ASDM ユーザ ガイド

Version 5.2(3)F

Text Part Number: OL-15463-01-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、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、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

CHAPTER 1

ASDM の概要

ASDM は、FWSM 上でソフトウェアを設定および管理します。ASDM は FWSM からロードされ、デバイスの設定、監視、および管理に使用されます。

ここでは、次の項目について説明します。

特記事項

- **CLI コマンドのサポート**：いくつかの例外を除き、ほとんどすべての CLI コマンドが ASDM でサポートされています。ASDM がサポートしていないコマンドのリストについては、P.1-3 の「サポートされていないコマンド」を参照してください。
- **多重 ASDM セッション**：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 FWSM ソフトウェアを使用できます。1 つの FWSM 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、特定の FWSM 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、FWSM あたり最大 80 セッションまで接続できます。
- **FWSM のリリース バージョン**：今回リリースされた ASDM に必要な FWSM バージョンは 3.2 です。これより以前にリリースされたバージョンの FWSM では実行できません。
- **警告**：Cisco.com の Bug Toolkit を利用して、現在の警告情報を確認してください。Bug Toolkit は次のアドレスからアクセスできます。

  http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl
- **OS カラー スキームの変更方法**：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。そうしない場合、一部の ASDM 画面が正常に表示されないことがあります。

今回のリリースで追加された機能

ASDM Version 5.2(3)F には次の新機能があります。

- SIP の強化：SIP Invite および SIP Disconnect のタイムアウト値の設定がサポートされています。P.23-9 の「Timeouts」を参照してください。
- インターフェイスごとの DHCP リレー：DHCP ヘルパ アドレス（サーバ アドレス）をインターフェイス単位で設定できます。P.9-2 の「DHCP Relay」を参照してください。
- 透過ファイアウォール NAT/PAT：透過モードで NAT をイネーブルにできます。P.21-1 の「NAT の設定」を参照してください。
- SNMP の強化：次のような新しい SNMP トラップをサポートします。
  - Alarm Asserted または Alarm Cleared
  - Redundancy Switchover（フェールオーバー状態の変更）
  - Resource Limit Reached
  - Rate Limit Reached
  - Packet Discarded
  - CPU Rising Threshold Reached
  - CPU Utilization and Monitoring

  P.8-9 の「SNMP」を参照してください。
- カットスルー プロキシの強化：ユーザ認証がタイムアウトになった後の接続のクリアをサポートします。P.18-18 の「Advanced AAA Configuration」を参照してください。
- 仮想 HTTP/SSH の強化：仮想 Telnet、仮想 SSH、および仮想 HTTP を設定します。P.11-13 の「Virtual Access」を参照してください。
- サービス ポリシー ルールの強化
  - TCP 状態のバイパス：ポリシーと一致するトラフィックをステートレスに検査できます。P.20-21 の「Rule Actions > Connection Settings タブ」を参照してください。
  - フロー ベースのタイムアウト：TCP、UDP、および ICMP など、ポリシー内のすべてのプロトコルに関する接続タイムアウトのサポートが追加されました。P.20-21 の「Rule Actions > Connection Settings タブ」を参照してください。
  - GGSN ロード バランシング：GSN プールに属する GSN が SGSN の要求に応答します。P.6-16 の「Add/Edit GTP Map > Action タブ」を参照してください。
- BGP スタブのルーティング：スタティック ルートおよび直接接続されたネットワークを BGP ピアにブロードキャストします。P.14-3 の「BGP スタブ ルーティング」を参照してください。
- フェールオーバー プリエンプト：Active/Standby フェールオーバーのペアでフェールオーバー プリエンプションを使用できるようになりました。P.12-18 の「Failover: Criteria」を参照してください。
- High Availability and Scalability ウィザード：Active/Active または Active/Standby のフェールオーバーの設定に使用します。また、このウィザードはピア デバイスの高度な設定を行います。P.12-5 の「High Availability and Scalability ウィザード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。

ASDM は次のように強化されました。

- ASDM Rule テーブルの強化：ASDM Rule テーブルの設計が変わり、ポリシーの作成が効率化されます。
- システム ログ メッセージで送信元 IP、宛先 IP、Syslog ID、日時が個々のカラムに表示されます。
- ネットワーク、サービス、プロトコル、および ICMP-type オブジェクト グループをサポートします。
- 名前と IP アドレスを関連付けられます。
- 検索が ASDM Assistant に変わりました。ASDM Assistant はタスク指向のガイダンスを提供し、AAA サーバ、ロギング フィルタなどの機能の設定に役立ちます。

サポートされていないコマンド

FWSM のコマンドはほとんどすべて ASDM 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が ASDM で無視される場合があります。通常、無視されるコマンドはユーザのコンフィギュレーションに記述されています。無視されるコマンドについては、Tools メニューを参照してください。

alias コマンドの場合、コンフィギュレーションからコマンドを削除しないと ASDM はモニタリング専用モードになります。

ここでは、次の項目について説明します。

サポートされていないコマンドによる影響

- 既存の実行コンフィギュレーションを ASDM にロードし、そこに IPv6 関連のコマンドがある場合、ASDM のダイアログボックスに IPv6 はサポートされていないというメッセージが表示されます。ASDM では IPv6 コマンドを一切設定できませんが、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、そこにサポートされていないコマンドがあっても、ASDM の操作には影響しません。サポートされていないコマンドを表示するには、**Options > Show Commands Ignored by ASDM on Device** を実行します。
- 既存の実行コンフィギュレーションを ASDM にロードし、そこに **alias** コマンドがあると、モニタリング専用モードになります。

  モニタリング専用モードの場合、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（**Tools > Command Line Interface**）。ここから CLI コマンドを実行できます。

  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、FWSM のコンソールで **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、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module 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 以下に設定すると、モニタリング専用モードにできるためです。詳細については、**Configuration > Properties > Device Administration > User Accounts** および **Configuration > Device Access > AAA Access** を参照してください。

無視される表示専用コマンド

次の表のコマンドを CLI で追加したコンフィギュレーションは ASDM で使用できますが、ASDM でコマンドの追加および編集はできません。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。

サポートされていないコマンド	ASDM の動作
すべての VPN コマンド、管理アクセス用	無視。
access-list	未使用の場合は無視。
capture	無視。
control-point tcp-normalizer	無視。
established	無視。
failover timeout	無視。
ipv6 （ IPv6 アドレスの場合）	無視。
pager	無視。
pim accept-register route-map	無視。**list** オプションを除き、ASDM では設定不可。
prefix-list	OSPF 領域で使用されていない場合は無視。
route-map	無視。

service-policy global	**match access-list** クラスで使用されている場合は無視。次の例を参考にしてください。
	`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。
sysopt uauth allow-http-cache	無視。
terminal	無視。

CLI のその他の制限事項

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、次のような記述はできません。

```
ip address inside 192.168.2.1 255.255.0.255
```

ASDM ウィンドウについて

ASDM ウィンドウから FWSM のさまざまな機能に簡単にアクセスできます。ASDM ウィンドウには、次のような機能があります。

- メニュー：ファイル、ツール、オプション、およびヘルプにすぐにアクセスできます。
- ツールバー：ASDM をナビゲーションできます。ツールバーからホームページ、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、機能の検索、コンフィギュレーションの保存、ヘルプの参照、ペイン間の前後ナビゲーションもできます。Home、Configuration、Monitoring ボタンをクリックすると、開いたペインから各種の便利なツールを使用できます。ホームページにはさまざまな情報が表示され、一目で確認できます。コンフィギュレーション パネルとモニタリング パネルには、左側のフレームに使いやすいカテゴリ ツリーがあり、そこから詳細なコンフィギュレーション データまたはモニタリング情報にアクセスできます。
- ステータスバー：時刻、接続ステータス、特権レベルを表示します。
- タイトルバー：ASDM のバージョン、デバイスの IP アドレス、およびマルチコンテキスト モードで選択したコンテキストの状態（アクティブまたはスタンバイ）を表示します。

メニュー

ASDM には、次のメニューがあります。

- File メニュー
- Rules メニュー
- Tools メニュー
- Wizards メニュー
- Help メニュー

File メニュー

File メニューから FWSM のコンフィギュレーション データを管理できます。また、次のメニュー項目もあります。

- 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。リフレッシュを実行すると、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できます。
- Show Running Configuration in New Window：現在の実行コンフィギュレーションを別の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：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 All Running Configurations to Flash：（マルチコンテキスト モード）実行コンテキスト 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 Internal Log Buffer to Flash...：ログ バッファをフラッシュ メモリに保存します。

- Print：現在のペインを印刷します。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。ASDM を Netscape Communicator で使用している場合、ユーザが Java アプレットに対する印刷権限を持っていないとセキュリティ ダイアログボックスが表示され、印刷権限を要求されます。Grant をクリックすると、アプレットの印刷権限が与えられます。Internet Explorer の場合は、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 イメージをクリアします。ASDM に接続すると、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 メッセージのバッファをクリアします。
- Exit：ASDM を終了します。

Save Running Configuration to TFTP Server

ダイアログボックスで、現在の実行コンフィギュレーションのコピーを TFTP サーバに保存します。

フィールド

- TFTP Server IP Address：TFTP サーバの IP アドレスを入力します。
- Configuration File Path：ファイルを保存する TFTP サーバのパスを入力します。

モード

次の表に、この機能を使用できるモードを示します。

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

Enter Log File Name

ログ バッファをフラッシュ メモリに保存します。

フィールド

- Use default file name option：ログ バッファの保存ファイル名は LOG-YYYY-MM-DD-hhmmss.txt になります。
- Use user-specified file name option：指定したファイル名でログ バッファを保存します。
- Field Name：保存したログ バッファのファイル名を入力します。

Rules メニュー

Rules メニューでは、NAT とセキュリティ ポリシー ルールを追加または調整できます。また、次のメニュー項目もあります。

- Add：リストの末尾にルールを追加します。
- Insert Before：選択したルールの前にルールを挿入します。
- Insert After：選択したルールの後ろにルールを挿入します。
- Edit：選択したルールを編集します。
- Cut：選択したルールを切り取ります。切り取ったルールはメモリに残り、ペーストできます。
- Copy：選択したルールをコピーします。
- Paste：リストの末尾にルールをペーストします。
- Paste Before：選択したルールの前にルールをペーストします。

- Paste After：選択したルールの後ろにルールをペーストします。
- Delete：選択したルールを削除します。

これらのメニュー項目は、コンフィギュレーション ペインで小さなアイコンとしても使用できます。

Tools メニュー

Tools メニューには ASDM のトラブルシューティング ツールがあります。ここから、別のソフトウェアを ASDM にアップロードしたり、接続状態を確認したり、コマンドラインからコマンドを実行したりできます。

- Command Line Interface：テキスト ベース ツールで FWSM にコマンドを送信し、結果を確認できます。詳細については、Command Line Interface 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 で無視された、サポートされていないコマンドを表示します。詳細については、Tools メニュー ダイアログボックスを参照してください。
- Ping：FWSM 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できる便利なツールで、他のネットワーク デバイスの基本的なテストにも使用できます。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。
- Service Groups：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）を関連付けます。以後、アクセス ルールや、その他の ASDM および CLI 内の機能でサービス グループを使用できます。
- File Management：フラッシュ メモリのディスク パーティションに保存されたファイルを表示、移動、コピー、削除できます。また、ディスク パーティション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で、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 システム間のファイル転送ができます。
- Upgrade Software：FWSM のイメージ ファイルや ASDM のイメージをユーザ PC にダウンロードし、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 ダイアログボックスを参照してください。
- Upload ASDM Assistant Guide：フラッシュ メモリに XML ファイルをアップロードし、ASDM Assistant が使用するデータを格納できます。これらのファイルは Cisco.com からダウンロードできます。
- System Reload：システムをリスタートし、保存したコンフィギュレーションをメモリにリロードします。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。
- Preferences：ASDM の機能の一部を、Web ブラウザのクッキー機能を使用してセッション間で変更します。

Command Line Interface

Command Line Interface ダイアログボックスのテキスト ベース ツールで FWSM にコマンドを送信し、結果を表示できます。

（注） ASDM の CLI ツールからコマンドを入力すると、FWSM の接続ターミナルからコマンドを入力したときと動作が異なる場合があります。

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、問題が生じたコマンドは実行されず、その他のコマンドはエラーを無視して実行されます。エラーが発生した場合は、Response ボックスの表示メッセージでエラー内容とその関連情報を確認できます。

(注)　コマンドのリストについては、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。いくつかの例外を除き、ほとんどすべての CLI コマンドが ASDM でサポートされています。

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 Command Line Interface ダイアログボックスで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、次のように、**noconfirm** キーワード（使用できる場合）を指定します。

```
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 FWSM 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 FWSM を設定すると、最後に加えられた変更が反映されます（**Monitoring** タブをクリックすると、同じ FWSM で現在アクティブな他の管理セッションを確認できます）。

ASDM のコンフィギュレーション変更の表示

CLI ツールでコンフィギュレーションを変更した場合、**Refresh** ボタンをクリックすると、ASDM の変更結果を表示できます。

前提条件

CLI ツールで実行できるコマンドは、ユーザ権限によって異なります。「Authorization」を参照してください。ASDM のメイン ウィンドウの下にあるステータス バーの権限レベルで、CLI 特権コマンドの実行権限の有無を確認できます。

フィールド

- Command：FWSM にコマンドを送信します。
  - Single Line：一度に 1 コマンドだけ入力します。直前に入力したコマンドが表示されていますが、別のコマンドを入力することもできます。
  - Multiple Line：複数のコマンドラインを入力します。
  - Enable context sensitive help (?)：コマンドの CLI ヘルプを表示するには、コマンドの後に「?」を入力します。Enter キーを押さなくても「?」を入力するだけでヘルプが表示されます。

    このチェックボックスをオフにすると、デバイスに送信する前に ASDM は「?」文字をエスケープし、テキスト文字列として「?」を入力することができます。したがって、コマンドのヘルプは表示されません。
- Response：コマンド ボックスに入力したコマンドの実行結果を表示します。
- Send：すべてのコマンドを FWSM に送信します。
- Clear Response：Response ボックスのテキストをすべてクリアします。

モード

次の表に、この機能を使用できるモードを示します。

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

Commands Ignored by ASDM on Device

一部のコマンドは ASDM でサポートされていません。通常、サポートされないコマンドは ASDM の実行時に無視されます。Show Commands Ignored by ASDM on Device を実行すると、未解析コマンドの一覧が表示されます。

ASDM が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、P.1-3 の「サポートされていないコマンド」を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ダイアログボックスの便利なツールで FWSM 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でき、他のネットワーク デバイスの基本的なテストもできます。

ping は、潜水艦の音波探知機と同等のネットワーク ツールです。ping を IP アドレスに送信すると、エコーまたは応答が返されます。この簡単なプロセスで、ネットワーク デバイス同士の検出、識別、およびテストができます。

Ping ツールは、RFC-777 と RFC-792 で規定された ICMP というプロトコルを使用します。ICMP で定めたのは、2 つのネットワーク デバイス間で送受される*エコー*と*エコー応答*のトランザクションで、これは ping として知られています。*エコー*（要求）パケットをネットワーク デバイスの IP アドレスに送信します。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、パケットを *エコー応答*として送り返します。

Ping ツールの使い方

管理者は ASDM の Ping ツールを利用し、次のようにさまざまな方法でインタラクティブな診断ができます。

- インターフェイス間のループバック テスト：同じ FWSM 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。
- FWSM インターフェイスへの ping 送信：他の FWSM のインターフェイスに対して Ping ツールまたは別の送信元から ping を送信すると、相手側がアップしていて応答することを確認できます。

- FWSM を通過する ping 送信：Ping ツールの送信 ping パケットがデバイスに到達する途中で、中間の FWSM 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 デバイスの動作に疑問がある場合:FWSM のインターフェイスから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 ping を送信する場合があります。インターフェイスの設定が正常にもかかわらずエコーを受信しない場合、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：エコー要求を返すことが分かる、動作が正常なネットワーク デバイスに FWSM のインターフェイスから ping を送信する場合があります。エコーを受信すると、中間にあるデバイスは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を確認できます。

Ping ツールのトラブルシューティング

ping でエコーを受信できない場合、FWSM 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が原因の場合もあります。必ずしも ping を送信された IP アドレス が「NO response」であることが原因とは限りません。Ping ツールを利用する前に次の点を確認してから、FWSM の*インターフェイスから*または*インターフェイス*へ、あるいは*インターフェイス経由で* ping を送信してください。

インターフェイスの基本的な確認事項

- インターフェイスが正常に設定されていることを、Configuration > Properties > Interfaces で確認します。
- 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かどうかを確認します。
- 「既知の正常な」送信元を使用して、他のタイプのトラフィックが正常に通過するかどうかを確認します。Monitoring > Interface Graphs を使用してください。

FWSM インターフェイスから ping を送信

インターフェイスの基本的なテストを行う場合、FWSM のインターフェイスからネットワーク デバイスに ping を送信する方法があります。その場合、他の方法でネットワーク デバイスが正常に動作し、中間通信パス経由でエコーが返されることを事前に確認しておきます。

- FWSM から送信した ping を「既知の正常な」デバイスで受信して確認します。受信できない場合、おそらくインターフェイスの送信側ハードウェアまたはコンフィギュレーションに問題があります。
- FWSM のインターフェイス設定が正しいにもかかわらず「既知の正常な」デバイスのエコーを受信できない場合、インターフェイスの受信側ハードウェアに問題があると考えられます。インターフェイスを「既知の正常な」受信機能に変更し、「既知の正常な」デバイスから ping のエコーを受信できれば、変更前のインターフェイスは受信側ハードウェアに問題があると確認できます。

FWSM インターフェイスへ ping を送信

FWSM のインターフェイスへ *ping を送信*する場合、Configuration > Properties > Administration > ICMP ペインのインターフェイスで ping 応答（ICMP の*エコー応答*）がイネーブルになっているかどうかを確認します。ping 機能がディセーブルになっていると、FWSM 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 ツールにも応答しません。

FWSM 経由で ping を送信

- まず、「既知の正常な」送信元から FWSM を経由し、他のタイプのネットワーク トラフィックが通過することを確認します。Monitoring > Interface Graphs、または SNMP 管理ステーションを使用します。

- イネーブルにした内部ホストから外部ホストに ping を送信するには、Configuration > Access Rules で内部および外部インターフェイスの ICMP アクセスを正しく設定する必要があります。

フィールド

- IP Address：ICMP エコー要求パケットの宛先 IP アドレス。

（注） Configuration > Hosts/Networks > Basic Information > Host Name ペインで設定したホスト名がある場合、IP アドレスとして使用できます。

- インターフェイス リスト：（オプション）エコー要求パケットを送信する FWSM インターフェイスを指定します。指定しない場合、FWSM 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。
- Ping Output：ping の実行結果。**Ping** をクリックすると、IP アドレスには ping が 3 回送信され、次のフィールドに実行結果が 3 つ表示されます。
  - Reply IP address/Device name：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。
  - Response time/timeout (ms)：ping を送信すると、ミリ秒タイマーが開始します。ここで指定する最大値がタイムアウト値になります。たとえば、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比較するテストで役立ちます。

    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
    ```

    ping に失敗すると、実行結果は次のようになります。

    ```
    Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
    Success rate is 0 percent (0/5).
    ```

- Ping：ICMP のエコー要求パケットを、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 アドレスへ送信し、応答タイマーを開始します。
- Clear Screen：これまでに実行した ping コマンドの実行結果を画面でクリアします。

モード

次の表に、この機能を使用できるモードを示します。

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

Preferences

Preferences ペインでは、プリファレンスをローカルに保存することにより、ASDM 機能の一部をセッション間で変更します。プリファレンスは *preferences.conf* というファイルに保存されます。Microsoft Windows の場合、このファイルは C:\Documents and Settings\user\.asdm\data\ ディレクトリに格納されます。

フィールド

- General Setting タブ：汎用プリファレンスを設定します。
  - Enable Large Fonts(Requires ASDM Restart)：ASDM を閉じて再接続した後に、ASDM のアイコンのフォント サイズを拡大します。すべてのフォントが大きくなるとは限りません。
  - Preview commands before sending to the device：ASDM により生成された CLI コマンドを表示できます。
  - Confirm before exiting from ASDM：ASDM を閉じるとき、プロンプトを表示して終了を確認します。このオプションは、デフォルトでオンになっています。
  - Restore Default：デフォルトの設定に戻します。
- Rules Table：Rules テーブルのプリファレンスを設定します。
  - Display Settings：ルールの表示方法に関連するプリファレンスを設定します。
  - Auto expand and service object group prefix：このチェックボックスをオンにすると、サービス オブジェクト グループのプレフィックスが表示されます。
  - Auto-Expand Prefix：サービス オブジェクト グループのプレフィックスを入力します。
  - Show members of network and service objects group：サービス オブジェクト グループのメンバーを表示します。
  - Limit members to：表示するネットワークおよびサービス オブジェクト グループの数をユーザが指定する値に制限します。
  - Show all actions for service policy rules check：Rules テーブルのサービス ポリシー アクションをすべて表示します。
  - Show filter pane by default check：デフォルトで Filter Rules ペインを表示します。
  - Show rule diagram pane by default check：デフォルトで、Rules テーブルのルール ダイアグラムをグラフィカルに表示します。
  - Deployment Settings：ルールの展開方法に関連するプリファレンスを設定します。
  - Issue 'clear xlate' cmd when access-lists are deployed：このチェックボックスをオンにすると、アクセスリストが変更される前に **clear xlate** コマンドが FWSM に送信されます。このコマンドは NAT 変換をすべてクリアします。デフォルト設定はオフです。
- Application Inspection：アプリケーション検査のプリファレンスを設定します。
  - Prompt to add an inspect map before applying changes：変更を適用する前に検査マップを追加するようにプロンプトを表示します。
  - Make the Advanced view the default inspect map view：デフォルトの検査ビューを Advanced ビューにします。
  - Ask to make Advanced View the default：オフにすると、Advanced ビューをデフォルトのビューにするよう要求するポップアップ ダイアログボックスが無効になります。
- Syslog Color：ホームページの背景色とシステム ログ メッセージの色を設定します。
  - Severity：重大度を表示します。
  - Background Color：重大度メッセージの背景色を設定します。色を変更するには、その行をクリックします。Pick a Color ダイアログボックスが表示されます。
  - Foreground Color：重大度のメッセージの前景色（テキスト色）を設定します。色を変更するには、その行をクリックします。Pick a Color ダイアログボックスが表示されます。
  - Restore Default：デフォルトの設定に戻し、白の背景色に黒の前景色で表示します。

（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 ファイルに書き込まれ、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。ASDM をリスタートすると、設定したプリファレンスが反映されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Management

フラッシュ メモリのディスク パーティションに保存されたファイルの表示、移動、コピー、削除ができます。また、ディスク パーティションにディレクトリを作成することもできます。

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でのみ使用できます。

フィールド

- Folders：ディスクにあるフォルダを表示します。
  - Flash Space：フラッシュ メモリのサイズと空き容量を示します。
    Total：フラッシュ メモリの全体のサイズを示します。
    Available：空き容量を示します。
- Files：選択したフォルダに含まれるファイルの情報を表示します。
  - Path
  - Filename
  - Size (bytes)
  - Time Modified
  - Status
- View：選択したファイルをブラウザに表示します。
- Cut：選択したファイルを切り取り、他のディレクトリに貼り付けられます。
- Copy：選択したファイルをコピーし、他のディレクトリに貼り付けられます。
- Paste：コピーしたファイルを選択した場所に貼り付けます。
- Delete：選択したファイルをフラッシュ メモリから削除します。
- Rename：ファイルの名前を変更します。
- New Directory：ファイルを保存するディレクトリを新規作成します。
- File Transfer：File Transfer ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Upload Software を使用すると、FWSM イメージ ファイルまたは ASDM イメージをユーザ PC 上で選択し、フラッシュ メモリにアップロードできます。

フィールド

- Image to upload：アップロードするイメージ タイプを選択します。
  - ASDM Image：ASDM イメージを FWSM にロードします。
  - FWSM Image：FWSM イメージをロードします。
- Local File Path：ユーザの PC 上のファイルのパスを入力します。
  - Browse Local：選択して PC 上のファイルを参照します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 により、HTTPS、TFTP、FTP を使用するかローカル イメージを参照して、FWSM との間でファイルを相互にコピーすることができます。

フィールド

- Source File：転送対象になるソース ファイルを選択します。
  - Remote Server：リモート サーバからファイルを転送する場合に選択します。
    Path：ファイルの場所のパスを入力します。サーバの IP アドレスを含めます。
    Port/Type：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。次の FTP タイプが有効です。
    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
  - Flash File System：ディスク パーティションのファイルをコピーする場合に選択します。
    Path：ファイルの場所のパスを入力します。
    Browse Flash：選択して、FWSM でコピーされたファイルの場所を参照します。
  - Local Computer：ローカル PC からファイルをコピーする場合に選択します。
    Path：ファイルの場所のパスを入力します。
    Browse Localhost：ローカル PC を参照し、転送対象ファイルを検索します。
- Destination File：転送先のファイルを選択します。送信元の場所によって、Flash File System と Remote Server のどちらかが自動選択されます。
  - Flash File System：ファイルをディスク パーティションに転送します。
    Path：ファイルの場所のパスを入力します。
    Browse Flash：選択して、FWSM でファイルが転送される場所を参照します。
  - Remote Server：リモート サーバにファイルを転送します。

Path：ファイルの場所のパスを入力します。

Type：FTP 転送の場合、タイプを入力します。次のタイプが有効です。

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

- Transfer File：ファイル転送を開始します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 を実行すると、システムをリスタートし、保存されたコンフィギュレーションをメモリにリロードします。System Reload ダイアログボックスで、システムのリロードのタイミング、実行コンフィギュレーションをフラッシュ メモリに保存する / しない、リロード時に接続しているユーザにメッセージを送信する / しない、を選択できます。

フィールド

- Reload Scheduling：リロードを実行するタイミングを設定します。
  - Configuration State：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しないかを選択します。

    Save the Running Configuration at Time of Reload：リロード時に実行コンフィギュレーションを保存します。

    Reload Without Saving the Running Configuration：リロード時に実行コンフィギュレーションに加えられた変更を破棄します。
- Reload Start Time：リロードのタイミングを選択します。
  - Now：リロードをただちに実行します。
  - Delay by：指定した時間だけ遅延させてリロードします。リロード開始までの経過時間を、時間と分、または分で入力します。
  - Schedule at：リロードする時刻と日付を指定してスケジュールを設定します。リロードの実行時刻を入力します。

    Date：リロードのスケジュール日を選択します。
- Reload Message：リロード時に ASDM のインスタンスを開いたときに送信されるメッセージを入力します。
- On Reload Failure Force Immediate Reload after：リロードに失敗した場合、もう一度リロードを実行するまでの経過時間を、時間と分、または分で指定します。
- Schedule Reload：設定に従ってリロードをスケジュールします。
- Reload Status：リロードのステータスを表示します。
- Cancel Reload：スケジュールされたリロードをキャンセルします。
- Refresh：Reload Status 画面をリフレッシュします。
- Details：スケジュールされたリロードの詳細を表示します。

モード

次の表に、この機能を使用できるモードを示します。

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

Wizards メニュー

Wizards メニューで、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：ASDM Startup Wizard を利用して、FWSM の初期コンフィギュレーションを段階的に設定することができます。コンフィギュレーション画面をクリックすると表示されるプロンプトに従って、使用する FWSM の情報を入力します。Startup Wizard で設定すると、FWSM の使用をすぐに開始できます。

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 FWSM の情報へのリンクも提供されます。

- Help Topics：新しいブラウザ ウィンドウが開き、左側のフレームに目次、画面の名前、索引で整列されたヘルプが表示されます。この画面で必要な項目のヘルプを見つけるか、上部の Search タブで検索します。
- Help for Current Screen：その時点で開いている画面、ペイン、ダイアログボックスの文脈依存ヘルプが開きます。また、「?」マークのヘルプ アイコンをクリックして文脈依存ヘルプを表示することもできます。
- Release Notes：Web サイトから最新バージョンの『*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：スタートアップ ガイドのヘルプ項目が表示され、ASDM の使用をすぐに開始できます。
- Glossary：用語および略語の定義が記載されています。
- Feature Search：ASDM の機能を検索できます。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、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。ASDM のツールバーにある Search アイコンをクリックすることもできます。
- Icon Legend：ASDM にあ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。
- How do I?：ASDM Assistant が開いて、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。特定のタスクの実行に関する詳細が分かります。
- About Cisco Firewall Service Module：FWSM に関するさまざまな情報を一覧表示します。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 イメージなどが含まれます。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 5.2F：ASDM に関する情報を表示します。ASDM ソフトウェア バージョン、ホスト名、特権レベル、オペレーティング システム、ブラウザのタイプ、Java のバージョンなどが含まれます。

ツールバー

ツールバーは ASDM ウィンドウ上部のメニュー項目の下にあり、ここからホームページ、コンフィギュレーション ページ、モニタリング ページ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、ナビゲーションなどよく使用する機能を実行したりできます。

- System/Contexts：下矢印をクリックすると左側のペインにコンテキストのリストが開いて表示され、上矢印をクリックするとコンテキストのドロップダウン リストが元に戻ります。リストが展開されているときに左向き矢印をクリックすると、ペイン全体は左側に折りたたまれます。右向き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：ホームページを表示します。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、FWSM の重要な情報を一目で確認できます。詳細については、「Home」を参照してください。マルチモードの場合、システムのホームページはありません。
- Configuration：FWSM を設定します。左側のペインで、設定する機能のボタンをクリックします。
- Monitoring：FWSM を監視します。左側のペインで、監視する機能のボタンをクリックします。
- 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。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、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 をクリックします。
- Refresh：選択すると、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。監視中のグラフはリフレッシュされません。
- Save：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。書き込みアクセスが禁止されているコンテキストの場合（HTTP にあるなど）、実行コンフィギュレーションは保存されません。
- Help：その時点で表示されている画面の文脈依存ヘルプを開きます。

ステータスバー

ステータスバーは ASDM ウィンドウの下部に表示されます。ステータスバーの左から右に、次のようなエリアが表示されます。

- Status：コンフィギュレーションのステータスが、「Device configuration loaded successfully」のように表示されます。
- User Name：ASDM を使用しているユーザの名前が表示されます。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 を使用しているユーザの権限レベルが表示されます。
- Commands Ignored by ASDM：アイコンをクリックすると、ASDM で実行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が表示されます。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、「Tools メニュー」を参照してください。
- Status of Connection to Device：ASDM と FWSM の接続ステータスを表示します。詳細については、「Connection to Device」を参照してください。
- Save to Flash Needed：ASDM のコンフィギュレーションを変更したが、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ていないことを示します。
- Refresh Needed：FWSM のコンフィギュレーションが変更された場合、ASDM のコンフィギュレーションを FWSM からリフレッシュする必要があるかどうかを示します。コンフィギュレーションを CLI で変更したような場合です。
- SSL Secure：ASDM への接続に SSL を使用し、安全であることを示します。

- Time：FWSM のスイッチで設定された時刻を示します。

Connection to Device

ASDM は FWSM 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ージ 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。その場合の接続はこのダイアログボックスに表示されません。

ペイン共通のボタン

ほとんどの ASDM ペインで使用できるボタンを次に示します。

- Apply：ASDM での変更内容を FWSM に送信し、実行中のコンフィギュレーションに適用します。実行中のコンフィギュレーションのコピーをフラッシュ メモリに書き込むには、Save をクリックします。File メニューでは、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、フェールオーバー スタンバイ装置に書き込むことができます。
- Reset：変更内容を破棄し、変更前に表示されていた情報、または Refresh か Apply を最後にクリックしたときに表示されていた情報に戻します。Reset したら Refresh を実行し、現在の実行コンフィギュレーション データが表示されることを確認してください。
- Cancel：変更内容を破棄して、前のペインに戻ります。
- Help：選択したペインのヘルプを表示します。

ヘルプ ウィンドウについて

ここでは、次の項目について説明します。

ヘッダー ボタン

ヘッダー ボタンを使用すると、ヘルプをナビゲーションして目的の項目を探し出せます。

- About ASDM：ASDM に関する情報を表示します。
- Search：ヘルプ項目を検索します。
- Using Help：オンライン ヘルプの活用方法を説明します。
- Glossary：ASDM およびネットワークの用語集を表示します。

左側のペインのタブ：オンライン ヘルプのナビゲーションを容易にします。

- Contents：目次を表示します。
- Screens：ヘルプ ファイル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。

注意

ヘルプをアプレット モードで起動したときヘルプ ページを表示中のウィンドウがあれば、同じブラウザのウィンドウ上に次のヘルプ ページを表示します。ヘルプ ページを表示中のウィンドウがなければ、新規のブラウザ ウィンドウに表示します。

Netscape がデフォルト ブラウザの場合、ヘルプをアプリケーション モードで起動すると、ヘルプを起動するたびに新規のブラウザ ウィンドウが開いてヘルプ ページが表示されます。IE がデフォルト ブラウザの場合、ユーザの設定により、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。IE の表示方法を設定するには、**Tools > Internet Options > Advanced > Reuse window** でショートカットを実行します。

Home

ASDM Home ページから、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、FWSM の重要な情報を一目で確認できます。ASDM のホームページに表示される詳細のほとんどは、ASDM の実行中に他の場所から確認できますが、Home ペインでは FWSM の実行状態をすぐに確認できるので便利です。Home ページのステータス情報は 10 秒ごとに更新されます。

フィールド

- Device Information：デバイス情報を表示するタブが 2 つあります。
  - General：次の情報が表示されます。

    Host Name：FWSM のホスト名を表示します。ホスト名の設定方法については、「Device」を参照してください。

    ASDM Version：ASDM のバージョンを表示します。

    FWSM Version：FWSM ソフトウェアのバージョンを表示します。

    Firewall Mode：ファイアウォール モードを示します。「ルーテッド」または「透過」です。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：FWSM と ASDM イメージのフラッシュメモリの合計容量を MB 単位で表示します。コンフィギュレーション ファイルのパーティション（ディスクと呼ばれます）は 64 MB ですが、これは表示されません。

    Device Uptime：FWSM の実行経過時間を示します。

    Device Type：FWSM のモデルを示します。

    Context Mode：コンテキスト モードを示します。「シングル」または「マルチ」です。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：RAM の全体の容量を示します。
  - License：FWSM でライセンスされた機能のサポート レベルを示します。すべての機能にライセンスが必要というわけではありません。
- System Resources Status：CPU およびメモリの使用状況に関する次の統計値を示します。
  - CPU：現在の CPU 使用率を示します。
  - CPU Usage (percent)：直前 5 分間の CPU 使用状況を示します。
  - Memory：現在のメモリ使用サイズを MB 単位で示します。
  - Memory Usage (MB)：直前 5 分間のメモリ使用状況を MB 単位で示します。
- Interface Status：インターフェイスごとにステータスが表示されます。インターフェイスの行を選択すると、入力と出力が Kbps でテーブルの下に表示されます。
  - Interface：インターフェイス名を示します。名前が設定されているインターフェイスだけがこの領域に表示されます。
  - IP Address/Mask：ルーテッド モードのみ。インターフェイスの IP アドレスとサブネットマスクを示します。
  - Line：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：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。
  - Current Kbps：現在のインターフェイス 通過速度を Kbps で示します。
- Traffic Status：インターフェイス全体の接続数 / 秒と、最も遅いセキュリティ インターフェイスのトラフィック スループットのグラフを示します。
  - Connections per Second Usage：直前 5 分間の UDP および TCP の接続数 / 秒を示します。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)：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。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：FWSM から直前に出力されたシステム メッセージを最大 100 個表示します。上向き矢印をクリックすると、ロギング グループ ボックスを上に拡大できます。下向き矢印をクリックすると、サイズが元に戻ります。ディバイダを上下にドラッグすると、領域のサイズを変更できます。現在のメッセージをクリアするには、グループ ボックスを右クリックして **Clear Content** チェックボックスをオンにします。現在のメッセージを PC 上のファイルに保存するには **Save Content** をクリックし、コンテンツをコピーするには **Copy** をクリックします。システム メッセージの背景色と前景色を重大度に応じて変更するには、**Color Settings** をクリックします。
  - Configure ASDM Syslog Filters：Logging Filters ペインを開きます。
  - Enable Logging：ASDM へのロギングがイネーブルになっていない場合、このボタンをクリックしてイネーブルにすることができます。
  - Stop message display：システム ログ メッセージの表示のアップデートを停止するには、右側の赤いアイコンをクリックします。
  - Resume message display：システム ログ メッセージの表示のアップデートを再開するには、右側の緑色のアイコンをクリックします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

始める前に

ここでは、次の項目について説明します。

ASDM アクセスに対する FWSM の設定

ASDM を使用するには、HTTPS サーバをイネーブルにし、FWSM への HTTPS 接続を許可する必要があります。**setup** コマンドを使用すれば、これらのタスクが実行されます。ここでは、ASDM へのアクセスを手動で設定する方法について説明します。

FWSM は、コンテキストごとに最大 5 つの同時 ASDM インスタンス、およびすべてのコンテキスト間で最大 80 の ASDM インスタンスを許可します。リソース クラスを使用すると、コンテキストごとに許可する ASDM セッションの数を制御できます(P.7-12 の「リソース クラスの設定」を参照)。

ASDM へのアクセスを設定するには、次の手順を実行します。

ステップ 1　FWSM が HTTPS 接続を受け入れる IP アドレスを識別するには、各アドレスまたはサブネットに次のコマンドを入力します。

```
hostname(config)# http source_IP_address mask source_interface
```

ステップ 2　HTTPS サーバ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)# http server enable
```

たとえば、HTTPS サーバをイネーブルにし、アドレスが 192.168.1.2 である内部インターフェイスのホストが ASDM にアクセスするには、次のコマンドを入力します。

```
hostname(config)# http server enable
hostname(config)# http 192.168.1.2 255.255.255.255 inside
```

192.168.3.0 ネットワークのすべてのユーザに内部インターフェイスの ASDM へのアクセスを許可するには、次のコマンドを入力します。

```
hostname(config)# http 192.168.3.0 255.255.255.0 inside
```

CLI での透過またはルーテッド ファイアウォール モードの設定

ASDM のシングルモードでは、モードの変更はできません。マルチモードでは、ASDM の管理コンテキストモードでのモード変更はできません。CLI でモードの変更をする必要があります。

モードを変更すると、FWSM はコンフィギュレーションをクリアします。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。すでに実装済みのコンフィギュレーションがある場合は、モードを変更する前に必ずコンフィギュレーションのバックアップを作成してください。新しくコンフィギュレーションを作成するときにこのバックアップを参照する場合があります。

firewall transparent コマンドでモードを変更する FWSM にテキスト コンフィギュレーションをダウンロードする場合は、必ずこのコマンドをコンフィギュレーションの最上部に置いてください。これによって、FWSM は、このコマンドを読み取り次第すぐにモードを変更し、その後は、ダウンロードしたコンフィギュレーションの読み取りを続けます。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、FWSM 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。

- 透過モードに設定するには、各コンテキストで次のコマンドを入力します。

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

- ルーテッド モードに設定するには、各コンテキストで次のコマンドを入力します。

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

ASDM ランチャのダウンロード

ASDM ランチャは Windows 専用です。ASDM ランチャは、ASDM を Java アプレットとして実行する改良点の 1 つです。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　FWSM のネットワークでサポートされている Web ブラウザで、次の URL を入力します。

https://*interface_ip_address*

透過ファイアウォール モードでは、管理 IP アドレスを入力します。

（注）　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。デフォルトでは、名前とパスワードは空白にします。

表示されるページに次のボタンがあります。

- **Download ASDM Launcher and Start ASDM**
- **Run ASDM as a Java Applet**

ステップ 3　**Download ASDM Launcher and Start ASDM** をクリックします。

インストーラが PC 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 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 ランチャによる ASDM の起動

ASDM ランチャは Windows 専用です。

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** メニューから起動します。

ステップ 2　FWSM の IP アドレスまたはホスト名、ユーザ名、パスワードを入力して **OK** をクリックします。

新しいバージョンの ASDM が FWSM にあれば ASDM ランチャが自動的にダウンロードされ、ASDM を起動します。

デモ モードでの ASDM の使用

ASDM デモ モードは、Windows で実行される別のアプリケーションとして使用できます。ASDM ランチャとあらかじめパッケージされているコンフィギュレーション ファイルを使用して、実デバイスを使用せずに ASDM を実行できます。ASDM デモ モードでは次のようなことができます。

- 実デバイス接続時と同じように、ASDM からコンフィギュレーションを実行して監視タスクを選択。
- ASDM インターフェイスによる ASDM または FWSM 機能のデモ。
- Content Security and Control SSM（CSC SSM）使用時のコンフィギュレーションおよび監視タスクの実行。

ASDM デモ モードは、リアルタイムのシステム ログ メッセージを含む監視結果のシミュレーションを提供します。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。

ASDM デモ モードでは、次の制限事項があります。

- コンフィギュレーション変更は GUI に表示されますが、コンフィギュレーション ファイルには適用されません。したがって、Refresh ボタンをクリックすると元のコンフィギュレーションに戻ります。変更はコンフィギュレーション ファイルに保存されません。
- ファイルとディスクの操作はサポートされていません。
- 監視データとログ データはシミュレーション結果です。履歴モニタリング データは使用できません。
- admin ユーザのみログインできます。つまり、monitor-only または read-only ユーザでログインできません。
- デモ モードでは、次の機能はサポートされていません。
  - 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 Image
  File Transfer
  Upload image from Local PC
  System Reload
- Toolbar/Status bar > Save
- Configuration > Interface > Edit Interface > Renew DHCP Lease
- Failover：スタンバイ デバイスの設定

- 次の操作を実行すると、コンフィギュレーションの再読み込みが行われ、結果として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 パネルの変更
  - NAT パネルの変更
  - Clock パネルの変更

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　デモ モード アプリケーションがインストールされていない場合、次の手順を実行します。

a. ASDM デモ モードのインストーラを、http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm からダウンロードします。

ファイル名は asdm-*version*-demo.msi です。

b. 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 2　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** メニューから起動します。

ステップ 3　**Run in Demo Mode** チェックボックスをオンにします。

ステップ 4　プラットフォーム、コンテキスト モード、ファイアウォール モード、ASDM バージョンを設定するには、**Demo** ボタンをクリックして、Demo Mode エリアから選択します。

ステップ 5　更新された ASDM イメージを使用する場合は、最新のインストーラをダウンロードするか、または通常の ASDM イメージをダウンロードしてからデモ モードにインストールします。

a. イメージは http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm からダウンロードできます。

ファイル名は asdm-*version*.bin です。

b. Demo Mode エリアで **Install ASDM Image** をクリックします。

ファイル ブラウザが表示されます。ブラウザで ASDM イメージ ファイルを検索します。

ステップ 6　**OK** をクリックして、ASDM デモ モードを起動します。

ウィンドウのタイトルバーに Demo Mode のラベルが表示されます。

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　FWSM のネットワークでサポートされている Web ブラウザで、次の URL を入力します。

https://*interface_ip_address*

透過ファイアウォール モードでは、管理 IP アドレスを入力します。

（注）　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。名前とパスワードのプロンプトでも同様です。デフォルトでは、名前とパスワードは空白にします。

表示されるページに次のボタンがあります。

- **Download ASDM Launcher and Start ASDM**
- **Run ASDM as a Java Applet**

ステップ 3　**Run ASDM as a Java Applet** をクリックします。

ステップ 4　すべての Java 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。デフォルトでは、名前とパスワードは空白にします。

History Metrics

History Metrics ペインで、FWSM を設定してさまざまな統計情報の履歴を保存し、ASDM を使用して Graph/Table 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。

フィールド

- ASDM History Metrics：履歴メトリックをイネーブルにします。このチェックボックスをオフにすると、履歴メトリックはクリアされ、ディセーブルになります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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の概要

FWSM 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　初期コンフィギュレーションには Startup Wizard を使用します。**Configuration** > **Properties** > **Startup Wizard** の順にクリックします。

ステップ 2　高度な機能を設定するには、ツールバーの **Configuration** ボタンをクリックし、機能のボタンをクリックします。次のような機能があります。

- ルーテッド インターフェイスの設定：IP アドレス、名前、セキュリティ レベルなどのインターフェイスの基本パラメータを設定します。透過モードでは、ブリッジ グループのパラメータも設定できます。
- セキュリティ ポリシー：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 ルールがあります。
  - アクセス ルールの設定：FWSM を通過する IP トラフィックを許可または拒否します。透過ファイアウォール 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 ルールの設定（透過モードのみ）：FWSM を通過する IP トラフィック以外を許可または拒否します。
  - AAA Rules：HTTP など特定のタイプのトラフィックに対して、認証と認可のいずれかまたは両方を要求します。FWSM 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：特定のウェブサイトまたは FTP サーバへの発信アクセスを禁止します。FWSM 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。URL フィルタリング サーバを設定するには、**Configuration** > **Properties** > **URL Filtering** を参照します。ルールを追加するには、まず設定が必要です。
  - Service Policy Rules：アプリケーション検査、接続の制限、TCP 正規化を適用します。検査エンジンは、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、FWSM が詳細なパケット検査を行うことが必要となります。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 の設定：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。これによって、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。
- 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：（シングルモードのみ）OSPF、RIP、マルチキャスト、非対称ルーティングを設定します。
- グローバル オブジェクトの追加：FWSM 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。再利用コンポーネントまたはグローバル 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
  - IP 名
  - サービス グループ
  - 検査マップ
  - 時間範囲

ステップ 3　FWSM を監視するには、ツールバーの **Monitoring** ボタンをクリックし、機能のボタンをクリックします。次のような機能があります。

- インターフェイス：ARP テーブル、DHCP、ダイナミック アクセスリスト、インターフェイスの統計値を監視します。
- ルーティングのモニタリング：ルート、OSPF LSA、OSPF ネイバーを監視します。
- プロパティのモニタリング：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します。
- システム ログ メッセージのモニタリング：システム ログ メッセージを監視します。
- フェールオーバーのモニタリング：（マルチモードのシステムの場合）システムのフェールオーバーを監視します。

CHAPTER 3

FWSM で使用するスイッチの設定

この章では、FWSM で使用する Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの設定方法について説明します。また、スイッチの CLI を使用して設定する必要のある機能について説明します。その他の手順は ASDM を使用して完了できます。

この章には、次の項があります。

スイッチの概要

この項では、ASDM がサポートするスイッチについて説明します。次の項目を取り上げます。

ASDM がサポートするスイッチのコンフィギュレーション

ASDM を使用して、次のスイッチの機能を設定できます。

- VLAN にポートを割り当てます。
- 管理ステータス、スピード、PortFast などのポートのパラメータを設定します。
- ポート モードをルーテッドまたはスイッチドに設定します。
- VLAN を設定します。
- SVI を設定します。
- ファイアウォール VLAN グループを設定し、FWSM に割り当てます。

（注） 次の機能は ASDM の Configuration > Switch ペインではサポートされていません。

- トランク ポートのコンフィギュレーション
- シャーシ内アクティブ / アクティブ フェールオーバーの VLAN グループ
- シャーシ内フェールオーバーの VLAN グループ

サポートされているスイッチのハードウェアとソフトウェア

Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータに FWSM をインストールできます。両シリーズのコンフィギュレーションは同じで、このガイドでは、どちらも一般的に「スイッチ」と呼んでいます。スイッチとは、スイッチ（スーパーバイザ エンジン）およびルータ（MSFC）のことです。

スイッチは 2 つのソフトウェア モードをサポートしています。

- スイッチ スーパーバイザ エンジンおよび統合された MSFC ルータ上の Cisco IOS ソフトウェア
- スーパーバイザ エンジン上の Catalyst オペレーティング システム ソフトウェアおよび MSFC 上の Cisco IOS ソフトウェア（ASDM がサポートしていない）

FWSM は独自のオペレーティング システムを実行します。

（注） ASDM は、Catalyst オペレーティング システム ソフトウェアをサポートしていません。したがって、このガイドでも、Cisco IOS ソフトウェアのみを取り扱います。Catalyst オペレーティング システムをはじめとする他のハードウェアおよびソフトウェアの設定については、スイッチの設定に CLI を使用する『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。

マルチコンテキスト モードでのスイッチの設定

マルチコンテキスト モードでは、管理コンテキストに接続した場合のみ、ASDM を使用してスイッチを設定できます。管理外コンテキストでは ASDM に接続しても、スイッチのコンフィギュレーションにアクセスできません。

CLI でのモジュール インストレーションの検証

スイッチが FWSM を確認し、オンラインになったことを検証するには、次のコマンドを入力してモジュール情報を表示します。

```
Router> show module [mod-num | all]
```

show module コマンドのサンプル出力は、次のようになります。

```
Router> show module
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1     2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE    SAD0444099Y
  2    48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD03475619
  3     2  Intrusion Detection System             WS-X6381-IDS       SAD04250KV5
  4     6  Firewall Module                        WS-SVC-FWM-1       SAD062302U4
```

(注)　**show module** コマンドは、FWSM の 6 つのポートを示しています。これらは EtherChannel としてまとめた内部ポートです。詳細については、P.3-16 の「CLI での FWSM の内部インターフェイスのカスタマイズ」を参照してください。

ASDM をサポートするスイッチの設定

スイッチの設定に ASDM を使用する前に、CLI を使用してスイッチに SNMP と SSH を設定する必要があります。スイッチを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを使用して、SNMP コミュニティを設定します。

```
Router(config)# snmp-server community string
```

string の引数が 1 ～ 32 文字の英数字から構成されていて、パスワードのように機能するコミュニティ ストリングは、SNMP へのアクセスを許可します。ブランク スペースはコミュニティ ストリングでは使用できません。@ のシンボルは、コンテキストの情報を区切るために使用します。このコマンドを設定するときには、@ のシンボルを SNMP コミュニティ ストリングの一部として使用しないようにします。

このコマンドの他のオプションの詳細については、Cisco IOS コマンド リファレンスを参照してください。

ステップ 2　SSH をイネーブルにするには、次のコマンドを入力します。

```
Router(config)# hostname hostname
Router(config)# ip domain-name domain-name
Router(config)# crypto key generate rsa usage-keys modulus 1024
Router(config)# line vty line-number [ending-line-number]
Router(config)# transport input ssh
Router(config)# ip ssh time-out 120
```

これらのコマンドの詳細については、Cisco IOS コマンド リファレンスを参照してください。

ステップ 3　ASDM を使用してスイッチに接続する際には、**login local**、**login tacacs**、または **login authentication** コマンドを使用して、ASDM ユーザのユーザ名とパスワードを設定します。ユーザ アカウントの詳細については、Cisco IOS ユーザ マニュアルを参照してください。

スイッチとの接続の確立

ASDM でスイッチに接続する場合は、SNMP と SSH のクレデンシャルを求められます。ASDM を再起動するたびに、クレデンシャルを再入力する必要があります。スイッチの IP アドレスと SSH のユーザ名だけが記憶されます。

スイッチのコンフィギュレーションの前提条件の詳細については、P.3-4 の「ASDM をサポートするスイッチの設定」を参照してください。

スイッチとの接続を確立するには、次の手順を実行します。

ステップ 1　**Configuration** をクリックし、次に **Switch** をクリックします。

Switch Credentials ダイアログボックスが表示されます。

ステップ 2　Sup IP Address フィールドで、スイッチ スーパーバイザ エンジンの管理 IP アドレスを入力します。

ステップ 3　SNMP Credentials > Read Community フィールドで、P.3-4 の「ASDM をサポートするスイッチの設定」で設定した SNMP コミュニティ ストリングを入力します。

ステップ 4　SSH Credentials 領域で、次の値を入力します。

- ユーザ名
- パスワード
- イネーブル パスワード

ステップ 5　**OK** をクリックします。

ASDM は、スイッチに接続されると、スイッチのインターフェイスと VLAN 情報をロードします。

ASDM がスイッチに接続できなかった場合は、Switch ボタンをオフにし、Switch Credentials ダイアログボックスに再アクセスするために **Switch** ボタンを再度クリックします。

（注）　**Refresh** ボタンをクリックすると、ASDM は、まず FWSM のコンフィギュレーションをリフレッシュし、次にスイッチのコンフィギュレーションをリフレッシュします。マルチモードでは、現在選択しているコンフィギュレーション（システムまたはコンテキスト）をリフレッシュし、次にスイッチのコンフィギュレーションをリフレッシュします。スイッチだけの別個の Refresh ボタンはありません。

スイッチ ポートの設定

ASDM を使用して、ポート パラメータの設定および VLAN へのスイッチ ポートの割り当てができます。ここでは、次の項目について説明します。

Interfaces ペインの使用

Configuration > Switch > Interfaces ペインでは、ポート パラメータの設定および VLAN へのスイッチ ポートの割り当てだけでなく、簡単なコンフィギュレーション フローのパラメータも多数設定できます。スイッチのコンフィギュレーションは、Configuration > Switch > Interfaces ペインを使用して行えますが、このタスクは、Vlans and Vlan Groups ペインを使用しても可能です。Configuration > Interfaces and Configuration > Security Contexts ペインを使用すると、FWSM のコンフィギュレーションを行うこともできます。このような重複した機能には、次のようなものがあります。

- VLAN のスイッチ仮想インターフェイス（SVI）としての設定、および IP アドレスとマスク（Vlans ペイン）の割り当て
- VLAN の VLAN グループへの割り当て（Vlan Groups ペイン）
- FWSM のインターフェイス パラメータの設定（Configuration > Interfaces ペイン）

Interfaces ペインには、必要な項目で含まれていないものも多いので、コンフィギュレーションを追加する場合は必ず他のペインを確認してください。たとえば、VLAN groups ペインで VLAN グループを追加できますが、Interfaces ペインではできません。

マルチコンテキスト モードでは、システムにいるか、管理コンテキストにいるか、または別のコンテキストにいるかによって、Interfaces ペインが変わります（Configuration > Switch ペインを使用するには、最初に管理コンテキストに接続する必要があります。接続した後で、システムまたは他のコンテキストに表示を切り替えられます）。

システムでは、すべてのコンテキストの VLAN の割り当てを表示できます。各コンテキスト内で、VLAN が現在のコンテキストに割り当てられているかどうかを確認できます。

（注） 各 FWSM にスイッチを接続している内部 EtherChannel には、それぞれ 6 つのポートがあります。これらは、Interfaces ペインに一覧表示されますが、ASDM でこれらのポートを設定することはできません。

ポート パラメータの設定

ポート パラメータには、スピード、管理ステート（up または down）、PortFast 設定、モード（ルーテッドまたはスイッチポート）が含まれます。

スイッチ ポート パラメータを設定するには、次の手順を実行します。

ステップ 1　Configuration > Switch > Interfaces ペインで、設定するポートをクリックします。

編集するセルをクリックして、テーブルの設定を直接編集するか、**Modify Port(s) Parameters** をクリックします。

ステップ 2　次のパラメータを設定します。

- Speed(Mb/s)：ドロップダウン リストから適切な値を選択します。
- Admin St：ドロップダウン リストから Up または Down を選択します。
- Port Fast：スイッチポート モードで、ボックスをクリックして、ポートの STP PortFast をイネーブルにします。STP PortFast は、リスニング ステートとラーニング ステートをバイパスして、ただちにフォワーディング ステートに入るアクセス ポートとして、Layer 2 LAN ポートを設定します。1 台のワークステーションまたはサーバに接続された Layer 2 アクセス ポートの PortFast を使用して、STP がコンバージするのを待機せずに、これらのデバイスがただちにネットワークに接続するのを許可できます。1 台のワークステーションまたはサーバに接続されたインターフェイスは、ブリッジ プロトコル データ ユニット（BPDU）を受信してはいけません。PortFast の設定時には、ポートはまだスパニング ツリー プロトコルを実行しています。PortFast イネーブルのポートは、必要に応じて（優位の BPDU を受信した場合に起こることがあります）、ただちにブロッキング ステートに移行できます。
- Mode：スイッチポート アクセス モードまたはルーテッド モードにモードを設定します。

（注） ASDM はポートにルーテッド モードを割り当てますが、VLAN にルーテッド ポートを割り当てられないため、FWSM ではそのポートを使用できません。

ステップ 3　モードをルーテッドに設定する場合、**Switch IP Add** と **Mask** のセルをダブルクリックし、値を入力することによって、スイッチの IP アドレスとマスクを設定できます。

マルチコンテキスト モードでコンテキスト内に IP アドレスを設定した場合、コンフィギュレーションを適用する際に ASDM は、IP アドレスがコンテキスト内のアドレスと重複していないことを確認します。システムに IP アドレスを設定すれば、照合は実行されません。

ステップ 4　**Apply** をクリックして変更を適用するか、スイッチポート モードのポートについて、P.3-7 の「VLAN へのポートの割り当て」を参照して引き続き設定を行います。

VLAN へのポートの割り当て

スイッチポート モードでポートを VLAN に割り当てられます。ポートを VLAN に割り当てるには、次の手順を実行します。

ステップ 1　Configuration > Switch > Interfaces ペインで、同じ VLAN に割り当てる 1 つ以上のポートを（スイッチポート モードで）クリックします。連続していないポートを選択するには、Ctrl キーを押した状態でポートをクリックします。連続しているポートを選択するには、Shift キーを押した状態でポートをクリックします。

（注） FWSM の内部シャーシ 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通信に予約されている VLAN にスイッチ ポートを割り当てないでください。

ステップ 2　**Assign Port(s) to Vlan** をクリックします。

Assign Ports to Vlan ダイアログボックスが表示されます。

ステップ 3　Vlan# ドロップダウン リストで VLAN ID を選択するか、**Add** をクリックして、新しい VLAN を追加します。

VLAN 追加の詳細については、P.3-9 の「VLAN とスイッチド仮想インターフェイスの設定」を参照してください。

また、ポートを 1 つ選択した場合は、Vlan Id セルをクリックし、ドロップダウン リストから VLAN を選択して、テーブルに VLAN を直接設定できます。

ステップ 4　**OK** をクリックします。

ステップ 5　（オプション）既存の VLAN グループに VLAN を割り当てるには、次のオプションのいずれかを使用します。

- Assign the VLAN to a VLAN group that is assigned to an FWSM：FWSM に割り当てられた VLAN グループにある VLAN は、*secured VLAN* と呼ばれます。**Secured** をクリックし、次に **VlanGroup** セルをクリックして、ドロップダウン メニューから VLAN グループ ID を選択します。FWSM に割り当てられた VLAN グループだけが一覧表示されます。マルチコンテキスト モードでは、デフォルトで、VLAN が現在のコンテキストに割り当てられます。システムにいる場合は、VLAN はどのコンテキストにも割り当てられません。
- Assign the VLAN to a VLAN group that is not yet assigned to an FWSM：**VlanGroup** セルをクリックし、ドロップダウン メニューから VLAN グループ ID を選択します。**Secured** をクリックしないでください。FWSM に割り当てられていない VLAN グループだけが一覧表示されます。

VLAN グループの追加と設定の詳細については、P.3-13 の「ファイアウォール VLAN グループの設定」を参照してください。

ステップ 6　（オプション）セキュアな VLAN については、テーブルのセルをダブルクリックし、値を入力して、FWSM のインターフェイス名、セキュリティ レベル、IP アドレス、マスクを設定できます（FWSM が透過モードの場合は、インターフェイス名とセキュリティ レベルのみを設定できます）。マルチコンテキスト モードでは、VLAN が現在のコンテキストに割り当てられている場合に、これらのフィールドの編集のみが行えます。システムでは、これらの設定を編集できません。

FWSM のインターフェイス設定の詳細については、第 5 章「インターフェイスの設定」を参照してください。

ステップ 7　（オプション）VLAN の SVI を作成するには、**Switch IP Add** セルと **Mask** セルをダブルクリックし、値を入力することによって、スイッチ IP アドレスとマスクを設定できます。

複数の SVI を追加する場合は、必ず Vlans ペインのこの機能をイネーブルにしてください。SVI の詳細については、P.3-9 の「VLAN とスイッチド仮想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 モードでコンテキスト内に IP アドレスを設定した場合、コンフィギュレーションを適用する際に ASDM は、IP アドレスがコンテキスト内のアドレスと重複していないことを確認します。システムに IP アドレスを設定すれば、照合は実行されません。

ステップ 8　**Apply** をクリックします。

（注） VLAN が Configuration > Switch > Vlans にないのにポートに割り当てる場合は、Vlan Name、Secured、Vlan Group、Switch IPAdd、Mask のオプションは変更できません。

マルチコンテキスト モードで、新しい VLAN をセキュリティ コンテキストに割り当てる場合は、システム コンフィギュレーションをリフレッシュする必要があります。

VLAN とスイッチド仮想インターフェイスの設定

ASDM によって、VLAN をスーパーバイザに追加でき、MSFC のスイッチ仮想インターフェイス（SVI）になる VLAN を設定できます。SVI で使用する VLAN を FWSM に割り当て（P.3-13 の「ファイアウォール VLAN グループの設定」を参照）、次に FWSM と他の Layer 3 VLAN の間の MSFC ルートに割り当てます。

ここでは、次の項目について説明します。

VLAN のガイドライン

FWSM での VLAN 使用については、次のガイドラインを参照してください。

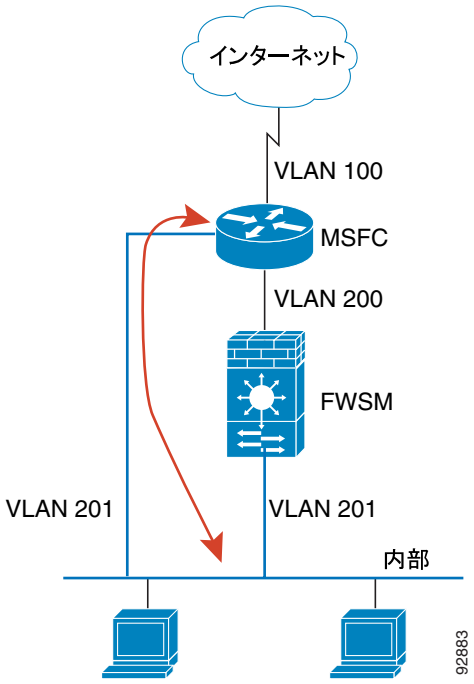
- FWSM ではプライベート VLAN を使用できます。FWSM にプライマリ VLAN を割り当てます。FWSM は、自動的にセカンダリ VLAN トラフィックを処理します。
- 予約済み VLAN を使用することはできません。
- VLAN 1 を使用することはできません。
- 2 ～ 1000 および 1025 ～ 4094 の VLAN ID を使用します。

（注） ルーテッド ポートと WAN ポートは、内部 VLAN を消費するので、1020 ～ 1100 の範囲の VLAN はすでに使用されている可能性があります。

SVI の概要

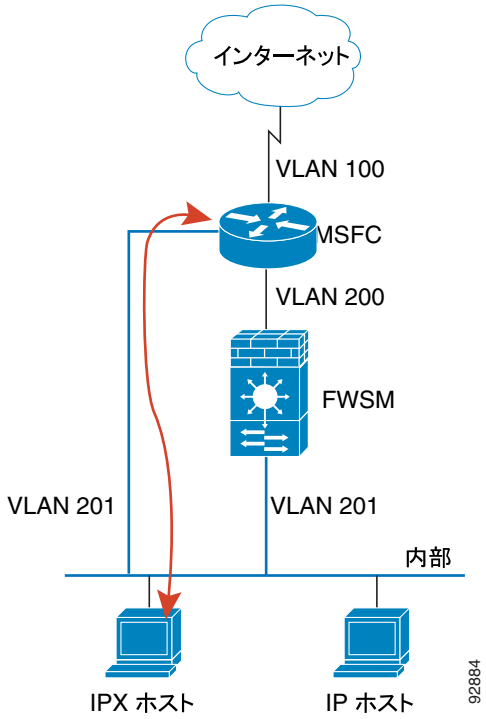
セキュリティ上の理由で、デフォルトでは、1 つの SVI しか MSFC と FWSM の間に存在できません。たとえば、複数の SVI をシステムに誤設定すると、MSFC に内部と外部の VLAN を割り当てることによって、トラフィックが FWSM を通過することを誤って許可してしまうことがあります。図 3-1 を参照してください。

図 3-1　マルチ SVI のミスコンフィギュレーション



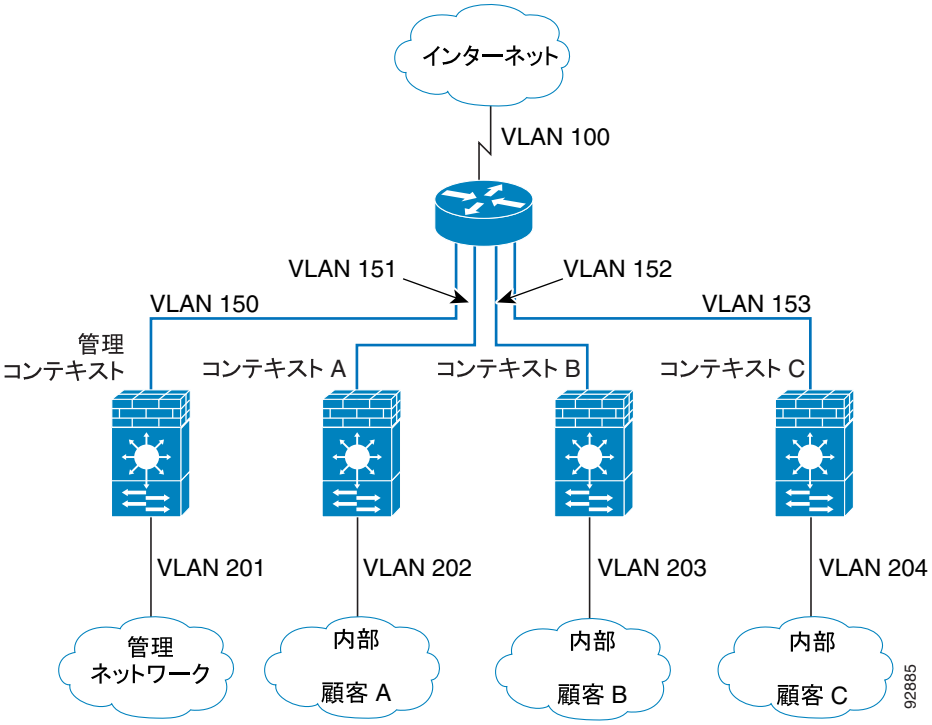
ただし、ネットワーク シナリオによっては、FWSM をバイパスする必要があります。図 3-2 は、IP ホストと同じイーサネット セグメント上の IPX ホストを示しています。FWSM はルーテッド ファイアウォール モードの場合、IP トラフィックのみを処理し、IPX（透過ファイアウォール モードは、オプションで IP 以外のトラフィックを許可します）などの他のプロトコルをドロップするため、IPX トラフィックについては FWSM をバイパスすることもできます。IPX トラフィックのみが VLAN 201 を通過することを許可するアクセスリストを使用して、MSFC を設定してください。

図 3-2　IPX 対応のマルチ SVI



マルチコンテキスト モードの透過ファイアフォールでは、各コンテキストが外部インターフェイスに固有の VLAN を必要とするため、マルチ SVI を使用する必要があります（図 3-3 を参照）。ルーテッド モードでもマルチ SVI を使用できます。その場合、外部インターフェイスで 1 つの VLAN を共有する必要はありません。

図 3-3　マルチコンテキスト モードでのマルチ SVI



VLAN および SVI の設定

VLAN および SVI を設定するには、次の手順を実行します。

ステップ 1　（オプション）Configuration > Switch > Vlans ペインに移動します。

ステップ 2　複数の SVI を FWSM に追加できるようにするには、**Allow to add more than one SVI to FWSM** をクリックします。

ステップ 3　VLAN を追加するには、**Add** をクリックします。

Add Vlan ダイアログボックスが表示されます。

ステップ 4　VLAN を 1 つまたは VLAN の範囲を追加できます。

- VLAN を 1 つ追加するには、**Add single VLAN** をクリックし、次の値を入力します。
  - Vlan Id：VLAN ID を入力します。FWSM で使用できる VLAN の詳細については、P.3-9 の「VLAN のガイドライン」を参照してください。
  - （オプション）Vlan Name：VLAN 名を入力します。デフォルトでは、名前は VLAN *number* です。

— （オプション）SVI：この VLAN を SVI にする場合は、**SVI** をクリックします。
Switch Interface IP：SVI の IP アドレスを入力します。
Switch Interface Mask：マスクを入力します。

- VLAN の範囲を追加するには、**Add VLAN Range** をクリックし、VLAN ID の範囲をカンマおよびダッシュで区切って入力します。たとえば、2-5,7,10-20 のようになります。
  VLAN の範囲を追加した後で、VLANs テーブルで個別のアトリビュートを設定できます。

ステップ 5　**OK** をクリックします。

VLAN は、Vlans テーブルに追加します。

ステップ 6　（オプション）Vlans テーブルでは、次のインライン編集ができます。

- VLAN 名を変更します。
  スイッチが VTP クライアント モードの場合、VLAN ID が 1 または 1002 ～ 1005 の場合に、VLAN 2 ～ 1001 については、VLAN 名は編集できません。
- **SVI** をオンにして、SVI をイネーブルまたはディセーブルにします。
  マルチ VLAN のこの設定をイネーブルにするには、必ずマルチ SVI をイネーブルにしてください（ステップ 2 を参照）。ただし、マルチ SVI 機能がディセーブルであっても、それらが（FWSM に割り当てられた）セキュアな VLAN でない場合は、マルチ VLAN の SVI ステートをイネーブルにできます。VLAN 1 では SVI ステートは編集できません。
- SVI の IP アドレスとマスクを変更します（SVI がイネーブルの場合）。
- VLAN を VLAN グループに割り当てます。詳細については、次の手順を参照してください。

（注）　Secured and Vlan Groups フィールドは、編集できません。

ステップ 7　VLAN を削除するには、テーブルのその VLAN の行を選択し、**Delete** をクリックします。

このアクションにより、その VLAN に対応する SVI が削除され、VLAN グループに割り当てられている場合は、そのグループからも削除されます。

ステップ 8　**Apply** をクリックします。

（注）　スイッチ上のプライベート VLAN のコンフィギュレーションは、ASDM によってサポートされていません。

ファイアウォール VLAN グループの設定

この項では、VLAN を FWSM に割り当てる方法について説明します。FWSM には、外部の物理インターフェイスはありません。代わりに、VLAN インターフェイスを使用します。FWSM への VLAN の割り当ては、スイッチ ポートへの VLAN の割り当てに類似しています。FWSM には、スイッチ ファブリック モジュール（存在する場合）または共有バスへの内部インターフェイスがあります。

ここでは、次の項目について説明します。

VLAN グループ ガイドライン

次の VLAN グループのガイドラインを参照してください。

- 最大 16 のファイアウォール VLAN グループを各 FWSM に割り当てられます。たとえば、すべての VLAN を 1 つのグループに割り当てたり、内部グループと外部グループを作成したり、各カスタマーのグループを作成したりすることができます。
- 各グループには、複数の VLAN があります。
- 同じ VLAN を複数の VLAN グループに割り当てることはできません。ただし、複数の VLAN グループを 1 つの FWSM に割り当てたり、1 つの VLAN グループを複数の FWSM に割り当てたりすることができます。たとえば、複数の FWSM に割り当てる VLAN は、各 FWSM に固有の VLAN から別個のグループで存在できます。

（注） ASDM では、VLAN グループを現在の FWSM とスタンバイ装置にだけ割り当てられます。ただし、同じスイッチ上の異なる FWSM に 別の ASDM セッションを開いたり、同じ割り当ての VLAN グループを表示したりすることができるので、FWSM 間で VLAN グループを共有できます。

- シャーシ内のフェールオーバーの場合、ASDM は自動的に同じ VLAN グループをセカンダリ装置に割り当てます。

（注） VLAN グループを FWSM に割り当てた後でフェールオーバーをイネーブルにすると、ASDM はそのグループをスタンバイ装置に追加しません。同様に、後でフェールオーバーをディセーブルにすると、ASDM は VLAN グループをスタンバイ装置から削除しません。このような変更を行うには、CLI を使用する必要があります。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。

- シャーシ内のフェールオーバーの場合は、同じ VLAN をセカンダリ装置に個別に割り当てる必要があります。シャーシ間のトランク ポートの VLAN についても同様です。詳細については、P.3-17 の「フェールオーバー用のスイッチの設定」を参照してください。

VLAN グループの設定および FWSM への割り当て

VLAN グループを作成し、それを FWSM へ割り当てるには、次の手順を実行します。

ステップ 1　Configuration > Switch > Vlan Groups ペインで、VLAN グループを追加または編集するには、**Add** または **Edit** をクリックします。

Add/Edit Firewall Vlan Group ダイアログボックスが表示されます。

ステップ 2　Vlan グループ領域で、Firewall vlan group フィールドに整数で VLAN グループ ID を入力します。

ステップ 3　左のテーブルで 1 つ以上の VLAN ID を選択し、>> ボタンをクリックして、グループに追加します。

VLAN を削除するには、右のテーブルでそれを選択し、<< ボタンをクリックします。

ステップ 4　VLAN グループを現在の FWSM に割り当てるには、**Assign vlan group to current FW module** をクリックします。

マルチコンテキスト モードのデフォルトでは、グループ内の VLAN は現在のコンテキストに割り当てられています。システムにいる場合は、VLAN を割り当てるコンテキストを選択できます（ステップ 6 を参照）。VLAN のコンテキストへの割り当ての詳細については、P.7-20 の「セキュリティ コンテキストの設定」を参照してください。

ステップ 5　シャーシ内のフェールオーバーがイネーブルの場合は、Standby module slot フィールドでスタンバイ装置のモジュール スロット番号を入力します。

同じ VLAN グループを両方のフェールオーバー装置に割り当てる必要があります。モジュール内のフェールオーバーの場合は、VLAN をスタンバイ装置に個別に割り当てる必要があります。FWSM スロットを表示するには、P.3-3 の「CLI でのモジュール インストレーションの検証」を参照してください。

（注）　VLAN グループを FWSM に割り当てた後でフェールオーバーをイネーブルにすると、ASDM はそのグループをスタンバイ装置に追加しません。同様に、後でフェールオーバーをディセーブルにすると、ASDM は VLAN グループをスタンバイ装置から削除しません。このような変更を行うには、CLI を使用する必要があります。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。

ステップ 6　（オプション）VLAN グループを現在の FWSM に割り当てると、FWSM のインターフェイスを設定でき、マルチコンテキスト モードでは、コンテキストを設定できます。

インターフェイスの設定の詳細については、第 5 章「インターフェイスの設定」を参照してください。コンテキストへの VLAN の割り当ての詳細については、P.7-20 の「セキュリティ コンテキストの設定」を参照してください。

後で Configuration > Switch > Interfaces テーブルで設定を編集できます。Vlan Groups 領域の設定については、適用後に編集することができません。

a. Firewall Configuration 領域では、FW Interface Name フィールドにインターフェイス名を入力します。

グループに 1 つしか VLAN がない場合、名前はそのままです。ただし、グループに複数の VLAN がある場合は、VLAN ID が名前に付加されます。たとえば、inside という名前を入力すると、グループに VLAN 2、3、4 があれば、その名前は、inside2、inside3、inside4 となります。

b. Security Level フィールドでは、セキュリティ レベルを 0 ～ 100 の間で入力します。

c. FW Interface IP フィールドでは、IP アドレスを入力します。同じ IP アドレスを複数のインターフェイスに割り当てることはできないため、このフィールドは、グループに 1 つしか VLAN がない場合のみ使用できます。システムで、VLAN を 1 つ持つグループがマルチコンテキストに割り当てられていると、マルチコンテキストでは共有 VLAN が同じ IP アドレスを持つことができないため、IP アドレスを割り当てられません。

d. FW Interface Mask フィールドでは、サブネット マスクを入力します。このフィールドは、グループに VLAN が 1 つしかない場合にのみ使用できます。システムで VLAN を 1 つ持つグループがマルチコンテキストに割り当てられていると、マスクを設定できません。

e. マルチコンテキスト モードでは、システムで左のテーブルから 1 つ以上のコンテキスト名を選択し、>> ボタンをクリックして、VLAN グループを割り当てるコンテキストを設定します。

新しいコンテキストを追加するには、**Add** をクリックします。コンフィギュレーション ファイルにコンテキスト名と URL を設定する必要があります。

コンテキストを削除するには、右側のテーブルで << ボタンをクリックします。

コンテキスト内にいる場合は、現在のコンテキストが選択され設定はできません。同じ VLAN を別のコンテキストに後で割り当てる場合は、別のコンテキストに移動し、Vlan Groups ペインでグループを編集できます。インターフェイスの設定は、新しい現在のコンテキストに割り当てられます。

マルチコンテキストを選択すると、そのインターフェイスの設定が各コンテキストによって継承されます。

（注） FWSM に割り当てられた VLAN グループに VLAN を追加すると、Firewall Configuration 領域は新しく追加された VLAN にのみ適用されます。

ステップ 7　**OK** をクリックします。

ステップ 8　Vlan Groups ペインで、**Apply** をクリックします。

CLI での FWSM の内部インターフェイスのカスタマイズ

FWSM とスイッチの接続は、6-GB 802.1Q トランキング EtherChannel です。この EtherChannel は、FWSM をインストールしたときに、自動的に作成されます。FWSM 側では、2 つの NP が 3 つのギガビット イーサネットのインターフェイスに個別に接続されており、これらのインターフェイスは、EtherChannel を構成しています。スイッチは、セッション情報に基づいた分散アルゴリズムにしたがって、トラフィックを EtherChannel のインターフェイスに分散します。ロード シェアリングは、パケットごとではなく、フローごとに実行されます。場合によっては、アルゴリズムはトラフィックをインターフェイス間、さらに 2 つの NP 間に不規則に割り当てます。FWSM の潜在的処理能力を十分に活用しないだけでなく、リソースの管理をマルチコンテキストに適用したときに、一貫した不均衡が予測外の動作を引き起こす結果になります。

```
Router(config)# port-channel load-balance {dst-ip | dst-mac | dst-port | src-dst-ip |
src-dst-mac | src-dst-port | src-ip | src-mac | src-port}
```

デフォルトは、**src-dst-ip** です。

フェールオーバー用のスイッチの設定

フェールオーバー用にスイッチを設定するには、次の項目を参照してください。

プライマリ スイッチとセカンダリ スイッチ間へのトランクの追加

スイッチ内のフェールオーバーを使用する場合、2 つのスイッチ間に 802.1Q VLAN トランクを設定して、フェールオーバー リンクおよびステート リンクを伝送する必要があります。トランクでは、QoS がイネーブルになっている必要があります。トランクで QoS がイネーブルになっていると、CoS 値が 5（優先順位がより高い）のフェールオーバーの VLAN パケットがこれらのポートでより高い優先順位で処理されます。

EtherChannel およびトランクを設定するには、スイッチのマニュアルを参照してください。

透過ファイアウォール モードとの互換性の確認

透過モードでフェールオーバーを使用するときにループを回避するには、BPDU の転送をサポートするスイッチ ソフトウェアを使用します。透過ファイアウォール モードのスイッチのサポートの詳細については、P.A-2 の「スイッチのハードウェアおよびソフトウェアの互換性」を参照してください。

FWSM が透過モードの場合は、スイッチの LoopGuard をグローバルにイネーブルにしないでください。LoopGuard は自動的にスイッチと FWSM 間の内部 EtherChannel に適用されます。そのため、フェールオーバーやフォールバックの後で、EtherChannel が err-disable 状態になり、LoopGuard によってセカンダリ装置が切断されます。

迅速なリンク障害検出用自動ステートメッセージのイネーブル化

Catalyst オペレーティング システムのソフトウェア リリース 8.4（1）以降、または Cisco IOS ソフトウェア リリース 12.2（18）SXF5 以降を使用して、スーパーバイザ エンジンは、FWSM の VLAN に関連付けられた物理インターフェイスの状態について、自動ステート メッセージを FWSM に送信できます。たとえば、VLAN に関連付けられたすべての物理インターフェイスがダウンしたとき、自動ステート メッセージが FWSM に VLAN がダウンしたことを伝えます。この情報に基づき、通常はどちら側がリンク障害を起こしたかを判断するのに必要なインターフェイスのモニタリング テストをバイパスすることによって、FWSM が VLAN のダウンを宣言します。自動ステート メッセージは、FWSM がリンク障害を検出する時間を大幅に短縮します（自動ステートのサポートがない場合の最長 45 秒に対し、数ミリ秒）。

スイッチ スーパーバイザは、次の場合に、自動ステート メッセージを FWSM に送信します。

- VLAN に属している最後のインターフェイスがダウンした場合。
- VLAN に属している最初のインターフェイスが復旧した場合。

（注） シャーシに FWSM を 1 つインストールした場合のみ、スイッチは自動ステート メッセージをサポートします。

Cisco IOS ソフトウェアでは、自動ステート メッセージは、デフォルトでディセーブルになっています。Cisco IOS ソフトウェアで、自動ステート メッセージをイネーブルにするには、次のコマンドを入力します。

```
Router(config)# firewall autostate
```

Catalyst オペレーティング システム ソフトウェアは、自動ステート メッセージがデフォルトでイネーブルになっており、設定はできません。ただし、Catalyst オペレーティング システムの自動ステートは、SVI でのみ使用できます。この機能を利用する場合は、すべての VLAN に「ダミー」の SVI を作成できますが、これらの SVI に IP アドレスは設定しないでください。たとえば、次のコンフィギュレーションによって、マルチ SVI をイネーブルにし、VLAN 55 および 56 の SVI を作成しますが、これらの SVI に IP アドレスは割り当てません。

```
Console> (enable) set vlan 55-56 firewall-vlan 8
Console> (enable) set firewall multiple-vlan-interfaces enable
Console> (enable) switch console
Router> enable
Password: ******
Router# configure terminal
Router(config)# interface vlan 55
Router(config-if)# interface vlan 56
Router(config-if)# end
Router# ^C^C^C
Console> (enable)
```

CLI での Firewall Services Module のブート パーティションの管理

この項では、スイッチから FWSM をリセットする方法とフラッシュ メモリ カードのブート パーティションを管理する方法について説明します。次の事項を取り上げます。

フラッシュ メモリの概要

FWSM は、オペレーティング システム、コンフィギュレーション、その他のデータを保存する 128 MB のフラッシュ メモリ カードを搭載しています。フラッシュ メモリには、6 つのパーティションがあり、Cisco IOS および Catalyst オペレーティング システム ソフトウェア コマンドの **cf:***n* と呼ばれます。

- Maintenance partition（**cf:1**）：メンテナンス ソフトウェアが含まれています。メンテナンス ソフトウェアを使用して、アプリケーション イメージをアップグレードまたはインストールしたり、アプリケーション パーティションをブートできない場合は、アプリケーション イメージのパスワードをリセットするか、クラッシュ ダンプ情報を表示したりします。
- Network configuration partition（**cf:2**）：メンテナンス ソフトウェアのネットワーク コンフィギュレーションが含まれています。FWSM が TFTP サーバに到達して、アプリケーション ソフトウェア イメージをダウンロードできるようにするためには、メンテナンス ソフトウェアに IP 設定が必要です。
- Crash dump partition（**cf:3**）：クラッシュ ダンプ情報を保存します。
- Application partitions（**cf:4** および **cf:5**）：アプリケーション ソフトウェア イメージ、システム コンフィギュレーション、ASDM を保存します。デフォルトで、**cf:4** のイメージがインストールされています。テスト パーティションとして **cf:5** を使用できます。たとえば、ソフトウェアをアップグレードする場合、新しいソフトウェアを **cf:5** にインストールし、問題が起きた場合のバックアップとして古いソフトウェアを保存しておくことができます。各パーティションには、独自のスタートアップ コンフィギュレーションが含まれています。
- Security context partition（**cf:6**）：このパーティションは、64 MB で、ナビゲート可能なファイル システムにセキュリティ コンテキスト コンフィギュレーション（必要に応じて）と RSA キーを保存します。その他のパーティションには、ファイルのリストなどの共通のタスクを実行できるファイル システムがありません。このパーティションは、**copy** コマンドを使用するときに **disk** と呼ばれます。

デフォルトのブート パーティションの設定

デフォルトで、FWSM は、**cf:4** アプリケーション パーティションからブートします。ただし、**cf:5** アプリケーション パーティションからブートするか、**cf:1** メンテナンス パーティションにブートするか選択できます。各アプリケーション パーティションは、独自のスタートアップ コンフィギュレーションを持ちます。

デフォルトのブート パーティションを変更するには、次のコマンドを入力します。

```
Router(config)# boot device module mod_num cf:n
```

n は、1（メンテナンス）、4（アプリケーション）、5（アプリケーション）です。

現在のブート パーティションを表示するには、次のコマンドを入力します。

```
Router# show boot device [mod_num]
```

次の例を参考にしてください。

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

FWSM のリセットまたは特定のパーティションからのブート

この項では、FWSM をリセットまたは特定のパーティションからブートする方法について説明します。CLI または外部 Telnet セッションを通じて到達できない場合は、FWSM をリセットする必要がある場合があります。メンテナンス パーティションにアクセスする必要のある場合、または、バックアップ アプリケーション パーティションの別のソフトウェア イメージからブートする場合は、デフォルトでないブート パーティションからブートする必要がある場合があります。メンテナンス パーティションは、トラブルシューティングに役立ちます。

リセットのプロセスは、数分かかる場合があります。

FWSM をリセットすると、フルメモリ テストの実行も選択できます。FWSM を最初にブートしたときには、部分的なメモリ テストのみが実行されます。フルメモリ テストには、約 6 分かかります。

（注） FWSM にログインした時に FWSM をリロードするには、**reload** または **reboot** と入力します。これらのコマンドによってデフォルトでないブート パーティションからブートすることはできません。

FWSM をリセットするには、次のコマンドを入力します。

```
Router# hw-module module mod_num reset [cf:n] [mem-test-full]
```

cf:*n* の引数は、1（メンテナンス）、4（アプリケーション）、5（アプリケーション）です。パーティションを指定しない場合は、デフォルトのパーティションが使用されます（通常は **cf:4**）。

mem-test-full オプションは、フルメモリ テストを実行します。このテストは、約 6 分かかります。

この例は、スロット 9 にインストールされた FWSM のリセットの方法を示しています。デフォルトのブート パーティションを使用します。

```
Router# hw-module module 9 reset

Proceed with reload of module? [confirm] y
% reset issued for module 9

Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

CHAPTER 4

Startup Wizard

ASDM Startup Wizard で、FWSM の初期コンフィギュレーションを段階的に設定することができます。コンフィギュレーション画面をクリックすると表示されるプロンプトに従って、使用する FWSM の情報を入力します。Startup Wizard で設定すると、FWSM の使用をすぐに開始できます。

Startup Wizard では、コンフィギュレーションで次のように定義します。

- 使用する FWSM のホスト名
- 使用する FWSM のドメイン名
- イネーブル パスワード。ASDM またはコマンドライン インターフェイスから FWSM への管理アクセスを制限するのに使用します。
- FWSM の外部インターフェイス IP アドレスの情報
- 内部インターフェイスまたは DMZ インターフェイスなど、FWSM で使用する他のインターフェイスも Startup Wizard ウィザードで設定できます。
- FWSM のネットワーク アドレス変換（NAT）またはポート アドレス変換（PAT）ルール
- DHCP サーバとして内部インターフェイスを設定するための動的ホスト制御プロトコル（DHCP）設定。

各設定の詳細情報を表示するには、該当するコンフィギュレーション画面で Help ボタンをクリックします。

Startup Wizard の使用には次の情報が必要です。事前に確認してください。

- 使用するネットワークで FWSM を識別する一意のホスト名
- 外部インターフェイス、内部インターフェイスなどの IP アドレス
- NAT または PAT のコンフィギュレーションに使用する IP アドレス
- DHCP サーバの IP アドレス範囲

次の点に注意してください。

- Startup Wizard は、ASDM の Wizards メニューからいつでもアクセスできます。
- Help のアイコンには疑問符「?」が表示されています。
- 以降の Startup Wizard ページでは、**Finish** をクリックしてウィザードをいつでも終了できます。ここでは、Startup Wizard での変更が FWSM に送信されます。

フィールド

Startup Wizard のすべてのペインで、次のボタンが表示されます。

- Back：直前のペインに戻ります（このペインではグレー表示されます）。
- Next：次のペインに進みます。
- Finish：このペインで行った選択に従い、コンフィギュレーションを FWSM に送信します（このペインではグレー表示されます）。

- Cancel：変更を破棄して適用しません。**Cancel** をクリックすると、Exit Wizard ダイアログボックスが表示されます。**Exit** をクリックすると Wizard は終了し、**Cancel** をもう一度クリックすると Wizard ペインに戻ります。Wizard で **Back** をクリックすると、いつでも直前のペインに戻れます。

Launch Startup Wizard：Startup Wizard を起動します。

（注） Launch Startup Wizard は、ツールバーから Wizards > Startup Wizard をクリックした場合、表示されません。

モード

次の表に、この機能を使用できるモードを示します。

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

Welcome to the Startup Wizard

利点

Welcome to the Startup Wizard ペインでは、Cisco ASDM Startup Wizard を導入します。

フィールド

Welcome to the Startup Wizard ペインには、Next、Cancel、Help ボタンが表示されます。

（注） この画面の Back と Finish ボタンはディセーブルになっています。

モード

次の表に、この機能を使用できるモードを示します。

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

Basic Configuration

利点

Basic Configuration ペインで、使用する FWSM のホスト名とイネーブル パスワード、および FWSM のドメイン名を設定できます。

ドメイン名は最大 63 文字の英数字で指定します。大文字と小文字を区別しません。

イネーブル パスワードを使用すると、ASDM または FWSM をコマンドライン インターフェイスから管理できます。パスワードは最大 16 文字の英数字で、大文字と小文字を区別します。現在のパスワードを変更するには、**Change privileged mode (enabled) password** チェックボックスをオンにし、変更前のパスワードと変更後のパスワードを入力してから、変更後のパスワードをフィールドで確認します。

（注） パスワード フィールドを空白にすると Password Confirmation 画面が表示されて、非常に大きなセキュリティ リスクであることを警告します。

フィールド

Basic Configuration ペインには、Back、Next、Finish、Cancel、Help ボタン、および次の項目が表示されます。

- **FWSM HostName**：FWSM のホスト名を入力します。ホスト名は最大 63 文字の英数字で、大文字と小文字を区別しません。
- Domain Name：FWSM の IPSec ドメイン名を指定します。後で認証に使用されます。ドメイン名は最大 63 文字の英数字で指定します。特殊文字とスペースは使用できません。

- Privileged Mode (Enable) Password：ASDM またはコマンドライン インターフェイスから FWSM への管理アクセスを制限します。
  - Change privileged mode (enable) password：現在のイネーブル パスワードを変更します。
  - Old Password：変更前のイネーブル パスワードがある場合、そのパスワードを入力します。
  - New Password：変更後のイネーブル パスワードを入力します。パスワードは最大 16 文字の英数字で、大文字と小文字を区別します。
  - Confirm New Password：変更後のイネーブル パスワードを再入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

この機能は、ASDM アプリケーションのメイン ウィンドウで利用できます。

Configuration > Properties > Device Administration > Device

Configuration > Properties > Device Administration > Password

Management IP Address Configuration

(注)　この機能は、透過モードだけで使用できます。

利点

Management IP Address Configuration ペインで、ホストの管理 IP アドレスをこのコンテキストに設定できます。

フィールド

Management IP Address Configuration ペインには、Back、Next、Finish、Cancel、Help ボタン、および次の項目が表示されます。

- Bridge Group：インターフェイスが属するブリッジ グループを指定します。ブリッジ グループは、1 ～ 63 の数字を含んでいます。
- Management IP Address：ASDM またはセッション プロトコルを利用して、管理のために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。
- Subnet Mask：管理 IP アドレスのサブネット マスク。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

この機能は、ASDM アプリケーションのメイン ウィンドウで利用できます。

Configuration > Features > Properties > Management IP

Auto Update Server

利点

Auto Update Server 画面で、FWSM をリモートで管理できます。設定すると、FWSM コンフィギュレーション、FWSM イメージ、ASDM イメージが自動更新されます。

フィールド

Auto Update Server 画面には、**Back**、**Next**、**Finish**、**Cancel**、**Help ボタン**、および次の項目が表示されます。

- Enable Auto Update：FWSM と Auto Update サーバの通信をイネーブルにします。
- Server エリア
  - Server URL：ドロップダウン リストからセキュア http（https）または http を選択し、Auto Update サーバの URL の先頭を指定します。次のボックスに、Auto Update サーバの残りの IP アドレスを入力します。
  - Verify server SSL certificate：Auto Update サーバで SSL 認証がイネーブルになっているか確認します。
- User エリア
  - Username：Auto Update サーバにログインするユーザ名を入力します。
  - Password：Auto Update サーバにログインするパスワードを入力します。
  - Confirm Password：パスワードを確認のために再入力します。
- Device Identify エリア
  - Device ID Type：ドロップダウン リストから、セキュリティ アプライアンスを識別する一意の ID タイプを選択します。User-defined name を選択すると Device ID フィールドがイネーブルになり、一意の ID を指定できます。
  - Device ID：セキュリティ アプライアンスの ID に使用する一意の文字列を入力します。

モード

次の表に、この機能を使用できるモードを示します。

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

Outside Interface Configuration

利点

Outside Interface Configuration ペインで、適切なインターフェイスを選択し、名前を付け、IP アドレスを指定すると、外部インターフェイスを設定できます。

(注)　LAN が設定されるとペインにメッセージが表示され、さらに変更するには Configuration > Features > Interfaces を選択することを示します。

フィールド

Outside Interface Configuration ペインには、Back、Next、Finish、Cancel、Help ボタン、および次の項目が表示されます。

- Interface：設定するインターフェイスを指定します。
- Interface Name：インターフェイスの名前を指定します。
- IP Address：インターフェイスの IP アドレスを指定します。

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

  Subnet Mask：外部インターフェイスのサブネット マスクを指定します。サブネット マスクの IP アドレスのリストが表示されます。

  Default Gateway：外部インターフェイスのデフォルト ゲートウェイを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

この機能は、ASDM アプリケーションのメイン ウィンドウで利用できます。

Configuration > Interfaces

Interface Configuration

利点

Interface Configuration ペインで、内部インターフェイスを設定できます。インターフェイスを選択して Edit ボタンをクリックし、Edit ペインで設定します。

（注） 外部インターフェイスは、Outside Interface Configuration ペインで設定する必要があります。外部インターフェイスを選択すると、Outside Interface Configuration ペインで設定するように求めるメッセージが表示されます。

フィールド

Interface Configuration ペインには、Back、Next、Finish、Cancel、Help ボタン、および次の項目が表示されます。

- Interface：元のホストまたはネットワークに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：編集するインターフェイスの名前を表示します。
- Enabled：インターフェイスのステートフル フェールオーバーまたは LAN ベース フェールオーバーがイネーブルかどうかを表示します。
- Security Level：インターフェイスのセキュリティ レベル範囲が 0 ～ 100 で表示されます。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。FWSM の各インターフェイスのセキュリティ レベルは、そのインターフェイスの背後にあるネットワークの信頼レベルを表します。数字が大きくなると、信頼レベルが上がります。
- IP Address：編集するホストまたはネットワーク インターフェイスの IP アドレスを表示します。
- Subnet Mask：IP アドレスのネットワーク サブマスクを表示します。

（注） 透過モードでは、Interface、Name、Security Level フィールドのみが表示されます。

- Edit：**Edit** をクリックし、Edit Interface ダイアログボックスでインターフェイスを設定します。

  Edit Interface ダイアログボックスを表示します。
  - Enable Interface：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には、このボックスをオンにします。
  - Interface：編集するインターフェイスを表示します。
  - Interface Name：編集するインターフェイス名を表示します。または、インターフェイス名を選択できます。
  - 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。外部ネットワークは 0、内部ネットワークは 100 です。境界インターフェイスには、1 ～ 99 の範囲の番号が使用されます。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。
  - IP Address：インターフェイスの IP アドレスです。
  - Subnet Mask：インターフェイスの IP アドレスのマスクです。

  （注） 透過モードの Edit Interface ダイアログボックスには、Interface、Interface Name、Security Level フィールドのみが表示されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

この機能は、ASDM アプリケーションのメイン ウィンドウで利用できます。

Configuration > Interfaces

Static Routes

利点

Static Route 画面で、すべてのインターフェイスで、ルータ接続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、または簡単な形式の 0 に設定します。

1 つの FWSM 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、FWSM 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、Metric はデフォルトの 1 にします。

Add/Edit Static Routes

利点

Add/Edit Static Route ダイアログボックスで、スタティック ルートを追加または編集できます。

DHCP Server

利点

DHCP Server ペインで、FWSM を、内部インターフェイスのホストに対するダイナミック ホスト コントロール プロトコル（DHCP）サーバとして設定できます。IP アドレスの範囲をアドレス プールに設定すると、内部インターフェイスのホストが DHCP で IP アドレスを要求したとき、FWSM はこのプールのアドレスを割り当てます。

特記事項

- DNS、WINS、および最も低いセキュリティ レベルのインターフェイス（内部インターフェイス）の情報をこのペインで設定できます。他のインターフェイスに DHCP サーバを設定するには、ASDM のメイン ウィンドウから Configuration > Features > Properties > DHCP Services > DHCP Server を選択します。
- DHCP プールで使用できるアドレス数は 256 です。

フィールド

DHCP Server ペインには、Back、Next、Finish、Cancel、Help ボタン、および次の項目が表示されます。

- Enable DHCP on inside interface：このチェックボックスをクリックすると、FWSM の DHCP が起動します。
- DHCP アドレス プール
  - Starting IP Address：DHCP サーバ プール範囲の開始を入力します。一連の IP アドレスは最小から最大の順です。FWSM でサポートされる IP アドレス数は 256 です。
  - Ending IP Address：DHCP サーバ プール範囲の終了を入力します。一連の IP アドレスは最小から最大の順です。FWSM でサポートされる IP アドレス数は 256 です。
- DHCP パラメータ
  - DNS Server 1：DNS を使用する DNS サーバの IP アドレスを入力します。
  - WINS Server 1：DNS を使用する WINS（Windows インターネット ネーミング サービス）サーバの IP アドレスを入力します。
  - DNS Server 2：DNS を使用する代替 DNS サーバの IP アドレスを入力します。
  - WINS Server 2：DNS を使用する代替 WINS サーバの IP アドレスを入力します。
  - Domain Name：DNS を使用する DNS サーバのドメイン名を入力します。
  - Lease Length (seconds)：リース期間が終了するまでクライアントが割り当てられた IP アドレスを使用できる時間（秒単位）を入力します。デフォルト値は、3600 秒（1 時間）です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

この機能は、ASDM アプリケーションのメイン ウィンドウで利用できます。

Configuration > Properties > DHCP Services > DHCP Server

Address Translation (NAT/PAT)

利点

Address Translation (NAT/PAT) ペインでは、ネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）を FWSM に設定できます。

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。PAT を使用すると、複数の発信セッションが 1 つの IP アドレスから発信されているように見せることができます。PAT がイネーブルになっていると、FWSM は、各発信変換スロット用に PAT IP アドレスから一意のポート番号を選択します。この機能は、発信接続に十分な数の一意の IP アドレスを割り当てられない場合に役立ちます。ポート アドレスに指定した IP アドレスは、他のグローバル アドレス プールで使用できません。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 を使用するには、内部インターフェイス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。

特記事項

NAT を利用する場合、このペインで要求された IP アドレス範囲から FWSM の発信時に使用されるアドレス プールが作成されます。インターネット サービス プロバイダー（ISP）がインターネット登録のグローバル IP アドレスの範囲を指定している場合、その範囲をここに入力します。

PAT アドレス コンフィギュレーションを使用する場合、次の制限事項があります。

- 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 FWSM を通過するには、該当する検査エンジンをイネーブルにする必要があります。
- established コマンドでは動作しません。
- パッシブ FTP で使用する場合、**Inspect protocol ftp strict** コマンド文を **access-list** コマンド文と同時に実行して、FTP の発信トラフィックを許可します。
- セキュリティ レベルの高いインターフェイスの DNS サーバが、外部インターフェイスのルート ネーム サーバから更新を取得する必要がある場合、PAT を使用できません。

フィールド

Address Translation (NAT/PAT) ペインには、Back、Next、Finish、Cancel、Help ボタン、および次の項目が表示されます。

- Use Network Address Translation (NAT)：NAT と変換に使用される IP アドレス範囲をイネーブルにします。
  - Starting Global IP Address：変換に使用される IP アドレス範囲で最初の IP アドレスを入力します。
  - Ending Global IP Address：変換に使用される IP アドレス範囲で最後の IP アドレスを入力します。
  - Subnet Mask：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 をイネーブルにします。このオプションを選択した場合、次の中から 1 つ選択してください。
  - Use the IP address on the outside interface：FWSM では PAT で外部インターフェイスの IP アドレスを使用します。
  - Specify an IP address：PAT で使用される IP アドレスを指定します。

- Do not translate any addresses：選択すると、FWSM ではホストの IP アドレスが変換されません。コマンドライン インターフェイスに精通している場合は、**nat (inside) 0 0.0.0.0 0.0.0.0** コマンドと使用方法が同じです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

この機能は、ASDM アプリケーションのメイン ウィンドウで利用できます。

Configuration > NAT

Administrative Access

利点

Administrative Access ペインで、セキュリティ アプライアンス上の他のインターフェイスの IP アドレスを設定できます。コンフィギュレーションに使用できるインターフェイスは自動で一覧表示されます。このペインで、IP アドレス、インターフェイス名、セキュリティ レベルを設定すると、それぞれのインターフェイスが一意になります。

（注） 他の場所ですでに設定されたインターフェイスへの管理アクセスを設定できます。このペインでインターフェイスのアドレスや名前などを変更することはできません。

フィールド

Administrative Access ペインには、Back、Next、Finish、Cancel、Help ボタン、および次の項目が表示されます。

- Type：ホストまたはネットワークが FWSM のアクセス時に ASDM/HTTPS、SSH、または Telnet のどれを使用するか指定します。
- Interface：ホスト名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。
- Add：アクセス タイプとインターフェイスを選択して、ホスト / ネットワークの IP アドレスとネットマスクが、管理目的のみでこのインターフェイスに接続できるように指定します。
- Add：アクセス タイプとインターフェイスを選択して、ホスト / ネットワークの IP アドレスとネットマスクが、管理目的のみでこのインターフェイスに接続できるように指定します。
- Delete：選択した管理アクセス エントリを削除します。
- Enable HTTP server for HTTPS/ASDM access：オンにすると、HTTP サーバをイネーブルにします。HTTP サーバをディセーブルにすると、FWSM への ASDM/HTTPS アクセスができなくなります。
- Enable ASDM history metrics：オンにすると、各メトリックの履歴「バケット」を保持できます。Graph ペインが表示されていない場合でも、データを保存できます。このチェックボックスをオフにすると、履歴メトリックは破棄され、ディセーブルになります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

この機能は、ASDM アプリケーションのメイン ウィンドウで利用できます。

Configuration > Properties > Device Access > HTTPS/ASDM

Configuration > Properties > Device Access > Telnet

Configuration > Properties > Device Access > SSH

Configuration > Properties > History Metrics

Add/Edit Administrative Access Entry

利点

Add/Edit Administrative Access Entry ペインで、ホストを設定できます。

コマンドライン インターフェイス コンソール セッションにあらかじめ設定されている接続を、次の中から選択します。

- Telnet protocol：ネットワーク接続に Telnet プロトコルを適用します。
- ASDM/HTTPS protocol：Tools > Command Line Interface のネットワーク接続に HTTPS（SSL を使用した HTTP）プロトコルを適用します。

（注） ASDM は、常に HTTPS で FWSM と通信します。

- Secure Shell (SSH) protocol：ネットワーク接続にセキュア シェル（SSH）プロトコルを適用します。

FWSM を ASDM の CLI ツールから設定する前に、FWSM の技術マニュアルを確認することをお勧めします。また、「Password」、「Authentication」も参照してください。

ASDM の各画面で使用される CLI コマンドの詳細については、Command Line Interface Commands Used by ASDM Screens Help > About the FWSM を参照してください。ここでは最後のコンフィギュレーションの変更が表示されるので、特に便利です。

フィールド

Add Administrative Access Entry ペインおよび Edit Administrative Access Entry ペインには、OK、Cancel、Help ボタン、および次の項目が表示されます。

- Administrative Access Type：CLI コンソール セッションに適用する、あらかじめ設定された接続方法（ASDM/HTTP、SSH、Telnet）をドロップダウン メニューから選択します。
- 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：インターフェイスのサブネット マスクを、サブネット マスクの IP アドレスのリストから選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

この機能は、ASDM アプリケーションのメイン ウィンドウで利用できます。

Configuration > Properties > Device Access > HTTPS/ASDM

Configuration > Properties > Device Access > Telnet

Configuration > Properties > Device Access > SSH

Configuration > Properties > History Metrics

Startup Wizard Completed

利点

Startup Wizard Completed ペインで、行ったすべての設定を FWSM に送信できます。

- 設定を変更するには、**Back** をクリックします。
- **Finish** をクリックすると、ウィザードで作成した設定が FWSM に送信され、フラッシュ メモリに保存されます。
- Startup Wizard を ASDM の中で実行した場合、他のコンフィギュレーション変更と同様に、コンフィギュレーション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。

フィールド

Startup Wizard Completed ペインには、Back、Finish、Cancel、Help ボタンが表示されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

ここでは、次の項目について説明します。

セキュリティ レベルの概要

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 を割り当てる場合があります。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。

各レベルは、次の動作を制御します。

- 検査エンジン：一部の検査エンジンはセキュリティ レベルに依存します。セキュリティ レベルが等位のインターフェイスの場合、検査エンジンはどちらの方向のトラフィックにも適用されます。
  - NetBIOS 検査エンジン：発信接続のみに適用されます。
  - OraServ 検査エンジン：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、着信データ接続のみ FWSM を通過することが許可されます。
- フィルタリング：HTTP（S）フィルタリングおよび FTP フィルタリングは、発信接続（高位レベルから低位レベルへの接続）に対してのみ適用されます。

  等位のセキュリティ レベルのインターフェイスの場合、どちらの方向のトラフィックにもフィルタリングが適用できます。
- NAT 制御：NAT 制御をイネーブルにする場合、低位のセキュリティ インターフェイス（外部）上のホストにアクセスする高位のセキュリティ インターフェイス（内部）上のホストに NAT を設定する必要があります。

  NAT 制御がない場合、またはセキュリティが等位のインターフェイスの場合は、任意のインターフェイス間で NAT を使用するように選択することも、NAT を使用しないように選択することもできます。外部インターフェイスに対して NAT を設定すると、特殊なキーワードが必要になる場合があることに留意してください。
- **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。

  等位のセキュリティ レベルのインターフェイスでは、両方向に対して **established** コマンドが設定できます。

ルーテッド インターフェイスの設定

この項では、ルーテッド モード 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。

ルーテッド インターフェイスの追加または編集

シングルコンテキスト モードでは、FWSM に割り当てられた VLAN ID をスイッチで追加できます。このダイアログボックスでは、インターフェイスをコンテキストに追加することはできません。インターフェイスをコンテキストに割り当てるには、Security Contexts ペインを参照してください。

フェールオーバーにインターフェイスを使用する場合、この手順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。設定すると、フェールオーバー リンクにインターフェイスを使用できなくなります。他のパラメータは無視されます。フェールオーバー リンクまたはステート リンクに割り当てたインターフェイスは、Interfaces ペインで編集できなくなります。

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 > Interfaces ペインで、**Add** または **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 2　シングルコンテキスト モードでインターフェイスを追加する場合は、Interface メニューから VLAN ID を選択します。

ステップ 3　インターフェイスが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。これをディセーブルにするには、ボックスをオフにします。

ステップ 4　（オプション）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。

通過トラフィックは、管理専用インターフェイスでは受け入れられません。

ステップ 5　Interface Name フィールドに、インターフェイス名を 48 文字以内で入力します。

ステップ 6　Security level フィールドに、0（最下位）～ 100（最上位）のレベルを入力します。

詳細については、P.5-1 の「セキュリティ レベルの概要」を参照してください。

ステップ 7　IP Address フィールドと Subnet Mask フィールドに、IP アドレスとマスクを入力します。

ステップ 8　（オプション）Description フィールドに、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。1 行で入力し、改行はできません。マルチコンテキスト モードでは、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 リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。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 リンクに設定すると、入力した説明は固定の説明に上書きされます。

ステップ 9　（オプション）MTU を設定するには、**Advanced** タブをクリックし、MTU フィールドに 300 ～ 65,535 バイトの数値を入力します。

デフォルトは 1500 バイトです。

等位セキュリティ レベル間の通信のイネーブル化

デフォルトでは、セキュリティ レベルが等位のインターフェイス同士は通信できません。セキュリティ レベルが等位のインターフェイス間の通信を許可すると、101 以上の通信インターフェイスを設定できます。各インターフェイスで異なるセキュリティ レベルを使用して、同じセキュリティ レベルに複数のインターフェイスを割り当てない場合は、各レベル（0 ～ 100）に 1 つのインターフェイスしか設定できません。

（注）　NAT 制御をイネーブルにする場合、セキュリティ レベルが等しいインターフェイス間に NAT を設定する必要はありません。

セキュリティ レベルが等位のインターフェイス間の通信をイネーブルにした場合でも、異なるセキュリティ レベルのインターフェイスも通常どおりに設定できます。

また、同じインターフェイスに接続されたホスト間の通信をイネーブルにできます。

- 等位のセキュリティ レベルのインターフェイス同士による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た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（ルーテッド）

この項では、Add/Edit Interface ダイアログボックスのフィールドの説明を一覧表示します。次の項目を取り上げます。

- Add/Edit Interface > General タブ（ルーテッド）（P.5-5）
- Add/Edit Interface > Advanced タブ（ルーテッド）（P.5-6）

Interface ペイン（ルーテッド）

Interfaces ペインでは、インターフェイス パラメータを表示できます。また、等位のセキュリティ レベルのインターフェイス間または同じインターフェイスに接続されたホスト間の通信をイネーブルにできます。

フィールド

- Interface：インターフェイス ID を表示します。マルチモードでは、すべての割り当てられたインターフェイスが自動的に一覧表示されます。インターフェイスをコンテキストに割り当てるには、Security Contexts ペインを参照してください。

  フェールオーバーを使用する場合、Failover > Setup タブ で、フェールオーバー リンクに専用のインターフェイスを割り当てます。ステートフル フェールオーバーにオプションのインターフェイスも割り当てられます（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）。フェールオーバーでインターフェイスを確実に使用するには、Interfaces ペインでインターフェイス名を設定しないでください。IP アドレスなどの他の設定が無視されます。すべての関連するパラメータは Failover > Setup タブ で設定します。フェールオーバー リンクまたはステート リンクに割り当てたインターフェイスは、このペインで編集および削除ができなくなります。マルチモードでは、システム コンフィギュレーションにフェールオーバー インターフェイスを設定できます。
- Name：インターフェイスの名前を表示します。
- Enabled：インターフェイスがイネーブルかどうかを Yes または No で示します。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、そのインターフェイス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 アドレスを表示します。
- Subnet Mask：サブネット マスクを表示します。
- Management Only：インターフェイスに FWSM への、管理専用のトラフィックを許可する場合を示します。
- MTU：MTU を表示します。デフォルトでは、MTU は 1500 です。
- Description：説明を表示します。フェールオーバーまたはステート リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など変更不能の説明が表示されます。この説明は編集できません。
- Add：シングルモードでのみ、インターフェイスを追加します。P.5-2 の「ルーテッド インターフェイスの追加または編集」を参照してください。FWSM に割り当てられた VLAN ID をスイッチで追加できます。このペインでは、インターフェイスをコンテキストに追加することはできません。インターフェイスをコンテキストに割り当てるには、Security Contexts ペイン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。P.5-2 の「ルーテッド インターフェイスの追加または編集」を参照してください。フェールオーバーまたはステート リンクに割り当てたインターフェイス（Failover > Setup タブ を参照）は、このペインで編集できません。
- Delete：シングルモードでのみ、インターフェイスを削除します。コンテキストからインターフェイスを削除するには、Security Contexts ペインを参照してください。
- Enable traffic between two or more interfaces which are configured with same security levels：等位のセキュリティ 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。セキュリティ レベルが等しいインターフェイス間の通信をイネーブルにした場合でも、異なるセキュリティ レベルのインターフェイスも通常どおりに設定できます。デフォルトでは、等位のセキュリティ レベルのインターフェイス同士は通信できません。等位のセキュリティ レベルのインターフェイス間の通信を許可すると、101 以上の通信インターフェイスを設定できます。各インターフェイスで異なるセキュリティ レベルを使用して、同一のセキュリティ レベルに複数のインターフェイスを割り当てない場合、各レベル（0 ～ 100）に 1 つのインターフェイスしか設定できません。NAT 制御をイネーブルにする場合、等位のセキュリティ レベルのインターフェイス間に NAT を設定する必要はありません。

- 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ホスト間の通信をイネーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過[1]	シングル	コンテキスト	システム
•	—	•	•	—

1. 透過ファイアウォールの Interfaces ペインについては、透過ファイアウォールの透過インターフェイスおよびブリッジ グループの設定ペインを参照してください。

Add/Edit Interface > General タブ（ルーテッド）

フィールド

- Interface：VLAN ID を設定します。FWSM に割り当てられた VLAN ID をスイッチで設定できます。
- 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。さらに、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 FWSM 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。
- 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（最下位）～ 100（最上位）の範囲で設定します。詳細については、「セキュリティ レベルの概要」を参照してください。
- 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。
- Description：（オプション）240 文字以内で入力します。1 行で入力し、改行はできません。マルチコンテキスト モードでは、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 リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。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 リンクに設定すると、入力した説明は固定の説明に上書きされます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過[1]	シングル	コンテキスト	システム
•	—	•	•	—

1. 透過ファイアウォールの Add/Edit Interfaces ダイアログボックスについては、透過ファイアウォールのルーテッド インターフェイスの追加または編集ダイアログボックスを参照してください。

Add/Edit Interface > Advanced タブ（ルーテッド）

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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過[1]	シングル	コンテキスト	システム
•	—	•	•	—

1. 透過ファイアウォールの Add/Edit Interfaces ダイアログボックスについては、透過ファイアウォールのルーテッド インターフェイスの追加または編集ダイアログボックスを参照してください。

透過インターフェイスおよびブリッジ グループの設定

この項では、透過モード インターフェイスとブリッジ グルー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。

ブリッジ グループの追加または編集

透過ファイアウォールでは、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。インターフェイスの各ペアがブリッジ グループに属しています。このブリッジ グループに管理 IP アドレスを割り当てる必要があります。2 つのインターフェイスを持つブリッジ グループを最大 8 つ設定できます。各ブリッジ グループは別々のネットワークに接続します。ブリッジ グループのトラフィックは、他のブリッジ グループから隔離され、トラフィックは FWSM 内の他のブリッジ グループにルーティングされません。また、トラフィックは、外部ルータから FWSM 内の他のブリッジ グループにルーティングされる前に、FWSM から出る必要があります。

（注） FWSM は、セカンダリ ネットワークのトラフィックはサポートしません。管理 IP アドレスと同じネットワーク上のトラフィックだけがサポートされます。

セキュリティ コンテキストのオーバーヘッドを持たずに、セキュリティ コンテキストを最大限に使用したい場合は、複数のブリッジ グループを使用してもかまいません。ブリッジング機能はブリッジ グループごとに別々のものですが、他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、すべてのブリッジ グループは syslog サーバまたは AAA サーバのコンフィギュレーションを共有します。セキュリティ ポリシーを完全に分離するには、各コンテキストで単一ブリッジ グループを持つセキュリティ コンテキストを使用します。

（注） すべての透過インターフェイスはブリッジ グループに属している必要があります。

ブリッジ グループ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 > Interfaces > Bridge Groups タブで、**Add** または **Edit** をクリックします。

Add/Edit Bridge Group ダイアログボックスが表示されます。

ステップ 2　Bridge Group フィールドで、1 ～ 100 のブリッジ グループ ID を入力します。

ステップ 3　IP Address フィールドで、管理 IP アドレスを入力します。

透過ファイアウォールは、IP ルーティングに参加しません。FWSM で必要とされる唯一の IP コンフィギュレーションは、各ブリッジ グループの管理 IP アドレスの設定です。このアドレスは、システム メッセージまたは AAA サーバとの通信など、FWSM 上で発信されるトラフィックの送信元アドレスとして FWSM が使用するために必要です。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。

FWSM は、セカンダリ ネットワークのトラフィックはサポートしません。管理 IP アドレスと同じネットワーク上のトラフィックだけがサポートされます。

ステップ 4　Subnet Mask フィールドで、サブネット マスクを入力するか、メニューから選択します。

単一ホスト アドレス（/32 つまり 255.255.255.255）を透過ファイアウォールに割り当てないでください。また、/30 サブネット（255.255.255.252）などのように、ホスト アドレスが 3 つ（アップストリーム ルータ、ダウンストリーム ルータ、透過ファイアウォール用に 1 つずつ）に満たないサブネットも使用しないでください。FWSM は、サブネットの最初と最後のアドレスに送受信される ARP パケットをすべてドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリーム ルータへの予約アドレスを割り当てた場合、FWSM は、ダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。

ステップ 5　（オプション）Description フィールドに、ブリッジ グループの説明を入力します。

透過インターフェイスの追加または編集

シングルモードでは、FWSM に割り当てられた VLAN ID をスイッチで追加できます。このダイアログボックスでは、インターフェイスをコンテキストに追加することはできません。インターフェイスをコンテキストに割り当てるには、Security Contexts ペインを参照してください。

フェールオーバーにインターフェイスを使用したい場合、この手順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。設定すると、フェールオーバー リンクにインターフェイスを使用できなくなります。他のパラメータは無視されます。

フェールオーバー リンクまたはステート リンクに割り当てたインターフェイスは、Interfaces ペインで編集できなくなります。

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 > Interfaces ペインで、**Add** または **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 2　シングルコンテキスト モードでインターフェイスを追加する場合は、Interface メニューから VLAN ID を選択します。

ステップ 3　インターフェイスをブリッジ グループに割り当てるには、ブリッジ グループ ID を Bridge Group メニューから選択します。

ブリッジ グループを表示または追加するには、P.5-7 の「ブリッジ グループの追加または編集」を参照してください。

ステップ 4　インターフェイスが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。これをディセーブルにするには、ボックスをオフにします。

ステップ 5　Interface Name フィールドに、インターフェイス名を 48 文字以内で入力します。

ステップ 6　Security level フィールドに、0（最下位）～ 100（最上位）のレベルを入力します。

詳細については、P.5-1 の「セキュリティ レベルの概要」を参照してください。

ステップ 7　IP Address フィールドと Subnet Mask フィールドに、IP アドレスとマスクを入力します。

ステップ 8　（オプション）Description フィールドに、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。1 行で入力し、改行はできません。マルチコンテキスト モードでは、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 リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。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 リンクに設定すると、入力した説明は固定の説明に上書きされます。

ステップ 9　（オプション）MTU を設定するには、**Advanced** タブをクリックし、MTU フィールドに 300 ～ 65,535 バイトの数値を入力します。

デフォルトは 1500 バイトです。

等位セキュリティ レベル間の通信のイネーブル化

デフォルトでは、等位のセキュリティ レベルのインターフェイス同士は通信できません。

（注）　NAT 制御をイネーブルにする場合、等位のセキュリティ レベルのインターフェイス間に NAT を設定する必要はありません。

セキュリティ レベルが等位のインターフェイス間の通信をイネーブルにした場合でも、異なるセキュリティ レベルのインターフェイスも通常どおりに設定できます。

等位のセキュリティ レベルのインターフェイス同士による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。

Interface フィールドの説明（透過）

この項では、Add/Edit Interface ダイアログボックスのフィールドの説明を一覧表示します。次の項目を取り上げます。

- Bridge Groups タブ（P.5-10）
- Add/Edit Bridge Group（P.5-10）
- Transparent Interfaces タブ（P.5-11）
- Add/Edit Interface > General タブ（透過）（P.5-12）
- Add/Edit Interface > Advanced タブ（透過）（P.5-13）

Bridge Groups タブ

フィールド

- Bridge Group：ブリッジ グループ ID を表示します。
- IP Address：ブリッジ グループの管理 IP アドレスを表示します。透過ファイアウォールは、IP ルーティングに参加しません。FWSM で必要とされる唯一の IP コンフィギュレーションは、各ブリッジ グループの管理 IP アドレスの設定です。このアドレスは、システム メッセージまたは AAA サーバとの通信など、FWSM 上で発信されるトラフィックの送信元アドレスとして FWSM が使用するために必要です。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。
- Network Mask：IP アドレスのサブネット マスクを示します。
- Description：ブリッジ グループの説明を示します。
- Add：ブリッジ グループを追加します。
- Edit：ブリッジ グループを編集します。
- Delete：ブリッジ グループを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Bridge Group

Add/Edit Bridge Group ダイアログボックスを使用して、ブリッジ グループの管理 IP アドレスの設定など、ブリッジ グループの追加または編集ができます。ブリッジ グループの詳細については、「ブリッジ グループの追加または編集」を参照してください。

フィールド

- Bridge Group：ブリッジ グループ ID を 1 ～ 100 の整数で設定します。
- IP Address：ブリッジ グループの管理 IP アドレスを表示します。透過ファイアウォールは、IP ルーティングに参加しません。FWSM で必要とされる唯一の IP コンフィギュレーションは、各ブリッジ グループの管理 IP アドレスの設定です。このアドレスは、システム メッセージまたは AAA サーバとの通信など、FWSM 上で発信されるトラフィックの送信元アドレスとして FWSM が使用するために必要です。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。FWSM は、セカンダリ ネットワークのトラフィックはサポートしません。管理 IP アドレスと同じネットワーク上のトラフィックだけがサポートされます。
- Subnet Mask：管理 IP アドレスのサブネット マスクを設定します。単一ホスト アドレス（/32 つまり 255.255.255.255）を透過ファイアウォールに割り当てないでください。また、/30 サブネット（255.255.255.252）などのように、ホスト アドレスが 3 つ（アップストリーム ルータ、ダウンストリーム ルータ、透過ファイアウォール用に 1 つずつ）に満たないサブネットも使用しないでください。FWSM は、サブネットの最初と最後のアドレスに送受信される ARP パケットをすべてドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリーム ルータへの予約アドレスを割り当てた場合、FWSM は、ダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。
- Description：ブリッジ グループの説明を追加します。

モード

次の表に、この機能を使用できるモードを示します。

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

Transparent Interfaces タブ

Transparent Interfaces タブには、インターフェイス パラメータを表示できます。また、等位のセキュリティ レベルのインターフェイス間または同じインターフェイスに接続されたホスト間の通信をイネーブルにできます。

フィールド

- Interface：インターフェイス ID を表示します。マルチモードでは、すべての割り当てられたインターフェイスが自動的に一覧表示されます。インターフェイスをコンテキストに割り当てるには、Security Contexts ペインを参照してください。

  フェールオーバーを使用する場合、Failover > Setup タブ で、フェールオーバー リンクに専用のインターフェイスを割り当てます。ステートフル フェールオーバーにオプションのインターフェイスも割り当てられます（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）。フェールオーバーでインターフェイスを確実に使用するには、Interfaces ペインでインターフェイス名を設定しないでください。他の設定が無視されます。すべての関連するパラメータは Failover > Setup タブで設定します。フェールオーバー リンクまたはステート リンクに割り当てたインターフェイスは、このペインで編集および削除ができなくなります。
- Name：インターフェイスの名前を表示します。
- Enabled：インターフェイスがイネーブルかどうかを Yes または No で示します。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、そのインターフェイス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。
- Bridge Group：インターフェイスが割り当てられたブリッジ グループを示します。詳細については、「ブリッジ グループの追加または編集」を参照してください。
- MTU：MTU を表示します。デフォルトでは、MTU は 1500 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 リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。この説明は編集できません。
- Add：シングルモードでのみ、インターフェイスを追加します。FWSM に割り当てられた VLAN ID をスイッチで追加できます。このペインでは、インターフェイスをコンテキストに追加することはできません。インターフェイスをコンテキストに割り当てるには、Security Contexts ペイン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。フェールオーバーまたはステート リンクに割り当てたインターフェイス（Failover > Setup タブ を参照）は、このペインで編集できません。
- Delete：シングルモードでのみ、インターフェイスを削除します。コンテキストからインターフェイスを削除するには、Security Contexts ペインを参照してください。
- Enable traffic between two or more interfaces which are configured with same security levels：等位のセキュリティ 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。セキュリティ レベルが等位のインターフェイス間の通信をイネーブルにした場合でも、異なるセキュリティ レベルのインターフェイスも通常どおりに設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド[1]	透過	シングル	コンテキスト	システム
—	•	•	•	—

1. ルーテッド ファイアウォールの Interfaces ペインについては、ルーテッド ファイアウォールの Interface ペイン（ルーテッド）を参照してください。

Add/Edit Interface > General タブ（透過）

フィールド

- Interface：VLAN ID を設定します。FWSM に割り当てられた VLAN ID をスイッチで設定できます。
- 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。デフォルトでは、すべてのインターフェイスは、イネーブルになっています。
- 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（最下位）～ 100（最上位）の範囲で設定します。多くのセキュリティ機能は、それぞれのインターフェイスの相対セキュリティ レベルに影響されます。
- Bridge Group：このインターフェイスのブリッジ グループを設定します。リストから番号を選択するか、1 ～ 100 の整数を入力します。1 つのブリッジ グループに対して 2 つのインターフェイスが割り当てられます。同じインターフェイスを複数のブリッジ グループに割り当てることはできません。詳細については、P.5-7 の「ブリッジ グループの追加または編集」を参照してください。
- Description：（オプション）240 文字以内で入力します。1 行で入力し、改行はできません。マルチコンテキスト モードでは、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 リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。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 リンクに設定すると、入力した説明は固定の説明に上書きされます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド[1]	透過	シングル	コンテキスト	システム
—	•	•	•	—

1. ルーテッド ファイアウォールの Add/Edit Interfaces ダイアログボックスについては、ルーテッド ファイアウォールの「Interface フィールドの説明（ルーテッド）」を参照してください。

Add/Edit Interface > Advanced タブ（透過）

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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド[1]	透過	シングル	コンテキスト	システム
—	•	•	•	—

1. ルーテッド ファイアウォールの Add/Edit Interfaces ダイアログボックスについては、ルーテッド ファイアウォールの「Interface フィールドの説明（ルーテッド）」を参照してください。

CHAPTER 6

グローバル オブジェクトの追加

Objects ペインでは、FWSM 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。

この章には、次の項があります。

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を使用する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 オブジェクトに、ホストおよびネットワークの IP アドレスをあらかじめ定義しておくと、以後の設定がスムーズになります。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だけで、手動で入力する代わりに事前定義済みのアドレスをクリックすることができます。さらに、オブジェクトの定義を変更すると、そのオブジェクトを使用するルールでその変更が自動的に継承されます。

ネットワーク オブジェクトを手動で追加することもできますが、アクセス ルールや AAA ルールなどの既存のコンフィギュレーションから ASDM で自動的にオブジェクトを作成することもできます。これらの取得済みオブジェクトのいずれかを編集すると、このオブジェクトを使用するルールを後で削除しても、そのオブジェクトは残っています。それ以外の場合、取得済みオブジェクトを更新すると、現在のコンフィギュレーションのみが反映されます。

複数のホストやネットワークをグループ化しておくと、アドレス グループにルールを簡単に適用できます。複数のネットワーク オブジェクト グループをネストして「グループのグループ」にすると、単一のグループとして参照できます。

ルールの設定時に、ASDM ウィンドウの右側の Addresses サイド ペインにも使用可能なネットワーク オブジェクトやネットワーク オブジェクト グループが表示されます。このサイド ペインから直接オブジェクトを追加、編集、削除できます。また、サイド 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追加するネットワーク オブジェクトおよびグループをドラッグすることもできます。

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 > Global 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を追加するか、またはオブジェクトを選択してから **Edit** をクリックします。

ルールを追加する場合、ルール ウィンドウの Addresses サイド ペインからもネットワーク オブジェクトを追加または編集できます。

リストにある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、**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（*）と疑問符（?）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：（オプション）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。64 文字以内で指定します。
- IP Address：ホストまたはネットワークの IP アドレス。
- Netmask：IP アドレスのサブネット マスク。
- Description：（オプション）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るようになります。編集済みオブジェクトの場合、このオブジェクトを使用するルールで変更が自動的に継承されます。

（注）　使用中のネットワーク オブジェクトを削除することはできません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > Global 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、またはオブジェクト グループを選択してから **Edit** をクリックします。

ルールを追加する場合、ルール ウィンドウの Addresses サイド ペインからもネットワーク オブジェクト グループを追加または編集できます。

リストにある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、**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（*）と疑問符（?）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 フィールドに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。64 文字以内で指定します。

ステップ 3　（オプション）Description フィールドに説明を最大 200 文字で入力します。

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（ネストされたグループを許可する）、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右クリックします。

  また、オブジェクトを選択してから **Add** ボタンをクリックすることもできます。オブジェクトまたはグループは右側の 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 領域に値を入力して **Add** をクリックします。

  オブジェクトまたはグループは右側の Members in Group ペインに追加されます。アドレスは、ネットワーク オブジェクトの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、または **Remove** ボタンをクリックします。

ステップ 5　メンバー オブジェクトをすべて追加したら、**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るようになります。編集済みオブジェクト グループの場合、このグループを使用するルールで変更が自動的に継承されます。

（注）　使用中のネットワーク オブジェクト グループを削除することはできません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

ルールを作成すると、IP アドレスを手動で入力するか、あるいはネットワーク オブジェクトまたはグループを参照してルールで使用できます。

（注）　アクセス ルールの場合のみ、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。

ネットワーク オブジェクトまたはグループをルールで使用するには、次の手順を実行します。

ステップ 1　ルールのダイアログボックスで、送信元または宛先アドレスのフィールドの隣にある参照ボタン **...** 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するか、あるいは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ます。

リストにある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、**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(*)と疑問符(?)を使用できます。

- 新しいネットワーク オブジェクトの追加するには、P.6-2 の「ネットワーク オブジェクトの設定」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には、P.6-3 の「ネットワーク オブジェクト グループの設定」を参照してください。

新しいオブジェクトを追加するか、または既存のオブジェクトをダブルクリックすると、それらのオブジェクトは 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、このフィールドで複数のオブジェクトまたはグループをカンマ区切りで追加できます。

ステップ 3　**OK** をクリックします。

ルールのダイアログボックスに戻ります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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するルールを表示するには、Configuration > Global Objects > Network Objects/Group ペインで、拡大鏡の Find アイコンをクリックします。

Usages ダイアログボックスに、ネットワーク オブジェクトまたはグループを使用中のすべてのルールが表示されます。このダイアログボックスには、そのオブジェクトを含むネットワーク オブジェクト グループも表示されます。

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。次の項目を取り上げます。

Service Groups

Service Groups ペインで、指定したグループに複数のサービスを関連付けます。1 つのグループでプロトコルとサービスの種類を指定することもできますが、次の種類ごとにサービス グループを作成することもできます。

- 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 グループをネストして「グループのグループ」にすると、単一のグループとして参照できます。

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、ほとんど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サイド ペインにもサービス グループなど使用可能なグローバル オブジェクトが表示されます。このサイド 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。ドロップダウン リストからサービス グループの種類を選択して追加するか、または Service Group から複数の種類を選択します。
- 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。アクセス ルールで使用しているサービス グループは、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 グループを空にすることはできません。
- Find：フィルタして名前が一致するものだけを表示します。**Find** をクリックすると、Filter フィールドが開きます。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。
  - Filter フィールド：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（*）と疑問符（?）を使用できます。
  - Filter：フィルタリングを実行します。
  - 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 グループの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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、サービスをサービス グループに割り当てます。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。重複するオブジェクト グループ名は指定できません。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アイテムを識別します。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 タイプによって異なります。定義済みのサービス グループが含まれます。
  - Predefined：定義済みのポート、タイプ、またはプロトコルが一覧表示されます。
- Create new member：新しいサービス グループのメンバーを作成します。
  - Service Type：新しいサービス グループ メンバーのサービス タイプを選択します。サービス タイプには TCP、UDP、TCP-UDP、ICMP、およびプロトコルがあります。
  - Destination Port/Range：新しい TCP、UDP、または TCP-UDP サービス グループ メンバーの宛先ポートまたは範囲を入力します。
  - Source Port/Range：新しい TCP、UDP、または TCP-UDP サービス グループ メンバーの送信元ポートまたは範囲を入力します。
  - ICMP Type：新しい ICMP サービス グループ メンバーの ICMP タイプを入力します。
  - Protocol：新しいプロトコルのサービス グループ メンバーのプロトコルを入力します。
- 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、サービス グループを選択します。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の場合、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:フィルタして名前が一致するものだけを表示します。**Find** をクリックすると、Filter フィールドが開きます。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。
  - Filter フィールド：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（*）と疑問符（?）を使用できます。
  - Filter：フィルタリングを実行します。
  - 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

次の表に、この機能を使用できるモードを示します。

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

検査マップの設定

ここでは、次の項目について説明します。

検査マップの概要

検査マップでは、専用のプロトコル検査エンジンの検査マップを作成できます。検査マップを利用して、プロトコル検査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、検査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 オプションから検査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、FWSM 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。

FWSM のステートフル アプリケーション検査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、専用の検査エンジンでそのような場合に対応します。特別なアプリケーション検査エンジンを必要とするのは、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か、またはダイナミックに割り当てられたポートでセカンダリ チャネルを開くアプリケーションです。

アプリケーション検査エンジンは 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 NAT では、それらの埋め込まれたアドレスを変換したり、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検査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。ウェルノウン ポート上の初期セッションは、ダイナミックに割り当てられたポート番号をネゴシエートするために使用されます。アプリケーション検査エンジンは、この初期セッションを監視し、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 アプリケーション検査により、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。FWSM 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。

表 6-1 に、検査マップ機能でサポートされているプロトコルの概要を示します。

表 6-1　検査マップ

DCERPC	DCERPC オプションで、DCERPC 検査マップを作成、表示、管理します。DCERPC は、Microsoft のクライアント / 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。
FTP	FTP オプションで、FTP 検査マップを作成、表示、管理します。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、セキュリティ アプライアンスを通過したり FTP サーバに到達したりする FTP PUT などの、特定の FTP プロトコル方式をブロックできます。
GTP	GTP オプションで、GTP 検査マップを作成、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、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.225	H.225 オプションで、H.225 検査マップを作成、表示、管理します。H.225 は、H.323 接続でコントロールおよびセットアップの呼び出しに使用するプロトコルです。
HTTP	HTTP オプションで、HTTP 検査マップを作成、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。
MGCP	MGCP オプションで、MGCP 検査マップを作成、表示、管理します。MGCP は、VoIP デバイスと MGCP コール エージェント間の接続を管理するためのプロトコルです。
SIP	SIP オプションで、SIP 検査マップを作成、表示、管理します。SIP は、VoIP 電話などのエンドポイントと SIP ゲートウェイまたはプロキシ サーバの間で VoIP 接続を確立するためのプロトコルです。
SNMP	SNMP オプションで、SNMP の検査マップを作成、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

DCERPC ペインで、DCERPC アプリケーションの事前に設定された検査マップを表示します。DCERPC マップでは、DCERPC アプリケーション検査のデフォルト設定値を変更できます。

DCERPC は、Microsoft のクライアント / 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。

DCERPC 検査マップは、TCP のウェルノウン 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。サーバの埋め込まれた 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番号で複数の接続を確立する可能性があるので、ピンホールを複数使用でき、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

- Map　Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Pinhole Timeout：DECRPC ピンホールのタイムアウト。デフォルト値は 2 分です。
- EPM Service：バインディング中にエンドポイント マッパー サービスの適用を強制するかどうかを一覧表示します。
- EPM 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するかどうかを一覧表示します。
- Add：Add DCERPC 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検査マップを定義できます。
- Edit：Edit DCERPC ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Map

Add/Edit DCERPC Map ダイアログボックスで、DCERPC のアプリケーション検査を制御する DCERPC マップを新規作成できます。

フィールド

- Name：DCERPC マップを追加する場合、DCERPC マップの名前を入力します。DCERPC マップを編集する場合、すでに設定されている DCERPC マップの名前が表示されます。
- 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。0:0:1 ～ 1193:0:0 の範囲で指定します。デフォルト値は 2 分です。
- Enforce endpoint-mapper service：バインディング中はエンドポイント マッパー サービスの適用を強制します。
- 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 ルックアップの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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

FTP ペインで、FTP アプリケーションの事前に設定された検査マップを表示します。FTP マップでは、FTP アプリケーション検査のデフォルト設定値を変更できます。FTP ペインでは、新しい FTP マップを追加するか、または既存のマップを変更または削除できます。

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検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Mask reply to system command：クライアントが、クライアントからの FTP 要求を含む FTP システム コマンドへのサーバ応答を表示できないようにします。
- Denied Request Commands：特定のアプリケーション検査マップで禁止されている FTP コマンドを一覧表示します。これらのコマンドを含む FTP 要求を受信すると、要求がドロップされます。
- Add：Add FTP 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検査マップを定義できます。
- Edit：Edit FTP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Map ダイアログボックスで、FTP アプリケーションの検査マップを定義します。FTP マップでは、FTP アプリケーション検査のデフォルト設定値を変更できます。

フィールド

- FTP Map Name：アプリケーション検査マップの名前を定義します。
- Mask reply to system command：クライアントが、クライアントからの FTP 要求を含む FTP システム コマンドへのサーバ応答を表示できないようにします。
- Denied Request Commands
  - APPE：ファイルに追加するコマンドを禁止します。
  - 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を禁止します。
  - DELE：ファイルを削除するコマンドを禁止します。
  - GET：ファイルを取得するコマンドを禁止します。
  - HELP：ヘルプ情報を提供するコマンドを禁止します。
  - MKD：ディレクトリを作成するコマンドを禁止します。
  - PUT：ファイルを送信するコマンドを禁止します。
  - RMD：ディレクトリを削除するコマンドを禁止します。
  - RNFR：変更元ファイル名を指定するコマンドを禁止します。
  - RNTO：変更先ファイル名を指定するコマンドを禁止します。

— SITE：サーバ システム固有のコマンドを禁止します。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を保存するコマンドを禁止します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

GTP ペインで、GTP アプリケーションの事前に設定された検査マップを表示します。GTP マップでは、GTP アプリケーション検査のデフォルト設定値を変更できます。GTP ペインでは、新しい GTP マップを追加するか、または既存のマップを変更または削除できます。

（注） GTP 検査は、特別なライセンスがなければ使用できません。

フィールド

- GTP Map Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Description：GTP マップごとに説明をテキストで表示します。
- Fields：選択した GTP マップでイネーブルにするフィールドを個々に表示します。
- Values：選択した GTP マップでイネーブルにするフィールドごとの値を表示します。
- Add：Add GTP 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検査マップを定義できます。
- Edit：Edit GTP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > IMSI Prefix タブ

IMSI Prefix タブで、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します。

フィールド

- **GTP Map Name**：アプリケーション検査マップの名前を識別します。
- **Description**：アプリケーション検査マップの説明をテキストで入力します。
- **IMSI Prefix to Allow**
  - **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。1 桁または 2 桁の値を指定すると、先頭に 0 が付加されて 3 桁になります。
  - **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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > Bounds タブ

Bounds タブでは、GTP アプリケーション検査がイネーブルの場合、メッセージの長さ、キュー サイズ、トンネル数の許容範囲を定義できます。

フィールド

- GTP Map Name：アプリケーション検査マップの名前を識別します。
- Description：アプリケーション検査マップの説明をテキストで入力します。
- Message Length：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：UDP ペイロードの最小バイト数を指定します。1 ～ 65536 の範囲の値を指定できます。
- Maximum：UDP ペイロードの最大バイト数を指定します。1 ～ 65536 の範囲の値を指定できます。
- Queue Size：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。最大要求キュー サイズのデフォルト値は 200 です。
- Queue Size：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 Tunnels Count：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。
- Maximum Tunnel Count：許容するトンネル数の最大値を指定します。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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > Timeouts タブ

Timeouts タブでは、GTP アプリケーション検査がイネーブルの場合の、GSN、PDP コンテキスト、要求キュー、シグナリング、および GTP トンネルで許可される非アクティブ期間の最大値を定義できます。

フィールド

- GTP Map Name：アプリケーション検査マップの名前を識別します。
- Description：アプリケーション検査マップの説明をテキストで入力します。
- GSN：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。
- GSN：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：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。
- PDP Context：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。
- Request Queue：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。
- Signaling：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。
- Tunnel：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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > APN タブ

APN タブでは、GTP アプリケーション検査がイネーブルの場合にドロップするアクセスポイントを定義できます。

フィールド

- GTP Map Name：アプリケーション検査マップの名前を識別します。
- Description：アプリケーション検査マップの説明をテキストで入力します。
- Access Points to Drop
  - Name：ドロップするアクセスポイントの名前を指定します。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。
  - Add：指定した APN を Access Point Name テーブルに追加します。
  - Delete：選択した APN を Access Point Name テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > Action タブ

Action タブでは、GTP アプリケーション検査がイネーブルの場合に実行する特定のアクションを定義できます。

フィールド

- GTP Map Name：アプリケーション検査マップの名前を識別します。
- Description：アプリケーション検査マップの説明をテキストで入力します。
- Permit packets with errors：無効なパケットまたは検査時にエラーが見つかったパケットを、ドロップしないで FWSM から送信します。デフォルトでは、無効なパケットや解析中に失敗したパケットはドロップされます。
- GTP Versions to Drop
  - GTP Version：ドロップするメッセージの GTP バージョンを指定します。有効な指定範囲は 0 ～ 255 です。0 は Version 0、1 は Version 1 を示します。GTP の Version 0 はポート 3386 を使用し、Version 1 はポート 2123 を使用します。デフォルトでは、すべての GTP バージョンが対象です。
  - Add：指定した GTP バージョンを Version テーブルに追加します。
  - Delete：選択した GTP バージョンを Version テーブルから削除します。
- Message IDs to Drop
  - Message ID：ドロップ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 が対象です。
  - Add：指定した Message ID を Message ID テーブルに追加します。
  - Delete：選択した Message ID を Message ID テーブルから削除します。

- Permit Response：GSN プールにある GSN が SGSN 要求に応答して、GGSN のロードバランシングを達成できるようにします。無効な GTP パケットや解析中に失敗したパケットはドロップされます。
  - Object Groups to Add：別のオブジェクト グループから応答を受信できるオブジェクト グループを指定します。

    From Object Group：応答を送信するオブジェクト グループの名前を指定します。

    Browse：定義済みオブジェクト グループの一覧を参照します。

    To Object Group：要求を送信するオブジェクト グループの名前を指定します。

    Browse：定義済みオブジェクト グループの一覧を参照します。
  - Add：指定した Object Group を Object Group テーブルに追加します。
  - Delete：選択した Object Group を Object Group テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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.225

H.225 ペインで、事前に設定された H.225 アプリケーションの検査マップ（H.225 マップ）を表示します。H.225 ペインでは、新しい H.225 マップを追加するか、または既存のマップを変更または削除できます。

H.225 マップでは、Cisco CallManager が HSI から取得した情報に基づいて H.323 エンドポイント間の接続を確立しようとすると、FWSM がポート固有のダイナミック ピンホールを開いて H.323 接続をイネーブルにすることができます。H.225 マップは HSI とその関連エンドポイントに関する情報を提供します。この情報は、FWSM で保護されているネットワークのセキュリティを侵害することなくこのような接続を確立するために必要です。

フィールド

- Name：すでに設定されている H.225 アプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- HSI Group ID：H.225 マップに関連付けられる HSI のグループ ID。

  HSI グループには、HSI とその関連エンドポイントが含まれています。H.225 マップ内の HSI グループの最大数は 5 です。
- IP Address：H.225 マップに関連付けられる IP アドレス。
- Endpoints：H.225 マップに関連付けられるエンドポイント。
- Add：Add H.225 Map 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検査マップを定義できます。
- Edit：Edit H.225 Map ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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.225 Map

Add/Edit H.225 Map ダイアログボックスで、H.225 のアプリケーション検査を制御する H.225 マップを新規作成できます。

Cisco CallManager が HSI から取得した情報に基づいて H.323 エンドポイント間の接続を確立しようとしたときに、FWSM がポート固有の中継ピンホールを開いて H.323 接続をイネーブルにできるようにするには、H.225 マップが必要です。H.225 マップは HSI とその関連エンドポイントに関する情報を提供します。この情報は、FWSM で保護されているネットワークのセキュリティを侵害することなくこのような接続を確立するために必要です。

フィールド

- HSI Group ID：H.225 マップに関連付けられる HSI のグループ ID。

  HSI グループには、HSI とその関連エンドポイントが含まれています。H.225 マップ内の HSI グループの最大数は 5 です。
- IP Address：H.225 マップに関連付けられる IP アドレス。
- Endpoints：H.225 マップに関連付けられるエンドポイント。

  HSI に関連付けることができるエンドポイントの最大数は 10 です。
- Add：Add HSI Group ダイアログボックスが表示され、新規の HSI グループを定義できます。
- Edit：Edit HSI Group ダイアログボックスが表示され、HSI Group テーブルで選択した HSI グループを修正できます
- Delete：HSI Group テーブルで選択した HSI グループを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、Cisco CallManager が HSI から取得した情報に基づいて H.323 エンドポイント間の接続を確立しようとしたときに、H.323 接続をイネーブルにするための HSI グループを新規作成できます。

フィールド

- Group ID：H.225 マップに関連付けられる HSI のグループ ID。

  HSI グループには、HSI とその関連エンドポイントが含まれています。H.225 マップ内の HSI グループの最大数は 5 です。
- IP Address：HSI グループに関連付けられる IP アドレス。
- Endpoints：HSI グループ内のエンドポイントの最大数は 10 です。
  - IP Address：エンドポイントの IP アドレス。
  - Interface：エンドポイントに接続されるインターフェイス。
  - Add：HSI グループに関連付けられるエンドポイントを追加します。
  - Delete：エンドポイント テーブルで選択したエンドポイントを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

HTTP ペインで、HTTP アプリケーションの事前に設定された検査マップを表示します。HTTP マップでは、HTTP アプリケーション検査のデフォルト設定値を変更できます。HTTP ペインでは、新しい HTTP マップを追加するか、または既存のマップを変更または削除できます。

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検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Checks Enabled：選択した HTTP マップでイネーブルにする検証およびチェックを識別します。
- Add：Add HTTP 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検査マップを定義できます。
- Edit：Edit HTTP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。
- Field：HTTP アプリケーション検査でサポートされる検査の種類を名前で一覧表示します。
- Enabled：特定の種類の検査がイネーブルかどうかを識別します。
- Value：RFC Compliance フィールドと Content Type フィールドがイネーブルの場合、これらのフィールドの値を表示します。
- Action：特定の種類のアプリケーション検査に応じて実行するアクションを識別します。
- Generate Syslog：特定の種類のアプリケーション検査に応じてシステム ログのエントリを生成するかどうかを指定します。
- Edit：Edit HTTP ダイアログボックスが表示され、選択したフィールドを修正できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > General タブ

General タブでは、コンテンツ タイプの検査をイネーブルにするために、準拠していない HTTP 要求を受信した場合に実行するアクションを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- Description：アプリケーション検査マップの説明をテキストで入力します。
- RFC Compliance
  - Action：FWSM が RFC 2616 に準拠しないトラフィックを受信した場合に実行するアクションを指定します。RFC 2616 では、許可される HTTP 方式とサポートされる拡張方式が定義されています。次のアクションを実行できます。

    Allow Packet：パケットが準拠していない方式を使用していても、FWSM はそのパケットを通過させます。

    Drop Packet：FWSM は準拠していない方式を使用するパケットを破棄します。

    Reset Connection：FWSM が準拠していない方式を使用するパケットを受信すると、TCP 接続をリセットします。
  - Generate Syslog：FWSM が準拠していない方式を使用するパケットを受信すると、システム ログ メッセージを生成します。
- コンテンツ タイプの検証
  - Verify Content-type field belongs to the supported internal content-type：HTTP 応答内のコンテンツ タイプのフィールドと、サポートされるコンテンツ タイプの事前設定リストの比較に基づいて、コンテンツ検証をイネーブルにします。イネーブルの場合、FWSM は HTML メッセージの本文とコンテンツ タイプが一致するかどうかも検証します。要求で受信したタイプが応答で送信したコンテンツ タイプと一致するかどうかを検証します。サポートされるコンテンツ タイプは次のとおりです。

audio/* |	audio/basic |	application/x-msn-messenger
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-java-xm	application/x-gzip
image |	image/cgf |	application/zip
image/jpeg |	image/png |	image/gif |
image/x-3ds |	image/x-bitmap |	image/tiff |
image/x-portable-bitmap |	image/x-portable-greymap |	image/x-niff |
text/* |	text/css	image/x-xpm |
text/plain |	text/richtext |	text/html |
text/xmcd	text/xml	text/sgml

video/-flc	video/mpeg	video/*
video/sgi	video/x-avi	video/quicktime
video/x-mng	video/x-msvideo	video/x-fli

- Verify Content-type field for response matches the Accept field of request：HTTP 応答内のコンテンツ タイプのフィールドと、HTTP 要求内の Accept フィールドで指定されているタイプの比較に基づいて、コンテンツ検証をイネーブルにします。
- Action：コンテンツ検証がイネーブルの場合に FWSM が実行するアクションを指定します。次のアクションを実行できます。

  Allow Packet：コンテンツ検証に失敗した場合でも、FWSM は HTTP 要求を許可します。

  Drop Packet：FWSM がコンテンツ検証に失敗したパケットを破棄します。

  Reset Connection：FWSM がコンテンツ検証に失敗したパケットを受信すると、TCP 接続をリセットします。
- Generate Syslog：FWSM がコンテンツ検証に失敗したパケットを受信すると、システム ログ メッセージを生成します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > Entity Length タブ

Entity Length タブでは、URI、HTTP ヘッダー、および HTTP 本文で許可される長さを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- URI の最大長
  - Inspect URI Length：FWSM が HTTP 要求の URI 長を検査します。
  - Maximum bytes：HTTP 要求で URI 長に許可される最大バイト数を指定します。許容範囲は 1 ～ 65535 です。
  - Action：URL の長さの検査に失敗した場合に FWSM が実行するアクションを指定します。次のアクションを実行できます。

    Allow Packet：HTTP 要求に許可されている最大長を超える URI が含まれていても、FWSM はその HTTP 要求を許可します。

    Drop Packet：HTTP 要求に許可されている最大長を超える URI が含まれている場合、FWSM はその HTTP 要求をドロップします。

    Reset Connection：許可されている最大長を超える URI が含まれている HTTP 要求を受信すると、FWSM は TCP 接続をリセットします。
  - Generate Syslog：FWSM が許可されている最大長を超える URI が含まれている HTTP 要求を受信すると、システム ログ メッセージを生成します。
- ヘッダーの最大長
  - Inspect Maximum Header Length：FWSM が HTTP 要求または応答にあるヘッダー長を検査します。
  - Request bytes：HTTP 要求でヘッダー長として許可される最大バイト数を指定します。許容範囲は 1 ～ 65535 です。

- Response bytes：HTTP 応答でヘッダー長として許可される最大バイト数を指定します。許容範囲は 1 ～ 65535 です。
- Action：HTTP ヘッダー長の検査に失敗した場合に FWSM が実行するアクションを指定します。次のアクションを実行できます。

  Allow Packet：HTTP 要求に許可されている最大長を超えるヘッダーが含まれていても、FWSM はその HTTP 要求を許可します。

  Drop Packet：HTTP 要求に許可されている最大長を超えるヘッダーが含まれている場合、FWSM はその HTTP 要求をドロップします。

  Reset Connection：許可されている最大長を超えるヘッダーが含まれている HTTP 要求を受信すると、FWSM は TCP 接続をリセットします。
- Generate Syslog：許可されている最大長を超えるヘッダーが含まれている HTTP 要求を受信すると、FWSM はシステム ログ メッセージを生成します。

• 本文の長さ
- Inspect Body Length：FWSM が HTTP 要求の本文の長さを検査します。
- Maximum bytes：HTTP メッセージで本文の長さとして許可される最小バイト数を指定します。許容範囲は 1 ～ 65535 です。
- Maximum bytes：HTTP メッセージで本文の長さとして許可される最大バイト数を指定します。許容範囲は 1 ～ 50000000 です。
- Action：HTTP 本文の長さの検査に失敗した場合に FWSM が実行するアクションを指定します。次のアクションを実行できます。

  Allow Packet：メッセージの本文が最大長よりも長い、または最小長よりも短い場合でも、FWSM はその HTTP 要求を許可します。

  Drop Packet：メッセージの本文が最大長よりも長い、または最小長よりも短い場合、FWSM はその HTTP 要求をドロップします。

  Reset Connection：メッセージの本文が最大長よりも長い、または最小長よりも短い場合、FWSM は TCP 接続をリセットします。
- Generate Syslog：メッセージの本文が最大長よりも長い、または最小長よりも短い場合、FWSM はシステム ログ メッセージを生成します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > RFC Request Method タブ

RFC Request Method タブでは、HTTP 要求で特定の要求方式を使用するときに実行するアクションを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- 方式固有のアクション
  - Method to be Added：FWSM が異なる方式を使用する HTTP 要求ごとに異なるアクションを実行するよう指定したい場合に使用可能な方式を一覧表示します。
  - Add：選択したアクションを実行する方式を、指定した方式のテーブルに追加します。

- Remove：選択した方式を、指定した方式のテーブルから削除します。
- Action：選択した要求方式に対するアクションを指定します。選択した方式を含む HTTP メッセージを FWSM が受信すると、このアクションが実行されます。選択した方式ごとにアクションを指定できます。次のアクションを実行できます。

  Allow Packet：FWSM が HTTP 要求を許可します。

  Drop Packet：FWSM が HTTP 要求をドロップします。

  Reset Connection：FWSM が TCP 接続をリセットします。
- Generate Syslog：FWSM がシステム ログ メッセージを生成します。選択した方式を含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択した方式ごとに異なるオプションを指定できます。

• デフォルトのアクション
- Action：指定した方式のテーブルに含まれていない方式を含む HTTP 要求を FWSM が受信した場合に実行するアクションを指定します。次のアクションを実行できます。

  Allow Packet：FWSM が HTTP 要求を許可します。

  Drop Packet：FWSM が HTTP 要求をドロップします。

  Reset Connection：FWSM が TCP 接続をリセットします。
- Generate Syslog：FWSM がシステム ログ メッセージを生成します。選択した方式を含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択した方式ごとに異なるオプションを指定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > Extension Request Method タブ

Extension Request Method タブでは、HTTP 要求で特定の拡張方式を使用する場合に実行するアクションを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- 方式固有のアクション
  - Method to be Added：FWSM が異なる方式を使用する HTTP 要求ごとに異なるアクションを実行するよう指定したい場合に使用可能な方式を一覧表示します。
  - Add：選択したアクションを実行する方式を、指定した方式のテーブルに追加します。
  - Remove：選択した方式を、指定した方式のテーブルから削除します。
  - Action：選択した要求方式に対するアクションを指定します。選択した方式を含む HTTP メッセージを FWSM が受信すると、このアクションが実行されます。選択した方式ごとにアクションを指定できます。次のアクションを実行できます。

    Allow Packet：FWSM が HTTP 要求を許可します。

    Drop Packet：FWSM が HTTP 要求をドロップします。

    Reset Connection：FWSM が TCP 接続をリセットします。

— Generate Syslog：FWSM がシステム ログ メッセージを生成します。選択した方式を含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択した方式ごとに異なるオプションを指定できます。

- デフォルトのアクション
  — Action：指定した方式のテーブルに含まれていない方式を含む HTTP 要求を FWSM が受信した場合に実行するアクションを指定します。次のアクションを実行できます。

  Allow Packet：指定した方式のテーブルに含まれない方式を含む HTTP 要求を FWSM が許可します。

  Drop Packet：指定した方式のテーブルに含まれない方式を含む HTTP 要求を FWSM がドロップします。

  Reset Connection：指定した方式のテーブルに含まれない方式が HTTP メッセージに含まれている場合、FWSM が TCP 接続をリセットします。

  — Generate Syslog：FWSM がシステム ログ メッセージを生成します。選択した方式を含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択した方式ごとに異なるオプションを指定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > Application Category タブ

Application Category タブでは、HTTP 要求に特定のアプリケーション タイプが含まれている場合に実行するアクションを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- カテゴリ固有のアクション
  — Category to be Added：FWSM が、異なるアプリケーション カテゴリを使用する HTTP 要求ごとに異なるアクションを実行するよう指定したい場合に、使用可能なアプリケーション カテゴリを一覧表示します。
  — Add：選択したアクションを実行するアプリケーション カテゴリを、指定したカテゴリのテーブルに追加します。
  — Remove：選択したアプリケーション　カテゴリを、指定したカテゴリのテーブルから削除します。
  — Action：選択したアプリケーション カテゴリに対するアクションを指定します。選択したアプリケーション カテゴリを含む HTTP メッセージを FWSM が受信すると、このアクションが実行されます。選択したアプリケーション カテゴリごとに異なるアクションを指定できます。次のアクションを実行できます。

  Allow Packet：FWSM が HTTP 要求を許可します。

  Drop Packet：FWSM が HTTP 要求をドロップします。

  Reset Connection：FWSM が TCP 接続をリセットします。

  — Generate Syslog：FWSM がシステム ログ メッセージを生成します。選択したアプリケーション カテゴリを含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択したアプリケーション カテゴリごとに異なるオプションを指定できます。

- デフォルトのアクション
  - Action：指定したカテゴリのテーブルに含まれていないアプリケーション カテゴリを含む HTTP 要求を FWSM が受信した場合に実行するアクションを指定します。次のアクションを実行できます。

    Allow Packet：指定したカテゴリのテーブルに含まれないアプリケーション カテゴリを含む HTTP 要求を FWSM が許可します。

    Drop Packet：指定したカテゴリのテーブルに含まれないアプリケーション カテゴリを含む HTTP 要求を FWSM がドロップします。

    Reset Connection：指定したカテゴリのテーブルに含まれないアプリケーション カテゴリが HTTP メッセージに含まれている場合、FWSM が TCP 接続をリセットします。
  - Generate Syslog：FWSM がシステム ログ メッセージを生成します。選択したアプリケーション カテゴリを含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択したアプリケーション カテゴリごとに異なるオプションを指定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 > Transfer-Encoding タブ

Transfer-Encoding タブでは、HTTP 要求で特定の転送符号化のタイプが使用されている場合に実行するアクションを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- 符号化のタイプに固有のアクション
  - Encoding-type to be Added：FWSM が異なる符号化のタイプを使用する HTTP 要求ごとに異なるアクションを実行するよう指定したい場合に使用可能な符号化のタイプを一覧表示します。
  - Add：選択した転送符号化のタイプを、指定した転送符号化のタイプのテーブルに追加します。
  - Remove：選択した転送符号化のタイプを、指定した転送符号化のタイプのテーブルから削除します。
  - Action：指定した転送符号化のタイプのテーブルにある転送符号化のタイプを含む HTTP 要求を FWSM が受信した場合に実行するアクションを指定します。次のアクションを実行できます。

    Allow Packet：指定した転送符号化のタイプのテーブルにある転送符号化のタイプを含む HTTP 要求を FWSM が許可します。

    Drop Packet：指定した転送符号化のタイプのテーブルにある転送符号化のタイプが HTTP 要求に含まれる場合、FWSM はその HTTP 要求をドロップします。

    Reset Connection：指定した転送符号化のタイプのテーブルにある転送符号化のタイプが HTTP メッセージに含まれる場合、FWSM は TCP 接続をリセットします。
  - Generate Syslog：指定した転送符号化のタイプのテーブルにある転送符号化のタイプが HTTP メッセージに含まれる場合、FWSM はシステム ログ メッセージを生成します。

- デフォルトのアクション
  - Action：指定した転送符号化のタイプのテーブルに含まれないが、サポートされている転送符号化のタイプを含む HTTP 要求を FWSM が受信した場合に実行するアクションを指定します。次のアクションを実行できます。

    Allow Packet：指定した転送符号化のタイプのテーブルに含まれていない転送符号化のタイプを含む HTTP 要求を FWSM が許可します。

    Drop Packet：指定した転送符号化のタイプのテーブルに含まれない転送符号化のタイプを含む HTTP 要求を FWSM がドロップします。

    Reset Connection：指定した転送符号化のタイプのテーブルに含まれない転送符号化のタイプが HTTP メッセージに含まれる場合、FWSM は TCP 接続をリセットします。
  - Generate Syslog：指定した転送符号化のタイプのテーブルに含まれていない転送符号化のタイプが HTTP メッセージに含まれる場合、FWSM はシステム ログ メッセージを生成します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

MGCP ペインで、MGCP アプリケーションの事前に設定された検査マップを表示します。MGCP マップでは、MGCP アプリケーション検査のデフォルト設定値を変更できます。MGCP ペインでは、新しい MGCP マップを追加するか、または既存のマップを変更または削除できます。

フィールド

- Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Command Queue Size：MGCP コマンドの許容キュー サイズを指定します。
- Group ID：コール エージェント グループの ID を識別します。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。
- 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検査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、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Map の追加および編集

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を使用してメディア ゲートウェイを制御するには、MGCP を使用します。MGCP マップ グループ テーブルには、現在の MGCP アプリケーション検査マップに設定されているグループが一覧表示されます。既存のグループを編集するには、グループを選択してから **Edit** をクリックします。このテーブルには、次のカラムがあります。

フィールド

- MGCP Map Name：アプリケーション検査マップの名前を定義します。
- 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。
- Group ID：0 ～ 2147483647 までのコール エージェント グループの ID が一覧表示されます。
- 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 アドレスが一覧表示されます。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：関連付けられた MGCP ゲートウェイを制御するメディア ゲートウェイ コントローラ（コール エージェント）の IP アドレスを一覧表示します。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を表示します。このダイアログボックスで新しい MGCP グループを追加できます。
- Edit：Edit MGCP Group 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既存の MGCP グループのコンフィギュレーションを変更できます。
- Delete：選択した MGCP グループを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、MGCP アプリケーション検査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します。

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。
- ゲートウェイ
  - 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。
- コール エージェント
  - 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

SIP ペインで、SIP アプリケーションの事前に設定された検査マップを表示します。SIP マップでは、SIP アプリケーション検査に対する IP アドレス プライバシーをイネーブルにできます。SIP ペインでは、新しい SIP マップを追加するか、または既存のマップを変更または削除できます。

IP アドレスのプライバシーがイネーブルの場合、1 つの IP 電話コールまたはインスタント メッセージ セッションに参加している 2 つの SIP エンドポイントが、同じ内部ファイアウォール インターフェイスを使用して外部ファイアウォール インターフェイスの SIP プロキシ サーバに接続している場合、SIP シグナリング メッセージはすべて SIP プロキシ サーバを通過します。

TCP または UDP 経由の SIP アプリケーション検査がイネーブルの場合に、IP アドレス プライバシーをイネーブルにできます。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。IP アドレス プライバシーがイネーブルの場合、FWSM は、着信 SIP トラフィックの TCP または UDP ペイロードに組み込まれた内部および外部のホスト IP アドレスを変換しません。これらの IP アドレスの変換ルールは無視されます。

フィールド

- Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- IP Address：IP アドレス プライバシーがイネーブルかどうかを示します。
- Add：Add SIP 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検査マップを定義できます。
- Edit：Edit SIP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Map

Add/Edit SIP Map ダイアログボックスでは、新しい SIP マップの作成、または既存のマップの修正ができます。IP アドレス プライバシーはデフォルトでディセーブルになっているので、イネーブルにするには SIP マップが必要です。

IP アドレスのプライバシーがイネーブルの場合、1 つの IP 電話コールまたはインスタント メッセージ セッションに参加している 2 つの SIP エンドポイントが、同じ内部ファイアウォール インターフェイスを使用して外部ファイアウォール インターフェイスの SIP プロキシ サーバに接続している場合、SIP シグナリング メッセージはすべて SIP プロキシ サーバを通過します。

TCP または UDP 経由の SIP アプリケーション検査がイネーブルの場合に、IP アドレス プライバシーをイネーブルにできます。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。IP アドレス プライバシーがイネーブルの場合、FWSM は、着信 SIP トラフィックの TCP または UDP ペイロードに組み込まれた内部および外部のホスト IP アドレスを変換しません。これらの IP アドレスの変換ルールは無視されます。

フィールド

- SIP Map Name：アプリケーション検査マップの名前を定義します。
- IP Address Privacy：IP アドレス プライバシーをイネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、SNMP アプリケーションの事前に設定された検査マップを表示します。SNMP マップでは、SNMP アプリケーション検査のデフォルト設定値を変更できます。SNMP ペインでは、新しい SNMP マップを追加するか、または既存のマップを変更または削除できます。

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検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Disallowed SNMP Versions：特定の SNMP アプリケーション検査マップで拒否される SNMP バージョンを識別します。
- Add：Add SNMP 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検査マップを定義できます。
- Edit：Edit SNMP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、SNMP のアプリケーション検査を制御する SNMP マップを新規作成できます。

フィールド

- SNMP Map Name：アプリケーション検査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検査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検査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検査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検査をイネーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 プールの設定

グローバル プールの詳細については、P.21-6 の「ダイナミック NAT」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、アクセスリストを時間範囲に添付して、FWSM へ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、および繰り返し時間範囲エントリ（オプション）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：時間範囲の始まる時期を指定します。
- End Time：時間範囲が終了する時期を指定します。
- 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Range

Add/Edit Time Range ペインで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、アクセスリストを時間範囲に添付して、FWSM へのアクセスを制限できます。時間範囲は FWSM のシステム クロックに依存します。ただし、最適に動作するのは NPT 同期を適用した場合です。

（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 at：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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ペインで時間範囲を詳細に指定し、日単位または週単位の設定を行います。

（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 まで一覧表示します。
  - Minute：分を 00 ～ 59 まで一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

セキュリティ コンテキストの設定

ここでは、次の項目について説明します。

セキュリティ コンテキストの概要

1 台の FWSM を、セキュリティ コンテキストと呼ばれる複数の仮想装置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ちます。マルチコンテキストは、複数のスタンドアロン装置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、管理など、多くの機能がサポートされます。ほとんどのダイナミック 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。

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、多数の顧客にセキュリティ サービスを販売する。FWSM 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、顧客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。
- 複数のファイアウォール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。

- ほとんどのダイナミック ルーティング プロトコル。BGP スタブ モードがサポートされています。

  セキュリティ コンテキストは、スタティック ルートまたは BGP スタブ モードのみをサポートします。マルチコンテキスト モードでは、OSPF または RIP をイネーブルにできません。
- マルチキャスト ルーティング。マルチキャスト ブリッジングがサポートされています。

コンテキスト コンフィギュレーション ファイル

この項では、FWSM でマルチコンテキスト モードのコンフィギュレーションを実装する方法について説明します。次の項目を取り上げます。

コンテキスト コンフィギュレーション

FWSM 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装置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。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。

システム コンフィギュレーション

システム管理者は、各コンテキスト コンフィギュレーションの場所、割り当てられたインターフェイス、およびシステム コンフィギュレーションのその他のコンテキスト実行パラメータを設定することでコンテキストを追加および管理します。システム コンフィギュレーションは、シングルモード コンフィギュレーションと同様に、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、FWSM 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、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。

管理コンテキスト コンフィギュレーション

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。管理コンテキストは一切制限されないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストに対する管理者特権が与えられるため、場合によっては管理コンテキストへのアクセスを適切なユーザに制限する必要があります。管理コンテキストは、リモートではなくフラッシュ メモリに置く必要があります。

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。

FWSM によるパケットの分類方法

FWSM 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、FWSM 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。FWSM では、すべてのインターフェイスに対してグローバル MAC アドレスを 1 つだけ使用します。通常、マルチコンテキストでインターフェイスの共有が必要でない限り、MAC アドレス 1 つで問題ありません。すべての IP アドレスが同じ MAC アドレスに解決されると、ルータは、パケットを同じネットワークの IP アドレスに転送できません。また、スイッチのブリッジング テーブルは、MAC アドレスが 1 つのインターフェイスから別のインターフェイスに移動するときに絶えず変化します。セキュリティ コンテキストの分類子は、この状況を解決するためのものです。

ここでは、次の項目について説明します。

- 有効な分類子の基準（P.7-4）
- 無効な分類子の基準（P.7-4）
- 分類の例（P.7-5）

有効な分類子の基準

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、FWSM はパケットをそのコンテキストに分類します。透過ファイアウォール 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。

マルチコンテキストでインターフェイスを共有している場合、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、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分類子が認識できなければなりません。分類子は、アクティブな NAT セッ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。アクティブな NAT セッションは、永続的なセッションを作成する **static** コマンドか、またはアクティブなダイナミック NAT セッションのいずれかで作成されます。

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
```

ダイナミック NAT を使用する場合、実際のホストが共有インターフェイスを通じて接続を作成するときに、アクティブ NAT セッションが作成されます。ホストに戻るトラフィックでは、パケットの分類にアクティブ NAT セッションが使用されます。

異なるコンテキスト間に重複があると接続問題の原因になります。この重複を迅速に識別するには、システム実行スペースで **show np 3 static** コマンドを入力します。

（注） インターフェイス用管理トラフィックでは、インターフェイス IP アドレスが分類用として使用されます。

無効な分類子の基準

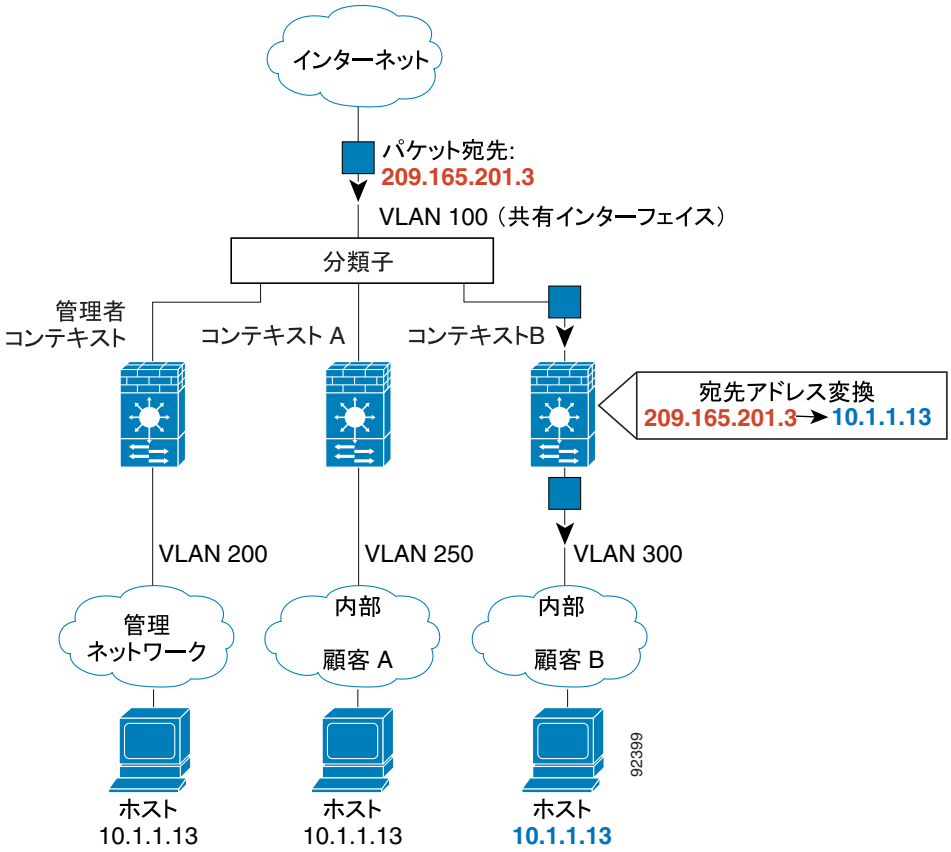
次のコンフィギュレーションは、パケットの分類に使用されません。

- 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を使用しません。これは、NAT 免除がマッピング（共有）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：分類子は、分類にルーティング テーブルを使用しません。たとえば、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 ルートがコンテキストに含まれていて、同じサブネットに対する **static** コマンドが別のコンテキストに含まれている場合、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 7-1 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。内部インターフェイスは固有であり、IP アドレスは重複が可能です。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 7-1　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 7-2 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 VLAN 300 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 7-2　内部ネットワークからの着信トラフィック

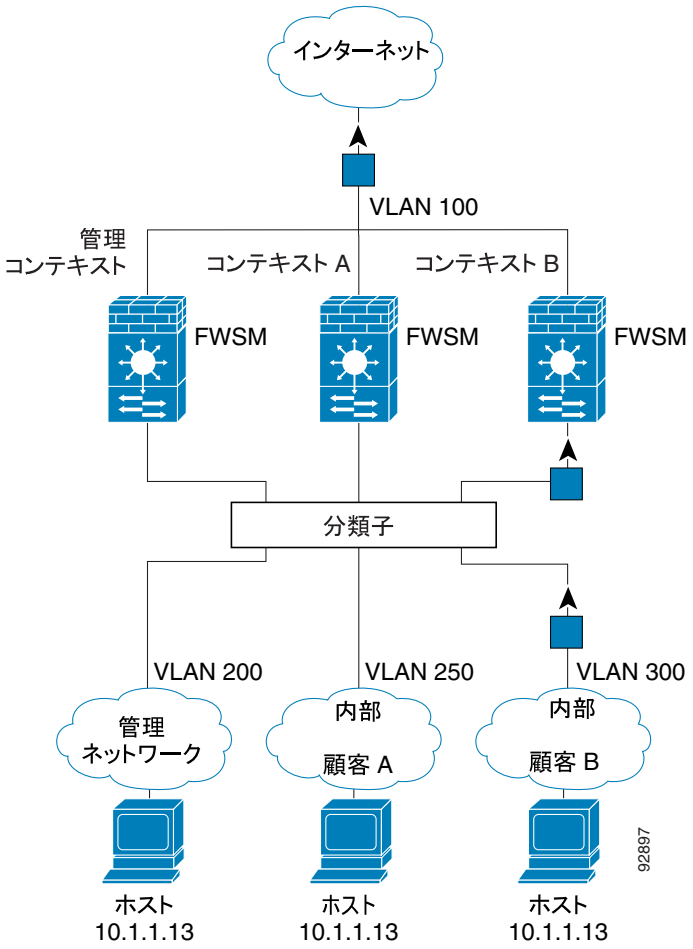
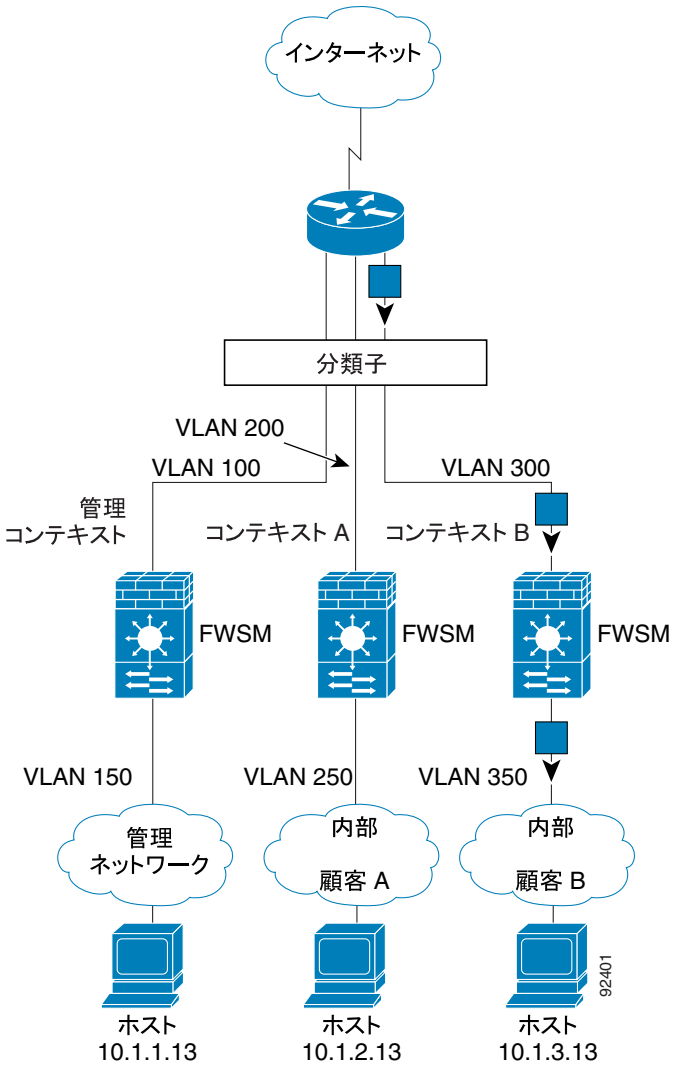


図 7-3 に、インターネットにアクセスするコンテキスト B 内部ネットワークにホストがある透過ファイアウォールを示します。分類子は、パケットをコンテキスト B に割り当てます。これは、入力インターフェイスが VLAN 300 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 7-3　透過ファイアウォールのコンテキスト



コンテキスト間のインターフェイス共有

ルーテッド モードのみ

FWSM では、複数のコンテキストで 1 つのインターフェイスを共有できます。ただし、パケット分類要件により、インターフェイスを共有できないことがあります。分類子は、アクティブ NAT セッションに基づいて宛先アドレスをコンテキストに分類するので、NAT の設定内容によって制限を受けます。NAT を実行しない場合は、固有のインターフェイスを使用する必要があります。

（注） FWSM では、コンテキストの外部インターフェイスを別のコンテキストの内部インターフェイスとして共有すること（カスケード コンテキスト）はサポートされていません。あるコンテキストからの発信トラフィック（高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスへ）は、着信トラフィック（低位から高位へ）としてのみ別のコンテキストに入ることができます。両方のコンテキストの発信にすることも、両方のコンテキストの着信にすることもできません。

ここでは、次の項目について説明します。

- NAT およびトラフィックの発信元（P.7-8）
- 外部インターフェイスの共有（P.7-8）
- 内部インターフェイスの共有（P.7-8）

NAT およびトラフィックの発信元

設定する NAT のタイプによって、共有インターフェイスでトラフィックを発信できるか、または既存の接続への応答のみが可能かが決まります。ダイナミック NAT を使用する場合、実際のアドレスへの接続を開始することはできません。このため、共有インターフェイスからのトラフィックは、既存の接続への応答でなければなりません。ただし、スタティック NAT では接続を開始できるため、共有インターフェイスで接続を開始できます。

外部インターフェイスの共有

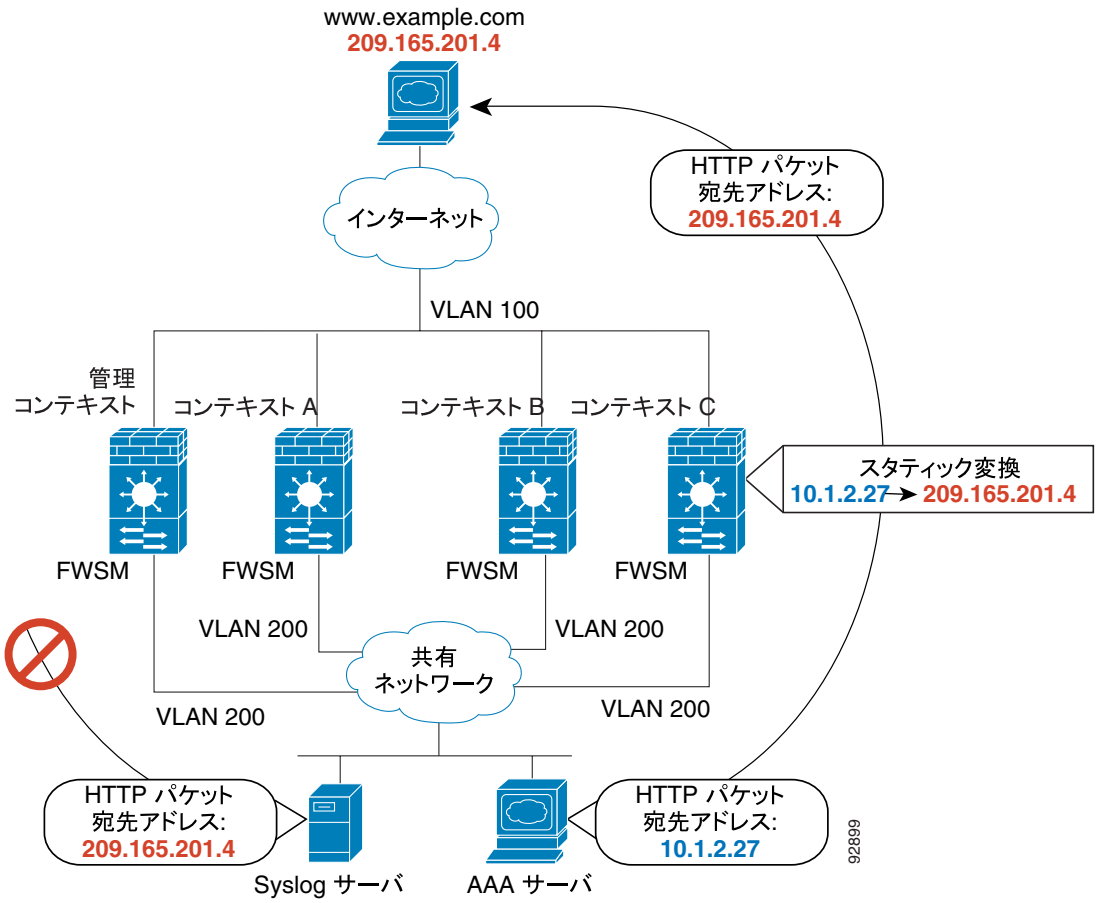
外部共有インターフェイス（インターネットへの接続など）を使用している場合、内部の宛先アドレスは数に限りがあり、システム管理者は内部の宛先アドレスについて把握しています。このため、スタティック NAT の場合でも、内部の宛先のアドレスに対する NAT の設定は簡単です。

内部インターフェイスの共有

一方、限りない宛先アドレスが存在する環境であるインターネットと共有インターフェイス間の通信を許可する場合、内部インターフェイスを共有に設定すると問題が生じます。たとえば、共有インターフェイス上の内部ホストからインターネットへのトラフィックの開始を許可する場合、各インターネット アドレスに対してスタティック NAT 文を設定する必要があります。この要件により、必然的に内部共有インターフェイス上のユーザに提供できるインターネット アクセスの種類が制限されます（インターネット サーバのアドレスをスタティックに変換する場合は、DNS エントリのアドレスと NAT によってそれがどのような影響を受けるかという点も考慮する必要があります。たとえば、サーバが www.example.com にパケットを送信すると、DNS サーバは変換対象アドレスを返す必要があります。NAT コンフィギュレーションによって DNS エントリの管理が決まります）。

図 7-4 に、内部共有インターフェイス上の 2 つのサーバを示します。一方のサーバは Web サーバの変換対象アドレスにパケットを送信します。FWSM はパケットを分類し、そのアドレスのスタティック変換がコンテキスト C にあるので、パケットをコンテキスト C に転送します。他方のサーバは、変換されない実際のアドレスにパケットを送信しますが、FWSM はパケットを分類できないので、そのパケットはドロップされます。

図 7-4　共有インターフェイス上を発信元とするトラフィック



CLI でのマルチコンテキスト モードのイネーブル化とディセーブル化

シスコへの発注内容によっては、FWSM 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 はモードの変更をサポートしていないため、CLI を使用してモードを変更する必要があります。

ここでは、次の項目について説明します。

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、FWSM 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、リブートしても保持されますが、コンフィギュレーション ファイルには保存されません。別の装置にコンフィギュレーションをコピーする必要がある場合、**mode** コマンドを実行して新しい装置のモードを一致するように設定します。

シングルモードからマルチモードに変換すると、FWSM 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。その 2 つは、システム コンフィギュレーションを構成する新しいスタートアップ コンフィギュレーションと、管理コンテキストを構成する admin.cfg です（内部フラッシュ メモリのルート　　ディレクトリに作成されます）。元の実行コンフィギュレーションは、old_running.cfg として保存されます（内部フラッシュ メモリのルート ディレクトリに保存されます）。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。管理コンテキストのエントリは、「admin」という名前でシステム コンフィギュレーションに FWSM によって自動的に追加されます。

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
```

FWSM 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、最初にスタートアップ コンフィギュレーション全体を FWSM にコピーします（可能な場合）。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、シングルモードの装置にとっては完全に機能するコンフィギュレーションではないからです。たとえば、以前のシングルモード実行コンフィギュレーションがある場合は、スタートップ コンフィギュレーションとして復元できます。システム コンフィギュレーションには、コンフィギュレーションの一部としてネットワーク インターフェイスが含まれていないので、スイッチ コンソールから FWSM にアクセスしてコピーを実行する必要があります。

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 old_running.cfg startup-config
```

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
```

FWSM 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、コンテキストごとの最大限度が設定されている場合を除いて、すべてのセキュリティ コンテキストは FWSM のリソースに無制限にアクセスできます。ただし、1 つまたは複数のコンテキストがリソースを使用し過ぎて、他のコンテキストが接続できなくなる場合には、リソース管理の設定を行い、コンテキストごとのリソースの使用を制限することができます。FWSM では、コンテキストをリソース クラスに割り当てることによりリソースを管理します。各コンテキストには、クラスごとに設定されたリソース制限が適用されます。

（注） FWSM　は、コンテキストごとに帯域幅を制限しませんが、FWSM　が搭載されているスイッチは VLAN ごとに帯域幅を制限できます。詳細については、スイッチのマニュアルを参照してください。

ここでは、次の項目について説明します。

- クラスおよびクラス メンバーの概要（P.7-12）
- リソース クラスの追加（P.7-15）

クラスおよびクラス メンバーの概要

FWSM では、コンテキストをリソース クラスに割り当てることによりリソースを管理します。各コンテキストには、クラスごとに設定されたリソース制限が適用されます。ここでは、次の項目について説明します。

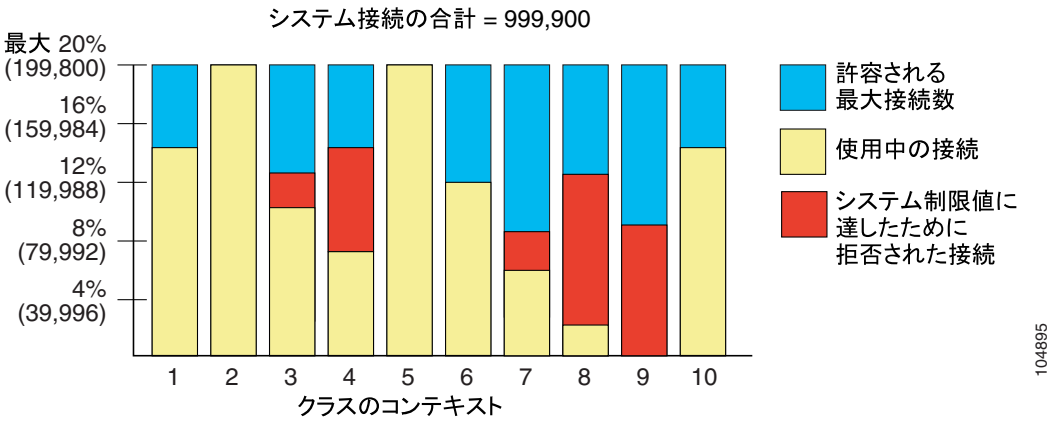
- リソース制限の概要（P.7-12）
- デフォルト クラスの概要（P.7-14）
- クラス　メンバーの概要（P.7-14）

リソース制限の概要

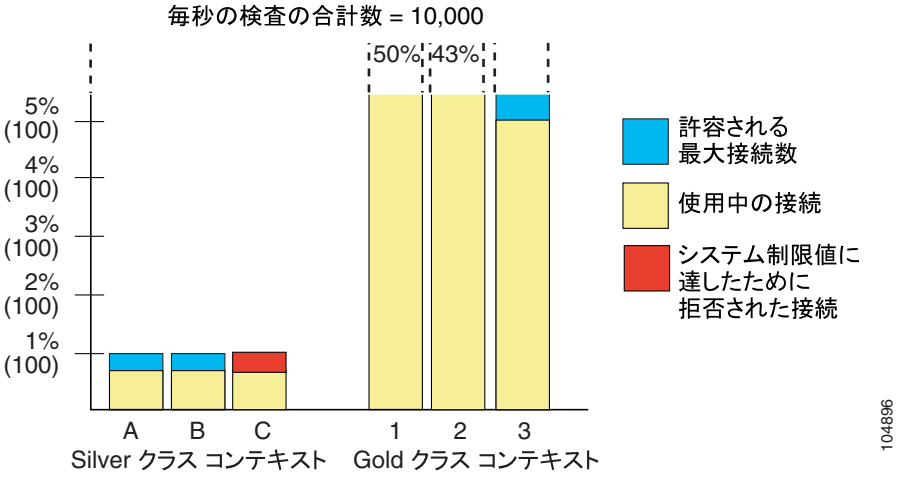
クラスを作成すると、FWSM は、そのクラスに割り当てられたコンテキストごとに一定のリソースを確保するのではなく、コンテキストが使用できるリソースの最大限度を設定します。リソースをオーバーサブスクライブしたり、特定のリソースを無制限にしたりすると、いくつかのコンテキストがリソースを使い果たして、他のコンテキストに対するサービスに影響が出ることがあります。

すべてのリソースを一括して制限を設定できます。デバイスで使用できる合計値をパーセントで指定します。また、個々のリソースに、制限をパーセントまたは絶対値で設定できます。

すべてのコンテキスト合計で 100% を超えるリソースを割り当てると、FWSM 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、Bronze クラスにはコンテキストごとに 20% の接続制限を設定してから、そのクラスに 10 のコンテキストを割り当てると、合計は 200% になります。いくつかのコンテキストがシステムの制限を超えて同時に使用すれば、各コンテキストは、当初想定した 20% に満たなくなります（次の図を参照）。



FWSM では、あるクラスの 1 つまたは複数のリソースに、パーセントや絶対値ではなく、無制限アクセスを割り当てることができます。あるリソースが無制限の場合、コンテキストは、システムで利用できるリソースをすべて使用できます。たとえば、Silver クラスの中にコンテキスト A、B、C があるとします。各クラス メンバーに毎秒 1% のシステム検査制限を課すと合計が 3% になりますが、3 つのコンテキストが、現在合計 2% しか使用していないとします。一方、Gold クラスには検査への無制限アクセスが設定されているとします。この場合、Gold クラスのコンテキストは、97% より多い「未割り当て」検査を使用できます。コンテキスト A、B、C が現在使用していない 1% の検査も使用できるからです（その結果、コンテキスト A、B、C が合計 3% の制限より少ないリソースしか使用できなくなることがあります）。次の図を参照してください。無制限アクセスの設定は、FWSM のオーバーサブスクライブに似ています。相違点は、システムのオーバーサブスクライブの程度をあまり制御できないという点です。



デフォルト クラスの概要

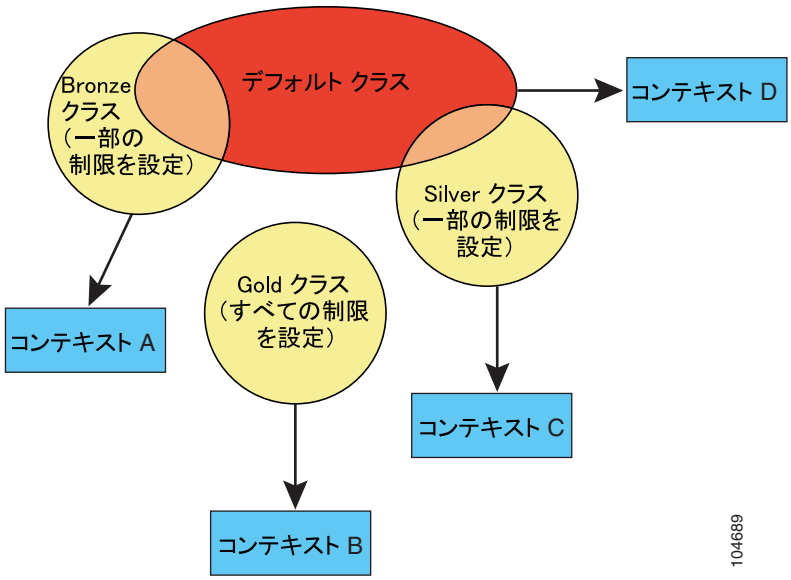
すべてのコンテキストは、別のクラスに割り当てられていなければ、デフォルト クラスに属します。したがって、コンテキストをデフォルト クラスに特に割り当てる必要はありません。

コンテキストがデフォルト クラス以外のクラスに属している場合、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、他のクラス設定が定義されていない場合、メンバー コンテキストはデフォルト クラスを制限用に使用します。たとえば、同時接続に 2% を設定されたクラスを作成し、その他の制限がない場合、その他すべての制限はデフォルト クラスから継承されます。反対に、すべてのリソースに 2% の制限のあるクラスを作成する場合、そのクラスはデフォルト クラス設定を使用しません。

デフォルトでは、デフォルト クラスのすべてのコンテキストには、リソースへの無制限アクセスが付与されます。ただし、次の制限については、デフォルトでコンテキストごとの最大値に設定されます。

- 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

次の図に、デフォルト クラスと他のクラスとの関係を示します。コンテキスト A と C は、いくつか制限のあるクラスに属しています。他の制限は、デフォルト クラスから継承されます。コンテキスト B は、すべての制限がそのクラス（Gold クラス）に設定されているので、デフォルト クラスから制限を継承することはありません。コンテキスト D はクラスに割り当てられていないため、デフォルトでデフォルト クラスのメンバーになります。



クラス メンバーの概要

クラスの設定を使用するには、コンテキストの定義時に、コンテキストをその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 クラスに特に割り当てる必要はありません。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、メンバー クラスで未定義の制限がデフォルト クラスから継承される点です。したがって、実際には、コンテキストはデフォルト クラスと別のクラスのメンバーということになります。

リソース クラスの追加

この項では、リソース クラスの設定で使用できるペインについて説明します。次の項目を取り上げます。

Resource Class

Resource Class ペインで、設定されているクラスと各クラスの情報を示します。クラスの追加、編集、削除もできます。

フィールド

- Class：クラスの名前を示します。
- 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。デフォルトは 0 で、無制限を意味します。
- Connections：任意の 2 つのホスト間の TCP 接続または UDP 接続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：FWSM 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 セッションは、2 つの HTTPS 接続を使用します。1 つは常駐の監視用、もう 1 つは変更時にのみ使用されるコンフィギュレーション変更用です。たとえば、ASDM セッション数のシステム制限値が 80 の場合は、すべてのコンテキスト合計で HTTPS セッション数が 160 に制限されます。
- IPSec：IPSec 管理セッションの制限値を示します。デフォルトは 5 です。
- MAC Addresses：透過ファイアウォール 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：アプリケーション検査数 / 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、コンテキストのクラスはデフォルトに戻ります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、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：クラスの名前を 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。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。デフォルト クラスが制限値を設定しない場合、デフォルトで制限値はシステム制限値になります。
  - All Resources：すべてのリソースに制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。また、特定のリソースに制限値を設定すると、設定した制限値は、すべてのリソースに設定した制限値より優先されます。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。また、無制限に設定するには、値を **0** に設定し、リストの **Absolute** をクリックします。その他の絶対値は設定できません。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。
  - Hosts：FWSM 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。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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）～ 262144 の範囲で整数を入力し、リストの **Absolute** をクリックします。
  - Telnet：Telnet　同時セッションの制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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、すべてのコンテキスト合計で 100 です。
  - IPSec：IPSec 同時セッションの制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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、すべてのコンテキスト合計で 10 です。
  - ASDM Sessions：ASDM の同時セッションの制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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、すべてのコンテキスト合計で 80 です。ASDM セッションは 2 つの HTTPS 接続を使用します。1 つは常駐の監視用、もう 1 つは変更時のみ使用されるコンフィギュレーション変更用です。たとえば、ASDM セッション数のシステム制限値が 80 の場合は、すべてのコンテキスト合計で HTTPS セッション数が 160 に制限されます。
  - Connections：任意の 2 つのホスト間の TCP または UDP の同時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。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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）～ 999900 の範囲で整数を入力し、リストの **Absolute** をクリックします。

（注） 同時接続の場合、FWSM は、接続を受け入れる 2 つの NP のそれぞれに制限値の半分を割り当てます。通常、接続数は NP 間で均等に分割されます。ただし、状況によっては、接続数が均等に分割されず、一方の NP で最大接続制限に達する前に、もう一方の NP で最大接続制限に達してしまうことがあります。このような場合、許可される最大接続数は設定した制限よりも少なくなります。NP への分配は、アルゴリズムに基づいてスイッチが制御します。スイッチでこのアルゴリズムを調整するか、不均衡の原因となる接続制限を引き上げて調整することができます。

  - Xlates：アドレス変換の制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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）～ 266144 の範囲で整数を入力し、リストの **Absolute** をクリックします。
  - SSH：SSH セッションの制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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：（透過モードのみ）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。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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。デフォルト クラスが制限値を設定しない場合、デフォルトで制限値はシステム制限値になります。
  - Conns/sec：接続数 / 秒の制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。また、制限値を絶対値で設定する場合は、0 ～ 102400 の範囲で整数を入力し、リストの **Absolute** をクリックします。
  - 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。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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）～ 102400 の範囲で整数を入力し、リストの **Absolute** をクリックします。
  - Fixups/sec：アプリケーション検査数 / 秒の制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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）～ 10000 の範囲で整数を入力し、リストの **Absolute** をクリックします。
- 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

次の表に、この機能を使用できるモードを示します。

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

メモリ パーティションの設定

マルチコンテキスト モードで、FWSM は、ルール コンフィギュレーションに割り当てられたメモリをパーティションに分割し、各コンテキストをパーティションに割り当てます。デフォルトで、コンテキストは、ACE、AAA ルールなど最大数のルールを提供する 12 のパーティションのうちの 1 つに属します。ルールの制限のリストについては、P.A-7 の「ルール制限」を参照してください。FWSM は、起動時にロードされる順番でコンテキストをパーティションに割り当てます。たとえば、12 のコンテキストを設定し、ルールの最大数が 14,103 の場合、各コンテキストはそれぞれ個別のパーティションに割り当てられ、14,103 のルールを使用できます。さらに 1 つのコンテキストを追加すると、コンテキスト番号 1 および新しいコンテキスト番号 13 の両方がパーティション 1 に割り当てられ、2 つのコンテキスト合計で 14,103 のルールを使用できます。他の 11 のコンテキストは、引き続きそれぞれが 14,103 のルールを使用できます。コンテキストを削除しても、パーティションのメンバーシップは変わりません。したがって、リブートしてコンテキストが均等に分配されるまで、コンテキストの分配が不均一になることがあります。

（注） ルールは先着順で使用されるため、コンテキストによっては使用するルールが他のコンテキストよりも多くなることがあります。

ルールの制限の詳細については、P.A-7 の「ルール制限」を参照してください。

コンテキストをパーティションに手動で割り当てることもできます。コンテキストをパーティションに割り当てるには、P.7-20 の「セキュリティ コンテキストの設定」を参照してください。また、コンテキストの数と一致するように、パーティションの数を減らすこともできます。

（注） パーティションの数を変更した場合、FWSM をリロードする必要があります。

メモリ パーティションの数を変更するには、次の手順を実行します。

ステップ 1　システム実行スペースで、Configuration > Security Contexts にアクセスし、Number of ACL Partitions フィールドにパーティションの数を 1 ～ 12 で設定します。

（注） コンテキストをパーティションに割り当てる場合、パーティション番号は 0 から始まります。したがって、パーティションが 12 個ある場合、パーティション番号は 0 ～ 11 になります。コンテキストをパーティションに割り当てる方法については、P.7-20 の「セキュリティ コンテキストの設定」を参照してください。

ステップ 2　**Apply** をクリックします。

ステップ 3　FWSM をリロードして変更を有効にするには、**Tools > System Reload** を選択します。

フェールオーバーを使用している場合、両方の装置でメモリ パーティションが一致しなければならないため、他のフェールオーバー装置もリロードする必要があります。両方の装置が同時にダウンするため、トラフィック ロスが生じる可能性があります。

ステップ 4　フェールオーバーを使用している場合、もう一方の装置をリロードします。

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。

前提条件

コンテキストを ASDM で設定する前に、FWSM がマルチコンテキスト モードになっていることを確認してください。Home > Device Information > General タブに、現在のコンテキスト モードがマルチかシングルかが表示されます。シングルモードからマルチモードに変更するには、「CLI でのマルチコンテキスト モードのイネーブル化とディセーブル化」を参照してください。

Security Contexts

Security Contexts ペインで、設定されたコンテキストと各コンテキストの情報を示します。コンテキストの追加、編集、削除もできます。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 コンテキストの概要」を参照してください。

フィールド

- Context：コンテキストの名前を示します。
- Mode：コンテキストがルーテッド モードか透過モードかを示します。
- Interfaces：コンテキストに割り当てられたインターフェイスを示します。コンテキストで表示するインターフェイスにエイリアス名を割り当てると、エイリアス名がカッコ内に表示されます。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：コンテキストが割り当てられるリソース 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。
- ACL Partition：コンテキストが割り当てられるメモリ パーティションを示します。デフォルトで、コンテキストは起動時の順番でパーティションに割り当てられます。
- 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。
- Change Firewall Mode：ファイアウォール モードを変更します。透過モードの場合は、ルーテッド モードに変更します。ルーテッド モードの場合は、透過モードに変更します。ASDM で管理コンテキストのモードを変更することはできません。CLI でのモードの変更については、「CLI での透過またはルーテッド ファイアウォール モードの設定」を参照してください。モードを変更すると、FWSM は実行コンフィギュレーションをクリアします。これは、多くのコマンドがどちらかのモードでしかサポートされていないからです。すでに実装済みのコンフィギュレーションがある場合は、モードを変更する前に必ずコンフィギュレーションのバックアップを作成してください。新しくコンフィギュレーションを作成するときにこのバックアップを参照する場合があります。Tools > File Management ペイン、または Tools > File Transfer ペインを参照してください。デフォルトのルーテッド モードで新しいコンテキストを追加した場合、ファイアウォール モードを変更する前に、新しいコンテキストを適用してください。モードを変更するには、コンテキストが実行中である必要があるからです。

- Delete：コンテキストを削除します。
- Number of ACL partitions (1-12)：メモリ パーティションの数を設定します。デフォルトは 12 です。マルチコンテキスト モードで、FWSM は、ルール コンフィギュレーションに割り当てられたメモリをパーティションに分割し、各コンテキストをパーティションに割り当てます。デフォルトで、コンテキストは、ACE、AAA ルールなど最大 12,130 のルールを提供する 12 のパーティションのうちの 1 つに属します。FWSM は、起動時にロードされる順番でコンテキストをパーティションに割り当てます。たとえば、12 のコンテキストがある場合、各コンテキストは個別のパーティションに割り当てられ、12,130 のルールを使用できます。さらに 1 つのコンテキストを追加すると、コンテキスト番号 1 および新しいコンテキスト番号 13 の両方がパーティション 1 に割り当てられ、2 つのコンテキスト合計で 12,130 のルールを使用できます。他の 11 のコンテキストは、引き続きそれぞれが 12,130 のルールを使用できます。コンテキストを削除しても、パーティションのメンバーシップは変わりません。したがって、リブートしてコンテキストが均等に分配されるまで、コンテキストの分配が不均一になることがあります。

  ルールは先着順で使用されるため、コンテキストによっては使用するルールが他のコンテキストよりも多くなることがあります。

  コンテキストをパーティションに手動で割り当てることもできます。また、コンテキストの数と一致するように、パーティションの数を減らすこともできます。

（注） パーティションの数を変更した場合、FWSM をリロードする必要があります。

詳細情報

セキュリティ コンテキストの概要

CLI でのマルチコンテキスト モードのイネーブル化とディセーブル化

ファイアウォール モードの概要

CLI での透過またはルーテッド ファイアウォール モードの設定

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Add/Edit Context ダイアログボックスで、セキュリティ コンテキストの追加または編集、およびコンテキスト パラメータの定義ができます。

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。大文字と小文字が区別されるため、たとえば「customerA」と「CustomerA」の 2 種類のコンテキストを使用できます。「System」および「Null」（大文字および小文字）は予約されている名前であるため、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を示します。
  - Interface：インターフェイス ID を示します。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：インターフェイスをコンテキストに追加します。
  - Edit：インターフェイスの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。
- Resource Assignment：コンテキストをリソース クラスとメモリ パーティションに割り当てます。
  - Resource Class：リストからクラスを選択します。
  - Edit：選択したリソース クラスを編集します。
  - New：リソース クラスを追加します。
  - ACL Partition：メモリ パーティションを選択します。FWSM が、起動時に次に使用可能なパーティションにコンテキストを割り当てるようにする場合は、**Default** を選択します。コンテキストをパーティションに手動で割り当てると、パーティションは*排他的*になります。排他的パーティションには、そのパーティションに特別に割り当てたコンテキストのみが含まれます。特別に割り当てたコンテキストがないパーティションは包括的であり、コンテキストはラウンドロビン式に割り当てられます。すべてのパーティションにコンテキストを割り当てた場合、すべて排他的になります。ただし、パーティションに割り当てられていないコンテキストを後から追加する場合は、デフォルトでパーティション 0 に割り当てられます。
- Config URL：コンテキスト コンフィギュレーションの場所を URL として指定します。リストでファイル システムのタイプをクリックして、サーバ（リモート ファイル システムの）、パス、ファイル名をボックスに入力します。FTP の場合、URL は次の形式になります。

  ftp://server.example.com/configs/admin.cfg

  ファイルがまだ存在しない場合は、FWSM がそのファイルを作成します。
- 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コンテキストにフェールオーバー グループを設定します。
- Firewall Mode：ファイアウォール モードを示します。「ルーテッド」または「透過」です。管理コンテキストでないコンテキストのファイアウォール モードを変更するには、Security Contexts ペインの Change Firewall Mode ボタンを表示してください。デフォルトは、ルーテッド モードです。
- Description：（オプション）コンテキストの説明を入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Add/Edit Interface Allocation ダイアログボックスで、インターフェイスをコンテキストに割り当て、インターフェイス パラメータを設定できます。

フィールド

- Vlans：コンテキストに割り当てるインターフェイスを指定します。
  - Vlan Range：インターフェイス ID またはインターフェイス ID の範囲を設定します。インターフェイスを 1 つだけ指定する場合は、最初のリストで ID をクリックします。範囲を指定する場合は、次のリストで最後の ID（ある場合）をクリックします。透過ファイアウォール 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。
- Aliased Names：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は英字、最後は英字または数字にします。間の文字として使用できるのは、英字、数字、下線だけです。このボックス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 ボックスで設定できます。マルチコンテキストで同じ名前を使用できます。また、マルチコンテキストの VLAN ID は、指定した名前と同じにすることも、違う名前にすることもできます。同じコンテキストの異なる VLAN ID に同じ名前を使用することはできません。
  - Range：エイリアス名の拡張子を数字で設定します。複数のインターフェイスを範囲指定する場合、名前の後に追加する数字を範囲で入力できます。
- Show Hardware Properties in Context：エイリアス名が設定されている場合でも、コンテキスト ユーザはコンテキスト内の VLAN ID を表示できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

デバイス プロパティの設定

ここでは、次の項目について説明します。

Device Administration

Device Administration で、FWSM に基本的なパラメータを設定できます。ここでは、次の項目について説明します。

Banner

Banner ペインで、当日のお知らせメッセージ、ログイン、セッション バナーを設定できます。

バナーを作成するには、該当するフィールドにテキストを入力します。テキストに入力したスペースはそのまま表示されます。タブは ASDM インターフェイスで入力します。コマンドラインから入力できません。トークンの $(domain) および $(hostname) は、FWSM のドメイン名およびホスト名に置き換えられます。

$(hostname) および $(domain) トークンを使用すると、特定のコンテキストで指定したホスト名とドメイン名を画面に表示できます。$(system) トークンを使用して、特定のコンテキストのシステム スペースで設定したバナーを画面に表示できます。

バナーが複数行の場合、行ごとに入力したテキストが既存のバナーの最後に追加されます。テキストが空の場合、復帰記号（CR）がバナーに追加されます。RAM やフラッシュ メモリの容量が許す限り、バナーの長さに制限はありません。ASCII 文字のみ使用できます。改行（Enter キー。2 文字に相当）も使用できます。

Telnet または SSH で FWSM にアクセスしたとき、システム メモリが不足してバナー メッセージを表示できなかったり、バナー メッセージを表示するときに TCP 書き込みエラーが発生したりするとセッションは終了します。

バナーを置き換えるには、該当するフィールドの内容を変更して **Apply** をクリックします。バナーをクリアするには、該当するフィールドの内容をクリアして **Apply** をクリックします。

システム コンテキストでは ASDM ペインから**バナー** コマンドを使用できませんが、**Tools** > **Command Line Interface** から設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Prompt

CLI Prompt ペインでは、CLI プロンプトに表示される情報およびそれらの情報の表示順序を設定できます。

プロンプトに情報を追加する機能によって、モジュールが複数あるときにログインしているモジュールを一目で確認することができます。これは、フェールオーバー中、両方のモジュールに同じホスト名がある場合に重要です。

プロンプトを設定するには、Available Prompts メニューから domain、priority、slot または state を選択するか、または Selected Prompts メニューから context または hostname を選択します。

Selected Prompts はデフォルト設定です。Available Prompts は、Add ボタンまたは Remove ボタンをクリックして追加または削除できるキーワードです。Selected Prompts および Available Prompts は、プロンプトを強調表示して Add ボタンまたは Remove ボタンをクリックすることで入れ替えることができます。

プロンプトを選択したら、Move Up ボタンまたは Move Down ボタンを使用して表示順序を決定します。プロンプトをプレビューするには、CLI Prompt Preview フィールドを確認します。その後、**Apply** または **Reset** をクリックします。

フィールド

Available Prompts メニュー

- context (Multiple mode only)：現在のコンテキストを表示するプロンプトを設定します。
- domain：ドメインを表示するプロンプトを設定します。
- priority：「failover lan unit」設定を表示するプロンプトを設定します。
- slot：スロットの場所を表示するプロンプトを設定します（該当する場合）。
- state：現在のトラフィックの処理状態を表示するプロンプトを設定します。

Selected Prompts メニュー

- context (Multiple mode only)：現在のコンテキストを表示するプロンプトを設定します。
- hostname：ホスト名を表示するプロンプトを設定します。

プロンプトをプレビューするには、CLI Prompt Preview フィールドを確認します。その後、**Apply** または **Reset** をクリックします。

- Apply：ASDM での変更内容を FWSM に送信し、実行中のコンフィギュレーションに適用します。実行中のコンフィギュレーションのコピーをフラッシュ メモリに書き込むには、Save をクリックします。
- Reset：変更内容を破棄し、変更前に表示されていた情報、または ***Refresh*** か ***Apply*** を最後にクリックしたときに表示されていた情報に戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Threshold

CPU Threshold ペインでは、CPU 使用状況のモニタリングを設定できます。CPU 使用状況のポーリング間隔、および上昇しきい値を示す CPU 使用状況の割合を設定することができます。CPU 使用状況のモニタリングは、CPU Utilization Traps がイネーブルになっている場合にのみイネーブルになります。

フィールド

- Enable CPU Threshold and interval：CPU しきい値のモニタリングをイネーブルします。
- Monitoring Interval：CPU 使用状況のモニタリング間隔を設定します（60 ～ 3600 秒）。デフォルト値は 1 秒です。
- CPU Utilization Threshold：CPU 使用状況しきい値を設定します（10 ～ 100%）。デフォルト値は 10% です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Device ペインで、ホスト名とドメイン名を FWSM に設定できます。

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。

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 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。

FWSM は、ドメイン名を未修飾名に拡張子として追加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバに未修飾名「jupiter」を指定すると、セキュリティ アプライアンスは、この名前を「jupiter.example.com」に限定します。FWSM は、RSA キーの生成にもドメイン名を使用します。

フィールド

- FWSM Host Name：ホスト名を設定します。デフォルト ホスト名は FWSM です。
- Domain Name：ドメイン名を設定します。デフォルトのドメイン名は、default.domain.invalid です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Mode

FTP Mode ペインで、FTP モードをアクティブまたはパッシブに設定できます。FWSM がイメージ ファイルまたはコンフィギュレーション ファイルを FTP サーバにアップロードしたり、FTP サーバからダウンロードできるようになります。パッシブ FTP クライアントは、コントロール接続とデータ接続を両方とも起動できます。サーバはパッシブ モードでデータ接続の宛先になり、特定の接続の受信時にポート番号に応答します。

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に設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Rules

ICMP Rules ペインで、ICMP ルール テーブルを表示し、FWSM に ICMP でアクセスするすべてのホストまたはネットワークの許可 / 拒否を指定します。このテーブルでホストまたはネットワークを追加、変更すると、FWSM に送信された ICMP メッセージを許可または禁止できます。

ICMP ルールは、FWSM インターフェイスに ICMP トラフィックが着信した場合の制御方法を表示します。ICMP コントロール リストが設定されていない場合、FWSM は外部インターフェイスも含め、インターフェイスに着信した ICMP トラフィックをすべて許可します。ただし、デフォルトでは、FWSM はブロードキャスト アドレスへの ICMP エコー要求に応答しません。

(注) Security Policy ペインで ICMP トラフィックのアクセス ルールを設定すると、宛先のインターフェイスが保護されていても FWSM を*通過*ルートにできます。

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 の到達不能メッセージを拒否すると、ICMP の Path MTU Discovery 機能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場合があります。Path MTU Discovery 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 リストを設定すると、FWSM 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。したがって、最初に一致したエントリが許可の場合は、ICMP パケットはそのまま処理されます。最初に一致したエントリが拒否の場合または一致しなかった場合は、FWSM で ICMP パケットは破棄され、システム ログ メッセージが出力されます。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、**許可**が設定されているものとして処理されます。

フィールド

- Interface：ICMP アクセスが許可される FWSM 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の ICMP メッセージの許可 / 拒否を表示します。
- IP Address：アクセスを許可 / 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：アクセスを許可す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 タイプを一覧表示します。表 8-1 に示す ICMP タイプがサポートされます。
- Add：Add ICMP Rule ダイアログボックスが表示され、新規の ICMP ルールをテーブルの最後に追加できます。
- Insert Before：ICMP ルールを選択中のルールの前に追加します。
- Insert After：ICMP ルールを選択中の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 8-1　ICMP タイプ リテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench

表 8-1　ICMP タイプ リテラル（続き）

ICMP タイプ	リテラル
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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ICMP Rule ダイアログボックスで、ICMP ルールの追加または変更ができます。ICMP ルールでは、FWSM への ICMP アクセスが許可 / 拒否されるホストまたはネットワークのアドレスをすべて指定できます。

フィールド

- ICMP Type：ルールを適用する ICMP メッセージ タイプを指定します。表 8-2 に示す ICMP タイプがサポートされます。
- Interface：ICMP アクセスが許可される FWSM のインターフェイスを特定します。
- IP Address：アクセスを許可 / 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のすべての受信アドレスにアクションを適用します。
- Mask：アクセスを許可す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の ICMP メッセージの許可 / 拒否を指定します。
  - Permit：指定したホストまたはネットワークと、アクセス許可されたインターフェイスの ICMP メッセージを作成します。
  - Deny：指定したホストまたはネットワークと、ドロップされたインターフェイスの ICMP メッセージを作成します。

表 8-2　ICMP タイプ 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

次の表に、この機能を使用できるモードを示します。

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

Password

Password ペインで、ログイン パスワードとイネーブル パスワードを設定できます。

Telnet または SSH セッションを使用して FWSM に接続する場合、またはスイッチから FWSM のセッションに入る場合、ログイン パスワードを使用してユーザ EXEC モードにアクセスできます（Telnet または SSH の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、ログイン パスワードを使用しません。AAA Access ペインを参照してください）。

イネーブル パスワードでログインすると、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 ユーザ名で ASDM にアクセスする場合にも使用します。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。AAA Access ペイン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

- Enable Password：イネーブル パスワードを設定します。デフォルトでは空白になっています。
  - Change the privileged mode password：イネーブル パスワードを変更できます。
  - 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：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。この領域は Telnet Password になっていますが、このパスワードで Telnet、SSH およびセッションにアクセスできます。
  - Change the password to access the FWSM console：ログイン パスワードを変更できます。
  - 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Copy

Secure Copy ペインで、FWSM のセキュア コピー サーバをイネーブルにできます。SSH を利用する FWSM 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 サーバの実装には、次の制限事項があります。

- サーバはセキュア コピー接続の受け入れと終了はできますが、起動はできません。
- サーバは、ディレクトリの指定をサポートしていません。そのため、リモート クライアント アクセスで FWSM の内部ファイル参照はできません。
- サーバは、バナーをサポートしていません。
- サーバは、ワイルドカードをサポートしていません。
- SSH バージョン 2 で接続するには、FWSM 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：FWSM のセキュア コピー サーバをイネーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、発生した重要イベントを電子メールで通知する SMTP クライアントをイネーブル / ディセーブルにできます。ここで追加できるのは SMTP サーバの IP アドレスで、オプションとしてバックアップ サーバの IP アドレスも設定できます。ASDM は IP アドレスが有効かどうかをチェックしません。アドレスを正確に入力してください。

警告を受信する電子メール アドレスは、***Configuration*** > ***Properties*** > ***Logging*** > ***Email Setup*** で設定します。

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 アドレスを入力します。
- 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入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、SNMP 管理ステーションを監視するように FWSM を設定できます。

ネットワーク管理ステーションを PC またはワークステーションで実行し、スイッチ、ルータ、FWSM など、さまざまなタイプのデバイスのステータスとヘルスを監視する標準的な方法を SNMP で定義できます。

SNMP の用語

- Management station：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、管理対象デバイスの標準データベースを管理します。ハードウェアの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。
- Agent：SNMP コンテキストでは、管理ステーションがクライアント、FWSM で動作する SNMP エージェントがサーバになります。
- OID：SNMP 規格では、システム オブジェクト ID（OID）を設定して、管理ステーションが SNMP エージェントがあるネットワーク デバイスを一意に識別したり、ユーザに分かるように監視情報の発生元を表示したりします。
- MIB：エージェントは Management Information Databases（MIB; 管理情報データベース）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。MIB は製品ごとに定義され、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も MIB に定義されています。SNMP 管理ステーションから 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、管理目的で MIB データを変更する場合があります。

- Trap：エージェントはアラーム条件も監視します。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ただちに通知します。この通知は SNMP トラップとも呼ばれます。

SNMP

シスコの 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

FWSM は、次の SNMP MIB をサポートしています。

（注） FWSM は、Cisco syslog MIB のブラウジングはサポートしません。

- MIB-II の System グループと Interface 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。
- FWSM 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

FWSM 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。FWSM の CPU 使用状況を監視する際、HP OpenView などの SNMP 管理ソフトウェアを利用すると、ネットワーク管理者は容量プランを作成できます。

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、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、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 of Entity MIB を FWSM 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 of Entity MIB を FWSM 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 FWSM 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、FWSM 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、FWSM ではサポートされていません。

- cpmCPUTotal5secRev
- cpmCPUTotal1minRev
- cpmCPUTotal5minRev

フィールド

- Community string (default)：パスワードを入力します。SNMP 管理ステーションは FWSM に要求を送信するとき、このパスワードを使用します。SNMP のコミュニティ ストリングは、SNMP 管理ステーションと管理対象ネットワーク ノード間で共有される秘密情報です。FWSM はパスワードを参照して、受信する SNMP 要求が有効かどうかを決定します。パスワードは、大文字と小文字が区別される最大 32 文字の値です。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：FWSM システム管理者の名前を入力します。テキストは最大 127 文字で、大文字と小文字を区別します。スペースは使用できますが、連続するスペースは 1 桁のスペースに縮められます。
- Security Appliance Location：FWSM の場所を指定します。テキストは最大 127 文字で、大文字と小文字を区別します。スペースは使用できますが、連続するスペースは 1 桁のスペースに縮められます。
- 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：イベントを設定すると、SNMP トラップを利用して通知できます。
- SNMP Management Station：
  - Interface：SNMP 管理ステーションが存在する FWSM のインターフェイス名を表示します。
  - IP Address：SNMP 管理ステーションの IP アドレスを表示します。FWSM はこのアドレスを使ってトラップ イベントを送信したり、要求またはポーリングを受信したりします。
  - Community string：管理ステーションでコミュニティ ストリングを指定しない場合、Community String (default) フィールドの設定値が使用されます。
  - 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の通信方式を表示します。ポーリングのみ、トラップのみ、ポーリングとトラップがあります。ポーリングとは、一定間隔で繰り返し送信される管理ステーションの要求を FWSM が待つことをいいます。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 ポートは 162 です。
- Add：Add SNMP Host Access Entry が開き、次のフィールドを設定できます。
- 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** または **Trap** を選択します。両方を選択することもできます。
- UDP Port：SNMP ホストの UDP ポートです。このフィールドを指定すると、SNMP ホストのデフォルト UDP ポート番号 162 が上書きされます。
- Help：詳細を表示します。

- Edit：Edit SNMP Host Access Entry ダイアログボックスが開き、追加の場合と同じフィールドが表示されます。
- Delete：選択した項目を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Host Access Entry

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、次の手順を実行します。

1. **Add** をクリックし、SNMP Host Access Entry ダイアログボックスを開きます。
2. Interface Name から 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。デフォルトは 162 です。
5. SNMP ホストの Community String パスワードを入力します。管理ステーションでコミュニティストリングを指定しない場合、SNMP Configuration ペインの Community String (default) フィールドに設定した値が使用されます。
6. **Poll** または **Trap** をクリックして選択します。両方を選択することもできます。
7. 前のペインに戻るには、次のいずれかをクリックします。
   - **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、Edit SNMP Host Access Entry を開きます。
3. Interface Name から 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 Community String パスワードを入力します。管理ステーションでコミュニティストリングを指定しない場合、SNMP Configuration ペインの 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。デフォルトは 162 です。
7. **Poll** または **Trap** をクリックして選択します。両方を選択することもできます。
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、次のいずれかをクリックします。
   - **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 テーブルの項目を選択します。
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 アップデートの送信先にする UDP ポートを入力します。デフォルトは 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します。ポーリングとは、一定間隔で繰り返し送信される管理ステーションの要求を FWSM が待つことをいいます。
  - Trap：トラップ情報を送信します。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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Trap Configuration

トラップ

トラップはブラウジングと異なり、特に要求しなくても、リンク アップ、リンク ダウン、syslog イベントなど特定のイベントが発生すると、管理対象デバイスから管理ステーションに「コメント」が送信されます。

FWSM の SNMP オブジェクト ID（OID）が、FWSM から送信される SNMP イベントに表示されます。FWSM のシステム OID は、SNMP のイベント トラップと SNMP の mib-2.system.sysObjectID に表示されます。

FWSM で実行される SNMP サービスには、2 つの異なる機能があります。

- 管理ステーション（または SNMP クライアント）が送信した SNMP 要求に応答を返します。
- 管理ステーション、または FWSM の通知を受信するように登録されたその他のデバイスに、トラップ（イベント通知）を送信します。

FWSM は、3 タイプのトラップをサポートします。

- ファイアウォール
- ジェネリック
- syslog

トラップの設定

SNMP Trap Configuration を開くと、次のフィールドが表示されます。

- Standard SNMP Traps：送信する標準トラップを選択します。
  - Authentication：認証の標準トラップをイネーブルにします。
  - Cold Start：コールド スタートの標準トラップをイネーブルにします。
  - Link Up：リンク アップの標準トラップをイネーブルにします。
  - Link Down：リンク ダウンの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）が取り外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。
  - Alarm Asserted：Entity MIB からアラーム アサート通知を受信した場合のトラップ通知をイネーブルにします。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 モードの管理コンテキストでのみ使用できます。
  - Alarm Clear：Entity MIB からアラーム クリア通知を受信した場合のトラップ通知をイネーブルにします。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 モードの管理コンテキストでのみ使用できます。
  - Redundancy Switchover：フェールオーバーの状態の変更に対する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 が開始した場合のトラップをイネーブルにします。
  - Stop：IPSec が停止した場合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 アクセスを開こうとしたセッション数が、設定されているセッション数の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。
- Resource Traps：リソース制限トラップをイネーブルにします。
  - Resource Limit Reached：任意のリソースがリソース マネージャの制限に達した場合のトラップ通知をイネーブルにします。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 モードの管理コンテキストでのみ使用できます。
  - Rate Limit Reached：レート制限されたリソースが制限に達した場合のトラップ通知をイネーブルにします。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 モードの管理コンテキストでのみ使用できます。
- NAT Traps：NAT 関連のトラップをイネーブルにします。
  - Packet discarded：使用可能なアドレス変換スロットがないためにパケットが破棄された場合のトラップ通知をイネーブルにします。
- CPU Utilization Traps：CPU しきい値のトラップをイネーブルにします。
  - CPU rising threshold reached：CPU 使用状況が上昇しきい値制限に達した場合のトラップ通知をイネーブルにします。

- CPU Utilization and Monitoring Interval：CPU 使用状況のモニタリングを設定します。
  - Configure threshold and interval：CPU 使用状況のモニタリングの間隔と上昇しきい値を設定します。
  - CPU Utilization threshold：CPU 上昇しきい値を示す CPU 使用状況の割合を入力します。10 ～ 100 の範囲の値を指定できます。
  - Monitoring interval：FWSM が CPU 使用状況のモニタリング間隔を秒単位で入力します。60 ～ 3600 の範囲の値を指定できます。
- Syslog：syslog 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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Server

TFTP Server ペインで FWSM を設定すると、TFTP を利用してファイル サーバにコンフィギュレーションを保存できます。

（注） このペインでは、サーバにファイルを書き込みません。このペインで FWSM を TFTP サーバ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 FWSM

TFTP は RFC783 および RFC1350 Rev. 2 で規定されているシンプルなクライアント / サーバ ファイル転送プロトコルです。このパネルで FWSM を TFTP *クライアント*に設定すると、実行コンフィギュレーションのコピーを TFTP *サーバ*に転送できます。転送するには、***File*** > ***Save Running Configuration to TFTP Server*** をクリックするか ***Tools*** > ***Command Line Interface*** をクリックします。この方法でコンフィギュレーション ファイルをバックアップし、複数の FWSM にプロパゲートできます。

configure net コマンドで TFTP サーバの IP アドレスを指定し、**tftp-server** コマンドでサーバのインターフェイスとパス / ファイル名を指定すると、そ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。この情報を実行コンフィギュレーションに設定すれば、ASDM で ***File*** > ***Save Running Configuration*** をクリックするだけで、**write net** コマンドで TFTP サーバにファイル転送できます。

FWSM でサポートされる TFTP サーバは 1 つだけです。TFTP サーバのフル パスを **Configuration > Properties > Device Administration > TFTP Server** で指定します。ここで設定すると、CLI の **configure net** および **write net** コマンドにコロン（:）で IP アドレスを指定できます。ただし、FWSM と TFTP サーバの通信に必要な、中間デバイスの認証またはコンフィギュレーションは、この機能とは別に実行されます。

show tftp-server 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-server** コマンド文を一覧表示できます。**no tftp server** コマンドで、サーバ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：クリックして選択すると、コンフィギュレーションに含まれる TFTP サーバの設定がイネーブルになります。
- Interface Name：FWSM のインターフェイス名を選択します。このインターフェイスで TFTP サーバの設定を使用します。
- IP Address：TFTP サーバの IP アドレスを入力します。
- Path：TFTP サーバ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が書き込まれます。

  TFTP サーバのパスの例：**/tftpboot/**FWSM/**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、使用するソフトウェア バージョンの FWSM の技術マニュアルを参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ペインで、ローカル ユーザ データベースを管理できます。ローカル ユーザ データベースは、次の機能で使用されます。

- ユーザごとの ASDM アクセス

  デフォルトでは、空白のユーザ名とイネーブル パスワードを指定して ASDM にログインできます（「Password」を参照）。ただし、（空白ユーザ名を使用しないで）ログイン画面でユーザ名とパスワードを入力すると、ASDM はローカル データベースをチェックして照合します。

（注） ローカル データベースを参照する HTTP 認証を設定できますが（「Authentication」を参照）、この機能はデフォルトで常にイネーブルです。RADIUS または TACACS+ サーバを認証に使用する場合は、HTTP 認証だけを設定します。

- Telnet および SSH 認証（「Authentication」を参照）。

  システム コンフィギュレーションでユーザ アカウントを設定することはできません。ただし、管理コンテキストで Telnet の認証をイネーブルにすると、システムの Telnet 認証もイネーブルになります。セッション /Telnet をスイッチから FWSM に変更する場合は、管理コンテキストのユーザ アカウントを使用します。

- **enable** コマンド認証（「Authentication」を参照）。

  CLI アクセスのみの設定です。ASDM ログインには影響しません。
- コマンド認可（「Authorization」を参照）。

  ローカル データベースを使用するコマンド認可をイネーブルにすると、セキュリティ アプライアンス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確認します。コマンド認可がディセーブルの場合、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 0 または 15 のどちらかになっています。ASDM にはイネーブルにできる特権レベルがあらかじめ定義されています。指定できるレベルは、15（管理）、5（読み取り専用）、3（監視専用）の 3 種類です。あらかじめ定義されたレベルを使用するには、3 種類の特権レベルのいずれかにユーザを設定します。

（注） CLI へのアクセス権を取得できるユーザを特権 EXEC モードに入れないようにするには、そのユーザをローカル データベースに追加する際にコマンド認可をイネーブルにする必要があります。コマンド認可を行わないと、ユーザは、特権レベルが 2 以上（2 がデフォルト）の場合、CLI で自分のパスワードを使用して特権モード（およびすべてのコマンド）にアクセスできます。あるいは、コンソール アクセスに RADIUS または TACACS+ 認証を使用して、ユーザが login コマンドを使用できないようにすることも、すべてのローカル ユーザをレベル 1 に設定して、システム イネーブル パスワードを使用して特権モードにアクセスできるユーザを制御することもできます。

- ネットワーク アクセス認証
- VPN クライアント認証（リモート管理のみ）

ネットワーク アクセス認可には、ローカル データベースは使用できません。

（Password でなく）このペインでイネーブル パスワードを設定するには、ユーザ名 enable_15 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。

CLI で他のイネーブル レベル パスワードを設定すると（**enable password 10** など）、そのユーザ名は enable_10 のようになります。

フィールド

- User Name カラム：ここに示すパラメータを適用するユーザ名を指定します。
- Privilege (Level) カラム：ユーザに設定する特権レベルを指定します。特権レベルは、ローカル コマンド認可で使用されます。詳細については、「Authorization」を参照してください。
- Add ボタン：Add User Account ダイアログボックスを表示します。
- Edit ボタン：Edit User Account ダイアログボックスを表示します。
- Delete ボタン：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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 タブ

このタブで指定したパラメータでユーザ アカウントを識別し、追加または変更ができます。変更は、OK をクリックすると User Accounts テーブルにただちに表示されます。

フィールド

- Username：アカウントのユーザ名を指定します。
- Password：ユーザの一意のパスワードを指定します。パスワードは 4 文字以上にする必要があります。また、最大 32 文字です。パスワードは、大文字と小文字を区別します。フィールドには、アスタリスクだけが表示されます。

（注） セキュリティ保護のため、パスワードは 8 文字以上にすることをお勧めします。

- Confirm Password：ユーザ パスワードを再入力して確認するように求めます。フィールドには、アスタリスクだけが表示されます。
- Privilege Level リスト：ローカル コマンド認可でユーザに適用する特権レベルを選択します。0（最低）～ 15（最高）の範囲の値を指定します。詳細については、「Authorization」を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Auto Update ペインで FWSM の管理リモート サーバを設定すると、リモート サーバで Auto Update 仕様をサポートできます。Auto Update を利用すると、FWSM 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、FWSM 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、中央から、リモート管理アプリケーションにより FWSM 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 FWSM 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、FWSM 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 FWSM 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 FWSM 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 FWSM に設定する必要があります。

FWSM の Auto Update 機能は、Cisco Secure Policy Manager などの製品と併用できますが、サードパーティ製品で FWSM を管理することもできます。

特記事項

- FWSM のコンフィギュレーションが Auto Update サーバで更新されても、ASDM には通知されません。**Refresh** または **File > Refresh ASDM with the Running Configuration on the Device** をクリックして、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、FWSM は SSL を使用します。その場合、FWSM 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、次のフィールドが表示されます。

- Enable Auto Update：FWSM を Auto Update サーバから設定できるようにします。

HTTP(S) server：Auto Update サーバの場所を設定できます。

- Verify Certificate：Auto Update サーバが返した証明書を、認証局（CA）のルート証明書と照合するように確認します。その場合、Auto Update サーバと FWSM は、同じ CA を使用する必要があります。
- Protocol：Auto Update サーバが FWSM との通信に使用するプロトコルを選択します。選択肢は http と https です。
- Server：Auto Update サーバの名前または IP アドレス。FWSM がホスト名を解決できる場合にのみ名前を指定します。
- 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。

- Port：Auto Update サーバで接続するポートを指定します。HTTP のデフォルトは TCP ポート 80、HTTPS のデフォルトは TCP ポート 443 です。
- Path：Auto Update サーバのパスを入力します。
- 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。

Timeout：FWSM 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。

- Enable Timeout Period：FWSM は、Auto Update サーバから応答を受信しなかった場合、タイムアウトします。
- Timeout Period (Minutes)：Auto Update サーバから応答がなかった場合の FWSM のタイムアウト時間（分単位）を指定します。

Polling Parameters：FWSM 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 Period (minutes)：FWSM 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）。
- Retry Period (minutes)：サーバのポーリングに失敗した場合、FWSM 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：FWSM 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。
- Advanced：Advanced Auto Update Properties を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Autoupdate Properties

フィールド

- Use Device ID：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、FWSM が Auto Update サーバで一意に識別できます。
- Device ID：使用するデバイス ID のタイプを入力します。
  - Hostname：ホストの名前です。
  - Serial Number：デバイスのシリアル番号です。
  - IP Address on：選択したインターフェイスの IP アドレス。FWSM 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：選択したインターフェイスの MAC アドレス。FWSM を Auto Update サーバが一意に識別する場合に使用します。
  - User Input：一意のユーザ ID です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

DHCP サービスと DNS サービスの設定

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。FWSM は、DHCP サーバまたは DHCP リレー サービスを FWSM 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することができます。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向こう側に位置する外部 DHCP サーバに渡します。

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 Relay
- DHCP Server
- DNS Client

DHCP Relay

DHCP Relay ペインでは、FWSM での 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向こう側に位置する外部 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 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。インターフェイスごとに追加の DHCP リレー サーバを設定できます。インターフェイス固有の DHCP リレー サーバを設定すると、そのインターフェイスで受信した DHCP 要求は指定のサーバに送信されます。インターフェイス固有のサーバが設定されていない場合は、グローバル サーバが使用されます。

制約事項

- DHCP リレー 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 FWSM 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内に少なくとも 1 つの DHCP リレー グローバル サーバまたは DHCP リレー インターフェイス 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：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：インターフェイス名を表示します。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。
- DHCP Relay：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 エージェントが設定されているかどうかが示されます。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 Servers：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。DHCP リレー エージェントがイネーブルになっているインターフェイス上で DHCP 要求を受信すると、インターフェイス固有のサーバが定義されていない限り、それらの要求はグローバル サーバに転送されます。

- Server：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 サーバの設定を編集できます。
- Interface：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 サーバを指定できます。FWSM では、DHCP リレー サーバを 4 つまで定義できます。すでに 4 つの DHCP リレー サーバが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 サーバの設定を編集できます。
- Delete：選択した DHCP リレー 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 FWSM 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許可する時間を秒単位で指定します。有効値の範囲は 1 ～ 3600 秒です。デフォルト値は、60 秒です。

DHCP Relay Interface Servers：各インターフェイスの DHCP サーバのリストの設定用のフィールドが含まれます。リレー エージェントがイネーブルになっているインターフェイスで受信した DHCP 要求、およびそのインターフェイスに定義された 1 つ以上のサーバは、グローバル サーバではなくインターフェイス固有のサーバに転送されます。

- Interface：インターフェイス固有の DHCP リレー サーバが定義されているインターフェイスの名前を表示します。
- Servers：インターフェイスで受信した DHCP 要求に使用される DHCP サーバの IP アドレスを一覧表示します。
- Add：新しい DHCP リレー サーバのセットを追加します。
- Edit：DHCP リレー サーバのリストを編集します。
- Delete：選択した DHCP リレー サーバのリストを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 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 FWSM 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 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 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Relay - Add/Edit DHCP Server

DHCP Relay - Add DHCP Server ダイアログボックスで新しい DHCP リレー 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 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 DHCP リレー サーバを定義することはできません。

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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 DHCP Relay Server

特定のインターフェイスで DHCP 要求を受信したときに、DHCP リレー エージェントがインターフェイスごとに使用する必要がある DHCP サーバを定義します。

フィールド

- Interface：使用するリレー エージェントに DHCP サーバを定義しているインターフェイスを選択します。
- Server to Add：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。
- Add：DHCP サーバのリストにサーバを追加します。
- Delete：選択したサーバをリストから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Server

DHCP Server ペインでは、FWSM のインターフェイスを DHCP サーバとして設定できます。FWSM 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 DHCP サーバを設定することはできません。DHCP リレーの詳細については、「DHCP Relay」を参照してください。

フィールド

- Interface：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、DHCP アドレス プールを選択したインターフェイスに割り当てることができます。
- DHCP Enabled：インターフェイス上で DHCP がイネーブル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：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。
- 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。
- Ping Timeout：アドレスの競合を避けるために、FWSM 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 ボックスでは、FWSM 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。
- 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。
- Other DHCP Options：オプションの DHCP パラメータが含まれます。
  - Enable Autoconfiguration on interface：DHCP 自動コンフィギュレーショ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。

    DHCP 自動コンフィギュレーションにより、DHCP サーバは、指定したインターフェイス上で実行している DHCP クライアントから取得した DHCP サーバ、ドメイン名、WINS サーバの各情報を DHCP クライアントに提供します。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。
  - Enable Autoconfiguration on interface：DNS、WINS、およびドメイン名パラメータを提供する DHCP クライアントを実行しているインターフェイスを指定します。
  - DNS Server 1：（オプション）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：（オプション）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：（オプション）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。
  - Primary WINS Server：（オプション）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：（オプション）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。
  - 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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、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 プールを指定します。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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 パラメータを設定します。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、TFTP サーバ情報を Cisco IP Phone および Cisco IOS ルータに提供します。

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 Server 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。
  - Select 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のみが表示され、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のみ使用可能です。たとえば、DHCP Option 2（Time Offset）を選択した場合、このオプションに指定できるのは 16 進数値のみです。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 オプション：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のみ使用可能です。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：（オプション）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 Option 2（Time Offset）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。接頭辞の 0x 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：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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ペインでは、FWSM に 1 つ以上の DNS サーバを指定できます。したがって、サーバ名を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（Add/Edit Trustpoint Configuration > Enrollment Settings タブ および Add/Edit Trustpoint Configuration > CRL Retrieval Policy タブ を参照）。サーバ名を定義するその他の機能（AAA など）は、DNS 解決をサポートしていません。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 Servers：DNS サーバ リストを管理します。アドレスは最大 6 つまで指定できます。FWSM は、応答を受け取るまで順番に各 DNS サーバを試行します。DNS サーバを追加する前に、DNS Lookup グループ ボックス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：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。
- DNS Server Parameters：タイムアウトを設定します。
  - Timeout：リスト内の次の DNS サーバを試行するまでの時間を 1 ～ 30 秒の間で指定します。デフォルトは 2 秒です。FWSM がサーバのリストを再試行するごとに、このタイムアウトは 2 倍になります。
  - Retries：DNS　サーバのリストの各サーバを試行する回数を指定します。デフォルトは、2 回です。
- 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：すべてのインターフェイス名を一覧表示します。
  - DNS Enabled：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 で示します。
  - Disable：選択したインターフェイスの DNS 検索をイネーブルにします。
  - 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

AAA サーバの設定

この章には、次の項があります。

AAA について

この章では、AAA について説明し、AAA サーバのサポートに関する情報、および ASDM における AAA の実装場所に関する情報について説明します。次の項目を取り上げます。

AAA の概要

AAA によって、FWSM が、ユーザが誰か（認証）、ユーザが何を実行できるか（認可）、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。認証のみで使用することも、認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。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングのみで使用することも、認証および認可とともに使用することもできます。

AAA には、ユーザ アクセスに対して、ACL のみ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内部インターフェイスのサーバ上の Telnet にアクセスできるようにする ACL を作成できます。一部のユーザのみがサーバにアクセスできるようにするが、そのユーザの IP アドレスを常に認識しているとは限らない場合、AAA を使用すると、認証済みまたは認可済み（あるいはその両方）のユーザのみが FWSM を介してアクセスすることが許可されるようにできます（Telnet サーバもまた、認証を実行します。FWSM は、認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）。

- **認証の概要**：認証では、ユーザ ID に基づいてアクセス権が許可されます。認証では、有効なユーザ クレデンシャルを要求してユーザ ID を確立します。このクレデンシャルは通常、ユーザ名とパスワードです。
- **認可の概要**：認可では、ユーザ認証後、ユーザごとにアクセスを制御します。認可では、各認証済みユーザが使用可能なサービスおよびコマンドを制御します。認可をイネーブルにしていない場合は、認証のみで、すべての認証済みユーザがサービスに同じようにアクセスできます。

  認可で提供される制御が必要な場合、広範な認証ルールを設定して、詳細な認可が設定できます。たとえば、外部ネットワーク上のサーバにアクセスする内部ユーザを認証して、特定のユーザがアクセスできる外部サーバを認可によって制限します。

  FWSM はユーザあたり最初の 16 個の認可要求をキャッシュするので、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、FWSM は認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、FWSM 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、そのセッションで FWSM を経由したバイト数、使用されたサービス、セッションの継続時間が含まれます。

AAA の準備

AAA サービスは、LOCAL データベース、または少なくとも 1 つの AAA サーバの使用に依存します。また、AAA サーバが提供するほとんどのサービスに対するフォールバックとして LOCAL データベースを使用することもできます。AAA を実装する前に LOCAL データベースを設定するとともに、AAA サーバ グループとサーバ群を設定する必要があります。

LOCAL データベースおよび AAA サーバの設定方法は、FWSM がサポートする AAA サービスによって異なります。AAA サーバを使用するかどうかに関係なく、管理アクセスをサポートするユーザ アカウントを使用して LOCAL データベースを設定する必要があります。これは、誤ってロックアウトされないためであると同時に、AAA サーバにアクセスできないときに、希望によりフォールバック方式を提供するためでもあります。詳細については、「LOCAL データベース」を参照してください。

表 10-1 では、AAA サーバ タイプごと、および LOCAL データベースごとの AAA サービスのサポートの要約を示しています。LOCAL データベースの管理は、Configuration > Properties > Device Administration > User Accounts ペインでユーザ プロファイルを設定して行います。AAA サーバ グループの確立は、Configuration > Properties > AAA Setup > AAA Server Groups ペインで行います。Configuration > Properties > AAA Setup > AAA Servers ペインで、個別の AAA サーバをサーバ グループに追加します。

表 10-1　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**
認証							
VPN ユーザ[1]	あり	あり	あり	あり	あり	あり	なし
ファイアウォール セッション	あり	あり	あり	なし	なし	なし	なし
管理者	あり	あり	あり	なし	なし	なし	なし
認可							
VPN ユーザ [1]	あり	あり	なし	なし	なし	なし	あり
ファイアウォール セッション	なし	あり[2]	あり	なし	なし	なし	なし
管理者	あり[3]	なし	あり	なし	なし	なし	なし
アカウンティング							
VPN 接続 [1]	なし	あり	あり	なし	なし	なし	なし
ファイアウォール セッション	なし	あり	あり	なし	なし	なし	なし
管理者	なし	あり	あり	なし	なし	なし	なし

1. VPN は、管理接続のみで使用でき、ASDM で設定することはできません。
2. ファイアウォール セッションの場合、RADIUS 認可はユーザ固有の ACL でのみサポートされます。この ACL は RADIUS 認証応答で受信または指定されます。
3. ローカル コマンド認可は、特権レベルに限りサポートされます。

LOCAL データベース

FWSM 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。

- User Profiles：ユーザ プロファイルには、少なくともユーザ名が含まれています。通常、パスワードはオプションであっても、各ユーザ名に割り当てられます。また、ユーザ プロファイルでは、ユーザごとの VPN アクセス ポリシーも指定されます。ユーザ プロファイルは、Configuration > Properties > Device Administration > User Accounts ペインを使用して管理できます。
- Fallback Support：ローカル データベースは、コンソールに対するフォールバック方式として機能し、コマンド認可、VPN 認証および認可に対するパスワード認証をイネーブルにします。この動作は、FWSM 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。この対処により、透過フォールバックがサポートされます。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。

FWSM での AAA の実装

ここでは、次の項目について説明します。

デバイス管理のための AAA

次のような、FWSM へのすべての管理接続を認証できます。

- Telnet
- SSH
- ASDM
- VPN 管理アクセス

また、イネーブル モードを入力しようとしている管理者も認証できます。さらに、管理コマンドを認可できます。管理セッションのアカウンティング データ、およびアカウンティング サーバに送信された、セッション中に発行済みのコマンドのアカウンティング データを保持できます。

Configuration > Properties > Device Access > AAA Access ペインを使用して、AAA をデバイス管理用に設定できます。

ネットワーク アクセス用の AAA

Configuration > Security Policy > AAA Rules ペインを使用して、ファイアウォールを通過するトラフィックの認証、認可、アカウンティングのルールの設定ができます。作成するルールはアクセス ルールに類似していますが、定義したトラフィックの認証、認可、アカウンティングを実行するかどうかを指定する点、また、AAA サービス要求の処理に FWSM が使用する AAA サーバ グループを指定する点が異なります。

AAA のセットアップ

AAA Setup ペインでは、AAA サーバ グループ、AAA サーバ、および認証プロンプトを設定できます。ここでは、次の項目について説明します。

- AAA Server Groups
- AAA Servers
- Auth. Prompt

AAA Server Groups

AAA Server Groups ペインでは、FWSM が各グループに表示されたサーバとの通信に使用する AAA サーバ グループとプロトコルを設定できます。外部グループに個別のサーバを設定する必要があります。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には、「AAA Servers」を参照してください。

シングルモードでは最大 15 のグループを、マルチモードでは最大 4 つのグループを指定できます。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き、アクセスされるサーバは一度に 1 つだけです。指定したサーバから、応答があるまで順に 1 つずつアクセスしていきます。

AAA アカウンティングが有効になっている場合、同時アカウンティングを設定していない限り、アカウンティング情報が送られるのはアクティブ サーバに対してだけです。

AAA サービスの概要については、「AAA のセットアップ」を参照してください。

フィールド

（注）　AAA Server Groups テーブルで任意の行をダブルクリックすると、Edit AAA Server Group 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、AAA Server Group 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。

カラムの先頭をクリックすると、そのカラムの内容に従って、テーブルの行が英数字順に並び替わります。

- Server Group：選択したサーバ グループのシンボリック名を指定します。
- Protocol：グループのサーバがサポートする AAA プロトコルが一覧表示されます。
- Accounting Mode：同時モード アカウンティングまたはシングルモード アカウンティングを選択します。シングルモードでは、FWSM はアカウンティング データを 1 つのサーバにのみ送信します。同時モードでは、FWSM 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：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のみ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：グループ内の最後のサーバをディセーブルにしてから、すべてのサーバを再度アクティブにするまでの経過時間を分数で指定します。このパラメータは、Depletion モードでのみ適用されます。
- Max Failed Attempts：応答のないサーバを非アクティブと宣言する前に許可される接続試行失敗の回数を指定します。

- Add：Add AAA Server Group ダイアログボックスが表示されます。
- Edit：Edit AAA Server Group ダイアログボックスを表示します。ただし、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：現在選択しているサーバ グループ エントリをサーバ グループ 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Server Group

Add/Edit AAA Server Group ダイアログボックスは、AAA Server Group ペインで **Add** または **Edit** ボタンをクリックしたときに表示されます。これによって、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：サーバ グループの名前を指定します。
- Protocol：グループのサーバでサポートされているプロトコルを指定します。サポートされているプロトコルは次のとおりです。
  - RADIUS
  - TACACS+
  - NT Domain
  - SDI
  - Kerberos
  - LDAP
- Accounting Mode：同時モード アカウンティングまたはシングルモード アカウンティングを選択します。
  - Single：FWSM は、アカウンティング データをサーバ 1 つだけに送信します。
  - Simultaneous：FWSM 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：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：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のみ再アクティブ化されます。
  - Timed：30 秒のダウン タイムの後、障害が発生したサーバは再アクティブ化されます。
- Dead Time：グループ内の最後のサーバをディセーブルにしてから、すべてのサーバを再度アクティブにするまでの経過時間を分数で指定します。このボックスは、Timed モードでは使用できません。
- Max Failed Attempts：応答がないサーバを非アクティブと宣言するまでに許可される接続試行失敗の回数（1 ～ 5）を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 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したり、ログイン試行の最大失敗回数を設定したりすることができます。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、認証に LOCAL データベースが使用されているときのみ適用されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Servers

AAA Servers ペインでは、既存の AAA サーバ グループに AAA サーバを追加および設定できます。サーバ グループを設定するには、「AAA Server Groups」を参照してください。このサーバには、RADIUS、TACACS+、NT、SDI、Kerberos、または LDAP サーバを指定できます。

AAA サービスの概要については、「AAA のセットアップ」を参照してください。

フィールド

- Server Group (Protocol)：サーバ グループが使用するサーバ グループ名と AAA プロトコルを指定します。
- Interface：認証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 IP Address：AAA サーバの IP アドレスを指定します。
- Timeout：タイムアウト間隔を秒数で指定します。この時間に達すると、FWSM はプライマリ AAA サーバに対する要求の送信を放棄します。スタンバイ AAA サーバがある場合、FWSM はバックアップ サーバに要求を送信します。
- Add：新しい AAA サーバをリストに追加します。
- Edit：すでにリストに存在する AAA サーバのパラメータを変更します。
- Delete：AAA サーバをリストから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Server

Add/Edit AAA Server ダイアログボックスでは、新しい AAA サーバを既存のグループに追加したり、または既存の AAA サーバのパラメータを変更したりします。

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：Configuration > Properties > AAA Setup > AAA Server Groups で設定されているとおりに、サーバ グループの名前を指定します。
- 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 IP Address：AAA サーバの IP アドレスを指定します。
- Timeout：タイムアウト間隔を秒数で指定します。この時間に達すると、FWSM はプライマリ AAA サーバに対する要求の送信を放棄します。スタンバイ AAA サーバがある場合、FWSM はバックアップ サーバに要求を送信します。
- RADIUS Parameters：RADIUS サーバの使用に必要なパラメータを指定します。選択したサーバ グループが RADIUS を使用するときにのみ、この領域が表示されます。
  - 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。最小時間は 1 秒です。デフォルト時間は 10 秒です。最大時間は 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 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、このデフォルトは 1812 への変更が必要になる場合があります。

  - Server Accounting Port：ユーザ アカウンティングに使用するサーバ ポートを指定します。デフォルト 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鍵（「共有秘密情報」とも呼ばれます）を指定します。この秘密鍵では、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。FWSM は、サーバ秘密鍵を使用して、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鍵は、RADIUS サーバで設定されたサーバ秘密鍵と一致する必要があります。RADIUS サーバのサーバ秘密鍵がわからない場合は、RADIUS サーバの管理者に問い合せてください。最大フィールド長は、64 文字です。

- Confirm Server Secret Key：正確であることを確認するため、サーバの秘密鍵を再度入力する必要があります。この秘密鍵では、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。
- Common Password：RADIUS 認可サーバで使用するための共通パスワードを指定します。パスワードは、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。RADIUS サーバを認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 認可サーバでは、接続しようとする各ユーザのパスワードとユーザ名が必要です。パスワードはここに入力します。RADIUS 認可サーバの管理者は、このパスワードを FWSM 経由でサーバに接続する各ユーザ認可に関連付けて RADIUS サーバを設定する必要があります。この情報は、必ず RADIUS サーバの管理者に提供してください。この FWSM 経由で RADIUS 認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「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 認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） RADIUS プロトコルではパスワード フィールドが必須であり、RADIUS サーバによっても要求されますが、ユーザはパスワードを知る必要がありません。

- Confirm Common Password：正確であることを確認するため、共通パスワードを再度入力する必要があります。パスワードは、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。

- TACACS+ Parameters：TACACS+ サーバの使用に必要なパラメータを指定します。選択したサーバ グループが TACACS+ を使用するときにのみ、この領域が表示されます。
  - 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鍵を指定します。この秘密鍵では、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。
  - Confirm Server Secret Key：正確であることを確認するため、サーバの秘密鍵を再度入力する必要があります。この秘密鍵では、大文字と小文字が区別されます。ボックスには、アスタリスクのみが表示されます。
- SDI Parameters：SDI サーバの使用に必要なパラメータを指定します。選択したサーバ グループが SDI を使用するときにのみ、この領域が表示されます。
  - 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。
  - SDI Version：このサーバで実行している SDI ソフトウェアのバージョンを、SDI バージョン 5.0 以降、または SDI バージョン 5.0 以前のバージョンで指定します。
- Kerberos Parameters：Kerberos サーバの使用に必要なパラメータを指定します。選択したサーバ グループが Kerberos を使用するときにのみ、この領域が表示されます。
  - 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。タイムアウト時間の経過後、サーバへのクエリー送信の再試行回数を入力します。再試行回数の入力を行った後でも応答がない場合、FWSM はこのサーバを操作不能であると宣言し、リスト内にある次の Kerberos および Active Directory サーバを使用します。最小リトライ数は 0、デフォルトのリトライ数は 2、最大リトライ数は 10 です。
  - Kerberos Realm：使用する Kerberos 領域の名前（USDOMAIN.EXAMPLE.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、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。この名前は入力するとき、IP アドレスを Server IP Address ボックスに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。選択したサーバ グループが LDAP を使用するときにのみ、この領域が表示されます。
  - 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。
  - Base DN：ベース DN を指定します。認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：サーバが認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。オプションは 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、時間がかかりません）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、多少時間がかかります）です。
  - Naming Attribute(s)：LDAP サーバのエントリを一意に識別する Relative Distinguished Name アトリビュートを指定します。共通の名前付きアトリビュートは、Common Name（cn）と User 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、FWSM 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。FWSM は、ユーザの認証要求に Login DN フィールドを付加することにより、自身が認証バインディングされていることを示します。Login DN フィールドは、FWSM 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。FWSM 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=XYZ 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ておきます。
  - 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。
  - Confirm Login Password：前のパラメータで指定したログイン パスワードと同じでなければなりません。
- 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。選択したサーバ グループが NT Domain サーバ グループの場合にのみ、この領域が表示されます。
  - Server Port：サーバにアクセスするための 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。この名前を入力するとき、Authentication Server Address に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。

モード

次の表に、この機能を使用できるモードを示します。

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

Auth. Prompt

Auth. Prompt ペインでは、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 サーバからユーザ認証が要求されたとき、FWSM を経由した HTTP、HTTPS、FTP、Telnet アクセスの AAA チャレンジ テキストを指定できます。このテキストは、主に表面的なものを整えることを目的としていて、ログイン時にユーザに対して表示される、ユーザ名とパスワード プロンプトの上に表示されます。

AAA サーバがユーザを認証する場合、指定されていれば、FWSM はユーザ承認テキストをユーザに対して表示します。それ以外の場合、指定されていればユーザ拒否テキストを表示します。拒否の原因が無効なクレデンシャル（正しくないユーザ名など）や、パスワードの期限切れである場合、ユーザ拒否テキストではなく、無効なクレデンシャル テキストまたは期限切れのパスワード テキストが表示されます。

(注)　Microsoft Internet Explorer では、認証プロンプトに最大 37 文字まで表示されます。Netscape Navigator では、認証プロンプトに最大 120 文字まで、Telnet および FTP では最大 235 文字まで表示されます。

フィールド

- Prompt：FWSM を経由したユーザ セッションに対して、AAA チャレンジ テキストの表示をイネーブルにします。
  - Prompt：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。文字列を終了するには、疑問符を入力するか **Enter** キーを押します（Enter キーを押すと文字列に疑問符が表示されます）。
- Messages：ユーザが承認または拒否されたときに表示するメッセージを設定します。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。文字列を終了するには、疑問符を入力するか **Enter** キーを押します（Enter キーを押すと文字列に疑問符が表示されます）。
  - User Accepted：ユーザ認証が承認されたときに表示するテキストを設定します。
  - User Rejected：ユーザ認証が拒否されたときに表示するテキストを設定します。無効なクレデンシャルまたは期限切れのパスワードが原因ではないすべての拒否に対して、この汎用プロンプトが表示されます。無効なクレデンシャルまたは期限切れのパスワードが原因の拒否に対しては、Invalid Credensials または Password Expired オプションで設定したプロンプトが表示されます。無効なクレデンシャルまたは期限切れのパスワードにプロンプトを設定していないと、すべての場合に汎用拒否プロンプトが表示されます。
  - Invalid Credentials：正しくないユーザ名またはパスワードなど、無効なクレデンシャルが原因でユーザ認証が拒否されたときに表示するテキストを設定します。
  - Password Expired：期限切れのパスワードが原因でユーザ認証が拒否されたときに表示するテキストを設定します。このプロンプトは、RADIUS サーバがユーザ名とパスワードに Windows Active Directory サーバを使用している場合にのみ使用されます。新しいパスワードの入力を求めるユーザに対して、このオプションを使用してプロンプトを設定する必要があります。

(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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Device Access

ここでは、次の項目について説明します。

AAA Access

AAA Access ペインには、認証、認可、アカウンティングを設定するためのタブが含まれます。AAA サービスの概要については、P.10-4 の「FWSM での AAA の実装」を参照してください。

- Authentication
- Authorization
- Accounting タブ

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

FWSM への管理者アクセスの認証をイネーブルにするには、このタブを使用します。認証では、有効なユーザ名およびパスワードを要求してアクセスを制御します。次の項目を認証するように、FWSM を設定できます。

- FWSM へのすべての管理接続（この接続は、次の方法を使用します）
  - Telnet
  - SSH
  - HTTPS/ASDM
- **enable** コマンド

フィールド

- Require authentication to allow use of privileged mode commands：特権モード コマンドへのアクセスを制御するパラメータを指定します。
  - Enable：特権モード コマンドの使用が許可される前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。
  - Server Group：ユーザの認証に使用するサーバ グループを選択し、特権モード コマンドを使用します。
  - Use LOCAL when server group fails：選択したサーバ グループに障害が発生した場合、ユーザの認証に LOCAL データベースの使用を許可し、特権モード コマンドを使用します。
- Require authentication for the following types of connections：認証を必要とする接続のタイプを指定するとともに、その認証に使用するサーバ グループを指定します。
  - HTTP/ASDM：HTTP/ASDM 接続に認証が必要かどうかを指定します。
  - Server Group：指定した接続タイプの認証に使用するサーバ グループを選択します。
  - Use LOCAL when server group fails：選択したサーバ グループに障害が発生した場合、指定した接続タイプの認証に LOCAL データベースを使用することを許可します。
  - SSH：SSH 接続に認証が必要かどうかを指定します。
  - Telnet：Telnet 接続に認証が必要かどうかを指定します。マルチコンテキスト モードでは、システム コンフィギュレーションで AAA を設定できません。ただし、管理コンテキストで Telnet の認証を設定した場合、認証はスイッチから FWSM へのセッション（システム実行スペースに入る）にも適用されます。

モード

次の表に、この機能を使用できるモードを示します。

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

Authorization

管理コマンドを認可するように FWSM を設定できます。コマンド認可では、有効なユーザ名およびパスワードで認証した後に、各ユーザに許可されるコマンドを制御できます。

認可では、ユーザが使用できるコマンドを制御できます。認証だけでは、ユーザに許可されるコマンドを制御しません。

コマンド認可をイネーブルにすると、（Configure Command Privileges ボタンを使用した）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るオプション、または（Set ASDM Defined User Roles ボタンを使用した）ASDM 定義済みユーザ ロールをイネーブルにするオプションが使用できます。

事前定義ユーザ	特権レベル	説明
管理者	15	すべての CLI コマンドへの完全アクセス
読み取り専用	5	すべてのコマンドへの読み取り専用アクセス
監視専用	3	タブの監視のみ

ASDM Defined User Role Setup ペインには、Yes をクリックした場合、ASDM が FWSM に発行するコマンドおよび特権のリストが表示されます。Yes により、ASDM は、管理者、読み取り専用、監視専用の 3 つの特権をサポートします。

Command Privilege Setup ペインには、ASDM が FWSM に発行しようとしているコマンドおよび特権のリストが表示されます。リスト内で 1 つまたは複数のコマンドを選択し、Edit ボタンを使用して、選択したコマンドの特権レベルを変更できます。

フィールド

- Enable：FWSM　コマンド　アクセスの認可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、このペインの残りのパラメータがアクティブになります。
- Server Group：コマンドアクセスに対するユーザの認可に使用するサーバ グループを選択します。
- Use LOCAL when server group fails：選択したサーバ グループに障害が発生した場合、ユーザの認可に LOCAL データベースの使用を許可し、特権モード コマンドを使用します。
- Set ASDM Defined User Roles：ASDM Defined User Roles Setup ペインを開きます。このペインでは、事前定義済みユーザ プロファイルを設定するとともに、選択済みのリスト化されたコマンドの特権レベルを設定できます。
- Configure Command Privileges：Command Privilege Setup ペインを開きます。このペインでは、個々のコマンドまたはコマンド グループに特権レベルを手動で割り当てることができます。

モード

次の表に、この機能を使用できるモードを示します。

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

Command Privilege Setup

個々のコマンドまたはコマンド グループに特権レベルを割り当てるには、Command Privilege Setup ペインを使用します。カラムの先頭をクリックすると、選択したカラムをキー フィールドとして使用し、テーブル全体が英数字順に並び替わります。

- Command Mode：特定のコマンド モードまたは -- All Modes -- を選択します。この選択により、リストのすぐ下の Command Modes テーブルに表示される内容が決まります。
- CLI Command：CLI コマンドの名前を指定します。
- Mode：このコマンドに適用されるモードを示します。一部のコマンドには、複数のモードが適用されます。
- Variant：特権レベルの適用先である特定のコマンドの形式（show または clear など）を示します。
- Privilege：このコマンドに現在割り当てられている特権レベルが表示されます。
- Edit：Select Command(s) Privilege ポップアップ ペインを表示します。このペインでは、親ペインで選択した 1 つまたは複数のコマンドの特権レベルをリストから選択できます。OK をクリックすると、ただちに変更内容が Command Modes テーブルに反映されます。
- Select All：Command Modes テーブルの内容全体を選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Defined User Roles Setup

ASDM Defined User Roles Setup ペインでは、管理者、読み取り専用、監視専用という名前が付いたユーザ プロファイルを、FWSM がセットアップするかどうかを尋ねます。このペインには、AAA Access ペインの Authorization タブにある **Set ASDM Defined User Roles . .** をクリックして移動します。

フィールド

- Command List：事前定義ユーザ アカウント特権のセットアップで影響を受ける CLI コマンド、そのモード、バリアント、特権が一覧表示されます。
  - CLI Command：CLI コマンドの名前を指定します。
  - Mode：このコマンドに適用されるモードを示します。一部のコマンドには、複数のモードが適用されます。

- Variant：特権レベルの適用先である特定のコマンドの形式（show または clear など）を示します。
- Privilege：このコマンドに現在割り当てられている特権レベルが表示されます。

- Yes：リストされたコマンドをそれぞれの特権レベルでセットアップするように、FWSM に指示します。このセットアップでは、User Accounts ペインを介して、特権レベル 15 の管理者、特権レベル 5 の読み取り専用、特権レベル 3 の監視専用というそれぞれの役割でユーザが作成されます。
- No：コマンドおよびユーザの特権レベルを手動で管理します。

モード

次の表に、この機能を使用できるモードを示します。

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

Accounting タブ

アカウンティングでは、FWSM を通過するトラフィックを追跡し続けることができます。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、AAA クライアント メッセージとユーザ名、そのセッションで FWSM を通過したバイト数、使用されたサービス、セッションの継続時間が含まれます。

（注） アカウンティングを設定できるのは、TACACS+ サーバ グループに対してだけです。TACACS+ サーバ グループがまだ設定されていない場合は、Configuration > Properties > AAA Setup > AAA Server Groups で移動します。

フィールド

- Require accounting to allow accounting of user activity：ユーザ アクティビティのアカウンティングに関連するパラメータを指定します。
  - Enable：ユーザ　アクティビティのアカウンティングを許可する要求をイネーブルまたはディセーブルにします。
  - Server Group：該当する場合は、ユーザ アカウンティングに使用する選択済みサーバ グループを指定します。TACACS+ サーバ グループが存在しない場合、このリストのデフォルト値は --None-- です。

（注） サーバ グループ リスト パラメータの定義は、このペインのすべての領域で同じです。

- Require accounting for the following types of connections：アカウンティングを必要とする接続タイプと、それぞれのサーバ グループを指定します。
  - SSH：Secure Shell（SSH; セキュア シェル）接続のアカウンティングを要求します。
  - Telnet：Telnet 接続のアカウンティングを要求します。

- Require command accounting for FWSM：コマンドのアカウンティングに関連するパラメータを指定します。
  - Enable：コマンドのアカウンティングを許可する要求をイネーブルまたはディセーブルにします。
  - Privilege level：コマンド アカウンティングを実行する、選択された特権レベルを示します。

モード

次の表に、この機能を使用できるモードを示します。

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

HTTPS\ASDM

HTTPS/ASDM ペインには、HTTPS を使用した ASDM へのアクセスを許可す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が用意されています。このテーブルを使用して、アクセスを許可す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を許可するアクセス元の FWSM 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：アクセスを許可す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。
- Enable HTTP Server：このチェックボックスをオフにすると、Web サーバがディセーブルになり、ASDM への HTTPS 接続が終了します。ASDM にアクセスするには、コマンドラインからこの設定を再度イネーブルにする必要があります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 での FWSM デバイス マネージャへの管理アクセスが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：FWSM デバイス マネージャへの管理アクセスを許可するアクセス元の FWSM 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。
- Mask：アクセスを許可す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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Secure Shell ペインでは、特定のホストまたはネットワークが、SSH プロトコルを使用して、管理アクセスのために FWSM へ接続することだけを許可するルールを設定できます。ルールでは、特定の IP アドレスおよびネットマスクへの SSH アクセスが制限されます。ルールに準拠した SSH 接続試行は、次に 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。

SSH セッションは、Monitoring > Administration > Secure Shell Sessions を使用して監視できます。

フィールド

Secure Shell ペインでは、次のフィールドが表示されます。

- Allowed SSH Versions：FWSM が受け入れる 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 および SSH バージョン 2 接続が受け入れられます。
- Timeout (minutes)：FWSM が SSH セッションを閉じる前にアイドルでいられる分数を 1 ～ 60 で表示します。デフォルトは 5 分です。
- SSH Access Rule：SSH を使用した FWSM へのアクセスが許可されるホストおよび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、選択したエントリを対象とした 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 FWSM のインターフェイスの名前が表示されます。
  - IP Address：指定したインターフェイスを介してこの FWSM 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。
  - Mask：指定したインターフェイスを介してこの FWSM 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、新しい SSH アクセス ルールをルール テーブルに追加できます。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 FWSM インターフェイスの名前を指定します。
- IP Address：FWSM との SSH 接続の確立が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 接続の確立が許可されるホストまたはネットワークのネットマスクです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 FWSM に接続できるルールを設定します。

ルールでは、FWSM 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。ルールに準拠した接続試行は、事前設定された 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 を使用して監視できます。

（注） コンフィギュレーション ファイルには 5 つ以上の Telnet セッションが含まれますが、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のは 5 つまでです。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 セッションのみアクティブになれます。

フィールド

- Interface：Telnet 接続を許可する FWSM 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 FWSM 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。

（注） これは、FWSM 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 FWSM 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。

（注） これは、FWSM インターフェイスの IP アドレスではありません。

- Timeout：FWSM が Telnet セッションを閉じる前にアイドルでいられる分数を 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：選択した項目を削除します。

- Apply：ASDM での変更内容を FWSM に送信し、実行中の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。実行中の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、変更前に表示されていた情報、または ***Refresh*** か ***Apply*** を最後にクリックしたときに表示されていた情報に戻します。Reset したら Refresh を実行し、現在の実行コンフィギュレーション データが表示されることを確認してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

フィールド

- Interface Name：FWSM 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：FWSM への Telnet 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：FWSM への Telnet 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：詳細を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 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て、Telnet > Add ダイアログボックスを開きます。
2. **Interface** をクリックし、FWSM 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 フィールドに、この FWSM インターフェイスを介した Telnet アクセスが許可される、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、FWSM 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、FWSM 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、次のいずれかをクリックします。

- **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 FWSM 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 FWSM インターフェイスを介した Telnet アクセスが許可される、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、FWSM 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、FWSM 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、次のいずれかをクリックします。

- **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。

変更内容の適用

Add、Edit、または Delete を使用してテーブルを変更した内容は、実行中の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破棄するには、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 FWSM に送信し、実行中の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。実行中の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、変更前に表示されていた情報、または **Refresh** か **Apply** を最後にクリックしたときに表示されていた情報に戻します。Reset をクリックした後は、**Refresh** を使用して、現在実行中の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。

Virtual Access

Virtual Access ペインでは、仮想 Telnet、仮想 SSH、および仮想 HTTP を設定できます。ここでは、次の項目について説明します。

FWSM での直接認証

仮想 Telnet、SSH、または HTTP では、通過トラフィックの認証が設定されるときに、ユーザは FWSM で直接認証できます（P.18-5 の「ネットワーク アクセス認証の設定」を参照）。仮想 IP アドレスを使用して、FWSM で直接認証を受けることができます。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、ユーザが直接認証を受けることができるのは、HTTP（S）、Telnet、または FTP のみです。認証を必要とする他のトラフィックが許可される前に、ユーザはまずこれらのサービスの 1 つを認証する必要があります。FWSM で HTTP、Telnet、または FTP は許可しないが、他のタイプのトラフィックを認証する場合、仮想 Telnet、SSH または HTTP を設定できます。ユーザが次のいずれかのサービスを使用して FWSM に設定された所定の IP アドレスに接続すると、FWSM はプロンプトを表示します。

仮想 Telnet アドレス、および AAA 認証ルールを使用して認証するその他のサービスに Telnet、HTTP または SSH アクセスの認証を設定する必要があります。

認証が済んでいないユーザが仮想 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尋ねられ、その後 AAA サーバにより認証されます。いったん認証されると、ユーザには「Authentication Successful.」メッセージが表示されます。その後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。

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アドレスを含める必要があります。

着信ユーザ（低位セキュリティから高位セキュリティへ）に対して、NAT が必要ない場合でも、仮想 IP アドレスのスタティック NAT ルールを追加する必要があります。通常、アイデンティティ NAT ルールが使用されます（アドレスをそのアドレス自体に変換する場合）。発信ユーザには、スタティック NAT ルールは必要ありません。

FWSM からログアウトするには、仮想 IP アドレスに再接続します。ログアウトを尋ねるプロンプトが表示されます。

HTTP 認証のカスケード

HTTP 認証のカスケードに、仮想 HTTP を使用することもできます。FWSM で HTTP 認証を使用し、HTTP サーバも認証を要求している場合、このコマンドを使用して、FWSM（AAA サーバを経由）および HTTP サーバで別々に認証できます。仮想 HTTP を使用しない場合、FWSM での認証に使用した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 サーバのユーザ名およびパスワードが別に要求されることはありません。ユーザ名とパスワードが AAA および HTTP サーバと同じでない場合、HTTP 認証は失敗します。

この機能は、AAA 認証が必要なすべての HTTP 接続を FWSM 上の仮想 HTTP サーバにリダイレクトします。FWSM は、AAA サーバのユーザ名とパスワードを求めるプロンプトを表示します。AAA サーバがユーザを認証すると、FWSM は HTTP 接続を元のサーバにリダイレクトしますが、AAA サーバのユーザ名およびパスワードは含まれません。HTTP パケットにユーザ名およびパスワードが含まれないため、HTTP サーバは HTTP サーバのユーザ名およびパスワードをユーザに個別に要求します。

フィールド

- Virtual Telnet Server：仮想 Telnet IP アドレスを設定します。
- Virtual SSH Server：仮想 SSH IP アドレスを設定します。
- Virtual HTTP Server：仮想 HTTP IP アドレスを設定します。
- Host：FWSM 上の仮想 HTTP サーバにホスト名を割り当てます。AAA ユーザ名とパスワードを入力するためにユーザが仮想 HTTP サーバに転送されるときに、次の認証ダイアログボックス メッセージにホスト名が表示されます。

  ```
  Username for 'HTTP Authentication (sessionID) from host_name' at server
  virtual_http_ip
  ```

  この情報は、AAA プロンプトと宛先 HTTP サーバ プロンプトを区別するのに役立ちます。
- Display Redirection Warning：HTTP 接続を FWSM にリダイレクトする必要があることをユーザに通知します。このオプションは、リダイレクトが自動的に実行されない場合、テキスト ベースのブラウザにのみ適用されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

フェールオーバー

ここでは、次の項目について説明します。

フェールオーバーについて

Failover パネルには、FWSM 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 パネルは、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 FWSM 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 FWSM 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。FWSM 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。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 リンクの状態
- 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 FWSM 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 リスクになる恐れがあります。FWSM 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。

FWSM 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/Active フェールオーバー
- ステートレス（通常）フェールオーバー
- ステートフル フェールオーバー

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 FWSM 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 FWSM は、アクティブ FWSM 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 FWSM 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 FWSM 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 FWSM はアクティブ装置になります。このとき、それまでアクティブだった装置の IP アドレスおよび MAC アドレスが引き継がれます。ネットワーク上の他のデバイスは IP アドレスまたは MAC アドレスの変更を参照できないため、ARP エントリが変わったり、ネットワーク上でタイム 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、FWSM で使用できます。

Active/Active 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 FWSM がネットワーク トラフィックを渡します。Active/Active フェールオーバーは、マルチコンテキスト モードの FWSM でのみ使用できます。

FWSM 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 グループを作成せずにフェールオーバーをイネーブルにすると、Active/Standby フェールオーバーをイネーブルにすることになります。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。FWSM では、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 グループは、フェールオーバー グループ 1 がアクティブ状態にある装置に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 のメンバーです。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 のメンバーです。

Active/Standby フェールオーバーと同様に、Active/Active フェールオーバー ペアの各装置には、プライマリ指定またはセカンダリ指定が設定されます。Active/Standby フェールオーバーの場合とは異なり、両方の装置が同時に起動された場合、この指定ではどちらの装置がアクティブになるか指示しません。コンフィギュレーション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役割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、両方の装置が同時に起動されたときに、フェールオーバー ペアのどちらの装置でフェールオーバー グループのコンテキストがアクティブ状態に表示されるのかが決まります。両方のフェールオーバー グループをペアのうちの一方の装置でアクティブ状態にして、もう一方の装置にはスタンバイ状態のフェールオーバー グループが含まれるようにできます。ただし、さらに一般的なコンフィギュレーションでは、各フェールオーバー グループに異なる役割プリファレンスを割り当て、装置ごとにそれぞれ 1 つをアクティブにして、装置全体でトラフィックのバランスが取れるようにします。

一方または両方の装置が起動すると、初期コンフィギュレーションの同期が発生します。この同期は、次のルールに従って発生します。

- 両方の装置が同時に起動した場合、コンフィギュレーションはプライマリ装置からセカンダリ装置へと同期されます。
- すでに片方の装置がアクティブの状態でもう一方の装置が起動した場合、起動している装置が、すでにアクティブの状態の装置からコンフィギュレーションを受け取ります。

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 がアクティブ状態の装置から、フェールオーバー グループ 1 がスタンバイ状態の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 がアクティブ状態の装置から、フェールオーバー グループ 1 がスタンバイ状態の装置に複製されます。

コマンド複製を行うのに適切な装置上でコマンドを入力しなかった場合は、コンフィギュレーションは非同期になります。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。

Active/Active 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、フェールオーバー グループ 1 が故障すると、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） Active/Active 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（通常）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

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。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
- ユーザ認証（uauth）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）
- ARP テーブル
- ルーティング テーブル

High Availability and Scalability ウィザードを使用したフェールオーバーの設定

High Availability and Scalability ウィザードでは、Active/Active フェールオーバー コンフィギュレーション、または Active/Standby フェールオーバー コンフィギュレーションの作成プロセスを、順を追って実行できます。

High Availability and Scalability ウィザード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 ウィザードへのアクセスと使用
- High Availability and Scalability ウィザードを使用した Active/Active フェールオーバーの設定
- High Availability and Scalability ウィザードを使用した Active/Standby フェールオーバーの設定
- High Availability and Scalability ウィザードのフィールド情報

High Availability and Scalability ウィザードへのアクセスと使用

High Availability and Scalability ウィザードを開くには、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。

ある時点で変更内容を保存せずにウィザードを終了するには、**Cancel** をクリックします。

ウィザードの最後にコンフィギュレーションを FWSM に送信するには、**Finish** をクリックします。

High Availability and Scalability ウィザードを使用した Active/Active フェールオーバーの設定

次の手順では、High Availability and Scalability ウィザードを使用した 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。それぞれの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、「Configuration Type」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、「Failover Peer Connectivity and Compatibility Check」を参照してください。

ステップ 3　FWSM 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。FWSM 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 FWSM 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」を参照してください。

ステップ 4　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」を参照してください。

ステップ 5　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」を参照してください。

ステップ 6　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」を参照してください。

ステップ 7　Standby Address Configuration 画面で、スタンバイ アドレスを FWSM 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」を参照してください。

ステップ 8　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」を参照してください。

ステップ 9　**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 FWSM とフェールオーバー ピアに送信されます。

High Availability and Scalability ウィザードを使用した Active/Standby フェールオーバーの設定

次の手順では、High Availability and Scalability ウィザードを使用した 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。それぞれの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、「Configuration Type」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、「Failover Peer Connectivity and Compatibility Check」を参照してください。

ステップ 3　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」を参照してください。

ステップ 4　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」を参照してください。

ステップ 5　Standby Address Configuration 画面で、スタンバイ アドレスを FWSM 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」を参照してください。

ステップ 6　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」を参照してください。

ステップ 7　**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 FWSM とフェールオーバー ピアに送信されます。

High Availability and Scalability ウィザードのフィールド情報

High Availability and Scalability ウィザードでは、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によって異なります。

- Configuration Type
- Failover Peer Connectivity and Compatibility Check
- Change Device to Multiple Mode
- Security Context Configuration
- Failover Link Configuration
- State Link Configuration
- Standby Address Configuration
- Summary

Configuration Type

Configuration Type 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、FWSM のフェールオーバー機能の決定に役立ちます。

- Hardware Model：（表示のみ）FWSM のモデル番号を表示します。
- No. of Interfaces：（表示のみ）FWSM 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：（表示のみ）FWSM にインストールされたモジュールの数を表示します。
- Software Version：（表示のみ）FWSM 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：（表示のみ）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：（表示のみ）ファイアウォール モード（ルーテッドまたは透過）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：FWSM に Active/Active フェールオーバーを設定します。
- Configure Active/Standby Failover：FWSM に Active/Standby フェールオーバーを設定します。
- Configure VPN Cluster Load Balancing：FWSM 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Peer Connectivity and Compatibility Check

Failover Peer Connectivity and Compatibility Check 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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のみ表示されます。Active/Active フェールオーバーでは、FWSM 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 FWSM 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、FWSM 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。

FWSM 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、FWSM はリブートされます。ただし、High Availability and Scalability ウィザードでは、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の Devices Status フィールドでステータスが報告されます。

次に進む前に、現在の FWSM とピア FWSM 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：FWSM 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、FWSM 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、FWSM のホスト名が入ります。
- Device Status：（表示のみ）マルチコンテキスト モードへの変換中に FWSM のステータスが表示されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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対してのみ表示されます。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することはできません。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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 画面でフェールオーバー インターフェイスを設定できます。

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：（オプション）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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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。
- 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、FWSM 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、このフィールドに行った変更は、ピア装置上の対応するインターフェイス用の 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して、スタンバイ IP アドレスを編集または追加できます。また、このフィールドに行った変更は、ピア装置上の対応するインターフェイス用の 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のみ使用可能です。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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

次の表に、この機能を使用できるモードを示します。

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

フェールオーバー 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変わります。

- 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 パネルには、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」を参照してください。Failover パネル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、透過ファイアウォール 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（透過ファイアウォール モード）
- Failover: Criteria

Failover: Setup

このタブを使用して、FWSM 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」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 FWSM 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** パネルで設定しておく必要があります。

- Use 32 hexadecimal character key：Shared Key ボックスに 16 進数値の暗号鍵を入力するには、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 進数の暗号鍵を入力してください。鍵は、32 桁の 16 進数文字（0 ～ 9、a ～ f）でなければなりません。

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、英字、句読点の任意の組み合せです。共有秘密情報は、暗号鍵の生成に使用されます。

- LAN Failover：LAN ベースの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。インターフェイスには、LAN ベースのフェールオーバーおよびステートフル フェールオーバーの両方のトラフィックを処理するのに十分な容量が必要です。

（注） 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。

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のみが表示され、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** パネル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 FWSM 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。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。インターフェイスには、LAN ベースのフェールオーバーおよびステートフル フェールオーバーの両方のトラフィックを処理するのに十分な容量が必要です。LAN ベースのフェールオーバーに使用するのと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対して選択した場合は、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。

（注） 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：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。
  - 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。
  - 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。
  - 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。

— 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 の複製をディセーブルにすると、ステート リンクでのトラフィック量を減らすことができます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」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、FWSM 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」を参照してください。

フィールド

- Interface：FWSM 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：インターフェイス名を示します。
  - — Active IP：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：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 アドレスを示します。
  - — Is Monitored：インターフェイスのヘルスをフェールオーバー用に監視するよう指定するには、このチェックボックスをオンにします。インターフェイスのステータスがフェールオーバーに影響しないようにするには、このチェックボックスをオフにします。
- Edit：選択したインターフェイスに対して、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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」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。FWSM で監視可能なインターフェイス数は 250 です。インターフェイス ポーリング時間の継続中には、その都度 FWSM 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。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、インターフェイスで hello メッセージが 5 ポーリング時間（25 秒間）聞こえなければ、そのインターフェイスでテストが開始されます。監視対象のフェールオーバー インターフェイスで可能なステータスは次のとおりです。
  - Unknown：初期ステータス。このステータスは、ステータスが判別できないことを示す場合もあります。
  - 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：インターフェイス上で 5 ポーリング時間、Hello メッセージが聞こえません。
  - 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が受信されていませんが、ピア インターフェイスではトラフィックが聞こえます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」を参照してください。

Failover: Interfaces（透過ファイアウォール 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、FWSM 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：FWSM 上のインターフェイスを一覧表示します。
  - Interface Name：インターフェイス名を示します。
  - Is Monitored：インターフェイスのヘルスをフェールオーバー用に監視するよう指定するには、このチェックボックスをオンにします。インターフェイスのステータスがフェールオーバーに影響しないようにするには、このチェックボックスをオフにします。

    FWSM で監視可能なインターフェイス数は 250 です。インターフェイス ポーリング時間の継続中には、その都度 FWSM 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。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、インターフェイスで hello メッセージが 5 ポーリング時間（25 秒間）聞こえなければ、そのインターフェイスでテストが開始されます。監視対象のフェールオーバー インターフェイスで可能なステータスは次のとおりです。

    Unknown：初期ステータス。このステータスは、ステータスが判別できないことを示す場合もあります。

    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：インターフェイス上で 5 ポーリング時間、Hello メッセージが聞こえません。

    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が受信されていませんが、ピア インターフェイスではトラフィックが聞こえます。
- Bridge Group：FWSM で定義されるブリッジ グループを一覧表示します。この一覧が表示されるのは、透過モードの FWSM 装置またはコンテキストのみです。
  - Bridge Group：透過ファイアウォール モードの FWSM またはコンテキストのブリッジ グループ名を示します。
  - Active IP Address：ブリッジ グループのアクティブ管理 IP アドレスを示します。
  - Network Mask：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。
  - Standby IP Address：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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」を参照してください。

Failover: Criteria

このタブを使用して、障害が発生した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フィールドが含まれます。
  - Number of failed interfaces that triggers failover：障害が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、FWSM はフェールオーバーを行います。障害の発生数は 1 ～ 250 の範囲で指定できます。
  - Percentage of failed interfaces that triggers failover：障害が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、FWSM 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 500 ～ 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（受信されない場合には、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。3 ～ 45 秒の範囲で指定できます。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。3 ～ 15 秒の範囲で指定できます。
- Preempt：フェールオーバー　プリエンプションを有効にするには、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 プリエンプションにより、リブート後またはフェールオーバー状態からの復帰後に、プライマリ装置が自動的にアクティブ装置になります。このチェックボックスをオフにすると、セカンダリ装置がアクティブな状態でプライマリ装置がブートした場合、または障害状態からプライマリ装置が復帰した場合、プライマリ装置はスタンバイ状態のままになります。スタンバイ状態は、フェールオーバーが発生するか、またはシステム管理者が強制的にプライマリ装置をアクティブにするまで継続します。
  - with optional delay of：プライマリ装置が、リブート後アクティブ装置として引き継ぐまでに待機する時間を秒数で指定します。1 ～ 1200 秒の範囲で指定できます。遅延なしに設定するには、このフィールドを空白のままにしておきます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」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、コンテキストが透過ファイアウォール 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、次の項目について説明します。

Failover - Routed

このパネルを使用して、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：FWSM 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：インターフェイス名を示します。
  - Active IP：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：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 ボタン：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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」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。FWSM で監視可能なインターフェイス数は 250 です。インターフェイス ポーリング時間の継続中には、その都度 FWSM 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。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、インターフェイスで hello メッセージが 5 ポーリング時間（25 秒間）聞こえなければ、そのインターフェイスでテストが開始されます。監視対象のフェールオーバー インターフェイスで可能なステータスは次のとおりです。
  - Unknown：初期ステータス。このステータスは、ステータスが判別できないことを示す場合もあります。
  - 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：インターフェイス上で 5 ポーリング時間、Hello メッセージが聞こえません。
  - 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が受信されていませんが、ピア インターフェイスではトラフィックが聞こえます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」を参照してください。

Failover - Transparent

このパネルを使用して、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：FWSM 上のインターフェイスを一覧表示します。
  - Interface Name：インターフェイス名を示します。
  - Is Monitored：インターフェイスのヘルスをフェールオーバー用に監視するよう指定するには、このチェックボックスをオンにします。インターフェイスのステータスがフェールオーバーに影響しないようにするには、このチェックボックスをオフにします。

    FWSM で監視可能なインターフェイス数は 250 です。インターフェイス ポーリング時間の継続中には、その都度 FWSM 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。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、インターフェイスで hello メッセージが 5 ポーリング時間（25 秒間）聞こえなければ、そのインターフェイスでテストが開始されます。監視対象のフェールオーバー インターフェイスで可能なステータスは次のとおりです。

Unknown：初期ステータス。このステータスは、ステータスが判別できないことを示す場合もあります。

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：インターフェイス上で 5 ポーリング時間、Hello メッセージが聞こえません。

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が受信されていませんが、ピア インターフェイスではトラフィックが聞こえます。

- Bridge Group：FWSM で定義されるブリッジ グループを一覧表示します。この一覧が表示されるのは、透過モードの FWSM 装置またはコンテキストのみです。
  - Bridge Group：透過ファイアウォール モードの FWSM またはコンテキストのブリッジ グループ名を示します。
  - Active IP Address：ブリッジ グループのアクティブ管理 IP アドレスを示します。
  - Network Mask：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。
  - Standby IP Address：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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」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。FWSM で監視可能なインターフェイス数は 250 です。インターフェイス ポーリング時間の継続中には、その都度 FWSM 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。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、インターフェイスで hello メッセージが 5 ポーリング時間（25 秒間）聞こえなければ、そのインターフェイスでテストが開始されます。監視対象のフェールオーバー インターフェイスで可能なステータスは次のとおりです。
  - Unknown：初期ステータス。このステータスは、ステータスが判別できないことを示す場合もあります。
  - 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：インターフェイス上で 5 ポーリング時間、Hello メッセージが聞こえません。
  - 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が受信されていませんが、ピア インターフェイスではトラフィックが聞こえます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」を参照してください。

Failover（マルチモード、システム）

このパネルには、マルチコンテキスト モードの FWSM 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。Active/Active 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」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 > 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 FWSM 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 FWSM 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場合は、フェールオーバーをイネーブルにする前に、Configuration > Interfaces パネルで設定しておく必要があります。

- Shared Key：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フェールオーバー共有秘密情報を指定します。
- LAN Failover：LAN ベースの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。インターフェイスには、LAN ベースのフェールオーバーおよびステートフル フェールオーバーの両方のトラフィックを処理するのに十分な容量が必要です。

（注） 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。

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のみが表示され、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** パネルで編集したり、コンテキストに割り当てたりすることはできません。

  - 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 FWSM 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。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。インターフェイスには、LAN ベースのフェールオーバーおよびステートフル フェールオーバーの両方のトラフィックを処理するのに十分な容量が必要です。LAN ベースのフェールオーバーに使用するのと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対して選択した場合は、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。

（注） 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 の複製をディセーブルにすると、ステート リンクでのトラフィック量を減らすことができます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」を参照してください。

Failover > Criteria タブ

このタブを使用して、障害が発生した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フィールドが含まれます。
  - Number of failed interfaces that triggers failover：障害が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、FWSM はフェールオーバーを行います。障害の発生数は 1 ～ 250 の範囲で指定できます。
  - Percentage of failed interfaces that triggers failover：障害が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、FWSM 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 500 ～ 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（受信されない場合には、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。3 ～ 45 秒の範囲で指定できます。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。3 ～ 15 秒の範囲で指定できます。

- Preempt：フェールオーバー プリエンプションを有効にするには、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 プリエンプションにより、リブート後またはフェールオーバー状態からの復帰後に、プライマリ装置が自動的にアクティブ装置になります。このチェックボックスをオフにすると、セカンダリ装置がアクティブな状態でプライマリ装置がブートした場合、または障害状態からプライマリ装置が復帰した場合、プライマリ装置はスタンバイ状態のままになります。スタンバイ状態は、フェールオーバーが発生するか、またはシステム管理者が強制的にプライマリ装置をアクティブにするまで継続します。
  - with optional delay of：プライマリ装置が、リブート後アクティブ装置として引き継ぐまでに待機する時間を秒数で指定します。1 ～ 1200 秒の範囲で指定できます。遅延なしに設定するには、このフィールドを空白のままにしておきます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」を参照してください。

Failover > Active/Active タブ

このタブを使用すると、フェールオーバー グループを定義して FWSM 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 FWSM 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 FWSM でのみ使用できます。

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。FWSM では、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 のメンバーです。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 のメンバーです。

（注） Active/Active 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 FWSM 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、フェールオーバー グループへのコンテキストの割り当てに使用されます。
  - Preferred Role：プライマリ装置とセカンダリ装置を同時に起動したり、preempt オプションのチェックボックスをオンにしたりしたときに、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 ペアの装置（プライマリまたはセカンダリ）を指定します。両方のフェールオーバー グループをペアのうちの一方の装置でアクティブ状態にして、もう一方の装置にはスタンバイ状態のフェールオーバー グループが含まれるようにできます。ただし、さらに一般的なコンフィギュレーションでは、各フェールオーバー グループに異なる役割プリファレンスを割り当て、装置ごとにそれぞれ 1 つをアクティブにして、装置全体でトラフィックのバランスが取れるようにします。

- 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。0 ～ 1200 秒の範囲で指定できます。
- 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、障害数 1 ～ 250 回、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。3 ～ 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 の複製をディセーブルにすると、ステート リンクでのトラフィック量を減らすことができます。この設定は、Setup タブでの HTTP 複製の設定を上書きします。

- Add ボタン：Add Failover Group ダイアログボックスが表示されます。存在するフェールオーバー グループが 2 つに満たない場合のみ、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 ボタン：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 ボタン：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のみイネーブルになります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」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。両方のフェールオーバー グループをペアのうちの一方の装置でアクティブ状態にして、もう一方の装置にはスタンバイ状態のフェールオーバー グループが含まれるようにできます。ただし、さらに一般的なコンフィギュレーションでは、各フェールオーバー グループに異なる役割プリファレンスを割り当て、装置ごとにそれぞれ 1 つをアクティブにして、装置全体でトラフィックのバランスが取れるようにします。

- 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** ボックス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。0 ～ 1200 秒の範囲で指定できます。
- 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：障害が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、FWSM はフェールオーバーを行います。障害の発生数は 1 ～ 250 の範囲で指定できます。
  - Percentage of failed interfaces that triggers failover：障害が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、FWSM 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。3 ～ 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 の複製をディセーブルにすると、ステート リンクでのトラフィック量を減らすことができます。この設定は、Setup タブでの HTTP 複製の設定を上書きします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」を参照してください。

CHAPTER 13

ロギングおよび SNMP の設定

ロギング機能で、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、リアルタイムでシステム ログ メッセージを表示できます。ログ表示機能の詳細については、第 25 章「システム ログ メッセージのモニタリング」を参照してください。

SNMP 機能の説明については、P.13-21 の「SNMP の設定」を参照してください。

ロギングの概要

FWSM は、アクティビティ（許可または拒否されたネットワーク トラフィックの種類など）を説明するシステム ログ メッセージの監査証跡の生成をサポートし、システム ロギングの設定を可能にします。

すべてのシステム ログ メッセージには、デフォルトの重大度レベルが設定されています。メッセージには、必要に応じて新しい重大度レベルを再割り当てできます。重大度レベルを選択するとき、そのレベルから下位のレベルへのロギング メッセージが生成されます。上位レベルからのメッセージは含まれません。重大度レベルが高いほど、含まれるメッセージは多くなります。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、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages*』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

各セキュリティ コンテキストは、ロギング コンフィギュレーションがあり、メッセージを生成します。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たシステム ログ メッセージにはフェールオーバー メッセージが含まれており、管理コンテキストで生成されたメッセージとともに管理コンテキストで表示されます。システム実行スペースで、ロギングを設定したり、ロギング情報を表示したりすることはできません。

各メッセージにコンテキスト名を表示するように FWSM を設定できます。単一の syslog サーバに送信されるコンテキスト メッセージを区別するのに役立ちます。この機能を使用すると、管理コンテキストで生成されたメッセージとシステムで生成されたメッセージを判別できます。システム実行スペースから送信されたメッセージはデバイス ID として **system** を使用し、管理コンテキストから送信されたメッセージはデバイス ID として管理コンテキスト名を使用します。デバイス ID を使用するには、P.13-6 の「Advanced Syslog Configuration」を参照してください。

ロギングの使用

ロギングをイネーブルにしたら、次の作業を実行します。

ステップ 1　Logging Setup ペインで、ロギング パラメータを設定します。詳細については、P.13-3 の「Logging Setup」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の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します。詳細については、P.13-5 の「Syslog Setup」を参照してください。

ステップ 3　E-Mail Setup ペインで、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 メッセージを指定します。詳細については、P.13-5 の「Syslog Setup」を参照してください。

ステップ 4　Event Lists ペインで、記録するメッセージを指定するイベントのカスタム リストを作成します。ここで作成したリストは、ログ フィルタのセットアップ時に使用されます。詳細については、P.13-9 の「Event Lists」を参照してください。

ステップ 5　Logging Filters ペインで、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します。フィルタの作成に使用する基準とは、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 リストです。詳細については、P.13-12 の「Logging Filters」を参照してください。

ステップ 6　Rate Limit ペインで、指定した時間間隔に生成可能なメッセージ数を制限します。詳細については、P.13-16 の「Rate Limit」を参照してください。

ステップ 7　Syslog Server ペインで、FWSM がシステム ログ メッセージを送信する syslog サーバを 1 つ以上指定します。詳細については、P.13-19 の「Syslog サーバ」を参照してください。

Logging Setup

Logging Setup ペインでは、FWSM でのシステム ロギングをイネーブルにして、スタンバイ装置がロギングを引き継ぐかどうか、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 FWSM のロギング キューのデフォルト設定も変更できます。

フィールド

- Enable logging：メイン FWSM のロギングをオンにします。
- Enable logging on the failover standby unit：使用可能な場合は、スタンバイ FWSM のロギングをオンにします。
- 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。したがって、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設定する必要があります。使用されるシステム ログ メッセージ番号は **711011** です。このシステム ログ メッセージのデフォルトの重大度レベルは debug です。
- Send syslogs in EMBLEM format：syslog サーバ以外のすべてのログの宛先に使用するため、EMBLEM 形式をイネーブルにします。
- Buffer Size：ロギング バッファがイネーブルになっている場合に、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。FTP サーバまたは内部フラッシュ メモリへのログの保存をイネーブルにしていない限り、バッファがいっぱいになったときは上書きされます。デフォルトのバッファ サイズは 4096 バイトです。範囲は 4096 ～ 1048576 です。
- Save Buffer To FTP Server：上書きされる前にバッファの内容を FTP サーバに保存するには、このチェックボックスをオンにします。FTP コンフィギュレーションを削除するには、チェックボックスをオフにします。
- Configure FTP Settings：FTP サーバを示し、バッファの内容の保存に使用する FTP パラメータを設定します。
- Save Buffer To Flash：上書きされる前にバッファの内容を内部フラッシュ メモリに保存するには、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、ルーテッドまたは透過シングルモードでのみ使用できます。

- Configure Flash Usage：ロギングのために内部フラッシュ メモリで使用される最大容量および維持する最小空き容量を、KB で指定します。このオプションをオンにすると、「syslog」という名前のディレクトリが、メッセージの格納先のデバイス ディスクに作成されます。

（注） このオプションは、ルーテッドまたは透過シングルモードでのみ使用できます。

- FWSM Logging Queue Size：FWSM で表示されるシステム ログのキュー サイズを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

- P.13-4 の「Configure FTP Settings」を参照してください。
- P.13-4 の「Configure Logging Flash Usage」を参照してください。

Configure FTP Settings

Configure FTP Settings ダイアログボックスでは、バッファの内容の保存に使用する FTP サーバのコンフィギュレーションを指定します。

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 アドレスです。
- Path：保存されたファイルを格納する FTP サーバ上のディレクトリ パスです。
- Username：FTP サーバにログインするためのユーザ名です。
- Password：FTP サーバに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です。
- Confirm Password：パスワードを確認します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Logging Flash Usage

Configure Logging Flash Usage ダイアログボックスでは、バッファの内容を内部フラッシュ メモリに保存するときの制限を指定します。

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 で指定します。
- Minimum Free Space to Be Preserved：保持する内部フラッシュ メモリの容量を、KB で指定します。内部フラッシュメモリが制限値に近づくと、新しいログが保存されなくなります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Setup

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し、システム ログ メッセージにタイムスタンプを含める必要があるかどうかを決定します。また、メッセージの重大度レベルを変更したり、記録しないメッセージを抑止したりもできます。

フィールド

- Facility code to include in syslogs：syslog サーバのシステム ログ ファシリティを、ファイル メッセージの基本として使用するように指定します。デフォルトは LOCAL(4)20 で、ほとんどの UNIX システムで想定されているコードです。ただし、ネットワーク デバイスでは使用可能な 8 つのファシリティを共有しているため、システム ログの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：送信されるすべてのシステム ログ メッセージに日付と時刻を含めます。
- 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：Syslog ID テーブルで、システム ログ メッセージ ID のリスト全体を表示するように指定します。
  - Show suppressed syslog IDs：Syslog ID テーブルで、明示的に抑止されたシステム ログ メッセージ ID のみを表示するように指定します。
  - Show syslog IDs with changed logging：Syslog ID テーブルで、デフォルト値から変更された重大度レベルを持つシステム ログ メッセージ ID のみを表示するように指定します。
  - Show syslog IDs that are suppressed or with a changed logging level：Syslog ID テーブルで、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 のみを表示するように指定します。
- 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 の抑止またはその重大度レベルの変更のいずれかを行えます。リスト内の複数のメッセージ ID を選択するには、範囲の最初の ID を選択し、Shift キーを押した状態で範囲の最後の 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

- P.13-6 の「Edit Syslog ID Settings」を参照してください。
- P.13-6 の「Advanced Syslog Configuration」を参照してください。

Edit Syslog ID Settings

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したり、選択したシステム ログ メッセージの抑止を指定したりできます。

フィールド

- Syslog ID(s)：このテキスト領域は読み取り専用です。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で決まります。
- Suppress Message(s)：Syslog ID 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 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。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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Syslog Configuration

FWSM 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、1 つのタイプだけのデバイス ID を表示できます。デバイス ID は、FWSM 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で指定できます。

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決定できます。この機能がイネーブルになっている場合、デバイス ID がすべての非 EMBLEM 形式のシステム ログ メッセージに含まれます。

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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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-Mail Setup

E-Mail Setup ペインでは、通知目的の電子メール メッセージとして送信される、指定したシステム ログ メッセージの受信者リストともに、送信元電子メール アドレスもセットアップします。送信先電子メール 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、どのエントリのセットアップが完了しているかが表示されます。

送信先電子メール 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。

送信先電子メール 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

- P.13-8 の「Add/Edit E-Mail Recipients」を参照してください。
- P.13-12 の「Logging Filters」を参照してください。

Add/Edit E-Mail Recipients

Add/Edit E-Mail Recipient ダイアログボックスでは、特定の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、送信先電子メール アドレスをセットアップします。

送信先電子メール アドレスへのメッセージのフィルタリングに使用される重大度レベルは、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。

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

次の表に、この機能を使用できるモードを示します。

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

Event Lists

Event Lists ペインでは、どのシステム ログ メッセージが特定の宛先に送信されるのかを選択するときに使用する、イベントのカスタム リストを作成できます。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 1 つ以上作成します。これらのリストは、イベントの各リストのロギング出力先を指定する場合に Logging Filters ペインで使用します。

イベント リストの定義には、次の 3 つの基準を使用できます。

- メッセージ クラス
- 重大度
- メッセージ ID

メッセージ クラスは、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るようにする、セキュリティ アプライアンスの機能に関連したシステム ログ メッセージのグループです。たとえば、ユーザ認証に関連したすべてのシステム ログ メッセージを選択するには、auth クラスを使用します。

重大度は、ネットワークの通常機能でのイベントの相対重要性に基づいて、システム ログ メッセージを分類します。最も高い重大度は emergency で、リソースが使用不能になっていることを表します。最も低い重大度は debugging で、各ネットワーク イベントに関する詳細情報を提供します。

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。システム ログ メッセージの範囲を識別するには、101001-101010 など、イベント リストのメッセージ ID を使用できます。

フィールド

- Name：イベント リストの名前を一覧表示します。
- Event Class/Severity：ロギング メッセージのイベント クラスおよびレベルを一覧表示します。イベント クラスは次のとおりです。
  - All：すべてのイベント クラス
  - auth：ユーザ認証
  - bridge：透過ファイアウォール
  - ca：PKI の認証局
  - config：コマンド インターフェイス
  - ha：フェールオーバー
  - ids：侵入検知システム
  - 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

- P.13-10 の「Add/Edit Event List」を参照してください。
- P.13-11 の「Add/Edit Syslog Message ID Filter」を参照してください。
- P.13-12 の「Logging Filters」を参照してください。

Add/Edit Event List

Add/Edit Event List ダイアログボックスでは、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るイベント リストを作成または編集できます。メッセージ クラスおよび重大度、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するイベント リストを作成できます。

メッセージ クラスは、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。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、ユーザ認証に関連したすべてのシステム ログ メッセージを選択するには、auth クラスを使用します。

重大度は、ネットワークの通常機能でのイベントの相対重要性に基づいて、システム ログ メッセージを定義します。最も高い重大度は emergency で、リソースが使用不能になっていることを表します。最も低い重大度は debugging で、各ネットワーク イベントに関する詳細情報を提供します。

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。システム ログ メッセージの範囲を識別するには、101001-101010 など、イベント リストのメッセージ ID を使用できます。

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 クラスは次のとおりです。
  - All：すべてのイベント クラス
  - auth：ユーザ認証
  - bridge：透過ファイアウォール
  - ca：PKI の認証局
  - config：コマンド インターフェイス
  - ha：フェールオーバー
  - ids：侵入検知システム

  - 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Syslog Message ID Filter

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 1 つ以上のシステム ログ メッセージ ID を指定できます。

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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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します。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したり、Event Lists ペインで作成可能なイベント リストを使用したりできます。

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。ロギングの宛先は次のとおりです。
  - コンソール
  - FWSM
  - 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：重大度、または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 リストを一覧表示するか、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指定します。
- 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

- P.13-12 の「Edit Logging Filters」を参照してください。
- P.13-11 の「Add/Edit Syslog Message ID Filter」を参照してください。
- P.13-14 の「Add/Edit Class and Severity Filter」を参照してください。
- P.13-9 の「Event Lists」を参照してください。

Edit Logging Filters

Edit Logging Filters ダイアログボックスでは、各ログの宛先にフィルタを適用したり、すでにログの宛先に適用されたフィルタを編集したり、ログの宛先に対するフィルタをディセーブルにしたりできます。

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したり、Event Lists ペインで作成可能なイベント リストを使用したりできます。

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 クラスは次のとおりです。
  - All：すべてのイベント クラス
  - auth：ユーザ認証
  - bridge：透過ファイアウォール
  - ca：PKI の認証局
  - config：コマンド インターフェイス
  - ha：フェールオーバー
  - ids：侵入検知システム
  - 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）

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Class and Severity Filter

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します。

メッセージ クラスは、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。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、ユーザ認証に関連したすべてのシステム ログ メッセージを選択するには、auth クラスを使用します。

重大度は、ネットワークの通常機能でのイベントの相対重要性に基づいて、システム ログを定義します。最も高い重大度は emergency で、リソースが使用不能になっていることを表します。最も低い重大度は debugging で、各ネットワーク イベントに関する詳細情報を提供します。

フィールド

- Event Class：イベント クラスを指定します。イベント クラスは次のとおりです。
  - All：すべてのイベント クラス
  - auth：ユーザ認証
  - bridge：透過ファイアウォール
  - ca：PKI の認証局
  - config：コマンド インターフェイス
  - ha：フェールオーバー
  - ids：侵入検知システム
  - 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）

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Syslog Message ID Filter

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 ID の範囲を指定します。

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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、ファイアウォールが送信できるシステム ログ メッセージ数を指定します。また、Logging Setup ペインを使用してロギングをイネーブルにする必要もあります。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 に適用されますが、宛先には適用されません。したがって、レート制限は、すべての設定済み宛先に送信されるメッセージの量に影響を与えます。

フィールド

syslog ロギング レベルのレート制限

- 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には、Number of Messages フィールドと Time Interval フィールドの両方を空白のままにします。
- 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には、Number of Messages と Time Interval の両方を空白のままにします。
- Edit：Edit Rate Limit ダイアログボックスを開き、選択したロギング レベルのプロパティを編集するには、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ます。
- 個別にレート制限された syslog メッセージ
  - 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、P.13-16 の「syslog ロギング レベルのレート制限」を参照してください。
  - No of Messages：指定された時間間隔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には、このボタンをクリックします。
- Apply：変更内容をファイアウォールに送信し、実行中のコンフィギュレーションに適用します。File メニューを使用して、実行中のコンフィギュレーションを内部フラッシュ メモリ、TFTP サーバ、またはフェールオーバー スタンバイ ファイアウォール装置に書き込みます。
- Reset：変更内容を破棄し、開いたときに表示された値、または開いている間に最後に Refresh をクリックしたときの値に戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

- P.13-17 の「Edit Rate Limit for Syslog Logging Level」を参照してください。
- P.13-18 の「Add/Edit Rate Limit for Syslog Message」を参照してください。

Edit Rate Limit for Syslog Logging Level

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

- 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メッセージを制限するときに使用される時間を、秒数で指定します。
- 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：詳細を表示します。
- Reset：変更内容を破棄し、開いたときに表示された値、または開いている間に最後に Refresh をクリックしたときの値に戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Rate Limit for Syslog Message

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には、Number of Messages と Time Interval の両方を空白のままにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、FWSM がシステム ログ メッセージを送信する syslog サーバを指定します。定義した 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 ペインで適切な宛先をセットアップする必要があります。

（注） コンテキストにつき、最大 4 つの syslog サーバをセットアップできます。

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 FWSM 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：メッセージをシスコ EMBLEM 形式（Protocol/Port 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、FWSM 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、キューに入れられるメッセージ数に制限がないことを意味します。
- 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。
- Deny connection upon queue full：キューがいっぱいのとき（つまり、Queue Size で設定した制限値に達したとき）に、接続を許可するかどうかを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

- P.13-20 の「Add/Edit Syslog Server」を参照してください。
- P.13-3 の「Logging Setup」を参照してください。
- P.13-12 の「Logging Filters」を参照してください。

Add/Edit Syslog Server

Add/Edit Syslog Server ダイアログボックスでは、FWSM がシステム ログ メッセージを送信する syslog サーバを追加または編集できます。定義した 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 ペインでログの宛先に適切なフィルタをセットアップする必要があります。

（注） コンテキストにつき、最大 4 つの syslog サーバをセットアップできます。

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 FWSM 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 FWSM 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)：メッセージをシスコ 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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 の設定

この項では、FWSM で SNMP 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。

SNMP の概要

FWSM では、SNMP V1 および V2c を使用したネットワーク モニタリングのサポートを提供します。FWSM では、トラップと SNMP 読み取りアクセスをサポートしますが、SNMP 書き込みアクセスはサポートしません。

ネットワーク管理ステーション（NMS; Network Management Station）にトラップ（イベント通知）を送信するように FWSM を設定したり、NMS を使用して FWSM 上の MIB をブラウジングしたりできます。MIB は定義の集合であり、FWSM は各定義の値のデータベースを保持します。MIB をブラウジングする場合は、NMS から SNMP get 要求を発行する必要があります。SNMP トラップを受信して MIB をブラウジングするには、CiscoWorks for Windows またはその他の SNMP V1 および V2c、MIB-II 互換ブラウザを使用してください。

表 13-1 に、サポートされている MIB および FWSM のトラップ、およびマルチモードの各コンテキストのトラップを示します。Cisco MIB は、次の Web サイトからダウンロードできます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

MIB をダウンロードした後、NMS 用にコンパイルします。

（注） パフォーマンスが低下する可能性があるため、データの取得に SNMP を使用する頻度は制限してください。リソースの使用状況データを効率的に収集するには、コンテキストごとにポーリングのスケジュールを設定してください。

表 13-1　SNMP の MIB とトラップのサポート

MIB とトラップ	説明
CISCO-CRYPTO-ACCELERATOR-MIB	FWSM は、MIB のブラウジングをサポートします。
• CISCO-ENTITY-MIB • CISCO-ENTITY-ALARM-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-ENTITY-REDUNDANCY-MIB	FWSM は、次のグループおよびテーブルのブラウジングをサポートします。 • entLogicalTable • entPhysicalTable FWSM は、次のトラップを送信します。 • alarm-asserted • alarm-cleared • config-change • fru-insert • fru-remove • redun-switchover

表 13-1　SNMP の MIB とトラップのサポート（続き）

MIB とトラップ	説明
CISCO-FIREWALL-MIB	FWSM は、MIB のブラウジングをサポートします。 FWSM は、次のグループのブラウジングをサポートします。 • cfwSystem フェールオーバー ステータスに関する cfwSystem.cfwStatus の情報は、シングルコンテキストだけではなくデバイス全体に関係します。 FWSM は、次のテーブルのブラウジングをサポートします。 • cfwConnectionStatTable
CISCO-IPSEC-FLOW-MONITOR-MIB	FWSM は、MIB のブラウジングをサポートします。 FWSM は、次のトラップを送信します。 • start • stop
CISCO-L4L7-RESOURCE-LIMIT-MIB	FWSM は、MIB のブラウジングをサポートします。 FWSM は、次のトラップのブラウジングをサポートします。 • limit-reached • rate-limit-reached FWSM は、次のテーブルのブラウジングをサポートします。 • ciscoL4L7ResourceLimitTable • ciscoL4L7ResourceRateLimitTable
CISCO-MEMORY-POOL-MIB	FWSM は、次のテーブルのブラウジングをサポートします。 • ciscoMemoryPoolTable：このテーブルに記載されるメモリ使用状況は、セキュリティ アプライアンスの汎用プロセッサのみに適用され、ネットワーク プロセッサには適用されません。
CISCO-NAT-EXT-MIB	FWSM は、MIB のブラウジングをサポートします。
CISCO-PROCESS-MIB	FWSM は、MIB のブラウジングをサポートします。 FWSM は、次のテーブルのブラウジングをサポートします。 • cpmCPUTotalTable FWSM は、次のトラップを送信します。 • rising threshold
CISCO-REMOTE-ACCESS-MONITOR-MIB	FWSM は、MIB のブラウジングをサポートします。 FWSM は、次のトラップを送信します。 • session-threshold-exceeded
CISCO-SYSLOG-MIB	FWSM は、次のトラップを送信します。 • clogMessageGenerated この MIB はブラウジングできません。

表 13-1　SNMP の MIB とトラップのサポート（続き）

MIB とトラップ	説明
CISCO-UNIFIED-FIREWALL-MIB	FWSM は、MIB のブラウジングをサポートします。 FWSM は、次のグループのブラウジングをサポートします。 • cufwUrlFilterGlobals：このグループは、グローバル URL フィルタリングの統計情報を提供します。
IF-MIB	FWSM は、次のテーブルのブラウジングをサポートします。 • ifTable • ifXTable
MIB-II	FWSM は、次のグループおよびテーブルのブラウジングをサポートします。 • system
NAT-MIB	FWSM は、MIB のブラウジングをサポートします。 FWSM は、次のトラップを送信します。 • packet-discard FWSM は、次のテーブルのブラウジングをサポートします。 • natAddrBindTable • natAddrPortBindTable
RFC1213-MIB	FWSM は、次のテーブルのブラウジングをサポートします。 • ip.ipAddrTable
SNMP コア トラップ	FWSM は、次の SNMP コア トラップを送信します。 • authentication：NMS が正しいコミュニティ ストリングで認証しなかったために、SNMP 要求が失敗する。 • linkup：インターフェイスが「up」状態に移行した。 • linkdown：**nameif** コマンドを削除した場合などに、インターフェイスがダウンする。 • coldstart：FWSM がリロード後に動作している。
SNMPv2-MIB	FWSM は、次のブラウジングをサポートします。 • snmp
TCP-MIB	FWSM は、次のテーブルのブラウジングをサポートします。 • tcpConnectionTable
UDP-MIB	FWSM は、次のテーブルのブラウジングをサポートします。 • udpEndpointTable

SNMP のイネーブル化

FWSM で動作する SNMP エージェントは、次の 2 つの機能を実行します。

- NMS から SNMP 要求に応答する。
- トラップ（イベント通知）を NMS に送信する。

SNMP エージェントをイネーブルにして、FWSM に接続できる NMS を識別するには、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。

CHAPTER 14

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

ルーティング機能で、スタティック ルート、RIP、プロキシ ARP、OSPF、BGP のコンフィギュレーション パラメータを指定できます。

FWSM でのルーティングの設定の詳細については、次の項目を参照してください。

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 ペインを使用します。

一部の場合では、セッションのリターン トラフィックが送信元とは異なるインターフェイスを経由してルート指定されることがあります。フェールオーバー コンフィギュレーションでは、1 つの装置で送信元となった接続のリターン トラフィックが、ピア装置を経由して戻る場合があります。これが最もよく発生するのは、1 つの FWSM 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 FWSM が、異なるサービス プロバイダーに接続されており、発信接続で NAT アドレスが使用されていない場合です。デフォルトでは、FWSM はリターン トラフィックをドロップします。これは、トラフィックの接続情報がないためです。

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がセッション情報を持た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。

（注） フェールオーバー コンフィギュレーションでは、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。

一致する情報が見つからないと、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 コンフィギュレーションのピア装置で発信すると、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で発信すると、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リダイレクトされます。

フィールド

ASR Group テーブルには、FWSM の各インターフェイスの次の情報が表示されます。

- Interface：FWSM 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。有効値の範囲は 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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Routing

Dynamic Routing 領域では、スタティック ルートの編集、または OSPF パラメータや RIP パラメータの設定ができます。詳細については、次の項目を参照してください。

- BGP スタブ ルーティング
- OSPF
- RIP

BGP スタブ ルーティング

FWSM は BGP スタブ ルーティングをサポートします。BGP スタブ ルーティング プロセスは、スタティック ルートおよび直接接続されたルートをアドバタイズします。詳細については、次の項目を参照してください。

- BGP スタブ ルーティングの制限事項（P.14-3）
- BGP スタブ ルーティングの設定（P.14-3）
- BGP（フィールド情報）（P.14-4）

BGP ルーティング プロセスのモニタリングの詳細については、P.28-1 の「BGP のモニタリング」を参照してください。

BGP スタブ ルーティングの制限事項

FWSM への BGP スタブ ルーティングの設定には、次の制限事項が適用されます。

- マルチコンテキスト モードであっても、BGP ルーティング プロセスは 1 つしか設定できません。
- BGP ネイバーは 1 つしか設定できません。
- FWSM では、BGP ネイバーから受信した UPDATE メッセージは処理されません。ルーティング アップデートを BGP ネイバーへ送信するだけです。
- 他のルーティング プロセスで検出されたルートを BGP ルーティング プロセスに再配布することはできません。
- BGP スタブでは、IPv6、VPN、NLRI のマルチキャストはサポートされていません。
- iBGP のみがサポートされており、eBGP はサポートされていません。

BGP スタブ ルーティングの設定

FWSM に BGP スタブ ルーティングを設定する前に、次の手順を実行します。

- BGP ネイバーでルート リフレクタをイネーブルにする必要があります。このオプションの設定の詳細については、BGP ネイバーのマニュアルを参照してください。
- FWSM がマルチコンテキスト モードの場合、BGP スタブ ルーティングを設定するには、管理コンテキストにいる必要があります。さらに、管理コンテキストはルーテッド モードである必要があります。

BGP ルーティング プロセスをイネーブルにし設定するには、次の手順を実行します。

ステップ 1　**Configuration > Routing > Dynamic Routing > BGP** に移動します。マルチコンテキスト モードの場合、BGP スタブ ルーティングを設定するには、管理コンテキストにいる必要があります。

ステップ 2　**Enable BGP Routing** チェックボックスをクリックして、BGP ルーティング プロセスをイネーブルにします。

ステップ 3　**Router AS** フィールドで、自律システム番号を FWSM に割り当てます。自律システム番号は、BGP ピアの AS 番号と同一でなければなりません。1 ～ 65535 の範囲の値を指定できます。

ステップ 4　（オプション）**Router ID** フィールドで、FWSM のルータ ID を入力します。ルータ ID は FWSM で設定されていないものも含め、任意の IP アドレスが可能です。ルータ ID を入力しない場合は、FWSM に設定されている最上位の IP アドレスが使用されます。

ステップ 5　次の手順を実行して、BGP アップデートが送信される BGP ネイバーを指定します。

a. **Neighbor Address** フィールドに、BGP ネイバーの IP アドレスを入力します。

b. **Remote AS** フィールドに、BGP ネイバーの自律システム番号を入力します。1 ～ 65535 の範囲の値を指定できます。

c. （オプション）**Password** フィールドに、ネイバーへの BGP メッセージの認証に使用するパスワードを入力します。**Confirm Password** フィールドに、同じパスワードを再入力します。

このパスワードは BGP メッセージ交換前に、ネイバーと FWSM の両方に設定する必要があります。パスワードは、数字、英字、または次の記号で構成できます。

` ~ ! @ # $ % ^ & * ( ) - _ = + | \ } ] { [ " ` : ; / > < . , ?

パスワードにスペースは使用できません。

ステップ 6　（オプション）**Mode** リストから認証モードを選択します。モードを選択すると、BGP ネイバーによってモード オプションがサポートされ、同一の値が設定されます。

ステップ 7　BGP ルーティング プロセスがどのスタティック ネットワークと直接接続されたネットワークをアドバタイズするかを指定します。アドバタイズするネットワークを指定するには、次の手順を実行します。FWSM では、最大 200 のネットワークを設定できます。

a. **IP Network** フィールドで、ネットワーク アドレスを入力します。

b. ネットワーク マスクを入力するか、**Netmask** フィールドから選択します。

c. **Add** をクリックして、ネットワークを BGP Networks リストに追加します。

d. （オプション）設定したネットワークを BGP Networks リストから削除するには、ネットワークを選択し **Delete** をクリックします。

ステップ 8　**Apply** をクリックして、FWSM に変更内容を保存します。

BGP（フィールド情報）

BGP ペインでは、BGP ルーティング プロセスをイネーブルにして、設定することができます。デバイスでは、1 度に 1 つずつのみ BGP ルーティング プロセスをイネーブルにできます。

フィールド

BGP Routing Parameters

- Enable BGP Routing：BGP 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。BGP ルーティング プロセス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。
- Router AS：FWSM の自律システム番号です。

- Router ID：FWSM のルータ ID です。ルータ ID は、IP アドレス形式で入力します。FWSM でローカルに設定されていないアドレスであっても、有効な IP アドレスであれば使用できます。入力しない場合、ルータ ID には FWSM に設定されている最上位の IP アドレスを使用します。

BGP Neighbor：BGP Neighbor 領域では、BGP ルーティング アップデートの送信先である BGP ネイバーを定義できます。

- Neighbor Address：BGP ネイバーの IP アドレスです。
- Remote AS：BGP ネイバーの自律システム番号です。
- Password：BGP メッセージの MD5 認証に使用されるパスワードを入力します。BGP ネイバーは、同一のパスワードを設定する必要があります。
- Mode：リストからパスワード モードを選択します。
- Confirm Password：パスワードを再入力します。

BGP Networks：BGP Networks 領域では、BGP ルーティング プロセスがアドバタイズできるネットワークを定義できます。

- BGP Networks：BGP ルーティング プロセスがアドバタイズできるネットワークを表示します。
- IP Network：ネットワーク アドレスを入力します。
- Netmask：IP Network に適用するマスクです。リストから標準のネットワーク マスクを選択するか、フィールドでマスクを入力できます。
- Add：クリックして、定義されたネットワークを BGP Networks テーブルに追加します。
- Delete：クリックして、BGP Networks テーブルから選択されたネットワークを削除します。

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
•	—	•	—	—

詳細情報

BGP スタブ ルーティング（P.14-3）

BGP のモニタリング（P.28-1）

OSPF

OSPF は、パスの選択に距離ベクトルではなくリンク状態を使用する内部ゲートウェイ ルーティング プロトコルです。OSPF は、ルーティング テーブル更新ではなくリンクステート アドバタイズメントをプロパゲートします。ルーティング テーブル全体ではなく、LSA だけが変更されるため、OSPF ネットワークは、RIP ネットワークよりすばやく集約できます。

OSPF は、MD5 およびクリア テキスト ネイバー認証をサポートします。OSPF と他のプロトコル（RIP など）の間でのルート再配布は、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、すべてのルーティング プロトコルに可能な限り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、パブリック エリアおよびプライベート エリアで OSPF が実行されている場合、およびアドレス フィルタリングが必須である場合、2 つの OSPF プロセスを実行する必要があります。このとき、1 つはパブリック エリアのプロセス用、もう 1 つはプライベート エリアのプロセス用になります。

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ルーティング プロトコルを使用している他のルータとの間に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、使用可能なルート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、FWSM 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）は、あるエリアから別のエリアにフィルタリングできます。このフィルタリングにより、プライベート ネットワークをアドバタイズすることなく NAT と OSPF を一緒に使用できます。

（注） フィルタリングできるのは、タイプ 3 LSA だけです。FWSM 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 ネットワークを記述するタイプ 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 エリアでのみ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、FWSM で保護されているプライベート ネットワークにスタティック ルートを設定する必要があります。また、同一 FWSM インターフェイス上にパブリック ネットワークとプライベート ネットワークを混在させないでください。

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。

- Setup
- Interface
- Static Neighbor
- Virtual Link
- Filtering
- Redistribution
- Summary Address

Setup

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て、OSPF ルート集約を定義できます。

（注） RIP がイネーブルの場合は、OSPF をイネーブルにできません。

これらのエリアの設定の詳細については、次の項目を参照してください。

- Setup > Process Instances タブ
- Setup > Area/Networks タブ
- Setup > Route Summarization タブ

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

OSPF プロセス インスタンスを 2 つまでイネーブルにできます。各 OSPF プロセスは、独自の関連エリアおよびネットワークを持ちます。

フィールド

- OSPF Process 1 および OSPF Process 2：各グループ ボックスには、特定の OSPF プロセスのための設定が含まれます。
- Enable this OSPF Process：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。FWSM で RIP がイネーブルの場合は、OSPF プロセスをイネーブルにできません。OSPF プロセスを削除するには、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。1 ～ 65535 の範囲の値を指定できます。
- 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、djacency Changes、Administrative Route Distances、Timers、および Default Information Originate の各種設定を実行できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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** ボックスに 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、FWSM 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：このチェックボックスをオンにすると、FWSM がタイプ 6（MOSPF）LSA パケットを受信したときの syslog メッセージの送信を抑止します。この機能はデフォルトでオフになっています。

- RFC 1583 Compatible：このチェックボックスをオンにすると、RFC 1583 あたりのサマリー ルート コストを計算します。このチェックボックスをオフにすると、RFC 2328 あたりのサマリー ルート コストが計算されます。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、syslog メッセージが送信されます。
  - Log Adjacency Changes：このチェックボックスをオンにすると、OSPF ネイバーが起動またはダウンするたびに FWSM が syslog メッセージを送信します。この設定は、デフォルトでオンになっています。
  - Log Adjacency Changes Detail：このチェックボックスをオンにすると、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 FWSM が syslog メッセージを送信します。この機能はデフォルトで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管理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管理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管理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管理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 がトポロジー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：このチェックボックスをオンにすると、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します。
  - Always advertise the default route：このチェックボックスをオンにすると、デフォルト ルートを常にアドバタイズします。このオプションは、デフォルトで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：（オプション）適用するルート マップの名前です。ルート マップが確認された場合、ルーティング プロセスではデフォルト ルートが生成されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 タブでは、FWSM 上の各 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、通常、スタブ、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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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。FWSM でイネーブルになっている OSPF プロセスが 1 つのみの場合は、デフォルトでそのプロセスが選択されています。既存のエリアを編集する場合、OSPF プロセス ID は変更できません。
- 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。エリア ID は、10 進数または IP アドレスのいずれかで指定できます。有効な 10 進数値の範囲は、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。最初にエリアを設定するときは、デフォルトでこのオプションが選択されています。

- 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 エリアは、範囲外のルータまたはエリアを持つことができません。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。このチェックボックスは、スタブ エリアの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、**Redistribute** 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。このチェックボックスは、NSSA のデフォルトでオンになっています。
- Default Information Originate：このチェックボックスをオンにすると、タイプ 7 デフォルトを NSSA に生成します。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 エリアの作成には、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 つのエリアでのみ使用できます。

    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 グループ ボックス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：このオプションを選択すると、OSPF エリア認証をディセーブルにします。これはデフォルトの設定です。
  - Password：このオプションを選択すると、エリア認証にクリア テキスト パスワードを使用します。セキュリティが重要な場合、このオプションはお勧めできません。
  - 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 つのエリアから別のエリアにネットワークを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ている外部ルートのサマリー アドレスを定義するには、「Summary Address」を参照してください。

フィールド

- Route Summarization：FWSM 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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。既存のルート集約エントリを編集するときは、この値を変更できません。
- Area ID：ルート集約を適用するエリア ID を選択します。既存のルート集約エントリを編集するときは、この値を変更できません。
- 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、ボックスにマスクを入力します。
- Advertise：このチェックボックスをオンにすると、アドレス範囲ステータスを「アドバタイズ」に設定します。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 を抑止するには、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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、インターフェイス固有の OSPF 認証ルーティング 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 タブでは、FWSM 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：FWSM 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。認証タイプは、次のいずれかです。

    None：OSPF 認証はディセーブルです。

    Password：クリア テキスト パスワード認証がイネーブルです。

    MD5：MD5 認証がイネーブルです。

    Area：エリアに指定した認証タイプがインターフェイス上でイネーブルです。インターフェイスでは、エリア認証がデフォルト値です。ただし、エリア認証はデフォルトでディセーブルです。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、エリア認証が表示されているインターフェイスでは、認証がディセーブルになっています。
- 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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：このオプションを選択すると、OSPF 認証をディセーブルにします。
  - 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。セキュリティが重要な場合、このオプションはお勧めできません。
  - 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：8 文字まで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 認証を使用しているインターフェイス上のすべてのデバイスが、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：数字キー ID を入力します。有効値の範囲は 1 ～ 255 です。
    Key：16 バイトまでの英数字の文字列です。
  - 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 タブでは、テーブル形式で各インターフェイスに定義された OSPF プロパティが表示されます。

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、「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の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、「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、「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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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：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ブロードキャスト インターフェイスであることを指定します。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定義できるネイバーは 1 つのみです。
  - ネイバーは手動で設定する必要があります（「Static Neighbor」を参照）。
  - 暗号化エンドポイントを指定しているスタティック　ルートを定義する必要があります（「Static Route」を参照）。
  - トンネル経由の　OSPF　がインターフェイス上で実行されている場合、アップストリーム ルータを使用した通常の OSPF は、同一インターフェイス上で実行できません。
  - OSPF の更新が VPN トンネルを通過するように OSPF ネイバーを指定する前に、暗号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暗号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、両方が代表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代表ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が代表ルータになります。

  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代表ルータになったり、代表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、ネイバーが DBD パケットを交換したときに実行されます。DBD パケットで受信される MTU が受信インターフェイスで設定された IP MTU より高い場合、OSPF 隣接関係は確立されません。
- Database Filter：このチェックボックスをオンにすると、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します。デフォルトでは、OSPF は、LSA が到達するインターフェイスを除き、同一エリア内のすべてのインターフェイスで新しい LSA をフラッディングします。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と、選択したインターフェイスでの OSPF LSA のフラッディングが抑止されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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のみ、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 間隔が小さいほど、トポロジの変更が速く検出されますが、インターフェイス上にはより多くのトラフィックが送信されることになります。この値は、すべてのルータに対して同じで、特定のインターフェイス上でサーバにアクセス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、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。ルータが LSA をネイバーに送信するとき、確認応答メッセージを受信するまで LSA を保持します。ルータが確認応答を受信しない場合、LSA を再送信します。この値の設定は慎重に行ってください。不要な再送信につながることがあります。値は、シリアル回線と仮想リンクに対して十分な大きさにしてください。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。更新パケットの LSA は、送信前にこのボックスで指定された時間により、有効期限が長くなります。リンクでの送信前に遅延が追加されない場合、LSA がリンクでプロパゲートする時間は考慮されません。割り当てられた値では、インターフェイスの送信およびプロパゲート遅延を考慮に入れる必要があります。この設定は、超低速リンクで顕著に現れます。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。有効値の範囲は、1 ～ 65535 です。この設定のデフォルト値は、Hello Interval ボックスで設定した間隔の 4 倍です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ペインでは、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、非ブロードキャスト インターフェイスのそれぞれに、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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、非ブロードキャスト インターフェイスのそれぞれに、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 Route」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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 エリアに直接接続することができない場合、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。いずれかの OSPF デバイスがバックボーン 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、選択したエントリを対象とした 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：選択したエントリを対象とした 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、新しい仮想リンクの定義や、既存の仮想リンクのプロパティの変更が実行できます。

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 エリアまたはスタブ エリアを選択することはできません。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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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：このオプションを選択すると、OSPF 認証をディセーブルにします。
  - 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。セキュリティが重要な場合、このオプションはお勧めできません。
  - 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：8 文字まで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 認証を使用しているインターフェイス上のすべてのデバイスが、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：数字キー ID を入力します。有効値の範囲は 1 ～ 255 です。

    Key：16 バイトまでの英数字の文字列です。
  - 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 間隔が小さいほど、トポロジの変更が速く検出されますが、インターフェイス上にはより多くのトラフィックが送信されることになります。この値は、すべてのルータに対して同じで、特定のインターフェイス上でサーバにアクセス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、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。ルータが LSA をネイバーに送信するとき、確認応答メッセージを受信するまで LSA を保持します。ルータが確認応答を受信しない場合、LSA を再送信します。この値の設定は慎重に行ってください。不要な再送信につながることがあります。値は、シリアル回線と仮想リンクに対して十分な大きさにしてください。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。更新パケットの LSA は、送信前にこのボックスで指定された時間により、有効期限が長くなります。リンクでの送信前に遅延が追加されない場合、LSA がリンクでプロパゲートする時間は考慮されません。割り当てられた値では、インターフェイスの送信およびプロパゲート遅延を考慮に入れる必要があります。この設定は、超低速リンクで顕著に現れます。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。有効値の範囲は、1 ～ 65535 です。このボックスのデフォルト値は、Hello Interval ボックスで設定した間隔の 4 倍です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ペインでは、各 OSPF プロセスに設定された ABR タイプ 3 LSA フィルタを表示します。

ABR タイプ 3 LSA フィルタにより、指定したプレフィックスのみを 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 エリアに、または OSPF エリアから同一の OSPF エリアに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

ABR から発信されたタイプ 3 LSA のみがフィルタリングされます。

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、選択したエントリを対象とした 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 に適用されているとき、最も低いシーケンス番号の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：選択したフィルタを変更するための 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、既存のフィルタを変更できます。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 に適用されているとき、最も低いシーケンス番号の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 ボックスに入力したネットワーク マスクの長さより大きく、Upper Range ボックスに入力した値がある場合は、その値と同じか小さい必要があります。
  - 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 ボックスに入力した値がある場合は、その値と同じかより大きい必要があります。Lower Range ボックスを空白のままにした場合は、Filtered Network ボックスに入力したネットワーク マスク長の長さより大きい必要があります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ペインでは、あるルーティング ドメインから別のルーティング ドメインへルートが再配布されるときのルールを表示します。

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、選択したエントリを対象とした 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：ルートはスタティック ルートです。
  - Connected：インターフェイス上で IP をイネーブルにしたことで、ルートが自動的に確立されました。これらのルートは、AS の外部として再配布されます。
  - OSPF：ルートは、別のプロセスからの OSPF ルートです。
- Match：あるルーティング プロトコルから別のルーティング プロトコルにルートが再配布されるときに使用する条件を表示します。
- Subnets：サブネット化されたルートが再配布される場合、「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しません。
- 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を使用する場合、再配布エントリに対してこのカラムは空白です。
- 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。この値を OSPF 自身が使用することはありません。ASBR 間の情報の通信に使用されます。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変更するための 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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：ルートはスタティック ルートです。
  - Connected：インターフェイス上で IP をイネーブルにしたことで、ルートが自動的に確立されました。接続済みルートは、AS の外部として再配布されます。
  - OSPF：ルートは、別のプロセスからの OSPF ルートです。

    OSPF：再配布されるルートの OSPF プロセス ID を選択します。
- Match：あるルーティング プロトコルから別のルーティング プロトコルにルートが再配布されるときに使用する条件を表示します。ルートが再配布されるには、選択した条件に一致する必要があります。次の一致条件から 1 つまたは複数を選択できます。
  - Internal：特定の AS に対してルートは内部的です。
  - External 1：ルートは自律システムに対して外部的ですが、タイプ 1 外部ルートとして OSPF にインポートされます。
  - External 2：ルートは自律システムに対して外部的ですが、タイプ 2 外部ルートとして OSPF にインポートされます。
  - NSSA External 1：ルートは自律システムに対して外部的ですが、タイプ 1 NSSA ルートとして OSPF にインポートされます。
  - NSSA External 2：ルートは自律システムに対して外部的ですが、タイプ 2 NSSA ルートとして OSPF にインポートされます。

- 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、ある OSPF プロセスから別の OSPF プロセスに再配布を行うとき、メトリック値が指定されていない場合は、あるプロセスから別のプロセスにメトリック値が引き継がれます。別のプロセスから 1 つの OSPF プロセスに再配布するとき、メトリック値が指定されていない場合のデフォルト値は 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。この値を OSPF 自身が使用することはありません。ASBR 間の情報の通信に使用されます。有効値の範囲は 0 ～ 4294967295 です。
- Use　Subnets：このチェックボックスをオンにして、サブネット化されたルートの再配布をイネーブルにします。サブネット化されていないルートのみを再配布するには、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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ペインでは、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を表示します。

他のルーティング プロトコルから取得したルートは、集約が可能です。サマリーのアドバタイズに使用されるメトリックは、すべての特定ルートの中で最も小さいメトリックです。サマリー ルートは、ルーティング テーブルのサイズを減らすのに役立ちます。

OSPF でサマリー ルートを使用すると、このアドレスでカバーされる再配布ルートすべての集約として、1 つの外部ルートが OSPF ASBR からアドバタイズされます。OSPF に再配布される他のルーティング プロトコルからのルートのみ集約可能です。

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、選択したエントリを対象とした 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。この値を OSPF 自身が使用することはありません。ASBR 間の情報の通信に使用されます。

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対象とした 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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ときは、この情報を変更できません。
- 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ときは、この情報を変更できません。
- 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ときは、この情報を変更できません。
- Advertise：このチェックボックスをオンにすると、サマリー ルートをアドバタイズします。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：（オプション）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。この値を OSPF 自身が使用することはありません。ASBR 間の情報の通信に使用されます。有効値の範囲は 0 ～ 4294967295 です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 とは、パスの選択のためのメトリックとしてホップ カウントを使用する、距離ベクトル ルーティング プロトコルです。インターフェイス上で RIP がイネーブルになっているとき、インターフェイスはネイバーのデバイスと RIP ブロードキャストを交換し、ダイナミックにルートを取得してアドバタイズします。

FWSM 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、可変長サブネット マスクをサポートします。さらに、RIP バージョン 2 は、ルーティング更新が交換されるときのネイバー認証をサポートします。認証により、FWSM は信頼できるルーティング情報を信頼の置けるソースから受け取ることができます。

（注） OSPF プロセスが実行中の場合は、RIP をイネーブルにできません。

制限事項

RIP には次の制限事項があります。

- FWSM は、インターフェイス間に RIP 更新を渡すことができません。
- RIP バージョン 1 は、可変長サブネット マスクをサポートしません。
- RIP の最大ホップ カウントは 15 です。ホップ カウントが 15 以上のルートは、到達不能と見なされます。
- RIP コンバージェンスは、他のルーティング プロトコルに比べ、低速です。

RIP バージョン 2 の注意点

次の情報は、RIP バージョン 2 にのみ該当します。

- ネイバー認証を使用する場合、認証キーおよびキー 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 デバイスで同じになっている必要があります。
- RIP バージョン 2 では、FWSM 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更新を受信します。
- RIP バージョン 2 がインターフェイス上に設定されているとき、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で登録されます。RIP バージョン 2 のコンフィギュレーションがインターフェイスから移動されると、マルチキャスト アドレスの登録は解除されます。

フィールド

- RIP：RIP の設定情報を表示します。RIP テーブルの行をダブルクリックすると、Add/Edit RIP Configuration ダイアログボックスが開き、選択した RIP 設定のパラメータを変更できます。
  - Interface：RIP がイネーブルになっているインターフェイス名を表示します。
  - Action：選択したインターフェイス上で RIP に設定したアクションを表示します。このカラムは、インターフェイスが RIP 更新のみを送信するように設定されている場合は「BCast default route」を、インターフェイスが RIP 更新のみを受信するように設定されている場合は「Passive RIP」を、インターフェイスが RIP 更新を送受信するように設定されている場合は「BCast default route & Passive RIP」を表示します。
  - Version：インターフェイス上で RIP のどのバージョンがイネーブルかを表示します。
  - Auth Type：指定したインターフェイス上の RIP バージョン 2 認証の認証タイプを表示します。このカラムは、MD5 認証がイネーブルの場合は「MD5」を、プレーンテキスト認証がイネーブルの場合は「Text」を表示し、認証がイネーブルでない場合は空白になります。

  - Auth Key：指定したインターフェイス上の RIP バージョン 2 認証に使用される認証キーを表示します。このカラムは認証がイネーブルでない場合は空白になります。
  - Key ID：指定したインターフェイス上の RIP バージョン 2 認証に使用される認証キーの ID 番号を表示します。このカラムは認証がイネーブルでない場合は空白になります。
- Add：Add/Edit RIP Configuration ダイアログボックスが開きます。新しい RIP 設定を FWSM に追加する場合は、このボタンを使用します。
- Edit：Add/Edit RIP Configuration ダイアログボックスが開きます。選択した RIP 設定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 RIP 設定を削除します。インターフェイスから RIP バージョン 2 のコンフィギュレーションを削除すると、マルチキャスト アドレス 224.0.0.9 はそのインターフェイスから登録解除されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 RIP Configuration

Add RIP Configuration ダイアログボックスでは、新しい RIP 設定を FWSM に追加できます。新しい RIP 設定を追加することによって、選択したインターフェイスの RIP をイネーブルにします。Edit RIP Configuration ダイアログボックスでは、既存の RIP 設定を変更できます。

フィールド

- Interface：RIP 設定用インターフェイスを指定します。同じインターフェイスに 2 つの異なる RIP 設定を指定することはできません。
- Action options：選択したインターフェイスの RIP 更新の動作を設定します。次のアクションから選択できます。
  - Broadcast/multicast default route：選択したインターフェイスを、RIP ルーティング更新を送信するように設定します。
  - Passive RIP：選択したインターフェイスを、RIP ルーティング ブロードキャストをリッスンし、その情報を使用してルーティング テーブルに入力するように設定します。ただし、RIP ルーティング更新は送信しないようにします。
  - BCast Default route & Passive RIP: 選択したインターフェイスを、RIP ルーティング更新を送受信するように設定します。
- Version options：選択したインターフェイス上でイネーブルである RIP のバージョンを選択します。次のバージョンから選択できます。
  - RIP バージョン 1：このオプションを選択すると、インターフェイス上で RIP バージョン 1 がイネーブルになります。
  - RIP バージョン 2：このオプションを選択すると、インターフェイス上で RIP バージョン 2 がイネーブルになります。インターフェイス上で RIP バージョン 2 を設定すると、マルチキャスト アドレス 224.0.0.9 を登録します。

- Version 2 Authentication：RIP バージョン 2 で使用される認証タイプをイネーブルにして選択できる設定を含んでいます。
  - Enable Authentication：このチェックボックスをオンにすると、RIP ネイバー認証をイネーブルにします。RIP ネイバー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。
  - MD5：（推奨）認証に MD5 ハッシュ アルゴリズムを使用します。
  - Clear text：認証のクリア テキストを使用します。
  - Key：認証に使用する共有キーです。このキーはアップデートを FWSM に送信し、FWSM から受信する他のすべてのデバイスと共有する必要があります。このボックスは、16 文字まで入力できます。
  - Key ID：認証キーの ID 番号です。この番号は、アップデートを FWSM に送信し、FWSM から受信する他のすべてのデバイスと共有する必要があります。有効値の範囲は 1 ～ 255 です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Route

Static Route ペインでは、スタティック ルートを作成し、FWSM がホストまたはネットワークを宛先としたネットワーク パケットを正しく転送できるようにします。また、スタティック ルートを使用して、ダイナミック ルートで検出されたメトリックより低いメトリックでスタティック ルートを指定することで、このホストまたはネットワークに対して検出されたダイナミック ルートを上書きできます。インターフェイス（ECMP）あたり最大 3 つの等コスト ルートが同じ宛先に定義できます。複数のインターフェイス間を通る Equal Cost Multi-Path routing（ECMP; 等コスト マルチパス ルーティング）はサポートされていません。ECMP では、トラフィックはルート間で必ずしも均等に分割されません。トラフィックは、送信元と宛先の IP アドレスをハッシュするアルゴリズムに従って指定のゲートウェイ間に分散されます。

デフォルト ルートを入力するには、IP アドレスとマスクを 0.0.0.0 または簡単な形式の 0 に設定します。デバイスあたり最大 3 つの等コスト デフォルト ルート エントリが定義できます。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。

1 つの FWSM 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、FWSM 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。

フィールド

Static Route ペインには、Static Route テーブルが表示されます。

- Interface：ルートが適用するインターフェイス名を一覧表示します。
- IP Address：宛先ネットワーク 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。IP アドレス 0.0.0.0 は、0 に短縮できます。
- Netmask：宛先アドレスのネットワーク マスクを一覧表示します。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：このルートのネクストホップ ルータの IP アドレスを一覧表示します。
- Metric：ルートの管理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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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では、スタティック ルートを追加または編集できます。

フィールド

- Interface Name：ルートが適用するインターフェイス名を指定します。
- IP Address：宛先ネットワーク 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。IP アドレス 0.0.0.0 は、0 に短縮できます。
- Mask：宛先アドレスのネットワーク マスクを指定します。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：このルートのネクストホップ ルータの IP アドレスを指定します。
- Metric：ルートの管理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。

  管理ディスタンスは、異なるルーティング プロトコルのルート比較に使用するパラメータです。スタティック ルートのデフォルトの管理ディスタンスは 1 です。これは、ダイナミック ルーティング プロトコルが検出したルートより優先されますが、直接接続されたルートよりは優先されません。OSPF が検出したルートのデフォルトの管理ディスタンスは 110 です。スタティック ルートがダイナミックに検出されたルートと同じ管理ディスタンスを持っている場合は、スタティック ルートが優先されます。接続されたルートは、常にスタティック ルートまたはダイナミックに検出されたルートに優先します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

状況によっては、グローバル アドレスのプロキシ ARP をディセーブルにする場合があります。

ホストが同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信するとき、ホストはそのデバイスの MAC アドレスを知っている必要があります。ARP は、MAC アドレスに対して IP アドレスを解決するレイヤ 2 プロトコルです。ホストは、「この IP アドレスはだれのものか」と尋ねる ARP 要求を送信します。その IP アドレスを持つデバイスは「その IP アドレスは自分のもので、これが MAC アドレスである」と応答します。

プロキシ ARP は、デバイスが自身の IP アドレスを持たなくても、ARP 要求に自身の MAC アドレスで応答する場合に使用されます。NAT を設定し、FWSM 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き、FWSM はプロキシ ARP を使用します。FWSM がプロキシ ARP を使用する場合、トラフィックがホストに到達するためには、FWSM 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必要があります。

フィールド

- Interface：インターフェイス名を一覧表示します。
- 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、すべての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ます。
- 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 15

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、シングルモード、ルーテッド モードでのみサポートされます。ここでは、次の項目について説明します。

- マルチキャスト ルーティング（P.15-2）：FWSM 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.15-3）：FWSM で IGMP を設定します。
- MForwarding（P.15-9）：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。
- MRoute（P.15-10）：スタティック マルチキャスト ルートを定義します。
- PIM（P.15-12）：セキュリティ アプライアンスで PIM を設定します。

マルチキャスト ルーティング

Multicast ペインでは、FWSM 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 ルーティングをイネーブルにすることで、デフォルトですべてのインターフェイス上の IGMP および PIM がイネーブルになります。IGMP は、直接接続されたサブネットにグループのメンバーが存在するかどうかを認識するために使用します。ホストは、IGMP レポート メッセージを送信してマルチキャスト 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転送テーブルを維持します。

（注） マルチキャスト ルーティングでサポートされているのは、UDP トランスポート レイヤだけです。

フィールド

Enable Multicast Routing：FWSM での IP マルチキャスト 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。IP マルチキャスト 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。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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ルーティングの詳細については、次の項目を参照してください。

- IGMP
- MForwarding
- PIM

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 はグループ アドレス（クラス D IP アドレス）を使用します。ホスト グループ アドレスは、224.0.0.0 ～ 239.255.255.255 の範囲で使用できます。アドレス UDP224.0.0.0 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。

FWSM での IGMP の設定の詳細については、次の項目を参照してください。

- Protocol
- Access Group
- Join Group
- Static Group

Access Group

アクセス グループ制御は、インターフェイス上で許可されるマルチキャスト グループを制限します。

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 グループを表示します。

  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、許可ルールにあるグループを含むマルチキャスト グループの範囲を拒否するアクセス グループ エントリは下方に配置します。そのグループは、拒否ルールの前に許可ルールが強制されるため、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、選択したエントリを対象とした 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を表示します。
  - Action：アクセス ルールでマルチキャスト グループ アドレスが許可される場合、「Permit」を表示します。アクセス ルールでマルチキャスト グループ アドレスが拒否される場合は「Deny」を表示します。
  - 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 アドレスを表示します。
  - Netmask：マルチキャスト グループ アドレスのネットワーク マスクを表示します。
- Insert：Add/Edit Access Group ダイアログボックスを開きます。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には、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。テーブルの一番下に新しいアクセス グループ エントリを追加するには、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には、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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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とき、一部のフィールドは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 グループを編集するときは、関連インターフェイスを変更できません。
- 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には「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には「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 マスクの 1 つを選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

FWSM をマルチキャスト グループのメンバーとして設定できます。Join Group ペインでは、FWSM がメンバーになっているマルチキャスト グループを表示します。

（注） 特定のグループのマルチキャスト パケットを、FWSM にグループの一部として受け入れさせずに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 メンバーシップを表示します。
  - Interface：FWSM インターフェイスの名前を表示します。

— Multicast Group Address：インターフェイスの属するマルチキャスト グループのアドレスを表示します。

- 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には、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には、このボタンを使用します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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には、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には、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 FWSM 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場合、この値は変更できません。
- Multicast Group Address：このボックスにマルチキャスト 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 で入力する必要があります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ペインでは、FWSM 上の各インターフェイスの IGMP パラメータを表示します。

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 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を表示します。
  — 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」を表示します。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」を表示します。
  — Version：インターフェイス上でイネーブルになっている IGMP のバージョンを表示します。
  — Query Interval：指定したルータが IGMP ホストクエリー メッセージを送信する間隔を秒数で表示します。

- Query Timeout：前のクエリアが引き継ぎを停止した後で、FWSM がインターフェイスのクエリアとして引き継ぐまでの期間を表示します。
- Response Time：IGMP クエリーでアドバタイズされる最大応答時間を秒数で表示します。この設定への変更は、IGMP バージョン 2 に対してのみ有効です。
- Group Limit：インターフェイスで許可される最大グループ数を表示します。
- Forward Interface：選択したインターフェイスが IGMP ホスト レポートを転送するインターフェイスの名前を表示します。

• Edit：選択したインターフェイスを対象とした Configure IGMP Parameters ダイアログボックスが開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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て、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

- Interface：設定しているインターフェイスの名前を表示します。このフィールドに表示される情報は変更できません。
- Enable IGMP：インターフェイスで IGMP 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。インターフェイスで IGMP 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。FWSM でマルチキャスト ルーティングをイネーブルにした場合、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、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。デフォルトでは、FWSM は IGMP バージョン 2 を使用します。
- Query Interval：指定したルータが IGMP ホストクエリー メッセージを送信する間隔を秒数で入力します。有効値の範囲は 1 ～ 3600 秒です。デフォルト値は、125 秒です。
- Query Timeout：前のクエリアが引き継ぎを停止した後で、FWSM がインターフェイスのクエリアとして引き継ぐまでの期間を秒数で入力します。有効値の範囲は 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数で入力します。指定した応答時間内に FWSM がホスト レポートを受信しない場合、IGMP グループはプルーニングされます。この値を少なくすると、FWSM がグループをプルーニングするのが速くなります。有効値の範囲は 1 ～ 12 秒です。デフォルト値は、10 秒です。この値への変更は、IGMP バージョン 2 に対してのみ有効です。
- 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には「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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

一部の場合では、IGMP クエリーへの応答を防ぐコンフィギュレーションがネットワーク上のホストに設定されていることがあります。それでもマルチキャスト トラフィックをそのネットワーク セグメントに転送するとします。その場合、マルチキャスト トラフィックをネットワーク セグメントに届ける方法は 2 つあります。

- Join Group ペインを使用して、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。この方法では、FWSM が、マルチキャスト パケットを指定したインターフェイスに転送するだけでなく、そのパケットを受け入れます。
- Static Group ペインを使用して、FWSM をスタティックに接続されたグループ メンバーになるように設定します。この方法では、FWSM はパケット自体を受け取ることはなく、転送するだけです。したがって、この方法では高速スイッチングが実現できます。発信インターフェイスが IGMP キャッシュに表示されますが、そのインターフェイス自身はマルチキャスト 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の、スタティックに割り当てられたマルチキャスト グループを表示します。
  - Interface：FWSM インターフェイスの名前を表示します。
  - 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を表示します。
- 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 グループを追加するには、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には、このボタンを使用します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

マルチキャスト グループをインターフェイスにスタティックに割り当てるには、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には、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 FWSM 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場合、この値は変更できません。
- Multicast Group Address：このボックスにマルチキャスト 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 で入力する必要があります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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。

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ると、他の方法で特に設定されていない限り、インターフェイスはマルチキャスト パケットを受け入れません。また、IGMP パケットは、マルチキャスト転送がディセーブルになっているときも拒否されます。

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：FWSM で設定されたインターフェイスを表示します。インターフェイスを選択するには、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 Yes を表示します。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 を表示します。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の 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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.15-1）

MRoute

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、発信元と宛先の間のパスがマルチキャスト ルーティングをサポートしていない場合、2 つのマルチキャスト デバイス間に GRE トンネルを設定し、そのトンネルを経由してマルチキャスト パケットを送信することが解決策となります。

スタティック マルチキャスト ルートは、FWSM に対してローカルであり、アドバタイズも再配布もされません。

フィールド

- Multicast Route：FWSM でスタティックに定義されたマルチキャスト ルートを表示します。テーブルのエントリをダブルクリックすると、そのエントリを対象とした Add/Edit Multicast Route ダイアログボックスが開きます。
  - Source Address：マルチキャストの発信元の IP アドレスとマスクを CIDR 表記で表示します。
  - Source Interface：マルチキャスト ルートの着信インターフェイスを表示します。
  - Destination Interface：マルチキャスト ルートの発信インターフェイスを表示します。
  - Admin Distance：スタティック マルチキャスト ルートの管理ディスタンスを表示します。
- 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 ルートを追加するには、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 ルートを変更するには、このボタンを使用します。
- Delete：選択したスタティック ルートを削除するには、このボタンを使用します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

新しいスタティック マルチキャスト ルートを FWSM に追加するには、Add Multicast Route を使用します。既存のスタティック マルチキャスト ルートを変更するには、Edit Multicast Route を使用します。

フィールド

- Source Address：マルチキャストの発信元の 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、この値を変更できません。
- Source Mask：マルチキャストの発信元の 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、この値を変更できません。
- 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：（オプション）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、選択したインターフェイスを介してルートが転送されます。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 ルートの管理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 ルートの管理ディスタンスがユニキャスト ルートの管理ディスタンスと同じ場合、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

次の表に、この機能を使用できるモードを示します。

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

PIM

ルータは、PIM を使用してマルチキャスト データグラムを転送する転送テーブルを維持します。

FWSM でマルチキャスト ルーティングをイネーブルにするとき、PIM はデフォルトですべてのインターフェイスでイネーブルになります。PIM はインターフェイスごとにディセーブルにできます。

PIM の設定の詳細については、次の項目を参照してください。

- Protocol
- Rendezvous Points
- Request Filter
- Route Tree

Protocol

Protocol ペインでは、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 設定を表示します。テーブルのエントリをダブルクリックすると、そのエントリを対象とした Edit PIM Protocol ダイアログボックスが開きます。
  - Interface：FWSM インターフェイスの名前を表示します。
  - 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」を、イネーブルになっていない場合は「No」を表示します。
  - DR Priority：インターフェイスの優先度を表示します。
  - Hello Interval：インターフェイスが PIM の hello メッセージを送信する頻度を秒数で表示します。
  - Join-Prune Interval：インターフェイスが PIM の加入およびプルーニング アドバタイズメントを送信する頻度を秒数で表示します。
- Edit：選択したエントリを対象とした Edit PIM Protocol ダイアログボックスが開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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：選択されたインターフェイスの名前を表示します。この値は編集できません。
- PIM Enabled：選択したインターフェイスで PIM 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で PIM 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。

- DR Priority：選択したインターフェイスの指定ルータの優先順位を設定します。サブネットで高い DR 優先順位を持つルータは、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 優先順位は 1 です。この値を 0 に設定すると、適切でない FWSM インターフェイスがデフォルト ルータになります。
- Hello Interval：インターフェイスが PIM hello メッセージを送信する頻度を秒数で入力します。有効値の範囲は 1 ～ 3600 秒です。デフォルト値は、30 秒です。
- Join-Prune Interval：インターフェイスが PIM 加入およびプルーニング アドバタイズメントを送信する頻度を秒数で入力します。有効値の範囲は 10 ～ 600 秒です。デフォルト値は、60 秒です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 を設定するとき、ランデブー ポイント（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、共有配布ツリーの単一で共通のルートで、各ルータでスタティックに設定されます。最初のホップ ルータは、RP を使用し、発信元マルチキャスト ホストの代わりに登録パケットを送信します。

1 つの RP が複数のグループに機能するように設定できます。特定のグループが指定されていない場合は、IP マルチキャスト グループ全体の範囲（224.0.0.0/4）にグループの RP が適用されます。

複数の RP を設定できますが、同じ RP 内で保持できるエントリは 1 つです。

フィールド

- Generate IOS compatible register messages：RP が Cisco IOS ルータの場合、このチェックボックスをオンにします。FWSM ソフトウェアは、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共に登録メッセージを受け入れる方法）ではなく、PIM ヘッダーにあるチェックサムおよび次の 4 バイトのみと共に登録メッセージを受け入れます。
- Rendezvous Points：FWSM で設定された RP を表示します。
  - Rendezvous Point：RP の IP アドレスを表示します。
  - Multicast Groups：RP に関連付けられたマルチキャスト グループを表示します。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、「--All Groups--」を表示します。
  - 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、「Yes」を表示します。指定したグループが希薄モードで動作する場合は「No」を表示します。
- 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には、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には、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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 アドレスを 2 回使用することはできません。
- 複数の RP に All Groups を指定することはできません。

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 エントリを編集するときは、この値を変更できません。
- 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、FWSM がマルチキャスト パケットを受信し、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、送信元にプルーニング メッセージを戻します。指定したマルチキャスト グループを希薄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） FWSM は、実際の双方向構成にかかわらず、PIM の hello メッセージを使用して双方向の機能を常時アドバタイズします。

- Use this RP for All Multicast Groups：インターフェイス上のすべてのマルチキャスト グループの指定した RP を使用するには、このオプションを選択します。
- Use this RP for the Multicast Groups as specified below：マルチキャスト グループを指定した RP で使用するように指定するには、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 グループを表示します。

  テーブル エントリは、上から下の順で処理されます。特定のグループの拒否ルールをテーブルの一番上に、マルチキャスト グループの範囲の許可ルールを deny 文の下にそれぞれ配置すれば、マルチキャスト グループの範囲を含みながらその範囲内の特定グループを除外する RP エントリを作成できます。

  エントリをダブルクリックすると、選択したエントリを対象とした 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」を、マルチキャスト グループが除外される場合は「deny」を表示します。

  — Multicast Group Address：マルチキャスト グループのアドレスを表示します。

  — Netmask：マルチキャスト グループ アドレスのネットワーク マスクを表示します。
- 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には、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に新しいマルチキャスト グループ エントリを追加するには、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。テーブルの一番下に新しいマルチキャスト グループ エントリを追加するには、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には、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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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。マルチキャスト グループには、1 つのマルチキャスト アドレスまたはマルチキャスト アドレスの範囲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 ルールを作成するには、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 ルールを変更するには、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 ルールを作成するには、「Permit」を選択します。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 ルールを作成するには、「Deny」を選択します。
- 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

FWSM が RP として動作しているとき、特定のマルチキャスト送信元の登録を制限できます。この制限により、認可されない送信元が RP で登録されなくなります。Request Filter ペインでは、FWSM が PIM 登録メッセージを受け入れるマルチキャストの送信元を定義できます。

フィールド

- Multicast Groups：要求フィルタ アクセス ルールを表示します。

  テーブル エントリは、上から下の順で処理されます。特定のグループの拒否ルールをテーブルの一番上に、マルチキャスト グループの範囲の許可ルールを deny 文の下にそれぞれ配置すれば、マルチキャスト グループの範囲を含みながらその範囲内の特定グループを除外するエントリを作成できます。

  エントリをダブルクリックすると、選択したエントリを対象とした 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」を、マルチキャストの送信元が除外される場合は「deny」を表示します。
  - Source：登録メッセージの送信元のアドレスを表示します。
  - Destination：マルチキャストの宛先アドレスを表示します。
- 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には、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に新しいマルチキャスト グループ エントリを追加するには、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。テーブルの一番下に新しいマルチキャスト グループ エントリを追加するには、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には、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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、FWSM が RP として動作するときにマルチキャストの送信元が FWSM で登録できるように定義します。フィルタ ルールは、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 FWSM での登録を許可するルールを作成するには「Permit」を選択します。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 FWSM での登録を許可しないルールを作成する場合は「Deny」を選択します。
- 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。この加入によって遅延は少なくなりますが、共有ツリーより多くのメモリが必要となります。

すべてのマルチキャスト グループに対して、または特定のマルチキャスト アドレスに対して、FWSM 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 ツリーを使用するには、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には、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には、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 グループを表示します。

  テーブル エントリは、上から下の順で処理されます。特定のグループの拒否ルールをテーブルの一番上に、マルチキャスト グループの範囲の許可ルールを deny 文の下にそれぞれ配置すれば、マルチキャスト グループの範囲を含みながらその範囲内の特定グループを除外するエントリを作成できます。

  エントリをダブルクリックすると、選択したエントリを対象とした 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」を、マルチキャスト グループが除外される場合は「deny」を表示します。
  - Multicast Group Address：マルチキャスト グループのアドレスを表示します。
  - Netmask：マルチキャスト グループ アドレスのネットワーク マスクを表示します。
- 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には、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に新しいマルチキャスト グループ エントリを追加するには、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。テーブルの一番下に新しいマルチキャスト グループ エントリを追加するには、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には、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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

ファイアウォール モードの概要

この章では、ファイアウォール モードの設定方法と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。ファイアウォール モードは、マルチコンテキスト モードのコンテキストごとに個別に設定できます。

FWSM（またはマルチモードの各コンテキスト) は、2 つのファイアウォール モードのいずれかで動作できます。

- ルーテッド モード
- 透過モード

この章には、次の項があります。

ルーテッド モードの概要

ルーテッド モードでは、FWSM はネットワーク内のルータ ホップと見なされます。（シングルコンテキスト モードでは）OSPF または受動 RIP を使用できます。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おり、各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が、いくつかの制限事項があります。

FWSM 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（パッシブ モードで）。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 FWSM 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。

透過モードの概要

透過ファイアウォールは、「bump-in-the-wire（BITW）」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、透過ファイアウォール モードについて説明します。次の項目を取り上げます。

透過ファイアウォール ネットワーク

FWSM 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。透過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。IP 再アドレッシングは必要ありません。

透過ファイアウォールに接続されているホストの NAT をオプションでイネーブルにできます。

ブリッジ グループ

セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、ブリッジ グループと呼ばれる最大 8 つのペアのインターフェイスを設定できます。各ブリッジ グループは別々のネットワークに接続します。ブリッジ グループのトラフィックは、他のブリッジ グループから隔離され、トラフィックは FWSM 内の他のブリッジ グループにルーティングされません。また、トラフィックは、外部ルータから FWSM 内の他のブリッジ グループにルーティングされる前に、FWSM から出る必要があります。ブリッジング機能はブリッジ グループごとに別々のものですが、他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、すべてのブリッジ グループはシステム ログ サーバまたは AAA サーバ コンフィギュレーションを共有します。セキュリティ ポリシーを完全に分離するには、各コンテキストで単一ブリッジ グループを持つセキュリティ コンテキストを使用します。

透過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。IP 再アドレッシングは必要ありません。トラブルシューティングが必要な複雑なルーティング パターンがないため、メンテナンスが容易です。

（注） 各ブリッジ グループには、管理 IP アドレスが必要です。FWSM は、この IP アドレスをブリッジ グループから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。

レイヤ 3 トラフィックの許可

透過モードはブリッジとして機能しますが、IP トラフィックなどのレイヤ 3 トラフィックは、拡張アクセスリストで明示的に許可されない限り、FWSM を通過できません。アクセスリストなしで透過ファイアウォールを通過できるトラフィックは ARP トラフィックだけです。ARP トラフィックは ARP 検査によって制御されます。

許可された MAC アドレス

次の宛先 MAC アドレスは、透過ファイアウォールから許可されます。このリストにない MAC アドレスはすべてドロップされます。

- 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 マルチキャストアドレス

ルーテッド モードで許可されてい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 FWSM を通過できません。一方、透過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（IP 以外のトラフィックの場合）を使用して、ほとんどのタイプのトラフィックを通過させることができます。

（注） 透過モードの FWSM は、CDP パケット、または 0x600 以上の有効な EtherType を持たないパケットは通過させません。たとえば、IS-IS パケットを通過させることはできません。サポートされている BPDU は例外です。

たとえば、透過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することができます。同様に、HSRP や VRRP などのプロトコルは FWSM 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。

透過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、（サポートされない DHCP リレー機能の代わりに）DHCP トラフィックを許可したり、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したりできます。

MAC アドレスとルート ルックアップ

FWSM が NAT を使用せずに透過モードで動作している場合、パケットの発信インターフェイスは、ルート ルックアップではなく MAC アドレス ルックアップを実行することによって決定されます。この場合もルート文を設定することはできますが、FWSM から発信されたトラフィックだけに適用されます。たとえば、syslog サーバがリモート ネットワークにある場合は、FWSM がそのサブネットに到達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。

このルールの例外は、音声検査を使用している場合とエンドポイントが FWSM から少なくとも 1 ホップ離れている場合です。たとえば、CCM と H.323 ゲートウェイの間に透過ファイアウォールを使用し、透過ファイアウォールと H.323 ゲートウェイの間にルータがあり、コールをうまく完了するために H.323 ゲートウェイの FWSM にスタティック ルートを追加する必要がある場合です。

NAT を使用する場合は、FWSM は MAC アドレス ルックアップではなく、ルート ルックアップを使用します。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、実際の宛先アドレスが FWSM に直接接続されていない場合は、ダウンストリーム ルータをポイントする実際の宛先アドレスの FWSM にスタティック ルートを追加する必要があります。

ネットワークでの透過ファイアウォールの使用

図 16-1 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透過ファイアウォール 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 16-1　透過ファイアウォール ネットワーク

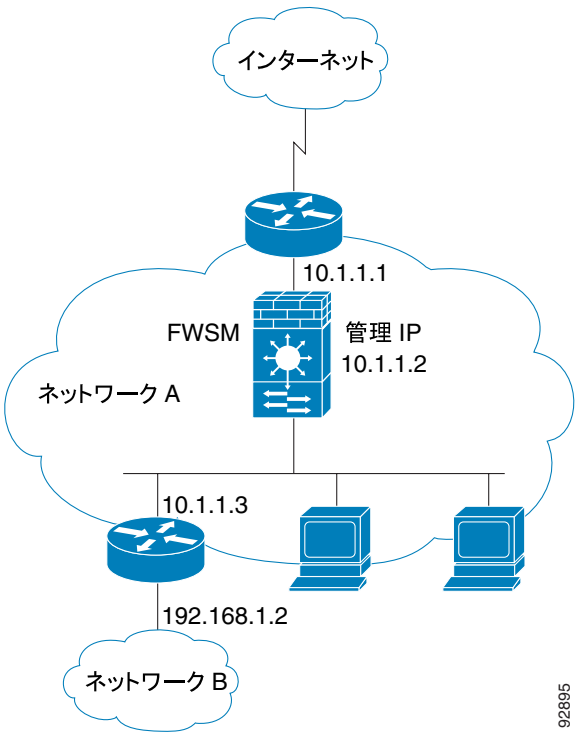
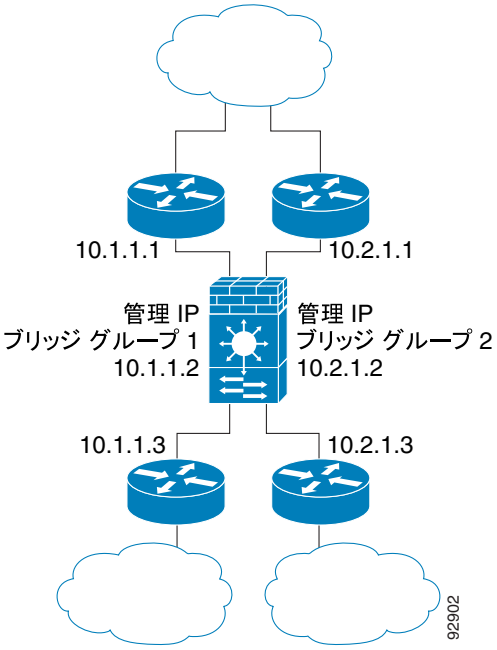


図 16-2 は、2 つのブリッジ グループを持つ FWSM に接続された 2 つのネットワークを示しています。

図 16-2　2 つのブリッジ グループを持つ透過ファイアウォール ネットワーク



透過ファイアウォール ガイドライン

透過ファイアウォール 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。

- ブリッジ グループごとに管理 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、透過ファイアウォールではブリッジ グループ全体に IP アドレスが割り当てられます。FWSM は、この IP アドレスを、システム メッセージや AAA 通信など、FWSM 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。管理 IP サブネットの詳細については、P.5-7 の「ブリッジ グループの追加または編集」を参照してください。
- 各ブリッジ グループは、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。
- 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ブリッジ グループ管理 IP アドレスを指定しないでください。デバイスは FWSM 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。
- 透過ファイアウォールのデフォルト ルートは、管理トラフィックにリターンパスを提供しなければならないため、1 つのブリッジ グループ ネットワークからの管理トラフィックにだけ適用されます。デフォルト ルートがブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定するため、デフォルト ルートを 1 つしか定義できません。複数のブリッジ グループ ネットワークからの管理トラフィックがある場合は、そこからの管理トラフィックを想定するネットワークを識別するスタティック ルートを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。
- 拡張アクセスリストを使用し、IP トラフィックなどのレイヤ 3 トラフィックが FWSM を通過できるようにする必要があります。

  オプションで、EtherType アクセスリストを使用して IP 以外のトラフィックの通過を許可することもできます。

透過モードでサポートされていない機能

表 16-1 に透過モードでサポートされていない機能を示します。

表 16-1　透過モードでサポートされていない機能

サポートされていない機能	説明
ダイナミック ルーティング プロトコル	ただし、FWSM 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 FWSM を通過できるようにすることもできます。
ブリッジ グループ IP アドレスの IPv6	ただし、EtherType アクセスリストを使用して IPv6 EtherType を通過させることができます。
DHCP リレー	透過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。拡張アクセスリストを使用して DHCP トラフィックの通過を許可できるため、DHCP リレーは不要です。
スイッチのループガード	FWSM が透過モードの場合は、スイッチの LoopGuard をグローバルにイネーブルにしないでください。ループガードは、スイッチと FWSM 間の内部 EtherChannel に自動的に適用されます。そのため、EtherChannel が err-disable 状態になると、フェールオーバーおよびフェールバック後にセカンダリ装置がループガードによって切断されます。
マルチキャスト	ただし、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 FWSM を通過できるようにすることができます。
管理用リモート アクセス VPN	管理用サイトツーサイト VPN を使用できます。

CLI での透過またはルーテッド ファイアウォール モードの設定

ASDM のシングルモードでは、モードの変更はできません。マルチモードでは、ASDM の管理コンテキストモードでのモード変更はできません。CLI でモードの変更をする必要があります。

モードを変更すると、FWSM はコンフィギュレーションをクリアします。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。すでに実装済みのコンフィギュレーションがある場合は、モードを変更する前に必ずコンフィギュレーションのバックアップを作成してください。新しくコンフィギュレーションを作成するときにこのバックアップを参照する場合があります。

firewall transparent コマンドでモードを変更する FWSM にテキスト コンフィギュレーションをダウンロードする場合は、必ずこのコマンドをコンフィギュレーションの最上部に置いてください。これによって、FWSM は、このコマンドを読み取り次第すぐにモードを変更し、その後は、ダウンロードしたコンフィギュレーションの読み取りを続けます。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、FWSM 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。

- 透過モードに設定するには、各コンテキストで次のコマンドを入力します。

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

- ルーテッド モードに設定するには、各コンテキストで次のコマンドを入力します。

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

CHAPTER 17

アクセス ルールと EtherType ルールの設定

この章では、アクセス ルールと EtherType ルール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) アクセス ルールを使用して、ルーテッド ファイアウォール モードおよび透過ファイアウォール モードの両方のネットワーク アクセスを制御します。透過モードでは、アクセス ルール（レイヤ 3 トラフィックの場合）と EtherType ルール（レイヤ 2 トラフィックの場合）の両方を使用できます。

管理アクセスのために FWSM インターフェイスにアクセスする場合、ホスト IP アドレスを許可するアクセス ルールも必要ありません。ただし、第 11 章「Device Access」に従って、管理アクセスを設定する必要があります。

アクセス ルールと EtherType ルールの概要

アクセス ポリシーは、1 つのインターフェイスごとに 1 つ以上のアクセス ルールと EtherType ルールで構成されます。

ルーテッド ファイアウォール モードおよび透過ファイアウォール モードでアクセス ルールを使用して、IP トラフィックを制御できます。アクセス ルールは、プロトコル、送信元および宛先 IP アドレスまたはネットワーク、オプションで送信元および宛先ポートに基づいてトラフィックを許可または拒否します。

（注） すべてのトラフィックが FWSM に入るのを許可するには、インターフェイスに着信アクセス ルールを設定する必要があります。設定しない場合、FWSM は、そのインターフェイスに入るすべてのトラフィックを自動的にドロップします。

透過モードでは、EtherType ルールは IP トラフィック以外のネットワーク アクセスを制御します。EtherType ルールは、EtherType に基づいてトラフィックを許可または拒否します。

ここでは、次の項目について説明します。

アクセス ルールと EtherType ルールについて

この項では、アクセス ルールと EtherType ルールの両方に関する情報を提供します。次の項目を取り上げます。

同じインターフェイスでのアクセス ルールと EtherType ルールの使用

インターフェイスの各方向に、アクセス ルールと EtherType ルールの両方を適用できます。

ルールの順序

ルールの順序は重要です。FWSM がパケットを転送するかドロップするかを決定すると、FWSM はルールが記載されている順序で各ルールに対してパケットをテストします。一致が見つかると、その後のルールはチェックされません。たとえば、最初にインターフェイスのすべてのトラフィックを明示的に許可するアクセス ルールを作成した場合、その後のルールは一切チェックされません。

ルールを非アクティブにすることで、そのルールをディセーブルにできます。

暗黙拒否

アクセス ルールまたは EtherType ルールのリストには、リストの最後に暗黙拒否があります。そのため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除いて、FWSM を経由してすべてのユーザがネットワークにアクセスできるようにする場合、特定のアドレスを拒否して、他のすべてのアドレスを許可する必要があります。

EtherType ルールでは、暗黙拒否は、IPv4 トラフィックまたは ARP に影響しません。たとえば、EtherType 8037（IPX の EtherType）を許可した場合、リストの最後の暗黙拒否は、アクセス ルールを使用して以前許可したすべての IP トラフィックをブロックしません。IPv4 および ARP トラフィックは、EtherType ルールで制御できません。

ルールのコミットメント

アクセス ルールまたは EtherType ルールを適用すると、FWSM は、そのルールをネットワーク プロセッサにコミットすることでアクティブにします。FWSM は、ルールを最後に適用した後、短時間待ってからルールをコミットします。コミットメントの開始後にルールを適用した場合、FWSM は、コミットメントを打ち切り、短時間待ってからルールを再コミットします。ルールをコミットした後、FWSM は次のようなメッセージを表示します。

```
Access Rules Download Complete: Memory Utilization: < 1%
```

サイズによっては、約 6 万個のルールで構成される大きなリストはコミットに 3 ～ 4 分かかることがあります。

メモリの制限を超える場合については、「アクセス ルールおよび EtherType ルールの最大数」の項を参照してください。

アクセス ルールおよび EtherType ルールの最大数

FWSM では、システム全体に対して、アクセス ルールおよび EtherType ルールの最大数をサポートしています。アクセス ルールと EtherType ルール、およびその他のタイプのルールを含む、ルールの制限については P.A-7 の「ルール制限」を参照してください。

アクセス ルールによっては他のルールよりも多くのメモリを使用するものがあり、それらには、広範囲のポート番号または重複ネットワークを使用するルールが含まれます（たとえば、あるアクセス ルールで 10.0.0.0/8 を指定し、他のルールで 10.1.1.0/24 を指定すると、結果的に重複ネットワークがあるルールとなります）。アクセス ルールのタイプによっては、システムがサポートできる実際の制限は最大数よりも少なくなります。

アクセス ルールでオブジェクト グループを使用すると、入力する実際のルールの数は少なくなりますが、*拡張*ルールの数はオブジェクト グループを使用しない場合と同じになり、拡張ルールの数はシステム制限に近づきます。アクセス ルールの拡張ルール数を表示するには、CLI ツールを使用して **show access-list** コマンドを入力します。

ルールを追加して、FWSM がルールをコミットすると、コンソールに使用されたメモリ量が次のようなメッセージで表示されます。

```
Access Rules Download Complete: Memory Utilization: < 1%
```

メモリ制限を超えた場合、エラー メッセージとシステム ログ メッセージ（106024）が表示され、そのコミットメントで追加されたすべてのアクセス ルールがコンフィギュレーションから削除されます。以前のコミットメントで正常にコミットされたルールのセットのみが使用されます。たとえば、1000 個のルールを適用し、最後のルールがメモリ制限を超えている場合、1000 個のルールがすべて拒否されます。

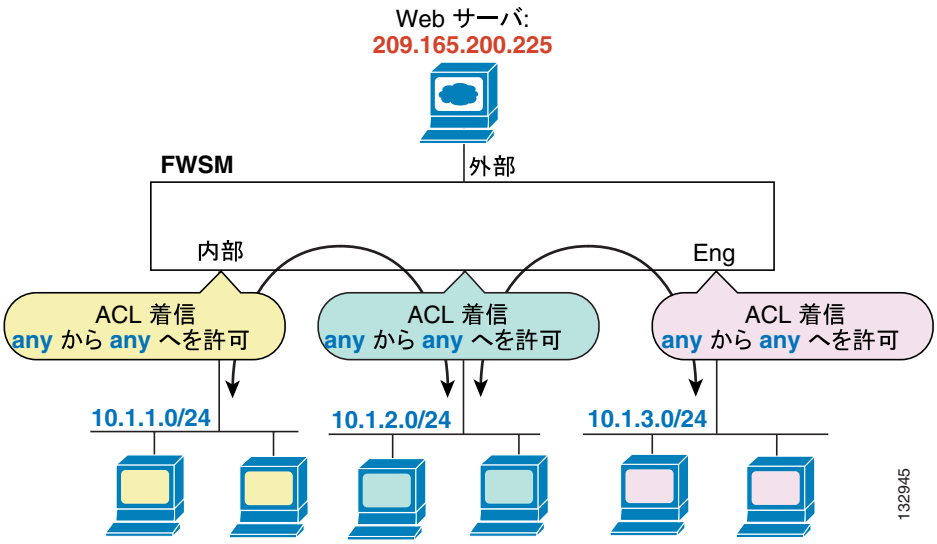
着信ルールと発信 ルール

FWSM のインターフェイスを流れるトラフィックは 2 つの方向で制御できます。FWSM に入るトラフィックは、送信元インターフェイスに着信アクセス ルールを設定することで制御できます。FWSM を出るトラフィックは、宛先インターフェイスに発信アクセス ルールを設定することで制御できます。すべてのトラフィックが FWSM に入るのを許可するには、インターフェイスに着信アクセス ルールを設定する必要があります。設定しない場合、FWSM は、そのインターフェイスに入るすべてのトラフィックを自動的にドロップします。デフォルトで、着信アクセス ルールですでに設定されているルールに制限を追加する発信アクセス ルールを使用して制限していない限り、トラフィックはすべてのインターフェイスで FWSM から出ることができます。

（注） 「着信」および「発信」とは、インターフェイスでのアクセス　ルールの適用のことであり、インターフェイス上の FWSM に入るトラフィック、またはインターフェイス上の FWSM を出るトラフィックのいずれかを指します。これらの用語は、一般に着信と呼ばれる、セキュリティの低いインターフェイスからセキュリティの高いインターフェイスへのトラフィックの移動、または一般に発信と呼ばれる、セキュリティの高いインターフェイスから低いインターフェイスへのトラフィックの移動のことを指すものではありません。

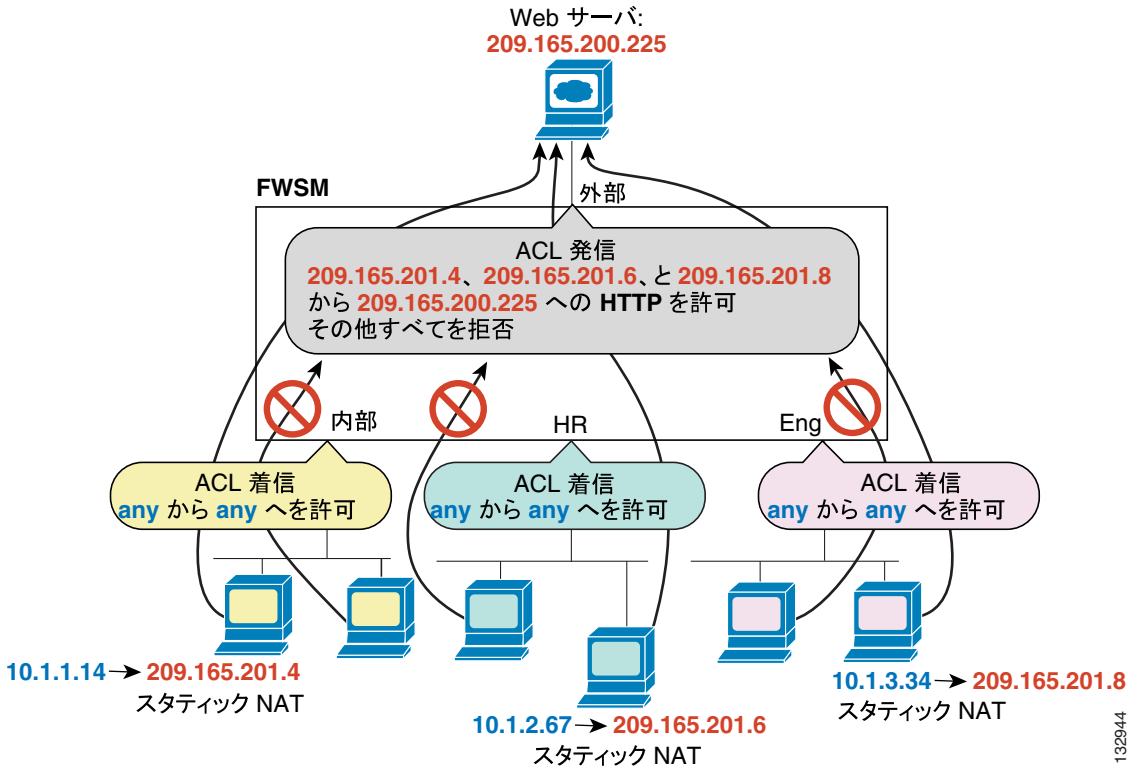
発信アクセス ルールを使用してコンフィギュレーションを単純化することも可能です。たとえば、3 つの異なるインターフェイスで 3 つの内部ネットワークの相互アクセスを許可する場合、各内部インターフェイスですべてのトラフィックを許可する単純な着信アクセス ルールを作成できます（図 17-1 を参照してください）。

図 17-1　着信アクセス ルール



内部ネットワークの特定のホストにのみ、外部ネットワークの Web サーバへのアクセスを許可する場合、指定したホストだけを許可するより限定的なアクセス ルールを作成して、外部インターフェイスの発信方向に適用することができます（図 17-2 を参照してください）。NAT および IP アドレスについては、P.17-5 の「NAT を使用する場合にアクセス ルールに使用される IP アドレス」を参照してください。発信アクセス ルールは、他のホストが外部ネットワークに到達することを防ぎます。

図 17-2　発信アクセス ルール



アクセス ルールの概要

この項では、アクセス ルールについて説明します。次の項目を取り上げます。

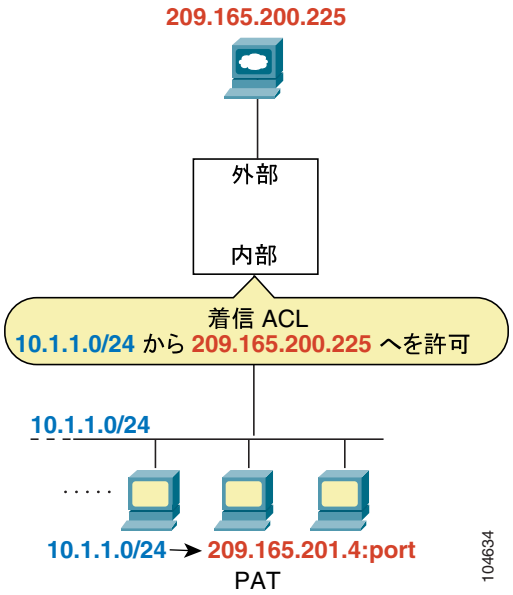
- NAT を使用する場合にアクセス ルールに使用される IP アドレス（P. 17-5）
- 戻りトラフィックのアクセス ルール（P. 17-7）
- アクセス　ルールを使用した透過ファイアウォール経由のブロードキャストおよびマルチキャスト トラフィックの許可（P. 17-7）

NAT を使用する場合にアクセス ルールに使用される IP アドレス

NAT を使用する場合、アクセス ルールに指定する IP アドレスは、アクセス ルールを設定するインターフェイスによって異なります。つまり、インターフェイスに接続されているネットワークで有効なアドレスを使用する必要があります。このガイドラインは、着信アクセス ルールと発信アクセス ルールの両方に適用されます。したがって、使用されるアドレスは方向によって決まりません。インターフェイスによってのみ決まります。

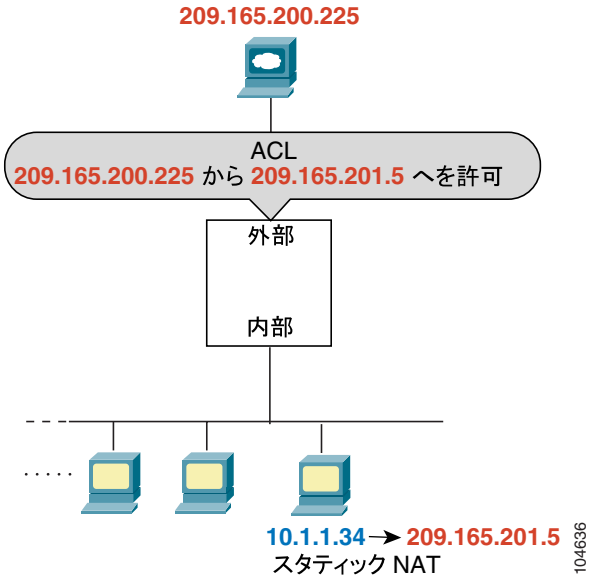
たとえば、内部インターフェイスの着信方向にアクセス ルールを適用するとします。この場合、内部送信元アドレスが外部アドレスにアクセスするときに、それらのアドレス上で NAT を実行するように FWSM を設定します。アクセス ルールは内部インターフェイスに適用されるため、送信元アドレスは元の変換されていないアドレスになります。外部アドレスは変換されていないため、アクセス ルールで使用される宛先アドレスは実際のアドレスになります（図 17-3 を参照してください）。

図 17-3　アクセス ルールの IP アドレス：送信元アドレスに使用される NAT



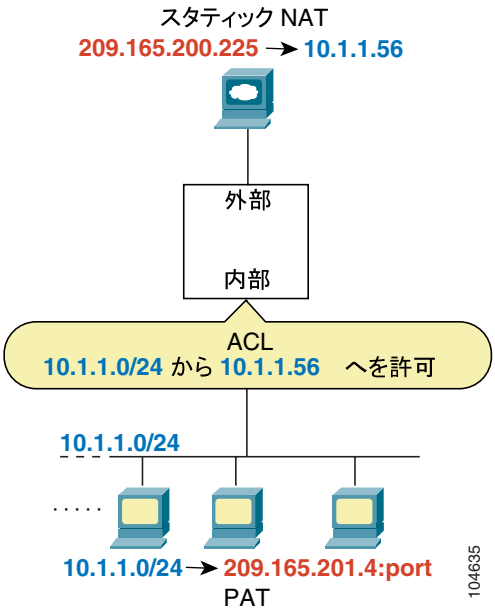
外部ホストが内部ホストにアクセスできるようにすると、外部インターフェイスで着信アクセス ルールを適用できます。内部ホストの変換済みアドレスは外部ネットワークで使用可能なアドレスであるため、アクセス ルールにそのアドレスを指定する必要があります（図 17-4 を参照してください）。

図 17-4　アクセス ルールの IP アドレス：宛先アドレスに使用される NAT



両方のインターフェイスで NAT を実行する場合、所定のインターフェイスから見えるアドレスに留意してください。図 17-5 では、変換済みアドレスが内部ネットワークに表示されるように、外部サーバはスタティック NAT を使用しています。

図 17-5　アクセス ルールの IP アドレス：送信元アドレスおよび宛先アドレスで使用される NAT



戻りトラフィックのアクセス ルール

ルーテッド モードと透過モードの両方の TCP 接続および UDP 接続で、FWSM は、確立された双方向接続に対してすべての戻りトラフィックを許可するため、戻りトラフィックを許可するためのアクセスリストは不要です。ただし、ICMP などのコネクションレス型プロトコルでは、FWSM は、単方向セッションを確立します。したがって、双方向での ICMP を許可するアクセスリストを使用するか（送信元インターフェイスおよび宛先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）、または ICMP 検査エンジンをイネーブルにする必要があります。ICMP 検査エンジンは、ICMP セッションを双方向接続として扱います。

アクセス ルールを使用した透過ファイアウォール経由のブロードキャストおよびマルチキャスト トラフィックの許可

ルーテッド ファイアウォール モードで、アクセス ルールで許可している場合でも、サポートされていないダイナミック ルーティング プロトコルおよび DHCP を含めて（DHCP リレーを設定している場合を除く）、ブロードキャスト トラフィックとマルチキャスト トラフィックはブロックされます。透過ファイアウォール モードでは、すべての IP トラフィックの通過を許可できます。この機能は、たとえばダイナミック ルーティングを許可しないマルチコンテキスト モードで特に便利です。

（注） これらの特殊なタイプのトラフィックはコネクションレス型であり、拡張アクセスリストを両方のインターフェイスに適用する必要があるため、戻りトラフィックの通過が可能です。

表 17-1 に、透過ファイアウォールを通過させることができる一般的なトラフィック タイプを示します。

表 17-1　透過ファイアウォールの特殊なトラフィック

トラフィック タイプ	プロトコルまたはポート	注意
DHCP	UDP ポート 67 および 68	DHCP サーバをイネーブルにした場合、FWSM は DCHP パケットを通過させません。
EIGRP	プロトコル 88	—
OSPF	プロトコル 89	—
マルチキャスト ストリーム	UDP ポートはアプリケーションによって異なります。	マルチキャスト ストリームは、常にクラス D アドレス（224.0.0.0 ～ 239.x.x.x）を宛先とします。
RIP（v1 または v2）	UDP ポート 520	—

EtherType ルールの概要

この項では、EtherType ルールについて説明します。次の項目を取り上げます。

- サポートされている EtherType（P. 17-8）
- 双方向での EtherType ルールの適用（P. 17-8）
- MPLS の許可（P. 17-9）

サポートされている EtherType

EtherType ルールは、16 ビットの 16 進数で識別されるすべての EtherType を制御します。

EtherType ルールは、イーサネット V2 フレームをサポートします。

802.3 フォーマットのフレームは、タイプ フィールドではなく長さフィールドを使用するため、EtherType ルールでは処理されません。

唯一の例外は、EtherType ルールで処理する BPDU です。BPDU は、SNAP でカプセル化され、FWSM は特に BPDU を処理できるように設計されています。

FWSM のポートはトランク ポート（シスコ独自）であるため、FWSM はトランク ポート BPDU を受信します。トランク BPDU にはペイロード内に VLAN 情報があるため、BPDU を許可した場合、FWSM は発信 VLAN を使用してペイロードを変更します。

（注） フェールオーバーを使用する場合、ブリッジング ループを防止するために、EtherType ルールを使用して両方のインターフェイスの BPDU を許可する必要があります。

双方向での EtherType ルールの適用

EtherType はコネクションレス型であるため、トラフィックを双方向に通過させる場合は、両方のインターフェイスにルールを適用する必要があります。

MPLS の許可

MPLS を許可する場合、Label Distribution Protocol（LDP; ラベル配布プロトコル）および Tag Distribution Protocol（TDP; タグ配布プロトコル）の TCP 接続が FWSM を経由して確立されるようにする必要があります。これは、FWSM に接続された両方の MPLS ルータが、LDP または TDP セッションの ルータ ID として FWSM インターフェイスの IP アドレスを使用するように設定することによって行います（LDP および TDP によって、MPLS ルータはパケット転送用ラベル（アドレス）をネゴシエートできます）。

Cisco IOS ルータで、使用しているプロトコル（LDP または TDP）に応じたコマンドを入力します。*interface* は、FWSM に接続されたインターフェイスです。

```
hostname(config)# mpls ldp router-id interface force
```

または

```
hostname(config)# tag-switching tdp router-id interface force
```

アクセス ルールの設定

Access Rules ウィンドウには、ルールで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とき、このウィンドウでは、使用可能なプロトコルやポートなど、特定ホストまたはネットワークによる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リストを定義できます。

テーブル セルをダブルクリックして（またはクリックして F2 を押す）、カラムの内容を編集できます。入力を開始すると、ASDM はドロップダウンに一致する可能性のあるものを表示します。また、サイド 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追加するネットワーク オブジェクトおよびグループをドラッグすることもできます。

アクセス ルールの詳細については、P.17-2 の「アクセス ルールと EtherType ルールの概要」を参照してください。

フィールド

注：カーソルをカラムの線に重ねて二重矢印になったら、その矢印を動かしてテーブル カラムの幅を調整できます。カラムの線をクリックして希望のサイズにドラッグします。

- 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、重複するルールがあると順序によって評価が異なります。
- 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、Paste ボタンを使用して、同じパラメータを持つ新しいルールを開始できます。
- Paste：コピーまたは切り取られたルールのパラメータがあらかじめ入力された状態で、Add/Edit Rule ダイアログボックスを開きます。ダイアログボックスで何らかの修正を行い、ルールをテーブルに追加することができます。Paste ボタンをクリックすると、選択したルールの上に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、選択したルールの後にルールが追加されます。
- Find：表示をフィルタリングして、一致するルールのみを表示します。**Find** をクリックすると、Filter フィールドが開きます。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。
  - Filter ドロップダウン リスト：フィルタリングする基準を、Interface、Source、Destination、Source or Destination、Destination Service、または Rule Query のいずれかから選択します。ルール クエリーは複数の基準の集合であり、保存して繰り返し使用できます。
  - Condition ドロップダウン リスト：基準の Source、Destination、Source or Destination、および Destination Service に対して、**is** または **contains** のいずれかの条件を選択します。**is** は完全一致を意味します。Source/Destination の場合、**contains** は、指定したアドレスが含まれるネットワークに一致します。また、サービス タイプの場合は、指定したサービスが含まれるネットワークに一致します。たとえば、10.1.1.1/32 は 10.1.1.1 を含むため、10.1.1.0/24 や 10.0.0.0/8 または「any」に一致します。tcp port 80 は、「tcp」または「any」に一致します。これは、両方とも tcp port 80 を含むためです。
  - Filter フィールド：Interface タイプの場合は、このフィールドがドロップダウン リストになります。リストからインターフェイス名を選択できます。Source タイプと Destination タイプの場合には、IP アドレスを指定できます。アドレスを手動で入力するか、または **...** ボタンをクリックして Browse Address ダイアログボックスを開いてアドレスを参照します。Destination Service タイプとしては、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを指定できます。プロトコル タイプを手動で入力するか、または **...** ボタンをクリッ

クして Browse Service Groups ダイアログボックスを開き、プロトコル タイプを参照します。Filter フィールドは、カンマまたはスペースで区切って、複数のエントリを受け入れます。また、ワイルドカードも受け入れます。

  - Filter：フィルタリングを実行します。
  - Clear：一致内容および表示内容をすべてクリアします。
  - Define Query：このボタンは、Flter ドロップダウン リストから Query を選択したときに表示されます。

- Diagram：ルール テーブルの下に Rule Flow Diagram 領域を表示します。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、フロー方向、およびアクションが表示されます。
- Export：ファイルをカンマ区切り値または HTML 形式のいずれかでエクスポートします。
- Show：Real-Time Log Viewer に、選択したアクセス ルールによって生成された syslog を表示します。

次の説明では、Access Rules テーブルのカラムをまとめています。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、上のボタンで示されるオプションすべてとともに、Insert 項目と Insert After 項目が表示されます。これらの項目により、選択したルールの前（Insert）または後（Insert After）に新しいルールを挿入します。

- 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へのトラフィックが許可または拒否される 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 Type フィールドで指定した送信元からのトラフィックを許可または拒否する 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。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。ホストが発信接続を作成した後、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。アクセス ルール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ので、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示します。
- Action：ルールに適用されるアクションです（Permit または Deny）。
- Hits：ルールのヒット数を示します。このカラムは、Preferences ダイアログボックスの頻度設定に応じて、ダイナミックにアップデートされます。ヒット数は、明示的なルールにのみ適用されます。Access Rules テーブルには、暗黙のルールのヒット数は表示されません。
- Logging：アクセス ルール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**：ルールを適用す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.」という説明が付けられます。
- Addresses：IP 名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、または検索できるタブです。IP アドレス オブジェクトは、その後のルール作成で簡単に選択できるように、ルール作成の間、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ます。手動では追加、編集、または削除できません。

- Services：サービスを追加、編集、削除、または検索できるタブです。
- Time Ranges：時間範囲を追加、編集、または削除できるタブです。

モード

次の表に、この機能を使用できるモードを示します。

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

Define Query

Define Query ダイアログボックスでは、ルールを検索するときに 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：この領域には、フィルタリングのための基準が一覧表示されます。
  - 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。インターフェイスまたは送信元などです。
  - Value：「inside」など、基準の値を一覧表示します。
  - 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、照合基準に追加します。
  - Field：ルール クエリーにネストされる Interface、Source、Destination、Service、Action、または他の Rule Query などの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 タイプの場合、このフィールドはドロップダウン リストになり、インターフェイス名を選択できます。Action タイプの場合、ドロップダウン リストには Permit と Deny が表示されます。Rule Query タイプの場合、ドロップダウン リストにはすべての定義済みルール クエリーが表示されます。Source タイプと Destination タイプの場合には、IP アドレスを指定できます。アドレスを手動で入力するか、または **...** ボタンをクリックして Browse Address ダイアログボックスを開いてアドレスを参照します。Service タイプには、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを指定できます。プロトコル タイプを手動で入力するか、または **...** ボタンをクリックして Browse Service Groups ダイアログボックスを開き、プロトコル タイプを参照します。
  - Add：Match Criteria テーブルに基準を追加します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Rule

Add/Edit Access Rule ダイアログボックスでは、新しいルールの作成、または既存のルールの変更が実行できます。

アクセス ルールの詳細については、P.17-2 の「アクセス ルールと EtherType ルールの概要」を参照してください。

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 タイプを決めます。Permit または Deny のいずれかを選択します。
  - Permit：すべての一致したトラフィックを許可します。
  - Deny：すべての一致した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へのトラフィックが許可または拒否される 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 フィールドで指定した送信元からのトラフィックを許可または拒否する 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、ポート範囲、またはウェルノウン サービス名またはグループを指定するには、このオプションを選択します。

  ...：事前に設定されたリストから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：（オプション）アクセス ルールの説明を入力します。
- Enable Logging：アクセス ルールのロギングをイネーブルにします。
  - Logging Level：default、emergencies、alerts、critical、errors、warnings、notifications、informational、または debugging を指定します。
- More Options：ルールの追加の設定オプションが表示されます。
  - 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決定します。オプションは incoming または outgoing のいずれかです。
  - Source Service：送信元のプロトコルおよびサービスを指定します（TCP または UDP サービスのみ）。

    ...：事前に設定されたリストから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、ロギングの間隔を秒数で指定します。
  - 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。

    ...：事前に設定されたリストから時間範囲を選択、追加、編集、削除または検索できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Service Groups

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）を関連付けます。以後、アクセスや、IPSec ルール、コンジットなどの ASDM および CLI 内の機能でサービス 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 ポート番号と「リテラル」名（ftp、telnet、smtp など）を持つ、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レイヤ プロトコルを指します。

FWSM は、次の TCP リテラル名を許可します。

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、一意である必要があります。たとえば、サービス グループとネットワーク グループで、同じ名前を共有することはできません。

複数のサービス グループを「グループのグループ」にネストして、単一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、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。

アクセス ルールで使用しているサービス グループは、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 グループを空にすることはできません。

フィールド

- TCP：TCP 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には、このオプションを選択します。
- UDP：UDP 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には、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には、このオプションを選択します。
- Service Group table：このテーブルには、各サービス オブジェクト グループの記述名を含みます。このリストのグループを変更または削除するには、グループを選択して **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には、**Add** をクリックします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 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。重複するオブジェクト グループ名は指定できません。サービス グループ名はネットワーク グループと名前を共有できません。
- Description：サービス グループの説明を指定します。
- Service：事前に定義されたドロップダウン 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Access Rule Configuration

Advanced Access Rule Configuration ダイアログボックスでは、グローバル アクセス ルールのロギング オプションを設定できます。

ロギングがイネーブルで、パケットがアクセス ルールと一致した場合、FWSM はフロー エントリを作成して、指定された時間内で受信したパケットの数を追跡します（「ログ オプション」を参照）。FWSM は、最初のヒットがあったとき、および各間隔の終わりにシステム ログ メッセージを生成し、その間隔におけるヒットの合計数を示します。各間隔の終わりに、FWSM はヒット数を 0 にリセットします。1 つの間隔内でアクセス ルールと一致するパケットがなかった場合、FWSM 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 リソースが無制限に消費されないようにするために、FWSM は同時拒否フロー数に制限を設定します。この制限は、拒否フローに対してのみ設定されます（許可フローには設定されません）。これは、拒否フローは攻撃を示している可能性があるためです。制限に達すると、FWSM 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を作成しません。DoS 攻撃（サービス拒絶攻撃）が開始された場合、FWSM は非常に大量の拒否フローをごく短時間のうちに作成する可能性があります。拒否フロー数を制限することにより、メモリおよび CPU リソースが無制限に消費されないようにします。

アクセス ルールの詳細については、P.17-2 の「アクセス ルールと EtherType ルールの概要」を参照してください。

前提条件

アクセス ルールのアクセス コントロール エントリ（ルールとも呼ばれます）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のみ、この設定が適用されます。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：FWSM がロギングを停止する前に許可される拒否フローの最大数で、1 とデフォルト値の間です。デフォルトは 4096 です。
- Alert Interval：拒否フローの最大数に達したことを識別するシステム ログ メッセージ（番号 106101）の間の時間（1 ～ 3600 秒）です。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 ルールでユーザごとの上書き機能がイネーブルになっている場合、RADIUS サーバによって提供されるアクセス ルールは、そのインターフェイス上で設定されたアクセス ルール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っている場合、RADIUS サーバによって提供されるアクセス ルールは、そのインターフェイス上で設定されたアクセス ルールに結合されます。インターフェイスに着信アクセス ルール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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Options

Log Options ダイアログボックスでは、各アクセス ルールのロギング オプションを設定できます。グローバル ロギング オプションの設定については、P.17-15 の「Advanced Access Rule Configuration」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、一定量のメモリを消費します。潜在的な DoS 攻撃のリスクを制御するには、Access Rules ウィンドウの **Advanced** を選択して、Maximum Deny-flow 設定を実行すると役立ちます。

フィールド

- Use default logging behavior：旧式のアクセス ルール ロギング メカニズムを使用します。FWSM は、パケットが拒否されるとシステム ログ メッセージ番号 106023 を記録します。デフォルト設定に戻すには、このオプションを選択します。
- Enable logging for the rule：新しいアクセス ルール ロギング メカニズムをイネーブルにします。FWSM は、パケットがアクセス ルール（許可または拒否のいずれか）に一致したとき、システム ログ メッセージ番号 106100 を記録します。

  パケットがアクセス ルールと一致した場合、FWSM 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（Logging Interval フィールドを参照）。FWSM は、最初のヒットがあったとき、および各間隔の終わりにシステム ログ メッセージを生成し、その間隔におけるヒットの合計数を示します。各間隔の終わりに、FWSM はヒット数を 0 にリセットします。1 つの間隔内でアクセス ルールと一致するパケットがなかった場合、FWSM 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。

  Emergencies（レベル 0）：FWSM 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：FWSM がフロー統計情報を syslog に送信する前に待機する時間を秒数（1 ～ 600 秒）で設定します。この設定は、アクセス ルールと一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機能します。デフォルトは 300 秒です。

- Disable logging for the rule：アクセス ルールのすべてのロギングをディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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

EtherType ルールの設定（透過モードのみ）

EtherType Rules ウィンドウには、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、透過モードで動作するときに FWSM で非 IP 関連トラフィック ポリシーを設定するのに使用されます。透過モードでは、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。

EtherType ルールの詳細については、P.17-2 の「アクセス ルールと EtherType ルールの概要」を参照してください。

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、重複するルールがあると順序によって評価が異なります。
- 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、Paste ボタンを使用して、同じパラメータを持つ新しいルールを開始できます。
- Paste：コピーまたは切り取られたルールのパラメータがあらかじめ入力された状態で、Add/Edit Rule ダイアログボックスを開きます。ダイアログボックスで何らかの修正を行い、ルールをテーブルに追加することができます。Paste ボタンをクリックすると、選択したルールの上に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、選択したルールの後にルールが追加されます。

次の説明では、EtherType Rules テーブルのカラムをまとめています。これらのカラムの内容は、テーブル セルをダブルクリックすると編集できます。カラム ヘッダーをダブルクリックすると、選択したカラムをソート キーとして、テーブルの内容がアルファベットの昇順で並べ替えられます。ルールを右クリックすると、上のボタンで示されるオプションすべてとともに、Insert 項目と Insert After 項目が表示されます。これらの項目により、選択したルールの前（Insert）または後（Insert After）に新しいルールを挿入します。

- No：ルールの評価順序を示します。
- Action：このルールの Permit または Deny アクションです。
- Ethervalue：EtherType 値で、IPX、BPDU、MPLS-Unicast、MPLS-Multicast、または 16 ビットの 16 進数値 0x600（1536）～ 0xffff のいずれかとなります。この値により EtherType が識別されます。
- Interface：ルールが適用されるインターフェイスです。
- Direction Applied：このルールの方向で、着信トラフィックまたは発信トラフィックです。
- Description：テキストによるルールの説明で、オプションです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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。

EtherType ルールの詳細については、P.17-2 の「アクセス ルールと EtherType ルールの概要」を参照してください。

フィールド

- Action：このルールの Permit または Deny アクションです。
- Interface：このルールのインターフェイス名です。
- Apply rule to：このルールの方向で、着信トラフィックまたは発信トラフィックです。
- Ethervalue：EtherType 値で、BPDU、IPX、MPLS-Unicast、MPLS-Multicast、any（0x600 ～ 0xffff の間の任意の値）、または 16 ビットの 16 進数値 0x600（1536）～ 0xffff のいずれかとなります。この値により EtherType が識別されます。
- Description：テキストによるルールの説明で、オプションです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

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）をイネーブルにする方法について説明します。

管理アクセスの AAA については、P.11-2 の「AAA Access」を参照してください。

この章には、次の項があります。

AAA パフォーマンス

FWSM は「カットスルー プロキシ」を使用します。この方法により、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。FWSM カットスルー プロキシは、アプリケーション レイヤで最初にユーザ確認を行い、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。FWSM 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。

AAA Rules

Security Policy ペインには、ルールに示されたネットワーク セキュリティ ポリシーが表示されます。このペインには、AAA ルールのほか、他のルールのタブもあります。この項目では AAA ルールを説明します。AAA サービスの概要については、第 10 章「AAA サーバの設定」を参照してください。

AAA Rules タブを選択すると、MAC 免除ルールとともに、認証、認可、またはアカウンティング（AAA）ルールを定義できます。AAA は FWSM に、ユーザが誰か、ユーザが何を実行できるか、およびユーザが何を実行したかを知らせます。認証のみで使用することも、認可とともに使用することもできます。認可には常に認証が必要です。たとえば、内部ネットワークのサーバにアクセスする外部ユーザを認証する場合、認証だけで十分に対応します。ただし、特定のユーザがアクセスする内部サーバを制限する場合は、認可サーバを設定し、どのサーバとサービスにユーザがアクセスできるのかを指定することができます。

AAA には、ユーザ アクセスに対して、アクセスリストのみ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。登録したユーザだけがサーバに Telnet できるようにするには、AAA を設定して、認証または認可、あるいはその両方が行われたユーザだけが FWSM を通過できるようにします。サーバに独自の認証および認可がある場合、ユーザは 2 番目のユーザ名とパスワードのセットを入力します（FTP の場合、ユーザはアット マーク（@）で区切ったユーザ名とパスワードの両方を入力する必要があります）。

各 AAA ルールでは、一致トラフィックの次の特性が識別されます。

- 送信元および宛先ネットワーク
- アクション（認証、認可、またはアカウンティング。ルールでは、AAA から MAC アドレスを除外することもできます）
- AAA サーバ グループ
- サービス グループ（Telnet や FTP など）

前提条件

1. Configuration > Features > Properties > AAA Setup > AAA Server Groups ペインで、各ホストまたはサーバを定義します。
2. ローカル データベースにユーザを追加します（**Configuration > Features > Properties > Administration > User Accounts** を参照）。
3. ユーザが指定したネットワークにアクセスできることを確認します（必要に応じて「アクセス ルールの設定」を参照）。
4. AAA サーバを正しくセットアップします。

フィールド

- **Add**：新しい AAA 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**：AAA ルールを編集します。
- **Delete**：AAA 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、テーブルに表示されている順に査定されます。したがって、重複するルールがある場合、その順序が問題になります。
- 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 パラメータをコピーします。Paste ボタンを使用すれば、新しいルールを同じパラメータで開始できます。

- Paste：コピーまたは切り取ったルール パラメータが入力済みの Add/Edit Rule ダイアログボックスが開きます。ダイアログボックスで何らかの修正を行い、ルールをテーブルに追加することができます。Paste ボタンをクリックすると、選択したルールの上に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、選択したルールの後にルールが追加されます。
- Find：表示をフィルタリングして、一致するルールのみを表示します。**Find** をクリックすると、Filter フィールドが表示されます。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。
  - Filter ドロップダウン リスト：Interface、Source、Destination、Service、Action、または Rule Query の中からフィルタの基準を選択します。ルール クエリーは複数の基準の集合であり、保存して繰り返し使用できます。
  - Filter フィールド：Interface タイプの場合は、このフィールドがドロップダウン リストになります。リストでは、インターフェイス名または **All Interfaces** を選択できます。Action タイプの場合、ドロップダウン リストには Permit と Deny が表示されます。Rule Query タイプの場合、ドロップダウン リストにはすべての定義済みルール クエリーが表示されます。Source タイプと Destination タイプの場合には、IP アドレスを指定できます。アドレスを手動で入力するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開き、アドレスを参照します。Service タイプには、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを指定できます。IP アドレスを 1 つ手動で入力するか、**...** 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します。
  - Filter：フィルタリングを実行します。
  - Clear：Filter フィールドをクリアします。
  - Rule Query：名前付きルール クエリーを管理できる Rule Queries ダイアログボックスが開きます。
- Show Rule Flow Diagram：ルール テーブルの下に Rule Flow Diagram 領域を表示します。この図では、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（Authenticate または Do Not Authenticate など）を示しています。

次の説明では、AAA Rules テーブルのカラムをまとめています。これらのカラムの内容は、テーブル セルをダブルクリックすると編集できます。カラム ヘッダーをダブルクリックすると、選択したカラムをソート キーとして、テーブルの内容がアルファベットの昇順で並べ替えられます。ルールを右クリックすると、上のボタンで示されるオプションすべてとともに、Insert 項目と Insert After 項目が表示されます。これらの項目により、選択したルールの前（Insert）または後（Insert After）に新しいルールを挿入します。

- **No**：ルールの評価順序を示します。
- **Enabled**：ルールがイネーブルになっているか、またはディセーブルになっているかを示します。
- **Action**：AAA ルールのタイプを指定します。
- **Source**：Destination カラムに一覧表示された IP アドレスにトラフィックが送信されたとき、AAA の対象となる IP アドレスを一覧表示します。
- **Destination**：Source カラムに一覧表示された IP アドレスからトラフィックが送信されたとき、AAA の対象となる IP アドレスを一覧表示します。
- **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：Authenticate、Do Not Authenticate、Authorize、Do Not Authorize など、ルールで指定されたアクションを表示します。
- **Server Group**：AAA Server Group タグを指定します。AAA サーバ グループの設定は、Properties > AAA Setup > AAA Server Groups で行います。新しい AAA ルールを作成するには、サーバ グループがあり、その中に 1 つ以上のサーバが存在する必要があります。
- **Time**：このルールで有効な時間範囲の名前を指定します。
- **Description**：ルールの追加時に入力した説明です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 アクセス認証の設定

ここでは、次の項目について説明します。

認証の概要

FWSM では、AAA サーバを利用してネットワーク アクセス認証を設定します。ここでは、次の項目について説明します。

ワンタイム認証

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、「Timeouts」を参照）。たとえば、Telnet および FTP を認証するように FWSM が設定されていて、ユーザが正常に Telnet 認証を受けた場合、認証セッションが継続している限り、ユーザは FTP 認証を受ける必要はありません。

HTTP 認証または HTTPS 認証では、タイムアウトが非常に短く設定されている場合でも、一度認証されたユーザの再認証が必要になることはありません。これは、ブラウザが「Basic=Uuhjksdkfhk==」文字列をキャッシュして、後続の接続のすべてに使用するからです。この文字列がクリアされるのは、ユーザが Web ブラウザの すべてのインスタンス終了してブラウザを再起動したときのみです。キャッシュをフラッシュしても意味がありません。

認証チャレンジの受信が必要なアプリケーション

どのプロトコルやサービスへのネットワーク アクセスについても、認証を必要とするように FWSM を設定できますが、ユーザが直接認証を受けられるのは HTTP、HTTPS、Telnet、または FTP を使用する場合のみです。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、FWSM は認証が必要な他のトラフィックを許可しません。

FWSM が AAA 用にサポートしている認証ポートは、次のように固定されています。

- ポート 21（FTP の場合）
- ポート 23（Telnet の場合）
- ポート 80（HTTP の場合）
- ポート 443（HTTPS の場合）

Telnet および FTP の場合、FWSM は認証プロンプトを生成します。正常に認証されると、FWSM 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。

HTTP の場合、ブラウザが提供する基本 HTTP 認証を使用してログインします。HTTPS の場合、FWSM は専用のログイン ウィンドウを生成します。

（注） HTTP クライアント認証（「Advanced AAA Configuration」を参照）を使用せずに HTTP 認証を使用する場合、ユーザ名とパスワードはクリア テキストで宛先 Web サーバに送信され、AAA サーバには送信されません。たとえば、内部ユーザが外部の Web サーバにアクセスするときに認証すると、有効なユーザ名とパスワードが外部から判別可能になります。HTTP 認証をイネーブルにする場合は、必ずセキュアな HTTP クライアント認証を使用することをお勧めします。

FTP の場合、FWSM 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、FWSM 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 認証でスタティック PAT が設定されている場合、FWSM は実際のポートをチェックします。FWSM 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 はポート 80（www）に変換され、すべての関連アクセスリストはトラフィックを許可するものとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask
255.255.255.255
```

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、FWSM はそのトラフィックを代行受信し、HTTP 認証を実行します。FWSM 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。

次の例のように、ローカル ポートが 80 ではないとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask
255.255.255.255
```

この場合、認証ページはユーザに表示されません。その代わりに、FWSM は、要求したサービスを使用するには認証を受ける必要があることを示すエラーメッセージを Web ブラウザに送信します。

FWSM での直接認証

FWSM で HTTP（S）、Telnet、または FTP は許可しないが、他のトラフィック タイプの認証する場合、仮想 Telnet、仮想 SSH、仮想 HTTP を設定できます。仮想 Telnet、SSH、HTTP では、ユーザが Telnet、SSH、または HTTP を使用して FWSM に設定された所定の IP アドレスに接続すると、FWSM はプロンプトを表示します。詳細については、P.11-13 の「Virtual Access」を参照してください。

認証ルールの追加および編集

このダイアログボックスでは、認証ルールを追加または編集できます。

フィールド

Interface and Action：インターフェイス、アクション、および AAA サーバ グループを選択します。

- Interface：このルールを適用するインターフェイスを選択します。
- Action：**Authenticate** または **Do not Authenticate** を選択します。
- AAA Server Group：AAA サーバ グループまたはローカル データベースを選択します。Properties > AAA Setup > AAA Server Groups でサーバ グループを追加する必要があります。
- **Add Server/User**：サーバを選択した AAA サーバ グループに追加するか、ユーザをローカル データベースに追加するには、このボタンをクリックします。

Source：認証するトラフィックの送信元アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  — IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。

  — Netmask：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。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  — Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  — 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。

Destination：認証するトラフィックの宛先アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  — IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。

  — Netmask：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。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  — Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  — 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。

Protocol and Service：認証するトラフィックのポートまたはプロトコルを指定します。

- Protocol：tcp、udp、ip、icmp、またはその他のいずれかのトラフィックのプロトコルを選択します。

  tcp または **udp** を選択した場合、次のフィールドが表示されます。

  — Source Port：認証するトラフィックの送信元ポートを設定します。

  Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、... ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

- Destination Port：認証するトラフィックの宛先ポートを設定します。

  Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

  Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、... ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

icmp を選択した場合、次のフィールドが表示されます。

- ICMP Type：ICMP タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
- ICMP Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、... ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

other を選択した場合、次のフィールドが表示されます。

- Protocol：IP プロトコル タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
- Protocol Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、... ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

Rule Flow Diagram：このルールの Rule Flow Diagram を表示します。この図では、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（Authenticate または Do Not Authenticate など）を示しています。

Options：このルールのオプションを設定します。

- **Time Range**：ドロップダウン リストから既存の時間範囲の名前を選択します。時間範囲では、指定した時間だけルールがイネーブルになります。時間範囲は「時間範囲の設定」で作成します。
- **Description**：このルールの説明を入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 アクセス認可の設定

ユーザが所定の接続の認証を受けると、FWSM は認可を使用して、そのユーザのトラフィックをさらに制御できます。

ここでは、次の項目について説明します。

TACACS+ 認可の設定

次のダイアログボックスでは、認証ルールを追加または編集できます。

TACACS+ でネットワーク アクセス認可を実行するように FWSM を設定できます。

認証ルールと認可ルールは互いに依存しませんが、認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。認可が成功するためには、ユーザは最初に FWSM で認証を受ける必要があります。所定の IP アドレスのユーザは、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ればよいため、認証セッションが期限切れになっていなければ、トラフィックが認証文で一致した場合でも、認可が発生することがあります。

ユーザの認証が完了すると、FWSM は、一致するトラフィックの認可ルールをチェックします。トラフィックが認可ルールに一致した場合、FWSM はユーザ名を TACACS+ サーバに送信します。TACACS+ サーバは FWSM 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。FWSM は、その応答内の認可ルールを実施します。

ユーザに対するネットワーク アクセス認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。

フィールド

Interface and Action：インターフェイス、アクション、および AAA サーバ グループを選択します。

- Interface：このルールを適用するインターフェイスを選択します。
- Action：**Authorize** または **Do not Authorize** を選択します。
- AAA Server Group：AAA サーバ グループまたはローカル データベースを選択します。Properties > AAA Setup > AAA Server Groups でサーバ グループを追加する必要があります。
- **Add Server/User**：サーバを選択した AAA サーバ グループに追加するか、ユーザをローカル データベースに追加するには、このボタンをクリックします。

Source：認可するトラフィックの送信元アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。
  - Netmask：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。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - 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。

Destination：認可するトラフィックの宛先アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。
  - Netmask：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。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - 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。

Protocol and Service：認可するトラフィックのポートまたはプロトコルを指定します。

- Protocol：tcp、udp、ip、icmp、またはその他のいずれかのトラフィックのプロトコルを選択します。

  tcp または **udp** を選択した場合、次のフィールドが表示されます。

  - Source Port：認可するトラフィックの送信元ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

    Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。
  - Destination Port：認可するトラフィックの宛先ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

    Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

  icmp を選択した場合、次のフィールドが表示されます。

  - ICMP Type：ICMP タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
  - ICMP Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

  other を選択した場合、次のフィールドが表示されます。

  - Protocol：IP プロトコル タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
  - Protocol Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

Rule Flow Diagram：このルールの Rule Flow Diagram を表示します。この図では、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（Authorize または Do Not Authorize など）を示しています。

Options：このルールのオプションを設定します。

- **Time Range**：ドロップダウン リストから既存の時間範囲の名前を選択します。時間範囲では、指定した時間だけルールがイネーブルになります。時間範囲は「時間範囲の設定」で作成します。
- **Description**：このルールの説明を入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 認可の設定

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 パケットでユーザ認可を返します。認証の設定の詳細については、P.18-5 の「ネットワーク アクセス認証の設定」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 FWSM を設定すると、RADIUS 認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、FWSM 上の RADIUS 認可の設定については取り上げません。ここでは、FWSM 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 FWSM にダウンロードするように RADIUS サーバを設定できます。または、認証時にアクセスリスト名をダウンロードするようにも設定できます。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認可されます。

（注） アクセス ルールを作成した場合、Per User Override オプションは、ユーザ固有のアクセスリストによる認可に対して次のような影響を与えますので注意してください。

- Per User Override オプションを使用しない場合、ユーザ セッションのトラフィックが、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。
- Per User Override 機能を使用した場合、ユーザ固有のアクセスリストによって許可される内容が決まります。

詳細については、P.17-15 の「Advanced Access Rule Configuration」を参照してください。

ここでは、次の項目について説明します。

ユーザごとの ACL をダウンロードするための RADIUS サーバの設定

この項では、Cisco Secure 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に関する Cisco Secure ACS の設定（P.18-12）
- 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.18-13）

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。

アクセスリスト定義は、次のプレフィックスがない点を除いて拡張 **access-list** コマンドに類似する、1 つまたは複数の FWSM コマンドで構成されます。

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 のマニュアルを参照してください。

FWSM 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 が生成した一意のバージョン ID です。

FWSM 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-xxx-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.254
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.254
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.254
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.253
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.253
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.253
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.252
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.252
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.252
access-list #ACSACL#-ip-xxx-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（VSA 番号 1）で FWSM 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 IOS RADIUS VSA は、RADIUS ベンダー ID 9 で識別されます。

cisco-av-pair VSA で、**access-list extended** コマンドと類似する 1 つまたは複数の ACE を設定します。ただし、次のコマンド プレフィックスを置き換える必要があります。

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、FWSM 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 アトリビュートで送信されるアクセスリストをユーザごとに一意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。

FWSM 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形式になります。

AAA-user-*username*

username 引数は、認証を受けるユーザの名前です。

FWSM 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 FWSM が作成したハッシュ値で、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。

ユーザごとの ACL 名をダウンロードするための RADIUS サーバの設定

ユーザ認証時に、FWSM で作成済みのアクセスリストの名前を RADIUS サーバからダウンロードするには、IETF RADIUS filter-id アトリビュート（アトリビュート番号 11）を次のように設定します。

filter-id=*acl_name*

（注） Cisco Secure ACS では、filter-id アトリビュートの値は、HTML インターフェイスのボックスで、**filter-id=** を省略し、*acl_name* だけを入力して指定します。

filter-id アトリビュートの値をユーザごとに一意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。

ネットワーク アクセスのアカウンティングの設定

ここでは、次の項目について説明します。

アカウンティング ルールの追加および編集

FWSM は、FWSM を通過する任意の TCP トラフィックまたは UDP トラフィックに関する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。そのトラフィックが認証されていない場合、AAA サーバは IP アドレスで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、そのセッションで FWSM を経由したバイト数、使用されたサービス、セッションの継続時間が含まれます。

フィールド

Interface and Action：インターフェイス、アクション、および AAA サーバ グループを選択します。

- Interface：このルールを適用するインターフェイスを選択します。
- Action：**Account** または **Do not Account** を選択します。
- AAA Server Group：AAA サーバ グループまたはローカル データベースを選択します。Properties > AAA Setup > AAA Server Groups でサーバ グループを追加する必要があります。
- **Add Server/User**：サーバを選択した AAA サーバ グループに追加するか、ユーザをローカル データベースに追加するには、このボタンをクリックします。

Source：認証するトラフィックの送信元アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。
  - Netmask：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。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - 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。

Destination：アカウンティングするトラフィックの宛先アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択すると、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから IP address を選択します。
  - Netmask：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。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

Interface IP を選択した場合、次のフィールドが表示されます。

— 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。

Protocol and Service：アカウンティングするトラフィックのポートまたはプロトコルを指定します。

- Protocol：tcp または udp の、いずれかのトラフィックのプロトコルを選択します。
  — Source Port：アカウンティングするトラフィックの送信元ポートを設定します。

  Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

  Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

  — Destination Port：アカウンティングするトラフィックの宛先ポートを設定します。

  Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。

  Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

Rule Flow Diagram：このルールの Rule Flow Diagram を表示します。この図では、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（Account または Do Not Account など）を示しています。

Options：このルールのオプションを設定します。

- **Time Range**：ドロップダウン リストから既存の時間範囲の名前を選択します。時間範囲では、指定した時間だけルールがイネーブルになります。時間範囲は「時間範囲の設定」で作成します。
- **Description**：このルールの説明を入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 アドレスによるトラフィックの認証と認可の免除

ここでは、次の項目について説明します。

MAC 免除ルールの追加および編集

FWSM は、特定の MAC アドレスからのトラフィックの認証および認可を免除できます。

たとえば、FWSM 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ても、特定のサーバからの未認証の TCP 接続を許可する場合に、MAC 免除ルールを使用すると、このルールが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認可が免除されます。

ベスト マッチ シナリオと異なり、パケットは照合する最初のエントリを使用するので、エントリの順番が重要になります。許可エントリがあり、そのエントリにより許可されたアドレスを拒否する場合は、許可エントリの前に拒否エントリを入力してください。

フィールド

- Action：**MAC Exempt** または **No MAC Exempt** を選択します。MAC Exempt オプションでは、認証または認可する必要なく MAC アドレスからのトラフィックを許可します。No MAC Exempt オプションでは、認証または認可を免除しない MAC アドレスを指定します。ffff.ffff.0000 などの MAC アドレス マスクを使用して MAC アドレスの範囲を許可する場合、拒否エントリを追加する必要があります。また、その範囲で認証および認可されるように MAC アドレスを強制します。
- MAC Address：12 桁の 16 進数の形式（nnnn.nnnn.nnnn）で送信元の MAC アドレスを指定します。
- MAC Mask：照合に使用される MAC アドレスの一部を指定します。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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 AAA Configuration

セキュアな HTTP 機能および Proxy Limit 機能をイネーブルまたはディセーブルにします。このダイアログボックスは、Configuration > Features > Security Policy ペインで Advanced をクリックすると表示されます。

フィールド

- **Secure HTTP**：Secure HTTP（HTTPS）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。
  - **Enable Secure HTTP**：ブラウザなどの HTTP クライアントがセキュアな HTTP（HTTPS）を使用する場合、FWSM で認証が必要です。このオプションがイネーブルでなければ FWSM は HTTP を使用します。パスワードはクリア テキストになります。

（注） Enable Secure HTTP のチェックボックスをオンにしても、AAA ルールに HTTP 認証が設定されていない場合、このオプションは機能しません。

- **Proxy Limit**：Proxy Limit パラメータを指定します。
  - **Enable Proxy Limit**：ユーザごとに許可される同時プロキシ接続の数を制限します。最大接続数は 128 です。この機能をイネーブルにしない場合、制限なしになります。
  - **Proxy Limit**：許可されるプロキシ同時接続数を指定します。指定できる値は 1 ～ 128、デフォルトは 16 です。
- Authentication Challenge：FWSM でユーザにユーザ名とパスワードを求めて、認証確認を行うかどうかを設定できます。新しいセッションのトラフィックでは認証を行うという AAA ルールが設定され、トラフィックのプロトコルが FTP または、Telnet、HTTP、HTTPS の場合、FWSM でプロンプトがデフォルトでユーザに表示されます。場合によって、上記のプロトコルのどれかで認証確認を不要にすることもあり得ます。

  あるプロトコルの認証確認をディセーブルにした場合は、そのプロトコルのトラフィックが認証済みのセッションに属していない限り許可されません。この認証は、認証確認がイネーブル状態のプロトコルを使用したトラフィックで実行できます。たとえば、FTP の認証確認をディセーブルにすると、トラフィックが認証ルールの対象になっている場合 FTP で開始したセッションは FWSM で拒否されます。認証確認がイネーブルになっているプロトコル（HTTP など）でセッションを確立すると、FTP のトラフィックは許可されます。
  - FTP：チェックボックスをオフにすると、FTP の認証確認がディセーブルになります。
  - HTTP：チェックボックスをオフにすると、HTTP の認証確認がディセーブルになります。
  - HTTPS：チェックボックスをオフにすると、HTTPS の認証確認がディセーブルになります。
  - Telnet：チェックボックスをオフにすると、Telnet の認証確認がディセーブルになります。
- Expired Connections：ユーザ認証でタイムアウトになったとき、または **clear uauth** コマンドを使用して認証セッションをクリアした場合、どのような IP アドレスであってもアクティブな接続をすぐに強制終了するには、このテーブルに IP アドレスを追加します。この機能を使用しない場合、ユーザの認証セッションが失効してもアクティブ接続は終了しません。接続の終了理由がこのオプションによる場合は、システム ログ メッセージ 109036 が表示されます。
  - Interface：ソース IP アドレスに接続するインターフェイス名です。
  - IP Address：ソース IP アドレスです。
  - Mask：サブネット マスクです。
  - Add：接続終了対象になる IP アドレスを追加します。
  - Edit：IP アドレスを編集します。
  - Delete：IP アドレスを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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

クリア接続の追加および編集

ユーザ認証でタイムアウトになったとき、または **clear uauth** コマンドを使用して認証セッションをクリアした場合、どのような IP アドレスであってもアクティブな接続をすぐに強制終了するには、このテーブルに IP アドレスを追加します。この機能を使用しない場合、ユーザの認証セッションが失効してもアクティブ接続は終了しません。接続の終了理由がこのオプションによる場合は、システム ログ メッセージ 109036 が表示されます。

フィールド

- Interface Name：ソース IP アドレスに接続するインターフェイス名を設定します。
- IP Address：ソース IP アドレスを設定します。
- Mask：サブネット マスクを設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 19

トラフィックのフィルタリング

ここでは、次の項目について説明します。

Filter Rules

Filter Rules ウィンドウ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、**Features** > **Configuration** > **Properties** > **URL Filtering** 画面を使用します。詳細については、「URL Filtering」を参照してください。

利点

Filter Rules ウィンドウでは、現在 FWSM 上に設定されているフィルタ ルールについての情報が提供されます。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 FWSM 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 ルールのタイプが表示されます。ルールの種類をクリックすると、指定したフィルタ ルールのタイプの **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配置します。
- 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。
  - Filter：ドロップダウン メニューを使用して、送信元、宛先、ソース、アクション、またはルール クエリーで検索できます。
  - ....：フィルタのソースを選択し、Select Source ダイアログボックスが表示されます。
  - Filter：フィルタを入力します。
  - Clear：フィルタ ルールをクリアします。
  - Rule Query：ルールを検索するクエリーを作成します。
- Rule Diagram：Rule Diagram の表示を切り替えます。
- 選択しているフィルタ ルールのソースを選ぶには、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します。All、IP Address Objects、IP Names、または Network Object の各グループから選択します。
  - 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します。All、IP Address Objects、IP Names、または Network Object の各グループから選択します。
  - 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、**Configuration** > **Properties** > **URL Filtering** 画面を使用します。詳細については、「URL Filtering」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 アクションに関して、次に挙げるリストを提供します。
  - Filter ActiveX
  - Do not filter ActiveX
  - Filter Java
  - Do not filter Java
  - Filter HTTP (URL)
  - Do not filter HTTP (URL)
  - Filter HTTPS
  - Do not filter HTTPS
  - Filter FTP

- Do not filter FTP

Rule Flow Diagram and the Filtering Option グループ ボックスは、選択するフィルタリング アクションによって変わります。

- Source Host/Network
  - IP Address：フィルタリング アクションの適用先であるトラフィックを指定する IP アドレスを使用します。
  - Name：フィルタリング　アクションの適用先であるトラフィックを指定する名前を使用します。
  - Name：Name ボタンが選択されているとき、フィルタリング アクションの適用先であるトラフィックの指定に使用される名前を指定します。
  - Interface：フィルタリング アクションの適用先であるインターフェイスを指定します。
  - IP Address：IP アドレスの選択時にフィルタリング アクションの適用先であるトラフィックの指定に使用される IP アドレスを指定します。
  - Mask：IP Address が選択されているとき、フィルタリング アクションの適用先であるトラフィックの指定に使用されるサブネット マスクを指定します。
- Destination Host/Network
  - IP Address：フィルタリング アクションの適用先であるトラフィックを指定します。
  - Name：フィルタリング アクションの適用先であるトラフィックを示します。
  - Name：Name　が選択されているとき、フィルタリング　アクションの適用先であるトラフィックの指定に使用される名前を指定します。
  - Interface：フィルタリング アクションの適用先であるインターフェイスを指定します。
  - IP Address：IP アドレスの選択時にフィルタリング アクションの適用先であるトラフィックの指定に使用される IP アドレスを指定します。
  - Mask：IP Address が選択されているとき、フィルタリング アクションの適用先であるトラフィックの指定に使用されるサブネット マスクを指定します。
- Browse：Select host/network 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、事前に設定されたリストからホストまたはネットワークを選択できます。
- Rule Flow Diagram：FWSM を介して転送されるトラフィックに特定のフィルタリング アクションが適用される仕組みをグラフィカルな表現で示します。
- HTTP Filtering Option：このグループ ボックスは、ドロップダウン リストで Filter HTTP オプションを選択したときにのみ表示されます。
  - Filter HTTP on port(s)：FWSM がフィルタリング アクションの適用先であるトラフィックをリッスンする TCP/UDP ポートを指定します。
  - Block connections to proxy server：プロキシ サーバを介した HTTP 要求を禁止します。
  - 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、FWSM 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になっている場合、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。
  - Truncate CGI requests by removing the CGI parameters：FWSM 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。
- Long URL：このグループ ボックスは、ドロップダウン リストで Filter HTTP オプションを選択したときにのみ表示されます。

  FWSM では、最大 1159 バイトの URL をフィルタリングできます。Websense フィルタリング サーバを使用する場合、フィルタリング可能な URL は最大 4 KB です。長い URL のフィルタリングをイネーブルにするには、**Configuration** > **Properties** > **URL Filtering** > **Advanced** 画面を使用します。詳細については、「URL Filtering」を参照してください。
  - Drop：FWSM は最大値よりも長い URL をドロップし、ユーザはターゲットのインターネット Web サイトに接続できません。

- Truncate：FWSM は URL を許可されている最大の長さに短縮し、短縮後の URL を分析のためにフィルタリング サーバに転送します。
- Block：許可されている最大値よりも長い URL にユーザが接続できないようにします。

- HTTPS Filtering Option：このグループ ボックスは、ドロップダウン リストで Filter HTTPS オプションを選択したときにのみ表示されます。
  - Filter HTTPS on port(s)：FWSM がフィルタリング アクションの適用先であるトラフィックをリッスンする TCP/UDP ポートを指定します。
  - 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、FWSM 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になっている場合、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 Filtering Option：このグループ ボックスは、ドロップダウン リストで Filter FTP オプションを選択したときにのみ表示されます。
  - Filter FTP on port(s)：FWSM がフィルタリング アクションの適用先であるトラフィックをリッスンする TCP/UDP ポートを指定します。
  - 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、FWSM 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になっている場合、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 outbound traffic 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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
- URL Filtering

URL Filtering

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。次のインターネット フィルタリング製品のいずれかを実行する別個のサーバを使用することにより、コンフィギュレーションを簡素化し、FWSM 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、FWSM では、Sentian での HTTP のフィルタリングのみをサポートしています。）

FWSM のパフォーマンスへの影響は、外部サーバを使用した方が小さくなりますが、フィルタリング サーバが FWSM から離れている場合は、Web サイトまたは FTP サーバへのアクセス時間が長くなることもあります。

フィルタリングがイネーブルで、コンテンツを求める要求が FWSM を経由して送信された場合、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 サーバがその接続を許可した場合、FWSM はコンテンツ サーバからの応答を発信元クライアントに転送します。フィルタリング サーバがその接続を拒否した場合、FWSM は応答をドロップし、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。

FWSM 上でユーザ認証がイネーブルの場合、FWSM 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。

一般的な手順

次に、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手順をまとめます。

ステップ 1　フィルタリング サーバを指定します。

ステップ 2　（オプション）コンテンツ サーバからの応答をバッファに格納します。

ステップ 3　（オプション）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。

ステップ 4　フィルタリング ルールを設定します。「**Filter Rules**」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

コンテキストごとに最大 4 つのフィルタリング サーバを指定できます。シングルモードでは、最大 16 個のサーバを指定できます。FWSM 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** 領域
  - **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。デフォルトは 4005 です。
  - **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。
  - **Insert**：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。
  - **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。
- **Apply**：実行中のコンフィギュレーションに変更を適用します。
- **Reset**：まだ適用されていない変更を削除します。
- **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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Add/Edit Parameters for Websense URL Filtering

- **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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Parameters for Secure Computing SmartFilter URL Filtering

- **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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 URL Filtering

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 FWSM 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。これによって、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、FWSM 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、すべてのユーザが Websense サーバ上で同一の URL フィルタリング ポリシーを共有してい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、FWSM 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。これによって、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。これによって、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。

Long URL Support 領域

デフォルトでは、FWSM 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、最大許容長を増やすことができます。

- **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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

サービス ルール

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 ルールでは、特定の種類のアプリケーション検査を、FWSM が受信するさまざまなタイプのトラフィックに適用する方法を定義します。定義により、特定のルールを 1 つのインターフェイスに、またはすべてのインターフェイスに対してグローバルに適用します。

ここでは、次の項目について説明します。

サービス ルール設定の一般的な手順

ASDM では、サービス ルール設定の順序が CLI とは少し異なります。ASDM にサービス ルールを設定するには、一般的に次の 3 つの手順に従って行います。

1. ポリシーを適用するインターフェイスを決定し、ポリシー名を指定します。
2. トラフィック フローを定義する基準を特定します。
3. 指定したトラフィック フローに適用するサービスを特定します。

インターフェイスごとに適用できるポリシーは 1 つだけですが、これに加えてグローバル ポリシーがすべてのインターフェイスに対して適用されます。複数のエントリ（ACE）を持つ ACL を使用する場合を除き、各ポリシーには、トラフィック選択に使用する基準が 1 つ含まれています。

サービス 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　**Security Policy** ペインで **Service Policy Rules** をクリックし、次に **Add** をクリックします。

Add Service Policy Rule Wizard - Service Policy 画面が表示されます。

ステップ 2　サービス ポリシーを作成します。

特定のインターフェイスのセキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Interface** オプション ボタンをクリックし、選択リストから使用可能なインターフェイスを選択します。

すべてのインターフェイスに適用するグローバル セキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Global** オプション ボタンをクリックします。

ステップ 3　**Policy Name** ボックスに最大 40 文字の名前を入力し、**Next** をクリックします。

Add Service Policy Rule Wizard - Traffic Classification Criteria 画面が表示されます。

ステップ 4　ポリシー ルールを適用するトラフィックを選択する基準を選択します。

Traffic match criteria グループ ボックスにある個々の基準の詳細については、**Add/Edit Security Policy Rules** ウィザードの **Traffic Criteria** 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。

トラフィック フローの定義に複数の基準を使用するには、**Source and destination IP address (uses ACL)** ボタンをクリックします。

ステップ 5　トラフィックに照合する基準を定義したら、**Next** をクリックします。

Add Service Policy Rule Wizard - Rule Actions 画面が表示されます。

ステップ 6　次のタブのいずれかを使用して、指定したトラフィック フローに適用するルール アクションを 1 つ以上定義します。

- **Protocol Inspection**
- **Connection Settings**

ステップ 7　**Finish** をクリックします。

Security Policy ペインの **Service Policy Rules** テーブルに、新しいサービス ポリシーが表示されます。

Service Policy Rules

一部のアプリケーションは、FWSM による特殊な処理を必要としており、この処理のための固有のアプリケーション検査エンジンが用意されています。特別なアプリケーション検査エンジンを必要とするのは、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か、またはダイナミックに割り当てられたポートでセカンダリ チャネルを開くアプリケーションです。アプリケーション検査は、多くのプロトコルではデフォルトでイネーブルになっていますが、それ以外のプロトコルではディセーブルになっています。多くの場合、アプリケーション検査でトラフィックをリッスンするポートを変更することができます。

アプリケーション検査エンジンは、埋め込まれたアドレッシング情報の場所を特定する NAT と連動します。これによって NAT では、それらの埋め込まれたアドレスを変換したり、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。

サービス ポリシー ルールでは、特定の種類のアプリケーション検査を、FWSM が受信するさまざまなタイプのトラフィックに適用する方法を定義します。定義により、特定のルールを 1 つのインターフェイスに、またはすべてのインターフェイスに対してグローバルに適用します。

トラフィック照合基準を使用して、アプリケーション検査を適用するトラフィックのセットを定義します。たとえば、ポートの値が 23 の TCP トラフィックは Telnet トラフィック クラスに分類できます。トラフィック クラスを使用して、変更が許可されているプロトコルの場合に、アプリケーション検査で使用するデフォルト ポートを変更できます。

1 つのインターフェイスに複数のトラフィック照合基準を割り当てることができますが、パケットは特定のサービス ポリシー ルール内の最初の基準にのみ一致します。

（注）　**Service Policy** > **Access Rules** ペインのテーブルにあるアクセスリスト ベースのルールを検索するには、メニューバーの Search オプションを使用します。検索しているテキストがアクセスリストに含まれていれば、このオプションを使用してルールを検索できます。

フィールド

- **Add**：新しいサービス ポリシー 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**：サービス ポリシー ルールを編集します。
- **Delete**：サービス ポリシー 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、重複するルールがあると順序によって評価が異なります。
- 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、Paste ボタンを使用して、同じパラメータを持つ新しいルールを開始できます。

- Paste：コピーまたは切り取られたルールのパラメータがあらかじめ入力された状態で、Add/Edit Rule ダイアログボックスを開きます。ダイアログボックスで何らかの修正を行い、ルールをテーブルに追加することができます。Paste ボタンをクリックすると、選択したルールの上に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、選択したルールの後にルールが追加されます。
- Find：表示をフィルタリングして、一致するルールのみを表示します。**Find** をクリックすると、Filter フィールドが開きます。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。
  - Filter：フィルタリングする基準を、Interface、Source、Destination、Service、または Rule Query のいずれかから選択します。ルール クエリーは複数の基準の集合であり、保存して繰り返し使用できます。
  - Filter：Interface タイプの場合は、このフィールドがドロップダウン リストになります。インターフェイス名または **All Interfaces** を選択できます。Rule Query タイプの場合、ドロップダウン リストにはすべての定義済みルール クエリーが表示されます。Source タイプと Destination タイプの場合には、IP アドレスを指定できます。アドレスを手動で入力するか、または **...** ボタンをクリックして Browse Address ダイアログボックスを開き、アドレスを参照します。Service タイプには、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを指定できます。プロトコル タイプを手動で入力するか、または **...** ボタンをクリックして Browse Service Groups ダイアログボックスを開き、プロトコル タイプを参照します。
  - Filter：フィルタリングを実行します。
  - Clear：Filter フィールドをクリアします。
  - Rule Query：Rule Queries ダイアログボックスを開き、名前付きルール クエリーを管理できます。
- Show Rule Flow Diagram：ルール テーブルの下に Rule Flow Diagram 領域を表示します。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を示すパラメータがあらかじめ入力された状態で Packet Tracer ツールが開きます。

次に、Service Policy Rules テーブルのカラムの概要を説明します。これらのカラムの内容は、テーブル セルをダブルクリックすると編集できます。カラム ヘッダーをダブルクリックすると、選択したカラムをソート キーとして、テーブルの内容がアルファベットの昇順で並べ替えられます。ルールを右クリックすると、上のボタンで示されるオプションすべてとともに、Insert 項目と Insert After 項目が表示されます。これらの項目により、選択したルールの前（Insert）または後（Insert After）に新しいルールを挿入します。

- **Name**：ルールの名前を示します。
- **No**：ルールの評価順序を示します。
- **Enabled**：ルールがイネーブルになっているか、またはディセーブルになっているかを示します。
- **Match**：トラフィックを含める（一致する）か除外する（一致しない）ために基準を使用するかどうかを示します。
- **Source**：Destination カラムのリストにある IP アドレス宛てにトラフィックが送信されるときのサービス ポリシーに従う IP アドレスを一覧表示します。
- **Destination**：Source カラムのリストにある IP アドレスからトラフィックが送信されるときのサービス ポリシーに従う IP アドレスを一覧表示します。
- **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。
- **Time**：ルールを適用する時間範囲が表示されます。
- Rule Actions：ルールで適用されるアクションを表示します。
- **Description**：ルールの追加時に入力した説明です。

モード

次の表に、この機能を使用できるモードを示します。

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

Service Policy

Service Policy ダイアログボックスでは、新しいサービス ポリシー ルールを追加したり、そのルールを特定のインターフェイスに適用したり、そのルールをすべてのインターフェイスに対してグローバルに適用したりすることができます。

フィールド

- Create a Service Policy and Apply to
  - Interface：ルールを特定のインターフェイスに適用します。アクセスリストを使用し、送信元または宛先 IP アドレスに基づいてトラフィックを照合する場合は、このフィールドを選択する必要があります。
  - Interface：ルールを適用するインターフェイスを指定します。
  - Policy Name：インターフェイス サービス ポリシーの名前を指定します。
  - Description：ポリシーの説明をテキストで入力します。
  - Global - applies to all interfaces：ルールをすべてのインターフェイスに適用します。アクセスリストを使用し、送信元または宛先 IP アドレスに基づいてトラフィックを照合する場合は、このフィールドを一緒に選択できません。
  - Policy Name：グローバル サービス ポリシーの名前を指定します。グローバル サービス ポリシーは、1 つしか適用できません。また、名前を変更することはできません。
  - Description：ポリシーの説明をテキストで入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Service Policy

Edit Service Policy ダイアログボックスでは、選択したサービス ポリシーの説明を変更できます。

フィールド

- Description：サービス ポリシーの説明をテキストで入力します。

モード

次の表に、この機能を使用できるモードを示します。

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

Traffic Classification Criteria

Edit Service Policy Rule 画面の Traffic Classification タブでは、セキュリティ ポリシー ルールを適用するトラフィックの照合の際に使用する基準を指定できます。

フィールド

- Name：トラフィック クラスの名前を特定します。
- Description (optional)：新しいトラフィック クラスの説明をテキストで入力します。
- Traffic match criteria：
  - Default Inspection Traffic：デフォルトの検査トラフィック ポリシーで指定された基準を使用します。
  - Source and Destination IP Address (uses ACL)：ACL を使用し、送信元と宛先 IP アドレスに基づいてトラフィックを照合します。このフィールドは、インターフェイス サービス ポリシーを使用して特定のインターフェイスにルールを適用する場合にのみ選択できます。
  - TCP or UDP Destination Port：TCP または UDP 宛先ポートに基づいてトラフィックを照合します。
  - RTP Range：RTP ポートの範囲に基づいてトラフィックを照合します。
  - IP DiffServ CodePoints (DSCP)：QoS の Differentiated Services モデルに基づいてトラフィックを照合します。
  - IP Precedence：QoS の IP precedence モデルに基づいてトラフィックを照合します。
  - Any traffic：トラフィック タイプに関係なくすべてのトラフィックを照合します。
- Add rule to existing traffic class：リストで選択した既存のトラフィック クラスにルールを追加します。
- Use class-default as the traffic class：トラフィックが他のトラフィック クラスのどれとも一致しない場合は、class-default トラフィック クラスを使用するように指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Inspections

Default Inspections ダイアログボックスには、Traffic Classification Criteria ダイアログボックスで Default Inspection Traffic 基準を選択する場合に使用される、デフォルトのポート割り当てがリストで表示されます。

- Service：アプリケーション検査エンジンのタイプをリストで表示します。
- Protocol：トランスポート プロトコルとして、TCP と UDP のどちらをアプリケーション検査で使用するかを特定します。
- Port：デフォルトの検査トラフィック基準で使用されるポート番号を特定します。

デフォルトの検査トラフィック基準の使用

fixup コマンドは、アプリケーション検査に簡易でグローバルなポリシーを提供しました。モジュラ ポリシー フレームワークには、さらにきめ細かなトラフィックの検査方法が用意されています。モジュラ ポリシー フレームワークでは、特定のアプリケーション検査で使用するトラフィックを選択することができ、これによって、FWSM のパフォーマンスを向上させることができます。パフォーマンスが向上する理由は、アプリケーション検査エンジンが限定された量のトラフィックのみを検査するからです。

デフォルト ポートでのアプリケーション検査のイネーブル化を簡単にするため、デフォルトの検査トラフィック基準を使用します。デフォルトの検査トラフィック基準を指定すると、FWSM は、ウェルノウン ポートのアプリケーション検査で使用するトラフィックをプロトコルごとに選択します。表 20-1 に、プロトコルごとのデフォルト ポートの割り当てを示します。

表 20-1　デフォルト ポートの割り当て

プロトコル名	プロトコル	セキュア ポート	宛先ポート
ctiqbe	tcp	該当なし	2748
dcerpc	tcp	該当なし	135
dns	udp	53	53
esmtp/smtp	tcp	該当なし	25
ftp	tcp	該当なし	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	該当なし	1720
h323 ras	udp	該当なし	1718-1719
http	tcp	該当なし	80
icmp	icmp	該当なし	該当なし
ils	tcp	該当なし	389
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	該当なし
pptp	tcp	1723	1723
rsh	tcp	該当なし	514
rtsp	tcp	該当なし	554
sip	tcp、udp	該当なし	5060
skinny	tcp	該当なし	2000
sqlnet	tcp	該当なし	1521
sunrpc	udp	111	111
tftp	udp	該当なし	69

表 20-1　デフォルト ポートの割り当て（続き）

プロトコル名	プロトコル	セキュア ポート	宛先ポート
waas	該当なし	該当なし	該当なし
xdmcp	udp	177	177

デフォルトの検査トラフィック基準を選択する場合は、Rule Actions 画面の Protocol Inspection タブで各プロトコルをイネーブルにすることができます。プロトコルは、そのプロトコルのデフォルト ポートでイネーブルにされます。検査対象を特定のフローに限定するには、Source and destination IP address (uses ACL) ボタンを使用し、Service Policy Rule 画面から Source Host/Network または Destination Host/Network などの具体的な基準を選択します。

(注)　デフォルトの検査トラフィック基準は、Protocol and Service グループ ボックスのどのポート設定よりも優先されます。つまり、デフォルトの検査トラフィック基準を使用している間は、どのプロトコルの場合にもデフォルト ポートの割り当てを一切変更できません。

inspection_default セキュリティ ポリシーは、デフォルトの検査トラフィック基準を使用したアプリケーション検査を可能にする事前設定済みのグローバル ポリシーです。このグローバル ポリシーは、FWSM の工場出荷時のデフォルト コンフィギュレーションでイネーブルに設定されます。

(注)　デフォルトの検査トラフィック基準をトラフィック照合基準に指定する場合は、指定されたインターフェイスのセキュリティ ポリシーで検査ルール アクションのみを適用できます。Connection Settings タブのアクションを適用することはできません。

アプリケーション検査のデフォルト ポートの変更

デフォルトの検査トラフィック基準は、Protocol and Service グループ ボックスのどのポート設定よりも優先されます。つまり、デフォルトの検査トラフィック基準を使用している間は、どのプロトコルの場合にもデフォルト ポートの割り当てを一切変更できません。

任意のプロトコルのデフォルト ポート割り当てを変更するには、各検査エンジンを手動で設定してイネーブルにする必要があります。

モジュラ ポリシー フレームワークを使用してプロトコルのデフォルト ポート割り当てを変更するには、次の手順を実行します。

ステップ 1　**Security Policy** ペインで **Service Policy Rules** をクリックし、次に **Add** をクリックします。

Add Service Policy Rule Wizard - Service Policy 画面が表示されます。

ステップ 2　サービス ポリシーを作成します。

特定のインターフェイスのセキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Interface** オプション ボタンをクリックし、選択リストから使用可能なインターフェイスを選択します。

すべてのインターフェイスに適用するグローバル セキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Global** オプション ボタンをクリックします。

ステップ 3　**Policy Name** ボックスに最大 40 文字の名前を入力し、**Next** をクリックします。

Add Service Policy Rule Wizard - Traffic Classification Criteria 画面が表示されます。

ステップ 4　**Source and destination IP address (uses ACL)** ボタンをクリックします。

ステップ 5　**Protocol and Service** グループ ボックスで、プロトコルの **Source Port** および **Destination Port** を選択し、**Next** をクリックします。

Add Service Policy Rule Wizard - Rule Actions 画面が表示されます。

ステップ 6　イネーブルにするプロトコルのチェックボックスをオンにし、**Finish** をクリックします。

Security Policy ペインの **Service Policy Rules** テーブルに、新しいサービス ポリシーが表示されます。

ステップ 7　別の検査エンジンをイネーブルにするには、サービス ポリシーを選択して **Add** をクリックします。

Add Service Policy Rule Wizard - Service Policy 画面が表示されます。

ステップ 8　**Next** をクリックします。

Add Service Policy Rule Wizard - Traffic Classification Criteria 画面が表示されます。

ステップ 9　**Create a new traffic class** をクリックし、必要に応じてトラフィック クラスの名前を変更します。

デフォルトでは、新しいクラスを追加するたびに各トラフィック クラスの名前の終わりにある番号が増分されます。

ステップ 10　**Source and destination IP address (uses ACL)** をクリックします。

ステップ 11　**Traffic Match** タブをクリックします。

ステップ 12　**Protocol and Service** グループ ボックスのプロトコル用に 2 番目のポート番号を選択し、**OK** をクリックします。

Security Policy ペインの **Service Policy Rules** テーブルに新しいアクセス コントロール エントリが表示されます。

複数ポートによるアプリケーション検査の設定

モジュラ ポリシー フレームワークを使用して複数のポートを使用するプロトコルのデフォルト ポート割り当てを変更するには、次の手順を実行します。

ステップ 1　**Security Policy** ペインで **Service Policy Rules** をクリックし、次に **Add** をクリックします。

Add Service Policy Rule Wizard - Service Policy 画面が表示されます。

ステップ 2　サービス ポリシーを作成します。

特定のインターフェイスのセキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Interface** オプション ボタンをクリックし、選択リストから使用可能なインターフェイスを選択します。

すべてのインターフェイスに適用するグローバル セキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Global** オプション ボタンをクリックします。

ステップ 3　**Policy Name** ボックスに最大 40 文字の名前を入力し、**Next** をクリックします。

Add Service Policy Rule Wizard - Traffic Classification Criteria 画面が表示されます。

ステップ 4　**Source and destination IP address (uses ACL)** ボタンをクリックします。

ステップ 5　**Protocol and Service** グループ ボックスのプロトコル用に最初のポート番号を選択し、**Next** をクリックします。

Add Service Policy Rule Wizard - Rule Actions 画面が表示されます。

ステップ 6　次のタブのいずれかを使用して、指定したトラフィック フローに適用するルール アクションを定義します。

- **Protocol Inspection**
- **Connection Settings**

ステップ 7　**Finish** をクリックします。

Security Policy ペインの **Service Policy Rules** テーブルに、新しいサービス ポリシーが表示されます。

ステップ 8　Service Policy Rules テーブルでセキュリティ ポリシーを右クリックします。

ステップ 9　表示されるポップアップ メニューで、**Insert After** を選択します。

Insert Service Policy Rule After 画面が表示されます。

ステップ 10　**Traffic Match** タブをクリックします。

ステップ 11　**Protocol and Service** グループ ボックスのプロトコル用に 2 番目のポート番号を選択し、**OK** をクリックします。

Security Policy ペインの **Service Policy Rules** テーブルに新しいアクセス コントロール エントリが表示されます。

Source and Destination Address（他のコンテキストでの名称は「ACL」）

（このダイアログボックスは、サービス ポリシー ルールを編集する場合は **ACL** と呼ばれます）

このダイアログボックスでは、送信側または受信側ホストの IP アドレスまたは TCP/UDP ポートに基づいて、サービス ポリシー ルールを適用するトラフィックを特定できます。また、このダイアログボックスを使用して、ポリシー ルールを有効にする **Time Range** を選択することもできます。

フィールド

- Select an action：このダイアログボックスで指定した基準にトラフィックが一致する必要がある、またはその基準に一致しないようにするかを指定できます。
- Time Range
  - Time Range：ポリシー ルールを有効にする時間範囲を選択できます。
  - New：Add Time Range ダイアログボックスにアクセスできます。詳細については、「Add/Edit Time Range」を参照してください。
- Source Host/Network x
  - IP Address：トラフィックの送信元を IP アドレスによって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Interface リスト、IP address ボックス、. . . ボタン、Mask リストが表示されます。
  - Name：トラフィックの送信元をインターフェイス名によって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Name リストが表示されます。
  - Group：トラフィックの送信元をオブジェクト グループによって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Interface リストと Group リストが表示されます。
  - Interface：トラフィックの送信元がオンになっているインターフェイスの名前を指定します。リストは、IP Address ボタンか Group ボタンが選択されている場合にのみ表示されます。
  - IP address：トラフィックの送信元を識別するために使用する IP アドレスを指定します。このボックスは、IP Address ボタンが選択されている場合にのみ表示されます。
  - . . .：Select host/network ダイアログボックスにアクセスできます。このダイアログボックスでは、事前に設定されたリストからホストまたはネットワークを選択できます。このボタンは、IP Address ボタンが選択されている場合にのみ表示されます。
  - Mask：IP address ボックスに入力したアドレスのサブネット マスクを指定します。このボックスは、IP Address ボタンが選択されている場合にのみ表示されます。
  - Name：トラフィックの送信元がオンになっているインターフェイスの名前を指定します。このリストは、Name ボタンが選択されている場合にのみ表示されます。
  - Group：トラフィックの送信元が属しているオブジェクト グループを指定します。リストの項目は、Hosts/Networks ペインで制御されます。このペインの詳細については、「ネットワーク オブジェクトの概要」を参照してください。このグループ リストは、Group ボタンが選択されている場合にのみ表示されます。
- Destination Host/Network
  - IP Address：トラフィックの宛先を IP アドレスによって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Interface リスト、IP address ボックス、. . . ボタン、Mask リストが表示されます。
  - Name：トラフィックの宛先をインターフェイス名によって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Name リストが表示されます。
  - Group：トラフィックの宛先をオブジェクト グループによって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Interface リストと Group リストが表示されます。
  - Interface：トラフィックの宛先がオンになっているインターフェイスの名前を指定します。このリストは IP Address ボタンまたは Group ボタンが選択されている場合にのみ表示されます。

  - IP address：トラフィックの宛先を識別するために使用する IP アドレスを指定します。このボックスは、IP Address ボタンが選択されている場合にのみ表示されます。
  - . . .：Select host/network ダイアログボックスにアクセスできます。このダイアログボックスでは、事前に設定されたリストからホストまたはネットワークを選択できます。このボタンは、IP Address ボタンが選択されている場合にのみ表示されます。
  - Mask：IP address ボックスに入力したアドレスのサブネット マスクを指定します。このボックスは、IP Address ボタンが選択されている場合にのみ表示されます。
  - Name：トラフィックの宛先がオンになっているインターフェイスの名前を指定します。このリストは、Name ボタンが選択されている場合にのみ表示されます。
  - Group：トラフィックの宛先が属しているオブジェクト グループを指定します。リストの項目は Hosts/Networks ペインで制御されます。このペインの詳細については、「ネットワーク オブジェクトの概要」を参照してください。このグループ リストは、Group ボタンが選択されている場合にのみ表示されます。

- Rule Flow Diagram：FWSM によって転送されるトラフィックに対する、特定のフィルタリング アクションの適用方法をグラフィカルに表現します。
- Protocol and Service
  - TCP：TCP プロトコルまたはサービスに基づいてトラフィックを照合します。
  - UDP：UDP プロトコルまたはサービスに基づいてトラフィックを照合します。
  - ICMP：ICMP プロトコルの値に基づいてトラフィックを照合します。
  - IP：IP プロトコルの値に基づいてトラフィックを照合します。
  - Manage Service Groups：Manage Service Groups 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、サービス グループを作成および編集できます。このボタンは、TCP ボタンが選択されている場合にのみ使用できます。
  - Source Port：TCP または UDP のオプション ボタンが選択されている場合にのみ表示されます。

    Service：送信元ポートの値に基づいてトラフィックを照合します。

    Operator：照合する 1 つのポート、またはポートの範囲を特定するかどうかを指定します。リストから、=（と等しい）、not=（と等しくない）、>（より大きい）、<（より小さい）を選択すると、. . . ボタンが表示されます。このボタンにより、特定の名前付きポートを選択できます。リストから range を選択すると、2 つのボックスが表示されます。それらのボックスに、範囲の開始ポートと終了ポートを入力できます。

    ...：Service 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、照合する TCP または UDP ポートの名前付きの値を選択できます。

    Service Group：送信元サービス グループに基づいてトラフィックを照合します。リストの項目を制御するには、**Manage Service Groups** ボタンを使用します。
  - Destination Port：TCP または UDP のオプション ボタンが選択されている場合にのみ表示されます。

    Service：宛先ポートの値に基づいてトラフィックを照合します。

    Operator：照合する 1 つのポート、またはポートの範囲を特定するかどうかを指定します。リストから、=（と等しい）、not=（と等しくない）、>（より大きい）、<（より小さい）を選択すると、. . . ボタンが表示されます。このボタンにより、特定の名前付きポートを選択できます。リストから range を選択すると、2 つのボックスが表示されます。それらのボックスに、範囲の開始ポートと終了ポートを入力できます。

    ...：Service 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、照合する TCP または UDP ポートの名前付きの値を選択できます。

    Service Group：宛先サービス グループに基づいてトラフィックを照合します。リストの項目を制御するには、Manage Service Groups ボタンを使用します。
  - ICMP Type：ICMP オプション ボタンが選択されている場合にのみ表示されます。

    ICMP type：トラフィックの ICMP タイプを入力できます。

    ... ：Service 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、事前に設定されたリストから ICMP タイプを選択できます。

— IP Protocol：IP オプション ボタンが選択されている場合にのみ表示されます。

IP protocol：トラフィックの IP プロトコルを入力できます。

...：Service 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、事前に設定されたリストから IP プロトコルを選択できます。

モード

次の表に、この機能を使用できるモードを示します。

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

Destination Port

Destination Port ダイアログボックスは、Traffic Match Criteria ダイアログボックスで TCP or UDP destination port を選択する場合、またはサービス ポリシー ルールの編集時に対応するタブをクリックする場合に表示されます。このダイアログボックスでは、TCP または UDP の宛先ポートに基づいて、サービス ポリシー ルールを適用するトラフィックを特定できます。

フィールド

- TCP：宛先で使用される TCP ポートに基づいてトラフィックを照合します。
- UDP：宛先で使用される UDP ポートに基づいてトラフィックを照合します。
- Operator：照合する 1 つのポート、またはポートの範囲を特定するかどうかを指定します。

  リストから =（等号）を選択すると、. . . ボタンが表示されます。このボタンにより、特定の名前付きポートを選択できます。

  リストから range を選択すると、2 つのボックスが表示されます。それらのボックスに、範囲の開始ポートと終了ポートを入力できます。
- ...：Service 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、照合する TCP または UDP ポートの名前付きの値を選択できます。

モード

次の表に、この機能を使用できるモードを示します。

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

Rule Actions > Protocol Inspection タブ

Protocol Inspection タブでは、使用可能なさまざまなタイプのアプリケーション検査をイネーブルまたはディセーブルにすることができます。特定のアプリケーション検査タイプの設定を表示または変更するには、**Configure** を選択します。これによって、プロトコルで使用するマップ名を選択できます。マップの設定については、P.6-9 の「検査マップの設定」を参照してください。

フィールド

- CTIQBE：CTIQBE プロトコルでのアプリケーション検査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検査をイネーブルにします
  - Configure：Configure DCERPC 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検査をイネーブルにします。
  - Configure：Configure DNS 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検査をイネーブルにします。ESMTP アプリケーション検査は、SMTP アプリケーション検査がディセーブルの場合のみ、イネーブルになります。ESMTP アプリケーション検査は、コントロール プレーン パス処理で行います。したがって、FWSM にある 1 台の汎用プロセッサに対して行います。
- FTP：FTP プロトコルでのアプリケーション検査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検査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 検査は、特別なライセンスがなければ使用できません。

- H323 H225：H323 H225 プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：Select H.225 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検査をイネーブルにします。
- HTTP：HTTP プロトコルでのアプリケーション検査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検査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検査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検査をイネーブルにします。
- MGCP：MGCP プロトコルでのアプリケーション検査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検査をイネーブルにします。
- PPTP：PPTP プロトコルでのアプリケーション検査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検査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検査をイネーブルにします。
- SIP：SIP プロトコルでのアプリケーション検査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。
- SKINNY：Skinny プロトコルでのアプリケーション検査をイネーブルにします。
- SMTP：SMTP プロトコルでのアプリケーション検査をイネーブルにします。SMTP アプリケーション検査は、ESMTP アプリケーション検査がディセーブルの場合のみ、イネーブルになります。SMTP アプリケーション検査は、高速パス処理で行います。したがって、FWSM にある 3 台のネットワーク プロセッサのうちの 1 台で行います。
- SNMP：SNMP プロトコルでのアプリケーション検査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検査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検査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検査をイネーブルにします。
- WAAS: WAAS プロトコルでのアプリケーション検査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検査をイネーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

- 検査マップの設定（P.6-9）
- 『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』にあるプロトコルごとの **Inspect** コマンド ページ

Configure DCERPC

Select DCERPC Inspect Map ダイアログボックスでは、DCERPC アプリケーション検査のイネーブル化、DCERPC マップの選択と編集、または新しい DCERPC マップの作成を行うことができます。DCERPC マップでは、DCERPC アプリケーション検査の設定値を変更できます。Select DCERPC Map テーブルには、アプリケーション検査をイネーブルにするときに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：DCERPC マップが DCERPC アプリケーション検査へ適用されるのを避けるためには、このボタンをイネーブルにします。
- Select a DCERPC map for fine control over inspection radio：DCERPC マップを DCERPC アプリケーション検査に適用するためには、このボタンをイネーブルにします。このボタンをイネーブルにしてから、事前に定義したマップを選択して適用するか、Add をクリックして新しいマップを定義します。
- Add：Add DCERPC Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 DNS

フィールド

Maximum DNS packet length (default 512)：FWSM の通過が許可されている DNS メッセージの最大パケット長を変更します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 アプリケーション検査のイネーブル化、FTP マップの選択と編集、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 アプリケーション検査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、アプリケーション検査をイネーブルにするときに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 アプリケーション検査をイネーブルにします。これによって FWSM は、埋め込みコマンドが FTP 要求に含まれている場合には接続をドロップします。
- Add：Add DCERPC Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 アプリケーション検査のイネーブル化、GTP マップの選択と編集、または新しい GTP マップの作成を行うことができます。GTP マップにより、GTP アプリケーション検査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、アプリケーション検査をイネーブルにするときに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 検査には、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 FWSM で GTP アプリケーション検査のイネーブル化を試みると、FWSM はエラー メッセージを表示します。

フィールド

- Add：Add GTP Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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.225 Map

Select H.225 Map ダイアログボックスでは、厳密な H.225 アプリケーション検査のイネーブル化（アプリケーション ファイアウォールと呼ばれる場合もある）、H.225 マップの選択と編集、または新しい H.225 マップの作成を行うことができます。H.225 マップにより、H.225 アプリケーション検査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.225 Map テーブルには、アプリケーション検査をイネーブルにするときに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**：Add H.225 Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、厳密な HTTP アプリケーション検査のイネーブル化（アプリケーション ファイアウォールと呼ばれる場合もある）、HTTP マップの選択と編集、または新しい HTTP マップの作成を行うことができます。HTTP マップにより、HTTP アプリケーション検査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、アプリケーション検査をイネーブルにするときに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：Add HTTP Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 アプリケーション検査のイネーブル化、MGCP マップの選択と編集、または新しい MGCP マップの作成を行うことができます。MGCP マップにより、MGCP アプリケーション検査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、アプリケーション検査をイネーブルにするときに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：Add MGCP Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、厳密な SIP アプリケーション検査のイネーブル化（アプリケーション ファイアウォールと呼ばれる場合もある）、SIP マップの選択と編集、または新しい SIP マップの作成を行うことができます。SIP マップでは、SIP アプリケーション検査の設定値を変更できます。Select SIP Map テーブルには、アプリケーション検査をイネーブルにするときに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：SIP マップが SIP アプリケーション検査へ適用されるのを避けるためには、このボタンをイネーブルにします。
- Select a SIP map for fine control over inspection radio：SIP マップを SIP アプリケーション検査に適用するためには、このボタンをイネーブルにします。このボタンをイネーブルにしてから、事前に定義したマップを選択して適用するか、Add をクリックして新しいマップを定義します。
- Add：Add SIP Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 アプリケーション検査のイネーブル化、SNMP マップの選択と編集、または新しい SNMP マップの作成を行うことができます。SNMP マップにより、SNMP アプリケーション検査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、アプリケーション検査をイネーブルにするときに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：Add SNMP Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ステート バイパスの概要

Rule Actions > Connection Settings タブで TCP State Bypass チェックボックスをオンにすると、TCP ステート バイパスを設定できます。この項では、TCP ステート バイパス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。

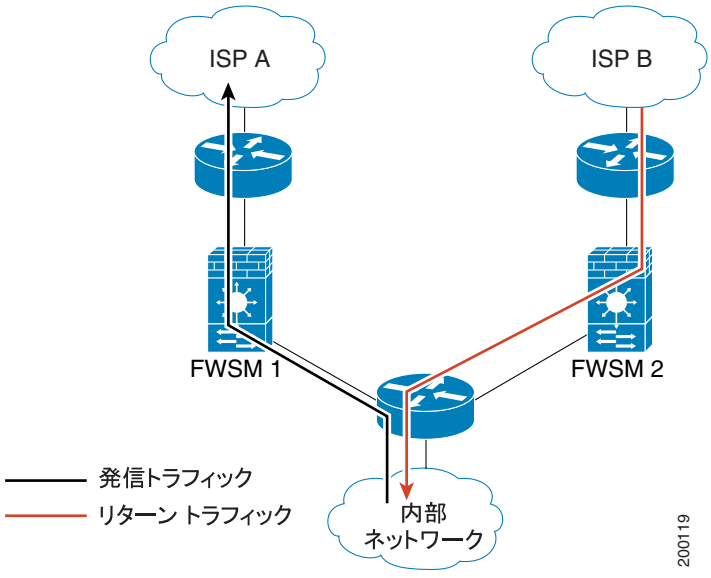
別個の FWSM を通過する発信および着信フローの許可

デフォルトでは、FWSM を通過するすべてのトラフィックは、アダプティブ セキュリティ アルゴリズムによって検査され、セキュリティ ポリシーに基づいて、許可またはドロップされます。FWSM は、各パケットの状態（新規接続か、既存接続か）をチェックし、セッション管理パス（新規接続の SYN パケット）、高速パス（既存接続）、コントロール プレーン パス（高度な検査）のいずれかに割り当てることによって、ファイアウォールのパフォーマンスを最大化します。

高速パスで既存接続を照合する TCP パケットは、セキュリティ ポリシーをすべて再照合しなくても FWSM を通過できます。この機能によって、パフォーマンスが最大化されます。ただし、SYN パケットを使用して高速パスでセッションを確立する方法や、高速パスで発生する照合（TCP シーケンス番号など）は、非対称ルーティング ソリューションの障害になることがあります。接続の発信および着信フローは同じ FWSM を通過する必要があります。

たとえば、新規接続は、FWSM 1 に向かいます。SYN パケットは、セッション管理パスを通過し、接続のエントリが高速パス テーブルに追加されます。この接続の後続のパケットは、FWSM 1 を通過した後で高速パスのエントリを照合し、通過します。ただし、後続のパケットが FWSM 2 へ向かうと、そこにはセッション管理パスを通過した SYN パケットがなく、接続の高速パスのエントリもないため、パケットは、ドロップします。図 20-1 は、発信トラフィックが着信トラフィックと異なる FWSM を通過する非対称ルーティングの例を示しています。

図 20-1　非対称ルーティング



アップストリーム ルータに非対称ルーティングが設定され、トラフィックが 2 つの FWSM を交互に通過する場合は、特定のトラフィックの TCP ステート バイパスを設定できます。TCP ステート バイパスは、高速パスに確立されているセッションの方法を変更し、高速パスの照合をディセーブルにします。この機能は、UDP 接続を処理するように TCP トラフィックを処理します。指定されたネットワークに照合する non-SYN パケットが FWSM に入り、高速パスのエントリがない場合、パケットは、高速パスに接続を確立するためにセッション管理パスを通過します。高速パスに入ると、トラフィックは高速パス照合をバイパスします。

サポートされていない機能

TCP ステート バイパスを使用する場合、次の機能はサポートされていません。

- アプリケーション検査：アプリケーション検査は、着信および発信トラフィックが同じ FWSM を通過することを要求します。したがって、アプリケーション検査は、TCP ステート バイパスではサポートされていません。
- AAA 認証セッション：1 つの FWSM を認証する場合、別の FWSM を経由するトラフィックは、ユーザがそれを認証していないため拒否されます。

NAT との互換性

変換セッションが各 FWSM に別個に確立されるため、スタティック NAT を TCP ステート バイパス トラフィックの両方の FWSM に必ず設定してください。ダイナミック NAT を使用する場合は、FWSM 1 のセッションに選択したアドレスが FWSM 2 のセッションに選択したアドレスと異なります。

接続タイムアウト

特定の接続に 2 分間トラフィックがない場合、接続はタイムアウトになります。Properties > Timeouts > Connection チェックボックスを使用して、このデフォルトを上書きできます。標準 TCP 接続は、デフォルトで 60 分後にタイムアウトになります。

Rule Actions > Connection Settings タブ

Connection Settings タブでは、最大接続数、最大初期接続、およびホストまたはネットワークでの TCP パケットのランダム化で使用するシーケンス番号を設定できます。また、接続タイムアウトと TCP 正規化も設定できます。

フィールド

- Maximum Connections：同時 TCP、UDP 接続、および初期接続の最大接続数を設定します。
  - Maximum TCP and UDP Connections：サブネット全体の同時 TCP および UDP 接続の最大接続数を 65,536 に指定します。両方のプロトコルのデフォルトは、0 で、これが最大接続数となります。
- Randomize Sequence Number：Randomize Sequence Number 機能の状態を、イネーブルまたはディセーブルに設定します。TCP の初期シーケンス番号のランダム化は、別のインライン ファイアウォールがシーケンス番号をランダム化していれば、ディセーブルにできます。これは、両方のファイアウォールがこのアクションを実行する必要がないためです。ただし、両方のファイアウォールの ISN のランダム化をイネーブルにしてもトラフィックへの影響はありません。

  各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。セキュリティ アプライアンスは、発信方向へ通過する 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が接続されている場合、ISN は、両方向の SYN でランダム化します。

保護されたホストの ISN をランダム化すると、攻撃者が新しい接続の次の ISN を予測できなくなり、新しいセッションを乗っ取ることができなくなります。

- TCP Timeout：接続タイムアウト ルールを指定します。
  - 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 と入力します。接続時間は 5 分以上にする必要があります。デフォルトは 30 分です。
  - 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 と入力します。接続時間は 5 分以上にする必要があります。デフォルトは 10 分です。
  - Connection Timeout：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 と入力します。接続時間は 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：TCP エンドポイントがタイムアウトの前にリセットされるように指定します。
- Idle Timeout：アイドル タイムアウト ルールを指定します。
  - Idle Timeout：接続がドロップ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、0:00:00 と入力します。接続時間は 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。
- Advanced Options：TCP ステート バイパス ルールを指定します。
  - TCP State Bypass：TCP ステート バイパスをイネーブルにします。詳細については、P.20-20 の「TCP ステート バイパスの概要」を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Class Map

Edit Class Map ダイアログボックスでは、クラスマップの説明を追加または編集できます。

フィールド

- Description：クラスマップ説明の名前を追加または変更します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Rule

Edit Rule 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

- Select an action：新しいルールのアクション タイプを決めます。Select an action リストから、Permit または Deny のいずれかを選択します。
  - Permit：すべての一致したトラフィックを許可します。
  - Deny：すべての一致したトラフィックを拒否します。
- Apply to traffic：ルールを適用するトラフィック タイプを決めます。
  - Incoming to source interface：送信元インターフェイスへの着信トラフィックを選択します。
  - Outgoing from destination interface：宛先インターフェイスからの発信トラフィックを選択します。
- Syslog status：syslog がイネーブルかどうかを示します。
- More Options：アクセスリストのロギングをイネーブルにして、ロギング オプションを設定します。More Options ボタンにより、ロギング オプションを設定できます。このボタンにより、次の操作を実行できます。
  - デフォルトのロギング動作を使用する。
  - ルールのロギングをイネーブルにする。
  - ルールのロギングをディセーブルにする。
  - 許可と拒否のログ レベルとロギング間隔を設定する。このオプションは、Enable Logging チェックボックスをオンにします。

    詳細については、「Log Options」を参照してください。また、グローバル ロギング オプションの設定については、「Advanced Access Rule Configuration」を参照してください。
- Time Range：このルールに定義されている時間範囲をリストから選択します。
- New：このルールの新しい時間範囲を作成します。「Add Time Range」を参照してください。
- Source and Destination Host/Network IP Address：IP アドレスによってネットワークを識別するには、このボタンを選択します。
  - Interface：ホストまたはネットワークが常駐するインターフェイス。
  - IP address：ホストまたはネットワークの IP アドレス。
  - Browse：Select Host/Network ペインのオプションをクリックして既存のホストまたはネットワークを選択し、Name、Interface、IP address、および Mask の各ボックスに、選択したホストまたはネットワークのプロパティ値を入力します。
  - Mask：ホストまたはネットワークのサブネット マスク。
- Name：ネットワークを名前で特定するには、このボタンをクリックします。ホスト / ネットワークへの名前付けについては、Hosts/Networks タブを参照してください。

  ホストまたはネットワークの名前。このオプションを選択し、再びルールを開いて編集すると、ボタン選択が IP Address に復帰し、名前付きホスト / ネットワーク IP アドレス情報がフィールドに表示されます。
- Group：Hosts/Networks　タブでグループ化したネットワークとホストのグループを特定するには、このボタンをクリックします。
  - Interface：グループ内のホストおよびネットワークに接続されたインターフェイス。
  - Group：グループ名。
- Protocol and Service: TCP and UDP ボタン：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、アクセスリスト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 Service：HTTP または FTP など、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 サービス名を指定するには、このオプションをクリックします。

- Source Port Service：演算子リストは、アクセスリスト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：その範囲のポート番号の 1 つと等しい。
- Source Port Service：サービスのリストから、ポート番号、ポート範囲、または HTTP や FTP などのウェルノウン サービス名を指定します。Browse ボタンをクリックすると Service 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、事前に設定されたリストから TCP または UDP サービスを選択できます。
- Source Port Service Group：Service Group リストからサービス グループを指定するには、このオプションをクリックします。

- Protocol and Service ICMP：ICMP タイプ ボックスで、ルールの ICMP タイプを指定します。Browse ボタンをクリックすると Service 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、事前に設定されたリストから ICMP タイプを選択できます。
- Protocol and Service 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。Browse ボタンをクリックすると Protocols 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、事前に設定されたリストから IP プロトコルを選択できます。
- Manage Service Groups：サービス グループを管理します。サービス グループを使用して、アクセスリストと照合させる複数の連続していないポート番号を特定できます。たとえば、HTTP、FTP、およびポート番号 5、8、9 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、および TCP-UDP のサービス 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。詳細については、「Manage Service Groups」を参照してください。
- Description：（オプション）アクセス ルールの説明を入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Service Policy Rule > Traffic Classification タブ

Traffic Classification タブでは、セキュリティ ポリシー ルールを適用するトラフィックの照合に使用する基準を指定できます。

フィールド

- Description：トラフィック分類の説明を指定します。
- Default Inspection Traffic：デフォルトの検査トラフィック ポリシーで指定された基準を使用します。
- Source and destination IP address (uses ACL)：アクセス コントロール リストを使用し、送信元と宛先 IP アドレスに基づいてトラフィックを照合します。このフィールドは、インターフェイス サービス ポリシーを使用して特定のインターフェイスにルールを適用する場合にのみ選択できます。
- TCP or UDP destination port：TCP または UDP 宛先ポートに基づいてトラフィックを照合します。
- Any traffic：トラフィック タイプに関係なくすべてのトラフィックを照合します。

モード

次の表に、この機能を使用できるモードを示します。

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

SUNRPC Server

SUNRPC Server ペインには、FWSM を通過できる SunRPC サービスとそれらのタイムアウト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：FWSM 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Add/Edit SUNRPC Service ダイアログボックスでは、FWSM 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：SunRPC サーバが常駐するインターフェイスを表示します。
- 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：FWSM 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

NAT の設定

この項では、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

この項では、FWSM で NAT がどのように機能するかを説明します。次の項目を取り上げます。

NAT の概要

アドレス変換は、パケット上にある実際のアドレスを、宛先ネットワークでルーティングできるマッピング済みアドレスに置き換えます。NAT は、実際のアドレスをマッピング済みアドレスに変換するプロセスと、トラフィックを返すために変換を元に戻すプロセスの 2 段階で構成されています。NAT はルーテッド モードと透過ファイアウォール モードの両方でサポートされています。

FWSM は、NAT のルールがトラフィックと一致した場合にアドレスを変換します。NAT のルールが一致しない場合、パケットの処理が続行されます。NAT の制御をイネーブルにする場合は例外です。NAT の制御では、上位のセキュリティ インターフェイス（内部）から下位のセキュリティ インターフェイス（外部）へ通過するパケットが NAT のルールと一致している必要があります。一致しない場合はパケットの処理が停止します（セキュリティ レベルの詳細については、P.5-3 の「等位セキュリティ レベル間の通信のイネーブル化」を参照してください。NAT 制御の詳細については、P.21-5 の「NAT 制御」を参照してください）。

（注） このマニュアルでは、変換の種類に関係なくすべて NAT としています。NAT について説明する場合、*内部*と*外部*は相対的であり、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。上位のセキュリティ レベルが内部で、下位のセキュリティ レベルが外部となっています。たとえば、インターフェイス 1 のセキュリティ レベルが 60 でインターフェイス 2 のセキュリティ レベルが 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」となります。

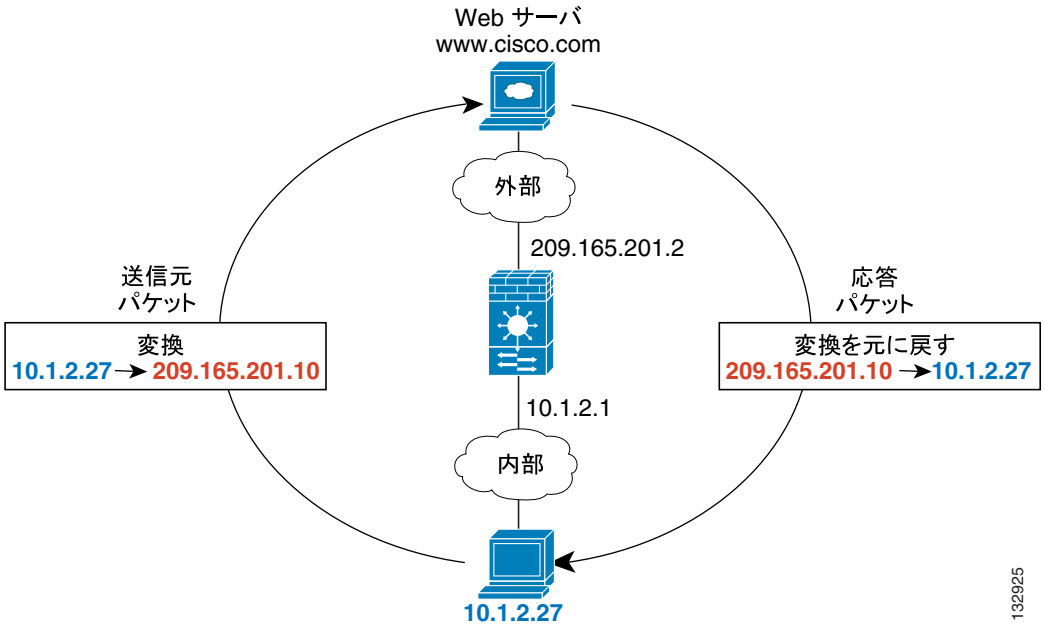
NAT の利点のいくつかを次に示します。

- 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 は実際のアドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- アドレスの重複などの IP ルーティングの問題点を解決できます。

ルーテッド モードの NAT

図 21-1 は、内部にプライベート ネットワークを持つ一般的なルーテッド モードの NAT シナリオを示しています。10.1.1.27 の内部ホストから Web サーバへパケットが送信される場合、パケットの実際の送信元アドレス 10.1.1.27 がマッピング済みアドレス 209.165.201.10 に変換されます。Web サーバは応答をマッピング済みアドレス 209.165.201.10 に送信し、FWSM はパケットを受信します。次に、FWSM がマッピング済みアドレス 209.165.201.10 の変換を実際のアドレス 10.1.1.27 に戻してから、ホストへ送信します。

図 21-1　NAT の例：ルーテッド モード



透過モードの NAT

透過モードで NAT を使用すると、そのネットワークに対する NAT をアップストリーム ルータまたはダウンストリーム ルータで実行する必要がなくなります。たとえば、透過ファイアウォール FWSM を 2 つの VRF 間に配置すると、VRF とグローバル テーブルの間で BGP ネイバーの関係を確立するのに役立ちます。ただし、VRF ごとの NAT はサポートされていない場合があります。この場合、透過モードで NAT を使用する必要があります。

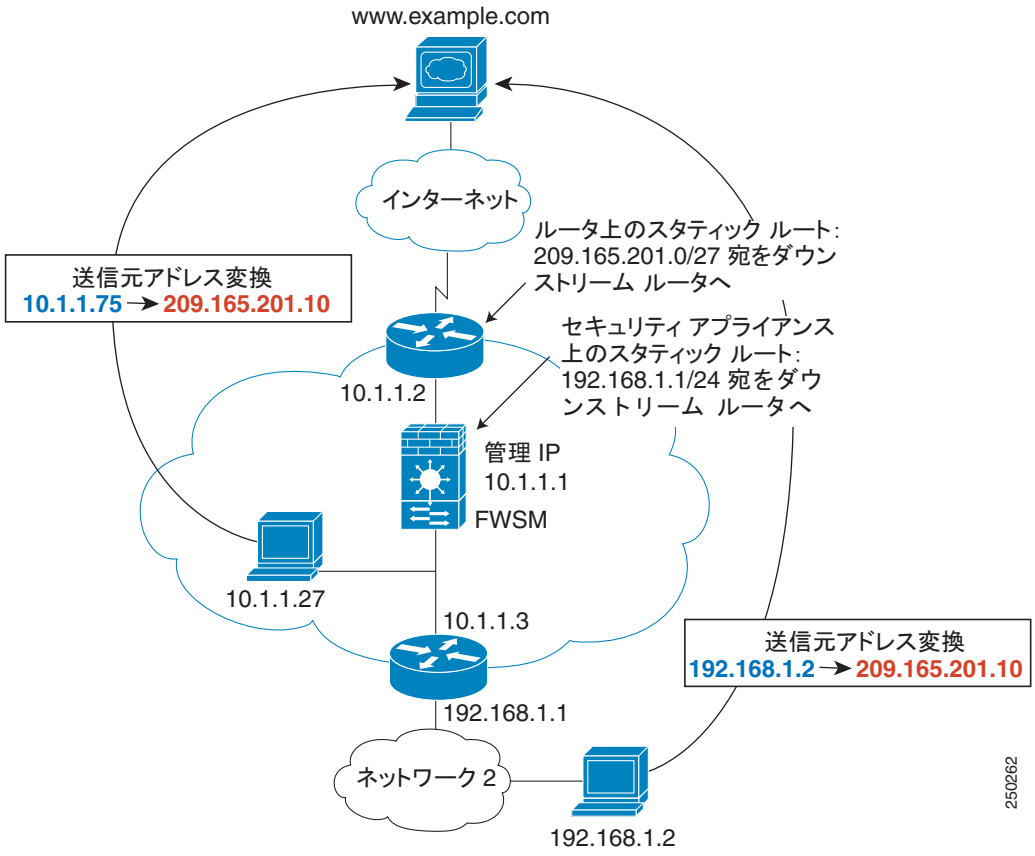
透過モードの NAT には、次のような要件および制限事項があります。

- マッピング済みアドレスが透過ファイアウォールと同じネットワークにない場合、（FWSM 経由で）ダウンストリーム ルータをポイントする、マッピング済みアドレスのスタティック ルートをアップストリーム ルータで追加する必要があります。
- 実際の宛先アドレスが直接 FWSM に接続されていない場合、ダウンストリーム ルータをポイントする実際の宛先アドレスのスタティック ルートも FWSM で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で MAC アドレス テーブルを使用するため、FWSM のルートは不要です。ただし、NAT により FWSM が MAC アドレス ルックアップではなくルート 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。

- 透過ファイアウォールにはインターフェイスの IP アドレスがないため、インターフェイスの PAT を使用できません。
- ARP 検査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内外のどちらかのホストから相手のホストに ARP 要求が送信され、開始側のホストの実際のアドレスが同じサブネットの別のアドレスにマッピングされた場合、実際のアドレスは ARP 要求で可視のままになっています。

図 21-2 に、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ある場合の、一般的な透過モードの NAT シナリオを示します。このシナリオでは、透過ファイアウォールが NAT サービスを実行するので、アップストリーム ルータで NAT を実行する必要がありません。10.1.1.27 の内部ホストから Web サーバにパケットが送信された場合、そのパケットの実際の送信元アドレス 10.1.1.27 は、マッピング済みアドレス 209.165.201.10 に変換されます。サーバは応答をマッピング済みアドレス 209.165.201.10 に送信し、FWSM はパケットを受信します。これは、アップストリーム ルータで、FWSM を経由するスタティック ルート内にこのマッピング済みネットワークが指定されているからです。次に、FWSM が変換を元に戻し、マッピング済みアドレス 209.165.201.10 を実際のアドレス 10.1.1.27 に戻します。実際のアドレスは直接に接続されているので、FWSM がホストに直接に応答を送信します。192.168.1.2 のホストの場合、FWSM は自分のルート テーブルでルートをルックアップし、スタティック ルートに基づいてパケットを 10.1.1.3 のダウンストリーム ルータへ送信すること以外は、同じプロセスが実行されます。

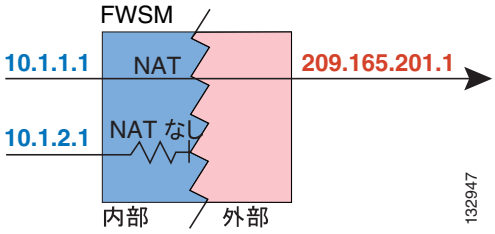
図 21-2　NAT の例：透過モード



NAT 制御

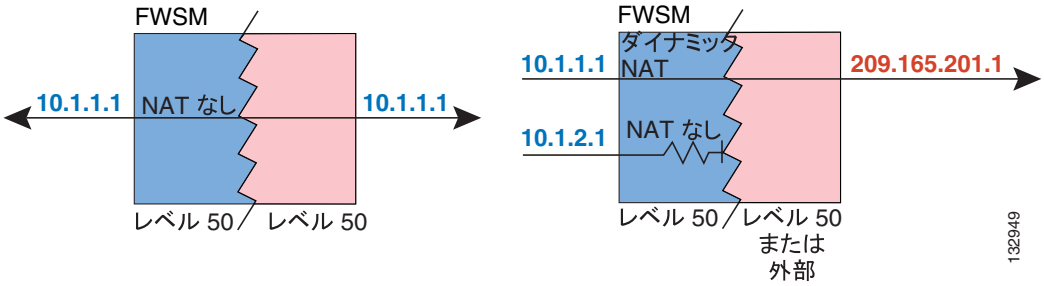
NAT 制御では、内部インターフェイスから外部インターフェイスへ通過するパケットが NAT のルールと一致している必要があります。内部ネットワークのホストから外部ネットワークのホストへアクセスする場合、内部ホストのアドレスを変換するよう NAT を設定する必要があります（図 21-3 を参照）。

図 21-3　NAT 制御と発信トラフィック



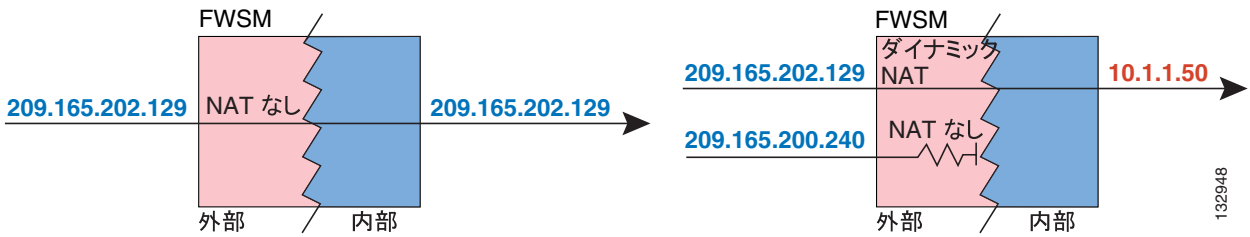
セキュリティ レベルが等位のインターフェイス間の通信では、NAT は必須ではありません。ただし、NAT 制御がイネーブルの状態でセキュリティが等位のインターフェイスにダイナミック NAT または PAT を設定すると、等位セキュリティのインターフェイスまたは外部インターフェイスからのトラフィックは、すべて NAT のルールと一致している必要があります（図 21-4 を参照）。

図 21-4　NAT 制御と等位セキュリティ レベルのトラフィック



同様に、NAT 制御がイネーブルの状態で外部ダイナミック NAT または PAT を設定すると、すべての外部トラフィックは、内部インターフェイスへのアクセス時に NAT のルールと一致している必要があります（図 21-5 を参照）。

図 21-5　NAT 制御と着信トラフィック



NAT 制御がイネーブルの状態でスタティック NAT を使用する場合は、このような制約事項はありません。

デフォルトでは NAT 制御がディセーブルになっているので、NAT を実行する事情が特にない限り、どのネットワークでも NAT を実行する必要はありません。ただし、旧バージョンのソフトウェアからアップグレードした場合は、NAT 制御をシステムでイネーブルにする場合があります。

NAT 制御でセキュリティを強化したいが、内部アドレスを変換したくない場合がいくつかあるときは、NAT 免除ルールまたはアイデンティティ NAT ルールをこれらの内部アドレスに適用できます（詳細については、P.21-37 の「NAT 免除の使用」を参照してください）。

NAT 制御の設定については、P.21-17 の「NAT 制御の設定」を参照してください。

（注） マルチコンテキスト モードの場合、パケット分類子が NAT の設定に従っ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。NAT 制御がディセーブルなので NAT を実行していない場合、分類子がネットワーク構成の変更を必要とする場合があります。分類子と NAT の関係の詳細については、P.7-3 の「FWSM によるパケットの分類方法」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 タイプについて説明します。アドレス変換は、ダイナミック NAT、Port Address Translation（PAT; ポート アドレス変換）、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せとして実装できます。また、たとえば NAT 制御をイネーブルにしたが NAT を実行したくない場合などは、NAT をバイパスするよう設定することもできます。この項では、次の項目を取り上げます。

ダイナミック NAT

ダイナミック NAT では、実際のアドレス グループを、宛先ネットワークでルーティング可能なマッピング済みアドレスのプールに変換します。マッピング済みプールに含まれるアドレスの数は、実際のアドレス グループよりも少ない場合があります。変換するホストが宛先ネットワークにアクセスすると、FWSM がマッピング済みアドレスのプールからそれらに IP アドレスを割り当てます。変換が追加されるのは、実際のホストが接続を開始した場合のみです。変換は接続が確立されている間のみ有効です。また、変換のタイムアウト後にユーザが同じ IP アドレスを維持することはできません（Timeout を参照）。そのため、宛先ネットワークのユーザは、（アクセスリストでその接続が許可されている場合でも）ダイナミック NAT を使用するホストに対しては、信頼できる接続を開始できません。また、実際のホスト アドレスに直接接続しようとすると、FWSM によって拒否されます。ホストへの信頼できるアクセスについては、以降の「スタティック NAT」または「スタティック PAT」の項目を参照してください。

図 21-6 に、実際のアドレスに接続しようとするリモート ホストを示します。FWSM はマッピング済みアドレスへのリターン接続のみを許可しているため、接続は拒否されます。

図 21-6　実際のアドレスに接続しようとするリモート ホスト

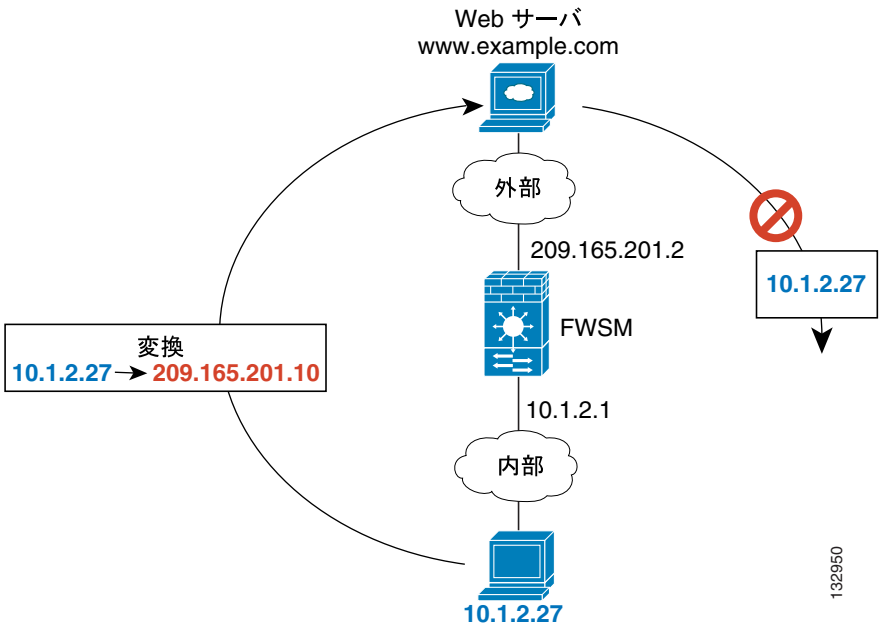
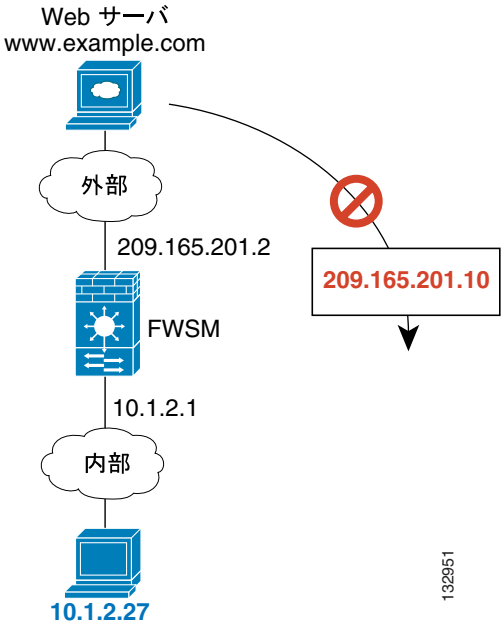


図 21-7 に、マッピング済みアドレスへの接続を開始しようとするリモート ホストを示します。現在、このアドレスは変換テーブルにないので、FWSM がパケットをドロップします。

図 21-7　マッピング済みアドレスへの接続を開始しようとするリモート ホスト



(注)　変換が確立されている間、アクセスリストで許可されていれば、リモート　ホストは変換対象ホストへの接続を試みることができます。アドレスを予測できないので、リモートホストが変換対象ホストに接続できる可能性は非常に低くなります。万一、接続が成功した場合でも、アクセスリストのセキュリティに頼ることができます。

ダイナミック NAT には、次の短所があります。

- マッピング済みプールのアドレスが実際のアドレスよりも少ない場合、トラフィック量が予想を超えた場合にアドレスが足りなくなる場合があります。

  このような現象が頻繁に発生した場合は 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 より多くの変換を実現できます。
- マッピング済みアドレスの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。宛先ネットワークでインターネットなどの登録済みアドレスを使用する必要がある場合、使用可能なアドレスが不足する可能性があります。

ダイナミック NAT の利点は、プロトコルによっては PAT が使用できない場合があることです。たとえば、オーバーロード変換用のポート番号がない IP プロトコル（GRE version 0 など）では、PAT は機能しません。また PAT は、データ ストリームと制御パスが異なるポートに存在する、非オープン スタンダードの一部のアプリケーション（一部のマルチメディア アプリケーションなど）では機能しません。NAT と PAT のサポートの詳細については、P.21-2 の「NAT の概要」を参照してください。

PAT

PAT は複数の実際のアドレスを単一のマッピング済み IP アドレスに変換します。特に FWSM は、実際のアドレスと送信元ポート（実際のソケット）を、マッピング済みアドレスと 1024 より多くの一意のポート（マッピング済みソケット）に変換します。送信元ポートが接続ごとに異なるため、接続ごとに個別の変換が必要です。たとえば、10.1.1.1:1025 の場合、10.1.1.1:1026 とは別の変換が必要です。

接続がタイムアウトになってから非アクティブ状態が 30 秒間続くと、ポート変換もタイムアウトになります。タイムアウト設定は変更できません。宛先ネットワークのユーザは、（アクセスリストで接続が許可されている場合でも）PAT を使用するホストへの信頼できる接続を開始できません。ホストの実際のポート番号またはマッピング済みポートの番号を予測できないだけでなく、変換対象ホストが開始側ホストでない限り、FWSM は変換をまったく作成しません。ホストへの信頼できるアクセスについては、以降の「スタティック NAT」または「スタティック PAT」の項目を参照してください。

PAT では単一のマッピング済みアドレスを使用できるため、ルーティング可能なアドレスを節約できます。FWSM 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することも可能です。PAT は、制御パスとデータ ストリームが異なるポートにある一部のマルチメディア アプリケーションでは機能しません。NAT と PAT のサポートの詳細については、P.21-2 の「NAT の概要」を参照してください。

（注） 変換が確立されている間、アクセスリストで許可されていれば、リモート　ホストは変換対象ホストへの接続を試みることができます。ポートのアドレス（実際のポートとマッピング済みポートの両方）を予測できないため、リモートホストが変換対象ホストに接続できる可能性は非常に低くなります。万一、接続が成功した場合でも、アクセスリストのセキュリティに頼ることができます。

スタティック NAT

スタティック NAT では、実際のアドレスからマッピング済みアドレスへの固定変換を行います。ダイナミック NAT および PAT では、ホストは以降の各変換で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、以降の接続でもマッピング済みアドレスは同一で、永続的な変換ルールが存在します。そのため、スタティック NAT では、宛先ネットワークのホストは変換対象ホストへのトラフィックを開始できます（アクセスリストでその接続が許可されている場合）。

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 ホストが変換対象ホストへの接続を開始できます（アクセスリストでその接続が許可されている場合）が、ダイナミック NAT の場合はそれができないという点です。また、スタティック NAT ではマッピング済みアドレスの数と実際のアドレスの数を同じにする必要があります。

スタティック PAT

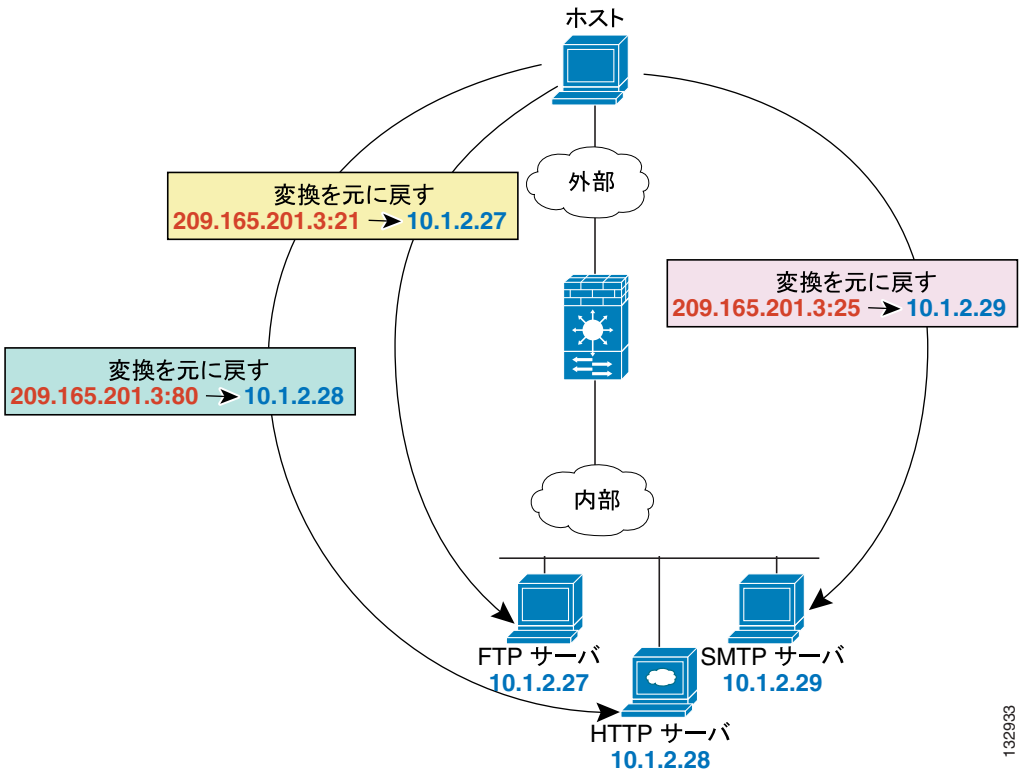
スタティック PAT は、実際のアドレスとマッピング済みアドレスに対してプロトコル（TCP または UDP）とポートを指定できること以外は、スタティック NAT と同じです。

この機能では、文ごとにポートが異なっていれば、多数の異なるスタティック文でマッピング済みアドレスを同じにすることができます（複数のスタティック *NAT* 文に対して同じマッピング済みアドレスを使用することはできません）。

セカンダリ チャネル（FTP、VoIP など）でアプリケーション検査が必要なアプリケーションの場合、FWSM 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、SMTP にアクセスするための単一アドレスをリモート ユーザに提供するが、実際のネットワーク上ではこれらが別のサーバである場合、使用するマッピング済みアドレスは同一だがポートは異なる各サーバに対してスタティック PAT 文を指定できます（図21-8 を参照）。

図 21-8　スタティック PAT



また、スタティック PAT を使用すると、ウェルノウン ポートと非標準ポートの変換が可能です。たとえば、内部 Web サーバでポート 8080 を使用している場合、外部ユーザにポート 80 への接続を許可してから、変換を元のポート 8080 に戻すことができます。同様に、セキュリティを強化したい場合、非標準のポート 6785 に接続するよう Web ユーザに通知してから、変換を元のポート 80 に戻すことができます。

NAT 制御がイネーブルの場合の NAT のバイパス

NAT 制御をイネーブルにすると、内部ホストは外部ホストへのアクセス時に NAT のルールと一致している必要があります。一部のホストに NAT を実行したくない場合、それらのホストで NAT をバイパスできます（または、NAT 制御をディセーブルにすることもできます）。たとえば、NAT をサポートしないアプリケーションを使用する場合、NAT をバイパスします（NAT をサポートしない検査エンジンの詳細については、P.21-2 の「NAT の概要」を参照してください）。

次の 3 つのいずれかの方法で、NAT をバイパスするようにトラフィックを設定できます。どの方法も検査エンジンとの互換性があります。ただし、それぞれの方法は次のように機能が若干異なります。

- アイデンティティ NAT：（ダイナミック NAT とよく似ている）アイデンティティ NAT を設定する場合、特定インターフェイスのホストに対して変換を制限するのではなく、すべてのインターフェイスの接続でアイデンティティ NAT を使用する必要があります。そのため、インターフェイス A にアクセスする場合は実際のアドレスで通常の変換を実行し、インターフェイス B にアクセスする場合はアイデンティティ NAT を使用するということはできません。一方、通常のダイナミック NAT では、アドレスを変換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 を使用する実際のアドレスが、アクセスリストで使用可能なすべてのネットワークでルーティング可能かどうか確認してください。

  アイデンティティ NAT の場合、マッピング済みアドレスが実際のアドレスと同じでも、（インターフェイス アクセスリストで許可されていても）外部から内部には接続を開始できません。外部から内部への接続には、スタティック アイデンティティ NAT または NAT 免除を使用します。
- 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、実際のアドレスを見せてもよいインターフェイスを指定できるので、インターフェイス A にアクセスする場合はアイデンティティ NAT を使用し、インターフェイス B にアクセスする場合は通常の変換を使用するということができます。また、スタティック アイデンティティ NAT では、ポリシー NAT を使用することもできます。ポリシー NAT では、変換する実際のアドレスを決定する際に、実際のアドレスと宛先アドレスを識別します（ポリシー NAT の詳細については、P.21-11 の「ポリシー NAT」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するときに、宛先がサーバ A の場合はスタティック アイデンティティ NAT を使用し、外部サーバ B にアクセスする場合は通常の変換を使用するということができます。
- NAT 免除：NAT 免除により、変換対象ホストとリモート 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、ホストの変換を特定のインターフェイスに制限するのではなく、すべてのインターフェイスの接続で NAT 免除を使用する必要があります。ただし、NAT 免除では、（ポリシー NAT と同様）変換する実際のアドレスを決定する際に実際のアドレスと宛先アドレスを指定できるので、NAT 免除を使用すると、より詳細な制御が可能になります。一方、ポリシー NAT とは異なり、NAT 免除ではアクセスリストでポートが考慮されません。

ポリシー NAT

ポリシー NAT では、拡張アクセスリストで送信元アドレスと宛先アドレスを指定することにより、アドレス変換に使用する実際のアドレスを識別します。また、送信元ポートと宛先ポートを指定することもできます。通常の NAT で考慮されるのは送信元アドレスのみで、宛先アドレスは考慮されません。たとえば、ポリシー NAT の場合、サーバ A にアクセスする場合は実際のアドレスをマッピング済みアドレス A に変換し、サーバ B にアクセスする場合は実際のアドレスをマッピング済みアドレス B に変換するということができます。

セカンダリ チャネル（FTP、VoIP など）でアプリケーション検査が必要なアプリケーションの場合、ポリシー NAT 文にセカンダリ ポートを指定する必要があります。ポートを予測できない場合は、ポリシーでセカンダリ チャネルの IP アドレスだけを指定する必要があります。この指定により、FWSM はセカンダリ ポートを変換します。

（注） NAT 免除以外のすべてのタイプの NAT で、ポリシー NAT がサポートされています。NAT 免除では、アクセスリストを使用して実際のアドレスを識別しますが、ポートを考慮しない点でポリシー NAT とは異なります。その他の違いについては、P.21-37 の「NAT 免除の使用」を参照してください。スタティック アイデンティティ NAT を使用しても、ポリシー NAT をサポートしているので NAT 免除と同じ結果が得られます。

図 21-9 に、2 つの異なるサーバにアクセスする 10.1.2.0/24 というネットワーク上のホストを示します。このホストが 209.165.201.11 のサーバにアクセスすると、実際のアドレスが 209.165.202.129 に変換されます。このホストが 209.165.200.225 のサーバにアクセスすると、実際のアドレスが 209.165.202 130 に変換されます。ホストがサーバと同じネットワーク上にあるように見えるので、ルーティングに役立ちます。

図 21-9　宛先アドレスが異なるポリシー NAT

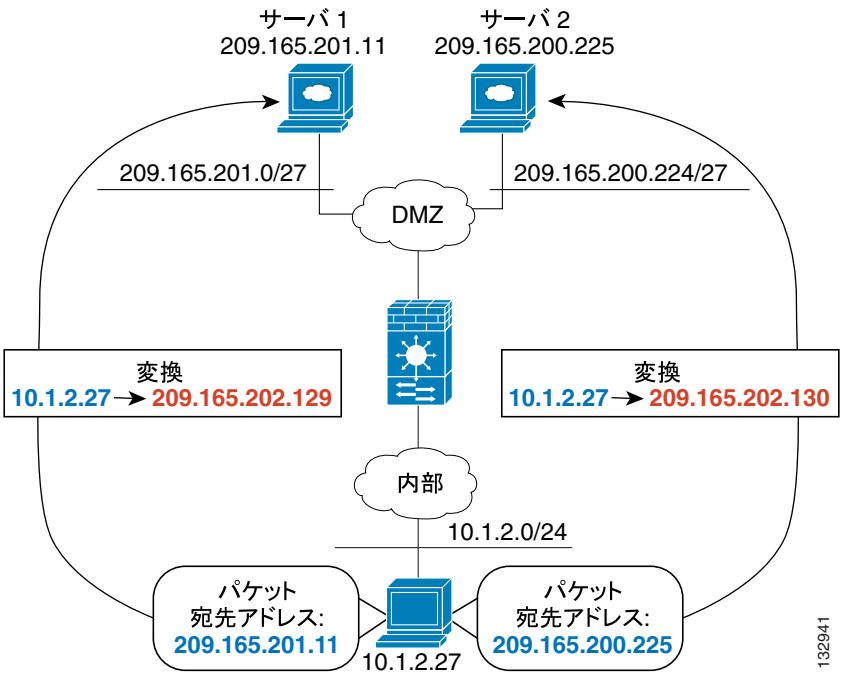
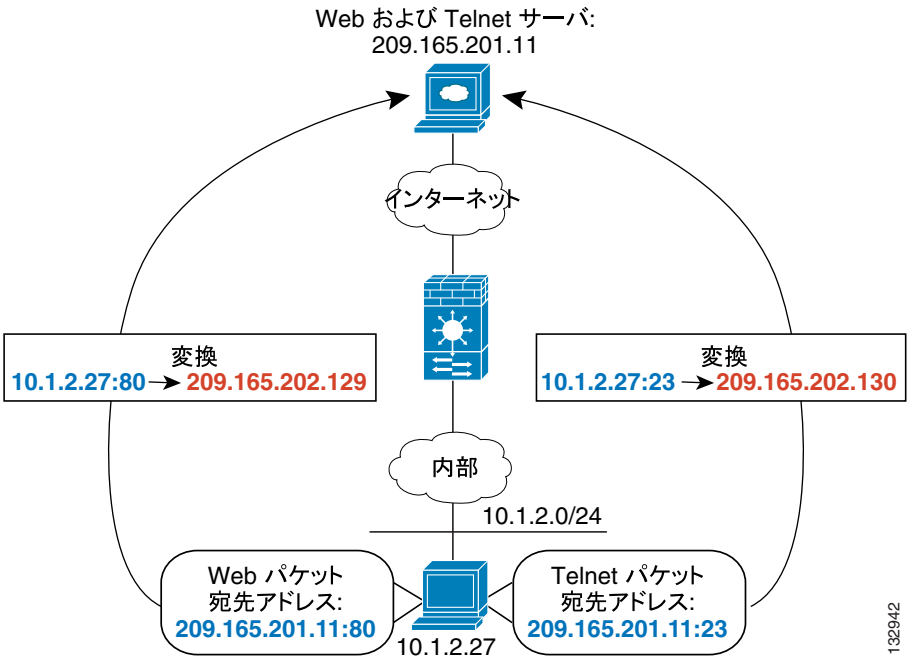


図 21-10 に、送信元と宛先のポートの使用例を示します。10.1.2.0/24 というネットワーク上にあるこのホストは、Web サービスと Telnet サービスの両方で同じホストにアクセスします。このホストが Web サービスのためにサーバにアクセスすると、実際のアドレスが 209.165.202.129 に変換されます。このホストが 同じサーバに Telnet サービスのためにアクセスすると、実際のアドレスが 209.165.202.130 に変換されます。

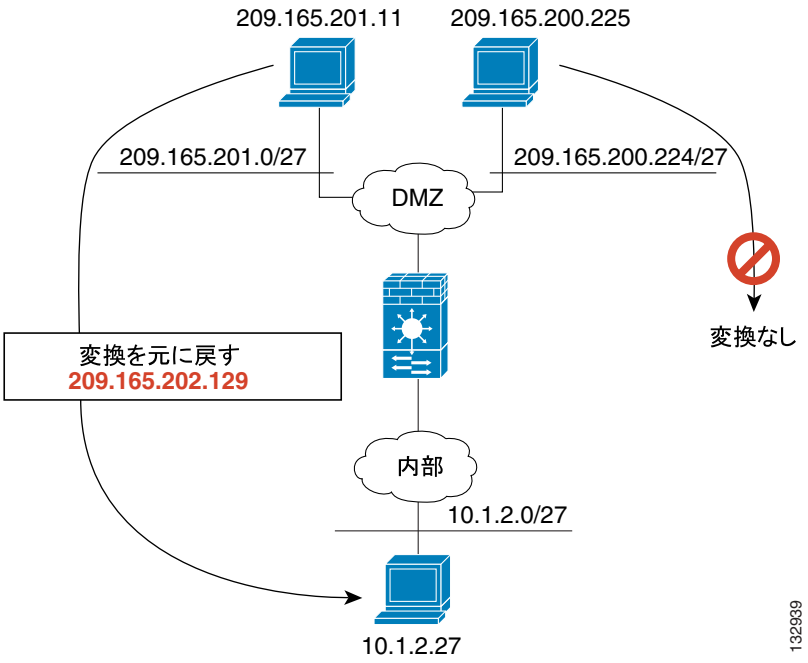
図 21-10　宛先ポートが異なるポリシー NAT



ポリシー スタティック NAT（および同様にアクセスリストを使用してトラフィックを識別する NAT 免除）の場合、変換対象ホストとリモート ホストの両方がトラフィックを発信できます。変換対象ネットワークから発信されるトラフィックの場合、NAT のアクセスリストで実際のアドレスと *宛先*アドレスを指定します。一方、リモート ネットワークから発信されるトラフィックの場合、実際のアドレスと、この変換によるホストへの接続が許可されているリモート ホストの *送信元*アドレスをアクセスリストで指定します。

図 21-11 に、変換対象ホストに接続するリモート ホストを示します。この変換対象ホストには、209.165.201.0/27 ネットワークとの送受信トラフィックだけについて、実際の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 ネットワークには、変換が設定されていないので、変換対象ホストはそのネットワークに接続できません。また、そのネットワークのホストも変換対象ホストに接続できません。

図 21-11　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 では SQL*Net がサポートされていませんが、通常の NAT ではサポートされています。他のプロトコルでの NAT のサポートについては、P.21-2 の「NAT の概要」を参照してください。

NAT セッション（Xlate）の作成

NAT を使用しない場合でも、デフォルトで FWSM がすべての接続に対して NAT セッションを作成します。たとえば、NAT 制御をイネーブルにしない場合、NAT 免除またはアイデンティティ NAT を使用する場合、またはセキュリティが等位のインターフェイスを使用しており NAT を設定しない場合でも、変換対象でない接続ごとに NAT セッションが作成されます。NAT セッションには最大数があるので（P.A-5 の「管理対象のシステム リソース」を参照）、これらの種類の NAT セッションにより制限に達してしまう場合があります。

このような制限に達するのを回避するために、変換対象でないトラフィックに対する NAT セッションをディセーブルにできます（xlate バイパスと呼ばれます）。xlate バイパスをイネーブルにする方法については、P.21-17 の「xlate バイパスのイネーブル」を参照してください。NAT 制御をディセーブルにして変換対象でないトラフィックを存在させる場合、または NAT 制御をイネーブルにして NAT 免除を使用する場合、xlate バイパスを使用すると、FWSM はこれらの変換対象でないトラフィックに対する NAT セッションを作成しません。ただし、次の場合は NAT セッションが作成されます。

- アイデンティティ NAT を設定する（NAT 制御がイネーブルまたはディセーブルの状態）。アイデンティティ NAT は変換と見なされます。
- NAT 制御でセキュリティが等位のインターフェイスを使用する。等位セキュリティのインターフェイス間のトラフィックの場合、そのトラフィックに対して NAT を設定しなくても NAT セッションが作成されます。このような場合に NAT セッションを回避するには、まず NAT 制御をディセーブルにするか、または NAT 免除を使用します。その上で xlate バイパスを使用します。

NAT およびセキュリティ レベルが等位のインターフェイス

セキュリティ レベルが等位のインターフェイス間では、NAT 制御をイネーブルにしている場合でも NAT は不要です。任意で NAT を設定することもできますが、必須ではありません。ただし、NAT 制御がイネーブルのときにダイナミック NAT を設定する場合、NAT は必須です。詳細については、P.21-5 の「NAT 制御」を参照してください。また、等位セキュリティのインターフェイスでダイナミック NAT または PAT の IP アドレス グループを指定する場合、そのアドレス グループが等位または下位のセキュリティ レベルのインターフェイスにアクセスする際に、（NAT 制御がイネーブルでない場合でも）そのアドレス グループに対して NAT を実行する必要があります。スタティック NAT として識別されるトラフィックは影響を受けません。

セキュリティが等位の通信をイネーブルにする方法については、P.5-3 の「等位セキュリティ レベル間の通信のイネーブル化」を参照してください。

（注） FWSM は、等位セキュリティのインターフェイスで NAT を設定する場合の VoIP 検査エンジンをサポートしていません。これらの検査エンジンには Skinny、SIP、H.323 などが含まれます。サポートされる検査エンジンについては、P.21-2 の「NAT の概要」を参照してください。

実際のアドレスの照合に使用する NAT ルールの順序

FWSM は、次の順序で実際のアドレスと NAT コマンドを照合します。

1. NAT 免除：最初の一致が見つかるまで順番に照合します。アイデンティティ NAT は、このカテゴリではなく通常のスタティック NAT または通常の NAT のカテゴリに含まれます。NAT 免除文でアドレスが重複すると予想外の結果が発生する場合があるため、お勧めできません。
2. スタティック NAT とスタティック PAT（通常およびポリシー）：最適な一致が見つかるまで照合します。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す。スタティック ルールでアドレスが重複する場合は警告が表示されますが、サポートされています。スタティック ルールの順序は関係なく、実際のアドレスと最も一致するスタティック ルールが使用されます。
3. ポリシー ダイナミック NAT：最初の一致が見つかるまで順番に照合されます。アドレスの重複は許可されています。
4. 通常のダイナミック NAT：最適な一致が見つかるまで照合されます。通常のアイデンティティ NAT はこのカテゴリに含まれます。NAT コマンドの順序は関係なく、実際のアドレスと最も一致する NAT 文が使用されます。たとえば、ある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。ユーザ ネットワークのサブセット（10.1.1.1）を別のアドレスに変換する場合、10.1.1.1 のみを変換する文を作成できます。10.1.1.1 の接続が開始されると、10.1.1.1 を指定した文が実際のアドレスと最も一致するので、この文が使用されます。重複文を使用するとメモリの使用量が増えて FWSM のパフォーマンスが低下する場合があるため、お勧めできません。

NAT 文の最大数

FWSM は、すべてのコンテキスト合計で、またはシングルモードで、次の数の **nat**、**global**、および **static** コマンドをサポートします。

- **nat** コマンド：2 K
- **global** コマンド：4 K
- **static** コマンド：2 K

また FWSM は、ポリシー NAT に使用するアクセスリストには、シングルモードで最大 3942 個、マルチモードで最大 7272 個の ACE をサポートします。

マッピング済みアドレスのガイドライン

実際のアドレスをマッピング済みアドレスに変換する場合、次のマッピング済みアドレスを使用できます。

- マッピング済みインターフェイスと同じネットワーク上にあるアドレス

  （トラフィックが FWSM から発信されるときに通過する）マッピング済みインターフェイスと同じネットワーク上にあるアドレスを使用すると、FWSM はプロキシ ARP を使用してマッピング済みアドレスへの要求に応答するので、実際のアドレス宛のトラフィックを代行受信します。同じネットワーク上のアドレスを使用すると、FWSM が追加ネットワークのゲートウェイである必要がないので、ルーティングが簡略化されます。ただし、同じネットワーク上のアドレスを使用すると、変換に使用できるアドレス数が制限されます。

  PAT の場合、マッピング済みインターフェイスの IP アドレスも使用できます。

- 一意のネットワーク上にあるアドレス

  マッピング済みインターフェイス のネットワークで使用できる数よりも多くのアドレスが必要な場合、別のサブネットにあるアドレスを指定できます。FWSM は、プロキシ ARP を使用してマッピング済みアドレスの要求に応答するので、実際のアドレス宛のトラフィックを代行受信します。OSPF を使用してマッピング済みインターフェイスのルートをアドバタイズする場合、FWSM はマッピング済みアドレスをアドバタイズします。マッピング済み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場合）、またはスタティック ルーティングを使用する場合、マッピング済みアドレス宛のトラフィックを FWSM に送信するスタティック ルートをアップストリーム ルータで追加する必要があります。

DNS と NAT

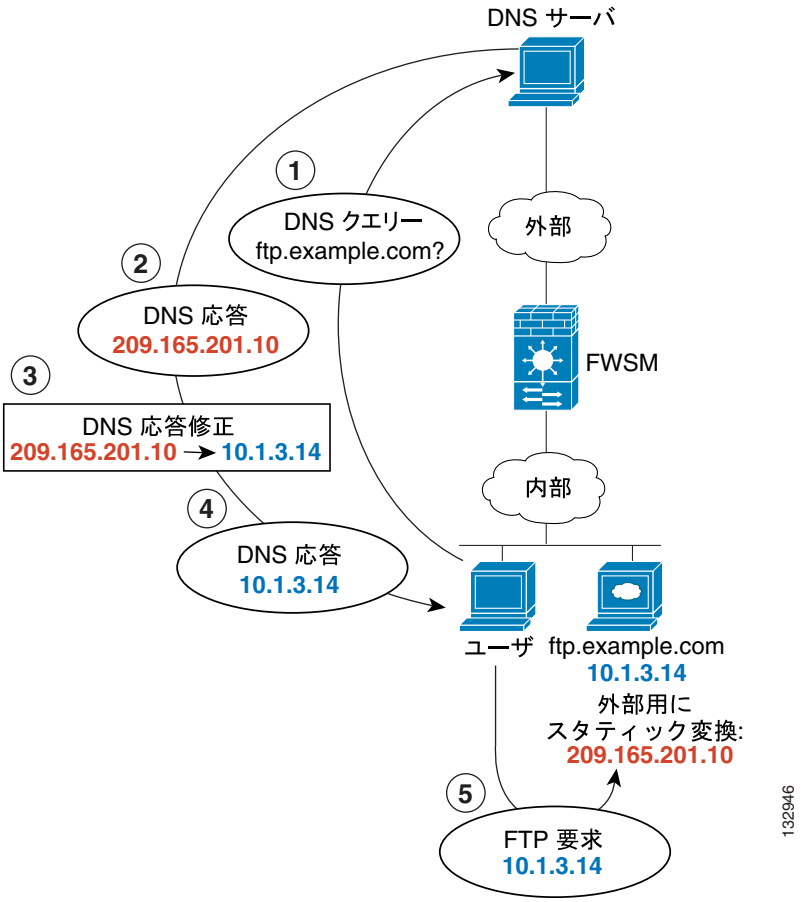
DNS 応答の修正を行うよう FWSM を設定する必要がある場合があります。修正では、NAT コンフィギュレーションと一致するアドレスに DNS 応答内のアドレスが置換されます。DNS の修正は、各変換の設定時に設定できます。

たとえば、DNS サーバに外部インターフェイスからアクセスできるとします。サーバ ftp.example.com は内部インターフェイスに接続されているとします。ftp.example.com の実際のアドレス（10.1.3.14）を、外部ネットワークから見えるマッピング済みアドレス（209.165.201.10）へスタティックに変換するように FWSM を設定できます（図 21-12 を参照）。この場合、このスタティック文で DNS 応答の修正をイネーブルにできます。DNS 応答の修正をイネーブルにすると、実際のアドレスを使用して ftp.example.com にアクセスする内部ユーザが、DNS サーバからマッピング済みアドレスではなく実際のアドレスを受信できるようになります。

内部ホストが ftp.example.com のアドレスに対して DNS 要求を送信すると、DNS サーバはマッピング済みアドレス（209.165.201.10）で応答します。FWSM は内部サーバのスタティック文を参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答の修正をイネーブルにしないと、内部ホストは ftp.example.com へ直接アクセスせずに、トラフィックを 209.165.201.10 へ送信しようとします。

（注） DNS クエリーの応答内に記述されている実際の IP アドレスへのルートが存在している必要があります。存在しない場合、FWSM はその IP アドレスへの NAT を実行しません。必要なルートは、スタティック ルーティングまたは RIP や OSPF など他のルーティング プロトコルからラーニングできます。

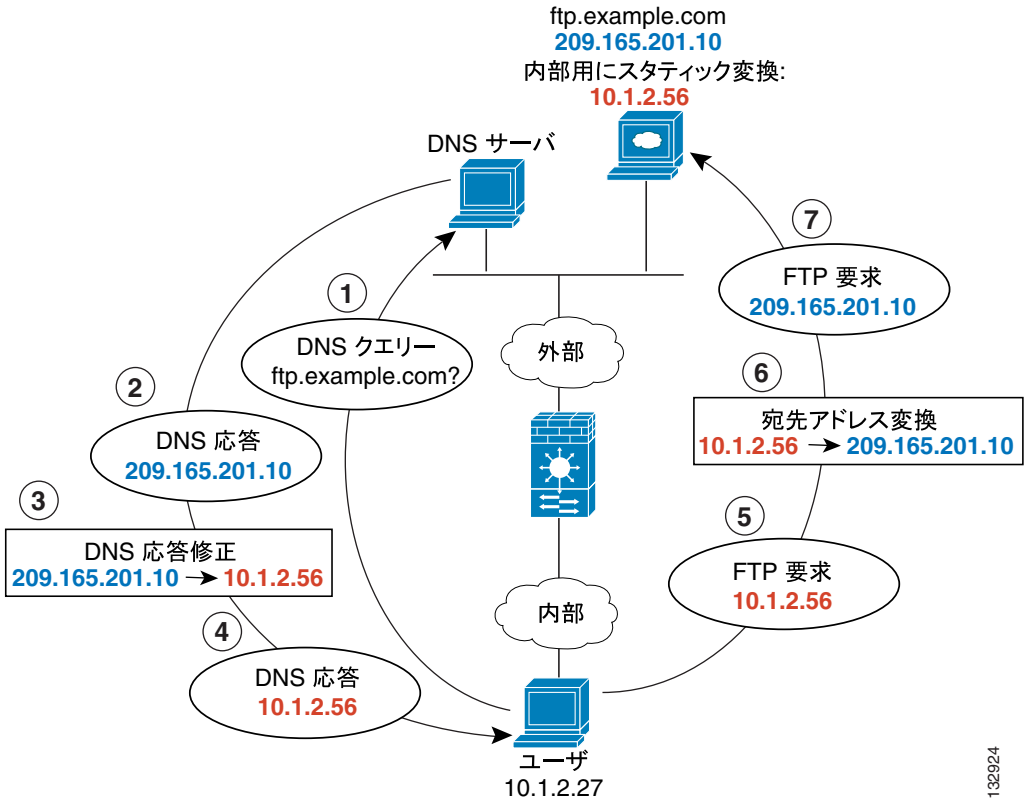
図 21-12　DNS 応答の変更



（注） 別のネットワーク（DMZ など）上のユーザが外部の DNS サーバに ftp.example.com の IP アドレスを要求した場合も、**static** コマンドで参照した内部インターフェイスにそのユーザが接続されていなくても、DNS 応答内の IP アドレスがそのユーザ用に変更されます。

図 21-13 に、外部の Web サーバと DNS サーバを示します。FWSM には外部サーバのスタティック変換があります。この場合、内部ユーザが DNS サーバから ftp.example.com のアドレスを要求すると、DNS サーバは実際のアドレス 209.165.201.10 で応答します。内部ユーザに ftp.example.com のマッピング済みアドレス（10.1.2.56）を使用させたい場合、そのスタティック変換用の DNS 応答の修正を設定する必要があります。

図 21-13　外部 NAT を使用した DNS 応答の修正



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通過するパケットが NAT のルールと一致している必要があります。詳細については、P.21-5 の「NAT 制御」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** チェックボックスをオンにします。

xlate バイパスのイネーブル

デフォルトでは、NAT を使用しない場合でも、FWSM がすべての接続に対して NAT セッションを作成します。詳細については、P.21-13 の「NAT セッション（Xlate）の作成」を参照してください。

xlate バイパスをイネーブルにするには、Configuration > Firewall > NAT Rules ペインで **Enable Xlate-bypass** チェックボックスをオンにします。

ダイナミック NAT の使用

この項では、ダイナミック NAT、ダイナミック PAT、ダイナミック ポリシー NAT/PAT、およびアイデンティティ NAT の設定方法について説明します。

ポリシー NAT では、送信元アドレスと宛先アドレスを指定することにより、アドレス変換を行う実際のアドレスを識別します。また、送信元ポートと宛先ポートを指定することもできます。通常の NAT で考慮されるのは送信元アドレスのみで、宛先アドレスは考慮されません。詳細については、P.21-11 の「ポリシー NAT」を参照してください。

ここでは、次の項目について説明します。

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。次の項目を取り上げます。

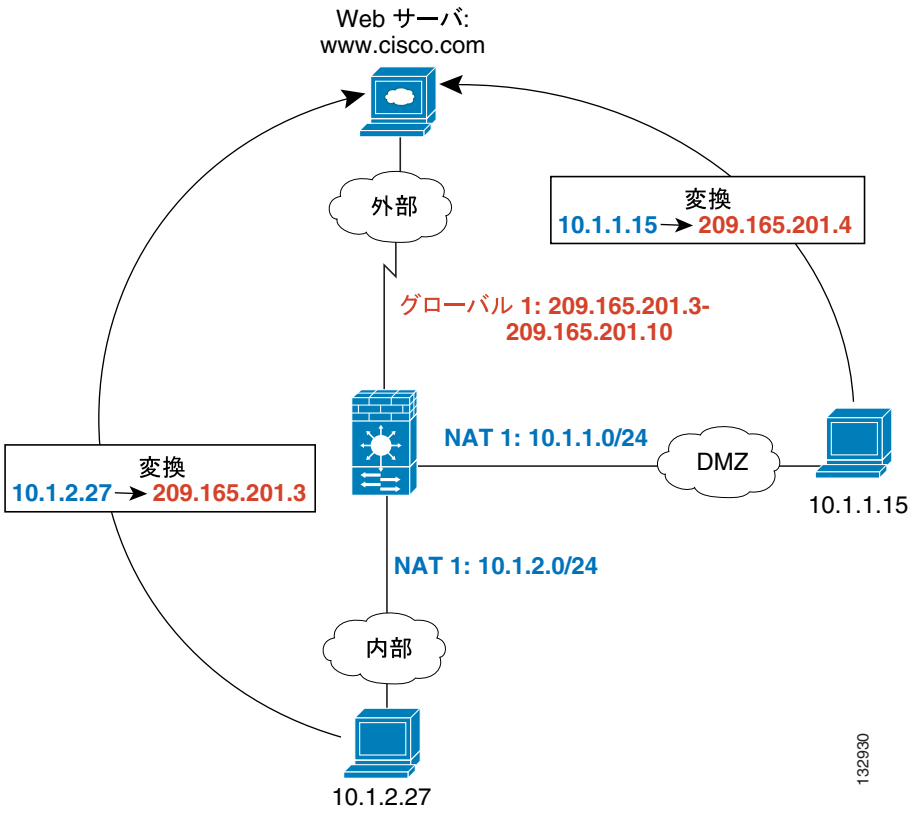
プール ID による実際のアドレスとグローバル プールの組み合せ

ダイナミック NAT ルールでは、実際のアドレスを指定してから、それを複数のアドレスから成るグローバル プールと組み合せます（ただし、PAT の場合は 1 つのアドレスを組み合わせに指定し、アイデンティティ NAT の場合は実際のアドレスと同一のアドレスを組み合わせに指定します）。実際のアドレスのトラフィックが別のインターフェイスから出るときに、組み合せに指定されたグローバル プールのアドレスに実際のアドレスがマッピングされます。各グローバル プールには個別のプール ID が割り当てられます。

同一グローバル プールによる複数インターフェイス上の 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、外部インターフェイスのグローバル プール 1 を使用して、内部インターフェイスと DMZ インターフェイスに 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、マッピング済みプールまたは PAT アドレスを共有します（図 21-14 を参照）。

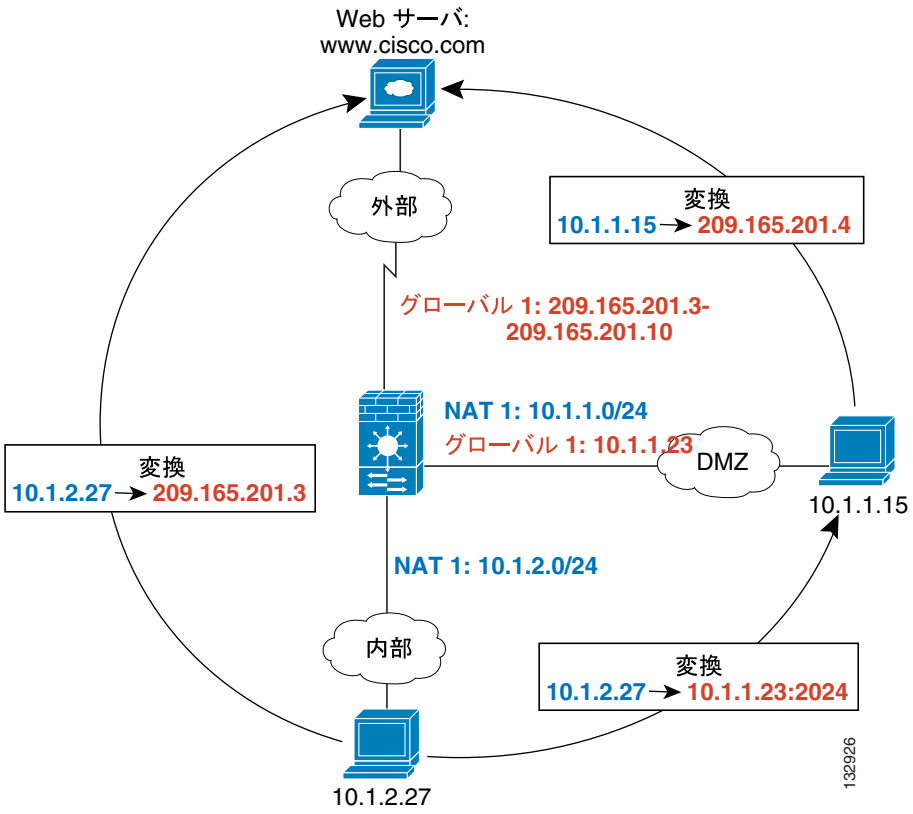
図 21-14　同一グローバル プールを使用する複数インターフェイス上の NAT ルール



同一プール ID による異なるインターフェイス上のグローバル プール

同じプール ID を使用するグローバル プールを各インターフェイスに作成できます。外部インターフェイスと DMZ インターフェイスに ID 1 のグローバル プールを作成すると、ID 1 に関連付けられた単一の NAT ルールにより、トラフィックが外部インターフェイスと DMZ インターフェイスへ向かう際に、変換されるトラフィックが識別されます。同様に、DMZ インターフェイスに対する ID 1 の NAT ルールを作成すると、ID 1 のすべてのグローバル プールが DMZ のトラフィックに使用されます（図 21-15 を参照）。

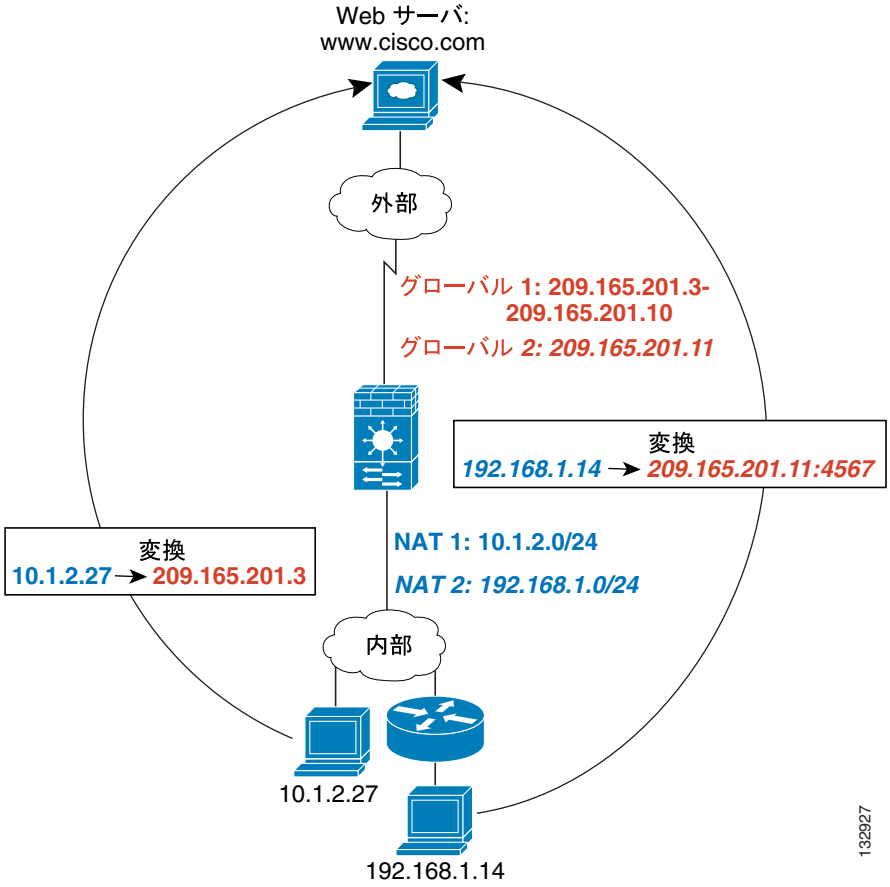
図 21-15　複数のインターフェイスで同じ ID を使用する NAT ルールとグローバル プール



同一インターフェイス上の異なるグローバル プールによる複数の NAT ルール

実際のアドレスの複数のグループを区別して、別々のマッピング済みアドレスを指定できます。たとえば、内部インターフェイスで、2 つの異なるプール ID で 2 つの NAT ルールを指定できます。外部インターフェイスでは、これら 2 つの ID に対してグローバル プールを 2 つ設定します。次に、内部ネットワーク A のトラフィックが外部インターフェイスを出る場合、IP アドレスはプール 1 のアドレスに変換されます。一方、内部ネットワーク B 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 21-16 を参照）。ポリシー NAT を使用する場合、宛先アドレスおよびポートがアクセスリストごとに一意であれば、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。

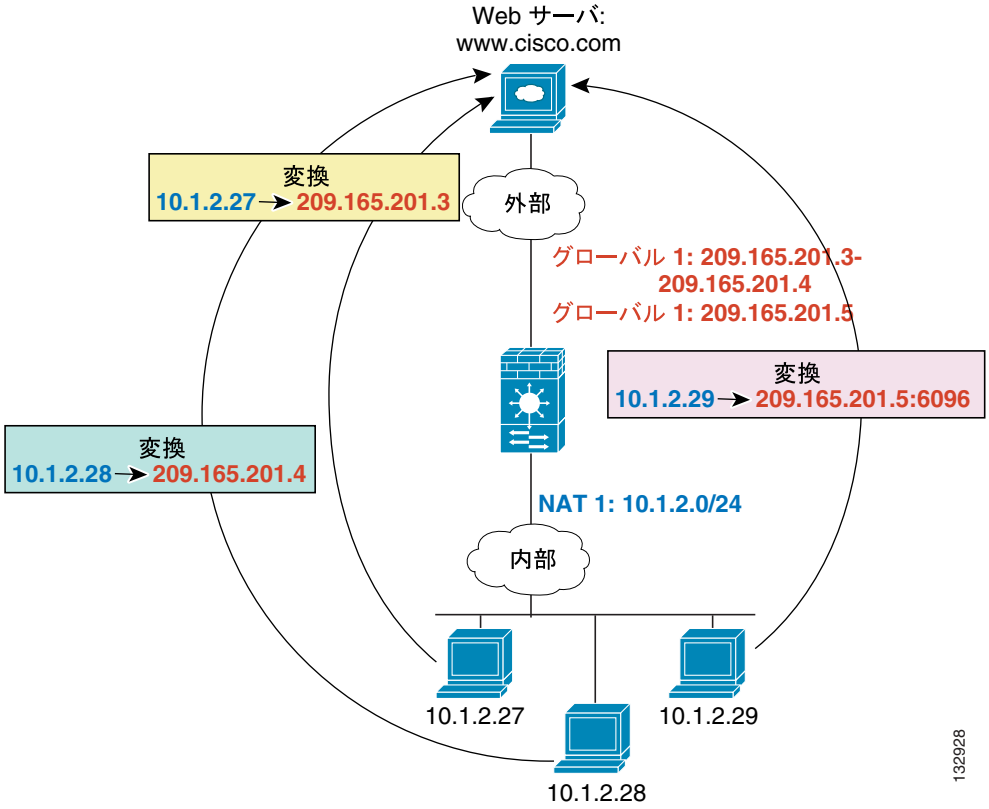
図 21-16　異なる NAT ID



同一グローバル プールの複数のアドレス

同一のグローバル プールで複数のアドレスを指定できます。FWSM は、設定されている順序でダイナミック NAT の範囲内のアドレスを使用してから、PAT の単一アドレスを順番に使用します。たとえば、特定のアプリケーションでダイナミック NAT を使用する必要があるが、ダイナミック NAT のアドレスが不足した場合に備えてバックアップ PAT ルールを用意したい場合、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 マッピング済みアドレスでサポートされる約 64,000 の PAT セッションよりも多くのアドレスが必要な場合は、プールで 2 つの PAT アドレスを使用できます（図 21-17 を参照）。

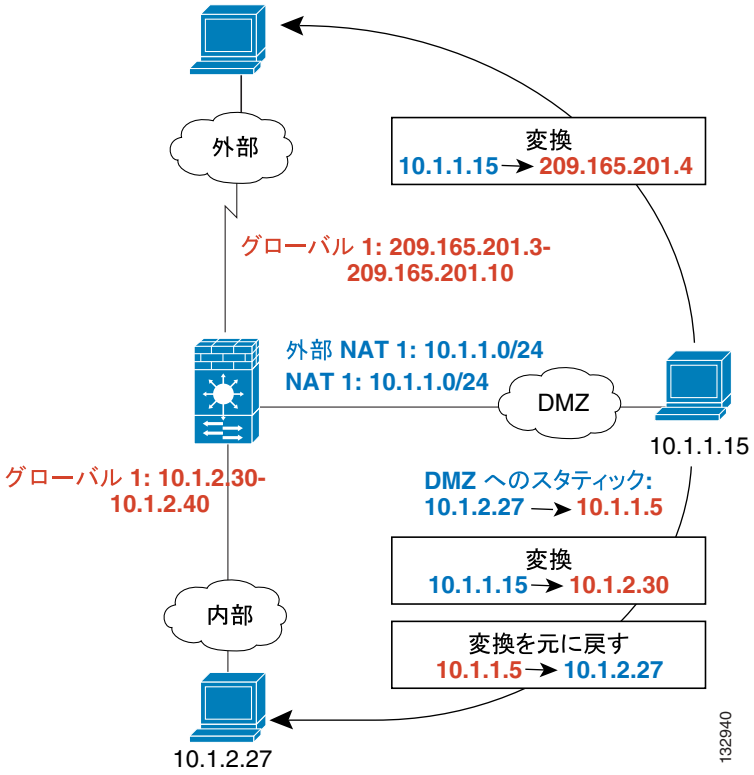
図 21-17　NAT と PAT の併用



外部 NAT

NAT ルールにより外部インターフェイスから内部インターフェイスにアドレスを変換する場合、そのルールは外部 NAT となるので、着信トラフィックを変換するように指定する必要があります。また、下位のセキュリティ インターフェイスにアクセスする際にも同じトラフィックを変換する場合（たとえば、内部インターフェイスと外部インターフェイスにアクセスする際に DMZ のトラフィックが変換される場合）、同じ NAT ID を使用する 2 番目の NAT ルールを作成できますが（図 21-18 を参照）、発信であることを指定する必要があります。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ため、送信元と宛先の両方のアドレスが変換されます。

図 21-18　外部 NAT と内部 NAT の組み合せ



NAT ルールの実際のアドレスをすべての下位または等位のセキュリティ インターフェイス上で変換する必要性

IP アドレス グループに対して NAT ルールを作成する場合、下位または等位のセキュリティ レベルのインターフェイスにアクセスする際にそのアドレス グループに NAT を実行する必要があります。同じプール ID を持つグローバル プールを各インターフェイスに作成するか、またはスタティック ルールを使用する必要があります。上位のセキュリティ インターフェイスにアクセスする場合は、NAT は不要です。外部 NAT ルールを作成すると、すべての上位セキュリティ インターフェイスにアクセスする際に、そのアドレス グループに対する前述の NAT の条件が適用されます。スタティック ルールにより識別される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 では、グローバル プールを使用して変換を行います。グローバル プールの仕組みについては、P.21-18 の「ダイナミック NAT の実装」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、またはプールを選択してから **Edit** をクリックします。

また、**Manage** ボタンをクリックすると、Add/Edit Dynamic NAT Rule ダイアログボックスからもグローバル 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　新規プールの場合、Interface ドロップダウン リストからマッピング済み 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　新規プールの場合、Pool ID フィールドに 1 ～ 2147483647 の数値を入力します。使用中のプール ID を入力すると、コンフィギュレーションが拒否されます。

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、FWSM はダイナミック NAT を実行します。Netmask フィールドでサブネット マスクを指定すると、その値により、ホストに割り当てられる際にマッピング済みアドレスに割り当てられるサブネット マスクが決まります。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。

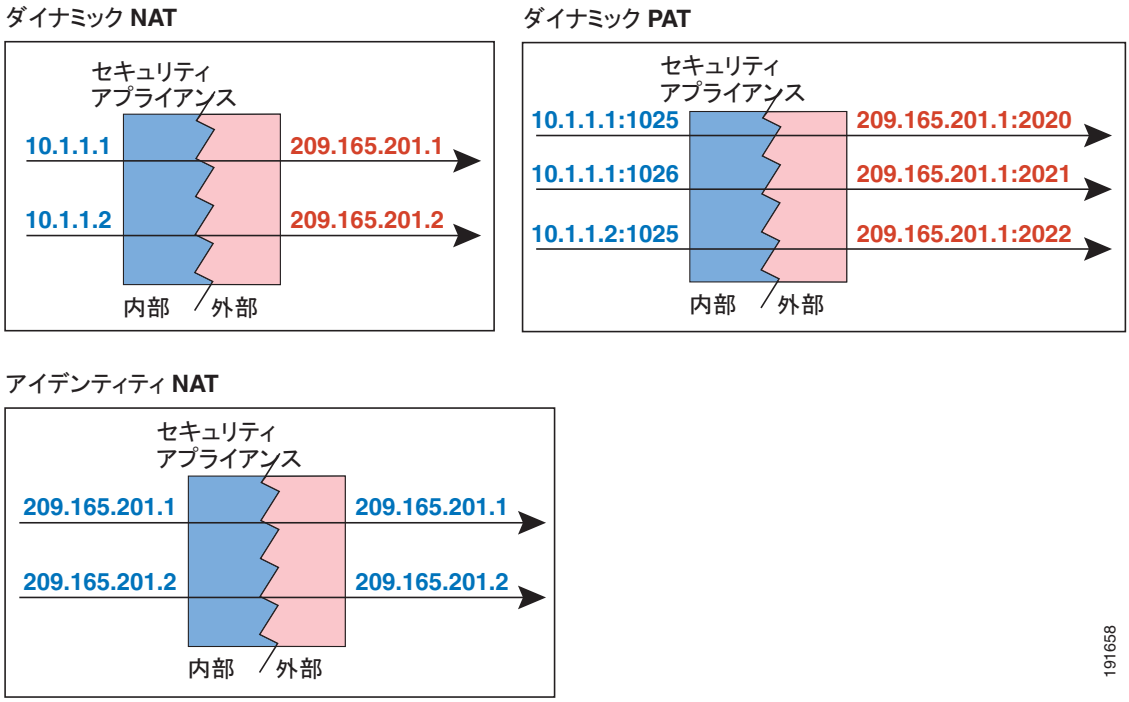
ステップ 6　（オプション）複数のアドレスをグローバル プールに追加できます。たとえば、ダイナミックな範囲を設定した後に PAT アドレスを追加する場合、PAT の値を入力してから再度 **Add** をクリックします。インターフェイスで同じプール ID のアドレスを複数使用する方法については、P.21-22 の「同一グローバル プールの複数のアドレス」を参照してください。

ステップ 7　**OK** をクリックします。

ダイナミック NAT、PAT、またはアイデンティティ NAT の設定

図 21-19 に、一般的なダイナミック NAT、ダイナミック PAT、およびアイデンティティ NAT のシナリオを示します。接続を開始できるのは実際のホストのみです。

図 21-19　ダイナミック NAT のシナリオ



ダイナミック NAT、ダイナミック PAT、またはアイデンティティ 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 領域の Interface ドロップダウン リストから、変換する実際のアドレスを持つホストに接続され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するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト 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。

- 定義済みのグローバル プールを選択します。

プールにアドレスの範囲を含めると、FWSM はダイナミック NAT を実行します。プールに単一のアドレスを含めると、FWSM はダイナミック PAT を実行します。プールに範囲と単一アドレスの両方を含めると、範囲が順番に使用されてから PAT アドレスが順番に使用されます。詳細については、P.21-22 の「同一グローバル プールの複数のアドレス」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 を共有している場合、それらはグループ化されます。複数のインターフェイスにかかるプール ID を選択すると、トラフィックは、プール内のインターフェイスにアクセスする際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、P.21-18 の「ダイナミック NAT の実装」を参照してください。

- 新しいグローバル プールを作成、または既存のプールを編集するには、**Manage** をクリックします。P.21-24 の「グローバル プールの管理」を参照してください。
- アイデンティティ NAT を選択するには、プール 0 を選択します。

ステップ 5　（オプション）DNS 応答内のアドレス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** チェックボックスをオンにします。

DNS サーバにエントリがあるホストの実際のアドレスを NAT ルールに指定するが、DNS サーバはクライアントとは別のインターフェイスにある場合、クライアントと DNS サーバではホストのアドレスとして別々のアドレスが必要となります。クライアントではマッピング済みアドレスが必要で、DNS サーバでは実際のアドレスが必要です。このオプションをイネーブルにすると、クライアントへの DNS 応答内のアドレスが修正されます。マッピング済みホストは、クライアントか DNS サーバのどちらかと同じインターフェイスになければなりません。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で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 ルールで使用する場合が多くなります。詳細については、P.21-15 の「DNS と NAT」を参照してください。

ステップ 6　（オプション）接続の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、次のいずれかのオプション（複数可）を設定します。

（注）　セキュリティ ポリシー ルールを使用してこれらの値の一部を設定することもできます（P.23-3 の「Connection Settings（透過モードのみ）」を参照）。両方で値の設定を行うと、FWSM は小さい値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、FWSM 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）、FWSM は TCP パケットのシーケンス番号をランダム化します。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。FWSM は、発信方向と着信方向の両方を通過する TCP SYN の ISN をランダム化します。

  保護されたホストの ISN をランダム化すると、攻撃者が新しい接続の次の ISN を予測できなくなり、新しいセッションを乗っ取ることができなくなります。

  必要に応じて TCP 初期シーケンス番号のランダム化をディセーブルにできます。次の例を参考にしてください。

  — 別のインライン ファイアウォールでも初期シーケンス番号をランダム化している場合。このアクションがトラフィックに影響しない場合でも、両方のファイアウォールが共にこのアクションを実行する必要はありません。

  — FWSM を経由して eBGP マルチホップを使用し、eBGP ピアで MD5 を使用する場合。ランダム化により MD5 チェックサムが中断されます。

— FWSM が接続のシーケンス番号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。

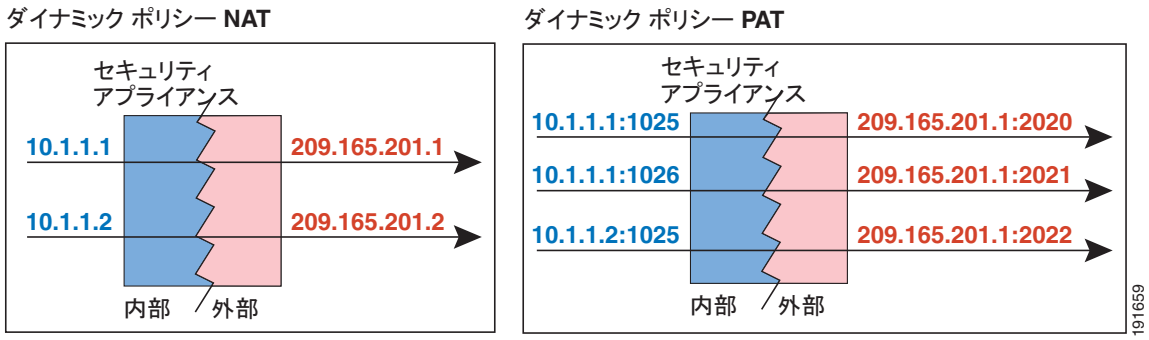
- **Maximum TCP Connections**：TCP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum UDP Connections**：UDP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum Embryonic Connections**：初期接続のホストごとの最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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 PAT の設定

図 21-20 に、一般的なダイナミック ポリシー NAT と PAT のシナリオを示します。接続を開始できるのは実際のホストのみです。

図 21-20　ダイナミック ポリシー NAT のシナリオ



ダイナミック ポリシー NAT または 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表示されます。

ステップ 2　Original 領域の Interface ドロップダウン リストから、変換する実際のアドレスを持つホストに接続され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するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

複数の実際のアドレス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するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

複数の宛先アドレスはカンマで区切ります。

デフォルトでは、この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。

- 定義済みのグローバル プールを選択します。

  プールにアドレスの範囲を含めると、FWSM はダイナミック NAT を実行します。プールに単一のアドレスを含めると、FWSM はダイナミック PAT を実行します。プールに範囲と単一アドレスの両方を含めると、範囲が順番に使用されてから PAT アドレスが順番に使用されます。詳細については、P.21-22 の「同一グローバル プールの複数のアドレス」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 を共有している場合、それらはグループ化されます。複数のインターフェイスにかかるプール ID を選択すると、トラフィックは、プール内のインターフェイスにアクセスする際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、P.21-18 の「ダイナミック NAT の実装」を参照してください。
- 新しいグローバル プールを作成、または既存のプールを編集するには、**Manage** をクリックします。P.21-24 の「グローバル プールの管理」を参照してください。
- アイデンティティ NAT を選択するには、プール 0 を選択します。

ステップ 6　（オプション）Description フィールドに説明を入力します。

ステップ 7　（オプション）DNS 応答内のアドレス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** チェックボックスをオンにします。

DNS サーバにエントリがあるホストの実際のアドレスを NAT ルールに指定するが、DNS サーバはクライアントとは別のインターフェイスにある場合、クライアントと DNS サーバではホストのアドレスとして別々のアドレスが必要となります。クライアントではマッピング済みアドレスが必要で、DNS サーバでは実際のアドレスが必要です。このオプションをイネーブルにすると、クライアントへの DNS 応答内のアドレスが修正されます。マッピング済みホストは、クライアントか DNS サーバのどちらかと同じインターフェイスになければなりません。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で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 ルールで使用する場合が多くなります。詳細については、P.21-15 の「DNS と NAT」を参照してください。

ステップ 8　（オプション）接続の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、次のいずれかのオプション（複数可）を設定します。

（注）　セキュリティ ポリシー ルールを使用してこれらの値の一部を設定することもできます（P.23-3 の「Connection Settings（透過モードのみ）」を参照）。両方で値の設定を行うと、FWSM は小さい値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、FWSM 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）、FWSM は TCP パケットのシーケンス番号をランダム化します。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。FWSM は、発信方向と着信方向の両方を通過する TCP SYN の ISN をランダム化します。

  保護されたホストの ISN をランダム化すると、攻撃者が新しい接続の次の ISN を予測できなくなり、新しいセッションを乗っ取ることができなくなります。

  必要に応じて TCP 初期シーケンス番号のランダム化をディセーブルにできます。次の例を参考にしてください。

  - 別のインライン ファイアウォールでも初期シーケンス番号をランダム化している場合。このアクションがトラフィックに影響しない場合でも、両方のファイアウォールが共にこのアクションを実行する必要はありません。
  - FWSM を経由して eBGP マルチホップを使用し、eBGP ピアで MD5 を使用する場合。ランダム化により MD5 チェックサムが中断されます。
  - FWSM が接続のシーケンス番号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 接続の最大数を 0 ～ 65,535 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 接続の最大数を 0 ～ 65,535 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**：初期接続のホストごとの最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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、通常またはポリシー スタティック NAT、PAT、またはアイデンティティ NAT を使用するスタティック変換の設定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、P.21-8 の「スタティック NAT」を参照してください。

ポリシー NAT では、送信元アドレスと宛先アドレスを指定することにより、アドレス変換に使用する実際のアドレスを識別します。また、送信元ポートと宛先ポートを指定することもできます。通常の NAT で考慮されるのは送信元アドレスのみで、宛先アドレスは考慮されません。詳細については、P.21-11 の「ポリシー NAT」を参照してください。

スタティック PAT では、実際の IP アドレスをマッピング済み IP アドレスに変換し、実際のポートをマッピング済みポートに変換します。実際のポートを同じポートに変換することもできます。この場合、指定した種類のトラフィックのみを変換するか、別のポートに変換することでさらに変換を実行することもできます。セカンダリ チャネル（FTP、VoIP など）でアプリケーション検査が必要なアプリケーションの場合、FWSM 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、P.21-9 の「スタティック PAT」を参照してください。

スタティック PAT を使用している場合を除き、同じ 2 つのインターフェイス間で複数のスタティック ルールに同一の実際のアドレスまたはマッピング済みアドレスを使用することはできません。同じマッピング済みインターフェイスのグローバル プールで定義されているマッピング済み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。

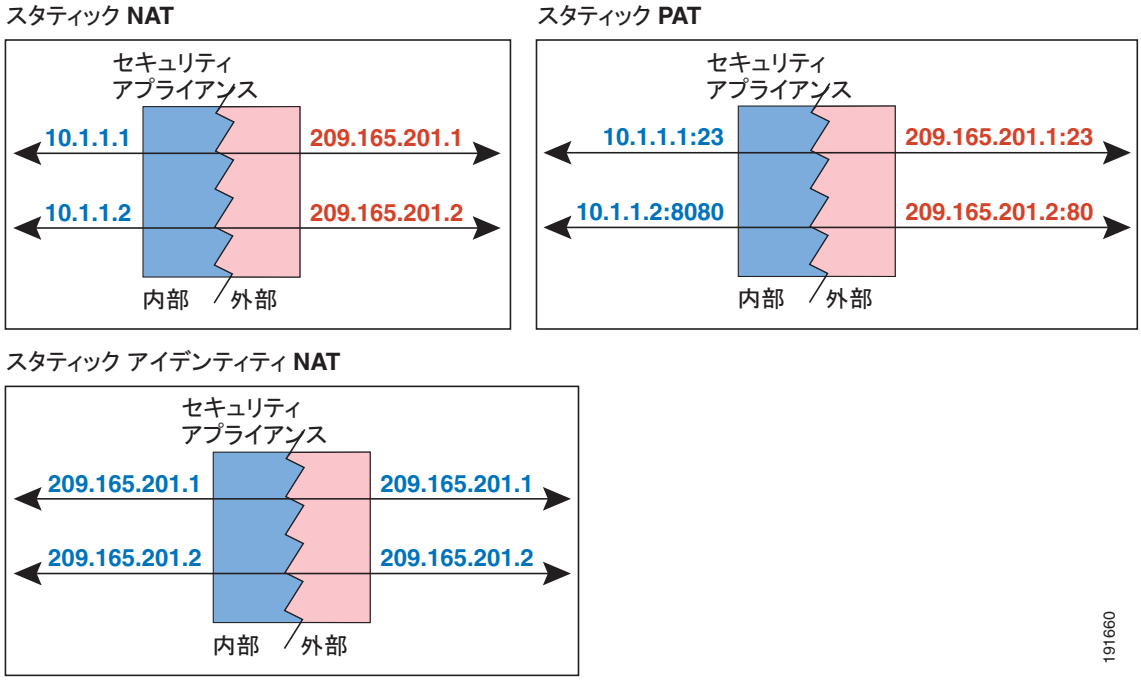
スタティック アイデンティティ NAT は、実際の IP アドレスを同じ IP アドレスに変換します。

ここでは、次の項目について説明します。

スタティック NAT、PAT、またはアイデンティティ NAT の設定

図 21-21 に、一般的なスタティック NAT、スタティック PAT、およびスタティック アイデンティティ NAT のシナリオを示します。変換は常にアクティブなので、変換対象ホストとリモート ホストの両方が接続を開始できます。

図 21-21　スタティック NAT のシナリオ



スタティック NAT、スタティック PAT、またはアイデンティティ 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 領域の Interface ドロップダウン リストから、変換する実際のアドレスを持つホストに接続され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するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

ステップ 4　Translated 領域の Interface ドロップダウン リストから、マッピング済み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　次のいずれかをクリックしてマッピング済み IP アドレスを指定します。

- **Use IP Address**

  IP アドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

  10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト 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済みアドレスのサブネット マスクが同じでなければなりません。

（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　（オプション）スタティック PAT を使用する場合、**Enable Port Address Translation (PAT)** チェックボックスをオンにします。

a.　Protocol で **TCP** または **UDP** をクリックします。

b.　Original Port フィールドに実際のポート番号を入力します。

c.　Translated Port フィールドにマッピング済みポート番号を入力します。

ステップ 7　（オプション）DNS 応答内のアドレス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** チェックボックスをオンにします。

DNS サーバにエントリがあるホストの実際のアドレスを NAT ルールに指定するが、DNS サーバはクライアントとは別のインターフェイスにある場合、クライアントと DNS サーバではホストのアドレスとして別々のアドレスが必要となります。クライアントではマッピング済みアドレスが必要で、DNS サーバでは実際のアドレスが必要です。このオプションをイネーブルにすると、クライアントへの DNS 応答内のアドレスが修正されます。マッピング済みホストは、クライアントか DNS サーバのどちらかと同じインターフェイスになければなりません。詳細については、P.21-15 の「DNS と NAT」を参照してください。

ステップ 8　（オプション）接続の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、次のいずれかのオプション（複数可）を設定します。

（注）　セキュリティ ポリシー ルールを使用してこれらの値の一部を設定することもできます（P.23-3 の「Connection Settings（透過モードのみ）」を参照）。両方で値の設定を行うと、FWSM は小さい値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、FWSM 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）、FWSM は TCP パケットのシーケンス番号をランダム化します。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。FWSM は、発信方向と着信方向の両方を通過する TCP SYN の ISN をランダム化します。

保護されたホストの ISN をランダム化すると、攻撃者が新しい接続の次の ISN を予測できなくなり、新しいセッションを乗っ取ることができなくなります。

必要に応じて TCP 初期シーケンス番号のランダム化をディセーブルにできます。次の例を参考にしてください。

- 別のインライン ファイアウォールでも初期シーケンス番号をランダム化している場合。このアクションがトラフィックに影響しない場合でも、両方のファイアウォールが共にこのアクションを実行する必要はありません。
- FWSM を経由して eBGP マルチホップを使用し、eBGP ピアで MD5 を使用する場合。ランダム化により MD5 チェックサムが中断されます。
- FWSM が接続のシーケンス番号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。

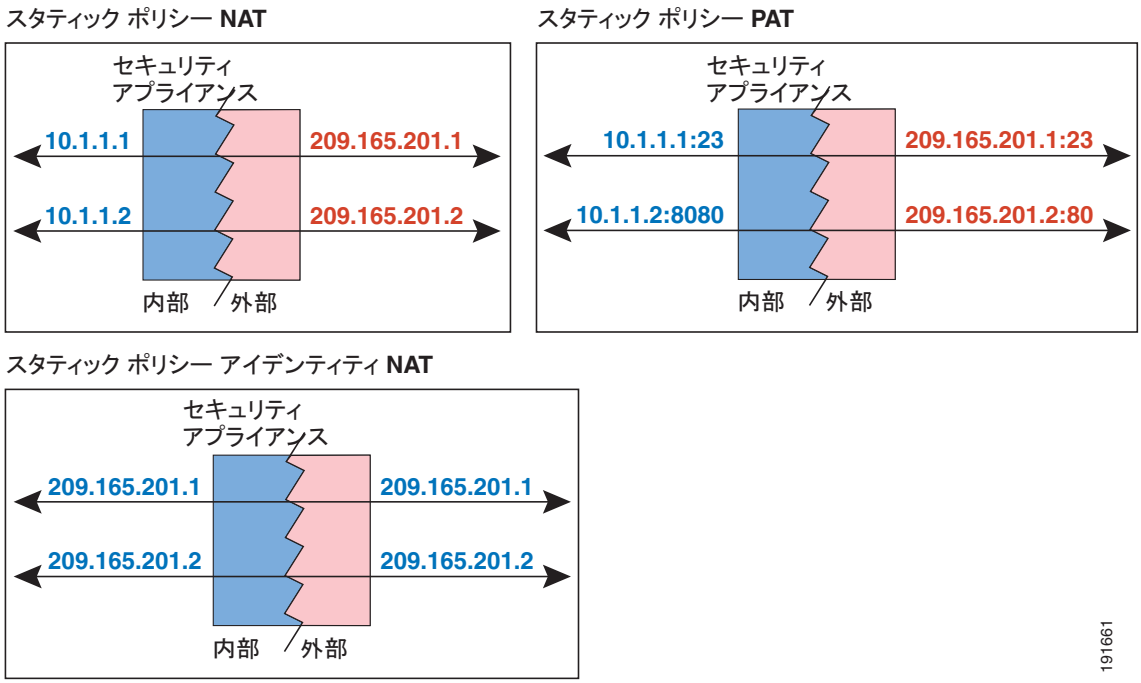
- **Maximum TCP Connections**：TCP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum UDP Connections**：UDP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum Embryonic Connections**：初期接続のホストごとの最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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、PAT、またはアイデンティティ NAT の設定

図 21-22 に、一般的なスタティック ポリシー NAT、スタティック ポリシー PAT、およびスタティック ポリシー アイデンティティ NAT のシナリオを示します。変換は常にアクティブなので、変換対象ホストとリモート ホストの両方が接続を開始できます。

図 21-22　スタティック ポリシー NAT のシナリオ



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 領域の Interface ドロップダウン リストから、変換する実際のアドレスを持つホストに接続され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するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト 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するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

複数の宛先アドレスはカンマで区切ります。

デフォルトでは、この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済み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　次のいずれかをクリックしてマッピング済み IP アドレスを指定します。

- **Use IP Address**

  IP アドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

  10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト 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済みアドレスのサブネット マスクが同じでなければなりません。

ステップ 7　（オプション）スタティック PAT を使用する場合、**Enable Port Address Translation (PAT)** チェックボックスをオンにします。

a.　Protocol で **TCP** または **UDP** をクリックします。

b.　Original Port フィールドに実際のポート番号を入力します。

c.　Translated Port フィールドにマッピング済みポート番号を入力します。

ステップ 8　（オプション）Description フィールドに説明を入力します。

ステップ 9　（オプション）DNS 応答内のアドレス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** チェックボックスをオンにします。

DNS サーバにエントリがあるホストの実際のアドレスを NAT ルールに指定するが、DNS サーバはクライアントとは別のインターフェイスにある場合、クライアントと DNS サーバではホストのアドレスとして別々のアドレスが必要となります。クライアントではマッピング済みアドレスが必要で、DNS サーバでは実際のアドレスが必要です。このオプションをイネーブルにすると、クライアントへの DNS 応答内のアドレスが修正されます。マッピング済みホストは、クライアントか DNS サーバのどちらかと同じインターフェイスになければなりません。詳細については、P.21-15 の「DNS と NAT」を参照してください。

ステップ 10　（オプション）接続の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、次のいずれかのオプション（複数可）を設定します。

（注） セキュリティ ポリシー ルールを使用してこれらの値の一部を設定することもできます（P.23-3 の「Connection Settings（透過モードのみ）」を参照）。両方で値の設定を行うと、FWSM は小さい値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、FWSM 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）、FWSM は TCP パケットのシーケンス番号をランダム化します。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。FWSM は、発信方向と着信方向の両方を通過する TCP SYN の ISN をランダム化します。

  保護されたホストの ISN をランダム化すると、攻撃者が新しい接続の次の ISN を予測できなくなり、新しいセッションを乗っ取ることができなくなります。

  必要に応じて TCP 初期シーケンス番号のランダム化をディセーブルにできます。次の例を参考にしてください。

  - 別のインライン ファイアウォールでも初期シーケンス番号をランダム化している場合。このアクションがトラフィックに影響しない場合でも、両方のファイアウォールが共にこのアクションを実行する必要はありません。
  - FWSM を経由して eBGP マルチホップを使用し、eBGP ピアで MD5 を使用する場合。ランダム化により MD5 チェックサムが中断されます。
  - FWSM が接続のシーケンス番号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 接続の最大数を 0 ～ 65,535 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 接続の最大数を 0 ～ 65,535 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**：初期接続のホストごとの最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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。

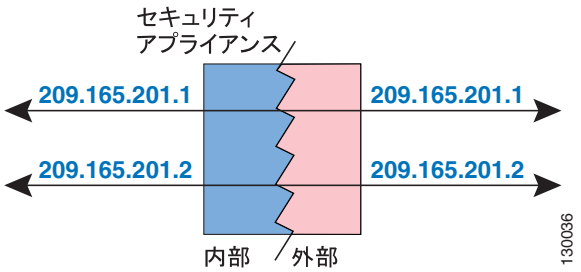
NAT 免除の使用

NAT 免除を使用すると、アドレスが変換から免除され、実際のホストとリモート ホストの両方が接続を発信できます。NAT 免除では、（ポリシー NAT と同様）免除するトラフィックを決定する場合に、実際のアドレスと宛先アドレスを指定できるので、ダイナミック アイデンティティ NAT よりも NAT 免除を使用した場合の方が、より詳細な制御が可能になります。ただし、ポリシー NAT とは異なり、NAT 免除で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 を使用します。

NAT 免除の詳細については、P.21-10 の「NAT 制御がイネーブルの場合の NAT のバイパス」を参照してください。

図 21-23 に、一般的な NAT 免除のシナリオを示します。

図 21-23　NAT 免除



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 ペインで **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 領域の Interface ドロップダウン リストから、免除する実際のアドレスを持つホストに接続され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するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

（注）　免除しないアドレスを後で指定することもできます。たとえば、10.1.1.0/24 のように免除するサブネットを指定できますが、10.1.1.50 を変換する場合、そのアドレスに対して免除を行わない別のルールを作成できます。

複数の実際のアドレス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するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

複数の宛先アドレスはカンマで区切ります。

デフォルトでは、この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、下位のセキュリティ インターフェイスに発信されるトラフィックを免除するか（デフォルト）、または、上位のセキュリティ インターフェイスに発信されるトラフィックを免除するかを、適切なオプション ボタンをクリックして選択します。

ステップ 7　（オプション）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　（オプション）NAT 免除のルールに含まれているアドレスの一部を免除しない場合、免除を除外する別のルールを作成できます。既存の NAT 免除ルールを右クリックして **Insert** チェックボックスをオンにします。

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. 手順 3 から 8 まで実行すると、ルールが完成します。

No Exempt ルールを Exempt ルールの前に追加します。Exempt ルールと No Exempt ルールの順序は重要です。FWSM がパケットを免除するかどうかを決定する場合、FWSM は、リスト上のルールの順序で NAT exempt および No Exempt のルールに照合してパケットをテストします。一致が見つかると、その後のルールはチェックされません。

CHAPTER 22

ARP 検査およびブリッジング パラメータの設定

この章では、ARP 検査をイネーブルにする方法と、透過ファイアウォール モードでの FWSM 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システム実行スペースではなくセキュリティ コンテキストで入力できます。

透過ファイアウォール モードの詳細については、第 16 章「ファイアウォール モードの概要」を参照してください。

この章には、次の項があります。

ARP 検査の設定

この項では、ARP 検査について説明し、これをイネーブルにする方法について説明します。次の事項を取り上げます。

ARP Inspection

ARP Inspection ペインでは、ARP 検査を設定できます。

デフォルトでは、すべての ARP パケットが FWSM を通過できます。ARP パケットのフローを制御するには、ARP 検査をイネーブルにします。

ARP 検査をイネーブルにすると、FWSM はすべての ARP パケットの MAC アドレス、IP アドレス、および発信元インターフェイスを ARP テーブルのスタティック 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、および発信元インターフェイスが ARP エントリと一致した場合、パケットは通過します。
- MAC アドレス、IP アドレス、またはインターフェイス間でミスマッチがある場合、FWSM 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 テーブルのどのエントリとも一致しない場合は、パケットをすべてのインターフェイスに転送するか（フラッド）、パケットをドロップするように FWSM を設定できます。

ARP 検査は、悪意のあるユーザが他のホストまたはルータになりすますこと（ARP スプーフィング）を防ぎます。ARP スプーフィングは、「man-in-the-middle」攻撃（介入者攻撃）を可能にすることがあります。たとえば、ホストは ARP 要求をゲートウェイ ルータに送信し、ゲートウェイ ルータはゲートウェイ ルータ MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスの代わりに攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これによって、攻撃者は、すべてのホスト トラフィックを傍受してからルータに転送できます。

ARP 検査を行うと、正しい MAC アドレスとそれに関連付けられている IP アドレスがスタティック ARP テーブルにある限り、攻撃者は、攻撃者の MAC アドレスで ARP 応答を送信することができなくなります。

フィールド

- Interface：インターフェイス名を示します。
- ARP Inspection Enabled：ARP 検査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。
- Flood Enabled：ARP 検査がイネーブルになっている場合には、アクションで未知のパケットをフラッドするようになっているかどうかを Yes または No で示します。ARP 検査がディセーブルになっている場合は、この値は常に No です。
- Edit：選択したインターフェイスの ARP 検査パラメータを編集します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 検査の設定値を設定できます。

フィールド

- Enable ARP Inspection：ARP 検査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にも一致しないパケットが、送信元のインターフェイスを除くすべてのインターフェイスからフラッドするように指定します。MAC アドレス、IP アドレス、またはインターフェイス間でミスマッチがある場合、FWSM 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、一致しないすべての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 FWSM 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。

専用の管理インターフェイスがある場合、こ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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、パケットの宛先を IP アドレスで識別しますが、イーサネット上でパケットが実際にどこに配信されるかは、イーサネットの MAC アドレスで決まります。ルータやホストが直接接続されているネットワークにパケットを配信する場合は、そのパケットの IP アドレスに関連付けられている MAC アドレスを尋ねる ARP 要求を送信します。次に、ARP 応答に従って、MAC アドレスにパケットを配信します。ホストやルータは、パケットを配信するたびに ARP 要求を送信しなくてもよいように、ARP テーブルを保持しています。ARP テーブルは、ARP 応答がネットワークに送信されるたびにダイナミックに更新され、一定の期間使用されなかったエントリはタイムアウトになります。エントリが正しくなくなった場合（IP アドレスに関連付けられていた MAC アドレスが変更された場合など）は、更新される前にタイムアウトになります。

（注） 透過ファイアウォールは、FWSM 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 ペインでは、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しないため、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たインターフェイスを示します。
- IP Address：ホストの IP アドレスを示します。
- MAC Address：ホストの MAC アドレスを示します。
- Proxy ARP：FWSM 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。FWSM 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：FWSM 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 テーブルが再構築されると、新しいホスト情報に自動的に更新され、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できます。このパラメータは ARP Static Table ペインに表示されますが、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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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るインターフェイスを設定します。
- IP Address：ホストの IP アドレスを設定します。
- MAC Address：ホストの MAC アドレスを設定します（00e0.1e4e.3d8b など）。
- Proxy ARP：FWSM 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。FWSM 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、次の項目について説明します。

概要

通常、ファイアウォールはルーティングされたホップであり、スクリーニング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、透過ファイアウォールは、「bump-in-the-wire（BITW）」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。FWSM 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。

セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、ブリッジ グループと呼ばれる最大 8 つのペアのインターフェイスを設定できます。各ブリッジ グループは別々のネットワークに接続します。ブリッジ グループのトラフィックは、他のブリッジ グループから隔離され、トラフィックは FWSM 内の他のブリッジ グループにルーティングされません。また、トラフィックは、外部ルータから FWSM 内の他のブリッジ グループにルーティングされる前に、FWSM から出る必要があります。ブリッジング機能はブリッジ グループごとに別々のものですが、他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、すべてのブリッジ グループは syslog サーバまたは AAA サーバのコンフィギュレーションを共有します。セキュリティ ポリシーを完全に分離するには、各コンテキストで単一ブリッジ グループを持つセキュリティ コンテキストを使用します。

透過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。IP 再アドレッシングは必要ありません。トラブルシューティングが必要な複雑なルーティング パターンや NAT コンフィギュレーションがないので、メンテナンスが容易です。

透過モードはブリッジとして機能しますが、IP トラフィックなどのレイヤ 3 トラフィックは、拡張アクセスリストで明示的に許可されない限り、FWSM を通過できません。アクセスリストなしで透過ファイアウォールを通過できるトラフィックは ARP トラフィックだけです。ARP トラフィックは ARP 検査によって制御されます。

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 FWSM を通過できません。一方、透過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（IP 以外のトラフィックの場合）を使用して、すべてのトラフィックを許可することができます。

（注） 透過モードの FWSM は、CDP パケットを通過させません。

たとえば、透過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することができます。同様に、HSRP や VRRP などのプロトコルは FWSM 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。

透過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。

FWSM が透過モードで動作している場合、パケットの発信インターフェイスは、ルート ルックアップではなく MAC アドレス ルックアップを実行することによって決定されます。この場合もルート文を設定することはできますが、FWSM から発信されたトラフィックだけに適用されます。たとえば、syslog サーバがリモート ネットワークにある場合は、FWSM がそのサブネットに到達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。

ブリッジングの下に、たとえば、スタティック MAC アドレス エントリを追加するか、または ARP 検査をイネーブルにすることで、透過ファイアウォールをカスタマイズできます。

前提条件

マルチコンテキスト モードの ASDM で、管理外コンテキストに対してファイアウォール モードを変更できます。シングルモードで、または管理コンテキストに対して、ルーテッドから透過にモードを変更するには、FWSM CLI にアクセスして **firewall transparent** コマンドを入力します。透過からルーテッドに変更するには、**no firewall transparent** コマンドを入力します。

モードを変更すると、FWSM はコンフィギュレーションをクリアします。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。すでに実装済みのコンフィギュレーションがある場合は、モードを変更する前に必ずコンフィギュレーションのバックアップを作成してください。新しくコンフィギュレーションを作成するときにこのバックアップを参照する場合があります。

firewall transparent コマンドでモードを変更する FWSM にテキスト コンフィギュレーションをダウンロードする場合は、必ずこのコマンドをコンフィギュレーションの最上部に置いてください。これによって、FWSM は、このコマンドを読み取り次第すぐにモードを変更し、その後は、ダウンロードしたコンフィギュレーションの読み取りを続けます。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、FWSM 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。

MAC Address Table

MAC Address Table ペインでは、スタティック MAC アドレスの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。必要に応じて、スタティック MAC アドレスを MAC アドレス テーブルに追加できます。

FWSM 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 FWSM 経由でパケットを送信すると、FWSM 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、FWSM 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。

FWSM 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、FWSM 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：FWSM は宛先 IP アドレスに対して ARP 要求を生成し、FWSM 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：FWSM は宛先 IP アドレスへの ping を生成し、FWSM 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に、MAC アドレス エントリが MAC アドレス テーブルに残る時間を 5 ～ 720 分（12 時間）の範囲で設定します。5 分がデフォルトです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 つとして、MAC スプーフィングの防止があります。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、スタティック エントリと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、FWSM 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：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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Learning

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。デフォルトにより、各インターフェイスは送信されてきたトラフィックの MAC アドレスを自動的にラーニングし、FWSM 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 FWSM 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示します。
- MAC Learning Enabled：MAC ラーニング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 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に対する MAC ラーニングをディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 23

ネットワーク攻撃の防止

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。次の項で構成されています。

Anti-Spoofing

Anti-Spoofing ペインでは、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）をイネーブルにすることができます。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、FWSM 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 FWSM に指示します。そのため、逆経路転送（Reverse Path Forwarding）と呼ばれます。FWSM 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 FWSM 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、FWSM はデフォルト ルートを使用して Unicast RPF 保護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、FWSM 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、FWSM 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、FWSM 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。
- Enable：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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Settings（透過モードのみ）

Connection Settings ペインでは、TCP および UDP の最大接続数や最大初期接続数を設定し、透過ファイアウォール モードでの発信トラフィック（内部から外部へ）の TCP シーケンスのランダム化をディセーブルにすることができます。

（注） 最大接続数、最大初期接続数、および TCP シーケンスのランダム化は、**Service Policy Rules** でも設定できます。サービス ポリシー ルールにより、これらの制限値の適用方法をより柔軟に制御し、発信接続だけでなく両方向のトラフィックの制限値を設定することができます。同じトラフィックに対して両方の方法でこれらの設定値を設定した場合、FWSM は小さ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でディセーブルにされている場合、FWSM 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。FWSM では、初期接続の制限を利用して TCP 代行受信を発生させます。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 シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合だけにします。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、1 つはサーバが生成します。FWSM は、ホスト / サーバによって生成される ISN をランダム化します。少なくとも 1 つの ISN をランダムに生成して、攻撃者が次の ISN を予想してセッションを乗っ取ることができないようにする必要があります。

フィールド

- Interface：接続制限がイネーブルになっているインターフェイスを示します。外部インターフェイスでは接続制限はサポートされていないため、このインターフェイスは常に内部インターフェイスとなります。
- Address：接続制限を適用するアドレスを示します。
- Maximum TCP Connections：最大 TCP 接続数を示します。値の 0 は、接続を制限しないことを意味します。
- Embryonic Limit：最大初期接続数を示します。値の 0 は、接続を制限しないことを意味します。
- Maximum UDP Connections：最大 UDP 接続数を示します。値の 0 は、接続を制限しないことを意味します。
- Randomize Sequence Number：TCP シーケンスのランダム化が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 で示します。
- Add：接続制限ルールを追加します。
- Edit：接続制限ルールを編集します。
- Delete：接続制限ルールを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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/Edit Connection Settings

Set/Edit Connection Settings ダイアログボックスでは、透過ファイアウォール モードでの発信トラフィック（内部から外部へ）の接続制限ルールを定義できます。

フィールド

- Host/Network：接続制限を設定するホストまたはネットワークを設定します。
  - Interface：接続制限を設定するインターフェイスを設定します。内部インターフェイスのみを選択します。
  - IP Address：接続制限を設定する IP アドレスを設定します。
  - Mask：サブネット マスクを設定します。ボックスにマスクを入力するか、またはリストから共通マスクを選択できます。
  - Browse：Select host/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、ネットワーク オブジェクトの概要 ペインで定義したホストとネットワークを選択できます。
- Maximum Connections：TCP および UDP の最大接続数を設定します。
  - Maximum TCP Connections：最大 TCP 接続数を 0 ～ 65535 の範囲で設定します。値の 0 は、接続を制限しないことを意味します。
  - Maximum UDP Connections：最大 UDP 接続数を 0 ～ 65535 の範囲で設定します。値の 0 は、接続を制限しないことを意味します。
- Maximum Embryonic Connections：最大初期接続数を 0 ～ 65535 の範囲で設定します。値の 0 は、接続を制限しないことを意味します。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。FWSM では、初期接続の制限を利用して TCP 代行受信を発生させます。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。
- Randomize Sequence Number：TCP シーケンス番号のランダム化をイネーブルにします。ランダム化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。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合だけにします。

モード

次の表に、この機能を使用できるモードを示します。

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

Fragment

Fragment ペインでは、FWSM の各インターフェイスにある IP フラグメント データベースの設定を行い、NFS との互換性を高めることができます。

フィールド

- Fragment テーブル：
  - Interface：FWSM 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ときに始動します。パケットのすべてのフラグメントが指定した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。
- Edit：Edit Fragment ダイアログボックスを開きます。
- Show Fragment：ペインが開き、FWSM 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** ペインの **Apply** をクリックします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ペインには、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：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：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：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ときに始動します。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：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：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：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：リアセンブリの失敗試行回数を表示します。
- Overflow：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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 ペイン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行った変更は、表示される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設定します。
- 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ときに始動します。パケットのすべてのフラグメントが指定した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。
- 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Options

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

- Force Maximum Segment Size for TCP Proxy：48 から最大数の間で、最大 TCP セグメント サイズをバイト単位で設定します。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することができます。ホストとサーバの両方は、接続を最初に確立するときに最大セグメント 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、FWSM 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、FWSM 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 Proxy：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 サイズを無効化します。この機能はデフォルトでディセーブルになっています（0 に設定）。ホストとサーバの両方は、最初に接続を確立するときに最大セグメント 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 ボックスで設定する値未満になる場合、FWSM 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、FWSM 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。この機能は、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の場合に使用できます。FWSM のデフォルト動作では、シャットダウン シーケンスが追跡され、2 つの FIN、および最後の FIN セグメントの ACK の後に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、FWSM 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率を維持することができます。ただし同時クローズでは、トランザクションの両エンドがクロージング シーケンスを開始します。これは、一方のエンドがクローズすると、もう一方のエンドは確認応答してからそれ自体のクロージング シーケンスを開始する、標準クローズ シーケンス（RFC 793 を参照）の場合とは対照的です。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。CLOSING 状態になっているソケットが数多く存在すると、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、このような動作が生じてメインフレーム サーバのパフォーマンスを低下させることで知られています。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。
- Reset Inbound：アクセスリストに基づいて、インターフェイスに着信して FWSM の搬送を試み、FWSM により拒否される、すべての TCP セッションに対し、FWSM が TCP リセットを送信します。このオプションをイネーブルにしない場合は、このようなセッションのパケットがすべて FWSM によって自動的に破棄されます。

モード

次の表に、この機能を使用できるモードを示します。

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

Timeouts

Timeouts ペインでは、FWSM 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中にスロットが使用されなかった場合は、リソースがフリー 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） Cisco TAC からの指示がない限り、これらの値を変更することはお勧めできません。

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 と入力します。接続時間は 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 状態がクローズされてからのアイドル時間を変更します。
- 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。
- 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 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 ポートがクローズされてから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 変換が削除されてからのアイドル時間を変更します。デフォルトは 5 分（00:00:05）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。
- 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。接続時間は 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。
- Non TCP UDP：TCP/UDP 接続がクローズしてからのアイドル時間を設定します。デフォルトは 10 分です。

- 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、Translation Slot の値より短くする必要があります。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、Translation Slot の値より短くする必要があります。
- 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。
- SIP Invite：PROVISIONAL 応答とメディア xlate のピンホールがクローズされてから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 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 disconnect：メディアが削除されてメディア xlates がクローズされてから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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

証明書

デジタル証明書は、認証のデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、社名、部署、IP アドレスなどのデバイスまたはユーザを特定する情報が含まれています。CA は、公開鍵 / 秘密鍵の暗号化を使用してセキュリティを確保する PKI のコンテキストでデジタル証明書を発行します。CA は、証明書に「署名」してその信頼性を確認し、デバイスまたはユーザの ID を保証する信頼できる認証局です。

CA 証明書は、他の証明書に署名するために使われるものです。自己署名される CA 証明書はルート証明書と呼ばれ、他の CA 証明書によって発行される CA 証明書は下位証明書と呼ばれます。また、CA は、特定のシステムまたはホストの証明書である ID 証明書も発行します。

デジタル証明書を使用する認証の場合、FWSM 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。これによって、複数の ID、ルートおよび証明書の階層が許可されます。

ここでは、次の項目について説明します。

Authentication

Authentication ペインでは、CA 証明書をトラストポイントに関連付けて、FWSM にインストールする CA 証明書を認証できます。既存のトラストポイント コンフィギュレーションを選択して編集することも、新しいトラストポイント コンフィギュレーションを作成することもできます。

選択したトラストポイントが手動登録用に設定されている場合、このパネルで CA 証明書を手動で取得してインポートできます。選択したトラストポイントが自動登録用に設定されている場合、FWSM は SCEP プロトコルを使用して CA にアクセスし、証明書を自動的に取得してデバイスにインストールします。

フィールド

- Trustpoint Name：CA 証明書を取得するために使用可能なトラストポイントが含まれるリストを表示します。リストのトラストポイントをクリックしてそのコンフィギュレーションを編集したり、新しいトラストポイント コンフィギュレーションを追加したりします。
- Edit：Trustpoint Name ボックスに表示されているトラストポイント コンフィギュレーションを変更します。
- New：リストに新しいトラストポイント コンフィギュレーションを追加します。
- Fingerprint：FWSM が CA 証明書の認証に使用する、英数字で構成されるキーを指定します。フィンガープリントを指定すると、FWSM は、そのフィンガープリントと CA 証明書の計算されたフィンガープリントを照合して、2 つの値が一致する場合のみ証明書を受け入れます。フィンガープリントがない場合、FWSM はフィンガープリントの照合を行わずに証明書を受け入れます。
- Import from a file：手動登録のみで、証明書をインポートするファイルを特定します。ボックスにファイルのパス名を入力することも、Browse をクリックしてファイルを検索することもできます。
  - Browse：Load Certificate File ダイアログボックスが表示されます。ここで証明書が含まれるファイルに移動できます。
- Enter the certificate text in base64 format：手動登録の場合、base64 形式でトラストポイント コンフィギュレーションを入力します。
- Authenticate：認証手順を完了させます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

デジタル証明書の認証、登録および管理

Enrollment

Enrollment ペインでは、リストからトラストポイント コンフィギュレーションを選択し、トラストポイント コンフィギュレーションを編集、または新規作成できます。ただし、自動登録の場合、CA 証明書を認証するまで登録要求を生成できません。

自動登録の場合、FWSM は SCEP プロトコルを使用して CA にアクセスし、ID 証明書を取得してデバイスにインストールします。手動登録の場合、証明書の登録要求を示す enrollment request ダイアログボックスが表示されます。この登録要求を使用して、CA の管理インターフェイスから ID 証明書を取得します。取得した ID 証明書は、base 64 形式または 16 進数形式である必要があります。その後、Import Certificate ダイアログボックスで ID 証明書をインポートできます。

フィールド

- Trustpoint Name：登録要求を生成するトラストポイントを指定します。リストから名前を選択したり、ボックスに表示されている名前を編集したり、または新しいトラストポイント コンフィギュレーションを追加します。
- Edit：Trustpoint Name ボックスに表示されているトラストポイント コンフィギュレーションを変更します。
- New：リストに新しいトラストポイント コンフィギュレーションを追加します。
- Enroll：CA での登録プロセスを開始します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

デジタル証明書の認証、登録および管理

Import Certificate

Import Certificate ペインでは、手動登録時に CA から受け取ったデバイス証明書をインストールできます。CA からの証明書をインポートするには、選択したトラストポイントに関連付けられている CA 証明書がある必要があります。該当する CA 証明書がない場合は、FWSM に警告が表示されます。

フィールド

- Trustpoint Name：証明書を受け取ったトラストポイントの名前を指定します。リストから名前を選択したり、ボックスに表示されている名前を編集したり、または新しいトラストポイント コンフィギュレーションを追加します。
- Edit：Trustpoint Name ボックスに表示されているトラストポイント コンフィギュレーションを変更します。
- New：リストに新しいトラストポイント コンフィギュレーションを追加します。
- Import from a file：ID 証明書をインポートするファイルを特定します。ボックスにファイルのパス名を入力することも、Browse をクリックしてファイルを検索することもできます。
  - Browse：Load CA certificate file ダイアログボックスが表示されます。ここで証明書が含まれるファイルに移動できます。
- Enter the certificate text in base64 format：手動登録では、カット アンド ペーストを使用して、エクスポート元から、この FWSM に証明書データを転送できます。

モード

次の表に、この機能を使用できるモードを示します。

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

Key Pair

キー ペアは、ID 証明書の登録時に必要です。FWSM では、複数のキー ペアをサポートします。

フィールド

- Key-pair Name：キー ペアに指定されている名前を表示します。
- Usage：RSA キー ペアの使用方法を表示します。RSA キーの使用方法には、General Purpose（デフォルト）と Special の 2 種類があります。Special を選択すると、FWSM は、署名用と暗号化用の 2 つのキー ペアを生成します。したがって、対応する ID ごとに 2 つの証明書が必要になります。
- Size：キー ペアの係数サイズが、512、768、1024 および 2048 で表示されます。デフォルトの係数サイズは 1024 です。
- Add：Add Key Pair ダイアログボックスが開きます。
- Show Details：名前、生成日、タイプ、係数サイズ、使用方法および DER-encoded キー データを表示します。
- Delete：選択したキー ペアを削除します。
- Refresh：表示をアップデートします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Key Pair

Add Key Pair ダイアログボックスで、キー ペアのリストに新しいキー ペアを追加できます。

フィールド

- Name：キー ペアの名前（デフォルトのキー <Default-RSA-Key> または特定のキー）を指定します。トラストポイントにキー ペアが設定されていない場合、FWSM はデフォルトのキー ペアを使用します。
- Size：キー ペアの係数サイズが、512、768、1024 および 2048 で表示されます。デフォルトの係数サイズは 1024 です。
- Usage：キー ペアの使用方法を指定します。このフィールドは、RSA キー ペアのみに適用されます。RSA キーの使用方法には、General Purpose（デフォルト）または Special の 2 種類があります。**Special** をクリックすると、FWSM は、署名用と暗号化用の 2 つのキー ペアを生成します。したがって、対応する ID ごとに 2 つの証明書が必要になります。
- Generate Now：キー ペアを生成します。

モード

次の表に、この機能を使用できるモードを示します。

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

Key Pair Details

Key Pair Details ダイアログボックスには、選択したキー ペアの情報が表示されます。

フィールド

- Key Pair：キー ペアに指定されている名前を表示します。
- Generation Time：キーが生成された日付と時刻を表示します。
- Size：キー ペアのタイプによって異なる係数サイズを表示します。RSA キーの場合、サイズは 512、768、1024 または 2048 を指定できます。デフォルトの係数サイズは 1024 です。
- Usage：RSA キー ペアの使用方法を表示します。RSA キーの使用方法には、General Purpose（デフォルト）と Special の 2 種類があります。キー ペアの使用方法が Special の場合、FWSM は署名用と暗号化用の 2 つのキー ペアを生成します。したがって、対応する ID ごとに 2 つの証明書が必要になります。
- Key Data text：DER-encoded キー データを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Certificate

Manage Certificates ペインには、テーブルの証明書がすべて表示されます。ここで証明書を追加および編集したり、証明書情報を表示したり、表示をリフレッシュしたり、FWSM から証明書を削除することができます。

フィールド

- Subject：証明書の所有者を特定します。
- Type：タイプ（CA、RA 汎用、RA 暗号化、RA シグニチャ、ID）を特定します。
- Trustpoint：トラストポイントを特定します。
- Status：ステータス（Available または Pending）を特定します。
  - Available は、CA が登録要求を受け入れて、ID 証明書を発行したことを意味します。
  - Pending は、登録要求が処理中であるため、CA が ID 証明書をまだ発行していないことを意味します。
- Usage：証明書が使用される方法（シグニチャ、汎用、または暗号化）を特定します。
- Add：Add Certificate ダイアログボックスを表示します。ここで FWSM に CA/RA/ID 証明書を追加できます。このダイアログボックスを使って、エクスポートしたファイルから証明書をインポートしたり、カット アンド ペーストで FWSM に証明書を入力できます。
- Show Details：Certificate Details ダイアログボックスを表示します。ここには選択した証明書に関する次の情報が表示されます。
  - General table：タイプ、シリアル番号、ステータス、使用方法、CRL 分散ポイント、および証明書の有効期間を表示します。これは、Available および Pending ステータスの両方に適用されます。
  - Subject table：サブジェクト DN または証明書所有者の X.500 フィールドと値を表示します。これは、Available ステータスだけに適用されます。
  - Issuer table：証明書を付与したエンティティの X.500 フィールドを表示します。これは、Available ステータスだけに適用されます。
- Refresh：Manage Certificates ペインのテーブルの表示を更新します。
- Delete：証明書の削除を確認する Delete Certificate ダイアログボックスを表示します。CA 証明書を削除すると、FWSM では関連付けられている ID 証明書もすべて削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

デジタル証明書の認証、登録および管理

Add Certificate

Add Certificate ダイアログボックスでは、CA/RA/ID 証明書を手動で追加できます。

フィールド

- Trustpoint Name：Manage Certificates テーブルに追加する証明書を指定します。
- Edit：Trustpoint Name ボックスに表示されているトラストポイント コンフィギュレーションを変更します。
- New：リストに新しいトラストポイント コンフィギュレーションを追加します。
- Certificate Type：タイプ（CA、RA 汎用、RA 暗号化、RA シグニチャ、ID）を指定します。
- Serial Number：証明書に FWSM のシリアル番号を含めます。
- Import from a file：証明書をインポートするファイルを特定します。ボックスにファイルのパス名を入力することも、**Browse** をクリックしてファイルを検索することもできます。
  - Browse：Add Certificate ダイアログボックスが表示されます。ここで証明書が含まれるファイルに移動できます。
- Enter the certificate text in base64 format：カット アンド ペースを使用してエクスポートしたソース テキストから、この FWSM に証明書データを 16 進数形式のみで転送できます。

モード

次の表に、この機能を使用できるモードを示します。

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

Trustpoint

トラストポイントは CA と ID のペアを表し、CA の ID、CA 固有のコンフィギュレーション パラメータ、および 1 つの登録済み ID 証明書とのアソシエーションを含んでいます。

ここでは、次の項目について説明します。

Configuration

Configuration ペインでは CA を特定し、ルート CA にすることができ、独自の公開鍵を含む自己署名された証明書を作成することができます。Configuration ペインでは、トラストポイントとして CA を追加、編集または削除したり、CRL を要求したりすることができます。

フィールド

- Trustpoint Name：トラストポイントの名前（IP アドレスやホスト名など）を表示します。
- Device Certificate Subject：FWSM システムの証明書を所有するサブジェクト DN を表示します。
- CA Certificate Subject：CA 証明書のサブジェクト名を表示します。
- Add：Add Trustpoint Configuration ダイアログボックスが開きます。
- Edit：Edit Trustpoint Configuration ダイアログボックスが開きます。
- Delete：選択したトラストポイントを削除します。
- Request CRL：選択したトラストポイントの CRL を取得します。CRL を参照するには、**Monitoring > Administration > CRL** を表示してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Trustpoint Configuration > Enrollment Settings タブ

Add Trustpoint Configuration > Enrollment Settings タブでは、トラストポイント テーブルにトラストポイントを追加できます。また、Edit Trustpoint Configuration > Enrollment Settings タブでは、選択したトラストポイントの情報を変更できます。

フィールド

- Trustpoint Name：CA に対応するトラストポイントの名前を指定します。たとえば、IP アドレスやホスト名を指定します。
- Generate a self-signed certificate on enrollment：登録時に FWSM の自己署名デバイス証明書を生成するためにクリックします。この操作により、SSL 接続を終了するときに使われる自己署名証明書を作成できます。この機能はデフォルトでオフになっています。このオプションがオンになっている場合、キー ペアと証明書パラメータのみを設定できます。

- Key Pair：リストで事前に定義したキー ペアを選択します。トラストポイントを追加する前に、キー ペアを設定する必要があります。このリストが空の場合、**New Key Pair** を選択してキー ペアを追加できます。
- Show Details：生成された場合に、名前、係数、使用方法（General Purpose または Special）および DER-encoded 形式のキー データといったキー ペアの情報を表示します。
- New Key Pair：Add Key Pair ダイアログボックスを表示します。ここで新しいキー ペア（RSA の場合）の名前、サイズ、タイプおよび使用方法を入力できます。
- Challenge Password：登録時に CA に登録されるチャレンジ フレーズを指定します。
- Confirm Challenge Password：チャレンジ パスワードを確認します。
- Use manual enrollment：PKCS10 証明書要求を生成することを指定します。CA は要求に基づいて FWSM 証明書を発行し、新しい証明書をインポートすることによって、FWSM に証明書がインストールされます。
- Use automatic enrollment：SCEP モードを使用することを指定します。トラストポイントが SCEP 登録用に設定されている場合、FWSM は SCEP プロトコルを使用して証明書をダウンロードします。
- Enrollment URL：自動登録の URL 名を指定します。最大長は 1000 文字です（事実上無制限）。
- Retry Period：証明書を要求した後、FWSM は CA からの証明書の受信を待ちます。FWSM は、指定されたリトライ間隔内に証明書を受け取らなかった場合は、証明書要求を再送信します。このフィールドに、登録要求の送信試行間隔を分単位で指定します。有効な範囲は 1 ～ 60 分です。デフォルト値は 1 です。
- Retry Count：証明書を要求した後、FWSM は CA からの証明書の受信を待ちます。FWSM は、指定されたリトライ間隔内に証明書を受け取らなかった場合は、証明書要求を再送信します。FWSM は、応答を受信するか、または指定したリトライの回数に達するまで要求を繰り返します。このフィールドで、登録要求の送信を試行する最大回数を指定します。有効なリトライの範囲は 0、1 ～ 100 回です。デフォルト値は 0 です。0 の場合はリトライ回数が無制限になります。
- Certificate Parameters：Certificate Parameters ダイアログボックスを表示します。ここで DN、FQDN など、登録時に証明書に含めるアトリビュートとその値を指定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Key Pair

Add Key Pair ダイアログボックスで、キー ペアのリストに新しいキー ペアを追加できます。

フィールド

- Name：キー ペアの名前（デフォルトのキー <Default-RSA-Key> または特定のキー）を指定します。トラストポイントにキー ペアが設定されていない場合、FWSM はデフォルトのキー ペアを使用します。
- Size：キー ペアの係数サイズが、512、768、1024 および 2048 で表示されます。デフォルトの係数サイズは 1024 です。
- Usage：キー ペアの使用方法を指定します。このフィールドは、RSA キー ペアのみに適用されます。RSA キーの使用方法には、General Purpose（デフォルト）または Special の 2 種類があります。Special をクリックすると、FWSM は、署名用と暗号化用の 2 つのキー ペアを生成します。したがって、対応する ID ごとに 2 つの証明書が必要になります。

- Generate Now：キー ペアを生成します。

モード

次の表に、この機能を使用できるモードを示します。

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

Certificate Parameters

Certificate Parameters ダイアログボックスで、登録時に含めるサブジェクト DN、FQDN、IP アドレスを指定できます。また、このダイアログボックスを使って、デバイスのシリアル番号を含めます。

フィールド

- Subject DN：サブジェクトの X.500 名に使用するアトリビュートと値を指定します。サブジェクトは証明書の所有者です。
  - **Edit** ボタンをクリックして Edit DN ダイアログボックスを表示して、Subject DN のアトリビュートと値を選択します。
- FQDN：証明書の Subject Alternative Name 拡張子に Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を含めます。FQDN は、要求が送信されるサーバ プログラムを完全に識別する URL の一部で、たとえば www.examplesite.com のようになります。
- E-mail：証明書の Subject Alternative Name 拡張子に指定の電子メール アドレスを含めます。
- IP Address：証明書の Subject Alternative Name 拡張子に指定の IP アドレスを含めます。
- Include device serial number：登録時に、証明書に FWSM のシリアル番号を含めます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 DN

Edit DN ダイアログボックスで証明書 DN を編集します。

Attributes リストで次のいずれかのアトリビュートを選択し、Value ボックスに値を入力して Add をクリックします。アトリビュートは必要な数だけ選択します。

フィールド

- Common Name (CN)：個々のユーザに指定されている名前。Pat など。
- Department (OU)：企業や大学といった大規模な組織の組織ユニットまたはサブグループ。Geology（地質学）部門など。

- Company Name (O)：企業や大学などの組織。University of Oz など。
- Country (C)：特定の国の 2 文字表記。OZ など。
- State (St)：国内の州や県。Kansas（カンザス州）など。
- Location (L)：サブジェクトの住所。49 Wizard St. など。
- Email Address (EA)：Pat@example.com。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Trustpoint Configuration > CRL Retrieval Policy タブ

CRL Retrieval Policy タブでは、CRL DP から CRL を取得するのか、または Static URLs テーブルに記載されている URL から CRL を取得するのかを指定できます。

フィールド

- Use CRL Distribution Point from the certificate：証明書に記載されている分散ポイントから CRL を取得します。
- Use Static URLs configured below：FWSM が CRL の取得を試みる URL を最大 5 つまで追加します。
- Add：Add Static URL ボックスを表示します。このボックスで、URL を最大 5 つ追加します。
  - URL：URL のタイプ（HTTP または LDAP）を選択します。
  - ://：CRL を分散する場所を入力します。
- Edit：Edit Static URL ボックスを表示して、選択した URL を変更します。
- Delete：選択した URL を削除します。
- Move Up：選択した URL をテーブルの一番上まで移動します。
- Move Down：選択した URL をテーブルの一番下まで移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 URL

フィールド

- URL:：URL のタイプ（HTTP、LDAP または SCEP）を選択します。
- ://：CRL を分散する場所を入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Trustpoint Configuration > CRL Retrieval Method タブ

CRL Retrieval Method タブで、CRL の取得方法を指定できます。すべての方法をイネーブルにすることができます。複数の方式をイネーブルにした場合、ASDM は指定した順番で使用します。

フィールド

- Enable Lightweight Directory Access Protocol (LDAP)：次のように LDAP パラメータを指定します。
  - Name：サーバ上の CRL へのアクセス権を持つユーザを指定します。
  - Password：Name に記載されているユーザのパスワードを指定します。
  - Confirm Password：パスワードを確認します。
  - Default Server：LDAP サーバのホスト名または IP アドレスを指定します。
  - Default Port：サーバのポート番号を指定します。デフォルトは 389 です。
- Enable HTTP：HTTP を CRL の取得に使用するプロトコルとして指定します。
- Enable Simple Certificate Enrollment Protocol (SCEP)：登録時ではなく、CRL の取得に登録時用と同じ方式を使用します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Trustpoint Configuration > Advanced タブ

Advanced タブで、CRL チェックおよびキャッシングのパラメータを指定できます。証明書は、発行されると一定の期間有効です。CA は、この期間が終了する前に証明書を無効にすることがあります。たとえば、セキュリティ上の問題が起こる可能性がある場合や、名前やアソシエーションが変わった場合です。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ています。CRL チェックをイネーブルにすることにより、FWSM が認証で証明書を使用するたびに、CA がその証明書を無効にしていないかどうかをチェックするようにします。

CA から同じ CRL を何度も受け取る必要のないように、FWSM 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で累積されます。新しく取得した CRL をキャッシュすると保存制限を超えそうな場合、FWSM は使用頻度が最も低い CRL を削除して容量を空けます。

フィールド

- CRL Check：CRL チェックの実行内容を決定します。次のいずれかをクリックします。
  - No Check：CRL チェックを実行しないことを示します。
  - Optional：要求した CRL が使用できない場合、FWSM がピア証明書を受け入れられることを示します。
  - Required：要求した CRL が使用可能でない限り、FWSM がピア証明書を検証しないことを示します。
- Cache Refresh Time：キャッシュのリフレッシュ間隔を分数で指定します。デフォルトは 60 分で、範囲は 1 ～ 1440 分です。
- Enforce next CRL update：Next Update 値の有効期限が切れていない有効な CRL を要求します。このボックスをオフにすると、Next Update 値のない有効な CRL、または Next Update 値の有効期限が切れた有効な CRL が許可されます。
- Accept certificates issued by this trustpoint：FWSM で、Trustpoint Name から証明書を受け取る必要があるかどうかを指定します。
- Use the configuration of this trustpoint to validate any remote user certificate issued by the CA corresponding to this trustpoint：イネーブルにすると、このトラストポイントがリモート証明書を発行した CA に認証されている場合、リモート ユーザ証明書の検証時にアクティブなコンフィギュレーションをこのトラストポイントから取得できます。

モード

次の表に、この機能を使用できるモードを示します。

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

Export

Export ペインでは、PKCS12 形式のすべての関連付けられているキーおよび証明書と一緒にトラストポイント コンフィギュレーションをエクスポートできます。これは base64 形式である必要があります。トラストポイント コンフィギュレーション全体には、チェーン全体（ルート CA 証明書、ID 証明書、キー ペア）が含まれますが、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、フェールオーバーまたはロードバランシング コンフィギュレーションで使用され、FWSM のグループ間でトラストポイントを複製します。たとえば、リモート アクセス クライアント コールをそのコールを提供する複数の装置を持つ中央組織に複製します。これらの装置には、同等のトラストポイント コンフィギュレーションが必要です。この場合、管理者は、トラストポイント コンフィギュレーションをエクスポートして、FWSM のグループ全体にインポートできます。

フィールド

- Trustpoint Name：リストのトラストポイントをクリックしてそのコンフィギュレーションを編集したり、新しいトラストポイント コンフィギュレーションを追加したりします。
- Edit：Trustpoint Name ボックスに表示されているトラストポイント コンフィギュレーションを変更します。
- New：リストに新しいトラストポイント コンフィギュレーションを追加します。
- Encryption Passphrase：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指定します。
- Confirm Passphrase：暗号化パスフレーズを確認します。
- Export to a file：トラストポイント 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指定します。PKCS12 は、公開鍵暗号化標準で、base64 エンコードまたは 16 進数を使用できます。
  - Browse：Select a File ダイアログボックスが表示され、ここでトラストポイント コンフィギュレーションをエクスポートするファイルに移動できます。
- Display the trustpoint configuration in PKCS12 format：Export Trustpoint Configuration ダイアログボックスが表示され、テキスト ボックスにトラストポイント コンフィギュレーションが表示されます。カット アンド ペーストを使用してデータを抽出し、Import ペインのウィンドウに配置することができます。終了するには OK をクリックします。
- Export：トラストポイント コンフィギュレーションをエクスポートします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Import ペインで、トラストポイント コンフィギュレーション全体を PKCS12 形式でインストールできます。トラストポイント コンフィギュレーション全体には、チェーン全体（ルート CA 証明書、RA 証明書、ID 証明書、キー ペア）が含まれますが、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、フェールオーバーまたはロードバランシング コンフィギュレーションで使用され、FWSM のグループ間でトラストポイントを複製します。たとえば、リモート アクセス クライアント コールをそのコールを提供する複数の装置を持つ中央組織に複製します。これらの装置には、同等のトラストポイント コンフィギュレーションが必要です。この場合、管理者は、トラストポイント コンフィギュレーションをエクスポートして、FWSM のグループ全体にインポートできます。

フィールド

- Trustpoint Name：トラストポイントを特定します。フェールオーバーまたはロードバランシング用に他の FWSM からインポートする場合、トラストポイント コンフィギュレーションがエクスポートされた FWSM と同じトラストポイント名を使用できます。ただし、同じ名前のトラストポイント / キー ペアがまだ存在していないことを確認する必要があります。
- Decryption Passphrase：トラストポイント コンフィギュレーションのエクスポート時に指定した暗号化パスフレーズを指定します。
- Confirm Passphrase：パスフレーズを確認します。
- Import from a file：証明書をインポートするファイルを特定します。ファイルからインポートされたテキストは、base64 形式または 16 進数形式の PKCS12 データである必要があります。ボックスにファイルのパス名を入力することも、Browse をクリックしてファイルを検索することもできます。
  - Browse：Load Certificate File ダイアログボックスが表示されます。ここでトラストポイント コンフィギュレーションが含まれるファイルに移動できます。
- Enter the trustpoint configuration in PKCS12 format：PKCS12 形式のトラストポイント コンフィギュレーションを base64 または 16 進数形式で貼り付けられます。この際、テキスト ボックスにカット アンド ペーストでデータを入力できます。
- Import：トラストポイント コンフィギュレーションをインポートします。

モード

次の表に、この機能を使用できるモードを示します。

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

デジタル証明書の認証、登録および管理

この項では、デジタル証明書の登録方法について説明します。登録が完了すると、証明書を使用してデバイスを VPN 管理ピアに認証することができます。

ここでは、次の項目について説明します。

設定手順の要約

CA を登録し、トンネルの認証に使用する ID 証明書を取得するための基本手順は次のとおりです。この例では、自動（SCEP）登録と手動登録の両方を示します。この手順に説明のないフィールドについては、**Help** ボタンをクリックしてください。

1. ID 証明書のキー ペアを作成します。
2. トラストポイントを作成します。
3. 登録 URL を設定します。
4. CA を認証します。
5. CA を登録し、ID 証明書を FWSM 上に置きます。

（注） 認証と登録はプロセスの 2 つの別個のフェーズです。まず認証する必要があります。その後、自動登録または手動登録のいずれかで登録することができます。

キー ペアの作成

最初に証明書のキー ペアを作成します。作成したキー ペアは、キー ペアの設定時に指定したラベルで識別されます。RSA キー ペアには、General Purpose と Usage の 2 種類があります。デフォルトは General Purpose で、1 組のキー ペアを作成します。Usage は、署名用と暗号化用の 2 つのキー ペアを作成します。したがって、対応する ID ごとに 2 つの証明書が必要です。

ASDM を使用して RSA キー ペアを作成するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Key Pair** で、**Add** ボタンをクリックします。

ステップ 2　**Add Key Pair** ダイアログボックスで情報を設定します。

ステップ 3　**Generate Now** ボタンをクリックします。

ステップ 4　生成されたキー ペアを表示するには、**Show Details** ボタンをクリックします。ASDM に、キー ペアに関する情報が表示されます。

自動登録による証明書の登録（SCEP）

トラストポイントを作成します。トラストポイントは CA と ID のペアを表し、CA の ID、固有のコンフィギュレーション パラメータ、および 1 つの登録済み ID 証明書とのアソシエーションを含んでいます。

トラストポイントを作成するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate >Trustpoint > Configuration** で、**Add** ボタンをクリックします。

ステップ 2　**Add Trustpoint Configuration** ダイアログボックスで、基本情報を設定します。その他のすべてのパラメータについては、デフォルト値を受け入れます。

a. **Trustpoint Name**：**Trustpoint Name** ボックスにトラストポイント名を入力します。

b. **Enrollment URL**：**Enrollment Settings** ペインの **Enrollment Mode** グループ ボックスで、SCEP の場合は **Use automatic enrollment** オプションをクリックします。次に、このボックスに登録 URL を入力します。たとえば、10.20.30.40/cgi-bin/pkiclient.exe のように入力します。

c. 証明書のパスワード確認をする場合は、**Challenge Password** ボックスおよび **Confirm Password** ボックスにパスワードを入力します。証明書を無効にする必要がある場合、このパスワードを CA 管理者に渡して自分が証明書所有者であることを証明することができます。このパスワードはコンフィギュレーションに保存されないため、書き留めておく必要があります。

ステップ 3　次にコンフィギュレーション パラメータを設定します。少なくとも、X.500 フィールドを使って証明書のサブジェクト名を設定する必要があります（Common Name（CN; 通常名）や Organizational Unit（OU; 組織ユニット）など）。

a. **Enrollment Settings** ペインの **Key Pair** リストから、このトラストポイントに対して設定したキー ペアを選択します。

b. **Enrollment Settings** ペインで、**Certificate Parameters** ボタンをクリックします。

c. サブジェクト DN の値を追加するには、**Certificate Parameters** ダイアログボックスで **Edit** ボタンをクリックします。

d. **Edit DN** ボックスで、**DN Attribute to be Added** の下にある **Attribute** リストからアトリビュートを選択し、**Value** ボックスに値を入力します。次に **Add** ボタンをクリックします。たとえば、まず **Command Name (CN)** を選択し、**Value** ボックスに Pat と入力します。次に **Department (OU)** を選択して、**Value** ボックスに Engineering と入力します。

e. サブジェクト DN 情報をすべて入力したら、**OK** ボタンをクリックします。

f. 必要に応じて、**FQDN**、**E-mail** および **IP Address** の値を入力し、**Include device serial number** オプションをオンにします。

g. **OK** ボタンをクリックします。

ステップ 4　**Apply** をクリックします。preview コマンドをオンにしておくと、ASDM には ASDM のコンフィギュレーションに基づいて CLI コマンドが表示され、送信するかキャンセルするかを選択できます。**Send** をクリックします。この手順を設定するすべての機能に対して実行します。

CA に対する認証

CA に対する認証により、CA 証明書を FWSM に置きます。SCEP 登録のトラストポイントを設定すると、CA 証明書は SCEP を通してダウンロードされます。設定しない場合は、CA 証明書をテキスト ボックスに貼り付けるか、または Browse ボタンを使用してファイルを指定する必要があります。この項では、SCEP 登録について説明します。

CA に対して認証するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Authentication** で、**Trustpoint Name** リストからトラストポイントの名前を選択します。

ステップ 2　**Authenticate** ボタンをクリックします。

ステップ 3　ASDM で **Authentication Successful** ダイアログが表示されたら、**OK** ボタンをクリックします。

CA の登録

トラストポイントを設定して認証したら、ID 証明書を登録できます。

ASDM を使用して ID 証明書を登録するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Enrollment** で、**Trustpoint Name** リストからトラストポイントを選択します。

ステップ 2　**Enroll** ボタンをクリックします。

作業が完了すると、ASDM に、トラストポイント コンフィギュレーションのエクスポート方法と登録ステータスのチェック方法を示す **Copy Trustpoint Configuration to Standby** ダイアログボックスが表示されます。このメッセージは、フェールオーバー コンフィギュレーションのみに関連します。フェールオーバーを設定していない場合は、この手順を無視して **OK** ボタンをクリックします。フェールオーバーを設定している場合、ダイアログボックスの指示に従ってスタンバイ デバイスに証明書をバックアップします。

手動登録による証明書の登録

自動登録以外の方法で CA から ID 証明書を受け取るときに、この方法を使用します。

ステップ 1　**Configuration > Properties > Certificate >Trustpoint > Configuration** で、**Add** ボタンをクリックします。

ステップ 2　**Add Trustpoint Configuration** ダイアログで、**Trustpoint Name** ボックスに名前を入力します。

ステップ 3　**Enrollment Settings** ペインで、**Key Pair** リストからキー ペアを選択するか、または **New Key Pair** ボタンをクリックして新しいキー ペアを追加します。

ステップ 4　必要に応じて、**Challenge Password** ボックスにパスワードを入力し、**Confirm Challenge Password** ボックスに再度入力して確認します。

ステップ 5　**Use manual enrollment** オプションをクリックします。

ステップ 6　**Certificate Parameters** ボタンをクリックします。

a. サブジェクト DN の値を追加するには、**Certificate Parameters** ダイアログボックスで **Edit** ボタンをクリックします。

b. **Edit DN** ボックスで、**DN Attribute to be Added** の下にある **Attribute** リストからアトリビュートを選択し、**Value** ボックスに値を入力します。次に **Add** ボタンをクリックします。たとえば、まず **Command Name (CN)** を選択し、**Value** ボックスに Pat と入力します。次に **Department (OU)** を選択して、**Value** ボックスに Engineering と入力します。

c. サブジェクト DN アトリビュートをすべて追加したら、**OK** ボタンをクリックします。

d. 必要に応じて、**FQDN**、**E-mail** および **IP Address** の値を入力し、**Include device serial number** オプションをクリックします。

e. **OK** ボタンをクリックします。

ステップ 7　**Configuration > Properties > Certificate > Enrollment** をクリックして、**Trustpoint Name** リストでトラストポイントを選択します。

ステップ 8　**Enroll** ボタンをクリックします。**Enrollment Request** ダイアログボックスに、次に行う作業の指示が表示されます。指示を読んだら **OK** ボタンをクリックします。

電子メールで要求を送信するか、または CA の Web インターフェイスを使用して登録します。

ステップ 9　CA から証明書を受け取ったら、**Configuration > Properties >Certificate > Import Certificate** をクリックし、**Trustpoint Name** リストでトラストポイントの名前を選択します。

ステップ 10　証明書のインポート方法を選択します。

a. **Import from a File**：ファイル名を入力するか、またはファイルを参照します。システムには、選択したトラストポイントに関連付けられている CA 証明書が必ずあり、CA からファイルで ID 証明書を受け取っているはずです。

または

b. **Enter the certificate text in base64 format**：テキスト ボックスに CA から受け取った ID 証明書のテキストを貼り付けます。詳細については、**Help** をクリックしてください。

ステップ 11　**Import** をクリックします。

ステップ 12　証明書登録設定をフラッシュ メモリに保存するには、**Save** 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向けの追加手順

ID 証明書、CA 証明書、および使用するネットワークの他の FWSM のキーをバックアップするには、まずそれらをファイルにエクスポートするか、またはエクスポート機能を使用してポップアップ ウィンドウに証明書を表示し、インポート機能で他の FWSM にコピー アンド ペーストします。

証明書のファイルまたは PKCS12 データへのエクスポート

トラストポイント コンフィギュレーション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　**Configuration > Properties > Certificate > Trustpoint > Export** に移動します。

ステップ 2　**Trustpoint Name**、**Encryption Passphrase**、および **Confirm Passphrase** フィールドに入力します。これらのフィールドの詳細については、**Help** をクリックしてください。

ステップ 3　トラストポイント コンフィギュレーションのエクスポート方法を選択します。

a. **Export to a File**：ファイル名を入力するか、またはファイルを参照します。

または

b. **Display the trustpoint configuration in PKCS12 format**：テキスト ボックスにトラストポイント コンフィギュレーション全体を表示し、コピーしてインポートすることができます。詳細については、**Help** をクリックしてください。

ステップ 4　**Export** をクリックします。

証明書のスタンバイ デバイスへのインポート

トラストポイント コンフィギュレーション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　**Configuration > Properties > Certificate > Trustpoint > Import** に移動します。

ステップ 2　**Trustpoint Name**、**Decryption Passphrase**、および **Confirm Passphrase** フィールドに入力します。これらのフィールドの詳細については、**Help** をクリックしてください。復号化パスフレーズは、トラストポイント コンフィギュレーションをエクスポートしたときに使用した暗号化パスフレーズと同じです。

ステップ 3　トラストポイント コンフィギュレーションのインポート方法を選択します。

a. **Import from a File**：ファイル名を入力するか、またはファイルを参照します。

または

b. **Enter the trustpoint configuration in PKCS12 format**：トラストポイント コンフィギュレーション全体をエクスポート元からテキスト ボックスに貼り付けます。詳細については、**Help** をクリックしてください。

Managing Certificates

証明書を管理するには、**Configuration > Properties > Certificate > Manage Certificates** に移動します。

このペインを使用して、新しい証明書の追加や証明書の削除を行うことができます。また、**Show Detail** ボタンをクリックして証明書に関する情報を表示することもできます。**Certificate Details** ダイアログボックスに、**General**、**Subject** および **Issuer** の 3 つのテーブルが表示されます。

General テーブルには次の情報が表示されます。

- Type：CA、RA または ID。
- Serial number：証明書のシリアル番号。
- Status：Available、in progress、error、fail。
- Usage：汎用またはシグニチャ。
- CRL DP：証明書の検証用に CRL が含まれる分散ポイントの URL。
- Dates/times within which the certificate is valid：証明書の有効期間の開始日と終了日。

Subject ペインには次の情報が表示されます。

- Name：証明書を所有するユーザまたはエンティティの名前。
- Serial Number：FWSM のシリアル番号。
- X.500 fields for the subject of the certificate：CN、OU など。
- Hostname of the certificate holder：wland.com など。
- Serial Number of the hostname：セキュリティ アプライアンスのシリアル番号。

Issuer ペインには、証明書を付与したエンティティの X.500 DN フィールドが表示されます。

- Common name (CN)
- Organizational unit or department (OU)
- Organization (O)
- Locality (L)
- State (ST)
- Country code (C)
- Email address of the issuer (EA)

CHAPTER 25

システム ログ メッセージのモニタリング

ログ表示機能を使って、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 メッセージを表示できます。FWSM ウィンドウで Cisco ASDM 5.2F を開くと、ウィンドウの下部に最新の ASDM システム ログ メッセージが表示されます。**Configure ASDM Logging Filters** リンクをクリックすると、Logging Filters ペインにアクセスできます。システム ログ メッセージのフィルタリングの詳細については、P.13-12 の「Logging Filters」を参照してください。

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 13 章「ロギングおよび SNMP の設定」を参照してください。

ログ表示機能の概要

ここでは、次の項目について説明します。

Log Buffer

このペインを使用して、バッファに保存されているログ メッセージを別のウィンドウに表示します。

フィールド

- Logging Level：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：別のウィンドウを開き、ログ メッセージを表示します。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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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。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 13 章「ロギングおよび SNMP の設定」を参照してください。

フィールド

- Refresh：表示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 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ように指定できます。
- Create Rule：メッセージを作成したアクセス 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 のみに適用されます。
- 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アクション（ある場合）が表示されます。Recommended Action タブには、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のみ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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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。

フィールド

- Logging Level：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：別のウィンドウを開き、ログ メッセージを表示します。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確認することもできます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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。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 13 章「ロギングおよび SNMP 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 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ように指定できます。
- Create Rule：メッセージを作成したアクセス 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 のみに適用されます。
- 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アクション（ある場合）が表示されます。Recommended Action タブには、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のみ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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

フェールオーバーのモニタリング

ここでは、次の項目について説明します。

Failover

フェールオーバー ペアとフェールオーバー関連の統計情報で、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を監視できます。詳細については、次の項目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」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。また、シングル コンテキスト モードで、システムのフェールオーバー状態を次の方法で制御することもできます。

- 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

フェールオーバーがイネーブルでない場合、system フィールドのフェールオーバー状態にある次の情報が表示されます。

```
Failover Off
Failover unit Primary
Failover LAN Interface: test Vlan 200 (Configuration incomplete)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 15 seconds
Interface Policy 50%
Monitored Interfaces 0 of 250 maximum
```

フェールオーバーがイネーブルの場合、次の情報が表示されます。

Failover state of the system：FWSM のフェールオーバー状態が表示されます。このボックスの情報は、**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のみが表示されます。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。
- 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。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が表示されます。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、またはフェールオーバー リンクが設定されていません。

    *Listen：装置は、ポーリング メッセージをリッスンすることでアクティブ装置の検出を試みます。

    *Learn：装置はアクティブ装置を検出し、スタンバイ モードに移る前にコンフィギュレーションを同期化していません。

    *Failed：装置で障害が発生しました。
  - *Active Time：装置がアクティブ状態になってからの時間（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。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ました。

    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：インターフェイスが正しく動作しています。

    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：FWSM 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ます。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、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：次のいずれかを表示します。
  - *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 フェールオーバーを使用していません。
- Stateful Obj：各フィールド型で、次の統計情報が表示されます。
  xmit：相手装置に送信されたパケットの数。
  xerr：相手装置にパケットを送信中に発生したエラーの数。
  rcv：受信されたパケットの数。
  rerr：相手装置からパケットを受信中に発生したエラーの数。
  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：Remote Procedure Call（リモート プロシージャ コール）接続の情報。
  - TCP conn：TCP 接続の情報。
  - UDP conn：ダイナミック UDP 接続の情報。
  - ARP tbl：ダイナミック ARP テーブルの情報。
  - L2BRIDGE tbl：レイヤ 2 ブリッジ テーブルの情報（透過ファイアウォール モードのみ）。
  - Xlate_Timeout：接続変換タイムアウトの情報を示します。
  - VPN IKE upd：IKE 接続の情報。
  - VPN IPSEC upd：IPSec 接続の情報。
  - VPN CTCP upd：cTCP トンネル接続の情報。
  - VPN SDI upd：SDI AAA 接続の情報。
  - VPN DHCP upd：トンネリングされた DHCP 接続の情報。
- *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のみ表示されます。

- 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：（シングルモードのみで使用可能）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 FWSM をアクティブ装置にします。

- Make Standby：（シングルモードのみで使用可能）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 FWSM をスタンバイ装置にします。
- Reset Failover：（シングルモードのみで使用可能）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リセットすることはできません。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：（シングルモードのみで使用可能）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。
- Suspend/Resume Config Sync：コンフィギュレーションの変更がスタンバイ装置に複製されないようにするには、**Suspend Config Sync** ボタンをクリックします。コンフィギュレーションの変更がスタンバイ装置に複製されるようにするには、**Resume Config Sync** ボタンをクリックします。

  複雑なコンフィギュレーションの FWSM をアップグレードすると、管理アプリケーションで接続が失われる場合があります。その結果、不完全なコンフィギュレーション ファイルがスタンバイ FWSM に適用される場合があります。不完全なコンフィギュレーションがスタンバイ FWSM に適用されないようにするには、自動コンフィギュレーション同期をディセーブルにします。アクティブな FWSM でソフトウェア イメージのアップグレードまたはコンフィギュレーションの変更を行うときに、コンフィギュレーションの同期をディセーブルにしてから、コンフィギュレーション ファイルが完全であることを確認してコンフィギュレーションをスタンバイ FWSM のコンフィギュレーションと同期させます。コンフィギュレーションが完全であることを確認後、コンフィギュレーションの同期を再度イネーブルにして、スタンバイ装置にそのコンフィギュレーションを複製します。
- Refresh：このボタンをクリックして、system ボックス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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」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のみで使用できます。

グラフの情報は、ステートフル フェールオーバーのみに関連します。

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。このボックスで統計タイプをダブルクリックして、Selected Graphs ボックスに移動します。このボックスで統計タイプを 1 回クリックして、エントリを選択します。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：FWSM の RPC サービス情報を表示します。
- TCP Connection Information：FWSM の TCP 接続情報を表示します。
- UDP Connection Information：FWSM の UDP 接続情報を表示します。
- ARP Table Information：FWSM の ARP テーブル情報を表示します。
- L2Bridge Table Information：（透過ファイアウォール モードのみ）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：（シングルモードのみ）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：（シングルモードのみ）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 ボックスに表示されます。ここでタイプを追加することができます（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 ボックスで選択したエントリを Selected Graphs ボックスに移動します。
- Remove：Selected Graphs ボックスから、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。タイプを 4 つまで含めることができます。このボックスで統計タイプをダブルクリックして、選択した統計タイプをボックスから削除します。このボックスで統計タイプを 1 回クリックして、統計タイプを選択します。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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」を参照してください。

Failover

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 and 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」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することもできます。

- 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：FWSM のフェールオーバー状態が表示されます。このボックスの情報は、**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。

- 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。
- 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。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が表示されます。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ました。

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：インターフェイスが正しく動作しています。

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：FWSM 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ます。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、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：次のいずれかを表示します。
  - *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 フェールオーバーを使用していません。
- Stateful Obj：各フィールド型で、次の統計情報が表示されます。

  xmit：相手装置に送信されたパケットの数。

  xerr：相手装置にパケットを送信中に発生したエラーの数。

  rcv：受信されたパケットの数。

  rerr：相手装置からパケットを受信中に発生したエラーの数。

  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：Remote Procedure Call（リモート プロシージャ コール）接続の情報。
  - TCP conn：TCP 接続の情報。
  - UDP conn：ダイナミック UDP 接続の情報。
  - ARP tbl：ダイナミック ARP テーブルの情報。
  - L2BRIDGE tbl：レイヤ 2 ブリッジ テーブルの情報（透過ファイアウォール モードのみ）。
  - Xlate_Timeout：接続変換タイムアウトの情報を示します。
  - VPN IKE upd：IKE 接続の情報。
  - VPN IPSEC upd：IPSec 接続の情報。
  - VPN CTCP upd：cTCP トンネル接続の情報。
  - VPN SDI upd：SDI AAA 接続の情報。
  - VPN DHCP upd：トンネリングされた DHCP 接続の情報。
- 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のみ表示されます。

- 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 FWSM 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、FWSM 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 FWSM 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、FWSM 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リセットすることはできません。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 ボックス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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」を参照してください。

Failover Group 1 and Failover Group 2

Failover Group 1 and 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*]：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が表示されます。このボックスに表示される情報は、**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、またはフェールオーバー リンクが設定されていません。

Listen：装置は、ポーリング メッセージをリッスンすることでアクティブ装置の検出を試みます。

Learn：装置はアクティブ装置を検出し、スタンバイ モードに移る前にコンフィギュレーションを同期化していません。

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ました。

  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：インターフェイスが正しく動作しています。

  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：FWSM 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ます。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、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：次のいずれかを表示します。

  - *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 フェールオーバーを使用していません。

  Stateful Obj：各フィールド型で、次の統計情報が表示されます。

  - xmit：相手装置に送信されたパケットの数。
  - xerr：相手装置にパケットを送信中に発生したエラーの数。
  - rcv：受信されたパケットの数。
  - rerr：相手装置からパケットを受信中に発生したエラーの数。

  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：Remote Procedure Call（リモート プロシージャ コール）接続の情報。
  - TCP conn：TCP 接続の情報。
  - UDP conn：ダイナミック UDP 接続の情報。
  - ARP tbl：ダイナミック ARP テーブルの情報。
  - L2BRIDGE tbl：レイヤ 2 ブリッジ テーブルの情報（透過ファイアウォール モードのみ）。
  - Xlate_Timeout：接続変換タイムアウトの情報を示します。
  - IKE upd：IKE 接続の情報。
  - VPN IPSEC upd：IPSec 接続の情報。
  - VPN CTCP upd：cTCP トンネル接続の情報。
  - VPN SDI upd：SDI AAA 接続の情報。
  - VPN DHCP upd：トンネリングされた DHCP 接続の情報。

- 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、FWSM 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、FWSM 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リセットすることはできません。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 ボックス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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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」を参照してください。

CHAPTER 27

インターフェイス

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。

ここでは、次の項目について説明します。

ARP Table

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表示します。
- IP Address：IP アドレスを示します。
- MAC Address：MAC アドレスを表示します。
- Proxy ARP：プロキシ ARP がこのインターフェイスでイネーブルの場合に表示されます。
- Clear Dynamic ARP Entries：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：FWSM 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：表示が更新された日付と時刻を示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

FWSM では、クライアントや DHCP 統計情報に割り当てられているアドレスを含む DHCP ステータスを監視できます。

ここでは、次の項目について説明します。

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 アドレスがリストされます。

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 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：FWSM 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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：FWSM で受信したメッセージの合計数を表示します。
- Total Messages Sent：FWSM 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時を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Address Table

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：FWSM の現在の情報でテーブルをリフレッシュします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、FWSM によって自動的に作成され、アクティブ化されて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、このテーブルのみに表示されます。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 ボックスに表示されます。

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。
- Refresh：ダイナミック 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時を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、FWSM には現在のコンテキストの統計情報のみが表示されます。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: ペイン：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。

  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、FWSM のデータ処理能力を超えたため、FWSM 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：FWSM 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。この数と無視された数を比較します。イーサネット ネットワークのブロードキャスト ストームが原因で、入力バッファ イベントが発生しなくなることがよくあります。
  - Packet Errors：次の統計情報を表示します。

    CRC：Cyclical Redundancy Check（巡回冗長検査）エラーの数。ステーションがフレームを送るときに、フレームの末尾に CRC を追加します。この CRC は、フレームのデータに基づいて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、FWSM は CRC が一致しない旨を指摘します。通常、CRC の数が多い場合の原因として、衝突か、またはステーションが不正なデータを伝送していることが考えられます。

    Frame：フレーム エラーの数。不正なフレームには、長さが正しくないかフレームのチェックサムに不良のあるパケットが含まれます。通常、このエラーの原因として、衝突またはイーサネット デバイスの不具合が考えられます。

    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、他の入力関連のエラーによって、入力エラー数が増え、一部のデータグラムに複数のエラーが存在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。通常、ラントは衝突によって発生します。また、配線や電気インターフェイスに問題がある可能性もあります。

    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 バイトを超えたイーサネット パケットは ジャイアントと見なされます。

    Deferred：FastEthernet インターフェイスのみ。リンクのアクティビティが原因で送信前に延期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 インターフェイスのみ。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 トラフィックが混雑しているときにのみ増加します。

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。通常、これは拡張しすぎた LAN（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、ステーション間にリピータが 3 つ以上ある、またはカスケード接続されたマルチポート トランシーバが多すぎる）で発生します。衝突したパケットは、出力パケットによって一度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。遅延衝突は、パケットの伝送で遅れて検出される衝突です。通常、このような状況は起こりません。2 つのイーサネット ホストが同時に伝送を試みた場合、両方のホストが早期にパケットの衝突を起こして両方がバックオフするか、2 番目のホストが 1 番目のホストの伝送を確認して待機します。遅延衝突が発生した場合、デバイスが割り込んでイーサネット上でパケットの送信を試みる一方で、FWSM はパケットの送信を一部終了します。FWSM は、パケットの最初の部分が入ったバッファをすでに開放している可能性があるため、パケットを再送信しません。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衝突に対処するように設計されているため、これは実際の問題ではありません。ただし、遅延衝突があるということ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、リピータを使用した大規模ネットワークと仕様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ペインから追加され、Available Graphs for: 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。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、タイプを追加することができます。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、「Graph」という形式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 ペイン：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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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** 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 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。
- Bookmark：ブラウザ ウィンドウに、Graph ウィンドウ上のすべてのグラフおよびテーブルへのリンク 1 つと、各グラフまたはテーブルへの個別のリンクが表示されます。ブラウザでこれらの URL をブックマークとしてコピーできます。グラフの URL を開くときに、ASDM を実行している必要はありません。ブラウザが ASDM を起動し、グラフが表示されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

ルーティングのモニタリング

FWSM で次のルーティング情報を監視できます。

BGP のモニタリング

次の BGP 情報を監視できます。

BGP ルーティング プロセスの設定方法の詳細については、P.14-3 の「BGP スタブ ルーティング」を参照してください。

BGP Neighbor

BGP Neighbor ペインには、BGP ネイバーへの接続に関する詳細情報が表示されます。

フィールド

- BGP Neighbor：BGP Neighbor フィールドには、**show bgp neighbors** コマンドの出力結果が含まれます。BGP ネイバーの接続に関する詳細情報が表示されます。表示される出力の情報については、『*Catalyst 6500 Series and Cisco 7600 Series Switch Firewall Services Module Command Reference*』にある **show bgp neighbors** コマンドの情報を参照してください。
- Clear BGP Session：ネイバーとの BGP 接続、あるいは BGP の統計カウンタをリセットします。

BGP Networks

BGP Networks モニタリング ペインには、BGP ルーティング プロセスによりアドバタイズされるネットワークが表示されます。

フィールド

- Router identifier：FWSM のルータ ID です。ルータ ID は、**bgp router-id** コマンドが割り当てる IP アドレスです。実行中のコンフィギュレーションにこのコマンドがない場合、デフォルトのルータ ID は FWSM で設定されている最上位の IP アドレスになります。
- BGP Networks：BGP ルーティング プロセスによりアドバタイズされるネットワークが表示されます。テーブルの各行には、次の情報が含まれています。
  - Network：アドバタイズされているネットワークの IP アドレスです。
  - Next Hop：宛先ネットワークにパケットを転送するための次のシステムの IP アドレスです。エントリが 0.0.0.0 の場合、宛先ネットワークへのパスに BGP 以外のルートがあることを示します。
  - Metric：値が表示されている場合、その値が自律システム　メトリック間の値となります。このフィールドは頻繁に使用されません。
  - LocPrf：ローカルのプリファレンス値です。デフォルト値は 100 です。
  - Weight：自律システム フィルタ経由で設定されるルートの比重です。
  - Path：宛先ネットワークへの自律システム パスです。このフィールドには、パス内の自律システムあたり 1 つのエントリがあります。
- Clear BGP Session：ネイバーとの BGP 接続、あるいは BGP の統計カウンタをリセットします。

BGP Summary

BGP Summary ペインには、BGP ネイバーとの BGP 接続のステータスが表示されます。

フィールド

- Router ID：FWSM のルータ ID です。ルータ ID は、**bgp router-id** コマンドが割り当てる IP アドレスです。実行中のコンフィギュレーションにこのコマンドがない場合、デフォルトのルータ ID は FWSM で設定されている最上位の IP アドレスになります。
- Local AS Number：FWSM の自律システム番号です。
- BGP Session Table：BGP セッションに関する情報が表示されます。各行には次の情報が含まれています。
  - Neighbor：BGP ネイバーの IP アドレスです。
  - Version：ネイバーに音声通知される BGP のバージョン番号です。
  - AS Number：ネイバーの自律システム番号です。
  - Messages Received：ネイバーから受信するメッセージ番号です。
  - Messages Sent：ネイバーへ送信するメッセージの番号です。
  - Table Version：ネイバーへ送信された BGP データベースの最新バージョンです。
  - InQ：ネイバーからキューに入れられて処理されるメッセージの数です。
  - OutQ：キューからネイバーに送信されるメッセージの数です。
  - Up/Down：BGP セッションの状態が Established になっている時間、または Established でない場合は現在の状態になっている時間です。
  - State/PfxRcd：BGP セッションの現在の状態、およびネイバーまたはピア グループから受信したプレフィックスの数です。最大数に達すると、「PfxRcd」という文字列がエントリに表示され、ネイバーがシャットダウンし、接続が Idle に設定されます。

    Idle ステータスのエントリ（Admin）は、接続がシャットダウンしていることを示します。
- Clear BGP Session：ネイバーとの BGP 接続、あるいは BGP の統計カウンタをリセットします。

OSPF LSA

FWSM 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、FWSM 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：LSA の OSPF プロセスを表示します。
- Area：LSA の OSPF エリアを表示します。
- Router ID：LSA を発信するルータの OSPF ルータ ID を表示します。
- Advertiser：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：リンク ステートの経過時間を表示します。
- Sequence #：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：LSA の内容のチェックサムを表示します。
- Link Count：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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	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：LSA の OSPF プロセスを表示します。
- Area：LSA の OSPF エリアを表示します。
- Designated Router：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：LSA を送信した代表ルータの OSPF ルータ ID を表示します。
- Age：リンク ステートの経過時間を表示します。
- Sequence #：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：LSA の内容のチェックサムを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	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：LSA の OSPF プロセスを表示します。
- Area：LSA の OSPF エリアを表示します。
- Destination：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：LSA を送信した ABR の ID を表示します。
- Age：リンク ステートの経過時間を表示します。
- Sequence #：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：LSA の内容のチェックサムを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	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：LSA の OSPF プロセスを表示します。
- Area：LSA の OSPF エリアを表示します。
- Router ID：ASBR のルータ ID を表示します。
- Advertiser：LSA を送信した ABR の ID を表示します。
- Age：リンク ステートの経過時間を表示します。
- Sequence #：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：LSA の内容のチェックサムを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	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：LSA の OSPF プロセスを表示します。
- Network：AS 外部ネットワークのアドレスを表示します。
- Advertiser：ASBR のルータ ID を表示します。
- Age：リンク ステートの経過時間を表示します。
- Sequence #：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：LSA の内容のチェックサムを表示します。
- Tag：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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	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 のみ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：LSA の OSPF プロセスを表示します。
- Area：LSA の OSPF エリアを表示します。
- Network：外部ネットワークのアドレスを表示します。
- Advertiser：LSA を送信した ASBR のルータ ID を表示します。
- Age：リンク ステートの経過時間を表示します。
- Sequence #：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：LSA の内容のチェックサムを表示します。
- Tag：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

次の表に、この機能を使用できるモードを示します。

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

OSPF Neighbors

OSPF Neighbor ペインには、FWSM 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。

フィールド

- Neighbor：ネイバーのルータ ID を表示します。
- Priority：ルータの優先順位を表示します。
- State：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、FWSM 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のみで有効です。Attempt ステートでは、FWSM 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、FWSM 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、FWSM 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、FWSM 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、FWSM は、指定されたルータとバックアップの代表ルータのみと 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、FWSM 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、FWSM 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、FWSM 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、このデバイスのみ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 ヘッダーのみが含まれ、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、スレーブによって明示的に確認されているマスターによってのみ増分されます。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をチェックします。
- 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、FWSM 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 のみで 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：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：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：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

次の表に、この機能を使用できるモードを示します。

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

Routes

Routes ペインには、FWSM 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：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。
  - 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：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 エリア（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：宛先ネットワークの IP アドレス / ネットマスクを表示します。
- Gateway：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：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]：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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

プロパティのモニタリング

ここでは、次の項目について説明します。

AAA Servers

AAA Servers ペインでは、ASDM にアクセスできるユーザと、AAA サービスを使用する接続の種類を表示できます。

前提条件

AAA をイネーブルにするかどうかを指定する前に、まずユーザ ネットワークで 1 つ以上の AAA サーバ グループを作成する必要があります。AAA サーバ グループを作成するには、Configuration > Properties タブの AAA Server Groups ペインを使用します。または、FWSM 自体のローカル データベースを使用します。

フィールド

AAA Server ペインには、次のフィールドが表示されます。

- 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。

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。Clear Server Stats を使って統計情報をクリアできます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Device Access 機能では、管理セッションおよびユーザを監視できます。ここでは、次の項目について説明します。

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 FWSM 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

AAA Local Lockouts エリアには、次のフィールドが表示されます。

- Currently locked out users：現在ロックアウトされているユーザのリスト。
- Lock Time：ユーザがシステムへのアクセスをロックアウトされてからの経過時間。
- Failed Attempts：失敗したログイン試行回数。
- User：ログイン試行に失敗したユーザ名。

次のボタンも使用できます。

- Refresh：最新情報で画面を更新します。
- Clear lockout：選択したユーザのロックアウト条件をクリアします。
- 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

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、FWSM に認証されているユーザを表示できます。

フィールド

- User：FWSM に認証されているユーザ名を表示します。
- IP Address：FWSM に認証されているユーザの IP アドレスを表示します。
- Dynamic ACL：FWSM に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り、選択したユーザを切断するまでにユーザを非アクティブな状態にしておく時間を表示します。

- Absolute Timeout：セッションを閉じ、選択したユーザを切断するまでにユーザを接続したままにできる時間を表示します。
- Refresh：現在認証されているユーザのリストを更新します。

モード

次の表に、この機能を使用できるモードを示します。

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

HTTPS/ASDM Sessions

HTTPS/ASDM ペインでは、現在接続中の HTTPS/ASDM セッションを表示できます。

ネットワーク ブラウザ ウィンドウで ASDM を実行している PC またはワークステーションが、FWSM と通信するために、セキュアな接続が必要です。

フィールド

HTTPS/ASDM ペインには、次のフィールドが表示されます。

- Session ID：接続中の HTTPS/ASDM セッションの名前を表示します。
- IP Address：この FWSM 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。
- Refresh：現在接続中の HTTPS/ASDM セッションのリストを更新します。
- Disconnect：接続中の HTTPS/ASDM セッションを切断します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、セキュア シェル（SSH）プロトコルを使用した管理アクセスのために、FWSM に接続されているホストを表示できます。

フィールド

Currently Connected Secure Shell Sessions ペインには、次のフィールドが表示されます。

- 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：FWSM への接続に使われる 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わ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わ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。
- Refresh：現在選択中の SSH セッションのリストを更新します。
- Disconnect：接続中の SSH セッションを切断します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 セッション

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

Telnet Sessions ペインには、次のフィールドが表示されます。

- 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 FWSM 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。
- Refresh：現在接続中の Telnet セッションのリストを更新します。
- Disconnect：接続中の Telnet セッションを切断します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 機能では、FWSM 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モニタリング情報を表示できます。詳細については、次の項目も参照してください。

- Perfmon
- Xlates

Perfmon

Perfmon 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 つのウィンドウに最大で 4 つのグラフを表示することができます。

この情報には、変換、接続、Websense 要求、アドレス変換、および毎秒実行される AAA トランザクションの数が含まれます。

フィールド

- 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 ボックスに表示されます。ここでタイプを追加することができます（1 つのウィンドウに最大 4 つ）。
- Graph Selection：ウィンドウに表示するグラフの種類を設定します。
  - 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：FWSM の AAA パフォーマンス情報を表示します。

    Inspection Perfmon：FWSM 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 FWSM の Web パフォーマンス情報を表示します。

    Connections Perfmon：FWSM の接続パフォーマンス情報を表示します。

    Xlate Perfmon：FWSM の NAT パフォーマンス情報を表示します。
  - Selected Graphs：追加してグラフ ウィンドウに表示するコンポーネントを表示します。
  - Add：Available Graphs ボックスから Selected Graphs ボックスに、選択したエントリを移動します。
  - Remove：Seleted Graphs ボックスから Available Graphs ボックスに、選択したエントリを移動します。
- Show Graphs：新しいグラフ ウィンドウまたは更新したグラフ ウィンドウに選択した統計情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Xlates 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 つのフレームに最大で 4 つのグラフを表示することができます。

フィールド

- 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 ボックスに表示されます。ここでタイプを追加することができます（1 つのウィンドウに最大 4 つ）。
- Graph Selection：ウィンドウに表示するグラフの種類を設定します。
  - 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：FWSM の NAT の使用状況を表示します。
  - Selected Graphs：追加してグラフ ウィンドウに表示するコンポーネントを表示します。
  - Add：このボタンをクリックして、Available Graphs For ボックスで選択したエントリを Selected Graphs ボックスに移動します。
  - Remove：Selected Graphs ボックスから、選択した統計タイプを削除します。
- Show Graphs：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウに選択した統計情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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、選択したトラストポイントの関連付けられた CRL を表示またはクリアできます。トラストポイントは、Configuration > Properties > Certificate > Trustpoint で設定されます。

フィールド

- Trustpoint name：選択したトラストポイントの名前。
- View CRL：選択した CRL を表示します。
- Clear CRL：選択した CRL をキャッシュからクリアします。
- CRL info：詳細な CRL 情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

ASDM キャッシュ情報が外部の DNS クエリーから返され、DNS 情報のローカル キャッシュが渡されます。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。
- キャッシュ全体をクリアするには、***Clear Cache*** を使用します。

フィールド

- Host：ホストの DNS 名。
- 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：ASDM が最後にそのエントリを参照してからの経過時間を示します。
- 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。キャッシュに十分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 キャッシュをクリアします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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 Resource Graphs

System Resource Graphs では、FWSM のメモリ、CPU およびブロックの使用状況を表示できます。1 つのフレームに最大で 4 つのグラフを表示することができます。

ここでは、次の項目について説明します。

Blocks

Blocks では、空きメモリ ブロックと使用中のメモリ ブロックをグラフ形式で表示できます。1 つのフレームに最大で 4 つのグラフを表示することができます。

フィールド

- Available Graphs For:：グラフ化できるコンポーネントを一覧表示します。
  - Blocks Used：FWSM で使用中のメモリ ブロックを表示します。
  - Blocks Free：FWSM の空きメモリ ブロックを表示します。
- 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 ボックスに表示されます。ここでタイプを追加することができます（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 ボックスで選択したエントリを Selected Graphs ボックスに移動します。
- Remove：Selected Graphs ボックスから、選択した統計タイプを削除します。
- Show Graphs：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウに選択した統計情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

CPU では、CPU の使用状況をグラフ形式で表示できます。1 つのフレームに最大で 4 つのグラフを表示することができます。

フィールド

- Available Graphs For:：グラフ化できるコンポーネントを一覧表示します。
  - CPU Utilization：FWSM の CPU の使用状況を表示します。

- 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 ボックスに表示されます。ここでタイプを追加することができます（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 ボックスで選択したエントリを Selected Graphs ボックスに移動します。
- Remove：Selected Graphs ボックスから、選択した統計タイプを削除します。
- Show Graphs：新しいグラフ ウィンドウまたは更新したグラフ ウィンドウに選択した統計情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			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

Memory では、メモリの使用状況をグラフ形式で表示できます。空きメモリと使用中のメモリをリアルタイムで監視できます。1 つのフレームに最大で 4 つのグラフを表示することができます。

フィールド

- Available Graphs For:：グラフ化できるコンポーネントを一覧表示します。
  - Free Memory：FWSM の空きメモリを表示します。
  - Used Memory：FWSM の使用中のメモリを表示します。
- 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 ボックスに表示されます。ここでタイプを追加することができます（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 ボックスで選択したエントリを Selected Graphs ボックスに移動します。
- Remove：Selected Graphs ボックスから、選択した統計タイプを削除します。
- Show Graphs：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウに選択した統計情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

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

APPENDIX A

仕様

この付録には、FWSM の仕様が一覧表示されています。次の項目を取り上げます。

スイッチのハードウェアおよびソフトウェアの互換性

FWSM をサポートするスイッチのモデルには、次のプラットフォームがあります。

- 次のコンポーネントを要件とする Catalyst 6500 シリーズのスイッチ。
  - Cisco IOS ソフトウェア（スーパーバイザ IOS）使用のスーパーバイザ エンジン *または* Catalyst オペレーティング システム（OS）。サポートされているスーパーバイザ エンジンおよびソフトウェア リリースの表 A-1 を参照してください。
  - Cisco IOS ソフトウェア使用の MSFC 2。サポートされている Cisco IOS ソフトウェア リリースの表 A-1 を参照してください。
- 次のコンポーネントを要件とする Cisco 7600 シリーズのルータ。
  - Cisco IOS ソフトウェア使用のスーパーバイザ エンジン。サポートされているスーパーバイザ エンジンおよびソフトウェア リリースの表 A-1 を参照してください。
  - Cisco IOS ソフトウェア使用の MSFC 2。サポートされている Cisco IOS ソフトウェア リリースの表 A-1 を参照してください。

（注） FWSM は、WAN ポートがスタティック VLAN を使用しないため、スイッチの WAN ポートへの直接接続をサポートしません。ただし、WAN ポートは、FWSM へ接続できる MSFC に接続できます。

表 A-1 では、スーパーバイザ エンジンのバージョンとソフトウェアを示しています。

表 A-1　FWSM 3.2 のサポート

	スーパーバイザ エンジン[1]
Cisco IOS ソフトウェア リリース	
12.2(18)SXF 以降	720, 32
12.2(18)SXF2 以降	2, 720, 32
Cisco IOS ソフトウェア モジュラリティ リリース	
12.2(18)SXF4	720, 32
Catalyst ソフトウェア リリース[2]	
8.5(3) 以降	2. 720, 32

1. FWSM は、スーパーバイザ 1 または 1A をサポートしていません。
2. スーパーバイザで Catalyst ソフトウェアを使用する場合は、上記のサポートされている Cisco IOS ソフトウェア リリースをどれでも MSFC で使用できます（スーパーバイザで Cisco IOS ソフトウェアを使用する場合も、同じリリースを MSFC で使用できます）。

ライセンス対象機能

FWSM は、次のライセンス対象機能をサポートしています。

- マルチセキュリティ コンテキスト。FWSM は、ライセンスのない計 3 つのセキュリティ コンテキストに対して、2 つのコンテキストと 1 つの管理コンテキストをサポートしています。4 つ以上のコンテキストには次のライセンスのいずれかを取得します。
  - 20
  - 50
  - 100
  - 250
- GTP/GPRS サポート。
- BGP スタブ サポート。

物理仕様

表 A-2 では、FWSM の物理仕様を示しています。

表 A-2　物理仕様

仕様	説明
帯域幅	スイッチ ファブリック モジュールへの 6-Gbps のパスを持つ CEF256 ラインカード（存在する場合）または 32-Gbps の共有バス。
メモリ	• 1 GB の RAM。 • 128 MB のフラッシュ メモリ。
スイッチごとのモジュール	スイッチごとに最大 4 つのモジュール。 フェールオーバーを使用する場合、2 つのモジュールがスタンバイ モードでも、スイッチごとに 4 つしかモジュールを持てません。

機能制限

表 A-3 では、FWSM の機能制限がリストされています。

表 A-3　機能制限

	コンテキスト モード	
仕様	**シングル**	**マルチ**
AAA サーバ（RADIUS および TACACS+）	16	コンテキストごとに 4 つ
フェールオーバー インターフェイスのモニタリング	250	すべてのコンテキスト合計で 250
フィルタリング サーバ（Websense Enterprise または Sentian を N2H2 で実行する）	16	コンテキストごとに 4 つ
ジャンボ イーサネット パケット	8500 バイト	8500 バイト
セキュリティ コンテキスト	該当なし	250 のセキュリティ コンテキスト（ソフトウェアのライセンスによる）。
Syslog サーバ	16	コンテキストごとに 4 つ すべてのコンテキスト合計で最大 16
VLAN インターフェイス		
ルーテッド モード	256	コンテキストごとに 100 つ FWSM 全体の VLAN インターフェイスの制限数は、すべてのコンテキスト合計で 1,000 です。コンテキスト間で外部インターフェイスを共有することができ、場合によっては、内部インターフェイスも共有できます。
透過モード	8 ペア	コンテキストごとに 8 ペア

管理対象のシステム リソース

表 A-4 では、FWSM の管理対象のシステム リソースをリストしています。リソース マネージャを使用して、コンテキストごとのリソースを管理できます。詳細については、P.7-12 の「リソース クラスの設定」を参照してください。

表 A-4　管理対象のシステム リソース

	コンテキスト モード	
仕様	**シングル**	**マルチ**
MAC アドレス（透過ファイアウォール モードのみ）	64 K	すべてのコンテキスト合計で 64 K
FWSM による接続を許可されるホスト、同時	256 K	すべてのコンテキスト合計で 256 K
インスペクション エンジン接続、レート	10,000/ 秒	すべてのコンテキスト合計で 10,000/ 秒
IPSec 管理接続、同時	5	コンテキストごとに 5 つ すべてのコンテキスト合計で最大 10
ASDM 管理セッション、同時[1]	5	コンテキストごとに最大 5 すべてのコンテキスト合計で最大 80
NAT 変換、同時	256 K	すべてのコンテキスト合計で 256 K
SSH 管理接続、同時[2]	5	コンテキストごとに 5 つ すべてのコンテキスト合計で最大 100
システム ログ メッセージ、レート	FWSM のターミナルまたはバッファへ送信されるメッセージの速度は 30,000/ 秒 syslog サーバへ送信されるメッセージの速度は 25,000/ 秒	FWSM のターミナルまたはバッファへ送信されるメッセージの速度は、すべてのコンテキスト合計で 30,000/ 秒 syslog サーバへ送信されるメッセージの速度は、すべてのコンテキスト合計で 25,000/ 秒
1 台のホストと他の複数台のホスト間の接続を含む[3,4]、任意の 2 つのホスト間の TCP または UDP 接続、同時およびレート	999,900[5] 100,000/ 秒	すべてのコンテキスト合計で 999,900[5] すべてのコンテキスト合計で 100,000/秒
Telnet 管理接続、同時[2]	5	コンテキストごとに 5 つ すべてのコンテキスト合計で最大 100 の接続。

1. ASDM セッションは、2 つの HTTPS 接続を使用します。1 つは常駐の監視用、もう 1 つは変更時にのみ使用されるコンフィギュレーション変更用です。たとえば、ASDM のセッション数のシステム制限値が 80 の場合は、HTTPS 接続数が 160 に制限されます。
2. 管理コンテキストでは、Telnet および SSH 接続が最大 15 まで使用できます。
3. 初期接続は合計接続数に含まれます。初期接続制限数を設定する場合、制限数を超える初期接続はカウントされません。
4. FWSM では、削除マークの付いた接続を削除するのに最大 500 ミリ秒かかる場合があります。削除中はその接続のトラフィックがドロップされるため、接続が削除されるまでは、同じ送信元ポートと宛先ポートを使用して、同じ宛先へ新しい接続を開始することはできません。ほとんどの TCP アプリケーションでは、逆並列接続で同一ポートが再利用されることはありませんが、RSH では同一ポートが再利用される場合があります。RSH または逆並列接続で同一ポートが再利用される他のアプリケーションを使用すると、FWSM はパケットをドロップする場合があります。
5. PAT では、各接続に個別の変換が必要なため、PAT を使用した効果的な接続制限は、変換制限（256K）になり、より高い接続制限ではありません。接続制限を使用するには、同一変換セッションを使用して複数の接続が許可される NAT を使用する必要があります。

固定システム リソース

表 A-5 では、FWSM の固定システム リソースをリストしています。

表 A-5　固定されたシステム リソース

	コンテキスト モード	
仕様	**シングル**	**マルチ**
AAA 接続、レート	80/ 秒	すべてのコンテキスト合計で 80/ 秒
ネットワーク アクセス許可のためにダウンロードされた ACE	3,500	すべてのコンテキスト合計で 3,500
ACL ロギング フロー、同時	32 K	すべてのコンテキスト合計で 32 K
エイリアス文	1 K	すべてのコンテキスト合計で 1 K
ARP テーブル エントリ、同時	64 K	すべてのコンテキスト合計で 64 K
DNS 検査、レート	5000/ 秒	すべてのコンテキスト合計で 5000/ 秒
グローバル文	4 K	すべてのコンテキスト合計で 4 K
検査文	32	コンテキストごとに 32
NAT 文	2 K	すべてのコンテキスト合計で 2 K
パケット リアセンブリ、同時	30,000	すべてのコンテキスト合計で 30,000 フラグメント
ルート テーブル エントリ、同時	32 K	すべてのコンテキスト合計で 32 K
Shun 文	5 K	すべてのコンテキスト合計で 5 K
スタティック NAT 文	2 K	すべてのコンテキスト合計で 2 K
TFTP セッション、同時[1]	999,100	すべてのコンテキスト合計で 999,100
URL フィルタリング要求	200/ 秒 では CPU 使用率は 50%	200/ 秒 ではすべてのコンテキスト合計の CPU 使用率は 50%
ユーザ認証セッション、同時	50 K	すべてのコンテキスト合計で 50 K
ユーザ許可セッション、同時	150 K ユーザごとに最大 15 セッション。	すべてのコンテキスト合計で 150 K ユーザごとに最大 15 セッション。

1. FWSM バージョン 1.1 では、TFTP セッション数は、1024 セッションに制限されていました。

ルール制限

FWSM では、システム全体でサポートされるルールの数が決まっています。この項では、機能ごとのデフォルト最大ルール数、機能間にルールを割り当てる方法、ルールをマルチコンテキスト間に分割する方法について説明します。次の項目を取り上げます。

デフォルトのルール割り当て

表 A-6 では、各ルール タイプの最大数をリストしています。

（注） 一部のアクセス ルールは、他のものよりメモリを多く使用します。アクセス ルールのタイプによっては、システムがサポートできる実際の制限は最大数よりも少なくなります。アクセス ルールとメモリ使用量の詳細については、P.17-3 の「アクセス ルールおよび EtherType ルールの最大数」を参照してください。

表 A-6　デフォルトのルール割り当て

	コンテキスト モード	
仕様	**シングル**	**12 個のプールを持つマルチ（パーティションごとの最大数）**
AAA ルール	6451	992
アクセス ルール	74,188	10,633
established コマンド[1]	460	70
フィルタ ルール	2764	425
ICMP、Telnet、SSH、HTTP ルール	1843	283
ポリシー NAT ACE[2]	1843	283
検査ルール	4147	1417
ルール合計	**92,156**	**14,173**

1. 各 **established** コマンドは、コントロール ルールとデータ ルールを作成するため、ルール合計の値は 2 倍になります。**established** コマンドは、CLI でのみサポートされているため、ASDM 内では設定できません。
2. この制限はリリース 2.3 より低くなっています。

マルチコンテキスト モードのルール

デフォルトで 12 のメモリ パーティションを持つマルチコンテキスト モードでは、各コンテキストが、表 A-6 にリストされている最大数をサポートします。コンテキストでサポートされている実際のルール数は、持っているコンテキスト数と設定したパーティション数によって異なります。コンテキスト間のメモリ分散についての詳細は、P.7-18 の「メモリ パーティションの設定」を参照してください。

パーティション数を減らすと、ルールの最大数が再計算され、12 のパーティションで使用可能な合計システム数と一致しない場合もあります。パーティションの最大ルール数を表示するには、「機能間のルールの再割り当て」の項を参照してください。

機能間のルールの再割り当て

1 つの機能から別の機能へルールを再割り当てできます。ルールを再割り当てするには、次の手順を実行します。

ステップ 1　再割り当ての計画ができるように現在使用されているルール数を表示するには、Command Line Interface ツールを使用して次のコマンドの 1 つを入力します。

- シングルモードまたはコンテキスト内で、次のコマンドを入力します。
  show np 3 acl count
- マルチコンテキスト モードのシステム実行スペースで、次のコマンドを入力します。
  show np 3 acl count *partition_number*

  パーティションの詳細については、P.A-7 の「マルチコンテキスト モードのルール」を参照してください。

たとえば、次の表には最大数 9216 に近い検査数（Fixup ルール）が表示されています。一部のアクセスリスト ルール（ACL ルール）を検査に再割り当てすることもできます。

```
show np 3 acl count

-------------- CLS Rule Current Counts --------------
CLS Filter Rule Count       :             0
CLS Fixup Rule Count        :          9001
CLS Est Ctl Rule Count      :             4
CLS AAA Rule Count          :            15
CLS Est Data Rule Count     :             4
CLS Console Rule Count      :            16
CLS Policy NAT Rule Count   :             0
CLS ACL Rule Count          :         30500
CLS ACL Uncommitted Add     :             0
CLS ACL Uncommitted Del     :             0
...
```

（注）　**established** コマンドは、管理とデータの 2 種類のルールを作成します。両方のタイプが表示されていますが、**established** コマンドの数を設定することで両方のルールを割り当て、各ルールの設定を個別には行いません。

established コマンドは、CLI でのみサポートされているため、ASDM 内では設定できません。

ステップ 2　機能間にルールを再割り当てするには、Configuration > Properties > Dynamic Resource Allocation へ移動します。マルチコンテキスト モードの場合は、この機能はシステム実行スペースでのみ使用できます。

ステップ 3　変更する各機能のフィールドに値を入力するか、デフォルトまたは最大値をドロップダウン リストから選択して、機能間にルールを再割り当てします。

マルチコンテキスト モードでは、このペインで*パーティションごと*のルールの割り当てを設定します。

設定したルール数、最大ルール数、使用可能なルール数が下の機能フィールドに表示されます。設定したルールのフィールドでは、機能の新しい値を入力するとダイナミックに更新します。Control ルールと Data ルールの両方をアカウンティングするには、Established ルールの数を 2 倍にします。**established** コマンドは、CLI でのみサポートされているため、ASDM 内では設定できません。

ステップ 4　**Apply** をクリックします。

新しい制限はすぐに反映されます。

INDEX

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

て

と

な

に

ね

は

ひ

ふ

よ

ら

り

る

れ

ろ