Cisco ASDM ユーザ ガイド

バージョン 6.0(3)

Customer Order Number:
Text Part Number: OL-14981-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

ASDM ユーザ ガイド

CONTENTS

はじめに

*ASDM ユーザ ガイド*には、ASDM オンライン ヘルプ システムで利用できる情報が含まれています。ここでは、次のトピックを扱います。

関連資料

詳細については、次のマニュアルを参照してください。

- 『*Cisco ASDM Release Notes*』
- 『*Cisco Security Appliance Command Line Configuration Guide*』
- 『*Cisco Security Appliance Command Reference*』
- 『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』
- 『*Cisco ASA 5505 Series Adaptive Security Appliance Getting Started Guide*』
- 『*Cisco ASA 5500 Series Release Notes*』
- 『*Cisco Security Appliance Logging Configuration and System Log Messages*』
- 『*Open Source Software Licenses for ASA and PIX Security Appliances*』

表記法

コマンドの説明では、次の表記法を使用しています。

- 波カッコ（{ }）は、選択すべき必須の要素を示します。
- 角カッコ（[ ]）は、省略可能な要素を示します。
- 縦線（|）は、二者択一、つまりどちらか一方を選択する要素を区切ります。
- 記載されているとおりに入力するコマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。

例を挙げて説明する場合は、次の表記法を使用しています。

- 画面に表示される情報は、`screen` フォントで示しています。

- ユーザが入力する情報は、**太字の** `screen` フォントで示しています。
- ユーザが値を指定する変数は、*イタリック体の* `screen` フォントで示しています。

（注） 「*注釈*」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報については、次の URL で毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

ASDM の概要

ASDM は、セキュリティ アプライアンスのソフトウェアの設定およびモニタリングに使用する、ブラウザ ベースの Java アプレットです。ASDM は、適応型セキュリティ アプライアンスによってロードされ、デバイスの設定、モニタリング、および管理に使用することができます。

(注) ASDM の実行時にオペレーティング システムのカラー スキームを変更した場合は、ASDM を再起動してください。再起動しないと、一部の ASDM 画面が正常に表示されないことがあります。

この項では、次のトピックについて取り上げます。

このリリースの新機能

このリリースの ASDM は、ASA バージョン 8.0(2) 以降のバージョンの 8.0(x) と互換性があります。以前の適応型セキュリティ アプライアンス リリースでは動作しません。新しいプラットフォームおよび ASDM 機能のリストについては、Cisco.com の『*Cisco ASDM Release Notes*』を参照してください。

複数 ASDM セッションのサポート

ASDM では複数の PC やワークステーションでそれぞれブラウザ セッションを開き、同じ適応型セキュリティ アプライアンス ソフトウェアを使用できます。1 つの適応型セキュリティ アプライアンスで、シングル ルーテッド モードの ASDM 並行セッションを 5 つまでサポートできます。PC またはワークステーションはそれぞれ、指定した適応型セキュリティ アプライアンスのセッションを 1 つだけブラウザで実行できます。マルチ コンテキスト モードの場合、コンテキストあたり 5 つの ASDM 並行セッションを実行でき、適応型セキュリティ アプライアンスあたり合計 32 セッションまで接続できます。

警告

現在の警告情報を表示するには、Cisco.com の Bug Toolkit を使用してください。次の URL から、Bug Toolkit にアクセスできます。

https://tools.cisco.com/Support/BugToolKit/action.do

サポートされていないコマンド

この項では、次のトピックについて取り上げます。

- 「無視される表示専用コマンド」（P.1-2）
- 「サポート対象外のコマンドによる影響」（P.1-3）

適応型 ASDM のコマンドはほとんどすべて セキュリティ アプライアンス でサポートされますが、既存のコンフィギュレーションのコマンドの一部は ASDM で無視される場合があります。これらのコマンドのほとんどが、コンフィギュレーションに残っている可能性があります。詳細については、Show Commands Ignored by ASDM on Device を参照してください。

また、ASDM では、255.255.0.255 のように連続していないサブネット マスクはサポートされていません。たとえば、次のように使用することはありません。

```
ip address inside 192.168.2.1 255.255.0.255
```

無視される表示専用コマンド

表 1-1 には、CLI で追加した場合に ASDM のコンフィギュレーションでサポートしているものの、ASDM で追加または編集ができないコマンドのリストが表示されています。ASDM で無視されるコマンドは ASDM の GUI に一切表示されません。表示専用コマンドは GUI に表示されますが、編集はできません。

表 1-1　サポート対象外のコマンド リスト

サポートされていないコマンド	ASDM の動作
access-list	未使用の場合は無視
capture	無視されます
dns-guard	無視されます
eject	サポートされていません
established	無視されます
failover timeout	無視されます
icmp-unreachable rate-limit	無視されます
ipv6、すべての IPv6 アドレス	無視されます
pager	無視されます
pim accept-register route-map	無視されます。ASDM では **list** オプションだけ設定可。
prefix-list	OSPF 領域で使用されていない場合は無視
route-map	無視されます

表 1-1　サポート対象外のコマンド リスト （続き）

サポートされていないコマンド	ASDM の動作

service-policy global	**match access-list** クラスで使用されている場合は無視。次に例を示します。
	`access-list myacl line 1 extended permit ip any any`
	`class-map mycm`
	`match access-list mycl`
	`policy-map mypm`
	`class mycm`
	`inspect ftp`
	`service-policy mypm global`

sysopt nodnsalias	無視されます
sysopt uauth allow-http-cache	無視されます
terminal	無視されます

サポート対象外のコマンドによる影響

ASDM が既存の実行コンフィギュレーションをロードし、IPv6 関連のコマンドを検出した場合、ASDM は IPv6 をサポートしていないことを伝えるダイアログボックスを表示します。ASDM では IPv6 コマンドを設定できませんが、その他のコンフィギュレーションは使用できます。

既存の実行コンフィギュレーションを ASDM にロードした場合、そこにサポート対象外のコマンドがあっても、ASDM の操作には影響しません。サポート対象外のコマンドのリストを表示するには、[Tools] > [Show Commands Ignored by ASDM on Device] を選択します。

alias コマンドが含まれる既存の実行コンフィギュレーションをロードすると、ASDM はモニタリング専用モードになります。このモードでは、次の機能にアクセスできます。

- モニタリング エリア
- CLI ツール。CLI ツールにアクセスするには、[Tools] > [Command Line Interface] を選択します。

モニタリング専用モードを終了させるには、CLI ツールを使用するか、適応型セキュリティ アプライアンス コンソールにアクセスして **alias** コマンドを削除します。**alias** コマンドの代わりに外部 NAT を使用できます。詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

（注） モニタリング専用モードになる場合が他にもあります。ASDM のメイン ウィンドウ下部のステータス バーに表示されているユーザ アカウント権限レベルを、システム管理者が 3 以下に設定した場合です。詳細については、[Configuration] > [Properties] > [Device Administration] > [User Accounts] を選択し、[Configuration] > [Device Access] > [AAA Access] を選択します。

ASDM インターフェイスについて

ASDM インターフェイスは、適応型セキュリティ アプライアンスがサポートしているさまざまな機能に簡単にアクセスできるように設計されています。ASDM インターフェイスには次のコンポーネントが含まれます。

- メニュー バー：ファイル、ツール、ウィザード、およびヘルプにすばやくアクセスできます。メニュー項目の多くにはキーボード ショートカットもあります。

- ツールバー：ASDM のナビゲーションを行います。ツールバーからホーム ペイン、コンフィギュレーション ペイン、およびモニタリング ペインにアクセスできます。また、ヘルプの参照やペイン間のナビゲーションもできます。
- ステータス バー：時刻、接続ステータス、ユーザ、および権限レベルを表示します。
- [Device List]：ASDM からアクセスできるデバイスのリストを表示します。詳細については、「デバイス リスト」（P.1-10）を参照してください。
- [Addresses/Services/Time Ranges]：アクセス、フィルタ、およびサービス ルールの作成時に、ルール テーブルで使用できるさまざまなオブジェクトを示す、ドッキング可能なペインを表示します。
- [Navigation]：コンフィギュレーション画面とモニタリング画面のナビゲーションを行うドッキング可能なペインを表示します。

（注）　ウィザード、コンフィギュレーション ペイン、およびモニタリング ペインなど、GUI のさまざまな部分にツールのヒントが追加されました。

この項では、次のトピックについて取り上げます。

メニュー

ASDM のメニューには、マウスまたはキーボードを使用してアクセスできます。キーボードを使用したメニュー バーへのアクセスの詳細については、「キーボード ショートカット」（P.1-11）を参照してください。ASDM には次のメニューがあります。

[File] メニュー

[File] メニューでは、適応型セキュリティ アプライアンス コンフィギュレーションを管理します。次の項目が含まれます。

- [Refresh ASDM with the Running Configuration on the Device]：実行コンフィギュレーションのコピーを ASDM にロードします。ASDM に現在の実行コンフィギュレーションのコピーがあるかどうかを確認するには、[Refresh] をクリックします。

- [Reset Device to the Factory Default Configuration]：コンフィギュレーションを出荷時の初期状態に戻します。詳細については、[Reset Device to the Factory Default Configuration] ダイアログボックスを参照してください。
- [Show Running Configuration in New Window]：現在の実行コンフィギュレーションを新しいウィンドウに表示します。
- [Save Running Configuration to Flash]：実行コンフィギュレーションのコピーをフラッシュ メモリに書き込みます。
- [Save Running Configuration to TFTP Server]：現在の実行コンフィギュレーション ファイルのコピーを TFTP サーバに保存します。詳細については、[Save Running Configuration to TFTP Server] ダイアログボックスを参照してください。
- [Save Running Configuration to Standby Unit]：プライマリ装置の実行コンフィギュレーション ファイルのコピーを、フェールオーバー スタンバイ装置の実行コンフィギュレーションに送信します。
- [Save Internal Log Buffer to Flash]：内部ログ バッファをフラッシュ メモリに保存します。
- [Print]：現在のページを印刷します。ルールを印刷する場合、ページを横方向にすることをお勧めします。Internet Explorer を使用している場合は、署名付きアプレットを最初に承認した時点で印刷権限が与えられています。
- [Clear ASDM Cache]：ASDM のローカル イメージを削除します。ASDM に接続すると、ASDM によりイメージがローカルにダウンロードされます。
- [Clear Internal Log Buffer]：システム ログ メッセージ バッファを空にします。
- [Exit]：ASDM を閉じます。

[View] メニュー

[View] メニューでは、ASDM インターフェイスのさまざまな部分を表示できます。現在のビューに応じた特定の項目が表示されます。現在のビューに表示できない項目は選択できません。たとえば、[Latest ASDM Syslog Messages] ペインは、ホーム ビューが表示されている場合のみ使用できます。

- [Home]：ホーム ビューを表示します。
- [Configuration]：コンフィギュレーション ビューを表示します。
- [Monitoring]：モニタリング ビューを表示します。
- [Device List]：ドッキング可能なペインにあるデバイスのリストを表示します。詳細については、「デバイス リスト」（P.1-10）を参照してください。
- [Navigation]：コンフィギュレーション ビューおよびモニタリング ビューでナビゲーション ペインを表示または非表示にします。
- [Latest ASDM Syslog Messages]：ホーム ビューの [Latest ASDM Syslog Messages] ペインを表示または非表示にします。
- [Addresses]：[Addresses] ペインを表示または非表示にします。[Addresses] ペインは、コンフィギュレーション ビューの [Access Rules]、[NAT Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでだけ使用できます。
- [Services]：[Services] ペインを表示または非表示にします。[Services] ペインは、コンフィギュレーション ビューの [Access Rules]、[NAT Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでだけ使用できます。
- [Time Ranges]：[Time Ranges] ペインを表示または非表示にします。[Time Ranges] ペインは、コンフィギュレーション ビューの [Access Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでだけ使用できます。

- [Global Pools]：[Global Pools] ペインを表示または非表示にします。[Global Pools] ペインは、コンフィギュレーション ビューの [NAT Rules] ペインでだけ使用できます。
- [Find]：機能や ASDM Assistant などの項目を検索します。
- [Back]：詳細については、共通ボタンを参照してください。
- [Forward]：詳細については、共通ボタンを参照してください。
- [Reset Layout]：レイアウトをデフォルト設定に戻します。
- [Office Look and Feel]：画面のフォントと色を Microsoft Office 設定に変更します。

[Tools] メニュー

[Tools] メニューには ASDM で使用する次の一連のツールがあります。

- [Command Line Interface]：コマンドを適応型セキュリティ アプライアンスに送信し、結果を表示するテキスト ベースのツールを提供します。詳細については、[コマンドライン インターフェイス] ダイアログボックスを参照してください。
- [Show Commands Ignored by ASDM on Device]：ASDM で考慮されていない、サポート対象外のコマンドを表示します。詳細については、[Show Commands Ignored by ASDM on Device] ダイアログボックスを参照してください。
- [Packet Tracer]：指定した送信元アドレスとインターフェイスから宛先まで、パケットをトレースできます。プロトコルおよびポートをデータ タイプに関わりなく指定でき、そこで実行された処理の詳細データを含むパケットの一部始終を表示できます。詳細については、[Packet Tracer] ダイアログボックスを参照してください。
- [Ping]：適応型セキュリティ アプライアンスおよび関係する通信リンクのコンフィギュレーションや動作を検証し、他のネットワーク デバイスの基本的なテストを実行できます。詳細については、[ping] ダイアログボックスを参照してください。
- [Traceroute]：パケットが宛先に到達するまでのルートを特定します。詳細については、[traceroute] ダイアログボックスを参照してください。
- [File Management]：フラッシュ メモリに保存されたファイルを表示、移動、コピー、および削除できます。また、フラッシュ メモリにディレクトリを作成することもできます。詳細については、[File Management] ダイアログボックスを参照してください。また、[File Transfer] ダイアログボックスを表示して、TFTP、フラッシュ メモリ、ローカル PC など、さまざまなファイル システム間でファイルを転送できます。
- [Upgrade Software from Local Computer]：適応型セキュリティ アプライアンス イメージ、ASDM イメージ、または PC 上の別のイメージを選択して、そのファイルをフラッシュ メモリにアップロードできます。詳細については、[Upgrade Software from Local Computer] ダイアログボックスを参照してください。
- [Upgrade Software from Cisco.com]：ウィザードを使用して適応型セキュリティ アプライアンス ソフトウェアおよび ASDM ソフトウェアをアップグレードできます。詳細については、Upgrade Software from Cisco.com Wizard を参照してください。
- [Upload ASDM Assistant Guide]：ASDM Assistant で使用する情報を含む XML ファイルをフラッシュ メモリにアップロードできます。これらのファイルは Cisco.com からダウンロードできます。詳細については、[Upload ASDM Assistant Guide] ダイアログボックスを参照してください。
- [System Reload]：ASDM を再起動し、保存したコンフィギュレーションをメモリにリロードすることができます。詳細については、[System Reload] ダイアログボックスを参照してください。
- [Administrator's Alerts to Clientless SSL VPN Users]：管理者が、クライアントレス SSL VPN ユーザにアラート メッセージを送信できるようにします。詳細については、[管理者によるクライアントレス SSL VPN ユーザへのアラート] ダイアログボックスを参照してください。

- [Preferences]：セッション間での特定の ASDM 機能の動作を変更します。詳細については、[Preferences] ダイアログボックスを参照してください。
- [ASDM Java Console]：Java コンソールを表示します。詳細については、[ASDM Java Console] ダイアログボックスを参照してください。

[Wizards] メニュー

[Wizards] メニューにより、さまざまな機能を設定するウィザードを実行できます。

- [Startup Wizard]：このウィザードでは、適応型セキュリティ アプライアンスの初期設定を順を追って進めます。詳細については、「Startup Wizard の使用」を参照してください。
- [IPSec VPN Wizard]：このウィザードでは、適応型セキュリティ アプライアンスに IPSec VPN ポリシーを設定できます。詳細については、VPN Wizard を参照してください。
- [SSL VPN Wizard]：このウィザードでは、適応型セキュリティ アプライアンスに SSL VPN ポリシーを設定できます。詳細については、VPN Wizard を参照してください。
- [High Availability and Scalability Wizard]：このウィザードでは、適応型セキュリティ アプライアンスにフェールオーバーを設定できます。詳細については、「ハイ アベイラビリティ」を参照してください。
- [Packet Capture Wizard]：このウィザードでは、適応型セキュリティ アプライアンスにパケット キャプチャを設定できます。このウィザードは、入出力インターフェイスのそれぞれでパケット キャプチャを 1 回実行します。キャプチャの実行後、キャプチャをコンピュータに保存し、パケット アナライザを使用してキャプチャを調査および分析できます。詳細については、「Packet Capture Wizard」を参照してください。

[Window] メニュー

[Window] メニューを使用して、ASDM のウィンドウ間を移動できます。アクティブなウィンドウが選択されたウィンドウとして表示されます。

[Help] メニュー

[Help] メニューでは、オンライン ヘルプへのリンクの他に、ASDM と適応型セキュリティ アプライアンスの情報も提供されます。

- [Help Topics]：新しいブラウザ ウィンドウを開いて、左側のフレームに目次、画面名、および索引で構成されたヘルプを表示します。これらの方法を使用して、任意のトピックのヘルプを検索するか、[Search] タブを使用して検索します。
- [Help for Current Screen]：その画面に関する状況依存ヘルプを開きます。ウィザードは、現在開いている画面、ペイン、またはダイアログボックスのヘルプを表示します。また、疑問符（**?**）のヘルプ アイコンをクリックして、状況依存ヘルプを表示することもできます。
- [Release Notes]：Cisco.com にある最新バージョンの『*Cisco ASDM Release Notes*』を開きます。リリース ノートには、ASDM のソフトウェアとハードウェア要件の最新情報、およびソフトウェア変更に関する最新情報が記載されています。
- [Getting Started]：Getting Started ヘルプ項目が開き、ASDM の使用をすぐに開始できます。
- [VPN 3000 Migration Guide]：Cisco.com にあるこのマニュアルが開き、バージョン 7.2 からバージョン 8.0(2) へのアップグレードに利用できます。
- [Glossary]：用語と略語の定義が含まれます。

- [Feature Search]：ASDM の機能を検索できます。検索機能は、各ペインのタイトルをすべて検索して一致項目を表示します。ハイパーリンクをクリックすると、該当ペインがただちに表示されます。検出された異なる 2 種類のペインをすばやく切り替えるには、[Back] および [Forward] ボタンをクリックします。ASDM の「ツールバー」（P.1-8）で [Search] アイコンをクリックすることもできます。
- [How Do I?]：ASDM Assistant が開き、特定のタスクの実行に関する詳細について、Cisco.com からダウンロード可能なコンテンツを検索できます。
- [Icon Legend]：ASDM で使用するアイコンとそれらの機能を説明したリストを表示します。
- [About Cisco Adaptive Security Appliance (ASA)]：ソフトウェア バージョン、ハードウェア構成、スタートアップ時にロードされるコンフィギュレーション ファイルやソフトウェア イメージなど、適応型セキュリティ アプライアンスに関する情報を表示します。これらはトラブルシューティングの際に役立つ情報です。
- [About Cisco ASDM 6.0]：ソフトウェア バージョン、ホスト名、権限レベル、オペレーティング システム、デバイス タイプ、Java のバージョンなど、ASDM に関する情報を表示します。

ツールバー

メニューバーの下にあるツールバーから、ホーム ビュー、コンフィギュレーション ビュー、およびモニタリング ビューにアクセスできます。また、マルチ コンテキスト モードでシステムとセキュリティ コンテキストを選択したり、ナビゲーションおよびその他よく使用する機能を実行できます。

- [System/Contexts]：左側のペインのコンテキストのリストを開くには、下矢印をクリックし、コンテキストのドロップダウン リストを元に戻すには、上矢印をクリックします。このリストが展開されているときに左矢印をクリックするとペインは折りたたまれ、右矢印をクリックするとペインが元に戻ります。システムを管理するには、リストから [System] を選択します。コンテキストを管理するには、リストから該当するコンテキストを選択します。
- [Home]：インターフェイスのステータス、実行中のバージョン、ライセンス情報、パフォーマンスなど、適応型セキュリティ アプライアンスの重要な情報を表示できる [Home] ペインを表示します。詳細については、「[Home] ペイン」を参照してください。マルチ モードの場合、[Home] ペインはありません。
- [Configuration]：適応型セキュリティ アプライアンスを設定します。左側のペインで、その機能を設定する機能ボタンを選択します。
- [Monitoring]：適応型セキュリティ アプライアンスをモニタします。左側のペインで、その機能をモニタする機能ボタンを選択します。
- [Back]：直前に表示した ASDM ペインに戻ります。
- [Forward]：直前に表示した ASDM ペインに進みます。
- [Search]：ASDM の機能を検索できます。検索機能は、各ペインのタイトルをすべて検索して一致項目を表示します。ハイパーリンクをクリックすると、該当ペインがただちに表示されます。検索された異なる 2 種類のペインをすばやく切り替えるには、[Back] または [Forward] ボタンをクリックします。詳細については、ASDM Assistant を参照してください。
- [Refresh]：現在の実行コンフィギュレーションで ASDM をリフレッシュします。ただし、モニタリング グラフはいずれもリフレッシュしません。
- [Save]：書き込みアクセスが可能なコンテキストに限り、実行コンフィギュレーションをスタートアップ コンフィギュレーションとして保存します。
- [Help]：その時点で表示されている画面の状況依存ヘルプを表示します。

ASDM Assistant

[ASDM Assistant] ダイアログボックスでは、タスクに応じた ASDM の使用方法のヘルプを検索できます。最初に、[Tools] メニューから ASDM Assistant Guide をアップロードして、ヘルプを使用できるようにする必要があります。詳細については、[Upload ASDM Assistant Guide] ダイアログボックスを参照してください。

このダイアログボックスには、2 つのペインで構成されるウィンドウが表示されます。左側のペインではクエリーを入力でき、そのクエリーによって得られた情報へのリンクが一覧表示されます。右側のペインには、選択した情報やその他のリンクが表示されます。

[How Do I?] タブでは、検索対象の特定の領域を選択できます。[Search] タブでは、詳細情報が必要な用語や機能を入力し、必要とする結果のタイプを指定します。

[How Do I?] タブ

フィールド

- [Show tasks]：必要な情報のタイプをドロップダウン リストから選択します。選択できるタイプは、[Security Policy]、[ASDM]、[Administration]、および [All] です。

[Search] タブ

フィールド

- [For]：詳細情報が必要な用語を入力します。
- [How Do I?]：特定のタスクの実行に関する詳細について、Cisco.com からダウンロード可能なコンテンツを含めるには、このチェックボックスをオンにします。
- [Features]：詳細情報が必要な機能を含める場合はオンにします。
- [Include]：含める情報のオプションを [Exact Phrase]、[Any Word]、または [All Words] から選択します。
- [Exclude]：除外する情報を指定します。
- [Search]：クエリーを開始する場合はクリックします。

ステータスバー

ステータス バーは [ASDM] ウィンドウの下に表示され、左から右に次の領域が表示されます。

- [Status]：コンフィギュレーションのステータス（「Device configuration loaded successfully」など）を表示します。
- [User Name]：ASDM ユーザのユーザ名を表示します。ユーザ名なしでログインするとユーザ名は「admin」になります。
- [User Privilege]：ASDM ユーザの特権を示します。
- [Commands Ignored by ASDM]：ASDM で処理されなかったコンフィギュレーションのコマンドのリストを表示するには、アイコンをクリックします。これらのコマンドはコンフィギュレーションから削除されません。詳細については、「Show Commands Ignored by ASDM on Device」を参照してください。
- [Status of Connection to Device]：と適応型セキュリティ アプライアンスに対する ASDM の接続ステータスを示します。詳細については、「Connection to Device」を参照してください。

- [Save to Flash Needed]：ASDM でコンフィギュレーションを変更したが、まだ実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存する必要があることを示します。
- [Refresh Needed]：適応型セキュリティ アプライアンスでコンフィギュレーションが変更されたため（CLI を使用してコンフィギュレーションを変更した場合など）、適応型セキュリティ アプライアンスから ASDM にコンフィギュレーションをリフレッシュする必要があることを示します。
- [SSL Secure]：SSL を使用しているため、ASDM への接続が安全であることを示します。
- [Time]：適応型セキュリティ アプライアンスを含むスイッチで設定された時刻を示します。

Connection to Device

ASDM は適応型セキュリティ アプライアンスとの接続を常に保ち、最新のモニタリング データおよびホーム ペイン データを表示します。このダイアログボックスに接続ステータスが表示されます。コンフィギュレーションを変更する場合、変更している間 ASDM は接続をもう一つ開き、変更が終わるとその接続を閉じますが、このダイアログボックスには 2 つ目の接続は表示されません。

デバイス リスト

[Device List] はドッキング可能なペインです。ヘッダーにある 4 つのボタンは、それぞれクリックすると、ペインを最大化または復元、移動可能なフローティング ペインに変更、ペインを非表示、またはペインを閉じることができます。このペインはホーム、コンフィギュレーション、モニタリング、およびシステムの各ビューで使用できます。このペインを使用して、別のデバイスに切り替えることができますが、そのデバイスでも現在実行しているものと同じバージョンの ASDM が実行されている必要があります。ペインを完全に表示するには、少なくとも 2 つのデバイスがリストに表示されている必要があります。

（注） 異なるバージョンの ASDM を実行している別のデバイスに切り替えることはできません。

このペインを使用して別のデバイスに接続するには、次の手順を実行します。

ステップ 1　[Add] をクリックしてリストに別のデバイスを追加します。

[Add Device] ダイアログボックスが表示されます。

ステップ 2　[Device/IP Address/Name] フィールドで、デバイス名またはデバイスの IP アドレスを入力し、[OK] をクリックします。

ステップ 3　リストから選択したデバイスを削除するには、[Delete] をクリックします。

ステップ 4　[Connect] をクリックして別のデバイスに接続します。

[Enter Network Password] ダイアログボックスが表示されます。

ステップ 5　ユーザ名とパスワードを該当するフィールドに入力し、[Login] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

共通ボタン

これらのボタンは、多くの ASDM ペインに表示されます。

- [Apply] : ASDM での変更内容を適応型セキュリティ アプライアンスに送信し、実行コンフィギュレーションに適用します。
- [Save] : 実行コンフィギュレーションのコピーをフラッシュ メモリに書き込みます。
- [Reset] : 変更内容を破棄して、変更前に表示されていた情報、または [Refresh] や [Apply] を最後にクリックした時点の表示情報に戻します。[Reset] をクリックした後、[Refresh] をクリックして、現在の実行コンフィギュレーションの情報が表示されていることを確認します。
- [Restore Default] : 選択した設定をクリアしてデフォルト設定に戻します。
- [Cancel] : 変更内容を破棄して、前のペインに戻ります。
- [Enable] : 機能について読み取り専用の統計情報を表示します。
- [Close] : 開いているダイアログボックスを閉じます。
- [Clear] : フィールドまたはボックスから情報を削除します。または、チェックボックスをオフにします。
- [Back] : 前のペインに戻ります。
- [Forward] : 次のペインに進みます。
- [Help] : 選択したペインのヘルプを表示します。

キーボード ショートカット

キーボードを使用して ASDM インターフェイスをナビゲートできます。

表 1-2 に、ASDM インターフェイスの 3 つの主要な領域間を移動するために使用できるキーボード ショートカットを示します。

表 1-2　ASDM のナビゲーション

表示対象	Windows/Linux	MacOS
Home Page	Ctrl+H	Shift+Command+H
コンフィギュレーション ページ	Ctrl+G	Shift+Command+G
モニタリング ページ	Ctrl+M	Shift+Command+M
Help	F1	Command+?
戻る	Alt+ 左矢印	Command+[
進む	Alt+ 右矢印	Command+]
表示のリフレッシュ	F5	Command+R

表 1-2　ASDM のナビゲーション （続き）

表示対象	Windows/Linux	MacOS
切り取り	Ctrl+X	Command+X
コピー	Ctrl+C	Command+C
貼り付け	Ctrl+V	Command+V
コンフィギュレーションの保存	Ctrl+S	Command+S
ポップアップ メニュー	Shift+F10	—
セカンダリ ウィンドウを閉じる	Alt+F4	Command+W
検索	Ctrl+F	Command+F
終了	Alt+F4	Command+Q
テーブルまたはテキスト領域の終了	Ctrl_Shift または Ctrl+Shift+Tab	Ctril+Shift または Ctrl+Shift+Tab

表 1-3 は、ペイン内部のナビゲーションに使用できるキーボード ショートカットの一覧です。

表 1-3　フォーカスの移動

フォーカスの移動先	キー
次のフィールド	Tab
前のフィールド	Shift+Tab
次のフィールド（テーブル内にフォーカスがある場合）	Ctrl+Tab
前のフィールド（テーブル内にフォーカスがある場合）	Shift+Ctrl+Tab
次のタブ（タブにフォーカスがある場合）	右矢印
前のタブ（タブにフォーカスがある場合）	左矢印
テーブル内の次のセル	Tab
テーブル内の前のセル	Shift+Tab
次のペイン（複数のペインが表示されている場合）	F6
前のペイン（複数のペインが表示されている場合）	Shift+F6

表 1-4 は、Log Viewer で使用できるキーボード ショートカットの一覧です。

表 1-4　Log Viewer のキーボード ショートカット

表示対象	Windows/Linux	MacOS
Real-Time Log Viewer の一時停止および再開	Ctrl+U	Command+.
ログ バッファ ウィンドウのリフレッシュ	F5	Command+R
内部ログ バッファのクリア	Ctrl+Delete	Command+Delete
選択したログ エントリのコピー	Ctrl+C	Command+C
ログの保存	Ctrl+S	Command+S
印刷	Ctrl+P	Command+P
セカンダリ ウィンドウを閉じる	Alt+F4	Command+W

表 1-5 は、メニュー項目へのアクセスに使用できるキーボード ショートカットの一覧です。

表 1-5　Log Viewer のキーボード ショートカット

アクセス対象	Windows/Linux
メニュー バー	Alt
次のメニュー	右矢印
前のメニュー	左矢印
次のメニュー オプション	下矢印
前のメニュー オプション	上矢印
選択したメニュー オプション	Enter

拡張スクリーン リーダ サポートのイネーブル化

デフォルトでは、Tab キーを押してペイン内を順に移動するとき、ラベルと説明にはタブは移動しません。JAWS のような一部のスクリーン リーダだけが、フォーカスのある画面オブジェクトを読み取ります。拡張スクリーン リーダ サポートをイネーブルにすると、ラベルと説明にもタブを移動させることができます。

拡張スクリーン リーダ サポートをイネーブルにするには、次の手順を実行します。

ステップ 1　ASDM アプリケーションのメイン ウィンドウで、[Tools] > [Preferences] を選択します。

[Preferences] ダイアログボックスが表示されます。

ステップ 2　[General] タブで、[Enable screen reader support] チェックボックスをオンにします。

ステップ 3　[OK] をクリックします。

ステップ 4　スクリーン リーダ サポートをアクティブにするには、ASDM を再起動します。

フォルダの整理

コンフィギュレーション画面およびモニタリング画面のナビゲーション ツリーに含まれる一部のノードには、関連付けられたコンフィギュレーション ペインやモニタリング ペインがありません。これらは、関連するコンフィギュレーション項目やモニタリング項目を整理するために使用します。これらのフォルダをクリックすると、右側のペインにサブ項目のリストが表示されます。サブ項目の名前をクリックするとその項目に移動できます。

ヘルプ ウィンドウについて

この項では、次のトピックについて取り上げます。

- 「ヘッダー ボタン」（P.1-14）
- 「ブラウザ ウィンドウ」（P.1-14）

ヘッダー ボタン

該当するボタンをクリックして、必要な情報を取得します。

- [About ASDM]：ASDM に関する情報を表示します。ホスト名、バージョン番号、デバイス タイプ、適応型セキュリティ アプライアンスのソフトウェア バージョン番号、権限レベル、ユーザ名、使用するオペレーティング システムなどが含まれます。
- [Search]：オンライン ヘルプ項目から情報を検索します。
- [Using Help]：オンライン ヘルプの最も効率的な使用方法について説明します。
- [Glossary]：ASDM および適応型セキュリティ アプライアンス デバイスで使用されている用語のリストを表示します。
- 左側のペインのリンク：オンライン ヘルプ項目間を移動します。
- [Contents]：目次を表示します。
- [Screens]：ヘルプ ファイルのリストを画面の名前ごとに表示します。
- [Index]：ASDM のオンライン ヘルプにあるヘルプ項目の索引を表示します。
- 右側のペインのヘルプ項目：選択した項目のヘルプを表示します。

ブラウザ ウィンドウ

ヘルプを開いて、すでにヘルプ ページを表示している場合、同じブラウザ ウィンドウに新しいヘルプ ページが表示されます。ヘルプ ページが表示中でなければ、新しいブラウザ ウィンドウにヘルプ ページが表示されます。

Internet Explorer がデフォルト ブラウザの場合、ブラウザの設定に応じて、ヘルプ ページが直前に使用していたウィンドウに表示される場合と、新しいウィンドウが開いて表示される場合があります。この Internet Explorer の動作は、[Tools] > [Internet Options] > [Advanced] > [Reuse windows for launching shortcuts] の順に選択して設定できます。

[Home] ペイン

ASDM ホーム ペインでは、適応型セキュリティ アプライアンスに関する重要な情報を表示できます。ホーム ペインのステータス情報は 10 秒間隔で更新されます。このペインには通常、[Device Dashboard] と [Firewall Dashboard] の 2 つのタブがあります。

適応型セキュリティ アプライアンスに CSC SSM がインストールされている場合、ホーム ペインには [Content Security] タブも表示されます。この追加されたタブには、CSC SSM のソフトウェアに関するステータス情報が表示されます。

適応型セキュリティ アプライアンスに IPS ソフトウェアがインストールされている場合、ホーム ペインには [Intrusion Prevention] タブも表示されます。この追加されたタブには、IPS ソフトウェアに関するステータス情報が表示されます。

この項では、次のトピックについて取り上げます。

- 「[Device Dashboard] タブ」（P.1-15）
- 「[Firewall Dashboard] タブ」（P.1-17）
- 「[Content Security] タブ」（P.1-19）
- 「[Intrusion Prevention] タブ」（P.1-21）

フィールド

- [Latest ASDM Syslog Messages] : 適応型セキュリティ アプライアンスが生成した最新のシステム メッセージが 100 件まで表示されます。

  ロギング ペインを展開するには、ヘッダーにある正方形のアイコンをクリックします。デフォルトのサイズに戻すには、ヘッダーにある二重正方形のアイコンをクリックします。ペインのサイズを変更するには、境界線を上または下にドラッグします。また、イベントを右クリックして次の操作を実行できます。[Clear Content] をクリックすると現在のメッセージをクリアします。[Save Content] をクリックすると現在のメッセージを PC 上のファイルに保存します。[Copy] をクリックすると内容をコピーします。[Color Settings] をクリックすると、システム メッセージの背景と前景の色を重大度に応じて変更できます。ヘッダーの右側にある 4 つのボタンは、それぞれクリックすると、ペインを最大化または復元、移動可能なフローティング ペインに変更、ペインを非表示、またはペインを閉じることができます。

- [Enable Logging] : ロギングをイネーブルにし、システム ログ メッセージを表示する場合にクリックします。
- [Stop message display] : システム ログ メッセージの表示更新を停止する場合は、右側にある赤いアイコンをクリックします。
- [Resume message display] : システム ログ メッセージの表示更新を続行する場合は、右側にある緑のアイコンをクリックします。
- [Configure ASDM Syslog Filters] : 右側にあるフィルタ アイコンをクリックすると、[Logging Filters] ペインが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

[Device Dashboard] タブ

[Device Dashboard] タブでは、インターフェイスのステータス、実行中のバージョン、ライセンス情報、パフォーマンスなど、適応型セキュリティ アプライアンスの重要な情報を一目で確認できます。

フィールド

- [Device Information] : デバイス情報を表示する 2 つのタブが含まれます。
  - [General] : 次の情報が表示されます。

    [Host Name] : *表示専用*。適応型セキュリティ アプライアンスのホスト名を示します。ホスト名の設定方法については、「Device Name/Password」を参照してください。

    [ASA Version] : *表示専用*。適応型セキュリティ アプライアンス ソフトウェアのバージョンを示します。

    [Device Uptime] : *表示専用*。適応型セキュリティ アプライアンスの実行経過時間を示します。

    [ASDM Version] : *表示専用*。ASDM バージョンを示します。

    [Device Type] : *表示専用*。適応型セキュリティ アプライアンスのモデルを示します。

[Firewall Mode]：*表示専用*。ファイアウォール モード（「ルーテッド」または「トランスペアレント」）を示します。詳細については、「ファイアウォール モードの概要」を参照してください。

[Total Flash]：*表示専用*。使用可能なフラッシュ メモリの総容量を示します。

[Context Mode]：*表示専用*。コンテキスト モード（シングルまたはマルチ）を表示します。詳細については、「セキュリティ コンテキストの概要」を参照してください。

[Total Memory]：*表示専用*。使用可能な RAM の総容量を示します。

- [License]：*表示専用*。適応型セキュリティ アプライアンスのライセンスされた機能のサポート レベルを示します。次の情報が表示されます。

  [License]：*表示専用*。ライセンスのタイプ（Base または Premium）を示します。

  時間ベースのライセンスの有効期限日数（該当する場合）。

  [Inside Hosts]：*表示専用*。内部ホスト（ASA 5505 専用）を示します。

  [Max VLANs]：*表示専用*。VLAN の最大許容数を示します。

  [Failover]：*表示専用*。フェールオーバー コンフィギュレーション（Active/Active または Active/Standby）を示します。

  [Security Contexts]：*表示専用*。セキュリティ コンテキストの最大許容数を示します。

  [Dual ISP Support]：*表示専用*。デュアル ISP サポート（イネーブルの場合。ASA 5505 専用）を示します。

  [GTP/GPRS]：*表示専用*。GTP/GPRS がイネーブルかディセーブルかを示します。

  [Encryption]：*表示専用*。イネーブルになっている暗号化のタイプを示します。

  [VPN Peers]：*表示専用*。VPN ピアの許容数を示します。VPN ピアがサポートされていない場合、このエントリは空白になります。

  [Clientless SSL VPN Peers]：*表示専用*。クライアントレス SSL VPN ピアの許容数を示します。

- [VPN Tunnels Status]：ルーテッド、シングル モードのみ。次の情報が表示されます。
  - [IKE]：*表示専用*。接続されている IKE トンネル数を示します。
  - [IPSec]：*表示専用*。接続されている IPSec トンネル数を示します。
  - [Clientless SSL VPN]：*表示専用*。接続されているクライアントレス SSL VPN トンネル数を示します。
  - [SSL VPN Client]：*表示専用*。接続されている SSL VPN クライアント トンネル数を示します。
- [System Resources Status]：CPU およびメモリの使用状況に関する次の統計情報を示します。
  - [CPU]：*表示専用*。現在の CPU 使用率を示します。
  - [CPU Usage (percent)]：*表示専用*。直前 5 分間の CPU 使用状況を示します。
  - [Memory]：*表示専用*。現在のメモリ使用量（MB 単位）を示します。
  - [Memory Usage (MB)]：*表示専用*。直前 5 分間のメモリ使用状況（MB 単位）を示します。
- [Interface Status]：インターフェイスごとのステータスを示します。インターフェイスの行を選択すると、入力および出力スループットが Kbps 単位でテーブルの下に表示されます。
  - [Interface]：*表示専用*。インターフェイス名を示します。
  - [IP Address/Mask]：*表示専用*。ルーテッド モードだけ。インターフェイスの IP アドレスおよびサブネット マスクを示します。

  - [Line]：*表示専用*。インターフェイスの管理ステータスを示します。アイコンが赤の場合は回線がダウン、緑の場合は回線がアップしています。
  - [Link]：*表示専用*。インターフェイスのリンク ステータスを示します。アイコンが赤の場合はリンクがダウン、緑の場合はリンクがアップしています。
  - [Kbps]：*表示専用*。インターフェイスを通過する現在のスループットの値（Kbps 単位）を示します。
- [Traffic Status]：すべてのインターフェイスにおける接続数/秒、およびセキュリティが最も低いインターフェイスにおけるトラフィック スループットのグラフを示します。
  - [Connections per Second Usage]：*表示専用*。直前 5 分間の UDP および TCP の接続数/秒を示します。このグラフには、現在の接続数が UDP と TCP のタイプごとに表示され、また合計値も表示されます。
  - [*Name* Interface Traffic Usage (Kbps)]：*表示専用*。最も低いセキュリティ インターフェイスのトラフィック スループットを示します。同じレベルのインターフェイスが複数ある場合、ASDM にはアルファベット順で先頭のインターフェイスが表示されます。このグラフには、現在のスループットが入力 Kbps と出力 Kbps のタイプごとに表示されます。
- [Latest ASDM Syslog Messages]：適応型セキュリティ アプライアンスが生成した最新のシステム メッセージを示します。
  - [Stop Message Display]：ASDM へのロギングを停止します。
  - [Resume Message Display]：ASDM へのロギングを続行します。
  - [Configure ASDM Filters]：ロギング フィルタを設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

[Firewall Dashboard] タブ

[Firewall Dashboard] タブでは、接続数、NAT 変換数、ドロップされたパケット数、攻撃数、使用状況ランキングの統計情報など、セキュリティ アプライアンスを通過するトラフィックに関する重要な情報を確認できます。

Traffic Overview の統計情報はデフォルトでイネーブルです。基本脅威検出をディセーブルにすると（「基本脅威検出の設定」（P.27-1）を参照）、このタブには [Enable] ボタンが表示されます。[Enable] ボタンを使用して基本脅威検出をイネーブルにできます。

Top 10 Access Rules もデフォルトでイネーブルになっています。アクセス ルールの脅威検出統計情報をディセーブルにすると（「脅威統計情報の設定」（P.27-4）を参照）、このタブには [Enable] ボタンが表示されます。[Enable] ボタンを使用してアクセス ルールの統計情報をイネーブルにできます。

Top Usage Status の統計情報はデフォルトでディセーブルです。このタブに表示されている [Enable] ボタンを使用して、この機能をイネーブルにできます。または、「脅威統計情報の設定」（P.27-4）に従ってイネーブルにすることもできます。[Top 10 Services Enable] ボタンを使用すると、ポートとプロト

コルの両方の統計情報がイネーブルになります（どちらも表示用にイネーブルにする必要があります）。[Top 10 Sources] ボタンおよび [Top 10 Destinations Enable] ボタンを使用すると、ホストの統計情報がイネーブルになります。

注意　統計情報をイネーブルにすると、イネーブルにする統計情報のタイプに応じて、セキュリティ アプライアンスのパフォーマンスが影響を受けます。ホストの統計情報をイネーブルにすると、パフォーマンスに大きな影響があります。トラフィックの負荷が高い場合は、このタイプの統計情報は一時的にイネーブルにすることを検討してください。ポートの統計情報をイネーブルにしても影響はそれほどありません。

フィールド

- [Traffic Overview]：*表示専用*。接続数、NAT 変換数、ドロップされたパケット数など、実行時の統計情報を示します。
  - [Connection Statistics]：*表示専用*。接続数と NAT 変換数を示します。
  - [Dropped Packets Rate]：*表示専用*。アクセス リストによる拒否およびアプリケーション インスペクションによってドロップされたパケット数/秒を示します。
  - [Possible Scan and SYN Attack Rates]：*表示専用*。ドロップ パケット数/秒を示します。これは、スキャン攻撃の一部として特定される場合と、不完全なセッションとして検出される場合（TCP SYN 攻撃やデータなし UDP セッション攻撃を検出した場合など）があります。
- [Top 10 Access Rules]：*表示専用*。最もアクティブなアクセス ルールを示します。
  - [Interval]：選択した間隔に基づいて情報を表示できます。選択できる値は、Last 1 hour、Last 8 hours、および Last 24 hours です。
  - [Based on]：*表示専用*。統計情報にパケットのヒット数だけが表示されていることを示します。
  - [Display]：同じ情報を 3 つの異なる形式（テーブル、円グラフ、棒グラフ）で表示できます。
  - [Interface]：ルールが適用されるインターフェイスを示します。
  - [Rule#]：使用されているルール番号を示します。
  - [Hits]：発生したパケット ヒット数を示します。
  - [Source]：送信元 IP アドレスを示します。
  - [Dest]：宛先 IP アドレスを示します。
  - [Service]：接続のサービス（プロトコルまたはポート）を示します。
  - [Action]：ルールが許可ルールであるか拒否ルールであるかを示します。

  テーブル ビューでは、リストからルールを選択して右クリックし、ポップアップ メニュー項目の [Show Rule] を表示できます。この項目を選択して [Access Rules] テーブルに移動し、テーブル内にあるそのルールを選択します。
- [Top Usage Status]：ホスト（送信元と宛先）およびポートとプロトコルの使用ステータスを表示します。
  - [Interval]：選択した間隔に基づいて情報を表示できます。選択できる値は、Last 1 hour、Last 8 hours、および Last 24 hours です。
  - [Based On]：統計情報をパケット ヒット数またはバイト単位で示します。
  - [Display]：同じ情報を 3 つの異なる形式（テーブル、円グラフ、棒グラフ）で表示できます。
  - [Top 10 Services]：TCP/UDP ポートと IP プロトコル タイプを合計した統計情報を含む、上位 10 位までのサービスの統計情報を示します。

– [Top 10 Sources]：上位 10 位までのホスト送信元アドレスを示します。
– [Top 10 Destinations]：上位 10 位までのホスト宛先アドレスを示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

[Content Security] タブ

[Content Security] タブでは、CSC（Content Security and Control）SSM に関する重要な情報を確認できます。このペインは、セキュリティ アプライアンスに CSC SSM がインストールされていないと表示されません。

CSC SSM の概要については、「CSC SSM について」を参照してください。

（注）　[Configuration] > [Trend Micro Content Security] > [CSC Setup] を選択して CSC Setup Wizard を完了していないと、[Home] > [Content Security] の下にあるペインにアクセスできません。代わりにダイアログボックスが表示され、この場所から Setup Wizard に直接アクセスできます。

フィールド

- [Device Information]：次の詳細情報が表示されます。
  – [Model]：*表示専用*。適応型セキュリティ アプライアンスにインストールされている SSM のタイプを示します。
  – [Mgmt IP]：*表示専用*。CSC SSM の管理インターフェイスの IP アドレスを示します。
  – [Version]：*表示専用*。CSC SSM ソフトウェアのバージョンを示します。
  – [Last Update]：*表示専用*。Trend Micro から取得した最後のソフトウェア アップデートの日付を示します。
  – [Daily Node #]：*表示専用*。過去 24 時間の間に CSC SSM のサービス対象になったネットワーク デバイス数を示します。ASDM によって深夜 0 時に更新されます。
  – [Base License]：*表示専用*。アンチウイルス、アンチスパイウェア、FTP ファイル ブロッキングなど、CSC SSM の基本機能に関するライセンス ステータスを示します。ライセンスの有効期限が表示されます。ライセンスの有効期限が切れている場合、期限が切れた日が表示されます。ライセンスが設定されていない場合、このフィールドには「Not Available」と表示されます。
  – [Plus License]：*表示専用*。アンチスパム、アンチフィッシング、電子メール コンテンツ フィルタリング、URL ブロッキングと URL フィルタリングなど、CSC SSM の高度な機能に関するライセンス ステータスを示します。ライセンスの有効期限が表示されます。ライセンスの有効期限が切れている場合、期限が切れた日が表示されます。ライセンスが設定されていない場合、このフィールドには「Not Available」と表示されます。

  - [Licensed Nodes]：*表示専用*。CSC SSM がライセンスによってサービス提供可能なネットワーク デバイスの最大数を示します。
- [System Resources Status] : CSC SSM の CPU およびメモリの使用状況に関する次の統計情報を示します。
  - [CPU]：*表示専用*。現在の CPU 使用率を示します。
  - [CSC SSM CPU Usage (percent)]：*表示専用*。直前 5 分間の CPU 使用状況を示します。
  - [Memory]：*表示専用*。現在のメモリ使用量（MB 単位）を示します。
  - [CSC SSM Memory Usage (MB)]：*表示専用*。直前 5 分間のメモリ使用状況（MB 単位）を示します。
- [Threat Summary]：CSC SSM により検出された脅威の集約データを示します。
  - [Threat Type]：*表示専用*。5 つの脅威タイプ（ウイルス、スパイウェア、ブロックされた URL、フィルタリングされた URL、およびスパム）を示します。
  - [Today]：*表示専用*。過去 24 時間に検出された脅威タイプごとの脅威の数を示します。
  - [Last 7 Days]：*表示専用*。過去 7 日間に検出された脅威タイプごとの脅威の数を示します。
  - [Last 30 Days]：*表示専用*。過去 30 日間以内に検出された脅威タイプごとの脅威の数を示します。
- [Email Scan]：スキャンされた電子メール、および検出された電子メール ウイルスとスパイウェアのグラフを示します。
  - [Email Scanned Count]：*表示専用*。スキャンされた電子メール数を、電子メール プロトコル（SMTP または POP3）ごとのそれぞれのグラフと、サポートされている電子メール プロトコルの両方を合計したグラフを示します。グラフには、10 秒間隔でデータが表示されます。
  - [Email Virus and Spyware]：*表示専用*。脅威タイプ（ウイルスまたはスパイウェア）ごとのグラフとしての電子メール スキャンで検出されたウイルスと電子メールの数を示します。グラフには、10 秒間隔でデータが表示されます。
- [Latest CSC Security Events]：CSC SSM から受信したセキュリティ イベント メッセージをリアルタイムに表示します。
  - [Time]：*表示専用*。イベントの発生時刻を示します。
  - [Source]：*表示専用*。脅威が検出された IP アドレスまたはホスト名を示します。
  - [Threat/Filter]：*表示専用*。脅威のタイプ、または、URL フィルタ イベントの場合は、イベントをトリガーしたフィルタを示します。
  - [Subject/File/URL]：*表示専用*。脅威が含まれる電子メールの件名、脅威が含まれる FTP ファイルの名前、またはブロックされたかフィルタリングされた URL を示します。
  - [Receiver/Host]：*表示専用*。脅威が含まれる電子メールの受信者、または脅威にさらされたノードの IP アドレスやホスト名を示します。
  - [Sender]：*表示専用*。脅威が含まれる電子メールの送信者を示します。
  - [Content Action]：*表示専用*。コンテンツを変更せずに配信、添付ファイルを削除、添付ファイルをクリーニングしてから配信するなど、メッセージやファイルのコンテンツに対して実行するアクションを示します。
  - [Msg Action]：*表示専用*。メッセージを変更せずに配信、添付ファイルを削除してからメッセージを配信、メッセージの配信を停止するなど、メッセージに対して実行するアクションを示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

[Intrusion Prevention] タブ

[Intrusion Prevention] タブでは、IPS に関する重要な情報を確認できます。このタブは、適応型セキュリティ アプライアンスにインストールされている AIP SSM で IPS ソフトウェアが実行されている場合にだけ表示されます。

侵入防御の詳細については、「IPS の設定」を参照してください。

IPS への接続

AIP SSM 上の IPS ソフトウェアに接続するには、次の手順を実行します。

ステップ 1　ASDM アプリケーションのメイン ウィンドウで、[Intrusion Prevention] タブをクリックします。

ステップ 2　[Connecting to IPS] ダイアログボックスで、次のオプションのいずれかを選択します。

- [Management IP Address]：SSM の管理ポートの IP アドレスに接続します。
- [Other IP Address or Hostname]：SSM の代替 IP アドレスまたはホスト名に接続します。

ステップ 3　[Port] フィールドにポート番号を入力し、[Continue] をクリックします。

ステップ 4　[Enter Network Password] ダイアログボックスで、ユーザ名とパスワードを該当するフィールドに入力し、[Login] をクリックします。

フィールド

- [Device Information]：次の情報が表示されます。
  - [Host Name]：*表示専用*。IPS のホスト名を示します。
  - [IPS Version]：*表示専用*。IPS ソフトウェアのバージョンを示します。
  - [IDM Version]：*表示専用*。IDM ソフトウェアのバージョンを示します。
  - [Bypass Mode]：*表示専用*。バイパス モードを示します。[On] または [Off] に設定できます。
  - [Missed Packets Percentage]：*表示専用*。失われたパケットの割合を示します。
  - [IP Address]：*表示専用*。適応型セキュリティ アプライアンスの IP アドレスを示します。
  - [Device Type]：*表示専用*。適応型セキュリティ アプライアンスのタイプとモデルを示します。
  - [Total Data Storage]：*表示専用*。使用可能なデータ ストレージの総容量を MB 単位で示します。
  - [Total Sensing Interface]：*表示専用*。検知インターフェイスの総数を示します。
- [System Resources Status]：IPS ソフトウェアの CPU およびメモリの使用状況に関する次の統計情報を表示します。

  - *表示のみ*。現在の CPU リソース使用率。
  - *表示のみ*。平均 CPU リソース使用率。
  - *表示のみ*。現在のメモリ使用量。
  - *表示のみ*。平均メモリ使用量。
  - *表示のみ*。空きメモリ容量と使用可能な総メモリ容量。
- [Interface Status]：次の情報を表示します。
  - [Interface]：*表示専用*。接続しているインターフェイスのタイプを表示します。送受信パケット数を表示するには、インターフェイスを選択します。
  - [Link]：*表示専用*。リンク ステータスを示します。Up または Down の場合があります。
  - [Enabled]：*表示専用*。現在の接続ステータスを示します。Yes（イネーブル）または No（イネーブルではない）の場合があります。
  - [Speed]：*表示専用*。現在の接続速度を示します。
  - [Mode]：*表示専用*。現在のモードを示します。Management または Paired の場合があります。
- [Alert Summary]：*表示専用*。アラートのリストを、割り当てられた値（High、Med、Low、Info）と割り当てられた脅威のランクとともに示します。
- [Alert Profile]：*表示専用*。受信したアラートを色分けしたグラフで表示します。割り当てられた値の High（赤）、Med（黄）、Low（緑）、Info（青）と、割り当てられた脅威のランク（マゼンタ）を使用します。
- [Auto-Refresh every 10 seconds] : 現在のペインを 10 秒間隔で自動的にリフレッシュするには、このチェックボックスをオンにします。
- [Refresh Page]：現在開いているペインを手動でリフレッシュします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

[System Home] ペイン

ASDM システム ホーム ペインでは、適応型セキュリティ アプライアンスに関する重要なステータス情報を表示できます。ASDM システム ホーム ペインに表示される詳細のほとんどは、ASDM の他の場所でも参照できますが、このペインでは適応型セキュリティ アプライアンスの動作状態を一目で確認できます。[System Home] ペインのステータス情報は 10 秒間隔で更新されます。

（注） このペインは、セキュリティ コンテキスト内だけで使用できます。

フィールド

- [Device List]：ユーザが接続できるデバイスのリストを表示します。詳細については、「デバイス リスト」（P.1-10）を参照してください。
- [Interface Status]：次の情報を表示します。
  - [Interface]：*表示専用*。接続しているインターフェイスのタイプを表示します。インターフェイスを通過するトラフィックの総数を表示するには、インターフェイスを選択します。
  - [Contexts]：*表示のみ*。ユーザの現在のコンテキスト（admin など）を示します。
  - [Line]：*表示専用*。回線ステータスを示します。Up または Down の場合があります。
  - [Link]：*表示専用*。リンク ステータスを示します。Up または Down の場合があります。
  - [Kbps]：*表示専用*。現在の接続速度（キロビット/秒）を示します。
- [CPU Status]：CPU およびコンテキストの使用状況に関する次の統計情報を示します。
  - [Total Usage] タブ：*表示専用*。CPU の合計使用率および CPU 合計使用率の履歴（秒単位）を示します。
  - [Context Usage] タブ：*表示専用*。3 つの形式（テーブル、円グラフ、または棒グラフ）で表示するコンテキストの合計使用率を示します。テーブル ビューでは、特定のリソースの上位 5 ユーザまたは上位 10 ユーザだけを表示するフィルタリング機能が提供されます。さらに、このビューにはピーク時の使用状況も表示できます。
- [Connection Status]：接続およびコンテキスト接続の使用状況に関する次の統計情報を示します。
  - [Total Connections] タブ：*表示専用*。接続の合計数を表示します。
  - [Context Connections] タブ：*表示専用*。3 つの形式（テーブル、円グラフ、または棒グラフ）で表示するコンテキスト接続の総数を示します。テーブル ビューでは、特定のリソースの上位 5 ユーザまたは上位 10 ユーザだけを表示するフィルタリング機能が提供されます。さらに、このビューにはピーク時の使用状況も表示できます。
- [Memory Status]：CPU およびコンテキストの使用状況に関する次の統計情報を示します。
  - [Total Usage] タブ：*表示専用*。メモリ合計使用量（MB 単位）およびメモリ合計使用量の履歴（MB 単位）を示します。
  - [Context Usage] タブ：*表示専用*。3 つの形式（テーブル、円グラフ、または棒グラフ）で表示されたさまざまなコンテキストでのメモリ合計使用量（MB 単位）を示します。テーブル ビューでは、特定のリソースの上位 5 ユーザまたは上位 10 ユーザだけを表示するフィルタリング機能が提供されます。さらに、このビューにはピーク時の使用状況も表示できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

CHAPTER 2

プリファレンスの定義およびコンフィギュレーション、診断、ファイル管理ツールの使用

この章では、プリファレンスについて、およびコンフィギュレーション、問題診断、ファイル管理で使用可能なツールについて説明します。この項では、次のトピックについて取り上げます。

プリファレンス

この機能により、セッション間での一部の ASDM 機能の動作を変更できます。

ASDM のさまざまな設定を変更するには、次の手順を実行します。

ステップ 1 ASDM アプリケーションのメイン ウィンドウで、[Tools] > [Preferences] の順に選択します。

[General]、[Rules Table]、および [Syslog Colors] の 3 つのタブのある [Preferences] ダイアログボックスが表示されます。

ステップ 2 これらのタブの 1 つをクリックして次のように設定を定義します。[General] タブでは汎用プリファレンスを指定し、[Rules Tables] タブでは Rules テーブルのプリファレンスを指定し、[Syslog Colors] タブでは、[Home] ペインに表示されるシステム ログ メッセージの背景色、前景色、およびフォントの色を指定します。

ステップ 3 [General] タブでは、次の項目を指定します。

a. ASDM によって生成される CLI コマンドを表示するには、[Preview commands before sending them to the device] チェックボックスをオンにします。

b. 適応型セキュリティ アプライアンスに複数のコマンドを 1 つのグループとして送信するには、[Enable cumulative (batch) CLI delivery] チェックボックスをオンにします。

c. ASDM を閉じるときに終了を確認するプロンプトが表示されるようにするには、[Confirm before exiting ASDM] チェックボックスをオンにします。このオプションは、デフォルトでオンです。

d. 起動時に read-only ユーザに対して次のメッセージを表示するには、[Show configuration restriction message to read-only user] チェックボックスをオンにします。このオプションは、デフォルトでオンです。

```
"You are not allowed to modify the ASA configuration, because you do not have
sufficient privileges."
```

e. スクリーン リーダーをイネーブルにするには、[Enable screen reader support (requires ASDM restart)] チェックボックスをオンにします。このオプションをイネーブルにするには、ASDM を再起動する必要があります。

f. ユーザが VPN 接続によって ASDM にアクセスするときに警告メッセージを表示するには、[Warn that Easy VPN is enabled when visiting VPN section] チェックボックスをオンにします。このオプションは、ASA 5505 でだけ使用可能です。

g. Packet Capture Wizard で、キャプチャされたパケットが表示されるようにするには、ネットワーク スニファ アプリケーションの名前を入力するか、または [Browse] をクリックして指定します。

ステップ 4　[Rules Tables] タブで、次の項目を指定します。

a. [Display settings] では、[Rules] テーブルでのルールの表示方法を変更できます。

- Auto-Expand Prefix に基づいて自動展開されたネットワークおよびサービス オブジェクト グループを表示するには、[Auto-expand network and service object groups with specified prefix] チェックボックスをオンにします。
- [Auto-Expand Prefix] フィールドで、表示されるときに自動で展開されるネットワークおよびサービス オブジェクト グループのプレフィックスを指定します。
- ネットワークおよびサービス オブジェクト グループのメンバーとそのグループ名を [Rules] テーブルに表示するには、[Show members of network and service object groups] チェックボックスをオンにします。チェックボックスがオフの場合は、グループ名だけが表示されます。
- [Limit Members To] フィールドに、表示するネットワークおよびサービス オブジェクト グループの数を入力します。オブジェクト グループ メンバが表示されるときには、最初の *n* 個のメンバだけが表示されます。
- [Rules] テーブルにすべてのアクションを表示するには、[Show all actions for service policy rules] チェックボックスをオンにします。オフの場合は、サマリーが表示されます。

b. [Deployment Settings] では、[Rules] テーブルに変更内容を適用するときのセキュリティ アプライアンスの動作を設定できます。

- 新しいアクセス リストを適用するときに [NAT] テーブルをクリアするには、[Issue "clear xlate" command when deploying access lists] チェックボックスをオンにします。この設定により、セキュリティ アプライアンスで設定されるアクセス リストが、すべての変換アドレスに対して確実に適用されるようにします。

c. [Access Rule Hit Count Settings] では、[Access Rules] テーブルのヒット数をアップデートする頻度を設定できます。ヒット数は、明示的なルールにだけ適用されます。暗黙的なルールのヒット数は、[Access Rules] テーブルには表示されません。

- [Access Rules] テーブルでヒット数が自動的にアップデートされるようにするには、[Update access rule hit counts automatically] チェックボックスをオンにします。
- [Update Frequency] フィールドで、[Access Rules] テーブルのヒット数カラムをアップデートする頻度を秒単位で指定します。有効値の範囲は 10 ～ 86400 秒です。

ステップ 5　[Syslog Colors] タブで、次の項目を指定します。

- 各重大度レベルでメッセージの背景テキストまたは前景テキストの色を変更するには、対応するカラムをクリックします。[Pick a Color] ダイアログボックスが表示されます。次のいずれかのタブを選択します。
  - [Swatches] タブでは、パレットから色を選択して [OK] をクリックします。
  - [HSB] タブでは、[H]、[S]、および [B] 設定を指定して [OK] をクリックします。
  - [RGB] タブでは、[Red]、[Green]、および [Blue] 設定を指定して [OK] をクリックします。

[Severity] カラムは編集できません。このカラムには、名前と番号ごとの各重大度レベルが一覧表示されます。

（注）　プリファレンスのチェックボックスのオン/オフを切り替えると、そのたびに変更結果が .conf ファイルに保存され、その時点でワークステーションで実行中の他のすべての ASDM セッションで使用可能になります。すべての変更を有効にするには、ASDM を再起動する必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

コンフィギュレーション ツール

この項では、次のトピックについて取り上げます。

- 「Reset Device to the Factory Default Configuration」（P.2-3）
- 「Save Running Configuration to TFTP Server」（P.2-4）
- 「Save Internal Log Buffer to Flash」（P.2-5）
- 「コマンドライン インターフェイス」（P.2-5）
- 「Show Commands Ignored by ASDM on Device」（P.2-7）

Reset Device to the Factory Default Configuration

デフォルト コンフィギュレーションには、ASDM を使用して適応型セキュリティ アプライアンスに接続するために必要な最小限のコマンドが含まれています。

（注）　この機能は、ルーテッド ファイアウォール モードでのみ使用できます。トランスペアレント モードの場合、インターフェイスの IP アドレスがサポートされません。さらに、この機能はシングル コンテキスト モードでのみ使用できます。コンフィギュレーションがクリアされたセキュリティ アプライアンスには、この機能を使用して自動的に設定する定義済みのコンテキストがありません。

適応型セキュリティ アプライアンスを工場出荷時のデフォルト コンフィギュレーションにリセットするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[File] > [Reset Device to the Factory Default Configuration] の順に選択します。

[Reset Device to the Default Configuration] ダイアログボックスが表示されます。

ステップ 2　デフォルト アドレスの 192.168.1.1 を使用する代わりに、管理インターフェイスの管理 IP アドレスを入力します。専用管理インターフェイスを備える適応型セキュリティ アプライアンスの場合、そのインターフェイスは「Management0/0」と呼ばれます。他の適応型セキュリティ アプライアンスの場合、設定済みインターフェイスは Ethernet 1 で、「inside」と呼ばれます。

ステップ 3　ドロップダウン リストから [Management（または Inside）Subnet Mask] を選択します。

ステップ 4　この設定を内部フラッシュ メモリに保存するには、[File] > [Save Running Configuration to Flash] を選択します。このオプションを選択すると、以前にシステム時刻で別の場所を設定している場合でも、実行コンフィギュレーションがスタートアップ コンフィギュレーションのデフォルトの場所に保存されます。コンフィギュレーションをクリアした場合は、このパスもクリアされています。工場出荷時のコンフィギュレーションの復元後、適応型セキュリティ アプライアンスを次回にリロードするときに、内部フラッシュ メモリの最初のイメージからこのデバイスがブートします。内部フラッシュ メモリにイメージがない場合、適応型セキュリティ アプライアンスはブートしません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Save Running Configuration to TFTP Server

この機能により、現在の実行コンフィギュレーション ファイルのコピーを TFTP サーバに保存します。

実行コンフィギュレーションを TFTP サーバに保存するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[File] > [Save Running Configuration to TFTP Server] の順に選択します。

[Save Running Configuration to TFTP Server] ダイアログボックスが表示されます。

ステップ 2　TFTP サーバの IP アドレスと、コンフィギュレーション ファイルの保存先となる TFTP サーバ上のファイル パスを入力して、[Save Configuration] をクリックします。

（注）　デフォルトの TFTP 設定を行うには、[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] の順に選択します。この設定を行った後は、このダイアログボックスに、TFTP サーバの IP アドレスと TFTP サーバ上でのファイル パスが自動的に表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

Save Internal Log Buffer to Flash

この機能により、内部ログ バッファをフラッシュ メモリに保存できます。

内部ログ バッファをフラッシュ メモリに保存するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[File] > [Save Internal Log Buffer to Flash] の順に選択します。

[Enter Log File Name] ダイアログボックスが表示されます。

ステップ 2　最初のオプションを選択し、LOG-YYYY-MM-DD-hhmmss.txt 形式のデフォルト ファイル名でログ バッファを保存します。

ステップ 3　2 番目のオプションを選択し、そのログ バッファのファイル名を指定します。

ステップ 4　ログ バッファのファイル名を入力して [OK] をクリックします。

コマンドライン インターフェイス

この機能には、コマンドを適応型セキュリティ アプライアンスに送信して結果を表示する、テキストベースのツールが用意されています。

CLI ツールによって入力可能なコマンドは、ユーザ権限によって異なります。詳細については、[システム管理者用 AAA の設定] ペインを参照してください。 メイン ASDM アプリケーション ウィンドウの下部にあるステータスバーの権限レベルを見て、CLI 特権コマンドを実行するために必要な特権があるかどうかを確認してください。

（注）　ASDM の CLI ツールから入力したコマンドは、適応型セキュリティ アプライアンスの接続ターミナルから入力したコマンドと異なる動作をする場合があります。

CLI ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Command Line Interface] の順に選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ 2　必要なコマンドのタイプ（1 行または複数行）を選択し、ドロップダウン リストからコマンドを選択するか、または表示されたフィールドにコマンドを入力します。

ステップ 3　[Send] をクリックしてコマンドを実行します。

ステップ 4　新しいコマンドを入力するには、[Clear Response] をクリックしてから、実行する別のコマンドを選択（または入力）します。

ステップ 5　この機能の状況依存ヘルプを表示するには、[Enable context-sensitive help (?)] チェックボックスをオンにします。文脈依存ヘルプをディセーブルにするには、このチェックボックスをオフにします。

ステップ 6　設定を変更した場合は、[Command Line Interface] ダイアログボックスを閉じた後に、[Refresh] をクリックして ASDM での変更内容を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

コマンド エラー

誤った入力コマンドによってエラーが発生した場合、その誤ったコマンドはスキップされ、その他のコマンドは処理されます。[Response] 領域には、他の関連情報とともに、エラーが発生したかどうかについての情報を示すメッセージが表示されます。

（注）　ASDM は、ほとんどすべての CLI コマンドをサポートしています。コマンドのリストについては、『*Cisco Security Appliance Command Reference*』を参照してください。

インタラクティブ コマンド

インタラクティブ コマンドは、CLI ツールではサポートされていません。これらのコマンドを ASDM で使用するには、次のコマンドに示すように、**noconfirm** キーワード（使用できる場合）を使用します。

```
crypto key generate rsa modulus 1024 noconfirm
```

管理者間の競合の回避

管理者権限を持つ複数のユーザが、適応型セキュリティ アプライアンスの実行コンフィギュレーションをアップデートできます。ASDM の CLI ツールでコンフィギュレーションを変更する場合は、アクティブな管理セッションが他にないことを事前に確認してください。複数のユーザが同時に適応型セキュリティ アプライアンスを設定する場合は、最新の変更が有効になります。

同じ適応型セキュリティ アプライアンスで現在アクティブな他の管理セッションを表示するには、[Monitoring] > [Properties] > [Device Access] の順に選択します。

Show Commands Ignored by ASDM on Device

この機能により、ASDM がサポートしていないコマンドの一覧を表示できます。通常 ASDM は、これらのコマンドを無視します。ASDM は、ユーザの実行コンフィギュレーションのコマンドを変更、削除することはありません。詳細については、「サポートされていないコマンド」を参照してください。

ASDM でサポートされていないコマンドの一覧を表示するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Show Commands Ignored by ASDM on Device] の順に選択します。

ステップ 2　完了したら、[OK] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

診断ツール

ASDM には、問題のトラブルシューティングで使用できる診断ツール セットがあります。この項では、次のトピックについて取り上げます。

- 「Packet Tracer」（P.2-7）
- 「ping」（P.2-8）
- 「traceroute」（P.2-11）
- 「管理者によるクライアントレス SSL VPN ユーザへのアラート」（P.2-12）
- 「ASDM Java コンソール」（P.2-13）
- 「Packet Capture Wizard」（P.2-13）

Packet Tracer

パケット トレーサ ツールは、パケット スニフィングとネットワーク障害箇所特定のためのパケット追跡を実現するとともに、パケットに関する詳細情報と適応型セキュリティ アプライアンスによるパケットの処理方法を示します。コンフィギュレーション コマンドによってパケットがドロップされたのではない場合、パケット トレーサ ツールは、その原因に関する情報をわかりやすく提供します。たとえば、無効なヘッダー検証が原因でパケットがドロップされた場合は、次のメッセージが表示されます。

```
"packet dropped due to bad ip header (reason)."
```

パケットをキャプチャするだけでなく、適応型セキュリティ アプライアンスを使用してパケットの一部始終をトレースし、パケットが想定どおり動作するかどうかを確認できます。パケット トレーサ ツールでは次のことができます。

- ネットワーク内にドロップするすべてのパケットをデバッグする。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適切なルールと、ルールを追加する CLI 行の表示
- データ パス内でのパケット変化を時系列で表示する。
- データ パスでパケットをトレースします。

パケット トレーサを開くには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Packet Tracer] の順に選択します。

[Cisco ASDM Packet Tracer] ダイアログボックスが表示されます。

ステップ 2　ドロップダウン リストからパケット トレースの送信元インターフェイスを選択します。

ステップ 3　パケット トレースのプロトコル タイプを指定します。指定できるプロトコル タイプは、ICMP、IP、TCP、および UDP です。

ステップ 4　[Source IP Address] フィールドにパケット トレースの送信元アドレスを入力します。

ステップ 5　ドロップダウン リストからパケット トレースの送信元ポートを選択します。

ステップ 6　[Destination IP Address] フィールドに、パケット トレースの宛先 IP アドレスを入力します。

ステップ 7　ドロップダウン リストからパケット トレースの宛先ポートを選択します。

ステップ 8　[Start] をクリックして、パケットをトレースします。

[Information Display Area] に、パケット トレースの詳細情報が表示されます。

（注）　パケット トレースをグラフィカルに表現するには、[Show animation] チェックボックスをオンにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

ping

ping ツールは、適応型セキュリティ アプライアンスおよび関係する通信リンクのコンフィギュレーションおよび動作を検証する場合、また他のネットワーク デバイスをテストする場合に便利です。

ping が IP アドレスに送信されると、応答が返されます。このプロセスを使用して、ネットワーク デバイスは、相互に検出、識別、およびテストすることができます。

ping ツールでは、ICMP（RFC-777 および RFC-792 に記載）を使用して、2 つのネットワーク デバイス間でのエコー要求とエコー応答のトランザクションを定義します。エコー要求パケットは、ネットワーク デバイスの IP アドレスへ送信されます。受信側のデバイスは送信元と宛先のアドレスを逆にしてから、そのパケットをエコー応答として送り返します。

ping ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Ping] の順に選択します。

[Ping] ダイアログボックスが表示されます。

ステップ 2　[IP Address] フィールドに、ICMP エコー要求パケットの宛先 IP アドレスを入力します。

（注）　[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] ペインでホスト名が割り当てられている場合は、IP アドレスの代わりにホスト名を使用できます。

ステップ 3　（任意）ドロップダウン リストから、エコー要求パケットを送信するセキュリティ アプライアンスのインターフェイスを選択します。指定しない場合、セキュリティ アプライアンスはルーティング テーブルを調べ、宛先アドレスを見つけて必要なインターフェイスを使用します。

ステップ 4　[Ping] をクリックして、指定したインターフェイスまたはデフォルトのインターフェイスから、指定した IP アドレスに ICMP エコー要求パケットを送信し、応答タイマーを開始します。

応答は [Ping Output] 領域に表示されます。IP アドレスへの ping は 3 回送信され、結果は次のフィールドに表示されます。

- ping が送信されたデバイスの IP アドレスまたはデバイス名（設定されている場合）。ホストやネットワークに割り当てたデバイス名は、結果が「NO response」でも表示される場合があります。
- ping が送信されると、指定した最大値つまりタイムアウト値でミリ秒タイマーが作動します。このタイマーは、異なるルートやアクティビティ レベルの相対応答時間をテストするのに便利です。
- ping の実行結果の例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
If the ping fails, the output is as follows:
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ステップ 5　新しい IP アドレスを入力するには、[Clear Screen] をクリックして、[Ping Output] 領域から前の応答を削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

ping ツールの使い方

管理者は、次の方法で ASDM の ping インタラクティブ診断ツールを使用できます。

- 2 つのインターフェイス間のループバック テスト：同じセキュリティ アプライアンスで一方のインターフェイスから相手側のインターフェイスに ping を外部ループバック テストとして起動すると、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証できます。
- セキュリティ アプライアンスへの ping 送信：ping ツールにより、別のセキュリティ アプライアンスのインターフェイスに ping を送信し、そのインターフェイスがアップしていて応答することを確認できます。
- セキュリティ アプライアンスを通過する ping 送信：ping ツールから発信した ping パケットは、デバイスに向かう途中、中間にあるセキュリティ アプライアンスを通過する場合があります。エコー パケットは、返されるときにそのインターフェイスを両方とも通過します。この手順によって、中間にある装置のインターフェイス、動作、応答時間についての基本的なテストができます。
- ネットワーク デバイスの疑わしい動作をテストするための ping 送信：正常に機能していないと思われるネットワーク デバイスに対して、適応型セキュリティ アプライアンスのインターフェイスから ping を送信できます。インターフェイスが正しく設定されているにもかかわらずエコーを受信しない場合は、デバイスに問題があると考えられます。
- 中間の通信状態をテストする場合の ping 送信：正常に機能し、エコー要求を返すことがわかっているネットワーク デバイスに対して、適応型セキュリティ アプライアンスのインターフェイスから ping を送信できます。エコーを受信した場合、中間にあるデバイスがすべて正常に動作し、物理的に正しく接続されていることが確認されたことになります。

ping ツールのトラブルシューティング

ping を送信してエコーを受信しない場合は、適応型セキュリティ アプライアンスのコンフィギュレーションまたは動作にエラーがあることも原因として考えられます。必ずしも ping を送信した IP アドレスから応答がないことが原因であるとは限りません。ping ツールを使用して、適応型セキュリティ アプライアンスのインターフェイスから、インターフェイスに、またはインターフェイスを通過させて ping を送信する前に、次の基本的な確認を行ってください。

- [Configuration] > [Device Setup] > [Interfaces] の順に選択して、インターフェイスが設定されていることを確認します。
- スイッチやルータなど通信パスの中間デバイスで、他のタイプのネットワーク トラフィックが正常に配信されていることを確認します。
- [Monitoring] > [Interfaces] > [Interface Graphs] の順に選択して、「既知の正常な」送信元からの他のタイプのトラフィックが通過することを確認します。

セキュリティ アプライアンスのインターフェイスからの ping 送信

インターフェイスの基本的なテストを行う場合は、正常に機能し、中間通信パスを経由して応答を返すことがわかっているネットワーク デバイスに対して、適応型セキュリティ アプライアンスのインターフェイスから ping 送信を開始できます。基本的なテストの場合は、次の手順を必ず実行してください。

- 「既知の正常な」デバイスが、適応型セキュリティ アプライアンスのインターフェイスから送信された ping を受信することを確認します。ping を受信しない場合は、送信ハードウェアまたはインターフェイスのコンフィギュレーションに問題がある可能性があります。
- 適応型セキュリティ アプライアンスのインターフェイスが正しく設定されているにもかかわらず、「既知の正常な」デバイスからエコー応答を受信しない場合は、インターフェイス ハードウェアの受信機能に問題があると考えられます。「既知の正常な」受信機能を持つ別のインターフェイスで、同じ「既知の正常な」デバイスに対して ping を送信してエコーを受信できる場合、最初のインターフェイスのハードウェアの受信機能に問題があると確認されたことになります。

セキュリティ アプライアンスのインターフェイスへの ping 送信

適応型セキュリティ アプライアンスのインターフェイスに ping を送信しようとする場合は、[Tools] > [Ping] の順に選択して、そのインターフェイスで ping 応答（ICMP エコー応答）がイネーブルになっていることを確認してください。ping 機能がディセーブルになっていると、適応型セキュリティ アプライアンスは他のデバイスやソフトウェア アプリケーションから検出されず、ASDM の ping ツールに応答しません。

セキュリティ アプライアンス経由の ping の実行

「既知の正常な」送信元からの他のタイプのネットワーク トラフィックが適応型セキュリティ アプライアンスを通過していることを確認するには、[Monitoring] > [Interfaces] > [Interface Graphs] または SNMP 管理ステーションを選択します。

内部ホストから外部ホストへの ping 送信をイネーブルにするには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] の順に選択して、内部および外部インターフェイスの両方の ICMP アクセスを正しく設定します。

traceroute

Traceroute ツールにより、パケットが宛先に到着するまでのルートを判断できます。このツールは、送信される各プローブの結果を出力します。出力の各行が 1 つの TTL 値に対応します（昇順）。次の表に、このツールによって出力される記号の一覧を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。
!H	ICMP ホストに到達できません。
!P	ICMP プロトコルに到達できません。
!A	ICMP が設定によって禁止されています。
?	ICMP の原因不明のエラーが発生しました。

Traceroute ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Traceroute] の順に選択します。

[Traceroute] ダイアログボックスが表示されます。

ステップ 2　ルート トレースの対象となるホストの名前を入力します。ホスト名が指定されている場合は、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] の順に選択して名前を定義するか、またはこのツールをイネーブルにするように DNS サーバを設定して、ホスト名を IP アドレスに解決します。

ステップ 3　応答を待機しているときの接続タイムアウト時間を秒単位で入力します。デフォルトは 3 秒です。

ステップ 4　UDP プローブ メッセージで使用される宛先ポートを入力します。デフォルト値は 33434 です。

ステップ 5　各 TTL レベルで送信されるプローブ数を入力します。デフォルトは 3 です。

ステップ 6　最初のプローブの最小および最大 TTL 値を指定します。デフォルトの最小値は 1 です。値を大きくすると、始めに表示される既知のホップが少なくなります。デフォルトの最大値は 30 です。トレースルートは、パケットが宛先に到達するか、または最大値に達すると終了します。

ステップ 7　UDP プローブ メッセージで使用される宛先ポートを入力します。デフォルト値は 33434 です。

ステップ 8　ドロップダウン リストから、パケット トレースの送信元インターフェイスまたは IP アドレスを選択します。この IP アドレスはいずれかのインターフェイスの IP アドレスにする必要があります。トランスペアレント モードでは、適応型セキュリティ アプライアンスの管理 IP アドレスにする必要があります。

ステップ 9　名前解決が設定されている場合、使用されたホップ名を出力結果に表示するには、[Reverse Resolve] チェックボックスをオンにします。出力結果に IP アドレスを表示するには、このチェックボックスをオフにします。

ステップ 10　UDP プローブ パケットの代わりに ICMP プローブ パケットを使用するよう指定するには、[Use ICMP] チェックボックスをオンにします。

ステップ 11　[Trace Route] をクリックしてトレースルートを開始します。

[Traceroute Output] 領域に、トレースルートの結果についての詳細なメッセージが表示されます。

ステップ 12　[Clear Output] をクリックして新しいトレースルートを開始します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

管理者によるクライアントレス SSL VPN ユーザへのアラート

この機能により、クライアントレス SSL VPN ユーザにアラート メッセージ（たとえば、接続ステータスについて）を送信できます。

アラート メッセージを送信するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Administrator's Alert Message to Clientless SSL VPN Users] の順に選択します。

[Administrator's Alert Message to Clientless SSL VPN Users] ダイアログボックスが表示されます。

ステップ 2　送信する新規または編集済みのアラート内容を入力して、[Post Alert] をクリックします。

ステップ 3　現在のアラート内容を削除して新しいアラート内容を入力するには、[Cancel Alert] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

ASDM Java コンソール

ASDM Java コンソールを使用して、ASDM エラーのトラブルシューティングに役立つ、記録されたエントリをテキスト形式で表示およびコピーできます。このツールにアクセスするには、メイン ASDM アプリケーション ウィンドウで、[Tools] > [ASDM Java Console] の順に選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

Packet Capture Wizard

Packet Capture Wizard を使用して、エラーのトラブルシューティングを行う場合のキャプチャを設定および実行できます。キャプチャでは、アクセス リストを使用して、送信元と宛先のアドレスとポート、および 1 つ以上のインターフェイスにキャプチャされるトラフィックのタイプを制限できます。このウィザードは、入出力インターフェイスのそれぞれでキャプチャを 1 回実行します。キャプチャしたパケットは、PC に保存してパケット アナライザで分析できます。

（注）　このツールは、クライアントレス SSL VPN キャプチャをサポートしていません。

キャプチャを設定および実行するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Wizards] > [Packet Capture Wizard] の順に選択します。

[Overview of Packet Capture] 画面には、ウィザードを完了するまでに行うタスクの一覧が表示されます。

ステップ 2　[Next] をクリックして [Ingress Traffic Selector] 画面を表示します。

ステップ 3　ドロップダウン リストから、入力インターフェイス（内部または外部）を選択します。

ステップ 4　送信元ホストの IP アドレスを入力し、ドロップダウン リストからネットワーク IP アドレスを選択します。

ステップ 5　ドロップダウン リストからプロトコルを選択します。

ステップ 6　選択したプロトコルによっては、送信元ポートのサービスと宛先ポートのサービスの両方を定義する必要もあります。次のいずれかのオプションを選択します。

- All Services
- Service group（ドロップダウン リストから選択）
- Service（事前定義済みパラメータのセットに従って選択）

ステップ 7　[Next] をクリックして、[Egress Traffic Selector] 画面を表示します。

ステップ 8　ドロップダウン リストから出力インターフェイスを選択します。

ステップ 9　送信元ホストの IP アドレスを入力し、ドロップダウン リストからネットワーク IP アドレスを選択します。

（注）　送信元ポートのサービスおよび宛先ポートのサービスは、[Ingress Traffic Selector] 画面での選択に基づいて読み取り専用になります。

ステップ 10　[Next] をクリックして [Buffers] 画面を表示します。バッファ サイズは、キャプチャがパケットを保存するために使用可能なメモリの最大容量です。パケット サイズは、キャプチャが保持できる最長のパケットです。できる限り多くの情報をキャプチャするため、最長パケット サイズを使用することを推奨します。

ステップ 11　パケット サイズを入力します。有効なサイズ範囲は 14 ～ 1522 バイトです。

ステップ 12　バッファ サイズを入力します。有効なサイズ範囲は 1534 ～ 33554432 バイトです。

ステップ 13　キャプチャされたパケットを保存するには、[Use circular buffer] チェックボックスをオンにします。

（注）　この設定を選択すると、すべてのバッファ ストレージが使用されている場合、キャプチャは最も古いパケットへの上書きを始めます。

ステップ 14　[Next] をクリックして [Summary] 画面を表示します。画面に、入力したトラフィック セレクタとバッファ パラメータが表示されます。

ステップ 15　[Next] をクリックして [Run Capture] 画面を表示し、次に [Start] をクリックしてパケットのキャプチャを開始します。[Stop] をクリックしてキャプチャを終了します。

ステップ 16　残りのバッファ スペースを確認するには、[Get Capture Buffer] をクリックします。現在のパケットの内容を削除して、バッファに別のパケットをキャプチャするスペースを確保するには、[Clear Buffer on Device] をクリックします。

ステップ 17　[Save captures] をクリックして、[Save Capture] ダイアログボックスを表示します。キャプチャしたパケットを保存するときの形式として、[ASCII] または [PCAP] を選択します。入力キャプチャ、出力キャプチャ、またはその両方を保存するオプションを選択できます。

ステップ 18　入力パケット キャプチャを保存するには、[Save Ingress Capture] をクリックして [Save capture file] ダイアログボックスを表示します。PC 上でのストレージの場所を指定し、[Save] をクリックします。

ステップ 19　出力パケット キャプチャを保存するには、[Save Egress Capture] をクリックして [Save capture file] ダイアログボックスを表示します。PC 上でのストレージの場所を指定し、[Save] をクリックします。

ステップ 20　[Close] をクリックし、次に [Finish] をクリックしてウィザードを終了します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

Packet Capture Wizard のフィールド情報

ここでは、次の内容について説明します。

- 「Ingress Traffic Selector」（P.2-15）
- 「Egress Traffic Selector」（P.2-16）
- 「Buffers」（P.2-16）
- 「Summary」（P.2-17）
- 「キャプチャの実行」（P.2-17）
- 「キャプチャの保存」（P.2-18）

Ingress Traffic Selector

[Ingress Traffic Selector] ダイアログボックスでは、パケット キャプチャの入力インターフェイス、送信元と宛先のホスト/ネットワーク、およびプロトコルを設定できます。

フィールド

- [Ingress Interface]：入力インターフェイス名を指定します。
- [Source Host/Network]：入力送信元ホストおよびネットワークを指定します。
- [Destination Host/Network]：入力宛先ホストおよびネットワークを指定します。
- [Protocol]：キャプチャするプロトコル タイプを指定します（ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、snp、tcp、または udp）。
  - [ICMP type]：ICMP プロトコルのみの ICMP タイプを指定します（all、alternate address、conversion-error、echo、echo-reply、information-reply、information-request、mask-reply、mask-request、mobile-redirect、parameter-problem、redirect、router-advertisement、router-solicitation、source-quench、time-exceeded、timestamp-reply、timestamp-request、traceroute、または unreachable）。
  - [Source/Destination Port Services]：TCP および UDP プロトコルのみの送信元および宛先ポートのサービスを指定します。

[All Services]：すべてのサービスを指定します。

[Service Group]：サービス グループを指定します。

[Service]：サービスを指定します（aol、bgp、chargen、cifx、citrix-ica、ctiqbe、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、https、ident、imap4、irc、kerberos、klogin、kshell、ldap、ldaps、login、lotusnotes、lpd、netbios-ssn、nntp、pcanywhere-data、pim-auto-rp、pop2、pop3、pptp、rsh、rtsp、sip、smtp、sqlnet、ssh、sunrpc、tacacs、talk、telnet、uucp、または whois）。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Egress Traffic Selector

[Egress Traffic Selector] ダイアログボックスでは、パケット キャプチャの出力インターフェイス、送信元と宛先のホスト / ネットワーク、および送信元と宛先ポートのサービスを設定できます。

フィールド

- [Egress Interface]：出力インターフェイス名を指定します。
- [Source Host/Network]：出力送信元ホストおよびネットワークを指定します。
- [Destination Host/Network]：出力宛先ホストおよびネットワークを指定します。
- [Protocol]：入力設定時に選択したプロトコル タイプを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Buffers

[Buffers] ダイアログボックスでは、パケット キャプチャのパケット サイズ、バッファ サイズ、および循環バッファを使用するかどうかを設定できます。

フィールド

- [Packet Size]：キャプチャが保持できる最長のパケットを指定します。できるだけ多くの情報をキャプチャするために、指定可能な最長サイズを使用してください。

- [Buffer Size]：パケットを保存するためにキャプチャが使用できるメモリの最大容量を指定します。
- [Use circular buffer]：パケットの保存に循環バッファを使用するかどうかを指定します。循環バッファのバッファ ストレージがすべて使い尽くされると、キャプチャは最も古いパケットから上書きを始めます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Summary

[Summary] ダイアログボックスには、パケット キャプチャのトラフィック セレクタおよびバッファ パラメータが表示されます。

フィールド

- [Traffic Selectors]：前の手順で指定したキャプチャおよびアクセス リストのコンフィギュレーションを表示します。
- [Buffer Parameters]：前の手順で指定したバッファ パラメータを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

キャプチャの実行

[Run Captures] ダイアログボックスでは、キャプチャ セッションを開始および停止できます。また、キャプチャ バッファの表示、ネットワーク アナライザ アプリケーションの起動、パケット キャプチャの保存、およびバッファのクリアも実行できます。

フィールド

- [Start]：選択したインターフェイスでパケット キャプチャ セッションを開始します。
- [Stop]：選択したインターフェイスでキャプチャ セッションを停止します。
- [Get Capture Buffer]：インターフェイスでキャプチャされたパケットのスナップショットを表示するよう指定します。
- [Ingress]：入力インターフェイスでのキャプチャ バッファを表示します。

  - [Launch Network Sniffer Application]：入力キャプチャを分析する場合に、[Tools] > [Preferences] で指定したパケット分析アプリケーションを起動します。
- [Egress]：出力インターフェイスでのキャプチャ バッファを表示します。
  - [Launch Network Sniffer Application]：出力キャプチャを分析する場合に、[Tools] > [Preferences] で指定したパケット分析アプリケーションを起動します。
- [Save Captures]：入力キャプチャと出力キャプチャを ASCII または PCAP 形式で保存できます。
- [Clear Buffer on Device]：デバイスのバッファをクリアします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

キャプチャの保存

[Save Captures] ダイアログボックスでは、パケットをさらに分析するために、入力および出力パケット キャプチャを ASCII または PCAP ファイル形式で保存できます。

フィールド

- [ASCII]：キャプチャ バッファを ASCII 形式で保存する場合に指定します。
- [PCAP]：キャプチャ バッファを PCAP 形式で保存する場合に指定します。
- [Save ingress capture]：入力パケット キャプチャを保存するファイルを指定します。
- [Save egress capture]：出力パケット キャプチャを保存するファイルを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ファイル管理ツール

ASDM には、基本的なファイル管理タスクを実行するのに便利なファイル管理ツール セットが用意されています。この項では、次のトピックについて取り上げます。

- 「File Management」（P.2-19）
- 「Manage Mount Points」（P.2-20）

File Management

ファイル管理ツールにより、フラッシュ メモリに保存されているファイルの表示、移動、コピー、および削除、ファイルの転送、およびリモート ストレージ デバイス（マウント ポイント）のファイルの管理を行うことができます。

（注） マルチコンテキスト モードの場合、このツールはシステムのセキュリティ コンテキストでだけ使用できます。

ファイル管理ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [File Management] の順に選択します。

[File Management] ダイアログボックスが表示されます。

- [Folders] ペインには、ディスク上にあるフォルダが表示されます。
- [Flash Space] は、フラッシュ メモリの合計容量と、使用可能なメモリ容量を示します。
- [Files] 領域には、選択したフォルダのファイルについて次の情報が表示されます。
  - パス
  - ファイル名
  - サイズ（バイト単位）
  - 修正時刻
  - 選択したファイルの種類（ブート コンフィギュレーション、ブート イメージ ファイル、ASDM イメージ ファイル、SVC イメージ ファイル、CSD イメージ ファイル、または APCF イメージ ファイル）を示す、ステータス

ステップ 2　選択したファイルをブラウザに表示するには、[View] をクリックします。

ステップ 3　選択したファイルを切り取って別のディレクトリに貼り付けるには、[Cut] をクリックします。

ステップ 4　選択したファイルをコピーして別のディレクトリに貼り付けるには、[Copy] をクリックします。

ステップ 5　コピーしたファイルを選択した場所に貼り付けるには、[Paste] をクリックします。

ステップ 6　選択したファイルをフラッシュ メモリから削除するには、[Delete] をクリックします。

ステップ 7　ファイルの名前を変更するには、[Rename] をクリックします。

ステップ 8　ファイルを保存するディレクトリを新規作成するには、[New Directory] をクリックします。

ステップ 9　[File Transfer] ダイアログボックスを開くには、[File Transfer] をクリックします。詳細については、「File Transfer」（P.2-23）を参照してください。

ステップ 10　[Manage Points] ダイアログボックスを開くには、[Mount Points] をクリックします。詳細については、「Manage Mount Points」（P.2-20）を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Manage Mount Points

この機能により、CIFS または FTP 接続を使用して、ネットワーク ファイル システムのリモート ストレージ（マウント ポイント）を設定できます。このダイアログボックスには、マウント ポイント、接続タイプ、サーバ名または IP アドレス、およびイネーブルにされた設定（yes または no）の一覧が表示されます。マウント ポイントは、追加、編集、または削除できます。詳細については、「CIFS/FTP マウント ポイントの追加/編集」（P.2-20）を参照してください。作成後に、CIFS マウント ポイントにアクセスできます。詳細については、「CIFS マウント ポイントのアクセス」（P.2-21）を参照してください。

（注）　シングル ルーテッド モードの PIX 535 セキュリティ アプライアンスでは、Manage Mount Point 機能を使用できません。

CIFS/FTP マウント ポイントの追加/編集

CIFS マウント ポイントを追加するには、次の手順を実行します。

ステップ 1　[Add] をクリックし、[CIFS Mount Point] を選択します。

[Add CIFS Mount Point] ダイアログボックスが表示されます。

[Enable mount point] チェックボックスは、デフォルトで自動的にオンになります。

ステップ 2　該当するフィールドに、マウント ポイント、サーバ名または IP アドレス、および共有名を入力します。

ステップ 3　[Authentication] セクションで、NT ドメイン、ユーザ名、およびパスワードを入力し、続いてパスワードを確認します。

ステップ 4　[OK] をクリックします。

FTP マウント ポイントを追加するには、次の手順を実行します。

ステップ 1　[Add] をクリックし、[FTP Mount Point] を選択します。

[Add FTP Mount Point] ダイアログボックスが表示されます。

[Enable mount point] チェックボックスは、デフォルトで自動的にオンになります。

ステップ 2　該当するフィールドに、マウント ポイント名と、サーバ名または IP アドレスを入力します。

ステップ 3　[FTP Mount Options] セクションで、[Active Mode] または [Passive Mode] オプションを選択します。

ステップ 4　リモート ストレージをマウントするパスを入力します。

ステップ 5　[Authentication] セクションで、NT ドメイン、ユーザ名、およびパスワードを入力し、続いてパスワードを確認します。

ステップ 6　[OK] をクリックします。

CIFS マウント ポイントを編集するには、次の手順を実行します。

ステップ 1　変更する CIFS マウント ポイントを選択し、[Edit] をクリックします。

[Edit CIFS Mount Point] ダイアログボックスが表示されます。

（注）　CIFS マウント ポイントは変更できません。

ステップ 2　残りの設定に変更を加え、変更が済んだら [OK] をクリックします。

FTP マウント ポイントを編集するには、次の手順を実行します。

ステップ 1　変更する FTP マウント ポイントを選択し、[Edit] をクリックします。

[Edit FTP Mount Point] ダイアログボックスが表示されます。

（注）　FTP マウント ポイントは変更できません。

ステップ 2　残りの設定に変更を加え、変更が済んだら [OK] をクリックします。

CIFS マウント ポイントのアクセス

作成後に CIFS マウント ポイントにアクセスするには、次の手順を実行します。

ステップ 1　セキュリティ アプライアンス CLI を起動します。

ステップ 2　**mount <name of mount> type cifs** コマンドを入力し、マウントを作成します。

ステップ 3　**show run mount** コマンドを入力します。

次の出力が表示されます。

（注）　この例では、マウント名は win2003 です。

```
server kmmwin2003
share sharefolder
username webvpnuser2
password ********
status enable
```

ステップ 4　**dir** コマンドを入力し、イネーブルになっているすべてのマウントをサブディレクトリとして表示します。これは、Windows PC でドライブをマウントするのに似ています。たとえば、次の出力結果 FTP2003:、FTPLINUX:、win2K: は設定されたマウントです。

次に、**dir** コマンドの出力例を示します。

```
FTP2003: Directory or file name
FTPLINUX: Directory or file name
WIN2003: Directory or file name
all-filesystems List files on all filesystems
disk0: Directory or file name
disk1: Directory or file name
flash: Directory or file name
system: Directory or file name
win2K: Directory or file name
```

ステップ 5　そのマウントに対して **dir** コマンドを入力します（たとえば、**dir WIN2003**）。そして、フラッシュ メモリ（disk0:）からリストされたマウントのいずれかへ、またはマウントからフラッシュメモリへファイルをコピーします。

次に、**dir WIN2003** コマンドの出力例を示します。

```
Directory of WIN2003:/
---- 14920928 08:33:36 Apr 03 2009 1_5_0_01-windows-i586-p.exe
---- 33 11:27:16 Jun 07 2007 AArenameIE70
---- 28213021 15:15:22 Apr 03 2009 atest2(3).bin
---- 61946730 12:09:40 Mar 17 2009 atest2.bin
---- 5398366 14:52:10 Jul 28 2008 atest222.bin
---- 2587728 10:07:44 Dec 06 2005 cCITRIXICA32t.exe
---- 1499578 15:26:50 Dec 02 2005 ccore.exe
---- 61946728 11:40:36 Dec 09 2005 CIFSTESTT.bin
---- 2828 13:46:04 May 11 2009 ClientCert.pfx
d--- 16384 14:48:28 Mar 20 2007 cookiefolder
---- 4399 15:58:46 Jan 06 2006 Cookies.plist
---- 2781710 12:35:00 Dec 12 2006 coreftplite1.3.exe
---- 0 10:22:52 Jul 13 2007 coreftplite1.3.exe.download
---- 245760 15:13:38 Dec 21 2005 Dbgview.exe
---- 1408249 11:01:34 Dec 08 2005 expect-5.21r1b1-setup.exe
d--- 16384 14:49:14 Jul 28 2008 folder157
---- 101 09:33:48 Dec 12 2005 FxSasser.log
---- 2307104 09:54:12 Dec 12 2005 ica32t.exe
---- 8732552 10:14:32 Apr 29 2009 iclientSetup_IFen_flex51.exe
d--- 16384 08:32:46 Apr 03 2009 IE8withVistaTitan
---- 15955208 08:34:18 Aug 14 2007 j2re.exe
---- 16781620 13:38:22 Jul 23 2008 jre-1_5_0_06-windows-i586-p.exe
<--- More --->
```

Upgrade Software from Local Computer

Upgrade Software from Local Computer ツールにより、PC からフラッシュ ファイル システムにイメージ ファイルをアップロードし、適応型セキュリティ アプライアンスをアップグレードできます。

PC からソフトウェアをアップグレードするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Local Computer] の順に選択します。

[Upgrade Software from Local Computer] ダイアログボックスが表示されます。

ステップ 2　ドロップダウン リストから、アップロードするイメージ ファイルを選択します。

ステップ 3　PC 上のファイルへのローカル パスを入力するか、または [Browse Local Files] をクリックして PC 上のファイルを指定します。

ステップ 4　フラッシュ ファイル システムへのパスを入力するか、または [Browse Flash] をクリックしてフラッシュ ファイル システムのディレクトリまたはファイルを指定します。

ステップ 5　[Image to Upload] をクリックします。アップグレード プロセスには数分かかる場合があります。必ず終了するまでお待ちください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

File Transfer

File Transfer ツールにより、HTTP、HTTP over SSL、TFTP、FTP、または SMB を使用して、PC またはフラッシュ ファイル システムのローカル ファイルをセキュリティ アプライアンスとの間でコピーできます。

ファイルを転送するには、次の手順を実行します。

ステップ 1　リモート サーバからファイルを転送するには、[Remote server] オプションを選択します。

ステップ 2　転送対象になるソース ファイルを定義します。

a. サーバの IP アドレスを含めたファイルの場所へのパスを選択します。

b. リモート サーバのポート番号またはタイプ（FTP の場合）を入力します。有効な FTP タイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 3　フラッシュ ファイル システムからファイルをコピーするには、[Flash file system] オプションを選択します。

ステップ 4　ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 5　ローカル PC からファイルをコピーするには、[Local computer] オプションを選択します。

ステップ 6　ファイルの場所へのパスを入力するか、[Browse Local Files] をクリックしてファイルの場所を指定します。

ステップ 7　また、CLI により、スタートアップ コンフィギュレーション、実行コンフィギュレーション、または SMB ファイル システムからファイルをコピーすることもできます。**copy** コマンドの使用方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

ステップ 8　転送するファイルの宛先を定義します。

a. フラッシュ ファイル システムにファイルを転送するには、[Flash file system] オプションを選択します。

b. ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 9　リモート サーバにファイルを転送するには、[Remote server] オプションを選択します。

a. ファイルの場所へのパスを入力します。

b. FTP 転送の場合はタイプを入力します。有効なタイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 10　[Transfer File] をクリックしてファイル転送を開始します。ファイル転送プロセスには数分かかる場合があります。必ず終了するまでお待ちください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Upgrade Software from Cisco.com Wizard

Upgrade Software from Cisco.com Wizard により、ASDM および適応型セキュリティ アプライアンスを最新のバージョンに自動的にアップグレードできます。

（注）　この機能は、コンテキスト モードでは使用できません。

このウィザードでは、次の操作を実行できます。

- Cisco.com から使用可能なリリースのリストをダウンロードする。
- アップグレード用の ASDM イメージ ファイルまたは ASA イメージ ファイルを選択する。
- 選択したイメージをアップグレードする。
- ASA イメージをアップグレードした場合はファイアウォールをリロードする（任意）。

（注）　1 つのバージョンから次のバージョンに、順次アップグレードする必要があります（たとえば、バージョン 5.1 から 5.2、バージョン 5.2 から 6.0(2) など）。バージョン 5.1 から 6.0(2) へはアップグレードできません。

Upgrade Software from Cisco.com Wizard を完了するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Cisco.com] の順に選択します。

[Upgrade Software from Cisco.com Wizard] が表示されます。[Overview] 画面に、イメージ アップグレード プロセスの手順が表示されます。

ステップ 2　[Next] をクリックして続行します。

[Authentication] 画面が表示されます。

ステップ 3　割り当てられている Cisco.com ユーザ名、および Cisco.com パスワードを入力し、[Next] をクリックします。

[Image Selection] 画面が表示されます。

ステップ 4　リストにある 2 つのオプションの一方または両方を選択します。

- アップグレードする最新の適応型セキュリティ アプライアンス イメージを指定するには、[Upgrade the ASA version] チェックボックスをオンにします。
- アップグレードする最新の ASDM バージョンを指定するには、[Upgrade the ASDM version] チェックボックスをオンにします。

（注）　ASA バージョン リストまたは ASDM バージョン リストが空の場合は、アップグレード可能な新しい ASA または ASDM イメージはないことを示す文が表示されます。この文が表示されたら、ウィザードを終了できます。

ステップ 5　[Next] をクリックして続行します。

[Selected Images] 画面が表示されます。

ステップ 6　選択したイメージ ファイルが正しいことを確認し、[Next] をクリックしてアップグレードを開始します。

アップグレードに数分かかることを示すメッセージがウィザードに表示されます。アップグレードの進行状況を示すステータスを表示できます。

[Results] 画面が表示されます。この画面には、アップグレードに失敗したかどうか、またはコンフィギュレーションを保存して適応型セキュリティ アプライアンスをリロードするかどうかなどの、詳細な情報が表示されます。

適応型セキュリティ アプライアンスのバージョンをアップグレードし、そのアップグレードに成功した場合は、コンフィギュレーションを保存して適応型セキュリティ アプライアンスをリロードするオプションが表示されます。

ステップ 7　[Yes] をクリックします。

アップグレード バージョンを有効にするには、コンフィギュレーションを保存し、適応型セキュリティ アプライアンスをリロードし、それから ASDM を再起動する必要があります。

（注）　次のバージョンへの 1 回のアップグレードを完了した後にウィザードを再起動する必要はありません。次のバージョンがある場合には、ウィザードの手順 3 に戻り、そのバージョンへのアップグレードを実行できます。

ステップ 8　アップグレードが終了した場合は、[Finish] をクリックしてウィザードを終了します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

Upload ASDM Assistant Guide

Upload ASDM Assistant Guide ツールにより、特定のタスクについての便利な ASDM の使用方法のヘルプを含む XML ファイルを、フラッシュ メモリにアップロードできます。Cisco.com からファイルを取得できます。

ファイルをアップロードした後は、メニュー バーの [Look For] フィールドから [Help] > [ASDM Assistant] > [How Do I?] を選択して、ファイルの情報にアクセスできます。[Find] ドロップダウン リストで、[How Do I?] を選択して検索を開始します。

ASDM Assistant Guide をアップロードするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Upload ASDM Assistant Guide] の順に選択します。

[Upload ASDM Assistant Guide] ダイアログボックスが表示されます。

ステップ 2　[File to Upload] フィールドに、PC 上の XML ファイルの名前を入力するか、または [Browse Local] をクリックしてアップロードする PC 上の XML ファイルを指定します。

ステップ 3　[Flash File System Path] フィールドのドロップダウン リストから、XML ファイルのコピー先となるパスを選択（または入力）します。

ステップ 4　アップロードを開始するには、[Upload File] をクリックします。

（注）　この機能は、PIX セキュリティ アプライアンスでは使用できません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

System Reload

System Reload ツールにより、システムのリロードをスケジュールしたり、保留中のリロードをキャンセルしたりできます。

リロードのスケジュールを設定するには、次の手順を実行します。

ステップ 1　[Reload Scheduling] セクションで、次のリロード スケジューリング設定を定義します。

a. [Configuration State] では、リロード時に実行コンフィギュレーションを保存するか、またはリロード時に実行コンフィギュレーションに対するコンフィギュレーション変更を破棄するかのどちらかを選択します。

b. [Reload Start Time] では、次のオプションから選択できます。

- リロードをただちに実行するには、[Now] をクリックします。
- 指定した時間だけリロードを遅らせるには、[Delay by] をクリックします。リロード開始までの経過時間を、時間と分単位、または分単位だけで入力します。
- 指定した時刻と日付にリロードを実行するようにスケジュールするには、[Schedule at] をクリックします。リロードの実行時刻を入力し、リロードのスケジュール日を選択します。

c. [Reload Message] フィールドに、リロード時に ASDM の開いているインスタンスに送信するメッセージを入力します。

d. リロードを再試行するまでの経過時間を時間と分単位で、または分単位だけで表示するには、[On reload failure force immediate reload after] チェックボックスをオンにします。

e. 設定に従ってリロードをスケジュールするには、[Schedule Reload] をクリックします。

ステップ 2　[Reload Status] 領域には、リロードのステータスが表示されます。

- スケジュールされたリロードを停止するには、[Cancel Reload] をクリックします。
- スケジュールされたリロードの終了後に [Reload Status] 表示をリフレッシュするには、[Refresh] をクリックします。
- スケジュールされたリロードの詳細を表示するには、[Details] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

CHAPTER 3

はじめる前に

この項では、ASDM を使用する前に実行する必要があるタスクについて説明します。次の項目を取り上げます。

工場出荷時のデフォルト コンフィギュレーション

工場出荷時のデフォルト コンフィギュレーションは、PIX 525 および PIX 535 モデルを除き、すべてのセキュリティ アプライアンスでサポートされています。

ASA 5505 モデルの場合、すぐに適応型セキュリティ アプライアンスをネットワークで利用できるように、工場出荷時のデフォルト コンフィギュレーションに事前定義済みのインターフェイスと NAT が含まれています。

PIX 515、PIX 515E、および ASA 5510 以降のバージョンのモデルの場合、工場出荷時のデフォルト コンフィギュレーションで管理インターフェイスが提供されており、ASDM を使用してセキュリティ アプライアンスに接続し、設定を完了できます。

工場出荷時のデフォルト コンフィギュレーションは、ルーテッド ファイアウォール モードおよびシングルコンテキスト モードでだけ利用可能です。マルチ コンテキスト モードの詳細については、セキュリティ コンテキストの設定を参照してください。ルーテッドおよびトランスペアレント ファイアウォール モードの詳細については、ファイアウォール モードの概要を参照してください。

この項では、次のトピックについて取り上げます。

工場出荷時のデフォルト コンフィギュレーションの復元

工場出荷時のデフォルト コンフィギュレーションを復元するには、次の手順を実行します。

ステップ 1　[File] > [Reset Device to the Factory Default Configuration] の順に選択します。

ステップ 2　デフォルトの IP アドレスを変更するには、次のいずれかの操作を実行します。

- ASA 5500 シリーズの場合、[Use this address for the Management 0/0 interface that will be named as management] チェックボックスをオンにし、[Management IP Address] フィールドに新しい IP アドレスを入力して、[Management Subnet Mask] ドロップダウン リストから新しいサブネット マスクを選択します。
- PIX シリーズの場合、[Use this address for the Ethernet 1 interface, which will be named inside] チェックボックスをオンにし、[Inside IP Address] フィールドに新しい内部 IP アドレスを入力して、[Inside Subnet Mask] ドロップダウン リストから新しい内部サブネット マスクを選択します。

ステップ 3　[OK] をクリックします。

（注）　工場出荷時のデフォルト コンフィギュレーションを復元すると、適応型セキュリティ アプライアンスは次にリロードするときに、内部フラッシュ メモリの最初のイメージを使用してブートします。内部フラッシュ メモリにイメージがない場合、適応型セキュリティ アプライアンスはブートしません。

ASA 5505 のデフォルト コンフィギュレーション

ASA 5505 適応型セキュリティ アプライアンスの工場出荷時のデフォルト コンフィギュレーションは、次のように設定されています。

- イーサネット 0/1 ～ 0/7 スイッチ ポートを含む内部 VLAN 1 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定していない場合、VLAN 1 の IP アドレスとマスクは、それぞれ 192.168.1.1 と 255.255.255.0 になります。
- イーサネット 0/0 スイッチ ポートを含む外部 VLAN 2 インターフェイス。VLAN 2 は、DHCP を使用してその IP アドレスを取得します。
- デフォルトのルートも DHCP から取得されます。
- すべての内部 IP アドレスは、外部インターフェイスにアクセスするときに PAT を使用して変換されます。
- デフォルトでは、内部ユーザはアクセス リストを使用して外部にアクセスでき、外部ユーザは内部にアクセスできません。
- DHCP サーバは適応型セキュリティ アプライアンス上でイネーブルになっているので、VLAN 1 インターフェイスに接続しているコンピュータは 192.168.1.2 ～ 192.168.1.254 の IP アドレスを受信します。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
```

```
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 以降のバージョンのデフォルト コンフィギュレーション

ASA 5510 以降のバージョンの適応型セキュリティ アプライアンスでは、工場出荷時のデフォルト コンフィギュレーションは次のように設定されています。

- 管理インターフェイスは Management 0/0 です。**configure factory-default** コマンドで IP アドレスを設定しなかった場合、IP アドレスおよびマスクは 192.168.1.1 および 255.255.255.0 です。
- DHCP サーバは適応型セキュリティ アプライアンス上でイネーブルになっているので、インターフェイスに接続しているコンピュータは 192.168.1.2 ～ 192.168.1.254 のアドレスを受信します。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
```

```
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E のデフォルト コンフィギュレーション

PIX 515/515E セキュリティ アプライアンスの工場出荷時のデフォルト コンフィギュレーションは、次のように設定されています。

- 内部 Ethernet1 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定していない場合は、IP アドレスとサブネット マスクは 192.168.1.1 と 255.255.255.0 です。
- DHCP サーバはセキュリティ アプライアンス上でイネーブルになっているので、インターフェイスに接続しているコンピュータは 192.168.1.2 ～ 192.168.1.254 のアドレスを受信します。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface ethernet 1
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

ASDM アクセスに対するセキュリティ アプライアンスの設定

CLI ではなく ASDM を使用してセキュリティ アプライアンスを設定する場合、工場出荷時のデフォルト設定があれば、ブラウザで https://192.168.1.1 に移動するとデフォルトの管理アドレスに接続できます。または、Cisco ASDM Launcher がインストールされていれば、それを使用して ASDM に接続できます。詳細については、「工場出荷時のデフォルト コンフィギュレーション」（P.3-1）を参照してください。

ASA 5505 適応型セキュリティ アプライアンスでは、ASDM への接続に使用するスイッチ ポートは Ethernet 0/0 以外であればどのポートでもかまいません。ASA 5510 以降のバージョンの適応型セキュリティ アプライアンスでは、ASDM に接続するインターフェイスは Management 0/0 です。PIX 515/515E セキュリティ アプライアンスでは、ASDM に接続するインターフェイスは Ethernet 1 です。

工場出荷時のデフォルト設定でない場合、CLI にアクセスする手順については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

CLI によるトランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モードの設定

デフォルトのルーテッド ファイアウォール モードまたはトランスペアレント ファイアウォール モードで稼働するように、適応型セキュリティ アプライアンスを設定できます。ファイアウォール モードの詳細については、ファイアウォール モードの概要を参照してください。マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのファイアウォール モードのみを使用できます。モードの設定は、システム実行スペースで行う必要があります。

モードを変更すると、適応型セキュリティ アプライアンスは設定をクリアします。これは、多くのコマンドが両方のモードでサポートされていないためです。すでにデータが入力された設定が用意されている場合、モードを変更する前に必ずその設定をバックアップしてください。新しい設定を作成する際に、このバックアップ設定を参照用に使用できます。

マルチ コンテキスト モードの場合は、システム設定が消去され、どのコンテキストも削除されます。誤ったモード用に作成された既存の設定を含むコンテキストを再度追加する場合、コンテキスト設定は正しく動作しません。

（注） 必ず正しいモード用のコンテキスト設定を作成してから、再追加を行ってください。そうしない場合は、新しい設定用の新しいパスを使用して新しいコンテキストを追加します。

firewall transparent コマンドを使用してモードを変更するテキスト コンフィギュレーションをセキュリティ アプライアンスにダウンロードする場合は、このコマンドをコンフィギュレーションの先頭に配置します。先頭に配置することによって、適応型セキュリティ アプライアンスでこのコマンドが読み込まれるとすぐにモードが変更され、その後引き続きダウンロードされたコンフィギュレーションが読み込まれます。このコマンドがコンフィギュレーションの後ろの方にあると、適応型セキュリティ アプライアンスはそれ以前に記述されているコンフィギュレーションの行をすべてクリアします。

ファイアウォール モードを設定するには、次の手順を実行します。

（注） マルチ コンテキスト モードの場合は、システム実行スペースでこれらの手順を実行する必要があります。

ステップ 1　新しいコンフィギュレーションを作成する前に、必ずスタートアップ コンフィギュレーション ファイルまたは実行コンフィギュレーション ファイルをバックアップして後で参照できるようにしてください。次のいずれかのコマンドを使用して、シングルコンテキスト モードまたはマルチモードのシステム コンフィギュレーションから、スタートアップ コンフィギュレーション ファイルまたは実行コンフィギュレーション ファイルを外部サーバやローカル フラッシュ メモリにコピーできます。

- TFTP サーバにコピーするには、次のコマンドを入力します。

  ```
  hostname# copy {startup-config | running-config} tftp://server[/path]/filename
  ```

  ここで、*server* は TFTP サーバの名前、*path* はコンフィギュレーション ファイルへのディレクトリ パス、*filename* はコンフィギュレーション ファイルの名前です。

- FTP サーバにコピーするには、次のコマンドを入力します。

  ```
  hostname# copy {startup-config | running-config}
  ftp://[user[:password]@]server[/path]/filename
  ```

  ここで、*user* は使用するユーザ名、*password* は FTP サーバへのパスワード、*server* は FTP サーバの名前、*path* はコンフィギュレーション ファイルへのディレクトリ パス、*filename* はコンフィギュレーション ファイルの名前です。

- ローカル フラッシュ メモリにコピーするには、次のコマンドを入力します。

```
hostname# copy {startup-config | running-config} {flash:/ | disk0:/ |
disk1:/}[path/]filename
```

ここで、*path* はコンフィギュレーション ファイルへのディレクトリ パス、*filename* はコンフィギュレーション ファイルの名前です。

（注）　宛先ディレクトリが存在することを確認してください。存在しない場合は、**mkdir** コマンドを使用して宛先ディレクトリを作成します。

ステップ 2　モードを変更するには、次のコマンドのいずれかを入力します。

- モードをトランスペアレントに設定するには、次のコマンドを入力します。

```
hostname(config)# firewall transparent
```

このコマンドは、各コンテキストのコンフィギュレーションにも情報提供の目的で表示されますが、このコマンドをコンテキストで入力することはできません。

- モードをルーテッドに設定するには、次のコマンドを入力します。

```
hostname(config)# no firewall transparent
```

ASDM の起動

この項では、ASDM を起動する方法について説明します。起動するには次の方法があります。

- 「ASDM ランチャのダウンロード」（P.3-6）
- 「ASDM ランチャによる ASDM の起動」（P.3-7）
- 「デモ モードでの ASDM の使用」（P.3-7）
- 「Web ブラウザによる ASDM の起動」（P.3-8）

ASDM ランチャのダウンロード

ASDM ランチャは Windows 専用です。重複する認証と証明書ダイアログボックスがなくなり、起動が高速化して、入力済みの IP アドレスとユーザ名をキャッシュします。

ASDM ランチャをダウンロードするには、次の手順を実行します。

ステップ 1　[ASDM Welcome] 画面で、適切なボタンをクリックして ASDM ランチャのインストール ファイルをダウンロードします。

ステップ 2　**asdm-launcher.exe** ファイルをダブルクリックします。

（注）　トランスペアレント ファイアウォール モードで、管理 IP アドレスを入力します。必ず **https** を入力してください。**http** ではありません。

ステップ 3　すべてのプロンプトで [OK] または [Yes] をクリックします。名前とパスワードのプロンプトでも同様です。名前とパスワードは空白にします。

インストーラがコンピュータにダウンロードされます。

ステップ 4　インストーラを実行して ASDM ランチャをインストールします。

ASDM ランチャによる ASDM の起動

ASDM ランチャから ASDM を起動するには、次の手順を実行します。

ステップ 1　デスクトップ上の Cisco ASDM Launcher のショートカットをダブルクリックするか、または、[Start] メニューから開きます。または、[ASDM Welcome] 画面から、[Run Startup Wizard] をクリックして ASDM を設定できます。

ステップ 2　接続先として適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力するか選択します。IP アドレスのリストをクリアするには、[Device/IP Address/Name] フィールドの横にあるゴミ箱アイコンをクリックします。

ステップ 3　ユーザ名とパスワードを入力し、[OK] をクリックします。

新しいバージョンの ASDM が適応型セキュリティ アプライアンスにある場合、ASDM ランチャは自動的に新しいバージョンをダウンロードし、ASDM を起動する前に現在のバージョンをアップデートするようにユーザに要求します。

デモ モードでの ASDM の使用

アプリケーション ASDM Demo Mode を別途インストールして使用すると、実デバイスを使用せずに ASDM を実行できます。このモードでは、次の操作を実行できます。

- 実デバイス接続時と同じように、ASDM から設定と選択した監視タスクを実行する。
- ASDM インターフェイスによる ASDM またはセキュリティ アプライアンス機能のデモを実行する。
- CSC SSM を使用して設定および監視タスクを実行する。
- リアルタイムのシステム ログ メッセージを含む、シミュレーションした監視データやログ データを取得する。表示データはランダムに生成されますが、実デバイスに接続しているような体験ができます。

このモードでは、次の機能はサポートされません。

- GUI に表示されたコンフィギュレーションに加えた変更内容の保存
- ファイルまたはディスクの操作
- 履歴モニタリングデータ
- 非管理ユーザ
- 次の機能
  - [File] メニュー

    Save Running Configuration to Flash

    Save Running Configuration to TFTP Server

    Save Running Configuration to Standby Unit

Save Internal Log Buffer to Flash

Clear Internal Log Buffer

– [Tools] メニュー

Command Line Interface

ping

File Management

Update Software

File Transfer

Upload image from Local PC

System Reload

– ツールバー / ステータスバー > [Save]
– [Configuration] > [Interface] > [Edit Interface] > [Renew DHCP Lease]
– フェールオーバー後のスタンバイ デバイスの設定

- コンフィギュレーションの再読み込みが発生する操作。再読み込みが行われると GUI が元のコンフィギュレーションに戻ります。
  – コンテキストの切り換え
  – [Interface] ペインの変更
  – [NAT] ペインの変更
  – [Clock] ペインの変更

ASDM のデモ モードを実行するには、次の手順を実行します。

ステップ 1　ASDM Demo Mode インストーラの asdm-demo-*version*.msi を次の場所からダウンロードします。

http://www.cisco.com/cisco/software/navigator.html

ステップ 2　インストーラをダブルクリックして、ソフトウェアをインストールします。

ステップ 3　デスクトップ上の Cisco ASDM Launcher のショートカットをダブルクリックするか、または、[Start] メニューから開きます。

ステップ 4　[Run in Demo Mode] チェックボックスをオンにします。

[Demo Mode] ウィンドウが表示されます。

Web ブラウザによる ASDM の起動

Web ブラウザから ASDM を起動するには、次の手順を実行します。

ステップ 1　セキュリティ アプライアンス ネットワーク上のサポートされる Web ブラウザで、次の URL を入力します。

https://*interface_ip_address*

ここで、*interface_ip_address* は、適応型セキュリティ アプライアンス ネットワーク上の ASDM の IP アドレスです。

（注）　トランスペアレント ファイアウォール モードで、管理 IP アドレスを入力します。必ず **https** を入力してください。**http** ではありません。

ステップ 2　すべてのブラウザのプロンプトで [OK] または [Yes] をクリックします。ユーザ名とパスワードのプロンプトでも同様です（空白のままにします）。

[Cisco ASDM 6.0(3) Welcome] ページに次のボタンが表示されます。

- Install ASDM Launcher and Run ASDM
- Run ASDM
- Run Startup Wizard

ステップ 3　[Run ASDM] をクリックします。

ステップ 4　すべてのブラウザのプロンプトで [OK] または [Yes] をクリックします。

設定の概要

適応型セキュリティ アプライアンスを設定および監視するには、次の手順を実行します。

ステップ 1　Startup Wizard の使用による初期設定を行うには、[Wizards] > [Startup Wizard] を選択します。

ステップ 2　IPSec VPN Wizard を使用して IPSec VPN 接続を設定するには、[Wizards] > [IPSec VPN Wizard] を選択して、表示される各画面で設定を行います。

ステップ 3　SSL VPN Wizard を使用して SSL VPN 接続を設定するには、[Wizards] > [SSL VPN Wizard] を選択して、表示される各画面で設定を行います。

ステップ 4　高可用性とスケーラビリティに関する設定値を設定するには、[Wizards] > [High Availability and Scalability Wizard] を選択します。詳細については、「High Availability and Scalability Wizard を使用したフェールオーバーの設定」を参照してください。

ステップ 5　Packet Capture Wizard を使用してパケット キャプチャを設定するには、[Wizards] > [Packet Capture Wizard] を選択します。

ステップ 6　ASDM GUI で使用できるさまざまな色とスタイルを表示するには、[View] > [Office Look and Feel] を選択します。

ステップ 7　機能を設定するには、ツールバーで [Configuration] ボタンをクリックし、[Device Setup]、[Device Management]、[Firewall]、[Remote Access VPN]、[Site-to-Site VPN]、[IPS]、[Trend Micro Content Security] のいずれかのボタンをクリックして関連する設定ペインを表示します。

（注）　[Configuration] 画面が空白の場合は、ツールバーで [Refresh] をクリックして、画面のコンテンツを表示します。

- [Device Setup] ペインでは次の操作を実行できます。
  - [Startup Wizard] を起動してセキュリティ ポリシーを作成する。
  - IP アドレス、名前、セキュリティ レベル、トランスペアレント モードのブリッジ グループなど、インターフェイスの基本パラメータを設定する。詳細については、「インターフェイスの設定」を参照してください。

  - OSPF、RIP、スタティック ルーティング、非対称ルーティングを設定する（シングル モードのみ）。詳細については、「ダイナミック ルーティングおよびスタティック ルーティングの設定」を参照してください。
  - AAA サービスを設定する。
  - デジタル証明書を設定する。
  - デバイス名とデバイス パスワードを設定する。
  - DHCP サービスを設定する。
  - DNS サービスを設定する。
- [Firewall] ペインでは、アクセス ルール、AAA ルール、フィルタ ルール、サービス ポリシー ルールなどのセキュリティ ポリシーと共に、NAT ルール、URL フィルタリング サーバ、グローバル オブジェクトを設定できます。また、次の高度な設定を行うこともできます。
  - アクセス ルールでは、IP トラフィックがセキュリティ アプライアンスにアクセスできるかどうかを決定します。トランスペアレント ファイアウォール モードでは、非 IP トラフィックを許可するための EtherType アクセス リストも適用できます。
  - Ethertype ルール（トランスペアレント モードのみ）では、非 IP トラフィックがセキュリティ アプライアンスにアクセスできるかどうかを決定します。
  - アクセス ルールでは、HTTP など特定のタイプのトラフィックに対して、認証と許可のいずれか、または両方を行うかどうかを決定します。セキュリティ アプライアンスは、RADIUS サーバまたは TACACS+ サーバにアカウンティング情報を送信することもあります。
  - 「Filter Rules」では、特定の Web サイトまたは FTP サーバへの発信アクセスを禁止します。セキュリティ アプライアンスは、Websense Enterprise または Sentian を N2H2 で実行する別のサーバと連携して動作します。[Configuration] > [Properties] > [URL Filtering] を選択して URL フィルタリング サーバを設定してから、ルールを追加する必要があります。
  - 「サービス ポリシー ルールの設定」により、アプリケーション インスペクション、接続の制限、TCP 正規化を適用します。インスペクション エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルは、適応型セキュリティ アプライアンスが詳細なパケット インスペクションを行うことを要求します。TCP 接続、UDP 接続、および初期接続を制限することもできます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。TCP 正規化は、正常に見えないパケットをドロップします。
  - 「NAT」は、保護されたネットワークで使用するアドレスをパブリック インターネットで使用するアドレスに変換します。この設定によって、プライベート アドレスを内部ネットワークで使用できます。プライベート アドレスは、インターネットにルーティングできません。
  - 「グローバル オブジェクトの追加」では、適用型セキュリティ アプライアンスにポリシーを組み込む際に不可欠な再利用可能コンポーネントの設定、表示、修正がすべてできます。再利用可能コンポーネントまたはオブジェクトには、次のものがあります。

    ネットワーク オブジェクト / グループ
    サービス グループ
    クラス マップ
    インスペクション マップ
    正規表現
    TCP マップ
    グローバル プール
    時間範囲

- [Remote Access VPN] ペインでは、ネットワーク クライアント アクセス、クライアントレス SSL VPN ブラウザ アクセスと高度な Web 関連の設定値、AAA 設定、証明書管理、ロードバランシングを設定できます。また、次のような高度な追加の設定を実行できます。
  - VPN トンネルの IPSec 接続を設定する。
  - クライアントレス SSL VPN 接続の設定。「クライアントレス SSL VPN」によりユーザは、Web ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。
  - 「IKE」で、クライアントが VPN トンネルから接続した後にクライアントの IP アドレスを設定する。
  - 「Load Balancing」で VPN 接続のロードバランシングを設定する。
  - 「電子メール プロキシ」で電子メール プロキシを設定する。電子メール プロキシを設定すると、リモート電子メール機能をクライアントレス SSL VPN ユーザに拡張できます。
- [Site-to-Site VPN] ペインでは、サイト間 VPN 接続、グループ ポリシー、証明書管理を設定できます。また、次のような高度な設定を実行できます。
  - IKE ポリシーと IKE パラメータ（ISAKMP とも呼ばれる）。2 台のホストで IPSec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルを提供します。
- [Device Management] ペインでは、次のようなアクセスと管理のための設定を実行できます。
  - ASDM と HTTP over SSL の管理セッション。
  - FTP および TFTP クライアント。
  - CLI。
  - SNMP および ICMP。
  - 電子メール、イベント リスト、フィルタ、レート制限、syslog サーバ、SMTP などのロギング。詳細については、「ロギングの設定」を参照してください。
  - ユーザおよび AAA 認証。
  - High Availability and Scalability Wizard およびフェールオーバー。
  - 高度な設定。

（注）　CSC SSM カードまたは IPS ソフトウェアがインストールされている場合、[Trend Micro Content Security] または [IPS] 機能ボタンも表示されます。

- [IPS] ペインでは、IPS センサーを設定できます。詳細については、「IPS の設定」を参照してください。
- [Trend Micro Content Security] ペインでは、CSC SSM を設定できます（ASA 5500 シリーズ適応型セキュリティ アプライアンスで使用可能）。詳細については、「Trend Micro Content Security の設定」を参照してください。

ステップ 8　適応型セキュリティ アプライアンスを監視するには、ツールバーの [Monitoring] ボタンをクリックし、続いて [Interfaces]、[VPN]、[Trend Micro Content Security]、[Routing]、[Properties]、[Logging] のいずれかの機能ボタンをクリックして関連する監視ペインを表示します。

- [Interfaces] ペインでは、ARP テーブル、DHCP サービス、ダイナミック アクセス リスト、PPPoE クライアント、接続ステータス、およびインターフェイスの統計情報を監視できます。詳細については、「インターフェイスのモニタリング」を参照してください。
- [VPN] ペインでは、VPN 接続を監視できます。詳細については、「VPN のモニタリング」を参照してください。

- [Routing] ペインでは、ルート、OSPF LSA、および OSPF ネイバーを監視できます。詳細については、「ルーティングのモニタリング」を参照してください。
- [Properties] ペインでは、管理セッション、AAA サーバ、フェールオーバー、CRL、DNS キャッシュ、システムの統計情報を監視できます。詳細については、「プロパティのモニタリング」を参照してください。
- [Logging] ペインでは、システム ログ メッセージ、Real-Time Log Viewer、およびログ バッファを監視できます。詳細については、「ロギングのモニタリング」を参照してください。
- [Trend Micro Content Security] ペインでは、CSC SSM 接続を監視できます。詳細については、「Trend Micro Content Security のモニタリング」を参照してください。

CHAPTER 4

Startup Wizard の使用

ASDM Startup Wizard の案内に従って適応型セキュリティ アプライアンスの初期設定を行い、適応型セキュリティ アプライアンスの次の設定を定義できます。

- ホスト名
- ドメイン名
- ASDM または CLI からの管理アクセスを制限するためのパスワード
- 外部インターフェイスの IP アドレス情報
- 内部インターフェイスや DMZ インターフェイスなどのその他のインターフェイス
- NAT または PAT ルール
- DHCP サーバで使用する場合の内部インターフェイスの DHCP 設定

メイン ASDM アプリケーション ウィンドウでこの機能にアクセスするには、次のいずれかの方法を選択します。

- [Wizards] > [Startup Wizard] を選択する。
- [Configuration] > [Device Setup] > [Startup Wizard] を選択して、[Launch Startup Wizard] をクリックする。

詳細情報

- 「Web ブラウザによる ASDM の起動」（P.3-8）を参照してください。
- 『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

この項では、次のトピックについて取り上げます。

- 「ASA 5500 シリーズおよび PIX 500 シリーズ セキュリティ アプライアンスの Startup Wizard 画面」（P.4-2）
- 「ASA 5505 適応型セキュリティ アプライアンスの Startup Wizard 画面」（P.4-3）

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ASA 5500 シリーズおよび PIX 500 シリーズ セキュリティ アプライアンスの Startup Wizard 画面

表 4-1 に、ASA 5500 シリーズ適応型セキュリティ アプライアンスおよび PIX 500 シリーズ セキュリティ アプライアンスのみを設定する場合に必要な Startup Wizard の画面を一覧表示します。画面の実際の順序は、設定時の選択によって決まります。示される順序は、ASA 5505 適応型セキュリティ アプライアンスにのみ適用されます。「使用できるモード」列には、各画面が表示されるときのモードおよび追加の設定情報が一覧表示されます。選択した画面の情報を表示するには、名前をクリックしてください。

表 4-1　ASA 5500 シリーズおよび PIX 500 シリーズ セキュリティ アプライアンスの Startup Wizard 画面

画面名	使用可能状況
「Step 1 - Starting Point or Welcome」（P.4-3）	すべてのモード。Step 1 の工場出荷時のデフォルト オプションは PIX セキュリティ アプライアンスでは使用できません。
「Step 2 - Basic Configuration」（P.4-4）	
「Step 3 - Auto Update Server」（P.4-5）	シングル ルーテッドおよびシングル トランスペアレント モード。シングル トランスペアレント モードでイネーブルにすると、インターフェイス コンフィギュレーション 画面と Step 13 - DHCP Server 画面は表示されません。
「Step 4 - Management IP Address Configuration」（P.4-6）	シングル トランスペアレント モードのみ。
「外部インターフェイスのコンフィギュレーション」（P.4-23）	シングル ルーテッド モードのみ。
「外部インターフェイスのコンフィギュレーション：PPPoE」（P.4-22）	
「インターフェイス コンフィギュレーション」（P.4-22）	シングル トランスペアレント モードのみ。
「その他のインターフェイスの設定」（P.4-20）	すべてのモード。
「Step 12 - Static Routes」（P.4-14）	
「Step 13 - DHCP Server」（P.4-14）	
「Step 14 - Address Translation (NAT/PAT)」（P.4-15）	シングル ルーテッド モードのみ。
「Step 15 - Administrative Access」（P.4-16）	すべてのモード。
「Step 17 - Startup Wizard Summary」（P.4-20）	

ASA 5505 適応型セキュリティ アプライアンスの Startup Wizard 画面

表 4-2 に、ASA 5505 適応型セキュリティ アプライアンスのみを設定する場合に必要な Startup Wizard のすべての画面を一覧表示します。一覧での画面の順序は、シングル ルーテッド モードでの設定を表します。「使用できるモード」列には、各画面が表示されるときのモードおよび追加の設定情報が一覧表示されます。選択した画面の情報を表示するには、名前をクリックしてください。

表 4-2　ASA 5505 適応型セキュリティ アプライアンスの Startup Wizard 画面

画面名および順序	使用可能状況
「Step 1 - Starting Point or Welcome」（P.4-3）	すべてのモード。Step 2 の Teleworker オプションは ASA 5505 でだけ選択できます。
「Step 2 - Basic Configuration」（P.4-4）	
「Step 3 - Auto Update Server」（P.4-5）	シングル ルーテッドおよびシングル トランスペアレント モード。Teleworker を使用する設定の場合にだけイネーブルにされます。
「Step 4 - Management IP Address Configuration」（P.4-6）	シングル トランスペアレント モードのみ。
「Step 5 - Interface Selection」（P.4-6）	シングル ルーテッド モードのみ。
「Step 6 - Switch Port Allocation」（P.4-7）	
「Step 7 - Interface IP Address Configuration」（P.4-8）	
「Step 8 - Internet Interface Configuration - PPoE」（P.4-9）	
「Step 9 - Business Interface Configuration - PPoE」（P.4-10）	
「Step 10 - Home Interface Configuration - PPoE」（P.4-12）	
「Step 11 - General Interface Configuration」（P.4-13）	
「Step 12 - Static Routes」（P.4-14）	すべてのモード。Teleworker を使用する設定の場合にだけイネーブルにされます。
「Step 13 - DHCP Server」（P.4-14）	すべてのモード。
「Step 14 - Address Translation (NAT/PAT)」（P.4-15）	シングル ルーテッド モードのみ。
「Step 15 - Administrative Access」（P.4-16）	すべてのモード。
「Step 16 - Easy VPN Remote Configuration」（P.4-18）	シングル ルーテッド モード。Teleworker を使用する場合にだけイネーブルにされます。
「Step 17 - Startup Wizard Summary」（P.4-20）	すべてのモード。

Step 1 - Starting Point or Welcome

メイン ASDM アプリケーション ウィンドウからこの機能にアクセスする（マルチモードの場合を除く）には、[File] > [Reset Device to the Factory Default Configuration] を選択します。

フィールド

- [Modify existing configuration]：既存の設定を変更するには、このオプションを選択します。

- [Reset configuration to factory defaults]：設定を内部インターフェイスの工場出荷時のデフォルト値に戻すには、このオプションを選択します。
- [Configure the IP address of the management interface]：管理インターフェイスの IP アドレスとサブネット マスクを設定するには、このチェックボックスをオンにします。
- [IP Address]：管理インターフェイスの IP アドレスを指定します。
- [Subnet Mask]：ドロップダウン リストから管理インターフェイスのサブネット マスクを選択します。

（注）　設定を工場出荷時のデフォルト値にリセットすると、[Cancel] をクリックしたり、この画面を閉じたりしても、変更を元に戻せません。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Step 2 - Basic Configuration

メイン ASDM アプリケーション ウィンドウでこの機能にアクセスするには、次のいずれかの方法を選択します。

- [Configuration] > [Properties] > [Device Administration] > [Device]
- [Configuration] > [Properties] > [Device Administration] > [Password]

フィールド

- [Configure the device for Teleworker usage]：リモート ワーカーを対象とした一群の設定値を指定するには、このチェックボックスをオンにします。詳細については、「Step 16 - Easy VPN Remote Configuration」（P.4-18）を参照してください。
- [Host Name]：適応型セキュリティ アプライアンスのホスト名を指定します。ホスト名は、大文字と小文字を含む最大 63 文字の英数字で指定できます。使用するセキュリティ アプライアンスに応じて、デバイス タイプが「ASA」または「PIX」と表示されます。
- [Domain Name]：証明書で使用できる、適応型セキュリティ アプライアンスの IPSec ドメイン名を指定します。ドメイン名は、特殊文字やスペースを含まない、最大 63 文字の英数字で指定できます。
- [Privileged Mode (Enable) Password section]：ASDM または CLI からの適応型セキュリティ アプライアンスへの管理アクセスを制限できます。

（注）　パスワード フィールドを空白にすると、非常に大きなセキュリティ リスクであることを警告する [Password Confirmation] ダイアログボックスが表示されます。

- [Change privileged mode (enable) password]：現在の特権モード（イネーブル）パスワードを変更するには、このチェックボックスをオンにします。
- [Old Password]：変更前のイネーブル パスワードがある場合は、そのパスワードを指定します。
- [New Password]：新しいイネーブル パスワードを指定します。パスワードは最大 32 文字の英数字で、大文字と小文字を区別します。
- [Confirm New Password]：新しいイネーブル パスワードを再入力します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Step 3 - Auto Update Server

この画面では、Auto Update サーバから適応型セキュリティ アプライアンスをリモートで管理することができます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、[Configuration] > [Interfaces] を選択します。

フィールド

- [Enable Auto Update]：セキュリティ アプライアンスと Auto Update サーバ間の通信をイネーブルにするには、このチェックボックスをオンにします。
- [Server URL]：ドロップダウン リストから、[HTTPS] または [HTTP] を選択して、Auto Update サーバの URL の先頭を定義します。
- [Verify Server SSL certificate]：SSL 証明書が Auto Update サーバでイネーブルであることを確認するには、このチェックボックスをオンにします。
- [Username]：Auto Update サーバにログインするためのユーザ名を指定します。
- [Password]：Auto Update サーバにログインするためのパスワードを指定します。
- [Confirm Password]：確認のためにパスワードを再入力します。
- [Device ID Type]：ドロップダウン リストをクリックし、適応型セキュリティ アプライアンスを一意に識別する ID タイプを選択します。[User-defined name] を選択し、一意の ID を指定するための [Device ID] フィールドをイネーブルにします。

- [Device ID]：適応型セキュリティ アプライアンス ID として使用する一意の文字列を指定します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Step 4 - Management IP Address Configuration

この画面では、このコンテキストでのホストの管理 IP アドレスを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、[Configuration] > [Properties] > [Management IP] を選択します。

フィールド

- [Management IP Address] : ASDM またはセッション プロトコルを使用し、管理目的でこのコンテキストにアクセスできるホストの IP アドレスを指定します。
- [Subnet Mask] : 管理 IP アドレスのサブネット マスクを指定します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	—	—	—

Step 5 - Interface Selection

この画面では、ASA 5505 の 8 つのファスト イーサネット スイッチ ポートを 3 つの VLAN にグループ化できます。これらの VLAN は、別のレイヤ 3 ネットワークとして機能します。グループ化後、外部（Internet）、内部（Business）、または DMZ（Home）で構成されるインターフェイスごとに、ネッ

トワークを定義する VLAN を 1 つずつ選択または作成できます。DMZ は、ニュートラル ゾーンにある別のネットワークで、プライベート（内部）ネットワークとパブリック（外部）ネットワークの間にあります。

フィールド

[Outside VLAN] または [Internet VLAN] セクション

- [Choose a VLAN]：ドロップダウン リストから事前定義済みの外部 VLAN を番号で選択します。
- [Create a VLAN]：新しい外部 VLAN を作成するには、このチェックボックスをオンにします。
- [Enable VLAN]：外部 VLAN をイネーブルにするには、このチェックボックスをオンにします。

[Inside VLAN] または [Business VLAN] セクション

- [Choose a VLAN]：ドロップダウン リストから事前定義済みの内部 VLAN を番号で選択します。
- [Create a VLAN]：新しい内部 VLAN を作成するには、このチェックボックスをオンにします。
- [Enable VLAN]：内部 VLAN をイネーブルにするには、このチェックボックスをオンにします。

[DMZ VLAN] または [Home VLAN (Optional)] セクション

- [Choose a VLAN]：ドロップダウン リストから事前定義済みの VLAN を番号で選択します。
- [Create a VLAN]：新しい VLAN を作成するには、このチェックボックスをオンにします。
- [Do not configure]：この VLAN の設定をディセーブルにするには、このチェックボックスをオンにします。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 6 - Switch Port Allocation

この画面では、外部（Internet）、内部（Business）、または DMZ（Home）インターフェイスにスイッチ ポートを割り当てることができます。DMZ インターフェイスはトランスペアレント モードでは使用できません。関連付けられた VLAN にポートを追加する必要があります。デフォルトでは、スイッチ ポートはすべて VLAN1 で始まります。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、[Configuration] > [Interfaces] を選択します。

フィールド

[Switch Ports for Outside VLAN (vlan*id*)] または [Switch Ports for Internet VLAN (vlan*id*)] セクション

- [Available Ports]：使用できるポートのリストから、追加または削除するポートを選択します。
- [Allocated Ports]：割り当てられたポートのリストから、追加または削除するポートを選択します。

- [Add]：使用できるポートのリスト、または割り当てられたポートのリストにポートを追加します。
- [Remove]：使用できるポートのリスト、または割り当てられたポートのリストからポートを削除します。

[Switch Ports for Inside VLAN (vlan*id*)] または [Switch Ports for Business VLAN (vlan*id)*] セクション

- [Available Ports]：使用できるポートのリストから、追加または削除するポートを選択します。
- [Allocated Ports]：割り当てられたポートのリストから、追加または削除するポートを選択します。
- [Add]：使用できるポートのリスト、または割り当てられたポートのリストにポートを追加します。
- [Remove]：使用できるポートのリスト、または割り当てられたポートのリストからポートを削除します。

[Switch Ports for DMZ VLAN (vlan*id*)] または [Switch Ports for Home VLAN (vlan*id)*] セクション

- [Available Ports]：使用できるポートのリストから、追加または削除するポートを選択します。
- [Allocated Ports]：割り当てられたポートのリストから、追加または削除するポートを選択します。
- [Add]：使用できるポートのリスト、または割り当てられたポートのリストにポートを追加します。
- [Remove]：使用できるポートのリスト、または割り当てられたポートのリストからポートを削除します。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 7 - Interface IP Address Configuration

この画面では、PPPoE サーバまたは DHCP サーバから IP アドレスを取得するか、または IP アドレスとサブネット マスクを指定することによって、インターフェイスを設定できます。

フィールド

[Outside IP Address] または [Internet IP Address] セクション

- [Use the following IP address]：外部 IP アドレスを指定するには、このオプションを選択します。
- [IP Address/Mask]：特定の IP アドレスを入力し、ドロップダウン リストからサブネット マスクを選択します。
- [Use DHCP]：DHCP サーバから外部 IP アドレスを取得するには、このオプションを選択します。

- [Obtain default rote using DHCP]：DHCP サーバから外部 IP アドレスのデフォルト ルートを取得するには、このチェックボックスをオンにします。
- [Use PPoE]：PPoE サーバから外部 IP アドレスを取得するには、このオプションを選択します。

[Inside IP Address] または [Business IP Address] セクション

- [Use the following IP address]：内部 IP アドレスを指定するには、このオプションを選択します。
- [IP Address/Mask]：特定の内部 IP アドレスを入力し、ドロップダウン リストからサブネット マスクを選択します。
- [Use DHCP]：DHCP サーバから内部 IP アドレスを取得するには、このオプションを選択します。
- [Use PPoE]：PPoE サーバから内部 IP アドレスを取得するには、このオプションを選択します。

[DMZ IP Address] または [Home IP Address] セクション

- [Use the following IP address]：DMZ IP アドレスを指定するには、このオプションを選択します。
- [IP Address/Mask]：特定の DMZ IP アドレスを入力し、ドロップダウン リストからサブネット マスクを選択します。
- [Use DHCP]：DHCP サーバから DMZ IP アドレスを取得するには、このオプションを選択します。
- [Use PPoE]：PPoE サーバから DMZ IP アドレスを取得するには、このオプションを選択します。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 8 - Internet Interface Configuration - PPoE

この画面では、PPPoE サーバから IP アドレスを取得することによって、指定された外部インターフェイスを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、[Configuration] > [Interfaces] を選択します。

（注） ASA 5505 以外のすべての ASA 5500 シリーズ モデルの場合、フル ライセンスの適応型セキュリティ アプライアンスは、最大で 3 つの外部インターフェイスを含む 5 つのインターフェイスをサポートします。制限モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 3 つ、トランスペアレント モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 2 つサポートします。最大数のインターフェイスを作成した後、または最大数のインターフェイスに名前を付けた後は、VLAN を新規作成できなくなり、既存の VLAN を選択することが必要になります。

フィールド

- [Group Name]：PPoE サーバにあるグループの名前を指定します。次に進むには、グループ名を指定する必要があります。

[User Authentication] セクション

- [PPoE Username]：PPoE サーバでのユーザ名を指定します。
- [PPoE Password]：PPoE サーバでのパスワードを指定します。
- [Confirm PPoE Password]：最初に入力した PPoE パスワードを指定します。

[Authentication Method] セクション

- [PAP]：PAP 認証を使用する場合にクリックします。
- [CHAP]：CHAP 認証を使用する場合にクリックします。
- [MSCHAP]：MSCHAP 認証を使用する場合にクリックします。

[IP Address] セクション

- [Obtain an IP address using PPoE]：PPoE サーバからインターフェイスの IP アドレスを取得するには、このオプションを選択します。このフィールドはトランスペアレント モードの場合には表示されません。
- [Specify an IP Address]：インターネット インターフェイスの IP アドレスを指定します。このフィールドはトランスペアレント モードの場合には表示されません。
  - [IP Address]：インターネット インターフェイスで使用する IP アドレスを指定します。
  - [Subnet Mask]：ドロップダウン リストからインターネット インターフェイスのサブネット マスクを選択します。
- [Obtain default route using PPoE]：PPoE サーバを使用してデフォルトのルーティングを設定するには、このチェックボックスをオンにします。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 9 - Business Interface Configuration - PPoE

この画面では、PPPoE サーバから IP アドレスを取得することによって、内部インターフェイスを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、[Configuration] > [Interfaces] を選択します。

（注）　ASA 5505 以外のすべての ASA 5500 シリーズ モデルの場合、フル ライセンスの適応型セキュリティ アプライアンスは、最大で 3 つの外部インターフェイスを含む 5 つのインターフェイスをサポートします。制限モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 3 つ、トランスペアレント モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 2 つサポートします。最大数のインターフェイスを作成した後、または最大数のインターフェイスに名前を付けた後は、VLAN を新規作成できなくなり、既存の VLAN を選択することが必要になります。

フィールド

- [Group Name] : PPoE サーバにあるグループの名前を指定します。次に進むには、グループ名を指定する必要があります。

[User Authentication] セクション

- [PPoE Username] : PPoE サーバでのユーザ名を指定します。
- [PPoE Password] : PPoE サーバでのパスワードを指定します。
- [Confirm PPoE Password] : 最初に入力した PPoE パスワードを指定します。

[Authentication Method] セクション

- [PAP] : PAP 認証を使用する場合にクリックします。
- [CHAP] : CHAP 認証を使用する場合にクリックします。
- [MSCHAP] : MSCHAP 認証を使用する場合にクリックします。

[IP Address] セクション

- [Obtain an IP address using PPoE] : PPoE サーバからインターフェイスの IP アドレスを取得するには、このオプションを選択します。このフィールドはトランスペアレント モードの場合には表示されません。
- [Specify an IP Address] : 内部インターフェイスの IP アドレスを指定します。このフィールドはトランスペアレント モードの場合には表示されません。
  - [IP Address] : 内部インターフェイスで使用する IP アドレスを指定します。
  - [Subnet Mask] : ドロップダウン リストからインターネット インターフェイスのサブネット マスクを選択します。
- [Obtain default route using PPoE] : PPoE サーバを使用してデフォルトのルーティングを設定するには、このチェックボックスをオンにします。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 10 - Home Interface Configuration - PPoE

この画面では、PPPoE サーバから IP アドレスを取得することによって、DMZ インターフェイスを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、[Configuration] > [Interfaces] を選択します。

（注）　ASA 5505 以外のすべての ASA 5500 シリーズ モデルの場合、フル ライセンスの適応型セキュリティ アプライアンスは、最大で 3 つの外部インターフェイスを含む 5 つのインターフェイスをサポートします。制限モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 3 つ、トランスペアレント モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 2 つサポートします。最大数のインターフェイスを作成した後、または最大数のインターフェイスに名前を付けた後は、VLAN を新規作成できなくなり、既存の VLAN を選択することが必要になります。

フィールド

- [Group Name] : PPoE サーバにあるグループの名前を指定します。次に進むには、グループ名を指定する必要があります。

[User Authentication] セクション

- [PPoE Username] : PPoE サーバでのユーザ名を指定します。
- [PPoE Password] : PPoE サーバでのパスワードを指定します。
- [Confirm PPoE Password] : 最初に入力した PPoE パスワードを指定します。

[Authentication Method] セクション

- [PAP] : PAP 認証を使用する場合にクリックします。
- [CHAP] : CHAP 認証を使用する場合にクリックします。
- [MSCHAP] : MSCHAP 認証を使用する場合にクリックします。

[IP Address] セクション

- [Obtain an IP address using PPoE] : PPoE サーバからインターフェイスの IP アドレスを取得するには、このオプションを選択します。このフィールドはトランスペアレント モードの場合には表示されません。
- [Specify an IP Address] : DMZ インターフェイスの IP アドレスを指定します。このフィールドはトランスペアレント モードの場合には表示されません。
  - [IP Address] : DMZ インターフェイスで使用する IP アドレスを指定します。
  - [Subnet Mask] : ドロップダウン リストからインターネット インターフェイスのサブネット マスクを選択します。
- [Obtain default route using PPoE] : PPoE サーバを使用してデフォルトのルーティングを設定するには、このチェックボックスをオンにします。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 11 - General Interface Configuration

この画面では、インターフェイス間のトラフィック、および同じインターフェイスに接続されたホスト間のトラフィックを、イネーブルにしたり制限したりできます。

トラフィック制限は、オプションの設定ではありません。制限付きのライセンスしか持っていない場合は、1 つのインターフェイスから他のすべてのインターフェイスへのトラフィックを制限する必要があります。フル ライセンスまたはデバイスがトランスペアレント モードの場合、[Restrict Traffic] エリアのフィールドは表示されません。

フィールド

- [Enable traffic between two or more interfaces with the same security level] : 同じセキュリティ レベルにある複数のインターフェイス間のトラフィックをイネーブルにするには、このチェックボックスをオンにします。
- [Enable traffic between two or more hosts connected to the same interface] : 同じインターフェイスに接続された複数のホスト間のトラフィックをイネーブルにするには、このチェックボックスをオンにします。

[Restrict traffic] エリア

- [From interface] : ドロップダウン リストからインターフェイスを選択することによって、そのインターフェイスからのトラフィックを制限できます。
- [To interface] : ドロップダウン メニューからインターフェイスを選択することによって、そのインターフェイスへのトラフィックを制限できます。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 12 - Static Routes

この画面では、任意のインターフェイスのルータに接続されたネットワークにアクセスするスタティック ルートを作成、編集、および削除できます。

詳細情報

- 「Static Routes」（P.16-43）
- 「Add/Edit Static Routes」（P.4-14）
- 『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Static Routes

このダイアログボックスでは、スタティック ルートを追加または編集できます。詳細については、「Add/Edit Static Route」（P.16-46）を参照してください。

Step 13 - DHCP Server

この画面では、内部インターフェイスでホストする DHCP サーバとして適応型セキュリティ アプライアンスを設定できます。メイン ASDM アプリケーション ウィンドウから他のインターフェイスの DHCP サーバを設定するには、[Configuration] > [Properties] > [DHCP Services] > [DHCP Server] を選択します。詳細については、「DHCP サーバ」（P.11-4）を参照してください。

フィールド

- [Enable DHCP server on the inside interface]：内部インターフェイスから DHCP サーバへの接続を許可するには、このチェックボックスをオンにします。

[DHCP Address Pool] セクション

- [Starting IP Address]：DHCP サーバ プールの開始範囲を、IP アドレス ブロックとして最下位から最上位の順に指定します。

（注）　適応型セキュリティ アプライアンスは、最大で 256 の IP アドレスをサポートします。

- [Ending IP Address]：DHCP サーバ プールの終了範囲を、IP アドレス ブロックとして最下位から最上位の順に指定します。

[DHCP Parameters] セクション

- [Enable auto-configuration] : DNS サーバ、WINS サーバ、リース期間、および ping タイムアウトの設定の自動コンフィギュレーションを許可するには、このチェックボックスをオンにします。
- [DNS Server 1] : DNS サーバの IP アドレスを指定します。
- [WINS Server 1] : WINS サーバの IP アドレスを指定します。
- [DNS Server 2] : 代替 DNS サーバの IP アドレスを指定します。
- [WINS Server 2] : 代替 WINS サーバの IP アドレスを指定します。
- [Lease Length (secs)] : リースの期間が終了する前に、割り当て IP アドレスをクライアントが使用できる時間を秒単位で指定します。デフォルト値は 3600 秒（1 時間）です。
- [Ping Timeout] : ping のタイムアウト値のパラメータをミリ秒単位で指定します。
- [Domain Name] : DNS を使用する DNS サーバのドメイン名を指定します。
- [Enable auto-configuration from interface] : DHCP 自動コンフィギュレーションをイネーブルにし、メニューからインターフェイスを選択するには、このチェックボックスをオンにします。画面の前のセクションで指定する値は、自動設定による設定値よりも優先されます。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Step 14 - Address Translation (NAT/PAT)

この画面では、使用するセキュリティ アプライアンスでの NAT および PAT を設定することができます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、[Configuration] > [NAT] を選択します。

PAT により、設定した IP アドレスの 1 つだけがグローバル アドレスとして使用されます。また、複数の発信セッションが 1 つの IP アドレスから開始されたかのように見せることができます。PAT では、最大 65,535 のホストが 1 つの外部 IP アドレスで接続を開始できます。

NAT を使用する場合は、内部インターフェイスのすべてのアドレスを外部インターフェイスのアドレスに変換するときに使用するアドレス範囲を入力します。プールのグローバル アドレスは、各発信接続で使用される IP アドレスと、発信接続が着信接続になった場合の IP アドレスに使用されます。

PAT を使用する場合は、以下の点に注意してください。

- PAT は、キャッシング ネーム サーバでは動作しません。
- マルチメディア アプリケーション プロトコルがセキュリティ アプライアンスを通過するには、該当するインスペクション エンジンをイネーブルにする必要があります。
- PAT は、**established** コマンドでは動作しません。

- パッシブ FTP を使用する場合は、**inspect protocol ftp strict** コマンドを **access-list** コマンドと一緒に使用して、発信 FTP トラフィックを許可します。
- 上位レベルのセキュリティ インターフェイス上の DNS サーバでは、PAT を使用できません。

フィールド

- [Use Network Address Translation (NAT)] : NAT および変換に使用される IP アドレス範囲をイネーブルにする場合に選択します。
- [Starting Global IP Address] : 変換に使用される IP アドレス範囲の最初の IP アドレスを指定します。
- [Ending Global IP Address] : 変換に使用される IP アドレス範囲の最後の IP アドレスを指定します。
- [Subnet Mask (optional)] : 変換に使用される IP アドレス範囲のサブネット マスクを指定します。
- [Use Port Address Translation (PAT)] : PAT をイネーブルにする場合に選択します。このオプションを選択した場合は、次のいずれかを選択してください。

（注） IPSec に PAT を使用すると正しく動作しない場合があります。これは、外部のトンネル エンドポイント デバイスが、同じ IP アドレスの複数のトンネルを処理できないためです。

  - [Use the IP address on the outside interface] : PAT で外部インターフェイスの IP アドレスを使用する場合に選択します。
  - [Specify an IP address] : PAT で使用する IP アドレスを入力します。

    [IP Address] : PAT の外部インターフェイスの IP アドレスを指定します。

    [Subnet Mask (optional)] : ドロップダウン リストからサブネット マスクを選択します。
- [Enable traffic through the firewall without translation] : トラフィックを変換しないでファイアウォールを通過させる場合に選択します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 15 - Administrative Access

この画面では、セキュリティ アプライアンスでの管理アクセスを設定できます。

フィールド

- [Type]：ホストまたはネットワークがセキュリティ アプライアンスにアクセスするときに、ASDM の HTTP over SSL、SSH、または Telnet のどれを使用するかを指定します。
- [Interface]：ホストまたはネットワーク名を表示します。
- [IP address]：ホストまたはネットワークの IP アドレスを表示します。
- [Mask]：ホストまたはネットワークのサブネット マスクを表示します。
- [Enable HTTP server for HTTPS/ASDM access]：ASDM にアクセスするための HTTP サーバへのセキュアな接続をイネーブルにするには、このチェックボックスをオンにします。
- [Add]：アクセス タイプとインターフェイスを追加し、次に管理目的でのみそのインターフェイスに接続するホスト ネットワークの IP アドレスとネットマスクを指定します。詳細については、「Add/Edit Administrative Access Entry」を参照してください。
- [Edit]：インターフェイスを変更します。詳細については、「Add/Edit Administrative Access Entry」を参照してください。
- [Delete]：インターフェイスを削除します。
- [Enable ASDM history metrics]：ASDM で統計を収集および表示できるようにするには、このチェックボックスをオンにします。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Administrative Access Entry

このダイアログボックスでは、ホストを設定できます。メイン ASDM アプリケーション ウィンドウでこの機能にアクセスするには、次のいずれかの方法を選択します。

- [Configuration] > [Properties] > [Device Access] > [HTTPS/ASDM]
- [Configuration] > [Properties] > [Device Access] > [Telnet]
- [Configuration] > [Properties] > [Device Access] > [SSH]
- [Configuration] > [Properties] > [History Metrics]

フィールド

- [Access Type]：ドロップダウン リストで、次に示す CLI コンソール セッションの事前設定された接続タイプの 1 つを選択します。
  - ASDM/HTTPS
  - SSH

– Telnet

（注）　ASDM は、セキュリティ アプライアンスとのすべての通信で HTTP over SSL を使用します。

- [Interface Name]：事前設定されたインターフェイスのリストから選択します。
- [IP Address]：インターフェイスの IP アドレスを指定します。
- [Subnet Mask]：サブネット マスクの IP アドレスの選択肢から、インターフェイスのサブネット マスクを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Step 16 - Easy VPN Remote Configuration

この画面では、適応型セキュリティ アプライアンスと、リモート Cisco VPN 3000 コンセントレータ、Cisco ルータ、または Easy VPN サーバとして動作している適応型セキュリティ アプライアンスとの間に、セキュアな VPN トンネルを設定できます。適応型セキュリティ アプライアンスは Easy VPN リモート デバイスとして動作するため、離れた場所に VPN を展開できます。

（注）　この画面にアクセスするには、Step 2 - Basic Configuration の [Configure the device for Teleworker usage] チェックボックスをオンにし、インターフェイス コンフィギュレーションの [Enable Auto Update] チェックボックスをオフにする必要があります。

次の 2 つの動作モードを使用できます。

- クライアント モード
- ネットワーク拡張モード

クライアント モードでは、適応型セキュリティ アプライアンスは内部ネットワークのクライアントの IP アドレスを公開しません。代わりに、適応型セキュリティ アプライアンスは、NAT を使用してプライベート ネットワークの IP アドレスを単一の割り当て済み IP アドレスに変換します。このモードでは、プライベート ネットワークの外部からデバイスに ping を実行したり、デバイスにアクセスしたりできません。

ネットワーク拡張モードでは、適応型セキュリティ アプライアンスが、割り当てられた IP アドレスを置き換えることによってローカル ホストの IP アドレスを保護することはありません。したがって、VPN 接続の相手側ホストは、ローカル ネットワークのホストと直接通信できます。

適応型セキュリティ アプライアンスをこれらの 2 つのモードのいずれかに設定するには、次のガイドラインに従ってください。

次の場合はクライアント モードを使用します。

- VPN 接続をクライアント トラフィックで開始する場合

- ローカル ホストの IP アドレスをリモート ネットワークで非表示にする場合
- ASA 5505 の DHCP からローカル ホストに IP アドレスを渡す場合

次の場合はネットワーク拡張モードを使用します。

- トラフィック転送の必要がなくても VPN 接続を開いておく場合
- リモート ホストをローカル ネットワークから直接通信を可能にする場合
- ローカル ネットワークのホストがスタティック IP アドレスの場合

フィールド

- [Enable Easy VPN remote]：適応型セキュリティ アプライアンスが Easy VPN リモート デバイスとして動作できるようにするには、このチェックボックスをオンにします。この機能をイネーブルにしない場合、VPN トンネルからインターフェイス外部の適応型セキュリティ アプライアンスにアクセスできるホストは、その適応型セキュリティ アプライアンスをリモート管理できます。

[Mode] セクション

- [Client Mode]：DHCP サーバを使用して、内部ネットワーク上のホストのダイナミック IP アドレスを生成する場合にクリックします。
- [Network extension]：内部ネットワークのホストにスタティック IP アドレスがある場合にクリックします。

[Group Settings] セクション

- [Use X.509 Certificate]：X.509 証明書を使用して、IPSec Main モードをイネーブルにする場合にクリックします。ドロップダウン リストからトラストポイントを選択するか、または入力します。
- [Use group password]：ユーザ グループのパスワードを入力します。
  - [Group Name]：ユーザ グループの名前を入力します。
  - [Password]：ユーザ グループのパスワードを入力します。
  - [Confirm password]：パスワードを確認する必要があります。

[User Settings] セクション

- [Username]：設定のユーザ名を入力します。
- [Password]：設定のパスワードを入力します。
- [Confirm Password]：設定のパスワードを確認する必要があります。

[Easy VPN Server] セクション

- [Primary server]：プライマリ Easy VPN サーバの IP アドレスを入力します。
- [Secondary server]：セカンダリ Easy VPN サーバの IP アドレスを入力します。

（注） 適応型セキュリティ アプライアンスは、1 台のプライマリ サーバと 10 台までのセカンダリ サーバで構成される、最大で 11 台の Easy VPN サーバをサポートします。ASA の Easy VPN リモート デバイスを Easy VPN サーバに接続できるようにするには、ISP を利用して両方のデバイス間のネットワーク接続を確立しておく必要があります。ASA 5500 シリーズ適応型セキュリティ アプライアンスを DSL またはケーブル モデムに接続した後は、ISP の指示に従ってネットワーク接続設定を完了してください。IP アドレスは、PPPoE サーバ、DHCP サーバ、またはスタティック コンフィギュレーションから取得できます。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 17 - Startup Wizard Summary

この画面には、セキュリティ アプライアンスに対して行ったすべての設定の概要が表示されます。

- 前の画面での設定を変更するには、[Back] をクリックします。
- Startup Wizard をブラウザから直接起動した場合は、[Finish] をクリックすると、ウィザードで作成された設定が適応型セキュリティ アプライアンスに自動的に送信され、フラッシュ メモリに保存されます。
- ASDM 内で Startup Wizard を実行した場合は、その設定を明示的にフラッシュ メモリに保存する必要があります。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

その他のインターフェイスの設定

この画面では、残りのインターフェイスを設定できます。

フィールド

- [Interface]：元のホストまたはネットワークが存在するネットワーク インターフェイスを表示します。
- [Name]：設定対象となるインターフェイスの名前を表示します。
- [Security Level]：インターフェイスのセキュリティ レベル範囲を 0 ～ 100 で表示します。100 は内部インターフェイス、0 は外部インターフェイスに割り当てられます。境界インターフェイスには、1 ～ 99 の範囲の番号が使用できます。0 ～ 100 のセキュリティ レベルは、デフォルトでは設定されません。

- [Enable traffic between two or more interfaces with same security levels] : 同じセキュリティ レベルを複数のインターフェイスに設定し、それらのインターフェイス間のトラフィックをイネーブルにするには、このチェックボックスをオンにします。
- [Enable traffic between two or more hosts connected to the same interface] : 複数のホストにあるインターフェイスでトラフィックをイネーブルにするには、このチェックボックスをオンにします。
- [Edit] : [インターフェイスの編集] ダイアログボックスでインターフェイスの設定を変更する場合にクリックします。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

インターフェイスの編集

メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、[Configuration] > [Interfaces] を選択します。

フィールド

- [Interface] : 編集対象として選択したインターフェイスの名前を表示します。
- [Interface Name] : 選択したインターフェイスの名前を表示します。このインターフェイスの名前は変更できます。
- [Security Level] : 選択したインターフェイスのセキュリティ レベルを表示します。インターフェイスのセキュリティ レベルは選択できます。インターフェイスのセキュリティ レベルを下げると、警告メッセージが表示されます。
- [Use PPPoE] : 外部インターフェイスに IP アドレスを割り当てる場合に PPPoE を認証方式として使用するには、このチェックボックスをオンにします。

（注）　PPPoE は複数のインターフェイスで使用できるので、PPPoE クライアントの各インスタンスでは、別のユーザ名とパスワードを持つ異なる認証レベルを必要とする場合があります。

- [Use DHCP] : 適応型セキュリティ アプライアンスを DHCP サーバとして使用するには、このチェックボックスをオンにします。
- [Uses the following IP address] : インターフェイスの特定の IP アドレスを入力するには、このチェックボックスをオンにします。
- [IP Address] : インターフェイスの IP アドレスを編集します。
- [Subnet Mask] : ドロップダウン リストから既存のサブネット マスクを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

インターフェイス コンフィギュレーション

この画面では、残りのインターフェイスを設定し、複数のインターフェイス間のトラフィックをイネーブルにすることができます。

フィールド

- [Edit] : [インターフェイスの編集] ダイアログボックスでインターフェイスの設定を変更する場合にクリックします。
- [Enable traffic between two or more interfaces with the same security level] : 同じセキュリティ レベルにある複数のインターフェイス間のトラフィックをイネーブルにするには、このチェックボックスをオンにします。

（注）　IP 関連のフィールドは、トランスペアレント モードでは表示されません。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

外部インターフェイスのコンフィギュレーション：PPPoE

この画面では、PPPoE サーバから IP アドレスを取得することによって、外部インターフェイスを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、[Configuration] > [Interfaces] を選択します。

フィールド

- [Group Name] : インターフェイスの名前を指定します。次に進むには、グループ名を指定する必要があります。

- [User Authentication] エリア
  - [PPPoE Username]：認証に必要な PPPoE ユーザ名を指定します。
  - [PPPoE Password]：認証に必要な PPPoE パスワードを指定します。
  - [Confirm PPPoE Password]：PPPoE パスワードを確認します。
- [Authentication Method] エリア

  PPPoE のデフォルトの認証方式は PAP です。CHAP または MS-CHAP を手動で設定するオプションも選択できます。
  - [PAP]：認証方式として PAP を選択する場合はこのチェックボックスをオンにします。この方式では、ユーザ名とパスワードは暗号化されません。
  - [CHAP]：CHAP 認証を選択する場合はこのチェックボックスをオンにします。CHAP はリモート エンドを識別するだけで、不正アクセスを防止するわけではありません。その後、アクセス サーバはユーザにアクセス権限があるかどうかを判断します。
  - [MSCHAP]：Windows オペレーティング システムを使用するコンピュータとアクセス サーバ間の PPP 接続用に MS-CHAP 認証を選択するには、このチェックボックスをオンにします。
- [IP Address] エリア

  PPPoE のデフォルトの認証方式は PAP です。CHAP または MS-CHAP を手動で設定するオプションも選択できます。
  - [Obtain IP Address using PPPoE]：PPPoE サーバを使用して IP アドレスを取得する場合にクリックします。
  - [Specify an IP address]：インターフェイスの IP アドレスを指定する場合にクリックします。

    [IP Address]：インターフェイスの IP アドレスを入力します。

    [Subnet Mask]：ドロップダウン リストからインターフェイスのサブネット マスクを入力または選択します。
  - [Obtain default route using PPPoE]：PPPoE サーバと PPPoE クライアント間のデフォルト ルートを取得する場合にクリックします。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

外部インターフェイスのコンフィギュレーション

この画面では、IP アドレスを指定するか、PPPoE サーバまたは DHCP サーバから IP アドレスを取得することによって、外部インターフェイスを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、[Configuration] > [Interfaces] を選択します。

（注）　ASA 5505 以外のすべての ASA 5500 シリーズ モデルの場合、フル ライセンスの適応型セキュリティ アプライアンスは、最大で 3 つの外部インターフェイスを含む 5 つのインターフェイスをサポートします。制限モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 3 つ、トランスペアレント モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 2 つサポートします。最大数のインターフェイスを作成した後、または最大数のインターフェイスに名前を付けた後は、VLAN を新規作成できなくなり、既存の VLAN を選択することが必要になります。

フィールド

- [Interface]：インターフェイスをドロップダウン リストから選択します。
- [Interface Name]：新しいインターフェイスに名前を追加するか、または既存のインターフェイスに関連付けられた名前を表示します。
- [Enable interface]：インターフェイスを特権モードでアクティブにするには、このチェックボックスをオンにします。
- [Security Level]：インターフェイスのセキュリティ レベル範囲を 0 ～ 100 で表示します。100 は内部インターフェイス、0 は外部インターフェイスに割り当てられます。境界インターフェイスには、1 ～ 99 の範囲の番号が使用できます。0 ～ 100 のセキュリティ レベルは、デフォルトでは設定されません。
- [Use PPPoE]：PPPoE サーバから IP アドレスを取得する場合にクリックします。
- [Use DHCP]：DHCP サーバから IP アドレスを取得する場合にクリックします。
- [Obtain default route using DHCP]：DHCP を使用してデフォルト ゲートウェイの IP アドレスを取得するには、このチェックボックスをオンにします。
- [Use the following IP address]：インターフェイスの IP アドレスを手動で指定するには、このオプションを選択します。このフィールドはトランスペアレント モードの場合には表示されません。
- [IP Address]：外部インターフェイスの IP アドレスを指定します。このフィールドはトランスペアレント モードの場合には表示されません。
- [Subnet Mask]：ドロップダウン リストから外部インターフェイスのサブネット マスクを選択します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

CHAPTER 5

インターフェイスの設定

この章では、物理イーサネット インターフェイスを設定してイネーブルにする方法、冗長インターフェイス ペアを作成する方法、およびサブインターフェイスを追加する方法について説明します。ファイバと銅線の両方のイーサネット ポートがある場合（ASA 5510 以降のシリーズの適応型セキュリティ アプライアンスに搭載されている 4GE SSM など）、この章ではインターフェイス メディア タイプの設定方法について説明します。各インターフェイス（物理、冗長、またはサブインターフェイス）では、名前、セキュリティ レベル、および IP アドレス（ルーテッド モードのみ）を設定する必要もあります。

（注） ASA 5505 適応型セキュリティ アプライアンスのインターフェイスを設定するには、第 7 章「Cisco ASA 5505 適応型セキュリティ アプライアンス用スイッチ ポートおよび VLAN インターフェイスの設定」を参照してください。

マルチ コンテキスト モードでインターフェイスを設定するには、第 6 章「マルチ モードのインターフェイスの設定」を参照してください。

この章は、次の項で構成されています。

インターフェイスの概要

この項では、物理インターフェイス、冗長インターフェイス、およびサブインターフェイスについて説明します。次の項目を取り上げます。

物理インターフェイスの概要

この項では、物理インターフェイスについて説明します。次の項目を取り上げます。

- 「物理インターフェイスのデフォルト設定」（P.5-2）
- 「コネクタ タイプ」（P.5-2）
- 「Auto-MDI/MDIX 機能」（P.5-2）

物理インターフェイスのデフォルト設定

デフォルトでは、銅線（RJ-45）インターフェイスの速度と二重通信は、オートネゴシエーションに設定されます。

コネクタ タイプ

ASA 5550 適応型セキュリティ アプライアンスと、ASA 5510 以降の適応型セキュリティ アプライアンスの 4GE SSM には、銅線 RJ-45 とファイバ SFP の 2 つのコネクタ タイプがあります。RJ-45 がデフォルトです。

ファイバ SFP コネクタを使用するには、メディア タイプを SFP に設定する必要があります。ファイバ インターフェイスでは、速度は固定であり、二重通信はサポートされていませんが、インターフェイスをリンク パラメータ ネゴシエーションあり（デフォルト）またはネゴシエーションなしに設定することができます。

Auto-MDI/MDIX 機能

ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

冗長インターフェイスの概要

論理冗長インターフェイスは、アクティブとスタンバイの物理インターフェイスからなるペアです。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定してセキュリティ アプライアンスの信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。最大 8 個の冗長インターフェイス ペアを設定できます。

その後のすべてのセキュリティ アプライアンス コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。

この項では、冗長インターフェイスの概要を説明します。次の項目を取り上げます。

- 「冗長インターフェイスとフェールオーバーのガイドライン」（P.5-3）
- 「冗長インターフェイスの MAC アドレス」（P.5-3）
- 「冗長インターフェイスで使用する場合の物理インターフェイスのガイドライン」（P.5-3）

冗長インターフェイスとフェールオーバーのガイドライン

メンバー インターフェイスを追加する場合は次のガイドラインに従います。

- フェールオーバーまたはステート リンク用に冗長インターフェイスを使用する場合は、プライマリ ユニットに加えてセカンダリ ユニット上の基本的なコンフィギュレーションの一部として冗長インターフェイスを設定する必要があります。
- フェールオーバーまたはステート リンク用に冗長インターフェイスを使用する場合は、2 つのユニット間にスイッチまたはハブを配置する必要があります。両ユニットは直接接続できません。スイッチやハブがなくても、プライマリ ユニット上のアクティブ ポートをセカンダリ ユニット上のスタンバイ ポートに直接接続できる場合もあります。
- フェールオーバーが発生しているかどうか冗長インターフェイスをモニタできます。必ず論理冗長インターフェイス名を参照してください。
- アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合、デバイスレベルのフェールオーバーをモニタしているときには、冗長インターフェイスで障害が発生しているように見えません。冗長インターフェイスで障害が発生しているように見えるのは、両方の物理インターフェイスで障害が発生したときだけです。

冗長インターフェイスの MAC アドレス

冗長インターフェイスは、最初に追加された物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに MAC アドレスを割り当てることができます。これはメンバ インターフェイスの MAC アドレスに関係なく使用されます（「インターフェイスの設定」（P.5-5）または 「セキュリティ コンテキストの設定」（P.9-20）を参照）。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

冗長インターフェイスで使用する場合の物理インターフェイスのガイドライン

メンバー インターフェイスを追加する場合は次のガイドラインに従います。

- 両方のメンバ インターフェイスが同じ物理タイプである必要があります。たとえば、両方ともイーサネットにする必要があります。
- 物理インターフェイスを冗長インターフェイスに追加すると、名前、IP アドレス、およびセキュリティ レベルは削除されます。

注意　コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

- 冗長インターフェイス ペアを構成する物理インターフェイスで設定できるのは物理パラメータだけです。
- アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。

VLAN サブインターフェイスと 802.1Q トランキングの概要

サブインターフェイスを使用すると、1 つの物理インターフェイスまたは冗長インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはセキュリティ アプライアンスを追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。

この項では、次のトピックについて取り上げます。

- 「最大サブインターフェイス数」（P.5-4）
- 「物理インターフェイス上のタグなしパケットの禁止」（P.5-4）

最大サブインターフェイス数

プラットフォームに許容されるサブインターフェイスの数を決定するには、付録 A「機能のライセンスと仕様」を参照してください。

物理インターフェイス上のタグなしパケットの禁止

物理インターフェイスはタグの付いていないパケットを通過させるため、サブインターフェイスを使用する場合、通常は物理インターフェイスでトラフィックを通過させないようにします。この特性は、冗長インターフェイス ペアのアクティブな物理インターフェイスにも当てはまります。サブインターフェイスでトラフィックを通過させるには物理的インターフェイスまたは冗長インターフェイスをイネーブルにする必要があるため、物理インターフェイスまたは冗長インターフェイスでは、トラフィックを名前指定しないことで通過させないようにします。物理インターフェイスまたは冗長インターフェイスでタグなしパケットを通過させる場合は、通常どおり name コマンドを設定できます。

インターフェイスのデフォルトの状態

インターフェイスには、次のデフォルト状態があります。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに名前「inside」を付けて、明示的にセキュリティ レベルを設定しないと、セキュリティ アプライアンスはセキュリティ レベルを 100 に設定します。

各インターフェイスには、0（最下位）～ 100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当

てられる場合があります。DMZ など、その他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。詳細については、「同じセキュリティ レベルの通信のイネーブル化」（P.5-9）を参照してください。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイス間では、同じセキュリティ レベル以下の他のインターフェイスへのアクセスが暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけがセキュリティ アプライアンスを通過することが許可されます。

- フィルタリング：HTTP(S) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信のいずれのトラフィックもフィルタリングできます。

- NAT コントロール：NAT コントロールをイネーブルにする場合、高いセキュリティ レベルのインターフェイス（内部）上のホストから低いセキュリティ レベルのインターフェイス（外部）上のホストにアクセスするときは、内部インターフェイスのホストに NAT を設定する必要があります。

  NAT コントロールをイネーブルにしない場合、または同じセキュリティ レベルのインターフェイス間においては、任意のインターフェイス間で NAT を使用することも、使用しないこともできます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要になることがあります。

- **established** コマンド：このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り接続が許可されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信の両方の接続に対して **established** コマンドを設定できます。

インターフェイスの設定

インターフェイスを設定するには、次の手順を実行します。概要については、「インターフェイスの概要」（P.5-1）を参照してください。

（注）　フェールオーバーを使用している場合は、フェールオーバー通信およびステートフル フェールオーバー通信に予約されているインターフェイスには、この方法で名前を付けないでください。フェールオーバーおよびステート リンクの設定については、第 14 章「ハイ アベイラビリティ」を参照してください。ただし、この手順を使用して速度やデュプレックスなどの物理インターフェイスのプロパティを設定できます。

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインに移動します。

デフォルトでは、すべての物理インターフェイスが一覧表示されます。物理インターフェイスを編集するか、サブインターフェイスまたは冗長インターフェイスを追加できます。

- 物理インターフェイスまたはその他の既存のインターフェイスを編集するには、そのインターフェイス行を選択して、[Edit] をクリックします。

  [Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。
- サブインターフェイスを追加および設定するには、次の手順を実行します。
  - **a.** [Add] > [Interface] をクリックします。

    [Add Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。
  - **b.** [Hardware Port] ドロップダウン リストから、サブインターフェイスを追加する物理インターフェイスを選択します。
  - **c.** [VLAN ID] フィールドに、1 ～ 4095 の VLAN ID を入力します。

    一部の VLAN ID は接続スイッチ用に予約されている場合があります。詳細については、スイッチのマニュアルを確認してください。
  - **d.** [Subinterface ID] フィールドに、サブインターフェイス ID を 1 ～ 4294967293 の整数で入力します。

    許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。
  - **e.** ステップ 2 に従ってインターフェイスの設定を続行します。
- 冗長インターフェイスを追加および設定するには、次の手順を実行します。
  - **a.** [Add] > [Redundant Interface] をクリックします。

    [Add Redundant Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。
  - **b.** [Redundant ID] フィールドで、1 ～ 8 の整数を入力します。
  - **c.** [Primary Interface] ドロップダウン リストから、プライマリにする物理インターフェイスを選択します。

    サブインターフェイスを持たず、まだコンテキストに割り当てられていないインターフェイスを必ず選択してください。
  - **d.** [Secondary Interface] ドロップダウン リストから、セカンダリにする物理インターフェイスを選択します。
  - **e.** ステップ 2 に従ってインターフェイスの設定を続行します。

ステップ 2　[Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 3　[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

詳細については、「デフォルトのセキュリティ レベル」（P.5-4）を参照してください。

ステップ 4　（任意）このインターフェイスを管理専用インターフェイスとして設定するには、[Dedicate this interface to management-only] をオンにします。

管理専用インターフェイスでは、通過トラフィックは受け入れられません。

ステップ 5　インターフェイスがまだイネーブルでない場合は、[Enable interface] をオンにします。

ステップ 6　IP アドレスを設定するには、次のいずれかのオプションを使用します。

ルーテッド ファイアウォール モードでは、すべてのインターフェイスに対する IP アドレスを設定します。トランスペアレント ファイアウォール モードでは、インターフェイスごとに IP アドレスを設定するのではなく、全体 セキュリティ アプライアンス またはコンテキスト全体に IP アドレスを設定します。トラフィックを通過させない Management 0/0 管理専用インターフェイスの場合は例外となります。トランスペアレント ファイアウォール モードのセキュリティ アプライアンス全体またはコンテキスト全体の管理 IP アドレスを設定するには、[管理 IP アドレス] ペインを参照してください。Management 0/0 インターフェイスまたはサブインターフェイスの IP アドレスを設定するには、この手順を使用します。

フェールオーバーで使用する場合、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブで、スタンバイ IP アドレスを設定します。

- IP アドレスを手動で設定するには、[Use Static IP] をクリックして IP アドレスとマスクを入力します。
- DHCP サーバから IP アドレスを取得するには、[Obtain Address via DHCP] をクリックします。

a. （任意）オプション 61 用に、デフォルトの内部生成文字列ではなく MAC アドレスを強制的に DHCP 要求パケット内に保存するには、[For the client identifier in DHCP option 61] > [Use MAC address] をクリックします。一部の ISP では、オプション 61 がインターフェイスの MAC アドレスであると想定しています。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。デフォルトの文字列を使用するには、[Use "Cisco-<MAC>-<interface_name>-<host>"] をクリックします。

b. （任意）DHCP サーバからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。

c. （任意）アドミニストレーティブ ディスタンスを既知のルートに割り当てるには、[DHCP Learned Route Metric] フィールドに 1 ～ 255 の値を入力します。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

d. （任意）DHCP の既知のルートのトラッキングをイネーブルにするには、[Enable Tracking for DHCP Learned Routes] をオンにします。次の値を設定します。

[Track ID] : ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

[Track IP Address] : トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。

（注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

[SLA ID] : SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。

[Monitoring Options] : [Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。

e. （任意）リースを更新するには、[Renew DHCP Lease] をクリックします。

f. （任意）セキュリティ アプライアンスが DHCP クライアント パケットにブロードキャスト フラグを設定できるようにするには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をクリックします。このオプションにより、DHCP クライアントが IP アドレスを要求する Discover を送信すると DHCP パケット ヘッダーのブロードキャスト フラグが 1 に設定されます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。このオプションを選択しな

いと、ブロードキャスト フラグは 0 に設定され、DHCP サーバは提供された IP アドレスを使用してクライアントに応答パケットをユニキャストします。DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

- PPPoE を使用して IP アドレスを取得するには、[Use PPPoE] をオンにします。
  a. [Group Name] フィールドで、グループ名を指定します。
  b. [PPPoE Username] フィールドで、ISP から提供されたユーザ名を指定します。
  c. [PPPoE Password] フィールドで、ISP から提供されたパスワードを指定します。
  d. [Confirm Password] フィールドに、パスワードを再入力します。
  e. PPP 認証の場合は、[PAP]、[CHAP]、または [MSCHAP] のいずれかをクリックします。

     PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

  f. （任意）フラッシュ メモリにユーザ名とパスワードを保存するには、[Store Username and Password in Local Flash] をオンにします。

     セキュリティ アプライアンスは、NVRAM の特定の場所にユーザ名とパスワードを保存します。Auto Update Server が **clear config** コマンドをセキュリティ アプライアンスに送信して、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再度認証できます。

  g. （任意）[PPPoE IP Address and Route Settings] ダイアログボックスを表示し、アドレッシングおよびトラッキングのオプションを選択するには、[IP Address and Route Settings] をクリックします。詳細については、「PPPoE IP Address and Route Settings」（P.5-19）を参照してください。

ステップ 7　（任意）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 8　（任意）メディア タイプ、デュプレックス、および速度を設定するには、[Configure Hardware Properties] ボタンをクリックします。

a. ASA 5550 適応型セキュリティ アプライアンスまたは 4GE SSM を使用している場合は、[Media Type] ドロップダウン リストから [RJ-45] または [SFP] を選択できます。

   RJ-45 がデフォルトです。

b. RJ-45 インターフェイスに二重通信を設定するには、[Duplex] ドロップダウン リストからインターフェイス タイプに応じて [Full]、[Half]、または [Auto] を選択します。

c. 速度を設定するには、[Speed] ドロップダウン リストから値を選択します。

   使用できる速度は、インターフェイス タイプによって異なります。常に 1000 Mbps である SFP インターフェイスでは、速度を [Negotiate] または [Nonegotiate] に設定できます。[Negotiate]（デフォルト）ではリンク ネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。[Nonegotiate] では、リンク パラメータのネゴシエーションを行いません。ASA 5500 シリーズの適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。

Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

d. [OK] をクリックして [Hardware Properties] の変更を受け入れます。

ステップ 9　（任意）MTU を設定するには、[Advanced] タブをクリックして、[MTU] フィールドに 300 ～ 65,535 バイトの値を入力します。

デフォルトは 1500 バイトです。

ステップ 10　（任意）MAC アドレスをこのインターフェイスに手動で割り当てるには、[Advanced] タブで、[Active Mac Address] フィールドに MAC アドレスを H.H.H 形式（H は 16 ビットの 16 進数）で入力します。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。

フェールオーバーを使用する場合、[Standby Mac Address] フィールドにスタンバイ MAC アドレスを入力します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。冗長インターフェイスは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。このフィールドを使用して冗長インターフェイスに MAC アドレスを割り当てると、メンバ インターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。

サブインターフェイスに一意の MAC アドレスを割り当てることが必要になる場合があります。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

ステップ 11　[OK] をクリックします。

同じセキュリティ レベルの通信のイネーブル化

デフォルトでは、セキュリティ レベルが同じインターフェイス同士は通信できません。同一セキュリティ レベルのインターフェイス間での通信を許可すると、101 を超える通信インターフェイスを設定できます。インターフェイスごとに異なるレベルを使用し、同じセキュリティ レベルにインターフェイスを割り当てないようにすると、1 レベルにつき 1 つのインターフェイスしか設定できません（0 ～ 100）。

（注）　NAT 制御をイネーブルにする場合、同一セキュリティ レベルのインターフェイス間では NAT を設定する必要がありません。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

同じインターフェイスに接続されているホスト間の通信をイネーブルにすることもできます。

- 同じセキュリティ レベルのインターフェイス間の通信をイネーブルにするには、[Configuration] > [Interfaces] ペインで、[Enable traffic between two or more interfaces which are configured with same security level] をオンにします。
- 同じインターフェイスに接続されているホスト間の通信をイネーブルにするには、[Enable traffic between two or more hosts connected to the same interface] をオンにします。

[Interface] フィールドの説明

この項では、次のトピックについて取り上げます。

Interfaces

フィールド

- [Interface]：インターフェイス ID を表示します。割り当てられているすべてのインターフェイスが自動的に表示されます。サブインターフェイスは、インターフェイス ID とそれに続く *.n* で示されます。*n* はサブインターフェイス番号です。冗長インターフェイスは、Redundant *n* と呼ばれます。
- [Name]：インターフェイス名を表示します。
- [Enabled]：インターフェイスがイネーブルであるかどうか（[Yes] または [No]）を示します。デフォルトでは、すべてのインターフェイスはコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。
- [Security Level]：インターフェイスのセキュリティ レベルを 0 ～ 100 の範囲で示します。デフォルトのセキュリティ レベルは 0 です。
- [IP Address]：IP アドレスが表示されます。トランスペアレント モードの場合「native」が表示されます。トランスペアレント モードのインターフェイスは IP アドレスを使用しません。IP アドレスをコンテキストまたはセキュリティ アプライアンスに設定するには、[管理 IP アドレス] ペインを参照してください。
- [Subnet Mask]：ルーテッド モードの場合のみ。サブネット マスクを表示します。
- [Redundant]：インターフェイスが冗長インターフェイスであるかどうか（[Yes] または [No]）を示します。
- [Member]：このインターフェイスが冗長インターフェイスのメンバであるかどうか（[Yes] または [No]）を示します。

- [Management Only] : インターフェイスでセキュリティ アプライアンスへのトラフィックが許可されるか、または管理のためだけかを示します。
- [MTU] : MTU を表示します。デフォルトでは、MTU は 1500 です。
- [Active MAC Address] : アクティブな MAC アドレスを示します。[Add/Edit Interface] > [Advanced] タブで手動で割り当てると表示されます。
- [Standby MAC Address] : スタンバイ MAC アドレス（フェールオーバー用）を示します。手動で設定すると表示されます。
- [Description] : 説明を表示します。
- [Add] > [Interface] : サブインターフェイスを追加します。
- [Add] > [Redundant Interface] : 冗長インターフェイスを追加します。
- [Edit] : 選択したインターフェイスを編集します。
- [Delete] : 選択したサブインターフェイスまたは冗長インターフェイスを削除します。物理インターフェイスは削除できません。フェールオーバー リンクまたはステート リンクとしてインターフェイスを割り当てた場合（[[Failover]: [Setup]] タブを参照）は、そのインターフェイスをこのペインで削除することはできません。
- [Enable traffic between two or more interfaces which are configured with same security levels] : 同じセキュリティ レベルのインターフェイス間の通信をイネーブルにします。同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。
- [Enable traffic between two or more hosts connected to the same interface] : 同一インターフェイスを出入りするトラフィックをイネーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

[Edit Interface] > [General (Physical Interface)]

フィールド

- [Hardware Port] : *表示専用*。インターフェイス ID を表示します。
- [Configure Hardware Properties] : 物理インターフェイスでは、[Hardware Properties] ダイアログボックスが開き、メディア タイプ、速度、およびデュプレックスを設定できます。
- [Interface Name] : インターフェイス名を 48 文字以内で設定します。
- [Security Level] : セキュリティ レベルを 0（最低）～ 100（最高）の範囲で設定します。セキュリティ アプライアンスは、内部ネットワークから外部ネットワーク（低いセキュリティ レベル）にトラフィックを自由に流すことを許可します。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。

- [Dedicate this interface to management only]：インターフェイスを設定してセキュリティ アプライアンスへのトラフィックだけを許可します。通過トラフィックは許可しません。
- [Enable Interface]：インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。
- [IP Address]：ルーテッド モードの場合のみ。マルチ コンテキスト モードの場合は、コンテキスト設定で IP アドレスを設定します。
  - [Use Static IP]：IP アドレスを手動で設定します。

    [IP address]：IP アドレスを設定します。

    [Subnet Mask]：サブネット マスクを設定します。
  - [Obtain Address via DHCP]：DHCP から IP アドレスを動的に設定します。

    [For the client identifier in DHCP option 61]：オプション 61 用にデフォルトの内部生成文字列ではなく MAC アドレスを強制的に DHCP 要求パケット内に保存するには、[Use MAC address] をクリックします。一部の ISP では、オプション 61 がインターフェイスの MAC アドレスであると想定しています。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。デフォルトの文字列を使用するには、[Use "Cisco-<MAC>-<interface_name>-<host>"] をクリックします。

    [Obtain Default Route Using DHCP]：デフォルト ルートを DHCP サーバから取得します。デフォルトのスタティック ルートの設定が不要になります。

    [Retry Count]：4 ～ 16 の範囲で回数を設定します。セキュリティ アプライアンスは最初の試行後に DHCP 要求に応答がない場合、要求を再送信します。合計試行回数は、再試行回数に最初の試行を加えたものになります。たとえば、再試行回数を 4 に設定すると、セキュリティ アプライアンスは DHCP 要求を 5 回まで送信します。

    [DHCP Learned Route Metric]：アドミニストレーティブ ディスタンスを既知のルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

    [Enable tracking]：DHCP の既知のルートのルート トラッキングをイネーブルにするには、このチェックボックスをオンにします。

    （注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

    [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

    [Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。

    [SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。

    [Monitoring Options]：[Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。

    [Enable DHCP Broadcast flag for DHCP request and discover messages]：セキュリティ アプライアンスが DHCP クライアント パケットにブロードキャスト フラグを設定できるようにします。このオプションにより、DHCP クライアントが IP アドレスを要求する Discover を送信すると DHCP パケット ヘッダーのブロードキャスト フラグが 1 に設定されます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。このオプションを選択しないと、ブロードキャスト フラグは 0

に設定され、DHCP サーバは提供された IP アドレスを使用してクライアントに応答パケットをユニキャストします。DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

[Renew DHCP Lease] : DHCP リースを更新します。

– [Use PPPoE] : PPPoE を使用して IP アドレスを動的に設定します。

[Group Name] : グループ名を指定します。

[PPPoE Username] : ISP によって提供されたユーザ名を指定します。

[PPPoE Password] : ISP によって提供されたパスワードを指定します。

[Confirm Password] : ISP によって提供されたパスワードを指定します。

[PPP Authentication] : [PAP]、[CHAP]、または [MSCHAP] のいずれかを選択します。PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

[Store Username and Password in Local Flash] : ユーザ名とパスワードを、セキュリティ アプライアンス上の NVRAM の特定の場所に保存します。Auto Update Server が **clear configure** コマンドをセキュリティ アプライアンスに送信し、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再認証できます。

[IP Address and Route Settings] : [PPPoE IP Address and Route Settings] ダイアログが表示され、アドレッシングおよびトラッキングのオプションを選択できます。

- [Description] : オプションの説明を 240 文字以内で入力します。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

[Add/Edit Interface] > [General (Subinterface)]

フィールド

- [Hardware Port] : サブインターフェイスを追加する場合、イネーブル状態の任意の物理インターフェイスをサブインターフェイスの追加先として選択できます。インターフェイス ID が表示されない場合、インターフェイスがイネーブルになっているかどうかを確認してください。

- [VLAN ID]：サブインターフェイスでは、1 ～ 4095 の範囲の番号で VLAN ID を設定します。一部の VLAN ID は接続スイッチ用に予約されている場合があります。詳細 については、スイッチのマニュアルを確認してください。マルチ コンテキスト モードの場合、VLAN はシステム設定でしか設定できません。
- [Subinterface ID]：サブインターフェイス ID を 1 ～ 4294967293 の範囲の整数で設定します。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。
- [Interface Name]：インターフェイス名を 48 文字以内で設定します。
- [Security Level]：セキュリティ レベルを 0（最低）～ 100（最高）の範囲で設定します。セキュリティ アプライアンスは、内部ネットワークから外部ネットワーク（低いセキュリティ レベル）にトラフィックを自由に流すことを許可します。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。
- [Dedicate this interface to management only]：インターフェイスを設定してセキュリティ アプライアンスへのトラフィックだけを許可します。通過トラフィックは許可しません。
- [Enable Interface]：インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。
- [IP Address]：ルーテッド モードの場合のみ。マルチ コンテキスト モードの場合は、コンテキスト設定で IP アドレスを設定します。
  - [Use Static IP]：IP アドレスを手動で設定します。

    [IP address]：IP アドレスを設定します。

    [Subnet Mask]：サブネット マスクを設定します。
  - [Obtain Address via DHCP]：DHCP から IP アドレスを動的に設定します。

    [For the client identifier in DHCP option 61]：オプション 61 用にデフォルトの内部生成文字列ではなく MAC アドレスを強制的に DHCP 要求パケット内に保存するには、[Use MAC address] をクリックします。一部の ISP では、オプション 61 がインターフェイスの MAC アドレスであると想定しています。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。デフォルトの文字列を使用するには、[Use "Cisco-<MAC>-<interface_name>-<host>"] をクリックします。

    [Obtain Default Route Using DHCP]：デフォルト ルートを DHCP サーバから取得します。デフォルトのスタティック ルートの設定が不要になります。

    [Retry Count]：4 ～ 16 の範囲で回数を設定します。セキュリティ アプライアンスは最初の試行後に DHCP 要求に応答がない場合、要求を再送信します。合計試行回数は、再試行回数に最初の試行を加えたものになります。たとえば、再試行回数を 4 に設定すると、セキュリティ アプライアンスは DHCP 要求を 5 回まで送信します。

    [DHCP Learned Route Metric]：アドミニストレーティブ ディスタンスを既知のルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

    [Enable tracking]：DHCP の既知のルートのルート トラッキングをイネーブルにするには、このチェックボックスをオンにします。

    （注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

    [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

[Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワークオブジェクトがあれば表示されます。

[SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。

[Monitoring Options]：[Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。

[Enable DHCP Broadcast flag for DHCP request and discover messages]：セキュリティ アプライアンスが DHCP クライアント パケットにブロードキャスト フラグを設定できるようにします。このオプションにより、DHCP クライアントが IP アドレスを要求する Discover を送信すると DHCP パケット ヘッダーのブロードキャスト フラグが 1 に設定されます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。このオプションを選択しないと、ブロードキャスト フラグは 0 に設定され、DHCP サーバは提供された IP アドレスを使用してクライアントに応答パケットをユニキャストします。DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

[Renew DHCP Lease]：DHCP リースを更新します。

– [Use PPPoE]：PPPoE を使用して IP アドレスを動的に設定します。

[Group Name]：グループ名を指定します。

[PPPoE Username]：ISP によって提供されたユーザ名を指定します。

[PPPoE Password]：ISP によって提供されたパスワードを指定します。

[Confirm Password]：ISP によって提供されたパスワードを指定します。

[PPP Authentication]：[PAP]、[CHAP]、または [MSCHAP] のいずれかを選択します。PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

[Store Username and Password in Local Flash]：ユーザ名とパスワードを、セキュリティ アプライアンス上の NVRAM の特定の場所に保存します。Auto Update Server が **clear configure** コマンドをセキュリティ アプライアンスに送信し、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再認証できます。

[IP Address and Route Settings]：[PPPoE IP Address and Route Settings] ダイアログが表示され、アドレッシングおよびトラッキングのオプションを選択できます。

- [Description]：オプションの説明を 240 文字以内で入力します。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

[Add/Edit Interface] > [General (Redundant Interface)]

フィールド

- [Redundant ID] : 冗長インターフェイス ID を 1 ～ 8 の範囲で設定します。
- [Primary Interface] : プライマリ インターフェイスを設定します。このインターフェイスはデフォルトでアクティブになります。
- [Secondary Interface] : セカンダリ インターフェイスを設定します。
- [Interface Name] : インターフェイス名を 48 文字以内で設定します。
- [Security Level] : セキュリティ レベルを 0（最低）～ 100（最高）の範囲で設定します。セキュリティ アプライアンスは、内部ネットワークから外部ネットワーク（低いセキュリティ レベル）にトラフィックを自由に流すことを許可します。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。
- [Dedicate this interface to management only] : インターフェイスを設定してセキュリティ アプライアンスへのトラフィックだけを許可します。通過トラフィックは許可しません。
- [Enable Interface] : インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。

  デフォルトでは、冗長インターフェイスはイネーブルになっています。イネーブルになっている冗長インターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。
- [IP Address] : ルーテッド モードの場合のみ。マルチ コンテキスト モードの場合は、コンテキスト設定で IP アドレスを設定します。
  - [Use Static IP] : IP アドレスを手動で設定します。

    [IP address] : IP アドレスを設定します。

    [Subnet Mask] : サブネット マスクを設定します。
  - [Obtain Address via DHCP] : DHCP から IP アドレスを動的に設定します。

    [For the client identifier in DHCP option 61] : オプション 61 用にデフォルトの内部生成文字列ではなく MAC アドレスを強制的に DHCP 要求パケット内に保存するには、[Use MAC address] をクリックします。一部の ISP では、オプション 61 がインターフェイスの MAC アドレスであると想定しています。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。デフォルトの文字列を使用するには、[Use "Cisco-<MAC>-<interface_name>-<host>"] をクリックします。

    [Obtain Default Route Using DHCP] : デフォルト ルートを DHCP サーバから取得します。デフォルトのスタティック ルートの設定が不要になります。

[Retry Count]：4 ～ 16 の範囲で回数を設定します。セキュリティ アプライアンスは最初の試行後に DHCP 要求に応答がない場合、要求を再送信します。合計試行回数は、再試行回数に最初の試行を加えたものになります。たとえば、再試行回数を 4 に設定すると、セキュリティ アプライアンスは DHCP 要求を 5 回まで送信します。

[DHCP Learned Route Metric]：アドミニストレーティブ ディスタンスを既知のルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

[Enable tracking]：DHCP の既知のルートのルート トラッキングをイネーブルにするには、このチェックボックスをオンにします。

（注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

[Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

[Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。

[SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。

[Monitoring Options]：[Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。

[Enable DHCP Broadcast flag for DHCP request and discover messages]：セキュリティ アプライアンスが DHCP クライアント パケットにブロードキャスト フラグを設定できるようにします。このオプションにより、DHCP クライアントが IP アドレスを要求する Discover を送信すると DHCP パケット ヘッダーのブロードキャスト フラグが 1 に設定されます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。このオプションを選択しないと、ブロードキャスト フラグは 0 に設定され、DHCP サーバは提供された IP アドレスを使用してクライアントに応答パケットをユニキャストします。DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

[Renew DHCP Lease]：DHCP リースを更新します。

- [Use PPPoE]：PPPoE を使用して IP アドレスを動的に設定します。

[Group Name]：グループ名を指定します。

[PPPoE Username]：ISP によって提供されたユーザ名を指定します。

[PPPoE Password]：ISP によって提供されたパスワードを指定します。

[Confirm Password]：ISP によって提供されたパスワードを指定します。

[PPP Authentication]：[PAP]、[CHAP]、または [MSCHAP] のいずれかを選択します。PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

[Store Username and Password in Local Flash] : ユーザ名とパスワードを、セキュリティ アプライアンス上の NVRAM の特定の場所に保存します。Auto Update Server が **clear configure** コマンドをセキュリティ アプライアンスに送信し、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再認証できます。

[IP Address and Route Settings] : [PPPoE IP Address and Route Settings] ダイアログが表示され、アドレッシングおよびトラッキングのオプションを選択できます。

- [Description] : オプションの説明を 240 文字以内で入力します。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

[Add/Edit Interface] > [Advanced]

フィールド

- [MTU] : 300 ～ 65,535 バイトの範囲で MTU を設定します。デフォルトは 1500 バイトです。マルチ コンテキスト モードの場合は、コンテキスト設定で MTU を設定します。
- [Mac Address Cloning] : 手動で MAC アドレスを割り当てます。

  デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

  サブインターフェイスに一意の MAC アドレスを割り当てることが必要になる場合があります。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

  - [Active Mac Address] : MAC アドレスを H.H.H 形式でインターフェイスに割り当てます。H は 16 ビットの 16 進数です。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。
  - [Standby Mac Address] : フェールオーバーを使用する場合は、スタンバイ MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Hardware Properties

フィールド

- [Hardware Port]：*表示専用*。インターフェイス ID を表示します。
- [Media Type]：メディア タイプを RJ45 または SFP に設定します。デフォルトの設定は RJ45 です。
- [Duplex]：インターフェイスのデュプレックス オプションが一覧表示されます。インターフェイス タイプに応じて [Full]、[Half]、または [Auto] があります。
- [Speed]：インターフェイスの速度オプションが表示されます。使用できる速度は、インターフェイス タイプによって異なります。常に 1000 Mbps である SFP インターフェイスでは、速度を [Negotiate] または [Nonegotiate] に設定できます。[Negotiate]（デフォルト）ではリンク ネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。[Nonegotiate] では、リンク パラメータのネゴシエーションを行いません。ASA 5500 シリーズの適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

PPPoE IP Address and Route Settings

[PPPoE IP Address and Route Settings] ダイアログでは、PPPoE 接続のアドレッシングおよびトラッキング オプションを選択できます。

インターフェイスでの PPPoE の使用の詳細については、「インターフェイスの設定」（P.5-5）を参照してください。

フィールド

- [IP Address] エリア：IP アドレスを PPP から取得する方法または IP アドレスを指定する方法を選択します。次のフィールドがあります。
  - [Obtain IP Address using PPP]：セキュリティ アプライアンスを選択してイネーブルにし、PPP を使用して IP アドレスを取得します。
  - [Specify an IP Address]：セキュリティ アプライアンスは、PPPoE サーバとネゴシエートするのではなく、IP アドレスとマスクを指定してアドレスを動的に割り当てます。
- [Route Settings] エリア：ルートおよびトラッキングの設定を行います。次のフィールドがあります。
  - [Obtain default route using PPPoE]：PPPoE クライアントがまだ接続を確立していない場合に、デフォルト ルートを設定します。このオプションを使用する場合は、スタティックに定義されたルートを設定に含めることができません。

    [PPPoE learned route metric]：アドミニストレーティブ ディスタンスを既知のルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。
  - [Enable tracking]：PPPoE の既知のルートのルート トラッキングをイネーブルにするには、このチェックボックスをオンにします。

    （注）　ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。
  - [Primary Track]：プライマリ PPPoE ルート トラッキングを設定するには、このオプションを選択します。
  - [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。
  - [Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。
  - [SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。
  - [Monitor Options]：[Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。
  - [Secondary Track]：セカンダリ PPPoE ルート トラッキングを設定するには、このオプションを選択します。
  - [Secondary Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

CHAPTER 6

マルチ モードのインターフェイスの設定

この章では、物理イーサネット インターフェイスを設定してイネーブルにする方法、冗長インターフェイス ペアを作成する方法、およびシステム設定にサブインターフェイスを追加する方法について説明します。ファイバと銅線の両方のイーサネット ポートがある場合（ASA 5510 以降のシリーズの適応型セキュリティ アプライアンスに搭載されている 4GE SSM など）、この章ではインターフェイス メディア タイプの設定方法について説明します。

この章では、コンテキストに割り当てられている各インターフェイス（物理、冗長、またはサブインターフェイス）ごとに、名前、セキュリティ レベル、および IP アドレス（ルーテッド ファイアウォール モードのみ）の設定方法を説明します。

（注） シングル コンテキスト モードでインターフェイスを設定するには、第 5 章「インターフェイスの設定」を参照してください。

この章は、次の項で構成されています。

システム設定のインターフェイスの設定

マルチ コンテキスト モードでは、物理インターフェイス パラメータを設定し、システム実行スペースに冗長インターフェイスとサブインターフェイスを追加します。

この章は、次の項で構成されています。

（注） フェールオーバーを使用する場合、[[Failover]: [Setup]] タブで、専用のインターフェイスをフェールオーバー リンクとして割り当てる必要があります。また、オプションでステートフル フェールオーバー用のインターフェイスを割り当てます。（フェールオーバーとステート トラフィックには同じインターフェイスを使用できますが、分けることをお勧めします）。物理インターフェイス、サブインター

フェイス、または冗長インターフェイスは、コンテキストに割り当てられていなければ、フェールオーバーとステート リンクに使用できます。サブインターフェイスを使用するには、物理インターフェイスをコンテキストに割り当てないでください。

物理インターフェイスの設定

この項では、物理インターフェイス設定値を設定する方法について説明します。次の項目を取り上げます。

- 「物理インターフェイスの概要」（P.6-2）
- 「物理インターフェイスの設定およびイネーブル化」（P.6-3）

物理インターフェイスの概要

この項では、物理インターフェイスについて説明します。次の項目を取り上げます。

- 「物理インターフェイスのデフォルトの状態」（P.6-2）
- 「コネクタ タイプ」（P.6-2）
- 「Auto-MDI/MDIX 機能」（P.6-2）

物理インターフェイスのデフォルトの状態

物理インターフェイスは、デフォルトではすべてシャットダウンされます。トラフィックが物理インターフェイス（単独か冗長インターフェイス ペアの一部）またはサブインターフェイスを通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチ コンテキスト モードの場合、インターフェイス（物理、冗長、またはサブインターフェイス）をコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、まずこの手順に従って物理インターフェイスをシステム コンフィギュレーションでイネーブルにする必要があります。

デフォルトでは、銅線（RJ-45）インターフェイスの速度と二重通信は、オートネゴシエーションに設定されます。

コネクタ タイプ

ASA 5550 適応型セキュリティ アプライアンスと、ASA 5510 以降の適応型セキュリティ アプライアンスの 4GE SSM には、銅線 RJ-45 とファイバ SFP の 2 つのコネクタ タイプがあります。RJ-45 がデフォルトです。

ファイバ SFP コネクタを使用するには、メディア タイプを SFP に設定する必要があります。ファイバ インターフェイスでは、速度は固定であり、二重通信はサポートされていませんが、インターフェイスをリンク パラメータ ネゴシエーションあり（デフォルト）またはネゴシエーションなしに設定することができます。

Auto-MDI/MDIX 機能

ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネー

ブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

物理インターフェイスの設定およびイネーブル化

物理インターフェイスを設定してイネーブルにするには、次の手順を実行します。

ステップ 1　[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Interfaces] ペインで、設定する物理インターフェイスをクリックし、[Edit] をクリックします。

ステップ 3　インターフェイスをイネーブルにするには、[Enable Interface] チェックボックスをオンにします。

ステップ 4　説明を追加するには、[Description] フィールドにテキストを入力します。

ステップ 5　（任意）メディア タイプ、デュプレックス、および速度を設定するには、[Configure Hardware Properties] ボタンをクリックします。

a. ASA 5550 適応型セキュリティ アプライアンスまたは 4GE SSM を使用している場合は、[Media Type] ドロップダウン リストから [RJ-45] または [SFP] を選択できます。

RJ-45 がデフォルトです。

b. RJ-45 インターフェイスに二重通信を設定するには、[Duplex] ドロップダウン リストからインターフェイス タイプに応じて [Full]、[Half]、または [Auto] を選択します。

c. 速度を設定するには、[Speed] ドロップダウン リストから値を選択します。

使用できる速度は、インターフェイス タイプによって異なります。常に 1000 Mbps である SFP インターフェイスでは、速度を [Negotiate] または [Nonegotiate] に設定できます。[Negotiate]（デフォルト）ではリンク ネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。[Nonegotiate] では、リンク パラメータのネゴシエーションを行いません。ASA 5500 シリーズの適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。
Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

d. [OK] をクリックして [Hardware Properties] の変更を受け入れます。

ステップ 6　[OK] をクリックして [Interface] の変更を受け入れます。

冗長インターフェイスの設定

論理冗長インターフェイスは、アクティブとスタンバイの物理インターフェイスからなるペアです。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定してセキュリティ アプライアンスの信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。最大 8 個の冗長インターフェイス ペアを設定できます。

その後のすべてのセキュリティ アプライアンス コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。

この項では、冗長インターフェイスを設定する方法について説明します。次の項目を取り上げます。

- 「冗長インターフェイスの概要」（P.6-4）
- 「冗長インターフェイスの追加」（P.6-5）

冗長インターフェイスの概要

この項では、冗長インターフェイスの概要を説明します。次の項目を取り上げます。

- 「冗長インターフェイスのデフォルトの状態」（P.6-4）
- 「冗長インターフェイスとフェールオーバーのガイドライン」（P.6-4）
- 「冗長インターフェイスの MAC アドレス」（P.6-4）
- 「冗長インターフェイスで使用する場合の物理インターフェイスのガイドライン」（P.6-5）

冗長インターフェイスのデフォルトの状態

追加された冗長インターフェイスは、デフォルトでイネーブルになっています。ただし、トラフィックを通過させるには、メンバー インターフェイスもイネーブルにする必要があります。

冗長インターフェイスとフェールオーバーのガイドライン

メンバー インターフェイスを追加する場合は次のガイドラインに従います。

- フェールオーバーまたはステート リンク用に冗長インターフェイスを使用する場合は、プライマリ ユニットに加えてセカンダリ ユニット上の基本的なコンフィギュレーションの一部として冗長インターフェイスを設定する必要があります。
- フェールオーバーまたはステート リンク用に冗長インターフェイスを使用する場合は、2 つのユニット間にスイッチまたはハブを配置する必要があります。両ユニットは直接接続できません。スイッチやハブがなくても、プライマリ ユニット上のアクティブ ポートをセカンダリ ユニット上のスタンバイ ポートに直接接続できる場合もあります。
- フェールオーバーが発生しているかどうか冗長インターフェイスをモニタできます。必ず論理冗長インターフェイス名を参照してください。
- アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合、デバイスレベルのフェールオーバーをモニタしているときには、冗長インターフェイスで障害が発生しているように見えません。冗長インターフェイスで障害が発生しているように見えるのは、両方の物理インターフェイスで障害が発生したときだけです。

冗長インターフェイスの MAC アドレス

冗長インターフェイスは、最初に追加された物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに MAC アドレスを割り当てることができます。これはメンバ インターフェイスの MAC アドレスに関係なく使用されます（「インターフェイス パラメータの設定」（P.6-12）または 「セキュリティ コンテキストの設定」（P.9-20）を参照）。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

冗長インターフェイスで使用する場合の物理インターフェイスのガイドライン

メンバー インターフェイスを追加する場合は次のガイドラインに従います。

- 両方のメンバ インターフェイスが同じ物理タイプである必要があります。たとえば、両方ともイーサネットにする必要があります。
- 物理インターフェイスを冗長インターフェイスに追加すると、名前、IP アドレス、およびセキュリティ レベルは削除されます。

注意　コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

- アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。

冗長インターフェイスの追加

最大 8 個の冗長インターフェイス ペアを設定できます。冗長インターフェイスを設定するには、次の手順を実行します。

ステップ 1　まだシステム コンフィギュレーション モードに入っていない場合、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Interfaces] ペインで、[Add] > [Redundant Interface] をクリックします。

ステップ 3　[Redundant ID] フィールドで、1 ～ 8 の整数を入力します。

ステップ 4　[Primary Interface] ドロップダウン リストから、プライマリにする物理インターフェイスを選択します。

サブインターフェイスを持たず、まだコンテキストに割り当てられていないインターフェイスを必ず選択してください。

ステップ 5　[Secondary Interface] ドロップダウン リストから、セカンダリにする物理インターフェイスを選択します。

ステップ 6　インターフェイスがまだイネーブルでない場合は、[Enable interface] をオンにします。

インターフェイスはデフォルトでイネーブルになっています。ディセーブルにするには、このボックスをオフにします。

ステップ 7　説明を追加するには、[Description] フィールドにテキストを入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。フェールオーバーまたはステートリンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 8　[OK] をクリックします。

VLAN サブインターフェイスと 802.1Q トランキングの設定

この項では、サブインターフェイスを設定する方法について説明します。次の項目を取り上げます。

サブインターフェイスの概要

サブインターフェイスを使用すると、1 つの物理インターフェイスまたは冗長インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはセキュリティ アプライアンスを追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。この機能は、各コンテキストに固有のインターフェイスを割り当てることができるので、マルチ コンテキスト モードで特に便利です。

この項では、次のトピックについて取り上げます。

サブインターフェイスのデフォルトの状態

追加されたサブインターフェイスは、デフォルトでイネーブルになっています。ただし、トラフィックを通過させるためには物理インターフェイスまたは冗長インターフェイスもイネーブルにする必要があります（物理インターフェイスのイネーブル化については、「物理インターフェイスの設定」（P.6-2）を参照してください。冗長インターフェイスのイネーブル化については、「冗長インターフェイスの設定」（P.6-3）を参照してください）。

最大サブインターフェイス数

プラットフォームに許容されるサブインターフェイスの数を決定するには、付録 A「機能のライセンスと仕様」を参照してください。

サブインターフェイスの追加

サブインターフェイスを追加して、そのサブインターフェイスに VLAN を割り当てるには、次の手順を実行します。

ステップ 1　まだシステム コンフィギュレーション モードに入っていない場合、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Interfaces] ペインで、[Add] > [Interface] をクリックします。

ステップ 3　[Hardware Port] ドロップダウン リストから、サブインターフェイスを追加する物理インターフェイスを選択します。

ステップ 4　インターフェイスがまだイネーブルでない場合は、[Enable interface] をオンにします。

インターフェイスはデフォルトでイネーブルになっています。ディセーブルにするには、このボックスをオフにします。

ステップ 5　[VLAN ID] フィールドに、1 ～ 4095 の VLAN ID を入力します。

一部の VLAN ID は接続スイッチ用に予約されている場合があります。詳細 については、スイッチのマニュアルを確認してください。マルチ コンテキスト モードの場合、VLAN はシステム設定でしか設定できません。

ステップ 6　[Subinterface ID] フィールドに、サブインターフェイス ID を 1 ～ 4294967293 の整数で入力します。

許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。

ステップ 7　（任意）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 8　[OK] をクリックします。

Interface (System) のフィールドの説明

この項では、次のトピックについて取り上げます。

Interfaces (System)

フィールド

- [Interface]：インターフェイス ID を表示します。すべての物理インターフェイスが自動的に表示されます。サブインターフェイスは、インターフェイス ID とそれに続く *.n* で示されます。*n* はサブインターフェイス番号です。
- [Enabled]：インターフェイスがイネーブルであるかどうか（[Yes] または [No]）を示します。

  物理インターフェイスは、デフォルトではすべてシャットダウンされます。イネーブルになっているサブインターフェイスまたは冗長インターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチ コンテキスト モードの場合、インターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。
- [Redundant]：インターフェイスが冗長インターフェイスであるかどうか（[Yes] または [No]）を示します。
- [Member]：このインターフェイスが冗長インターフェイスのメンバであるかどうか（[Yes] または [No]）を示します。

- [VLAN]：サブインターフェイスに割り当てられた VLAN を示します。物理インターフェイスおよび冗長インターフェイスには「native」が表示されます。これは、タグがないインターフェイスという意味です。
- [Description]：説明を表示します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。
- [Add] > [Interface]：サブインターフェイスを追加します。詳細については、「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.6-6）を参照してください。
- [Add] > [Redundant Interface]：冗長インターフェイスを追加します。詳細については、「冗長インターフェイスの設定」（P.6-3）を参照してください。
- [Edit]：選択したインターフェイスを編集します。
- [Delete]：選択したサブインターフェイスまたは冗長インターフェイスを削除します。物理インターフェイスまたはコンテキストで割り当てたインターフェイスは削除できません。フェールオーバー リンクまたはステート リンクとしてインターフェイスを割り当てた場合（[[Failover]: [Setup]] タブを参照）は、そのインターフェイスをこのペインで削除することはできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

Add/Edit Interface (System)

フィールド

- [Hardware Port]：サブインターフェイスを追加する場合、イネーブル状態の任意の物理インターフェイスをサブインターフェイスの追加先として選択できます。インターフェイス ID が表示されない場合、インターフェイスがイネーブルになっているかどうかを確認してください。
- [Configure Hardware Properties]：物理インターフェイスでは、[Hardware Properties (System)] ダイアログボックスが開き、メディア タイプ、速度、およびデュプレックスを設定できます。
- [Enable Interface]：インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。

  物理インターフェイスは、デフォルトではすべてシャットダウンされます。イネーブルになっているサブインターフェイスまたは冗長インターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチ コンテキスト モードの場合、インターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

- [VLAN ID]：サブインターフェイスでは、1 ～ 4095 の範囲の番号で VLAN ID を設定します。一部の VLAN ID は接続スイッチ用に予約されている場合があります。詳細 については、スイッチのマニュアルを確認してください。マルチ コンテキスト モードの場合、VLAN はシステム設定でしか設定できません。
- [Subinterface ID]：サブインターフェイス ID を 1 ～ 4294967293 の範囲の整数で設定します。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。
- [Description]：オプションの説明を 240 文字以内で入力します。改行を入れずに 1 行で入力します。システムの説明はコンテキストの説明に依存しません。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

Add/Edit Redundant Interface (System)

フィールド

- [Redundant ID]：冗長インターフェイス ID を 1 ～ 8 の範囲で設定します。
- [Primary Interface]：プライマリ インターフェイスを設定します。このインターフェイスはデフォルトでアクティブになります。
- [Secondary Interface]：セカンダリ インターフェイスを設定します。
- [Enable Interface]：インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。

  デフォルトでは、冗長インターフェイスはイネーブルになっています。イネーブルになっている冗長インターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチ コンテキスト モードの場合、インターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。
- [Description]：オプションの説明を 240 文字以内で入力します。改行を入れずに 1 行で入力します。システムの説明はコンテキストの説明に依存しません。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE

Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

Hardware Properties (System)

フィールド

- [Hardware Port]：*表示専用*。インターフェイス ID を表示します。
- [Media Type]：メディア タイプを RJ45 または SFP に設定します。デフォルトの設定は RJ45 です。
- [Duplex]：インターフェイスのデュプレックス オプションが一覧表示されます。インターフェイス タイプに応じて [Full]、[Half]、または [Auto] があります。
- [Speed]：インターフェイスの速度オプションが表示されます。使用できる速度は、インターフェイス タイプによって異なります。常に 1000 Mbps である SFP インターフェイスでは、速度を [Negotiate] または [Nonegotiate] に設定できます。[Negotiate]（デフォルト）ではリンク ネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。[Nonegotiate] では、リンク パラメータのネゴシエーションを行いません。ASA 5500 シリーズの適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

コンテキストへのインターフェイスの割り当て

インターフェイスをコンテキストに割り当てるには、「セキュリティ コンテキストの設定」（P.9-20）を参照してください。

各コンテキスト内でのインターフェイス パラメータの設定

各コンテキスト内で、各インターフェイスの名前、セキュリティ レベル、および IP アドレスを設定します。同じセキュリティ レベルの通信をイネーブルにすることもできます。この項では、次のトピックについて取り上げます。

インターフェイス パラメータの概要

この項では、インターフェイス パラメータについて説明します。次の項目を取り上げます。

インターフェイスのデフォルトの状態

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングル モードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに名前「inside」を付けて、明示的にセキュリティ レベルを設定しないと、セキュリティ アプライアンスはセキュリティ レベルを 100 に設定します。

（注）　インターフェイスのセキュリティ レベルを変更したときに、既存の接続がタイムアウトするまで待機せずに新しいセキュリティ情報を使用する必要がある場合は、**clear local-host** コマンドを使用して接続をクリアできます。

各インターフェイスには、0（最下位）～ 100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。DMZ など、その他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。詳細については、「同じセキュリティ レベルの通信のイネーブル化」（P.6-14）を参照してください。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイス間では、同じセキュリティ レベル以下の他のインターフェイスへのアクセスが暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけがセキュリティ アプライアンスを通過することが許可されます。

- フィルタリング：HTTP(S) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信のいずれのトラフィックもフィルタリングできます。

- NAT コントロール：NAT コントロールをイネーブルにする場合、高いセキュリティ レベルのインターフェイス（内部）上のホストから低いセキュリティ レベルのインターフェイス（外部）上のホストにアクセスするときは、内部インターフェイスのホストに NAT を設定する必要があります。

  NAT コントロールをイネーブルにしない場合、または同じセキュリティ レベルのインターフェイス間においては、任意のインターフェイス間で NAT を使用することも、使用しないこともできます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要になることがあります。

- **established** コマンド：このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り接続が許可されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信の両方の接続に対して **established** コマンドを設定できます。

インターフェイス パラメータの設定

インターフェイスを追加または編集するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device List] ペインで、アクティブなデバイスの [IP address] > [Contexts] の下にあるコンテキスト名をダブルクリックします。

ステップ 2　[Device Setup] > [Interfaces] ペインで、設定するインターフェイスをクリックし、[Edit] をクリックします。

[Add/Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 4　[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

詳細については、「デフォルトのセキュリティ レベル」（P.6-11）を参照してください。

ステップ 5　（任意）このインターフェイスを管理専用インターフェイスとして設定するには、[Dedicate this interface to management-only] をオンにします。

管理専用インターフェイスでは、通過トラフィックは受け入れられません。

ステップ 6　インターフェイスがまだイネーブルでない場合は、[Enable interface] をオンにします。

インターフェイスはデフォルトでイネーブルになっています。ディセーブルにするには、このボックスをオフにします。

ステップ 7　IP アドレスを設定するには、次のいずれかのオプションを使用します。

ルーテッド ファイアウォール モードでは、すべてのインターフェイスに対する IP アドレスを設定します。トランスペアレント ファイアウォール モードでは、インターフェイスごとに IP アドレスを設定するのではなく、全体 セキュリティ アプライアンス またはコンテキスト全体に IP アドレスを設定します。トラフィックを通過させない Management 0/0 管理専用インターフェイスの場合は例外となります。トランスペアレント ファイアウォール モードのセキュリティ アプライアンス全体またはコンテキスト全体の管理 IP アドレスを設定するには、[管理 IP アドレス] ペインを参照してください。Management 0/0 インターフェイスまたはサブインターフェイスの IP アドレスを設定するには、この手順を使用します。

フェールオーバーとともに使用する場合は、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP はサポートされません。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブで、スタンバイ IP アドレスを設定します。

- IP アドレスを手動で設定するには、[Use Static IP] をクリックして IP アドレスとマスクを入力します。
- DHCP サーバから IP アドレスを取得するには、[Obtain Address via DHCP] をクリックします。
  - **a.**（任意）DHCP サーバからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。
  - **b.**（任意）リースを更新するには、[Renew DHCP Lease] をクリックします。

ステップ 8　（任意）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。システムの説明はコンテキストの説明に依存しません。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 9　（任意）MTU を設定するには、[Advanced] タブをクリックして、[MTU] フィールドに 300 ～ 65,535 バイトの値を入力します。

デフォルトは 1500 バイトです。

ステップ 10　（任意）MAC アドレスをこのインターフェイスに手動で割り当てるには、[Advanced] タブで、[Active Mac Address] フィールドに MAC アドレスを H.H.H 形式（H は 16 ビットの 16 進数）で入力します。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。

フェールオーバーを使用する場合、[Standby Mac Address] フィールドにスタンバイ MAC アドレスを入力します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。冗長インターフェイスは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。このフィールドを使用して冗長インターフェイスに MAC アドレスを割り当てると、メンバ インターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。

コンテキスト間でインターフェイスを共有している場合、固有の MAC アドレスをそれぞれのコンテキストのインターフェイスに割り当てることができます。この機能を使用すると、セキュリティ アプライアンスはパケットを適切なコンテキストに容易に分類できます。固有の MAC アドレスがなくても共有インターフェイスを使用できますが、制限があります。詳細については、「セキュリティ アプライアンスによるパケットの分類方法」（P.9-3）を参照してください。コンテキストの共有インターフェイスには、手動で各 MAC アドレスを割り当てることも、自動生成することもできます。MAC アドレスの自動生成については、「セキュリティ コンテキスト」（P.9-23）を参照してください。MAC アドレスを自動生成する場合、このオプションを使用して、生成されたアドレスを上書きできます。

共有しないインターフェイスについては、サブインターフェイスに固有の MAC アドレスを割り当てることができます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

ステップ 11　[OK] をクリックします。

同じセキュリティ レベルの通信のイネーブル化

デフォルトでは、セキュリティ レベルが同じインターフェイス同士は通信できません。同一セキュリティ レベルのインターフェイス間での通信を許可すると、101 を超える通信インターフェイスを設定できます。インターフェイスごとに異なるレベルを使用し、同じセキュリティ レベルにインターフェイスを割り当てないようにすると、1 レベルにつき 1 つのインターフェイスしか設定できません（0 ～ 100）。

（注）　NAT 制御をイネーブルにする場合、同一セキュリティ レベルのインターフェイス間では NAT を設定する必要がありません。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

同じインターフェイスに接続されているホスト間の通信をイネーブルにすることもできます。

- 同じセキュリティ レベルのインターフェイス間の通信をイネーブルにするには、[Configuration] > [Interfaces] ペインで、[Enable traffic between two or more interfaces which are configured with same security level] をオンにします。
- 同じインターフェイスに接続されているホスト間の通信をイネーブルにするには、[Enable traffic between two or more hosts connected to the same interface] をオンにします。

[Interface (Context)] フィールドの説明

この項では、次のトピックについて取り上げます。

Interfaces (Context)

フィールド

- [Interface]：インターフェイス ID を表示します。割り当てられているすべてのインターフェイスが自動的に表示されます。サブインターフェイスは、インターフェイス ID とそれに続く *.n* で示されます。*n* はサブインターフェイス番号です。冗長インターフェイスは、Redundant *n* と呼ばれます。
- [Name]：インターフェイス名を表示します。
- [Enabled]：インターフェイスがイネーブルであるかどうか（[Yes] または [No]）を示します。デフォルトでは、すべてのインターフェイスはコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。
- [Security Level]：インターフェイスのセキュリティ レベルを 0 ～ 100 の範囲で示します。デフォルトのセキュリティ レベルは 0 です。
- [IP Address]：IP アドレスが表示されます。トランスペアレント モードの場合「native」が表示されます。トランスペアレント モードのインターフェイスは IP アドレスを使用しません。IP アドレスをコンテキストまたはセキュリティ アプライアンスに設定するには、[管理 IP アドレス] ペインを参照してください。
- [Subnet Mask]：ルーテッド モードの場合のみ。サブネット マスクを表示します。
- [Management Only]：インターフェイスでセキュリティ アプライアンスへのトラフィックが許可されるか、または管理のためだけかを示します。
- [MTU]：MTU を表示します。デフォルトでは、MTU は 1500 です。
- [Active MAC Address]：アクティブな MAC アドレスを示します。[Edit Interface] > [Advanced (Context)] タブで手動で割り当てると表示されます。
- [Standby MAC Address]：スタンバイ MAC アドレス（フェールオーバー用）を示します。手動で設定すると表示されます。
- [Description]：説明を表示します。
- [Add]：*適用されません。*サブインターフェイスと冗長インターフェイスは、システム実行スペースでのみ追加できます。
- [Edit]：選択したインターフェイスを編集します。
- [Delete]：*適用されません。*サブインターフェイスと冗長インターフェイスは、システム実行スペースでのみ削除できます。

- [Enable traffic between two or more interfaces which are configured with same security levels] : 同じセキュリティ レベルのインターフェイス間の通信をイネーブルにします。同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。
- [Enable traffic between two or more hosts connected to the same interface] : 同一インターフェイスを出入りするトラフィックをイネーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	•	—

[Edit Interface] > [General (Context)]

フィールド

- [Hardware Port] : *表示専用*。インターフェイス ID を表示します。
- [Enable Interface] : インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。この設定に加えて、トラフィックがセキュリティ ポリシーに従って通過できるように、IP アドレス（ルーテッド モード）と名前を事前に設定する必要があります。デフォルトでは、インターフェイスはコンテキスト内でイネーブルになっています。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。
- [Interface Name] : インターフェイス名を 48 文字以内で設定します。
- [Dedicate this interface to management only] : インターフェイスを設定してセキュリティ アプライアンスへのトラフィックだけを許可します。通過トラフィックは許可しません。
- [Security Level] : セキュリティ レベルを 0（最低）～ 100（最高）の範囲で設定します。セキュリティ アプライアンスは、内部ネットワークから外部ネットワーク（低いセキュリティ レベル）にトラフィックを自由に流すことを許可します。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。
- [IP Address] : ルーテッド モードの場合のみ。マルチ コンテキスト モードの場合は、コンテキスト設定で IP アドレスを設定します。
  - [Use Static IP] : IP アドレスを手動で設定します。

    [IP address] : IP アドレスを設定します。

    [Subnet Mask] : サブネット マスクを設定します。
  - [Obtain Address via DHCP] : DHCP から IP アドレスを動的に設定します。

    [Obtain Default Route Using DHCP] : デフォルト ルートを DHCP サーバから取得します。デフォルトのスタティック ルートの設定が不要になります。

    [Renew DHCP Lease] : DHCP リースを更新します。

- [Description]：オプションの説明を 240 文字以内で入力します。改行を入れずに 1 行で入力します。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	•	—

[Edit Interface] > [Advanced (Context)]

フィールド

- [MTU]：300 ～ 65,535 バイトの範囲で MTU を設定します。デフォルトは 1500 バイトです。マルチ コンテキスト モードの場合は、コンテキスト設定で MTU を設定します。
- [Mac Address Cloning]：手動で MAC アドレスを割り当てます。

  デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

  マルチ コンテキスト モードでは、コンテキスト間でインターフェイスを共有している場合、固有の MAC アドレスをそれぞれのコンテキストのインターフェイスに割り当てることができます。この機能を使用すると、セキュリティ アプライアンスはパケットを適切なコンテキストに容易に分類できます。固有の MAC アドレスがなくても共有インターフェイスを使用できますが、制限があります。詳細については、「セキュリティ アプライアンスによるパケットの分類方法」（P.9-3）を参照してください。コンテキストの共有インターフェイスには、手動で各 MAC アドレスを割り当てることも、自動生成することもできます。MAC アドレスの自動生成については、「セキュリティ コンテキスト」（P.9-23）を参照してください。MAC アドレスを自動生成する場合、このオプションを使用して、生成されたアドレスを上書きできます。

  シングル コンテキスト モード、またはマルチ コンテキスト モードで共有されないインターフェイスの場合は、固有の MAC アドレスをサブインターフェイスに割り当てることを推奨します。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

  - [Active Mac Address]：MAC アドレスを H.H.H 形式でインターフェイスに割り当てます。H は 16 ビットの 16 進数です。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。
  - [Standby Mac Address]：フェールオーバーを使用する場合は、スタンバイ MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	•	—

CHAPTER 7

Cisco ASA 5505 適応型セキュリティ アプライアンス用スイッチ ポートおよび VLAN インターフェイスの設定

この章では、ASA 5505 適応型セキュリティ アプライアンスのスイッチ ポートと VLAN インターフェイスを設定する方法について説明します。

（注） 他のモデルのインターフェイスを設定するには、第 5 章「インターフェイスの設定」を参照してください。

この章は、次の項で構成されています。

インターフェイスの概要

この項では、ASA 5505 適応型セキュリティ アプライアンスのポートおよびインターフェイスについて説明します。次の項目を取り上げます。

ASA 5505 のポートおよびインターフェイスについて

ASA 5505 適応型セキュリティ アプライアンスでは、組み込みスイッチがサポートされています。次の 2 種類のポートおよびインターフェイスを設定する必要があります。

- 物理スイッチ ポート：適応型セキュリティ アプライアンスには、ハードウェアのスイッチング機能を使用して、レイヤ 2 でトラフィックを転送する 8 つのファスト イーサネット スイッチ ポートがあります。これらのポートのうちの 2 つは PoE ポートです。詳細については、「同じセキュリティ レベルのインターフェイス間では、発信と着信の両方の接続に対して established コマンドを設定できます。」（P.7-5）を参照してください。これらのインターフェイスを、PC、IP 電話、DSL モデムなどのユーザ機器に直接接続できます。または、別のスイッチに接続できます。
- 論理 VLAN インターフェイス：ルーテッド モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ 3 の VLAN ネットワーク間でトラフィックを転送します。トランスペアレント モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォール サービスを適用することによって、レイヤ 2 の同じネットワーク上の VLAN 間でトラフィックを転送します。最大 VLAN インターフェイス数の詳細については、「ライセンスで使用できる最大アクティブ VLAN インターフェイス数」を参照してください。VLAN インターフェイスを使用することにより、別々の VLAN、たとえばホーム VLAN、ビジネス VLAN、インターネット VLAN などに装置を分けることができます。

スイッチ ポートを別々の VLAN に分離するには、各スイッチ ポートを VLAN インターフェイスに割り当てます。同じ VLAN 上のスイッチ ポートは、ハードウェア スイッチングを使用して相互に通信できます。ただし、VLAN 1 上のスイッチ ポートが VLAN 2 上のスイッチ ポートと通信する場合、適応型セキュリティ アプライアンスはセキュリティ ポリシーをトラフィックに適用し、2 つの VLAN 間でルーティングまたはブリッジングします。

（注）　サブインターフェイスは、ASA 5505 適応型セキュリティ アプライアンスでは使用できません。

ライセンスで使用できる最大アクティブ VLAN インターフェイス数

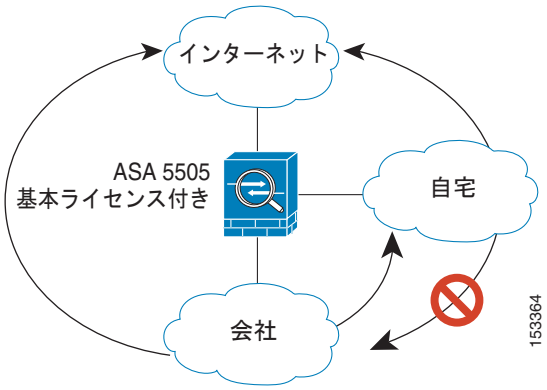
トランスペアレント ファイアウォール モードでは、基本ライセンスはアクティブ VLAN を 2 つ、Security Plus ライセンスは 3 つ設定できます。そのうちの 1 つは、フェールオーバー用です。

ルーテッド モードでは、基本ライセンスはアクティブ VLAN を 3 つまで、Security Plus ライセンスは 20 まで設定できます。

アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。

基本ライセンスの場合、3 つめの VLAN は他の 1 つの VLAN にのみトラフィックを開始するように設定できます。図 7-1 のネットワークの例では、ホーム VLAN はインターネットと通信できますが、ビジネス VLAN とは接続を開始できません。

図 7-1　基本ライセンスでの ASA 5505 適応型セキュリティ アプライアンス

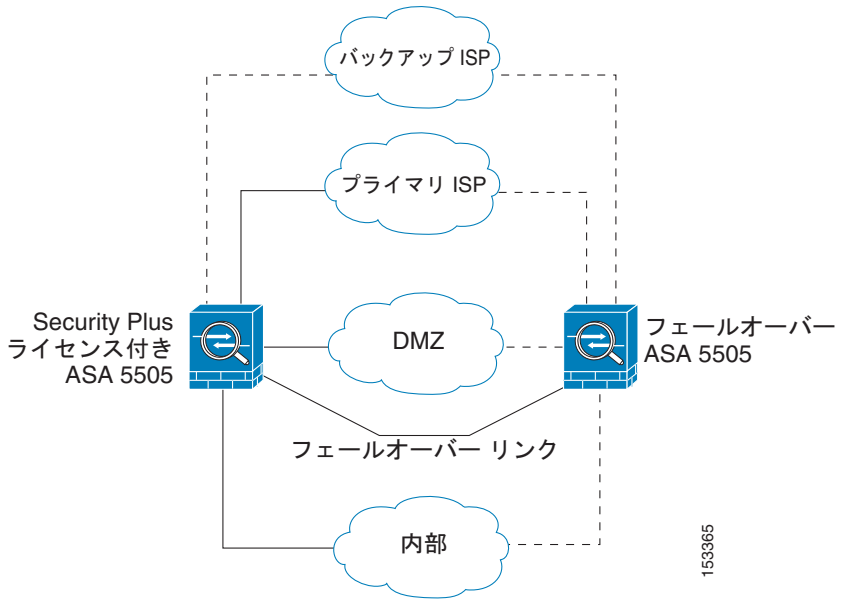


Security Plus ライセンスでは、20 の VLAN インターフェイスを設定できます。トランク ポートを設定して、1 つのポートで複数の VLAN を使用できます。

（注） ASA 5505 適応型セキュリティ アプライアンスは、Active/Standby フェールオーバーをサポートしますが、ステートフル フェールオーバーをサポートしていません。

ネットワークの例については、図 7-2 を参照してください。

図 7-2　Security Plus ライセンスでの ASA 5505 適応型セキュリティ アプライアンス



デフォルト インターフェイス コンフィギュレーション

ご使用の適応型セキュリティ アプライアンスに工場出荷時のデフォルト コンフィギュレーションが含まれている場合、インターフェイスは次のように設定されています。

- 外部インターフェイス（セキュリティ レベル 0）は VLAN 2 です。

  イーサネット 0/0 が VLAN 2 に割り当てられ、イネーブルになります。

  VLAN 2 の IP アドレスは DHCP サーバから取得します。
- 内部インターフェイス（セキュリティ レベル 100）は VLAN 1 です。

  イーサネット 0/1 ～イーサネット 0/7 が VLAN 1 に割り当てられ、イネーブルになります。

  VLAN 1 の IP アドレスは 192.168.1.1 です。

configure factory-default コマンドを使用して、工場出荷時のデフォルト コンフィギュレーションを復元します。

この章の手順に従い、デフォルト コンフィギュレーションを変更します。たとえば、VLAN インターフェイスの追加を行います。

工場出荷時のデフォルト コンフィギュレーションになっていない場合は、すべてのスイッチ ポートが VLAN 1 ですが、その他のパラメータは未設定です。

VLAN MAC アドレス

ルーテッド ファイアウォール モードでは、すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。

トランスペアレント ファイアウォール モードでは、各 VLAN に固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。

Power Over Ethernet

Ethernet 0/6 および Ethernet 0/7 は、IP 電話や無線アクセス ポイントなどのデバイス用に PoE をサポートしています。非 PoE デバイスをインストールした場合やこれらのスイッチ ポートに接続しない場合、適応型セキュリティ アプライアンスはスイッチ ポートに電源を供給しません。

[Edit Switch Port] ダイアログボックスでスイッチ ポートをシャットダウンすると、デバイスへの電源がディセーブルになります。再度イネーブルにするよう入力すれば、電源が復元します。

接続されているデバイスのタイプ（Cisco または IEEE 802.3af）など、PoE スイッチ ポートのステータスを確認するには、**show power inline** コマンドを使用します。

SPAN を使用したトラフィックのモニタリング

1 つまたは複数のスイッチ ポートを出入りするトラフィックをモニタするには、スイッチ ポート モニタリングとも呼ばれる SPAN をイネーブルにします。SPAN をイネーブルにしたポート（宛先ポートと呼ばれる）は、特定の送信元ポートで送受信するすべてのパケットのコピーを受信します。SPAN 機能を使用すれば、スニファを宛先ポートに添付して、すべてのトラフィックをモニタできます。SPAN を使用しないと、モニタするポートごとにスニファを添付しなければなりません。SPAN をイネーブルにすることができるのは、1 つの宛先ポートのみです。

SPAN 監視をイネーブルにするには、Command Line Interface ツールを使用し、**switchport monitor** コマンドを入力する必要があります。詳細については、『*Cisco Security Appliance Command Reference*』の **switchport monitor** コマンドを参照してください。

セキュリティ レベルの概要

各 VLAN インターフェイスには、0 ～ 100（最下位～最上位）までのセキュリティ レベルを割り当てる必要があります。たとえば、内部ビジネス ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。ホーム ネットワークなどその他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイス間では、同じセキュリティ レベル以下の他のインターフェイスへのアクセスが暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけが適応型セキュリティ アプライアンスを通過することを許可されます。

- フィルタリング：HTTP(S) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信のいずれのトラフィックもフィルタリングできます。

- NAT コントロール：NAT コントロールをイネーブルにする場合、高いセキュリティ レベルのインターフェイス（内部）上のホストから低いセキュリティ レベルのインターフェイス（外部）上のホストにアクセスするときは、内部インターフェイスのホストに NAT を設定する必要があります。

  NAT コントロールをイネーブルにしない場合、または同じセキュリティ レベルのインターフェイス間においては、任意のインターフェイス間で NAT を使用することも、使用しないこともできます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要になることがあります。

- **established** コマンド：このコマンドを使用すると、高位レベルのホストから低位レベルのホストに接続がすでに確立されている場合に、低位のセキュリティのホストから高位のセキュリティのホストへのリターン接続が許可されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信の両方の接続に対して **established** コマンドを設定できます。

VLAN インターフェイスの設定

設定可能な VLAN 数については、「ライセンスで使用できる最大アクティブ VLAN インターフェイス数」（P.7-2）を参照してください。

（注）　フェールオーバーを使用している場合、フェールオーバー通信に予約されているインターフェイスには、この方法で名前を付けないでください。フェールオーバー リンクを設定するには、第 14 章「ハイアベイラビリティ」を参照してください。

Easy VPN をイネーブルにすると、VLAN インターフェイスを追加または削除できません。また、セキュリティ レベルまたはインターフェイス名の変更もできません。インターフェイスをすべて設定してから Easy VPN をイネーブルにすることをお勧めします。

この項では、次のトピックについて取り上げます。

[Interfaces] > [Interfaces]

[Interfaces] タブでは、設定済みの VLAN インターフェイスを表示します。VLAN インターフェイスを追加または削除したり、同じセキュリティ レベルのインターフェイス間の通信をイネーブルにしたり、同一インターフェイスを出入りするトラフィックをイネーブルにすることができます。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過できます。

フィールド

- [Name]：インターフェイス名を表示します。
- [Switch Ports]：この VLAN インターフェイスに割り当てられたスイッチ ポートを表示します。
- [Enabled]：インターフェイスがイネーブルであるかどうか（[Yes] または [No]）を示します。
- [Security Level]：インターフェイスのセキュリティ レベルを 0 ～ 100 の範囲で示します。デフォルトのセキュリティ レベルは 0 です。
- [IP Address]：IP アドレスが表示されます。トランスペアレント モードの場合「native」が表示されます。トランスペアレント モードのインターフェイスは IP アドレスを使用しません。IP アドレスをコンテキストまたはセキュリティ アプライアンスに設定するには、[管理 IP アドレス] ペインを参照してください。
- [Subnet Mask]：ルーテッド モードの場合のみ。サブネット マスクを表示します。
- [Restrict Traffic Flow]：このインターフェイスから別の VLAN への接続開始が制限されているかどうかを示します。

  基本ライセンスでは、このオプションを使用して制限した場合だけ、3 つ目の VLAN を設定できます。

たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。ホーム ネットワークはビジネス ネットワークにアクセスする必要がないので、ホーム VLAN で [Restrict Traffic Flow] オプションを使用できます。ビジネス ネットワークはホーム ネットワークにアクセスできますが、その反対はできません。

2 つの VLAN インターフェイスに名前をすでに設定している場合、必ず [Restrict Traffic Flow] オプションをイネーブルにしてから 3 番目のインターフェイスに名前を付けてください。ASA 5505 適応型セキュリティ アプライアンスの基本ライセンスでは、3 つの VLAN インターフェイスがフル機能を持つことは許可されていません。

（注） Security Plus ライセンスにアップグレードすれば、このオプションを削除して、このインターフェイスのフル機能を取得できます。このオプションをイネーブルにしたままにすると、アップグレード後もインターフェイスの制限はそのまま残ります。

- [Backup Interface]：このインターフェイスに使用されるバックアップ ISP インターフェイスを示します。インターフェイスに障害が発生すると、バックアップ インターフェイスに切り替わります。

  プライマリ インターフェイスによるデフォルト ルートに障害が発生しない限り、バックアップ インターフェイスはトラフィックを通過させません。このオプションは Easy VPN で便利です。バックアップ インターフェイスがプライマリになると、セキュリティ アプライアンスは新しいプライマリ インターフェイスに VPN ルールを適用します。

  プライマリに障害が発生した場合に、トラフィックがバックアップ インターフェイスを通過できるようにするには、プライマリとバックアップの両方のインターフェイスにデフォルト ルートを設定して、プライマリでの障害発生時にバックアップ インターフェイスを使用できるようにします。たとえば、2 つのデフォルト ルートを設定して、1 つはアドミニストレーティブ ディスタンスが低いプライマリ インターフェイス用とし、もう 1 つはアドミニストレーティブ ディスタンスが高いバックアップ インターフェイス用とすることができます。デュアル ISP サポートを設定するには、「スタティック ルート トラッキング」（P.16-44）を参照してください。
- [VLAN]：このインターフェイスの VLAN ID を示します。
- [Management Only]：インターフェイスでセキュリティ アプライアンスへのトラフィックが許可されるか、または管理のためだけかを示します。
- [MTU]：MTU を表示します。デフォルトでは、MTU は 1500 です。
- [Active MAC Address]：アクティブな MAC アドレスを示します。[Add/Edit Interface] > [Advanced] タブで手動で割り当てると表示されます。
- [Standby MAC Address]：スタンバイ MAC アドレス（フェールオーバー用）を示します。手動で設定すると表示されます。
- [Description]：説明を表示します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。
- [Add]：インターフェイスを追加します。Easy VPN をイネーブルにしている場合、VLAN インターフェイスを追加できません。
- [Edit]：選択したインターフェイスを編集します。フェールオーバー リンクまたはステート リンクとしてインターフェイスを割り当てている場合（[[Failover]: [Setup]] タブを参照）は、そのインターフェイスをこのペインで編集することはできません。Easy VPN をイネーブルにすると、セキュリティ レベルまたはインターフェイス名を編集できません。

- [Delete] : 選択したインターフェイスを削除します。フェールオーバー リンクまたはステート リンクとしてインターフェイスを割り当てた場合（[[Failover]: [Setup]] タブを参照）は、そのインターフェイスをこのペインで削除することはできません。Easy VPN をイネーブルにしている場合、VLAN インターフェイスを削除できません。
- [Enable traffic between two or more interfaces which are configured with same security levels] : 同じセキュリティ レベルのインターフェイス間の通信をイネーブルにします。同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。
- [Enable traffic between two or more hosts connected to the same interface] : 同一インターフェイスを出入りするトラフィックをイネーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

[Add/Edit Interface] > [General]

[Add/Edit Interface] > [General] タブでは、VLAN インターフェイスを追加または編集できます。

フェールオーバーにインターフェイスを使用する場合は、このダイアログボックスでインターフェイスを設定しないでください。代わりに、[[Failover]: [Setup]] タブを使用します。特に、インターフェイス名は設定しないでください。このパラメータを設定すると、インターフェイスをフェールオーバー リンクとして使用できなくなります。その他のパラメータは無視されます。

Easy VPN をイネーブルにすると、セキュリティ レベルまたはインターフェイス名を編集できません。インターフェイスをすべて設定してから Easy VPN をイネーブルにすることをお勧めします。

インターフェイスをフェールオーバー リンクまたはステート リンクとして割り当てた後で、そのインターフェイスを [Interfaces] ペインから編集または削除することはできません。ただし、唯一の例外として、物理インターフェイスをステート リンクとして設定している場合は、その速度とデュプレックスを設定できます。

フィールド

- [Switch Ports] : スイッチ ポートを VLAN インターフェイスに割り当てます。
  - [Available Switch Ports] : 他のインターフェイスに現在割り当てられている場合でも、すべてのスイッチ ポートを一覧表示します。
  - [Selected Switch Ports] : このインターフェイスに割り当てられているスイッチ ポートを一覧表示します。
  - [Add] : 選択したスイッチ ポートをインターフェイスに追加します。次のメッセージが表示されます。

    「*switchport* is associated with *name* interface.Adding it to this interface, will remove it from *name* interface.Do you want to continue?」

    [OK] をクリックして、スイッチ ポートを追加します。

スイッチ ポートをインターフェイスに追加する場合、このメッセージは常に表示されます。コンフィギュレーションがない場合でも、スイッチ ポートは VLAN 1 インターフェイスにデフォルトで割り当てられています。

  - [Remove]：インターフェイスからスイッチ ポートを削除します。スイッチ ポートのデフォルト VLAN インターフェイスは VLAN 1 であるため、インターフェイスからスイッチ ポートを削除すると、基本的にそのスイッチ ポートは VLAN 1 に単に再割り当てされます。

- [Enable Interface]：インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。この設定に加えて、トラフィックがセキュリティ ポリシーに従って通過できるように、IP アドレス（ルーテッド モード）と名前を事前に設定する必要があります。
- [Dedicate this interface to management only]：インターフェイスを設定してセキュリティ アプライアンスへのトラフィックだけを許可します。通過トラフィックは許可しません。プライマリまたはバックアップ ISP インターフェイスは管理専用に設定できません。
- [Interface Name]：インターフェイス名を 48 文字以内で設定します。
- [Security Level]：セキュリティ レベルを 0（最低）～ 100（最高）の範囲で設定します。セキュリティ アプライアンスは、内部ネットワークから外部ネットワーク（低いセキュリティ レベル）にトラフィックを自由に流すことを許可します。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。
- [IP Address]：ルーテッド モードの場合のみ、IP アドレスを設定します。
  - [Use Static IP]：IP アドレスを手動で設定します。

    [IP address]：IP アドレスを設定します。

    [Subnet Mask]：サブネット マスクを設定します。
  - [Obtain Address via DHCP]：DHCP から IP アドレスを動的に設定します。

    [For the client identifier in DHCP option 61]：オプション 61 用にデフォルトの内部生成文字列ではなく MAC アドレスを強制的に DHCP 要求パケット内に保存するには、[Use MAC address] をクリックします。一部の ISP では、オプション 61 がインターフェイスの MAC アドレスであると想定しています。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。デフォルトの文字列を使用するには、[Use "Cisco-<MAC>-<interface_name>-<host>"] をクリックします。

    [Obtain Default Route Using DHCP]：デフォルト ルートを DHCP サーバから取得します。デフォルトのスタティック ルートの設定が不要になります。

    [Retry Count]：4 ～ 16 の範囲で回数を設定します。セキュリティ アプライアンスは最初の試行後に DHCP 要求に応答がない場合、要求を再送信します。合計試行回数は、再試行回数に最初の試行を加えたものになります。たとえば、再試行回数を 4 に設定すると、セキュリティ アプライアンスは DHCP 要求を 5 回まで送信します。

    [DHCP Learned Route Metric]：アドミニストレーティブ ディスタンスを既知のルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

    [Enable tracking]：DHCP の既知のルートのルート トラッキングをイネーブルにするには、このチェックボックスをオンにします。

    （注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

    [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

[Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワークオブジェクトがあれば表示されます。

[SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。

[Monitoring Options]：[Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。

[Enable DHCP Broadcast flag for DHCP request and discover messages]:セキュリティ アプライアンスが DHCP クライアント パケットにブロードキャスト フラグを設定できるようにします。このオプションにより、DHCP クライアントが IP アドレスを要求する Discover を送信すると DHCP パケット ヘッダーのブロードキャスト フラグが 1 に設定されます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。このオプションを選択しないと、ブロードキャスト フラグは 0 に設定され、DHCP サーバは提供された IP アドレスを使用してクライアントに応答パケットをユニキャストします。DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

[Renew DHCP Lease]：DHCP リースを更新します。

– [Use PPPoE]：PPPoE を使用して IP アドレスを動的に設定します。

[Group Name]：グループ名を指定します。

[PPPoE Username]：ISP によって提供されたユーザ名を指定します。

[PPPoE Password]：ISP によって提供されたパスワードを指定します。

[Confirm Password]：ISP によって提供されたパスワードを指定します。

[PPP Authentication]：[PAP]、[CHAP]、または [MSCHAP] のいずれかを選択します。PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存および比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

[Store Username and Password in Local Flash]：ユーザ名とパスワードを、セキュリティ アプライアンス上の NVRAM の特定の場所に保存します。Auto Update Server が clear config コマンドをセキュリティ アプライアンスに送信し、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再認証できます。

[IP Address and Route Settings]：[PPPoE IP Address and Route Settings] ダイアログが表示され、アドレッシングおよびトラッキングのオプションを選択できます。「PPPoE IP Address and Route Settings」（P.5-19）を参照してください。

• [Description]：オプションの説明を 240 文字以内で入力します。改行を入れずに 1 行で入力します。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

[Add/Edit Interface] > [Advanced]

[Add/Edit Interface] > [Advanced] タブでは、MTU、VLAN ID、MAC アドレスなどのオプションを設定できます。

フィールド

- [MTU] : 300 ～ 65,535 バイトの範囲で MTU を設定します。デフォルトは 1500 バイトです。マルチ コンテキスト モードの場合は、コンテキスト設定で MTU を設定します。
- [VLAN ID] : このインターフェイスの VLAN ID を 1 ～ 4090 の範囲で設定します。VLAN ID を割り当てない場合、ASDM により ID がランダムに割り当てられます。
- [Mac Address Cloning] : 手動で MAC アドレスを割り当てます。

  ルーテッド モードではデフォルトで、すべての VLAN が同じ MAC アドレスを使用します。トランスペアレント モードでは、VLAN は固有の MAC アドレスを使用します。スイッチに必要な場合、またはアクセス コントロールの目的で、固有の VLAN を設定したり、生成された VLAN を変更したりすることができます。

  - [Active Mac Address] : MAC アドレスを H.H.H 形式でインターフェイスに割り当てます。H は 16 ビットの 16 進数です。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。
  - [Standby Mac Address] : フェールオーバーを使用する場合は、スタンバイ MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。
- [Block Traffic] : この VLAN インターフェイスから別の VLAN への接続開始を制限します。

  基本ライセンスでは、このオプションを使用して制限した場合だけ、3 つ目の VLAN を設定できます。

  たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。ホーム ネットワークはビジネス ネットワークにアクセスする必要がないので、ホーム VLAN で [Restrict Traffic Flow] オプションを使用できます。ビジネス ネットワークはホーム ネットワークにアクセスできますが、その反対はできません。

  2 つの VLAN インターフェイスに名前をすでに設定している場合、必ず [Restrict Traffic Flow] オプションをイネーブルにしてから 3 番目のインターフェイスに名前を付けてください。ASA 5505 適応型セキュリティ アプライアンスの基本ライセンスでは、3 つの VLAN インターフェイスがフル機能を持つことは許可されていません。したがって、インターフェイスを設定できません。

（注）　Security Plus ライセンスにアップグレードすれば、このオプションを削除して、このインターフェイスのフル機能を取得できます。このオプションをイネーブルにしたままにすると、アップグレード後もインターフェイスの制限はそのまま残ります。

  - [Block Traffic from this Interface to]：リスト内の VLAN ID を選択します。

- [Select Backup Interface]：このインターフェイスのバックアップ ISP インターフェイスを示します。インターフェイスに障害が発生すると、バックアップ インターフェイスに切り替わります。プライマリ インターフェイスによるデフォルト ルートに障害が発生しない限り、バックアップ インターフェイスはトラフィックを通過させません。このオプションは Easy VPN で便利です。バックアップ インターフェイスがプライマリになると、セキュリティ アプライアンスは新しいプライマリ インターフェイスに VPN ルールを適用します。

  プライマリに障害が発生した場合に、トラフィックがバックアップ インターフェイスを通過できるようにするには、プライマリとバックアップの両方のインターフェイスにデフォルト ルートを設定して、プライマリでの障害発生時にバックアップ インターフェイスを使用できるようにします。たとえば、2 つのデフォルト ルートを設定して、1 つはアドミニストレーティブ ディスタンスが低いプライマリ インターフェイス用とし、もう 1 つはアドミニストレーティブ ディスタンスが高いバックアップ インターフェイス用とすることができます。デュアル ISP サポートを設定するには、「スタティック ルート トラッキング」（P.16-44）を参照してください。

  - [Backup Interface]：リスト内の VLAN ID を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

スイッチ ポートの設定

この項では、スイッチ ポートの設定方法について説明します。次の項目を取り上げます。

- 「[Interfaces] > [Switch Ports]」（P.7-12）
- 「Edit Switch Port」（P.7-13）

注意　ASA 5505 適応型セキュリティ アプライアンスは、ネットワーク内のループ検出用のスパニングツリー プロトコルをサポートしていません。したがって、適応型セキュリティ アプライアンスとのすべての接続は、ネットワーク ループ内で終わらないようにする必要があります。

[Interfaces] > [Switch Ports]

[Switch Ports] タブで、スイッチ ポート パラメータを表示します。

フィールド

- [Switch Port]：セキュリティ アプライアンスのスイッチ ポートを一覧表示します。
- [Enabled]：スイッチ ポートがイネーブルかどうか（[Yes] または [No]）を示します。
- [Associated VLANs]：スイッチ ポートが割り当てられている VLAN インターフェイスを一覧表示します。トランク スイッチ ポートは複数の VLAN に割り当てることができます。
- [Associated Interface Names]：VLAN インターフェイス名を一覧表示します。
- [Mode]：モードはアクセスまたはトランクです。アクセス ポートは 1 つの VLAN に割り当てることができます。トランク ポートは、802.1Q タギングを使用して複数の VLAN を伝送できます。トランク モードが使用できるのは Security Plus ライセンスだけです。
- [Protected]：スイッチ ポートが保護されているかどうか（[Yes] または [No]）を示します。このオプションによって、スイッチ ポートは同じ VLAN 上の他の保護されたスイッチ ポートと通信できなくなります。スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに [Protected] オプションを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。
- [Edit]：スイッチ ポートを編集します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Edit Switch Port

[Edit Switch Port] ダイアログボックスでは、モードの設定、VLAN へのスイッチ ポート割り当て、および [Protected] オプションを設定できます。

フィールド

- [Switch Port]：*表示専用*。選択したスイッチ ポート ID を示します。
- [Enable Switch Port]：このスイッチ ポートをイネーブルにします。
- [Mode and VLAN IDs]：モードと割り当てた VLAN を設定します。
  - [Access VLAN ID]：モードをアクセス モードに設定します。このスイッチ ポートを割り当てる VLAN ID を入力します。デフォルトでは、VLAN ID を [Interfaces] > [Interfaces] で設定した VLAN インターフェイス コンフィギュレーションから取得します。VLAN の割り当てはこのダイアログボックスで変更できます。変更を適用する場合、必ず [Interfaces] > [Interfaces] タブを新しい情報で更新してください。まだ追加していない VLAN を指定する場合、このダイアログボックスで指定するのではなく、VLAN を [Interfaces] > [Interfaces] タブから追加

し、スイッチ ポートを [Add/Edit Interface] > [General] タブで指定することをお勧めします。どちらの場合も、VLAN を [Interfaces] > [Interfaces] タブで追加してからスイッチ ポートを割り当てる必要があります。

  - [Trunk VLAN IDs] : モードを、802.1Q タグ付けを使用するトランク モードに設定します。トランク モードが使用できるのは Security Plus ライセンスだけです。このスイッチ ポートに割り当てる VLAN ID をカンマで区切って入力します。トランク ポートでは、タグが付いていないパケットはサポートされません。ネイティブ VLAN サポートはなく、このコマンドで指定されたタグが含まれていないパケットはすべて、適応型セキュリティ アプライアンスによってドロップされます。VLAN を設定済みの場合、変更を適用すると、[Interfaces] > [Interfaces] タブで、各 VLAN に追加されたこのスイッチ ポートを確認できます。まだ追加していない VLAN を指定する場合、このダイアログボックスで指定するのではなく、VLAN を [Interfaces] > [Interfaces] タブから追加し、スイッチ ポートを [Add/Edit Interface] > [General] タブで指定することをお勧めします。どちらの場合も、VLAN を [Interfaces] > [Interfaces] タブで追加してからスイッチ ポートを割り当てる必要があります。

- [Isolated] : このオプションによって、スイッチ ポートは同じ VLAN 上の他の保護されたスイッチ ポートと通信できなくなります。スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに [Protected] オプションを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。
  - [Isolated] : 保護ポートとしてこのスイッチ ポートを設定します。
- [Duplex] : インターフェイスのデュプレックス オプションが一覧表示されます。[Full]、[Half]、または [Auto] があります。デフォルトの設定は Auto です。PoE ポート Ethernet 0/6 または 0/7 でデュプレックスを [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。
- [Speed] : デフォルトの設定は Auto です。PoE ポート Ethernet 0/6 または 0/7 で速度を [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。デフォルトの [Auto] 設定には、Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかを [Auto] に設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

CHAPTER 8

グローバル オブジェクトの追加

[Objects] ペインでは、セキュリティ アプライアンスにポリシーを組み込む際に不可欠な再利用コンポーネントの設定、表示、修正がすべてできます。たとえば、セキュリティ ポリシーの対象ホストやネットワークを定義すると、ホストやネットワークを選択するだけで機能を適用でき、適用対象を何度も定義する必要がなくなります。そのため、時間を短縮できると同時に、一貫性のあるセキュリティ ポリシーを高い精度で実現できます。ホストやネットワークの追加、削除が必要な場合、[Objects] ペインを利用して 1 箇所から変更できます。

この章は、次の項で構成されています。

ネットワーク オブジェクトおよびグループの使用

この項では、ネットワーク オブジェクトおよびグループの使用方法について説明します。次の項目を取り上げます。

ネットワーク オブジェクトの概要

ネットワーク オブジェクトを使用すると、ホストおよびネットワークの IP アドレスを事前に定義して、以降の設定を効率よく行えます。アクセス ルールや AAA ルールなどのセキュリティ ポリシーを設定すると、手動で入力する代わりに事前定義済みのアドレスを選択できます。さらに、オブジェクトの定義を変更した場合、変更内容は自動的にそのオブジェクトを使用するすべてのルールに継承されます。

ネットワーク オブジェクトは手動で追加できます。または、ASDM にアクセス ルールや AAA ルールのような既存のコンフィギュレーションからオブジェクトを自動的に作成させることもできます。このような派生したオブジェクトのいずれかを編集した場合、後でそのオブジェクトを使用していたルールを削除してもその編集内容は残ります。編集しない場合、リフレッシュすると、派生したオブジェクトには現在のコンフィギュレーションが反映されるだけです。

ネットワーク オブジェクト グループは、複数のホストとネットワークが一緒に含まれるグループです。ネットワーク オブジェクト グループには、他のネットワーク オブジェクト グループを含めることもできます。このため、ネットワーク オブジェクト グループを送信元アドレスまたは宛先アドレスとしてアクセス ルールに指定できます。

ルールの設定時に、[ASDM] ウィンドウの右側には [Addresses] サイド ペインがあり、使用可能なネットワーク オブジェクトとネットワーク オブジェクト グループが表示されます。[Addresses] ペインで直接オブジェクトを追加、編集、または削除できます。また、追加するネットワーク オブジェクトおよびグループを [Addresses] ペインから選択したアクセス ルールの送信元または宛先にドラッグできます。

ネットワーク オブジェクトの設定

ネットワーク オブジェクトを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Network Objects/Group] ペインで、[Add] > [Network Object] をクリックして新しいオブジェクト グループを追加するか、オブジェクトを選択して [Edit] をクリックします。

ルール ウィンドウの [Addresses] サイド ペインで、またはルールの追加時に、ネットワーク オブジェクトを追加または編集することもできます。

リスト内のオブジェクトを検索するには、[Filter] フィールドに名前または IP アドレスを入力して [Filter] をクリックします。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。

[Add/Edit Network Object] ダイアログボックスが表示されます。

ステップ 2　次の値を入力します。

- [Name]：（任意）オブジェクト名。使用できる文字は、a ～ z、A ～ Z、0 ～ 9、ドット（.）、ダッシュ（-）、およびアンダースコア（_）です。名前は 64 文字以下にする必要があります。
- [IP Address]：IP アドレス（ホストまたはネットワーク アドレス）。
- [Netmask]：IP アドレスのサブネット マスク。
- [Description]：（任意）ネットワーク オブジェクトの説明。

ステップ 3　[OK] をクリックします。

これでルールの作成時にこのネットワーク オブジェクトを使用できます。編集したオブジェクトの場合、変更内容は自動的にそのオブジェクトを使用するすべてのルールに継承されます。

（注）　使用中のネットワーク オブジェクトは削除できません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ネットワーク オブジェクト グループの設定

ネットワーク オブジェクト グループを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Network Objects/Group] ペインで、[Add] > [Network Object Group] をクリックして新しいオブジェクト グループを追加するか、オブジェクト グループを選択して [Edit] をクリックします。

ルール ウィンドウの [Addresses] サイド ペインで、またはルールの追加時に、ネットワーク オブジェクト グループを追加または編集できます。

リスト内のオブジェクトを検索するには、[Filter] フィールドに名前または IP アドレスを入力して [Filter] をクリックします。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。

[Add/Edit Network Object Group] ダイアログボックスが表示されます。

ステップ 2　[Group Name] フィールドで、グループ名を入力します。

使用できる文字は、a ～ z、A ～ Z、0 ～ 9、ドット（.）、ダッシュ（-）、およびアンダースコア（_）です。名前は 64 文字以下にする必要があります。

ステップ 3　（任意）[Description] フィールドで、説明を長さ 200 文字以内で入力します。

ステップ 4　既存のオブジェクトまたはグループを新しいグループに追加したり（グループのネストが可能）、新しいアドレスを作成してグループに追加したりできます。

- 既存のネットワーク オブジェクトまたはグループを新しいグループに追加するには、[Existing Network Objects/Groups] ペインでオブジェクトをダブルクリックします。

  または、オブジェクトを選択して、[Add] をクリックします。オブジェクトまたはグループが右側の [Members in Group] ペインに追加されます。
- 新しいアドレスを追加するには、[Create New Network Object Member] 領域で値を入力し、[Add] をクリックします。

  オブジェクトまたはグループが右側の [Members in Group] ペインに追加されます。このアドレスはネットワーク オブジェクト リストにも追加されます。

オブジェクトを削除するには、[Members in Group] ペインでオブジェクトをダブルクリックするか、[Remove] をクリックします。

ステップ 5　すべてのメンバ オブジェクトを追加し終えたら、[OK] をクリックします。

これでルールの作成時にこのネットワーク オブジェクト グループを使用できます。編集したオブジェクト グループの場合、変更内容は自動的にそのグループを使用するすべてのルールに継承されます。

（注）　使用中のネットワーク オブジェクト グループは削除できません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ルールでのネットワーク オブジェクトおよびグループの使用

ルールの作成時には、手動で IP アドレスを入力したり、ルールで使用するネットワーク オブジェクトまたはグループを参照したりできます。

（注）　アクセス ルールのみの場合は、ネットワーク オブジェクトおよびグループを [Addresses] ペインから選択したアクセス ルールの送信元または宛先にドラッグ アンド ドロップできます。

ルールでネットワーク オブジェクトまたはグループを使用するには、次の手順を実行します。

ステップ 1　ルール ダイアログボックスで、送信元または宛先のアドレス フィールドの横にある [...] 参照ボタンをクリックします。

[Browse Source Address] または [Browse Destination Address] ダイアログボックスが表示されます。

ステップ 2　新しいネットワーク オブジェクトまたはグループを追加したり、既存のネットワーク オブジェクトまたはグループをダブルクリックして選択したりできます。

リスト内のオブジェクトを検索するには、[Filter] フィールドに名前または IP アドレスを入力して [Filter] をクリックします。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。

- 新しいネットワーク オブジェクトを追加する方法について、「ネットワーク オブジェクトの設定」（P.8-2）を参照してください。
- 新しいネットワーク オブジェクト グループを追加する方法については、「ネットワーク オブジェクト グループの設定」（P.8-3）を参照してください。

新しいオブジェクトを追加するか、既存のオブジェクトをダブルクリックすると、そのオブジェクトが [Selected Source/Destination] フィールドに表示されます。アクセス ルールの場合、このフィールドに複数のオブジェクトをカンマで区切って入力できます。

ステップ 3　[OK] をクリックします。

ルール ダイアログボックスに戻ります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ネットワーク オブジェクトまたはグループの使用状況の表示

ネットワーク オブジェクトまたはグループを使用しているルールを表示するには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Group] ペインで拡大鏡の形をした [Find] アイコンをクリックします。

[Usages] ダイアログボックスが表示され、現在ネットワーク オブジェクトまたはグループを使用しているすべてのルールが一覧表示されます。このダイアログボックスには、そのオブジェクトが含まれるネットワーク オブジェクト グループもすべて一覧表示されます。

サービス グループの設定

この項では、サービス グループを設定する方法について説明します。説明する内容は次のとおりです。

- 「Service Groups」（P.8-5）
- 「Add/Edit Service Group」（P.8-6）
- 「Browse Service Groups」（P.8-7）

Service Groups

[Service Groups] ペインでは、指定したグループに複数のサービスを関連付けられます。1 つのグループに任意のタイプのプロトコルとサービスを指定できます。または、次のタイプごとにサービス グループを作成できます。

- TCP ポート
- UDP ポート
- TCP-UDP ポート
- ICMP タイプ
- IP プロトコル

複数のサービス グループをネストすれば、「グループのグループ」を構成できます。「グループのグループ」は 1 つのグループとして使用できます。

サービス グループは、ポート、ICMP タイプ、プロトコルを識別する必要がある多くのコンフィギュレーションで使用できます。NAT ルールやセキュリティ ポリシー ルールの設定時に、[ASDM] ウィンドウの右側の [Services] ペインにもサービス グループやその他の使用可能なグローバル オブジェクトが表示されます。この [Services] ペインから直接オブジェクトを追加、編集、削除できます。

フィールド

- [Add]：サービス グループを追加します。追加するサービス グループのタイプをドロップダウンリストから選択します。複数タイプの場合は [Service Group] を選択します。
- [Edit]：サービス グループを編集します。
- [Delete]：サービス グループを削除します。サービス グループを削除すると、使用されているすべてのサービス グループから削除されます。サービス グループがアクセス ルールで使用されている場合は、削除しないでください。アクセス ルールで使用されているサービス グループを空にはできません。
- [Find]：一致する名前だけを表示するように、表示内容をフィルタリングします。[Find] をクリックすると、[Filter] フィールドが開きます。もう一度 [Find] をクリックすると、[Filter] フィールドは非表示になります。
  - [Filter field]：サービス グループの名前を入力します。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。
  - [Filter]：フィルタを実行します。
  - [Clear]：[Filter] フィールドをクリアします。
- [Name]：サービス グループ名を一覧表示します。名前の隣にあるプラス（[+]）アイコンをクリックすると、サービス グループが展開され、サービスを確認できます。マイナス（[-]）アイコンをクリックすると、サービス グループが折りたたまれます。
- [Protocol]：サービス グループ プロトコルを一覧表示します。
- [Source Ports]：プロトコルの送信元ポートを一覧表示します。
- [Destination Ports]：プロトコルの宛先ポートを一覧表示します。
- [ICMP Type]：サービス グループの ICMP タイプを一覧表示します。
- [Description]：サービス グループの説明を一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Service Group

[Add/Edit Service Group] ダイアログボックスでは、サービスをサービス グループに割り当てられます。このダイアログボックス名は追加するサービス グループのタイプと同じ名前になります。たとえば、追加するサービス グループが TCP の場合、[Add/Edit TCP Service Group] ダイアログボックスが表示されます。

フィールド

- [Group Name]：グループ名を 64 文字以内で入力します。名前は、すべてのオブジェクト グループで一意であることが必要です。サービス グループの名前にネットワーク オブジェクト グループで使用した名前は使用できません。
- [Description]：サービス グループの説明を 200 文字以内で入力します。
- [Existing Service/Service Group]：サービス グループに追加可能な項目を示します。定義済みのサービス グループから選択するか、よく使用されるポート、タイプ、プロトコルの名前のリストから選択します。
  - [Service Groups]：このテーブルのタイトルは、追加するサービス グループのタイプによって異なります。定義済みサービス グループが含まれます。
  - [Predefined]：事前定義済みのポート、タイプ、またはプロトコルを一覧表示します。
- [Create new member]：新しいサービス グループ メンバを作成できます。
  - [Service Type]：新しいサービス グループ メンバのサービス タイプを選択できます。サービス タイプには、TCP、UDP、TCP-UDP、ICMP、および protocol があります。
  - [Destination Port/Range]：新しい TCP、UDP、または TCP-UDP サービス グループ メンバの宛先ポートまたは範囲を入力できます。
  - [Source Port/Range]：新しい TCP、UDP、または TCP-UDP サービス グループ メンバの送信元ポートまたは範囲を入力できます。
  - [ICMP Type]：新しい ICMP サービス グループ メンバの ICMP タイプを入力できます。
  - [Protocol]：新しい protocol サービス グループ メンバのプロトコルを入力できます。
- [Members in Group]：サービス グループに追加済みのアイテムを示します。
- [Add]：選択したアイテムをサービス グループに追加します。
- [Remove]：選択したアイテムをサービス グループから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Browse Service Groups

[Browse Service Groups] ダイアログボックスでは、サービス グループを選択できます。このダイアログボックスはさまざまなコンフィギュレーション画面で使用され、その時のタスクに該当する名前で表示されます。たとえば、[Add/Edit Access Rule] ダイアログボックスから使用した場合、このダイアログボックス名は [Browse Source Port] または [Browse Destination Port] になります。

フィールド

- [Add]：サービス グループを追加します。
- [Edit]：選択したサービス グループを編集します。

- [Delete]：選択したサービス グループを削除します。
- [Find]：一致する名前だけを表示するように、表示内容をフィルタリングします。[Find] をクリックすると、[Filter] フィールドが開きます。もう一度 [Find] をクリックすると、[Filter] フィールドは非表示になります。
  - [Filter field]：サービス グループの名前を入力します。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。
  - [Filter]：フィルタを実行します。
  - [Clear]：[Filter] フィールドをクリアします。
- [Type]：TCP、UDP、TCP-UDP、ICMP、Protocol など、表示するサービス グループのタイプを選択できます。タイプをすべて表示するには、[All] を選択します。通常、ルールのタイプを設定する場合、使用できるサービス グループのタイプは 1 つだけです。TCP のアクセス ルールに UDP のサービス グループは選択できません。
- [Name]：サービス グループ名を示します。アイテムの名前の隣にあるプラス（[+]）アイコンをクリックすると、アイテムが展開されます。マイナス（[-]）アイコンをクリックすると、アイテムが折りたたまれます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

クラス マップの設定

クラス マップの詳細については、「クラス マップのフィールドの説明」（P.24-40）を参照してください。

インスペクション マップの設定

インスペクション マップの詳細については、「インスペクション マップのフィールドの説明」（P.24-61）を参照してください。

正規表現の設定

この項では、正規表現を設定する方法について説明します。説明する内容は次のとおりです。

- 「Add/Edit Regular Expression Class Map」（P.8-14）

正規表現

「クラス マップの設定」や「インスペクション マップの設定」の一部で、パケット内のテキストを照合する正規表現を指定できます。正規表現のクラス マップ内に単独またはグループのいずれかで作成する場合でも、クラス マップまたはインスペクション マップを設定する前に、必ず正規表現を作成してください。

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、*metacharacters* を使用してテキスト ストリングの複数のバリアントと照合することもできます。正規表現を使用して、特定のアプリケーション トラフィックの内容（HTTP パケット内の本文テキストなど）を照合できます。

フィールド

- [Regular Expressions]：正規表現を示します。
  - [Name]：正規表現の名前を示します。
  - [Value]：正規表現の定義値を示します。
  - [Add]：正規表現を追加します。
  - [Edit]：正規表現を編集します。
  - [Delete]：正規表現を削除します。
- [Regular Expression Classes]：正規表現クラス マップを示します。
  - [Name]：正規表現クラス マップの名前を示します。
  - [Match Conditions]：クラス マップの照合タイプと正規表現を示します。

    [Match Type]：照合タイプを示します。正規表現の場合、常に基準の肯定一致タイプ（等号（=）を表示したアイコン）になります。また、インスペクション クラス マップで否定一致（赤丸を表示したアイコン）の作成もできます。クラス マップに正規表現が複数ある場合は、照合タイプ アイコンの隣にそれぞれ「OR」を表示し、「match any」クラス マップになっていることを示します。正規表現のいずれか 1 つと一致するだけで、トラフィックがクラス マップに一致します。

    [Regular Expression]：クラス マップごとに登録されている正規表現を一覧表示します。
  - [Description]：クラス マップの説明を示します。
  - [Add]：正規表現クラス マップを追加します。
  - [Edit]：正規表現クラス マップを編集します。
  - [Delete]：正規表現クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Regular Expression

[Add/Edit Regular Expression] ダイアログボックスでは、正規表現を定義しテストできます。

フィールド

- [Name]：正規表現の名前を 40 文字以内で入力します。
- [Value]：正規表現を 100 文字以内で入力します。表 8-1 に示すメタ文字を使用するか、または [Build] をクリックし、Build Regular Expression のダイアログボックスを利用してテキストを手動で入力します。

（注） 最適化のために、セキュリティ アプライアンスでは、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（/）が単一のスラッシュに圧縮されます。「http://」などの、一般的に 2 つのスラッシュが使用されるストリングでは、代わりに「http:/」を検索してください。

表 8-1 に、特別な意味を持つメタ文字の一覧を示します。

表 8-1　　regex メタ文字

文字	説明	注意事項
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp*)	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。 **（注）** Ctrl+V を入力してから疑問符を入力しないと、ヘルプ機能が呼び出されます。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は lse、lose、loose、などと一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{*x*} または {*x*,}	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc*]	文字クラス	カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。

表 8-1　regex メタ文字 （続き）

文字	説明	注意事項
[^*abc*]	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は、a、b、c 以外の任意の文字に一致します。**[^A-Z]** は、大文字のアルファベット文字以外の任意の単一の文字に一致します。
[*a-c*]	文字範囲クラス	範囲内の任意の文字と一致します。**[a-z]** は、任意の小文字のアルファベット文字に一致します。文字と範囲を組み合わせて使用することもできます。**[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。
""	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**" test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	Tab	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

- [Build]：Build Regular Expression のダイアログボックスを利用して正規表現を作成できます。
- [Test]：正規表現を適切なサンプル テキストでテストします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Build Regular Expression

[Build Regular Expression] ダイアログボックスでは、文字やメタ文字を構成して正規表現を作成できます。メタ文字の挿入フィールドでは、カッコで囲まれたメタ文字がフィールド名に表示されます。

（注） 最適化のために、セキュリティ アプライアンスでは、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（/）が単一のスラッシュに圧縮されます。「http://」などの、一般的に 2 つのスラッシュが使用されるストリングでは、代わりに「http:/」を検索してください。

フィールド

[Build Snippet]：このエリアで、正規表現テキストの部分式を作成したり、メタ文字を [Regular Expression] フィールドに挿入したりできます。

- [Starts at the beginning of the line (^)]：部分式は行頭から開始し、開始場所はメタ文字のカレット（^）で示します。このオプションを使用して作成した部分式は、正規表現の先頭に挿入してください。
- [Specify Character String]：テキスト文字列を手動で入力します。
  - [Character String]：テキスト文字列を入力します。
  - [Escape Special Characters]：テキスト文字列に入力したメタ文字を文字そのものとして扱う場合、このボックスをオンにすると、メタ文字の前にエスケープ文字であるバックスラッシュ（\）が追加されます。たとえば、「example.com」と入力すると「example\.com」に変換されます。
  - [Ignore Case]：大文字と小文字を両方とも照合する場合、このチェックボックスをオンにすると、両方を照合するテキストが自動的に追加されます。たとえば、「cats」と入力すると「[cC][aA][tT][sS]」に変換されます。
- [Specify Character]：正規表現に挿入するメタ文字を指定します。
  - [Negate the character]：識別した文字を照合の対象外に指定します。
  - [Any character (.)]：すべての文字と一致させる、メタ文字のピリオド（.）を挿入します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
  - [Character set]：文字セットを挿入します。テキストをこのセットに含まれるすべての文字と照合します。次のようなセットがあります。

    [0-9A-Za-z]

    [0-9]

    [A-Z]

    [a-z]

    [aeiou]

    [\n\f\r\t]（改行、改ページ、復帰、タブを示す）

    たとえば、[0-9A-Za-z] の場合、部分式は 0 ～ 9 の数字と A ～ Z の大文字および小文字と照合します。
  - [Special character]：エスケープが必要な文字 \、?、*、+、|、.、[、(、^ を挿入します。エスケープ文字はバックスラッシュ（\）で、このオプションを選択すると自動的に入力されます。
  - [Whitespace character]：空白スペースには \n（改行）、\f（改ページ）、\r（復帰）、\t（タブ）があります。

  - [Three digit octal number]：8 進数を使用する ASCII 文字（3 桁まで）と一致します。たとえば、\040 はスペースを意味します。バックスラッシュ（\）は自動的に入力されます。
  - [Two digit hexadecimal number]：16 進数を使用する ASCII 文字（2 桁まで）と一致します。バックスラッシュ（\）は自動的に入力されます。
  - [Specified character]：任意の 1 文字を入力します。
- [Snippet Preview]：*表示専用*。正規表現に入力される部分式を示します。
- [Append Snippet]：部分式を正規表現の最後に追加します。
- [Append Snippet as Alternate]：部分式をパイプ記号（|）で区切って、正規表現の最後に追加します。区切られた表現の一方と照合します。たとえば、**dog|cat** は、dog または cat に一致します。
- [Insert Snippet at Cursor]：部分式をカーソル位置に挿入します。

[Regular Expression]：このエリアには、手動で入力して部分式で作成できる正規表現テキストが含まれます。その後、[Regular Expression] フィールドのテキストを選択して、選択部分に数量詞を適用できます。

- [Selection Occurrences]：[Regular Expression] フィールドのテキストを選択し、次のいずれかのオプションをクリックしてから [Apply to Selection] をクリックします。たとえば、正規表現「test me」の「me」を選択して [One or more times] を適用すると、この正規表現は「test (me)+」になります。
  - [Zero or one times (?)]：この記号よりも前の表現が 0 または 1 つあることを示す数量詞です。たとえば、**lo?se** は、lse または lose に一致します。
  - [One or more times (+)]：この記号よりも前の表現が少なくとも 1 つあることを示す数量詞です。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
  - [Any number of times (*)]：この記号よりも前の表現が 0、1、またはそれ以上あることを示す数量詞です。たとえば、**lo*se** は lse、lose、loose、などと一致します。
  - [At least]：少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は abxyxyz、abxyxyxyz などと一致します。
  - [Exactly]：*x* 回だけ繰り返します。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
  - [Apply to Selection]：数量詞を選択部分に適用します。
- [Test]：正規表現を適切なサンプル テキストでテストします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Test Regular Expression

[Test Regular Expression] ダイアログボックスでは、入力テキストを正規表現でテストし、意図したとおりに一致するかどうかを確認できます。

フィールド

- [Regular Expression]：テストする正規表現を入力します。デフォルトでは、Add/Edit Regular Expression または Build Regular Expression ダイアログボックスで入力した正規表現が、このフィールドに入力されます。テスト中に正規表現を変更した場合、[OK] をクリックすると [Add/Edit Regular Expression] や [Build Regular Expression] ダイアログボックスにその変更内容が継承されます。[Cancel] をクリックすると、変更内容は失われます。
- [Test String]：正規表現で一致すると想定されたテキスト文字列を入力します。
- [Test]：[Text String] のテキスト文字列を [Regular Expression] の正規表現でテストします。
- [Test Result]：*表示専用*。テストの成功 / 失敗を示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Regular Expression Class Map

[Add/Edit Regular Expression Class Map] ダイアログボックスで、正規表現をグループ化します。正規表現クラス マップは、インスペクション クラス マップとインスペクション ポリシー マップで使用できます。

フィールド

- [Name]：クラス マップの名前を 40 文字以内で入力します。「class-default」という名前は予約されています。すべてのタイプのクラス マップで同じ名前スペースが使用されるため、別のタイプのクラス マップですでに使用されている名前は再度使用できません。
- [Description]：説明を 200 文字以内で入力します。
- [Available Regular Expressions]：クラス マップに割り当てられていない正規表現を一覧表示します。
  - [Edit]：選択した正規表現を編集します。
  - [New]：新しい正規表現を作成します。
- [Add]：選択した正規表現をクラス マップに追加します。
- [Remove]：選択した正規表現をクラス マップから削除します。
- [Configured Match Conditions]：クラス マップの正規表現を照合タイプとともに示します。
  - [Match Type]：照合タイプを示します。正規表現の場合、常に基準の肯定一致タイプ（等号（=）を表示したアイコン）になります。また、インスペクション クラス マップで否定一致（赤丸を表示したアイコン）の作成もできます。クラス マップに正規表現が複数ある場合は、照合タイプ アイコンの隣にそれぞれ「OR」を表示し、「match any」クラス マップになっていることを示します。正規表現のいずれか 1 つと一致するだけで、トラフィックがクラス マップに一致します。
  - [Regular Expression]：このクラス マップに含まれている正規表現の名前を一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

TCP マップの設定

TCP マップの詳細については、「接続設定と TCP 正規化のイネーブル化」（P.27-8）を参照してください。

グローバル プールの設定

グローバル プールの詳細については、「ダイナミック NAT の使用」（P.25-18）を参照してください。

時間範囲の設定

[Time Ranges] オプションで開始時間と終了時間を定義する再利用コンポーネントを作成し、さまざまなセキュリティ機能に適用します。時間範囲を 1 回だけ定義すれば、後は時間範囲を選択して、スケジューリングが必要なさまざまなオプションに適用できます。

時間範囲機能を使用して時間の範囲を定義し、トラフィックのルールやアクションに使用できます。たとえば、アクセス リストに時間範囲を設定すると、セキュリティ アプライアンスのアクセスを制限できます。

時間範囲は、開始時間、終了時間、およびオプションの繰り返しエントリで構成されます。

（注）　時間範囲を作成してもデバイスへのアクセスは制限されません。このペインでは時間範囲だけを定義します。

フィールド

- [Name]：時間範囲の名前を指定します。
- [Start Time]：時間範囲の開始時刻を指定します。
- [End Time]：時間範囲の終了時刻を指定します。
- [Recurring Entries]：指定した開始時刻と停止時刻の範囲内でアクティブな時間の追加制限を指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Time Rnage

[Add/Edit Time Range] ペインでは、特定の日付と時刻を定義し、アクションに設定できます。たとえば、アクセス リストに時間範囲を設定すると、セキュリティ アプライアンスのアクセスを制限できます。時間範囲はセキュリティ アプライアンスのシステム クロックに依存しています。ただし、この機能は、NTP 同期化により最適に動作します。

（注） 時間範囲を作成してもデバイスへのアクセスは制限されません。このペインでは時間範囲だけを定義します。

フィールド

- [Time Range Name]：時間範囲の名前を指定します。スペースや引用符は使用できません。また、先頭にはアルファベットか数字を使用します。
- [Start now/Started]：時間範囲がただちに開始するか、または時間範囲がすでに始まっているかを指定します。このボタンのラベルは、追加/編集する時間範囲の設定状態によって変わります。時間範囲を新規追加する場合または固定の開始時間が定義された時間範囲を編集する場合、ボタンは [Start Now] になります。開始時間が非固定の時間範囲を編集する場合は、ボタンが [Started] になります。
- [Start Time]：時間範囲の開始時刻を指定します。
  - [Month]：月を 1 月～ 12 月の範囲で指定します。
  - [Day]：日を 01 ～ 31 の範囲で指定します。
  - [Year]：年を 1993 ～ 2035 の範囲で指定します。
  - [Hour]：時間を 00 ～ 23 の範囲で指定します。
  - [Minute]：分を 00 ～ 59 の範囲で指定します。
- [Never end]：時間範囲が終了しない場合に指定します。
- [End at (inclusive)]：時間範囲の終了時刻を指定します。指定した終了時刻も範囲に含まれます。たとえば、指定した時間範囲が 11:30 で終了する場合、11 時 30 分 59 秒まで有効です。この場合、時間範囲は 11:31 になったとき終了します。
  - [Month]：月を 1 月～ 12 月の範囲で指定します。
  - [Day]：日を 01 ～ 31 の範囲で指定します。
  - [Year]：年を 1993 ～ 2035 の範囲で指定します。
  - [Hour]：時間を 00 ～ 23 の範囲で指定します。
  - [Minute]：分を 00 ～ 59 の範囲で指定します。

- [Recurring Time Ranges]：時間範囲を日単位または週単位で設定します。
  - [Add]：繰り返し時間範囲を追加します。
  - [Edit]：選択した繰り返し時間範囲を編集します。
  - [Delete]：選択した繰り返し時間範囲を削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Recurring Time Range

[Add/Edit Recurring Time Range] ペインでは、日単位または週単位で時間範囲を詳細に指定できます。

（注）　時間範囲を作成してもデバイスへのアクセスは制限されません。このペインでは時間範囲だけを定義します。

フィールド

- Days of the week
  - [Every day]：週の毎日を指定します。
  - [Weekdays]：月曜日～金曜日を指定します。
  - [Weekends]：土曜日と日曜日を指定します。
  - [On these days of the week]：特定の曜日を指定します。
  - [Daily Start Time]：時間範囲が開始する時間と分を指定します。
  - [Daily End Time (inclusive)] エリア：時間範囲が終了する時間と分を指定します。指定した終了時刻も範囲に含まれます。
- Weekly Interval
  - [From]：月曜日～日曜日までの曜日を一覧表示します。
  - [Through]：月曜日～日曜日までの曜日を一覧表示します。
  - [Hour]：時間を 00 ～ 23 の範囲で一覧表示します。
  - [Minute]：分を 00 ～ 59 の範囲で一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

暗号化トラフィック インスペクション

この項では、暗号化トラフィック インスペクションを設定する方法について説明します。説明する内容は次のとおりです。

TLS プロキシ

[TLS Proxy] オプションを使用して、Cisco CallManager と対話する SSL 暗号化 VoIP シグナリング（Skinny および SIP）の検査をイネーブルにします。

[TLS Proxy] ペインでは、Transaction Layer Security（TLS）Proxy を定義および設定して暗号化トラフィック インスペクションをイネーブルにできます。

フィールド

- [TLS Proxy Name]：TLS Proxy 名を一覧表示します。
- [Server]：トラストポイントを一覧表示します。自己署名または証明書サーバに登録済みのいずれかになります。
- [Local Dynamic Certificate Issuer]：クライアント ダイナミック証明書またはサーバ ダイナミック証明書を発行するローカル認証局を一覧表示します。
- [Local Dynamic Certificate Key Pair]：クライアント ダイナミック証明書またはサーバ ダイナミック証明書が使用する RSA キー ペアを一覧表示します。
- [Add]：TLS Proxy を追加します。
- [Edit]：TLS Proxy を編集します。
- [Delete]：TLS Proxy を削除します。
- [Maximum Sessions]：サポートする TLS Proxy の最大セッション数を指定できます。
  - ASA がサポートする必要がある TLS Proxy の最大セッション数を指定します。デフォルトでは、ASA がサポートするセッション数は 300 です。[Maximum number of sessions] オプションをイネーブルにします。
  - セッションの最大数：最小数は 1 です。最大値は、プラットフォームによって異なります。デフォルトは 300 です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit TLS Proxy

[Add/Edit TLS Proxy] ダイアログボックスでは、TLS Proxy のパラメータを定義できます。

フィールド

- [TLS Proxy Name]：TLS Proxy 名を指定します。
- [Server Configuration]：プロキシ証明書名を指定します。
  - [Server]：TLS ハンドシェイク中に提示するトラストポイントを指定します。トラストポイントは自己署名の場合と、ローカルでプロキシの証明書サービスに登録済みの場合があります。
- [Client Configuration]：ローカル ダイナミック証明書の発行者とキー ペアを指定します。
  - [Local Dynamic Certificate Issuer]：クライアント ダイナミック証明書またはサーバ ダイナミック証明書を発行するローカル認証局を一覧表示します。

    [Certificate Authority Server]：認証局サーバを指定します。

    [Certificate]：証明書を指定します。

    [Manage]：ローカル認証局を設定します。初期設定の終了後にコンフィギュレーションを変更する場合は、ローカル認証局をディセーブルにします。
  - [Local Dynamic Certificate Key Pair]：クライアント ダイナミック証明書が使用する RSA キー ペアを一覧表示します。

    [Key-Pair Name]：定義済みキー ペアを指定します。

    [Show]：生成時刻、使用方法、係数サイズ、キー データなど、キー ペアの詳細を表示します。

    [New]：新しいキー ペアを定義できます。
- [More Options]：TLS ハンドシェイク中に通知または照合する使用可能でアクティブなアルゴリズムを指定します。
  - [Available Algorithms]：TLS ハンドシェイク中に通知または照合する使用可能なアルゴリズム（des-sha1、3des-sha1、aes128-sha1、aes256-sha1、null-sha1）を一覧表示します。

    [Add]：選択したアルゴリズムをアクティブ リストに追加します。

    [Remove]：選択したアルゴリズムをアクティブ リストから削除します。
  - [Active Algorithms]：TLS ハンドシェイク中に通知または照合するアクティブなアルゴリズム（des-sha1、3des-sha1、aes128-sha1、aes256-sha1、null-sha1）を一覧表示します。クライアント プロキシ（サーバに対する TLS クライアントとして機能）の場合、2 つの TLS レッグ間の非対称暗号化方式のために、ユーザ定義のアルゴリズムで hello メッセージの元のアルゴリズムが置き換えられます。たとえば、CallManager をオフロードするために、プロキシと CallManager の間のレッグにはヌル暗号化が使用される場合があります。

    [Move Up]：アルゴリズムをリストの上に移動します。

    [Move Down]：アルゴリズムをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CTL Provider

[CTL Provider] オプションは、Certificate Trust List（CTL）プロバイダー サービスを設定するために使用します。

[CTL Provider] ペインでは、Certificate Trust List プロバイダー サービスを定義および設定して、暗号化トラフィック インスペクションをイネーブルにできます。

フィールド

- [CTL Provider Name]：CTL プロバイダー名を一覧表示します。
- [Client Details]：クライアントの名前と IP アドレスを一覧表示します。
  - [Interface Name]：定義されているインターフェイス名を一覧表示します。
  - [IP Address]：定義されているインターフェイス IP アドレスを一覧表示します。
- [Certificate Name]：エクスポートする証明書を一覧表示します。
- [Add]：CTL プロバイダーを追加します。
- [Edit]：CTL プロバイダーを編集します。
- [Delete]：CTL プロバイダーを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit CTL Provider

[Add/Edit CTL Provider] ダイアログボックスでは、CTL プロバイダーのパラメータを定義できます。

フィールド

- [CTL Provider Name]：CTL プロバイダー名を指定します。
- [Certificate to be Exported]：クライアントにエクスポートする証明書を指定します。

- [Certificate Name]：クライアントにエクスポートする証明書の名前を指定します。
- [Manage]：ID 証明書を管理します。

- [Client Details]：接続を許可するクライアントを指定します。
  - [Client to be Added]：クライアント リストに追加するクライアント インターフェイスと IP アドレスを指定します。

    [Interface]：クライアント インターフェイスを指定します。

    [IP Address]：クライアント IP アドレスを指定します。

    [Add]：クライアント リストに新しいクライアントを追加します。

    [Delete]：クライアント リストから選択したクライアントを削除します。
- [More Options]：TLS ハンドシェイク中に通知または照合する使用可能でアクティブなアルゴリズムを指定します。
  - [Parse the CTL file provided by the CTL Client and install trustpoints]：このオプションでインストールされたトラストポイントの名前には「_internal_CTL_」というプレフィックスがつきます。ディセーブルにした場合、各 CallManager サーバと CAPF 証明書を手動でインポートおよびインストールする必要があります。
  - [Port Number]：CTL プロバイダーがリッスンするポートを指定します。ポートは、クラスタの CallManager サーバがリッスンするポート（[CallManager administration] ページの [Enterprise Parameters] で設定されたもの）と同じである必要があります。デフォルト値は 2444 です。
  - [Authentication]：クライアントがプロバイダーの認証を受けるためのユーザ名とパスワードを指定します。

    [Username]：クライアントのユーザ名。

    [Password]：クライアントのパスワード。

    [Confirm Password]：クライアントのパスワード。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 9

セキュリティ コンテキストの設定

この章では、セキュリティ コンテキストの使用方法とマルチ コンテキスト モードをイネーブルにする方法について説明します。この章は、次の項で構成されています。

セキュリティ コンテキストの概要

1 台のセキュリティ アプライアンスを、セキュリティ コンテキストと呼ばれる複数の仮想デバイスに分割することができます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、多くの機能がサポートされます。VPN、ダイナミック ルーティング プロトコルなど、いくつかの機能はサポートされません。

マルチ コンテキスト モードの場合、セキュリティ アプライアンス には、セキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイスで設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者は、システム コンフィギュレーションに設定することでコンテキストを追加および管理します。このコンフィギュレーションは、シングル モードのコンフィギュレーション同様、スタートアップ コンフィギュレーションです。システム コンフィギュレーションは、セキュリティ アプライアンス の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

この項では、セキュリティ コンテキストの概要について説明します。次の項目を取り上げます。

- 「セキュリティ コンテキストへの管理アクセス」（P.9-9）

セキュリティ コンテキストの一般的な使用方法

マルチセキュリティ コンテキストを使用する状況には次のようなものがあります。

- サービス プロバイダーとして、多数のカスタマーにセキュリティ サービスを販売する。セキュリティ アプライアンス上でマルチセキュリティ コンテキストをイネーブルにすることによって、費用対効果の高い、省スペース ソリューションを実装できます。このソリューションでは、カスタマーのトラフィックすべての分離とセキュリティが確保され、設定も容易です。
- 大企業または広大な大学の構内で、各部門の完全な独立を維持する必要がある。
- 企業で、部門ごとに個別のセキュリティ ポリシーの提供が求められている。
- 複数のセキュリティ アプライアンスが必要なネットワークを使用している。

サポートされていない機能

マルチ コンテキスト モードでサポートされていない機能は、次のとおりです。

- ダイナミック ルーティング プロトコル

  セキュリティ コンテキストは、スタティック ルートのみサポートします。マルチコンテキスト モードで OSPF または Routing Information Protocol（RIP）をイネーブルにすることはできません。
- VPN
- マルチキャスト ルーティング。マルチキャスト ブリッジはサポートされています。
- 脅威の検出

コンテキスト コンフィギュレーション ファイル

それぞれのコンテキストにコンフィギュレーション ファイルがあり、セキュリティ ポリシーおよびインターフェイスが指定されます。サポートされる機能のオプションはすべて、スタンドアロン装置で設定できます。コンテキスト コンフィギュレーションは、内部フラッシュ メモリまたは外部フラッシュ メモリ カードに保存することも、TFTP サーバ、FTP サーバ、または HTTP（S）サーバからダウンロードすることもできます。

セキュリティ アプライアンスには、個別のセキュリティ コンテキストだけでなく、コンテキストのリストなどセキュリティ アプライアンスの基本設定を識別するシステム コンフィギュレーションが含まれています。シングル モード コンフィギュレーションと同様、このコンフィギュレーションもスタートアップ コンフィギュレーションに常駐しています。

システム コンフィギュレーションには、自分自身のネットワーク インターフェイスまたはネットワーク設定は含まれません。システムがネットワーク リソースにアクセスする必要が生じたとき（サーバからコンテキストをダウンロードするときなど）は、管理コンテキストとして指定されたコンテキストのいずれかを使用します。システム コンフィギュレーションに含まれているものに、フェールオーバー トラフィック専用の特殊なフェールオーバー インターフェイスがあります。システムがすでにマルチコンテキスト モードになっている場合、またはシングルモードから変換された場合、管理コンテキストが admin.cfg と呼ばれるファイルとして内部フラッシュ メモリに自動的に作成されます。このコンテキストは「admin」と名付けられます。admin.cfg を管理コンテキストとして使用しない場合は、管理コンテキストを変更できます。

セキュリティ アプライアンスによるパケットの分類方法

セキュリティ アプライアンスに入ってくるパケットはいずれも分類する必要があります。その結果、セキュリティ アプライアンスは、どのコンテキストにパケットを送信するかを決定できます。この項では、次のトピックについて取り上げます。

（注）　宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製され、各コンテキストに送信されます。

有効な分類子の基準

この項では、分類子で使用される基準について説明します。次の項目を取り上げます。

固有のインターフェイス

入力インターフェイスに関連付けられているコンテキストが 1 つだけの場合、セキュリティ アプライアンスはパケットをそのコンテキストに分類します。トランスペアレント ファイアウォール モードでは、各コンテキストに固有のインターフェイスが必要なため、この方法は、常にパケット分類の目的で使用されます。

固有の MAC アドレス

マルチ コンテキストがインターフェイスを共有している場合、分類子はインターフェイス MAC アドレスを使用します。セキュリティ アプライアンスでは、各コンテキストで異なる MAC アドレスを同一の共有インターフェイス（共有物理インターフェイスまたは共有サブインターフェイス）に割り当てることができます。デフォルトでは、共有インターフェイスには固有の MAC アドレスがありません。インターフェイスは、すべてのコンテキストの物理インターフェイスの焼き付け済み MAC アドレスを使用します。固有の MAC アドレスがないと、アップストリーム ルータはコンテキストに直接ルーティングできません。それぞれのインターフェイスを設定するときに、手動で MAC アドレスを設定できます（[Add/Edit Interface] > [Advanced] を参照）。または、自動的に MAC アドレスを生成することもできます（セキュリティ コンテキストを参照）。

NAT コンフィギュレーション

固有の MAC アドレスがない場合、分類子はパケットを代行受信し、宛先 IP アドレス ルックアップを実行します。その他のすべてのフィールドは無視され、宛先 IP アドレスだけが使用されます。分類に宛先アドレスを使用するには、分類子が、各セキュリティ コンテキストの背後にあるサブネットを認識できる必要があります。分類子は、Network Address Translation（NAT; ネットワーク アドレス変換）コンフィギュレーションに基づいて各コンテキストのサブネットを判別します。分類子は、宛先 IP アドレスを **static** コマンドまたは **global** コマンドのいずれかと照合します。**global** コマンドの場

合、分類子は、**nat** コマンドまたはアクティブな NAT セッションを照合してパケットを分類する必要がありません。分類後にパケットが宛先 IP アドレスと通信ができるかどうかは、NAT および NAT 制御の設定方法によります。

たとえば、コンテキスト管理者が各コンテキストの **static** コマンドを次のように設定した場合、分類子はサブネット 10.10.10.0、10.20.10.0、および 10.30.10.0 を認識します。

- コンテキスト A：

```
static (inside,shared) 10.10.10.0 10.10.10.0 netmask 255.255.255.0
```

- コンテキスト B：

```
static (inside,shared) 10.20.10.0 10.20.10.0 netmask 255.255.255.0
```

- コンテキスト C：

```
static (inside,shared) 10.30.10.0 10.30.10.0 netmask 255.255.255.0
```

（注） インターフェイス宛の管理トラフィックでは、インターフェイス IP アドレスが分類に使用されます。

無効な分類子の基準

次のコンフィギュレーションは、パケットの分類に使用されません。

- NAT 免除：分類子は、分類の目的では NAT 免除コンフィギュレーションは使用しません。これは、NAT 免除がマッピング インターフェイスを識別しないためです。
- ルーティング テーブル：コンテキストに、あるサブネットへのネクストホップとして外部ルータをポイントするスタティック ルートが含まれており、別のコンテキストに、同じサブネットに対する **static** コマンドが含まれている場合、分類子は **static** コマンドを使用してそのサブネットを宛先とするパケットを分類し、スタティック ルートを無視します。

分類の例

図 9-1 に、外部インターフェイスを共有するマルチ コンテキストを示します。コンテキスト B にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをコンテキスト B に割り当てます。

図 9-1　MAC アドレスを使用した共有インターフェイスを持つパケット分類

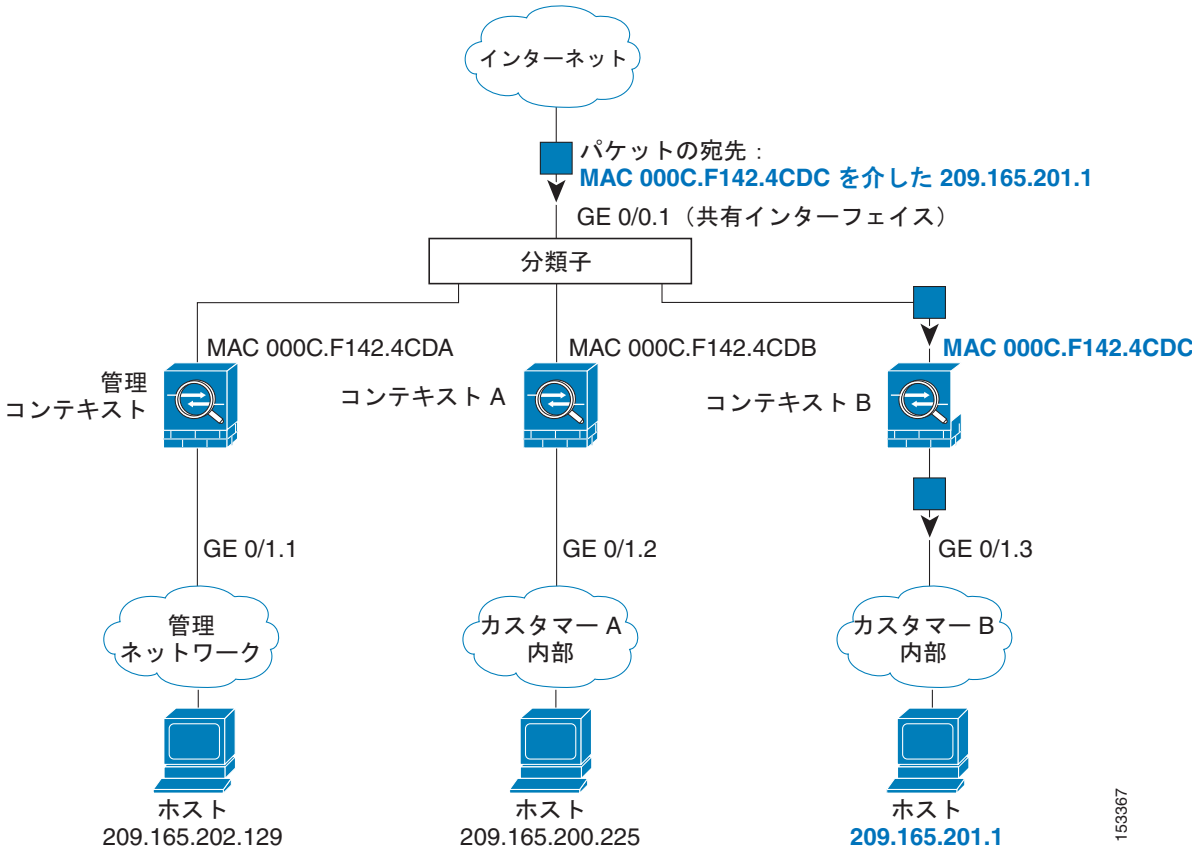
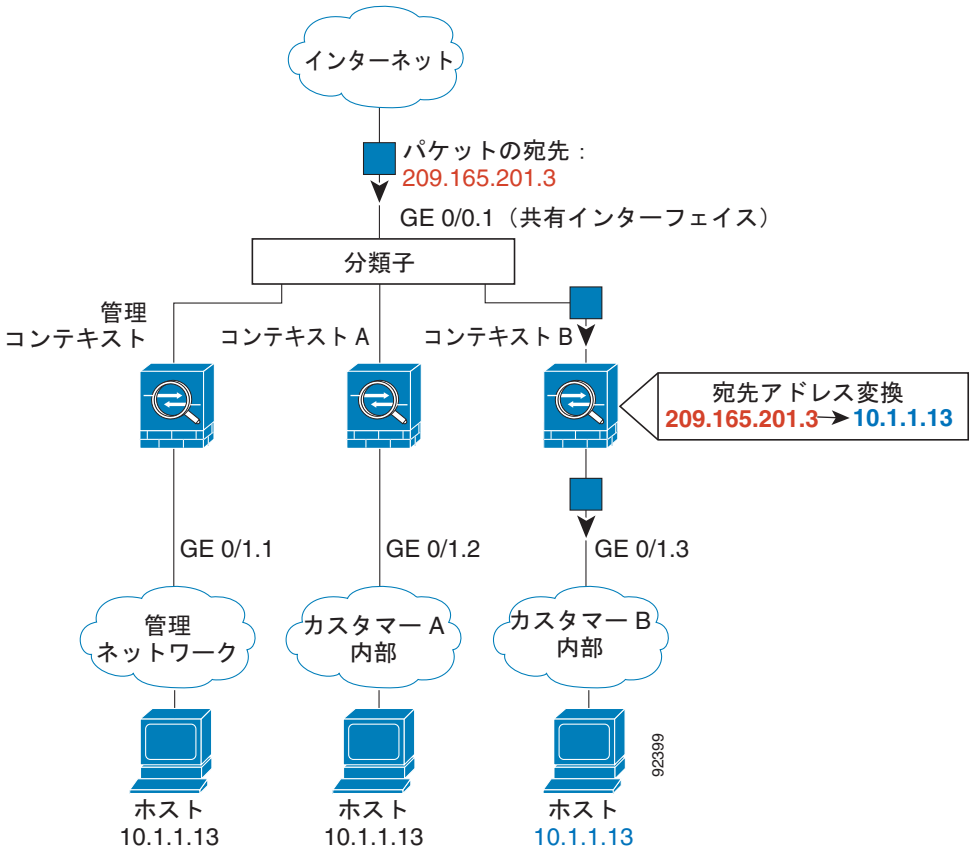


図 9-2 に、MAC アドレスが割り当てられていない外部インターフェイスを共有するマルチコンテキストを示します。コンテキスト B には宛先アドレスに一致するアドレス変換が含まれるため、分類子はパケットをコンテキスト B に割り当てます。

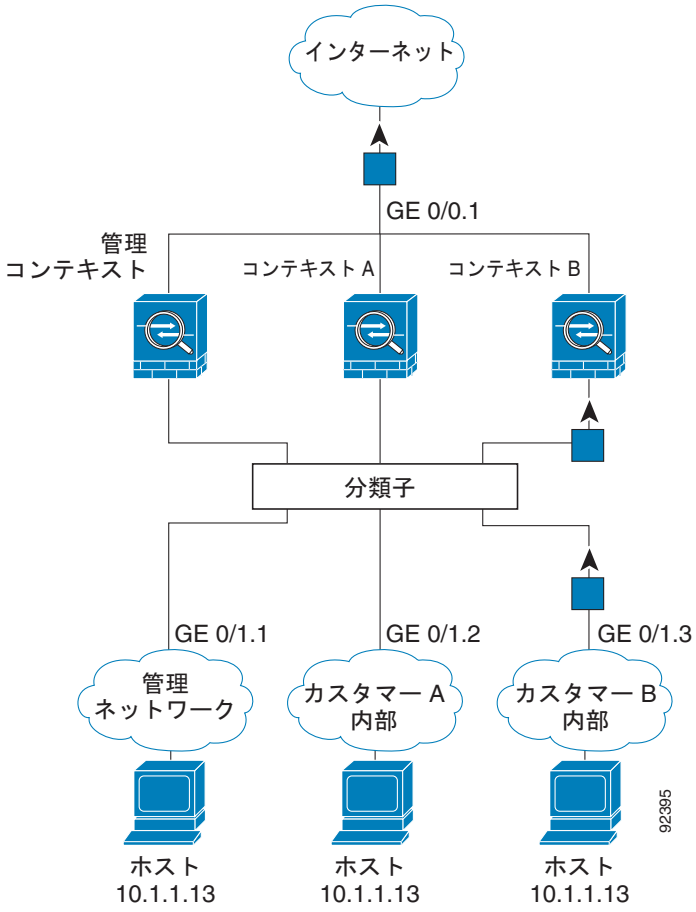
図 9-2　NAT を使用した共有インターフェイスを持つパケット分類



内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。図 9-3 に、内部ネットワークのコンテキスト B 上のホストがインターネットにアクセスしている場合を示します。分類子は、パケットをコンテキスト B に割り当てます。これは、入力インターフェイスがギガビット イーサネット 0/1.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

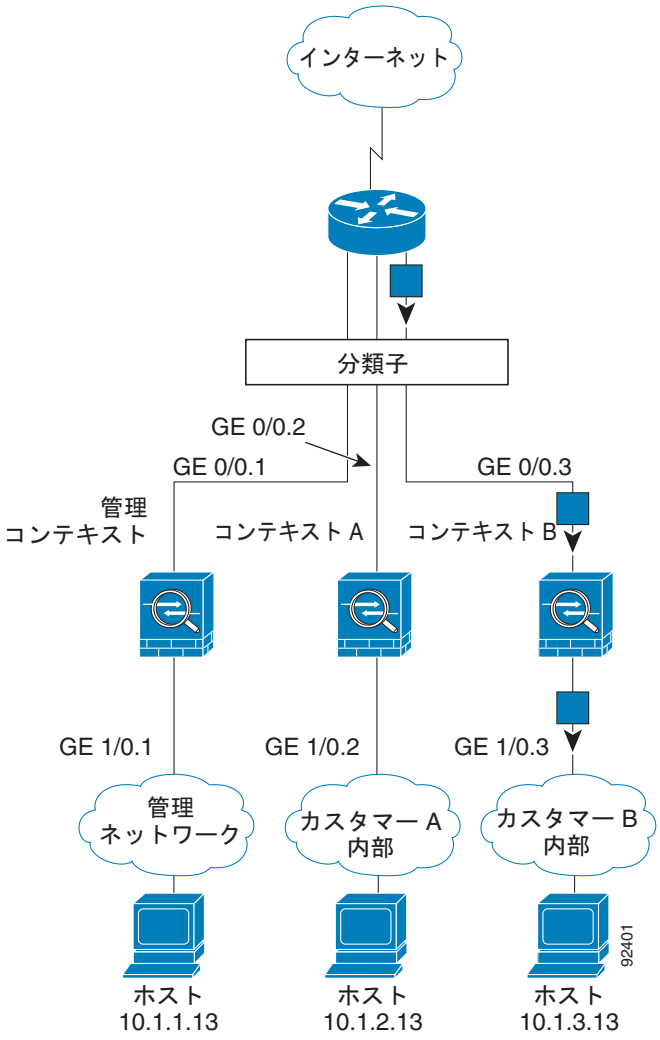
（注）　*内部*インターフェイスを共有し、固有の MAC アドレスを使用していない場合、分類子には重要な制限事項がいくつかあります。分類子は、アドレス変換コンフィギュレーションに基づいてコンテキスト内のパケットを分類します。そのトラフィックの*宛先*アドレスを変換する必要があります。通常は外部アドレスに対して NAT を実行しないため、パケットを共有インターフェイスの内部から外部へ送信できない場合もあります。これは、Web のように巨大な外部ネットワークで、外部 NAT コンフィギュレーションのアドレスを予測できないためです。内部インターフェイスを共有する場合、固有の MAC アドレスを使用することをお勧めします。

図 9-3　内部ネットワークからの着信トラフィック



トランスペアレント ファイアウォールでは、固有のインターフェイスを使用する必要があります。図 9-4 に、内部ネットワークのコンテキスト B 上のホストがインターネットにアクセスしている場合を示します。分類子は、パケットをコンテキスト B に割り当てます。これは、入力インターフェイスがギガビット イーサネット 1/0.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 9-4　トランスペアレント ファイアウォールのコンテキスト



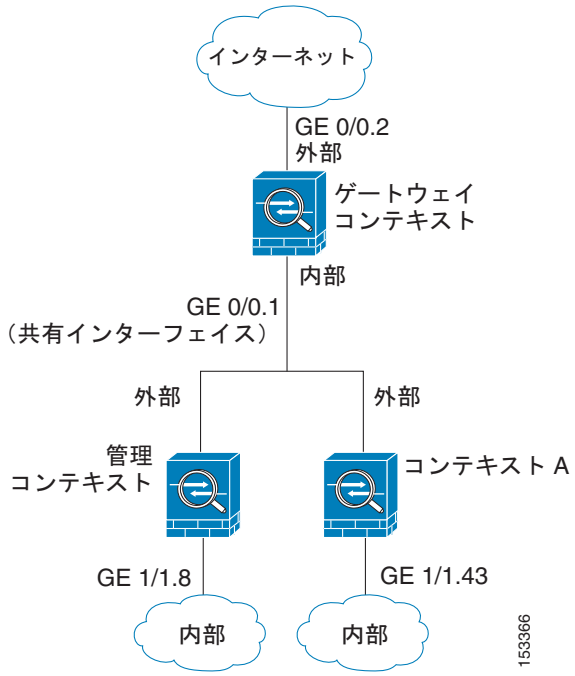
セキュリティ コンテキストのカスケード接続

コンテキストを別のコンテキストの前に置くことを、コンテキストをカスケード接続するといいます。あるコンテキストの外部インターフェイスは、別のコンテキストの内部インターフェイスと同じインターフェイスです。いくつかのコンテキストのコンフィギュレーションを単純化する場合、最上位のコンテキストの共有パラメータを設定することで、コンテキストをカスケード接続できます。

（注）　コンテキストをカスケード接続するには、各コンテキスト インターフェイスに固有の MAC アドレスを設定する必要があります。MAC アドレスのない共有インターフェイスのパケットを分類するには限界があるため、固有の MAC アドレスを設定しないでコンテキストのカスケード接続を使用することはお勧めしません。

図 9-5 に、ゲートウェイの背後に 2 つのコンテキストがあるゲートウェイ コンテキストを示します。

図 9-5　コンテキストのカスケード接続



セキュリティ コンテキストへの管理アクセス

セキュリティ アプライアンスでは、マルチ コンテキスト モードでのシステム管理アクセスと、各コンテキスト管理者のアクセスを提供します。次の各項では、システム管理者またはコンテキスト管理者としてのログインについて説明します。

- 「システム管理者のアクセス」（P.9-10）
- 「コンテキスト管理者のアクセス」（P.9-10）

システム管理者のアクセス

セキュリティ アプライアンスにシステム管理者としてアクセスするには、次の 2 つの方法があります。

- セキュリティ アプライアンス コンソールにアクセスする

  コンソールからシステム実行スペースにアクセスします。

- Telnet、SSH、または ASDM を使用して管理コンテキストにアクセスする

  Telnet、SSH、および ASDM アクセスをイネーブルにする方法については、第 13 章「管理アクセスの設定」を参照してください。

システム管理者として、すべてのコンテキストにアクセスできます。

管理またはシステム コンテキストから特定のコンテキストに変更すると、ユーザ名がデフォルトの「enable_15」ユーザ名に変更されます。そのコンテキストでコマンド許可を設定した場合は、「enable_15」というユーザの許可特権を設定するか、またはコンテキストのコマンド許可コンフィギュレーションで十分な特権を与えられる別の名前でログインできます。ユーザ名でログインするには、**login** コマンドを入力します。たとえば、「admin」というユーザ名で管理コンテキストにログインします。管理コンテキストにコマンド許可コンフィギュレーションはありませんが、それ以外のすべてのコンテキストにはコマンド許可があります。便宜を図るために、各コンテキスト コンフィギュレーションには、最大特権を持つ「admin」ユーザが含まれています。管理コンテキストからコンテキスト A に変更したら、ユーザ名が変わるため、**login** コマンドを入力して再度「admin」でログインする必要があります。コンテキスト B に変更したときは、再度 **login** コマンドを入力して「admin」としてログインする必要があります。

システム実行スペースでは AAA コマンドはサポートされていませんが、個別のログインのために、固有のイネーブル パスワードおよびユーザ名をローカル データベースに設定することができます。

コンテキスト管理者のアクセス

Telnet、SSH、または ASDM を使用して、コンテキストにアクセスできます。管理外コンテキストにログインすると、アクセスできるのはそのコンテキストのコンフィギュレーションだけになります。そのコンテキストに個別のログインを付与できます。Telnet、SSH、および SDM アクセスをイネーブルにして管理認証を設定するには、第 13 章「管理アクセスの設定」を参照してください。

CLI でのマルチ コンテキスト モードのイネーブル化またはディセーブル化

シスコへの発注方法によっては、セキュリティ アプライアンスがすでにマルチセキュリティ コンテキスト用に設定されている場合があります。ただし、アップグレードする場合は、この項で説明する手順に従ってシングル モードからマルチ モードに変換することが必要になる場合があります。

ASDM では、High Availability and Scalability Wizard を使用し、Active/Active フェールオーバーをイネーブルにした場合、シングル モードからマルチ モードへの変更をサポートします。詳細については、「High Availability and Scalability Wizard へのアクセスと使用」（P.14-5）を参照してください。

Active/Active フェールオーバーを使用しない場合、またはシングル モードに戻す場合は、CLI でモードを変更する必要があります。この項では、CLI でのモード変更について説明します。説明する内容は次のとおりです。

この項では、次のトピックについて取り上げます。

- 「シングルコンテキスト モードの復元」（P.9-11）

シングル モード コンフィギュレーションのバックアップ

シングル モードからマルチ モードに変換すると、セキュリティ アプライアンスは実行コンフィギュレーションを 2 つのファイルに変換します。元のスタートアップ コンフィギュレーションは保存されないため、実行コンフィギュレーションと異なる場合は、手順を進める前にバックアップを取る必要があります。

マルチ コンテキスト モードのイネーブル化

コンテキスト モード（シングルまたはマルチ）は、リブートされても持続されますが、コンフィギュレーション ファイルには保存されません。コンフィギュレーションを別のデバイスにコピーする必要がある場合は、**mode** コマンドを使用して、新規デバイスのモードを match に設定します。

シングル モードからマルチ モードに変換すると、セキュリティ アプライアンスは実行コンフィギュレーションを 2 つのファイルに変換します。システム コンフィギュレーションで構成される新規スタートアップ コンフィギュレーションと、（内部フラッシュ メモリのルート ディレクトリの）管理コンテキストで構成される admin.cfg です。元の実行コンフィギュレーションは、old_running.cfg（内部フラッシュ メモリのルート ディレクトリ内）として保存されます。元のスタートアップ コンフィギュレーションは保存されません。セキュリティ アプライアンスは、管理コンテキストのエントリをシステム コンフィギュレーションに「admin」という名前で自動的に追加します。

マルチモードをイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# mode multiple
```

セキュリティ アプライアンス をリブートするよう求められます。

シングルコンテキスト モードの復元

マルチ モードからシングル モードに変換する場合は、先にスタートアップ コンフィギュレーション全体（使用可能な場合）をセキュリティ アプライアンスにコピーすることを推奨します。マルチ モードから継承されるシステム コンフィギュレーションは、シングル モード デバイスで完全に機能するコンフィギュレーションではありません。システム コンフィギュレーションは、自身のコンフィギュレーションの一部としてネットワーク インターフェイスを持たないため、コンソールからセキュリティ アプライアンスにアクセスしてコピーをとる必要があります。

以前の実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてモードをシングルモードに変更するには、システム実行スペースで次の手順を実行します。

ステップ 1　元の実行コンフィギュレーションのバックアップ バージョンを現在のスタートアップ コンフィギュレーションにコピーするには、システムの実行スペースで次のコマンドを入力します。

```
hostname(config)# copy flash:old_running.cfg startup-config
```

（注）　現在実行中のコンフィギュレーションを保存しないように注意してください。保存するとコピーしたコンフィギュレーションが上書きされます。

ステップ 2　モードをシングルモードに設定するには、システム実行スペースで次のコマンドを入力します。

```
hostname(config)# mode single
```

セキュリティ アプライアンス がリブートします。

リソース クラスの設定

デフォルトでは、すべてのセキュリティ コンテキストは、コンテキストあたりの最大制限が適用されている場合を除いて、セキュリティ アプライアンスのリソースに無制限にアクセスできます。ただし、1 つ以上のコンテキストがリソースを大量に使用しており、他のコンテキストが接続を拒否されている場合は、リソース管理を設定してコンテキストごとのリソースの使用を制限できます。

この項では、次のトピックについて取り上げます。

クラスおよびクラス メンバーの概要

セキュリティ アプライアンスでは、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。この項では、次のトピックについて取り上げます。

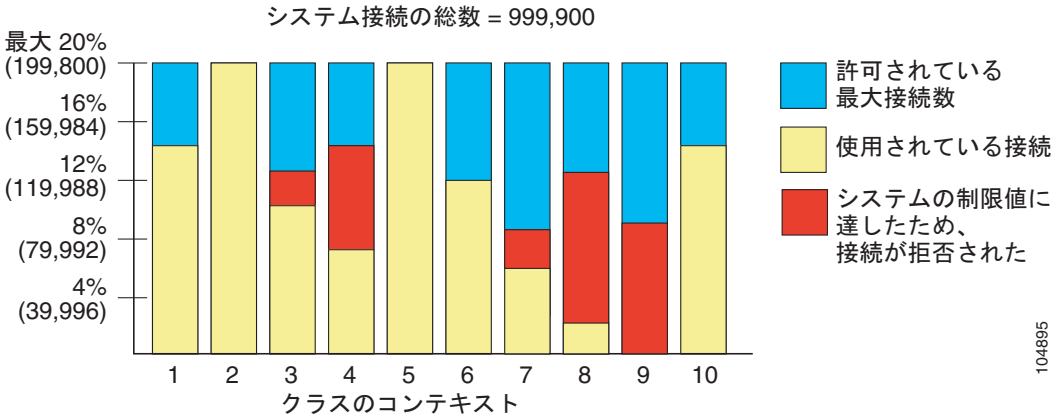
リソース制限

クラスを作成すると、セキュリティ アプライアンスは、クラスに割り当てられる各コンテキストに対してリソースの一部を確保しなくなります。その代わりに、セキュリティ アプライアンスは、コンテキストの上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。

個々のリソースには、割合（ハードウェアのシステム制限がある場合）または絶対値で制限を設定できます。

コンテキスト全体に渡って 100% を超えるリソースを割り当てることにより、セキュリティ アプライアンスをオーバーサブスクライブすることができます。たとえば、接続がコンテキストあたり 20% までに制限されるように Bronze クラスを設定し、それから 10 個のコンテキストをそのクラスに割り当てれば、リソースの合計を 200% にできます。コンテキストがシステム制限を超えて同時に使用する場合、各コンテキストは意図した 20% を下回ります。（図 9-6 を参照）。

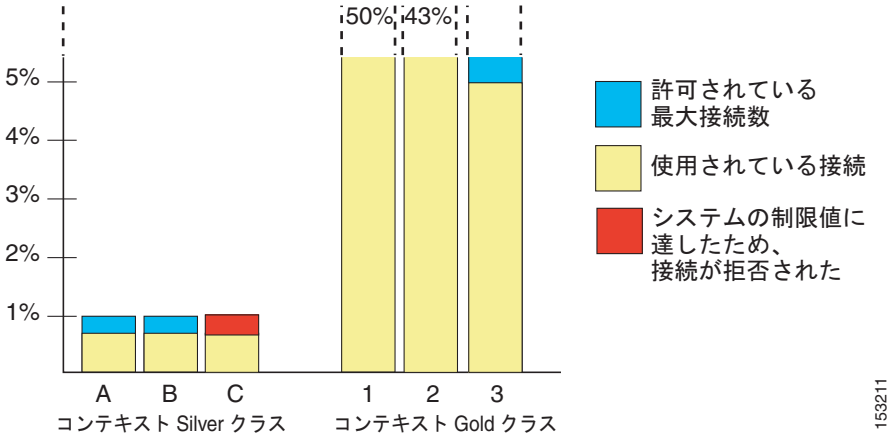
図 9-6　リソースのオーバーサブスクライブ



コンテキスト全体に渡って、セキュリティ アプライアンスの実際の制限を超える絶対値をリソースに割り当てると、セキュリティ アプライアンスのパフォーマンスが低下する場合があります。

セキュリティ アプライアンスでは、割合や絶対値ではなく、クラス内の 1 つ以上のリソースへの無制限アクセスを割り当てることができます。リソースに制限がない場合、コンテキストは、システムに存在する（実際に使用可能な）だけのリソースを使用できます。たとえば、コンテキスト A、B、C が Silver クラスに属しており、クラスの各メンバの使用量が接続の 1% に制限されていて、合計 3% が割り当てられているが、3 つのコンテキストが現在使用しているのは合計 2% だけだとします。Gold クラスは、接続に無制限にアクセスできます。Gold クラスのコンテキストは、「未割り当て」接続のうち 97% を超える分も使用できます。つまり、現在コンテキスト A、B、C で使用されていない、接続の 1% も使用できます。その場合は、コンテキスト A、B、C の使用量が、この 3 つの制限の合計である 3% に達することは不可能になります。（図 9-7 を参照）。無制限アクセスの設定は、システムのオーバーサブスクライブ量を制御する機能が劣る点を除いて、セキュリティ アプライアンスのオーバーサブスクライブに類似しています。

図 9-7　無制限リソース



デフォルト クラス

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルト クラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

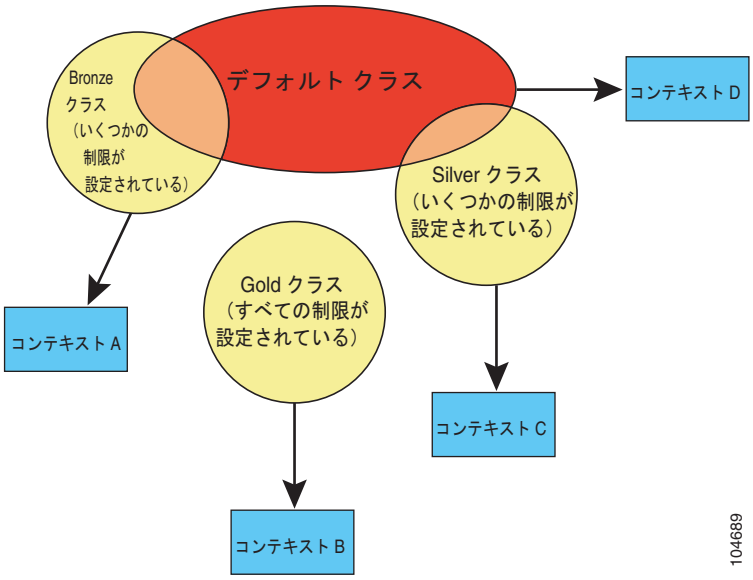
コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルト クラスから継承されます。これとは逆に、すべてのリソースに対する制限値を設定してクラスを作成すると、そのクラスではデフォルト クラスの設定を何も使用しません。

デフォルトでは、デフォルト クラスは、すべてのコンテキストにリソースへのアクセスを無制限に提供します。ただし、次の制限が適用されます（この制限は、デフォルトではコンテキストあたりの最大許容値が設定されます）。

- Telnet セッション：5 セッション。
- SSH セッション：5 セッション。
- IPSec セッション：5 セッション。
- MAC アドレス：65,535 エントリ。

図 9-8 に、デフォルト クラスと他のクラスの関係を示します。コンテキスト A および C は、いくつかの制限が設定されたクラスに属しており、それ以外の制限はデフォルト クラスから継承します。コンテキスト B は、属している Gold クラスですべての制限が設定されているため、デフォルト クラスから制限値を継承しません。コンテキスト D はクラスに割り当てられなかったため、デフォルトでデフォルト クラスのメンバになります。

図 9-8　　リソース クラス



クラス メンバ

クラスの設定を使用するには、コンテキストを定義するときに、そのコンテキストをクラスに割り当てます。すべてのコンテキストは、別のクラスに割り当てられていなければ、デフォルト クラスに属します。したがって、コンテキストをデフォルト クラスに割り当てる必要は特にありません。コンテキストは 1 つのリソース クラスにだけ割り当てることができます。このルールの例外は、メンバ クラスで未定義の制限はデフォルト クラスから継承されることです。そのため実際には、コンテキストがデフォルト クラスおよび別のクラスのメンバになります。

リソース クラスの追加

リソース クラスを追加するには、次の手順を実行します。

ステップ 1　まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Resource Class] ペインで、[Add] をクリックします。

[Add Resource Class] ダイアログボックスが表示されます。

ステップ 3　[Resource Class] フィールドに、クラスの名前を 20 文字以内で入力します。

ステップ 4　[Count Limited Resources] 領域で、リソースの同時接続制限を設定します。

システム制限のないリソースは、パーセント（%）で設定できません。設定できるのは絶対値だけです。制限を設定しない場合、デフォルト クラスの制限値が継承されます。制限値がデフォルト クラスにない場合は、リソースは無制限またはシステム制限値（使用できる場合）に設定されます。

次の制限から 1 つまたは複数を設定できます。

- [Hosts] : セキュリティ アプライアンスを通して同時に接続できるホスト数の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
- [Telnet] : Telnet 同時セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 100 です。
- [ASDM Sessions] : ASDM の同時セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 80 です。ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に存在するモニタリング用の接続、もう 1 つは変更時にのみ存在するコンフィギュレーション変更用の接続です。たとえば、ASDM セッション数のシステム制限値が 32 の場合は、すべてのコンテキストで HTTPS セッション数が 64 で制限されます。
- [Connections] : TCP または UDP で同時接続する、任意の 2 つのホスト間の接続数の制限値を設定します。これには、1 台のホストと他の複数台のホストとの接続も含まれます。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合、0（システム制限値）と使用するモデルのシステム制限値の範囲で整数を入力し、リストの [Absolute] をクリックします。使用するモデルの接続制限については、『*Cisco ASDM Release Notes*』を参照してください。
- [Xlates] : アドレス変換の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
- [SSH] : SSH セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り

当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 100 です。

- [MAC Entries]：（トランスペアレント モードの場合だけ）MAC アドレス テーブルに登録できる MAC アドレス エントリの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、0（システム制限値）～ 65535 の範囲で整数を入力し、リストの [Absolute] をクリックします。

ステップ 5　[Rate Limited Resources] 領域で、リソースのレート制限を設定します。

制限を設定しない場合、デフォルト クラスの制限値が継承されます。制限値がデフォルト クラスにない場合は、デフォルトでは無制限になります。

次の制限から 1 つまたは複数を設定できます。

- [Conns/sec]：接続数 / 秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
- [Syslogs/sec]：システム ログ メッセージ数 / 秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
- [Inspects/sec]：アプリケーション インスペクション数 / 秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。

ステップ 6　[OK] をクリックします。

コンテキスト リソースの使用状況のモニタ

システム実行スペースからすべてのコンテキストのリソース使用状況を監視するには、次の手順を実行します。

ステップ 1　まだシステム モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　ツールバーの [Monitoring] ボタンをクリックします。

ステップ 3　[Context Resource Usage] をクリックします。

すべてのコンテキストのリソース使用状況を表示するには、次の各リソース タイプをクリックします。

- [ASDM]：ASDM 接続の使用状況を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Existing Connections (#)]：既存の接続の数を表示します。
  - [Existing Connections (%)]：このコンテキストで使用されている接続数を、すべてのコンテキストで使用されている接続の総数のパーセントとして表示します。
  - [Peak Connections (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク接続数を表示します。
- [Telnet]：Telnet 接続の使用状況を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Existing Connections (#)]：既存の接続の数を表示します。

  - [Existing Connections (%)]：このコンテキストで使用されている接続数を、すべてのコンテキストで使用されている接続の総数のパーセントとして表示します。
  - [Peak Connections (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク接続数を表示します。
- [SSH]：SSH 接続の使用状況を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Existing Connections (#)]：既存の接続の数を表示します。
  - [Existing Connections (%)]：このコンテキストで使用されている接続数を、すべてのコンテキストで使用されている接続の総数のパーセントとして表示します。
  - [Peak Connections (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク接続数を表示します。
- [Xlates]：ネットワーク アドレス変換の使用状況を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Xlates (#)]：現在の xlate の数を表示します。
  - [Xlates (%)]：このコンテキストで使用されている xlate 数を、すべてのコンテキストで使用されている xlate の総数のパーセントとして表示します。
  - [Peak (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク xlate 数を表示します。
- [NATs]：NAT ルールの数を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [NATs (#)]：現在の NAT ルールの数を表示します。
  - [NATs (%)]：このコンテキストで使用されている NAT ルール数を、すべてのコンテキストで使用されている NAT ルールの総数のパーセントとして表示します。
  - [Peak NATs (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク NAT ルール数を表示します。
- [Syslogs]：システム ログ メッセージのレートを表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Syslog Rate (#/sec)]：システム ログ メッセージの現在のレートを表示します。
  - [Syslog Rate (%)]：このコンテキストで生成されたシステム ログ メッセージ数を、すべてのコンテキストで生成されたシステム ログ メッセージの総数のパーセントとして表示します。
  - [Peak Syslog Rate (#/sec)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のシステム ログ メッセージのピーク レートを表示します。

ステップ 4　表示をリフレッシュするには、[Refresh] をクリックします。

[Resource Class] フィールドの説明

この項では、[Resource Class] 画面のフィールドについて説明します。次の項目を取り上げます。

- 「Resource Class」（P.9-18）
- 「Add/Edit Resource Class」（P.9-18）

Resource Class

[Resource Class] ペインには、設定されているクラスと各クラスの情報を示します。クラスを追加、編集、または削除することもできます。

フィールド

- [Class]：クラス名を示します。
- [All Resources]：個別設定されていないすべてのリソース制限を示します。0 のみを使用でき、無制限を意味します。
- [Connections]：TCP または UDP で接続する、任意の 2 つのホスト間の接続数の制限値を示します。これには、1 台のホストと他の複数台のホストとの接続も含まれます。
- [Hosts]：セキュリティ アプライアンスを通して接続できるホスト数の制限値を示します。
- [Xlates]：アドレス変換の制限値を示します。
- [Telnet]：Telnet セッション数の制限値を示します。デフォルトは 5 です。
- [SSH]：SSH セッション数の制限値を示します。デフォルトは 5 です。
- [ASDM Sessions]：ASDM 管理セッション数の制限値を示します。デフォルトは 5 です。ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に存在するモニタリング用の接続、もう 1 つは変更時にのみ存在するコンフィギュレーション変更用の接続です。たとえば、ASDM セッション数のシステム制限値が 32 の場合は、すべてのコンテキストで HTTPS セッション数が 64 で制限されます。
- [MAC]：トランスペアレント ファイアウォール モードで MAC アドレス テーブルに登録できる MAC アドレス数の制限値を示します。デフォルトは 65535 です。
- [Conns/sec]：接続数/秒の制限値を示します。
- [Fixups/sec]：アプリケーション インスペクション数/秒の制限値を示します。
- [Syslogs/sec]：システム ログ メッセージ数/秒の制限値を示します。
- [Contexts]：このクラスに割り当てられたコンテキストを示します。
- [Add]：クラスを追加します。
- [Edit]：クラスを編集します。
- [Delete]：クラスを削除します。デフォルト クラスは削除できません。コンテキストが割り当てられているクラスを削除すると、コンテキストはデフォルト クラスに戻ります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

Add/Edit Resource Class

[Add/Edit Resource Class] ダイアログボックスでは、リソース クラスを追加または編集できます。

フィールド

- [Resource Class]：クラス名を 20 文字以内で設定します。
- [Count Limited Resources]：リソースの同時接続制限を設定します。システム制限のないリソースは、パーセント（%）で設定できません。設定できるのは絶対値だけです。制限を設定しない場合、デフォルト クラスの制限値が継承されます。制限値がデフォルト クラスにない場合は、リソースは無制限またはシステム制限値（使用できる場合）に設定されます。
  - [Hosts]：セキュリティ アプライアンスを通して同時に接続できるホスト数の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
  - [Telnet]：Telnet 同時セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 100 です。
  - [ASDM Sessions]：ASDM の同時セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 80 です。ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に存在するモニタリング用の接続、もう 1 つは変更時にのみ存在するコンフィギュレーション変更用の接続です。たとえば、ASDM セッション数のシステム制限値が 32 の場合は、すべてのコンテキストで HTTPS セッション数が 64 で制限されます。
  - [Connections]：TCP または UDP で同時接続する、任意の 2 つのホスト間の接続数の制限値を設定します。これには、1 台のホストと他の複数台のホストとの接続も含まれます。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合、0（システム制限値）と使用するモデルのシステム制限値の範囲で整数を入力し、リストの [Absolute] をクリックします。使用するモデルの接続制限については、『*Cisco ASDM Release Notes*』を参照してください。
  - [Xlates]：アドレス変換の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
  - [SSH]：SSH セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 100 です。
  - [MAC Entries]：（トランスペアレント モードの場合だけ）MAC アドレス テーブルに登録できる MAC アドレス エントリの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、0（システム制限値）～ 65535 の範囲で整数を入力し、リストの [Absolute] をクリックします。
- [Rate Limited Resources]：リソースのレート制限を設定します。制限を設定しない場合、デフォルト クラスの制限値が継承されます。制限値がデフォルト クラスにない場合は、デフォルトでは無制限になります。

  - [Conns/sec]：接続数/秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
  - [Syslogs/sec]：システム ログ メッセージ数/秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
  - [Inspects/sec]：アプリケーション インスペクション数/秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
- [Show Actual Class Limits]：（デフォルト クラス以外の場合のみ）クラスを編集した場合、このボタンをクリックすると、設定した制限値と、設定しなかったがデフォルト クラスから継承された制限値が表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

セキュリティ コンテキストの設定

この項では、セキュリティ コンテキストを追加する方法について説明します。次の項目を取り上げます。

- 「セキュリティ コンテキストの追加」（P.9-20）
- 「MAC アドレスの自動割り当て」（P.9-22）
- 「[Security Context] フィールドの説明」（P.9-23）

セキュリティ コンテキストの追加

セキュリティ コンテキストを追加するには、次の手順を実行します。

ステップ 1　まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Security Contexts] ペインで、[Add] をクリックします。

[Add Context] ダイアログボックスが表示されます。

ステップ 3　[Security Context] フィールドに、コンテキストの名前を 32 文字以内の文字列で入力します。

コンテキスト名は、大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。

ステップ 4　[Interface Allocation] 領域で、[Add] ボタンをクリックし、コンテキストにインターフェイスを割り当てます。

ステップ 5　[Interfaces] > [Physical Interface] ドロップダウン リストからインターフェイスを選択します。

メイン インターフェイスを割り当てる場合、サブインターフェイス ID を空白にします。サブインターフェイスまたはその範囲を指定すると、このインターフェイスに設定されます。トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないインターフェイスだけが表示されます。メイン インターフェイスが他のコンテキストに割り当てられている場合、サブインターフェイスを選択する必要があります。

ステップ 6　（任意）[Interfaces] > [Subinterface Range] (optional) ドロップダウン リストで、サブインターフェイス ID を選択します。

サブインターフェイス ID の範囲を指定する場合、2 つ目のドロップダウン リストが有効であれば、そこから最後の ID を選択します。

トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないサブインターフェイスだけが表示されます。

ステップ 7　（任意）[Aliased Names] 領域で、[Use Aliased Name in Context] をオンにして、このインターフェイスに対して、コンテキスト コンフィギュレーションでインターフェイス ID の代わりに使用するエイリアス名を設定します。

a. [Name] フィールドに、エイリアス名を設定します。

エイリアス名の先頭および最後は英字にします。間の文字として使用できるのは、英字、数字、下線だけです。このフィールドで名前の最後を英字または下線にした場合、その名前の後に追加する数字を [Range] フィールドで設定できます。

b. （任意）[Range] フィールドで、エイリアス名のサフィックスを数字で設定します。

サブインターフェイスに範囲がある場合、範囲の数字を入力して名前の後に追加できます。

ステップ 8　（任意）エイリアス名を設定した場合でもコンテキスト ユーザが物理インターフェイスのプロパティを表示できるようにするには、[Show Hardware Properties in Context] をオンにします。

ステップ 9　[OK] をクリックして、[Add Context] ダイアログボックスに戻ります。

ステップ 10　（任意）IPS 仮想センサーを使用する場合、センサーを [IPS Sensor Allocation] 領域のコンテキストに割り当てます。

IPS および仮想センサーの詳細については、第 39 章「IPS の設定」を参照してください。

ステップ 11　（任意）このコンテキストをリソース クラスに割り当てるには、[Resource Assignment] > [Resource Class] ドロップダウン リストからクラス名を選択します。

この領域から直接リソース クラスを追加または編集できます。詳細については、「リソース クラスの設定」（P.9-12）を参照してください。

ステップ 12　コンテキスト コンフィギュレーションの場所を設定するには、[Config URL] ドロップダウン リストからファイル システム タイプを選択し、フィールドにパスを入力して URL を指定します。

FTP の場合、URL は次の形式になります。

ftp://server.example.com/configs/admin.cfg

ステップ 13　（任意）外部ファイルシステムの場合、[Login] をクリックしてユーザ名とパスワードを設定します。

ステップ 14　（任意）Active/Active フェールオーバーのフェールオーバー グループを設定するには、[Failover Group] ドロップダウン リストでグループ名を選択します。

ステップ 15　（任意）[Description] フィールドに説明を追加します。

MAC アドレスの自動割り当て

この項では、コンテキスト インターフェイスに一意の MAC アドレスを割り当てる方法について説明します。次の項目を取り上げます。

MAC アドレスの概要

コンテキストでインターフェイスを共有するには、一意の MAC アドレスを各コンテキストのインターフェイスに割り当てることをお勧めします。MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。インターフェイスを共有するものの、各コンテキストにインターフェイスの固有の MAC アドレスがない場合は、宛先 IP アドレスがパケットの分類に使用されます。宛先アドレスは、コンテキスト NAT コンフィギュレーションと照合されます。この方法には、MAC アドレスの方法に比べるといくつか制限があります。パケットの分類の詳細については、「セキュリティ アプライアンスによるパケットの分類方法」（P.9-3）を参照してください。

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

フェールオーバーで使用できるように、セキュリティ アプライアンスはインターフェイスごとにアクティブとスタンバイの両方の MAC アドレスを生成します。アクティブ ユニットがフェールオーバーしてスタンバイ ユニットがアクティブになると、その新規アクティブ ユニットがアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。

インターフェイスをコンテキストに割り当てると、新しい MAC アドレスがただちに生成されます。コンテキスト インターフェイスの作成後にこのオプションをイネーブルにすると、その直後に、MAC アドレスがすべてのインターフェイス用に生成されます。このオプションをディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。

MAC アドレスは次の形式を使用して生成します。

- アクティブ ユニットの MAC アドレス：12*_slot.port_subid.contextid*.
- スタンバイ ユニットの MAC アドレス：02*_slot.port_subid.contextid*.

インターフェイス スロットがないプラットフォームの場合、スロットは常に 0 です。*port* はインターフェイス ポートです。*subid* は、表示不可能なサブインターフェイスの内部 ID です。*contextid* はコンテキストの内部 ID です。たとえば、ID 1 のコンテキスト内のインターフェイス GigabitEthernet 0/1.200 には、次の生成済み MAC アドレスがあります。サブインターフェイス 200 の内部 ID は 31 です。

- アクティブ：1200.0131.0001
- スタンバイ：0200.0131.0001

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。MAC アドレスの手動設定の詳細については、「インターフェイスの設定」（P.5-5）を参照してください。

MAC アドレス自動割り当てのイネーブル化

MAC アドレスの自動割り当てをイネーブルにするには、次の手順を実行します。

ステップ 1　まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Security Contexts] ペインで、[Mac-Address auto] をオンにします。

[Security Context] フィールドの説明

この項では、[Resource Class] 画面のフィールドについて説明します。次の項目を取り上げます。

- 「セキュリティ コンテキスト」（P.9-23）
- 「Add/Edit Context」（P.9-24）
- 「Add/Edit Interface Allocation」（P.9-26）

セキュリティ コンテキスト

フィールド

- [Context]：コンテキスト名を示します。
- [Interfaces]：コンテキストに割り当てられたインターフェイスおよびサブインターフェイスを示します。コンテキストで表示するインターフェイス名にエイリアスを割り当てると、エイリアス名がカッコ内に表示されます。サブインターフェイスの範囲を指定すると、先頭のインターフェイス番号と最後のインターフェイス番号の範囲がダッシュで示されます。
- [Resource]：各コンテキストのリソース クラスを示します。
- [Config URL]：コンテキスト コンフィギュレーションの場所を示します。
- [Group]：このコンテキストが属するフェールオーバー グループを示します。
- [Description]：コンテキストの説明を示します。
- [Add]：コンテキストを追加します。
- [Edit]：コンテキストを編集します。
- [Delete]：コンテキストを削除します。
- [Mac-Address auto]：プライベート MAC アドレスを各共有コンテキスト インターフェイスに自動的に割り当てます。

  コンテキストでインターフェイスを共有するには、一意の MAC アドレスを各コンテキストのインターフェイスに割り当てることをお勧めします。MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。インターフェイスを共有するものの、各コンテキストにインターフェイスの固有の MAC アドレスがない場合は、宛先 IP アドレスがパケットの分類に使用されます。宛先アドレスは、コンテキスト NAT コンフィギュレーションと照合されます。この方法には、MAC アドレスの方法に比べるといくつか制限があります。パケットの分類の詳細については、「セキュリティ アプライアンスによるパケットの分類方法」（P.9-3）を参照してください。

  デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

  フェールオーバーで使用できるように、セキュリティ アプライアンスはインターフェイスごとにアクティブとスタンバイの両方の MAC アドレスを生成します。アクティブ ユニットがフェールオーバーしてスタンバイ ユニットがアクティブになると、その新規アクティブ ユニットがアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。

インターフェイスをコンテキストに割り当てると、新しい MAC アドレスがただちに生成されます。コンテキスト インターフェイスの作成後にこのオプションをイネーブルにすると、その直後に、MAC アドレスがすべてのインターフェイス用に生成されます。このオプションをディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。

MAC アドレスは次の形式を使用して生成します。

アクティブ ユニットの MAC アドレス：12*_slot.port_subid.contextid*.

スタンバイ ユニットの MAC アドレス：02*_slot.port_subid.contextid*.

インターフェイス スロットがないプラットフォームの場合、スロットは常に 0 です。*port* はインターフェイス ポートです。*subid* は、表示不可能なサブインターフェイスの内部 ID です。*contextid* はコンテキストの内部 ID です。たとえば、ID 1 のコンテキスト内のインターフェイス GigabitEthernet 0/1.200 には、次の生成済み MAC アドレスがあります。サブインターフェイス 200 の内部 ID は 31 です。

アクティブ：1200.0131.0001

スタンバイ：0200.0131.0001

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。MAC アドレスの手動設定の詳細については、「インターフェイスの設定」（P.5-5）を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

Add/Edit Context

フィールド

- [Security Context]：コンテキスト名を 32 文字以内で設定します。コンテキスト名は、大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。
- [Interface Allocation]：コンテキストに割り当てられたインターフェイスおよびサブインターフェイスを示します。
  - [Interface]：インターフェイス ID を表示します。サブインターフェイスの範囲を指定すると、先頭のインターフェイス番号と最後のインターフェイス番号の範囲がダッシュで示されます。
  - [Aliased Name]：インターフェイス ID の代わりにコンテキスト コンフィギュレーションで使用できるインターフェイスのエイリアス名を示します。
  - [Visible]：エイリアス名が設定されている場合でも、コンテキスト ユーザが物理インターフェイスのプロパティを表示できるかどうかを示します。

  - [Add]：コンテキストにインターフェイスを追加します。
  - [Edit]：インターフェイス プロパティを編集します。
  - [Delete]：インターフェイスを削除します。
- [IPS Sensor Allocation]：各コンテキストに 1 つ以上の IPS 仮想センサーを割り当てることができます。次に、トラフィックを AIP SSM に送信するようコンテキストを設定する場合、コンテキストに割り当てられるセンサーを指定できます。コンテキストに割り当てなかったセンサーは指定できません。コンテキストにセンサーが割り当てられていない場合は、AIP SSM に設定されているデフォルト センサーが使用されます。同じセンサーを複数のコンテキストに割り当てることができます。詳細については、「仮想センサーの使用」（P.39-3）を参照してください。
  - [Sensor Name]：割り当てられているセンサーを示します。AIP SSM で使用できるセンサーのみを割り当てることができます。
  - [Mapped Sensor Name]：センサーのマッピング名を示します。このセンサー名は、コンテキスト内で実際のセンサー名の代わりに使用できます。マッピング名を指定しない場合、センサー名がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているセンサーをコンテキスト管理者に知らせない場合があります。または、コンテキスト コンフィギュレーションを一般化する場合もあります。たとえば、すべてのコンテキストで「sensor1」および「sensor2」というセンサーを使用する場合、コンテキスト A の sensor1 と sensor2 に「highsec」センサーと「lowsec」センサーをマッピングし、コンテキスト B の sensor1 と sensor2 に「medsec」センサーと「lowsec」センサーをマッピングできます。
  - [Add]：センサーを追加します。
  - [Delete]：センサーを削除します。
  - [Default Sensor]：セキュリティ コンテキストにデフォルト センサーを割り当てます。コンテキスト コンフィギュレーション内に IPS を設定するときにセンサー名を指定しない場合、コンテキストはデフォルト センサーを使用します。コンテキストごとに設定できるデフォルト センサーは 1 つのみです。センサーをデフォルトとして指定せず、コンテキスト コンフィギュレーションにセンサー名が含まれていない場合、トラフィックは AIP SSM のデフォルト センサーを使用します。
- [Resource Assignment]：コンテキストをリソース クラスに割り当てます。
  - [Resource Class]：リストからクラスを選択します。
  - [Edit]：選択されたリソース クラスを編集します。
  - [New]：リソース クラスを追加します。
- [Config URL]：URL としてコンテキスト コンフィギュレーションの場所を指定します。リストのファイル システム タイプを選択し、フィールドにサーバ（リモート ファイル システムの場合）、パス、およびファイル名を入力します。FTP の場合、URL は次の形式になります。

  ftp://server.example.com/configs/admin.cfg
- [Login]：リモート ファイル システムのユーザ名とパスワードを設定します。
- [Failover Group]：アクティブ/アクティブ フェールオーバーのフェールオーバー グループを設定します。
- [Description]：コンテキストのオプションの説明を設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

Add/Edit Interface Allocation

フィールド

- [Interfaces]：物理インターフェイスおよびサブインターフェイス ID を指定します。
  - [Physical Interface]：コンテキストに割り当てるように物理インターフェイスを設定します。メイン インターフェイスを割り当てる場合、サブインターフェイス ID を空白にします。サブインターフェイスまたはその範囲を指定すると、このインターフェイスに設定されます。トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないインターフェイスだけが表示されます。メイン インターフェイスが他のコンテキストに割り当てられている場合、サブインターフェイスを選択する必要があります。
  - [Sub Interface Range (Optional)]：サブインターフェイス ID またはサブインターフェイス ID の範囲を設定します。1 つのサブインターフェイスを指定するには、最初のリスト内の ID を選択します。範囲を指定するには、（使用可能な場合）2 つめのリスト内の最後の ID を選択します。トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないサブインターフェイスだけが表示されます。
- [Aliased Name]：インターフェイス ID の代わりにコンテキスト コンフィギュレーションで使用できるインターフェイスのエイリアス名を設定します。
  - [Use Aliased Name in Context]：コンテキストのエイリアス名をイネーブルにします。
  - [Name]：エイリアス名を設定します。エイリアス名の先頭および最後は英字にします。間の文字として使用できるのは、英字、数字、下線だけです。このフィールドで名前の最後を英字または下線にした場合、その名前の後に追加する数字を [Range] フィールドで設定できます。
  - [Range]：エイリアス名の数値のサフィックスを設定します。サブインターフェイスに範囲がある場合、範囲の数字を入力して名前の後に追加できます。
- [Show Hardware Properties in Context]：エイリアス名を設定した場合でも、コンテキスト ユーザが物理インターフェイスのプロパティを表示できるようにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

CHAPTER 10

デバイスの設定値と管理の設定

ここでは、次の内容について説明します。

管理 IP アドレス

[Management IP] ペインでは、セキュリティ アプライアンスの管理 IP アドレスまたはトランスペアレント ファイアウォール モードのコンテキストの管理 IP アドレスを設定できます。トランスペアレント ファイアウォールは、IP ルーティングに参加しません。セキュリティ アプライアンスで必要とされる唯一の IP コンフィギュレーションは、管理 IP アドレスです。例外として、Management 0/0 管理専用インターフェイスに IP アドレスを設定できますが、トラフィックはこのインターフェイスを通過できません。Management 0/0 の IP アドレスの設定については、「インターフェイスの設定」の章を参照してください。

このアドレスが必要になるのは、セキュリティ アプライアンスがシステム メッセージや AAA サーバとの通信などセキュリティ アプライアンスで発信されるトラフィックの送信元アドレスとしてこのアドレスを使用するためです。このアドレスは、リモート管理アクセスにも使用できます。

フィールド

- [Management IP Address]：管理 IP アドレスを設定します。
- [Subnet Mask]：サブネット マスクを設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

システム時刻

システムの日付または時刻を手動で設定するか、セキュリティ アプライアンスが NTP サーバを使用してシステムの日付と時刻を動的に設定するようにできます。

詳細については、次のトピックを参照してください。

- 「Clock」（P.10-2）
- 「NTP」（P.10-3）

Clock

[Clock] ペインでは、セキュリティ アプライアンスの日付と時刻を手動で設定できます。時刻は [ASDM] メイン ペインの下部にあるステータスバーに表示されます。

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

NTP サーバを使用して時刻を動的に設定する場合については、[NTP] ペインを確認してください。[Clock] ペインで手動設定した時刻は、NTP サーバから取得した時刻によって上書きされます。

フィールド

- [Time Zone]：適切な時差を GMT に加えた（または GMT から差し引いた）時間帯を設定します。[Eastern Time]、[Central Time]、[Mountain Time]、または [Pacific Time] ゾーンを選択すると、次の時間帯で、時間が自動的に夏時間に調整されます。3 月の第二日曜日の午前 2 時～11 月の第一日曜日の午前 2 時。

  （注）　セキュリティ アプライアンスの時間帯を変更すると、インテリジェント SSM との接続がドロップされる場合があります。

- [Date]：日付を設定します。[Date] ドロップダウン リストをクリックしてカレンダーを表示します。続いて、次の方法を使用して正しい日付に移動します。
  - 月の名前をクリックして、月のリストを表示します。設定する月をクリックします。カレンダーがその月に変わります。
  - 年をクリックして年を変更します。上矢印と下矢印を使用して複数年をスクロールすることも、入力フィールドに年を入力することもできます。
  - 年月表示の左右にある矢印をクリックすると、カレンダーが一度に 1 か月ずつ前後にスクロールします。
  - カレンダーの日にちをクリックして日を設定します。
- [Time]：時刻を 24 時間制で設定します。

  - [hh]、[mm]、[ss] の各ボックス：時、分、秒を設定します。
- [Update Display Time]：[ASDM] ペインの右下の表示時刻が更新されます。現在時刻は 10 秒ごとに自動更新されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

NTP

[NTP] ペインでは、セキュリティ アプライアンスで時刻を動的に設定するように NTP サーバを定義できます。時刻は [ASDM] メイン ペインの下部にあるステータスバーに表示されます。

[Clock] ペインで手動設定した時刻はすべて、NTP サーバから取得した時刻によって上書きされます。

NTP を利用して階層的なサーバ システムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。複数の NTP サーバを設定できます。セキュリティ アプライアンスは一番下の階層からサーバを選択し、データ信頼度の尺度にします。

フィールド

- [NTP Server List]：定義されている NTP サーバを示します。
  - [IP Address]：NTP サーバの IP アドレスを示します。
  - [Interface]：NTP パケットの発信インターフェイスを指定します（設定されている場合）。システムにインターフェイスがない場合、管理コンテキスト インターフェイスが使用されます。インターフェイスが空白の場合、セキュリティ アプライアンスが使用するデフォルトの管理コンテキスト インターフェイスは、ルーティング テーブルによって決まります。
  - [Preferred?]：この NTP サーバが優先サーバかどうかを [Yes] または [No] で示します。NTP では、どのサーバの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバに同期します。精度が同じ程度であれば、優先サーバを使用します。ただし、優先サーバよりも精度が大幅に高いサーバがある場合、セキュリティ アプライアンス では、精度の高いそのサーバを使用します。たとえば、セキュリティ アプライアンスはより精度の高いサーバを使用し、優先サーバの精度が低ければ使用しません。
  - [Key Number]：認証キーの ID 番号を示します。
  - [Trusted Key?]：キーが trusted key かどうかを [Yes] または [No] で示します。trusted key だけが認証されます。
- [Enable NTP Authentication]：すべてのサーバの認証をイネーブルにします。
- [Add]：NTP サーバを追加します。
- [Edit]：NTP サーバを編集します。
- [Delete]：NTP サーバを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Add/Edit NTP Server Configuration

[Add/Edit NTP Server Configuration] ダイアログボックスでは、NTP サーバを追加または編集できます。

フィールド

- [IP Address]：NTP サーバの IP アドレスを設定します。
- [Preferred]：このサーバを優先サーバに設定します。NTP では、どのサーバの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバに同期します。精度が同じ程度であれば、優先サーバを使用します。ただし、優先サーバよりも精度が大幅に高いサーバがある場合、セキュリティ アプライアンス では、精度の高いそのサーバを使用します。たとえば、セキュリティ アプライアンスはより精度の高いサーバを使用し、優先サーバの精度が低ければ使用しません。
- [Interface]：ルーティング テーブルに従ってデフォルト インターフェイスを無効にする場合は、NTP パケットの発信インターフェイスを設定します。システムにインターフェイスがない場合、管理コンテキスト インターフェイスが使用されます。管理コンテキスト（使用できるインターフェイス）を変更する場合は、安定性のために None（デフォルト インターフェイス）を選択してください。
- [Authentication Key]：NTP サーバとの通信に MD5 認証を使用する場合は、認証キーの属性を設定します。
  - [Key Number]：認証キーのキー ID を設定します。NTP サーバのパケットも、常にこのキー ID を使用する必要があります。以前に別のサーバに対してキー ID を設定した場合は、そのキー ID をリストから選択できます。それ以外の場合は、1 ～ 4294967295 の数字を入力します。
  - [Trusted]：このキーを trusted key として設定します。このチェックボックスをオンにしないと、認証されません。
  - [Key Value]：認証キーを 32 文字以内で設定します。
  - [Reenter Key Value]：正しいキーであることを確認するため、キーを再度入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

高度なデバイス管理機能の設定

次の各項では、[Advanced] メニューの項目を設定する方法について説明します。

HTTP リダイレクトの設定

HTTP Redirect テーブルには、セキュリティ アプライアンスの各インターフェイス、そのインターフェイスが HTTP 接続を HTTPS にリダイレクトするように設定されているかどうか、および接続のリダイレクトに使用するポート番号が表示されます。

（注） HTTP をリダイレクトするには、インターフェイスに HTTP を許可するアクセス リストが必要です。そうでないと、インターフェイスは HTTP ポートをリッスンできません。

インターフェイスの HTTP リダイレクト設定または HTTP 接続のリダイレクトに使用するポートを変更するには、テーブルでインターフェイスを選択し、[Edit] をクリックします。インターフェイスをダブルクリックすることもできます。[Edit HTTP/HTTPS Settings] ダイアログボックスが表示されます。

[Edit HTTP/HTTPS] ペインのフィールド

[Edit HTTP/HTTPS Settings] ダイアログボックスには、次のフィールドが表示されます。

- [Interface] : セキュリティ アプライアンスが HTTP 要求を HTTPS にリダイレクトする（またはしない）インターフェイスを示します。
- [Redirect HTTP to HTTPS] : HTTP 要求を HTTPS にリダイレクトするにはオンにし、リダイレクトしない場合はオフにします。
- [HTTP Port] : インターフェイスが HTTP 接続のリダイレクトに使用するポートを指定します。デフォルトでは、インターフェイスはポート 80 をリッスンします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Configuring Maximum SSL VPN Sessions

この画面では、SSL VPN セッションの最大数を設定できます。

フィールド

[Maximum Sessions] : 許可するクライアントレス SSL VPN セッションの最大数を入力します。ASA モデルが異なれば、サポートされるクライアントレス SSL VPN セッション数も異なることに注意してください。ASA 5510 は最大 250、ASA 5520 は同 750、ASA 5540 は同 2500、ASA 5550 は同 5000 です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

History Metrics

[History Metrics] ペインでは、さまざまな統計情報の履歴を保存するように適応型セキュリティ アプライアンスを設定し、ASDM を使用してグラフやテーブルで表示できます。履歴メトリックをイネーブルにしない場合、監視できるのはリアルタイムの統計情報だけです。履歴メトリックをイネーブルにすると、直前の 10 分間、60 分間、12 時間、5 日間の統計グラフを表示できます。

履歴メトリックを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Advanced] > [History Metrics] を選択します。

[History Metrics] ペインが表示されます。

ステップ 2　[ASDM History Metrics] チェックボックスをオンにして履歴メトリックをイネーブルにし、[Apply] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

System Image/Configuration

ここでは、次の内容について説明します。

- 「Activation Key」（P.10-7）
- 「Auto Update」（P.10-7）
- 「Boot Image/Configuration」（P.10-11）

Activation Key

[Activation Key] ペインでは、デバイスのシリアル番号と、実行コンフィギュレーションとフラッシュ メモリにあるアクティベーション キーを表示できます。このペインでアクティベーション キーを更新することもできます。

アクティベーション キーを更新するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [System Image/Configuration] > [Activation Key] に移動します。

ステップ 2　[New Activation Key] フィールドに新しいアクティベーション キーを入力します。アクティベーション キーは、4 つまたは 5 つの 16 進数文字列の要素で構成され、各要素の間に 1 つのスペースがあります。たとえば、次のようになります。

0x00000000 0x00000000 0x00000000 0x00000000

先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。キーはコンフィギュレーション ファイルに保存されず、シリアル番号に関連付けられます。

ステップ 3　[Update Activation Key] をクリックします。

Auto Update

[Auto Update] ペインでは、セキュリティ アプライアンスを、Auto Update 仕様をサポートするサーバによってリモートで管理されるように設定できます。Auto Update を利用すると、セキュリティ アプライアンスにコンフィギュレーションの変更を適用したり、離れた場所からソフトウェア アップデートを取得したりできます。

Auto Update は、セキュリティ アプライアンスの管理者が直面するさまざまな課題を解決できる便利な機能です。

- ダイナミック アドレッシングおよび NAT に関する問題点を解決します。
- 基本アクションのコンフィギュレーション変更を確実に反映します。
- 信頼度の高い方式でソフトウェアを更新します。
- 十分に実績のある方式を応用し、高い拡張性があります。
- オープン インターフェイスで、きわめて高い開発自由度があります。
- サービス プロバイダー環境のセキュリティ ソリューションに容易に対応できます。
- 高い信頼性と豊富なセキュリティ管理機能を、さまざまな製品により幅広くサポートします。

Auto Update の概要

Auto Update 仕様は、中央、または複数の場所から、リモート管理アプリケーションによりセキュリティ アプライアンスのコンフィギュレーションやソフトウェア イメージをダウンロードしたり、基本的な監視機能を実行したりする場合に必要なインフラストラクチャです。

Auto Update 仕様に従うことで、Auto Update サーバはセキュリティ アプライアンスにコンフィギュレーション情報をプッシュしたり、要求を送信して情報を取得したりできます。また、セキュリティ アプライアンスから Auto Update サーバへ定期的にポーリングさせ、最新のコンフィギュレーション情報を送ることもできます。また、Auto Update サーバはいつでもセキュリティ アプライアンスにコマン

ドを送信し、ただちにポーリング要求を送信させることもできます。Auto Update サーバとセキュリティ アプライアンスの通信では、通信パスとローカル CLI コンフィギュレーションをすべてのセキュリティ アプライアンスに設定する必要があります。

セキュリティ アプライアンスの Auto Update 機能は、シスコのセキュリティ製品と併用できますが、サード パーティ製品でセキュリティ アプライアンスを管理することもできます。

特記事項

- セキュリティ アプライアンスのコンフィギュレーションが Auto Update で更新されても、ASDM には通知されません。[Refresh] または [File] > [Refresh ASDM with the Running Configuration on the Device] を選択して、最新のコンフィギュレーションを取得する必要があります。また、ASDM でコンフィギュレーションに加えた変更は失われます。
- Auto Update サーバとの通信プロトコルとして HTTPS を選択すると、セキュリティ アプライアンスは SSL を使用します。その場合、セキュリティ アプライアンスに DES または 3DES のライセンスが必要です。

フィールド

[Auto Update] ペインには、[Auto Update Servers] テーブルの他に [Timeout] エリアと [Polling] エリアがあります。

[Auto Update Servers] テーブルで、Auto Update サーバにすでに設定されているパラメータを確認できます。セキュリティ アプライアンスは、テーブルの一番上にあるサーバを最初にポーリングします。テーブルのサーバ表示順序を変更するには、[Move Up] または [Move Down] ボタンをクリックします。[Auto Update Servers] テーブルには次のカラムがあります。

- [Server]：Auto Update サーバの名前または IP アドレス。
- [User Name]：Auto Update サーバのアクセス時に使用されるユーザ名。
- [Interface]：Auto Update サーバへの要求送信時に使用されるインターフェイス。
- [Verify Certificate]：Auto Update サーバが返した証明書を、セキュリティ アプライアンスで認証局（CA）のルート証明書と照合して確認するかどうかを指定します。その場合、Auto Update サーバとセキュリティ アプライアンスは、同じ CA を使用する必要があります。

[Auto Update Server] テーブルの行のいずれかをダブルクリックすると、[Edit Auto Update Server] ダイアログボックスが開き、Auto Update サーバのパラメータを変更できます。ここで行った変更はただちにテーブルに反映されますが、コンフィギュレーションに保存するには [Apply] をクリックする必要があります。

[Timeout] エリアでは、セキュリティ アプライアンスが Auto Update サーバのタイムアウトを待つ時間を設定できます。[Timeout] エリアには次のフィールドがあります。

- [Enable Timeout Period]：セキュリティ アプライアンスが Auto Update サーバから応答を受信しなかった場合にタイムアウトするには、オンにします。
- [Timeout Period (Minutes)]：Auto Update サーバから応答がなかった場合のセキュリティ アプライアンスのタイムアウト時間（分単位）を指定します。

[Polling] エリアで、セキュリティ アプライアンスから Auto Update サーバの情報をポーリングする頻度を設定できます。[Polling] エリアには次のフィールドがあります。

- [Polling Period (minutes)]：セキュリティ アプライアンスから Auto Update サーバに新しい情報をポーリングするときの待ち時間（分単位）。
- [Poll on Specified Days]：ポーリングのスケジュールを指定します。
- [Set Polling Schedule]：[Set Polling Schedule] ダイアログボックスが表示され、Auto Update サーバをポーリングする日付と時刻を設定できます。

- [Retry Period (minutes)] : サーバのポーリングに失敗した場合、セキュリティ アプライアンスから Auto Update サーバに新しい情報をポーリングするまでの待ち時間（分単位）。
- [Retry Count] : セキュリティ アプライアンスから Auto Update サーバに新しい情報をポーリングするときの再試行回数。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Set Polling Schedule

[Set Polling Schedule] ダイアログボックスでは、セキュリティ アプライアンスから Auto Update サーバをポーリングする特定の日付と時刻を設定できます。

フィールド

[Set Polling Schedule] ダイアログボックスには次のフィールドがあります。

[Days of the Week] : セキュリティ アプライアンスから Auto Update サーバをポーリングする曜日のチェックボックスを選択します。

[Daily Update] ペイン グループでは、セキュリティ アプライアンスが Auto Update サーバをポーリングする時刻を設定できます。次のフィールドがあります。

- [Start Time] : Auto Update のポーリング開始時刻を入力します。
- [Enable randomization] : セキュリティ アプライアンスから Auto Update サーバをランダムに選択した時刻にポーリングするには、オンにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Auto Update サーバの追加および編集

[Edit Auto Update Server] ダイアログボックスには次のフィールドがあります。

- [URL] : Auto Update サーバがセキュリティ アプライアンスと通信する際に使用する、http または https のプロトコルと Auto Update サーバのパス。
- [Interface] : Auto Update サーバに要求を送信する際に使用するインターフェイス。

- [Verify Certificate]：セキュリティ アプライアンスは Auto Update サーバが返した証明書を認証局（CA）のルート証明書と比較して検証します。その場合、Auto Update サーバとセキュリティ アプライアンスは、同じ CA を使用する必要があります。

[User] エリアには次のフィールドがあります。

- [User Name (Optional)]：Auto Update サーバのアクセス時に必要なユーザ名を入力します。
- [Password]：Auto Update サーバのユーザ パスワードを入力します。
- [Confirm Password]：Auto Update サーバのユーザ パスワードを再入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

高度な Auto Update 設定

フィールド

- [Use Device ID to uniquely identify the ASA]：デバイス ID による認証をイネーブルにします。デバイス ID により、セキュリティ アプライアンスが Auto Update サーバを一意に識別できます。
- [Device ID]：使用するデバイス ID のタイプ。
  - [Hostname]：ホストの名前。
  - [Serial Number]：デバイスのシリアル番号。
  - [IP Address on interface]：選択したインターフェイスの IP アドレス。セキュリティ アプライアンスを Auto Update サーバが一意に識別する場合に使用します。
  - [MAC Address on interface]：選択したインターフェイスの MAC アドレス。セキュリティ アプライアンスを Auto Update サーバが一意に識別する場合に使用します。
  - [User-defined value]：一意のユーザ ID。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Boot Image/Configuration

[Boot Image/Configuration] では、イメージ ファイルを選択して、そのファイルからセキュリティ アプライアンスをブートできます。また、起動時に使用するコンフィギュレーション ファイルもここで選択できます。

起動イメージとして使用するバイナリ イメージ ファイルは、ローカルから 4 つまで指定できます。また TFTP サーバのイメージを 1 つ指定し、そこからデバイスをブートできます。TFTP サーバに格納されているイメージを指定する場合は、そのファイルをリスト内の先頭に配置する必要があります。TFTP サーバにアクセスできず、イメージ ファイルをそこからロードできない場合は、リストでその次に指定されたイメージ ファイルがフラッシュ メモリからロードされます。

ブート変数を指定しなければ、内部フラッシュ メモリの先頭にある有効なイメージからシステムがブートされます。

フィールド

- [Boot Order]：ブート時に使用されるバイナリ イメージ ファイルの順序を表示します。
- [Boot Image Location]：ブート ファイルの物理的な場所とパスを表示します。
- [Boot Configuration File Path]：コンフィギュレーション ファイルの場所を表示します。
- [Add]：ブート プロセスで使用するフラッシュ メモリまたは TFTP ブート イメージ エントリを追加します。
- [Edit]：フラッシュ メモリまたは TFTP ブート イメージ エントリを編集します。
- [Delete]：選択されたフラッシュ メモリまたは TFTP ブート イメージ エントリを削除します。
- [Move Up]：選択したフラッシュ メモリまたは TFTP ブート イメージ エントリをブート順序の上に移動します。
- [Move Down]：選択したフラッシュ メモリまたは TFTP ブート イメージ エントリをブート順序の下に移動します。
- [Browse Flash]：ブート イメージ ファイルまたはコンフィギュレーション ファイルの場所を指定します。

ASDM イメージ コンフィギュレーション

- [ASDM Image File Path]：デバイスが起動時に使用するコンフィギュレーション ファイルの場所を表示します。
- [Browse Flash]：ブート イメージ ファイルまたはコンフィギュレーション ファイルの場所を指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

ブート イメージの追加

ブート イメージ エントリをブート順序リストに追加するには、[Boot Image/Configuration] ペインの [Add] をクリックします。

フラッシュ メモリまたは TFTP サーバのイメージを選択して、ブート イメージをブート順序リストに追加できます。

イメージのパスを入力するか [Browse Flash] をクリックして、イメージの場所を指定します。TFTP の場合、イメージの場所のパスを入力する必要があります。

フィールド

- [Flash Image]：フラッシュ ファイル システムにあるブート イメージを追加する場合に選択します。
  - [Path]：フラッシュ ファイル システムにあるブート イメージのパスを指定します。
- [TFTP Image]：TFTP サーバにあるブート イメージを追加する場合に選択します。
  - [Path]：ブート イメージ ファイルの、TFTP サーバ上のパス（サーバの IP アドレスを含む）を入力します。
- [OK]：変更内容を受け入れて、前のペインに戻ります。
- [Cancel]：変更内容を破棄して、前のペインに戻ります。
- [Help]：詳細情報を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Device Name/Password

[Device Name/Password] ペインでは、セキュリティ アプライアンスのホスト名とドメイン名、およびイネーブル パスワードと Telnet パスワードを設定できます。

ホスト名はコマンドラインのプロンプトに表示されます。このホスト名によって、複数のデバイスとのセッションを確立する場合に、コマンドを入力する場所が常に把握できます。ホスト名はシステム メッセージでも使用されます。

マルチコンテキスト モードでは、システム実行スペースで設定したホスト名がすべてのコンテキストのコマンド ラインのプロンプトに表示されます。コンテキストで設定したホスト名を、コマンドラインに表示せず、バナーに表示するオプションもあります。

セキュリティ アプライアンス は、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバを修飾子を持たない名前の「jupiter」に指定した場合、セキュリティ アプライアンスによって名前は「jupiter.example.com」に修飾されます。

[Telnet Password] にはログイン パスワードを設定します。デフォルトでは「cisco」です。このエリアは [Telnet Password] となっていますが、このパスワードは Telnet および SSH アクセスに適用されます。セキュリティ アプライアンスに接続して Telnet または SSH セッションを実行している場合、ログイン パスワードで EXEC モードにアクセスできます （Telnet または SSH アクセスのユーザ認証を設定する場合は、ユーザごとに専用のパスワードを指定します。このログイン パスワードは使用しません。システム管理者用 AAA の設定を参照）。

イネーブル パスワードを使用すると、ログイン後に特権 EXEC モードにアクセスできます また、このパスワードは、デフォルト ユーザとして ASDM にアクセスする場合に使用します。デフォルト ユーザ名は空白になっています。デフォルト ユーザ名は、[User Accounts] ペインに「enable_15」と表示されます。（イネーブル アクセスにユーザ認証を設定すると、ユーザは自分のパスワードを使用し、イネーブル パスワードを使用しません。システム管理者用 AAA の設定を参照してください。さらに、HTTP/ASDM アクセスにも認証を設定できます）。

フィールド

[Hostname and Domain Name] 領域には次のフィールドがあります。

- [Hostname]：ホスト名を設定します。デフォルトのホスト名はプラットフォームによって異なります。
- [Domain Name]：ドメイン名を設定します。デフォルト ドメイン名は default.domain.invalid です。

[Enable Password] 領域には次のフィールドがあります。マルチ コンテキスト モードの場合は、[Enable Password] 領域はコンテキストだけに表示され、システム実行スペースには表示されません。

- [Change the privileged mode password]：イネーブル パスワードを変更します。
- [Old Password]：変更前のパスワードを入力します。
- [New Password]：変更後のパスワードを入力します。
- [Confirm New Password]：変更後のパスワードを確認します。

[Telnet Password] 領域には次のフィールドがあります。マルチ コンテキスト モードの場合は、[Telnet Password] 領域はコンテキストだけに表示され、システム実行スペースには表示されません。

- [Change the password to access the platform console]：ログイン パスワードを変更します。
- [Old Password]：変更前のパスワードを入力します。
- [New Password]：変更後のパスワードを入力します。
- [Confirm New Password]：変更後のパスワードを確認します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

System Software

[System Software] ペインでは、このセキュリティ アプライアンスが Auto Update サーバとして機能するときに Auto Update クライアントとして設定されるセキュリティ アプライアンスのパラメータを設定できます。

Auto Update サーバの場合、Auto Update クライアントとして設定されたセキュリティ アプライアンスにプラットフォームと ASDM のイメージを指定できます。イメージのリビジョン番号と場所、使用するデバイス ID、デバイス ファミリ、クライアントのデバイス タイプなどが含まれます。

Auto Update サーバと Client Update の概要

Auto Update 仕様は、中央から、リモート管理アプリケーションによりセキュリティ アプライアンスのコンフィギュレーションやソフトウェア イメージをダウンロードしたり、基本的な監視機能を実行したりする場合に必要なインフラストラクチャです。

Auto Update サーバの仕様に従うことで、Auto Update サーバはセキュリティ アプライアンスにコンフィギュレーション情報をプッシュしたり、要求を送信して情報を取得したりできます。また、セキュリティ アプライアンスから Auto Update サーバへ定期的にポーリングさせ、最新のコンフィギュレーション情報を送ることもできます。また、Auto Update サーバはいつでもセキュリティ アプライアンスにコマンドを送信し、ただちにポーリング要求を送信させることもできます。Auto Update サーバとセキュリティ アプライアンスの通信では、通信パスとローカル CLI コンフィギュレーションをすべてのセキュリティ アプライアンスに設定する必要があります。

フィールド

[Client Update] ペインには次のフィールドがあります。

- [Enable Client Update]：セキュリティ アプライアンスは、Auto Update クライアントに設定された他のセキュリティ アプライアンスが使用しているイメージを更新します。
- [Client Images] テーブル：設定済みの Client Update エントリを表示します。次のカラムがあります。
  - [Device]：クライアントのデバイス ID に対応するテキスト文字列を表示します。
  - [Device Family]：クライアントのファミリ名（asa、pix、テキスト文字列のいずれか）を表示します。
  - [Device Type]：クライアントのタイプ名を表示します。
  - [Image Type]：イメージ タイプ（ASDM イメージまたは Boot イメージ）を指定します。
  - [Image URL]：ソフトウェア コンポーネントの URL を指定します。
  - [Client Revision]：ソフトウェア コンポーネントのリビジョン番号を指定します。

  [Client Images] テーブルの行のいずれかをダブルクリックすると、[Edit Client Update Entry] ダイアログボックスが開き、クライアント パラメータを変更できます。ここで行った変更はただちにテーブルに反映されますが、コンフィギュレーションに保存するには [Apply] をクリックする必要があります。
- [Live Client Update] エリア：現在トンネルを介してセキュリティ アプライアンスに接続されている Auto Update クライアントを、ただちに更新します。
  - [Tunnel Group]：「all」を選択すると、すべてのトンネル グループ上で接続している Auto Update クライアントをすべて更新します。また、トンネル グループを指定してクライアントを更新することもできます。
  - [Update Now]：ただちに更新を開始します。

（注）　[Live Client Update] は、セキュリティ アプライアンスがルーテッド モードに設定されている場合にだけ使用できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Add/Edit Client Update

フィールド

[Add/Edit Client Update] ダイアログボックスには次のフィールドがあります。

- Device Identification グループ
  - [Device ID] : クライアントの識別を一意の文字列で行う設定になっている場合に、イネーブルにします。クライアントが使用している同じ文字列を指定します。最大で 63 文字です。
  - [Device Family] : クライアントの識別をデバイス ファミリで行う設定になっている場合に、イネーブルにします。クライアントが使用している同じデバイス ファミリを指定します。これは、asa、pix、または最大 7 文字のテキスト ストリングです。
  - [Device Type] : クライアントの識別をデバイス タイプで行う設定になっている場合に、イネーブルにします。クライアントが使用している同じデバイス タイプを指定します。指定できるタイプは、pix-515、pix-515e、pix-525、pix-535、asa5505、asa5510、asa5520、asa5540 です。また、15 文字以内のテキスト文字列を指定します。
  - [Not Specified] : クライアントが上記に該当しない場合に、選択します。
- [Image Type] : イメージ タイプ（ASDM イメージまたは Boot イメージ）を指定します。この URL は、クライアントに適合するファイルを指している必要があります。最大 255 文字です。
- [Client Revision] : ソフトウェア コンポーネントのリビジョン番号に対応するテキスト文字列を指定します。たとえば、7.1(0)22 のように指定します。
- [Image URL] : ソフトウェア コンポーネントの URL を指定します。この URL は、クライアントに適合するファイルを指している必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

CHAPTER 11

DHCP、DNS、および WCCP サービス

DHCP サーバは、IP アドレスなどのネットワーク コンフィギュレーション パラメータを DHCP クライアントに提供します。セキュリティ アプライアンスは、DHCP サーバまたは DHCP リレー サービスをセキュリティ アプライアンスのインターフェイスに接続されている DHCP クライアントに提供できます。DHCP サーバは、ネットワーク コンフィギュレーション パラメータを DHCP クライアントに直接提供します。DHCP リレーでは、1 つのインターフェイスで受信した DHCP 要求を、別のインターフェイスの背後に位置する外部 DHCP サーバに渡します。

ドメイン ネーム システム（DNS）は、インターネット内にあるシステムで、オブジェクトの名前（通常はホスト名）を IP 番号や他のリソース レコード値にマッピングします。インターネットのネームスペースはドメインに分割され、各ドメイン内で名前を管理する役割は、通常、各ドメイン内のシステムが代行します。DNS クライアント サービスにより、セキュリティ アプライアンスが DNS 要求を送信する DNS サーバ、要求タイムアウト時間、その他のパラメータを指定できます。

Dynamic DNS（DDNS; ダイナミック DNS）アップデートにより、DNS を DHCP に組み込みます。これら 2 つのプロトコルは相互補完します。DHCP は、IP アドレス割り当てを集中化および自動化します。DDNS アップデートは、割り当てられたアドレスとホスト名の間のアソシエーションを事前定義された間隔で自動的に記録します。DDNS は、頻繁に変わるアドレスとホスト名のアソシエーションを頻繁にアップデートできるようにします。これにより、たとえばモバイル ホストは、ユーザまたは管理者が操作することなく、ネットワーク内を自由に移動できます。

これらのサービスの設定の詳細については、次の項目を参照してください。

- DHCP リレー
- DHCP サーバ
- DNS Client
- ダイナミック DNS
- WCCP

DHCP リレー

[DHCP Relay] ペインでは、セキュリティ アプライアンスの DHCP リレー サービスを設定できます。DHCP リレーでは、1 つのインターフェイスで受信した DHCP 要求を、別のインターフェイスの背後に位置する外部 DHCP サーバに渡します。DHCP リレーを設定するには、少なくとも 1 つの DHCP リレー グローバル サーバを指定し、DHCP 要求を受信するインターフェイス上で DHCP リレー エージェントをイネーブルにする必要があります。

制約事項

- DHCP リレー グローバル サーバが設定済みのインターフェイス上では、DHCP リレー エージェントをイネーブルにできません。
- DHCP リレー エージェントが動作するのは外部 DHCP サーバだけです。DHCP サーバとして設定されたセキュリティ アプライアンスのインターフェイスには DHCP 要求が転送されません。

前提条件

インターフェイス上で DHCP リレー エージェントをイネーブルにする前に、コンフィギュレーションまたは DHCP リレー インターフェイス サーバ内に少なくとも 1 つの DHCP リレー グローバル サーバが存在している必要があります。

フィールド

- [DHCP Relay Agent]：*表示専用* DHCP リレー エージェントの設定用フィールドが含まれます。
  - [Interface]：インターフェイス ID を表示します。インターフェイスをダブルクリックすると、[Edit DHCP Relay Agent Settings] ダイアログボックスが開きます。このダイアログボックスでは、DHCP リレー エージェントをイネーブルにし、リレー エージェント パラメータを設定できます。

  （注）　特定のインターフェイスの行をダブルクリックすると、そのインターフェイスのダイアログボックスが開きます。

  - [DHCP Relay Enabled]：DHCP リレー エージェントがインターフェイス上でイネーブルになっているかどうかが示されます。インターフェイス上で DHCP リレー エージェントがイネーブルになっている場合は「Yes」が、イネーブルになっていない場合は「No」が、このカラムに表示されます。
  - [Set Route]：DHCP サーバから返される情報にあるデフォルトのルータ アドレスを変更するように DHCP リレー エージェントを設定するかどうかを指定します。デフォルトのルータ アドレスをインターフェイスのアドレスに変更するように DHCP リレー エージェントが設定されている場合は「Yes」が、DHCP リレー エージェントではデフォルトのルータ アドレスが変更されない場合は「No」が、このカラムに表示されます。
  - [Edit]：[Edit DHCP Relay Agent Settings] ダイアログボックスを開きます。このダイアログボックスでは、DHCP リレー エージェントをイネーブルにし、リレー エージェント パラメータを設定できます。
- [DHCP Relay Global Server]：DHCP リレー グローバル サーバの設定用フィールドが含まれます。
  - [Server]：*表示専用*。設定済みの外部 DHCP サーバの IP アドレスを表示します。サーバのアドレスをダブルクリックすると、[DHCP Relay - Edit DHCP Server] ダイアログボックスが開きます。このダイアログボックスで DHCP リレー グローバル サーバの設定を編集できます。
  - [Interface]：*表示専用*。指定した DHCP サーバが接続されているインターフェイスを表示します。
  - [Add]：[DHCP Relay - Add DHCP Server] ダイアログボックスが開きます。このダイアログボックスで新しい DHCP リレー グローバル サーバを指定できます。セキュリティ アプライアンスでは、DHCP リレー グローバル サーバを 4 つまで定義できます。4 つの DHCP リレー グローバル サーバがすでに定義されている場合、このボタンは使用できません。
  - [Edit]：[DHCP Relay - Edit DHCP Server] ダイアログボックスが開きます。このダイアログボックスで DHCP リレー グローバル サーバの設定を編集できます。

– [Delete]：選択した DHCP リレー グローバル サーバを削除します。変更内容を適用または保存したときに、サーバがセキュリティ アプライアンスのコンフィギュレーションから削除されます。

– [Timeout]：DHCP アドレスのネゴシエーションに確保する時間を秒単位で指定します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 60 秒です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Edit DHCP Relay Agent Settings

[Edit DHCP Relay Agent Settings] ダイアログボックスでは、DHCP リレー エージェントをイネーブルにして、選択したインターフェイスのリレー エージェント パラメータを設定できます。

制約事項

- DHCP リレー グローバル サーバが設定済みのインターフェイス上では、DHCP リレー エージェントをイネーブルにできません。
- インターフェイスで DHCP サーバが設定されたセキュリティ アプライアンスでは、DHCP リレー エージェントをイネーブルにできません。

前提条件

選択したインターフェイス上で DHCP リレー エージェントをイネーブルにする前に、コンフィギュレーション内に少なくとも 1 つの DHCP リレー グローバル サーバが存在している必要があります。

フィールド

- [Enable DHCP Relay Agent]：オンにすると、選択したインターフェイス上で DHCP リレー エージェントがイネーブルになります。DHCP リレー エージェントをイネーブルにする前に、DHCP リレー グローバル サーバを定義しておく必要があります。
- [Set Route]：DHCP サーバから返される情報にあるデフォルトのルータ アドレスを変更するように DHCP リレー エージェントを設定するかどうかを指定します。このチェックボックスをオンにすると、DHCP リレー エージェントは、DHCP サーバから返された情報にあるデフォルトのルータ アドレスを、選択したインターフェイスのアドレスに置き換えます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

DHCP リレー グローバル サーバの追加および編集

[DHCP Relay - Add DHCP Server] ダイアログボックスで新しい DHCP リレー グローバル サーバを定義するか、[DHCP Relay - Edit DHCP Server] ダイアログボックスで既存のサーバ情報を編集します。DHCP リレー グローバル サーバは 4 つまで定義できます。

制約事項

DHCP サーバがイネーブルになっているインターフェイス上では、DHCP リレー グローバル サーバを定義できません。

フィールド

- [DHCP Server]：DHCP 要求の転送先である外部 DHCP サーバの IP アドレスを指定します。
- [Interface]：DHCP 要求が外部 DHCP サーバに転送されるときに通過するインターフェイスを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

DHCP サーバ

[DHCP Server] ペインでは、セキュリティ アプライアンスのインターフェイスを DHCP サーバとして設定できます。セキュリティ アプライアンスのインターフェイスごとに 1 つの DHCP サーバを設定できます。

（注） DHCP リレーが設定されたインターフェイス上では、DHCP サーバを設定できません。DHCP リレーの詳細については、DHCP リレーを参照してください。

フィールド

- [Interface]：*表示専用*。インターフェイス ID を表示します。インターフェイス ID をダブルクリックすると、[Edit DHCP Server] ダイアログボックスが開きます。このダイアログボックスでは、DHCP をイネーブルにして、選択したインターフェイスに DHCP アドレス プールを割り当てることができます。

（注）　特定のインターフェイスの行をダブルクリックすると、そのインターフェイスのダイアログボックスが開きます。

- [DHCP Enabled]：*表示専用*。インターフェイス上で DHCP がイネーブルになっているかどうかを示します。インターフェイス上で DHCP がイネーブルになっている場合は「Yes」が、イネーブルになっていない場合は「No」が、このカラムに表示されます。
- [Address Pool]：*表示専用*。DHCP アドレス プールに割り当てられた IP アドレスの範囲が表示されます。
- [DNS Servers]：*表示専用*。インターフェイスに設定された DNS サーバが表示されます。
- [WINS Servers]：*表示専用*。インターフェイスに設定された WINS サーバが表示されます。
- [Domain Name]：*表示専用*。インターフェイスのドメイン名が表示されます。
- [Ping Timeout]：*表示専用*。インターフェイス上でセキュリティ アプライアンスが ICMP ping の応答を待つ時間がミリ秒単位で表示されます。
- [Lease Length]：*表示専用*。インターフェイス上に設定された DHCP サーバが、DHCP クライアントによる割り当て済み IP アドレスの使用を許可する時間が表示されます。
- [Auto Interface]：*表示専用*。自動コンフィギュレーションに DNS、WINS、ドメイン名の各情報を提供する DHCP クライアント上のインターフェイスが表示されます。
- [Options]：*表示専用*。インターフェイスに設定された高度な DHCP オプションが表示されます。
- [Dynamic DNS Settings]：*表示専用*。表示
- [Edit]：選択したインターフェイスの [Edit DHCP Server] ダイアログボックスが開きます。[Edit DHCP Server] ダイアログボックスでは、DHCP をイネーブルにして、DHCP アドレス プールを指定できます。
- [Global DHCP Options]：オプションの DHCP パラメータが含まれます。
  - [Enable Auto-configuration from interface]：DHCP 自動コンフィギュレーションをイネーブルにし、メニューからインターフェイスを選択する場合にオンにします。

    DHCP 自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。自動コンフィギュレーションを介して取得された情報の一部が、[Other DHCP Options] 領域でも手動で指定されている場合、検索された情報より手動で指定した情報が優先されます。
  - [DNS Server 1]：（任意）DHCP クライアントのプライマリ DNS サーバの IP アドレスを指定します。
  - [DNS Server 2]：（任意）DHCP クライアントの代替 DNS サーバの IP アドレスを指定します。
  - [Domain Name]：（任意）DHCP クライアントの DNS ドメイン名を指定します。example.com などの有効な DNS ドメイン名を入力します。
  - [Lease Length]：（任意）リースの期間が終了する前に、割り当て IP アドレスをクライアントが使用できる時間を秒単位で指定します。有効値の範囲は 300 ～ 1048575 秒です。デフォルト値は 3600 秒（1 時間）です。

  - [Primary WINS Server]：（任意）DHCP クライアントのプライマリ WINS サーバの IP アドレスを指定します。
  - [Secondary WINS Server]：（任意）DHCP クライアントの代替 WINS サーバの IP アドレスを指定します。
  - [Ping Timeout]：（任意）アドレスの競合を避けるために、セキュリティ アプライアンスは、1 つのアドレスに ICMP ping パケットを 2 回送信してから、そのアドレスを DHCP クライアントに割り当てます。[Ping Timeout] フィールドでは、セキュリティ アプライアンスが DHCP ping 試行のタイムアウトを待つ時間をミリ秒単位で指定します。有効値の範囲は 10 ～ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。
  - [Advanced]：Advanced DHCP Options ダイアログボックスを開きます。このダイアログボックスでは、DHCP オプションとそのパラメータを指定できます。
- [Dynamic DNS Settings for DHCP Server]：この領域では、DHCP サーバの DDNS 更新設定を実行できます。
  - [Update DNS Clients]：クライアント PTR リソース レコードの更新のデフォルト アクションに加え、DHCP サーバも次の更新アクションを（選択した場合に）実行するように指定する場合にオンにします。
  - [Update Both Records]：DHCP サーバが A レコードと PTR RR の両方を更新するように指定する場合にオンにします。
  - [Override Client Settings]：DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションを上書きするように指定する場合にオンにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Edit DHCP Server

[Edit DHCP Server] ダイアログボックスでは、DHCP をイネーブルにして、選択したインターフェイスの DHCP アドレス プールを指定できます。

フィールド

- [Enable DHCP Server]：選択したインターフェイス上で DHCP サーバをイネーブルにするには、このチェックボックスをオンにします。選択したインターフェイス上で DHCP をディセーブルにするには、チェックボックスをオフにします。選択したインターフェイス上で DHCP サーバをディセーブルにしても、指定した DHCP アドレス プールはクリアされません。
- [DHCP Address Pool]：DHCP サーバが使用する IP アドレス プールを入力します。IP アドレスの最下位から最上位の間で範囲指定して入力します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
- [Optional Parameters]：DHCP サーバの次のパラメータをオプションで設定できます。

- [DNS Server 1] : DHCP クライアントのプライマリ DNS サーバの IP アドレスを入力します。
- [DNS Server 2] : DHCP クライアントの代替 DNS サーバの IP アドレスを入力します。
- [Domain Name] : DHCP クライアントの DNS ドメイン名を入力します。example.com などの有効な DNS ドメイン名を入力します。
- [Lease Length] : リースの期間が終了する前に、割り当て IP アドレスをクライアントが使用できる時間を秒単位で入力します。有効値の範囲は 300 ～ 1048575 秒です。デフォルト値は 3600 秒（1 時間）です。
- [Primary WINS Server]:DHCP クライアントのプライマリ WINS サーバの IP アドレスを入力します。
- [Secondary WINS Server] : DHCP クライアントの代替 WINS サーバの IP アドレスを入力します。
- [Ping Timeout] : セキュリティ アプライアンスが DHCP ping 試行のタイムアウトを待つ時間をミリ秒単位で入力します。有効値の範囲は 10 ～ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。
- [Enable Auto-configuration on interface] : DHCP 自動コンフィギュレーションをイネーブルにし、メニューからインターフェイスを選択する場合にオンにします。
- [Advanced] : Advanced DHCP Options ダイアログボックスを開きます。このダイアログボックスでは、DHCP オプションとそのパラメータを指定できます。

- [Dynamic DNS Settings for DHCP Server] : この領域では、DHCP サーバの DDNS 更新設定を実行できます。
  - [Update DNS Clients] : クライアント PTR リソース レコードの更新のデフォルト アクションに加え、DHCP サーバも次の更新アクションを（選択した場合に）実行するように指定する場合にオンにします。
  - [Update Both Records] : DHCP サーバが A レコードと PTR RR の両方を更新するように指定する場合にオンにします。
  - [Override Client Settings] : DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションを上書きするように指定する場合にオンにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Advanced DHCP Options

[Advanced DHCP Options] ダイアログボックスでは、DHCP オプション パラメータを設定できます。DHCP オプションは、DHCP クライアントに追加情報を提供する場合に使用します。たとえば、DHCP オプション 150 および DHCP オプション 66 は、Cisco IP Phone および Cisco IOS ルータに TFTP サーバ情報を提供します。

高度な DHCP オプションを使用すれば、DHCP クライアントに DNS、WINS、およびドメイン名パラメータを提供できます。また、DHCP 自動コンフィギュレーション設定を使用すれば、これらの値を取得したり、DHCP サーバ ペインで値を手動で指定したりもできます。この情報の指定に 2 つ以上の方法を使用すると、次の優先順位で情報が DHCP クライアントに渡されます。

1. 手動で行われた設定
2. 高度な DHCP オプションの設定
3. DHCP 自動コンフィギュレーション

たとえば、DHCP クライアントが受け取るドメイン名を手動で定義し、次に DHCP 自動コンフィギュレーションをイネーブルにできます。DHCP 自動コンフィギュレーションは、DNS および WINS サーバとともにドメインを検索しますが、手動で定義されたドメイン名が検索された DNS および WINS サーバ名とともに DHCP クライアントに渡されます。DHCP 自動コンフィギュレーション プロセスで検索されたドメイン名は、手動で定義されたドメイン名を優先させるために破棄されます。

フィールド

- [Option to be Added]：DHCP オプションの設定に使用されるフィールドが含まれます。
  - [Choose the option code]：使用可能なオプション コードが一覧表示されます。オプション 1、12、50 ～ 54、58 ～ 59、61、67、82 を除き、すべての DHCP オプション（オプション 1 ～ 255）がサポートされています。設定するオプションを選択します。

    一部のオプションは標準です。標準オプションの場合、オプション名がオプション番号の後のカッコ内に表示され、オプション番号およびオプション パラメータは、オプションでサポートされるものに制限されます。他のすべてのオプションにはオプション番号だけが表示され、オプションに指定する適切なパラメータを選択する必要があります。

    標準 DHCP オプションの場合、サポートされるオプションの値タイプだけが使用可能です。たとえば、DHCP オプション 2（タイム オフセット）を選択した場合、このオプションに指定できるのは 16 進数値だけです。他のすべての DHCP オプションでは、すべてのオプション値タイプを使用できますが、適切なオプション値タイプを選択する必要があります。
- [Option Data]：これらのオプションは、オプションが DHCP クライアントに返す情報のタイプを指定します。標準 DHCP オプションの場合、サポートされるオプションの値タイプだけが使用可能です。他のすべての DHCP オプションでは、すべてのオプション値タイプを使用できます。
- [IP Address]：この値を選択すると、IP アドレスを DHCP クライアントに返すように指定されます。IP アドレスは最大 2 つまで指定できます。

  （注） 関連付けられた [IP Address] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、[DHCP Option 3（Router）] を選択した場合、フィールド名は [Router 1] および [Router 2] に変わります。

  - [IP Address 1]：ドット付き 10 進数表記の IP アドレス。
  - [IP Address 2]：（任意）ドット付き 10 進数表記の IP アドレス。
- [ASCII]：このオプションを選択すると、ASCII 値が DHCP クライアントに返されるように指定されます。

  （注） 関連付けられた [Data] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、[DHCP Option 14（Merit Dump File）] を選択した場合、関連付けられた [Data] フィールドの名前は [File Name] に変わります。

  - [Data]：ASCII 文字列。文字列に空白スペースを含めることはできません。

- [Hex]：このオプションを選択すると、DHCP クライアントに 16 進数値を返すように指定されます。

（注）　関連付けられた [Data] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、DHCP オプション 2（タイム オフセット）を選択した場合、関連付けられた [Data] フィールドは [Offset] フィールドになります。

  - [Data]：スペースなしの偶数で構成される 16 進数文字列。0x プレフィックスを使用する必要はありません。
- [Add]：設定済みのオプションを DHCP オプション テーブルに追加します。
- [Delete]：選択したオプションを DHCP オプション テーブルから削除します。
- DHCP オプション テーブル：設定されている DHCP オプションを一覧表示します。
  - [Option Code]：DHCP オプション コードを表示します。標準 DHCP オプションの場合、オプション名はオプション コードの隣のカッコ内に表示されます。
  - [Option Data]：選択したオプションに対して設定されたパラメータを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

DNS Client

[DNS Client] ペインには、セキュリティ アプライアンスの DNS サーバ グループおよび DNS 検索情報が表示されます。これにより、サーバ名をクライアントレス SSL VPN コンフィギュレーションまたは証明書コンフィギュレーションに解決できます。サーバ名（AAA など）を定義するその他の機能は、DNS 解決をサポートしていません。これらの場合、IP アドレスを入力するか、[ネットワーク オブジェクトの概要] ペインにサーバ名を追加して名前を手動で IP アドレスに解決する必要があります。

フィールド

- [DNS Server Groups]：DNS サーバ リストを表示および管理します。DNS 要求を転送できるアドレスは最大 6 つです。セキュリティ アプライアンス では、応答を受信するまで各 DNS サーバを順に試します。DNS サーバを追加する前に、[DNS Lookup] 領域のインターフェイスの少なくとも 1 つで DNS をイネーブルにする必要があります。この領域のテーブルの内容は次のとおりです。
  - [Name]：*表示専用*。設定済みの各 DNS サーバ グループの名前を表示します。
  - [Servers]：*表示専用*。設定済みサーバの IP アドレスを表示します。
  - [Timeout]：*表示専用*。リスト内の次の DNS サーバを試行するまでに待機する秒数（1 ～ 30 秒）を表示します。デフォルトは 2 秒です。セキュリティ アプライアンスがサーバのリストを再試行するたびに、このタイムアウトは倍増します。

  - [Retries]：*表示専用*。リスト内の次の DNS サーバを試行するまでに待機する秒数を表示します。
  - [Domain Name]：*表示専用*。セキュリティ アプライアンスが要求を再試行する回数を表示します。
- [DNS Lookup]：インターフェイス上での DNS 検索をイネーブルまたはディセーブルにします。
  - [Interface]：*表示専用*。すべてのインターフェイス名を一覧表示します。
  - [DNS Enabled]：*表示専用*。インターフェイスが DNS 検索をサポートするかどうかを Yes または No で表示します。
  - [Disable]：選択したインターフェイスの DNS 検索をディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

DNS サーバ グループの追加および編集

[Add or Edit DNS Server Group] ペインでは、セキュリティ アプライアンスの 1 つまたは複数の DNS サーバを指定または変更できます。これにより、サーバ名をクライアントレス SSL VPN コンフィギュレーションまたは証明書コンフィギュレーションの IP アドレスに解決できます。サーバ名（AAA など）を定義するその他の機能は、DNS 解決をサポートしていません。このような場合、IP アドレスを入力するか、[ネットワーク オブジェクトの概要] ペインにサーバ名を追加して名前を手動で IP アドレスに解決する必要があります。

フィールド

- [Name]：サーバ名を指定します。Edit 機能においては、このフィールドは*表示専用*です。
- [DNS Servers]：DNS サーバ リストを管理します。DNS 要求を転送できるアドレスは、最大 6 つまで指定できます。セキュリティ アプライアンス では、応答を受信するまで各 DNS サーバを順に試します。DNS サーバを追加する前に、[DNS Lookup] 領域のインターフェイスの少なくとも 1 つで DNS をイネーブルにする必要があります。
  - [Server to be Added]：DNS サーバの IP アドレスを指定します。
  - [Add]：DNS サーバをリストの下に追加します。
  - [Delete]：選択した DNS サーバをリストから削除します。
  - [Servers]：*表示専用*。DNS サーバ リストを表示します。
  - [Move Up]：選択した DNS サーバをリストの上方向に移動します。
  - [Move down]：選択した DNS サーバをリストの下方向に移動します。
- [Timeout]：リスト内の次の DNS サーバを試行するまでの秒数を 1 ～ 30 秒の間で指定します。デフォルトは 2 秒です。セキュリティ アプライアンスがサーバのリストを再試行するたびに、このタイムアウトは倍増します。

- [Retries] : セキュリティ アプライアンスが要求を再試行する回数を設定します。再試行の範囲は 1 ～ 10 回です。
- [Domain Name] :（任意）サーバの DNS ドメイン名を指定します。example.com などの有効な DNS ドメイン名を入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ダイナミック DNS

Dynamic DNS はアドレスとドメイン名のマッピングを提供して、各ホストの DHCP 割り当てにより IP アドレスが頻繁に変化しても、ホスト同士が互いに検索できるようにします。DDNS の名前とアドレスのマッピングは、2 つのリソース レコードの DHCP サーバ上で行われます。A RR は名前から IP アドレスへのマッピングを保持し、PTR RR はアドレスから名前へのマッピングを行います。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準、および一般的な HTTP 方式）のうち、セキュリティ アプライアンスのこのリリースでは、IETF 方式をサポートしています。

[Dynamic DNS] ペインには、設定済みの DDNS 更新方法および DDNS 用に設定されたインターフェイスが表示されます。事前定義された間隔で割り当て済みアドレスとホスト名の間のアソシエーションを自動的に記録することで、DDNS では頻繁に変更されるアドレスとホスト名間のアソシエーションを頻繁に更新できます。これにより、たとえばモバイル ホストは、ユーザまたは管理者が操作することなく、ネットワーク内を自由に移動できます。

フィールド

- [Update Methods] : セキュリティ アプライアンスで設定された DDNS 更新方法を一覧表示します。テーブルに含まれるのは次の各項目です。
  - [Method Name] : *表示専用*。DDNS 更新方法のユーザ定義名が表示されます。
  - [Interval] : *表示専用*。更新方法に設定された DNS 更新の試行間の時間が表示されます。
  - [Update DNS Server Records] : *表示専用*。その方法で A リソース レコード（名前から IP アドレスへ）と PTR リソース レコード（IP アドレスから名前へ）の両方が更新されるのか、または両方とも更新されないのかが表示されます。
  - [Add/Edit] : [Add/Edit Dynamic DNS Update Methods] ダイアログボックスが表示されます。
  - [Delete] : 現在選択されている更新方法がテーブルから削除されます。
- [Dynamic DNS Interface Settings] : DDNS 用に設定された各インターフェイスの DDNS 設定を一覧表示します。
  - [Interface] : *表示専用*。DDNS 用に設定されたセキュリティ アプライアンス インターフェイスの名前が表示されます。
  - [Method Name] : *表示専用*。各インターフェイスに割り当てられた更新方法が表示されます。
  - [Hostname] : *表示専用*。DDNS クライアントのホスト名が表示されます。

- [Update DHCP Server Records] : *表示専用*。インターフェイスが A および PTR ソース レコードを両方とも更新するか、または両方とも更新しないかが表示されます。
- [Add/Edit] : [Add/Edit Dynamic DNS Interface Settings] ダイアログボックスが表示されます。
- [Delete] : 選択したインターフェイスの DDNS 更新設定を削除します。

• [DHCP Clients Update DNS Records]：DHCP クライアントが DHCP サーバで更新されるように要求するレコードを指定する、グローバル設定です。次のいずれかのオプション ボタンをクリックします。

- [Default（PTR Records）] では、サーバによりクライアントが PTR レコードの更新を要求するように指定されます。

  または

- [Both]（PTR Records および A Records）では、サーバによりクライアントが A および PTR DNS リソース レコードの両方を要求するように指定されます。

  または

- [None] では、サーバによりクライアントが更新を要求しないように指定されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Add/Edit Dynamic DNS Update Methods

[Add/Edit Dynamic DNS Update Methods] ダイアログボックスでは、新しい方法の追加、または以前に追加した方法の編集が実行できます。方法の名前を指定したり（方法を追加した場合）、DDNS 更新の試行間隔を指定したり、DDNS クライアントが A レコードと PTR レコードの両方の更新を試行するかどうか、または両方の更新を試行しないかどうかを指定できます。

フィールド

- [Name]：方法を追加する場合、このフィールドに新しい方法の名前を入力します。既存の方法を編集する場合、このフィールドは*表示専用*となり、選択した方法の名前が編集用に表示されます。
- [Update Interval]：更新試行間の経過時間を指定します。間隔の範囲は 0 ～ 約 1 年です。
  - [Days]：更新試行間の日数を 0 ～ 364 日の間で選択します。
  - [Hours]：更新試行間の時間数を 0 ～ 23 時間（整数）から選択します。
  - [Minutes]：更新試行間の分数を 0 ～ 59 分（整数）から選択します。
  - [Seconds]：更新試行間の秒数を 0 ～ 59 秒（整数）から選択します。
  - [Update Records]：クライアントが A および PTR DNS リソース レコードの両方の更新を試行する場合は [Both]（A および PTR Records）を、A レコードだけ更新する場合は [A Records Only] をクリックします。これは、クライアントが更新する DNS サーバ レコードの個別の設定方法です。

これらの単位は、追加式です。つまり、日数に 0、時間数に 0、分数に 5、秒数に 15 を入力した場合、このアップデート方式がアクティブである限り、5 分 15 秒ごとにアップデートが試行されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Add/Edit Dynamic DNS Interface Settings

[Add/Edit Dynamic DNS Interface Settings] では、セキュリティ アプライアンス インターフェイス上で DDNS を設定できます。更新方法を割り当てたり、ホスト名を指定したり、クライアントによる A レコードおよび PTR レコードの両方を更新またはいずれも更新しない DHCP サーバを設定したりできます。

フィールド

- [Interface]：メニューから DDNS を設定するインターフェイスを選択します。
- [Update Method]：メニューから使用可能な DDNS 更新方法を選択します。
- [Hostname]：DDNS クライアントのホスト名を入力します。

- [DHCP Client]：この領域では、DHCP クライアントが A レコードおよび PTR DNS レコードの両方を更新するか、またはどちらも更新しないかを指定できます。このインターフェイス設定は、[Configuration] > [Properties] > [DNS] > [Dynamic DNS] で、グローバル設定を上書きします。
- [DHCP Client Updates DNS Records]：次のオプション ボタンのいずれかをクリックします。
  - [Default]（PTR Records のみ）では、サーバによりクライアントが PTR レコードだけの更新を要求するように指定されます。

    または
  - [Both]（PTR Records および A Records）では、サーバによりクライアントが A および PTR DNS リソース レコードの両方を要求するように指定されます。

    または
  - [None] では、サーバによりクライアントが更新を要求しないように指定されます。

（注） このアクションを有効にするには、選択したインターフェイス上で DHCP がイネーブルになっている必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

WCCP

Web Cache Communication Protocol（WCCP）機能により、WCCP サービス グループとリダイレクト Web キャッシュ トラフィックを指定できます。この機能は、選択したタイプのトラフィックを Web キャッシュ エンジンのグループに透過的にリダイレクトして、リソースの使用状況を最適化し、応答時間を短縮します。

WCCP サービス グループ

[Service Groups] パネルでは、スペースを割り当て、指定した Web Cache Communication Protocol（WCCP）サービス グループのサポートをイネーブルにできます。

フィールド

- [Service]：WCCP サポートのサービス グループ名またはサービス グループ番号を表示します。
- [Redirect List]：特定のサービス グループにリダイレクトされるトラフィックを制御するアクセス リストの名前を表示します。

- [Group List]：サービス グループに参加が許可される Web キャッシュを決定するアクセス リストの名前を表示します。

WCCP サービス グループの追加または編集

[Add or Edit Service Group] ダイアログボックスでは、設定されたサービス グループのサービス グループ パラメータを変更できます。

フィールド

- [Service]：サービス グループを指定します。Web キャッシュ サービス、またはそのサービスの ID 番号を指定できます。
- [Web Cache]：Web キャッシュ サービスを指定します。ダイナミック サービス ID で指定されるサービスを含め、サービスの最大数は 256 です。
- [Dynamic Service Number]：ダイナミック サービス ID。これにより、サービス定義がキャッシュによって指定されます。ダイナミック サービス番号は 0 ～ 254 の範囲で指定できます。これは、サービス グループの名前として使用されます。
- [Redirect List]：このサービス グループにリダイレクトされるトラフィックを制御する事前定義済みのアクセス リスト。
- [Group List]：サービス グループに参加が許可される Web キャッシュを決定する、事前定義済みのアクセス リスト。
- [Password]：最大 7 文字までのパスワードを入力します。このパスワードは、サービス グループから受信したメッセージの MD5 認証で使用されます。パスワードの長さは 1 ～ 8 文字です。
- [Confirm Password]：パスワードを再入力します。
- [Manage]：アクセス リスト マネージャを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

Redirection

[Redirection] パネルでは、インターフェイスの入力側での WCCP によるパケット リダイレクションをイネーブルにできます。

フィールド

- [Interface]：WCCP リダイレクションがイネーブルになっているインターフェイスを表示します。
- [Service Group]：WCCP に設定されているサービス グループの名前を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

WCCP リダイレクションの追加または編集

[Redirection] パネルでは、インターフェイスの入力側での WCCP によるパケット リダイレクションをイネーブルにできます。

フィールド

- [Interface]：WCCP リダイレクションをイネーブルにするインターフェイスを選択します。
- [Service Group]：サービス グループを選択します。
- [Add Service]：[Add/Edit WCCP Service Group] ダイアログボックスが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

CHAPTER 12

AAA サーバおよびユーザ アカウントの設定

この章では、AAA （「トリプル エー」と発音）のサポート、および AAA サーバとローカル データベースの設定方法について説明します。

この章の内容は、次のとおりです。

AAA の概要

AAA によって、セキュリティ アプライアンスが、ユーザが誰か（認証）、ユーザが何を実行できるか（許可）、およびユーザが何を実行したか（アカウンティング）を判別することが可能になります。

AAA には、ユーザ アクセスに対して、アクセス リストだけを使用する場合よりもレベルの高い保護および制御機能が用意されています。たとえば、すべての外部ユーザが DMZ ネットワークのサーバ上の Telnet にアクセスできるようにするアクセス リストを作成できます。サーバへのアクセスを一部のユーザだけに限定する場合で、対象ユーザの IP アドレスが必ずしも明らかでないときには、AAA をイネーブルにして、認証または許可されたユーザだけに セキュリティ アプライアンス を通過させることができます （Telnet サーバもまた、認証を実行します。セキュリティ アプライアンスは、許可されないユーザがサーバにアクセスできないようにします）。

認証だけで使用することも、許可およびアカウンティングとともに使用することもできます。許可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および許可とともに使用することもできます。

この項では、次のトピックについて取り上げます。

認証の概要

認証では、有効な証明書（一般にはユーザ名とパスワード）を要求することによって、アクセスを制御します。次の項目を認証するように、セキュリティ アプライアンスを設定できます。

- セキュリティ アプライアンスへのすべての管理接続（この接続には、次のセッションが含まれます）
  - Telnet
  - SSH
  - シリアル コンソール
  - ASDM（HTTPS を使用）
  - VPN 管理アクセス
- **enable** コマンド
- ネットワーク アクセス
- VPN アクセス

許可の概要

許可では、ユーザを認証したあと、*各ユーザ*のアクセスを制御できます。次の項目を許可するように、セキュリティ アプライアンスを設定できます。

- 管理コマンド
- ネットワーク アクセス
- VPN アクセス

許可は、認証された個々のユーザが使用できるサービスおよびコマンドを制御します。許可をイネーブルにせずに認証だけを使用する場合、認証されたすべてのユーザに対し、サービスへのアクセスが一様に提供されます。

許可で提供される制御を必要とする場合は、広範な認証ルールを設定してから、詳細な許可を設定できます。たとえば、内部ユーザを認証して外部ネットワークの任意サーバにアクセスできるようにしたあと、外部サーバへのアクセスを制限して、特定のユーザだけが許可を使用してアクセスできるように設定することができます。

セキュリティ アプライアンスはユーザあたり最初の 16 件の許可要求をキャッシュするため、ユーザが現在の認証セッション中に同じサービスにアクセスした場合、セキュリティ アプライアンスは許可サーバに要求を再送信しません。

アカウンティングの概要

アカウンティングは、セキュリティ アプライアンスを通過するトラフィックを追跡して、ユーザ アクティビティを記録できるようにします。トラフィックの認証をイネーブルにすると、ユーザごとにトラフィックをアカウンティングできます。トラフィックを認証しない場合は、IP アドレスごとにトラフィックをアカウンティングできます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、セキュリティ アプライアンスを通過するセッションのバイト数、使用されたサービス、および各セッションの継続時間などの情報が含まれます。

AAA サーバおよびローカル データベースのサポート

セキュリティ アプライアンスは、さまざまな AAA サーバ タイプおよびセキュリティ アプライアンスに保存されているローカル データベースをサポートします。ここでは、各 AAA サーバ タイプおよびローカル データベースのサポートについて説明します。

ここでは、次の内容について説明します。

サポートの要約

表 12-1 に、各 AAA サービスのサポート状況の要約を AAA サーバ タイプ（ローカル データベースを含む）別に示します。特定の AAA サーバ タイプのサポートの詳細については、表に続く項目を参照してください。

表 12-1　AAA サポートの要約

	データベース タイプ							
AAA サービス	**ローカル**	**RADIUS**	**TACACS+**	**SDI**	**NT**	**Kerberos**	**LDAP**	**HTTP Form**
認証								
VPN ユーザ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[1]
ファイアウォール セッション	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
管理者	Yes	Yes	Yes	Yes[2]	Yes	Yes	Yes	No
許可								
VPN ユーザ	Yes	Yes	No	No	No	No	Yes	No
ファイアウォール セッション	No	Yes[3]	Yes	No	No	No	No	No
管理者	Yes[4]	No	Yes	No	No	No	No	No
アカウンティング								
VPN 接続	No	Yes	Yes	No	No	No	No	No
ファイアウォール セッション	No	Yes	Yes	No	No	No	No	No
管理者	No	Yes[5]	Yes	No	No	No	No	No

1. HTTP Form プロトコルは、クライアントレス SSL VPN 接続に対してだけシングル サインオン認証をサポートします。
2. SDI は、HTTP 管理アクセスについてはサポートされません。
3. ファイアウォール セッションの場合、RADIUS 許可はユーザ固有のアクセス リストでだけサポートされます。このアクセス リストは RADIUS 認証応答で受信または指定されます。
4. ローカル コマンド許可は、特権レベルに限りサポートされます。
5. コマンド アカウンティングは、TACACS+ でのみ使用できます。

RADIUS サーバのサポート

ASA は、ASA 自体で使用可能な RADIUS サーバの他、AAA について、次の RADIUS サーバをサポートしています。

- Cisco Secure ACS 3.2、4.0、4.1
- RSA Authentication Manager 5.2 および 6.1 の RSA Radius

認証方法

セキュリティ アプライアンスは、RADIUS で次の認証方法をサポートします。

- PAP：すべての接続タイプの場合。
- CHAP：L2TP-over-IPSec の場合。
- MS-CHAPv1：L2TP-over-IPSec の場合。
- MS-CHAPv2：L2TP-over-IPSec 用、およびパスワード管理機能がイネーブルの場合は通常の IPSec リモート アクセス接続用。

属性のサポート

セキュリティ アプライアンスは、次の RADIUS 属性のセットをサポートします。

- RFC 2138 に定義されている認証属性
- RFC 2139 に定義されているアカウンティング属性
- RFC 2868 に定義されているトンネル プロトコル サポート用の RADIUS 属性
- RADIUS ベンダー ID 9 によって識別される Cisco IOS VSA
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA
- RFC 2548 に定義されている Microsoft VSA

RADIUS 許可機能

セキュリティ アプライアンスでは RADIUS サーバを使用して、ダイナミック アクセス リストまたはユーザごとのアクセス リスト名を使用するネットワーク アクセスに対して、ユーザ許可を実行できます。ダイナミック アクセス リストを実装するには、これをサポートするように RADIUS サーバを設定する必要があります。ユーザを認証する場合、RADIUS サーバによってダウンロード可能なアクセス リスト、またはアクセス リスト名がセキュリティ アプライアンスに送信されます。所定のサービスへのアクセスがアクセス リストによって許可または拒否されます。認証セッションの有効期限が切れると、セキュリティ アプライアンスによってアクセス リストが削除されます。

TACACS+ サーバのサポート

セキュリティ アプライアンスは、ASCII、PAP、CHAP、および MS-CHAPv1 で TACACS+ 認証をサポートします。

SDI サーバのサポート

RSA SecureID サーバは、SDI サーバとも呼ばれます。

ここでは、次の内容について説明します。

SDI バージョンのサポート

セキュリティ アプライアンスでは、SDI バージョン 5.0 および 6.0 がサポートされています。SDI は、SDI プライマリ サーバおよび SDI レプリカ サーバの概念を使用します。各プライマリおよびそのレプリカは、シングル ノード秘密ファイルを共有します。そのノード秘密ファイルの名前は、.sdi が付加された ACE/サーバ IP アドレスの 16 進数値に基づきます。

セキュリティ アプライアンスに設定するバージョン 5.0 または 6.0 SDI サーバは、プライマリでも、レプリカのいずれか 1 つでもかまいません。ユーザ認証のための SDI エージェントによるサーバの選択方法の詳細については、「SDI プライマリ サーバとレプリカ サーバ」の項を参照してください。

2 ステップ認証プロセス

SDI バージョン 5.0 および 6.0 は 2 ステップのプロセスを使用して、侵入者が RSA SecurID 認証要求から情報をキャプチャし、この情報を使用して別のサーバに認証を証明しないように防止します。エージェントはまず、SecurID サーバにロック要求を送信してから、ユーザ認証要求を送信します。サーバはユーザ名をロックして、別の（レプリカ）サーバがユーザ名を受信できないようにします。そのため、同じユーザが同じ認証サーバを同時に使用して、2 台の セキュリティ アプライアンス に認証することができなくなります。ユーザ名のロックに成功すると、セキュリティ アプライアンスはパスコードを送信します。

SDI プライマリ サーバとレプリカ サーバ

セキュリティ アプライアンスは、最初のユーザが設定済みサーバ（プライマリでもレプリカでもかまいません）に認証を証明するときに、サーバ リストを取得します。次に、セキュリティ アプライアンスはリスト上の各サーバにプライオリティを割り当て、その後のサーバ選択では、この割り当てられたプライオリティのサーバから無作為に抽出します。最もプライオリティの高いサーバが選択される可能性が高くなります。

NT サーバのサポート

セキュリティ アプライアンスは、NTLM バージョン 1（集合的に NT サーバと呼びます）をサポートしている Microsoft Windows サーバ オペレーティング システムをサポートします。

（注）　NT サーバでは、ユーザ パスワードの最大長は 14 文字です。15 文字めからは切り捨てられます。これは、NTLM バージョン 1 の制限です。

Kerberos サーバのサポート

セキュリティ アプライアンスは、3DES、DES、および RC4 暗号タイプをサポートしています。

（注）　セキュリティ アプライアンスは、トンネル ネゴシエーション中のユーザ パスワードの変更はサポートしていません。この状況が意図せずに発生することを回避するために、セキュリティ アプライアンスに接続するユーザの Kerberos/Active Directory サーバでのパスワード期限切れをディセーブルにします。

LDAP サーバのサポート

この項では、ユーザ認証と VPN 許可にセキュリティ アプライアンスを利用する LDAP ディレクトリの使用方法について説明します。

認証中、セキュリティ アプライアンスは、ユーザの LDAP サーバへのクライアント プロキシとして機能し、プレーン テキストまたは Simple Authentication and Security Layer（SASL）プロトコルのいずれかを使って LDAP サーバに対する認証を行います。デフォルトで、セキュリティ アプライアンスは、通常はユーザ名とパスワードである認証パラメータを LDAP サーバにプレーン テキストで渡します。SASL とプレーン テキストのどちらを使用する場合でも、セキュリティ アプライアンスと LDAP サーバの間での通信のセキュリティは SSL で確保されます。

（注）　SASL を設定しない場合、SSL で LDAP 通信を保護することを強くお勧めします。

ユーザ LDAP 認証が成功すると、LDAP サーバは認証されたユーザの属性を返します。VPN 認証では、通常これらの属性には、VPN セッションに適用される許可データが含まれます。したがって、LDAP を使用すると、認証と許可が 1 つのステップで行われます。

LDAP による認証または許可をセットアップする設定手順の例については、付録 B「許可および認証用の外部サーバの設定」を参照してください。

HTTP Form でのクライアントレス SSL VPN に対する SSO のサポート

セキュリティ アプライアンスでは、クライアントレス SSL VPN のシングル サインオン（SSO）認証だけに HTTP Form プロトコルを使用できます。シングル サインオンのサポートによって、ユーザはユーザ名とパスワードを 1 回だけ入力して、複数の保護されているサービスおよび Web サーバにアクセスできます。セキュリティ アプライアンスで実行するクライアントレス SSL VPN サーバは、認証サーバに対するユーザのプロキシとして動作します。ユーザがログインすると、クライアントレス SSL VPN サーバは、ユーザ名とパスワードを含む SSO 認証要求を HTTPS を使用して認証サーバに送信します。サーバが認証要求を受け入れた場合は、クライアントレス SSL VPN サーバに SSO 認証クッキーを戻します。セキュリティ アプライアンスは、ユーザの代わりにこのクッキーを保持し、ユーザの認証にこのクッキーを使用して、SSO サーバで保護されているドメイン内の Web サイトの安全を守ります。

管理者は、SSO の設定に対して、HTTP Form プロトコルの他にも、基本 HTTP 認証プロトコルや NTLM 認証プロトコル（**auto-signon** コマンド）、あるいは Computer Associates eTrust SiteMinder SSO サーバ（旧 Netegrity SiteMinder）を選択できます。HTTP Form、**auto-signon** または SiteMinder を使用した SSO の設定の詳細については、「クライアントレス SSL VPN」の章を参照してください。

ローカル データベースのサポート

セキュリティ アプライアンスは、ユーザ プロファイルを取り込むことができるローカル データベースを管理します。

ここでは、次の内容について説明します。

- 「ユーザ プロファイル」（P.12-7）
- 「フォールバック サポート」（P.12-7）

ユーザ プロファイル

ユーザ プロファイルには、少なくともユーザ名が含まれます。通常、パスワードはオプションですが、各ユーザ名にパスワードが割り当てられます。別の情報を特定のユーザ プロファイルに追加できます。追加可能な情報には、VPN 関連属性（VPN セッション タイムアウト値など）が含まれます。

フォールバック サポート

ローカル データベースは、複数の機能のフォールバック方式として動作できます。この動作は、セキュリティ アプライアンスから誤ってロックアウトされないようにすることを意図しています。

フォールバック サポートを必要とするユーザでは、ローカル データベース内のユーザ名とパスワードと AAA サーバ内のユーザ名とパスワードを一致させることをお勧めします。これにより、トランスペアレント フォールバック サポートが提供されます。ユーザは、AAA サーバとローカル データベースのどちらがサービスを提供しているかが判別できないので、ローカル データベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを AAA サーバで使用することは、指定するべきユーザ名とパスワードをユーザが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- コンソールおよびイネーブル パスワード認証：グループ内のサーバがすべて使用できない場合、セキュリティ アプライアンスはローカル データベースを使用して管理アクセスを認証します。これにもイネーブル パスワードの認証を含めることができます。
- コマンド許可：グループ内の TACACS+ サーバがすべて使用できない場合、特権レベルに基づいてコマンドを許可するためにローカル データベースが使用されます。
- VPN 認証および許可：VPN 認証および許可は、通常この VPN サービスをサポートしている AAA サーバが使用できない場合、セキュリティ アプライアンスへのリモート アクセスをイネーブルにするためにサポートされます。管理者の VPN クライアントが、ローカル データベースへのフォールバックに設定されたトンネル グループを指定する場合、AAA サーバ グループを利用できなくても、ローカル データベースに必要な属性が設定されていれば、VPN トンネルを確立できます。

ローカル データベースの設定

ここでは、ローカル データベース内のユーザの管理方法について説明します。ローカル データベースは、CLI アクセス認証、特権モード認証、コマンド許可、ネットワーク アクセス認証、および VPN 認証および許可に使用できます。ローカル データベースはネットワーク アクセス許可には使用できません。ローカル データベースはアカウンティングをサポートしません。

マルチコンテキスト モードの場合、システム実行スペースでユーザ名を設定し、**login** コマンドを使用して個々のログインを指定できます。しかし、システム実行スペースでは **aaa** コマンドは設定できません。

この項では、次のトピックについて取り上げます。

User Accounts

[User Accounts] ペインでは、ローカル ユーザ データベースを管理できます。次の各機能は、ローカル データベースを使用して実行されます。

- ASDM ユーザごとのアクセス

  デフォルトでは、ユーザ名のフィールドはブランクにしたまま、パスワードのフィールドにイネーブル パスワードを指定すれば ASDM にログインできます（「Device Name/Password」（P.10-12）を参照）。ただし、ログイン画面で（ユーザ名のフィールドをブランクにせず）ユーザ名とパスワードを入力すると、ASDM ではそれらを照合するためにローカル データベースのチェックが行われます。

（注）　ローカル データベースを使用する HTTP 認証を設定することもできますが、デフォルトではこの機能は常にイネーブルです。認証用に RADIUS または TACACS+ サーバを使用する場合は、HTTP 認証を設定するだけで済みます。

- コンソール認証
- Telnet 認証および SSH 認証
- enable コマンド認証

  この設定は、CLI アクセスにだけ使用され、ASDM ログインには影響しません。

- コマンド許可

  ローカル データベースを使用するコマンド許可を有効にすると、セキュリティ アプライアンスでは、ユーザ特権レベルを参照して、どのコマンドが使用できるかが特定されます。コマンド許可がディセーブルの場合は通常、特権レベルは参照されません。デフォルトでは、コマンドの特権レベルはすべて、0 または 15 のどちらかです。ASDM には、コマンドへの割り当てをイネーブルにできる特権レベルが事前に定義されています。割り当てることができるレベルは、15（管理）、5（読み取り専用）、3（監視専用）の 3 種類です。事前定義済みのレベルを使用する場合は、ユーザを 3 種類の特権レベルのいずれかに割り当てます。

- ネットワーク アクセス認証
- VPN クライアント認証

ローカル データベースはネットワーク アクセス許可には使用できません。

マルチ コンテキスト モードの場合、**login** コマンドを使用して CLI で個別のログインを入力できるように、システム実行スペースでユーザ名を設定できます。ただし、ローカル データベースを使用する **aaa** コマンドは、システム実行スペースでは設定できません。

（注）　VPN 機能は、マルチ コンテキスト モードではサポートされません。

（「Device Name/Password」（P.10-12）ではなく）このペインでイネーブル パスワードを設定するには、enable_15 ユーザのパスワードを変更します。ユーザ名 enable_15 は常時このペインに表示されます。これがデフォルトのユーザ名です。この方法は、ASDM のシステム コンフィギュレーションでイネーブル パスワードを設定する唯一の方法です。CLI で他のイネーブル レベル パスワード（**enable password 10** など）を設定すると、そのユーザ名は enable_10 という形式で表示されます。

フィールド

- [User Name]：これらのパラメータを適用するユーザ名を指定します。
- [Privilege (Level)]：そのユーザに割り当てる特権レベルを指定します。特権レベルは、ローカル コマンド許可で使用されます。
- [VPN Group Policy]：このユーザに対して VPN グループ ポリシーの名前を指定します。マルチ モードでは使用できません。
- [VPN Group Lock]：このユーザに対してグループ ロック ポリシー（ある場合）を指定します。マルチ モードでは使用できません。
- [Add]：[Add User Account] ダイアログボックスを表示します。
- [Edit]：[Edit User Account] ダイアログボックスを表示します。
- [Delete]：選択した行をテーブルから削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

[Add/Edit User Account] > [Identity]

ユーザが追加または変更するユーザ アカウントを識別するパラメータを指定するには、このペインを使用します。[OK] をクリックすると、[User Accounts] テーブルに変更内容がすぐに表示されます。

フィールド

- [Username]：このアカウントのユーザ名を指定します。
- [Change user password]：既存のユーザを編集する場合は、このボックスをオンにして、パスワードを変更します。

  - [Password]：このユーザの固有のパスワードを指定します。パスワードの最小長は 4 文字です。最大で 32 文字まで指定可能です。エントリは、大文字と小文字が区別されます。フィールドには、アスタリスクだけが表示されます。

    セキュリティを確保するために、パスワードの長さは 8 文字以上にすることを推奨します。
  - [Confirm Password]：確認のためにユーザ パスワードを再入力するよう求められます。フィールドには、アスタリスクだけが表示されます。

- [User authenticated using MSCHAP]：パスワードを入力後に unicode に変換し、MD4 を使用してハッシュすることを指定します。このオプションは、ユーザを MSCHAPv1 または MSCHAPv2 を使用して認証する場合に使用します。
- [Member-of]：ユーザが属する VPN グループを指定します。
  - [Member-of]：VPN グループの名前を入力します。
  - [Add]：リストに VPN グループを追加します。
  - [Delete]：リストから VPN グループを削除します。
- [Access Restriction]：このセクションでは、ユーザの管理アクセス レベルを設定します。まず、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] タブの [Perform authorization for exec shell access] オプションを使用して、管理許可をイネーブルにする必要があります。
  - [Full Access (ASDM, Telnet, SSH and console)]：ローカル データベースを使用した管理アクセスの認証を設定する場合（「CLI、ASDM、および enable コマンドの認証の設定」（P.13-27）を参照）、このオプションを指定するとユーザは ASDM、SSH、Telnet、およびコンソール ポートを使用できます。さらにイネーブル認証も設定すると、ユーザはグローバル コンフィギュレーション モードにアクセスできます。

    [Privilege Level]：ローカル コマンド許可でユーザに適用する特権レベルを選択します。範囲は、0（最低）～ 15（最高）です。詳細については、「ローカル コマンド許可の設定」（P.13-31）を参照してください。
  - [CLI login prompt for SSH, Telnet and console (no ASDM access)]：ローカル データベースを使用した管理アクセスの認証を設定する場合（「CLI、ASDM、および enable コマンドの認証の設定」（P.13-27）を参照）、このオプションを指定するとユーザは SSH、Telnet、およびコンソール ポートを使用できます。ユーザは設定に ASDM を使用できません（HTTP 認証を設定している場合）。ASDM 監視は可能です。さらにイネーブル認証も設定すると、ユーザはグローバル コンフィギュレーション モードにアクセスできません。
  - [No ASDM, SSH, Telnet, or console access]：ローカル データベースを使用した管理アクセスの認証を設定する場合（「CLI、ASDM、および enable コマンドの認証の設定」（P.13-27）を参照）、このオプションを指定すると、ユーザは認証用に設定した管理アクセス方式を利用できなくなります（ただし、[Serial] オプションは除きます。つまり、シリアル アクセスは許可されます）。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

[Add/Edit User Account] > [VPN Policy]

このペインを使用して、このユーザの VPN ポリシーを指定します。対応する設定がグループ ポリシーから値を取得するようにするには、[Inherit] チェックボックスをオンにします。

フィールド

- [Group Policy] : 使用可能なグループ ポリシーを示します。
- [Tunneling Protocols] : ユーザが使用できるトンネリング プロトコルを指定するか、またはグループ ポリシーから値を継承するかどうかを指定します。目的の [Tunneling Protocols] チェックボックスをオンにし、ユーザが使用できる VPN トンネリング プロトコルを選択します。ユーザは、選択されているプロトコルだけを使用できます。次の選択肢があります。

  [IPsec] : IP Security Protocol（IP セキュリティ プロトコル）。IPSec は、VPN トンネルのアーキテクチャをほぼ完全に実現しており、最もセキュアなプロトコルとされています。IPSec は、LAN 間（ピアツーピア）接続に使用することも、クライアントと LAN との接続に使用することもできます。

  [Clientless SSL VPN] : SSL/TLS を利用する VPN。Web ブラウザを使用して VPN コンセントレータへのセキュアなリモートアクセス トンネルを確立し、ソフトウェア クライアントもハードウェア クライアントも必要としません。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。

  [SSL VPN Client] : Cisco AnyConnect Client アプリケーションのダウンロード後にユーザが接続できるようにします。ユーザは、最初にクライアントレス SSL VPN 接続を使用してこのアプリケーションをダウンロードします。ユーザが接続するたびに、必要に応じてクライアント アップデートが自動的に行われます。

  [L2TP over IPSec] : 多くの PC やモバイル PC に採用されている一般的なオペレーティング システムに付属の VPN クライアントを使用するリモート ユーザが、パブリック IP ネットワークを介してセキュリティ アプライアンスおよびプライベート企業ネットワークへのセキュアな接続を確立できるようにします。

  （注） プロトコルを選択しなかった場合は、エラー メッセージが表示されます。

- [Filter] : 使用するフィルタを指定するか、またはグループ ポリシーの値を継承するかどうかを指定します。フィルタは、セキュリティ アプライアンスを経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。フィルタおよびルールを設定する場合は、[Configuration] > [VPN] > [VPN General] > [Group Policy] ペインを参照してください。
- [Manage] : アクセス コントロール リスト（ACL）と拡張アクセス コントロール リスト（ACE）を追加、編集、および削除できる [ACL Manager] ペインを表示します。
- [Tunnel Group Lock] : トンネル グループ ロックがある場合、それを継承するかどうか、または選択したトンネル グループ ロックを使用するかどうかを指定します。特定のロックを選択すると、ユーザのリモート アクセスはこのグループだけに制限されます。[Tunnel Group Lock] では、VPN クライアントで設定されたグループと、そのユーザが割り当てられているグループが同じかどうかをチェックすることによって、ユーザが制限されます。同一ではなかった場合、セキュリティ アプライアンスはユーザによる接続を禁止します。[Inherit] チェックボックスがオフの場合、デフォルト値は [--None--] です。

- [Store Password on Client System]：この設定をグループから継承するかどうかを指定します。[Inherit] チェックボックスをオフにすると、[Yes] および [No] のオプション ボタンが有効になります。[Yes] を選択すると、ログイン パスワードがクライアント システムに保存されます（セキュリティが低下するおそれのあるオプションです）。[No]（デフォルト）を選択すると、ユーザは接続するたびにパスワードの入力を求められます。セキュリティを最大限に確保するためにも、パスワードの保存は*許可しない*ことをお勧めします。VPN 3002 の場合、このパラメータは、対話型ハードウェア クライアント認証や個別ユーザ認証には適用されません。
- [Connection Settings]：接続設定パラメータを指定します。
  - [Access Hours]：[Inherit] チェックボックスがオフになっている場合、このユーザに適用されるアクセス時間ポリシーがすでに存在する場合にはその名前を選択でき、存在しない場合には、新しいアクセス時間ポリシーを作成できます。デフォルト値は [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルト値は [--Unrestricted--] です。
  - [New]：[Add Time Range] ダイアログボックスが開きます。このダイアログボックスでアクセス時間の新規セットを指定できます。
  - [Simultaneous Logins]：[Inherit] チェックボックスがオフになっている場合、このパラメータには、このユーザに許可される同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザ アクセスを禁止します。

    （注） 最大数の制限はありませんが、複数の同時接続の許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

  - [Maximum Connect Time]：[Inherit] チェックボックスがオフになっている場合、このパラメータには、ユーザの最大接続時間を分単位で指定します。ここで指定した時間が経過すると、システムは接続を終了します。最短時間は 1 分、最長時間は 2147483647 分（4000 年超）です。接続時間を無制限にする場合は、[Unlimited] チェックボックスをオンにします（デフォルト）。
  - [Idle Timeout]：[Inherit] チェックボックスがオフになっている場合、このパラメータには、ユーザのアイドル タイムアウト時間を分単位で指定します。この期間、ユーザ接続に通信アクティビティがなかった場合、システムは接続を終了します。最短時間は 1 分で、最長時間は 10080 分です。この値は、クライアントレス SSL VPN 接続のユーザには適用されません。
- 専用 IP アドレス（任意）：
  - [IP Address] ボックス：オプションの専用 IP アドレスを指定します。
  - [Subnet Mask] リスト：専用 IP アドレスのサブネット マスクを指定します。

このグループだけによるリモート アクセスにユーザを制限するには、[Group Lock] チェックボックスをオンにします。[Group Lock] では、VPN クライアントで設定されたグループと、そのユーザが割り当てられているグループが同じかどうかをチェックすることによって、ユーザが制限されます。一致していない場合、VPN コンセントレータによりユーザは接続できなくなります。

このボックスがオフ（デフォルト）の場合、ユーザは、割り当てられているグループに関係なく認証されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

AAA サーバ グループおよびサーバの識別

認証、許可、またはアカウンティングに外部 AAA サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの AAA サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバ グループは名前で識別されます。各サーバ グループは、Kerberos、LDAP、NT、RADIUS、SDI、または TACACS+ というサーバの 1 つのタイプ専用となります。

セキュリティ アプライアンス は、グループ内の最初のサーバと通信します。最初のサーバが使用できない場合、セキュリティ アプライアンス はグループ内の次のサーバ（設定されている場合）と通信します。グループ内のすべてのサーバが使用できない場合、セキュリティ アプライアンスは、ローカル データベースがフォールバック方式として設定されていると、ローカル データベースに接続しようとします（管理認証および許可限定）。フォールバック方式として設定されていない場合、セキュリティ アプライアンスは引き続き AAA サーバにアクセスしようとします。

この項では、次のトピックについて取り上げます。

- 「AAA Server Groups」（P.12-13）
- 「Add/Edit AAA Server Group」（P.12-15）
- 「Edit AAA Local Server Group」（P.12-16）
- 「Add/Edit AAA Server」（P.12-16）
- 「Test AAA Server」（P.12-22）

AAA Server Groups

[AAA Server Groups] ペインでは、次のことを実行できます。

- 各グループで示されているサーバと通信するように、セキュリティ アプライアンスが使用する AAA サーバ グループおよびプロトコルを設定します。
- 個々のサーバを設定して、AAA サーバ グループに追加します。

シングル モードで最大 15 のグループ、またはマルチ モードで最大 4 つのグループを含めることができます。各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。ユーザがログインすると、指定した最初のサーバから順に、サーバが応答するまでこれらのサーバが一度に 1 つずつアクセスされます。

AAA アカウンティングが有効の場合、同時アカウンティングをイネーブルにしない限り、アカウンティング情報はアクティブなサーバにのみ送信されます。

AAA サービスの概要については、「AAA の概要」（P.12-1）を参照してください。

フィールド

[AAA Server Groups] ペインのフィールドは 2 つの主要領域（[AAA Server Groups] 領域と [Servers In The Selected Group] 領域）にグループ化されます。[AAA Server Groups] 領域では、AAA サーバ グループ、およびセキュリティ アプライアンスが各グループに示されたサーバとの通信に使用するプロトコルを設定できます。

（注）　[AAA Server Groups] テーブルの行をダブル クリックすると、AAA サーバ グループのパラメータを変更できる [Edit AAA Server Group] ダイアログボックスが開きます。ここで行った変更はただちにテーブルに反映されますが、コンフィギュレーションに保存するには [Apply] をクリックする必要があります。

カラム ヘッダーをクリックすると、そのカラムの内容に従ってテーブル行が英数字順にソートされます。

- [Server Group]：*表示専用*。選択したサーバ グループのシンボリック名を表示します。
- [Protocol]：*表示専用*。グループ内のサーバによってサポートされる AAA プロトコルを一覧表示します。
- [Accounting Mode]：*表示専用*。同時またはシングル モード アカウンティングを表示します。シングル モードでは、セキュリティ アプライアンスはアカウンティング データを 1 つのサーバにだけ送信します。同時モードでは、セキュリティ アプライアンスはアカウンティング データをグループ内のすべてのサーバに送信します。
- [Reactivation Mode]：*表示専用*。障害が発生したサーバを再アクティブ化する方法を [Depletion] または [Timed] 再アクティブ化モードから指定します。[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。
- [Dead Time]：*表示専用*。グループの最後のサーバがディセーブルになってから、すべてのサーバを次に再度イネーブルにするまでの経過時間を分単位で示します。このパラメータは Depletion モードにだけ適用されます。
- [Max Failed Attempts]：*表示専用*。応答しないサーバが非アクティブであると宣言するまでの失敗接続試行回数を示します。
- [Add] : [Add AAA Server Group] ダイアログボックスを表示します。
- [Edit] : [Edit AAA Server Group] ダイアログボックスを表示するか、サーバ グループとして [LOCAL] を選択した場合は [Edit AAA Local Server Group] ダイアログボックスを表示します。
- [Delete]：サーバ グループ テーブルから、現在選択されているサーバ グループ エントリを削除します。確認されず、やり直しもできません。

[AAA Server Groups] ペインの 2 番目の領域である [Servers In Selected Group] 領域では、既存の AAA サーバ グループに AAA サーバを追加および設定することができます。サーバは、RADIUS、TACACS+、NT、SDI、Kerberos、LDAP、または HTTP Form サーバです。

- [Server Name or IP Address]：*表示専用*。AAA サーバの名前または IP アドレスを表示します。
- [Interface]：*表示専用*。認証サーバが存在するネットワーク インターフェイスを表示します。
- [Timeout]：*表示専用*。タイムアウトの間隔（秒）を表示します。この時間を超えると、セキュリティ アプライアンスはプライマリ AAA サーバへの要求を断念します。スタンバイ AAA サーバが存在する場合、セキュリティ アプライアンスは要求をそのバックアップ サーバに送信します。
- [Add/Edit] : [Add/Edit AAA Server] ダイアログボックスを表示します。
- [Delete]：選択した AAA サーバをリストから削除します。

- [Move up]：選択した AAA サーバを AAA シーケンス内で上に移動します。
- [Move down]：選択した AAA サーバを AAA シーケンス内で後ろに移動します。
- [Test]：[Test AAA Server] ダイアログボックスを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	• [1]	•	•	—

1. HTTP Form とクライアントレス SSL VPN は、シングル ルーテッド モードだけでサポートされます。

Add/Edit AAA Server Group

[Add/Edit AAA Server Group] ダイアログボックスでは、AAA サーバ グループを追加または変更できます。結果は、[AAA Server] テーブルに表示されます。

フィールド

- [Server Group]：*表示専用*。選択したサーバ グループの名前を表示します。
- [Protocol] ドロップダウン リスト：グループのサーバでサポートされるプロトコルを指定します。これらには、RADIUS、TACACS+、NT ドメイン、SDI、Kerberos、LDAP、およびシングル サイン オン用 HTTP Form（クライアントレス SSL VPN のユーザ専用）があります。

（注） 次のフィールドは、[HTTP Form] プロトコルを選択すると使用できなくなります。

- [Accounting Mode]：サーバ グループに使用するアカウンティング モードを指定します。
  - [Simultaneous]：アカウンティング データをグループ内のすべてのサーバに送信するようにセキュリティ アプライアンスを設定します。
  - [Single]：アカウンティング データをグループ内の 1 つのサーバだけに送信するようにセキュリティ アプライアンスを設定します。
- [Reactivation Mode]：障害が発生したサーバを再アクティブ化する方法を指定します。
  - [Depletion]：グループ内のすべてのサーバが非アクティブになった後にのみ、障害の発生したサーバを再アクティブ化するようにセキュリティ アプライアンスを設定します。
  - [Timed]：障害が発生したサーバを 30 秒の停止時間の後に再アクティブ化するようにセキュリティ アプライアンスを設定します。
- [Dead Time]：グループの最後のサーバがディセーブルになってから、すべてのサーバを次に再度イネーブルにするまでの経過時間を分単位で指定します。このフィールドは、Timed モードでは使用できません。
- [Max Failed Attempts]：応答しないサーバが非アクティブであると宣言するまでの失敗接続試行回数（1 ～ 5）を指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	• [1]	•	•	—

1. HTTP Form とクライアントレス SSL VPN は、シングル ルーテッド モードだけでサポートされます。

Edit AAA Local Server Group

[Edit AAA Local Server Group] ダイアログボックスでは、ローカル ユーザ ロックアウトをイネーブルにするかどうか、また、ユーザをロックアウトする前に許可するログイン試行の最大失敗回数を指定します。ユーザがロックアウトされた場合、正常にログインするには、管理者がロックアウト状態をクリアしておく必要があります。

フィールド

- [Enable Local User Lockout]：設定された認証試行の最大失敗回数を超えたユーザのロックアウトと、そのユーザのアクセス拒否をイネーブルにします。
- [Maximum Attempts]：ユーザをロックアウトし、そのユーザのアクセスを拒否する前に許可するログイン試行の最大失敗回数を指定します。この制限は、LOCAL データベースが認証に使用されているときにのみ適用されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	• [1]	•	•	—

1. HTTP Form とクライアントレス SSL VPN は、シングル ルーテッド モードだけでサポートされます。

Add/Edit AAA Server

[Add/Edit AAA Server] ダイアログボックスでは、既存の AAA サーバのパラメータを変更したり、AAA サーバ グループ テーブルで選択した既存のグループに新しい AAA サーバを追加したりできます。

フィールド

（注）　最初の 4 つのフィールドは、すべてのサーバ タイプに共通です。コンテンツ領域は、各サーバ タイプに固有です。

- [Server Group]：*表示専用*。サーバ グループの名前を示します。
- [Interface Name]：サーバが常駐するネットワーク インターフェイスを指定します。
- [Server Name or IP Address]：AAA サーバの名前または IP アドレスを指定します。
- [Timeout]：タイムアウト間隔を秒単位で指定します。この時間を超えると、セキュリティ アプライアンスはプライマリ AAA サーバへの要求を断念します。スタンバイ AAA サーバが存在する場合、セキュリティ アプライアンスは要求をそのバックアップ サーバに送信します。
- [RADIUS Parameters] 領域：RADIUS サーバの使用に必要なパラメータを指定します。この領域は、選択したサーバ グループが RADIUS を使用するときにのみ表示されます。
  - [Retry Interval]：サーバにクエリーを送信しても応答がないときに、接続を再試行する前に待機する秒数を指定します。最短時間は 1 秒です。デフォルトの時間は 10 秒です。最長時間は 10 秒です。
  - [Server Authentication Port]：ユーザ認証に使用するサーバ ポートを指定します。デフォルトのポートは 1645 です。

（注）　最新の RFC では、RADIUS を UDP ポート番号 1812 に設定すべきだとしているので、このデフォルト値を 1812 に変更する必要がある場合があります。

  - [Server Accounting Port]：ユーザ認証に使用するサーバ ポートを指定します。デフォルトのポートは 1646 です。
  - [Server Secret Key]：暗号化に使用する、たとえば C8z077f のようなサーバ秘密キー（共有秘密とも呼ばれる）を指定します。秘密キーでは大文字と小文字が区別されます。セキュリティ アプライアンスはサーバ秘密キーを使用して、RADIUS サーバに対する認証を行います。ここで設定したサーバ秘密キーは、RADIUS サーバで設定されたサーバ秘密キーと一致する必要があります。RADIUS サーバのサーバ秘密キーがわからない場合は、RADIUS サーバの管理者に問い合わせてください。最大フィールド長は、64 文字です。
  - [Common Password]：グループの共通パスワードを指定します。パスワードでは大文字と小文字が区別されます。RADIUS サーバを許可ではなく認証に使用するよう定義する場合は、共通パスワードを設定しないでください。

    RADIUS 許可サーバでは、各接続ユーザに対してパスワードおよびユーザ名が必要です。ここでは、パスワードを入力します。RADIUS 許可サーバ管理者は、このセキュリティ アプライアンス経由で RADIUS サーバに対して許可を行う各ユーザにこのパスワードが関連付けられるように RADIUS サーバを設定する必要があります。この情報は、RADIUS サーバ管理者に伝えてください。このセキュリティ アプライアンス経由で RADIUS 許可サーバにアクセスするすべてのユーザの共通パスワードを入力します。

    このフィールドを空白のままにすると、各ユーザのユーザ名がパスワードになります。たとえば、ユーザ名が「jsmith」であるユーザの場合、「jsmith」と入力されます。セキュリティ上の予防措置として、RADIUS 許可サーバを絶対に認証に使用しないでください。共通パスワードを使用したり、パスワードとしてユーザ名を使用したりすることは、ユーザごとに強力なパスワードを使用するのに比べてはるかにセキュリティが低くなります。

（注）　パスワード フィールドは RADIUS プロトコルに必要であり、RADIUS サーバが要求しますが、ユーザがこのフィールドを認識する必要はありません。

- [ACL Netmask Convert] : ダウンロード可能なアクセス リストから受け取ったネットマスクをセキュリティ アプライアンスが処理する方法を指定します。セキュリティ アプライアンスは、ダウンロード可能なアクセス リストに標準ネットマスク表現が含まれていることを想定しますが、Cisco Secure VPN 3000 シリーズ コンセントレータは、ダウンロード可能なアクセス リストに、標準ネットマスク表現とは反対のワイルドカード ネットマスク表現が含まれていることを想定します。ワイルドカード マスクには、無視するビット位置に 1 が、一致するビット位置に 0 が入っています。[ACL Netmask Convert] リストは、RADIUS サーバ上でのダウンロード可能なアクセス リストの設定方法の違いによる影響を最小限に抑えます。

  [Detect automatically] を選択すると、使用されているネットマスク表現のタイプをセキュリティ アプライアンスが判定します。ワイルドカード ネットマスク表現が検出された場合は、標準のネットマスク表現に変換されます。しかし、一部のワイルドカード表現は明確な検出が困難であるため、この設定を使用すると、ワイルドカード ネットマスク表現が、標準のネットマスク表現と誤解される場合があります。

  [Standard] を選択すると、セキュリティ アプライアンスは、RADIUS サーバから受け取ったダウンロード可能なアクセス リストに、標準ネットマスク表現だけが入っていると想定します。ワイルドカード ネットマスク表現からの変換は実行されません。

  [Wildcard] を選択すると、セキュリティ アプライアンスは、RADIUS サーバから受け取ったダウンロード可能なアクセス リストに、ワイルドカード ネットマスク表現だけが含まれていると想定し、アクセス リストがダウンロードされたときにすべてを標準ネットマスク表現に変換します。

- [SDI Messages Table] : SDI サーバへのプロキシとして設定された RADIUS サーバによってセキュリティ アプライアンスに転送される SDI メッセージを指定します。

  リモート ユーザが AnyConnect VPN クライアントでセキュリティ アプライアンスに接続し、RSA SecurID トークンを使用して認証を試みると、セキュリティ アプライアンスは RADIUS サーバと通信を行い、次に、RADIUS サーバは認証のために SDI サーバと通信を行います。[SDI message] テーブルには、セキュリティ アプライアンスが認識し、リモート クライアントに渡される SDI メッセージが示されます。

  表 12-1 に、SDI メッセージ（操作コード）、デフォルトのメッセージ テキスト、および各メッセージの機能を示します。

表 12-2　SDI 操作コード、デフォルトのメッセージ テキスト、およびメッセージの機能

SDI 操作コード	デフォルトの SDI メッセージ テキスト	メッセージ機能
next-code	Enter Next PASSCODE	ユーザは PIN を入力せずに次のトークンコードを入力する必要があることを示します。
new-pin-sup	Please remember your new PIN	新しいシステムの PIN が提供されており、ユーザにその PIN を表示することを示します。
new-pin-meth	Do you want to enter your own pin	新しい PIN の作成にどの新しい PIN 方式を使用するかをユーザに尋ねます。
new-pin-req	Enter your new Alpha-Numerical PIN	ユーザ生成の PIN を入力することを要求することを示します。

SDI 操作コード	デフォルトの SDI メッセージ テキスト	メッセージ機能
new-pin-reenter	Reenter PIN:	ユーザが提供した PIN の確認のためにセキュリティ アプライアンスが内部的に使用します。ユーザにプロンプトを表示せずに、クライアントが PIN を確認します。
new-pin-sys-ok	New PIN Accepted	ユーザが提供した PIN が受け入れられたことを示します。
next-ccode-and-reauth	new PIN with the next card code	PIN 操作後、次のトークンコードを待ってから、認証のために新しい PIN と次のトークンコードの両方を入力する必要があることをユーザに示します。
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN	ユーザがシステム生成の PIN に対する準備ができていることを示すためにセキュリティ アプライアンスが内部的に使用します。

SDI メッセージは SDI サーバ上で設定が可能なため、セキュリティ アプライアンス上の SDI メッセージのメッセージ テキストは、SDI サーバ上のメッセージに一致する必要があります。一致しない場合、リモート クライアント ユーザに表示されるプロンプトは、認証中に必要とされるアクションに対して適切でない場合があります。そのため、AnyConnect クライアントが応答できずに、認証が失敗する可能性があります。

セキュリティ アプライアンスは、表 12-1 に表示される順番に文字列を検索するため、操作コードに使用する文字列が、別の文字列のサブセットでないようにする必要があります。たとえば、new-pin-req を「New PIN」として、および new-pin-sys-ok を「New PIN Accepted」として設定すると、new-pin-req は、そのメッセージ テキストが「New PIN Accepted」のサブセットであるため、常に一致するようになります。このため、メッセージ テキストは、誤った一致を発生させることがない一意のものとする必要があります。

メッセージ テキストを編集するには、[Message Text] フィールドをダブルクリックします。

[Restore default message texts]：メッセージをデフォルトのメッセージ（Cisco ACS のデフォルト メッセージ）に復元します。

- [TACACS+ Parameters]：TACACS+ サーバの使用に必要なパラメータを指定します。この領域は、選択したサーバ グループが TACACS+ を使用するときにのみ表示されます。
  - [Server Port]：使用するサーバ ポートを指定します。
  - [Server Secret Key]：暗号化に使用するサーバ秘密キーを指定します。秘密キーでは大文字と小文字が区別されます。フィールドには、アスタリスクだけが表示されます。
- [SDI Parameters]：SDI サーバの使用に必要なパラメータを指定します。この領域は、選択したサーバ グループが SDI を使用するときにのみ表示されます。
  - [Server Port]：使用するサーバ ポートを指定します。
  - [Retry Interval]：接続を再試行する前に待機する秒数を指定します。
- [Kerberos Parameters]：Kerberos サーバの使用に必要なパラメータを指定します。この領域は、選択したサーバ グループが Kerberos を使用するときにのみ表示されます。
  - [Server Port]：Kerberos サーバがリッスンするサーバ ポートを指定します。
  - [Retry Interval]：再試行間隔値とは、再試行から次の再試行までの時間であり、1 ～ 10 秒の範囲で指定します。

  - [Kerberos Realm]：使用する Kerberos レルムの名前（USDOMAIN.ACME.COM など）を指定します。最大長は、64 文字です。サーバ タイプが Windows 2000、Windows XP、および Windows.NET の場合、領域名はすべて大文字で入力する必要があります。ここに入力する名前は、[Server IP Address] フィールドに IP アドレスを入力したサーバの領域名に一致している必要があります。

- [LDAP Parameters]：LDAP サーバの使用に必要なパラメータを指定します。この領域は、選択したサーバ グループが LDAP を使用するときにのみ表示されます。
  - [Enable LDAP Over SSL]：セキュリティ アプライアンスと LDAP サーバ間の通信を SSL でセキュリティ保護するように指定します。セキュア LDAP とも呼ばれます。
  - [Server Port]：使用するサーバ ポートを指定します。サーバにアクセスするための TCP ポート番号を入力します。
  - [Server Type]：手動で LDAP サーバ タイプを設定するか、または、サーバ タイプの判別に自動検出を指定します。
  - [Base DN]：ベース DN を指定します。許可要求を受信したときに、サーバが検索を開始する LDAP 階層の位置を入力します。たとえば、`OU=people, dc=cisco, dc=com` となります。
  - [Scope]：サーバが許可要求を受け取ったときに行う、LDAP 階層での検索範囲を指定します。[One Level]（ベース DN の下にある 1 レベルのみを検索します。このオプションは高速です）および [All Levels]（ベース DN の下にあるすべてのレベルを検索します。つまり、サブツリー階層全体を検索します。このオプションは、時間がかかります）。
  - [Naming Attribute(s)]：LDAP サーバのエントリを一意に識別する相対識別名属性（複数可）を指定します。共通の命名属性は、一般名（cn）とユーザ ID（uid）です。
  - [Login DN]：ログイン DN を指定します。一部の LDAP サーバ（Microsoft Active Directory サーバなど）は、セキュリティ アプライアンスに対し、他のあらゆる LDAP 操作の要求を受け入れる前に、認証済みバインディングを介してハンドシェイクを確立することを要求します。セキュリティ アプライアンスは、ログイン DN フィールドをユーザ認証要求にアタッチして、認証済みバインディングに対して識別情報を示します。[Login DN] フィールドでは、セキュリティ アプライアンスの認証特性を定義します。これらの特性は、管理者の権限が与えられているユーザの特性に対応します。セキュリティ アプライアンスの認証済みバインディングのディレクトリ オブジェクト名を入力します。たとえば、cn=Administrator, cn=users, ou=people, dc=Example Corporation, dc=com となります。匿名アクセスの場合は、このフィールドをブランクのままにします。
  - [Login Password]：ログイン パスワードを指定します。入力した文字はアスタリスクに置き換えられます。
  - [LDAP Attribute Map]：LDAP サーバに適用可能な LDAP 属性マップを一覧表示します。LDAP 属性マップでは、Cisco 属性名をユーザ定義の属性名および値に変換します。
  - [SASL MD5 authentication]：Simple Authentication and Security Layer の MD5 メカニズムが、セキュリティ アプライアンスと LDAP サーバ間の認証通信をセキュリティ保護するように指定します。
  - [SASL Kerberos authentication]：Simple Authentication and Security Layer の Kerberos メカニズムが、セキュリティ アプライアンスと LDAP サーバ間の認証通信をセキュリティ保護するように指定します。
  - [Kerberos Server Group]：認証に使用する Kerberos サーバまたはサーバ グループを指定します。[Kerberos Server Group] オプションはデフォルトでディセーブルになっており、SASL Kerberos 認証が選択された場合だけイネーブルになります。

- [NT Domain Parameters]：NT サーバの使用に必要なパラメータを指定します。次のフィールドがあります。

- [Server Port]：ユーザがサーバにアクセスする TCP ポート番号を指定します。デフォルト ポート番号は、139 です。
- [NT Domain Controller]：このサーバの NT プライマリ ドメイン コントローラのホスト名（PDC01 など）を指定します。ホスト名の最大長は 15 文字です。ここに入力する名前は、[Authentication Server Address] に IP アドレスを入力したサーバのホスト名に一致している必要があります。名前が正しくないと、認証が失敗します。

• [HTTP Form Parameters]：シングル サインオン認証用に HTTP Form プロトコルのパラメータを指定します。クライアントレス SSL VPN のユーザのみが使用できます。この領域は、選択したサーバ グループが HTTP Form を使用しているときにのみ表示され、サーバ グループ名とプロトコルのみが表示されます。HTTP Form を使用している場合、他のフィールドは使用できません。

（注） HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

次のパラメータが不明の場合は、セキュリティ アプライアンス を介さず認証 Web サーバへ直接ログインしているときに、HTTP ヘッダー アナライザを使用して GET および POST による HTTP 交換からデータを抽出します。これらのパラメータを HTTP 交換から抽出する方法については、『*Cisco Security Appliance Command Line Configuration Guide*』のクライアントレス SSL VPN に関する章を参照してください。

- [Start URL]：事前ログイン クッキーが取得できる認証 Web サーバの場所を表す完全 URL を指定します。このパラメータは、ログイン ページとともに事前ログイン クッキーが認証 Web サーバへロードされる場合以外は、設定する必要はありません。ドロップダウン リストには、HTTP と HTTPS の両方が表示されます。入力できる最大文字数は 1024 文字で、最小文字数の制限はありません。
- [Action URI]：許可 Web サーバ上の認証プログラムの完全 Uniform Resource Identifier を指定します。URI 全体の最大文字数は、2048 文字です。
- [Username]：SSO 認証に使用される HTTP Form の一部として送信する必要があるユーザ名パラメータの名前（特定のユーザ名ではありません）を指定します。入力できる最大文字数は 128 文字で、最少文字数の制限はありません。
- [Password]：SSO 認証に使用される HTTP Form の一部として送信する必要があるユーザ パスワード パラメータの名前（特定のパスワード値ではありません）を指定します。入力できる最大文字数は 128 文字で、最少文字数の制限はありません。
- [Hidden Values]：SSO 認証用として認証 Web サーバに送信される HTTP POST 要求の非表示パラメータを指定します。HTTP POST 要求内に含まれることからもわかるように、このパラメータは認証 Web サーバから要求があった場合に限り必要となります。入力できる最大文字数は 2048 文字です。
- [Authentication Cookie Name]：（任意）正常にログインが行われた際、サーバによって認証情報を保存するために設定されるクッキーの名前を指定します。Web サーバから返される他のクッキーと区別しやすいよう、認証クッキーに対して意味のある名前を割り当てる場合に使用されます。入力できる最大文字数は 128 文字で、最少文字数の制限はありません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	• [1]	•	• [1.]	—

1. HTTP Form とクライアントレス SSL VPN は、シングル ルーテッド モードだけでサポートされます。

Test AAA Server

（注）　HTTP Form 認証サーバでは、[Test AAA Server] は使用できません。

セキュリティ アプライアンスが選択した AAA サーバと通信できるかどうかを判別するには、[Test] ボタンを使用します。AAA サーバに到達できない場合は、ASDM での設定が正しくないか、ネットワーク設定による制限やサーバのダウンタイムなど他に AAA サーバに到達できない原因があることが考えられます。

このダイアログボックスのフィールドに入力して [OK] をクリックすると、セキュリティ アプライアンスは適切なテスト メッセージを選択したサーバに送信します。テストが失敗した場合、ASDM は、発生したエラー タイプに関するエラー メッセージを表示します。ASDM のエラー メッセージで設定エラーが示されている場合、設定を修正してから再度テストします。

ヒント　トラブルシューティングを行うとき、AAA サーバへの基本的なネットワーク接続を確認することをお勧めします。基本的な接続をテストするには、[Tools] > [Ping] をクリックします。

フィールド

- [AAA Server Group] : *表示専用*。選択した AAA サーバが属する AAA サーバ グループを表示します。
- [Host] : *表示専用*。選択した AAA サーバのホスト名を表示します。
- [Authorization] : ASDM が選択した AAA サーバを使用したユーザの認証をテストするように指定します。選択したサーバ タイプが許可をサポートしていない場合、このオプション ボタンは使用できません。たとえば、セキュリティ アプライアンスは Kerberos サーバを使用した許可をサポートできません。
- [Authentication] : ASDM が選択した AAA サーバを使用したユーザの認証をテストするように指定します。選択したサーバ タイプが認証をサポートしていない場合、このオプション ボタンは使用できません。たとえば、セキュリティ アプライアンスは LDAP サーバを使用した認証をサポートしていません。
- [Username] : AAA サーバのテストに使用するユーザ名を指定します。ユーザ名が AAA サーバに存在することを確認してください。存在しないと、テストは失敗します。
- [Password] : [Username] フィールドに入力したユーザ名のパスワードを指定します。[Password] フィールドは、認証テストにのみ使用できます。入力したユーザ名に対してパスワードが正しいことを確認します。正しくない場合、認証テストは失敗します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	• [1]	•	•	—

1. HTTP Form とクライアントレス SSL VPN は、シングル ルーテッド モードだけでサポートされます。

認証プロンプトの設定

[Authentication Prompt] ペイン（[Configuration] > [Device Management] > [Users/AAA]）では、AAA 認証チャレンジ プロセス中にユーザに対して表示されるテキストを指定できます。TACACS+ または RADIUS サーバからのユーザ認証を要求するとき、セキュリティ アプライアンス経由の HTTP、FTP、および Telnet アクセスに AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワード プロンプトの上に表示されます。

Telnet からのユーザ認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証試行が AAA サーバにより受け入れられた、または拒否されたことを示すさまざまな状態のプロンプトを表示できます。

これらのメッセージ テキストをそれぞれ指定した場合、セキュリティ アプライアンスでは、AAA サーバにより認証されたユーザに対してはユーザ承認メッセージ テキストが表示され、認証されなかったユーザに対してはユーザ拒否メッセージ テキストが表示されます。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストのみが表示されます。ユーザ承認メッセージ テキストおよびユーザ拒否メッセージ テキストは表示されません。

（注） Microsoft Internet Explorer では、認証プロンプトに最大 37 文字表示されます。Telnet および FTP では、認証プロンプトに最大 235 文字表示されます。

フィールド

- [Prompt]：（任意）セキュリティ アプライアンスを経由したユーザ セッションに対して、チェックボックスの下のフィールドに指定した AAA チャレンジ テキストの表示をイネーブルにします。
- [Text]：（任意）235 文字までの英数字または 31 ワードまでの文字列を指定します。いずれかの最大値に達したときに制限されます。特殊文字は使用できませんが、スペースと句読点は使用できます。疑問符を入力するか、または Enter キーを押すと、ストリングが終了します（疑問符はストリングに含まれます）。
- [User accepted message]：（任意）チェックボックスの下のフィールドで指定した、ユーザが認証されたことを確認するテキストの表示をイネーブルにします。
- [User rejected message]：（任意）チェックボックスの下のフィールドで指定した、認証が失敗したことを示すテキストの表示をイネーブルにします。

（注）　このペインのフィールドはすべてオプションです。認証プロンプトを指定していない場合、FTP ユーザには「FTP authentication」が、HTTP ユーザには「HTTP Authentication」が表示され、Telnet ユーザにはチャレンジ テキストが表示されません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

LDAP 属性マップの設定

[LDAP Attribute Map] ペイン（[Configuration] > [Remote Access VPN] > [AAA Setup]）では、カスタマー（ユーザ定義）属性名をシスコの LDAP 属性名にマッピングするための属性マップを作成し、名前を付けることができます。既存の LDAP ディレクトリにセキュリティ アプライアンスを導入する場合、既存のカスタマー LDAP 属性の名前および値は、シスコ属性の名前および値とは異なる場合があります。既存の属性の名前を変更するのではなく、カスタマー属性名と値をシスコ属性名と値にマッピングする、LDAP 属性マップを作成できます。簡単な文字列の置き換えを使用すると、セキュリティ アプライアンスがユーザ独自のカスタマー名および値のみを提供するようになります。

次に、ユーザは、必要に応じてこれらの属性マップを LDAP サーバにバインドしたり、削除したりできます。属性マップ全体を削除したり、名前および値の個々のエントリを削除したりできます。

（注）　属性マッピング機能を適切に使用するには、シスコの LDAP 属性の名前と値およびユーザ定義の属性の名前と値を理解する必要があります。

フィールド

- [Name]：編集可能な LDAP 属性マップの名前を表示します。
- [Attribute Map Name]：各属性マップ内にある、カスタマー属性名からシスコ属性名へのマッピングを表示します。
- [Add]：[Add LDAP Attribute Map] ダイアログボックスを表示します。
- [Edit]：[Edit LDAP Attribute Map] ダイアログボックスを表示します。
- [Delete]：選択した LDAP 属性マップを削除します。

Add/Edit LDAP Attribute Map

[Add/Edit LDAP Attribute Map] ダイアログボックスでは、既存の LDAP 属性マップの変更または削除、新しい LDAP 属性マップの追加、および属性マップへの属性名と値のマッピングの入力を行うことができます。

[LDAP Attribute Map] ダイアログボックスを使用した新しい属性マップの標準的な追加手順は次のとおりです。

1. 新しい、何も入力されていない属性マップを作成します。
2. シスコ属性名をカスタマー（ユーザ定義）属性名に変換する名前マッピングを、属性マップに入力します。
3. カスタマー（ユーザ定義）属性の値をカスタマー属性名、および一致するシスコ属性名と値に適用する値マッピングを、属性マップに入力します。

次に、[Add/Edit AAA Server] ダイアログボックスを使用して LDAP サーバを追加または編集するときに、その属性マップを LDAP サーバにバインドします。

フィールド

- [Name]：追加または編集する LDAP 属性マップの名前を指定します。新しいマップを追加する場合、このフィールドにマップの名前を入力します。[LDAP Attribute Map] ペインで選択したマップを編集する場合は、選択したマップの名前がこのフィールドに読み取り専用テキストとして表示されます。マップを変更するには、[LDAP Attribute Map] ペインに戻り、目的のマップを選択する必要があります。
- [Name Map]：カスタマー属性名をシスコ属性名にマッピングするのに必要なフィールドを表示します。
- [Value Map]：カスタマー属性の値を、カスタマー属性名、および一致するシスコの属性名と値にマッピングするのに必要なフィールドを表示します。

[Add/Edit LDAP Attribute Map] > [Map Name] タブ

[Add/Edit LDAP Attribute Map] ダイアログボックスでは、既存の LDAP 属性マップの変更または削除、新しい LDAP 属性マップの追加、および属性マップへの属性名と値のマッピングの入力を行うことができます。「Add/Edit LDAP Attribute Map」も参照してください。

一部のフィールドは [Map Name] タブを選択するか、[Map Value] タブを選択するかによって異なります。[Map Name] タブをクリックした場合、次のフィールドが表示されます。

フィールド

- [Name]：追加または編集する LDAP 属性マップの名前を指定します。新しいマップを追加する場合、このフィールドにマップの名前を入力します。[LDAP Attribute Map] ペインで選択したマップを編集する場合は、選択したマップの名前がこのフィールドに読み取り専用テキストとして表示されます。マップを変更するには、[LDAP Attribute Map] ペインに戻り、目的のマップを選択する必要があります。
- [Customer Name]：[Cisco Name] ドロップダウン リストから選択した属性名にマッピングするカスタマー（ユーザ定義）属性名を指定します。
- [Cisco Name]：[Customer Name] フィールドにある、ユーザ定義名にマッピングするシスコ属性名を指定します。
- [Add]：属性マップに名前マッピングを挿入します。
- [Remove]：属性マップから選択した名前マッピングを削除します。
- [Customer Name]：属性マップにあるマッピングのカスタマー属性名を表示します。
- [Cisco Name]：属性マップにあるマッピングのシスコ属性名を表示します。

[Add/Edit LDAP Attribute Map] > [Map Value] タブ

[Add/Edit LDAP Attribute Map] ダイアログボックスでは、既存の LDAP 属性マップの変更または削除、新しい LDAP 属性マップの追加、および属性マップへの属性名と値のマッピングの入力を行うことができます。「Add/Edit LDAP Attribute Map」も参照してください。

一部のフィールドは [Map Name] タブを選択するか、[Map Value] タブを選択するかによって異なります。[Map Value] タブをクリックした場合、次のフィールドが表示されます。

フィールド

- [Name]：追加または編集する LDAP 属性マップの名前を指定します。新しいマップを追加する場合、このフィールドにマップの名前を入力します。[LDAP Attribute Map] ペインで選択したマップを編集する場合は、選択したマップの名前がこのフィールドに読み取り専用テキストとして表示されます。マップを変更するには、[LDAP Attribute Map] ペインに戻り、目的のマップを選択する必要があります。
- [Customer Name]：属性マップにあるマッピングのカスタマー属性名を表示します。
- [Customer to Cisco Map Value]：シスコ値へのカスタマー属性のカスタマー値のマッピングを表示します。
- [Add]：[Add LDAP Attributes Map Value] ダイアログボックスを表示します。
- [Edit]：[Edit LDAP Attributes Map Value] ダイアログボックスを表示します。
- [Delete]：LDAP 属性マップから選択した属性値マッピングを削除します。

Add/Edit LDAP Attributes Value Map

[Add/Edit LDAP Attribute Map Value] ダイアログボックスでは、カスタマー属性名のカスタマー属性値を、関連付けられたシスコ属性名のシスコ値にマッピングできます。

フィールド

- [Customer Name]：新しい属性値マッピングを追加する場合、これは、まだシスコ属性値にマッピングするカスタマー値を持たない属性リストからカスタマー属性名を選択できるドロップダウンリストになります。既存の属性値マッピングを編集する場合、これは、[Add/Edit LDAP Attribute Map] ダイアログボックスの [Map Value] タブで選択したカスタマー属性の名前を表示する読み取り専用フィールドになります。
- [Customer Value]：選択したカスタマー属性のカスタマー値を指定します。
- [Cisco Value]：選択したカスタマー属性のシスコ値を指定します。
- [Add]：カスタマー属性値マップに値マッピングを追加します。
- [Remove]：カスタマー属性値マップから値マッピングを削除します。
- [Customer Name]：カスタマー属性名のカスタマー値を表示します。
- [Cisco Name]：シスコの属性名のシスコ値を表示します。

CHAPTER 13

管理アクセスの設定

この章は、次の内容で構成されています。

HTTPS/ASDM

[HTTPS/ASDM] ペインは、HTTPS を使用した ASDM へのアクセスを許可されているすべてのホストまたはネットワークのアドレスを指定するテーブルを提供します。このテーブルを使用して、アクセスを許可されているホストやネットワークを追加または変更できます。

フィールド

- [Interface]：デバイス マネージャへの管理アクセスが許可されている、セキュリティ アプライアンス上のインターフェイスを一覧表示します。
- [IP Address]：アクセスを許可されているネットワークまたはホストの IP アドレスを一覧表示します。
- [Mask]：アクセスを許可されているネットワークまたはホストに関連付けられたネットワーク マスクを一覧表示します。
- [Add]：新しいホストまたはネットワークを追加するための [Add HTTP Configuration] ダイアログボックスを表示します。
- [Edit]：選択したホストまたはネットワークを編集するための [Edit HTTP Configuration] ダイアログボックスを表示します。
- [Delete]：選択したホストまたはネットワークを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Configuration

[Add/Edit HTTP Configuration] ダイアログボックスでは、HTTPS を介したセキュリティ アプライアンス デバイス マネージャへの管理アクセスを許可されるホストまたはネットワークを追加できます。

フィールド

- [Interface Name]：セキュリティ アプライアンス デバイス マネージャへの管理アクセスが許可されている、セキュリティ アプライアンス上のインターフェイスを指定します。
- [IP Address]：アクセスを許可されているネットワークまたはホストの IP アドレスを指定します。
- [Mask]：アクセスを許可されているネットワークまたはホストに関連付けられたネットワーク マスクを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

コマンドライン

この項では、コマンドライン インターフェイスの機能について説明します。次の項目を取り上げます。

- 「バナー」（P.13-2）
- 「Console Timeout」（P.13-4）
- 「セキュア シェル」（P.13-5）
- 「Telnet」（P.13-6）

バナー

[Banner] ペインでは、その日のバナー、ログイン バナー、およびセッション バナーのメッセージを設定できます。

バナーを作成するには、該当するボックスにテキストを入力します。テキスト内のスペースは保持されます。ただし、タブは ASDM インターフェイスで入力できますが、コマンドライン インターフェイスから入力することはできません。$(domain) トークンと $(hostname) トークンは、セキュリティ アプライアンスのドメイン名とホスト名に置き換えられます。

$(hostname) トークンと $(domain) トークンを使用して、特定のコンテキストで指定されたホスト名とドメイン名をエコーします。$(system) トークンを使用して、特定のコンテキストのシステム スペースで設定されているバナーをエコーします。

複数行のバナーを設定するには、追加する行ごとに 1 行のテキストを入力します。各行は、既存のバナーの末尾に追加されていきます。テキストが空の場合は、Carriage Return（CR; 復帰）がバナーに追加されます。バナーの長さについて、RAM およびフラッシュ メモリの制限以外の制限はありません。使用できるのは、改行（Enter キー、2 文字としてカウントされる）を含む ASCII 文字だけです。

Telnet または SSH を介してセキュリティ アプライアンスにアクセスしたときに、バナー メッセージを処理するのに十分なシステム メモリがなかった場合や、バナー メッセージの表示の試行時に TCP 書き込みエラーが発生した場合には、セッションが閉じます。

バナーを置換するには、該当するボックスの内容を変更し、[Apply] をクリックします。バナーをクリアするには、該当するボックスの内容をクリアし、[Apply] をクリックします。

banner コマンドは [ASDM] ペインを通じてシステム コンテキストで使用できませんが、[Tools] > [Command Line Interface] で設定できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CLI プロンプト

[CLI Prompt] ペインで、CLI セッション時に使用するプロンプトをカスタマイズできます。デフォルトでは、プロンプトにセキュリティ アプライアンスのホスト名が表示されます。マルチ コンテキスト モードでは、プロンプトにコンテキスト名も表示されます。CLI プロンプトには次の項目を表示できます。

context	（マルチ モードのみ）現在のコンテキストの名前を表示します。
domain	ドメイン名を表示します。
hostname	ホスト名を表示します。

priority	フェールオーバー プライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。
state	装置のトラフィック通過状態を表示します。状態に関して次の値が表示されます。 • [act]：フェールオーバーがイネーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stby]：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailove]：フェールオーバーはディセーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover]：フェールオーバーはディセーブルであり、装置ではトラフィックを通過させていません。これは、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。

CLI プロンプトを設定するには、次の手順を実行します。

ステップ 1　プロンプトに属性を追加する場合は、[Available Prompts] リストで目的の属性をクリックし、[Add] をクリックします。プロンプトには複数の属性を追加できます。属性が [Available Prompts] リストから [Selected Prompts] リストに移動します。

ステップ 2　プロンプトから属性を削除する場合は、[Selected Prompts] リストで属性をクリックし、[Delete] をクリックします。属性が [Selected Prompts] リストから [Available Prompts] リストに移動します。

ステップ 3　コマンド プロンプトに属性が表示される順序を変更する場合は、[Selected Prompts] リストで目的の属性をクリックし、[Move Up] または [Move Down] をクリックして順序を変更します。

[CLI Prompt Preview] フィールドのペイン下部でコマンド プロンプトをプレビューできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Console Timeout

[Console Timeout] ペインでは、管理コンソールがアクティブな状態のままでいる期間（分単位）を指定できます。ここで指定した時間制限に到達すると、コンソールは自動的にシャット ダウンします。

[Console Timeout] フィールドに期間を入力します。タイムアウト期間を設定しない場合は 0 を入力します。デフォルト値は 0 です

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

セキュア シェル

[Secure Shell] ペインでは、SSH プロトコルを使用した管理アクセス目的でのセキュリティ アプライアンスへの接続を特定のホストまたはネットワークにだけ許可するルールを設定できます。ルールでは、特定の IP アドレスとネットマスクへの SSH アクセスが制限されます。このルールに準拠する SSH 接続試行は、AAA サーバまたは Telnet パスワードによって認証される必要があります。

[Monitoring] > [Administration] > [Secure Shell Sessions] を使用して SSH セッションをモニタできます。

フィールド

[Secure Shell] ペインには次のフィールドが表示されます。

- [Allowed SSH Versions]：セキュリティ アプライアンスによって受け入れられる SSH のバージョンを制限します。デフォルトでは、SSH バージョン 1 接続および SSH バージョン 2 接続が受け入れられます。
- [Timeout (minutes)]：セキュア シェル セッションがセキュリティ アプライアンスによって閉じられる前にアイドル状態でいられる時間（分単位）を 1 ～ 60 で表示します。デフォルトは 5 分です。
- [SSH Access Rule]：SSH を使用してセキュリティ アプライアンスにアクセスすることを許可するホストとネットワークを表示します。このテーブルの行をダブルクリックすると、選択したエントリの [Edit SSH Configuration] ダイアログボックスが開きます。
  - [Interface]：SSH 接続を許可するセキュリティ アプライアンス インターフェイスの名前を表示します。
  - [IP Address]：指定したインターフェイスを介してこのセキュリティ アプライアンスへの接続を許可されている各ホストまたはネットワークの IP アドレスを表示します。
  - [Mask]：指定したインターフェイスを介してこのセキュリティ アプライアンスへの接続が許可されている各ホストまたはネットワークの IP アドレスのネットマスクを表示します。
- [Add]：[Add SSH Configuration] ダイアログボックスが開きます。
- [Edit]：[Edit SSH Configuration] ダイアログボックスが開きます。
- [Delete]：選択した SSH アクセス ルールを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SSH Configuration

[Add SSH Configuration] ダイアログボックスでは、ルール テーブルに新規の SSH アクセス ルールを追加できます。[Edit SSH Configuration] ダイアログボックスでは、既存のルールを変更できます。

フィールド

- [Interface]：SSH 接続を許可するセキュリティ アプライアンス インターフェイスの名前を指定します。
- [IP Address]：セキュリティ アプライアンスとの SSH 接続の確立を許可されるホストまたはネットワークの IP アドレスを指定します。
- [Mask]：セキュリティ アプライアンスとの SSH 接続の確立を許可されるホストまたはネットワークのネットマスク。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Telnet

[Telnet] ペインでは、ASDM を実行している特定のホストまたはネットワークだけが Telnet プロトコルを使用してセキュリティ アプライアンスに接続できるルールを設定します。

このルールでは、セキュリティ アプライアンス インターフェイスを介した特定の IP アドレスおよびネットマスクへの管理 Telnet アクセスが制限されます。このルールに準拠する接続試行は、設定済みの AAA サーバまたは Telnet パスワードによって認証される必要があります。Telnet セッションは、[Monitoring] > [Telnet Sessions] を使用してモニタできます。

（注） コンフィギュレーション ファイルにはそれより多く含まれますが、シングルコンテキスト モードで同時にアクティブになれる Telnet セッションは 5 つのみです。マルチコンテキスト モードでは、コンテキストごとに 5 つの Telnet セッションのみがアクティブになれます。

フィールド

[Telnet] ペインには次のフィールドが表示されます。

Telnet ルール テーブル：

- [Interface]：Telnet 接続を許可するセキュリティ アプライアンス インターフェイス（ASDM を実行している PC またはワークステーションがあるインターフェイス）の名前を表示します。
- [IP Address]：指定したインターフェイスを介してこのセキュリティ アプライアンスへの接続を許可されている各ホストまたはネットワークの IP アドレスを表示します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

- [Netmask]：指定したインターフェイスを介してこのセキュリティ アプライアンスへの接続を許可されている各ホストまたはネットワークの IP アドレスのネットマスクを表示します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

- [Timeout]：Telnet セッションがセキュリティ アプライアンスによって閉じられる前にアイドル状態でいられる時間（分単位）を 1 ～ 60 で表示します。デフォルトは 5 分です。
- [Add]：[Add Telnet Configuration] ダイアログボックスが開きます。
- [Edit]：[Edit Telnet Configuration] ダイアログボックスが開きます。
- [Delete]：選択したアイテムを削除します。
- [Apply]：ASDM での変更内容をセキュリティ アプライアンスに送信し、実行コンフィギュレーションに適用します。[Save] をクリックすると、実行コンフィギュレーションのコピーがフラッシュ メモリに書き込まれます。実行コンフィギュレーションのコピーをフラッシュ メモリ、TFTP サーバ、またはフェールオーバー スタンバイ装置に書き込むには、[File] メニューを使用します。
- [Reset]：変更内容を破棄して、変更前に表示されていた情報、または [Refresh] や [Apply] を最後にクリックした時点の表示情報に戻します。リセット後、[Refresh] を使用して、現在の実行コンフィギュレーションの情報が表示されていることを確認します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Telnet Configuration

Telnet ルールの追加

Telnet ルール テーブルにルールを追加するには、次の手順を実行します。

1. [Add] ボタンをクリックし、[Telnet] > [Add] ダイアログボックスを開きます。
2. [Interface] をクリックし、セキュリティ アプライアンス インターフェイスをルール テーブルに追加します。
3. [IP Address] ボックスに、このセキュリティ アプライアンス インターフェイスを介した Telnet アクセスを許可する、ASDM を実行中のホストの IP アドレスを入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

4. [Mask] リストで、Telnet アクセスを許可する IP アドレスのネットマスクを選択または入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスのマスクではありません。

5. 前のペインに戻るには、次をクリックします。

- [OK]：変更内容を受け入れて、前のペインに戻ります。
- [Cancel]：変更内容を破棄して、前のペインに戻ります。
- [Help]：詳細情報を表示します。

Telnet ルールの編集

Telnet ルール テーブルのルールを編集するには、次の手順を実行します。

1. [Edit] をクリックし、[Telnet] > [Edit] ダイアログボックスを開きます。
2. [Interface] をクリックし、ルール テーブルからセキュリティ アプライアンス インターフェイスを選択します。
3. [IP Address] フィールドに、このセキュリティ アプライアンス インターフェイスを介した Telnet アクセスを許可する、ASDM を実行中のホストの IP アドレスを入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

4. [Mask] リストで、Telnet アクセスを許可する IP アドレスのネットマスクを選択または入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスのマスクではありません。

5. 前のウィンドウに戻るには、次のいずれかのボタンをクリックします。

- [OK]：変更内容を受け入れて、前のペインに戻ります。
- [Cancel]：変更内容を破棄して、前のペインに戻ります。
- [Help]：詳細情報を表示します。

Telnet ルールの削除

Telnet テーブルからルールを削除するには、次の手順を実行します。

1. Telnet ルール テーブルからルールを選択します。
2. [Delete] をクリックします。

変更の適用

[Add]、[Edit]、または [Delete] を使用してテーブルに加えた変更内容は、実行コンフィギュレーションにただちに適用されるわけではありません。変更内容を適用または廃棄するには、次のいずれかのボタンをクリックします。

1. [Apply]：ASDM での変更内容をセキュリティ アプライアンスに送信し、実行コンフィギュレーションに適用します。[Save] をクリックすると、実行コンフィギュレーションのコピーがフラッシュ メモリに書き込まれます。実行コンフィギュレーションのコピーをフラッシュ メモリ、TFTP サーバ、またはフェールオーバー スタンバイ装置に書き込むには、[File] メニューを使用します。
2. [Reset]：変更内容を破棄して、変更前に表示されていた情報、または [Refresh] や [Apply] を最後にクリックした時点の表示情報に戻します。リセット後、[Refresh] を使用して、現在の実行コンフィギュレーションの情報が表示されていることを確認します。

フィールド

- [Interface Name]：セキュリティ アプライアンスへの Telnet アクセスを許可するインターフェイスを選択します。
- [IP Address]：セキュリティ アプライアンスへの Telnet 接続が許可されたホストまたはネットワークの IP アドレスを入力します。
- [Mask]：セキュリティ アプライアンスへの Telnet 接続が許可されたホストまたはネットワークのサブネット マスクを入力します。
- [OK]：変更内容を受け入れて、前のペインに戻ります。
- [Cancel]：変更内容を破棄して、前のペインに戻ります。
- [Help]：詳細情報を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

File Access

この項では、ファイル アクセス機能について説明します。次の項目を取り上げます。

- 「FTP クライアント」（P.13-10）
- 「セキュア コピー」（P.13-10）
- 「TFTP Client」（P.13-11）
- 「Mount Points」（P.13-12）

FTP クライアント

[FTP Mode] ペインでは、FTP モードをアクティブまたはパッシブとして設定できます。セキュリティ アプライアンスでは、FTP サーバとの間で、イメージ ファイルやコンフィギュレーション ファイルのアップロードおよびダウンロードを実行できます。パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバは、今回の特定の接続においてリッスンするポート番号を応答として返します。

フィールド

- [Specify FTP mode as passive] : FTP モードをアクティブまたはパッシブとして設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

セキュア コピー

[Secure Copy] ペインでは、セキュリティ アプライアンスのセキュア コピー サーバをイネーブルにできます。SSH によるセキュリティ アプライアンスへのアクセスを許可されたクライアントだけが、セキュア コピー接続を確立できます。

制限事項

セキュア コピー サーバのこの実装には、次の制限があります。

- サーバはセキュア コピーの接続を受け入れまたは終了できますが、開始はできません。
- サーバにはディレクトリ サポートがありません。そのため、リモート クライアント アクセスでセキュリティ アプライアンスの内部ファイル参照はできません。
- サーバではバナーがサポートされません。
- サーバではワイルドカードがサポートされません。
- SSH バージョン 2 接続をサポートするには、セキュリティ アプライアンスのライセンスに VPN-3DES-AES 機能が必要です。

フィールド

- [Enable Secure Copy Server] : セキュリティ アプライアンスのセキュア コピー サーバをイネーブルにするには、このチェックボックスをオンにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

TFTP Client

このペインでは、セキュリティ アプライアンスが TFTP クライアントとして機能するように設定できます。

（注）　このペインでサーバにファイルを書き込むことはありません。このペインでセキュリティ アプライアンスを TFTP クライアントで使用できるように設定してから、[File] > [Save Running Configuration to TFTP Server] をクリックします。

TFTP サーバとセキュリティ アプライアンス

TFTP は、単純なクライアント/サーバ ファイル転送プロトコルで、RFC783 および RFC1350 Rev. 2 で規定されています。このペインでセキュリティ アプライアンスを TFTP *クライアント*として設定すると、その実行コンフィギュレーション ファイルのコピーを TFTP *サーバ*へ転送できるようになります。設定は、[File] > [Save Running Configuration to TFTP Client or Tools] > [Command Line Interface] で行います。これにより、コンフィギュレーション ファイルをバックアップし、それらを複数のセキュリティ アプライアンスにプロパゲートできます。

このペインでは、TFTP クライアントの IP アドレスを指定する場合は **configure net** コマンドを使用し、実行コンフィギュレーション ファイルが書き込まれるサーバのインターフェイスおよびパスまたはファイル名を指定する場合は、**tftp-server** コマンドを使用します。この情報が実行コンフィギュレーションに適用されると、ASDM の [File] > [Save Running Configuration to TFTP client] で **copy** コマンドを使用してファイル転送を実行できます。

セキュリティ アプライアンスでサポートされる TFTP クライアントは 1 つだけです。TFTP クライアントのフル パスは、[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] で指定します。この設定を行えば、それ以降は CLI の **configure net** コマンドおよび **copy** コマンドで、コロン（:）を使用した IP アドレスを指定できます。ただし、セキュリティ アプライアンスと TFTP クライアントの通信に必要となる中間デバイスの認証や設定は、この機能とは別に行われます。

show tftp-client コマンドで、現在のコンフィギュレーションに含まれている **tftp-client** コマンド ステートメントを一覧表示できます。**no tftp client** コマンドで、クライアントへのアクセスをディセーブルにします。

フィールド

[TFTP] ペインには次のフィールドがあります。

- [Enable] : コンフィギュレーション内の TFTP クライアント設定を選択およびイネーブルにする場合にクリックします。
- [Interface Name] : これらの TFTP クライアント設定を使用するセキュリティ アプライアンス インターフェイスの名前を選択します。
- [IP Address] : TFTP サーバの IP アドレスを入力します。

- [Path]：TFTP クライアントのパスを入力します。先頭にスラッシュ（/）を付け、最後にファイル名を指定します。ここに実行コンフィギュレーション ファイルが書き込まれます。

  TFTP クライアントのパスの例：**/tftpboot/** セキュリティ アプライアンス **/config3**

（注）　パスの先頭には必ずスラッシュ（/）を付けます。

詳細情報

TFTP の詳細については、使用しているソフトウェア バージョンのセキュリティ アプライアンスの技術マニュアルを参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Mount Points

[Mount Points] テーブルには、現在ファイル アクセス用に設定されている共通インターネット ファイル システム（CIFS）およびファイル転送プロトコル（FTP）のマウント ポイントが表示されます。

マウント ポイントを追加、変更、または削除するには、次のいずれかの操作を実行します。

- マウント ポイントを追加するには、[Add] > [CIFS Mount Point] または [Add] > [FTP Mount Point] を選択します。パラメータの詳細については、「[Add or Edit FTP Mount Point] ダイアログボックスのフィールド」（P.13-13）または「[Add or Edit FTP Mount Point] ダイアログボックスのフィールド」（P.13-13）を参照してください。
- マウント ポイントを変更するには、テーブルでエントリを選択し、[Edit] をクリックします。エントリをダブルクリックして、そのエントリを編集することもできます。パラメータの詳細については、「[Add or Edit FTP Mount Point] ダイアログボックスのフィールド」（P.13-13）または「[Add or Edit FTP Mount Point] ダイアログボックスのフィールド」（P.13-13）を参照してください。
- マウント ポイントを削除するには、削除するエントリを選択し、[Delete] をクリックします。

（注）　[Delete] ボタンをクリックすると、ダイアログが表示されることなく、選択したマウント ポイントがただちにテーブルから削除され、指定したファイル システムにアクセスできなくなります。

適用とリセット。フィールド値に対して行った追加や変更はただちに画面に反映されますが、それをコンフィギュレーションに保存するには [Apply] をクリックする必要があります。

[Add or Edit CIFS Mount Point] ダイアログボックスのフィールド

[Add or Edit CIFS Mount Point] ダイアログボックスには次のフィールドが表示されます。

- [Enable mount point]：選択したマウント ポイントへのアクセスをイネーブルまたはディセーブルにします。このオプションをオンにすると、セキュリティ アプライアンスの CIFS ファイル システムが UNIX ファイル ツリーにアタッチされます。反対に、オフにするとマウント ポイントがデタッチされます。
- [Mount-Point Name]：既存のファイル システムの名前を入力するか変更します。
- [Server Name or IP Address]：CIFS サーバの事前定義済みの名前（またはドット付き 10 進数形式の IP アドレス）を入力します。
- [Share Name]：CIFS サーバ内のファイル データにアクセスするためのサーバ共有（フォルダ）の名前を入力します。
- [NT Domain Name]：事前定義済みの Windows NT ドメイン名を入力します。最大 63 文字が許可されます。
- [User Name]：ファイル システムのマウントを許可されているユーザの名前を入力します。
- [Password]：ファイル システムをマウントするために許可されているパスワードを入力します。
- [Confirm Password]：許可されているパスワードを再入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add or Edit FTP Mount Point] ダイアログボックスのフィールド

[Add or Edit FTP Mount Point] ダイアログボックスには次のフィールドがあります。

- [Enable mount point]：選択したマウント ポイントへのアクセスをイネーブルまたはディセーブルにします。このオプションをオンにすると、セキュリティ アプライアンスの FTP ファイル システムが UNIX ファイル ツリーにアタッチされます。反対に、チェックボックスをオフにするとマウント ポイントがデタッチされます。
- [Mount-Point Name]：既存の FTP ファイル システムの名前を入力するか変更します。
- [Server Name or IP Address]：FTP ファイル システム サーバの事前定義済みの名前（またはドット付き 10 進数形式の IP アドレス）を入力します。
- [Mode]：FTP マウント オプションの FTP 転送モードを [Passive] または [Active] から選択します。FTP 転送モードの詳細については、FTP クライアントを参照してください。
- [Path To Mount]：FTP ファイル サーバへのディレクトリ パス名を入力します。スペースは使用できません。
- [User Name]：ファイル システムのマウントを許可されているユーザの名前を入力します。
- [Password]：ファイル システムをマウントするために許可されているパスワードを入力します。
- [Confirm Password]：許可されているパスワードを再入力します。

（注）　FTP マウント ポイントの場合、FTP サーバには UNIX のディレクトリ リスト スタイルが必要です。Microsoft FTP サーバには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

ICMP

[ICMP Rules] ペインでは、ICMP ルールを一覧表示するテーブルを表示し、セキュリティ アプライアンスへの ICMP アクセスを許可または拒否されるすべてのホストまたはネットワークのアドレスを指定します。このテーブルを使用して、セキュリティ アプライアンスへの ICMP メッセージの送信を許可または禁止するホストやネットワークを追加または変更することができます。

ICMP ルール リストでは、セキュリティ アプライアンス インターフェイス上で終了する ICMP トラフィックを制御します。ICMP コントロール リストが設定されていない場合、セキュリティ アプライアンスは外部インターフェイスを含め任意のインターフェイスで終了するすべての ICMP トラフィックを受け付けます。ただし、セキュリティ アプライアンスはデフォルトではブロードキャスト アドレスに送信される ICMP エコー要求に応答しません。

（注）　[Security Policy] ペインを使用して、セキュリティ アプライアンス*経由*で保護されたインターフェイス上の宛先にルーティングされる ICMP トラフィックのアクセス ルールを設定します。

ICMP の到達不能メッセージ タイプ（type 3）の権限は、常に許可にすることをお勧めします。ICMP 到達不能メッセージが拒否されると、ICMP パス MTU ディスカバリがディセーブルになり、IPSec および PPTP トラフィックが停止する可能性があります。パス MTU ディスカバリの詳細については、RFC 1195 および RFC 1435 を参照してください。

ICMP コントロール リストが設定されている場合、セキュリティ アプライアンスでは最初に一致した条件を ICMP トラフィックに適用し、暗黙的にすべてを拒否します。つまり、最初に一致したエントリが許可エントリである場合、ICMP パケットは引き続き処理されます。最初に一致したエントリが拒否エントリであるか、エントリに一致しない場合、セキュリティ アプライアンスによって ICMP パケットは破棄され、syslog メッセージが生成されます。例外は、ICMP コントロール リストが設定されていない場合です。その場合、**permit** ステートメントがあるものと見なされます。

フィールド

- [Interface]：ICMP アクセスが許可されるセキュリティ アプライアンスのインターフェイスを一覧表示します。
- [Action]：指定したネットワークまたはホストからの ICMP 受信メッセージを許可するかまたは拒否するかを表示します。

- [IP Address] : アクセスを許可または拒否するネットワークまたはホストの IP アドレスを一覧表示します。
- [Mask] : アクセスを許可されているネットワークまたはホストに関連付けられたネットワーク マスクを一覧表示します。
- [ICMP Type] : ルールを適用する ICMP メッセージのタイプを一覧表示します。表 13-1 に、サポートされる ICMP タイプの値を一覧表示します。
- [Add] : 新しい ICMP ルールをテーブルの最後に追加するための [Add ICMP Rule] ダイアログボックスを表示します。
- [Insert Before] : ICMP ルールを現在選択されているルールの前に追加します。
- [Insert After] : ICMP ルールを現在選択されているルールの後に追加します。
- [Edit] : 選択したホストまたはネットワークを編集するための [Edit ICMP Rule] ダイアログボックスを表示します。
- [Delete] : 選択したホストまたはネットワークを削除します。

表 13-1　ICMP タイプのリテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit ICMP Rule

[Add/Edit ICM Rule] ダイアログボックスでは、ICMP ルールの追加または変更ができます。ICMP ルールでは、セキュリティ アプライアンスへの ICMP アクセスが許可または拒否されるすべてのホストまたはネットワークのアドレスを指定します。

フィールド

- [ICMP Type]：ルールを適用する ICMP メッセージのタイプを指定します。表 13-2 に、サポートされる ICMP タイプの値を一覧表示します。
- [Interface]：ICMP アクセスが許可されるセキュリティ アプライアンスのインターフェイスを指定します。
- [IP Address]：アクセスを許可または拒否するネットワークまたはホストの IP アドレスを指定します。
- [Any Address]：指定したインターフェイスで受信されたすべてのアドレスにアクションを適用します。
- [Mask]：アクセスを許可されているネットワークまたはホストに関連付けられたネットワーク マスクを指定します。
- [Action]：指定したネットワークまたはホストからの ICMP メッセージを許可するかまたは拒否するかを指定します。
  - [Permit]：指定したホストまたはネットワークおよびインターフェイスからの ICMP メッセージを許可します。
  - [Deny]：指定したホストまたはネットワークおよびインターフェイスからの ICMP メッセージをドロップします。

表 13-2　ICMP タイプのリテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem

表 13-2　ICMP タイプのリテラル （続き）

ICMP タイプ	リテラル
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

管理インターフェイス

[Management Interface] ペインでは、高度なセキュリティ インターフェイスの管理インターフェイスをイネーブルまたはディセーブルにすることができ、これにより、セキュリティ アプライアンスの管理機能を実行できます。管理インターフェイスをイネーブルにすると、IPSec VPN トンネルを介して固定 IP アドレスを持つ内部インターフェイスで ASDM を実行できます。この機能は、VPN がセキュリティ アプライアンスで設定されており、外部インターフェイスが動的に割り当てられた IP アドレスを使用している場合に使用します。たとえば、この機能は、VPN クライアントを使用して自宅からセキュリティ アプライアンスに対する安全なアクセスおよび管理を行う場合に役立ちます。

フィールド

- [Management Interface] : セキュリティ アプライアンスの管理に使用するインターフェイスを指定します。[None] は管理インターフェイスをディセーブルにし、これがデフォルトです。管理インターフェイスをイネーブルにする場合は、最も高いセキュリティを設定したインターフェイス（内部インターフェイス）を選択します。管理インターフェイスは、一度に 1 つのインターフェイスのみでイネーブルにすることができます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

SNMP

[SNMP] ペインでは、セキュリティ アプライアンスを簡易ネットワーク管理プロトコル（SNMP）管理ステーションからモニタできるように設定できます。

SNMP は、PC またはワークステーションで実行されるネットワーク管理ステーションが、スイッチ、ルータ、セキュリティ アプライアンスなど、さまざまなタイプのデバイスのヘルスとステータスをモニタする標準的な方法を定義します。

SNMP の用語

- 管理ステーション：PC またはワークステーションで実行されるネットワーク管理ステーションです。SNMP プロトコルを使用して、管理対象デバイス上の標準データベースを管理します。管理ステーションでは、ハードウェア障害など注意が必要なイベントのメッセージも受信できます。
- エージェント：SNMP コンテキストでは、管理ステーションがクライアント、セキュリティ アプライアンスで動作する SNMP エージェントがサーバになります。
- OID：SNMP 標準は、管理ステーションが SNMP エージェントでネットワーク デバイスを一意に識別したり、モニタおよび表示される情報のソースをユーザに示したりできるように、システム オブジェクト ID（OID）を割り当てます。
- MIB：エージェントは管理情報データベース（MIB）と呼ばれる標準データ構造を保持します。これが管理ステーションに蓄積されます。MIB は、パケット、接続、エラー カウンタ、バッファの使用状況、フェールオーバー ステータスなどの情報を収集します。通常のネットワーク デバイスで使用される一般的なプロトコルとハードウェア規格用の MIB に加えて、MIB は製品ごとに定義されています。SNMP 管理ステーションでは、MIB を参照したり、特定のフィールドだけを要求したりできます。一部のアプリケーションでは、管理の目的で MIB データを修正できます。
- トラップ：エージェントはアラーム条件もモニタします。リンク アップ、リンク ダウン、syslog イベントなど、トラップに定義したアラーム条件が発生すると、エージェントは指定された管理ステーションに通知（SNMP トラップとも呼ばれます）をただちに送信します。

SNMP

Cisco MIB ファイルおよび OID については、http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml を参照してください。OID は、次の URL からダウンロードすることもできます。ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz。

MIB のサポート

セキュリティ アプライアンスは、次の SNMP MIB サポートを提供しています。

（注）　セキュリティ アプライアンスは、Cisco syslog MIB のブラウジングはサポートしません。

- MIB-II のシステム グループとインターフェイス グループをブラウジングできます。MIB のブラウジングはトラップの送信とは違います。ブラウジングとは、管理ステーションから MIB ツリーの snmpget や snmpwalk を実行し、値を決定することです。
- Cisco MIB および Cisco Memory Pool MIB を使用できます。
- セキュリティ アプライアンスは、次の Cisco MIB をサポートしていません。
- cfwSecurityNotification NOTIFICATION-TYPE
- cfwContentInspectNotification NOTIFICATION-TYPE
- cfwConnNotification NOTIFICATION-TYPE
- cfwAccessNotification NOTIFICATION-TYPE
- cfwAuthNotification NOTIFICATION-TYPE
- cfwGenericNotification NOTIFICATION-TYPE

SNMP CPU 使用状況

セキュリティ アプライアンスは、SNMP を利用する CPU 使用状況のモニタリングをサポートしています。この機能により、ネットワーク管理者は、HP OpenView などの SNMP 管理ソフトウェアを使用してセキュリティ アプライアンスの CPU 使用率をモニタし、キャパシティ プランニングを行うことができます。

この機能は、Cisco Process MIB（CISCO-PROCESS-MIB.my）の cpmCPUTotalTable のサポート機能によって組み込まれています。MIB には他に 2 つのテーブル（cpmProcessTable および cpmProcessExtTable）がありますが、今回のリリースではサポートされていません。

cpmCPUTotalTable の各行には、各 CPU のインデックスと次のオブジェクトが含まれます。

MIB オブジェクト名	説明
cpmCPUTotalPhysicalIndex	このオブジェクトの値は 0 になります。Entity MIB の entPhysicalTable をセキュリティ アプライアンスの SNMP エージェントがサポートしていないためです。
cpmCPUTotalIndex	このオブジェクトの値は 0 になります。Entity MIB の entPhysicalTable をセキュリティ アプライアンスの SNMP エージェントがサポートしていないためです。
cpmCPUTotal5sec	直前 5 秒間の CPU 全体のビジー率。
cpmCPUTotal1min	直前 1 分間の CPU 全体のビジー率。
cpmCPUTotal5min	直前 5 分間の CPU 全体のビジー率。

（注）　現在のすべてのセキュリティ アプライアンス ハードウェア プラットフォームは単一 CPU だけサポートしているため、セキュリティ アプライアンスが返す cpmCPUTotalTable は 1 行だけで、インデックスは常に 1 になります。

直前の 3 要素の値は、**show cpu usage** コマンドの出力値と同じです。

次の新しい MIB オブジェクトが cpmCPUTotalTable にありますが、セキュリティ アプライアンスではサポートされていません。

- cpmCPUTotal5secRev
- cpmCPUTotal1minRev

- cpmCPUTotal5minRev

フィールド

- [Community string (default)]：セキュリティ アプライアンスへの要求送信時に SNMP 管理ステーションが使用するパスワードを入力します。SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理対象のネットワーク ノード間の共有秘密キーです。セキュリティ アプライアンスでは、パスワードを基にして、受信する SNMP 要求が有効かどうかの判断が行われます。パスワードは、大文字と小文字が区別され、最大 32 文字です。スペースは使用できません。デフォルトは「public」です。SNMPv2c では、管理ステーションごとに、別々のコミュニティ ストリングを設定できます。コミュニティ ストリングがどの管理ステーションにも設定されていない場合、ここで設定した値がデフォルトとして使用されます。
- [Contact]：セキュリティ アプライアンスのシステム管理者の名前を入力します。テキストは、大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
- [Security Appliance Location]：セキュリティ アプライアンスの場所を指定します。テキストは、大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
- [Listening Port]：SNMP トラフィックが送信されるポートを指定します。デフォルトは 161 です。
- [Configure Traps]：SNMP トラップを利用して通知するイベントを設定します。
- [SNMP Management Stations] ボックス：
  - [Interface]：SNMP 管理ステーションが存在するセキュリティ アプライアンスのインターフェイスの名前を表示します。
  - [IP Address]：セキュリティ アプライアンスがトラップ イベントを送信し、要求またはポーリングを受信する SNMP 管理ステーションの IP アドレスを表示します。
  - [Community string]：管理ステーションのコミュニティ ストリングを指定しない場合、[Community String (default)] フィールドに設定された値が使用されます。
  - [SNMP Version]：管理ステーションに設定されている SNMP のバージョンを表示します。
  - [Poll/Trap]：この管理ステーションと通信する方法を表示します（ポーリングのみ、トラップのみ、またはトラップとポーリングの両方）。ポーリングとは、管理ステーションからの定期的な要求をセキュリティ アプライアンスが待機することを意味します。トラップを設定すると、発生した syslog イベントが送信されます。
  - [UDP Port]：SNMP ホストの UDP ポートです。デフォルトはポート 162 です。
- [Add]：次のフィールドが含まれた [Add SNMP Host Access Entry] が開きます。
- [Interface Name]：管理ステーションが存在するインターフェイスを選択します。
- [IP Address]：管理ステーションの IP アドレスを指定します。
- [Server Poll/Trap Specification]：[Poll] と [Trap] のいずれかまたは両方を選択します。
- [UDP Port]：SNMP ホストの UDP ポートです。このフィールドでは、SNMP ホストの UDP ポートのデフォルト値である 162 を上書きできます。
- [Help]：詳細情報を表示します。
- [Edit]：[Add] と同じフィールドが含まれた [Edit SNMP Host Access Entry] ダイアログボックスが開きます。
- [Delete]：選択したアイテムを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SNMP ホストのアクセス エントリの追加/編集

SNMP 管理ステーションの追加

SNMP 管理ステーションを追加するには、次の手順をします。

1. [Add] をクリックして、[SNMP Host Access Entry] ダイアログボックスを開きます。
2. [Interface Name] で、SNMP 管理ステーションが存在するインターフェイスを選択します。
3. 管理ステーションの IP アドレスを [IP Address] に入力します。
4. SNMP ホストの UDP ポートを入力します。デフォルト値は 162 です。
5. SNMP ホストのコミュニティ ストリング パスワードを入力します。管理ステーションのコミュニティ ストリングを指定しない場合、[SNMP Configuration] 画面の [Community String (default)] フィールドに設定した値が使用されます。
6. [Poll] と [Trap] のいずれかまたは両方をクリックして選択します。
7. 前のペインに戻るには、次をクリックします。

- [OK]：変更内容を受け入れて、前のペインに戻ります。
- [Cancel]：変更内容を破棄して、前のペインに戻ります。
- [Help]：詳細情報を表示します。

SNMP 管理ステーションの編集

SNMP 管理ステーションを編集するには、次の手順を実行します。

1. [SNMP] ペインで、SNMP 管理ステーション テーブルのリスト項目を選択します。
2. [Edit] をクリックして、[Edit SNMP Host Access Entry] を開きます。
3. [Interface Name] で、SNMP 管理ステーションが存在するインターフェイスを選択します。
4. 管理ステーションの IP アドレスを [IP Address] に入力します。
5. SNMP ホストのコミュニティ ストリング パスワードを入力します。管理ステーションのコミュニティ ストリングを指定しない場合、[SNMP Configuration] 画面の [Community String (default)] フィールドに設定した値が使用されます。
6. SNMP ホストの UDP ポートを入力します。デフォルト値は 162 です。
7. [Poll] と [Trap] のいずれかまたは両方をクリックして選択します。
8. SNMP のバージョンを選択します。
9. 前のペインに戻るには、次をクリックします。

- [OK]：変更内容を受け入れて、前のペインに戻ります。
- [Cancel]：変更内容を破棄して、前のペインに戻ります。
- [Help]：詳細情報を表示します。

SNMP 管理ステーションの削除

テーブルから SNMP 管理ステーションを削除するには、次の手順を実行します。

1. [SNMP] ペインで、SNMP 管理ステーション テーブルから項目を選択します。
2. [Delete] をクリックします。

フィールド

- [Interface name]：SNMP ホストが存在するインターフェイスを選択します。
- [IP Address]：SNMP ホストの IP アドレスを入力します。
- [UDP Port]：SNMP アップデートを送信する UDP ポートを入力します。デフォルト値は 162 です。
- [Community String]：SNMP サーバのコミュニティ ストリングを入力します。
- [SNMP Version]：SNMP のバージョンを選択します。
- Server Port/Trap Specification
  - [Poll]：ポーリング情報を送信する場合に選択します。ポーリングとは、管理ステーションからの定期的な要求をセキュリティ アプライアンスが待機することを意味します。
  - [Trap]：トラップ情報を送信する場合に選択します。トラップを設定すると、発生した syslog イベントが送信されます。
- [OK]：変更内容を受け入れて、前のペインに戻ります。
- [Cancel]：変更内容を破棄して、前のペインに戻ります。
- [Help]：詳細情報を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SNMP トラップの設定

トラップ

トラップは参照とは異なります。生成されるリンク アップ イベント、リンク ダウン イベント、syslog イベントなど、特定のイベントに対する管理対象デバイスから管理ステーションへの割り込み「コメント」です。

セキュリティ アプライアンスの SNMP オブジェクト ID（OID）が、セキュリティ アプライアンスから送信される SNMP イベント トラップに表示されます。セキュリティ アプライアンスでは、SNMP イベント トラップおよび SNMP mib-2.system.sysObjectID にシステム OID が提供されます。

セキュリティ アプライアンスで実行される SNMP サービスでは、次の 2 つの異なる機能を実行します。

- 管理ステーション（SNMP クライアントとも呼ばれます）からの SNMP 要求に応答します。

- セキュリティ アプライアンスからのトラップ（イベント通知）を受信するように登録されている管理ステーションまたはその他のデバイスにトラップを送信します。

セキュリティ アプライアンスは、次に示す 3 種類のトラップをサポートします。

- firewall
- generic
- syslog

トラップの設定

次のフィールドが含まれる [SNMP Trap Configuration] を開きます。

- [Standard SNMP Traps]：送信する標準トラップを選択します。
  - [Authentication]：認証標準トラップをイネーブルにします。
  - [Cold Start]：コールド スタート標準トラップをイネーブルにします。
  - [Link Up]：リンク アップ標準トラップをイネーブルにします。
  - [Link Down]：リンク ダウン標準トラップをイネーブルにします。
- Entity MIB Notifications
  - [FRU Insert]：現場交換可能ユニット（FRU）が挿入された場合のトラップ通知をイネーブルにします。
  - [FRU Remove]：現場交換可能ユニット（FRU）が削除された場合のトラップ通知をイネーブルにします。
  - [Configuration Change]：ハードウェア変更が行われた場合のトラップ通知をイネーブルにします。
- [IPSec Traps]：IPSec トラップをイネーブルにします。
  - [Start]：IPSec 開始時のトラップをイネーブルにします。
  - [Stop]：IPSec 停止時のトラップをイネーブルにします。
- [Remote Access Traps]：リモート アクセス トラップをイネーブルにします。
  - [Session threshold exceeded]：リモート アクセス セッション試行数が、設定されているしきい値を超過した場合のトラップをイネーブルにします。
- [Enable Syslog traps]：SNMP 管理ステーションへの syslog メッセージの送信をイネーブルにします。
- [OK]：変更内容を受け入れて、前のペインに戻ります。
- [Cancel]：変更内容を破棄して、前のペインに戻ります。
- [Help]：詳細情報を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

管理アクセス ルール

[Management Access Rules] ペインでは、インターフェイスに関連付けられるアクセス ルールを定義できます。特定のピア（または複数のピア）との間で送受信されるトラフィックを許可または拒否するために使用されるのがアクセス ルールです。それに対して、管理アクセス ルールは、to-the-box トラフィックのアクセス コントロールに使用されます。

たとえば、管理アクセス ルールを使用することにより、IKE サービス拒否攻撃を検出するだけでなく、それらをブロックすることもできます。

フィールド

注：テーブル カラムの幅はカーソルを使用して調整できます。カーソルをカラムの線に重ね、二重矢印になるまで移動します。カラムの線をクリックして、目的のサイズになるまでドラッグします。

- [Add]：新しい管理アクセス ルールを追加します。
- [Edit]：管理アクセス ルールを編集します。
- [Delete]：管理アクセス ルールを削除します。
- [Move Up]：ルールを上に移動します。ルールは、このテーブルに表示される順序で評価されるため、重複したルールがある場合は、それらを表示する順序に注意が必要です。
- [Move Down]：ルールを下に移動します。
- [Cut]：ルールを切り取ります。
- [Copy]：ルールのパラメータをコピーします。[Paste] ボタンを使用すれば、それと同じパラメータを持つルールを新たに作成できます。
- [Paste]：ルールからコピーしたパラメータまたは切り取ったパラメータがあらかじめ入力された状態の [Add/Edit Rule] ダイアログボックスが表示されます。このダイアログボックスでは、それらのパラメータを修正して新しいルールを作成し、それをテーブルに追加できます。[Paste] ボタンをクリックすると、選択したルールのすぐ前にそのルールが追加されます。[Paste] ドロップダウン リストから [Paste After] 項目を選択すると、選択したルールのすぐ後にそのルールが追加されます。

次に、[Management Access Rules] テーブルのカラムについて説明します。これらのカラムの内容を編集する場合は、テーブル行をダブルクリックします。ルールは、実行順に表示されます。ルールを右クリックすると、上記のボタンで選択できるすべてオプションのほか、[Insert] 項目および [Insert After] 項目が表示されます。[Insert] 項目を指定すると、選択したルールのすぐ前に新しいルールが挿入され、[Insert After] 項目を指定すると、選択したルールのすぐ後に新しいルールが挿入されます。

- [No]：ルールの評価順序を示します。
- [Enabled]：ルールがイネーブルかディセーブルかを示します。
- [Source]：[Destination Type] フィールドで指定された宛先に対してトラフィックを許可または拒否する送信元の IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。アドレス カラムには、単語 any が付いたインターフェイス名が表示される場合があります（inside: any など）。これは、内部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。
- [Service]：ルールで指定されるサービスまたはプロトコルを表示します。
- [Action]：ルールに適用されるアクション（[Permit] または [Deny]）が表示されます。
- [Logging]：アクセス リストのロギングをイネーブルにしている場合、このカラムには、ロギング レベル、およびログ メッセージ間の間隔が秒数で表示されます。
- [Time]：ルールが適用される時間範囲が表示されます。

- [Description]：ルールを追加したときに入力した説明が表示されます。暗黙のルールには、「Implicit outbound rule」という説明が含まれます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Management Access Rules

[Add/Edit Management Access Rule] ダイアログボックスでは、新しい管理ルールの作成、または既存の管理ルールの変更ができます。

- [Interface]：ルールを適用するインターフェイスを指定します。
- [Action]：新しいルールのアクション タイプを指定します。[Permit] と [Deny] のいずれかを選択します。
  - [Permit]：一致するすべてのトラフィックを許可します。
  - [Deny]：一致するすべてのトラフィックを拒否します。
- [Source]：[Destination] フィールドで指定された宛先に対してトラフィックを許可または拒否する送信元の IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。

  [...]：既存の IP アドレス オブジェクト、IP 名、ネットワーク オブジェクト グループ、またはそれらすべてを選択、追加、編集、削除、または検索できます。
- [Destination]：[Source Type] フィールドで指定された送信元に対してトラフィックを許可または拒否する宛先の IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。

  [...]：既存の IP アドレス オブジェクト、IP 名、ネットワーク オブジェクト グループ、またはそれらすべてを選択、追加、編集、削除、または検索できます。
- [Service]：サービスのリストからポート番号、ポートの範囲、またはウェルノウン サービス名やグループを指定する場合にこのオプションを選択します。

  [...]：事前に設定したリストで、既存のサービスを選択、追加、編集、削除、または検索できます。
- [Description]：（任意）管理アクセス ルールの説明を入力します。
- [Enable Logging]：アクセス リストのロギングをイネーブルにします。
  - [Logging Level]：デフォルトの値をそのまま使用するか、または [Emergency]、[Alert]、[Critical]、[Error]、[Warning]、[Notification]、[Informational]、[Debugging] のいずれかを指定します。
- [More Options]：ルールの追加設定オプションを表示します。
  - [Enable Rule]：ルールをイネーブルまたはディセーブルにします。

- [Traffic Direction]：どちらの方向のトラフィックにルールを適用するかを指定します。[Incoming] と [Outgoing] のいずれかを選択できます。
- [Source Service]：送信元のプロトコルとサービスを指定します（TCP または UDP サービスに限る）。

  [...]：事前に設定したリストで、送信元サービスを選択、追加、編集、削除、または検索できます。
- [Logging Interval]：ロギングが設定されている場合、ロギング間隔を秒単位で指定します。
- [Time Range]：このルールに定義されている時間範囲をドロップダウン リストから指定します。

  [...]：事前に設定したリストで、時間範囲を選択、追加、編集、削除、または検索できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

システム管理者用 AAA の設定

この項では、システム管理者の認証とコマンド許可をイネーブルにする方法について説明します。システム管理者の AAA を設定する前に、まずローカル データベースまたは AAA サーバを設定する必要があります（「ローカル データベースの設定」（P.12-8）または「AAA サーバ グループおよびサーバの識別」（P.12-13）を参照）。

この項では、次のトピックについて取り上げます。

CLI、ASDM、および enable コマンドの認証の設定

CLI 認証をイネーブルにすると、セキュリティ アプライアンスはログインのためユーザ名とパスワードの入力を求めるプロンプトを表示します。情報を入力した後、ユーザ EXEC モードにアクセスできるようになります。

特権 EXEC モードを開始するには、**enable** コマンドまたは **login** コマンドを入力します（ローカル データベースのみを使用している場合）。

イネーブル認証を設定した場合、セキュリティ アプライアンスではユーザ名とパスワードの入力を求めるプロンプトが表示されます。**enable** 認証を設定しない場合は、**enable** コマンドを入力する際に、（**enable password** コマンドで設定した）システム イネーブル パスワードを入力します。ただし、**enable** 認証を使用しない場合は、**enable** コマンドを入力した後、特定のユーザとしてログインしていないことになります。ユーザ名を保持するには、**enable** 認証を使用します。

ローカル データベースを使用する認証の場合、**login** コマンドを使用できます。このコマンドでは、ユーザ名は維持されますが、認証をオンにするコンフィギュレーションは必要ありません。

（注） セキュリティ アプライアンスで Telnet ユーザ、SSH ユーザ、または HTTP ユーザを認証できるようにするには、まずセキュリティ アプライアンスへのアクセスを設定する必要があります（「セキュア シェル」（P.13-5）、「Telnet」（P.13-6）、または「HTTPS/ASDM」（P.13-1）を参照）。これらのペインでは、セキュリティ アプライアンスとの通信が許可される IP アドレスを指定します。

CLI、ASDM、または**イネーブル**認証を設定するには、次の手順を実行します。

ステップ 1　**enable** コマンドを使用するユーザを認証する場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] に移動し、次のように設定を行います。

a. [Enable] チェックボックスを選択します。

b. [Server Group] ドロップダウン リストから、サーバ グループ名または LOCAL データベースを選択します。

c. （任意）AAA サーバを選択する場合は、AAA サーバが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるようにセキュリティ アプライアンスを設定できます。[Use LOCAL when server group fails] チェックボックスをオンにします。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、セキュリティ アプライアンスのプロンプトでは、いずれの方式が使用されているかが示されないためです。

ステップ 2　CLI または ASDM にアクセスするユーザを認証する場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] に移動し、次のように設定を行います。

a. 次のチェックボックスをオンにします（複数可）。

- [HTTP/ASDM]：HTTPS を使用して ASDM にアクセスする セキュリティ アプライアンス クライアントを認証します。AAA サーバを使用する場合は、HTTP 認証だけを設定する必要があります。デフォルトでは、このコマンドを設定しなくても、ASDM によってローカル データベースが認証に使用されます。HTTP 管理認証では、AAA サーバ グループの SDI プロトコルをサポートしていません。
- [Serial]：コンソール ポートを使用してセキュリティ アプライアンスにアクセスするユーザを認証します。
- [SSH]：SSH を使用してセキュリティ アプライアンスにアクセスするユーザを認証します。
- [Telnet]：Telnet を使用してセキュリティ アプライアンスにアクセスするユーザを認証します。

b. 対応するチェックボックスをオンにしたサービスごとに、[Server Group] ドロップダウン リストから、サーバ グループ名または LOCAL データベースを選択します。

c. （任意）AAA サーバを選択する場合は、AAA サーバが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるようにセキュリティ アプライアンスを設定できます。[Use LOCAL when server group fails] チェックボックスをオンにします。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、セキュリティ アプライアンスのプロンプトでは、いずれの方式が使用されているかが示されないためです。

ステップ 3　[Apply] をクリックします。

管理許可によるユーザ CLI および ASDM アクセスの制限

CLI 認証または **enable** 認証を設定すると、ローカル ユーザ、RADIUS、TACACS+、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）からの CLI、ASDM、または **enable** コマンドへのアクセスを制限できます。

（注）　管理許可にはシリアル アクセスは含まれないため、[Authentication] > [Serial] オプションをイネーブルにすると、認証されたユーザはすべて、コンソール ポートにアクセスできます。

管理許可を設定するには、次の手順を実行します。

ステップ 1　管理許可をイネーブルにする場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] に移動し、[Perform authorization for exec shell access] > [Enable] チェックボックスをオンにします。

このオプションを選択すると、RADIUS の管理ユーザ特権レベルのサポートもイネーブルになります。管理ユーザ特権レベルは、ローカル コマンド特権レベルと組み合わせて、コマンド許可に使用できます。詳細については、「ローカル コマンド許可の設定」（P.13-31）を参照してください。

ステップ 2　ユーザを管理認証対象に設定するには、次の各 AAA サーバ タイプまたはローカル ユーザの要件を参照してください。

- RADIUS または LDAP（マッピングされた）ユーザ：次の値のいずれかについて、Service-Type 属性を設定します
  - [admin]：[Authentication] タブのオプションで指定されたすべてのサービスへのフル アクセスを許可します。
  - [nas-prompt]：Telnet 認証または SSH 認証のオプションを設定した場合は CLI へのアクセスを許可し、HTTP オプションを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。[Enable] オプションで**イネーブル**認証を設定した場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - [remote-access]：管理アクセスを拒否します。ユーザは、[Authentication] タブのオプションで指定されたいずれのサービスも使用できません（[Serial] オプションは除きます。つまり、シリアル アクセスは許可されます）。
- TACACS+ ユーザ：「service=shell」で許可が要求され、サーバは PASS または FAIL で応答します。

  - PASS（特権レベル 1）：[Authentication] タブのオプションで指定されたすべてのサービスへのフル アクセスを許可します。
  - PASS（特権レベル 2 以上）：Telnet 認証または SSH 認証のオプションを設定した場合は CLI へのアクセスを許可し、HTTP オプションを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。[Enable] オプションで**イネーブル**認証を設定した場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - FAIL：管理アクセスを拒否します。ユーザは、[Authentication] タブのオプションで指定されたいずれのサービスも使用できません（[Serial] オプションは除きます。つまり、シリアル アクセスは許可されます）。
- ローカル ユーザ：[Access Restriction] オプションを設定します。「[Add/Edit User Account] > [Identity]」（P.12-9）を参照してください。アクセス制限のデフォルト値は [Full Access] です。この場合は、[Authentication] タブのオプションで指定されたすべてのサービスに対して、フル アクセスが許可されます。

コマンド許可の設定

コマンドへのアクセスを制御する場合、セキュリティ アプライアンスではコマンド許可を設定でき、ユーザが使用できるコマンドを決定できます。デフォルトでは、ログインするとユーザ EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカル データベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。

この項では、次のトピックについて取り上げます。

- 「コマンド許可の概要」（P.13-29）
- 「ローカル コマンド許可の設定」（P.13-31）
- 「TACACS+ コマンド許可の設定」（P.13-33）

コマンド許可の概要

この項では、コマンド許可について説明します。次の項目を取り上げます。

- 「サポートされるコマンド許可方式」（P.13-29）
- 「ユーザ クレデンシャルの維持について」（P.13-30）
- 「セキュリティ コンテキストとコマンド許可」（P.13-30）

サポートされるコマンド許可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：セキュリティ アプライアンスでコマンド特権レベルを設定します。ローカル ユーザ、RADIUS ユーザ、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、セキュリティ アプライアンスはそのユーザをローカル データベース、RADIUS、または LDAP サーバで定義されている特権レベルに所属させます。ユーザは、その特権レベル以下のコマンドにアクセスできます。すべてのユーザは、初めてログインするときに、ユーザ EXEC モード（レベル 0 または 1 のコマンド）にアクセスします。ユーザは、特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするために再び **enable** コマンドで認証するか、**login** コマンドでログイン（ローカル データベースに限る）できます。

（注）　ローカル データベース内にユーザが存在しなくても、また CLI 認証や **enable** 認証がない場合でも、ローカル コマンド許可を使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、セキュリティ アプライアンスによってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、セキュリティ アプライアンスによってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド許可をオンにするまで使用されません（後述の「ローカル コマンド許可の設定」を参照してください）。（**enable** の詳細については、『*Cisco Security Appliance Command Reference*』を参照してください）

- TACACS+ サーバ特権レベル：TACACS+ サーバで、ユーザまたはグループが CLI アクセスについて認証した後で使用できるコマンドを設定します。CLI でユーザが入力するすべてのコマンドは、TACACS+ サーバでチェックされます。

ユーザ クレデンシャルの維持について

ユーザがセキュリティ アプライアンスにログインする場合、ユーザとパスワードを入力して認証される必要があります。セキュリティ アプライアンスは、同じセッションで後ほど認証が再び必要になる場合に備えて、これらのセッション クレデンシャルを保持します。

次のコンフィギュレーションが設定されている場合、ユーザはログイン時にローカル サーバだけで認証されればよいことになります。その後に続く許可では、保存されたクレデンシャルが使用されます。また、特権レベル 15 のパスワードの入力を求めるプロンプトが表示されます。特権モードを出るときに、ユーザは再び認証されます。ユーザのクレデンシャルは特権モードでは保持されません。

- ローカル サーバは、ユーザ アクセスの認証を行うように設定されます。
- 特権レベル 15 のコマンド アクセスは、パスワードを要求するように設定されます。
- ユーザのアカウントは、シリアル許可専用（コンソールまたは ASDM へのアクセスなし）として設定されます。
- ユーザのアカウントは、特権レベル 15 のコマンド アクセス用に設定されます。

次の表に、セキュリティ アプライアンスでのクレデンシャルの使用方法を示します。

必要なクレデンシャル	ユーザ名とパスワードによる認証	シリアル許可	特権モード コマンド許可	特権モード終了許可
ユーザ名	Yes	No	No	Yes
パスワード	Yes	No	No	Yes
特権モードのパスワード	No	No	Yes	No

セキュリティ コンテキストとコマンド許可

マルチ セキュリティ コンテキストでコマンド許可を実装する場合の重要な考慮点を次に示します。

- AAA 設定はコンテキストごとに個別であり、コンテキスト間で共有されません。

  コマンド許可を設定する場合は、各セキュリティ コンテキストを別々に設定する必要があります。これにより、異なるセキュリティ コンテキストに対して異なるコマンド許可を実行できます。

  セキュリティ コンテキストを切り替える場合、管理者は、ログイン時に指定したユーザ名で許可されるコマンドが新しいコンテキスト セッションでは異なる可能性があることや、新しいコンテキストではコマンド許可がまったく設定されていない可能性があることを念頭に置いてください。

コマンド許可がセキュリティ コンテキストによって異なる場合があることを管理者が理解していないと、混乱が生じる可能性があります。この動作は、次の仕組みによってさらに複雑になります。

- **changeto** コマンドによって開始された新しいコンテキスト セッションでは、前のコンテキスト セッションで使用されたユーザ名に関係なく、管理者 ID として常にデフォルトの「enable_15」ユーザ名が使用されます。これにより、enable_15 ユーザに対してコマンド許可が設定されていない場合や、enable_15 ユーザの許可が前のコンテキスト セッションでのユーザの許可と異なる場合に、混乱が生じる可能性があります。

  これは、発行される各コマンドを特定の管理者に正確に関連付けることができる場合に限り有効となる、コマンド アカウンティングにも影響します。**changeto** コマンドの使用が許可されているすべての管理者は enable_15 ユーザ名を他のコンテキストで使用できるため、enable_15 ユーザ名でログインしたユーザをコマンド アカウンティング レコードで簡単に特定できるとは限りません。コンテキストごとに異なるアカウンティング サーバを使用する場合は、enable_15 ユーザ名を使用していたユーザを追跡するために数台のサーバのデータを相関させる必要が生じます。

  コマンド許可を設定する場合は、次の点を考慮します。

  - **changeto** コマンドの使用が許可されている管理者は、実質的に、他のコンテキストそれぞれで enable_15 ユーザに許可されているすべてのコマンドを使用する許可を持ちます。
  - コンテキストごとに別々にコマンドを許可する場合は、**changeto** コマンドの使用許可を持つ管理者に対しても拒否されるコマンドが enable_15 ユーザ名でも拒否されることを、各コンテキストで確認してください。

  セキュリティ コンテキストを切り替える場合、管理者は特権 EXEC モードを終了し、再度 **enable** コマンドを入力して必要なユーザ名を使用できます。

（注）　システム実行スペースでは AAA コマンドがサポートされないため、システム実行スペースではコマンド許可を使用できません。

ローカル コマンド許可の設定

ローカル コマンド許可を使用して、コマンドを 16 の特権レベル（0 ～ 15）の 1 つに割り当てることができます。デフォルトでは、各コマンドは特権レベル 0 または 15 に割り当てられます。各ユーザを特定の特権レベルに定義でき、各ユーザは定義された特権レベル以下のコマンドを入力できます。セキュリティ アプライアンスは、ローカル データベース、RADIUS サーバ、または LDAP サーバ（LDAP 属性を RADIUS 属性にマッピングする場合）で定義されたユーザ特権レベルをサポートしています。「LDAP 属性マップの設定」（P.12-24）を参照してください。

この項では、次のトピックについて取り上げます。

ローカル コマンド許可の前提条件

コマンド許可コンフィギュレーションの一部として、次のタスクを実行します。

- **enable** 認証を設定します（「CLI、ASDM、および enable コマンドの認証の設定」（P.13-27）を参照）。

  enable 認証は、ユーザが **enable** コマンドにアクセスした後にユーザ名を保持するためには不可欠です。

あるいは、設定を必要としない **login** コマンド（これは、認証されている **enable** コマンドと同じでローカル データベースの場合に限る）を使用することもできます。このオプションは **enable** 認証ほど安全ではないため、お勧めしません。

CLI 認証を使用することもできますが、必須ではありません。

- 次に示すユーザ タイプごとの前提条件を確認してください。
  - ローカル データベース ユーザ: ローカル データベース内の各ユーザの特権レベルを 0 ～ 15 で設定します。

    ローカル データベースを設定するには、「ローカル データベースの設定」（P.12-8）を参照してください。
  - RADIUS ユーザ：ユーザの Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。
  - LDAP ユーザ：ユーザを特権レベル 0 ～ 15 の間で設定し、次に「LDAP 属性マップの設定」（P.12-24）の説明に従って、LDAP 属性を Cisco VAS CVPN3000-Priviledge-Level にマッピングします。

デフォルトのコマンド特権レベル

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のすべてのコマンドは、レベル 15 です。

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、**configure** コマンドも同じレベルに移動してください。このようにしないと、ユーザはコンフィギュレーション モードに入ることができません。

コマンドへの特権レベルの割り当てと許可のイネーブル化

コマンドを新しい特権レベルに割り当て、許可をイネーブル化するには、次の手順を実行します。

ステップ 1　コマンド許可をイネーブルにする場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] に移動し、[Enable authorization for command access] > [Enable] チェックボックスをオンにします。

ステップ 2　[Server Group] ドロップダウン リストから、[LOCAL] を選択します。

ステップ 3　ローカル コマンド許可をイネーブルにすると、オプションで、特権レベルを個々のコマンドまたはコマンド グループに手動で割り当てたり、事前定義済みユーザ アカウント特権をイネーブルにしたりできます。

- 事前定義済みユーザ アカウント特権を使用する場合は、[Set ASDM Defined User Roles] をクリックします。

  [ASDM Defined User Roles Setup] ダイアログボックスに、コマンドとそのレベルが表示されます。[Yes] をクリックすると、事前定義済みユーザ アカウント特権を使用できるようになります。事前定義済みユーザ アカウント特権には、[Admin]（特権レベル 15、すべての CLI コマンドへのフル アクセス権）、[Read Only]（特権レベル 5、読み取り専用アクセス権）、[Monitor Only]（特権レベル 3、[Monitoring] セクションへのアクセス権のみ）があります。

- コマンド レベルを手動で設定する場合は、[Configure Command Privileges] ボタンをクリックします。

  [Command Privileges Setup] ダイアログボックスが表示されます。[Command Mode] ドロップダウン リストから [--All Modes--] を選択すると、すべてのコマンドを表示できます。代わりに、コンフィギュレーション モードを選択し、そのモードで使用可能なコマンドを表示することもできます。たとえば、[context] を選択すると、コンテキスト コンフィギュレーション モードで使用可能なすべてのコマンドを表示できます。コンフィギュレーション モードだけでなく、ユーザ EXEC モードや特権 EXEC モードでも入力が可能で、かつモードごとに異なるアクションが実行されるようなコマンドを使用する場合は、これらのモードに対して別個に特権レベルを設定できます。

  [Variant] カラムには、[show]、[clear]、または [cmd] が表示されます。特権は、コマンドの show 形式、clear 形式、または configure 形式に対してのみ設定できます。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。

  コマンドのレベルを変更する場合は、コマンドをダブルクリックするか、[Edit] をクリックします。レベルは 0 ～ 15 の範囲で設定できます。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。

  表示されているすべてのコマンドのレベルを変更する場合は、[Select All] をクリックした後に、[Edit] をクリックします。

  [OK] をクリックして変更内容を確定します。

ステップ 4　RADIUS の管理ユーザ特権レベルをサポートする場合は、[Perform authorization for exec shell access] > [Enable] チェックボックスをオンにします。

このオプションを設定しないと、セキュリティ アプライアンスではローカル データベース ユーザの特権レベルだけがサポートされ、他のタイプのユーザにはデフォルトのレベル 15 がそのまま適用されます。

また、このオプションを設定すると、ローカル ユーザ、RADIUS ユーザ、LDAP（マッピング済み）ユーザ、および TACACS+ ユーザに対する管理許可がイネーブルになります。詳細については、「管理許可によるユーザ CLI および ASDM アクセスの制限」（P.13-28）を参照してください。

ステップ 5　[Apply] をクリックします。

TACACS+ コマンド許可の設定

TACACS+ コマンド許可をイネーブルにし、ユーザが CLI でコマンドを入力すると、セキュリティ アプライアンスはそのコマンドとユーザ名を TACACS+ サーバに送信し、コマンドが許可されているかどうかを判別します。

TACACS+ サーバによるコマンド許可を設定するときは、意図したとおりに機能することが確認できるまで、コンフィギュレーションを保存しないでください。間違いによりロック アウトされた場合、通常はセキュリティ アプライアンスを再起動することによってアクセスを回復できます。それでもロックアウトされたままの場合は、「ロックアウトからの回復」（P.13-39）を参照してください。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバ システムとセキュリティ アプライアンスへの完全冗長接続が必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続された 1 つのサーバとインターフェイス 2 に接続された別のサーバを含めます。TACACS+ サーバが使用できない場合にフォールバック方式としてローカル コマンド許可を設定することもできます。この場合は、「コマンド許可の設定」（P.13-29）に従ってローカル ユーザとコマンド特権レベルを設定する必要があります。

この項では、次のトピックについて取り上げます。

TACACS+ コマンド許可の前提条件

CLI および**イネーブル**認証を設定します（「CLI、ASDM、および enable コマンドの認証の設定」（P.13-27）を参照）。

TACACS+ サーバでのコマンドの設定

グループまたは個々のユーザの共有プロファイル コンポーネントとしての Cisco Secure Access Control Server（ACS）TACACS+ サーバでコマンドを設定できます。サードパーティの TACACS+ サーバの場合は、コマンド許可サポートの詳細については、ご使用のサーバのマニュアルを参照してください。

Cisco Secure ACS バージョン 3.1 でコマンドを設定する場合は、次のガイドラインを参照してください。

- セキュリティ アプライアンスは、「シェル」コマンドとして許可するコマンドを送信し、TACACS+ サーバでシェル コマンドとしてコマンドを設定します。

（注） Cisco Secure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれている場合があります。このタイプはセキュリティ アプライアンス コマンド許可に使用しないでください。

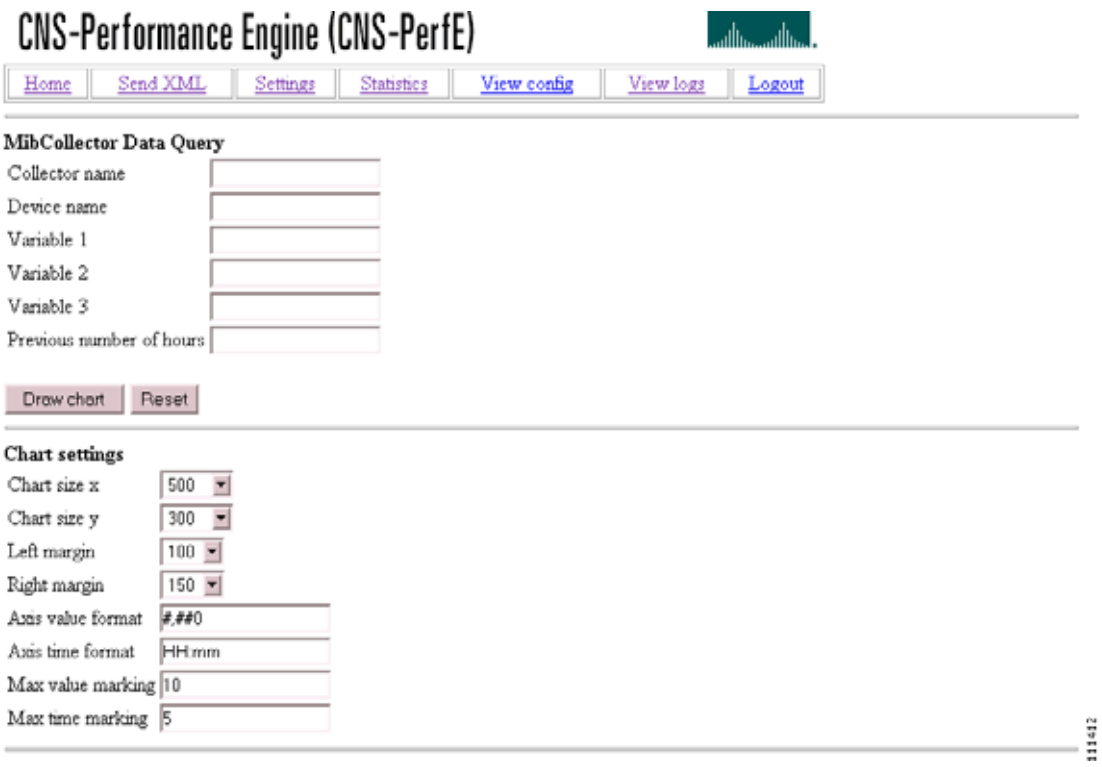
- コマンドの最初のワードは、メイン コマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。

  たとえば、**show running-configuration aaa-server** コマンドを許可するには、**show running-configuration** をコマンド ボックスに追加し、**permit aaa-server** を引数ボックスに入力します。

- [Permit Unmatched Args] チェックボックスを選択することによって、明示的に拒否していないコマンドのすべての引数を許可することができます。

  たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す **?** や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします（図 13-1 を参照）。

図 13-1　関連するすべてのコマンドの許可



- **enable** や **help** など、単一ワードのコマンドについては、そのコマンドに引数がない場合でも、一致しない引数を許可する*必要があります*（図 13-2 を参照）。

図 13-2　単一ワードのコマンドの許可

- 引数を拒否するには、その引数の前に **deny** を入力します。

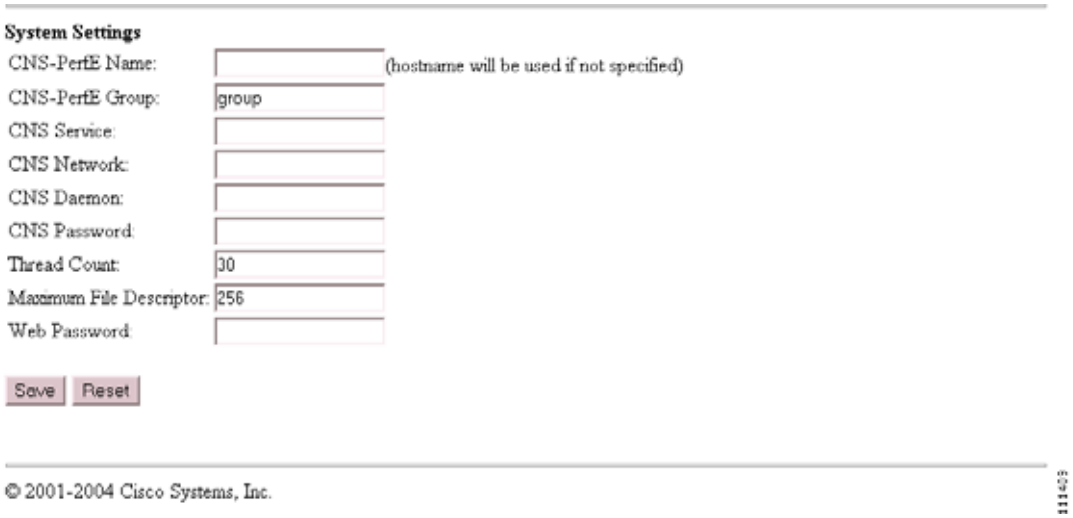
  たとえば、**enable** を許可し、**enable password** を許可しない場合は、コマンド ボックスに **enable** と入力し、引数ボックスに **deny password** と入力します。**enable** だけが許可されるように、[Permit Unmatched Args] チェックボックスを選択してください（図 13-3 を参照）。

図 13-3　引数の拒否

- コマンドラインでコマンドを省略形で入力した場合、セキュリティ アプライアンスはプレフィックスとメイン コマンドを完全なテキストに展開しますが、その他の引数は入力したとおりに TACACS+ サーバに送信します。

  たとえば、**sh log** と入力すると、セキュリティ アプライアンスは完全なコマンド **show logging** を TACACS+ サーバに送信します。一方、**sh log mess** と入力すると、セキュリティ アプライアンスは展開されたコマンド **show logging message** ではなく、**show logging mess** を TACACS+ サーバに送信します。省略形を予想して同じ引数に複数のスペルを設定できます（図 13-4 を参照）。

図 13-4　省略形の指定



- すべてのユーザに対して次の基本コマンドを許可することをお勧めします。
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**
  - **clear pager**
  - **quit**
  - **show version**

TACACS+ コマンド許可のイネーブル化

TACACS+ コマンド許可をイネーブルにする前に、TACACS+ サーバで定義されたユーザとしてセキュリティ アプライアンスにログインしていること、およびセキュリティ アプライアンスの設定を続けるために必要なコマンド許可があることを確認してください。たとえば、すべてのコマンドが許可された管理ユーザとしてログインする必要があります。このようにしないと、意図せずロックアウトされる可能性があります。

TACACS+ コマンド許可を設定するには、次の手順を実行します。

ステップ 1　TACACS+ サーバを使用したコマンド許可を実行する場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] に移動し、[Enable authorization for command access] > [Enable] チェックボックスをオンにします。

ステップ 2　[Server Group] ドロップダウン リストから、AAA サーバ グループ名を選択します。

ステップ 3　（任意）AAA サーバが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるようにセキュリティ アプライアンスを設定できます。[Use LOCAL when server group fails] チェックボックスをオンにします。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、セキュリティ アプライアンスのプロンプトでは、いずれの方式が使用されているかが示されないためです。

ステップ 4　[Apply] をクリックします。

管理アクセス アカウンティングの設定

管理アクセスのアカウンティングをイネーブルにするには、次の手順を実行します。

ステップ 1　最初にセキュリティ アプライアンスで認証したユーザだけを計上できるので、「CLI、ASDM、および enable コマンドの認証の設定」（P.13-27）を使用して認証を設定します。

ステップ 2　ユーザが **enable** コマンドを入力した場合にそのユーザのアカウンティングをイネーブルにするには、次の手順を実行します。

a. [Configuration] > [Device Management] > [Users/AAA] >[AAA Access] > [Accounting] に移動し、[Require accounting to allow accounting of user activity] > [Enable] チェックボックスをオンにします。

b. [Server Group] ドロップダウン リストから、RADIUS サーバ グループまたは TACACS+ サーバ グループの名前を選択します。

ステップ 3　ユーザが Telnet、SSH、またはシリアル コンソールを使用してセキュリティ アプライアンスにアクセスした場合にそのユーザのアカウンティングをイネーブルにするには、次の手順を実行します。

a. [Require accounting for the following types of connections] 領域で、[Serial]、[SSH]、[Telnet] の中から目的のチェックボックスをオンにします（複数可）。

b. 接続タイプごとに、[Server Group] ドロップダウン リストから RADIUS サーバ グループまたは TACACS+ サーバ グループの名前を選択します。

ステップ 4　コマンド アカウンティングを設定するには、次の手順を実行します。

a. [Require command accounting] 領域で、[Enable] チェックボックスをオンにします。

b. [Server Group] ドロップダウン リストから、TACACS+ サーバ グループの名前を選択します。RADIUS はサポートされていません。

CLI で **show** コマンド以外のコマンドを入力する場合、アカウンティング メッセージを TACACS+ アカウンティング サーバに送信できます。

c. [Command Privilege Setup] ダイアログボックスを使用してコマンド特権レベルをカスタマイズする際（「コマンドへの特権レベルの割り当てと許可のイネーブル化」（P.13-32）を参照）、[Privilege level] ドロップダウン リストで最小特権レベルを指定することで、セキュリティ アプライアンスのアカウンティング対象となるコマンドを制限できます。最小特権レベルよりも下のコマンドは、セキュリティ アプライアンスで処理の対象となりません。

ステップ 5　[Apply] をクリックします。

ロックアウトからの回復

状況によっては、コマンド許可や CLI 認証をオンにすると、セキュリティ アプライアンス CLI からロックアウトされる場合があります。通常は、セキュリティ アプライアンスを再起動することによってアクセスを回復できます。ただし、すでにコンフィギュレーションを保存した場合は、ロックアウトされたままになる可能性があります。表 13-3 に、一般的なロックアウト条件と回復方法を示します。

表 13-3　CLI 認証およびコマンド許可のロックアウト シナリオ

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
ローカル CLI 認証	ローカル データベース内にユーザが存在しない。	ローカル データベース内にユーザが存在しない場合は、ログインできず、ユーザの追加もできません。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザを追加することができます。
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバがダウンしているか到達不能で、フォールバック方式を設定していない。	サーバが到達不能である場合は、ログインもコマンドの入力もできません。	1. ログインし、パスワードと AAA コマンドをリセットします。 2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。	1. セキュリティ アプライアンスでネットワーク コンフィギュレーションが正しくないためサーバが到達不能である場合は、スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてネットワークを再設定することができます。 2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。

表 13-3　CLI 認証およびコマンド許可のロックアウト シナリオ （続き）

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
TACACS+ コマンド許可	十分な特権のないユーザまたは存在しないユーザとしてログインした。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	TACACS+ サーバのユーザ アカウントを修正します。 TACACS+ サーバへのアクセス権がなく、セキュリティ アプライアンスをすぐに設定する必要がある場合は、メンテナンス パーティションにログインして、パスワードと **aaa** コマンドをリセットします。	スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてコンフィギュレーションの変更を完了することができます。また、TACACS+ コンフィギュレーションを修正するまでコマンド許可をディセーブルにすることもできます。
ローカル コマンド許可	十分な特権のないユーザとしてログインしている。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザ レベルを変更することができます。

CHAPTER 14

ハイ アベイラビリティ

ここでは、次の内容について説明します。

フェールオーバーについて

[Failover] ペインには、セキュリティ アプライアンスでフェールオーバーを構成するための各種設定が含まれています。ただし、[Failover] ペインは、マルチ モードであるかシングル モードであるかによって変化し、マルチ モードのときは使用しているセキュリティ コンテキストに基づいて変化します。

フェールオーバーを使用すると、2 台のセキュリティ アプライアンスを設定して、一方に障害が発生した場合にもう一方がその動作を引き継ぐようにすることができます。ペアになっているセキュリティ アプライアンスを使用することで、オペレータの介入を必要としない高可用性を実現できます。セキュリティ アプライアンスは、専用のフェールオーバー リンクでフェールオーバー情報を伝達します。このフェールオーバー リンクには、LAN ベースの接続、または PIX セキュリティ アプライアンス プラットフォームでは専用シリアル フェールオーバー ケーブルのいずれかを使用できます。次の情報がフェールオーバー リンク経由で伝達されています。

- フェールオーバーの状態（アクティブまたはスタンバイ）
- Hello メッセージ（キープアライブ）
- ネットワーク リンク ステータス
- MAC アドレス交換
- コンフィギュレーションの複製

注意 フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

セキュリティ アプライアンスは、Active/Standby と Active/Active の 2 つのフェールオーバー タイプをサポートします。また、フェールオーバーは、ステートフルにもステートレスにもできます。フェールオーバーのタイプの詳細については、次の項目を参照してください。

Active/Standby フェールオーバー

Active/Standby コンフィギュレーションでは、アクティブ セキュリティ アプライアンスが、フェールオーバー ペアを通過するすべてのネットワーク トラフィックを処理します。スタンバイ セキュリティ アプライアンスは、アクティブ セキュリティ アプライアンスに障害が発生するまでネットワーク トラフィックを処理しません。アクティブ セキュリティ アプライアンスのコンフィギュレーションが変更されると、その都度コンフィギュレーション情報がフェールオーバー リンク経由でスタンバイ セキュリティ アプライアンスに送信されます。

フェールオーバーが実行されると、スタンバイ セキュリティ アプライアンスはアクティブ装置になります。前のアクティブ装置の IP アドレスと MAC アドレスが使用されます。IP アドレスまたは MAC アドレスの変更はネットワーク上の他のデバイスには認識されないため、ARP エントリがネットワーク上で変更されたりタイムアウトしたりすることはありません。

Active/Standby フェールオーバーは、シングル モードでもマルチ モードでも、セキュリティ アプライアンスで使用できます。

アクティブ/アクティブ フェールオーバー

Active/Active フェールオーバー コンフィギュレーションでは、両方のセキュリティ アプライアンスがネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードのセキュリティ アプライアンスでのみ使用できます。

セキュリティ アプライアンスで Active/Active フェールオーバーをイネーブルにするには、フェールオーバー グループを作成する必要があります。フェールオーバー グループを作成しないでフェールオーバーをイネーブルにすると、アクティブ/スタンバイ フェールオーバーがイネーブルになります。フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。セキュリティ アプライアンスには、2 つのフェールオーバー グループを作成できます。フェールオーバー グループ 1 がアクティブ状態になる装置にフェールオーバー グループを作成する必要があります。管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバです。

アクティブ/スタンバイ フェールオーバーと同様、アクティブ/アクティブ フェールオーバー ペアの各装置には、プライマリまたはセカンダリのどちらかが指定されます。アクティブ/スタンバイ フェールオーバーとは異なり、両方の装置が同時に起動した場合にどちらの装置がアクティブになるかは指示されていません。設定の各フェールオーバー グループには、プライマリまたはセカンダリ ロール プリファレンスが設定されます。このプリファレンスにより、両方の装置を同時に起動したときに、グループのコンテキストがアクティブ ステートになるフェールオーバー ペアの装置が決まります。ペアの一方の装置にアクティブ状態の両方のフェールオーバー グループを含めて、もう一方の装置にスタンバイ状態のフェールオーバー グループを含めることができます。ただし、一般的な設定では、各フェールオーバー グループに別々のロール プリファレンスを割り当てて、それぞれを別の装置上でアクティブにすることでデバイスにトラフィックを分散させます。

初期設定同期は、一方または両方の装置が起動すると実行されます。この同期は、次のように実行されます。

- 両方の装置が同時に起動した場合、設定はプライマリ装置からセカンダリ装置に同期されます。
- 一方の装置がすでにアクティブであるときに、もう一方の装置が起動した場合は、起動した装置が、すでにアクティブな装置から設定を受信します。

両方の装置が動作中になった後で、次のように、コマンドが一方の装置からもう一方の装置に複製されます。

- セキュリティ コンテキスト内で入力されたコマンドは、そのセキュリティ コンテキストがアクティブ状態で表示される装置からピア装置に複製されます。

（注） あるコンテキストがある装置でアクティブ状態と見なされるのは、そのコンテキストが属するフェールオーバー グループがその装置上でアクティブ状態である場合です。

- システム実行スペースに入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態である装置から、フェールオーバー グループ 1 がスタンバイ状態である装置に複製されます。
- 管理コンテキストで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態である装置から、フェールオーバー グループ 1 がスタンバイ状態である装置に複製されます。

コマンドの複製の実行に適切な装置上でコマンドを入力しなかった場合は、設定が非同期になります。この変更内容は、次回に初期コンフィギュレーション同期が行われると失われることがあります。

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、フェールオーバーは、システムごとに行うのではなく、フェールオーバー グループごとに行われます。たとえば、プライマリ装置で両方のフェールオーバー グループをアクティブと指定した場合にフェールオーバー グループ 1 で障害が発生すると、フェールオーバー グループ 2 はプライマリ装置でアクティブのままですが、フェールオーバー グループ 1 はセカンダリ装置でアクティブになります。

（注） アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。

ステートレス（標準）フェールオーバー

ステートレス フェールオーバーは、通常フェールオーバーとも呼ばれます。ステートレス フェールオーバーでは、フェールオーバーが行われると、アクティブ接続はすべてドロップされます。新しいアクティブ装置が引き継ぐ場合、クライアントは接続を再確立する必要があります。

ステートフル フェールオーバー

（注） ステートフル フェールオーバーは、ASA 5505 シリーズ適応型セキュリティ アプライアンスではサポートされていません。

ステートフル フェールオーバーがイネーブルになっている場合、フェールオーバー ペアのアクティブ装置は接続ごとのステート情報をスタンバイ装置に常に渡しています。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

（注）　ステートおよび LAN フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。

ステートフル フェールオーバーを使用するには、ステート リンクがすべてのステート情報をスタンバイ装置に渡すように設定する必要があります。シリアル フェールオーバー インターフェイス（PIX セキュリティ アプライアンス プラットフォームだけで使用可）ではなく、LAN フェールオーバー接続を使用している場合、フェールオーバー リンクとしてステート リンクに同じインターフェイスを使用できます。ただし、スタンバイ装置にステート情報を渡すときは、専用のインターフェイスを使用することをお勧めします。

ステートフル フェールオーバーがイネーブルになっているとき、次の情報がスタンバイ装置に渡されます。

- NAT 変換テーブル
- タイムアウト接続などの TCP 接続テーブル（HTTP を除く）
- HTTP 接続状態（HTTP 複製がイネーブルの場合）
- H.323、SIP、および MGCP UDP メディア接続
- システム クロック
- ISAKMP および IPSec SA テーブル

ステートフル フェールオーバーがイネーブルになっているとき、次の情報はスタンバイ装置にコピーされません。

- HTTP 接続テーブル（HTTP 複製がイネーブルでない場合）
- ユーザ認証（uauth）テーブル
- ARP テーブル
- ルーティング テーブル

High Availability and Scalability Wizard を使用したフェールオーバーの設定

High Availability and Scalability Wizard では、Active/Active フェールオーバー コンフィギュレーション、および Active/Standby フェールオーバー コンフィギュレーション、または VPN Cluster Load Balancing コンフィギュレーションを作成するプロセスの手順が示されます。

High Availability and Scalability Wizard の使用の詳細については、次の項目を参照してください。

- 「High Availability and Scalability Wizard へのアクセスと使用」（P.14-5）
- 「High Availability and Scalability Wizard を使用した Active/Active フェールオーバーの設定」（P.14-5）
- 「High Availability and Scalability Wizard を使用した Active/Standby フェールオーバーの設定」（P.14-6）
- 「High Availability and Scalability Wizard を使用した VPN ロード バランシングの設定」（P.14-7）
- 「High Availability and Scalability Wizard のフィールド情報」（P.14-7）

High Availability and Scalability Wizard へのアクセスと使用

High Availability and Scalability Wizard を開くには、ASDM メニューバーで [Wizards] > [High Availability and Scalability Wizard] の順に選択します。ウィザードの最初の画面が表示されます。

ウィザードの次の画面に移動するには、[Next] ボタンをクリックします。次の画面に移動する前に、各画面の必須フィールドへの入力を完了する必要があります。

ウィザードの前の画面に戻るには、[Back] ボタンをクリックします。ウィザードの後の画面に入力した情報に前の画面で行った変更が反映されていない場合でも、ウィザードを進んでいけば入力した情報は画面上に残っています。情報を再度入力する必要はありません。

[Cancel] をクリックすると、変更内容を保存せずにいつでもウィザードを終了できます。

ウィザードの最後にコンフィギュレーションをセキュリティ アプライアンスに送信するには、[Finish] をクリックします。

High Availability and Scalability Wizard を使用した Active/Active フェールオーバーの設定

次の手順では、High Availability and Scalability Wizard を使用した Active/Active フェールオーバーの設定の概要を説明します。手順の各ステップは、ウィザード画面に対応しています。各ステップを実行したら、次のステップに進む前に [Next] をクリックします（ただし、最終ステップを除きます）。また、各ステップには、実行に必要な追加情報への参照も含まれています。

ステップ 1　[Choose the type of failover configuration] 画面で [Configure Active/Active] フェールオーバーを選択します。

この画面の詳細については、「Choose the Type of Failover Configuration」（P.14-8）を参照してください。

ステップ 2　[Check Failover Peer Connectivity and Compatibility] 画面にフェールオーバー ピアの IP アドレスを入力します。[Test Compatibility] をクリックします。すべての互換性テストに合格するまで、次の画面に進むことはできません。

この画面の詳細については、「Check Failover Peer Connectivity and Compatibility」（P.14-9）を参照してください。

ステップ 3　セキュリティ アプライアンスまたはフェールオーバー ピアがシングル コンテキスト モードである場合、[Change Device to Multiple Mode] 画面でマルチ コンテキスト モードに変更します。セキュリティ アプライアンスをマルチ コンテキスト モードに変更すると、リブートされます。リブートが完了すると、ASDM は自動的にセキュリティ アプライアンスとの通信を再確立します。

この画面の詳細については、「Change Device to Multiple Mode」（P.14-9）を参照してください。

ステップ 4　（PIX 500 シリーズ セキュリティ アプライアンスのみ）[Select Failover Communication Media] 画面で、ケーブルベース フェールオーバーまたは LAN ベース フェールオーバーを選択します。

この画面の詳細については、「Select Failover Communication Media」（P.14-10）を参照してください。

ステップ 5　[Context Configuration] 画面で、フェールオーバー グループにセキュリティ コンテキストを割り当てます。この画面では、コンテキストを追加または削除できます。

この画面の詳細については、「Security Context Configuration」（P.14-10）を参照してください。

ステップ 6　[Failover Link Configuration] 画面でフェールオーバー リンクを定義します。

この画面の詳細については、「Failover Link Configuration」（P.14-11）を参照してください。

ステップ 7　（ASA 5505 セキュリティ アプライアンスでは使用不可）[State Link Configuration] 画面でステートフル フェールオーバー リンクを定義します。

この画面の詳細については、「State Link Configuration」（P.14-12）を参照してください。

ステップ 8　[Standby Address Configuration] 画面で、スタンバイ アドレスをセキュリティ アプライアンス インターフェイスに追加します。

この画面の詳細については、「Standby Address Configuration」（P.14-12）を参照してください。

ステップ 9　[Summary] 画面でコンフィギュレーションを確認します。必要に応じて [Back] ボタンを使用し、前の画面に戻って変更します。

この画面の詳細については、「Summary」（P.14-15）を参照してください。

ステップ 10　[Finish] をクリックします。

フェールオーバー コンフィギュレーションがセキュリティ アプライアンスとフェールオーバー ピアに送信されます。

High Availability and Scalability Wizard を使用した Active/Standby フェールオーバーの設定

次の手順では、High Availability and Scalability Wizard を使用した Active/Standby フェールオーバーの設定の概要を説明します。手順の各ステップは、ウィザード画面に対応しています。各ステップを実行したら、次のステップに進む前に [Next] をクリックします（ただし、最終ステップを除きます）。また、各ステップには、実行に必要な追加情報への参照も含まれています。

ステップ 1　[Choose the type of failover configuration] 画面で [Configure Active/Standby] フェールオーバーを選択します。[Next] をクリックします。

この画面の詳細については、「Choose the Type of Failover Configuration」（P.14-8）を参照してください。

ステップ 2　[Check Failover Peer Connectivity and Compatibility] 画面にフェールオーバー ピアの IP アドレスを入力します。[Test Compatibility] をクリックします。すべての互換性テストに合格するまで、次の画面に進むことはできません。

この画面の詳細については、「Check Failover Peer Connectivity and Compatibility」（P.14-9）を参照してください。

ステップ 3　（PIX 500 シリーズ セキュリティ アプライアンスのみ）[Select Failover Communication Media] 画面で、ケーブルベース フェールオーバーまたは LAN ベース フェールオーバーを選択します。

この画面の詳細については、「Select Failover Communication Media」（P.14-10）を参照してください。

ステップ 4　[Failover Link Configuration] 画面でフェールオーバー リンクを定義します。

この画面の詳細については、「Failover Link Configuration」（P.14-11）を参照してください。

ステップ 5　（ASA 5505 セキュリティ アプライアンスでは使用不可）[State Link Configuration] 画面でステートフル フェールオーバー リンクを定義します。

この画面の詳細については、「State Link Configuration」（P.14-12）を参照してください。

ステップ 6　[Standby Address Configuration] 画面で、スタンバイ アドレスをセキュリティ アプライアンス インターフェイスに追加します。

この画面の詳細については、「Standby Address Configuration」（P.14-12）を参照してください。

ステップ 7　[Summary] 画面でコンフィギュレーションを確認します。必要に応じて [Back] ボタンを使用し、前の画面に戻って変更します。

この画面の詳細については、「Summary」（P.14-15）を参照してください。

ステップ 8　[Finish] をクリックします。

フェールオーバー コンフィギュレーションがセキュリティ アプライアンスとフェールオーバー ピアに送信されます。

High Availability and Scalability Wizard を使用した VPN ロード バランシングの設定

次の手順では、High Availability and Scalability Wizard を使用した VPN クラスタ ロード バランシングの設定の概要を説明します。手順の各ステップは、ウィザード画面に対応しています。各ステップを実行したら、次のステップに進む前に [Next] をクリックします（ただし、最終ステップを除きます）。また、各ステップには、実行に必要な追加情報への参照も含まれています。

ステップ 1　[Choose the type of failover configuration] 画面で [Configure VPN Cluster Load Balancing] フェールオーバーを選択します。

この画面の詳細については、「Choose the Type of Failover Configuration」（P.14-8）を参照してください。

ステップ 2　[VPN Cluster Load Balancing Configuration] 画面で VPN ロード バランシング設定を実行します。

この画面の詳細については、「VPN クラスタ ロード バランシングの設定」（P.14-13）を参照してください。

ステップ 3　[Summary] 画面でコンフィギュレーションを確認します。必要に応じて [Back] ボタンを使用し、前の画面に戻って変更します。

この画面の詳細については、「Summary」（P.14-15）を参照してください。

ステップ 4　[Finish] をクリックします。

フェールオーバー コンフィギュレーションがセキュリティ アプライアンスとフェールオーバー ピアに送信されます。

High Availability and Scalability Wizard のフィールド情報

High Availability and Scalability Wizard では、次のダイアログが使用できます。ウィザードの実行中に、すべてのダイアログボックスが表示されるわけではありません。表示される各ダイアログボックスは、設定するフェールオーバーのタイプと、その設定を行っているハードウェア プラットフォームによって異なります。

- 「Choose the Type of Failover Configuration」（P.14-8）
- 「Check Failover Peer Connectivity and Compatibility」（P.14-9）
- 「Change Device to Multiple Mode」（P.14-9）
- 「Security Context Configuration」（P.14-10）
- 「Failover Link Configuration」（P.14-11）

Choose the Type of Failover Configuration

[Choose the Type of Failover Configuration] 画面では、設定するフェールオーバーのタイプを選択できます。

フィールド

[Choose the Type of Failover Configuration] には、次の情報フィールドが表示されます。これらの情報フィールドは、セキュリティ アプライアンスのフェールオーバー機能の決定に役立ちます。

- [Hardware Model]：（*表示専用*）セキュリティ アプライアンスのモデル番号を表示します。
- [No. of Interfaces]：（*表示専用*）セキュリティ アプライアンスで使用可能なインターフェイスの数を表示します。
- [No. of Modules]：（*表示専用*）セキュリティ アプライアンスに取り付けられているモジュールの数を表示します。
- [Software Version]：（*表示専用*）セキュリティ アプライアンス上のプラットフォーム ソフトウェアのバージョンを表示します。
- [Failover License]：（*表示専用*）デバイスにインストールされたフェールオーバー ライセンスのタイプを表示します。フェールオーバーを設定するには、アップグレードしたライセンスの購入が必要になる場合があります。
- [Firewall Mode]：（*表示専用*）ファイアウォール モード（ルーテッドまたはトランスペアレント）およびコンテキスト モード（シングルまたはマルチ）を表示します。

設定しているフェールオーバー コンフィギュレーションのタイプを選択します。

- [Configure Active/Active Failover]：セキュリティ アプライアンスに Active/Active フェールオーバーを設定します。
- [Configure Active/Standby Failover]：セキュリティ アプライアンスに Active/Standby フェールオーバーを設定します。
- [Configure VPN Cluster Load Balancing]：セキュリティ アプライアンスがクラスタの一部として VPN ロード バランシングに参加するように設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Check Failover Peer Connectivity and Compatibility

[Check Failover Peer Connectivity and Compatibility] 画面では、選択したフェールオーバー ピアが到達可能で、現在の装置と互換性があることを確認できます。接続および互換性テストが失敗した場合、ウィザードの先に進む前に、問題を修正する必要があります。

フィールド

- [Peer IP Address]：ピア装置の IP アドレスを入力します。このアドレスはフェールオーバー リンクのアドレスでなくても構いませんが、ASDM アクセスがイネーブルになっているインターフェイスでなければなりません。
- [Test Compatibility]：このボタンをクリックして、次の接続テストおよび互換性テストを実行します。
  - ASDM からピア装置への接続テスト
  - ファイアウォール デバイスからピア ファイアウォール デバイスへの接続テスト
  - ハードウェア互換性テスト
  - ソフトウェア バージョンの互換性
  - フェールオーバー ライセンスの互換性
  - ファイアウォール モードの互換性

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Change Device to Multiple Mode

[Change Device to Multiple Mode] ダイアログボックスは、Active/Active フェールオーバー コンフィギュレーションでだけ表示されます。Active/Active フェールオーバーでは、セキュリティ アプライアンスがマルチ コンテキスト モードになっている必要があります。このダイアログボックスでは、シングルコンテキスト モードのセキュリティ アプライアンスをマルチ コンテキスト モードに変換します。

シングルコンテキスト モードからマルチ コンテキスト モードに変換するとき、セキュリティ アプライアンスは、現在実行しているコンフィギュレーションからシステム コンフィギュレーションと管理コンテキストを作成します。管理コンテキスト コンフィギュレーションは、admin.cfg というファイルに格納されます。変換プロセスでは、以前のスタートアップ コンフィギュレーションが保存されないので、スタートアップ コンフィギュレーションが実行中のコンフィギュレーションと異なる場合は、異なる部分が失われます。

セキュリティ アプライアンスをシングルコンテキスト モードからマルチ コンテキスト モードに変換すると、セキュリティ アプライアンスはリブートされます。ただし、High Availability and Scalability Wizard では、新規作成された管理コンテキストとの接続が復元され、このダイアログボックスで [Devices Status] フィールドのステータスが報告されます。

次に進む前に、現在のセキュリティ アプライアンスとピア セキュリティ アプライアンスの両方をマルチ コンテキスト モードに変換する必要があります。

フィールド

- [Change *device* To Multiple Context] : セキュリティ アプライアンスをマルチ コンテキスト モードに変更します。*device* の部分には、セキュリティ アプライアンスのホスト名が入ります。
- [Change *device* (peer) To Multiple Context] : ピア装置をマルチ コンテキスト モードに変更します。*device* の部分には、セキュリティ アプライアンスのホスト名が入ります。
- [Device Status] :（*表示専用*）マルチ コンテキスト モードへの変換中にセキュリティ アプライアンスのステータスが表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Select Failover Communication Media

[Select Failover Communication Media] は、PIX 500 シリーズ セキュリティ アプライアンスだけに表示されます。この画面では、フェールオーバー リンクにフェールオーバー ケーブルを使用するか、LAN ベースの接続を使用するかを選択できます。

フィールド

- [Use Failover Cable] : フェールオーバー通信に専用フェールオーバー ケーブルを使用するには、このオプションを選択します。
- [Use LAN-based connection] : フェールオーバー通信にネットワーク接続を使用するには、このオプションを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Security Context Configuration

[Security Context Configuration] 画面は、Active/Active コンフィギュレーションにだけ表示されます。[Security Context Configuration] 画面では、セキュリティ コンテキストをフェールオーバー グループに割り当てることができます。この画面では、デバイスで現在設定されているセキュリティ コンテキストが表示され、必要に応じて新しいセキュリティ コンテキストを追加したり、既存のコンテキストを削除したりできます。この画面でセキュリティ コンテキストを作成できますが、作成したコンテキ

ストにインターフェイスを割り当てたり、作成したコンテキストの他のプロパティを設定したりできません。コンテキスト プロパティを設定し、インターフェイスをコンテキストに割り当てるには、[System] > [Security Contexts] ペインを使用する必要があります。

フィールド

- [Name]：セキュリティ コンテキストの名前を表示します。名前を変更するには、名前をクリックして新しい名前を入力します。
- [Failover Group]：コンテキストの割り当て先であるフェールオーバー グループを表示します。セキュリティ コンテキストのフェールオーバー グループを変更するには、フェールオーバー グループをクリックし、ドロップダウン リストから新しいフェールオーバー グループ番号を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Failover Link Configuration

[Failover Link Configuration] 画面は、LAN ベースのフェールオーバーを設定している場合にだけ表示されます。ケーブルベースのフェールオーバーを PIX 500 シリーズ セキュリティ アプライアンスで設定している場合は表示されません。

フィールド

- [LAN Interface]：フェールオーバー通信に使用するインターフェイスをドロップダウン リストから選択します。
- [Logical Name]：インターフェイスの名前を入力します。
- [Active IP]：アクティブ状態のフェールオーバー グループ 1 がある装置上のフェールオーバー リンクに使用する IP アドレスを入力します。
- [Standby IP]：スタンバイ状態のフェールオーバー グループ 1 がある装置上のフェールオーバー リンクに使用する IP アドレスを入力します。
- [Subnet Mask]：アクティブ IP アドレスまたはスタンバイ IP アドレスのサブネット マスクを入力または選択します。
- [Secret Key]：（任意）フェールオーバー通信の暗号化に使用するキーを入力します。このフィールドを空白のままにした場合、コンフィギュレーション内のパスワードまたはキーをはじめ、コマンド複製中に送信されるフェールオーバー通信は、クリア テキストになります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

State Link Configuration

[State Link Configuration] 画面は、ASA 5505 プラットフォーム上で実行している ASDM のウィザードには表示されません。

[State Link Configuration] 画面では、ステートフル フェールオーバーをイネーブルにして、ステートフル フェールオーバー リンク プロパティを設定できます。

フィールド

- [Use the LAN link as the State Link] : LAN ベースのフェールオーバー リンクでステート情報を渡すには、このオプションを選択します。このオプションは、ケーブルベースのフェールオーバー向けに設定された PIX 500 シリーズ セキュリティ アプライアンスでは使用できません。
- [Disable Stateful Failover] : ステートフル フェールオーバーをディセーブルにするには、このオプションを選択します。
- [Configure another interface for Stateful failover] : 未使用のインターフェイスをステートフル フェールオーバー インターフェイスとして設定するには、このオプションを選択します。
  - [State Interface] : ステートフル フェールオーバー通信に使用するインターフェイスをドロップダウン リストから選択します。
  - [Logical Name] : ステートフル フェールオーバー インターフェイスの名前を入力します。
  - [Active IP] : アクティブ状態のフェールオーバー グループ 1 がある装置上のステートフル フェールオーバー リンクの IP アドレスを入力します。
  - [Standby IP] : スタンバイ状態のフェールオーバー グループ 1 がある装置上のステートフル フェールオーバー リンクの IP アドレスを入力します。
  - [Subnet Mask] : アクティブ IP アドレスまたはスタンバイ IP アドレスのサブネット マスクを入力または選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Standby Address Configuration

[Standby Address Configuration] 画面を使用して、セキュリティ アプライアンス上のインターフェイスにスタンバイ アドレスを割り当てます。

フィールド

- [Device/Interface]：（Active/Standby フェールオーバー）フェールオーバー装置上で設定されたインターフェイスを表示します。デバイス名の横のプラス記号（+）をクリックすると、そのデバイス上のインターフェイスが表示されます。デバイス名の横のマイナス記号（-）をクリックすると、そのデバイス上のインターフェイスが非表示になります。
- [Device/Group/Context/Interface]：（Active/Active フェールオーバー）フェールオーバー装置上で設定されたインターフェイスを表示します。インターフェイスはコンテキストでグループ化され、コンテキストはフェールオーバー グループでグループ化されます。デバイス、フェールオーバー グループ、コンテキスト名の横のプラス記号（+）をクリックすると、リストが展開されます。デバイス、フェールオーバー グループ、コンテキスト名の横のマイナス記号（-）をクリックすると、リストが折りたたまれます。
- [Active IP]：このフィールドをダブルクリックして、アクティブ IP アドレスを編集または追加できます。また、このフィールドに移動すると、ピア装置上の対応するインターフェイスが [Standby IP] フィールドに表示されます。
- [Standby IP]：このフィールドをダブルクリックすると、スタンバイ IP アドレスを編集または追加できます。また、このフィールドに移動すると、ピア装置上の対応するインターフェイスが [Active IP] フィールドに表示されます。
- [Is Monitored]：インターフェイスのヘルス モニタリングをイネーブルにするには、このチェックボックスをオンにします。チェックボックスをオフにすると、ヘルス モニタリングがディセーブルになります。デフォルトでは、物理インターフェイスのヘルス モニタリングはイネーブルに、仮想インターフェイスのヘルス モニタリングはディセーブルになっています。
- [ASR Group]：非同期グループ ID をドロップダウン リストから選択します。この設定は、物理インターフェイスにだけ使用可能です。仮想インターフェイスの場合、このフィールドには「None」が表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

VPN クラスタ ロード バランシングの設定

リモートクライアント コンフィギュレーションで、複数のセキュリティ アプライアンスを同じネットワークに接続してリモート セッションを処理している場合、これらのデバイスでセッション負荷を分担するように設定できます。この機能は、*ロード バランシング*と呼ばれます。ロード バランシングでは、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。これによって、システム リソースを効率的に利用でき、パフォーマンスと可用性が向上します。

[VPN Cluster Load Balancing Configuration] 画面を使用して、このデバイスがロード バランシング クラスタに参加するのに必要なパラメータを設定します。

（注） VPN ロード バランシングを使用するには、Plus ライセンスの ASA モデル 5510、あるいは ASA モデル 5520 または 5540 が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

ロード バランシングをイネーブルにするには、次の手順を実行します。

- 共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタの IPSec 共有秘密情報を確立することによりロード バランシング クラスタを設定する。これらの値は、クラスタ内のすべてのデバイスで同一です。
- デバイスでロード バランシングをイネーブルにし、デバイス固有のプロパティを定義することにより、参加デバイスを設定する。これらの値はデバイスによって異なります。

（注） ロード バランシングは、Cisco VPN Client（リリース 3.0 以降）、Cisco VPN 3002 Hardware Client（リリース 3.5 以降）、または Easy VPN クライアントとして動作している ASA 5505 で開始されたリモート セッションだけで有効です。LAN 間接続を含む他のすべてのクライアントは、ロード バランシングがイネーブルなセキュリティ アプライアンスに接続できますが、ロード バランシングには参加できません。

ロード バランシングを実装するには、同じプライベート LAN 間ネットワーク上の複数のデバイスを、論理的に*仮想クラスタ*としてグループ化します。

フィールド

- [Cluster IP Address]：仮想クラスタ全体を表す単一の IP アドレスを指定します。仮想クラスタ内のすべてのセキュリティ アプライアンスが共有するパブリック サブネットのアドレス範囲内で、IP アドレスを選択します。
- [Cluster UDP Port]：このデバイスが参加する仮想クラスタの UDP ポートを指定します。デフォルト値は 9023 です。別のアプリケーションでこのポートが使用されている場合は、ロードバランシングに使用する UDP の宛先ポート番号を入力します。
- [Enable IPSec Encryption]：IPSec 暗号化をイネーブルまたはディセーブルにします。このチェックボックスをオンにする場合は、共有秘密情報を指定し、確認する必要もあります。仮想クラスタ内のセキュリティ アプライアンスは、IPSec を使用して LAN-to-LAN トンネルを介して通信します。デバイス間で通信されるすべてのロード バランシング情報が暗号化されるようにするには、このチェックボックスをオンにします。

（注） 暗号化を使用する場合、事前にロードバランシング内部インターフェイスを設定しておく必要があります。そのインターフェイスがロードバランシング内部インターフェイスでイネーブルになっていない場合、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

クラスタの暗号化を設定したときにロードバランシング内部インターフェイスがイネーブルに設定されたが、仮想クラスタへのデバイス参加を設定する前にディセーブルにされた場合は、[Participate in Load Balancing Cluster] チェックボックスをオンにしたときにエラー メッセージが表示され、そのクラスタに対して暗号化はイネーブルになりません。

  - [Shared Secret Key]：IPSec 暗号化をイネーブルにするときに、IPSec ピア間の共有秘密情報を指定します。ボックスに入力する値は、連続するアスタリスク文字として表示されます。

- [Priority Of This Device]：クラスタ内でこのデバイスに割り当てられる優先順位を指定します。指定できる範囲は 1 ～ 10 です。プライオリティは、起動時または既存のマスターで障害が発生したときに、このデバイスが仮想クラスタ マスターになる可能性を表します。優先順位を高く設定すれば（10 など）、このデバイスが仮想クラスタ マスターになる可能性が高くなります。

（注） 仮想クラスタ内のデバイスを異なるタイミングで起動した場合、最初に起動したデバイスが、仮想クラスタ マスターの役割を果たすと想定されます。仮想クラスタにはマスターが必要であるため、起動したときに仮想クラスタ内の各デバイスはチェックを行い、クラスタに仮想マスターがあることを確認します。仮想マスターがない場合、そのデバイスがマスターの役割を果たします。後で起動し、クラスタに追加されたデバイスは、セカンダリ デバイスになります。仮想クラスタ内のすべてのデバイスが同時に起動されたときは、最高の優先順位が設定されたデバイスが仮想クラスタ マスターになります。仮想クラスタ内の複数のデバイスが同時に起動され、いずれも最高の優先順位が設定されている場合、最も低い IP アドレスを持つデバイスが仮想クラスタ マスターになります。

- [Public Interface Of This Device]：このデバイスのパブリック インターフェイスの名前または IP アドレスを指定します。
- [Private Interface Of This Device]：このデバイスのプライベート インターフェイスの名前または IP アドレスを指定します。
- [Send FQDN to client]：このチェックボックスをオンにすると、VPN クラスタ マスターが VPN クライアント接続をクラスタ デバイスにリダイレクトするときに、外部 IP アドレスの代わりにクラスタ デバイスのホスト名とドメイン名を使用して完全修飾ドメイン名が送信されるようになります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Summary

[Summary] 画面では、これまでのウィザード パネルで実行した設定手順の結果が表示されます。

フィールド

設定内容は画面中央に表示されます。設定を確認して [Finish] をクリックすると、設定内容がデバイスに送信されます。フェールオーバーを設定している場合、設定内容はフェールオーバー ピアにも送信されます。設定を変更する必要がある場合は、[Back] をクリックして変更する必要のある画面まで戻ります。変更を行ったら [Next] をクリックして [Summary] 画面まで戻ります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

[Failover] ペインのフィールド情報

フェールオーバー ペインに表示される内容は、現在のモード（シングル コンテキスト モードまたはマルチ コンテキスト モード）およびシステム実行スペースにいるか、セキュリティ コンテキスト内にいるかによって異なります。

ここでは、次の内容について説明します。

- [Failover]（シングル モード）
- [Failover]（マルチ モード、セキュリティ コンテキスト）
- [Failover]（マルチ モード、システム）

[Failover]（シングル モード）

[Failover] ペインには、シングルコンテキスト モードで Active/Standby フェールオーバーを設定できるタブが含まれています。フェールオーバーの詳細については、フェールオーバーについてを参照してください。[Failover] ペインの各タブでの設定の詳細については、次の情報を参照してください。ルーテッド ファイアウォール モードであるか、トランスペアレント ファイアウォール モードであるかによって、[Interfaces] タブが変わります。

- [Failover]: [Setup]
- [Failover]: [Interfaces]（ルーテッド ファイアウォール モード）
- [Failover]: [Interfaces]（トランスペアレント ファイアウォール モード）
- [Failover]: [Criteria]
- [Failover]: [MAC Addresses]

[Failover]: [Setup]

このタブを使用して、セキュリティ アプライアンスでフェールオーバーをイネーブルにします。また、ステートフル フェールオーバーを使用している場合、このタブではフェールオーバー リンクおよびステート リンクも指定できます。

一般的なフェールオーバーの設定方法の詳細については、「フェールオーバーについて」を参照してください。

フィールド

- [Enable Failover]：このチェックボックスをオンにすると、フェールオーバーがイネーブルになり、スタンバイ セキュリティ アプライアンスを設定できます。

（注）　フェールオーバー インターフェイスの速度と二重通信の設定は、フェールオーバーがイネーブルになっても変わりません。フェールオーバー インターフェイスの速度や二重通信の設定を変更するには、フェールオーバーをイネーブルにする前に、[Configuration] > [Interfaces] ペインで設定しておく必要があります。

ASDM では、フェールオーバーをイネーブルにするときに、ピア装置を設定するかどうかを確認するダイアログボックスが表示されます。このダイアログボックスは、Preferred Role 設定、または PIX セキュリティ アプライアンス プラットフォームでの（シリアル ケーブル フェールオーバーではなく）Enable LAN 設定が変更されたときにも表示されます。

  - [Peer IP Address]：ASDM が接続されているピア装置での IP アドレスを入力します。このフィールドは、[Do you want to configure the failover peer firewall] ダイアログボックスに表示されます。

- [Use 32 hexadecimal character key]：[Shared Key] ボックスに 16 進数値の暗号キーを入力するには、このチェックボックスをオンにします。[Shared Key] ボックスに英数字の共有秘密情報を入力する場合は、このチェックボックスをオフにします。
- [Shared Key]：フェールオーバー共有秘密情報またはフェールオーバー ペア間での暗号化および認証済み通信のためのキーを指定します。

  [Use 32 hexadecimal character key] チェックボックスをオンにした場合、16 進数の暗号キーを入力してください。キーは、32 文字の 16 進数文字（0 ～ 9、a ～ f）である必要があります。

  [Use 32 hexadecimal character key] チェックボックスをオフにした場合は、英数字の共有秘密情報を入力してください。共有秘密情報は、1 ～ 63 文字で入力できます。有効な文字は、数字、文字、または句読点の任意の組み合わせです。共有秘密は、暗号キーを生成するために使用されます。
- [Enable LAN rather than serial cable failover]:（PIX セキュリティ アプライアンス プラットフォームのみ）LAN フェールオーバーをイネーブルにするには、このチェックボックスをオンにします。フェールオーバー リンクとして専用シリアル ケーブルを使用するには、このチェックボックスをオフにします。
- [LAN Failover]：LAN フェールオーバーを設定するためのフィールドが含まれます。
  - [Interface]：フェールオーバー通信に使用するインターフェイスを指定します。フェールオーバーには専用インターフェイスが必要ですが、ステートフル フェールオーバーとインターフェイスを共有できます。

    このリストには、未設定のインターフェイスまたはサブインターフェイスだけが表示され、LAN フェールオーバー インターフェイスとして選択できます。インターフェイスを LAN フェールオーバー インターフェイスに指定すると、そのインターフェイスは [Configuration] > [Interfaces] ペインでは編集できません。
  - [Active IP]：アクティブ装置のフェールオーバー インターフェイスの IP アドレスを指定します。
  - [Subnet Mask]：プライマリ装置およびセカンダリ装置のフェールオーバー インターフェイスのマスクを指定します。
  - [Logical Name]：フェールオーバー通信に使用するインターフェイスの論理名を指定します。
  - [Standby IP]：セカンダリ装置がプライマリ装置との通信に使用する IP アドレスを指定します。
  - [Preferred Role]：このセキュリティ アプライアンスの優先の役割が、LAN フェールオーバーのプライマリ装置であるか、セカンダリ装置であるかを指定します。
- [State Failover]：ステートフル フェールオーバーの設定のためのフィールドが含まれます。

（注）　ステートフル フェールオーバーは、ASA 5505 プラットフォームでは使用できません。この領域は、ASA 5505 セキュリティ アプライアンスで実行している ASDM には表示されません。

- [Interface]：ステート通信に使用するインターフェイスを指定します。選択できるのは、未設定のインターフェイスまたはサブインターフェイス、LAN フェールオーバー インターフェイス、または [Use Named] オプションです。

（注）　LAN フェールオーバー インターフェイスとステートフル フェールオーバー インターフェイスには、2 つの個別の専用インターフェイスを使用することをお勧めします。

未設定のインターフェイスまたはサブインターフェイスを選択した場合、そのインターフェイスのアクティブ IP、サブネット マスク、スタンバイ IP、および論理名を入力する必要があります。

LAN フェールオーバー インターフェイスを選択した場合は、アクティブ IP、サブネット マスク、論理名、およびスタンバイ IP の値を指定する必要はありません。LAN フェールオーバー インターフェイスに指定されている値が使用されます。

[Use Named] オプションを選択した場合、[Logical Name] フィールドは、名前のついたインターフェイスのドロップダウン リストになります。このリストからインターフェイスを選択します。アクティブ IP、サブネット マスク、スタンバイ IP の値を指定する必要はありません。そのインターフェイスに指定された値が使用されます。[Interfaces] タブで選択したインターフェイスにスタンバイ IP アドレスを指定してください。

（注）　ステートフル フェールオーバーでは、大量のトラフィックが生成されることがあるため、ステートフル フェールオーバーと通常トラフィックの両方のパフォーマンスが、名前付きインターフェイスを使用することで影響を受けることがあります。

- [Active IP]：プライマリ装置のステートフル フェールオーバー インターフェイスの IP アドレスを指定します。[Interface] ドロップダウン リストで LAN フェールオーバー インターフェイスまたは [Use Named] オプションが選択されている場合、このフィールドはグレー表示されます。
- [Subnet Mask]：プライマリ装置およびセカンダリ装置のステートフル フェールオーバー インターフェイスのマスクを指定します。[Interface] ドロップダウン リストで LAN フェールオーバー インターフェイスまたは [Use Named] オプションが選択されている場合、このフィールドはグレー表示されます。
- [Logical Name]：フェールオーバー通信に使用される論理インターフェイスを指定します。[Interface] ドロップダウン リストで [Use Named] オプションを選択した場合、このフィールドには、名前付きインターフェイスのリストが表示されます。[Interface] ドロップダウン リストで LAN フェールオーバー インターフェイスが選択されている場合、このフィールドはグレー表示されます。
- [Standby IP]：セカンダリ装置がプライマリ装置との通信に使用する IP アドレスを指定します。[Interface] ドロップダウン リストで LAN フェールオーバー インターフェイスまたは [Use Named] オプションが選択されている場合、このフィールドはグレー表示されます。
- [Enable HTTP replication]：このチェックボックスをオンにすると、ステートフル フェールオーバーによるアクティブ HTTP セッションからスタンバイ ファイアウォールへのコピーがイネーブルになります。HTTP の複製を許可しない場合、HTTP 接続はフェールオーバーで切断されます。HTTP レプリケーションをディセーブルにすると、ステート リンク上のトラフィックの量が少なくなります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]: [Interfaces]（ルーテッド ファイアウォール モード）

このタブを使用して、セキュリティ アプライアンス上の各インターフェイスのスタンバイ IP アドレスを定義し、インターフェイスのステータスを監視するかどうかを指定します。

一般的なフェールオーバーの設定方法の詳細については、「フェールオーバーについて」を参照してください。

フィールド

- [Interface]：セキュリティ アプライアンスのインターフェイスを一覧表示し、そのアクティブ IP アドレス、スタンバイ IP アドレス、モニタリング ステータスを示します。
  - [Interface Name column]：インターフェイス名を示します。
  - [Active IP column]：このインターフェイスのアクティブ IP アドレスを示します。
  - [Standby IP Address]：スタンバイ フェールオーバー装置上の対応するインターフェイスの IP アドレスを指定します。
  - [Is Monitored column]：このインターフェイスの障害を監視するかどうかを指定します。
- [Edit]：選択したインターフェイスの [Edit Failover Interface Configuration]（ルーテッド ファイアウォール モード）ダイアログボックスを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Edit Failover Interface Configuration]（ルーテッド ファイアウォール モード）

[Edit Failover Interface Configuration] ダイアログボックスは、インターフェイスのスタンバイ IP アドレスを定義し、インターフェイスのステータスをモニタするかどうかを指定する場合に使用します。

フィールド

- [Interface Name]：インターフェイス名を示します。
- [Active IP Address]：このインターフェイスの IP アドレスを示します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Subnet Mask]：このインターフェイスのマスクを示します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Standby IP Address]：スタンバイ フェールオーバー装置上の対応するインターフェイスの IP アドレスを指定します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Monitor interface for failure]：このインターフェイスの障害を監視するかどうかを指定します。セキュリティ アプライアンスのモニタ可能なインターフェイスの数は 250 です。モニタ対象のフェールオーバー インターフェイスには、次のステータスが設定されます。
  - [Unknown]：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
  - [Normal]：インターフェイスはトラフィックを受信しています。
  - [Testing]：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
  - [Link Down]：インターフェイスは管理上ダウンしています。
  - [No Link]：インターフェイスの物理リンクがダウンしています。
  - [Failed]：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]: [Interfaces]（トランスペアレント ファイアウォール モード）

このタブを使用してスタンバイ管理 IP アドレスを定義し、セキュリティ アプライアンス上のインターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface]：セキュリティ アプライアンスのインターフェイスを一覧表示し、そのモニタリング ステータスを示します。
  - [Interface Name column]：インターフェイス名を示します。
  - [Is Monitored column]：このインターフェイスの障害を監視するかどうかを指定します。
- [Edit]：選択したインターフェイスの [Edit Failover Interface Configuration]（トランスペアレント ファイアウォール モード）ダイアログボックスを表示します。
- [Management IP Address]：セキュリティ アプライアンスまたはトランスペアレント ファイアウォール モードのコンテキストのアクティブおよびスタンバイ管理 IP アドレスを示します。
  - [Active]：アクティブ管理 IP アドレスを示します。
  - [Standby]：スタンバイ フェールオーバー装置の管理 IP アドレスを指定します。
- [Management Netmask]：アクティブおよびスタンバイ管理 IP アドレスに関連付けられたマスクを示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Edit Failover Interface Configuration]（トランスペアレント ファイアウォール モード）

[Edit Failover Interface Configuration] ダイアログボックスを使用して、インターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface Name]：インターフェイス名を示します。
- [Monitor interface for failure]：このインターフェイスの障害を監視するかどうかを指定します。セキュリティ アプライアンスのモニタ可能なインターフェイスの数は 250 です。インターフェイスのポーリング時間中、セキュリティ アプライアンスのフェールオーバー ペア間で Hello メッセージが交換されます。モニタ対象のフェールオーバー インターフェイスには、次のステータスが設定されます。
  - [Unknown]：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
  - [Normal]：インターフェイスはトラフィックを受信しています。
  - [Testing]：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
  - [Link Down]：インターフェイスは管理上ダウンしています。
  - [No Link]：インターフェイスの物理リンクがダウンしています。

– [Failed] : インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]: [Criteria]

このタブを使用して、障害が発生するときのインターフェイスの数、ポーリング間に待機する時間など、フェールオーバーの基準を定義します。保持時間では、装置がフェールオーバーする前にポーリングへの応答を受信しないまま待機する間隔が指定されます。

フィールド

- [Interface Policy] : モニタリングでインターフェイスの障害が検出されたときのフェールオーバーのポリシーを定義するためのフィールドが含まれます。
  - [Number of failed interfaces that triggers failover] : 障害の発生した監視対象インターフェイスの数がこのコマンドで設定した値を超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。値の範囲は 1 ～ 250 です。
  - [Percentage of failed interfaces that triggers failover] : 障害の発生した監視対象インターフェイスの数がこのコマンドで設定したパーセンテージを超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。
- [Failover Poll Times] : フェールオーバー リンクで Hello メッセージが送信される頻度、およびオプションで、Hello メッセージが受信されない場合にピアの障害をテストする前に待機する時間を定義するためのフィールドが含まれます。
  - [Unit Failover] : 装置間の Hello メッセージの間の時間。範囲は 1 ～ 15 秒または 200 ～ 999 ミリ秒です。
  - [Unit Hold Time] : 装置がフェールオーバー リンク上で Hello メッセージを受信する必要がある時間（それ以外の場合は、装置がピアの障害のテスト プロセスを開始する）を設定します。範囲は 1 ～ 45 秒または 800 ～ 999 ミリ秒です。ポーリング時間の 3 倍より少ない値は入力できません。
  - [Monitored Interfaces] : インターフェイス間でのポーリングの間の時間。範囲は 1 ～ 15 秒または 500 ～ 999 ミリ秒です。
  - [Interface Hold Time] : データ インターフェイスがそのデータ インターフェイス上で Hello メッセージを受信し、その後ピアの障害発生が宣言される時間を設定します。有効な値は 5 ～ 75 秒です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]: [MAC Addresses]

[MAC Addresses] タブでは、Active/Standby フェールオーバー ペアのインターフェイスの仮想 MAC アドレスを設定できます。

（注）　このタブは、ASA 5505 プラットフォームでは使用できません。

アクティブ/スタンバイ フェールオーバーでは、プライマリ装置の MAC アドレスは常にアクティブ IP アドレスに関連付けられています。セカンダリ装置は、最初にブートされてアクティブになると、そのインターフェイスの焼き付け済み MAC アドレスを使用します。プライマリ装置がオンラインになると、セカンダリ装置はプライマリ装置から MAC アドレスを取得します。この変更によって、ネットワーク トラフィックが中断することがあります。

各インターフェイスに仮想 MAC アドレスを設定して、セカンダリ装置がプライマリ装置よりも前にオンラインになっても、セカンダリ装置がアクティブ装置である場合、正しい MAC アドレスを使用するようにします。仮想 MAC アドレスを指定しない場合、フェールオーバー ペアは焼き付け済み NIC アドレスを MAC アドレスとして使用します。

（注）　フェールオーバーまたはステート リンクには、仮想 MAC アドレスは設定できません。これらのリンクの MAC アドレスおよび IP アドレスは、フェールオーバー中に変更されません。

フィールド

- [MAC Addresses]：アクティブおよびスタンバイ仮想 MAC アドレスが設定されているセキュリティ アプライアンス上の物理インターフェイスを一覧表示します。
  - [Physical Interface column]：フェールオーバー仮想 MAC アドレスが設定されている物理インターフェイスを示します。
  - [Active MAC Address column]：アクティブ セキュリティ アプライアンス（通常プライマリ）の MAC アドレスを示します。
  - [Standby MAC Address column]：スタンバイ セキュリティ アプライアンス（通常セカンダリ）の MAC アドレスを示します。
- [Add]：[Add Interface MAC Address] ダイアログボックスを表示します。仮想 MAC アドレスは、LAN フェールオーバーおよびステートフル フェールオーバー インターフェイスには割り当てることができません。詳細については、「Add/Edit Interface MAC Address」を参照してください。

- [Edit]：選択したインターフェイスに対して [Edit Interface MAC Address] ダイアログボックスを表示します。詳細については、「Add/Edit Interface MAC Address」を参照してください。
- [Delete]：現在選択されているインターフェイスを MAC アドレス テーブルから削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Add/Edit Interface MAC Address

[Add/Edit Interface MAC Address] ダイアログボックスを使用して、インターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを定義します。

フィールド

- [Physical Interface]：フェールオーバー仮想 MAC アドレスを定義する物理インターフェイスを指定します。フェールオーバー中は、LAN フェールオーバーおよびステートフル フェールオーバー インターフェイスに対して MAC アドレスは変更されないので、これらのインターフェイスは選択できません。
- [MAC Addresses]：インターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを指定するためのフィールドが含まれます。
  - [Active Interface]：アクティブ セキュリティ アプライアンス（通常プライマリ）上のインターフェイスの MAC アドレスを指定します。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。
  - [Standby Interface]：スタンバイ セキュリティ アプライアンス（通常セカンダリ）上のインターフェイスの MAC アドレスを指定します。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]（マルチ モード、セキュリティ コンテキスト）

マルチ コンテキスト モードの [Failover] ペインに表示されるフィールドは、コンテキストがトランスペアレント ファイアウォール モードであるか、ルーテッド ファイアウォール モードであるかによって変わります。

ここでは、次の内容について説明します。

- [Failover] : [Routed]
- [Failover] : [Transparent]

[Failover] : [Routed]

このペインを使用して、セキュリティ コンテキストの各インターフェイスのスタンバイ IP アドレスを定義し、インターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface table] : セキュリティ アプライアンスのインターフェイスを一覧表示し、そのアクティブ IP アドレス、スタンバイ IP アドレス、モニタリング ステータスを示します。
  - [Interface Name column] : インターフェイス名を示します。
  - [Active IP column] : このインターフェイスのアクティブ IP アドレスを示します。
  - [Standby IP Address] : スタンバイ フェールオーバー装置上の対応するインターフェイスの IP アドレスを指定します。
  - [Is Monitored column] : このインターフェイスの障害を監視するかどうかを指定します。
- [Edit] : 選択したインターフェイスの [Edit Failover Interface Configuration] ダイアログボックスを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	—	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Edit Failover Interface Configuration

[Edit Failover Interface Configuration] ダイアログボックスを使用して、インターフェイスのスタンバイ IP アドレスを定義し、インターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface Name]：インターフェイス名を示します。
- [Active IP Address]：このインターフェイスの IP アドレスを示します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Subnet Mask]：このインターフェイスのマスクを示します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Standby IP Address]：スタンバイ フェールオーバー装置上の対応するインターフェイスの IP アドレスを指定します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Monitor interface for failure]：このインターフェイスの障害を監視するかどうかを指定します。セキュリティ アプライアンスのモニタ可能なインターフェイスの数は 250 です。インターフェイスのポーリング時間中、セキュリティ アプライアンスのフェールオーバー ペア間で Hello メッセージが交換されます。モニタ対象のフェールオーバー インターフェイスには、次のステータスが設定されます。
  - [Unknown]：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
  - [Normal]：インターフェイスはトラフィックを受信しています。
  - [Testing]：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
  - [Link Down]：インターフェイスは管理上ダウンしています。
  - [No Link]：インターフェイスの物理リンクがダウンしています。
  - [Failed]：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	—	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]：[Transparent]

このペインを使用して、セキュリティ コンテキストの管理インターフェイスのスタンバイ IP アドレスを定義し、セキュリティ コンテキストのインターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface]：セキュリティ コンテキストのインターフェイスを一覧表示し、そのモニタリング ステータスを示します。
  - [Interface Name]：インターフェイス名を示します。

  - [Is Monitored]：このインターフェイスの障害を監視するかどうかを指定します。
- [Edit]：選択したインターフェイスの [Edit Failover Interface Configuration] ダイアログボックスを表示します。
- [Management IP Address]：セキュリティ コンテキストのアクティブおよびスタンバイ管理 IP アドレスを示します。
  - [Active]：アクティブ フェールオーバー装置の管理 IP アドレスを示します。
  - [Standby]：スタンバイ フェールオーバー装置の管理 IP アドレスを指定します。
- [Management Netmask]：管理アドレスに関連付けられたマスクを示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	—	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Edit Failover Interface Configuration

[Edit Failover Interface Configuration] ダイアログボックスを使用して、インターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface Name]：インターフェイス名を示します。
- [Monitor interface for failure]：このインターフェイスの障害を監視するかどうかを指定します。セキュリティ アプライアンスのモニタ可能なインターフェイスの数は 250 です。インターフェイスのポーリング時間中、セキュリティ アプライアンスのフェールオーバー ペア間で Hello メッセージが交換されます。モニタ対象のフェールオーバー インターフェイスには、次のステータスが設定されます。
  - [Unknown]：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
  - [Normal]：インターフェイスはトラフィックを受信しています。
  - [Testing]：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
  - [Link Down]：インターフェイスは管理上ダウンしています。
  - [No Link]：インターフェイスの物理リンクがダウンしています。
  - [Failed]：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	—	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]（マルチ モード、システム）

このペインには、マルチ コンテキスト モードのセキュリティ アプライアンスの、システム コンテキストでのシステムレベル フェールオーバー設定を行うためのタブが含まれます。マルチ モードでは、Active/Standby フェールオーバーまたは Active/Active フェールオーバーを設定できます。アクティブ/アクティブ フェールオーバーは、デバイス マネージャでフェールオーバー グループを作成するときに、自動的にイネーブルになります。どちらのタイプのフェールオーバーの場合も、システム コンテキストでのシステムレベル フェールオーバー設定、および個々のセキュリティ コンテキストでのコンテキストレベル フェールオーバー設定を入力する必要があります。一般的なフェールオーバーの設定方法の詳細については、「フェールオーバーについて」を参照してください。

詳細については、次の項目も参照してください。

- [Failover] > [Setup] タブ
- [Failover] > [Criteria] タブ
- [Failover] > [Active/Active] タブ
- [Failover] > [MAC Addresses] タブ

[Failover] > [Setup] タブ

このタブを使用して、マルチ コンテキスト モードのセキュリティ アプライアンスでフェールオーバーをイネーブルにします。また、ステートフル フェールオーバーを使用している場合、このタブではフェールオーバー リンクおよびステート リンクも指定できます。

フィールド

- [Enable Failover]：このチェックボックスをオンにすると、フェールオーバーがイネーブルになり、スタンバイ セキュリティ アプライアンスを設定できます。

（注） インターフェイスの速度と二重通信の設定は、フェールオーバーがイネーブルになっても変更されません。フェールオーバー インターフェイスの速度や二重通信の設定を変更するには、フェールオーバーをイネーブルにする前に、[Configuration] > [Interfaces] ペインで設定しておく必要があります。

- [Use 32 hexadecimal character key]：[Shared Key] フィールドに 16 進数値の暗号キーを入力するには、このチェックボックスをオンにします。[Shared Key] フィールドに英数字の共有秘密情報を入力する場合は、このチェックボックスをオフにします。

- [Shared Key]：フェールオーバー共有秘密情報またはフェールオーバー ペア間での暗号化および認証済み通信のためのキーを指定します。

  [Use 32 hexadecimal character key] チェックボックスをオンにした場合、16 進数の暗号キーを入力してください。キーは、32 文字の 16 進数文字（0 ～ 9、a ～ f）である必要があります。

  [Use 32 hexadecimal character key] チェックボックスをオフにした場合は、英数字の共有秘密情報を入力してください。共有秘密情報は、1 ～ 63 文字で入力できます。有効な文字は、数字、文字、または句読点の任意の組み合わせです。共有秘密は、暗号キーを生成するために使用されます。

- [Enable LAN rather than serial cable failover]:（PIX セキュリティ アプライアンス プラットフォームのみ）LAN フェールオーバーをイネーブルにするには、このチェックボックスをオンにします。フェールオーバー リンクとして専用シリアル リンクを使用するには、このチェックボックスをオフにします。

- [LAN Failover]：LAN フェールオーバーを設定するためのフィールドが含まれます。
  - [Interface]：フェールオーバー通信に使用するインターフェイスを指定します。フェールオーバーには専用インターフェイスが必要ですが、同じインターフェイスをステートフル フェールオーバーにも使用できます。

    このリストには、コンテキストに割り当てられていない、未設定のインターフェイスまたはサブインターフェイスだけが表示され、LAN フェールオーバー インターフェイスとして選択できます。インターフェイスを LAN フェールオーバー インターフェイスとして設定すると、[Configuration] > [Interfaces] ペインで編集したり、コンテキストに割り当てたりできません。
  - [Active IP]：アクティブ装置のフェールオーバー インターフェイスの IP アドレスを指定します。
  - [Subnet Mask]：アクティブ装置のフェールオーバー インターフェイスのマスクを指定します。
  - [Logical Name]：フェールオーバー インターフェイスの論理名を指定します。
  - [Standby IP]：スタンバイ装置の IP アドレスを指定します。
  - [Preferred Role]：このセキュリティ アプライアンスの優先の役割が、LAN フェールオーバーのプライマリ装置であるか、セカンダリ装置であるかを指定します。

- [State Failover]：ステートフル フェールオーバーの設定のためのフィールドが含まれます。
  - [Interface]：フェールオーバー通信に使用するインターフェイスを指定します。未設定のインターフェイス、サブインターフェイス、または LAN フェールオーバー インターフェイスを選択できます。

    LAN フェールオーバー インターフェイスを選択した場合、インターフェイスには、LAN フェールオーバーおよびステートフル フェールオーバー トラフィックの両方を処理できる十分な容量が必要です。また、アクティブ IP、サブネット マスク、論理名、スタンバイ IP の値は指定する必要はありません。LAN フェールオーバー インターフェイスに指定されている値が使用されます。

  （注）　LAN フェールオーバー インターフェイスとステートフル フェールオーバー インターフェイスには、2 つの個別の専用インターフェイスを使用することをお勧めします。

  - [Active IP]：アクティブ装置のステートフル フェールオーバー インターフェイスの IP アドレスを指定します。
  - [Subnet Mask]：アクティブ装置のステートフル フェールオーバー インターフェイスのマスクを指定します。
  - [Logical Name]：ステートフル フェールオーバー インターフェイスの論理名を指定します。
  - [Standby IP]：スタンバイ装置の IP アドレスを指定します。

– [Enable HTTP replication]：このチェックボックスをオンにすると、ステートフル フェールオーバーによるアクティブ HTTP セッションからスタンバイ ファイアウォールへのコピーがイネーブルになります。HTTP の複製を許可しない場合、HTTP 接続はフェールオーバーで切断されます。HTTP レプリケーションをディセーブルにすると、ステート リンク上のトラフィックの量が少なくなります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover] > [Criteria] タブ

このタブを使用して、障害が発生するときのインターフェイスの数、ポーリング間に待機する時間など、フェールオーバーの基準を定義します。保持時間では、装置がフェールオーバーする前にポーリングへの応答を受信しないまま待機する間隔が指定されます。

（注）　Active/Active フェールオーバーを設定している場合、インターフェイス ポリシーの定義にこのタブを使用しないでください。各フェールオーバー グループのインターフェイス ポリシーを定義するには、[Failover] > [Active/Active] タブを使用します。Active/Active フェールオーバーでは、各フェールオーバー グループに定義されたインターフェイス ポリシー設定がこのタブでの設定を上書きします。Active/Active フェールオーバーをディセーブルにした場合は、このタブの設定が使用されます。

フィールド

- [Interface Policy]：モニタリングでインターフェイスの障害が検出されたときのフェールオーバーのポリシーを定義するためのフィールドが含まれます。
  - [Number of failed interfaces that triggers failover]：障害の発生した監視対象インターフェイスの数がこのコマンドで設定した値を超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。値の範囲は 1 ～ 250 です。
  - [Percentage of failed interfaces that triggers failover]：障害の発生した監視対象インターフェイスの数がこのコマンドで設定したパーセンテージを超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。
- [Failover Poll Times]：フェールオーバー リンクで Hello メッセージが送信される頻度、およびオプションで、Hello メッセージが受信されない場合にピアの障害をテストする前に待機する時間を定義するためのフィールドが含まれます。
  - [Unit Failover]：装置間の Hello メッセージの間の時間。範囲は 1 ～ 15 秒または 200 ～ 999 ミリ秒です。

– [Unit Hold Time]：装置がフェールオーバー リンク上で Hello メッセージを受信する必要がある時間（それ以外の場合は、装置がピアの障害のテスト プロセスを開始する）を設定します。範囲は 1 ～ 45 秒または 800 ～ 999 ミリ秒です。ポーリング時間の 3 倍より少ない値は入力できません。

– [Monitored Interfaces]：インターフェイス間でのポーリングの間の時間。範囲は 1 ～ 15 秒または 500 ～ 999 ミリ秒です。

– [Interface Hold Time]：データ インターフェイスがそのデータ インターフェイス上で Hello メッセージを受信し、その後ピアの障害発生が宣言される時間を設定します。有効な値は 5 ～ 75 秒です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover] > [Active/Active] タブ

このタブを使用して、フェールオーバー グループを定義し、セキュリティ アプライアンスで Active/Active フェールオーバーをイネーブルにします。Active/Active フェールオーバー コンフィギュレーションでは、両方のセキュリティ アプライアンスがネットワーク トラフィックを渡すことができます。Active/Active フェールオーバーは、マルチ モードのセキュリティ アプライアンスでだけ使用できます。

フェールオーバー グループは、1 つのセキュリティ コンテキストの論理グループにすぎません。セキュリティ アプライアンスには、2 つのフェールオーバー グループを作成できます。フェールオーバー ペアのアクティブ装置にフェールオーバー グループを作成する必要があります。管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバです。

（注）　アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。

フィールド

- [Failover Groups]：現在セキュリティ アプライアンスに定義されているフェールオーバー グループを一覧表示します。
  – [Group Number]：フェールオーバー グループ番号を指定します。この番号は、コンテキストをフェールオーバー グループに割り当てるときに使用されます。
  – [Preferred Role]：同時に起動したり、preempt オプションが指定されたりしたときに、フェールオーバー グループがアクティブ状態として表示される、フェールオーバー ペアのプライマリ装置またはセカンダリ装置を指定します。ペアの一方の装置にアクティブ状態の両方の

フェールオーバー グループを含めて、もう一方の装置にスタンバイ状態のフェールオーバー グループを含めることができます。ただし、一般的な設定では、各フェールオーバー グループに別々のロール プリファレンスを割り当てて、それぞれを別の装置上でアクティブにすることでデバイスにトラフィックを分散させます。

  - [Preempt Enabled]：このフェールオーバー グループの優先フェールオーバー デバイスである装置がリブート後にアクティブ装置になるかどうかを指定します。
  - [Preempt Delay]：優先フェールオーバー デバイスが、このフェールオーバー グループのアクティブ装置として引き継ぐ前に、リブート後に待機する秒数を指定します。値の範囲は 0 ～ 1200 秒です。
  - [Interface Policy]：グループがフェールオーバーする前に許可される監視対象インターフェイス障害の数または障害のパーセンテージのいずれかを指定します。範囲は 1 ～ 250 回の障害、または 1 ～ 100% です。
  - [Interface Poll Time]：インターフェイス間のポーリング間隔の時間を指定します。1 ～ 15 秒の範囲で指定できます。
  - [Replicate HTTP]：ステートフル フェールオーバーがアクティブ HTTP セッションをこのフェールオーバー グループのスタンバイ ファイアウォールにコピーするかどうかを示します。HTTP の複製を許可しない場合、HTTP 接続はフェールオーバーで切断されます。HTTP レプリケーションをディセーブルにすると、ステート リンク上のトラフィックの量が少なくなります。この設定は、[Setup] タブの HTTP レプリケーションの設定を上書きします。

- [Add]：[Add Failover Group] ダイアログボックスを表示します。存在するフェールオーバー グループが 2 つに満たない場合にだけ、このボタンがイネーブルになります。詳細については、「Add/Edit Failover Group」を参照してください。
- [Edit]：選択したフェールオーバー グループに対して [Edit Failover Group] ダイアログボックスを表示します。詳細については、「Add/Edit Failover Group」を参照してください。
- [Delete]：現在選択されているフェールオーバー グループをフェールオーバー グループ テーブルから削除します。このボタンは、リストの最終フェールオーバー グループが選択されている場合にだけイネーブルになります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Add/Edit Failover Group

[Add/Edit Failover Group] ダイアログボックスを使用して、Active/Active フェールオーバー コンフィギュレーションにフェールオーバー グループを定義します。

フィールド

- [Preferred Role]：フェールオーバー グループがアクティブ状態として表示される、フェールオーバー ペアのプライマリ装置またはセカンダリ装置を指定します。ペアの一方の装置にアクティブ状態の両方のフェールオーバー グループを含めて、もう一方の装置にスタンバイ状態のフェールオーバー グループを含めることができます。ただし、一般的な設定では、各フェールオーバー グループに別々のロール プリファレンスを割り当てて、それぞれを別の装置上でアクティブにすることでデバイスにトラフィックを分散させます。
- [Preempt after booting with optional delay of]：このチェックボックスをオンにすると、フェールオーバー グループの優先フェールオーバー デバイスである装置が、リブート後にアクティブ装置になります。また、このチェックボックスをオンにすると、デバイスがアクティブ装置になる前に待機しなければならない時間を指定できる [Preempt after booting with optional delay of] フィールドとともに、リブート後に Preempt もイネーブルになります。
- [Preempt after booting with optional delay of]：優先フェールオーバー デバイスである装置が、いずれかのフェールオーバー グループのアクティブ装置として引き継ぐ前に、リブート後に待機する秒数を指定します。値の範囲は 0 ～ 1200 秒です。
- [Interface Policy]：モニタリングでインターフェイスの障害が検出されたときのフェールオーバーのポリシーを定義するためのフィールドが含まれます。これらの設定は、[Criteria] タブのインターフェイス ポリシー設定を上書きします。
  - [Number of failed interfaces that triggers failover]：障害の発生した監視対象インターフェイスの数がこのコマンドで設定した値を超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。値の範囲は 1 ～ 250 です。
  - [Percentage of failed interfaces that triggers failover]：障害の発生した監視対象インターフェイスの数がこのコマンドで設定したパーセンテージを超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。
- [Poll time interval for monitored interfaces]：インターフェイス間でのポーリングの間の時間。1 ～ 15 秒の範囲で指定できます。
- [Enable HTTP replication]：このチェックボックスをオンにすると、ステートフル フェールオーバーによるアクティブ HTTP セッションからスタンバイ ファイアウォールへのコピーがイネーブルになります。HTTP の複製を許可しない場合、HTTP 接続はフェールオーバーで切断されます。HTTP レプリケーションをディセーブルにすると、ステート リンク上のトラフィックの量が少なくなります。この設定は、[Setup] タブの HTTP レプリケーションの設定を上書きします。
- [MAC Addresses]：アクティブおよびスタンバイ仮想 MAC アドレスが設定されているセキュリティ アプライアンス上の物理インターフェイスを一覧表示します。
  - [Physical Interface]：フェールオーバー仮想 MAC アドレスが設定されている物理インターフェイスを示します。
  - [Active MAC Address]：フェールオーバー グループがアクティブになっている装置上のインターフェイスおよびフェールオーバー グループの MAC アドレスを表示します。
  - [Standby MAC Address]：フェールオーバー グループがスタンバイ状態になっている装置上のインターフェイスおよびフェールオーバー グループの MAC アドレスを表示します。
- [Add]：[Add Interface MAC Address] ダイアログボックスを表示します。仮想 MAC アドレスは、LAN フェールオーバーおよびステートフル フェールオーバー インターフェイスには割り当てることができません。詳細については、「Add/Edit Interface MAC Address」を参照してください。
- [Edit]：選択したインターフェイスに対して [Edit Interface MAC Address] ダイアログボックスを表示します。詳細については、「Add/Edit Interface MAC Address」を参照してください。
- [Delete]：現在選択されているインターフェイスを MAC アドレス テーブルから削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Add/Edit Interface MAC Address

[Add/Edit Interface MAC Address] ダイアログボックスを使用して、フェールオーバー グループのインターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを定義します。インターフェイスに仮想 MAC アドレスを指定しない場合、次のようにデフォルトの仮想 MAC アドレスが指定されます。

- アクティブ ユニットのデフォルトの MAC アドレス：00a0.c9*physical_port_number.failover_group_id*01
- スタンバイ装置のデフォルト MAC アドレス：00a0.c9:*physical_port_number.failover_group_id*02

（注） 同じネットワーク上にアクティブ/アクティブ フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上で MAC アドレスが重複することを回避するには、必ず各物理インターフェイスに仮想のアクティブおよびスタンバイ MAC アドレスを割り当てます。

これらの MAC アドレスは、インターフェイスの物理 MAC アドレスを上書きします。

フィールド

- [Physical Interface]：フェールオーバー仮想 MAC アドレスを定義する物理インターフェイスを指定します。フェールオーバー中は、LAN フェールオーバーおよびステートフル フェールオーバー インターフェイスに対して MAC アドレスは変更されないので、これらのインターフェイスは選択できません。
- [MAC Addresses]：インターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを指定するためのフィールドが含まれます。
  - [Active Interface]：フェールオーバー グループがアクティブになっている装置上のインターフェイスおよびフェールオーバー グループの MAC アドレスを指定します。各インターフェイスには、MAC アドレスを 2 つまで指定できます。それぞれ各フェールオーバー グループのための MAC アドレスで、物理 MAC アドレスを上書きします。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。
  - [Standby Interface]：フェールオーバー グループがスタンバイ状態になっている装置上のインターフェイスおよびフェールオーバー グループの MAC アドレスを指定します。各インターフェイスには、MAC アドレスを 2 つまで指定できます。それぞれ各フェールオーバー グループのための MAC アドレスで、物理 MAC アドレスを上書きします。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover] > [MAC Addresses] タブ

[MAC Addresses] タブでは、Active/Standby フェールオーバー ペアのインターフェイスの仮想 MAC アドレスを設定できます。

アクティブ/スタンバイ フェールオーバーでは、プライマリ装置の MAC アドレスは常にアクティブ IP アドレスに関連付けられています。セカンダリ装置は、最初にブートされてアクティブになると、そのインターフェイスの焼き付け済み MAC アドレスを使用します。プライマリ装置がオンラインになると、セカンダリ装置はプライマリ装置から MAC アドレスを取得します。この変更によって、ネットワーク トラフィックが中断することがあります。

各インターフェイスに仮想 MAC アドレスを設定して、セカンダリ装置がプライマリ装置よりも前にオンラインになっても、セカンダリ装置がアクティブ装置である場合、正しい MAC アドレスを使用するようにします。仮想 MAC アドレスを指定しない場合、フェールオーバー ペアは焼き付け済み NIC アドレスを MAC アドレスとして使用します。

（注）　フェールオーバーまたはステート リンクには、仮想 MAC アドレスは設定できません。これらのリンクの MAC アドレスおよび IP アドレスは、フェールオーバー中に変更されません。

Active/Active フェールオーバーでは、このタブで設定された MAC アドレスは無効になります。代わりに、フェールオーバー グループで定義された MAC アドレスが使用されます。

フィールド

- [MAC Addresses]：アクティブおよびスタンバイ仮想 MAC アドレスが設定されているセキュリティ アプライアンス上の物理インターフェイスを一覧表示します。
  - [Physical Interface]：フェールオーバー仮想 MAC アドレスが設定されている物理インターフェイスを示します。
  - [Active MAC Address]：アクティブ セキュリティ アプライアンス（通常プライマリ）の MAC アドレスを示します。
  - [Stanby MAC Address]：スタンバイ セキュリティ アプライアンス（通常セカンダリ）の MAC アドレスを示します。
- [Add]：[Add/Edit Interface MAC Address] ダイアログボックスを表示します。
- [Edit]：選択したインターフェイスの [Add/Edit Interface MAC Address] ダイアログボックスを表示します。

- [Delete]：現在選択されているインターフェイスを MAC アドレス テーブルから削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Add/Edit Interface MAC Address

[Add/Edit Interface MAC Address] ダイアログボックスを使用して、インターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを定義します。

フィールド

- [Physical Interface]：フェールオーバー仮想 MAC アドレスを定義する物理インターフェイスを指定します。フェールオーバー中は、LAN フェールオーバーおよびステートフル フェールオーバー インターフェイスに対して MAC アドレスは変更されないので、これらのインターフェイスは選択できません。
- [MAC Addresses]：インターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを指定するためのフィールドが含まれます。
  - [Active Interface]：アクティブ セキュリティ アプライアンス（通常プライマリ）上のインターフェイスの MAC アドレスを指定します。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。
  - [Standby Interface]：スタンバイ セキュリティ アプライアンス（通常セカンダリ）上のインターフェイスの MAC アドレスを指定します。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

CHAPTER 15

ロギングの設定

ロギング機能では、ロギングをイネーブルにしてログ情報の処理方法を指定できます。ログ表示機能では、システム ログ メッセージをリアルタイムで表示できます。ログ表示機能の詳細については、第 41 章「ロギングのモニタリング」を参照してください。

ロギングについて

セキュリティ アプライアンスでは、システム ログ メッセージの監査証跡を生成できます。この監査証跡は、実行されたアクティビティ（許可または拒否されたネットワーク トラフィックのタイプなど）の内容を記録するためのもので、システム ロギングの設定に使用できます。

すべてのシステム ログ メッセージにデフォルトの重大度があります。必要に応じて、メッセージを新しい重大度に再割り当てすることができます。重大度を選択すると、そのレベルおよびより低いレベルのロギング メッセージが生成されます。より高いレベルのメッセージは生成されません。重大度が高くなるほど、生成されるメッセージが増えます。ロギングおよびシステム ログ メッセージの詳細については、『*Cisco Security Appliance System Log Messages Guide*』を参照してください。

ロギングのセキュリティ コンテキスト

それぞれのセキュリティ コンテキストには、独自のロギング コンフィギュレーションが含まれており、独自のメッセージが生成されます。システム コンテキストまたは管理コンテキストにログインし、他のコンテキストに変更した場合、セッションで表示されるメッセージは現在のコンテキストに関連するメッセージだけです。

システム実行スペースで生成されるフェールオーバー メッセージなどのシステム ログ メッセージは、管理コンテキストで生成されるメッセージとともに管理コンテキストで表示できます。システム実行スペースでは、ロギングの設定やロギング情報の表示はできません。

セキュリティ アプライアンスは、それぞれのメッセージとともにコンテキスト名を含めるように設定できます。これによって、単一の syslog サーバに送信されるコンテキスト メッセージを区別できます。この機能は、管理コンテキストから送信されたメッセージとシステムから送信されたメッセージの判別にも役立ちます。これが可能なのは、送信元がシステム実行スペースであるメッセージでは**システム**のデバイス ID が使用され、管理コンテキストが送信元であるメッセージではデバイス ID として管理コンテキストの名前が使用されるからです。デバイス ID の使用方法については、「高度な syslog 設定」（P.15-6）を参照してください。

ロギングの使用方法

セキュリティ コンテキストを定義したら、[Configuration] > [Device Management] > [Logging] を選択します。[Logging] では、次の操作を実行できます。

ステップ 1　[Logging Setup] ペインでは、ロギングをイネーブルにしたり、ロギング パラメータを設定したりできます。詳細については、「ロギングの設定」（P.15-2）を参照してください。

ステップ 2　[Syslog Setup] ペインでは、syslog サーバに送信されるシステム ログ メッセージにファシリティ コードを含めるように設定したり、各メッセージにタイムスタンプを含めるように指定したり、メッセージの重大度レベルを表示または変更したり、メッセージを抑止したりできます。詳細については、「syslog の設定」（P.15-5）を参照してください。

ステップ 3　[E-Mail Setup] ペインでは、通知を目的として電子メールで送信されるシステム ログ メッセージを指定できます。詳細については、「syslog の設定」（P.15-5）を参照してください。

ステップ 4　[Event Lists] ペインでは、記録するメッセージを指定するイベントのカスタム リストを作成できます。ここで作成したリストは、ログ フィルタの設定時に使用されます。詳細については、「イベント リスト」（P.15-9）を参照してください。

ステップ 5　[Logging Filters] ペインでは、各ログの宛先に送信されるメッセージのフィルタリングに使用する基準を指定できます。作成するフィルタの基準としては、重大度レベル、メッセージ クラス、メッセージ ID、またはイベント リストが使用できます。詳細については、「Logging Filters」（P.15-12）を参照してください。

ステップ 6　[Rate Limit] ペインでは、指定した期間内に生成可能なメッセージ数を制限できます。詳細については、「「Rate Limit」（P.15-16）」を参照してください。

ステップ 7　[Syslog Server] ペインでは、セキュリティ アプライアンスから送信されるシステム ログ メッセージの宛先となる syslog サーバを指定できます（複数可）。詳細については、「Syslog サーバ」（P.15-19）を参照してください。

ステップ 8　[SMTP] ペインでは、ASDM から送信される E メール アラートおよび通知メッセージの宛先となる SMTP サーバを指定できます（複数可）。詳細については、「SMTP」（P.15-20）を参照してください。

ロギングの設定

[Logging Setup] ペインでは、セキュリティ アプライアンスに対してシステム ロギングをイネーブルにし、スタンバイ装置でロギングを引き継ぐことが可能かどうか、デバッグ メッセージを送信するかどうか、EMBLEM 形式を使用するかどうかなど、一般的なロギング パラメータを指定できます。また、内部ログ バッファやセキュリティ アプライアンスのロギング キューのデフォルト設定を変更することもできます。このペインにアクセスするには、[Configuration] > [Device Management] > [Logging] > [Logging Setup] を選択します。

フィールド

- [Enable logging]：メイン セキュリティ アプライアンスのロギングをオンにします。
- [Enable logging on the failover standby unit]：スタンバイ セキュリティ アプライアンスに対するロギングをオンにします（可能な場合）。
- [Send debug messages as syslogs]：すべてのデバッグ トレース出力をシステム ログにリダイレクトします。このオプションがイネーブルになっている場合、システム ログ メッセージはコンソールに表示されません。そのため、デバッグ メッセージを表示するには、コンソールでロギングを

イネーブルにし、デバッグ システム ログ メッセージ番号および重大度レベルの宛先としてコンソールを設定する必要があります。使用するシステム ログ メッセージ番号は **711001** です。このシステム ログ メッセージに対するデフォルトの重大度レベルは debug です。

- [Send syslogs in EMBLEM format]：EMBLEM 形式をイネーブルにします。これにより、syslog サーバを除くログの宛先すべてに対して EMBLEM 形式が使用されます。
- [Buffer Size]：ロギング バッファがイネーブルの場合にシステム ログ メッセージが保存される内部ログ バッファのサイズを指定します。バッファの空き容量がなくなると、FTP サーバまたは内部フラッシュ メモリにログを保存していない限り、メッセージは上書きされます。デフォルトのバッファ サイズは 4096 バイトです。有効な範囲は 4096 ～ 1048576 です。
- [Save Buffer To FTP Server]：バッファ内のデータが上書きされる前に、それらを FTP サーバに保存する場合は、このチェックボックスをオンにします。バッファ内のデータが上書きされるようにする場合は、このチェックボックスをオフにします。
- [Configure FTP Settings]：FTP サーバを指定し、バッファ内のデータを保存する際に使用する FTP パラメータを設定する場合にクリックします。
- [Save Buffer To Flash]：バッファ内のデータが上書きされる前に、それらを内部フラッシュ メモリに保存する場合は、このチェックボックスをオンにします。

（注） このオプションは、ルーテッドまたはトランスペアレント シングル モードだけで使用できます。

- [Configure Flash Usage]：ロギングに使用する内部フラッシュ メモリの最大容量、および最低限維持すべき空き容量を KB 単位で指定する場合にクリックします。このオプションをイネーブルにすると、メッセージが格納されるデバイス ディスク上に、「syslog」という名前のディレクトリが作成されます。

（注） このオプションは、ルーテッドまたはトランスペアレント シングル モードだけで使用できます。

- [Queue Size]：セキュリティ アプライアンスに表示するシステム ログのキュー サイズを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

- 「FTP の設定」（P.15-4）を参照してください。
- 「ロギングに使用するフラッシュ メモリの設定」（P.15-4）を参照してください。

FTP の設定

[Configure FTP Settings] ダイアログボックスでは、ログ バッファ内のデータを保存する際に使用する FTP サーバのコンフィギュレーションを指定できます。

フィールド

- [Enable FTP client] : FTP クライアントのコンフィギュレーションをイネーブルにします。
- [Server IP Address] : FTP サーバの IP アドレスを指定します。
- [Path] : 保存済みログ バッファ データの格納先となる FTP サーバ上のディレクトリ パスを指定します。
- [Username] : FTP サーバにログインするためのユーザ名を指定します。
- [Password] : FTP サーバへログインするためのユーザ名に関連付けられたパスワードを指定します。
- [Confirm Password] : 確認のためにパスワードを再入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ロギングに使用するフラッシュ メモリの設定

[Configure Logging Flash Usage] ダイアログボックスでは、ログ バッファ内のデータを内部フラッシュ メモリに保存する際の制限事項を指定できます。

フィールド

- [Maximum Flash to Be Used by Logging] : ロギングに使用できる内部フラッシュ メモリの最大容量を、KB 単位で指定します。
- [Minimum Free Space to Be Preserved] : 最低限維持すべき内部フラッシュ メモリの空き容量を、KB 単位で指定します。内部フラッシュ メモリがこの制限値に近づくと、新しいログが保存されなくなります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

syslog の設定

[Syslog Setup] ペインでは、syslog サーバを宛先とするメッセージにファシリティ コードを含めるように設定できるほか、システム ログ メッセージにタイムスタンプを含めるかどうかを指定できます。このペインでは、メッセージの重大度レベルを変更したり、ログに記録しないメッセージを抑止したりすることもできます。このペインにアクセスするには、[Configuration] > [Device Management] > [Logging] > [Syslog Setup] を選択します。

フィールド

- [Facility code to include in syslogs]：syslog サーバでメッセージを保存する際の基準として使用するシステム ログ ファシリティを選択します。デフォルトは LOCAL(4)20 です。これは、ほとんどの UNIX システムで必要となるコードです。ただし、ネットワーク デバイス間では 8 つのファシリティが共用されているため、システム ログではこの値を変更しなければならない場合があります。
- [Include timestamp in syslogs]：送信される各システム ログ メッセージに日時を含めます。
- [Syslog ID Setup]：[Syslog ID] テーブルに表示される情報を選択します。オプションは次のように定義されています。
  - [Show all syslog IDs]：すべての syslog メッセージ ID が [Syslog ID] テーブルに表示されるよう指定します。
  - [Show suppressed syslog IDs]：明示的に抑止されたシステム ログ メッセージ ID のみが [Syslog ID] テーブルに表示されるよう指定します。
  - [Show syslog IDs with changed logging]：重大度がデフォルト値から変更されたシステム ログ メッセージ ID のみが [Syslog ID] テーブルに表示されるよう指定します。
  - [Show syslog IDs that are suppressed or with a changed logging level]：重大度レベルが変更されたシステム ログ メッセージ ID と、明示的に抑止されたシステム ログ メッセージ ID のみが [Syslog ID] テーブルに表示されるよう指定します。
- [Syslog ID Table]：[Syslog ID Table View] にある設定に基づいてシステム ログ メッセージのリストを表示します。変更する個々のメッセージ ID またはメッセージ ID の範囲を選択します。選択したメッセージ ID は、抑止することも、その重大度レベルを変更することもできます。リストから複数のメッセージ ID を選択する場合は、その範囲の先頭にあたる ID を選択し、Shift キーを押しながらその範囲の最後にあたる ID をクリックします。
- [Advanced]：システム ログ メッセージにデバイス ID を含めるように設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

- 「syslog ID 設定の編集」（P.15-6）を参照してください。
- 「高度な syslog 設定」（P.15-6）を参照してください。

syslog ID 設定の編集

[Edit Syslog ID Settings] ダイアログボックスでは、選択したシステム ログ メッセージの重大度レベルを変更できるほか、選択したシステム ログ メッセージを抑止することもできます。

フィールド

- [Syslog ID(s)]：*表示専用*。この領域に表示される値は、[Syslog Setup] ペインにある [Syslog ID] テーブルで選択されたエントリにより決まります。
- [Suppress Message(s)]：[Syslog ID(s)] リストに表示されるシステム ログ メッセージ ID のメッセージを抑止するには、このチェックボックスをオンにします。
- [Logging Level]：[Syslog ID(s)] リストに表示されるシステム ログ メッセージ ID に送信されるメッセージの重大度レベルを選択します。重大度レベルは次のように定義されています。
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

高度な syslog 設定

セキュリティ アプライアンスが非 EMBLEM 形式のシステム ログ メッセージにデバイス ID を含めるように設定できます。システム ログ メッセージには、1 つのタイプのデバイス ID だけを指定できます。デバイス ID としては、適応型セキュリティ アプライアンスのホスト名、インターフェイス IP アドレス、コンテキスト、またはテキスト文字列を使用できます。

[Advanced Syslog Configuration] ダイアログボックスでは、システム ログ メッセージにデバイス ID を含めるかどうかを指定できます。この機能をイネーブルにすると、非 EMBLEM 形式のシステム ログ メッセージすべてに、デバイス ID が追加されます。

フィールド

- [Enable Syslog Device ID]：デバイス ID をすべての非 EMBLEM 形式のシステム ログ メッセージに含めるように指定します。
- [Hostname]：デバイス ID としてホスト名を使用するように指定します。

- [IP Address]：デバイス ID としてインターフェイスの IP アドレスを使用するように指定します。
  - [Interface Name]：指定した IP アドレスに対応するインターフェイス名を指定します。
- [String]：デバイス ID としてユーザ定義の文字列を使用するように指定します。
  - [User-defined ID]：英数字のユーザ定義文字列を指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

E メールの設定

[E-Mail Setup] ペインでは、送信元の電子メール アドレスを設定できるほか、通知用の電子メール メッセージとして送信される指定済みシステム ログ メッセージの受信者リストを設定することもできます。宛先電子メール アドレスに送信されるシステム ログ メッセージは、重大度レベルでフィルタリングできます。テーブルには、どのエントリの作成が完了しているかが表示されます。このペインにアクセスするには、[Configuration] > [Device Management] > [Logging] > [E-Mail Setup] を選択します。

宛先の電子メール アドレスのメッセージ フィルタリングに使用されるシステム ログ メッセージの重大度レベルは、[Logging Filters] ペインですべての電子メール受信者に対して設定されたグローバル フィルタに比べ、ここで選択した方がより高くなっています。

宛先の電子メール アドレスに使用されるシステム ログ メッセージの重大度フィルタにより、指定された重大度レベル以上のメッセージが送信されます。[Logging Filters] ペインで指定されたグローバル フィルタも、各電子メール受信者に適用されます。

フィールド

- [Source E-Mail address]：電子メール メッセージとして送信されるシステム ログ メッセージの送信元アドレスとなる電子メール アドレスを指定します。
- [Destination E-Mail Address]：指定したシステム ログ メッセージの受信者の電子メール アドレスを指定します。
- [Syslog Severity]：この受信者に送信されるシステム ログ メッセージの重大度レベルを指定します。指定した重大度またはそれ以上の重大度を持つメッセージが送信されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

- 「E メール受信者の追加と編集」（P.15-8）を参照してください。
- 「SMTP」（P.15-8）を参照してください。
- 「Logging Filters」（P.15-12）を参照してください。

E メール受信者の追加と編集

[Add/Edit E-Mail Recipient] ダイアログボックスでは、指定した重大度を持つシステム ログ メッセージを電子メール メッセージとして送信する、宛先の電子メール アドレスを設定できます。

宛先電子メール アドレスへのメッセージのフィルタリングに使用する重大度レベルは、ここで選択した重大度レベルと、[Logging Filters] ペインですべての電子メール受信者に対して設定したグローバル フィルタの重大度レベルのうち、上位にある方が使用されます。

フィールド

- [Destination E-Mail Address]：選択したシステム ログ メッセージの受信者の電子メール アドレスを指定します。
- [Syslog Severity]：この受信者に送信されるシステム ログ メッセージの重大度レベルを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SMTP

[SMTP] ペインでは、発生した重要イベントをアラートなどの電子メールで通知する SMTP クライアントをイネーブルまたはディセーブルにできます。SMTP サーバの IP アドレスを追加でき、オプションとしてバックアップ SMTP サーバの IP アドレスも追加できます。ASDM は IP アドレスが有効かどうかを確認しません。このため、アドレスを正確に入力してください。このペインにアクセスするには、[Configuration] > [Properties] > [Logging] > [Email Setup] を選択します。

フィールド

- [Remote SMTP Server]：プライマリ SMTP サーバとセカンダリ SMTP サーバを設定できます。
- [Primary Server IP Address]：SMTP サーバの IP アドレスを指定します。
- [Secondary Server IP Address (Optional)]：セカンダリ SMTP サーバの IP アドレスをオプションで指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

イベント リスト

[Event Lists] ペインでは、イベントのカスタム リストを作成できます。このリストは、特定の宛先に送信するシステム ログ メッセージを選択する際に使用します。ロギングをイネーブルにし、[Logging Setup] ペインを使用してロギング パラメータを設定したら、[Event Lists] ペインでイベントのリストを作成します（複数可）。これらのイベント リストは、[Logging Filters] ペインでイベントのリストごとにロギングの宛先を指定する際に使用します。このペインにアクセスするには、[Configuration] > [Device Management] > [Logging] > [Event Lists] を選択します。

イベント リストの定義には、次の 3 つの基準を使用します。

- メッセージ クラス
- 重大度
- メッセージ ID

メッセージ クラスとは、セキュリティ アプライアンスの機能に関連するシステム ログ メッセージのグループです。メッセージ クラスを使用すると、メッセージごとに個別にクラスを指定するのではなく、複数のメッセージから成るクラス全体を指定できます。たとえば、auth クラスを使用すると、ユーザ認証に関連するすべてのシステム ログ メッセージを選択できます。

重大度レベルは、ネットワークの通常機能におけるイベントの相対的な重要度に基づいて、システム ログ メッセージを分類するためのものです。最も高い重大度レベルは [Emergency] で、リソースが使用不能になっていることを表します。最も低い重大度レベルは [Debugging] で、各ネットワーク イベントに関する詳細情報が通知されます。

メッセージ ID は、各メッセージを一意に識別する数値です。イベント リストのメッセージ ID を使用すれば、ある範囲（101001 ～ 101010 など）に属するシステム ログ メッセージを識別できます。

フィールド

- [Name]：イベント リストの名前を示します。
- [Event Class/Severity]：ロギング メッセージのイベント クラスと重大度を示します。イベント クラスには、次のものが含まれます。
  - [All]：すべてのイベント クラス
  - [auth]：ユーザ認証
  - [bridge]：トランスペアレント ファイアウォール
  - [ca]：PKI 認証局
  - [config]：コマンド インターフェイス
  - [ha]：フェールオーバー
  - [ips]：侵入防御サービス
  - [ip]：IP スタック
  - [np]：ネットワーク プロセッサ

- [ospf]：OSPF ルーティング
- [rip]：RIP ルーティング
- [rm]：リソース マネージャ
- [session]：ユーザ セッション
- [snmp]：SNMP
- [sys]：システム

重大度レベルは次のとおりです。

- Emergency（レベル 0、システムが使用不能）
- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ中のみ表示）

- [Message IDs]：フィルタに含めるシステム ログ メッセージ ID または ID の範囲（101001-101010 など）を一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

- 「イベント リストの追加と編集」（P.15-10）を参照してください。
- 「syslog メッセージ ID フィルタの追加と編集」（P.15-12）を参照してください。
- 「Logging Filters」（P.15-12）を参照してください。

イベント リストの追加と編集

[Add/Edit Event List] ダイアログボックスでは、イベント リストの作成や編集ができます。イベント リストは、ログの宛先に送信するメッセージを指定する場合に使用できます。作成したイベント リストでは、メッセージ クラスと重大度レベル、またはメッセージ ID に基づいてメッセージをフィルタリングできます。

メッセージ クラスは、適応型セキュリティ アプライアンスの機能に関連するシステム ログ メッセージのグループです。イベント リストを作成するとき、各メッセージを個々に指定するのではなく、メッセージのクラス全体を指定できます。たとえば、auth クラスを使用すると、ユーザ認証に関連するすべてのシステム ログ メッセージを選択できます。

重大度レベルは、ネットワークの通常機能におけるイベントの相対的な重要度に基づいて、システム ログ メッセージを定義するためのものです。最も高い重大度レベルは [Emergency] で、リソースが使用不能になっていることを表します。最も低い重大度レベルは [Debugging] で、各ネットワーク イベントに関する詳細情報が通知されます。

メッセージ ID は、各メッセージを一意に識別する数値です。イベント リストのメッセージ ID を使用すれば、ある範囲（101001 ～ 101010 など）に属するシステム ログ メッセージを識別できます。

フィールド

- [Name]：イベント リストの名前を入力します。
- [Event Class]：イベント クラスを一覧表示します。イベント クラスには、次のものが含まれます。
  - [All]：すべてのイベント クラス
  - [auth]：ユーザ認証
  - [bridge]：トランスペアレント ファイアウォール
  - [ca]：PKI 認証局
  - [config]：コマンド インターフェイス
  - [ha]：フェールオーバー
  - [ips]：侵入防御サービス
  - [ip]：IP スタック
  - [np]：ネットワーク プロセッサ
  - [ospf]：OSPF ルーティング
  - [rip]：RIP ルーティング
  - [rm]：リソース マネージャ
  - [session]：ユーザ セッション
  - [snmp]：SNMP
  - [sys]：システム
- [Severity]：ロギング メッセージのレベルを一覧表示します。重大度レベルは次のとおりです。
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）
- [Message IDs Filters]：フィルタに含めるシステム ログ メッセージ ID またはシステム ログ メッセージ ID の範囲（101001-101010 など）を一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

syslog メッセージ ID フィルタの追加と編集

[Add/Edit Syslog Message ID Filter] ダイアログボックスでは、イベント リストに含めるシステム ログ メッセージ ID を指定できます（複数可）。

フィールド

- [Message IDs] : 記録するシステム ログ メッセージ ID または ID の範囲を指定します。範囲を指定するには、ハイフンを使用します（101001-101010 など）。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Logging Filters

[Logging Filters] ペインでは、メッセージ フィルタをログの宛先に適用できます。ログの宛先に適用されたフィルタにより、その宛先に送信するメッセージが選択されます。メッセージ クラスおよび重大度レベルに従ってメッセージをフィルタリングできるほか、[Event Lists] ペインで作成可能なイベント リストを使用することもできます。このペインにアクセスするには、[Configuration] > [Device Management] > [Logging] > [Logging Filters] を選択します。

フィールド

- [Logging Destination] : フィルタを適用できるロギングの宛先の名前を一覧表示します。ロギング先は次のとおりです。
  - コンソール
  - セキュリティ アプライアンス
  - Syslog サーバ
  - SNMP トラップ
  - 電子メール
  - 内部バッファ
  - Telnet セッション

- [Syslogs From All Event Classes]：ログの宛先へのメッセージをフィルタリングする際に使用する重大度やイベント クラスが一覧表示されるほか、すべてのイベント クラスに対してロギングをディセーブルにするかどうかを選択することもできます。
- [Syslogs From Specific Event Classes]：ログの宛先へのメッセージのフィルタリングに使用するイベント クラスを一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

- 「ロギング フィルタの編集」（P.15-13）を参照してください。
- 「syslog メッセージ ID フィルタの追加と編集」（P.15-12）を参照してください。
- 「クラスおよび重大度によるフィルタの追加と編集」（P.15-14）を参照してください。
- 「イベント リスト」（P.15-9）を参照してください。

ロギング フィルタの編集

[Edit Logging Filters] ダイアログボックスでは、ログの各宛先に対するフィルタの適用、すでにログの宛先に適用されているフィルタの編集、ログの宛先に対するフィルタのディセーブル化が可能です。メッセージ クラスおよび重大度レベルに従ってメッセージをフィルタリングできるほか、[Event Lists] ペインで作成可能なイベント リストを使用することもできます。

フィールド

- [Logging Destination]：このフィルタに対してロギングの宛先を指定します。
- [Filter on severity]：重大度レベルに従って、システム ログ メッセージをフィルタリングします。
  - [Filter on severity]：フィルタリングを行うシステム ログ メッセージのレベルを指定します。
- [Use event list]：このフィルタへのイベント リストの使用を指定します。
  - [Use event]：使用するイベント リストを指定します。
- [New]：新しいイベント リストを追加できます。
- [Disable logging from all event classes]：選択した宛先へのすべてのロギングをディセーブルにします。
- [Event Class]：イベント クラスを指定します。イベント クラスには、次のものが含まれます。
  - [All]：すべてのイベント クラス
  - [auth]：ユーザ認証
  - [bridge]：トランスペアレント ファイアウォール
  - [ca]：PKI 認証局

  - [config]：コマンド インターフェイス
  - [ha]：フェールオーバー
  - [ips]：侵入防御サービス
  - [ip]：IP スタック
  - [np]：ネットワーク プロセッサ
  - [ospf]：OSPF ルーティング
  - [rip]：RIP ルーティング
  - [rm]：リソース マネージャ
  - [session]：ユーザ セッション
  - [snmp]：SNMP
  - [sys]：システム
- [Severity]：ロギング メッセージのレベルを指定します。重大度は次のとおりです。
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

クラスおよび重大度によるフィルタの追加と編集

[Add/Edit Class and Severity Filter] ダイアログボックスでは、メッセージのフィルタリングに使用するメッセージ クラスおよび重大度レベルを指定できます。

メッセージ クラスは、適応型セキュリティ アプライアンスの機能に関連するシステム ログ メッセージのグループです。イベント リストを作成するとき、各メッセージを個々に指定するのではなく、メッセージのクラス全体を指定できます。たとえば、auth クラスを使用すると、ユーザ認証に関連するすべてのシステム ログ メッセージを選択できます。

重大度レベルは、ネットワークの通常機能におけるイベントの相対的な重要度に基づいて、システム ログを定義するためのものです。最も高い重大度レベルは [Emergency] で、リソースが使用不能になっていることを表します。最も低い重大度レベルは [Debugging] で、各ネットワーク イベントに関する詳細情報が通知されます。

フィールド

- [Event Class]：イベント クラスを指定します。イベント クラスには、次のものが含まれます。
  - [All]：すべてのイベント クラス
  - [auth]：ユーザ認証
  - [bridge]：トランスペアレント ファイアウォール
  - [ca]：PKI 認証局
  - [config]：コマンド インターフェイス
  - [ha]：フェールオーバー
  - [ips]：侵入防御サービス
  - [ip]：IP スタック
  - [np]：ネットワーク プロセッサ
  - [ospf]：OSPF ルーティング
  - [rip]：RIP ルーティング
  - [rm]：リソース マネージャ
  - [session]：ユーザ セッション
  - [snmp]：SNMP
  - [sys]：システム
- [Severity]：ロギング メッセージのレベルを指定します。重大度は次のとおりです。
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

syslog メッセージ ID フィルタの追加と編集

[Add/Edit Syslog Message ID Filter] ダイアログボックスでは、イベント リスト フィルタに含める個々のシステム ログ メッセージ ID またはシステム ログ メッセージ ID の範囲を指定できます。

フィールド

- [Message IDs]：システム ログ メッセージ ID、または ID の範囲を指定します。範囲を指定するには、ハイフンを使用します（101001-101010 など）。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Rate Limit

[Rate Limit] ペインでは、ファイアウォールから送信できるシステム ログ メッセージの数を指定できます。メッセージ ロギング レベルのレート制限を具体的に指定して、特定のメッセージのレートを制限することができます。レート レベルは、重大度レベルまたはメッセージ ID には適用されますが、宛先には適用されません。そのため、レート制限の程度によっては、設定済みの宛先すべてに送信されるメッセージの量が変更されることになります。このペインにアクセスするには、[Configuration] > [Device Management] > [Logging] > [Rate Limit] を選択します。

フィールド

syslog ロギング レベルのレート制限セクション

- [Logging Level]：メッセージの重大度レベルを一覧表示します。レベルは次のように定義されています。
  - Disabled（ロギングなし）
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）
  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）
- [No of Messages]：送信されるメッセージ数を表示します。メッセージ数を制限なしにする場合は、[Number of Messages] フィールドおよび [Time Interval] フィールドをともにブランクのままにします。

- [Interval (Seconds)]：このロギング レベルで送信できるメッセージ数を制限するのに使用される間隔を、秒数で表示します。メッセージ数を制限なしにする場合は、[Number of Messages] および [Time Interval] をともにブランクのままにします。
- [Edit]：テーブルからロギング レベルを選択し、このボタンをクリックして [Edit Rate Limit] ダイアログボックスを開きます。このダイアログボックスでは、選択したロギング レベルのプロパティを編集できます。

個別にレート制限された syslog メッセージ セクション

- [Syslog ID]：制限されているシステム ログ メッセージの ID を表示します。
- [Logging Level]：メッセージの重大度レベルを表示します。重大度レベルのリストについては、「syslog ロギング レベルのレート制限セクション」（P.15-16）を参照してください。
- [No of Messages]：指定した時間内に送信できるメッセージの最大数を表示します。
- [Interval (Seconds)]：システム ログ メッセージの制限に使用される間隔を秒数で表示します。
- [Add]：特定のメッセージのレートを制限する場合にクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

- 「syslog ロギング レベルに対するレート制限の編集」（P.15-17）を参照してください。
- 「syslog メッセージに対するレート制限の追加と削除」（P.15-18）を参照してください。

syslog ロギング レベルに対するレート制限の編集

[Edit Rate Limit for Syslog Logging Level] ボックスでは、指定した時間間隔にファイアウォールが送信できるメッセージ数を制限します。

フィールド

syslog ロギング レベルのレート制限セクション

- [Logging Level]：選択したメッセージの重大度レベルを表示します。特定のメッセージ ID のレート制限を変更すると、ロギング レベルを指定できる場合があります。レベルは次のように定義されています。
  - Disabled（ロギングなし）
  - Emergency（レベル 0、システムが使用不能）
  - Alert（レベル 1、即時対処が必要）
  - Critical（レベル 2、クリティカル条件）
  - Error（レベル 3、エラー条件）

  - Warning（レベル 4、警告条件）
  - Notification（レベル 5、正常だが顕著な条件）
  - Informational（レベル 6、情報メッセージのみ）
  - Debugging（レベル 7、デバッグ中のみ表示）
- [No of Messages]：このロギング レベルで送信可能なメッセージの最大数を指定します。
- [Time Interval (seconds)]：このロギング レベルでのメッセージのレートを制限するときに使用される時間を、秒数で指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

syslog メッセージに対するレート制限の追加と削除

[Add/Edit Rate Limit for Syslog Message] ダイアログボックスでは、レート制限を特定のシステム ログ メッセージに割り当てることができます。

フィールド

- [Syslog Message ID]：制限するシステム ログ メッセージのメッセージ ID を指定します。
- [Number of Messages]：指定された時間間隔にこのメッセージを送信できる最大回数を指定します。
- [Time Interval]：指定したメッセージの制限に使用される時間を秒数で指定します。

（注） メッセージ数を制限なしにする場合は、[Number of Messages] フィールドおよび [Time Interval] フィールドをともにブランクのままにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Syslog サーバ

[Syslog Servers] ペインでは、セキュリティ アプライアンスから送信されるシステム ログ メッセージの宛先となる syslog サーバを指定できます。指定した syslog サーバを使用するには、[Logging Setup] ペインを使用してロギングをイネーブルにし、[Logging Filters] ペインで使用可能な宛先を設定する必要があります。このペインにアクセスするには、[Configuration] > [Device Management] > [Logging] > [Syslog Server] を選択します。

（注）　セキュリティ コンテキストごとに最大 4 つの syslog サーバを設定できます。

フィールド

- [Interface]：syslog サーバとの通信に使用するインターフェイスを表示します。
- [IP Address]：syslog サーバとの通信に使用されるインターフェイスの IP アドレスを表示します。
- [Protocol/Port]：syslog サーバがセキュリティ アプライアンスとの通信に使用するプロトコルおよびポートを表示します。
- [EMBLEM]：メッセージを Cisco EMBLEM 形式（[Protocol/Port] 設定で UDP が選択されている場合にのみ使用可能）で記録するかどうかを指定します。
- [Queue Size]：syslog サーバがビジー状態の場合、セキュリティ アプライアンスでキューに入れることができるメッセージ数を指定します。値がゼロの場合は、キューに入れられるメッセージ数が無制限になります。
- [Allow user traffic to pass when TCP syslog server is down]：syslog サーバがダウンしている場合に、すべてのトラフィックを制限するかどうかを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

- 「syslog サーバの追加と編集」（P.15-19）を参照してください。
- 「ロギングの設定」（P.15-2）を参照してください。
- 「Logging Filters」（P.15-12）を参照してください。

syslog サーバの追加と編集

[Add/Edit Syslog Server] ダイアログボックスでは、セキュリティ アプライアンスから送信されるシステム ログ メッセージの宛先となる syslog サーバを追加または編集できます。指定した syslog サーバを使用するには、[Logging Setup] ペインでロギングをイネーブルにし、[Logging Filters] ペインで、指定したフィルタをログの宛先に対して設定する必要があります。

（注）　コンテキストごとに最大 4 つの syslog サーバを設定できます。

フィールド

- [Interface]：syslog サーバとの通信に使用するインターフェイスを指定します。
- [IP Address]：syslog サーバとの通信に使用する IP アドレスを指定します。
- [Protocol]：syslog サーバがセキュリティ アプライアンスとの通信に使用するプロトコル（TCP または UDP）を表示します。
- [Port]：syslog サーバがセキュリティ アプライアンスとの通信に使用するポートを指定します。
- [Log messages in Cisco EMBLEM format (UDP only)]：メッセージを Cisco EMBLEM 形式（[Protocol] で UDP が選択されている場合にのみ使用可能）で記録するかどうかを指定します。
- [Enable secure logging using SSL/TLS (TCP only)]：syslog サーバへの接続が SSL/TLS over TCP の使用により保護され、システム ログ メッセージの内容が暗号化されるよう指定します。

（注）　PIX セキュリティ アプライアンスは、セキュア ロギング オプションをサポートしていません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SMTP

[SMTP] ペインでは、特定のイベントが発生したときに送信される電子メール アラートと通知の宛先となるリモート SMTP サーバの IP アドレスを設定できます。このペインにアクセスするには、[Configuration] > [Device Setup] > [Logging] > [SMTP] を選択します。

フィールド

- [Primary Server IP Address]：プライマリ SMTP サーバの IP アドレスを指定します。
- [Secondary Server IP Address (optional)]：スタンバイ SMTP サーバの IP アドレスを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 16

ダイナミック ルーティングおよびスタティック ルーティングの設定

スタティック ルーティング プロトコルとダイナミック ルーティング プロトコルを設定するには、ASDM インターフェイスの [Configuration] > [Device Setup] > [Routing] 領域に移動します。

セキュリティ アプライアンスでは、最大で OSPF ルーティング プロセスを 2 つ、EIGRP ルーティング プロセスを 1 つ、および RIP ルーティング プロセスを 1 つまで同時に設定できます。ダイナミック ルーティングは、ルーテッド ファイアウォール モードのセキュリティ アプライアンスでだけ使用でき、セキュリティ アプライアンスがトランスペアレント ファイアウォール モードのときには設定できません。

スタティック ルートは、ルーテッド ファイアウォール モードまたはトランスペアレント ファイアウォール モードのセキュリティ アプライアンスで設定できます。プライマリ スタティック ルートを使用できなくなった場合は、スタティック ルート トラッキング機能によってセキュリティ アプライアンスにバックアップ スタティック ルートを指定できます。

ここでは、次の内容について説明します。

ダイナミック ルーティング

ここでは、次の内容について説明します。

OSPF

OSPF は、パスの選択に距離ベクトル型ではなくリンク ステートを使用する Interior Gateway Routing Protocol（IGRP）です。OSPF は、ルーティング テーブル アップデートではなく、リンクステート アドバタイズメントを伝搬します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、MD5 とクリア テキスト ネイバー認証をサポートしています。OSPF と他のプロトコル（RIP など）の間のルートの再配布は、攻撃者によるルーティング情報の悪用に使用される可能性があるため、できる限りすべてのルーティング プロトコルで認証を使用する必要があります。

NAT が使用されている場合、OSPF がパブリック エリアおよびプライベート エリアで動作している場合、またアドレス フィルタリングが必要な場合は、2 つの OSPF プロセス（1 つはパブリック エリア用、1 つはプライベート エリア用）を実行する必要があります。

複数のエリアにインターフェイスを持つルータは、Area Border Router（ABR; エリア境界ルータ）と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティング プロトコルを使用しているルータの間でトラフィックを再配布するルータは、Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）と呼ばれます。

ABR は LSA を使用して、使用可能なルータに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用すれば、セキュリティ アプライアンスが ABR として動作するプライベート エリアおよびパブリック エリアを分けることができます。タイプ 3 LSA（エリア間ルート）を 1 つのエリアから他のエリアにフィルタリングできます。このことにより、プライベート ネットワークをアドバタイズしなくても、NAT と OSPF を一緒に使用できます。

（注）　タイプ 3 LSA だけをフィルタリングできます。セキュリティ アプライアンスを ASBR としてプライベート ネットワークで設定している場合、プライベート ネットワークを説明するタイプ 5 LSA が送信され、パブリック エリアを含む AS 全体に対してフラッディングされます。

NAT は使用されているが、OSPF がパブリック エリアでだけ実行されている場合、パブリック ネットワークへのルートは、プライベート ネットワーク内でデフォルトまたはタイプ 5 AS External LSA として再配布できます。ただし、セキュリティ アプライアンスにより保護されているプライベート ネットワークにはスタティック ルートを設定する必要があります。また、同一のセキュリティ アプライアンス インターフェイス上で、パブリック ネットワークとプライベート ネットワークを混在させることはできません。

セキュリティ アプライアンスでは、2 つの OSPF ルーティング プロセス（1 つの RIP ルーティング プロセスと 1 つの EIGRP ルーティング プロセス）を同時に実行できます。

OSPF のイネーブル化および設定の詳細については、次の項目を参照してください。

- 「セットアップ」（P.16-2）
- 「Filtering」（P.16-9）
- 「Interface」（P.16-11）
- 「Redistribution」（P.16-16）
- 「Static Neighbor」（P.16-18）
- 「Summary Address」（P.16-19）
- 「Virtual Link」（P.16-21）

セットアップ

[Setup] ペインでは、OSPF プロセスをイネーブルにし、OSPF エリアおよびネットワークを設定し、OSPF ルート集約を定義できます。

これらのエリアの設定の詳細については、次の項を参照してください。

- 「[Setup] > [Process Instances] タブ」（P.16-3）
- 「[Setup] > [Area/Networks] タブ」（P.16-5）
- 「[Setup] > [Route Summarization] タブ」（P.16-7）

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Setup] > [Process Instances] タブ

最大 2 つの OSPF プロセス インスタンスをイネーブルにできます。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。

フィールド

- [OSPF Process 1] エリアおよび [OSPF Process 2] エリア：各エリアには、特定の OSPF プロセスのための設定が含まれます。
- [Enable this OSPF Process]：このチェックボックスをオンにすると、OSPF プロセスをイネーブルにします。OSPF プロセスを削除するには、このチェックボックスをオフにします。
- [OSPF Process ID]：OSPF プロセスの一意の数値 ID を入力します。このプロセス ID は内部的に使用され、他の OSPF デバイス上の OSPF プロセス ID に一致している必要はありません。有効な値は 1 ～ 65535 です。
- [Advanced]：[Edit OSPF Process Advanced Properties] ダイアログボックスが開きます。このダイアログボックスでは、[Router ID]、[Adjacency Changes]、[Administrative Route Distances]、[Timers]、および [Default Information Originate] の各種設定を実行できます。詳細については、「[Edit OSPF Process Advanced Properties]」（P.16-3）を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Edit OSPF Process Advanced Properties]

[Edit OSPF Process Advanced Properties] ダイアログボックスでは、[Router ID]、[Adjacency Changes]、[Administrative Route Distances]、[Timers]、および [Default Information Originate] 設定など、プロセス固有の設定を編集できます。

フィールド

- [OSPF Process]：設定している OSPF プロセスを表示します。この値は変更できません。

- [Router ID] : 固定ルータ ID を使用するには、[Router ID] フィールドに IP アドレス形式でルータ ID を入力します。この値を空白にすると、セキュリティ アプライアンスで最高レベルの IP アドレスがルータ ID として使用されます。
- [Ignore LSA MOSPF] : セキュリティ アプライアンスがタイプ 6（MOSPF）LSA パケットを受信したときのシステム ログ メッセージの送信を抑制するには、このチェックボックスをオンにします。デフォルトでは、この設定はオフになっています。
- [RFC 1583 Compatible] : RFC 1583 あたりのサマリー ルート コストを計算するには、このチェックボックスをオンにします。RFC 2328 あたりのサマリー ルート コストを計算するには、このチェックボックスをオフにします。ルーティング ループが発生する可能性を最小限にするため、OSPF ルーティング ドメインのすべての OSPF デバイスには、同じように RFC 互換性が設定されている必要があります。この設定は、デフォルトでオンになっています。
- [Adjacency Changes] : 隣接関係の変更を定義する設定が含まれます。隣接関係が変更されると、システム ログ メッセージが送信されます。
  - [Log Adjacency Changes] : OSPF ネイバーが起動またはダウンするたびにセキュリティ アプライアンスがシステム ログ メッセージを送信するようにするには、このチェックボックスをオンにします。この設定は、デフォルトでオンになっています。
  - [Log Adjacency Changes Detail] : ネイバーが起動またはダウンしたときだけでなく、状態の変更が発生するたびにセキュリティ アプライアンスがシステム ログ メッセージを送信するようにするには、このチェックボックスをオンにします。デフォルトでは、この設定はオフになっています。
- [Administrative Route Distances] : ルート タイプに基づくルートのアドミニストレーティブ ディスタンスの設定を含みます。
  - [Inter Area] : 1 つのエリアから別のエリアへのすべてのルートのアドミニストレーティブ ディスタンスを設定します。有効値の範囲は、1 ～ 255 です。デフォルト値は 100 です。
  - [Intra Area] : エリア内のすべてのルートのアドミニストレーティブ ディスタンスを設定します。有効値の範囲は、1 ～ 255 です。デフォルト値は 100 です。
  - [External] : 再配布を通じて取得される他のルーティング ドメインからのすべてのルートのアドミニストレーティブ ディスタンスを設定します。有効値の範囲は、1 ～ 255 です。デフォルト値は 100 です。
- [Timers] : LSA ペーシングおよび SPF 計算タイマーの設定に使用する設定が含まれます。
  - [SPF Delay Time] : OSPF がトポロジの変更を受信してから SPF の計算が開始されるまでの時間を指定します。有効値の範囲は、0 ～ 65535 です。デフォルト値は 5 です。
  - [SPF Hold Time] : 連続する SPF 計算の間の保持時間を指定します。有効値の範囲は 1 ～ 65534 です。デフォルト値は 10 です。
  - [LSA Group Pacing] : LSA がグループに収集され、更新、チェックサム、または時間経過する間隔を指定します。有効値の範囲は 10 ～ 1800 です。デフォルト値は 240 です。
- [Default Information Originate] : ASBR がデフォルトの外部ルートを OSPF ルーティング ドメインに生成するときに使用する設定を含みます。
  - [Enable Default Information Originate] : OSPF ルーティング ドメインへのデフォルト ルートの生成をイネーブルにするには、このチェックボックスをオンにします。
  - [Always advertise the default route] : デフォルト ルートを常にアドバタイズするには、このチェックボックスをオンにします。このオプションは、デフォルトではオフになっています。
  - [Metric Value] : OSPF デフォルト メトリックを指定します。有効値の範囲は 0 ～ 16777214 です。デフォルト値は、1 です

- [Metric Type]：OSPF ルーティング ドメインにアドバタイズされたデフォルト ルートに関連付けられた外部リンク タイプを指定します。有効値は 1 または 2 です。それぞれタイプ 1 またはタイプ 2 外部ルートを示します。デフォルト値は 2 です。
- [Route Map]：（任意）適用するルート マップの名前です。ルート マップが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Setup] > [Area/Networks] タブ

[Area/Networks] タブには、セキュリティ アプライアンスの各 OSPF プロセスのエリア、およびそこに含まれるネットワークが表示されます。

フィールド

- [Area/Networks]：各 OSPF プロセスに対して設定されたエリアおよびエリア ネットワークに関する情報を表示します。このテーブルの行をダブルクリックすると、選択したエリアを対象とした Add/Edit OSPF Area ダイアログボックスが開きます。
  - [OSPF Process]：エリアの適用先である OSPF プロセスを表示します。
  - [Area ID]：エリア ID を表示します。
  - [Area Type]：エリア タイプを表示します。エリア タイプは、[Normal]、[Stub]、[NSSA] のいずれかです。
  - [Networks]：エリア ネットワークを表示します。
  - [Authentication]：そのエリアに設定された認証タイプを表示します。認証タイプは、[None]、[Password]、[MD5] のいずれかです。
  - [Options]：そのエリア タイプに設定されたオプションを表示します。
  - [Cost]：そのエリアのデフォルト コストを表示します。
- [Add]：[Add/Edit OSPF Area] ダイアログボックスが開きます。新しいエリア設定を追加する場合は、このボタンを使用します。
- [Edit]：[Add/Edit OSPF Area] ダイアログボックスが開きます。選択したエリアのパラメータを変更する場合は、このボタンを使用します。
- [Delete]：選択したエリアを設定から削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit OSPF Area

[Add/Edit OSPF Area] ダイアログボックスでは、エリア パラメータ、そのエリアに含まれるネットワーク、およびエリアに関連付けられた OSPF プロセスを定義します。

フィールド

- [OSPF Process]：新しいエリアを追加するときに、そのエリアが追加される OSPF プロセスの OSPF プロセス ID を選択します。セキュリティ アプライアンス上で OSPF プロセスが 1 つしかイネーブルになっていないと、そのプロセスがデフォルトで選択されます。既存のエリアを編集する場合、OSPF プロセス ID を変更することはできません。
- [Area ID]：新しいエリアを追加するときに、エリア ID を入力します。このエリア ID には、10 進数か IP アドレスを指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。既存のエリアを編集する場合、エリア ID は変更できません。
- [Area Type]：設定しているエリアのタイプに対する設定を含みます。
  - [Normal]：エリアを標準 OSPF エリアとする場合に、このオプションを選択します。エリアを最初に作成するときは、このオプションがデフォルトで選択されています。
  - [Stub]：このオプションを選択すると、エリアがスタブ エリアになります。スタブ エリアには、その向こう側にルータまたはエリアはありません。スタブ エリアでは、AS External LSA（タイプ 5 LSA）がスタブ エリアにフラッディングされないようになっています。スタブ エリアを作成するとき、[Summary] チェックボックスをオフにすることでサマリー LSA（タイプ 3 および 4）がそのエリアにフラッディングされないようにするオプションがあります。
  - [Summary]：定義しているエリアがスタブ エリアのときにこのチェックボックスをオフにすると、LSA がスタブ エリアに送信されません。スタブ エリアの場合、このチェックボックスはデフォルトでオンになっています。
  - [NSSA]：エリアを [not so stubby] エリアにするには、このオプションを選択します。NSSA はタイプ 7 LSA を受け入れます。[NSSA] エリアを作成するときに、[Summary] チェックボックスをオフにすることでサマリー LSA がそのエリアにフラッディングされないようにするオプションがあります。また、[Redistribut]e チェックボックスをオフにして [Default Information Originate] をイネーブルにすることで、ルートの再配布をディセーブルにもできます。
  - [Redistribute]：このチェックボックスをオフにすると、ルートは NSSA にインポートされません。このチェックボックスは、デフォルトでオンになっています。
  - [Summary]：定義しているエリアが NSSA のとき、このチェックボックスをオフにすると、LSA がスタブ エリアに送信されません。NSSA の場合、このチェックボックスはデフォルトでオンになっています。
  - [Default Information Originate]：タイプ 7 デフォルトを NSSA に生成するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。
  - [Metric Value]：デフォルト ルートの OSPF メトリック値を指定します。有効値の範囲は 0 ～ 16777214 です。デフォルト値は、1 です

- [Metric Type]：デフォルト ルートの OSPF メトリック タイプです。選択肢は 1（タイプ 1）または 2（タイプ 2）です。デフォルト値は 2 です。

- [Area Networks]：OSPF エリアを定義するための設定を含みます。
  - [Enter IP Address and Mask]：そのエリア内のネットワークを定義するのに使用する設定を含みます。

    [IP Address]：そのエリアに追加するネットワークまたはホストの IP アドレスを入力します。デフォルト エリアを作成するには、0.0.0.0 およびネットマスク 0.0.0.0 を使用します。0.0.0.0 は 1 つのエリア内だけで使用できます。

    [Netmask]：エリアに追加する IP アドレスまたはホストのネットワーク マスクを選択します。ホストを追加する場合、255.255.255.255 マスクを選択します。
  - [Add]：[Enter IP Address and Mask] エリアで定義したネットワークをエリアに追加します。追加されたネットワークは、[Area Networks] テーブルに表示されます。
  - [Delete]：選択したネットワークを [Area Networks] テーブルから削除します。
  - [Area Networks]：そのエリアに対して定義されたネットワークを表示します。

    [IP Address]：ネットワークの IP アドレスを表示します。

    [Netmask]：ネットワークのネットワーク マスクを表示します。

- [Authentication]：OSPF エリア認証の設定を含みます。
  - [None]：OSPF エリア認証をディセーブルにするには、このオプションを選択します。これがデフォルト設定です。
  - [Password]：エリア認証にクリア テキスト パスワードを使用するには、このオプションを選択します。セキュリティ面が懸念される場合、このオプションは推奨しません。
  - [MD5]：MD5 認証を使用するには、このオプションを選択します。

- [Default Cost]：エリアのデフォルト コストを指定します。有効値の範囲は、0 ～ 65535 です。デフォルト値は、1 です

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Setup] > [Route Summarization] タブ

OSPF では、ABR が 1 つのエリアのネットワークを別のエリアにアドバタイズします。あるエリアにおいて連続する複数のネットワーク番号が割り当てられている場合、指定された範囲に含まれるエリア内の個別のネットワークをすべてカバーするサマリー ルートをアドバタイズするように ABR を設定できます。OSPF エリアに再配布される外部ルートのサマリー アドレスを定義する方法については、Summary Address を参照してください。

フィールド

- [Route Summarization]：セキュリティ アプライアンスで定義されたルート集約についての情報を表示します。このテーブルの行をダブルクリックすると、選択したルート集約を対象とした Add/Edit Route Summarization ダイアログボックスが開きます。
  - [OSPF Process]：ルート集約に関連付けられた OSPF プロセスの OSPF プロセス ID を表示します。
  - [Area ID]：ルート集約に関連付けられたエリアを表示します。
  - [IP Address]：サマリー アドレスを表示します。
  - [Network Mask]：サマリー マスクを表示します。
  - [Advertise]：アドレスとマスクのペアに一致するときにルート集約がアドバタイズされる場合は「yes」、アドレスとマスクのペアに一致するときにルート集約が抑止される場合は「no」を表示します。
- [Add]：[Add/Edit Route Summarization] ダイアログボックスが開きます。新しいルート集約を定義するには、このボタンを使用します。
- [Edit]：[Add/Edit Route Summarization] ダイアログボックスが開きます。選択したルート集約のパラメータを変更するには、このボタンを使用します。
- [Delete]：選択したルート集約を設定から削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Route Summarization

新しいエントリを [Route Summarization] テーブルに追加するには、[Add Route Summarization] ダイアログボックスを使用します。既存のエントリを変更するには、[Edit Route Summarization] ダイアログボックスを使用します。

フィールド

- [OSPF Process]：ルート集約を適用する OSPF プロセスを選択します。既存のルート要約エントリを編集する場合、この値は変更できません。
- [Area ID]：ルート集約を適用するエリア ID を選択します。既存のルート要約エントリを編集する場合、この値は変更できません。
- [IP Address]：集約するルートのネットワーク アドレスを入力します。
- [Network Mask]：リストから共通ネットワーク マスクの 1 つを選択するか、フィールドにマスクを入力します。
- [Advertise]：アドレス範囲ステータスを「アドバタイズ」に設定するには、このチェックボックスをオンにします。これによって、タイプ 3 サマリー LSA が生成されます。指定したネットワークのタイプ 3 サマリー LSA を抑制するには、このチェックボックスをオフにします。このチェックボックスは、デフォルトでオンになっています。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Filtering

[Filtering] ペインには、各 OSPF プロセスに設定された ABR タイプ 3 LSA フィルタが表示されます。

ABR タイプ 3 LSA フィルタにより、指定したプレフィックスだけを 1 つのエリアから別のエリアに送信し、その他すべてのプレフィックスを制限できます。このタイプのエリア フィルタリングは、特定の OSPF エリアから、特定の OSPF エリアへ、または同じ OSPF エリアへ同時に適用できます。

利点

OSPF ABR タイプ 3 LSA フィルタリングにより、OSPF エリア間のルート配布を詳細に制御できます。

制約事項

フィルタリングされるのは、ABR から送信されるタイプ 3 LSA だけです。

フィールド

[Filtering] テーブルには、次の情報が表示されます。テーブル エントリをダブルクリックすると、選択したエントリに対応する Add/Edit Filtering Entry ダイアログボックスが開きます。

- [OSPF Process]：フィルタ エントリに関連付けられた OSPF プロセスを表示します。
- [Area ID]：フィルタ エントリに関連付けられたエリアの ID を表示します。
- [Filtered Network]：フィルタリングされているネットワーク アドレスを表示します。
- [Traffic Direction]：OSPF エリアに着信する LSA にフィルタ エントリが適用される場合「Inbound」を、OSPF エリアから発信される LSA に適用される場合は「Outbound」を表示します。
- [Sequence #]：フィルタ エントリのシーケンス番号を表示します。複数のフィルタが LSA に適用されている場合、最もシーケンス番号の小さいフィルタが使用されます。
- [Action]：フィルタに一致する LSA が許可される場合は「Permit」を、フィルタに一致する LSA が拒否される場合は「Deny」を表示します。
- [Lower Range]：照合される最小プレフィックス長を表示します。
- [Upper Range]：照合される最大プレフィックス長を表示します。

[Filtering] テーブルのエントリでは、次のアクションを実行できます。

- [Add]：新しいエントリを [Filter] テーブルに追加するための Add/Edit Filtering Entry ダイアログボックスが開きます。
- [Edit]：選したフィルタを修正するための Add/Edit Filtering Entry ダイアログボックスが開きます。
- [Delete]：選択したフィルタを [Filter] テーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Filtering Entry

[Add/Edit Filtering Entry] ダイアログボックスでは、新しいフィルタを [Filter] テーブルに追加するか、既存のフィルタを修正できます。既存のフィルタを編集するとき、一部のフィルタ情報は変更できません。

フィールド

- [OSPF Process]：フィルタ エントリに関連付けられた OSPF プロセスを選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。
- [Area ID]：フィルタ エントリに関連付けられたエリアの ID を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。
- [Filtered Network]：CIDR 表記（a.b.c.d/m）を使用して、フィルタリングしているネットワークのアドレスおよびマスクを入力します。
- [Traffic Direction]：フィルタリングされているトラフィックの方向を選択します。OSPF エリアに着信する LSA をフィルタリングするには「Inbound」を、OSPF エリアから発信される LSA をフィルタリングするには「Outbound」を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。
- [Sequence #]：フィルタのシーケンス番号を入力します。有効値の範囲は 1 ～ 4294967294 です。複数のフィルタが LSA に適用されている場合、最もシーケンス番号の小さいフィルタが使用されます。
- [Action]：LSA トラフィックを許可する場合は「Permit」を、LSA トラフィックをブロックする場合は「Deny」を選択します。
- [Optional]：フィルタのオプション設定を含みます。
  - [Lower Range]：照合される最小プレフィックス長を指定します。この設定の値は、[Filtered Network] フィールドに入力するネットワーク マスクの長さよりも大きく、[Upper Range] フィールドに入力する値（ある場合）以下である必要があります。
  - [Upper Range]：照合される最大プレフィックス長を入力します。この設定の値は、[Lower Range] フィールドに入力する値（ある場合）以上である必要があります。または、[Lower Range] フィールドがブランクの場合は、[Filtered Network] フィールドに入力するネットワーク マスクの長さよりも大きい値である必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Interface

[Interface] ペインでは、OSPF メッセージ認証やプロパティなどの、インターフェイス固有の OSPF ルーティング プロパティを設定できます。これらのプロパティの設定の詳細については、次の項目を参照してください。

- [Interface] > [Authentication] タブ
- [Interface] > [Properties] タブ

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Interface] > [Authentication] タブ

[Authentication] タブには、セキュリティ アプライアンス インターフェイスの OSPF 認証情報が表示されます。

フィールド

- [Authentication Properties]：セキュリティ アプライアンス インターフェイスの認証情報を表示します。このテーブルの行をダブルクリックすると、選択したインターフェイスを対象とした Edit OSPF Interface Properties ダイアログボックスが開きます。
  - [Interface]：インターフェイス名を表示します。
  - [Authentication Type]：インターフェイスでイネーブルになっている OSPF 認証のタイプを表示します。認証タイプには、次のいずれかの値を指定できます。

    [None]：OSPF 認証はディセーブルになります。

    [Password]：クリア テキスト パスワード認証がイネーブルになります。

    [MD5]：MD5 認証がイネーブルになります。

    [Area]：エリアに対して指定された認証タイプがインターフェイスでイネーブルになります。エリア認証が、インターフェイスのデフォルト値です。ただし、エリア認証は、デフォルトではディセーブルになっています。そのため、あらかじめエリア認証タイプを指定してある場合を除いて、エリア認証を指定したインターフェイスでは認証がディセーブルになります。
- [Edit]：選択したインターフェイスを対象とした Edit OSPF Interface Properties ダイアログボックスが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit OSPF Interface Authentication

[Edit OSPF Interface Authentication] ダイアログボックスでは、選択したインターフェイスの OSPF 認証タイプおよびパラメータを設定できます。

フィールド

- [Interface]：認証を設定するインターフェイスの名前を表示します。このフィールドは編集できません。
- [Authentication]：OSPF 認証オプションを含みます。
  - [None]：OSPF 認証をディセーブルにするには、このオプションを選択します。
  - [Password]：クリア テキスト パスワード認証を使用するには、このオプションを選択します。セキュリティ面が懸念される場合は推奨しません。
  - [MD5]：MD5 認証を使用するには、このオプションを選択します（推奨）。
  - [Area]：（デフォルト）エリアに指定された認証タイプを使用するには、このオプションを選択します（エリア認証の設定の詳細については、Add/Edit OSPF Area を参照してください）。エリア認証はデフォルトでディセーブルになっています。したがって、それ以前にエリア認証タイプを指定していない限り、エリア認証を設定するインターフェイスでは、設定するまで認証がディセーブルになっています。
- [Authentication Password]：パスワード認証がイネーブルになっているとき、パスワードの入力のための設定が含まれます。
  - [Enter Password]：最大 8 文字のテキスト文字列を入力します。
  - [Re-enter Password]：パスワードを再入力します。
- [MD5 IDs and Keys]：MD5 認証がイネーブルになっているとき、MD5 キーおよびパラメータの入力のための設定が含まれます。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。
  - [Enter MD5 ID and Key]：MD5 キー情報を入力するための設定が含まれます。

    [Key ID]：数値のキー ID を入力します。有効値の範囲は、1 ～ 255 です。

    [Key]：最大 16 バイトの英数字文字列。
  - [Add]：指定した MD5 キーを [MD5 ID] および [Key] テーブルに追加します。
  - [Delete]：選択した MD5 キーおよび ID を [MD5 ID] および [Key] テーブルから削除します。
  - [MD5 ID and Key]：設定済みの MD5 キーおよびキー ID を表示します。

    [Key ID]：選択したキーのキー ID を表示します。

    [Key]：選択したキー ID のキーを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Interface] > [Properties] タブ

[Properties] タブには、各インターフェイスに定義された OSPF プロパティがテーブル形式で表示されます。

フィールド

- [OSPF Interface Properties]：インターフェイス固有の OSPF プロパティを表示します。このテーブルの行をダブルクリックすると、選択したインターフェイスを対象とした Edit OSPF Interface Properties ダイアログボックスが開きます。
  - [Interface]：OSPF 設定が適用されるインターフェイスの名前を表示します。
  - [Broadcast]：インターフェイスが非ブロードキャスト（ポイントツーポイント）に設定されている場合は、「No」を表示します。インターフェイスがブロードキャストに設定されている場合は、「Yes」を表示します。「Yes」は、イーサネット インターフェイスのデフォルト設定です。
  - [Cost]：インターフェイスを介したパケット送信のコストを表示します。
  - [Priority]：インターフェイスに割り当てられた OSPF 優先順位を表示します。
  - [MTU Ignore]：MTU ミスマッチ検出がイネーブルになっている場合は、「No」を表示します。MTU ミスマッチ検出がディセーブルになっている場合は、「Yes」を表示します。
  - [Database Filter]：同期化およびフラッディングの間に発信 LSA がフィルタリングされる場合は、「Yes」を表示します。フィルタリングがイネーブルでない場合は、「No」を表示します。
- [Edit]：選択したインターフェイスを対象とした Edit OSPF Interface Properties ダイアログボックスが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit OSPF Interface Properties

フィールド

- [Interface]：OSPF プロパティを設定するインターフェイスの名前を表示します。このフィールドは編集できません。
- [Broadcast]：インターフェイスがブロードキャスト インターフェイスであることを指定するには、このチェックボックスをオンにします。このチェックボックスは、イーサネット インターフェイスのデフォルトでオンになっています。インターフェイスをポイントツーポイント、非ブロードキャスト インターフェイスとして指定するには、このチェックボックスをオフにします。インターフェイスをポイントツーポイント、非ブロードキャストとして指定すると、OSPF ルートが VPN トンネルで送信されます。

  インターフェイスをポイントツーポイント、非ブロードキャストとして設定すると、次の制限が適用されます。

  - インターフェイスにはネイバーを 1 つだけ定義できます。
  - ネイバーは手動で設定する必要があります（Static Neighbor を参照）。
  - クリプト ポイントを指すスタティック ルートを定義する必要があります（Static Routes を参照）。
  - トンネル経由の OSPF がインターフェイスで実行中である場合は、その同じインターフェイスでは上流のルータがある通常の OSPF を実行できません。
  - OSPF 更新が VPN トンネルを通過できるように、OSPF ネイバーを指定する前に、クリプト マップをインターフェイスにバインドする必要があります。OSPF ネイバーを指定した後でクリプト マップをインターフェイスにバインドする場合は、**clear local-host all** コマンドを使用して OSPF 接続をクリアし、OSPF の隣接関係が VPN トンネル経由で確立されるようにします。
- [Cost]：インターフェイスを介したパケット送信のコストを指定します。デフォルト値は 10 です。
- [Priority]：OSPF ルータの優先順位を指定します。2 つのルータがネットワークに接続している場合、両方が指定ルータになろうとします。ルータ優先順位の高いデバイスが指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。

  この設定の有効値の範囲は、0 ～ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが指定ルータになったり、指定ルータのバックアップが行われたりします。この設定は、ポイントツーポイント、非ブロードキャスト インターフェイスとして設定されているインターフェイスには適用されません。
- [MTU Ignore]：OSPF は、ネイバーが共通インターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーによる DBD パケットの交換時に行われます。DBD パケットに受信した MTU が着信インターフェイスに設定されている IP MTU より高い場合、OSPF の隣接性は確立されません。
- [Database Filter]：同期化およびフラッディングの間に発信 LSA インターフェイスをフィルタリングするには、このチェックボックスをオンにします。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。完全メッシュ化トポロジでは、この設定が帯域幅を無駄にして、過剰なリンクおよび CPU の使用につながることがあります。このチェックボックスをオンにすることで、選択したインターフェイスでの OSPF LSA のフラッディングを防ぎます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit OSPF Interface Advanced Properties

[Edit OSPF Interface Advanced Properties] ダイアログボックスでは、OSPF の hello 間隔、再送信間隔、送信遅延、dead 間隔の値を変更できます。通常は、ネットワーク上で OSPF の問題が発生した場合にだけ、これらの値をデフォルトから変更する必要があります。

フィールド

- [Hello Interval] : hello パケットがインターフェイスで送信される間隔を秒数で指定します。hello 間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバで同じである必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 10 秒です。
- [Retransmit Interval] : インターフェイスに属する隣接関係の LSA 再送信の間隔を秒数で指定します。ルータはそのネイバーに LSA を送信すると、確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
- [Transmit Delay] : インターフェイス上で LSA パケットを送信するのに必要な予想時間を秒数で指定します。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。
- [Dead Interval] : hello パケットが受信されず、ネイバーがルータのダウンを宣言する間隔を秒数で指定します。有効な値の範囲は 1 ～ 65535 です。この設定のデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Redistribution

[Redistribution] ペインには、1 つのルーティング プロセスから OSPF ルーティング プロセスへのルートを再配布する場合のルールが表示されます。

フィールド

[Redistribution] テーブルには、次の情報が表示されます。テーブル エントリをダブルクリックすると、選択したエントリに対応する Add/Edit OSPF Redistribution Entry ダイアログボックスが開きます。

- [OSPF Process]：ルート再配布エントリに関連付けられた OSPF プロセスを表示します。
- [Protocol]：ルートの再配布元であるソース プロトコルを表示します。有効なエントリは次のとおりです。
  - [Static]：スタティック ルートは OSPF ルーティング プロセスに再配布されます。
  - [Connected]：ルートは、インターフェイス上で IP をイネーブルにすることによって、自動的に確立されました。これらのルートは、AS の外部ルートとして OSPF ルーティング プロセスに再配布されます。
  - [OSPF]：別の OSPF ルーティング プロセスからのルートは OSPF ルーティング プロセスに再配布されます。
  - [EIGRP]：ルートは、EIGRP ルーティング プロセスから OSPF ルーティング プロセスに再配布されます。
  - [RIP]：ルートは RIP ルーティング プロセスから OSPF ルーティング プロセスに再配布されます。
- [Match]：1 つの OSPF ルーティング プロセスから別の OSPF ルーティング プロセスにルートを再配布する場合に適用される条件を表示します。
- [Subnets]：サブネットされたルートが再配布される場合は「Yes」を表示します。サブネット化されていないルートだけが再配布される場合は、何も表示されません。
- [Metric Value]：ルートに使用されるメトリックを表示します。デフォルトのメトリックが使用される場合、このカラムは再配布エントリに対してブランクです。
- [Metric Type]：メトリックがタイプ 1 外部ルートの場合は「1」を、メトリックがタイプ 2 外部ルートの場合は「2」を表示します。
- [Tag Value]：各外部ルートに付加される 32 ビットの 10 進数値です。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。有効値の範囲は、0 ～ 4294967295 です。
- [Route Map]：再配布エントリに適用されるルート マップの名前を表示します。

[Redistribution] テーブル エントリでは次のアクションを実行できます。

- [Add]：新しい再配布エントリを追加するための Add/Edit OSPF Redistribution Entry ダイアログボックスが開きます。
- [Edit]：選択した再配布エントリを修正するための Add/Edit OSPF Redistribution Entry ダイアログボックスが開きます。
- [Delete]：選択した再配布エントリを [Redistribution] テーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit OSPF Redistribution Entry

[Add/Edit OSPF Redistribution Entry] ダイアログボックスでは、[Redistribution] テーブルに新しい再配布ルールを追加したり、既存の再配布ルールを編集したりできます。既存の再配布ルールを編集するとき、一部の再配布ルール情報は変更できません。

フィールド

- [OSPF Process] : ルート再配布エントリに関連付けられた OSPF プロセスを選択します。既存の再配布ルールを編集している場合、この設定は変更できません。
- [Protocol] : ルートの再配布元であるソース プロトコルを選択します。次のいずれかのオプションを選択できます。
  - [Static] : スタティック ルートを OSPF ルーティング プロセスに再配布します。
  - [Connected] : 接続されたルート（インターフェイス上で IP をイネーブルにすることによって自動的に確立されるルート）を OSPF ルーティング プロセスに再配布します。接続済みルートは、AS の外部として再配布されます。
  - [OSPF] : 別の OSPF ルーティング プロセスからルートを再配布します。リストから OSPF プロセス ID を選択してください。
  - [RIP] : RIP ルーティングプロセスからルートを再配布します。
  - [EIGRP] : EIGRP ルーティング プロセスからルートを再配布します。リストから EIGRP ルーティング プロセスの自律システム番号を選択してください。
- [Match] : 別の OSPF ルーティング プロセスから、選択した OSPF ルーティング プロセスに、ルートを再配布する場合に適用される条件を表示します。これらのオプションは、スタティック、接続済み、RIP、または EIGRP ルートを再配布するときに選択できます。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。
  - [Internal] : ルートは特定の AS の内部です。
  - [External 1] : 自律システムの外部だが、OSPF にタイプ 1 外部ルートとしてインポートされるルート。
  - [External 2] : 自律システムの外部だが、OSPF にタイプ 2 外部ルートとしてインポートされるルート。
  - [NSSA External 1] : 自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。
  - [NSSA External 2] : 自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。
- [Metric Value] : 再配布するルートのメトリック値を指定します。有効値の範囲は 1 ～ 16777214 です。同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。

- [Metric Type]：メトリックがタイプ 1 外部ルートである場合は「1」を、メトリックがタイプ 2 外部ルートである場合は「2」を選択します。
- [Tag Value]：タグ値は、各外部ルートに付加される 32 ビットの 10 進数値です。これは OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。有効値の範囲は、0 ～ 4294967295 です。
- [Use Subnets]：サブネット ルートの再配布をイネーブルにするには、このチェックボックスをオンにします。サブネットされていないルートだけを再配布するには、このチェックボックスをオフにします。
- [Route Map]：再配布エントリに適用されるルート マップの名前を入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Static Neighbor

[Static Neighbor] ペインには、手動で定義されたネイバーが表示されます。検出されたネイバーは表示されません。

ポイントツーポイントの非ブロードキャスト インターフェイスごとに、スタティック ネイバーを定義する必要があります。また、[Static Neighbor] テーブルにある各スタティック ネイバーに対してスタティック ルートを定義する必要もあります。

フィールド

- [Static Neighbor]：各 OSPF プロセスに定義されたスタティック ネイバーの情報を表示します。このテーブルの行をダブルクリックすると、Add/Edit OSPF Neighbor Entry ダイアログボックスが開きます。
  - [OSPF Process]：スタティック ネイバーに関連付けられた OSPF プロセスを表示します。
  - [Neighbor]：スタティック ネイバーの IP アドレスを表示します。
  - [Interface]：スタティック ネイバーに関連付けられたインターフェイスを表示します。
- [Add]：[Add/Edit OSPF Neighbor Entry] ダイアログボックスが開きます。このボタンを使用して、新しいスタティック ネイバーを定義します。
- [Edit]：[Add/Edit OSPF Neighbor Entry] ダイアログボックスが開きます。このボタンを使用して、スタティック ネイバーの設定を変更します。
- [Delete]：選択したエントリを [Static Neighbor] テーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit OSPF Neighbor Entry

[Add/Edit OSPF Neighbor Entry] ダイアログボックスでは、新しいスタティック ネイバーを定義するか、既存のスタティック ネイバーの情報を変更できます。

ポイントツーポイントの非ブロードキャスト インターフェイスごとに、スタティック ネイバーを定義する必要があります。

制約事項

- 異なる 2 つの OSPF プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティック ネイバーにスタティック ルートを定義する必要があります（「Static Routes」（P.16-45）を参照）。

フィールド

- [OSPF Process]：スタティック ネイバーに関連付けられた OSPF プロセスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。
- [Neighbor]：スタティック ネイバーの IP アドレスを入力します。
- [Interface]：スタティック ネイバーに関連付けられたインターフェイスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Summary Address

[Summary Address] ペインには、各 OSPF ルーティング プロセスに設定されたサマリー アドレスに関する情報が表示されます。

他のルーティング プロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。サマリー ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。

OSPF のサマリー ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1 つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティング プロトコルからのルートだけをサマライズできます。

フィールド

[Summary Address] テーブルには、次の情報が表示されます。テーブルのエントリをダブルクリックすると、選択したエントリに対応する [Add/Edit OSPF Summary Address Entry] ダイアログボックスが開きます。

- [OSPF Process]：サマリー アドレスに関連付けられた OSPF プロセスを表示します。
- [IP Address]：サマリー アドレスの IP アドレスを表示します。
- [Netmask]：サマリー アドレスのネットワーク マスクを表示します。
- [Advertise]：サマリー ルートがアドバタイズされる場合は、「Yes」を表示します。サマリー ルートがアドバタイズされない場合は、「No」を表示します。
- [Tag]：各外部ルートに付加される 32 ビットの 10 進数値を表示します。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。

[Summary Address] テーブルのエントリでは、次のアクションを実行できます。

- [Add]：新しいサマリー アドレス エントリを追加するための [Add/Edit OSPF Summary Address Entry] ダイアログボックスが開きます。
- [Edit]：選択したエントリを編集するための [Add/Edit OSPF Summary Address Entry] ダイアログボックスが開きます。
- [Delete]：選択したサマリー アドレス エントリを [Summary Address] テーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit OSPF Summary Address Entry

[Add/Edit OSPF Summary Address Entry] ダイアログボックスでは、[Summary Address] テーブルに新しいエントリを追加したり、[Summary Address] テーブルの既存のエントリを変更したりできます。既存のエントリを編集するとき、一部のサマリー アドレス情報は変更できません。

フィールド

- [OSPF Process]：サマリー アドレスに関連付けられた OSPF プロセスを選択します。既存のエントリを編集する場合、この情報は変更できません。
- [IP Address]：サマリー アドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。
- [Netmask]：サマリー アドレスのネットワーク マスクを入力するか、共通マスクのリストからネットワーク マスクを選択します。既存のエントリを編集する場合、この情報は変更できません。
- [Advertise]：サマリー ルートをアドバタイズするには、このチェックボックスをオンにします。サマリー アドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、チェックボックスがオンになっています。

- [Tag]：（任意）タグ値は、各外部ルートに付加される 32 ビットの 10 進数値です。これは OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。有効値の範囲は、0 ～ 4294967295 です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Virtual Link

OSPF ネットワークにエリアを追加し、そのエリアをバックボーン エリアに直接接続できない場合、仮想リンクを作成する必要があります。仮想リンクは、通過エリアと呼ばれる共通エリアを持つ 2 つの OSPF デバイスを接続します。OSPF デバイスのいずれかは、バックボーン エリアに接続されている必要があります。

フィールド

[Virtual Link] テーブルには、次の情報が表示されます。テーブルのエントリをダブルクリックすると、選択したエントリに対応する [Add/Edit Virtual Link] ダイアログボックスが開きます。

- [OSPF Process]：仮想リンクに関連付けられた OSPF プロセスを表示します。
- [Area ID]：通過エリアの ID を表示します。
- [Peer Router ID]：仮想リンク ネイバーのルータ ID を表示します。
- [Authentication]：仮想リンクが使用する認証のタイプを表示します。
  - [None]：認証は使用されません。
  - [Password]：クリア テキスト パスワード認証が使用されます。
  - [MD5]：MD5 認証が使用されます。

[Virtual Link] テーブルのエントリでは、次のアクションを実行できます。

- [Add]：新しいエントリを [Virtual Link] テーブルに追加するための [Add/Edit Virtual Link] ダイアログボックスが開きます。
- [Edit]：選択したエントリに対応する [Add/Edit Virtual Link] ダイアログボックスが開きます。
- [Delete]：選択したエントリを [Virtual Link] テーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Virtual Link

[Add/Edit Virtual Link] ダイアログボックスでは、新しい仮想リンクを定義したり、既存の仮想リンクのプロパティを変更したりできます。

フィールド

- [OSPF Process] : 仮想リンクに関連付けられた OSPF プロセスを選択します。既存の仮想リンクを編集している場合、この値は変更できません。
- [Area ID] : ネイバー OSPF デバイスと共有するエリアを選択します。[NSSA] エリアまたは [Stub] エリアは選択できません。既存の仮想リンクを編集している場合、この値は変更できません。
- [Peer Router ID] : 仮想リンク ネイバーのルータ ID を入力します。既存の仮想リンクを編集している場合、この値は変更できません。
- [Advanced] : [Advanced OSPF Virtual Link Properties] ダイアログボックスが開きます。このエリアにある仮想リンクに対して、OSPF プロパティを設定できます。プロパティには、認証およびパケット間隔設定が含まれます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Advanced OSPF Virtual Link Properties

[Advanced OSPF Virtual Link Properties] ダイアログボックスでは、OSPF 認証およびパケット間隔を設定できます。

フィールド

- [Authentication] : OSPF 認証オプションを含みます。
  - [None] : OSPF 認証をディセーブルにするには、このオプションを選択します。
  - [Password] : クリア テキスト パスワード認証を使用するには、このオプションを選択します。セキュリティ面が懸念される場合は推奨しません。
  - [MD5] : MD5 認証を使用するには、このオプションを選択します（推奨）。
- [Authentication Password] : パスワード認証がイネーブルになっているとき、パスワードの入力のための設定が含まれます。

- [Enter Password]：最大 8 文字のテキスト文字列を入力します。
- [Re-enter Password]：パスワードを再入力します。

- [MD5 IDs and Keys]：MD5 認証がイネーブルになっているとき、MD5 キーおよびパラメータの入力のための設定が含まれます。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。
  - [Enter MD5 ID and Key]：MD5 キー情報を入力するための設定が含まれます。

    [Key ID]：数値のキー ID を入力します。有効値の範囲は、1 ～ 255 です。

    [Key]：最大 16 バイトの英数字文字列。
  - [Add]：指定した MD5 キーを [MD5 ID] および [Key] テーブルに追加します。
  - [Delete]：選択した MD5 キーおよび ID を [MD5 ID] および [Key] テーブルから削除します。
  - [MD5 ID and Key]：設定済みの MD5 キーおよびキー ID を表示します。

    [Key ID]：選択したキーのキー ID を表示します。

    [Key]：選択したキー ID のキーを表示します。
- [Intervals]：パケット間隔のタイミングを変更するための設定を含みます。
  - [Hello Interval]：hello パケットがインターフェイスで送信される間隔を秒数で指定します。hello 間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバで同じである必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 10 秒です。
  - [Retransmit Interval]：インターフェイスに属する隣接関係の LSA 再送信の間隔を秒数で指定します。ルータはそのネイバーに LSA を送信すると、確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
  - [Transmit Delay]：インターフェイス上で LSA パケットを送信するのに必要な予想時間を秒数で指定します。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。
  - [Dead Interval]：hello パケットが受信されず、ネイバーがルータのダウンを宣言する間隔を秒数で指定します。有効な値の範囲は 1 ～ 65535 です。このフィールドのデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

RIP

RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトル ルーティング プロトコルです。RIP がインターフェイス上でイネーブルの場合、そのインターフェイスは、ネイバー デバイスと RIP ブロードキャストを交換して、ルートの動的な学習およびアドバタイズを行います。

セキュリティ アプライアンスは、RIP バージョン 1 と RIP バージョン 2 の両方をサポートします。RIP バージョン 1 は、ルーティング更新でサブネット マスクを送信しません。RIP バージョン 2 は、ルーティング更新でサブネット マスクを送信し、変数長サブネット マスクをサポートします。また、RIP バージョン 2 では、ルーティング更新の交換時にネイバー認証がサポートされます。この認証により、信頼できるソースからの信頼性のあるルーティング情報が セキュリティ アプライアンス で受信されることが保証されます。

制限事項

RIP には、次の制限事項があります。

- RIP アップデートは、セキュリティ アプライアンス のインターフェイス間を通過できません。
- RIP バージョン 1 では、可変長サブネット マスクがサポートされていません。
- RIP の最大ホップ カウントは 15 です。ホップ カウントが 15 を超えるルートは、到達不能と見なされます。
- RIP の収束は、他のルーティング プロトコルと比べて時間がかかります。
- セキュリティ アプライアンス では、RIP プロセスを 1 つだけイネーブルにできます。

RIP バージョン 2 の注意事項

次の情報は、RIP バージョン 2 だけに適用されます。

- ネイバー認証を使用する場合、認証キーとキー ID は、RIP バージョン 2 更新をインターフェイスに提供するすべてのネイバー デバイスで同じである必要があります。
- RIP バージョン 2 では、セキュリティ アプライアンスがマルチキャスト アドレス 224.0.0.9 を使用してデフォルト ルートの更新を送信および受信します。パッシブ モードでは、そのアドレスでルート アップデートが受信されます。
- RIP バージョン 2 がインターフェイスで設定されている場合、マルチキャスト アドレス 224.0.0.9 がそのインターフェイス上に登録されます。RIP バージョン 2 構成がインターフェイスから削除されると、そのマルチキャスト アドレスは登録解除されます。

Setup

[Setup] ペインを使用して、セキュリティ アプライアンスで RIP をイネーブルにし、グローバル RIP プロトコル パラメータを設定します。セキュリティ アプライアンス では、RIP プロセスを 1 つだけイネーブルにできます。

フィールド

- [Enable RIP Routing] : セキュリティ アプライアンスでの RIP ルーティングをイネーブルにするには、このチェックボックスをオンにします。RIP をイネーブルにすると、すべてのインターフェイス上でイネーブルになります。また、このチェックボックスをオンにすると、このペインの他のフィールドもイネーブルになります。セキュリティ アプライアンスでの RIP ルーティングをディセーブルにするには、このチェックボックスをオフにします。
- [Enable Auto-summarization] : このチェックボックスをオフにすると、自動ルート集約をディセーブルにします。自動ルート集約を再度イネーブルにするには、このチェックボックスをオンにします。RIP バージョン 1 では、常に自動集約が使用されます。RIP バージョン 1 に対して自動集

約をディセーブルにすることはできません。RIP バージョン 2 を使用している場合は、このチェックボックスをオフにすれば自動集約をオフにできます。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズをディセーブルにします。自動サマライズをディセーブルにすると、サブネットがアドバタイズされます。

- [Enable RIP version]：セキュリティ アプライアンスが使用する RIP のバージョンを指定するには、このチェックボックスをオンにします。このチェックボックスがオフになっている場合、セキュリティ アプライアンスは RIP バージョン 1 更新を送信し、RIP バージョン 1 およびバージョン 2 の更新を受け入れます。この設定は、Interface ペインでインターフェイスごとに上書きできます。
  - [Version 1]：セキュリティ アプライアンスが RIP バージョン 1 更新だけを送信および受信するように指定します。受信されたバージョン 2 更新はドロップされます。
  - [Version 2]：セキュリティ アプライアンスが RIP バージョン 2 更新だけを送信および受信するように指定します。受信されたバージョン 1 更新はドロップされます。
- [Enable default information originate]：RIP ルーティング プロセスにデフォルト ルートを生成するには、このチェックボックスをオンにします。デフォルト ルートの生成前に満たす必要のあるルート マップを設定できます。
  - [Route-map]：適用するルート マップの名前を入力します。ルート マップが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。
- [IP Network to Add]：RIP ルーティング プロセスのネットワークを定義します。指定されたネットワーク番号は、サブネット情報に含めないでください。セキュリティ アプライアンスの設定に追加できるネットワーク数に制限はありません。指定されたネットワーク上のインターフェイスのみを経由して、RIP ルーティング更新が送受信されます。また、インターフェイスのネットワークを指定しない場合、インターフェイスは RIP 更新でアドバタイズされません。
  - [Add]：指定したネットワークをネットワークのリストに追加するには、このボタンをクリックします。
  - [Delete]：選択したネットワークをネットワークのリストから削除するには、このボタンをクリックします。
- [Configure interfaces as passive globally]：セキュリティ アプライアンス上のすべてのインターフェイスをパッシブ RIP モードに設定するには、このチェックボックスをオンにします。セキュリティ アプライアンスはすべてのインターフェイス上の RIP ルーティング ブロードキャストを受信し、その情報を使用してルーティング テーブルを取り込みますが、ルーティング更新をブロードキャストすることはありません。特定のインターフェイスをパッシブ RIP に設定するには、[Passive Interfaces] テーブルを使用します。
- [Passive Interfaces] テーブル：セキュリティ アプライアンスでの設定済みインターフェイスを一覧表示します。パッシブ モードで操作するインターフェイスの [Passive] カラムにあるチェックボックスをオンにします。他のインターフェイスは、引き続き RIP ブロードキャストを送信および受信します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Interface

[Interface] ペインでは、インターフェイスが送受信する RIP のバージョン、また使用される場合には RIP ブロードキャストの認証方式など、インターフェイス固有の RIP 設定を行えます。

フィールド

- [Interface] テーブル：各行に、インターフェイスのインターフェイス固有 RIP 設定が表示されます。エントリの行をダブルクリックすると、そのインターフェイスを対象とした [Edit RIP Interface Entry] ダイアログボックスが開きます。
- [Edit] : [Interface] テーブルで選択したインターフェイスを対象とした [Edit RIP Interface Entry] ダイアログボックスが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit RIP Interface Entry

[Edit RIP Interface Entry] ダイアログボックスでは、インターフェイス固有 RIP を設定できます。

フィールド

- [Override Global Send Version] : インターフェイスが送信する RIP バージョンを指定するには、このチェックボックスをオンにします。次のオプションを選択できます。
  - Version 1
  - Version 2
  - Version 1 & 2

  このチェックボックスをオフにすると、グローバル設定が復元されます。
- [Override Global Receive Version] : インターフェイスが受け入れる RIP バージョンを指定するには、このチェックボックスをオンにします。サポート対象外のバージョンの RIP から更新された RIP をインターフェイスが受信すると、その RIP はドロップされます。次のオプションを選択できます。
  - Version 1
  - Version 2
  - Version 1 & 2

  このチェックボックスをオフにすると、グローバル設定が復元されます。
- [Enable Authentication] : RIP 認証をイネーブルにするには、このチェックボックスをオンにします。RIP ブロードキャスト認証をディセーブルにするには、このチェックボックスをオフにします。
  - [Key] : 認証方式で使用するキーです。最大 16 文字です。

– [Key ID]：キー ID です。有効な値は、0 ～ 255 です。
– [Authentication Mode]：次の認証モードを選択できます。
[MD5]：RIP メッセージ認証に MD5 を使用します。
[Text]：RIP メッセージ認証にクリア テキストを使用します（お勧めしません）。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Filter Rules

フィルタ ルールにより、RIP ルーティング更新で受信したネットワーク、または RIP ルーティング更新で送信したネットワークをフィルタリングできます。各フィルタ ルールは、1 つ以上のネットワーク ルールで構成されます。

フィールド

- [Filter Rules] テーブル：設定済み RIP フィルタ ルールを表示します。
- [Add]：このボタンをクリックすると、[Add/Edit Filter Rule] ダイアログボックスが開きます。新しいフィルタ ルールは、リストの最下部に追加されます。
- [Edit]：このボタンをクリックすると、選択したフィルタ ルールを対象とした [Add/Edit Filter Rule] ダイアログボックスが開きます。
- [Delete]：このボタンをクリックすると、選択したフィルタ ルールが削除されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Filter Rule

フィルタ ルールを作成するには、[Add/Edit Filter Rule] ペインを使用します。すべてのインターフェイスに適用されるフィルタ ルール、または特定のインターフェイスに適用されるフィルタ ルールを作成できます。

フィールド

- [Direction]：フィルタが動作する方向を次の中から 1 つ選択します。

  - [In]：受信 RIP 更新でネットワークをフィルタリングします。
  - [Out]：送信 RIP 更新からのネットワークをフィルタリングします。
- [Interface]：フィルタ ルールに対して特定のインターフェイスを選択することも、[All Interfaces] オプションを選択してフィルタをすべてのインターフェイスに適用することもできます。
- [Action]：（*表示専用*）受信または送信 RIP アドバタイズメントから指定されたネットワークがフィルタリングされない場合は、[Permit] を表示します。受信または送信 RIP アドバタイズメントから指定されたネットワークがフィルタリングされる場合は、[Deny] を表示します。
- [IP Address]：（*表示専用*）フィルタリングするネットワークの IP アドレスを表示します。
- [Netmask]：（*表示専用*）IP アドレスに適用されるネットワーク マスクを表示します。
- [Insert]：リストで選択したルールの上にネットワーク ルールを追加するには、このボタンをクリックします。このボタンをクリックすると、[Network Rule] ダイアログボックスが開きます。
- [Edit]：選択したルールを編集するには、このボタンをクリックします。このボタンをクリックすると、[Network Rule] ダイアログボックスが開きます。
- [Add]：リストで選択したルールの下にネットワーク ルールを追加するには、このボタンをクリックします。このボタンをクリックすると、[Network Rule] ダイアログボックスが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Network Rule

[Network Rule] ペインでは、フィルタ ルールにある特定ネットワークに対して、許可ルールと拒否ルールを設定できます。

フィールド

- [Action]：RIP 更新で指定ネットワークがアドバタイズされる、または RIP ルーティング プロセスに受け入れられるのを許可するには、[Permit] を選択します。指定ネットワークが RIP 更新でアドバタイズされる、または RIP ルーティング プロセスに受け入れられるのを防ぐには、[Deny] を選択します。
- [IP Address]：許可されるまたは拒否されるネットワークの IP アドレスを入力します。
- [Netmask]：ネットワーク IP アドレスに適用されるネットワーク マスクを指定します。このフィールドにネットワーク マスクを入力するか、リストから共通マスクの 1 つを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Redistribution

[Redistribution] ペインには、他のルーティング プロセスから RIP ルーティング プロセスに再配布されるルートが表示されます。

フィールド

- [Protocol]：（*表示専用*）RIP ルーティング プロセスに再配布されるルーティング プロトコルを表示します。
  - [Static]：スタティック ルートです。
  - [Connected]：ネットワークに直接接続されています。
  - [OSPF]：指定した OSPF ルーティング プロセスで検出されたネットワークです。
  - [EIGRP]：指定した EIGRP ルーティング プロセスで検出されたネットワークです。
- [Metric]：再配布されたルートに適用される RIP メトリックです。
- [Match]：（*表示専用*）RIP ルーティング プロセスに再配布される OSPF ルートのタイプを表示します。OSPF 再配布ルールに対して [Match] カラムが空白の場合、[Internal]、[External 1]、および [External 2] ルートは、RIP ルーティング プロセスに再配布されます。
- [Route Map]：（*表示専用*）再配布に適用されるルート マップの名前がある場合は、その名前を表示します。ルート マップは、どのルートが指定したルーティング プロセスから RIP に再配布されるかといった非常に詳細な内容を指定するのに使用されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Route Redistribution

新しい再配布ルールを追加するには、[Add Route Redistribution] ダイアログボックスを使用します。既存のルールを変更するには、[Edit Route Redistribution] ダイアログボックスを使用します。

フィールド

- [Protocol]：RIP ルーティング プロセスに再配布するルーティング プロトコルを選択します。
  - [Static]：スタティック ルートです。

  - [Connected]：ネットワークに直接接続されています。
  - [OSPF and OSPF ID]：OSPF ルーティング プロセスで検出されたルートです。OSPF を選択する場合、OSPF プロセス ID を入力する必要もあります。さらに、[Match] 領域から再配布する OSPF ルートの特定タイプを選択できます。
  - [EIGRP and EIGRP ID]：EIGRP ルーティング プロセスで検出されたルートです。[EIGRP] を選択する場合は、[EIGRP ID] フィールドで EIGRP ルーティング プロセスの自律システム番号を指定する必要もあります。
- [Route Map]：ルートが RIP ルーティング プロセスに再配布される前に満たす必要のあるルート マップの名前を指定します。
- [Configure Metric Type]：再配布されるルートのメトリックを指定するには、このチェックボックスをオンにします。指定しない場合、ルートにはメトリック 0 が割り当てられます。
  - [Transparent]：現在のルート メトリックを使用するには、このオプションを選択します。
  - [Value]：特定のメトリック値を割り当てるには、このオプションを選択します。入力できる値は、0 ～ 16 です。
- [Match]：OSPF ルートを RIP ルーティング プロセスに再配布する場合、ルート タイプの隣にあるチェックボックスをオンにすれば、再配布する OSPF ルートの特定タイプを選択できます。いずれのルート タイプもオンにしない場合、デフォルトでは、[Internal]、[External 1]、および [External 2] ルートが再配布されます。
  - [Internal]：AS に対して内部のルートが再配布されます。
  - [External 1]：AS に対して外部のタイプ 1 ルートが再配布されます。
  - [External 2]：AS に対して外部のタイプ 2 ルートが再配布されます。
  - [NSSA External 1]：NSSA に対して外部のタイプ 1 ルートが再配布されます。
  - [NSSA External 2]：NSSA に対して外部のタイプ 2 ルートが再配布されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

EIGRP

EIGRP は、シスコが開発した、IGRP の拡張バージョンです。IGRP や RIP と異なり、EIGRP が定期的にルート アップデートを送信することはありません。EIGRP アップデートは、ネットワーク トポロジが変更された場合にだけ送信されます。

セキュリティ アプライアンスでは、EIGRP ルーティング プロセスを 1 つだけイネーブルにすることができます。

ここでは、次の内容について説明します。

- 「EIGRP の設定」（P.16-31）
- 「EIGRP の各ペインのフィールド情報」（P.16-32）

動的に検出された EIGRP ネイバーの監視の詳細については、「EIGRP ネイバーのモニタリング」（P.45-8）を参照してください。

EIGRP の設定

セキュリティ アプライアンスで EIGRP を設定するには、次の手順を実行します。

ステップ 1　ASDM インターフェイスの [Configuration] > [Device Setup] > [Routing] > [EIGRP] 領域に移動します。

ステップ 2　[Setup] > [Process Instances] タブで EIGRP ルーティング プロセスをイネーブルにします。詳細については、「Process Instances」（P.16-32）を参照してください。

ステップ 3　（任意）EIGRP ルーティング プロセスのパラメータを設定します。[Setup] > [Process Instances] タブで [Advanced] をクリックします。

EIGRP ルーティング プロセスをスタブ ルーティング プロセスとして設定し、自動ルート集約をディセーブルにし、再配布されるルートのデフォルト メトリックを定義できます。また、内外 EIGRP ルートのアドミニストレーティブ ディスタンスを変更し、スタティック ルータ ID を設定し、隣接関係の変更のロギングをイネーブルまたはディセーブルにすることもできます。詳細については、「Edit EIGRP Process Advanced Properties」（P.16-33）を参照してください。

ステップ 4　[Setup] > [Networks] タブで、EIGRP ルーティングに参加するネットワークとインターフェイスを定義します。詳細については、「Networks」（P.16-34）を参照してください。

定義済みネットワークの範囲内にある直接接続されたスタティック ネットワークには、セキュリティ アプライアンスがアドバタイズします。また、IP アドレスが定義済みネットワークの範囲内にあるインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

EIGRP ルーティングに参加させないインターフェイスがアドバタイズ先のネットワークに接続されている場合は、そのインターフェイスが接続されているネットワーク エントリを [Setup] > [Networks] タブで設定し、次にそのインターフェイスをパッシブ インターフェイスとして設定して、インターフェイスが EIGRP 更新を送受信できないようにします。パッシブに設定されたインターフェイスは、EIGRP 更新を送受信しません。詳細については、「Passive Interfaces」（P.16-35）を参照してください。

ステップ 5　（任意）[Filter Rules] ペインでルート フィルタを定義します。ルート フィルタにより、EIGRP 更新で送受信することを許可されているルートをより細かく制御できます。詳細については、「Filter Rules」（P.16-36）を参照してください。

ステップ 6　（任意）[Redistribution] ペインでルート再配布を定義します。

RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。スタティックまたは接続されているルートが、[Setup] > [Networks] タブで設定されたネットワークの範囲内にある場合は、そのルートを再配布する必要はありません。詳細については、「Redistribution」（P.16-38）を参照してください。

ステップ 7　（任意）[Static Neighbor] ペインでスタティック EIGRP ネイバーを定義します。

EIGRP hello パケットはマルチキャスト パケットとして送信されます。EIGRP ネイバーが、トンネルなど、非ブロードキャスト ネットワークを越えた場所にある場合、そのネイバーを手動で定義する必要があります。手動で EIGRP ネイバーを定義すると、hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。詳細については、「Static Neighbor」（P.16-40）を参照してください。

ステップ 8　（任意）[Summary Address] ペインで、サマリー アドレスを定義します。

ネットワーク番号の境界以外でサマリー アドレスを作成する場合、または自動ルート集約がディセーブルになったセキュリティ アプライアンスでサマリー アドレスを使用する場合は、手動でサマリー アドレスを定義する必要があります。サマリー アドレスの定義の詳細については、「Summary Address」（P.16-41）を参照してください。自動ルート集約をイネーブルおよびディセーブルにする方法については、「Edit EIGRP Process Advanced Properties」（P.16-33）を参照してください。

ステップ 9　（任意）[Interfaces] ペインで、インターフェイス固有の EIGRP パラメータを定義します。これらのパラメータには、EIGRP メッセージ認証、保持時間、hello 間隔、遅延メトリック、スプリットホライズンの使用などがあります。詳細については、「Interface」（P.16-37）を参照してください。

ステップ 10　（任意）[Default Information] ペインで、EIGRP 更新でのデフォルト ルート情報の送受信を制御します。デフォルトでは、デフォルト ルートが送信され、受け入れられます。詳細については、「Default Information」（P.16-41）を参照してください。

EIGRP の各ペインのフィールド情報

ここでは、次の内容について説明します。

Setup

[Setup] ペインでは、EIGRP プロセスをイネーブルにし、そのプロセスの基本設定を行います。[Setup] ペインには次のタブがあります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Process Instances

[Process Instances] タブでは、EIGRP ルーティング プロセスをイネーブルにすることができます。

フィールド

- [Enable this EIGRP Process]：EIGRP ルーティング プロセスをイネーブルにするには、このチェックボックスをオンにします。デバイスでイネーブルにすることができる EIGRP ルーティング プロセスは 1 つだけです。変更を保存できるようにするには、まず [EIGRP Process] フィールドにルーティング プロセスの自律システム番号を入力する必要があります。
- [EIGRP Process]：EIGRP プロセスの自律システム番号を入力します。自律システム番号は 1 ～ 65535 の範囲で指定できます。
- [Advanced]：ルータ ID、デフォルト メトリック、スタブ ルーティング設定、ネイバー変更と警告ロギング、および EIGRP ルートのアドミニストレーティブ ディスタンスなどの EIGRP プロセス設定を行うには、このボタンをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit EIGRP Process Advanced Properties

[Edit EIGRP Process Advanced Properties] ダイアログボックスでは、EIGRP ルーティング プロセスのルータ ID、デフォルト メトリック、スタブ ルーティング設定、ネイバー変更と警告ロギング、および EIGRP ルートのアドミニストレーティブ ディスタンスを設定できます。

フィールド

- [EIGRP]：*表示専用。* EIGRP ルーティング プロセスの自律システム番号を表示します。
- [Router Id]：EIGRP ルーティング プロセスでセキュリティ アプライアンスのルータ ID として使用する IP アドレスを入力します。ルータ ID は、外部ルートの発信元ルータを識別するために使用されます。IP アドレスは、セキュリティ アプライアンスで設定されたアドレスにする必要はありませんが、ルーティング ドメイン内で一意になっている必要があります。指定しない場合、セキュリティ アプライアンス上で最上位の IP アドレスがルータ ID として使用されます。
- [Auto-Summary]：自動ルート集約をイネーブルにするには、このボックスをオンにします。自動ルート集約をディセーブルにするには、このボックスをオフにします。この設定はデフォルトでイネーブルになっています。
- [Default Metrics]：デフォルトのメトリックが EIGRP ルーティング プロセスに再配布されるルートに適用されます。指定しない場合は、再配布を設定するときにメトリックを指定する必要があります（「Redistribution」（P.16-38）を参照）。
  - [Bandwidth]：ルートの最小帯域幅（キロバイト/秒）です。有効な値は、1 ～ 4294967295 です。
  - [Loading]：1 ～ 255（255 は 100% の負荷）の数値で表現したルートの有効帯域幅です。
  - [Reliability]：0 ～ 255 の数値として表現した、パケットが正常に伝送される見込みです。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。
  - [Delay]：10 マイクロ秒単位のルート遅延です。有効な値は、1 ～ 4294967295 です。
  - [MTU]：最大伝送単位の最小許容値（バイト）です。有効な値は 1 ～ 65535 です。

- [Stub]：スタブ エリアには、EIGRP スタブ ルーティング プロセスを作成するための設定があります。スタブ ルーティング プロセスでは、完全なトポロジ テーブルは維持されません。スタブ ルーティングには、ルーティングの決定を行うために、少なくとも配布ルータへのデフォルト ルートが必要です。
  - [Stub Receive only]：隣接ルータからルート情報を受信しても、それらの隣接ルータにルート情報を送信しない EIGRP スタブ ルーティング プロセスを設定します。このオプションを選択する場合は、他のスタブ ルーティング オプションを選択できません。
  - [Stub Connected]：接続済みルートをアドバタイズします。
  - [Stub Static]：スタティック ルートをアドバタイズします。
  - [Stub Redistributed]：再配布ルートをアドバタイズします。
  - [Stub Summary]：サマリー ルートをアドバタイズします。
- [Adjacency Changes]：ネイバーの警告および変更メッセージのロギングを設定できます。どちらのメッセージのロギングも、デフォルトでイネーブルになっています。
  - [Log Neighbor Changes]：ネイバー隣接関係の変更のロギングをイネーブルにするにはボックスをオンに、ディセーブルにするにはボックスをオフにします。
  - [Log Neighbor Warnings]：ネイバー隣接関係の変更をイネーブルにするにはボックスをオンに、ディセーブルにするにはボックスをオフにします。ネイバー警告メッセージの繰り返し間隔（秒）を入力します。有効な値は 1 ～ 65535 です。この間隔内に警告が繰り返し発生した場合、それらの警告はログに記録されません。
- [Administrative Distance]：内外 EIGRP ルートのアドミニストレーティブ ディスタンスを設定できます。
  - [Internal Distance]：EIGRP 内部ルートのアドミニストレーティブ ディスタンスです。内部ルートとは、同じ自律システム内の別のエンティティから学習されるルートです。有効な値は、1 ～ 255 です。デフォルトは 90 です。
  - [External Distance]：EIGRP 外部ルートのアドミニストレーティブ ディスタンスです。外部ルートとは、最適パスを自律システムの外部にあるネイバーから学習するルートです。有効な値は、1 ～ 255 です。デフォルト値は 170 です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Networks

[Network] タブでは、EIGRP ルーティング プロセスで使用されるネットワークを指定できます。EIGRP ルーティングに参加するインターフェイスは、これらのネットワーク エントリで定義されるアドレスの範囲内に存在する必要があります。アドバタイズされる直接接続およびスタティックのネットワークも、これらのネットワーク エントリの範囲内である必要があります。

[Network] テーブルに、EIGRP ルーティング プロセス用に設定するネットワークが表示されます。このテーブルの各行には、指定した EIGRP ルーティング プロセス用に設定するネットワーク アドレスおよび関連するマスクが表示されます。ネットワークを追加または修正するには、次のいずれかの操作を実行します。

- 新しいネットワーク エントリを追加するには、[Add] をクリックします。[Add EIGRP Network] ダイアログボックスが表示されます。
- ネットワーク エントリを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。
- ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

フィールド

[Add EIGRP Network Entry] ダイアログボックスには、次のフィールドがあります。

- [EIGRP AS] : EIGRP ルーティング プロセスの自律システム番号を表示します。
- [IP Address] : EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。
- [Network Mask] : IP アドレスに適用するネットワーク マスクを選択または入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Passive Interfaces

[Passive Interface] タブでは、1 つ以上のインターフェイスをパッシブ インターフェイスとして設定できます。EIGRP の場合、受動インターフェイスではルーティング アップデートが送受信されません。

[Passive Interface] テーブルには、パッシブ インターフェイスとして設定された各インターフェイスが一覧表示されます。インターフェイスが EIGRP ルーティングに参加するかどうかを設定するには、次のいずれかの操作を実行します。

- すべてのインターフェイスをパッシブとして指定するには、[Suppress routing updates on all interfaces] チェックボックスをオンにします。[Passive Interface] テーブルに表示されていないインターフェイスであっても、このチェックボックスをオンにするとパッシブに設定されます。
- パッシブ インターフェイス エントリを追加するには、[Add] をクリックします。[Add EIGRP Passive Interface] ダイアログボックスが表示されます。このダイアログボックスでは、パッシブにするインターフェイスを選択できます。
- パッシブ インターフェイスを削除するには、テーブルでそのインターフェイスを選択し、[Delete] をクリックします。

フィールド

[Passive Interface] ペインには次のフィールドがあります。

- [EIGRP Process] : EIGRP ルーティング プロセスの自律システム番号です。

- [Suppress routing updates on all interfaces]：すべてのインターフェイスをパッシブに設定するには、このチェックボックスをオンにします。すべてのインターフェイスで EIGRP 更新を送受信できるようにするには、このチェックボックスをオフにします。また、EIGRP ルーティングに参加するには、インターフェイスにネットワーク エントリを関連付ける必要があります。
- [Passive Interfaces table]：パッシブに設定されているインターフェイスを表示します。
  - [Interface]：インターフェイスの名前が表示されます。
  - [EIGRP Process]：EIGRP プロセスの自律システム番号を表示します。
  - [Passive]：インターフェイスがパッシブ モードで動作している場合には、「true」と表示されます。

[Add Passive Interface] ダイアログボックスには次のフィールドがあります。

- [EIGRP AS]：EIGRP ルーティング プロセスの自律システム番号です。
- [Interface]：リストからインターフェイスを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

- 「EIGRP の設定」（P.16-31）

Filter Rules

[Filter Rules] ペインには、EIGRP ルーティング プロセスに設定されているルート フィルタリング ルールが表示されます。フィルタ ルールによって、EIGRP ルーティング プロセスで受け入れまたはアドバタイズされるルートを制御できます。

[Filter Rule] テーブルの各行には、特定のインターフェイスまたはルーティング プロトコルに適用されるフィルタ ルールについての情報が記載されます。たとえば、外部インターフェイスで「in」方向のフィルタ ルールの場合は、外部インターフェイスが受信する EIGRP 更新すべてにフィルタリングが適用されます。ルーティング プロトコルとして OSPF 10 が指定された「out」方向のフィルタ ルールの場合は、発信 EIGRP 更新の EIGRP ルーティング プロセスに再配布されるルートにフィルタ ルールが適用されます。

フィルタ ルールを設定するには、次のいずれかの操作を実行します。

- フィルタ ルールを追加するには、[Add] をクリックします。[Add Filter Rules] ダイアログボックスが表示されます。
- フィルタ ルールを編集するには、テーブルでそのフィルタ ルールを選択し、[Edit] をクリックします。フィルタ ルールをダブルクリックして編集することもできます。[Edit Filter Rules] ダイアログボックスが表示されます。
- フィルタ ルールを削除するには、テーブルでそのフィルタ ルールを選択し、[Delete] をクリックします。

フィールド

[Add/Edit EIGRP Filter Rule] ダイアログボックスには、次のフィールドがあります。

- [EIGRP]：EIGRP ルーティング プロセスの自律システム番号です。
- [Direction]：着信 EIGRP ルーティング更新からのルートをフィルタリングするルールの場合は、「in」を選択します。セキュリティ アプライアンスによって送信される EIGRP ルーティング更新からのルートをフィルタリングするには、「out」を選択します。
- [Routing process]：（発信フィルタの場合のみ）フィルタされるルートのタイプを指定します。スタティック、接続済み、RIP、および OSPF のルーティング プロセスから再配布されるルートをフィルタリングできます。ルーティング プロセスを指定するフィルタは、すべてのインターフェイスで送信される更新からのルートをフィルタリングします。
- [Id]：OSPF プロセス ID です。
- [Interface]：フィルタが適用されるインターフェイスです。
- [Add：Network Rule] ダイアログボックスが開きます。
- [Edit]：選択したネットワーク ルールを対象とした [Network Rule] ダイアログボックスが開きます。

[Add/Edit Network Rule] ダイアログボックスでは、フィルタ ルールのアクセス リストを定義できます。このダイアログボックスには、次のフィールドがあります。

- [Action]：指定したネットワークへのアドバタイズを許可するには、[Permit] を選択します。指定したネットワークへのアドバタイズを拒否するには、[Deny] を選択します。
- [IP Address]：許可されるまたは拒否されるネットワークの IP アドレスを入力します。すべてのアドレスを許可または禁止するには、IP アドレス 0.0.0.0 とネットワーク マスク 0.0.0.0 を使用します。
- [Netmask]：ネットワーク IP アドレスに適用されるネットワーク マスクを指定します。このフィールドにネットワーク マスクを入力するか、リストから共通マスクの 1 つを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

- 「EIGRP の設定」（P.16-31）

Interface

[Interface] ペインには、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、セキュリティ アプライアンスのインターフェイスすべてが表示され、インターフェイスごとに次の設定を修正できます。

- 認証キーとモード。
- EIGRP hello 間隔と保持時間。

- EIGRP メトリックの計算で使用されるインターフェイス遅延メトリック。
- インターフェイスでのスプリットホライズンの使用。

インターフェイスの EIGRP パラメータを設定するには、インターフェイス エントリをダブルクリックするか、そのエントリを選択して [Edit] をクリックします。[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

フィールド

[Edit EIGRP Interface Entry] ダイアログボックスには、次のフィールドがあります。

- [Interface]：*表示専用。*修正されるインターフェイスを表示します。
- [AS]：EIGRP 自律システム番号です。
- [Hello Interval：EIGRP hello] パケットがインターフェイスで送信される間隔を入力します。有効な値は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
- [Hold Time]：保持時間を秒数で指定します。有効な値は、1 ～ 65535 秒です。デフォルト値は 15 秒です。
- [Split Horizon]：インターフェイスでスプリット ホライズンをイネーブルにするには、このチェックボックスをオンにします。スプリット ホライズンをディセーブルにするには、チェックボックスをオフにします。スプリット ホライズンはデフォルトでイネーブルになっています。
- [Delay]：このフィールドに遅延値を入力します。遅延時間は 10 マイクロ秒単位です。有効な値は、1 ～ 16777215 です。
- [Enable MD5 Authentication]：EIGRP プロセス メッセージの MD5 認証をイネーブルにするには、このチェックボックスをオンにします。
  - [Key]：EIGRP 更新を認証するキーです。このキーには、最大 16 文字を含めることができます。
  - [Key ID]：キー ID です。有効値の範囲は 1 ～ 255 です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

- 「EIGRP の設定」（P.16-31）

Redistribution

[Redistribution] ペインには、他のルーティング プロトコルから EIGRP ルーティング プロセスにルートを再配布する場合のルールが表示されます。[Redistribution] ペインの各行には、ルート再配布エントリが表示されます。

EIGRP ルーティング プロセスにルート再配布を追加するか、または表示されるルート再配布を修正するには、次のいずれかの操作を実行します。

- 新しい再配布ルールを追加するには、[Add] をクリックします。[Add EIGRP Redistribution Entry] ダイアログボックスが開きます。
- 既存の EIGRP スタティック ネイバーを編集するには、テーブルでそのアドレスを選択し、[Edit] をクリックします。テーブルのエントリをダブルクリックして編集することもできます。[Edit EIGRP Redistribution Entry] ダイアログボックスが開きます。

フィールド

[Add/Edit EIGRP Redistribution Entry] ダイアログボックスには、次のフィールドがあります。

- [AS]：エントリが適用される EIGRP ルーティング プロセスの自律システム番号を表示します。
- [Static]：スタティック ルートを EIGRP ルーティング プロセスに再配布します。ネットワーク設定の範囲内にあるスタティック ルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。
- [Connected]：接続済みルートを EIGRP ルーティング プロセスに再配布します。ネットワーク設定の範囲内にある接続済みルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。
- [RIP]：RIP ルーティング プロセスによって検出されたルートを EIGRP に再配布します。
- [Optional Metrics]：再配布されるルートで使用するメトリックを定義します。[Edit EIGRP Process Advanced Properties] ダイアログボックスでデフォルト メトリックをすでに定義済みの場合は、これらの値を定義する必要はありません（デフォルト メトリックの設定の詳細については、「Edit EIGRP Process Advanced Properties」（P.16-33）を参照してください）。
  - [Bandwidth]：EIGRP 帯域幅メトリック（キロビット/秒）です。有効な値は、1 ～ 4294967295 です。
  - [Delay]：EIGRP 遅延メトリック（10 マイクロ秒単位）です。有効な値は、0 ～ 4294967295 です。
  - [Reliability]：EIGRP 信頼性メトリックです。有効な値は、0 ～ 255 です（255 は 100% の信頼性を示します）。
  - [Loading]：EIGRP 有効帯域幅（負荷）メトリックです。有効な値は、1 ～ 255 です（255 は 100% の負荷を示します）。
  - [MTU]：パスの MTU です。有効な値は 1 ～ 65535 です。
- [Route Map]：EIGRP ルーティング プロセスに再配布されるルートをさらに細かく定義するには、ルート マップの名前を入力します。
- [Optional OSPF Redistribution]：これらのオプションにより、EIGRP ルーティング プロセスに再配布される OSPF ルートをさらに細かく指定できます。
  - [Match Internal]：指定した OSPF プロセスに対して内部の一致ルートです。
  - [Match External 1]：指定した OSPF プロセスに対して外部の一致タイプ 1 のルートです。
  - [Match External 2]：指定した OSPF プロセスに対して外部の一致タイプ 2 のルートです。
  - [Match NSSA-External 1]：指定した OSPF NSSA に対して外部の一致タイプ 1 のルートです。
  - [Match NSSA-External 2]：指定した OSPF NSSA に対して外部の一致タイプ 2 のルートです。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

- 「EIGRP の設定」（P.16-31）

Static Neighbor

[Static Neighbor] ペインには、スタティックに定義された EIGRP ネイバーが表示されます。EIGRP ネイバーは、セキュリティ アプライアンスとの間で EIGRP ルーティング情報を送受信します。通常は、ネイバー探索プロセスによってネイバーがダイナミックに検出されます。ただし、ポイントツーポイントの非ブロードキャスト ネットワークでは、ネイバーをスタティックに定義する必要があります。

[Static Neighbor] テーブルの各行には、ネイバーの EIGRP 自律システム番号、ネイバー IP アドレス、およびネイバーに接続するためのインターフェイスが表示されます。

スタティック ネイバーを設定するには、次のいずれかの操作を実行します。

- 新しい EIGRP スタティック ネイバーを追加するには、[Add] をクリックします。[Add EIGRP Neighbor Entry] ダイアログボックスが開きます。
- 既存の EIGRP スタティック ネイバーを編集するには、テーブルでそのアドレスを選択し、[Edit] をクリックします。テーブルのエントリをダブルクリックして編集することもできます。[Edit EIGRP Neighbor Entry] ダイアログボックスが開きます。

フィールド

[Add/Edit EIGRP Neighbor Entry] ダイアログボックスには、次のフィールドがあります。

- [EIGRP AS]：ネイバーの設定対象となる EIGRP プロセスの自律システム番号です。
- [Interface Name]：リストから、ネイバーに接続するときに使用するインターフェイスを選択します。
- [Neighbor IP Address]：ネイバーの IP アドレスを入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

- 「EIGRP の設定」（P.16-31）

Summary Address

[Summary Address] ペインには、スタティックに定義された EIGRP サマリー アドレスのテーブルが表示されます。デフォルトでは、EIGRP はサブネット ルートをネットワーク レベルに集約します。[Summary Address] ペインでは、サブネット レベルに集約されるスタティックに定義された EIGRP サマリー アドレスを作成できます。

サマリー アドレスを作成または修正するには、次のいずれかの操作を実行します。

- 新しい EIGRP サマリー アドレスを追加するには、[Add] をクリックします。[Add Summary Address] ダイアログボックスが開きます。
- 既存の EIGRP サマリー アドレスを編集するには、テーブルでそのアドレスを選択し、[Edit] をクリックします。テーブルのエントリをダブルクリックして編集することもできます。[Edit Summary Address] ダイアログボックスが開きます。

フィールド

[Add/Edit EIGRP Summary Address Entry] ダイアログボックスには、次のフィールドがあります。これらのフィールドは、[Summary Address] テーブルにも表示されます。

- [EIGRP AS] : サマリー アドレスが適用される EIGRP ルーティング プロセスの自律システム番号を選択します。
- [Interface] : サマリー アドレスのアドバタイズ元となるインターフェイスです。
- [IP Address] : サマリー ルートの IP アドレスを入力します。
- [Netmask] : IP アドレスに適用するネットワーク マスクを選択または入力します。
- [Administrative Distance] : ルートのアドミニストレーティブ ディスタンスを入力します。空白のままにすると、ルートのアドミニストレーティブ ディスタンスはデフォルト値の 5 になります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

- 「EIGRP の設定」（P.16-31）

Default Information

[Default Information] ペインには、EIGRP 更新でのデフォルト ルート情報の送受信を制御するルールのテーブルが表示されます。EIGRP ルーティング プロセスごとに、「in」ルールと「out」ルールを 1 つずつ設定できます（現在は 1 つのプロセスだけがサポートされています）。

デフォルトでは、デフォルト ルートが送信され、受け入れられます。デフォルトのルート情報の送受信を制限またはディセーブルにするには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Default Information] ペインを開きます。

ステップ 2　次のいずれかを実行します。

- 新しいエントリを作成するには、[Add] をクリックします。
- エントリを編集するには、テーブルでそのエントリをダブルクリックするか、またはテーブルでエントリを選択し、[Edit] をクリックします。

そのエントリを対象とした [Add or Edit Default Information] ダイアログボックスが開きます。[EIGRP] フィールドでは、EIGRP 自律システム番号が自動的に選択されます。

ステップ 3　[Direction] フィールドでルールの方向を設定します。

- [in] : ルールは、着信 EIGRP 更新からのデフォルト ルート情報をフィルタリングします。
- [out] : ルールは、発信 EIGRP 更新からのデフォルト ルート情報をフィルタリングします。

EIGRP プロセスごとに、「in」ルールと「out」ルールを 1 つずつ設定できます。

ステップ 4　ネットワーク ルール テーブルにネットワーク ルールを追加します。ネットワーク ルールでは、デフォルト ルート情報を送受信するときに許可されるネットワークと拒否されるネットワークを定義します。デフォルト情報フィルタ ルールに追加するネットワーク ルールごとに、次の手順を繰り返します。

a. ネットワーク ルールを追加するには [Add] をクリックします。既存のネットワーク ルールをダブルクリックしてルールを編集します。

b. [Action] フィールドで、[Permit] を選択してネットワークを許可するか、または [Deny] を選択してネットワークをブロックします。

c. [IP Address] フィールドと [Network Mask] フィールドに、ルールによって許可または拒否されるネットワークの IP アドレスとネットワーク マスクを入力します。

すべてのデフォルト ルート情報の受け入れまたは送信を拒否するには、ネットワーク アドレスとして 0.0.0.0 を使用し、ネットワーク マスクとして 0.0.0.0 を選択します。

d. 指定したネットワーク ルールをデフォルト情報フィルタ ルールに追加するには、[OK] をクリックします。

ステップ 5　デフォルト情報フィルタ ルールを受け入れるには、[OK] をクリックします。

フィールド

[Add/Edit Default Information] ダイアログボックスには、次のフィールドがあります。

- [EIGRP] : デフォルト情報フィルタが適用される EIGRP ルーティング プロセスの自律システム番号を選択します。
- [Direction] : 着信ルート更新からのデフォルト ルート情報をフィルタリングするには、「in」を選択します。発信ルート更新からのデフォルト ルート情報をフィルタするには、「out」を選択します。
- [Add] : デフォルト情報フィルタ ルールにネットワーク ルールを追加します。
- [Edit] : 既存のネットワーク ルールを修正します。

[Network Rule] ダイアログボックス。[Default Information filter rule] テーブルの [Filter Rules] カラムには、ネットワーク ルールが表示されます。

- [Action] : 指定したネットワークへのアドバタイズを許可するには、[Permit] を選択します。指定したネットワークへのアドバタイズを拒否するには、[Deny] を選択します。
- [IP Address] : 許可されるまたは拒否されるネットワークの IP アドレスを入力します。すべてのアドレスを許可または禁止するには、IP アドレス 0.0.0.0 とネットワーク マスク 0.0.0.0 を使用します。
- [Netmask] : ネットワーク IP アドレスに適用されるネットワーク マスクを指定します。このフィールドにネットワーク マスクを入力するか、リストから共通マスクの 1 つを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

- 「EIGRP の設定」（P.16-31）

Static Routes

マルチ コンテキスト モードは、ダイナミック ルーティングをサポートしていません。したがって、セキュリティ アプライアンスが直接接続されないネットワークに対してスタティック ルートを定義する必要があります。

トランスペアレント ファイアウォール モードでは、セキュリティ アプライアンスから直接接続されていないネットワークに宛てたトラフィック用にデフォルト ルートまたはスタティック ルートを設定して、セキュリティ アプライアンスがトラフィックの送信先インターフェイスを認識できるようにする必要があります。セキュリティ アプライアンスから発信されるトラフィックには、syslog サーバ、Websense サーバまたは N2H2 サーバ、あるいは AAA サーバとの通信もあります。1 つのデフォルト ルートで到達できないサーバがある場合、スタティック ルートを設定する必要があります。

最も単純なオプションは、すべてのトラフィックをアップストリーム ルータに送信するようにデフォルト ルートを設定して、トラフィックのルーティングをルータに任せることです。しかし、デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティック ルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部インターフェイス上にある場合、デフォルト ルートは、セキュリティ アプライアンスに直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。

また、スタティック ルートをダイナミック ルーティング プロトコルと共に使用し、ダイナミックに検出されたルートがダウンしたときに使用されるフローティング スタティック ルートを提供できます。ダイナミック ルーティング プロトコルのアドミニストレーティブ ディスタンスよりも長いアドミニストレーティブ ディスタンスを指定してスタティック ルートを作成すると、ルーティング プロトコルで検出される指定の宛先へのルートがスタティック ルートより優先されます。スタティック ルートは、ダイナミックに検出されたルートがルーティング テーブルから削除された場合に限り使用されます。

スタティック ルートは、指定されたゲートウェイが利用できなくなってもルーティング テーブルに保持されています（この場合の例外については、「スタティック ルート トラッキング」（P.16-44）を参照してください）。指定されたゲートウェイが利用できなくなった場合は、スタティック ルートをルーティング テーブルから手動で削除する必要があります。ただし、スタティック ルートは、セキュリティ アプライアンスの関連インターフェイスがダウンした場合にルーティング テーブルから削除されます。インターフェイスが元に戻ると、スタティック ルートは復旧します。

インターフェイスごとに同じ宛先でコストの等しいルートを 3 つまで定義できます。ECMP は複数のインターフェイス間ではサポートされていません。ECMP では、トラフィックは必ずしもルート間で均等に分割されるわけではありません。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレスをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

デフォルト ルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてをセキュリティ アプライアンスが送信する、ゲートウェイの IP アドレスを特定するルートです。デフォルト ルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティック ルートです。特定の宛先が特定されたルートはデフォルト ルートより優先されます。

デバイスあたり最大 3 つの等コスト デフォルト ルート エントリを定義することができます。複数の等コスト デフォルト ルート エントリを定義すると、デフォルト ルートに送信されるトラフィックは、指定されたゲートウェイの間に分散されます。複数のデフォルト ルートを定義する場合は、各エントリに同じインターフェイスを指定する必要があります。

4 つ以上の等コスト デフォルト ルートを定義しようとした場合、またはすでに定義されているデフォルト ルートとは別のインターフェイスでデフォルト ルートを定義しようとした場合は、エラー メッセージが表示されます。

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。[tunneled] オプションを使用してデフォルト ルートを作成すると、セキュリティ アプライアンスに着信し、既知のルートでもスタティック ルートでもルーティングできない暗号化されたトラフィックはすべて、このルートに送信されます。これ以外の暗号化されていないトラフィックには、標準のデフォルト ルート エントリが使用されます。[tunneled] オプションでは、複数のデフォルト ルートは定義できません。トンネル トラフィックでは ECMP がサポートされていません。

ASDM を使用したスタティック ルートおよびデフォルト ルートの表示と設定の詳細については、「[Static Routes] のフィールド情報」（P.16-45）を参照してください。

スタティック ルート トラッキング

セキュリティ アプライアンスがマルチ コンテキスト モードやトランスペアレント モードの場合など、必ずしもセキュリティ アプライアンスでダイナミック ルーティング プロトコルを使用できるとは限りません。この場合、スタティック ルートを使用する必要があります。

スタティック ルートの問題の 1 つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。ネクスト ホップ ゲートウェイがダウンしても、ルーティング テーブルに保持されます。セキュリティ アプライアンスの関連インターフェイスがダウンした場合にのみルーティング テーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。これを利用すると、たとえば、ISP ゲートウェイへのデフォルト ルートを定義し、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップ用のデフォルト ルートを定義することができます。

セキュリティ アプライアンスでは、定義されたモニタリング対象にスタティック ルートを関連付けることで、この機能を実行します。対象のモニタリングは、ICMP エコー要求を使用して行います。指定された時間内にエコー応答がない場合は、そのオブジェクトはダウンしていると見なされ、関連付けられたルートはルーティング テーブルから削除されます。削除されたルートに代わって、すでに定義されているバックアップ ルートが使用されます。

モニタリング対象の選択時には、その対象が ICMP エコー要求に応答できることを確認してください。対象には、ICMP エコー要求に応答する任意のネットワーク オブジェクトを選択できます。選択肢には、次のものがあります。

- ISP ゲートウェイ アドレス（デュアル ISP サポート用）
- ネクスト ホップ ゲートウェイ アドレス（ゲートウェイの使用可能状況に懸念がある場合）
- セキュリティ アプライアンスが通信を行う必要のあるサーバ（AAA サーバなど）
- 宛先ネットワーク上の永続的なネットワーク オブジェクト（夜間にシャットダウンするデスクトップ PC やノートブック PC は適しません）

スタティック ルート トラッキングの設定の詳細については、「スタティック ルート トラッキングの設定」（P.16-45）を参照してください。スタティック ルート トラッキング プロセスのモニタリング方法については、「interface connection」（P.44-9）を参照してください。

スタティック ルート トラッキングの設定

ここで説明する手順では、スタティック ルート トラッキングの設定の概要を示します。この機能の設定に使用するさまざまなフィールドの詳細については、「[Static Routes] のフィールド情報」（P.16-45）を参照してください。

スタティック ルートのトラッキングを設定するには、次の手順を実行します。

ステップ 1　対象を選択します。対象がエコー要求に応答することを確認してください。

ステップ 2　[Static Routes] ページを開きます。[Configuration] > [Routing] > [Static Routes] に移動します。

ステップ 3　[Add] をクリックし、選択した対象の使用可能状況に基づいて使用されるスタティック ルートを設定します。このルートのインターフェイス、IP アドレス、マスク、ゲートウェイ、およびメトリックを入力する必要があります。これらのフィールドの詳細については、「Add/Edit Static Route」（P.16-46）を参照してください。

ステップ 4　このルートの [Options] 領域で [Tracked] を選択します。

ステップ 5　トラッキング プロパティを設定します。一意のトラック ID、一意の SLA ID、および対象の IP アドレスを入力する必要があります。これらのフィールドの詳細については、「Add/Edit Static Route」（P.16-46）を参照してください。

ステップ 6　（任意）モニタリング プロパティを設定するには、[Add Static Route] ダイアログボックスの [Monitoring Options] をクリックします。モニタリング プロパティに関する詳細情報については、「Route Monitoring Options」（P.16-47）を参照してください。

ステップ 7　[OK] をクリックして変更を保存します。

追跡するルートを保存するとすぐに、モニタリング プロセスが開始されます。

ステップ 8　セカンダリ ルートを作成します。セカンダリ ルートは、追跡されたルートと同じ宛先へのスタティック ルートですが、異なるインターフェイスまたはゲートウェイを経由します。このルートは、追跡されたルートより長いアドミニストレーティブ ディスタンス（メトリック）に割り当てる必要があります。

[Static Routes] のフィールド情報

特定のペインの詳細については、次の項目を参照してください。

- 「Static Routes」（P.16-45）
- 「Add/Edit Static Route」（P.16-46）
- 「Route Monitoring Options」（P.16-47）

Static Routes

[Static Route] ペインでは、任意のインターフェイスのルータに接続されたネットワークにアクセスするスタティック ルートを作成することができます。デフォルトのルートを入力するには、IP アドレスとマスクを 0.0.0.0 と設定するか、または短縮形式の 0 と設定します。

1 つのセキュリティ アプライアンスインターフェイスの IP アドレスがゲートウェイの IP アドレスとして使用される場合、セキュリティ アプライアンスは、ゲートウェイ IP アドレスに ARP を実行するのではなく、パケットの指定 IP アドレスに ARP を実行します。

ゲートウェイ ルータまでのホップ数を確認できない限り、メトリックをデフォルト設定の 1 のままにします。

フィールド

[Static Route] ペインには、次が含まれる [Static Route] テーブルが表示されます。

- [Interface]：（*表示専用*）インターフェイスでイネーブルになっている内部または外部のネットワーク インターフェイス名を一覧表示します。
- [IP Address]：（*表示専用*）内部または外部ネットワーク IP アドレスを一覧表示します。デフォルト ルートを指定するには、**0.0.0.0** を使用します。**0.0.0.0** の IP アドレスは、**0** と省略できます。
- [Netmask]：（*表示専用*）IP アドレスに適用されるネットワーク マスクのアドレスを一覧表示します。デフォルト ルートを指定するには、**0.0.0.0** を使用します。ネットマスク **0.0.0.0** は、**0** に短縮できます。
- [Gateway IP]：（*表示専用*）このルートのネクスト ホップ アドレスであるゲートウェイ ルータの IP アドレスを一覧表示します。
- [Metric]：（*表示専用*）ルートのアドミニストレーティブ ディスタンスを一覧表示します。メトリックが指定されない場合、デフォルトは 1 です。
- [Options]：（*表示専用*）スタティック ルートに指定されたオプションを表示します。
  - [None]：スタティック ルートにはオプションが指定されていません。
  - [Tunneled]：ルートを、VPN トラフィックのデフォルト トンネル ゲートウェイとして指定します。デフォルト ルートだけに使用されます。1 つのデバイスに設定できるのは 1 つのトンネル ルートだけです。トランスペアレント モードではトンネル オプションがサポートされていません。
  - [Tracked]：ルートを追跡することを指定します。トラッキング オブジェクトの ID およびトラッキング対象のアドレスも表示されます。追跡オプションは、シングル ルーテッド モードでだけサポートされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Static Route

[Add/Edit Static Route] ダイアログボックスを使用して、スタティック ルートのプロパティを設定します。このダイアログボックスは、Startup Wizard の [Static Routes] 画面、および [Configuration] > [Routing] > [Static Route] ペインの両方で使用できます。

フィールド

- [Interface Name]：ルートの出力インターフェイスを選択します。

- [IP Address]：内部または外部ネットワーク IP アドレスを指定します。デフォルト ルートを指定するには、**0.0.0.0** を使用します。**0.0.0.0** の IP アドレスは、**0** と省略できます。
- [Mask]：IP アドレスに適用するネットワーク マスク アドレスを指定します。デフォルト ルートを指定するには、**0.0.0.0** を使用します。ネットマスク **0.0.0.0** は、**0** に短縮できます。
- [Gateway IP]：このルータのネクスト ホップ アドレスであるゲートウェイ ルータの IP アドレスを指定します。
- [Metric]：ルートのアドミニストレーティブ ディスタンスを指定します。メトリックが指定されない場合、デフォルトは **1** です。

スタティック ルートでは次のオプションを使用できます。これらのいずれかのオプションのみをスタティック ルートに選択できます。デフォルトでは、オプションなし（[None]）が選択されています。

- [None]：スタティック ルートにはオプションが指定されていません。
- [Tunneled]：デフォルト ルートだけに使用されます。セキュリティ アプライアンスごとに、デフォルトのトンネリングされるゲートウェイが 1 つだけ許可されます。[Tunneled] オプションは、トランスペアレント モードではサポートされていません。
- [Tracked]：ルートが追跡されるよう指定するには、このオプションを選択します。このオプションを指定すると、ルート トラッキング プロセスが開始されます。
  - [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。
  - [Track IP Address/DNS Name]：追跡される対象の IP アドレスまたはホスト名を入力します。通常、ルートのネクスト ホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。

（注）　ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

  - [SLA ID]：SLA モニタリング プロセスの一意の ID です。
  - [Monitor Options]：[Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Route Monitoring Options

[Route Monitoring Options] ダイアログボックスを使用して、トラッキング オブジェクトのモニタリング プロパティを変更します。

フィールド

- [Frequency]：追跡対象の存在をセキュリティ アプライアンスがテストする頻度を秒数で入力します。デフォルト値は 60 秒です。有効な値は、1 ～ 604800 秒です。

- [Threshold]：しきい値を超えたイベントを示す時間をミリ秒数で入力します。この値に、タイムアウト値より大きい値は指定できません。
- [Timeout]：ルート モニタリング操作が要求パケットからの応答を待つ時間をミリ秒数で入力します。デフォルト値は 5000 ミリ秒です。有効値の範囲は、0 ～ 604800000 ミリ秒です。
- [Data Size]：エコー要求パケットで使用するデータ ペイロードのサイズを入力します。デフォルト値は 28 です。有効な値は、0 ～ 16384 です。

（注）　この設定では、ペイロードのサイズだけが指定されます。パケット全体のサイズは指定されません。

- [ToS]：エコー要求の IP ヘッダーにあるサービス バイトのタイプの値を入力します。デフォルト値は 0 です 有効な値は、0 ～ 255 です。
- [Number of Packets]：各テストに送信されるエコー要求の数です。デフォルト値は、1 です 有効な値は、1 ～ 100 です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

ASR Group

非同期ルーティング グループ ID 番号をインターフェイスに割り当てるには、[ASR Group] 画面を使用します。

場合によっては、セッションのリターン トラフィックが送信元とは別のインターフェイスでルーティングされることがあります。フェールオーバー設定では、ある装置から発信された接続の戻りトラフィックが、ピア装置を経由して返送されることがあります。これは一般に、1 つの セキュリティ アプライアンス 上の 2 つのインターフェイス、またはフェールオーバー ペアの 2 つの セキュリティ アプライアンス が別々のサービス プロバイダーに接続され、発信接続で NAT アドレスを使用しない場合に起こります。セキュリティ アプライアンス では、戻りトラフィックは接続情報がないためデフォルトでは廃棄されます。

リターン トラフィックのドロップは、ドロップが発生する可能性のあるインターフェイスで ASR Group を使用することで防止できます。[ASR Group] で設定されたインターフェイスは、セッション情報を持っていないパケットを受信すると、同じグループにある他のインターフェイスのセッション情報をチェックします。

一致する情報が見つからない場合、パケットはドロップされます。一致する情報が見つかると、次の動作のうちいずれかが開始します。

- 着信トラフィックがフェールオーバー設定のピア装置で発信された場合、レイヤ 2 ヘッダーの一部または全部が書き換えられ、パケットは他の装置にリダイレクトされます。このリダイレクトは、セッションがアクティブである限り続行されます。

- 着信トラフィックが同じ装置の別のインターフェイスに発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットはストリームに再注入されます。

前提条件

セッション情報の Stateful Failover がスタンバイ フェールオーバー グループからアクティブ フェールオーバー グループに渡されるようにイネーブルにする必要があります。

フィールド

[ASR Group] テーブルには、セキュリティ アプライアンスの各インターフェイスの次の情報が表示されます。

- [Interface] : セキュリティ アプライアンスのインターフェイスの名前を表示します。
- [ASR Group ID] : インターフェイスが属する ASR Group の数を表示します。インターフェイスに ASR Group 番号が割り当てられていない場合、このカラムには「-- None --」が表示されます。有効な値は、1 ～ 32 です。

  ASR Group 番号をインターフェイスに割り当てるには、割り当てるインターフェイスの行の [ASR Group ID] セルをクリックします。有効な ASR Group 番号のリストが表示されます。希望の ASR Group 番号をリストから選択します。1 つの ASR Group には最高 8 つのインターフェイスを割り当てることができます。他のコンテキストに、ASR Group に割り当てられたインターフェイスがある場合、これらのインターフェイスは、現在設定されているコンテキストに対しても合計 8 つにカウントされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	•	—

プロキシ ARP

まれに、グローバル アドレスに対するプロキシ ARP をディセーブルにした方がよい場合もあります。

ホストによって IP トラフィックが同じイーサネット ネットワーク上の別のデバイスに送信される場合、ホストではそのデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが IP アドレスを所有していなくても、その固有の MAC アドレスで ARP 要求に応答する場合に使用します。NAT を設定し、セキュリティ アプライアンスのインターフェイスと同じネットワーク上にあるグローバル アドレスを指定すると、セキュリティ アプライアンスによってプロキシ ARP が使用されます。トラフィックがホストにアクセスできる唯一の方法は、セキュリティ アプライアンスでプロキシ ARP が使用されている場合、セキュリティ アプライアンスの MAC アドレスが宛先グローバル アドレスに割り当てられていると主張することです。

フィールド

- [Interface]：インターフェイス名を一覧表示します。
- [Proxy ARP Enabled]：プロキシ ARP が NAT グローバル アドレスに対してイネーブルになっているか、ディセーブルになっているかを Yes または No で表示します。
- [Enable]：選択したインターフェイスのプロキシ ARP をイネーブルにします。デフォルトでは、プロキシ ARP はすべてのインターフェイスに対してイネーブルです。
- [Disable]：選択したインターフェイスのプロキシ ARP をディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 17

マルチキャスト ルーティングの設定

マルチキャスト ルーティングは、シングル ルーテッド モードでだけサポートされます。ここでは、次の内容について説明します。

- 「Multicast」（P.17-1）：セキュリティ アプライアンスでのマルチキャスト ルーティングをイネーブルまたはディセーブルにします。
- 「IGMP」（P.17-2）：セキュリティ アプライアンスで IGMP を設定します。
- 「Multicast Route」（P.17-8）：スタティック マルチキャスト ルートを定義します。
- 「MBoundary」（P.17-10）：管理用に範囲を定めたマルチキャスト アドレスの境界を設定します。
- 「MForwarding」（P.17-12）：インターフェイスごとのマルチキャスト転送をイネーブルまたはディセーブルにします。
- 「PIM」（P.17-13）：セキュリティ アプライアンスで PIM を設定します。

Multicast

[Multicast] ペインでは、セキュリティ アプライアンスでのマルチキャスト ルーティングをイネーブルにできます。

マルチキャスト ルーティングがイネーブルになれば、デフォルトですべてのインターフェイス上の IGMP と PIM がイネーブルになります。IGMP は、直接接続されているサブネット上にグループのメンバが存在するかどうか学習するために使用されます。ホストは、IGMP 報告メッセージを送信することにより、マルチキャスト グループに参加します。PIM は、マルチキャスト データグラムを転送するための転送テーブルを維持するために使用されます。

（注） マルチキャスト ルーティングでは、UDP トランスポート レイヤだけがサポートされています。

フィールド

[Enable Multicast Routing]：このチェックボックスをオンにすると、セキュリティ アプライアンスでの IP マルチキャスト ルーティングがイネーブルになります。IP マルチキャスト ルーティングをディセーブルにする場合は、このチェックボックスをオフにします。デフォルトでは、マルチキャストはディセーブルになっています。マルチキャストをイネーブルにすると、すべてのインターフェイス上でマルチキャストがイネーブルになります。マルチキャストはインターフェイスごとにディセーブルにできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

「マルチキャスト ルーティングの設定」（P.17-1）
「IGMP」（P.17-2）
「Multicast Route」（P.17-8）
「MBoundary」（P.17-10）
「MForwarding」（P.17-12）
「PIM」（P.17-13）

IGMP

IP ホストは、自身のグループ メンバーシップを直接接続されているマルチキャスト ルータに報告するために IGMP を使用します。IGMP では、グループ アドレス（クラス D IP アドレス）が使用されます。ホスト グループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。アドレス 224.0.0.0 がグループに割り当てられることはありません。アドレス 224.0.0.1 は、サブネットのシステムすべてに割り当てられます。アドレス 224.0.0.2 は、サブネットのルータすべてに割り当てられます。

セキュリティ アプライアンスでの IGMP の設定に関する詳細については、次の各項目を参照してください。

- アクセス グループ
- Join Group
- Protocol
- Static Group

アクセス グループ

アクセス グループは、インターフェイス上で許可されるマルチキャスト グループを制御するためのものです。

フィールド

- [Access Groups]：各インターフェイスに定義されたアクセス グループが表示されます。

  テーブル エントリは、上から下の順で処理されます。具体的なエントリはテーブルの上方に、一般的なエントリは下方に配置してください。たとえば、特定のマルチキャスト グループを許可するためのアクセス グループ エントリはテーブルの上方に配置し、許可ルールに指定されたグループなど、一定のまとまりを持った複数のマルチキャスト グループを拒否するようなアクセス グループ エントリは下方に配置します。ただし、拒否ルールよりも許可ルールの方が優先的に適用されるため、許可ルールに指定されているグループは、拒否ルールが適用された場合でも許可されます。

テーブルのエントリをダブルクリックすると、選択したエントリに対応する [Add/Edit Access Group] ダイアログボックスが開きます。

- [Interface]：アクセス グループが関連付けられたインターフェイスが表示されます。
- [Action]：アクセス ルールにおいて、該当するマルチキャスト グループ アドレスが許可されている場合は、[Permit] が表示されます。アクセス ルールにおいて、該当するマルチキャスト グループ アドレスが拒否されている場合は、[Deny] が表示されます。
- [Multicast Group Address]：アクセス ルールが適用されるマルチキャスト グループ アドレスが表示されます。
- [Netmask]：マルチキャスト グループ アドレスのネットワーク マスクが表示されます。

- [Insert Before]：[Add/Edit Access Group] ダイアログボックスが開きます。テーブルで選択したエントリの前に新しいアクセス グループ エントリを追加する場合は、このボタンを使用します。
- [Insert After]：[Add/Edit Access Group] ダイアログボックスが開きます。テーブルで選択したエントリの後に新しいアクセス グループ エントリを追加する場合は、このボタンを使用します。
- [Add]：[Add/Edit Access Group] ダイアログボックスが開きます。テーブルの最後尾に新しいアクセス グループ エントリを追加する場合は、このボタンを使用します。
- [Edit]：[Add/Edit Access Group] ダイアログボックスが開きます。選択したアクセス グループ エントリの情報を変更する場合は、このボタンを使用します。
- [Delete]：選択したアクセス グループ エントリをテーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Access Group

[Add Access Group] ダイアログボックスでは、新しいアクセス グループを [Access Group] テーブルに追加できます。[Edit Access Group] ダイアログボックスでは、既存のアクセス グループ エントリの情報を変更できます。既存のエントリを編集する場合、一部のフィールドがブロックされていることがあります。

フィールド

- [Interface]：アクセス グループが関連付けられたインターフェイスを選択します。既存のアクセス グループを編集しているときは、関連インターフェイスは変更できません。
- [Action]：選択したインターフェイスでマルチキャスト グループを許可する場合は [permit] を選択します。選択したインターフェイスからマルチキャスト グループをフィルタリングする場合は、[deny] を選択します。
- [Multicast Group Address]：アクセス グループが適用されるマルチキャスト グループのアドレスを入力します。
- [Netmask]：マルチキャスト グループ アドレスのネットワーク マスクを入力するか、リストから共通ネットワーク マスクをいずれか 1 つ選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Join Group

セキュリティ アプライアンスがマルチキャスト グループのメンバになるように設定できます。[Join Group] ペインには、セキュリティ アプライアンスがメンバになっているマルチキャスト グループが表示されます。

（注）　特定のグループのマルチキャスト パケットを、そのグループに属するセキュリティ アプライアンスに取得されることなく、インターフェイスに転送する場合は、Static Group を参照してください。

フィールド

- [Join Group]：各インターフェイスのマルチキャスト グループ メンバーシップが表示されます。
  - [Interface]：セキュリティ アプライアンス インターフェイスの名前が表示されます。
  - [Multicast Group Address]：インターフェイスが属するマルチキャスト グループのアドレスが表示されます。
- [Add]：[Add/Edit IGMP Join Group] ダイアログボックスが開きます。インターフェイスに新しいマルチキャスト グループ メンバーシップを追加する場合は、このボタンを使用します。
- [Edit]：[Add/Edit IGMP Join Group] ダイアログボックスが開きます。既存のマルチキャスト グループ メンバーシップ エントリを編集する場合は、このボタンを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit IGMP Join Group

インターフェイスをマルチキャスト グループのメンバーに設定する場合は、[Add IGMP Join Group] ダイアログボックスを使用します。既存のメンバーシップ情報を変更する場合は、[Edit IGMP Join Group] ダイアログボックスを使用します。

フィールド

- [Interface]：マルチキャスト グループ メンバーシップを設定するセキュリティ アプライアンス インターフェイスの名前を選択します。既存のエントリを編集しているときは、この値は変更できません。
- [Multicast Group Address]：このフィールドには、マルチキャスト グループのアドレスを入力します。グループ アドレスは、224.0.0.0 ～ 239.255.255.255 の値である必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Protocol

[Protocol] ペインには、セキュリティ アプライアンス上の各インターフェイスの IGMP パラメータが表示されます。

フィールド

- [Protocol]：各インターフェイスに設定された IGMP パラメータが表示されます。このテーブルの行をダブルクリックすると、選択したインターフェイスを対象とした [Configure IGMP Parameters] ダイアログボックスが開きます。
  - [Interface]：インターフェイスの名前が表示されます。
  - [Enabled]：IGMP がインターフェイス上でイネーブルになっている場合は、[Yes] が表示されます。IGMP がインターフェイス上でディセーブルになっている場合は、[No] が表示されます。
  - [Version]：インターフェイス上でイネーブルになっている IGMP のバージョンが表示されます。
  - [Query Interval]：指定したルータから IGMP ホストクエリー メッセージが送信される時間間隔が秒単位で表示されます。
  - [Query Timeout]：インターフェイスのクエリアが停止してから、セキュリティ アプライアンスによりクエリアが引き継がれるまでの時間間隔が秒単位で表示されます。
  - [Response Time]：IGMP クエリーでアドバタイズされる最大応答時間が秒単位で表示されます。この設定への変更内容は、IGMP バージョン 2 に対してだけ有効です。
  - [Group Limit]：インターフェイスで許可される最大グループ数が表示されます。
  - [Forward Interface]：選択したインターフェイスから転送され IGMP ホスト レポートの転送先となるインターフェイスの名前が表示されます。
- [Edit]：選択したインターフェイスを対象とした [Configure IGMP Parameters] ダイアログボックスが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Configure IGMP Parameters

[Configure IGMP Parameters] ダイアログボックスでは、IGMP をディセーブルにし、選択したインターフェイス上の IGMP パラメータを変更できます。

フィールド

- [Name]：設定対象となるインターフェイスの名前が表示されます。このフィールドに表示される情報は変更できません。
- [Enable IGMP]：このチェックボックスをオンにすると、インターフェイスがイネーブルになります。インターフェイスで IGMP をディセーブルにする場合は、このチェックボックスをオフにします。セキュリティ アプライアンスでのマルチキャスト ルーティングをイネーブルにしてある場合、IGMP はデフォルトでイネーブルになっています。
- [Version]：インターフェイスでイネーブルにする IGMP のバージョンを選択します。IGMP バージョン 1 をイネーブルにするには 1 を選択し、IGMP バージョン 2 をイネーブルにするには 2 を選択します。一部の機能では、IGMP バージョン 2 が必要になります。デフォルトの場合、セキュリティ アプライアンスで使用されるのは IGMP バージョン 2 です。
- [Query Interval]：指定したルータから IGMP ホストクエリー メッセージが送信される時間間隔を秒単位で入力します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 125 秒です。
- [Query Timeout]：インターフェイスのクエリアが停止してから、セキュリティ アプライアンスによりクエリアが引き継がれるまでの時間間隔を秒単位で入力します。有効な値の範囲は 60 ～ 300 秒です。デフォルト値は 255 秒です。
- [Response Time]：IGMP クエリーでアドバタイズされる最大応答時間を秒単位で入力します。セキュリティ アプライアンスでは、指定した応答時間内にホスト レポートが受信できない場合、IGMP グループがプルーニングされます。この値を小さくすると、セキュリティ アプライアンスでグループのプルーニングが行われるまでの時間が短くなります。有効な値の範囲は 1 ～ 12 秒です。デフォルト値は 10 秒です。この値の変更は、IGMP Version 2 の場合にだけ有効です。
- [Group Limit]：インターフェイス上で加入する最大ホスト数を入力します。有効な値の範囲は 1 ～ 500 です。デフォルト値は 500 です。
- [Forward Interface]：IGMP ホスト レポートの送信先となるインターフェイスの名前を選択します。ホスト レポートの転送をディセーブルにする場合、[None] を選択します。デフォルトでは、ホスト レポートは転送されません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Static Group

ネットワーク上のホストによっては、IGMP クエリーに応答しないよう設定されていることがあります。しかし、そうしたネットワーク セグメントに対しても、マルチキャスト トラフィックを転送することが必要となる場合もあります。マルチキャスト トラフィックをネットワーク セグメントにプルする方法が 2 つあります。

- [Join Group] ペインで、インターフェイスをマルチキャスト グループのメンバーとして設定します。この方法を使用すると、セキュリティ アプライアンスでは、指定したインターフェイスにマルチキャスト パケットが転送されるだけでなく、そのパケットが取得されます。
- [Static Group] ペインで、セキュリティ アプライアンスを、スタティックに接続されたグループ メンバーとして設定します。この方法を使用した場合、セキュリティ アプライアンスでは、パケットが転送されるだけで、パケット自体は取得されません。そのため、スイッチングが高速に実施されます。発信インターフェイスは IGMP キャッシュに表示されますが、インターフェイス自体はマルチキャスト グループのメンバーではありません。

フィールド

- [Static Group] : 各インターフェイスに対してスタティックに割り当てられたマルチキャスト グループが表示されます。
  - [Interface] : セキュリティ アプライアンス インターフェイスの名前が表示されます。
  - [Multicast Group Address] : インターフェイスに割り当てられたマルチキャスト グループのアドレスが表示されます。
- [Add] : [Add/Edit IGMP Static Group] ダイアログボックスが開きます。インターフェイスに新しいスタティック グループを割り当てる場合は、このボタンを使用します。
- [Edit] : [Add/Edit IGMP Static Group] ダイアログボックスが開きます。既存のスタティック グループ メンバーシップを編集する場合は、このボタンを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit IGMP Static Group

インターフェイスに対してマルチキャスト グループをスタティックに割り当てる場合は、[Add IGMP Static Group] ダイアログボックスを使用します。既存のスタティック グループの割り当てを変更する場合は、[Edit IGMP Static Group] ダイアログボックスを使用します。

フィールド

- [Interface]：マルチキャスト グループを設定するセキュリティ アプライアンス インターフェイスの名前を選択します。既存のエントリを編集しているときは、この値は変更できません。
- [Multicast Group Address]：このフィールドには、マルチキャスト グループのアドレスを入力します。グループ アドレスは、224.0.0.0 ～ 239.255.255.255 の値である必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Multicast Route

スタティック マルチキャスト ルートを定義すると、マルチキャスト トラフィックをユニキャスト トラフィックから分離できます。たとえば、送信元と宛先の間のパスでマルチキャスト ルーティングがサポートされていない場合は、その解決策として、2 つのマルチキャスト デバイスの間に GRE トンネルを設定し、マルチキャスト パケットをそのトンネル経由で送信します。

スタティック マルチキャスト ルートは、セキュリティ アプライアンスに対してローカルであり、アドバタイズまたは再配布されることはありません。

フィールド

- [Multicast Route]：セキュリティ アプライアンスでスタティックに定義されたマルチキャスト ルートが表示されます。テーブルのエントリをダブルクリックすると、そのエントリに対応する [Add/Edit Multicast Route] ダイアログボックスが開きます。
  - [Source Address]：マルチキャスト送信元の IP アドレスとマスクが CIDR 表記で表示されます。
  - [Source Interface]：マルチキャスト ルートの着信インターフェイスが表示されます。
  - [Destination Interface]：マルチキャスト ルートの発信インターフェイスが表示されます。
  - [Admin Distance]：スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスが表示されます。
- [Add]：[Add/Edit Multicast Route] ダイアログボックスが開きます。新しいスタティック ルートを追加する場合は、このボタンを使用します。
- [Edit]：[Add/Edit Multicast Route] ダイアログボックスが開きます。選択したスタティック マルチキャスト ルートを変更する場合は、このボタンを使用します。
- [Delete]：選択したスタティック ルートを削除する場合は、このボタンを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Multicast Route

セキュリティ アプライアンスに新しいスタティック マルチキャスト ルートを追加する場合は、[Add Multicast Route] ダイアログボックスを使用します。既存のスタティック マルチキャスト ルートを変更する場合は、[Edit Multicast Route] ダイアログボックスを使用します。

フィールド

- [Source Address] : マルチキャスト送信元の IP アドレスを入力します。既存のスタティック マルチキャスト ルートを編集しているときは、この値は変更できません。
- [Source Mask] : マルチキャスト送信元の IP アドレスのネットワーク マスクを入力するか、リストから共通マスクを選択します。既存のスタティック マルチキャスト ルートを編集しているときは、この値は変更できません。
- [Source Interface] : マルチキャスト ルートの着信インターフェイスを選択します。
- [Destination Interface] :（任意）マルチキャスト ルートの発信インターフェイスを選択します。宛先インターフェイスを指定した場合、ルートは選択したインターフェイス経由で転送されます。宛先インターフェイスを選択しない場合、ルートの転送には RPF が使用されます。
- [Admin Distance] : スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスを入力します。スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスがユニキャスト ルートのアドミニストレーティブ ディスタンスと同じである場合は、スタティック マルチキャスト ルートが優先されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

MBoundary

[MBoundary] ペインでは、管理用に範囲を定めたマルチキャスト アドレスのマルチキャスト境界を設定できます。マルチキャスト境界により、マルチキャスト データ パケット フローが制限され、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できるようになります。インターフェイスに対してマルチキャスト境界が定義されている場合、フィルタ ACL により許可されたマルチキャスト トラフィックだけが、そのインターフェイスを通過します。

フィールド

[Multicast Boundary] テーブルには、次の情報が表示されます。テーブル エントリをダブルクリックすると、マルチキャスト境界のフィルタ設定を編集できます。

- [Interface]：デバイス上のインターフェイスが一覧表示されます。
- [Boundary Filter]：指定したインターフェイスの境界フィルタ エントリが一覧表示されます。このカラムでは、マルチキャスト境界が定義されていないインターフェイスに対して、「No Boundary Filters Configured」と表示されます。
- [AutoFilter]：Auto-RP メッセージが境界 ACL により拒否されたかどうかが表示されます。[AutoFilter] がイネーブルになっている場合、Auto-RP メッセージのフローも ACL によって制限されます。[AutoFilter] がディセーブルになっている場合は、すべての Auto-RP メッセージがインターフェイスを通過します。デフォルトでは、この機能はディセーブルになっています。

[Boundary] テーブルのエントリに対しては、次のアクションを実行できます。

- [Edit]：[Edit Boundary Filter] ダイアログボックスが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit Boundary Filter

[Edit Boundary Filter] ダイアログボックスには、マルチキャスト境界フィルタ ACL が表示されます。このダイアログボックスを使用すれば、境界フィルタ ACL エントリを追加したり削除したりできます。

境界フィルタのコンフィギュレーションがセキュリティ アプライアンスに適用されると、実行コンフィギュレーションには、*interface-name*_multicast という名前の ACL が表示されます。ただし、*interface-name* は、マルチキャスト境界フィルタが適用されるインターフェイスの名前です。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。

フィールド

- [Interface]：マルチキャスト境界フィルタ ACL を設定しているインターフェイスが表示されます。
- [Remove any Auto-RP group range]：境界 ACL により拒否された送信元からの Auto-RP メッセージをフィルタリングする場合は、このチェックボックスをオンにします。チェックボックスをオフにすると、すべての Auto-RP メッセージが通過します。

[Boundary Filter] テーブルには、次の情報が表示されます。

- [Action] : フィルタ エントリのアクションが表示されます。[Permit] が表示されている場合は、指定したトラフィックの通過が許可されます。[Deny] が表示されている場合は、指定したトラフィックによるインターフェイスの通過が拒否されます。インターフェイスに対してマルチキャスト境界フィルタが設定されている場合、デフォルトでは、マルチキャスト トラフィックは拒否されます。
- [Network Address] : 許可されるまたは拒否されるグループのマルチキャスト グループ アドレスが表示されます。
- [Netmask] : マルチキャスト グループ アドレスに適用されるネットワーク マスクが表示されます。

[Boundary Filter] テーブルに対しては、次のアクションを実行できます。

- [Insert] : 選択したエントリの前にネイバー フィルタ エントリを挿入します。
- [Add] : 選択したエントリの後ろにネイバー フィルタ エントリを追加します。
- [Edit] : 選択した境界フィルタを編集します。
- [Delete] : 選択したネイバー フィルタ エントリを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit/Insert Neighbor Filter Entry

[Add/Edit/Insert Neighbor Filter Entry] ダイアログボックスでは、マルチキャスト境界 ACL の ACL エントリを作成できます。

フィールド

- [Action] : ネイバー フィルタ ACL エントリに対して [Permit] または [Deny] を選択します。[Permit] を選択すると、インターフェイスを介したマルチキャスト グループのアドバタイズメントが許可されます。[Deny] を選択すると、指定したマルチキャスト グループ アドバタイズメントによるインターフェイスの通過が拒否されます。インターフェイスに対してマルチキャスト境界を設定すると、ネイバー フィルタ エントリで許可されていない限り、すべてのマルチキャスト トラフィックが、インターフェイスの通過を拒否されます。
- [Multicast Group Address] : 許可されるまたは拒否されるマルチキャスト グループのアドレスを入力します。有効なグループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。
- [Netmask] : マルチキャスト グループ アドレスのネットマスクを入力または選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

MForwarding

[MForwarding] ペインでは、インターフェイスごとにマルチキャスト転送をディセーブル化および再イネーブル化できます。デフォルトでは、すべてのインターフェイスでマルチキャスト転送がイネーブルになっています。

マルチキャスト転送がディセーブルになっているインターフェイスでは、他の方法で特に設定されていない限り、マルチキャスト パケットは取得されません。また、マルチキャスト転送がディセーブルになっている場合は、IGMP パケットも拒否されます。

フィールド

- [Multicast Forwarding] テーブルには、次の情報が表示されます。
  - [Interface] : セキュリティ アプライアンスで設定済みのインターフェイスが表示されます。インターフェイスを選択する場合は、そのインターフェイス名をクリックします。インターフェイス名をダブルクリックすると、インターフェイスの [Multicast Forwarding Enabled] ステータスが切り替わります。
  - [Multicast Forwarding Enabled] : 指定したインターフェイスでマルチキャスト転送がイネーブルになっている場合は [Yes] が表示されます。指定したインターフェイスでマルチキャスト転送がディセーブルになっている場合は [No] が表示されます。このエントリをダブルクリックすると、選択したインターフェイスについて、[Yes] と [No] が切り替わります。
- [Enable] : 選択したインターフェイスでのマルチキャスト転送をイネーブルにします。
- [Disable] : 選択したインターフェイスでのマルチキャスト転送をディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

- 「マルチキャスト ルーティングの設定」（P.17-1）

PIM

ルータでは、マルチキャスト データグラムの転送に使用する転送テーブルが、PIM を使用して管理されます。

セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにすると、すべてのインターフェイスでは PIM がデフォルトでイネーブルになります。インターフェイスごとに PIM をディセーブルにできます。

PIM の設定に関する詳細については、次の各項目を参照してください。

- Protocol
- 「Neighbor Filter」（P.17-14）
- 「Bidirectional Neighbor Filter」（P.17-16）
- Rendezvous Points
- Route Tree
- Request Filter

Protocol

[Protocol] ペインには、インターフェイス固有の PIM プロパティが表示されます。

フィールド

- [Protocol]：各インターフェイスの PIM 設定が表示されます。テーブルのエントリをダブルクリックすると、そのエントリに対応する [Edit PIM Protocol] ダイアログボックスが開きます。
  - [Interface]：セキュリティ アプライアンス インターフェイスの名前が表示されます。
  - [PIM Enabled]：インターフェイスで PIM がイネーブルになっている場合は [Yes] が、イネーブルになっていない場合は [No] がそれぞれ表示されます。
  - [DR Priority]：インターフェイスの優先度が表示されます。
  - [Hello Interval]：インターフェイスから PIM hello メッセージが送信される時間間隔が、秒単位で表示されます。
  - [Join-Prune Interval]：インターフェイスから PIM の加入アドバタイズメントおよびプルーニング アドバタイズメントが送信される時間間隔が、秒単位で表示されます。
- [Edit]：選択したエントリに対応する [Edit PIM Protocol] ダイアログボックスが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit PIM Protocol

[Edit PIM Protocol] ダイアログボックスでは、選択したインターフェイスの PIM プロパティを変更できます。

フィールド

- [Interface]：*表示専用*。選択したインターフェイスの名前が表示されます。この値は編集できません。
- [PIM Enabled]：このチェックボックスをオンにすると、選択したインターフェイスで PIM をイネーブルにできます。選択したインターフェイスで PIM をディセーブルにする場合は、このチェックボックスをオフにします。
- [DR Priority]：選択したインターフェイスに対して指定ルータ優先度を設定します。サブネットで DR プライオリティが最も高いルータが指定ルータになります。有効な値の範囲は 0 ～ 4294967294 です。デフォルトの DR プライオリティは 1 です。この値を 0 に設定した場合は、そのセキュリティ アプライアンス インターフェイスがデフォルトのルータになることはありません。
- [Hello Interval]：インターフェイスから PIM hello メッセージが送信される時間間隔を秒単位で入力します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 30 秒です。
- [Join-Prune Interval]：インターフェイスから PIM の加入アドバタイズメントおよびプルーニング アドバタイズメントが送信される時間間隔を秒単位で入力します。有効な値の範囲は、10 ～ 600 秒です。デフォルト値は 60 秒です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Neighbor Filter

セキュリティ アプライアンスで設定された PIM ネイバー フィルタがもしあれば、[Neighbor Filter] ペインには、その PIM ネイバー フィルタが表示されます。PIM ネイバー フィルタは、PIM に参加できるネイバー デバイスを定義する ACL です。インターフェイスのネイバー フィルタが設定されていない場合、制限はありません。PIM ネイバー フィルタが設定されている場合、フィルタ リストで許可されるネイバーだけがセキュリティ アプライアンスでの PIM に参加できます。

PIM ネイバー フィルタのコンフィギュレーションがセキュリティ アプライアンスに適用されると、実行コンフィギュレーションには、*interface-name*_multicast という名前の ACL が表示されます。ただし *interface-name* は、マルチキャスト境界フィルタが適用されるインターフェイスの名前です。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。この ACL により、どのデバイスがセキュリティ アプライアンスの PIM ネイバーになれるか定義されます。

フィールド

[PIM Neighbor Filter] テーブルには、次の情報が表示されます。テーブルのエントリをダブルクリックすると、選択したエントリに対応する [Edit Neighbor Filter Entry] ダイアログボックスが開きます。

- [Interface]：PIM ネイバー フィルタ エントリが適用されるインターフェイスの名前が表示されます。
- [Action]：指定したネイバーが PIM への参加を許可される場合は、[Permit] が表示されます。指定したネイバーが PIM への参加を拒否される場合は、[Deny] が表示されます。
- [Network Address]：許可または拒否されるネイバーのネットワーク アドレスが表示されます。
- [Netmask]：[Network Address] に表示されるアドレスとともに使用するネットワーク マスクが表示されます。

次の操作を実行できます。

- [Insert]：選択したエントリの前にネイバー フィルタ エントリを挿入します。
- [Add]：選択したエントリの後ろにネイバー フィルタ エントリを追加します。
- [Edit]：選択したネイバー フィルタ エントリを編集できます。
- [Delete]：選択したネイバー フィルタ エントリを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

「Add/Edit/Insert Neighbor Filter Entry」（P.17-15）

Add/Edit/Insert Neighbor Filter Entry

[Add/Edit/Insert Neighbor Filter Entry] では、PIM ネイバー フィルタ ACL の ACL エントリを作成できます。

フィールド

- [Interface]：PIM ネイバー フィルタ エントリが適用されるインターフェイスの名前をリストから選択します。
- [Action]：[Permit] を選択すると、指定したネイバーが PIM へ参加を許可されます。[Deny] を選択すると、指定したネイバーは PIM への参加を拒否されます。
- [Network Address]：許可または拒否されるネイバーのネットワーク アドレスが表示されます。
- [Netmask]：[Network Address] に表示されるアドレスとともに使用するネットワーク マスクが表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Bidirectional Neighbor Filter

セキュリティ アプライアンスに PIM 双方向ネイバー フィルタが設定されている場合、[Bidirectional Neighbor Filter] ペインにそれらのフィルタが表示されます。PIM 双方向ネイバー フィルタは、DF 選定に参加できるネイバー デバイスを定義する ACL です。PIM 双方向ネイバー フィルタがインターフェイスに設定されていなければ、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合は、ACL で許可されるネイバーだけが DF 選択プロセスに参加できます。

PIM 双方向ネイバー フィルタのコンフィギュレーションがセキュリティ アプライアンスに適用されると、実行中のコンフィギュレーションには、*interface-name*_multicast という名前の ACL が表示されます。ただし *interface-name* は、マルチキャスト境界フィルタが適用されるインターフェイスの名前です。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。この ACL により、どのデバイスがセキュリティ アプライアンスの PIM ネイバーになれるか定義されます。

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。双方向で DF を選定するために、セグメント内のすべてのマルチキャスト ルータが双方向でイネーブルになっている必要があります。

PIM 双方向ネイバー フィルタでは、すべてのルータがスパース モード ドメインに参加できるようにしたまま、DF 選定に参加するルータを指定できるので、スパース モード専用ネットワークから双方向ネットワークへの移行が可能になります。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方向グループから PIM メッセージやデータが双方向サブセット クラウドに出入りできないようにします。

PIM 双方向ネイバー フィルタがイネーブルになると、ACL により許可されるルータは双方向機能があると見なされます。したがって、次のようにします。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

フィールド

[PIM Bidirectional Neighbor Filter] テーブルには、次のエントリが含まれます。エントリをダブルクリックして、そのエントリの [Edit Bidirectional Neighbor Filter Entry] ダイアログボックスを開きます。

- [Interface]：双方向ネイバー フィルタが適用されるインターフェイスが表示されます。
- [Action]：双方向ネイバー フィルタにより DF 選定プロセスへの参加が許可される場合は、[Permit] が表示されます。そのエントリで、指定したアドレスが DF 選定プロセスへの参加を拒否される場合は、[Deny] が表示されます。
- [Network Address]：許可または拒否されているアドレスが表示されます。
- [Netmask]：[Network Address] に適用されるネットワーク マスクが表示されます。

次の操作を実行できます。

- [Insert]：選択したエントリの前に双方向ネイバー フィルタ エントリを挿入します。
- [Add]：選択したエントリの後ろに双方向ネイバー フィルタ エントリを追加します。
- [Edit]：選択した双方向ネイバー フィルタ エントリを編集できます。
- [Delete]：選択した双方向ネイバー フィルタ エントリを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

「Add/Edit/Insert Bidirectional Neighbor Filter Entry」（P.17-17）

Add/Edit/Insert Bidirectional Neighbor Filter Entry

[Add/Edit/Insert Bidirectional Neighbor Filter Entry] ダイアログボックスでは、PIM 双方向ネイバー フィルタ ACL の ACL エントリを作成できます。

フィールド

- [Interface]：PIM 双方向ネイバー フィルタ ACL エントリを設定するインターフェイスを選択します。
- [Action]：指定したデバイスが DF 選定への参加を許可される場合は、[Permit] を選択します。指定したデバイスが DF 選定への参加を拒否される場合は、[Deny] を選択します。
- [Network Address]：許可または拒否されるネイバーのネットワーク アドレスが表示されます。
- [Netmask]：[Network Address] に表示されるアドレスとともに使用するネットワーク マスクが表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Rendezvous Points

PIM を設定する場合は、RP として動作するルータを 1 つ以上選択する必要があります。RP は、共有配布ツリーの唯一かつ共通のルートで、各ルータではスタティックに設定されます。第 1 ホップ ルータは、RP を使用して、送信元のマルチキャスト ホストに代わって登録パケットを送信します。

複数のグループにサービスを提供するように単一の RP を設定できます。特定のグループを指定していない場合、そのグループの RP は IP マルチキャスト グループ範囲（224.0.0.0/4）全体に適用されます。

複数の RP を設定できますが、同じ RP に複数のエントリは設定できません。

フィールド

- [Generate IOS compatible register messages]：RP が Cisco IOS ルータの場合は、このチェックボックスをオンにします。セキュリティ アプライアンス ソフトウェアでは、Cisco IOS ソフトウェア方式（すべての PIM メッセージ タイプの PIM メッセージ全体のチェックサムとともに登録メッセージを受け取る方法）によってではなく、PIM ヘッダーにあるチェックサムとそれに続く 4 バイトと共に登録メッセージを受け取ります。
- [Rendezvous Points]：セキュリティ アプライアンスで設定された RP が表示されます。
  - [Rendezvous Point]：RP の IP アドレスが表示されます。
  - [Multicast Groups]：RP に関連付けられたマルチキャスト グループが表示されます。RP がインターフェイス上のすべてのマルチキャスト グループに関連付けられている場合は、[--All Groups--] が表示されます。
  - [Bi-directional]：指定したマルチキャスト グループが双方向モードで動作する場合は、[Yes] が表示されます。指定したグループがスパース モードで動作する場合は、[No] が表示されます。
- [Add]：[Add/Edit Rendezvous Point] ダイアログボックスが開きます。新しい RP エントリを追加する場合は、このボタンを使用します。
- [Edit]：[Add/Edit Rendezvous Point] ダイアログボックスが開きます。既存の RP エントリを変更する場合は、このボタンを使用します。
- [Delete]：選択した RP エントリを [Rendezvous Point] テーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Rendezvous Point

[Add Rendezvous Point] ダイアログボックスでは、新しいエントリを [Rendezvous Point] テーブルに追加できます。[Edit Rendezvous Point] ダイアログボックスでは、既存の RP エントリを変更できます。

制約事項

- 同じ RP アドレスは、2 度使用できません。

- 複数の RP に対しては、[All Groups] を指定できません。

フィールド

- [Rendezvous Point IP Address] : RP の IP アドレスを入力します。これはユニキャスト アドレスです。既存の RP エントリを編集しているときは、この値は変更できません。
- [Use bi-directional forwarding] : 指定したマルチキャスト グループを双方向モードで動作させる場合は、このチェックボックスをオンにします。双方向モードでは、直接接続されたメンバーまたは PIM ネイバーが存在しない場合、マルチキャスト パケットを受信したセキュリティ アプライアンスから送信元にプルーニング メッセージが戻されます。指定したマルチキャスト グループをスパース モードで動作させる場合は、このチェックボックスをオフにします。

（注） セキュリティ アプライアンスは、実際の双方向コンフィギュレーションとは関係なく、常に双方向機能を PIM hello メッセージ内でアドバタイズします。

- [Use this RP for All Multicast Groups] : 指定した RP をインターフェイス上のすべてのマルチキャスト グループに対して使用する場合は、このオプションを選択します。
- [Use this RP for the Multicast Groups as specified below] : 指定した RP をマルチキャスト グループで使用するように指定する場合は、このオプションを選択します。
- [Multicast Groups] : 指定した RP に関連付けられたマルチキャスト グループが表示されます。

  テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャスト グループを含みながら、その範囲の中から特定のグループが除外されるような RP エントリを作成する場合は、除外する特定のグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャスト グループ全体に対する許可ルールを deny 文の下に配置します。

  エントリをダブルクリックすると、選択したエントリに対応する [Multicast Group] ダイアログボックスが開きます。

  - [Action] : マルチキャスト グループが含まれる場合は [Permit] が、マルチキャスト グループが除外される場合は [Deny] がそれぞれ表示されます。
  - [Multicast Group Address] : マルチキャスト グループのアドレスが表示されます。
  - [Netmask] : マルチキャスト グループ アドレスのネットワーク マスクが表示されます。
- [Insert Before] : [Multicast Group] ダイアログボックスが開きます。テーブルで選択したエントリの前に新しいマルチキャスト グループ エントリを追加する場合は、このボタンを使用します。
- [Insert After] : [Multicast Group] ダイアログボックスが開きます。テーブルで選択したエントリの後ろに新しいマルチキャスト グループ エントリを追加する場合は、このボタンを使用します。
- [Add] : [Multicast Group] ダイアログボックスが開きます。テーブルの最後尾に新しいマルチキャスト グループ エントリを追加する場合は、このボタンを使用します。
- [Edit] : [Multicast Group] ダイアログボックスが開きます。選択したマルチキャスト グループ エントリの情報を変更する場合は、このボタンを使用します。
- [Delete] : 選択したマルチキャスト グループ エントリをテーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Multicast Group

マルチキャスト グループとは、どのマルチキャスト アドレスがグループの一部であるかを定義するアクセス ルールのリストです。1 つのマルチキャスト グループには、単独のマルチキャスト アドレスまたはある範囲に属する複数のマルチキャスト アドレスを含めることができます。新しいマルチキャスト グループ ルールを作成する場合は、[Add Multicast Group] ダイアログボックスを使用します。既存のマルチキャスト グループ ルールを修正する場合は、[Edit Multicast Group] ダイアログボックスを使用します。

フィールド

- [Action]:指定したマルチキャスト アドレスを許可するグループ ルールを作成する場合は [Permit] を、指定したマルチキャスト アドレスをフィルタリングするグループ ルールを作成する場合は [Deny] をそれぞれ選択します。
- [Multicast Group Address]：グループに関連付けられたマルチキャスト アドレスを入力します。
- [Netmask]：マルチキャスト グループ アドレスのネットワーク マスクを入力または選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Request Filter

セキュリティ アプライアンスが RP として動作している場合、特定のマルチキャスト ソースをそれに登録できないように制限できます。これにより、未許可の送信元が RP に登録されることを回避できます。[Request Filter] ペインでは、セキュリティ アプライアンスで PIM 登録メッセージが受け入れられるマルチキャスト ソースを定義できます。

フィールド

- [Multicast Groups]：要求フィルタ アクセス ルールが表示されます。

  テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャスト グループを含みながら、その範囲の中から特定のグループが除外されるようなエントリを作成する場合は、除外する特定のグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャスト グループ全体に対する許可ルールを deny 文の下に配置します。

エントリをダブルクリックすると、選択したエントリに対応する [Request Filter Entry] ダイアログボックスが開きます。

  - [Action]：マルチキャストの送信元による登録が許可される場合は [Permit] が、マルチキャストの送信元が除外される場合は [Deny] がそれぞれ表示されます。
  - [Source]：登録メッセージの送信元のアドレスが表示されます。
  - [Destination]：マルチキャストの宛先アドレスが表示されます。

- [Insert Before]：[Request Filter Entry] ダイアログボックスが開きます。テーブルで選択したエントリの前に新しいマルチキャスト グループ エントリを追加する場合は、このボタンを使用します。
- [Insert After]：[Request Filter Entry] ダイアログボックスが開きます。テーブルで選択したエントリの後ろに新しいマルチキャスト グループ エントリを追加する場合は、このボタンを使用します。
- [Add]：[Request Filter Entry] ダイアログボックスが開きます。テーブルの最後尾に新しいマルチキャスト グループ エントリを追加する場合は、このボタンを使用します。
- [Edit]：[Request Filter Entry] ダイアログボックスが開きます。選択したマルチキャスト グループ エントリの情報を変更する場合は、このボタンを使用します。
- [Delete]：選択したマルチキャスト グループ エントリをテーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Request Filter Entry

[Request Filter Entry] ダイアログボックスでは、セキュリティ アプライアンスが RP として動作する場合に、セキュリティ アプライアンスに登録できるマルチキャスト送信元を定義できます。送信元 IP アドレスおよび宛先マルチキャスト アドレスに基づいて、フィルタ ルールを作成します。

フィールド

- [Action]：指定したマルチキャスト トラフィックの指定送信元によるセキュリティ アプライアンスへの登録を許可するルールを作成する場合は [Permit] を、指定したマルチキャスト トラフィックの指定送信元によるセキュリティ アプライアンスへの登録を許可しないルールを作成する場合は [Deny] をそれぞれ選択します。
- [Source IP Address]：登録メッセージの送信元の IP アドレスを入力します。
- [Source Netmask]：登録メッセージの送信元のネットワーク マスクを入力または選択します。
- [Destination IP Address]：マルチキャスト宛先アドレスを入力します。
- [Destination Netmask]：マルチキャスト宛先アドレスのネットワーク マスクを入力または選択します。

モード

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Route Tree

デフォルトでは、PIM リーフ ルータは、新しい送信元から最初のパケットが到着した直後に、最短パス ツリーに加入します。これにより、遅延が短縮されます。ただし、共有ツリーよりも多くのメモリが必要になります。

すべてのマルチキャスト グループ、または特定のマルチキャスト アドレスに対して、セキュリティ アプライアンスが最短パス ツリーに加入するか、共有ツリーを使用するかを設定できます。

フィールド

- [Use Shortest Path Tree for All Groups] : すべてのマルチキャスト グループに最短パス ツリーを使用する場合は、このオプションを選択します。
- [Use Shared Tree for All Groups] : すべてのマルチキャスト グループに共有ツリーを使用する場合は、このオプションを選択します。
- [Use Shared Tree for the Groups specified below] : [Multicast Groups] テーブルで指定したグループに共有ツリーを使用する場合は、このオプションを選択します。[Multicast Groups] テーブルで指定されていないグループには最短パス ツリーが使用されます。
- [Multicast Groups] : 共有ツリーを使用するマルチキャスト グループが表示されます。

  テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャスト グループを含みながら、その範囲の中から特定のグループが除外されるようなエントリを作成する場合は、除外する特定のグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャスト グループ全体に対する許可ルールを deny 文の下に配置します。

  エントリをダブルクリックすると、選択したエントリに対応する [Multicast Group] ダイアログボックスが開きます。

  - [Action] : マルチキャスト グループが含まれる場合は [Permit] が、マルチキャスト グループが除外される場合は [Deny] がそれぞれ表示されます。
  - [Multicast Group Address] : マルチキャスト グループのアドレスが表示されます。
  - [Netmask] : マルチキャスト グループ アドレスのネットワーク マスクが表示されます。
- [Insert Before] : [Multicast Group] ダイアログボックスが開きます。テーブルで選択したエントリの前に新しいマルチキャスト グループ エントリを追加する場合は、このボタンを使用します。
- [Insert After] : [Multicast Group] ダイアログボックスが開きます。テーブルで選択したエントリの後ろに新しいマルチキャスト グループ エントリを追加する場合は、このボタンを使用します。
- [Add] : [Multicast Group] ダイアログボックスが開きます。テーブルの最後尾に新しいマルチキャスト グループ エントリを追加する場合は、このボタンを使用します。
- [Edit] : [Multicast Group] ダイアログボックスが開きます。選択したマルチキャスト グループ エントリの情報を変更する場合は、このボタンを使用します。
- [Delete] : 選択したマルチキャスト グループ エントリをテーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

CHAPTER 18

ファイアウォール モードの概要

この章では、各ファイアウォール モードでファイアウォールがどのように機能するかを説明します。CLI でモードを設定するには、「CLI によるトランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モードの設定」（P.3-5）を参照してください。

（注） マルチ コンテキスト モードでは、コンテキストごとに個別にファイアウォール モードを設定できません。ファイアウォール モードはセキュリティ アプライアンス全体に対してだけ設定できます。

この章は、次の項で構成されています。

ルーテッド モードの概要

ルーテッド モードでは、セキュリティ アプライアンスはネットワーク内のルータ ホップと見なされます。OSPF または RIP を使用できます（シングル コンテキスト モードの場合）。ルーテッド モードは多数のインターフェイスをサポートしています。インターフェイスはそれぞれ異なるサブネット上に置かれます。コンテキスト間でインターフェイスを共有することもできます。

この項では、次のトピックについて取り上げます。

IP ルーティング サポート

セキュリティ アプライアンスは、接続されたネットワーク間のルータとして機能します。インターフェイスごとに、異なるサブネット上の IP アドレスが必要です。シングルコンテキスト モードでは、ルーテッド ファイアウォールは OSPF および RIP をサポートします。マルチ コンテキスト モードでは、スタティック ルートだけがサポートされます。過度なルーティングのニーズをセキュリティ アプライアンスに頼るのではなく、アップストリーム ルータとダウンストリーム ルータの拡張ルーティング機能を使用することをお勧めします。

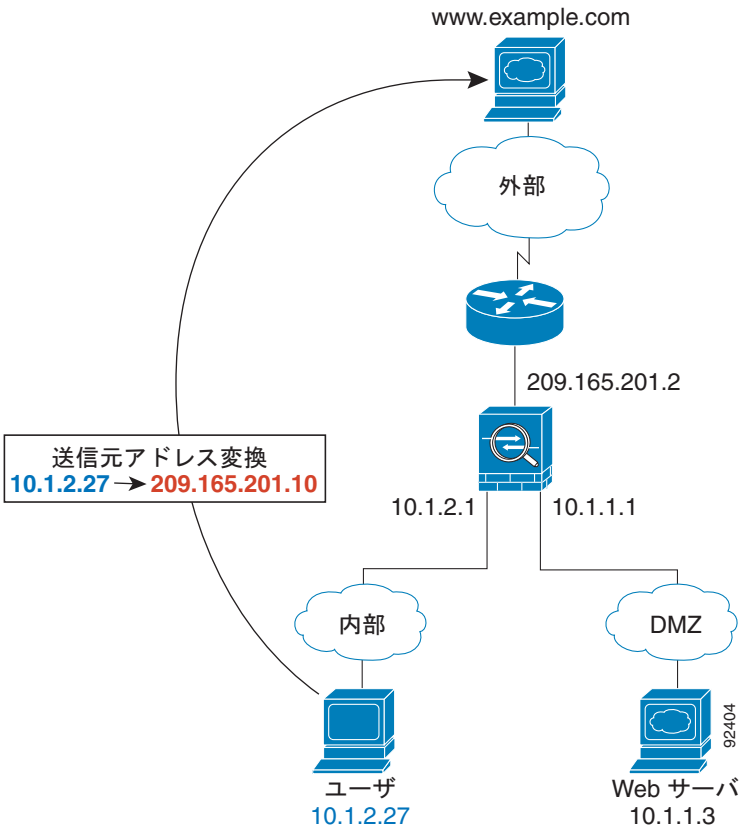
ルーテッド ファイアウォール モードでデータがセキュリティ アプライアンスを通過する方法

ここでは、ルーテッド ファイアウォール モードにおいて、データが セキュリティ アプライアンス をどのように通過するかについて説明します。内容は次のとおりです。

内部ユーザが Web サーバにアクセスする

図 18-1 は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 18-1　　内部から外部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 18-1 を参照）。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。

2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、コンテキストに関連付けられる固有なインターフェイスまたは固有な宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストでのアドレス変換と照合することによって関連付けられます。この場合、インターフェイスは固有です。www.example.com IP アドレスは、コンテキスト内に最新のアドレス変換を持っていません。

3. セキュリティ アプライアンスは、ローカル送信元アドレス（10.1.2.27）を、外部インターフェイス サブネット上のグローバル アドレス 209.165.201.10 に変換します。

   グローバル アドレスは任意のサブネット上に置くことができますが、外部インターフェイス サブネットに置くとルーティングが簡素化されます。

4. 次に、セキュリティ アプライアンスはセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。

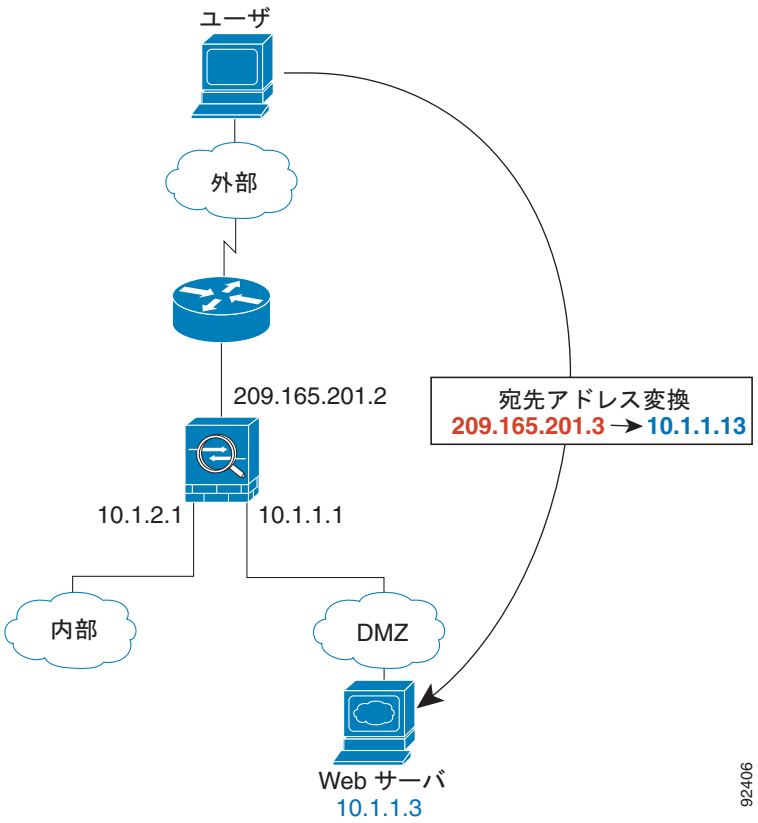
5. www.example.com が要求に応答すると、パケットはセキュリティ アプライアンスを通過します。これはすでに確立されているセッションであるため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。セキュリティ アプライアンスは、グローバル宛先アドレスをローカル ユーザ アドレス 10.1.2.27 に変換することによって、NAT を実行します。

6. セキュリティ アプライアンスは、パケットを内部ユーザに転送します。

外部ユーザが DMZ 上の Web サーバにアクセスする

図 18-2 は、外部ユーザが DMZ Web サーバにアクセスしていることを示しています。

図 18-2　外部から DMZ へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 18-2 を参照）。

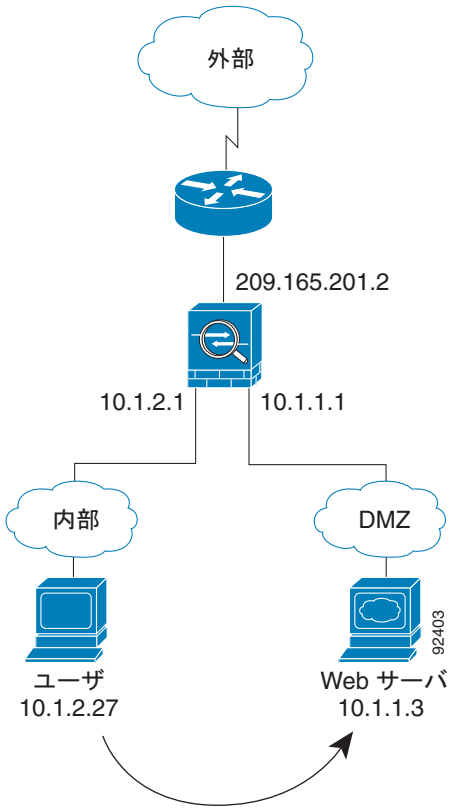
1. 外部ネットワーク上のユーザは、外部インターフェイス サブネット上にあるグローバル宛先アドレス 209.165.201.3 を使用して DMZ Web サーバから Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、コンテキストに関連付けられる固有なインターフェイスまたは固有な宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストでのアドレス変換と照合することによって関連付けられます。この場合、分類子は DMZ Web サーバ アドレスがサーバ アドレス変換のため特定のコンテキストに属すことを「認識」しています。
3. セキュリティ アプライアンスは、宛先アドレスをローカル アドレス 10.1.1.3 に変換します。
4. 次に、セキュリティ アプライアンスはセッション エントリを高速パスに追加し、DMZ インターフェイスからパケットを転送します。
5. DMZ Web サーバが要求に応答すると、パケットはセキュリティ アプライアンスを通過します。また、セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。セキュリティ アプライアンスは、ローカル送信元アドレスを 209.165.201.3 に変換することによって、NAT を実行します。
6. セキュリティ アプライアンスは、パケットを外部ユーザに転送します。

内部ユーザが DMZ 上の Web サーバにアクセスする

図 18-3 は、内部ユーザが DMZ Web サーバにアクセスしていることを示しています。

図 18-3　　内部から DMZ へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 18-3 を参照）。

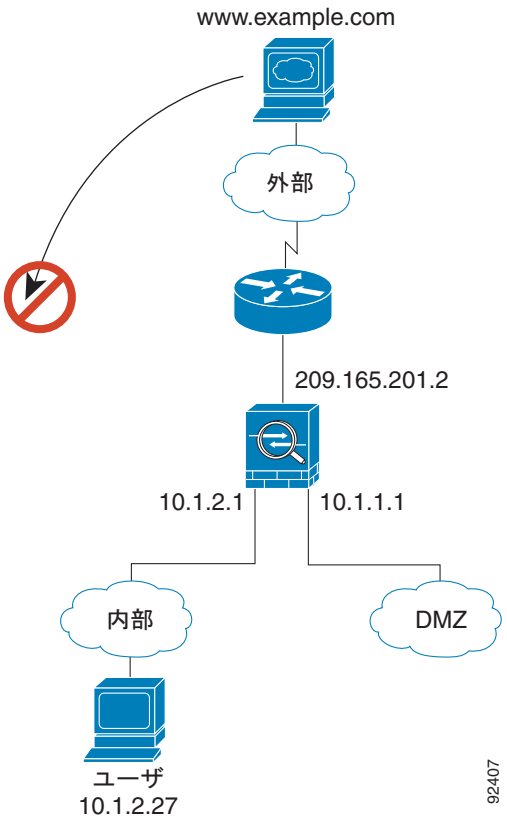
1. 内部ネットワーク上のユーザは、宛先アドレス 10.1.1.3 を使用して DMZ Web サーバから Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、コンテキストに関連付けられる固有なインターフェイスまたは固有な宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストでのアドレス変換と照合することによって関連付けられます。この場合、インターフェイスは固有です。Web サーバ IP アドレスは、最新のアドレス変換を持っていません。
3. 次に、セキュリティ アプライアンスはセッションが確立されたことを記録し、DMZ インターフェイスからパケットを転送します。
4. DMZ Web サーバが要求に応答すると、パケットは高速パスを通過します。これのため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
5. セキュリティ アプライアンスは、パケットを内部ユーザに転送します。

外部ユーザが内部ホストにアクセスしようとする

図 18-4 は、外部ユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 18-4　　外部から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 18-4 を参照）。

1. 外部ネットワーク上のユーザが、内部ホストに到達しようとします（ホストにルーティング可能な IP アドレスがあると想定します）。

   内部ネットワークがプライベート アドレスを使用している場合、外部ユーザが NAT なしで内部ネットワークに到達することはできません。外部ユーザは既存の NAT セッションを使用して内部ユーザに到達しようとすることが考えられます。

2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）に従って、パケットが許可されているかどうかを確認します。

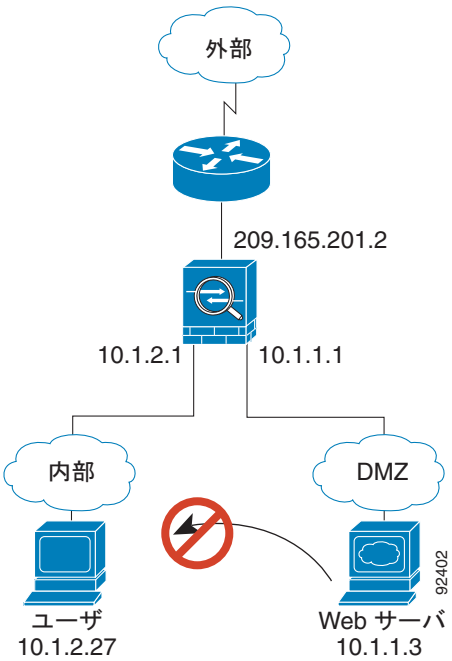
3. パケットが拒否され、セキュリティ アプライアンスはパケットをドロップし、接続試行をログに記録します。

   外部ユーザが内部ネットワークを攻撃しようとした場合、セキュリティ アプライアンスは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

DMZ ユーザが内部ホストにアクセスしようとする

図 18-5 は、DMZ 内のユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 18-5　　DMZ から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 18-5 を参照）。

1. DMZ ネットワーク上のユーザが、内部ホストに到達しようとします。DMZ はインターネット上のトラフィックをルーティングする必要がないので、プライベート アドレッシング方式はルーティングを回避しません。
2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）に従って、パケットが許可されているかどうかを確認します。
3. パケットが拒否され、セキュリティ アプライアンスはパケットをドロップし、接続試行をログに記録します。

トランスペアレント モードの概要

従来、ファイアウォールはルーテッド ホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとは見なされません。

ここでは、トランスペアレント ファイアウォール モードについて次の項目で説明します。

- 「トランスペアレント ファイアウォール ネットワーク」（P.18-8）
- 「レイヤ 3 トラフィックの許可」（P.18-8）

トランスペアレント ファイアウォール ネットワーク

セキュリティ アプライアンスでは、内部インターフェイスと外部インターフェイスに同じネットワークが接続されます。トランスペアレント ファイアウォールはルーティングされたホップではないので、既存のネットワークに簡単に導入できます。

レイヤ 3 トラフィックの許可

セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへの IPv4 トラフィックは、アクセス リストとは無関係に、トランスペアレント ファイアウォールを自動的に通過できます。ARP は、アクセス リストに関係なく、両方向ともトランスペアレント ファイアウォールを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。低いセキュリティ インターフェイスから高いセキュリティ インターフェイスに移動するレイヤ 3 トラフィックの場合は、拡張アクセス リストが必要です。

許可される MAC アドレス

次の宛先 MAC アドレスは、トランスペアレント ファイアウォールを通過できます。このリストに存在しない MAC アドレスはドロップされません。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ～ 0100.5EFE.FFFF までの IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ～ 3333.FFFF.FFFF までの IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD の BPDU マルチキャスト アドレス
- 0900.0700.0000 ～ 0900.07FF.FFFF までの AppleTalk マルチキャスト MAC アドレス

ルーテッド モードで許可されないトラフィックの通過

ルーテッド モードでは、アクセス リストで許可しても、いくつかのタイプのトラフィックはセキュリティ アプライアンスを通過できません。ただし、トランスペアレント ファイアウォールは、拡張アクセス リスト（IP トラフィックの場合）または EtherType アクセス リスト（非 IP トラフィックの場合）を使用してほとんどすべてのトラフィックを許可できます。

（注）　トランスペアレント モードのセキュリティ アプライアンスは、CDP パケット、IPv6 パケット、および 0x600 以上の有効な EtherType を持たないパケットの通過を拒否します。たとえば、IS-IS パケットは通過できません。例外として、BPDU はサポートされています。

たとえば、トランスペアレント ファイアウォールでルーティング プロトコルの隣接関係を確立できます。つまり、拡張アクセス リストに基づいて、OSPF、RIP、EIGRP、または BGP トラフィックを許可できます。同様に、protocols like HSRP や VRRP などのプロトコルは セキュリティ アプライアンスを通過できます。

IP 以外のトラフィック（AppleTalk、IPX、BPDU、および MPLS など）は、EtherType アクセス リストを使用して通過するように構成できます。

トランスペアレント ファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、拡張アクセス リストを使用して、DHCP トラフィック（サポートされない DHCP リレー機能の代わりに）または IP/TV によって作成されたマルチキャスト トラフィックを許可できます。

MAC アドレス ルックアップと ルート ルックアップ

セキュリティ アプライアンス が NAT を使用せずにトランスペアレント モードで稼働している場合、パケットの発信インターフェイスはルート検索ではなく、MAC アドレス検索を実行することによって判別されます。ルート ステートメントも設定できますが、適用されるのは セキュリティ アプライアンス を起点とするトラフィックだけです。たとえば、Syslog サーバがリモート ネットワークに配置されている場合、セキュリティ アプライアンス がそのサブネットにアクセスできるように、スタティック ルートを使用する必要があります。

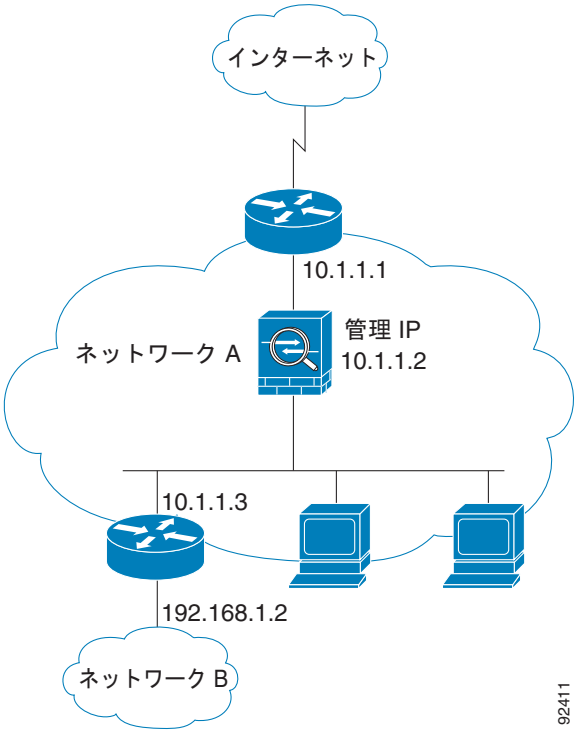
ただし、音声検査を使用しており、エンドポイントが セキュリティ アプライアンス から 1 ホップ以上離れている場合は例外です。たとえば、CCM と H.323 ゲートウェイ間でトランスペアレント ファイアウォールを使用しており、トランスペアレント ファイアウォールと H.323 ゲートウェイ間にルータが存在する場合、H.323 ゲートウェイが正常にコールを完了できるようにするには、セキュリティ アプライアンス でスタティック ルートを追加する必要があります。

NAT を使用する場合は、セキュリティ アプライアンス で MAC アドレス検索の代わりにルート検索が使用されます。場合によっては、スタティック ルートが必要になります。たとえば、実宛先アドレスが セキュリティ アプライアンス に直接接続されていない場合、セキュリティ アプライアンス でその実宛先アドレス用に、ダウンストリーム ルータをポイントするスタティック ルートを追加する必要があります。

ネットワークでのトランスペアレント ファイアウォールの使用

図 18-6 に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレント ファイアウォール ネットワークを示します。内部ルータとホストは、外部ルータに直接接続されているように見えます。

図 18-6　トランスペアレント ファイアウォール ネットワーク



トランスペアレント ファイアウォール ガイドライン

トランスペアレント ファイアウォール ネットワークを計画する場合は、次のガイドラインに従ってください。

- 管理 IP アドレスが必要です。マルチ コンテキスト モードの場合は、各コンテキストごとに IP アドレスが必要です。

  インターフェイスごとに IP アドレスが必要なルーテッド モードと異なり、トランスペアレント ファイアウォールではデバイス全体に IP アドレスが割り当てられます。セキュリティ アプライアンスは、この IP アドレスを、システム メッセージや AAA 通信など、セキュリティ アプライアンスで発信されるパケットの送信元アドレスとして使用します。

  管理 IP アドレスは、接続されているネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。

  管理専用インターフェイス（Management 0/0）の IP アドレスを設定できます。この IP アドレスは、メインの管理 IP アドレスとは別のサブネットに設定できます。

- 透過セキュリティ アプライアンスは、内部インターフェイスと外部インターフェイスだけを使用します。プラットフォームに専用の管理インターフェイスが含まれている場合は、管理トラフィック専用の管理インターフェイスまたはサブインターフェイスを設定することもできます。

  シングルモードでは、セキュリティ アプライアンスに 3 つ以上のインターフェイスが含まれている場合でも、2 つのデータ インターフェイス（および使用可能な場合は専用の管理インターフェイス）だけを使用できます。
- 直接に接続された各ネットワークは同一のサブネット上にある必要があります。
- 接続されたデバイス用のデフォルト ゲートウェイとしてセキュリティ アプライアンス管理 IP アドレスを指定しないでください。デバイスはセキュリティ アプライアンスの他方の側のルータをデフォルト ゲートウェイとして指定する必要があります。
- マルチ コンテキスト モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。
- マルチ コンテキスト モードでは、通常、各コンテキストが別個のサブネットを使用します。重複するサブネットを使用することもできますが、ルーティング スタンドポイントから可能にするため、ネットワーク トポロジにルータと NAT コンフィギュレーションが必要です。

トランスペアレント モードでサポートされていない機能

表 18-1 にトランスペアレント モードでサポートされていない機能を示します。

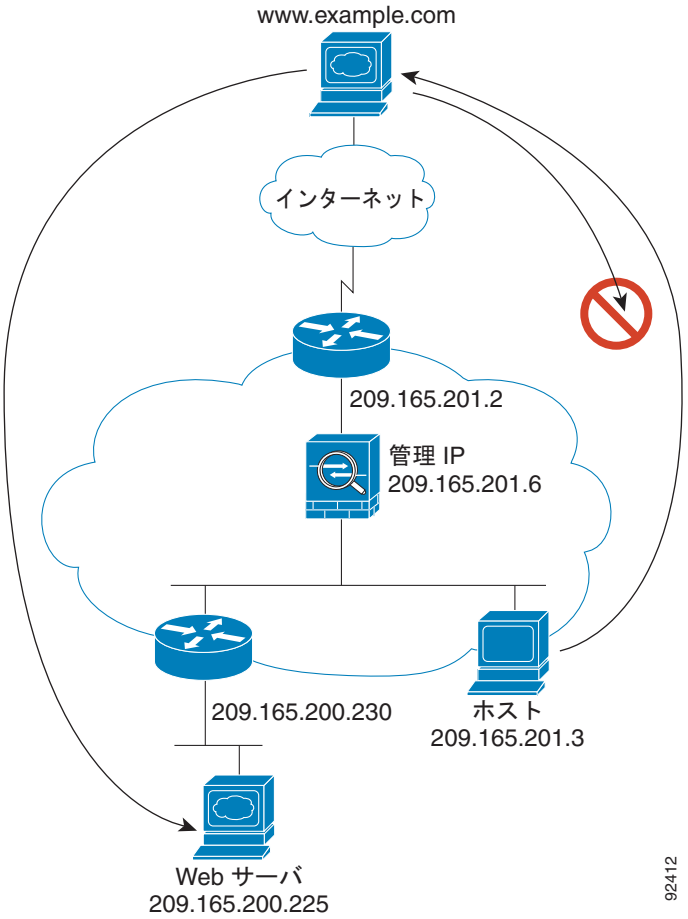
表 18-1　トランスペアレント モードでサポートされていない機能

機能	説明
ダイナミック DNS	—
DHCP リレー	トランスペアレント ファイアウォールは DHCP サーバとして機能することができますが、DHCP リレー コマンドはサポートしません。2 つの拡張アクセス リストを使用して DHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。1 つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう 1 つはサーバからの応答を逆方向に許可します。
ダイナミック ルーティング プロトコル	ただし、セキュリティ アプライアンスで発信されたトラフィックのスタティック ルートを追加できます。拡張アクセス リストを使用して、ダイナミック ルーティング プロトコルがセキュリティ アプライアンスを通過できるようにすることもできます。
IPv6	EtherType アクセス リストを使用した IPv6 は許可できません。
マルチキャスト	拡張アクセス リストで許可することによって、マルチキャスト トラフィックがセキュリティ アプライアンスを通過できるようにすることができます。
QoS	—
通過トラフィック用の VPN ターミネーション	トランスペアレント ファイアウォールは、管理接続に対してのみサイトツーサイト VPN トンネルをサポートします。これは、セキュリティ アプライアンスを通過するトラフィックに対して VPN 接続を終端しません。拡張アクセス リストを使用して VPN トラフィックにセキュリティ アプライアンスを通過させることはできますが、非管理接続は終端されません。クライアントレス SSL VPN もサポートされていません。

トランスペアレント ファイアウォールを通過するデータの動き

図 18-7 に、パブリック Web サーバを含む内部ネットワークを持つ一般的なトランスペアレント ファイアウォールの実装を示します。内部ユーザがインターネット リソースにアクセスできるよう、セキュリティ アプライアンスにはアクセス リストがあります。別のアクセス リストによって、外部ユーザは内部ネットワーク上の Web サーバだけにアクセスできます。

図 18-7　一般的なトランスペアレント ファイアウォールのデータ パス



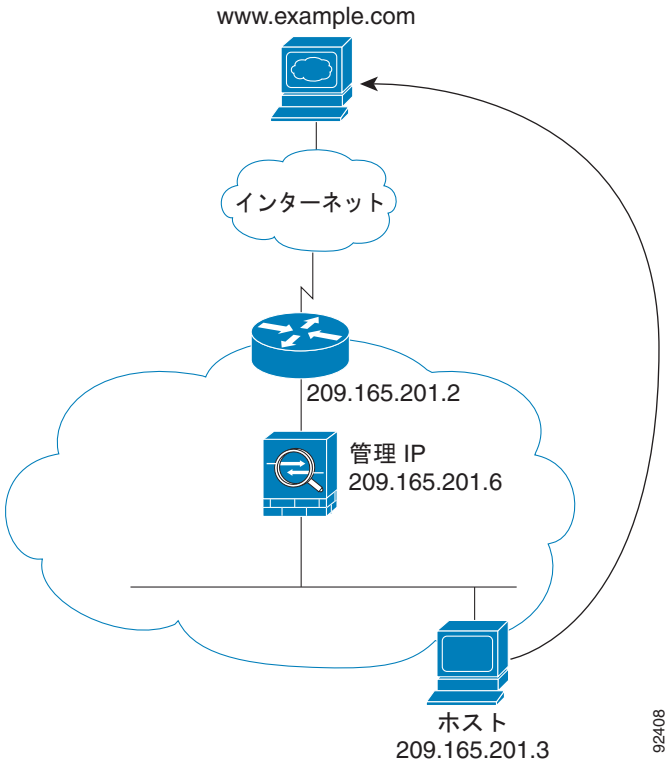
ここでは、データが セキュリティ アプライアンス をどのように通過するかについて説明します。内容は次のとおりです。

- 「内部ユーザが Web サーバにアクセスする」（P.18-13）
- 「NAT を使用して内部ユーザが Web サーバにアクセスする」（P.18-14）
- 「外部ユーザが内部ネットワーク上の Web サーバにアクセスする」（P.18-15）
- 「外部ユーザが内部ホストにアクセスしようとする」（P.18-16）

内部ユーザが Web サーバにアクセスする

図 18-8 は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 18-8　　内部から外部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 18-8 を参照）。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

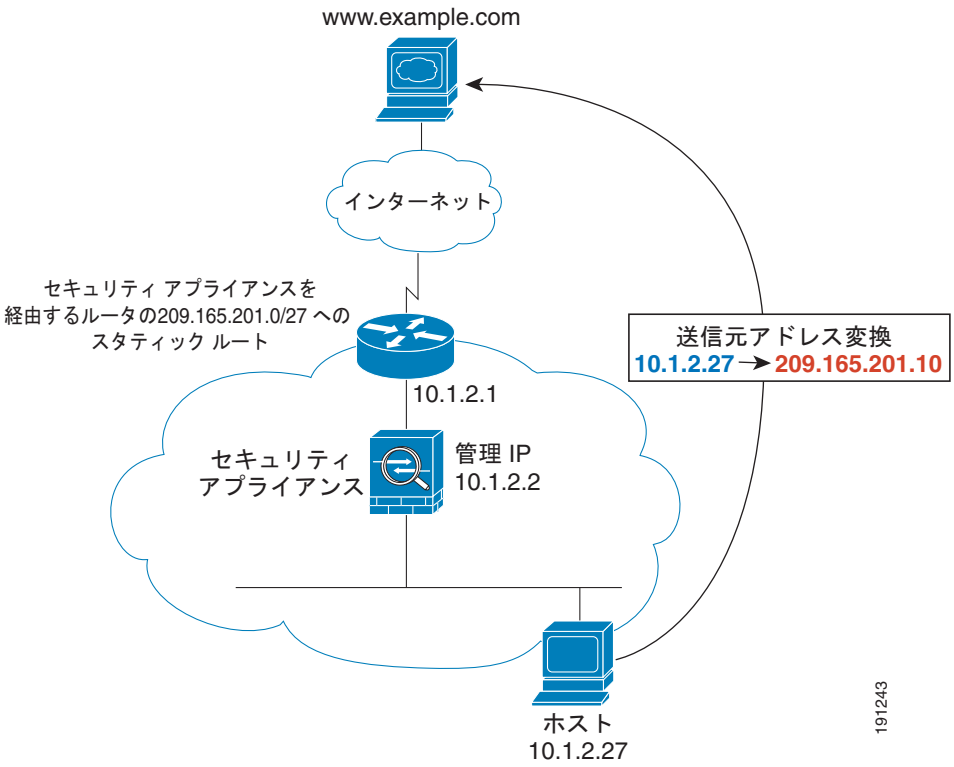
   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、固有なインターフェイスに従ってパケットを分類します。
3. セキュリティ アプライアンスは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、セキュリティ アプライアンスは外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータ 209.186.201.2 のアドレスです。

   宛先 MAC アドレスがセキュリティ アプライアンスのテーブルにない場合、セキュリティ アプライアンスは、ARP 要求と ping を送信して、MAC アドレスを検出しようとします。最初のパケットはドロップされます。
5. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. セキュリティ アプライアンスは、パケットを内部ユーザに転送します。

NAT を使用して内部ユーザが Web サーバにアクセスする

図 18-8 は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 18-9　　NAT を使用して内部から外部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 18-8 を参照）。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、固有なインターフェイスに従ってパケットを分類します。
3. セキュリティ アプライアンスは実際のアドレス（10.1.2.27）をマッピング アドレス 209.165.201.10 に変換します。

   マッピング アドレスは外部インターフェイスと同じネットワーク上にないため、アップストリーム ルータにセキュリティ アプライアンスをポイントするマッピング ネットワークへのスタティック ルートがあることを確認します。
4. 次に、セキュリティ アプライアンスはセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。
5. 宛先 MAC アドレスがテーブル内にある場合、セキュリティ アプライアンスは外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 209.165.201.2 です。

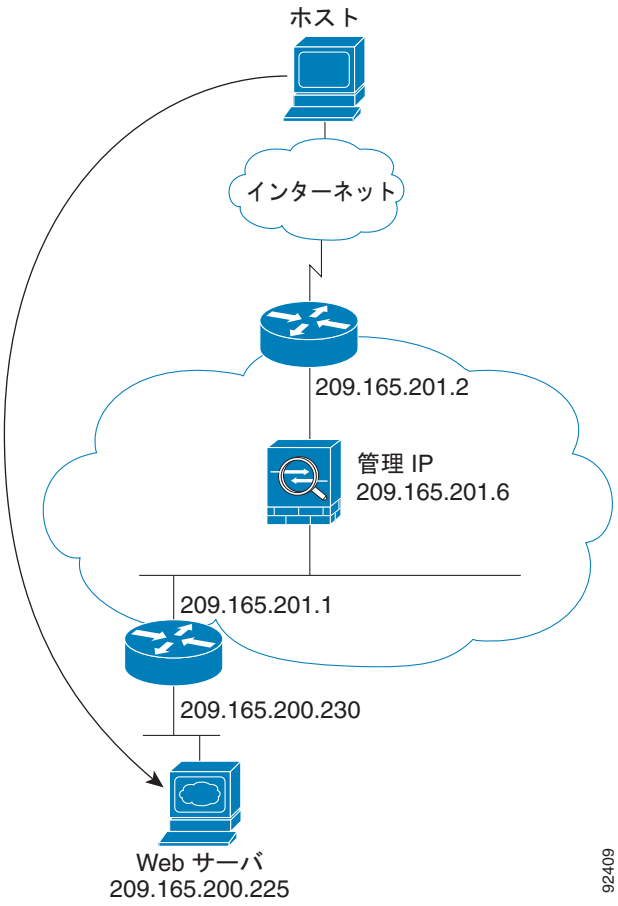
宛先 MAC アドレスがセキュリティ アプライアンスのテーブルにない場合、セキュリティ アプライアンスは、ARP 要求と ping を送信して、MAC アドレスを検出しようとします。最初のパケットはドロップされます。

6. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
7. セキュリティ アプライアンスは、マッピング アドレスを実際のアドレス 10.1.2.27 に変換することによって、NAT を実行します。

外部ユーザが内部ネットワーク上の Web サーバにアクセスする

図 18-10 は、外部ユーザが内部 Web サーバにアクセスしていることを示しています。

図 18-10　外部から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 18-10 を参照）。

1. 外部ネットワーク上のユーザは、内部 Web サーバから Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、固有なインターフェイスに従ってパケットを分類します。

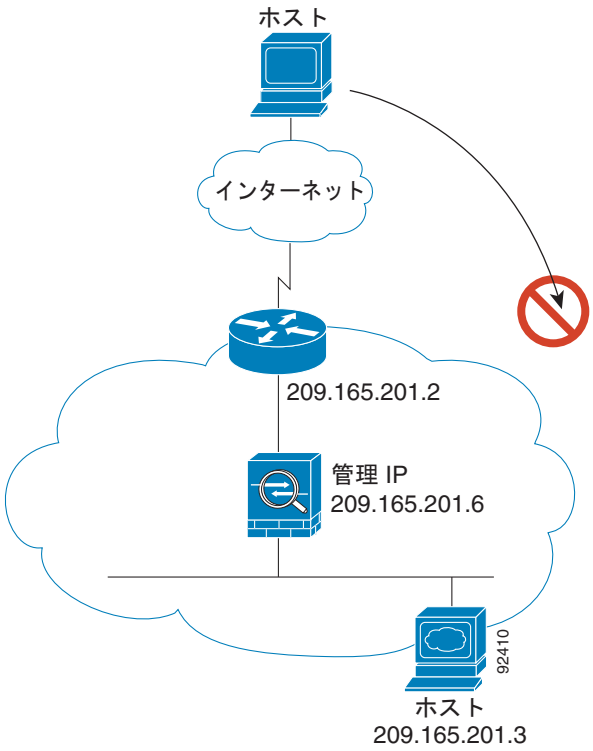
3. セキュリティ アプライアンスは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、セキュリティ アプライアンスは内部インターフェイスからパケットを転送します。宛先 MAC アドレスは、ダウンストリーム ルータのアドレス 209.186.201.1 です。

   宛先 MAC アドレスがセキュリティ アプライアンスのテーブルにない場合、セキュリティ アプライアンスは、ARP 要求と ping を送信して、MAC アドレスを検出しようとします。最初のパケットはドロップされます。
5. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. セキュリティ アプライアンスは、パケットを外部ユーザに転送します。

外部ユーザが内部ホストにアクセスしようとする

図 18-11 は、外部ユーザが内部ネットワーク上のホストにアクセスしようとしていることを示しています。

図 18-11　外部から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 18-11 を参照）。

1. 外部ネットワーク上のユーザが、内部ホストに到達しようとします。

2. セキュリティ アプライアンスはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されているかどうかを確認します。

   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、固有なインターフェイスに従ってパケットを分類します。

3. パケットが拒否され、セキュリティ アプライアンス がパケットを廃棄します。

4. 外部ユーザが内部ネットワークを攻撃しようとした場合、セキュリティ アプライアンスは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

CHAPTER 19

アクセス ルールの設定

アクセル ルール

[Access Rules] ウィンドウには、ルールとして表現されたネットワーク全体のセキュリティ ポリシーが表示されます。

[Access Rules] オプションを選択する場合は、使用可能なプロトコルやポートなど、特定のホストまたはネットワークから別のホストまたはネットワークへのアクセスを制御するアクセス コントロール リストをこのウィンドウで定義できます。アクセス リストはコンジット リストおよび発信リストに取って代わります。

デフォルトではセキュリティ アプライアンスで、より高いセキュリティ レベルからのトラフィック（内部など）は低いセキュリティ レベル（外部など）にアクセスできます。内部ネットワークからのすべての発信 IP トラフィックを許可する内部インターフェイスには、暗黙のアクセス リストがあります。（セキュリティ アプライアンスは、アダプティブ セキュリティ アルゴリズムを使用して外部ネットワークから内部ネットワークに宛てたトラフィックを拒否します。アダプティブ セキュリティ アルゴリズムは、セキュリティへのステートフルなアプローチ方法です。各受信パケットは、アダプティブ セキュリティ アルゴリズムおよびメモリの接続状態情報に対して検査されます）。ASDM には暗黙のアクセス リストが表示されますが、編集することはできません。発信トラフィックを制限するには、アクセス リストを追加します（この場合、暗黙のアクセス リストは削除されます）。

接続がすでに確立されていない限り、各受信パケットはアダプティブ セキュリティ アルゴリズムを使用して検査されます。デフォルトでは、許可するアクセス リストを追加しない限り、セキュリティ アプライアンスでトラフィックはファイアウォールを通過できません。

通常、アダプティブ セキュリティ アルゴリズムで拒否されるトラフィックを許可するには、アクセス リストを追加します。たとえば、外部インターフェイスにアクセス リストを追加すれば、DMZ ネットワーク上の Web サーバへのパブリック アクセスを許可できます。

制約事項

各アクセス リストの最後には、許可されないすべてのトラフィックを拒否する、表記されない暗黙のルールが含まれます。トラフィックは、アクセス コントロール エントリによって明示的に許可されていない場合、拒否されます。このトピックでは、ACE をルールと呼びます。

前提条件

必要に応じて、[Addresses] タブでネットワーク グループを作成します。

フィールド

注：テーブル カラムの幅はカーソルを使用して調整できます。カーソルをカラムの線に重ね、二重矢印になるまで移動します。カラムの線をクリックして、目的のサイズになるまでドラッグします。

- [Add]：新しいアクセス ルールを追加します。

- [Edit]：アクセス ルールを編集します。
- [Delete]：アクセス ルールを削除します。
- [Move Up]：ルールを上に移動します。ルールは、このテーブルに表示される順序で評価されるため、重複したルールがある場合は、それらを表示する順序に注意が必要です。
- [Move Down]：ルールを下に移動します。
- [Cut]：ルールを切り取ります。
- [Copy]：ルールのパラメータをコピーします。[Paste] ボタンを使用すれば、それと同じパラメータを持つルールを新たに作成できます。
- [Paste]：ルールからコピーしたパラメータまたは切り取ったパラメータがあらかじめ入力された状態の [Add/Edit Rule] ダイアログボックスが表示されます。このダイアログボックスでは、それらのパラメータを修正して新しいルールを作成し、それをテーブルに追加できます。[Paste] ボタンをクリックすると、選択したルールのすぐ前にそのルールが追加されます。[Paste] ドロップダウン リストから [Paste After] 項目を選択すると、選択したルールのすぐ後にそのルールが追加されます。
- [Find]：一致するルールだけを表示するように、表示内容をフィルタリングします。[Find] をクリックすると、[Filter] フィールドが開きます。もう一度 [Find] をクリックすると、[Filter] フィールドは非表示になります。
  - [Filter] ドロップダウン リスト：フィルタリングする基準として、[Interface]、[Source]、[Destination]、[Source or Destination]、[Destination Service]、[Rule Query] の中からいずれかを選択します。ルール クエリーとは、複数の基準を 1 つにまとめたもので、保存しておけば繰り返し使用できます。
  - [Condition] ドロップダウン リスト：基準が [Source]、[Destination]、[Source or Destination]、および [Destination Service] の場合、条件として [is] または [includes] のいずれかを選択します。
  - [Filter] フィールド：[Interface] タイプが選択された場合、このフィールドはドロップダウン リストになり、そこからインターフェイス名を選択できます。[Rule Query] タイプが選択された場合、このドロップダウン リストには、選択肢としてすべての定義済みルール クエリーが表示されます。[Source] タイプおよび [Destination] タイプが選択された場合は、IP アドレスを指定できます。手動で入力できるほか、[...] ボタンをクリックし、[Browse Address] ダイアログボックスを開いて参照することもできます。[Destination Service] タイプが選択された場合は、プロトコル タイプとして、TCP、UDP、TCP-UDP、ICMP、IP のいずれかを指定できます。手動で入力できるほか、[...] ボタンをクリックし、[Browse Service Groups] ダイアログボックスを開いて参照することもできます。[Filter] フィールドには、複数のエントリを指定できます。その際、各エントリは、カンマまたはスペースで区切ります。また、ワイルドカードも使用できます。
  - [Filter]：フィルタを実行します。
  - [Clear]：一致内容および表示内容をすべてクリアします。
  - [Rule Query]：[Rule Queries] ダイアログボックスが表示されます。このダイアログボックスでは、名前付きルール クエリーを管理できます。
- [Diagram]：ルール テーブルの下に [Rule Flow Diagram] 領域が表示されます。この図には、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクションが表示されます。
- [Export]：カンマ区切り形式または html 形式のファイルにエクスポートします。
- [Show]：選択したアクセス ルールにより生成された syslog が、Real-Time Log Viewer に表示されます。

次に、[Access Rules] テーブルのカラムについて説明します。これらのカラムの内容を編集する場合は、テーブル行をダブルクリックします。ルールは、実行順に表示されます。ルールを右クリックすると、上記のボタンで選択できるすべてオプションのほか、[Insert] 項目および [Insert After] 項目が表示されます。[Insert] 項目を指定すると、選択したルールのすぐ前に新しいルールが挿入され、[Insert After] 項目を指定すると、選択したルールのすぐ後に新しいルールが挿入されます。

- [No] : ルールの評価順序を示します。
- [Enabled] : ルールがイネーブルかディセーブルかを示します。
- [Source] : [Destination Type] フィールドで指定された宛先に対してトラフィックを許可または拒否する送信元の IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。アドレス カラムには、単語 any が付いたインターフェイス名が表示される場合があります（inside: any など）。これは、内部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。
- [Destination] : [Source Type] フィールドで指定された送信元に対してトラフィックを許可または拒否する宛先の IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。アドレス カラムには、単語 any が付いたインターフェイス名が表示される場合があります（outside: any など）。これは、外部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。また、詳細モードでは、アドレス カラムに角カッコで囲まれた IP アドレスが表示されることもあります（[209.165.201.1-209.165.201.30] など）。これらのアドレスは、変換済みアドレスです。内部ホストが外部ホストへの接続を作成すると、ファイアウォールは内部ホストのアドレスをプールのアドレスにマッピングします。ホストがアウトバウンド接続を作成した後、ファイアウォールはこのアドレス マッピングを維持します。アドレス マッピング構造は xlate と呼ばれ、一定の時間、メモリに保持されます。外部ホストでは、アクセス リストにより許可されている場合は、この間にプールの変換済みアドレスを使用して、内部ホストへの接続を開始できます。通常、内部ホストは常に同じ IP アドレスを使用するため、外部から内部への接続にはスタティック変換が必要です。
- [Service] : ルールで指定されるサービスまたはプロトコルを表示します。
- [Action] : ルールに適用されるアクション（[Permit] または [Deny]）が表示されます。
- [Hits] : ルールに対するヒット数が表示されます。このカラムは、[Preferences] ダイアログボックスで設定した頻度に応じて動的にアップデートされます。ヒット数は、明示的なルールにだけ適用されます。暗黙的なルールのヒット数は [Access Rules] テーブルには表示されません。
- [Logging] : アクセス リストのロギングをイネーブルにしている場合、このカラムには、ロギング レベル、およびログ メッセージ間の間隔が秒数で表示されます。
- [Time] : ルールが適用される時間範囲が表示されます。
- [Description] : ルールを追加したときに入力した説明が表示されます。暗黙のルールには、「Implicit outbound rule」という説明が含まれます。
- [Addresses] : このタブでは、サービス グループまたはネットワーク オブジェクト グループを追加、編集、削除、または検索できます。IP アドレス オブジェクトは、ルールの作成時に、送信元エントリおよび宛先エントリに基づいて自動的に作成されるため、それ以降のルールを作成する際には容易に選択できます。IP アドレス オブジェクトの追加、編集、および削除は、手動で行うことはできません。
- [Services] : このタブでは、サービスを追加、編集、削除、または検索できます。
- [Time Ranges] : このタブでは、時間範囲を追加、編集、または削除できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ルール クエリー

[Rule Queries] ダイアログボックスでは、ルールの検索時に [Filter] フィールドで使用できる名前付きルール クエリーを管理できます。

フィールド

- [Add]：ルール クエリーを追加します。
- [Edit]：ルール クエリーを編集します。
- [Delete]：ルール クエリーを削除します。
- [Name]：ルール クエリーの名前を一覧表示します。
- [Description]：ルール クエリーの説明を一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ルール クエリーの新規作成と編集

[New/Edit Rule Query] ダイアログボックスでは、ルールの検索時に [Filter] フィールドで使用できる名前付きルール クエリーを追加または編集できます。

フィールド

- [Name]：ルール クエリーの名前を入力します。
- [Description]：ルール クエリーの説明を入力します。
- [Match Criteria]：この領域では、フィルタリングのための基準を一覧表示します。
  - [any of the following criteria]：一覧表示された任意の基準に一致するようにルール クエリーを設定します。
  - [all of the following criteria]：一覧表示されたすべての基準に一致するようにルール クエリーを設定します。
  - [Field]：基準のタイプを一覧表示します。これには、インターフェイスまたは送信元などがあります。

  - [Value]：基準の値を一覧表示します（[inside] など）。
  - [Remove]：選択した基準を削除します。
- [Define New Criteria]：この領域では、新しい基準を定義して、それを一致基準に追加します。
  - [Field]：[Interface]、[Source]、[Destination]、[Service]、[Action]、別の [Rule Query] など、ルール クエリーにネストされる基準のタイプを選択します。
  - [Value]：検索する値を入力します。[Interface] タイプが選択された場合、このフィールドはドロップダウン リストになり、そこからインターフェイス名を選択できます。[Action] タイプが選択された場合、ドロップダウン リストには [Permit] および [Deny] が表示されます。[Rule Query] タイプが選択された場合、このドロップダウン リストには、選択肢としてすべての定義済みルール クエリーが表示されます。[Source] タイプおよび [Destination] タイプが選択された場合は、IP アドレスを指定できます。手動で入力できるほか、[...] ボタンをクリックし、[Browse Address] ダイアログボックスを開いて参照することもできます。[Service] タイプが選択された場合は、プロトコル タイプとして、TCP、UDP、TCP-UDP、ICMP、IP のいずれかを指定できます。手動で入力できるほか、[...] ボタンをクリックし、[Browse Service Groups] ダイアログボックスを開いて参照することもできます。
  - [Add]：[Match Criteria] テーブルに基準を追加します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

アクセス ルールの追加と編集

[Add/Edit Rule] ダイアログボックスでは、新しいルールの作成や、既存のルールの修正を行うことができます。

フィールド

- [Interface]：ルールを適用するインターフェイスを指定します。
- [Action]：新しいルールのアクション タイプを指定します。[Permit] と [Deny] のいずれかを選択します。
  - [Permit]：一致するすべてのトラフィックを許可します。
  - [Deny]：一致するすべてのトラフィックを拒否します。
- [Source]：[Destination] フィールドで指定された宛先に対してトラフィックを許可または拒否する送信元の IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。

  [...]：既存の IP アドレス オブジェクト、IP 名、ネットワーク オブジェクト グループ、またはそれらすべてを選択、追加、編集、削除、または検索できます。
- [Destination]：[Source Type] フィールドで指定された送信元に対してトラフィックを許可または拒否する宛先の IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。

[...] : 既存の IP アドレス オブジェクト、IP 名、ネットワーク オブジェクト グループ、またはそれらすべてを選択、追加、編集、削除、または検索できます。

- [Service] : サービスのリストからポート番号、ポートの範囲、またはウェルノウン サービス名やグループを指定する場合にこのオプションを選択します。

  [...] : 事前に設定したリストで、既存のサービスを選択、追加、編集、削除、または検索できます。

- [Description] :（任意）アクセス ルールの説明を入力します。
- [Enable Logging] : アクセス リストのロギングをイネーブルにします。
  - [Logging Level] : デフォルトの値をそのまま使用するか、または [Emergency]、[Alert]、[Critical]、[Error]、[Warning]、[Notification]、[Informational]、[Debugging] のいずれかを指定します。
- [More Options] : ルールの追加設定オプションを表示します。
  - [Enable Rule] : ルールをイネーブルまたはディセーブルにします。
  - [Traffic Direction] : どちらの方向のトラフィックにルールを適用するかを指定します。[Incoming] と [Outgoing] のいずれかを選択できます。
  - [Source Service] : 送信元のプロトコルとサービスを指定します（TCP または UDP サービスに限る）。

    [...] : 事前に設定したリストで、送信元サービスを選択、追加、編集、削除、または検索できます。
  - [Logging Interval] : ロギングが設定されている場合、ロギング間隔を秒単位で指定します。
  - [Time Range] : このルールに定義されている時間範囲をドロップダウン リストから指定します。

    [...] : 事前に設定したリストで、時間範囲を選択、追加、編集、削除、または検索できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

サービス グループの管理

[Manage Service Groups] ダイアログボックスでは、名前付きグループにある複数の TCP、UDP、または TCP-UDP サービス（ポート）を関連付けることができます。それにより、アクセス ルール、IPSec ルール、コンジットなど、ASDM および CLI 内のさまざまな機能でサービス グループを使用できます。

用語の *サービス*は、ウェルノウン ポート番号および「リテラル」名（ftp、telnet、smtp など）を持ち、アプリケーション レベル サービスと関連付けられた上位層プロトコルを指します。

セキュリティ アプライアンスでは、次の TCP リテラル名を使用できます。

bgp、chargen、cmd、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、ident、irc、klogin、kshell、lpd、nntp、pop2、pop3、pptp、smtp、sqlnet、sunrpc、tacacs、talk、telnet、time、uucp、whois、www。

サービス グループの名前は、オブジェクト グループの 4 つすべてのタイプで、一意であることが必要です。たとえば、サービス グループとネットワーク グループには、同じ名前は使用できません。

複数のサービス グループをネストすれば、「グループのグループ」を構成できます。「グループのグループ」は 1 つのグループとして使用できます。サービス オブジェクト グループを削除すると、それが使用されているすべてのサービス オブジェクト グループから削除されます。

サービス グループがアクセス ルールで使用されている場合は、削除しないでください。アクセス ルールで使用されているサービス グループを空にはできません。

フィールド

- [TCP] : TCP サービスまたは TCP ポート番号をオブジェクト グループに追加する場合は、このオプションを選択します。
- [UDP] : UDP サービスまたは UDP ポート番号をオブジェクト グループに追加する場合は、このオプションを選択します。
- [TCP-UDP] : TCP および UDP に共通のサービスまたはポート番号をオブジェクト グループに追加する場合は、このオプションを選択します。
- [Service Group] テーブル：このテーブルには、各サービス オブジェクト グループの記述名が表示されます。このリストのグループを修正または削除する場合は、グループを選択し、[Edit] または [Delete] をクリックします。新しいグループをこのリストに追加する場合は、[Add] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Service Group

[Add/Edit Service Group] ダイアログボックスでは、TCP および UDP のサービスまたはポートのグループを管理できます。

フィールド

- [Service Group Name] : サービス グループの名前を指定します。名前は、すべてのオブジェクト グループで一意であることが必要です。サービス グループに、ネットワーク グループと同じ名前を指定することはできません。
- [Description] : サービス グループの説明を指定します。
- [Service] : 事前定義済みドロップダウン リストから、サービス グループのサービスを選択できます。
- [Range/Port #] : サービス グループのポートの範囲を指定できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

高度なアクセス ルール設定

[Advanced Access Rule Configuration] ダイアログボックスでは、グローバル アクセス リストのロギング オプションを設定できます。

ロギングがイネーブルで、パケットが ACE に合致した場合、セキュリティ アプライアンスでは、フロー エントリが作成され、指定された時間内に受信したパケット数の追跡が行われます（「Log Options」を参照）。セキュリティ アプライアンス は、最初のヒット時と各間隔の終了時に、その間隔での合計ヒット数を示すシステム ログ メッセージを生成します。各間隔の終わりに、セキュリティ アプライアンスはヒット数を 0 にリセットします。1 つの間隔内で ACE と一致するパケットがなかった場合、セキュリティ アプライアンスはそのフロー エントリを削除します。

どの時点でも大量のフローが同時に存在する可能性があります。メモリおよび CPU のリソースが無制限に消費されないようにするため、セキュリティ アプライアンスでは同時拒否フロー数に制限が設定されます。この制限は、拒否フローに対してだけ設定されます（許可フローには設定されません）。これは、拒否フローが攻撃を示している可能性があるためです。制限に達した場合、セキュリティ アプライアンスでは既存の拒否フローが期限切れになるまで新しい拒否フローは作成されません。DoS 攻撃（サービス拒絶攻撃）が開始された場合、セキュリティ アプライアンスではごく短時間のうちに大量の拒否フローが作成される可能性があります。拒否フロー数を制限することで、メモリおよび CPU のリソースが無制限に消費されるのを防ぐことができます。

前提条件

これらの設定は、アクセス リストのアクセス コントロール エントリ（別名ルール）に対して、さらに新しいロギング メカニズムをイネーブルにする場合に限り適用されます。詳細については、「Log Options」を参照してください。

フィールド

- [Maximum Deny-flows]：セキュリティ アプライアンスによりロギングが停止される前に許可される拒否フローの最大数を、1 からデフォルト値までの間で指定します。デフォルトは 4096 です。
- [Alert Interval]：拒否フローが最大数に達したことを示すシステム ログ メッセージ（番号 106101）が生成される時間間隔（1 ～ 3600 秒）を指定します。デフォルトは 300 秒です。
- [Per User Override table]：ユーザごとの上書き機能の状態を指定します。着信アクセス リストに対してユーザごとの上書き機能がイネーブルになると、RADIUS サーバによって提供されるアクセス リストは、そのインターフェイス上で設定されたアクセス リストに置き換えられます。ユーザごとの上書き機能がディセーブルになると、RADIUS サーバによって提供されるアクセス リストは、そのインターフェイス上で設定されたアクセス リストと結合されます。インターフェイスに着信アクセス リストが設定されていない場合、ユーザごとの上書きは設定できません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ログ オプション

[Log Options] ダイアログボックスでは、アクセス コントロール リストの各アクセス コントロール エントリ（別名ルール）のロギング オプションを設定できます。コンジットと発信リストはロギングをサポートしていません。グローバル ロギング オプションの設定については、「高度なアクセス ルール設定」を参照してください。

このダイアログボックスでは、旧式のロギング メカニズム（拒否されたトラフィックだけが記録される）を使用したり、新しいロギング メカニズム（許可および拒否されたトラフィックがパケットのヒット数などの追加情報と共に記録される）を使用したり、ロギングをディセーブルにしたりできます。

[Log] オプションをイネーブルにすると、一定量のメモリが消費されます。潜在的なサービス拒否攻撃のリスクを制御するには、[Maximum Deny-flow] 設定が便利です。この設定を使用する場合は、[Access Rules] ウィンドウの [Advanced] を選択します。

フィールド

- [Use default logging behavior]：パケットが拒否されると、セキュリティ アプライアンスによりシステム ログ メッセージ番号 106023 が記録される、旧式のアクセス リスト ロギング メカニズムが使用できるようになります。このオプションは、デフォルト設定に戻す場合に使用します。
- [Enable logging for the rule]：パケットが ACE に合致すると（許可または拒否のいずれか）、セキュリティ アプライアンスによりシステム ログ メッセージ番号 106100 が記録される、新しいアクセス リスト ロギング メカニズムがイネーブルになります。

  パケットが ACE と一致した場合、セキュリティ アプライアンスは、フロー エントリを作成して、指定された間隔で受信したパケットの数を追跡します（後述の [Logging Interval] フィールドを参照）。セキュリティ アプライアンス は、最初のヒット時と各間隔の終了時に、その間隔での合計ヒット数を示すシステム ログ メッセージを生成します。各間隔の終わりに、セキュリティ アプライアンスはヒット数を 0 にリセットします。1 つの間隔内で ACE と一致するパケットがなかった場合、セキュリティ アプライアンスはそのフロー エントリを削除します。

  - [Logging Level]：syslog サーバに送信されるロギング メッセージのレベルをドロップダウン リストから選択します。レベルは次のように定義されています。

    Emergency（レベル 0）：セキュリティ アプライアンスでは、このレベルは使用しません。

    Alert（レベル 1、即時対処が必要）

    Critical（レベル 2、クリティカル条件）

    Error（レベル 3、エラー条件）

    Warning（レベル 4、警告条件）

    Notification（レベル 5、正常だが顕著な条件）

    Informational（レベル 6、情報メッセージのみ）

    Debugging（レベル 7、デバッグ中のみ表示）

  - [Logging Interval]：セキュリティ アプライアンスにおいて、フロー統計情報が syslog に送信されるまでの待機時間を秒単位で設定します（1 ～ 600 秒）。この設定は、ACE に合致するパケットがない場合に、フローを削除するタイムアウト値としても使用されます。デフォルトは 300 秒です。

- [Disable logging for the rule]：ACE に対するロギングをすべてディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 20

EtherType ルールの設定

Ethertype Rules（トランスペアレント モードのみ）

[EtherType Rules] ウィンドウに、パケット EtherType に基づくアクセス ルールが表示されます。EtherType ルールは、トランスペアレント モードで動作する セキュリティ アプライアンス において、非 IP 関連トラフィック ポリシーを設定する場合に使用されます。トランスペアレント モードでは、拡張アクセス ルールと EtherType アクセス ルールの両方をインターフェイスに適用できます。EtherType ルールは、拡張アクセス ルールに優先されます。

フィールド

- [Add]：新しい EtherType ルールを追加します。ドロップダウン リストから追加するルールのタイプを選択します。
- [Edit]：EtherType ルールを編集します。
- [Delete]：EtherType ルールを削除します。
- [Move Up]：ルールを上に移動します。ルールは、このテーブルに表示される順序で評価されるため、重複したルールがある場合は、それらを表示する順序に注意が必要です。
- [Move Down]：ルールを下に移動します。
- [Cut]：ルールを切り取ります。
- [Copy]：ルールのパラメータをコピーします。[Paste] ボタンを使用すれば、それと同じパラメータを持つルールを新たに作成できます。
- [Paste]：ルールからコピーしたパラメータまたは切り取ったパラメータがあらかじめ入力された状態の [Add/Edit Rule] ダイアログボックスが表示されます。このダイアログボックスでは、それらのパラメータを修正して新しいルールを作成し、それをテーブルに追加できます。[Paste] ボタンをクリックすると、選択したルールのすぐ前にそのルールが追加されます。[Paste] ドロップダウン リストから [Paste After] 項目を選択すると、選択したルールのすぐ後にそのルールが追加されます。

次に、[EtherType Rules] テーブルのカラムについて説明します。カラムの内容を編集する場合は、テーブル セルをダブルクリックします。カラム ヘッダーをダブルクリックすると、選択されたカラムをソート キーとして、テーブルが英数字の昇順でソートされます。ルールを右クリックすると、上記のボタンで選択できるすべてオプションのほか、[Insert] 項目および [Insert After] 項目が表示されます。[Insert] 項目を指定すると、選択したルールのすぐ前に新しいルールが挿入され、[Insert After] 項目を指定すると、選択したルールのすぐ後に新しいルールが挿入されます。

- [No]：ルールの評価順序を示します。
- [Action]：このルールのアクションを許可または拒否します。

- [Ethervalue]：EtherType を識別するための EtherType 値。IPX、BPDU、MPLS-Unicast、MPLS-Multicast、または 0x600（1536）～ 0xffff の 16 ビットの 16 進数値です。
- [Interface]：ルールが適用されるインターフェイスです。
- [Direction Applied]：このルールの方向。着信トラフィックまたは発信トラフィックです。
- [Description]：ルールを説明するオプションのテキストです。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

Add/Edit EtherType Rule

[Add/Edit EtherType Rules] ダイアログボックスでは、EtherType ルールを追加または編集できます。

フィールド

- [Action]：このルールのアクションを許可または拒否します。
- [Interface]：このルールのインターフェイスの名前です。
- [Apply rule to]：このルールの方向。着信トラフィックまたは発信トラフィックです。
- [Ethervalue]：EtherType を識別するための EtherType 値。BPDU、IPX、MPLS-Unicast、MPLS-Multicast、any（0x600 ～ 0xffff の任意の値）、または 0x600（1536）～ 0xffff の 16 ビットの 16 進数値です。
- [Description]：ルールを説明するオプションのテキストです。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

CHAPTER 21

AAA ルールの設定

この章では、ネットワーク アクセスに対して AAA（「トリプル エー」と発音）をイネーブルにする方法について説明します。この章は、次の項で構成されています。

（注） 管理アクセスの AAA については、「システム管理者用 AAA の設定」（P.13-26）を参照してください。

AAA サービスの概要については、第 12 章「AAA サーバおよびユーザ アカウントの設定」を参照してください。

AAA のパフォーマンス

セキュリティ アプライアンスは「カットスルー プロキシ」を使用します。これにより、従来のプロキシ サーバと比較して、パフォーマンスが大幅に向上します。従来のプロキシ サーバは、OSI モデルのアプリケーション レイヤですべてのパケットを分析するため、プロキシ サーバのパフォーマンスに負担がかかります。セキュリティ アプライアンス カットスルー プロキシは、アプリケーション層で最初にユーザ確認を行い、続いて標準 AAA サーバまたはローカル データベースで認証します。セキュリティ アプライアンスはユーザを認証した後、セッション フローをシフトするため、セッション ステート情報を維持したまま、すべてのトラフィックが送信元と宛先の間で直接かつ迅速に流れます。

ネットワーク アクセス認証の設定

この項では、次のトピックについて取り上げます。

- 「ネットワーク アクセス許可の設定」（P.21-5）

認証の概要

セキュリティ アプライアンスでは、AAA サーバを使用するネットワーク アクセス認証を設定できます。この項では、次のトピックについて取り上げます。

- 「一度だけの認証」（P.21-2）
- 「認証確認を受けるために必要なアプリケーション」（P.21-2）
- 「セキュリティ アプライアンスの認証プロンプト」（P.21-2）
- 「スタティック PAT および HTTP」（P.21-3）
- 「Web クライアントのセキュアな認証」（P.21-3）

一度だけの認証

所定の IP アドレスのユーザは、認証セッションが期限切れになるまで、すべてのルールおよびタイプに対して一度だけ認証を受ける必要があります（タイムアウト値については、「グローバル タイムアウトの設定」（P.27-23）を参照してください）。たとえば、セキュリティ アプライアンスに Telnet と FTP の認証を設定した場合、最初に Telnet の認証に成功したユーザは、その認証セッションが存在する限り、FTP の認証を受ける必要がありません。

認証確認を受けるために必要なアプリケーション

プロトコルまたはサービスへのネットワーク アクセス認証を要求するようにセキュリティ アプライアンスを設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP、HTTPS、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、セキュリティ アプライアンスは認証が必要な他のトラフィックを許可しません。

セキュリティ アプライアンスが AAA 用にサポートしている認証ポートは固定値です。

- ポート 21 は FTP 用
- ポート 23 は Telnet 用
- ポート 80 は HTTP 用
- ポート 443 は HTTPS 用

セキュリティ アプライアンスの認証プロンプト

Telnet および FTP の場合、セキュリティ アプライアンスは認証プロンプトを生成します。

HTTP の場合、セキュリティ アプライアンスはデフォルトで基本 HTTP 認証を使用し、認証プロンプトを提供します。オプションで、ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（「高度な AAA 機能の設定」（P.21-14）を参照）。

HTTPS の場合、セキュリティ アプライアンスはカスタム ログイン画面を生成します。オプションで、ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（「高度な AAA 機能の設定」（P.21-14）を参照）。

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、セキュリティ アプライアンスでの直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

正常に認証されると、セキュリティ アプライアンスにより元の宛先にリダイレクトされます。宛先サーバにも独自の認証がある場合、ユーザは別のユーザ名とパスワードを入力します。基本 HTTP 認証を使用していて、宛先サーバ用に別のユーザ名とパスワードを入力する必要がある場合は、仮想 HTTP を設定する必要があります（「仮想アクセスの設定」（P.21-16）を参照）。

（注）　HTTP 認証を使用する場合、デフォルトでクリア テキストのユーザ名とパスワードがクライアントからセキュリティ アプライアンスに送信されます。さらにこのユーザ名とパスワードは宛先 Web サーバにも送信されます。クレデンシャルの保護の詳細については、「Web クライアントのセキュアな認証」（P.21-3）を参照してください。

FTP の場合、セキュリティ アプライアンス ユーザ名、アット マーク（@）、FTP ユーザ名（name1@name2）を入力するオプションがあります。パスワードには、セキュリティ アプライアンス パスワード、アット マーク（@）、FTP パスワード（password1@password2）を入力します。たとえば、次のテキストを入力します。

```
name> jamiec@patm
password> letmein@he110
```

この機能は、複数のログインを必要とするファイアウォールをカスケード接続している場合に有用です。複数の名前およびパスワードは、複数のアット マーク（@）で区切ることができます。

スタティック PAT および HTTP

HTTP 認証では、スタティック PAT が設定されている場合、セキュリティ アプライアンスは実際のポートをチェックします。セキュリティ アプライアンスは、マッピング ポートにかかわらず、実際のポート 80 を宛先とするトラフィックを検出した場合、HTTP 接続を代行受信し、認証を実行します。

たとえば、外部 TCP ポート 889 が次のようにポート 80（www）に変換されていて、関係するすべてのアクセス ルールでこのトラフィックが許可されているとします。

この場合、ユーザはポート 889 で 10.48.66.155 にアクセスを試み、セキュリティ アプライアンスはそのトラフィックを代行受信して、HTTP 認証を実行します。セキュリティ アプライアンスが HTTP 接続の完了を許可する前に、ユーザの Web ブラウザには HTTP 認証ページが表示されます。

ローカル ポートがポート 80 ではない場合、ユーザには認証ページは表示されません。代わりに、セキュリティ アプライアンスは Web ブラウザにエラー メッセージを送信して、要求されたサービスを使用する前にユーザが認証を受ける必要があることを通知します。

Web クライアントのセキュアな認証

HTTP 認証を使用する場合、デフォルトでクリア テキストのユーザ名とパスワードがクライアントからセキュリティ アプライアンスに送信されます。さらにこのユーザ名とパスワードは宛先 Web サーバにも送信されます。セキュリティ アプライアンスでは、次のような複数の方式で HTTP 認証を保護できます。

- リダイレクション方式による HTTP 認証：詳細については、「インタラクティブ認証ルールの追加」（P.21-15）を参照してください。この方式では、認証クレデンシャルがその後続けて宛先サーバに送信されないようにします。
- 仮想 HTTP をイネーブルにする：「仮想 HTTP の設定」（P.21-17）を参照して、セキュリティ アプライアンスの認証と HTTP サーバの認証を別々に受けることができます。HTTP サーバが 2 次認証を必要としない場合でも、このコマンドにより基本認証クレデンシャルは HTTP GET 要求から除去されます。
- Web クライアントとセキュリティ アプライアンスとの間の HTTPS によるユーザ名とパスワードの交換をイネーブルにする：「HTTPS を使用した HTTP 認証のクレデンシャルの交換」（P.21-14）を参照して、Web クライアントとセキュリティ アプライアンスとの間の HTTPS によるユーザ名とパスワードの交換をイネーブルにします。これはセキュリティ アプライアンスと宛先サーバの間だけでなく、クライアントとセキュリティ アプライアンスの間のクレデンシャルを保護する唯一の方式です。この方式だけを使用することも、または他の方式のいずれかと組み合わせてセキュリティを最大限にすることもできます。

ネットワーク アクセス認証のイネーブル化

ネットワーク アクセス認証をイネーブルにするには、次の手順を実行します。

ステップ 1　第 12 章「AAA サーバおよびユーザ アカウントの設定」に従って、AAA サーバ グループを設定します。

ステップ 2　[Configuration] > [Firewall] > [AAA Rules] ペインから、[Add] > [Add Authentication Rule] を選択します。

[Add Authentication Rule] ダイアログボックスが表示されます。

ステップ 3　[Interface] ドロップダウン リストから、ルールを適用するインターフェイスを選択します。

ステップ 4　[Authenticate] または [Do not Authenticate] をクリックします。

10.1.1.50 を除く 10.1.1.0/24 を認証する場合、2 つのルール（1 つには [Authenticate] オプションを使用、もう 1 つには [Do not Authenticate] オプションを使用）を作成します。ルールは必ず適切な順序に並べてください。たとえば、上記の [Do not Authenticate] ルールを [Authenticate] ルールよりも上に置き、10.1.1.50 からのトラフィックが最初に [Do not Authenticate] ルールに一致するようにします。

ステップ 5　[AAA Server Group] ドロップダウン リストから、サーバ グループまたは LOCAL ユーザ データベースを選択します。

ステップ 6　（任意）AAA サーバをサーバ グループに追加するには、[Add Server] をクリックします。ユーザを LOCAL データベースに追加するには、[Add User] をクリックします。

サーバ グループとローカル ユーザ データベースの設定の詳細については、第 12 章「AAA サーバおよびユーザ アカウントの設定」を参照してください。

ステップ 7　[Source] フィールドで、送信元 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

任意の送信元アドレスを指定するには、**any** を入力します。

アドレスが複数ある場合はカンマで区切ります。

ステップ 8　[Destination] フィールドで、宛先 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

任意の宛先アドレスを指定するには、**any** を入力します。

アドレスが複数ある場合はカンマで区切ります。

ステップ 9　[Service] フィールドで、宛先サービスの IP サービス名または番号を入力するか、[...] ボタンをクリックしてサービスを選択します。

TCP または UDP のポート番号、あるいは ICMP サービス番号を指定する場合は、*プロトコル / ポート* を入力します。たとえば、TCP/8080 と入力します。

デフォルトでは、サービスは TCP です。

サービスが複数ある場合はカンマで区切ります。

HTTP、HTTPS、Telnet、または FTP のいずれかの宛先ポートを必ず含めます。これは、ユーザがこれらのサービスのいずれかの認証を受けないと、他のサービスがセキュリティ アプライアンスの通過を許可されないためです。

ステップ 10　（任意）[Description] フィールドに説明を入力します。

ステップ 11　（任意）TCP または UDP の送信元サービスを指定するには、[More Options] 領域をクリックして開き、[Source Service] フィールドに TCP サービスまたは UDP サービスを入力します。

宛先サービスと送信元サービスは同じである必要があります。[Destination Service] フィールドをコピーし、[Source Service] フィールドに貼り付けます。

ステップ 12　（任意）ルールを非アクティブにするには、[More Options] 領域をクリックして開き、[Enable Rule] をオフにします。

この設定は、ルールを削除せずに無効にしたい場合に便利です。

ステップ 13　（任意）ルールの時間範囲を指定するには、[More Options] 領域をクリックして開き、[Time Range] ドロップダウン リストから時間範囲を選択します。

新しい時間範囲を追加するには、[...] ボタンをクリックします。詳細については、「時間範囲の設定」（P.8-15）を参照してください。

この設定は、事前に設定した時間にだけルールをアクティブにする場合に便利です。

ステップ 14　[OK] をクリックします。

ネットワーク アクセス許可の設定

ユーザが所定の接続のための認証を受けると、セキュリティ アプライアンスは許可を使用して、ユーザからのトラフィックをさらに制御できます。

この項では、次のトピックについて取り上げます。

TACACS+ 許可の設定

TACACS+ でネットワーク アクセス許可を実行するように、セキュリティ アプライアンスを設定できます。

認証ルールと許可ルールは相互に独立したものですが、許可ルールで一致した未認証トラフィックはすべて拒否されます。ユーザが許可を受けるには、まずセキュリティ アプライアンスに認証される必要があります。認証セッションが期限切れになっていない場合、所定の IP アドレスを持つユーザが認証を受ける必要があるのは、すべてのルールおよびタイプで 1 回だけです。このため、トラフィックが認証ステートメントに一致した場合でも許可が発生する可能性があります。

ユーザの認証が完了すると、セキュリティ アプライアンスは、一致するトラフィックの許可ルールをチェックします。トラフィックが許可ルールに一致した場合は、セキュリティ アプライアンスによりユーザ名が TACACS+ サーバに送信されます。TACACS+ サーバはセキュリティ アプライアンスに応答し、ユーザ プロファイルに基づいてそのトラフィックの許可または拒否を示します。セキュリティ アプライアンスは、その応答内の許可ルールを実施します。

ユーザに対するネットワーク アクセス許可の設定については、ご使用の TACACS+ サーバのマニュアルを参照してください。

TACACS+ 許可を設定するには、次の手順を実行します。

ステップ 1　許可するトラフィックの認証をイネーブルにします。詳細については、「ネットワーク アクセス認証の設定」（P.21-1）を参照してください。すでに認証をイネーブルにしてある場合は、次の手順に進みます。

ステップ 2　[Configuration] > [Firewall] > [AAA Rules] ペインから、[Add] > [Add Authorization Rule] を選択します。

[Add Authorization Rule] ダイアログボックスが表示されます。

ステップ 3　[Interface] ドロップダウン リストから、ルールを適用するインターフェイスを選択します。

ステップ 4　[Authorize] または [Do not Authorize] をクリックします。

たとえば、10.1.1.50 を除く 10.1.1.0/24 を許可する場合、2 つのルール（1 つには [Authorize] オプションを使用、もう 1 つには [Do not Authorize] オプションを使用）を作成します。ルールは必ず適切な順序に並べてください。たとえば、上記の [Do not Authorize] ルールを [Authorize] ルールよりも上に置き、10.1.1.50 からのトラフィックが最初に [Do not Authorize] ルールに一致するようにします。

ステップ 5　[AAA Server Group] ドロップダウン リストから、サーバ グループまたは LOCAL ユーザ データベースを選択します。

ステップ 6　（任意）AAA サーバをサーバ グループに追加するには、[Add Server] をクリックします。ユーザを LOCAL データベースに追加するには、[Add User] をクリックします。

サーバ グループとローカル ユーザ データベースの設定の詳細については、第 12 章「AAA サーバおよびユーザ アカウントの設定」を参照してください。

ステップ 7　[Source] フィールドで、送信元 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

任意の送信元アドレスを指定するには、**any** を入力します。

アドレスが複数ある場合はカンマで区切ります。

ステップ 8　[Destination] フィールドで、宛先 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

任意の宛先アドレスを指定するには、**any** を入力します。

アドレスが複数ある場合はカンマで区切ります。

ステップ 9　[Service] フィールドで、宛先サービスの IP サービス名または番号を入力するか、[...] ボタンをクリックしてサービスを選択します。

TCP または UDP のポート番号、あるいは ICMP サービス番号を指定する場合は、*プロトコル / ポート* を入力します。たとえば、TCP/8080 と入力します。

デフォルトでは、サービスは TCP です。

サービスが複数ある場合はカンマで区切ります。

ステップ 10　（任意）[Description] フィールドに説明を入力します。

ステップ 11　（任意）TCP または UDP の送信元サービスを指定するには、[More Options] 領域をクリックして開き、[Source Service] フィールドに TCP サービスまたは UDP サービスを入力します。

宛先サービスと送信元サービスは同じである必要があります。[Destination Service] フィールドをコピーし、[Source Service] フィールドに貼り付けます。

ステップ 12　（任意）ルールを非アクティブにするには、[More Options] 領域をクリックして開き、[Enable Rule] をオフにします。

この設定は、ルールを削除せずに無効にしたい場合に便利です。

ステップ 13　（任意）ルールの時間範囲を指定するには、[More Options] 領域をクリックして開き、[Time Range] ドロップダウン リストから時間範囲を選択します。

新しい時間範囲を追加するには、[...] ボタンをクリックします。詳細については、「時間範囲の設定」（P.8-15）を参照してください。

この設定は、事前に設定した時間にだけルールをアクティブにする場合に便利です。

ステップ 14　[OK] をクリックします。

RADIUS 許可の設定

認証が成功すると、RADIUS プロトコルは RADIUS サーバによって送信される access-accept メッセージでユーザ許可を返します。認証の設定の詳細については、「ネットワーク アクセス認証の設定」（P.21-1）を参照してください。

ネットワーク アクセスについてユーザを認証するようにセキュリティ アプライアンスを設定すると、RADIUS 許可も暗黙的にイネーブルになっています。したがって、この項では、セキュリティ アプライアンス上の RADIUS 許可の設定については取り上げません。ここでは、セキュリティ アプライアンスが RADIUS サーバから受信したアクセス リスト情報をどのように処理するかについて説明します。

アクセス リストをセキュリティ アプライアンスにダウンロードするように RADIUS サーバを設定できます。ユーザは、ユーザ固有のアクセス リストで許可された操作だけを許可されます。

（注）　アクセス ルールをすでに設定している場合、ユーザごとの上書き設定が、ユーザ固有のアクセス リストによる許可に対して次のような影響を与えることに注意してください（「高度なアクセス ルール設定」（1-7 ページ）を参照）。

- ユーザごとの上書き設定を使用しない場合、ユーザ セッションのトラフィックは、インターフェイス アクセス リストとユーザ固有のアクセス リストの両方によって許可される必要があります。
- ユーザごとの上書き設定を使用した場合、許可される内容は、ユーザ固有のアクセス リストによって決定されます。

この項では、Cisco Secure Access Control Server（ACS）およびサードパーティ RADIUS サーバを設定する方法について説明します。次の項目を取り上げます。

- 「ダウンロード可能なアクセス リストの機能と Cisco Secure ACS について」（P.21-8）
- 「ダウンロード可能なアクセス リストに関する Cisco Secure ACS の設定」（P.21-10）
- 「ダウンロード可能なアクセス リストに関する任意の RADIUS サーバの設定」（P.21-11）
- 「ダウンロード可能なアクセス リスト内のワイルドカード ネットマスク表現の変換」（P.21-11）

ダウンロード可能なアクセス リストの機能と Cisco Secure ACS について

ダウンロード可能なアクセス リストは、Cisco Secure ACS を使用して各サーバに適切なアクセス リストを提供する場合に最もスケーラブルな方法です。次の機能があります。

- 無制限のアクセス リスト サイズ：ダウンロード可能なアクセス リストは、完全なアクセス リストを Cisco Secure ACS からセキュリティ アプライアンスに転送するために必要な数の RADIUS パケットを使用して送信されます。
- アクセス リスト管理の簡素化および集中化：ダウンロード可能なアクセス リストにより、一度記述したアクセス リスト セットを多数のユーザ プロファイルまたはグループ プロファイルに適用することや、多数のセキュリティ アプライアンスに配布することができます。

この方法は、複数の Cisco Secure ACS ユーザまたはグループに適用する非常に大きいアクセス リスト セットがある場合に最適ですが、Cisco Secure ACS ユーザおよびグループの管理を簡素化できることから、アクセス リストのサイズを問わず有用です。

セキュリティ アプライアンスは、ダウンロード可能なアクセス リストを Cisco Secure ACS から次のプロセスで受信します。

1. セキュリティ アプライアンスがユーザ セッションのための RADIUS 認証要求パケットを送信します。
2. Cisco Secure ACS がそのユーザを正常に認証した場合、Cisco Secure ACS は、該当するダウンロード可能なアクセス リストの内部名が含まれた RADIUS access-accept メッセージを返します。Cisco IOS cisco-av-pair RADIUS VSA（ベンダー 9、属性 1）には、ダウンロード可能なアクセス リスト セットを特定する次の AV のペアが含まれています。

   ```
   ACS:CiscoSecure-Defined-ACL=acl-set-name
   ```

   acl-set-name はダウンロード可能なアクセス リストの内部名です。この名前は、Cisco Secure ACS 管理者がアクセス リストに割り当てた名前とアクセス リストが最後に変更された日時の組み合わせです。
3. セキュリティ アプライアンスはダウンロード可能なアクセス リストの名前を検査し、以前にその名前のダウンロード可能なアクセス リストを受信したことがあるかどうかを判別します。
   - セキュリティ アプライアンスが以前にその名前のダウンロード可能なアクセス リストを受信したことがある場合は、Cisco Secure ACS との通信は完了し、セキュリティ アプライアンスはアクセス リストをユーザ セッションに適用します。ダウンロード可能なアクセス リストの名前には最後に変更された日時が含まれているため、Cisco Secure ACS から送信された名前

と、以前にダウンロードしたアクセス リストの名前が一致するということは、セキュリティ アプライアンスはダウンロード可能なアクセス リストの最新バージョンを持っていることになります。

- セキュリティ アプライアンスが以前にその名前のダウンロード可能なアクセス リストを受信したことがない場合は、そのアクセス リストの古いバージョンを持っているか、そのアクセス リストのどのバージョンもダウンロードしたことがないことになります。いずれの場合でも、セキュリティ アプライアンスは、ダウンロード可能なアクセス リスト名を RADIUS 要求内のユーザ名として使用し、ヌル パスワード属性とともに RADIUS 認証要求を発行します。cisco-av-pair RADIUS VSA では、この要求に次の属性と値のペアも含まれます。

  ```
  AAA:service=ip-admission
  AAA:event=acl-download
  ```

  これに加えて、セキュリティ アプライアンスは Message-Authenticator 属性（IETF RADIUS 属性 80）で要求に署名します。

4. ダウンロード可能なアクセス リストの名前が含まれているユーザ名属性を持つ RADIUS 認証要求を受信すると、Cisco Secure ACS は Message-Authenticator 属性をチェックして要求を認証します。Message-Authenticator 属性がない場合、または正しくない場合、Cisco Secure ACS はその要求を無視します。Message-Authenticator 属性の存在により、ダウンロード可能なアクセス リスト名がネットワーク アクセスの不正取得に悪用されることが防止されます。Message-Authenticator 属性とその使用方法は、RFC 2869「RADIUS Extensions」で定義されています。この文書は、http://www.ietf.org で入手できます。

5. 要求されたアクセス リストの長さが約 4 KB 未満の場合、Cisco Secure ACS はそのアクセス リストを含めた access-accept メッセージで応答します。メッセージには他の必須属性を含める必要があるので、1 つの access-accept メッセージに収まるアクセス リストの最大サイズは 4 KB よりわずかに小さくなります。

   Cisco Secure ACS はダウンロード可能なアクセス リストを cisco-av-pair RADIUS VSA で送信します。アクセス リストは、一連の属性と値のペアという形式をとります。各ペアには ACE が 1 つ含まれ、シリアル番号が付けられます。

   ```
   ip:inacl#1=ACE-1
   ip:inacl#2=ACE-2
   .
   .
   .
   ip:inacl#n=ACE-n
   ```

   属性と値のペアの例を次に示します。

   ```
   ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
   ```

6. 要求されたアクセス リストの長さが約 4 KB を超える場合、Cisco Secure ACS は、上記の形式のアクセス リストの一部が含まれた access-challenge メッセージで応答します。メッセージには、State 属性（IETF RADIUS 属性 24）も含まれています。State 属性には、Cisco Secure ACS がダウンロードの進捗を追跡するために使用する制御データが含まれています。Cisco Secure ACS は、RADIUS メッセージの最大サイズ以内で可能な限り多数の完全な属性と値のペアを cisco-av-pair RADIUS VSA に含めます。

   セキュリティ アプライアンスはアクセス リストの一部を受信すると、それを保存し、新しい access-request メッセージで応答します。これには、ダウンロード可能なアクセス リストを求める最初の要求と同じ属性と、access-challenge メッセージで受信した State 属性のコピーが含まれています。

   これは、Cisco Secure ACS がアクセス リストの最後の部分を access-accept メッセージで送信するまで続行されます。

ダウンロード可能なアクセス リストに関する Cisco Secure ACS の設定

Cisco Secure ACS 上のダウンロード可能なアクセス リストを共有プロファイル コンポーネントとして設定し、そのアクセス リストをグループまたは個々のユーザに割り当てることができます。

アクセス リストの定義には、拡張 **access-list** コマンドと同様の 1 つまたは複数の セキュリティ アプライアンス コマンドを設定します。ただし、次のプレフィックスは不要です。

access-list *acl_name* **extended**

Cisco Secure ACS バージョン 3.3 上のダウンロード可能なアクセス リスト定義の例を次に示します。

```
+-------------------------------------------+
| Shared profile Components                 |
|                                           |
|      Downloadable IP ACLs Content         |
|                                           |
| Name:    acs_ten_acl                      |
|                                           |
|      ACL Definitions                      |
|                                           |
| permit tcp any host 10.0.0.254            |
| permit udp any host 10.0.0.254            |
| permit icmp any host 10.0.0.254           |
| permit tcp any host 10.0.0.253            |
| permit udp any host 10.0.0.253            |
| permit icmp any host 10.0.0.253           |
| permit tcp any host 10.0.0.252            |
| permit udp any host 10.0.0.252            |
| permit icmp any host 10.0.0.252           |
| permit ip any any                         |
+-------------------------------------------+
```

ダウンロード可能なアクセス リストを作成する方法、およびそれらをユーザと関連付ける方法の詳細については、ご使用のバージョンの Cisco Secure ACS のガイドを参照してください。

セキュリティ アプライアンス上では、ダウンロードされたアクセス リストの名前は次のようになります。

```
#ACSACL#-ip-acl_name-number
```

acl_name 引数は Cisco Secure ACS で定義された名前（上記の例では acs_ten_acl）、*number* は Cisco Secure ACS が生成した固有のバージョン ID です。

セキュリティ アプライアンス上にダウンロードされたアクセス リストは、次の行で構成されます。

```
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit ip any any
```

ダウンロード可能なアクセス リストに関する任意の RADIUS サーバの設定

ユーザ固有のアクセス リストを Cisco IOS RADIUS cisco-av-pair VSA（ベンダー 9、属性 1）でセキュリティ アプライアンスに送信するように、Cisco IOS RADIUS VSA をサポートする任意の RADIUS サーバを設定できます。

cisco-av-pair VSA では、**access-list extended** コマンドと同様の 1 つまたは複数の ACE を設定してください。ただし、次のコマンド プレフィックスは、

access-list *acl_name* **extended**

次のテキストに置き換えます。

ip:inacl#*nnn***=**

nnn 引数は、0 ～ 999999999 の番号で、セキュリティ アプライアンス上に設定するコマンド文の順序を指定します。このパラメータを省略すると、順番は 0 となり、cisco-av-pair RADIUS VSA 内部の ACE の順序が使用されます。

RADIUS サーバ上の cisco-av-pair VSA に対して設定されている必要のあるアクセス リスト定義の例を次に示します。

```
ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#99=deny tcp any any
ip:inacl#2=permit udp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#100=deny udp any any
ip:inacl#3=permit icmp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
```

cisco-av-pair 属性で送信されるアクセス リストをユーザごとに固有にする方法については、ご使用の RADIUS サーバのマニュアルを参照してください。

セキュリティ アプライアンス上では、ダウンロードされたアクセス リストの名前は次のようになります。

AAA-user-*username*

username 引数は、認証を受けるユーザの名前です。

セキュリティ アプライアンス上にダウンロードされたアクセス リストは、次の行で構成されます。RADIUS サーバ上で指定された番号に基づいた順序になっています。

```
access-list  AAA-user-bcham34-79AD4A08 permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 permit udp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 permit icmp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 deny tcp any any
access-list  AAA-user-bcham34-79AD4A08 deny udp any any
```

ダウンロードされたアクセス リストの「access-list」という単語と名前の間には、2 個のスペースがあります。これらのスペースにより、ダウンロードされたアクセス リストとローカルのアクセス リストが区別されます。この例では、「79AD4A08」はセキュリティ アプライアンスによって作成されたハッシュ値で、RADIUS サーバ上でアクセス リスト定義がいつ変更されたかを判別するために役立ちます。

ダウンロード可能なアクセス リスト内のワイルドカード ネットマスク表現の変換

RADIUS サーバを使用して、ダウンロード可能なアクセス リストを Cisco VPN 3000 Series Concentrator およびセキュリティ アプライアンスに提供する場合は、ワイルドカード ネットマスク表現を標準のネットマスク表現に変換するようにセキュリティ アプライアンスを設定しなければならない場合があります。これは、Cisco VPN 3000 Series Concentrator はワイルドカード ネットマスク表現をサポートしますが、セキュリティ アプライアンスは標準のネットマスク表現しかサポートしないためです。これらの違いは、RADIUS サーバ上のダウンロード可能なアクセス リストを設定する方法に影響しますが、ワイルドカード ネットマスク表現を変換するようにセキュリティ アプライアンスを設

定することで、その影響を最小限に抑えることができます。ワイルドカード ネットマスク表現の変換により、RADIUS サーバ上のダウンロード可能なアクセス リストのコンフィギュレーションを変更することなく、Cisco VPN 3000 Series Concentrator 用に記述されたダウンロード可能なアクセス リストをセキュリティ アプライアンスで使用できます。

[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] > [Add/Edit AAA Server] ダイアログボックスで使用可能な [ACL Netmask Convert] オプションを使用して、アクセス リスト ネットマスク変換をサーバごとに設定します。RADIUS サーバの設定方法の詳細については、第 12 章「AAA サーバおよびユーザ アカウントの設定」を参照してください。

ネットワーク アクセスのアカウンティングの設定

セキュリティ アプライアンスは、セキュリティ アプライアンスを通過する任意の TCP トラフィックまたは UDP トラフィックについてのアカウンティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。そのトラフィックも認証されている場合、AAA サーバはユーザ名でアカウンティング情報を保持できます。トラフィックが認証済みでない場合、AAA サーバは IP アドレスによってアカウンティング情報を保持できます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、セキュリティ アプライアンスを通過するセッションのバイト数、使用されたサービス、および各セッションの継続時間などの情報が含まれます。

アカウンティングを設定するには、次の手順を実行します。

ステップ 1　ユーザごとのアカウンティング データを提供するようにセキュリティ アプライアンスを設定する場合は、認証をイネーブルにする必要があります。詳細については、「ネットワーク アクセス認証の設定」（P.21-1）を参照してください。IP アドレスごとのアカウンティング データを提供するようにセキュリティ アプライアンスを設定する場合は、認証をイネーブルにする必要はありません。次のステップに進みます。

ステップ 2　[Configuration] > [Firewall] > [AAA Rules] ペインから、[Add] > [Add Accounting Rule] を選択します。

[Add Accounting Rule] ダイアログボックスが表示されます。

ステップ 3　[Interface] ドロップダウン リストから、ルールを適用するインターフェイスを選択します。

ステップ 4　[Account] または [Do not Account] をクリックします。

たとえば、10.1.1.50 を除く 10.1.1.0/24 をアカウンティングする場合、2 つのルール（1 つには [Account] オプションを使用、もう 1 つには [Do not Account] オプションを使用）を作成します。ルールは必ず適切な順序に並べてください。たとえば、上記の [Do not Account] ルールを [Account] ルールよりも上に置き、10.1.1.50 からのトラフィックが最初に [Do not Account] ルールに一致するようにします。

ステップ 5　[AAA Server Group] ドロップダウン リストから、サーバ グループまたは LOCAL ユーザ データベースを選択します。

ステップ 6　（任意）AAA サーバをサーバ グループに追加するには、[Add Server] をクリックします。ユーザを LOCAL データベースに追加するには、[Add User] をクリックします。

サーバ グループとローカル ユーザ データベースの設定の詳細については、第 12 章「AAA サーバおよびユーザ アカウントの設定」を参照してください。

ステップ 7　[Source] フィールドで、送信元 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

任意の送信元アドレスを指定するには、**any** を入力します。

アドレスが複数ある場合はカンマで区切ります。

ステップ 8　[Destination] フィールドで、宛先 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

任意の宛先アドレスを指定するには、**any** を入力します。

アドレスが複数ある場合はカンマで区切ります。

ステップ 9　[Service] フィールドで、宛先サービスの IP サービス名または番号を入力するか、[...] ボタンをクリックしてサービスを選択します。

TCP または UDP のポート番号、あるいは ICMP サービス番号を指定する場合は、*プロトコル / ポート* を入力します。たとえば、TCP/8080 と入力します。

デフォルトでは、サービスは TCP です。

サービスが複数ある場合はカンマで区切ります。

ステップ 10　（任意）[Description] フィールドに説明を入力します。

ステップ 11　（任意）TCP または UDP の送信元サービスを指定するには、[More Options] 領域をクリックして開き、[Source Service] フィールドに TCP サービスまたは UDP サービスを入力します。

宛先サービスと送信元サービスは同じである必要があります。[Destination Service] フィールドをコピーし、[Source Service] フィールドに貼り付けます。

ステップ 12　（任意）ルールを非アクティブにするには、[More Options] 領域をクリックして開き、[Enable Rule] をオフにします。

この設定は、ルールを削除せずに無効にしたい場合に便利です。

ステップ 13　（任意）ルールの時間範囲を指定するには、[More Options] 領域をクリックして開き、[Time Range] ドロップダウン リストから時間範囲を選択します。

新しい時間範囲を追加するには、[...] ボタンをクリックします。詳細については、「時間範囲の設定」（P.8-15）を参照してください。

この設定は、事前に設定した時間にだけルールをアクティブにする場合に便利です。

ステップ 14　[OK] をクリックします。

MAC アドレスによるトラフィックの認証と許可の免除

セキュリティ アプライアンスは、特定の MAC アドレスからのトラフィックの認証および許可を免除できます。たとえば、セキュリティ アプライアンスが特定のネットワークから発信される TCP トラフィックを認証し、特定のサーバからの未認証の TCP 接続は許可する場合、MAC 免除規則を使用すると、この規則で指定したサーバからのすべてのトラフィックに対して認証および許可が免除されます。

この機能は、認証プロンプトに応答できない IP 電話などのデバイスを免除する場合に特に便利です。

MAC アドレスを使用してトラフィックの認証および許可を免除するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [AAA Rules] ペインから、[Add] > [Add MAC Exempt Rule] を選択します。

[Add MAC Exempt Rule] ダイアログボックスが表示されます。

ステップ 2　[Action] ドロップダウン リストから、[MAC Exempt] または [No MAC Exempt] を選択します。

たとえば、00a0.c95d.0000 ffff.ffff.0000 は免除するが、00a0.c95d.0282 ffff.ffff.ffff は免除対象外とする場合、2 つのルール（1 つには [MAC Exempt] オプションを使用、もう 1 つには [No MAC Exempt] オプションを使用）を作成します。ルールは必ず適切な順序に並べてください。たとえば、上記の [No MAC Exempt] ルールを [MAC Exempt] ルールよりも上に置き、00a0.c95d.0282 ffff.ffff.ffff からのトラフィックが最初に [No MAC Exempt] ルールに一致するようにします。

ステップ 3　[MAC Address] フィールドに、送信元の MAC アドレスを 12 桁の 16 進数の形式（nnnn.nnnn.nnnn）で入力します。

ステップ 4　[MAC Mask] フィールドに、MAC アドレスの中で照合に使用される部分を入力します。

たとえば、ffff.ffff.ffff は完全に MAC アドレスと一致します。ffff.ffff.0000 は最初の 8 桁だけ一致します。

ステップ 5　[OK] をクリックします。

高度な AAA 機能の設定

この項では、拡張 AAA 機能の設定方法について説明します。次の項目を取り上げます。

- 「HTTPS を使用した HTTP 認証のクレデンシャルの交換」（P.21-14）
- 「インタラクティブ認証ルールの追加」（P.21-15）

HTTPS を使用した HTTP 認証のクレデンシャルの交換

セキュリティ アプライアンス は、安全に HTTP 認証を行う方法を提供します。HTTP 認証を保護しないと、クライアントからセキュリティ アプライアンスに送信されるユーザ名およびパスワードは、クリア テキストとして渡されます。Secure HTTP 機能を使用すると、Web クライアントとセキュリティ アプライアンスとの間で HTTPS を使用したユーザ名とパスワードの交換がイネーブルになります。

この機能をイネーブルにすると、ユーザが HTTP の使用時に認証を必要とする場合は、セキュリティ アプライアンスが HTTP ユーザを HTTPS プロンプトにリダイレクトします。正常に認証されると、ユーザはセキュリティ アプライアンスにより元の HTTP URL にリダイレクトされます。

セキュアな Web クライアント認証では、次の制限事項があります。

- 同時に行うことができる HTTPS 認証セッションは、最大 16 個です。16 個の HTTPS 認証プロセスがすべて実行されている場合、認証を必要とする新しい接続は失敗します。
- 認証の絶対タイムアウト値を 0 に設定すると（「グローバル タイムアウトの設定」（P.27-23）の [Authentication absolute] オプションを参照）、HTTPS 認証が機能しない場合があります。HTTPS 認証を受けた後、ブラウザが複数の TCP 接続を開始して Web ページのロードを試みると、最初の接続はそのまま許可されますが、後続の接続に対しては認証が発生します。その結果、ユーザが認証ページに正しいユーザ名とパスワードを毎回入力しても、繰り返し認証ページが表示されます。これを回避するには、認証の絶対タイムアウトを 1 秒に設定します。ただし、この回避策では、同じ送信元 IP アドレスからアクセスした認証されていないユーザがファイアウォールを通過できる期間が 1 秒間発生します。

- HTTPS 認証は SSL ポート 443 上で実行されるため、HTTP クライアントから HTTP サーバへのトラフィックをポート 443 でブロックするというアクセス ルールは設定しないようにしてください。また、ポート 80 上の Web トラフィックに対してスタティック PAT を設定する場合は、SSL ポートに対してもスタティック PAT を設定する必要があります。

Web クライアントのセキュアな認証をイネーブルにする手順は、次のとおりです。

ステップ 1　[Configuration] > [Firewall] > [AAA Rules] ペインから、ペインの下部にある [Advanced] ボタンをクリックします。

[AAA Rules Advanced Options] ダイアログボックスが表示されます。

ステップ 2　[Enable Secure HTTP] をオンにします。

ステップ 3　[OK] をクリックします。

インタラクティブ認証ルールの追加

HTTP のデフォルトでは、セキュリティ アプライアンスは基本 HTTP 認証を使用します。HTTPS の場合、セキュリティ アプライアンスは同様のカスタム ログイン画面を生成します。[Configuration] > [Security Policy] > [AAA Rules] > [Advanced AAA Configuration] > [Add Interactive Authentication] ダイアログボックスを使用して、ユーザがユーザ名とパスワードを入力できる内部 Web ページにセキュリティ アプライアンスがユーザをリダイレクトするように設定できます。

HTTP および HTTPS 認証のリダイレクト方式をイネーブルにした場合、セキュリティ アプライアンスでの直接認証も自動的にイネーブルになります。HTTP、HTTPS、Telnet、または FTP によるセキュリティ アプライアンスの通過は許可しないが他のタイプのトラフィックは認証する場合は、直接認証が役立ちます。他のトラフィックが許可される前に、ユーザは HTTP または HTTPS を使用するセキュリティ アプライアンスを直接認証できます。通過トラフィックに基本 HTTP 認証を引き続き使用する場合は、直接認証を独立して設定できます。直接認証のログイン ページにアクセスするには、次の URL のいずれかを入力します。

http://*interface_ip*[:*port*]**/netaccess/connstatus.html**
https://*interface_ip*[:*port*]**/netaccess/connstatus.html**

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、セキュリティ アプライアンスでの直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

インタラクティブ認証ルールを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [AAA Rules] ペインから、ペインの下部にある [Advanced] ボタンをクリックします。

[AAA Rules Advanced Options] ダイアログボックスが表示されます。

ステップ 2　[Interactive Authentication] 領域で、[Add] をクリックします。

ステップ 3　[Protocol] メニューから、[HTTP] または [HTTPS] を選択します。

HTTP と HTTPS の両方のリスナーをイネーブルにするには、2 つの別のルールを作成する必要があります。

ステップ 4　[Interface] メニューから、リスナーをイネーブルにするインターフェイスを選択します。

ステップ 5　[Port] メニューで、共通ポートを選択するか、またはリスンするポート番号を入力します。

HTTP のデフォルトは 80、HTTPS のデフォルトは 443 です。

ステップ 6　通過トラフィックを認証用のリスニング ポートにリダイレクトするには、[Redirect network users for authentication requests] チェックボックスをオンにします。

このチェックボックスをオンにしない場合、直接認証だけがイネーブルになります。

ステップ 7　[OK] をクリックします。

仮想アクセスの設定

この項では、Telnet を使用して直接認証を設定する方法、または仮想 HTTP サーバを基本 HTTP 認証と一緒に使用できるように設定する方法について説明します。この項では、次のトピックについて取り上げます。

- 「Telnet による直接認証のイネーブル化」（P.21-16）
- 「仮想 HTTP の設定」（P.21-17）

Telnet による直接認証のイネーブル化

任意のプロトコルまたはサービスのネットワーク アクセス認証を設定できますが（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、HTTP、Telnet、または FTP のみで直接認証することもできます。ユーザはまずこれらのサービスのいずれかで認証を行ってから、認証を要求する他のトラフィックの通過を許可する必要があります。HTTP、Telnet、または FTP のセキュリティ アプライアンスの通過を許可せず、その他のタイプのトラフィックを認証する場合は、セキュリティ アプライアンス上で設定された所定の IP アドレスにユーザが Telnet で接続し、セキュリティ アプライアンスによって Telnet プロンプトが表示されるように、仮想 Telnet を設定できます。

仮想 Telnet アドレスへの Telnet アクセスの認証を、AAA 認証ルールを使用して認証するその他のサービスに対する認証と同様に設定する必要があります（「ネットワーク アクセス認証の設定」（P.21-1）を参照）。

認証が済んでいないユーザが仮想 Telnet IP アドレスに接続すると、ユーザはユーザ名とパスワードを求められ、その後 AAA サーバにより認証されます。認証されると、ユーザには「Authentication Successful.」というメッセージが表示されます。それ以降、ユーザは認証を必要とする他のサービスに正常にアクセスできます。

着信ユーザ（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセス ルールに、宛先インターフェイスとして仮想 Telnet アドレスを追加する必要もあります。さらに、NAT が必要ない場合であっても、仮想 Telnet IP アドレスに対するスタティック NAT ルールを追加する必要があります。通常は、アイデンティティ NAT ルールが使用されます（アドレスをそれ自身に変換）。

発信ユーザについては、トラフィックに明示的な許可がありますが、内部インターフェイスにアクセス ルールを適用する場合は、必ず仮想 Telnet アドレスへのアクセスを許可する必要があります。スタティック NAT ルールは必要ありません。

セキュリティ アプライアンスからログアウトするには、仮想 Telnet IP アドレスに再接続します。ログアウトするように求められます。

仮想 Telnet サーバを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Advanced] > [Virtual Access] ペインで、[Enable Telnet Server] をオンにします。

ステップ 2　[Virtual Telnet Server] フィールドで、Telnet 接続する対象の IP アドレスを入力します。

このアドレスは必ず、セキュリティ アプライアンスにルーティングされる未使用のアドレスにしてください。たとえば、外部にアクセスするときに内部アドレス用の NAT を実行し、仮想 Telnet サーバへの外部アクセスを提供する場合、仮想 Telnet サーバ アドレスにグローバル NAT アドレスのいずれかを使用できます。

ステップ 3　[OK] をクリックします。

仮想 HTTP の設定

セキュリティ アプライアンスで HTTP 認証を使用する場合（「ネットワーク アクセス認証の設定」（P.21-1）を参照）、セキュリティ アプライアンスでは、基本 HTTP 認証がデフォルトで使用されます。この認証方式を、セキュリティ アプライアンスが HTTP 接続をセキュリティ アプライアンス自身が生成した Web ページにリダイレクトするように変更できます（「インタラクティブ認証ルールの追加」（P.21-15）を参照）。

ただし、基本 HTTP 認証を引き続き使用する場合、HTTP 認証をカスケードするには仮想 HTTP サーバが必要になることがあります。

セキュリティ アプライアンスに加えて宛先 HTTP サーバで認証が必要な場合は、virtual http コマンドを使用すると、セキュリティ アプライアンス（AAA サーバ経由）の認証と HTTP サーバの認証を個別に行うことができます。仮想 HTTP を使用しない場合は、セキュリティ アプライアンスに対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。AAA サーバと HTTP サーバでユーザ名とパスワードが異なる場合、HTTP 認証は失敗します。

この機能を使用すると、AAA 認証を必要とする HTTP 接続がすべて、セキュリティ アプライアンス上の仮想 HTTP サーバにリダイレクトされます。セキュリティ アプライアンスにより、AAA サーバのユーザ名とパスワードの入力を求めるプロンプトが表示されます。AAA サーバがユーザを認証すると、セキュリティ アプライアンスは HTTP 接続を元のサーバにリダイレクトして戻しますが、AAA サーバのユーザ名とパスワードは含めません。HTTP パケットにユーザ名とパスワードが含まれていないため、HTTP サーバによりユーザに HTTP サーバのユーザ名とパスワードの入力を求めるプロンプトが別途表示されます。

着信ユーザ（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセス ルールに、宛先インターフェイスとして仮想 HTTP アドレスを追加する必要もあります。さらに、NAT が必要ない場合であっても、仮想 HTTP IP アドレスに対するスタティック NAT ルールを追加する必要があります。通常は、アイデンティティ NAT ルールが使用されます（アドレスをそれ自身に変換）。

発信ユーザについては、トラフィックに明示的な許可がありますが、内部インターフェイスにアクセス ルールを適用する場合は、必ず仮想 HTTP アドレスへのアクセスを許可する必要があります。スタティック NAT ルールは必要ありません。

仮想 HTTP サーバを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Advanced] > [Virtual Access] ペインで、[Enable HTTP Server] をオンにします。

ステップ 2　[Virtual HTTP Server] フィールドで、仮想 HTTP サーバの IP アドレスを入力します。

このアドレスは必ず、セキュリティ アプライアンスにルーティングされる未使用のアドレスにしてください。たとえば、外部にアクセスするときに内部アドレスに NAT を実行し、仮想 HTTP サーバに外部からアクセスする場合は、仮想 HTTP サーバ アドレスにグローバル NAT アドレスを 1 つ使用します。

ステップ 3　（任意）ユーザに HTTP 接続をセキュリティ アプライアンスにリダイレクトする必要があることを通知するには、[Display redirection warning] をオンにします。

このオプションは、リダイレクトが自動的に行われないテキストベースのブラウザにのみ適用されます。

ステップ 4　[OK] をクリックします。

CHAPTER 22

フィルタ ルールの設定

ここでは、次の内容について説明します。

URL フィルタリング

フィルタリングは、セキュリティの高いネットワークからセキュリティの低いネットワークに発信される接続要求に対して適用できます。ACL を使用して特定のコンテンツ サーバに対する発信アクセスを禁止することはできますが、サイズおよびインターネットのダイナミックな性質により、このような手段で使用方法を管理することは困難です。次のいずれかのインターネット フィルタリング製品で稼働する別途サーバを使用することで、設定を簡素化し、セキュリティ アプライアンス のパフォーマンスを向上できます。

- HTTP、HTTPS、および FTP フィルタリング用の Websense Enterprise
- HTTP のフィルタリング専用の Secure Computing SmartFilter （Sentian の一部のバージョンでは HTTPS をサポートしていますが、セキュリティ アプライアンスでは、Sentian での HTTP のフィルタリングだけをサポートしています）

外部サーバを使用するときは セキュリティ アプライアンス のパフォーマンスはほとんど影響を受けませんが、フィルタリング サーバが セキュリティ アプライアンス から離れた場所にある場合には、Web サイトまたは FTP サーバへのアクセス時間が大幅に長くなることがあります。

フィルタリングがイネーブルで、接続要求を セキュリティ アプライアンス 経由で転送すると、その要求はコンテンツ サーバとフィルタリング サーバに同時に送信されます。フィルタリング サーバによって接続が許可されると、セキュリティ アプライアンス はコンテンツ サーバからの応答を発信元のクライアントに転送します。フィルタリング サーバが接続を拒否した場合、セキュリティ アプライアンス は応答を廃棄し、接続が成功しなかったことを示すメッセージまたはリターン コードを送信します。

セキュリティ アプライアンス上でユーザ認証がイネーブルの場合、セキュリティ アプライアンス はフィルタリング サーバにユーザ名も送信します。フィルタリング サーバは、ユーザ固有のフィルタリング設定を使用したり、使用方法に関する高度なレポートを提供したりすることができます。

ここでは、次の内容について説明します。

URL フィルタリングの設定

外部フィルタリング サーバを使用するフィルタリングをイネーブルにするための手順を次にまとめます。

ステップ 1　[Configuration] > [Firewall] > [URL Filter Servers] に移動し、外部フィルタリング サーバを指定します。「URL Filtering Servers」（P.22-2）を参照してください。

ステップ 2　（任意）コンテンツ サーバからの応答をバッファに格納します。「高度な URL フィルタリング」（P.22-4）を参照してください。

ステップ 3　（任意）コンテンツ サーバのアドレスをキャッシュしてパフォーマンスを向上させます。「高度な URL フィルタリング」（P.22-4）を参照してください。

ステップ 4　[Configuration] > [Firewall] > [Filter Rules] に移動し、フィルタ ルールを設定します。「Filter Rules」（P.22-5）を参照してください。

ステップ 5　外部フィルタリング サーバを設定します。詳細については、次の Web サイトを参照してください。

- http://www.websense.com
- http://www.securecomputing.com

URL Filtering Servers

[URL Filtering Servers] ペインでは、使用する外部フィルタ サーバを指定できます。コンテキストごとに最大 4 つの同じタイプのフィルタリング サーバを指定できます。シングル モードでは、最大 16 台の同じタイプのフィルタリング サーバが許容されます。セキュリティ アプライアンスは、1 つのサーバが応答するまで、それらのサーバを順番に使用します。コンフィギュレーション内に設定できるサーバのタイプは、1 つだけ（Websense または Secure Computing SmartFilter）です。

（注）　HTTP、HTTPS、または FTP フィルタリング ルールのフィルタリングを設定する前に、フィルタリング サーバを追加する必要があります。

フィールド

[URL Filtering Server Type] 領域には次のフィールドがあります。

- [Websense]：Websense URL フィルタリング サーバをイネーブルにします。
- [Secure Computing SmartFilter]：Secure Computing SmartFilter URL フィルタリング サーバをイネーブルにします。
- [Secure Computing SmartFilter Port]：Secure Computing SmartFilter ポートを指定します。デフォルト値は 4005 です。

[URL Filtering Servers] 領域には次のフィールドがあります。

- [Interface]：フィルタリング サーバに接続しているインターフェイスを表示します。
- [IP Address]：フィルタリング サーバの IP アドレスを表示します。
- [Timeout]：フィルタリング サーバへの要求がタイムアウトになってからの秒数を表示します。
- [Protocol]：フィルタリング サーバとの通信に使用されるプロトコルを表示します。
- [TCP Connections]：URL フィルタリング サーバと通信できる TCP 接続の最大数を表示します。

- [Add] : Websense または Secure Computing SmartFilter を選択したかどうかにより、新しいフィルタリング サーバを追加します。詳細については、次のトピックを参照してください。
  - 「Websense URL フィルタリングに関するパラメータの追加と編集」（P.22-3）
  - 「Secure Computing SmartFilter URL フィルタリングに関するパラメータの追加と編集」（P.22-4）
- [Insert Before] : 現在選択しているサーバより優先順位の高い位置に新しいフィルタリング サーバを追加します。
- [Insert After] : 現在選択しているサーバより優先順位の低い位置に新しいフィルタリング サーバを追加します。
- [Edit] : 選択したフィルタリング サーバのパラメータを変更できます。
- [Delete] : 選択したフィルタリング サーバを削除します。

このペインで次のアクションを実行できます。

- [Advanced] : バッファリング キャッシング、長い URL のサポートなど、高度なフィルタリング パラメータを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「高度な URL フィルタリング」（P.22-4）

「Filter Rules」（P.22-5）

Websense URL フィルタリングに関するパラメータの追加と編集

- [Interface] : URL フィルタリング サーバの接続を行うインターフェイスを指定します。
- [IP Address] : URL フィルタリング サーバの IP アドレスを指定します。
- [Timeout] : フィルタリング サーバへの要求がタイムアウトになってからの秒数を指定します。
- [Protocol] 領域
  - [TCP 1] : Websense URL フィルタリング サーバとの通信に TCP バージョン 1 を使用します。
  - [TCP 4] : Websense URL フィルタリング サーバとの通信に TCP バージョン 4 を使用します。
  - [UDP 4] : Websense URL フィルタリング サーバとの通信に UDP バージョン 4 を使用します。
- [TCP Connections] : URL フィルタリング サーバと通信できる TCP 接続の最大数を指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Secure Computing SmartFilter URL フィルタリングに関するパラメータの追加と編集

- [Interface] : URL フィルタリング サーバの接続を行うインターフェイスを指定します。
- [IP Address] : URL フィルタリング サーバの IP アドレスを指定します。
- [Timeout] : フィルタリング サーバへの要求がタイムアウトになってからの秒数を指定します。
- [Protocol] 領域
  - [TCP] : Secure Computing SmartFilter URL フィルタリング サーバとの通信に TCP を使用します。
  - [UDP] : Secure Computing SmartFilter URL フィルタリング サーバとの通信に UDP を使用します。

[TCP Connections] : URL フィルタリング サーバと通信できる TCP 接続の最大数を指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

高度な URL フィルタリング

フィールド

[URL Cache Size] 領域

ユーザがサイトにアクセスすると、フィルタリング サーバはセキュリティ アプライアンスに対して、サーバ アドレスを一定時間キャッシュすることを許可できます。ただし、そのアドレスでホストされているサイトはいずれも、常に許可されるカテゴリに属している必要があります。これにより、そのユーザがそのサーバに再度アクセスするか、別のユーザがそのサーバにアクセスしたときに、セキュリティ アプライアンスがフィルタリング サーバに再度照会する必要がなくなります。

（注） キャッシュされた IP アドレス要求は、フィルタリング サーバに渡されず、記録もされません。そのため、このアクティビティはどのレポートにも表示されません。

- [Enable caching based on]：指定した基準に基づいて、キャッシングをイネーブルにします。

- [Destination Address] : URL 宛先アドレスに基づいてエントリをキャッシュします。このモードは、Websense サーバ上ですべてのユーザが同じ URL フィルタリング ポリシーを共有する場合に選択します。
  - [Source/Destination Address] : URL 要求を開始した送信元アドレスと、URL 宛先アドレスの両方に基づいてエントリをキャッシュします。このモードは、ユーザがサーバ上で同じ URL フィルタリング ポリシーを共有していない場合に選択します。
  - [Cache size] : キャッシュのサイズを指定します。

[URL Buffer Size] 領域

ユーザがコンテンツ サーバへの接続要求を発行した場合、その要求は、セキュリティ アプライアンスによって、コンテンツ サーバとフィルタリング サーバの両方に同時に送信されます。フィルタリング サーバがコンテンツ サーバより早く応答しなかった場合、サーバ応答はドロップされます。これにより、Web クライアント側の視点で Web サーバ応答が表示されます。これは、クライアントが要求を再発行する必要があるためです。

HTTP 応答バッファをイネーブルにすると、Web コンテンツ サーバからの応答はバッファリングされ、フィルタリング サーバによって接続が許可された場合に、要求クライアントに転送されます。これにより、バッファリングしない場合に発生する可能性のある遅延が回避されます。

- [Enable buffering] : 要求のバッファリングをイネーブルにします。
  - [Number of 1550-byte buffers] : 1550 バイト バッファの数を指定します。1 ～ 128 の範囲の値を指定できます。
- [Long URL Support] 領域

  デフォルトでは、セキュリティ アプライアンスは、1159 文字を超える HTTP URL を長い URL と見なします。Websense サーバの場合、最大長を増加できます。
  - [Use Long URL] : Websense フィルタリング サーバの長い URL をイネーブルにします。
  - [Maximum Long URL Size] : URL の最大許容長を 4 KB を上限として指定します。
  - [Memory Allocated for Long URL] : 長い URL に割り当てるメモリを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Filter Rules

[Filter Rules] ペインには設定済みのフィルタ ルールが表示され、新しいフィルタ ルールを追加、または既存のルールを変更するためのオプションが提供されます。フィルタ ルールでは、適用するフィルタリングのタイプと、適用先となるトラフィックの種類が指定されます。

（注）　HTTP、HTTPS、または FTP フィルタ ルールを追加する前に、URL フィルタリング サーバをイネーブルにする必要があります。URL フィルタリング サーバをイネーブルにするには、[Configuration] > [Firewall] > [URL Filtering Servers] ペインを使用します。詳細については、「URL フィルタリング」（P.22-1）を参照してください。

利点

[Filter Rules] ウィンドウでは、現在セキュリティ アプライアンス上に設定されているフィルタ ルールについての情報が表示されます。また、フィルタ ルールを追加または変更し、ウィンドウに表示される詳細の量の増減に使用できるボタンも提供されます。

フィルタリングにより、セキュリティ ポリシーでセキュリティ アプライアンスの通過を許可するトラフィックを自在に制御できます。アクセスを全面的にブロックする代わりに、ActiveX オブジェクトや Java アプレットなど、特定の状況でセキュリティ上の脅威をもたらす可能性のある特定の不適切なオブジェクトを HTTP トラフィックから取り除くことができます。また、URL フィルタリングを使用して、Secure Computing SmartFilter や Websense などの外部フィルタリング サーバに特定のトラフィックを誘導することもできます。これらのサーバは、セキュリティ ポリシーで指定されている特定のサイトまたは特定のタイプのサイトに向かうトラフィックをブロックできます。

URL フィルタリングは CPU に大きな負荷がかかるため、外部フィルタリング サーバを使用することにより、他のトラフィックのスループットに影響を与えることがなくなります。ただし、ネットワークの速度および URL フィルタリング サーバのキャパシティによっては、フィルタ対象のトラフィックの最初の接続に必要な時間が著しく長くなる場合もあります。

フィールド

- [No]：ルールの数値識別子。数値の順序でルールが適用されます。
- [Source]：フィルタリング アクションが適用されるソース ホストまたはネットワーク。
- [Destination]：フィルタリング アクションが適用される宛先ホストまたはネットワーク。
- [Service]：フィルタリング アクションが適用されるプロトコルまたはサービスを指定します。
- [Action]：適用するフィルタリング アクションのタイプ。
- [Options]：特定のアクションに対してイネーブルになっているオプションを示します。
- [Add]：追加できるフィルタ ルールのタイプを表示します。ルール タイプをクリックすると、指定されたフィルタ ルール タイプの [Add Filter Rule] ダイアログボックスが開きます。
  - Add Filter ActiveX Rule
  - Add Filter Java Rule
  - Add Filter HTTP Rule
  - Add Filter HTTPS Rule
  - Add Filter FTP Rule
- [Edit]：選択したフィルタリング ルールを編集するための [Edit Filter Rule] ダイアログボックスを表示します。
- [Delete]：選択したフィルタリング ルールを削除します。
- [Cut]：フィルタ ルールを切り取って別の場所に貼り付けます。
- [Copy]：フィルタ ルールをコピーできます。
- [Paste]：フィルタ ルールを別の場所に貼り付けます。
- [Find]：フィルタ ルールを検索します。このボタンをクリックすると、拡張ツールバーが表示されます。詳細については、「ルール テーブルのフィルタリング」（P.22-10）を参照してください。

- [Rule Diagram]：Rule Diagram の表示を切り替えます。
- [Packet Trace]：Packet Tracer ユーティリティを起動します。
- 選択しているフィルタ ルールのソースを選択するには、[Addresses] タブを使用します。
  - [Type]：ドロップダウン メニューからソースを選択できます。[All]、[IP Address Objects]、または [Network Object groups] から選択します。
  - [Name]：フィルタ ルール名を一覧表示します。
  - [Add]：フィルタ ルールを追加します。
  - [Edit]：フィルタ ルールを編集します。
  - [Delete]：フィルタ ルールを削除します。
  - [Find]：フィルタ ルールを検索します。
- 事前定義済みフィルタ ルールを選択するには、[Services] タブを使用します。
  - [Type]：ドロップダウン メニューからソースを選択できます。[All]、[IP Address Objects]、または [Network Object groups] から選択します。
  - [Name]：フィルタ ルール名を一覧表示します。
  - [Edit]：フィルタ ルールを編集します。
  - [Delete]：フィルタ ルールを削除します。
  - [Find]：フィルタ ルールを検索します。
- フィルタ ルールの時間範囲を選択するには、[Time Ranges] を使用します。
  - [Add]：フィルタ ルールの時間範囲を追加します。
  - [Edit]：フィルタ ルールの時間範囲を編集します。
  - [Delete]：フィルタ ルールの時間範囲を削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Filter Rule

ルールを適用するインターフェイスの指定、ルールを適用するトラフィックの指定、または特定タイプのフィルタリング アクションの設定には、[Add Filter Rule] ダイアログボックスを使用します。

（注）　HTTP、HTTPS、または FTP フィルタ ルールを追加する前に、URL フィルタリング サーバをイネーブルにする必要があります。URL フィルタリング サーバをイネーブルにするには、[Features] > [Configuration] > [Properties] > [URL Filtering] 画面を使用します。詳細については、URL フィルタリングを参照してください。

フィールド

- [Action]：適用するさまざまなフィルタリング アクションに対して、次に挙げるドロップダウン リストを提供します（表示されるアクションは、作成中または編集中のフィルタ ルールのタイプに応じて異なります）。
  - Filter ActiveX
  - Do not filter ActiveX
  - Filter Java Applet
  - Do not filter Java Applet
  - Filter HTTP (URL)
  - Do not filter HTTP (URL)
  - Filter HTTPS
  - Do not filter HTTPS
  - Filter FTP
  - Do not filter FTP
- [Source]：フィルタリング アクションが適用されるトラフィックの送信元を入力します。送信元は次のいずれかの方法で入力できます。
  - any：任意の送信元アドレスを指定するには、「any」（かぎカッコなし）と入力します。
  - *name*：ホスト名を入力します。
  - *address*/*mask*：IP アドレスと、オプションでネットワーク マスクを入力します。ネットマスクの表現は、CIDR またはドット付き 10 進数表記のいずれでも可能です。たとえば、10.1.1.0/24 または 10.1.1.0/255.255.255.0 と入力できます。
  - [...]：[Browse Source] ダイアログボックスを開きます。リストからホストまたはアドレスを選択できます。
- [Destination]：フィルタリング アクションが適用されるトラフィックの宛先を指定します。宛先は次のいずれかの方法で入力できます。
  - any：任意の宛先アドレスを指定するには、「any」（かぎカッコなし）と入力します。
  - *name*：ホスト名を入力します。
  - *address*/*mask*：IP アドレスと、オプションでネットワーク マスクを入力します。ネットマスクの表現は、CIDR またはドット付き 10 進数表記のいずれでも可能です。たとえば、10.1.1.0/24 または 10.1.1.0/255.255.255.0 と入力できます。
  - [...]：[Browse Destination] ダイアログボックスを開きます。リストからホストまたはアドレスを選択できます。
- [Service]：フィルタリング アクションが適用されるトラフィックのサービスを指定します。宛先は次のいずれかの方法で入力できます。
  - tcp/*port*：1 ～ 65535 のポート番号を指定できます。さらに、TCP サービスには次の修飾子を使用できます。

    !=：～と等しくない。たとえば、!=tcp/443 と指定します。

    <：～より小さい。たとえば、<tcp/2000 と指定します。

    >：～より大きい。たとえば、>tcp/2000 と指定します。

    -：範囲。たとえば、tcp/2000-3000 と指定します。
  - *name*：ウェルノウン サービス名（http や ftp など）を入力します。

  - [...] : [Browse Service] ダイアログボックスを開きます。リストからサービスを選択できます。
- [HTTP Options] : この領域は HTTP フィルタ ルールの場合だけ表示されます。
  - [When URL exceeds maximum permitted size] : URL が指定されたサイズを超えた場合に実行するアクションを選択します。URL の切り捨て、またはトラフィックのブロックを選択できます。
  - [Allow outbound traffic if URL server is not available] : イネーブルになっているとき、URL フィルタリング サーバがダウンしたり、セキュリティ アプライアンスへの接続が中断されたりする場合、ユーザは URL フィルタリングが実行されない状態で接続できます。このオプションがディセーブルの場合、URL サーバが使用不能になると、ユーザはインターネット Web サイトに接続できません。
  - [Block users from connecting to an HTTP proxy server] : プロキシ サーバを介した HTTP 要求を禁止します。
  - [Truncate CGI parameters from URL sent to URL server] : セキュリティ アプライアンスは、パラメータなしの CGI スクリプトの場所とスクリプト名だけをフィルタリング サーバに転送します。
- [HTTPS Options] : この領域は、ドロップダウン リストで [Filter HTTPS] オプションを選択した場合にだけ表示されます。
  - [Allow outbound traffic if URL server is not available] : イネーブルになっているとき、URL フィルタリング サーバがダウンしたり、セキュリティ アプライアンスへの接続が中断されたりする場合、ユーザは URL フィルタリングが実行されない状態で接続できます。このオプションがディセーブルの場合、URL サーバが使用不能になると、ユーザはインターネット Web サイトに接続できません。
- [FTP Options] : この領域は、ドロップダウン リストで [Filter FTP] オプションを選択した場合にだけ表示されます。
  - [Allow outbound traffic if URL server is not available] : イネーブルになっているとき、URL フィルタリング サーバがダウンしたり、セキュリティ アプライアンスへの接続が中断されたりする場合、ユーザは URL フィルタリングが実行されない状態で接続できます。このオプションがディセーブルの場合、URL サーバが使用不能になると、ユーザはインターネット Web サイトに接続できません。
  - [Block interactive FTP sessions (block if absolute FTP path is not provided)] : イネーブルになっているとき、FTP ディレクトリへの相対パス名を使用している場合は、FTP 要求がドロップされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ルール テーブルのフィルタリング

ルール テーブルに大量のエントリがあると、特定のルールを見つけにくくなる場合があります。ルール テーブルにフィルタを適用し、フィルタで指定されたルールだけを表示させることができます。ルール テーブルをフィルタリングするには、次の手順を実行します。

ステップ 1　ツールバーの [Find] をクリックします。[Filter] ツールバーが表示されます。

ステップ 2　フィルタ リストから次のフィルタ タイプを選択します。

- [Source]：指定した送信元アドレスまたはホスト名に基づいてルールを表示します。
- [Destination]：指定した宛先アドレスまたはホスト名に基づいてルールを表示します。
- [Source or Destination]：指定した送信元アドレスや宛先アドレスまたはホスト名に基づいてルールを表示します。
- [Service]：指定したサービスに基づいてルールを表示します。
- [Rule Type]：指定したルール タイプに基づいてルールを表示します。
- [Query]：送信元、宛先、サービス、およびルール タイプ情報で構成される複合クエリーに基づいてルールを表示します。

ステップ 3　Source、Destination、Source or Destination、および Service がフィルタの場合は、次の手順を実行します。

a. リストから一致基準を選択します。文字列を完全一致させるには「is」（かぎカッコなし）、部分一致させるには「contains」を選択します。

b. 照合する文字列を次のいずれかの方法で入力します。

- [Condition] フィールドに、送信元、宛先、またはサービスの名前を入力します。
- [...] をクリックすると参照ダイアログが開き、そこから既存のサービス、IP アドレス、またはホスト名を選択できます。

ステップ 4　Rule Type フィルタの場合は、リストからルール タイプを選択します。

ステップ 5　Query フィルタの場合は、[Define Query] をクリックし、複合クエリーを設定します。複合クエリーの設定の詳細については、「Browse Source/Destination/Service」（P.22-11）を参照してください。

ステップ 6　ルール テーブルにフィルタを適用するには、[Filter] をクリックします。

ステップ 7　ルール テーブルからフィルタをクリアしてすべてのルール エントリを表示するには、[Clear] をクリックします。

Define Query

[Define Query] ダイアログボックスでは、送信元、宛先、サービス、ルール タイプなど、複数の基準に基づいてルール テーブル フィルタを定義できます。

クエリーを作成したら、[OK] をクリックします。フィルタがただちにルール テーブルに適用されます。[Clear] をクリックすると、フィルタをクリアできます。

フィールド

- [Source]：送信元の IP アドレスまたはホスト名。完全一致には「is」、部分一致には「contains」を選択します。[...] をクリックすると選択ダイアログが開きます。CIDR 表記（アドレス/ビットカウント）を使用してネットワーク マスクを指定できます。複数のアドレスは、カンマ（,）で区切って指定できます。
- [Destination]：宛先の IP アドレスまたはホスト名。完全一致には「is」、部分一致には「contains」を選択します。[...] をクリックすると選択ダイアログが開きます。CIDR 表記（アドレス/ビットカウント）を使用してネットワーク マスクを指定できます。複数のアドレスは、カンマ（,）で区切って指定できます。
- [Source or Destination]：送信元または宛先の IP アドレスまたはホスト名。完全一致には「is」、部分一致には「contains」を選択します。[...] をクリックすると選択ダイアログが開きます。CIDR 表記（アドレス/ビットカウント）を使用してネットワーク マスクを指定できます。複数のアドレスは、カンマ（,）で区切って指定できます。
- [Service]：サービスのプロトコル/ポートまたは名前。完全一致には「is」、部分一致には「contains」を選択します。[...] をクリックすると選択ダイアログが開きます。複数のサービスは、カンマ（,）で区切って指定できます。
- [Rule Type]：リストからルール タイプを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「ルール テーブルのフィルタリング」（P.22-10）

Browse Source/Destination/Service

[Browse Source/Destination/Service] ダイアログボックスでは、既存の IP アドレス オブジェクト、名前オブジェクト、またはサービス オブジェクトから選択できます。

フィールド

- [Add]：新しい IP アドレス オブジェクト、名前オブジェクト、またはサービス オブジェクトを追加します。
- [Edit]：既存の IP アドレス オブジェクト、名前オブジェクト、またはサービス オブジェクトを編集します。
- [Filter/Clear]：ダイアログボックスに表示されている情報をフィルタリングするための文字列を入力します。ダイアログボックスに表示されている情報にフィルタを適用するには、[Filter] をクリックします。フィルタを削除し、すべてのオブジェクトを表示するには、[Clear] をクリックします。
- [Type]：表示されているオブジェクトをタイプ（IP アドレス オブジェクトなど）別に整理します。

- [Name]：オブジェクトの名前。サービスの場合はサービス名です。IP アドレス オブジェクトの場合は IP アドレス、IP 名オブジェクトの場合はホスト名です。
- [IP Address]：アドレス オブジェクトの IP アドレス。
- [Netmask]：アドレス オブジェクトのネットワーク マスク。
- [Protocol]：サービスが使用するネットワーク プロトコル（tcp、udp、icmp など）。
- [Source Ports]：サービスが使用する送信元ポート。
- [Destination Ports]：サービスが使用する宛先ポート。
- [ICMP Type]：ICMP タイプ（たとえば、ルータ アドバタイズメントの 9 など）。
- [Description]（任意）：オブジェクトの説明を指定します。
- [Source/Destination/Service] ボタン：フィルタ ルールまたはクエリーにアドレス オブジェクトまたはサービス オブジェクトを追加します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「Filter Rules」（P.22-5）
「URL フィルタリング」（P.22-1）

CHAPTER 23

サービス ポリシー ルールの設定

この章では、サービス ポリシー ルールをイネーブルにする方法を説明します。サービス ポリシーでは、一貫性と柔軟性を備えた方法で セキュリティ アプライアンス 機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。

この章は、次の項で構成されています。

サービス ポリシーの概要

この項では、セキュリティ ポリシーの概要について説明します。説明する内容は次のとおりです。

サポートされる機能

セキュリティ ポリシーは、次の機能をサポートします。

- TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化
- CSC
- アプリケーション インスペクション
- IPS

- QoS 入力ポリシング
- QoS 出力ポリシング
- QoS プライオリティ キュー

サービス ポリシーの要素

サービス ポリシーの設定では、インターフェイスあたりのサービス ポリシー ルール、またはグローバル ポリシーのサービス ポリシー ルールを 1 つ以上追加します。それぞれのルールごとに、次の要素を指定します。

1. ルールを適用するインターフェイスを指定するか、またはグローバル ポリシーを指定します。
2. アクションを適用するトラフィックを指定します。レイヤ 3 および 4 の通過トラフィックを指定できます。
3. トラフィック クラスにアクションを適用します。トラフィック クラスごとに複数のアクションを適用できます。

デフォルトのグローバル ポリシー

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、特定のインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。すべてのインスペクションがデフォルトでイネーブルになっているわけではありません。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。（インターフェイス ポリシーはグローバル ポリシーに優先します）。

デフォルト ポリシーには、次のアプリケーション インスペクションが含まれます。

- メッセージの最大長 512 バイトに対する DNS インスペクション
- FTP
- H323（H225）
- H323（RAS）
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny（SCCP）
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP

機能の方向

アクションは、機能に応じて双方向または単方向にトラフィックに適用されます。双方向に適用される機能の場合、トラフィックが両方向のクラス マップと一致した場合に、ポリシー マップを適用するインターフェイスを出入りするすべてのトラフィックが影響を受けます。

（注）　グローバル ポリシーを使用する場合は、すべての機能が単方向です。単一インターフェイスに適用する場合に通常双方向の機能は、グローバルに適用される場合、各インターフェイスの入力にのみ適用されます。ポリシーはすべてのインターフェイスに適用されるため、ポリシーは両方向に適用され、この場合の双方向は冗長になります。

たとえば、QoS プライオリティ キューのような単方向に適用される機能の場合は、ポリシー マップを適用するインターフェイスを出るトラフィックだけが影響を受けます。各機能の方向については、表 23-1 を参照してください。

表 23-1　機能の方向

機能	単一インターフェイスでの方向	グローバルでの方向
TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化	双方向	入力
CSC	双方向	入力
アプリケーション インスペクション	双方向	入力
IPS	双方向	入力
QoS 入力ポリシング	入力	入力
QoS 出力ポリシング	出力	出力
QoS プライオリティ キュー	出力	出力

複数のサービス ポリシーの場合の機能照合ガイドライン

TCP および UDP トラフィック（およびステートフル ICMP インスペクションがイネーブルの場合は ICMP）の場合、サービス ポリシーはトラフィック フローに対して作用し、個々のパケットに限定されません。トラフィックが、1 つのインターフェイスのポリシーで定義されている機能に一致する既存の接続の一部である場合、そのトラフィック フローを別のインターフェイスのポリシーにある同じ機能と照合することはできません。最初のポリシーのみが使用されます。

たとえば、HTTP トラフィックが、HTTP トラフィックを検査する内部インターフェイスのポリシーと一致するときに、HTTP インスペクション用の外部インターフェイスに別のポリシーがある場合、そのトラフィックが外部インターフェイスの出力側でも検査されることはありません。同様に、その接続のリターン トラフィックが外部インターフェイスの入力ポリシーによって検査されたり、内部インターフェイスの出力ポリシーによって検査されたりすることもありません。

ステートフル ICMP インスペクションをイネーブルにしない場合の ICMP のように、フローとして扱われないトラフィックの場合は、リターン トラフィックを戻り側のインターフェイスの別のポリシー マップと照合できます。たとえば、内部および外部のインターフェイスで IPS 検査を設定し、内部ポリシーでは仮想センサー 1、外部ポリシーでは仮想センサー 2 を使用している場合、非ステートフル ping は仮想センサー 1 の発信側と照合するだけでなく、仮想センサー 2 の着信側とも照合します。

ルール内の複数の機能アクションが適用される順序

1 つのルール内のアクションは次の順序で実行されます。

- TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化

（注）　セキュリティ アプライアンスがプロキシ サービス（AAA や CSC など）を実行したり、TCP ペイロード（FTP インスペクション）を変更したりするときは、TCP ノーマライザはデュアル モードで動作します。その場合、サービスを変更するプロキシやペイロードの前後で適用されます。

- CSC
- アプリケーション インスペクション
- IPS
- QoS 入力ポリシング
- QoS 出力ポリシング
- QoS プライオリティ キュー

通過トラフィックのサービス ポリシー ルールの追加

通過トラフィックのサービス ポリシー ルールを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] で、[Add] をクリックします。

[Add Service Policy Rule Wizard - Service Policy] ダイアログボックスが表示されます。

（注）　[Add] ボタンの右側にある小さな矢印ではなく [Add] ボタンをクリックすると、通過トラフィック ルールがデフォルトで追加されます。[Add] ボタン上の矢印をクリックすると、通過トラフィック ルールと管理トラフィック ルールのいずれかを選択できます。

ステップ 2　[Create a Service Policy and Apply To] 領域で、次のオプションの 1 つをクリックします。

- [Interface]。このオプションでは、サービス ポリシーが 1 つのインターフェイスに適用されます。インターフェイス ポリシーは、グローバル ポリシーより優先されます。
  - **a.** ドロップダウン リストからインターフェイスを選択します。

    すでにポリシーが適用されているインターフェイスを選択する場合は、ウィザードの指示に従って、新しいサービス ポリシー ルールをそのインターフェイスに追加できます。
  - **b.** 新しいサービス ポリシーの場合は、[Policy Name] フィールドに名前を入力します。
  - **c.** （任意）[Description] フィールドに説明を入力します。
- [Global - applies to all interfaces]。このオプションでは、サービス ポリシーがすべてのインターフェイスにグローバルに適用されます。デフォルト アプリケーション インスペクションのサービス ポリシー ルールを含むグローバル ポリシーは、デフォルトで存在します。詳細については、「デフォルトのグローバル ポリシー」（P.23-2）を参照してください。ウィザードを使用してルールをグローバル ポリシーに追加できます。

ステップ 3　[Next] をクリックします。

[Add Service Policy Rule Wizard - Traffic Classification Criteria] ダイアログボックスが表示されます。

ステップ 4　次のオプションのいずれかをクリックして、ポリシーのアクションを適用するトラフィックを指定します。

- [Create a new traffic class]。[Create a new traffic class] フィールドにトラフィック クラス名を入力し、説明（任意）を入力します。

  基準のいずれかを使用してトラフィックを特定します。

  - [Default Inspection Traffic]：このクラスは、セキュリティ アプライアンス が検査可能なすべてのアプリケーションによって使用される、デフォルトの TCP および UDP ポートを照合します。

    デフォルト ポートのリストについては、「デフォルトの検査ポリシー」（P.24-3）を参照してください。セキュリティ アプライアンス には、デフォルトのインスペクション トラフィックに一致して、すべてのインターフェイス上のトラフィックに共通検査を適用するデフォルト グローバル ポリシーが含まれます。Default Inspection Traffic クラスにポートが含まれているすべてのアプリケーションが、ポリシー マップにおいてデフォルトでイネーブルになっているわけではありません。

    Source and Destination IP Address (uses ACL) クラスを Default Inspection Traffic クラスと一緒に指定して、照合されるトラフィックを絞り込むことができます。Default Inspection Traffic クラスによって照合するポートが指定されるため、アクセス リストのポートはすべて無視されます。

  - [Source and Destination IP Address (uses ACL)]：このクラスは拡張アクセス リストで指定されているトラフィックを照合します。セキュリティ アプライアンスがトランスペアレント ファイアウォール モードで動作している場合は、EtherType アクセス リストを使用できます。

    （注）　このタイプの新しいトラフィック クラスを作成する場合は、最初にアクセス コントロール エントリ（ACE）を 1 つだけ指定できます。ルールを追加した後は、同じインターフェイスまたはグローバル ポリシーに新しいルールを追加し、それから [Traffic Classification] ダイアログボックス（以下を参照）で [Add rule to existing traffic class] を指定することによって、ACE を追加できます。

  - [Tunnel Group]：このクラスは、QoS を適用するトンネル グループのトラフィックを照合します。その他にもう 1 つのトラフィック照合オプションを指定してトラフィック照合対象をさらに絞込み、[Any Traffic]、[Source and Destination IP Address (uses ACL)]、または [Default Inspection Traffic] を排除できます。
  - [TCP or UDP Destination Port]：1 つのポートまたは連続する一定範囲のポートを照合します。

    ヒント　複数の非連続ポートを使用するアプリケーションの場合は、[Source and Destination IP Address (uses ACL)] を使用して各ポートを照合します。

  - [RTP Range]：クラス マップは、RTP トラフィックを照合します。
  - [IP DiffServ CodePoints (DSCP)]：このクラスは、IP ヘッダーの最大 8 つの DSCP 値を照合します。
  - [IP Precedence]：このクラス マップは、IP ヘッダーの TOS バイトによって表される、最大 4 つの Precedence 値を照合します。
  - [Any Traffic]：すべてのトラフィックを照合します。
- [Add rule to existing traffic class]。すでに同じインターフェイスにサービス ポリシー ルールを指定している場合、またはグローバル サービス ポリシーを追加する場合は、このオプションによって既存のアクセス リストに ACE を追加できます。このインターフェイスのサービス ポリシー

ルールで [Source and Destination IP Address (uses ACL)] オプションを選択した場合は、事前に作成したすべてのアクセス リストに ACE を追加できます。このトラフィック クラスでは、複数の ACE を追加する場合であっても、1 セットのルール アクションしか指定できません。この手順全体を繰り返すことによって、複数の ACE を同じトラフィック クラスに追加できます。ACE の順序の変更方法については、「サービス ポリシー ルールの順序の管理」（P.23-11）を参照してください。

- [Use an existing traffic class]。別のインターフェイスのルールで使用されるトラフィック クラスを作成した場合は、そのトラフィック クラス定義をこのルールで再使用できます。1 つのルールのトラフィック クラスを変更すると、その変更は同じトラフィック クラスを使用するすべてのルールに継承されます。コンフィギュレーションに CLI で入力した **class-map** コマンドが含まれている場合は、それらのトラフィック クラス名も使用できます（ただし、そのトラフィック クラスの定義を表示するには、そのルールを作成する必要があります）。
- [Use class default as the traffic class]。このオプションでは、すべてのトラフィックを照合する class-default クラスを使用します。class-default クラスは、セキュリティ アプライアンスによって自動的に作成され、ポリシーの最後に配置されます。アクションを何も適用しない場合でもセキュリティ アプライアンスによって作成されますが、内部での使用に限られます。必要に応じて、このクラスにアクションを適用できます。これは、すべてのトラフィックを照合する新しいトラフィック クラスを作成するよりも便利な場合があります。class-default クラスを使用して、このサービス ポリシーにルールを 1 つだけ作成できます。これは、各トラフィック クラスを関連付けることができるのは、サービス ポリシーごとに 1 つのルールだけであるためです。

ステップ 5　[Next] をクリックします。

ステップ 6　次に表示されるダイアログボックスは、選択したトラフィック照合基準に応じて異なります。

（注）　[Any Traffic] オプションの場合には、追加設定を行うための特別なダイアログボックスはありません。

- [Default Inspections]：このダイアログボックスは情報提供の目的でだけ表示され、トラフィック クラスに含まれるアプリケーションとポートが示されます。
- [Source and Destination Address]：このダイアログボックスでは、送信元アドレスと宛先アドレスを設定できます。

  a. [Match] または [Do Not Match] をクリックします。

  [Match] オプションでは、アドレスが一致するトラフィックにアクションを適用する場合のルールを作成します。[Do Not Match] オプションでは、トラフィックを指定したアクションの適用から免除します。たとえば、10.1.1.25 を除いて、10.1.1.0/24 のトラフィックすべてを照合し、そのトラフィックに接続制限を適用するとします。この場合は、2 つのルール（[Match] オプションを使用した 10.1.1.0/24 に対するルールおよび [Do Not Match] オプションを使用した 10.1.1.25 に対するルール）を作成します。必ず、Do Not Match ルールが Match ルールの上になるように配置してください。順序を逆にすると、10.1.1.25 が最初に Match ルールを照合することになります。

  b. [Source] フィールドで、送信元 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

  任意の送信元アドレスを指定するには、**any** を入力します。

  アドレスが複数ある場合はカンマで区切ります。

  c. [Destination] フィールドで、宛先 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

任意の宛先アドレスを指定するには、**any** を入力します。

アドレスが複数ある場合はカンマで区切ります。

d. [Service] フィールドで、宛先サービスの IP サービス名または番号を入力するか、[...] ボタンをクリックしてサービスを選択します。

TCP または UDP のポート番号、あるいは ICMP サービス番号を指定する場合は、*プロトコル / ポート*を入力します。たとえば、TCP/8080 と入力します。

デフォルトでは、サービスは IP です。

サービスが複数ある場合はカンマで区切ります。

e. （任意）[Description] フィールドに説明を入力します。

f. （任意）TCP または UDP の送信元サービスを指定するには、[More Options] 領域をクリックして開き、[Source Service] フィールドに TCP サービスまたは UDP サービスを入力します。

宛先サービスと送信元サービスは同じである必要があります。[Destination Service] フィールドをコピーし、[Source Service] フィールドに貼り付けます。

g. （任意）ルールを非アクティブにするには、[More Options] 領域をクリックして開き、[Enable Rule] をオフにします。

この設定は、ルールを削除せずに無効にしたい場合に便利です。

h. （任意）ルールの時間範囲を指定するには、[More Options] 領域をクリックして開き、[Time Range] ドロップダウン リストから時間範囲を選択します。

新しい時間範囲を追加するには、[...] ボタンをクリックします。詳細については、「時間範囲の設定」（P.8-15）を参照してください。

この設定は、事前に設定した時間にだけルールをアクティブにする場合に便利です。

- [Tunnel Group] : [Tunnel Group] ドロップダウン リストからトンネル グループを選択するか、または [New] をクリックして新しいトンネル グループを追加します。詳細については、「[Add IPSec Remote Access Connection] および [Add SSL VPN Access Connection]」（P.32-68）を参照してください。

  各フローをポリシングするには、[Match flow destination IP address] をオンにします。固有の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。

- [Destination Port] : [TCP] または [UDP] をクリックします。

  [Service] フィールドに、ポート番号または名前を入力するか、または [...] をクリックして ASDM で定義済みのサービスを選択します。

- [RTP Range] : RTP ポート範囲を 2000 ～ 65534 の間で入力します。範囲内の最大ポート数は、16383 です。

- [IP DiffServ CodePoints (DSCP)] : [DSCP Value to Add] 領域で、[Select Named DSCP Values] から値を選択するか、または [Enter DSCP Value (0-63)] フィールドに値を入力し、[Add] をクリックします。

  必要に応じて値を追加するか、または [Remove] ボタンを使用して値を削除します。

- [IP Precedence] : [Available IP Precedence] 領域で値を選択し、[Add] をクリックします。

  必要に応じて値を追加するか、または [Remove] ボタンを使用して値を削除します。

ステップ 7　[Next] をクリックします。

[Add Service Policy Rule - Rule Actions] ダイアログボックスが表示されます。

ステップ 8　次の項の説明に従って 1 つ以上のルール アクションを設定します。

- 第 24 章「アプリケーション レイヤ プロトコル インスペクションの設定」
- 「接続の設定」（P.27-6）
- 「[QoS] タブのフィールド情報」（P.28-2）
- 第 39 章「IPS の設定」
- 第 40 章「Trend Micro Content Security の設定」

ステップ 9　[Finish] をクリックします。

管理トラフィックのサービス ポリシー ルールの追加

管理目的でセキュリティ アプライアンスに転送されるトラフィックのサービス ポリシーを作成できます。このタイプのセキュリティ ポリシーでは、RADIUS アカウンティング検査と接続制限を実行できます。この項では、次のトピックについて取り上げます。

- 「RADIUS アカウンティング インスペクションの概要」（P.23-8）
- 「管理トラフィックのサービス ポリシー ルールの設定」（P.23-8）

RADIUS アカウンティング インスペクションの概要

よく知られている問題の 1 つに GPRS ネットワークでの過剰請求攻撃があります。過剰請求攻撃では、利用していないサービスについて料金を請求されるため、ユーザが怒りや不満を感じるおそれがあります。この場合、悪意のある攻撃者は、サーバへの接続をセットアップし、SGSN から IP アドレスを取得します。攻撃者がコールを終了しても、攻撃者のサーバはパケットの送信を続けます。このパケットは GGSN によってドロップされますが、サーバからの接続はアクティブなままです。攻撃者に割り当てられていた IP アドレスが解放され、正規ユーザに再割り当てされるので、正規ユーザは、攻撃者が利用するサービスの分まで請求されることになります。

RADIUS アカウンティング インスペクションでは、GGSN によって検出されるトラフィックが正規のものであることを確認することによって、このタイプの攻撃を防止します。RADIUS アカウンティングの機能を正しく設定しておくと、セキュリティ アプライアンスは、RADIUS アカウンティング要求の開始メッセージと終了メッセージに含まれる Framed IP 属性との照合結果に基づいて接続を切断します。終了メッセージの Framed IP 属性の IP アドレスが一致している場合、セキュリティ アプライアンスは、一致する IP アドレスを持つ送信元との接続をすべて検索します。

セキュリティ アプライアンスでメッセージを検証できるように、RADIUS サーバとの事前共有秘密キーを設定することもできます。事前共有秘密キーを設定しないと、セキュリティ アプライアンスは、メッセージの送信元を検証する必要がなく、その IP アドレスが、RADIUS メッセージの送信を許可されているアドレスの 1 つかどうかだけをチェックします。

管理トラフィックのサービス ポリシー ルールの設定

管理トラフィックのサービス ポリシーを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] ペインで、[Add] の横の下矢印をクリックします。

ステップ 2　[Add Management Service Policy Rule] を選択します。

[Add Management Service Policy Rule Wizard - Service Policy] ダイアログボックスが表示されます。

ステップ 3　[Create a Service Policy and Apply To] 領域で、次のオプションの 1 つをクリックします。

- [Interface]。このオプションでは、サービス ポリシーが 1 つのインターフェイスに適用されます。インターフェイス ポリシーは、グローバル ポリシーより優先されます。
  - **a.** ドロップダウン リストからインターフェイスを選択します。

    すでにポリシーが適用されているインターフェイスを選択する場合は、ウィザードの指示に従って、新しいサービス ポリシー ルールをそのインターフェイスに追加できます。
  - **b.** 新しいサービス ポリシーの場合は、[Policy Name] フィールドに名前を入力します。
  - **c.** （任意）[Description] フィールドに説明を入力します。
- [Global - applies to all interfaces]。このオプションでは、サービス ポリシーがすべてのインターフェイスにグローバルに適用されます。デフォルト アプリケーション インスペクションのサービス ポリシー ルールを含むグローバル ポリシーは、デフォルトで存在します。詳細については、「デフォルトのグローバル ポリシー」（P.23-2）を参照してください。ウィザードを使用してルールをグローバル ポリシーに追加できます。

ステップ 4　[Next] をクリックします。

[Add Management Service Policy Rule Wizard - Traffic Classification Criteria] ダイアログボックスが表示されます。

ステップ 5　次のオプションのいずれかをクリックして、ポリシーのアクションを適用するトラフィックを指定します。

- [Create a new traffic class]。[Create a new traffic class] フィールドにトラフィック クラス名を入力し、説明（任意）を入力します。

  基準のいずれかを使用してトラフィックを特定します。
  - [Source and Destination IP Address (uses ACL)] : このクラスは拡張アクセス リストで指定されているトラフィックを照合します。セキュリティ アプライアンスがトランスペアレント ファイアウォール モードで動作している場合は、EtherType アクセス リストを使用できます。

    （注）　このタイプの新しいトラフィック クラスを作成する場合は、最初にアクセス コントロール エントリ（ACE）を 1 つだけ指定できます。ルールを追加した後は、同じインターフェイスまたはグローバル ポリシーに新しいルールを追加し、それから [Traffic Classification] ダイアログボックス（以下を参照）で [Add rule to existing traffic class] を指定することによって、ACE を追加できます。
  - [TCP or UDP Destination Port] : 1 つのポートまたは連続する一定範囲のポートを照合します。

ヒント　複数の非連続ポートを使用するアプリケーションの場合は、[Source and Destination IP Address (uses ACL)] を使用して各ポートを照合します。

- [Add rule to existing traffic class]。すでに同じインターフェイスにサービス ポリシー ルールを指定している場合、またはグローバル サービス ポリシーを追加する場合は、このオプションによって既存のアクセス リストに ACE を追加できます。このインターフェイスのサービス ポリシー ルールで [Source and Destination IP Address (uses ACL)] オプションを選択した場合は、事前に作成したすべてのアクセス リストに ACE を追加できます。このトラフィック クラスでは、複数の ACE を追加する場合であっても、1 セットのルール アクションしか指定できません。この手順全体を繰り返すことによって、複数の ACE を同じトラフィック クラスに追加できます。ACE の順序の変更方法については、「サービス ポリシー ルールの順序の管理」（P.23-11）を参照してください。

- [Use an existing traffic class]。別のインターフェイスのルールで使用されるトラフィック クラスを作成した場合は、そのトラフィック クラス定義をこのルールで再使用できます。1 つのルールのトラフィック クラスを変更すると、その変更は同じトラフィック クラスを使用するすべてのルールに継承されます。コンフィギュレーションに CLI で入力した **class-map** コマンドが含まれている場合は、それらのトラフィック クラス名も使用できます（ただし、そのトラフィック クラスの定義を表示するには、そのルールを作成する必要があります）。

ステップ 6　[Next] をクリックします。

ステップ 7　次に表示されるダイアログボックスは、選択したトラフィック照合基準に応じて異なります。

- [Source and Destination Address]：このダイアログボックスでは、送信元アドレスと宛先アドレスを設定できます。

  a. [Match] または [Do Not Match] をクリックします。

  [Match] オプションでは、アドレスが一致するトラフィックにアクションを適用する場合のルールを作成します。[Do Not Match] オプションでは、トラフィックを指定したアクションの適用から免除します。たとえば、10.1.1.25 を除いて、10.1.1.0/24 のトラフィックすべてを照合し、そのトラフィックに接続制限を適用するとします。この場合は、2 つのルール（[Match] オプションを使用した 10.1.1.0/24 に対するルールおよび [Do Not Match] オプションを使用した 10.1.1.25 に対するルール）を作成します。必ず、Do Not Match ルールが Match ルールの上になるように配置してください。順序を逆にすると、10.1.1.25 が最初に Match ルールを照合することになります。

  b. [Source] フィールドで、送信元 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

  任意の送信元アドレスを指定するには、**any** を入力します。

  アドレスが複数ある場合はカンマで区切ります。

  c. [Destination] フィールドで、宛先 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

  任意の宛先アドレスを指定するには、**any** を入力します。

  アドレスが複数ある場合はカンマで区切ります。

  d. [Service] フィールドで、宛先サービスの IP サービス名または番号を入力するか、[...] ボタンをクリックしてサービスを選択します。

  TCP または UDP のポート番号、あるいは ICMP サービス番号を指定する場合は、*プロトコル / ポート*を入力します。たとえば、TCP/8080 と入力します。

  デフォルトでは、サービスは IP です。

  サービスが複数ある場合はカンマで区切ります。

  e.（任意）[Description] フィールドに説明を入力します。

  f.（任意）TCP または UDP の送信元サービスを指定するには、[More Options] 領域をクリックして開き、[Source Service] フィールドに TCP サービスまたは UDP サービスを入力します。

  宛先サービスと送信元サービスは同じである必要があります。[Destination Service] フィールドをコピーし、[Source Service] フィールドに貼り付けます。

  g.（任意）ルールを非アクティブにするには、[More Options] 領域をクリックして開き、[Enable Rule] をオフにします。

この設定は、ルールを削除せずに無効にしたい場合に便利です。

h. （任意）ルールの時間範囲を指定するには、[More Options] 領域をクリックして開き、[Time Range] ドロップダウン リストから時間範囲を選択します。

新しい時間範囲を追加するには、[...] ボタンをクリックします。詳細については、「時間範囲の設定」（P.8-15）を参照してください。

この設定は、事前に設定した時間にだけルールをアクティブにする場合に便利です。

- [Destination Port]：[TCP] または [UDP] をクリックします。

  [Service] フィールドに、ポート番号または名前を入力するか、または [...] をクリックして ASDM で定義済みのサービスを選択します。

ステップ 8　[Next] をクリックします。

「Add Management Service Policy Rule - Rule Actions」ダイアログボックスが表示されます。

ステップ 9　RADIUS アカウンティング インスペクションを設定するには、[RADIUS Accounting Map] ドロップダウン リストからインスペクション マップを選択するか、または [Configure] をクリックしてマップを追加します。

詳細については、「RADIUS アカウンティング フィールドの説明」（P.23-12）を参照してください。

ステップ 10　最大接続数を設定するには、[Maximum Connections] 領域で次の値を 1 つ以上入力します。

- [TCP & UDP Connections]：トラフィック クラスのすべてのクライアントで同時に接続される TCP および UDP 接続の最大数を 65,536 までの範囲で指定します。どちらのプロトコルともデフォルトは **0** で、接続可能な最大許容数に設定されています。
- [Embryonic Connections]：ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

ステップ 11　[Finish] をクリックします。

サービス ポリシー ルールの順序の管理

インターフェイス上またはグローバル ポリシー内でのサービス ポリシー ルールの順序は、トラフィックへのアクションの適用方法に影響します。パケットがサービス ポリシーのルールを照合する方法については、次のガイドラインを参照してください。

- パケットは、機能タイプごとにサービス ポリシーのルールを 1 つだけ照合できます。
- パケットが、1 つの機能タイプのアクションを含むルールを照合する場合、セキュリティ アプライアンスは、その機能タイプを含む、後続のどのルールに対してもそのパケットを照合しません。
- ただし、そのパケットが異なる機能タイプの後続のルールを照合する場合、セキュリティ アプライアンスは後続ルールのアクションも適用します。

たとえば、パケットが接続制限のルールを照合し、アプリケーション インスペクションのルールも照合する場合は、両方のアクションが適用されます。

パケットがアプリケーション インスペクションのルールを照合し、アプリケーション インスペクションを含む別のルールを照合する場合、2 番目のルール アクションは適用されません。

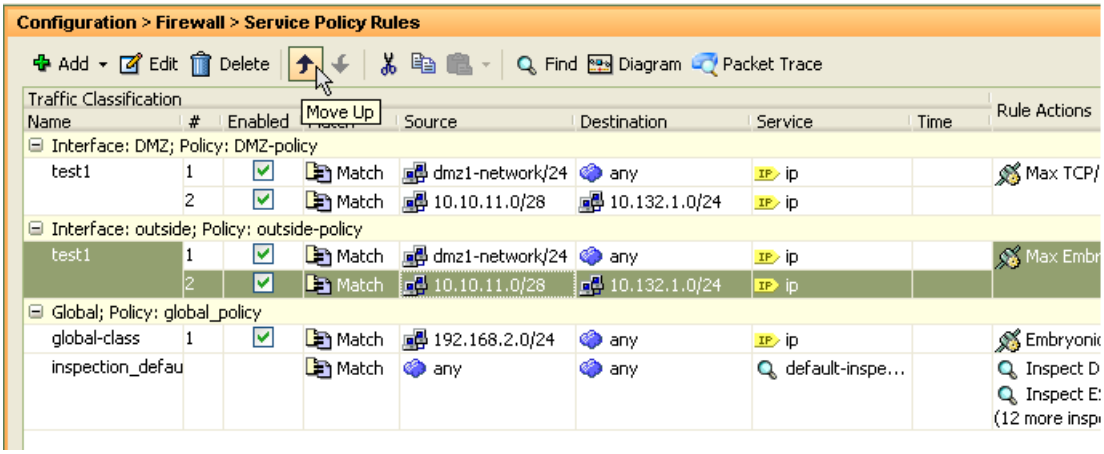
ルールに複数の ACE が組み込まれたアクセス リストが含まれる場合は、ACE の順序もパケット フローに影響します。FWSM は、リストのエントリの順序に従って、各 ACE に対してパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。たとえば、アクセス リストの先頭にすべてのトラフィックを明示的に許可する ACE を作成した場合、残りのステートメントはチェックされません。

ルールまたはルール内での ACE の順序を変更するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] ペインで、上または下に動かすルールまたは ACE を選択します。

ステップ 2　[Move Up] または [Move Down] カーソルをクリックします（図 23-1 を参照してください）。

図 23-1　　ACE の移動



（注）　複数のサービス ポリシーで使用されるアクセス リストで ACE を並べ替えると、その変更はすべてのサービス ポリシーで継承されます。

ステップ 3　ルールまたは ACE を並べ替えたら、[Apply] をクリックします。

RADIUS アカウンティング フィールドの説明

この項では、RADIUS アカウンティング フィールドの一覧を示します。説明する内容は次のとおりです。

Select RADIUS Accounting Map

[Select RADIUS Accounting Map] ダイアログボックスでは、定義済み RADIUS アカウンティング マップを選択するか、新しい RADIUS アカウンティング マップを定義できます。

フィールド

- [Add]：新しい RADIUS アカウンティング マップを追加できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add RADIUS Accounting Policy Map

[Add RADIUS Accounting Policy Map] ダイアログボックスでは、RADIUS アカウンティング マップの基本設定を追加できます。

フィールド

- [Name]：事前に設定されている RADIUS アカウンティング マップの名前を入力します。
- [Description]：RADIUS アカウンティング マップの説明を 100 文字以内で入力します。
- [Host Parameters] タブ：
  - [Host IP Address]：RADIUS メッセージの送信元となるホストの IP アドレスを指定します。
  - [Key: (optional)]：キーを指定します。
  - [Add]：[Host] テーブルにホスト エントリを追加します。
  - [Delete]：[Host] テーブルからホスト エントリを削除します。
- [Other Parameters] タブ：
  - [Attribute Number]：「Accounting Start」を受信したときに確認する属性番号を指定します。
  - [Add]：[Attribute] テーブルにエントリを追加します。
  - [Delete]：[Attribute] テーブルからエントリを削除します。
  - [Send response to the originator of the RADIUS message]：RADIUS メッセージの送信元ホストにメッセージを返信します。
  - [Enforce timeout]：ユーザのタイムアウトをイネーブルにします。
  - [Users Timeout]：データベース内のユーザのタイムアウト（hh:mm:ss）。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

RADIUS インスペクション マップ

[RADIUS] ペインでは、事前に設定された RADIUS アプリケーション インスペクション マップを表示できます。RADIUS マップでは、RADIUS アプリケーション インスペクションで使用されるコンフィギュレーションのデフォルト値を変更できます。RADIUS マップを使用すると、過剰請求攻撃を防御できます。

フィールド

- [Name]：インスペクション マップの名前を 40 文字以内で入力します。
- [Description]：インスペクション マップの説明を 200 文字以内で入力します。
- [RADIUS Inspect Maps]：定義されている RADIUS インスペクション マップを一覧表示するテーブルです。定義されているインスペクション マップは、[Inspect Maps] ツリーの [RADIUS] エリアにも表示されます。
- [Add]：新規の RADIUS インスペクション マップを、[RADIUS Inspect Maps] テーブルの定義リストと [Inspect Maps] ツリーの [RADIUS] エリアに追加します。RADIUS マップを新たに設定するには、[Inspect Maps] ツリーで [RADIUS] エントリを選択します。
- [Delete]：[RADIUS Inspect Maps] テーブルで選択したアプリケーション インスペクション マップを削除します。[Inspect Maps] ツリーの [RADIUS] エリアからも削除されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

RADIUS インスペクション マップ（ホスト）

[RADIUS Inspect Map Host Parameters] ペインでは、インスペクション マップのホスト パラメータを設定できます。

フィールド

- [Name]：事前に設定されている RADIUS アカウンティング マップの名前を示します。
- [Description]：RADIUS アカウンティング マップの説明を 200 文字以内で入力します。
- [Host Parameters]：ホストのパラメータを設定できます。

  - [Host IP Address]：RADIUS メッセージの送信元となるホストの IP アドレスを指定します。
  - [Key: (optional)]：キーを指定します。
- [Add]：[Host] テーブルにホスト エントリを追加します。
- [Delete]：[Host] テーブルからホスト エントリを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

RADIUS インスペクション マップ（その他）

[RADIUS Inspect Map Other Parameters] ペインでは、インスペクション マップに追加するパラメータを設定できます。

フィールド

- [Name]：事前に設定されている RADIUS アカウンティング マップの名前を示します。
- [Description]：RADIUS アカウンティング マップの説明を 200 文字以内で入力します。
- [Other Parameters]：追加するパラメータを設定できます。
  - [Send response to the originator of the RADIUS message]：RADIUS メッセージの送信元ホストにメッセージを返信します。
  - [Enforce timeout]：ユーザのタイムアウトをイネーブルにします。

    [Users Timeout]：データベース内のユーザのタイムアウト（hh:mm:ss）。
  - [Enable detection of GPRS accounting]：GPRS アカウンティングの検出をイネーブルにします。このオプションは、GTP/GPRS ライセンスがイネーブルの場合にだけ使用できます。
  - [Validate Attribute]：属性情報です。

    [Attribute Number]：「Accounting Start」を受信したときに確認する属性番号を指定します。

    [Add]：[Attribute] テーブルにエントリを追加します。

    [Delete]：[Attribute] テーブルからエントリを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 24

アプリケーション レイヤ プロトコル インスペクションの設定

この章では、アプリケーション レイヤ プロトコル インスペクションを設定する方法について説明します。インスペクション エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルでは、高速パスでパケットを渡すのではなく、セキュリティ アプライアンスで詳細なパケット インスペクションを行う必要があります。そのため、インスペクション エンジンがスループット全体に影響を与えることがあります。

セキュリティ アプライアンス では、デフォルトでいくつかの一般的なインスペクション エンジンがイネーブルになっていますが、ネットワークによっては他のインスペクション エンジンをイネーブルにしなければならない場合があります。この章は、次の項で構成されています。

インスペクション エンジンの概要

この項では、次のトピックについて取り上げます。

アプリケーション プロトコル インスペクションを使用するタイミング

ユーザが接続を確立すると、セキュリティ アプライアンス はアクセス リストと照合してパケットをチェックし、アドレス変換を作成し、高速パスでのセッション用にエントリを作成して、後続のパケットが時間のかかるチェックをバイパスできるようにします。ただし、高速パスは予測可能なポート番号に基づいており、パケット内部のアドレス変換を実行しません。

多くのプロトコルは、セカンダリの TCP ポートまたは UDP ポートを開きます。既知のポートで初期セッションが使用され、動的に割り当てられたポート番号がネゴシエーションされます。

パケットに IP アドレスを埋め込むアプリケーションもあります。この IP アドレスは送信元アドレスと一致する必要があり、通常、セキュリティ アプライアンスを通過するときに変換されます。

これらのアプリケーションを使用する場合は、アプリケーション インスペクションをイネーブルにする必要があります。

IP アドレスを埋め込むサービスに対してアプリケーション インスペクションをイネーブルにすると、セキュリティ アプライアンス は埋め込まれたアドレスを変換し、チェックサムや変換の影響を受けたその他のフィールドを更新します。

ダイナミックに割り当てられたポートを使用するサービスに対してアプリケーション インスペクションをイネーブルにすると、セキュリティ アプライアンス はセッションをモニタしてダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポートでのデータ交換を許可します。

検査の制限事項

アプリケーション プロトコル検査には、次の制限事項があります。

- インスペクションが必要なマルチメディア セッションのステート情報は、ステートフル フェールオーバーのステート リンク経由では渡されません。GTP は例外で、ステート リンクで複製されます。
- 一部のインスペクション エンジンは、PAT、NAT、外部 NAT、または同一セキュリティ インターフェイス間の NAT をサポートしません。NAT サポートの詳細については、「デフォルトの検査ポリシー」を参照してください。

デフォルトの検査ポリシー

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、すべてのインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。デフォルト アプリケーション インスペクション トラフィックには、各プロトコルのデフォルト ポートへのトラフィックが含まれます。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する（標準以外のポートにインスペクションを適用する場合や、デフォルトでイネーブルになっていないインスペクションを追加する場合など）には、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用する必要があります。

表 24-1 にサポートされているすべてのインスペクション、デフォルトのクラス マップで使用されるデフォルトのポート、およびデフォルトでオンになっているインスペクション エンジン（太字）を示します。この表には、NAT に関する制限事項も含まれています。

表 24-1　サポートされているアプリケーション インスペクション エンジン

アプリケーション[1]	デフォルト ポート	NAT に関する制限事項	標準[2]	コメント
CTIQBE	TCP/2748	—	—	—
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	RFC 1123	PTR レコードは変更されません。
FTP	TCP/21	—	RFC 959	—
GTP	UDP/3386 UDP/2123	—	—	特別なライセンスが必要です。
H.323 H.225 および **RAS**	TCP/1720 UDP/1718 UDP (RAS) 1718-1719	同一セキュリティのインターフェイス上の NAT はサポートされません。 スタティック PAT はサポートされません。	ITU-T H.323、H.245、H225.0、Q.931、Q.932	—
HTTP	TCP/80	—	RFC 2616	ActiveX と Java を除去する場合の MTU 制限に注意してください。MTU が小さすぎて Java タグまたは ActiveX タグを 1 つのパケットに納められない場合は、除去の処理は行われません。

表 24-1　サポートされているアプリケーション インスペクション エンジン （続き）

アプリケーション[1]	デフォルト ポート	NAT に関する制限事項	標準[2]	コメント
ICMP	—	—	—	すべての ICMP トラフィックは、デフォルトのクラス マップで照合されます。
ICMP ERROR	—	—	—	すべての ICMP トラフィックは、デフォルトのクラス マップで照合されます。
ILS（LDAP）	TCP/389	PAT はサポートされません。	—	—
MGCP	UDP/2427、2727	—	RFC 2705bis-05	—
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	—	—	NetBIOS は、NBNS UDP ポート 137 および NBDS UDP ポート 138 に対してパケットの NAT 処理を実行することでサポートされます。
PPTP	TCP/1723	—	RFC 2637	—
RADIUS Accounting	1646	—	RFC 2865	—
RSH	TCP/514	PAT はサポートされません。	Berkeley UNIX	—
RTSP	TCP/554	PAT はサポートされません。 外部 NAT はサポートされません。	RFC 2326、2327、1889	HTTP クローキングは処理しません。
SIP	TCP/5060 UDP/5060	外部 NAT はサポートされません。 同一セキュリティのインターフェイス上の NAT はサポートされません。	RFC 2543	—
SKINNY（SCCP）	TCP/2000	外部 NAT はサポートされません。 同一セキュリティのインターフェイス上の NAT はサポートされません。	—	一定の条件下で、Cisco IP Phone 設定をアップロード済みの TFTP は処理しません。
SMTP および **ESMTP**	TCP/25	—	RFC 821、1123	—
SNMP	UDP/161、162	NAT および PAT はサポートされません。	RFC 1155、1157、1212、1213、1215	v.2 RFC 1902 ～ 1908、v.3 RFC 2570 ～ 2580
SQL*Net	TCP/1521	—	—	v.1 および v.2
Sun RPC over UDP および TCP	UDP/111	NAT および PAT はサポートされません。	—	デフォルトのルールには UDP ポート 111 が含まれています。TCP ポート 111 の Sun RPC インスペクションをイネーブルにする場合は、TCP ポート 111 を照合する新しいルールを作成し、Sun RPC インスペクションを実行する必要があります。

表 24-1　サポートされているアプリケーション インスペクション エンジン （続き）

アプリケーション[1]	デフォルト ポート	NAT に関する制限事項	標準[2]	コメント
TFTP	UDP/69	—	RFC 1350	ペイロード IP アドレスは変換されません。
XDCMP	UDP/177	NAT および PAT はサポートされません。	—	—

1. デフォルト ポートに対してデフォルトでイネーブルになっているインスペクション エンジンは太字で表記されています。
2. セキュリティ アプライアンス は、これらの標準に準拠していますが、検査対象のパケットには準拠を強制しません。たとえば、各 FTP コマンドは特定の順序である必要がありますが、セキュリティ アプライアンス によってその順序を強制されることはありません。

アプリケーション検査の設定

この機能では、サービス ポリシー ルールを使用します。サービス ポリシーでは、一貫性と柔軟性を備えた方法で セキュリティ アプライアンス 機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。詳細については、「第 23 章「サービス ポリシー ルールの設定」」を参照してください。

一部のアプリケーションでは、デフォルトでインスペクションがイネーブルになっています。詳細については、「デフォルトの検査ポリシー」を参照してください。この項を参照してインスペクション ポリシーを変更してください。

アプリケーション インスペクションを設定する手順は、次のとおりです。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] をクリックします。

ステップ 2　「通過トラフィックのサービス ポリシー ルールの追加」（P.23-4）を参照して、サービス ポリシー ルールを追加または編集します。

標準以外のポートを照合する場合は、非標準ポート用の新しいルールを作成します。各インスペクション エンジンの標準ポートについては、「デフォルトの検査ポリシー」（P.24-3）を参照してください。必要に応じて同じサービス ポリシー内に複数のルールを組み合わせることができるため、照合するトラフィックに応じたルールを作成できます。ただし、トラフィックがインスペクション アクションを含むルールと一致し、その後同様にインスペクション アクションを含む別のルールとも一致した場合、最初に一致したルールだけが使用されます。

ステップ 3　[Edit Service Policy Rule] > [Rule Actions] ダイアログボックスで、[Protocol Inspection] タブをクリックします。

新しいルールの場合、[Add Service Policy Rule Wizard - Rule Actions] というダイアログボックス名が表示されます。

ステップ 4　適用する各インスペクション タイプをオンにします。

ステップ 5　（任意）一部のインスペクション エンジンでは、トラフィックにインスペクションを適用するときの追加パラメータを制御できます。インスペクション マップを設定するには、各インスペクション タイプの [Configure] をクリックします。

既存のマップを選択することも、新しいマップを作成することもできます。[Configuration] > [Firewall] > [Objects] > [Inspect Maps] ペインから、インスペクション マップを事前に定義できます。各インスペクション マップ タイプの詳細については、「インスペクション マップのフィールドの説明」（P.24-61）を参照してください。

ステップ 6　必要に応じて、他の [Rule Actions] タブを使用し、このルールに対して他の機能を設定できます。

ステップ 7　[OK] をクリックします（またはウィザードで [Finish] をクリックします）。

CTIQBE インスペクション

この項では、CTIQBE アプリケーション インスペクションについて説明します。この項では、次のトピックについて取り上げます。

CTIQBE インスペクションの概要

CTIQBE プロトコル インスペクションは、NAT、PAT、および双方向 NAT をサポートします。これによって、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と連動し、セキュリティ アプライアンス を越えてコール セットアップを行えるようになります。

TAPI と JTAPI は、多くの Cisco VoIP アプリケーションで使用されます。CTIQBE は、Cisco TSP が Cisco CallManager と通信するために使用されます。

制限事項

CTIQBE アプリケーション インスペクションの使用時に適用される制限を次にまとめます。

- CTIQBE アプリケーション インスペクションは、**alias** コマンドを使用するコンフィギュレーションをサポートしません。
- CTIQBE コールのステートフル フェールオーバーはサポートされていません。
- **debug ctiqbe** コマンドを入力すると、メッセージの伝送が遅れる場合があり、リアルタイム環境のパフォーマンスに影響することがあります。このデバッグまたはログをイネーブルにし、セキュリティ アプライアンス を介して Cisco IP SoftPhone でコール セットアップを完了できない場合は、Cisco IP SoftPhone の動作するシステムで Cisco TSP 設定のタイムアウト値を増やしてください。

次に、CTIQBE アプリケーション インスペクションを特定の事例で使用する際に、特別に注意が必要な事項をまとめます。

- 2 つの Cisco IP SoftPhone が異なる Cisco CallManager に登録されていて、各 CallManager が セキュリティ アプライアンス の異なるインターフェイスに接続されている場合、これら 2 つの電話間のコールは失敗します。
- Cisco IP SoftPhone と比較して Cisco CallManager の方がセキュリティの高いインターフェイス上に配置されている状態で、NAT または外部 NAT が Cisco CallManager IP アドレスに必要な場合、マッピングはスタティックである必要があります。Cisco IP SoftPhone では Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定することが必要なためです。
- PAT または外部 PAT の使用時に Cisco CallManager IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録させるには、TCP ポート 2748 を PAT（インターフェイス）アドレスと同じポートにスタティックにマッピングする必要があります。CTIQBE 受信ポート（TCP 2748）は固定されていて、Cisco CallManager、Cisco IP SoftPhone、Cisco TSP のいずれにおいてもユーザによる設定はできません。

DCERPC インスペクション

DCERPC は、Microsoft 社の分散クライアント/サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。

通常、このプロトコルの接続では、クライアントが予約済みポート番号で接続を受け入れるエンドポイント マッパーというサーバに、必要なサービスについてダイナミックに割り当てられるネットワーク情報を問い合わせます。次に、クライアントは、サービスを提供しているサーバのインスタンスへのセカンダリ接続をセットアップします。セキュリティ アプライアンスは、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許可し、必要に応じて Network Address Translation（NAT; ネットワーク アドレス変換）を適用します。

DCERPC インスペクション マップは、TCP の予約済みポート 135 を経由した、EPM とクライアント間のネイティブ TCP の通信を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバは、どのセキュリティ ゾーンにあってもかまいません。埋め込まれたサーバの IP アドレスとポート番号は、EPM からの応答メッセージで受け取ります。クライアントが EPM から返されたサーバのポートに対して複数の接続を試みる可能性があるので、ピンホールが複数使用でき、ユーザがそのタイムアウトを設定できるようになっています。

DNS インスペクション

この項では、DNS アプリケーション インスペクションについて説明します。この項では、次のトピックについて取り上げます。

- 「DNS アプリケーション インスペクションの動作」（P.24-7）
- 「DNS リライトの動作」（P.24-8）

DNS アプリケーション インスペクションの動作

セキュリティ アプライアンス で DNS 応答が転送されるとすぐに、セキュリティ アプライアンス は DNS クエリーに関連付けられた DNS セッションを切断します。セキュリティ アプライアンス はまた、メッセージ交換をモニタして DNS 応答の ID が DNS クエリーの ID と一致することを確認します。

DNS インスペクションをイネーブルにすると（デフォルト）、セキュリティ アプライアンス は次の追加のタスクを実行します。

- NAT ルールを使用して作成されたコンフィギュレーションに基づいて DNS レコードを変換します。変換は、DNS 応答の A レコードだけに適用されるため、DNS リライトによって PTR レコードを必要とする逆ルックアップが影響を受けることはありません。

（注） 1 つの A レコードには複数の PAT ルールが適用可能で、使用する PAT ルールがあいまいなため、DNS リライトは PAT には適用できません。

- 最大 DNS メッセージ長を指定します（デフォルトは 512 バイト、最大長は 65535 バイト）。セキュリティ アプライアンス は必要に応じてリアセンブリを実行し、パケット長が設定されている最大長よりも短いことを確認します。セキュリティ アプライアンス は、最大長を超えるパケットをドロップします。
- ドメイン名の長さを 255 バイトに制限し、ラベルの長さを 63 バイトに制限します。

- DNS メッセージに圧縮ポインタが出現した場合、ポインタが参照するドメイン名の整合性を確認します。
- 圧縮ポインタのループが終了するかどうかを確認します。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元/宛先 IP アドレス、送信元/宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つだけ作成されます。DNS ID は *app_id* で追跡され、各 app_id のアイドル タイマーは独立して実行されます。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内だけであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力した場合、新しい DNS セッションによってリセットされている DNS 接続のアイドル タイマーが表示されます。これは共有 DNS 接続の性質によるものであり、仕様です。

DNS リライトの動作

DNS インスペクションがイネーブルであるとき、DNS リライトは、任意のインターフェイスから送信された DNS メッセージの NAT を完全にサポートします。

内部のネットワーク上のクライアントが、外部インターフェイス上の DNS サーバから送信される内部アドレスの DNS 解決を要求した場合、DNS A レコードは正しく変換されます。DNS インスペクション エンジンがディセーブルである場合、A レコードは変換されません。

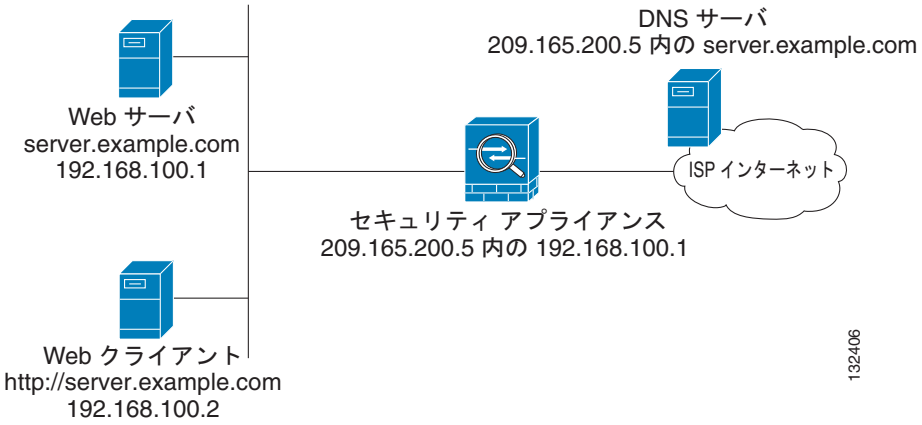
DNS インスペクションがイネーブルであれば、NAT ルールを使用して DNS リライトを設定できます。

DNS リライトは次の 2 つの機能を実行します。

- DNS クライアントがプライベート インターフェイスにある場合、*DNS 応答*のパブリック アドレス（ルーティング可能なアドレスまたは「マッピング」アドレス）をプライベート アドレス（「実際の」アドレス）に変換します。
- DNS クライアントがパブリック インターフェイスにある場合、プライベート アドレスをパブリック アドレスに変換します。

図 24-1 では、DNS サーバは外部（ISP）ネットワークにあります。サーバの実際のアドレス（192.168.100.1）は、スタティック NAT ルールを使用して ISP が割り当てるアドレス（209.165.200.5）にマッピングされています。内部インターフェイスの Web クライアントが http://server.example.com という URL の Web サーバにアクセスしようとすると、Web クライアントが動作するホストが、Web サーバの IP アドレスの解決を求める DNS 要求を DNS サーバに送信します。セキュリティ アプライアンス は、IP ヘッダーに含まれるルーティング不可の送信元アドレスを変換し、外部インターフェイスの ISP ネットワークに要求を転送します。DNS 応答が返されると、セキュリティ アプライアンス はアドレス変換を宛先アドレスだけではなく、DNS 応答の A レコードに含まれる、埋め込まれた Web サーバの IP アドレスにも適用します。結果として、内部ネットワーク上の Web クライアントは、内部ネットワーク上の Web サーバとの接続に使用する正しいアドレスを取得します。

図 24-1　DNS 応答に含まれるアドレスの変換（DNS リライト）



DNS リライトは、DNS 要求を作成するクライアントが DMZ ネットワークにあり、DNS サーバが内部インターフェイスにある場合にも機能します。

ESMTP インスペクション

ESMTP インスペクションは、スパム、フィッシング、不正な形式のメッセージによる攻撃、バッファオーバーフロー / アンダーフロー攻撃を検出します。また、アプリケーション セキュリティとプロトコル準拠により、正常な ESMTP メッセージだけを通し、各種の攻撃の検出や送受信者およびメール中継のブロックも行います。

FTP インスペクション

この項では、FTP インスペクション エンジンについて説明します。この項では、次のトピックについて取り上げます。

- 「FTP インスペクションの概要」（P.24-9）
- 「厳密な FTP の使用方法」（P.24-10）
- 「FTP 検査の確認とモニタリング」（P.24-11）

FTP インスペクションの概要

FTP アプリケーション インスペクションは、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックな二次的データ接続の準備
- FTP コマンド応答シーケンスの追跡
- 監査証跡の生成
- 埋め込み IP アドレスの変換

FTP アプリケーション インスペクションによって、FTP データ転送用にセカンダリ チャネルが用意されます。これらのチャネルのポートは、PORT コマンドまたは PASV コマンドを使用してネゴシエートされます。セカンダリ チャネルは、ファイル アップロード、ファイル ダウンロード、またはディレクトリ リスト イベントへの応答で割り当てられます。

（注）　FTP インスペクション エンジンをディセーブルにすると、発信ユーザはパッシブ モードでしか接続を開始できなくなり、着信 FTP はすべてディセーブルになります。

厳密な FTP の使用方法

strict オプションにより厳密な FTP を使用すると、Web ブラウザが FTP 要求内の埋め込みコマンドを送信できなくなるため、保護されたネットワークのセキュリティが強化されます。厳密な FTP をイネーブルにするには、[Configuration] > [Firewall] > [Service Policy Rules] > [Edit Service Policy Rule] > [Rule Actions] > [Protocol Inspection] タブで、FTP の横にある [Configure] ボタンをクリックします。

（注）　セキュリティ アプライアンスの通過を禁止する FTP コマンドを指定するには、「FTP Class Map」（P.24-44）にしたがって FTP インスペクション マップを作成します。

インターフェイスに対して Strict オプションをオンにすると、FTP インスペクションによって次の動作が適用されます。

- FTP コマンドが確認応答されてからでないと、セキュリティ アプライアンスは新しいコマンドを許可しません。
- セキュリティ アプライアンスは、埋め込みコマンドを送信する接続をドロップします。
- 227 コマンドと PORT コマンドが、エラー文字列に表示されないように確認されます。

注意　strict オプションを使用すると、FTP RFC に厳密に準拠していない FTP クライアントは失敗することがあります。

strict オプションがイネーブルの場合、各 FTP コマンドと応答シーケンスが追跡され、次の異常なアクティビティがないか確認されます。

- 切り捨てされたコマンド：PORT コマンドおよび PASV 応答コマンドのカンマの数が 5 であるかどうかが確認されます。カンマの数が 5 でない場合は、PORT コマンドが切り捨てられていると見なされ、TCP 接続は閉じられます。
- 不正なコマンド：FTP コマンドが、RFC の要求どおりに <CR><LF> 文字で終了しているかどうか確認されます。終了していない場合は、接続が閉じられます。
- RETR コマンドと STOR コマンドのサイズ：これらが、固定の定数と比較チェックされます。サイズが定数より大きい場合は、エラー メッセージがロギングされ、接続が閉じられます。
- コマンド スプーフィング：PORT コマンドは、常にクライアントから送信されます。PORT コマンドがサーバから送信される場合、TCP 接続は拒否されます。
- 応答スプーフィング：PASV 応答コマンド（227）は、常にサーバから送信されます。PASV 応答コマンドがクライアントから送信される場合、TCP 接続は拒否されます。これにより、ユーザが「227 xxxxx a1, a2, a3, a4, p1, p2.」を実行する場合のセキュリティ ホールが予防できます。
- TCP ストリーム編集：セキュリティ アプライアンスは、TCP ストリーム編集を検出した場合に接続が閉じられます。

- 無効ポート ネゴシエーション：ネゴシエートされたダイナミック ポート値が、1024 未満であるかどうかが調べられます。1 ～ 1024 の範囲のポート番号は、予約済み接続用に指定されているため、ネゴシエートされたポートがこの範囲内であった場合、TCP 接続は解放されます。
- コマンド パイプライン：PORT コマンドと PASV 応答コマンド内のポート番号の後に続く文字数が、定数の 8 と比べられます。8 より大きい場合は、TCP 接続が閉じられます。
- セキュリティ アプライアンスは、SYST コマンドに対する FTP サーバ応答を X の連続に置き換えることで、FTP クライアントがサーバのシステム タイプを取得できないようにします。このデフォルトの動作を無効にするには、FTP マップで Low 設定を使用します。

FTP 検査の確認とモニタリング

FTP アプリケーション インスペクションでは、次のログ メッセージが生成されます。

- An Audit record 302002 is generated for each file that is retrieved or uploaded.
- The FTP command is checked to see if it is RETR or STOR and the retrieve and store commands are logged.
- The username is obtained by looking up a table providing the IP address.
- The username, source IP address, destination IP address, NAT address, and the file operation are logged.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

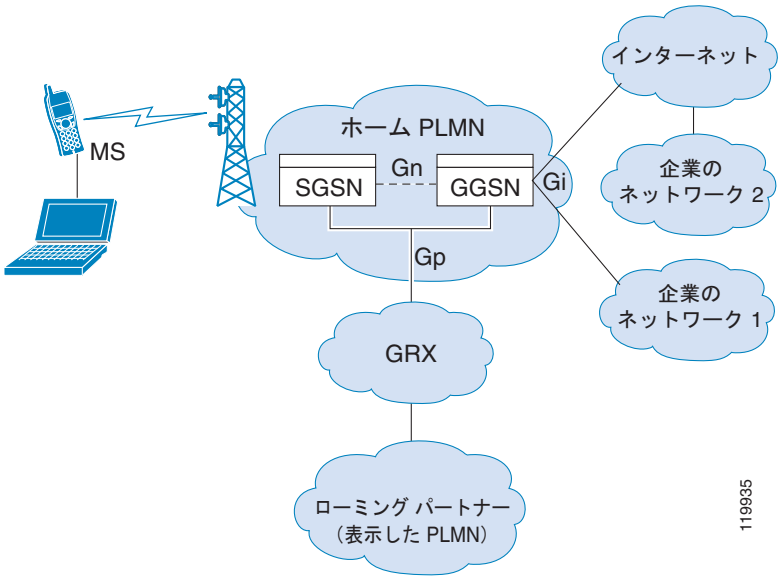
NAT と連携することにより、FTP アプリケーション インスペクションでは、アプリケーション ペイロード内の IP アドレスが変換されます。これは、RFC 959 に詳細に記述されています。

GTP インスペクション

（注）　GTP インスペクションには、特別なライセンスが必要です。

GPRS は、モバイル ユーザに対して、GSM ネットワークと企業ネットワークまたはインターネットとの間で中断しない接続を提供します。GGSN は、GPRS 無線データ ネットワークと他のネットワークとの間のインターフェイスです。SGSN は、モビリティ、データ セッション管理、およびデータ圧縮を実行します（図 24-2 を参照）。

図 24-2　GPRS トンネリング プロトコル



UMTS は、固定回線テレフォニー、モバイル、インターネット、コンピュータ テクノロジーの商用コンバージェンスです。UTRAN は、このシステムで無線ネットワークを実装するためのネットワーキング プロトコルです。GTP を使用すると、GGSN、SGSN、および UTRAN 間の UMTS/GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。

GTP には固有のセキュリティやユーザ データの暗号化は含まれていませんが、セキュリティ アプライアンス で GTP を使用することによって、これらの危険性からネットワークを保護できます。

SGSN は、GTP を使用する GGSN に論理的に接続されます。GTP を使用すると、GSN 間の GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによって、SGSN は、トンネルの作成、変更、および削除を行い、モバイル ステーションに GPRS ネットワーク アクセスを提供できます。GTP は、トンネリング メカニズムを使用して、ユーザ データ パケットを伝送するためのサービスを提供します。

（注）　GTP をフェールオーバーと同時に使用しているとき、GTP 接続が確立され、データがトンネルを超えて伝送される前にアクティブ装置に障害が発生した場合、GTP データ接続（「j」フラグが設定されています）は、スタンバイ装置に複製されません。これは、アクティブ装置が初期接続をスタンバイ装置に複製しないためです。

H.323 インスペクション

この項では、H.323 アプリケーション インスペクションについて説明します。この項では、次のトピックについて取り上げます。

- 「H.323 インスペクションの概要」（P.24-13）
- 「H.323 の動作」（P.24-13）
- 「制限事項」（P.24-14）

H.323 インスペクションの概要

H.323 インスペクションは、Cisco CallManager や VocalTec Gatekeeper など、H.323 準拠のアプリケーションをサポートします。H.323 は、International Telecommunication Union（ITU; 国際電気通信連合）によって定義されている、LAN を介したマルチメディア会議用のプロトコル群です。セキュリティ アプライアンスは、H.323 v3 機能の同一コール シグナリング チャネルでの複数コールを含めて、H.323 を Version 4 までサポートします。

H.323 検査をイネーブルにした場合、セキュリティ アプライアンスは、H.323 Version 3 で導入された機能である同一コール シグナリング チャネルでの複数コールをサポートします。この機能によってセットアップ時間が短縮され、セキュリティ アプライアンス でのポート使用が減少します。

H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、セキュリティ アプライアンス では ASN.1 デコーダを使用して H.323 メッセージを復号化します。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。

H.323 の動作

H.323 のプロトコル コレクションでは、あわせて最大 2 つの TCP 接続と 4 ～ 6 つの UDP 接続を使用できます。FastConnect は 1 つの TCP 接続だけを使用し、RAS は登録、アドミッション、およびステータス用に 1 つの UDP 接続を使用します。

H.323 クライアントは最初に、TCP ポート 1720 を使用して H.323 サーバへの TCP 接続を確立し、Q.931 コール設定を要求します。H.323 端末は、コール セットアップ プロセスの一部として、H.245 TCP 接続に使用するため、クライアントに 1 つのポート番号を供給します。H.323 ゲートキーパーが使用されている環境では、初期パケットは UDP を使用して送信されます。

H.323 インスペクションは、Q.931 TCP 接続をモニタして、H.245 ポート番号を決定します。H.323 端末が、FastConnect を使用していない場合は、セキュリティ アプライアンス が H.225 メッセージのインスペクションに基づいて、H.245 接続をダイナミックに割り当てます。

各 H.245 メッセージ内で、H.323 エンドポイントが、後続の UDP データ ストリームに使用するポート番号を交換します。H.323 インスペクションは、H.245 メッセージを調査して、ポート番号を識別し、メディア交換用の接続をダイナミックに作成します。RTP はネゴシエートされたポート番号を使用し、RTCP はその次に高いポート番号を使用します。

H.323 制御チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 インスペクションでは、次のポートが使用されます。

- 1718：ゲートキーパー検出 UDP ポート
- 1719：RAS UDP ポート
- 1720：TCP 制御ポート

H.225 コール シグナリングについて、well-known の H.323 ポート 1720 のトラフィックを許可しておく必要があります。ただし、H.245 シグナリング ポートは、H.225 シグナリング内のエンドポイントの間でネゴシエートされます。H.323 ゲートキーパーが使用されると、セキュリティ アプライアンスは ACF メッセージのインスペクションに基づいて H.225 接続を開きます。

H.225 メッセージを検査した後、セキュリティ アプライアンス は H.245 チャネルを開き、H.245 チャネルで送信されるトラフィックも検査します。セキュリティ アプライアンスを通過するすべての H.245 メッセージは、H.245 アプリケーション インスペクションを受けます。このインスペクションでは、埋め込み IP アドレスが変換され、H.245 メッセージでネゴシエートされたメディア チャネルが開かれます。

H.323 ITU 規準では、メッセージ長を定義する TPKT ヘッダーが最初に送信されてから、H.225 と H.245 が信頼できる接続上を送信されることが要求されています。TPKT ヘッダーは、必ずしも H.225 メッセージや H.245 メッセージと同一の TCP パケットで送信される必要はないため、セキュリティ アプライアンス は、メッセージを正しく処理して復号化するために TPKT 長を記憶しておく必要があります。セキュリティ アプライアンスは、次のメッセージに備えて、TPKT 長が含まれるレコードを接続ごとに保持します。

セキュリティ アプライアンスでメッセージ内の IP アドレスに NAT を行う必要がある場合、チェックサム、UUIE 長、および TPKT（H.225 メッセージが入っている TCP パケットに含まれている場合）は変更されます。TPKT が別の TCP パケットで送信される場合、セキュリティ アプライアンス がその TPKT へのプロキシ ACK を実行し、新しい TPKT を新しい長さで H.245 メッセージに追加します。

（注）　セキュリティ アプライアンスは、TPKT に対する ACK の代理処理では TCP オプションをサポートしていません。

H.323 インスペクションを受けるパケットが通る各 UDP 接続は、H.323 接続としてマークされ、[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインで設定された H.323 タイムアウト値でタイムアウトします。

制限事項

H.323 アプリケーション インスペクションの使用に関して、次の既知の問題および制限があります。

- スタティック PAT は、H.323 メッセージのオプション フィールドに埋め込まれた IP アドレスを正しく変換できないことがあります。この問題が発生した場合は、H.323 でスタティック PAT を使用しないでください。
- H.323 アプリケーション インスペクションは、同一セキュリティ レベルのインターフェイス間の NAT ではサポートされていません。
- NetMeeting クライアントが H.323 ゲートキーパーに登録し、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイを呼び出そうとすると、接続は確立されますが、どちらの方向でも音声が聞こえません。この問題は、セキュリティ アプライアンス の問題ではありません。
- ネットワーク スタティック アドレスを設定した場合、このネットワーク スタティック アドレスが第三者のネットマスクおよびアドレスと同じであると、すべての発信 H.323 接続が失敗します。

HTTP インスペクション

HTTP インスペクション エンジンを使用して、特定の攻撃、および HTTP トラフィックに関係する可能性があるその他の脅威から保護します。HTTP インスペクションは、次のようないくつかの機能を実行します。

- 拡張 HTTP インスペクション
- N2H2 または Websense を使用する URL のスクリーニング
- Java と ActiveX のフィルタリング

2 つ目と 3 つ目の機能は、フィルタ ルールと共に設定します。

拡張 HTTP インスペクション機能はアプリケーション ファイアウォールとも呼ばれ、HTTP インスペクション マップを設定すると使用できます（「HTTP Class Map」（P.24-50）を参照）。この機能を使用すると、攻撃者が HTTP メッセージを使用してネットワーク セキュリティ ポリシーを回避することを阻止できます。この機能は、すべての HTTP メッセージについて次のことを確認します。

- RFC 2616 への準拠
- RFC で定義された方式だけを使用していること
- 追加の基準への準拠

インスタント メッセージ インスペクション

インスタント メッセージ（IM）インスペクション エンジンを使用すると、IM アプリケーションの制御を細かく調整して、ネットワークの使用を制御し、機密情報の漏洩やワームの繁殖などの企業のネットワークへの脅威を阻止できます。

ICMP インスペクション

ICMP インスペクション エンジンを使用すると、ICMP トラフィックが「セッション」を持つようになるため、TCP トラフィックや UDP トラフィックのように検査することが可能になります。ICMP インスペクション エンジンを使用しない場合、アクセス リストで ICMP にセキュリティ アプライアンスの通過を許可しないことをお勧めします。ステートフル インスペクションを実行しないと、ICMP がネットワーク攻撃に利用される可能性があります。ICMP インスペクション エンジンは、要求ごとに応答が 1 つだけであること、シーケンス番号が正しいことを確認します。

ICMP エラー インスペクション

この機能がイネーブルの場合、セキュリティ アプライアンスは、NAT コンフィギュレーションに基づいて ICMP エラー メッセージを送信する中間ホップ用の変換セッションを作成します。セキュリティ アプライアンスは、変換後の IP アドレスでパケットを上書きします。

ディセーブルの場合、セキュリティ アプライアンスは、ICMP エラー メッセージを生成する中間ノード用の変換セッションを作成しません。内部ホストとセキュリティ アプライアンスの間にある中間ノードによって生成された ICMP エラー メッセージは、NAT リソースをそれ以上消費することなく、外部ホストに到達します。外部ホストが traceroute コマンドを使用してセキュリティ アプライアンスの内部にある宛先までのホップをトレースする場合、これは適切ではありません。セキュリティ アプライアンスが中間ホップを変換しない場合、すべての中間ホップは、マッピングされた宛先 IP アドレスとともに表示されます。

ICMP ペイロードがスキャンされて、元のパケットから 5 つのタプルが取得されます。取得した 5 つのタプルを使用してルックアップを実行し、クライアントの元のアドレスを判別します。ICMP エラー インスペクション エンジンは、ICMP パケットに対して次の変更を加えます。

- IP ヘッダー内のマッピング IP を実際の IP（宛先アドレス）に変更し、IP チェックサムを修正する。
- ICMP パケットに変更を加えたため、ICMP ヘッダー内の ICMP チェックサムを修正する。
- ペイロードに次の変更を加える。
  - 元のパケットのマッピング IP を実際の IP に変更する。
  - 元のパケットのマッピング ポートを実際のポートに変更する。
  - 元のパケットの IP チェックサムを再計算する。

ILS インスペクション

ILS インスペクション エンジンは、LDAP を使用してディレクトリ情報を ILS サーバと交換する Microsoft NetMeeting、SiteServer、および Active Directory の各製品に対して Network Address Translation（NAT; ネットワーク アドレス変換）をサポートします。

セキュリティ アプライアンス は ILS に対して NAT をサポートします。NAT は、ILS または SiteServer Directory のエンドポイントの登録および検索で使用されます。LDAP データベースには IP アドレスだけが保存されるため、Port Address Translation（PAT; ポート アドレス交換）はサポートされません。

LDAP サーバが外部にある場合、内部ピアが外部 LDAP サーバに登録された状態でローカルに通信できるように、検索応答に対して NAT を行うことを検討してください。このような検索応答では、最初に xlate が検索され、次に DNAT エントリが検索されて正しいアドレスが取得されます。これらの検索が両方とも失敗した場合、アドレスは変更されません。NAT 0（NAT なし）を使用していて、DNAT の相互作用を想定していないサイトの場合は、パフォーマンスを向上させるためにインスペクション エンジンをオフにすることをお勧めします。

ILS サーバがセキュリティ アプライアンス境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが指定されたポート（通常は TCP 389）の LDAP サーバにアクセスするためのホールが必要となります。

ILS トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は一定の間隔 TCP アクティビティがなければ切断されます。デフォルトでは、この間隔は 60 分です。この値は、[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインで設定できます。

ILS/LDAP はクライアント/サーバ モデルに従っており、セッションは 1 つの TCP 接続で処理されます。クライアントのアクションに応じて、このようなセッションがいくつか作成されることがあります。

接続ネゴシエーション時間中、クライアントからサーバに BIND PDU が送信されます。サーバから成功を示す BIND RESPONSE を受信すると、ILS Directory に対する操作を実行するためのその他の操作メッセージ（ADD、DEL、SEARCH、MODIFY など）が交換される場合があります。ADD REQUEST PDU および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323（SETUP および CONNECT メッセージ）によって使用される、NetMeeting ピアの IP アドレスが含まれている場合があります。Microsoft NetMeeting v2.X および v3.X は、ILS をサポートしています。

ILS インスペクションでは、次の操作が実行されます。

- BER 復号化機能を使用して LDAP REQUEST PDU/RESPONSE PDU を復号化する。
- LDAP パケットを解析する。
- IP アドレスを抽出する。
- 必要に応じて IP アドレスを変換する。
- BER 符号化機能を使用して、変換後のアドレスが含まれる PDU を符号化する。
- 新しく符号化された PDU を元の TCP パケットにコピーする。
- TCP チェックサムとシーケンス番号の増分を調整する。

ILS インスペクションには、次の制限事項があります。

- 参照要求および応答はサポートされない。
- 複数のディレクトリ内のユーザは統合されない。
- 1 人のユーザが複数のディレクトリで複数の ID を持つ場合、NAT はそのユーザを認識できない。

（注）　H225 コール シグナリング トラフィックはセカンダリ UDP チャネルだけで発生するため、[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインの TCP オプションで指定された間隔が経過すると、TCP 接続は切断されます。デフォルトで、この間隔は 60 分に設定されています。

IPSec パススルー検査

Internet Protocol Security（IPSec）は、データ ストリームの各 IP パケットを認証および暗号化することによって、IP 通信をセキュリティで保護するためのプロトコル スイートです。IPSec には、セッションの開始時、およびセッション中に使用される暗号キーのネゴシエーション時に、エージェント間の相互認証を確立するためのプロトコルも含まれています。IPSec を使用して、ホスト（コンピュータ ユーザまたはサーバなど）のペア間、セキュリティ ゲートウェイ（ルータやファイアウォールなど）のペア間、またはセキュリティ ゲートウェイとホスト間のデータ フローを保護できます。

IPSec パススルー アプリケーション インスペクションは、IKE UDP ポート 500 接続に関連付けられた ESP（IP プロトコル 50）および AH（IP プロトコル 51）トラフィックを簡単に横断できます。このインスペクションは、冗長なアクセス リスト コンフィギュレーションを回避して ESP および AH トラフィックを許可し、タイムアウトと最大接続数を使用してセキュリティも確保します。

検査用パラメータの定義に使用する特定のマップを識別するには、IPSec パススルー検査パラメータを指定します。所定の IPSec パススルー検査のポリシーマップを設定し、パラメータ コンフィギュレーションにアクセスします。このコンフィギュレーションでは、ESP または AH トラフィックの制限を指定できます。パラメータ コンフィギュレーションでは、クライアントあたりの最大接続数と、アイドル タイムアウトを設定できます。

NAT および非 NAT トラフィックは許可されます。ただし、PAT はサポートされません。

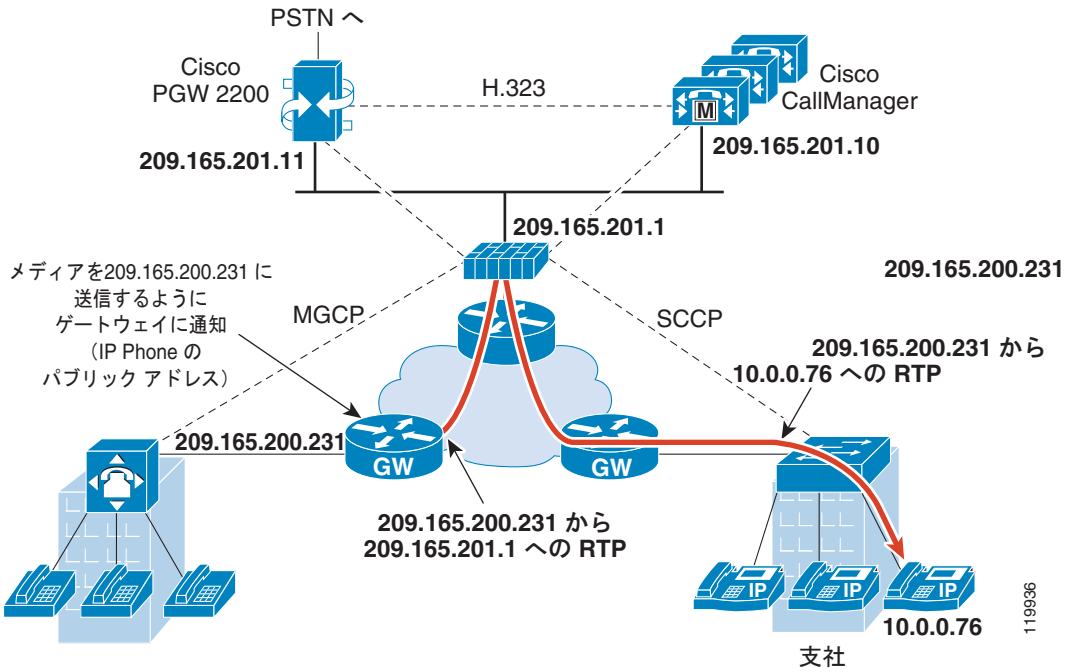
MGCP インスペクション

MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部のコール制御要素からメディア ゲートウェイを制御するために使用するマスター / スレーブ プロトコルです。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP とともに使用すると、限られた外部（グローバル）アドレスのセットで、内部ネットワークの多数のデバイスをサポートできます。メディア ゲートウェイの例は次のとおりです。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ（RJ11）インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブル モデムやケーブル セットトップ ボックス、xDSL デバイス、ブロードバンド ワイヤレス デバイスなどがあります。
- ビジネス ゲートウェイ。従来のデジタル PBX（構内交換機）インターフェイスまたは統合 *soft PBX* インターフェイスを Voice over IP ネットワークに提供します。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス（IP アドレスと UDP ポート番号）に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用されているときに、コマンドを受信したコール エージェントが制御をバックアップ コール エージェントに引き渡し、バックアップ コール エージェントが応答を送信する場合に起こる可能性があります。図 24-3 に、MGCP でどのように NAT が使用されるかを示します。

図 24-3　NAT と MGCP の使用



MGCP エンドポイントは、物理または仮想のデータ送信元および宛先です。メディア ゲートウェイには、他のマルチメディア エンドポイントとのメディア セッションを確立して制御するために、コール エージェントが接続を作成、変更、および削除できるエンドポイントが含まれています。また、コール エージェントは、特定のイベントを検出してシグナルを生成するようにエンドポイントに指示できます。エンドポイントは、サービス状態の変化を自動的にコール エージェントに伝達します。

MGCP トランザクションは、コマンドと必須応答で構成されます。次の 8 種類のコマンドがあります。

- CreateConnection
- ModifyConnection
- DeleteConnection
- NotificationRequest
- Notify
- AuditEndpoint
- AuditConnection
- RestartInProgress

最初の 4 つのコマンドは、コール エージェントからゲートウェイに送信されます。Notify コマンドは、ゲートウェイからコール エージェントに送信されます。ゲートウェイは、DeleteConnection を送信することもあります。MGCP ゲートウェイをコール エージェントに登録するには、RestartInProgress コマンドを使用します。AuditEndpoint コマンドおよび AuditConnection コマンドは、コール エージェントからゲートウェイに送信されます。

すべてのコマンドは、コマンド ヘッダーと、その後ろに続くオプションのセッション記述で構成されます。すべての応答は、応答ヘッダーと、その後ろに続くオプションのセッション記述で構成されます。

- ゲートウェイがコール エージェントからのコマンドを受信するポート。通常、ゲートウェイは UDP ポート 2427 を受信します。

- コール エージェントがゲートウェイからのコマンドを受信するポート。通常、コール エージェントは UDP ポート 2727 を受信します。

（注）　MGCP インスペクションでは、MGCP シグナリングと RTP データで異なる IP アドレスを使用することはサポートされていません。一般的かつ推奨される方法は、ループバック IP アドレスや仮想 IP アドレスなどの復元力のある IP アドレスから RTP データを送信することです。ただし、セキュリティ アプライアンス は、MGCP シグナリングと同じアドレスから RTP データを受信する必要があります。

NETBIOS インスペクション

NETBIOS インスペクションはデフォルトでイネーブルになっています。NetBios インスペクション エンジンは、セキュリティ アプライアンスの NAT コンフィギュレーションに基づいて、NetBios Name Service（NBNS; NetBios ネーム サービス）パケット内の IP アドレスを変換します。

PPTP インスペクション

PPTP は、PPP トラフィックのトンネリングに使用されるプロトコルです。PPTP セッションは、1 つの TCP チャネルと通常 2 つの PPTP GRE トンネルで構成されます。TCP チャネルは、PPTP GRE トンネルのネゴシエートと管理に使用される制御チャネルです。GRE トンネルは、2 つのホスト間の PPP セッションを伝送します。

PPTP アプリケーション インスペクションは、イネーブルになると、PPTP プロトコル パケットを検査し、PPTP トラフィックを許可するために必要な GRE 接続と xlate をダイナミックに作成します。RFC 2637 で定義されているバージョン 1 だけがサポートされます。

PAT は、PPTP TCP 制御チャネル上で修正バージョンの GRE（RFC 2637）がネゴシエートされたときに、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行 *されません*。

具体的には、セキュリティ アプライアンスは、PPTP のバージョン通知と発信コールの要求/応答シーケンスを検査します。RFC 2637 で定義されている PPTP バージョン 1 だけが検査されます。どちらかの側から通知されたバージョンがバージョン 1 でない場合、TCP 制御チャネルでのそれ以降のインスペクションはディセーブルになります。また、発信コールの要求と応答のシーケンスは追跡されます。接続と xlate は、後続のセカンダリ GRE データ トラフィックを許可するために、必要に応じてダイナミックに割り当てられます。

PPTP インスペクション エンジンは、PPTP トラフィックを PAT で変換できるように、イネーブルにする必要があります。また、PAT は、PPTP TCP 制御チャネルで修正バージョンの GRE（RFC 2637）がネゴシエートされた場合に限り、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行されません。

RFC 2637 で定義されているように、PPTP プロトコルは、主に、モデム バンク PPTP Access Concentrator（PAC; PPTP アクセス コンセントレータ）から開始されたヘッドエンド PPTP Network Server（PNS; PPTP ネットワーク サーバ）への PPP セッションのトンネリングに使用されます。このように使用された場合、PAC がリモート クライアントで PNS がサーバです。

ただし、Windows によって VPN で使用された場合、この関係は逆になります。PNS は、中央のネットワークにアクセスするためにヘッドエンド PAC への接続を開始するリモートのシングル ユーザ PC です。

RADIUS アカウンティング インスペクション

RADIUS アカウンティング インスペクションの詳細については、「Select RADIUS Accounting Map」（P.23-13）を参照してください。

RSH インスペクション

RSH インスペクションはデフォルトでイネーブルになっています。RSH プロトコルは、TCP ポート 514 で RSH クライアントから RSH サーバへの TCP 接続を使用します。クライアントとサーバは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インスペクションは、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

RTSP インスペクション

この項では、RTSP アプリケーション インスペクションについて説明します。この項では、次のトピックについて取り上げます。

RTSP インスペクションの概要

RTSP インスペクション エンジンを使用することにより、セキュリティ アプライアンスは RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV 接続によって使用されます。

（注）　Cisco IP/TV では、RTSP TCP ポート 554 と TCP 8554 を使用します。

RTSP アプリケーションは、制御チャネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。セキュリティ アプライアンスは、RFC 2326 に準拠して、TCP だけをサポートします。この TCP 制御チャネルは、クライアント上で設定されているトランスポート モードに応じて、音声 / ビデオ トラフィックの送信に使用されるデータ チャネルのネゴシエーションに使用されます。

サポートされている RDT トランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

セキュリティ アプライアンスは、ステータス コード 200 の SETUP 応答メッセージを解析します。SETUP 応答メッセージが、着信方向に移動している場合は、サーバは セキュリティ アプライアンスとの相対位置関係で外部に存在することになるため、サーバから着信する接続に対してダイナミック チャネルを開くことが必要になります。この応答メッセージが発信方向である場合、セキュリティ アプライアンス は、ダイナミック チャネルを開く必要はありません。

RFC 2326 では、クライアント ポートとサーバ ポートが、SETUP 応答メッセージ内に含まれていることは必要でないため、セキュリティ アプライアンス では、状態を維持し、SETUP メッセージ内のクライアント ポートを記憶します。QuickTime が、SETUP メッセージ内にクライアント ポートを設定すると、サーバは、サーバ ポートだけで応答します。

RTSP インスペクションは、PAT またはデュアル NAT をサポートしていません。また、セキュリティ アプライアンスは、RTSP メッセージが HTTP メッセージ内に隠される HTTP クローキングを認識できません。

RealPlayer の使用方法

RealPlayer を使用するときは、転送モードを正しく設定することが重要です。セキュリティ アプライアンスの場合、サーバからクライアントに、またはその逆にアクセス ルールを追加します。RealPlayer の場合、[Options] > [Preferences] > [Transport] > [RTSP] [Settings] をクリックして転送モードを変更します。

RealPlayer で TCP モードを使用する場合は、[Use TCP to Connect to Server] チェックボックスおよび [Attempt to use TCP for all content] チェックボックスをオンにします。セキュリティ アプライアンスで、インスペクション エンジンを設定する必要はありません。

RealPlayer で UDP モードを使用する場合、[Use TCP to Connect to Server] および [Attempt to use UDP for static content] チェックボックスをオンにします。マルチキャストでの使用ができないライブ コンテンツについては、セキュリティ アプライアンス で、**inspect rtsp** *port* コマンドを追加します。

制限事項

RTSP インスペクションには、次の制限が適用されます。

- セキュリティ アプライアンス は、マルチキャスト RTSP または UDP による RTSP メッセージをサポートしません。
- PAT はサポートされていません。
- セキュリティ アプライアンス には、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- 埋め込み IP アドレスが HTTP メッセージまたは RTSP メッセージの一部として SDP ファイル内に含まれているため、セキュリティ アプライアンスは、RTSP メッセージに NAT を実行できません。パケットはフラグメント化する可能性があり、セキュリティ アプライアンスはフラグメント化されたパケットに対して NAT を実行できません。
- Cisco IP/TV では、メッセージの SDP 部分に対してセキュリティ アプライアンスが実行する変換の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバが内部ネットワークにあるときにだけ NAT を使用できます。

SIP インスペクション

この項では、SIP アプリケーション インスペクションについて説明します。この項では、次のトピックについて取り上げます。

- 「SIP インスペクションの概要」（P.24-22）
- 「SIP インスタント メッセージ」（P.24-22）

SIP インスペクションの概要

IETF で定義されている SIP により、特に 2 者間の音声会議などのコール処理セッションまたは「コール」が使用可能になります。SIP は、コール シグナリング用の SDP で動作します。SDP は、メディア ストリーム用のポートを指定します。SIP を使用することにより、セキュリティ アプライアンス は SIP VoIP ゲートウェイおよび VoIP プロキシ サーバをサポートできます。SIP と SDP の定義は、次の RFC に記載されています。

- SIP：Session Initiation Protocol、RFC 2543
- SDP：Session Description Protocol、RFC 2327

セキュリティ アプライアンス経由の SIP コールをサポートする場合は、シグナリング メッセージは予約済みの宛先ポート（UDP/TCP 5060）経由で送信され、メディア ストリームはダイナミックに割り当てられるため、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。また、SIP は、IP パケットのユーザデータ部分に IP アドレスを埋め込みます。SIP インスペクションは、それらの埋め込まれた IP アドレスに NAT を適用します。

PAT を SIP で使用する場合、次の制限事項が適用されます。

- セキュリティ アプライアンスで保護されているネットワークの SIP プロキシにリモート エンドポイントを登録しようとすると、次のような一定の条件下で登録が失敗します。
  - PAT がリモート エンドポイント用に設定されている。
  - SIP レジストラ サーバが外部ネットワークにある。
  - エンドポイントからプロキシ サーバに送信された REGISTER メッセージの接続先フィールドにポートが設定されていない。
- SDP 部分の所有者 / 作成者フィールド（o=）の IP アドレスが接続フィールド（c=）の IP アドレスと異なるパケットを SIP デバイスが送信すると、o= フィールドの IP アドレスが正しく変換されない場合があります。これは、o= フィールドでポート値を提供しない SIP プロトコルの制限によるものです。

SIP インスタント メッセージ

インスタント メッセージとは、ほぼリアルタイムにユーザ間でメッセージを転送することです。SIP は、Windows Messenger RTC Client バージョン 4.7.0105 を使用する Windows XP のチャット機能のみをサポートします。次の RFC で定義されているように、MESSAGE/INFO 方式および 202 Accept 応答を使用して IM をサポートします。

- Session Initiation Protocol（SIP）Specific Event Notification、RFC 3265
- Session Initiation Protocol（SIP）Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録または加入の後、任意の時点で着信する可能性があります。たとえば、2 人のユーザはいつでもオンラインになる可能性がありますが、何時間もチャットをすることはありません。そのため、SIP インスペクション エンジンは、設定されている SIP タイムアウト値に従ってタイムアウトするピンホールを開きます。この値は、登録継続時間よりも 5 分以上長く設定する必要があります。登録継続時間は Contact Expires 値で定義し、通常 30 分です。

MESSAGE/INFO 要求は、通常、ポート 5060 以外の動的に割り当てられたポートを使用して送信されるため、SIP インスペクション エンジンを通過する必要があります。

（注） 現在は、チャット機能のみがサポートされています。ホワイトボード、ファイル転送、アプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

SIP インスペクションは、テキストベースの SIP メッセージを変換し、メッセージの SDP 部分の内容長を再計算した後、パケット長とチェックサムを再計算します。また、エンドポイントが受信すべきアドレスまたはポートとして、SIP メッセージの SDP 部分に指定されたポートに対するメディア接続をダイナミックに開きます。

SIP インスペクションでは、SIP ペイロードから取得したインデックス CALL_ID/FROM/TO を持つデータベースが使用されます。これらのインデックスにより、コール、送信元、宛先が識別されます。このデータベースには、SDP のメディア情報フィールド内で見つかったメディア アドレスとメディア ポート、およびメディア タイプが格納されます。1 つのセッションに対して、複数のメディア アドレスとポートが存在することが可能です。セキュリティ アプライアンスは、これらのメディア アドレス/ポートを使用して、2 つのエンドポイント間に RTP/RTCP 接続を開きます。

初期コール セットアップ（INVITE）メッセージでは、予約済みポート 5060 を使用する必要があります。ただし、後続のメッセージにはこのポート番号がない場合もあります。SIP インスペクション エンジンはシグナリング接続のピンホールを開き、それらの接続を SIP 接続としてマークします。これは、SIP アプリケーションに到達した変換対象のメッセージに対して行われます。

コールのセットアップ時に、SIP セッションは、着信側エンドポイントから応答メッセージでメディア アドレスとメディア ポートを受信し、着信側エンドポイントがどの RTP ポートで受信するかを知らされるまで「一時的な」状態にあります。1 分以内に、応答メッセージの受信に障害があった場合は、シグナリング接続は切断されます。

最終的なハンドシェイクが行われると、コール状態はアクティブに移行し、シグナリング接続は、BYE メッセージの受信まで継続されます。

内部エンドポイントが、外部エンドポイントに発呼した場合、メディア ホールが、外部インターフェイスに対して開き、内部エンドポイントから送信された INVITE メッセージで指定された内部エンドポイントのメディア アドレスとメディア ポートに、RTP/RTCP UDP パケットが流れることが許可されます。内部インターフェイスに対する要求外の RTP/RTCP UDP パケットは、セキュリティ アプライアンス のコンフィギュレーションで特別に許可されない限り、セキュリティ アプライアンス を通過できません。

Skinny（SCCP）インスペクション

この項では、SCCP アプリケーション インスペクションについて説明します。この項では、次のトピックについて取り上げます。

- 「SCCP インスペクションの概要」（P.24-23）
- 「Cisco IP Phone のサポート」（P.24-24）
- 「制限事項」（P.24-24）

SCCP インスペクションの概要

Skinny（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。Cisco CallManager と併用すると、SCCP クライアントは、H.323 準拠端末と同時使用できます。セキュリティ アプライアンスのアプリケーション層機能は、SCCP バージョン 3.3 を認識します。SCCP プロトコルには、2.4、3.0.4、3.1.1、3.2、3.3.2 の 5 つのバージョンがあります。セキュリティ アプライアンスでは、バージョン 3.3.2 までのすべてのバージョンをサポートしています。

セキュリティ アプライアンスは、SCCP に対して PAT と NAT をサポートします。IP 電話で使用できるグローバル IP アドレスよりも IP 電話が多い場合は、PAT が必要です。Skinny アプリケーション インスペクションは、SCCP シグナリング パケットの NAT と PAT をサポートすることで、すべての SCCP シグナリング パケットとメディア パケットが セキュリティ アプライアンス を通過できるようにします。

Cisco CallManager と Cisco IP Phones 間の通常のトラフィックは SCCP を使用しており、特別な設定をしなくても SCCP インスペクションによって処理されます。セキュリティ アプライアンスは、TFTP サーバの場所を Cisco IP Phone とその他の DHCP クライアントに送信することで、DHCP オプション 150 および 66 もサポートします。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone と比べてセキュリティの高いインターフェイスにあるトポロジでは、NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングは**スタティック**である必要があります。これは、Cisco IP Phone では Cisco CallManager の IP アドレスをコンフィギュレーションで明示的に指定する必要があるためです。スタティック アイデンティティ エントリを使用すると、セキュリティが高いインターフェイス上にある Cisco CallManager が Cisco IP Phone からの登録を受け付けるようにできます。

Cisco IP Phone では、TFTP サーバにアクセスして、Cisco CallManager サーバに接続するために必要な設定情報をダウンロードする必要があります。

TFTP サーバと比較して Cisco IP Phone の方がセキュリティの低いインターフェイス上にある場合は、アクセス リストを使用して UDP ポート 69 の保護された TFTP サーバに接続する必要があります。TFTP サーバに対してはスタティック エントリが必要ですが、識別スタティック エントリにする必要はありません。NAT を使用する場合、識別スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスとポートにマッピングされます。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager と比べてセキュリティの*高い*インターフェイス上にある場合、Cisco IP Phone が接続を開始できるようにするために、アクセス リストやスタティック エントリは必要ありません。

制限事項

SCCP に対する現在のバージョンの PAT および NAT サポートに適用される制限は、次のとおりです。

- PAT は、**alias** コマンドを含むコンフィギュレーションでは動作しません。
- 外部 NAT および PAT はサポート *されません*。

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスかポートを設定している場合、セキュリティ アプライアンスは現在のところ TFTP を経由して転送するファイルの内容に対して NAT または PAT をサポートしていないため、外部の Cisco IP Phone 用の登録は失敗します。セキュリティ アプライアンスは TFTP メッセージの NAT をサポートし、TFTP ファイル用にピンホールを開きますが、セキュリティ アプライアンス は電話の登録中に TFTP によって転送された Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれた Cisco CallManager の IP アドレスとポートを変換することはできません。

（注） セキュリティ アプライアンスは、コール セットアップ中のコールを除き、SCCP コールのステートフル フェールオーバーをサポートします。

SMTP および拡張 SMTP インスペクション

ESMTP アプリケーション インスペクションを使用すると、セキュリティ アプライアンスを通過できる SMTP コマンドの種類を制限し、モニタ機能を追加することによって、SMTP ベースの攻撃からより強固に保護できます。

ESMTP は SMTP プロトコルの拡張で、ほとんどの観点で SMTP に似ています。便宜上、このマニュアルでは、SMTP という用語を SMTP と ESMTP の両方に使用します。拡張 SMTP に対するアプリケーション インスペクション処理は、SMTP アプリケーション インスペクションに似ており、SMTP セッションのサポートが含まれています。拡張 SMTP セッションで使用するほとんどのコマンドは、SMTP セッションで使用するコマンドと同じですが、ESMTP セッションの方が大幅に高速で、配信ステータス通知など信頼性およびセキュリティに関するオプションが増えています。

拡張 SMTP アプリケーション インスペクションでは、AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、VRFY の 8 つの拡張 SMTP コマンドのサポートが追加されます。セキュリティ アプライアンスは、7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）をサポートするとともに、合計 15 の SMTP コマンドをサポートします。

他の拡張 SMTP コマンド（ATRN、STARTLS、ONEX、VERB、CHUNKING など）やプライベート拡張はサポートされていません。サポートされないコマンドは、内部サーバにより拒否される X に変換されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、廃棄されます。

ESMTP インスペクション エンジンは、「2」、「0」、「0」を除いて、サーバ SMTP バナー内の文字をアスタリスクに変更します。Carriage Return（CR; 復帰）、および Linefeed（LF; 改行）は無視されます。

SMTP インスペクションをイネーブルにする場合、次のルールに従わないと、対話型の SMTP に使用する Telnet セッションが停止することがあります。SMTP コマンドの長さは 4 文字以上にする必要があります。復帰と改行で終了する必要があります。次の応答を発行する前に現在の応答を待機する必要があります。

SMTP サーバは、数値の応答コード、およびオプションの可読文字列でクライアント要求に応答します。SMTP アプリケーション インスペクションは、ユーザが使用できるコマンドとサーバが返送するメッセージを制御し、その数を減らします。SMTP インスペクションは、次の 3 つの主要なタスクを実行します。

- SMTP 要求を 7 つの基本 SMTP コマンドと 8 つの拡張コマンドに制限します。
- SMTP コマンド応答シーケンスをモニタします。
- 監査証跡の生成：メール アドレス内に埋め込まれている無効な文字が置き換えられたときに、監査レコード 108002 を生成します。詳細については、RFC 821 を参照してください。

SMTP インスペクションでは、次の異常な署名がないかどうか、コマンドと応答のシーケンスをモニタします。

- 切り捨てられたコマンド
- 不正なコマンド終端（<CR><LR> で終了していない）
- MAIL コマンドと RCPT コマンドでは、メールの送信者と受信者が指定されます。異常な文字がないか、メール アドレスがスキャンされます。パイプ（|）が削除（空白スペースに変更）され、「<」および「>」については、メール アドレスの定義に使用される場合だけ許可されます（「<」の後には、必ず「>」が使用されている必要があります）。
- SMTP サーバによる不意の移行
- 未知のコマンドに対しては、セキュリティ アプライアンスはパケット内のすべての文字を X に変更します。この場合、サーバがクライアントに対してエラー コードを生成します。パケット内が変更されているため、TCP チェックサムは、再計算または調節する必要があります。
- TCP ストリーム編集

- コマンド パイプライン

SNMP Inspection

SNMP アプリケーション インスペクションでは、SNMP トラフィックを特定のバージョンの SNMP に制限できます。以前のバージョンの SNMP は安全性が低いため、セキュリティ ポリシーを使用して特定の SNMP バージョンを拒否する必要が生じる場合もあります。セキュリティ アプライアンスは、SNMP バージョン 1、2、2c、または 3 を拒否できます。許可するバージョンは、SNMP マップを作成して制御します。

SQL*Net インスペクション

SQL*Net インスペクションはデフォルトでイネーブルになっています。

SQL*Net プロトコルは、さまざまなパケット タイプで構成されています。セキュリティ アプライアンスはこれらのパケットを処理して、セキュリティ アプライアンス のどちらの側の Oracle アプリケーションにも一貫性のあるデータ ストリームが表示されるようにします。

SQL*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL*Net 用に使用している値ですが、Structured Query Language（SQL; 構造化照会言語）の IANA ポート割り当てとは一致しません。SQL*Net インスペクションを一連のポート番号に適用するには、**class-map** コマンドを使用します。

セキュリティ アプライアンスは、すべてのアドレスを変換し、パケットを調べて、SQL*Net バージョン 1 用に開くすべての埋め込みポートを見つけます。

SQL*Net バージョン 2 の場合、データ長ゼロの REDIRECT パケットの直後に続くすべての DATA パケットまたは REDIRECT パケットはフィックスアップされます。

フィックスアップが必要なパケットには、埋め込みホスト アドレスおよびポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net バージョン 2 の各 TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker）は、NAT 対象のアドレスがあるかどうかがスキャンされません。また、インスペクションがパケット内に埋め込まれたポートにダイナミック接続を開くこともありません。

SQL*Net バージョン 2 の TNSFrame、Redirect パケット、および Data パケットは、ペイロードのデータ長がゼロの REDIRECT TNSFrame タイプの後に続く場合、開くポートおよび NAT 対象のアドレスがあるかどうかスキャンされます。データ長ゼロの Redirect メッセージが セキュリティ アプライアンス を通過すると、後に続く Data メッセージまたは Redirect メッセージは変換対象であり、ポートはダイナミックに開かれると想定するフラグが、接続データ構造に設定されます。先行するパラグラフの TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL*Net インスペクション エンジンは、チェックサムを再計算し、IP および TCP の長さを変更し、新旧のメッセージの長さの差を使用してシーケンス番号と確認応答番号を再調整します。

SQL*Net バージョン 1 では、その他のすべての場合を想定しています。TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker、Redirect、Data）とすべてのパケットは、ポートおよびアドレスがあるかどうかスキャンされます。アドレスが変換され、ポート接続が開かれます。

Sun RPC インスペクション

この項では、Sun RPC アプリケーション インスペクションについて説明します。この項では、次のトピックについて取り上げます。

Sun RPC インスペクションの概要

Sun RPC インスペクション エンジンは、Sun RPC プロトコルのアプリケーション インスペクションをイネーブルまたはディセーブルにします。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはどのポート上でも実行できます。サーバ上の Sun RPC サービスにアクセスしようとするクライアントは、そのサービスが実行されているポートを知る必要があります。そのためには、予約済みポート 111 でポート マッパー プロセス（通常は rpcbind）に照会します。

クライアントがサービスの Sun RPC プログラム番号を送信すると、ポート マッパー プロセスはサービスのポート番号を応答します。クライアントは、ポート マッパー プロセスによって特定されたポートを指定して、Sun RPC クエリーをサーバに送信します。サーバが応答すると、セキュリティ アプライアンス はこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。

（注）　Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

SUNRPC Server

[Configuration] > [Firewall] > [Advanced] > [SUNRPC Server] ペインには、セキュリティ アプライアンスを通過できる SunRPC サービスと、その固有のタイムアウト値がサーバ単位で表示されます。

フィールド

- [Interface]：SunRPC サーバが常駐するインターフェイスを表示します。
- [IP address]：SunRPC サーバの IP アドレスを表示します。
- [Mask]：SunRPC サーバの IP アドレスのサブネット マスクを表示します。
- [Service ID]：セキュリティ アプライアンスを通過することを許可する、SunRPC プログラム番号、またはサービス ID を表示します。
- [Protocol]：SunRPC 転送プロトコル（TCP または UDP）を表示します。
- [Port]：SunRPC プロトコルのポート範囲を表示します。
- [Timeout]：SunRPC サービス トラフィックへのアクセスが閉じられるまでのアイドル時間を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SUNRPC Service

[Configuration] > [Firewall] > [Advanced] > [SUNRPC Server] > [Add/Edit SUNRPC Service] ダイアログボックスでは、セキュリティ アプライアンス を通過することを許可する SunRPC サービス、およびそれらの固有タイムアウトをサーバ単位で指定できます。

フィールド

- [Interface Name]：SunRPC サーバが常駐するインターフェイスを指定します。
- [Protocol]：SunRPC 転送プロトコル（TCP または UDP）を指定します。
- [IP address]：SunRPC サーバの IP アドレスを指定します。
- [Port]：SunRPC プロトコルのポート範囲を指定します。
- [Mask]：SunRPC サーバの IP アドレスのサブネット マスクを指定します。
- [Timeout]：SunRPC サービス トラフィックへのアクセスが閉じられるまでのアイドル時間を指定します。形式は、HH:MM:SS です。
- [Service ID]：セキュリティ アプライアンスを通過することを許可する、SunRPC プログラム番号、またはサービス ID を指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

TFTP インスペクション

TFTP インスペクションはデフォルトでイネーブルになっています。

TFTP は、RFC 1350 に記述されているように、TFTP サーバとクライアントの間のファイルの読み書きを行うための簡易プロトコルです。

セキュリティ アプライアンスは、TFTP トラフィックを検査し、必要に応じてダイナミックに接続と変換を作成し、TFTP クライアントとサーバの間のファイル転送を許可します。具体的には、インスペクション エンジンは TFTP Read Request（RRQ; 読み取り要求）、Write Request（WRQ; 書き込み要求）、およびエラー通知（ERROR）を検査します。

有効な読み取り要求（RRQ）または書き込み要求（WRQ）を受信すると、必要に応じて、ダイナミックなセカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、これ以降 TFTP によってファイル転送またはエラー通知用に使用されます。

TFTP サーバだけがセカンダリ チャネル経由のトラフィックを開始できます。また、TFTP クライアントとサーバの間に存在できる不完全なセカンダリ チャネルは 1 つまでです。サーバからのエラー通知があると、セカンダリ チャネルは閉じます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP インスペクションをイネーブルにする必要があります。

XDMCP インスペクション

XDMCP インスペクションはデフォルトでイネーブルになっていますが、XDMCP インスペクション エンジンは、**established** コマンドが適切に構成されていないと使用できません。

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは確立時に TCP を使用します。

XWindows セッションを正常にネゴシエートして開始するために、セキュリティ アプライアンスは、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。戻り接続を許可するには、セキュリティ アプライアンスで **established** コマンドを使用します。XDMCP がディスプレイを送信するポートをネゴシエートすると、**established** コマンドが参照され、この戻り接続を許可すべきかどうかが確認されます。

XWindows セッション中、マネージャは予約済みポート 6000 | n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。

```
setenv DISPLAY Xserver:n
```

n はディスプレイ番号です。

XDMCP が使用されている場合、ディスプレイは IP アドレスを使用してネゴシエートされます。IP アドレスは、セキュリティ アプライアンスが必要に応じて NAT を行うことができます。XDCMP インスペクションでは、PAT はサポートされません。

サービス ポリシーのフィールドの説明

この項では、各プロトコル インスペクション ダイアログボックスのフィールドについて説明します。次の項目を取り上げます。

- 「[Rule Actions] > [Protocol Inspection] タブ」（P.24-30）
- 「Select DCERPC Map」（P.24-32）
- 「Select DNS Map」（P.24-32）
- 「Select ESMTP Map」（P.24-33）
- 「Select FTP Map」（P.24-33）
- 「Select GTP Map」（P.24-34）
- 「Select H.323 Map」（P.24-35）
- 「Select HTTP Map」（P.24-35）
- 「Select IM Map」（P.24-36）
- 「Select IPSec-Pass-Thru Map」（P.24-36）

- 「Select MGCP Map」（P.24-37）
- 「Select NETBIOS Map」（P.24-37）
- 「Select RTSP Map」（P.24-38）
- 「Select SCCP (Skinny) Map」（P.24-38）
- 「Select SIP Map」（P.24-39）
- 「Select SNMP Map」（P.24-39）

[Rule Actions] > [Protocol Inspection] タブ

フィールド

- [CTIQBE] : CTIQBE プロトコルでのアプリケーション インスペクションをイネーブルにします。
- [DCERPC] : DCERPC プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select DCERPC Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [DNS] : DNS プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select DNS Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [ESMTP] : ESMTP プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select ESMTP Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [FTP] : FTP プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select FTP Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [GTP] : GTP プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select GTP Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。

（注）　GTP インスペクションには、特別なライセンスが必要です。

- [H323 H225] : H323 H225 プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select H323 H225 Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [H323 RAS] : H323 RAS プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select H323 RAS Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [HTTP] : HTTP プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select HTTP Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。

- [ICMP] : ICMP プロトコルでのアプリケーション インスペクションをイネーブルにします。
- [ICMP Error] : ICMP Error プロトコルでのアプリケーション インスペクションをイネーブルにします。
- [ILS] : ILS プロトコルでのアプリケーション インスペクションをイネーブルにします。
- [IM] : IM プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select IM Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [IPSec-Pass-Thru] : IPSec プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select IPSec Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [MGCP] : MGCP プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select MGCP Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [NETBIOS] : NetBIOS プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select NETBIOS Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [PPTP] : PPTP プロトコルでのアプリケーション インスペクションをイネーブルにします。
- [RSH] : RSH プロトコルでのアプリケーション インスペクションをイネーブルにします。
- [RTSP] : RTSP プロトコルでのアプリケーション インスペクションをイネーブルにします。
- [SCCP SKINNY] : Skinny プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select SCCP (Skinny) Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [SIP] : SIP プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select SIP Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [SNMP] : SNMP プロトコルでのアプリケーション インスペクションをイネーブルにします。
  - [Configure] : [Select SNMP Map] ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- [SQLNET] : SQLNET プロトコルでのアプリケーション インスペクションをイネーブルにします。
- [SUNRPC] : SunRPC プロトコルでのアプリケーション インスペクションをイネーブルにします。
- [TFTP] : TFTP プロトコルでのアプリケーション インスペクションをイネーブルにします。
- [XDMCP] : XDMCP プロトコルでのアプリケーション インスペクションをイネーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「インスペクション マップのフィールドの説明」（P.24-61）

『*Cisco Security Appliance Command Reference*』にあるプロトコルごとの **Inspect** コマンド ページ

Select DCERPC Map

[Select DCERPC Map] ダイアログボックスでは、DCERPC マップを選択または新しく作成できます。DCERPC マップにより、DCERPC アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select DCERPC Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default DCERPC inspection map]：デフォルトの DCERPC マップの使用を指定します。
- [Select a DCERPC map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select DNS Map

[Select DNS Map] ダイアログボックスでは、DNS マップを選択または新しく作成できます。DNS マップにより、DNS アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select DNS Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default DNS inspection map]：デフォルトの DNS マップの使用を指定します。
- [Select a DNS map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。

- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select ESMTP Map

[Select ESMTP Map] ダイアログボックスでは、ESMTP マップを選択または新しく作成できます。ESMTP マップにより、ESMTP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select ESMTP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default ESMTP inspection map]：デフォルトの ESMTP マップの使用を指定します。
- [Select an ESMTP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select FTP Map

[Select FTP Map] ダイアログボックスでは、厳密な FTP アプリケーション インスペクションのイネーブル化、FTP マップの選択、または新しい FTP マップの作成を行うことができます。FTP マップにより、FTP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select FTP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [FTP Strict (prevent web browsers from sending embedded commands in FTP requests)]：厳密な FTP アプリケーション インスペクションをイネーブルにします。これによって、埋め込みコマンドが FTP 要求に含まれている場合、セキュリティ アプライアンスは接続をドロップします。

- [Use the default FTP inspection map]：デフォルトの FTP マップの使用を指定します。
- [Select an FTP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select GTP Map

[Select GTP Map] ダイアログボックスでは、GTP マップを選択または新しく作成できます。GTP マップにより、GTP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select GTP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

（注） GTP インスペクションには、特別なライセンスが必要です。必要なライセンスがないときにセキュリティ アプライアンスで GTP アプリケーション インスペクションのイネーブル化を試みると、セキュリティ アプライアンスはエラー メッセージを表示します。

フィールド

- [Use the default GTP inspection map]：デフォルトの GTP マップの使用を指定します。
- [Select an GTP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select H.323 Map

[Select H.323 Map] ダイアログボックスでは、H.323 マップを選択または新しく作成できます。H.323 マップにより、H.323 アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select H.323 Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default H.323 inspection map]：デフォルトの H.323 マップの使用を指定します。
- [Select an H.323 map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select HTTP Map

[Select HTTP Map] ダイアログボックスでは、HTTP マップを選択または新しく作成できます。HTTP マップにより、HTTP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select HTTP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default HTTP inspection map]：デフォルトの HTTP マップの使用を指定します。
- [Select an HTTP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select IM Map

[Select IM Map] ダイアログボックスでは、IM マップを選択または新しく作成できます。IM マップにより、IM アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select IM Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Add] : そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select IPSec-Pass-Thru Map

[Select IPSec-Pass-Thru] ダイアログボックスでは、IPSec マップを選択または新しく作成できます。IPSec マップにより、IPSec アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select IPSec Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default IPSec inspection map] : デフォルトの IPSec マップの使用を指定します。
- [Select an IPSec map for fine control over inspection] : 定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add] : そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select MGCP Map

[Select MGCP Map] ダイアログボックスでは、MGCP マップを選択または新しく作成できます。MGCP マップにより、MGCP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select MGCP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default MGCP inspection map] : デフォルトの MGCP マップの使用を指定します。
- [Select an MGCP map for fine control over inspection] : 定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add] : そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select NETBIOS Map

[Select NETBIOS Map] ダイアログボックスでは、NetBIOS マップを選択または新しく作成できます。NetBIOS マップにより、NetBIOS アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select NetBIOS Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default IM inspection map] : デフォルトの NetBIOS マップの使用を指定します。
- [Select a NetBIOS map for fine control over inspection] : 定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add] : そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select RTSP Map

[Select RTSP Map] ダイアログボックスでは、RTSP マップを選択または新しく作成できます。RTSP マップにより、RTSP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select RTSP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default RTSP inspection map]：デフォルトの RTSP インスペクション マップの使用を指定します。
- [Select a RTSP inspect map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select SCCP (Skinny) Map

[Select SCCP (Skinny) Map] ダイアログボックスでは、SCCP (Skinny) マップを選択または新しく作成できます。[SCCP (Skinny)] マップにより、SCCP (Skinny) アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select SCCP (Skinny) Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default SCCP (Skinny) inspection map]：デフォルトの SCCP (Skinny) マップの使用を指定します。
- [Select an SCCP (Skinny) map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。
- [TLS Proxy]：インスペクション マップの TLS プロキシ設定を指定できます。
  - [Use TLS Proxy to enable inspection of encrypted traffic]：TLS プロキシを使用して、暗号化されたトラフィックのインスペクションをイネーブルにすることを指定します。

    [TLS Proxy Name]：既存の TLS プロキシの名前。

    [New]：TLS プロキシを追加するための [Add TLS Proxy] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select SIP Map

[Select SIP Map] ダイアログボックスでは、SIP マップを選択または新しく作成できます。SIP マップにより、SIP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select SIP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default SIP inspection map]：デフォルトの SIP マップの使用を指定します。
- [Select a SIP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。
- [TLS Proxy]：インスペクション マップの TLS プロキシ設定を指定できます。
  - [Use TLS Proxy to enable inspection of encrypted traffic]：TLS プロキシを使用して、暗号化されたトラフィックのインスペクションをイネーブルにすることを指定します。

    [TLS Proxy Name]：既存の TLS プロキシの名前。

    [New]：TLS プロキシを追加するための [Add TLS Proxy] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Select SNMP Map

[Select SNMP Map] ダイアログボックスでは、SNMP マップを選択または新しく作成できます。SNMP マップにより、SNMP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select SNMP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default SNMP inspection map]：デフォルトの SNMP マップの使用を指定します。

- [Select an SNMP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

クラス マップのフィールドの説明

インスペクション クラス マップで、アプリケーションのトラフィックを、URL 文字列などアプリケーション固有の基準と照合します。次に、クラス マップをインスペクション マップから特定して、アクションをイネーブルにします。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。インスペクション クラス マップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

この項では、インスペクション クラス マップを設定する方法について説明します。次の項目を取り上げます。

- 「DNS Class Map」（P.24-40）
- 「FTP Class Map」（P.24-44）
- 「H.323 Class Map」（P.24-47）
- 「HTTP Class Map」（P.24-50）
- 「IM Class Map」（P.24-55）
- 「SIP Class Map」（P.24-58）

DNS Class Map

[DNS Class Map] パネルでは、DNS インスペクションの DNS クラス マップを設定できます。

インスペクション クラス マップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラス マップをインスペクション マップから特定して、アクションをイネーブルにします。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。インスペクション クラス マップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- [Name]：DNS クラス マップの名前を示します。
- [Match Conditions]：クラス マップに設定されているタイプ、照合基準、値を示します。

  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：DNS クラス マップの基準を示します。
  - [Value]：DNS クラス マップで照合する値を示します。
- [Description]：クラス マップの説明を示します。
- [Add]：DNS クラス マップの照合条件を追加します。
- [Edit]：DNS クラス マップの照合条件を編集します。
- [Delete]：DNS クラス マップの照合条件を削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DNS Traffic Class Map

[Add/Edit DNS Traffic Class Map] ダイアログボックスでは、DNS クラス マップを定義できます。

フィールド

- [Name]：DNS クラス マップの名前を 40 文字以内で入力します。
- [Description]：DNS クラス マップの説明を入力します。
- [Add]：DNS クラス マップを追加します。
- [Edit]：DNS クラス マップを編集します。
- [Delete]：DNS クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DNS Match Criterion

[Add/Edit DNS Match Criterion] ダイアログボックスでは、DNS クラス マップの照合基準と値を定義できます。

フィールド

- [Match Type]：基準に一致したトラフィックをクラス マップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

- [Criterion]：DNS トラフィックに適用する照合基準を指定します。
  - [Header Flag]：ヘッダーの DNS フラグを照合します。
  - [Type]：DNS クエリーまたはリソース レコードのタイプを照合します。
  - [Class]：DNS クエリーまたはリソース レコードのクラスを照合します。
  - [Question]：DNS の問い合わせを照合します。
  - [Resource Record]：DNS リソース レコードを照合します。
  - [Domain Name]：DNS クエリーやリソース レコードのドメイン名を照合します。
- [Header Flag Criterion Values]：DNS ヘッダー フラグの照合値の詳細を指定します。
  - [Match Option]：完全一致または全ビット一致（ビット マスク一致）のどちらかを指定します。
  - [Match Value]：ヘッダー フラグについて名前と値のどちらを照合するか指定します。

    [Header Flag Name]：照合するヘッダー フラグ名を 1 つ以上選択できます。AA（authoritative answer）、QR（query）、RA（recursion available）、RD（recursion denied）、TC（truncation）のフラグ ビットがあります。

    [Header Flag Value]：任意の 16 ビットの値を 16 進数で入力して照合できます。
- [Type Criterion Values]：DNS タイプの照合値の詳細を指定します。
  - [DNS Type Field Name]：選択する DNS タイプを一覧表示します。

    [A]：IPv4 アドレス

    [NS]：権限ネーム サーバ

    [CNAME]：正規名

    [SOA]：信頼ゾーンの開始

    [TSIG]：トランザクション シグニチャ

    [IXFR]：増分（ゾーン）転送

    [AXFR]：フル（ゾーン）転送
  - [DNS Type Field Value]：DNS タイプ フィールドについて値と範囲のどちらを照合するか指定します。

    [Value]：0 ～ 65535 の範囲の値を入力して照合できます。

    [Range]：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。
- [Class Criterion Values]：DNS クラスの照合値の詳細を指定します。
  - [DNS Class Field Name]：インターネットで照合する DNS クラス フィールド名を指定します。
  - [DNS Class Field Value]：DNS クラス フィールドについて値と範囲のどちらを照合するか指定します。

    [Value]：0 ～ 65535 の範囲の値を入力して照合できます。

    [Range]：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。
- [Question Criterion Values]：DNS の問い合わせセクションの照合方法を指定します。

- [Resource Record Criterion Values]：DNS リソース レコードのセクションの照合方法を指定します。
  - [Resource Record]：照合対象セクションを一覧表示します。

    [Additional]：DNS 追加リソース レコード

    [Answer]：DNS 応答リソース レコード

    [Authority]：DNS 認証リソース レコード
- [Domain Name Criterion Values]：DNS ドメイン名の照合方法を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Manage Regular Expressions

[Manage Regular Expressions] ダイアログボックスでは、正規表現を設定し、パターン照合で使用できます。「_default」で始まる正規表現はデフォルトの正規表現です。変更または削除はできません。

フィールド

- [Name]：正規表現の名前を示します。
- [Value]：正規表現の定義値を示します。
- [Add]：正規表現を追加します。
- [Edit]：正規表現を編集します。
- [Delete]：正規表現を削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Manage Regular Expression Class Maps

[Manage Regular Expression Class Maps] ダイアログボックスでは、正規表現クラス マップを設定できます。詳細については、「正規表現」を参照してください。

フィールド

- [Name]：正規表現クラス マップの名前を示します。
- [Match Conditions]：クラス マップの照合タイプと正規表現を示します。
  - [Match Type]：照合タイプを示します。正規表現の場合、常に基準の肯定一致タイプ（等号（=）を表示したアイコン）になります。また、インスペクション クラス マップで否定一致（赤丸を表示したアイコン）の作成もできます。クラス マップに正規表現が複数ある場合は、照合タイプ アイコンの隣にそれぞれ「OR」を表示し、「match any」クラス マップになっていることを示します。正規表現のいずれか 1 つと一致するだけで、トラフィックがクラス マップに一致します。
  - [Regular Expression]：クラス マップごとに登録されている正規表現を一覧表示します。
- [Description]：クラス マップの説明を示します。
- [Add]：正規表現クラス マップを追加します。
- [Edit]：正規表現クラス マップを編集します。
- [Delete]：正規表現クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

FTP Class Map

[FTP Class Map] パネルでは、FTP インスペクションの FTP クラス マップを設定できます。

インスペクション クラス マップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラス マップをインスペクション マップから特定して、アクションをイネーブルにします。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。インスペクション クラス マップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- [Name] : FTP クラス マップの名前を示します。
- [Match Conditions] : クラス マップに設定されているタイプ、照合基準、値を示します。
  - [Match Type] : 一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion] : FTP クラス マップの基準を示します。
  - [Value] : FTP クラス マップで照合する値を示します。
- [Description] : クラス マップの説明を示します。
- [Add] : FTP クラス マップを追加します。
- [Edit] : FTP クラス マップを編集します。
- [Delete] : FTP クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit FTP Traffic Class Map

[Add/Edit FTP Traffic Class Map] ダイアログボックスでは、FTP クラス マップを定義できます。

フィールド

- [Name] : FTP クラス マップの名前を 40 文字以内で入力します。
- [Description] : FTP クラス マップの説明を入力します。
- [Add] : FTP クラス マップを追加します。
- [Edit] : FTP クラス マップを編集します。
- [Delete] : FTP クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit FTP Match Criterion

[Add/Edit FTP Match Criterion] ダイアログボックスでは、FTP クラス マップの照合基準と値を定義できます。

フィールド

- [Match Type]：基準に一致したトラフィックをクラス マップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

- [Criterion]：FTP トラフィックに適用する照合基準を指定します。
  - [Request-Command]：FTP 要求コマンドを照合します。
  - [File Name]：FTP 転送のファイル名を照合します。
  - [File Type]：FTP 転送のファイル タイプを照合します。
  - [Server]：FTP サーバを照合します。
  - [User Name]：FTP ユーザを照合します。
- [Request-Command Criterion Values]：FTP 要求コマンドの照合値の詳細を指定します。
  - [Request Command]：照合する要求コマンドを 1 つ以上選択できます。

    [APPE]：ファイルに追加します。

    [CDUP]：現在のディレクトリから親ディレクトリへ移動します。

    [DELE]：サーバ サイトのファイルを削除します。

    [GET]：retr（retrieve a file）コマンドの FTP クライアント コマンドです。

    [HELP]：サーバのヘルプ情報です。

    [MKD]：ディレクトリを作成します。

    [PUT]：stor（store a file）コマンドの FTP クライアント コマンドです。

    [RMD]：ディレクトリを削除します。

    [RNFR]：変更元ファイル名

    [RNTO]：変更先ファイル名

    [SITE]：サーバ固有のコマンドを指定します。

    [STOU]：ファイルに一意の名前をつけて保存します。
- [File Name Criterion Values]：FTP 転送のファイル名の照合方法を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。

  - [Manage] : [Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class] : 照合する定義された正規表現クラスを一覧表示します。
  - [Manage] : [Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [File Type Criterion Values] : FTP 転送のファイル タイプの照合方法を指定します。
  - [Regular Expression] : 照合する定義された正規表現を一覧表示します。
  - [Manage] : [Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class] : 照合する定義された正規表現クラスを一覧表示します。
  - [Manage] : [Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Server Criterion Values] : FTP サーバの照合方法を指定します。
  - [Regular Expression] : 照合する定義された正規表現を一覧表示します。
  - [Manage] : [Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class] : 照合する定義された正規表現クラスを一覧表示します。
  - [Manage] : [Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [User Name Criterion Values] : FTP ユーザの照合方法を指定します。
  - [Regular Expression] : 照合する定義された正規表現を一覧表示します。
  - [Manage] : [Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class] : 照合する定義された正規表現クラスを一覧表示します。
  - [Manage] : [Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

H.323 Class Map

[H.323 Class Map] パネルでは、H.323 インスペクションの H.323 クラス マップを設定できます。

インスペクション クラス マップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラス マップをインスペクション マップから特定して、アクションをイネーブルにします。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定

義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。インスペクション クラス マップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- [Name] : H.323 クラス マップの名前を示します。
- [Match Conditions] : クラス マップに設定されているタイプ、照合基準、値を示します。
  - [Match Type] : 一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion] : H.323 クラス マップの基準を示します。
  - [Value] : H.323 クラス マップで照合する値を示します。
- [Description] : クラス マップの説明を示します。
- [Add] : H.323 クラス マップを追加します。
- [Edit] : H.323 クラス マップを編集します。
- [Delete] : H.323 クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit H.323 Traffic Class Map

[Add/Edit H.323 Traffic Class Map] ダイアログボックスでは、H.323 クラス マップを定義できます。

フィールド

- [Name] : H.323 クラス マップの名前を 40 文字以内で入力します。
- [Description] : H.323 クラス マップの説明を入力します。
- [Add] : H.323 クラス マップを追加します。
- [Edit] : H.323 クラス マップを編集します。
- [Delete] : H.323 クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit H.323 Match Criterion

[Add/Edit H.323 Match Criterion] ダイアログボックスでは、H.323 クラス マップの照合基準と値を定義できます。

フィールド

- [Match Type]：基準に一致したトラフィックをクラス マップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

- [Criterion]：H.323 トラフィックに適用する照合基準を指定します。
  - [Called Party]：受信側を照合します。
  - [Calling Party]：発信元を照合します。
  - [Media Type]：メディア タイプを照合します。
- [Called Party Criterion Values]：H.323 受信側の照合方法を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Calling Party Criterion Values]：H.323 発信元の照合方法を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Media Type Criterion Values]：照合するメディア タイプを指定します。
  - [Audio]：音声タイプを照合します。
  - [Video]：ビデオ タイプを照合します。
  - [Data]：データ タイプを照合します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

HTTP Class Map

[HTTP Class Map] パネルでは、HTTP インスペクションの HTTP クラス マップを設定できます。

インスペクション クラス マップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラス マップをインスペクション マップから特定して、アクションをイネーブルにします。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。インスペクション クラス マップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- [Name] : HTTP クラス マップの名前を示します。
- [Match Conditions] : クラス マップに設定されているタイプ、照合基準、値を示します。
  - [Match Type] : 一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion] : HTTP クラス マップの基準を示します。
  - [Value] : HTTP クラス マップで照合する値を示します。
- [Description] : クラス マップの説明を示します。
- [Add] : HTTP クラス マップを追加します。
- [Edit] : HTTP クラス マップを編集します。
- [Delete] : HTTP クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Traffic Class Map

[Add/Edit HTTP Traffic Class Map] ダイアログボックスでは、HTTP クラス マップを定義できます。

フィールド

- [Name] : HTTP クラス マップの名前を 40 文字以内で入力します。

- [Description] : HTTP クラス マップの説明を入力します。
- [Add] : HTTP クラス マップを追加します。
- [Edit] : HTTP クラス マップを編集します。
- [Delete] : HTTP クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Match Criterion

[Add/Edit HTTP Match Criterion] ダイアログボックスでは、HTTP クラス マップの照合基準と値を定義できます。

フィールド

- [Match Type] : 基準に一致したトラフィックをクラス マップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

- [Criterion] : HTTP トラフィックに適用する照合基準を指定します。
  - [Request/Response Content Type Mismatch] : 応答のコンテンツ タイプが要求の accept フィールドの MIME タイプの 1 つと一致する必要があることを指定します。
  - [Request Arguments] : 要求の引数に正規表現照合を適用します。

    [Regular Expression] : 照合する定義された正規表現を一覧表示します。

    [Manage] : [Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

    [Regular Expression Class] : 照合する定義された正規表現クラスを一覧表示します。

    [Manage] : [Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
  - [Request Body Length] : 要求の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

    [Greater Than Length] : 要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。
  - [Request Body] : 要求の本文に正規表現照合を適用します。

    [Regular Expression] : 照合する定義された正規表現を一覧表示します。

    [Manage] : [Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

[Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

[Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。

- [Request Header Field Count]：要求ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

  [Predefined]：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Greater Than Count]：ヘッダー フィールド数の最大値を入力します。

- [Request Header Field Length]：要求ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  [Predefined]：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Greater Than Length]：要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- [Request Header Field]：要求のヘッダーに正規表現照合を適用します。

  [Predefined]：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

  [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。

- [Request Header Count]：要求ヘッダー数が最大値の場合、正規表現で照合します。

[Greater Than Count]：ヘッダー数の最大値を入力します。

- [Request Header Length]：要求ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

  [Greater Than Length]：ヘッダーの長さをバイト単位で入力します。

- [Request Header non-ASCII]：要求ヘッダーに含まれる ASCII 以外の文字を照合します。
- [Request Method]：要求の方式を正規表現で照合します。

  [Method]：照合する要求方式を次の中から指定します。bcopy、bdelete、bmove、bpropfind、bproppatch、connect、copy、delete、edit、get、getattribute、getattributenames、getproperties、head、index、lock、mkcol、mkdir、move、notify、options、poll、post、propfind、proppatch、put、revadd、revlabel、revlog、revnum、save、search、setattribute、startrev、stoprev、subscribe、trace、unedit、unlock、unsubscribe。

  [Regular Expression]：正規表現の照合方法を指定します。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

  [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。

- [Request URI Length]：要求の URI が指定したバイト数より長い場合、正規表現で照合します。

  [Greater Than Length]：URI の長さをバイト単位で入力します。

- [Request URI]：要求の URI に正規表現照合を適用します。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

  [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。

- [Response Body]：要求の本文を regex で照合します。

  [ActiveX]：ActiveX の照合方法を指定します。

  [Java Applet]：Java アプレットの照合方法を指定します。

  [Regular Expression]：正規表現の照合方法を指定します。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

  [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。

- [Response Body Length]：応答の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  [Greater Than Length]：応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- [Response Header Field Count]：応答ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

  [Predefined]：応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Greater Than Count]：ヘッダー フィールド数の最大値を入力します。

- [Response Header Field Length]：応答ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  [Predefined]：応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Greater Than Length]：応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- [Response Header Field]：応答のヘッダーに正規表現照合を適用します。

  [Predefined]：応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

  [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。

- [Response Header Count]：応答ヘッダー数が最大値の場合、正規表現で照合します。

  [Greater Than Count]：ヘッダー数の最大値を入力します。

- [Response Header Length]：応答ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

  [Greater Than Length]：ヘッダーの長さをバイト単位で入力します。

- [Response Header non-ASCII]：応答ヘッダーに含まれる ASCII 以外の文字を照合します。

- [Response Status Line]：ステータス行を正規表現で照合します。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

[Manage] : [Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

[Regular Expression Class] : 照合する定義された正規表現クラスを一覧表示します。

[Manage] : [Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

IM Class Map

[IM Class Map] パネルでは、IM インスペクションの IM クラス マップを設定できます。

インスペクション クラス マップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラス マップをインスペクション マップから特定して、アクションをイネーブルにします。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。インスペクション クラス マップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- [Name] : IM クラス マップの名前を示します。
- [Match Conditions] : クラス マップに設定されているタイプ、照合基準、値を示します。
  - [Match Type] : 一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion] : IM クラス マップの基準を示します。
  - [Value] : IM クラス マップで照合する値を示します。
- [Description] : クラス マップの説明を示します。
- [Add] : IM クラス マップを追加します。
- [Edit] : IM クラス マップを編集します。
- [Delete] : IM クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IM Traffic Class Map

[Add/Edit IM Traffic Class Map] ダイアログボックスでは、IM クラス マップを定義できます。

フィールド

- [Name] : IM クラス マップの名前を 40 文字以内で入力します。
- [Description] : IM クラス マップの説明を入力します。
- [Add] : IM クラス マップを追加します。
- [Edit] : IM クラス マップを編集します。
- [Delete] : IM クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IM Match Criterion

[Add/Edit IM Match Criterion] ダイアログボックスでは、IM クラス マップの照合基準と値を定義できます。

フィールド

- [Match Type] : 基準に一致したトラフィックをクラス マップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion] : IM トラフィックに適用する照合基準を指定します。
  - [Protocol] : IM プロトコルを照合します。
  - [Service] : IM サービスを照合します。
  - [Version] : IM ファイル転送のサービス バージョンを照合します。
  - [Client Login Name] : IM サービスのクライアント ログイン名を照合します。

  - [Client Peer Login Name]：IM サービスのクライアントのピア ログイン名を照合します。
  - [Source IP Address]：送信元 IP アドレスを照合します。
  - [Destination IP Address]：宛先 IP アドレスを照合します。
  - [Filename]：IM ファイル転送サービスのファイル名を照合します。
- [Protocol Criterion Values]：照合する IM プロトコルを指定します。
  - [Yahoo! Messenger]：Yahoo!Messenger のインスタント メッセージを照合します。
  - [MSN Messenger]：MSN Messenger のインスタント メッセージを照合します。
- [Service Criterion Values]：照合する IM サービスを指定します。
  - [Chat]：IM メッセージ チャット サービスを照合します。
  - [Conference]：IM コンファレンス サービスを照合します。
  - [File Transfer]：IM ファイル転送サービスを照合します。
  - [Games]：IM ゲーム サービスを照合します。
  - [Voice Chat]：IM 音声チャット サービスを照合します（Yahoo の IM は対象外です）。
  - [Web Cam]：IM Web カメラ サービスを照合します。
- [Version Criterion Values]：IM ファイル転送サービスで照合するバージョンを指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Client Login Name Criterion Values]：IM サービスで照合するクライアント ログイン名を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Client Peer Login Name Criterion Values]：IM サービスで照合するクライアントのピア ログイン名を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Source IP Address Criterion Values]：IM サービスで照合する送信元 IP アドレスを指定します。
  - [IP Address]：IM サービスの送信元 IP アドレスを入力します。

  - [IP Mask]：送信元 IP アドレスのマスクです。
- [Destination IP Address Criterion Values]：IM サービスで照合する宛先 IP アドレスを指定します。
  - [IP Address]：IM サービスの宛先 IP アドレスを入力します。
  - [IP Mask]：宛先 IP アドレスのマスクです。
- [Filename Criterion Values]：IM ファイル転送サービスで照合するファイル名を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SIP Class Map

[SIP Class Map] パネルでは、SIP インスペクションの SIP クラス マップを設定できます。

インスペクション クラス マップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラス マップをインスペクション マップから特定して、アクションをイネーブルにします。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。インスペクション クラス マップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- [Name]：SIP クラス マップの名前を示します。
- [Match Conditions]：クラス マップに設定されているタイプ、照合基準、値を示します。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：SIP クラス マップの基準を示します。
  - [Value]：SIP クラス マップで照合する値を示します。
- [Description]：クラス マップの説明を示します。
- [Add]：SIP クラス マップを追加します。
- [Edit]：SIP クラス マップを編集します。
- [Delete]：SIP クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SIP Traffic Class Map

[Add/Edit SIP Traffic Class Map] ダイアログボックスでは、SIP クラス マップを定義できます。

フィールド

- [Name] : SIP クラス マップの名前を 40 文字以内で入力します。
- [Description] : SIP クラス マップの説明を入力します。
- [Add] : SIP クラス マップを追加します。
- [Edit] : SIP クラス マップを編集します。
- [Delete] : SIP クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SIP Match Criterion

[Add/Edit SIP Match Criterion] ダイアログボックスでは、SIP クラス マップの照合基準と値を定義できます。

フィールド

- [Match Type]：基準に一致したトラフィックをクラス マップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

- [Criterion]：SIP トラフィックに適用する照合基準を指定します。
  - [Called Party]：To ヘッダーに指定された受信側を照合します。
  - [Calling Party]：From ヘッダーに指定された発信元を照合します。

  - [Content Length]：ヘッダーのコンテンツの長さを照合します。0 ～ 65536 の範囲の値です。
  - [Content Type]：ヘッダーのコンテンツ タイプを照合します。
  - [IM Subscriber]：SIP IM の加入者を照合します。
  - [Message Path]：SIP の Via ヘッダーを照合します。
  - [Request Method]：SIP の要求方式を照合します。
  - [Third-Party Registration]：サード パーティの登録要求者を照合します。
  - [URI Length]：SIP ヘッダーにある URI を照合します。0 ～ 65536 の範囲の値です。
- [Called Party Criterion Values]：照合する受信側を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Calling Party Criterion Values]：照合する発信元を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Content Length Criterion Values]：指定値より長い SIP コンテンツ ヘッダーを照合します。
  - [Greater Than Length]：ヘッダーの長さをバイト単位で入力します。
- [Content Type Criterion Values]：照合する SIP コンテンツ ヘッダーのタイプを指定します。
  - [SDP]：SDP タイプの SIP コンテンツ ヘッダーを照合します。
  - [Regular Expression]：正規表現を照合します。

    [Regular Expression]：照合する定義された正規表現を一覧表示します。

    [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

    [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

    [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [IM Subscriber Criterion Values]：照合する IM 登録者を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。

- [Message Path Criterion Values]：照合する SIP の Via ヘッダーを指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Request Method Criterion Values]：照合する SIP 要求方式を指定します。
  - [Request Method]：次の中から要求方式を指定します。ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。
- [Third-Party Registration Criterion Values]：照合するサード パーティの登録要求者を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [URI Length Criterion Values]：SIP ヘッダーで指定した値より長い、選択したタイプの URI を照合します。
  - [URI type]：SIP URI または TEL URI を指定して照合します。
  - [Greater Than Length]：長さをバイト単位で指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

インスペクション マップのフィールドの説明

この項では、インスペクション マップを設定する方法について説明します。次の項目を取り上げます。

（注）　RADIUS インスペクション マップの詳細については、「管理トラフィックのサービス ポリシー ルールの追加」（P.23-8）を参照してください。

- 「ESMTP Inspect Map」（P.24-74）
- 「FTP Inspect Map」（P.24-82）
- 「GTP Inspect Map」（P.24-87）
- 「H.323 Inspect Map」（P.24-92）
- 「HTTP Inspect Map」（P.24-99）
- 「Instant Messaging (IM) Inspect Map」（P.24-107）
- 「IPSec Pass Through Inspect Map」（P.24-110）
- 「MGCP Inspect Map」（P.24-113）
- 「NetBIOS Inspect Map」（P.24-116）
- 「RTSP Inspect Map」（P.24-117）
- 「SCCP (Skinny) Inspect Map」（P.24-119）
- 「SIP Inspect Map」（P.24-125）
- 「SNMP Inspect Map」（P.24-131）

セキュリティ アプライアンスのステートフル アプリケーション インスペクションにアルゴリズムを適用して、アプリケーションのセキュリティとサービスを保証します。アプリケーションの中には特別な処理を必要とするものがあり、専用のインスペクション エンジンでそのような場合に対応します。専用のインスペクション エンジンが必要なアプリケーションとは、ユーザのデータ パケットの中に IP アドレッシング情報を埋め込むサービスや、動的に割り当てられたポートでセカンダリ チャネルを開くサービスなどです。

アプリケーション インスペクション エンジンは NAT と連携し、アドレッシング情報が埋め込まれている場所の識別をサポートします。これによって、このような埋め込みアドレスを NAT で変換したり、変換の影響を受けるチェックサムやその他のフィールドをアップデートしたりできます。

各アプリケーション インスペクション エンジンはセッションを監視して、セカンダリ チャネルのポート番号も確認します。多くのプロトコルは、パフォーマンスを向上させるために、TCP または UDP のセカンダリ ポートを開きます。既知のポートで初期セッションが使用され、動的に割り当てられたポート番号がネゴシエーションされます。アプリケーション インスペクション エンジンは、この初期セッションをモニタし、ダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポート上でのデータ交換を許可します。

また、ステートフル アプリケーション インスペクションにより、検査中のプロトコルの過程で発行されたコマンドと応答の有効性を監査します。セキュリティ アプライアンスは攻撃を確実に防御するため、トラフィックが検査されるプロトコルごとに RFC 仕様に準拠しているかどうかチェックします。

インスペクション マップ機能で、専用のプロトコル インスペクション エンジンを作成できます。インスペクション マップを利用して、プロトコル インスペクション エンジンのコンフィギュレーションを保存します。それから、グローバル セキュリティ ポリシーや特定のインターフェイスのセキュリティ ポリシーを使用して特定のトラフィック タイプにマップを関連付け、インスペクション マップのコンフィギュレーション設定をイネーブルにします。

[Security Policy] ペインの [Service Policy Rules] タブからインスペクション マップをトラフィックに適用すると、サービス ポリシーで指定した基準に従って照合が行われます。サービス ポリシーは、セキュリティ アプライアンスの特定のインターフェイスまたはすべてのインターフェイスに適用することができます。

DCERPC	DCERPC インスペクションで、DCERPC インスペクション マップを作成、表示、管理します。DCERPC マップでクライアントとエンドポイント マッパーの間で送受される DCERPC メッセージを検査し、必要に応じてセカンダリ接続に NAT を適用します。DCERPC はリモート プロシージャ コール メカニズムの仕様です。
DNS	DNS インスペクションで、DNS インスペクション マップを作成、表示、管理します。このマップを使用して DNS メッセージをより詳細に制御し、DNS スプーフィングとキャッシュ ポイズニングを保護できます。DNS は、IP アドレスやメール サーバなどのドメイン名の情報を解決します。
ESMTP	ESMTP インスペクションで、ESMTP インスペクション マップを作成、表示、管理します。ESMTP マップを使用してアプリケーションのセキュリティおよびプロトコル準拠性を検査し、攻撃の防御、送信者や受信者のブロック、メール中継のブロックができます。ESMTP（Extended SMTP）は SMTP 規格のプロトコル拡張を定義します。
FTP	FTP インスペクションで、FTP インスペクション マップを作成、表示、管理します。FTP は、インターネットなど、TCP/IP ネットワークを介してファイルを転送する通信プロトコルです。FTP マップを使用して、FTP PUT などの特定の FTP プロトコル方式がセキュリティ アプライアンスを通過して FTP サーバに到達するのをブロックできます。
GTP	GTP インスペクションで、GTP インスペクション マップを作成、表示、管理します。GTP は比較的新しいプロトコルで、インターネットなど TCP/IP ネットワークと無線接続する場合のセキュリティを提供します。GTP マップを使用して、タイムアウト値、メッセージ サイズ、トンネル数、およびセキュリティ アプライアンスを通過する GTP バージョンを制御できます。
H.323	H.323 インスペクションで、H.323 インスペクション マップを作成、表示、管理します。H.323 マップを使用して、RAS、H.225、H.245 の VoIP プロトコルを検査し、ステートのトラッキングとフィルタリングができます。
HTTP	HTTP インスペクションで、HTTP インスペクション マップを作成、表示、管理します。HTTP はワールドワイド ウェブのクライアントとサーバ間の通信で使用されるプロトコルです。HTTP マップを使用して、RFC 準拠の HTTP ペイロード コンテンツ タイプを設定できます。また、特定の HTTP 方式をブロックし、一部のトンネル アプリケーションによる HTTP 転送を防止できます。
IM	IM インスペクションで、IM インスペクション マップを作成、表示、管理します。IM マップを使用してネットワークの使用を制御し、IM アプリケーションによる機密情報の漏洩や他のネットワークの脅威を防止できます。
IPSec Pass Through	IPSec パススルー インスペクションで、IPSec パススルーのインスペクション マップを作成、表示、管理します。IPSec パススルー マップを使用すると、アクセス リストを参照しなくても、特定のフローを許可できます。
MGCP	MGCP インスペクションで、MGCP インスペクション マップを作成、表示、管理します。MGCP マップを使用して、VoIP デバイスと MGCP コール エージェント間の接続を管理できます。

NetBIOS	NetBIOS インスペクションで、NetBIOS インスペクション マップを作成、表示、管理します。NetBIOS マップを使用して、NetBIOS プロトコルに確実に準拠し、フィールドの数と長さの整合性やメッセージなどをチェックできます。
RADIUS Accounting	RADIUS アカウンティング インスペクションで、RADIUS アカウンティング インスペクション マップを作成、表示、管理します。RADIUS マップを使用すると、過剰請求攻撃を防御できます。
RTSP	RTSP インスペクションで、RTSP インスペクション マップを作成、表示、管理できます。RTSP マップを使用して、RTSP PAT を含む RTSP トラフィックを保護できます。
SCCP（Skinny）	SCCP（Skinny）インスペクションで、SCCP（Skinny）のインスペクション マップを作成、表示、管理します。SCCP マップを使用して、プロトコル準拠チェックと基本的なステート トラッキングができます。
SIP	SIP インスペクションで、SIP のインスペクション マップを作成、表示、管理します。SIP マップを使用して、アプリケーションのセキュリティとプロトコル準拠をチェックし、SIP を利用した攻撃を防御できます。SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、インスタント メッセージ機能で幅広く利用されているプロトコルです。
SNMP	SNMP インスペクションで、SNMP のインスペクション マップを作成、表示、管理します。SNMP は、ネットワーク管理デバイスとネットワーク管理ステーション間の通信に利用されるプロトコルです。SNMP マップを使用して、SNMP v1、2、2c、3 など特定の SNMP バージョンをブロックできます。

DCERPC Inspect Map

[DCERPC] ペインでは、DCERPC アプリケーションの事前に設定されたインスペクション マップを表示できます。DCERPC マップでは、DCERPC アプリケーション インスペクションのデフォルト設定値を変更できます。

DCERPC は、Microsoft 社の分散クライアント/サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。

通常、このプロトコルの接続では、クライアントがウェルノウン ポート番号で接続を受け入れるエンドポイント マッパー（EPM）というサーバに、必要なサービスについて動的に割り当てられるネットワーク情報を問い合わせます。次に、クライアントは、サービスを提供しているサーバのインスタンスへのセカンダリ接続をセットアップします。セキュリティ アプライアンスは、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許可し、必要に応じて Network Address Translation（NAT; ネットワーク アドレス変換）を適用します。

DCERPC インスペクション マップは、TCP の予約済みポート 135 を経由した、EPM とクライアント間のネイティブ TCP の通信を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバは、どのセキュリティ ゾーンにあってもかまいません。埋め込まれたサーバの IP アドレスとポート番号は、EPM からの応答メッセージで受け取ります。クライアントが EPM から返されたサーバのポートに対して複数の接続を試みる可能性があるので、ピンホールが複数使用でき、ユーザがそのタイムアウトを設定できるようになっています。

フィールド

- [DCERPC Inspect Maps] : 定義されている DCERPC インスペクション マップを一覧表示するテーブルです。

- [Add] : 新しい DCERPC インスペクションを設定します。DCERPC インスペクション マップを編集するには、[DCERPC Inspect Maps] テーブルで DCERPC のエントリを選択し、[Customize] をクリックします。
- [Delete] : [DCERPC Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level] : セキュリティ レベル（High、Medium、Low）を選択します。
  - Low

    ピンホールのタイムアウト : 00:02:00

    エンドポイント マッパー サービス : 適用強制しない

    エンドポイント マッパー サービス ルックアップ : イネーブル

    エンドポイント マッパー サービス ルックアップのタイムアウト : 00:05:00
  - Medium : デフォルト

    ピンホールのタイムアウト : 00:01:00

    エンドポイント マッパー サービス : 適用強制しない

    エンドポイント マッパー サービス ルックアップ : ディセーブル
  - High

    ピンホールのタイムアウト : 00:01:00

    エンドポイント マッパー サービス : 適用強制する

    エンドポイント マッパー サービス ルックアップ : ディセーブル
  - [Customize] : [Add/Edit DCERPC Policy Map] ダイアログボックスを開き、追加の設定を行います。
  - [Default Level] : セキュリティ レベルをデフォルトの Medium レベルに戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DCERPC Policy Map

[Add/Edit DCERPC Policy Map] ペインでは、DCERPC アプリケーション インスペクション マップのセキュリティ レベルとパラメータを設定できます。

フィールド

- [Name] : DCERPC マップの追加時に DCERPC マップの名前を入力します。DCERPC マップの編集時には、事前に設定した DCERPC マップの名前が表示されます。
- [Description] : DCERPC マップの説明を 200 文字以内で入力します。
- [Security Level] : セキュリティ レベル（High、Medium、Low）を選択します。

- Low

  ピンホールのタイムアウト：00:02:00

  エンドポイント マッパー サービス：適用強制しない

  エンドポイント マッパー サービス ルックアップ：イネーブル

  エンドポイント マッパー サービス ルックアップのタイムアウト：00:05:00

- Medium：デフォルト

  ピンホールのタイムアウト：00:01:00

  エンドポイント マッパー サービス：適用強制しない

  エンドポイント マッパー サービス ルックアップ：ディセーブル

- High

  ピンホールのタイムアウト：00:01:00

  エンドポイント マッパー サービス：適用強制する

  エンドポイント マッパー サービス ルックアップ：ディセーブル

- [Default Level]：セキュリティ レベルをデフォルトの Medium レベルに戻します。

• [Details]：詳細な設定を行うためのパラメータを表示します。

- [Pinhole Timeout]：ピンホール タイムアウトを設定します。クライアントが使用するサーバ情報は、複数の接続のエンドポイント マッパーから返される場合があるため、タイムアウト値はクライアントのアプリケーション環境を考慮して設定します。範囲は、0:0:1 ～ 1193:0:0 です。デフォルトは 2 分です。

- [Enforce endpoint-mapper service]：バインディング中にエンドポイント マッパー サービスを適用します。

- [Enable endpoint-mapper service lookup]：エンドポイント マッパー サービスのルックアップをイネーブルにします。ディセーブルの場合、ピンホール タイムアウトが適用されます。

  [Enforce Service Lookup Timeout]：指定されたサービス ルックアップ タイムアウトを適用します。

  [Service Lookup Timeout]：ルックアップでピンホールした場合のタイムアウトを設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

DNS Inspect Map

[DNS] ペインでは、DNS アプリケーションの事前に設定されたインスペクション マップを表示できます。DNS マップを使用すると、DNS アプリケーション インスペクションに使用するデフォルト設定値を変更できます。

DNS アプリケーション インスペクションは、DNS スプーフィングとキャッシュ ポイズニングを防ぐための DNS メッセージ制御をサポートしています。ユーザが設定できるルールを使用して、特定の DNS タイプを許可、ドロップ、ロギングし、他の DNS タイプをブロックすることができます。たとえば、ゾーン転送をこの機能のあるサーバ間だけに制限できます。

公開サーバが特定の内部ゾーンだけをサポートしている場合に、DNS ヘッダーにある Recursion Desired フラグと Recursion Available フラグをマスクして、サーバを攻撃から守ることができます。また、DNS のランダム化をイネーブルにすると、ランダム化をサポートしていないサーバや強度の低い疑似乱数ジェネレータを使用するサーバのスプーフィングやキャッシュ ポイズニングを回避できます。照会できるドメイン名を制限することにより、公開サーバの保護がさらに確実になります。

不一致の DNS 応答数が過度に増えた場合（キャッシュ ポイズニング攻撃を示している可能性がある）、DNS 不一致のアラートを設定して通知することができます。さらに、すべての DNS メッセージにトランザクション署名（TSIG）を付けるようにチェックする設定も行うことができます。

フィールド

- [DNS Inspect Maps]：定義されている DNS インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい DNS インスペクション マップを設定します。DNS インスペクション マップを編集するには、[DNS Inspect Maps] テーブルで DNS のエントリを選択し、[Customize] をクリックします。
- [Delete]：[DNS Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level]：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    DNS Guard：イネーブル

    NAT のリライト：イネーブル

    プロトコル適用：イネーブル

    ID のランダム化：ディセーブル

    メッセージの長さのチェック：イネーブル

    メッセージの最大長：512

    不一致レートのロギング：ディセーブル

    TSIG リソース レコード：適用強制しない
  - Medium

    DNS Guard：イネーブル

    NAT のリライト：イネーブル

    プロトコル適用：イネーブル

    ID のランダム化：イネーブル

    メッセージの長さのチェック：イネーブル

    メッセージの最大長：512

    不一致レートのロギング：イネーブル

    TSIG リソース レコード：適用強制しない
  - High

    DNS Guard：イネーブル

    NAT のリライト：イネーブル

プロトコル適用：イネーブル

ID のランダム化：イネーブル

メッセージの長さのチェック：イネーブル

メッセージの最大長：512

不一致レートのロギング：イネーブル

TSIG リソース レコード：適用強制する

- [Customize]：[Add/Edit DNS Policy Map] ダイアログボックスを開き、追加の設定を行います。
- [Default Level]：セキュリティ レベルをデフォルトの Low レベルに戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DNS Policy Map（セキュリティ レベル）

[Add/Edit DNS Policy Map] ペインでは、DNS アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：DNS マップの追加時に DNS マップの名前を入力します。DNS マップの編集時には、事前に設定した DNS マップの名前が表示されます。
- [Description]：DNS マップの説明を 200 文字以内で入力します。
- [Security Level]：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    DNS Guard：イネーブル

    NAT のリライト：イネーブル

    プロトコル適用：イネーブル

    ID のランダム化：ディセーブル

    メッセージの長さのチェック：イネーブル

    メッセージの最大長：512

    不一致レートのロギング：ディセーブル

    TSIG リソース レコード：適用強制しない
  - Medium

    DNS Guard：イネーブル

    NAT のリライト：イネーブル

プロトコル適用：イネーブル

ID のランダム化：イネーブル

メッセージの長さのチェック：イネーブル

メッセージの最大長：512

不一致レートのロギング：イネーブル

TSIG リソース レコード：適用強制しない

– High

DNS Guard：イネーブル

NAT のリライト：イネーブル

プロトコル適用：イネーブル

ID のランダム化：イネーブル

メッセージの長さのチェック：イネーブル

メッセージの最大長：512

不一致レートのロギング：イネーブル

TSIG リソース レコード：適用強制する

– [Default Level]：セキュリティ レベルをデフォルトの Low レベルに戻します。

- [Details]：詳細な設定を行うための [Protocol Conformance] タブ、[Filtering] タブ、[Mismatch Rate] タブ、および [Inspection] タブを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DNS Policy Map（詳細）

[Add/Edit DNS Policy Map] ペインでは、DNS アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：DNS マップの追加時に DNS マップの名前を入力します。DNS マップの編集時には、事前に設定した DNS マップの名前が表示されます。
- [Description]：DNS マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルを表示します。
- [Protocol Conformance]：このタブで DNS のプロトコル準拠を設定します。

- [Enable DNS guard function]：DNS ヘッダーの識別フィールドを使用して、DNS クエリーと応答の不一致のチェックを行います。クエリーごとに 1 つの応答がセキュリティ アプライアンスを通過できます。
- [Enable NAT re-write function]：DNS 応答の A レコードにある IP アドレスの変換をイネーブルにします。
- [Enable protocol enforcement]：DNS メッセージの形式チェックをイネーブルにします。ドメイン名、ラベルの長さ、圧縮、ループしたポインタなどをチェックします。
- [Randomize the DNS identifier for DNS query]：DNS クエリー メッセージの DNS 識別子をランダム化します。
- [Enforce TSIG resource record to be present in DNS message]：TSIG リソース レコードが DNS トランザクションに存在する必要があります。TSIG を強制的に適用すると、次のアクションが実行されます。

  [Drop packet]：パケットをドロップします（ロギングはイネーブルまたはディセーブルに指定できます）。

  [Log]：ロギングをイネーブルにします。

- [Filtering]：このタブで DNS のフィルタリングを設定します。
  - [Global Settings]：設定がグローバルに適用されます。

    [Drop packets that exceed specified maximum length (global)]：最大長（バイト）を超えるパケットをドロップします。

    [Maximum Packet Length]：パケットの最大長をバイト単位で入力します。
  - [Server Settings]：サーバの設定だけを適用します。

    [Drop packets that exceed specified maximum length]：最大長（バイト）を超えるパケットをドロップします。

    [Maximum Packet Length]：パケットの最大長をバイト単位で入力します。

    [Drop packets sent to server that exceed length indicated by the RR]：[Resource Record] で指定された長さを超えるパケットがサーバに送信された場合はドロップします。
  - [Client Settings]：クライアントの設定だけを適用します。

    [Drop packets that exceed specified maximum length]：最大長（バイト）を超えるパケットをドロップします。

    [Maximum Packet Length]：パケットの最大長をバイト単位で入力します。

    [Drop packets sent to client that exceed length indicated by the RR]：[Resource Record] で指定された長さを超えるパケットがクライアントに送信された場合はドロップします。
- [Mismatch Rate]：このタブで DNS の ID 不一致レートを設定します。
  - [Enable Logging when DNS ID mismatch rate exceeds specified rate]：DNS 識別子の不一致が多く発生した場合にレポートを表示します。

    [Mismatch Instance Threshold]：不一致のインスタンスの最大数を入力します。この値を超えると、システム メッセージ ログに出力されます。

    [Time Interval]：監視間隔時間（秒単位）を入力します。
- [Inspections]：このタブで DNS インスペクションのコンフィギュレーションを表示して、追加や編集ができます。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：DNS インスペクションの基準を示します。

- [Value]：DNS インスペクションで照合する値を示します。
- [Action]：照合条件が一致したときのアクションを示します。
- [Log]：ログの状態を示します。
- [Add]：[Add DNS Inspect] ダイアログボックスが開き、DNS インスペクションを追加できます。
- [Edit]：[Edit DNS Inspect] ダイアログボックスが開き、DNS インスペクションを編集できます。
- [Delete]：DNS インスペクションを削除します。
- [Move Up]：インスペクションをリストの上に移動します。
- [Move Down]：インスペクションをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DNS Inspect

[Add/Edit DNS Inspect] ダイアログボックスでは、DNS インスペクション マップの照合基準と値を定義できます。

フィールド

- [Single Match]：DNS インスペクションに照合文が 1 つだけの場合に指定します。
- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：DNS トラフィックに適用する照合基準を指定します。
  - [Header Flag]：ヘッダーの DNS フラグを照合します。
  - [Type]：DNS クエリーまたはリソース レコードのタイプを照合します。
  - [Class]：DNS クエリーまたはリソース レコードのクラスを照合します。
  - [Question]：DNS の問い合わせを照合します。
  - [Resource Record]：DNS リソース レコードを照合します。
  - [Domain Name]：DNS クエリーやリソース レコードのドメイン名を照合します。
- [Header Flag Criterion Values]：DNS ヘッダー フラグの照合値の詳細を指定します。
  - [Match Option]：完全一致または全ビット一致（ビット マスク一致）のどちらかを指定します。
  - [Match Value]：ヘッダー フラグについて名前と値のどちらを照合するか指定します。

[Header Flag Name]：照合するヘッダー フラグ名を 1 つ以上選択できます。AA（authoritative answer）、QR（query）、RA（recursion available）、RD（recursion denied）、TC（truncation）のフラグ ビットがあります。

[Header Flag Value]：任意の 16 ビットの値を 16 進数で入力して照合できます。

- [Type Criterion Values]：DNS タイプの照合値の詳細を指定します。
  - [DNS Type Field Name]：選択する DNS タイプを一覧表示します。

    [A]：IPv4 アドレス

    [NS]：権限ネーム サーバ

    [CNAME]：正規名

    [SOA]：信頼ゾーンの開始

    [TSIG]：トランザクション シグニチャ

    [IXFR]：増分（ゾーン）転送

    [AXFR]：フル（ゾーン）転送
  - [DNS Type Field Value]：DNS タイプ フィールドについて値と範囲のどちらを照合するか指定します。

    [Value]：0 ～ 65535 の範囲の値を入力して照合できます。

    [Range]：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。
- [Class Criterion Values]：DNS クラスの照合値の詳細を指定します。
  - [DNS Class Field Name]：インターネットで照合する DNS クラス フィールド名を指定します。
  - [DNS Class Field Value]：DNS クラス フィールドについて値と範囲のどちらを照合するか指定します。

    [Value]：0 ～ 65535 の範囲の値を入力して照合できます。

    [Range]：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。
- [Question Criterion Values]：DNS の問い合わせセクションの照合方法を指定します。
- [Resource Record Criterion Values]：DNS リソース レコードのセクションの照合方法を指定します。
  - [Resource Record]：照合対象セクションを一覧表示します。

    [Additional]：DNS 追加リソース レコード

    [Answer]：DNS 応答リソース レコード

    [Authority]：DNS 認証リソース レコード
- [Domain Name Criterion Values]：DNS ドメイン名の照合方法を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Multiple Matches]：DNS インスペクションの複数の照合文を指定します。
  - [DNS Traffic Class]：DNS トラフィック クラスを照合します。

  - [Manage] : [Manage DNS Class Maps] ダイアログボックスが開き、DNS クラス マップの追加、編集、削除ができます。
- [Actions] : プライマリ アクションおよびログを設定します。
  - [Primary Action] : Mask、Drop packet、Drop connection、None。
  - [Log] : イネーブルまたはディセーブルにします。
  - [Enforce TSIG] : 適用強制しない、パケットをドロップ、ログに出力、パケットをドロップしてログに出力。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Manage Class Maps

[Manage Class Map] ダイアログボックスでは、インスペクションのクラス マップを設定できます。

インスペクション クラス マップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラス マップをインスペクション マップから特定して、アクションをイネーブルにします。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。インスペクション クラス マップは DNS、FTP、H.323、HTTP、インスタント メッセージ（IM）、SIP のアプリケーションでサポートされます。

フィールド

- [Name] : クラス マップの名前を示します。
- [Match Conditions] : クラス マップに設定されているタイプ、照合基準、値を示します。
  - [Match Type] : 一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion] : クラス マップの基準を示します。
  - [Value] : クラス マップで照合する値を示します。
- [Description] : クラス マップの説明を示します。
- [Add] : クラス マップの照合条件を追加します。
- [Edit] : クラス マップの照合条件を編集します。
- [Delete] : クラス マップの照合条件を削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ESMTP Inspect Map

[ESMTP] ペインでは、ESMTP アプリケーションの事前に設定されたインスペクション マップを表示できます。ESMTP マップでは、ESMTP アプリケーション インスペクションのデフォルト設定値を変更できます。

スパム、フィッシング、不正な形式のメッセージ、バッファ オーバーフロー/アンダーフローなどの攻撃の大部分は ESMTP トラフィックから発生するので、ESMTP トラフィックのパケットを詳細に検査して制御します。アプリケーション セキュリティとプロトコルで正常な ESMTP メッセージだけを通し、各種の攻撃の検出、送受信者およびメール中継のブロックも行います。

フィールド

- [ESMTP Inspect Maps]：定義されている ESMTP インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい ESMTP インスペクション マップを設定します。ESMTP インスペクション マップを編集するには、[ESMTP Inspect Maps] テーブルで ESMTP のエントリを選択し、[Customize] をクリックします。
- [Delete]：[ESMTP Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level]：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    コマンドラインの長さが 512 を超える場合、ログを出力

    コマンドの宛先の数が 100 を超える場合、ログを出力

    本文の行の長さが 1000 を超える場合、ログを出力

    送信者のアドレスの長さが 320 を超える場合、ログを出力

    MIME ファイル名の長さが 255 を超える場合、ログを出力
  - Medium

    サーバ バナーを難読化

    コマンドラインの長さが 512 を超える場合、接続をドロップ

    コマンドの宛先の数が 100 を超える場合、接続をドロップ

    本文の行の長さが 1000 を超える場合、接続をドロップ

    送信者のアドレスの長さが 320 を超える場合、接続をドロップ

    MIME ファイル名の長さが 255 を超える場合、接続をドロップ
  - High

    サーバ バナーを難読化

    コマンドラインの長さが 512 を超える場合、接続をドロップ

コマンドの宛先の数が 100 を超える場合、接続をドロップ

本文の行の長さが 1000 を超える場合、接続をドロップ

送信者のアドレスの長さが 320 を超える場合、接続をドロップしてログを出力

MIME ファイル名の長さが 255 を超える場合、接続をドロップしてログを出力

- [MIME File Type Filtering] : [MIME Type Filtering] ダイアログボックスを開き、MIME ファイル タイプのフィルタを設定します。
- [Customize] : [Add/Edit ESMTP Policy Map] ダイアログボックスを開き、追加の設定を行います。
- [Default Level] : セキュリティ レベルをデフォルトの Low レベルに戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

MIME File Type Filtering

[MIME File Type Filtering] ダイアログボックスでは、MIME ファイル タイプのフィルタを設定できます。

フィールド

- [Match Type] : 一致タイプを示します。肯定一致と否定一致があります。
- [Criterion] : インスペクションの基準を示します。
- [Value] : インスペクションで照合する値を示します。
- [Action] : 照合条件が一致したときのアクションを示します。
- [Log] : ログの状態を示します。
- [Add] : [Add MIME File Type Filter] ダイアログボックスが開き、MIME ファイル タイプのフィルタを追加できます。
- [Edit] : [Edit MIME File Type Filter] ダイアログボックスが開き、MIME ファイル タイプのフィルタを編集できます。
- [Delete] : MIME ファイル タイプのフィルタを削除します。
- [Move Up] : エントリをリストの上に移動します。
- [Move Down] : エントリをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit ESMTP Policy Map（セキュリティ レベル）

[Add/Edit ESMTP Policy Map] ペインでは、ESMTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：ESMTP マップの追加時に ESMTP マップの名前を入力します。ESMTP マップの編集時には、事前に設定した ESMTP マップの名前が表示されます。
- [Description]：ESMTP マップの説明を 200 文字以内で入力します。
- [Security Level]：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    コマンドラインの長さが 512 を超える場合、ログを出力

    コマンドの宛先の数が 100 を超える場合、ログを出力

    本文の行の長さが 1000 を超える場合、ログを出力

    送信者のアドレスの長さが 320 を超える場合、ログを出力

    MIME ファイル名の長さが 255 を超える場合、ログを出力
  - Medium

    サーバ バナーを難読化

    コマンドラインの長さが 512 を超える場合、接続をドロップ

    コマンドの宛先の数が 100 を超える場合、接続をドロップ

    本文の行の長さが 1000 を超える場合、接続をドロップ

    送信者のアドレスの長さが 320 を超える場合、接続をドロップ

    MIME ファイル名の長さが 255 を超える場合、接続をドロップ
  - High

    サーバ バナーを難読化

    コマンドラインの長さが 512 を超える場合、接続をドロップ

    コマンドの宛先の数が 100 を超える場合、接続をドロップ

    本文の行の長さが 1000 を超える場合、接続をドロップ

    送信者のアドレスの長さが 320 を超える場合、接続をドロップしてログを出力

    MIME ファイル名の長さが 255 を超える場合、接続をドロップしてログを出力
  - [MIME File Type Filtering]：[MIME Type Filtering] ダイアログボックスを開き、MIME ファイル タイプのフィルタを設定します。
  - [Default Level]：セキュリティ レベルをデフォルトの Low レベルに戻します。

- [Details]：詳細な設定を行うための [Parameters] タブと [Inspections] タブを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit ESMTP Policy Map（詳細）

[Add/Edit ESMTP Policy Map] ペインでは、ESMTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：ESMTP マップの追加時に ESMTP マップの名前を入力します。ESMTP マップの編集時には、事前に設定した ESMTP マップの名前が表示されます。
- [Description]：ESMTP マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルと MIME ファイル タイプ フィルタリング設定を表示します。
- [Parameters]：このタブで ESMTP インスペクション マップのパラメータを設定します。
  - [Mask server banner]：バナーを難読化します。
  - [Configure Mail Relay]：ESMTP のメール中継をイネーブルにします。

    [Domain Name]：ローカル ドメインを指定します。

    [Action]：Drop connection または Log。

    [Log]：イネーブルまたはディセーブルにします。
- [Inspections]：このタブで ESMTP インスペクションのコンフィギュレーションを表示して、追加や編集ができます。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：ESMTP インスペクションの基準を示します。
  - [Value]：ESMTP インスペクションで照合する値を示します。
  - [Action]：照合条件が一致したときのアクションを示します。
  - [Log]：ログの状態を示します。
  - [Add]：[Add ESMTP Inspect] ダイアログボックスが開き、ESMTP インスペクションを追加できます。
  - [Edit]：Edit [ESMTP Inspect] ダイアログボックスが開き、ESMTP インスペクションを編集できます。
  - [Delete]：ESMTP インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。
  - [Move Down]：インスペクションをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit ESMTP Inspect

[Add/Edit ESMTP Inspect] ダイアログボックスでは、ESMTP インスペクション マップの照合基準と値を定義できます。

フィールド

- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

- [Criterion]：ESMTP トラフィックに適用する照合基準を指定します。
  - [Body Length]：本文の長さと指定した長さをバイト単位で照合します。
  - [Body Line Length]：本文の行の長さと指定した長さをバイト単位で照合します。
  - [Commands]：ESMTP プロトコルで交換されるコマンドを照合します。
  - [Command Recipient Count]：コマンド宛先の数が指定した数より大きい場合に照合します。
  - [Command Line Length]：コマンドラインが指定した長さより長い場合に、バイト単位で照合します。
  - [EHLO Reply Parameters]：ESMTP の EHLO 応答パラメータを照合します。
  - [Header Length]：ヘッダーの長さと指定した長さをバイト単位で照合します。
  - [Header To Fields Count]：ヘッダーの [To] フィールドの数が指定した数より大きい場合に照合します。
  - [Invalid Recipients Count]：無効な宛先の数が指定した数より大きい場合に照合します。
  - [MIME File Type]：MIME ファイル タイプを照合します。
  - [MIME Filename Length]：MIME ファイル名を照合します。
  - [MIME Encoding]：MIME の符号化を照合します。
  - [Sender Address]：送信者の電子メール アドレスを照合します。
  - [Sender Address Length]：送信者の電子メール アドレスの長さを照合します。
- [Body Length Criterion Values]：本文の長さの照合値に関する詳細を指定します。
  - [Greater Than Length]：本文の長さをバイト単位で指定します。
  - [Action]：Reset、Drop connection、または Log。
  - [Log]：イネーブルまたはディセーブルにします。
- [Body Line Length Criterion Values]：本文の行の長さの照合値に関する詳細を指定します。

  - [Greater Than Length]：本文の行の長さをバイト単位で指定します。
  - [Action]：Reset、Drop connection、または Log。
  - [Log]：イネーブルまたはディセーブルにします。
- [Commands Criterion Values]：コマンドの照合値の詳細を指定します。
  - [Available Commands] テーブル

    AUTH

    DATA

    EHLO

    ETRN

    HELO

    HELP

    MAIL

    NOOP

    QUIT

    RCPT

    RSET

    SAML

    SOML

    VRFY
  - [Add]：[Available Commands] テーブルで選択したコマンドを [Selected Commands] テーブルに追加します。
  - [Remove]：選択したコマンドを [Selected Commands] テーブルから削除します。
  - [Primary Action]：Mask、Reset、Drop Connection、None、または Limit Rate (pps)。
  - [Log]：イネーブルまたはディセーブルにします。
  - [Rate Limit]：Do not limit rate、Limit Rate (pps)。
- [Command Recipient Count Criterion Values]：コマンド宛先の数の照合値に関する詳細を指定します。
  - [Greater Than Count]：コマンド宛先の数を指定します。
  - [Action]：Reset、Drop connection、または Log。
  - [Log]：イネーブルまたはディセーブルにします。
- [Command Line Length Criterion Values]：コマンドラインの長さの値に関する詳細を指定します。
  - [Greater Than Length]：コマンドラインの長さをバイト単位で指定します。
  - [Action]：Reset、Drop connection、または Log。
  - [Log]：イネーブルまたはディセーブルにします。
- [EHLO Reply Parameters Criterion Values]：EHLO 応答パラメータの照合値の詳細を指定します。
  - [Available Parameters] テーブル

    8bitmime

    auth

binarymime

checkpoint

dsn

ecode

etrn

others

pipelining

size

vrfy

  - [Add] : [Available Parameters] テーブルで選択したパラメータを [Selected Parameters] テーブルに追加します。
  - [Remove] : 選択したコマンドを [Selected Commands] テーブルから削除します。
  - [Action] : Reset、Drop Connection、Mask、または Log。
  - [Log] : イネーブルまたはディセーブルにします。
- [Header Length Criterion Values] : ヘッダーの長さの照合値に関する詳細を指定します。
  - [Greater Than Length] : ヘッダーの長さをバイト単位で指定します。
  - [Action] : Reset、Drop Connection、Mask、または Log。
  - [Log] : イネーブルまたはディセーブルにします。
- [Header To Fields Count Criterion Values]:ヘッダーの To フィールド数の照合値に関する詳細を指定します。
  - [Greater Than Count] : コマンド宛先の数を指定します。
  - [Action] : Reset、Drop connection、または Log。
  - [Log] : イネーブルまたはディセーブルにします。
- [Invalid Recipients Count Criterion Values] : 無効な宛先の数の照合値に関する詳細を指定します。
  - [Greater Than Count] : コマンド宛先の数を指定します。
  - [Action] : Reset、Drop connection、または Log。
  - [Log] : イネーブルまたはディセーブルにします。
- [MIME File Type Criterion Values] : MIME ファイル タイプの照合値の詳細を指定します。
  - [Regular Expression] : 照合する定義された正規表現を一覧表示します。
  - [Manage] : [Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class] : 照合する定義された正規表現クラスを一覧表示します。
  - [Manage] : [Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
  - [Action] : Reset、Drop connection、または Log。
  - [Log] : イネーブルまたはディセーブルにします。
- [MIME Filename Length Criterion Values] : MIME ファイル名の長さの照合値に関する詳細を指定します。
  - [Greater Than Length] : MIME ファイル名の長さをバイト単位で指定します。

  - [Action]：Reset、Drop Connection、または Log。
  - [Log]：イネーブルまたはディセーブルにします。
- [MIME Encoding Criterion Values]：MIME の符号化の照合値に関する詳細を指定します。
  - [Available Encodings] テーブル

    7bit

    8bit

    base64

    binary

    others

    quoted-printable
  - [Add]：[Available Encodings] テーブルで選択したパラメータを [Selected Encodings] テーブルに追加します。
  - [Remove]：選択したコマンドを [Selected Commands] テーブルから削除します。
  - [Action]：Reset、Drop Connection、または Log。
  - [Log]：イネーブルまたはディセーブルにします。
- [Sender Address Criterion Values]：送信者アドレスの照合値の詳細を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
  - [Action]：Reset、Drop Connection、または Log。
  - [Log]：イネーブルまたはディセーブルにします。
- [Sender Address Length Criterion Values]：送信者アドレスの長さの照合値に関する詳細を指定します。
  - [Greater Than Length]：送信者アドレスの長さをバイト単位で指定します。
  - [Action]：Reset、Drop Connection、または Log。
  - [Log]：イネーブルまたはディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

FTP Inspect Map

[FTP] ペインでは、FTP アプリケーションの事前に設定されたインスペクション マップを表示できます。FTP マップでは、FTP アプリケーション インスペクションのデフォルト設定値を変更できます。

厳密な FTP インスペクションには、セキュリティと制御を向上させるためのコマンド フィルタリングとセキュリティ チェック機能が用意されています。プロトコルとの適合性のインスペクションには、パケットの長さのチェック、デリミタとパケットの形式のチェック、コマンドのターミネータのチェック、およびコマンドの検証が含まれます。

また、ユーザの値に基づいて FTP 接続をブロックできるので、FTP サイトにダウンロード用のファイルを置き、アクセスを特定のユーザだけに制限できます。ファイルのタイプ、サーバ名、および他の属性に基づいて、FTP 接続をブロックできます。インスペクション時に FTP 接続が拒否されると、システム メッセージのログが作成されます。

フィールド

- [FTP Inspect Maps]：定義されている FTP インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい FTP インスペクション マップを設定します。FTP インスペクション マップを編集するには、[FTP Inspect Maps] テーブルで FTP のエントリを選択し、[Customize] をクリックします。
- [Delete]：[FTP Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level]：セキュリティ レベル（Medium または Low）を選択します。
  - Low

    Mask Banner：ディセーブル

    Mask Reply：ディセーブル
  - Medium：デフォルト

    Mask Banner：イネーブル

    Mask Reply：イネーブル
  - [File Type Filtering]：[Type Filtering] ダイアログボックスを開き、ファイル タイプのフィルタを設定します。
  - [Customize]：[Add/Edit FTP Policy Map] ダイアログボックスを開き、追加の設定を行います。
  - [Default Level]：セキュリティ レベルをデフォルトの Medium レベルに戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

File Type Filtering

[File Type Filtering] ダイアログボックスでは、ファイル タイプ フィルタを設定できます。

フィールド

- [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
- [Criterion]：インスペクションの基準を示します。
- [Value]：インスペクションで照合する値を示します。
- [Action]：照合条件が一致したときのアクションを示します。
- [Log]：ログの状態を示します。
- [Add]：[Add File Type Filter] ダイアログボックスが開き、ファイル タイプのフィルタを追加できます。
- [Edit]：[Edit File Type Filter] ダイアログボックスが開き、ファイル タイプのフィルタを編集できます。
- [Delete]：ファイル タイプのフィルタを削除します。
- [Move Up]：エントリをリストの上に移動します。
- [Move Down]：エントリをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit FTP Policy Map（セキュリティ レベル）

[Add/Edit FTP Policy Map] ペインでは、FTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：FTP マップの追加時に FTP マップの名前を入力します。FTP マップの編集時には、事前に設定した FTP マップの名前が表示されます。
- [Description]：FTP マップの説明を 200 文字以内で入力します。
- [Security Level]：セキュリティ レベル（Medium または Low）を選択します。
  - Low

    Mask Banner：ディセーブル

    Mask Reply：ディセーブル
  - Medium：デフォルト

    Mask Banner：イネーブル

Mask Reply：イネーブル

- [File Type Filtering]：[Type Filtering] ダイアログボックスを開き、ファイル タイプのフィルタを設定します。
- [Default Level]：セキュリティ レベルをデフォルトの Medium レベルに戻します。

- [Details]：詳細な設定を行うための [Parameters] タブと [Inspections] タブを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit FTP Policy Map（詳細）

[Add/Edit FTP Policy Map] ペインでは、FTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：FTP マップの追加時に FTP マップの名前を入力します。FTP マップの編集時には、事前に設定した FTP マップの名前が表示されます。
- [Description]：FTP マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルとファイル タイプ フィルタリング設定を表示します。
- [Parameters]：このタブで FTP インスペクション マップのパラメータを設定します。
  - [Mask greeting banner from the server]：FTP サーバとの接続時に表示されるバナーをマスクし、クライアントに対するサーバ情報の公開を防止します。
  - [Mask reply to SYST command]：syst コマンドに対する応答をマスクし、クライアントに対するサーバ情報の公開を防止します。
- [Inspections]：このタブで FTP インスペクションのコンフィギュレーションを表示して、追加や編集ができます。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：FTP インスペクションの基準を示します。
  - [Value]：FTP インスペクションで照合する値を示します。
  - [Action]：照合条件が一致したときのアクションを示します。
  - [Log]：ログの状態を示します。
  - [Add]：[Add FTP Inspect] ダイアログボックスが開き、FTP インスペクションを追加できます。
  - [Edit]：[Edit FTP Inspect] ダイアログボックスが開き、FTP インスペクションを編集できます。

- [Delete]：FTP インスペクションを削除します。
- [Move Up]：インスペクションをリストの上に移動します。
- [Move Down]：インスペクションをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit FTP Map

[Add/Edit FTP Inspect] ダイアログボックスでは、FTP インスペクション マップの照合基準と値を定義できます。

フィールド

- [Single Match]：FTP インスペクションに照合文が 1 つだけの場合に指定します。
- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：FTP トラフィックに適用する照合基準を指定します。
  - [Request-Command]：FTP 要求コマンドを照合します。
  - [File Name]：FTP 転送のファイル名を照合します。
  - [File Type]：FTP 転送のファイル タイプを照合します。
  - [Server]：FTP サーバを照合します。
  - [User Name]：FTP ユーザを照合します。
- [Request Command Criterion Values]：FTP 要求コマンドの照合値の詳細を指定します。
  - 要求コマンド

    APPE：ファイルに追加するコマンド

    CDUP：現在の作業ディレクトリの親ディレクトリに移動するコマンド

    DELE：ファイルを削除するコマンド

    GET：ファイルを取得するコマンド

    HELP：ヘルプ情報を提供するコマンド

    MKD：ディレクトリを作成するコマンド

    PUT：ファイルを送信するコマンド

    RMD：ディレクトリを削除するコマンド

    RNFR：変更元ファイル名を指定するコマンド

RNTO：変更先ファイル名を指定するコマンド

SITE：サーバ システム固有のコマンド。通常、リモート管理に使用します。

STOU：一意のファイル名を使用してファイル名を保存するコマンド

- [File Name Criterion Values]：FTP ファイル名の照合値の詳細を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [File Type Criterion Values]：FTP ファイル タイプの照合値の詳細を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Server Criterion Values]：FTP サーバの照合値の詳細を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [User Name Criterion Values]：FTP ユーザ名の照合値の詳細を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Multiple Matches]：FTP インスペクションの複数の照合文を指定します。
  - [FTP Traffic Class]：FTP トラフィック クラスを照合します。
  - [Manage]：[Manage FTP Class Maps] ダイアログボックスが開き、FTP クラス マップの追加、編集、削除ができます。
- [Action]：Reset。
- [Log]：イネーブルまたはディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

GTP Inspect Map

[GTP] ペインでは、GTP アプリケーションの事前に設定されたインスペクション マップを表示できます。GTP マップでは、GTP アプリケーション インスペクションのデフォルト設定値を変更できます。

GTP は比較的新しいプロトコルで、インターネットなど TCP/IP ネットワークと無線接続する場合のセキュリティを提供します。GTP マップを使用して、タイムアウト値、メッセージ サイズ、トンネル数、およびセキュリティ アプライアンスを通過する GTP バージョンを制御できます。

（注） GTP インスペクションには、特別なライセンスが必要です。

フィールド

- [GTP Inspect Maps] : 定義されている GTP インスペクション マップを一覧表示するテーブルです。
- [Add] : 新しい GTP インスペクション マップを設定します。GTP インスペクション マップを編集するには、[GTP Inspect Maps] テーブルで GTP のエントリを選択し、[Customize] をクリックします。
- [Delete] : [GTP Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level] : セキュリティ レベルは常に Low です。
  - エラーを許可しない
  - トンネルの最大数 : 500
  - GSN タイムアウト : 00:30:00
  - PDP コンテキスト タイムアウト : 00:30:00
  - 要求タイムアウト : 00:01:00
  - シグナリング タイムアウト : 00:30:00
  - トンネル タイムアウト : 01:00:00
  - T3 応答タイムアウト : 00:00:20
  - 未知のメッセージ ID をドロップしてログを出力
- [IMSI Prefix Filtering] : [IMSI Prefix Filtering] ダイアログボックスを開き、IMSI プレフィックス フィルタを設定します。
- [Customize] : [Add/Edit GTP Policy Map] ダイアログボックスを開き、追加の設定を行います。
- [Default Level] : セキュリティ レベルをデフォルトに戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

IMSI Prefix Filtering

[IMSI Prefix] タブでは、GTP 要求の中で使用できるように IMSI プレフィックスを定義できます。

フィールド

- [Mobile Country Code] : 0 以外の 3 桁の値でモバイル カントリ コードを定義します。エントリが 1 桁または 2 桁の場合には、その先頭に 0 が付加されて 3 桁の値が作成されます。
- [Mobile Network Code] : 2 桁または 3 桁の数字でネットワーク コードを定義します。
- [Add] : 指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
- [Delete] : 指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit GTP Policy Map（セキュリティ レベル）

[Add/Edit GTP Policy Map] ペインでは、GTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name] : GTP マップの追加時に GTP マップの名前を入力します。GTP マップの編集時には、事前に設定した GTP マップの名前が表示されます。
- [Description] : GTP マップの説明を 200 文字以内で入力します。
- [Security Level] : セキュリティ レベルは常に Low です。

  エラーを許可しない

  トンネルの最大数 : 500

  GSN タイムアウト : 00:30:00

  PDP コンテキスト タイムアウト : 00:30:00

要求タイムアウト：00:01:00

シグナリング タイムアウト：00:30:00

トンネル タイムアウト：01:00:00

T3 応答タイムアウト：00:00:20

未知のメッセージ ID をドロップしてログを出力

- [IMSI Prefix Filtering] : [IMSI Prefix Filtering] ダイアログボックスを開き、IMSI プレフィックス フィルタを設定します。
- [Default Level] : セキュリティ レベルをデフォルトに戻します。

- [Details] : 詳細な設定を行うための [Parameters] タブ、[IMSI Prefix Filtering] タブ、および [Inspections] タブを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit GTP Policy Map（詳細）

[Add/Edit GTP Policy Map] ペインでは、GTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name] : GTP マップの追加時に GTP マップの名前を入力します。GTP マップの編集時には、事前に設定した GTP マップの名前が表示されます。
- [Description] : GTP マップの説明を 200 文字以内で入力します。
- [Security Level] : 設定するセキュリティ レベルと IMSI プレフィックス フィルタリング設定を表示します。
- [Permit Parameters] : このタブで GTP インスペクション マップの許可パラメータを設定します。
  - Object Groups to Add

    [From object group] : オブジェクト グループを指定して、または [Browse] ボタンをクリックして、[Add Network Object Group] ダイアログボックスを開きます。

    [To object group] : オブジェクト グループを指定して、または [Browse] ボタンをクリックして、[Add Network Object Group] ダイアログボックスを開きます。
  - [Add] : 指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
  - [Delete] : 指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。

- [Permit Errors]：無効なパケットやインスペクション時にエラーが見つかったパケットを、ドロップしないでセキュリティ アプライアンスから送信します。デフォルトでは、解析時に失敗したすべての無効パケットがドロップされます。

- [General Parameters]：このタブで GTP インスペクション マップの一般パラメータを設定します。
  - [Maximum Number of Requests]：許容される要求キュー サイズのデフォルト最大値を変更できます。要求キュー サイズのデフォルト最大値は 200 です。キューで応答待ちができる GTP 要求数の最大値を指定します。1 ～ 9999999 の範囲で指定できます。
  - [Maximum Number of Tunnels]：許容されるトンネル数のデフォルト最大値を変更できます。デフォルトのトンネル制限値は 500 です。許可されるトンネルの最大数を指定します。グローバルなトンネル全体の制限値を 1 ～ 9999999 の範囲で指定できます。
  - Timeouts

    [GSN timeout]：GSN を削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

    [PDP-Context timeout]：GTP セッションで PDP コンテキストを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

    [Request Queue]：GTP セッション中に GTP メッセージを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

    [Signaling]：GTP シグナリングを削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

    [Tunnel]：GTP トンネルの非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 時間です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は切断しないことを意味します。

    [Request timeout]：GTP 要求のアイドル タイムアウト値を指定します。

    [T3-Response timeout]：接続を削除するまでの、応答待ち時間の最大値を指定します。

- [IMSI Prefix Filtering]：このタブで GTP インスペクション マップの IMSI プレフィックス フィルタリングを設定します。
  - [Mobile Country Code]：0 以外の 3 桁の値でモバイル カントリ コードを定義します。エントリが 1 桁または 2 桁の場合には、その先頭に 0 が付加されて 3 桁の値が作成されます。
  - [Mobile Network Code]：2 桁または 3 桁の数字でネットワーク コードを定義します。
  - [Add]：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
  - [Delete]：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。

- [Inspections]：このタブで GTP インスペクション マップを設定します。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：GTP インスペクションの基準を示します。
  - [Value]：GTP インスペクションで照合する値を示します。
  - [Action]：照合条件が一致したときのアクションを示します。

- [Log]：ログの状態を示します。
- [Add]：[Add GTP Inspect] ダイアログボックスが開き、GTP インスペクションを追加できます。
- [Edit]：[Edit GTP Inspect] ダイアログボックスが開き、GTP インスペクションを編集できます。
- [Delete]：GTP インスペクションを削除します。
- [Move Up]：インスペクションをリストの上に移動します。
- [Move Down]：インスペクションをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit GTP Map

[Add/Edit GTP Inspect] ダイアログボックスでは、GTP インスペクション マップの照合基準と値を定義できます。

フィールド

- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：GTP トラフィックに適用する照合基準を指定します。
  - [Access Point Name]：アクセス ポイント名を照合します。
  - [Message ID]：メッセージ ID を照合します。
  - [Message Length]：メッセージの長さを照合します。
  - [Version]：バージョンを照合します。
- [Access Point Name Criterion Values]：照合するアクセス ポイント名を指定します。デフォルトでは、有効な APN のメッセージをすべて検査します。すべての APN が指定できます。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
  - [Action]：Drop。
  - [Log]：イネーブルまたはディセーブルにします。

- [Message ID Criterion Values]：照合するメッセージの数値識別子を指定します。有効な指定範囲は 1 ～ 255 です。デフォルトでは、すべての有効なメッセージ ID が許可されます。
  - [Value]：値を完全一致で照合するか、範囲で照合するかを指定します。

    [Equals]：値を入力します。

    [Range]：値の範囲を入力します。
  - [Action]：Drop packet または limit rate (pps)。
  - [Log]：イネーブルまたはディセーブルにします。
- [Message Length Criterion Values]：許可される UDP ペイロードの、メッセージの長さのデフォルト最大値を変更できます。
  - [Minimum value]：UDP ペイロードの最小バイト数を指定します。範囲は、1 ～ 65536 です。
  - [Maximum value]：UDP ペイロードの最大バイト数を指定します。範囲は、1 ～ 65536 です。
  - [Action]：Drop packet。
  - [Log]：イネーブルまたはディセーブルにします。
- [Version Criterion Values]：照合するメッセージの GTP バージョンを指定します。有効な指定範囲は 0 ～ 255 です。バージョン 0 を指定するには 0 を使用し、バージョン 1 を指定するには 1 を使用します。GTP のバージョン 0 はポート 3386 を使用し、バージョン 1 はポート 2123 を使用します。デフォルトでは、すべての GTP バージョンが許可されます。
  - [Value]：値を完全一致で照合するか、範囲で照合するかを指定します。

    [Equals]：値を入力します。

    [Range]：値の範囲を入力します。
  - [Action]：Drop packet。
  - [Log]：イネーブルまたはディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

H.323 Inspect Map

[H.323] ペインでは、H.323 アプリケーションの事前に設定されたインスペクション マップを表示できます。H.323 マップでは、H.323 アプリケーション インスペクションのデフォルト設定値を変更できます。

H.323 インスペクションは RAS、H.225、H.245 をサポートし、埋め込まれた IP アドレスとポートをすべて変換する機能を備えています。ステートのトラッキングとフィルタリングを実行し、インスペクション機能のアクティベーションをカスケードできます。H.323 インスペクションは、電話番号のフィルタリング、T.120 のダイナミック制御、H.245 のトンネル機能制御、HSI グループ、プロトコルのステート トラッキング、H.323 通話時間制限の適用、音声 / ビデオ制御をサポートします。

フィールド

- [H.323 Inspect Maps] : 定義されている H.323 インスペクション マップを一覧表示するテーブルです。
- [Add] : 新しい H.323 インスペクション マップを設定します。H.323 インスペクション マップを編集するには、[H.323 Inspect Maps] テーブルで H.323 のエントリを選択し、[Customize] をクリックします。
- [Delete] : [H.323 Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level] : セキュリティ レベル（High、Medium、Low）を選択します。
  - Low : デフォルト

    H.225 状態確認 : ディセーブル

    RAS 状態確認 : ディセーブル

    発信側の番号 : ディセーブル

    通話制限時間 : ディセーブル

    RTP 準拠 : 適用強制しない
  - Medium

    H.225 状態確認 : イネーブル

    RAS 状態確認 : イネーブル

    発信側の番号 : ディセーブル

    通話制限時間 : ディセーブル

    RTP 準拠 : 適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用 : しない
  - High

    H.225 状態確認 : イネーブル

    RAS 状態確認 : イネーブル

    発信側の番号 : イネーブル

    通話制限時間 : 1:00:00

    RTP 準拠 : 適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用 : する
  - [Phone Number Filtering] : [Phone Number Filtering] ダイアログボックスが開き、電話番号フィルタを設定できます。
  - [Customize] : [Add/Edit H.323 Policy Map] ダイアログボックスを開き、追加の設定を行います。
  - [Default Level] : セキュリティ レベルをデフォルトの Medium レベルに戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Phone Number Filtering

[Phone Number Filtering] ダイアログボックスでは、電話番号のフィルタを設定できます。

フィールド

- [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
- [Criterion]：インスペクションの基準を示します。
- [Value]：インスペクションで照合する値を示します。
- [Action]：照合条件が一致したときのアクションを示します。
- [Log]：ログの状態を示します。
- [Add]：[Add Phone Number Filter] ダイアログボックスが開き、電話番号のフィルタを追加できます。
- [Edit]：[Edit Phone Number Filter] ダイアログボックスが開き、電話番号を編集できます。
- [Delete]：電話番号のフィルタを削除します。
- [Move Up]：エントリをリストの上に移動します。
- [Move Down]：エントリをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit H.323 Policy Map（セキュリティ レベル）

[Add/Edit H.323 Policy Map] ペインでは、H.323 アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name] : H.323 マップの追加時に H.323 マップの名前を入力します。H.323 マップの編集時には、事前に設定した H.323 マップの名前が表示されます。
- [Description] : H323 マップの説明を 200 文字以内で入力します。
- [Security Level] : セキュリティ レベル（High、Medium、Low）を選択します。
  - Low : デフォルト

    H.225 状態確認 : ディセーブル

    RAS 状態確認 : ディセーブル

    発信側の番号 : ディセーブル

    通話制限時間 : ディセーブル

    RTP 準拠 : 適用強制しない
  - Medium

    H.225 状態確認 : イネーブル

    RAS 状態確認 : イネーブル

    発信側の番号 : ディセーブル

    通話制限時間 : ディセーブル

    RTP 準拠 : 適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用 : しない
  - High

    H.225 状態確認 : イネーブル

    RAS 状態確認 : イネーブル

    発信側の番号 : イネーブル

    通話制限時間 : 1:00:00

    RTP 準拠 : 適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用 : する
  - [Phone Number Filtering] : [Phone Number Filtering] ダイアログボックスが開き、電話番号のフィルタを設定できます。
  - [Default Level] : セキュリティ レベルをデフォルトに戻します。
- [Details] : 詳細な設定を行うための [State Checking] タブ、[Call Attributes] タブ、[Tunneling and Protocol Conformance] タブ、[HSI Group Parameters] タブ、および [Inspections] タブを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit H.323 Policy Map（詳細）

[Add/Edit H.323 Policy Map] ペインでは、H.323 アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：H.323 マップの追加時に H.323 マップの名前を入力します。H.323 マップの編集時には、事前に設定した H.323 マップの名前が表示されます。
- [Description]：H.323 マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルと電話番号フィルタリング設定を表示します。
- [State Checking]：このタブで H.323 インスペクション マップの状態確認パラメータを設定します。
  - [Check state transition of H.225 messages]：H.323 の状態確認を H.225 メッセージに適用します。
  - [Check state transition of RAS messages]：H.323 の状態確認を RAS メッセージに適用します。
- [Call Attributes]：このタブで H.323 インスペクション マップのコール属性パラメータを設定します。
  - [Enforce call duration limit]：通話を一定の時間で制限します。

    [Call Duration Limit]：通話制限時間（hh:mm:ss）。
  - [Enforce presence of calling and called party numbers]：通話設定時に、強制的に発信側の番号を送信します。
- [Tunneling and Protocol Conformance]：このタブで H.323 インスペクション マップのトンネリングとプロトコル準拠パラメータを設定します。
  - [Check for H.245 tunneling]：H.245 のトンネリングを許可します。

    [Action]：Drop connection または Log。
  - [Check RTP packets for protocol conformance]：ピンホールの RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    [Limit payload to audio or video, based on the signaling exchange]：ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- [HSI Group Parameters]：このタブで HSI グループを設定します。
  - [HSI Group ID]：HSI グループの ID を示します。
  - [IP Address]：HSI グループの IP アドレスを示します。
  - [Endpoints]：HSI グループのエンドポイントを示します。
  - [Add]：[Add HSI Group] ダイアログボックスが開き、HSI グループを追加できます。
  - [Edit]：[Edit HSI Group] ダイアログボックスが開き、HSI グループを編集できます。
  - [Delete]：HSI グループを削除します。
- [Inspections]：このタブで H.323 インスペクションのコンフィギュレーションを表示して、追加や編集ができます。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：H.323 インスペクションの基準を示します。
  - [Value]：H.323 インスペクションで照合する値を示します。

- [Action]：照合条件が一致したときのアクションを示します。
- [Log]：ログの状態を示します。
- [Add]：[Add H.323 Inspect] ダイアログボックスが開き、H.323 インスペクションを追加できます。
- [Edit]：[Edit H.323 Inspect] ダイアログボックスが開き、H.323 インスペクションを編集できます。
- [Delete]：H.323 インスペクションを削除します。
- [Move Up]：インスペクションをリストの上に移動します。
- [Move Down]：インスペクションをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HSI Group

[Add/Edit HSI Group] ダイアログボックスでは、HSI グループを設定できます。

フィールド

- [Group ID]：HSI のグループ ID を入力します。
- [IP Address]：HSI の IP アドレスを入力します。
- [Endpoints]：エンドポイントの IP アドレスとインターフェイスを設定します。
  - [IP Address]：エンドポイントの IP アドレスを入力します。
  - [Interface]：エンドポイントのインターフェイスを指定します。
- [Add]：定義された HSI グループを追加します。
- [Delete]：選択した HSI グループを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit H.323 Map

[Add/Edit H.323 Inspect] ダイアログボックスでは、H.323 インスペクション マップの照合基準と値を定義できます。

フィールド

- [Single Match]：H.323 インスペクションに照合文が 1 つだけの場合に指定します。
- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：H.323 トラフィックに適用する照合基準を指定します。
  - [Called Party]：受信側を照合します。
  - [Calling Party]：発信元を照合します。
  - [Media Type]：メディア タイプを照合します。
- [Called Party Criterion Values]：H.323 受信側の照合方法を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Calling Party Criterion Values]：H.323 発信元の照合方法を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Media Type Criterion Values]：照合するメディア タイプを指定します。
  - [Audio]：音声タイプを照合します。
  - [Video]：ビデオ タイプを照合します。
  - [Data]：データ タイプを照合します。
- [Multiple Matches]：H.323 インスペクションの複数の照合文を指定します。
  - [H323 Traffic Class]：H.323 トラフィック クラスを照合します。
  - [Manage]：[Manage H.323 Class Maps] ダイアログボックスが開き、H.323 クラス マップの追加、編集、削除ができます。
- [Action]：Drop Packet、Drop Connection、または Reset。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

HTTP Inspect Map

[HTTP] ペインでは、HTTP アプリケーションの事前に設定されたインスペクション マップを表示できます。HTTP マップでは、HTTP アプリケーション インスペクションのデフォルト設定値を変更できます。

HTTP アプリケーション インスペクションで HTTP のヘッダーと本文をスキャンし、さまざまなデータ チェックができます。これらのチェックで、HTTP 構築、コンテンツ タイプ、トンネル プロトコル、メッセージ プロトコルなどがセキュリティ アプライアンスを通過することを防止します。

HTTP アプリケーション インスペクションでトンネル アプリケーションと ASCII 以外の文字を含む HTTP 要求や応答をブロックして、悪意のあるコンテンツが Web サーバに到達することを防ぎます。HTTP 要求や応答ヘッダーのさまざまな要素のサイズ制限、URL のブロッキング、HTTP サーバ ヘッダー タイプのスプーフィングもサポートされています。

フィールド

- [HTTP Inspect Maps] : 定義されている HTTP インスペクション マップを一覧表示するテーブルです。
- [Add] : 新しい HTTP インスペクション マップを設定します。HTTP インスペクション マップを編集するには、[HTTP Inspect Maps] テーブルで HTTP のエントリを選択し、[Customize] をクリックします。
- [Delete] : [HTTP Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level] : セキュリティ レベル（High、Medium、Low）を選択します。
  - Low : デフォルト

    プロトコル違反時のアクション : Drop connection

    安全でない方式の接続ドロップ : ディセーブル

    要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ : ディセーブル

    URI フィルタリング : 設定しない

    高度なインスペクション : 設定しない
  - Medium

    プロトコル違反時のアクション : Drop connection

    安全でない方式の接続ドロップ : GET、HEAD、POST だけを許可

    要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ : ディセーブル

    URI フィルタリング : 設定しない

    高度なインスペクション : 設定しない
  - High

    プロトコル違反時のアクション : Drop Connection と Log

安全でない方式の接続ドロップ：GET、HEAD だけを許可

要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：イネーブル

URI フィルタリング：設定しない

高度なインスペクション：設定しない

- [URI Filtering]：[URI Filtering] ダイアログボックスが開き、URI フィルタを設定できます。
- [Customize]：[Edit HTTP Policy Map] ダイアログボックスを開き、追加の設定を行います。
- [Default Level]：セキュリティ レベルをデフォルトの Medium レベルに戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

URI Filtering

[URI Filtering] ダイアログボックスでは、URI フィルタを設定できます。

フィールド

- [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
- [Criterion]：インスペクションの基準を示します。
- [Value]：インスペクションで照合する値を示します。
- [Action]：照合条件が一致したときのアクションを示します。
- [Log]：ログの状態を示します。
- [Add]：[Add URI Filtering] ダイアログボックスが開き、URI フィルタを追加できます。
- [Edit]：[Edit URI Filtering] ダイアログボックスが開き、URI フィルタを編集できます。
- [Delete]：URI フィルタを削除します。
- [Move Up]：エントリをリストの上に移動します。
- [Move Down]：エントリをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Policy Map（セキュリティ レベル）

[Add/Edit HTTP Policy Map] ペインでは、HTTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：HTTP マップの追加時に HTTP マップの名前を入力します。HTTP マップの編集時には、事前に設定した HTTP マップの名前が表示されます。
- [Description]：HTTP マップの説明を 200 文字以内で入力します。
- [Security Level]：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    プロトコル違反時のアクション：Drop connection

    安全でない方式の接続ドロップ：ディセーブル

    要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：ディセーブル

    URI フィルタリング：設定しない

    高度なインスペクション：設定しない
  - Medium

    プロトコル違反時のアクション：Drop connection

    安全でない方式の接続ドロップ：GET、HEAD、POST だけを許可

    要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：ディセーブル

    URI フィルタリング：設定しない

    高度なインスペクション：設定しない
  - High

    プロトコル違反時のアクション：Drop Connection と Log

    安全でない方式の接続ドロップ：GET、HEAD だけを許可

    要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：イネーブル

    URI フィルタリング：設定しない

    高度なインスペクション：設定しない
  - [URI Filtering]：[URI Filtering] ダイアログボックスが開き、URI フィルタを設定します。
  - [Default Level]：セキュリティ レベルをデフォルトに戻します。
- [Details]：詳細な設定を行うための [Parameters] タブと [Inspections] タブを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Policy Map（詳細）

[Add/Edit HTTP Policy Map] ペインでは、HTTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：HTTP マップの追加時に HTTP マップの名前を入力します。HTTP マップの編集時には、事前に設定した HTTP マップの名前が表示されます。
- [Description]：HTTP マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルと URI フィルタリング設定を表示します。
- [Parameters]：このタブで HTTP インスペクション マップのパラメータを設定します。
  - [Check for protocol violations]：HTTP プロトコル違反の有無をチェックします。

    [Action]：Drop Connection、Reset、Log。

    [Log]：イネーブルまたはディセーブルにします。
  - [Spoof server string]：サーバの HTTP ヘッダーの値を指定の文字列で置き換えます。

    [Spoof String]：サーバのヘッダー フィールドと置き換える文字列を入力します。最大 82 文字まで入力できます。
  - [Body Match Maximum]：HTTP メッセージの本文照合時に検索される、最大文字数です。デフォルトは 200 バイトです。大きな値を指定すると、パフォーマンスに大きな影響を与えます。
- [Inspections]：このタブで HTTP インスペクションのコンフィギュレーションを表示して、追加や編集ができます。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：HTTP インスペクションの基準を示します。
  - [Value]：HTTP インスペクションで照合する値を示します。
  - [Action]：照合条件が一致したときのアクションを示します。
  - [Log]：ログの状態を示します。
  - [Add]：[Add HTTP Inspect] ダイアログボックスが開き、HTTP インスペクションを追加できます。
  - [Edit]：[Edit HTTP Inspect] ダイアログボックスが開き、HTTP インスペクションを編集できます。
  - [Delete]：HTTP インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。
  - [Move Down]：インスペクションをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Map

[Add/Edit HTTP Inspect] ダイアログボックスでは、HTTP インスペクション マップの照合基準と値を定義できます。

フィールド

- [Single Match]：HTTP インスペクションに照合文が 1 つだけの場合に指定します。
- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：HTTP トラフィックに適用する照合基準を指定します。
  - [Request/Response Content Type Mismatch]：応答のコンテンツ タイプが要求の accept フィールドの MIME タイプの 1 つと一致する必要があることを指定します。
  - [Request Arguments]：要求の引数に正規表現照合を適用します。

    [Regular Expression]：照合する定義された正規表現を一覧表示します。

    [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

    [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

    [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
  - [Request Body Length]：要求の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

    [Greater Than Length]：要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。
  - [Request Body]：要求の本文に正規表現照合を適用します。

    [Regular Expression]：照合する定義された正規表現を一覧表示します。

    [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

    [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

    [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
  - [Request Header Field Count]：要求ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

    [Predefined]：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、

content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

[Regular Expression]：照合する定義された正規表現を一覧表示します。

[Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

[Greater Than Count]：ヘッダー フィールド数の最大値を入力します。

- [Request Header Field Length]：要求ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  [Predefined]：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Greater Than Length]：要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- [Request Header Field]：要求のヘッダーに正規表現照合を適用します。

  [Predefined]：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

  [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。

- [Request Header Count]：要求ヘッダー数が最大値の場合、正規表現で照合します。

  [Greater Than Count]：ヘッダー数の最大値を入力します。

- [Request Header Length]：要求ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

  [Greater Than Length]：ヘッダーの長さをバイト単位で入力します。

- [Request Header non-ASCII]：要求ヘッダーに含まれる ASCII 以外の文字を照合します。
- [Request Method]：要求の方式を正規表現で照合します。

[Method]：照合する要求方式を次の中から指定します。bcopy、bdelete、bmove、bpropfind、bproppatch、connect、copy、delete、edit、get、getattribute、getattributenames、getproperties、head、index、lock、mkcol、mkdir、move、notify、options、poll、post、propfind、proppatch、put、revadd、revlabel、revlog、revnum、save、search、setattribute、startrev、stoprev、subscribe、trace、unedit、unlock、unsubscribe。

[Regular Expression]：正規表現の照合方法を指定します。

[Regular Expression]：照合する定義された正規表現を一覧表示します。

[Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

[Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

[Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。

- [Request URI Length]：要求の URI が指定したバイト数より長い場合、正規表現で照合します。

  [Greater Than Length]：URI の長さをバイト単位で入力します。

- [Request URI]：要求の URI に正規表現照合を適用します。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

  [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。

- [Response Body]：要求の本文を regex で照合します。

  [ActiveX]：ActiveX の照合方法を指定します。

  [Java Applet]：Java アプレットの照合方法を指定します。

  [Regular Expression]：正規表現の照合方法を指定します。

  [Regular Expression]：照合する定義された正規表現を一覧表示します。

  [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

  [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。

- [Response Body Length]：応答の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  [Greater Than Length]：応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- [Response Header Field Count]：応答ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

  [Predefined]：応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。

[Regular Expression]：照合する定義された正規表現を一覧表示します。

[Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

[Greater Than Count]：ヘッダー フィールド数の最大値を入力します。

– [Response Header Field Length]：応答ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

[Predefined]：応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。

[Regular Expression]：照合する定義された正規表現を一覧表示します。

[Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

[Greater Than Length]：応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

– [Response Header Field]：応答のヘッダーに正規表現照合を適用します。

[Predefined]：応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。

[Regular Expression]：照合する定義された正規表現を一覧表示します。

[Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

[Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

[Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。

– [Response Header Count]：応答ヘッダー数が最大値の場合、正規表現で照合します。

[Greater Than Count]：ヘッダー数の最大値を入力します。

– [Response Header Length]：応答ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

[Greater Than Length]：ヘッダーの長さをバイト単位で入力します。

– [Response Header non-ASCII]：応答ヘッダーに含まれる ASCII 以外の文字を照合します。

– [Response Status Line]：ステータス行を正規表現で照合します。

[Regular Expression]：照合する定義された正規表現を一覧表示します。

[Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

[Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

[Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。

- [Multiple Matches]：HTTP インスペクションの複数の照合文を指定します。
  – [H323 Traffic Class]：HTTP トラフィック クラスを照合します。

  - [Manage] : [Manage HTTP Class Maps] ダイアログボックスが開き、HTTP クラス マップの追加、編集、削除ができます。
- [Action] : Drop connection、Reset、または Log。
- [Log] : イネーブルまたはディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Instant Messaging (IM) Inspect Map

[IM] ペインでは、インスタント メッセージ（IM）アプリケーションの事前に設定されたインスペクション マップを表示できます。インスタント メッセージ（IM）マップでは、インスタント メッセージ（IM）アプリケーション インスペクションのデフォルト設定値を変更できます。

インスタント メッセージ（IM）アプリケーション インスペクションで、ネットワーク アクセスの使用量を詳細に制御できます。また、機密情報の漏洩やその他の攻撃からネットワークを守ります。正規表現データベースのさまざまな検索パターンを使って、インスタント メッセージ（IM）をフィルタできます。フローが認識されない場合は、syslog が生成されます。

スコープを限定するには、アクセス リストから検査するトラフィック ストリームを指定します。UDP メッセージの場合、対応する UDP ポート番号も設定できます。Yahoo!Messenger および MSN Messenger のインスタント メッセージのインスペクションもサポートされています。

フィールド

- [Name] : インスペクション マップの名前を 40 文字以内で入力します。
- [Description] : インスペクション マップの説明を 200 文字以内で入力します。
- [IM Inspect Maps] : 定義されている IM インスペクション マップを一覧表示するテーブルです。
- [Add] : 新しい IM インスペクション マップを設定します。
- [Edit] : [IM Inspect Maps] テーブルで選択した IM のエントリを編集します。
- [Delete] : [IM Inspect Maps] テーブルで選択したインスペクション マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Instant Messaging (IM) Policy Map

[Add/Edit Instant Messaging (IM) Policy Map] ペインでは、IM アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：IM マップの追加時に IM マップの名前を入力します。IM マップの編集時には、事前に設定した IM マップの名前が表示されます。
- [Description]：IM マップの説明を 200 文字以内で入力します。
- [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
- [Criterion]：IM インスペクションの基準を示します。
- [Value]：IM インスペクションで照合する値を示します。
- [Action]：照合条件が一致したときのアクションを示します。
- [Log]：ログの状態を示します。
- [Add]：[Add IM Inspect] ダイアログボックスが開き、IM インスペクションを追加できます。
- [Edit]：[Edit IM Inspect] ダイアログボックスが開き、IM インスペクションを編集できます。
- [Delete]：IM インスペクションを削除します。
- [Move Up]：インスペクションをリストの上に移動します。
- [Move Down]：インスペクションをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IM Map

[Add/Edit IM Inspect] ダイアログボックスでは、IM インスペクション マップの照合基準と値を定義できます。

フィールド

- [Single Match]：IM インスペクションに照合文が 1 つだけの場合に指定します。
- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：IM トラフィックに適用する照合基準を指定します。
  - [Protocol]：IM プロトコルを照合します。
  - [Service]：IM サービスを照合します。

  - [Source IP Address]：送信元 IP アドレスを照合します。
  - [Destination IP Address]：宛先 IP アドレスを照合します。
  - [Version]：IM ファイル転送のサービス バージョンを照合します。
  - [Client Login Name]：IM サービスのクライアント ログイン名を照合します。
  - [Client Peer Login Name]：IM サービスのクライアントのピア ログイン名を照合します。
  - [Filename]：IM ファイル転送サービスのファイル名を照合します。
- [Protocol Criterion Values]：照合する IM プロトコルを指定します。
  - [Yahoo!Messenger]：Yahoo!Messenger のインスタント メッセージを照合します。
  - [MSN Messenger]：MSN Messenger のインスタント メッセージを照合します。
- [Service Criterion Values]：照合する IM サービスを指定します。
  - [Chat]：IM メッセージ チャット サービスを照合します。
  - [Conference]：IM コンファレンス サービスを照合します。
  - [File Transfer]：IM ファイル転送サービスを照合します。
  - [Games]：IM ゲーム サービスを照合します。
  - [Voice Chat]：IM 音声チャット サービスを照合します（Yahoo の IM は対象外です）。
  - [Web Cam]：IM Web カメラ サービスを照合します。
- [Source IP Address Criterion Values]：IM サービスで照合する送信元 IP アドレスを指定します。
  - [IP Address]：IM サービスの送信元 IP アドレスを入力します。
  - [IP Mask]：送信元 IP アドレスのマスクです。
- [Destination IP Address Criterion Values]：IM サービスで照合する宛先 IP アドレスを指定します。
  - [IP Address]：IM サービスの宛先 IP アドレスを入力します。
  - [IP Mask]：宛先 IP アドレスのマスクです。
- [Version Criterion Values]：IM ファイル転送サービスで照合するバージョンを指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Client Login Name Criterion Values]：IM サービスで照合するクライアント ログイン名を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Client Peer Login Name Criterion Values]：IM サービスで照合するクライアントのピア ログイン名を指定します。正規表現で照合します。

  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Filename Criterion Values]：IM ファイル転送サービスで照合するファイル名を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Multiple Matches]：IM インスペクションの複数の照合文を指定します。
  - [IM Traffic Class]：IM トラフィック クラスを照合します。
  - [Manage]：[Manage IM Class Maps] ダイアログボックスが開き、IM クラス マップの追加、編集、削除ができます。
- [Action]：Drop connection、Reset、または Log。
- [Log]：イネーブルまたはディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

IPSec Pass Through Inspect Map

[IPSec Pass Through] ペインでは、IPSec パススルー アプリケーションの事前に設定されたインスペクション マップを表示できます。IPSec パススルー マップでは、IPSec パススルー アプリケーション インスペクションのデフォルト設定値を変更できます。IPSec パススルー マップを使用すると、アクセス リストを参照しなくても、特定のフローを許可できます。

フィールド

- [IPSec Pass Through Inspect Maps]：定義されている IPSec パススルー インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい IPSec パススルー インスペクション マップを設定します。IPSec パススルー インスペクション マップを編集するには、[IPSec Pass Through Inspect Maps] テーブルで IPSec パススルーのエントリを選択し、[Customize] をクリックします。

- [Delete] : [IPSec Pass Through Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level] : セキュリティ レベル（High または Low）を選択します。
  - Low : デフォルト

    クライアントごとの最大 ESP フロー : 無制限

    ESP アイドル タイムアウト : 00:10:00

    クライアントごとの最大 AH フロー : 無制限

    AH アイドル タイムアウト : 00:10:00
  - High

    クライアントごとの最大 ESP フロー : 10

    ESP アイドル タイムアウト : 00:00:30

    クライアントごとの最大 AH フロー : 10

    AH アイドル タイムアウト : 00:00:30
  - [Customize] : [Add/Edit IPSec Pass Thru Policy Map] ダイアログボックスを開き、追加の設定を行います。
  - [Default Level] : セキュリティ レベルをデフォルトの Low レベルに戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IPSec Pass Thru Policy Map（セキュリティ レベル）

[Add/Edit IPSec Pass Thru Policy Map] ペインでは、IPSec パススルー アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name] : IPSec パススルー マップの追加時に IPSec パススルー マップの名前を入力します。IPSec パススルー マップの編集時には、事前に設定した IPSec パススルー マップの名前が表示されます。
- [Security Level] : セキュリティ レベル（High または Low）を選択します。
  - Low : デフォルト

    クライアントごとの最大 ESP フロー : 無制限

    ESP アイドル タイムアウト : 00:10:00

    クライアントごとの最大 AH フロー : 無制限

    AH アイドル タイムアウト : 00:10:00

- High

  クライアントごとの最大 ESP フロー：10

  ESP アイドル タイムアウト：00:00:30

  クライアントごとの最大 AH フロー：10

  AH アイドル タイムアウト：00:00:30
- [Default Level]：セキュリティ レベルをデフォルトの Low レベルに戻します。

- [Details]：追加の設定を行うパラメータを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IPSec Pass Thru Policy Map（詳細）

[Add/Edit IPSec Pass Thru Policy Map] ペインでは、IPSec パススルー アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：IPSec パススルー マップの追加時に IPSec パススルー マップの名前を入力します。IPSec パススルー マップの編集時には、事前に設定した IPSec パススルー マップの名前が表示されます。
- [Description]：IPSec パススルー インスペクション マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルを表示します。
- [Parameters]：ESP および AH パラメータを設定します。
  - [Limit ESP flows per client]：クライアントごとの ESP フローを制限します。

    [Maximum]：最大限度を指定します。
  - [Apply ESP idle timeout]：ESP アイドル タイムアウトを適用します。

    [Timeout]：タイムアウト値を指定します。
  - [Limit AH flows per client]：クライアントごとの AH フローを制限します。

    [Maximum]：最大限度を指定します。
  - [Apply AH idle timeout]：AH アイドル タイムアウトを適用します。

    [Timeout]：タイムアウト値を指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

MGCP Inspect Map

[MGCP] ペインでは、MGCP アプリケーションの事前に設定されたインスペクション マップを表示できます。MGCP マップでは、MGCP アプリケーション インスペクションのデフォルト設定値を変更できます。MGCP マップを使用して、VoIP デバイスと MGCP コール エージェント間の接続を管理できます。

フィールド

- [MGCP Inspect Maps]：定義されている MGCP インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい MGCP インスペクション マップを設定します。
- [Edit]：[MGCP Inspect Maps] テーブルで選択した MGCP のエントリを編集します。
- [Delete]：[MGCP Inspect Maps] テーブルで選択したインスペクション マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Gateways and Call Agents

[Gateways and Call Agents] ダイアログボックスでは、ゲートウェイとコール エージェントのグループをマップに設定できます。

フィールド

- [Group ID]：コール エージェント グループの ID を指定します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。ゲートウェイの IP アドレスは、1 つのグループ ID だけに関連付けできます。同じゲートウェイを別のグループ ID で使用できません。0 ～ 2147483647 の範囲の値を指定できます。
- [Criterion]：インスペクションの基準を示します。

- [Gateways] : 関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを識別します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
- [Call Agents] : コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを識別します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
- [Add] : [Add MGCP] ダイアログボックスが表示され、新規のアプリケーション インスペクション マップを定義できます。
- [Edit] : [Edit MGCP] ダイアログボックスが表示され、アプリケーション インスペクション マップ テーブルで選択したインスペクション マップを修正できます。
- [Delete] : アプリケーション インスペクション マップ テーブルで選択したインスペクション マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit MGCP Policy Map

[Add/Edit MGCP Policy Map] ペインでは、MGCP アプリケーション インスペクション マップのコマンド キュー、ゲートウェイ、およびコール エージェントの設定値を設定できます。

フィールド

- [Name] : MGCP マップの追加時に MGCP マップの名前を入力します。MGCP マップの編集時には、事前に設定した MGCP マップの名前が表示されます。
- [Description] : MGCP マップの説明を 200 文字以内で入力します。
- [Command Queue] : このタブで MGCP コマンドの許容キュー サイズを指定します。
  - [Command Queue Size] : キューに入れるコマンドの最大数を指定します。1 ～ 2147483647 の範囲の値を指定できます。
- [Gateways and Call Agents] : このタブでゲートウェイとコール エージェント グループをマップに設定します。
  - [Group ID] : コール エージェント グループの ID を指定します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。ゲートウェイの IP アドレスは、1 つのグループ ID だけに関連付けできます。同じゲートウェイを別のグループ ID で使用できません。0 ～ 2147483647 の範囲の値を指定できます。
  [Criterion] : インスペクションの基準を示します。

- [Gateways]：関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを識別します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
- [Call Agents]：コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを識別します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
- [Add]：[Add MGCP Group] ダイアログボックスが表示され、ゲートウェイとコール エージェントの新規の MGCP グループを定義できます。
- [Edit]：[Edit MGCP] ダイアログボックスが表示され、[Gateways and Call Agents] テーブルで選択した MGCP グループを修正できます。
- [Delete]：[Gateways and Call Agents] テーブルで選択した MGCP グループを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit MGCP Group

[Add/Edit MGCP Group] ダイアログボックスでは、MGCP アプリケーション インスペクションがイネーブルのときに使用される MGCP グループのコンフィギュレーションを定義できます。

フィールド

- [Group ID]：コール エージェント グループの ID を指定します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。0 ～ 2147483647 の範囲の値を指定できます。
- [Gateways] 領域
  - [Gateway to Be Added]：関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを指定します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
  - [Add]：指定した IP アドレスを IP アドレス テーブルに追加します。
  - [Delete]：選択した IP アドレスを IP アドレス テーブルから削除します。
  - [IP Address]：コール エージェント グループに設定されているゲートウェイの IP アドレスを一覧表示します。
- Call Agents

- [Call Agent to Be Added]：コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを指定します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
- [Add]：指定した IP アドレスを IP アドレス テーブルに追加します。
- [Delete]：選択した IP アドレスを IP アドレス テーブルから削除します。
- [IP Address]：コール エージェント グループに設定されているコール エージェントの IP アドレスを一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

NetBIOS Inspect Map

[NetBIOS] ペインでは、NetBIOS アプリケーションの事前に設定されたインスペクション マップを表示できます。NetBIOS マップでは、NetBIOS アプリケーション インスペクションのデフォルト設定値を変更できます。

NetBIOS アプリケーション インスペクションでは、NetBIOS ネーム サービス パケットおよび NetBIOS データグラム サービス パケットに埋め込まれている IP アドレスで NAT を実行します。また、プロトコル準拠チェックを行って、さまざまなフィールドの数や長さの整合性を確認します。

フィールド

- [NetBIOS Inspect Maps]：定義されている NetBIOS インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい NetBIOS インスペクション マップを設定します。
- [Edit]：[NetBIOS Inspect Maps] テーブルで選択した NetBIOS のエントリを編集します。
- [Delete]：[NetBIOS Inspect Maps] テーブルで選択したインスペクション マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit NetBIOS Policy Map

[Add/Edit NetBIOS Policy Map] ペインでは、NetBIOS アプリケーション インスペクション マップのプロトコル違反の設定値を設定できます。

フィールド

- [Name]：NetBIOS マップの追加時に NetBIOS マップの名前を入力します。NetBIOS マップの編集時には、事前に設定した NetBIOS マップの名前が表示されます。
- [Description]：NetBIOS マップの説明を 200 文字以内で入力します。
- [Check for protocol violations]：プロトコル違反の有無をチェックして、指定したアクションを実行します。
  - [Action]：Drop packet または Log。
  - [Log]：イネーブルまたはディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

RTSP Inspect Map

[RTSP] ペインでは、RTSP アプリケーションの事前に設定されたインスペクション マップを表示できます。RTSP マップでは、RTSP アプリケーション インスペクションのデフォルト設定値を変更できます。RTSP マップを使用して、RTSP トラフィックを保護できます。

フィールド

- [RTSP Inspect Maps]：定義されている RTSP インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい RTSP インスペクション マップを設定します。
- [Edit]：[RTSP Inspect Maps] テーブルで選択した RTSP のエントリを編集します。
- [Delete]：[RTSP Inspect Maps] テーブルで選択したインスペクション マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit RTSP Policy Map

[Add/Edit RTSP Policy Map] ペインでは、RTSP アプリケーション インスペクション マップのパラメータとインスペクション設定値を設定できます。

フィールド

- [Name]：RTSP マップの追加時に RTSP マップの名前を入力します。RTSP マップの編集時には、事前に設定した RTSP マップの名前が表示されます。
- [Description]：RTSP マップの説明を 200 文字以内で入力します。
- [Parameters]：このタブで、メディア ポート ネゴシエーション中の予約済みポートの使用を制限し、URL の長さ制限を設定できます。
  - [Enforce Reserve Port Protection]：メディア ポート ネゴシエーション中の予約済みポートの使用を制限できます。
  - [Maximum URL Length]：メッセージで許容される URL の最大長を指定します。6000 以下の値を指定します。
- [Inspections]：このタブで RTSP インスペクションのコンフィギュレーションを表示して、追加や編集ができます。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：RTSP インスペクションの基準を示します。
  - [Value]：RTSP インスペクションで照合する値を示します。
  - [Action]：照合条件が一致したときのアクションを示します。
  - [Log]：ログの状態を示します。
  - [Add]：[Add RTSP Inspect] ダイアログボックスが開き、RTSP インスペクションを追加できます。
  - [Edit]：[Edit RTSP Inspect] ダイアログボックスが開き、RTSP インスペクションを編集できます。
  - [Delete]：RTSP インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。
  - [Move Down]：インスペクションをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit RTSP Inspect

[Add/Edit RTSP Inspect] ダイアログボックスでは、RTSP インスペクション マップの照合基準、値、およびアクションを定義できます。

フィールド

- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

- [Criterion]：RTSP トラフィックに適用する照合基準を指定します。
  - [URL Filter]：URL フィルタリングを照合します。
  - [Request Method]：RTSP の要求方式を照合します。
- [URL Filter Criterion Values]：URL フィルタリングを照合するために指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [URL Filter Actions]：プライマリ アクションおよびログを設定します。
  - [Action]：Drop connection または Log。
  - [Log]：イネーブルまたはディセーブルにします。
- [Request Method Criterion Values]：照合する RTSP 要求方式を指定します。
  - [Request Method]：要求方式を announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameters、teardown のいずれかから指定します。
- [Request Method Actions]：プライマリ アクションを設定します。
  - [Action]：Limit rate (pps)。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SCCP (Skinny) Inspect Map

[SCCP (Skinny)] ペインでは、SCCP（Skinny）アプリケーションの事前に設定されたインスペクション マップを表示できます。SCCP（Skinny）マップでは、SCCP（Skinny）アプリケーション インスペクションのデフォルト設定値を変更できます。

Skinny アプリケーション インスペクションでは、パケット データ、ピンホールの動的開放に埋め込まれている IP アドレスとポート番号を変換します。また、追加のプロトコル準拠チェックと基本的なステート トラッキングも行います。

フィールド

- [SCCP (Skinny) Inspect Maps]：定義されている SCCP (Skinny) インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい SCCP（Skinny）インスペクション マップを設定します。SCCP (Skinny) インスペクション マップを編集するには、[SCCP (Skinny) Inspect Maps] テーブルで SCCP (Skinny) のエントリを選択し、[Customize] をクリックします。
- [Delete]：[SCCP (Skinny) Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level]：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    登録：適用強制しない

    メッセージの最大 ID：0x181

    プレフィックスの長さの最小値：4

    メディア タイムアウト：00:05:00

    シグナリング タイムアウト：01:00:00

    RTP 準拠：適用強制しない
  - Medium

    登録：適用強制しない

    メッセージの最大 ID：0x141

    プレフィックスの長さの最小値：4

    メディア タイムアウト：00:01:00

    シグナリング タイムアウト：00:05:00

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：しない
  - High

    登録：適用強制する

    メッセージの最大 ID：0x141

    プレフィックスの長さの最小値：4

    プレフィックスの長さの最大値：65536

    メディア タイムアウト：00:01:00

    シグナリング タイムアウト：00:05:00

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：する
  - [Message ID Filtering]：[Messaging ID Filtering] ダイアログボックスが開き、メッセージ ID フィルタを設定できます。
  - [Customize]：[Add/Edit SCCP (Skinny) Policy Map] ダイアログボックスを開き、追加の設定を行います。
  - [Default Level]：セキュリティ レベルをデフォルトの Low レベルに戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Message ID Filtering

[Message ID Filtering] ダイアログボックスでは、メッセージ ID のフィルタを設定できます。

フィールド

- [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
- [Criterion]：インスペクションの基準を示します。
- [Value]：インスペクションで照合する値を示します。
- [Action]：照合条件が一致したときのアクションを示します。
- [Log]：ログの状態を示します。
- [Add]：[Add Message ID Filtering] ダイアログボックスが開き、メッセージ ID のフィルタを追加できます。
- [Edit]：[Edit Message ID Filtering] ダイアログボックスが開き、メッセージ ID のフィルタを編集できます。
- [Delete]：メッセージ ID のフィルタを削除します。
- [Move Up]：エントリをリストの上に移動します。
- [Move Down]：エントリをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SCCP (Skinny) Policy Map（セキュリティ レベル）

[Add/Edit SCCP (Skinny) Policy Map] ペインでは、SCCP（Skinny）アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：SCCP（Skinny）マップの追加時に SCCP（Skinny）マップの名前を入力します。SCCP（Skinny）マップの編集時には、事前に設定した SCCP（Skinny）マップの名前が表示されます。
- [Description]：SCCP（Skinny）マップの説明を 200 文字以内で入力します。
- [Security Level]：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    登録：適用強制しない

    メッセージの最大 ID：0x181

    プレフィックスの長さの最小値：4

    メディア タイムアウト：00:05:00

    シグナリング タイムアウト：01:00:00

    RTP 準拠：適用強制しない
  - Medium

    登録：適用強制しない

    メッセージの最大 ID：0x141

    プレフィックスの長さの最小値：4

    メディア タイムアウト：00:01:00

    シグナリング タイムアウト：00:05:00

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：しない
  - High

    登録：適用強制する

    メッセージの最大 ID：0x141

    プレフィックスの長さの最小値：4

    プレフィックスの長さの最大値：65536

    メディア タイムアウト：00:01:00

    シグナリング タイムアウト：00:05:00

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：する
  - [Message ID Filtering]：[Messaging ID Filtering] ダイアログボックスが開き、メッセージ ID フィルタを設定できます。
  - [Default Level]：セキュリティ レベルをデフォルトに戻します。
- [Details]：追加の設定を行うパラメータ、RTP 準拠、メッセージ ID のフィルタリング設定値を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SCCP (Skinny) Policy Map（詳細）

[Add/Edit SCCP (Skinny) Policy Map] ペインでは、SCCP（Skinny）アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：SCCP（Skinny）マップの追加時に SCCP（Skinny）マップの名前を入力します。SCCP（Skinny）マップの編集時には、事前に設定した SCCP（Skinny）マップの名前が表示されます。
- [Description]：DNS マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルとメッセージ ID のフィルタリング設定を表示します。
- [Parameters]：このタブで SCCP（Skinny）のパラメータを設定します。
  - [Enforce endpoint registration]：Skinny エンドポイントを登録してから通話を受発信します。

    [Maximum Message ID]：SCCP メッセージ ID に使用できる最大値を指定します。
  - [SCCP Prefix Length]：Skinny メッセージのプレフィックスの長さを指定します。

    [Minimum Prefix Length]：SCCP プレフィックスの長さの許容最小値を指定します。

    [Maximum Prefix Length]：SCCP プレフィックスの長さの許容最大値を指定します。
  - [Media Timeout]：メディア接続時のタイムアウト値を指定します。
  - [Signaling Timeout]：シグナリング接続時のタイムアウト値を指定します。
- [RTP Conformance]：このタブで SCCP（Skinny）の RTP 準拠を設定します。
  - [Check RTP packets for protocol conformance]：ピンホールをフローする RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    [Limit payload to audio or video, based on the signaling exchange]：ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- [Message ID Filtering]：このタブで SCCP（Skinny）のメッセージ ID フィルタリングを設定します。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：インスペクションの基準を示します。
  - [Value]：インスペクションで照合する値を示します。
  - [Action]：照合条件が一致したときのアクションを示します。
  - [Log]：ログの状態を示します。
  - [Add]：[Add Message ID Filtering] ダイアログボックスが開き、メッセージ ID のフィルタを追加できます。

- [Edit]：[Edit Message ID Filtering] ダイアログボックスが開き、メッセージ ID のフィルタを編集できます。
- [Delete]：メッセージ ID のフィルタを削除します。
- [Move Up]：エントリをリストの上に移動します。
- [Move Down]：エントリをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Message ID Filter

[Add Message ID Filter] ダイアログボックスでは、メッセージ ID のフィルタを設定できます。

フィールド

- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：SCCP (Skinny) トラフィックに適用する照合基準を指定します。
  - [Message ID]：指定したメッセージ ID を照合します。

    [Message ID]：SCCP メッセージ ID に使用できる最大値を指定します。
  - [Message ID Range]：指定範囲のメッセージ ID を照合します。

    [Lower Message ID]：SCCP メッセージ ID に使用できる下限値を指定します。

    [Upper Message ID]：SCCP メッセージ ID に使用できる上限値を指定します。
- [Action]：Drop packet。
- [Log]：イネーブルまたはディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SIP Inspect Map

[SIP] ペインでは、SIP アプリケーションの事前に設定されたインスペクション マップを表示できます。SIP マップでは、SIP アプリケーション インスペクションのデフォルト設定値を変更できます。

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタント メッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。

SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーション セキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

フィールド

- [SIP Inspect Maps]：定義されている SIP インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい SIP インスペクション マップを設定します。SIP インスペクション マップを編集するには、[SIP Inspect Maps] テーブルで SIP のエントリを選択し、[Customize] をクリックします。
- [Delete]：[SIP Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level]：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

    SIP トラフィック以外の SIP ポート使用：許可

    サーバとエンドポイントの IP アドレスを非表示：ディセーブル

    ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル

    1 以上の宛先ホップ カウントを保証：イネーブル

    RTP 準拠：適用強制しない

    SIP 準拠：ステート チェックとヘッダー検証を実行しない
  - Medium

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

    SIP トラフィック以外の SIP ポート使用：許可

    サーバとエンドポイントの IP アドレスを非表示：ディセーブル

    ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル

    1 以上の宛先ホップ カウントを保証：イネーブル

    RTP 準拠：適用強制する

    ペイロードを音声やビデオに限定してシグナリング交換を適用：しない

    SIP 準拠：ステート チェックで失敗したパケットをドロップ
  - High

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

    SIP トラフィック以外の SIP ポート使用：禁止

    サーバとエンドポイントの IP アドレスを非表示：ディセーブル

    ソフトウェアのバージョンと SIP 以外の URI をマスク：イネーブル

    1 以上の宛先ホップ カウントを保証：イネーブル

RTP 準拠：適用強制する

ペイロードを音声やビデオに限定してシグナリング交換を適用：する

SIP 準拠：ステート チェックとヘッダー検証で失敗したパケットをドロップ

- [Customize]：[Add/Edit SIP Policy Map] ダイアログボックスを開き、追加の設定を行います。
- [Default Level]：セキュリティ レベルをデフォルトの Low レベルに戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SIP Policy Map（セキュリティ レベル）

[Add/Edit SIP Policy Map] ペインでは、SIP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：SIP の追加時に SIP マップの名前を入力します。SIP マップの編集時には、事前に設定した SIP マップの名前が表示されます。
- [Description]：SIP マップの説明を 200 文字以内で入力します。
- [Security Level]：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

    SIP トラフィック以外の SIP ポート使用：許可

    サーバとエンドポイントの IP アドレスを非表示：ディセーブル

    ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル

    1 以上の宛先ホップ カウントを保証：イネーブル

    RTP 準拠：適用強制しない

    SIP 準拠：ステート チェックとヘッダー検証を実行しない
  - Medium

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

    SIP トラフィック以外の SIP ポート使用：許可

    サーバとエンドポイントの IP アドレスを非表示：ディセーブル

    ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル

    1 以上の宛先ホップ カウントを保証：イネーブル

    RTP 準拠：適用強制する

ペイロードを音声やビデオに限定してシグナリング交換を適用：しない

SIP 準拠：ステート チェックで失敗したパケットをドロップ

– High

SIP インスタント メッセージ（IM）の拡張機能：イネーブル

SIP トラフィック以外の SIP ポート使用：禁止

サーバとエンドポイントの IP アドレスを非表示：ディセーブル

ソフトウェアのバージョンと SIP 以外の URI をマスク：イネーブル

1 以上の宛先ホップ カウントを保証：イネーブル

RTP 準拠：適用強制する

ペイロードを音声やビデオに限定してシグナリング交換を適用：する

SIP 準拠：ステート チェックとヘッダー検証で失敗したパケットをドロップ

– [Default Level]：セキュリティ レベルをデフォルトに戻します。

- [Details]：追加の設定を行うフィルタリング、IP アドレスのプライバシー、ホップ カウント、RTP 準拠、SIP 準拠、フィールド マスク、およびインスペクションの設定値を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SIP Policy Map（詳細）

[Add/Edit SIP Policy Map] ペインでは、SIP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：SIP の追加時に SIP マップの名前を入力します。SIP マップの編集時には、事前に設定した SIP マップの名前が表示されます。
- [Description]：SIP マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルを表示します。
- [Filtering]：このタブで SIP のフィルタリングを設定します。
  – [Enable SIP instant messaging (IM) extensions]：インスタント メッセージの拡張機能をイネーブルにします。デフォルトはイネーブルです。
  – [Permit non-SIP traffic on SIP port]：SIP トラフィック以外に SIP ポートの使用を許可します。デフォルトは許可です。
- [IP Address Privacy]：このタブで SIP の IP アドレスのプライバシーを設定します。
  – [Hide server's and endpoint's IP addresses]：IP アドレスのプライバシーをイネーブルにします。デフォルトでは、ディセーブルです。

- [Hop Count]：このタブで SIP のホップ カウントを設定します。
  - [Ensure that number of hops to destination is greater than 0]：Max-Forwards ヘッダーの値が 0 かどうかのチェックをイネーブルにします。

    [Action]：Drop packet、Drop Connection、Reset、または Log。

    [Log]：イネーブルまたはディセーブルにします。
- [RTP Conformance]：このタブで SIP の RTP 準拠を設定します。
  - [Check RTP packets for protocol conformance]：ピンホールをフローする RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    [Limit payload to audio or video, based on the signaling exchange]：ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- [SIP Conformance]：このタブで SIP の SIP 準拠を設定します。
  - [Enable state transition checking]：SIP のステート チェックをイネーブルにします。

    [Action]：Drop packet、Drop Connection、Reset、または Log。

    [Log]：イネーブルまたはディセーブルにします。
  - [Enable strict validation of header fields]：SIP ヘッダー フィールドの検証をイネーブルにします。

    [Action]：Drop packet、Drop Connection、Reset、または Log。

    [Log]：イネーブルまたはディセーブルにします。
- [Field Masking]：このタブで SIP のフィールド マスクを設定します。
  - [Inspect non-SIP URIs]：Alert-Info と Call-Info ヘッダーに含まれる SIP 以外の URI インスペクションをイネーブルにします。

    [Action]：Mask または Log。

    [Log]：イネーブルまたはディセーブルにします。
  - [Inspect server's and endpoint's software version]：User-Agent と Server ヘッダーに含まれる SIP エンドポイントのソフトウェア バージョンをインスペクションします。

    [Action]：Mask または Log。

    [Log]：イネーブルまたはディセーブルにします。
- [Inspections]：このタブで SIP インスペクションのコンフィギュレーションを表示して、追加や編集ができます。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：SIP インスペクションの基準を示します。
  - [Value]：SIP インスペクションで照合する値を示します。
  - [Action]：照合条件が一致したときのアクションを示します。
  - [Log]：ログの状態を示します。
  - [Add]：[Add SIP Inspect] ダイアログボックスが開き、SIP インスペクションを追加できます。
  - [Edit]：[Edit SIP Inspect] ダイアログボックスが開き、SIP インスペクションを編集できます。
  - [Delete]：SIP インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。
  - [Move Down]：インスペクションをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SIP Inspect

[Add/Edit SIP Inspect] ダイアログボックスでは、SIP インスペクション マップの照合基準と値を定義できます。

フィールド

- [Single Match]：SIP インスペクションに照合文が 1 つだけの場合に指定します。
- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：SIP トラフィックに適用する照合基準を指定します。
  - [Called Party]：To ヘッダーに指定された受信側を照合します。
  - [Calling Party]：From ヘッダーに指定された発信元を照合します。
  - [Content Length]：ヘッダーのコンテンツの長さを照合します。
  - [Content Type]：ヘッダーのコンテンツ タイプを照合します。
  - [IM Subscriber]：SIP IM の加入者を照合します。
  - [Message Path]：SIP の Via ヘッダーを照合します。
  - [Request Method]：SIP の要求方式を照合します。
  - [Third-Party Registration]：サード パーティの登録要求者を照合します。
  - [URI Length]：SIP ヘッダーの URI を照合します。
- [Called Party Criterion Values]：照合する受信側を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Calling Party Criterion Values]：照合する発信元を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [Content Length Criterion Values]：指定値より長い SIP コンテンツ ヘッダーを照合します。
  - [Greater Than Length]：ヘッダーの長さをバイト単位で入力します。
- [Content Type Criterion Values]：照合する SIP コンテンツ ヘッダーのタイプを指定します。
  - [SDP]：SDP タイプの SIP コンテンツ ヘッダーを照合します。
  - [Regular Expression]：正規表現を照合します。

    [Regular Expression]：照合する定義された正規表現を一覧表示します。

    [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

    [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

    [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [IM Subscriber Criterion Values]：照合する IM 登録者を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [Message Path Criterion Values]：照合する SIP の Via ヘッダーを指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [Request Method Criterion Values]：照合する SIP 要求方式を指定します。
  - [Request Method]：次の中から要求方式を指定します。ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。
- [Third-Party Registration Criterion Values]：照合するサード パーティの登録要求者を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [URI Length Criterion Values]：指定値より長い SIP ヘッダーの URI を指定して照合します。
  - [URI type]：SIP URI または TEL URI を指定して照合します。

  - [Greater Than Length]：長さをバイト単位で指定します。
- [Multiple Matches]：SIP インスペクションの複数の照合文を指定します。
  - [SIP Traffic Class]：SIP トラフィック クラスを照合します。
  - [Manage]：[Manage SIP Class Maps] ダイアログボックスが開き、SIP クラス マップの追加、編集、削除ができます。
- [Actions]：プライマリ アクションおよびログを設定します。
  - [Action]：Drop packet、Drop Connection、Reset、または Log。（注）要求方式が invite か register の場合は、Limit rate (pps) アクションを使用できます。
  - [Log]：イネーブルまたはディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SNMP Inspect Map

[SNMP] ペインでは、SNMP アプリケーションの事前に設定されたインスペクション マップを表示できます。SNMP マップでは、SNMP アプリケーション インスペクションのデフォルト設定値を変更できます。

フィールド

- [Map Name]：すでに設定されているアプリケーション インスペクション マップを一覧表示します。マップをオンにし、[Edit] をクリックして、既存のマップの表示または変更ができます。
- [Add]：新しい SNMP インスペクション マップを設定します。
- [Edit]：[SNMP Inspect Maps] テーブルで選択した SNMP のエントリを編集します。
- [Delete]：[SNMP Inspect Maps] テーブルで選択したインスペクション マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SNMP Map

[Add/Edit SNMP Map] ダイアログボックスでは、SNMP のアプリケーション インスペクションを制御する SNMP マップを新規作成できます。

フィールド

- [SNMP Map Name]：アプリケーション インスペクション マップの名前を定義します。
- [SNMP version 1]：SNMP バージョン 1 のアプリケーション インスペクションをイネーブルにします。
- [SNMP version 2 (party based)]：SNMP バージョン 2 のアプリケーション インスペクションをイネーブルにします。
- [SNMP version 2c (community based)]：SNMP バージョン 2c のアプリケーション インスペクションをイネーブルにします。
- [SNMP version 3]：SNMP バージョン 3 のアプリケーション インスペクションをイネーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 25

NAT の設定

この章では、ネットワーク アドレス変換について説明します。次の項目を取り上げます。

NAT の概要

ここでは、セキュリティ アプライアンス 上での NAT の機能について説明します。次の項目を取り上げます。

NAT の概要

アドレス変換は、パケット内の実際のアドレスを、宛先ネットワーク上でルーティング可能な、マッピングされたアドレスで置き換えます。NAT は 2 つのステップで構成されます。実際のアドレスをマッピング アドレスに変換するプロセスと、リターン トラフィック用に変換を元に戻すプロセスです。

セキュリティ アプライアンスは、NAT ルールがトラフィックに一致すると、アドレスを変換します。NAT ルールが一致しなかった場合、パケットの処理が続行されます。ただし、NAT 制御をイネーブルにしている場合は例外です。NAT 制御では、セキュリティの高いインターフェイス（内部）からセキュリティの低いインターフェイス（外部）に移動するパケットが NAT 規則と一致することが要求さ

れます。一致しない場合、パケットの処理は停止されます。セキュリティ レベルの詳細については、「デフォルトのセキュリティ レベル」（P.5-4）を参照してください。NAT 制御の詳細については、「NAT コントロール」（P.25-5）を参照してください。

（注）　このマニュアルでは、すべてのタイプの変換を NAT と呼びます。NAT の説明では、*内部*および*外部*という用語は任意の 2 つのインターフェイス間のセキュリティ関係を表しています。セキュリティ レベルの高い方が内部で、セキュリティ レベルの低い方が外部になります。たとえば、インターフェイス 1 が 60 でインターフェイス 2 が 50 の場合、インターフェイス 1 が「内部」、インターフェイス 2 が「外部」です。

NAT の利点の一部を紹介します。

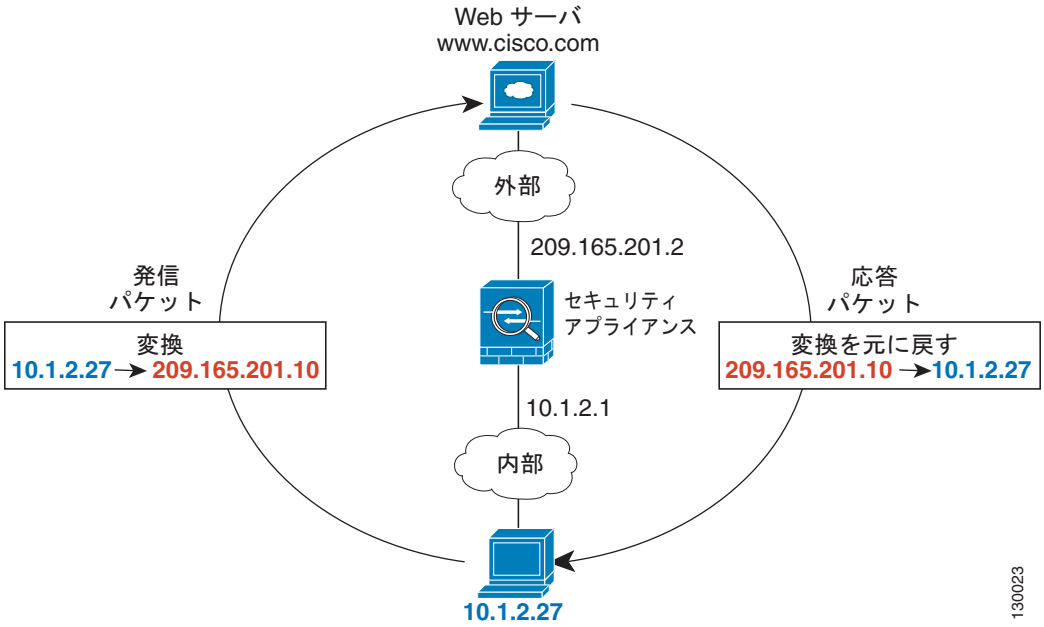
- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT は他のネットワークから実アドレスを隠すので、攻撃側はホストの実アドレスを突き止めることができません。
- 重複アドレスなど、IP ルーティングの問題を解決できます。

NAT でサポートされないプロトコルについては、表 24-1（P.24-3）を参照してください。

ルーテッド モードの NAT

図 25-1 は、内部にプライベート ネットワークを持つ、ルーテッド モードの一般的な NAT の例を示しています。10.1.1.27 にある内部ホストが Web サーバにパケットを送信すると、そのパケットの送信元実アドレス 10.1.1.27 がマップ アドレス 209.165.201.10 に変更されます。サーバが応答すると、応答がマッピング アドレス 209.165.201.10 に送信されます。そのパケットをセキュリティ アプライアンスが受信します。セキュリティ アプライアンスはその後、パケットをホストに送信する前に、変換したマッピング アドレス 209.165.201.10 を元の実際のアドレス 10.1.1.1.27 に戻します。

図 25-1　NAT の例：ルーテッド モード



トランスペアレント モードの NAT

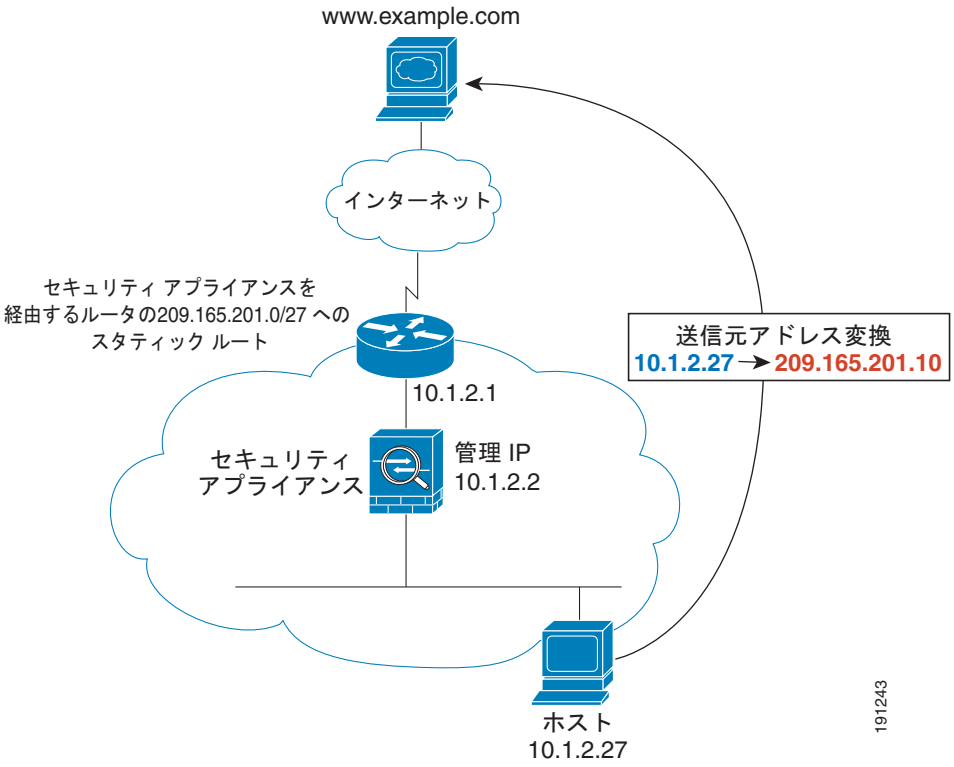
NAT をトランスペアレント モードで使用すると、ネットワークで NAT を実行するためのアップストリーム ルータまたはダウンストリーム ルータが必要なくなります。たとえば、トランスペアレント ファイアウォール セキュリティ アプライアンス は 2 つの VRF 間で役立ちます。つまり、VRF およびグローバル テーブル間で BGP ネイバー関係を確立できます。ただし、VRF ごとの NAT はサポートされない場合があります。この場合、トランスペアレント モードで NAT を使用することが必要不可欠です。

トランスペアレント モードの NAT には、次の要件および制限があります。

- マッピング アドレスがトランスペアレント ファイアウォールと同じネットワーク上にない場合、アップストリーム ルータで、（セキュリティ アプライアンス から）ダウンストリーム ルータを指しているマッピング アドレスにスタティック ルートを追加する必要があります。
- 実際の宛先アドレスがセキュリティ アプライアンスに直接接続されていない場合、セキュリティ アプライアンスで、ダウンストリーム ルータを指している実際の宛先にもスタティック ルートを追加する必要があります。NAT を使用しない場合、アップストリーム ルータからダウンストリーム ルータへのトラフィックは MAC アドレス テーブルを使用するため、セキュリティ アプライアンスでルートを何も必要としません。ただし、NAT を使用する場合、セキュリティ アプライアンスは MAC アドレス ルックアップの代わりにルート ルックアップを使用するため、ダウンストリーム ルータへのスタティック ルートが必要になります。
- **alias** コマンドはサポートされていません。
- トランスペアレント ファイアウォールにはインターフェイス IP アドレスがないため、インターフェイス PAT を使用できません。
- ARP インスペクションはサポートされていません。さらに、何らかの理由でファイアウォールの片側にあるホストからもう片側にあるホストに ARP 要求が送信され、送信側ホストの実アドレスが同じサブネット上の別のアドレスにマップされている場合、その実アドレスは ARP 要求で表示されたままになります。

図 25-2 に、インターフェイス内部と外部に同じネットワークを持つ、トランスペアレント モードの一般的な NAT のシナリオを示します。このシナリオのトランスペアレント ファイアウォールは NAT サービスを実行しているため、アップストリーム ルータは NAT を実行する必要がありません。内部ホスト 10.1.1.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.27 はマッピング アドレス 209.165.201.10 に変更されます。サーバが応答すると、マッピング アドレス 209.165.201.10 に応答を送信し、セキュリティ アプライアンス がそのパケットを受信します。これは、アップストリーム ルータには、セキュリティ アプライアンス を経由するスタティック ルートのこのマッピング ネットワークが含まれるためです。その後、セキュリティ アプライアンス はマッピング アドレス 209.165.201.10 を変換して実際のアドレス 10.1.1.1.27 に戻します。実際のアドレスは直接接続されているため、セキュリティ アプライアンスはそのアドレスを直接ホストに送信します。

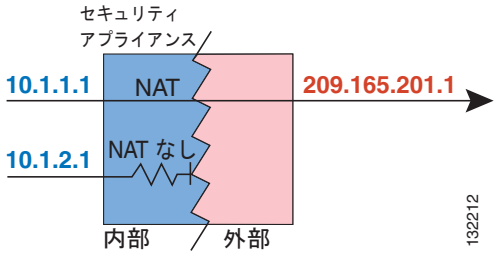
図 25-2　　NAT の例：トランスペアレント モード



NAT コントロール

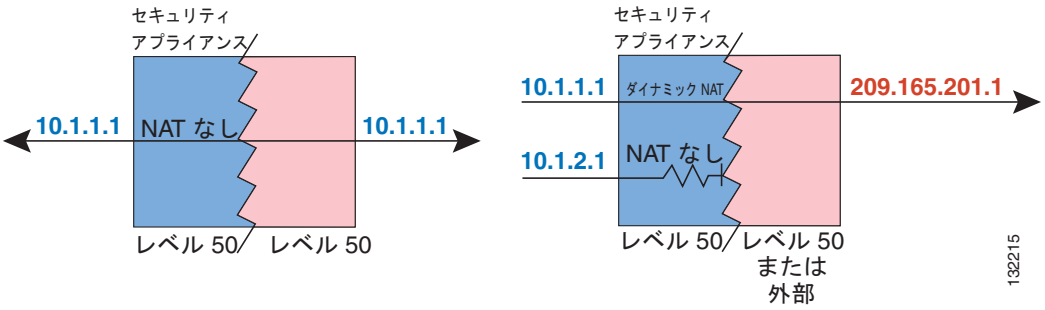
NAT 制御では、内部インターフェイスから外部インターフェイスに移動するパケットが NAT 規則と一致する必要があります。内部ネットワークの任意のホストが外部ネットワークのホストにアクセスできるようにするには、内部ホスト アドレスが変換されるように NAT を設定する必要があります（図 25-3 を参照）。

図 25-3　NAT 制御と発信トラフィック



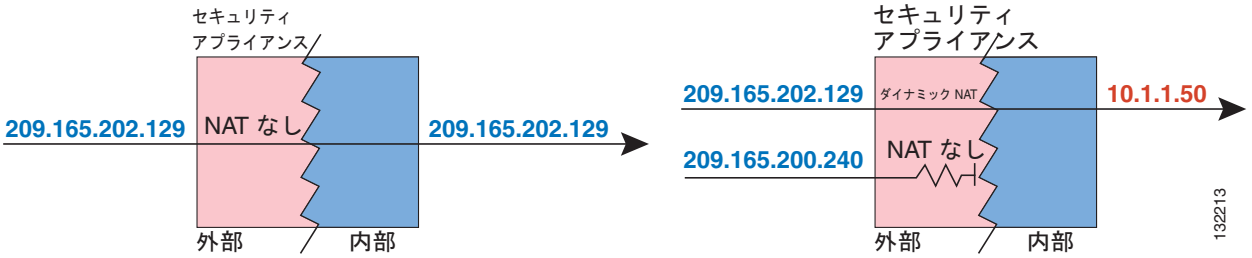
セキュリティ レベルが同じインターフェイス同士で通信する場合には、NAT を使用する必要はありません。ただし、ダイナミック NAT または PAT を同じセキュリティ レベルのインターフェイス上に設定した場合は、そのインターフェイスから同じセキュリティ レベルのインターフェイス、または外部インターフェイスに向かうすべてのトラフィックは、NAT 規則と一致する必要があります（図 25-4 を参照）。

図 25-4　NAT 制御と同一セキュリティ トラフィック



同様に、外部のダイナミック NAT または PAT をイネーブルにした場合、すべての外部トラフィックは、内部インターフェイスにアクセスするときに、NAT 規則と一致する必要があります（図 25-5 を参照）。

図 25-5　NAT 制御と着信トラフィック



スタティック NAT では、これらの制約は発生しません。

デフォルトでは、NAT 制御はディセーブルになっています。したがって、NAT を実行する場合以外、いずれのネットワークにおいても NAT を実行する必要はありません。ただし、新バージョンのソフトウェアにアップグレードした場合、NAT 制御がイネーブルになっていることがあります。NAT 制御がディセーブルになっている場合でも、ダイナミック NAT を設定するすべてのアドレスで NAT を実行する必要があります。ダイナミック NAT の適用方法については、「ダイナミック NAT の実装」（P.25-18）を参照してください。

NAT 制御によってセキュリティ レベルを上げる必要があるが、一部のケースで内部アドレスを変換しない場合、このようなアドレスに NAT 除外またはアイデンティティ NAT ルールを適用できます。（詳細については、「NAT 免除の使用」（P.25-32）を参照してください）。

NAT 制御を設定するには、「NAT 制御の設定」（P.25-17）を参照してください。

（注）　マルチ コンテキスト モードでは、共有インターフェイスで固有の MAC アドレスをイネーブルにしない場合、パケット分類子が NAT コンフィギュレーションに依存してパケットをコンテキストに割り当てる場合があります。分類機能と NAT の関係の詳細については、「セキュリティ アプライアンスによるパケットの分類方法」（P.9-3）を参照してください。

NAT のタイプ

この項では、使用可能な NAT のタイプについて説明します。次の項目を取り上げます。

- 「ダイナミック NAT」（P.25-6）
- 「PAT」（P.25-9）
- 「スタティック NAT」（P.25-9）
- 「スタティック PAT」（P.25-9）
- 「NAT 制御がイネーブルな状態での NAT のバイパス」（P.25-10）

アドレス変換は、ダイナミック NAT、ポート アドレス変換（PAT）、スタティック NAT、スタティック PAT、またはこれらのタイプの組み合わせとして実装できます。NAT をバイパスする規則を設定することもできます。たとえば、NAT を実行しない場合に、NAT 制御をイネーブルにします。

ダイナミック NAT

ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。マッピングされたプールにあるアドレスは、実際のグループより少ないことがあります。変換対象のホストが宛先ネットワークにアクセスすると、セキュリティ アプライアンスは、マッピングされたプールから IP アドレスをそのホストに割り当てます。この

変換は、実ホストが接続を開始するときにだけ追加されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセス リストでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用しているホストへの確実な接続を開始できません。また、セキュリティ アプライアンスは、実際のホスト アドレスに直接接続しようとする試みを拒否します。ホストへの確実なアクセスについては、「スタティック NAT」の項または「スタティック PAT」の項を参照してください。

（注）　セキュリティ アプライアンスがセッションを拒否した場合でも、接続に変換が追加されることがあります。この状況は通常、変換がタイムアウトになる着信アクセス リスト、管理専用インターフェイス、またはバックアップ インターフェイスで発生します。

図 25-6 は、リモート ホストによる実アドレスへの接続試行を示しています。セキュリティ アプライアンスはマッピング アドレスへのリターン接続だけを許可するため、この接続は拒否されています。

図 25-6　リモート ホストによる実アドレスへの接続試行

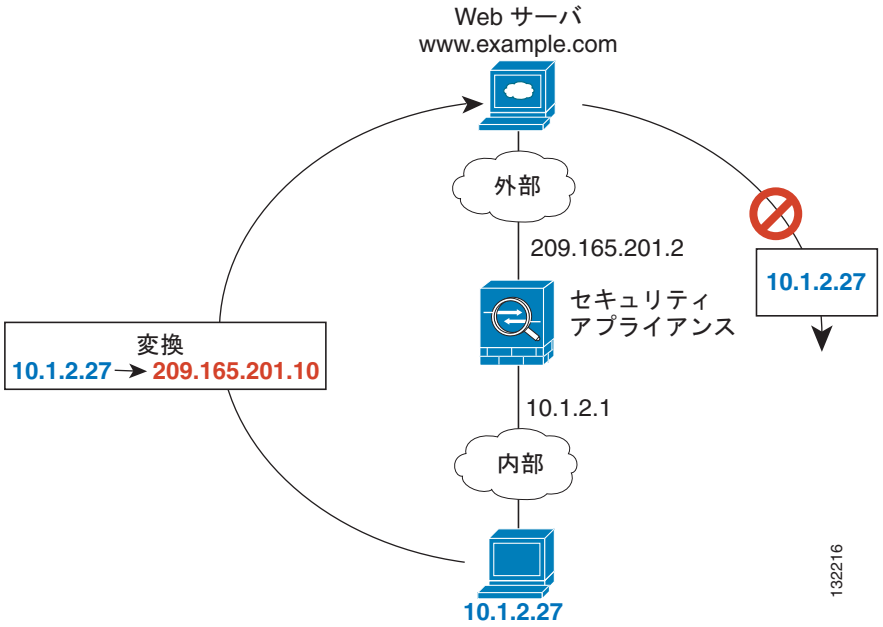
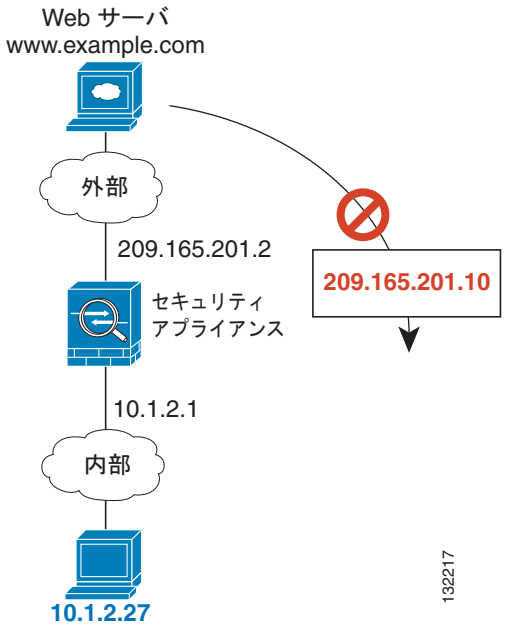


図 25-7 に、マッピング アドレスへの接続開始を試みているリモート ホストを示します。このアドレスは、現時点では変換テーブルにないため、セキュリティ アプライアンスはパケットをドロップしています。

図 25-7　マッピング アドレスへの接続開始を試みているリモート ホスト



（注）　変換の実施中、リモート ホストから、変換されたホストへの接続を開始できます（その接続がアクセス リストで許可されている場合）。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス リストのセキュリティに依存できます。

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

  この事象が発生した場合には、PAT を使用します。PAT では、単一アドレスのポートを使用して 64,000 を超える変換を処理できるためです。

- マッピング プールでは、ルーティング可能なアドレスを多数使用する必要があります。インターネットのように宛先ネットワークで登録済みアドレスが必要になる場合は、使用可能なアドレスが不足することがあります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は次の場合は機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。
- 一部のマルチメディア アプリケーションなどのように、1 つのポート上にデータ ストリームを持ち、別のポート上に制御パスを持ち、公開規格ではないアプリケーションでも機能しません。

NAT および PAT のサポートの詳細については、「アプリケーション プロトコル インスペクションを使用するタイミング」（P.24-2）を参照してください。

PAT

PAT は、複数の実アドレスを単一のマッピング IP アドレスに変換します。具体的には、セキュリティ アプライアンスが複数の実際のアドレスおよび送信元ポート（実際のソケット）を 1 つのマッピング アドレスおよび 1024 より上の一意のポート（マッピング ソケット）に変換します。接続ごとに送信元ポートが異なるため、それぞれの接続で個別に変換を行う必要があります。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

接続の有効期限が切れると、ポート変換も 30 秒間の非アクティブ状態の後に有効期限切れになります。このタイムアウトは変更できません。宛先ネットワーク上のユーザは、PAT を使用するホストに対して（アクセス リストによって接続が許可されていた場合でも）、接続を確実に開始することはできません。ホストの実またはマップ ポート番号を予測できないだけでなく、セキュリティ アプライアンス は変換対象ホストが接続を開始する側でない限り、変換を作成しません。ホストへの確実なアクセスについては、次の「スタティック NAT」または「スタティック PAT」の項を参照してください。

PAT では単一のマッピング先のアドレスを使用するため、ルーティング可能なアドレスの使用を抑えることができます。さらに、セキュリティ アプライアンス インターフェイスの IP アドレスを PAT アドレスとして使用できます。PAT は、データ ストリームが制御パスとは別のものであるマルチメディア アプリケーションでは機能しません。NAT および PAT のサポートの詳細については、「アプリケーション プロトコル インスペクションを使用するタイミング」（P.24-2）を参照してください。

（注）　変換の実施中、リモート ホストから、変換されたホストへの接続を開始できます（その接続がアクセス リストで許可されている場合）。実際のポート アドレスおよびマッピング ポート アドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス リストのセキュリティに依存できます。ただし、ポリシー PAT では時間ベースの ACL をサポートしていません。

スタティック NAT

スタティック NAT では、実アドレスからマッピング先のアドレスへの固定変換が作成されます。ダイナミック NAT および PAT では、各ホストは、後続の変換ごとに異なるアドレスまたはポートを使用します。スタティック NAT では、マッピング アドレスは連続する各接続で同じであり、永続的な変換規則が存在するため、宛先ネットワークのホストは変換済みのホストへのトラフィックを開始できます（そのトラフィックを許可するアクセス リストがある場合）。

ダイナミック NAT とスタティック NAT のアドレス範囲との主な違いは、スタティック NAT ではリモート ホストが変換済みのホストへの接続を開始でき（それを許可するアクセス リストがある場合）、ダイナミック NAT では開始できないという点です。また、スタティック NAT では、実アドレスと同じ数のマッピング先のアドレスが必要です。

スタティック PAT

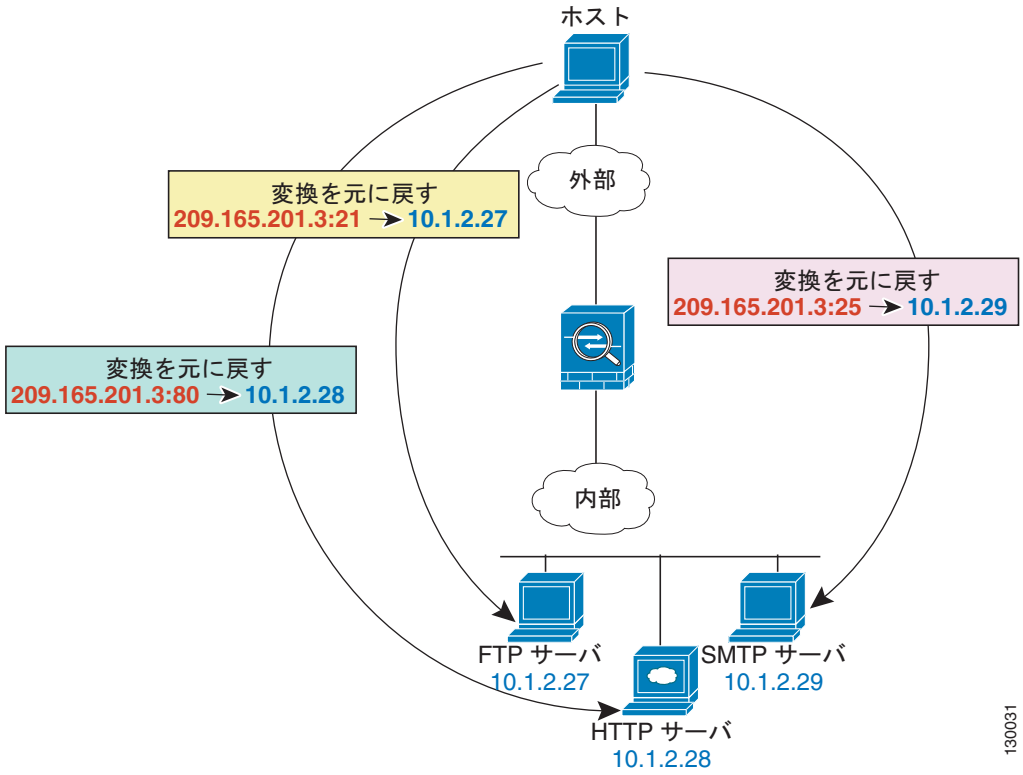
スタティック PAT は、プロトコル（TCP または UDP）および実際のアドレスとマッピング アドレスのポートを指定できる点を除いて、スタティック NAT と同じです。

この機能により、各文のポートが別個である限り、多数の異なるスタティック文にわたって同じマッピング アドレスを指定できます。複数のスタティック NAT 文に対しては、同じマッピング アドレスを使用できません。

セカンダリ チャネルの検査が必要なアプリケーション（FTP、VoIP など）を使用する場合は、セキュリティ アプライアンスが自動的にセカンダリ ポートを変換します。

たとえば、FTP、HTTP、および SMTP にアクセスする複数のリモート ユーザに単一アドレスを提供し、実際にはそれぞれが実ネットワーク上の別々のサーバである場合、マップ IP アドレスは同じでもポートが異なる各サーバに対し、スタティック PAT ステートメントを指定できます（図 25-8 を参照）。

図 25-8　スタティック PAT



スタティック PAT を使用して、well-known ポートを非標準ポートに、またはその逆に変換することもできます。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

NAT 制御がイネーブルな状態での NAT のバイパス

NAT コントロールをイネーブルにした場合、内部ホストは、外部ホストにアクセスするときに NAT ルールに一致する必要があります。一部のホストに対して NAT が実行されないようにするには、ホストに対する NAT をバイパスするか、NAT 制御をディセーブルにします。NAT をサポートしないアプリケーションを使用している場合などには、NAT をバイパスすることを推奨します。NAT をサポートしないインスペクション エンジンについては、「アプリケーション プロトコル インスペクションを使用するタイミング」（P.24-2）を参照してください。

3 通りの方法で、NAT をバイパスするようにトラフィックを設定できます。どの方法でも、インスペクション エンジンとの互換性が確保されます。ただし、機能は少しずつ異なります。

- アイデンティティ NAT：アイデンティティ NAT（ダイナミック NAT と類似）を設定するときは、変換を特定のインターフェイス上のホストに限定しません。つまり、アイデンティティ NAT は、すべてのインターフェイスを通過する接続に対して使用する必要があります。このため、インターフェイス A にアクセスするときには実アドレスに対して通常の変換の実行を選択できませんが、インターフェイス B にアクセスするときにはアイデンティティ NAT を使用できます。一方、通常

のダイナミック NAT では、アドレス変換を実施する特定のインターフェイスを指定できます。アイデンティティ NAT を使用する実アドレスが、アクセス リストに従って使用できるすべてのネットワークでルーティング可能であることを確認します。

アイデンティティ NAT の場合、マッピング先のアドレスは実アドレスと同じですが、外部から内部への接続を（インターフェイスのアクセス リストで許可されていても）開始できません。この機能には、スタティックなアイデンティティ NAT または NAT 免除を使用してください。

- スタティック アイデンティティ NAT：スタティック アイデンティティ NAT では、インターフェイスを指定して実際のアドレスを見えるようにするかどうかを許可できるため、インターフェイス A にアクセスするときにアイデンティティ NAT を使用し、インターフェイス B にアクセスするときに標準の変換を使用できます。スタティック アイデンティティ NAT では、ポリシー NAT も使用できます。この場合、変換する実アドレスを決定するときに、実アドレスと宛先アドレスを指定します（ポリシー NAT の詳細については、「ポリシー NAT」（P.25-11）を参照してください）。たとえば、内部アドレスから外部インターフェイスにアクセスし、宛先がサーバ A の場合に、内部アドレスにスタティック アイデンティティ NAT を使用し、外部サーバ B にアクセスするときには標準変換を使用するといったことが可能です。
- NAT 免除：NAT 免除では、変換済みのホストとリモート ホストの両方が接続を開始できます。アイデンティティ NAT と同様に、特定のインターフェイスでホストの変換を制限するのではなく、すべてのインターフェイスを経由する接続に NAT 免除を使用する必要があります。ただし、NAT 免除では、変換する実アドレスを判別するときに実アドレスおよび宛先アドレスを指定できるため（ポリシー NAT に似ています）、NAT 免除を使用する方が制御の柔軟性が増します。その反面、ポリシー NAT と異なり、NAT 免除ではアクセス リストのポートが考慮されません。NAT 免除では、最大 TCP 接続数など、接続制限の設定もできません。

ポリシー NAT

ポリシー NAT を使用すると、送信元アドレスおよび宛先アドレスを指定することにより、アドレス変換対象の実際のアドレスを指定できます。任意で送信元ポートおよび宛先ポートを指定することもできます。標準 NAT では送信元アドレスだけが考慮され、宛先は考慮されません。たとえば、ポリシー NAT を使用した場合、サーバ A にアクセスするときには実アドレスをマップ アドレス A に変換しますが、サーバ B にアクセスするときには実アドレスをマップ アドレス B に変換します。

セカンダリ チャネルのアプリケーション インスペクションを必要とするアプリケーション（FTP、VoIP など）では、ポリシー NAT ルールで指定されたポリシーにセカンダリ ポートが含まれている必要があります。ポートを予測できない場合、ポリシーはセカンダリ チャネルの IP アドレスだけを指定する必要があります。このコンフィギュレーションを使用して、セキュリティ アプライアンスはセカンダリ ポートを変換します。

図 25-9 に、2 台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129 に変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130 に変換されます。その結果、ホストはサーバと同じネットワークにあるように見え、ルーティングに役立ちます。

図 25-9　異なる宛先アドレスを使用するポリシー NAT

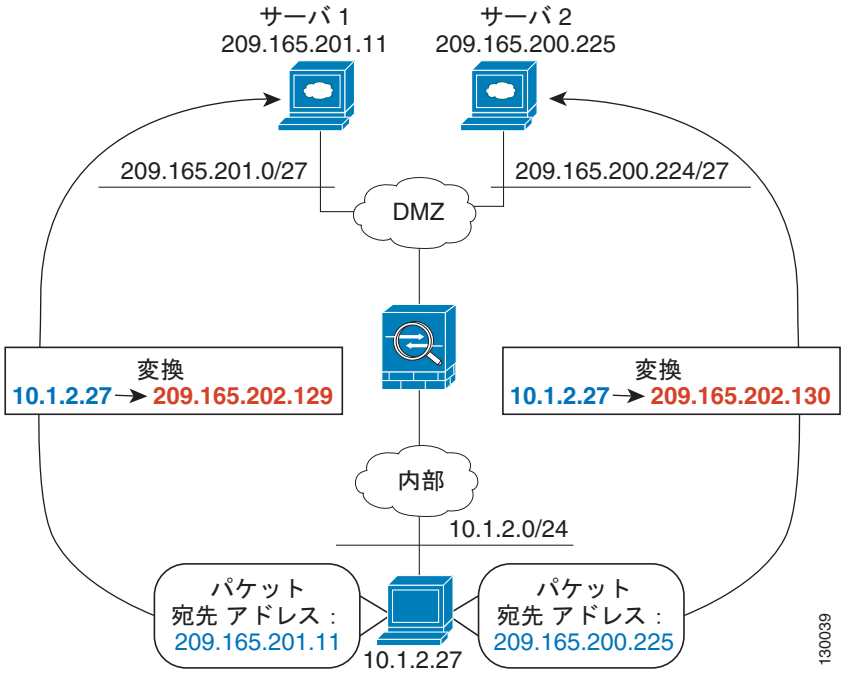
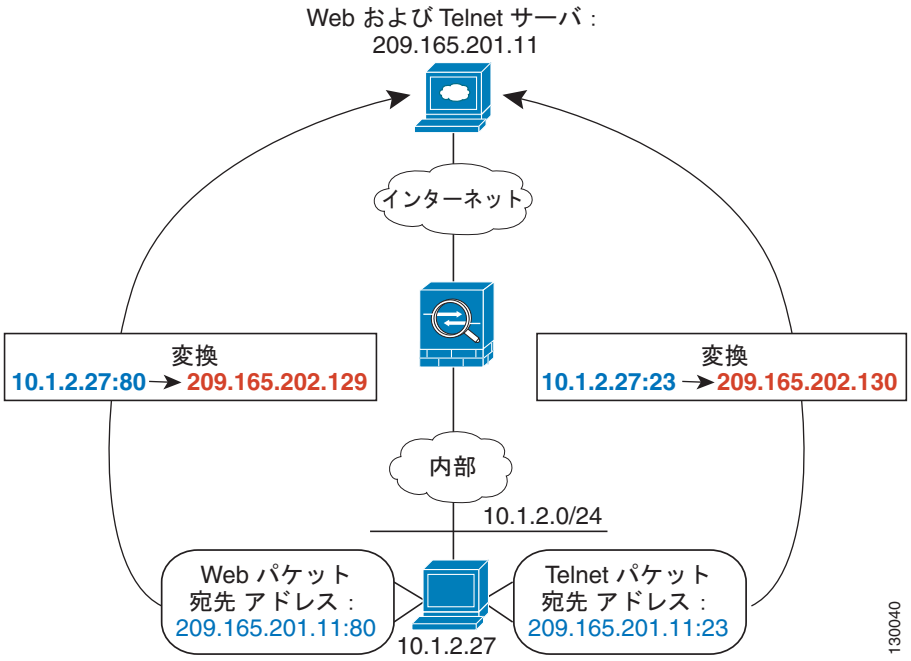


図 25-10 に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Web サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129 に変換されます。ホストが Telnet サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130 に変換されます。

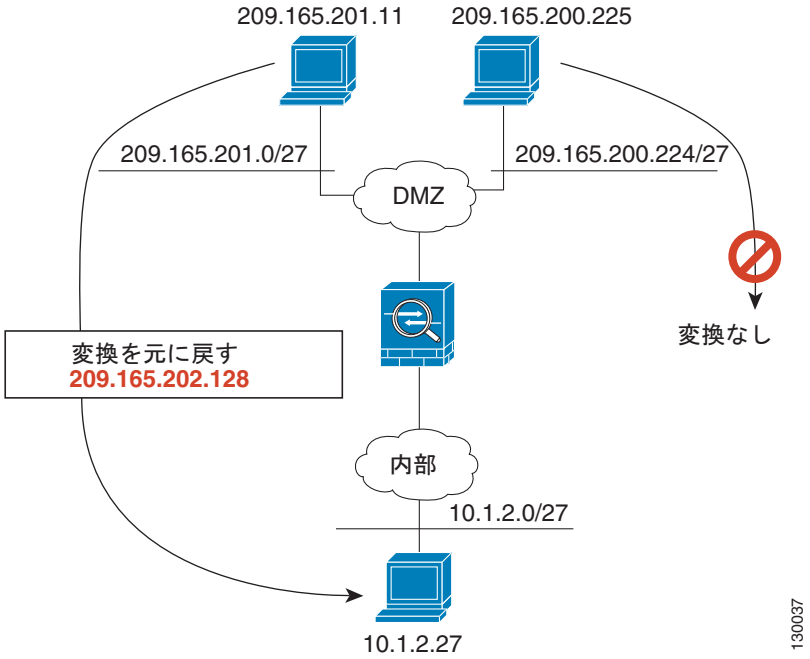
図 25-10　異なる宛先ポートを使用するポリシー NAT



ポリシー スタティック NAT では、変換済みのホストとリモート ホストの両方がトラフィックを発信できます。変換済みのネットワークで発信されたトラフィックについては、NAT ルールで実際のアドレスと*宛先*アドレスが指定されますが、リモート ネットワークで発信されたトラフィックについては、この変換を使用してホストに接続することを許可されているリモート ホストの実際のアドレスと*送信元*アドレスがルールで指定されます。

図 25-11 に、変換済みのホストに接続するリモート ホストを示します。変換対象ホストには、ネットワーク 209.165.201.0/27 との双方向のトラフィックだけに対し実アドレスを変換する、ポリシー スタティック NAT 変換が設定されています。209.165.200.224/27 ネットワーク用の変換は存在しません。したがって、変換済みのホストはそのネットワークに接続できず、そのネットワークのホストも変換済みのホストに接続できません。

図 25-11　宛先アドレス変換を行うポリシー スタティック NAT



（注）　ポリシー NAT は SQL*Net をサポートしませんが、標準 NAT は SQL*Net をサポートします。他のプロトコルの NAT サポートについては、「アプリケーション プロトコル インスペクションを使用するタイミング」（P.24-2）を参照してください。

NAT および同じセキュリティ レベルのインターフェイス

セキュリティ レベルが同じインターフェイス間では、NAT コントロールをイネーブルにした場合でも、NAT は必要ありません。必要に応じて任意で NAT を設定できます。ただし、NAT 制御がイネーブルになっている場合にダイナミック NAT を設定するときは、NAT が必要です。詳細については、「NAT コントロール」（P.25-5）を参照してください。また、同一セキュリティ レベルのインターフェイス上でダイナミック NAT または PAT に対して IP アドレス グループを指定する場合、そのアドレス グループが下位または同一セキュリティ レベルのインターフェイスにアクセスするときには、アドレス グループに対して NAT を実行する必要があります（NAT 制御がイネーブルでない場合でも）。スタティック NAT として識別されたトラフィックは影響を受けません。

（注）　同一セキュリティ レベルのインターフェイス上に NAT を設定した場合、セキュリティ アプライアンスは VoIP インスペクション エンジンをサポートしません。これらのインスペクション エンジンには、Skinny、SIP、および H.323 が含まれます。サポートされるインスペクション エンジンについては、「アプリケーション プロトコル インスペクションを使用するタイミング」（P.24-2）を参照してください。

実際のアドレスとの照合に使用される NAT ルールの順序

セキュリティ アプライアンスは、次の順序で実際のアドレスを NAT ルールと照合します。

1. NAT 免除：順序に従って、最初の一致が見つかるまで続行されます。
2. スタティック NAT とスタティック PAT（標準およびポリシー）：順序に従って、最初の一致が見つかるまで続行されます。スタティック アイデンティティ NAT はこのカテゴリに含まれません。
3. ポリシー ダイナミック NAT：順序に従って、最初の一致が見つかるまで続行されます。アドレスの重複は可能です。
4. 標準のダイナミック NAT：最も適合する一致を見つけます。標準アイデンティティ NAT はこのカテゴリに含まれます。NAT ルールの順序は関係なく、実際のアドレスと最も適合する NAT ルールが使用されます。たとえば、インターフェイス上のすべてのアドレス（0.0.0.0）を変換する汎用文を作成できます。ネットワークのサブネット（10.1.1.1）を別のアドレスに変換する場合は、10.1.1.1 だけを変換する文を作成できます。10.1.1.1 が接続を開始すると、10.1.1.1 用の特定のルールが使用されます。これは、それが実際のアドレスに最も適合するからです。重複するルールを使用することはお勧めしません。重複するルールにより、使用メモリが増え、セキュリティ アプライアンスのパフォーマンスが低下する可能性があります。

マッピング アドレスの注意事項

実際のアドレスをマッピング アドレスに変換するときは、次のマッピング アドレスを使用できます。

- マッピング インターフェイスと同じネットワーク上のアドレス

  （セキュリティ アプライアンス から出ていくトラフィックが通過する）マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、セキュリティ アプライアンス はプロキシ ARP を使用してマッピング アドレスの要求に応答することによって、実アドレス宛てのトラフィックを代行受信します。この方法では、セキュリティ アプライアンス がその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。ただし、この方法では、変換に使用できるアドレス数に限度があります。

  PAT では、マッピング インターフェイスの IP アドレスも使用できます。

- 固有のネットワーク上のアドレス

  マッピング インターフェイスで使用可能なアドレスより多くのアドレスが必要な場合は、別のサブネット上のアドレスを指定できます。セキュリティ アプライアンス は、プロキシ ARP を使用してマッピング アドレス要求に応答することによって、実アドレス宛てのトラフィックを代行受信します。OSPF を使用し、マッピング インターフェイス上でルートをアドバタイズする場合、セキュリティ アプライアンス はマッピング アドレスをアドバタイズします。マッピング インターフェイスがパッシブの場合（ルートをアドバタイズしない）、またはスタティック ルーティングを使用する場合は、マッピング アドレス宛てのトラフィックを セキュリティ アプライアンス に送信するアップストリーム ルータ上でスタティック ルートを追加する必要があります。

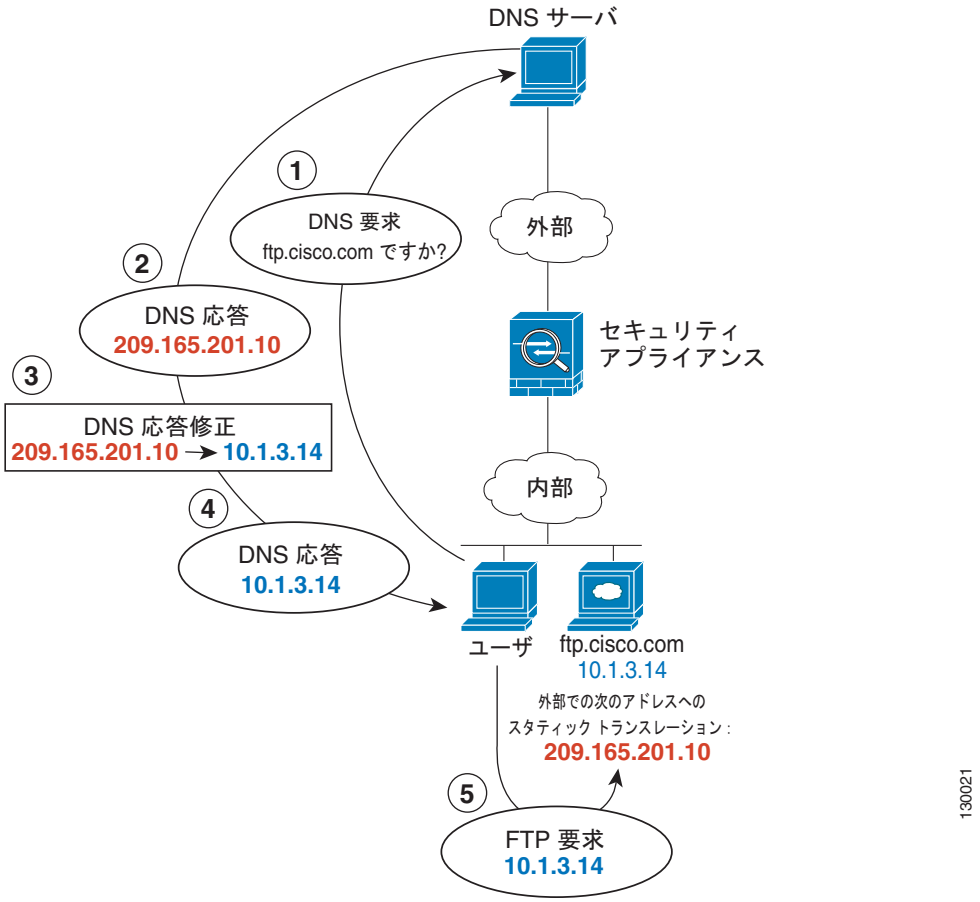
DNS および NAT

応答内のアドレスを NAT コンフィギュレーションと一致するアドレスに置き換えて、DNS 応答を修正するようにセキュリティ アプライアンスを設定することが必要になる場合があります。DNS 修正は、各変換を設定するときに設定できます。

たとえば、DNS サーバが外部インターフェイスからアクセス可能であるとします。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）を、外部ネットワーク上で可視のマッピング アドレス（209.165.201.10）にスタティックに変換するように、セキュリティ アプライアンスを設定します（図 25-12 を参照）。この場合、このスタティック文で DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。セキュリティ アプライアンス は内部サーバのスタティック ステートメントを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正をイネーブルにしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックを送信することを試みます。

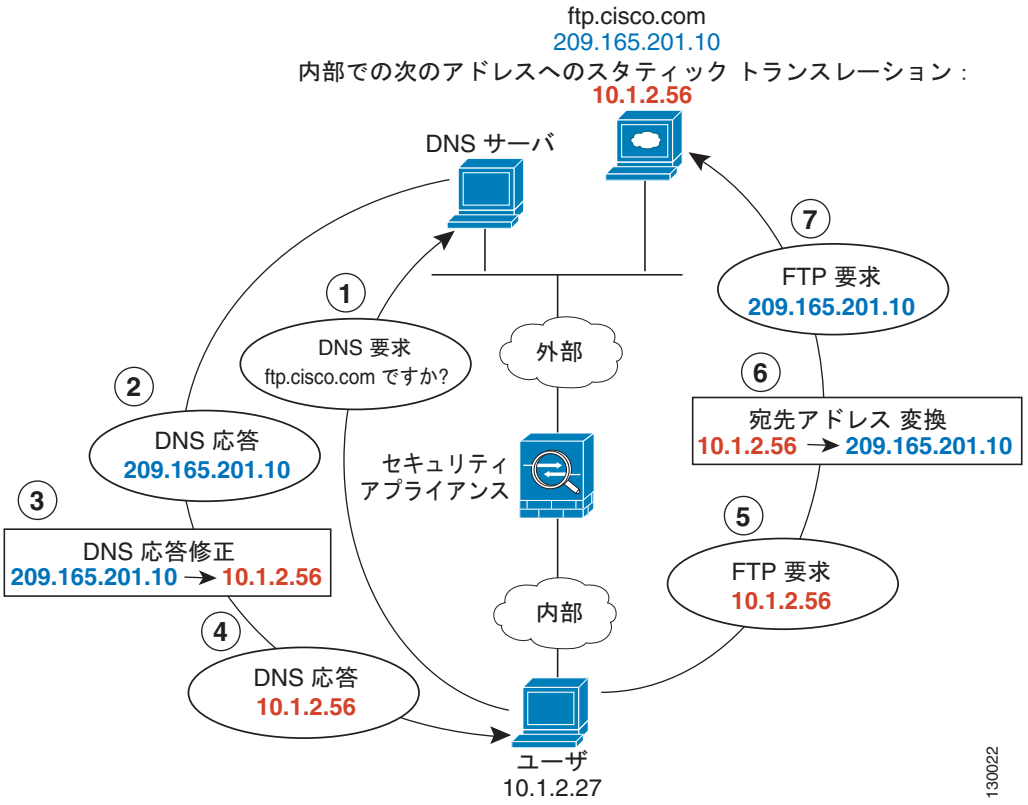
図 25-12　DNS 応答修正



（注）　他のネットワーク（DMZ など）のユーザも外部 DNS サーバから ftp.cisco.com の IP アドレスを要求している場合、そのユーザがスタティック規則で参照される内部インターフェイスに存在しない場合でも、そのユーザに対して DNS 応答の IP アドレスも修正されます。

図 25-13 に、外部の Web サーバと DNS サーバを示します。セキュリティ アプライアンスには、外部サーバ用のスタティック変換があります。この場合、ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.20.10 を示します。ftp.cisco.com のマッピング アドレス（10.1.2.56）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。

図 25-13　外部 NAT を使用する DNS 応答修正



NAT 制御の設定

NAT 制御では、内部インターフェイスから外部インターフェイスへのパケットは NAT ルールと一致する必要があります。詳細については、「NAT コントロール」（P.25-5）を参照してください。

NAT 制御をイネーブルにするには、[Configuration] > [Firewall] > [NAT Rules] ペインで、[Enable traffic through the firewall without address translation] をオンにします。

ダイナミック NAT の使用

この項では、ダイナミック NAT および PAT、ダイナミック ポリシー NAT および PAT、アイデンティティ NAT を含む、ダイナミック NAT の設定方法について説明します。

ポリシー NAT を使用すると、送信元アドレスおよび宛先アドレスを指定することにより、アドレス変換対象の実際のアドレスを指定できます。任意で送信元ポートおよび宛先ポートを指定することもできます。標準 NAT では送信元アドレスだけが考慮され、宛先は考慮されません。詳細については、「ポリシー NAT」（P.25-11）を参照してください。

この項では、次のトピックについて取り上げます。

ダイナミック NAT の実装

この項では、ダイナミック NAT の実装方法について説明します。説明する内容は次のとおりです。

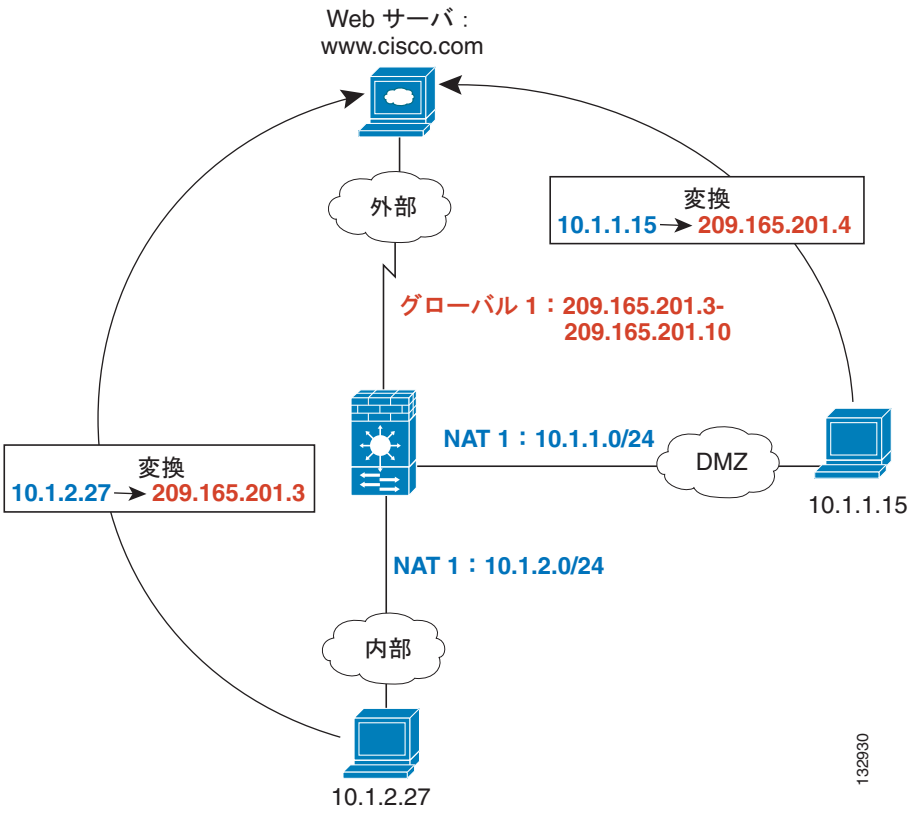
プール ID を使用した実際のアドレスとグローバル プールのペア

ダイナミック NAT ルールでは、実際のアドレスを指定し、それをアドレスのグローバル プールとペアにします。実際のアドレスは別のインターフェイスを出るときにこのグローバル プールにマッピングされます（PAT の場合、これは 1 つのアドレスになり、アイデンティティ NAT の場合は同じ実際のアドレスになります）。各グローバル プールにはプール ID が割り当てられます。

別のインターフェイス上の同じグローバル プールを使用する NAT ルール

同じグローバル アドレス プールを使用してインターフェイスごとに NAT ルールを作成できます。たとえば、内部インターフェイス用と DMZ インターフェイス用の両方に外部インターフェイス上のグローバル プール 1 を使用して NAT ルールを設定できます。内部インターフェイスと DMZ インターフェイスからのトラフィックは、外部インターフェイスを出るときに、マップ プールまたは PAT アドレスを共有します（図 25-14 を参照）。

図 25-14　複数のインターフェイス上の同じグローバル プールを使用する NAT ルール

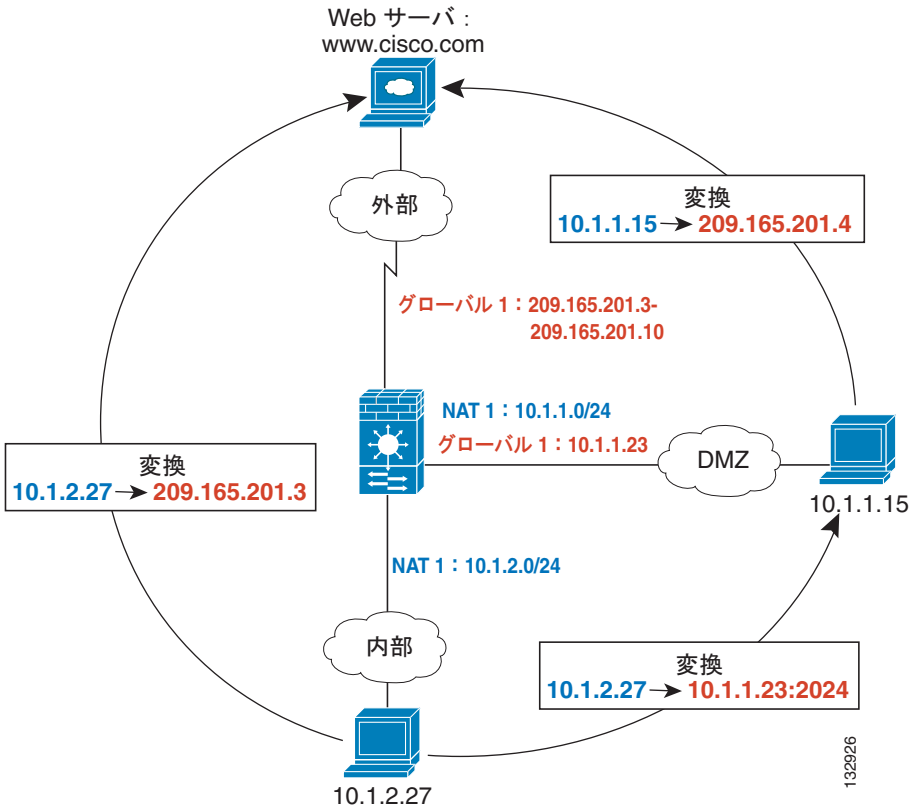


複数のインターフェイス上の同じプール ID を持つグローバル プール

同じプール ID を使用してインターフェイスごとにグローバル プールを作成できます。ID 1 で外部インターフェイスと DMZ インターフェイス用にグローバル プールを作成した場合、トラフィックが外部インターフェイスと DMZ インターフェイスの両方に向かうとき、ID 1 に関連付けられた 1 つの NAT

ルールが変換対象のトラフィックを識別します。同様に、ID 1 で DMZ インターフェイス用の NAT ルールを作成した場合、ID 1 のすべてのグローバル プールもまた DMZ トラフィックに使用されます（図 25-15 を参照）。

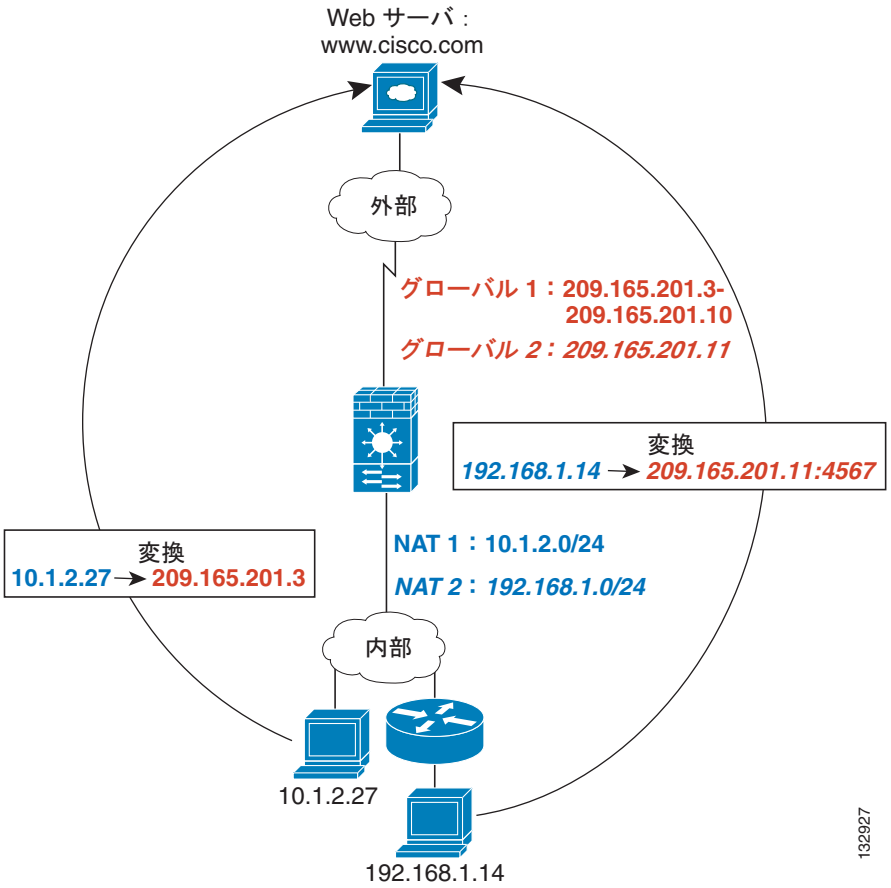
図 25-15　複数のインターフェイス上の同じ ID を使用する NAT ルールとグローバル プール



同じインターフェイス上の異なるグローバル プールを使用する複数の NAT ルール

異なる実際のアドレス セットが異なるマッピング アドレスを持つように指定できます。たとえば、内部インターフェイスに 2 つの異なるプール ID で 2 つの NAT ルールを設定できます。外部インターフェイスに、これらの 2 つの ID に対する 2 つのグローバル プールを設定します。設定後、内部ネットワーク A からのトラフィックが外部インターフェイスを出ると、IP アドレスはプール 1 のアドレスに変換され、内部ネットワーク B からのトラフィックはプール 2 のアドレスに変換されます（図 25-16 を参照）。ポリシー NAT を使用すると、宛先アドレスとポートが各アクセス リスト内で一意である限り、複数の NAT ルールに対して同じ実際のアドレスを指定できます。

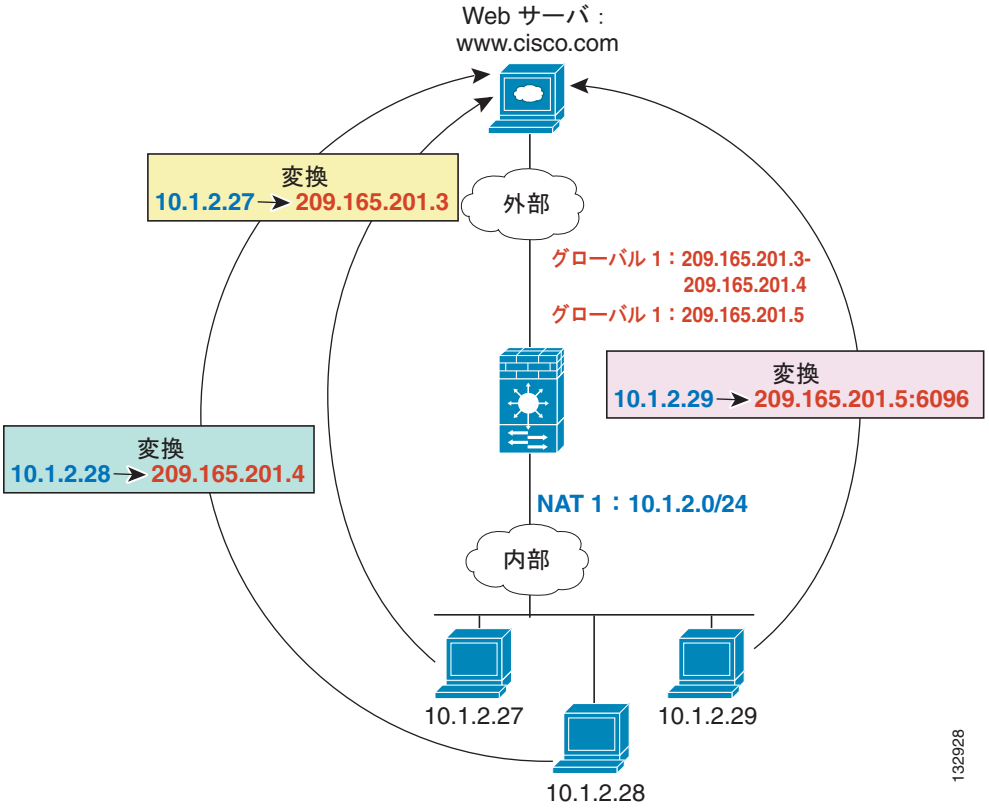
図 25-16　異なる NAT ID



同じグローバル プール内の複数のアドレス

同じグローバル プール内に複数のアドレスを持てます。セキュリティ アプライアンスは最初にダイナミック NAT のアドレス範囲をコンフィギュレーション内の順序に従って使用し、次に PAT の 1 つのアドレスを順序に従って使用します。さらに、特定のアプリケーションにはダイナミック NAT を使用し、ダイナミック NAT のアドレスをすべて使い切ったときに備えて予備の PAT ルールを用意する必要がある場合、アドレス範囲と PAT アドレスの両方を追加できます。同様に、1 つの PAT マッピング アドレスがサポートするおよそ 64,000 より多くの PAT セッションが必要な場合、プールに 2 つの PAT アドレスを持てます（図 25-17 を参照）。

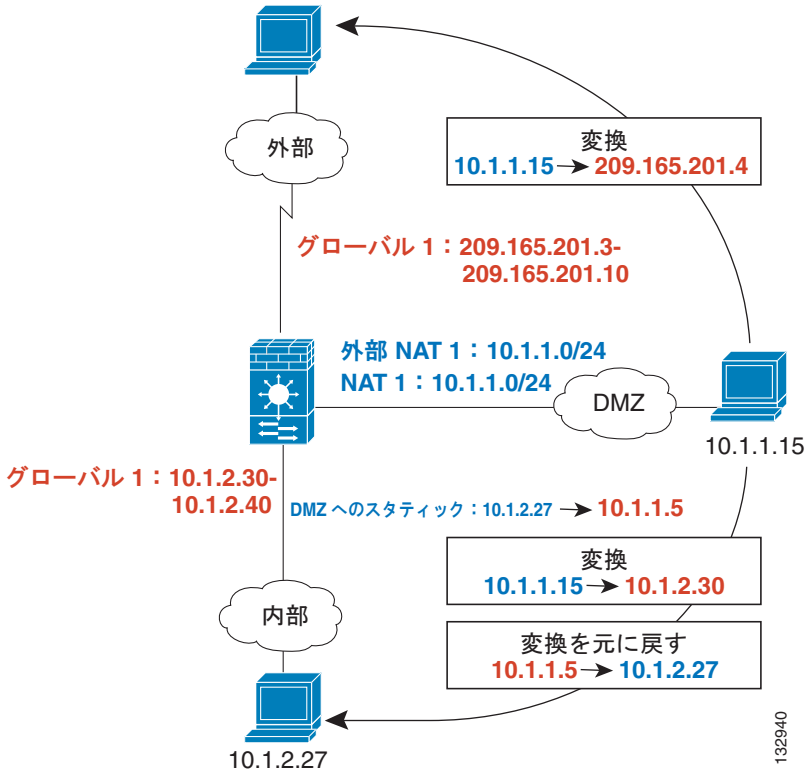
図 25-17　NAT および PAT の併用



外部 NAT

アドレスを外部インターフェイスから内部インターフェイスに変換する NAT ルールは外部 NAT ルールです。外部 NAT ルールが着信トラフィックを変換することを指定する必要があります。同じトラフィックがセキュリティの低いインターフェイスにアクセスするときも変換が必要な場合（たとえば、DMZ のトラフィックを内部および外部インターフェイスにアクセスするときに変換する場合など）、同じ NAT ID を使用して、発信を指定する 2 つ目の NAT ルールを作成できます（図 25-18 を参照）。外部 NAT（DMZ インターフェイスから内部インターフェイス）の場合、内部ホストはスタティック ルールを使用して外部アクセスを許可するので、送信元アドレスと宛先アドレスの両方が変換されます。

図 25-18　外部 NAT および内部 NAT の組み合わせ



NAT ルール内の実際のアドレスは同位または低位のセキュリティ レベルのインターフェイスすべてで変換が必要

IP アドレス グループに対する NAT ルールを作成した場合、そのグループが同位か低位のセキュリティ レベルのインターフェイスにアクセスするときに NAT を実行する必要があります。また、各インターフェイスに同じプール ID を持つグローバル プールを作成するか、スタティック ルールを使用する必要があります。グループが高位のセキュリティ インターフェイスにアクセスするときには、NAT は必要ありません。外部 NAT ルールを作成した場合、上記の NAT 要件は、そのアドレス グループが高位のセキュリティ インターフェイスにアクセスするときは常に適用されます。スタティック ルールで指定されたトラフィックは影響を受けません。

グローバル プールの管理

ダイナミック NAT は変換にグローバル プールを使用します。グローバル プールの動作については、「ダイナミック NAT の実装」（P.25-18）を参照してください。

グローバル プールを管理するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Global Pools] ペインで、[Add] をクリックして新しいプールを追加するか、プールを選択して [Edit] をクリックします。

[Add/Edit Dynamic NAT Rule] ダイアログボックスで [Manage] ボタンをクリックしてもグローバル プールを管理できます。

[Add/Edit Global Address Pool] ダイアログボックスが表示されます。

ステップ 2　新しいプールの場合、[Interface] ドロップダウン リストから、マッピング IP アドレスを使用するインターフェイスを選択します。

ステップ 3　新しいプールの場合、[Pool ID] フィールドに 1 ～ 2147483647 の範囲の数値を入力します。すでに使用されているプール ID は入力しないでください。すでに使用されている場合、設定は拒否されます。

ステップ 4　[IP Addresses to Add] 領域で、[Range]、[Port Address Translation (PAT)]、または [PAT Address Translation (PAT) Using IP Address of the interface] をクリックします。

アドレスの範囲を指定すると、セキュリティ アプライアンスはダイナミック NAT を実行します。[Netmask] フィールドにサブネット マスクを指定すると、その値がマッピング アドレスがホストに割り当てられるときに使用されるサブネット マスクになります。マスクを指定しない場合は、アドレス クラスのデフォルト マスクが使用されます。

ステップ 5　[Addresses Pool] ウィンドウにアドレスを追加するには、[Add] をクリックします。

ステップ 6　（任意）グローバル プールには複数のアドレスを追加できます。たとえば、ダイナミック範囲を設定した後に PAT アドレスを追加する場合、PAT アドレスの値を入力して再度 [Add] をクリックします。1 つのインターフェイスに同じプール ID で複数のアドレスを使用する方法については、「同じグローバル プール内の複数のアドレス」（P.25-21）を参照してください。

ステップ 7　[OK] をクリックします。

ダイナミック NAT、ダイナミック PAT、またはダイナミック アイデンティティ NAT の設定

ダイナミック NAT、ダイナミック PAT、またはダイナミック アイデンティティ NAT のルールを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインで、[Add] > [Add Dynamic NAT Rule] を選択します。

[Add Dynamic NAT Rule] ダイアログボックスが表示されます。

ステップ 2　[Original] 領域で、[Interface] ドロップダウン リストから、変換対象の実際のアドレスを持つホストに接続するインターフェイスを選択します。

ステップ 3　[Source] フィールドに実際のアドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

ステップ 4　グローバル プールを選択するには、次のいずれかのオプションを使用します。

- すでに定義されているグローバル プールを選択する。

  プールにアドレス範囲が含まれている場合、セキュリティ アプライアンスはダイナミック NAT を実行します。プールに含まれるアドレスが 1 つだけの場合、セキュリティ アプライアンスはダイナミック PAT を実行します。プールにアドレス範囲と単一アドレスの両方が含まれている場合、範囲が順序に従って使用され、続いて PAT アドレスが順序に従って使用されます。詳細については、「同じグローバル プール内の複数のアドレス」（P.25-21）を参照してください。

プールはプール ID で識別されます。異なるインターフェイスにある複数のグローバル プールが同じプール ID を共有する場合、それらのプールはグループとなります。複数のインターフェイスを持つプール ID を選択すると、トラフィックはプールのいずれかのインターフェイスにアクセスしたときに指定どおりに変換されます。プール ID の詳細については、「ダイナミック NAT の実装」（P.25-18）を参照してください。

- [Manage] をクリックして新しいグローバル プールを作成するか既存のプールを編集する。「グローバル プールの管理」（P.25-23）を参照してください。
- [global pool 0] を選択してアイデンティティ NAT を選択する。

ステップ 5　（任意）DNS 応答内部のアドレスの変換をイネーブルにするには、[Connection Settings] 領域をクリックして開き、[Translate the DNS replies that match the translation rule] をオンにします。

NAT ルールに DNS サーバ内にエントリを持つホストの実際のアドレスが含まれており、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一方には実際のアドレスが必要です。このオプションは、クライアントに送信される DNS 応答内のアドレスを書き換えます。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。通常、他のインターフェイスからのアクセスを許可する必要があるホストはスタティック変換を使用するため、このオプションはスタティック ルールで使用される可能性があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。

ステップ 6　（任意）接続設定をイネーブルにするには、[Connection Settings] 領域をクリックして開き、次のオプションを 1 つ以上設定します。

（注）　これらの値は、セキュリティ ポリシー ルールを使用しても設定できます（「接続の設定」（P.27-6）を参照）。これらのオプションを両方に設定した場合、セキュリティ アプライアンスは低い方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

- [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  - 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
  - セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
  - セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
- [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。

- [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

ステップ 7　[OK] をクリックします。

ダイナミック ポリシー NAT またはダイナミック ポリシー PAT の設定

ダイナミック ポリシー NAT またはダイナミック ポリシー PAT を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインで、[Add] > [Advanced] > [Add Dynamic Policy NAT Rule] を選択します。

[Add Dynamic Policy NAT Rule] ダイアログボックスが開きます。

ステップ 2　[Original] 領域で、[Interface] ドロップダウン リストから、変換対象の実際のアドレスを持つホストに接続するインターフェイスを選択します。

ステップ 3　[Source] フィールドに実際のアドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

実際のアドレスが複数ある場合はカンマで区切ります。

ステップ 4　[Destination] フィールドに宛先アドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

宛先アドレスが複数ある場合はカンマで区切ります。

デフォルトでは、フィールドには任意の宛先アドレスを許可する **any** が表示されています。

ステップ 5　グローバル プールを選択するには、次のいずれかのオプションを使用します。

- すでに定義されているグローバル プールを選択する。

  プールにアドレス範囲が含まれている場合、セキュリティ アプライアンスはダイナミック NAT を実行します。プールに含まれるアドレスが 1 つだけの場合、セキュリティ アプライアンスはダイナミック PAT を実行します。プールにアドレス範囲と単一アドレスの両方が含まれている場合、範囲が順序に従って使用され、続いて PAT アドレスが順序に従って使用されます。詳細については、「同じグローバル プール内の複数のアドレス」（P.25-21）を参照してください。

プールはプール ID で識別されます。異なるインターフェイスにある複数のグローバル プールが同じプール ID を共有する場合、それらのプールはグループとなります。複数のインターフェイスを持つプール ID を選択すると、トラフィックはプールのいずれかのインターフェイスにアクセスしたときに指定どおりに変換されます。プール ID の詳細については、「ダイナミック NAT の実装」（P.25-18）を参照してください。

- [Manage] をクリックして新しいグローバル プールを作成するか既存のプールを編集する。「グローバル プールの管理」（P.25-23）を参照してください。
- [global pool 0] を選択してアイデンティティ NAT を選択する。

ステップ 6　（任意）[Description] フィールドに説明を入力します。

ステップ 7　（任意）DNS 応答内部のアドレスの変換をイネーブルにするには、[Connection Settings] 領域をクリックして開き、[Translate the DNS replies that match the translation rule] をオンにします。

NAT ルールに DNS サーバ内にエントリを持つホストの実際のアドレスが含まれており、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一方には実際のアドレスが必要です。このオプションは、クライアントに送信される DNS 応答内のアドレスを書き換えます。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。通常、他のインターフェイスからのアクセスを許可する必要があるホストはスタティック変換を使用するため、このオプションはスタティック ルールで使用される可能性があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。

ステップ 8　（任意）接続設定をイネーブルにするには、[Connection Settings] 領域をクリックして開き、次のオプションを 1 つ以上設定します。

（注）　これらの値は、セキュリティ ポリシー ルールを使用しても設定できます（「接続の設定」（P.27-6）を参照）。これらのオプションを両方に設定した場合、セキュリティ アプライアンスは低い方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

- [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  - 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
  - セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
  - セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
- [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。

- [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

ステップ 9　[OK] をクリックします。

スタティック NAT の使用

この項では、標準またはポリシー スタティック NAT、PAT、またはアイデンティティ NAT を使用してスタティック変換を設定する方法について説明します。

スタティック NAT の詳細については、「スタティック NAT」（P.25-9）を参照してください。

ポリシー NAT を使用すると、送信元アドレスおよび宛先アドレスを指定することにより、アドレス変換対象の実際のアドレスを指定できます。任意で送信元ポートおよび宛先ポートを指定することもできます。標準 NAT では送信元アドレスだけが考慮され、宛先は考慮されません。詳細については、「ポリシー NAT」（P.25-11）を参照してください。

スタティック PAT を使用すると、実 IP アドレスをマップ IP アドレスに変換し、さらに実ポートをマップ ポートに変換できます。同じポートを変換する場合は、特定のトラフィック タイプを変換できます。または、別のポートに変換することによってさらに細かく制御することもできます。セカンダリ チャネルのアプリケーション インスペクションが必要なアプリケーション（FTP、VoIP など）を使用する場合は、セキュリティ アプライアンスが自動的にセカンダリ ポートを変換します。スタティック PAT の詳細については、「スタティック PAT」（P.25-9）を参照してください。

同じ 2 つのインターフェイス間で複数のスタティック ルールに同じ実際のアドレスまたはマッピング アドレスを使用するには、スタティック PAT を使用する必要があります。同じマッピング インターフェイスのグローバル プールにも定義されているマッピング アドレスをスタティック ルールに使用しないでください。

スタティック アイデンティティ NAT では、実際の IP アドレスが同じ IP アドレスに変換されます。

この項では、次のトピックについて取り上げます。

- 「スタティック NAT、スタティック PAT、またはスタティック アイデンティティ NAT の設定」（P.25-28）
- 「スタティック ポリシー NAT、スタティック ポリシー PAT、またはスタティック ポリシー アイデンティティ NAT の設定」（P.25-30）

スタティック NAT、スタティック PAT、またはスタティック アイデンティティ NAT の設定

スタティック NAT、スタティック PAT、またはスタティック アイデンティティ NAT を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインで、[Add] > [Add Static NAT Rule] を選択します。

[Add Static NAT Rule] ダイアログボックスが表示されます。

ステップ 2　[Original] 領域で、[Interface] ドロップダウン リストから、変換対象の実際のアドレスを持つホストに接続するインターフェイスを選択します。

ステップ 3　[Source] フィールドに実際のアドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

ステップ 4　[Translated] 領域で、[Interface] ドロップダウン リストから、マッピング アドレスを使用するインターフェイスを選択します。

ステップ 5　マッピング IP アドレスを指定するには、次のいずれかをクリックします。

- **Use IP Address**

  IP アドレスを入力するか、[...] ボタンをクリックして ASDM ですでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

- **Use Interface IP Address**

実際のアドレスとマッピング アドレスのサブネット マスクは同じである必要があります。

（注）　アイデンティティ NAT の場合、[Original] フィールドと [Translated] フィールドに同じ IP アドレスを入力します。

ステップ 6　（任意）スタティック PAT を使用するには、[Enable Port Address Translation (PAT)] をオンにします。

a.　[Protocol] では、[TCP] または [UDP] をクリックします。

b.　[Original Port] フィールドで、実際のポート番号を入力します。

c.　[Translated Port] フィールドで、マッピング ポート番号を入力します。

ステップ 7　（任意）DNS 応答内部のアドレスの変換をイネーブルにするには、[Connection Settings] 領域をクリックして開き、[Translate the DNS replies that match the translation rule] をオンにします。

NAT ルールに DNS サーバ内にエントリを持つホストの実際のアドレスが含まれており、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一方には実際のアドレスが必要です。このオプションは、クライアントに送信される DNS 応答内のアドレスを書き換えます。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。

ステップ 8　（任意）接続設定をイネーブルにするには、[Connection Settings] 領域をクリックして開き、次のオプションを 1 つ以上設定します。

（注）　これらの値は、セキュリティ ポリシー ルールを使用しても設定できます（「接続の設定」（P.27-6）を参照）。これらのオプションを両方に設定した場合、セキュリティ アプライアンスは低い方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

- [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  - 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
  - セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
  - セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
- [Maximum TCP Connections] : TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum UDP Connections] : UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが､TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

ステップ 9　[OK] をクリックします。

スタティック ポリシー NAT、スタティック ポリシー PAT、またはスタティック ポリシー アイデンティティ NAT の設定

スタティック ポリシー NAT、スタティック ポリシー PAT、またはスタティック ポリシー アイデンティティ NAT を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインで、[Add] > [Advanced] > [Add Static Policy NAT Rule] を選択します。

[Add Static Policy NAT Rule] ダイアログボックスが表示されます。

ステップ 2　[Original] 領域で、[Interface] ドロップダウン リストから、変換対象の実際のアドレスを持つホストに接続するインターフェイスを選択します。

ステップ 3　[Source] フィールドに実際のアドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

ステップ 4　[Destination] フィールドに宛先アドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

宛先アドレスが複数ある場合はカンマで区切ります。

デフォルトでは、フィールドには任意の宛先アドレスを許可する **any** が表示されています。

ステップ 5　[Translated] 領域で、[Interface] ドロップダウン リストから、マッピング アドレスを使用するインターフェイスを選択します。

ステップ 6　マッピング IP アドレスを指定するには、次のいずれかをクリックします。

- Use IP Address

  IP アドレスを入力するか、[...] ボタンをクリックして ASDM ですでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。
- Use Interface IP Address

実際のアドレスとマッピング アドレスのサブネット マスクは同じである必要があります。

ステップ 7　（任意）スタティック PAT を使用するには、[Enable Port Address Translation (PAT)] をオンにします。

a.　[Protocol] では、[TCP] または [UDP] をクリックします。

b.　[Original Port] フィールドで、実際のポート番号を入力します。

c.　[Translated Port] フィールドで、マッピング ポート番号を入力します。

ステップ 8　（任意）[Description] フィールドに説明を入力します。

ステップ 9　（任意）DNS 応答内部のアドレスの変換をイネーブルにするには、[Connection Settings] 領域をクリックして開き、[Translate the DNS replies that match the translation rule] をオンにします。

NAT ルールに DNS サーバ内にエントリを持つホストの実際のアドレスが含まれており、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一方には実際のアドレスが必要です。このオプションは、クライアントに送信される DNS 応答内のアドレスを書き換えます。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。

ステップ 10　（任意）接続設定をイネーブルにするには、[Connection Settings] 領域をクリックして開き、次のオプションを 1 つ以上設定します。

（注）　これらの値は、セキュリティ ポリシー ルールを使用しても設定できます（「接続の設定」（P.27-6）を参照）。これらのオプションを両方に設定した場合、セキュリティ アプライアンスは低い方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

- [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  - 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
  - セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
  - セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
- [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが､TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

ステップ 11　[OK] をクリックします。

NAT 免除の使用

NAT 除外ではアドレスを変換処理から除外して、実ホストとリモート ホストの両方で接続を開始できるようにします。NAT 免除では、免除対象の実際のトラフィックを決定するときに実際のアドレスと宛先アドレスを指定できるので（ポリシー NAT と同様）、NAT 免除を使用するとダイナミック アイデンティティ NAT よりも詳細に制御が可能です。ただし、ポリシー NAT とは異なり、NAT 免除ではポートは考慮されません。ポートを考慮するには、スタティック ポリシー アイデンティティ NAT を使用してください。

NAT 免除の詳細については、「NAT 制御がイネーブルな状態での NAT のバイパス」（P.25-10）を参照してください。

NAT 免除を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインから、[Add] > [Add NAT Exempt Rule] を選択します。

[Add NAT Exempt Rule] ダイアログボックスが表示されます。

ステップ 2　[Action: Exempt] をクリックします。

ステップ 3　[Original] 領域で、[Interface] ドロップダウン リストから、免除対象の実際のアドレスを持つホストに接続するインターフェイスを選択します。

ステップ 4　[Source] フィールドに実際のアドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

（注）　免除対象外のアドレスは後で指定できます。たとえば、免除対象のサブネット（10.1.1.0/24 など）を指定できますが、10.1.1.50 を変換する必要がある場合は、そのアドレスについて免除を除外する別のルールを作成できます。

実際のアドレスが複数ある場合はカンマで区切ります。

ステップ 5　[Destination] フィールドに宛先アドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

宛先アドレスが複数ある場合はカンマで区切ります。

デフォルトでは、フィールドには任意の宛先アドレスを許可する **any** が表示されています。

ステップ 6　[NAT Exempt Direction] 領域で、低位のセキュリティ インターフェイス（デフォルト）と高位のセキュリティ インターフェイスのどちらに向かうトラフィックを免除対象とするかを、該当するオプション ボタンをクリックして選択します。

ステップ 7　（任意）[Description] フィールドに説明を入力します。

ステップ 8　[OK] をクリックします。

ステップ 9　（任意）NAT 免除ルールに含まれていた一部のアドレスを免除対象外とする場合、免除を削除する別のルールを作成します。既存の NAT Exempt ルールを右クリックし、[Insert] を選択します。

[Add NAT Exempt Rule] ダイアログボックスが表示されます。

a.　[Action: Do not exempt] をクリックします。

b.　ステップ 3 ～ 8 を実行してルールを完成させます。

No Exempt ルールが Exempt ルールの前に追加されます。Exempt ルールと No Exempt ルールの順序は重要です。セキュリティ アプライアンスがパケットを免除するかどうか判断するとき、セキュリティ アプライアンスは、ルールが並んでいる順序に従い、パケットをそれぞれの NAT Exempt ルールと No Exempt ルールについて検証します。いずれかのルールに合致した場合、それ以降のルールはチェックされません。

[NAT] フィールドの説明

この項では、[NAT] 画面のフィールドについて説明します。次の項目を取り上げます。

- 「NAT Rules」（P.25-34）

- 「Add/Edit Static NAT Rule」（P.25-37）
- 「Add/Edit Dynamic NAT Rule」（P.25-39）
- 「Manage Global Pool」（P.25-40）
- 「Add/Edit Global Address Pool」（P.25-41）
- 「Add/Edit Static Policy NAT Rule」（P.25-41）
- 「Add/Edit Dynamic Policy NAT Rule」（P.25-43）
- 「Add/Edit NAT Exempt Rule」（P.25-45）

NAT Rules

フィールド

メニュー項目：

- [Add]：新しい NAT ルールを追加します。ドロップダウン リストから追加するルールのタイプを選択します。
  - [Add Static NAT Rule]：スタティック NAT ルール、スタティック PAT ルール、またはスタティック アイデンティティ NAT ルールを追加します。
  - [Add Dynamic NAT Rule]：ダイナミック NAT ルール、ダイナミック PAT ルール、またはアイデンティティ NAT ルールを追加します。
  - [Add NAT Exempt Rule]：NAT 免除ルールを追加します。
  - [Advanced]：ポリシー NAT ルールを追加します。

    [Add Static Policy NAT Rule]：スタティック ポリシー NAT ルール、スタティック ポリシー PAT ルール、またはスタティック ポリシー アイデンティティ NAT ルールを追加します。

    [Add Dynamic Policy NAT Rule]：ダイナミック ポリシー NAT ルールまたはダイナミック ポリシー PAT ルールを追加します。
  - [Insert]：テーブルで選択したルールの上に同じタイプの新しいルールを挿入します。
  - [Insert After]：テーブルで選択したルールの下に同じタイプの新しいルールを挿入します。
- [Edit]：NAT ルールを編集します。
- [Delete]：NAT ルールを削除します。
- [Move Up]：ルールを上に移動します。ルールは、このテーブルに表示される順序で評価されるため、重複したルールがある場合は、それらを表示する順序に注意が必要です。
- [Move Down]：ルールを下に移動します。
- [Cut]：ルールを切り取ります。
- [Copy]：ルールのパラメータをコピーします。[Paste] ボタンを使用すれば、それと同じパラメータを持つルールを新たに作成できます。
- [Paste]：ルールからコピーしたパラメータまたは切り取ったパラメータがあらかじめ入力された状態の [Add/Edit Rule] ダイアログボックスが表示されます。このダイアログボックスでは、それらのパラメータを修正して新しいルールを作成し、それをテーブルに追加できます。[Paste] ボタンをクリックすると、選択したルールのすぐ前にそのルールが追加されます。[Paste] ドロップダウン リストから [Paste After] 項目を選択すると、選択したルールのすぐ後にそのルールが追加されます。

- [Find] : 一致するルールだけを表示するように、表示内容をフィルタリングします。[Find] をクリックすると、[Filter] フィールドが開きます。もう一度 [Find] をクリックすると、[Filter] フィールドは非表示になります。
  - [Filter] ドロップダウン リスト : [Interface]、[Original Source]、[Original Service]、[Translated Interface]、[Translated Address]、[Translated Service]、[Rule Type]、[Query] の中からフィルタ基準を選択します。ルール クエリーとは、複数の基準を 1 つにまとめたもので、保存しておけば繰り返し使用できます。
  - [Condition] ドロップダウン リスト : 基準が [Original Source] または [Translate Address] の場合、条件を [is] または [contains] から選択します。他のすべての基準では、[is] 条件を使用します。
  - [Filter] フィールド : [Interface] タイプが選択された場合、このフィールドはドロップダウン リストになり、そこからインターフェイス名を選択できます。[Rule] タイプの場合、ドロップダウン リストには [Exempt]、[Static]、および [Dynamic] が含まれます。[Query] タイプの場合、このドロップダウン リストには、すべての定義済みルール クエリーが含まれます。[Original Source] タイプおよび [Translated Address] タイプには、IP アドレスを指定できます。手動で入力できるほか、[...] ボタンをクリックし、[Browse Address] ダイアログボックスを開いて参照することもできます。[Translated Service] タイプには、複数のプロトコル タイプを指定できます。手動で入力できるほか、[...] ボタンをクリックし、[Browse Translated Service] ダイアログボックスを開いて参照することもできます。
  - [Filter] : フィルタを実行します。
  - [Clear] : [Filter] フィールドをクリアします。
  - [Define Query] : [Define Query] ダイアログボックスが表示されます。このダイアログボックスでは、名前付きルール クエリーを管理できます。
- [Diagram] : ルール テーブルの下に [Rule Flow Diagram] 領域が表示されます。この図には、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクションが表示されます。
- [Packet Trace] : 選択したルールの特性とともにパラメータがあらかじめ入力されたパケット トレーサ ツールを開きます。

[NAT Rules] テーブル :

カラムの内容を編集する場合は、テーブル セルをダブルクリックします。カラム ヘッダーをダブルクリックすると、選択されたカラムをソート キーとして、テーブルが英数字の昇順でソートされます。ルールを右クリックすると、上記のボタンで選択できるすべてオプションのほか、[Insert] 項目および [Insert After] 項目が表示されます。[Insert] 項目を指定すると、選択したルールのすぐ前に新しいルールが挿入され、[Insert After] 項目を指定すると、選択したルールのすぐ後に新しいルールが挿入されます。

- [Real Interface Name] : NAT ルールは送信元インターフェイスごとにまとめられ、送信元インターフェイスは、変換対象となる実際のホストに接続されます。+ または - ボタンをクリックして、インターフェイスの NAT ルールを表示または非表示にできます。
- [#] : ルールの評価順序を示します。
- [Type] : 変換ルール タイプを表示します。
- [Original] : 実際のアドレスを表示します。
  - [Source] : 変換する実際のアドレスを示します。
  - [Destination] : ポリシー NAT と NAT 免除の場合は、実際のアドレスの宛先ネットワークを示します。標準 NAT の場合、表示は空白になります。
  - [Service] : スタティック PAT の場合、変換元のサービスを示します。
- [Translated] : マッピング アドレスとそれに関連付けられたインターフェイスを表示します。

  - [Interface]：マッピング インターフェイスを示します。
  - [Address]：マッピング アドレスを示します。
  - [Service]：スタティック PAT の場合、変換先のサービスを示します。
- [Options]：次の項目があります。
  - [DNS Rewrite]：NAT ルールに DNS サーバ内にエントリを持つホストの実際のアドレスが含まれており、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一方には実際のアドレスが必要です。このオプションは、クライアントに送信される DNS 応答内のアドレスを書き換えます。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。このオプションはテーブルで直接オンまたはオフにできます。
  - [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは 0 で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。
  - [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

    保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

    TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

    別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。

    セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。

    セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

    このオプションはテーブルで直接オンまたはオフにできます。
- [Description]（Policy NAT の場合のみ）：ルールの説明がある場合は、このカラムに表示されます。

その他の領域：

- [Enable traffic through the firewall without address translation]：NAT 制御をイネーブルまたはディセーブルにします。詳細については、「NAT コントロール」（P.25-5）を参照してください。
- [Addresses]：このタブでは、IP アドレス オブジェクトまたはネットワーク オブジェクト グループを追加、編集、削除、または検索できます。
- [Services]：このタブでは、サービスを追加、編集、削除、または検索できます。
- [Global Pools]：このタブでは、ダイナミック NAT コンフィギュレーションで使用されるグローバル アドレスの NAT プールを管理できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Static NAT Rule

フィールド

- [Original]：ネットワーク変換が適用される前の実際のアドレスとそれに関連付けられているインターフェイス。
  - [Interface]：実際のホストまたはネットワークがある、セキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - [Source]：ルールを適用するホストまたはネットワークの IP アドレスを指定します。

    プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
- [Translated]：マッピング インターフェイスと IP アドレスを指定できます。実際のアドレスとマッピング アドレスのサブネット マスクは同じである必要があります。
  - [Interface]：マッピング アドレスを使用するインターフェイスを設定します。
  - [IP address]：マッピング IP アドレスを設定します。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
  - [Use Interface IP address]：[Interface] ドロップダウン リストで選択したインターフェイスのインターフェイス IP アドレスとなるマッピング IP アドレスを設定します。
- [Port Address Translation (PAT)]：PAT パラメータを設定します。
  - [Enable Port Address Translation (PAT)]：スタティック PAT をイネーブルにします。
  - [Protocol]：TCP または UDP。
  - [Original Port]：ポート番号または名前を入力します。
  - [Translated Port]：ポート番号または名前を入力します。

- [Connection Settings] : [DNS Rewrite]、[Maximum Connections]、[Embryonic Limit]、および [Randomize Sequence Number] を設定できます。
  - [DNS Rewrite] : NAT ルールに DNS サーバ内にエントリを持つホストの実際のアドレスが含まれており、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一方には実際のアドレスが必要です。このオプションは、クライアントに送信される DNS 応答内のアドレスを書き換えます。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。このオプションはテーブルで直接オンまたはオフにできます。
  - [Maximum TCP Connections] : TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Maximum Embryonic Connections] : 初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。
  - [Maximum UDP Connections] : UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Randomize sequence number] : このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

    保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

    TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

    別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。

    セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。

    セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

    このオプションはテーブルで直接オンまたはオフにできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Dynamic NAT Rule

フィールド

- [Original]：ネットワーク変換が適用される前の実際のアドレスとそれに関連付けられているインターフェイス。
  - [Interface]：実際のホストまたはネットワークがある、セキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - [Source]：ルールを適用するホストまたはネットワークの IP アドレスを指定します。

    プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
- [Translated]：ダイナミック インターフェイスとグローバル アドレス プールを指定できます。
  - [Pool ID]：グローバル プールのプール ID を示します。
  - [Interface]：プール ID に関連付けられたインターフェイスを示します。
  - [Addresses Pool]：インターフェイスごとにプール内のアドレスを示します。
  - [Manage]：グローバル プールを管理します。
- [Connection Settings]：[DNS Rewrite]、[Maximum Connections]、[Embryonic Limit]、および [Randomize Sequence Number] を設定できます。
  - [DNS Rewrite]：NAT ルールに DNS サーバ内にエントリを持つホストの実際のアドレスが含まれており、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一方には実際のアドレスが必要です。このオプションは、クライアントに送信される DNS 応答内のアドレスを書き換えます。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。このオプションはテーブルで直接オンまたはオフにできます。
  - [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは 0 で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

- [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。

  セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。

  セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

  このオプションはテーブルで直接オンまたはオフにできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Manage Global Pool

フィールド

- [Add]：新しいグローバル プールを追加します。
- [Edit]：選択したグローバル プールを編集します。
- [Delete]：選択したグローバル プールを削除します。
- [Pool ID]：プール ID を示します。
- [Interface]：アドレス プールに関連付けられているインターフェイス名を表示します。
- [Addresses Pool]：プール内のアドレスを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Global Address Pool

フィールド

- [Interface]：新しいアドレス プールに関連付けるインターフェイス名を指定します。[Interface] ドロップダウン リストで名前を選択します。
- [Pool ID]：このアドレス プールを参照するためにダイナミック NAT ルールが使用する ID 番号を指定します。[Pool ID] フィールドに番号を入力します。
- [Range]：IP アドレスの範囲を新しいアドレス プールで使用することを指定するには、このオプションを選択します。このオプションを選択する場合は、次の値を指定します。
  - [Starting IP address]：範囲の開始 IP アドレスを指定します。
  - [Ending IP Address]：範囲の終了 IP アドレスを指定します。
  - [Netmask]（任意）：この値により、変換後の IP アドレスがメンバーになるネットワークのマスクを指定します。
- [Port Address Translation (PAT)]：IP アドレスが PAT で使用されることを指定するには、このオプションを選択します。このオプションを選択する場合は、次の値を指定します。
  - [IP Address]：PAT アドレスを指定します。
  - [Netmask]（任意）：この値により、変換後の IP アドレスがメンバーになるネットワークのマスクを指定します。
- [Port Address Translation (PAT) using IP address of the interface]：[Interface] ドロップダウン リストで選択したインターフェイスに割り当てられている IP アドレスを、PAT の変換後のアドレスとして使用することを指定するには、このオプションを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Static Policy NAT Rule

- [Original]：ネットワーク変換が適用される前の実際のアドレスとそれに関連付けられているインターフェイス。

- [Interface]：実際のホストまたはネットワークがある、セキュリティ アプライアンスのネットワーク インターフェイスを選択します。
- [Source]：ルールを適用するホストまたはネットワークの IP アドレスを指定します。

  プレフィックス/長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。
- [...]：ASDM ですでに定義されている IP アドレスを選択できます。
- [Destination]：宛先アドレスを指定します。

  プレフィックス/長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

  宛先アドレスが複数ある場合はカンマで区切ります。

  デフォルトでは、フィールドには任意の宛先アドレスを許可する **any** が表示されています。
- [...]：ASDM ですでに定義されている IP アドレスを選択できます。

- [Translated]：マッピング インターフェイスと IP アドレスを指定できます。実際のアドレスとマッピング アドレスのサブネット マスクは同じである必要があります。
  - [Interface]：マッピング アドレスを使用するインターフェイスを設定します。
  - [Use IP address]：マッピング IP アドレスを設定します。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
  - [Use Interface IP address]：[Interface] ドロップダウン リストで選択したインターフェイスのインターフェイス IP アドレスとなるマッピング IP アドレスを設定します。
- [Port Address Translation (PAT)]：PAT パラメータを設定します。
  - [Enable Port Address Translation (PAT)]：スタティック PAT をイネーブルにします。
  - [Protocol]：TCP または UDP。
  - [Original Port]：ポート番号または名前を入力します。
  - [Translated Port]：ポート番号または名前を入力します。
- [Description]：このルールの説明を設定します。
- [Connection Settings]：[DNS Rewrite]、[Maximum Connections]、[Embryonic Limit]、および [Randomize Sequence Number] を設定できます。
  - [DNS Rewrite]：NAT ルールに DNS サーバ内にエントリを持つホストの実際のアドレスが含まれており、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一方には実際のアドレスが必要です。このオプションは、クライアントに送信される DNS 応答内のアドレスを書き換えます。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。このオプションはテーブルで直接オンまたはオフにできます。
  - [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは 0 で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してイン

ターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

- [Maximum UDP Connections] : UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Randomize sequence number] : このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。

  セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。

  セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

  このオプションはテーブルで直接オンまたはオフにできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Dynamic Policy NAT Rule

- [Original] : ネットワーク変換が適用される前の実際のアドレスとそれに関連付けられているインターフェイス。
  - [Interface] : 実際のホストまたはネットワークがある、セキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - [Source] : ルールを適用するホストまたはネットワークの IP アドレスを指定します。

    プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

    実際のアドレスが複数ある場合はカンマで区切ります。

  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
  - [Destination]：宛先アドレスを指定します。

    プレフィックス/長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

    宛先アドレスが複数ある場合はカンマで区切ります。

    デフォルトでは、フィールドには任意の宛先アドレスを許可する any が表示されています。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
- [Translated]：ダイナミック インターフェイスとグローバル アドレス プールを指定できます。
  - [Pool ID]：グローバル プールのプール ID を示します。
  - [Interface]：プール ID に関連付けられたインターフェイスを示します。
  - [Addresses Pool]：インターフェイスごとにプール内のアドレスを示します。
  - [Manage]：グローバル プールを管理します。
- [Description]：このルールの説明を設定します。
- [Connection Settings]：[DNS Rewrite]、[Maximum Connections]、[Embryonic Limit]、および [Randomize Sequence Number] を設定できます。
  - [DNS Rewrite]：NAT ルールに DNS サーバ内にエントリを持つホストの実際のアドレスが含まれており、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一方には実際のアドレスが必要です。このオプションは、クライアントに送信される DNS 応答内のアドレスを書き換えます。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。このオプションはテーブルで直接オンまたはオフにできます。
  - [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。
  - [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

    保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。

セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。

セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

このオプションはテーブルで直接オンまたはオフにできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit NAT Exempt Rule

フィールド

- [Action] : アドレスを免除するかどうかを設定します。
  - [Exempt] : アドレスの NAT を免除します。
  - [Do not exempt] : アドレスに対する免除を削除します。
- [Original] : NAT 免除ルール対象のアドレスを指定します。
  - [Interface] : 実際のホストまたはネットワークがある、セキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - [Source] : ホストまたはネットワークの実際の IP アドレスを指定します。

    プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

    実際のアドレスが複数ある場合はカンマで区切ります。
  - [...] : ASDM ですでに定義されている IP アドレスを選択できます。
  - [Destination] : 宛先アドレスを指定します。

    プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

    宛先アドレスが複数ある場合はカンマで区切ります。

    デフォルトでは、フィールドには任意の宛先アドレスを許可する **any** が表示されています。
  - [...] : ASDM ですでに定義されている IP アドレスを選択できます。

- [NAT Exempt Direction]：着信または発信トラフィックの NAT ルールを設定します。
  - [NAT Exempt outbound traffic from interface "*real interface*" to lower security interfaces (default)]：発信トラフィック用の NAT ルールを設定します。
  - [NAT Exempt inbound traffic from interface "*real interface*" to higher security interfaces]：着信トラフィック用の NAT ルールを設定します。
- [Description]：このルールの説明を設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 26

ARP インスペクションおよびブリッジング パラメータの設定

この章では、ARP インスペクションをイネーブルにする方法と、トランスペアレント ファイアウォール モードでセキュリティ アプライアンスのブリッジング オペレーションをカスタマイズする方法について説明します。マルチコンテキスト モードでは、この章のコマンドはセキュリティ コンテキストに入力できますが、システムには入力できません。

トランスペアレント ファイアウォール モードの詳細については、第 18 章「ファイアウォール モードの概要」を参照してください。

この章は、次の項で構成されています。

ARP インスペクションの設定

この項では、ARP インスペクションについて説明し、これをイネーブルにする方法について説明します。次の項目を取り上げます。

ARP Inspection

[ARP Inspection] ペインでは、ARP インスペクションを設定できます。

デフォルトでは、すべての ARP パケットがセキュリティ アプライアンスを通過できます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。

ARP インスペクションをイネーブルにすると、セキュリティ アプライアンスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。

- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、セキュリティ アプライアンスはパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするようにセキュリティ アプライアンスを設定できます。

（注） 専用の管理インターフェイス（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

ARP インスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングは、「中間者」攻撃をイネーブルにすることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホスト トラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

フィールド

- [Interface]：インターフェイス名を示します。
- [ARP Inspection Enabled]：ARP インスペクションがイネーブルであるかどうか（[Yes] または [No]）を示します。
- [Flood Enabled]：ARP インスペクションがイネーブルの場合、アクションが不明なパケットをフラッディングするかどうか（[Yes] または [No]）を示します。ARP インスペクションがディセーブルの場合、この値は常に [No] になります。
- [Edit]：選択したインターフェイスの ARP インスペクション パラメータを編集します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

Edit ARP Inspection Entry

[Edit ARP Inspection Entry] ダイアログボックスでは、ARP インスペクション設定値を設定できます。

フィールド

- [Enable ARP Inspection]：ARP インスペクションをイネーブルにします。

- [Flood ARP Packets]：スタティック ARP エントリのどの要素とも一致しないパケットをすべてのインターフェイス（発信元インターフェイスを除く）にフラッディングすることを指定します。MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、セキュリティ アプライアンスはパケットをドロップします。このチェックボックスをオフにすると、すべての不一致パケットがドロップされます。

（注）　デフォルト設定では、一致しないパケットはフラッドします。スタティック エントリにある ARP だけがセキュリティ アプライアンスを通過するように制限するには、このコマンドを **no-flood** に設定します。

Management 0/0 インターフェイスまたはサブインターフェイスがある場合、これらのインターフェイスは、このパラメータがフラッドに設定されていてもパケットをフラッドしません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

ARP Static Table

ホストは IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、エントリは更新される前にタイムアウトします。

（注）　トランスペアレント ファイアウォールは、セキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）に、ARP テーブルのダイナミック ARP エントリを使用します。

[ARP Static Table] パネルでは、MAC アドレスを特定のインターフェイスの IP アドレスにマッピングするスタティック ARP エントリを追加できます。スタティック ARP エントリはタイムアウトせず、ネットワーク問題の解決に役立つ場合があります。

フィールド

- [Interface]：ホスト ネットワークに接続されているインターフェイスを表示します。
- [IP Address]：ホスト IP アドレスを表示します。

- [MAC Address]：ホスト MAC アドレスを表示します。
- [Proxy ARP]：セキュリティ アプライアンスがこのアドレスでプロキシ ARP を実行するかどうかを示します。セキュリティ アプライアンスは、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。
- [Add]：スタティック ARP エントリを追加します。
- [Edit]：スタティック ARP エントリを編集します。
- [Delete]：スタティック ARP エントリを削除します。
- [ARP Timeout]：セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を、60 ～ 4294967 秒の範囲で設定します。デフォルトは 14400 秒です。ARP テーブルを再構築すると、自動的に新しいホスト情報が更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることが必要になる場合があります。このパラメータは [Static ARP Table] パネルに表示されますが、タイムアウトはダイナミック ARP テーブルに適用されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit ARP Static Configuration

[Add/Edit ARP Static Configuration] ダイアログボックスでは、スタティック ARP エントリを追加または編集できます。

フィールド

- [Interface]：ホスト ネットワークに接続されているインターフェイスを設定します。
- [IP Address]：ホスト IP アドレスを設定します。
- [MAC Address]：ホスト MAC アドレス（00e0.1e4e.3d8b など）を設定します。
- [Proxy ARP]：セキュリティ アプライアンスがこのアドレスでプロキシ ARP を実行できるようにします。セキュリティ アプライアンスは、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

MAC アドレス テーブルのカスタマイズ

ここでは、MAC アドレス テーブルについて説明します。内容は次のとおりです。

MAC Address Table

[MAC Address Table] ペインでは、スタティック MAC アドレス エントリを追加できます。通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。スタティック MAC アドレスは、必要に応じて MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、セキュリティ アプライアンスはトラフィックをドロップし、システム メッセージを生成します。スタティック ARP エントリを追加するときに（「ARP Static Table」（P.26-3）を参照）、スタティック MAC アドレス エントリは MAC アドレス テーブルに自動的に追加されます。

セキュリティ アプライアンスは、通常のブリッジやスイッチと同様の方法で、MAC アドレス テーブルをラーニングし、構築します。デバイスがセキュリティ アプライアンス経由でパケットを送信すると、セキュリティ アプライアンスはこの MAC アドレスをテーブルに追加します。テーブルで MAC アドレスと発信元インターフェイスが関連付けられているため、セキュリティ アプライアンスは、パケットが正しいインターフェイスからデバイスにアドレス指定されていることがわかります。

ASA 5505 適応型セキュリティ アプライアンスには、組み込みスイッチがあります。このスイッチの MAC アドレス テーブルは、各 VLAN 内のトラフィックの MAC アドレスとスイッチ ポートのマッピングを維持します。この項では、VLAN 間のトラフィックの MAC アドレスと VLAN インターフェイスのマッピングを維持する、ブリッジの MAC アドレス テーブルについて説明します。

セキュリティ アプライアンスはファイアウォールなので、パケットの宛先 MAC アドレスがテーブルにない場合、セキュリティ アプライアンスは通常のブリッジとは異なり、元のパケットをすべてのインターフェイスにフラッドすることはありません。代わりに、直接接続されたデバイスまたはリモート デバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット：セキュリティ アプライアンスは宛先 IP アドレスに対して ARP 要求を生成し、セキュリティ アプライアンスは ARP 応答を受信したインターフェイスをラーニングします。
- リモート デバイスへのパケット：セキュリティ アプライアンスは宛先 IP アドレスへの ping を生成し、セキュリティ アプライアンスは ping 応答を受信したインターフェイスをラーニングします。

元のパケットはドロップされます。

フィールド

- [Interface]：MAC アドレスに関連付けられたインターフェイスを表示します。
- [MAC Address]：MAC アドレスを表示します。
- [Add]：スタティック MAC アドレス エントリを追加します。
- [Edit]：スタティック MAC アドレス エントリを編集します。
- [Delete]：スタティック MAC アドレス エントリを削除します。

- [Dynamic Entry Timeout]：タイムアウトするまで MAC アドレス エントリが MAC アドレス テーブルにとどまることができる時間を設定します。有効な値は、5 ～ 720 分（12 時間）です。5 分がデフォルトです。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

Add/Edit MAC Address Entry

[Add/Edit MAC Address Entry] ダイアログボックスでは、スタティック MAC アドレス エントリを追加または編集できます。通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、セキュリティ アプライアンスはトラフィックをドロップし、システム メッセージを生成します。

フィールド

- [Interface Name]：MAC アドレスに関連付けられたインターフェイスを設定します。
- [MAC Address]：MAC アドレスを設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

MAC ラーニング

[MAC Learning] ペインでは、インターフェイスでの MAC アドレス ラーニングをディセーブルにすることができます。デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、セキュリティ アプライアンスは対応するエントリを MAC アドレス テーブルに追加します。必要に応じて MAC アドレス ラーニングをディセーブルにできますが、この場合、MAC アドレスをテーブルにスタティックに追加しないと、トラフィックがセキュリティ アプライアンスを通過できなくなります。

フィールド

- [Interface]：インターフェイス名を表示します。
- [MAC Learning Enabled]：MAC ラーニングがイネーブルであるかどうか（[Yes] または [No]）を示します。
- [Enable]：選択したインターフェイスでの MAC ラーニングをイネーブルにします。
- [Disable]：選択したインターフェイスでの MAC ラーニングをディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

CHAPTER 27

高度なファイアウォール保護の設定

この章では、保護機能を設定することによってネットワーク攻撃を防止する方法を説明します。この章には、次の項があります。

（注） [Configuration] > [Firewall] > [Advanced] 領域で設定する、Sun RPC サーバと暗号化トラフィック検査の設定値（およびこの章に含まれる多くの項目）については、第 24 章「アプリケーション レイヤ プロトコル インスペクションの設定」を参照してください。

脅威検出の設定

この項では、スキャン脅威検出と基本脅威検出を設定する方法について説明します。説明する内容は次のとおりです。脅威検出はシングル モードだけで使用できます。

この項では、次のトピックについて取り上げます。

脅威検出の統計情報を表示するには、「[Firewall Dashboard] タブ」（P.1-17）を参照してください。

基本脅威検出の設定

基本脅威検出では、DoS 攻撃のような攻撃に関連している可能性があるアクティビティを検出します。基本脅威検出は、デフォルトでイネーブルになっています。

この項では、次のトピックについて取り上げます。

基本脅威検出の概要

セキュリティ アプライアンスは、基本脅威検出を使用して、次の理由でドロップしたパケットおよびセキュリティ イベントの割合を監視します。

- アクセス リストによる拒否
- 不正なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）
- 接続制限の超過（システム全体のリソース制限とコンフィギュレーションで設定されている制限の両方）
- DoS 攻撃の検出（無効な SPI、ステートフル ファイアウォール検査の不合格など）
- 基本ファイアウォール検査の不合格（このオプションは、ここに列挙されているファイアウォール関連のパケット ドロップすべてを含む総合レートです。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません）
- 疑わしい ICMP パケットの検出
- アプリケーション インスペクションに不合格のパケット
- インターフェイスの過負荷
- 検出されたスキャン攻撃（このオプションでは、スキャン攻撃をモニタします。たとえば、最初の TCP パケットが SYN パケットでないことや、TCP 接続で 3 ウェイ ハンドシェイクに失敗することなどです。フル スキャン脅威検出（「スキャン脅威検出の設定」（P.27-3）を参照）では、このスキャン攻撃レート情報を収集し、ホストを攻撃者として分類して自動的に排除することによって対処します）
- 不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）

セキュリティ アプライアンスは、脅威を検出するとただちにシステム ログ メッセージ（730100）を送信します。

基本脅威検出は、ドロップや潜在的な脅威があった場合に限りパフォーマンスに影響を与えます。この状況でも、パフォーマンスへの影響は大きくありません。

基本脅威検出の設定

基本脅威検出をイネーブルまたはディセーブルにするには、[Configuration] > [Firewall] > [Threat Detection] ペインで、[Enable Basic Threat Detection] チェックボックスをオンまたはオフにします。

このオプションはデフォルトで、パケット ドロップや不完全なセッションの検出など、特定のタイプのセキュリティ イベントの検出をイネーブルにします。必要に応じて、各イベント タイプのデフォルト設定を上書きできます。

イベント レートが超過すると、セキュリティ アプライアンスはシステム メッセージを送信します。セキュリティ アプライアンスは、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト レート間隔は、平均レート間隔の 1/60 と 10 秒のうち、いずれか大きいほうです。セキュリティ アプライアンスは、受信するイベントごとに平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、セキュリティ アプライアンスは、バースト期間におけるレート タイプごとに最大 1 つのメッセージの割合で 2 つの別々のシステム メッセージを送信します。

表 27-1 に、デフォルト設定を示します。

表 27-1　基本脅威検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	平均レート	バースト レート
• DoS 攻撃の検出 • 不正なパケット形式 • 接続制限の超過 • 疑わしい ICMP パケットの検出	直前の 600 秒間で 100 ドロップ / 秒。	直前の 10 秒間で 400 ドロップ / 秒。
	直前の 3600 秒間で 80 ドロップ / 秒。	直近の 320 秒間で 60 ドロップ / 秒。
スキャン攻撃の検出	直前の 600 秒間で 5 ドロップ / 秒。	直前の 10 秒間で 10 ドロップ / 秒。
	直前の 3600 秒間で 4 ドロップ / 秒。	直近の 60 秒間で 8 ドロップ / 秒。
不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）（複合）	直前の 600 秒間で 100 ドロップ / 秒。	直前の 10 秒間で 200 ドロップ / 秒。
	直前の 3600 秒間で 80 ドロップ / 秒。	直近の 60 秒間で 160 ドロップ / 秒。
アクセス リストによる拒否	直前の 600 秒間で 400 ドロップ / 秒。	直前の 10 秒間で 800 ドロップ / 秒。
	直前の 3600 秒間で 320 ドロップ / 秒。	直近の 60 秒間で 640 ドロップ / 秒。
• 基本ファイアウォール検査に不合格	直前の 600 秒間で 400 ドロップ / 秒。	直前の 10 秒間で 1600 ドロップ / 秒。
• アプリケーション インスペクションに不合格のパケット	直前の 3600 秒間で 320 ドロップ / 秒。	直近の 60 秒間で 1280 ドロップ / 秒。
インターフェイスの過負荷	直前の 600 秒間で 2000 ドロップ / 秒。	直前の 10 秒間で 8000 ドロップ / 秒。
	直前の 3600 秒間で 1600 ドロップ / 秒。	直近の 60 秒間で 6400 ドロップ / 秒。

スキャン脅威検出の設定

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、セキュリティ アプライアンス のスキャンによる脅威の検出機能では、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、アクティビティを返さない接続、閉じられているサービス ポートへのアクセス、非ランダム IPID などの脆弱な TCP の動作、およびその他の疑わしいアクティビティを追跡します。

攻撃者に関するシステム ログ メッセージを送信するように セキュリティ アプライアンス を設定したり、自動的にホストを排除したりできます。

注意　スキャン脅威検出機能は、ホストベースとサブネットベースのデータ構造と情報を作成および収集する間、セキュリティ アプライアンスのパフォーマンスとメモリに大きな影響を与える可能性があります。

スキャン脅威検出を設定するには、次の手順を実行します。

ステップ 1　スキャン脅威検出をイネーブルにするには、[Configuration] > [Firewall] > [Threat Detection] ペインで、[Enable Scanning Threat Detection] チェックボックスをオンにします。

デフォルトでは、ホストが攻撃者として識別されると、システム ログ メッセージ 730101 が生成されます。

セキュリティ アプライアンスは、スキャン脅威レートが超過すると、ホストを攻撃者またはターゲットとして特定します。セキュリティ アプライアンスは、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト イベント レートは、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の値です。スキャン攻撃の一部と見なされるイベントが検出されるたびに、セキュリティ アプライアンスは平均レート制限とバースト レート制限をチェックします。ホストから送信されるトラフィックがどちらかのレートを超えると、そのホストは攻撃者と見なされます。ホストが受信したトラフィックがどちらかのレートを超えると、そのホストはターゲットと見なされます。

表 27-2 に、スキャン脅威検出のデフォルトのレート制限を示します。

表 27-2　スキャンによる脅威の検出のデフォルトのレート制限

平均レート	バースト レート
直前の 600 秒間で 5 ドロップ/秒。	直前の 10 秒間で 10 ドロップ/秒。
直前の 3600 秒間で 5 ドロップ/秒。	直前の 60 秒間で 10 ドロップ/秒。

ステップ 2　（任意）ホストが セキュリティ アプライアンス によって攻撃者と判定された場合に自動的にそのホスト接続を終了するには、[Shun Hosts detected by scanning threat] チェックボックスをオンにします。

ステップ 3　（任意）ホストの IP アドレスを排除対象から外すには、[Networks excluded from shun] フィールドにアドレスを入力します。

複数のアドレスまたはサブネットは、カンマで区切って入力できます。IP アドレス オブジェクトのリストからネットワークを選択するには、[...] ボタンをクリックします。

脅威統計情報の設定

広範な統計情報を収集するようにセキュリティ アプライアンスを設定することができます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。デフォルトでは、アクセス リストの統計情報はイネーブルになっています。

脅威検出の統計情報を表示するには、「[Firewall Dashboard] タブ」（P.1-17）を参照してください。

注意　統計情報をイネーブルにすると、イネーブルにする統計情報のタイプに応じて、セキュリティ アプライアンスのパフォーマンスが影響を受けます。ホストの統計情報をイネーブルにすると、パフォーマンスに大きな影響があります。トラフィックの負荷が高い場合は、このタイプの統計情報は一時的にイネーブルにすることを検討してください。ポートの統計情報をイネーブルにしても影響はそれほどありません。

- すべての統計情報をイネーブルにするには、[Configuration] > [Firewall] > [Threat Detection] ペインで、[Enable All Statistics] オプション ボタンをオンにします。
- すべての統計情報をディセーブルにするには、[Configuration] > [Firewall] > [Threat Detection] ペインで、[Disable All Statistics] オプション ボタンをオンにします。
- 特定の統計情報だけをイネーブルにするには、[Configuration] > [Firewall] > [Threat Detection] ペインで、[Enable Only Following Statistics] オプション ボタンをオンにし、次のチェックボックスの中から 1 つ以上をオンにします。
  - [Hosts] : ホスト統計情報をイネーブルにします。ホストがアクティブで、スキャン脅威ホスト データベース内に存在する限り、ホスト統計情報は累積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます（統計情報もクリアされます）。
  - [Access Rules]（デフォルトでイネーブル）：アクセス ルールの統計情報をイネーブルにします。
  - [Port] : TCP/UDP ポートの統計情報をイネーブルにします。
  - [Protocol] : TCP/UDP 以外の IP プロトコルの統計情報をイネーブルにします。

[Threat Detection] フィールドの説明

[Threat Detection] ペインでは、基本脅威検出およびスキャン脅威検出を設定できます。

フィールド

- [Basic Threat Detection] : 基本脅威検出では、DoS 攻撃のような攻撃に関連している可能性があるアクティビティを検出します。基本脅威検出は、デフォルトでイネーブルになっています。
  - [Enable Basic Threat Detection] : 基本脅威検出をイネーブルにします。詳細については、「基本脅威検出の設定」（P.27-1）を参照してください。
- [Scanning Threat Detection] : スキャン脅威検出機能は、いつホストがスキャンを実行するかを決定します。
  - [Enable Scanning Threat Detection] : スキャン脅威検出をイネーブルにします。詳細については、「スキャン脅威検出の設定」（P.27-3）を参照してください。
  - [Shun Hosts detected by scanning threat] : セキュリティ アプライアンスがホストを攻撃者として識別すると自動的にホスト接続を終了します。

    [Networks excluded from shun] : ホスト IP アドレスを回避対象から除外します。複数のアドレスまたはサブネットは、カンマで区切って入力できます。IP アドレス オブジェクトのリストからネットワークを選択するには、[...] ボタンをクリックします。
- [Scanning Threat Statistics] : セキュリティ アプライアンスが広範な統計情報を収集できるようにします。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。デフォルトでは、アクセス リストの統計情報はイネーブルになっています。脅威検出の統計情報を表示するには、「[Firewall Dashboard] タブ」（P.1-17）を参照してください。

注意 統計情報をイネーブルにすると、イネーブルにする統計情報のタイプに応じて、セキュリティ アプライアンスのパフォーマンスが影響を受けます。ホストの統計情報をイネーブルにすると、パフォーマンスに大きな影響があります。トラフィックの負荷が高い場合は、このタイプの統計情報は一時的にイネーブルにすることを検討してください。ポートの統計情報をイネーブルにしても影響はそれほどありません。

- [Disable All Statistics]：すべての統計情報をディセーブルにします。
- [Enable All Statistics]：すべての統計情報をイネーブルにします。
- [Enable only following statistics]：特定の統計情報をイネーブルにします。

  [Hosts]：ホスト統計情報をイネーブルにします。ホストがアクティブで、スキャン脅威ホスト データベース内に存在する限り、ホスト統計情報は累積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます（統計情報もクリアされます）。

  [Access Rules]（デフォルトでイネーブル）：アクセス ルールの統計情報をイネーブルにします。

  [Port]：TCP/UDP ポートの統計情報をイネーブルにします。

  [Protocol]：TCP/UDP 以外の IP プロトコルの統計情報をイネーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

接続の設定

この項では、TCP と UDP の最大接続数、最大初期接続数、クライアントあたりの最大接続数、接続タイムアウト、デッド接続検出を設定する方法、および TCP シーケンスのランダム化をディセーブルにする方法について説明します。この項では、TCP 正規化を設定する方法についても説明します。TCP 正規化によって、異常なパケットを識別する基準を指定できます。セキュリティ アプライアンスは、異常なパケットが検出されるとそれらをドロップします。

この項では、次のトピックについて取り上げます。

- 「接続制限値の概要」（P.27-7）
- 「接続設定と TCP 正規化のイネーブル化」（P.27-8）

（注） NAT コンフィギュレーションで最大接続数、最大初期接続数、および TCP シーケンス ランダム化を設定することもできます。両方の方法を使用して同じトラフィックにこれらの設定を行う場合は、セキュリティ アプライアンスは低い方の制限を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

接続制限値の概要

この項では、接続を制限する目的について説明します。次の項目を取り上げます。

TCP 代行受信の概要

初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、クライアントあたりの制限値と初期接続の制限を利用して TCP 代行受信を開始します。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。TCP 代行受信では、SYN クッキー アルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、セキュリティ アプライアンスはサーバのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。セキュリティ アプライアンスがクライアントから ACK を受信すると、クライアントを認証し、サーバへの接続を許可できます。

クライアントレス SSL VPN の互換性を目的とした管理パケットの TCP 代行受信のディセーブル化

デフォルトでは、TCP 管理接続では TCP 代行受信が常にイネーブルになっています。TCP 代行受信は、イネーブルになると 3 ウェイ TCP 接続確立ハンドシェイク パケットを代行受信するため、セキュリティ アプライアンスはクライアントレス（ブラウザベースの）SSL VPN からのパケットを処理できなくなります。クライアントレス SSL VPN では、3 ウェイ ハンドシェイク パケットを処理し、選択的な ACK とクライアントレス SSL VPN 接続への TCP オプションを提供できなければなりません。管理トラフィックの TCP 代行受信をディセーブルにするには、初期接続制限を設定します。初期接続制限に達した後にだけ TCP 代行受信をイネーブルにできます。

デッド接続検出の概要

デッド接続検出（DCD）では、デッド接続を検出し、トラフィックをまだ処理できる接続を期限切れにすることなく、デッド接続を期限切れにできます。DCD は、アイドル状態でも有効な接続を維持する場合に設定します。

DCD をイネーブルにすると、アイドル タイムアウト動作が変化します。アイドル タイムアウトになると、DCD プローブが 2 つのエンドホストそれぞれに送信され、接続の有効性が判断されます。設定された間隔でプローブが送信された後にエンドホストが応答を返さないと、その接続は解放され、リセット値が設定されていれば各エンドホストに送信されます。両方のエンドホストが応答して接続の有効性が確認されると、アクティビティ タイムアウトが現在の時間に更新され、それに応じてタイムアウトが再スケジュールされます。

TCP シーケンスランダム化概要

それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

- 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
- セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
- セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

接続設定と TCP 正規化のイネーブル化

接続設定値と TCP 正規化を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] ペインで、第 23 章「サービス ポリシー ルールの設定」に従ってサービス ポリシーを設定します。

新しいサービス ポリシー ルールの一部として接続制限を設定できます。または、既存のサービス ポリシーを編集することもできます。

ステップ 2　[Rule Actions] ダイアログボックスで、[Connection Settings] タブをクリックします。

ステップ 3　最大接続数を設定するには、[Maximum Connections] 領域で次の値を設定します。

- [TCP & UDP Connections]：トラフィック クラスのすべてのクライアントで同時に接続される TCP および UDP 接続の最大数を 65,536 までの範囲で指定します。どちらのプロトコルともデフォルトは **0** で、接続可能な最大許容数に設定されています。
- [Embryonic Connections]：ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。
- [Per Client Connections]：クライアントごとに、同時接続できる TCP 接続と UDP 接続の最大数を指定します。クライアントあたりの最大接続数の接続をすでに開いているクライアントが新しい接続を試みると、セキュリティ アプライアンスは、その接続を拒否してパケットをドロップします。
- [Per Client Embryonic Connections]：クライアントごとに、同時接続できる TCP 初期接続の最大数を指定します。クライアントあたりの最大初期接続数の接続をセキュリティ アプライアンスからすでに開いているクライアントが新しい TCP 接続を要求すると、セキュリティ アプライアンスは、その要求の処理を TCP 代行受信機能に代行させ、接続を阻止します。

ステップ 4　TCP タイムアウトを設定するには、[TCP Timeout] 領域で次の値を設定します。

- [Connection Timeout]：接続スロットを解放するまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。この期間は 5 分以上にする必要があります。デフォルトは **1 時間**です。
- [Send reset to TCP endpoints before timeout]：セキュリティ アプライアンスが、接続スロットを解放する前に接続のエンドポイントに TCP リセット メッセージを送信するように指定します。
- [Embryonic Connection Timeout]：初期接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。デフォルトは **30 秒**です。
- [Half Closed Connection Timeout]：ハーフ クローズ接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。この期間は 5 分以上にする必要があります。デフォルトは **10 分**です。

ステップ 5　シーケンス番号のランダム化をディセーブルにするには、[Randomize Sequence Number] をオフにします。

別のインライン ファイアウォールで TCP イニシャル シーケンス番号のランダム化をイネーブルにしている場合は、そのランダム化をディセーブルにできます。2 つのファイアウォールで同じ動作を実行する必要はないからです。ただし、両方のファイアウォールで ISN ランダム化をイネーブルにしたままにしてもトラフィックには影響しません。

それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスでは、発信方向に通過する TCP SYN の ISN をランダム化します。同一セキュリティ レベルの 2 つのインターフェイス間の接続の場合、ISN は双方向の SYN でランダム化されます。

保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

ステップ 6　TCP 正規化を設定するには、[Use TCP Map] をオンにします。

ドロップダウン リストから既存の TCP マップを選択するか（選択可能な場合）、[New] をクリックして新しい TCP マップを追加します。

[Add TCP Map] ダイアログボックスが表示されます。

a. [TCP Map Name] フィールドで、名前を入力します。

b. [Queue Limit] フィールドで、異常なパケットの最大数を 0 ～ 250 の範囲で指定します。

c. [Reserved Bits] 領域で、[Clear and allow]、[Allow only]、または [Drop] をクリックします。

[Allow only] を指定すると、TCP ヘッダーに予約ビットのあるパケットだけが許可されます。

[Clear and allow] を指定すると、TCP ヘッダーの予約ビットをクリアしてパケットを許可します。

[Drop] を指定すると、TCP ヘッダーに予約ビットのあるパケットをドロップします。

d. 次のいずれかのオプションをオンにします。

- [Clear Urgent Flag]：セキュリティ アプライアンスを通じて URG ポインタを許可またはクリアします。
- [Drop Connection on Window Variation]：予想外のウィンドウ サイズの変更が発生した接続をドロップします。
- [Drop Packets that Exceed Maximum Segment Size]：ピアで設定した MSS を超過したパケットを許可またはドロップします。
- [Check if transmitted data is the same as original]：再送信データ チェックをイネーブルおよびディセーブルにします。
- [Drop SYN Packets With Data]：データを持つ SYN パケットを許可またはドロップします。

- [Enable TTL Evasion Protection]：セキュリティ アプライアンスの TTL 回避保護をイネーブルまたはディセーブルにします。
- [Verify TCP Checksum]：チェックサム検証をイネーブルおよびディセーブルにします。

e. TCP オプションを設定するには、次のいずれかのオプションをオンにします。

- [Clear Selective Ack]：[selective-ack TCP] オプションを許可するかクリアするかを示します。
- [Clear TCP Timestamp]：TCP タイムスタンプ オプションを許可するかクリアするかを示します。
- [Clear Window Scale]：ウィンドウ スケール タイムスタンプ オプションを許可するかクリアするかを示します。
- [Range]：有効な TCP オプションの範囲を示します。正しい範囲は 6 ～ 7 と 9 ～ 255 です。下限境界値は上限境界値以下でなければなりません。

f. [OK] をクリックします。

ステップ 7　存続可能時間を設定するには、[Decrement time to live for a connection] をオンにします。

ステップ 8　[OK] または [Finish] をクリックします。

IP 監査の設定

IP 監査機能は、基本的な IPS 機能を提供します。サポートされるプラットフォームで高度な IPS 機能を実現する場合には、AIP SSM をインストールできます。

この機能により、名前付き監査ポリシーを作成し、パケットが事前定義済みの攻撃シグニチャまたは情報シグニチャと一致する場合に実行するアクションを特定できます。シグニチャは、既知の攻撃パターンに一致するアクティビティです。たとえば、DoS 攻撃に一致するシグニチャがあります。セキュリティ アプライアンスは、パケットをドロップ、アラームを生成、または接続をリセットするように設定できます。

IP Audit Policy

[IP Audit Policy] パネルでは、監査ポリシーを追加し、そのポリシーをインターフェイスに割り当てられます。攻撃ポリシーと情報ポリシーは、各インターフェイスに割り当てられます。攻撃ポリシーにより、パケットが攻撃シグニチャに一致するときに実行するアクションが決まります。そのパケットは、DoS 攻撃など、ネットワークでの攻撃の一部である可能性があります。情報ポリシーにより、パケットが情報シグニチャに一致するときに実行するアクションが決まります。そのパケットは、現時点ではネットワークを攻撃していなくても、ポート スイープなどの情報収集アクティビティの一部になる可能性があります。すべてのシグニチャのリストについては、IP 監査のシグニチャ リストを参照してください。

フィールド

- [Name]：定義済み IP 監査ポリシーの名前を示します。このテーブルには名前付きポリシーのデフォルト アクションが一覧表示されていますが（「--Default Action--」）、インターフェイスに割り当てることができる名前付きポリシーではありません。デフォルト アクションは、ポリシーでアクションを設定しない場合に、名前付きポリシーによって使用されます。デフォルト アクションを変更するには、そのアクションを選択して [Edit] ボタンをクリックします。
- [Type]：ポリシー タイプ（[Attack] または [Info]）を示します。

- [Action]：ポリシーに一致するパケットに対して実行されるアクション（[Alarm]、[Drop]、または [Reset]）を示します。複数のアクションが一覧表示されることもあります。
- [Add]：新しい IP 監査ポリシーを追加します。
- [Edit]：IP 監査ポリシーまたはデフォルト アクションを編集します。
- [Delete]：IP 監査ポリシーを削除します。デフォルト アクションは削除できません。
- [Policy-to-Interface Mappings]：攻撃および情報ポリシーを各インターフェイスに割り当てます。
  - [Interface]：インターフェイス名を表示します。
  - [Attack Policy]：使用できる攻撃監査ポリシー名を一覧表示します。リストにある名前をクリックして、ポリシーをインターフェイスに割り当てます。
  - [Info Policy]：使用できる情報監査ポリシー名を一覧表示します。リストにある名前をクリックして、ポリシーをインターフェイスに割り当てます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IP Audit Policy Configuration

[Add/Edit IP Audit Policy Configuration] ダイアログボックスでは、インターフェイスに割り当てられる名前付き IP 監査ポリシーを追加または編集し、シグニチャ タイプごとにデフォルト アクションを変更できます。

フィールド

- [Policy Name]：IP 監査ポリシー名を設定します。ポリシー名は、追加した後では変更できません。
- [Policy Type]：ポリシー タイプを設定します。ポリシー タイプは、追加した後では変更できません。
  - [Attack]：ポリシー タイプを攻撃として設定します。
  - [Information]：ポリシー タイプを情報として設定します。
- [Action]：パケットがシグニチャに一致するときに実行するアクションを 1 つ以上設定します。アクションを選択しない場合には、デフォルト ポリシーが使用されます。
  - [Alarm]：パケットがシグニチャに一致したことを示すシステム メッセージを生成します。すべてのシグニチャのリストについては、「IP 監査のシグニチャ リスト」を参照してください。
  - [Drop]：パケットをドロップします。
  - [Reset]：パケットをドロップし、接続を閉じます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

IP Audit Signatures

[IP Audit Signatures] ペインでは、監査シグニチャをディセーブルにできます。正規のトラフィックが頻繁にシグニチャに一致する場合には、シグニチャをディセーブルにしてみてください。リスクが伴うことを承知でシグニチャをディセーブルにすると、多数のアラームを回避できます。

すべてのシグニチャのリストについては、「IP 監査のシグニチャ リスト」を参照してください。

フィールド

- [Enabled]：イネーブルになっているシグニチャを一覧表示します。
- [Disabled]：ディセーブルになっているシグニチャを一覧表示します。
- [Disable]：選択したシグニチャを [Disabled] ペインに移動します。
- [Enable]：選択したシグニチャを [Enabled] ペインに移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

IP 監査のシグニチャ リスト

表 27-3 に、サポートされているシグニチャおよびメッセージ番号の一覧を示します。

表 27-3　シグニチャ ID とシステム メッセージ番号

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1000	400000	IP options-Bad Option List	Informational	IP データグラム ヘッダーの IP オプションのリストが不完全であるか、または不正な形式になっている IP データグラムを受信するとトリガーされます。IP オプションのリストには、さまざまなネットワーク管理タスクまたはデバッグ タスクを実行するオプションが 1 つ以上含まれています。
1001	400001	IP options-Record Packet Route	Informational	データグラムの IP オプション リスト中にオプション 7（記録パケット ルート）を含む IP データグラムを受信するとトリガーされます。
1002	400002	IP options-Timestamp	Informational	データグラムの IP オプション リスト中にオプション 4（タイムスタンプ）を含む IP データグラムを受信するとトリガーされます。
1003	400003	IP options-Security	Informational	データグラムの IP オプション リスト中にオプション 2（セキュリティ オプション）を含む IP データグラムを受信するとトリガーされます。
1004	400004	IP options-Loose Source Route	Informational	データグラムの IP オプション リスト中にオプション 3（緩慢な送信元ルート）を含む IP データグラムを受信するとトリガーされます。
1005	400005	IP options-SATNET ID	Informational	データグラムの IP オプション リスト中にオプション 8（SATNET ストリーム ID）を含む IP データグラムを受信するとトリガーされます。
1006	400006	IP options-Strict Source Route	Informational	データグラムの IP オプション リスト中にオプション 2（厳密な送信元ルーティング）を含む IP データグラムを受信するとトリガーされます。
1100	400007	IP Fragment Attack	Attack	オフセット フィールドのオフセット値が 0 より大きく 5 未満になっている IP データグラムを受信するとトリガーされます。
1102	400008	IP Impossible Packet	Attack	送信元と宛先が同じアドレスになっている IP パケットが到着するとトリガーされます。このシグニチャは、いわゆる Land Attack を捕捉します。

表 27-3　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1103	400009	IP Overlapping Fragments（Teardrop）	Attack	同じ IP データグラム内に含まれている 2 つのフラグメントのオフセット値が、そのデータグラム内の位置決めを共有していることを示す場合にトリガーされます。これは、フラグメント A がフラグメント B によって完全に上書きされること、またはフラグメント A がフラグメント B によって部分的に上書きされることを意味します。オペレーティング システムによっては、このように重複するフラグメントが正しく処理されず、重複フラグメントを受信すると例外をスローしたり、他の不適切な動作を行ったりします。Teardrop 攻撃では、これにより DoS 状態を引き起こします。
2000	400010	ICMP Echo Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 0（エコー応答）に設定された IP データグラムを受信するとトリガーされます。
2001	400011	ICMP Host Unreachable	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 3（ホスト到達不能）に設定された IP データグラムを受信するとトリガーされます。
2002	400012	ICMP Source Quench	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 4（ソース クエンチ）に設定された IP データグラムを受信するとトリガーされます。
2003	400013	ICMP Redirect	Informational	P ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 5（リダイレクト）に設定された IP データグラムを受信するとトリガーされます。
2004	400014	ICMP Echo Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 8（エコー要求）に設定された IP データグラムを受信するとトリガーされます。
2005	400015	ICMP Time Exceeded for a Datagram	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 11（データグラムの超過時間）に設定された IP データグラムを受信するとトリガーされます。

表 27-3　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2006	400016	ICMP Parameter Problem on Datagram	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 12（データグラムのパラメータ問題）に設定された IP データグラムを受信するとトリガーされます。
2007	400017	ICMP Timestamp Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 13（タイムスタンプ要求）に設定された IP データグラムを受信するとトリガーされます。
2008	400018	ICMP Timestamp Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 14（タイムスタンプ応答）に設定された IP データグラムを受信するとトリガーされます。
2009	400019	ICMP Information Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 15（情報要求）に設定された IP データグラムを受信するとトリガーされます。
2010	400020	ICMP Information Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 16（ICMP 情報応答）に設定された IP データグラムを受信するとトリガーされます。
2011	400021	ICMP Address Mask Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 17（アドレス マスク要求）に設定された IP データグラムを受信するとトリガーされます。
2012	400022	ICMP Address Mask Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 18（アドレス マスク応答）に設定された IP データグラムを受信するとトリガーされます。
2150	400023	Fragmented ICMP Traffic	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、他にも 1（ICMP）に設定されたフラグメント フラグが存在するか、またはオフセット フィールドにオフセット値が指定されている IP データグラムを受信するとトリガーされます。
2151	400024	Large ICMP Traffic	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、IP 長が 1024 より大きくなっている IP データグラムを受信するとトリガーされます。

表 27-3　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2154	400025	Ping of Death Attack	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、Last Fragment ビットが設定され、（IP オフセット * 8）+（IP データ長）> 65535 になっている（つまり、IP オフセット（元のパケットでのこのフラグメントの開始位置、8 バイト単位）と残りのパケットの合計が IP パケットの最大サイズより大きくなっている）IP データグラムを受信するとトリガーされます。
3040	400026	TCP NULL flags	Attack	SYN、FIN、ACK、または RST のいずれのフラグも設定されていない 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3041	400027	TCP SYN+FIN flags	Attack	SYN および FIN のフラグが設定されている 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3042	400028	TCP FIN only flags	Attack	1 つの孤立 TCP FIN パケットが特定のホストの特権ポート（ポート番号が 1024 未満）に送信されるとトリガーされます。
3153	400029	FTP Improper Address Specified	Informational	要求側ホストと異なるアドレスを指定して port コマンドが発行された場合にトリガーされます。
3154	400030	FTP Improper Port Specified	Informational	1024 未満または 65535 より大きい値のデータ ポートを指定して port コマンドが発行された場合にトリガーされます。
4050	400031	UDP Bomb attack	Attack	指定されている UDP 長が、指定されている IP 長より短い場合にトリガーされます。この不正な形式のパケット タイプは、サービス拒絶攻撃と関連付けられています。
4051	400032	UDP Snork attack	Attack	送信元ポートが 135、7、または 19 のいずれかで、宛先ポートが 135 になっている UDP パケットが検出されるとトリガーされます。
4052	400033	UDP Chargen DoS attack	Attack	このシグニチャは、送信元ポート 7 および宛先ポート 19 において UDP パケットが検出されるとトリガーされます。
6050	400034	DNS HINFO Request	Informational	DNS サーバから HINFO レコードへのアクセスが試みられるとトリガーされます。
6051	400035	DNS Zone Transfer	Informational	送信元ポートが 53 の通常の DNS ゾーン転送が実行されるとトリガーされます。
6052	400036	DNS Zone Transfer from High Port	Informational	送信元ポートが 53 以外のときに不正な DNS ゾーン転送が発生するとトリガーされます。
6053	400037	DNS Request for All Records	Informational	すべてのレコードに対する DNS 要求があるとトリガーされます。
6100	400038	RPC Port Registration	Informational	ターゲット ホストで新しい RPC サービスを登録する試みがあるとトリガーされます。

表 27-3　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
6101	400039	RPC Port Unregistration	Informational	ターゲット ホストで既存の RPC サービスを登録解除する試みがあるとトリガーされます。
6102	400040	RPC Dump	Informational	ターゲット ホストに対して RPC ダンプ要求が発行されるとトリガーされます。
6103	400041	Proxied RPC Request	Attack	ターゲット ホストのポートマッパーにプロキシ RPC 要求が送信されるとトリガーされます。
6150	400042	ypserv (YP server daemon) Portmap Request	Informational	YP サーバ デーモン（ypserv）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6151	400043	ypbind (YP bind daemon) Portmap Request	Informational	YP バインド デーモン（ypbind）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6152	400044	yppasswdd (YP password daemon) Portmap Request	Informational	YP パスワード デーモン（yppasswdd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6153	400045	ypupdated (YP update daemon) Portmap Request	Informational	YP 更新デーモン（ypupdated）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	Informational	YP 転送デーモン（ypxfrd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6155	400047	mountd (mount daemon) Portmap Request	Informational	マウント デーモン（mountd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6175	400048	rexd (remote execution daemon) Portmap Request	Informational	リモート実行デーモン（rexd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6180	400049	rexd (remote execution daemon) Attempt	Informational	rexd プログラムの呼び出しが行われるとトリガーされます。リモート実行デーモンは、プログラムをリモート実行する役割を担うサーバです。rexd プログラムの呼び出しは、システム リソースへの不正アクセスの試みを示唆している場合があります。
6190	400050	statd Buffer Overflow	Attack	サイズの大きな statd 要求が送信されるとトリガーされます。これは、バッファをオーバーフローさせてシステムへアクセスしようとする試みの可能性があります。

フラグメント サイズの設定

デフォルトでは、セキュリティ アプライアンスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、フラグメントがセキュリティ アプライアンスを通過できないようにすることをお勧めします。フラグメント化されたパケットは、DoS 攻撃によく使われます。

フィールド

- [Fragment] テーブル：
  - [Interface]：セキュリティ アプライアンスの使用可能なインターフェイスを一覧表示します。
  - [Size]：リアセンブリを待機する IP リアセンブリ データベースに格納可能なパケットの最大数を設定します。デフォルトは 200 です。
  - [Chain Length]：1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。デフォルトは 24 パケットです。
  - [Timeout]：フラグメント化されたパケット全体の到着を待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。デフォルトは 5 秒です。
- [Edit]：[Edit Fragment] ダイアログボックスを開きます。
- [Show Fragment]：パネルが開き、セキュリティ アプライアンスのインターフェイスごとに現在の IP フラグメント データベースの統計情報が表示されます。

フラグメント パラメータの変更

インターフェイスの IP フラグメント データベースのパラメータを変更するには、次の手順を実行します。

ステップ 1　[Fragment] テーブルで変更するインターフェイスを選択し、[Edit] をクリックします。[Edit Fragment] ダイアログボックスが表示されます。

ステップ 2　[Edit Fragment] ダイアログボックスで、[Size]、[Chain]、および [Timeout] の値を必要に応じて変更し、[OK] をクリックします。間違った場合は、[Restore Defaults] をクリックします。

ステップ 3　[Fragment] パネルの [Apply] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Show Fragment

[Show Fragment] パネルには、IP フラグメント リアセンブリ モジュールの動作データが表示されます。

フィールド

- [Size]：*表示専用*。リアセンブリを待機する IP リアセンブリ データベース内のパケット数を表示します。デフォルトは 200 です。
- [Chain]：*表示専用*。1 つの完全な IP パケットにフラグメント化できる最大パケット数を表示します。デフォルトは 24 パケットです。
- [Timeout]：*表示専用*。フラグメント化されたパケットの全体の到着を待機する最大秒数を表示します。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。パケットのすべてのフラグメントが表示の秒数内に到着しないと、すでに受信しているパケットのフラグメントはすべて破棄されます。デフォルトは 5 秒です。
- [Threshold]：*表示専用*。IP パケットのしきい値、つまりその値を超えるとリアセンブリ モジュールで新しいチェーンを作成できなくなる限界を表示します。
- [Queue]：*表示専用*。キュー内でリアセンブリを待機している IP パケットの数を表示します。
- [Assembled]：*表示専用*。正常にリアセンブリされた IP パケットの数を表示します。
- [Fail]：*表示専用*。リアセンブリの失敗試行回数を表示します。
- [Overflow]：*表示専用*。オーバーフロー キュー内の IP パケットの数を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Edit Fragment

[Edit Fragment] ダイアログボックスでは、選択したインターフェイスの IP フラグメント データベースを設定できます。

フィールド

- [Interface]：[Fragment] パネルで選択したインターフェイスを表示します。[Edit Fragment] ダイアログボックスでの変更内容は、表示されたインターフェイスに適用されます。
- [Size]：リアセンブリを待機する IP リアセンブリ データベースに格納可能なパケットの最大数を設定します。
- [Chain Length]：1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。
- [Timeout]：フラグメント化されたパケット全体の到着を待機する最大秒数を設定します。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。

- [Restore Defaults]：工場出荷時のデフォルト設定に戻します。
  - [Size] は 200 です。
  - [Chain] は 24 パケットです。
  - Timeout は 5 秒です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Anti-Spoofing の設定

[Anti-Spoofing] ウィンドウでは、インターフェイスで Unicast Reverse Path Forwarding（Unicast RPF; ユニキャスト逆経路転送）をイネーブルにできます。Unicast RPF は、ルーティング テーブルに従い、すべてのパケットが正しい発信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護します。

通常、セキュリティ アプライアンスは、パケットの転送先を判定するときに宛先アドレスだけを調べます。Unicast RPF は、送信元アドレスも調べるようにセキュリティ アプライアンスに指示します。そのため、逆経路転送（Reverse Path Forwarding）と呼ばれます。セキュリティ アプライアンスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートをセキュリティ アプライアンスのルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、セキュリティ アプライアンスはデフォルト ルートを使用して Unicast RPF 保護の条件を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティング テーブルにない場合、セキュリティ アプライアンスはデフォルト ルートを使用して、外部インターフェイスを発信元インターフェイスとして正しく識別します。

ルーティング テーブルにあるアドレスから外部インターフェイスにトラフィックが入り、このアドレスが内部インターフェイスに関連付けられている場合、セキュリティ アプライアンスはパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合は、一致するルート（デフォルト ルート）が外部インターフェイスを示しているため、セキュリティ アプライアンスはパケットをドロップします。

Unicast RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルート ルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

フィールド

- [Interface]：インターフェイス名を一覧表示します。

- [Anti-Spoofing Enabled]：インターフェイスで Unicast RPF がイネーブルになっているかどうかを、Yes または No で示します。
- [Enable]：選択したインターフェイスに対する Unicast RPF をイネーブルにします。
- [Disable]：選択したインターフェイスに対する Unicast RPF をディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

TCP オプションの設定

[TCP Options] ペインでは、TCP 接続のパラメータを設定できます。

フィールド

- [Inbound and Outbound Reset]：着信および発信トラフィックの拒否された TCP 接続をリセットするかどうかを設定します。
  - [Interface]：インターフェイス名を表示します。
  - [Inbound Reset]：着信 TCP トラフィックのインターフェイスのリセット設定を、Yes または No で示します。この設定をイネーブルにすると、セキュリティ アプライアンスは、セキュリティ アプライアンスの通過を試み、アクセス リストまたは AAA の設定に基づいてセキュリティ アプライアンスにより拒否されたすべての着信 TCP セッションについて TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。
  - [Outbound Reset]：発信 TCP トラフィックのインターフェイスのリセット設定を、Yes または No で示します。この設定をイネーブルにすると、セキュリティ アプライアンス は、セキュリティ アプライアンス の通過を試み、アクセス リストまたは AAA の設定に基づいて セキュリティ アプライアンス により拒否されたすべての発信 TCP セッションについて TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。
  - [Edit]：インターフェイスの着信および発信のリセット設定値を設定します。
- [Other Options]：追加の TCP オプションを設定します。
  - [Send Reset Reply for Denied Outside TCP Packets]：セキュリティ レベルが最も低いインターフェイスで終了し、またアクセス リストまたは AAA の設定に基づいてセキュリティ アプライアンスにより拒否された TCP パケットのリセットをイネーブルにします。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。セキュリティ レベルが最も低いインターフェイスの Inbound Resets をイネーブルにする場合（TCP Reset Settings を参照）は、この設定もイネーブルにする必要はありません。Inbound Resets は、セキュリティ アプライアンスへのトラフィックとともに、セキュリティ アプライアンスを通過するトラフィックも処理します。

- [Force Maximum Segment Size for TCP] : 最大 TCP セグメント サイズを 48 から最大数の範囲のバイト数で設定します。デフォルト値は 1380 バイトです。この機能は、0 バイトに設定することによってディセーブルにできます。ホストとサーバが最初に接続を確立するときに、両方で最大セグメント サイズを設定できます。どちらかの最大値がここで設定する値を超えると、セキュリティ アプライアンスはその最大値を無効化し、ユーザが設定した値を挿入します。たとえば、ユーザが最大サイズを 1200 バイトに設定した場合に、ホストが最大サイズとして 1300 バイトを要求すると、セキュリティ アプライアンスは 1200 バイトを要求するようにパケットを変更します。
- [Force Minimum Segment Size for TCP] : 48 から最大数の間で、ユーザが設定したバイト数未満にならないように最大セグメント サイズを上書きします。この機能は、デフォルトでディセーブルです（0 に設定）。ホストとサーバが最初に接続を確立するときに、両方で最大セグメント サイズを設定できます。いずれかの最大値が [Force Minimum Segment Size for TCP Proxy] フィールドで設定した値未満になる場合、セキュリティ アプライアンスはその最大値を無効化し、ユーザが設定した「最小」値を挿入します（最小値は、実際には許容される最大値の中での最小の値です）。たとえば、ユーザが最小サイズを 400 バイトに設定した場合に、ホストが最大値として 300 バイトを要求すると、セキュリティ アプライアンスは 400 バイトを要求するようにパケットを変更します。
- [Force TCP Connection to Linger in TIME_WAIT State for at Least 15 Seconds] : 最後の標準 TCP クローズダウン シーケンスの後、最低でも 15 秒間、各 TCP 接続が短縮 TIME_WAIT 状態に保持するように強制します。エンド ホスト アプリケーションのデフォルト TCP 終了シーケンスが同時クローズである場合に、この機能を使用することを推奨します。セキュリティ アプライアンスのデフォルトの動作では、シャットダウン シーケンスが追跡され、2 つの FIN と最後の FIN セグメントの ACK の後で接続が解放されます。この即時解放ヒューリスティックにより、セキュリティ アプライアンスでは、標準クローズ シーケンスと呼ばれる最も一般的なクロージング シーケンスに基づいて、高い接続レートを維持できます。ただし、一方の端が閉じ、もう一方の端が確認応答してから独自のクロージング シーケンスを開始する標準クローズ シーケンスとは異なり、同時クローズでは、トランザクションの両端がクロージング シーケンスを開始します（RFC 793 を参照）。したがって、同時クローズでは、接続の一方の側が即時解放によって強制的に CLOSING 状態に保持されます。多くのソケットを CLOSING 状態にすると、エンド ホストのパフォーマンスが低下する可能性があります。たとえば、一部の WinSock メインフレーム クライアントはこの動作を示し、メインフレーム サーバのパフォーマンスを低下させることが知られています。この機能を使用すると、同時クローズダウン シーケンスを完了するためのウィンドウが作成されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

TCP Reset Settings

このダイアログボックスでは、インターフェイスの着信および発信のリセット設定値を設定します。

フィールド

- [Send Reset Reply for Denied Inbound TCP Packets] : セキュリティ アプライアンスの通過を試み、アクセス リストまたは AAA の設定に基づいてセキュリティ アプライアンスにより拒否されたすべての着信 TCP セッションについて TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。

  アイデンティティ要求（IDENT）接続をリセットする必要がある場合は、着信トラフィックに対して明示的にリセットを送信できます。拒否されたホストに TCP RST（TCP ヘッダーのリセット フラグ）を送信すると、RST によって着信 IDENT プロセスが停止されるため、IDENT がタイムアウトするのを待機する必要がなくなります。外部ホストは IDENT がタイムアウトするまで SYN を継続的に再送信するため、IDENT がタイムアウトするのを待機するとトラフィックの速度低下の原因となる可能性があります。そのため、**service resetinbound** コマンドによってパフォーマンスが向上する可能性があります。

- [Send Reset Reply for Denied Outbound TCP Packets] : セキュリティ アプライアンスの通過を試み、アクセス リストまたは AAA の設定に基づいてセキュリティ アプライアンスにより拒否されたすべての発信 TCP セッションについて TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。このオプションは、デフォルトで有効です。たとえば、トラフィック ストーム時に CPU の負荷を軽減するためなどに発信リセットをディセーブルにできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

グローバル タイムアウトの設定

[imeouts] ペインでは、セキュリティ アプライアンスで使用するタイムアウトの期間を設定できます。すべての期間は、hh:mm:ss の形式で表示されます。さまざまなプロトコルの接続スロットと変換スロットのアイドル時間を設定します。指定したアイドル時間の間スロットが使用されなかった場合、リソースは空いているプールに戻されます。TCP 接続スロットは、標準接続クローズ シーケンスのおよそ 60 秒後に解放されます。

（注）　カスタマー サポートによる指示がない限り、これらの値を変更しないことをお勧めします。

フィールド

[Authentication absolute] と [Authentication inactivity] を除くすべての場合において、チェックボックスをオフにすることはタイムアウト値を指定しないことを意味します。これら 2 つの場合にチェックボックスをオフにすることは、新しい接続ごとに再認証することを意味します。

- [Connection]：接続スロットが解放されるまでのアイドル時間を変更します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。この期間は 5 分以上にする必要があります。デフォルトは 1 時間です。
- [Half-closed]：TCP ハーフクローズ接続がクローズするまでのアイドル時間を変更します。最小値は 5 分です。デフォルトは 10 分です。ハーフクローズ接続のタイムアウトをディセーブルにするには、0:0:0 と入力します。
- [UDP]：UDP プロトコル接続がクローズするまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。タイムアウトをディセーブルにするには、0:0:0 と入力します。
- [ICMP]：全般的な ICMP 状態がクローズするまでのアイドル時間を変更します。
- [H.323]：H.323 メディア接続がクローズするまでのアイドル時間を変更します。デフォルトは 5 分です。タイムアウトをディセーブルにするには、0:0:0 と入力します。
- [H.225]：H.225 シグナリング接続がクローズするまでのアイドル時間を変更します。H.225 のデフォルトのタイムアウトは 1 時間（01:00:00）です。値を 00:00:00 にすると、この接続はクローズされません。すべての呼び出しがクリアされた後にこの接続をすぐにクローズするには、値を 1 秒（00:00:01）にすることをお勧めします。
- [MGCP]：MGCP メディア ポートがクローズするまでのアイドル時間を表す MGCP のタイムアウト値を変更します。MGCP のデフォルト タイムアウトは 5 分（00:05:00）です。タイムアウトをディセーブルにするには、0:0:0 と入力します。
- [MGCP PAT]：MGCP PAT 変換が削除されるまでのアイドル時間を変更します。デフォルトは 5 分（00:05:00）です。最小時間は 30 秒です。デフォルト値に戻すには、チェックボックスをオフにします。
- [SUNRPC]：SunRPC スロットが解放されるまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 10 分です。タイムアウトをディセーブルにするには、0:0:0 と入力します。
- [SIP]：SIP シグナリング ポート接続がクローズするまでのアイドル時間を変更します。この期間は 5 分以上にする必要があります。デフォルトは 30 分です。
- [SIP Media]：SIP メディア ポート接続がクローズするまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。
- [SIP Invite]：PROVISIONAL 応答とメディア xlate のピンホールがクローズされるまでのアイドル時間を変更します。最小値は 0:1:0 で、最大値は 0:30:0 です。デフォルト値は 0:03:00 です。
- [SIP Disconnect]：CANCEL または BYE メッセージで 200 個の OK を受信しない場合に、SIP セッションを削除するまでのアイドル時間を変更します。最小値は 0:0:1 で、最大値は 0:10:0 です。デフォルト値は 0:02:00 です。
- [Authentication absolute]：認証キャッシュがタイムアウトになり、新しい接続を再認証する必要が生じるまでの期間を変更します。この期間は、変換スロット値よりも短い必要があります。システムは、新しい接続を開始して再びプロンプトが表示されるまで待機します。新しい接続のすべてでキャッシングと再認証をディセーブルにするには、0:0:0 と入力します。

（注） 接続でパッシブ FTP を使用する場合は、この値を 0:0:0 に設定しないでください。

- [Authentication inactivity]：認証キャッシュがタイムアウトになり、ユーザが新しい接続を再認証する必要が生じるまでのアイドル時間を変更します。この期間は、変換スロット値よりも短い必要があります。

- [Translation Slot]：変換スロットが解放されるまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 3 時間です。タイムアウトをディセーブルにするには、0:0:0 と入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 28

QoS の設定

QoS は、基盤となるテクノロジーの限られた帯域幅で全体的に最良のサービスを実現するさまざまなテクノロジーによって、特定のネットワーク トラフィックに、より良いサービスを提供するネットワークの機能を指します。

セキュリティ アプライアンスでの QoS の主要な目的は、個別のフローおよび VPN トンネル フローの両方で、選択したネットワーク トラフィックのレートを制限し、限られた帯域幅の中ですべてのトラフィックが適切な割り当て分を得ることができるようにすることです。フローはさまざまな方法で定義できます。セキュリティ アプライアンスでは、送信元 IP アドレスと宛先 IP アドレスの組み合わせ、送信元ポート番号と宛先ポート番号の組み合わせ、および IP ヘッダーの TOS バイトに QoS を適用できます。

ここでは、次の内容について説明します。

QoS サービス ポリシーの設定

QoS サービス ポリシーは、通常のサービス ポリシーと同様の方法で作成されます。この手順では、通常のサービス ポリシーの作成プロセスの概要を示し、そのサービス ポリシーの QoS 機能の設定に重点を置いています。サービス ポリシー ルールの作成の詳細については、「通過トラフィックのサービス ポリシー ルールの追加」（P.23-4）を参照してください。

QoS サービス ポリシーを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Firewall] > [Service Policy Rules] ペインを開きます。

ステップ 2 [Add] をクリックして新しいサービス ポリシー ルールを作成します。

Service Policy Wizard が開きます。

ステップ 3 サービス ポリシー ルールの範囲を定義します。サービス ポリシー ルールは、グローバル（すべてのインターフェイス）に適用することも、特定のインターフェイスに適用することもできます。[Next] をクリックします。

ステップ 4 サービス ポリシーに一致するトラフィックを定義します。選択した一致基準によっては、複数のウィザード画面が表示され、順に実行する必要がある場合があります。一致基準の設定の詳細については、「通過トラフィックのサービス ポリシー ルールの追加」（P.23-4）を参照してください。[Next] をクリックします。

[Rules Actions] 画面が表示されます。

ステップ 5 [QoS] タブをクリックします。

ステップ 6　QoS を設定するには、次のいずれかの操作を実行します。

- 特定のトラフィックをプライオリティの高いトラフィックとして定義するには、[Enable priority for this flow] をクリックします。これにより、トラフィックが高プライオリティとして定義され、そのプライオリティ キューを設定できるようになります。このオプションを選択すると、トラフィック ポリシングはイネーブルにできません。
- トラフィックのレート制限を設定するには、[Enable policing] をクリックします。これにより、入力または出力（または両方）のトラフィック レートの制限、バースト レートの定義、および適合トラフィックと非適合トラフィックに対して実行するアクションの指定を行うことができます。これらの設定の詳細については、「[QoS] タブのフィールド情報」（P.28-2）を参照してください。

ステップ 7　[Finish] をクリックします。サービス ポリシー ルールがルール テーブルに追加されます。[Apply] をクリックしてコンフィギュレーションをデバイスに送信します。

ステップ 8　トラフィックのプライオリティをイネーブルにした場合、特定のインターフェイスのプライオリティ キューを設定する必要があります。プライオリティ キューの設定の詳細については、「プライオリティ キュー」（P.28-3）を参照してください。

[QoS] タブのフィールド情報

[QoS] タブでは、厳密なスケジュール プライオリティとレート制限トラフィックを適用できます。

制約事項

確立済みの VPN クライアント /LAN-to-LAN または非トンネル トラフィックが存在するインターフェイスに対して、サービス ポリシーが適用または削除されると、トラフィック ストリームに対して QoS ポリシーは適用または削除されません。そのような接続の QoS ポリシーを適用または削除するには、接続をクリア（つまりドロップ）して再確立する必要があります。

フィールド

- [Enable Priority for this flow]：このフローでの厳密なスケジュール プライオリティをイネーブルまたはディセーブルにします。プライオリティは、プライオリティ キューが設定されるまで有効になりません。プライオリティ キューを設定するには、「プライオリティ キュー」（P.28-3）を参照してください。
- [Enable policing]：入力および出力のトラフィック ポリシングをイネーブルにするには、このチェックボックスをオンにします。次に、指定したタイプのトラフィック ポリシングをイネーブルにするには、[Input policing] または [Output policing]（または両方の）チェックボックスをオンにします。トラフィック ポリシングのタイプごとに、次のフィールドを設定します。
  - [Committed Rate]：このトラフィック フローのレート制限。これは、8000 ～ 2000000000 の範囲の値で、許容最大速度（ビット / 秒）を指定します。
  - [Conform Action]：レートが適合バースト値未満の場合に実行するアクション。値は、transmit または drop です。
  - [Exceed Action]：レートが適合レート値と適合バースト値の間になっている場合に、このアクションを実行します。値は、transmit または drop です。
  - [Burst Rate]：1000 ～ 512000000 の範囲の値で、適合レート値までトラフィックを抑制するまでに、持続したバーストにおいて許可される最大瞬間バイト数を指定します。

（注）　[Enable Policing] チェックボックスは、最大速度および最大バースト レートを強制し、それらの値を適合レート値に強制的に合わせるだけです。**conform-action** または **exceed-action** の指定は、存在する場合でも適用されません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

プライオリティ キュー

トラフィックを高プライオリティとして定義する QoS サービス ポリシー ルールを定義した場合は、1 つ以上のインターフェイスでプライオリティ キューをイネーブルにし、それらのインターフェイスを通過するトラフィックに対してサービス ルールがイネーブルになるようにする必要があります。プライオリティ キューイングはデフォルトでディセーブルです。プライオリティ キューを設定するには、[Configuration] > [Device Management] > [Advanced] > [Priority Queue] に移動します。

[Priority Queue] ペインは、プライオリティ キュー テーブルを表示します。[Priority Queue] テーブルは、プライオリティ キューが設定されているインターフェイスごとに次の情報を表示します。

- [Interface]：キューが設定されたインターフェイス。
- [Queue Limit]：接続がドロップされるまでの、通常キューまたはプライオリティ キューに入れることができるパケットの最大数です。両方のキューに同じ制限があります。プライオリティ キュー内のパケットは、通常のプライオリティ キュー内のパケットが送信される前に完全に排出されます。
- [Transmission Ring Limit]：プライオリティ キューの深さを指定します。プライオリティ キューイングがイネーブルでない場合、このカラムはメッセージ「Ring Disabled」を表示します。

プライオリティ キュー コンフィギュレーションを追加または変更するには、次のいずれかを実行します。

- 新しいプライオリティ キューを追加するには、[Add] をクリックします。[Add Priority Queue] ダイアログボックスが表示されます。
- 既存のプライオリティ キューを編集するには、テーブルでキューのエントリをクリックし、[Edit] をクリックします。または、テーブルでキューのエントリをダブルクリックします。[Edit Priority Queue] ダイアログボックスが表示されます。

フィールド

[Add/Edit Priority Queue] ダイアログボックスには次のフィールドがあります。

- [Interface]：プライオリティ キューをイネーブルにするインターフェイスを選択します。インターフェイスごとに 1 つのプライオリティ キューのみを設定できます。このフィールドには、プライオリティ キューが設定されていないインターフェイスがすべて表示されます。

- [Queue Limit]：接続がドロップされるまでの、通常キューまたはプライオリティ キューに入れることができるパケットの最大数を指定します。最小値は 0 パケットで、最大は、利用可能なメモリに基づいて実行時に動的に決まります。理論的な最大パケット数は、2147483647 です。

（注） 両方のキューに同じ制限があります。プライオリティ キュー内のパケットは、通常のプライオリティ キュー内のパケットが送信される前に完全に排出されます。

- [Transmission Ring Limit]：イーサネット送信ドライバが受け入れる低遅延パケットまたは通常プライオリティ パケットの最大数を設定します。この制限に達すると、ドライバはパケットをインターフェイスのキューに差し戻し、輻輳が解消されるまでパケットをバッファに格納できるようにします。最小値は 3 です。値の範囲の上限は、実行時にダイナミックに決定されます。主な決定要素は、キューをサポートするために必要なメモリと、デバイス上で使用可能なメモリです。キューは、使用可能なメモリを超えることはできません。理論上の最大パケット数は 2147483647（つまり、全二重回線速度まで）です。プライオリティ キューイングがイネーブルでない場合、このカラムはメッセージ「Ring Disabled」を表示します。

  伝送リング制限は、ドライバが許容できる両方のタイプのパケットの数です。このパケット数を超えると、ドライバはインターフェイスの先頭にある複数のキューにパケットを戻し、輻輳が解消するまでそのキューでパケットをバッファしておきます。通常は、queue-limit パラメータと伝送リング制限パラメータを調整し、低遅延トラフィックのフローを最適化できます。

  キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが、*テール ドロップ*です。キューがいっぱいになることを避けるには、queue-limit パラメータを調整して、キューのバッファ サイズを大きくします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 29

VPN

セキュリティ アプライアンスは、ユーザがプライベートな接続と見なす TCP/IP ネットワーク（インターネットなど）全体でセキュアな接続を確立することにより、バーチャル プライベート ネットワークを構築します。これによって、single-user-to-LAN 接続と LAN-to-LAN 接続を確立できます。セキュアな接続はトンネルと呼ばれ、セキュリティ アプライアンス は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。セキュリティ アプライアンスは、双方向のトンネル エンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方の側に送信できます。そのエンドポイントで、パケットはカプセル化が解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。

セキュリティ アプライアンスは次の VPN 機能を実行します。

- トンネルを確立する。
- トンネル パラメータをネゴシエートする。
- VPN ポリシーを適用する。
- ユーザを認証する。
- ユーザが特定レベルで使用およびアクセスすることを許可する。
- アカウンティング機能を実行する。
- ユーザ アドレスを割り当てる。
- データを暗号化および復号化する。
- セキュリティ キーを管理する。
- トンネルを通したデータ転送を管理する。
- トンネル エンドポイントまたはルータとしての着信データと発信データの転送を管理する。

セキュリティ アプライアンスは、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

VPN Wizard

VPN Wizard では、基本的な LAN-to-LAN 接続とリモート アクセス VPN 接続を設定できます。ASDM を使用して拡張機能を編集および設定してください。

（注）　VPN Wizard では、認証用の事前共有キーまたはデジタル証明書のいずれかを割り当てられます。ただし、証明書を使用するには、認証局に登録し、ウィザードを使用する前にトラストポイントを設定しておく必要があります。これらのタスクを実行するには、[ASDM Device Administration] > [Certificate] パネルとオンライン ヘルプを使用してください。

VPN の概要

セキュリティ アプライアンスは、ユーザがプライベートな接続と見なす TCP/IP ネットワーク（インターネットなど）全体でセキュアな接続を確立することにより、バーチャル プライベート ネットワークを構築します。これによって、single-user-to-LAN 接続と LAN-to-LAN 接続を確立できます。

セキュアな接続はトンネルと呼ばれ、セキュリティ アプライアンス は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。セキュリティ アプライアンスは、双方向のトンネル エンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方の側に送信することができます。そのエンドポイントで、パケットはカプセル化が解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。

セキュリティ アプライアンスが実行する機能は次のとおりです。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザの認証
- ユーザ アドレスの割り当て
- データの暗号化と復号化
- セキュリティ キーの管理
- トンネルを通したデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

VPN Tunnel Type

[VPN Tunnel Type] パネルでは、定義する VPN トンネルのタイプ（リモート アクセスまたは LAN-to-LAN）を選択し、リモート IPSec ピアに接続するインターフェイスを特定します。

フィールド

- [Site-to-Site] : LAN-to-LAN VPN コンフィギュレーションを作成します。2 つの IPSec セキュリティ ゲートウェイの間で使用します。このゲートウェイには、セキュリティ アプライアンス、VPN コンセントレータ、またはサイトツーサイト IPSec 接続をサポートする他のデバイスなどがあります。このオプションを選択すると、VPN Wizard に、サイトツーサイト VPN で必要とされる属性を入力するための一連のパネルが表示されます。
- [Remote Access] : モバイル ユーザなどの VPN クライアントへのセキュアなリモート アクセスを実現するコンフィギュレーションを作成します。このオプションにより、リモート ユーザは、中央集中型ネットワーク リソースに安全にアクセスできます。このオプションを選択すると、VPN Wizard に、リモート アクセス VPN で必要とされる属性を入力するための一連のパネルが表示されます。

- [VPN Tunnel Interface]：リモート IPSec ピアとのセキュアなトンネルを確立するインターフェイスを選択します。セキュリティ アプライアンスに複数のインターフェイスがある場合は、このウィザードを実行する前に VPN コンフィギュレーションを計画し、セキュアな接続を確立する予定のリモート IPSec ピアごとに、使用するインターフェイスを特定しておく必要があります。
- [Enable inbound IPSec sessions to bypass interface access lists]：セキュリティ アプライアンスによって常に許可される（つまり、インターフェイスの access-list 文をチェックしない）ように、IPSec 認証の着信セッションをイネーブルにします。着信セッションがバイパスするのは、インターフェイス ACL だけです。設定されたグループ ポリシー、ユーザ、およびダウンロードされた ACL は適用されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Remote Site Peer

[Remote Site Peer] パネルでは、次のタスクを実行します。

1. この VPN トンネルの終端となるリモート IPSec ピアの IP アドレスを指定する。
2. リモート ピアに対して作成する。
3. 認証方式を選択および設定する。

フィールド

- [Peer IP Address]：VPN トンネルの終端となるリモート IPSec ピアの IP アドレスを入力します。ピアは、別のセキュリティ アプライアンス、VPN コンセントレータ、または IPSec をサポートする他のゲートウェイ デバイスです。
- [Authentication Method]：リモート サイト ピアは、事前共有キーか証明書のいずれかを使用して認証します。
  - [Pre-shared Key]：ローカル セキュリティ アプライアンスとリモート IPSec ピアの間の認証で事前共有キーを使用する場合にクリックします。

    事前共有キーを使用すると、リモート ピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPSec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

    IPSec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモート サイトの管理者と事前共有キーを交換してください。
  - [Pre-shared Key]：事前共有キーを入力します。最大 127 文字です。

- [Certificate]：ローカル セキュリティ アプライアンスとリモート IPSec ピアの間の認証で証明書を使用する場合にクリックします。このセクションを完了するには、あらかじめ CA への登録を済ませ、1 つ以上の証明書をセキュリティ アプライアンスにダウンロードしておく必要があります。

  デジタル証明書を使用すると、IPSec トンネルを確立するために使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザまたはデバイスを識別する情報が記述されています。またデジタル証明書には、所有者の公開キーのコピーも含まれています。

  デジタル証明書を使用するには、デジタル証明書を発行する Certification Authority（CA; 認証局）に各ピアを登録します。CA は、信頼できるベンダーまたは組織内で設置したプライベート CA の場合もあります。

  2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

- [Certificate Signing Algorithm]：デジタル証明書に署名するアルゴリズムを、RSA 用の rsa-sig、または DSA 用の dsa-sig から選択します。
- [Trustpoint Name]：セキュリティ アプライアンスがリモート ピアに送信する証明書を識別する名前を選択します。このリストには、トラストポイントが、証明書の署名アルゴリズム リストで先に選択したタイプの証明書と一緒に表示されます。
- [Challenge/response authentication (CRACK)]：クライアントが RADIUS などの一般的な方式を使用して認証を行い、サーバが公開キーによる認証方式を使用している場合に、強力な相互認証を実現します。セキュリティ アプライアンスは、Nokia 92xx Communicator Series デバイスで Nokia VPN Client を認証するために、IKE オプションとして CRACK をサポートしています。

- [Name]：名前を入力して、この IPSec 接続のトンネル接続ポリシーを含むレコードを作成します。接続ポリシーでは、認証、許可、アカウンティング サーバ、デフォルト グループ ポリシー、および IKE 属性を指定できます。この VPN ウィザードで設定するポリシーでは、認証方式を指定し、セキュリティ アプライアンス デフォルト グループ ポリシーを使用します。

  デフォルトでは、ASDM は、このボックスにピア IP アドレスの値を入力します。この名前は変更できます。最大 64 文字です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

IKE Policy

Internet Security Association and Key Management Protocol（ISAKMP）とも呼ばれる IKE は、2 台のホストで IPSec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。各 IKE ネゴシエーションは、フェーズ 1 とフェーズ 2 と呼ばれる 2 つの部分に分かれます。

- フェーズ 1 は、以後の IKE ネゴシエーション メッセージを保護する最初のトンネルを作成します。
- フェーズ 2 では、データを保護するトンネルが作成されます。

[IKE Policy] パネルでは、フェーズ 1 IKE ネゴシエーションの条件を設定します。次の項目があります。

- データを保護しプライバシーを守る暗号化方式。
- ピアの ID を確認する認証方式。
- 暗号キー判別アルゴリズムを強化する Diffie-Hellman グループ。このアルゴリズムを使用して、セキュリティ アプライアンスは暗号キーとハッシュ キーを導出します。

フィールド

- [Encryption]：フェーズ 2 ネゴシエーションを保護するフェーズ 1 SA を確立するためにセキュリティ アプライアンスが使用する、対称暗号化アルゴリズムを選択します。セキュリティ アプライアンスは、次の暗号化アルゴリズムをサポートします。

アルゴリズム	説明
DES	データ暗号規格。56 ビット キーを使用します。
3DES	Triple DES。56 ビット キーを使用して暗号化を 3 回実行します。
AES-128	高度暗号化規格。128 ビット キーを使用します。
aes-192	192 ビット キーを使用する AES。
AES-256	256 ビット キーを使用する AES。

  デフォルトの 3DES は DES よりもセキュアですが、暗号化と復号化には、より多くの処理を必要とします。同様に、AES オプションによるセキュリティは強力ですが、必要な処理量も増大します。

- [Authentication]：認証やデータ整合性の確保のために使用するハッシュ アルゴリズムを選択します。デフォルトは SHA です。MD5 のダイジェストは小さく、SHA よりもわずかに速いとされています。MD5 は、（きわめて困難ですが）攻撃により破れることが実証されています。ただし、セキュリティ アプライアンスで使用される Keyed-Hash Message Authentication Code（HMAC）バージョンはこの攻撃を防ぎます。
- [DH Group]：Diffie-Hellman グループ ID を選択します。2 つのピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルトの Group 2（1024 ビット Diffie-Hellman）は、Group 5（1536 ビット）と比較して、CPU の実行時間は短いですが、安全性は低くなります。

（注） VPN 3000 シリーズ コンセントレータのデフォルト値は MD5 です。セキュリティ アプライアンスと VPN コンセントレータの間の接続では、接続の両方の側で、フェーズ 1 と 2 の IKE ネゴシエーションの認証方式を同じにする必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

IPSec Encryption and Authentication

[IPSec Encryption and Authentication] パネルでは、セキュアな VPN トンネルを作成するフェーズ 2 IKE ネゴシエーションで使用する暗号化方式と認証方式を選択します。これらの値は、両方のピアでまったく同じにする必要があります。

フィールド

- [Encryption]：VPN トンネルを確立するためにセキュリティ アプライアンスが使用する対称暗号化アルゴリズムを選択します。セキュリティ アプライアンスは、暗号化を使用してトンネルを通過するデータを保護し、プライバシーを守ります。有効な暗号化方式には、次のものがあります。

暗号化方式	説明
DES	データ暗号規格。56 ビット キーを使用します。
3DES	Triple DES。56 ビット キーを使用して 3 回暗号化します。
AES-128	高度暗号化規格。128 ビット キーを使用します。
aes-192	192 ビット キーを使用する AES。
AES-256	256 ビット キーを使用する AES。

  デフォルトの 3DES は DES よりもセキュアですが、暗号化と復号化には、より多くの処理を必要とします。同様に、AES オプションによるセキュリティは強力ですが、必要な処理量も増大します。

- [Authentication]：認証やデータ整合性の確保のために使用するハッシュ アルゴリズムを選択します。デフォルトは SHA です。MD5 のダイジェストは小さく、SHA よりもわずかに速いとされています。MD5 は、（きわめて困難ですが）攻撃により破れることが実証されています。ただし、セキュリティ アプライアンスで使用される Keyed-Hash Message Authentication Code（HMAC）バージョンはこの攻撃を防ぎます。

（注） VPN 3000 シリーズ コンセントレータのデフォルト値は MD5 です。セキュリティ アプライアンスと VPN コンセントレータの間の接続では、接続の両方の側で、フェーズ 1 とフェーズ 2 の IKE ネゴシエーションの認証方式を同じにする必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Hosts and Networks

[Hosts and Networks] パネルでは、この LAN-to-LAN IPSec トンネルを使用してデータを送受信することができる、ローカルおよびリモートのホストとネットワークを特定します。

IPSec に従って動作するには、LAN-to-LAN 接続における両方のピアのホストおよびネットワークのエントリが、互換性を持っている必要があります。このパネルでローカルのホストとネットワークとして設定するホストおよびネットワークは、LAN-to-LAN 接続のリモート サイトにあるデバイスのリモートのホストとネットワークとして設定する必要があります。ローカルのセキュリティ アプライアンスとリモート デバイスには、この LAN-to-LAN 接続で使用する共通のトランスフォーム セットが少なくとも 1 つ必要です。

フィールド

- [Action]：ローカル ネットワークとリモート ネットワークの間を移動するデータを保護するかどうかを指定します。
- [Local networks]：ローカルのホストとネットワークを選択します。
- [Remote networks]：リモートのホストとネットワークを選択します。
- [Exempt ASA side host/network from address translation]：トラフィックがアドレス変換なしでセキュリティ アプライアンスを通過できるようにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Summary

[Summary] パネルには、この VPN LAN-to-LAN 接続の属性すべてが設定どおりに表示されます。

フィールド

[Back]：変更するには、目的のパネルに到達するまで [Back] をクリックします。

[Finish]：設定に問題なければ、[Finish] をクリックします。ASDM によって LAN-to-LAN のコンフィギュレーションが保存されます。[Finish] をクリックした後は、この VPN ウィザードを使用してこのコンフィギュレーションを変更することはできません。ASDM を使用して拡張機能を編集および設定してください。

[Cancel]：このコンフィギュレーションを削除するには、[Cancel] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Remote Access Client

[Remote Access Client] パネルでは、この接続を使用するリモート アクセス ユーザのタイプを特定します。

フィールド

- [Cisco VPN Client Release 3.x or higher, or other Easy VPN Remote product]：ここで名前が指定されたもの以外の互換性のあるソフトウェア クライアントとハードウェア クライアントを含む、IPSec 接続の場合にクリックします。
- [Microsoft Windows client using L2TP over IPSec]：パブリック IP ネットワークを経由する、Microsoft Windows クライアントおよび Microsoft Windows Mobile クライアントからの接続をイネーブルにする場合にクリックします。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。次の PPP 認証プロトコルの 1 つ以上をイネーブルにします。
  - [PAP]：認証中にクリアテキストのユーザ名とパスワードを渡すので、安全ではありません。
  - [CHAP]：サーバのチャレンジに対する応答で、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。このプロトコルは、PAP より安全ですが、データは暗号化されません。
  - [MS-CHAP, Version 1]：CHAP と似ていますが、サーバは、CHAP のようなクリアテキストのパスワードではなく、暗号化したパスワードだけを保存および比較するので安全です。
  - [MS-CHAP, Version 2]：MS-CHAP, Version 1 以上のセキュリティ強化機能が含まれています。
  - [EAP]：EAP をイネーブルにします。これによってセキュリティ アプライアンスは、PPP の認証プロセスを外部の RADIUS 認証サーバに代行させます。
- [Client will send the tunnel group name as username@tunnelgroup]：セキュリティ アプライアンスが、L2TP over IPSec 接続を確立する別々のユーザを異なるトンネル グループと関連付けることができるようにします。各トンネル グループはそれぞれの AAA サーバ グループと IP アドレス プールを持つため、ユーザはそのトンネル グループ特定の方法で認証を受けられます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

VPN Client Authentication Method and Tunnel Group Name

[VPN Client Authentication Method and Tunnel Group Name] パネルでは、認証方式を設定し、トンネル グループを作成します。

フィールド

- [Authentication Method]：リモート サイト ピアは、事前共有キーか証明書のいずれかを使用して認証します。
  - [Pre-shared Key]：ローカル セキュリティ アプライアンスとリモート IPSec ピアの間の認証で事前共有キーを使用する場合にクリックします。

    事前共有キーを使用すると、リモート ピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPSec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

    IPSec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモート サイトの管理者と事前共有キーを交換してください。
  - [Pre-shared Key]：事前共有キーを入力します。
  - [Certificate]：ローカル セキュリティ アプライアンスとリモート IPSec ピアの間の認証で証明書を使用する場合にクリックします。このセクションを完了するには、あらかじめ CA への登録を済ませ、1 つ以上の証明書をセキュリティ アプライアンスにダウンロードしておく必要があります。

    デジタル証明書を使用すると、IPSec トンネルを確立するために使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザまたはデバイスを識別する情報が記述されています。またデジタル証明書には、所有者の公開キーのコピーも含まれています。

    デジタル証明書を使用するには、デジタル証明書を発行する Certification Authority（CA; 認証局）に各ピアを登録します。CA は、信頼できるベンダーまたは組織内で設置したプライベート CA の場合もあります。

    2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。
  - [Trustpoint Name]：セキュリティ アプライアンスがリモート ピアに送信する証明書を識別する名前を選択します。
  - [Certificate Signing Algorithm]：デジタル証明書に署名するアルゴリズムを、RSA 用の rsa-sig、または DSA 用の dsa-sig から選択します。

  - [Challenge/response authentication (CRACK)] : クライアントが RADIUS などの一般的な方式を使用して認証を行い、サーバが公開キーによる認証方式を使用している場合に、強力な相互認証を実現します。セキュリティ アプライアンスは、Nokia 92xx Communicator Series デバイスで Nokia VPN Client を認証するために、IKE オプションとして CRACK をサポートしています。

- [Name] : 名前を入力して、この IPSec 接続のトンネル接続ポリシーを含むレコードを作成します。接続ポリシーでは、認証、許可、アカウンティング サーバ、デフォルト グループ ポリシー、および IKE 属性を指定できます。この VPN ウィザードで設定するポリシーでは、認証方式を指定し、セキュリティ アプライアンス デフォルト グループ ポリシーを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

クライアント認証

[Client Authentication] パネルでは、セキュリティ アプライアンスがリモート ユーザを認証するときに使用する方法を選択します。

フィールド

次のオプションのいずれかを選択します。

- [Authenticate using the local user database] : セキュリティ アプライアンスの内部の認証方式を使用する場合にクリックします。この方式は、ユーザの数が少なくて安定している環境で使用します。次のパネルでは、セキュリティ アプライアンスに個々のユーザのアカウントを作成できます。
- [Authenticate using an AAA server group] : リモート ユーザ認証で外部サーバ グループを使用する場合にクリックします。
- [AAA Server Group] : 前に設定されている AAA サーバ グループを選択します。
- [New ...] : 新しい AAA サーバ グループを設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

New Authentication Server Group

[New Authentication Server Group] パネルでは、新しい AAA サーバを 1 つ以上定義します。

フィールド

サーバを 1 つだけ含む AAA サーバ グループを設定するには、次の情報を入力します。

- [Server Group Name]：サーバ グループの名前を入力します。この名前は、このサーバを使用して認証する対象のユーザに関連付けます。
- [Authentication Protocol]：サーバで使用する認証プロトコルを選択します。オプションには、TACACS+、RADIUS、SDI、NT、および Kerberos などがあります。
- [Server IP Address]：AAA サーバの IP アドレスを入力します。
- [Interface]：AAA サーバが常駐するセキュリティ アプライアンスのインターフェイスを選択します。
- [Server Secret Key]：大文字と小文字が区別される最大 127 文字の英数字キーワードを入力します。サーバとセキュリティ アプライアンスは、そのキーを使用して両者の間を移動するデータを暗号化します。キーは、セキュリティ アプライアンスとサーバの両方で同じにする必要があります。スペース以外の特殊文字を使用することができます。
- [Confirm Server Secret Key]：もう一度秘密キーを入力します。

この新しいグループにサーバを追加するか、または他の AAA サーバの設定を変更するには、[Configuration] > [Features] > [Properties] > [AAA] に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

User Accounts

[User Accounts] パネルでは、認証を目的として、セキュリティ アプライアンスの内部ユーザ データベースに新しいユーザを追加します。

フィールド

次の情報を入力します。

- このセクションのフィールドを使用してユーザを追加します。
  - [Username]：ユーザ名を入力します。
  - [Password]：（任意）パスワードを入力します。
  - [Confirm Password]：（任意）パスワードを再入力します。
- [Change user password]：ユーザ パスワードを変更する場合にオンにします。

- [User authentication using MSCHAP]：ユーザ認証用に MS-CHAP を使用する場合にオンにします。
- [Add]：ユーザ名と任意指定のパスワードを入力した後でクリックすると、データベースにユーザが追加されます。
- [Edit]：データベースに追加したユーザを編集する場合にクリックします。
- [Access Restriction]：次のオプションのいずれかを選択します。
  - Full access (ASDM, SSH, Telnet, and console)

    [Privilege Level]：ドロップダウン リストから適切なものを選択します。管理者は、通常、使用できるうち最高の 15 を割り当てています。
  - CLI login prompt for SSH, Telnet, and console (no ASDM access)
  - No ASDM, SSH, Telnet, or console access
- [Delete]：データベースからユーザを削除するには、該当するユーザ名を強調表示させ、[Delete] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Address Pool

[Address Pool] パネルでは、セキュリティ アプライアンスがリモート VPN クライアントに割り当てるローカル IP アドレスのプールを設定します。

フィールド

- [Name]：アドレス プールが適用されるトンネル グループの名前を表示します。この名前は、[VPN Client Name and Authentication Method] パネルで設定したものです。
- [Pool Name]：アドレス プールの記述 ID を選択します。
- [New...]：新しいアドレス プールを設定します。
- [Range Start Address]：アドレス プールの開始 IP アドレスを入力します。
- [Range End Address]：アドレス プールの終了 IP アドレスを入力します。
- [Subnet Mask]：（任意）これらの IP アドレスのサブネット マスクを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Attributes Pushed to Client

[Attributes Pushed to Client (Optional)] パネルでは、DNS サーバと WINS サーバおよびデフォルト ドメイン名についての情報をリモート アクセス クライアントに渡す動作をセキュリティ アプライアンスに実行させます。

フィールド

リモート アクセス クライアントで使用する情報を入力します。

- ：アドレス プールが適用される接続ポリシーの名前を表示します。この名前は、[VPN Client Name and Authentication Method] パネルで設定したものです。
- [Primary DNS Server]：プライマリ DNS サーバの IP アドレスを入力します。
- [Secondary DNS Server]：セカンダリ DNS サーバの IP アドレスを入力します。
- [Primary WINS Server]：プライマリ WINS サーバの IP アドレスを入力します。
- [Secondary WINS Server]：セカンダリ WINS サーバの IP アドレスを入力します。
- [Default Domain Name]：デフォルトのドメイン名を入力します。モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Address Translation Exemption

[Address Translation Exemption (Optional)] パネルを使用して、アドレス変換を必要としないローカル ホスト/ネットワークを識別します。デフォルトによりセキュリティ アプライアンスは、ダイナミックまたはスタティックのネットワーク アドレス変換（NAT）を使用して、内部ホストおよびネットワークの本当の IP アドレスを外部ホストから隠します。NAT は、信頼できない外部ホストによる攻撃の危険性を最小限に抑えますが、VPN によって認証および保護されているホストに対しては不適切な場合があります。

たとえば、ダイナミック NAT を使用する内部ホストは、プールから無作為に選択したアドレスと照合することにより、その IP アドレスを変換させます。外部ホストからは、変換されたアドレスだけが見えるようになります。本当の IP アドレスにデータを送信することによってこれらの内部ホストに到達しようとするリモート VPN クライアントは、NAT 免除ルールを設定しない限り、これらのホストには接続できません。

（注）　すべてのホストとネットワークを NAT から免除する場合は、このパネルでは何も設定しません。エントリが 1 つでも存在すると、他のすべてのホストとネットワークは NAT に従います。

フィールド

- [Host/Network to Be Added]：これらのフィールドに値を入力して、NAT から特定のホストまたはネットワークを免除します。
  - [Interface]：選択したホストまたはネットワークに接続するインターフェイスの名前を選択します。
  - [IP address]：ホストまたはネットワークの IP アドレスを選択します。IP アドレスを入力するか、または隣の [...] ボタンをクリックしてネットワーク図を表示し、ホストまたはネットワークを選択します。
- [Add]：適切なフィールドへの入力を済ませた後に、ホストまたはネットワークを [Selected Hosts/Networks] リストに追加します。
- [Selected Hosts/Networks]：NAT から免除するホストとネットワークを表示します。すべてのホストとネットワークを NAT から免除する場合は、このリストには何も入力しません。
- [Enable split tunneling]：リモート アクセス クライアントからのパブリック インターネット宛のトラフィックを暗号化せずに送信する場合に選択します。スプリット トンネリングにより、保護されたネットワークのトラフィックが暗号化され、保護されていないネットワークのトラフィックは暗号化されません。スプリット トンネリングをイネーブルにすると、セキュリティ アプライアンスは、認証後に IP アドレスのリストをリモート VPN クライアントにプッシュします。リモート VPN クライアントは、セキュリティ アプライアンスの背後にある IP アドレスへのトラフィックを暗号化します。他のすべてのトラフィックは、暗号化なしでインターネットに直接送り出され、セキュリティ アプライアンスは関与しません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

CHAPTER 30

SSL VPN Wizard

SSL VPN 機能

クライアントレス ブラウザベース SSL VPN によって、ユーザはブラウザを使用してセキュリティ アプライアンスへのセキュアなリモート アクセス VPN トンネルを確立できます。認証後にポータル ページを開き、サポートされる特定の内部リソースにアクセスできます。ネットワーク管理者は、グループ単位でユーザごとにリソースへのアクセスを提供します。ユーザは、内部ネットワーク上のリソースには直接アクセスできません。

Cisco AnyConnect VPN クライアントによって、リモートユーザは、企業リソースへの完全な VPN トンネリングを使用して、セキュリティ アプライアンスにセキュアな SSL 接続を実行できます。リモート ユーザは、あらかじめインストール済みのクライアントがなくても、クライアントレス SSL VPN 接続を受け入れるように設定されたインターフェイスのブラウザに IP アドレスを入力します。セキュリティ アプライアンスは、リモート コンピュータのオペレーティング システムに適合するクライアントをダウンロードします。ダウンロード後に、クライアントはクライアント自体をインストールして設定し、セキュアな SSL 接続を確立して、接続の終了時には（セキュリティ アプライアンスの設定に応じて）インストールされたまま残るか、またはクライアント自体をアンインストールします。あらかじめインストール済みのクライアントの場合、ユーザが認証を行うと、セキュリティ アプライアンスはクライアントのリビジョンを調べ、必要に応じてクライアントをアップグレードします。

フィールド

- [Clientless SSL VPN Access]：サポートされる特定の内部リソースに対する、ポータル ページからのクライアントレス ブラウザベース接続をイネーブルにします。
- [Cisco SSL VPN Client (AnyConnect VPN Client)]：完全なネットワーク アクセスを実現する SSL VPN クライアント接続をイネーブルにします。セキュリティ アプライアンスをイネーブルにして、AnyConnect クライアントをリモート ユーザにダウンロードします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

[SSL VPN Interface]

このウィンドウでは、接続名（以前の *トンネル グループ*）を指定し、SSL VPN 接続のインターフェイスをイネーブルにし、デジタル証明書情報を指定します。

フィールド

- [Connection Name]：このコネクション型アトリビュート グループの接続名を指定します。
- [SSL VPN Interface]：SSL VPN 接続を許可するインターフェイスを指定します。
- [Digital Certificate]：セキュリティ アプライアンスがリモート PC に送信する証明書が存在する場合は、その証明書を指定します。
  - [Certificate]：証明書の名前を指定します。
- [Connection Group Settings]：セキュリティ アプライアンスをイネーブルにして、この接続のグループ エイリアスをログイン ページに表示できます。
  - [Connection Group Alias]：接続のエイリアス名を指定します。
  - [Display Group Alias list at the login page]：グループ エイリアスを表示する場合にイネーブルにします。
- [Information]：SSL VPN 接続と ASDM 接続を確立するためのリモート ユーザが必要とする情報を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

[User Authentication]

この画面では、認証情報を指定します。

フィールド

- [Authenticate using a AAA server group]：セキュリティ アプライアンスがリモート AAA サーバ グループにアクセスしてユーザを認証できるようにする場合にイネーブルにします。
- [AAA Server Group Name]：事前設定されたグループのリストから AAA サーバ グループを選択するか、または [New] をクリックして新しいグループを作成します。
- [Authenticate using the local user database]：セキュリティ アプライアンスに保存されているローカル データベースに新しいユーザを追加します。
  - [Username]：ユーザのユーザ名を作成します。
  - [Password]：ユーザのパスワードを作成します。
  - [Confirm Password]：確認のために同じパスワードを再入力します。
  - [Add/Delete]：ローカル データベースにユーザを追加またはデータベースから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランス ペアレント	シングル	コンテキスト	システム
•	—	•	—	—

[Group Policy]

グループ ポリシーによって、ユーザ グループの共通アトリビュートを設定します。新しいグループ ポリシーを作成するか、または既存のポリシーを選択して修正します。

フィールド

- [Create new group policy]：新しいグループ ポリシーを作成する場合にイネーブルにします。新しいポリシーの名前を入力します。
- [Modify existing group policy]：修正する既存のグループ ポリシーを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランス ペアレント	シングル	コンテキスト	システム
•	—	•	—	—

[Bookmark List]

ブックマーク リストは、クライアントレス ブラウザベース接続のポータル ページに表示されます。SSL VPN クライアント ユーザには、これらのブックマークは表示されません。このウィンドウでは、新しいブックマーク リストを作成します。

フィールド

- [Bookmark List]：既存のリストを選択するか、または [Manage] をクリックして新しいリストを作成します。あるいは、ブックマーク リストをインポートまたはエクスポートします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

[IP Address Pools and Client Image]

このウィンドウでは、リモート SSL VPN ユーザに対する IP アドレス範囲を入力し、セキュリティ アプライアンスに対する SSL VPN クライアント イメージを指定します。

フィールド

- [IP Address Pool] : SSL VPN クライアントはセキュリティ アプライアンスに接続するときに新しい IP アドレスを受け取ります。クライアントレス接続では新しい IP アドレスは不要です。アドレス プールでは、リモート クライアントが受け取ることのできるアドレス範囲が定義されます。
- [IP Address Pool] : 既存の IP アドレス プールを選択するか、または [New] をクリックして新しいプールを作成します。
- [AnyConnect VPN Client Image Location] : フラッシュメモリ内の SSL VPN クライアント イメージであるセキュリティ アプライアンス ファイルに対して指定します。[Browse] をクリックしてローカル PC 上のイメージの場所を指定します。
  - [Location] : フラッシュ メモリに保存されている有効な SSL VPN クライアント イメージのパスおよびファイル名を入力します。
  - [Download Latest AnyConnect VPN Client form CCO] : 最新クライアント イメージのソフトウェア ダウンロード ページに移動するには、このリンクをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

[Summary]

これまでのウィザードのウィンドウで行った選択の要約を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランス パアレント	シングル	コンテキスト	システム
•	—	•	—	—

[Summary]

CHAPTER 31

IKE

IKE は ISAKMP とも呼ばれ、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。バーチャル プライベート ネットワークのセキュリティ アプライアンスを設定するには、システム全体に適用するグローバル IKE パラメータを設定します。また、VPN 接続を確立するためにピアがネゴシエートする IKE ポリシーも作成します。

IKE Parameters

このパネルでは、VPN 接続を使用する場合のシステム全体の値を設定できます。次の項では、各オプションについて説明します。

インターフェイスでの IKE のイネーブル化

VPN 接続を使用するインターフェイスごとに、IKE をイネーブルにする必要があります。

IPsec over NAT-T のイネーブル化

NAT-T により IPSec ピアは、リモート アクセスと LAN-to-LAN の両方の接続を NAT デバイスを介して確立できます。NAT-T は UDP データグラムの IPsec トラフィックをカプセル化し、ポート 4500 を使用して、NAT デバイスにポート情報を提供します。NAT-T はすべての NAT デバイスを自動検出し、必要な場合だけ IPsec トラフィックをカプセル化します。この機能はデフォルトで無効に設定されています。

- セキュリティ アプライアンスは、データ交換を行うクライアントに応じて、標準の IPSec、IPSec over TCP、NAT-T、および IPSec over UDP を同時にサポートできます。
- NAT-T と IPsec over UDP の両方がイネーブルになっている場合、NAT-T が優先されます。
- イネーブルになっている場合、IPsec over TCP は他のすべての接続方式よりも優先されます。

セキュリティ アプライアンスによる NAT-T の実装では、次の場合において、単一の NAT/PAT デバイスの背後にある IPSec ピアをサポートします。

- LAN-to-LAN 接続。
- LAN-to-LAN 接続または複数のリモート アクセス クライアントのいずれか。ただし、両方を混在させることはできません。

NAT-T を使用するには、次の手順を実行する必要があります。

- セキュリティ アプライアンスでポート 4500 を開きます。
- このパネルで、IPsec over NAT-T をグローバルにイネーブルにします。

- [Configuration] > [VPN] > [IPsec] > [Pre-Fragmentation] パネルで、フラグメンテーション ポリシー パラメータの 2 番目と 3 番目のオプションを選択します。これらのオプションにより、トラフィックは、IP フラグメンテーションをサポートしていない NAT デバイス間を移動できます。これによって、IP フラグメンテーションをサポートする NAT デバイスの動作が妨げられることはありません。

IPsec over TCP のイネーブル化

IPSec over TCP を使用すると、標準 ESP や標準 IKE が機能できない環境、または既存のファイアウォール ルールを変更した場合に限って機能できる環境で、VPN クライアントが動作可能になります。IPSec over TCP は TCP パケット内で IKE プロトコルと IPSec プロトコルをカプセル化し、NAT と PAT の両方のデバイスおよびファイアウォールによりセキュアなトンネリングを実現します。この機能はデフォルトで無効に設定されています。

（注）　この機能は、プロキシベースのファイアウォールでは動作しません。

IPsec over TCP は、リモート アクセス クライアントで動作します。また、すべての物理インターフェイスと VLAN インターフェイスでも動作します。これは、セキュリティ アプライアンス機能に対応するクライアントに限られます。LAN-to-LAN 接続では機能しません。

- セキュリティ アプライアンスは、データ交換を行うクライアントに応じて、標準の IPsec、IPsec over TCP、NAT-Traversal、および IPsec over UDP を同時にサポートできます。
- 1 度に 1 つのトンネルをサポートする VPN 3002 ハードウェア クライアントは、標準の IPsec、IPsec over TCP、NAT-Traversal、または IPsec over UDP を使用して接続できます。
- イネーブルになっている場合、IPsec over TCP は他のすべての接続方式よりも優先されます。

セキュリティ アプライアンスとその接続先のクライアントの両方で IPsec over TCP をイネーブルにします。

最大 10 個のポートを指定して、それらのポートに対して IPsec over TCP をイネーブルにできます。ポート 80（HTTP）やポート 443（HTTPS）などのウェルノウン ポートを入力すると、そのポートに関連付けられているプロトコルが機能しなくなることを示す警告がシステムに表示されます。その結果、ブラウザを使用して、IKE がイネーブルのインターフェイスからセキュリティ アプライアンスを管理することができなくなります。この問題を解決するには、HTTP/HTTPS 管理を別のポートに再設定します。

セキュリティ アプライアンスだけでなく、クライアントでも TCP ポートを設定する必要があります。クライアントの設定には、セキュリティ アプライアンス用に設定したポートを少なくとも 1 つ含める必要があります。

識別方式の決定

IKE ネゴシエーションでは、ピアが相互に相手を識別する必要があります。この識別方式は、次のオプションから選択できます。

アドレス	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
ホスト名	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
キー ID	リモート ピアが事前共有キーの検索に使用する文字列を使用します。
自動	接続タイプによって IKE ネゴシエーションを決定します。 • 事前共有キーの IP アドレス • 証明書認証の cert DN。

インバウンド Aggressive モード接続のディセーブル化

フェーズ 1 の IKE ネゴシエーションでは、Main モードと Aggressive モードのいずれかを使用できます。どちらのモードも同じサービスを提供しますが、Aggressive モードの場合にピア間で必要とされる交換処理は、3 つではなく 2 つだけです。Agressive モードの方が高速ですが、通信パーティの ID は保護されません。そのため、情報を暗号化するセキュアな SA を確立する前に、ピア間で ID 情報を交換する必要があります。この機能はデフォルトで無効に設定されています。

接続解除の前にピアに警告

セキュリティ アプライアンスのシャットダウンまたはリブート、セッション アイドル タイムアウト、最大接続時間の超過、または管理者による停止などのいくつかの理由で、クライアント セッションまたは LAN-to-LAN セッションがドロップすることがあります。

セキュリティ アプライアンスは、（LAN-to-LAN コンフィギュレーションの場合）限定されたピアである VPN クライアントと VPN 3002 ハードウェア クライアントに、セッションが接続解除される直前に通知し、その理由を伝えることができます。アラートを受信したピアまたはクライアントは、その理由を復号化してイベント ログまたはポップアップ パネルに表示します。この機能はデフォルトで無効に設定されています。

このパネルでは、セキュリティ アプライアンスがこれらのアラートを送信し、接続解除の理由を伝えることができるように、この機能をイネーブルにできます。

限定されたクライアントとピアには次のものが含まれます。

- アラートがイネーブルになっているセキュリティ アプライアンス デバイス。
- バージョン 4.0 以降のソフトウェアを実行している VPN クライアント（設定は不要）。
- 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっている VPN 3002 ハードウェア クライアント。
- バージョン 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっている VPN 3000 シリーズ Concentrator。

リブート前のアクティブ セッションの終了を待機

すべてのアクティブ セッションが自発的に終了した場合に限り、セキュリティ アプライアンスがリブートするようにスケジュールを設定できます。この機能はデフォルトで無効に設定されています。

フィールド

- [Enable IKE]：設定されたすべてのインターフェイスの IKE ステータスを表示します。
  - [Interface]：設定されたすべてのセキュリティ アプライアンス インターフェイス名を表示します。
  - [IKE Enabled]：設定されたインターフェイスごとに IKE がイネーブルになっているかどうかを示します。
  - [Enable/Disables]：強調表示されたインターフェイスの IKE をイネーブルまたはディセーブルにする場合にクリックします。
- [NAT Transparency]：IPsec over NAT-T および IPsec over TCP をイネーブルまたはディセーブルにできます。
  - [Enable IPsec over NAT-T]：IPsec over NAT-T をイネーブルにする場合に選択します。
  - [NAT Keepalive]：セキュリティ アプライアンスが NAT-T セッションを終了させるまでに許容する、トラフィックなしの経過時間を秒数で入力します。デフォルトは 20 秒です。範囲は、10 ～ 3600 秒（1 時間）です。
  - [Enable IPsec over TCP]：IPsec over TCP をイネーブルにする場合に選択します。

  - [Enter up to 10 comma-separated TCP port values] : IPsec over TCP をイネーブルにするポートを最大で 10 ポートまで入力します。ポート間はカンマで区切ります。スペースは不要です。デフォルト ポートは 10,000 です。範囲は 1 ～ 65,635 です。

- [Identity to Be Sent to Peer] : IPsec のピアがお互いを識別する方法を設定できます。
  - [Identity] : IPsec のピアがお互いを識別する方法を、次の中から 1 つ選択します。

Address	ホストの IP アドレスを使用します。
Hostname	ホストの完全修飾ドメイン名を使用します。この名前は、ホスト名とドメイン名で構成されます。
キー ID	リモート ピアが事前共有キーの検索に使用する文字列を使用します。
自動	接続タイプ（事前共有キーの IP アドレスまたは証明書認証の cert DN）によって IKE ネゴシエーションを判断します。

  - [Key Id String] : ピアが事前共有キーの検索に使用する英数文字列を入力します。

- [Disable inbound aggressive mode connections] : アグレッシブ モードの接続をディセーブルにする場合に選択します。
- [Alert peers before disconnecting] : セッションを接続解除する前に、セキュリティ アプライアンスから限定された LAN-to-LAN ピアとリモートアクセス クライアントに通知する場合に選択します。
- [Wait for all active sessions to voluntarily terminate before rebooting] : セキュリティ アプライアンスにより、すべてのアクティブなセッションが終了するまで、予定されたリブートを延期させる場合に選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

IKE ポリシー

各 IKE ネゴシエーションは、フェーズ 1 とフェーズ 2 と呼ばれる 2 つの部分に分かれます。

フェーズ 1 は、以後の IKE ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 では、データを保護するトンネルが作成されます。

IKE ネゴシエーションの条件を設定するには、次に示す項目を含む IKE ポリシーを 1 つ以上作成します。

- 一意のプライオリティ（1 ～ 65,543、1 が最高のプライオリティ）。
- ピアの ID を確認する認証方式。
- データを保護し、プライバシーを守る暗号化方式。
- HMAC 方式。送信者の身元を保証し、搬送中にメッセージが変更されていないことを保証します。

- 暗号キー判別アルゴリズムを強化する Diffie-Hellman グループ。このアルゴリズムを使用して、セキュリティ アプライアンスは暗号キーとハッシュ キーを導出します。
- セキュリティ アプライアンスが暗号キーを置き換える前に、この暗号キーを使用する最長時間の制限。

IKE ポリシーを何も設定しない場合、セキュリティ アプライアンスはデフォルトのポリシーを使用します。デフォルト ポリシーは常に最下位のプライオリティに設定され、パラメータごとのデフォルト値が含まれています。特定のパラメータの値を指定しない場合、デフォルト値が適用されます。

IKE ネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモート ピアに送信します。リモート ピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。

暗号化、ハッシュ、認証、および Diffie-Hellman の値が同じで、SA ライフタイムが送信されたポリシーのライフタイム以下の場合には、IKE ポリシー間に一致が存在します。ライフタイムが等しくない場合は、（リモート ピア ポリシーからの）短い方のライフタイムが適用されます。一致するポリシーがない場合、IKE はネゴシエーションを拒否し、IKE SA は確立されません。

フィールド

- [Policies]：設定された IKE ポリシーごとのパラメータの設定値を表示します。
  - [Priority #]：ポリシーのプライオリティを示します。
  - [Encryption]：暗号化方式を示します。
  - [Hash]：ハッシュ アルゴリズムを示します。
  - [D-H Group]：Diffie-Hellman グループを示します。
  - [Authentication]：認証方式を示します。
  - [Lifetime（secs）]：SA ライフタイムを秒数で示します。
- [Add]/[Edit]/[Delete]：IKE ポリシーを追加、編集、または削除する場合にクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

IKE ポリシーの追加 / 編集

フィールド

[Priority #]：IKE ポリシーのプライオリティを設定する数字を入力します。範囲は 1 ～ 65,543 で、1 が最高のプライオリティです。

[Encryption]：暗号化方式を選択します。これは、2 つの IPSec ピア間で伝送されるデータを保護する対称暗号化アルゴリズムです。次の中から選択できます。

des	56 ビット DES-CBC。安全性は低いですが、他の選択肢より高速です。デフォルト。
3des	168 ビット Triple DES。
aes	128 ビット AES。
aes-192	192 ビット AES。
aes-256	256 ビット AES。

[Hash]：データの整合性を保証するハッシュ アルゴリズムを選択します。パケットが、そのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。

sha	SHA-1	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。
md5	MD5	

[Authentication]：各 IPsec ピアの ID を確立するためにセキュリティ アプライアンスが使用する認証方式を選択します。事前共有キーは拡大するネットワークに対応して拡張が困難ですが、小規模ネットワークではセットアップが容易です。次の選択肢があります。

pre-share	事前共有キー。
rsa-sig	RSA シグニチャ アルゴリズムによって生成されたキー付きのデジタル証明書。
crack	モバイル IPSec がイネーブルになっているクライアントの IKE Challenge/Response for Authenticated Cryptographic Keys プロトコル。証明書以外の認証技術を使用します。

[D-H Group]：Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。

1	Group 1（768 ビット）	これがデフォルトです。Group 2（1024 ビット Diffie-Hellman）では、実行に必要な CPU 時間が少なくなりますが、Group 2 または 5 より安全性が劣ります。
2	Group 2（1024 ビット）	
5	Group 5（1536 ビット）	

[Lifetime (secs)]：[Unlimited] を選択するか、SA ライフタイムを整数で入力します。デフォルトは 86,400 秒、つまり 24 時間です。ライフタイムを長くするほど、セキュリティ アプライアンスは以後の IPSec セキュリティ アソシエーションをより迅速にセットアップします。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することを推奨します。

[Time Measure]：時間基準を選択します。セキュリティ アプライアンスでは、次の値を使用できます。

120 ～ 86,400 秒

2 ～ 1,440 分

1 ～ 24 時間

1 日

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Assignment Policy

インターネットワーク接続は、IP アドレスによって可能になります。IP アドレスは、送信者と受信者の両方に接続用の番号が割り当てられている必要があるという点で、電話番号に似ています。ただし実際の VPN では、2 つのアドレス セットを使用します。最初のセットは、パブリック ネットワークのクライアントとサーバを接続し、その接続が確立されると、2 番目のセットが VPN トンネル経由でクライアントとサーバを接続します。

セキュリティ アプライアンスのアドレス管理では、この IP アドレスの 2 番目のセットを扱います。これらのプライベート IP アドレスは、クライアントをトンネル経由でプライベート ネットワーク上のリソースに接続し、プライベート ネットワークに直接接続されているかのようなクライアント機能を提供します。また、ここでは、クライアントに割り当てられたプライベート IP アドレスのみを扱います。プライベート ネットワーク上のその他のリソースに割り当てられた IP アドレスは、セキュリティ アプライアンスの管理ではなく、ネットワーク管理業務の一部に位置づけられます。

したがって、ここで IP アドレスに言及する場合は、クライアントをトンネルのエンドポイントとして機能させる、プライベート ネットワークのアドレッシング方式で取得される IP アドレスを意味します。

[Assignment Policy] パネルでは、IP アドレスをリモートアクセス クライアントに割り当てる方法を選択できます。

フィールド

- [Use authentication server] : 認証サーバから取得した IP アドレスをユーザ単位で割り当てる場合に選択します。IP アドレスが設定された認証サーバ（外部または内部）を使用している場合は、この方式を使用することを推奨します。AAA サーバの設定は、[Configuration] > [AAA Setup] パネルで行います。
- [Use DHCP] : DHCP サーバから IP アドレスを取得する場合に選択します。DHCP を使用する場合は、[Configuration] > [DHCP Server] パネルで DHCP サーバを設定します。
- [Use internal address pools] : セキュリティ アプライアンスにより、内部で設定されたプールから IP アドレスを割り当てる場合に選択します。内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。この方法を使用する場合は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] パネルで IP アドレス プールを設定します。
  - [Allow the reuse of an IP address __ minutes after it is released] : IP アドレスがアドレス プールに戻された後に、IP アドレスを再利用するまでの時間を指定します。遅延時間を設けることにより、IP アドレスがすぐに再割り当てされることによって発生する問題がファイアウォール

で生じないようにできます。デフォルトでは、このオプションはオフになっています。つまり、セキュリティ アプライアンスは遅延時間を課しません。遅延時間を設定する場合は、チェックボックスをオンにし、IP アドレスを再割り当てするまでの時間を 1 ～ 480 の範囲で指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Address Pools

[IP Pool] ボックスには、設定された各アドレス プールが、名前ごとに、それぞれの IP アドレス範囲（たとえば、10.10.147.100 ～ 10.10.147.177）とともに表示されます。プールが存在しない場合、ボックスは空です。セキュリティ アプライアンスは、リストに表示される順番でこれらのプールを使用します。最初のプールのすべてのアドレスが割り当てられると、次のプールのアドレスが使用され、以下同様に処理されます。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することをお勧めします。

フィールド

- [Pool Name]：設定された各アドレス プールの名前を表示します。
- [Starting Address]：設定されたそれぞれのプールで使用可能な最初の IP アドレスを示します。
- [Ending Address]：設定されたそれぞれのプールで使用可能な最後の IP アドレスを示します。
- [Subnet Mask]：設定されたそれぞれのプールにあるアドレスのサブネット マスクを示します。
- [Add]：新しいアドレス プールを追加する場合にクリックします。
- [Edit/Delete]：すでに設定されているアドレス プールを編集または削除する場合にクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit IP Pool

これらのパネルでは、次のことを行えます。

- セキュリティ アプライアンスがクライアントにアドレスを割り当てるときに使用する、IP アドレスの新しいプールを追加します。
- 事前に設定した IP アドレス プールを変更します。

プール範囲内の IP アドレスを他のネットワーク リソースに割り当てることはできません。

フィールド

- [Name]：アドレス プールに英数字の名前を割り当てます。最大で 64 文字です。
- [Starting IP Address]：このプールで使用可能な最初の IP アドレスを入力します。たとえば 10.10.147.100 のように、ドット付き 10 進数表記を使用します。
- [Ending IP Address]：このプールで使用可能な最後の IP アドレスを入力します。たとえば 10.10.147.100 のように、ドット付き 10 進数表記を使用します。
- [Subnet Mask]：IP アドレス プールのサブネット マスクを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

IPSec

セキュリティ アプライアンス では、IPsec は LAN-to-LAN VPN 接続に使用され、client-to-LAN VPN 接続にも IPsec を使用できます。IPsec 用語で「ピア」とは、リモート アクセス クライアントまたは別のセキュアなゲートウェイを意味します。

（注）　ASA は、シスコのピアや、関連するすべての標準に準拠したサードパーティのピアとの LAN-to-LAN IPsec 接続をサポートしています。

トンネルを確立する間に、2 つのピアは、認証、暗号化、カプセル化、キー管理を制御する Security Association（SA; セキュリティ アソシエーション）をネゴシエートします。これらのネゴシエーションには、トンネルの確立（IKE SA）と、トンネル内のトラフィックの制御（IPsec SA）という 2 つのフェーズが含まれます。

LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。IPsec LAN-to-LAN 接続では、セキュリティ アプライアンスは発信側または応答側として機能します。IPsec client-to-LAN 接続では、セキュリティ アプライアンスは応答側としてだけ機能します。発信側は SA を提案し、応答側は、設定された SA パラメータに従って、SA の提示を受け入れるか、拒否するか、または対案を提示します。接続を確立するには、両方のエンティティで SA が一致する必要があります。

セキュリティ アプライアンスは、次の IPsec 属性をサポートします。

- 認証でデジタル証明書を使用するときに、フェーズ 1 ISAKMP セキュリティ アソシエーションをネゴシエートする場合の Main モード
- 認証で事前共有キーを使用するときに、フェーズ 1 ISAKMP セキュリティ アソシエーション（SA）をネゴシエートする場合の Aggressive モード
- 認証アルゴリズム：
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- 認証モード：
  - 事前共有キー
  - X.509 デジタル証明書
- Diffie-Hellman Group 1、2、および 5
- 暗号化アルゴリズム：
  - AES-128、-192、および -256
  - 3DES-168
  - DES-56
  - ESP-NULL
- 拡張認証（XAuth）
- モード コンフィギュレーション（別名 ISAKMP コンフィギュレーション方式）
- トンネル カプセル化モード
- LZS を使用した IP 圧縮（IPCOMP）

クリプト マップ

このペインには、IPSec ルールを含め、現在設定されているクリプト マップが表示されます。このペインで、IPSec ルールを追加、編集、削除、切り取り、および貼り付けしたり、上下に移動させたりします。

フィールド

（注） 暗黙のルールは、編集、削除、またはコピーできません。セキュリティ アプライアンスは、ダイナミック トンネル ポリシーが設定されている場合、リモート クライアントからトラフィックの選択提案を暗黙的に受け入れます。特定のトラフィックを選択することによって、その提案を無効化できます。

- [Add] : [Add IPsec Rule] ダイアログを開く場合にクリックします。このダイアログでは、ルールの基本、詳細、およびトラフィックの選択パラメータを設定したり、選択することができます。
- [Edit] : 既存のルールを編集します。
- [Delete] : テーブルで選択したルールを削除します。
- [Cut] : テーブルで選択したルールを切り取り、コピーできるようにクリップボードに保持します。
- [Copy] : テーブルで選択したルールをコピーします。
- [Find] : 検索する既存ルールのパラメータを指定するための [Find] ツールバーをイネーブルにします。

  - [Filter] : [is] または [contains] を選択し、フィルタ パラメータを入力することによって、Interface、Source、Destination Service、または Rule Query を基準にして検索結果をフィルタリングします。[...] をクリックして、選択可能なすべての既存エントリが表示された参照ダイアログを開きます。
- [Diagram] : 選択した IPsec ルールを示す図を表示します。
- [Type: Priority] : ルールのタイプ（Static または Dynamic）とそのプライオリティを表示します。
- Traffic Selection
  - [#] : ルール番号を示します。
  - [Source] : トラフィックを [Remote Side Host/Network] カラムのリストにある IP アドレス宛てに送信するときに、このルールに従う IP アドレスを示します。詳細モード（[Show Detail] ボタンを参照）では、アドレス カラムに、単語 **any** が付いたインターフェイス名が含まれることがあります（**inside:any** など）。**any** とは、内部インターフェイスにある任意のホストが、ルールによって影響を受けることを意味します。
  - [Destination]:トラフィックが [Security Appliance Side Host/Network] カラムのリストにある IP アドレスから送信されるときに、このルールに従う IP アドレスを一覧表示します。詳細モード（[Show Detail] ボタンを参照）では、アドレス カラムに、単語 **any** が付いたインターフェイス名が含まれることがあります（**outside:any** など）。**any** とは、外部インターフェイスにある任意のホストが、ルールによって影響を受けることを意味します。さらに詳細モードでは、アドレス カラムに角カッコで囲まれた IP アドレスが含まれることもあります（[209.165.201.1-209.165.201.30] など）。これらのアドレスは、変換済みアドレスです。内部ホストが外部ホストへの接続を作成すると、セキュリティ アプライアンスは内部ホストのアドレスをプールのアドレスにマッピングします。ホストがアウトバウンド接続を作成した後、セキュリティ アプライアンスはこのアドレス マッピングを維持します。このアドレス マッピング構造は xlate と呼ばれ、一定の時間メモリに保持されます。
  - [Service] : ルールによって指定されるサービスとプロトコルを指定します（TCP、UDP、ICMP、または IP）。
  - [Action] : IPsec ルールのタイプ（保護する、または保護しない）を指定します。
- [Transform Set] : ルールのトランスフォーム セットを表示します。
- [Peer] : IPsec ピアを識別します。
- [PFS] : ルールの完全転送秘密設定値を表示します。
- [NAT-T Enabled] : ポリシーで NAT Traversal がイネーブルになっているかどうかを示します。
- [Reverse Route Enabled] : ポリシーで逆ルート注入がイネーブルになっているかどうかを示します。
- [Connection Type] :（スタティック トンネル ポリシーでだけ適用）このポリシーの接続タイプを、bidirectional、originate-only、または answer-only として識別します。
- [SA Lifetime] : ルールの SA ライフタイムを表示します。
- [CA Certificate] : ポリシーの CA 証明書を表示します。これは、スタティック接続にだけ適用されます。
- [IKE Negotiation Mode] : IKE ネゴシエーションで、Main モードまたは Aggressive モードを使用するかどうかを表示します。
- [Description] :（任意）このルールの簡単な説明を指定します。既存ルールの場合は、ルールの追加時に入力した説明になります。暗黙のルールには「Implicit rule」という説明が加えられます。暗黙のルール以外のルールの説明を編集するには、このカラムを右クリックして [Edit Description] を選択するか、またはカラムをダブルクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Create IPsec Rule/Tunnel Policy (Crypto Map) - Basic] タブ

このペインでは、IPSec ルールの新しいトンネル ポリシーを定義します。ここで定義する値は、[OK] をクリックした後に [IPSec Rules] テーブルに表示されます。すべてのルールは、デフォルトで [IPSec Rules] テーブルに表示されるとすぐにイネーブルになります。

[Tunnel Policy] パネルでは、IPsec（フェーズ 2）セキュリティ アソシエーション（SA）のネゴシエートで使用するトンネル ポリシーを定義できます。ASDM は、ユーザのコンフィギュレーション編集結果を取り込みますが、[Apply] をクリックするまでは実行中のコンフィギュレーションに保存しません。

すべてのトンネル ポリシーでは、トランスフォーム セットを指定し、適用するセキュリティ アプライアンス インターフェイスを特定する必要があります。トランスフォーム セットでは、IPSec の暗号化処理と復号化処理を実行する暗号化アルゴリズムおよびハッシュ アルゴリズムを特定します。すべての IPSec ピアが同じアルゴリズムをサポートするとは限らないため、多くのポリシーを指定して、それぞれに 1 つのプライオリティを割り当てるようにすることもできます。その後セキュリティ アプライアンスは、リモートの IPSec ピアとネゴシエートして、両方のピアがサポートするトランスフォーム セットを一致させます。

トンネル ポリシーは、*スタティック*または*ダイナミック*にすることができます。スタティック トンネル ポリシーでは、セキュリティ アプライアンスで IPSec 接続を許可する 1 つ以上のリモート IPSec ピアまたはサブネットワークを特定します。スタティック ポリシーを使用して、セキュリティ アプライアンスで接続を開始するか、またはリモート ホストから接続要求を受信するかどうかを指定できます。スタティック ポリシーでは、許可されるホストまたはネットワークを識別するために必要な情報を入力する必要があります。

ダイナミック トンネル ポリシーは、セキュリティ アプライアンスとの接続を開始することを許可されるリモート ホストについての情報を指定できないか、または指定しない場合に使用します。リモート VPN 中央サイト デバイスとの関係で、セキュリティ アプライアンスを VPN クライアントとしてしか使用しない場合は、ダイナミック トンネル ポリシーを設定する必要はありません。ダイナミック トンネル ポリシーが最も効果的なのは、リモートアクセス クライアントが、VPN 中央サイト デバイスとして動作するセキュリティ アプライアンスからユーザ ネットワークへの接続を開始できるようにする場合です。ダイナミック トンネル ポリシーは、リモートアクセス クライアントにダイナミックに割り当てられた IP アドレスがある場合、または多くのリモートアクセス クライアントに別々のポリシーを設定しないようにする場合に役立ちます。

フィールド

- [Interface]：このポリシーを適用するインターフェイス名を選択します。
- [Policy Type]：このトンネル ポリシーのタイプとして、[Static] または [Dynamic] を選択します。
- [Priority]：ポリシーのプライオリティを入力します。

- [Transform Set to Be Added]：ポリシーのトランスフォーム セットを選択し、[Add] をクリックしてアクティブなトランスフォーム セットのリストに移動します。[Move Up] または [Move Down] をクリックして、リスト ボックス内でのトランスフォーム セットの順番を入れ替えます。クリプト マップ エントリまたはダイナミック クリプト マップ エントリには、最大で 11 のトランスフォーム セットを追加できます。
- [Peer Settings - Optional for Dynamic Crypto Map Entries]：ポリシーのピア設定値を設定します。
  - [Connection Type]：（スタティック トンネルの場合にだけ該当）このポリシーの接続タイプを、bidirectional、originate-only、または answer-only から選択します。LAN-to-LAN 接続の場合は、bidirectional または answer-only（originate-only ではない）を選択します。LAN-to-LAN 冗長接続の場合は、answer-only を選択します。
  - [IP Address of Peer to Be Added]：追加する IPsec ピアの IP アドレスを入力します。
- [Enable Perfect Forwarding Secrecy]：ポリシーの完全転送秘密をイネーブルにする場合にオンにします。PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトです。IPSec ネゴシエーションでのフェーズ 2 キーは、PFS を指定しない限りフェーズ 1 に基づいて生成されます。
- [Diffie-Hellman Group]：PFS をイネーブルにする場合は、セキュリティ アプライアンスがセッション キーの生成に使用する Diffie-Hellman グループも選択する必要があります。次の選択肢があります。
  - [Group 1（768 ビット）]：完全転送秘密を使用し、Diffie-Hellman Group 1 を使用して IPsec セッション キーを生成します。このときの素数と generator 数は 768 ビットです。このオプションは高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。
  - [Group 2（1024 ビット）]：完全転送秘密を使用し、Diffie-Hellman Group 2 を使用して IPsec セッション キーを生成します。このときの素数と generator 数は 1024 ビットです。このオプションは Group 1 より高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。
  - [Group 5（1536 ビット）]：完全転送秘密を使用し、Diffie-Hellman Group 5 を使用して IPsec セッション キーを生成します。このときの素数と generator 数は 1536 ビットです。このオプションは Group 2 より高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Create IPsec Rule/Tunnel Policy (Crypto Map) - Advanced] タブ

フィールド

- [Security Association Lifetime] パラメータ：セキュリティ アソシエーション（SA）の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。

  - [Time]：時（hh）、分（mm）、および秒（ss）単位で SA のライフタイムを指定します。
  - [Traffic Volume]：キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロード データのキロバイト数を入力します。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。
- [Enable NAT-T]：このポリシーの NAT Traversal（NAT-T）をイネーブルにします。
- [Enable Reverse Route Injection]：このポリシーの逆ルート注入をイネーブルにします。
- [Static Type Only Settings]：スタティック トンネル ポリシーのパラメータを指定します。
  - [CA Certificate]：使用する証明書を選択します。デフォルトの [None]（事前共有キーを使用）以外の値を選択すると、[Enable entire chain transmission] チェックボックスがオンになります。
  - [Enable entire chain transmission]：トラスト ポイント チェーン全体での伝送をイネーブルにします。
  - [IKE Negotiation Mode]：IKE ネゴシエーション モード（Main または Aggressive）を選択します。このパラメータにより、キー情報の交換と SA のセットアップを行う場合のモードを設定します。ネゴシエーションの発信側が使用するモードを設定し、応答側は自動ネゴシエーションします。Aggressive モードは高速で、使用するパケットと交換回数を少なくすることができますが、通信パーティの ID は保護されません。Main モードは低速で、パケットと交換回数が多くなりますが、通信パーティの ID を保護します。このモードはより安全性が高く、デフォルトで選択されています。Aggressive を選択すると、Diffie-Hellman Group リストがアクティブになります。
  - [Diffie-Hellman Group]：適用する Diffie-Hellman グループを選択します。Group 1（768 ビット）、Group 2（1024 ビット）、および Group 5（1536 ビット）の中から選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Create IPsec Rule/Traffic Selection] タブ

このペインでは、保護する（許可）トラフィックまたは保護しない（拒否）トラフィックを定義できます。

フィールド

- [Action]：このルールで実行するアクションを指定します。選択肢は、[protect] と [do not protect] です。
- [Source]：送信元ホストまたはネットワークの IP アドレス、ネットワーク オブジェクト グループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。[...] をクリックして、次のフィールドを含む [Browse Source] ダイアログを開きます。
  - [Add/Edit]：送信元アドレスまたはグループを追加するには、[IP Address] または [Network Object Group] を選択します。

  - [Delete]：エントリを削除します。
  - [Filter]：表示される結果をフィルタリングする IP アドレスを入力します。
  - [Name]：続くパラメータが、送信元ホストまたはネットワークの名前を指定することを示します。
  - [IP Address]：続くパラメータが、送信元ホストまたはネットワークのインターフェイス、IP アドレス、およびサブネット マスクを指定することを示します。
  - [Netmask]：IP アドレスに適用する標準サブネット マスクを選択します。このパラメータは、[IP Address] オプション ボタンを選択すると表示されます。
  - [Description]：説明を入力します
  - [Selected Source]：選択したエントリを送信元として含めるには [Source] をクリックします。
- [Destination]：宛先ホストまたはネットワークの IP アドレス、ネットワーク オブジェクト グループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。[...] をクリックして、次のフィールドを含む [Browse Destination] ダイアログを開きます。
  - [Add/Edit]：[IP Address] または [Network Object Group] を選択して、宛先アドレスまたはグループを追加します。
  - [Delete]：エントリを削除します。
  - [Filter]：表示される結果をフィルタリングする IP アドレスを入力します。
  - [Name]：続くパラメータが、宛先ホストまたはネットワークの名前を指定することを示します。
  - [IP Address]：続くパラメータが、宛先ホストまたはネットワークのインターフェイス、IP アドレス、およびサブネット マスクを指定することを示します。
  - [Netmask]：IP アドレスに適用する標準サブネット マスクを選択します。このパラメータは、[IP Address] オプション ボタンを選択すると表示されます。
  - [Description]：説明を入力します
  - [Selected Destination]：選択したエントリを宛先として含めるには [Destination] をクリックします。
- [Service]：サービスを入力するか、または [...] をクリックして [Browse Service] ウィンドウを開き、サービスのリストから選択できます。
- [Description]：[Traffic Selection] のエントリの説明を入力します。
- More Options
  - [Enable Rule]：このルールをイネーブルにします。
  - [Source Service]：サービスを入力するか、または [...] をクリックして [Browse Service] ウィンドウを開き、サービスのリストから選択できます。
  - [Time Range]：このルールを適用する時間範囲を定義します。
  - [Group]：続くパラメータが、送信元ホストまたはネットワークのインターフェイスとグループ名を指定することを示します。
  - [Interface]：IP アドレスのインターフェイス名を選択します。このパラメータは、[IP Address] オプション ボタンを選択すると表示されます。
  - [IP address]：このポリシーが適用されるインターフェイスの IP アドレスを指定します。このパラメータは、[IP Address] オプション ボタンを選択すると表示されます。

- [Destination]：送信元または宛先のホストまたはネットワークについて、IP アドレス、ネットワーク オブジェクト グループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。これらのフィールドのいずれかで [...] をクリックし、次のフィールドを含む [Browse] ダイアログを開きます。
- [Name]：送信元または宛先のホストまたはネットワークとして使用するインターフェイス名を選択します。このパラメータは、[Name] オプション ボタンを選択すると表示されます。これは、このオプションに関連付けられる唯一のパラメータです。
- [Interface]：IP アドレスのインターフェイス名を選択します。このパラメータは、[Group] オプション ボタンを選択すると表示されます。
- [Group]：送信元または宛先のホストまたはネットワークに指定されたインターフェイスに存在するグループの名前を選択します。リストにエントリが何もない場合は、既存グループの名前を入力できます。このパラメータは、[Group] オプション ボタンを選択すると表示されます。

• [Protocol and Service]：このルールに関連するプロトコル パラメータとサービス パラメータを指定します。

（注）「Any - any」IPsec ルールは使用できません。このタイプのルールにより、デバイスおよびそのピアが複数の LAN-to-LAN トンネルをサポートできなくなります。

- [TCP]：このルールを TCP 接続に適用することを指定します。これを選択すると、[Source Port] グループ ボックスと [Destination Port] グループ ボックスも表示されます。
- [UDP]：このルールを UDP 接続に適用することを指定します。これを選択すると、[Source Port] グループ ボックスと [Destination Port] グループ ボックスも表示されます。
- [ICMP]：このルールを ICMP 接続に適用することを指定します。これを選択すると、[ICMP Type] グループ ボックスも表示されます。
- [IP]：このルールを IP 接続に適用することを指定します。これを選択すると、[IP Protocol] グループ ボックスも表示されます。
- [Manage Service Groups]：[Manage Service Groups] パネルが表示され、ここで TCP/UDP サービス / ポートのグループを追加、編集、または削除できます。
- [Source Port] および [Destination Port]：[Protocol and Service] グループ ボックスで選択したオプション ボタンに応じて、TCP または UDP のポート パラメータが表示されます。
- [Service]：個々のサービスのパラメータを指定しようとしていることを示します。フィルタの適用時に使用するサービス名とブーリアン演算子を指定します。
- [Boolean operator]（ラベルなし）：[Service] ボックスで指定したサービスを照合するときに使用するブーリアン条件（等号、不等号、大なり、小なり、または範囲）を一覧表示します。
- [Service]（ラベルなし）：照合対象のサービス（https、kerberos、その他）を指定します。range サービス演算子を指定すると、このパラメータは 2 つのボックスに変わります。ボックスに、範囲の開始値と終了値を入力します。
- [...]：サービスのリストが表示され、ここで選択したサービスが [Service] ボックスに表示されます。
- [Service Group]：送信元ポートのサービス グループの名前を指定しようとしていることを示します。
- [Service]（ラベルなし）：使用するサービス グループを選択します。
- [ICMP Type]：使用する ICMP タイプを指定します。デフォルトは any です。[...] ボタンをクリックすると、使用可能なタイプのリストが表示されます。

- オプション
  - [Time Range]：既存の時間範囲の名前を指定するか、新しい範囲を作成します。
  - [...]：[Add Time Range] ペインが表示され、ここで新しい時間範囲を定義できます。
  - [Please enter the description below (optional)]：ルールについて簡単な説明を入力するためのスペースです。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Pre-Fragmentation

このパネルでは、任意のインターフェイスの IPsec の Pre-Fragmentation ポリシーと Do-Not-Fragment（DF）ビット ポリシーを設定します。

IPSec Pre-Fragmentation ポリシーでは、パブリック インターフェイスを介してトラフィックをトンネリングするときに、最大伝送単位（MTU）の設定を超えるパケットの処理方法を指定します。この機能により、セキュリティ アプライアンスとクライアントの間のルータまたは NAT デバイスが IP フラグメントを拒否またはドロップする場合に対処できます。たとえば、クライアントがセキュリティ アプライアンスの背後の FTP サーバに対して FTP get コマンドを実行するとします。FTP サーバから送信されるパケットは、カプセル化されたときにパブリック インターフェイス上のセキュリティ アプライアンスの MTU サイズを超過します。選択したオプションにより、セキュリティ アプライアンスでのこれらのパケットの処理方法が決まります。事前フラグメンテーション ポリシーは、セキュリティ アプライアンスのパブリック インターフェイスから送出されるすべてのトラフィックに適用されます。

セキュリティ アプライアンスは、トンネリングされたすべてのパケットをカプセル化します。カプセル化した後、セキュリティ アプライアンスは、パブリック インターフェイスから送信する前に MTU の設定値を超えるパケットをフラグメント化します。これがデフォルトのポリシーです。このオプションは、フラグメント化されたパケットが、障害なしでトンネル通過を許可される状況で機能します。FTP の例では、大きなパケットがカプセル化されてから、IP レイヤでフラグメント化されます。中間デバイスは、フラグメントをドロップするか、または異常なフラグメントだけをドロップします。ロードバランシング デバイスが、異常フラグメントを取り入れる可能性があります。

事前フラグメンテーションをイネーブルにすると、セキュリティ アプライアンスは、MTU の設定値を超えるトンネリングされたパケットをカプセル化する前に、フラグメント化します。これらのパケットで DF ビットが設定されている場合、セキュリティ アプライアンスは DF ビットをクリアし、パケットをフラグメント化してからカプセル化します。このアクションにより、パブリック インターフェイスを離れる 2 つの独立した非フラグメント化 IP パケットが作成され、ピア サイトで再構成される完全なパケットにフラグメントを変換することにより、これらのパケットがピア サイトに正常に伝送されます。ここでの例では、セキュリティ アプライアンスが MTU を無効にし、DF ビットをクリアすることによってフラグメンテーションを許可します。

（注）　*いずれ*のインターフェイスであっても、[MTU] または [Pre-Fragmentation] オプションを変更すると、すべての既存接続が切断されます。たとえば、パブリック インターフェイスで 100 件のアクティブなトンネルが終了し、そのときに外部インターフェイスで [MTU] または [Pre-Fragmentation] オプションを変更すると、パブリック インターフェイスのすべてのアクティブなトンネルがドロップされます。

フィールド

- [Pre-Fragmentation]：設定済みインターフェイスごとに、現在の事前フラグメンテーションの設定を示します。
  - [Interface]：設定済みインターフェイスの名前を示します。
  - [Pre-Fragmentation Enabled]：インターフェイスごとに、事前フラグメンテーションがイネーブルになっているかどうかを示します。
  - [DF Bit Policy]：各インターフェイスの DF ビット ポリシーを示します。
- [Edit]：[Edit IPsec Pre-Fragmentation Policy] ダイアログボックスを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit IPSec Pre-Fragmentation Policy

このパネルでは、親パネル（[Configuration] > [VPN] > [IPsec] > [Pre-Fragmentation]）で選択したインターフェイスの、既存の IPsec 事前フラグメンテーション ポリシーと Do-Not-Fragment（DF）ビット ポリシーを変更します。

フィールド

- [Interface]：選択したインターフェイスを識別します。このダイアログボックスを使用しても、このパラメータは変更できません。
- [Enable IPsec pre-fragmentation]：IPSec の事前フラグメンテーションをイネーブルまたはディセーブルにします。セキュリティ アプライアンスは、カプセル化する前に、MTU の設定を超えるトンネリングされたパケットをフラグメント化します。これらのパケットで DF ビットが設定されている場合、セキュリティ アプライアンスは DF ビットをクリアし、パケットをフラグメント化してからカプセル化します。このアクションにより、パブリック インターフェイスを離れる 2 つの独立した非フラグメント化 IP パケットが作成され、ピア サイトで再構成される完全なパケットにフラグメントを変換することにより、これらのパケットがピア サイトに正常に伝送されます。
- [DF Bit Setting Policy]：Do-Not-Fragment ビット ポリシー（[Copy]、[Clear]、または [Set]）を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

IPSec Transform Sets

このパネルでは、トランスフォーム セットを表示、追加、または編集します。トランスフォームは、データ フローで実行される操作のセットで、データ認証、データ機密性、およびデータ圧縮を実現します。たとえば、1 つのトランスフォームは、3DES 暗号化と HMAC-MD5 認証アルゴリズム（ESP-3DES-MD5）による ESP プロトコルです。

フィールド

- [Transform Sets]：設定されたトランスフォーム セットを示します。
  - [Name]：トランスフォーム セットの名前を示します。
  - [Mode]：トランスフォーム セットのモード（Tunnel）を示します。このパラメータにより、ESP 暗号化と認証を適用する場合のモードを指定します。言い換えると、ESP が適用されている元の IP パケットの部分を指定します。Tunnel モードでは、ESP 暗号化と認証が元の IP パケット全体（IP ヘッダーとデータ）に適用されるため、本来の送信元アドレスと宛先アドレスが隠されることになります。
  - [ESP Encryption]：トランスフォーム セットのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズムを示します。ESP では、データ プライバシー サービス、オプションのデータ認証、およびリプレイ攻撃防止サービスが提供されます。ESP は、保護されているデータを*カプセル化*します。
  - [ESP Authentication]：トランスフォーム セットの ESP 認証アルゴリズムを示します。
- [Add]：[Add Transform Set] ダイアログボックスが開き、ここで新しいトランスフォーム セットを追加できます。
- [Edit]：[Edit Transform Set] ダイアログボックスが開き、ここで既存のトランスフォーム セットを変更できます。
- [Delete]：選択したトランスフォーム セットを削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Transform Set

このパネルでは、トランスフォーム セットを追加または変更します。トランスフォームは、データ フローで実行される操作のセットで、データ認証、データ機密性、およびデータ圧縮を実現します。たとえば、1 つのトランスフォームは、3DES 暗号化と HMAC-MD5 認証アルゴリズム（ESP-3DES-MD5）による ESP プロトコルです。

フィールド

- [Set Name]：このトランスフォーム セットの名前を指定します。
- [Properties]：このトランスフォーム セットのプロパティを設定します。これらのプロパティは、[Transform Sets] テーブルに表示されます。
  - [Mode]：トランスフォーム セットのモード（Tunnel）を示します。このフィールドは、ESP 暗号化と認証を適用する場合のモードを示します。言い換えると、ESP を適用している元の IP パケットの部分を指定します。Tunnel モードでは、ESP 暗号化と認証が元の IP パケット全体（IP ヘッダーとデータ）に適用されるため、本来の送信元アドレスと宛先アドレスが隠されることになります。
  - [ESP Encryption]：トランスフォーム セットのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズムを選択します。ESP では、データ プライバシー サービス、オプションのデータ認証、およびリプレイ攻撃防止サービスが提供されます。ESP は、保護されているデータを*カプセル化*します。
  - [ESP Authentication]：トランスフォーム セットの ESP 認証アルゴリズムを選択します。

（注） IPSec ESP（Encapsulating Security Payload）プロトコルでは、暗号化と認証の両方の機能が提供されます。パケット認証により、データが、データに記述されている送信元から送信されたことを保証します。これは、「データ整合性」とも呼ばれます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Load Balancing

（注） VPN ロード バランシングを使用するには、Plus ライセンスを備えた ASA モデル 5510、または ASA モデル 5520 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

このウィンドウでは、セキュリティ アプライアンスでのロード バランシングをイネーブルにすることができます。ロード バランシングをイネーブルにするには、次の手順を実行します。

- 共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタの IPsec 共有秘密情報を確立することによりロードバランシング クラスタを設定する。これらの値は、クラスタ内のすべてのデバイスで同一です。
- デバイスでロード バランシングをイネーブルにし、デバイス固有のプロパティを定義することにより、参加デバイスを設定する。これらの値はデバイスによって異なります。

リモートクライアント コンフィギュレーションで、複数のセキュリティ アプライアンスを同じネットワークに接続してリモート セッションを処理している場合、これらのデバイスでセッション負荷を分担するように設定できます。この機能は、*ロード バランシング*と呼ばれます。ロード バランシングでは、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。これによって、システム リソースを効率的に利用でき、パフォーマンスと可用性が向上します。

（注） ロード バランシングは、Cisco VPN Client（リリース 3.0 以降）、Cisco VPN 3002 Hardware Client（リリース 3.5 以降）、または Easy VPN クライアントとして動作している ASA 5505 で開始されたリモート セッションだけで有効です。LAN 間接続を含む他のすべてのクライアントは、ロード バランシングがイネーブルなセキュリティ アプライアンスに接続できますが、ロード バランシングには参加できません。

ロード バランシングを実装するには、同じプライベート LAN 間ネットワーク上の複数のデバイスを、論理的に*仮想クラスタ*としてグループ化します。

セッションの負荷は、仮想クラスタ内のすべてのデバイスに分散されます。仮想クラスタ内の 1 つのデバイスである*仮想クラスタ マスター*は、着信コールを*セカンダリ デバイス*と呼ばれる他のデバイスに転送します。仮想クラスタ マスターは、クラスタ内のすべてのデバイスをモニタし、各デバイスの負荷を追跡して、その負荷に基づいてセッションの負荷を分散します。仮想クラスタ マスターの役割は、1 つの物理デバイスに結び付けられるものではなく、デバイス間でシフトできます。たとえば、現在の仮想クラスタ マスターで障害が発生すると、クラスタ内のセカンダリ デバイスの 1 つがその役割を引き継いで、すぐに新しい仮想クラスタ マスターになります。

仮想クラスタは、外部のクライアントには 1 つの*仮想クラスタ IP アドレス*として表示されます。この IP アドレスは、特定の物理デバイスに結び付けられていません。現在の仮想クラスタ マスターに属しているため、仮想のアドレスです。接続の確立を試みている VPN クライアントは、最初にこの仮想クラスタ IP アドレスに接続します。仮想クラスタ マスターは、クラスタ内で使用できるホストのうち、最も負荷の低いホストのパブリック IP アドレスをクライアントに返します。2 回目のトランザクションで、クライアントは直接そのホストに接続します（この動作はユーザには透過的です）。仮想クラスタ マスターは、このようにしてリソース全体に均等かつ効率的にトラフィックを転送します。

（注） Cisco VPN Client、Cisco VPN 3002 ハードウェア クライアント、または Easy VPN クライアントとして動作している ASA 5505 以外のすべてのクライアントは、通常どおりセキュリティ アプライアンスに直接接続し、仮想クラスタ IP アドレスを使用しません。

クラスタ内のマシンで障害が発生すると、終了されたセッションはただちに仮想クラスタ IP アドレスに再接続できます。次に、仮想クラスタ マスターは、クラスタ内の別のアクティブ デバイスにこれらの接続を転送します。仮想クラスタ マスター自体に障害が発生した場合、クラスタ内のセカンダリ デバイスが、ただちに新しい仮想セッション マスターを自動的に引き継ぎます。クラスタ内の複数のデバイスで障害が発生しても、クラスタ内のデバイスが 1 つ稼働していて使用可能である限り、ユーザはクラスタに引き続き接続できます。

前提条件

ロード バランシングはデフォルトではディセーブルになっています。ロード バランシングは明示的にイネーブルにする必要があります。

まず、パブリック インターフェイスとプライベート インターフェイスを設定するとともに、仮想クラスタ IP アドレスの参照先の仮想クラスタ IP のインターフェイスをあらかじめ設定する必要があります。

クラスタに参加するすべてのデバイスは、同じクラスタ固有の値（IP アドレス、暗号化設定、暗号キー、およびポート）を共有する必要があります。クラスタ内のロードバランシング デバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

フィールド

- [VPN Load Balancing]：仮想クラスタ デバイスのパラメータを設定します。
  - [Participate in Load Balancing Cluster]：このデバイスがロードバランシング クラスタの参加デバイスであることを指定します。
  - [VPN Cluster Configuration]：デバイスのパラメータを設定します。パラメータは、仮想クラスタ全体で同じにする必要があります。すべてのクラスタに同一のクラスタ設定を行う必要があります。
  - [Cluster IP Address]：仮想クラスタ全体を表す単一の IP アドレスを指定します。仮想クラスタ内のすべてのセキュリティ アプライアンスが共有するパブリック サブネットのアドレス範囲内で、IP アドレスを選択します。
  - [UDP Port]：このデバイスが参加する仮想クラスタの UDP ポートを指定します。デフォルト値は 9023 です。別のアプリケーションでこのポートが使用されている場合は、ロードバランシングに使用する UDP の宛先ポート番号を入力します。
  - [Enable IPSec Encryption]：IPSec 暗号化をイネーブルまたはディセーブルにします。このチェックボックスをオンにする場合は、共有秘密情報を指定し、確認する必要もあります。仮想クラスタ内のセキュリティ アプライアンスは、IPsec を使用して LAN-to-LAN トンネルを介して通信します。デバイス間で通信されるすべてのロード バランシング情報が暗号化されるようにするには、このチェックボックスをオンにします。

（注） 暗号化を使用する場合、事前にロードバランシング内部インターフェイスを設定しておく必要があります。そのインターフェイスがロードバランシング内部インターフェイスでイネーブルになっていない場合、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

クラスタの暗号化を設定したときにロード バランシング内部インターフェイスがイネーブルに設定されたが、仮想クラスタへのデバイス参加を設定する前にディセーブルにされた場合は、[Participate in Load Balancing Cluster] チェックボックスをオンにしたときにエラー メッセージが表示され、そのクラスタに対して暗号化はイネーブルになりません。

  - [IPSec Shared Secret] : IPSec 暗号化がイネーブルになっているときに、IPSec ピア間の共有秘密を指定します。ボックスに入力する値は、連続するアスタリスク文字として表示されます。
  - [Verify Secret] : [IPSec Shared Secret] ボックスに入力された共有秘密情報の値を確認します。
- [VPN Server Configuration]：この特定のデバイスのパラメータを設定します。
  - [Interfaces]：パブリックとプライベートのインターフェイス、およびそれぞれの関連パラメータを設定します。

- [Public]：このデバイスのパブリック インターフェイスの名前または IP アドレスを指定します。
- [Private]：このデバイスのプライベート インターフェイスの名前または IP アドレスを指定します。
- [Priority]：クラスタ内でこのデバイスに割り当てるプライオリティを指定します。指定できる範囲は 1 ～ 10 です。プライオリティは、起動時または既存のマスターで障害が発生したときに、このデバイスが仮想クラスタ マスターになる可能性を表します。優先順位を高く設定すれば（10 など）、このデバイスが仮想クラスタ マスターになる可能性が高くなります。

（注） 仮想クラスタ内のデバイスを異なるタイミングで起動した場合、最初に起動したデバイスが、仮想クラスタ マスターの役割を果たすと想定されます。仮想クラスタにはマスターが必要であるため、起動したときに仮想クラスタ内の各デバイスはチェックを行い、クラスタに仮想マスターがあることを確認します。仮想マスターがない場合、そのデバイスがマスターの役割を果たします。後で起動し、クラスタに追加されたデバイスは、セカンダリ デバイスになります。仮想クラスタ内のすべてのデバイスが同時に起動されたときは、最高の優先順位が設定されたデバイスが仮想クラスタ マスターになります。仮想クラスタ内の複数のデバイスが同時に起動され、いずれも最高の優先順位が設定されている場合、最も低い IP アドレスを持つデバイスが仮想クラスタ マスターになります。

- [NAT Assigned IP Address]：このデバイスの IP アドレスを NAT によって変換した結果の IP アドレスを指定します。NAT が使用されない場合、またはデバイスが NAT を使用するファイアウォールの背後にない場合は、0.0.0.0 を入力します。
- [Send FQDN to client]：このチェックボックスをオンにすると、VPN クラスタ マスターが VPN クライアント接続をクラスタ デバイスにリダイレクトするときに、外部 IP アドレスの代わりにクラスタ デバイスのホスト名とドメイン名を使用して完全修飾ドメイン名が送信されるようになります。

IP アドレスではなく FQDN を使用してクライアントレス SSL VPN ロード バランシングをイネーブルにするには、次の設定手順を実行する必要があります。

ステップ 1　[Send FQDN to client...] チェックボックスをオンにして、ロード バランシングでの FQDN の使用をイネーブルにします。

ステップ 2　使用するセキュリティ アプライアンスの外部インターフェイスのエントリがまだ存在しない場合は、各インターフェイスのエントリを DNS サーバに追加します。セキュリティ アプライアンスの各外部 IP アドレスには、ルックアップ用に関連付けられている DNS エントリが含まれている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。

ステップ 3　[Configuration] > [Device Management] > [DNS] > [DNS Client] ダイアログボックスで、DNS サーバへのルートを持つインターフェイスのセキュリティ アプライアンスでの DNS 検索をイネーブルにします。

ステップ 4　セキュリティ アプライアンスで DNS サーバの IP アドレスを定義します。これには、このダイアログボックスの [Add] をクリックします。[Add DNS Server Group] ダイアログボックスが開きます。追加する DNS サーバの IP アドレスを入力します。たとえば、`192.168.1.1`（DNS サーバの IP アドレス）と入力できます。

ステップ 5　[OK] および [Apply] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

グローバル NAC パラメータの設定

セキュリティ アプライアンスは、Extensible Authentication Protocol（EAP）over UDP（EAPoUDP）のメッセージを使用して、リモート ホストのポスチャを確認します。ポスチャ検証では、リモート ホストにネットワーク アクセス ポリシーを割り当てる前に、そのホストがセキュリティの必要条件を満たしているかどうかが調べられます。セキュリティ アプライアンスでネットワーク アドミッション コントロールを設定する前に、NAC 用に Access Control Server を設定しておく必要があります。

フィールド

[NAC] ウィンドウでは、すべての NAC 通信に適用される属性を設定できます。ウィンドウの一番上に表示される次のグローバル属性は、セキュリティ アプライアンスとリモート ホストの間の EAPoUDP メッセージングに適用されます。

- [Port] : ホストの Cisco Trust Agent（CTA）との EAP over UDP 通信で使用するポート番号。この番号は、CTA で設定されているポート番号と一致する必要があります。値は 1024 ～ 65535 の範囲で入力します。デフォルト設定は 21862 です。
- [Retry if no response] : セキュリティ アプライアンスが EAP over UDP メッセージを再送信する回数。この属性により、Rechallenge Interval の期限切れに対して送信されるメッセージの連続再試行回数を制限します。この設定は秒単位です。値は 1 ～ 3 の範囲で入力します。デフォルト設定は 3 です。
- [Rechallenge Interval] : セキュリティ アプライアンスは、EAPoUDP メッセージをホストに送信するときにこのタイマーを開始します。ホストからの応答があるとタイマーがクリアされます。応答を受信する前にタイマーが期限切れになると、セキュリティ アプライアンスはメッセージを再送信します。この設定は秒単位です。1 ～ 60 の範囲で値を入力します。デフォルト設定は 3 です。
- [Wait before new PV Session] : セキュリティ アプライアンスは、リモート ホストの NAC セッションを保持状態にしたときにこのタイマーを開始します。セッションが保持状態になるのは、送信された EAPoUDP メッセージの数が [Retry if no response] 設定の値に達しても応答を受信できない場合です。セキュリティ アプライアンスは、ACS サーバから「Access Reject」メッセージを受信した後にも、このタイマーを開始します。タイマーが期限切れになると、セキュリティ アプライアンスはリモート ホストとの新しい EAP over UDP アソシエーションの開始を試みます。この設定は秒単位です。60 ～ 86400 の範囲で値を入力します。デフォルト設定は 180 です。

[NAC] ウィンドウの [Clientless Authentication] 領域では、EAPoUDP 要求に応答しないホストの設定値を設定できます。CTA が実行されていないホストは、これらの要求に応答しません。

- [Enable clientless authentication] : クライアントレス認証をイネーブルにします。セキュリティ アプライアンスは、ユーザ認証要求の形式で、設定されているクライアントレス ユーザ名とパスワードを Access Control Server に送信します。次に、ACS はクライアントレス ホストのアクセス ポリシーを要求します。この属性をブランクのままにすると、セキュリティ アプライアンスはクライアントレス ホストのデフォルト ACL を適用します。

- [Clientless Username] : ACS のクライアントレス ホストに設定するユーザ名。デフォルト設定は clientless です。1 ～ 64 文字の ASCII 文字を入力します。先頭および末尾のスペース、ポンド記号（#）、疑問符（?）、一重または二重引用符（' と "）、アスタリスク（*）、山カッコ（< と >）は除外します。
- [Password] : ACS のクライアントレス ホストに設定するパスワード。デフォルト設定は clientless です。4 ～ 32 文字の ASCII 文字を入力します。
- [Confirm Password] : 確認のために再入力する、ACS のクライアントレス ホストに設定するパスワード。
- [Enable Audit] : クライアントがポスチャ検証要求に応答しない場合に、クライアントの IP アドレスをオプションの監査サーバに渡します。監査サーバ（Trend サーバなど）では、ホスト IP アドレスを使用して、ホストに対して直接チャレンジを行い、ホストのヘルスを評価します。たとえば、ホストに対してチャレンジを行い、そのウイルス チェック ソフトウェアがアクティブで最新の状態かどうかを判断します。監査サーバは、リモート ホストとの対話を完了すると、リモート ホストのヘルスを示すトークンをポスチャ検証サーバに渡します。
- [None] : クライアントレス認証と監査サービスをディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

ネットワーク アドミッション コントロールのポリシーの設定

[NAC Policies] テーブルには、セキュリティ アプライアンスで設定されているネットワーク アドミッション コントロール（NAC）のポリシーが表示されます。

NAC ポリシーを追加、変更、または削除するには、次のいずれかの操作を実行します。

- NAC ポリシーを追加するには、[Add] を選択します。[Add NAC Framework Policy] ダイアログボックスが開きます。
- NAC ポリシーを変更するには、そのポリシーをダブルクリックするか、ポリシーを選択して [Edit] をクリックします。[Edit NAC Framework Policy] ダイアログボックスが開きます。
- NAC ポリシーを削除するには、ポリシーを選択して [Delete] をクリックします。

次の各項では、NAC、NAC の要件、およびポリシー属性への値の割り当て方法を説明します。

NAC について

NAC は、エンドポイント準拠および脆弱性チェックをネットワークへの実稼働アクセスの条件として実行することにより、ワーム、ウイルス、および不正なアプリケーションの侵入や感染からエンタープライズ ネットワークを保護します。これらのチェックは、*ポスチャ検証* と呼ばれます。イントラネット上の脆弱なホストにアクセスする前に、ポスチャ検証を設定して、AnyConnect またはクライアントレス SSL VPN セッションを使用するホスト上のアンチウイルス ファイル、パーソナル ファイア ウォール ルール、または侵入保護ソフトウェアが最新の状態であることを確認できます。ポスチャ検証の一部として、リモート ホストで実行されているアプリケーションが最新のパッチで更新されているか検証することもできます。NAC は、ユーザ認証およびトンネルの設定の完了後に行われます。自動ネットワーク ポリシー実施が適用されないホスト（ホーム PC など）からエンタープライズ ネットワークを保護する場合は、NAC が特に有用です。

エンドポイントとセキュリティ アプライアンス間でトンネルを確立すると、ポスチャ検証がトリガーされます。

クライアントがポスチャ検証の要求に応答しない場合は、セキュリティ アプライアンスを設定して、そのクライアントの IP アドレスをオプションの監査サーバに渡すことができます。監査サーバ（Trend サーバなど）では、ホスト IP アドレスを使用して、ホストに対して直接チャレンジを行い、ホストのヘルスを評価します。たとえば、ホストに対してチャレンジを行い、そのウイルス チェック ソフトウェアがアクティブで最新の状態かどうかを判断します。監査サーバは、リモート ホストとの対話を完了すると、リモート ホストのヘルスを示すトークンをポスチャ検証サーバに渡します。

ポスチャ検証が成功する、またはリモート ホストが正常であることを示すトークンを受信すると、ポスチャ検証サーバは、トンネル上のトラフィックに対するアプリケーション用のネットワーク アクセス ポリシーをセキュリティ アプライアンスに送信します。

セキュリティ アプライアンスを含む *NAC Framework* のコンフィギュレーションには、クライアントで実行されている Cisco Trust Agent だけがポスチャ エージェントの役割を果たすことができ、Cisco Access Control Server（ACS）だけがポスチャ検証サーバの役割を果たすことができます。ACS はダイナミック ACL を使用して、各クライアントのアクセス ポリシーを決定します。

RADIUS サーバである ACS は、ポスチャ検証サーバとしての役割を果たすことに加え、トンネルの確立に必要なログイン クレデンシャルを認証できます。

（注） セキュリティ アプライアンスに設定されている NAC Framework ポリシーだけが、監査サーバの使用をサポートしています。

ACS はそのポスチャ検証サーバとしての役割において、アクセス コントロール リストを使用します。ポスチャ検証が成功し、ACS によって、セキュリティ アプライアンスに送信するアクセス ポリシーの一部としてリダイレクト URL が指定されると、セキュリティ アプライアンスは、リモート ホストからのすべての HTTP 要求と HTTPS 要求をリダイレクト URL にリダイレクトします。ポスチャ検証サーバによってアクセス ポリシーがセキュリティ アプライアンスにアップロードされると、関連するすべてのトラフィックはその宛先に到達するためにセキュリティ アプライアンスと ACS（またはその逆も同じ）の両方を通過する必要があります。

NAC フレームワーク ポリシーがグループ ポリシーに割り当てられている場合は、リモート ホストとセキュリティ アプライアンスの間にトンネルが確立されるとポスチャ検証が実行されます。ただし、NAC Framework ポリシーでは、ポスチャ検証を免除されているオペレーティング システムを特定し、そのようなトラフィックをフィルタリングするためにオプションの ACL を指定できます。

使用方法、要件、および制限

NAC をサポートするように設定すると、セキュリティ アプライアンスは、Cisco Secure Access Control Server のクライアントとして機能します。そのため、NAC 認証サービスを提供するために、ネットワーク上に少なくとも 1 台の Access Control Server をインストールする必要があります。

ネットワークで 1 台以上の Access Control Server を設定した後は、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add or Edit External] メニュー オプションを使用して Access Control Server グループを登録する必要があります。その後、NAC ポリシーを追加します。

ASA による NAC フレームワークのサポートは、リモート アクセス IPSec セッションとクライアントレス SSL VPN セッションに限られています。NAC Framework コンフィギュレーションは、シングル モードだけをサポートしています。

ASA における NAC では、レイヤ 3（非 VPN）および IPv6 トラフィックはサポートされていません。

フィールド

- [Policy Name]：新しい NAC ポリシーの名前を最大 64 文字で入力します。

  NAC ポリシーのコンフィギュレーションに続いて、Network (Client) Access グループ ポリシーの NAC Policy 属性の隣にポリシー名が表示されます。属性または目的を、設定する他の属性または目的と区別できるように名前を割り当てます。

- [Status Query Period]：セキュリティ アプライアンスは、ポスチャ検証とステータス クエリーの応答が成功するたびに、このタイマーを開始します。このタイマーが切れると、ホスト ポスチャの変化を調べるクエリー（*ステータス クエリー*と呼ばれる）がトリガーされます。30 ～ 1800 の範囲で秒数を入力します。デフォルトの設定は 300 秒です。

- [Revalidation Period]：セキュリティ アプライアンスは、ポスチャ検証が成功するたびに、このタイマーを開始します。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。セキュリティ アプライアンスでは、再検証中はポスチャ検証が維持されます。ポスチャ検証または再検証中にアクセス コントロール サーバが使用できない場合、デフォルトのグループ ポリシーが有効になります。ポスチャを検証する間隔を秒数で入力します。指定できる範囲は 300 ～ 86400 です。デフォルトの設定は 36000 秒です。

- [Default ACL]：（任意）ポスチャ検証が失敗した場合、セキュリティ アプライアンスは、選択された ACL に関連付けられているセキュリティ ポリシーを適用します。[None] を選択するか、リストの拡張 ACL を選択します。デフォルト設定は [None] です。設定が [None] のときにポスチャ検証に失敗した場合、セキュリティ アプライアンスはデフォルト グループ ポリシーを適用します。

  [Manage] ボタンを使用して、ドロップダウン リストを読み込み、リストに ACL の設定を表示します。

- [Manage]：[ACL Manager] ダイアログボックスを開きます。クリックして、標準 ACL および各 ACL の ACE を表示、イネーブル化、ディセーブル化、削除します。[Default ACL] 属性の横のリストに [ACL] が表示されます。

- [Authentication Server Group]：ポスチャ検証用に使用する認証サーバ グループを指定します。この属性の横にあるドロップダウン リストには、セキュリティ アプライアンスに設定され、リモート アクセス トンネルで利用できる RADIUS タイプのすべてのサーバ グループ名が表示されます。NAC をサポートするように設定された、少なくとも 1 台のサーバで構成される ACS グループを選択します。

- [Posture Validation Exception List]：ポスチャ検証からリモート コンピュータを除外する 1 つ以上の属性が表示されます。各エントリには、少なくともオペレーティング システムと、[Yes] または [No] いずれかの [Enabled] 設定が含まれています。オプションのフィルタが、リモート コンピュータの追加属性を一致させる ACL を識別します。ポスチャ検証からリモート コンピュータを除外するには、オペレーティング システムで構成されたエントリとフィルタの両方に一致する必要があります。セキュリティ アプライアンスは、[Enabled] 設定が [No] に設定されているエントリを無視します。

- [Add]：エントリを [Posture Validation Exception] リストに追加します。

- [Edit]：[Posture Validation Exception] リストのエントリを修正します。

- [Delete]：エントリを [Posture Validation Exception] リストから削除します。

次の作業

NAC ポリシーのコンフィギュレーションに続いて、そのポリシーをアクティブにするためにグループ ポリシーに割り当てる必要があります。このようにするには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [General] > [More Options] を選択し、[NAC Policy] 属性の横にあるドロップダウン リストから NAC ポリシー名を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Posture Validation Exception

[Add/Edit Posture Validation Exception] ダイアログ ウィンドウでは、オペレーティング システム、およびフィルタに一致するオプションの属性に基づいてリモート コンピュータをポスチャ検証から除外できます。

- [Operating System]：リモート コンピュータのオペレーティング システムを選択します。コンピュータでこのオペレーティング システムが実行されている場合は、ポスチャ検証から除外されます。デフォルト設定は空白です。
- [Enable]：[Enabled] をオンにした場合にだけ、セキュリティ アプライアンスは、このウィンドウに表示される属性設定がリモート コンピュータに存在するかどうかをチェックします。オフにした場合は、属性設定が無視されます。デフォルト設定では、無効になっています。
- [Filter]（任意）：コンピュータのオペレーティング システムが Operating System 属性の値に一致する場合に、トラフィックに ACL を適用してフィルタリングします。
- [Manage]：[ACL Manager] ダイアログボックスを開きます。クリックして、標準 ACL および各 ACL の ACE を表示、イネーブル化、ディセーブル化、削除します。[Default ACL] 属性の横のリストに [ACL] が表示されます。このボタンを使用して、[Filter] 属性の横のリストに入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

CHAPTER 32

General

バーチャル プライベート ネットワーク（VPN）とは、インターネットなどのパブリック ネットワーク経由でプライベート トラフィックを伝送する仮想回線のネットワークのことです。VPN は、2 か所以上の LAN、またはリモート ユーザと LAN を接続できます。VPN は、すべてのユーザに認証を義務付け、すべてのデータ トラフィックを暗号化することにより、プライバシーとセキュリティを確保します。

Client Software

[Client Software] ペインにより、中央にいる管理者は次のアクションを実行できます。

- クライアント アップデートをイネーブルにする。アップデートを適用するクライアントのタイプとリビジョン番号を指定する。
- アップデートを取得する URL または IP アドレスを指定する。
- Windows クライアントの場合に、オプションで VPN クライアント バージョンをアップデートする必要があることをユーザに通知する。

（注） [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [Upload Software] > [Client Software] で選択できるクライアント アップデート機能は、IPSec VPN クライアント（Windows、MAC OS X、および Linux）と VPN 3002 ハードウェア クライアントにだけ適用されます。これは、Cisco AnyConnect VPN クライアントには適用されません。接続時にセキュリティ アプライアンスによって自動的にアップデートされます。

IPSec VPN クライアントの場合は、アップデートを実行するメカニズムをユーザに提供できます。VPN 3002 ハードウェア クライアント ユーザの場合、アップデートは通知せずに自動的に行われます。クライアント アップデートは、IPSec リモートアクセス トンネルグループのタイプだけに適用できます。

（注） IPSec Site-to-Site IPSec 接続またはクライアントレス VPN IPSec 接続を対象にクライアント アップデートを試みても、エラー メッセージは表示されず、アップデート通知やクライアント アップデートがそれらのタイプの IPSec 接続に届くことはありません。

特定のクライアント タイプのすべてのクライアントに対してクライアント アップデートをグローバルにイネーブルにするには、このウィンドウを使用します。また、このウィンドウから、アップグレードが必要であることをすべての Windows、MAC OS X、および Linux クライアントに通知し、すべての

VPN 3002 ハードウェア クライアントのアップグレードを開始することもできます。アップデートの適用先クライアント リビジョンと、アップデートのダウンロード元 URL または IP アドレスを設定するには、[Edit] をクリックします。

特定のトンネル グループのクライアント アップデート リビジョンとソフトウェア アップデート ソースを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPSec] > [Add/Edit] > [Advanced] > [IPSec] > [Client Software Update] を参照してください。

フィールド

- [Enable Client Update]：すべてのトンネル グループと特定のトンネル グループの両方を対象にクライアント アップデートをイネーブルまたはディセーブルにします。クライアント アップデートをイネーブルにしてから、Windows、MAC OS X、および Linux の VPN クライアントにクライアント アップデート通知を送信するか、またはハードウェア クライアントの自動アップデートを開始する必要があります。
- [Client Type]：アップグレードするクライアント（ソフトウェアまたはハードウェア）を一覧表示します。Windows ソフトウェア クライアントの場合には、すべての Windows またはサブセットを表示します。[All Windows Based] をクリックした場合には、Windows 95、98 または ME と Windows NT、2000 または XP を個別に指定しません。ハードウェア クライアントは、ASA 5505 ソフトウェアまたは VPN 3002 ハードウェア クライアントのリリースと一緒にアップデートされます。
- [VPN Client Revisions]：このクライアントに合ったソフトウェア イメージ リビジョンのカンマ区切りリストを格納しています。ユーザのクライアント リビジョン番号が、指定されているリビジョン番号のいずれかと一致している場合には、クライアントを更新する必要はありません。Windows ベースのクライアントの場合には、アップデート通知を受信しません。次の警告が適用されます。
  - リビジョン リストには、このアップデートのソフトウェア バージョンが記載されている必要があります。
  - 自分のエントリが、VPN クライアントの場合には URL と、ハードウェア クライアントの場合には TFTP サーバと正確に一致する必要があります。
  - ハードウェア クライアント イメージを配布するための TFTP サーバは堅牢である必要があります。
  - VPN クライアント ユーザは、一覧表示されている URL から適切なソフトウェア バージョンをダウンロードする必要があります。
  - VPN 3002 ハードウェア クライアント ソフトウェアは、ユーザに通知することなく、自動的に TFTP 経由でアップデートされます。
- [Image URL]：ソフトウェア イメージのダウンロード元 URL または IP アドレスを格納しています。この URL は、クライアントに適合するファイルを指している必要があります。Windows、MAC OS X、および Linux ベースのクライアントの場合は、URL を http:// または https:// 形式にする必要があります。ハードウェア クライアントの場合、URL は tftp:// という形式にする必要があります。
  - Windows、MAC OS X、および Linux ベースの VPN クライアントの場合：VPN クライアント通知で [Launch] ボタンをアクティブにするには、URL に、HTTP または HTTPS というプロトコル名と、アップデートが格納されているサイトのサーバ アドレスを含める必要があります。URL の形式は、http(s):// *サーバ_ アドレス: ポート/ ディレクトリ/ ファイル名*です。DNS サーバが設定済みの場合、IP アドレスまたはホスト名のどちらもサーバ アドレスとして使用できます。次に例を示します。

    http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe

    ディレクトリはオプションです。ポート番号は、80 以外の HTTP ポート、443 以外の HTTPS ポートを使用する場合にだけ必要です。

  - ハードウェア クライアントの場合、URL の形式は、tftp:// *サーバ_アドレス/ディレクトリ/ファイル名*です。DNS サーバが設定済みの場合、IP アドレスまたはホスト名のどちらもサーバ アドレスとして使用できます。次に例を示します。

    tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin

- [Edit] : [Edit Client Update Entry] ダイアログボックスを開きます。このボックスを使用して、クライアント アップデート パラメータを設定または変更できます。[Edit Client Update] のエントリを参照してください。
- [Live Client Update] : 現在接続中のすべての VPN クライアント、または選択したトンネル グループにアップグレード通知メッセージを送信します。
  - [Tunnel Group] : すべてまたは特定のトンネル グループをアップデートの対象として選択します。
  - [Update Now] : アップグレード通知をただちに送信します。この通知には、選択したトンネル グループまたは接続中のすべてのトンネル グループ内で現在接続中の VPN クライアントを対象とするアップデート済みソフトウェアの取得場所を指定する URL が記載されています。メッセージには、ソフトウェアの新バージョンをダウンロードする場所が記載されています。その VPN クライアントの管理者は、新しいソフトウェア バージョンを取得し、VPN クライアント ソフトウェアをアップデートできます。

    VPN 3002 ハードウェア クライアントの場合、アップグレードは通知せずに自動的に行われます。

    アップグレードを実行するには、ウィンドウ内の [Enable Client Update] をオンにする必要があります。接続していないクライアントは、アップグレード通知を受信するか、次回ログインしたときに自動的にアップグレードされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Edit Client Update] のエントリ

[Edit Client Update] ダイアログボックスでは、表示されたクライアント タイプの VPN クライアント リビジョンと URL に関する情報を変更できます。クライアントは、表示されたクライアント タイプ用として指定されているいずれかのリビジョンを実行している必要があります。該当するリビジョンを実行していないと、そのクライアントは、アップグレードが必要であると通知されます。

フィールド

- [Client Type] :（*表示専用*）編集対象として選択したクライアント タイプを表示します。
- [VPN Client Revisions] : このクライアントに合ったソフトウェアまたはファームウェア イメージのカンマ区切りリストを入力できます。ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントを更新する必要はありません。クライアントがリストにあるソフトウェア バージョンを実行していなくても、更新は正しく実行されます。

Windows、MAC OS X、または Linux ベースの VPN クライアントのユーザは、一覧表示されている URL から適切なソフトウェア バージョンをダウンロードする必要があります。VPN 3002 ハードウェア クライアント ソフトウェアは、自動的に TFTP 経由でアップデートされます。

- [Image URL]：ソフトウェアまたはファームウェア イメージの URL を指定できます。この URL は、クライアントに適合するファイルを指している必要があります。
  - Windows、MAC OS X、または Linux ベースの VPN クライアントの場合は、URL に、HTTP または HTTPS というプロトコル名と、アップデートが存在するサイトのサーバ アドレスが指定されている必要があります。URL の形式は、http(s):// *サーバ_アドレス: ポート/ディレクトリ/ファイル名*です。DNS サーバが設定済みの場合、IP アドレスまたはホスト名のどちらもサーバ アドレスとして使用できます。次に例を示します。

    ```
    http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe
    ```

    ディレクトリはオプションです。ポート番号は、80 以外の HTTP ポート、443 以外の HTTPS ポートを使用する場合にだけ必要です。
  - ハードウェア クライアントの場合、URL の形式は、tftp:// *サーバ_アドレス/ディレクトリ/ファイル名*です。DNS サーバが設定済みの場合、IP アドレスまたはホスト名のどちらもサーバ アドレスとして使用できます。次に例を示します。

    tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin

    ディレクトリはオプションです。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

デフォルトのトンネル ゲートウェイ

デフォルトのトンネル ゲートウェイを設定するには、このウィンドウにある [Static Route] リンクをクリックします。[Configuration] > [Routing] > [Routing] > [Static Route] ウィンドウが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

グループ ポリシー

[Group Policies] ウィンドウでは、VPN グループ ポリシーを管理できます。VPN グループ ポリシーは、デバイスの内部（ローカル）または外部の RADIUS または LDAP サーバに格納されているユーザ指向の属性と値のペアのセットです。VPN グループ ポリシーを設定することによって、個別のグループまたはユーザ名レベルで設定しなかった属性をユーザが継承するようにできます。デフォルトでは、VPN ユーザにはグループ ポリシーが関連付けられません。グループ ポリシー情報は、VPN トンネル グループおよびユーザ アカウントで使用されます。

「子」の関係のウィンドウとダイアログボックスでは、デフォルト グループのパラメータを含むグループ パラメータを設定できます。デフォルト グループ パラメータは、すべてのグループおよびユーザに共通であると考えられるパラメータで、これらによってコンフィギュレーション タスクが効率化されます。グループはデフォルト グループからパラメータを「継承」でき、ユーザは自身のグループまたはデフォルト グループからパラメータを「継承」できます。これらのパラメータは、グループおよびユーザを設定するときに上書きできます。

内部または外部いずれかのグループ ポリシーを設定できます。内部グループ ポリシーはローカルに保存され、外部グループ ポリシーは RADIUS サーバまたは LDAP サーバに外部で保存されます。[Edit] をクリックすると類似のダイアログボックスが開き、新しいグループ ポリシーを作成したり、既存のグループ ポリシーを編集したりできます。

これらのダイアログボックスで、次の種類のパラメータを設定します。

- 一般属性：名前、バナー、アドレス プール、プロトコル、フィルタリング、および接続の設定。
- サーバ：DNS および WINS サーバ、DHCP スコープ、およびデフォルト ドメイン名。
- 詳細属性：スプリット トンネリング、IE ブラウザ プロキシ、SSL VPN クライアントと AnyConnect クライアント、および IPSec クライアント。

これらのパラメータを設定する前に、次の項目を設定する必要があります。

- アクセス時間
- ルールとフィルタ
- IPSec セキュリティ アソシエーション
- フィルタリングおよびスプリット トンネリング用のネットワーク リスト
- ユーザ認証サーバ（特に、内部認証サーバ）

フィールド

- [Group Policy]：現在設定されているグループ ポリシーの一覧と、VPN グループ ポリシーを管理するための [Add]、[Edit]、および [Delete] ボタンが表示されます。
  - [Name]：現在設定されているグループ ポリシーの名前を一覧表示します。
  - [Type]：現在設定されている各グループ ポリシーのタイプを一覧表示します。
  - [Tunneling Protocol]：現在設定されている各グループ ポリシーが使用するトンネリング プロトコルを一覧表示します。
  - [AAA Server Group]：現在設定されている各グループ ポリシーが属する AAA サーバ グループが存在すれば、一覧表示します。
  - [Add]：ドロップダウン メニューが表示され、内部または外部のグループ ポリシーを追加するかどうかを選択できます。単に [Add] をクリックする場合は、デフォルトにより内部グループ ポリシーを作成することになります。[Add] をクリックすると、[Add Internal Group Policy] ダイアログボックスまたは [Add External Group Policy] ダイアログボックスが開きます。これらのダイアログボックスを使用して、新しいグループ ポリシーを一覧に追加できます。このダイアログボックスには、3 つのメニュー セクションがあります。それぞれのメニュー項目を

クリックすると、その項目のパラメータが表示されます。項目間を移動するとき、ASDM は設定を保持します。すべてのメニュー セクションでパラメータの設定が終了したら、[Apply] または [Cancel] をクリックします。ドロップダウン メニューが表示され、内部または外部のグループ ポリシーを追加するかどうかを選択できます。単に [Add] をクリックする場合は、デフォルトにより内部グループ ポリシーを作成することになります。

- [Edit] : [Edit Group Policy] ダイアログボックスを表示します。このダイアログボックスを使用して、既存のグループ ポリシーを編集できます。
- [Delete] : AAA グループ ポリシーをリストから削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit External Group Policy

[Add or Edit External Group Policy] ダイアログボックスを使用して、外部グループ ポリシーを設定できます。

フィールド

- [Name] : 追加または変更するグループ ポリシーを特定します。[Edit External Group Policy] の場合、このフィールドは表示専用です。
- [Server Group] : このポリシーの適用先として利用できるサーバ グループを一覧表示します。
- [Password] : このサーバ グループ ポリシーのパスワードを指定します。
- [New] : 新しい RADIUS サーバ グループまたは新しい LDAP サーバ グループを作成するかどうかを選択できるダイアログボックスを開きます。どちらの場合も [Add AAA Server Group] ダイアログボックスが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add AAA Server Group

[Add AAA Server Group] ダイアログボックスでは、新しい AAA サーバ グループを設定できます。[Accounting Mode] 属性は、RADIUS および TACACS+ プロトコルにだけ適用されます。

フィールド

- [Server Group]：サーバ グループの名前を指定します。
- [Protocol]：（*表示専用*）RADIUS サーバ グループか、LDAP サーバ グループかを示します。
- [Accounting Mode]：同時アカウンティング モードかシングル アカウンティング モードかを示します。シングル モードでは、セキュリティ アプライアンスはアカウンティング データを 1 つのサーバにだけ送信します。同時モードでは、セキュリティ アプライアンスはアカウンティング データをグループ内のすべてのサーバに送信します。[Accounting Mode] 属性は、RADIUS および TACACS+ プロトコルにだけ適用されます。
- [Reactivation Mode]：障害が発生したサーバを再アクティブ化する方法を Depletion または Timed 再アクティブ化モードから指定します。Depletion モードでは、障害が発生したサーバは、グループ内のサーバのすべてが非アクティブになった場合にだけ再アクティブ化されます。Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。
- [Dead Time]：Depletion モードで、グループの最後のサーバがディセーブルになってから、すべてのサーバを次に再度イネーブルにするまでの経過時間を分単位（0 ～ 1440）で指定します。デフォルト値は 10 分です。このフィールドは、Timed モードでは使用できません。
- [Max Failed Attempts]：応答しないサーバが非アクティブであると宣言するまでの失敗接続試行回数を指定します（1 ～ 5 の整数）。デフォルト値は 3 回です。

リモート アクセスの内部グループ ポリシーの追加または編集、一般属性

[Add or Edit Group Policy] ウィンドウでは、追加または編集するグループ ポリシーのトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定できます。このウィンドウの各フィールドで、[Inherit] チェックボックスをオンにすると、対応する設定の値をデフォルト グループ ポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

フィールド

[Add Internal Group Policy] > [General] ウィンドウには、次の属性が表示されます。これらは、SSL VPN と IPSec セッション、またはクライアントレス SSL VPN セッションに適用されます。そのため、いくつかの属性は、1 つのタイプのセッションに表示され、他のタイプには表示されません。

- [Name]：このグループ ポリシーの名前を指定します。Edit 機能の場合、このフィールドは読み取り専用です。
- [Banner]：ログイン時にユーザに対して表示するバナー テキストを指定します。長さは最大 491 文字です。デフォルト値はありません。
- [Address Pools]：（Network (Client) Access 専用）このグループ ポリシーで使用する 1 つ以上のアドレス プールの名前を指定します。
- [Select]：（Network (Client) Access 専用）[Select Address Pools] ウィンドウが開きます。このウィンドウには、クライアント アドレス割り当てで選択可能なアドレス プールのプール名、開始アドレスと終了アドレス、およびサブネット マスクが表示され、そのリストからエントリを選択、追加、編集、削除、および割り当てできます。
- [More Options]：このグループ ポリシーで設定可能な追加のオプションを表示します。
- [Tunneling Protocols]：このグループが使用できるトンネリング プロトコルを指定します。ユーザは、選択されているプロトコルだけを使用できます。次の選択肢があります。

- [Clientless SSL VPN] : SSL/TLS による VPN の使用法を指定します。この VPN では、ソフトウェアやハードウェアのクライアントを必要とせずに、Web ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス トンネルを確立します。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
- [SSL VPN Client] : Cisco AnyConnect VPN クライアントまたはレガシー SSL VPN クライアントの使用を指定します。
- [IPsec] : IP Security Protocol（IP セキュリティ プロトコル）。IPSec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、およびクライアントと LAN 間の接続の両方で IPSec を使用できます。
- [L2TP over IPSec] : 多くの PC およびモバイル PC のオペレーティング システムで提供される VPN クライアントを使用しているリモート ユーザが、パブリック IP ネットワークを介してセキュリティ アプライアンスおよびプライベート企業ネットワークへのセキュアな接続を確立できるようにします。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。セキュリティ アプライアンスは、IPSec 転送モード用に設定する必要があります。

（注） プロトコルを選択しないと、エラー メッセージが表示されます。

- [Filter] :（Network (Client) Access 専用）使用するアクセス コントロール リストを指定するか、またはグループ ポリシーから値を継承するかどうかを指定します。フィルタは、セキュリティ アプライアンスを経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。フィルタおよびルールを設定する方法については、[Group Policy] ウィンドウを参照してください。
- [Web ACL] :（クライアントレス SSL VPN 専用）トラフィックをフィルタリングする場合は、ドロップダウン リストからアクセス コントロール リスト（ACL）を選択します。選択する前に ACL を表示、変更、追加、または削除する場合は、リストの横にある [Manage] をクリックします。
- [Manage] : アクセス コントロール リスト（ACL）と拡張アクセス コントロール リスト（ACE）を追加、編集、および削除できる [ACL Manager] ウィンドウを表示します。ACL Manager の詳細については、そのウィンドウのオンライン ヘルプを参照してください。
- [NAC Policy] : このグループ ポリシーに適用するネットワーク アドミッション コントロール ポリシーの名前を選択します。オプションの NAC ポリシーを各グループ ポリシーに割り当てることができます。デフォルト値は --None-- です。
- [Manage] : [Configure NAC Policy] ダイアログボックスが開きます。1 つ以上の NAC ポリシーを設定すると、[NAC Policy] 属性の横のドロップダウン リストに、設定した NAC ポリシー名がオプションとして表示されます。
- [Access Hours] : このユーザに適用される既存のアクセス時間ポリシーがある場合はその名前を選択するか、または新しいアクセス時間ポリシーを作成します。デフォルト値は [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルト値は [--Unrestricted--] です。
- [Manage] : [Browse Time Range] ダイアログボックスを開きます。このダイアログボックスでは、時間範囲を追加、編集、または削除できます。
- [Simultaneous Logins] : このユーザに許可する同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザ アクセスを禁止します。

（注）　最大数の制限はありませんが、複数の同時接続の許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

- [Restrict Access to VLAN]：（任意）「VLAN マッピング」とも呼ばれます。このパラメータにより、このグループ ポリシーが適用されるセッションの出力 VLAN インターフェイスを指定します。セキュリティ アプライアンスは、このグループのトラフィックすべてを、選択した VLAN に転送します。この属性を使用して VLAN をグループ ポリシーに割り当て、アクセス コントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。ドロップダウン リストには、デフォルト値（Unrestricted）の他に、このセキュリティ アプライアンスで設定されている VLAN だけが表示されます。

  （注）　この機能は、HTTP 接続の場合には有効ですが、FTP および CIFS 接続では使用できません。

- [Maximum Connect Time]：[Inherit] チェックボックスがオフになっている場合、このパラメータには、ユーザの最大接続時間を分単位で指定します。ここで指定した時間が経過すると、システムは接続を終了します。最短時間は 1 分で、最長時間は 35791394 分（4000 年超）です。接続時間を無制限にするには、[Unlimited] を選択します（デフォルト）。
- [Idle Timeout]：[Inherit] チェックボックスがオフになっている場合、このパラメータには、ユーザのアイドル タイムアウト時間を分単位で指定します。この期間、ユーザ接続に通信アクティビティがなかった場合、システムは接続を終了します。最短時間は 1 分で、最長時間は 10080 分です。デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

グループ ポリシーのポータルの設定

[Portal] 属性により、クライアントレス SSL VPN 接続を確立するこのグループ ポリシーのメンバのポータル ページに表示されるコンテンツが決まります。このペインでは、ブックマーク リストと URL エントリ、ファイル サーバ アクセス、ポート転送とスマート トンネル、ActiveX リレー、および HTTP の設定をイネーブルにできます。

フィールド

- [Bookmark List]：あらかじめ設定されたブックマーク リストを選択するか、または [Manage] をクリックして新しいリストを作成します。ブックマークはリンクとして表示され、ユーザはこのリンクを使用してポータル ページから移動できます。
- [URL Entry]：リモート ユーザが URL をポータル URL フィールドに直接入力できるようにする場合にイネーブルにします。

- [File Access Control]：共通インターネット ファイル システム（CIFS）ファイルの「非表示共有」の表示状態を制御します。非表示共有は、共有名の末尾のドル記号（$）で識別されます。たとえば、ドライブ C は C$ として共有されます。非表示共有では、共有フォルダは表示されず、ユーザはこれらの非表示リソースを参照またはアクセスすることを禁止されます。
  - [File Server Entry]：リモート ユーザがファイル サーバの名前を入力できるようにする場合にイネーブルにします。
  - [File Server Browsing]：リモート ユーザが使用可能なファイル サーバを参照できるようにする場合にイネーブルにします。
  - [Hidden Share Access]：共有フォルダを非表示にする場合にイネーブルにします。
- [Port Forwarding Control] : Java Applet によるクライアントレス SSL VPN 接続により、ユーザが TCP ベースのアプリケーションにアクセスできるようにします。
  - [Port Forwarding List]：このグループ ポリシーに関連付ける事前設定済み TCP アプリケーションのリストを選択します。新しいリストを作成したり、既存のリストを編集したりするには、[Manage] をクリックします。
  - [Auto Applet Download]：ユーザが始めてログインするときに実行される、Java Applet の自動インストールおよび起動をイネーブルにします。
  - [Applet Name]：[Applet] ウィンドウのタイトルバーの名前を、指定する名前に変更します。デフォルトの名前は [Application Access] です。
- [Smart Tunnel List]：スマート トンネル アクセスを提供する場合は、ドロップダウン メニューからリスト名を選択します。スマート トンネルは、Winsock 2 の TCP ベースのアプリケーションとプライベート サイト間の接続です。このスマート トンネルは、セキュリティ アプライアンスをパスウェイとして、また、セキュリティ アプライアンスをプロキシ サーバとして使用するクライアントレス（ブラウザベース）SSL VPN セッションを使用します。スマート トンネル リストをグループ ポリシーまたはユーザ名に割り当てると、そのグループ ポリシーまたはユーザ名にセッションが関連付けられているすべてのユーザの場合にスマート トンネル アクセスがイネーブルになりますが、リストで指定されているアプリケーションへのスマート トンネル アクセスは制限されます。

  スマート トンネル リストを表示、追加、変更、または削除するには、[Manage] ボタンをクリックします。
  - [Auto Start (Smart Tunnel List)]：ユーザのログイン時にスマート トンネル アクセスを自動的に開始する場合にオンにします。ユーザのログイン時にスマート トンネル アクセスをイネーブルにするが、ユーザはクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、スマート トンネル アクセスを手動で開始するようにユーザに要求する場合にオフにします。
- [ActiveX Relay]：クライアントレス ユーザが ActiveX をブラウザから起動できるようにします。アプリケーションは、セッションを使用して ActiveX コントロールのダウンロードとアップロードを行います。ActiveX のリレーは、クライアントレス SSL VPN セッションを終了するまで有効なままです。

その他のオプション：

- [HTTP Proxy]：クライアントへの HTTP アプレット プロキシの転送をイネーブルまたはディセーブルにします。このプロキシは、適切なコンテンツ変換に干渉するテクノロジー（Java、ActiveX、Flash など）に対して有用です。このプロキシによって、セキュリティ アプライアンスの使用を継続しながら、マングリングを回避できます。転送されたプロキシは、自動的にブラウザの古いプロキシ コンフィギュレーションを変更して、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTTP アプレット プロキシでは、HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。

- [Auto Start (HTTP Proxy)] : ユーザのログイン時に HTTP プロキシを自動的にイネーブルにする場合にオンにします。ユーザ ログイン時にスマート トンネル アクセスをイネーブルにして、ユーザに手動で開始するように要求する場合はオフにします。
- [HTTP Compression] : クライアントレス SSL VPN セッションでの HTTP データの圧縮をイネーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

グループ ポリシーのカスタマイゼーションの設定

グループ ポリシーのカスタマイゼーションを設定するには、事前設定済みのポータル カスタマイゼーション オブジェクトを選択するか、またはデフォルト グループ ポリシーで定義されているカスタマイゼーションを受け入れます。表示する URL を設定することもできます。

フィールド

[Portal Customization] : エンド ユーザ ポータルのカスタマイゼーション オブジェクトを設定します。

- [Inherit] : デフォルト グループ ポリシーからポータル カスタマイゼーションを継承するには、[Inherit] をクリックします。事前設定済みのカスタマイゼーション オブジェクトを指定するには、[Inherit] の選択を解除し、ドロップダウン リストからカスタマイゼーション オブジェクトを選択します。
- [Manage] : 新しいカスタマイゼーション オブジェクトをインポートします。

[Homepage URL]（任意）: グループ ポリシーに関連付けられたユーザのホームページの URL を指定するには、このフィールドに入力します。デフォルト グループ ポリシーからホームページを継承するには、[Inherit] をクリックします。

[Access Deny Message] : アクセスを拒否するユーザに対するメッセージを作成するには、このフィールドに入力します。デフォルト グループ ポリシーのメッセージを受け入れるには、[Inherit] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Site-to-Site 内部グループ ポリシーの追加または編集

[Add or Edit Group Policy] ウィンドウでは、追加または編集するグループ ポリシーのトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定できます。このウィンドウの各フィールドで、[Inherit] チェックボックスをオンにすると、対応する設定の値をデフォルト グループ ポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

フィールド

[Add Internal Group Policy] > [General] ウィンドウには、次の属性が表示されます。これらは、SSL VPN と IPSec セッション、またはクライアントレス SSL VPN セッションに適用されます。そのため、いくつかの属性は、1 つのタイプのセッションに表示され、他のタイプには表示されません。

- [Name]：このグループ ポリシーの名前を指定します。Edit 機能の場合、このフィールドは読み取り専用です。
- [Tunneling Protocols]：このグループが使用できるトンネリング プロトコルを指定します。ユーザは、選択されているプロトコルだけを使用できます。次の選択肢があります。
  - [Clientless SSL VPN]：SSL/TLS による VPN の使用法を指定します。この VPN では、ソフトウェアやハードウェアのクライアントを必要とせずに、Web ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス トンネルを確立します。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
  - [SSL VPN Client]：Cisco AnyConnect VPN クライアントまたはレガシー SSL VPN クライアントの使用を指定します。
  - [IPsec]：IP Security Protocol（IP セキュリティ プロトコル）。IPSec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、およびクライアントと LAN 間の接続の両方で IPSec を使用できます。
  - [L2TP/IPSec]：多くの PC およびモバイル PC のオペレーティング システムで提供される VPN クライアントを使用しているリモート ユーザが、パブリック IP ネットワークを介してセキュリティ アプライアンスおよびプライベート企業ネットワークへのセキュアな接続を確立できるようにします。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。セキュリティ アプライアンスは、IPSec 転送モード用に設定する必要があります。

（注） プロトコルを選択しないと、エラー メッセージが表示されます。

- [Filter]：（Network (Client) Access 専用）使用するアクセス コントロール リストを指定するか、またはグループ ポリシーから値を継承するかどうかを指定します。フィルタは、セキュリティ アプライアンスを経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。フィルタおよびルールを設定する方法については、[Group Policy] ウィンドウを参照してください。
- [Manage]：アクセス コントロール リスト（ACL）と拡張アクセス コントロール リスト（ACE）を追加、編集、および削除できる [ACL Manager] ウィンドウを表示します。ACL Manager の詳細については、そのウィンドウのオンライン ヘルプを参照してください。

Browse Time Range

[Browse Time Range] ダイアログボックスを使用して、時間範囲を追加、編集、または削除します。時間範囲とは、グループ ポリシーに適用できる開始および終了時刻を定義する、再利用可能なコンポーネントのことです。時間範囲を定義した後、その時間範囲を選択し、スケジューリングが必要な各種オプションに適用できます。たとえば、アクセス リストに時間範囲を設定すると、セキュリティ アプライアンスのアクセスを制限できます。時間範囲は、開始時刻、終了時刻、およびオプションの繰り返し（つまり定期的な）エントリで構成されます。時間範囲の詳細については、[Add or Edit Time Range] ダイアログボックスのオンライン ヘルプを参照してください。

フィールド

- [Add] : [Add Time Range] ダイアログボックスを開きます。このダイアログボックスでは、新しい時間範囲を作成できます。

（注） 時間範囲を作成してもデバイスへのアクセスは制限されません。

- [Edit] : [Edit Time Range] ダイアログボックスを開きます。このダイアログボックスでは、既存の時間範囲を修正できます。このボタンは、[Browse Time Range] テーブルから既存の時間範囲を選択した場合にだけアクティブになります。
- [Delete] : 選択した時間範囲を [Browse Time Range] テーブルから削除します。この処理は、確認されず、やり直しもできません。
- [Name] : 時間範囲の名前を指定します。
- [Start Time] : 時間範囲の開始時刻を指定します。
- [End Time] : 時間範囲の終了時刻を指定します。
- [Recurring Entries] : 指定した開始時刻と停止時刻の範囲内でアクティブな時間の追加制限を指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Time Rnage

[Add or Edit Time Range] ダイアログボックスでは、新しい時間範囲を設定できます。

フィールド

- [Time Range Name] : この時間範囲に割り当てる名前を指定します。
- [Start Time] : 時間範囲を開始する時刻を定義します。
  - [Start now] : 時間範囲がただちに開始されるように指定します。

  - [Start at]：時間範囲を開始する月、日、年、時間、および分を選択します。
- [End Time]：時間範囲を終了する時刻を定義します。
  - [Never end]：時間範囲でエンド ポイントを定義しないように指定します。
  - [End at (inclusive)]：時間範囲を終了する月、日、年、時間、および分を選択します。
- [Recurring Time Ranges]：時間範囲がアクティブである場合に、開始時刻から終了時刻までの範囲内でアクティブな時間を制限します。たとえば、開始時刻が Start now で終了時刻が Never end であり、月曜日から金曜日までの毎日 8:00 AM ～ 5:00 PM を有効な時間範囲とする場合には、繰り返し時間範囲を、平日の 08:00 ～ 17:00 までアクティブになるように設定します。
- [Add] : [Add Recurring Time Range] ダイアログボックスを開きます。このダイアログボックスで、繰り返し時間範囲を設定できます。
- [Edit] : [Edit Recurring Time Range] ダイアログボックスを開きます。このダイアログボックスで、選択した繰り返し時間範囲を修正できます。
- [Delete]：選択した繰り返し時間範囲を削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Recurring Time Range

[Add or Edit Recurring Time Range] ダイアログボックスでは、繰り返し時間範囲を設定または変更できます。

フィールド

- [Specify days of the week and times on which this recurring range will be active] : [Days of week] 領域のオプションを使用可能にします。たとえば、時間範囲を毎週月曜日から木曜日の 08:00 ～ 16:59 の間だけアクティブにする場合に、このオプションを使用します。
  - [Days of the week]：この繰り返し時間範囲に含める曜日を選択します。可能なオプションは、[Every day]、[Weekdays]、[Weekends]、および [On these days of week] です。これらのうち最後については、範囲に入れる曜日ごとにチェックボックスをオンにできます。
  - [Daily Start Time]：選択した各曜日に繰り返し時間範囲をアクティブにする場合に、時間と分を 24 時間形式で指定します。
  - [Daily End Time (inclusive)] : 選択した各曜日に繰り返し時間範囲をアクティブにする場合に、時間と分を 24 時間形式で指定します。
- [Specify a weekly interval when this recurring range will be active] : [Weekly Interval] 領域のオプションを使用可能にします。範囲は終了時刻まで拡張されます。この領域の時間は、すべて 24 時間形式です。たとえば、時間範囲を月曜日から金曜日の 8:00 AM ～ 4:30 PM の間で連続的にアクティブにする場合に、このオプションを使用します。
  - [From]：毎週の時間範囲を開始する日、時間、および分を選択します。

– [Through]：毎週の時間範囲を終了する日、時間、および分を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ACL Manager

[ACL Manager] ダイアログボックスでは、アクセス コントロール リスト（ACL）を定義することにより、特定のホストまたはネットワークから別のホストまたはネットワークへのアクセス（使用できるプロトコルやポートなど）を制御できます。

ユーザ セッションに適用する ACL（アクセス コントロール リスト）を設定できます。ACL は、特定のネットワーク、サブネット、ホスト、および Web サーバへのユーザ アクセスを許可または拒否するフィルタです。

- フィルタを定義しない場合は、すべての接続が許可されます。
- セキュリティ アプライアンスは、インターフェイスのインバウンド ACL だけをサポートします。
- 各 ACL の最後には、許可されないすべてのトラフィックを拒否する、表記されない暗黙のルールが含まれます。トラフィックがアクセス コントロール エントリ（ACE）によって明示的に許可されていない場合には、セキュリティ アプライアンスがそのトラフィックを拒否します。このトピックでは、ACE をルールと呼びます。

Standard ACL

このペインには、標準 ACL に関する要約情報が表示され、このペインを使用して、ACL と ACE を追加または削除できます。

フィールド

- [Add] : 新しい ACL を追加できます。既存の ACL を選択すると、その ACL について新しい ACE を追加できます。
- [Edit] : [Edit ACE] ダイアログボックスを開きます。このダイアログボックスでは、既存のアクセス コントロール リスト ルールを変更できます。
- [Delete] : ACL または ACE を削除します。確認されず、やり直しもできません。
- [Move Up/Move Down] : [ACL Manager] テーブルでのルールの位置を変更します。
- [Cut] : [ACL Manager] テーブルから選択内容を削除し、クリップボードに保存します。
- [Copy] : 選択内容のコピーをクリップボードに保存します。
- [Paste] : [Paste ACE] ダイアログボックスを開きます。このダイアログボックスでは、既存のルールから新しい ACL ルールを作成できます。

- [No]：ルールの評価順序を示します。暗黙のルールには番号が付けられず、ハイフンで表されます。
- [Address]：ACE が適用されるアプリケーションまたはサービスの IP アドレスまたは URL を表示します。
- [Action]：このフィルタがトラフィック フローを許可するか拒否するかを指定します。
- [Description]：ルールを追加したときに入力した説明が表示されます。暗黙のルールには、「Implicit outbound rule」という説明が含まれます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Extended ACL

このペインには、拡張 ACL に関する要約情報が表示され、ACL と ACE を追加または編集できます。

フィールド

- [Add]：新しい ACL を追加できます。既存の ACL を選択すると、その ACL について新しい ACE を追加できます。
- [Edit]：[Edit ACE] ダイアログボックスを開きます。このダイアログボックスでは、既存のアクセス コントロール リスト ルールを変更できます。
- [Delete]：ACL または ACE を削除します。確認されず、やり直しもできません。
- [Move Up/Move Down]：[ACL Manager] テーブルでのルールの位置を変更します。
- [Cut]：[ACL Manager] テーブルから選択内容を削除し、クリップボードに保存します。
- [Copy]：選択内容のコピーをクリップボードに保存します。
- [Paste]：[Paste ACE] ダイアログボックスを開きます。このダイアログボックスでは、既存のルールから新しい ACL ルールを作成できます。
- [No]：ルールの評価順序を示します。暗黙のルールには番号が付けられず、ハイフンで表されます。
- [Enabled]：ルールをイネーブルまたはディセーブルにします。暗黙のルールはディセーブルにできません。
- [Source]：[Destination] カラムにリストされている IP アドレスへのトラフィックの送信を許可または拒否する IP アドレス（ホストまたはネットワーク）を指定します。詳細モード（[Show Detail] オプション ボタンを参照）では、アドレス カラムに、単語 any が付いたインターフェイス名が含まれることがあります（inside: any など）。これは、内部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。
- [Destination]：[Source] カラムにリストされている IP アドレスへのトラフィックの送信を許可または拒否する IP アドレス（ホストまたはネットワーク）を指定します。アドレス カラムには、単語 any が付いたインターフェイス名が含まれることがあります（outside: any など）。これは、外部

インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。アドレス カラムには、IP アドレスが含まれることもあります（209.165.201.1-209.165.201.30 など）。これらのアドレスは、変換済みアドレスです。内部ホストが外部ホストへの接続を作成すると、ファイアウォールは内部ホストのアドレスをプールのアドレスにマッピングします。ホストがアウトバウンド接続を作成した後、ファイアウォールはこのアドレス マッピングを維持します。アドレス マッピング構造は xlate と呼ばれ、一定の時間、メモリに保持されます。ACL で許可されていれば、この時間内に、外部ホストはプールの変換済みアドレスを使用して、内部ホストへの接続を開始できます。通常、内部ホストは常に同じ IP アドレスを使用するため、外部から内部への接続にはスタティック変換が必要です。

- [Service]：ルールで指定されるサービスとプロトコルの名前。
- [Action]：このフィルタがトラフィック フローを許可するか拒否するかを指定します。
- [Logging]：ログ レベルと、ログ メッセージ間の間隔（秒単位）が表示されます（ACL のロギングをイネーブルにした場合）。ロギング オプション（ロギングのイネーブル化とディセーブル化を含む）を設定するには、このカラムを右クリックして、[Edit Log Option] を選択します。[Log Options] ウィンドウが表示されます。
- [Time]：このルールで適用される時間範囲の名前を指定します。
- [Description]：ルールを追加したときに入力した説明が表示されます。暗黙のルールには、「Implicit outbound rule」という説明が含まれます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit/Paste ACE

[Add/Edit/Paste ACE] ダイアログボックスでは、新しい拡張アクセス リスト ルールを作成するか、または既存のルールを修正することができます。[Paste] オプションは、ルールを切り取りまたはコピーするときにだけ利用できるようになります。

フィールド

- [Action]：新しいルールのアクション タイプを指定します。[Permit] と [Deny] のいずれかを選択します。
  - [Permit]：一致するすべてのトラフィックを許可します。
  - [Deny]：一致するすべてのトラフィックを拒否します。
- [Source/Destination]：送信元または宛先タイプを指定し、そのタイプに応じて、送信元または宛先ホストまたはネットワーク IP アドレスが記載されているその他の該当パラメータを指定します。使用できる値は、any、IP address、Network Object Group、および Interface IP です。その後のフィールドは、[Type] フィールドの値によって異なります。
  - [any]：その送信元または宛先ホストまたはネットワークがどのタイプでも可能であることを指定します。[Type] フィールドのこの値については、[Source] または [Destination] 領域にその他のフィールドがありません。

  - [IP Address]：送信元または宛先ホストまたはネットワークの IP アドレスを指定します。このフィールドを選択すると、[IP Address]、省略符号ボタン、および [Netmask] フィールドが利用できるようになります。IP アドレスまたはホスト名を [IP Address] フィールドのドロップダウン リストから選択するか、省略符号（[...]）ボタンをクリックして、IP アドレスまたは名前を参照します。ネットワーク マスクをドロップダウン リストから選択します。
  - [Network Object Group]：ネットワーク オブジェクト グループの名前を指定します。ドロップダウン リストから名前を選択するか、省略符号（[...]）ボタンをクリックして、ネットワーク オブジェクト グループ名を参照します。
  - [Interface IP]：ホストまたはネットワークが存在するインターフェイスを指定します。インターフェイスをドロップダウン リストから選択します。デフォルト値は、inside と outside です。参照機能はありません。

- [Protocol and Service]：この ACE フィルタが適用されるプロトコルとサービスを指定します。サービス グループを使用して、ACL と一致させる複数の連続していないポート番号を識別できます。たとえば、ポート番号 5、8、9 で HTTP および FTP をフィルタリングする場合は、これらのすべてのポートを含むサービス グループを定義します。サービス グループを使用しない場合は、ポートごとに個別のルールを作成する必要があります。

  TCP、UDP、TCP-UDP、ICMP、およびその他の IP プロトコル用にサービス グループを作成できます。TCP-UDP プロトコルを使用するサービス グループには、TCP または UDP プロトコルを使用するサービス、ポート、および範囲が含まれます。

  - [Protocol]：このルールが適用されるプロトコルを選択します。使用できる値は、ip、tcp、udp、icmp などです。[Protocol and Service] 領域のその他のフィールドは、選択するプロトコルによって異なります。次の項目で、各選択内容の結果について説明します。
  - [Protocol: TCP and UDP]：そのルールの TCP/UDP プロトコルを選択します。[Source Port] 領域と [Destination Port] 領域で、ACL がパケットを照合するために使用するポートを指定できます。
  - [Source Port/Destination Port]：（*TCP および UDP プロトコルの場合だけ使用可能*）演算子、ポート番号、ポート範囲、またはサービスのリストにあるウェルノウン サービス名（HTTP や FTP など）を指定します。演算子リストで、ACL がポートを照合する方法を指定します。次のいずれかの演算子を選択します。=（ポート番号と等しい）、not =（ポート番号と等しくない）、>（ポート番号より大きい）、<（ポート番号より小さい）、range（範囲内のポート番号のいずれかと等しい）。
  - [Group]：（*TCP と UDP プロトコルの場合だけ使用可能*）送信元ポート サービス グループを選択します。[Browse (...)] ボタンをクリックすると、[Browse Source Port] または [Browse Destination Port] ダイアログボックスが開きます。
  - [Protocol: ICMP]：定義済みリストから ICMP タイプまたは ICMP グループを選択するか、[Browse (...)] をクリックして、ICMP グループを選択できます。[Browse] ボタンをクリックすると、[Browse ICMP] ダイアログボックスが表示されます。
  - [Protocol: IP]：IP プロトコル ボックスで、そのルールの IP プロトコルを指定します。このフィールドを選択した場合、他のフィールドは表示されません。
  - [Protocol: Other]：ドロップダウン リストからプロトコルまたはプロトコル グループを選択するか、またはプロトコル グループを参照できます。[Browse (...)] ボタンをクリックすると、[Browse Other] ダイアログボックスが表示されます。

- [Rule Flow Diagram]：（*表示専用*）設定済みのルール フローをグラフィカルに表示します。この表示を明示的に閉じない限り、[ACL Manager] ダイアログボックスに同じ図が表示されます。
- [Options]：ロギング パラメータ、時間範囲、説明など、このルールのオプション機能を設定します。

- [Logging]：ロギングをイネーブルまたはディセーブルにします。または、デフォルト ロギング設定を使用するように指定します。ロギングをイネーブルにすると、[Syslog Level] および [Log Interval] フィールドが使用可能になります。
- [Syslog Level]：ロギング アクティビティのレベルを選択します。デフォルトは Informational です。
- [Log Interval]：許可および拒否のロギング間隔を指定します。デフォルトは 300 秒です。範囲は 1 ～ 6000 秒です。
- [Time Range]：このルールを使用する時間範囲の名前を選択します。デフォルトは (any) です。[Browse (...)] ボタンをクリックして [Browse Time Range] ダイアログボックスを開き、時間範囲を選択または追加します。
- [Description]：（*任意*）このルールの簡単な説明を示します。説明行の長さは最大 100 文字ですが、説明を改行して複数行にすることができます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Browse Source/Destination Address

[Browse Source or Destination Address] ダイアログボックスでは、このルールの送信元または宛先として使用するオブジェクトを選択できます。

フィールド

- [Type]：このルールの送信元または宛先として使用するオブジェクトのタイプを決めます。選択肢は、[IP Address Objects]、[IP Names]、[Network Object Groups]、および [All] です。このフィールドに続くテーブルの内容は、選択肢によって変わります。
- [Source/Destination Object Table]：送信元または宛先オブジェクトの選択元オブジェクトを表示します。[type] フィールドで All を選択すると、各カテゴリのオブジェクトが、それぞれの見出しの下に表示されます。テーブルの見出しは次のとおりです。
  - [Name]：各オブジェクトのネットワーク名（IP アドレスの場合もあります）を表示します。
  - [IP address]：各オブジェクトの IP アドレスを表示します。
  - [Netmask]：各オブジェクトで使用するネットワーク マスクを表示します。
  - [Description]：[Add/Edit/Paste Extended Access List Rule] ダイアログボックスに入力された説明を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Browse Source/Destination Port

[Browse Source or Destination Port] ダイアログボックスでは、このルールでのこのプロトコルの送信元または宛先ポートを選択できます。

フィールド

- [Add] : [Add TCP Service Group] ダイアログボックスを開きます。このダイアログボックスで、新しい TCP サービス グループを設定できます。
- [Find] : [Filter] フィールドを開きます。
- [Filter/Clear] : [Name] リストの項目を検索するために使用できるフィルタ基準を指定し、その基準に一致する項目だけが表示されるようにします。[Filter] フィールドに入力すると、[Filter] ボタンがアクティブになります。[Filter] ボタンをクリックすると、検索が実行されます。検索を実行した後は、[Filter] ボタンがグレー表示になり、[Clear] ボタンがアクティブになります。[Clear] ボタンをクリックすると、[filter] フィールドがクリアされ、[Clear] ボタンがグレー表示になります。
- [Type] : このルールの送信元または宛先として使用するオブジェクトのタイプを決めます。選択肢は、[IP Address Objects]、[IP Names]、[Network Object Groups]、および [All] です。このフィールドに続くテーブルの内容は、選択肢によって変わります。
- [Name] : 選択したタイプの定義済みプロトコルとサービス グループを一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add TCP Service Group

[Add TCP Service Group] ダイアログボックスでは、新しい TCP サービス グループまたはポートを設定し、このルールでのこのプロトコルに使用する参照可能な送信元または宛先ポート リストに追加できます。[Members not in Group] リストまたは [Members in Group] リストのメンバを選択すると、[Add] と [Remove] ボタンがアクティブになります。

フィールド

- [Group Name] : 新しい TCP サービス グループの名前を指定します。
- [Description] :（任意）このグループの簡単な説明を示します。

- [Members not in Group] : [Members in Group] リストに追加するサービスまたはサービス グループ、あるいはポート番号を選択するためのオプションを表示します。
- [Service/Service Group] : [Members in Group] リストに追加する TCP サービスまたはサービス グループの名前を選択するためのオプションを選択します。
- [Port #] : [Members in Group] リストに追加するポート番号の範囲を指定するためのオプションを選択します。
- [Add] : 選択した項目を [Members not in Group] リストから [Members in Group] リストに移動します。
- [Remove] : 選択した項目を [Members in Group] リストから [Members not in Group] リストに移動します。
- [Members in Group] : すでにこのサービス グループで設定されているメンバを一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Browse ICMP

[Browse ICMP] ダイアログボックスでは、このルールの ICMP グループを選択できます。

フィールド

- [Add] : [Add ICMP Group] ダイアログボックスを開きます。このダイアログボックスで、新しい TCP サービス グループを設定できます。
- [Find] : [Filter] フィールドを開きます。
- [Filter/Clear] : [Name] リストの項目を検索するために使用できるフィルタ基準を指定し、その基準に一致する項目だけが表示されるようにします。[Filter] フィールドに入力すると、[Filter] ボタンがアクティブになります。[Filter] ボタンをクリックすると、検索が実行されます。検索を実行した後は、[Filter] ボタンがグレー表示になり、[Clear] ボタンがアクティブになります。[Clear] ボタンをクリックすると、[filter] フィールドがクリアされ、[Clear] ボタンがグレー表示になります。
- [Type] : このルールの ICMP グループとして使用するオブジェクトのタイプを決めます。選択肢は、[IP Address Objects]、[IP Names]、[Network Object Groups]、および [All] です。このフィールドに続くテーブルの内容は、選択肢によって変わります。
- [Name] : 選択したタイプを対象とする定義済みの ICMP グループを一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add ICMP Group

[Add ICMP Group] ダイアログボックスでは、新しい ICMP グループの名前または番号を設定して、このルールでのプロトコルに使用する参照可能な ICMP リストに追加できます。[Members not in Group] リストまたは [Members in Group] リストのメンバを選択すると、[Add] と [Remove] ボタンがアクティブになります。

フィールド

- [Group Name]：新しい TCP サービス グループの名前を指定します。
- [Description]：（任意）このグループの簡単な説明を示します。
- [Members not in Group]：[Members in Group] リストに追加する ICMP タイプ /ICMP グループまたは ICMP 番号を選択するためのオプションを表示します。
- [ICMP Type/ICMP Group]：[Members in Group] リストに追加する ICMP グループの名前を選択するためのオプションを選択します。
- [ICMP #]：[Members in Group] リストに追加する ICMP メンバを番号で指定するためのオプションを選択します。
- [Add]：選択した項目を [Members not in Group] リストから [Members in Group] リストに移動します。
- [Remove]：選択した項目を [Members in Group] リストから [Members not in Group] リストに移動します。
- [Members in Group]：すでにこのサービス グループで設定されているメンバを一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Browse Other

[Browse Other] ダイアログボックスでは、このルールのプロトコル グループを選択できます。

フィールド

- [Add]：[Add Protocol Group] ダイアログボックスを開きます。このダイアログボックスで、新しいサービス グループを設定できます。

- [Find] : [Filter] フィールドを開きます。
- [Filter/Clear] : [Name] リストの項目を検索するために使用できるフィルタ基準を指定し、その基準に一致する項目だけが表示されるようにします。[Filter] フィールドに入力すると、[Filter] ボタンがアクティブになります。[Filter] ボタンをクリックすると、検索が実行されます。検索を実行した後は、[Filter] ボタンがグレー表示になり、[Clear] ボタンがアクティブになります。[Clear] ボタンをクリックすると、[filter] フィールドがクリアされ、[Clear] ボタンがグレー表示になります。
- [Type] : このルールのプロトコル グループとして使用するオブジェクトのタイプを決めます。選択肢は、[IP Address Objects]、[IP Names]、[Network Object Groups]、および [All] です。このフィールドに続くテーブルの内容は、選択肢によって変わります。
- [Name] : 選択したタイプを対象とする定義済みのプロトコル グループを一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add Protocol Group

[Add Protocol Group] ダイアログボックスでは、新しいプロトコル グループの名前または番号を設定して、このルールでのプロトコルに使用する参照可能なプロトコル リストに追加できます。[Members not in Group] リストまたは [Members in Group] リストのメンバを選択すると、[Add] と [Remove] ボタンがアクティブになります。

フィールド

- [Group Name] : 新しい TCP サービス グループの名前を指定します。
- [Description] :（任意）このグループの簡単な説明を示します。
- [Members not in Group] : [Members in Group] リストに追加するプロトコル / プロトコル グループまたはプロトコル番号を選択するためのオプションを表示します。
- [Protocol/Protocol Group] : [Members in Group] リストに追加するプロトコルまたはプロトコル グループの名前を選択するためのオプションを選択します。
- [Protocol #] : [Members in Group] リストに追加するプロトコルを番号で指定するためのオプションを選択します。
- [Add] : 選択した項目を [Members not in Group] リストから [Members in Group] リストに移動します。
- [Remove] : 選択した項目を [Members in Group] リストから [Members not in Group] リストに移動します。
- [Members in Group] : すでにこのサービス グループで設定されているメンバを一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Internal Group Policy] > [Servers]

[Add or Edit Group Policy] ウィンドウの [Servers] 項目により、DNS サーバと WINS サーバ、および DHCP スコープとデフォルト ドメインを指定できます。

[Add/Edit Internal Group Policy] > [IPSec Client]

[Add or Edit Group Policy] > [IPSec] ダイアログボックスでは、追加または編集するグループ ポリシーのトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定できます。

フィールド

- [Re-Authentication on IKE Re-key] : [Inherit] チェックボックスがオフである場合に、IKE キーの再生成が行われたときの再認証をイネーブルまたはディセーブルにします。
- [IP Compression] : [Inherit] チェックボックスがオフである場合に、IP 圧縮をイネーブルまたはディセーブルにします。
- [Perfect Forward Secrecy] : [Inherit] チェックボックスがオフである場合に、完全転送秘密（PFS）をイネーブルまたはディセーブルにします。PFS は、特定の IPSec SA のキーが他のシークレット（他のキーなど）から導出されたものでないことを保証します。つまり、PFS では、攻撃者があるキーを突破しても、そこから他のキーを導出することはできないことが保証されます。PFS がイネーブルになっていない場合は、IKE SA の秘密キーが突破されると、その攻撃者は、IPSec のすべての保護データをコピーし、IKE SA のシークレットの知識を使用して、その IKE SA によって設定された IPSec SA のセキュリティを侵すことができると推測されます。PFS を使用すると、攻撃者が IKE を突破しても、直接 IPSec にはアクセスできません。その場合、攻撃者は各 IPSec SA を個別に突破する必要があります。
- [Store Password on Client System] : クライアント システムでのパスワードの保管をイネーブルまたはディセーブルにします。

（注） パスワードをクライアント システムで保管すると、潜在的なセキュリティ リスクが発生します。

- [IPSec over UDP] : IPSec over UDP の使用をイネーブルまたはディセーブルにします。
- [IPSec over UDP Port] : IPSec over UDP で使用する UDP ポートを指定します。
- [Tunnel Group Lock] : [Inherit] チェックボックスまたは値 None が選択されていない場合に、リストから選択したトンネル グループのロックをイネーブルにします。
- [IPSec Backup Servers] : [Server Configuration] フィールドと [Server IP Addresses] フィールドをアクティブにします。これによって、これらの値が継承されない場合に使用する UDP バックアップ サーバを指定できます。

– [Server Configuration] : IPSec バックアップ サーバとして使用するサーバ設定オプションを一覧表示します。使用できるオプションは、[Keep Client Configuration]（デフォルト）、[Use Backup Servers Below]、および [Clear Client Configuration] です。

– [Server Addresses（space delimited）] : IPSec バックアップ サーバの IP アドレスを指定します。このフィールドは、[Server Configuration] で選択した値が Use Backup Servers Below である場合にだけ使用できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Client Access Rules

このダイアログボックスのテーブルには、クライアント アクセス ルールを 25 件まで表示できます。[Inherit] チェックボックスをオフにすると、[Add]、[Edit]、および [Delete] ボタンがアクティブになり、次のカラム見出しがテーブルに表示されます。

– [Priority] : このルールの優先順位が表示されます。

– [Action] : このルールがアクセスを許可するか拒否するかを指定します。

– [Client Type] : このルールを適用する VPN クライアントのタイプ（ソフトウェアまたはハードウェア）を指定します。ソフトウェア クライアントの場合は、すべての Windows クライアントかサブセットかを指定します。

– [VPN Client Version] : このルールを適用する VPN クライアントのバージョンを指定します（複数可）。このボックスには、このクライアントに適用されるソフトウェアまたはファームウェア イメージのカンマ区切りリストが含まれます。

モード

次の表は、この機能を使用できるモードを示したものです。

Add/Edit Client Access Rule

[Add or Edit Client Access Rule] ダイアログボックスでは、IPSec グループ ポリシーの新しいクライアント アクセス ルールを追加するか、または既存のルールを修正できます。

フィールド

- [Priority] : このルールの優先順位が表示されます。
- [Action] : このルールがアクセスを許可するか拒否するかを指定します。
- [VPN Client Type] : このルールを適用する VPN クライアントのタイプ（ソフトウェアまたはハードウェア）を指定します。ソフトウェア クライアントの場合は、すべての Windows クライアントかサブセットかを指定します。VPN クライアント タイプの共通値としては、VPN 3002、PIX、

Linux、*（すべてのクライアント タイプと一致）、Win9x（Windows 95、Windows 98、および Windows ME）、および WinNT（Windows NT、Windows 2000、および Windows XP）があります。* を選択した場合は、Windows NT など、個々の Windows のタイプを設定しません。

- [VPN Client Version] : このルールを適用する VPN クライアントのバージョンを指定します（複数可）。このボックスには、このクライアントに適用されるソフトウェアまたはファームウェア イメージのカンマ区切りリストが含まれます。次の警告が適用されます。
  - このクライアントのソフトウェア バージョンを指定する必要があります。* を指定して、任意のバージョンと一致させることができます。
  - 自分のエントリが、VPN クライアントの場合には URL と、VPN 3002 の場合には TFTP サーバと正確に一致する必要があります。
  - ハードウェア クライアント イメージを配布するための TFTP サーバは堅牢である必要があります。
  - クライアントがリストにあるソフトウェア バージョンをすでに実行している場合、ソフトウェアをアップデートする必要はありません。クライアントがリストにあるソフトウェア バージョンを実行していなくても、更新は正しく実行されます。
  - VPN クライアント ユーザは、一覧表示されている URL から適切なソフトウェア バージョンをダウンロードする必要があります。
  - VPN 3002 ハードウェア クライアント ソフトウェアは、自動的に TFTP 経由でアップデートされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Internal Group Policy] > [Client Configuration] タブ

[Add or Edit Group Policy] ウィンドウの [Client Configuration] タブには、全般的なクライアント パラメータ、Cisco クライアント パラメータ、および Microsoft クライアント パラメータを設定するための 3 つのタブがあります。

個々のタブの詳細については、次のリンクを参照してください。

- [Add/Edit Internal Group Policy] > [Client Configuration] タブ > [General Client Parameters] タブ
- [Add/Edit Internal Group Policy] > [Client Configuration] タブ > [Cisco Client Parameters] タブ
- [Add or Edit Internal Group Policy] > [Advanced] > [IE Browser Proxy]

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Internal Group Policy] > [Client Configuration] タブ > [General Client Parameters] タブ

このタブでは、バナー テキスト、デフォルト ドメイン、スプリット トンネル パラメータ、アドレス プールなど、Cisco クライアントと Microsoft クライアントに共通のクライアント属性を設定します。

（注）　AnyConnect VPN クライアントおよび SSL VPN クライアントは、スプリット DNS をサポートしません。

フィールド

- [Inherit]：（複数のインスタンス）対応する設定の値をデフォルト グループ ポリシーから取得できます。[Inherit] チェックボックスをオフにすると、パラメータのその他のオプションが使用できるようになります。このタブの属性すべてのデフォルト オプションです。
- [Banner]：デフォルト グループ ポリシーからバナーを継承するか、新しいバナー テキストを入力するかを指定します。詳細については、View/Config バナーを参照してください。
- [Edit Banner]：[View/Config Banner] ダイアログボックスが表示され、500 文字までのバナー テキストを入力できます。
- [Default Domain]：デフォルト グループ ポリシーからデフォルト ドメインを継承するか、このフィールドで指定する新しいデフォルト ドメインを使用するかを指定します。
- [Split Tunnel DNS Names (space delimited)]：デフォルト グループ ポリシーからスプリット トンネル DNS 名を継承するか、このフィールドで新しい名前または名前のリストを指定するかを指定します。
- [Split Tunnel Policy]：デフォルト グループ ポリシーからスプリット トンネル ポリシーを継承するか、メニューからポリシーを選択するかを指定します。メニュー オプションは、「すべてのネットワークをトンネリングする」、「下のネットワーク リストに含まれるネットワークをトンネリングする」、または「下のネットワーク リストに含まれるネットワークを除外する」です。
- [Split Tunnel Network List]：デフォルト グループ ポリシーからスプリット トンネル ネットワーク リストを継承するか、ドロップダウン リストから選択するかを指定します。
- [Manage]：[ACL Manager] ダイアログボックスを開き、標準および拡張アクセス コントロール リストを管理できます。
- [Address Pools]：このグループ ポリシーを通じて使用できるアドレス プールを設定します。
  - [Available Pools]：リモート クライアントにアドレスを割り当てるためのアドレス プールのリストを指定します。[Inherit] チェックボックスがオフで、[Assigned Pools] リストにアドレス プールがない場合、アドレス プールは設定されず、グループ ポリシーの他のソースから継承されません。
  - [Add]：アドレス プールの名前を [Available Pools] リストから [Assigned Pools] リストに移動します。

– [Remove] : アドレス プールの名前を [Assigned Pools] リストから [Available Pools] リストに移動します。

– [Assigned Pools (up to 6 entries)] : 割り当て済みプール リストに追加したアドレス プールをリストします。このテーブルのアドレス プール設定は、グループのローカル プール設定を上書きします。ローカル アドレスの割り当てに使用する最大 6 個のローカル アドレス プールのリストを指定できます。プールの指定順序は重要です。セキュリティ アプライアンスでは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

View/Config バナー

[View/Config Banner] ダイアログボックスでは、指定したクライアントのバナーとして表示される最大 500 文字のテキストをこのテキスト ボックスに入力できます。

（注）　Enter キーを押したときに作成される復帰または改行は 2 文字としてカウントされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Internal Group Policy] > [Client Configuration] タブ > [Cisco Client Parameters] タブ

このタブでは、パスワード保管、IPSec over UDP のイネーブルまたはディセーブル化、UDP ポート番号の設定、IPSec バックアップ サーバの設定など、Cisco クライアントに固有のクライアント属性を設定します。

フィールド

- [Store Password on Client System] : クライアント システムでのパスワードの保管をイネーブルまたはディセーブルにします。

（注）　パスワードをクライアント システムで保管すると、潜在的なセキュリティ リスクが発生します。

- [IPSec over UDP]：IPSec over UDP の使用をイネーブルまたはディセーブルにします。
- [IPSec over UDP Port]：IPSec over UDP で使用する UDP ポートを指定します。
- [IPSec Backup Servers]：[Server Configuration] フィールドと [Server IP Addresses] フィールドをアクティブにします。これによって、これらの値が継承されない場合に使用する UDP バックアップ サーバを指定できます。
- [Server Configuration]：IPSec バックアップ サーバとして使用するサーバ設定オプションを一覧表示します。使用できるオプションは、[Keep Client Configuration]（デフォルト）、[Use Backup Servers Below]、および [Clear Client Configuration] です。
- [Server Addresses（space delimited）]：IPSec バックアップ サーバの IP アドレスを指定します。このフィールドは、[Server Configuration] で選択した値が Use Backup Servers Below である場合にだけ使用できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add or Edit Internal Group Policy] > [Advanced] > [IE Browser Proxy]

このダイアログボックスでは、Microsoft Internet Explorer の属性を設定します。

フィールド

- [Proxy Server Policy]：クライアント PC の Microsoft Internet Explorer ブラウザのプロキシ アクション（「メソッド」）を設定します。
  - [Do not modify client proxy settings]：このクライアント PC の Internet Explorer の HTTP ブラウザ プロキシ サーバ設定を変更しません。
  - [Do not use proxy]：クライアント PC の Internet Explorer の HTTP プロキシ設定をディセーブルにします。
  - [Select proxy server settings from the following]：選択内容に応じて、[Auto detect proxy]、[Use proxy server settings given below]、および [Use proxy auto configuration (PAC) given below] のチェックボックスをオンにします。
  - [Auto-detect proxy]：クライアント PC で、Internet Explorer の自動プロキシ サーバ検出の使用をイネーブルにします。
  - [Use proxy server settings specified below]：[Proxy Server Name or IP Address] フィールドで設定された値を使用するように、Internet Explorer の HTTP プロキシ サーバ設定値を設定します。

  - [Use proxy auto configuration (PAC) given below] : [Proxy Auto Configuration (PAC)] フィールドで指定したファイルを、自動コンフィギュレーション属性のソースとして使用するように指定します。

- [Proxy Server Settings] : Microsoft Internet Explorer を使用して、Microsoft クライアントのプロキシ サーバ パラメータを設定します。
  - [Server Address and Port] : このクライアント PC で適用される、Microsoft Internet Explorer サーバの IP アドレスまたは名前、およびポートを指定します。
  - [Bypass Proxy Server for Local Addresses]:クライアント PC での Microsoft Internet Explorer ブラウザ プロキシ ローカル バイパス設定値を設定します。[Yes] を選択するとローカル バイパスがイネーブルになり、[No] を選択するとローカル バイパスがディセーブルになります。
  - [Exception List] : プロキシ サーバ アクセスから除外するサーバの名前と IP アドレスを一覧表示します。プロキシ サーバ経由のアクセスを行わないアドレスのリストを入力します。このリストは、Internet Explorer の [Proxy Stteings] ダイアログボックスにある [Exceptions] ボックスに相当します。
- [PAC URL] : 自動コンフィギュレーション ファイルの URL を指定します。このファイルには、ブラウザがプロキシ情報を探せる場所が記述されています。プロキシ自動コンフィギュレーション（PAC）機能を使用する場合、リモート ユーザは、Cisco AnyConnect VPN クライアントを使用する必要があります。

  多くのネットワーク環境が、Web ブラウザを特定のネットワーク リソースに接続する HTTP プロキシを定義しています。HTTP トラフィックがネットワーク リソースに到達できるのは、プロキシがブラウザに指定され、クライアントが HTTP トラフィックをプロキシにルーティングする場合だけです。SSLVPN トンネルにより、HTTP プロキシの定義が複雑になります。企業ネットワークにトンネリングするときに必要なプロキシが、ブロードバンド接続経由でインターネットに接続されるときや、サード パーティ ネットワーク上にあるときに必要なものとは異なることがあるためです。

  また、大規模ネットワークを構築している企業では、複数のプロキシ サーバを設定し、一時的な状態に基づいてユーザがその中からプロキシ サーバを選択できるようにすることが必要になる場合があります。.pac ファイルを使用すると、管理者は数多くのプロキシからどのプロキシを社内のすべてのクライアント コンピュータに使用するかを決定する単一のスクリプト ファイルを作成できます。

  次に、PAC ファイルを使用する例をいくつか示します。

  - ロード バランシングのためリストからプロキシをランダムに選択します。
  - サーバのメンテナンス スケジュールに対応するために、時刻または曜日別にプロキシを交代で使用します。
  - プライマリ プロキシで障害が発生した場合に備えて、使用するバックアップ プロキシ サーバを指定します。
  - ローカル サブネットを元に、ローミング ユーザ用に最も近いプロキシを指定します。

  テキスト エディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション（.pac）ファイルを作成できます。.pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシ サーバを指定するロジックを含む JavaScript ファイルです。[PAC URL] フィールドを使用して、.pac ファイルの取得元 URL を指定します。ブラウザは、.pac ファイルを使用してプロキシ設定を判断します。.pac ファイルの詳細については、次の Microsoft サポート技術情報の記事を参照してください。

  http://www.microsoft.com/mind/0599/faq/faq0599.asp

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Standard Access List Rule

[Add/Edit Standard Access List Rule] ダイアログボックスでは、新しいルールを作成するか、または既存のルールを修正できます。

フィールド

- [Action]：新しいルールのアクション タイプを指定します。[Permit] と [Deny] のいずれかを選択します。
  - [Permit]：一致するすべてのトラフィックを許可します。
  - [Deny]：一致するすべてのトラフィックを拒否します。
- [Host/Network IP Address]：IP アドレスによってネットワークを識別します。
  - [IP address]：ホストまたはネットワークの IP アドレス。
  - [Mask]：ホストまたはネットワークのサブネット マスク。
- [Description]：（任意）アクセス ルールの説明を入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Internal Group Policy] > [Client Firewall] タブ

[Add or Edit Group Policy] ウィンドウ、[Client Firewall] タブでは、追加または変更するグループ ポリシーに対して VPN クライアントのファイアウォール設定値を設定できます。

（注） これらのファイアウォール機能を使用できるのは、Microsoft Windows を実行する VPN クライアントだけです。現在、ハードウェア クライアントまたは他（Windows 以外）のソフトウェア クライアントでは、これらの機能は使用できません。

*ファイアウォール*は、データの個々の着信パケットと発信パケットをそれぞれ検査して、パケットを許可するかドロップするかどうかを決定することにより、コンピュータをインターネットから分離して保護します。ファイアウォールは、グループのリモート ユーザがスプリット トンネリングを設定している場合、セキュリティの向上をもたらします。この場合ファイアウォールにより、インターネットまたはユーザのローカル LAN を経由する不正侵入からユーザの PC が保護され、ひいては企業ネットワークも保護されます。VPN クライアントを使用してセキュリティ アプライアンスに接続しているリモート ユーザは、適切なファイアウォール オプションを選択できます。

最初のシナリオでは、リモート ユーザの PC 上にパーソナル ファイアウォールがインストールされています。VPN クライアントは、ローカル ファイアウォールで定義されているファイアウォール ポリシーを適用し、そのファイアウォールが実行されていることを確認するためにモニタします。ファイアウォールの実行が停止すると、VPN クライアントはセキュリティ アプライアンスへの通信をドロップします。（このファイアウォール適用メカニズムは *Are You There（AYT）*と呼ばれます。VPN クライアントが定期的に「are you there?」メッセージを送信することによってファイアウォールをモニタするからです。応答が返されない場合、VPN クライアントは、ファイアウォールがダウンしたためセキュリティ アプライアンスへの接続が終了したことを認識します）。ネットワーク管理者がこれらの PC ファイアウォールを独自に設定する場合もありますが、この方法を使用すれば、ユーザは各自の設定をカスタマイズできます。

第 2 のシナリオでは、VPN クライアント PC のパーソナル ファイアウォールに中央集中型ファイアウォール ポリシーを適用することが選択されることがあります。一般的な例としては、スプリット トンネリングを使用してグループのリモート PC へのインターネット トラフィックをブロックすることが挙げられます。この方法は、トンネルが確立されている間、インターネット経由の侵入から PC を保護するので、中央サイトも保護されます。このファイアウォールのシナリオは、*プッシュ ポリシー*または *Central Protection Policy（CPP）*と呼ばれます。セキュリティ アプライアンスでは、VPN クライアントに適用するトラフィック管理ルールのセットを作成し、これらのルールをフィルタに関連付けて、そのフィルタをファイアウォール ポリシーに指定します。セキュリティ アプライアンスは、このポリシーを VPN クライアントまで配信します。その後、VPN クライアントはポリシーをローカル ファイアウォールに渡し、そこでポリシーが適用されます。

フィールド

- [Inherit]：グループ ポリシーがデフォルト グループ ポリシーからクライアントのファイアウォール設定を取得するかどうかを決めます。このオプションはデフォルト設定です。設定すると、このタブにある残りの属性がその設定によって上書きされ、名前がグレー表示になります。
- [Client Firewall Attributes]：実装されているファイアウォールのタイプ（実装されている場合）やそのファイアウォールのポリシーなど、クライアント ファイアウォール属性を指定します。
- [Firewall Setting]：ファイアウォールが存在するかどうかを一覧表示します。存在する場合には、そのファイアウォールが必須かオプションかを一覧表示します。No Firewall（デフォルト）を選択すると、このウィンドウにある残りのフィールドは、いずれもアクティブになりません。このグループのユーザをファイアウォールで保護する場合は Firewall Required または Firewall Optional 設定を選択します。

  [Firewall Required] を選択した場合は、このグループのユーザ全員が、指定されたファイアウォールを使用する必要があります。セキュリティ アプライアンスは、指定された、サポートされているファイアウォールがインストールおよび実行されていない状態で接続を試行したセッションをドロップします。この場合、セキュリティ アプライアンスは、ファイアウォール設定が一致しないことを VPN クライアントに通知します。

（注） グループでファイアウォールを必須にする場合には、そのグループに Windows VPN クライアント以外のクライアントが存在しないことを確認してください。Windows VPN クライアント以外のクライアント（クライアント モードの ASA 5505 と VPN 3002 ハードウェア クライアントを含む）は接続できません。

このグループに、まだファイアウォールに対応していないリモート ユーザがいる場合は、Firewall Optional を選択します。Firewall Optional 設定を使用すると、グループ内のすべてのユーザが接続できるようになります。ファイアウォールに対応しているユーザは、ファイアウォールを使用できます。ファイアウォールなしで接続するユーザには、警告メッセージが表示されます。この設定は、一部のユーザがファイアウォールをサポートしており、他のユーザがサポートしていないグループを作成するときに役立ちます。たとえば、移行途中のグループでは、一部のメンバはファイアウォール機能を設定し、別のユーザはまだ設定していないことがあります。

- [Firewall Type]：シスコを含む複数のベンダーのファイアウォールを一覧表示します。Custom Firewall を選択すると、Custom Firewall の下のフィールドがアクティブになります。指定したファイアウォールが、使用できるファイアウォール ポリシーと相関している必要があります。設定したファイアウォールにより、サポートされるファイアウォール ポリシー オプションが決まります。
- [Custom Firewall]：カスタム ファイアウォールのベンダー ID、製品 ID、および説明を指定します。
  - [Vendor ID]：このグループ ポリシーのカスタム ファイアウォールのベンダーを指定します。
  - [Product ID]：このグループ ポリシー用に設定されるカスタム ファイアウォールの製品またはモデル名を指定します。
  - [Description]：（任意）カスタム ファイアウォールについて説明します。
- [Firewall Policy]：カスタム ファイアウォール ポリシーのタイプと送信元を指定します。
  - [Policy defined by remote firewall (AYT)]：ファイアウォール ポリシーがリモート ファイアウォール（Are You There）によって定義されるように指定します。Policy defined by remote firewall（AYT）は、このグループのリモート ユーザのファイアウォールが、各自の PC に存在することを意味しています。このローカル ファイアウォールが、VPN クライアントにファイアウォール ポリシーを適用します。セキュリティ アプライアンスは、指定されたファイアウォールがインストールされ、実行中である場合にだけ、このグループの VPN クライアントが接続できるようにします。指定されたファイアウォールが実行されていない場合、接続は失敗します。接続が確立すると、VPN クライアントがファイアウォールを 30 秒ごとにポーリングして、そのファイアウォールが実行されていることを確認します。ファイアウォールの実行が停止すると、VPN クライアントはセッションを終了します。
  - [Policy pushed (CPP)]：ポリシーがピアからプッシュされるように指定します。このオプションを選択する場合は、[Inbound Traffic Policy] および [Outbound Traffic Policy] リストと [Manage] ボタンがアクティブになります。セキュリティ アプライアンスは、[Policy Pushed (CPP)] ドロップダウン メニューで選択されたフィルタによって定義されるトラフィック管理ルールをこのグループの VPN クライアントに適用します。メニューで使用できる選択肢は、このセキュリティ アプライアンスで定義されているフィルタで、デフォルト フィルタも含まれます。セキュリティ アプライアンスがこれらのルールを VPN クライアントにプッシュすることに注意してください。セキュリティ アプライアンスではなく VPN クライアントから見たルールを作成し、定義する必要があります。たとえば、「in」と「out」はそれぞれ、VPN クライアントに着信するトラフィックと、VPN クライアントから発信されるトラフィックです。VPN クライアントにローカル ファイアウォールもある場合、セキュリティ アプライアンスからプッシュされたポリシーは、ローカル ファイアウォールのポリシーと同時に機能します。いずれかのファイアウォールのルールでブロックされたすべてのパケットがドロップされます。
  - [Inbound Traffic Policy]：着信トラフィックに対して使用できるプッシュ ポリシーを一覧表示します。
  - [Outbound Traffic Policy]：発信トラフィックに対して使用できるプッシュ ポリシーを一覧表示します。

– [Manage] : [ACL Manager] ウィンドウを表示します。このウィンドウで、アクセス コントロール リスト（ACL）を設定できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Internal Group Policy] > [Hardware Client] タブ

[Add or Edit Group Policy] > [Hardware Client] ダイアログボックスでは、追加または変更するグループ ポリシーでの VPN 3002 ハードウェア クライアントの設定を行うことができます。[Hardware Client] タブのパラメータは、クライアント モードの ASA 5505 とは無関係です。

フィールド

- [Inherit] :（複数インスタンス）対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。これは、このタブの属性すべてのデフォルト設定になります。
- [Require Interactive Client Authentication] : インタラクティブ クライアント認証の要求をイネーブルまたはディセーブルにします。このパラメータはデフォルトではディセーブルになっています。インタラクティブ ハードウェア クライアント認証は、VPN 3002 がトンネルを開始するたびに、手動で入力したユーザ名とパスワードで認証を行うように VPN 3002 に要求することによって、追加のセキュリティを提供します。この機能をイネーブルにすると、VPN 3002 はユーザ名とパスワードを保存しません。ユーザ名とパスワードを入力すると、VPN 3002 は接続するセキュリティ アプライアンスにクレデンシャルを送信します。セキュリティ アプライアンスは、内部または外部認証サーバを利用して認証を行います。ユーザ名とパスワードが有効な場合、トンネルが確立されます。

  グループのインタラクティブ ハードウェア クライアント認証をイネーブルにすると、セキュリティ アプライアンスがグループ内の VPN 3002 にポリシーをプッシュします。以前、VPN 3002 でユーザおよびパスワードを設定していた場合、ソフトウェアによってコンフィギュレーション ファイルから削除されます。接続しようとすると、ソフトウェアによって、ユーザ名とパスワードを要求するプロンプトが表示されます。

  後で、セキュリティ アプライアンスでグループのインタラクティブ ハードウェア認証をディセーブルにすると、VPN 3002 でローカルにイネーブルにされ、ユーザ名とパスワードを要求するプロンプトが表示され続けます。これによって、保存されたユーザ名およびパスワードがなく、セキュリティ アプライアンス でインタラクティブ ハードウェア クライアント認証がディセーブルにされても、VPN 3002 は接続できます。後で、ユーザ名とパスワードを設定し、機能をディセーブルにすると、プロンプトは表示されなくなります。VPN 3002 は、保存されたユーザ名とパスワードを使用して、セキュリティ アプライアンスに接続します。
- [Require Individual User Authentication] : クライアント モードの ASA 5505 またはグループ内の VPN 3002 ハードウェア クライアントの後ろにいるユーザに対する個々のユーザ認証の要求をイネーブルまたはディセーブルにします。グループ内のハードウェア クライアントにバナーを表示するには、個別ユーザ認証をイネーブルにする必要があります。このパラメータはデフォルトではディセーブルになっています。

個別ユーザ認証は、VPN 3002 のプライベート ネットワークの許可されないユーザが中央サイトにアクセスできないように保護します。個別ユーザ認証をイネーブルにした場合、ハードウェア クライアントを介して接続する各ユーザは、トンネルがすでに存在していても、Web ブラウザを開いて手動で有効なユーザ名とパスワードを入力し、セキュリティ アプライアンスの後ろにあるネットワークにアクセスする必要があります。

（注）　ユーザ認証をイネーブルにした場合、コマンドライン インターフェイスを使用してもログインできません。ブラウザを使用する必要があります。

セキュリティ アプライアンスの後ろにあるリモート ネットワークがデフォルト ホームページの場合、または、セキュリティ アプライアンスの後ろにあるリモート ネットワークの Web サイトをブラウザで開く場合、ハードウェア クライアントは、ユーザ ログイン用の適切なページをブラウザで開きます。正常にログインすると、元々入力していたページがブラウザに表示されます。

セキュリティ アプライアンスの後ろにあるネットワークにある Web ベースではないリソース（電子メールなど）にアクセスしようとすると、ブラウザを使用して認証を行うまで、接続に失敗します。

認証を行うには、ブラウザの [Location] フィールドまたは [Address] フィールドに、ハードウェア クライアントのプライベート インターフェイスの IP アドレスを入力する必要があります。ブラウザに、ハードウェア クライアントのログイン画面が表示されます。認証するには、[Connect/Login Status] ボタンをクリックします。

1 人のユーザは、同時に最大 4 セッションのログインを実行できます。個別のユーザは、グループに対して設定された認証サーバの順序に従って認証されます。

- [User Authentication Idle Timeout] : ユーザ タイムアウト期間を設定します。セキュリティ アプライアンスは、この期間にユーザ トラフィックを受信しないと、接続を終了します。タイムアウト期間は、具体的な分数または無期限です。
  - [Unlimited] : 接続がタイムアウトにならないように指定します。このオプションは、デフォルト グループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
  - [Minutes] : タイムアウト期間を分単位で指定します。1 ～ 35791394 の整数を使用します。デフォルト値は Unlimited です。

  show uauth コマンドに対する応答に示されているアイドル タイムアウトは、常に、Cisco Easy VPN リモート デバイスでのトンネルを認証したユーザのアイドル タイムアウト値です。
- [Cisco IP Phone Bypass] : Cisco IP Phone にインタラクティブ個別ユーザ認証プロセスをバイパスさせます。イネーブルにした場合、ハードウェア クライアント認証は有効のままです。デフォルトでは、Cisco IP Phone Bypass はディセーブルになっています。

（注）　IP Phone 接続にネットワーク拡張モードを使用するように、クライアント モードの ASA 5505 または VPN 3002 ハードウェア クライアントを設定する必要があります。

- [LEAP Bypass] : シスコの無線デバイスからの LEAP パケットに、個々のユーザ認証プロセスをバイパスさせます（イネーブルの場合）。LEAP Bypass を使用して、ハードウェア クライアントの後ろにあるデバイスからの LEAP パケットを、ユーザ認証の*前に* VPN トンネルを通過させることができます。これにより、シスコ ワイヤレス アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できるようになります。その後、ユーザ単位で再度認証を実行できます（イネーブルの場合）。LEAP Bypass は、デフォルトでディセーブルになっています。

（注）　インタラクティブ ハードウェア クライアント認証をイネーブルにした場合、この機能は正常に動作しません。

IEEE 802.1X は、有線および無線ネットワークにおける認証規格です。この規格は、クライアントと認証サーバの間の強力な相互認証を無線 LAN に提供します。ユーザごと、セッションごとのダイナミック WEP（wireless encryption privacy）キーを提供することで、スタティック WEP キーで発生する管理作業とセキュリティ上の問題を軽減します。

シスコは、Cisco LEAP と呼ばれる 802.1X 無線認証タイプを開発しました。LEAP は、無線クライアントと RADIUS サーバの間の接続における相互認証を実装します。パスワードなど、認証に使用されるクレデンシャルは、ワイヤレス媒体を経由して送信される前に必ず暗号化されます。

（注）　Cisco LEAP では、無線クライアントを RADIUS サーバに対して認証します。RADIUS アカウンティング サービスは提供されません。

ハードウェア クライアントの後ろにいる LEAP ユーザには、面倒な問題があります。トンネルで中央サイト デバイスの後ろにある RADIUS サーバにクレデンシャルを送信することができないため、LEAP 認証をネゴシエートできません。トンネル経由でクレデンシャルを送信できない理由は、無線ネットワークで認証されていないためです。この問題を解決するために、LEAP バイパスは、個別のユーザ認証の前に LEAP パケット（LEAP パケットだけ）をトンネルで転送し、RADIUS サーバへの無線接続を認証できるようにします。これによって、ユーザは、個別のユーザ認証に進むことができます。

LEAP バイパスは、次の条件下で、意図されたとおりに機能します。

- インタラクティブ ユニット認証機能（有線デバイス用）が、ディセーブルであること。インタラクティブ ユニット認証がイネーブルの場合、トンネルを使用して LEAP デバイスが接続できるようになる前に、非 LEAP（有線）デバイスがハードウェア クライアントを認証する必要があります。
- 個別のユーザ認証がイネーブルであること（イネーブルでない場合、LEAP バイパスを使用する必要はありません）。
- 無線環境のアクセス ポイントが Cisco Aironet Access Point であること。PC の NIC カードは、他のブランドの製品でもかまいません。
- Cisco Aironet Access Point で、Cisco Discovery Protocol（CDP）を実行していること。
- ASA 5505 または VPN 3002 が、クライアント モードまたはネットワーク拡張モードで動作していること（どちらでもかまいません）。
- LEAP パケットが、ポート 1645 または 1812 経由で RADIUS サーバへのトンネルに転送されること。

（注）　未認証のトラフィックがトンネルを通過するのを許可すると、セキュリティ リスクが発生する可能性があります。

- [Allow Network Extension Mode] : ハードウェア クライアントでのネットワーク拡張モードの使用を制限します。このオプションを選択すると、ハードウェア クライアントがネットワーク拡張モードを使用できるようになります。Call Manager は実際の IP アドレスでだけ通信できるため、ハードウェア クライアントが IP Phone 接続をサポートするには、ネットワーク拡張モードが必要です。

（注）　ネットワーク拡張モードをディセーブルにすると（デフォルト設定）、ハードウェア クライアントはこのセキュリティ アプライアンスに PAT モードでだけ接続できるようになります。ここでネットワーク拡張モードを禁止するときは、グループ内のすべてのハードウェア クライアントを PAT モード用に設定してください。ネットワーク拡張モードを使用するようにハードウェア クライアントが設定されていて、接続しようとするセキュリティ アプライアンスがネットワーク拡張モードをディセーブルにしている場合、ハードウェア クライアントは 4 秒ごとに接続を試行し、すべての試行が拒否されます。この場合、ハードウェア クライアントは、接続しようとするセキュリティ アプライアンスに不要な処理負荷をかけることになります。多数のハードウェア クライアントがこのように誤設定されている場合、セキュリティ アプライアンスのサービス提供能力が損なわれます。

モード

次の表は、この機能を使用できるモードを示したものです。

Add/Edit Server and URL List

[Add or Edit Server and URL List] ダイアログボックスでは、指定された URL リストの項目を、編集、削除、および並べ替えできます。

フィールド

- [List Name]：追加するリストの名前を指定するか、変更または削除するリストの名前を選択します。
- [URL Display Name]：ユーザに表示する URL 名を指定します。
- [URL]：表示名に関連付けられている URL を指定します。
- [Add]：[Add Server or URL] ダイアログボックスを開きます。このダイアログボックスで、新しいサーバまたは URL と表示名を設定できます。
- [Edit]：[Edit Server or URL] ダイアログボックスを開きます。このダイアログボックスで、新しいサーバまたは URL と表示名を設定できます。
- [Delete]：選択した項目をサーバと URL リストから削除します。確認されず、やり直しもできません。
- [Move Up/Move Down]：サーバと URL リストでの、選択した項目の位置を変更します。

Add/Edit Server or URL

[Add or Edit Server or URL] ダイアログボックスでは、指定された URL リストの項目を追加、編集、削除、および並べ替えできます。

フィールド

- [URL Display Name]：ユーザに表示する URL 名を指定します。
- [URL]：表示名に関連付けられている URL を指定します。

Configuring SSL VPN Connections

このウィンドウおよびその子ウィンドウを使用して、クライアントベース接続の SSL VPN 接続属性を指定します。これらの属性は、Cisco AnyConnect VPN クライアントとレガシー SSL VPN クライアントに適用されます。

メイン ウィンドウでは、選択するインターフェイスでのクライアント アクセスをイネーブルにし、接続（トンネル グループ）を選択、追加、編集、および削除できます。ログイン時にユーザが特定の接続を選択できるようにするかどうかも指定できます。

フィールド

[Access Interfaces] : テーブルの一覧にあるインターフェイスごとに SSL VPN クライアント アクセスを指定します。

- [Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces in the table below] : [Allow Access] がオンになっているインターフェイスでのアクセスをイネーブルにします。
- [Interface] : SSL VPN クライアント接続をイネーブルにするインターフェイス。
- [Allow Access] : アクセスを許可する場合にオンにします。
- [Require Client Certificate] : 接続を許可する前にクライアントからの有効な証明書が必要な場合にオンにします。
- [Enable DTLS] : Datagram Transport Layer Security（DTLS）をイネーブルにする場合にオンにします。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。
- [Access Port] : SSL VPN クライアント接続のポートを指定します。
- [DTLS Port] : DTLS 接続のポートを指定します。

[Connection Profiles] : 接続（トンネル グループ）のプロトコル固有属性を設定します。

- [Add/Edit] : 接続プロファイル（トンネル グループ）を追加または編集します。
- [Name] : 接続プロファイルの名前。
- [Aliases] : 接続プロファイルの別名。
- [SSL VPN Client Protocol] : SSL VPN クライアントにアクセス権を与えるかどうかを指定します。
- [Group Policy] : この接続プロファイルのデフォルト グループ ポリシーを表示します。
- [Allow user to select connection, identified by alias in the table above, at login page] : [Login] ページでの接続プロファイル（トンネル グループ）エイリアスの表示をイネーブルにする場合はオンにします。

SSL VPN 接続の基本属性の設定

SSL VPN 接続の基本属性を設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [SSL VPN Connections] > [Add or Edit] > [Basic] を選択します。[Add SSL VPN Connection (Basic)] ウィンドウが開きます。

フィールド

[Add SSL VPN Connection (Basic)] ウィンドウで次の属性を設定します。

- [Aliases] :（任意）この接続の代替名を 1 つ以上入力します。名前は、スペースまたは句読点で区切ることができます。

- [Authentication]：[AAA]、[Certificate]、または [Both] から使用する認証処理の種類を選択します。
- [AAA Server Group]：ドロップダウン リストから AAA サーバ グループを選択します。デフォルト設定は LOCAL です。この場合は、セキュリティ アプライアンスが認証を処理するように指定されます。選択する前に、[Manage] をクリックして、このウィンドウに重ねてダイアログボックスを開き、AAA サーバ グループのセキュリティ アプライアンス コンフィギュレーションを表示したり、変更を加えたりすることができます。

  LOCAL 以外を選択すると、[Use LOCAL if Server Group Fails] チェックボックスが選択できるようになります。
- [Use LOCAL if Server Group fails]：Authentication Server Group 属性によって指定されたグループに障害が発生したときに、LOCAL データベースをイネーブルにする場合はオンに、ディセーブルにする場合はオフにします。
- [DHCP Servers]：使用する DHCP サーバの名前または IP アドレスを入力します。
- [Client Address Pools]：クライアント アドレス割り当てで使用する、選択可能な設定済みの IP アドレス プールの名前を入力します。選択する前に、[Select] をクリックして、このウィンドウに重ねてダイアログボックスを開き、アドレス プールを表示したり、変更を加えたりすることができます。
- [Group Policy]：この接続のデフォルト グループ ポリシーとして割り当てる VPN グループ ポリシーを選択します。VPN グループ ポリシーは、ユーザ指向属性値のペアの集合で、デバイスで内部に、または RADIUS サーバで外部に保存できます。デフォルト値は DfltGrpPolicy です。[Manage] をクリックして別のダイアログボックスを重ねて開き、グループ ポリシー コンフィギュレーションに変更を加えることができます。
- [SSL VPN Client Protocol]：SSL VPN をイネーブルにする場合は [Enabled] をオンにし、ディセーブルにする場合はオフにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

IPSec または SSL VPN 接続の高度な属性の設定

高度な属性を使用して、IPSec または SSL VPN 接続のパラメータを微調整します。

IPSec または SSL VPN 接続の一般属性の設定

[Add IPsec Remote Access Connection] または [Add SSL VPN Connection] で [Advanced] > [General] を選択して、AAA サーバに渡す前にユーザ名からレルムとグループを除去するかどうかを指定し、パスワード管理パラメータを設定します。

フィールド

このウィンドウ [Add IPsec Remote Access Connection] または [Add SSL VPN Connection (General)] ウィンドウで、次のように属性を設定します。

- [Strip the realm from the username before passing it on to the AAA server] : レルム（管理ドメイン）をユーザ名から除去してから、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のレルム修飾子を削除するには、[Strip Realm] チェックボックスをオンにします。レルム名は、AAA（認証、許可、アカウンティング）のユーザ名に追加できます。レルムに対して有効なデリミタは @ だけです。形式は、username@realm です。たとえば、JaneDoe@it.cisco.com です。この [Strip Realm] チェックボックスをオンにすると、認証はユーザ名のみに基づいて行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。

（注） レルムとグループは、両方をユーザ名に追加できます。その場合、セキュリティ アプライアンスは、グループと AAA 機能用のレルムに対して設定されたパラメータを使用します。このオプションのフォーマットは *JaneDoe@it.cisco.com#VPNGroup* のように、*ユーザ名 [@realm][<# または !> グループ]* という形式を取ります。このオプションを選択した場合は、グループ デリミタとして # または ! を使用する必要があります。これは、@ がレルム デリミタとしても使用されている場合には、セキュリティ アプライアンスが @ をグループ デリミタと解釈できないためです。

Kerberos レルムは特殊事例です。Kerberos レルムの命名規則として、Kerberos レルムと関連付けられている DNS ドメイン名を大文字で表記します。たとえば、ユーザが it.cisco.com ドメインに存在する場合には、Kerberos レルムを IT.CISCO.COM と表記します。

- [Strip the group from the username before passing it on to the AAA server]: グループ名をユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のグループ名を削除するには、[Strip Group] チェックボックスをオンにします。このオプションは、[Enable Group Lookup] をオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザ名に追加し、Group Lookup をイネーブルにすると、セキュリティ アプライアンスは、デリミタの左側にある文字をすべてユーザ名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループ デリミタは @、#、および ! で、@ が Group Lookup のデフォルトです。*JaneDoe@VPNGroup*、*JaneDoe#VPNGroup* や *JaneDoe!VPNGroup* のように、*ユーザ名<デリミタ>グループ*の形式でグループをユーザ名に追加します。
- [Password Management] : AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。

  セキュリティ アプライアンスでは、RADIUS および LDAP プロトコルのパスワード管理をサポートします。LDAP の場合には、「password-expire-in-days」オプションだけがサポートされています。このパラメータは、その通知をサポートする AAA サーバの場合に有効です。RADIUS または LDAP 認証が設定されていない場合、セキュリティ アプライアンスではこのコマンドが無視されます。

  IPSec リモート アクセスおよび SSL VPN トンネル グループのパスワード管理を設定できます。

（注） MSCHAP をサポートする一部の RADIUS サーバは、現在 MSCHAPv2 をサポートしていません。この機能では MSCHAPv2 が必要になるので、この点についてベンダーにお問い合わせください。

セキュリティ アプライアンスのリリース 7.1 以降では通常、LDAP による認証時、または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- AnyConnect VPN クライアント
- IPSec VPN クライアント
- クライアントレス SSL VPN

Kerberos/Active Directory（Windows パスワード）または NT 4.0 ドメインでは、これらの接続タイプのいずれについても、パスワード管理はサポート*されません*。RADIUS サーバ（Cisco ACS など）は、認証要求を別の認証サーバにプロキシする場合があります。ただし、セキュリティ アプライアンスからは RADIUS サーバのみに対して通信しているように見えます。

（注） LDAP でパスワードを変更するには、市販の LDAP サーバごとに独自の方法が使用されています。現在、セキュリティ アプライアンスでは Microsoft Active Directory および Sun LDAP サーバに対してのみ、独自のパスワード管理ロジックを実装しています。

ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。

- [Override account-disabled indication from AAA server]：AAA サーバからの account-disabled インジケータを上書きします。

（注） override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

- [Enable notification upon password expiration to allow user to change password]：この属性をオンにすると、次の 2 つのパラメータが利用できるようになります。パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時にユーザに通知するか、またはパスワードが期限切れになる当日にユーザに通知するかを選択できます。デフォルトでは、パスワードが期限切れになるより 14 日前にユーザへの通知を開始し、以後、ユーザがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ～ 180 日です。

  どちらの場合でも、変更されずにパスワードが期限切れになると、セキュリティ アプライアンスはパスワードを変更する機会をユーザに提供します。現在のパスワードの期限が切れていなければ、ユーザはそのパスワードで引き続きログインできます。

（注） この処理によってパスワードの期限が切れるまでの日数が変わるのではなく、通知がイネーブルになるだけであるという点に注意してください。このオプションを選択する場合は、日数も指定する必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

SSL VPN Client 接続の設定

Cisco AnyConnect VPN クライアントによりリモート ユーザは、セキュリティ アプライアンスへのセキュアな SSL 接続を確立できます。このクライアントにより、ネットワーク管理者がリモート コンピュータにクライアントをインストールして設定しなくても、リモート ユーザは SSL VPN クライアントを活用できます。

事前にインストールされたクライアントがない場合、リモート ユーザは、SSL VPN 接続を受け入れるように設定されたそれぞれのブラウザ インターフェイスに IP アドレスを入力します。http:// リクエストを https:// リクエストにリダイレクトするよう セキュリティ アプライアンス が設定されていない場合、ユーザは https://<*address*> 形式で URL を入力する必要があります。

URL が入力されると、ブラウザはそのインターフェイスに接続し、ログイン画面を表示します。ユーザがログインと認証に成功し、そのユーザがクライアントを要求しているとセキュリティ アプライアンスで識別されると、セキュリティ アプライアンスは、リモート コンピュータのオペレーティング システムに合うクライアントをダウンロードします。ダウンロード後、クライアントがインストールおよび設定され、セキュアな SSL 接続が確立されます。接続の終了時には、セキュリティ アプライアンス コンフィギュレーションに従って、クライアントはそのまま残るかアンインストールされます。

以前にインストールされているクライアントの場合は、ユーザの認証時に、セキュリティ アプライアンスがクライアントのリビジョンを検査して、必要に応じてクライアントをアップグレードします。

クライアントがセキュリティ アプライアンスと SSL VPN 接続をネゴシエートした場合は、Transport Layer Security（TLS）を使用して接続します。状況に応じて、Datagram Transport Layer Security（DTLS）が使用されます。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

AnyConnect クライアントは、セキュリティ アプライアンスからダウンロードできます。または、システム管理者が手動でリモート PC にインストールできます。クライアントの手動インストールの詳細については、『*Cisco AnyConnect VPN Client Release Notes*』を参照してください。

セキュリティ アプライアンスは、ユーザが確立している接続のグループ ポリシーまたはユーザ名属性に基づきクライアントをダウンロードします。自動的にクライアントをダウンロードするようにセキュリティ アプライアンスを設定するか、またはクライアントをダウンロードするかをリモート ユーザに確認するように設定できます。後者の場合、ユーザが応答しなかった場合は、タイムアウト時間が経過した後にクライアントをダウンロードするか、ログイン ページを表示するようにセキュリティ アプライアンスを設定できます。

フィールド

- [Inherit]：（複数インスタンス）対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。これは、このペインの属性すべてのデフォルト設定になります。
- [Keep Installer on Client System]：リモート コンピュータ上で永続的なクライアントのインストールを可能にします。これをイネーブルにすることにより、クライアントの自動的なアンインストール機能がディセーブルになります。クライアントは、後続の接続のためにリモート コンピュータにインストールされたままなので、リモート ユーザの接続時間が短縮されます。
- [Compression]：圧縮を行うと、転送されるパケットのサイズが減少するため、セキュリティ アプライアンスとクライアント間の通信パフォーマンスが向上します。
- [Datagram Transport Layer Security (DTLS)]：DTLS により、一部の SSL 接続に関連する遅延と帯域幅の問題を回避し、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスを改善します。

- [Keepalive Messages] : [Interval] フィールドに 15 秒から 600 秒までの数を入力することにより、接続がアイドルの時間がデバイスによって制限されている場合でも、キープアライブ メッセージの間隔を有効および調整して、プロキシ、ファイアウォール、または NAT デバイスを通した接続を確実に開いたままにすることができます。また、間隔を調整することにより、リモート ユーザが、Microsoft Outlook や Microsoft Internet Explorer などのソケット ベースのアプリケーションを実際に実行していないときでも、クライアントが切断と再接続を行わないことが保証されます。
- [MTU] : SSL 接続の MTU サイズを調整します。256 ～ 1410 バイトの範囲で値を入力します。デフォルトでは、IP/UDP/DTLS のオーバーヘッド分を差し引き、接続で使用するインターフェイスの MTU に基づいて、自動的に MTU サイズが調整されます。
- [Client Profile to Download] : プロファイルは、ホスト コンピュータの名前およびアドレスなど、ユーザ インターフェイスに表示される接続エントリを設定するために AnyConnect クライアントが使用するコンフィギュレーション パラメータのグループです。
- [Optional Client Module to Download] : ダウンロード時間を最小限に抑えるため、AnyConnect クライアントは、サポートする各機能で必要とされるモジュールだけを（セキュリティ アプライアンスから）ダウンロードするように要求します。Start Before Logon（SBL）機能をイネーブルにする *sbl* など、他の機能をイネーブルにするモジュールの名前を指定する必要があります。

  各クライアント機能に対して入力する値のリストについては、Cisco AnyConnect VPN Client のリリース ノートを参照してください。

モード

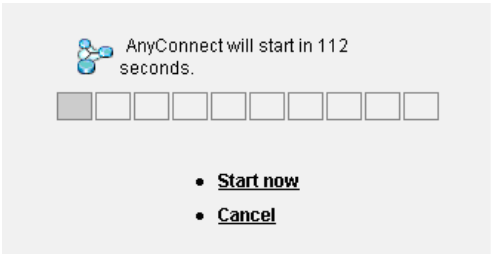
次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Login Setting

このウィンドウでは、リモート ユーザに AnyConnect クライアントのダウンロードを求めるプロンプトを表示するようにセキュリティ アプライアンスを設定できます。図 32-1 に、表示されるプロンプトを示します。

図 32-1　SSL VPN Client のダウンロードに関してリモート ユーザに表示されるプロンプト



フィールド

- [Inherit] : デフォルト グループ ポリシーから値を継承する場合はオンにします。

- [Post Login Setting] : ユーザにプロンプトを表示して、デフォルトのポスト ログイン選択を実行するためのタイムアウトを設定する場合に選択します。
- [Default Post Login Selection] : ログイン後に実行するアクションを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

キーの再生成

セキュリティ アプライアンスとクライアントがキーを再生成し、暗号キーと初期ベクトルについて再ネゴシエーションするときには、キーの再生成ネゴシエーションが行われ、接続のセキュリティが強化されます。

フィールド

- [Renegotiation Interval] : [Unlimited] チェックボックスをオフにして、セッションの開始時からキーの再生成が行われるまでの時間を分単位で、1 ～ 10080（1 週間）の範囲内で指定します。
- [Renegotiation Method] : [None] チェックボックスをオンにすると、キーの再生成がディセーブルになり、[SSL] チェックボックスをオンにして、キーの再生成中の SSL 再ネゴシエーションを指定するか、または [New Tunnel] チェックボックスをオンにして、キーの再生成中に新しいトンネルを確立します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Dead Peer Detection

Dead Peer Detection（DPD）により、ピアが応答してしない、接続で障害が発生している状態を、セキュリティ アプライアンス（ゲートウェイ）またはクライアントがすばやく確実に検出できるようにします。

フィールド

- [Gateway Side Detection] : DPD がセキュリティ アプライアンス（ゲートウェイ）によって実行されるように指定するには、[Disable] チェックボックスをオフにします。セキュリティ アプライアンスが DPD を実行するときの間隔を 30 ～ 3600 秒の範囲で入力します。

- [Client Side Detection] : DPD がクライアントによって実行されるように指定するには、[Disable] チェックボックスをオフにします。クライアントが DPD を実行するときの間隔を 30 ～ 3600 秒の範囲で入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

カスタマイゼーション

フィールド

- [Portal Customization] : [AnyConnect Client/SSL VPN] ポータル ページに適用するカスタマイゼーションを選択します。デフォルトは DfltCustomization です。
- [Manage] : [Configure GUI Customization objects] ダイアログボックスが開きます。このダイアログボックスでは、カスタマイゼーション オブジェクトの追加、編集、削除、インポート、またはエクスポートを指定できます。
- [Access Deny Message] : 接続が拒否されたときにエンド ユーザに対して表示するメッセージを指定します。デフォルト グループ ポリシーのメッセージを受け入れるには、[Inherit] を選択します。[Inherit] を選択しない場合、次のデフォルト メッセージが表示されます。「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.」

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

ACL

このウィンドウでは、クライアントレス SSL VPN の ACL を設定できます。

フィールド

- [View (Unlabeled)] : 選択したエントリが展開されている（マイナス記号）か閉じられている（プラス記号）かを示します。
- [#] カラム：ACE ID 番号を指定します。
- [Enable] : この ACL がイネーブルかディセーブルかを示します。このチェックボックスを使用して、ACL をイネーブルまたはディセーブルにできます。

- [Action]：この ACL がアクセスを許可するか拒否するかを指定します。
- [Type]：この ACL が URL または TCP アドレス/ポートに適用されるかどうかを指定します。
- [Filter]：適用されるフィルタのタイプを指定します。
- [Syslog Level (Interval)]：この ACL の syslog パラメータを指定します。
- [Time Range]：この ACL の時間範囲（存在する場合）の名前を指定します。時間範囲には、1 つの間隔または複数の定期的な範囲を設定できます。
- [Description]：ACL の説明（存在する場合）を指定します。
- [Add ACL]：[Add Web Type ACL] ダイアログボックスを表示します。このダイアログボックスで、ACL ID を指定できます。
- [Add ACE]：[Add Web Type ACE] ダイアログボックスを表示します。このダイアログボックスで、名前付き ACL のパラメータを指定します。このボタンは、[Web Type ACL] テーブルに 1 つ以上のエントリが存在する場合にだけアクティブになります。
- [Edit ACE/Delete]：選択されている ACL または ACE を編集または削除する場合にクリックします。ACL を削除すると、その ACE もすべて削除されます。警告は表示されず、復元もできません。
- [Move Up/Move Down]：ACL または ACE を選択してこれらのボタンをクリックすると、ACL および ACE の順序が変更されます。セキュリティ アプライアンスは、ACL と ACE を、ACL リストボックスでの優先順位に応じて、一致するものが見つかるまでチェックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

クライアントレス SSL VPN 接続の設定

[Clientless SSL VPN Access Connections] ウィンドウを使用して、クライアントレス SSL VPN アクセスのパラメータを設定します。このウィンドウでは、その子ダイアログボックスでのコンフィギュレーションの選択内容も記録されます。

フィールド

- [Access Interfaces]：アクセスをイネーブルにするインターフェイスをテーブルから選択できます。このテーブルのフィールドには、インターフェイス名やチェックボックスが表示され、アクセスを許可して認証のための証明書を要求するかどうかを設定できます。
- [Access Port]：接続で使用するアクセス ポートを指定します。デフォルト値は 443 です。
- [Connections]：この接続（トンネル グループ）の接続ポリシーを決定するレコードを示した接続テーブルを表示します。各レコードによって、その接続のデフォルト グループ ポリシーが識別されます。レコードには、プロトコル固有の接続パラメータが含まれています。
  - [Add]：選択した接続の [Add Clientless SSL VPN] ダイアログボックスが開きます。
  - [Edit]：選択した接続の [Edit Clientless SSL VPN] ダイアログボックスが開きます。

- [Delete]：選択した接続をテーブルから削除します。確認されず、やり直しもできません。
- [Allow user to select connection, identified by alias in the table above, at login page]：ユーザのログイン ページに、ユーザが接続で使用する特定のトンネル グループを選択するためのドロップダウン メニューが表示されるように指定します。

クライアントレス SSL VPN 接続の追加または編集

[Add or Edit SSL VPN] ダイアログボックスは、ダイアログボックス左側の展開メニューからアクセス可能な [Basic] セクションと [Advanced] セクションで構成されてます。

[Add or Edit Clientless SSL VPN Connections] > [Basic]

[Basic] ダイアログボックスでは、この接続の基本的な特性を設定できます。

フィールド

- [Name]：接続名を指定します。編集機能の場合、このフィールドは読み取り専用です。
- [Aliases]：（任意）この接続の代替名を 1 つ以上指定します。[Clientless SSL VPN Access Connections] ウィンドウでそのオプションを設定している場合に、ログイン ページに別名が表示されます。
- [Authentication]：認証パラメータを指定します。
  - [Method]：この接続で、AAA 認証、証明書認証、またはその両方を使用するかどうかを指定します。デフォルトは AAA 認証です。
  - [AAA server Group]：この接続の認証処理で使用する AAA サーバ グループを選択します。デフォルトは LOCAL です。
  - [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。
- [Default Group Policy]：この接続で使用するデフォルト グループ ポリシーのパラメータを指定します。
  - [Group Policy]：この接続で使用するデフォルト グループ ポリシーを選択します。デフォルトは DfltGrpPolicy です。
  - [Clientless SSL VPN Protocol]：この接続でのクライアントレス SSL VPN プロトコルをイネーブルまたはディセーブルにします。

[Add or Edit Clientless SSL VPN Connections] > [Advanced]

[Advanced] メニュー項目とそのダイアログボックスでは、この接続について次の特性を設定できます。

- 一般属性
- 認証属性
- 許可属性
- アカウンティング属性
- ネーム サーバ属性
- クライアントレス SSL VPN 属性

[Add or Edit Clientless SSL VPN Connections] > [Advanced] > [General]

このウィンドウを使用して、AAA サーバに渡す前にユーザ名からレルムとグループを除去するかどうかを指定し、パスワード管理オプションを指定します。

フィールド

- [Strip the realm from the username before passing it on to the AAA server]：レルム（管理ドメイン）をユーザ名から除去してから、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のレルム修飾子を削除するには、[Strip Realm] チェックボックスをオンにします。レルム名は、AAA（認証、許可、アカウンティング）のユーザ名に追加できます。レルムに対して有効なデリミタは @ だけです。形式は、username@realm です。たとえば、JaneDoe@it.cisco.com です。この [Strip Realm] チェックボックスをオンにすると、認証はユーザ名のみに基づいて行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。

（注）　レルムとグループは、両方をユーザ名に追加できます。その場合、セキュリティ アプライアンスは、グループと AAA 機能用のレルムに対して設定されたパラメータを使用します。このオプションのフォーマットは *JaneDoe@it.cisco.com#VPNGroup* のように、*ユーザ名[@realm][<# または !> グループ]* という形式を取ります。このオプションを選択した場合は、グループ デリミタとして # または ! を使用する必要があります。これは、@ がレルム デリミタとしても使用されている場合には、セキュリティ アプライアンスが @ をグループ デリミタと解釈できないためです。

Kerberos レルムは特殊事例です。Kerberos レルムの命名規則として、Kerberos レルムと関連付けられている DNS ドメイン名を大文字で表記します。たとえば、ユーザが it.cisco.com ドメインに存在する場合には、Kerberos レルムを IT.CISCO.COM と表記します。

- [Strip the group from the username before passing it on to the AAA server]: グループ名をユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のグループ名を削除するには、[Strip Group] チェックボックスをオンにします。このオプションは、[Enable Group Lookup] ボックスをオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザ名に追加し、Group Lookup をイネーブルにすると、セキュリティ アプライアンスは、デリミタの左側にある文字をすべてユーザ名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループ デリミタは @、#、および ! で、@ が Group Lookup のデフォルトです。*JaneDoe@VPNGroup*、*JaneDoe#VPNGroup* や *JaneDoe!VPNGroup* のように、*ユーザ名< デリミタ> グループ*の形式でグループをユーザ名に追加します。
- [Password Management]：AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。
  - [Override account-disabled indication from AAA server]：AAA サーバからの account-disabled インジケータを上書きします。

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

  - [Enable notification upon password expiration to allow user to change password]：このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時にユーザに通知するか、またはパスワードが期限切れになる当日にユーザに通知するかを選択できます。デ

フォルトでは、パスワードが期限切れになるより 14 日前にユーザへの通知を開始し、以後、ユーザがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ～ 180 日です。

（注）　この処理によってパスワードの期限が切れるまでの日数が変わるのではなく、通知がイネーブルになるだけであるという点に注意してください。このオプションを選択する場合は、日数も指定する必要があります。

どちらの場合でも、変更されずにパスワードが期限切れになると、セキュリティ アプライアンスはパスワードを変更する機会をユーザに提供します。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS または LDAP 認証が設定されていない場合、セキュリティ アプライアンスではこのコマンドが無視されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add or Edit Clientless SSL VPN Connection Profile or IPSec Connection Profiles] > [Advanced] > [Authentication]

[Authentication] ダイアログボックスでは、インターフェイス固有の認証サーバ グループを表示、追加、編集、または削除できます。このダイアログボックスのテーブルの各行には、インターフェイス固有サーバ グループのステータスが表示されます。表示されるのは、インターフェイス名、それに関連付けられたサーバ グループ、および選択したサーバ グループで障害が発生したときにローカル データベースへのフォールバックがイネーブルになっているかどうかです。

フィールド

- [Add or Edit] : [Assign Authentication Server Group to Interface] ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスとサーバ グループを指定するとともに、選択したサーバ グループで障害が発生した場合に LOCAL データベースへのフォールバックを許可するかどうかを指定できます。
- [Delete] : 選択したサーバ グループをテーブルから削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Assign Authentication Server Group to Interface

このダイアログボックスでは、インターフェイスを AAA サーバ グループに関連付けられます。結果は、[Authentication] ダイアログボックスのテーブルに表示されます。

フィールド

- [Interface]：DMZ、Outside、または Inside から選択します。デフォルトは DMZ です。
- [Server Group]：選択したインターフェイスに割り当てるサーバ グループを選択します。デフォルトは LOCAL です。
- [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。
- [Fallback]：選択したサーバ グループで障害が発生した場合の LOCAL へのフォールバックをイネーブルまたはディセーブルにします。

[Add or Edit SSL VPN Connections] > [Advanced] > [Authorization]

このダイアログボックスでは、デフォルトの許可サーバ グループ、インターフェイス固有の許可サーバ グループ、およびユーザ名マッピング属性を設定できます。属性は、SSL VPN およびクライアントレス SSL VPN 接続の場合と同じです。

フィールド

- [Default Authorization Server Group]：デフォルトの許可サーバ グループ属性を設定します。
  - [Server Group]：この接続で使用する認証サーバ グループを選択します。デフォルトは [None] です。
  - [Manage]：[Configure AAA Server Groups] ウィンドウが開きます。
  - [Users must exist in the authorization database to connect]：この要件をイネーブルまたはディセーブルにします。
- Interface-specific Authorization Server Groups
  - [Table]：設定されている各インターフェイスと、それに関連付けられているサーバ グループの一覧を表示します。
  - [Add or Edit]：[Assign Authorization Server Group to Interface] ウィンドウが開きます。
  - [Delete]：選択した行をテーブルから削除します。
- [User Name Mapping]：ユーザ名マッピング属性を指定します。
  - [Use the entire DN as the username]：DN 全体をユーザ名として使用する要件をイネーブルまたはディセーブルにします。

– 個々の DN フィールドをユーザ名として指定します。デフォルトが CN（一般名）のプライマリ DN フィールドと、デフォルトが OU（組織単位）のセカンダリ DN フィールドの両方を選択できます。

Assign Authorization Server Group to Interface

このダイアログボックスでは、インターフェイスを AAA サーバ グループに関連付けられます。結果は、[Authorization] ダイアログボックスのテーブルに表示されます。

フィールド

- [Interface]：DMZ、Outside、または Inside から選択します。デフォルトは DMZ です。
- [Server Group]：選択したインターフェイスに割り当てるサーバ グループを選択します。デフォルトは LOCAL です。
- [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。

[Add or Edit SSL VPN Connections] > [Advanced] > [SSL VPN]

このダイアログボックスでは、ログイン時のリモート ユーザの画面に影響する属性を設定できます。

フィールド

- [Login Page Customization]：適用する事前設定されたカスタマイゼーション属性を指定することにより、ユーザのログイン ページのルックアンドフィールを設定します。デフォルトは DfltCustomization です。
- [Manage]：[Configure GUI Customization Objects] ウィンドウが開きます。
- [Connection Aliases]：既存の接続エイリアスとそのステータスの一覧がテーブルに表示されます。各項目をテーブルに追加したり、テーブルから削除したりできます。ログイン時にユーザが特定の接続（トンネル グループ）を選択できるように接続が設定されている場合は、ユーザのログイン ページに接続エイリアスが表示されます。
  - [Add]：[Add Connection Alias] ウィンドウが開きます。このウィンドウでは、接続エイリアスを追加し、イネーブルにすることができます。
  - [Delete]：選択した行を接続エイリアス テーブルから削除します。確認されず、やり直しもできません。
- [Group URLs]：既存のグループ URL とそのステータスの一覧がテーブルに表示されます。各項目をテーブルに追加したり、テーブルから削除したりできます。ログイン時にユーザが特定のグループを選択できるように接続が設定されている場合は、ユーザのログイン ページにグループ URL が表示されます。
  - [Add]：[Add Group URL] ウィンドウが開きます。このウィンドウでは、グループ URL を追加し、イネーブルにすることができます。
  - [Delete]：選択した行を接続エイリアス テーブルから削除します。確認されず、やり直しもできません。

[Add or Edit Clientless SSL VPN Connections] > [Advanced] > [SSL VPN]

このダイアログボックスでは、ログイン時のリモート ユーザの画面に影響する属性を設定できます。

フィールド

- [Portal Page Customization]：適用する事前設定されたカスタマイゼーション属性を指定することにより、ユーザのログイン ページのルックアンドフィールを設定します。デフォルトは DfltCustomization です。
- [Manage]：[Configure GUI Customization Objects] ウィンドウが開きます。
- [Enable the display of Radius Reject]：認証が拒否されたときのログイン画面へのメッセージ。
- [Enable the display of SecureID messages on the login screen]：RADIUS サーバによってプロキシ処理された SDI メッセージがログイン画面に表示されます。
- [Connection Aliases]：既存の接続エイリアスとそのステータスの一覧がテーブルに表示されます。各項目をテーブルに追加したり、テーブルから削除したりできます。ログイン時にユーザが特定の接続（トンネル グループ）を選択できるように接続が設定されている場合は、ユーザのログイン ページに接続エイリアスが表示されます。
  - [Add]：[Add Connection Alias] ウィンドウが開きます。このウィンドウでは、接続エイリアスを追加し、イネーブルにすることができます。
  - [Delete]：選択した行を接続エイリアス テーブルから削除します。確認されず、やり直しもできません。
- [Group URLs]：既存のグループ URL とそのステータスの一覧がテーブルに表示されます。各項目をテーブルに追加したり、テーブルから削除したりできます。ログイン時にユーザが特定のグループを選択できるように接続が設定されている場合は、ユーザのログイン ページにグループ URL が表示されます。
  - [Add]：[Add Group URL] ウィンドウが開きます。このウィンドウでは、グループ URL を追加し、イネーブルにすることができます。
  - [Delete]：選択した行を接続エイリアス テーブルから削除します。確認されず、やり直しもできません。

[Add or Edit Clientless SSL VPN Connections] > [Advanced] > [Name Servers]

このダイアログボックスのテーブルには、設定済みの NetBIOS サーバの属性が表示されます。クライアントレス SSL VPN アクセスでの [Add or Edit Tunnel Group] ウィンドウの NetBIOS ダイアログボックスでは、トンネル グループの NetBIOS 属性を設定できます。クライアントレス SSL VPN では、NetBIOS と Common Internet File System（共通インターネット ファイル システム）プロトコルを使用して、リモート システム上のファイルにアクセスしたり、ファイルを共有したりします。Windows コンピュータにそのコンピュータ名を使用してファイル共有接続をしようとすると、指定されたファイル サーバはネットワーク上のリソースを識別する特定の NetBIOS 名と対応します。

セキュリティ アプライアンス は、NetBIOS 名を IP アドレスにマップするために NetBIOS ネーム サーバにクエリーを送信します。クライアントレス SSL VPN では、リモート システムのファイルをアクセスまたは共有するための NetBIOS が必要です。

NBNS 機能を動作させるには、少なくとも 1 台の NetBIOS サーバ（ホスト）を設定する必要があります。冗長性を確保するため、最大 3 つの NBNS サーバを設定できます。セキュリティ アプライアンスは、リストの最初のサーバを NetBIOS/CIFS 名前解決に使用します。クエリーが失敗すると、次のサーバが使用されます。

フィールド

- [IP Address]：設定された NetBIOS サーバの IP アドレスを表示します。
- [Master Browser]：サーバが WINS サーバであるか、あるいは CIFS サーバ（つまりマスタ ブラウザ）にもなれるサーバであるかを表します。
- [Timeout (seconds)]：サーバが NBNS クエリーに対する応答を待つ最初の時間を秒単位で表示します。この時間を過ぎると、次のサーバにクエリーを送信します。
- [Retries]：設定されたサーバに対する NBNS クエリーの送信を順番にリトライする回数を表示します。言い換えれば、エラーを返すまでサーバのリストを巡回する回数ということです。最小リトライ数は 0 です。デフォルトの再試行回数は 2 回です。最大リトライ数は 10 です。
- [Add/Edit]：NetBIOS サーバを追加します。[Add or Edit NetBIOS Server] ダイアログボックスが開きます。
- [Delete]：選択した NetBIOS 行をリストから削除します。
- [Move Up/Move Down]：セキュリティ アプライアンスが、このボックスに表示された順序で NetBIOS サーバに NBNS クエリーを送信します。このボックスを使用して、クエリーをリスト内で上下に動かすことにより、優先順位を変更します。

フィールド

- [DNS Server Group]：この接続の DNS サーバ グループとして使用するサーバを選択します。デフォルトは DefaultDNS です。
- [Manage]：[Configure DNS Server Group] ダイアログボックスが開きます。

Configure DNS Server Groups

このダイアログボックスでは、サーバ グループ名、サーバ、タイムアウトの秒数、許容リトライ回数、およびドメイン名を含む、設定済みの DNS サーバがテーブルに表示されます。このダイアログボックスで、DNS サーバ グループを追加、編集、または削除できます。

フィールド

- [Add or Edit]：[Add or Edit DNS Server Group] ダイアログボックスが開きます。
- [Delete]：選択した行をテーブルから削除します。確認されず、やり直しもできません。

[Add or Edit Clientless SSL VPN Connections] > [Advanced] > [Clientless SSL VPN]

このダイアログボックスでは、クライアントレス SSL VPN 接続のポータル関連属性を指定できます。

フィールド

- [Portal Page Customization]：ユーザ インターフェイスに適用するカスタマイゼーションを選択します。
- [Manage]：[Configure GUI Customization Objects] ダイアログボックスが開きます。

IPSec リモート アクセス接続のプロファイル

[IPSec ConnectionProfiles] ウィンドウのパラメータにより、IPSec リモート アクセス接続を設定できます。このセクションのほとんどのパラメータは、以前トンネル グループのセクションで設定していたパラメータです。IPSec 接続は、IPSec 接続とクライアントレス SSL VPN 接続の接続固有レコードを表します。

IPSec グループは、IPSec 接続パラメータを使用してトンネルを作成します。IPSec 接続は、リモートアクセスまたは Site-to-Site のいずれかです。IPSec グループは、内部サーバまたは外部 RADIUS サーバ上で設定されます。クライアント モードの ASA 5505 または VPN 3002 ハードウェア クライアント パラメータ（インタラクティブ ハードウェア クライアント認証と個別ユーザ認証をイネーブルまたはディセーブルにする）の場合は、ユーザとグループに対して設定されたパラメータよりも IPSec 接続パラメータが優先されます。

クライアントレス SSL VPN トンネルグループのパラメータは、この IPSec 接続に適用するクライアントレス SSL VPN グループのパラメータです。クライアントレス SSL VPN アクセスは、[Configuration] > [Clientless SSL VPN] ウィンドウで設定します。

フィールド

- [Access Interfaces]：IPSec アクセスでイネーブルにするインターフェイスを選択します。デフォルトでは、アクセス方式は何も選択されていません。
- [Connections]：既存の IPSec 接続の設定済みパラメータを表形式で表示します。[Connections] テーブルには、接続ポリシーを決定するレコードが表示されます。1 つのレコードによって、その接続のデフォルト グループ ポリシーが識別されます。レコードにはプロトコル固有の接続パラメータが含まれています。テーブルには、次のカラムがあります。
  - [Name]：IPSec 接続の名前または IP アドレスを指定します。
  - [ID Certificate]：ID 証明書がある場合は、その名前を指定します。
  - [IPSec Protocol]：IPSec プロトコルがイネーブルになっているかどうかを示します。このプロトコルは、[Add or Edit IPSec Remote Access Connection] の [Basic] ウィンドウでイネーブルにします。
  - [L2TP/IPSec Protocol]：L2TP/IPSec プロトコルがイネーブルになっているかどうかを示します。このプロトコルは、[Add or Edit IPSec Remote Access Connection] の [Basic] ウィンドウでイネーブルにします。
  - [Group Policy]：この IPSec 接続のグループ ポリシーの名前を示します。
- [Add or Edit]：[Add or Edit IPSec Remote Access Connection Profile] ダイアログボックスが開きます。
- [Delete]：選択したサーバ グループをテーブルから削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add or Edit an IPSec Remote Access Connection Profile

[Add or Edit IPSec Remote Access Connection Profile] ダイアログボックスのナビゲーション ペインでは、設定する基本エレメントまたは詳細エレメントを選択できます。

Add or Edit IPSec Remote Access Connection Profile Basic

[Add or Edit IPSec Remote Access Connection Profile Basic] ダイアログボックスでは、IPSec 接続の共通属性を設定できます。

フィールド

- [Name]：接続名を指定します。
- [IKE Peer Authentication]：IKE ピアを設定します。
  - [Pre-shared key]：接続の事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Identity Certificate]：ID 証明書が設定および登録されている場合は、ID 証明書の名前を選択します。
  - [Manage]：[Manage Identity Certificates] ウィンドウが開きます。このウィンドウでは、選択した証明書の詳細を追加、編集、削除、エクスポート、または表示できます。
- [User Authentication]：ユーザ認証で使用するサーバの情報を指定します。詳細な認証情報は [Advanced] セクションで設定できます。
  - [Server Group]：ユーザ認証で使用するサーバ グループを選択します。デフォルトは LOCAL です。LOCAL 以外のサーバ グループを選択すると、[Fallback] チェックボックスが選択できるようになります。
  - [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。
  - [Fallback]：指定したサーバ グループで障害が発生した場合に、ユーザ認証で LOCAL を使用するかどうかを指定します。
- [Client Address Assignment]：クライアント属性の割り当てに関連した属性を指定します。
  - [DHCP Servers]：使用する DHCP サーバの IP アドレスを指定します。最大で 10 台までのサーバをスペースで区切って追加できます。
  - [Client Address Pools]：事前定義済みのアドレス プールを 6 個まで指定します。アドレス プールを定義するには、[Configuration] > [Remote Access VPN] > [Network Client Access] > [Address Assignment] > [Address Pools] に移動します。
  - [Select]：[Select Address Pools] ダイアログボックスが開きます。
- [Default Group Policy]：デフォルト グループ ポリシーに関連した属性を指定します。
  - [Group Policy]：この接続で使用するデフォルト グループ ポリシーを選択します。デフォルトは DfltGrpPolicy です。
  - [Manage]：[Configure Group Policies] ダイアログボックスが開きます。このダイアログボックスでは、グループ ポリシーを追加、編集、または削除できます。
  - [Client Protocols]：この接続で使用するプロトコルを選択します。デフォルトでは、IPSec と L2TP over IPSec の両方が選択されています。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

IPSec または SSL VPN 接続プロファイルへの証明書のマッピング

セキュリティ アプライアンスは、クライアント証明書認証で IPSec または SSL 接続要求を受け取ると、一致するルールが見つかるまで、ルール セットを使用して証明書の属性を評価します。一致するルールが見つかると、そのルールに関連付けられた接続プロファイルを接続に割り当てます。一致するルールが見つからない場合、セキュリティ アプライアンスは DefaultWEBVPNGroup プロファイルを接続に割り当て、これによりユーザは、接続プロファイルがイネーブルになっていれば、ポータル ページに表示されるドロップダウン メニューからその接続プロファイルを選択できます。

証明書基準ベース ルールに対する IPSec または SSL VPN 接続の評価を設定するには、[IPSec Certificate to Connection Maps] > [Rules or Certificate to SSL VPN Connections Profile Maps] パネルを使用します。

このパネルでは、次のようにして、IPSec および SSL VPN 接続プロファイルごとに証明書ベース基準を作成できます。

ステップ 1　上部（[Certificate to Connection Profile Maps]）に表示されるテーブルを使用して、次のいずれかを実行します。

- 「map」というリスト名を作成し、リストのプライオリティを指定して、そのリストを接続プロファイルに割り当てます。

  リストをテーブルに追加すると、ASDM で強調表示されます。

- 証明書ベース ルールを追加する接続プロファイルにリストが割り当てられていることを確認します。

  テーブルにリストを追加すると、ASDM で強調表示されます。ASDM のペインの下部のテーブルには、関連付けられたリスト エントリが表示されます。

ステップ 2　下部のテーブル（[Mapping Criteria]）を使用して、選択したリストのエントリを表示、追加、変更、または削除します。

リストの各エントリは、1 つの証明書ベース ルールで構成されています。セキュリティ アプライアンスが関連付けられたマップ インデックスを選択するには、マッピング基準リストのルールすべてが証明書の内容と一致する必要があります。1 つまたは別の基準が一致する場合に接続を割り当てるには、照合基準ごとにリストを 1 つ作成します。

フィールドの詳細については、次の項を参照してください。

- Add/Edit Certificate Matching Rule
- Add/Edit Certificate Matching Rule Criterion

Add/Edit Certificate Matching Rule

[Add/Edit Certificate Matching Rule] ダイアログボックスを使用して、接続プロファイルにリストの名前（map）を割り当てます。

フィールド

- [Map]：次のいずれかを選択します。
  - [Existing]：ルールを含めるマップの名前を選択します。
  - [New]：ルールの新しいマップ名を入力します。
- [Rule Priority]：10 進数を入力して、接続要求を受け取ったときに セキュリティ アプライアンスがマップを評価する順序を指定します。定義されている最初のルールのデフォルト プライオリティは 10 です。セキュリティ アプライアンスは、最低位のプライオリティ番号のマップと最初に比較して各接続を評価します。
- [Mapped to Connection Profile]：以前は「トンネル グループ」と呼んでいた接続プロファイルを選択して、このルールにマッピングします。

  次の項の説明にあるマップへのルール基準の割り当てを行わない場合、セキュリティ アプライアンスはそのマップ エントリを無視します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Certificate Matching Rule Criterion

[Add/Edit Certificate Matching Rule Criterion] ダイアログボックスを使用して、選択したグループの証明書照合ルールの基準を設定します。

フィールド

- [Rule Priority]：（表示専用）接続要求を受け取ったときにセキュリティ アプライアンスがマップを評価する順番。セキュリティ アプライアンスは、最低位のプライオリティ番号のマップと最初に比較して各接続を評価します。
- [Mapped to Group]：（表示専用）ルールが割り当てられている接続プロファイル。
- [Field]：ドロップダウン リストから、評価する証明書の部分を選択します。
  - [Subject]：証明書を使用するユーザまたはシステム。CA のルート証明書の場合は、Subject と Issuer が同じです。
  - [Alternative Subject]：サブジェクト代替名拡張により、追加する ID を証明書のサブジェクトにバインドできます。

  - [Issuer]：証明書を発行した CA または他のエンティティ（管轄元）。
- [Component]：（[Subject of Issuer] が選択されている場合にだけ適用）ルールで使用する識別名コンポーネントを次の中から選択します。

DN フィールド	定義
Whole Field	DN 全体。
Country（C）	2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name（CN）	ユーザ、システム、その他のエンティティの名前。これは、ID 階層の最下位（最も固有性の高い）レベルです。
DN Qualifier（DNQ）	特定の DN 属性。
E-mail Address（EA）	証明書を所有するユーザ、システム、またはエンティティの電子メール アドレス。
Generational Qualifier（GENQ）	Jr.、Sr.、または III などの世代修飾子。
Given Name（GN）	証明書所有者の名前（名）。
Initials（I）	証明書所有者の姓と名の最初の文字。
Locality（L）	組織が所在する市町村。
Name（N）	証明書所有者の名前。
Organization（O）	会社、団体、機関、協会、その他のエンティティの名前。
Organizational Unit（OU）	組織内のサブグループ。
Serial Number（SER）	証明書のシリアル番号。
Surname（SN）	証明書所有者の姓。
State/Province（S/P）	組織が所在する州や県。
Title（T）	証明書所有者の役職（Dr. など）。
User ID（UID）	証明書所有者の ID 番号。
Unstructured Name（UNAME）	unstructuredName 属性タイプは、サブジェクトの名前を非構造化 ASCII 文字列として指定します。
IP Address (IP)	IP アドレス フィールド。

- [Operator]：ルールで使用する演算子を選択します。
  - [Equals]：識別名フィールドが値に完全一致する必要があります。
  - [Contains]：識別名フィールドに値が含まれている必要があります。
  - [Does Not Equal]：識別名フィールドが値と一致しないようにします。
  - [Does Not Contain]：識別名フィールドに値が含まれないようにします。

[Value]：255 文字までの範囲で演算子のオブジェクトを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Site-to-Site トンネル グループの設定

[Tunnel Groups] ウィンドウには、現在設定されている Site-to-Site トンネル グループの属性が表示されます。このウィンドウでは、トンネル グループ名を解析するときに使用するデリミタ文字を選択し、トンネル グループを追加、変更、または削除できます。

フィールド

- [Add] : [Add IPSec Site-to-Site Tunnel Group] ダイアログボックスが開きます。
- [Edit] : [Edit IPSec Site-to-Site Tunnel Group] ダイアログボックスが開きます。
- [Delete] : 選択したトンネル グループを削除します。確認されず、やり直しもできません。
- [Table of Tunnel Groups] : トンネル グループ名、CA 証明書、IPSec プロトコル ステータス（イネーブルまたはディセーブル）、および各設定済みトンネル グループに適用されるグループ ポリシーの一覧を表示します。
- [Group Delimiter] : トンネルのネゴシエーションが行われるときに受信するユーザ名からトンネル グループ名を解析するときに使用する、デリミタ文字を選択します。

Site-to-Site 接続の追加および編集

[Add or Edit IPSec Site-to-Site Connection] ダイアログボックスでは、IPSec Site-to-Site 接続を作成または変更できます。このダイアログボックスでは、IP アドレスの指定、接続名の指定、インターフェイスの選択、IKE ピアとユーザ認証パラメータの指定、保護されたネットワークの指定、および暗号化アルゴリズムの指定を行うことができます。

フィールド

- [Peer IP Address] : IP アドレスを指定し、そのアドレスをスタティックにするかどうかを指定できます。
- [Connection Name] : このトンネル グループに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。接続名が、[Peer IP Address] フィールドで指定される IP アドレスと同じになるように指定できます。
- [Interface] : この接続で使用するインターフェイスを選択します。
- [IKE Authentication] : IKE ピアの認証で使用する事前共有キーと ID 証明書を指定します。
  - [Pre-shared Key] : トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Identity Certificate] : 認証で使用する ID 証明書がある場合は、その名前を指定します。
  - [Manage] : [Manage CA Certificates] ウィンドウが開きます。このウィンドウでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。

- [Protected Networks]：この接続で保護されているローカルおよびリモート ネットワークを選択または指定します。
  - [Local Network]：ローカル ネットワークの IP アドレスを指定します。
  - [...]：[Browse Local Network] ダイアログボックスが開きます。このダイアログボックスでは、ローカル ネットワークを選択できます。
  - [Remote Network]：リモート ネットワークの IP アドレスを指定します。
  - [...]：[Browse Remote Network] ダイアログボックスが開きます。このダイアログボックスでは、リモート ネットワークを選択できます。
- [Encryption Algorithm]：IKE および IPSec 提案で使用する暗号化アルゴリズムを指定します。
  - [IKE Proposal]：IKE 提案で使用する暗号化アルゴリズムを 1 つ以上指定します。
  - [Manage]：[Configure IKE Proposals] ダイアログボックスが開きます。
  - [IPSec Proposal]：IPSec 提案で使用する暗号化アルゴリズムを 1 つ以上指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Site-to-Site トンネル グループの追加または編集

[Add or Edit IPSec Site-to-Site Tunnel Group] ダイアログボックスでは、追加する IPSec Site-to-Site 接続の属性を指定できます。また、IKE ピアとユーザ認証パラメータの選択、IKE キープアライブ モニタリングの設定、およびデフォルト グループ ポリシーの選択も行うことができます。

フィールド

- [Name]：このトンネル グループに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。
- [IKE Authentication]：IKE ピアの認証で使用する事前共有キーおよび ID 証明書パラメータを指定します。
  - [Pre-shared Key]：トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Identity Certificate]：認証で使用する ID 証明書がある場合は、その名前を指定します。
  - [Manage]：[Manage Identity Certificates] ウィンドウが開きます。このウィンドウでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
  - [IKE Peer ID Validation]：IKE ピア ID の有効性をチェックするかどうかを指定します。デフォルトは Required です。
- [IKE Keepalive]：IKE キープアライブ モニタリングをイネーブルにし、設定を行います。次の属性の中から 1 つだけ選択できます。

- [Disable Keep Alives]：IKE キープアライブをイネーブルまたはディセーブルにします。
- [Monitor Keep Alives]：IKE キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
- [Confidence Interval]：IKE キープアライブの信頼間隔を指定します。これは、ピアがキープアライブ モニタリングを開始するまでにセキュリティ アプライアンスが許可するアイドル時間を表す秒数です。最小 10 秒、最大 300 秒です。リモート アクセス グループのデフォルトは 10 秒です。
- [Retry Interval]：IKE キープアライブのリトライ間の待機秒数を指定します。デフォルトは 2 秒です。
- [Head end will never initiate keepalive monitoring]：中央サイトのセキュリティ アプライアンスがキープアライブ モニタリングを開始しないように指定します。

- [Default Group Policy]：この接続のデフォルトとして使用するグループ ポリシーとクライアント プロトコルを選択します。VPN グループ ポリシーは、ユーザ指向属性値のペアの集合で、デバイスで内部に、または RADIUS サーバで外部に保存できます。IPSec 接続とユーザ アカウントは、グループ ポリシー情報を参照します。
  - [Group Policy]：現在設定されているグループ ポリシーを一覧表示します。デフォルト値は DfltGrpPolicy です。
  - [Manage]：[Configure Group Policies] ウィンドウが開きます。このウィンドウでは、設定済みのグループ ポリシーを表示し、リストのグループ ポリシーを追加、編集、または削除できます。
  - [IPSec Protocol]：このグループ ポリシーで使用する IPSec プロトコルをイネーブルまたはディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Crypto Map Entry

このウィンドウでは、接続プロファイルの暗号パラメータを指定します。

フィールド

- [Priority]：一意のプライオリティ（1 ～ 65,543、1 が最高のプライオリティ）。IKE ネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモート ピアに送信します。リモート ピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。
- [Perfect Forward Secrecy]：特定の IPSec SA のキーが他のシークレット（他のキーなど）から導出されたものでないことを保証します。PFS により、攻撃者がキーを突破できたとしても、そのキーから他のキーを導出できないようにします。PFS をイネーブルにすると、Diffie-Hellman Group リストがアクティブになります。

  - [Diffie-Hellman Group]：2 つの IPSec ピアが、相互に共有秘密情報を転送することなく共有秘密情報を導出するために使用する ID。Group 1（768 ビット）、Group 2（1024 ビット）、および Group 5（1536 ビット）の中から選択します。
- [Enable NAT-T]：このポリシーの NAT Traversal（NAT-T）をイネーブルにします。これにより IPSec ピアは、NAT デバイスを介してリモート アクセスと LAN-to-LAN の両方の接続を確立できます。
- [Enable Reverse Route Injection]：リモート トンネルのエンドポイントによって保護されているネットワークとホストのルーティング プロセスに、スタティック ルートが自動的に挿入されるようにすることができます。
- [Security Association Lifetime]：セキュリティ アソシエーション（SA）の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。
  - [Time]：時（hh）、分（mm）、および秒（ss）単位で SA のライフタイムを指定します。
  - [Traffic Volume]：キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロード データのキロバイト数を入力します。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。

Crypto Map Entry for Static Peer Address

このウィンドウでは、ピアの IP アドレスがスタティック アドレスである場合に、接続プロファイルの暗号パラメータを指定します。

フィールド

- [Priority]：一意のプライオリティ（1 ～ 65,543、1 が最高のプライオリティ）。IKE ネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモート ピアに送信します。リモート ピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。
- [Perfect Forward Secrecy]：特定の IPSec SA のキーが他のシークレット（他のキーなど）から導出されたものでないことを保証します。PFS により、攻撃者がキーを突破できたとしても、そのキーから他のキーを導出できないようにします。PFS をイネーブルにすると、Diffie-Hellman Group リストがアクティブになります。
  - [Diffie-Hellman Group]：2 つの IPSec ピアが、相互に共有秘密情報を転送することなく共有秘密情報を導出するために使用する ID。Group 1（768 ビット）、Group 2（1024 ビット）、および Group 5（1536 ビット）の中から選択します。
- [Enable NAT-T]：このポリシーの NAT Traversal（NAT-T）をイネーブルにします。これにより IPSec ピアは、NAT デバイスを介してリモート アクセスと LAN-to-LAN の両方の接続を確立できます。
- [Enable Reverse Route Injection]：リモート トンネルのエンドポイントによって保護されているネットワークとホストのルーティング プロセスに、スタティック ルートが自動的に挿入されるようにすることができます。
- [Security Association Lifetime]：セキュリティ アソシエーション（SA）の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。
  - [Time]：時（hh）、分（mm）、および秒（ss）単位で SA のライフタイムを指定します。

  - [Traffic Volume]：キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロード データのキロバイト数を入力します。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。

- [Static Crypto Map Entry Parameters]：ピア IP アドレスが [Static] に指定されている場合に、次の追加パラメータを指定します。
  - [Connection Type]：許可されるネゴシエーションを、bidirectional、answer-only、または originate-only として指定します。
  - [Send ID Cert. Chain]：証明書チェーン全体の送信をイネーブルにします。
  - [IKE Negotiation Mode]：SA、Main、または Aggressive の中から、セットアップでキー情報を交換するときのモードを設定します。ネゴシエーションの発信側が使用するモードも設定されます。応答側は自動ネゴシエーションします。Aggressive モードは高速で、使用するパケットと交換回数を少なくすることができますが、通信パーティの ID は保護されません。Main モードは低速で、パケットと交換回数が多くなりますが、通信パーティの ID を保護します。このモードはより安全性が高く、デフォルトで選択されています。Aggressive を選択すると、Diffie-Hellman Group リストがアクティブになります。
  - [Diffie-Hellman Group]：2 つの IPSec ピアが、相互に共有秘密情報を転送することなく共有秘密情報を導出するために使用する ID。Group 1（768 ビット）、Group 2（1024 ビット）、および Group 5（1536 ビット）の中から選択します。

CA 証明書の管理

[IKE Peer Authentication] の下にある [Manage] をクリックすると、[Manage CA Certificates] ウィンドウが開きます。このウィンドウを使用して、IKE ピア認証で使用可能な CA 証明書のリストのエントリを表示、追加、編集、および削除します。

[Manage CA Certificates] ウィンドウには、証明書の発行先、証明書の発行元、証明書の有効期限、および利用データなど、現在設定されている証明書の情報が一覧表示されます。

フィールド

- [Add or Edit]：[Install Certificate] ウィンドウまたは [Edit Certificate] ウィンドウが開きます。これらのウィンドウでは、証明書の情報を指定し、証明書をインストールできます
- [Show Details]：テーブルで選択する証明書の詳細情報を表示します。
- [Delete]：選択した証明書をテーブルから削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Install Certificate

このウィンドウを使用して、新しい CA 証明書をインストールします。次のいずれかの方法で証明書を取得できます。

- 証明書ファイルを参照してファイルからインストールします。
- 事前取得済みの PEM 形式の証明書テキストをこのウィンドウのボックスに貼り付けます。
- [Use SCEP] : Simple Certificate Enrollment Protocol（SCEP）の使用を指定します。証明書サービスのアドオンは、Windows Server 2003 ファミリで実行されます。SCEP プロトコルのサポートを提供し、これによりシスコのルータおよび他の中間ネットワーク デバイスは、証明書を取得できます。
  - [SCEP URL: http://] : SCEP 情報のダウンロード元の URL を指定します。
  - [Retry Period] : SCEP クエリー間の必須経過時間を分数で指定します。
  - [Retry Count] : リトライの最大許容回数を指定します。
- [More Options] : [Configure Options for CA Certificate] ウィンドウが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Configure Options for CA Certificate

このウィンドウを使用して、この IPSec リモート アクセス接続の CA 証明書の取得に関する詳細を指定します。このウィンドウに含まれるタブは、[Revocation Check]、[CRL Retrieval Policy]、[CRL Retrieval Method]、[OCSP Rules]、および [Advanced] です。

[Revocation Check] タブ

このタブを使用して、CA 証明書の失効チェックについての情報を指定します。

フィールド

- オプション ボタンにより、失効状態について証明書をチェックするかどうかを指定します。オプション ボタンの値は次のとおりです。
  - Do not check certificates for revocation
  - Check Certificates for revocation
- [Revocation Methods area] : 失効チェックで使用する方法（CRL または OCSP）、およびそれらの方法を使用する順序を指定できます。いずれか一方または両方の方法を選択できます。

[Add/Edit Remote Access Connections] > [Advanced] > [General]

このウィンドウを使用して、AAA サーバに渡す前にユーザ名からレルムとグループを除去するかどうかを指定し、パスワード管理パラメータを指定します。

フィールド

- [Strip the realm from the username before passing it on to the AAA server]：レルム（管理ドメイン）をユーザ名から除去してから、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のレルム修飾子を削除するには、[Strip Realm] チェックボックスをオンにします。レルム名は、AAA（認証、許可、アカウンティング）のユーザ名に追加できます。レルムに対して有効なデリミタは @ だけです。形式は、username@realm です。たとえば、JaneDoe@it.cisco.com です。この [Strip Realm] チェックボックスをオンにすると、認証はユーザ名のみに基づいて行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。

（注）　レルムとグループは、両方をユーザ名に追加できます。その場合、セキュリティ アプライアンスは、グループと AAA 機能用のレルムに対して設定されたパラメータを使用します。このオプションのフォーマットは *JaneDoe@it.cisco.com#VPNGroup* のように、*ユーザ名[@realm][<# または !> グループ]* という形式を取ります。このオプションを選択した場合は、グループ デリミタとして # または ! を使用する必要があります。これは、@ がレルム デリミタとしても使用されている場合には、セキュリティ アプライアンスが @ をグループ デリミタと解釈できないためです。

Kerberos レルムは特殊事例です。Kerberos レルムの命名規則として、Kerberos レルムと関連付けられている DNS ドメイン名を大文字で表記します。たとえば、ユーザが it.cisco.com ドメインに存在する場合には、Kerberos レルムを IT.CISCO.COM と表記します。

- [Strip the group from the username before passing it on to the AAA server]: グループ名をユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のグループ名を削除するには、[Strip Group] チェックボックスをオンにします。このオプションは、[Enable Group Lookup] ボックスをオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザ名に追加し、Group Lookup をイネーブルにすると、セキュリティ アプライアンスは、デリミタの左側にある文字をすべてユーザ名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループ デリミタは @、#、および ! で、@ が Group Lookup のデフォルトです。*JaneDoe@VPNGroup*、*JaneDoe#VPNGroup* や *JaneDoe!VPNGroup* のように、*ユーザ名<デリミタ>グループ*の形式でグループをユーザ名に追加します。
- [Password Management]：AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。
  - [Override account-disabled indication from AAA server]：AAA サーバからの account-disabled インジケータを上書きします。

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

  - [Enable notification upon password expiration to allow user to change password]：このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時にユーザに通知するか、またはパスワードが期限切れになる当日にユーザに通知するかを選択できます。デ

フォルトでは、パスワードが期限切れになるより 14 日前にユーザへの通知を開始し、以後、ユーザがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ～ 180 日です。

（注）　この処理によってパスワードの期限が切れるまでの日数が変わるのではなく、通知がイネーブルになるだけであるという点に注意してください。このオプションを選択する場合は、日数も指定する必要があります。

どちらの場合でも、変更されずにパスワードが期限切れになると、セキュリティ アプライアンスはパスワードを変更する機会をユーザに提供します。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS または LDAP 認証が設定されていない場合、セキュリティ アプライアンスではこのコマンドが無視されます。

この機能では、MS-CHAPv2 を使用する必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

クライアント アドレス指定の設定

クライアント IP アドレスの割り当てポリシーを指定し、アドレス プールをすべての IPsec 接続および SSL VPN 接続に割り当てるには、[Config] > [Remote Access VPN] > [Network (Client) Access] > [IPsec or SSL VPN Connections] > [Add or Edit] > [Advanced] > [Client Addressing] を選択します。[Add IPSec Remote Access Connection] または [Add SSL VPN Access Connection] が開きます。これらのウィンドウを使用して、アドレス プールを追加し、それらをインターフェイスに割り当て、それらを表示、編集、または削除します。ウィンドウ下部のテーブルには、設定されているインターフェイス固有のアドレス プールの一覧が表示されます。

このウィンドウおよびその従属ウィンドウのフィールドについては、以降の各項を参照してください。アドレス プールのコンフィギュレーションおよびそのインターフェイスへの割り当て状態を表示または変更するには、次の手順を実行します。

- アドレス プールのコンフィギュレーションを表示または変更するには、[Add IPSec Remote Access Connection] または [Add SSL VPN Access Connection] ウィンドウで、[Add] または [Edit] をクリックします。[Assign Address Pools to Interface] ウィンドウが開きます。このウィンドウでは、セキュリティ アプライアンスで設定されたインターフェイスに IP アドレス プールを割り当てることができます。[Select] をクリックします。[Select Address Pools] ウィンドウが開きます。このウィンドウを使用して、アドレス プールのコンフィギュレーションを表示します。アドレス プールのコンフィギュレーションを変更するには、次の手順を実行します。
  - セキュリティ アプライアンス にアドレス プールを追加するには、[Add] を選択します。[Add IP Pool] ダイアログボックスが開きます。

- セキュリティ アプライアンス のアドレス プールのコンフィギュレーションを変更するには、[Edit] を選択します。プール内のアドレスが使用されていない場合には、[Edit IP Pool] ダイアログボックスが開きます。

（注）　使用中の場合はアドレス プールを変更できません。[Edit] をクリックしたときにアドレス プールが使用中であった場合、ASDM は、エラー メッセージとともに、プール内のそのアドレスを使用している接続名およびユーザ名の一覧を表示します。

- セキュリティ アプライアンス のアドレス プールを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

（注）　使用中の場合はアドレス プールを削除できません。[Delete] をクリックしたときにアドレス プールが使用中であった場合、ASDM は、エラー メッセージとともに、プール内のそのアドレスを使用している接続名の一覧を表示します。

- アドレス プールをインターフェイスに割り当てるには、[Add IPSec Remote Access Connection] または [Add SSL VPN Access Connection] ウィンドウで [Add] をクリックします。[Assign Address Pools to Interface] ウィンドウが開きます。アドレス プールを割り当てるインターフェイスを選択します。[Address Pools] フィールドの横にある [Select] をクリックします。[Select Address Pools] ウィンドウが開きます。インターフェイスに割り当てる個々の未割り当てプールをダブルクリックするか、または個々の未割り当てプールを選択して [Assign] をクリックします。隣のフィールドにプール割り当ての一覧が表示されます。[OK] をクリックして、これらのアドレス プールの名前を [Address Pools] フィールドに取り込み、もう一度 [OK] をクリックして割り当てのコンフィギュレーションを完了します。
- インターフェイスに割り当てられているアドレス プールを変更するには、そのインターフェイスをダブルクリックするか、[Add IPSec Remote Access Connection] または [Add SSL VPN Access Connection] ウィンドウでインターフェイスを選択して、[Edit] をクリックします。[Assign Address Pools to Interface] ウィンドウが開きます。アドレス プールを削除するには、各プール名をダブルクリックし、キーボードの [Delete] キーを押します。インターフェイスにその他のフィールドを割り当てる場合は、[Address Pools] フィールドの横にある [Select] をクリックします。[Select Address Pools] ウィンドウが開きます。[Assign] フィールドには、インターフェイスに割り当てられているアドレス プール名が表示されます。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。[Assign] フィールドのプール割り当て一覧が更新されます。[OK] をクリックして、これらのアドレス プールの名前で [Address Pools] フィールドを確認し、もう一度 [OK] をクリックして割り当てのコンフィギュレーションを完了します。
- [Add IPSec Remote Access Connection] または [Add SSL VPN Access Connection] ウィンドウからエントリを削除するには、エントリを選択して [Delete] をクリックします。

[Add IPSec Remote Access Connection] ウィンドウ、[Add SSL VPN Access Connection] ウィンドウ、およびそれらの従属ウィンドウは同一です。次の各項では、これらのウィンドウのフィールドについて説明し、値の割り当て方法を示します。

- [Add IPSec Remote Access Connection] および [Add SSL VPN Access Connection]
- Assign Address Pools to Interface
- Select Address Pools
- Add or Edit IP Pool
- Add or Edit IP Pool

[Add IPSec Remote Access Connection] および [Add SSL VPN Access Connection]

[Add IPSec Remote Access Connection] および [Add SSL VPN Access Connection] ウィンドウにアクセスするには、[Config] > [Remote Access VPN] > [Network (Client) Access] > [IPsec or SSL VPN Connections] > [Add or Edit] > [Advanced] > [Client Addressing] を選択します。

フィールド

次の説明に従って、このウィンドウのフィールドに値を割り当てます。

- [Global Client Address Assignment Policy] : すべての IPSec 接続と SSL VPN Client 接続（AnyConnect クライアント接続を含む）に影響するポリシーを設定します。セキュリティ アプライアンスは、アドレスを見つけるまで、選択されたソースを順番に使用します。
  - [Use authentication server] : クライアント アドレスのソースとして、セキュリティ アプライアンスが認証サーバの使用を試みるように指定します。
  - [Use DHCP] : クライアント アドレスのソースとして、セキュリティ アプライアンスが DHCP の使用を試みるように指定します。
  - [Use address pool] : クライアント アドレスのソースとして、セキュリティ アプライアンスがアドレス プールの使用を試みるように指定します。
- [Interface-Specific Address Pools] : 設定されているインターフェイス固有のアドレス プールの一覧を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Assign Address Pools to Interface

[Assign Address Pools to Interface] ウィンドウを使用して、インターフェイスを選択し、そのインターフェイスに 1 つ以上のアドレス プールを割り当てます。このウィンドウにアクセスするには、[Config] > [Remote Access VPN] > [Network (Client) Access] > [IPsec or SSL VPN Connections] > [Add or Edit] > [Advanced] > [Client Addressing] > [Add or Edit] を選択します。

フィールド

次の説明に従って、このウィンドウのフィールドに値を割り当てます。

- [Interface] : アドレス プールの割り当て先インターフェイスを選択します。デフォルトは DMZ です。
- [Address Pools] : 指定したインターフェイスに割り当てるアドレス プールを指定します。
- [Select] : [Select Address Pools] ダイアログボックスが開きます。このダイアログボックスでは、このインターフェイスに割り当てるアドレス プールを 1 つ以上選択できます。選択内容は、[Assign Address Pools to Interface] ダイアログボックスの [Address Pools] フィールドに表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Select Address Pools

[Select Address Pools] ウィンドウには、クライアント アドレスの割り当てで選択可能なプール名、開始アドレスと終了アドレス、およびアドレス プールのサブネットマスクが表示され、リストのエントリを追加、編集、削除できます。このウィンドウにアクセスするには、[Config] > [Remote Access VPN] > [Network (Client) Access] > [IPsec or SSL VPN Connections] > [Add or Edit] > [Advanced] > [Client Addressing] > [Add or Edit] > [Select] を選択します。

フィールド

次の説明に従って、このウィンドウのフィールドに値を割り当てます。

- [Add] : [Add IP Pool] ウィンドウが開きます。このウィンドウでは、新しい IP アドレス プールを設定できます。
- [Edit] : [Edit IP Pool] ウィンドウが開きます。このウィンドウでは、選択した IP アドレス プールを変更できます。
- [Delete] : 選択したアドレス プールを削除します。確認されず、やり直しもできません。
- [Assign] : インターフェイスに割り当てられているアドレス プール名を表示します。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。[Assign] フィールドのプール割り当て一覧が更新されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add or Edit IP Pool

[Add or Edit IP Pool] ウィンドウでは、クライアント アドレス割り当てで使用する IP アドレスの範囲を指定または変更できます。このウィンドウにアクセスするには、[Config] > [Remote Access VPN] > [Network (Client) Access] > [IPsec or SSL VPN Connections] > [Add or Edit] > [Advanced] > [Client Addressing] > [Add or Edit] > [Select] > [Add or Edit] を選択します。

フィールド

次の説明に従って、このウィンドウのフィールドに値を割り当てます。

- [Name]：IP アドレス プールに割り当てられている名前を指定します。
- [Starting IP Address]：プールの最初の IP アドレスを指定します。
- [Ending IP Address]：プールの最後の IP アドレスを指定します。
- [Subnet Mask]：プール内のアドレスに適用するサブネット マスクを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Tunnel Group] > [General] タブ > [Authentication]

このダイアログボックスは、IPSec on Remote Access および Site-to-Site トンネル グループの場合に表示されます。このダイアログボックスでの設定は、セキュリティ アプライアンス全体のトンネル グループにグローバルに適用されます。インターフェイスごとに認証サーバ グループを設定するには、[Advanced] をクリックします。このダイアログボックスでは、次の属性を設定できます。

- [Authentication Server Group]：LOCAL グループ（デフォルト）などの利用可能な認証サーバ グループを一覧表示します。None も選択可能です。None または Local 以外を選択すると、[Use LOCAL if Server Group Fails] チェックボックスが利用できるようになります。インターフェイスごとに認証サーバ グループを設定するには、[Advanced] をクリックします。
- [Use LOCAL if Server Group fails]：Authentication Server Group 属性によって指定されたグループに障害が発生した場合の LOCAL データベースへのフォールバックをイネーブルまたはディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit SSL VPN Connection > General > Authorization

このダイアログボックスでの設定は、セキュリティ アプライアンス全体の接続（トンネル グループ）にグローバルに適用されます。このダイアログボックスでは、次の属性を設定できます。

- [Authorization Server Group]：LOCAL グループを含む、利用可能な許可サーバ グループを一覧表示します。None（デフォルト）も選択可能です。None 以外を選択すると、[Users must exist in authorization database to connect] チェックボックスが利用できるようになります。

- [Users must exist in authorization database to connect]：セキュリティ アプライアンスに対し、許可データベース内のユーザだけに接続を許可するように命令します。デフォルトでは、この機能はディセーブルになっています。許可サーバでこの機能を使用するように設定しておく必要があります。
- [Interface-Specific Authorization Server Groups]：（任意）インターフェイスごとに許可サーバ グループを設定できます。インターフェイスに固有の許可サーバ グループは、グローバル サーバ グループよりも優先されます。インターフェイスに固有の許可を明示的に設定していない場合には、グループ レベルでだけ許可が実行されます。
  - [Interface]：許可を実行するインターフェイスを選択します。標準のインターフェイスは、outside（デフォルト）、inside、および DMZ です。他のインターフェイスを設定した場合には、そのインターフェイスもリストに表示されます。
  - [Server Group]：LOCAL グループを含む、先に設定した利用可能な許可サーバ グループを選択します。サーバ グループは、複数のインターフェイスと関連付けることができます。
  - [Add]：[Add] をクリックすると、インターフェイスまたはサーバ グループ設定がテーブルに追加され、利用可能なリストからインターフェイスが削除されます。
  - [Remove]：[Remove] をクリックすると、インターフェイスまたはサーバ グループがテーブルから削除され、利用可能なリストにインターフェイスが戻ります。
- [Authorization Settings]：セキュリティ アプライアンスが許可のために認識するユーザ名の値を設定できるようにします。この名前は、デジタル証明書を使用して認証し、LDAP または RADIUS 許可を必要とするユーザに適用されます。
  - [Use entire DN as username]：認定者名（DN）全体をユーザ名として使用することを許可します。
  - [Specify individual DN fields as the username]：個々の DN フィールドをユーザ名として使用することをイネーブルにします。
  - [Primary DN Field]：選択内容の DN フィールド識別子すべてを一覧表示します。

DN フィールド	定義
Country（C）	2 文字の国名略記。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name（CN）	人やシステム、その他のエンティティの名前。これは、ID 階層の最下位（最も固有性の高い）レベルです。
DN Qualifier（DNQ）	特定の DN 属性。
E-mail Address（EA）	証明書を所有する人、システム、またはエンティティの電子メール アドレス。
Generational Qualifier（GENQ）	Jr.、Sr.、III などの世代修飾子。
Given Name（GN）	証明書所有者の名。
Initials（I）	証明書所有者の姓と名の最初の文字。
Locality（L）	組織が所在する市または町。
Name（N）	証明書所有者の名。
Organization（O）	会社、施設、機関、協会、その他のエンティティの名前。
Organizational Unit（OU）	組織内のサブグループ。
Serial Number（SER）	証明書のシリアル番号。
Surname（SN）	証明書所有者の姓。

DN フィールド	定義
State/Province（S/P）	組織が所在する州や県。
Title（T）	博士など、証明書の所有者の肩書。
User ID（UID）	証明書の所有者の識別番号。
User Principal Name（UPN）	スマート カードによる証明書認証で使用。

  - [Secondary DN Field]：選択内容の DN フィールド識別子のすべて（上記の表を参照）を一覧表示し、選択していない場合には None オプションを追加します。

[Add/Edit SSL VPN Connections] > [Advanced] > [Accounting]

このダイアログボックスでの設定は、セキュリティ アプライアンス全体の接続（トンネル グループ）にグローバルに適用されます。このダイアログボックスでは、次の属性を設定できます。

- [Accounting Server Group]：利用可能なアカウンティング サーバ グループを一覧表示します。None（デフォルト）も選択可能です。LOCAL はオプションではありません。
- [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Tunnel Group] > [General] > [Client Address Assignment]

アドレス割り当てに DHCP またはアドレス プールを使用するかどうかを指定するには、[Configuration] > [VPN] > [I P Address Management] > [Assignment] に移動します。[Add or Edit Tunnel Group] ウィンドウ > [General] > [Client Address Assignment] ダイアログボックスでは、次の Client Address Assignment 属性を設定できます。

- [DHCP Servers]：使用する DHCP サーバを指定します。一度に最大 10 台のサーバを追加できます。
  - [IP Address]：DHCP サーバの IP アドレスを指定します。
  - [Add]：指定された DHCP サーバを、クライアント アドレス割り当て用のリストに追加します。
  - [Delete]：指定された DHCP サーバを、クライアント アドレス割り当て用のリストから削除します。確認されず、やり直しもできません。
- [Address Pools]：次のパラメータを使用して、最大 6 つのアドレス プールを指定できます。
  - [Available Pools]：選択可能な設定済みのアドレス プールを一覧表示します。
  - [Add]：選択したアドレス プールをクライアント アドレス割り当て用のリストに追加します。

- [Remove]：選択したアドレス プールを [Assigned Pools] リストから [Available Pools] リストに移動します。
- [Assigned Pools]：アドレス割り当て用に選択したアドレス プールを一覧表示します。

（注）　インターフェイスに固有のアドレス プールを設定するには、[Advanced] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Tunnel Group] > [General] > [Advanced]

[Add or Edit Tunnel Group] ウィンドウの [General] の [Advanced] ダイアログボックスでは、インターフェイスに固有の次の属性を設定できます。

- [Interface-Specific Authentication Server Groups]：インターフェイスとサーバ グループを認証用に設定できます。
  - [Interface]：選択可能なインターフェイスを一覧表示します。
  - [Server Group]：このインターフェイスで利用可能な認証サーバ グループを一覧表示します。
  - [Use LOCAL if server group fails]：サーバ グループに障害が発生した場合の LOCAL データベースへのフォールバックをイネーブルまたはディセーブルにします。
  - [Add]：選択した利用可能なインターフェイスと認証サーバ グループ間のアソシエーションを、割り当てられたリストに追加します。
  - [Remove]：選択したインターフェイスと認証サーバ グループのアソシエーションを、割り当てられたリストから利用可能なリストに移動します。
  - [Interface/Server Group/Use Fallback]：割り当てられたリストに追加した選択内容を表示します。
- [Interface-Specific Client IP Address Pools]：インターフェイスとクライアントの IP アドレス プールを指定できます。最大 6 個のプールを指定できます。
  - [Interface]：追加可能なインターフェイスを一覧表示します。
  - [Address Pool]：このインターフェイスと関連付けできるアドレス プールを一覧表示します。
  - [Add]：選択した利用可能なインターフェイスとクライアントの IP アドレス プール間のアソシエーションを、割り当てられたリストに追加します。
  - [Remove]：選択したインターフェイスまたはアドレス プールのアソシエーションを、割り当てられたリストから利用可能なリストに移動します。
  - [Interface/Address Pool]：割り当てられたリストに追加された選択内容を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Tunnel Group] > [IPSec for Remote Access] > [IPSec]

[IPSec for Remote Access] の [Add or Edit Tunnel Group] ウィンドウにある [IPSec] ダイアログボックスでは、IPSec に固有のトンネル グループ パラメータを設定または編集できます。

フィールド

- [Pre-shared Key]：トンネル グループの事前共有キーの値を指定できます。事前共有キーの最大長は 128 文字です。
- [Trustpoint Name]：トラストポイントが設定されている場合には、トラストポイント名を選択します。トラストポイントとは、認証局を表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。
- [Authentication Mode]：認証モードを、none、xauth、または hybrid の中から指定します。
  - [none]：認証モードを指定しません。
  - [xauth]：IKE 拡張認証モードを使用するように指定します。この認証モードは、TACACS+ または RADIUS を使用する IKE 内のユーザを認証する機能を提供します。
  - [hybrid]：ハイブリッド モードを使用するように指定します。この認証モードでは、セキュリティ アプライアンス認証にデジタル認証を使用でき、リモート VPN ユーザ認証に別のレガシー方式（RADIUS、TACACS+、SecurID など）を使用できます。このモードでは、インターネット キー交換（IKE）のフェーズ 1 が次の手順に分かれています。これらを合わせてハイブリッド認証と呼びます。

    1. セキュリティ アプライアンスでは、リモート VPN ユーザが標準公開キー技術で認証されます。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。
    2. 次に、拡張認証（xauth）交換でリモート VPN ユーザが認証されます。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注） 認証タイプをハイブリッドに設定する前に、認証サーバを設定し、事前共有キーを作成する必要があります。

- [IKE Peer ID Validation]：IKE ピア ID 確認要求を無視するか、必須とするか、あるいは証明書によってサポートされている場合にだけチェックするかを選択します。
- [Enable sending certificate chain]：証明書チェーン全体の送信をイネーブルまたはディセーブルにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
- [ISAKMP Keep Alive]：ISAKMP キープアライブ モニタリングをイネーブルにし、設定します。
  - [Disable Keep Alives]：ISAKMP キープアライブをイネーブルまたはディセーブルにします。

  - [Monitor Keep Alives] : ISAKMP キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
  - [Confidence Interval] : ISAKMP キープアライブの信頼間隔を指定します。これは、ピアがキープアライブ モニタリングを開始するまでにセキュリティ アプライアンスが許可するアイドル時間を表す秒数です。最小 10 秒、最大 300 秒です。リモート アクセス グループのデフォルトは 300 秒です。
  - [Retry Interval] : ISAKMP キープアライブのリトライ間の待機秒数を指定します。デフォルトは 2 秒です。
  - [Head end will never initiate keepalive monitoring] : 中央サイトのセキュリティ アプライアンスがキープアライブ モニタリングを開始しないように指定します。
- [Interface-Specific Authentication Mode] : 認証モードをインターフェイスごとに指定します。
  - [Interface] : インターフェイス名を選択できます。デフォルトのインターフェイスは inside と outside ですが、別のインターフェイス名を設定した場合には、その名前がリストに表示されます。
  - [Authentication Mode] : 認証モードを、上記の none、xauth、または hybrid の中から選択できます。
  - [Interface/Authentication Mode] テーブル : インターフェイス名と、選択されている関連認証モードを表示します。
  - [Add] : 選択したインターフェイスと認証モードのペアを [Interface/Authentication Modes] テーブルに追加します。
  - [Remove] : 選択したインターフェイスと認証モードのペアを [Interface/Authentication Modes] テーブルから削除します。
- [Client VPN Software Update Table] : クライアント タイプ、VPN クライアントのリビジョン、およびインストールされている各クライアント VPN ソフトウェア パッケージのイメージ URL を一覧表示します。クライアント タイプごとに、許可されるクライアント ソフトウェア リビジョンと、必要に応じて、ソフトウェア アップグレードをダウンロードする URL または IP アドレスを指定できます。クライアント アップデート メカニズム（[Client Update] ウィンドウに詳細説明があります）は、この情報を使用して、各 VPN クライアントが適切なリビジョン レベルで実行されているかどうか、適切であれば、通知メッセージとアップデート メカニズムを、旧式のソフトウェアを実行しているクライアントに提供するかどうかを判断します。
  - [Client Type] : VPN クライアント タイプを識別します。
  - [VPN Client Revisions] : 許可される VPN クライアントのリビジョン レベルを指定します。
  - [Image URL] : 適切な VPN クライアント ソフトウェア イメージをダウンロードできる URL または IP アドレスを指定します。Windows ベースの VPN クライアントの場合、URL は http:// または https:// という形式です。クライアント モードの ASA 5505 または VPN 3002 ハードウェア クライアントの場合、URL は tftp:// という形式です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Site-to-Site VPN のトンネル グループの追加および編集

[Add or Edit Tunnel Group] ダイアログボックスでは、この Site-to-Site 接続プロファイルのトンネル グループ パラメータを設定または編集できます。

フィールド

- [Certificate Settings]：次の証明書チェーンと IKE ピア検証の属性を設定します。
  - [Send certificate chain]：証明書チェーン全体の送信をイネーブルまたはディセーブルにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
  - [IKE Peer ID Validation]：IKE ピア ID 確認要求を無視するか、必須とするか、あるいは証明書によってサポートされている場合にだけチェックするかを選択します。
- [IKE Keep Alive]：IKE（ISAKMP）キープアライブ モニタリングをイネーブルにして設定します。
  - [Disable Keep Alives]：IKE キープアライブをイネーブルまたはディセーブルにします。
  - [Monitor Keep Alives]：IKE キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
  - [Confidence Interval]：IKE キープアライブの信頼間隔を指定します。これは、ピアがキープアライブ モニタリングを開始するまでにセキュリティ アプライアンスが許可するアイドル時間を表す秒数です。最小 10 秒、最大 300 秒です。リモート アクセス グループのデフォルトは 300 秒です。
  - [Retry Interval]：IKE キープアライブのリトライ間の待機秒数を指定します。デフォルトは 2 秒です。
  - [Head end will never initiate keepalive monitoring]：中央サイトのセキュリティ アプライアンスがキープアライブ モニタリングを開始しないように指定します。
- [Default Group Policy]：次のグループ ポリシーの属性を指定します。
  - [Group Policy]：デフォルトのグループ ポリシーとして使用するグループ ポリシーを選択します。デフォルト値は DfltGrpPolicy です。
  - [Manage]：[Configure Group Policies] ダイアログボックスが開きます。
  - [IPSec Protocol]：この接続プロファイルでの IPSec プロトコルの使用をイネーブルまたはディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Tunnel Group] > [PPP]

IPSec リモート アクセス トンネル グループの [Add or Edit Tunnel Group] ウィンドウの [PPP] ダイアログボックスでは、PPP 接続で許可される認証プロトコルを設定または編集できます。このダイアログボックスは、IPSec リモートアクセス トンネルグループ*にだけ*適用されます。

フィールド

- [CHAP] : PPP 接続で CHAP プロトコルの使用をイネーブルにします。
- [MS-CHAP-V1] : PPP 接続で MS-CHAP-V1 プロトコルの使用をイネーブルにします。
- [MS-CHAP-V2] : PPP 接続で MS-CHAP-V2 プロトコルの使用をイネーブルにします。
- [PAP] : PPP 接続で PAP プロトコルの使用をイネーブルにします。
- [EAP-PROXY] : PPP 接続で EAP-PROXY プロトコルの使用をイネーブルにします。EAP は、Extensible Authentication protocol（拡張認証プロトコル）を意味します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Tunnel Group] > [IPSec for LAN to LAN Access] > [General] > [Basic]

Site-to-Site リモート アクセスの [Add or Edit Tunnel Group] ウィンドウにある、[General] タブの [Basic] ダイアログボックスでは、追加するトンネル グループの名前を指定し（Add 機能だけ）、グループ ポリシーを選択できます。

[Edit Tunnel Group] ウィンドウの [General] ダイアログボックスには、変更するトンネル グループの名前とタイプが表示されます。

フィールド

- [Name] : このトンネル グループに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。
- [Type] :（*表示専用*）追加または編集するトンネル グループのタイプを表示します。このフィールドの内容は、前のウィンドウでの選択内容によって異なります。
- [Group Policy] : 現在設定されているグループ ポリシーを一覧表示します。デフォルト値は、デフォルト グループ ポリシーである DfltGrpPolicy です。

- [Strip the realm (administrative domain) from the username before passing it on to the AAA server]: レルムをユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のレルム修飾子を削除するには、[Strip Realm] チェックボックスをオンにします。レルム名は、AAA（認証、許可、アカウンティング）のユーザ名に追加できます。レルムに対して有効なデリミタは @ だけです。形式は、username@realm です。たとえば、JaneDoe@it.cisco.com です。この [Strip Realm] チェックボックスをオンにすると、認証はユーザ名のみに基づいて行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。

（注）　レルムとグループは、両方をユーザ名に追加できます。その場合、セキュリティ アプライアンスは、グループと AAA 機能用のレルムに対して設定されたパラメータを使用します。このオプションのフォーマットは *JaneDoe@it.cisco.com#VPNGroup* のように、*ユーザ名[@realm][<# または !> グループ]* という形式を取ります。このオプションを選択した場合は、グループ デリミタとして # または ! を使用する必要があります。これは、@ がレルム デリミタとしても使用されている場合には、セキュリティ アプライアンスが @ をグループ デリミタと解釈できないためです。

Kerberos レルムは特殊事例です。Kerberos レルムの命名規則として、Kerberos レルムと関連付けられている DNS ドメイン名を大文字で表記します。たとえば、ユーザが it.cisco.com ドメインに存在する場合には、Kerberos レルムを IT.CISCO.COM と表記します。

- [Strip the group from the username before passing it on to the AAA server]: グループ名をユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のグループ名を削除するには、[Strip Group] チェックボックスをオンにします。このオプションは、[Enable Group Lookup] ボックスをオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザ名に追加し、Group Lookup をイネーブルにすると、セキュリティ アプライアンスは、デリミタの左側にある文字をすべてユーザ名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループ デリミタは @、#、および ! で、@ が Group Lookup のデフォルトです。*JaneDoe@VPNGroup*、*JaneDoe#VPNGroup* や *JaneDoe!VPNGroup* のように、*ユーザ名<デリミタ>グループ*の形式でグループをユーザ名に追加します。
- [Password Management]：AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。
  - [Override account-disabled indication from AAA server]：AAA サーバからの account-disabled インジケータを上書きします。

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

  - [Enable notification upon password expiration to allow user to change password]：このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。[Enable notification prior to expiration] チェックボックスをオンにしないと、ユーザは、パスワードの期限が切れた後で通知を受信します。
  - [Enable notification prior to expiration]：このオプションをオンにすると、セキュリティ アプライアンスは、リモート ユーザのログイン時に、現在のパスワードの期限切れが迫っているか、期限が切れていることを通知し、パスワードを変更する機会をユーザに提供します。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS または LDAP 認証が設定されていない場合、セキュリティ アプライアンスではこのコマンドが無視されます。

この処理によってパスワードの期限が切れるまでの日数が変わるわけではなく、通知がイネーブルになるということに注意してください。このチェックボックスをオンにしたら、日数も指定する必要があります。

– [Notify...days prior to expiration]：現在のパスワードの期限切れが迫っていることをユーザに通知する日を、期限切れになるまでの日数で指定します。範囲は 1 ～ 180 日です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Tunnel Group] > [IPSec for LAN to LAN Access] > [IPSec]

Site-to-Site アクセス用 IPSec の [Add or Edit Tunnel Group] ウィンドウの [IPSec] ダイアログボックスでは、IPSec Site-to-Site に固有のトンネル グループ パラメータを設定または編集できます。

フィールド

- [Name]：このトンネル グループに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。
- [Type]：（*表示専用*）追加または編集するトンネル グループのタイプを表示します。このフィールドの内容は、前のウィンドウでの選択内容によって異なります。
- [Pre-shared Key]：トンネル グループの事前共有キーの値を指定できます。事前共有キーの最大長は 128 文字です。
- [Trustpoint Name]：トラストポイントが設定されている場合には、トラストポイント名を選択します。トラストポイントとは、認証局を表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。
- [Authentication Mode]：認証モードを、none、xauth、または hybrid の中から指定します。
  – [none]：認証モードを指定しません。
  – [xauth]：IKE 拡張認証モードを使用するように指定します。この認証モードは、TACACS+ または RADIUS を使用する IKE 内のユーザを認証する機能を提供します。
  – [hybrid]：ハイブリッド モードを使用するように指定します。この認証モードでは、セキュリティ アプライアンス認証にデジタル認証を使用でき、リモート VPN ユーザ認証に別のレガシー方式（RADIUS、TACACS+、SecurID など）を使用できます。このモードでは、インターネット キー交換（IKE）のフェーズ 1 が次の手順に分かれています。これらを合わせてハイブリッド認証と呼びます。
  1. セキュリティ アプライアンスでは、リモート VPN ユーザが標準公開キー技術で認証されます。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。
  2. 次に、拡張認証（xauth）交換でリモート VPN ユーザが認証されます。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注）　認証タイプをハイブリッドに設定する前に、認証サーバを設定し、事前共有キーを作成する必要があります。

- [IKE Peer ID Validation]：IKE ピア ID 確認要求を無視するか、必須とするか、あるいは証明書によってサポートされている場合にだけチェックするかを選択します。
- [Enable sending certificate chain]：証明書チェーン全体の送信をイネーブルまたはディセーブルにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
- [ISAKMP Keep Alive]：ISAKMP キープアライブ モニタリングをイネーブルにし、設定します。
  - [Disable Keep Alives]：ISAKMP キープアライブをイネーブルまたはディセーブルにします。
  - [Monitor Keep Alives]：ISAKMP キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
  - [Confidence Interval]：ISAKMP キープアライブの信頼間隔を指定します。これは、ピアがキープアライブ モニタリングを開始するまでにセキュリティ アプライアンスが許可するアイドル時間を表す秒数です。最小 10 秒、最大 300 秒です。リモート アクセス グループのデフォルトは 300 秒です。
  - [Retry Interval]：ISAKMP キープアライブのリトライ間の待機秒数を指定します。デフォルトは 2 秒です。
  - [Head end will never initiate keepalive monitoring]：中央サイトのセキュリティ アプライアンスがキープアライブ モニタリングを開始しないように指定します。
- [Interface-Specific Authentication Mode]：認証モードをインターフェイスごとに指定します。
  - [Interface]：インターフェイス名を選択できます。デフォルトのインターフェイスは inside と outside ですが、別のインターフェイス名を設定した場合には、その名前がリストに表示されます。
  - [Authentication Mode]：認証モードを、上記の none、xauth、または hybrid の中から選択できます。
  - [Interface/Authentication Mode] テーブル：インターフェイス名と、選択されている関連認証モードを表示します。
  - [Add]：選択したインターフェイスと認証モードのペアを [Interface/Authentication Modes] テーブルに追加します。
  - [Remove]：選択したインターフェイスと認証モードのペアを [Interface/Authentication Modes] テーブルから削除します。
- [Client VPN Software Update Table]：クライアント タイプ、VPN クライアントのリビジョン、およびインストールされている各クライアント VPN ソフトウェア パッケージのイメージ URL を一覧表示します。クライアント タイプごとに、許可されるクライアント ソフトウェア リビジョンと、必要に応じて、ソフトウェア アップグレードをダウンロードする URL または IP アドレスを指定できます。クライアント アップデート メカニズム（[Client Update] ウィンドウに詳細説明があります）は、この情報を使用して、各 VPN クライアントが適切なリビジョン レベルで実行されているかどうか、適切であれば、通知メッセージとアップデート メカニズムを、旧式のソフトウェアを実行しているクライアントに提供するかどうかを判断します。
  - [Client Type]：VPN クライアント タイプを識別します。
  - [VPN Client Revisions]：許可される VPN クライアントのリビジョン レベルを指定します。

– [Image URL]：適切な VPN クライアント ソフトウェア イメージをダウンロードできる URL または IP アドレスを指定します。Windows ベースの VPN クライアントの場合、URL は http:// または https:// という形式です。クライアント モードの ASA 5505 または VPN 3002 ハードウェア クライアントの場合、URL は tftp:// という形式です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Tunnel Group] > [Clientless SSL VPN Access] > [General] > [Basic]

[Add or Edit] ペインの [General] タブの [Basic] ダイアログボックスでは、追加するトンネル グループの名前の指定、グループ ポリシーの選択、およびパスワード管理の設定を行うことができます。

[Edit Tunnel Group] ウィンドウの [General] ダイアログボックスには、選択したトンネル グループの名前とタイプが表示されます。その他の機能は、[Add Tunnel Group] ウィンドウと同じです。

フィールド

- [Name]：このトンネル グループに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。
- [Type]：追加または削除するトンネル グループのタイプを表示します。Edit の場合、このフィールドは表示専用で、その内容は、[Add] ウィンドウでの選択内容によって異なります。
- [Group Policy]：現在設定されているグループ ポリシーを一覧表示します。デフォルト値は、デフォルト グループ ポリシーである DfltGrpPolicy です。
- [Strip the realm]：クライアントレス SSL VPN では使用できません。
- [Strip the group]：クライアントレス SSL VPN では使用できません。
- [Password Management]：AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。
  – [Override account-disabled indication from AAA server]：AAA サーバからの account-disabled インジケータを上書きします。

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

  – [Enable notification upon password expiration to allow user to change password]：このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。[Enable notification prior to expiration] チェックボックスをオンにしないと、ユーザは、パスワードの期限が切れた後で通知を受信します。
  – [Enable notification prior to expiration]：このオプションをオンにすると、セキュリティ アプライアンスは、リモート ユーザのログイン時に、現在のパスワードの期限切れが迫っているか、期限が切れていることを通知し、パスワードを変更する機会をユーザに提供します。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けるこ

とができます。このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS または LDAP 認証が設定されていない場合、セキュリティ アプライアンスではこのコマンドが無視されます。

この処理によってパスワードの期限が切れるまでの日数が変わるわけではなく、通知がイネーブルになるということに注意してください。このチェックボックスをオンにしたら、日数も指定する必要があります。

– [Notify...days prior to expiration]：現在のパスワードの期限切れが迫っていることをユーザに通知する日を、期限切れになるまでの日数で指定します。範囲は 1 ～ 180 日です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[Add/Edit Tunnel Group] > [Clientless SSL VPN] > [Basic]

クライアントレス SSL VPN の [Add/Edit Tunnel Group General Tab] ダイアログボックスの属性は、IPSec リモート アクセスの [Add/Edit Tunnel Group General] ダイアログボックスの属性と同じです。次の説明は、[Clientless SSL VPN] ダイアログボックスに表示されるフィールドに適用されます。

フィールド

[Basic] ダイアログボックスでは、クライアントレス SSL VPN の次の属性を設定できます。

- [Authentication]：実行する認証のタイプを、[AAA]、[Certificate]、または [Both] の中から指定します。デフォルト値は [AAA] です。
- [DNS Group]：接続プロファイルで使用する DNS サーバを指定します。デフォルト値は DefaultDNS です。
- [CSD Failure group policy]：この属性は、Cisco Secure Desktop がインストールされているセキュリティ アプライアンスでのみ有効です。Cisco Secure Desktop Manager を使用して VPN 機能ポリシーを次のいずれかのオプションに設定すると、セキュリティ アプライアンスがこの属性を使用して、アクセス権をリモート CSD クライアントに制限します。
  – 「Use Failure Group-Policy」。
  – 「Use Success Group-Policy, if criteria match」、および条件が一致しない。

  この属性は、適用される失敗グループ ポリシーの名前を指定します。グループ ポリシーを選択して、アクセス権限を、デフォルト グループ ポリシーに関連付けられているアクセス権限と区別します。デフォルト値は DfltGrpPolicy です。

（注） VPN 機能ポリシーを「Always use Success Group-Policy」に設定している場合、セキュリティ アプライアンスではこの属性を使用しません。

詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administration Guide*』を参照してください。

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Configuring Internal Group Policy IPSec Client Attributes

このウィンドウを使用して、AAA サーバに渡す前にユーザ名からレルムとグループを除去するかどうかを指定し、パスワード管理オプションを指定します。

フィールド

- [Strip the realm from the username before passing it on to the AAA server] : レルム（管理ドメイン）をユーザ名から除去してから、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のレルム修飾子を削除するには、[Strip Realm] チェックボックスをオンにします。レルム名は、AAA（認証、許可、アカウンティング）のユーザ名に追加できます。レルムに対して有効なデリミタは @ だけです。形式は、username@realm です。たとえば、JaneDoe@it.cisco.com です。この [Strip Realm] チェックボックスをオンにすると、認証はユーザ名のみに基づいて行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。

（注） レルムとグループは、両方をユーザ名に追加できます。その場合、セキュリティ アプライアンスは、グループと AAA 機能用のレルムに対して設定されたパラメータを使用します。このオプションのフォーマットは *JaneDoe@it.cisco.com#VPNGroup* のように、*ユーザ名 [@realm][<# または !> グループ]* という形式を取ります。このオプションを選択した場合は、グループ デリミタとして # または ! を使用する必要があります。これは、@ がレルム デリミタとしても使用されている場合には、セキュリティ アプライアンスが @ をグループ デリミタと解釈できないためです。

Kerberos レルムは特殊事例です。Kerberos レルムの命名規則として、Kerberos レルムと関連付けられている DNS ドメイン名を大文字で表記します。たとえば、ユーザが it.cisco.com ドメインに存在する場合には、Kerberos レルムを IT.CISCO.COM と表記します。

- [Strip the group from the username before passing it on to the AAA server]: グループ名をユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のグループ名を削除するには、[Strip Group] チェックボックスをオンにします。このオプションは、[Enable Group Lookup] ボックスをオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザ名に追加し、Group Lookup をイネーブルにすると、セキュリティ アプライアンスは、デリミタの左側にある文字をすべてユーザ名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループ デリミタは @、#、および ! で、@ が Group Lookup のデフォルトです。*JaneDoe@VPNGroup*、*JaneDoe#VPNGroup* や *JaneDoe!VPNGroup* のように、*ユーザ名< デリミタ> グループ*の形式でグループをユーザ名に追加します。
- [Password Management] : AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。

– [Override account-disabled indication from AAA server]：AAA サーバからの account-disabled インジケータを上書きします。

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

– [Enable notification upon password expiration to allow user to change password]：このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時にユーザに通知するか、またはパスワードが期限切れになる当日にユーザに通知するかを選択できます。デフォルトでは、パスワードが期限切れになるより 14 日前にユーザへの通知を開始し、以後、ユーザがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ～ 180 日です。

（注）　この処理によってパスワードの期限が切れるまでの日数が変わるのではなく、通知がイネーブルになるだけであるという点に注意してください。このオプションを選択する場合は、日数も指定する必要があります。

どちらの場合でも、変更されずにパスワードが期限切れになると、セキュリティ アプライアンスはパスワードを変更する機会をユーザに提供します。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS または LDAP 認証が設定されていない場合、セキュリティ アプライアンスではこのコマンドが無視されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Configuring Client Addressing for SSL VPN Connections

このウィンドウを使用して、グローバル クライアント アドレスの割り当てポリシーを指定し、インターフェイスに固有のアドレス プールを設定します。このウィンドウを使用して、インターフェイスに固有のアドレス プールを追加、編集、または削除することもできます。ウィンドウ下部のテーブルには、設定されているインターフェイス固有のアドレス プールの一覧が表示されます。

フィールド

- [Global Client Address Assignment Policy]：すべての IPSec 接続と SSL VPN Client 接続（AnyConnect クライアント接続を含む）に影響するポリシーを設定します。セキュリティ アプライアンスは、アドレスを見つけるまで、選択されたソースを順番に使用します。
  – [Use authentication server]：クライアント アドレスのソースとして、セキュリティ アプライアンスが認証サーバの使用を試みるように指定します。

  - [Use DHCP] : クライアント アドレスのソースとして、セキュリティ アプライアンスが DHCP の使用を試みるように指定します。
  - [Use address pool] : クライアント アドレスのソースとして、セキュリティ アプライアンスがアドレス プールの使用を試みるように指定します。
- [Interface-Specific Address Pools] : 設定されているインターフェイス固有のアドレス プールの一覧を表示します。
- [Add] : [Assign Address Pools to Interface] ウィンドウが開きます。このウィンドウでは、インターフェイスおよび割り当てるアドレス プールを選択できます。
- [Edit] : インターフェイスとアドレス プールのフィールドに値が取り込まれた状態で、[Assign Address Pools to Interface] ウィンドウが開きます。
- [Delete] : 選択したインターフェイスに固有のアドレス プールを削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Assign Address Pools to Interface

このダイアログボックスを使用して、インターフェイスを選択し、そのインターフェイスにアドレス プールを 1 つ以上割り当てます。

フィールド

- [Interface] : アドレス プールの割り当て先インターフェイスを選択します。デフォルトは DMZ です。
- [Address Pools] : 指定したインターフェイスに割り当てるアドレス プールを指定します。
- [Select] : [Select Address Pools] ダイアログボックスが開きます。このダイアログボックスでは、このインターフェイスに割り当てるアドレス プールを 1 つ以上選択できます。選択内容は、[Assign Address Pools to Interface] ダイアログボックスの [Address Pools] フィールドに表示されます。

Select Address Pools

[Select Address Pools] ウィンドウには、クライアント アドレスの割り当てで選択可能なプール名、開始アドレスと終了アドレス、およびアドレス プールのサブネットマスクが表示され、リストのエントリを追加、編集、削除できます。

フィールド

- [Add] : [Add IP Pool] ウィンドウが開きます。このウィンドウでは、新しい IP アドレス プールを設定できます。

- [Edit] : [Edit IP Pool] ウィンドウが開きます。このウィンドウでは、選択した IP アドレス プールを変更できます。
- [Delete] : 選択したアドレス プールを削除します。確認されず、やり直しもできません。
- [Assign] : インターフェイスに割り当てられているアドレス プール名を表示します。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。[Assign] フィールドのプール割り当て一覧が更新されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add or Edit an IP Address Pool

IP アドレス プールを設定または変更します。

フィールド

- [Name] : IP アドレス プールに割り当てられている名前を指定します。
- [Starting IP Address] : プールの最初の IP アドレスを指定します。
- [Ending IP Address] : プールの最後の IP アドレスを指定します。
- [Subnet Mask] : プール内のアドレスに適用するサブネット マスクを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

SSL VPN 接続の認証

[SSL VPN Connections] > [Advanced] > [Authentication] ウィンドウでは、SSL VPN 接続の認証属性を設定できます。

System Options

[System Options] ペインでは、セキュリティ アプライアンスでの VPN セッションに固有の機能を設定できます。

永続的な IPsec トンネル フローの設定

リリース 8.0.4 よりも前の ASA ソフトウェア バージョンを実行するネットワークでは、IPSec トンネルを通過する既存の IPsec LAN-to-LAN またはリモート アクセス TCP トラフィック フローは、トンネルがドロップするとドロップされます。これらのフローは、トンネルが元に戻ると、必要に応じて再作成されます。このポリシーは、リソース管理およびセキュリティの観点から有効です。ただし、このような動作がユーザ（特に PIX および VPN 3000 コンセントレータから ASA のみの環境に移行しているユーザ）およびレガシー TCP アプリケーション（容易に再起動しない、またはトンネルを頻繁にドロップするゲートウェイが含まれたネットワーク内にある）に問題を引き起こす場合があります。

永続的な IPsec トンネル フロー機能で、この問題に対処します。この機能をイネーブルにすると、セキュリティ アプライアンスはステートフル（TCP）トンネル フローを維持して再開します。他のすべてのフローは、トンネルがドロップしたときにドロップされ、新しいトンネルが設定されたときに再確立する必要があります。

（注）　この機能は、ネットワーク拡張モードで実行されている IPsec LAN-to-LAN トンネルおよび IPsec リモートアクセス トンネルをサポートします。IPSec または AnyConnect/SSL VPN リモート アクセス トンネルはサポートしていません。

ネットワーク拡張モードで実行されている LAN-to-LAN 接続で永続的な IPsec トンネル フロー機能をイネーブルにするには、[Preserve stateful VPN flows when the tunnel drops for Network-Extension-Mode (NEM)] チェックボックスをオンにします。

ディセーブル化された永続的な IPsec トンネル フロー

LAN-to-LAN トンネルがドロップすると、エンドツーエンドのフローとトンネルを通過するフローの両方、およびそれらに属するすべてのステート情報が削除されます。その後、トンネルが再確立され、そのトンネルを通過するフローが再作成され、トンネリングされたデータの伝送を再開できるようになります。ただし、TCP/FTP エンドツーエンドのフローには問題が発生します。この時点までの FTP 転送のフローを説明するステート情報が削除されているため、ステートフル ファイアウォールは、インフライト FTP データをブロックし、エンドツーエンドのフローの作成を拒否します。今まで存在していたこのフロー履歴が失われると、ファイアウォールは FTP 転送を迷子の TCP パケットとして処理し、ドロップします。これはデフォルトの動作です。

イネーブル化された永続的な IPsec トンネル フロー

永続的 IPsec トンネル フロー機能がイネーブルの場合、タイムアウト期間内にトンネルが再作成される限り、セキュリティ アプライアンスでエンドツーエンド フロー内のステート情報にアクセスできるため、データは正常に流れ続けます。

この機能がイネーブルの場合、セキュリティ アプライアンスはフローを個別に処理します。これは、トンネルを通過するフローで定義されたトンネルがドロップされた場合、エンドツーエンド フローが削除されないことを意味します。セキュリティ アプライアンスは、ステートフル（TCP）トンネル フローを維持して再開します。他のフローはすべてドロップされ、新しいトンネルで再確立される必要があります。これによって、トンネル フローのセキュリティが弱くなることはありません。トンネルがダウンしている間、セキュリティ アプライアンスはエンドツーエンド フローに到着するあらゆるパケットをドロップするためです。

（注）　トンネル TCP フローはドロップされないため、クリーンアップは TCP タイムアウトに依存します。ただし、特定のトンネル フローのタイムアウトがディセーブルになってる場合、手動または他の方法（ピアからの TCP RST など）によってクリアされるまで、そのフローはシステム内で保持されます。

フィールド

- インターフェイスの access-lists を迂回するには、インバウンド IPSec セッションをイネーブルにします。グループ ポリシーおよびユーザ単位の許可アクセス リストは、引き続きトラフィックに適用されます。セキュリティ アプライアンスは、VPN トラフィックがセキュリティ アプライアンス インターフェイスで終了することをデフォルトで許可しているため、IKE または ESP（またはその他のタイプの VPN パケット）をアクセス ルールで許可する必要はありません。このオプションをオンにしている場合は、復号化された VPN パケットのローカル IP アドレスに対するアクセス ルールは不要です。VPN トンネルは VPN セキュリティ メカニズムを使用して正常に終端されたため、この機能によって、コンフィギュレーションが簡略化され、セキュリティ アプライアンスのパフォーマンスはセキュリティ リスクを負うことなく最大化されます （グループ ポリシーおよびユーザ単位の許可アクセス リストは、引き続きトラフィックに適用されます）。

  このオプションをオフにすることにより、アクセス ルールをローカル IP アドレスに適用することを強制的に適用できます。アクセス ルールはローカル IP アドレスに適用され、VPN パケットが復号化される前に使用されていた元のクライアント IP アドレスには適用されません。

- [Limit maximum number of active IPSec VPN sessions]：アクティブな IPSec VPN セッションの最大数の制限をイネーブルまたはディセーブルにします。範囲は、ハードウェア プラットフォームとソフトウェア ライセンスによって異なります。
  - [Maximum Active IPSec VPN Sessions]：アクティブな IPSec VPN セッションの最大許可数を指定します。このフィールドは、上記のチェックボックスをオンにして、アクティブな IPSec VPN セッションの最大数を制限した場合にだけアクティブになります。
- [L2TP Tunnel Keep-alive Timeout]：キープアライブ メッセージの頻度を秒単位で指定します。範囲は 10 ～ 300 秒です。デフォルトは 60 秒です。
- [Reclassify existing flows when VPN tunnels establish]：既存のフローを再分類して、暗号化が必要なフローが、確実に分解されて再作成されるようにします。
- [Preserve stateful VPN flows when the tunnel drops]：永続的な IPsec トンネル フローをイネーブルにします。[Remote Access VPN] > [Network（Client）Access] > [Advanced] > [IPsec] > [System Options] パスからこのウィンドウが表示された場合、次のテキストが選択のオプションの末尾に表示されます。「(for Network-Extension-Mode (NEM)」。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

SSL VPN 接続の拡張設定

Advanced オプションには、スプリット トンネリング、IE ブラウザ プロキシ、およびグループ ポリシーに関連した、SSL VPN/AnyConnect クライアントと IPSec クライアントの属性の設定が含まれます。

スプリット トンネリングの設定

スプリット トンネリングにより、特定のデータ トラフィックを暗号化し（「トンネルを通過」）、それ以外のトラフィックはクリア（非暗号化）で送信するように指定できます。スプリット トンネリング ネットワーク リストによって、トラフィックがトンネルを通過する必要があるネットワークと、トンネリングを必要としないネットワークが区別されます。セキュリティ アプライアンス は、ネットワーク リストに基づいてスプリット トンネリングを実行するかどうかを決定します。ネットワーク リストは、プライベート ネットワーク上のアドレスのリストで構成された ACL です。

フィールド

- [DNS Names]：このポリシーを適用する DNS 名を 1 つ以上指定します。
- [Policy]：スプリット トンネリング ポリシーを選択し、指定されたネットワーク リストにトンネルを含めるか、またはリストからトンネルを除外するかどうかを指定します。Inherit を選択しない場合、デフォルトは Exclude Network List Below です。
- [Network List]：スプリット トンネリング ポリシーを適用するネットワークを選択します。Inherit を選択しない場合、デフォルトは --None-- です。
- [Manage]：[ACL Manager] ダイアログボックスが開きます。このダイアログボックスでは、ネットワーク リストとして使用するアクセス コントロール リストを設定できます。
- [Intercept DHCP Configuration Message from Microsoft Clients]：DHCP 代行受信に固有の追加パラメータを示します。DHCP 代行受信を使用すると、Microsoft XP クライアントがセキュリティ アプライアンスでスプリット トンネリングを使用できるようになります。Windows クライアントが XP 以前である場合は、DHCP 代行受信により、ドメイン名およびサブネット マスクが提供されます。
  - [Intercept]：DHCP 代行受信を許可するかどうかを指定します。Inherit を選択しない場合、デフォルト設定は No です。
  - [Subnet Mask]：使用するサブネット マスクを選択します。

Zone Labs Integrity Server

[Zone Labs Integrity Server] パネルでは、Zone Labs Integrity Server をサポートするようにセキュリティ アプライアンスを設定できます。このサーバは、プライベート ネットワークにアクセスするリモート クライアントでセキュリティ ポリシーを適用する目的で設計された Integrity System というシステムの一部です。本質的には、セキュリティ アプライアンスが、ファイアウォール サーバに対するクライアント PC のプロキシとして機能し、Integrity クライアントと Integrity サーバ間で必要なすべての Integrity 情報をリレーします。

（注）　現在のリリースのセキュリティ アプライアンスでは同時に 1 台の Integrity サーバのみがサポートされていますが、ユーザ インターフェイスでは最大 5 台の Integrity サーバの設定がサポートされています。アクティブなサーバに障害が発生した場合は、セキュリティ アプライアンス上で別の Integrity サーバを設定して、クライアント VPN セッションを再確立してください。

フィールド

- [Server IP address]：Integrity Server の IP アドレスを入力します。ドット付き 10 進数を使用します。
- [Add]：新しいサーバ IP アドレスを Integrity Server のリストに追加します。このボタンは、Server IP アドレス フィールドにアドレスが入力されるとアクティブになります。
- [Delete]：選択したサーバを Integrity Server リストから削除します。
- [Move Up]：選択したサーバを Integrity Server のリスト内で上に移動します。このボタンは、リストにサーバが 1 台以上存在する場合にだけ使用できます。
- [Move Down]：選択したサーバを Integrity Server のリスト内で下に移動します。このボタンは、リストにサーバが 1 台以上存在する場合にだけ使用できます。
- [Server Port]：アクティブな Integrity サーバをリッスンするセキュリティ アプライアンスのポート番号を入力します。このフィールドは、Integrity Server のリストにサーバが少なくとも 1 台以上存在する場合にだけ使用できます。デフォルト ポート番号は 5054、範囲は 10 ～ 10000 です。このフィールドは、Integrity Server リスト内にサーバが存在する場合にだけ使用できます。
- [Interface]：アクティブな Integrity Server と通信するセキュリティ アプライアンス インターフェイスを選択します。このインターフェイス名メニューは、Integrity Server リスト内にサーバが存在する場合にだけ使用できます。
- [Fail Timeout]：セキュリティ アプライアンスが、アクティブな Integrity Server に到達不能であることを宣言するまでの待機秒数を入力します。デフォルトは 10 で、範囲は、5 ～ 20 です。
- [SSL Certificate Port]：SSL 認証で使用するセキュリティ アプライアンスのポートを指定します。デフォルトのポートは 80 です。
- [Enable SSL Authentication]：セキュリティ アプライアンスによるリモート クライアントの SSL 証明書の認証をイネーブルにする場合にオンにします。デフォルトでは、クライアント SSL 認証はディセーブルになっています。
- [Close connection on timeout]：タイムアウト時に、セキュリティ アプライアンスと Integrity Server 間の接続を終了する場合にオンにします。デフォルトでは、接続が維持されます。
- [Apply]：設定を実行しているセキュリティ アプライアンスに Integrity Server 設定を適用します。
- [Reset]：まだ適用されていない Integrity Server 設定の変更を削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Easy VPN Remote

Easy VPN Remote により、ASA 5505 を Easy VPN クライアント デバイスとして動作させることができます。ASA 5505 は、Easy VPN サーバへの VPN トンネルを開始できます。Easy VPN サーバの種類としては、セキュリティ アプライアンス、Cisco VPN 3000 コンセントレータ、IOS ベースのルータ、または Easy VPN サーバとして動作するファイアウォールがあります。

Easy VPN クライアントは次の 2 つの操作モードのいずれかをサポートします。クライアント モードまたは Network Extension Mode（NEM; ネットワーク拡張モード）です。操作モードによって、Easy VPN クライアントの内部ホストがトンネルを経由して企業ネットワークからアクセスできるかどうかが決まります。Easy VPN クライアントにはデフォルト モードがないため、接続前に動作モードを指定する必要があります。

クライアント モードは、ポート アドレス変換（PAT）モードとも呼ばれ、Easy VPN クライアント プライベート ネットワーク上のすべてのデバイスを企業ネットワークの IP アドレスから分離します。Easy VPN クライアントは、内部ホストのすべての VPN トラフィックに対してポート アドレス変換（PAT）を実行します。Easy VPN クライアント内部インターフェイスまたは内部ホストで、IP アドレスの管理は必要ではありません。

NEM は、内部インターフェイスとすべての内部ホストをトンネルを介した企業ネットワーク上でルーティングできるようにします。内部ネットワークのホストは、スタティック IP アドレスで事前設定されたアクセス可能なサブネット（スタティックまたは DHCP を介して）から IP アドレスを取得します。NEM では、PAT は VPN トラフィックに適用されません。このモードでは、各クライアントに VPN を設定する必要がありません。NEM モード用に設定された Cisco ASA 5505 では、自動トンネル起動をサポートしています。コンフィギュレーションには、グループ名、ユーザ名、およびパスワードを保存する必要があります。セキュア ユニット認証がイネーブルの場合は、トンネルの自動開始がディセーブルになります。

Easy VPN クライアントのプライベート側のネットワークとアドレスは非表示になっており、直接のアクセスはできません。

フィールド

- [Enable Easy VPN Remote] : Easy VPN Remote 機能をイネーブルにし、このウィンドウの残りのフィールドを設定できるようにします。
- [Mode] : Client mode か Network extension mode のどちらかを選択します。
  - [Client mode] : ポート アドレス変換（PAT）モードを使用して、クライアントに関連する内部ホストのアドレスを企業ネットワークから分離します。
  - [Network extension mode] : このようなアドレスを企業ネットワークからアクセス可能にします。

    （注）　Easy VPN Remote が NEM を使用し、セカンダリ サーバに接続されている場合は、各ヘッドエンドへの ASDM 接続を確立し、[Configuration] > [VPN] > [IPSec] > [IPSec Rules] > [Tunnel Policy (Crypto Map) - Advanced] ダイアログボックスの [Enable Reverse Route Injection] をオンにし、RRI を使用したリモート ネットワークのダイナミック アナウンスメントを設定します。

  - [Auto connect] : ネットワーク拡張モードがローカルに設定され、かつ Easy VPN Remote にプッシュされたグループ ポリシーでスプリット トンネリングが設定されている場合を除き、Easy VPN Remote は、自動 IPSec データ トンネルを確立します。両方の条件を満たしている場合は、この属性をオンにすると、IPSec データ トンネルの確立が自動化されます。両方の条件を満たしていて、この属性をオフにした場合、この属性は無視されます。

- [Group Settings]：事前共有キーまたは X.509 証明書をユーザ認証に使用するかどうかを指定します。
  - [Pre-shared key]：認証に事前共有キーを使用することをイネーブルにし、この属性を指定すると、その後の、[Group Name]、[Group Password]、[Confirm Password] の各フィールドに、そのキーに含まれるグループ ポリシー名とパスワードを指定できるようになります。
  - [Group Name]：認証に使用するグループ ポリシーの名前を指定します。
  - [Group Password]：指定したグループ ポリシーで使用するパスワードを指定します。
  - [Confirm Password]：入力したグループ パスワードの確認を必須にします。
  - [X.509 Certificate]：認証用に、認証局から提供された X.509 デジタル証明書の使用を指定します。
  - [Select Trustpoint]：ドロップダウン リストからトラストポイントを選択できます。トラストポイントは、IP アドレスまたはホスト名前です。トラストポイントを定義するには、この領域の下部にある [Trustpoint(s) configuration] リンクをクリックします。
  - [Send certificate chain]：証明書自体だけでなく、証明書チェーンの送信もイネーブルにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
- [User Settings]：ユーザ ログイン情報を設定します。
  - [User Name]：Easy VPN Remote 接続用の VPN ユーザ名を設定します。Xauth には、TACACS+ または RADIUS を使用して IKE 内のユーザを認証する機能があります。Xauth は、RADIUS または別のサポートされているユーザ認証プロトコルを使用して、ユーザを認証します（この場合、Easy VPN ハードウェア クライアント）。セキュア ユニット認証がディセーブルになっており、サーバが Xauth クレデンシャルを要求する場合には、Xauth ユーザ名とパスワード パラメータが使用されます。セキュア ユニット認証がイネーブルの場合、これらのパラメータは無視され、セキュリティ アプライアンスによって、ユーザにユーザ名とパスワードの入力を求めるプロンプトが表示されます。
  - [User Password]：Easy VPN Remote 接続用の VPN ユーザ パスワードを設定します。
  - [Confirm Password]：入力したユーザ パスワードの確認を必須にします。
- [Easy VPN Server To Be Added]：Easy VPN サーバを追加または削除します。どの ASA または VPN 3000 コンセントレータ シリーズでも Easy VPN サーバとして動作できます。接続を確立する前にサーバを設定する必要があります。セキュリティ アプライアンスは、IPv4 アドレス、名前データベース、または DNS 名をサポートしており、この順序でアドレスを解決します。Easy VPN Server(s) リストの最初のサーバはプライマリ サーバです。プライマリ サーバに加え、最大 10 台のバックアップ サーバを指定できます。
  - [Name or IP Address]：リストに追加する Easy VPN サーバの名前または IP アドレス。
  - [Add]：指定したサーバを Easy VPN Server(s) リストに移動します。
  - [Remove]：Easy VPN Server(s) リストから選択したサーバを Name または IP Address ファイルに移動します。ただし、この作業を実行した場合には、[Name] または [IP Address] フィールドにそのアドレスを再入力しないと、同じアドレスを再度追加することができません。
  - [Easy VPN Server(s)]：設定した VPN サーバを優先順位に応じて一覧表示します。
  - [Move Up/Move Down]：Easy VPN Server(s) リスト内でのサーバの位置を変更します。これらのボタンは、リストにサーバが 1 台以上存在する場合にだけ使用できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

高度な Easy VPN プロパティ

デバイス パススルー

Cisco IP Phone やプリンタなどのデバイスは、認証を実行できないため、個別ユニット認証に追加できません。これらのデバイスに対応するために、Individual User Authentication がイネーブルになっている場合には、MAC Exemption 属性によってイネーブルにされるデバイス パススルー機能が、指定した MAC アドレスを持つデバイスの認証を免除します。

MAC アドレスの最初の 24 ビットは、その機器の製造元を示します。最後の 24 ビットは、ユニットの 16 進形式のシリアル番号です。

管理トンネル

ASA モデル 5505 デバイスを NAT デバイスの後ろで稼働させるときに、Tunneled Management 属性を使用して、デバイス管理の設定方法（クリアまたはトンネリング）を指定し、トンネル経由での Easy VPN Remote 接続の管理を許可するネットワークを指定できます。ASA 5505 のパブリック アドレスが NAT デバイスの後ろにある場合は、NAT デバイスで静的 NAT マッピングを追加しなければアクセスできません。

NAT デバイスの背後で Cisco ASA 5505 を稼働させるときに、**vpnclient management** コマンドを使用して、デバイスの管理方法（暗号化の追加または暗号化なし）を指定し、管理アクセスを与えるホストまたはネットワークを指定します。ASA 5505 のパブリック アドレスが NAT デバイスの後ろにある場合は、NAT デバイスで静的 NAT マッピングを追加しなければアクセスできません。

フィールド

- [MAC Exemption] : Easy VPN Remote 接続のデバイス パススルーで使用する MAC アドレスとマスクを設定します。
  - [MAC Address] : 指定した MAC アドレスを持つデバイスの認証を免除します。このフィールドで MAC アドレスを指定するための形式は 3 桁の 16 進数値で、45ab.ff36.9999 のようにピリオドで区切られます。
  - [MAC Mask] : このフィールドで MAC アドレスを指定するための形式は 3 桁の 16 進数値で、たとえば ffff.ffff.ffff という MAC マスクは、指定した MAC アドレスとだけ一致します。すべてがゼロの MAC マスクは、いずれの MAC アドレスとも一致しません。MAC マスク ffff.ff00.0000 は、製造業者が同じであるすべてのデバイスと一致します。
  - [Add] : 指定した MAC アドレスとマスクのペアを MAC Address/Mask リストに追加します。
  - [Remove] : MAC Address/MAC リストから選択した MAC アドレスとマスクのペアを、個々の [MAC Address] および [MAC Mask] フィールドに移動します。
- [Tunneled Management] : デバイス管理のための IPSec の暗号化を設定し、トンネル経由での Easy VPN ハードウェア クライアント接続の管理を許可するネットワークを指定します。[Clear Tunneled Management] を選択しても、IPSec の暗号化レベルが削除されるだけで、SSH や https など、その接続に存在する他の暗号化には影響しません。

- [Enable Tunneled Management]：すでに管理トンネルに存在する SSH または HTTPS 暗号化に IPSec 暗号化レイヤを追加します。
- [Clear Tunneled Management]：暗号化を追加せず、すでに管理トンネルに存在する暗号化を使用します。
- [IP Address]：VPN トンネル経由での Easy VPN ハードウェア クライアントへの管理アクセスを許可するホストまたはネットワークの IP アドレスを指定します。1 つ以上の IP アドレスと各ネットワーク マスクを個別に追加できます。
- [Mask]：対応する IP アドレスのネットワーク マスクを指定します。
- [Add]：指定した IP アドレスとマスクを IP Address/Mask リストに移動します。
- [Remove]：選択した IP アドレスとマスクのペアを、IP Address/Mask リストから、この領域にある個々の [IP Address/Mask] フィールドに移動します。
- [IP Address/Mask]：この領域の Enable または Clear 機能によって処理される、設定した IP アドレスとマスクのペアを一覧表示します。

- [IPSec Over TCP]：Easy VPN Remote 接続に TCP でカプセル化された IPSec を使用するように設定します。
  - [Enable]：IPSec over TCP をイネーブルにします。

（注） Easy VPN Remote 接続で、TCP でカプセル化された IPSec を使用する場合は、[Configuration] > [VPN] > [IPSec] > [Pre-Fragmentation] を選択し、外部インターフェイスをダブルクリックし、DF Bit Setting Policy を Clear に設定します。Clear 設定を使用して、セキュリティ アプライアンスに大きいパケットを送信させることができます。

  - [Enter Port Number]：IPSec over TCP 接続で使用するポート番号を指定します。
- [Server Certificate]：Easy VPN Remote 接続が、証明書マップが指定した特定の証明書を持つ Easy VPN サーバとの接続だけを許可するように設定します。このパラメータを使用して、Easy VPN サーバ証明書のフィルタリングをイネーブルにします。証明書マップを定義するには、[Configuration] > [VPN] > [IKE] > [Certificate Group Matching] > [Rules] にアクセスします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

CHAPTER 33

ダイナミック アクセス ポリシーの設定

次の項では、ダイナミック アクセス ポリシーについての情報を提供します。

VPN 環境でのアクセス ポリシーについて

VPN ゲートウェイは動的な環境で動作します。個々の VPN 接続には、頻繁に変更されるイントラネット設定、組織内の各ユーザが持つさまざまなロール、および設定とセキュリティ レベルが異なるリモート アクセス サイトからのログインなど、複数の変数が影響する可能性があります。VPN 環境でのユーザ許可のタスクは、スタティックな設定のネットワークでの許可タスクよりもかなり複雑です。

セキュリティ アプライアンスでのダイナミック アクセス ポリシー（DAP）により、これらの多くの変数に対処する許可機能を設定できます。ダイナミック アクセス ポリシーは、特定のユーザ トンネルまたはユーザ セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。これらの属性により、複数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。つまり、セキュリティ アプライアンスでは、定義したポリシーに基づき、特定のユーザに対して、特定のセッションのアクセスが許可されます。セキュリティ アプライアンスは、ユーザが接続するときに、1 つまたは複数の DAP レコードから属性を選択または集約して、DAP を生成します。DAP レコードは、リモート デバイスのエンドポイント セキュリティ情報および認証されたユーザの AAA 許可情報に基づいて選択されます。選択された DAP レコードは、ユーザ トンネルまたはセッションに適用されます。

DAP システムには、注意を必要とする次のコンポーネントがあります。

- DAP 選択コンフィギュレーション ファイル：セッション確立中に DAP レコードを選択および適用するためにセキュリティ アプライアンスが使用する、基準が記述されたテキスト ファイル。セキュリティ アプライアンスに保存されています。ASDM を使用して、このファイルを変更したり、XML データ形式でセキュリティ アプライアンスにアップロードしたりできます。DAP 選択設定ファイルには、ユーザが設定するすべての属性が記載されています。たとえば、AAA 属性、エンドポイント属性、ネットワーク ACL と Web-type ACL のフィルタで設定されるアクセス ポリシー、ポート転送リスト、および URL リストなどがあります。
- DfltAccess ポリシー：常に DAP サマリー テーブルの最後のエントリで、プライオリティは必ず 0。デフォルト アクセス ポリシーのアクセス ポリシー属性を設定できますが、AAA 属性またはエンドポイント属性は含まれておらず、これらの属性は設定できません。DfltAccessPolicy は削除できません。また、サマリー テーブルの最後のエントリになっている必要があります。

ダイナミック アクセス ポリシーの詳細については、次のリンクをクリックしてください。

- リモート アクセス接続タイプに対する DAP サポート
- DAP と AAA
- DAP とエンドポイント セキュリティ

- DAP 接続シーケンス
- Tesy Dynamic Access Policies
- DAP の例

ダイナミック アクセス ポリシーの設定

ダイナミック アクセス ポリシーを設定するには、ASDM の [Configuration] > [Remote Access VPN] > [Network (Client) Access] *または* [Clientless SSL VPN Access] > [Dynamic Access Policies] ペインで、次の手順を実行します。

ステップ 1　特定のアンチウイルス、アンチスパイウェア、またはパーソナル ファイアウォールのエンドポイント属性を含めるには、ペインの最上部近くの [*CSD configuration*] リンクをクリックします。次に、Cisco Secure Desktop *および*ホスト スキャンの拡張機能をイネーブルにします。このリンクは、これら両方の機能をすでにイネーブルにしている場合には表示されません。

Cisco Secure Desktop 拡張機能をイネーブルにして Host Scan 拡張機能はイネーブルにしない場合、変更を適用すると、ASDM は Host Scan コンフィギュレーションをイネーブルにするリンクを表示します。

ステップ 2　新しいダイナミック アクセス ポリシーを作成するには、[Add] をクリックします。既存のポリシーを変更するには、[Edit] をクリックします。

ステップ 3　すでに設定済みのポリシーをテストするには、[Test Dynamic Access Policies] ボタンをクリックします。

フィールド

- [Priority]：DAP レコードのプライオリティを表示します。セキュリティ アプライアンスは、複数の DAP レコードからネットワーク ACL と Web-type ACL を集約するときに、この値を使用してアクセス リストを論理的に順序付けします。セキュリティ アプライアンスは、最上位のプライオリティ番号から最下位のプライオリティ番号の順にレコードを並べ、最下位のプライオリティをテーブルの一番下に配置します。番号が大きいほどプライオリティが高いことを意味します。たとえば、値が 4 の DAP レコードは値が 2 のレコードよりも高いプライオリティを持つことになります。プライオリティは、手動での並べ替えはできません。
- [Name]：DAP レコードの名前を表示します。
- [Network ACL List]：セッションに適用されるファイアウォール アクセス リストの名前を表示します。
- [Web-Type ACL List]：セッションに適用される SSL VPN アクセス リストの名前を表示します。
- [Description]：DAP レコードの目的を説明します。
- [Test Dynamic Access Policies] ボタン：設定済みの DAP レコードをテストします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

リモート アクセス接続タイプに対する DAP サポート

DAP システムは、次のリモート アクセス方式をサポートします。

- IPsec VPN
- クライアントレス（ブラウザベース）SSL VPN
- Cisco AnyConnect SSL VPN
- PIX カットスルー プロキシ（ポスチャ評価は使用不可）

DAP と AAA

DAP は AAA サービスを補完します。用意されている許可属性のセットはかぎられていますが、それらの属性によって AAA で提供される許可属性を無効にできます。セキュリティ アプライアンスは、ユーザの AAA 許可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。セキュリティ アプライアンスは、この情報に基づいて複数の DAP レコードを選択でき、それらのレコードを集約して DAP 許可属性を作成します。

AAA 属性は、Cisco AAA 属性階層から、またはセキュリティ アプライアンスが RADIUS または LDAP サーバから受信する一式の応答属性セットから指定できます。

AAA 属性の定義

表 33-1 に、DAP で使用できる AAA 選択属性名の定義を示します。属性名フィールドは、LUA 論理式での各属性名の入力方法を示しており、[Add/Edit Dynamic Access Policy] ペインの [Advanced] セクションで使用します。

表 33-1　AAA 選択属性名

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
シスコ	aaa.cisco.memberof	AAA	文字列	128	memberof の値
	aaa.cisco.username	AAA	文字列	64	ユーザ名の値
	aaa.cisco.class	AAA	文字列	64	クラス属性値
	aaa.cisco.ipaddress	AAA	番号	-	framed-ip アドレスの値
	aaa.cisco.tunnelgroup	AAA	文字列	64	トンネル グループ名
LDAP	aaa.ldap.<label>	LDAP	文字列	128	LDAP 属性値ペア
RADIUS	aaa.radius.<number>	RADIUS	文字列	128	RADIUS 属性値ペア

DAP とエンドポイント セキュリティ

セキュリティ アプライアンスは、設定するポスチャ評価方式を使用してエンドポイント セキュリティの属性を取得します。これには、Cisco Secure Desktop および NAC が含まれます。詳細については、「ASDM」の「Cisco Secure Desktop」セクションを参照してください。表 33-2 に、DAP がサポートしている各リモート アクセス プロトコル、その方式で使用可能なポスチャ評価ツール、およびそのツールによって提供される情報を示します。

表 33-2　DAP ポスチャ評価

リモート アクセス プロトコル	Cisco Secure Desktop	ホスト スキャン	NAC	Cisco NAC アプライアンス
	ファイル情報、レジストリ キーの値、実行プロセス、オペレーティング システムを返す	アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール ソフトウェアの情報を返す	NAC ステータスを返す	VLAN タイプと VLAN ID を返す
IPsec VPN	No	No	Yes	Yes
Cisco AnyConnect VPN	Yes	Yes	Yes	Yes
Clientless VPN	Yes	Yes	No	No
PIX Cut-through Proxy	No	No	No	No

エンドポイント属性の定義

表 33-3 に DAP で使用可能なエンドポイント選択属性名の定義を示します。属性名フィールドは、LUA 論理式での各属性名の入力方法を示しており、[Add/Edit Dynamic Access Policy] ペインの [Advanced] エリアで使用します。*label* 変数は、アプリケーション、ファイル名、プロセス、またはレジストリ エントリを示します。

表 33-3　エンドポイント属性の定義

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
アンチスパイウェア（Cisco Secure Desktop が必要）	endpoint.as.*label*.exists	ホスト スキャン	true	—	アンチスパイウェア プログラムが存在する
	endpoint.as.*label*.version		文字列	32	バージョン
	endpoint.as.*label*.description		文字列	128	アンチスパイウェアの説明
	endpoint.as.*label*.lastupdate		整数	—	アンチスパイウェア定義を更新してからの経過時間（秒）
ウイルス対策（Cisco Secure Desktop が必要）	endpoint.av.*label*.exists	ホスト スキャン	true	—	アンチウイルス プログラムが存在する
	endpoint.av.*label*.version		文字列	32	バージョン
	endpoint.av.*label*.description		文字列	128	アンチウイルスの説明
	endpoint.av.*label*.lastupdate		整数	—	アンチウイルス定義を更新してからの経過時間（秒）

表 33-3　エンドポイント属性の定義 （続き）

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
アプリケーション	endpoint.application.clienttype	アプリケーション	文字列	—	クライアント タイプ： CLIENTLESS ANYCONNECT IPSEC L2TP
File	endpoint.file.*label*.exists	Secure Desktop	true	—	ファイルが存在する
	endpoint.file.*label*.lastmodified		整数	—	ファイルが最後に変更されてからの経過時間（秒）
	endpoint.file.*label*.crc.32		整数	—	ファイルの CRC32 ハッシュ
NAC	endpoint.nac.status	NAC	文字列	—	ユーザ定義ステータス ストリング
オペレーティング システム	endpoint.os.version	Secure Desktop	文字列	32	オペレーティング システム
	endpoint.os.servicepack		整数	—	Windows のサービス パック
Personal Firewall (Secure Desktop が必要)	endpoint.fw.*label*.exists	ホスト スキャン	true	—	パーソナル ファイアウォールが存在する
	endpoint.fw.*label*.version		文字列	32	バージョン
	endpoint.fw.*label*.description		文字列	128	パーソナル ファイアウォールの説明
Policy	endpoint.policy.location	Secure Desktop	文字列	64	Cisco Secure Desktop からのロケーション値
プロセス	endpoint.process.*label*.exists	Secure Desktop	true	—	プロセスが存在する
	endpoint.process.*label*.path		文字列	255	プロセスのフル パス
Registry	endpoint.registry.*label*.type	Secure Desktop	*dword* *文字列*	—	dword
	endpoint.registry.*label*.value		文字列	255	レジストリ エントリの値
VLAN	endoint.vlan.type	CNA	文字列	—	VLAN タイプ： ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

DAP とアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール プログラム

セキュリティ アプライアンスは、ユーザ属性が、設定済みの AAA 属性およびエンドポイント属性に一致する場合に DAP ポリシーを使用します。Cisco Secure Desktop のプリログイン評価モジュールおよびホスト スキャン モジュールは、設定済みエンドポイント属性の情報をセキュリティ アプライアンスに返し、DAP サブシステムでは、その情報に基づいてそれらの属性値に一致する DAP レコードを選択します。

すべてではありませんが、ほとんどのアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォールのプログラムは、アクティブ スキャンをサポートしています。つまり、それらのプログラムはメモリ常駐型であり、常に動作しています。ホスト スキャンは、エンドポイントにプログラムがインストールされているかどうか、およびそのプログラムがメモリ常駐型かどうかを、次のようにしてチェックします。

- インストールされているプログラムがアクティブ スキャンをサポートしない場合、ホスト スキャンはそのソフトウェアの存在をレポートします。DAP システムは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブ スキャンをサポートしており、そのプログラムでアクティブ スキャンがイネーブルになっている場合、ホスト スキャンはそのソフトウェアの存在をレポートします。この場合も、セキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブ スキャンをサポートしており、そのプログラムでアクティブ スキャンがディセーブルになっている場合、ホスト スキャンはそのソフトウェアの存在を無視します。セキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択しません。さらに、そのプログラムがインストールされているとしても、DAP についての情報が多く含まれる **debug trace** コマンドの出力にはプログラムの存在が示されません。

DAP 接続シーケンス

次のシーケンスに、標準的なリモート アクセス接続を確立する場合の概要を示します。

1. リモート クライアントが VPN 接続を試みます。
2. セキュリティ アプライアンスは、設定された NAC 値と Cisco Secure Desktop の Host Scan 値を使用してポスチャ評価を実行します。
3. セキュリティ アプライアンスが、AAA を介してユーザを認証します。AAA サーバは、ユーザの許可属性も返します。
4. セキュリティ アプライアンスが、AAA 許可属性をそのセッションに適用し、VPN トンネルを確立します。
5. セキュリティ アプライアンスが、AAA 許可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。
6. セキュリティ アプライアンスが、選択した DAP レコードから DAP 属性を集約します。集約された属性が DAP ポリシーを構成します。
7. セキュリティ アプライアンスがその DAP ポリシーをセッションに適用します。

Tesy Dynamic Access Policies

このペインでは、許可属性値のペアを指定することによって、デバイスで設定される DAP レコードセットが取得されるかどうかをテストできます。属性値のペアを指定するには、[AAA Attribute] テーブルと [Endpoint Attribute] テーブルに関連づけられた [Add/Edit] ボタンを使用します。[Add/Edit] ボタンをクリックすると表示されるダイアログは、[Add/Edit AAA Attributes] ウィンドウと [Add/Edit Endpoint Attributes] ウィンドウに表示されるダイアログに似ています。

属性値のペアを入力して [Test] ボタンをクリックすると、デバイス上の DAP サブシステムはこれらの値を参照して、各レコードの AAA およびエンドポイント選択属性を評価します。結果は、[Test Results] テキスト領域に表示されます。

フィールド

- [Selection Criteria]：ダイナミック アクセス ポリシーを取得するときにテストする AAA 属性とエンドポイント属性を決定します。
- AAA 属性
  - [AAA Attribute]：AAA 属性を特定します。
  - [Operation Value]：属性を指定された値に対して =/!= として指定します。
  - [Add/Edit]：AAA 属性を追加または編集します。
- [Endpoint Attributes]：エンドポイント属性を特定します。
  - [Endpoint ID]：エンドポイント属性 ID を入力します。
  - [Name/Operation/Value]：
  - [Add/Edit/Delete]：エンドポイント属性を追加、編集、または削除します。
- [Test Result]：テスト結果を表示します。
- [Test]：設定したポリシーが取得されることをテストします。
- [Close]：ペインを閉じます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

ダイナミック アクセス ポリシーの追加および編集

ダイナミック アクセス ポリシーを追加または編集するには、次の手順を実行します。

ステップ 1　[Add/Edit Dynamic Access Policy] ペインの上部で、このダイナミック アクセス ポリシーの名前（必須）と説明（任意）を入力します。

ステップ 2　[Priority] フィールドで、そのダイナミック アクセス ポリシーのプライオリティを設定します。セキュリティ アプライアンスは、ここで設定される順序に従ってアクセス ポリシーを適用します。最も大きな番号のプライオリティが最上位のプライオリティです。プライオリティの設定が同じで ACL ルールが競合する DAP レコードの場合は、最も制約の多いルールが適用されます。

ステップ 3　[Add/Edit AAA Attributes] フィールドの [ANY/ALL/NONE] ドロップダウン ボックス（ラベルなし）を使用して、このダイナミック アクセス ポリシーを使用するために、ユーザは設定する AAA 属性値のいずれかまたはすべてを必要とするのか、または一切不要なのかを選択します。

ステップ 4　AAA 属性を設定するには、[AAA Attributes] フィールドの [Add/Edit] をクリックします。

ステップ 5　エンドポイント属性を設定する前に、CSD Host Scan を設定します。

ステップ 6　エンドポイント セキュリティ属性を設定するには、[Endpoint ID] フィールドの [Add/Edit] をクリックします。

ステップ 7　各タイプのエンドポイント属性のインスタンスを複数作成できます。これらのタイプごとに、ユーザがあるタイプのインスタンスのすべてを持つように DAP ポリシーで要求する（Match all = AND）のか、またはそれらのインスタンスを 1 つだけ持つように要求する（Match Any = OR）のかを決定する必要があります。エンドポイント属性のそれぞれに対してこの値を設定するには、[Logical Op.] ボタンをクリックします。

ステップ 8　[Advanced] フィールドには、上の [AAA] 領域および [Endpoint] 領域で入力可能な属性以外の AAA またはエンドポイントの属性を設定する論理式を 1 つ以上入力できます。

ステップ 9　ネットワーク /Web-type ACL、ファイル ブラウジング、ファイル サーバ入力、HTTP プロキシ、URL 入力、ポート転送リスト、および URL リストを設定するには、[Access Policy Attributes] の各フィールドで値を設定します。

フィールド

- [Policy Name] : 4 ～ 32 文字の文字列。スペースは使用できません。
- [Description] :（任意）DAP レコードの目的を説明します。最大 80 文字です。
- [Priority] : DAP のプライオリティを設定します。セキュリティ アプライアンスは、ここで設定した順序でアクセス ポリシーを適用します。数が大きいほどプライオリティは高くなります。有効値の範囲は 0 ～ 2147483647 です。デフォルト = 0。
- [ANY/ALL/NONE] ドロップダウン ボックス : ユーザ許可属性が、設定する AAA 属性の値のいずれかまたはすべてに一致するか、あるいはいずれの値にも一致せず、同時にすべてのエンドポイント属性を満たすように要求する場合に設定します。重複するエントリは許可されません。AAA またはエンドポイント属性なしの DAP レコードを設定すると、セキュリティ アプライアンスは常にそのレコードを選択します。これは、そのレコードがすべての選択基準を満たすことになるからです。
- [AAA Attributes] : 設定された AAA 属性を表示します。
  - [Attribute] : AAA 属性の名前を表示します。
  - [Operation/Value] : =/!=
  - [Add/Edit/Delete] : 選択した AAA 属性を追加、編集、または削除する場合にクリックします。
- [Endpoint Attributes] : 設定されたエンドポイント属性を表示します。
  - [Endpoint ID] : エンドポイント属性を識別します。
  - [Name/Operation/Value] : エンドポイント属性ごとに設定されている値の概要を表示します。
  - [Add/Edit/Delete] : 選択したエンドポイント属性を追加、編集、または削除します。

（注） Cisco Secure Desktop により、Application と NAC 以外のすべてのエンドポイント属性をセキュリティ アプライアンスに対して指定できます。他のすべてのエンドポイント属性を設定するには、まず Cisco Secure Desktop をイネーブルにし、そこで関連するエンドポイント属性も設定する必要があります。

  - [Logical Op.] : それぞれのタイプのエンドポイント属性のインスタンスを複数作成できます。ユーザがあるタイプのインスタンスのすべてを持つように DAP ポリシーで要求する（Match all = AND）のか、またはそれらのインスタンスを 1 つだけ持つように要求する（Match Any = OR）のかを設定します。たとえば OS などの一部のエンドポイント属性では、ユーザが属性のインスタンスを複数持つことはありません。

  - [Advanced]：ダイナミック アクセス ポリシーの追加属性を設定します。これは、LUA についての知識が要求される高度な機能です。
  - [AND/OR]：基本的な選択ルールと、ここで入力する論理式との関係を定義します。つまり、すでに設定されている AAA 属性およびエンドポイント属性に新しい属性を追加するのか、またはそれら設定済みの属性に置き換えるのかを指定します。デフォルトの設定は AND です。
  - [Logical Expressions]：それぞれのタイプのエンドポイント属性のインスタンスを複数設定できます。新しい AAA 選択属性またはエンドポイント選択属性（あるいはその両方）を定義するフリー形式の LUA テキストを入力します。ASDM は、ここで入力されるテキストの検証を行わず、単にこのテキストを DAP XML ファイルにコピーします。セキュリティ アプライアンスがそれを処理し、解析不能な式があれば破棄します。
  - [Guide]：これらの論理演算の作成に関するオンライン ヘルプを表示します。

- [Access Policy Attributes]：これらのタブにより、ネットワーク ACL と Web-type ACL のフィルタ、ファイル アクセス、HTTP プロキシ、URL エントリとリスト、ポート転送、およびクライアントレス SSL VPN アクセス方式の属性を設定できます。ここで設定する属性値は、既存のユーザ、グループ、トンネル グループ、およびデフォルトのグループ レコードを含め、AAA システムの許可値を上書きします。
- [Action] タブ
  - [Action]：特定の接続またはセッションに適用する特殊な処理を指定します。
  - [Continue]：（デフォルト）セッションにアクセス ポリシー属性を適用します。
  - [Terminate]：セッションを終了します。
  - [User Message]：この DAP レコードが選択されるときに、ポータル ページに表示するテキスト メッセージを入力します。最大 128 文字を入力できます。ユーザ メッセージは、黄色のオーブとして表示されます。ユーザがログインすると、メッセージは 3 回点滅してから静止します。数件の DAP レコードが選択され、それぞれにユーザ メッセージがある場合は、ユーザ メッセージがすべて表示されます。

（注） このようなメッセージには、URL やその他の埋め込みテキストを含めることができます。この場合は、正しい HTML タグを使用する必要があります。

例：すべてのコントラクタは、ご使用のアンチウイルス ソフトウェアのアップグレード手順について、http://wwwin.abc.com/procedure.html を参照してください。

- [Network ACL Filters] タブ：この DAP レコードに適用するネットワーク ACL を選択および設定できます。DAP の ACL には、許可ルールまたは拒否ルールを含めることができますが、両方を含めることはできません。ACL に許可ルールと拒否ルールの両方が含まれている場合、セキュリティ アプライアンスはその ACL を拒否します。
  - [Network ACL] ドロップダウン ボックス：この DAP レコードに追加する、すでに設定済みのネットワーク ACL を選択します。すべての許可ルールまたはすべての拒否ルールを含む ACL だけが適格とされ、これらの適格な ACL だけがここに表示されます。
  - [Manage...]：ネットワーク ACL を追加、編集、および削除するときにクリックします。
  - [Network ACL] リスト：この DAP レコードのネットワーク ACL が表示されます。
  - [Add]：ドロップダウン ボックスから選択したネットワーク ACL を右側の [Network ACLs] リストに追加します。
  - [Delete]：クリックすると、強調表示されているネットワーク ACL が [Network ACLs] リストから削除されます。セキュリティ アプライアンスから ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。

- [Web-Type ACL Filters] タブ：この DAP レコードに適用する Web-type ACL を選択および設定できます。DAP の ACL には、許可または拒否ルールだけを含めることができます。ACL に許可ルールと拒否ルールの両方が含まれている場合、セキュリティ アプライアンスはその ACL を拒否します。
  - [Web-Type ACL] ドロップダウン ボックス：この DAP レコードに追加する、設定済みの Web-type ACL を選択します。すべての許可ルールまたはすべての拒否ルールを含む ACL だけが適格とされ、これらの適格な ACL だけがここに表示されます。
  - [Manage...] : Web-type ACL を追加、編集、および削除するときにクリックします。
  - [Web-Type ACL] リスト：この DAP レコードの Web-type ACL が表示されます。
  - [Add] : ドロップダウン ボックスから選択した Web-type ACL を右側の [Web-Type ACLs] リストに追加します。
  - [Delete] : クリックすると、Web-type ACL の 1 つが [Web-Type ACLs] リストから削除されます。セキュリティ アプライアンスから ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。
- [Functions] タブ : DAP レコードのファイル サーバ入力とブラウジング、HTTP プロキシ、および URL 入力を設定できます。
  - [File Server Browsing] : ファイル サーバまたは共有機能の CIFS ブラウジングをイネーブルまたはディセーブルにします。

    （注） ブラウズには、NBNS（マスター ブラウザまたは WINS）が必要です。NBNS に障害が発生した場合や、NBNS が設定されていない場合は、DNS を使用します。

    （注） CIFS ブラウズ機能では、国際化がサポートされていません。

  - [File Server Entry] : ポータル ページでユーザがファイル サーバのパスおよび名前を入力できるようにするかどうかを設定します。イネーブルになっている場合、ポータル ページにファイル サーバ エントリのドロワが配置されます。ユーザは、Windows ファイルへのパス名を直接入力できます。ユーザは、ファイルをダウンロード、編集、削除、名前変更、および移動できます。また、ファイルおよびフォルダを追加することもできます。適用可能な Windows サーバでユーザ アクセスに対して共有を設定する必要もあります。ネットワークの要件によっては、ユーザがファイルへのアクセス前に認証を受ける必要があることもあります。
  - [HTTP Proxy] : クライアントへの HTTP アプレット プロキシの転送に関与します。このプロキシは、適切なコンテンツ変換に干渉するテクノロジー（Java、ActiveX、Flash など）に対して有用です。このプロキシによって、セキュリティ アプライアンスの使用を継続しながら、マングリングを回避できます。転送されたプロキシは、自動的にブラウザの古いプロキシ コンフィギュレーションを変更して、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTTP アプレット プロキシでは、HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。
  - [URL Entry] : ポータル ページでユーザが HTTP/HTTPS URL を入力できるようにするかどうかを設定します。この機能がイネーブルになっている場合、ユーザは URL エントリ ボックスに Web アドレスを入力できます。また、クライアントレス SSL VPN を使用して、これらの Web サイトにアクセスできます。

SSL VPN を使用しても、すべてのサイトとの通信が必ずしもセキュアになるとはかぎりません。SSL VPN は、リモート ユーザの PC またはワークステーションと、企業ネットワークのセキュリティ アプライアンスの間におけるデータ送信のセキュリティを確保します。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業のセキュリティ アプライアンスから目的の Web サーバまでの通信はセキュアではありません。

クライアントレス VPN 接続では、セキュリティ アプライアンスはエンド ユーザの Web ブラウザとターゲット Web サーバとの間のプロキシとして機能します。ユーザが SSL 対応 Web サーバに接続すると、セキュリティ アプライアンスはセキュアな接続を確立し、SSL 証明書を検証します。エンド ユーザ ブラウザでは提示された証明書を受信しないため、証明書を調査して検証することはできません。SSL VPN の現在の実装では、期限切れになった証明書を提示するサイトとの通信は許可されません。また、セキュリティ アプライアンスは、信頼できる CA 証明書の検証も実行しません。このため、ユーザは、SSL 対応の Web サーバと通信する前に、そのサーバにより提示された証明書を分析することはできません。

ユーザのインターネット アクセスを制限するには、[URL Entry] フィールドで [Disable] を選択します。これにより、SSL VPN ユーザはクライアントレス VPN 接続中に Web をサーフィンできなくなります。

- [Unchanged]：（デフォルト）クリックすると、このセッションに適用されるグループ ポリシーからの値が使用されます。
- [Enable/Disable]：機能をイネーブルにするかディセーブルにするかを指定します。
- [Auto-start]：クリックすると HTTP プロキシがイネーブルになり、これらの機能に関連付けられたアプレットが DAP レコードによって自動的に起動するようになります。

- [Port Forwarding Lists] タブ：ユーザ セッションのためのポート転送リストを選択して設定できます。

  ポート転送によりグループ内のリモート ユーザは、既知の固定 TCP/IP ポートで通信するクライアント/サーバ アプリケーションにアクセスできます。リモート ユーザは、ローカル PC にインストールされたクライアント アプリケーションを使用して、そのアプリケーションをサポートするリモート サーバに安全にアクセスできます。シスコでは、Windows Terminal Services、Telnet、Secure FTP（FTP over SSH）、Perforce、Outlook Express、および Lotus Notes についてテストしています。その他の TCP ベースのアプリケーションの一部も機能すると考えられますが、シスコではテストしていません。

（注） ポート転送は、一部の SSL/TLS バージョンでは使用できません。

注意 ポート転送（アプリケーション アクセス）およびデジタル証明書をサポートする Sun Microsystems Java™ Runtime Environment（JRE）1.4+ がリモート コンピュータにインストールされていることを確認します。

- [Port Forwarding]：この DAP レコードに適用されるポート転送リストのオプションを選択します。このフィールドのその他の属性は、[Port Forwarding] を [Enable] または [Auto-start] に設定した場合にだけイネーブルになります。
- [Unchanged]：クリックすると、属性が実行コンフィギュレーションから削除されます。
- [Enable/Disable]：ポート転送をイネーブルにするかディセーブルにするかを指定します。
- [Auto-start]：クリックするとポート転送がイネーブルになり、DAP レコードのポート転送リストに関連付けられたポート転送アプレットが自動的に起動するようになります。

  - [Port Forwarding List] ドロップダウン ボックス：DAP レコードに追加する、すでに設定済みのポート転送リストを選択します。
  - [New...]：新規のポート転送リストを設定するときにクリックします。
  - [Port Forwarding Lists]（ラベルなし）：DAP レコードのポート転送リストが表示されます。
  - [Add]：ドロップダウン ボックスから選択したポート転送リストを右側のポート転送リストに追加する場合にクリックします。
  - [Delete]：クリックすると、選択されているポート転送リストがポート転送リストから削除されます。セキュリティ アプライアンスからポート転送リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。
- [URL Lists] タブ：ユーザ セッションでの URL リストを選択して設定できます。
  - [Enable URL Lists]：イネーブルにします。このボックスが選択されていない場合は、接続のポータル ページに URL リストが表示されません。
  - [URL List] ドロップダウン ボックス：DAP レコードに追加する、設定済みの URL リストを選択します。
  - [Manage...]：URL リストを追加、インポート、エクスポート、および削除します。
  - [URL Lists]（ラベルなし）：DAP レコードの URL リストを表示します。
  - [Add]：ドロップダウン ボックスから選択した URL リストを右側の URL リスト ボックスに追加する場合にクリックします。
  - [Delete]：選択した URL リストを URL リスト ボックスから削除する場合にクリックします。セキュリティ アプライアンスから URL リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。
- [Access Method] タブ：許可するリモート アクセスのタイプを設定できます。
  - [Unchanged]：現在のリモート アクセス方式を引き続き使用します。
  - [AnyConnect Client]：Cisco AnyConnect VPN クライアントを使用して接続します。
  - [Web-Portal]：クライアントレス VPN で接続します。
  - [Both-default-Web-Portal]：クライアントレスまたは AnyConnect クライアントを介して接続します。デフォルトはクライアントレスです。
  - [Both default AnyConnect Client]：クライアントレスまたは AnyConnect クライアントを介して接続します。デフォルトは AnyConnect です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Add/Edit AAA Attributes

DAP レコードの選択基準として AAA 属性を設定するには、[Add/Edit AAA Attributes] ダイアログ ボックスで、使用する Cisco、LDAP、または RADIUS 属性を設定します。これらの属性は、入力する値に対して「=」または「!=」のいずれかに設定できます。各 DAP レコードに設定可能な AAA 属性の数に制限はありません。AAA 属性の詳細については、「AAA 属性の定義」を参照してください。

フィールド

- [AAA Attributes Type]：ドロップダウン ボックスを使用して、Cisco、LDAP、または RADIUS 属性を選択します。
- [Cisco]：AAA 階層モデルに保存されているユーザ許可属性を参照します。DAP レコードの AAA 選択属性に、これらのユーザ許可属性の小規模なサブセットを指定できます。次の属性が含まれます。
  - [Class]：ユーザに関連付けられた AAA グループ名。最大 64 文字です。
  - [IP Address]：割り当てられている IP アドレス。
  - [Member of]：ユーザに適用するグループ ポリシー名のカンマ区切り文字列。この属性により、複数のグループ メンバーシップを指定できます。最大 128 文字を入力できます。
  - [Tunnel Group]：接続名。最大 64 文字です。
  - [Username]：認証されたユーザのユーザ名。最大 64 文字です。
  - [=/!=]：と等しい / と等しくない
- [LDAP]：LDAP クライアントは、ユーザの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ LDAP 応答属性値のペアを保存します。LDAP クライアントでは、受信した順に応答属性をデータベースに書き込みます。その名前の後続の属性はすべて破棄されます。ユーザ レコードとグループ レコードの両方が LDAP サーバから読み込まれると、このシナリオが発生する場合があります。ユーザ レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

  Active Directory グループ メンバーシップをサポートするために、AAA LDAP クライアントでは、LDAP memberOf 応答属性に対する特別な処理が行われます。AD memberOf 属性は、AD 内のグループ レコードの DN 文字列を指定します。グループの名前は、DN 文字列内の最初の CN 値です。LDAP クライアントでは、DN 文字列からグループ名を抽出して、AAA memberOf 属性として格納し、応答属性データベースに LDAP memberOf 属性として格納します。LDAP 応答メッセージ内に追加の memberOf 属性が存在する場合、それらの属性からグループ名が抽出され、前の AAA memberOf 属性と結合されて、グループ名がカンマで区切られた文字列が生成されます。この文字列は応答属性データベース内で更新されます。

  LDAP 属性は、DAP レコード内の属性名と属性値のペアで構成されています。
- [RADIUS]：RADIUS クライアントは、ユーザの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ RADIUS 応答属性値のペアを保存します。RADIUS クライアントは、受け取った順序で応答属性をデータベースに書き込みます。その名前の後続の属性はすべて破棄されます。ユーザ レコードおよびグループ レコードの両方が RADIUS サーバから読み込まれた場合、このシナリオが発生する可能性があります。ユーザ レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

  RADIUS 属性は、DAP レコード内の属性番号と属性値のペアで構成されています。
- LDAP および RADIUS 属性には、次の値があります。
  - [Attribute ID]：属性の名前 / 番号。最大 64 文字です。
  - [Value]：
  - [=/!=]：と等しい / と等しくない

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

エンドポイント属性の追加および編集

エンドポイント属性には、エンドポイント システム環境、ポスチャ評価結果、およびアプリケーションに関する情報が含まれています。セキュリティ アプライアンスは、セッション中にエンドポイント属性の集合体を動的に生成し、それらの属性をセッションに関連付けられたデータベースに保存します。各 DAP レコードに設定可能なエンドポイント属性の数に制限はありません。

各 DAP レコードには、セキュリティ アプライアンスが DAP レコードを選択するために満たす必要があるエンドポイント選択属性が指定されます。セキュリティ アプライアンスは、設定されたすべての条件を満たす DAP レコードだけを選択します。

エンドポイント属性の詳細については、次のリンクをクリックしてください。

- エンドポイント属性の定義

エンドポイント属性を DAP レコードの選択基準として設定するには、[Add/Edit Endpoint Attribute] ダイアログボックスでコンポーネントを設定します。これらのコンポーネントは、選択する属性のタイプに応じて異なります。

フィールド

- [Endpoint Attribute Type]：設定するエンドポイント属性をドロップダウン リストから選択します。[Antispyware]、[Antivirus]、[Application]、[File]、[NAC]、[Operating System]、[Personal Firewall]、[Process]、[Registry]、[VLAN]、および [Priority] から選択できます。

エンドポイント属性にはこれらのコンポーネントがありますが、すべての属性にすべてのコンポーネントが含まれているわけではありません。次の説明では、各コンポーネントが適用される属性を括弧で囲んで示しています。

- [Exists/Does not exist] ボタン（[Antispyware]、[Antivirus]、[Application]、[File]、[NAC]、[Operating System]、[Personal Firewall]、[Process]、[Registry]、[VLAN]、[Priority]）：適切なボタンをクリックして、選択したエンドポイント属性とそれに伴う修飾子（[Exists/Does not exist] ボタン下のフィールド）を表示するかどうかを指定します。
- [Vendor ID]（[Antispyware]、[Antivirus]、[Personal Firewall]）：アプリケーション ベンダーの ID です。
- [Vendor Description]（[Antispyware]、[Antivirus]、[Personal Firewall]）：アプリケーション ベンダーの説明をテキストで入力します。
- [Version]（[Antispyware]、[Antivirus]、[Personal Firewall]）：アプリケーションのバージョンを特定し、エンドポイント属性をそのバージョンと等しくするかどうかを指定します。
- [Last Update]（[Antispyware]、[Antivirus]、[File]）：最後の更新時からの経過日数を指定します。更新を、ここで入力した日数よりも早く（[<]）実行するか、遅く（[>]）実行するかを指定できます。

- [Client Type]（[Application]）：リモート アクセス接続のタイプを、AnyConnect、Clientless、Cut-through Proxy、IPsec、または L2TP から指定します。
- [Checksum]（File）：ファイルを選択し、[Compute Checksum] ボタンをクリックしてこの値を求めます。
- [Compute CRC32 Checksum]（File）：このカルキュレータを使用してファイルのチェックサム値を求めます。
- [Posture Status]（NAC）：ACS から受け取るポスチャ トークン文字列が含まれています。
- [OS Version]（Operating System）：Windows（複数のバージョン）、MAC、Linux、Pocket PC。
- [Service Pack]（Operating System）：オペレーティング システムのサービス パックを指定します。
- [Endpoint ID]（[File]、[Process]、[Registry]）：ファイル、プロセス、またはレジストリ エントリのエンドポイントを識別する文字列。DAP は、この ID を使用して、DAP 選択で Cisco Secure Desktop ホスト スキャン属性を照合します。この属性を設定する前に、[Host Scan] を設定する必要があります。[Host Scan] を設定した場合は設定がこのペインに表示されるため、設定を選択して、入力エラーまたは構文エラーの可能性を低減できます。
- [Path]（[Process]、[Policy]）：この属性を設定する前に Host Scan を設定します。[Host Scan] を設定した場合は設定がこのペインに表示されるため、設定を選択して、入力エラーまたは構文エラーの可能性を低減できます。
- [Value]（[Registry]）：dword または文字列。
- [Caseless]（[Registry]）：レジストリ エントリの大文字と小文字を区別しない場合に選択します。
- [VLAN ID]（[VLAN]）：1 ～ 4094 の範囲の有効な 802.1q 番号。
- [VLAN Type]（[VLAN]）：次の値を指定できます。

ACCESS	ポスチャ評価合格
STATIC	適用するポスチャ評価なし
TIMEOUT	応答がないためにポスチャ評価失格
AUTH	ポスチャ評価は依然アクティブ
GUEST	ポスチャ評価合格、ゲスト VLAN に切り替え
QUARANTINE	ポスチャ評価失格、隔離 VLAN に切り替え
ERROR	重大エラーのためにポスチャ評価失格

- [Policy]（[Location]）：Cisco Secure Desktop Microsoft Windows のロケーション プロファイルを、大文字と小文字を区別して入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

ガイド

この項では、AAA またはエンドポイント属性の論理式の作成方法について説明します。これを行うには、LUA（www.lua.org）についての高度な知識が必要になります。

テキスト ボックスに、AAA またはエンドポイント、あるいはその両方の選択論理演算を表す自由形式の LUA テキストを入力します。ASDM は、ここで入力されるテキストを検証せず、このテキストを単に DAP ポリシー ファイルにコピーするだけです。セキュリティ アプライアンスがそれを処理し、解析不能な式があれば破棄されます。

このオプションは、上の説明にある AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加する場合に有効です。たとえば、指定された条件のいずれかまたはすべてを満たす、あるいはいずれも満たさない AAA 属性を使用するようにセキュリティ アプライアンスを設定できます。エンドポイント属性は累積され、すべて満たす必要があります。セキュリティ アプライアンスが任意のエンドポイント属性を使用できるようにするには、LUA で適切な論理式を作成し、ここでその式を入力する必要があります。

- 論理式を作成する場合の正しい名前の構文を含む AAA 選択属性のリストについては、表 33-1 を参照してください。
- 論理式を作成する場合の正しい名前の構文を含むエンドポイント選択属性のリストについては、表 33-3 を参照してください。

DAP 論理式の例

LUA で論理式を作成する場合は、次の例を参考にしてください。

- この AAA LUA 式は、「b」で始まるユーザ名に一致するかどうかをテストします。この式では、ストリング ライブラリおよび正規表現を使用しています。

```
not(string.find(aaa.cisco.username, "^b") == nil)
```

- このエンドポイント式は、CLIENTLESS または CVC クライアント タイプに一致するかどうかをテストします。

```
endpoint.application.clienttype=="CLIENTLESS" or
endpoint.application.clienttype=="CVC"
```

- このエンドポイント式は、Norton Antivirus バージョン 10.x かどうかをテストしますが、10.5.x は除外します。

```
(endpoint.av.NortonAV.version > "10" and endpoint.av.NortonAV.version < "10.5") or
endpoint.av.NortonAV.version > "10.6"
```

Operator for Endpoint Category

各タイプのエンドポイントのインスタンスを複数設定できます。このペインでは、あるタイプのインスタンスを 1 つだけ必要とする（Match Any = OR）ように、またはあるタイプのインスタンスのすべてを持つ（Match All = AND）ように、各タイプのエンドポイントを設定します。

- エンドポイント カテゴリの 1 つのインスタンスだけを設定する場合、値を設定する必要はありません。
- 一部のエンドポイント属性の場合は、複数のインスタンスを設定しても意味がありません。たとえば、複数の OS を実行するユーザがいない場合、などです。
- 各エンドポイント タイプ内に [Match Any]/[Match All] 操作を設定するとします。

この場合、セキュリティ アプライアンスは、エンドポイント属性の各タイプを評価したあと、設定されたすべてのエンドポイントで論理 AND 演算を実行します。つまり、各ユーザは、AAA 属性だけでなく、設定したエンドポイントのすべての条件を満たす必要があります。

DAP の例

次の各項に、便利なダイナミック アクセス ポリシーの例を示します。

DAP を使用したネットワーク リソースの定義

この例は、ユーザまたはグループのネットワーク リソースを定義する方法として、ダイナミック アクセス ポリシーを設定する方法を示しています。Trusted_VPN_Access という名前の DAP ポリシーは、クライアントレス VPN アクセスと AnyConnect VPN アクセスを許可します。Untrusted_VPN_Access という名前のポリシーは、クライアントレス VPN アクセスだけを許可します。表 33-4 に、これらのポリシーそれぞれのコンフィギュレーションをまとめています。

ASDM パスは、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [Endpoint] です。

表 33-4　ネットワーク リソースの簡単な DAP コンフィギュレーション

属性	Trusted_VPN_Access	Untrusted_VPN_Access
Endpoint Attribute Type Policy	信頼できる	信頼できない
Endpoint Attribute Process	ieexplore.exe	—
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	信頼できる	信頼できない
LDAP memberOf	Engineering、Managers	ベンダー
ACL		Web-Type ACL
Access	**AnyConnect** ***および*** **Web Portal**	**Web Portal**

DAP を使用した WebVPN ACL の適用

DAP では、Network ACLs（IPsec および AnyConnect の場合）、Clientless SSL VPN Web-Type ACLs、URL リスト、および Functions を含め、アクセス ポリシー属性のサブセットを直接適用できます。グループ ポリシーが適用されるバナーまたはスプリット トンネル リストなどには、直接適用できません。[Add/Edit Dynamic Access Policy] ペインの [Access Policy Attributes] タブには、DAP が直接適用される属性の完全なメニューが表示されます。

Active Directory/LDAP は、ユーザ グループ ポリシー メンバーシップをユーザ エントリの「memberOf」属性として保存します。DAP は、AD グループ（memberOf）のユーザ = セキュリティ アプライアンスが設定済み Web-Type ACL を適用する Engineering となるように定義できます。このタスクを完了するには、次の手順を実行します。

ステップ 1　[Add AAA Attributes] ペイン（[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [AAA Attributes] セクション > [Add AAA Attribute]）に移動します。

ステップ 2　AAA 属性タイプとしては、ドロップダウン メニューを使用して [LDAP] を選択します。

ステップ 3　[Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 4　[Value] フィールドで、ドロップダウン メニューを使用して [=] を選択し、隣のテキスト ボックスに「Engineering」と入力します。

ステップ 5　ペインの [Access Policy Attributes] 領域で、[Web-Type ACL Filters] タブをクリックします。

ステップ 6　[Web-Type ACL] ドロップダウン メニューを使用して、AD グループ（memberOf）= Engineering のユーザに適用する ACL を選択します。

CSD チェックの強制と DAP によるポリシーの適用

この例では、ユーザが 2 つの特定 AD/LDAP グループ（Engineering および Employees）と 1 つの特定 ASA トンネル グループに属することをチェックする DAP を作成します。その後、ACL をユーザに適用します。

DAP が適用される ACL により、リソースへのアクセスを制御します。それらは、セキュリティ アプライアンスのグループ ポリシーで定義されるどの ACL よりも優先されます。またセキュリティ アプライアンスは、スプリット トンネリング リスト、バナー、および DNS など、DAP で定義または制御しない要素の通常の AAA グループ ポリシー継承ルールおよび属性を適用します。

ステップ 1　[Add AAA Attributes] ペイン（[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [AAA Attributes] セクション > [Add AAA Attribute]）に移動します。

ステップ 2　AAA 属性タイプとしては、ドロップダウン メニューを使用して [LDAP] を選択します。

ステップ 3　[Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 4　[Value] フィールドで、ドロップダウン メニューを使用して [=] を選択し、隣のテキスト ボックスに「Engineering」と入力します。

ステップ 5　[Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 6　[Value] フィールドで、ドロップダウン メニューを使用して [=] を選択し、隣のテキスト ボックスに「Employees」と入力します。

ステップ 7　AAA 属性タイプとしては、ドロップダウン メニューを使用して [Cisco] を選択します。

ステップ 8　[Tunnel] グループ ボックスをオンにし、ドロップダウン メニューを使用して [=] を選択し、隣のドロップダウン ボックスで適切なトンネル グループ（接続ポリシー）を選択します。

ステップ 9　[Access Policy Attributes] 領域の [Network ACL Filters] タブで、前のステップで定義した DAP 基準を満たすユーザに適用する ACL を選択します。

CHAPTER 34

クライアントレス SSL VPN

クライアントレス SSL VPN によってユーザは、Web ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェアまたはハードウェア クライアントは必要ありません。クライアントレス SSL VPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースと、Web 対応およびレガシー アプリケーションに簡単にアクセスできます。クライアントレス SSL VPN は Secure Sockets Layer（SSL）プロトコルおよびその後継の Transport Layer Security（SSL/TLS1）を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。セキュリティ アプライアンスはプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ネットワーク管理者は、ユーザまたはグループ単位でネットワーク リソースへのアクセスを提供します。ユーザは、これらのリソースに直接アクセスすることはできません。

クライアントレス SSL VPN は、プラットフォームにて、シングル ルーテッド モードで動作します。

エンド ユーザ向けのクライアントレス SSL VPN の設定方法については、「クライアントレス SSL VPN のエンド ユーザ設定」を参照してください。

セキュリティ対策

セキュリティ アプライアンス上のクライアントレス SSL VPN 接続は、リモート アクセス IPSec 接続とは異なっています。特に SSL 対応サーバとの対話方法やセキュリティ上のリスクを減らすための対策に違いがあります。

クライアントレス SSL VPN 接続では、セキュリティ アプライアンスは、エンド ユーザの Web ブラウザとターゲット Web サーバとの間のプロキシとして機能します。ユーザが SSL 対応 Web サーバに接続すると、セキュリティ アプライアンスはセキュアな接続を確立し、SSL 証明書を検証します。ブラウザは提示された SSL 証明書を受信しないため、この証明書を検証することはできません。

セキュリティ アプライアンス上の現在のクライアントレス SSL VPN 実装では、有効期限が切れた証明書を提示するサイトとの通信は許可されません。また、セキュリティ アプライアンスは、それらの SSL 対応サイトに対して信頼できる CA 証明書の検証も実行しません。このため、Web 対応サービスで使用する前に、SSL 対応 Web サーバが配信するページの証明書を検証することによるメリットは、ユーザにはありません。

注意 デフォルトでは、セキュリティ アプライアンスはすべての Web リソース（HTTPS、CIFS、RDP、およびプラグイン）に対するすべてのポータル トラフィックを許可します。セキュリティ アプライアンス クライアントレス サービスは、各 URL をそれ自体だけに意味のあるものに書き換えます。ユーザは、要求したサイト上にあることを確認するためにアクセスしたページに表示される、その書き換えられた URL を使用できません。ユーザを危険にさらさないようにするために、クライア

ントレス アクセス用に設定されたポリシー（グループ ポリシー、ダイナミック アクセス ポリシー、またはその両方）に Web ACL を割り当てて、ポータルからのトラフィック フローを制御してください。たとえば、このような ACL がないと、ユーザは不正な銀行や商用サイトからの認証要求を受け取る可能性があります。また、これらのポリシー上の URL エントリをディセーブルにして、ユーザがアクセスできるページについて混乱しないようにすることをお勧めします。クライアントレス SSL VPN アクセスにより引き起こされるリスクを最小限に抑えるためには、次のことを実行することをお勧めします。

ステップ 1　クライアントレス SSL VPN アクセスを必要とするすべてのユーザにグループ ポリシーを設定し、そのグループ ポリシーに対してだけクライアントレス SSL VPN をイネーブルにします。

ステップ 2　グループ ポリシーを開き、[General] > [More Options] > [Web ACL] を選択して [Manage] をクリックします。プライベート ネットワーク内の特定のターゲットへのアクセスだけを許可する、プライベート ネットワークへのアクセスだけを許可する、インターネット アクセスを拒否する、または信頼できるサイトへのアクセスだけを許可する Web ACL を作成します。クライアントレス アクセス用に設定しているすべてのポリシー（グループ ポリシー、ダイナミック アクセス ポリシー、またはその両方）に Web ACL を適用します。DAP 上では、[Network ACL Filters] タブでネットワーク ACL を選択します。

ステップ 3　ユーザがブラウザベースの接続を確立するときに表示される *ポータル* ページ上の URL エントリをディセーブルにします。そのためには、グループ ポリシーのポータル フレームと DAP の [Functions] タブの両方で、[URL Entry] の横にある [Disable] をクリックします。

ステップ 4　ユーザに、ポータル ページの上のネイティブ ブラウザの Address フィールドに外部 URL を入力するか、別のブラウザ ウィンドウを開いて、外部サイトにアクセスするかを指示します。

クライアントレス SSL VPN のシステム要件について

クライアントレス SSL VPN は、次の OS とブラウザからのアクセスをサポートしています。

OS	ブラウザと Java バージョン	機能に関する注意事項[1]
Windows Vista SP2 KB952876 を適用した Vista SP1 以降	Microsoft Internet Explorer 7 Firefox 2.0 以降	Windows Vista は、Windows Shares（CIFS）Web フォルダをサポートしていません。 追加の要件と制限事項が、スマート トンネルとポート転送に適用されます。
Windows XP SP2 以降	Microsoft Internet Explorer 7 および 6 Firefox 2.0 以降	Windows XP SP2 以降で Web フォルダをサポートするには、Microsoft KB892211 修正プログラムが必要です。 追加の要件と制限事項が、スマート トンネルとポート転送に適用されます。
Windows 2000 SP4	Microsoft Internet Explorer 7 および 6 Firefox 2.0 以降	Windows Vista は、Windows Shares（CIFS）Web フォルダをサポートしていません。 Windows 2000 SP4 では、Web フォルダをサポートするために Microsoft KB892211 ホットフィックスが必要です。 追加の要件と制限事項が、スマート トンネルとポート転送に適用されます。

OS	ブラウザと Java バージョン	機能に関する注意事項[1]
Apple：Mac OS X 10.4 および 10.5	Safari 2.0 以降、または Firefox 2.0 以降	DoD Common Access Card および SmartCard を含む証明書認証は、Safari キーチェーンだけで動作します。 Web フォルダは Mac OS をサポートしていません。 追加の要件と制限事項が、スマート トンネルとポート転送に適用されます。
Linux	Firefox 2.0 以降	Web フォルダとスマート トンネルは Linux をサポートしていません。 追加の要件がポート転送に適用されます。

1. MAPI プロトコルを使用した Microsoft Outlook Exchange 通信では、リモート ユーザが AnyConnect を使用する必要があります。

ActiveX ページでは、関連するポリシー グループに対する ActiveX リレーのデフォルト設定（イネーブル）を使用する必要があります。あるいは、スマート トンネル リストをポリシーに割り当て、エンドポイント上のブラウザ プロキシ例外リストにプロキシが指定されている場合、ユーザはそのリストに「shutdown.webvpn.relay.」エントリを追加する必要があります。

Windows 7、Vista、Internet Explorer 8、Mac OS、および Linux では、クライアントレス SSL VPN アクセスで Windows Shares（CIFS）Web フォルダがサポートされていません。Windows XP SP2 で Web フォルダをサポートするには、Microsoft 社が提供するホットフィックスが必要です。

ASA は DSA 証明書をサポートしていません。サポートしているのは RSA 証明書です。

次の名前のクライアントレス アプリケーションでサポートされているプラットフォームについては、以降のセクションを参照してください。

- 「ポート転送の要件と制限事項」（P.34-23）
- 「スマート トンネルの要件および制限」（P.34-42）
- 「プラグインの要件および制限事項」（P.34-75）

ACL

ユーザ セッションに適用する ACL（アクセス コントロール リスト）を設定できます。ACL は、特定のネットワーク、サブネット、ホスト、および Web サーバへのユーザ アクセスを許可または拒否するフィルタです。

- フィルタを定義しない場合は、すべての接続が許可されます。
- セキュリティ アプライアンスは、インターフェイスのインバウンド ACL だけをサポートします。
- 各 ACL の最後には、許可されないすべてのトラフィックを拒否する、表記されない暗黙のルールが含まれます。トラフィックがアクセス コントロール エントリ（ACE）によって明示的に許可されていない場合には、セキュリティ アプライアンスがそのトラフィックを拒否します。このトピックでは、ACE をルールと呼びます。

このペインでは、クライアントレス SSL VPN セッションで使用される ACL、および各 ACL に含まれる ACL エントリを追加および編集できます。また、このペインには ACL と ACE に関する要約情報が表示され、それらをイネーブルまたはディセーブルにしたり、プライオリティ順を変更したりすることもできます。

フィールド

- [Add ACL] : ACL または ACE を追加する場合にクリックします。既存の ACE の前後に新しい ACE を挿入するには、[Insert] または [Insert After] をクリックします。
- [Edit] : 選択されている ACE を編集する場合にクリックします。ACL を削除すると、その ACE もすべて削除されます。警告は表示されず、復元もできません。
- [Delete] : 選択されている ACL または ACE を削除する場合にクリックします。ACL を削除すると、その ACE もすべて削除されます。警告は表示されず、復元もできません。
- [Move UP/Move Down] : ACL または ACE を選択してこれらのボタンをクリックすると、ACL および ACE の順序が変更されます。セキュリティ アプライアンスは、一致するエントリを見つけるまで、ACL リスト内での位置の順に、クライアントレス SSL VPN セッションに適用される ACL およびその ACE をチェックします。
- [+/-] : 各 ACL 下の ACE のリストを展開したり（+）折りたたんだり（-）して、表示または非表示にする場合にクリックします。
- [No] : 各 ACL 下の ACE の優先順位を表示します。リスト内での順序によって優先順位が決まります。
- [Enabled] : ACE がイネーブルになっているかどうかを表示します。ACE は、作成されるとデフォルトでイネーブルになります。ACE をディセーブルにするには、チェックボックスをオフにします。
- [Address] : ACE が適用されるアプリケーションまたはサービスの IP アドレスまたは URL を表示します。
- [Service] : ACE が適用される TCP サービスを表示します。
- [Action] : ACE でクライアントレス SSL VPN アクセスが許可または拒否されているかどうかを表示します。
- [Time] : ACE に関連付けられている時間範囲を表示します。
- [Logging (Interval)] : 設定されているロギング動作を表示します。ディセーブルにするか、指定されたレベルと間隔で表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add ACL

このペインでは、新規 ACL を作成できます。

フィールド

- [ACL Name] : ACL の名前を入力します。最大 55 文字です。

Add/Edit ACE

アクセス コントロール エントリは、特定の URL およびサービスへのアクセスを許可または拒否します。ACL に対して、複数の ACE を設定できます。ACL は、初回一致ルールに従って、優先順位に応じて ACE を適用します。

フィールド

- [Action] : [Filter] グループ ボックスで指定されている特定のネットワーク、サブネット、ホスト、および Web サーバへのユーザ アクセスを許可または拒否します。
- [Filter] : フィルタを適用する（ユーザ アクセスを許可または拒否する）URL または IP アドレスを指定します。
  - [URL] : 指定された URL にフィルタを適用します。
  - [Protocols (unlabeled)] : URL アドレスのプロトコル部分を指定します。
  - [://x] : フィルタを適用する Web ページの URL を指定します。
  - [TCP] : 指定された IP アドレス、サブネット、およびポートにフィルタを適用します。
  - [IP Address] : フィルタを適用する IP アドレスを指定します。
  - [Netmask] : [IP Address] ボックス内のアドレスに適用する標準サブネット マスクを一覧表示します。
  - [Service] : 一致するサービス（https や Kerberos など）を特定します。[Service] ボックスに表示するサービスの選択元サービスの一覧を表示します。
  - [Boolean operator]（ラベルなし）: [Service] ボックスで指定したサービスを照合するときに使用するブーリアン条件（等号、不等号、大なり、小なり、または範囲）を一覧表示します。
- [Rule Flow Diagram] : このフィルタを使用して、トラフィックをグラフィカルに描写します。この領域は非表示の場合もあります。
- [Options] : ロギング ルールを指定します。デフォルトは Default Syslog です。
  - [Logging] : 特定のログレベルをイネーブルにする場合は、[enable] を選択します。
  - [Syslog Level] : Logging 属性に対して [Enable] を選択するまではグレー表示です。セキュリティ アプライアンスが表示する syslog メッセージの種類を選択できます。
  - [Log Interval] : ログ メッセージ間の秒数を選択できます。
  - [Time Range] : 事前定義済みの時間範囲パラメータ セットの名前を選択できます。
  - [...] : 設定済みの時間範囲を参照する場合や、新たに追加する場合にクリックします。

例

クライアントレス SSL VPN の ACL の例を次に示します。

アクション	フィルタ	影響
拒否	url http://*.yahoo.com/	Yahoo! すべてへのアクセスを拒否します。
拒否	url cifs://fileserver/share/directory	指定された場所にあるすべてのファイルへのアクセスを拒否します。
拒否	url https://www.company.com/ directory/file.html	指定されたファイルへのアクセスを拒否します。

アクション	フィルタ	影響
許可	url https://www.company.com/directory	指定された場所へのアクセスを許可します。
拒否	url http://*:8080/	ポート 8080 を介した任意の場所への HTTPS アクセスを拒否します。
拒否	url http://10.10.10.10	10.10.10.10 への HTTP アクセスを拒否します。
許可	url any	任意の URL へのアクセスを許可します。通常は、url アクセスを拒否する ACL のあとに使用されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Cisco Secure Desktop の設定

Cisco Secure Desktop イメージがセキュリティ アプライアンスにインストールされている場合は、そのイメージのバージョンと状態が Cisco Secure Desktop Setup ウィンドウに表示され、イネーブルになっているかどうかが示されます。また、セキュリティ アプライアンスには、Cisco Secure Desktop および SSL VPN Client を保持するためのキャッシュのサイズも表示されます。

次のようにして、ウィンドウのボタンを使用できます。

- Cisco Secure Desktop イメージのコピーを、ローカル コンピュータからセキュリティ アプライアンスのフラッシュ デバイスに転送するには、[Upload] をクリックします。

  Cisco Secure Desktop のインストールまたはアップグレードの準備をするには、インターネット ブラウザを使用して、http://www.cisco.com/cisco/software/navigator.html から自分の PC の任意の場所に、securedesktop_asa_<*n*>_<*n*>*.pkg ファイルをダウンロードします。次に、このボタンを使用して、そのファイルをローカル コンピュータからフラッシュ デバイスに転送します。[Browse Flash] をクリックして、実行コンフィギュレーションにインストールします。最後に、[Enable Secure Desktop] をオンにします。
- セキュリティ アプライアンス のフラッシュ デバイスにある Cisco Secure Desktop イメージをインストールしたり、置き換えたりするには、[Browse Flash] をクリックします。

（注）　[Browse Flash] ボタンをクリックして Cisco Secure Desktop イメージをアップグレードまたはダウングレードし、インストールするパッケージを選択して [OK] をクリックすると、[Uninstall Cisco Secure Desktop] ダイアログ ウィンドウが表示され、現在実行コンフィギュレーションにある Cisco Secure Desktop ディストリビューションをフラッシュ デバイスから削除するかどうか尋ねられます。フラッシュ デバイスのスペースを節約する場合は [Yes] をクリックします。このオプションを残してこのバージョンの Cisco Secure Desktop に戻す場合は [No] をクリックします。

- 実行コンフィギュレーションから Cisco Secure Desktop イメージとコンフィギュレーション ファイル（sdesktop/data.xml）を削除するには、[Uninstall] をクリックします。

  このボタンをクリックすると、[Uninstall Cisco Secure Desktop] ダイアログ ウィンドウが表示され、「[Secure Desktop Image] フィールド」で命名された Cisco Secure Desktop イメージと、すべての Cisco Secure Desktop データ ファイル（Cisco Secure Desktop コンフィギュレーション全体を含む）をフラッシュ デバイスから削除するかどうか尋ねられます。これらのファイルを実行コンフィギュレーションとフラッシュ デバイスの両方から削除する場合は、[Yes] をクリックします。これらのファイルを実行コンフィギュレーションから削除するが、フラッシュ デバイスには残しておく場合は、[No] をクリックします。

フィールド

[Cisco Secure Desktop Setup] ペインに次のフィールドが表示されます。

- [Secure Desktop Image]：実行コンフィギュレーションにロードされた Cisco Secure Desktop イメージを表示します。デフォルトでのファイル名の形式は、securedesktop_asa_<n>_<n>*.pkg です。このフィールドに値を挿入したり、値を編集したりするには、[Browse Flash] をクリックします。
- [Enable Secure Desktop]：次の処理を実行するには、オンにして、[Apply] をクリックします。
  a. ファイルが有効な Cisco Secure Desktop イメージであることを確認する。
  b. 「sdesktop」フォルダが disk0 に存在しない場合には作成する。
  c. data.xml（Cisco Secure Desktop コンフィギュレーション）ファイルがまだ存在しない場合には、そのファイルを sdesktop フォルダに挿入する。
  d. data.xml ファイルを実行コンフィギュレーションにロードする。

  （注）　data.xml ファイルを転送または置換する場合は、Cisco Secure Desktop を一度ディセーブルにし、その後再びイネーブルにしてファイルをロードします。

  e. Cisco Secure Desktop をイネーブルにする。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Upload Image

[Upload Image] ダイアログボックスでは、Cisco Secure Desktop イメージのコピーをローカル コンピュータからセキュリティ アプライアンスのフラッシュ デバイスに転送できます。このウィンドウを使用して、Cisco Secure Desktop をインストールまたはアップグレードします。

（注）　このウィンドウを使用する前に、インターネット ブラウザを使用して、http://www.cisco.com/cisco/software/navigator.html からローカル コンピュータの任意の場所に securedesktop_asa_<*n*>_<*n*>*.pkg ファイルをダウンロードしてください。

次のようにして、ウィンドウのボタンを使用できます。

- 転送する securedesktop_asa_<*n*>_<*n*>*.pkg ファイルのパスを選択するには、[Browse Local Files] をクリックします。[Selected File Path] ダイアログボックスに、自分のローカル コンピュータで最後にアクセスしたフォルダの内容が表示されます。securedesktop_asa_<*n*>_<*n*>*.pkg ファイルのある場所に移動し、そのファイルを選択して [Open] をクリックします。
- ファイルのターゲット ディレクトリを選択するには、[Browse Flash] をクリックします。[Browse Flash] ダイアログボックスに、フラッシュ カードの内容が表示されます。
- ローカル コンピュータからフラッシュ デバイスに securedesktop_asa_<*n*>_<*n*>*.pkg ファイルをアップロードするには、[Upload File] をクリックします。[Status] ウィンドウが表示され、ファイル転送中は開いたままの状態を維持します。転送が終わり、[Information] ウィンドウに「File is uploaded to flash successfully.」というメッセージが表示されたら、[OK] をクリックします。[Upload Image] ダイアログ ウィンドウから、[Local File Path] フィールドと [Flash File System Path] フィールドの内容が削除されます。
- [Upload Image] ダイアログ ウィンドウを閉じるには、[Close] をクリックします。このボタンは、Cisco Secure Desktop イメージをフラッシュ デバイスにアップロードした後に、またはイメージをアップロードしない場合にクリックしてください。アップロードした場合には、[Cisco Secure Desktop Setup] ウィンドウの [Secure Desktop Image] フィールドにそのファイル名が表示されます。アップロードしなかった場合には、「Are you sure you want to close the dialog without uploading the file?」と尋ねる [Close Message] ダイアログボックスが表示されます。ファイルをアップロードしない場合は、[OK] をクリックします。[Close Message] ダイアログボックスと [Upload Image] ダイアログボックスが閉じられ、[Cisco Secure Desktop Setup] ペインが表示されます。この処理が実行されない場合は、[Close Message] ダイアログボックスの [Cancel] をクリックします。ダイアログボックスが閉じられ、フィールドの値がそのままの状態で [Upload Image] ダイアログボックスが再度表示されます。[Upload File] をクリックします。

フィールド

[Upload Image] ダイアログボックスには、次のフィールドが表示されます。

- [Local File Path]：ローカル コンピュータでの、securedesktop_asa_<*n*>_<*n*>*.pkg ファイルへのパスを指定します。[Browse Local] をクリックしてこのフィールドにパスを自動的に挿入するか、パスを入力します。次の例を参考にしてください。

  D:\Documents and Settings*Windows_user_name*.AMER\My Documents\My Downloads\securedesktop_asa_3_1_1_16.pkg

  ASDM が [Local File Path] フィールドにファイルのパスを挿入します。
- [Flash File System Path]：セキュリティ アプライアンスのフラッシュ デバイス上のアップロード先パスと、対象ファイルの名前を指定します。[Browse Flash] をクリックしてこのフィールドにパスを自動的に挿入するか、パスを入力します。次に例を示します。

  disk0:/securedesktop_asa_3_1_1_16.pkg

- [File Name]：このフィールドは、[Browse Flash] をクリックした場合に表示される [Browse Flash] ダイアログボックスに配置されており、ローカル コンピュータで選択した Cisco Secure Desktop イメージの名前が表示されます。混乱を防ぐために、この名前を使用することをお勧めします。このフィールドに、選択したローカル ファイルと同じ名前が表示されていることを確認し、[OK] をクリックします。[Browse Flash] ダイアログボックスが閉じます。ASDM が [Flash File System Path] フィールドにアップロード先のファイル パスを挿入します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Application Helper の設定

クライアントレス SSL VPN に組み込まれているアプリケーション プロファイル カスタマイゼーション フレームワーク オプションにより、セキュリティ アプライアンス は標準以外のアプリケーションや Web リソースを処理し、クライアントレス SSL VPN 接続で正しく表示できます。APCF プロファイルには、特定のアプリケーションに関して、いつ（事前、事後）、どこの（ヘッダー、本文、要求、応答）、どのデータを変換するかを指定するスクリプトがあります。スクリプトは XML 形式で記述され、sed（ストリーム エディタ）の構文を使用して文字列およびテキストを変換します。

一般的には、Cisco TAC によって APCF を書き込んで適用できます。

APCF プロファイルは、セキュリティ アプライアンス上で数種類を同時に実行するように設定できます。1 つの APCF プロファイルのスクリプト内に複数の APCF ルールを適用することができます。この場合、セキュリティ アプライアンスは、設定履歴に基づいて最も古いルールを最初に処理し、次に 2 番目に古いルール、その次は 3 番目という順序で処理します。

APCF プロファイルは、セキュリティ アプライアンスのフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバに保存できます。このパネルは、APCF パッケージを追加、編集、および削除する場合と、パッケージを優先順位に応じて並べ替える場合に使用します。

フィールド

- [APCF File Location]：APCF パッケージの場所についての情報を表示します。セキュリティ アプライアンスのフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバのいずれかです。
- [Add/Edit]：新規または既存の APCF プロファイルを追加または編集します。
- [Delete]：既存の APCF プロファイルを削除します。確認されず、やり直しもできません。
- [Move Up]：リスト内の APCF プロファイルを再配置します。リストにより、セキュリティ アプライアンスが APCF プロファイルを使用するときの順序が決まります。

Add/Edit APCF Profile

このパネルでは、APCF パッケージを追加または編集できます。この作業を行うに当たっては、パッケージの場所を特定します。場所は、セキュリティ アプライアンスのフラッシュ メモリの場合もあれば、HTTP サーバ、HTTPS サーバ、または TFTP サーバの場合もあります。

フィールド

- [Flash file]：セキュリティ アプライアンスのフラッシュ メモリに保存されている APCF ファイルを指定する場合にオンにします。
- [Path]：ユーザがフラッシュ メモリに格納されている APCF ファイルを指定するために参照した後、そのファイルへのパスを表示します。このフィールドにパスを手動で入力することもできます。
- [Browse Flash]：フラッシュ メモリを参照して APCF ファイルを指定します。[Browse Flash Dialog] パネルが表示されます。[Folders] および [Files] 列を使用して APCF ファイルを指定します。APCF ファイルを選択して、[OK] をクリックします。ファイルへのパスが [Path] フィールドに表示されます。

（注） 最近ダウンロードした APCF ファイルの名前が表示されない場合には、[Refresh] ボタンをクリックします。

- [Upload]：APCF ファイルをローカル コンピュータからセキュリティ アプライアンスのフラッシュ ファイル システムにアップロードします。[Upload APCF package] ペインが表示されます。
- [URL]：HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存されている APCF ファイルを使用する場合にオンにします。
- [ftp, http, https, and tftp (unlabeled)]：サーバ タイプを特定します。
- [URL (unlabeled)]：FTP、HTTP、HTTPS、または TFTP サーバへのパスを入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Upload APCF package

フィールド

- [Local File Path]：コンピュータ上にある APCF ファイルへのパスを表示します。[Browse Local] をクリックしてこのフィールドにパスを自動的に挿入するか、パスを入力します。
- [Browse Local Files]：自分のコンピュータ上の転送する APCF ファイルを指定および選択します。[Select File Path] ダイアログボックスに、自分のローカル コンピュータで最後にアクセスしたフォルダの内容が表示されます。APCF ファイルに移動して選択し、[Open] をクリックします。ASDM が [Local File Path] フィールドにファイルのパスを挿入します。
- [Flash File System Path]：APCF ファイルをアップロードするセキュリティ アプライアンス上のパスを表示します。
- [Browse Flash]：APCF ファイルをアップロードするセキュリティ アプライアンス上の場所を特定します。[Browse Flash] ダイアログボックスに、フラッシュ メモリの内容が表示されます。

- [File Name]：このフィールドは、[Browse Flash] をクリックしたときに表示される [Browse Flash] ダイアログボックスにあり、ローカル コンピュータで選択した APCF ファイルの名前を表示します。混乱を防ぐために、この名前を使用することをお勧めします。このファイルの名前が正しく表示されていることを確認し、[OK] をクリックします。[Browse Flash] ダイアログボックスが閉じます。ASDM が [Flash File System Path] フィールドにアップロード先のファイル パスを挿入します。
- [Upload File]：自分のコンピュータの APCF ファイルの場所と、APCF ファイルをセキュリティ アプライアンスにダウンロードする場所を特定します。
- [Status] ウィンドウが表示され、ファイル転送中は開いたままの状態を維持します。転送が終わり、[Information] ウィンドウに「File is uploaded to flash successfully.」というメッセージが表示されたら、[OK] をクリックします。[Upload Image] ダイアログ ウィンドウから、[Local File Path] フィールドと [Flash File System Path] フィールドの内容が削除されます。これは、別のファイルをアップロードできることを表します。別のファイルをアップロードするには、上記の手順を繰り返します。そうでない場合は、[Close] ボタンをクリックします。
- [Close]：[Upload Image] ダイアログウィンドウを閉じます。APCF ファイルをフラッシュ メモリにアップロードした後、またはアップロードしない場合に、このボタンをクリックします。アップロードする場合には、[APCF] ウィンドウの [APCF File Location] フィールドにファイル名が表示されます。アップロードしない場合には、「Are you sure you want to close the dialog without uploading the file?」と尋ねる [Close Message] ダイアログボックスが表示されます。ファイルをアップロードしない場合は、[OK] をクリックします。[Close Message] ダイアログボックスと [Upload Image] ダイアログボックスが閉じられ、APCF [Add/Edit] ペインが表示されます。この処理が実行されない場合は、[Close Message] ダイアログボックスの [Cancel] をクリックします。ダイアログボックスが閉じられ、フィールドの値がそのままの状態で [Upload Image] ダイアログボックスが再度表示されます。[Upload File] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

SharePoint アクセスのクロック精度

セキュリティ アプライアンスのクライアントレス SSL VPN サーバは、クッキーを使用して、エンドポイントの Microsoft Word などのアプリケーションと対話します。セキュリティ アプライアンスで設定されたクッキーの有効期間により、セキュリティ アプライアンスの時間が正しくない場合、SharePoint サーバ上の文書にアクセスするときに Word が正しく機能しなくなる可能性があります。このような誤作動を回避するには、ASA クロックを正しく設定します。NTP サービスと動的に同期できるよう、セキュリティ アプライアンスを設定することをお勧めします。手順については、「Clock」（P.10-2）を参照してください。

Auto Signon

[Auto Signon] ウィンドウまたはタブでは、クライアントレス SSL VPN ユーザの自動サインオンを設定または編集できます。自動サインオンは、内部ネットワークに SSO 方式をまだ展開していない場合に使用できる簡素化された単一サインオン方式です。特定の内部サーバに対して自動サインオンを設定すると、セキュリティ アプライアンス は、クライアントレス SSL VPN ユーザが セキュリティ アプライアンス へのログインで入力したログイン クレデンシャル（ユーザ名とパスワード）をそれら特定の内部サーバに渡します。特定の範囲のサーバの特定の認証方式に応答するように、セキュリティ アプライアンスを設定します。セキュリティ アプライアンスが応答するように設定可能な認証方式は、Basic（HTTP）、NTLM、FTP と CIFS、またはこれらの方式すべてを使用する認証で構成されます。

自動サインオンは、特定の内部サーバに SSO を設定する直接的な方法です。この項では、自動サインオンを行うように SSO をセットアップする手順について説明します。Computer Associates の SiteMinder SSO サーバを使用して SSO をすでに展開しているか、または Security Assertion Markup Language（SAML）Browser Post Profile SSO を使用している場合、およびこのソリューションをサポートするようにセキュリティ アプライアンスを設定する場合は、SSO Servers を参照してください。HTTP Form プロトコルで SSO を使用し、この方法をサポートするようにセキュリティ アプライアンスを設定する場合は、HTTP Form でのクライアントレス SSL VPN に対する SSO のサポートを参照してください。

（注） 認証が不要なサーバ、またはセキュリティ アプライアンスとは異なるクレデンシャルを使用するサーバでは、自動サインオンをイネーブルにしないでください。自動サインオンがイネーブルの場合、セキュリティ アプライアンスは、ユーザ ストレージにあるクレデンシャルに関係なく、ユーザがセキュリティ アプライアンスへのログインで入力したログイン クレデンシャルを渡します。

フィールド

- [IP Address]：*表示専用*。次の [Mask] と組み合わせて、認証されるサーバの IP アドレスの範囲を [Add/Edit Auto Signon] ダイアログボックスで設定されたとおりに表示します。サーバは、サーバの URI またはサーバの IP アドレスとマスクで指定できます。
- [Mask]：*表示専用*。前の [IP Address] と組み合わせて、[Add/Edit Auto Signon] ダイアログボックスで自動サインオンをサポートするように設定されたサーバの IP アドレスの範囲を表示します。
- [URI]：*表示専用*。[Add/Edit Auto Signon] ダイアログボックスで設定されたサーバを識別する URI マスクを表示します。
- [Authentication Type]：*表示専用*。認証タイプを表示します。[Add/Edit Auto Signon] ダイアログボックスで設定された、Basic（HTTP）、NTLM、FTP と CIFS、またはこれらの方式すべて。NTLM には NTLMv1 と NTLMv2 の両方が含まれます。
- [Add/Edit]：自動サインオン命令を追加または編集します。自動サインオン命令は、自動サインオン機能を使用する内部サーバの範囲と、特定の認証方式を定義します。
- [Delete]：[Auto Signon] テーブルで選択した自動サインオン命令を削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Auto Signon Entry

[Add/Edit Auto Signon Entry] ダイアログボックスでは、新しい自動サインオン命令を追加または編集できます。自動サインオン命令は、自動サインオン機能を使用する内部サーバの範囲と、特定の認証方式を定義します。

フィールド

- [IP Block]：IP アドレスとマスクを使用して内部サーバの範囲を指定します。
  - [IP Address]：自動サインオンを設定する範囲の最初のサーバの IP アドレスを入力します。
  - [Mask]：[subnet mask] メニューで、自動サインオンをサポートするサーバのサーバ アドレス範囲を定義するサブネット マスクをクリックします。
- [URI]：URI によって自動サインオンをサポートするサーバを指定し、このボタンの横にあるフィールドに URI を入力します。
- [Authentication Type]：サーバに割り当てられている認証方式。指定された範囲のサーバの場合には、Basic HTTP 認証要求、NTLM 認証要求、FTP と CIFS の認証要求、またはこれらの方式のいずれかを使用する要求に応答するように、セキュリティ アプライアンスを設定できます。
  - [Basic]：サーバが Basic（HTTP）認証をサポートする場合は、このボタンをクリックします。
  - [NTLM]：サーバが NTLMv1 認証をサポートする場合は、このボタンをクリックします。
  - [FTP/CIFS]：サーバが FTP と CIFS の認証をサポートする場合は、このボタンをクリックします。
  - [Basic, NTLM, and FTP/CIFS]：サーバが上のすべての方式をサポートする場合は、このボタンをクリックします。

（注） 一定範囲のサーバに対して 1 つの方式（HTTP Basic など）を設定する場合に、その中の 1 台のサーバが異なる方式（NTLM など）で認証を試みると、セキュリティ アプライアンスはユーザのログイン クレデンシャルをそのサーバに渡しません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

セッションの設定

[Clientless SSL VPN Add/Edit Internal Group Policy] > [More Options] > [Session Settings] ウィンドウでは、クライアントレス SSL VPN のセッションからセッションの間にパーソナライズされたユーザ情報を指定できます。デフォルトにより、各グループ ポリシーはデフォルトのグループ ポリシーから設定を継承します。このウィンドウを使用して、デフォルト グループ ポリシーのパーソナライズされたクライアントレス SSL VPN ユーザ情報、およびこれらの設定値を区別するグループ ポリシーすべてを指定します。

フィールド

- [User Storage Location] : [none] を選択するか、またはドロップダウン メニューからファイル サーバ プロトコル（smb または ftp）を選択します。[smb] または [ftp] を選択する場合は、次の構文を使用して、隣のテキスト フィールドにファイル システムの宛先を入力します。

  username:*password*@*host*:*port-number*/*path*

  次に例を示します。

  mike:mysecret@ftpserver3:2323/public

  （注） このコンフィギュレーションには、ユーザ名、パスワード、および事前共有キーが示されていますが、セキュリティ アプライアンスは、内部アルゴリズムを使用して暗号化された形式でデータを保存し、そのデータを保護します。

- [Storage Key]：必要な場合は、保管場所へユーザがアクセスできるようにするためにセキュリティ アプライアンスが渡す文字列を入力します。
- [Storage Objects]：ドロップダウン メニューから次のいずれかのオプションを選択して、ユーザとの関連でサーバが使用するオブジェクトを指定します。セキュリティ アプライアンスは、これらのオブジェクトを保存してクライアントレス SSL VPN 接続をサポートします。
  - cookies,credentials
  - cookies
  - credentials
- [Transaction Size] : セッションをタイムアウトするときの限界値を KB 単位で入力します。この属性は、1 つのトランザクションにだけ適用されます。この値よりも大きなトランザクションだけが、セッションの期限切れクロックをリセットします。

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Java Code Signer

コード署名により、デジタル署名が、実行可能なコードそのものに追加されます。このデジタル署名には、さまざまな情報が保持されています。署名以降にそのコードが変更されていないことを保証するだけでなく、署名者を認証する場合に使用することもできます。

コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。

[Java Code Signer] を選択するには、ドロップダウン リストを使用します。

Java Code Signer を設定するには、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Java Code Signer] に移動します。

コンテンツ キャッシュ

キャッシュにより、クライアントレス SSL VPN のパフォーマンスを強化します。頻繁に再利用されるオブジェクトをシステム キャッシュに格納することで、書き換えの繰り返しやコンテンツの圧縮の必要性を低減します。キャッシュを使用することでトラフィック量が減り、結果として多くのアプリケーションがより効率的に実行されます。

フィールド

- [Enable cache]：キャッシングをイネーブルにする場合にオンにします。デフォルト値は disable です。
- [Parameters]：キャッシング条件を定義できます。
  - [Enable caching of compressed content]：圧縮されたコンテンツをキャッシュする場合にオンにします。このパラメータをディセーブルにすると、セキュリティ アプライアンスがオブジェクトを保存してから圧縮します。
  - [Maximum Object Size]：セキュリティ アプライアンスがキャッシュできるドキュメントの最大サイズを KB 単位で入力します。セキュリティ アプライアンスが、オブジェクトの元の（書き換えまたは圧縮されていない）コンテンツの長さを測定します。範囲は 0 ～ 10,000 KB で、デフォルトは 1,000 KB です。
  - [Minimum Object Size]：セキュリティ アプライアンスがキャッシュできるドキュメントの最小サイズを KB 単位で入力します。セキュリティ アプライアンスが、オブジェクトの元の（書き換えまたは圧縮されていない）コンテンツの長さを測定します。範囲は 0 ～ 10,000 KB で、デフォルトは 0 KB です。

（注） [Maximum Object Size] は、[Minimum Object Size] よりも大きい値にする必要があります。

  - [Expiration Time]：0 ～ 900 の整数を入力して、オブジェクトを再検証しないでキャッシュする分数を設定します。デフォルトは 1 分です。
  - [LM Factor]：1 ～ 100 の整数を入力します。デフォルトは 20 です。

    LM 因数は、最終変更タイムスタンプだけを持つオブジェクトをキャッシュするためのポリシーを設定します。これによって、サーバ設定の変更値を持たないオブジェクトが再検証されます。セキュリティ アプライアンスは、オブジェクトが変更された後、およびオブジェクトが期限切れの時刻を呼び出した後の経過時間を推定します。推定された期限切れ時刻は、最終変更後の経過時間と LM 因数の積に一致します。LM 因数を 0 に設定すると、ただちに再検証が実行され、100 に設定すると、再検証までの許容最長時間になります。

期限切れ時刻は、セキュリティ アプライアンスが、最終変更タイムスタンプがなく、サーバ設定の期限切れ時刻も明示されていないオブジェクトをキャッシュする時間の長さを設定します。

  - [Cache static content]：たとえば PDF ファイルやイメージなど、リライトされることのないすべてのコンテンツをキャッシュします。

- [Restore Cache Default]：すべてのキャッシュ パラメータをデフォルト値に戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Content Rewrite

[Content Rewrite] ペインには、コンテンツのリライトがイネーブルまたはディセーブルであるすべてのアプリケーションが一覧表示されます。

クライアントレス SSL VPN では、コンテンツ変換およびリライト エンジンによって、JavaScript、VBScript、Java、マルチバイト文字などの高度な要素からプロキシ HTTP へのトラフィックまでを含む、アプリケーション トラフィックを処理します。このようなトラフィックでは、ユーザがアプリケーションにアクセスするのに SSL VPN デバイス内部からアプリケーションを使用しているか、SSL VPN デバイスに依存せずに使用しているかによって、セマンティックやアクセス コントロールのルールが異なる場合があります。

デフォルトでは、セキュリティ アプライアンスはすべてのクライアントレス トラフィックをリライト、または変換します。公開 Web サイトなどの一部のアプリケーションや Web リソースによっては、セキュリティ アプライアンスを通過しない設定が求められる場合があります。このため、セキュリティ アプライアンスでは、特定のサイトやアプリケーションをセキュリティ アプライアンスを通過せずにブラウズできるリライト規則を作成できます。これは、IPSec VPN 接続のスプリット トンネリングと同様の機能です。

リライト ルールは複数作成できます。セキュリティ アプライアンスはリライト ルールを順序番号に従って検索するため、ルールの番号は重要です。このとき、最下位の番号から順に検索して行き、最初に一致したルールが適用されます。

コンテンツ リライト ルールの例に、コンテンツ リライト ルールを例示します。

フィールド

- Content Rewrite
  - [Rule Number]：リスト内でのルールの位置を示す整数を表示します。
  - [Rule Name]：ルールが適用されるアプリケーションの名前を付けます。
  - [Rewrite Enabled]：コンテンツのリライトを、イネーブルかディセーブルで表示します。
  - [Resource Mask]：リソース マスクを入力します。
- [Add/Edit]：リライト エントリを追加、または選択したリライト エントリを編集します。

- [Delete]：選択したリライト エントリを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

コンテンツ リライト ルールの追加と編集

- [Enable content rewrite]：このリライト ルールでコンテンツのリライトをイネーブルにする場合に選択します。
- [Rule Number]：（任意）このルールの番号を入力します。この番号は、リストの他のルールに相対的に、そのルールの優先順位を示します。番号がないルールはリストの最後に配置されます。有効な範囲は 1 ～ 65534 です。
- [Rule Name]：（任意）ルールについて説明する英数字を指定します。最大 128 文字です。
- [Resource Mask]：ルールを適用するアプリケーションやリソースに対応する文字列を入力します。文字列の長さは最大で 300 文字です。次のいずれかのワイルドカードを使用できますが、少なくとも 1 つの英数字を指定する必要があります。

  * ：すべてに一致します。ASDM では、* または *.* で構成されるマスクは受け付けません。

  ? ：任意の 1 文字に一致します。

  [!seq]：シーケンスにない任意の文字に一致します。

  [seq]：シーケンス内の任意の文字に一致します。

コンテンツ リライト ルールの例

機能	コンテンツのリライトをイネーブルにする	ルール番号	ルール名	リソース マスク
すべての HTTP URL を ASA 外に強制的に配信する（スプリット トンネル）	Check	1	split-tunnel-all-http	http://*
すべての HTTP URL を ASA 外に強制的に配信する	Check	2	split-tunnel-all-https	https://*

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Java Code Signer

クライアントレス SSL VPN によって変換された Java オブジェクトは、その後、トラストポイントに関連付けられている PKCS12 デジタル証明書を使用して署名することができます。[Java Trustpoint] ペインでは、指定されたトラストポイントの場所から PKCS12 証明書とキー関連情報を使用するように、クライアントレス SSL VPN Java オブジェクト署名機能を設定できます。トラストポイントをインポートするには、[Configuration] > [Properties] > [Certificate] > [Trustpoint] > [Import] を参照してください。

フィールド

- [Code Signer Certificate]：Java オブジェクト署名で使用する、設定された証明書を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Encoding

このウィンドウでは、クライアントレス SSL VPN ポータル ページの文字エンコーディングを表示または指定できます。

文字エンコーディング（「文字コーディング」または「文字セット」とも呼ばれます）は、raw データ（0 と 1 からなるデータなど）と文字をペアにすることで、データを表します。使用する文字エンコード方式は、言語によって決まります。単一の方式を使う言語もあれば、使わない言語もあります。通常は、地域によってブラウザで使用されるデフォルトのコード方式が決まりますが、リモート ユーザが変更することもできます。ブラウザはページに指定されたエンコードを検出することもでき、そのエンコードに従ってドキュメントを表示します。

エンコード属性によりポータル ページで使用される文字コード方式の値を指定することで、ユーザがブラウザを使用している地域や、ブラウザに対する何らかの変更に関係なく、ページが正しく表示されるようにできます。

デフォルトでは、セキュリティ アプライアンスは「Global Encoding Type」を共通インターネット ファイル システム サーバからのページに適用します。CIFS サーバと適切な文字エンコーディングとのマッピングを、[Global Encoding Type] 属性によってグローバルに、そしてテーブルに示されている

ファイル エンコーディング例外を使用して個別に行うことにより、ファイル名やディレクトリ パス、およびページの適切なレンダリングが問題となる場合に、CIFS ページが正確に処理および表示できるようにします。

フィールド

- [Global Encoding Type]：この属性によって、表に記載されている CIFS サーバからの文字エンコーディングを除いて、すべてのクライアントレス SSL VPN ポータル ページが継承する文字エンコーディングが決まります。文字列を入力するか、ドロップダウン リストから選択肢を 1 つ選択します。リストには、最も一般的な次の値だけが表示されます。
  - big5
  - gb2312
  - ibm-850
  - iso-8859-1
  - shift_jis

  （注）　日本語の Shift_jis 文字エンコーディングを使用している場合は、関連付けられている [Select Page Font] ペインの [Font Family] 領域にある [Do not specify] をクリックして、このフォント ファミリを削除します。

  - unicode
  - windows-1252
  - none

    [none] を選択するか、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのエンコーディングが使用されます。

  最大 40 文字から成り、http://www.iana.org/assignments/character-sets で指定されているいずれかの有効文字セットと同じ文字列を入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されません。セキュリティ アプライアンスの設定を保存したときに、コマンド インタープリタが大文字を小文字に変換します。
- [CIFS Server]：コード要件が「Global Encoding Type」属性設定とは異なる各 CIFS サーバの名前または IP アドレス。

  CIFS サーバのファイル名とディレクトリのコードが異なる場合は、コードが正しいことをサーバに認識させるために、場合によってはエントリを追加する必要があることを表します。
- [Encoding Type]：関連付けられている CIFS サーバで優先される文字コードを表示します。
- [Add]：「Global Encoding Type」設定を上書きする CIFS サーバごとに 1 回クリックします。
- [Edit]：テーブルから CIFS サーバを選択し、このボタンをクリックして文字コードを変更します。
- [Delete]：テーブルから CIFS サーバを選択し、このボタンをクリックして、関連付けられているエントリをテーブルから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

エンコードの追加と編集

[Add CIFS Server Encoding] ダイアログ ウィンドウでは、[Add CIFS Encoding] ウィンドウの「Global Encoding Type」属性設定に対する例外を保持できます。このウィンドウには、このダイアログボックスを開く [Add] および [Edit] ボタンがあります。

フィールド

- [CIFS Server] : エンコーディング要件が「Global Encoding Type」属性設定とは異なる CIFS サーバの名前または IP アドレスを入力します。セキュリティ アプライアンスでは、指定した大文字と小文字の区別が保持されますが、名前をサーバと照合するときには大文字と小文字は区別されません。
- [Encoding Type] : CIFS サーバがクライアントレス SSL VPN ポータル ページで使用する文字エンコーディングを選択します。文字列を入力するか、ドロップダウン リストから選択します。リストには、最も一般的な次の値だけが登録されています。
  - big5
  - gb2312
  - ibm-850
  - iso-8859-1
  - shift_jis

  （注）　日本語の Shift_jis 文字エンコーディングを使用している場合は、関連付けられている [Select Page Font] ペインの [Font Family] 領域にある [Do not specify] をクリックして、このフォント ファミリを削除します。

  - unicode
  - windows-1252
  - none

    [none] を選択するか、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのエンコーディングが使用されます。

  最大 40 文字から成り、http://www.iana.org/assignments/character-sets で指定されているいずれかの有効文字セットと同じ文字列を入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されません。セキュリティ アプライアンスの設定を保存したときに、コマンド インタープリタが大文字を小文字に変換します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Web ACLs

[Web ACLs] テーブルには、セキュリティ アプライアンスで設定されている、クライアントレス SSL VPN トラフィックに適用できるフィルタが表示されます。このテーブルには、各アクセス コントロール リスト（ACL）の名前、および ACL 名の下で右にインデントされて、その ACL に割り当てられているアクセス コントロール エントリ（ACE）が表示されます。

各 ACL により、特定のネットワーク、サブネット、ホスト、および Web サーバへのアクセスを許可または拒否します。各 ACE は、ACL の機能を提供する 1 つのルールを指定します。

ACL は、クライアントレス SSL VPN トラフィックに適用されるように設定できます。次の規則が適用されます。

- フィルタを設定しない場合は、すべての接続が許可されます。
- セキュリティ アプライアンスは、インターフェイスのインバウンド ACL だけをサポートします。
- 各 ACL の最後では、表記されない暗黙のルールにより、明示的に許可されていないすべてのトラフィックが拒否されます。

ACL および ACE を追加するには、次の手順を実行します。

- ACL を追加するには、テーブルの上にあるプラス記号の横の下矢印をクリックし、[Add ACL] をクリックします。

（注）　ACE を追加するには、テーブルに ACL が表示されている必要があります。

- テーブル内にすでに表示されている ACL に ACE を追加するには、追加する ACE を選択し、テーブルの上にあるプラス記号の横の下矢印をクリックして、[Add ACE] をクリックします。
- テーブル内にすでに存在する ACE の前に ACE を追加するには、追加する ACE を選択し、テーブルの上にあるプラス記号の横の下矢印をクリックして、[Insert] をクリックします。
- テーブル内にすでに存在する ACE の後に ACE を追加するには、追加する ACE を選択し、テーブルの上にあるプラス記号の横の下矢印をクリックして、[Insert After] をクリックします。

ACE に割り当てられている値を変更するには、その値をダブルクリックするか、選択して [Edit] をクリックします。

ACL または ACE を削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

ACL 内での ACE の相対的な位置により、セキュリティ アプライアンスがインターフェイスのトラフィックに ACE を適用するときの順番が決まります。テーブル内の ACE を並べ替えて再使用するには、次の手順を実行します。

- ACE を他の ACE の上または下に移動させるには、移動させる ACE を選択して、テーブルの上にある上へまたは下へアイコンをクリックします。

- ACE を移動させるには、その ACE を選択し、テーブルの上にあるはさみアイコンをクリックします。ターゲットの ACL または ACE を選択し、クリップボード アイコンの横の矢印をクリックして、選択したエントリの上に貼り付けるには [Paste] を、選択したエントリの後に貼り付けるには [Paste After] をクリックします。[Edit ACE] ダイアログ ウィンドウが開きます。このダイアログボックスでは、値を変更できます。[OK] をクリックします。
- ACE をコピーするには、コピーする ACE を選択し、テーブルの上にある見開きページ アイコンをクリックします。ターゲットの ACL または ACE を選択し、クリップボード アイコンの横の矢印をクリックして、選択したエントリの上に貼り付けるには [Paste] を、選択したエントリの後に貼り付けるには [Paste After] をクリックします。[Edit ACE] ダイアログ ウィンドウが開きます。このダイアログボックスでは、値を変更できます。[OK] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Port Forwarding

[Port Forwarding] ペインと [Configure Port Forwarding Lists] ダイアログボックスでは、ポート転送リストを表示できます。[Port Forwarding] ペインと [Add or Edit Port Forwarding Entry] ダイアログボックスの両方で、ポート転送リストの名前を指定し、リストのポート転送エントリを追加、表示、編集、および削除できます。

ポート転送リストを追加、変更、または削除するには、次のいずれかの操作を実行します。

- ポート転送リストを追加し、そのリストにエントリを追加するには、[Add] をクリックします。[Add Port Forwarding List] ダイアログボックスが開きます。リストに名前を付けたら、もう一度 [Add] をクリックします。ASDM が [Add Port Forwarding Entry] ダイアログボックスを開きます。このダイアログボックスでは、エントリの属性をリストに割り当てることができます。属性を割り当てて [OK] をクリックすると、ASDM のリストにそれらの属性が表示されます。必要に応じて手順を繰り返してリストを完成させ、[Add Port Forwarding List] ダイアログボックスで [OK] をクリックします。
- ポート転送リストを変更するには、そのリストをダブルクリックするか、またはテーブル内のリストを選択して [Edit] をクリックします。次に、[Add] をクリックして新しいエントリをリストに挿入するか、またはリストのエントリをクリックし、[Edit] または [Delete] をクリックします。
- リストを削除するには、テーブル内のリストを選択して [Delete] をクリックします。

ポート転送を使用する理由

ポート転送は、クライアントレス SSL VPN 接続を介して TCP ベースのアプリケーションをサポートするためのレガシー テクノロジーです。ポート転送テクノロジーをサポートする設定を事前に構築している場合は、ポート転送の使用を選択することもできます。

ポート転送の代替方法として次を検討してください。

- スマート トンネル アクセスを使用すると、ユーザには次のような利点があります。
  - スマート トンネルは、プラグインよりもパフォーマンスが向上します。
  - ポート転送とは異なり、スマート トンネルでは、ローカル ポートへのローカル アプリケーションのユーザ接続を要求しないことにより、ユーザ エクスペリエンスが簡略化されます。
  - ポート転送とは異なり、スマート トンネルでは、ユーザは管理者特権を持つ必要がありません。
- ポート転送およびスマート トンネル アクセスとは異なり、プラグインでは、クライアント アプリケーションをリモート コンピュータにインストールする必要がありません。

セキュリティ アプライアンスでポート転送を設定する場合は、アプリケーションが使用するポートを指定します。スマート トンネル アクセスを設定する場合は、実行ファイルまたはそのパスの名前を指定します。

ポート転送の要件と制限事項

ポート転送には次の制限が適用されます。

- リモート ホストで、次のいずれかの 32 ビット バージョンが実行されている必要がある。
  - Microsoft Windows Vista、Windows XP SP2 または SP3、または Windows 2000 SP4
  - Apple Mac OS X 10.4 または 10.5 と Safari 2.0.4(419.3)
  - Fedora Core 4
- また、リモート ホストで Sun JRE 1.5 以降が動作していることも必要です。
- Mac OS X 10.5.3 上の Safari のブラウザベースのユーザは、Safari での URL の解釈方法に従って、使用するクライアント証明書を、1 回目は末尾にスラッシュを含め、もう 1 回はスラッシュを含めずに、セキュリティ アプライアンスの URL を使用して指定する必要があります。次に例を示します。
  - https://example.com/
  - https://example.com

  詳細については、『Safari, Mac OS X 10.5.3: Changes in client certificate authentication』を参照してください。
- ポート転送またはスマート トンネルを使用する Microsoft Windows Vista ユーザは、ASA の URL を信頼済みサイト ゾーンに追加する。信頼済みサイト ゾーンにアクセスするには、Internet Explorer を起動し、[Tools] > [Internet Options] > [Security] タブを選択する必要があります。Vista ユーザは、[Protected Mode] をディセーブルにしてスマート トンネル アクセスを容易にすることもできます。ただし、攻撃に対するコンピュータの脆弱性が増すため、この方法は推奨しません。
- ポート転送は、スタティック TCP ポートを使用する TCP アプリケーションのみをサポートしています。ダイナミック ポートまたは複数の TCP ポートを使用するアプリケーションはサポートしていません。たとえば、ポート 22 を使用する SecureFTP は、クライアントレス SSL VPN のポート転送を介して動作しますが、ポート 20 と 21 を使用する標準 FTP は動作しません。
- ポート転送は、UDP を使用するプロトコルをサポートしていません。
- セキュリティ アプライアンスは Microsoft Outlook Exchange（MAPI）プロキシをサポートしていません。MAPI プロトコルを使用した Microsoft Outlook Exchange 通信では、リモート ユーザが AnyConnect を使用する必要があります。

- ステートフル フェールオーバーでは、Application Access（ポート転送またはスマート トンネル アクセス）を使用して確立したセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。
- ポート転送は、Personal Digital Assistants（PDA; 携帯情報端末）への接続はサポートしていません。
- ポート転送を使用するには、Java アプレットをダウンロードしてローカル クライアントを設定する必要があります。これには、ローカル システムに対する管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。

注意　ポート転送（アプリケーション アクセス）およびデジタル証明書をサポートするために、リモート コンピュータに Sun Microsystems Java Runtime Environment（JRE）1.5.x 以降がインストールされていることを確認してください。JRE 1.4.x が実行中で、ユーザがデジタル証明書で認証される場合、JRE は Web ブラウザの証明書ストアにアクセスできないため、アプリケーションは起動しません。

Java アプレットは、エンド ユーザの HTML インターフェイスにあるアプレット独自のウィンドウに表示されます。このウィンドウには、ユーザが使用できる転送ポートのリストの内容、アクティブなポート、および送受信されたトラフィック量（バイト単位）が表示されます。

- ポート転送も ASDM Java アプレットも、デジタル証明書を使用するユーザ認証では動作しません。Java には、Web ブラウザ キーストアにアクセスする機能はありません。このため、Java はブラウザがユーザの認証に使用する証明書を使用できず、アプリケーションは起動できません。
- 次の項で説明するように、ポート転送には DNS を設定する必要があります。

ポート転送用の DNS の設定

ポート転送では、リモート サーバのドメイン名またはその IP アドレスを ASA に転送して、解決および接続を行います。つまり、ポート転送アプレットは、アプリケーションからの要求を受け入れて、その要求を ASA に転送します。ASA は適切な DNS クエリーを作成し、ポート転送アプレットの代わりに接続を確立します。ポート転送アプレットは、ASA に対する DNS クエリーだけを作成します。ポート転送アプレットはホスト ファイルをアップデートして、ポート転送アプリケーションが DNS クエリーを実行したときに、クエリーがループバック アドレスにリダイレクトされるようにします。

次のように、DNS 要求をポート転送アプレットから受け入れるように、セキュリティ アプライアンスを設定します。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] の順にクリックします。

DefaultWEBVPNGroup エントリは、クライアントレス接続に使用されるデフォルトの接続プロファイルです。

ステップ 2　クライアント接続において DefaultWEBVPNGroup エントリが使用されるようにコンフィギュレーションを設定する場合は、このエントリを強調表示し、[Edit] をクリックします。このエントリが使用されない場合は、クライアント接続のコンフィギュレーションで使用される接続プロファイルを強調表示し、[Edit] をクリックします。

[Basic] ウィンドウが開きます。

ステップ 3　[DNS] 領域にスキャンし、ドロップダウン リストから DNS サーバを選択します。ドメイン名をメモしておきます。使用したい DNS サーバが ASDM に表示されている場合は、残りのステップを飛ばし、次のセクションに移動します。ポート転送リストのエントリを設定する際、リモート サーバの指定時には、同じドメイン名を入力する必要があります。コンフィギュレーションに DNS サーバがない場合は、残りのステップを続けます。

ステップ 4　[DNS] 領域で [Manage] をクリックします。

[Configure DNS Server Groups] ウィンドウが開きます。

ステップ 5　[Configure Multiple DNS Server Groups] をクリックします。

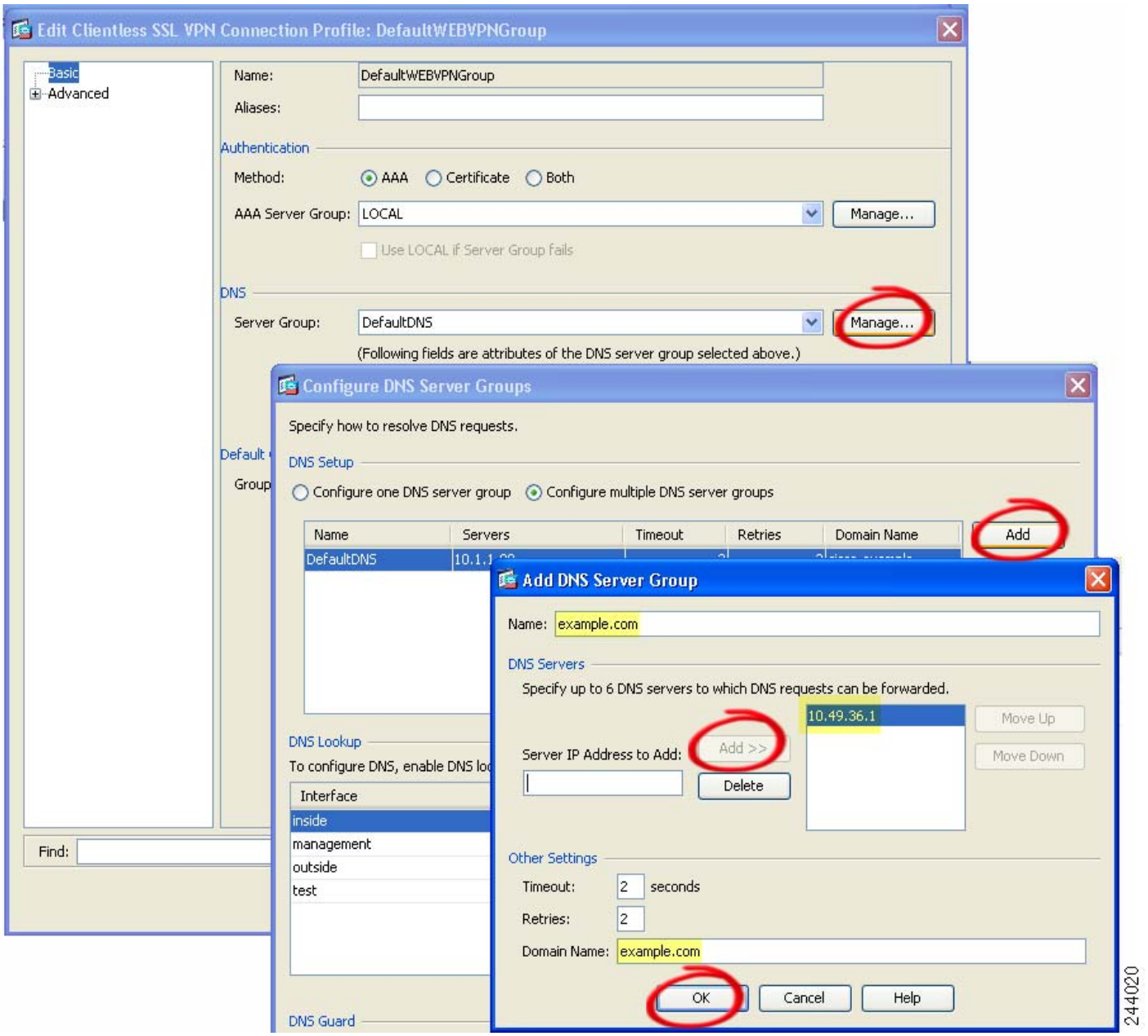
ウィンドウに、DNS サーバのエントリの一覧表が表示されます。

ステップ 6　[Add] をクリックします。

[Add DNS Server Group] ウィンドウが開きます。

ステップ 7　[Name] フィールドに新しいサーバ グループ名を入力し、IP アドレスとドメイン名を入力します（図 34-1 を参照）。

図 34-1　ポート転送の DNS サーバ値の例



入力したドメイン名をメモしておきます。後ほど、ポート転送エントリを設定する際、リモート サーバを指定するために必要になります。

ステップ 8　[Connection Profiles] ウィンドウが再度アクティブになるまで、[OK] をクリックします。

ステップ 9　クライアントレス接続の設定で使用される、残りすべての接続プロファイルについて、手順 2 ～ 8 を繰り返します。

ステップ 10　[Apply] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Port Forwarding List

[Add/Edit Port Forwarding List] ダイアログボックスでは、クライアントレス SSL VPN 接続によるアクセスに適用されるユーザまたはグループ ポリシーに関連付ける TCP アプリケーションの名前付きリストを追加または編集できます。

フィールド

- [List Name]：英数字で表したリストの名前。最大 64 文字です。
- [Local TCP Port]：アプリケーションのトラフィックを受信するローカル ポート。
- [Remote Server]：リモート サーバの IP アドレスまたは DNS 名。
- [Remote TCP Port]：アプリケーションのトラフィックを受信するリモート ポート。
- [Description]：TCP アプリケーションを説明するテキスト。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Port Forwarding Entry

[Add/Edit Port Forwarding Entry] ダイアログボックスでは、クライアントレス SSL VPN 接続によるアクセスに適用されるユーザまたはグループ ポリシーに関連付ける TCP アプリケーションを指定できます。これらのウィンドウで属性に値を割り当てるには、次の手順を実行します。

- [Local TCP Port]：アプリケーションが使用する TCP ポート番号を入力します。ローカル ポート番号は、1 つの listname に対して一度だけ使用できます。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。
- [Remote Server]：リモート アクセス サーバのドメイン名または IP アドレスを入力します。特定の IP アドレスに対してクライアント アプリケーションを設定しなくて済むよう、ドメイン名を使用することをお勧めします。

注意　トンネルを確立し、IP アドレスを解決するためには、「ポート転送用の DNS の設定」（P.34-24）に記載のとおり、[Remote Server] パラメータで割り当てた DNS 名は、[Domain Name] および [Server Group] パラメータと一致する必要があります。[Domain] および [Server Group] パラメータのデフォルト設定は、いずれも DefaultDNS です。

- [Remote TCP Port]：そのアプリケーション用の既知のポート番号を入力します。
- [Description]：アプリケーションの説明を入力します。最大 64 文字です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

外部プロキシ サーバの使用法の設定

[Proxies] ペインを使用して、外部プロキシ サーバによって HTTP 要求と HTTPS 要求を処理するようにセキュリティ アプライアンスを設定します。これらのサーバは、ユーザとインターネットの仲介役として機能します。すべてのインターネット アクセスがユーザ制御のサーバを経由するように指定することで、別のフィルタリングが可能になり、セキュアなインターネット アクセスと管理制御が保証されます。

（注）　HTTP および HTTPS プロキシ サービスでは、PDA への接続をサポートしていません。

フィールド

[Use an HTTP proxy server]：外部 HTTP プロキシ サーバを使用します。

- [Specify IP address of proxy server]：IP アドレスまたはホスト名によって HTTP プロキシ サーバを特定します。
- [IP Address]：外部 HTTP プロキシ サーバのホスト名または IP アドレスを入力します。
- [Port]：HTTP 要求をリッスンするポートを入力します。デフォルトのポートは 80 です。
- [Exception Address List]：（任意）HTTP プロキシ サーバに送信可能な URL から除外する URL、または数個の URL のカンマ区切りリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。
  - ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。
  - **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。
  - [*x*-*y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。

  - [**!***x-y*] は、この範囲内に存在しない任意の 1 文字に一致します。
- [UserName]：（任意）このキーワードを入力して、各 HTTP プロキシ要求にユーザ名を添付し、基本的なプロキシ認証を行います。
- [Password]：各 HTTP 要求と一緒にプロキシ サーバに送信するパスワードを入力します。
- [Specify PAC file URL]：HTTP プロキシ サーバの IP アドレスを指定する方法の代替として、このオプションをクリックして、ブラウザにダウンロードするプロキシ自動コンフィギュレーション ファイルを指定できます。ダウンロードが完了すると、PAC ファイルは JavaScript 機能を使用して各 URL のプロキシを識別します。隣接するフィールドに、**http://** を入力し、プロキシ自動設定ファイルの URL を入力します。**http://** の部分を省略すると、セキュリティ アプライアンスはその URL を無視します。

[Use an HTTPS proxy server]：外部 HTTPS プロキシ サーバを使用します。

- [Specify IP address of proxy server]：IP アドレスまたはホスト名によって HTTPS プロキシ サーバを特定します。
- [IP Address]：HTTPS プロキシ サーバのホスト名または IP アドレスを入力します。
- [Port]：HTTPS 要求をリッスンするポートを入力します。デフォルトのポートは 443 です。
- [Exception Address List]：（任意）HTTPS プロキシ サーバに送信可能な URL から除外する URL、または数個の URL のカンマ区切りリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。
  - ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。
  - **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。
  - [*x-y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。
  - [**!***x-y*] は、この範囲内に存在しない任意の 1 文字に一致します。
- [UserName]：（任意）このキーワードを入力して、各 HTTPS プロキシ要求にユーザ名を添付し、基本的なプロキシ認証を行います。
- [Password]：各 HTTPS 要求と一緒にプロキシ サーバに送信するパスワードを入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

プロキシ バイパスの設定

ユーザはプロキシ バイパスを使用するようにセキュリティ アプライアンスを設定できます。これは、プロキシ バイパスが提供する特別なコンテンツ リライト機能を使用した方が、アプリケーションや Web リソースをより有効活用できる場合に設定します。プロキシ バイパスはコンテンツの書き換えに代わる手法であり、元のコンテンツの変更を最小限に抑えます。多くの場合、カスタム Web アプリケーションでこれを使用すると有効です。

プロキシ バイパスには複数のエントリを設定できます。エントリを設定する順序は重要ではありません。インターフェイスとパス マスク、またはインターフェイスとポートにより、プロキシ バイパス ルールが一意に指定されます。

パス マスクではなくポートを使用してプロキシ バイパスを設定する場合、ネットワーク コンフィギュレーションによっては、これらのポートがセキュリティ アプライアンスにアクセスできるようにするために、ファイアウォール コンフィギュレーションの変更が必要になることがあります。この制限を回避するには、パス マスクを使用します。ただし、パス マスクは変化することがあるため、複数のパス マスク ステートメントを使用して変化する可能性をなくすことが必要になる場合があります。

パスは、URL 内のドメイン名に続くテキストです。たとえば、www.example.com/hrbenefits という URL では、*hrbenefits* がパスになります。同様に、www.example.com/hrinsurance という URL では、*hrinsurance* がパスです。すべての hr サイトでプロキシ バイパスを使用する場合は、*（ワイルドカード）を /hr* のように使用して、コマンドを複数回使用しないようにできます。

フィールド

- [Interface]：プロキシ バイパス用に設定された VLAN を表示します。
- [Port]：プロキシ バイパス用に設定されたポートを表示します。
- [Path Mask]：プロキシ バイパスに一致する URI パスを表示します。
- [URL]：ターゲット URL を表示します。
- [Rewrite]：リライト オプションを表示します。これらのオプションは、XML やリンクの組み合わせ、またはなしです。
- [Add/Edit]：プロキシ バイパス エントリを追加、または選択したエントリを編集します。
- [Delete]：プロキシ バイパス エントリを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Proxy Bypass Rule

このパネルでは、セキュリティ アプライアンスがコンテンツ リライトをほとんどまたはまったく実行しない場合のルールを設定できます。

フィールド

- [Interface Name]：プロキシ バイパス用の VLAN を選択します。

- [Bypass Condition]：プロキシ バイパス用のポートまたは URI を指定します。
  - [Port]：（オプション ボタン）プロキシ バイパスにポートを使用します。有効なポート番号は 20000 ～ 21000 です。
  - [Port]：（フィールド）セキュリティ アプライアンスがプロキシ バイパス用に予約する大きな番号のポートを入力します。
  - [Path Mask]：（オプション ボタン）プロキシ バイパスに URL を使用します。
  - [Path Mask]：（フィールド）プロキシ バイパス用の URL を入力します。この URL には、正規表現を使用できます。
- [URL]：プロキシ バイパスのターゲット URL を定義します。
  - [URL]：（ドロップダウン リスト）プロトコルとして、http または https を選択します。
  - [URL]：（テキスト フィールド）プロキシ バイパスを適用する URL を入力します。
- [Content to Rewrite]：リライトするコンテンツを指定します。選択肢は、なし、または XML、リンク、およびクッキーの組み合わせです。
  - [XML]：XML コンテンツをリライトする場合に選択します。
  - [Hostname]：リンクをリライトする場合に選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

DTLS 設定

Datagram Transport Layer Security（DTLS）をイネーブルにすることにより、SSL VPN 接続を確立する AnyConnect VPN クライアントは、SSL トンネルおよび DTLS トンネルという 2 つの同時トンネルを使用できます。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

DTLS をイネーブルにしない場合、SSL VPN 接続を確立する AnyConnect クライアント ユーザは、SSL VPN トンネルでだけ接続します。

フィールド

- [Interface]：セキュリティ アプライアンスのインターフェイスのリストを表示します。
- [DTLS Enabled]：インターフェイスで AnyConnect クライアントによる DTLS 接続をイネーブルにする場合にオンにします。
- [UDP Port (default 443)]：（任意）DTLS 接続用に別の UDP ポートを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

SSL VPN Client の設定

Cisco AnyConnect VPN クライアントによりリモート ユーザは、セキュリティ アプライアンスへのセキュアな SSL 接続を確立できます。このクライアントにより、ネットワーク管理者がリモート コンピュータにクライアントをインストールして設定しなくても、リモート ユーザは SSL VPN クライアントを活用できます。

事前にインストールされたクライアントがない場合、リモート ユーザは、SSL VPN 接続を受け入れるように設定されたそれぞれのブラウザ インターフェイスに IP アドレスを入力します。http:// リクエストを https:// リクエストにリダイレクトするよう セキュリティ アプライアンス が設定されていない場合、ユーザは https://<*address*> 形式で URL を入力する必要があります。

URL が入力されると、ブラウザはそのインターフェイスに接続し、ログイン画面を表示します。ユーザがログインと認証に成功し、そのユーザがクライアントを要求しているとセキュリティ アプライアンスで識別されると、セキュリティ アプライアンスは、リモート コンピュータのオペレーティング システムに合うクライアントをダウンロードします。ダウンロード後、クライアントがインストールおよび設定され、セキュア SSL 接続が確立されます。接続終了時にクライアントが維持されるか、アンインストールされるかは、セキュリティ アプライアンスの設定で決まります。

以前にインストールされているクライアントの場合は、ユーザの認証時に、セキュリティ アプライアンスがクライアントのリビジョンを検査して、必要に応じてクライアントをアップグレードします。

クライアントがセキュリティ アプライアンスと SSL VPN 接続をネゴシエートした場合は、Transport Layer Security（TLS）を使用して接続します。状況に応じて、Datagram Transport Layer Security（DTLS）が使用されます。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

AnyConnect クライアントは、セキュリティ アプライアンスからダウンロードできます。または、システム管理者が手動でリモート PC にインストールできます。クライアントを手動でインストールする方法の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

セキュリティ アプライアンスは、ユーザが確立している接続のグループ ポリシーまたはユーザ名属性に基づきクライアントをダウンロードします。自動的にクライアントをダウンロードするようにセキュリティ アプライアンスを設定するか、またはクライアントをダウンロードするかをリモート ユーザに確認するように設定できます。後者の場合、ユーザが応答しなかった場合は、タイムアウト時間が経過した後にクライアントをダウンロードするか、ログイン ページを表示するようにセキュリティ アプライアンスを設定できます。

フィールド

- [SSL VPN Client Images table]：SSL VPN クライアント イメージとして指定されたパッケージ ファイルを表示します。セキュリティ アプライアンスがイメージをリモート PC にダウンロードする順序は指定できます。

  - [Add] : [Add SSL VPN Client Image] ウィンドウが表示されます。このウィンドウでは、フラッシュ メモリ内のファイルをクライアント イメージ ファイルとして指定したり、フラッシュ メモリから、クライアント イメージとして指定するファイルを参照したりできます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。
  - [Replace] : [Replace SSL VPN Client Image] ウィンドウが表示されます。このウィンドウでは、フラッシュ メモリ内のファイルをクライアント イメージとして指定して、[SSL VPN Client Image] テーブルで選択したイメージと置換できます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。
  - [Delete] : テーブルからイメージを削除します。イメージを削除しても、パッケージ ファイルはフラッシュから削除されません。
  - [Move Up and Move Down] : セキュリティ アプライアンスがクライアント イメージをリモート PC にダウンロードするときの順序を変更します。テーブルの一番上にあるイメージを最初にダウンロードします。このため、最もよく使用するオペレーティング システムで使用されるイメージを一番上に移動する必要があります。

- [SSL VPN Client Profiles] テーブル : SSL VPN クライアント プロファイルとして指定された XML ファイルを表示します。これらのプロファイルは、AnyConnect VPN クライアント ユーザ インターフェイスにホスト情報を表示します。
  - [Add] : [Add SSL VPN Client Profiles] ウィンドウが表示されます。このウィンドウでは、フラッシュ メモリ内のファイルをプロファイルとして指定したり、フラッシュ メモリから、プロファイルとして指定するファイルを参照したりできます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。
  - [Edit] : [Edit SSL VPN Client Profiles] ウィンドウが表示されます。このウィンドウでは、フラッシュ メモリ内のファイルをプロファイルとして指定し、[SSL VPN Client Profiles] テーブルで選択したプロファイルと置換できます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。
  - [Delete] : テーブルからプロファイルを削除します。プロファイルを削除しても、XML ファイルはフラッシュから削除されません。
- [Cache File System] : セキュリティ アプライアンスは、キャッシュ メモリ内で SSL VPN クライアントと CSD イメージを展開します。イメージを展開するのに十分なスペースが確保されるように、キャッシュ メモリのサイズを調整してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

Add/Replace SSL VPN Client Image

このウィンドウでは、SSL VPN クライアント イメージとして追加するか、またはテーブルのリストにすでに含まれているイメージと置換する、セキュリティ アプライアンス フラッシュ メモリのファイルの名前を指定できます。また、識別するファイルをフラッシュ メモリから参照したり、ローカル コンピュータからファイルをアップロードしたりすることもできます。

フィールド

- [Flash SVC Image]：SSL VPN クライアント イメージとして識別する、フラッシュ メモリ内のファイルを指定します。
- [Browse Flash]：フラッシュ メモリに格納されているすべてのファイルを参照できる [Browse Flash Dialog] ウィンドウを表示します。
- [Upload]：[Upload Image] ウィンドウが表示されます。このウィンドウでは、クライアント イメージとして指定するファイルをローカル PC からアップロードできます。
- [Regular expression to match user-agent]：セキュリティ アプライアンスが、ブラウザによって渡された User-Agent 文字列に一致させる文字列を指定します。モバイル ユーザの場合、この機能を使用してモバイル デバイスの接続時間を短縮できます。ブラウザがセキュリティ アプライアンスに接続するとき、User-Agent ストリングが HTTP ヘッダーに含められます。セキュリティ アプライアンスによってストリングが受信され、そのストリングがあるイメージ用に設定された式と一致すると、そのイメージがただちにダウンロードされます。この場合、他のクライアント イメージはテストされません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Upload Image

このウィンドウでは、ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリに格納されている、SSL VPN クライアント イメージとして識別するファイルのパスを指定できます。ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリから、識別するファイルを参照できます。

フィールド

- [Local File Path]：ローカル コンピュータに格納されている、SSL VPN クライアント イメージとして識別するファイルの名前を指定します。
- [Browse Local Files]：[Select File Path] ウィンドウが表示されます。このウィンドウでは、ローカル コンピュータに格納されているすべてのファイルを表示し、クライアント イメージとして識別するファイルを選択できます。

- [Flash File System Path]：セキュリティ アプライアンスのフラッシュ メモリに格納されている、SSL VPN クライアント イメージとして識別するファイルの名前を指定します。
- [Browse Flash]：[Browse Flash Dialog] ウィンドウが表示されます。このウィンドウでは、セキュリティ アプライアンスのフラッシュ メモリに格納されているすべてのファイルを表示し、クライアント イメージとして識別するファイルを選択できます。
- [Upload File]：ファイルのアップロードを開始します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit SSL VPN Client Profiles

このウィンドウでは、ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリに格納されている、SSL VPN クライアント プロファイルとして識別するファイルのパスを指定できます。これらのプロファイルは、AnyConnect VPN クライアント ユーザ インターフェイスにホスト情報を表示します。ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリから、識別するファイルを参照できます。

フィールド

- [Profile Name]：テーブルに表示される XML ファイルに名前を関連付けます。XML プロファイル ファイルで特定されているホストを思い出しやすい名前を付けてください。
- [Profile Package]：ローカル コンピュータのフラッシュ メモリに格納されている、SSL VPN クライアント プロファイルとして識別するファイルの名前を指定します。
- [Browse Flash]：[Browse Flash Dialog] ウィンドウが表示されます。このウィンドウでは、セキュリティ アプライアンスのフラッシュ メモリに格納されているすべてのファイルを表示し、プロファイルとして識別するファイルを選択できます。
- [Upload File]：ファイルのアップロードを開始します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Upload Package

このウィンドウでは、ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリに格納されている、SSL VPN クライアント プロファイルとして識別するファイルのパスを指定できます。ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリから、識別するファイルを参照できます。

フィールド

- [Local File Path] : ローカル コンピュータに格納されている、SSL VPN クライアント プロファイルとして識別するファイルの名前を指定します。
- [Browse Local Files] : [Select File Path] ウィンドウが表示されます。このウィンドウでは、ローカル コンピュータに格納されているすべてのファイルを表示し、クライアント プロファイルとして識別するファイルを選択できます。
- [Flash File System Path] : セキュリティ アプライアンスのフラッシュ メモリに格納されている、クライアント プロファイルとして識別するファイルの名前を指定します。
- [Browse Flash] : [Browse Flash Dialog] ウィンドウが表示されます。このウィンドウでは、セキュリティ アプライアンスのフラッシュ メモリに格納されているすべてのファイルを表示し、クライアント プロファイルとして識別するファイルを選択できます。
- [Upload File] : ファイルのアップロードを開始します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Bypass Interface Access List

このオプションをオフにすることにより、アクセス ルールをローカル IP アドレスに適用することを強制的に適用できます。アクセス ルールはローカル IP アドレスに適用され、VPN パケットが復号化される前に使用されていた元のクライアント IP アドレスには適用されません。

- インターフェイスの access-lists を迂回するには、インバウンド IPSec セッションをイネーブルにします。グループ ポリシーおよびユーザ単位の許可アクセス リストは、引き続きトラフィックに適用されます。セキュリティ アプライアンスは、VPN トラフィックがセキュリティ アプライアンス インターフェイスで終了することをデフォルトで許可しているため、IKE または ESP（またはその他のタイプの VPN パケット）をアクセス ルールで許可する必要はありません。このオプションをオンにしている場合は、復号化された VPN パケットのローカル IP アドレスに対するアクセス ルールは不要です。VPN トンネルは VPN セキュリティ メカニズムを使用して正常に終端されたため、この機能によって、コンフィギュレーションが簡略化され、セキュリティ アプライアンスのパフォーマンスはセキュリティ リスクを負うことなく最大化されます （グループ ポリシーおよびユーザ単位の許可アクセス リストは、引き続きトラフィックに適用されます）。

SSO Servers

[SSO Server] ウィンドウでは、Computer Associates SiteMinder SSO サーバまたは Security Assertion Markup Language（SAML）バージョン 1.1 Browser Post Profile SSO サーバに接続するクライアントレス SSL VPN のユーザの、シングル サインオン（SSO）を設定または削除できます。クライアントレス SSL VPN でだけ使用できる SSO のサポートにより、ユーザは、ユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。

SSO の方式は、基本 HTTP または NTLMv1 認証を使用した自動サインオン、HTTP Form プロトコル、Computer Associates eTrust SiteMinder（以前の名称は Netegrity SiteMinder）、または SAML バージョン 1.1 Browser Post Profile の 4 方式の中から選択できます。

（注）　SAML Browser Artifact プロファイル方式のアサーション交換は、サポートされていません。

この項では、SiteMinder と SAML Browser Post Profile を使用して SSO を設定する手順について説明します。

- 基本 HTTP または NTLM 認証で SSO を設定するには、Auto Signon を参照してください。
- HTTP Form プロトコルで SSO を設定するには、HTTP Form でのクライアントレス SSL VPN に対する SSO のサポートを参照してください。

SSO のメカニズムは、AAA プロセス（HTTP Form）の一部として開始されるか、AAA サーバ（SiteMinder）または SAML Browser Post Profile サーバへのユーザ認証に成功した直後に開始されます。これらの場合、セキュリティ アプライアンス 上で実行されているクライアントレス SSL VPN サーバは、認証サーバに対するユーザのプロキシとして機能します。ユーザがログインすると、クライアントレス SSL VPN サーバは、ユーザ名とパスワードを含む SSO 認証要求を HTTPS を使用して認証サーバに送信します。

認証サーバが認証要求を承認すると、SSO 認証クッキーがクライアントレス SSL VPN サーバに返されます。このクッキーは、ユーザの代理としてセキュリティ アプライアンスで保持され、ユーザ認証でこのクッキーを使用して、SSO サーバで保護されているドメイン内部の Web サイトの安全を確保します。

SiteMinder と SAML Browser Post Profile

SiteMinder または SAML Browser Post Profile による SSO 認証は AAA から切り離されており、AAA プロセスの完了後に実施されます。ユーザまたはグループが対象の SiteMinder SSO を設定するには、まず AAA サーバ（RADIUS や LDAP など）を設定する必要があります。AAA サーバがユーザを認証した後、クライアントレス SSL VPN サーバは、HTTPS を使用して認証要求を SiteMinder SSO サーバに送信します。

SiteMinder SSO の場合は、セキュリティ アプライアンスの設定を行う以外に、シスコの認証スキームによって CA SiteMinder Policy Server を設定する必要があります。シスコの認証スキームの SiteMinder への追加を参照してください。

SAML Browser Post Profile の場合は、認証で使用する Web Agent（Protected Resource URL）を設定する必要があります。SAML Browser Post Profile SSO サーバの設定の詳細については、「SAML POST SSO サーバのコンフィギュレーション」を参照してください。

フィールド

- [Server Name]：*表示専用*。設定された SSO サーバの名前を表示します。入力できる文字の範囲は、4 ～ 31 文字です。

- [Authentication Type]：*表示専用*。SSO サーバのタイプを表示します。セキュリティ アプライアンスは現在、SiteMinder タイプと SAML Browser Post Profile タイプをサポートしています。
- [URL]：*表示専用*。セキュリティ アプライアンスが SSO 認証要求を行う SSO サーバの URL を表示します。
- [Secret Key]：*表示専用*。SSO サーバとの認証通信の暗号化に使用される秘密キーを表示します。キーは、任意の標準またはシフト式英数字で構成されます。文字の最小数や最大数の制限はありません。
- [Maximum Retries]：*表示専用*。SSO 認証が失敗した場合にセキュリティ アプライアンスがリトライする回数を表示します。リトライの範囲は 1 ～ 5 回で、デフォルトのリトライ数は 3 回です。
- [Request Timeout (seconds)]：*表示専用*。失敗した SSO 認証試行をタイムアウトさせるまでの秒数を表示します。範囲は 1 ～ 30 秒で、デフォルトの秒数は 5 秒です。
- [Add/Edit]：[Add/Edit SSO Server] ダイアログボックスを開きます。
- [Delete]：選択した SSO サーバを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

SAML POST SSO サーバのコンフィギュレーション

サーバ ソフトウェア ベンダーが提供する SAML サーバのマニュアルに従って、SAML サーバを Relying Party モードで設定します。次の手順には、Browser Post Profile に SAML サーバを設定するために必要な値が一覧表示されています。

ステップ 1　アサーティング パーティ（セキュリティ アプライアンス）を表す SAML サーバ パラメータを設定します。

- 宛先コンシューマ（Web Agent）URL（ASA で設定されるアサーション コンシューマ URL と同じ）
- Issuer ID（通常はアプライアンスのホスト名である文字列）
- Profile type：Browser Post Profile

ステップ 2　証明書を設定します。

ステップ 3　アサーティング パーティのアサーションには署名が必要なことを指定します。

ステップ 4　SAML サーバがユーザを特定する方法を、次のように選択します。

- Subject Name Type が DN
- Subject Name format が uid=<user>

シスコの認証スキームの SiteMinder への追加

SiteMinder による SSO を使用するためのセキュリティ アプライアンスの設定に加え、Java プラグインとして提供されている、シスコの認証スキームを使用するようにユーザの CA SiteMinder Policy Server を設定する必要もあります。

（注）
- SiteMinder Policy Server を設定するには、SiteMinder の経験が必要です。
- この項では、手順のすべてではなく、一般的なタスクを取り上げます。
- カスタム認証スキームを追加するための完全な手順については、CA SiteMinder のマニュアルを参照してください。

ユーザの SiteMinder Policy Server にシスコの認証スキームを設定するには、次のタスクを実行します。

ステップ 1　Siteminder Administration ユーティリティを使用して、次の特定の引数を使用できるようにカスタム認証スキームを作成します。
- [Library] フィールドに、**smjavaapi** と入力します。
- [Secret] フィールドで、[Add SSO Server] ダイアログの [Secret Key] フィールドで設定したものと同じ秘密キーを入力します。
- [Parameter] フィールドに、**CiscoAuthAPI** と入力します。

ステップ 2　Cisco.com にログインして、http://www.cisco.com/cisco/software/navigator.html から **cisco_vpn_auth.jar** ファイルをダウンロードして、SiteMinder サーバのデフォルトのライブラリ ディレクトリにコピーします。この .jar ファイルは、Cisco セキュリティ アプライアンス CD にも含まれています。

Add/Edit SSO Servers

（注）　この SSO 方式では、CA SiteMinder と SAML Browser Post Profile を使用します。また、HTTP Form プロトコルまたは基本 HTML および NTLM 認証を使用して SSO を設定することもできます。HTTP Form プロトコルを使用する場合は、「HTTP Form でのクライアントレス SSL VPN に対する SSO のサポート」を参照してください。基本 HTML または NTLM 認証を使用するように設定する場合は、コマンドライン インターフェイスで **auto-signon** コマンドを使用します。

フィールド

- [Server Name]：サーバを追加する場合は、新しい SSO の名前を入力します。サーバを編集する場合、このフィールドは表示専用です。選択した SSO サーバの名前が表示されます。
- [Authentication Type]：*表示専用*。SSO サーバのタイプを表示します。セキュリティ アプライアンスが現在サポートしているタイプは、SiteMinder と SAML Browser Post Profile です。
- [URL]：セキュリティ アプライアンスが SSO 認証要求を行う SSO サーバの URL を入力します。

- [Secret Key]：SSO サーバへの認証要求を暗号化するために使用する秘密キーを入力します。キーに使用する文字には、通常の英数字と、シフト キーを押して入力した英数字を使用できます。文字の最小数や最大数の制限はありません。秘密キーはパスワードに似ており、作成、保存、設定ができます。Cisco Java プラグイン認証スキームを使用して、セキュリティ アプライアンス、SSO サーバ、および SiteMinder Policy Server で設定されます。
- [Maximum Retries]：失敗した SSO 認証試行をセキュリティ アプライアンスが再試行する回数を入力します。この回数を超えて失敗すると認証タイムアウトになります。範囲は 1 ～ 5 回で、1 回と 5 回も含まれます。デフォルトは 3 回です。
- [Request Timeout]：失敗した SSO 認証試行をタイムアウトさせるまでの秒数を入力します。範囲は 1 ～ 30 秒で、1 秒と 30 秒も含まれます。デフォルトは 5 秒です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

サーバと URL

ASDM の [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] ウィンドウでは、クライアントレス SSL VPN 接続によるアクセス用のサーバと URL リストを確認し、追加し、読み込むことができます。

（注） ファイル ブラウジングでは、NetBIOS サーバを設定する必要があります（[Configuration] > [VPN] > [General] > [Tunnel Group] > [Add/Edit Tunnel Group] > [WebVPN] > [NetBIOS Servers]）。

フィールド

[Add/Edit Bookmark List] ウィンドウでは、WebVPN を介したアクセスに使用するサーバと URL のリストを設定します。ファイルおよび URL アクセスを設定するには、ファイル サーバおよび URL の 1 つ以上の名前付きリストを作成してから、そのリスト名を個々のユーザに割り当てる（[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account] / [VPN Policy] > [Clientless SSL VPN] ウィンドウ）か、グループ ポリシーに割り当てます（[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add/Edit Group Policy] > [Portal] ウィンドウ）。ユーザまたはグループ ポリシーに関連付けることができるリストは 1 つだけです。

[Add/Edit Bookmark List] ダイアログボックスでは、URL リストを追加、編集、または削除でき、指定された URL リストの項目を並べ替えることもできます。

フィールド

- [Bookmark List Name]：追加するリストの名前を指定するか、修正または削除するリストの名前を選択します。
- [Name]：ユーザに表示する URL 名を指定します。

- [URL]：表示名に関連付けられている URL を指定します。
- [Add]：[Add Bookmark Entry] ダイアログボックスを開きます。このダイアログボックスでは、新しいサーバまたは URL と表示名を設定できます。
- [Edit]：[Edit Bookmark Entry] ダイアログボックスを開きます。このダイアログボックスでは、新しいサーバまたは URL と表示名を設定できます。
- [Delete]：選択した項目を URL リストから削除します。確認されず、やり直しもできません。
- [Move Up/Move Down]：URL リストでの選択した項目の位置を変更します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

スマート トンネル アクセスの設定

[Smart Tunnels] テーブルには、スマート トンネルのリストが表示されます。各リストは、スマート トンネル アクセスに適格な 1 つ以上のアプリケーションと、対応する OS で構成されています。各グループ ポリシーまたはローカル ユーザ ポリシーでは 1 つのスマート トンネル リストがサポートされているため、ブラウザベースではないアプリケーションをサポート対象とするために、グループ化してスマート トンネル リストに加える必要があります。リストのコンフィギュレーションに続いて、1 つ以上のグループ ポリシーまたはローカル ユーザ ポリシーに割り当てることができます。

[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] ウィンドウでは、次のことを行えます。

- スマート トンネル リストを追加し、リストにアプリケーションを追加するには、[Add] をクリックします。[Add Smart Tunnel List] ダイアログボックスが開きます。リストに名前を付けたら、もう一度 [Add] をクリックします。ASDM が [Add Smart Tunnel Entry] ダイアログボックスを開きます。このダイアログボックスでは、スマート トンネルの属性をリストに割り当てることができます。属性を割り当てて [OK] をクリックすると、ASDM のリストにそれらの属性が表示されます。必要に応じて手順を繰り返してリストを完成させ、[Add Smart Tunnel List] ダイアログボックスで [OK] をクリックします。
- スマート トンネル リストを変更するには、そのリストをダブルクリックするか、またはテーブル内のリストを選択して [Edit] をクリックします。次に、[Add] をクリックしてスマート トンネル属性の新しいセットをリストに挿入するか、またはリストのエントリを選択して [Edit] または [Delete] をクリックします。
- リストを削除するには、テーブル内のリストを選択して [Delete] をクリックします。

スマート トンネル リストの設定と割り当てを行った後は、サービスのブックマークを追加し、[Edit Bookmark] ダイアログボックスの [Enable Smart Tunnel Option] をクリックすることで、スマート トンネルを簡単に使えるようにできます。

スマート トンネルについて

スマート トンネルは、TCP ベースのアプリケーションとプライベート サイト間の接続です。このスマート トンネルは、セキュリティ アプライアンスをパスウェイとして、また、セキュリティ アプライアンスをプロキシ サーバとして使用するクライアントレス（ブラウザベース）SSL VPN セッションを使用します。スマート トンネル アクセスを許可するアプリケーションを特定し、各アプリケーションのローカル パスを指定できます。Microsoft Windows で実行するアプリケーションの場合は、チェックサムの SHA-1 ハッシュの一致を、スマート トンネル アクセスを許可する条件として要求もできます。

Lotus SameTime および Microsoft Outlook Express は、スマート トンネル アクセスを許可できるアプリケーションの例です。

スマート トンネルを設定するには、アプリケーションがクライアントであるか、Web 対応アプリケーションであるかに応じて、次の手順のいずれかを実行する必要があります。

- クライアント アプリケーションの 1 つ以上のスマート トンネル リストを作成し、スマート トンネル アクセスを提供するグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。
- スマート トンネル アクセスに適格な Web 対応アプリケーションの URL を指定するブックマーク リスト エントリを 1 つ以上作成し、スマート トンネル アクセスを提供する DAP、グループ ポリシー、ローカル ユーザ ポリシーにそのリストを割り当てます。

また、クライアントレス SSL VPN セッションを介したスマート トンネル接続でのログイン クレデンシャルの送信を自動化する Web 対応アプリケーションのリストも作成できます。

スマート トンネルを使用する理由

スマート トンネル アクセスを使用すると、クライアントの TCP ベースのアプリケーションがブラウザベースの VPN 接続を使用してサービスに接続します。この方法では、プラグインやレガシー テクノロジーであるポート転送と比較して、ユーザには次のような利点があります。

- スマート トンネルは、プラグインよりもパフォーマンスが向上します。
- ポート転送とは異なり、スマート トンネルでは、ローカル ポートへのローカル アプリケーションのユーザ接続を要求しないことにより、ユーザ エクスペリエンスが簡略化されます。
- ポート転送とは異なり、スマート トンネルでは、ユーザは管理者特権を持つ必要がありません。

プラグインの利点は、クライアント アプリケーションをリモート コンピュータにインストールする必要がないという点です。

スマート トンネルの要件および制限

以降のセクションでは、スマート トンネルの要件と制限事項について分類ごとに説明します。

一般的な要件と制限事項

スマート トンネルには、次の一般的な要件と制限事項があります。

- スマート トンネル接続を開始するリモート ホストでは、32 ビット バージョンの Microsoft Windows Vista、Windows XP、Windows 2000、Mac OS 10.4 または 10.5 が実行されている必要があります。

- スマート トンネルの自動サインオンは、Windows の Microsoft Internet Explorer だけサポートします。
- ブラウザで Java、Microsoft ActiveX、またはその両方をイネーブルにする必要があります。
- スマート トンネルは、Microsoft Windows を実行しているコンピュータとセキュリティ アプライアンス間に配置されたプロキシだけをサポートします。スマート トンネルは、Internet Explorer 設定（つまり、Windows でシステム全体での使用を目的とした設定）を使用します。リモート コンピュータがセキュリティ アプライアンスにアクセスするためにプロキシ サーバを必要とする場合、接続の終端側の URL が、プロキシ サービスから除外される URL のリストに存在する必要があります。プロキシ設定で、ASA を宛先とするトラフィックのプロキシ経由を指定すると、すべてのスマート トンネル トラフィックがプロキシ経由になります。

  HTTP ベースのリモート アクセスのシナリオでは、サブネットが VPN ゲートウェイへのユーザ アクセスを提供しない場合があります。この場合、Web とエンド ユーザの場所との間のトラフィックをルーティングするために ASA の前に配置されているプロキシが、Web アクセスを提供します。ただし、ASA の前に配置されるプロキシを設定できるのは、VPN ユーザだけです。このように実行する場合、これらのプロキシが CONNECT 方式をサポートすることを確認する必要があります。認証が必要なプロキシの場合、スマート トンネルは、基本ダイジェスト認証タイプだけをサポートします。
- スマート トンネルが開始されると、セキュリティ アプライアンスは、ブラウザ プロセスが同じである場合に VPN セッション経由ですべてのブラウザ トラフィックをデフォルトで送信します。tunnel-all ポリシーが適用されている場合にも、セキュリティ アプライアンスは同じ処理を行います。ユーザがブラウザ プロセスの別のインスタンスを開始すると、VPN セッション経由ですべてのトラフィックが送信されます。ブラウザ プロセスが同じで、セキュリティ アプライアンスが URL へのアクセスを提供しない場合、ユーザはその URL を開くことはできません。回避策として、tunnel-all ではないトンネル ポリシーを割り当てます。
- ステートフル フェールオーバーが発生したとき、スマート トンネル接続は保持されません。ユーザはフェールオーバー後に再接続する必要があります。

Windows の要件と制限事項

次の要件と制限は Windows だけに適用されます。

- Winsock 2 の TCP ベースのアプリケーションだけ、スマート トンネル アクセスに適します。
- セキュリティ アプライアンスは Microsoft Outlook Exchange（MAPI）プロキシをサポートしていません。ポート転送もスマート トンネルも MAPI をサポートしません。MAPI プロトコルを使用した Microsoft Outlook Exchange 通信では、リモート ユーザが AnyConnect を使用する必要があります。
- スマート トンネルまたはポート転送を使用する Microsoft Windows Vista ユーザは、ASA の URL を信頼済みサイト ゾーンに追加する必要があります。信頼済みサイト ゾーンにアクセスするには、Internet Explorer を起動し、[Tools] > [Internet Options] > [Security] タブを選択する必要があります。Vista ユーザは、保護モードをディセーブルにしてスマート トンネル アクセスの使用もできます。ただし、攻撃を受けやすくなるため、この方法の使用はお勧めしません。

Mac OS の要件と制限事項

次の要件と制限は Mac OS だけに適用されます。

- Safari 3.1.1 以降または Firefox 3.0 以降。
- Sun JRE 1.5 以降。

- ポータル ページから起動されたアプリケーションだけ、スマート トンネル接続を確立できる。この要件には、Firefox に対するスマート トンネルのサポートも含まれます。スマート トンネルを最初に使用する際に、Firefox を使用して Firefox の別のインスタンスを起動するには、csco_st という名前のユーザ プロファイルが必要です。このユーザ プロファイルが存在しない場合、セッションでは、作成するようにユーザに要求します。
- SSL ライブラリにダイナミックにリンクされている TCP を使用するアプリケーションは、スマート トンネルを介して動作できる。
- Mac OS では、スマート トンネルは次をサポートしない。
  - プロキシ サービス
  - 自動サインオン
  - 2 つのレベルの名前スペースを使用するアプリケーション
  - Telnet、SSH、cURL などのコンソールベースのアプリケーション
  - dlopen または dlsym を使用して libsocket コールを見つけ出すアプリケーション
  - libsocket コールを見つけ出すスタティックにリンクされたアプリケーション

スマート トンネルの設定（Lotus の例）

スマート トンネルを設定するには、次の手順を実行します。

（注）　この例では、アプリケーションでのスマート トンネル サポートを追加するために必要な最小限の指示だけを示します。詳細については、以降の各項にあるフィールドの説明を参照してください。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] を選択します。

ステップ 2　アプリケーションを追加するスマート トンネル リストをダブルクリックするか、または [Add] をクリックしてアプリケーションのリストを作成し、[List Name] フィールドにそのリストの名前を入力して [Add] をクリックします。

たとえば、[Smart Tunnels] ペインで [Add] をクリックし、[List Name] フィールドに Lotus と入力して [Add] をクリックします。

ステップ 3　[Add or Edit Smart Tunnel List] ダイアログボックスで [Add] をクリックします。

ステップ 4　[Application ID] フィールドに、スマート トンネル リスト内のエントリに対する一意のインデックスとして使用する文字列を入力します。

ステップ 5　[Process Name] ダイアログボックスに、ファイル名とアプリケーションの拡張子を入力します。

表 34-1 に、[Application ID] 文字列の例と、Lotus をサポートするために必要な関連付けられたパスを示します。

表 34-1　スマート トンネルの例：Lotus 6.0 Thick Client with Domino Server 6.5.5

アプリケーション ID の例	必要最小限のプロセス名
lotusnotes	notes.exe
lotusnlnotes	nlnotes.exe
lotusntaskldr	ntaskldr.exe
lotusnfileret	nfileret.exe

ステップ 6　[OS] の横の [Windows] を選択します。

ステップ 7　[OK] をクリックします。

ステップ 8　リストに追加するアプリケーションごとに、ステップ 3 ～ 7 を繰り返します。

ステップ 9　[Add or Edit Smart Tunnel List] ダイアログボックスで [OK] をクリックします。

ステップ 10　次のようにして、関連付けられたアプリケーションへのスマート トンネル アクセスを許可する、グループ ポリシーとローカル ユーザ ポリシーにリストを割り当てます。

- グループ ポリシーにリストを割り当てるには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add] または [Edit] > [Portal] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。
- ローカル ユーザ ポリシーにリストを割り当てるには、[Configuration] > [Remote Access VPN] > [AAA Setup] > [Local Users] > [Add] または [Edit] > [VPN Policy] > [Clientless SSL VPN] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。

Add or Edit Smart Tunnel List

[Add Smart Tunnel List] ダイアログボックスでは、スマート トンネル エントリのリストをセキュリティ アプライアンスのコンフィギュレーションに追加できます。[Edit Smart Tunnel List] ダイアログボックスでは、リストの内容を修正できます。

フィールド

- [List Name] : アプリケーションまたはプログラムのリストに付ける一意の名前を入力します。名前に使用される文字数には制限はありません。スペースは使用しないでください。

  スマート トンネル リストのコンフィギュレーションに続いて、クライアントレス SSL VPN のグループ ポリシーとローカル ユーザ ポリシーの [Smart Tunnel List] 属性の横にリスト名が表示されます。他に設定する可能性があるリストと、内容および目的を区別できるような名前を付けてください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add or Edit Smart Tunnel Entry

[Add or Edit Smart Tunnel Entry] ダイアログボックスでは、スマート トンネル リストにあるアプリケーションの属性を指定できます。

- [Application ID]：スマート トンネル リストのエントリに命名する文字列を入力します。この文字列は、OS ごとに一意です。通常は、スマート トンネル アクセスを許可されるアプリケーションに付けられる名前です。異なるパスまたはハッシュ値を指定するアプリケーションの複数バージョンをサポートするには、この属性を使用してエントリを差別化し、OS、および各リスト エントリによってサポートされているアプリケーションの名前とバージョンの両方を指定します。文字列は最大 64 文字まで使用できます。
- [Process Name]：アプリケーションのファイル名またはパスを入力します。ストリングには最大 128 文字を使用できます。

  Windows では、アプリケーションにスマート トンネル アクセスを許可する場合に、この値とリモート ホストのアプリケーション パスの右側の値が完全に一致している必要があります。Windows でファイル名のみを指定すると、SSL VPN では、アプリケーションにスマート トンネル アクセスを許可する場合に、リモート ホストに対して場所の制限を強制しません。

  アプリケーションのパスを指定し、ユーザが別の場所にインストールした場合は、そのアプリケーションは許可されません。アプリケーションは、入力する値と文字列の右側の値が一致している限り、任意のパスに配置できます。

  アプリケーションがリモート ホストの複数のパスのいずれかにある場合に、アプリケーションにスマート トンネル アクセスを許可するには、このフィールドにアプリケーションの名前と拡張子だけを指定するか、またはパスごとに固有のスマート トンネル エントリを作成します。

  （注） スマート トンネル アクセスで突然問題が発生する場合、*Process Name* 値がアップグレードされたアプリケーションに対して最新ではない可能性があります。たとえば、アプリケーションへのデフォルト パスは、そのアプリケーションおよび次のアップグレード版を製造する企業が買収されると変更されることがあります。

  Windows の場合、コマンド プロンプトから開始したアプリケーションにスマート トンネル アクセスを追加する場合は、スマート トンネル リストの 1 つのエントリの Process Name に「cmd.exe」を指定し、別のエントリにアプリケーション自体へのパスを指定する必要があります。これは「cmd.exe」がアプリケーションの親であるためです。

  Mac OS では、プロセスへのフル パスが必要です。また、このパスは大文字と小文字が区別されます。各ユーザ名のパスを指定しないようにするには、部分パスの前にチルダ（~）を入力します（例：~/bin/vnc）。
- [OS]：[Windows] または [Mac] をクリックし、アプリケーションのホスト OS を指定します。
- [Hash]：（オプション。Windows にだけ適用）この値を取得するには、アプリケーションのチェックサム（つまり、実行ファイルのチェックサム）を、SHA-1 アルゴリズムを使用してハッシュ計算するユーティリティに入力します。このようなユーティリティの例として、Microsoft File Checksum Integrity Verifier（FCIV; ファイル チェックサム整合性検証）を挙げることができます。このユーティリティは、http://support.microsoft.com/kb/841290/ で入手できます。FCIV のインストール後、スペースを含まないパス（c:/fciv.exe など）に、ハッシュするアプリケーションの一時コピーを置き、コマンドラインで **fciv.exe -sha1** *application* と入力して（**fciv.exe -sha1 c:\msimn.exe** など）、SHA-1 ハッシュを表示します。

  SHA-1 ハッシュは、常に 16 進数 40 文字です。

  クライアントレス SSL VPN は、アプリケーションにスマート トンネル アクセスの許可を与える前に、[Application ID] に一致するアプリケーションのハッシュを計算します。結果が [*Hash*] の値と一致すれば、アプリケーションにスマート トンネル アクセスの資格を与えます。

ハッシュを入力することにより、[*Application ID*] で指定した文字列に一致する不正ファイルに対して SSL VPN が資格を与えないようにしています。チェックサムは、アプリケーションのバージョンまたはパッチによって異なるため、入力する [*Hash*] 値は、リモート ホストの 1 つのバージョンやパッチにしか一致しない可能性があります。複数のバージョンのアプリケーションにハッシュを指定するには、[*Hash*] 値ごとに固有のスマート トンネル エントリを作成します。

（注） [*Hash*] を入力し、スマート トンネル アクセスで今後のバージョンまたはパッチのアプリケーションをサポートする場合は、将来的にスマート トンネル リストを更新する必要が生じます。スマート トンネル アクセスに突然問題が発生した場合は、[*Hash*] 値を含むアプリケーション リストが、アプリケーションのアップグレードによって最新の状態になっていない可能性があります。この問題は hash を入力しないことによって回避できます。

スマート トンネル リストのコンフィギュレーションに続いて、そのリストをアクティブにするには、グループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てる必要があります。

- グループ ポリシーにリストを割り当てるには、[Config] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add] または [Edit] > [Portal] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。
- ローカル ユーザ ポリシーにリストを割り当てるには、[Config] > [Remote Access VPN] > [AAA Setup] > [Local Users] > [Add] または [Edit] > [VPN Policy] > [Clientless SSL VPN] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。

表 34-2　スマート トンネル エントリの例

スマート トンネルのサポート	アプリケーション ID（一意の文字列であればどれでも OK）	プロセス名	OS
Mozilla Firefox	firefox	firefox.exe	Windows
Microsoft Outlook Express	outlook-express	msimn.exe	Windows
より制限的なオプション：実行ファイルが事前定義済みのパスにある場合は、Microsoft Outlook Express 専用。	outlook-express	\Program Files\Outlook Express\msimn.exe	Windows
Mac で新しいターミナル ウィンドウを開く（ワンタイムパスワードが実装されているので、それ以降、同じターミナル ウィンドウでのアプリケーションの起動は失敗します）。	terminal	Terminal	Mac
新しいウィンドウでスマート トンネルを開始	new-terminal	Terminal open -a MacTelnet	Mac
Mac ターミナル ウィンドウでアプリケーションを起動	curl	Terminal curl www.example.com	Mac

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

次の作業

スマート トンネル リストのコンフィギュレーションに続いて、そのリストをアクティブにするには、次のようにグループ ポリシーまたはユーザ名にそのリストを割り当てる必要があります。

- グループ ポリシーにリストを割り当てるには、[Config] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add] または [Edit] > [Portal] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。
- ユーザ名にリストを割り当てるには、[Config] > [Remote Access VPN] > [AAA Setup] > [Local Users] > [Add] または [Edit] > [VPN Policy] > [Clientless SSL VPN] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。

カスタマイゼーション オブジェクトの設定

クライアントレス SSL VPN ポータル上で見ることができるすべてのエンドユーザ コンテンツは、カスタマイズできます。カスタマイズするには、ASDM で Customization Editor という XML テンプレートを使用するか、すでに存在するカスタマイゼーション オブジェクトをエクスポートして編集してから、セキュリティ アプライアンスに再インポートします。

バージョン 8.0 ソフトウェアでは、カスタマイゼーションの設定機能が拡張されており、新しいプロセスは以前のバージョンと互換性がありません。8.0 ソフトウェアへのアップグレードの間、セキュリティ アプライアンスは、古い設定を使用して新しいカスタマイゼーション オブジェクトを作成することにより、現在のコンフィギュレーションを維持します。このプロセスは 1 回のみ実行されます。また、古い値は新しい値の一部を構成するサブセットに過ぎないため、このプロセスは古い形式から新しい形式への単なる変換ではありません。

（注） バージョン 7.2 ポータルのカスタマイズと URL リストは、バージョン 8.0 にアップグレードする*前*にバージョン 7.2（x）のコンフィギュレーション ファイルの適切なインターフェイスでクライアントレス SSL VPN（WebVPN）がイネーブルになっていた場合にだけ、Beta 8.0 コンフィギュレーションで使用できます。

現在のペインで、テンプレートに基づいて新しいカスタマイゼーション オブジェクトを追加するか、すでにインポート済みのカスタマイゼーション オブジェクトを修正できます。

フィールド

[Add] : [Add Customization] ペインを表示します。このペインでは、デフォルトのカスタマイゼーション オブジェクトのコピーを作成し、一意の名前を付けて保存できます。その後、ASDM SSL VPN Customization Editor を使用して、要件に応じてオブジェクトを修正できます。

[Edit] : 既存の選択されたカスタマイゼーション オブジェクトを編集します。クリックすると、SSL VPN Customization Editor が起動します。

[Delete] : カスタマイゼーション オブジェクトを削除します。

[Import]：XML ファイル形式のカスタマイゼーション オブジェクトをインポートします。XML ファイルの作成の詳細については、「XML ベースのポータル カスタマイゼーション オブジェクトおよび URL リストの作成」を参照してください。

[Export]：選択した既存のカスタマイゼーション オブジェクトをエクスポートします。エクスポートにより、そのオブジェクトを編集し、このセキュリティ アプライアンスか別のセキュリティ アプライアンスに再インポートできます。

[Customization Objects]：セキュリティ アプライアンスの既存のカスタマイゼーション オブジェクトを一覧表示します。

[OnScreen Keyboard]：エンド ユーザに対して OnScreen Keyboard を表示するタイミングを指定します。このキーボードを使用することにより、ログインや認証を行う場合にキーボードのキーを押してパスワードを入力する必要がなくなるため、セキュリティを高めることができます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

カスタマイゼーション オブジェクトの追加

カスタマイゼーション オブジェクトを追加するには、DfltCustomization オブジェクトのコピーを作成して一意の名前を付けます。次に、要件に合うようにそのオブジェクトを修正または編集できます。

フィールド

[Customization Object Name]：新しいカスタマイゼーション オブジェクトの名前を入力します。最大 64 文字で、スペースは使用できません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

カスタマイゼーション オブジェクトのインポートおよびエクスポート

既存のカスタマイゼーション オブジェクトをインポートまたはエクスポートできます。インポートするのは、エンド ユーザに適用するオブジェクトです。セキュリティ アプライアンスにすでに存在するカスタマイゼーション オブジェクトは、編集のためにエクスポートし、その後再インポートできます。

フィールド

- [Customization Object Name]：カスタマイゼーション オブジェクトを名前で特定します。最大 64 文字で、スペースは使用できません。
- [Select a file]：カスタマイゼーション ファイルをインポートまたはエクスポートするときに使用する方式を選択します。
  - [Local computer]：ローカル PC にあるファイルをインポートする場合は、この方式を選択します。
  - [Path]：ファイルへのパスを入力します。
  - [Browse Local Files]：ファイルへのパスを参照します。
  - [Flash file system]：セキュリティ アプライアンスに常駐するファイルをエクスポートするには、この方式を選択します。
  - [Path]：ファイルへのパスを入力します。
  - [Browse Flash]：ファイルへのパスを参照します。
  - [Remote server]：セキュリティ アプライアンスからアクセスできるリモート サーバに常駐するカスタマイゼーション ファイルをインポートするには、このオプションを選択します。
  - [Path]：ファイルにアクセスする方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
- [Import Now]/[Export Now]：クリックすると、ファイルをインポートまたはエクスポートします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

XML ベースのポータル カスタマイゼーション オブジェクトおよび URL リストの作成

この項では、次のトピックについて取り上げます。

- XML カスタマイゼーション ファイルの構成について
- カスタマイゼーションの例
- カスタマイゼーション テンプレートの使用

XML カスタマイゼーション ファイルの構成について

表 34-3 に、XML カスタマイゼーション オブジェクトのファイル構造を示します。

（注）　XML カスタマイゼーション ファイルの空白のタグ <param></param> は、微小値（(hostname)# param value "" ）を含む CLI コマンドに相当します。
パラメータ / タグが指定されなければデフォルト / 継承値が使用されます。存在する場合は、空の文字列であってもパラメータ / タグ値が設定されます。

表 34-3　XML ベース カスタマイゼーション ファイルの構造

タグ	タイプ	値	プリセット値	説明
custom	**ノード**			**ルート タグ**
auth-page	**ノード**			**認証ページ コンフィギュレーションのタグ コンテナ**
window	**ノード**			**ブラウザ ウィンドウ**
title-text	文字列	任意の文字列	空の文字列	
title-panel	**ノード**			**ロゴおよびテキストを表示したページの先頭パネル**
mode	テキスト	イネーブル|ディセーブル	ディセーブル	
text	テキスト	任意の文字列	空の文字列	
logo-url	テキスト	任意の URL	空のイメージ URL	
copyright-panel	**ノード**			**著作権情報を示したページの下部パネル**
mode	テキスト	イネーブル|ディセーブル	ディセーブル	
text	テキスト	任意の URL	空の文字列	
info-panel	**ノード**			**カスタム テキストとイメージを表示したパネル**
mode	文字列	イネーブル|ディセーブル	ディセーブル	
image-position	文字列	**above**|below	above	テキストに対する相対的なイメージの位置
image-url	文字列	任意の URL	空のイメージ	
text	文字列	任意の文字列	空の文字列	
logon-form	**ノード**			**ユーザ名、パスワード、グループ プロンプトのフォーム**
title-text	文字列	任意の文字列	Logon	
message-text	文字列	任意の文字列	空の文字列	
username-prompt-text	文字列	任意の文字列	Username	
password-prompt-text	文字列	任意の文字列	Password	

表 34-3　XML ベース カスタマイゼーション ファイルの構造 （続き）

internal-password-prompt-text	文字列	任意の文字列	Internal Password	
group-prompt-text	文字列	任意の文字列	Group	
submit-button-text	文字列	任意の文字列	Logon	
logout-form	**ノード**			**ログアウト メッセージと、ログインまたはウィンドウを閉じるためのボタンを表示したフォーム**
title-text	文字列	任意の文字列	Logout	
message-text	文字列	任意の文字列	空の文字列	
login-button-text	文字列	任意の文字列	Login	
close-button-text	文字列	任意の文字列	Close window	
language-selector	**ノード**			**言語を選択するドロップダウン ボックス**
mode	文字列	イネーブル|ディセーブル	disable	
title	テキスト		Language	言語を選択するよう求めるプロンプト テキスト
language	**ノード（複数）**			
code	文字列			
text	文字列			
portal	**ノード**			**ポータル ページ コンフィギュレーションのタグコンテナ**
window	**ノード**			**認証ページの説明を参照**
title-text	文字列	任意の文字列	空の文字列	
title-panel	**ノード**			**認証ページの説明を参照**
mode	文字列	イネーブル|ディセーブル	Disable	
text	文字列	任意の文字列	空の文字列	
logo-url	文字列	任意の URL	空のイメージ URL	
navigation-panel	**ノード**			**アプリケーション タブの左側のパネル**
mode	文字列	イネーブル|ディセーブル	enable	

表 34-3　XML ベース カスタマイゼーション ファイルの構造 （続き）

application	**ノード（複数）**		**該当なし**	**ノードは（ID によって）設定されているアプリケーションのデフォルトを変更する**
id	文字列	ストック アプリケーションの場合： web-access file-access app-access net-access help ins の場合： 固有のプラグイン	該当なし	
tab-title	文字列		該当なし	
order	番号		該当なし	エレメントの並べ替えで使用する値。デフォルトのエレメント順の値には、1000、2000、3000 などの段階があります。たとえば、最初と 2 番目のエレメントの間にエレメントを挿入するには、1001 ～ 1999 の値を使用します。
url-list-title	文字列		該当なし	アプリケーションにブックマークがある場合は、グループ化されたブックマークを表示したペインのタイトル
mode	文字列	イネーブル|ディセーブル	該当なし	
toolbar	**ノード**			
mode	文字列	イネーブル|ディセーブル	イネーブル	
prompt-box-title	文字列	任意の文字列	Address	URL プロンプト ボックスのタイトル
browse-button-text	文字列	任意の文字列	ブラウズ	[Browse] ボタンのテキスト
logout-prompt-text	文字列	任意の文字列	Logout	
column	**ノード（複数）**			**デフォルトで 1 列を表示**

表 34-3　XML ベース カスタマイゼーション ファイルの構造 （続き）

width	文字列		該当なし	
order	番号		該当なし	エレメントの並べ替えで使用する値。
url-lists	**ノード**			**URL リストは、明示的にディセーブルになっていない場合、ポータル ホーム ページのデフォルト エレメントと見なされる**
mode	文字列	group | nogroup	group	モード： group：Web Bookmarks や File Bookmarks などのアプリケーション タイプによってグループ化されたエレメント no-group：URL リストを別々のペインに表示する disable：デフォルトで URL リストを表示しない
pane	**ノード（複数）**			**追加ペインの設定を許可**
mode	文字列	イネーブル|ディセーブル		コンフィギュレーションを削除せずにペインを一時的にディセーブルにする場合に使用する
title	文字列			
type	文字列			サポートされるタイプ RSS IMAGE TEXT HTML
url url-mode	文字列 文字列			RSS、IMAGE、または HTML タイプのペインの URL モード：mangle、no-mangle
text	文字列			TEXT タイプ ペインのテキスト
column	番号			

カスタマイゼーションの例

次の例は、次のカスタマイゼーション オプションを示しています。

- File アクセス アプリケーションのタブを非表示にする。
- Web Access アプリケーションのタイトルと順序を変更する。
- ホーム ページで 2 つのカラムを定義する。
- RSS ペインを追加する。
- 2 番目のペインの上部に 3 つのペイン（テキスト、イメージ、および html）を追加する。

```
<custom name="Default">
  <auth-page>

    <window>
          <title-text l10n="yes">title WebVPN Logon</title>
    </window>

    <title-panel>
         <mode>enable</mode>
         <text l10n="yes">XYZ WebVPN</text>
         <logo-url>http://www.xyz.com/images/XYZ.gif</logo-url>
    </title-panel>

    <copyright>
         <mode>enable</mode>
         <text l10n="yes">(c)Copyright, XYZ Inc., 2006</text>
    </copyright>

    <info-panel>
        <mode>enable</mode>
        <image-url>/+CSCOE+/custom/XYZ.jpg</image-url>
      <text l10n="yes">
            <![CDATA[
            <div>
            <b>Welcome to WebVPN !.</b>
            </div>
            ]]>
      </text>
    </info-panel>

    <logon-form>
      <form>
          <title-text l10n="yes">title WebVPN Logon</title>
          <message-text l10n="yes">message WebVPN Logon</title>
          <username-prompt-text l10n="yes">Username</username-prompt-text>
          <password-prompt-text l10n="yes">Password</password-prompt-text>
          <internal-password-prompt-text l10n="yes">Domain
password</internal-password-prompt-text>
          <group-prompt-text l10n="yes">Group</group-prompt-text>
          <submit-button-text l10n="yes">Logon</submit-button-text>
      </form>
    </logon-form>

    <logout-form>
      <form>
          <title-text l10n="yes">title WebVPN Logon</title>
          <message-text l10n="yes">message WebVPN Logon</title>
          <login-button-text l10n="yes">Login</login-button-text>
          <close-button-text l10n="yes">Logon</close-button-text>
      </form>
```

```
  </logout-form>

  <language-slector>
    <language>
        <code l10n="yes">code1</code>
        <text l10n="yes">text1</text>
    </language>
    <language>
        <code l10n="yes">code2</code>
        <text l10n="yes">text2</text>
    </language>
  </language-slector>

</auth-page>

<portal>

  <window>
        <title-text l10n="yes">title WebVPN Logon</title>
  </window>

  <title-panel>
       <mode>enable</mode>
       <text l10n="yes">XYZ WebVPN</text>
       <logo-url>http://www.xyz.com/logo.gif</logo-url>
  </title-panel>

  <navigation-panel>
       <mode>enable</mode>
  </navigation-panel>

  <application>
          <id>file-access</id>
          <mode>disable</mode>
  </application>
  <application>
          <id>web-access</id>
          <tab-title>XYZ Intranet</tab-title>
          <order>3001</order>
  </application>

 <column>
          <order>2</order>
          <width>40%</width>
<column>
 <column>
          <order>1</order>
          <width>60%</width>
<column>

<url-lists>
  <mode>no-group</mode>
</url-lists>

<pane>
 <id>rss_pane</id>
  <type>RSS</type>
 <url>rss.xyz.com?id=78</url>
</pane>

<pane>
  <id>text_pane</id>
  <type>TEXT</type>
 <url>rss.xyz.com?id=78</url>
```

```
    <column>1</column>
    <row>0</row>
    <text>Welcome to XYZ  WebVPN Service</text>
   </pane>

   <pane>
    <type>IMAGE</type>
   <url>http://www.xyz.com/logo.gif</url>
    <column>1</column>
    <row>2</row>
   </pane>

   <pane>
    <type>HTML</type>
   <title>XYZ news</title>
   <url>http://www.xyz.com/news.html</url>
    <column>1</column>
    <row>3</row>
   </pane>

   </portal>

</custom>
```

カスタマイゼーション テンプレートの使用

Template という名前のカスタマイゼーション テンプレートには、現在使用されているタグすべてと、その使用法を説明した対応するコメントが含まれています。export コマンドを使用し、次のようにしてセキュリティ アプライアンスからカスタマイゼーション テンプレートをダウンロードします。

```
hostname# export webvpn customization Template tftp://webserver/default.xml
```

Template ファイルは、変更または削除できません。この例のようにしてエクスポートする場合は、*default.xml* という新しい名前で保存します。このファイルで変更を行った後、そのファイルを使用して組織の必要を満たすカスタマイゼーション オブジェクトを作成し、*default.xml* または選択する別の名前のファイルとしてセキュリティ アプライアンスにインポートします。次に例を示します。

```
hostname# import webvpn customization General tftp://webserver/custom.xml
```

ここで *custom.xml* という名前の XML オブジェクトをインポートし、セキュリティ アプライアンス で *General* と命名します。

カスタマイゼーション テンプレート

Template という名前のカスタマイゼーション テンプレートを次に示します。

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--

Copyright (c) 2006,2007 by Cisco Systems, Inc.
All rights reserved.

Note: all white spaces in tag values are significant and preserved.


Tag: custom
Description: Root customization tag

Tag: custom/languages
Description: Contains list of languages, recognized by ASA
```

```
Value: string containing comma-separated language codes. Each language code is
       a set dash-separated alphanumeric characters, started with
       alpha-character (for example: en, en-us, irokese8-language-us)
Default value: en-us

Tag: custom/default-language
Description: Language code that is selected when the client and the server
             were not able to negotiate the language automatically.
             For example the set of languages configured in the browser
             is "en,ja", and the list of languages, specified by
             'custom/languages' tag is "cn,fr", the default-language will be
             used.
Value: string, containing one of the language coded, specified in
       'custom/languages' tag above.
Default value: en-us

*********************************************************

Tag: custom/auth-page
Description: Contains authentication page settings

*********************************************************
Tag: custom/auth-page/window
Description: Contains settings of the authentication page browser window

Tag: custom/auth-page/window/title-text
Description: The title of the browser window of the authentication page
Value: arbitrary string
Default value: Browser's default value

*********************************************************

Tag: custom/auth-page/title-panel
Description: Contains settings for the title panel

Tag: custom/auth-page/title-panel/mode
Description: The title panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/title-panel/text
Description: The title panel text.
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/title-panel/logo-url
Description: The URL of the logo image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/auth-page/title-panel/background-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #FFFFFF

Tag: custom/auth-page/title-panel/font-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/title-panel/font-weight
Description: The font weight
Value: CSS font size value, for example bold, bolder,lighter etc.
Default value: empty string
```

```
Tag: custom/auth-page/title-panel/font-size
Description: The font size
Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.
Default value: empty string

Tag: custom/auth-page/title-panel/gradient
Description: Specifies using the background color gradient
Value: yes|no
Default value:no

Tag: custom/auth-page/title-panel/style
Description: CSS style of the title panel
Value: CSS style string
Default value: empty string

*******************************************************

Tag: custom/auth-page/copyright-panel
Description: Contains the copyright panel settings

Tag: custom/auth-page/copyright-panel/mode
Description: The copyright panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/copyright-panel/text
Description: The copyright panel text
Value: arbitrary string
Default value: empty string

*******************************************************

Tag: custom/auth-page/info-panel
Description: Contains information panel settings

Tag: custom/auth-page/info-panel/mode
Description: The information panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/info-panel/image-position
Description: Position of the image, above or below the informational panel text
Values: above|below
Default value: above

Tag: custom/auth-page/info-panel/image-url
Description: URL of the information panel image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/auth-page/info-panel/text
Description: Text of the information panel
Text: arbitrary string
Default value: empty string

*******************************************************

Tag: custom/auth-page/logon-form
Description: Contains logon form settings

Tag: custom/auth-page/logon-form/title-text
Description: The logon form title text
Value: arbitrary string
```

```
Default value: "Logon"

Tag: custom/auth-page/logon-form/message-text
Description: The message inside of the logon form
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/logon-form/username-prompt-text
Description: The username prompt text
Value: arbitrary string
Default value: "Username"

Tag: custom/auth-page/logon-form/password-prompt-text
Description: The password prompt text
Value: arbitrary string
Default value: "Password"

Tag: custom/auth-page/logon-form/internal-password-prompt-text
Description: The internal password prompt text
Value: arbitrary string
Default value: "Internal Password"

Tag: custom/auth-page/logon-form/group-prompt-text
Description: The group selector prompt text
Value: arbitrary string
Default value: "Group"


Tag: custom/auth-page/logon-form/submit-button-text
Description: The submit button text
Value: arbitrary string
Default value: "Logon"

Tag: custom/auth-page/logon-form/internal-password-first
Description: Sets internal password first in the order
Value: yes|no
Default value: no


Tag: custom/auth-page/logon-form/title-font-color
Description: The font color of the logon form title
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/logon-form/title-background-color
Description: The background color of the logon form title
Value: HTML color format, for example #FFFFFF
Default value: #000000


Tag: custom/auth-page/logon-form/font-color
Description: The font color of the logon form
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/logon-form/background-color
Description: The background color of the logon form
Value: HTML color format, for example #FFFFFF
Default value: #000000


*******************************************************

Tag: custom/auth-page/logout-form
```

```
Description: Contains the logout form settings

Tag: custom/auth-page/logout-form/title-text
Description: The logout form title text
Value: arbitrary string
Default value: "Logout"

Tag: custom/auth-page/logout-form/message-text
Description: The logout form message text
Value: arbitrary string
Default value: Goodbye.
               For your own security, please:
               Clear the browser's cache
               Delete any downloaded files
               Close the browser's window

Tag: custom/auth-page/logout-form/login-button-text
Description: The text of the button sending the user to the logon page
Value: arbitrary string
Default value: "Logon"

*******************************************************

Tag: custom/auth-page/language-selector
Description: Contains the language selector settings

Tag: custom/auth-page/language-selector/mode
Description: The language selector mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/language-selector/title
Description: The language selector title
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/language-selector/language (multiple)
Description: Contains the language settings

Tag: custom/auth-page/language-selector/language/code
Description: The code of the language
Value (required): The language code string

Tag: custom/auth-page/language-selector/language/text
Description: The text of the language in the language selector drop-down box
Value (required): arbitrary string

*******************************************************

Tag: custom/portal
Description: Contains portal page settings

*******************************************************

Tag: custom/portal/window
Description: Contains the portal page browser window settings

Tag: custom/portal/window/title-text
Description: The title of the browser window of the portal page
Value: arbitrary string
Default value: Browser's default value

*******************************************************
```

```
Tag: custom/portal/title-panel
Description: Contains settings for the title panel

Tag: custom/portal/title-panel/mode
Description: The title panel mode
Value: enable|disable
Default value: disable

Tag: custom/portal/title-panel/text
Description: The title panel text.
Value: arbitrary string
Default value: empty string

Tag: custom/portal/title-panel/logo-url
Description: The URL of the logo image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/portal/title-panel/background-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #FFFFFF

Tag: custom/auth-pa/title-panel/font-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/portal/title-panel/font-weight
Description: The font weight
Value: CSS font size value, for example bold, bolder,lighter etc.
Default value: empty string

Tag: custom/portal/title-panel/font-size
Description: The font size
Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.
Default value: empty string

Tag: custom/portal/title-panel/gradient
Description: Specifies using the background color gradient
Value: yes|no
Default value:no

Tag: custom/portal/title-panel/style
Description: CSS style for title text
Value: CSS style string
Default value: empty string

*******************************************************

Tag: custom/portal/application (multiple)
Description: Contains the application setting

Tag: custom/portal/application/mode
Description: The application mode
Value: enable|disable
Default value: enable

Tag: custom/portal/application/id
Description: The application ID. Standard application ID's are: home, web-access,
file-access, app-access, network-access, help
Value: The application ID string
Default value: empty string
```

```
Tag: custom/portal/application/tab-title
Description: The application tab text in the navigation panel
Value: arbitrary string
Default value: empty string

Tag: custom/portal/application/order
Description: The order of the application's tab in the navigation panel. Applications with
lesser order go first.
Value: arbitrary number
Default value: 1000

Tag: custom/portal/application/url-list-title
Description: The title of the application's URL list pane (in group mode)
Value: arbitrary string
Default value: Tab tite value concatenated with "Bookmarks"

*******************************************************

Tag: custom/portal/navigation-panel
Description: Contains the navigation panel settings

Tag: custom/portal/navigation-panel/mode
Description: The navigation panel mode
Value: enable|disable
Default value: enable

*******************************************************

Tag: custom/portal/toolbar
Description: Contains the toolbar settings

Tag: custom/portal/toolbar/mode
Description: The toolbar mode
Value: enable|disable
Default value: enable

Tag: custom/portal/toolbar/prompt-box-title
Description: The universal prompt box title
Value: arbitrary string
Default value: "Address"

Tag: custom/portal/toolbar/browse-button-text
Description: The browse button text
Value: arbitrary string
Default value: "Browse"

Tag: custom/portal/toolbar/logout-prompt-text
Description: The logout prompt text
Value: arbitrary string
Default value: "Logout"

*******************************************************

Tag: custom/portal/column (multiple)
Description: Contains settings of the home page column(s)

Tag: custom/portal/column/order
Description: The order the column from left to right. Columns with lesser order values go
first
Value: arbitrary number
Default value: 0

Tag: custom/portal/column/width
Description: The home page column width
```

```
Value: percent
Default value: default value set by browser
Note: The actual width may be increased by browser to accommodate content


**********************************************************

Tag: custom/portal/url-lists
Description: Contains settings for URL lists on the home page

Tag: custom/portal/url-lists/mode
Description: Specifies how to display URL lists on the home page:
             group URL lists by application (group) or
             show individual URL lists (nogroup).
             URL lists fill out cells of the configured columns, which are not taken
             by custom panes.
             Use the attribute value "nodisplay" to not show URL lists on the home page.

Value: group|nogroup|nodisplay
Default value: group

**********************************************************

Tag: custom/portal/pane (multiple)
Description: Contains settings of the custom pane on the home page

Tag: custom/portal/pane/mode
Description: The mode of the pane
Value: enable|disable
Default value: disable

Tag: custom/portal/pane/title
Description: The title of the pane
Value: arbitrary string
Default value: empty string

Tag: custom/portal/pane/notitle
Description: Hides pane's title bar
Value: yes|no
Default value: no

Tag: custom/portal/pane/type
Description: The type of the pane. Supported types:
             TEXT - inline arbitrary text, may contain HTML tags;
             HTML - HTML content specified by URL shown in the individual iframe;
             IMAGE - image specified by URL
             RSS - RSS feed specified by URL
Value: TEXT|HTML|IMAGE|RSS
Default value: TEXT

Tag: custom/portal/pane/url
Description: The URL for panes with type  HTML,IMAGE or RSS
Value: URL string
Default value: empty string

Tag: custom/portal/pane/text
Description: The text value for panes with type TEXT
Value: arbitrary string
Default value:empty string

Tag: custom/portal/pane/column
Description: The column where the pane located.
Value: arbitrary number
Default value: 1
```

```
Tag: custom/portal/pane/row
Description: The row where the pane is located
Value: arbitrary number
Default value: 1

Tag: custom/portal/pane/height
Description: The height of the pane
Value: number of pixels
Default value: default value set by browser


*******************************************************

Tag: custom/portal/browse-network-title
Description: The title of the browse network link
Value: arbitrary string
Default value: Browse Entire Network


Tag: custom/portal/access-network-title
Description: The title of the link to start a network access session
Value: arbitrary string
Default value: Start AnyConnect

-->
- <custom>
- <localization>
<languages>en,ja,zh,ru,ua</languages>
<default-language>en</default-language>
</localization>
- <auth-page>
- <window>
- <title-text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</title-text>
</window>
- <language-selector>
<mode>disable</mode>
<title l10n="yes">Language:</title>
- <language>
<code>en</code>
<text>English</text>
</language>
- <language>
<code>zh</code>
<text>?? (Chinese)</text>
</language>
- <language>
<code>ja</code>
<text>?? (Japanese)</text>
</language>
- <language>
<code>ru</code>
<text>??????? (Russian)</text>
</language>
- <language>
<code>ua</code>
<text>?????????? (Ukrainian)</text>
</language>
</language-selector>
- <logon-form>
```

```
- <title-text l10n="yes">
- <![CDATA[
Login
]]>
</title-text>
- <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
- <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
- <message-text l10n="yes">
- <![CDATA[
Please enter your username and password.
]]>
</message-text>
- <username-prompt-text l10n="yes">
- <![CDATA[
USERNAME:
]]>
</username-prompt-text>
- <password-prompt-text l10n="yes">
- <![CDATA[
PASSWORD:
]]>
</password-prompt-text>
<internal-password-prompt-text l10n="yes" />
<internal-password-first>no</internal-password-first>
- <group-prompt-text l10n="yes">
- <![CDATA[
GROUP:
]]>
</group-prompt-text>
- <submit-button-text l10n="yes">
- <![CDATA[
Login
]]>
</submit-button-text>
- <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
- <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
</logon-form>
- <logout-form>
- <title-text l10n="yes">
- <![CDATA[
Logout
]]>
</title-text>
- <message-text l10n="yes">
- <![CDATA[
Goodbye.
```

```
]]>
</message-text>
</logout-form>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
- <font-size>
- <![CDATA[
larger
]]>
</font-size>
- <font-color>
- <![CDATA[
#800000
]]>
</font-color>
- <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
- <info-panel>
<mode>disable</mode>
<image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
<image-position>above</image-position>
<text l10n="yes" />
</info-panel>
- <copyright-panel>
<mode>disable</mode>
<text l10n="yes" />
</copyright-panel>
</auth-page>
- <portal>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
- <font-size>
- <![CDATA[
larger
```

```
]]>
</font-size>
- <font-color>
- <![CDATA[
#800000
]]>
</font-color>
- <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
<access-network-title l10n="yes">Start AnyConnect</access-network-title>
- <application>
<mode>enable</mode>
<id>home</id>
<tab-title l10n="yes">Home</tab-title>
<order>1</order>
</application>
- <application>
<mode>enable</mode>
<id>web-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Web Applications
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
Web Bookmarks
]]>
</url-list-title>
<order>2</order>
</application>
- <application>
<mode>enable</mode>
<id>file-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Browse Networks
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
File Folder Bookmarks
]]>
</url-list-title>
<order>3</order>
</application>
- <application>
<mode>enable</mode>
<id>app-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Application Access
]]>
</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>net-access</id>
```

```
<tab-title l10n="yes">AnyConnect</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>help</id>
<tab-title l10n="yes">Help</tab-title>
<order>1000000</order>
</application>
- <toolbar>
<mode>enable</mode>
<logout-prompt-text l10n="yes">Logout</logout-prompt-text>
<prompt-box-title l10n="yes">Address</prompt-box-title>
<browse-button-text l10n="yes">Browse</browse-button-text>
</toolbar>
- <column>
<width>100%</width>
<order>1</order>
</column>
- <pane>
<type>TEXT</type>
<mode>disable</mode>
<title />
<text />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>IMAGE</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>HTML</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>RSS</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <url-lists>
<mode>group</mode>
</url-lists>
</portal>
</custom>
```

ヘルプのカスタマイゼーション

セキュリティ アプライアンスは、クライアントレス セッションの間、アプリケーション パネルにヘルプ コンテンツを表示します。各クライアントレス アプリケーションのパネルには、事前に設定されたファイル名を使用して独自のヘルプ ファイル コンテンツが表示されます。たとえば、[Application Access] パネルに表示されるヘルプ コンテンツは、app-access-hlp.inc というファイルの内容です。表 34-4 に、クライアントレス アプリケーション パネルと、ヘルプのコンテンツの事前設定されたファイル名を示します。

表 34-4　　クライアントレス アプリケーション

アプリケーション タイプ	パネル	ファイル名
標準	Application Access	app-access-hlp.inc
標準	Browse Networks	file-access-hlp.inc
標準	AnyConnect Client	net-access-hlp.inc
標準	Web Access	web-access-hlp.inc
プラグイン	MetaFrame Access	ica-hlp.inc
プラグイン	Terminal Servers	rdp-hlp.inc
プラグイン	Telnet/SSH Servers	ssh,telnet-hlp.inc
プラグイン	VNC Connections	vnc-hlp.inc

シスコが提供するヘルプ ファイルをカスタマイズするか、または別の言語でヘルプ ファイルを作成できます。次に [Import] ボタンを使用して、セキュリティ アプライアンスのフラッシュ メモリにそれらのファイルをコピーし、その後のクライアントレス セッション中に表示します。また、以前にインポートしたヘルプ コンテンツ ファイルをエクスポートし、カスタマイズして、フラッシュ メモリに再インポートすることもできます。

次の各項では、クライアントレス セッションに表示されるヘルプ コンテンツのカスタマイズ方法または作成方法を説明します。

- シスコが提供するヘルプ ファイルのカスタマイズ
- シスコが提供していない言語用のヘルプ ファイルの作成

フィールド

[Import]：[Import Application Help Content] ダイアログを起動します。このダイアログでは、クライアントレス セッション中に表示する新しいヘルプ コンテンツをフラッシュ メモリにインポートできます。

[Export]：テーブルから選択し、以前にインポートしたヘルプ コンテンツを取得します。

[Delete]：テーブルから選択し、以前にインポートしたヘルプ コンテンツを削除します。

[Language]：ブラウザで表示される言語の略語を表示します。このフィールドは、ファイル変換には*使用されません*。ファイル内で使用される言語を示します。テーブル内の略語に関連付ける言語名を特定するには、ブラウザで表示される言語のリストを表示します。たとえば、次の手順のいずれかを使用すると、ダイアログ ウィンドウに言語と関連の言語コードが表示されます。

- Internet Explorer を起動して、[Tools] > [Internet Options] > [Languages] > [Add] を選択します。

- Mozilla Firefox を起動して、[Tools] > [Options] > [Advanced] > [General] を選択し、[Languages] の隣にある [Choose] をクリックして、[Select a language to add] をクリックします。

[Filename]：ヘルプ コンテンツ ファイルがインポートされたときのファイル名を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

シスコが提供するヘルプ ファイルのカスタマイズ

シスコが提供するヘルプ ファイルをカスタマイズするには、まずフラッシュ メモリ カードからファイルのコピーを取得する必要があります。次の手順で、コピーを取得してカスタマイズします。

ステップ 1　ブラウザを使用して、セキュリティ アプライアンスとのクライアントレス セッションを確立します。

ステップ 2　表 34-5 の「セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL」欄にある文字列をセキュリティ アプライアンスのアドレスに追加し、次の説明に従って *language* の部分を置き換え、次に Enter を押します。

表 34-5　クライアントレス アプリケーション用にシスコが提供するヘルプ ファイル

アプリケーション タイプ	パネル	セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL
標準	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc
標準	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc
標準	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc
標準	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc
プラグイン	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc
プラグイン	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc
プラグイン	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc

language は、ブラウザで表示される言語の略語です。略語はファイル変換では*使用されません*。これは、ファイルで使用される言語を示します。シスコが提供する英語版のヘルプ ファイルを表示する場合は、略語として **en** と入力します。

次のアドレス例は、Terminal Servers のヘルプの英語版を表示します。

https://*address_of_security_appliance*/+CSCOE+/help/en/rdp-hlp.inc**

ステップ 3　[File] > [Save (Page) As] を選択します。

注意　[File name] ボックスの内容は変更しないでください。

ステップ 4　[Save as type] オプションを [Web Page, HTML only] に変更して、[Save] をクリックします。

ステップ 5　任意の HTML エディタを使用してファイルをカスタマイズします。

（注）　ほとんどの HTML タグを使用できますが、ドキュメントとその構造を定義するタグは*使用しないでください*（たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください）。<b> タグなどの文字タグ、およびコンテンツを構築するための <p>、<ol>、<ul>、および <li> などのタグは使用できます。

ステップ 6　オリジナルのファイル名と拡張子を指定して、HTML only としてファイルを保存します。

ステップ 7　ファイル名が表 34-5 にあるファイル名のいずれかと一致すること、および余分なファイル拡張子がないことを確認します。

ASDM に戻り、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Help Customization] > [Import] を選択して、修正されたヘルプ ファイルをフラッシュ メモリにインポートします。

シスコが提供していない言語用のヘルプ ファイルの作成

標準 HTML を使用して他の言語のヘルプ ファイルを作成します。サポートするそれぞれの言語に別のフォルダを作成することをお勧めします。

（注）　ほとんどの HTML タグを使用できますが、ドキュメントとその構造を定義するタグは*使用しないでください*（たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください）。<b> タグなどの文字タグ、およびコンテンツを構築するための <p>、<ol>、<ul>、および <li> などのタグは使用できます。

HTML only としてファイルを保存します。表 34-4 のファイル名列にあるファイル名を使用してください。

ASDM に戻り、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Help Customization] > [Import] を選択して、新しいヘルプ ファイルをフラッシュ メモリにインポートします。

アプリケーションのヘルプ コンテンツのインポートおよびエクスポート

[Import Application Help Content] ダイアログボックスを使用して、クライアントレス セッション中にポータル ページに表示するために、ヘルプ ファイルをフラッシュ メモリにインポートします。[Export Application Help Content] ダイアログボックスを使用して、以前にインポートしたヘルプ ファイルをその後の編集のために取得します。

フィールド

[Language]：[Import Application Help Content] ダイアログボックス向けにのみ、このフィールドでブラウザに表示される言語を指定します（この [Language] フィールドは、[Export Application Help Content] ダイアログボックスでは非アクティブになっています）。このフィールドはファイル変換には使用されません。ファイルで使用される言語を示すだけです。[Language] フィールドの横にあるドット（複数）をクリックし、[Browse Language Code] ダイアログボックスで、ヘルプ ファイルで使用される言語を含む行をダブルクリックし、[Language Code] フィールドの略語がその行の略語と一致することを確認して、[OK] をクリックします。ヘルプ コンテンツを表示するための言語が [Browse Language Code] ダイアログボックスに表示されない場合は、[Language Code] フィールドに必要な言

語の略語を入力して [OK] をクリックするか、ドットの左側にある [Language] テキストボックスに言語を入力します。[Browse Language Code] ダイアログボックスに表示されない場合に、インポートするヘルプ ファイルの言語の略語を指定するには、ブラウザによって表示される言語と略号の一覧を表示します。たとえば、次の手順のいずれかを使用すると、ダイアログ ウィンドウに言語と関連の言語コードが表示されます。

- Internet Explorer を起動して、[Tools] > [Internet Options] > [Languages] > [Add] を選択します。
- Mozilla Firefox を起動して、[Tools] > [Options] > [Advanced] > [General] を選択し、[Languages] の隣にある [Choose] をクリックして、[Select a language to add] をクリックします。

[File Name] : インポートする場合は、ドロップダウン リストから新しいヘルプ コンテンツ ファイルのファイル名を指定します。エクスポートする場合は、このフィールドは使用できません。

[Select a File] : ソース ファイル（インポートの場合）または転送先ファイル（エクスポートの場合）のパラメータを設定します。

[Local computer] : ソースまたは転送先ファイルがローカル コンピュータにある場合に選択します。

- [Path] : ソースまたは転送先ファイルのパスを指定します。
- [Browse Local Files] : ソースまたは転送先ファイルのローカル コンピュータを参照します。

[Flash file system] : ソースまたは転送先ファイルがセキュリティ アプライアンスのフラッシュ メモリにある場合に選択します。

- [Path] : フラッシュ メモリ内のソースまたは転送先ファイルのパスを指定します。
- [Browse Flash] : ソースまたは転送先ファイルのあるフラッシュ メモリを参照します。

[Remote server] : ソースまたは転送先ファイルがリモート サーバにある場合に選択します。

- [Path] : ftp、tftp、または http（インポートの場合のみ）の中からファイル転送（コピー）方式を選択し、パスを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

クライアント/サーバ プラグインへのブラウザ アクセスの設定

[Client-Server Plug-in] テーブルには、セキュリティ アプライアンス によってクライアントレス SSL VPN セッションのブラウザで使用できるようになるプラグインが表示されます。

プラグインを追加、変更、または削除するには、次のいずれかを実行します。

- プラグインを追加するには、[Import] をクリックします。[Import Plug-ins] ダイアログボックスが開きます。
- プラグインを削除するには、そのプラグインを選択して [Delete] をクリックします。

ブラウザ プラグインのインストールについて

ブラウザ プラグインは、Web ブラウザによって呼び出される独立したプログラムで、ブラウザ ウィンドウ内でクライアントをサーバに接続するなどの専用の機能を実行します。セキュリティ アプライアンスを使用すると、クライアントレス SSL VPN セッション中に、リモート ブラウザにダウンロードするプラグインをインポートできます。通常、シスコでは再配布するプラグインのテストを行っており、再配布できないプラグインの接続性をテストする場合もあります。ただし、現時点では、ストリーミング メディアをサポートするプラグインのインポートは推奨しません。

（注）　シスコでは、GNU General Public License（GPL; 一般公的使用許諾）に従い、変更を加えることなくプラグインを再配布しています。GPL により、これらのプラグインを直接改良できません。

プラグインをフラッシュ デバイスにインストールすると、セキュリティ アプライアンスは次の処理を実行します。

- （シスコが配布したプラグインのみ）*URL* で指定した jar ファイルを解凍する。
- セキュリティ アプライアンス ファイル システムの csco-config/97/plugin ディレクトリにファイルを書き込む。
- ASDM の URL 属性の横にあるドロップダウン メニューに情報を入力します。
- 将来のすべてのクライアントレス SSL VPN セッションに対するプラグインのイネーブル化、およびメイン メニュー オプションの追加とポータル ページの [Address] フィールドの隣にあるドロップダウン メニューへのオプションの追加

  表 34-6 に、次の項で説明するプラグインを追加したときの、ポータル ページのメイン メニューと [Address] フィールドの変更点を示します。

表 34-6　クライアントレス SSL VPN ポータル ページへのプラグインの影響

プラグイン	ポータル ページに追加されるメイン メニュー オプション	ポータル ページに追加される [Address] フィールド オプション
ica	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
rdp2	Terminal Servers Vista	rdp2://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

（注）　セカンダリ セキュリティ アプライアンスは、プライマリ セキュリティ アプライアンスからプラグインを取得します。

クライアントレス SSL VPN セッションのユーザがポータル ページで関連するメニュー オプションをクリックすると、ポータル ページにインターフェイスへのウィンドウが開き、ヘルプ ペインが表示されます。ドロップダウン メニューに表示されたプロトコルをユーザが選択して [Address] フィールドに URL を入力すると、接続を確立できます。

（注）　Java プラグインによっては、宛先サービスへのセッションが設定されていない場合でも、接続済みまたはオンラインというステータスがレポートされることがあります。open-source プラグインは、セキュリティ アプライアンスではなくステータスをレポートします。

1 つ目のプラグインをインストールする前に、次の項の指示に従う必要があります。

プラグインの要件および制限事項

プラグインへのリモートアクセスを提供するには、セキュリティ アプライアンスでクライアントレス SSL VPN をイネーブルにする必要があります。

リモートで使用するために必要な最低限のアクセス権は、ゲスト特権モードに属しています。

ステートフル フェールオーバーが発生すると、プラグインを使用して確立されたセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。

プラグインのためのセキュリティ アプライアンスの準備

プラグインをインストールする前に、次の手順を実行してセキュリティ アプライアンスを準備します。

ステップ 1　セキュリティ アプライアンス インターフェイスでクライアントレス SSL VPN（「webvpn」）がイネーブルになっていることを確認します。

ステップ 2　リモート ユーザが Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用して接続するセキュリティ アプライアンス インターフェイスに SSL 証明書をインストールします。

（注）　SSL 証明書の 一般名（CN）として IP アドレスを指定しないでください。リモート ユーザは、セキュリティ アプライアンスと通信するために FQDN の使用を試行します。リモート PC は、DNS または System32\drivers\etc\hosts ファイル内のエントリを使用して、FQDN を解決できる必要があります。

クライアントレス SSL VPN アクセスで使用可能にするプラグインのタイプに該当する項を参照してください。

- シスコによって再配布されたプラグインのインストール
- サードパーティ プラグインのアセンブリとインストール : Citrix Java Presentation Server Client の場合

シスコによって再配布されたプラグインのインストール

シスコでは、クライアントレス SSL VPN セッションで Web ブラウザのプラグインとしてアクセスされる、次のオープンソースの Java ベースのコンポーネントを再配布しています。

表 34-7　シスコが再配布しているプラグイン

シスコのダウンロード リンク	プロトコル	説明	再配布しているプラグインのソース
rdp2-plugin.090211.jar	RDP2	Windows Vista および Windows 2003 R2 でホストされる Microsoft Terminal Services にアクセスします。 リモート デスクトップ ActiveX コントロールをサポートします。 （注）RDP プラグインと RDP2 プラグインをインポートして、クライアントレス ユーザが両方を利用できるようにできます。	シスコでは、GNU 一般公的使用許諾に従って、変更を加えることなくこのプラグインを再配布します。再配布プラグインの元のソースは、http://properjavardp.sourceforge.net/ です。
rdp-plugin.080506.jar	RDP	Windows 2003 R1 でホストされる Microsoft Terminal Services にアクセスします。 リモート デスクトップ ActiveX コントロールをサポートします。	シスコでは、GNU 一般公的使用許諾に従って、変更を加えることなくこのプラグインを再配布します。再配布プラグインのソースは、http://properjavardp.sourceforge.net/ です。
ssh-plugin.080430.jar	SSH	Secure Shell-Telnet プラグインにより、リモート ユーザはリモート コンピュータへの Secure Shell または Telnet 接続を確立できます。	シスコでは、GNU 一般公的使用許諾に従って、変更を加えることなくこのプラグインを再配布します。この再配布プラグインのソースがある Web サイトは、http://javassh.org/ です。
vnc-plugin.080130.jar	VNC	Virtual Network Computing プラグインを使用すると、リモート ユーザはリモート デスクトップ共有をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。このバージョンでは、テキストのデフォルトの色が変更されています。また、フランス語と日本語のヘルプ ファイルもアップデートされています。	シスコでは、GNU 一般公的使用許諾に従って、変更を加えることなくこのプラグインを再配布します。この再配布プラグインのソースがある Web サイトは、http://www.tightvnc.com/ です。

シスコによって再配布されるプラグインを取得し、それをセキュリティ アプライアンスにインポートするには、次の手順を実行します。

ステップ 1　セキュリティ アプライアンスとの ASDM セッションを確立するために使用するコンピュータに、[plugins] という名前の一時ディレクトリを作成します。

ステップ 2　次に、シスコの Web サイトから、必要なプラグインを [plugins] ディレクトリにダウンロードします。

ステップ 3　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Client-Server Plug-ins] を選択します。

このペインには、クライアントレス SSL セッションで使用可能なプラグインが表示されます。

ステップ 4　[Import] をクリックします。

[Import Client-Server Plug-in] ダイアログボックスが開きます。

ステップ 5　フィールドに値を入力するには、次の説明を参考にしてください。

フィールド

[Import Client-Server Plug-in] ダイアログボックスには、次のフィールドがあります。

- [Plug-in Name]：次のいずれかの値を入力します。
  - Citrix MetaFrame サービスへのプラグイン アクセスを提供する場合は **ica**。その後、次の説明に従って [Remote Server] フィールドに ica-plugin.jar ファイルへのパスを指定します。
  - Remote Desktop Protocol サービスへのプラグイン アクセスを提供するには、**rdp** を入力します。次に、[Remote Server] フィールドで rdp-plugin.jar ファイルへのパスを指定します。
  - セキュア シェル サービスと Telnet サービスの*両方*にプラグイン アクセスを提供するには、**ssh,telnet** を入力します。次に、[Remote Server] フィールドで ssh-plugin.jar ファイルへのパスを指定します。
  - Virtual Network Computing サービスにプラグイン アクセスを提供するには、**vnc** を入力します。次に、[Remote Server] フィールドで vnc-plugin.jar ファイルへのパスを指定します。

（注） このメニューの、記載のないオプションは実験的なものであるため、サポートされていません。

- [Select a file]：次のいずれかのオプションをクリックし、テキスト フィールドにパスを挿入します。
  - [Local computer]：ASDM セッションを確立した相手のコンピュータからプラグインを取得します。関連する [Path] フィールドにプラグインの場所と名前を入力するか、[Browse Local Files] をクリックしてプラグインにナビゲートし、プラグインを選択して [Select] をクリックします。
  - [Flash file system]：セキュリティ アプライアンスのファイル システムにプラグインが存在する場合にクリックします。関連する [Path] フィールドにプラグインの場所と名前を入力するか、[Browse Flash] をクリックしてプラグインにナビゲートし、プラグインを選択して [OK] をクリックします。
  - [Remote Server]：FTP または TFTP サーバを実行しているホストからプラグインを取得します。リモート サーバで実行されているサービスに応じて、関連付けられた [Path] 属性の横にあるドロップダウン メニューで [ftp]、[tftp]、または [HTTP] を選択します。隣にあるテキスト フィールドに、サーバのホスト名またはアドレスおよびプラグインへのパスを入力します。

ステップ 6　[Import Now] をクリックします。

[Apply] をクリックします。

これで、以降のクライアントレス SSL VPN セッションでプラグインが使用できるようになりました。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

サードパーティ プラグインのアセンブリとインストール：Citrix Java Presentation Server Client の場合

セキュリティ アプライアンスのオープン フレームワークにより、サードパーティの Java クライアント/サーバ アプリケーションをサポートするためにプラグインを追加することができます。サードパーティのプラグインに、クライアントレス SSL VPN ブラウザ アクセスを提供する方法の例として、この項では、Citrix Presentation Server Client にクライアントレス SSL VPN のサポートを追加する方法について説明します。

注意　シスコでは、シスコが再配布していない特定のプラグインに対して、直接的なサポートや推奨はしていません。クライアントレス SSL VPN サービスの提供者として、ユーザはプラグインの使用に際して必要となるライセンス契約を確認および遵守する責任があります。

セキュリティ アプライアンスに Citrix プラグインがインストールされている場合、クライアントレス SSL VPN ユーザは、セキュリティ アプライアンスへの接続を使用して、Citrix MetaFrame サービスにアクセスできます。

ステートフル フェールオーバーでは、Citrix プラグインを使用して確立したセッションは保持されません。Citrix のユーザは、フェールオーバー後に再認証を行う必要があります。

Citrix プラグインへのアクセスを提供するには、次の項で説明する手順に従ってください。

クライアントレス SSL VPN アクセスのための Citrix MetaFrame Server の準備

Citrix クライアントが Citrix MetaFrame Server に接続するときに、セキュリティ アプライアンスは Citrix セキュア ゲートウェイの接続機能を実行します。（Citrix）「セキュア ゲートウェイ」を使用しないモードで動作するように、Citrix Web Interface ソフトウェアを設定する必要があります。この設定をしないと、Citrix クライアントは Citrix MetaFrame Server に接続できません。

まだプラグインのサポートを提供していない場合は、次の項に進む前に、「プラグインのためのセキュリティ アプライアンスの準備」（P.34-75）の指示に従う必要があります。

Citrix プラグインの作成、インストール、およびテスト

Citrix プラグインを作成およびインストールするには、次の手順に従います。

ステップ 1　Cisco Software Download Web サイトから ica-plugin.zip ファイルをダウンロードします。

このファイルには、Citrix プラグインを使用するためにシスコがカスタマイズしたファイルが含まれています。

ステップ 2　Citrix のサイトから Citrix Java クライアントをダウンロードします。

ステップ 3　Citrix Java クライアントから次のファイルを抽出します。

- JICA-configN.jar
- JICAEngN.jar

この手順と次の手順は、WinZip を使用して行えます。

ステップ 4　抽出したファイルを ica-plugin.zip ファイルに追加します。

ステップ 5　Citrix Java に含まれている EULA によって、Web サーバ上にクライアントを配置するための権限が与えられていることを確認します。

ステップ 6　セキュリティ アプライアンスとの ASDM セッションを確立します。[Config] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Client-Server Plug-ins] > [Import] を選択し、ica-plugin.zip ファイルをインポートします。

（注）　クライアントレス SSL VPN セッションのユーザは、[Address] ボックスに URL を入力して Citrix セッションでの SSO サポートを得ることはできません。Citrix プラグインに SSO サポートを提供するには、次の手順のとおりにブックマークを挿入する必要があります。

ステップ 7　ユーザが接続しやすいよう、適切なブックマーク リストにブックマークを追加します。[ica] を選択し、[Address] フィールドに次の情報を入力します。

citrix-server/**?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

ステップ 8　プラグインをテストするには、セキュリティ アプライアンスとのクライアントレス セッションを確立し、ブックマークをクリックします。

必要に応じて、『Client for Java Administrator's Guide』を参照してください。

ブックマークの設定

[Bookmarks] パネルでは、ブックマーク リストを追加、編集、削除、インポート、およびエクスポートできます。

[Bookmarks] パネルを使用して、クライアントレス SSL VPN でアクセスするための、サーバおよび URL のリストを設定します。ブックマーク リストのコンフィギュレーションに続いて、そのリストを 1 つ以上のポリシー（グループ ポリシー、ダイナミック アクセス ポリシー、またはその両方）に割り当てることができます。各ポリシーのブックマーク リストは 1 つのみです。リスト名は、各 DAP の [URL Lists] タブのドロップダウン リストに表示されます。

注意　ブックマークを設定することでは、ユーザが不正なサイトや会社のアクセプタブル ユース ポリシーに違反するサイトにアクセスすることを防ぐことはできません。ブックマーク リストをグループ ポリシー、ダイナミック アクセス ポリシー、またはその両方に割り当てる以外に、Web ACL をこれらのポリシーに割り当てて、トラフィック フローへのアクセスを制御します。これらのポリシー上の URL エントリをディセーブルにして、ユーザがアクセスできるページについて混乱しないようにします。手順については、「セキュリティ対策」（P.34-1）を参照してください。

バージョン 8.0 ソフトウェアでは、ブックマーク リストを設定するための機能が拡張されており、新しいプロセスは以前のバージョンと互換性がありません。8.0 ソフトウェアへのアップグレード中に、セキュリティ アプライアンスは、古い設定を使用して新しいリストを作成することによって現在のコンフィギュレーションを維持します。このプロセスは 1 回のみ実行されます。また、古い値は新しい値の一部を構成するサブセットに過ぎないため、このプロセスは古い形式から新しい形式への単なる変換ではありません。

（注）　バージョン 7.2 ポータルのカスタマイズと URL リストは、バージョン 8.0 にアップグレードする*前*にバージョン 7.2（x）のコンフィギュレーション ファイルの適切なインターフェイスでクライアントレス SSL VPN（WebVPN）がイネーブルになっていた場合にだけ、Beta 8.0 コンフィギュレーションで使用できます。

フィールド

- [Bookmarks List]：既存のブックマーク リストを表示します。
- [Add]：新しいブックマーク リストを追加します。

- [Edit]：選択したブックマーク リストを編集します。
- [Delete]：選択したブックマーク リストを削除します。
- [Import]：ブックマーク リストをインポートします。
- [Export]：ブックマーク リストをエクスポートします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Add/Edit Bookmark List

[Add/Edit Bookmark List] ダイアログボックスでは、URL リストを追加、編集、または削除でき、指定された URL リストの項目を並べ替えることもできます。

フィールド

- [Bookmark List Name]：追加するリストの名前を指定するか、修正または削除するリストの名前を選択します。
- [Name]：ユーザに表示する URL 名を指定します。
- [URL]：表示名に関連付けられている URL を指定します。
- [Add]：[Add Bookmark Entry] ダイアログボックスを開きます。このダイアログボックスでは、新しいサーバまたは URL と表示名を設定できます。
- [Edit]：[Edit Bookmark Entry] ダイアログボックスを開きます。このダイアログボックスでは、新しいサーバまたは URL と表示名を設定できます。
- [Delete]：選択した項目を URL リストから削除します。確認されず、やり直しもできません。
- [Move Up/Move Down]：URL リストでの選択した項目の位置を変更します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Add Bookmark Entry

[Add Bookmark Entry] ダイアログボックスでは、URL リストのリンクまたはブックマークを作成できます。

フィールド

- [Bookmark Title]：ブックマークの名前を指定します。
- [URL Value]：プルダウン メニューを使用して、URL タイプ（http、https、cifs、または ftp）を選択します。
- [URL]（テキスト ボックス）：ブックマークの DNS 名または IP アドレスを入力します。プラグインの場合は、サーバの名前を入力します。サーバ名の後にスラッシュと疑問符（/?）を入力すると、オプションのパラメータを指定できます。それに続いてアンパサンドを使用すると、次の構文に示すように、パラメータ/値ペアを分けられます。

  server/**?***Parameter*=*Value*&*Parameter*=*Value*

  次に例を示します。

  host/**?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

  プラグインによって、入力できるオプションのパラメータ/値ペアが決まります。

  プラグインに対して、シングル サインオン サポートを提供するには、パラメータ/値ペア **csco_sso=1** を使用します。次に例を示します。

  host/**?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

  （注）　`\\server\share\subfolder\personal` *フォルダ*にアクセスするには、`personal` *フォルダ*上のすべてのポイントに対するリスト権限がユーザに必要です。

- [Advanced Options]：（任意）ブックマークの特徴の詳細を設定します。
  - [Subtitle]：ユーザに表示するブックマーク エントリについての説明テキストを入力します。
  - [Thumbnail]：プルダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。
  - [Manage]：サムネールとして使用するイメージをインポートまたはエクスポートします。
  - [URL Method]：単純なデータ取得の場合には [Get] を選択します。データの保存または更新、製品の注文、電子メールの送信など、データを処理することによってデータに変更が加えられる可能性がある場合には、[Post] を選択します。
  - [Enable Favorite Option]：ポータル ホームページ上にブックマーク エントリを表示する場合は [Yes] を選択します。アプリケーション ページのみに表示する場合は [No] を選択します。
  - [Enable Smart-Tunnel Option]：セキュリティ アプライアンスとの間でデータを受け渡すスマート トンネル機能を使用する新しいウィンドウでブックマークを開く場合に選択します。
  - [Post Parameters]：Post URL 方式の詳細を設定します。
  - [Add]：post パラメータを追加します。
  - [Edit]：選択した post パラメータを編集します。
  - [Delete]：選択した post パラメータを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

ブックマーク リストのインポートおよびエクスポート

すでに設定済みのブックマーク リストは、インポートまたはエクスポートできます。使用準備ができているリストをインポートします。リストをエクスポートして修正または編集してから、再インポートすることもできます。

フィールド

- [Bookmark List Name]：名前によってリストを特定します。最大 64 文字で、スペースは使用できません。
- [Select a file]：リスト ファイルをインポートまたはエクスポートするときに使用する方法を選択します。
  - [Local computer]：ローカル PC に常駐するファイルをインポートする場合に選択します。
  - [Flash file system]：セキュリティ アプライアンスに常駐するファイルをエクスポートする場合に選択します。
  - [Remote server]：セキュリティ アプライアンスからアクセス可能なリモート サーバに常駐する URL リスト ファイルをインポートする場合に選択します。
  - [Path]：ファイルにアクセスする方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
  - [Browse Local Files/Browse Flash]：ファイルのパスを参照します。
- [Import/Export Now]：リスト ファイルをインポートまたはエクスポートします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Configure Web Contents

このダイアログボックスでは、Web コンテンツ オブジェクトをインポートおよびエクスポートできます。

フィールド

- [File Name]：Web コンテンツ オブジェクトの名前を表示します。

- [File Type]：ファイル タイプを特定します。
- [Import/Export]：Web コンテンツ オブジェクトをインポートまたはエクスポートします。
- [Delete]：オブジェクトを削除します。

Web コンテンツのインポートおよびエクスポート

Web コンテンツには、全体的に設定されたホーム ページから、エンド ユーザ ポータルをカスタマイズするときに使用するアイコンやイメージまで、さまざまな種類があります。設定済みの Web コンテンツは、インポートまたはエクスポートできます。使用準備ができている Web コンテンツをインポートします。Web コンテンツをエクスポートして修正または編集してから、再インポートすることもできます。

フィールド

- [Source]：ファイルのインポートまたはエクスポート元の場所を選択します。
  - [Local computer]：ローカル PC に常駐するファイルをインポートまたはエクスポートする場合に選択します。
  - [Flash file system]：セキュリティ アプライアンスに常駐するファイルをインポートまたはエクスポートする場合に選択します。
  - [Remote server]：セキュリティ アプライアンスからアクセス可能なリモート サーバに常駐するファイルをインポートする場合に選択します。
  - [Path]：ファイルにアクセスする方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
  - [Browse Local Files.../Browse Flash...]：ファイルのパスを参照します。
- Destination
  - [Require authentication to access its content?]：[Yes] または [No] をクリックします。
  - [WebContent Path]：パスのプレフィックスは、認証を要求するかどうかに応じて異なります。セキュリティ アプライアンスは、認証が必要なオブジェクトの場合には /+CSCOE+/ を使用し、認証が不要なオブジェクトの場合には /+CSCOU+/ を使用します。セキュリティ アプライアンスはポータル ページにだけ /+CSCOE+/ オブジェクトを表示するのに対し、/+CSCOU+/ オブジェクトは、ログイン ページまたはポータル ページのどちらかで表示または使用可能です。
- [Import Now]/[Export Now]：クリックすると、ファイルをインポートまたはエクスポートします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Add/Edit Post Parameter

このペインでは、ブックマーク エントリと URL リストのポスト パラメータを設定します。

これらは、ユーザ ID とパスワード、または他の入力パラメータを含む個人別のリソースであることが多く、クライアントレス SSL VPN マクロ置換を定義する必要がある場合があります。詳細な手順については、リンクをクリックしてください。

フィールド

- [Name, Value]：パラメータの名前と値を、対応する HTML フォームのとおりに指定します。たとえば、<input name="*param_name*" value="*param_value*"> です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

クライアントレス SSL VPN マクロ置換

クライアントレス SSL VPN マクロ置換を使用すると、ユーザ ID とパスワード、または他の入力パラメータを含む個人別のリソースにユーザがアクセスできるように設定できます。このようなリソースの例には、ブックマーク エントリ、URL リスト、およびファイル共有などがあります。

（注） セキュリティ上の理由から、パスワード置換はファイル アクセス URL（cifs://）に対してはディセーブルにされています。

同様に、セキュリティ上の理由から、Web リンク（特に非 SSL インスタンス）にパスワード置換を導入する場合は注意が必要です。

次のマクロ置換がサポートされています。

番号	マクロ置換	定義
1	CSCO_WEBVPN_USERNAME	SSL VPN ユーザ ログイン ID
2	CSCO_WEBVPN_PASSWORD	SSL VPN ユーザ ログイン パスワード
3	CSCO_WEBVPN_INTERNAL_PASSWORD	SSL VPN ユーザ内部リソース パスワード
4	CSCO_WEBVPN_CONNECTION_PROFILE	SSL VPN ユーザ ログイン グループ ドロップダウン、接続プロファイル内のグループ エイリアス
5	CSCO_WEBVPN_MACRO1	RADIUS/LDAP ベンダー固有属性によって設定
6	CSCO_WEBVPN_MACRO2	RADIUS/LDAP ベンダー固有属性によって設定

マクロ 1 ～ 4 の使用

セキュリティ アプライアンスは、[SSL VPN Login] ページから最初の 4 つの置き換えの値を取得します。それには、ユーザ名、パスワード、内部パスワード（任意）、およびグループのフィールドが含まれます。ユーザ要求内のこれらのストリングを認識し、このストリングをユーザ固有の値で置き換えてから、リモート サーバに要求を渡します。

たとえば、URL リストに http://someserver/homepage/CSCO_WEBVPN_USERNAME.html というリンクが含まれていると、セキュリティ アプライアンスはこのリンクを次の一意のリンクに変換します。

- USER1 の場合、リンクは http://someserver/homepage/USER1.html となります。
- USER2 の場合、リンクは http://someserver/homepage/USER2.html となります。

cifs://server/users/CSCO_WEBVPN_USERNAME の場合、セキュリティ アプライアンスは、次のようにファイル ドライブを特定のユーザにマップできます。

- USER1 の場合、リンクは cifs://server/users/USER1 となります。
- USER1 の場合、リンクは cifs://server/users/USER2 となります。

マクロ 5 および 6 の使用

マクロ 5 および 6 の値は、RADIUS または LDAP のベンダー固有属性（VSA）です。これらの置き換えにより、RADIUS または LDAP サーバのどちらかで設定される置き換えを設定できます。

例 1：ホームページの設定

次の例では、ホームページの URL を設定します。

- WebVPN-Macro-Value1 (ID=223), type string, は、*wwwin-portal.abc.com* として返されます。
- WebVPN-Macro-Value2 (ID=224), type string, は *401k.com* として返されます。

ホームページの値を設定するには、次のようにマクロを設定します。

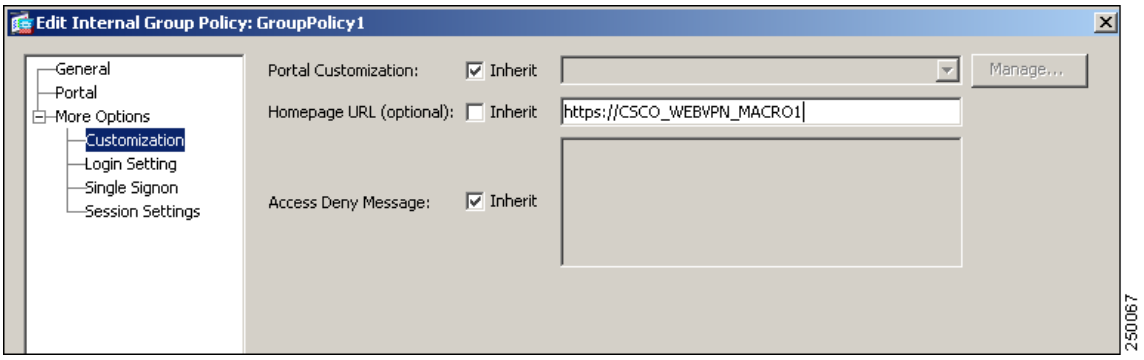
https://CSCO_WEBVPN_MACRO1。これは、https://wwwin-portal.abc.com に変換されます。

この場合の最善の方法は、ASDM で Homepage URL パラメータを設定することです。

図 34-2ASDM を使用した、ホームページを設定するマクロのコンフィギュレーションに示すように、ASDM の Network Client SSL VPN または Clientless SSL VPN Access セクションから、[Add/Edit Group Policy] ペインに移動します。パスは次のとおりです。

- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit Group Policy] > [Advanced] > [SSL VPN Client] > [Customization] > [Homepage URL] 属性
- [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add/Edit Group Policy] > [More Options] > [Customization] > [Homepage URL] 属性

図 34-2　ASDM を使用した、ホームページを設定するマクロのコンフィギュレーション



例 2：ブックマークまたは URL エントリの設定

SSL VPN 認証で RSA ワンタイム パスワード（OTP）を使用し、続いて OWA 電子メール アクセスでスタティックな内部パスワードを使用することによって、HTTP Post を使用して OWA リソースにログインできます。この場合の最善の方法は、図（図 34-3 ブックマーク エントリのコンフィギュレーション）のように ASDM でブックマーク エントリを追加または編集することです。

次のパスを含め、[Add Bookmark Entry] ペインへのパスは数通り存在します。

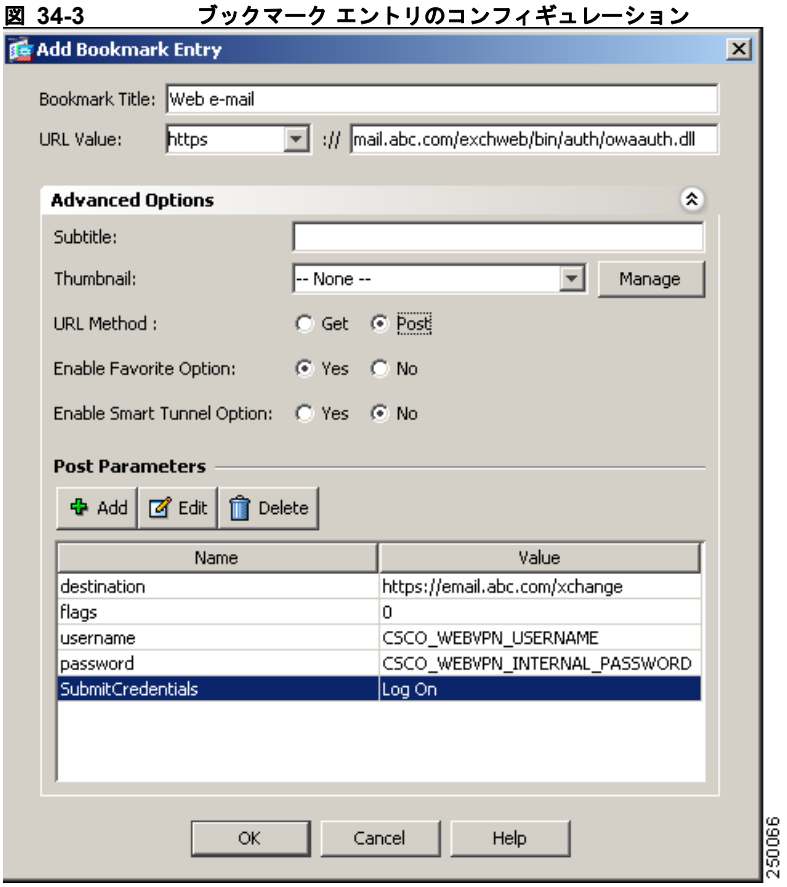
- [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] > [Add/Edit Bookmark Lists] > [Add/Edit Bookmark Entry] > [Advanced Options] 領域 > [Add/Edit Post Parameters]（URL Method 属性の [Post] をクリックすると表示されます）
- [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access]

  または

  （[URL Method] 属性の [Post] をクリックすると表示されます）

  [Network (Client) Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [URL Lists] タブ > [Manage] ボタン > [Configured GUI Customization Objects] > [Add/Edit] ボタン > [Add/Edit Bookmark List] > [Add/Edit Bookmark Entry] > [Advanced Options] 領域 > [Add/Edit Post Parameters]

図 34-3　ブックマーク エントリのコンフィギュレーション



言語のローカリゼーション

セキュリティ アプライアンスでは、ブラウザベースのクライアントレス SSL VPN 接続を開始したユーザに表示されるポータルおよび画面、オプションのプラグインに関連付けられた画面、および Cisco AnyConnect VPN Client ユーザに表示されるインターフェイスで、言語変換を行います。

この項では、これらのユーザ メッセージを変換するためにセキュリティ アプライアンスを設定する方法について説明します。次の項目を取り上げます。

- 「言語変換の概要」（P.34-87）
- 「変換テーブルの作成」（P.34-89）
- 「Add/Edit Localization Entry」（P.34-89）
- 「言語ローカリゼーションのインポートとエクスポート」（P.34-91）

言語変換の概要

各機能領域と、リモート ユーザに表示されるメッセージは、変換ドメインに分けられています。表 34-8 に、変換ドメインと変換される機能エリアを示します。

表 34-8　変換ドメインと影響を受ける機能エリア

変換ドメイン	変換される機能エリア
AnyConnect	Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。
CSD	Cisco Secure Desktop（CSD）のメッセージ。
customization	ログイン ページ、ログアウト ページ、ポータル ページのメッセージ、およびユーザによるカスタマイズが可能なすべてのメッセージ。
keepout	VPN アクセスを拒否された場合にリモート ユーザに表示されるメッセージ。
PortForwarder	ポート フォワーディング ユーザに表示されるメッセージ。
url-list	ユーザがポータル ページの URL ブックマークに指定するテキスト。
webvpn	カスタマイズできないすべてのレイヤ 7 メッセージ、AAA メッセージ、およびポータル メッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。

セキュリティ アプライアンスのソフトウェア イメージ パッケージには、標準機能の一部になっているドメインごとの言語ローカリゼーション テンプレートが組み込まれています。プラグインのテンプレートはプラグインとともに含まれており、独自の変換ドメインを定義します。

変換ドメインのテンプレートをエクスポートできます。これで、入力する URL にテンプレートの XML ファイルが作成されます。このファイルのメッセージ フィールドは空です。メッセージをカスタマイズしてテンプレートをインポートし、フラッシュ メモリに常駐させる新しい言語ローカリゼーション テーブルを作成できます。

また、既存の言語ローカリゼーション テーブルをエクスポートすることもできます。作成した XML ファイルに事前に編集したメッセージが表示されます。同じ言語名でこの XML ファイルを再インポートすると、以前のメッセージは上書きされ、新しいバージョンの言語ローカリゼーション テーブルが作成されます。

テンプレートにはスタティックのものも、セキュリティ アプライアンスの設定に基づいて変化するものもあります。ログインとログアウト ページ、ポータル ページ、およびクライアントレス セッションの URL ブックマークはカスタマイズできるため、セキュリティ アプライアンスは **customization** および **url-list** 変換ドメイン テンプレートをダイナミックに生成し、テンプレートにはこれらの機能領域に対する変更が自動的に反映されます。

言語ローカリゼーション テーブルを作成した後は、作成してグループ ポリシーまたはユーザ属性に適用するカスタマイゼーション オブジェクトとして使用できます。カスタマイゼーション オブジェクトを作成し、そのオブジェクトで使用する言語ローカリゼーション テーブルを特定し、グループ ポリシーまたはユーザのカスタマイゼーションを指定するまでは、言語ローカリゼーション テーブルによる影響はなく、ユーザ画面でメッセージは変換されません。

フィールド

[Add]：[Add Localization Entry] ダイアログを呼び出します。このダイアログで、追加するローカリゼーション テンプレートの選択、およびテンプレートの内容の編集ができます。

[Edit]：選択したテーブル内の言語の [Edit Localization Entry] ダイアログを呼び出します。このダイアログで、以前インポートした言語ローカリゼーション テーブルを編集できます。

[Delete]：選択した言語ローカリゼーション テーブルを削除します。

[Import]：[Import Language Localization] ダイアログを呼び出します。このダイアログで、言語ローカリゼーション テンプレートまたはテーブルをインポートできます。

[Export]：[Export Language Localization] ダイアログが起動します。このダイアログでは、言語ローカリゼーションのテンプレートまたはテーブルを、テーブルまたはテンプレートに変更を加えることが可能な URL にエクスポートできます。

[Language]：既存の言語ローカリゼーション テーブルの言語です。

[Language Localization Template]：テーブルの元になっているテンプレート。

変換テーブルの作成

ここでは、変換テーブルの作成方法について説明します。

ステップ 1　[Remove Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Advanced] > [Language Localization] に移動します。[Language Localization] ペインが表示されます。[Add] をクリックします。[Add Language Localization] ウィンドウが表示されます。

ステップ 2　ドロップダウン ボックスから、[Language Localization Template] を選択します。このボックスのエントリは、変換する機能エリアに対応します。テンプレートごとの機能の詳細については、表 34-8 を参照してください。

ステップ 3　テンプレートの言語を指定します。テンプレートはキャッシュメモリ内の変換テーブルになり、指定した名前が付きます。ブラウザの言語オプションと互換性のある短縮形を使用してください。たとえば、中国語のテーブルを作成するときに IE を使用している場合は、IE によって認識される *zh* という略語を使用します。

ステップ 4　変換テーブルを編集します。msgid フィールドで表される変換対象のメッセージごとに、対応する msgstr フィールドの引用符の間に変換済みテキストを入力します。次の例では、メッセージ Connected の msgstr フィールドにスペイン語テキストを入力しています。

```
msgid "Connected"
msgstr "Conectado"
```

ステップ 5　[OK] をクリックします。新しいテーブルが変換テーブルのリストに表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Localization Entry

このペインから、新しい変換テーブルや基準とするテンプレートの追加、またはすでにインポートされている変換テーブルの変更ができます。

フィールド

[Language Localization Template]：修正するテンプレートを選択し、新しい変換テーブルの基礎として使用します。テンプレートは変換ドメインに構成され、特定の機能領域に影響します。次の表に、変換ドメインと影響を受ける機能領域を示します。

変換ドメイン	変換される機能エリア
AnyConnect	Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。
CSD	Cisco Secure Desktop（CSD）のメッセージ。
customization	ログイン ページ、ログアウト ページ、ポータル ページのメッセージ、およびユーザによるカスタマイズが可能なすべてのメッセージ。
keepout	VPN アクセスを拒否された場合にリモート ユーザに表示されるメッセージ。
PortForwarder	ポート フォワーディング ユーザに表示されるメッセージ。
url-list	ユーザがポータル ページの URL ブックマークに指定するテキスト。
webvpn	カスタマイズできないすべてのレイヤ 7 メッセージ、AAA メッセージ、およびポータル メッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。

[Language]：言語を指定します。ブラウザの言語オプションと互換性のある略語を使用してください。セキュリティ アプライアンスは、この名前で新しい変換テーブルを作成します。

[Text Editor]：エディタを使用してメッセージ変換を変更します。メッセージ ID フィールド（msgid）には、デフォルトの変換が含まれています。msgid に続くメッセージ文字列フィールド（msgstr）で変換を指定します。変換を作成するには、msgstr 文字列の引用符の間に変換対象のテキストを入力します。たとえば、「Connected」というメッセージをスペイン語に変換するには、msgstr の引用符の間にスペイン語のテキストを挿入します。

```
msgid "Connected"
msgstr "Conectado"
```

変更を行った後、[Apply] をクリックして変換テーブルをインポートします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

言語ローカリゼーションのインポートとエクスポート

[Import Translation Table] および [Export Translation Table] ウィンドウでは、変換テーブルをセキュリティ アプライアンスにインポートまたはエクスポートして、ユーザ メッセージの変換機能を提供できます。

変換テンプレートは、変換済みメッセージで編集できるメッセージ フィールドが含まれている XML ファイルです。テンプレートをエクスポートし、メッセージフィールドを編集し、新しい変換テーブルとしてテンプレートをインポートするか、既存の変換テーブルをエクスポートし、メッセージフィールドを編集し、テーブルを再インポートして以前のバージョンを上書きすることができます。

フィールド

- [Language]：言語の名前を入力します。

  *エクスポート*の場合は、テーブルで選択したエントリの名前が自動的に取り込まれます。

  *インポート*の場合は、識別する方法で言語名を入力します。インポートされた変換テーブルは、指定した短縮形でリストに表示されます。ブラウザが言語を認識できるように、ブラウザの言語オプションと互換性のある言語短縮形を使用してください。たとえば、IE を使用する場合は、中国語の略語として ***zh*** を使用します。

- [Localization Template Name]：メッセージ フィールドが含まれている XML ファイルの名前。次のテンプレートを使用できます。
  - AnyConnect：Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。
  - CSD：Cisco Secure Desktop（CSD）のメッセージ。
  - customization：ログイン ページおよびログアウト ページのメッセージ、ポータル ページ、およびユーザがカスタマイズできるすべてのメッセージ。
  - keepout：VPN アクセスが拒否されたときに、リモート ユーザに対して表示されるメッセージ。
  - PortForwarder：Port Forwarding ユーザに表示されるメッセージ。
  - url-list：ユーザが、ポータル ページの URL ブックマークに指定したテキスト。
  - webvpn：カスタマイズできないレイヤ 7、AAA、およびポータルのすべてのメッセージ。
  - plugin-ica：Citrix プラグインのメッセージ。
  - plugin-rdp：Remote Desktop Protocol プラグインのメッセージ。
  - plugin-telnet,ssh：Telnet プラグインおよび SSH プラグインのメッセージ。
  - plugin-vnc：VNC プラグインのメッセージ。
- [Select a file]：ファイルをインポートまたはエクスポートする方式を選択します。
  - [Remote server]：セキュリティ アプライアンスからアクセスできるリモート サーバに常駐するカスタマイゼーション ファイルをインポートするには、このオプションを選択します。
  - [Path]：ファイルにアクセスする方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
  - [Flash file system]：セキュリティ アプライアンスに常駐するファイルをエクスポートするには、この方式を選択します。
  - [Path]：ファイルへのパスを入力します。
  - [Browse Flash]：ファイルへのパスを参照します。
  - [Local computer]：ローカル PC にあるファイルをインポートする場合は、この方式を選択します。

- [Path]：ファイルへのパスを入力します。
- [Browse Local Files]：ファイルへのパスを参照します。

- [Import Now]/[Export Now]：クリックすると、ファイルをインポートまたはエクスポートします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

AnyConnect のカスタマイゼーション

Resources

このパネルでは、AnyConnect VPN クライアントをカスタマイズするか、または再区分化するリソース ファイルを指定します。

（注）　セキュリティ アプライアンスは、AnyConnect VPN クライアントのバージョン 2.0 および 2.1 の場合に、この機能をサポートしません。クライアントの手動でのカスタマイズの詳細については、『AnyConnect VPN Client Administrator's Guide』および AnyConnect VPN Client のリリース ノートを参照してください。

フィールド

[Import]：[Import AnyConnect Customization Objects] ダイアログが起動します。このダイアログでは、オブジェクトとしてインポートするファイルを指定できます。

[Export]：[Export AnyConnect Customization Objects] ダイアログが起動します。このダイアログでは、オブジェクトとしてエクスポートするファイルを指定できます。

[Delete]：選択されたオブジェクトを削除します。

[Platform]：オブジェクトによってサポートされるリモート PC プラットフォームのタイプ。

[Object Name]：オブジェクトの名前。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Binary

このパネルでは、AnyConnect VPN クライアント API を使用するサードパーティ プログラムを指定します。セキュリティ アプライアンスは、ユーザ インターフェイスまたはコマンドライン インターフェイスをカスタマイズするクライアントに、これらのプログラムをダウンロードします。

（注）　セキュリティ アプライアンスは、AnyConnect VPN クライアントのバージョン 2.0 および 2.1 の場合に、この機能をサポートしません。クライアントの手動でのカスタマイズの詳細については、『AnyConnect VPN Client Administrator's Guide』および AnyConnect VPN Client のリリース ノートを参照してください。

フィールド

[Import]：[Import AnyConnect Customization Objects] ダイアログが起動します。このダイアログでは、オブジェクトとしてインポートするファイルを指定できます。

[Export]：[Export AnyConnect Customization Objects] ダイアログが起動します。このダイアログでは、オブジェクトとしてエクスポートするファイルを指定できます。

[Delete]：選択されたオブジェクトを削除します。

[Platform]：オブジェクトによってサポートされるリモート PC プラットフォームのタイプ。

[Object Name]：オブジェクトの名前。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Installs

このパネルでは、AnyConnect クライアント インストールのカスタマイズに使用するファイルを指定します。

（注）　セキュリティ アプライアンスは、AnyConnect VPN クライアントのバージョン 2.0 および 2.1 の場合に、この機能をサポートしません。クライアントの手動でのカスタマイズの詳細については、『AnyConnect VPN Client Administrator's Guide』および AnyConnect VPN Client のリリース ノートを参照してください。

フィールド

[Import]：[Import AnyConnect Customization Objects] ダイアログが起動します。このダイアログでは、オブジェクトとしてインポートするファイルを指定できます。

[Export]：[Export AnyConnect Customization Objects] ダイアログが起動します。このダイアログでは、オブジェクトとしてエクスポートするファイルを指定できます。

[Delete]：選択されたオブジェクトを削除します。

[Platform]：オブジェクトによってサポートされるリモート PC プラットフォームのタイプ。

[Object Name]：オブジェクトの名前。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Import AnyConnect Customization Objects

このダイアログでは、カスタマイゼーション オブジェクトをインポートまたはエクスポートできます。インポートするのは、AnyConnect クライアント ユーザに適用するオブジェクトです。セキュリティ アプライアンスにすでに存在するカスタマイゼーション オブジェクトは、編集のためにエクスポートし、その後再インポートできます。

（注）　セキュリティ アプライアンスは、AnyConnect VPN クライアントのバージョン 2.0 および 2.1 の場合に、この機能をサポートしません。クライアントの手動でのカスタマイズの詳細については、『AnyConnect VPN Client Administrator's Guide』および AnyConnect VPN Client のリリース ノートを参照してください。

フィールド

- [Customization Object Name]：カスタマイゼーション オブジェクトを名前で特定します。最大 64 文字で、スペースは使用できません。
- [Select a file]：カスタマイゼーション ファイルをインポートまたはエクスポートするときに使用する方式を選択します。
- [Local computer]：ローカル PC にあるファイルをインポートする場合は、この方式を選択します。
- [Path]：ファイルへのパスを入力します。
- [Browse Local Files]：ファイルへのパスを参照します。

- [Flash file system]：セキュリティ アプライアンスにあるファイルをエクスポートする場合は、この方式を選択します。
- [Path]：ファイルへのパスを入力します。
- [Browse Flash]：ファイルへのパスを参照します。
- [Remote server]：セキュリティ アプライアンスがアクセスできるリモート サーバにあるカスタマイゼーション ファイルをインポートする場合は、このオプションを選択します。
- [Path]：ファイルにアクセスする方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
- [Import Now]/[Export Now]：クリックすると、ファイルをインポートまたはエクスポートします。

CHAPTER 35

クライアントレス SSL VPN のエンド ユーザ設定

この章は、エンド ユーザのためのクライアントレス（ブラウザベース）SSL VPN を設定するシステム管理者を対象としています。ここでは、ユーザ リモート システムの設定要件と作業の概要を説明します。また、ユーザがクライアントレス SSL VPN の使用を開始するために、ユーザに伝える必要のある情報も明確にします。この項では、次のトピックについて取り上げます。

- ユーザ名とパスワードの要求
- セキュリティのヒントの通知
- クライアントレス SSL VPN の機能を使用するためのリモート システムの設定
- クライアントレス SSL VPN データのキャプチャ

（注） 次の説明では、すでにクライアントレス SSL VPN 用にセキュリティ アプライアンスが設定済みと想定しています。

ユーザ名とパスワードの要求

ネットワークによっては、リモート セッション中にユーザが、コンピュータ、インターネット サービス プロバイダー、クライアントレス SSL VPN、メール サーバ、ファイル サーバ、企業アプリケーションの一部またはすべてにログインする必要が生じることがあります。ユーザはさまざまなコンテキストで認証を行うために、固有のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。

表 35-1 に、クライアントレス SSL VPN ユーザが知っておく必要のあるユーザ名とパスワードのタイプを示します。

表 35-1　クライアントレス SSL VPN ユーザに通知するユーザ名とパスワード

ログイン ユーザ名 / パスワード タイプ	目的	入力するタイミング
コンピュータ	コンピュータへのアクセス	コンピュータの起動
Internet Service Provider : インターネット サービス プロバイダー	インターネットへのアクセス	インターネット サービス プロバイダーへの接続
クライアントレス SSL VPN	リモート ネットワークへのアクセス	クライアントレス SSL VPN セッションを開始するとき

表 35-1　クライアントレス SSL VPN ユーザに通知するユーザ名とパスワード （続き）

ログイン ユーザ名 / パスワード タイプ	目的	入力するタイミング
ファイル サーバ	リモート ファイル サーバへのアクセス	クライアントレス SSL VPN ファイル ブラウジング機能を使用して、リモート ファイル サーバにアクセスするとき
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバへのアクセス	クライアントレス SSL VPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メール サーバ	クライアントレス SSL VPN 経由によるリモート メール サーバへのアクセス	電子メール メッセージの送受信

セキュリティのヒントの通知

セッションから必ずログアウトするようにユーザに通知してください（クライアントレス SSL VPN からログアウトするには、クライアントレス SSL VPN ツールバーの logout アイコンをクリックするか、またはブラウザを閉じます）。

クライアントレス SSL VPN を使用してもすべてのサイトとの通信がセキュアであるとは限らないことを、ユーザに通知してください。クライアントレス SSL VPN は、企業ネットワーク上のリモート PC やワークステーションとセキュリティ アプライアンスとの間のデータ転送のセキュリティを保証するものです。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業のセキュリティ アプライアンスから目的の Web サーバまでの通信はセキュアではありません。

クライアントレス SSL VPN の機能を使用するためのリモート システムの設定

表 35-2 に、クライアントレス SSL VPN を使用するためのリモート システムの設定に関する、次の各種情報を示します。

- クライアントレス SSL VPN の起動
- クライアントレス SSL VPN フローティング ツールバーの使用
- Web ブラウジング
- ネットワーク ブラウジングとファイル管理
- アプリケーションの使用（ポート転送）
- ポート転送を介した電子メールの使用
- Web アクセスを介した電子メールの使用
- 電子メール プロキシを介した電子メールの使用

表 35-2 には、次の項目に関する情報も記載されています。

- クライアントレス SSL VPN の要件（機能別）
- クライアントレス SSL VPN がサポートされているアプリケーション
- クライアント アプリケーションのインストールとコンフィギュレーションの要件

- エンド ユーザに提供する必要のある情報
- エンド ユーザのためのヒントや使用上の推奨事項

ユーザ アカウントを異なって設定したことにより、クライアントレス SSL VPN ユーザがそれぞれに使用できる機能が異なる可能性があります。表 35-2 に、機能別の情報をまとめています。使用できない機能の情報についてはスキップしてください。

表 35-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
クライアントレス SSL VPN の起動	インターネットへの接続	サポートされているインターネット接続は、次のとおりです。 • 家庭の DSL、ケーブル、ダイヤルアップ • 公共のキオスク • ホテルの回線 • 空港の無線ノード • インターネット カフェ
	クライアントレス SSL VPN がサポートされているブラウザ	次のオペレーティング システムとブラウザでクライアントレス SSL VPN をテスト済みですが、他のオペレーティング システムとブラウザでも機能する場合があります。 • Internet Explorer 6.0 または 7.0、あるいは Firefox 1.5 または 2.0 を搭載した Microsoft Windows XP • Internet Explorer 7.0 または Firefox 2.0 を搭載した Microsoft Windows Vista • Safari 2.0 または Firefox 2.0 を搭載した Macintosh OS X • Firefox 1.5 または 2.0 を搭載した Linux
	ブラウザでイネーブルにされているクッキー	ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
	クライアントレス SSL VPN の URL	https アドレスの形式は次のとおりです。 https://*address* *address* は、クライアントレス SSL VPN がイネーブルになっているセキュリティ アプライアンス（またはロード バランシング クラスタ）のインターフェイスの IP アドレスまたは DNS ホスト名です。たとえば、https://10.89.192.163 または https://cisco.example.com のようになります。
	クライアントレス SSL VPN のユーザ名とパスワード	
	（任意）ローカル プリンタ	クライアントレス SSL VPN は、Web ブラウザからネットワーク プリンタへの印刷をサポートしていません。ローカル プリンタへの印刷はサポートされています。

表 35-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件 （続き）

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
クライアントレス SSL VPN 接続でのフローティング ツールバーの使用		フローティング ツールバーを使用すると、クライアントレス SSL VPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。 ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。 フローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。[Close] ボタンをクリックすると、セキュリティ アプライアンスはクライアントレス SSL VPN セッションの終了を確認するプロンプトを表示します。 **ヒント** ヒント：テキストをテキスト フィールドに貼り付けるには、Ctrl+V キーを使用します（クライアントレス SSL VPN ツールバーでは、右クリックはディセーブルになっています）。

表 35-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件 （続き）

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
Web ブラウジング	保護されている Web サイトのユーザ名とパスワード	クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。セキュリティのヒントの通知を参照してください。
		クライアントレス SSL VPN での Web ブラウジングのルックアンドフィールは、ユーザが使い慣れたものと異なる場合があります。次に例を示します。 • クライアントレス SSL VPN のタイトルバーが各 Web ページの上部に表示される。 • Web サイトへのアクセス方法： – [Clientless SSL VPN Home] ページ上の [Enter Web Address] フィールドに URL を入力する。 – [Clientless SSL VPN Home] ページ上にある設定済みの Web サイト リンクをクリックする。 – 上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする。 また、特定のアカウントの設定によっては、次のようになる場合もあります。 • 一部の Web サイトがブロックされている。 • アクセス可能な Web サイトが、[Clientless SSL VPN Home] ページにリンクとして表示されるサイトに限定される。
ネットワーク ブラウジングとファイル管理	共有リモート アクセス用に設定されたファイル アクセス権	クライアントレス SSL VPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。
	保護されているファイル サーバのサーバ名とパスワード	—
	フォルダとファイルが存在するドメイン、ワークグループ、およびサーバ名	ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。
	—	コピー処理の進行中は、**Copy File to Server** コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。

表 35-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件 （続き）

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
アプリケーションの使用 （ポート転送またはアプリケーション アクセスと呼ばれる）	（注）　Macintosh OS X の場合、この機能をサポートしているのは Safari ブラウザだけです。	
	（注）　この機能を使用するには、Sun Microsystems Java™ Runtime Environment をインストールしてローカル クライアントを設定する必要があります。これには、ローカル システムで管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。	
	注意　ユーザは、[Close] アイコンをクリックしてアプリケーションを終了したら、必ず [Application Access] ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体がディセーブルになる可能性があります。参照先	
	インストール済みのクライアント アプリケーション	—
	ブラウザでイネーブルにされているクッキー	—
	管理者特権	ユーザは、DNS 名を使用してサーバを指定する場合、ホスト ファイルを変更するのに必要になるため、PC に対する管理者アクセス権が必要になります。
	インストール済みの Sun Microsystems Java Runtime Environment（JRE）バージョン 1.4.x と 1.5.x ブラウザで Javascript をイネーブルにする必要があります。デフォルトでは有効に設定されています。	JRE がインストールされていない場合は、ポップアップ ウィンドウが表示され、ユーザに対して使用可能なサイトが示されます。 まれに、JAVA 例外エラーで、ポート転送アプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。 1. ブラウザのキャッシュをクリアして、ブラウザを閉じます。 2. JAVA アイコンがコンピュータのタスク バーに表示されていないことを確認します。JAVA のインスタンスをすべて閉じます。 3. クライアントレス SSL VPN セッションを確立し、ポート転送 JAVA アプレットを起動します。
	設定済みのクライアント アプリケーション（必要な場合）。 （注）　Microsoft Outlook クライアントの場合、この設定手順は不要です。 Windows 以外のすべてのクライアント アプリケーションでは、設定が必要です。 Windows アプリケーションの設定が必要かどうかを確認するには、[Remote Server] の値をチェックします。 • [Remote Server] にサーバ ホスト名が含まれている場合、クライアント アプリケーションの設定は不要です。 • [Remote Server] フィールドに IP アドレスが含まれている場合、クライアント アプリケーションを設定する必要があります。	クライアント アプリケーションを設定するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用します。この情報を見つけるには、次の手順を実行します。 1. リモート システムでクライアントレス SSL VPN を起動し、[Clientless SSL VPN Home] ページで Application Access リンクをクリックします。[Application Access] ウィンドウが表示されます。 2. [Name] カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を [Local] カラムで確認します。 3. この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、クライアント アプリケーションによって異なります。
	（注）　クライアントレス SSL VPN で実行されているアプリケーションで URL（電子メール内の URL など）をクリックしても、クライアントレス SSL VPN ではそのサイトは開きません。クライアントレス SSL VPN でこのようなサイトを開くには、[Enter (URL) Address] フィールドに URL をカット アンド ペーストします。	

表 35-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件 （続き）

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
Application Access を介した電子メールの使用	Application Access の要件を満たす（「アプリケーションの使用」を参照）	電子メールを使用するには、[Clientless SSL VPN Home] ページから Application Access を起動します。これにより、メール クライアントが使用できるようになります。
	（注）　IMAP クライアントの使用中にメール サーバとの接続が中断したり、新しく接続を確立できない場合は、IMAP アプリケーションを終了してクライアントレス SSL VPN を再起動します。	
	その他のメール クライアント	Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。 クライアントレス SSL VPN は、Lotus Notes および Eudora などの、ポート転送を介したその他の SMTPS、POP3S、または IMAP4S 電子メール プログラムをサポートしますが、動作確認は行っていません。
Web アクセスを介した電子メールの使用	インストールされている Web ベースの電子メール製品	サポートされている製品は次のとおりです。 • Outlook Web Access 最適な結果を得るために、Internet Explorer 6.x 以上、または Firefox 2.0 で OWA を使用してください。 • Louts iNotes その他の Web ベースの電子メール製品も動作しますが、動作確認は行っていません。
電子メール プロキシを介した電子メールの使用	インストール済みの SSL 対応メール アプリケーション セキュリティ アプライアンス SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。	サポートされているメール アプリケーションは次のとおりです。 • Microsoft Outlook • Microsoft Outlook Express バージョン 5.5 および 6.0 • Eudora 4.2 for Windows 2000 その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。
	設定済みのメール アプリケーション	

クライアントレス SSL VPN データのキャプチャ

CLI キャプチャ コマンドにより、クライアントレス SSL VPN 接続では正しく表示されない Web サイトに関する情報を記録できます。このデータは、シスコ カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ちます。次の各項では、キャプチャ コマンドの使用方法について説明します。

- キャプチャ ファイルの作成
- キャプチャ データを表示するためのブラウザの使用

（注）　クライアントレス SSL VPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成したら、キャプチャを必ずディセーブルにしてください。

キャプチャ ファイルの作成

次の手順を実行して、クライアントレス SSL VPN セッションに関するデータをファイルにキャプチャします。

ステップ 1　クライアントレス SSL VPN のキャプチャ ユーティリティを開始するには、特権 EXEC モードで **capture** コマンドを使用します。

capture *capture_name* **type webvpn user** *webvpn_username*

値は次のとおりです。

- *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *webvpn_user* は、キャプチャの対象となるユーザ名です。

キャプチャ ユーティリティが開始されます。

ステップ 2　ユーザがクライアントレス SSL VPN セッションを開始するためにログインします。キャプチャ ユーティリティは、パケットをキャプチャしています。

コマンドの **no** バージョンを使用してキャプチャを停止します。

no capture *capture_name*

キャプチャ ユーティリティは *capture_name*.zip ファイルを作成し、このファイルはパスワード **koleso** で暗号化されます。

ステップ 3　.zip ファイルをシスコに送信するか、Cisco TAC サービス リクエストに添付します。

ステップ 4　.zip ファイルの内容を確認するには、パスワード **koleso** を使用してファイルを解凍します。

次の例では、*hr* という名前のキャプチャを作成します。これは、user2 へのトラフィックを次のようにファイルにキャプチャします。

```
hostname# capture hr type webvpn user user2
WebVPN capture started.
   capture name   hr
   user name      user2
hostname# no capture hr
```

キャプチャ データを表示するためのブラウザの使用

次の手順を実行して、クライアントレス SSL VPN セッションに関するデータをキャプチャして、ブラウザに表示します。

ステップ 1　クライアントレス SSL VPN のキャプチャ ユーティリティを開始するには、特権 EXEC モードで **capture** コマンドを使用します。

capture *capture_name* **type webvpn user** *webvpn_username*

値は次のとおりです。

- *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *webvpn_user* は、キャプチャの対象となるユーザ名です。

キャプチャ ユーティリティが開始されます。

ステップ 2　ユーザがクライアントレス SSL VPN セッションを開始するためにログインします。キャプチャ ユーティリティは、パケットをキャプチャしています。

コマンドの **no** バージョンを使用してキャプチャを停止します。

ステップ 3　ブラウザを開き、[Address] ボックスに次のように入力します。

https://*asdm_enabled_interface_of_the_security_appliance***:***port***/admin/capture/***capture_name*/pcap

次のコマンド例は、hr という名前のキャプチャを表示します。

https://192.0.2.1:60000/admin/capture/hr/pcap

キャプチャされたコンテンツが sniffer 形式で表示されます。

ステップ 4　キャプチャ コンテンツを調べ終えたら、コマンドの **no** バージョンを使用してキャプチャを停止します。

CHAPTER 36

電子メール プロキシ

電子メール プロキシを設定すると、リモート電子メール機能をクライアントレス SSL VPN のユーザに拡張できます。ユーザが電子メール プロキシ経由で電子メール セッションを試行すると、電子メール クライアントが SSL プロトコルを使用してトンネルを確立します。

電子メール プロキシ プロトコルは次のとおりです。

POP3S

POP3S は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 995 をリッスンし、ポート 995 または設定されたポートとの接続が自動的に許可されます。POP3 プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に POP3 プロトコルが開始され、認証が行われます。POP3S は、電子メール受信用のプロトコルです。

IMAP4S

IMAP4S は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 993 をリッスンし、ポート 993 または設定されたポートとの接続が自動的に許可されます。IMAP4S プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に IMAP4S プロトコルが開始され、認証が行われます。IMAP4S は、電子メール受信用のプロトコルです。

SMTPS

SMTPS は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 988 をリッスンし、ポート 988 または設定されたポートとの接続が自動的に許可されます。SMTPS プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に SMTPS プロトコルが開始され、認証が行われます。SMTPS は、電子メール送信用のプロトコルです。

電子メール プロキシの設定

電子メール プロキシの設定は、次のタスクで構成されます。

- インターフェイスで電子メール プロキシをイネーブルにする。
- 電子メール プロキシ用のデフォルト サーバを設定する。
- AAA サーバ グループとデフォルトのグループ ポリシーを設定する。
- デリミタを設定する。

また、電子メール プロキシを設定するに当たっては、次の要件があります。

- 電子メール プロキシを経由してローカルとリモートの両方から電子メールにアクセスするユーザは、電子メール プログラムで、ローカル アクセス用とリモート アクセス用に別々の電子メール アドレスが必要です。
- 電子メール プロキシ セッションでユーザが認証される必要があります。

AAA

このパネルには、3 つのタブがあります。

- [POP3S] タブ
- [IMAP4S] タブ
- [SMTPS] タブ

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[POP3S] タブ

POP3S AAA パネルでは、AAA サーバ グループを関連付け、POP3S セッションに適用するデフォルトのグループ ポリシーを設定します。

フィールド

- [AAA server groups] : [AAA Server Groups] パネル（[Configuration] > [Features] > [Properties] > [AAA Setup] > [AAA Server Groups]）に移動する場合にクリックします。ここでは、AAA サーバ グループを追加または編集できます。
- [group policy] : [Group Policy] パネル（[Configuration] > [Features] > [VPN] > [General] > [Group Policy]）に移動する場合にクリックします。ここでは、グループ ポリシーを追加または編集できます。
- [Authentication Server Group] : POP3S ユーザ認証用の認証サーバ グループを選択します。デフォルトでは、認証サーバが設定されていません。AAA を POP3S 用の認証方式として設定した場合には（[Configuration] > [Features AAA] > [VPN] > [E-Mail Proxy] > [Authentication] パネル）、AAA サーバを設定してここで選択しないと、常に認証に失敗します。
- [Authorization Server Group] : POP3S ユーザ許可用の許可サーバ グループを選択します。デフォルトでは、許可サーバが設定されていません。
- [Accounting Server Group] : POP3S ユーザ アカウンティング用のアカウンティング サーバ グループを選択します。デフォルトでは、アカウンティング サーバが設定されていません。

- [Default Group Policy]：AAA が CLASSID 属性を返さない場合に POP3S ユーザに適用するグループ ポリシーを選択します。長さは、4 ～ 15 文字の英数字です。デフォルトのグループ ポリシーを指定しなかった場合と、CLASSID が存在しない場合には、セキュリティ アプライアンスがセッションを確立できません。
- [Authorization Settings]：セキュリティ アプライアンスが POP3S 許可のために認識するユーザ名の値を設定できるようにします。この名前は、デジタル証明書を使用して認証し、LDAP または RADIUS 許可を必要とする POP3S ユーザに適用されます。
  - [User the entire DN as the username]：POP3S 許可用の認定者名を使用する場合に選択します。
  - [Specify individual DN fields as the username]：ユーザ許可用に特定の DN フィールドを指定する場合に選択します。

    [DN] フィールドは、プライマリとセカンダリの 2 つを選択できます。たとえば、EA を選択した場合には、ユーザは電子メール アドレスによって認証されます。John Doe という一般名（CN）と johndoe@cisco.com という電子メール アドレスを持つユーザは、John Doe または johndoe として認証されません。彼は johndoe@cisco.com として認証される必要があります。EA および O を選択した場合、John Does は johndoe@cisco.com および Cisco Systems, Inc. として認証される必要があります。
  - [Primary DN Field]：POP3S 許可用に設定するプライマリ [DN] フィールドを選択します。デフォルトの設定は CN です。オプションには、次のものが含まれます。

DN フィールド	定義
Country（C）	2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name（CN）	ユーザ、システム、その他のエンティティの名前。これは、ID 階層の最下位（最も固有性の高い）レベルです。
DN Qualifier（DNQ）	特定の DN 属性。
E-mail Address（EA）	証明書を所有するユーザ、システム、またはエンティティの電子メール アドレス。
Generational Qualifier（GENQ）	Jr.、Sr.、または III などの世代修飾子。
Given Name（GN）	証明書所有者の名前（名）。
Initials（I）	証明書所有者の姓と名の最初の文字。
Locality（L）	組織が所在する市町村。
Name（N）	証明書所有者の名前。
Organization（O）	会社、団体、機関、協会、その他のエンティティの名前。
Organizational Unit（OU）	組織内のサブグループ。
Serial Number（SER）	証明書のシリアル番号。
Surname（SN）	証明書所有者の姓。
State/Province（S/P）	組織が所在する州や県。
Title（T）	証明書所有者の役職（Dr. など）。
User ID（UID）	証明書所有者の ID 番号。

  - [Secondary DN Field]：（任意）POP3S 許可用に設定するセカンダリ DN フィールドを選択します。デフォルトの設定は OU です。オプションには、上記の表に記載されているものすべてに加えて、[None] があります。これは、セカンダリ フィールドを指定しない場合に選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[IMAP4S] タブ

IMAP4S AAA パネルでは、AAA サーバ グループを関連付け、IMAP4S セッションに適用するデフォルトのグループ ポリシーを設定します。

フィールド

- [AAA server groups]：[AAA Server Groups] パネル（[Configuration] > [Features] > [Properties] > [AAA Setup] > [AAA Server Groups]）に移動する場合にクリックします。ここでは、AAA サーバ グループを追加または編集できます。
- [group policy]：[Group Policy] パネル（[Configuration] > [Features] > [VPN] > [General] > [Group Policy]）に移動する場合にクリックします。ここでは、グループ ポリシーを追加または編集できます。
- [Authentication Server Group]：IMAP4S ユーザ認証用の認証サーバ グループを選択します。デフォルトでは、認証サーバが設定されていません。AAA を IMAP4S 用の認証方式として設定した場合には（[Configuration] > [Features AAA] > [VPN] > [E-Mail Proxy] > [Authentication] パネル）、AAA サーバを設定してここで選択しないと、常に認証に失敗します。
- [Authorization Server Group]：IMAP4S ユーザ許可用の許可サーバ グループを選択します。デフォルトでは、許可サーバが設定されていません。
- [Accounting Server Group]：IMAP4S ユーザ アカウンティング用のアカウンティング サーバ グループを選択します。デフォルトでは、アカウンティング サーバが設定されていません。
- [Default Group Policy]：AAA が CLASSID 属性を返さない場合に IMAP4S ユーザに適用するグループ ポリシーを選択します。デフォルトのグループ ポリシーを指定しなかった場合と、CLASSID が存在しない場合には、セキュリティ アプライアンスがセッションを確立できません。
- [Authorization Settings]：セキュリティ アプライアンスが IMAP4S 許可のために認識するユーザ名の値を設定できるようにします。この名前は、デジタル証明書を使用して認証し、LDAP または RADIUS 許可を必要とする IMAP4S ユーザに適用されます。
  - [User the entire DN as the username]：IMAP4S 許可用の完全修飾ドメイン名を使用する場合に選択します。
  - [Specify individual DN fields as the username]：ユーザ許可用に特定の DN フィールドを指定する場合に選択します。

    [DN] フィールドは、プライマリとセカンダリの 2 つを選択できます。たとえば、EA を選択した場合には、ユーザは電子メール アドレスによって認証されます。John Doe という一般名（CN）と johndoe@cisco.com という電子メール アドレスを持つユーザは、John Doe または johndoe として認証されません。彼は johndoe@cisco.com として認証される必要があります。EA および O を選択した場合、John Does は johndoe@cisco.com *および*Cisco Systems, Inc. として認証される必要があります。

– [Primary DN Field]：IMAP4S 許可用に設定するプライマリ DN フィールドを選択します。デフォルトの設定は CN です。オプションには、次のものが含まれます。

DN フィールド	定義
Country（C）	2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name（CN）	ユーザ、システム、その他のエンティティの名前。これは、ID 階層の最下位（最も固有性の高い）レベルです。
DN Qualifier（DNQ）	特定の DN 属性。
E-mail Address（EA）	証明書を所有するユーザ、システム、またはエンティティの電子メール アドレス。
Generational Qualifier（GENQ）	Jr.、Sr.、または III などの世代修飾子。
Given Name（GN）	証明書所有者の名前（名）。
Initials（I）	証明書所有者の姓と名の最初の文字。
Locality（L）	組織が所在する市町村。
Name（N）	証明書所有者の名前。
Organization（O）	会社、団体、機関、協会、その他のエンティティの名前。
Organizational Unit（OU）	組織内のサブグループ。
Serial Number（SER）	証明書のシリアル番号。
Surname（SN）	証明書所有者の姓。
State/Province（S/P）	組織が所在する州や県。
Title（T）	証明書所有者の役職（Dr. など）。
User ID（UID）	証明書所有者の ID 番号。

– [Secondary DN Field]：（任意）IMAP4S 許可用に設定するセカンダリ DN フィールドを選択します。デフォルトの設定は OU です。オプションには、上記の表に記載されているものすべてに加えて、[None] があります。これは、セカンダリ フィールドを指定しない場合に選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

[SMTPS] タブ

SMTPS AAA パネルでは、AAA サーバ グループを関連付け、SMTPS セッションに適用するデフォルトのグループ ポリシーを設定します。

フィールド

- [AAA server groups] : [AAA Server Groups] パネル（[Configuration] > [Features] > [Properties] > [AAA Setup] > [AAA Server Groups]）に移動する場合にクリックします。ここでは、AAA サーバ グループを追加または編集できます。
- [group policy] : [Group Policy] パネル（[Configuration] > [Features] > [VPN] > [General] > [Group Policy]）に移動する場合にクリックします。ここでは、グループ ポリシーを追加または編集できます。
- [Authentication Server Group] : SMTPS ユーザ認証用の認証サーバ グループを選択します。デフォルトでは、認証サーバが設定されていません。AAA を SMTPS 用の認証方式として設定した場合には（[Configuration] > [Features AAA] > [VPN] > [E-Mail Proxy] > [Authentication] パネル）、AAA サーバを設定してここで選択しないと、常に認証に失敗します。
- [Authorization Server Group] : SMTPS ユーザ許可用の許可サーバ グループを選択します。デフォルトでは、許可サーバが設定されていません。
- [Accounting Server Group] : SMTPS ユーザ アカウンティング用のアカウンティング サーバ グループを選択します。デフォルトでは、アカウンティング サーバが設定されていません。
- [Default Group Policy] : AAA が CLASSID 属性を返さない場合に SMTPS ユーザに適用するグループ ポリシーを選択します。デフォルトのグループ ポリシーを指定しなかった場合と、CLASSID が存在しない場合には、セキュリティ アプライアンスがセッションを確立できません。
- [Authorization Settings] : セキュリティ アプライアンスが SMTPS 許可のために認識するユーザ名の値を設定できるようにします。この名前は、デジタル証明書を使用して認証し、LDAP または RADIUS 許可を必要とする SMTPS ユーザに適用されます。
  - [User the entire DN as the username] : SMTPS 許可用の完全修飾ドメイン名を使用する場合に選択します。
  - [Specify individual DN fields as the username] : ユーザ許可用に特定の DN フィールドを指定する場合に選択します。

    [DN] フィールドは、プライマリとセカンダリの 2 つを選択できます。たとえば、EA を選択した場合には、ユーザは電子メール アドレスによって認証されます。John Doe という一般名（CN）と johndoe@cisco.com という電子メール アドレスを持つユーザは、John Doe または johndoe として認証されません。彼は johndoe@cisco.com として認証される必要があります。EA および O を選択した場合、John Does は johndoe@cisco.com *および* Cisco Systems, Inc. として認証される必要があります。
  - [Primary DN Field] : SMTPS 許可用に設定するプライマリ DN フィールドを選択します。デフォルトの設定は CN です。オプションには、次のものが含まれます。

DN フィールド	定義
Country（C）	2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name（CN）	ユーザ、システム、その他のエンティティの名前。これは、ID 階層の最下位（最も固有性の高い）レベルです。
DN Qualifier（DNQ）	特定の DN 属性。
E-mail Address（EA）	証明書を所有するユーザ、システム、またはエンティティの電子メール アドレス。
Generational Qualifier（GENQ）	Jr.、Sr.、または III などの世代修飾子。
Given Name（GN）	証明書所有者の名前（名）。
Initials（I）	証明書所有者の姓と名の最初の文字。
Locality（L）	組織が所在する市町村。

DN フィールド	定義
Name（N）	証明書所有者の名前。
Organization（O）	会社、団体、機関、協会、その他のエンティティの名前。
Organizational Unit（OU）	組織内のサブグループ。
Serial Number（SER）	証明書のシリアル番号。
Surname（SN）	証明書所有者の姓。
State/Province（S/P）	組織が所在する州や県。
Title（T）	証明書所有者の役職（Dr. など）。
User ID（UID）	証明書所有者の ID 番号。

  - [Secondary DN Field]：（任意）SMTPS 許可用に設定するセカンダリ DN フィールドを選択します。デフォルトの設定は OU です。オプションには、上記の表に記載されているものすべてに加えて、[None] があります。これは、セカンダリ フィールドを指定しない場合に選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

アクセス

[E-mail Proxy Access] 画面では、電子メール プロキシを設定するインターフェイスを識別できます。電子メール プロキシは、個々のインターフェイスで設定および編集できます。また、1 つのインターフェイスで電子メール プロキシを設定および編集すれば、その設定をすべてのインターフェイスに適用できます。管理専用のインターフェイスやサブインターフェイスに対して電子メール プロキシは設定できません。

フィールド

- [Interface]：設定されているすべてのインターフェイスの名前を表示します。
- [POP3S Enabled]：そのインターフェイスで POP3S がイネーブルかどうかを示します。
- [IMAP4s Enabled]：そのインターフェイスで IMAP4S がイネーブルかどうかを示します。
- [SMTPS Enabled]：そのインターフェイスで SMTPS がイネーブルかどうかを示します。
- [Edit]：強調表示されているインターフェイスの電子メール プロキシ設定を編集する場合にクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit E-Mail Proxy Access

[E-mail Proxy Access] 画面では、電子メール プロキシを設定するインターフェイスを識別できます。電子メール プロキシは、個々のインターフェイスで設定できます。また、1 つのインターフェイスで電子メール プロキシを設定すると、その設定をすべてのインターフェイスに適用できます。

フィールド

- [Interface]：選択されたインターフェイスの名前を表示します。
- [POP3S Enabled]：そのインターフェイスで POP3S をイネーブルにする場合に選択します。
- [IMAP4S Enabled]：そのインターフェイスで IMAP4S をイネーブルにする場合に選択します。
- [SMTPS Enabled]：そのインターフェイスで SMTPS をイネーブルにする場合に選択します。
- [Apply to all interface]：現在のインターフェイスの設定を、設定されているすべてのインターフェイスに適用する場合に選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Authentication

このパネルでは、電子メール プロキシ セッションの認証方式を設定できます。

フィールド

[POP3S/IMAP4S/SMTPS Authentication]：各種電子メール プロキシの認証方式を設定します。複数の認証方式を選択できます。

- [AAA]：AAA 認証を必須にする場合に選択します。このオプションを使用するには、AAA サーバを設定する必要があります。ユーザは、ユーザ名、サーバ、およびパスワードを入力します。ユーザは、VPN ユーザ名と電子メール ユーザ名の両方を入力する必要があります。そのとき、互いのユーザ名が異なる場合にだけ、VPN 名デリミタによって区切ります。
- [Certificate]：現在のセキュリティ アプライアンス ソフトウェア リリースでは、電子メール プロキシに対して証明書認証が機能しません。

- [Piggyback HTTPS]：ピギーバック認証を必須にする場合に選択します。

  この認証スキームは、ユーザがすでにクライアントレス SSL VPN セッションを確立していることを必須とします。そのため、ユーザは電子メール ユーザ名だけを入力します。パスワードは不要です。ユーザは、VPN ユーザ名と電子メール ユーザ名の両方を入力する必要があります。そのとき、互いのユーザ名が異なる場合にだけ、VPN 名デリミタによって区切ります。

  SMTPS 電子メールは、最も頻繁にピギーバックを使用します。ほとんどの SMTP サーバが、ユーザがログインすることを許可していないためです。

（注）IMAP は、同時ユーザ数によって制限されない多数のセッションを生成しますが、ユーザ名に対して許可されている同時ログインの数を数えません。IMAP セッションの数がこの最大値を超え、クライアントレス SSL VPN 接続の有効期限が切れた場合には、その後ユーザが新しい接続を確立できません。以下の解決策があります。

- ユーザが IMAP アプリケーションを終了して セキュリティ アプライアンス とのセッションをクリアしてから、新しいクライアントレス SSL VPN 接続を確立する。
- 管理者が IMAP ユーザの同時ログイン数を増やす（[Configuration] > [Features] > [VPN] > [General] > [Group Policy] > [Edit Group Policy] > [General]）。
- 電子メール プロキシの HTTPS/ ピギーバック認証をディセーブルにする。

- [Mailhost]：（SMTPS のみ）メールホスト認証を必須にする場合に選択します。POP3S と IMAP4S は必ずメールホスト認証を実行するため、このオプションは、SMTPS の場合にだけ表示されます。この認証方式では、ユーザの電子メール ユーザ名、サーバ、およびパスワードが必要です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Default Servers

このパネルでは、セキュリティ アプライアンスのプロキシ サーバを識別できます。適切なプロキシ サーバの IP アドレスとポートを入力します。

フィールド

- [POP3S/IMAP4S/SMTPS Default Server]：電子メール プロキシのデフォルト サーバ、ポート、および非認証セッション制限を設定します。
- [Name or IP Address]：デフォルトの電子メール プロキシ サーバの DNS 名または IP アドレスを入力します。

- [Port] : セキュリティ アプライアンスがプロキシ トラフィックをリッスンするポート番号を入力します。設定されたポートに対する接続が自動的に許可されます。電子メール プロキシは、SSL 接続だけをこのポートで許可します。SSL トンネルが確立された後に電子メール プロキシ プロトコルが開始され、認証が行われます。

  POP3S のデフォルトのポートは 995 で、IMAP4S は 993、SMTPS は 988 です。

- [Enable non-authenticated session limit] : 非認証電子メール プロキシ セッションの数を制限する場合に選択します。

  電子メール プロキシ接続には、3 つの状態があります。

  1. 新規に電子メール接続が確立されると、「認証されていない」状態になります。
  2. この接続でユーザ名が提示されると、「認証中」状態になります。
  3. セキュリティ アプライアンスが接続を認証すると、「認証済み」状態になります。

  この機能により、認証プロセスでのセッションの制限を設定でき、それによって DOS 攻撃を防ぎます。新しいセッションが、設定された制限を超えると、セキュリティ アプライアンスが最も古い非認証接続を終了します。非認証接続が存在しない場合には、最も古い認証接続が終了します。それによって認証済みのセッションが終了することはありません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Delimiters

このパネルでは、電子メール プロキシ認証で使用するユーザ名 / パスワード デリミタとサーバ デリミタを設定します。

フィールド

- [POP3S/IMAP4S/SMTPS Delimiters] : 各種電子メール プロキシのユーザ名 / パスワード デリミタとサーバ デリミタを設定します。
  - [Username/Password Delimiter] : VPN ユーザ名と電子メール ユーザ名を区切るためのデリミタを選択します。電子メール プロキシで AAA 認証を使用する場合、および VPN ユーザ名と電子メール ユーザ名が異なる場合に両方のユーザ名を使用します。ユーザは、両方のユーザ名を入力し、ここで設定したデリミタで区切ります。電子メール プロキシ セッションにログインする場合には、電子メール サーバ名も入力します。

（注） クライアントレス SSL VPN 電子メール プロキシ ユーザのパスワードに、デリミタとして使用されている文字を含めることはできません。

– [Server Delimiter] : ユーザ名と電子メール サーバ名を区切るためのデリミタを選択します。このデリミタは、VPN 名デリミタとは別にする必要があります。電子メール プロキシ セッションにログインする場合には、ユーザ名フィールドにユーザ名とサーバの両方を入力します。

  たとえば、VPN 名デリミタとして : を使用し、サーバ デリミタとして @ を使用する場合には、電子メール プロキシ経由で電子メール プログラムにログインするときに、vpn_username:e-mail_username@server という形式でユーザ名を入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

CHAPTER 37

SSL 設定の指定

SSL

セキュリティ アプライアンス は、Secure Sockets Layer（SSL）プロトコルおよびその後継である Transport Layer Security（TLS）を使用して、ASDM セッションとクライアントレス ブラウザベース セッションのセキュアなメッセージ伝送を実現します。SSL ウィンドウでは、クライアントとサーバ、および暗号化アルゴリズムの SSL バージョンを設定できます。また、以前に設定したトラストポイントを特定のインターフェイスに適用したり、関連付けられたトラストポイントのないインターフェイスのフォールバック トラストポイントを設定したりすることもできます。

フィールド

- [Server SSL Version]：サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコル バージョンを指定します。選択できるのは 1 つだけです。

Server SSL バージョンのオプションは、次のとおりです。

Any	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、SSL バージョン 3 または TLS バージョン 1 がネゴシエートされます。
Negotiate SSL V3	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、SSL バージョン 3 にネゴシエートされます。
Negotiate TLS V1	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、TLS バージョン 1 にネゴシエートされます。
SSL V3 Only	セキュリティ アプライアンスによって SSL バージョン 3 クライアントの hello のみが受け入れられ、SSL バージョン 3 のみが使用されます。
TLS V1 Only	セキュリティ アプライアンスによって TLSv1 クライアントの hello のみが受け入れられ、TLS バージョン 1 のみが使用されます。

（注） クライアントレス SSL VPN のポート転送を使用するには、Any または Negotiate SSL V3 を選択する必要があります。問題は、ポート フォワーディング アプリケーションを起動すると、JAVA ではクライアントの Hello パケットで SSLv3 のみがネゴシエートされることです。

- [Client SSL Version]：サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコル バージョンを指定します。選択できるのは 1 つだけです。

Client SSL バージョンのオプションは、次のとおりです。

any	セキュリティ アプライアンスによって SSL バージョン 3 の hello が送信され、SSL バージョン 3 または TLS バージョン 1 がネゴシエートされます。
sslv3-only	セキュリティ アプライアンスによって SSL バージョン 3 の hello が送信され、SSL バージョン 3 のみが受け入れられます。
tlsv1-only	セキュリティ アプライアンスによって TLSv1 クライアントの hello が送信され、TLS バージョン 1 のみが受け入れられます。

- [Encryption]：SSL 暗号化アルゴリズムを設定できます。
  - [Available Algorithms]：セキュリティ アプライアンス がサポートし、SSL 接続で使用されていない暗号化アルゴリズムを一覧表示します。使用可能なアルゴリズムを使用するか、またはアクティブにするには、アルゴリズムを選択して [Add] をクリックします。
  - [Active Algorithms]：セキュリティ アプライアンスがサポートし、現在 SSL 接続で使用中の暗号化アルゴリズムを一覧表示します。使用を中止するか、アクティブなアルゴリズムを [Available] ステータスに変更するには、アルゴリズムを選択して [Remove] をクリックします。
  - [Add/Remove]：[Available] または [Active Algorithms] カラムの暗号化アルゴリズムのステータスを変更します。
  - [Move Up] および [Move Down]：アルゴリズムを選択し、これらのボタンをクリックして優先順位を変更します。セキュリティ アプライアンスは、アルゴリズムの使用を試みます。
- [Certificates]：フォールバック証明書を選択できます。設定済みのインターフェイスおよびそれらに関連付けられている設定済みの証明書が表示されます。
  - [Fallback Certificate]：証明書が関連付けられていないインターフェイスで使用する証明書を選択します。[None] を選択すると、セキュリティ アプライアンス はデフォルトの RSA キーペアと証明書を使用します。
  - [Interface] カラムおよび [ID Certificate] カラム：設定済みインターフェイス、および存在する場合にはそのインターフェイスの証明書を表示します。
  - [Edit]：選択したインターフェイスのトラストポイントを変更します。
- [Apply]：変更を適用します。
- [Reset]：変更内容を取り消し、SSL パラメータをリセットして、ウィンドウを開いたときに保存されていた値に戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Edit SSL Certificate

フィールド

- [Interface]：編集中のインターフェイスの名前を表示します。
- [Certificate]：名前付きインターフェイスに関連付ける登録済みの証明書を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SSL 証明書

このペインでは、デバイス管理セッションで SSL 認証のユーザ証明書を必要とするように指定できます。

フィールド

- [Interface]：編集中のインターフェイスの名前を表示します。
- [User Certificate Required]：名前付きインターフェイスに関連付ける登録済み証明書を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 38

証明書の設定

この章では、デジタル証明書の設定方法について説明します。次の項目を取り上げます。

デジタル証明書に関する情報

デジタル証明書は、認証に使用されるデジタル ID を保持しています。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、適応型セキュリティ アプライアンス に 1 つ以上の ID 証明書と、その発行元の CA 証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。次に、使用可能な各種デジタル証明書について説明します。

- *CA 証明書*は、他の証明書に署名するために使用されます。これは自己署名され、*ルート証明書*と呼ばれます。別の CA 証明書により発行される証明書は、*下位証明書*と呼ばれます。詳細については、「CA 証明書認証の設定」（P.38-2）を参照してください。
- *ID 証明書*は、特定のシステムまたはホストの証明書です。この証明書も CA により発行されます。詳細については、「ID 証明書の認証の設定」（P.38-9）を参照してください。
- *コード署名者証明書*は、コードに署名するためのデジタル署名を作成する際に使用される特殊な証明書であり、署名されたコードそのものが証明書の作成元を示しています。詳細については、「コード署名者証明書の設定」（P.38-14）を参照してください。

ローカル CA は、適応型セキュリティ アプライアンス の独立認証局機能を統合したもので、証明書の配布と、発行された証明書に対するセキュアな失効チェックを行います。Web サイトのログイン ページからユーザ登録を行う場合には、ローカル CA により実現されるセキュアで設定可能な内部認証局機能によって、証明書の認証を行うことができます。詳細については、「ローカル CA を使用した認証」（P.38-16）、「ユーザ証明書の管理」（P.38-23）、および「ユーザ データベースの管理」（P.38-20）を参照してください。

（注）　CA 証明書および ID 証明書は、サイトツーサイト VPN 接続およびリモート アクセス VPN 接続の両方に適用されます。このマニュアルに記載の手順は、ASDM GUI でリモート アクセス VPN を使用する場合の手順です。

デジタル証明書のライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

フェールオーバーのガイドライン

ステートフル フェールオーバーではセッションの複製はサポートされません。

IPv6 のガイドライン

IPv6 をサポートします。

CA 証明書認証の設定

[CA Certificates] ペインには、使用可能な証明書、発行先および発行元の CA サーバによる識別、証明書の有効期限日、関連付けられているトラストポイント、および証明書の使用法と目的が表示されます。[CA Certificates] ペインでは、次のタスクを実行できます。

- 自己署名または下位 CA 証明書を認証します。
- CA 証明書を 適応型セキュリティ アプライアンス にインストールします。
- 新しい証明書コンフィギュレーションを作成します。

- 既存の証明書コンフィギュレーションを編集します。
- CA 証明書を手動で取得してインポートします。
- 適応型セキュリティ アプライアンス が SCEP を使用して CA に接続して、自動的に証明書を取得およびインストールするようにします。
- 選択した証明書の詳細と発行元情報を表示します。
- 既存の CA 証明書の CRL にアクセスします。
- 既存の CA 証明書のコンフィギュレーションを削除します。
- 新規作成または修正した CA 証明書コンフィギュレーションを保存します。
- 変更内容をすべて破棄して、証明書コンフィギュレーションを元の設定に戻します。

この項では、次のトピックについて取り上げます。

CA 証明書の追加またはインストール

PEM 形式での証明書の手動による貼り付けや、SCEP を使用した自動登録により、既存のファイルから証明書コンフィギュレーションを新たに追加できます。SCEP は、ユーザの介入を最小限しか必要としない、セキュアなメッセージング プロトコルです。SCEP を使用すると、VPN Concentrator Manager のみを使用して証明書を登録およびインストールできます。

CA 証明書を追加またはインストールするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Remote Access VPN] > [Certificate Management] > [CA Certificates] の順に選択します。

ステップ 2　[Add] をクリックします。

[Install Certificate] ダイアログボックスが表示されます。選択されたトラストポイント名が読み取り専用形式で表示されます。

ステップ 3　既存のファイルから証明書コンフィギュレーションを追加するには、[Install from a file] オプション ボタンをクリックします（これがデフォルトの設定です）。

ステップ 4　パスおよびファイル名を入力するか、または [Browse] をクリックしてファイルを検索します。次に、[Install Certificate] をクリックします。

ステップ 5　手動で登録するには、[Paste certificate in PEM format] オプション ボタンをクリックします。

ステップ 6　PEM 形式（base64 または 16 進数）の証明書をコピーして、指定の領域に貼り付け、[Install Certificate] をクリックします。

ステップ 7　自動で登録するには、[Use SCEP] オプション ボタンをクリックします。適応型セキュリティ アプライアンス が、SCEP を使用して CA に接続し、証明書を取得して、証明書をデバイスにインストールします。SCEP を使用するには、インターネットを介して、SCEP をサポートする CA に登録する必要があります。SCEP を使用した自動登録では、ユーザは次の情報を入力する必要があります。

- 自動インストールする証明書のパスとファイル名。
- 証明書のインストールの最大再試行分数。デフォルトは 1 分です。
- 証明書のインストールの再試行回数。デフォルトは 0 です。この場合は、再試行時間内であれば何度でも再試行できます。

ステップ 8　新規および既存の証明書のその他のコンフィギュレーション オプションを表示するには、[More Options] をクリックします。

[Configuration Options for CA Certificates] ペインが表示されます。

ステップ 9　以降の手順については、「失効に関する CA 証明書の設定」（P.38-5）を参照してください。

CA 証明書コンフィギュレーションの編集または削除

既存の CA 証明書コンフィギュレーションを変更または削除するには、次の手順を実行します。

ステップ 1　既存の CA 証明書コンフィギュレーションを変更するには、コンフィギュレーションを選択し、[Edit] をクリックします。

[Edit Options for CA Certificates] ペインが表示されます。これらのいずれかの設定を変更するには、後述の項で手順を参照してください。

- 「失効に関する CA 証明書の設定」（P.38-5）
- 「CRL 取得ポリシーの設定」（P.38-5）
- 「CRL 取得方式の設定」（P.38-6）
- 「OCSP ルールの設定」（P.38-7）
- 「高度な CRL および OCSP の設定」（P.38-7）

ステップ 2　CA 証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

（注）　証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

CA 証明書の詳細の表示

選択した CA 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの*表示専用*タブが含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

CRL の要求

現在のバージョンの CRL を更新するには、[Request CRL] をクリックします。CRL の更新により、証明書ユーザに現在のステータスが反映されます。要求が失敗した場合は、エラー メッセージが表示されます。CRL は、更新された後、期限が切れるまで自動的に再生成されますが、[Request CRL] をクリックすれば、CRL ファイルの更新と再生成がその場で実行されます。

失効に関する CA 証明書の設定

失効に関して CA 証明書を設定するには、次の手順を実行します。

ステップ 1　[Configuration Options for CA Certificates] ペインで、[Revocation Check] タブをクリックします。

ステップ 2　証明書の失効チェックをディセーブルにするには、[Do not check certificates for revocation] オプション ボタンをクリックします。

ステップ 3　1 つ以上の失効チェック方式（CRL または OCSP）を選択するには、[Check certificates for revocation] オプション ボタンをクリックします。

ステップ 4　[Revocation Methods] 領域の左側に、選択可能な方式が表示されます。[Add] をクリックして方式を右側に移動すると、その方式が使用可能になります。[Move Up] または [Move Down] をクリックして、方式の順序を変更します。

選択した方式は、追加した順序で実装されます。方式からエラーが返された場合は、その次の失効チェック方式がアクティブになります。

ステップ 5　証明書の検証中に失効チェックのエラーを無視するには、[Consider certificate valid if revocation checking returns errors] チェックボックスをオンにします。

ステップ 6　[OK] をクリックして、[Revocation Check] タブを閉じます。また、続行する場合は「CRL 取得ポリシーの設定」（P.38-5）を参照してください。

CRL 取得ポリシーの設定

CRL 取得ポリシーを設定するには、次の手順を実行します。

ステップ 1　[Configuration Options for CA Certificates] ペインで、[CRL Retrieval Policy] タブをクリックします。

ステップ 2　[Use CRL Distribution Point from the certificate] チェックボックスをオンにして、チェック対象の証明書から CRL 分散ポイントに失効チェックを転送します。

ステップ 3　[Use Static URLs configured below] チェックボックスをオンにして、CRL の取得に使用する特定の URL を一覧表示します。選択した URL は、追加した順序で実装されます。指定した URL でエラーが発生した場合は、その次の URL が使用されます。

ステップ 4　[Static Configuration] 領域で、[Add] をクリックします。

[Add Static URL] ダイアログボックスが表示されます。

ステップ 5　[URL] フィールドに、CRL の分散に使用するスタティック URL を入力して、[OK] をクリックします。

入力した URL が [Static URLs] リストに表示されます。

ステップ 6　スタティック URL を変更するには、URL を選択し、[Edit] をクリックします。

ステップ 7　既存のスタティック URL を削除するには、URL を選択し、[Delete] をクリックします。

ステップ 8　スタティック URL の表示順序を変更するには、[Move Up] または [Move Down] をクリックします。

ステップ 9　[OK] をクリックして、このタブを閉じます。また、続行する場合は「CRL 取得方式の設定」（P.38-6）を参照してください。

CRL 取得方式の設定

CRL 取得方式を設定するには、次の手順を実行します。

ステップ 1　[Configuration Options for CA Certificates] ペインで、[CRL Retrieval Methods] タブをクリックします。

ステップ 2　次の 3 つの取得方式のいずれかを選択します。

- CRL の取得で LDAP をイネーブルにするには、[Enable Lightweight Directory Access Protocol (LDAP)] チェックボックスをオンにします。LDAP を使用して CRL を取得する場合は、指定した LDAP サーバにパスワードを使用して接続することで、LDAP セッションが開始されます。デフォルトの場合、この接続には TCP ポート 389 が使用されます。次の必須パラメータを入力します。
  - 名前
  - パスワード
  - パスワードの確認
  - デフォルト サーバ（サーバ名）
  - デフォルト ポート（389）
- CRL の取得で HTTP をイネーブルにするには、[Enable HTTP] チェックボックスをオンにします。
- CRL の取得で SCEP をイネーブルにするには、[Enable Simple Certificate Enrollment Protocol (SCEP)] チェックボックスをオンにします。

ステップ 3　[OK] をクリックして、このタブを閉じます。また、続行する場合は「OCSP ルールの設定」（P.38-7）を参照してください。

OCSP ルールの設定

適応型セキュリティ アプライアンスでは、プライオリティ順に OCSP ルールが検証され、最初に一致したルールが適用されます。CRL の代わりに X.509 デジタル証明書が使用されます。

（注）　OCSP ルールを追加する前に、必ず証明書マップを設定しておいてください。証明書マップが設定されていない場合、エラー メッセージが表示されます。証明書マップを設定するには、[Configuration] > [Network (Client) Access, Advanced] > [IPSec] > [Certificate to Connection Profile Maps] > [Rules] > [Add] を選択します。

X.509 デジタル証明書の失効ステータスを取得するための OCSP ルールを設定するには、次の手順を実行します。

ステップ 1　[Configuration Options for CA Certificates] ペインで、[OCSP Rules] タブをクリックします。

ステップ 2　この OCSP ルールと照合する証明書マップを選択します。証明書マップにより、ユーザ権限と、証明書の特定のフィールドとの照合が行われます。[Certificate] フィールドに、適応型セキュリティ アプライアンス において応答側の証明書の検証に使用される CA の名前が表示されます。[Index] フィールドに、ルールのプライオリティ番号が表示されます。[URL] フィールドに、この証明書の OCSP サーバの URL が表示されます。

ステップ 3　新しい OCSP ルールを追加するには、[Add] をクリックします。

[Add OCSP Rule] ダイアログボックスが表示されます。

ステップ 4　使用する証明書マップをドロップダウン リストから選択します。

ステップ 5　使用する証明書をドロップダウン リストから選択します。

ステップ 6　ルールのプライオリティ番号を入力します。

ステップ 7　この証明書の OCSP サーバの URL を入力します。

ステップ 8　完了したら、[OK] をクリックして、このダイアログボックスを閉じます。

新しく追加された OCSP ルールがリストに表示されます。

ステップ 9　既存の OCSP ルールを編集するには、ルールを選択し、[Edit] をクリックします。

ステップ 10　OCSP ルールを削除するには、ルールを選択し、[Delete] をクリックします。

ステップ 11　[OK] をクリックして、このタブを閉じます。また、続行する場合は「高度な CRL および OCSP の設定」（P.38-7）を参照してください。

高度な CRL および OCSP の設定

証明書は発行されると、一定期間有効です。CA は、安全上の問題や名前またはアソシエーションの変更などの理由で、期限が切れる前に証明書を無効にすることがあります。CA は、無効になった証明書の署名付きリストを定期的に発行します。失効チェックをイネーブルにすると、適応型セキュリティ アプライアンスでは、検証中の証明書が CA により無効になっていないかについてのチェックが行われます。適応型セキュリティ アプライアンスでは、失効ステータスに対して、CRL および OCSP という 2 つのチェック方法がサポートされています。

CRL および OCSP の追加設定を行うには、次の手順を実行します。

ステップ 1　[Configuration Options for CA Certificates] ペインで、[Advanced] タブをクリックします。

ステップ 2　[CRL Options] 領域で、キャッシュのリフレッシュを行う間隔を分数で入力します。デフォルトは 60 分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、適応型セキュリティ アプライアンス では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、適応型セキュリティ アプライアンスにより使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

ステップ 3　[Enforce next CRL update] チェックボックスをオンにして、Next Update 値の有効期限が切れていない CRL に限り、有効な CRL として使用できるようにします。[Enforce next CRL update] チェックボックスをオフにすると、Next Update 値がない場合や、Next Update 値の有効期限が切れている場合でも有効な CRL として使用できます。

ステップ 4　[OCSP Options] 領域で、OCSP サーバの URL を入力します。適応型セキュリティ アプライアンス で使用される OCSP サーバは、次の順に選択されます。

1. 一致証明書上書きルールの OCSP URL に対応するサーバ
2. 選択された [OCSP Options] 属性に設定した OCSP URL に対応するサーバ
3. リモート ユーザ証明書の AIA フィールドで指定されたサーバ

ステップ 5　デフォルトでは、[Disable nonce extension] チェックボックスがオンになっています。この設定では、暗号化によって要求を応答にバインドし、リプレイ アタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張を照合し、両者が同一であることを確認することで、リプレイ アタックを防ぐことができます。ただし、事前に生成した応答には、各要求と一致するナンス拡張は含まれていません。そのため、使用している OCSP サーバから、事前に生成した応答を送信する場合は、[Disable nonce extension] チェックボックスをオフにしてください。

ステップ 6　[Validation Policy] 領域で、次のオプションのいずれかを選択します。

- この CA を使用して検証できるリモート セッションのタイプを制限するには、[SSL] オプション ボタンまたは [IPsec] オプション ボタンをクリックします。
- いずれのタイプのセッションも CA で検証できるようにするには、[SSL and IPSec] オプション ボタンをクリックします。

ステップ 7　[Other Options] 領域で、次のオプションのいずれかを選択します。

- 指定した CA の証明書を 適応型セキュリティ アプライアンス で受け入れるようにするには、[Accept certificates issued by this CA] チェックボックスをオンにします。
- 下位 CA の証明書を 適応型セキュリティ アプライアンス で受け入れるようにするには、[Accept certificates issued by the subordinate CAs of this CA] チェックボックスをオンにします。

ステップ 8　[OK] をクリックしてこのタブを閉じ、[Apply] をクリックしてコンフィギュレーションの変更を保存します。

次の作業

「ID 証明書の認証の設定」（P.38-9）を参照してください。

ID 証明書の認証の設定

ID 証明書は、適応型セキュリティ アプライアンス 経由の VPN アクセスの認証に使用できます。[Identity Certificates Authentication] ペインでは、次のタスクを実行できます。

- 新しい ID 証明書を追加またはインポートする。
- ID 証明書の詳細を表示する。
- 既存の ID 証明書を削除する。
- 既存の ID 証明書をエクスポートする。
- 既存の ID 証明書をインストールする。
- Entrust に ID 証明書を登録する。

この項では、次のトピックについて取り上げます。

ID 証明書の追加またはインポート

新しい ID 証明書コンフィギュレーションを追加またはインポートするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Identity Certificates] の順に選択します。

ステップ 2　[Add] をクリックします。

選択されたトラストポイント名が上部に示された [Add Identity Certificate] ダイアログボックスが表示されます。

ステップ 3　既存のファイルから ID 証明書をインポートするには、[Import the identity certificate from a file] オプション ボタンをクリックします。

ステップ 4　PKCS12 ファイルの復号化に使用するパスフレーズを入力します。

ステップ 5　ファイルのパス名を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示します。証明書ファイルを見つけて、[Import ID Certificate File] をクリックします。

ステップ 6　新しい ID 証明書を追加するには、[Add a new identity certificate] オプション ボタンをクリックします。

ステップ 7　[New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。

ステップ 8　デフォルトのキー ペア名を使用する場合は、[Use default keypair name] オプション ボタンをクリックします。

ステップ 9　新しいキー ペア名を使用する場合は、[Enter a new key pair name] オプション ボタンをクリックし、新しい名前を入力します。適応型セキュリティ アプライアンスでは、複数のキー ペアをサポートします。

ステップ 10　ドロップダウン リストから係数サイズを選択します。

ステップ 11　[General purpose] オプション ボタン（デフォルト）または [Special] オプション ボタンをクリックして、キー ペアの用途を選択します。[Special] オプション ボタンを選択すると、適応型セキュリティ アプライアンス により署名用と暗号化用の 2 つのキー ペアが生成されます。この選択は、対応する識別用に 2 つの証明書が必要なことを示します。

ステップ 12　[Generate Now] をクリックして新しいキー ペアを作成し、[Show] をクリックして [Key Pair Details] ダイアログボックスを表示します。ここには、次の*表示専用*の情報が示されます。

- 公開キーが認証の対象となるキー ペアの名前。
- キー ペアの生成日時。
- RSA キー ペアの用途。
- キー ペアの係数サイズ（512、768、1024、および 2048 ビット）。デフォルト値は 1024 です。
- テキスト形式の特定のキー データを含むキー データ。

ステップ 13　完了したら [OK] をクリックして、[Key Pair Details] ダイアログボックスを閉じます。

ステップ 14　ID 証明書で DN を形成するための証明書サブジェクト DN を選択します。次に [Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 15　ドロップダウン リストから追加する DN 属性を 1 つ以上選択し、値を入力し、[Add] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- Common Name（CN）
- Department（OU）
- Company Name（O）
- Country（C）
- State/Province（ST）
- Location（L）
- E-mail Address（EA）

ステップ 16　完了したら [OK] をクリックして、[Certificate Subject DN] ダイアログボックスを閉じます。

ステップ 17　自己署名証明書を作成するには、[Generate self-signed certificate] チェックボックスをオンにします。

ステップ 18　ID 証明書がローカル CA として動作するようにするには、[Act as local certificate authority and issue dynamic certificates to TLS proxy] チェックボックスをオンにします。

ステップ 19　追加の ID 証明書設定を行うには、[Advanced] をクリックします。

[Certificate Parameters]、[Enrollment Mode]、および [SCEP Challenge Password] の 3 つのタブを持つ [Advanced Options] ダイアログボックスが表示されます。

（注）　登録モード設定と SCEP チャレンジ パスワードは自己署名証明書では使用できません。

ステップ 20　[Certificate Parameters] タブをクリックし、次の情報を入力します。

- DNS ツリー階層内のノードの位置を示す FQDN（完全修飾ドメイン名）。
- ID 証明書に関連付けられている電子メール アドレス。
- 4 分割ドット付き 10 進表記の、ネットワーク上の 適応型セキュリティ アプライアンス IP アドレスです。

- 適応型セキュリティ アプライアンス シリアル番号を証明書パラメータに追加するには、[Include serial number of the device] チェックボックスをオンにします。

ステップ 21　[Enrollment Mode] タブをクリックし、次の情報を入力します。

- [Request by manual enrollment] オプション ボタンまたは [Request from a CA] オプション ボタンをクリックして、登録方式を選択します。
- SCEP を介して自動的にインストールされる証明書の登録 URL。
- ID 証明書のインストールに許可される最大再試行分数。デフォルトは 1 分です。
- ID 証明書のインストールに許可される最大再試行回数。デフォルトは 0 です。この場合は、再試行時間内であれば何度でも再試行できます。

ステップ 22　[SCEP Challenge Password] タブをクリックし、次の情報を入力します。

- SCEP パスワード
- SCEP パスワードを確認のために再入力

ステップ 23　完了したら [OK] をクリックして、[Advanced Options] ダイアログボックスを閉じます。

ステップ 24　[Add Identity Certificate] ペインで、[Add Certificate] をクリックします。

[Identity Certificates] リストに新しい ID 証明書が表示されます。

ステップ 25　[Apply] をクリックし、新しい ID 証明書コンフィギュレーションを保存します。

ID 証明書の詳細の表示

選択した ID 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの*表示専用タブ*が含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

ID 証明書の削除

ID 証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

（注）　証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

ID 証明書のエクスポート

証明書コンフィギュレーションおよび関連付けられているすべてのキーと証明書を、公開キーの暗号化標準である PKCS12 形式でエクスポートできます。これには、base64 エンコードまたは 16 進数形式を使用できます。完全なコンフィギュレーションには、チェーン全体（ルート CA 証明書、ID 証明書、キー ペア）は含まれますが、登録設定（サブジェクト名、FQDN など）は含まれません。通常、この機能は、同じグループ内の適応型セキュリティ アプライアンス間で証明書を複製するために行うフェールオーバーまたはロードバランシングの設定に使用されます。たとえば、リモート アクセス クライアントから中央処理装置への呼び出しが複数のユニットで処理されている場合、これらのユニット間では、証明書コンフィギュレーションが同一であることが必要となります。このような場合、管理者は、証明書コンフィギュレーションをエクスポートしたうえで、適応型セキュリティ アプライアンスのグループ全体にインポートできます。

ID 証明書をエクスポートするには、次の手順を実行します。

ステップ 1　[Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。

ステップ 2　証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。または、[Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。

ステップ 3　[PKCS12 Format] オプション ボタンまたは [PEM Format] オプション ボタンをクリックして、証明書の形式を選択します。

ステップ 4　PKCS12 ファイルをエクスポート用に暗号化するために使用するパスフレーズを入力します。

ステップ 5　暗号化パスフレーズを確認のために再入力します。

ステップ 6　[Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

情報ダイアログボックスが表示され、証明書コンフィギュレーション ファイルが指定の場所に正常にエクスポートされたことが示されます。

証明書署名要求の生成

（注）　Entrust がサポートしているのは、モジュラスのサイズが 1024 のキー*だけ*です。それ以外のキーを使用している場合は、Entrust にお問い合わせください。

Entrust に送信する証明書署名要求を生成するには、次の手順を実行します。

ステップ 1　[Enroll ASA SSL VPN with Entrust] をクリックして、[Generate Certificate Signing Request] ダイアログボックスを表示します。

ステップ 2　[Key Pair] 領域で、次の手順を実行します。

a.　ドロップダウン リストから、設定されたキー ペアのいずれかを選択します。

b.　[Show] をクリックして [Key Details] ダイアログボックスを表示します。ここには、選択されたキー ペアの生成日時、用途（一般的または特殊な用途）、係数サイズ、およびキー データといった情報が示されます。

c.　完了したら [OK] をクリックして、[Key Details] ダイアログボックスを閉じます。

d. [New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。以降の手順については、「ID 証明書の追加またはインポート」（P.38-9）の手順 8 に進みます。生成したキー ペアは 適応型セキュリティ アプライアンス に送信するか、ファイルに保存できます。

ステップ 3　[Certificate Subject DN] 領域で、次の情報を入力します。

a. 適応型セキュリティ アプライアンス の FQDN または IP アドレス。

b. 会社の名前。

c. 2 文字の国番号。

ステップ 4　[Optional Parameters] 領域で、次の手順を実行します。

a. [Select] をクリックして、[Additional DN Attributes] ダイアログボックスを表示します。

b. ドロップダウン リストから追加する属性を選択し、値を入力します。

c. [Add] をクリックして、各属性を [attribute] テーブルに追加します。

d. [Delete] をクリックして、[attribute] テーブルから属性を削除します。

e. 完了したら [OK] をクリックして、[Additional DN Attributes] ダイアログボックスを閉じます。

[Additional DN Attributes] フィールドに追加された属性が表示されます。

ステップ 5　CA から要求された場合は、完全修飾ドメイン名情報を追加で入力します。

ステップ 6　[Generate Request] をクリックして、証明書署名要求を生成します。生成した証明書署名要求については、Entrust に送信するか、ファイルに保存するか、または後で送信するかを選択できます。

CSR が示された [Enroll with Entrust] ダイアログボックスが表示されます。

ステップ 7　登録プロセスを完了するには、http://www.entrust.net/cisco/ にある [request a certificate from Entrust] リンクをクリックします。その際、示された CSR をコピーして貼り付け、それを Entrust Web フォームを使用して送信します。後で登録する場合は、生成された CSR をファイルに保存し、[Identity Certificates] ペインの [enroll with Entrust] リンクをクリックして登録プロセスを完了します。

ステップ 8　Entrust により、要求の認証が確認された後、証明書が発行されます。これには数日間かかる場合があります。次に、[Identity Certificate] ペインで保留中の要求を選択し、[Install] をクリックして、証明書をインストールする必要があります。[Close] をクリックして、[Enroll with Entrust] ダイアログボックスを閉じます。

アイデンティティ証明書のインストール

[Identity Certificates] ペインの [Install] ボタンは、保留中の登録がない場合はグレー表示されます。適応型セキュリティ アプライアンス が CSR を受信した場合は必ず、[Identity Certificates] ペインに保留中の ID 証明書が表示されます。保留中の ID 証明書を選択すると、[Install] ボタンがアクティブになります。

保留中の要求を CA に転送すると、CA はそのファイルを登録して証明書を 適応型セキュリティ アプライアンス に返します。証明書を受信したら、[Install] をクリックし、該当する ID 証明書を選択して操作を完了します。

保留中の ID 証明書をインストールするには、次の手順を実行します。

ステップ 1　[Identity Certificates] ペインで、[Add] をクリックし、[Add Identity Certificate] ダイアログボックスを表示します。

ステップ 2　[Add Identity Certificate] ダイアログボックスで、[Add a new identity certificate] オプション ボタンをクリックします。

ステップ 3　（任意）キー ペアを変更するか、新しいキー ペアを作成します。キー ペアは必須です。

ステップ 4　[Certificate Subject DN] に情報を入力し、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 5　関係する CA で必要なサブジェクト DN 属性をすべて指定し、[OK] をクリックして [Certificate Subject DN] ダイアログボックスを閉じます。

ステップ 6　[Add Identity Certificate] ダイアログボックスで、[Advanced] をクリックして [Advanced Options] ダイアログボックスを表示します。

ステップ 7　以降の手順については、「ID 証明書の認証の設定」（P.38-9）の手順 17 ～ 23 を参照してください。

ステップ 8　[Add Identity Certificate] ダイアログボックスで、[Add Certificate] をクリックします。

[Identity Certificate Request] ダイアログボックスが表示されます。

ステップ 9　テキスト タイプの CSR ファイル名（c:\verisign-csr.txt など）を入力し、[OK] をクリックします。

ステップ 10　CSR テキスト ファイルを CA に送信します。送信する代わりに、CA の Web サイトにある CSR 登録ページにテキスト ファイルを貼り付けることもできます。

ステップ 11　CA から ID 証明書が返されたら、[Identity Certificates] ペインに移動し、保留中の証明書エントリを選択して、[Install] をクリックします。

[Install Identity Certificate] ダイアログボックスが表示されます。

ステップ 12　該当するオプション ボタンをクリックして、次のいずれかのオプションを選択します。

- Install from a file

  または、[Browse] をクリックし、ファイルを検索します。
- Paste the certificate data in base-64 format

  コピーした証明書データを指定された領域に貼り付けます。

ステップ 13　[Install Certificate] をクリックします。

ステップ 14　[Apply] をクリックし、新しくインストールした証明書とその 適応型セキュリティ アプライアンス コンフィギュレーションを保存します。

次の作業

「コード署名者証明書の設定」（P.38-14）を参照してください。

コード署名者証明書の設定

コード署名により、デジタル署名が、実際の実行可能なコードに追加されます。このデジタル署名には、署名者を認証し、署名以降にそのコードが変更されていないことを保証するのに十分な情報が含まれています。

コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードが証明書の発生元を示します。[Code Signer] ペインで、または [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Java Code Signer] を選択して、コード署名者証明書をインポートできます。

[Code Signer] ペインでは、次のタスクを実行できます。

- コード署名者証明書の詳細を表示する。

- 既存のコード署名者証明書を削除する。
- 既存のコード署名者証明書をインポートする。
- 既存のコード署名者証明書をエクスポートする。
- Entrust にコード署名者証明書を登録する。

この項では、次のトピックについて取り上げます。

コード署名者証明書の詳細の表示

選択した ID 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの*表示専用タブ*が含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

コード署名者証明書の削除

コード署名者証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

（注） 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Import] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

コード署名者証明書のインポート

コード署名者証明書をインポートするには、次の手順を実行します。

ステップ 1　[Code Signer] ペインで、[Import] をクリックし、[Import Certificate] ダイアログボックスを表示します。

ステップ 2　PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。

ステップ 3　インポートするファイルの名前を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示し、ファイルを検索します。

ステップ 4　インポートするファイルを選択し、[Import ID Certificate File] をクリックします。

[Import Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。

ステップ 5　[Import Certificate] をクリックします。

[Code Signer] ペインにインポートされた証明書が表示されます。

ステップ 6　[Apply] をクリックし、新しくインポートしたコード署名者証明書コンフィギュレーションを保存します。

コード署名者証明書のエクスポート

コード署名者証明書をエクスポートするには、次の手順を実行します。

ステップ 1　[Code Signer] ペインで、[Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。

ステップ 2　証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。

ステップ 3　公開キー暗号化標準（base64 エンコードまたは 16 進数形式を使用できます）を使用するには、[Certificate Format] 領域で [PKCS12 format] オプション ボタンをクリックします。使用しない場合は、[PEM format] オプション ボタンをクリックします。

ステップ 4　[Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。

ステップ 5　ファイルを選択し、[Export ID Certificate File] をクリックします。

[Export Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。

ステップ 6　エクスポート用の PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。

ステップ 7　復号化パスフレーズを確認のために再入力します。

ステップ 8　[Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

次の作業

「ローカル CA を使用した認証」（P.38-16）を参照してください。

ローカル CA を使用した認証

ブラウザベースおよびクライアントベースの SSL VPN 接続では、ローカル CA により実現される、適応型セキュリティ アプライアンス 上に存在するセキュアで設定可能な内部認証局によって、証明書の認証を行うことができます。

ユーザの登録は、指定された Web サイトにログインすることによって行われます。ローカル CA は、適応型セキュリティ アプライアンス の基本認証局の動作を統合したもので、証明書の配布と、発行された証明書に対するセキュアな失効チェックを行います。

ローカル CA を使用すると、次のタスクを実行できます。

- ローカル CA サーバを設定する。
- ローカル CA 証明書の失効/失効解除を行う。

- CRL を更新する。
- ローカル CA ユーザを追加、編集、および削除する。

この項では、次のトピックについて取り上げます。

- 「ローカル CA サーバの設定」（P.38-17）
- 「ローカル CA サーバの削除」（P.38-20）

ローカル CA サーバの設定

適応型セキュリティ アプライアンス でローカル CA サーバを設定するには、次の手順を実行します。

ステップ 1　[CA Server] ペインで、ローカル CA サーバをアクティブにするには、[Enable] オプション ボタンをクリックします。デフォルトではディセーブルになっています。ローカル CA サーバをイネーブルにすると、適応型セキュリティ アプライアンスによりローカル CA サーバ証明書、キー ペア、および必要なデータベース ファイルが生成され、ローカル CA サーバ証明書とキー ペアが PKCS12 ファイルにアーカイブされます。

（注）　設定済みのローカル CA をイネーブルにする前に、オプションのすべての設定を慎重に見直してください。イネーブルにした後で、証明書の発行者名とキー サイズ サーバ値を変更することはできません。

自己署名した証明書のキーの使用拡張により、キー暗号化、キー シグニチャ、CRL 署名、および証明書署名がイネーブルになります。

ステップ 2　ローカル CA を初めてイネーブルにするときには、英数字のイネーブル パスフレーズを指定する必要があります。イネーブル パスフレーズは、7 文字以上の英数字である必要があります。このパスフレーズにより、ストレージにアーカイブされたローカル CA 証明書およびローカル CA 証明書のキー ペアが保護され、不正なシャットダウンや予期しないシャットダウンが発生しないようにローカル CA サーバが保護されます。ローカル CA 証明書またはキー ペアが失われ、その復元が必要となった場合、PKCS12 アーカイブのロックを解除するためには、このパスフレーズが必要です。

（注）　ローカル CA サーバをイネーブルにするには、イネーブル パスフレーズが必要です。イネーブル パスフレーズの記録は、必ず安全な場所に保管してください。

ステップ 3　適応型セキュリティ アプライアンス をリブートしてもコンフィギュレーションが失われないように、[Apply] をクリックして、ローカル CA 証明書とキー ペアを保存します。

ステップ 4　ローカル CA の初回設定後にローカル CA を変更または再設定する場合は、[Disable] オプション ボタンをクリックして、適応型セキュリティ アプライアンス上のローカル CA サーバをシャットダウンする必要があります。この状態では、コンフィギュレーションおよびすべての関連ファイルはストレージ内に保持され、登録はディセーブルになっています。

設定したローカル CA がイネーブルになると、次の 2 つの設定が*表示専用*になります。

- [Issuer Name] フィールド。発行元のサブジェクト名とドメイン名がリストで示されます。これは、ユーザ名とサブジェクト名のデフォルト DN 設定により構成され、cn=FQDN という形式で示されます。ローカル CA サーバは、証明書を付与するエンティティです。証明書のデフォルト名は、cn=hostname.domainname という形式で表示されます。

- [CA Server Key Size] 設定。これは、ローカル CA サーバに生成されるサーバ証明書を対象とします。キー サイズには、キーごとに 512、768、1024、または 2048 ビットのいずれかを指定できます。デフォルトは、1 つのキーあたり 1024 ビットです。

ステップ 5　ドロップダウン リストから、ローカル CA サーバが発行した各ユーザ証明書に対して生成されるキーペアのクライアント キー サイズを選択します。キー サイズには、キーごとに 512、768、1024、または 2048 ビットのいずれかを指定できます。デフォルトは、1 つのキーあたり 1024 ビットです。

ステップ 6　CA 証明書のライフタイム値を入力します。これは、CA サーバ証明書の有効期間を日数単位で指定するものです。デフォルトは、3650 日（10 年）です。

ローカル CA サーバでは、CA 証明書の期限が切れる 30 日前に後継の CA 証明書が自動的に生成されます。この証明書をエクスポートし、他のデバイスにインポートすることにより、ローカル CA が発行したユーザ証明書のローカル CA 証明書検証を、期限が切れた後に行うことができます。

期限切れが近付いていることをユーザに通知するために、次の syslog メッセージが [ASDM Syslog Messages] ペインに表示されます。

```
%ASA-1-717049: Local CA Server certificate is due to expire in days and a replacement
certificate is available for export.
```

（注）　この自動ロールオーバーが通知されたら、管理者は、新しいローカル CA 証明書が有効期限の前に必要なすべてのデバイスにインポートされるようにする必要があります。

ステップ 7　クライアント証明書のライフタイム値を入力します。これは、CA サーバが発行したユーザ証明書の有効期間を日数単位で指定するものです。デフォルトは 365 日（1 年）です。

[SMTP Server & Email Settings] 領域で、次の設定を指定して、ローカル CA サーバに対する電子メール アクセスを設定します。

a.　SMTP メール サーバ名または IP アドレスを入力します。または、省略符号（[...]）をクリックして [Browse Server Name/IP Address] ダイアログボックスを表示し、ここからサーバ名または IP アドレスを選択します。完了したら [OK] をクリックして、[Browse Server Name/IP Address] ダイアログボックスを閉じます。

b.　ローカル CA ユーザに電子メール メッセージを送信する際に使用する From アドレスを adminname@host.com という形式で入力します。自動電子メール メッセージは、新規登録ユーザへのワンタイム パスワードの送信や、証明書の更新が必要なときの電子メール メッセージの発行に使用されます。

c.　ローカル CA サーバからユーザに送信されるすべてのメッセージで使用される件名を入力します。件名を指定しない場合のデフォルトは「Certificate Enrollment Invitation」です。

ステップ 8　その他のオプションを設定するには、[More Options] ドロップダウン矢印をクリックします。

ステップ 9　CRL 分散ポイント（適応型セキュリティ アプライアンス 上の CRL の場所）を入力します。デフォルトの場所は、http://hostname.domain/+CSCOCA+/asa_ca.crl です。

ステップ 10　特定のインターフェイスおよびポートで、CRL に HTTP ダウンロードできるようにするには、ドロップダウン リストから publish-CRL インターフェイスを選択します。次に、1 ～ 65535 の任意のポート番号を入力します。デフォルトのポート番号は TCP ポート 80 です。

（注）　CRL の名前は変更できません。LOCAL-CA-SERVER.crl という名前が常に使用されます。

たとえば、http://10.10.10.100/user8/my_crl_file という URL を入力します。この場合、指定された IP アドレスを持つインターフェイスのみが動作します。要求を受信すると、適応型セキュリティ アプライアンス によってパス /user8/my_crl_file と設定済み URL が照合されます。パスが一致すると、適応型セキュリティ アプライアンスから、保存されている CRL ファイルが返されます。

ステップ 11　CRL の有効期間である CRL ライフタイムを時間単位で入力します。CA 証明書のデフォルトは 6 時間です。

ローカル CA では、ユーザ証明書が失効するたびまたは失効解除されるたびに、更新された CRL が再発行されますが、失効状態に変更がない場合、CRL の再発行は、そのライフタイムの中で 1 回しか行われません。[CA Certificates] ペインで [Request CRL] をクリックすると、CRL を即時に更新して再生成できます。

ステップ 12　データベース ストレージの場所を入力して、ローカル CA コンフィギュレーションとデータ ファイル用のストレージ領域を指定します。適応型セキュリティ アプライアンスでは、ユーザ情報、発行済み証明書、および失効リストへのアクセスと実装にローカル CA データベースが使用されます。外部ファイルを指定する場合は、外部ファイルへのパス名を入力するか、[Browse] をクリックして [Database Storage Location] ダイアログボックスを表示します。

ステップ 13　表示されるフォルダのリストからストレージの場所を選択し、[OK] をクリックします。

（注）　フラッシュ メモリには、3500 人以下のユーザを持つデータベースを保存できます。ユーザの数がそれを超えるデータベースでは外部ストレージが必要になります。

ステップ 14　発行された証明書のユーザ名に追加されるデフォルト サブジェクト（DN 文字列）を入力します。次に示す DN 属性を指定できます。

- CN（一般名）
- SN（姓名の姓）
- O（組織名）
- L（地名）
- C（国）
- OU（組織ユニット）
- EA（電子メール アドレス）
- ST（州 / 都道府県）
- T（タイトル）

ステップ 15　登録されたユーザがユーザ証明書を登録および取得するための PKCS12 登録ファイルを取得できる期間を、時間単位で入力します。この登録期間は、ワンタイム パスワードの有効期間とは関係ありません。デフォルトは 24 時間です。

（注）　ローカル CA の証明書の登録は、クライアントレス SSL VPN 接続でのみサポートされます。このタイプの接続の場合、クライアントと 適応型セキュリティ アプライアンス の通信は、標準の HTML を使用して Web ブラウザ経由で行われます。

ステップ 16　登録ユーザに電子メールで送信されたワンタイム パスワードの有効期間を入力します。デフォルトは 72 時間です。

ステップ 17　期限の何日前になったら、ユーザに期限切れ通知の電子メールを送信するかを入力します。デフォルトは、14 日です。

ステップ 18　[Apply] をクリックし、新しいまたは変更された CA 証明書コンフィギュレーションを保存します。変更を破棄して元の設定に戻す場合は、[Reset] をクリックします。

ローカル CA サーバの削除

適応型セキュリティ アプライアンス からローカル CA サーバを削除するには、次の手順を実行します。

ステップ 1　[CA Server] ペインで、[Delete Certificate Authority Server] をクリックします。

[Delete Certificate Authority] ダイアログボックスが表示されます。

ステップ 2　CA サーバを削除する場合は、[OK] をクリックします。CA サーバを保持する場合は、[Cancel] をクリックします。

（注）　削除したローカル CA サーバは、復元および復旧できません。削除した CA サーバ コンフィギュレーションを再作成する場合は、CA サーバ コンフィギュレーション情報をすべて再入力する必要があります。

次の作業

「ユーザ データベースの管理」（P.38-20）を参照してください。

ユーザ データベースの管理

ローカル CA ユーザ データベースには、ユーザ識別情報とユーザ ステータス（登録済み、許可、失効など）が格納されています。[Manage User Database] ペインでは、次のタスクを実行できます。

- ローカル CA データベースにユーザを追加する。
- 既存のユーザ識別情報を変更する。
- ローカル CA データベースからユーザを削除する。
- ユーザを登録する。
- CRL を更新する。
- ユーザに OTP を電子メールで送信する。
- OTP を表示または再生成（置換）する。

この項では、次のトピックについて取り上げます。

ローカル CA ユーザの追加

ローカル CA ユーザを追加するには、次の手順を実行します。

ステップ 1　新しいユーザをローカル CA データベースに追加するには、[Add] をクリックして、[Add User] ダイアログボックスを表示します。

ステップ 2　有効なユーザ名を入力します。

ステップ 3　既存の有効な電子メール アドレスを入力します。

ステップ 4　サブジェクト（DN 文字列）を入力します。または、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 5　ドロップダウン リストから追加する DN 属性を 1 つ以上選択し、値を入力し、[Add] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- Common Name（CN）
- Department（OU）
- Company Name（O）
- Country（C）
- State/Province（ST）
- Location（L）
- E-mail Address（EA）

ステップ 6　完了したら [OK] をクリックして、[Certificate Subject DN] ダイアログボックスを閉じます。

ステップ 7　[Allow enrollment] チェックボックスをオンにしてユーザを登録し、[Add User] をクリックします。

[Manage User Database] ペインに新しいユーザが表示されます。

最初の OTP の送信または OTP の置換

新規追加されたユーザに対して、一意の OTP とローカル CA 登録 URL が記載された登録許可の電子メール通知を自動的に送信するには、[Email OTP] をクリックします。

OTP が新規ユーザに送信されたことを示す [Information] ダイアログボックスが表示されます。

自動的に新しい OTP を再発行して、新しいパスワードが記載された電子メール通知を既存のユーザまたは新規ユーザに送信するには、[Replace OTP] をクリックします。

ローカル CA ユーザの編集

データベース内の既存のローカル CA ユーザに関する情報を変更するには、次の手順を実行します。

ステップ 1　特定のユーザを選択し、[Edit] をクリックして [Edit User] ダイアログボックスを表示します。

ステップ 2　有効なユーザ名を入力します。

ステップ 3　既存の有効な電子メール アドレスを入力します。

ステップ 4　サブジェクト（DN 文字列）を入力します。または、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 5　ドロップダウン リストから変更する DN 属性を 1 つ以上選択し、値を入力し、[Add] または [Delete] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- Common Name（CN）
- Department（OU）
- Company Name（O）
- Country（C）
- State/Province（ST）
- Location（L）
- E-mail Address（EA）

ステップ 6　完了したら [OK] をクリックして、[Certificate Subject DN] ダイアログボックスを閉じます。

ステップ 7　[Allow enrollment] チェックボックスをオンにしてユーザを再登録し、[Edit User] をクリックします。

[Manage User Database] ペインに更新されたユーザ詳細が表示されます。

ローカル CA ユーザの削除

ユーザをデータベースから削除し、そのユーザに発行されたすべての証明書をローカル CA データベースから削除するには、ユーザを選択し、[Delete] をクリックします。

（注）　削除されたユーザは復元できません。削除したユーザ レコードを再作成するには、[Add] をクリックして、そのユーザの情報をすべて再入力します。

ユーザ登録の許可

選択したユーザを登録するには、[Allow Enrollment] をクリックします。

[Manage User Database] ペインに示されるユーザのステータスが [enrolled] に変わります。

（注）　ユーザがすでに登録されている場合は、エラー メッセージが表示されます。

OTP の表示または再生成

選択したユーザの OTP を表示または再生成するには、次の手順を実行します。

ステップ 1　[View/Regenerate OTP] をクリックして、[View & Regenerate OTP] ダイアログボックスを表示します。

現在の OTP が表示されます。

ステップ 2　完了したら [OK] をクリックし、[View & Regenerate OTP] ダイアログボックスを閉じます。

ステップ 3　OTP を再生成するには、[Regenerate OTP] をクリックします。

新しく生成された OTP が表示されます。

ステップ 4　[OK] をクリックして、[View & Regenerate OTP] ダイアログボックスを閉じます。

次の作業

「ユーザ証明書の管理」（P.38-23）を参照してください。

ユーザ証明書の管理

証明書のステータスを変更するには、次の手順を実行します。

ステップ 1　[Manage User Certificates] ペインで、ユーザ名または証明書のシリアル番号で特定の証明書を選択します。

ステップ 2　次のいずれかのオプションを選択します。

- ユーザ証明書のライフタイムが期限切れになった場合は、ユーザのアクセス権を削除するために、[Revoke] をクリックします。また、ローカル CA により、証明書データベース内にあるその証明書に失効のマークが付けられ、情報が自動的に更新されて、CRL が再発行されます。
- アクセス権を復元するには、ユーザの失効した証明書を選択して、[Unrevoke] をクリックします。また、ローカル CA により、証明書データベース内にあるその証明書に失効解除のマークが付けられ、証明書の情報が自動的に更新された後、更新された CRL が再発行されます。

ステップ 3　完了したら [Apply] をクリックして、変更を保存します。

次の作業

「CRL のモニタリング」（P.38-23）を参照してください。

CRL のモニタリング

CRL をモニタするには、次の手順を実行します。

ステップ 1　ASDM メイン アプリケーション ウィンドウで、[Monitoring] > [Properties] > [CRL] の順に選択します。

ステップ 2　[CRL] 領域で、ドロップダウン リストから CA 証明書名を選択します。

ステップ 3　CRL の詳細を表示するには、[View CRL] をクリックします。次に例を示します。

```
CRL Issuer Name:
    cn=asa4.cisco.com
    LastUpdate: 09:58:34 UTC Nov 11 2009
    NextUpdate: 15:58:34 UTC Nov 11 2009
    Cached Until: 15:58:34 UTC Nov 11 2009
    Retrieved from CRL Distribution Point:
      ** CDP Not Published - Retrieved via SCEP
    Size (bytes): 224
    Associated Trustpoints: LOCAL-CA-SERVER
```

ステップ 4　完了したら [Clear CRL] をクリックして CRL の詳細を削除し、表示する別の CA 証明書を選択します。

証明書管理の機能履歴

表 38-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 38-1　証明書管理の機能履歴

機能名	プラットフォーム リリース	機能情報
Certificate Management	7.0(1)	デジタル証明書（CA 証明書、ID 証明書、およびコード署名者証明書など）は、認証用のデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。 次のパスが、使用される VPN 接続の種類に基づいて導入されました。 • [Configuration] > [Remote Access VPN] > [Certificate Management] • [Configuration] > [Site-to-Site VPN] > [Certificate Management]。

CHAPTER 39

IPS の設定

この章では、適応型セキュリティ アプライアンスにインストールされている AIP SSM をサポートするように適応型セキュリティ アプライアンスを設定する方法について説明します。

（注） Cisco PIX 500 シリーズ セキュリティ アプライアンスは、SSM をサポートしていません。

この章は、次の項で構成されています。

AIP SSM の概要

ASA 5500 シリーズ適応型セキュリティ アプライアンスに AIP SSM をインストールできます。AIP SSM は、予防的なフル機能の侵入防御サービスを提供する高度な IPS ソフトウェアを実行し、ワームやネットワーク ウイルスなどの悪意のあるトラフィックがネットワークに影響を与える前に、これらを阻止します。この項では、次のトピックについて取り上げます。

適応型セキュリティ アプライアンスとの AIP SSM の動作

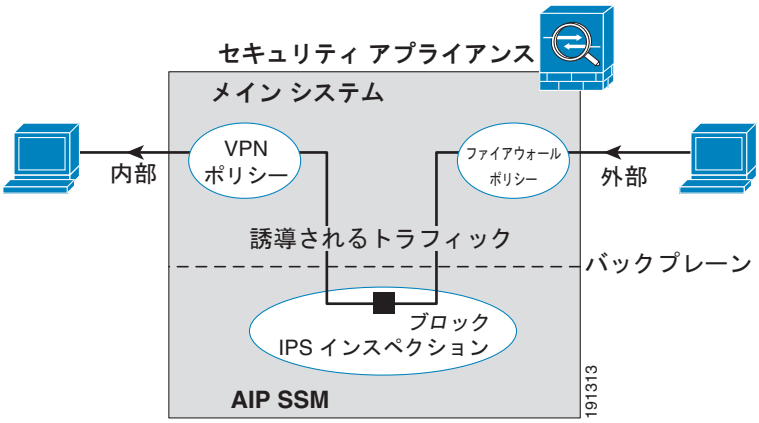
AIP SSM は、適応型セキュリティ アプライアンスとは別のアプリケーションを実行します。ただし、アプリケーションは適応型セキュリティ アプライアンスのトラフィック フローに統合されています。AIP SSM には、管理インターフェイス以外に外部インターフェイス自体は含まれていません。IPS 検査のため適応型セキュリティ アプライアンスでトラフィックを指定する場合、トラフィックは適応型セキュリティ アプライアンスと AIP SSM を通して次のように流れます。

1. トラフィックが適応型セキュリティ アプライアンスに入ります。
2. ファイアウォール ポリシーが適用されます。
3. バックプレーンからトラフィックが AIP SSM に送信されます。

   トラフィックのコピーの AIP SSM への送信だけについては、「動作モード」（P.39-2）を参照してください。
4. AIP SSM が、セキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
5. 有効なトラフィックがバックプレーン経由で適応型セキュリティ アプライアンスに返送されます。AIP SSM が、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、そのトラフィックは渡されません。
6. VPN ポリシーが適用されます（設定されている場合）。
7. トラフィックが適応型セキュリティ アプライアンスを終了します。

図 39-1 は、AIP SSM をインライン モードで動作している場合のトラフィック フローを示します。この例では、AIP SSM は攻撃と見なしたトラフィックを自動的にブロックしています。それ以外のトラフィックは、セキュリティ アプライアンスを通って転送されます。

図 39-1　適応型セキュリティ アプライアンスの AIP SSM トラフィック フロー：インライン モード



動作モード

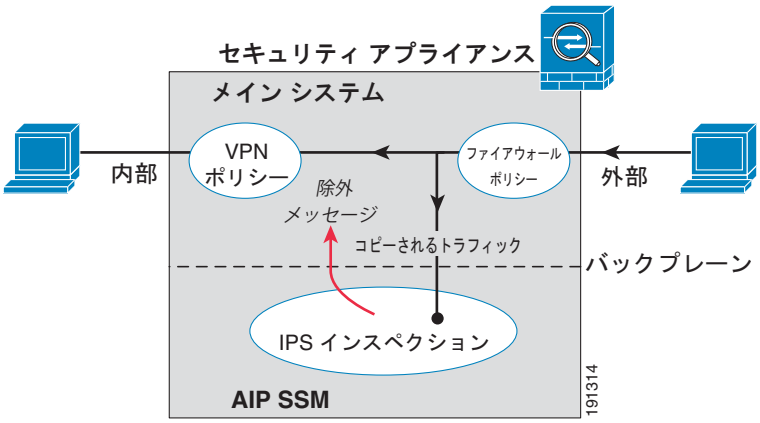
次のいずれかのモードを使用して、トラフィックを AIP SSM に送信できます。

- インライン モード：このモードでは、AIP SSM はトラフィック フローに直接配置されます（図 39-1 を参照）。IPS 検査に指定したトラフィックがセキュリティ アプライアンスを経由するには、まず AIP SSM を通り、その検査を受ける必要があります。インスペクション対象と識別され

たすべてのパケットは通過する前に分析されるため、このモードは最もセキュアです。また、AIP SSM では、パケットごとにブロッキング ポリシーを実装できます。ただし、このモードは、スループットに影響を与えることがあります。

- 無差別モード：このモードでは、トラフィックの重複したストリームが AIP SSM に送信されます。このモードは安全性では劣りますが、トラフィックのスループットにほとんど影響を与えません。インライン モードとは異なり、無差別モードでは、AIP SSM はセキュリティ アプライアンスにトラフィックを回避するか、セキュリティ アプライアンスへの接続をリセットするよう指示することでだけ、トラフィックをブロックできます。また、AIP SSM がトラフィックを分析している間、AIP SSM がトラフィックを回避する前に少量のトラフィックがセキュリティ アプライアンスを通過する場合があります。図 39-2 は無差別モードの AIP SSM を示しています。この例では、AIP SSM は脅威として指定されたトラフィックに対してセキュリティ アプライアンスに回避メッセージを送信します。

図 39-2　適応型セキュリティ アプライアンスの AIP SSM トラフィック フロー：無差別モード



仮想センサーの使用

IPS ソフトウェア バージョン 6.0 以降を実行している AIP SSM は複数の仮想センサーを実行できます。つまり、AIP SSM で複数のセキュリティ ポリシーを設定できます。各コンテキストまたはシングル モードセキュリティ アプライアンスを 1 つまたは複数の仮想センサーに割り当てる、または複数のセキュリティ コンテキストを同じ仮想センサーに割り当てることができます。仮想センターの詳細（サポートされている最大センサー数など）については、IPS のマニュアルを参照してください。

図 39-3 では、1 つのセキュリティ コンテキストと 1 つの仮想センター（インライン モード）がペアになり、2 つのセキュリティ コンテキストが同じ仮想センサーを共有しています。

図 39-3　セキュリティ コンテキストと仮想センサー

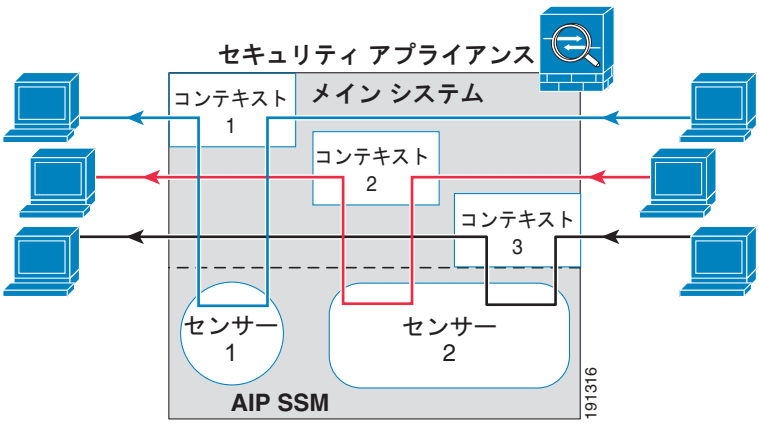
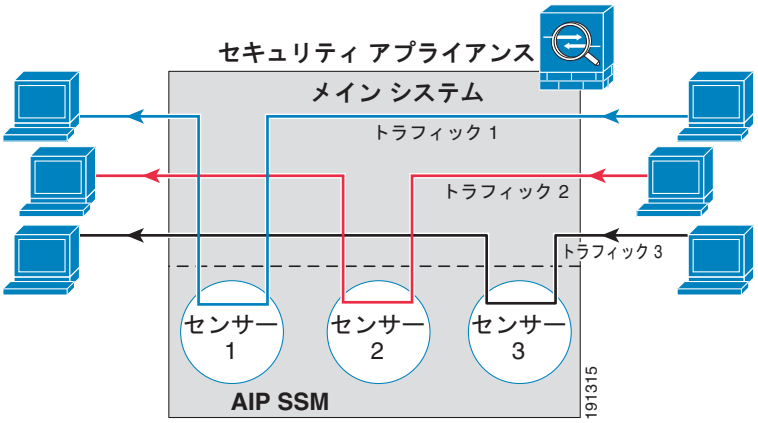


図 39-4 では、シングル モードのセキュリティ アプライアンスが複数の仮想センサー（インライン モード）とペアになっています。定義されている各トラフィック フローは異なるセンサーに進みます。

図 39-4　複数の仮想センサーがあるシングルモードのセキュリティ アプライアンス



AIP SSM 手順の概要

AIP SSM の設定は、AIP SSM を設定してから ASA 5500 シリーズ適応型セキュリティ アプライアンスを設定するプロセスです。

1. ASDM から IDM を起動します。「ASDM からの IDM へのアクセス」（P.39-5）を参照してください。ASDM では、IDM を使用して AIP SSM を設定します。
2. IDM で、インスペクションおよび保護ポリシーを設定します。このポリシーにより、トラフィックの検査方法と侵入が検出された場合の処理が決まります。マルチ センサー モードで AIP SSM を実行する場合は、各仮想センサーに対して検査および保護ポリシーを設定します。「IDM での AIP SSM セキュリティ ポリシーの設定」（P.39-5）を参照してください。
3. マルチ コンテキスト モードで ASA 5500 シリーズ適応型セキュリティ アプライアンスの ASDM を使用して、各コンテキストに使用できる IPS 仮想センサーを指定します（仮想センサーを設定した場合）。「仮想センサーのセキュリティ コンテンツへの割り当て」（P.39-5）を参照してください。

4. ASA 5500 シリーズ適応型セキュリティ アプライアンスの ASDM を使用して、AIP SSM に転送するトラフィックを指定します。「トラフィックの AIP SSM への転送」（P.39-6）を参照してください。

ASDM からの IDM へのアクセス

ASDM では、IDM を使用して AIP SSM を設定します。AIP SSM で IPS バージョン 6.0 以降を実行している場合、ASDM は AIP SSM から IDM を取得して、IDM を ASDM インターフェイスの一部として表示します。IPS ソフトウェアの以前のバージョンでは、IDM は別のブラウザ ウィンドウで起動します。

ASDM から IDM にアクセスするには、[Configuration] > [IPS] をクリックします。

AIP SSM の IP アドレスまたはホスト名の入力を要求されます。

- AIP SSM で IPS バージョン 6.0 以降を実行している場合、ASDM は AIP SSM から IDM を取得して、IDM を ASDM インターフェイスの一部として表示します。AIP SSM のパスワードを入力して [OK] をクリックします。

  ASDM ウィンドウに [IDM] ペインが表示されます。

- AIP SSM が以前のバージョンの IPS ソフトウェアを実行していると、ASDM に IDM へのリンクが表示されます。リンクをクリックして、新しいブラウザ ウィンドウで IDM を起動します。IDM にアクセスするには、ユーザ名とパスワードを入力する必要があります。

IDM にアクセスするためのパスワードがわからない場合は、ASDM を使用してパスワードをリセットできます。詳細については、「AIP SSM パスワードのリセット」（P.39-8）を参照してください。

IDM での AIP SSM セキュリティ ポリシーの設定

AIP SSM で、検査および保護ポリシーを設定します。これにより、トラフィックの検査方法と侵入が検出されたときに行う作業が決まります。IPS バージョン 6.0 以降で仮想センサーを設定する場合、いずれかのセンサーをデフォルトとして指定します。ASA 5500 シリーズセキュリティ アプライアンスのコンフィギュレーションで仮想センサー名を指定しない場合は、デフォルト センサーが使用されます。

AIP SSM で実行される IPS ソフトウェアは、このマニュアルではそれらの機能について説明していないため、詳細な設定情報については IDM オンライン ヘルプを参照してください。IDM オンライン ヘルプは、ASDM に表示される [IDM] ペインで使用できます。また、次の URL にある Cisco.com で IDM および IPS のマニュアルを参照することができます。

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_installation_and_configuration_guides_list.html

仮想センサーのセキュリティ コンテンツへの割り当て

セキュリティ アプライアンスがマルチ コンテキスト モードにある場合、1 つまたは複数の IPS 仮想センサーを各コンテキストに割り当てることができます。次に、トラフィックを AIP SSM に送信するようコンテキストを設定する場合、コンテキストに割り当てられるセンサーを指定できます。コンテキストに割り当てなかったセンサーは指定できません。コンテキストにセンサーが割り当てられていない場合は、AIP SSM に設定されているデフォルト センサーが使用されます。同じセンサーを複数のコンテキストに割り当てることができます。

（注）　仮想センサーを使用するためにマルチ コンテキスト モードを開始する必要はありません。シングル モードでトラフィック フローごとに異なるセンサーを使用できます。

1 つまたは複数のセンサーをセキュリティ コンテキストに割り当てるには、次の手順に従います。

ステップ 1　[ASDM Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Security Contexts] ペインで、設定するコンテキストを選択し、[Edit] をクリックします。

[Edit Context] ダイアログボックスが表示されます。コンテキストの設定の詳細については、「セキュリティ コンテキストの設定」（P.9-20）を参照してください。

ステップ 3　[IPS Sensor Allocation] 領域で、[Add] をクリックします。

[IPS Sensor Selection] ダイアログボックスが表示されます。

ステップ 4　[Sensor Name] ドロップダウン リストで、AIP SSM に設定されているセンサーの中からセンサー名を選択します。

ステップ 5　（任意）センサーにマッピング名を割り当てるには、[Mapped Sensor Name] フィールドに値を入力します。

このセンサー名は、コンテキスト内で実際のセンサー名の代わりに使用できます。マッピング名を指定しない場合、センサー名がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているセンサーをコンテキスト管理者に知らせない場合があります。または、コンテキスト コンフィギュレーションを一般化する場合もあります。たとえば、すべてのコンテキストで「sensor1」と「sensor2」という名前のセンサーが使用されるようにする場合に、コンテキスト A ではセンサー「highsec」と「lowsec」を sensor1 と sensor2 にマッピングし、コンテキスト B ではセンサー「medsec」と「lowsec」を sensor1 と sensor2 にマッピングします。

ステップ 6　[OK] をクリックして [Edit Context] ダイアログボックスに戻ります。

ステップ 7　（任意）1 つのセンサーをこのコンテキストのデフォルト センサーとして設定するには、[Default Sensor] ドロップダウン リストからセンサー名を選択します。

コンテキスト コンフィギュレーション内に IPS を設定するときにセンサー名を指定しない場合、コンテキストはデフォルト センサーを使用します。コンテキストごとに設定できるデフォルト センサーは 1 つのみです。センサーをデフォルトとして指定せず、コンテキスト コンフィギュレーションにセンサー名が含まれていない場合、トラフィックは AIP SSM のデフォルト センサーを使用します。

ステップ 8　この手順をセキュリティ コンテキストごとに繰り返します。

ステップ 9　IPS セキュリティ ポリシーを設定するには各コンテキストに切り替えます（「トラフィックの AIP SSM への転送」（P.39-6）で説明されています）。

トラフィックの AIP SSM への転送

セキュリティ アプライアンスから AIP SSM へトラフィックを転送するよう指定するには、次の手順に従います。マルチ コンテキスト モードでは、各コンテキスト実行スペースでこれらの手順を実行します。

この機能は、サービス ポリシー ルールを使用してイネーブルにします。サービス ポリシー作成の詳細については、第 23 章「サービス ポリシー ルールの設定」を参照してください。

ステップ 1　[ASDM Device List] ペインで、アクティブなデバイスの [IP address] > [Contexts] の下にあるコンテキスト名をダブルクリックします。

ステップ 2　[Configuration] > [Firewall] > [Service Policy Rules] をクリックします。

ステップ 3　既存のルールを編集する、または新しいルールを作成するには、次の手順を実行します。

- 既存のルールの場合、ルールを選択して [Edit] をクリックします。

  [Edit Service Policy Rule] ダイアログボックスが表示されます。
- 新しいルールの場合、[Add] > [Add Service Policy Rule] を選択します。

  [Add Service Policy Rule Wizard - Service Policy] ダイアログボックスが表示されます。[Service Policy] ダイアログボックスおよび [Traffic Classification Criteria] ダイアログボックスで設定を完了します。詳細については、「通過トラフィックのサービス ポリシー ルールの追加」（P.23-4）を参照してください。[Next] をクリックして [Add Service Policy Rule Wizard - Rule Actions] ダイアログボックスを表示します。

ステップ 4　[Intrusion Prevention] タブをクリックします。

他のタブを使用し、この同じトラフィックに対して他の機能アクションを設定することもできます。

ステップ 5　[Enable IPS for this traffic flow] チェックボックスをオンにします。

ステップ 6　[Mode] 領域で、[Inline Mode] または [Promiscuous Mode] をクリックします。

詳細については、「動作モード」（P.39-2）を参照してください。

ステップ 7　[If IPS Card Fails] 領域で、[Permit traffic] または [Close traffic] をクリックします。

[Close traffic] オプションを選択すると、AIP SSM が使用できない場合、適応型セキュリティ アプライアンスはすべてのトラフィックをブロックします。

[Permit traffic] オプションは、AIP SSM が使用できない場合は検査を行わずにすべてのトラフィックの通過を許可するように適応型セキュリティ アプライアンスを設定します。

ステップ 8　（任意）[IPS Sensor to use] ドロップダウン リストから、仮想センサー名を選択します。

AIP SSM で仮想センサーを使用する場合、このオプションを使用してセンサー名を指定できます。セキュリティ アプライアンスでマルチ コンテキスト モードを使用する場合、コンテキストに割り当てたセンサーだけを指定できます（「仮想センサーのセキュリティ コンテンツへの割り当て」（P.39-5）を参照）。センサー名を指定しないと、トラフィックはデフォルトのセンサーを使用します。マルチ コンテキスト モードでは、コンテキストのデフォルトのセンサーを指定できます。シングル モードの場合、またはマルチ モードでデフォルトのセンサーを指定しない場合、トラフィックは AIP SSM に設定されているデフォルトのセンサーを使用します。

ステップ 9　[OK] をクリックします。

[Intrusion Prevention] タブのフィールドの説明

フィールド

- [Enable IPS for this traffic flow]：このトラフィック フローの侵入防御をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、このウィンドウの他のパラメータがアクティブになります。
- [Mode]：侵入防御の動作モードを設定します。詳細については、「動作モード」（P.39-2）を参照してください。
  - [Inline Mode]：インライン モードを選択します。このモードでは、パケットを IPS に向けて送ります。パケットは、IPS が動作した結果、ドロップされる場合があります。

  - [Promiscuous Mode]：無差別モードを選択します。このモードでは、元のパケットの複製パケットに対して IPS が作動します。元のパケットはドロップできません。
- [If IPS card fails]：AIP SSM が動作しなくなった場合に実行するアクションを設定します。
  - [Permit traffic]：AIP SSM の障害発生時にトラフィックを許可します。
  - [Close traffic]：AIP SSM の障害発生時にトラフィックをブロックします。
- [IPS Sensor Selection]：このトラフィック フローに使用する仮想センサーを選択します。詳細については、「仮想センサーの使用」（P.39-3）を参照してください。
  - [IPS Sensor to Use]：仮想センサー名を設定します。AIP SSM で仮想センサーを使用する場合、このオプションを使用してセンサー名を指定できます。セキュリティ アプライアンスでマルチ コンテキスト モードを使用する場合、コンテキストに割り当てたセンサーだけを指定できます（「仮想センサーのセキュリティ コンテンツへの割り当て」（P.39-5）を参照）。センサー名を指定しないと、トラフィックはデフォルトのセンサーを使用します。マルチ コンテキスト モードでは、コンテキストのデフォルトのセンサーを指定できます。シングル モードの場合、またはマルチ モードでデフォルトのセンサーを指定しない場合、トラフィックは AIP SSM に設定されているデフォルトのセンサーを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

AIP SSM パスワードのリセット

AIP SSM で IPS バージョン 6.0 以降を実行している場合、ASDM を使用して AIP SSM パスワードをデフォルト設定にリセットできます。デフォルトのパスワードは「cisco」（かぎカッコは除く）です。パスワードをリセットしたら、IDM で一意のパスワードに変更する必要があります。ASDM から IDM にアクセスする方法については、「ASDM からの IDM へのアクセス」（P.39-5）を参照してください。

AIP SSM パスワードをリセットすると、AIP SSM が再起動します。AIP SSM の再起動中、IPS サービスは使用できません。

AIP SSM パスワードをデフォルト設定にリセットするには、次の手順を実行します。

ステップ 1　ASDM メニューバーの [Tools] > [IPS Password Reset] を選択します。

（注）　SSM がインストールされていないと、このオプションはメニューに表示されません。CSC SSM がインストールされている場合、このオプションは [CSC Password Reset] と表示されます。

[IPS Password Reset] 確認ダイアログボックスが表示されます。

ステップ 2　[OK] をクリックして、AIP SSM パスワードをデフォルト設定にリセットします。

ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。パスワードがリセットされなかったときは、適応型セキュリティ アプライアンスでバージョン 7.2(2) 以降のプラットフォーム ソフトウェアを使用していること、および AIP SSM で IPS バージョン 6.0 以降を使用していることを確認してください。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。

CHAPTER 40

Trend Micro Content Security の設定

この章では、CSC SSM を設定する方法について説明します。次の項目を取り上げます。

CSC SSM への接続

ASDM で開始する各セッションでは、CSC SSM に関する機能にアクセスするたびに、管理 IP アドレスを指定して、CSC SSM のパスワードを入力する必要があります。CSC SSM に正常に接続した後は、管理 IP アドレスとパスワードの入力を求めるプロンプトは再表示されません。新しい ASDM セッションを開始すると、CSC SSM への接続がリセットされるので、IP アドレスと CSC SSM パスワードを再び指定する必要があります。適応型セキュリティ アプライアンスで時間帯を変更すると、CSC SSM への接続もリセットされます。

（注） CSC SSM には、ASDM パスワードとは別に保持されるパスワードがあります。同じパスワードを 2 つ設定することもできますが、CSC SSM パスワードを変更しても ASDM パスワードには影響しません。

CSC SSM に接続するには、次の手順を実行します。

ステップ 1 ASDM アプリケーションのメイン ウィンドウで、[Content Security] タブをクリックします。

ステップ 2 [Connecting to CSC] ダイアログボックスで、次のオプションのいずれかを選択します。

- [Management IP Address]：SSM の管理ポートの IP アドレスに接続します。ASDM によって適応型セキュリティ アプライアンスの SSM の IP アドレスが自動的に検出されます。この検出に失敗した場合は、手動で管理 IP アドレスを指定できます。
- [Other IP Address or Hostname]：SSM の代替 IP アドレスまたはホスト名に接続します。

ステップ 3 [Port] フィールドにポート番号を入力し、[Continue] をクリックします。

ステップ 4 [CSC Password] ダイアログボックスで、CSC パスワードを入力し、[OK] をクリックします。

（注）　CSC Setup Wizard（[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Wizard Setup] ウィンドウ）をまだ完了していない場合は、CSC Setup Wizard での設定を完了してください。この中に、デフォルト パスワード「cisco」の変更が含まれています。

パスワード入力後の 10 分間は、CSC SSM GUI の他の部分にアクセスするために CSC SSM パスワードを再入力する必要はありません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

CSC SSMの管理

この項では、CSC SSM を管理する方法について説明します。次の項目を取り上げます。

CSC SSM について

ASDM では、アクティベーション コードなど、Content Security and Control（CSC）SSM および CSC 関連機能の基本操作パラメータを設定できます。ASA 5500 シリーズ適応型セキュリティ アプライアンスは、Content Security and Control ソフトウェアを実行する CSC SSM をサポートしています。CSC SSM は、ウイルス、スパイウェア、スパムなどの好ましくないトラフィックを予防します。これは、FTP、HTTP、POP3、および SMTP トラフィックをスキャンすることで実現されます。そのためには、これらのトラフィックを CSC SSM に送信するように適応型セキュリティ アプライアンスを設定しておきます。

（注）　CSC SSM は、適応型セキュリティ アプライアンスで FTP 検査がイネーブルになっている場合にだけ FTP ファイル転送をスキャンできます。FTP 検査はデフォルトでイネーブルになっています。

CSC SSM のシステム セットアップとモニタリングには、ASDM を使用します。CSC SSM ソフトウェアにコンテンツ セキュリティ ポリシーを設定するには、ASDM 内のリンクをクリックして、CSC SSM の Web ベース GUI にアクセスします。CSC SSM GUI は、別個の Web ブラウザ ウィンドウに表示されます。CSC SSM にアクセスするには、CSC SSM のパスワードを入力する必要があります。CSC SSM GUI を使用するには、『*Cisco Content Security and Control SSM Administrator Guide*』を参照してください。

（注） ASDM と CSC SSM では、別個のパスワードが保持されます。それぞれのパスワードを同一にすることはできますが、これら 2 つのパスワードの 1 つを変更しても他のパスワードには影響を与えません。

ASDM を実行しているホストと適応型セキュリティ アプライアンスの間の接続は、適応型セキュリティ アプライアンスの管理ポートを通じて確立されます。CSC SSM GUI への接続は、SSM 管理ポートを通じて確立されます。これら 2 つの接続は、CSC SSM の管理に必要であるため、ASDM を実行しているホストは、適応型セキュリティ アプライアンスの管理ポートと SSM の管理ポートの両方の IP アドレスにアクセスできる必要があります。

CSC SSM の準備

CSC SSM のセキュリティ効果を得るには、SSM のハードウェアの取り付けだけでなく、他にもいくつかの手順を実行する必要があります。

適応型セキュリティ アプライアンスおよび CSC SSM を設定するには、次の手順を実行します。

ステップ 1　CSC SSM が Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに事前に取り付けられていない場合は、CSC SSM を取り付け、ネットワーク ケーブルを SSM の管理ポートに接続します。SSM の取り付けと接続については、『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

CSC SSM ソフトウェアの管理と自動アップデートを可能にするには、CSC SSM の管理ポートがネットワークに接続されている必要があります。また、CSC SSM は、電子メール通知とシステム ログ メッセージングの生成に管理ポートを使用します。

ステップ 2　CSC SSM には、Product Authorization Key（PAK）が付属しています。PAK を使用して、次の URL で CSC SSM を登録します。

http://www.cisco.com/go/license

登録後、E メールでアクティベーション キーを受信します。ステップ 5 を完了するには、アクティベーション キーが必要です。

ステップ 3　ステップ 5 で必要となる次の情報を収集します。

- ステップ 2 を完了した後に受信したアクティベーション キー。
- SSM 管理ポートの IP アドレス、ネットマスク、およびゲートウェイ IP アドレス。SSM 管理ポートの IP アドレスは、ASDM の実行で使用されるホストによりアクセスできなければなりません。SSM 管理ポートと適応型セキュリティ アプライアンス管理インターフェイスの IP アドレスは、異なるサブネットに属していてもかまいません。
- DNS サーバの IP アドレス。
- HTTP プロキシ サーバの IP アドレス（セキュリティ ポリシーで、インターネットへの HTTP アクセスにプロキシ サーバの使用が求められている場合に限り必要）。
- SSM のドメイン名とホスト名。

- 電子メール通知に使用する、電子メール アドレスおよび SMTP サーバの IP アドレスとポート番号。
- CSC SSM の管理を許可されたホストまたはネットワークの IP アドレス。
- CSC SSM 用のパスワード。

ステップ 4　ASDM で、セキュリティ アプライアンス上の時刻設定を確認します。時刻設定が正確であることは、セキュリティ イベントのロギングや CSC SSM ソフトウェアの自動アップデートで重要です。

- 時刻設定を手動で制御する場合は、時間帯を含む、クロック設定を確認します。[Configuration] > [Device Setup] > [System Time] > [Clock] を選択します。
- NTP を使用している場合は、NTP コンフィギュレーションを確認します。[Configuration] > [Device Setup] > [System Time] > [NTP] を選択します。

ステップ 5　CSC Setup Wizard を完了させます。

- [Configuration] > [Trend Micro Content Security] を選択します。CSC SSM に接続し、ログインします。[CSC Setup] > [Wizard Setup] を選択し、[Launch Setup Wizard] をクリックします。
- CSC Setup Wizard を再度実行する場合、上記の箇条書きと同じ手順を実行します。

CSC Setup Wizard については、[Help] をクリックします。

ステップ 6　スキャンするトラフィックを CSC SSM に誘導するようにサービス ポリシーを設定します。

グローバル ポリシーを作成してスキャンするトラフィックを誘導する場合、サポートされているプロトコルのトラフィック（着信と発信）がすべてスキャンされます。適応型セキュリティ アプライアンスと CSC SSM のパフォーマンスを最大化するには、非信頼送信元からのトラフィックだけをスキャンします。

トラフィックを CSC SSM に誘導するための最良の方法については、「スキャンするトラフィックの指定」（P.40-5）を参照してください。

スキャンするトラフィックを誘導するグローバル ポリシーを作成する場合は、次の手順を実行します。

a. [Configuration] > [Firewall] > [Service Policy Rules] を選択して、[Add] をクリックします。

[Add Service Policy Rule Wizard] ウィンドウが表示されます。

b. [Global - applies to all interfaces] オプションをクリックして、[Next] をクリックします。

[Traffic Classification Criteria] ウィンドウが表示されます。

c. [Create a new traffic class] オプションをクリックして、隣のフィールドにトラフィック クラスの名前を入力し、[Any traffic] チェックボックスをオンにしてから、[Next >] をクリックします。

[Rules Actions] ウィンドウが表示されます。

d. [CSC Scan] タブをクリックして、[Enable CSC scan for this traffic flow] チェックボックスをオンにします。

e. [If CSC card fails, then] というラベルの付いた領域で適切な選択を行って、CSC SSM が使用不可の場合に、選択したトラフィックの通過をセキュリティ アプライアンスで許可するか拒否するかを選択します。

f. [Finish] をクリックします。

[Service Policy Rules] ペインに新しいサービス ポリシーが表示されます。

g. [Apply] をクリックします。

適応型セキュリティ アプライアンスは、購入したライセンスによってイネーブルになったコンテンツ セキュリティ スキャンを実行する CSC SSM へのトラフィックの誘導を開始します。

ステップ 7　（任意）CSC SSM GUI でデフォルトのコンテンツ セキュリティ ポリシーを確認します。デフォルトのコンテンツ セキュリティ ポリシーは、ほとんどの実装に適しています。これらの修正には高度な設定が必要であるため、必ず『*Cisco Content Security and Control SSM Administrator Guide*』を読んでから実行してください。

（注）　コンテンツ セキュリティ ポリシーを確認するには、CSC SSM GUI でイネーブルになっている機能を表示します。使用できる機能は、購入したライセンスによって異なります。デフォルトでは、購入したライセンスに含まれているすべての機能がイネーブルになっています。

基本ライセンスの場合、デフォルトでイネーブルになっている機能は、SMTP ウイルス スキャン、POP3 ウイルス スキャン、コンテンツ フィルタリング、Web メール ウイルス スキャン、HTTP ファイル ブロッキング、FTP ウイルス スキャンとファイル ブロッキング、ロギング、および自動アップデートです。

Plus ライセンスの場合、デフォルトでイネーブルになっている追加機能は、SMTP アンチスパム、SMTP コンテンツ フィルタリング、POP3 アンチスパム、URL ブロッキング、および URL フィルタリングです。

ASDM の CSC SSM GUI にアクセスするには、[Configuration] > [Trend Micro Content Security] を選択し、[Web]、[Mail]、[File Transfer]、または [Updates] のいずれかのリンクをクリックします。CSC SSM GUI を開くには、これらのペイン内のいずれかのリンクをクリックします。

スキャンするトラフィックの指定

CSC SSM は、FTP、HTTP、POP3、SMTP のトラフィックをスキャンできますが、これらのプロトコルは、接続要求パケットの宛先ポートがそのプロトコルに設定されたポートである場合に限りサポートされます。CSC SSM がスキャンできる接続は、次の接続に限られます。

- TCP ポート 21 に対してオープンされている FTP 接続。
- TCP ポート 80 に対してオープンされている HTTP 接続。
- TCP ポート 110 に対してオープンされている POP3 接続。
- TCP ポート 25 に対してオープンされている SMTP 接続。

これらすべてのプロトコルのトラフィックをスキャンすることも、任意のプロトコルの組み合わせをスキャンすることもできます。たとえば、ネットワーク ユーザに POP3 電子メールの受信を許可しない場合に、POP3 トラフィックを CSC SSM に誘導するように適応型セキュリティ アプライアンスを設定する必要はありません。代わりに、POP3 トラフィックをブロックするように設定できます。

適応型セキュリティ アプライアンスと CSC SSM のパフォーマンスを最大化するには、CSC SSM でスキャンするトラフィックだけを CSC SSM に誘導します。信頼できる送信元と宛先の間のトラフィックなど、スキャンする必要のないトラフィックまでも誘導すると、ネットワーク パフォーマンスに悪影響を与える可能性があります。

（注）　トラフィックが最初に CSC 検査用に分類されるときは、フローベースとなります。トラフィックが既存の接続の一部である場合、トラフィックはその接続のポリシー セットに直接移動します。

[Add Service Policy Rule Wizard Rule Actions] ウィンドウの [CSC Scan] タブで、CSC SSM でのトラフィック スキャンをイネーブルにします。CSC スキャンを含むサービス ポリシーはグローバルにも、特定のインターフェイスにも適用できるので、CSC スキャンをグローバルにイネーブルにするか、特定のインターフェイスに対してイネーブルにするかを選択できます。詳細については、「CSC スキャンのルール アクション」（P.40-7）を参照してください。

csc コマンドをグローバル ポリシーに追加すると、適応型セキュリティ アプライアンスを通過する暗号化されていないすべての接続は、確実に CSC SSM でスキャンされます。ただし、このように設定すると、信頼できる送信元からのトラフィックが不必要にスキャンされることもあります。

CSC スキャンをインターフェイス固有のサービス ポリシーでイネーブルにした場合、これらのスキャンは双方向性を持ちます。双方向性のスキャンとは、適応型セキュリティ アプライアンスが新しい接続を開くとき、その接続の着信インターフェイスまたは発信インターフェイスのいずれかで CSC スキャンがアクティブで、サービス ポリシーでスキャン対象のトラフィックが特定されていれば、適応型セキュリティ アプライアンスはそのトラフィックを CSC SSM に誘導するということです。また、スキャンに双方向性があることにより、特定のインターフェイスを通過するサポート対象のトラフィック タイプを CSC SSM に誘導した場合に、信頼できる内部ネットワークからのトラフィックに対して不必要なスキャンを実行する可能性もあります。たとえば、DMZ ネットワークの Web サーバから要求された URL とファイルは、内部ネットワークのホストに対してコンテンツ セキュリティ リスクをもたらす可能性は低いため、適応型セキュリティ アプライアンスでこのようなトラフィックを CSC SSM に誘導する必要はほとんどありません。

したがって、CSC スキャンを定義するサービス ポリシーでアクセス リストを使用して、選択したトラフィックを制限することを強くお勧めします。特に、次の条件を満たすアクセス リストを使用することをお勧めします。

- 外部ネットワークへの HTTP 接続
- 適応型セキュリティ アプライアンスの内部のクライアントから、適応型セキュリティ アプライアンスの外部のサーバへの FTP 接続
- 適応型セキュリティ アプライアンスの内部のクライアントから適応型セキュリティ アプライアンスの外部のサーバへの POP3 接続。
- 内部メール サーバを宛先とする着信 SMTP 接続

inside-policy の最初のクラスである inside-class1 では、適応型セキュリティ アプライアンスによって内部ネットワークと DMZ ネットワークの間の HTTP トラフィックがスキャンされないことが保証されています。[Match] カラムに表示された [Do not match] アイコンが、この設定を示しています。この設定は、192.168.10.0 ネットワークから 192.168.20.0 ネットワークの TCP ポート 80 に送信されたトラフィックを適応型セキュリティ アプライアンスがブロックするということを意味するものではありません。この設定では、内部インターフェイスに適用されるサービス ポリシーによる照合からトラフィックを除外し、適応型セキュリティ アプライアンスによってトラフィックが CSC SSM に送信されないようにします。

inside-policy の 2 番目のクラスである inside-class では、内部ネットワークとすべての宛先との間の FTP、HTTP、および POP3 トラフィックが照合されます。DMZ ネットワークへの HTTP 接続は、inside-class1 の設定によって除外されます。前述のとおり、CSC スキャンを特定のインターフェイスに適用するポリシーは、着信トラフィックと発信トラフィックの両方に影響しますが、送信元ネットワークとして 192.168.10.0 を指定することにより、inside-class1 では内部ネットワークのホストから開始された接続だけが照合されます。

outside-policy では、outside-class で外部送信元から DMZ ネットワークへの SMTP トラフィックが照合されます。この設定では、SMTP クライアントからサーバへの接続をスキャンせずに、SMTP サーバと、DMZ ネットワーク上の SMTP サーバから電子メールをダウンロードする内部ユーザが保護されます。

DMZ ネットワーク上の Web サーバで、HTTP によって外部ホストからアップロードされたファイルを受信した場合は、任意の送信元から DMZ ネットワークへの HTTP トラフィックを照合するルールを外部ポリシーに追加できます。ポリシーは外部インターフェイスに適用されるので、このルールでは、適応型セキュリティ アプライアンス外部の HTTP クライアントからの接続だけが照合されます。

CSC スキャンのルール アクション

[CSC Scan] タブでは、CSC SSM が、現在のトラフィック クラスによって特定されるトラフィックをスキャンするかどうかを判別できます。このタブは、適応型セキュリティ アプライアンスに CSC SSM が取り付けられていないと表示されません。

CSC SSM は、HTTP、SMTP、POP3、および FTP のトラフィックだけをスキャンします。使用するサービス ポリシーに、これら 4 種類のプロトコル以外のプロトコルをサポートするトラフィックが含まれていると、他のプロトコルのパケットは、スキャンされることなく CSC SSM を通過します。CSC SSM に対する負荷を軽減するには、パケットを CSC SSM に送信して HTTP、SMTP、POP3、または FTP トラフィックだけをサポートするサービス ポリシー規則を設定します。

フィールド

- [Enable CSC scan for this traffic flow]: このトラフィック フローでの CSC SSM の使用をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、このウィンドウの他のパラメータがアクティブになります。
- [If CSC card fails] : CSC SSM が動作しなくなった場合に実行するアクションを設定します。
  - [Permit traffic] : CSC SSM が失敗した場合にトラフィックを許可します。
  - [Close traffic] : CSC SSM が失敗した場合にトラフィックをブロックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

CSC SSM のセットアップ

[CSC Setup] の下にあるペインでは、CSC SSM の基本操作パラメータを設定できます。各ペインを個別に設定する前に、CSC Setup Wizard を少なくとも一度完了する必要があります。CSC Setup Wizard を完了した後は、このウィザードを再度使用しなくても各ペインを個別に変更できます。

また、CSC Setup Wizard を完了するまでは、[Home] > [Trend Micro Content Security] > [Content Security] タブまたは [Monitoring] > [Trend Micro Content Security] > [Content Security] タブのペインにアクセスできません。このウィザードが完了する前にそれらのペインにアクセスしようとすると、ダイアログボックスが表示され、そこからウィザードに直接アクセスして設定を完了させることができます。

CSC SSM の概要については、「CSC SSM について」（P.40-2）を参照してください。詳細については、次のトピックを参照してください。

- 「Activation/License」（P.40-8）
- 「IP 設定」（P.40-9）
- 「ホスト設定と通知設定」（P.40-10）
- 「管理アクセスホストとネットワーク」（P.40-11）
- 「パスワード」（P.40-12）
- 「デフォルト パスワードの復元」（P.40-13）
- 「ウィザードの設定」（P.40-14）

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、CSC Setup ノードのペインは管理コンテキストでだけ使用できます。

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

Activation/License

[Activation/License] ペインでは、CSC SSM の次の 2 つのコンポーネントのアクティベーション コードを設定できます。

- 基本ライセンス
- Plus ライセンス

ASDM を使用して、2 つのライセンスにそれぞれ一度だけ CSC ライセンスを設定できます。ソフトウェアのアップデートをスケジュールしておくと、更新されたライセンス アクティベーション コードが自動的にダウンロードされます。ライセンス ステータス ページと CSC UI ホームページへのリンクがこのウィンドウの下部に表示されます。割り当てられたライセンスのシリアル番号が自動的に入力されます。

フィールド

- [Product]：*表示専用*。コンポーネントの名前が表示されます。

- [Activation Code]：対応する [Product] フィールドのアクティベーション コードが含まれます。
- [License Status]：*表示専用*。ライセンスのステータスに関する情報を表示します。ライセンスが有効な場合、有効期限が表示されます。有効期限が過ぎている場合は、このフィールドにライセンスが失効している旨が表示されます。
- [Nodes]：*表示専用*。CSC SSM の基本ライセンスでサポートされるネットワーク デバイスの最大数を示します。Plus ライセンスはサポートされているネットワーク デバイスの数に影響しません。したがって、[Plus License] 領域には [Nodes] フィールドが表示されません。
- ライセンス ステータスを確認する、またはライセンスを更新するには、表示されるリンクをクリックします。
- ASDM の CSC ホームページに移動するには、表示されるリンクをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、[Activation/License] ペインは管理コンテキストでだけ使用できます。

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

IP 設定

[IP Configuration] ペインでは、CSC SSM、使用する DNS サーバ、および CSC SSM ソフトウェアのアップデートを取得するための IP アドレスおよびその他の関連する詳細を設定できます。

フィールド

- [Management Interface]：CSC SSM への管理アクセス用のパラメータが含まれます。
  - [IP Address]：CSC SSM への管理アクセス用の IP アドレスを設定します。
  - [Mask]：CSC SSM の管理 IP アドレスが含まれるネットワークのネットマスクを設定します。
  - [Gateway]：CSC SSM の管理 IP アドレスが含まれるネットワークのゲートウェイ デバイスの IP アドレスを設定します。
- [DNS Servers]：CSC SSM の管理 IP アドレスが含まれるネットワークの DNS サーバに関するパラメータが含まれます。
  - [Primary DNS]：プライマリ DNS サーバの IP アドレスを設定します。
  - [Secondary DNS]：（任意）セカンダリ DNS サーバの IP アドレスを設定します。
- [Proxy Server]：CSC SSM が CSC SSM ソフトウェアのアップデート サーバに接続するために使用するオプションの HTTP プロキシ サーバのパラメータが含まれます。ネットワーク コンフィギュレーションで、CSC SSM でプロキシ サーバの使用を必要としない場合、このグループのフィールドを空白のままにすることができます。

- [Proxy Server]：（任意）プロキシ サーバの IP アドレスを設定します。
- [Proxy Port]：（任意）プロキシ サーバのリスニング ポートを設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、[IP Configuration] ペインは管理コンテキストだけで使用できます。

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

ホスト設定と通知設定

[Host/Notification Settings] ペインでは、ホスト名、ドメイン名、電子メール通知、および詳細なスキャンから除外する電子メールのドメイン名に関する詳細を設定できます。

フィールド

- [Host and Domain Names]：CSC SSM のホスト名とドメイン名に関する情報が含まれます。
  - [HostName]：CSC SSM のホスト名を設定します。
  - [Domain Name]：CSC SSM が含まれたドメイン名を設定します。
- [Incoming E-mail Domain Name]：SMTP ベース電子メールの信頼できる着信電子メール ドメイン名に関する情報が含まれます。
  - [Incoming Email Domain]：着信電子メール ドメイン名を設定します。CSC SSM は、このドメインに送信された SMTP 電子メールをスキャンします。CSC SSM がスキャンする脅威のタイプは、購入した CSC SSM のライセンスと、CSC SSM ソフトウェアのコンフィギュレーションによって異なります。

（注） CSC SSM では、着信電子メールド メインのリストを多数設定できます。ASDM は、最初のドメインだけをリストに表示します。着信電子メールのドメインを追加設定するには、CSC SSM インターフェイスにアクセスします。これを行うには、[Configuration] > [Trend Micro Content Security] > [Email] を選択し、いずれかのリンクをクリックします。CSC SSM にログインしたら、[Mail (SMTP)] > [Configuration] を選択して [Incoming Mail] タブをクリックします。

- [Notification Settings]：イベントの電子メール通知に必要な情報が含まれます。
  - [Administrator Email]：電子メール通知の送信先となるアカウントの電子メール アドレスを設定します。
  - [Email Server IP Address]：SMTP サーバの IP アドレスを設定します。

– [Port]：SMTP サーバがリッスンするポートを設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、[Host/Notification Settings] ペインは管理コンテキストだけで使用できます。

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

管理アクセスホストとネットワーク

[Management Access Host/Networks] ペインでは、CSC SSM への管理アクセスを許可するホストとネットワークを制御できます。許可するホストまたはネットワークを少なくとも 1 つ指定する必要があります。最大 8 つの許可するホストまたはネットワークを指定できます。

フィールド

- [IP Address]：[Selected Hosts/Network] リストに追加するホストまたはネットワークのアドレスを設定します。
- [Mask]：[IP Address] フィールドに指定したホストまたはネットワークのネットマスクを設定します。

  すべてのホストとネットワークを許可するには、[IP Address] フィールドに **0.0.0.0** と入力し、[Mask] リストから 0.0.0.0 を選択します。
- [Selected Hosts/Networks]：CSC SSM への管理アクセスに信頼できるホストまたはネットワークが表示されます。ASDM では、少なくとも 1 つのホストまたはネットワークを設定する必要があります。最大 8 つのホストまたはネットワークを設定できます。

  リストからホストまたはネットワークを削除するには、リストのエントリを選択し、[Delete] をクリックします。
- [Add >>]：[IP Address] フィールドで指定したホストまたはネットワークを、[Selected Hosts/Networks] リストに追加します。
- [Delete]：[Selected Hosts/Networks] リストで選択したホストまたはネットワークを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、[Management Access Host/Networks] ペインは管理コンテキストだけで使用できます。

詳細情報

「CSC SSM の管理」（P.40-2）

パスワード

[Password] ペインでは、CSC SSM への管理アクセスに必要なパスワードを変更できます。CSC SSM には、ASDM パスワードとは別に保持されるパスワードがあります。それらに同じパスワードを設定できますが、CSC SSM のパスワードを変更しても ASDM のパスワードは変更されません。

ASDM が CSC SSM に接続されているときに CSC SSM パスワードを変更すると、CSC SSM への接続はドロップされます。その結果、ASDM には確認ダイアログボックスが表示されるので、パスワードを変更する前に応答する必要があります。

ヒント　CSC SSM への接続がドロップされた場合は、常にその接続を再確立できます。再確立するには、ステータス バーの [Connection to Device] アイコンをクリックして [Connection to Device] ダイアログボックスを表示し、[Reconnect] をクリックします。ASDM は、CSC SSM のパスワードを要求するプロンプトを表示します。このパスワードは、定義済みの新規パスワードです。

パスワードの長さは、5 ～ 32 文字で指定します。

パスワードを入力するとアスタリスクで表示されます。

（注）　デフォルトのパスワードは「cisco」です。

フィールド

- [Old Password]：CSC SSM に管理アクセスするための現在のパスワードが必要です。
- [New Password]：CSC SSM に管理アクセスするための新しいパスワードを設定します。
- [Confirm New Password]：CSC SSM に管理アクセスするための新しいパスワードを確認のために入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、[Password] ペインは管理コンテキストだけで使用できます。

詳細情報

「CSC SSM の管理」（P.40-2）

デフォルト パスワードの復元

ASDM を使用して CSC SSM のパスワードをリセットできます。このパスワードは、「cisco」（かぎカッコなし）というデフォルト値に戻すことができます。CSC パスワードリセット ポリシーが「Denied」に設定されていると、ASDM CLI を使用してパスワードをリセットできません。このポリシーを変更するには、CSC SSM へのセッションを確立する必要があります。詳細については、『*Cisco Content Security and Control SSM Administrator Guide*』を参照してください。

（注） SSM がインストールされていないと、このオプションはメニューに表示されません。

CSC SSM パスワードをデフォルト値にリセットするには、次の手順を実行します。

ステップ 1　ASDM メニュー バーで、[Tools] > [CSC Password Reset] を選択します。

[CSC Password Reset confirmation] ダイアログボックスが表示されます。

ステップ 2　[OK] をクリックして、CSC SSM パスワードをデフォルト値にリセットします。

ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。パスワードがリセットされなかったときは、適応型セキュリティ アプライアンスでバージョン 8.0(2) のソフトウェアを使用していること、および CSC SSM で最新のバージョン 6.1.x ソフトウェアを使用していることを確認してください。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。

ステップ 4　パスワードをリセットしたら、一意のパスワードに変更する必要があります。

（注） この機能は、システム コンテキストのマルチコンテキスト モードだけで使用できます。

詳細情報

「パスワード」（P.40-12）を参照してください。

ウィザードの設定

[Wizard Setup] ペインでは、CSC Setup Wizard を起動できます。

[CSC Setup] で他のペインに直接アクセスする前に、CSC Setup Wizard を完了する必要があります。このウィザードには、次のペインがあります。

- 「CSC Setup Wizard アクティベーション コードの設定」（P.40-14）
- 「CSC Setup Wizard の IP コンフィギュレーション」（P.40-15）
- 「CSC Setup Wizard のホスト コンフィギュレーション」（P.40-16）
- 「CSC Setup Wizard の管理アクセス コンフィギュレーション」（P.40-16）
- 「CSC Setup Wizard のパスワード コンフィギュレーション」（P.40-17）
- 「CSC Setup Wizard の CSC スキャンのためのトラフィック選択」（P.40-17）
- 「CSC Setup Wizard の要約」（P.40-19）

CSC Setup Wizard を完了したら、CSC Setup Wizard を再度使用しなくても CSC SSM の関連ペインで設定を変更できます。

フィールド

- [Launch Setup Wizard]：CSC Setup Wizard を起動する場合にクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、[Wizard Setup] ペインは管理コンテキストだけで使用できます。

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

CSC Setup Wizard アクティベーション コードの設定

[CSC Setup Wizard Activation Codes Configuration] ウィンドウには、CSC SSM の機能をイネーブルにするために入力したアクティベーション コードが、所有するライセンスのタイプに応じて表示されます。

フィールド

- [Activation Code]：*表示専用*。このウィンドウで行ったアクティベーション コードの設定を表示します。
  - [Base License]：アクティベーション コードを示します。基本ライセンスには、アンチウイルス、アンチスパイウェア、およびファイル ブロッキングが含まれます。

– [Plus License]：アクティベーション コードを入力した場合は、そのアクティベーション コードを表示します。入力していないときは、空白になります。Plus ライセンスには、アンチスパム、アンチフィッシング、コンテンツ フィルタリング、および URL ブロッキングと URL フィルタリングが含まれます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

CSC Setup Wizard の IP コンフィギュレーション

[CSC Setup Wizard IP Configuration] ウィンドウには、CSC SSM 用に入力した IP コンフィギュレーション設定が表示されます。

フィールド

- [IP Address]：CSC SSM の管理インターフェイスの IP アドレスを表示します。
- [Mask]：ドロップダウン リストから選択した CSC SSM の管理インターフェイスのネットワーク マスクを表示します。
- [Gateway]：CSC SSM 管理インターフェイスが含まれるネットワークのゲートウェイ デバイスの IP アドレスを表示します。
- [Primary DNS]：プライマリ DNS サーバの IP アドレスを表示します。
- [Secondary DNS]（任意）：セカンダリ DNS サーバの IP アドレスを表示します（設定している場合）。
- [Proxy Server]（任意）：プロキシ サーバを表示します（設定している場合）。
- [Proxy Port]（任意）：プロキシ ポートを表示します（設定している場合）。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

CSC Setup Wizard のホスト コンフィギュレーション

[CSC Setup Wizard Host Configuration] ウィンドウには、CSC SSM 用に入力したホスト名とドメイン名、着信電子メールのドメイン名、管理者の電子メール アドレス、電子メール サーバの IP アドレス、およびポート番号が表示されます。

フィールド

- [Hostname]：CSC SSM のホスト名を表示します。
- [Domain Name]：CSC SSM が常駐するドメインの名前を表示します。
- [Incoming Email Domain]：着信電子メールのドメイン名を表示します。
- [Administrator E-mail]：ドメイン管理者の電子メール アドレスを表示します。
- [E-mail Server IP Address]：電子メール サーバの IP アドレスを表示します。
- [Port]：CSC SSM への接続に使用するポート番号を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

CSC SSM の管理を参照してください。

CSC Setup Wizard の管理アクセス コンフィギュレーション

[CSC Setup Wizard IP Configuration] ウィンドウには、CSC SSM へのアクセス権を付与するために入力したサブネットおよびホスト設定が表示されます。

フィールド

- [IP Address]：CSC SSM への接続が許可されているネットワークおよびホストの IP アドレスを表示します。
- [Mask]：ドロップダウン リストから選択した CSC SSM への接続が許可されているネットワークとホストのネットワーク マスクを表示します。
- [Add]：CSC SSM への接続を許可するネットワークおよびホストの IP アドレスを追加する場合にクリックします。
- [Delete]：CSC SSM に接続する必要がなくなったネットワークまたはホストの IP アドレスを削除する場合にクリックします。
- [Selected Hosts/Networks]：追加した CSC SSM に接続可能なネットワークおよびホストの IP アドレスを一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

CSC Setup Wizard のパスワード コンフィギュレーション

[CSC Setup Wizard Password Configuration] ウィンドウには、CSC SSM へのアクセス権を付与するために入力したパスワード設定が表示されます。

フィールド

- [Old Password]：CSC SSM にアクセスするために現在のパスワードが必要です。
- [New Password]：CSC SSM にアクセスするための新しいパスワードを設定します。
- [Confirm New Password]：CSC SSM にアクセスするための新しいパスワードを確認のために入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

CSC Setup Wizard の CSC スキャンのためのトラフィック選択

[CSC Setup Wizard Traffic Selection for CSC Scan] ウィンドウには、CSC スキャン対象のトラフィックを選択するために行った設定が表示されます。

フィールド

- [Interface]：ドロップダウン リストから選択した CSC SSM へのインターフェイスを指定します。
- [Source]：CSC SSM がスキャンするネットワーク トラフィックの送信元を指定します。
- [Destination]：CSC SSM がスキャンするネットワーク トラフィックの宛先を指定します。

- [Service] : CSC SSM がスキャンする送信元サービスまたは宛先サービスを指定します。
- [Add] : CSC スキャンに関する追加のトラフィック詳細を指定する場合にクリックします。詳細については、「CSC スキャンのためのトラフィック指定」（P.40-18）を参照してください。
- [Edit] : CSC スキャンに関する追加のトラフィック詳細を変更する場合にクリックします。詳細については、「CSC スキャンのためのトラフィック指定」（P.40-18）を参照してください。
- [Delete] : CSC スキャンに関する追加のトラフィック詳細を削除する場合にクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

CSC スキャンのためのトラフィック指定

[Specify traffic for CSC Scan] ダイアログボックスでは、CSC スキャン対象のトラフィックを選択するための追加の設定を定義、変更、または削除できます。

フィールド

- [Interface] : CSC SSM へのインターフェイスのタイプをドロップダウン リストから指定します。指定できる設定値は、global（すべてのインターフェイス）、inside、management、outside です。
- [Source] : CSC SSM がスキャンするネットワーク トラフィックの送信元をドロップダウン リストから指定します。
- [Destination] : CSC SSM がスキャンするネットワーク トラフィックの宛先をドロップダウン リストから指定します。
- [Service] : CSC SSM がスキャンするサービスのタイプをドロップダウン リストから指定します。
- [Description] : CSC SSM がスキャンするように定義したネットワーク トラフィックについて説明します。
- [If CSC card fails] : CSC カードに障害が発生した場合に、CSC SSM にネットワーク トラフィックのスキャンを許可するかどうかを指定します。

  スキャンされていないトラフィックを許可するには、[Permit] をクリックします。スキャンされていないトラフィックが通過しないようにするには、[Close] をクリックします。[OK] をクリックして設定内容を保存します。[CSC Setup Wizard Traffic selection for CSC Scan] ウィンドウに、追加したトラフィック詳細が表示されます。これらの設定内容を破棄して [CSC Setup Wizard Traffic selection for CSC Scan] ウィンドウに戻るには、[Cancel] をクリックします。[Cancel] をクリックすると、ASDM にはユーザの決定を確認するダイアログボックスが表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC Setup Wizard の CSC スキャンのためのトラフィック選択」（P.40-17）を参照してください。

CSC Setup Wizard の要約

[CSC Setup Wizard Summary] ウィンドウには、CSC Setup Wizard で行った設定が表示されます。ウィザードを終了する前に選択内容を確認できます。設定を変更する場合は、[< Back] をクリックして変更する設定のウィンドウまで戻り、必要な変更を加えてから [Next >] をクリックしてこのウィンドウに戻ります。

（注）　[Finish] をクリックした後は、CSC Setup Wizard を再度使用しなくても CSC SSM に関連するいずれのウィンドウも変更できます。

フィールド

- [Activation Codes]：*表示専用*。[Activation Codes Configuration] ウィンドウで行った設定の要約を表示します。
  - [Base]：基本ライセンスのアクティベーション コードを表示します。
  - [Plus]：Plus ライセンスのアクティベーション コードを入力した場合は、そのアクティベーション コードを表示します。入力していないときは、空白になります。
- [IP Parameters]：*表示専用*。[IP Configuration] ウィンドウで行った設定の要約を表示します。次の情報が含まれています。
  - CSC SSM の管理インターフェイスの IP アドレスとネットマスク。
  - CSC SSM 管理インターフェイスが含まれるネットワーキング用のゲートウェイ デバイスの IP アドレス。
  - プライマリ DNS サーバの IP アドレス。
  - セカンダリ DNS サーバの IP アドレス（設定している場合）。
  - プロキシ サーバおよびポート（設定している場合）。
- [Host and Domain Names]：*表示専用*。[Host Configuration] ウィンドウで行った設定の要約を表示します。次の情報が含まれています。
  - CSC SSM のホスト名。
  - CSC SSM が含まれるドメインのドメイン名。
  - 着信電子メールのドメイン名。
  - 管理者の電子メール アドレス。
  - 電子メール サーバの IP アドレスとポート番号。

- [Management Access List]：[Management Access Configuration] ウィンドウで行った設定の要約を表示します。ドロップダウン リストには、CSC SSM が管理接続を許可するホストとネットワークが含まれています。
- [Password]：*表示専用*。[Password Configuration] ウィンドウでパスワードを変更したかどうかを示します。
- [< Back]：CSC Setup Wizard の前のペインに戻る場合にクリックします。
- [Next >]：グレー表示されています。ただし、[< Back] をクリックしてこのウィザード内の前のウィンドウにアクセスした場合は [Next >] をクリックするとこのウィンドウに戻ります。
- [Finish]：CSC Setup Wizard を終了し、ウィザードで行ったすべての設定を保存します。
- [Cancel]：選択した設定内容を保存しないで CSC Setup Wizard を終了します。[Cancel] をクリックすると、ASDM にはユーザの決定を確認するダイアログボックスが表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

Web

[Web] ペインでは、Web 関連機能がイネーブルになっているかどうかを確認したり、CSC SSM にアクセスして Web 関連機能を設定することができます。

（注）　CSC SSM にアクセスするには、CSC SSM パスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザ ウィンドウのセッションがタイムアウトになります。CSC SSM ブラウザ ウィンドウを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

フィールド

- [URL Blocking and Filtering]：URL ブロッキングおよび URL フィルタリングに関連する情報とリンクが含まれています。
  - [URL Blocking]：*表示専用*。CSC SSM で URL ブロッキングがイネーブルになっているかどうかを示します。
  - [Configure URL Blocking]：CSC SSM で URL ブロッキングを設定するためのウィンドウを開きます。
  - [URL Filtering]：*表示専用*。CSC SSM で URL フィルタリングがイネーブルになっているかどうかを示します。

  - [Configure URL Filtering Rules] : CSC SSM で URL フィルタリング ルールを設定するためのウィンドウを開きます。
  - [Configure URL Filtering Settings] : CSC SSM で URL フィルタリング設定を行うためのウィンドウを開きます。
- [File Blocking] : CSC SSM の HTTP ファイル ブロッキングに関するフィールドとリンクが含まれています。
  - [File Blocking] : *表示専用*。CSC SSM でファイル ブロッキングがイネーブルになっているかどうかを示します。
  - [Configure File Blocking] : CSC SSM で HTTP ファイル ブロッキング設定を行うためのウィンドウを開きます。
- [Scanning] : CSC SSM の HTTP スキャンに関するフィールドとリンクが含まれています。
  - [HTTP Scanning] : *表示専用*。CSC SSM で HTTP スキャンがイネーブルになっているかどうかを示します。
  - [Configure Web Scanning] : CSC SSM で HTTP スキャンを設定するためのウィンドウを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

MAIL

[Mail] ペインでは、電子メール関連の機能がイネーブルになっているかどうかを確認し、CSC SSM にアクセスして電子メール関連機能を設定できます。

これらの領域の設定の詳細については、次の項目を参照してください。

- 「[SMTP] タブ」（P.40-22）
- 「[POP3] タブ」（P.40-23）

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

[SMTP] タブ

[SMTP] タブには、CSC SSM の SMTP 電子メール機能に固有のフィールドとリンクが表示されます。

（注）　CSC SSM GUI にアクセスするには、CSC SSM のパスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

フィールド

- [Scanning] : SMTP スキャンに関するフィールドとリンクが含まれています。
  - [Incoming Scan] : *表示専用*。CSC SSM で着信 SMTP スキャン機能がイネーブルになっているかどうかを示します。
  - [Configure Incoming Scan] : CSC SSM で着信 SMTP スキャン設定を行うためのウィンドウを開きます。
  - [Outgoing Scan] : *表示専用*。CSC SSM で発信 SMTP スキャン機能がイネーブルになっているかどうかを示します。
  - [Configure Outgoing Scan] : CSC SSM で発信 SMTP スキャン設定を行うためのウィンドウを開きます。
- [Content Filtering] : SMTP コンテンツ フィルタリングに関するフィールドとリンクが含まれています。
  - [Incoming Filtering] : *表示専用*。CSC SSM で着信 SMTP 電子メールのコンテンツ フィルタリングがイネーブルになっているかどうかを示します。
  - [Configure Incoming Filtering] : CSC SSM で着信 SMTP コンテンツ フィルタリングを設定するためのウィンドウを開きます。
  - [Outgoing Filtering] : *表示専用*。CSC SSM で発信 SMTP 電子メールのコンテンツ フィルタリングがイネーブルになっているかどうかを示します。
  - [Configure Outgoing Filtering] : CSC SSM で発信 SMTP コンテンツ フィルタリングを設定するためのウィンドウを開きます。
- [Anti-spam] : SMTP アンチスパム機能に関するフィールドとリンクが含まれています。
  - [Spam Prevention] : *表示専用*。CSC SSM で SMTP アンチスパム機能がイネーブルになっているかどうかを示します。
  - [Configure Anti-spam] : CSC SSM で SMTP アンチスパムを設定するためのウィンドウを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

[POP3] タブ

[POP3] タブには、CSC SSM の POP3 電子メール機能に固有のフィールドとリンクが表示されます。

（注）　CSC SSM GUI にアクセスするには、CSC SSM のパスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

フィールド

- [Scanning]：*表示専用*。CSC SSM で POP3 電子メール スキャンがイネーブルになっているかどうかを示します。
- [Configure Scanning]：CSC SSM で POP3 電子メール スキャンを設定するためのウィンドウを開きます。
- [Anti-spam]：*表示専用*。CSC SSM で POP3 アンチスパム機能がイネーブルになっているかどうかを示します。
- [Configure Anti-spam]：CSC SSM で POP3 アンチスパム機能を設定するためのウィンドウを開きます。
- [Content Filtering]：*表示専用*。CSC SSM で POP3 電子メール コンテンツ フィルタリング機能がイネーブルになっているかどうかを示します。
- [Configure Content Filtering]：CSC SSM で POP3 電子メール コンテンツ フィルタリングを設定するためのウィンドウを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

File Transfer

[File Transfer] ペインでは、FTP 関連の機能がイネーブルになっているかどうかを確認し、CSC SSM にアクセスして FTP 関連機能を設定できます。

（注）　CSC SSM GUI にアクセスするには、CSC SSM のパスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

フィールド

- [File Scanning] : *表示専用*。CSC SSM で FTP ファイル スキャンがイネーブルになっているかどうかを示します。
- [Configure File Scanning] : CSC SSM で FTP ファイル スキャン設定を行うためのウィンドウを開きます。
- [File Blocking] : *表示専用*。CSC SSM で FTP ファイル ブロッキングがイネーブルになっているかどうかを示します。
- [Configure File Blocking] : CSC SSM で FTP ファイル ブロッキング設定を行うためのウィンドウを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

アップデート

[Updates] ペインでは、アップデートのスケジュール設定がイネーブルになっているかどうかを確認し、CSC SSM にアクセスしてアップデートのスケジュールを設定できます。

（注）　CSC SSM GUI にアクセスするには、CSC SSM のパスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

フィールド

- [Scheduled Updates]：*表示専用*。CSC SSM でアップデートのスケジュール設定がイネーブルになっているかどうかを示します。
- [Scheduled Update Frequency]：アップデートを実行するスケジュールに関する情報（「Hourly at 10 minutes past the hour」など）を表示します。
- [Component]：アップデート可能な CSC SSM ソフトウェアのコンポーネントの名前を表示します。
- [Scheduled Updates]：*表示専用*。対応するコンポーネントでアップデートのスケジュール設定がイネーブルになっているかどうかを示します。
- [Configure Updates]：CSC SSM でアップデートのスケジュール設定を行うためのウィンドウを開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」（P.40-2）を参照してください。

CHAPTER 41

ロギングのモニタリング

ログ バッファに表示されるリアルタイムのシステム ログ メッセージを確認できます。Cisco ASDM 6.0(2) for ASA 8.0(2) のメイン アプリケーション ウィンドウを開くと、最新の ASDM システム ログ メッセージがスクロール ウィンドウの一番下に表示されます。

これらのメッセージは、エラーのトラブルシューティングや、システムの使用状況およびパフォーマンスの監視に役立ちます。ロギング機能の説明については、第 15 章「ロギングの設定」を参照してください。

ログ表示について

この項では、システム ログ メッセージの表示について説明します。次の項目を取り上げます。

Log Buffer

このペインを使用して、バッファに保存されたログ メッセージを別のウィンドウで表示します。このペインにアクセスするには、[Monitoring] > [Logging] > [Log Buffer] を選択します。

フィールド

- [Logging Level]：表示するロギング メッセージのレベルを [Emergency] から [Debugging] の範囲で選択します。
- [View]：ログ メッセージが表示される別のウィンドウを開きます。ここでメッセージ ウィンドウをクリアして、ログの内容を保存できます。また、メッセージ内の特定のテキストを検索することもできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Log Buffer Viewer

このペインを使用して、ログ バッファに示されるメッセージを表示し、メッセージの説明、メッセージの詳細、および、実行したり、必要に応じて解決したりするための推奨アクションを確認します。このペインにアクセスするには、[Monitoring] > [Logging] > [Log Buffer] > [View] を選択します。

ビューアのメッセージを右クリックするとメニューが表示され、[Refresh]、[Copy]、[Save]、[Clear]、[Color Settings]、[Create Rule]、[Show Rule]、および [Show Details] オプションの中から選択できます。このペインの下部には、それぞれの重大度に関連付けられているアイコンのリストが表示されます。重大度の詳細については、第 15 章「ロギングの設定」を参照してください。

フィールド

- [Refresh]：画面をリフレッシュします。
- [Copy]：選択したメッセージをコピーします。
- [Save]：ログの内容をコンピュータに保存します。
- [Clear]：メッセージのリストをクリアします。
- [Color Settings]：さまざまな重大度のメッセージを異なる色で表示することを指定できます。
- [Create Rule]：メッセージを最初に作成したアクセス コントロール ルールと逆のアクションを実行するアクセス コントロール ルールを作成できます。
- [Show Rule]：選択したメッセージを作成したアクセス コントロール ルールを表示します。この機能は、システム ログ メッセージ ID 106100 および 106023 にだけ適用されます。
- [Show Details]：[Explanation] タブ、[Recommended Action] タブ、および [Details] タブを表示または非表示にします。[Explanation] タブには、メッセージ構文、メッセージの説明、および推奨される修正処置（ある場合）が表示されます。[Recommended Action] タブでは、このメッセージを受け取った際に実行する手順が説明されています。[Details] タブには、日付、時刻、重大度、syslog ID、送信元の IP アドレス、宛先の IP アドレス、およびメッセージの説明が表示されます。
- [Find]：メッセージで検索するテキストを入力します。入力したテキストに基づいてメッセージを検索します。
- [Help]：詳細情報を表示します。
- [Filter By]：メッセージのフィルタ条件になるテキストを入力できます。Enter を押すか、または [Filter] をクリックして、表示されたメッセージにフィルタを適用します。
- [Show All]：すべてのメッセージを表示します。フィルタは、表示から除外されます。このボタンは、表示されたログ メッセージにフィルタが適用されている場合にだけアクティブになります。
- [Filter]：メッセージ リストにフィルタを適用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Real-Time Log Viewer

このペインを使用して、別のウィンドウにリアルタイムのシステム ログ メッセージを表示します。このペインにアクセスするには、[Monitoring] > [Logging] > [Real-Time Log Viewer] を選択します。

フィールド

- [Logging Level]：表示するロギング メッセージのレベルを [Emergency] から [Debugging] の範囲で選択します。
- [Buffer Limit]：表示するログ メッセージの最大数。デフォルトは 1000 です。
- [View]：ログ メッセージが表示される別のウィンドウを開きます。ここで着信メッセージを一時停止して、メッセージ ウィンドウをクリアし、ログの内容を保存できます。また、メッセージ内の特定のテキストを検索したり、重大度ごとに色を設定したり、アクセス ルールを作成および表示したり、メッセージの詳細を表示することもできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Real-Time Log Viewer

このペインを使用して、着信メッセージをリアルタイムで表示して、指定したテキストを基準にメッセージをフィルタリングします。このペインにアクセスするには、[Monitoring] > [Logging] > [Real-Time Log Viewer] > [View] を選択します。

ビューアのメッセージを右クリックするとメニューが表示され、[Refresh]、[Copy]、[Save]、[Clear]、[Color Settings]、[Create Rule]、[Show Rule]、および [Show Details] オプションの中から選択できます。このペインの下部には、それぞれの重大度に関連付けられている色分けされたアイコンのリストが表示されます。重大度の詳細については、第 15 章「ロギングの設定」を参照してください。

フィールド

- [Pause]：Real-time Log Viewer のスクロールを一時停止します。
- [Copy]：選択したメッセージをコピーします。
- [Save]：コンピュータにログを保存します。

- [Clear]：メッセージのリストをクリアします。
- [Color Settings]：さまざまな重大度のメッセージを異なる色で表示することを指定できます。
- [Create Rule]：メッセージを最初に作成したアクセス コントロール ルールと逆のアクションを実行するアクセス コントロール ルールを作成できます。
- [Show Rule]：選択したメッセージを作成したアクセス コントロール ルールを表示します。この機能は、システム ログ メッセージ ID 106100 および 106023 にだけ適用されます。
- [Show Details]：[Explanation] タブ、[Recommended Action] タブ、および [Details] タブを表示または非表示にします。[Explanation] タブには、メッセージ構文、メッセージの説明、および推奨される修正処置（ある場合）が表示されます。[Recommended Action] タブでは、このメッセージを受け取った際に実行する手順が説明されています。[Details] タブには、日付、時刻、重大度、syslog ID、送信元の IP アドレス、宛先の IP アドレス、およびメッセージの説明が表示されます。
- [Find]：ログで検索するテキストを入力します。入力したテキストに基づいてメッセージを検索します。
- [Help]：詳細情報を表示します。
- [Filter By]：メッセージのフィルタ条件になるテキストを入力できます。Enter を押すか、または [Filter] をクリックして、表示されたログ メッセージにフィルタを適用します。
- [Show All]：すべてのメッセージを表示します。フィルタは、表示から除外されます。このボタンは、表示されたログ メッセージにフィルタが適用されている場合にだけアクティブになります。
- [Filter]：表示されたメッセージにフィルタを適用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 42

Trend Micro Content Security のモニタリング

ASDM では、CSC SSM の統計情報や CSC SSM 関連の機能を監視できます。

CSC SSM の概要については、CSC SSM についてを参照してください。

（注） [Configuration] > [Trend Micro Content Security] > [CSC Setup] で [CSC Setup Wizard] を完了していないと、[Monitoring] > [Trend Micro Content Security] のペインにアクセスできません。その代わりに、ダイアログボックスが表示され、[Monitoring] > [Trend Micro Content Security] から [CSC Setup Wizard] に直接アクセスできます。

Threats

[Threats] ペインでは、CSC SSM によって検出されたさまざまなタイプの脅威に関する情報がグラフで表示されます。1 つのフレームに最大で 4 つのグラフを表示できます。このペインにアクセスするには、[Monitoring] > [Trend Micro Content Security] > [Threats] を選択します。

フィールド

- [Available Graphs]：統計情報をグラフで表示できるコンポーネントを一覧表示します。グラフには、10 秒間隔でリアルタイム データが表示されます。
  - [Viruses detected]：検出されたウイルスに関する統計情報を表示します。
  - [URL Filtered, URL Blocked]：フィルタリングおよびブロックされた URL の統計情報を表示します。
  - [Spam detected]：検出されたスパム電子メールに関する統計情報を表示します。
  - [Spyware blocked]：ブロックされたスパイウェアに関する統計情報を表示します。
- [Graph Window Title]：統計タイプを追加するグラフ ウィンドウ名を表示します。すでにグラフ ウィンドウを開いている場合は、デフォルトで新しいグラフ ウィンドウが一覧表示されます。すでに開いているグラフに統計タイプを追加するには、開いているグラフ ウィンドウの名前を選択します。グラフ ウィンドウにすでに含まれている統計情報は、[Selected Graphs] リストに表示されます。ここでタイプを追加できます（1 つのウィンドウに最大 4 つ）。
- [Add]：[Available Graphs For] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択した統計タイプを削除するには、このフィールドをクリックします。

- [Show Graphs]：新しいウィンドウを表示してその [Graph] タブに選択した統計情報の最新のグラフを表示する場合にクリックします。同じ情報を表形式で表示するには、[Table] タブをクリックします。
- グラフまたは表形式の情報をローカル PC にファイルとして保存するには、[Graph] タブまたは [Table] タブで、メニューバーの [Export] をクリックするか、[File] > [Export] を選択します。
- ウィンドウに表示されている情報を印刷するには、[Graph] タブまたは [Table] タブで、メニューバーの [Print] をクリックするか、[File] > [Print] を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

CSC SSM の管理を参照してください。

Live Security Events

[Live Security Events] ペインを使用して、別のウィンドウにライブかつリアルタイムのセキュリティ イベントを表示します。このペインにアクセスするには、[Monitoring] > [Trend Micro Content Security] > [Live Security Events] を選択します。

フィールド

- [Buffer Limit]：表示するログ メッセージの最大数を表示します。デフォルトは 1000 です。
- [View]：イベント メッセージ ログを表示する別のウィンドウを開きます。着信メッセージを一時停止して、メッセージ ウィンドウをクリアし、イベント メッセージを保存できます。また、メッセージ内の特定のテキストを検索することもできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

CSC SSM の管理を参照してください。

Live Security Events Log

[Live Log] ダイアログボックスでは、CSC SSM から受信したリアルタイム セキュリティ イベント メッセージを表示できます。指定したテキストに基づいてセキュリティ イベント メッセージをフィルタリングできます。このログには、Damage Cleanup Services のイベントと統計情報が含まれます。

フィールド

- [Filter By:]：ドロップダウン リストから次のいずれかを選択します。
  - [Show All]：すべてのメッセージを表示します。
  - [Filter by Text]：入力したテキストに基づいて表示するメッセージをフィルタリングできます。
- [Filter]：メッセージをフィルタリングする場合にクリックします。
- [Find Messages]：ユーザが入力したテキストに基づいてメッセージを検索します。
  - [Text]：メッセージ ログで検索するテキストを入力します。
  - [Find]：このフィールドに入力したテキストに一致する次のエントリを検索する場合にクリックします。
- [Columns]：次の、読み取り専用カラムを表示します。
  - [Time]：イベントの発生時刻を表示します。
  - [Source]：脅威が検出された IP アドレスまたはホスト名を表示します。
  - [Threat/Filter]：脅威のタイプ、または、URL フィルタリング イベントの場合は、イベントをトリガーしたフィルタを表示します。
  - [Subject/File/URL]：脅威が含まれる電子メールの件名、脅威が含まれる FTP ファイルの名前、またはブロックされたかフィルタリングされた URL を表示します。
  - [Receiver/Host]：脅威が含まれる電子メールの宛先、または脅威にさらされたノードの IP アドレスかホスト名を表示します。
  - [Sender]：脅威が含まれる電子メールの送信者を表示します。
  - [Content Action]：添付ファイルのクリーニングや削除など、メッセージの内容に対して実行するアクションを表示します。
  - [Msg Action]：メッセージを変更せずに配信、添付ファイルを削除してから配信、添付ファイルをクリーニングしてから配信など、メッセージに対して実行するアクションを表示します。
- [Pause]：Live Security Events ログのスクロールを一時停止する場合にクリックします。
- [Save]：ログを PC のファイルに保存する場合にクリックします。
- [Clear Display]：メッセージのリストを削除する場合にクリックします。
- [Close]：ペインを閉じて前の画面に戻る場合にクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

CSC SSM の管理を参照してください。

Software Updates

[Software Updates] ペインでは、CSC SSM ソフトウェアの更新に関する情報を表示します。このペインは 10 秒ごとに自動的に更新されます。このペインにアクセスするには、[Monitoring] > [Trend Micro Content Security] > [Software Updates] を選択します。

フィールド

- [Component]：アップデート可能な CSC SSM ソフトウェアのコンポーネントの名前を表示します。
- [Version]：対応するコンポーネントの現在のバージョンを表示します。
- [Last Update]：対応するコンポーネントが最後にアップデートされた日付と時刻を表示します。CSC SSM ソフトウェアをインストールしてからコンポーネントをアップデートしたことがなければ、このカラムに「None」と表示されます。
- [Last Refresh]：ASDM でソフトウェア アップデートについて CSC SSM から情報を最後に受け取った日付と時刻を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

CSC SSM の管理を参照してください。

Resource Graphs

適応型セキュリティ アプライアンスでは、CPU リソースとメモリの使用状況など、CSC SSM のステータスを監視できます。

- 「CSC CPU」（P.42-4）
- 「CSC Memory」（P.42-5）

CSC CPU

[CSC CPU] ペインでは、CSC SSM での CPU 使用状況に関する情報をグラフで表示できます。このペインにアクセスするには、[Monitoring] > [Trend Micro Content Security] > [Resource Graphs] > [CSC CPU] を選択します。

フィールド

- [Available Graphs]：統計情報をグラフで表示できるコンポーネントを一覧表示します。
  - [CSC CPU, CPU Utilization]：CSC SSM での CPU の使用状況に関する統計情報を表示します。
- [Graph Window Title]：統計タイプを追加するグラフ ウィンドウ名を表示します。すでにグラフ ウィンドウを開いている場合は、デフォルトで新しいグラフ ウィンドウが一覧表示されます。すでに開いているグラフに統計タイプを追加するには、開いているグラフ ウィンドウの名前を選択します。グラフ ウィンドウにすでに含まれている統計情報は、[Selected Graphs] リストに表示されます。ここでタイプを追加できます（1 つのウィンドウに最大 4 つ）。
- [Add]：[Available Graphs For] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択した統計タイプを削除するには、このフィールドをクリックします。
- [Show Graphs]：新しいウィンドウを表示してその [Graph] タブに選択した統計情報の最新のグラフを表示する場合にクリックします。同じ情報を表形式で表示するには、[Table] タブをクリックします。
- グラフまたは表形式の情報をローカル PC にファイルとして保存するには、[Graph] タブまたは [Table] タブで、メニューバーの [Export] をクリックするか、[File] > [Export] を選択します。
- ウィンドウに表示されている情報を印刷するには、[Graph] タブまたは [Table] タブで、メニューバーの [Print] をクリックするか、[File] > [Print] を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

CSC SSM の管理を参照してください。

CSC Memory

[CSC Memory] ペインでは、CSC SSM でのメモリ使用状況に関する情報をグラフで表示できます。このペインにアクセスするには、[Monitoring] > [Trend Micro Content Security] > [Resource Graphs] > [CSC Memory] を選択します。

フィールド

- [Available Graphs]：統計情報をグラフで表示できるコンポーネントを一覧表示します。
  - [Free Memory]：使用していないメモリの量に関する統計情報を表示します。
  - [Used Memory]：使用中のメモリの量に関する統計情報を表示します。

- [Graph Window Title]：統計タイプを追加するグラフ ウィンドウ名を表示します。すでにグラフ ウィンドウを開いている場合は、デフォルトで新しいグラフ ウィンドウが一覧表示されます。すでに開いているグラフに統計タイプを追加するには、開いているグラフ ウィンドウの名前を選択します。グラフ ウィンドウにすでに含まれている統計情報は、[Selected Graphs] リストに表示されます。ここでタイプを追加できます（1 つのウィンドウに最大 4 つ）。
- [Add]：[Available Graphs For] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択した統計タイプを削除するには、このフィールドをクリックします。
- [Show Graphs]：新しいウィンドウを表示してその [Graph] タブに選択した統計情報の最新のグラフを表示する場合にクリックします。同じ情報を表形式で表示するには、[Table] タブをクリックします。
- グラフまたは表形式の情報をローカル PC にファイルとして保存するには、[Graph] タブまたは [Table] タブで、メニューバーの [Export] をクリックするか、[File] > [Export] を選択します。
- ウィンドウに表示されている情報を印刷するには、[Graph] タブまたは [Table] タブで、メニューバーの [Print] をクリックするか、[File] > [Print] を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

CSC SSM の管理を参照してください。

CHAPTER 43

フェールオーバー動作のモニタ

ASDM でのフェールオーバーのモニタリングは、デバイスのモードによって異なります。シングルコンテキスト モード、またはマルチ コンテキスト モードのセキュリティ コンテキスト内では、デバイスのフェールオーバーの状態を監視し、ステートフル フェールオーバーの統計情報を表示できます。マルチ コンテキスト モードのシステム実行スペースでは、フェールオーバー グループごとのフェールオーバー状態を監視できます。

各システム コンフィギュレーションでのフェールオーバーのモニタリングに関する詳細については、次の項目を参照してください。

- 「シングルコンテキスト モードまたはセキュリティ コンテキストでのフェールオーバーのモニタリング」（P.43-1）
- 「システム実行スペースでのフェールオーバーのモニタリング」（P.43-6）

シングルコンテキスト モードまたはセキュリティ コンテキストでのフェールオーバーのモニタリング

[Monitoring] > [Properties] > [Failover] 領域で、フェールオーバー ペアのアクティブ デバイスおよびスタンバイ デバイスのステータスと、フェールオーバー関連の統計情報を監視できます。詳細については、次の画面を参照してください。

- Status：デバイスのフェールオーバー ステータスを表示します。
- Graphs：さまざまなフェールオーバー通信統計情報のグラフを表示します。

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Status

[Status] ペインには、システムのフェールオーバー状態が表示されます。シングルコンテキスト モードでは、システムのフェールオーバー状態を次の方法で制御できます。

- デバイスのアクティブ/スタンバイ状態を切り替える。
- 障害が発生したデバイスをリセットする。
- スタンバイ装置をリロードする。

マルチ コンテキスト モードでは、これらの設定値をシステム実行スペースで制御できます。「システム実行スペースでのフェールオーバーのモニタリング」（P.43-6）を参照してください。

フィールド

[Failover state of the system]：*表示専用*。セキュリティ アプライアンスのフェールオーバー状態を表示します。このフィールドの情報は、show failover コマンドで受け取る出力と同じです。次の情報が含まれます。

（注） セキュリティ コンテキスト内でフェールオーバー ステータスを表示すると、次のフィールドのサブセットだけが表示されます。これらのフィールドには、フィールド名の前にアスタリスク（*）が付きます。

- *[Failover]：フェールオーバーがイネーブルの場合は「On」が、イネーブルでない場合は「Off」が表示されます。
- [Cable Status]：（PIX セキュリティ アプライアンス プラットフォームだけ）シリアル フェールオーバー ケーブルのステータスを表示します。ケーブルのステータスには次のものがあります。
  - [Normal]：ケーブルは両方の装置に接続されており、両方の装置とも電源が入っています。
  - [My side not connected]：シリアル ケーブルがこの装置に接続されていません。ケーブルがもう一方の装置に接続されているかどうかは不明です。
  - [Other side is not connected]：シリアル ケーブルはこの装置に接続されていますが、もう一方の装置には接続されていません。
  - [Other side powered off]：相手装置の電源がオフになっています。
  - [N/A]：LAN ベースのフェールオーバーはイネーブルです。
- [Failover unit]：フェールオーバー ペアにおけるシステムの役割を「Primary」または「Secondary」のいずれかで表示します。
- [Failover LAN Interface]：LAN フェールオーバー インターフェイスの論理名および物理名を表示します。PIX プラットフォームで専用のフェールオーバー ケーブルを使用している場合、このフィールドに「N/A - Serial-based failover enabled」と表示されます。フェールオーバー インターフェイスを設定していない場合、このフィールドに「Not configured」と表示されます。
- [Unit Poll frequency/holdtime]：フェールオーバー リンクに送信される hello メッセージの頻度、および hello メッセージを受信していないときにピアの障害テストを実行するまでに待機する時間を表示します。
- [Interface Poll frequency]：監視対象インターフェイスでの hello メッセージの間隔を秒数で表示します。
- [Interface Policy]：インターフェイスの数を表示します。この数を超えたインターフェイスが故障すると、フェールオーバーがトリガーされます。
- [Monitored Interfaces]：フェールオーバーを監視しているヘルスのあるインターフェイスの数を表示します。
- [failover replication http]：HTTP の複製がイネーブルになっている場合に表示されます。
- *[Last Failover]：最後にフェールオーバーが発生した日付と時刻を表示します。
- *[This Host(Context)/Other Host(Context)]：フェールオーバー ペアの各ホスト（または、マルチコンテキスト モードで選択したコンテキスト）について、次の情報が表示されます。
  - [Primary or Secondary]：装置がプライマリ装置か、セカンダリ装置かを表示します。また、次のステータスも表示されます。

    *[Active]：装置はアクティブ装置です。

    *[Standby]：装置はスタンバイ装置です。

*[Disabled]：装置のフェールオーバーがディセーブルになっているか、フェールオーバー リンクが設定されていません。

*[Listen]：装置によって、ポーリング メッセージのリッスンによるアクティブ装置の検出が試行中です。

*[Learn]：装置によってアクティブ装置が検出されましたが、スタンバイ モードに移る前のコンフィギュレーションの同期化は行われていません。

*[Failed]：装置に障害が発生しています。

- *[Active Time]：装置がアクティブ状態になってからの時間（秒数）を示します。
- *[[context_name] Interface name (n.n.n.n)]：インターフェイスごとに、各装置で現在使用されている IP アドレス、および次の状態のいずれかが表示されます。マルチ コンテキスト モードでは、各インターフェイスの前にコンテキスト名が表示されます。

  [Failed]：インターフェイスに障害が発生しています。

  [Link Down]：インターフェイスの回線プロトコルがダウンしています。

  [Normal]：インターフェイスは正常に動作しています。

  [No Link]：インターフェイスは管理上シャットダウンされました。

  [Unknown]：セキュリティ アプライアンスがインターフェイスのステータスを判別できません。

  [(Waiting)]：インターフェイスは、相手装置からポーリング メッセージを受信していません。

  [Testing]：インターフェイスはテスト中です。

*[Stateful Failover Logical Updates Statistics]：次のフィールドは、ステートフル フェールオーバー機能に関連したものです。[Link] フィールドにインターフェイス名が表示されている場合は、ステートフル フェールオーバー統計情報が表示されます。

（注） ステートフル フェールオーバーは、ASA 5505 シリーズ適応型セキュリティ アプライアンスではサポートされていません。これらの統計情報は、ASA 5505 セキュリティ アプライアンスで実行されている ASDM には表示されません。

- [Link]：次のいずれかが表示されます。
  - [interface_name]：ステートフル フェールオーバー リンクに使用するインターフェイス。
  - [Unconfigured]：ステートフル フェールオーバーが使用されていません。
- [Stateful Obj]：各フィールド型に関して、次の統計情報が表示されます。

  [xmit]：他方の装置への送信パケット数

  [xerr]：他方の装置へのパケット送信中に発生したエラー数

  [rcv]：受信パケット数

  [rerr]：他方の装置からのパケット受信中に発生したエラー数

  ステートフル オブジェクトのフィールド型は次のとおりです。
  - [General]：ステートフル オブジェクトの総数。
  - [sys cmd]：論理更新システム コマンド（LOGIN、Stay Alive など）。
  - [up time]：アップ タイム（アクティブ装置がスタンバイ装置に渡す値）。
  - [RPC services]：リモート プロシージャ コール接続情報。
  - [TCP conn]：TCP 接続の情報。

  - [UDP conn]：ダイナミック UDP 接続情報。
  - [ARP tbl]：ダイナミック ARP テーブル情報。
  - [L2BRIDGE tbl]：レイヤ 2 ブリッジ テーブルの情報（トランスペアレント ファイアウォール モードだけ）。
  - [Xlate_Timeout]：接続変換タイムアウト情報を示します。
  - [VPN IKE upd]：IKE 接続情報。
  - [VPN IPSEC upd]：IPSec 接続情報。
  - [VPN CTCP upd]：cTCP トンネル接続情報。
  - [VPN SDI upd]：SDI AAA 接続情報。
  - [VPN DHCP upd]：トンネル型 DHCP 接続情報。
- *[Logical Update Queue Information]：次の統計情報を表示します。
  - [Recv Q]：受信キューのステータス。
  - [Xmit Q]：送信キューのステータス。

  各キューに対して、次の情報が表示されます。
  - [Cur]：キューの現在のパケット数。
  - [Max]：パケットの最大数。
  - [Total]：パケットの合計数。

*[Lan-based Failover is active]：このフィールドは、LAN ベースのフェールオーバーがイネーブルの場合にだけ表示されます。

- [interface name (n.n.n.n) and peer (n.n.n.n)]：各装置で現在使用されているフェールオーバー リンクの名前と IP アドレス。

[Status] ペインでは、次のアクションを使用できます。

- [Make Active]：（シングル モードだけで使用可能）このボタンをクリックして、アクティブ/スタンバイ コンフィギュレーションでセキュリティ アプライアンスをアクティブ装置にします。
- [Make Standby]：（シングル モードだけで使用可能）このボタンをクリックして、アクティブ/スタンバイ ペアでセキュリティ アプライアンスをスタンバイ装置にします。
- [Reset Failover]：（シングル モードだけで使用可能）このボタンをクリックして、システムを障害状態からスタンバイ状態にリセットします。システムをアクティブ状態にはリセットできません。アクティブ装置でこのボタンをクリックすると、スタンバイ装置がリセットされます。
- [Reload Standby]：（シングル モードだけで使用可能）このボタンをクリックして、スタンバイ装置を強制的にリロードします。
- [Refresh]：このボタンをクリックして、[system] フィールドのフェールオーバー状態にあるステータス情報をリフレッシュします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Graphs

[Graphs] ペインでは、フェールオーバーの統計情報をグラフ形式またはテーブル形式で表示できます。マルチ コンテキスト モードでは、[Graphs] ペインは管理コンテキストでだけ使用できます。

グラフの情報は、ステートフル フェールオーバーだけに関連します。

フィールド

- [Available Graphs for]：モニタリングに使用可能な統計情報のタイプを一覧表示します。1 つのグラフ ウィンドウに表示する統計タイプを 4 つまで選択できます。このフィールドで統計タイプをダブルクリックすると、その統計タイプが [Selected Graphs] フィールドに移動します。このフィールドで統計タイプを一回クリックすると、エントリが選択されます。複数のエントリを選択できます。

  グラフ ウィンドウで、次の統計タイプをグラフ形式またはテーブル形式で使用できます。これらの統計タイプでは、フェールオーバー ペアで相手装置と送受信するパケット数を表示します。

  - [RPC services information]：セキュリティ アプライアンスの RPC サービス情報を表示します。
  - [TCP Connection Information]：セキュリティ アプライアンスの TCP 接続情報を表示します。
  - [UDP Connection Information]：セキュリティ アプライアンスの UDP 接続情報を表示します。
  - [ARP Table Information]：セキュリティ アプライアンスの ARP テーブル情報を表示します。
  - [L2Bridge Table Information]：（トランスペアレント ファイアウォール モードだけ）レイヤ 2 ブリッジ テーブルのパケット数を表示します。
  - [Xmit Queue]：（シングル モードだけ）送信されたパケットの現在の数、最大数、および合計数を表示します。
  - [Receive Queue]：（シングル モードだけ）受信されたパケットの現在の数、最大数、および合計数を表示します。
- [Graph Window]：統計タイプを追加するグラフ ウィンドウ名を表示します。すでにグラフ ウィンドウを開いている場合は、デフォルトで新しいグラフ ウィンドウがリストされます。すでに開いているグラフに統計タイプを追加する場合は、開いているグラフ ウィンドウの名前を選択します。グラフ ウィンドウにすでに含まれている統計情報は、[Selected Graphs] フィールドに表示されます。ここでタイプを追加できます（1 つのウィンドウに最大 4 つ）。
- [Add]：このボタンをクリックして、[Available Graphs for] フィールドで選択したエントリを [Selected Graphs] フィールドに移動します。
- [Remove]：[Selected Graphs] フィールドから、選択した統計タイプを削除します。

- [Selected Graphs]：選択したグラフ ウィンドウに表示する統計タイプを表示します。表示できるタイプは 4 つまでです。このフィールドで統計タイプをダブルクリックすると、選択した統計タイプがフィールドから削除されます。このフィールドで統計タイプを一回クリックすると、統計タイプが選択されます。複数の統計タイプを選択できます。
- [Show Graphs]：このボタンをクリックして、新しいグラフ ウィンドウ、または更新したグラフ ウィンドウに選択した統計情報を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

システム実行スペースでのフェールオーバーのモニタリング

システム コンテキストのシステムおよび個々のフェールオーバー グループのフェールオーバー ステータスを監視できます。システム コンテキストからのフェールオーバー ステータスの監視については、次の項目を参照してください。

- System
- [Failover Group 1] と [Failover Group 2]

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

System

[System] ペインには、システムのフェールオーバー状態が表示されます。また、システムのフェールオーバー状態を次の方法で制御できます。

- デバイスのアクティブ/スタンバイ状態を切り替える。
- 障害が発生したデバイスをリセットする。
- スタンバイ装置をリロードする。

フィールド

[Failover state of the system]：*表示専用*。セキュリティ アプライアンスのフェールオーバー状態を表示します。表示される情報は、**show failover** コマンドで受け取る出力と同じです。次の情報が含まれます。

- [Failover]：フェールオーバーがイネーブルの場合は「On」が、イネーブルでない場合は「Off」が表示されます。
- [Cable Status]：（PIX セキュリティ アプライアンス プラットフォームだけ）シリアル フェールオーバー ケーブルのステータスを表示します。ケーブルのステータスには次のものがあります。
  - [Normal]：ケーブルは両方の装置に接続されており、両方の装置とも電源が入っています。
  - [My side not connected]：シリアル ケーブルがこの装置に接続されていません。ケーブルがもう一方の装置に接続されているかどうかは不明です。
  - [Other side is not connected]：シリアル ケーブルはこの装置に接続されていますが、もう一方の装置には接続されていません。
  - [Other side powered off]：相手装置の電源がオフになっています。
  - [N/A]：LAN ベースのフェールオーバーはイネーブルです。
- [Failover unit]：フェールオーバー ペアにおけるシステムの役割を「Primary」または「Secondary」のいずれかで表示します。
- [Failover LAN Interface]：LAN フェールオーバー インターフェイスの論理名および物理名を表示します。PIX プラットフォームで専用のフェールオーバー ケーブルを使用している場合、このフィールドに「N/A - Serial-based failover enabled」と表示されます。フェールオーバー インターフェイスを設定していない場合、このフィールドに「Not configured」と表示されます。
- [Unit Poll frequency/holdtime]：フェールオーバー リンクに送信される hello メッセージの頻度、および hello メッセージを受信していないときにピアの障害テストを実行するまでに待機する時間を表示します。
- [Interface Poll frequency]：監視対象インターフェイスでの hello メッセージの間隔を秒数で表示します。
- [Interface Policy]：インターフェイスの数を表示します。この数を超えたインターフェイスが故障すると、フェールオーバーがトリガーされます。
- [Monitored Interfaces]：フェールオーバーを監視しているヘルスのあるインターフェイスの数を表示します。
- [failover replication http]：HTTP の複製がイネーブルになっていることを示します。
- [Group x Last Failover]：各フェールオーバー グループで、最後にフェールオーバーが発生した日付と時刻を表示します。
- [This Host/Other Host]：フェールオーバー ペアの各ホストについて、次の情報が表示されます。
  - [Primary or Secondary]：装置がプライマリ装置か、セカンダリ装置かを表示します。
  - [Group x]：各フェールオーバー グループについて、次の情報が表示されます。

    [State]：Active または Standby Ready。

    [Active Time]：フェールオーバー グループがアクティブ状態にあった時間（秒数）。
  - [context_name Interface name (n.n.n.n)]：インターフェイスごとに、各装置で現在使用している IP アドレス、および次の状態のいずれかが表示されます。

    [Failed]：インターフェイスに障害が発生しています。

    [Link Down]：インターフェイスの回線プロトコルがダウンしています。

    [Normal]：インターフェイスは正常に動作しています。

    [No Link]：インターフェイスは管理上シャットダウンされました。

    [Unknown]：セキュリティ アプライアンスがインターフェイスのステータスを判別できません。

[(Waiting)]：インターフェイスは、相手装置からポーリング メッセージを受信していません。

[Testing]：インターフェイスはテスト中です。

[Stateful Failover Logical Updates Statistics]：次のフィールドは、ステートフル フェールオーバー機能に関連したものです。[Link] フィールドにインターフェイス名が表示されている場合は、ステートフル フェールオーバー統計情報が表示されます。

（注）　ステートフル フェールオーバーは、ASA 5505 シリーズ適応型セキュリティ アプライアンスではサポートされていません。これらの統計情報は、ASA 5505 セキュリティ アプライアンスで実行されている ASDM には表示されません。

- [Link]：次のいずれかが表示されます。
  - [*interface_name*]：ステートフル フェールオーバー リンクに使用されているインターフェイスです。
  - [Unconfigured]：ステートフル フェールオーバーが使用されていません。
- [Stateful Obj]：各フィールド型に関して、次の統計情報が表示されます。

  [xmit]：他方の装置への送信パケット数

  [xerr]：他方の装置へのパケット送信中に発生したエラー数

  [rcv]：受信パケット数

  [rerr]：他方の装置からのパケット受信中に発生したエラー数

  ステートフル オブジェクトのフィールド型は次のとおりです。
  - [General]：ステートフル オブジェクトの総数。
  - [sys cmd]：論理更新システム コマンド（LOGIN、Stay Alive など）。
  - [up time]：アップ タイム（アクティブ装置がスタンバイ装置に渡す値）。
  - [RPC services]：リモート プロシージャ コール接続情報。
  - [TCP conn]：TCP 接続の情報。
  - [UDP conn]：ダイナミック UDP 接続情報。
  - [ARP tbl]：ダイナミック ARP テーブル情報。
  - [L2BRIDGE tbl]：レイヤ 2 ブリッジ テーブルの情報（トランスペアレント ファイアウォール モードだけ）。
  - [Xlate_Timeout]：接続変換タイムアウト情報を示します。
  - [VPN IKE upd]：IKE 接続情報。
  - [VPN IPSEC upd]：IPSec 接続情報。
  - [VPN CTCP upd]：cTCP トンネル接続情報。
  - [VPN SDI upd]：SDI AAA 接続情報。
  - [VPN DHCP upd]：トンネル型 DHCP 接続情報。
- [Logical Update Queue Information]：次の統計情報を表示します。
  - [Recv Q]：受信キューのステータス。
  - [Xmit Q]：送信キューのステータス。

  各キューに対して、次の情報が表示されます。
  - [Cur]：キューの現在のパケット数。

- [Max]：パケットの最大数。
- [Total]：パケットの合計数。

[Lan-based Failover is active]：このフィールドは、LAN ベースのフェールオーバーがイネーブルの場合にだけ表示されます。

- [interface *name* (*n.n.n.n*) and peer (*n.n.n.n*)]：各装置で現在使用されているフェールオーバー リンクの名前と IP アドレス。

[System] ペインでは、次のアクションを使用できます。

- [Make Active]：このボタンをクリックして、アクティブ/スタンバイ コンフィギュレーションでセキュリティ アプライアンスをアクティブ装置にします。アクティブ/アクティブ コンフィギュレーションで、このボタンをクリックすると、セキュリティ アプライアンスで両方のフェールオーバー グループがアクティブになります。
- [Make Standby]：このボタンをクリックして、アクティブ/スタンバイ ペアでセキュリティ アプライアンスをスタンバイ装置にします。アクティブ/アクティブ コンフィギュレーションで、このボタンをクリックすると、セキュリティ アプライアンスで両方のフェールオーバー グループがスタンバイ状態になります。
- [Reset Failover]：このボタンをクリックして、システムを障害状態からスタンバイ状態にリセットします。システムをアクティブ状態にはリセットできません。アクティブ装置でこのボタンをクリックすると、スタンバイ装置がリセットされます。
- [Reload Standby]：このボタンをクリックして、スタンバイ装置を強制的にリロードします。
- [Refresh]：このボタンをクリックして、[system] フィールドのフェールオーバー状態にあるステータス情報をリフレッシュします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover Group 1] と [Failover Group 2]

[Failover Group 1] ペインおよび [Failover Group 2] ペインには、選択したグループのフェールオーバー状態が表示されます。また、グループのアクティブ/スタンバイ状態を切り替えるか、または障害が発生したグループをリセットして、グループのフェールオーバー状態を制御することもできます。

フィールド

[Failover state of Group[*x*]]：*表示専用*。選択したフェールオーバー グループのフェールオーバー状態を表示します。表示される情報は、**show failover group** コマンドで受け取る出力と同じです。次の情報が含まれます。

- [Last Failover]：最後のフェールオーバーの日付と時刻。

- [This Host/Other Host]：フェールオーバー ペアの各ホストについて、次の情報が表示されます。
  - [Primary or Secondary]：装置がプライマリ装置か、セカンダリ装置かを表示します。フェールオーバー グループについて次の情報も表示されます。

    [Active]：指定した装置でフェールオーバー グループがアクティブです。

    [Standby]：指定した装置でフェールオーバー グループがスタンバイ状態です。

    [Disabled]：装置のフェールオーバーがディセーブルになっているか、フェールオーバー リンクが設定されていません。

    [Listen]：装置によって、ポーリング メッセージのリッスンによるアクティブ装置の検出が試行中です。

    [Learn]：装置によってアクティブ装置が検出されましたが、スタンバイ モードに移る前のコンフィギュレーションの同期化は行われていません。

    [Failed]：指定した装置でフェールオーバー グループが障害状態です。
  - [Active Time]：指定した装置でフェールオーバー グループがアクティブ状態にあった時間（秒数）。
  - [*context_name* Interface *name* (n.n.n.n)]：選択したフェールオーバー グループのインターフェイスごとに、そのグループが所属するコンテキストと、各装置で現在使用されている IP アドレス、および次のいずれかの状態が表示されます。

    [Failed]：インターフェイスに障害が発生しています。

    [Link Down]：インターフェイスの回線プロトコルがダウンしています。

    [Normal]：インターフェイスは正常に動作しています。

    [No Link]：インターフェイスは管理上シャットダウンされました。

    [Unknown]：セキュリティ アプライアンスがインターフェイスのステータスを判別できません。

    [(Waiting)]：インターフェイスは、相手装置からポーリング メッセージを受信していません。

    [Testing]：インターフェイスはテスト中です。
- [Stateful Failover Logical Updates Statistics]：次のフィールドは、ステートフル フェールオーバー機能に関連したものです。[Link] フィールドにインターフェイス名が表示されている場合は、ステートフル フェールオーバー統計情報が表示されます。

  [Link]：次のいずれかが表示されます。
  - [*interface_name*]：ステートフル フェールオーバー リンクに使用されているインターフェイスです。
  - [Unconfigured]：ステートフル フェールオーバーが使用されていません。

  [Stateful Obj]：各フィールド型に関して、次の統計情報が表示されます。
  - [xmit]：他方の装置への送信パケット数
  - [xerr]：他方の装置へのパケット送信中に発生したエラー数
  - [rcv]：受信パケット数
  - [rerr]：他方の装置からのパケット受信中に発生したエラー数

  ステートフル オブジェクトのフィールド型は次のとおりです。
  - [General]：ステートフル オブジェクトの総数。
  - [sys cmd]：論理更新システム コマンド（LOGIN、Stay Alive など）。
  - [up time]：アップ タイム（アクティブ装置がスタンバイ装置に渡す値）。

  - [RPC services]：リモート プロシージャ コール接続情報。
  - [TCP conn]：TCP 接続の情報。
  - [UDP conn]：ダイナミック UDP 接続情報。
  - [ARP tbl]：ダイナミック ARP テーブル情報。
  - [L2BRIDGE tbl]：レイヤ 2 ブリッジ テーブルの情報（トランスペアレント ファイアウォール モードだけ）。
  - [Xlate_Timeout]：接続変換タイムアウト情報を示します。
  - [IKE upd]：IKE 接続の情報。
  - [VPN IPSEC upd]：IPSec 接続情報。
  - [VPN CTCP upd]：cTCP トンネル接続情報。
  - [VPN SDI upd]：SDI AAA 接続情報。
  - [VPN DHCP upd]：トンネル型 DHCP 接続情報。
- [Logical Update Queue Information]：次の統計情報を表示します。
  - [Recv Q]：受信キューのステータス。
  - [Xmit Q]：送信キューのステータス。

  各キューに対して、次の情報が表示されます。
  - [Cur]：キューの現在のパケット数。
  - [Max]：パケットの最大数。
  - [Total]：パケットの合計数。

このペインで次のアクションを実行できます。

- [Make Active]：このボタンをクリックして、セキュリティ アプライアンスでフェールオーバー グループをアクティブ装置にします。
- [Make Standby]：このボタンをクリックして、セキュリティ アプライアンスでフェールオーバー グループを強制的にスタンバイ状態にします。
- [Reset Failover]：このボタンをクリックして、システムを障害状態からスタンバイ状態にリセットします。システムをアクティブ状態にはリセットできません。アクティブ装置でこのボタンをクリックすると、スタンバイ装置がリセットされます。
- [Refresh]：このボタンをクリックして、[system] フィールドのフェールオーバー状態にあるステータス情報をリフレッシュします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

CHAPTER 44

インターフェイスのモニタリング

ASDM では、インターフェイスの統計情報やインターフェイス関連の機能を監視できます。

ARP テーブル

[ARP Table] ペインには、スタティック エントリやダイナミック エントリを含む ARP テーブルが表示されます。ARP テーブルには、MAC アドレスを所定のインターフェイスの IP アドレスにマッピングするエントリが含まれます。ARP テーブルの詳細については、[Configuration] > [Properties] > ARP Static Table を参照してください。

フィールド

- [Interface]：マッピングに関連付けられているインターフェイス名を一覧表示します。
- [IP Address]：IP アドレスを表示します。
- [MAC Address]：MAC アドレスを表示します。
- [Proxy ARP]：インターフェイスでプロキシ ARP がイネーブルになっている場合は Yes と表示します。インターフェイスでプロキシ ARP がイネーブルになっていない場合は No と表示します。
- [Clear]：ダイナミック ARP テーブルのエントリをクリアします。スタティック エントリはクリアされません。
- [Refresh]：セキュリティ アプライアンスの現在の情報でテーブルをリフレッシュし、[Last Updated] の日付と時刻を更新します。
- [Last Updated]：*表示専用*。表示が更新された日付と時刻を示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

DHCP

セキュリティ アプライアンスでは、クライアントに割り当てられているアドレス、セキュリティ アプライアンス インターフェイスのリース情報、および DHCP 統計情報を含む DHCP の統計情報を監視できます。

DHCP Server Table

[DHCP Server Table] には、DHCP クライアントに割り当てられている IP アドレスが一覧表示されます。

フィールド

- [IP Address]：クライアントに割り当てられている IP アドレスを表示します。
- [Client-ID]：クライアントの MAC アドレスまたは ID を表示します。
- [Lease Expiration]：DHCP リースの期限が満了する日付を表示します。リースは、クライアントが割り当てられている IP アドレスを使用できる期間を示します。また、残り時間は、[Last Updated] 表示専用フィールドのタイムスタンプを基準に秒数で表示されます。
- [Number of Active Leases]：DHCP リースの合計数を表示します。
- [Refresh]：セキュリティ アプライアンスの情報をリフレッシュします。
- [Last Updated]：テーブルのデータが最後に更新された日付を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

DHCP Client Lease Information

DHCP サーバからセキュリティ アプライアンス インターフェイスの IP アドレスを取得すると、[DHCP Client Lease Information] パネルに、DHCP リースに関する情報が表示されます。

フィールド

- [Select an interface]：セキュリティ アプライアンスのインターフェイスを一覧表示します。DHCP リースを表示するインターフェイスを選択します。インターフェイスに DHCP リースが複数ある場合、表示するインターフェイスと IP アドレスのペアを選択します。
- [Attribute and Value]：インターフェイス DHCP リースの属性と値を一覧表示します。
  - [Temp IP addr]：*表示専用*。インターフェイスに割り当てられている IP アドレス。
  - [Temp sub net mask]：*表示専用*。インターフェイスに割り当てられているサブネット マスク。
  - [DHCP lease server]：*表示専用*。DHCP サーバ アドレス。

- [state]：*表示専用*。DHCP リースの状態で、次のとおりです。

  [Initial]：セキュリティ アプライアンスがリースの取得プロセスを開始する初期化状態。この状態は、リースが終了したか、リースのネゴシエーションに失敗したときにも表示されます。

  [Selecting]：セキュリティ アプライアンスは、1 つ以上の DHCP サーバからの DHCPOFFER メッセージの受信を待っているため、1 つ選択できます。

  [Requesting]：セキュリティ アプライアンスは、要求を送信したサーバからの応答を待っています。

  [Purging]：セキュリティ アプライアンスは、エラーが発生したためリースを削除しています。

  [Bound]：セキュリティ アプライアンスには、有効なリースがあり、正常に動作しています。

  [Renewing]：セキュリティ アプライアンスは、リースを更新しようとしています。DHCPREQUEST メッセージを現在の DHCP サーバに定期的に送信し、応答を待機します。

  [Rebinding]：セキュリティ アプライアンスは、元のサーバでリースを更新できなかったため、いずれかのサーバから応答を得るかリースが終了するまで DHCPREQUEST メッセージを送信します。

  [Holddown]：セキュリティ アプライアンスは、リースを削除するプロセスを開始しました。

  [Releasing]：セキュリティ アプライアンスは、IP アドレスが不要になったことを示すリース メッセージをサーバに送信します。

- [Lease]：*表示専用*。DHCP サーバによって指定される、インターフェイスがこの IP アドレスを使用できる時間の長さ。
- [Renewal]：*表示専用*。インターフェイスがこのリースを自動的に更新しようとするまでの時間の長さ。
- [Rebind]：*表示専用*。セキュリティ アプライアンスが、DHCP サーバへのリバインドを試みるまでの時間。リバインドは、セキュリティ アプライアンスが元の DHCP サーバと通信できず、リース期間の 87.5 % を過ぎているときに実行されます。セキュリティ アプライアンスは、DHCP 要求をブロードキャストすることで、使用可能な DHCP サーバにアクセスしようとします。
- [Next timer fires after]：*表示専用*。内部タイマーがトリガーするまでの秒数。
- [Retry count]：*表示専用*。セキュリティ アプライアンスがリースを確立しようとしている場合、このフィールドに、セキュリティ アプライアンスが DHCP メッセージを送信しようとした回数が表示されます。たとえば、セキュリティ アプライアンスが Selecting 状態にある場合、この値には、セキュリティ アプライアンスが検出メッセージを送信した回数が表示されます。また、セキュリティ アプライアンスが Requesting 状態にある場合、この値には、セキュリティ アプライアンスが要求メッセージを送信した回数が表示されます。
- [Client-ID]：*表示専用*。サーバとのすべての通信に使用したクライアント ID。
- [Proxy]：*表示専用*。このインターフェイスが VPN クライアント用のプロキシ DHCP クライアントかどうかを True または False で指定します。
- [Hostname]：*表示専用*。クライアントのホスト名。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

DHCP Statistics

[DHCP Statistics] ペインには、DHCP サーバ機能の統計情報が表示されます。

フィールド

- [Message Type]：送受信された DHCP メッセージのタイプを一覧表示します。
  - BOOTREQUEST
  - DHCPDISCOVER
  - DHCPREQUEST
  - DHCPDECLINE
  - DHCPRELEASE
  - DHCPINFORM
  - BOOTREPLY
  - DHCPOFFER
  - DHCPACK
  - DHCPNAK
- [Count]：特定のメッセージが処理された回数を表示します。
- [Direction]：メッセージ タイプが Sent か Received かを示します。
- [Total Messages Received]：セキュリティ アプライアンスで受信したメッセージの合計数を表示します。
- [Total Messages Sent]：セキュリティ アプライアンスで送信したメッセージの合計数を表示します。
- [Counter]：次のような DHCP の全般的な統計データを表示します。
  - DHCP UDP Unreachable Errors
  - DHCP Other UDP Errors
  - Address Pools
  - Automatic Bindings
  - Expired Bindings
  - Malformed Messages
- [Value]：各カウンタ項目の数を表示します。
- [Refresh]：DHCP テーブルのリストを更新します。
- [Last Updated]：テーブルのデータが最後に更新された日付を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

MAC アドレス テーブル

[MAC Address Table] ペインには、スタティックおよびダイナミック MAC アドレス エントリが表示されます。MAC アドレス テーブル、およびスタティック エントリの追加については、[Configuration] > [Properties] > [Bridging] > MAC Address Table を参照してください。

フィールド

- [Interface]：エントリに関連付けられているインターフェイス名を表示します。
- [MAC Address]：MAC アドレスを表示します。
- [Type]：エントリがスタティックかダイナミックかを表示します。
- [Age]：エントリの経過時間を分数で表示します。タイムアウトを設定するには、「MAC Address Table」を参照してください。
- [Refresh]：セキュリティ アプライアンスの現在の情報でテーブルをリフレッシュします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

Dynamic ACLs

[Dynamic ACLs] ペインには、ダイナミック ACL のテーブルが表示されます。ダイナミック ACL は、セキュリティ アプライアンスによって自動的に作成、アクティブ化、および削除される点を除いて、ユーザ設定の ACL と機能上同じです。これらの ACL はコンフィギュレーションには表示されず、このテーブルだけに表示されます。ダイナミック ACL は、ACL ヘッダーの「(dynamic)」キーワードで区別されます。

このテーブルで ACL を選択すると、その ACL の内容が下部のテキスト フィールドに表示されます。

フィールド

- [ACL]：ダイナミック ACL の名前を表示します。

- [Element Count]：ACL の要素の数を表示します。
- [Hit Count]：ACL のすべての要素に対する合計ヒット数を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Interface Graphs

[Interface Graphs] ペインでは、インターフェイスの統計情報をグラフ形式またはテーブル形式で表示できます。インターフェイスをコンテキスト間で共有している場合、セキュリティ アプライアンスには現在のコンテキストの統計情報だけが表示されます。サブインターフェイスに表示される統計情報の数は、物理インターフェイスに表示される統計情報の数のサブセットです。

フィールド

- [Available Graphs for]：モニタリングに使用可能な統計情報のタイプを一覧表示します。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。
  - [Byte Counts]：インターフェイスのバイト入力およびバイト出力の数を表示します。
  - [Packet Counts]：インターフェイスのパケット入力およびパケット出力の数を表示します。
  - [Packet Rates]：インターフェイスのパケット入力およびパケット出力のレートを表示します。
  - [Bit Rates]：インターフェイスの入出力のビット レートを表示します。
  - [Drop Packet Count]：インターフェイスでドロップされたパケットの数を表示します。

  物理インターフェイスに追加して表示できる統計情報は次のとおりです。
  - [Buffer Resources]：次の統計情報を表示します。

    [Overruns]：入力速度が、セキュリティ アプライアンスのデータ処理能力を超えたため、セキュリティ アプライアンスがハードウェア バッファに受信したデータを処理できなかった回数。

    [Underruns]：セキュリティ アプライアンスで処理できる速度より速くトランスミッタが動作した回数。

    [No Buffer]：メイン システムにバッファ スペースがなかったために廃棄された受信パケットの数。この数を、無視された数と比較してください。イーサネット ネットワーク上のブロードキャスト ストームは、多くの場合、入力バッファ イベントがないことに原因があります。
  - [Packet Errors]：次の統計情報を表示します。

    [CRC]：Cyclical Redundancy Check（CRC; 巡回冗長検査）エラーの数。ステーションがフレームを送信すると、フレームの末尾に CRC を付加します。この CRC は、フレーム内のデータに基づくアルゴリズムから生成されます。送信元と宛先の間でフレームが変更された場

合、セキュリティ アプライアンスは CRC が一致しないことを通知します。CRC の数値が高いことは、通常、コリジョンの結果であるか、ステーションが不良データを送信することが原因です。

[Frame]：フレーム エラーの数。不良フレームには、長さが正しくないパケットや、フレーム チェックサムが正しくないパケットがあります。このエラーは通常、コリジョンまたはイーサネット デバイスの誤動作が原因です。

[Input Errors]：ここにリストされている他のタイプのものも含めた入力エラーの合計数。また、その他の入力関連のエラーによって入力エラー数が増えたり、一部のデータグラムに複数のエラーが存在していたりする可能性があります。したがって、この合計は、他のタイプにリストされているエラーの数を超えることがあります。

[Runts]：最小パケット サイズの 64 バイトよりも小さかったために廃棄されたパケットの数。ラントは通常、コリジョンによって発生します。不適切な配線や電気干渉によって発生することもあります。

[Giants]：最大パケット サイズを超えたために廃棄されたパケットの数。たとえば、1518 バイトよりも大きいイーサネット パケットはジャイアントと見なされます。

[Deferred]：FastEthernet インターフェイスだけ。リンク上のアクティビティが原因で送信前に保留されたフレームの数。

- [Miscellaneous]：受信したブロードキャストの統計情報を表示します。
- [Collision Counts]：FastEthernet インターフェイスだけ。次の統計情報を表示します。

  [Output Errors]：設定されている衝突の最大数を超えたために伝送されなかったフレームの数。このカウンタは、ネットワーク トラフィックが多い場合にのみ増加します。

  [Collisions]：イーサネット衝突（1 つまたは複数の衝突）が原因で、再度伝送されたメッセージ数。これは通常、過渡に延長した LAN で発生します（イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間のリピータが 2 つよりも多い、またはマルチポート トランシーバのカスケードが多すぎる場合）。衝突するパケットは、出力パケットによって 1 回だけカウントされます。

  [Late Collisions]：通常の衝突ウィンドウの外で衝突が発生したために伝送されなかったフレームの数。レイト コリジョンは、パケットの送信中に遅れて検出されるコリジョンです。これは通常発生しません。2 つのイーサネット ホストが同時に通信しようとした場合、早期にパケットが衝突して両者がバックオフするか、2 番目のホストが 1 番目のホストの通信状態を確認して待機します。レイト コリジョンが発生すると、デバイスは割り込みを行ってイーサネット上にパケットを送信しようとしますが、セキュリティ アプライアンスはパケットの送信を部分的に完了しています。セキュリティ アプライアンスは、パケットの最初の部分を保持するバッファを解放した可能性があるため、パケットを再送しません。このことはあまり問題になりません。その理由は、ネットワーキング プロトコルはパケットを再送することでコリジョンを処理する設計になっているためです。ただし、レイト コリジョンはネットワークに問題が存在することを示しています。一般的な問題は、リピータで接続された大規模ネットワーク、および仕様の範囲を超えて動作しているイーサネット ネットワークです。

- [Input Queue]：入力キューの現在のパケット数および最大パケット数を表示します。次の統計情報が含まれます。

  [Hardware Input Queue]：ハードウェア キューのパケット数。

  [Software Input Queue]：ソフトウェア キューのパケット数。

- [Output Queue]：出力キューの現在のパケット数および最大パケット数を表示します。次の統計情報が含まれます。

  [Hardware Output Queue]：ハードウェア キューのパケット数。

  [Software Output Queue]：ソフトウェア キューのパケット数。

  - [Drop Packet Queue]：ドロップされたパケット数を表示します。
- [Add]：選択した統計タイプを、選択したグラフ ウィンドウに追加します。
- [Remove]：選択したグラフ ウィンドウから、選択した統計タイプを削除します。削除している項目が他のパネルから追加され、[Available Graphs] ペインに戻されていない場合、このボタン名は [Delete] に変わります。
- [Show Graphs]：統計タイプを追加するグラフ ウィンドウ名を表示します。すでにグラフ ウィンドウを開いている場合は、デフォルトで新しいグラフ ウィンドウがリストされます。すでに開いているグラフに統計タイプを追加する場合は、開いているグラフ ウィンドウの名前を選択します。すでにグラフに含まれている統計情報が [Selected Graphs] ペインに表示され、タイプを追加できます。グラフ ウィンドウには ASDM、インターフェイスの IP アドレス、および「Graph」という順番で名前が付けられます。後続のグラフは、「Graph (2)」のように名前が付けられます。
- [Selected Graphs]：選択したグラフ ウィンドウに表示する統計タイプを表示します。タイプを 4 つまで含めることができます。
  - [Show Graphs]：グラフ ウィンドウを表示するか、または、追加した場合は追加の統計タイプでグラフを更新します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Graph/Table

[Graph] ウィンドウには、選択した統計情報のグラフが表示されます。[Graph] ウィンドウには、最大 4 つのグラフおよびテーブルを同時に表示することができます。デフォルトで、グラフまたはテーブルにリアルタイムな統計情報が表示されます。「History Metrics」（P.10-6）をイネーブルにすると、過去の期間の統計情報を表示できます。

フィールド

- [View]：グラフまたはテーブルを表示する期間を設定します。リアルタイム以外の期間で表示する場合は、「History Metrics」（P.10-6）をイネーブルにします。次のオプションの指定に従ってデータが更新されます。
  - Real-time, data every 10 sec
  - Last 10 minutes, data every 10 sec
  - Last 60 minutes, data every 1 min
  - Last 12 hours, data every 12 min
  - Last 5 days, data every 2 hours
- [Export]：グラフをカンマ区切り形式でエクスポートします。[Graph] ウィンドウに複数のグラフまたはテーブルがある場合、[Export Graph Data] ダイアログボックスが表示されます。名前の横のチェックボックスを選択して、リストされているグラフおよびテーブルを 1 つ以上選択します。

- [Print]：グラフまたはテーブルを印刷します。[Graph] ウィンドウに複数のグラフまたはテーブルがある場合、[Print Graph] ダイアログボックスが表示されます。[Graph/Table Name] リストから印刷するグラフまたはテーブルを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

PPPoE Client

[PPPoE Client Lease Information] ペインには、現在の PPPoE 接続に関する情報が表示されます。

フィールド

[Select a PPPoE interface]：PPPoE クライアントのリース情報を表示するインターフェイスを選択します。

[Refresh]：セキュリティ アプライアンスから最新の PPPoE 接続情報をロードして表示します。

interface connection

[Monitoring] > [*Interfaces*] ツリーの interface connection ノードは、スタティック ルート トラッキングが設定されている場合にだけ表示されます。複数のルートを追跡している場合、追跡されるルートが含まれている各インターフェイスにノードがあります。

ルート トラッキングに関する詳細については、次の項を参照してください。

- 「Track Status for」（P.44-9）
- 「Monitoring Statistics for」（P.44-10）

Track Status for

[Track Status for] ペインには、追跡されたオブジェクトに関する情報が表示されます。

フィールド

- [Tracked Route]：*表示専用*。トラッキング プロセスに関連付けられているルートを表示します。
- [Route Statistics]：*表示専用*。オブジェクトの到達性情報を表示します。到達性情報で最後に変更があった場合は、オペレーションのリターンコード、およびトラッキングを実行するプロセスを表示します。

モード

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Monitoring Statistics for

[Monitoring Statics for] ペインには、SLA モニタリング プロセスの統計情報が表示されます。

フィールド

- [SLA Monitor ID]：*表示専用*。SLA モニタリング プロセスの ID を表示します。
- [SLA statistics]：*表示専用*。プロセスが変更された最後の時刻、試行されたオペレーション回数、スキップされたオペレーション回数などの SLA モニタリング統計情報を表示します。

モード

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

CHAPTER 45

ルーティングのモニタリング

ASDM を使用して、OSPF LSA、OSPF、EIGRP ネイバー、およびルーティング テーブルを監視できます。ルーティング モニタリング画面にアクセスするには、ASDM インターフェイスで [Monitoring] > [Routing] に移動します。

この項は、次の内容で構成されています。

OSPF LSA のモニタリング

[Monitoring] > [Routing] > [OSPF LSAs] 領域で、セキュリティ アプライアンスの OSPF データベースに格納されている LSA を表示できます。データベースには 4 つのタイプの LSA があり、それぞれのタイプに特定の形式があります。LSA のタイプの概要は次のとおりです。

- ルータ LSA（タイプ 1 LSA）は、ネットワークに接続されているルータを記述します。
- ネットワーク LSA（タイプ 2 LSA）は、OSPF ルータに接続されているネットワークを記述します。
- 集約 LSA（タイプ 3 およびタイプ 4 LSA）は、エリア境界のルーティング情報を集約します。
- 外部 LSA（タイプ 5 およびタイプ 7 LSA）は、外部ネットワークへのルートを記述します。

各 LSA タイプに表示される情報の詳細については、次の項を参照してください。

- [Type 1]
- [Type 2]
- [Type 3]
- [Type 4]
- [Type 5]
- [Type 7]

[Type 1]

タイプ 1 LSA は、エリア内ですべての OSPF ルータによって渡されるルータ リンク アドバタイズメントです。タイプ 1 LSA は、ネットワークへのルータ リンクを記述します。タイプ 1 LSA は、特定のエリア内だけでフラッドされます。

[Type 1] ペインには、セキュリティ アプライアンスで受信したすべてのタイプ 1 LSA が表示されます。テーブルの各行は、1 つの LSA を表します。

フィールド

- [Process]：*表示専用*。LSA の OSPF プロセスを表示します。
- [Area]：*表示専用*。LSA の OSPF エリアを表示します。
- [Router ID]：*表示専用*。LSA を発信するルータの OSPF ルータ ID を表示します。
- [Advertiser]：*表示専用*。LSA を発信するルータの ID を表示します。ルータ LSA の場合、[Router ID] と同一です。
- [Age]：*表示専用*。リンク ステートの経過時間を表示します。
- [Sequence #]：*表示専用*。リンク ステートのシーケンス番号を表示します。リンク ステートのシーケンス番号は、古い LSA や重複 LSA の検出に使われます。
- [Checksum]：*表示専用*。LSA の内容のチェックサムを表示します。
- [Link Count]：*表示専用*。ルータで検出されたインターフェイスの数を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

[Type 2]

タイプ 2 LSA は、エリア内で代表ルータによってフラッドされるネットワーク リンク アドバタイズメントです。タイプ 2 LSA は、特定のネットワークに接続されているルータを記述します。

[Type 2] ペインには、ルータをアドバタイズする代表ルータの IP アドレスが表示されます。

フィールド

- [Process]：*表示専用*。LSA の OSPF プロセスを表示します。
- [Area]：*表示専用*。LSA の OSPF エリアを表示します。
- [Designated Router]：*表示専用*。LSA を送信した代表ルータ インターフェイスの IP アドレスを表示します。
- [Advertiser]：*表示専用*。LSA を送信した代表ルータの OSPF ルータ ID を表示します。
- [Age]：*表示専用*。リンク ステートの経過時間を表示します。

- [Sequence #]：*表示専用*。リンク ステートのシーケンス番号を表示します。リンク ステートのシーケンス番号は、古い LSA や重複 LSA の検出に使われます。
- [Checksum]：*表示専用*。LSA の内容のチェックサムを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

[Type 3]

タイプ 3 LSA は、エリア間で渡されるサマリー リンク アドバタイズメントです。タイプ 3 LSA は、エリア内のネットワークを記述します。

フィールド

- [Process]：*表示専用*。LSA の OSPF プロセスを表示します。
- [Area]：*表示専用*。LSA の OSPF エリアを表示します。
- [Destination]：*表示専用*。アドバタイズされている宛先ネットワークのアドレスを表示します。
- [Advertiser]：*表示専用*。LSA を送信した ABR の ID を表示します。
- [Age]：*表示専用*。リンク ステートの経過時間を表示します。
- [Sequence #]：*表示専用*。リンク ステートのシーケンス番号を表示します。リンク ステートのシーケンス番号は、古い LSA や重複 LSA の検出に使われます。
- [Checksum]：*表示専用*。LSA の内容のチェックサムを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

[Type 4]

タイプ 4 LSA は、エリア間で渡されるサマリー リンク アドバタイズメントです。タイプ 4 LSA は、ASBR へのパスを記述します。タイプ 4 LSA は、スタブ エリアにフラッドされません。

フィールド

- [Process]：*表示専用*。LSA の OSPF プロセスを表示します。
- [Area]：*表示専用*。LSA の OSPF エリアを表示します。
- [Router ID]：*表示専用*。ASBR のルータ ID を表示します。
- [Advertiser]：*表示専用*。LSA を送信した ABR の ID を表示します。
- [Age]：*表示専用*。リンク ステートの経過時間を表示します。
- [Sequence #]：*表示専用*。リンク ステートのシーケンス番号を表示します。リンク ステートのシーケンス番号は、古い LSA や重複 LSA の検出に使われます。
- [Checksum]：*表示専用*。LSA の内容のチェックサムを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

[Type 5]

タイプ 5 LSA は、ABSR によってエリア間で渡され、エリアにフラッドされます。タイプ 5 LSA は、AS の外へのルートを記述します。スタブ エリアおよび NSSA では、これらの LSA を受信しません。

フィールド

- [Process]：*表示専用*。LSA の OSPF プロセスを表示します。
- [Network]：*表示専用*。AS 外部ネットワークのアドレスを表示します。
- [Advertiser]：*表示専用*。ASBR のルータ ID を表示します。
- [Age]：*表示専用*。リンク ステートの経過時間を表示します。
- [Sequence #]：*表示専用*。リンク ステートのシーケンス番号を表示します。リンク ステートのシーケンス番号は、古い LSA や重複 LSA の検出に使われます。
- [Checksum]：*表示専用*。LSA の内容のチェックサムを表示します。
- [Tag]：*表示専用*。各外部ルートに接続されている、32 ビット フィールドの外部ルート タグを表示します。これは、OSPF プロトコル自体では使われません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

[Type 7]

タイプ 7 LSA は、ASBR によってフラッドされる NSSA AS 外部ルートです。タイプ 7 LSA は、タイプ 5 LSA に似ていますが、複数のエリアにフラッドされるタイプ 5 LSA と異なり、NSSA だけにフラッドされます。タイプ 7 LSA は、エリア バックボーンにフラッドされる前に ABR によってタイプ 5 LSA に変換されます。

フィールド

- [Process]：*表示専用*。LSA の OSPF プロセスを表示します。
- [Area]：*表示専用*。LSA の OSPF エリアを表示します。
- [Network]：*表示専用*。外部ネットワークのアドレスを表示します。
- [Advertiser]：*表示専用*。LSA を送信した ASBR のルータ ID を表示します。
- [Age]：*表示専用*。リンク ステートの経過時間を表示します。
- [Sequence #]：*表示専用*。リンク ステートのシーケンス番号を表示します。リンク ステートのシーケンス番号は、古い LSA や重複 LSA の検出に使われます。
- [Checksum]：*表示専用*。LSA の内容のチェックサムを表示します。
- [Tag]：*表示専用*。各外部ルートに接続されている、32 ビット フィールドの外部ルート タグを表示します。これは、OSPF プロトコル自体では使われません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

OSPF ネイバーのモニタリング

[OSPF Neighbor] ペインには、セキュリティ アプライアンスでダイナミックに検出された OSPF ネイバーとスタティックに設定された OSPF ネイバーが表示されます。[OSPF Neighbor] ペインは、ASDM インターフェイスの [Monitoring] > [Routing] > [OSPF Neighbors] にあります。

フィールド

- [Neighbor]：*表示専用*。隣接ルータ ID を表示します。
- [Priority]：*表示専用*。ルータの優先順位を表示します。
- [State]：*表示専用*。ネイバーの OSPF ステートを表示します。
  - Down：最初の OSPF ネイバー ステートです。このネイバーから hello パケットを受信していないが、このステートで hello パケットをネイバーにまだ送信可能であることを意味します。

    完全に隣接したネイバー ステートでは、セキュリティ アプライアンスがデッド時間間隔内にネイバーから hello パケットを受信しない場合、または手動で設定したネイバーがコンフィギュレーションから削除されようとしている場合、ネイバー ステートは Full から Down に変わります。
  - Attempt：このステートは、NBMA 環境で、手動で設定したネイバーだけで有効です。Attempt ステートでは、セキュリティ アプライアンスは、デッド時間間隔内に hello を受信しなかったネイバーにポーリング時間間隔ごとにユニキャスト hello パケットを送信します。
  - Init：このステートは、セキュリティ アプライアンスがネイバーから hello パケットを受信したが、hello パケットに受信するルータの ID が含まれていなかったことを示します。ルータがネイバーから hello パケットを受信すると、有効な hello パケットを受信した確認として送信側のルータ ID を hello パケットにリストします。
  - 2-Way：このステートは、セキュリティ アプライアンスとネイバーの間で双方向通信が確立されたことを示します。双方向とは、各デバイスで相手側デバイスからの hello パケットを確認したことを意味します。hello パケットを受信するルータ自体の Router ID が、受信した hello パケットの [neighbor] フィールド内にある場合は、このステートになります。このステートで、セキュリティ アプライアンスは、このネイバーと隣接になるかどうかを決定します。ブロードキャスト メディア ネットワークおよび非ブロードキャスト マルチアクセス ネットワークで、セキュリティ アプライアンスは、指定されたルータとバックアップの代表ルータだけと Full になります。他のすべてのネイバーとは 2-way ステートのままになります。ポイントツーポイント ネットワークおよびポイントツーマルチポイント ネットワークで、セキュリティ アプライアンスは、接続されているすべてのネイバーと Full になります。

    この段階の最後に、ブロードキャストと非ブロードキャスト マルチアクセス ネットワークの DR および BDR が選定されます。

（注） また、Init ステートでネイバーから Database Descriptor パケットを受信すると、2-way ステートへの移行が発生します。

  - Exstart：DR および BDR が選定されると、セキュリティ アプライアンスと DR および BDR の間でリンク ステート情報交換の実際のプロセスが開始されます。

    このステートで、セキュリティ アプライアンスと DR および BDR はマスタースレーブ関係を確立し、隣接関係形成の初期シーケンス番号を選択します。ルータ ID が大きいデバイスがマスターになり、交換を開始します。したがって、このデバイスだけがシーケンス番号を増やせます。

（注）　DR/BDR の選定は、ルータ ID の最も大きいものではなく、デバイスで設定された優先順位の高い方によって行われます。したがって、このステートで DR はスレーブの役割を果たすことができます。マスター / スレーブの選定は、ネイバーごとに行われます。複数のデバイスの DR 優先順位が等しい場合、最上位の IP アドレスを持つデバイスが DR になります。

  - Exchange：exchange ステートで、OSPF ネイバーは DBD パケットを交換します。Database Descriptor には LSA ヘッダーだけが含まれ、リンク ステート データベース全体の内容が記述されています。各 DBD パケットにはシーケンス番号があり、そのシーケンス番号を増分するのは、スレーブによって明示的に確認されているマスターだけです。また、このステートで、ルータはリンク ステート要求パケットとリンク ステート アップデート パケット（LSA 全体を含む）を送信します。受信した DBD の内容は、ルータ リンク ステート データベースに含まれる情報と比較され、ネイバーに新規または最新のリンク ステート情報があるかどうかがチェックされます。
  - Loading：このステートで、リンク ステート情報の実際の交換が実行されます。DBD からの情報に基づいて、ルータはリンク ステート要求パケットを送信します。次に、ネイバーは、リンク ステート アップデート パケットで要求されたリンク ステート情報を提供します。隣接中に、セキュリティ アプライアンスは古い LSA または不足している LSA を受信すると、リンク ステート要求パケットを送信してその LSA を要求します。すべてのリンク ステート アップデート パケットが確認されます。
  - Full：このステートで、ネイバーは互いに完全に隣接しています。すべてのルータおよびネットワーク LSA が交換され、ルータ データベースは完全に同期化されます。

    Full は、OSPF ルータの通常のステートです。唯一の例外は、2-way ステートです。2-way ステートは、ブロードキャスト ネットワークでは通常です。ルータは、DR および BDR だけで Full ステートに達します。ネイバーは、常に互いを 2-way と見なします。

- [Dead Time]：*表示専用*。ルータがネイバーからの OSPF hello パケットの受信を待機する残り時間を表示します。時間になると、ネイバーのダウン状態が宣言されます。
- [Address]：*表示専用*。このネイバーが直接接続されているインターフェイスの IP アドレスを表示します。
- [Interface]：*表示専用*。OSPF ネイバーが隣接を形成したインターフェイスを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

EIGRP ネイバーのモニタリング

[EIGRP Neighbors] ペインには、ダイナミックに検出された EIGRP ネイバーが表示されます。スタティックに定義されたネイバーは、このペインには表示されません。スタティックに定義された EIGRP ネイバーを表示するには、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Static Neighbor] を選択します。

フィールド

- [Address]：EIGRP ネイバーの IP アドレス。
- [Interface]：セキュリティ アプライアンスがネイバーから hello パケットを受信するインターフェイス。
- [Holdtime]：この時間（秒単位）の間、セキュリティ アプライアンスがネイバーからの受信を待機し、時間が経過するとネイバーがダウンしていることを宣言します。この保持時間は hello パケットでネイバーから受信し、次の hello パケットをネイバーから受信するまで減っていきます。

  ネイバーがデフォルトの保持時間を使用する場合、この数は 15 未満になります。ピアがデフォルト以外の保持時間を設定している場合、デフォルト以外の保持時間が表示されます。

  この値が 0 になると、セキュリティ アプライアンスはネイバーが到達不能であると見なします。
- [Uptime]：セキュリティ アプライアンスが最初にこのネイバーから受信してからの経過時間（hh:mm:ss）。
- [Queue Length]：セキュリティ アプライアンスで送信待ちになっている EIGRP パケット（アップデート、クエリー、応答）の数。
- [Sequence Number]：ネイバーから受信した最後のアップデート、クエリー、または応答パケットのシーケンス番号。
- [SRTT]：平滑化ラウンドトリップ時間。これは、EIGRP パケットをこのネイバーに送信してからセキュリティ アプライアンスがそのパケットの確認応答を受信するまでに必要な時間（ミリ秒）です。
- [RTO]：再送信タイムアウト（ミリ秒単位）。この時間、セキュリティ アプライアンスは待機し、時間が経過したら再送信キューからネイバーにパケットを再送信します。
- [Clear Neighbors]：ネイバー テーブルからダイナミックに取得されたネイバーをクリアするには、[Clear Neighbors] ボタンをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	トランスペアレント	シングル	コンテキスト	システム
•	—	•	—	—

ルートの表示

[Routes] ペインには、セキュリティ アプライアンスのルーティング テーブルでスタティックに設定、接続および検出されたルートが表示されます。

フィールド

- [Protocol]：*表示専用*。ルート情報の発信元を表示します。
  - RIP：ルートは RIP を使用して取得されました。
  - OSPF：ルートは OSPF を使用して取得されました。
  - EIGRP：ルートは EIGRP を使用して取得されました。
  - CONNECTED：ルートは、インターフェイスに直接接続されたネットワークです。
  - STATIC：ルートはスタティックに定義されています。
- [Type]：*表示専用*。ルートのタイプを表示します。次のいずれかの値になります。
  - -（ダッシュ）：タイプ カラムが指定のルートに適用されていないことを示します。
  - IA：ルートは OSPF のエリア間ルートです。
  - E1：ルートは OSPF の外部タイプ 1 ルートです。
  - E2：ルートは OSPF の外部タイプ 2 ルートです。
  - N1：ルートは、OSPF の not so stubby area（NSSA）の外部タイプ 1 ルートです。
  - N2：ルートは、OSPF NSSA 外部タイプ 2 ルートです。
- [Destination]：*表示専用*。宛先ネットワークの IP アドレスとネットマスクを表示します。
- [Gateway：*表示専用*。リモート ネットワークの次のルータの IP アドレスを表示します。
- [Interface]：*表示専用*。指定されたネットワークに到達可能なインターフェイスを表示します。
- [AD/Metric]：*表示専用*。ルートの管理ディスタンスとメトリックを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
	トランス		マルチ	
ルーテッド	ペアレント	シングル	コンテキスト	システム
•	•	•	•	—

CHAPTER 46

VPN のモニタリング

VPN のモニタリング セクションには、次のパラメータと統計情報が表示されます。

- 特定のリモート アクセス、LAN 間、クライアントレス SSL VPN、および電子メール プロキシ セッションの VPN 統計情報
- トンネル グループの暗号化統計情報
- トンネル グループのプロトコル統計情報
- グローバル IPSec および IKE の統計情報
- IPSec、IKE、SSL およびその他のプロトコルの暗号統計情報
- クラスタ VPN サーバ負荷の統計情報

VPN 接続グラフ

セキュリティ アプライアンスの VPN 接続データをグラフ形式または表形式で表示します。

IPSec Tunnels

このウィンドウを使用して、表示や、エクスポートまたは印刷の準備を行う IPSec トンネル タイプのグラフとテーブルを指定します。

フィールド

- [Graph Window Title] : [Show Graphs] をクリックしたときに、ウィンドウに表示されるデフォルトのタイトルを表示します。この属性は、特に印刷またはエクスポートする前にウィンドウでデータを確認するときに便利です。タイトルを変更するには、ドロップダウン リストから他のタイトルを選択するか、またはタイトルを入力します。
- [Available Graphs] : 表示できるアクティブなトンネルのタイプを示します。1 つのウィンドウにまとめて表示するタイプごとに、このボックスのエントリをクリックし、[Add] をクリックします。
- [Selected Graphs] : 選択したトンネルのタイプを示します。

  [Show Graphs] をクリックすると、ASDM は、このボックスにリストされているアクティブなトンネル タイプを 1 つのウィンドウに表示します。

  強調表示されているエントリは、[Remove] をクリックした場合にリストから削除されるトンネルのタイプを示します。

- [Add] : [Available Graphs] ボックスから [Selected Graphs] ボックスに、選択したトンネル タイプを移動します。
- [Remove] : [Selected Graphs] ボックスから [Available Graphs] ボックスに、選択したトンネル タイプを移動します。
- [Show Graphs] : [Selected Graphs] ボックスに表示されるトンネル タイプのグラフで構成されるウィンドウを表示します。表示されるウィンドウ内の各タイプには、[Graph] タブと [Table] タブがあり、アクティブなトンネル データの表示をクリックして切り替えられます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

セッション

このパネルを使用して、表示や、エクスポートまたは印刷の準備を行う VPN セッション タイプのグラフとテーブルを指定します。

フィールド

- [Graph Window Title] : [Show Graphs] をクリックしたときに、ウィンドウに表示されるデフォルトのタイトルを表示します。この属性は、特に印刷またはエクスポートする前にウィンドウでデータを確認するときに便利です。タイトルを変更するには、ドロップダウン リストから他のタイトルを選択するか、またはタイトルを入力します。
- [Available Graphs] : 表示できるアクティブなセッションのタイプを示します。1 つのウィンドウにまとめて表示するタイプごとに、このボックスのエントリをクリックし、[Add] をクリックします。
- [Selected Graphs] : 選択したアクティブなセッションのタイプを示します。

  [Show Graphs] をクリックすると、ASDM は、このボックスにリストされているアクティブなセッション タイプを 1 つのウィンドウにすべて表示します。

  強調表示されているエントリは、[Remove] をクリックするとリストから削除されるセッションのタイプを示します。
- [Add] : [Available Graphs] ボックスから [Selected Graphs] ボックスに、選択したセッション タイプを移動します。
- [Remove] : [Selected Graphs] ボックスから [Available Graphs] ボックスに、選択したセッション タイプを移動します。
- [Show Graphs] : [Selected Graphs] ボックスに表示されるセッション タイプのグラフで構成されるウィンドウを表示します。表示されるウィンドウ内の各タイプには、[Graph] タブと [Table] タブがあり、アクティブなセッション データの表示をクリックして切り替えられます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

VPN 統計情報

これらのパネルには、特定のリモート アクセス、LAN-to-LAN、クライアントレス SSL VPN、または電子メール プロキシ セッションの詳細なパラメータおよび統計情報が表示されます。パラメータと統計情報は、セッション プロトコルによって異なります。また、統計情報テーブルの内容は、選択した接続のタイプによって異なります。各詳細テーブルには、それぞれのセッションの関連パラメータがすべて表示されます。

セッション

このパネルを使用して、このサーバのセッション統計情報を表示します。

フィールド

- [Session types]（ラベルなし）：各タイプの現在アクティブなセッションの数、合計制限および合計累積セッション数を一覧表示します。
  - [Remote Access]：リモート アクセス セッションの数を示します。
  - [Site-to-Site]：LAN 間セッションの数を示します。
  - [SSL VPN–Clientless]：ブラウザベースのクライアントレス VPN セッションの数を示します。
  - [SSL VPN–With Client]：リモート コンピュータにクライアント アプリケーションが必要な SSL VPN セッションの数を示します。
  - [SSL VPN–Total]：クライアントベースおよびクライアントレスの SSL VPN セッションの数を示します。
  - [E-mail Proxy]：電子メール プロキシ セッションの数を示します。
  - [VPN Load Balancing]：ロードバランシングが行われている VPN セッションの数を示します。
  - [Total]：アクティブな同時セッションの合計数を示します。
  - [Total Cumulative]：最後にセキュリティ アプライアンスをリブートまたはリセットしたときからの累積セッション数を示します。
- [Filter By]：次のテーブル内の統計情報が示すセッションのタイプを指定します。
  - [Session type]（ラベルなし）：監視するセッション タイプを指定します。デフォルトは [Remote Access] です。

- [Session filter]（ラベルなし）：次のテーブル内のフィルタをオンにするカラム ヘッダーを指定します。デフォルトは、--All Sessions-- です。
- [Filter name]（ラベルなし）：適用するフィルタの名前を指定します。Session filter リストに --All Sessions-- を指定した場合、このフィールドは使用できません。他の Session filter を選択した場合、このフィールドをブランクにできません。
- [Filter]：フィルタリング オペレーションを実行します。

このパネルの 2 番目のテーブル（これもラベルはありません）の内容は、[Filter By] リストの選択によって異なります。次のリストで、箇条書きの第 1 レベルは [Filter By] の選択を、第 2 レベルはこのテーブルのカラム ヘッダーを示します。

- [Remote Access]：このテーブルの値がリモート トラフィックに関連することを示します。
  - [Username/Tunnel Group]：セッションのユーザ名またはログイン名、およびトンネル グループを示します。クライアントが認証にデジタル証明書を使用している場合、フィールドに証明書の Subject CN または Subject OU が表示されます。
  - [Assigned IP Address/Public IP Address]：このセッションのリモート クライアントに割り当てられているプライベート（「割り当てられた」）IP アドレスが表示されます。これは「内部」または「仮想」IP アドレスとも呼ばれ、クライアントはプライベート ネットワーク上のホストとして表示されます。また、このリモート アクセス セッションのクライアントのパブリック IP アドレスも表示します。パブリック IP アドレスは、「外部」IP アドレスとも呼ばれます。通常、これは ISP によってクライアントに割り当てられます。このアドレスにより、クライアントは、パブリック ネットワーク上のホストとして機能することが可能となります。
  - [Protocol/Encryption]：このセッションで使用しているプロトコルとデータ暗号化アルゴリズムがある場合に表示されます。
  - [Login Time/Duration]：セッションがログインした日付と時刻（MMM DD HH:MM:SS）、およびセッションの長さを表示します。時刻の表示は 24 時間表示です。
  - [Client Type/Version]：ユーザ名でソートされた接続されたクライアントのソフトウェア バージョン番号（例：rel.7.0_int 50）を示します。
  - [Bytes Tx/Bytes Rx]：セキュリティ アプライアンスとリモート ピアまたはクライアントの間で送受信される合計バイト数を表示します。
  - [NAC Result and Posture Token]：セキュリティ アプライアンスでネットワーク アドミッション コントロールを設定している場合にだけ、このカラムに値が表示されます。

    [NAC Result] には、次の値のいずれかが表示されます。

    [Accepted]：ACS は正常にリモート ホストのポスチャを検証しました。

    [Rejected]：ACS はリモート ホストのポスチャの検証に失敗しました。

    [Exempted]：セキュリティ アプライアンスに設定されたポスチャ検証免除リストに従って、リモート ホストはポスチャ検証を免除されました。

    [Non-Responsive]：リモート ホストは EAPoUDP Hello メッセージに応答しませんでした。

    [Hold-off]：ポスチャ検証に成功した後、セキュリティ アプライアンスとリモート ホストの EAPoUDP 通信が途絶えました。

    [N/A]：VPN NAC グループ ポリシーに従い、リモート ホストの NAC はディセーブルにされています。

    [Unknown]：ポスチャ検証が進行中です。

ポスチャ トークンは、Access Control Server で設定可能な情報文字列です。ACS は情報提供のためにセキュリティ アプライアンスにポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。[NAC Result] フィールドに続く [Posture Token] フィールドの一般的な値は、[Healthy]、[Checkup]、[Quarantine]、[Infected] または [Unknown] です。

- [Site-toSite]：このテーブルの値が LAN-to-LAN トラフィックに関連することを示します。
  - [Tunnel Group/IP Address]：トンネル グループの名前とピアの IP アドレスを示します。
  - [Protocol/Encryption]：このセッションで使用しているプロトコルとデータ暗号化アルゴリズムがある場合に表示されます。
  - [Login Time/Duration]：セッションがログインした日付と時刻（MMM DD HH:MM:SS）、およびセッションの長さを表示します。時刻の表示は 24 時間表示です。
  - [Bytes Tx/Bytes Rx]：セキュリティ アプライアンスとリモート ピアまたはクライアントの間で送受信される合計バイト数を表示します。
- [Clientless SSL VPN]：このテーブルの値がクライアントレス SSL VPN トラフィックに関連することを示します。
  - [Username/IP Address]：セッションのユーザ名またはログイン名、およびクライアントの IP アドレスを示します。
  - [Protocol/Encryption]：このセッションで使用しているプロトコルとデータ暗号化アルゴリズムがある場合に表示されます。
  - [Login Time/Duration]：セッションがログインした日付と時刻（MMM DD HH:MM:SS）、およびセッションの長さを表示します。時刻の表示は 24 時間表示です。
  - [Client Type/Version]：ユーザ名でソートされた接続されたクライアントのソフトウェア バージョン番号（例：rel.7.0_int 50）を示します。
  - [Bytes Tx/Bytes Rx]：セキュリティ アプライアンスとリモート ピアまたはクライアントの間で送受信される合計バイト数を表示します。
- [E-Mail Proxy]：このテーブルの値がクライアントレス SSL VPN セッションのトラフィックに関連することを示します。
  - [Username/IP Address]：セッションのユーザ名またはログイン名、およびクライアントの IP アドレスを示します。
  - [Protocol/Encryption]：このセッションで使用しているプロトコルとデータ暗号化アルゴリズムがある場合に表示されます。
  - [Login Time/Duration]：セッションがログインした日付と時刻（MMM DD HH:MM:SS）、およびセッションの長さを表示します。時刻の表示は 24 時間表示です。
  - [Client Type/Version]：ユーザ名でソートされた接続されたクライアントのソフトウェア バージョン番号（例：rel.7.0_int 50）を示します。
  - [Bytes Tx/Bytes Rx]：セキュリティ アプライアンスとリモート ピアまたはクライアントの間で送受信される合計バイト数を表示します。

この項の残りの部分では、テーブルの近くや下にあるボタンおよびフィールドについて説明します。

- [Details]：選択したセッションの詳細を表示します。パラメータと値は、セッションのタイプによって異なります。
- [Logout]：選択したセッションを終了します。
- [Ping]：ネットワークの接続テストのために、ICMP `ping`（Packet Internet Groper）パケットを送信します。具体的には、セキュリティ アプライアンスは、選択したホストに ICMP Echo Request メッセージを送信します。ホストが到達可能な場合、Echo Reply メッセージを返し、セキュリ

ティ アプライアンスはテストしたホストの名前が記された Success メッセージ、および要求を送信して応答を受信するまでの経過時間を表示します。何らかの理由でシステムが到達不可能な場合（ホストがダウンしている、ICMP がホストで実行していない、ルートが設定されていない、中間ルータがダウンしている、ネットワークがダウンまたは輻輳しているなど）、セキュリティ アプライアンスには、テストしたホストの名前が記された [Error] 画面が表示されます。

- [Logout By]：ログアウトするセッションのフィルタリングに使う基準を選択します。--All Sessions-- 以外を選択した場合、[Logout By] リストの右側のボックスがアクティブになります。値に Protocol for Logout By を選択した場合、ボックスがリストに変わり、ログアウト フィルタとして使用するプロトコル タイプを選択できます。このリストのデフォルト値は IPSec です。Protocol 以外の値を選択した場合は、このボックスに適切な値を入力する必要があります。
- [Logout Sessions]：指定した Logout By 基準に合うすべてのセッションを終了します。
- [Refresh]：画面とそのデータを更新します。日付と時刻は、画面が最後に更新された日時を示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Sessions Details

[Session Details] ウィンドウには、選択したセッションのコンフィギュレーション設定、統計情報およびステート情報が表示されます。

[Session Details] ウィンドウの一番上にある [Remote Detailed] テーブルには、次のカラムが表示されます。

- [Username]：セッションに関連付けられているユーザ名またはログイン名を示します。リモート ピアが認証にデジタル証明書を使用している場合、フィールドに証明書の Subject CN または Subject OU が表示されます。
- [Group Policy and Tunnel Group]：セッションに割り当てられているグループ ポリシーとセッションが確立されたトンネル グループの名前。
- [Assigned IP Address and Public IP Address]：このセッションのリモート ピアに割り当てられているプライベート IP アドレス。内部または仮想 IP アドレスとも呼ばれ、割り当てられている IP アドレスによって、リモート ピアはプライベート ネットワーク上にあるように見えます。2 番目のフィールドには、このセッションのリモート コンピュータのパブリック IP アドレスが表示されます。外部 IP アドレスとも呼ばれ、通常、パブリック IP アドレスは ISP によってリモート コンピュータに割り当てられます。これによって、リモート コンピュータはパブリック ネットワークのホストとして機能できます。
- [Protocol/Encryption]：このセッションで使用しているプロトコルとデータ暗号化アルゴリズム（ある場合）。
- [Login Time and Duration]：セッションの開始日時とセッションの長さ。セッションの開始時刻は、24 時間表記で表示されます。

- [Client Type and Version] : リモート コンピュータのクライアントのタイプおよびソフトウェア バージョン番号（例：rel.7.0_int 50）。
- [Bytes Tx and Bytes Rx] : セキュリティ アプライアンスとリモート ピアの間で送受信される合計バイト数を示します。
- [NAC Result and Posture Token] : ASDM では、セキュリティ アプライアンスでネットワーク アドミッション コントロールを設定している場合にだけ、このカラムに値が表示されます。

  [NAC Result] には、次の値のいずれかが表示されます。

  - [Accepted] : ACS は正常にリモート ホストのポスチャを検証しました。
  - [Rejected] : ACS はリモート ホストのポスチャの検証に失敗しました。
  - [Exempted] : セキュリティ アプライアンスに設定されたポスチャ検証免除リストに従って、リモート ホストはポスチャ検証を免除されました。
  - [Non-Responsive] : リモート ホストは EAPoUDP Hello メッセージに応答しませんでした。
  - [Hold-off] : ポスチャ検証に成功した後、セキュリティ アプライアンスとリモート ホストの EAPoUDP 通信が途絶えました。
  - [N/A] : VPN NAC グループ ポリシーに従い、リモート ホストの NAC はディセーブルにされています。
  - [Unknown] : ポスチャ検証が進行中です。

  ポスチャ トークンは、Access Control Server で設定可能な情報文字列です。ACS は情報提供のためにセキュリティ アプライアンスにポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。NAC Result に続く一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected または Unknown です。

[Session Details] ウィンドウの [Details] タブには、次のカラムが表示されます。

- [ID] : セッションにダイナミックに割り当てられた一意の ID。ID は、セッションへのセキュリティ アプライアンスのインデックスとして機能します。このインデックスを使用して、セッションに関する情報を維持および表示します。
- [Type] : セッションのタイプ。IKE、IPSec または NAC。
- [Local Addr., Subnet Mask, Protocol, Port, Remote Addr., Subnet Mask, Protocol, and Port] : 実際の（ローカル）ピアの両方に割り当てられているアドレスとポートと外部ルーティングのためにそのピアに割り当てられているアドレスとポート。
- [Encryption] : このセッションで使用しているデータ暗号化アルゴリズム（ある場合）。
- [Assigned IP Address and Public IP Address] : このセッションのリモート ピアに割り当てられているプライベート IP アドレスを示します。内部または仮想 IP アドレスとも呼ばれ、割り当てられている IP アドレスによって、リモート ピアはプライベート ネットワーク上にあるように見えます。2 番目のフィールドには、このセッションのリモート コンピュータのパブリック IP アドレスが表示されます。外部 IP アドレスとも呼ばれ、通常、パブリック IP アドレスは ISP によってリモート コンピュータに割り当てられます。これによって、リモート コンピュータはパブリック ネットワークのホストとして機能できます。
- [Other] : セッションに関連付けられているその他の属性。

  次の属性は、IKE セッションに適用されます。

  次の属性は、IPSec セッションに適用されます。

  次の属性は、NAC セッションに適用されます。

  - [Revalidation Time Interval] : 成功した各ポスチャ検証間に必要とされる間隔（秒数）。

- [Time Until Next Revalidation]：最後のポスチャ検証試行が成功しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
- [Status Query Time Interval]：成功したポスチャ検証またはステータス クエリーの応答と次のステータス クエリーの応答との間に許容される時間（秒数）。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、セキュリティ アプライアンスがリモート ホストに発行する要求です。
- [EAPoUDP Session Age]：最後に成功したポスチャ検証から経過した秒数。
- [Hold-Off Time Remaining]：最後のポスチャ検証が成功した場合は 0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
- [Posture Token]：Access Control Server で設定可能な情報文字列。ACS は情報提供のためにセキュリティ アプライアンスにポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
- [Redirect URL]：ポスチャ検証またはクライアントなしの認証が終わると、ACS はセッション用のアクセス ポリシーをセキュリティ アプライアンスにダウンロードします。Redirect URL は、アクセス ポリシー ペイロードのオプションの一部です。セキュリティ アプライアンスは、リモート ホストのすべての HTTP（ポート 80）要求および HTTPS（ポート 443）要求を Redirect URL（存在する場合）にリダイレクトします。アクセス ポリシーに Redirect URL が含まれていない場合、セキュリティ アプライアンスはリモート ホストからの HTTP 要求および HTTPS 要求をリダイレクトしません。

  Redirect URL は、IPSec セッションが終了するか、ポスチャ再検証が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーをダウンロードします。

  [More]：このボタンを押して、セッションやトンネル グループを再検証または初期化します。

ACL タブには、セッションに一致した ACE が含まれる ACL が表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

サブセッション詳細：[NAC Details]

[NAC Details] ウィンドウでは、NAC セッションの統計情報およびステート情報を表示したり、セッションやトンネル グループを再検証または初期化することができます。

このウィンドウの統計情報およびステート情報の属性は次のとおりです。

- [Reval Int (T)]：再検証の時間間隔。正常に完了した各ポスチャ確認間に、設ける必要のある間隔（秒単位）。
- [Reval Left (T)]：次の再検証までの時間。直前のポスチャ確認試行が正常に完了しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。

- [SQ Int (T)]：ステータス クエリーの時間間隔。正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、セキュリティ アプライアンスがリモート ホストに発行する要求です。
- [EoU Age (T)]：EAPoUDP セッション経過時間。正常に完了した直前のポスチャ確認からの経過秒数。
- [Hold Left (T)]：残りの遅延時間。直前のポスチャ確認が正常に完了した場合は、0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
- [Posture Token]：Access Control Server で設定可能な情報文字列。ACS は情報提供のためにセキュリティ アプライアンスにポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
- [Redirect URL]：ポスチャ検証またはクライアントなしの認証が終わると、ACS はセッション用のアクセス ポリシーをセキュリティ アプライアンスにダウンロードします。Redirect URL は、アクセス ポリシー ペイロードのオプションの一部です。セキュリティ アプライアンスは、リモート ホストのすべての HTTP（ポート 80）要求および HTTPS（ポート 443）要求を Redirect URL（存在する場合）にリダイレクトします。アクセス ポリシーに Redirect URL が含まれていない場合、セキュリティ アプライアンスはリモート ホストからの HTTP 要求および HTTPS 要求をリダイレクトしません。

  Redirect URL は、IPSec セッションが終了するか、ポスチャ再検証が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーをダウンロードします。

このウィンドウのボタンは、次のとおりです。

（注） ポスチャ検証の対象のセッションをすべて再検証または初期化する場合は、[Monitoring] > [VPN] > [VPN Statistics] > [NAC Session Summary] を選択します。

- [Revalidate Session]：ピアのポスチャまたは割り当てられているアクセス ポリシー（ある場合にはダウンロードされた ACL）が変更された場合にクリックします。このボタンをクリックすると、新しい無条件のポスチャ検証を開始します。このボタンをクリックするまで有効だったポスチャ検証と割り当てられているアクセス ポリシーは、新しいポスチャ検証が成功または失敗するまで有効のままとなります。セッションがポスチャ検証から免除されている場合、このボタンをクリックしてもセッションに影響はありません。
- [Initialize Session]：ピアのポスチャ、または割り当てられているアクセス ポリシー（ある場合にはダウンロードされた ACL）が変更され、セッションに割り当てられているリソースをクリアする場合にクリックします。このボタンをクリックすると、EAPoUDP アソシエーションをパージし、新しい無条件のポスチャ検証を開始します。再検証中には NAC のデフォルトの ACL が有効となるため、セッションを初期化するとユーザ トラフィックに影響する場合があります。セッションがポスチャ検証から免除されている場合、このボタンをクリックしてもセッションに影響はありません。
- [Revalidate Tunnel Group]：選択したセッション、または割り当てられているアクセス ポリシー（ダウンロードされた ACL）の専用のトンネル グループにあるピアのポスチャが変更された場合にクリックします。このボタンをクリックすると、新しい無条件のポスチャ検証を開始します。このボタンをクリックするまでトンネル グループの各セッションに対して有効だったポスチャ検証と割り当てられているアクセス ポリシーは、新しいポスチャ検証が成功または失敗するまで有効のままとなります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。

- [Initialize Tunnel Group]：選択したセッションまたは割り当てられているアクセス ポリシー（ダウンロードされた ACL）の専用のトンネル グループにあるピアのポスチャが変更され、セッションに割り当てられているリソースをクリアする場合にクリックします。このボタンをクリックすると、選択したセッションの専用のトンネル グループにあるポスチャ検証で使用される EAPoUDP アソシエーションと、アクセス ポリシー（ある場合にはダウンロードされた ACL）をパージし、有効なピアの新しい無条件のポスチャ検証を開始します。再検証中には NAC のデフォルトの ACL が有効となるため、セッションを初期化するとユーザ トラフィックに影響する場合があります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Encryption Statistics

このパネルには、セキュリティ アプライアンスで、現在アクティブなユーザおよび管理者セッションによって使用されるデータ暗号化アルゴリズムが表示されます。テーブルの各行は、1 つの暗号化アルゴリズム タイプを表します。

フィールド

- [Show Statistics For]：特定のサーバやグループ、またはすべてのトンネル グループを選択します。
- [Encryption Statistics]：現在アクティブなセッションで使用中のすべてのデータ暗号化アルゴリズムの統計情報を示します。
  - [Encryption Algorithm]：この行の統計情報が適用される暗号化アルゴリズムを一覧表示します。
  - [Sessions]：このアルゴリズムを使用するセッションの数を一覧表示します。
  - [Percentage]：アクティブなセッションの合計に対する、このアルゴリズムを使用しているセッションの割合を数値で示します。このカラムの合計は 100 % になります（端数は処理）。
- [Total Active Sessions]：現在アクティブなセッションの数を示します。
- [Cumulative Sessions]：セキュリティ アプライアンスを最後にブートまたはリセットしたときからのセッションの合計数を示します。
- [Refresh]：[Encryption Statistics] テーブルに表示される統計情報を更新します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

NAC Session Summary

[Monitoring] > [VPN] > [VPN Statistics] > [NAC Session Summary]

[NAC Session Summary] ウィンドウでは、アクティブな累積ネットワーク アドミッション コントロール セッションを表示できます。

フィールド

- [Active NAC Sessions]：ポスチャ検証の対象のリモート ピアに関する一般的な統計情報。
- [Cumulative NAC Sessions]：現在ポスチャ検証の対象か、または以前から対象だったリモート ピアに関する一般的な統計情報。
- [Accepted]：ポスチャ検証に成功し、Access Control Server によってアクセス ポリシーが与えられたピアの数。
- [Rejected]：ポスチャ検証に失敗し、Access Control Server によってアクセス ポリシーが与えられなかったピアの数。
- [Exempted]：セキュリティ アプライアンスで設定された [Posture Validation Exception] リストのエントリに一致するため、ポスチャ検証の対象になっていないピアの数。
- [Non-responsive]：Extensible Authentication Protocol（EAP）over UDP のポスチャ検証要求に応答しないピアの数。CTA が実行されていないピアは、この要求に応答しません。セキュリティ アプライアンスのコンフィギュレーションがクライアントレス ホストをサポートする場合、Access Control Server は、クライアントレス ホストに関連付けられているアクセス ポリシーをこれらのピアのセキュリティ アプライアンスにダウンロードします。クライアントレス ホストをサポートしない場合、セキュリティ アプライアンスは NAC デフォルト ポリシーを割り当てます。
- [Hold-off]：ポスチャ検証が成功した後に、セキュリティ アプライアンスが EAPoUDP 通信を失ったピアの数。NAC Hold Timer 属性（[Configuration] > [VPN] > [NAC]）は、このタイプのイベントと次のポスチャ検証試行との間の遅延時間を判定します。
- [N/A]：VPN NAC グループ ポリシーに従って NAC が無効になっているピアの数。
- [Revalidate All]：ピアのポスチャまたは割り当てられているアクセス ポリシー（ダウンロードされた ACL）が変更された場合にクリックします。このボタンをクリックすると、セキュリティ アプライアンスによって管理されるすべての NAC セッションの新しい無条件のポスチャ検証を開始します。このボタンをクリックするまで各セッションに対して有効だったポスチャ検証と割り当てられているアクセス ポリシーは、新しいポスチャ検証が成功または失敗するまで有効のままとなります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。
- [Initialize All]：ピアのポスチャまたは割り当てられているアクセス ポリシー（ダウンロードされた ACL）が変更され、セッションに割り当てられているリソースをクリアする場合にクリックします。このボタンをクリックすると、セキュリティ アプライアンスによって管理されるすべての NAC セッションのポスチャ検証で使用される EAPoUDP アソシエーションと割り当てられているアクセス ポリシーをパージし、新しい無条件のポスチャ検証を開始します。再検証中には NAC の

デフォルトの ACL が有効となるため、セッションを初期化するとユーザ トラフィックに影響する場合があります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Protocol Statistics

このパネルには、セキュリティ アプライアンスで現在アクティブなユーザおよび管理者セッションによって使用されるプロトコルが表示されます。テーブルの各行は、1 つのプロトコル タイプを表します。

フィールド

- [Show Statistics For]：特定のサーバやグループ、またはすべてのトンネル グループを選択します。
- [Protocol Statistics]：現在アクティブなセッションで使用中のすべてのプロトコルの統計情報を示します。
  - [Protocol]：この行の統計情報が適用されるプロトコルを一覧表示します。
  - [Sessions]：このプロトコルを使用するセッションの数を一覧表示します。
  - [Percentage]：アクティブなセッションの合計に対する、このプロトコルを使用しているセッションの割合を数値で示します。このカラムの合計は 100 % になります（端数は処理）。
- [Total Active Sessions]：現在アクティブなセッションの数を示します。
- [Cumulative Sessions]：セキュリティ アプライアンスを最後にブートまたはリセットしたときからのセッションの合計数を示します。
- [Refresh]：[Protocol Statistics] テーブルに表示される統計情報を更新します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

VLAN Mapping Sessions

このパネルには、使用中の各グループ ポリシーの Restrict Access to VLAN パラメータの値で判別された、出力 VLAN に割り当てられているセッション数が表示されます。セキュリティ アプライアンスはすべてのトラフィックを指定された VLAN に転送します。

フィールド

- [Active VLAN Mapping Sessions]：出力 VLAN に割り当てられている VPN セッションの数。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Global IKE/IPSec Statistics

このパネルには、セキュリティ アプライアンスで現在アクティブなユーザおよび管理者セッションのグローバル IKE/IPSec 統計情報が表示されます。テーブルの各行は、1 つのグローバル統計情報を表します。

フィールド

- [Show Statistics For]：特定のプロトコル、[IKE Protocol]（デフォルト）または [IPSec Protocol] を選択します。
- [Global IKE/IPSec Statistics]：現在アクティブなセッションで使用中のすべてのプロトコルの統計情報を示します。
  - [Statistic]：統計変数の名前を一覧表示します。このカラムの内容は、Show Statistics For パラメータで選択した値によって異なります。
  - [Value]：この行にある統計情報の数値。
- [Refresh]：[Global IKE/IPSec Statistics] テーブルに表示される統計情報を更新します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Crypto Statistics

このパネルには、セキュリティ アプライアンスで現在アクティブなユーザおよび管理者セッションの暗号統計情報が表示されます。テーブルの各行は、1 つの暗号統計情報を表します。

フィールド

- [Show Statistics For]：特定のプロトコル、IKE Protocol（デフォルト）、IPSec Protocol、SSL Protocol、または他のプロトコルを選択します。
- [Crypto Statistics]：現在アクティブなセッションで使用中のすべてのプロトコルの統計情報を示します。
  - [Statistic]：統計変数の名前を一覧表示します。このカラムの内容は、Show Statistics For パラメータで選択した値によって異なります。
  - [Value]：この行にある統計情報の数値。
- [Refresh]：[Crypto Statistics] テーブルに表示される統計情報を更新します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Compression Statistics

このパネルには、セキュリティ アプライアンスで現在アクティブなユーザおよび管理者セッションの圧縮統計情報が表示されます。テーブルの各行は、1 つの圧縮統計情報を表します。

フィールド

- [Show Statistics For]: クライアントレス SSL VPN または SSL VPN クライアント セッションの圧縮統計情報を選択できます。
- [Statistics]：選択した VPN タイプの統計情報をすべて表示します。
  - [Statistic]：統計変数の名前を一覧表示します。このカラムの内容は、Show Statistics For パラメータで選択した値によって異なります。
  - [Value]：この行にある統計情報の数値。
- [Refresh]：[Compression Statistics] テーブルに表示される統計情報を更新します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Cluster Loads

このパネルを使用して、VPN ロードバランシング クラスタ内のサーバ間における現在のトラフィックの負荷分散を表示します。サーバがクラスタの一部でない場合、このサーバが VPN ロードバランシング クラスタに参加していない旨を伝える情報メッセージが表示されます。

フィールド

- [VPN Cluster Loads] : VPN ロードバランシング クラスタの現在の負荷分散を表示します。カラム ヘッダーをクリックすると、選択したカラムをソート キーとしてテーブルがソートされます。
  - [Public IP Address] : 外部から可視となっているサーバの IP アドレスを表示します。
  - [Role] : このサーバが、クラスタ内のマスター デバイスかバックアップ デバイスかを示します。
  - [Priority] : クラスタ内のこのサーバに割り当てられているプライオリティを示します。プライオリティは、1（最低）～ 10（最高）の範囲の整数である必要があります。プライオリティは、VPN ロード バランシング クラスタ内でクラスタのマスターまたはプライマリ デバイスになるデバイスを決定する方法の 1 つとして、マスター選出プロセスで使用されます。
  - [Model] : このサーバのセキュリティ アプライアンスのモデル名と番号を示します。
  - [Load %] : サーバの容量に基づいて、サーバの合計容量のうち使用中の割合を示します。
  - [Sessions] : 現在アクティブなセッションの数を示します。
- [Refresh] : テーブルに更新後の統計情報をロードします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

SSO Statistics for Clientless SSL VPN Session

このパネルには、セキュリティ アプライアンスに設定されている現在アクティブな SSO サーバのシングル サインオン統計情報が表示されます。

（注）　これらの統計情報は、SiteMinder サーバおよび SAML Browser Post Profile サーバの SSO に関するものだけです。

フィールド

- [Show Statistics For SSO Server]：SSO サーバを選択します。
- [SSO Statistics]：選択した SSO サーバで現在アクティブなセッションの統計情報を示します。次のような SSO 統計情報が表示されます。
  - SSO サーバの名前
  - SSO サーバのタイプ
  - 認証スキームのバージョン（SiteMinder サーバ）
  - Web エージェントの URL（SiteMinder サーバ）
  - アサーション コンシューマの URL（SAML POST サーバ）
  - 発行元（SAML POST サーバ）
  - 保留中の要求の数
  - 許可要求数
  - 再送信の数
  - 受け入れ数
  - 拒否数
  - タイムアウトの回数
  - 認識されない応答の数
- [Refresh]：[SSO Statistics] テーブルに表示される統計情報を更新します。
- [Clear SSO Server Statistics]：表示されているサーバの統計情報をリセットします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

VPN Connection Status

このパネルを使用して、Easy VPN クライアントとして設定されているセキュリティ アプライアンスのステータスを表示します。この機能は ASA 5505 だけに適用されます。

フィールド

[VPN Client Detail]：Easy VPN クライアントとして設定されている ASA 5505 の設定情報を表示します。

[Connect]：クライアント接続を確立します。

[Refresh]：[VPN Client Detail] パネルに表示されている情報をリフレッシュします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

CHAPTER 47

プロパティのモニタリング

この章は、次の内容で構成されています。

AAA サーバ

このペインでは、AAA サーバの統計情報を表示およびリフレッシュできます。

フィールド

- [Server Group]：設定されているサーバ グループ、または何も設定されていない場合は [LOCAL] を表示します。
- [Protocol]：AAA でサーバ グループが使用するプロトコルを表示します。
- [IP address]：設定されている AAA サーバの IP アドレスを表示します。
- [Status]：設定されている AAA サーバのステータス（[Active] または [Inactive]）を表示します。

AAA サーバのリストの下は、設定されている各サーバの統計情報です。統計情報をクリアするには、[Clear Server Statistics] をクリックします。サーバ ステータスをリフレッシュするには、[Update Server Status] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Device Access

このペインでは、管理セッション、AAA にロックアウトされたユーザ、および認証されたユーザをモニタできます。この項では、次のトピックについて取り上げます。

- AAA Local Locked Out Users
- Authenticated Users
- ASDM/HTTPS セッション
- Secure Shell Sessions
- Telnet Sessions

AAA Local Locked Out Users

[AAA Local Locked Out Users] ペインでは、ログイン試行が失敗したために、ASDM からロックアウトされたユーザのリストを表示できます。また、選択したロックアウト条件またはすべてのロックアウトをクリアすることもできます。

フィールド

- [Currently locked out users]：現在ロックアウトされているユーザのリストを表示します。
- [Lock Time]：ユーザがシステムからロック アウトされてからの経過時間を指定します。
- [Failed Attempts]：失敗したログイン試行回数を指定します。
- [User]：ログイン試行に失敗したユーザ名。
- [Clear lockout]：選択したユーザのロックアウト条件をクリアする場合にクリックします。
- [Clear all lockouts]：すべてのユーザのロックアウト条件をクリアする場合にクリックします。すべてのロックアウトをクリアする前に、ロックアウト条件のリストを更新することをお勧めします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Authenticated Users

このペインでは、セキュリティ アプライアンスの使用を認証されているユーザを表示できます。各行が 1 ユーザを表します。

フィールド

- [User]：セキュリティ アプライアンスの使用を認証されているユーザのユーザ名を表示します。
- [IP Address]：セキュリティ アプライアンスの使用を認証されているユーザの IP アドレスを表示します。
- [Dynamic ACL]：セキュリティ アプライアンスの使用を認証されているユーザのダイナミック アクセス リストを表示します。
- [Inactivity Timeout]：セッションがタイムアウトになってユーザが切断されるまでに、選択したユーザが非アクティブのままでいなければならない時間を表示します。
- [Absolute Timeout]：セッションが閉じ、ユーザが切断されるまでに、選択したユーザが接続したままでいられる時間を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ASDM/HTTPS セッション

[ASDM/HTTPS] ペインでは、現在接続中の ASDM/HTTPS セッションを表示できます。

フィールド

- [Session ID]：接続中の ASDM/HTTPS セッションの名前を表示します。
- [IP Address]：このセキュリティ アプライアンスへの接続が許可されている各ホストまたはネットワークの IP アドレスを表示します。
- [Disconnect]：接続中の ASDM/HTTPS セッションを切断する場合に選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Secure Shell Sessions

[Secure Shell Sessions] ペインでは、SSH プロトコルを使用して管理アクセスのために、セキュリティ アプライアンスに接続されているホストを表示できます。

フィールド

- [Client]：選択した SSH セッションのクライアント タイプを表示します。
- [User]：選択した SSH セッションのユーザ名を表示します。
- [State]：選択した SSH セッションのステートを表示します。
- [Version]：セキュリティ アプライアンスへの接続に使用されている SSH のバージョンを表示します。
- [Encryption (in)]：選択したセッションで使用されているインバウンド暗号化方法を表示します。
- [Encryption (out)]：選択したセッションで使用されているアウトバウンド暗号化方法を表示します。
- [HMAC (in)]：選択したインバウンド SSH セッションに設定されている HMAC を表示します。
- [HMAC (out)]：選択したアウトバウンド SSH セッションに設定されている HMAC を表示します。
- [SID]：選択したセッションのセキュア ID を表示します。
- [Disconnect]：接続中の SSH セッションを切断する場合にクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Telnet Sessions

[Telnet Sessions] ペインでは、現在接続中の Telnet セッションを表示できます。

フィールド

- [Session ID]：接続中の Telnet セッションの名前を表示します。
- [IP Address]：Telnet を通したセキュリティ アプライアンスへの接続が許可されている各ホストの IP アドレスを表示します。
- [Disconnect]：接続中の Telnet セッションを切断する場合にクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Connection Graphs

[Connection Graphs] ペインでは、セキュリティ アプライアンスの接続情報をグラフ形式で表示できます。NAT に関する情報と、UDP 接続、AAA パフォーマンスおよび検査情報などのパフォーマンス モニタリング情報を表示できます。この項では、次のトピックについて取り上げます。

- Perfmon
- Xlates

Perfmon

[Perfmon] ペインでは、パフォーマンス情報をグラフ形式で表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [AAA Perfmon]：セキュリティ アプライアンスの AAA パフォーマンス情報を表示します。
  - [Inspection Perfmon]：セキュリティ アプライアンスの検査パフォーマンス情報を表示します。
  - [Web Perfmon]：URL アクセスおよび URL サーバ要求などのセキュリティ アプライアンスの Web パフォーマンス情報を表示します。
  - [Connections Perfmon]：セキュリティ アプライアンスの接続パフォーマンス情報を表示します。
  - [Xlate Perfmon]：セキュリティ アプライアンスの NAT パフォーマンス情報を表示します。
- [Graph Window Title]：グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add]：[Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：選択した統計タイプを [Selected Graphs] フィールドから削除する場合にクリックします。
- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Xlates

このペインでは、アクティブなネットワーク アドレス変換をグラフ形式で表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [Xlate Utilization]：セキュリティ アプライアンスの NAT の使用状況を表示します。
- [Graph Window Title]：グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add]：[Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択したエントリを削除するには、このフィールドをクリックします。
- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CRL

このペインでは、選択した CA 証明書の関連付けられた CRL を表示またはクリアできます。

フィールド

- [CA Certificate Name]：ドロップダウン リストから選択した証明書の名前を選択します。
- [View CRL]：選択した CRL を表示するには、このフィールドをクリックします。

- [Clear CRL]：選択した CRL をキャッシュからクリアするには、このフィールドをクリックします。
- [CRL Info]：*表示専用*。詳細な CRL 情報を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

DNS Cache

セキュリティ アプライアンス では、特定のクライアントレス SSL VPN および certificate コマンドに送信された外部 DNS クエリーの DNS 情報のローカル キャッシュを提供します。各 DNS 変換要求は、ローカル キャッシュで最初に検索されます。ローカル キャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカル キャッシュで要求を解決できない場合、設定されているさまざまな DNS サーバに DNS クエリーが送信されます。外部 DNS サーバによって要求が解決された場合、結果の IP アドレスと、対応するホスト名が一緒にローカル キャッシュに格納されます。

特記事項

- DNS キャッシュ エントリには、タイムスタンプが付いています。タイムスタンプは、未使用のエントリをエージング アウトするために使われます。エントリがキャッシュに追加されると、タイムスタンプが初期化されます。エントリにアクセスするたびに、タイムスタンプは更新されます。DNS キャッシュは、設定されている時間間隔ですべてのエントリをチェックし、設定されているエージング アウト タイマーを過ぎたエントリをパージします。
- 新しいエントリが到着して、サイズを超えているかメモリ不足のためにキャッシュに空き領域がない場合、エントリの経過時間に基づいてキャッシュを 3 分の 1 に減らします。一番古いエントリが削除されます。

フィールド

- [Host]：ホストの DNS 名を表示します。
- [IP Address]：ホスト名に解決するアドレスを示します。
- [Permanent]：エントリが **name** コマンドで作成されたかどうかを示します。
- [Idle Time]：セキュリティ アプライアンスが最後にそのエントリを参照してからの経過時間を指定します。
- [Active]：エントリがエージング アウトしたかどうかを示します。キャッシュに適切なスペースがないときに、このエントリは削除されることがあります。
- [Clear Cache]：DNS キャッシュ全体をクリアします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

IP Audit

[IP Audit] ペインでは、情報シグニチャおよび攻撃シグニチャに一致するパケットの数をグラフ形式、または表形式で表示できます。各グラフ タイプには、この機能がイネーブルになっているすべてのインターフェイスの合計パケット数が表示されます。

フィールド

- [Available Graphs]：モニタリングに使用可能なシグニチャのタイプを一覧表示します。各シグニチャ タイプの詳細については、「IP Audit Signatures」を参照してください。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。
  - [IP Options]：次のシグニチャのパケット数を表示します。
    Bad Options List (1000)
    Timestamp (1002)
    Provide s, c, h, tcc (1003)
    SATNET ID (1005)
  - [IP Route Options]：次のシグニチャのパケット数を表示します。
    Loose Source Route (1004)
    Record Packet Route (1001)
    Strict Source Route (1006)
  - [IP Attacks]：次のシグニチャのパケット数を表示します。
    IP Fragment Attack (1100)
    Impossible IP Packet (1102)
    IP Teardrop (1103)
  - [ICMP Requests]：次のシグニチャのパケット数を表示します。
    Echo Request (2004)
    Time Request (2007)
    Info Request (2009)
    Address Mask Request (2011)
  - [ICMP Responses]：次のシグニチャのパケット数を表示します。
    Echo Reply (2000)
    Source Quench (2002)
    Redirect (2003)

Time Exceeded (2005)

Parameter Problem (2006)

- [ICMP Replies]：次のシグニチャのパケット数を表示します。
  Unreachable (2001)
  Time Reply (2008)
  Info Reply (2010)
  Address Mask reply (2012)
- [ICMP Attacks]：次のシグニチャのパケット数を表示します。
  Fragmented ICMP (2150)
  Large ICMP (2151)
  Ping of Death (2154)
- [TCP Attacks]：次のシグニチャのパケット数を表示します。
  No Flags (3040)
  SYN & FIN Flags Only (3041)
  FIN Flag Only (3042)
- [UDP Attacks]：次のシグニチャのパケット数を表示します。
  Bomb (4050)
  Snork (4051)
  Chargen (4052)
- [DNS Attacks]：次のシグニチャのパケット数を表示します。
  Host Info (6050)
  Zone Transfer (6051)
  Zone Transfer High Port (6052)
  All Records (6053)
- [FTP Attacks]：次のシグニチャのパケット数を表示します。
  Improper Address (3153)
  Improper Port (3154)
- [RPC Requests to Target Hosts]：次のシグニチャのパケット数を表示します。
  Port Registration (6100)
  Port Unregistration (6101)
  Dump (6102)
- [YP Daemon Portmap Requests]：次のシグニチャのパケット数を示します。
  ypserv Portmap Request (6150)
  ypbind Portmap Request (6151)
  yppasswdd Portmap Request (6152)
  ypupdated Portmap Request (6153)
  ypxfrd Portmap Request (6154)
- [Miscellaneous Portmap Requests]：次のシグニチャのパケット数を示します。

mountd Portmap Request (6155)

rexd Portmap Request (6175)

- [Miscellaneous RPC Calls]：次のシグニチャのパケット数を示します。

  rexd Attempt (6180)

- [RPC Attacks]：次のシグニチャのパケット数を表示します。

  statd Buffer Overflow (6190)

  Proxied RPC (6103)

- [Add]：選択したグラフ タイプを [Selected Graphs] リストに追加するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択したグラフ タイプを削除するには、このフィールドをクリックします。
- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。
- [Selected Graphs]：[Selected Graphs] リストに表示するグラフ タイプを一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

System Resources Graphs

このペインでは、セキュリティ アプライアンスのメモリ、CPU およびブロックの使用状況を表示できます。この項では、次のトピックについて取り上げます。

- Blocks
- CPU
- Memory

Blocks

[Blocks] では、空きメモリ ブロックと使用中のメモリ ブロックを表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [Blocks Used]：セキュリティ アプライアンスで使用中のメモリ ブロックを表示します。
  - [Blocks Free]：セキュリティ アプライアンスの空きメモリ ブロックを表示します。

- [Graph Window Title] : グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add] : [Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove] : [Selected Graphs] リストから選択した統計タイプを削除するには、このフィールドをクリックします。
- [Show Graphs] : 新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CPU

このペインでは、CPU の使用状況を表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs] : グラフ化できるコンポーネントを一覧表示します。
  - [CPU Utilization] : セキュリティ アプライアンスの CPU の使用状況を表示します。
- [Graph Window Title] : グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add] : [Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove] : [Selected Graphs] リストから選択したグラフ タイプを削除するには、このフィールドをクリックします。
- [Show Graphs] : 新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Memory

このペインでは、メモリの使用状況を表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [Free Memory]：セキュリティ アプライアンスの空きメモリを表示します。
  - [Used Memory]：セキュリティ アプライアンスの使用中のメモリを表示します。
- [Graph Window Title]：グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add]：[Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択したグラフ タイプを削除するには、このフィールドをクリックします。
- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

WCCP

Web Cache Communication Protocol（WCCP）は IPv4 トラフィック フローをリアルタイムで Web キャッシュにリダイレクトします。ASDM では、WCCP を使用するインターフェイスのパケット リダイレクションを監視できます。WCCP は、ロードバランシング、スケーリング、耐障害性、およびフェールセーフ サービスも提供します。ロードバランシングは、宛先 IP アドレスに基づくハッシュによって提供されます。ハッシュ値を使用して、トラフィック フローの出力インターフェイスが選択さ

れます。また、このプロトコルを使用すると、セキュリティ アプライアンスと WCCP クライアントでサービス グループを形成してサービスをサポートすることもできます。この項では、次のトピックについて取り上げます。

- Service Groups
- Redirection

Service Groups

このペインでは、サービス グループ、表示モード、およびハッシュ設定を表示およびリフレッシュできます。

フィールド

- [Service Group]：ドロップダウン リストから該当するサービス グループを選択します。
- [Display Mode]：ドロップダウン リストから表示モードを選択します。
- [Destination IP Address]：宛先 IP アドレスを指定します。
- [Source IP Address]：送信元 IP アドレスを指定します。
- [Destination Port]：宛先ポート番号を指定します。
- [Source Port]：送信元ポート番号を指定します。

Redirection

このペインでは、WCCP インターフェイスの統計情報を要約または詳細形式で表示およびリフレッシュできます。

フィールド

- [Show Summary]：統計情報を要約形式で表示するには、このオプションを選択します。
- [Show Details]：統計情報を詳細形式で表示するには、このオプションを選択します。

APPENDIX A

機能のライセンスと仕様

この付録では、機能のライセンスと仕様について説明します。この付録は、次の項で構成されています。

セキュリティ アプライアンスと ASDM リリースの互換性

表 1 に、セキュリティ アプライアンスの各リリースで使用できる ASDM または PDM のバージョンを示します。

表 1　セキュリティ アプライアンスと ASDM/PDM リリースの互換性

セキュリティ アプライアンスのリリース	ASDM/PDM バージョン
8.0(x)	ASDM 6.0(x)
7.2(x)	ASDM 5.2(x)
7.1(x)	ASDM 5.1(x)
7.0(x)	ASDM 5.0(x)
PIX 6.3(x)	PDM 4.1(x)

クライアント PC のオペレーティング システムとブラウザの要件

表 2 に、ASDM でサポートされる推奨プラットフォームを一覧表示します。ASDM は他のブラウザやブラウザ バージョンで動作する場合もありますが、公式にサポートされているブラウザのみを示します。以前の PDM 版とは異なり、Java をインストールしておく必要があることに注意してください。Windows のネイティブ JVM はサポートされなくなっており、動作しません。

表 2　オペレーティング システム、ブラウザ、および Java の要件

	オペレーティング システム	Java アプレットを実行するブラウザ	ASDM ランチャ	その他の要件
Windows[1] プロセッサ：Intel Pentium IV、AMD Athlon または同等品 メモリ：最小 512 MB RAM ディスプレイ：最小解像度 1024x768、および 256 色	Windows 2000（Service Pack 4）または Windows XP オペレーティング システム、英語または日本語	Java[2] プラグイン 1.4.2 または 5.0（1.5）をインストール済みの Internet Explorer 6.0 （注）　**HTTP 1.1**：[Internet Options] > [Advanced] > [HTTP 1.1] の設定では、プロキシ接続と非プロキシ接続の両方で HTTP 1.1 を使用してください。 Java プラグイン[2] 1.4.2 または 5.0（1.5）をインストール済みの Firefox 1.5	Java 1.4.2 または 5.0（1.5）[2]	**SSL 暗号化設定**：ブラウザの詳細設定で、SSL で使用可能な暗号化オプションがすべてイネーブルになります。
Sun SPARC Solaris メモリ：最小 512 MB RAM ディスプレイ：最小解像度 1024x768、および 256 色	Sun Solaris 8 または 9	Java プラグイン[2] 1.4.2 または 5.0（1.5）をインストール済みの Firefox 1.5	使用できません。	
Linux メモリ：最小 256 MB RAM ディスプレイ：最小解像度 1024x768、および 256 色	Red Hat Linux Desktop または Red Hat Enterprise Linux WS、バージョン 3 GNOME または KDE デスクトップ環境	Java プラグイン[2] 1.4.2 または 5.0（1.5）をインストール済みの Firefox 1.5	使用できません。	

1. ASDM は、Windows 3.1、95、98、Me または Windows NT4 ではサポートされません。
2. 最新の Java を http://java.sun.com/ からダウンロードします。

サポートされているプラットフォームと機能

このソフトウェア バージョンでは、次のプラットフォームをサポートしています。各モデルでサポートされる機能については関連テーブルを参照してください。

- ASA 5505、表 A-3
- ASA 5510、表 A-4
- ASA 5520、表 A-5
- ASA 5540、表 A-6
- ASA 5550、表 A-7
- PIX 515/515E、表 A-8
- PIX 525、表 A-9

- PIX 535、表 A-10

（注）　イタリック体で示された項目は、基本ライセンスを変更できる個別のオプション ライセンスです。ライセンスは、混合し組み合わせることができます。たとえば、10 セキュリティ コンテキスト ライセンスと Strong Encryption ライセンス、500 Clientless SSL VPN ライセンスと GTP/GPRS ライセンス、または 4 つのライセンスを同時に使用することができます。

表 A-3　ASA 5505 適応型セキュリティ アプライアンス ライセンスの機能

ASA 5505	基本ライセンス		セキュリティ プラス	
ユーザ、同時[1]	10	*オプションのライセンス：*	10	*オプションのライセンス：*
		50　*無制限*		*50*　*無制限*
セキュリティ コンテキスト	サポートなし		サポートなし	
VPN セッション[2]	IPSec とクライアントレス SSL VPN の合計で 10		IPSec とクライアントレス SSL VPN の合計で 25	
最大 IPSec セッション数	10		25	
最大クライアントレス SSL VPN セッション数	2	*オプション ライセンス：10*	2	*オプション ライセンス：10*
VPN ロード バランシング	サポートなし		サポートなし	
SIP と Skinny インスペクションのための TLS プロキシ	サポートあり		サポートあり	
フェールオーバー	サポートなし		アクティブ/スタンバイ（ステートフル フェールオーバーなし）	
GTP/GPRS	サポートなし		サポートなし	
最大 VLAN/ゾーン	3（2 つの正規ゾーンともう 1 つの制限ゾーンだけが他の 1 つのゾーンと通信可能）		20	
最大 VLAN トランク数	サポートなし		無制限	
ファイアウォールの同時接続[3]	10 K		25 K	
最大物理インターフェイス数	無制限、VLAN/ゾーンに割り当て済み		無制限、VLAN/ゾーンに割り当て済み	
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*	基本（DES）	*オプション ライセンス：強化（3DES/AES）*
RAM の最小値	256 MB（デフォルト）		256 MB（デフォルト）	

1. ルーテッド モードの場合、内部（ビジネス VLAN およびホーム VLAN）のホストでは、それらが外部（インターネット VLAN）と通信する場合（内部が外部への接続を開始した場合、および外部が内部への接続を開始した場合を含む）にだけ、制限に対してカウントされます。外部が内部への接続を開始した場合でも、外部ホストは制限に対してカウント*されず*、内部ホストだけがカウントされることに注意してください。ビジネスとホーム間のトラフィックを開始するホストも制限に対してカウントされません。デフォルト ルートに関連付けられたインターフェイスは、外部インターネット インターフェイスと見なされます。デフォルト ルートがない場合、すべてのインターフェイス上のホストが制限値にカウントされます。トランスペアレント モードでは、ホスト数が最小のインターフェイスがホスト制限値にカウントされます。ホストの制限を表示するには、**show local-host** コマンドを参照してください。

2. IPSec セッションおよびクライアントレス SSL VPN セッションの最大数の合計は、VPN セッションの最大数を超えることができますが、両セッションを組み合わせた場合は VPN セッションの上限を超えることはできません。VPN の最大セッション数を超えた場合、セキュリティ アプライアンスをオーバーロードして、ネットワークのサイズを適切にすることができます。
3. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

表 A-4　ASA 5510 適応型セキュリティ アプライアンス ライセンスの機能

ASA 5510	基本ライセンス					セキュリティ プラス					
ユーザ、同時	無制限					無制限					
セキュリティ コンテキスト	サポートなし					2	*オプションのライセンス：*				
							5				
VPN セッション[1]	IPSec とクライアントレス SSL VPN の合計で 250					IPSec とクライアントレス SSL VPN の合計で 250					
最大 IPSec セッション数	250					250					
最大クライアントレス SSL VPN セッション数	2	*オプションのライセンス：*				2	*オプションのライセンス：*				
		10	*25*	*50*	*100*	250	*10*	*25*	*50*	*100*	250
VPN ロード バランシング	サポートなし					サポートなし					
SIP と Skinny インスペクションのための TLS プロキシ	サポートあり					サポートあり					
フェールオーバー	サポートなし					アクティブ/スタンバイまたはアクティブ/アクティブ					
GTP/GPRS	サポートなし					サポートなし					
最大 VLAN 数	50					100					
ファイアウォールの同時接続[2]	50 K					130 K					
最大物理インターフェイス数	ファスト イーサネットの速度で無制限					ギガビット イーサネット速度で無制限					
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*				基本（DES）	*オプション ライセンス：強化（3DES/AES）*				
最小 RAM 容量	256 MB（デフォルト）					256 MB（デフォルト）					

1. IPSec セッションおよびクライアントレス SSL VPN セッションの最大数の合計は、VPN セッションの最大数を超えることができますが、両セッションを組み合わせた場合は VPN セッションの上限を超えることはできません。VPN の最大セッション数を超えた場合、セキュリティ アプライアンスをオーバーロードして、ネットワークのサイズを適切にすることができます。
2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

表 A-5　ASA 5520 適応型セキュリティ アプライアンス ライセンスの機能

ASA 5520	基本ライセンス			
ユーザ、同時	無制限			無制限
セキュリティ コンテキスト	2	*オプションのライセンス：*		
		5	10	20

表 A-5　ASA 5520 適応型セキュリティ アプライアンス ライセンスの機能 （続き）

ASA 5520	基本ライセンス											
VPN セッション[1]	IPSec とクライアントレス SSL VPN の合計で 750											
最大 IPSec セッション数	750											
最大クライアントレス SSL VPN セッション数	2	*オプションのライセンス：*										
		10	*25*	*50*	*100*	250	*500*	*750*				
VPN ロード バランシング	サポートあり											
SIP と Skinny インスペクションのための TLS プロキシ	サポートあり											
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ											
GTP/GPRS	なし	*オプション ライセンス：イネーブル*										
最大 VLAN 数	150											
ファイアウォールの同時接続[2]	280 K											
最大物理インターフェイス数	無制限											
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*										
最小 RAM 容量	512 MB（デフォルト）											

1. IPSec セッションおよびクライアントレス SSL VPN セッションの最大数の合計は、VPN セッションの最大数を超えることができますが、両セッションを組み合わせた場合は VPN セッションの上限を超えることはできません。VPN の最大セッション数を超えた場合、セキュリティ アプライアンスをオーバーロードして、ネットワークのサイズを適切にすることができます。
2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

表 A-6　ASA 5540 適応型セキュリティ アプライアンス ライセンスの機能

ASA 5540	基本ライセンス								
ユーザ、同時	無制限					無制限			
セキュリティ コンテキスト	2	オプション ライセンス：							
		5	*10*	*20*	*50*				
VPN セッション[1]	IPSec とクライアントレス SSL VPN の合計で 5000								
最大 IPSec セッション数	5000								
最大クライアントレス SSL VPN セッション数	2	*オプションのライセンス：*							
		10	*25*	*50*	*100*	250	*500*	*750*	*1000*	*2500*
VPN ロード バランシング	サポートあり								
SIP と Skinny インスペクションのための TLS プロキシ	サポートあり								
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ								
GTP/GPRS	なし	*オプション ライセンス：イネーブル*							

表 A-6　ASA 5540 適応型セキュリティ アプライアンス ライセンスの機能 （続き）

ASA 5540	基本ライセンス	
最大 VLAN 数	200	
ファイアウォールの同時接続[2]	400 K	
最大物理インターフェイス数	無制限	
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*
最小 RAM 容量	1 GB（デフォルト）	

1. IPSec セッションおよびクライアントレス SSL VPN セッションの最大数の合計は、VPN セッションの最大数を超えることができますが、両セッションを組み合わせた場合は VPN セッションの上限を超えることはできません。VPN の最大セッション数を超えた場合、セキュリティ アプライアンスをオーバーロードして、ネットワークのサイズを適切にすることができます。
2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

表 A-7　ASA 5550 適応型セキュリティ アプライアンス ライセンスの機能

ASA 5550	基本ライセンス									
ユーザ、同時	無制限									
セキュリティ コンテキスト	2	オプション ライセンス：								
		5	*10*	*20*	*50*					
VPN セッション[1]	IPSec とクライアントレス SSL VPN の合計で 5000									
最大 IPSec セッション数	5000									
最大クライアントレス SSL VPN セッション数	2	*オプションのライセンス：*								
		10	*25*	*50*	*100*	250	*500*	*750*	*1000*	*2500*	5000
VPN ロード バランシング	サポートあり									
SIP と Skinny インスペクションのための TLS プロキシ	サポートあり									
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ									
GTP/GPRS	なし	*オプション ライセンス：イネーブル*								
最大 VLAN 数	250									
ファイアウォールの同時接続[2]	650 K									
最大物理インターフェイス数	無制限									
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*								
最小 RAM 容量	4 GB（デフォルト）									

1. IPSec セッションおよびクライアントレス SSL VPN セッションの最大数の合計は、VPN セッションの最大数を超えることができますが、両セッションを組み合わせた場合は VPN セッションの上限を超えることはできません。VPN の最大セッション数を超えた場合、セキュリティ アプライアンスをオーバーロードして、ネットワークのサイズを適切にすることができます。

2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

表 A-8　PIX 515/515E セキュリティ アプライアンス ライセンスの機能

PIX 515/515E	R（制限付き）	UR（制限なし）	FO（フェールオーバー）[1]	FO-AA（フェールオーバー Active/Active）[1]
ユーザ、同時	無制限	無制限	無制限	無制限
セキュリティ コンテキスト	サポートなし	2　オプション ライセンス：5	2　オプション ライセンス：5	2　オプション ライセンス：5
IPSec セッション	2000	2000	2000	2000
クライアントレス SSL VPN セッション	サポートなし	サポートなし	サポートなし	サポートなし
VPN ロード バランシング	サポートなし	サポートなし	サポートなし	サポートなし
SIP と Skinny インスペクションのための TLS プロキシ	サポートなし	サポートなし	サポートなし	サポートなし
フェールオーバー	サポートなし	アクティブ/スタンバイ アクティブ/アクティブ	アクティブ/スタンバイ	アクティブ/スタンバイ アクティブ/アクティブ
GTP/GPRS	なし	*オプション ライセンス：イネーブル*	なし	*オプション ライセンス：イネーブル*	なし	*オプション ライセンス：イネーブル*	なし	*オプション ライセンス：イネーブル*
最大 VLAN 数	10	25	25	25
ファイアウォールの同時接続[2]	48 K	130 K	130 K	130 K
最大物理インターフェイス数	3	6	6	6
暗号化	なし	*オプション ライセンス：基本（DES）* / *強力（3DES/AES）*	なし	*オプション ライセンス：基本（DES）* / *強力（3DES/AES）*	なし	*オプション ライセンス：基本（DES）* / *強力（3DES/AES）*	なし	*オプション ライセンス：基本（DES）* / *強力（3DES/AES）*
最小 RAM 容量	64 MB（デフォルト）	128 MB	128 MB	128 MB

1. このライセンスは、UR ライセンスを持つ別の装置とのフェールオーバー ペアだけで使用できます。どちらの装置も同じモデルである必要があります。
2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

表 A-9　PIX 525 セキュリティ アプライアンス ライセンスの機能

PIX 525	R（制限付き）	UR（制限なし）	FO（フェールオーバー）[1]	FO-AA（フェールオーバー Active/Active）[1]
ユーザ、同時	無制限	無制限	無制限	無制限
セキュリティ コンテキスト	サポートなし	2 オプション ライセンス： *5* *10* *20* *50*	2 オプション ライセンス： *5* *10* *20* *50*	2 オプション ライセンス： *5* *10* *20* *50*
IPSec セッション	2000	2000	2000	2000
クライアントレス SSL VPN セッション	サポートなし	サポートなし	サポートなし	サポートなし
VPN ロード バランシング	サポートなし	サポートなし	サポートなし	サポートなし
SIP と Skinny インスペクションのための TLS プロキシ	サポートなし	サポートなし	サポートなし	サポートなし
フェールオーバー	サポートなし	アクティブ/スタンバイ アクティブ/アクティブ	アクティブ/スタンバイ	アクティブ/スタンバイ アクティブ/アクティブ
GTP/GPRS	なし *オプション ライセンス：イネーブル*	なし *オプション ライセンス：イネーブル*	なし *オプション ライセンス：イネーブル*	なし *オプション ライセンス：イネーブル*
最大 VLAN 数	25	100	100	100
ファイアウォールの同時接続[2]	140 K	280 K	280 K	280 K
最大物理インターフェイス数	6	10	10	10
暗号化	なし *オプション ライセンス：* *基本（DES）*　*強力（3DES/AES）*	なし *オプション ライセンス：* *基本（DES）*　*強力（3DES/AES）*	なし *オプション ライセンス：* *基本（DES）*　*強力（3DES/AES）*	なし *オプション ライセンス：* *基本（DES）*　*強力（3DES/AES）*
最小 RAM 容量	128 MB（デフォルト）	256 MB	256 MB	256 MB

1. このライセンスは、UR ライセンスを持つ別の装置とのフェールオーバー ペアだけで使用できます。どちらの装置も同じモデルである必要があります。
2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

表 A-10　PIX 535 セキュリティ アプライアンス ライセンスの機能

PIX 535	R（制限付き）		UR（制限なし）		FO（フェールオーバー）[1]		FO-AA（フェールオーバー Active/Active）[1]	
ユーザ、同時	無制限		無制限		無制限		無制限	
セキュリティ コンテキスト	サポートなし		2	*オプション ライセンス：*	2	*オプション ライセンス：*	2	*オプション ライセンス：*
			5	*10* *20* *50*	*5*	*10* *20* *50*	*5*	*10* *20* *50*
IPSec セッション	2000		2000		2000		2000	
クライアントレス SSL VPN セッション	サポートなし		サポートなし		サポートなし		サポートなし	
VPN ロード バランシング	サポートなし		サポートなし		サポートなし		サポートなし	
SIP と Skinny インスペクションのための TLS プロキシ	サポートなし		サポートなし		サポートなし		サポートなし	
フェールオーバー	サポートなし		アクティブ/スタンバイ アクティブ/アクティブ		アクティブ/スタンバイ		アクティブ/スタンバイ アクティブ/アクティブ	
GTP/GPRS	なし	*オプション ライセンス：イネーブル*	なし	*オプション ライセンス：イネーブル*	なし	*オプション ライセンス：イネーブル*	なし	*オプション ライセンス：イネーブル*
最大 VLAN 数	50		150		150		150	
ファイアウォールの同時接続[2]	250 K		500 K		500 K		500 K	
最大物理インターフェイス数	8		14		14		14	
暗号化	なし	*オプション ライセンス：*	なし	*オプション ライセンス：*	なし	*オプション ライセンス：*	なし	*オプション ライセンス：*
		基本（DES） *強力（3DES/AES）*		*基本（DES）* *強力（3DES/AES）*		*基本（DES）* *強力（3DES/AES）*		*基本（DES）* *強力（3DES/AES）*
最小 RAM 容量	512 MB（デフォルト）		1024 MB		1024 MB		1024 MB	

1. このライセンスは、UR ライセンスを持つ別の装置とのフェールオーバー ペアだけで使用できます。どちらの装置も同じモデルである必要があります。
2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

セキュリティ サービス モジュールのサポート

表 A-11 に、各プラットフォームでサポートされる SSM を示します。

表 A-11　SSM サポート

プラットフォーム	SSM モデル
ASA 5505	サポートなし
ASA 5510	10AIP SSM CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5520	10AIP SSM AIP SSM 20 CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5540	10AIP SSM AIP SSM 20 CSC SSM 10[1] CSC SSM 20[1] 4GE SSM
ASA 5550	サポートなし（4GE SSM が組み込まれており、ユーザが取り除くことはできません）
PIX 515/515E	サポートなし
PIX 525	サポートなし
PIX 535	サポートなし

1. CSC SSM ライセンスでは最大 1,000 ユーザをサポートでき、Cisco ASA 5540 シリーズ アプライアンスではさらに多くのユーザをサポートできます。CSC SSM を ASA 5540 適応型セキュリティ アプライアンスとともに展開する場合、スキャンする必要があるトラフィックにだけ CSC SSM が送信されるようにセキュリティ アプライアンスを設定してください。

VPN 仕様

この項では、セキュリティ アプライアンスの VPN 仕様について説明します。この項では、次のトピックについて取り上げます。

- 「Cisco VPN Client サポート」（P.A-11）
- 「Cisco Secure Desktop のサポート」（P.A-11）
- 「サイトツーサイト VPN の互換性」（P.A-11）
- 「暗号標準」（P.A-12）

Cisco VPN Client サポート

セキュリティ アプライアンスは、表 A-12 に示すように、ソフトウェアベースとハードウェアベースの幅広いさまざまな Cisco VPN クライアントをサポートします。

表 A-12　Cisco VPN Client サポート

クライアント タイプ	クライアントのバージョン
SSL VPN クライアント	Cisco SSL VPN Client、バージョン 1.1 以降
ソフトウェア IPSec VPN クライアント	Windows 版 Cisco VPN Client、バージョン 3.6 以降 Linux 版 Cisco VPN Client、バージョン 3.6 以降 Solaris 版 Cisco VPN Client、バージョン 3.6 以降 Mac OS X 版 Cisco VPN Client、バージョン 3.6 以降
ハードウェア IPSec VPN クライアント（Cisco Easy VPN リモート）	Cisco VPN 3002 ハードウェア クライアント、バージョン 3.0 以降 Cisco IOS ソフトウェア Easy VPN リモート、リリース 12.2(8)YJ Cisco PIX 500 シリーズ セキュリティ アプライアンス、バージョン 6.2 以降 Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、バージョン 7.0 以降

Cisco Secure Desktop のサポート

セキュリティ アプライアンスは CSD ソフトウェア バージョン 3.1.1.16 をサポートしています。

サイトツーサイト VPN の互換性

多くのサードパーティ VPN 製品との相互運用性に加えて、セキュリティ アプライアンスは、表 A-13 に示すサイトツーサイト VPN 接続向けの Cisco VPN 製品との相互運用性も提供します。

表 A-13　サイトツーサイト VPN の互換性

プラットフォーム	ソフトウェア バージョン
Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス	バージョン 7.0(1) 以降
Cisco IOS ルータ	リリース 12.1(6)T 以降
Cisco PIX 500 シリーズ セキュリティ アプライアンス	バージョン 5.1(1) 以降
Cisco VPN 3000 シリーズ コンセントレータ	バージョン 3.6(1) 以降

暗号標準

セキュリティ アプライアンスは、表 A-14 に示す項目を含め、数多くの暗号標準と関連のサード パーティ製品およびサービスをサポートしています。

表 A-14　暗号標準

タイプ	説明
非対称（公開キー）暗号化アルゴリズム	RSA 公開 / 秘密キー ペア、512 ビット ～ 4096 ビット DSA 公開 / 秘密キー ペア、512 ビット ～ 1024 ビット
対称暗号化アルゴリズム	AES：128、192、および 256 ビット DES：56 ビット 3DES：168 ビット RC4：40、56、64、および 128 ビット
完全転送秘密（Diffie-Hellman キー ネゴシエーション）	グループ 1：768 ビット グループ 2：1024 ビット グループ 5：1536 ビット グループ 7：163 ビット（Elliptic Curve Diffie-Hellman） **（注）** **グループ 7** コマンド オプションは ASA バージョン 8.0(4) で**非推奨**になりました。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。
ハッシュ アルゴリズム	MD5：128 ビット SHA-1：160 ビット
X.509 認証局	Cisco IOS ソフトウェア Baltimore UniCERT Entrust Authority iPlanet CMS Microsoft Certificate Services RSA Keon VeriSign OnSite
X.509 証明書登録方法	SCEP PKCS #7 および #10

APPENDIX B

許可および認証用の外部サーバの設定

この付録では、セキュリティ アプライアンスで AAA をサポートするための外部 LDAP、RADIUS、または TACACS+ サーバの設定方法について説明します。外部サーバを使用するようにセキュリティ アプライアンスを設定する前に、正しいセキュリティ アプライアンス認証属性でサーバを設定し、それらの属性のサブセットから個々のユーザに対する個別の許可を割り当てる必要があります。

この付録は、次の項で構成されています。

権限および属性のポリシー実施の概要

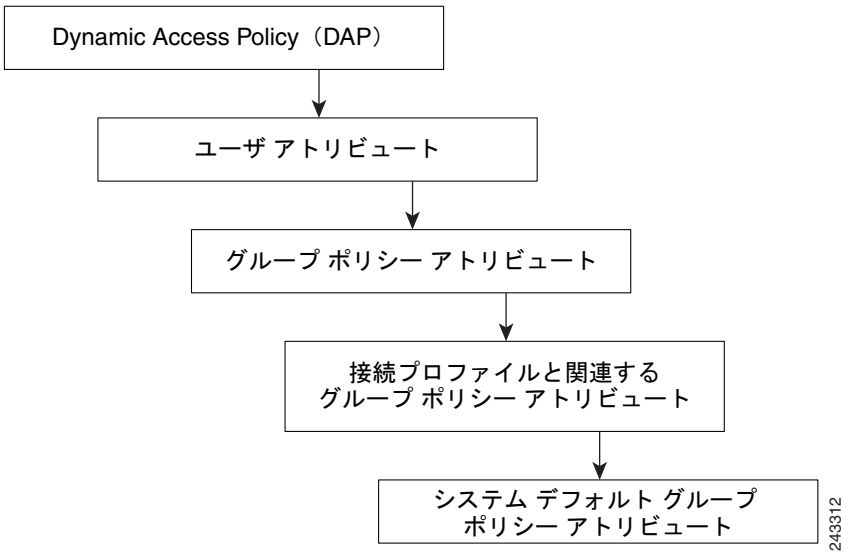
セキュリティ アプライアンスは、ユーザ許可属性（ユーザ権利またはユーザ権限とも呼ばれる）を VPN 接続に適用するためのいくつかの方法をサポートしています。ユーザ属性を、セキュリティ アプライアンスの Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）から、外部認証サーバや許可 AAA サーバ（RADIUS または LDAP）から、セキュリティ アプライアンスのグループ ポリシーから、またはこれら 3 つのすべてから取得できるようにセキュリティ アプライアンスを設定できます。

セキュリティ アプライアンスがすべてのソースから属性を受信すると、それらの属性は評価および集約され、ユーザ ポリシーに適用されます。DAP、AAA サーバ、またはグループ ポリシーから取得した属性の間で衝突がある場合、DAP から取得した属性が常に優先されます。

セキュリティ アプライアンスは、次の順序で属性を適用します（図 B-1 も参照してください）。

1. セキュリティ アプライアンスの DAP 属性：バージョン 8.0 に導入され、最も優先されます。DAP にブックマーク /URL リストを設定した場合、そのリストはグループ ポリシーのブックマーク /URL リスト セットよりも優先されます。
2. AAA サーバのユーザ属性：ユーザ認証または許可が成功すると、AAA サーバはこれらの属性を返します。これらの属性を、セキュリティ アプライアンスのローカル AAA データベースの個々のユーザに設定されている属性（ASDM のユーザ アカウント）と混同しないでください。
3. セキュリティ アプライアンスで設定されたグループ ポリシー：RADIUS サーバがユーザに対して RADIUS CLASS 属性 IETF-Class-25（OU=<group-policy>）の値を返す場合、セキュリティ アプライアンスは、ユーザを同じ名前のグループ ポリシーに配置し、サーバから返されないすべての属性をそのグループ ポリシーで適用します。LDAP サーバでは、任意の属性名を使用してセッションのグループ ポリシーを設定できます。セキュリティ アプライアンスで設定した LDAP 属性マップは、LDAP 属性を Cisco 属性 IETF-Radius-Class にマッピングします。
4. 接続プロファイル（CLI では *トンネル グループ*と呼ばれます）により割り当てられるグループ ポリシー：接続プロファイルは、接続の暫定的な設定を含み、認証前のユーザに適用されるデフォルトのグループ ポリシーが設定されています。セキュリティ アプライアンスに接続するすべてのユーザは、最初にこのグループに所属します。このグループでは、DAP、サーバから返されるユーザ属性、またはユーザに割り当てられるグループ ポリシーで不足しているすべての属性が提供されます。
5. セキュリティ アプライアンスで割り当てられたデフォルトのグループ ポリシー（DfltGrpPolicy）：システムのデフォルト属性は、DAP、ユーザ属性、グループ ポリシー、または接続プロファイルで不足している値を提供します。

図 B-1　ポリシー実施フロー



外部 LDAP サーバの設定

VPN 3000 コンセントレータと ASA/PIX 7.0 では、認証作業に Cisco LDAP スキーマが必要でした。バージョン 7.1.x 以降では、セキュリティ アプライアンスは、ネイティブ LDAP スキーマを使用して認証*および*許可を行うため、Cisco スキーマは必要とされません。

許可（権限ポリシー）の設定は、LDAP 属性マップを使用して行います。例については、次を参照してください。
「許可および認証用の外部サーバの設定」（P.B-1）。

この項では、LDAP サーバの構造、スキーマ、および属性について説明します。説明する項目は次のとおりです。

- 「LDAP 操作のためのセキュリティ アプライアンスの構成」（P.B-3）
- 「セキュリティ アプライアンスの LDAP コンフィギュレーションの定義」（P.B-5）
- 「ASDM を使用して LDAP を設定する場合の追加情報」（P.B-14）

上記のプロセスは、使用する LDAP サーバのタイプによって異なります。

（注）　LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

LDAP 操作のためのセキュリティ アプライアンスの構成

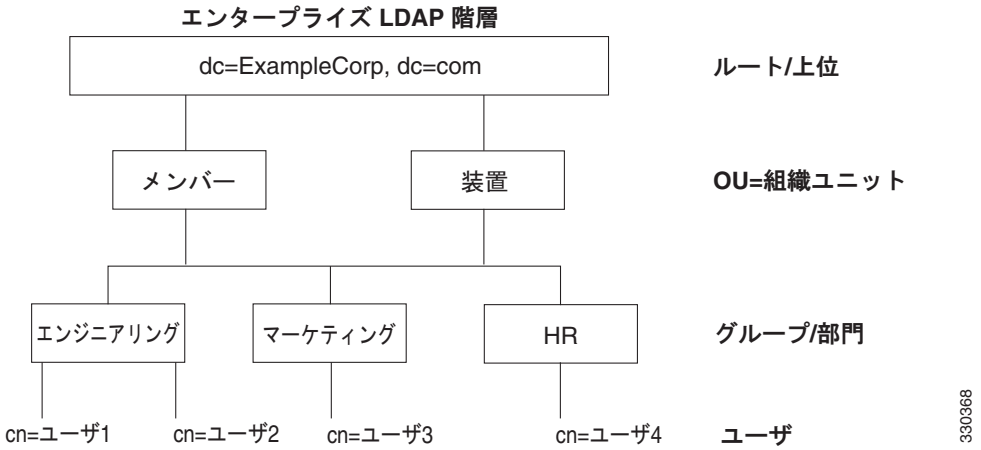
この項では、LDAP 階層、およびセキュリティ アプライアンスの LDAP サーバへの認証済みバインディング内で検索を実行する方法について説明します。説明する項目は次のとおりです。

- 「階層の検索」（P.B-4）
- 「セキュリティ アプライアンスと LDAP サーバのバインディング」（P.B-5）
- 「Active Directory の Login DN の例」（P.B-5）

LDAP コンフィギュレーションは、組織の論理階層が反映されたものにする必要があります。たとえば、Example Corporation という企業の従業員 Terry を例に考えてみます。Terry はエンジニアリング グループに従事しています。この企業の LDAP 階層は 1 つ以上のレベルを持つことができます。Terry を Example Corporation のメンバーと想定して、浅いシングルレベルの階層をセットアップすることを決定できます。あるいは、マルチレベルの階層をセットアップすることもできます。この場合、Terry は Engineering 部門のメンバーであると想定され、この部門は People と呼ばれる組織ユニットのメンバーであり、Example Corporation のメンバーです。マルチレベルの階層の例については、図 B-2 を参照してください。

マルチレベル階層はより細かく設定できますが、シングルレベル階層の方が迅速に検索できます。

図 B-2　マルチレベルの LDAP 階層



階層の検索

セキュリティ アプライアンスでは、LDAP 階層内での検索を調整できます。セキュリティ アプライアンスに次の 3 種類のフィールドを設定すると、LDAP 階層での検索開始場所とその範囲、および検索する情報のタイプを定義できます。これらのフィールドを組み合わせて使用することにより、ユーザの権限が含まれているツリーの部分だけを検索するように階層の検索を限定できます。

- LDAP Base DN は、サーバがセキュリティ アプライアンスから許可要求を受信したときにユーザ情報の検索を開始する LDAP 階層を定義します。
- Search Scope では、LDAP 階層の検索範囲を定義します。この指定では、LDAP Base DN よりもかなり下位のレベルまで検索します。サーバが行う検索を直下の 1 レベルだけにするか、サブツリー全体を検索するかを選択できます。シングルレベルの検索の方が高速ですが、サブツリー検索の方が広範囲に検索できます。
- Naming Attribute では、LDAP サーバのエントリを一意に識別する RDN を定義します。一般的な名前属性には、cn（一般名）、sAMAccountName、および userPrincipalName を含めることができます。

図 B-2 では、Example Corporation で可能な LDAP 階層の例を示します。この階層が指定されると、複数の方法で検索を定義できます。表 B-1 は、使用可能な 2 種類の検索のコンフィギュレーションを示します。

最初のコンフィギュレーションの例では、Terry が必要な LDAP 許可を得て自身の IPSec トンネル接続を確立すると、セキュリティ アプライアンスは LDAP サーバに検索要求を送信します。この要求では、サーバが Terry を代行して Engineering グループの検索を実行することを指定します。この検索は短時間でできます。

2 番目のコンフィギュレーションの例では、セキュリティ アプライアンスは、Terry を代行してサーバが Example Corporation 全体を検索するよう指示する検索要求を送信します。この検索には時間がかかります。

表 B-1　検索コンフィギュレーションの例

#	LDAP Base DN	検索範囲	名前属性	結果
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	1 レベル	cn=Terry	検索が高速
2	dc=ExampleCorporation,dc=com	サブツリー	cn=Terry	検索に時間がかかる

セキュリティ アプライアンスと LDAP サーバのバインディング

一部の LDAP サーバ（Microsoft Active Directory サーバなど）は、セキュリティ アプライアンスに対し、他のあらゆる LDAP 操作の要求を受け入れる前に、認証済みバインディングを介してハンドシェイクを確立することを要求します。セキュリティ アプライアンスは、ログイン DN フィールドをユーザ認証要求にアタッチして、認証済みバインディングに対して識別情報を示します。Login DN フィールドでは、セキュリティ アプライアンスの認証特性を定義します。これらの特性は、管理特権を持つユーザの特性に対応している必要があります。たとえば、Login DN フィールドを cn=Administrator、cn=users、ou=people、dc=example、dc=com のように定義できます。

（注） LDAP クライアントとして、セキュリティ アプライアンスは、匿名のバインドまたは要求の送信をサポートしていません。

Active Directory の Login DN の例

Login DN は、ユーザ検索が行われる前に、セキュリティ アプライアンスがバインドの交換中に LDAP クライアントと LDAP サーバ間の信頼性を確立するために使用する LDAP サーバ上のユーザ名です。

VPN の認証/許可の操作、および、バージョン 8.0.4 以降の AD グループの取得（password-management の変更が不要なときの読み取り専用操作）では、特権の低い Login DN を使用できます。たとえば、Login DN には、Domain Users グループの memberOf で指定されているユーザを指定できます。

VPN の password-management の変更では、Login DN にはアカウント オペレータの特権が必要となります。

これらのいずれの場合でも、Login/Bind DN には、スーパーユーザ レベルの特権は必要ありません。特定の Login DN 要件については、LDAP アドミニストレータ ガイドを参照してください。

セキュリティ アプライアンスの LDAP コンフィギュレーションの定義

この項では、LDAP AV-pair 属性の構文の定義方法について説明します。説明する項目は次のとおりです。

- 「LDAP 許可でサポートされている Cisco 属性」（P.B-6）
- 「Cisco-AV-Pair 属性構文」（P.B-12）

（注）　セキュリティ アプライアンスは、数値の ID ではなく属性名に基づいて LDAP 属性を使用します。一方、RADIUS 属性には、名前ではなく数値の ID が使用されます。

許可では、権限または属性を使用するプロセスを参照します。認証サーバまたは許可サーバとして定義されている LDAP サーバは、権限または属性が設定されている場合はこれらを使用します。

ソフトウェア バージョン 7.0 の LDAP 属性には、cVPN3000 プレフィックスが含まれています。バージョン 7.1 以降では、このプレフィックスは削除されています。

LDAP 許可でサポートされている Cisco 属性

この項では、ASA 5500、VPN 3000、および PIX 500 シリーズのセキュリティ アプライアンスで使用される属性の詳細なリスト（表 B-2）を示します。この表には、これらのセキュリティ アプライアンスを組み合わせたネットワーク構成に役立つ VPN 3000 と PIX 500 シリーズの属性サポート情報が含まれています。

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Access-Hours	Y	Y	Y	文字列	シングル	time-range の名前（Business-Hours など）
Allow-Network-Extension- Mode	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
Authenticated-User-Idle- Timeout	Y	Y	Y	整数型	シングル	1 ～ 35791394 分
Authorization-Required	Y			整数型	シングル	0 = しない 1 = する
Authorization-Type	Y			整数型	シングル	0 = なし 1 = RADIUS 2 = LDAP
Auth-Service-Type						
Banner1	Y	Y	Y	文字列	シングル	バナー文字列
Banner2	Y	Y	Y	文字列	シングル	バナー文字列
Cisco-AV-Pair	Y	Y	Y	文字列	マルチ	次の形式のオクテット文字列： [Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port] 詳細については、Cisco-AV-Pair 属性構文を参照してください。
Cisco-IP-Phone-Bypass	Y	Y	Y	整数型	シングル	0 = ディセーブル 1 = イネーブル
Cisco-LEAP-Bypass	Y	Y	Y	整数型	シングル	0 = ディセーブル 1 = イネーブル

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Client-Intercept-DHCP-Configure-Msg	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
Client-Type-Version-Limiting	Y	Y	Y	文字列	シングル	IPSec VPN クライアントのバージョン番号を示す文字列
Confidence-Interval	Y	Y	Y	整数型	シングル	10 ～ 300 秒
DHCP-Network-Scope	Y	Y	Y	文字列	シングル	IP アドレス
DN-Field	Y	Y	Y	文字列	シングル	有効な値：UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name
Firewall-ACL-In		Y	Y	文字列	シングル	アクセス リスト ID
Firewall-ACL-Out		Y	Y	文字列	シングル	アクセス リスト ID
IE-Proxy-Bypass-Local				ブール	シングル	0=ディセーブル 1=イネーブル
IE-Proxy-Exception-List				文字列	シングル	DNS ドメインのリスト。エントリは改行文字シーケンス（\n）で区切る必要があります。
IE-Proxy-Method	Y	Y	Y	整数型	シングル	1 = プロキシ設定を変更しない 2 = プロキシを使用しない 3 = 自動検出 4 = セキュリティ アプライアンス 設定を使用する
IE-Proxy-Server	Y	Y	Y	整数型	シングル	IP アドレス
IETF-Radius-Class	Y	Y	Y		シングル	リモート アクセス VPN セッションのグループ ポリシーを設定します。
IETF-Radius-Filter-Id	Y	Y	Y	文字列	シングル	セキュリティ アプライアンスで定義されたアクセス リスト名
IETF-Radius-Framed-IP-Address	Y	Y	Y	文字列	シングル	IP アドレス
IETF-Radius-Framed-IP-Netmask	Y	Y	Y	文字列	シングル	IP アドレス マスク
IETF-Radius-Idle-Timeout	Y	Y	Y	整数型	シングル	分
IETF-Radius-Service-Type	Y	Y	Y	整数型	シングル	
IETF-Radius-Session-Timeout	Y	Y	Y	整数型	シングル	
IKE-Keep-Alives	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Allow-Passwd-Store	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
IPSec-Authentication	Y	Y	Y	整数型	シングル	0 = なし 1 = RADIUS 2 = LDAP（許可のみ） 3 = NT ドメイン 4 = SDI（RSA） 5 = 内部 6 = RADIUS での Expiry 7 = Kerberos/Active Directory
IPSec-Auth-On-Rekey	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Backup-Server-List	Y	Y	Y	文字列	シングル	サーバ アドレス（スペース区切り）
IPSec-Backup-Servers	Y	Y	Y	文字列	シングル	1 = クライアントが設定したリストを使用する 2 = クライアント リストをディセーブルにして消去する 3 = バックアップ サーバ リストを使用する
IPSec-Client-Firewall-Filter- Name	Y			文字列	シングル	クライアントにファイアウォール ポリシーとして配信するフィルタの名前を指定します。
IPSec-Client-Firewall-Filter-Optional	Y	Y	Y	整数型	シングル	0 = 必須 1 = オプション
IPSec-Default-Domain	Y	Y	Y	文字列	シングル	クライアントに送信する 1 つのデフォルト ドメイン名を指定します（1 ～ 255 文字）。
IPSec-IKE-Peer-ID-Check	Y	Y	Y	整数型	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IPSec-IP-Compression	Y	Y	Y	整数型	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Mode-Config	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Over-UDP	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Over-UDP-Port	Y	Y	Y	整数型	シングル	4001 ～ 49151、デフォルトは 10000
IPSec-Required-Client-Firewall-Capability	Y	Y	Y	整数型	シングル	0 = なし 1 = リモート FW Are-You-There（AYT）で定義されているポリシー 2 = Policy pushed CPP 4 = サーバからのポリシー
IPSec-Sec-Association	Y			文字列	シングル	セキュリティ アソシエーションの名前

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
IPSec-Split-DNS-Names	Y	Y	Y	文字列	シングル	クライアントに送信するセカンダリ ドメイン名のリストを指定します（1 ～ 255 文字）。
IPSec-Split-Tunneling-Policy	Y	Y	Y	整数型	シングル	0 = すべてをトンネリング 1 = スプリット トンネリング 2 = ローカル LAN を許可
IPSec-Split-Tunnel-List	Y	Y	Y	文字列	シングル	スプリット トンネルの包含リストを記述したネットワークまたはアクセス リストの名前を指定します。
IPSec-Tunnel-Type	Y	Y	Y	整数型	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPSec-User-Group-Lock	Y			ブール	シングル	0 = ディセーブル 1 = イネーブル
L2TP-Encryption	Y			整数型	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビット 4 =128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化 / ステートレスが必要
L2TP-MPPC-Compression	Y			整数型	シングル	0 = ディセーブル 1 = イネーブル
MS-Client-Subnet-Mask	Y	Y	Y	文字列	シングル	IP アドレス
PFS-Required	Y	Y	Y	ブール	シングル	0 = しない 1 = する
Port-Forwarding-Name	Y	Y		文字列	シングル	名前の文字列（「Corporate-Apps」など）
PPTP-Encryption	Y			整数型	シングル	ビットマップ： 1 = 暗号化が必要 2 =40 ビット 4 =128 ビット 8 = ステートレスが必要 例： 15 = 40/128 ビットで暗号化 / ステートレスが必要
PPTP-MPPC-Compression	Y			整数型	シングル	0 = ディセーブル 1 = イネーブル
Primary-DNS	Y	Y	Y	文字列	シングル	IP アドレス
Primary-WINS	Y	Y	Y	文字列	シングル	IP アドレス
Privilege-Level						

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Required-Client-Firewall-Vendor-Code	Y	Y	Y	整数型	シングル	1 = シスコ（Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = シスコ（Cisco Intrusion Prevention Security Agent を使用）
Required-Client-Firewall-Description	Y	Y	Y	文字列	シングル	文字列
Required-Client-Firewall-Product-Code	Y	Y	Y	整数型	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client（CIC） Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Agent Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Require-HW-Client-Auth	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
Require-Individual-User-Auth	Y	Y	Y	整数型	シングル	0 = ディセーブル 1 = イネーブル
Secondary-DNS	Y	Y	Y	文字列	シングル	IP アドレス
Secondary-WINS	Y	Y	Y	文字列	シングル	IP アドレス
SEP-Card-Assignment				整数型	シングル	未使用
Simultaneous-Logins	Y	Y	Y	整数型	シングル	0-2147483647
Strip-Realm	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
TACACS-Authtype	Y	Y	Y	整数	シングル	
TACACS-Privilege-Level	Y	Y	Y	整数	シングル	
Tunnel-Group-Lock		Y	Y	文字列	シングル	トンネル グループの名前または「none」

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Tunneling-Protocols	Y	Y	Y	整数型	シングル	1 = PPTP 2 = L2TP 4 = IPSec 8 = L2TP/IPSec 16 = WebVPN. 8 および 4 は相互排他値 （0 ～ 11、16 ～ 27 は有効値）
Use-Client-Address	Y			ブール	シングル	0 = ディセーブル 1 = イネーブル
User-Auth-Server-Name	Y			文字列	シングル	IP アドレスまたはホスト名
User-Auth-Server-Port	Y			整数型	シングル	サーバ プロトコルのポート番号
User-Auth-Server-Secret	Y			文字列	シングル	サーバのパスワード
WebVPN-ACL-Filters		Y		文字列	シングル	アクセス リスト名
WebVPN-Apply-ACL-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Citrix-Support-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Content-Filter-Parameters	Y	Y		整数型	シングル	1 = Java および ActiveX 2 = Java スクリプト 4 = イメージ 8 = イメージに含まれるクッキー 複数のパラメータをフィルタリングするには値を加算します。たとえば、Java スクリプトとクッキーの両方をフィルタリングするには 10 を入力します。（10 = 2 + 8）
WebVPN-Enable-functions				整数型	シングル	使用しない（廃止）
WebVPN-Exchange-Server-Address				文字列	シングル	使用しない（廃止）
WebVPN-Exchange-Server-NETBIOS-Name				文字列	シングル	使用しない（廃止）
WebVPN-File-Access-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Browsing-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Entry- Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Forwarded-Ports		Y		文字列	シングル	ポート転送リスト名
WebVPN-Homepage	Y	Y		文字列	シングル	URL（http://example-portal.com など）
WebVPN-Macro-Substitution-Value1	Y	Y		文字列	シングル	

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
WebVPN-Macro-Substitution-Value2	Y	Y		文字列	シングル	
WebVPN-Port-Forwarding-Auto-Download-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding- Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-HTTP-Proxy-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Single-Sign-On-Server-Name		Y		文字列	シングル	SSO サーバの名前（1 ～ 31 文字）
WebVPN-SVC-Client-DPD	Y	Y		整数型	シングル	0 = ディセーブル n = デッドピア検出値（30 ～ 3600 秒）
WebVPN-SVC-Compression	Y	Y		整数型	シングル	0 = なし 1 = デフレート圧縮
WebVPN-SVC-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Gateway-DPD	Y	Y		整数型	シングル	0 = ディセーブル n = デッドピア検出値（30 ～ 3600 秒）
WebVPN-SVC-Keepalive	Y	Y		整数型	シングル	0 = ディセーブル n = キープアライブ値（15 ～ 600 秒）
WebVPN-SVC-Keep-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Rekey-Method	Y	Y		整数型	シングル	0 = なし 1 = SSL 2 = 新規トンネル 3 = 任意（SSL に設定）
WebVPN-SVC-Rekey-Period	Y	Y		整数型	シングル	0 = ディセーブル n = 分単位の再試行間隔 （4 ～ 10080 分）
WebVPN-SVC-Required-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-URL-Entry-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-URL-List		Y		文字列	シングル	URL リスト名

Cisco-AV-Pair 属性構文

Cisco-AV-Pair ルールの構文は次のとおりです。

[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]

表 B-3 で構文のルールについて説明します。

表 B-3　AV-Pair 属性の構文ルール

フィールド	説明
Prefix	AV ペアの固有の識別子。例：ip:inacl#1=（標準アクセス リスト用）または webvpn:inacl#（クライアントレス SSL VPN アクセス リスト用）。このフィールドは、フィルタが AV ペアとして送信された場合にだけ表示されます。
Action	deny、permit など、ルールが一致した場合に実行するアクション。
Protocol	IP プロトコルの番号または名前。0 ～ 255 の整数値、または icmp、igmp、ip、tcp、udp のいずれかのキーワード。
Source	パケットを送信するネットワークまたはホスト。IP アドレス、ホスト名、またはキーワード「any」で指定します。IP アドレスを使用する場合、続いて Source Wildcard Mask を指定する必要があります。
Source Wildcard Mask	送信元アドレスに適用されるワイルドカード マスク。
Destination	パケットを受信するネットワークまたはホスト。IP アドレス、ホスト名、またはキーワード「any」で指定します。IP アドレスを使用する場合、続いて Source Wildcard Mask を指定する必要があります。
Destination Wildcard Mask	宛先アドレスに適用されるワイルドカード マスク。
Log	FILTER ログ メッセージを生成します。重大度レベル 9 のイベントを生成するには、このキーワードを使用する必要があります。
Operator	論理演算子：greater than、less than、equal to、not equal to。
Port	TCP または UDP ポートの番号（0 ～ 65535）。

次に例を示します。

```
ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log

webvpn:inacl#1=permit url http://www.website.com
webvpn:inacl#2=deny smtp any host 10.1.3.5
webvpn:inacl#3=permit url cifs://mar_server/peopleshare1
```

（注） リモート IPSec トンネルおよび SSL VPN Client（SVC）トンネルにアクセス リストを適用するには、Cisco-AV-Pair エントリにプレフィックス ip:inacl# を追加して使用してください。

SSL VPN クライアントレス（ブラウザモード）トンネルにアクセス リストを適用するには、Cisco-AV-Pair エントリにプレフィックス webvpn:inacl# を追加して使用してください。

表 B-4 に、Cisco-AV-Pair 属性のトークンの一覧を示します。

表 B-4　セキュリティ アプライアンスでサポートされるトークン

トークン	構文のフィールド	説明
ip:inacl#*Num*=	該当なし（識別子）	（*Num* は固有の整数）。AV ペアのアクセス コントロール リストをすべて開始します。リモート IPSec トンネルと SSL VPN（SVC）トンネルにアクセス リストを適用します。
webvpn:inacl#*Num*=	該当なし（識別子）	（*Num* は固有の整数）。クライアントレス SSL AV ペアのアクセス コントロール リストをすべて開始します。クライアントレス（ブラウザモード）トンネルにアクセス リストを適用します。
deny	アクション	アクションを拒否します。（デフォルト）
permit	アクション	アクションを許可します。
icmp	プロトコル	インターネット制御メッセージ プロトコル（ICMP）
1	プロトコル	インターネット制御メッセージ プロトコル（ICMP）
IP	プロトコル	インターネット プロトコル（IP）
0	プロトコル	インターネット プロトコル（IP）
TCP	プロトコル	伝送制御プロトコル（TCP）
6	プロトコル	伝送制御プロトコル（TCP）
UDP	プロトコル	ユーザ データグラム プロトコル（UDP）
17	プロトコル	ユーザ データグラム プロトコル（UDP）
any	ホスト名	すべてのホストにルールを適用します。
host	ホスト名	ホスト名を示す任意の英数字文字列。
log	ログ	イベントが一致すると、フィルタ ログ メッセージが表示されます （permit and log または deny and log の場合と同様）。
lt	演算子	値より小さい
gt	演算子	値より大きい
eq	演算子	値と等しい
neq	演算子	値と等しくない
range	演算子	この範囲に含まれる。range の後に 2 つの値を続けます。

ASDM を使用して LDAP を設定する場合の追加情報

ASDM を使用して LDAP を設定する場合の追加情報は、次の URL の Cisco.com のセキュリティ アプライアンスに関するマニュアル領域で入手できます。

http://www.cisco.com/en/US/products/ps6121/products_installation_and_configuration_guides_list.html

カテゴリ「*Selected ASDM Configuration Topics for ASA*」には、Microsoft Active Directory サーバを使用してセキュリティ アプライアンス上で認証および許可を設定する手順の例が含まれています。

- ユーザベースの属性ポリシーの適用
- 特定のグループ ポリシーへの LDAP ユーザの配置
- AnyConnect トンネルへのスタティック IP アドレスの割り当て
- ダイヤルインの許可または拒否アクセスの適用

- ログイン時間と Time-of-Day ルールの適用

その他の設定例については、Cisco.com にある次のテクニカル ノートを参照してください。

- 『*ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example*』
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml
- 『*PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login*』
  http://www.cisco.com/en/US/partner/products/ps6120/products_configuration_example09186a00808d1a7c.shtml

外部 RADIUS サーバの設定

この項では、RADIUS の設定手順の概要を示し、Cisco RADIUS 属性を定義します。説明する項目は次のとおりです。

RADIUS 設定手順の確認

この項では、セキュリティ アプライアンスのユーザ認証および許可をサポートするために必要な RADIUS 設定手順について説明します。次の手順に従って、セキュリティ アプライアンスと相互作用する RADIUS サーバをセットアップします。

ステップ 1　セキュリティ アプライアンスの属性を RADIUS サーバにロードします。属性をロードするために使用する方法は、使用する RADIUS サーバのタイプによって異なります。

- Cisco ACS を使用している場合：サーバには、これらの属性がすでに統合されています。したがって、この手順をスキップできます。
- FUNK RADIUS サーバを使用している場合：シスコは、セキュリティ アプライアンスの属性がすべて含まれるディクショナリ ファイルを提供しています。このディクショナリ ファイル `cisco3k.dct` は、CCO のソフトウェア センターまたはセキュリティ アプライアンスの CD-ROM から入手してください。ディクショナリ ファイルをサーバにロードします。
- 他のベンダーの RADIUS サーバ（Microsoft Internet Authentication Service など）：セキュリティ アプライアンスの各属性を手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダー コード（3076）を使用します。セキュリティ アプライアンス RADIUS 許可属性および値のリストについては、表 B-5 を参照してください。

ステップ 2　権限および属性を持つユーザまたはグループをセットアップし、IPSec または SSL トンネルの確立時に送信します。

セキュリティ アプライアンスの RADIUS 許可属性

許可では、権限または属性を使用するプロセスを参照します。認証サーバとして定義されている RADIUS サーバは、権限または属性が設定されている場合はこれらを使用します。

表 B-5 に、ユーザ許可に使用でき、セキュリティ アプライアンスがサポートしている使用可能なすべての RADIUS 属性の一覧を示します。

（注）　RADIUS 属性名には、cVPN3000 プレフィックスは含まれていません。Cisco Secure ACS 4.x は、この新しい名前をサポートしますが、4.0 以前の ACS の属性名にはまだ cVPN3000 プレフィックスが含まれています。アプライアンスは、属性名ではなく数値の属性 ID に基づいて、RADIUS 属性を使用します。LDAP 属性は、ID ではなく属性名で使用します。

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
Access-Hours	Y	Y	Y	1	文字列	シングル	時間範囲の名前（Business-hours など）
Simultaneous-Logins	Y	Y	Y	2	整数型	シングル	0 ～ 2147483647 の整数
Primary-DNS	Y	Y	Y	5	文字列	シングル	IP アドレス
Secondary-DNS	Y	Y	Y	6	文字列	シングル	IP アドレス
Primary-WINS	Y	Y	Y	7	文字列	シングル	IP アドレス
Secondary-WINS	Y	Y	Y	8	文字列	シングル	IP アドレス
SEP-Card-Assignment				9	整数型	シングル	未使用
Tunneling-Protocols	Y	Y	Y	11	整数型	シングル	1 = PPTP 2 = L2TP 4 = IPSec 8 = L2TP/IPSec 16 = WebVPN. 4 および 8 は相互排他値、0 ～ 11 および 16 ～ 27 は有効値
IPSec-Sec-Association	Y			12	文字列	シングル	セキュリティ アソシエーションの名前
IPSec-Authentication	Y			13	整数型	シングル	0 = なし 1 = RADIUS 2 = LDAP（許可のみ） 3 = NT ドメイン 4 = SDI 5 = 内部 6 = RADIUS での Expiry 7 = Kerberos/Active Directory
Banner1	Y	Y	Y	15	文字列	シングル	バナー文字列
IPSec-Allow-Passwd-Store	Y	Y	Y	16	ブール	シングル	0 = ディセーブル 1 = イネーブル

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
Use-Client-Address	Y			17	ブール	シングル	0 = ディセーブル 1 = イネーブル
PPTP-Encryption	Y			20	整数型	シングル	ビットマップ： 1 = 暗号化が必要 2 =40 ビット 4 =128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化 / ステートレスが必要
L2TP-Encryption	Y			21	整数型	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビット 4 =128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化 / ステートレスが必要
IPSec-Split-Tunnel-List	Y	Y	Y	27	文字列	シングル	スプリット トンネルの包含リストを記述したネットワークまたはアクセス リストの名前を指定します。
IPSec-Default-Domain	Y	Y	Y	28	文字列	シングル	クライアントに送信する 1 つのデフォルト ドメイン名を指定します（1 ～ 255 文字）。
IPSec-Split-DNS-Names	Y	Y	Y	29	文字列	シングル	クライアントに送信するセカンダリ ドメイン名のリストを指定します（1 ～ 255 文字）。
IPSec-Tunnel-Type	Y	Y	Y	30	整数型	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPSec-Mode-Config	Y	Y	Y	31	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-User-Group-Lock	Y			33	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Over-UDP	Y	Y	Y	34	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Over-UDP-Port	Y	Y	Y	35	整数型	シングル	4001 ～ 49151、デフォルトは 10000

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
Banner2	Y	Y	Y	36	文字列	シングル	Banner1 文字列に連結されているバナー文字列（設定されている場合）。
PPTP-MPPC-Compression	Y			37	整数型	シングル	0 = ディセーブル 1 = イネーブル
L2TP-MPPC-Compression	Y			38	整数型	シングル	0 = ディセーブル 1 = イネーブル
IPSec-IP-Compression	Y	Y	Y	39	整数型	シングル	0 = ディセーブル 1 = イネーブル
IPSec-IKE-Peer-ID-Check	Y	Y	Y	40	整数型	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IKE-Keep-Alives	Y	Y	Y	41	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Auth-On-Rekey	Y	Y	Y	42	ブール	シングル	0 = ディセーブル 1 = イネーブル
Required-Client- Firewall-Vendor-Code	Y	Y	Y	45	整数型	シングル	1 = シスコ（Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = シスコ（Cisco Intrusion Prevention Security Agent を使用）

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
Required-Client-Firewall-Product-Code	Y	Y	Y	46	整数型	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client（CIC） Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Agent Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Required-Client-Firewall-Description	Y	Y	Y	47	文字列	シングル	文字列
Require-HW-Client-Auth	Y	Y	Y	48	ブール	シングル	0 = ディセーブル 1 = イネーブル
Required-Individual-User-Auth	Y	Y	Y	49	整数型	シングル	0 = ディセーブル 1 = イネーブル
Authenticated-User-Idle-Timeout	Y	Y	Y	50	整数型	シングル	1 ～ 35791394 分
Cisco-IP-Phone-Bypass	Y	Y	Y	51	整数型	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Split-Tunneling-Policy	Y	Y	Y	55	整数型	シングル	0 = スプリット トンネリングなし 1 = スプリット トンネリング 2 = ローカル LAN を許可
IPSec-Required-Client-Firewall-Capability	Y	Y	Y	56	整数型	シングル	0 = なし 1 = リモート FW Are-You-There（AYT）で定義されているポリシー 2 = Policy pushed CPP 4 = サーバからのポリシー

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
IPSec-Client-Firewall-Filter-Name	Y			57	文字列	シングル	クライアントにファイアウォール ポリシーとして配信するフィルタの名前を指定します。
IPSec-Client-Firewall-Filter-Optional	Y	Y	Y	58	整数型	シングル	0 = 必須 1 = オプション
IPSec-Backup-Servers	Y	Y	Y	59	文字列	シングル	1 = クライアントが設定したリストを使用する 2 = クライアント リストをディセーブルにして消去する 3 = バックアップ サーバ リストを使用する
IPSec-Backup-Server-List	Y	Y	Y	60	文字列	シングル	サーバ アドレス（スペース区切り）
DHCP-Network-Scope	Y	Y	Y	61	文字列	シングル	IP アドレス
Intercept-DHCP-Configure-Msg	Y	Y	Y	62	ブール	シングル	0 = ディセーブル 1 = イネーブル
MS-Client-Subnet-Mask	Y	Y	Y	63	ブール	シングル	IP アドレス
Allow-Network-Extension-Mode	Y	Y	Y	64	ブール	シングル	0 = ディセーブル 1 = イネーブル
Authorization-Type	Y	Y	Y	65	整数型	シングル	0 = なし 1 = RADIUS 2 = LDAP
Authorization-Required	Y			66	整数型	シングル	0 = しない 1 = する
Authorization-DN-Field	Y	Y	Y	67	文字列	シングル	有効な値：UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name
IKE-KeepAlive-Confidence-Interval	Y	Y	Y	68	整数型	シングル	10 ～ 300 秒
WebVPN-Content-Filter-Parameters	Y	Y		69	整数型	シングル	1 = Java ActiveX 2 = Java スクリプト 4 = イメージ 8 = イメージに含まれるクッキー

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
WebVPN-URL-List		Y		71	文字列	シングル	URL リスト名
WebVPN-Port-Forward-List		Y		72	文字列	シングル	ポート転送リスト名
WebVPN-Access-List		Y		73	文字列	シングル	アクセス リスト名
Cisco-LEAP-Bypass	Y	Y	Y	75	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Homepage	Y	Y		76	文字列	シングル	URL（http://example-portal.com など）
Client-Type-Version-Limiting	Y	Y	Y	77	文字列	シングル	IPSec VPN のバージョン番号を示す文字列
WebVPN-Port-Forwarding-Name	Y	Y		79	文字列	シングル	名前の文字列（「Corporate-Apps」など） このテキストでクライアントレス ポータル ホームページのデフォルト文字列「Application Access」が置き換えられます。
IE-Proxy-Server	Y			80	文字列	シングル	IP アドレス
IE-Proxy-Server-Policy	Y			81	整数型	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検出 4 = コンセントレータ設定を使用する
IE-Proxy-Exception-List	Y			82	文字列	シングル	改行（\n）区切りの DNS ドメインのリスト
IE-Proxy-Bypass-Local	Y			83	整数型	シングル	0 = なし 1 = ローカル
IKE-Keepalive-Retry-Interval	Y	Y	Y	84	整数型	シングル	2 ～ 10 秒
Tunnel-Group-Lock		Y	Y	85	文字列	シングル	トンネル グループの名前または「none」
Access-List-Inbound		Y	Y	86	文字列	シングル	アクセス リスト ID
Access-List-Outbound		Y	Y	87	文字列	シングル	アクセス リスト ID

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
Perfect-Forward-Secrecy-Enable	Y	Y	Y	88	ブール	シングル	0 = しない 1 = する
NAC-Enable	Y			89	整数型	シングル	0 = しない 1 = する
NAC-Status-Query-Timer	Y			90	整数型	シングル	30 ～ 1800 秒
NAC-Revalidation-Timer	Y			91	整数型	シングル	300 ～ 86400 秒
NAC-Default-ACL	Y			92	文字列		アクセス リスト
WebVPN-URL-Entry-Enable	Y	Y		93	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Access-Enable	Y	Y		94	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Entry-Enable	Y	Y		95	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Browsing-Enable	Y	Y		96	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-Enable	Y	Y		97	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Outlook-Exchange-Proxy-Enable	Y	Y		98	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-HTTP-Proxy	Y	Y		99	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Auto-Applet-Download-Enable	Y	Y		100	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Citrix-Metaframe-Enable	Y	Y		101	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Apply-ACL	Y	Y		102	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSL-VPN-Client-Enable	Y	Y		103	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSL-VPN-Client-Required	Y	Y		104	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSL-VPN-Client-Keep-Installation	Y	Y		105	整数型	シングル	0 = ディセーブル 1 = イネーブル

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
SVC-Keepalive	Y	Y		107	整数型	シングル	0 = オフ 15 ～ 600 秒
SVC-DPD-Interval-Client	Y	Y		108	整数型	シングル	0 = オフ 5 ～ 3600 秒
SVC-DPD-Interval-Gateway	Y	Y		109	整数型	シングル	0 = オフ 5 ～ 3600 秒
SVC-Rekey-Time		Y		110	整数型	シングル	0 = ディセーブル 1 ～ 10080 分
WebVPN-Deny-Message		Y		116	文字列	シングル	有効な文字列（500 文字以内）
SVC-DTLS		Y		123	整数型	シングル	0 = False 1 = True
SVC-MTU		Y		125	整数型	シングル	MTU 値 256 ～ 1406 バイト
SVC-Modules		Y		127	文字列	シングル	文字列（モジュールの名前）
SVC-Profiles		Y		128	文字列	シングル	文字列（プロファイルの名前）
SVC-Ask		Y		131	文字列	シングル	0 = ディセーブル 1 = イネーブル 3 = デフォルト サービスをイネーブルにする 5 = デフォルト クライアントレスをイネーブルにする （2 と 4 は使用しない）
SVC-Ask-Timeout		Y		132	整数型	シングル	5 ～ 120 秒
IE-Proxy-PAC-URL		Y		133	文字列	シングル	PAC アドレス文字列
Strip-Realm	Y	Y	Y	135	ブール	シングル	0 = ディセーブル 1 = イネーブル
Smart-Tunnel		Y		136	文字列	シングル	スマート トンネルの名前

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
WebVPN-ActiveX-Relay		Y		137	整数型	シングル	0 = ディセーブル Otherwise = イネーブル
Smart-Tunnel-Auto		Y		138	整数型	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動スタート
VLAN		Y		140	整数型	シングル	0 ～ 4094
NAC-Settings		Y		141	文字列	シングル	NAC ポリシーの名前
Member-Of		Y	Y	145	文字列	シングル	カンマ区切りの文字列。例： エンジニアリング、営業
Address-Pools		Y	Y	217	文字列	シングル	IP ローカル プールの名前
IPv6-Address-Pools		Y		218	文字列	シングル	IP ローカル プール IPv6 の名前
IPv6-VPN-Filter		Y		219	文字列	シングル	ACL 値
Privilege-Level		Y	Y	220	整数型	シングル	0 ～ 15 の整数。
WebVPN-Macro-Value1		Y		223	文字列	シングル	無制限
WebVPN-Macro-Value2		Y		224	文字列	シングル	無制限

外部 TACACS+ サーバの設定

セキュリティ アプライアンス は、TACACS+ 属性をサポートします。TACACS+ は、認証、許可、アカウンティングの機能を分離します。プロトコルでは、必須とオプションの 2 種類の属性をサポートします。サーバとクライアントの両方で必須属性を解釈できる必要があり、また、必須属性はユーザに適用する必要があります。オプションの属性は、解釈または使用できることも、できないこともあります。

（注）　TACACS+ 属性を使用するには、NAS で AAA サービスをイネーブルにしておいてください。

表 B-6 に、カットスルー プロキシ接続に対してサポートされている TACACS+ 許可応答属性の一覧を示します。表 B-7 に、サポートされている TACACS+ アカウンティング属性の一覧を示します。

表 B-6　サポートされる TACACS+ 許可応答属性

属性	説明
acl	接続に適用する、ローカルで設定済みのアクセス リストを識別します。
idletime	認証済みユーザ セッションが終了する前に許可される非アクティブ時間（分）を示します。
timeout	認証済みユーザ セッションが終了する前に認証クレデンシャルがアクティブな状態でいる絶対時間（分）を指定します。

表 B-7　サポートされる TACACS+ アカウンティング属性

属性	説明
bytes_in	この接続中に転送される入力バイト数を指定します（ストップ レコードのみ）。
bytes_out	この接続中に転送される出力バイト数を指定します（ストップ レコードのみ）。
cmd	実行するコマンドを定義します（コマンド アカウンティングのみ）。
disc-cause	切断理由を特定する数字コードを示します（ストップ レコードのみ）。
elapsed_time	接続の経過時間（秒）を定義します（ストップ レコードのみ）。
foreign_ip	トンネル接続のクライアントの IP アドレスを指定します。最下位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
local_ip	トンネル接続したクライアントの IP アドレスを指定します。最上位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
NAS port	接続のセッション ID が含まれます。
packs_in	この接続中に転送される入力パケット数を指定します。
packs_out	この接続中に転送される出力パケット数を指定します。
priv-level	コマンド アカウンティング要求に対するユーザの権限レベル、または 1 に設定されます。
rem_iddr	クライアントの IP アドレスを示します。
service	使用するサービスを指定します。コマンド アカウンティングだけは、常に「シェル」に設定されます。
task_id	アカウンティング トランザクションに固有のタスク ID を指定します。
username	ユーザの名前を示します。

INDEX

数字

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

て

と

な

に

ね

は

ひ

ふ

ほ

ま

め

も

ゆ

ら

り

る

れ

ろ

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/