VPN 3000 シリーズ コンセントレータ管理者用 ASA への移行手順 Version 7.2

Text Part Number: OL-10669-01-J

CONTENTS

このマニュアルについて

このマニュアルでは、Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）ソフトウェアの多数の基本的な VPN 機能を設定する方法について説明します。ほとんどの場合、CLI を使用した設定手順とデバイス マネージャを使用した設定手順の両方を示します。各機能の説明では、例を 1 つ以上使用し、基本的で簡潔なシナリオによって設定手順を解説しています。原則として、CLI による手順と ASDM による手順では同じ値を使用しています（いくつか例外はあります）。

対象読者

このマニュアルは、バーチャル プライベート ネットワーク用に ASA の設定および構成を行うシステム エンジニア（SE）およびネットワーク管理者を対象としています。こうした SE および顧客は、VPN 3000 コンセントレータの観点からはバーチャル プライベート ネットワークを理解していますが、ASA ソフトウェア環境で通常の作業を実行する際にはガイダンスが必要です。

このマニュアルは、すぐに新しいシステムで迅速に作業できるようになるために役立ちます。読者は、ネットワーク機器、ネットワークの基本的な概念、バーチャル プライベート ネットワーク、および VPN 3000 Concentrator Manager を理解していることが必要です。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章番号	タイトル	説明
第 1 章	機能の相違	VPN 3000 コンセントレータの機能と ASA の機能を比較します。
第 2 章	ASA システムの導入	VPN 3000 コンセントレータと異なる ASA の主な機能について説明します。
第 3 章	設定の開始	ASDM のスタートアップ ウィザードと VPN ウィザードについて説明し、ウィザードを使用する前に収集する必要がある情報を示します。また、VPN 3000 コンセントレータの Getting Started プログラムとこれらのウィザードを比較します。
第 4 章	基本的な IPSec VPN トンネルの構築	CLI コマンドおよび Adaptive Security Device Manager（ASDM）を使用して VPN LAN 間トンネルおよびリモート アクセス トンネルを設定する方法を示します。また、デジタル証明書の登録方法についても説明します。
第 5 章	選択したユーザ管理タスクの実行	スプリット トンネリング、クライアント ファイアウォールの設定方法および RADIUS を使用した認証方法を示します。
第 6 章	トラフィック管理の設定	ロード バランシングおよびサービス機能の品質の設定方法を示します。
付録 A	VPN 3000 シリーズ コンセントレータと ASDM の項目の比較	VPN 3000 Concentrator Manager の設定項目および管理項目の ASDM へのマッピングを示します。
付録 B	VPN 3000 シリーズ コンセントレータと ASA のデバッグ レベルまたは イベント レベルの比較	VPN 3000 Concentrator Manager のロギング セキュリティ レベルの ASA へのマッピングを示します。

関連資料

このマニュアルは、次のユーザ ガイドと併せてご使用ください。

- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASDM Release Notes*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Quick Start Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Release Notes for Cisco Secure Desktop*
- *Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series*
- *Cisco Security Appliance Logging Configuration and System Log Messages*

表記法

このマニュアルは、次の表記法を使用しています。

表記法	説明
太字	ユーザのアクションおよびコマンドは、**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で示しています。
screen フォント	システムが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の **screen** フォント	入力する必要のある情報は、コマンドライン インターフェイスで太字の **screen** フォントで示しています（たとえば、**vpnclient stat**）。

（注）は、次のように表しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意は、次のように表しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項または条件を警告します。

システムの設定および管理を行う際には、他に指示が示されていなければ次の形式でデータを入力します。

データの種類	形式
IP アドレス	IP アドレスは、4 バイトのドット付き 10 進数で表します（たとえば、192.168.12.34）。例で示したように、バイト位置の先頭にあるゼロは省略できます。
サブネット マスクとワイルドカード マスク	サブネット マスクは、4 バイトのドット付き 10 進数で表します（たとえば、255.255.255.0）。ワイルドカード マスクも同じように表します（たとえば、0.0.0.255）。例で示したように、バイト位置の先頭にあるゼロは省略できます。
MAC アドレス	MAC アドレスは、6 バイトの 16 進数で表します（たとえば、0001.03cf.0238）。
ホスト名	ホスト名は、正しいネットワーク ホスト名またはエンドシステム名で表します（たとえば、VPN01）。スペースは使用できません。ホスト名は、ネットワークで特定のシステムを一意に識別する必要があります。
テキスト文字列	テキスト文字列は、英数字（大文字および小文字）を使用します。ほとんどのテキスト文字列は、大文字と小文字を区別します（たとえば、simon と Simon は異なるユーザ名を表します）。通常、テキスト文字列の最大長は 48 文字です。
ポート番号	ポート番号は、0 から 65535 までの 10 進数を使用します。番号にカンマまたはスペースは使用できません。

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/univercd/home/home.htm

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

マニュアルの発注方法（英語版）

英文マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

シスコ製品の英文マニュアルは、次の方法で発注できます。

- Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、Ordering ツールからシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/en/US/partner/ordering/index.shtml
- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

テクニカル サポート

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。Cisco.com の Cisco Technical Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support Web サイト

Cisco Technical Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間 365 日、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） Web または電話でサービス リクエストを発行する前に、Cisco Product Identification（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、Cisco TAC のエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、Cisco TAC のエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- 『*Cisco Product Catalog*』には、シスコシステムズが提供するネットワーキング製品のほか、発注方法やカスタマー サポート サービスについての情報が記載されています。『*Cisco Product Catalog*』には、次の URL からアクセスしてください。

  http://cisco.com/univercd/cc/td/doc/pcat/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンライン サービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

機能の相違

このマニュアルは、VPN 3000 シリーズ コンセントレータの現行のユーザがセキュリティ アプライアンスに移行する場合に役立ちます。このマニュアルでは、2 つのデバイス、およびデバイスに付属するソフトウェアの違いについて説明します。セキュリティ アプライアンスの機能の詳細については、次に示すマニュアルを参照してください。

- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5505 Getting Started Guide*
- *Cisco ASA 5550 Getting Started Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 シリーズ製品 CD*
- *Release Notes for Cisco Secure Desktop*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASDM オンライン ヘルプ*
- *Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series*
- *Cisco ASDM Release Notes*

セキュリティ アプライアンスは、VPN 3000 シリーズ コンセントレータのほとんどの機能を実装しますが、状況によっては、それらの機能の設定方法や使用方法が VPN 3000 の従来の方法と異なる場合があります。この章では、セキュリティ アプライアンス ソフトウェアと VPN 3000 シリーズ コンセントレータのソフトウェアの具体的な違いをリストで示します。VPN 3000 Concentrator Manager と Adaptive Security Appliance Device Manager のグラフィカル ユーザ インターフェイスの違いについては、付録 A「VPN 3000 シリーズ コンセントレータと ASDM の項目の比較」にリストを示します。

VPN 3000 コンセントレータと ASA Version 7.1 の機能の比較

表 1-1 は、VPN 3000 シリーズ コンセントレータの機能と、ASA Version 7.1 までで使用できる機能の比較を要約しています。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較

機能名	VPN 3000	ASA
デフォルトの暗号化アルゴリズム	3DES がすべての暗号化操作のデフォルトです。いずれの暗号化アルゴリズムでもライセンスは必要ありません。	DES が「基本」の暗号化アルゴリズムです。3DES および AES には「追加」ライセンスが必要です。
IKE ネゴシエーション	IKE フェーズ 1 ID は、グループ名（受信専用）、IP アドレス、または証明書 DN のいずれかです。送信されるフェーズ 1 ID は、VPN 3000 コンセントレータが事前共有鍵または証明書のどちらのネゴシエーションを行っているかによって異なります。	ASA は IKE フェーズ 2 の複数のトランスフォームをサポートしており、IKE フェーズ 1 の複数の提案事項を送信できます。IKE フェーズ 1 ID は設定可能で、複数のオプションがあります。
フェーズ 2 データ整合性のデフォルト設定	フェーズ 2 データ整合性のデフォルト設定は MD5 です。	フェーズ 2 データ整合性値のデフォルト設定は、「off」です。この設定により、以前のバージョンの PIX および IOS との互換性が保たれます。VPN 3000 コンセントレータと連携するようにセキュリティ アプライアンスを設定する場合、状況によっては、フェーズ 2 データ整合性をイネーブルにする必要があります。ハッシュ アルゴリズムのいずれか（SHA1 または MD5）を使用して、IPSec データが認証されていることを*保証*するには、ネットワーク管理者はフェーズ 2 データ整合性をオンにする必要があります。 フェーズ 2 データ整合性をイネーブルにするには、この表の次にある項 P.1-12 の「ASA のフェーズ 2 データ整合性のイネーブル化」の手順に従って、使用している暗号マップに関連付けられたトランスフォーム セットで SHA1 または MD5 をオンにします。これらのコマンドは、ハッシュ アルゴリズムとして SHA/HMAC-160 をイネーブルにします。
低メモリ アクション	低メモリ状態は、メモリが不足しているときに新しく接続しないようにします。	デバイスのメモリが不足しているときに、新しく接続しないようにします。「低メモリ」状態は存在しません。
「正常リブート」コンフィギュレーション	「正常リブート」機能をサポートしています。この機能は、一部のアプリケーションが適正にクリーンアップされるまで、VPN 3000 コンセントレータをリブートしないようにします。IKE の場合、すべてのトンネルがダウンになるまでコンセントレータはリブートされません。	「正常リブート」機能は、VPN 3000 の場合と同じように動作しますが、設定方法が異なります。最初に、サブシステムがクリーンアップされるまで待機してからリブートを行うようにリブートを設定します。次に、リブートの通知を受け取り、すべてのトンネルがダウンしたときにリブートを許可するように、IKE を設定します。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
ハブアンドスポーク構成のサポート	ハブアンドスポーク構成をサポートしています。	ハブアンドスポーク構成をサポートしています。ハブアンドスポーク構成では、暗号化されたトラフィックはインターフェイスで受信されてそこで復号化され、ファイアウォール規則の適用後、同じインターフェイスからクリア テキストで送信されます。このような「クライアント U ターン」リモート アクセス接続は、セキュリティ アプライアンスの外部インターフェイスで終端できます。そのため、リモート アクセス ユーザの VPN　トンネルからインターネットへのトラフィックは、ファイアウォール規則の適用後、受信されたのと同じインターフェイスから送信されます。
DoS 攻撃（サービス拒絶攻撃）からの保護	DoS 攻撃を防ぐために、アグレッシブ モードをブロックできます。 DHCP リレーもディセーブルにできます。	DoS 攻撃を防ぐために、アグレッシブ モードをブロックできます。
CLI	メニュー主導の選択。製品の主要なインターフェイスは GUI です。	PIX/IOS に類似の文シンタックス
グラフィカル ユーザ インターフェイス	HTML ベースの管理アプリケーションを使用します。	Java ベースの管理アプリケーションを使用します。
パケット検査	VPN 3000 コンセントレータでは、通過するデータは検査されません。	ASA はファイアウォールなので、すべてのデータの検査と、一定レベルのインテリジェント検査を実行します。
ユーザの設定	User Management でユーザを設定します。	Properties > Device Administration でユーザを設定します。
AIP SSM（Advanced Inspection and Prevention Security Services Module）	利用できません。	使用できる AIP SSM 機能は、ASA モデルによって異なります。
ロギング	13 段階のイベント ロギングの重大度を許可します。	次の 2 つのロギング メカニズムをサポートしています。 • syslog。レベルは 1 ～ 7 です。VPN 3000 イベント ロギング機能と同等です。 • dbgtrace。このトラブルシューティング インターフェイスではレポート機能が制限されており、たとえば dbgtrace はコンソールにしか表示されません。dbgtrace のロギング レベルは、1 ～ 11、および 254 と 255 です（これらのレベルの説明については、付録 B「VPN 3000 シリーズ コンセントレータと ASA のデバッグ レベルまたは イベント レベルの比較」を参照）。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
ワイルドカード マスク	VPN 3000 コンセントレータは、0.0.0.255 のバリエーションであるワイルドカード マスク、およびワイルドカード マスクの逆、つまり 255.255.255.0 のバリエーションであるネットワーク マスクを使用します。 VPN 3000 フィルタおよびダウンロード可能な ACL は、ワイルドカード ベースです。	セキュリティ アプライアンスでは、常にネットワーク マスクが予期されているため、ワイルドカード マスクは正しく動作しません。 • VPN 3000 コンセントレータからセキュリティ アプライアンスに移行する場合、ネットワーク管理者は、ワイルドカードではなくネットマスクを使用してセキュリティ アプライアンスの暗号およびインターフェイス ACL を設定する必要があります。 • 既存の VPN 3000 RADIUS DACL コンフィギュレーションを、ネットマスクに変更する必要があります。 • VPN 3000 とセキュリティ アプライアンスが混在して導入されている場合に RADIUS から ACL をダウンロードするときは、VPN 3000 がワイルドカードを使用して DACL を取得し、セキュリティ アプライアンスがネットマスクを使用して DACL を取得できるよう、いくらかのセグメンテーションが必要になります。
セッション タイムアウト	TCP 接続を確立したアプリケーションは、データを渡すことがなくても、無制限にアップ状態にとどまることができます。この動作は VPN 3000 コンセントレータでは許容されますが、セキュリティ アプライアンスでは許容されません。	ASA は TCP 接続を監視して、接続がアクティブであることを確認します。接続が非アクティブな時間が一定の時間（設定可能）に達すると、ASA は TCP 接続を強制的に終了します。長時間使用されていないトンネルを終了するのと同様です。セキュリティ アプライアンスでは、理由が示されることなく、これらのセッションはタイムアウトになります。このため、アプリケーションが続行するにはセッションを再確立する必要があります。
PKI および X.509 証明書のサポート	トラストポイントの概念はありません。	次のように、大きな概念上の変更、および多数のシンタックスの変更があります。 • トラストポイントの新しい概念、およびトラストポイントに証明書を関連付ける方法。 • VPN 3000 PKI 機能が追加された IOS ベースの PKI 機能のサポート。
	RSA 鍵の最大長は 2K です。	暗号化 / 復号化の操作では、セキュリティ アプライアンスは長さが最大 4K の RSA 鍵を処理できます。
	X.509 証明書を使用した VPN クライアント認証をサポートしています。	X.509 証明書のサポートには、n ティア証明書チェーン（複数レベルの認証局階層を使用する環境用）と、手動登録（オフライン認証局を使用する環境用）のサポートが含まれています。ASA は、Cisco IOS で導入された新しい認証局である、ライトウェイト X.509 認証局もサポートしています。この認証局は、PKI がイネーブルになっているサイトツーサイト VPN 環境のロールアウトを簡略化するように設計されています。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
	DSA 鍵と RSA 鍵をサポートしています。	Version 7.0.x と 7.1.x では、DSA 鍵と RSA 鍵をサポートしています。Version 7.2(1) 以上では、RSA 鍵のみをサポートします。
WebVPN	すべてのモデルで設定および使用できます。最新の VPN 3000 コンセントレータ Release 4.7 で使用できる機能を提供します。次の機能が含まれます。 • Cisco Secure Desktop • SSL VPN Client • ネットワーク アドミッション制御 • NTLM 認証 • Citrix • PDA サポート	WebVPN のサポートは、VPN 3000 シリーズ コンセントレータより広い範囲を提供しています。次のサポートが含まれます。 • Cisco Secure Desktop • SSL VPN Client • ネットワーク アドミッション制御 • 認証と認可に関する機能拡張 • Citrix サポート • PDA サポート • シングル サインオン • WebVPN パフォーマンスの最適化 • CIFS ファイルの文字符号化の WebVPN サポート • WebVPN と SSL VPN クライアントの接続の圧縮 • WebVPN 接続のアクティブ / スタンバイ ステートフル フェールオーバー 詳細については『*Cisco ASA 5500 Series Release Notes*』を参照してください。 **注**：WebVPN は、PIX ハードウェアでは利用できません。
SSL VPN Client	Keep Cisco SSL VPN Client 機能が含まれます。この機能は、SVC 常時インストールをイネーブルにするか、または SVC 自動アンインストール機能をディセーブルにします。SVC は後続の SVC 接続に備えてリモート コンピュータにインストールされたまま残り、リモート ユーザの SVC 接続時間を短縮します。	ASA は、Keep Cisco SSL VPN Client（VPN 3000 シリーズ コンセントレータ) の名前を Keep Installer on Client System に変更します。 SVC サポートは、たとえば以下の点で VPN コンセントレータのサポートより優れています。 • 圧縮：SVC 接続上の圧縮をイネーブルまたはディセーブルにします。 • 鍵再ネゴシエーション設定：セキュリティ アプライアンスと SVC が鍵の再生成を行うと、暗号鍵と初期ベクトルを再ネゴシエーションし、接続のセキュリティを強化します。 • デッド ピア検知：Dead Peer Detection（DPD; デッド ピア検知）によって、ピアが応答しない状態、または接続が失敗した状態をセキュリティ アプライアンスまたは SVC がすばやく検出することが保証されます。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
ライセンス	ライセンスは必要ありません。	ハードウェア プラットフォームによっては、個別のオプション ライセンスを基本ライセンスに追加することにより、追加の機能にアクセスできます。ハードウェア プラットフォームに見合ったライセンスを独自に組み合せることができます。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の付録 A を参照してください。
AAA	基本グループ、グループ、およびユーザの概念を使用します。	• ASA には、基本グループの代わりに 3 つのデフォルト トンネル グループがあります。これは、IPSec リモート アクセス、LAN 間 IPSec、および WebVPN の各接続タイプに対応しています。デフォルト グループ ポリシーは 1 つしかありません。証明書ベースのトンネルでデフォルト グループを基本グループとして使用することはできません。 • トンネル グループおよびグループ ポリシーの機能は、VPN 3000 とは異なる方法で分割されています。一部のアトリビュートは、トンネル グループに移動されました。これらのアトリビュートは、外部 AAA サーバでは設定できません。 • 外部グループで使用できないアトリビュートは、次のとおりです。 — strip-realm — peer-id-validate — authorization-required — authorization-dn-attributes — authentication server type selection — authorization server type selection — radius-with-expiry
	ハイブリッド サーバ グループをサポートしています（つまり、1 つのグループに異なるタイプのサーバを配置できます）。	サーバ グループの概念を使用します。1 つのサーバ グループ内のサーバはすべて同じタイプにする必要があります。
	フォールバック メカニズムはありません。	新しいフォールバック メカニズム。ネームド サーバが使用できない場合の LOCAL へのフォールバックが含まれます。
	管理トラフィックのアカウンティングはありません。	強化された AAA 機能。管理トラフィックのアカウンティングが含まれます。
	RADIUS アカウンティング データは、単一のサーバに送信されます。	同時 RADIUS アカウンティングをサポートしています。アカウンティング メッセージを単一サーバに送信するか（Single モード）、グループ内のすべてのサーバに送信するか（Simultaneous モード）を指定できます。
IPSec	トンネル型 ESP（ESP トンネル内の ESP）をサポートしていません。	トンネル型 ESP をサポートしています。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
オブジェクト グループ	使用されていません。その代わり、VPN 3000 はネットワーク リストを使用して、コンフィギュレーションを簡略化します。	オブジェクト グループを使用して、アクセス リストの作成とメンテナンスを簡略化します。
グループ アトリビュート：グループ ロック	グループ ロック機能は、イネーブルかディセーブルのいずれかです。イネーブルにすると、VPN 3000 は、VPN クライアントが接続を確立するときに使用したグループ名が、ユーザに割り当てられたグループ名と同じかどうかをチェックします。同じでない場合、接続はドロップされます。同じである場合、接続は許可されます。	ASA では、group-lock アトリビュートはグループ ポリシーの一部であり、パラメータがとる値はトンネル グループの実際の名前です。group-lock がグループ ポリシーに存在する場合、ASA は接続中に、VPN クライアントで使用されたグループ名が、group-lock アトリビュートにあるトンネル グループ名と同じかどうかをチェックします。
ロード バランシング	Cisco VPN Client（Release 3.0 以降）、Cisco VPN 3002 Hardware Client（Release 3.5 以降）、または Cisco PIX 501/506E（Easy VPN クライアントとして動作）で開始されたリモート セッション用にサポートされています。 ロード バランシングは、IPSec クライアントと WebVPN セッションの両方で機能します。	ASA5520 以上のシステムでのみ使用できます。PIX ハードウェアまたは ASA 5505 または 5510 システムでは使用できません。
モード	同等の概念はありません。	• 仮想コンテキスト、および透過モードとルーテッド モードをサポートしています。 • VPN は単一ルーテッド モードでのみ動作します。例外として、透過モードでも、ASA に対する 1 つの管理セッションを実行できます。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
Quality of Service（QoS）	すべてのモデルで設定できます。	ASA 5520 以上のモデルでのみ設定できます。PIX ハードウェア、ASA 5505 および 5510 では使用できません。
	最大レートでの帯域幅ポリシングを提供します。最大レートを超えるトラフィックはドロップされます。	トンネル型または非トンネル型を問わず、すべてのトラフィックにレート制限（ポリシング）を適用できますが、優先クラス トラフィックにはレート制限を適用できません。ASA では、最大レートを超えるトラフィックも送信されますが、レートは最大レートに抑制されます。
	• トンネル トラフィックの最小帯域幅レートを保証します。この結果、1 人のユーザによってインターフェイスでの回線レートが過剰になり他のユーザが使用できる帯域幅が不足することがなくなります。 • 予約されている未使用の帯域幅を、「盗む」ことを許可します。	帯域幅予約はサポートされていません。最小帯域幅保証はありません。
	低遅延キューイングはありません。	• Low-Latency Queueing（LLQ; 低遅延キューイング）を使用します。その結果、デバイスを経由する特定のトラフィック タイプの優先順位を設定できます。LLQ はレート制限*されません*。 • LLQ トラフィック以外のすべてのトラフィックは、「ベストエフォート」と見なされます。すべての LLQ トラフィックにサービスが提供された後、このトラフィックにベストエフォート サービスが提供されます。上限は、ベストエフォート キューの項目数です。ベストエフォート キューがいっぱいになると、以降のベストエフォート トラフィックはドロップされます。
	トンネル トラフィックにのみ適用されます。通常は、パブリック インターフェイスに適用されます。	トンネルグループ情報または ACL のいずれかに基づいて QoS を設定できます。
VPN を許可するためのファイアウォール機能のロック解除	VPN 3000 には適用されません。	ロック解除は必要ありません。1 つのインターフェイスで ISAKMP をイネーブルにすると、セキュリティ アプライアンスはトンネルをネゴシエートできるようになります。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
フィルタ /ACL	フィルタは、トラフィックに適用される規則で構成されています。これらの規則は、フィルタに配置された順序で適用されます。規則で指定したすべてのパラメータにパケットが一致すると、その規則で指定されたアクションがシステムによって実行されます。一致しない規則パラメータが 1 つでもあれば次の規則が適用され、その後も同様に続行されます。一致する規則がない場合は、フィルタで指定されたデフォルトのアクションがシステムにより実行されます。 • WebVPN では、フィルタを使用して、指定された URL へのアクセスを制御します。 • VPN 3000 コンセントレータで使用するフィルタを、VPN コンセントレータまたは外部の RADIUS サーバで設定できます。 フィルタを設定するには次の 2 つの手順に従います。 • 基本フィルタ パラメータ（名前、デフォルト アクションなど）の設定 • フィルタへの規則の割り当て インターフェイスにフィルタを適用します。これらのフィルタは、インターフェイスを経由するすべてのトラフィックを管理するため、セキュリティ上、最も重要なフィルタです。グループとユーザにもフィルタを適用することにより、インターフェイスを経由するトンネル型トラフィックを管理します。	• ACL はすべてのトラフィックを管理します。 • Cisco ASA 5500 シリーズ セキュリティ アプライアンスは、発信 ACL と時間ベース ACL（既存の着信 ACL サポートの上に構築）をサポートしています。管理者は、トラフィックがインターフェイスで受信されるかインターフェイスから送信されるときに、アクセス コントロールを適用できます。時間ベースのアクセス コントロール リストを使用すると、管理者は、特定の ACL エントリをアクティブにする時間を定義することにより、リソースの使用方法をより強力に制御できます。管理者は新しいコマンドを使用して、時間範囲を定義し、それらの時間範囲を特定の ACL に適用できます。 • 特定の ACL エントリに「active」または「inactive」キーワードを追加することにより、それらのエントリをイネーブルまたはディセーブルにできます（キーワードのない規則はアクティブです）。このトラブルシューティング ツールを使用すると、ACL を簡単に微調整できます。

VPN 3000 コンセントレータと ASA Version 7.2 の機能の比較

表 1-2 に、ASA が VPN コンセントレータからさまざまな方法で実装する新しい機能の比較を要約しています。

表 1-2　VPN コンセントレータと ASA Version 7.2 の新しい機能の比較

機能名	VPN 3000	ASA
L2TP、L2TP over IPSec、および PPTP のサポート	L2TP、L2TP over IPSec、および PPTP 機能をサポートしています。	Release7.2(1) では、L2TP over IPSec のサポートが追加されています。ASA では、L2TP 機能も PPTP 機能もサポートされません。 • 1 つまたは複数の NAT デバイスへの複数のクライアントへのリモート　アクセス L2TP-over-IPSec 接続を正常に確立する機能が含まれます。 • グループ　ポリシーまたはユーザ　ベースの L2TP over IPSec を設定します。 • さらに、IPSec トランスフォーム セットをトンネル モードでなくトランスポート モードで設定する必要があります。
ネットワーク アドミッション制御	NAC は、PPP、IPSec などのアクセス方法が提供する ID ベースの検証に加えて、ピアをそのポスチャまたは状態に基づいて検証する方法を提供します。	NAC の ASA サポートには、VPN 3000 コンセントレータ シリーズが提供するすべての NAC 機能が含まれます。
	• ステートフル フェールオーバーはサポートされません。	• NAC ステートフル フェールオーバーは、セキュリティ アプライアンス上の VPN ステートフル フェールオーバー機能を使用します。フェールオーバーが発生すると、それまでアクティブ ユニットに接続されていた VPN 接続がスタンバイ ユニットに接続されます。スタンバイ ユニットの状態変化によって、該当するすべての VPN セッションのフル ポスチャ検証がトリガーされます。
	• グループ ベースまたはユーザ ベースの NAC セッションを初期設定または再検証できます。	• トンネル　グループに関連付けられたすべての NAC セッションを初期設定または再検証できます。
	• グループ ベースまたはユーザ ベースのポスチャ検証の対象から除外するオペレーティング システムを設定できます。	• グループ　ポリシーごとに、ポスチャ検証の対象から除外するオペレーティング システムのリストを設定できます。
証明書失効チェック	CRL をチェックし、証明書のステータスを確認します。	CRL チェックに加えて、Online Certificate Status Protocol（OCSP）もサポートします。OCSP は、CRL チェックに代わって X.509 デジタル証明書の失効ステータスを確認します。クライアントが大きな証明書失効リスト全体をダウンロードする必要はなく、OCSP が Validation Authority（VA; 検証局）の証明書ステータスを確認します。OCSP は、個々の証明書のステータスについてこの検証局に照会します。

表 1-2　VPN コンセントレータと ASA Version 7.2 の新しい機能の比較

機能名	VPN 3000	ASA
RIPv2　アクティブおよびパッシブ	サポートされています。	ASA は、現在 RIP Version 1 と RIP Version 2 をサポートします。セキュリティ アプライアンス上で唯一の RIP ルーティング プロセスをイネーブルにできます。RIP ルーティング プロセスをイネーブルにすると、すべてのインターフェイス上で RIP がイネーブルになります。セキュリティ アプライアンスは、デフォルトで RIP Version 1 アップデートを送信し、RIP Version 1 と Version 2 のアップデートを受け入れます。
DDNS	サポートされていません。	ダイナミック DNS（DDNS）アップデート方法を作成し、必要な任意の頻度で DNS サーバ上の Resource Records（RR）をアップデートするように設定できます。 DDNS は DHCP を補足します。DHCP を使用すると、ユーザはクライアントに再利用可能な IP アドレスを動的かつ透過的に割り当てることができます。さらに、DDNS はダイナミック アップデートおよび DNS サーバ上の名前 / アドレス マップとアドレス / 名前マップの同期を可能にします。このバージョンにより、セキュリティ アプライアンスは DNS レコード アップデートのための IETF 標準をサポートします。
Zone Labs Integrity サーバ	Zone Labs Integrity システムを導入するネットワーク内のセキュリティ アプライアンスは、リモート VPN クライアントにセキュリティ ポリシーを強制的に適用するように設定できます。	ASA が実装するこの機能は、VPN コンセントレータと次のように異なります。 • アプライアンス SSL 証明書を受信する場合に、Integrity サーバが接続するセキュリティ アプライアンス上の特定のポートを設定できます。 • Integrity サーバ通信に使用するセキュリティ アプライアンス上のインターフェイスを指定できます。

ASA のフェーズ 2 データ整合性のイネーブル化

ハッシュ アルゴリズム（SHA1 または MD5）のいずれかを使用して IPSec データが認証されていることを保証するには、ネットワーク管理者はフェーズ 2 データ整合性をオンにする必要があります。フェーズ 2 データ整合性をイネーブルにするには、次の手順に従って、使用している暗号マップに関連付けられたトランスフォーム セットで SHA1 または MD5 をオンにします。これらのコマンドは、ハッシュ アルゴリズムとして SHA/HMAC-160 をイネーブルにします。

（注） 次の説明では、IKE と ISAKMP は同等です。VPN のマニュアルでは IKE が使用され、ASA では ISAKMP が使用されます（PIX と同様）。ASA では、すべてのコマンドが **isakmp** を使用します。

ステップ 1　使用しているトランスフォーム セットの SHA/HMAC-160 をイネーブルにします。

crypto ipsec transform-set *transform-set-name* **esp-3des esp-sha-hmac**

ステップ 2　使用している暗号マップにトランスフォーム セットをバインドします。

crypto map *map-name seq-num* **set transform-set** *transform-set-name*

次の例では、ttt という名前のトランスフォーム セットで SHA1 をイネーブルにし、ttt を abc という名前の暗号マップにバインドします。シーケンス番号（seq-num）は 1 です。

```
hostname(config)# crypto ipsec transform-set ttt esp-3des esp-sha-hmac
hostname(config)# crypto map abc 1 set transform-set ttt
hostname(config)#
```

ASA システムの導入

この章では、VPN 3000 コンセントレータと Adaptive Security Appliance（ASA; 適応型セキュリティアプライアンス）の主な相違点、特に VPN について説明します。この章は、次の項で構成されています。

- セキュリティ ポリシー機能の概要
- ユーザ管理の相違点
- ASA での PKI 実装
- インターフェイスごとの ASDM セッションおよび WebVPN セッション

セキュリティ ポリシー機能の概要

ASA は、シスコの最も強力なファイアウォールである VPN と侵入保護機能とを結合します。

- ASA は、Web VPN など、VPN 3000 コンセントレータでサポートされているソフトウェア機能のほとんどを提供します。WebVPN には、PIX ファイアウォールではなく ASA デバイス上で動作している ASA ソフトウェアが必要です。
- ASA は、より高速なインターフェイス（10/100/1000）と追加インターフェイス（4）を提供し、追加セキュリティ サービス用のスロットも用意された拡張可能なハードウェアです。
- オペレーティング システムでは IOS に類似の CLI コマンドを使用します。このコマンドは、より強力で柔軟性があり、VPN 3000 コンセントレータのメニューベースのコマンドライン インターフェイスを拡張し、スクリプトを使用して設定プロセスや監視プロセスを自動化する機能を追加します。CLI コマンドは、VPN コンセントレータから ASA に移行した機能をサポートしています。多数の新しいコマンドが VPN 機能専用に設計されています。CLI コマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。
- ASA のパフォーマンスは VPN 3000 コンセントレータのものより優れています。
- ASA はスケーラビリティと投資保護を提供します。同一デバイス内で複数のサービスを使用可能で、後でインターフェイスやサービスを追加することによって拡張できます。
- Adaptive Security Device Manager ソフトウェアは、ASA システムにマルチコンテキスト管理インターフェイスを提供します。

次の項では、ASA と VPN 3000 コンセントレータの概念上の主な相違点を説明します。

ユーザ管理の相違点

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）のセキュリティを管理し、セキュリティ アプライアンスを設定する際は、グループとユーザが中心的な概念になります。グループとユーザにより、VPN へのユーザ アクセスおよび VPN の使用を決定するアトリビュートが指定されます。*グループ*は複数ユーザの集合で、単一のエンティティとして扱われます。*ユーザ*は、自分のアトリビュートを*グループ ポリシー*から取得します。*トンネル グループ*は、特定の接続のグループ ポリシーを特定します。特定のグループ ポリシーをユーザに割り当てない場合、当該接続のデフォルト グループ ポリシーが適用されます。VPN 3000 コンセントレータの場合と異なり、基本グループはありません。

トンネル グループおよびグループ ポリシーを使用することで、システム管理が簡略化されます。セキュリティ アプライアンスにより、設定タスクの効率化に役立つデフォルト LAN 間トンネル グループ、デフォルト リモート アクセス トンネル グループ、デフォルト WebVPN トンネル グループ、およびデフォルト グループ ポリシー（DfltGrpPolicy）が提供されます。デフォルトのトンネル グループおよびグループ ポリシーは、多くのユーザが共通して使用できる可能性のある設定値を提供します。ユーザを追加するときは、グループ ポリシーからパラメータを「継承」するように設定できます。これで、多数のユーザの VPN アクセスをすばやく設定できます。

VPN ユーザすべてに同一の権限を付与するのであれば、特定のトンネル グループまたはグループ ポリシーを設定する必要はありません。しかし実際には、VPN をそのように動作させることはほとんどありません。たとえば、財務グループにプライベート ネットワークの一部へのアクセスを許可し、顧客サポート グループに別の部分へのアクセスを、MIS グループにその他の部分へのアクセスを許可する場合があります。さらに、MIS グループの特定のユーザ数人に、他の MIS ユーザからアクセスできないシステムへのアクセスを許可する場合もあります。トンネル グループとグループ ポリシーには柔軟性があり、このような設定をセキュアに実行できます。

(注)　セキュリティ アプライアンスには、ネットワーク リストのスーパーセットであるオブジェクト グループの概念も含まれます。オブジェクト グループを使用すると、ネットワークだけでなくポートへの VPN アクセスも定義できます。ACL は、グループ ポリシーやトンネル グループよりも、オブジェクト グループに関連があります。

ASA トンネル グループ

トンネル グループは、トンネル接続ポリシーを決定するレコードのセットで構成されます。これらのレコードは、接続情報の送信先であるアカウンティング サーバ（存在する場合）だけでなく、トンネル ユーザの認証先サーバを特定します。さらに、接続のデフォルト グループ ポリシーを特定します。これらのレコードには、プロトコル固有の接続パラメータが含まれています。トンネル グループには、トンネル自体の作成に関連する少数のアトリビュートがあります。トンネル グループには、ユーザ指向アトリビュートを定義するグループ ポリシーへのポインタが含まれています。

セキュリティ アプライアンスには、LAN 間接続用の DefaultL2LGroup、リモート アクセス接続用の DefaultRAGroup、WebVPN 接続用の DefaultWEBVPNGroup というデフォルト トンネル グループがあります。これらのデフォルト トンネル グループは変更できますが、削除はできません。また、環境に固有のトンネル グループを 1 つ以上作成できます。トンネル グループはセキュリティ アプライアンスのローカルのものであるため、外部サーバでは設定できません。

トンネル グループは次のアトリビュートを指定します。

- 一般パラメータ
- IPSec 接続パラメータ
- WebVPN 接続パラメータ

一般的なトンネル グループ接続パラメータ

一般パラメータは、IPSec 接続と WebVPN 接続の両方に共通です。一般パラメータには、次のものがあります。

- トンネル グループ名：トンネル グループを追加または編集するときにトンネル グループ名を指定します。次の事項を考慮する必要があります。
  - 認証に事前共有鍵を使用するクライアントの場合、トンネル グループ名は、IPSec クライアントがセキュリティ アプライアンスに渡すグループ名と同じです。
  - 認証に証明書を使用するクライアントは、この名前を証明書の一部として渡し、セキュリティ アプライアンスはこの名前を証明書から抽出します。

  トンネル グループ レコードには、トンネル接続ポリシーの情報が含まれています。これらのレコードは、接続情報の送信先であるアカウンティング サーバ（存在する場合）だけでなく、トンネル ユーザの認証先サーバを特定します。さらに、接続のデフォルト グループ ポリシーを特定します。これらのレコードには、プロトコル固有の接続パラメータが含まれています。
- 接続タイプ：接続タイプには、IPSec リモート アクセス、IPSec LAN 間、および WebVPN があります。トンネル グループに設定できる接続タイプは 1 つだけです。
- 認証、認可、アカウンティング サーバ：これらのパラメータは、セキュリティ アプライアンスが次の目的で使用するサーバ グループまたはリストを特定します。
  - ユーザの認証
  - ユーザがアクセスを認可されているサービスに関する情報の取得
  - アカウンティング レコードの格納

  サーバ グループは、1 つ以上のサーバによって構成できます。

- 接続のデフォルト グループ ポリシー：グループ ポリシーは、ユーザ指向アトリビュートのセットです。デフォルト グループ ポリシーは、トンネル ユーザの認証または認可の際にセキュリティ アプライアンスがデフォルトとして使用するアトリビュートを持つグループ ポリシーです。
- クライアント アドレスの割り当て方式：この方式には、セキュリティ アプライアンスがクライアントに割り当てる DHCP サーバやアドレス プールの値が含まれます。
- アカウント無効の上書き：このパラメータを使用すると、AAA サーバから受け取る「アカウント無効」インジケータを上書きできます。
- パスワード管理：このパラメータを使用すると、指定日数（デフォルトは 14 日）が経過すると現在のパスワードの有効期限が切れることをユーザに警告し、パスワードを変更する機会を提供できます。
- グループ除去およびレルム除去：これらのパラメータにより、受信するユーザ名をセキュリティ アプライアンスが処理する方法が決まります。これらのパラメータは、user@realm という形式で受信するユーザ名だけに適用されます。レルムは、ユーザ名に @ デリミタで付加される管理ドメインです（user@abc）。

  管理者がグループ除去処理を指定すると、セキュリティ アプライアンスは、VPN クライアントによって提示されたユーザ名からグループ名を取得することで、ユーザ接続のトンネル グループを選択します。次にセキュリティ アプライアンスは、認可または認証のためにユーザ名のユーザ部分だけを送信します。それ以外の場合（ディセーブルの場合）、セキュリティ アプライアンスはレルムを含むユーザ名全体を送信します。

  レルム除去処理では、認証または認可サーバへのユーザ名の送信時にユーザ名からレルムが削除されます。コマンドがイネーブルの場合、セキュリティ アプライアンスはユーザ名認可または認証のユーザ部分だけを送信します。ディセーブルの場合、セキュリティ アプライアンスはユーザ名全体を送信します。
- 認可の要求：このパラメータを使用すると、ユーザ アクセスの前に認可を要求したり、その要求を取り下げたりできます。
- 認可 DN アトリビュート：このパラメータは、認可を実行するときに使用する認定者名アトリビュートを指定します。

IPSec トンネル グループ接続パラメータ

IPSec トンネル グループ パラメータには、次のものがあります。

- クライアント認証方式：事前共有鍵または証明書、あるいは両方。
  - 事前共有鍵に基づいた IKE 接続の場合、接続ポリシーに関連付けられた英数字の鍵自体（最大 128 文字）。
  - ピア ID 確認の要求：このパラメータは、ピアの証明書を使用してピアの ID を確認することを要求するかどうかを指定します。
- ISAKMP（IKE）キープアライブ設定：この機能を使用すると、セキュリティ アプライアンスはリモート ピアが引き続き存在していることを監視し、当該ピアに自身の存在を報告できます。ピアが反応しなくなった場合、セキュリティ アプライアンスは接続を削除します。IKE キープアライブをイネーブルにすることで、IKE ピアが接続を失ったときに接続がハングしないように防止できます。

  IKE キープアライブにはさまざまな形式があります。この機能が正しく動作するには、セキュリティ アプライアンスとそのリモート ピアとが共通の形式をサポートしている必要があります。この機能は次のピアで使用できます。
  - Cisco VPN Client（Release 3.0 以降）
  - Cisco VPN 3000 Client（Release 2.x）
  - Cisco VPN 3002 Hardware Client
  - Cisco VPN 3000 シリーズ コンセントレータ
  - Cisco IOS ソフトウェア

— Cisco Secure PIX Firewall

シスコ以外の VPN クライアントは IKE キープアライブをサポートしていません。

IKE キープアライブをサポートするピアとサポートしないピアが混在するグループを設定している場合、グループ全体に対して IKE キープアライブをイネーブルにします。この機能をサポートしないピアに影響はありません。

IKE キープアライブをディセーブルにする場合、反応しないピアとの接続はタイムアウトするまでアクティブのままなので、アイドル アイムアウトを短く維持するようお勧めします。

(注) ISDN 回線経由で接続するクライアントがこのグループに含まれる場合、接続コストを削減するために IKE キープアライブをディセーブルにします。通常、ISDN 接続はアイドル時に解除されます。しかし IKE キープアライブ メカニズムによって接続がアイドルにならないため、接続解除されません。

IKE キープアライブをディセーブルにすると、クライアントは IKE 鍵または IPSec 鍵いずれかの有効期限が切れたときにのみ接続解除されます。IKE キープアライブがイネーブルになっている場合とは異なり、障害が発生したトラフィックは、ピア タイムアウト プロファイル値を持つトンネルから接続解除されません。

(注) IKE メイン モードを使用する LAN 間設定がある場合は、2 つのピアが同じ IKE キープアライブ設定を使用していることを確認します。両方のピアで IKE キープアライブをどちらもイネーブルにするか、またはどちらもディセーブルにする必要があります。

- デジタル証明書を使用して認証を設定する場合、証明書チェーン全体を送信するか（つまりピアに ID 証明書およびすべての発行証明書を送信する）、または ID 証明書のみを送信するかを指定できます。
- 古いバージョンの Windows クライアント ソフトウェアを使用しているユーザに、クライアントをアップデートする必要があることを通知し、クライアントのアップデート バージョンを取得するためのメカニズムをそのユーザに提供できます。VPN 3002 Hardware Client ユーザの場合、自動アップデートをトリガーできます。クライアント アップデートの設定と変更は、すべてのトンネル グループまたは特定のトンネル グループのどちらに対しても実行できます。
- デジタル証明書を使用して認証を設定する場合、IKE ピアに送信する証明書を特定するトラストポイントの名前を指定する必要があります。

WebVPN トンネル グループ接続パラメータ

次のアトリビュートは WebVPN 接続に固有です。

- 認証方式。AAA または証明書。
- 適用するカスタマイゼーションの名前。カスタマイゼーションにより、WebVPN ポータル ページの外観が決まります。カスタマイゼーション パラメータは WebVPN の設定の一環として設定します。
- DNS サーバ グループ名。DNS サーバ グループは、DNS サーバ名、ドメイン名、ネーム サーバ、リトライ回数、および DNS サーバがトンネル グループに使用するタイムアウト値を指定します。
- 1 つまたは複数のグループ エイリアス。これらは、トンネル グループへの参照にサーバが使用する代替名です。ログイン時、ユーザはグループ名をドロップダウン メニューから選択します。
- 1 つまたは複数のグループ URL。このパラメータを設定すると、指定 URL に参加するユーザは、ログイン時にグループを選択する必要がありません。

- デフォルト グループ ポリシーとは異なるアクセス権を WebVPN ユーザに付与するグループ ポリシー。
- CIFS 名前解決に使用する NetBIOS Name Service サーバの名前（nbns-server）。

グループ ポリシー

グループ ポリシーは、IPSec 接続用のユーザ指向アトリビュートと値のペアのセットで、内部的（ローカル）にデバイスに格納されるか、または外部的に RADIUS サーバに格納されます。トンネル グループでは、トンネルが確立されると、ユーザ接続の条件を設定するグループ ポリシーを使用します。グループ ポリシーを使用すると、ユーザまたはユーザのグループごとに各アトリビュートを個別に指定する必要がなく、ユーザにアトリビュートのセット全体を適用できます。

グループ ポリシーをユーザに割り当てる、または特定ユーザのグループ ポリシーを変更するには、グローバル コンフィギュレーション モードで **group-policy** コマンドを入力します。

セキュリティ アプライアンスにはデフォルト グループ ポリシーがあります。デフォルト グループ ポリシー（変更できますが削除はできません）に加えて、環境に固有のグループ ポリシーを 1 つまたは複数作成できます。

内部グループおよび外部グループについてポリシーを設定できます。内部グループは、セキュリティ アプライアンスの内部データベースに設定されます。外部グループは、RADIUS などの外部認証サーバに設定されます。グループ ポリシーには、次のアトリビュートが含まれます。

- ID
- サーバ定義
- クライアント ファイアウォールの設定
- トンネリング プロトコル
- IPSec の設定
- ハードウェア クライアントの設定
- フィルタ
- クライアント設定の設定値
- WebVPN 機能
- 接続設定

デフォルト グループ ポリシー

セキュリティ アプライアンスは、デフォルト グループ ポリシーを提供します。このデフォルト グループ ポリシーは変更できますが、削除できません。DfltGrpPolicy という名前のデフォルト グループ ポリシーはセキュリティ アプライアンスに常に存在します。しかしこのデフォルト グループ ポリシーは、セキュリティ アプライアンスで使用するように設定しない限り、有効になりません。他のグループ ポリシーを設定する場合、明示的に指定しないアトリビュートがあると、そのアトリビュートはデフォルト グループ ポリシーから値を取得します。デフォルト グループ ポリシーを表示するには、次のコマンドを入力します。

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

グループ ポリシーの設定

グループ ポリシーは、すべての種類のトンネルに適用できます。いずれの場合でも、パラメータを明示的に定義しないと、グループはデフォルト グループ ポリシーから値を取得します。グループ ポリシーは、外部と内部のどちらも設定できます。グループ ポリシーを設定するには、まずグループ ポリシーの名前とタイプを指定し、次に、内部グループ ポリシーの場合はアトリビュートを指定します。

外部グループ ポリシーの設定

外部グループ ポリシーは、指定の外部サーバからアトリビュート値を取得します。外部グループ ポリシーの場合、セキュリティ アプライアンスがアトリビュートについて照会できる AAA サーバ グループを特定し、その外部 AAA サーバ グループからアトリビュートを取得するときに使用するパスワードを指定する必要があります。外部認証サーバを使用している場合は、ユーザ名とグループ名が一意である必要があるので注意してください。グループに名前を付けるときは、外部ユーザの名前と一致するものを選択しないようにします。逆に、外部ユーザに名前を割り当てるときは、既存のグループの名前を選択しないようにします。

(注) セキュリティ アプライアンスは、外部 LDAP サーバまたは外部 RADIUS サーバでのユーザ認可をサポートしています。外部サーバを使用するようにセキュリティ アプライアンスを設定する前に、正しいセキュリティ アプライアンス認可アトリビュートでサーバを設定し、これらのアトリビュートのサブセットから、個々のユーザに特定の権限を割り当てる必要があります。外部グループ ポリシーの場合、サポートされている AAA サーバ タイプは RADIUS だけです。

内部グループ ポリシーの設定

内部グループ ポリシー用のアトリビュートと値のペアは、内部的（ローカル）にセキュリティ アプライアンスに格納されます。内部グループ ポリシーを設定するには、グループ ポリシーの名前とタイプを指定し、次にアトリビュートを指定します。内部グループ ポリシーのアトリビュートは、キーワード ***from*** を付加し、以前から存在しているグループ ポリシーの名前を指定することで、その既存グループ ポリシーの値に初期設定できます。内部グループ ポリシーには次のアトリビュートを指定できます。

- プライマリとセカンダリの WINS サーバおよび DNS サーバ
- VPN 固有のアトリビュート（アクセス時間、同時ログインの回数、VPN アイドル タイムアウトとセッション タイムアウト、VPN 接続に使用する ACL の名前、このグループ ポリシーの VPN トンネル タイプ（IPSec リモート アクセス、LAN 間、または WebVPN））
- セキュリティ設定（パスワード ストレージ、IP 圧縮、IKE 鍵の再生成でユーザ再認証を要求するかどうか、リモート ユーザのアクセスをトンネル グループのみに制限するかどうか、完全転送秘密をイネーブルにするかどうか）
- バナー メッセージ
- IPSec over UDP（IPSec through NAT と呼ばれる場合もある）
- スプリットトンネリング ポリシーとネットワーク リスト
- ドメイン アトリビュート
- VPN 3002 Hardware Client のアトリビュート（セキュア ユニット認証、ユーザ認証、ユーザ認証アイドル タイムアウト、IP Phone バイパス、LEAP バイパス、およびネットワーク拡張モード）
- バックアップ サーバ アトリビュート
- クライアント ファイアウォール ポリシー
- クライアント アクセス規則

明示的に指定しないアトリビュートがある場合、グループ ポリシーにはデフォルト グループから値が継承されます。

グループ ポリシー WebVPN アトリビュートの設定

WebVPN では、ユーザは、セキュリティ アプライアンスへのセキュアなリモート アクセス VPN トンネルを Web ブラウザを使用して確立できます。ソフトウェア クライアントとハードウェア クライアントはいずれも必要ありません。WebVPN では、多様な Web リソースおよび Web 対応アプリケーションへのアクセスが、HTTPS インターネット サイトに到達可能なコンピュータほとんどすべてで容易になります。WebVPN では、SSL およびその後継バージョンである TLS1 が使用され、中央サイトで設定済みの特定のサポート対象内部リソースとリモート ユーザとの間にセキュアな接続が提供されます。セキュリティ アプライアンスはプロキシ処理が必要な接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。デフォルトでは、WebVPN はディセーブルです。

WebVPN 設定は、特定の内部グループ ポリシー用にカスタマイズできます。

(注) グローバル コンフィギュレーション モードから移行する WebVPN モードでは、WebVPN のグローバル設定値を設定できます。この項で説明する WebVPN モード（グループ ポリシー コンフィギュレーション モードから移行するモード）では、特定のグループ ポリシーの WebVPN 設定をカスタマイズできます。

グループ ポリシーの WebVPN コンフィギュレーション モードでは、すべての機能について設定値を継承するか、または次のパラメータをカスタマイズするかを指定できます。

- WebVPN 機能（自動ダウンロード、Citrix、ファイル アクセス、ファイル参照、ファイル エントリ、フィルタ、HTTP プロキシ、MAPI、ポート転送、URL エントリ）。
- ACL とフィルタ対象トラフィックのタイプ。
- ログイン時にユーザに表示されるウィンドウのルックアンドフィールを変更するカスタマイゼーション。
- HTML コンテンツ フィルタ。
- ホームページ。
- WebVPN セッションの Java、ActiveX、イメージ、スクリプト、および cookie のフィルタリング。
- このグループの WebVPN 接続で使用するアクセス コントロール リスト。
- このグループの WebVPN ホームページに表示される URL リスト。
- ポート転送とポート転送表示名。
- デッド ピア検知アトリビュート。
- シングル サインオン サーバ（SSO サーバ）。WebVPN でのみ可能なシングル サイン オンのサポートにより、ユーザは、ユーザ名とパスワードを入力し直すことなく、さまざまなサーバからさまざまなセキュア サービスにアクセスできます。
- 自動サインオン。WebVPN ユーザのログイン資格情報を内部サーバに自動的に送信します。
- ログオンに成功するが VPN 特権を持っていない WebVPN ユーザへの拒否メッセージ。
- SSL VPN Client（SVC）アトリビュート。SVC は、IPSec VPN クライアントの利点をリモート ユーザが活用できる VPN トンネリング テクノロジーです。これを使用すると、ネットワーク管理者が IPSec VPN クライアントをリモート コンピュータにインストールして設定する必要はありません。

- SVC キープアライブ アトリビュート。キープアライブ メッセージの頻度を調整し（*seconds* で指定）、プロキシ、ファイアウォール、または NAT デバイス経由の SVC 接続をオープンのまま維持します。接続のアイドル状態が維持される時間がデバイスで制限されている場合でも同様に機能します。
- SVC インストールの維持。この設定により、リモート コンピュータへの SVC 常時インストールがイネーブルになります。

（注） WebVPN は **vpn-filter** コマンドで定義された ACL を使用しません。

多くの場合、WebVPN の設定の一環として WebVPN アトリビュートを定義し、その後、グループ ポリシー WebVPN アトリビュートを設定するときにそれらの定義を特定のグループに適用します。WebVPN アトリビュートの設定の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』および『*Cisco Security Appliance Command Reference*』にある WebVPN の説明を参照してください。

ユーザ アトリビュートの設定

デフォルトでは、ユーザは割り当てられたグループ ポリシーからすべてのユーザ アトリビュートを継承します。セキュリティ アプライアンスでは、個々のアトリビュートをユーザ レベルに割り当て、そのユーザに適用されるグループ ポリシーの値を上書きすることもできます。たとえば、業務時間中のアクセスをすべてのユーザに許可するグループ ポリシーを指定し、その後で、特定のユーザに 24 時間のアクセスを設定することができます。

特定ユーザのアトリビュートの設定

特定のユーザのアトリビュートを設定するには、**username** コマンドを使用してユーザ名モードを開始し、1 つ（またはゼロ個）のパスワード、およびその他の値をユーザに割り当てます。指定しないアトリビュートはグループ ポリシーから継承されます。

内部ユーザ認証データベースは、**username** コマンドによって入力されたユーザで構成されます。セキュリティ アプライアンス データベースにユーザを追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザを削除するには、削除対象のユーザ名に対してこのコマンドの **no** バージョンを使用します。ユーザ名をすべて削除するには、ユーザ名を付加せずに **clear configure username** コマンドを使用します。

指定できるユーザ名アトリビュートは、次のとおりです。

- このユーザのパスワードと特権レベル
- 明示的に設定されていないアトリビュートの値の継承元であるグループ ポリシー
- VPN アクセス時間と許可されている同時ログイン回数
- VPN アイドル タイムアウトと最大接続時間
- VPN 接続のフィルタとして使用する、以前に設定されたユーザ固有の ACL の名前
- このユーザに割り当てる IP アドレスとネットマスク
- このユーザが使用できる VPN トンネル タイプ（IPSec リモート アクセスまたは WebVPN）
- リモート ユーザのアクセスを、以前から存在している指定のトンネル グループ経由のみに制限するかどうか
- ログイン パスワードをユーザがクライアント システムに格納することを許可するかどうか

特定ユーザの WebVPN の設定

WebVPN では、ユーザは、セキュリティ アプライアンスへのセキュアなリモート アクセス VPN トンネルを Web ブラウザを使用して確立できます。ソフトウェア クライアントとハードウェア クライアントはいずれも必要ありません。WebVPN では、多様な Web リソースおよび Web 対応アプリケーションへのアクセスが、HTTPS インターネット サイトに到達可能なコンピュータほとんどすべてで容易になります。WebVPN では、SSL およびその後継バージョンである TLS1 が使用され、中央サイトで設定済みの特定のサポート対象内部リソースとリモート ユーザとの間にセキュアな接続が提供されます。セキュリティ アプライアンスはプロキシ処理が必要な接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

特定ユーザの WebVPN 設定をカスタマイズするには、ユーザ名コンフィギュレーション モードで **webvpn** コマンドを使用することにより、ユーザ名 WebVPN コンフィギュレーション モードを開始します。ユーザ名に対して **webvpn** コマンドを使用すると、ファイル、MAPI プロキシ、URL および TCP アプリケーションへの WebVPN 経由のアクセスを定義できます。さらに、ACL とフィルタ対象トラフィックのタイプも特定できます。WebVPN は、デフォルトではディセーブルです。これらの **webvpn** コマンドは、設定元のユーザ名にのみ適用されます。

ユーザ名 WebVPN コンフィギュレーション モードでは、すべての機能について設定値を継承するか、または次のパラメータをカスタマイズするかを指定できます。

- WebVPN 機能（自動ダウンロード、Citrix、ファイル アクセス、ファイル参照、ファイル エントリ、フィルタ、HTTP プロキシ、MAPI、ポート転送、URL エントリ）。
- ログイン時にユーザに表示されるウィンドウのルックアンドフィールを変更するカスタマイゼーション。
- HTML コンテンツ フィルタ。
- ホームページ。
- WebVPN セッションの Java、ActiveX、イメージ、スクリプト、および cookie のフィルタリング。
- このグループの WebVPN 接続で使用するアクセス コントロール リスト。
- このグループの WebVPN ホームページに表示される URL リスト。
- ポート転送とポート転送表示名。
- デッド ピア検知アトリビュート。
- シングル サインオン サーバ（SSO サーバ）。WebVPN でのみ可能なシングル サイン オンのサポートにより、ユーザは、ユーザ名とパスワードを入力し直すことなく、さまざまなサーバからさまざまなセキュア サービスにアクセスできます。
- 自動サインオン（WebVPN ユーザのログイン資格情報を内部サーバに自動的に送信します）。
- ログオンに成功するが VPN 特権を持っていない WebVPN ユーザへの拒否メッセージ。
- SSL VPN Client（SVC）アトリビュート。SVC は、IPSec VPN クライアントの利点をリモート ユーザが活用できる VPN トンネリング テクノロジーです。これを使用すると、ネットワーク管理者が IPSec VPN クライアントをリモート コンピュータにインストールして設定する必要はありません。
- SVC キープアライブ アトリビュート。キープアライブ メッセージの頻度を調整し（*seconds* で指定）、プロキシ、ファイアウォール、または NAT デバイス経由の SVC 接続をオープンのまま維持します。接続のアイドル状態が維持される時間がデバイスで制限されている場合でも同様に機能します。
- SVC インストールの維持。この設定により、リモート コンピュータへの SVC 常時インストールがイネーブルになります。

（注） WebVPN は **vpn-filter** コマンドで定義された ACL を使用しません。

多くの場合、WebVPN の設定の一環として WebVPN アトリビュートを定義し、その後、ユーザ名 WebVPN アトリビュートを設定するときにそれらの定義を特定のユーザ名に適用します。WebVPN アトリビュートの設定の詳細については、Web VPN の説明を参照してください。ユーザ名コンフィギュレーション モードで **webvpn** コマンドを使用することにより、ユーザ名 WebVPN コンフィギュレーション モードを開始します。ユーザ名に対して WebVPN 関連のコマンドを使用すると、ファイル、MAPI プロキシ、URL および TCP アプリケーションへの WebVPN 経由のアクセスを定義できます。さらに、ACL とフィルタ対象トラフィックのタイプも特定できます。WebVPN は、デフォルトではディセーブルです。

ASA での PKI 実装

ASA における PKI 実装は、VPN 3000 コンセントレータの実装とは異なります。ASA 上の PKI モデルの重要な概念はトラストポイントです。トラストポイントには、次の特性があります。

- トラストポイントは、ローカル ID と 1 対 1 の関係を持ちます。
- トラストポイントは、CA ID と 多対 1 の関係を持ちます。
- トラストポイントは、登録要求の内容、デフォルト、および登録方法を指定します。
- トラストポイントは、CRL コンフィギュレーション パラメータを指定します。

ASA では、CLI でトラストポイントを設定するために **crypto ca trustpoint** コマンドが用意されています。このコマンドには、IOS オプションのサブセットと、既存の VPN 3000 機能を ASA に移行するための追加パラメータが含まれています。このコマンドと、そのサブコマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。すべての PKI 機能は、ASDM で設定できます（詳細については、このマニュアルの「デジタル証明書の登録」を参照してください）。

表 2-1 は、その他の新しい PKI コマンドのリストを示しています。

表 2-1　ASA の新しい PKI コマンド

コマンド セット	アクション
crypto key	RSA または DSA の鍵ペアを生成します。
crl configure	**crypto ca trustpoint** 下でこのコマンドを使用すると、**crl** コンフィギュレーション モードを開始して CRL パラメータを設定できます。
crl	VPN 3000 コンセントレータから引き継いだ多数のパラメータを設定できます。
crypto ca authenticate	認証局から証明書をダウンロードまたはペーストすることで、CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。
crypto ca import（新しいコマンドではありません）	手動登録要求への応答として CA から受信した証明書をインストールします。
crypto ca crl request	指定したコンフィギュレーションの設定に基づいて、証明書失効リストを要求します。
crypto ca certificate map	証明書マッピング規則の優先順位付きリストを管理します。このコマンドは、VPN 3000 コンセントレータでの証明書グループのマッチング用に提供されています。
tunnel-group-map	証明書ベースの IKE セッションをトンネル グループにマッピングするためのポリシーと規則を設定します。

インターフェイスごとの ASDM セッションおよび WebVPN セッション

ASA Version 7.1(1) 以降は、インターフェイス上で WebVPN 管理セッションおよび ASDM 管理セッションの両方を同時にサポートします。唯一の制約は、これらの機能にそれぞれ異なるポートを割り当てる必要があるという点です。たとえば、HTTPS トラフィック用にポート 443 を使用して WebVPN を実行する場合、ASDM 管理セッションには別のポートを割り当てます。

ASDM を使用して、Configuration > VPN > WebVPN > WebVPN Access ウィンドウでポートを設定します。

CHAPTER 3

設定の開始

この章では、VPN 3000 コンセントレータの クイック コンフィギュレーション プログラムの概要を示し、対応する機能を ASDM のどこで設定するかを説明します。また、設定タスクの概要に続いて、サイトツーサイトおよびリモート アクセスのトンネルを設定するための VPN ウィザードの実行に必要な情報のリストも提供します。

クイック コンフィギュレーションのタスクと対応する ASDM の機能

表 3-1 に、次の設定タスクと、ASDM でこれらを実行する場所を示します。

- IP インターフェイスの設定
- システム情報の設定
- トンネリング プロトコルとオプションの設定
- アドレス管理方式の設定
- 認証の設定
- 内部サーバのユーザ データベースの設定
- IPSec グループの設定
- 管理者パスワードの設定

表 3-1　最初のタスク

VPN 3000 クイック コンフィギュレーションのタスク	ASA の対応する機能
IP インターフェイスの設定 プライベート イーサネット接続およびパブリック イーサネット接続のアドレスとサブネット マスクを入力します。オプションとして、外部インターフェイスのアドレスを入力します。 • イネーブル / ディセーブル • DHCP クライアント / システムの名前 • 固定 IP アドレッシング（IP アドレス / サブネット マスク） • インターフェイスのタイプ（パブリックまたはプライベート） • MAC アドレス • フィルタ • 速度 • 二重化 • MTU	**Configuration > Interfaces** に移動します。 • 次の項目を追加 / 編集します。 — ハードウェア ポートの選択 — インターフェイスのイネーブル化 • 次の項目を入力します。 — VLAN ID — サブインターフェイス ID — インターフェイス名 — セキュリティ レベル — IP アドレスの送信元：固定 IP または DHCP — IP アドレス — サブネット マスク — MTU • **Configure Hardware Properties...** をクリックします。 — 二重化タイプを選択：全二重、半二重、自動 — 速度を選択：10、100、自動 • オプションとして、同一のセキュリティ レベルが設定された 2 つ以上のインターフェイス間のトラフィックをイネーブルにできます。
システム情報の設定 • システムのホスト名 • 日時 • DNS サーバ情報（IP アドレス、インターネット ドメイン名、デフォルト ゲートウェイ）	**Configuration > Properties > Device Administration > Device** に移動します。 • ホスト名とドメイン名を入力します。 • **Configuration > Properties >Device Administration > Clock** に移動して、日時を入力します。 • **Configuration > Properties > DNS Client** に移動します。 — サーバを追加します（上限は 6）。 — タイムアウトを秒で入力します。 — リトライ回数を入力します。 — インターフェイスの DNS ルックアップをイネーブルにします。
トンネリング プロトコルとオプションの設定 • PPTP：暗号化オプション • L2TP：暗号化オプション • IPSec（リモート アクセスのみを許可します。QC を介したサイトツーサイトでは実行できません）。	トンネル グループを定義するには、**Configuration > VPN > General > Tunnel Group** に移動します。 IPSec には次の 2 つのデフォルト トンネル グループがあります。 • LAN 間用の DefaultL2LGroup • リモート アクセス用の DefaultRAGroup

表 3-1　最初のタスク

VPN 3000 クイック コンフィギュレーションのタスク	ASA の対応する機能
アドレス管理方式の設定 • クライアントが独自に IP アドレスを指定します。 • ユーザごとに IP アドレスを割り当てます（認証サーバを使用）。 • DHCP を使用します（サーバ アドレスまたはサーバ名を指定）。 • プールを設定します（開始 / 終了の範囲）。	**Configuration > VPN > IP Address Management > Assignment** に移動します。 いずれかを選択します。 • 認証サーバから付与されたアドレスを使用します。 • DHCP を使用します。 • 内部アドレス プールを使用します。 • **Configuration > VPN > IP Address Management > IP Pools** で IP アドレス プールを設定します。
認証の設定 • サーバ タイプを選択します：内部、RADIUS、NTDomain、SDI、Kerberos/Active Directory。 • 選択した認証サーバの情報を入力します。それぞれ独自の画面が用意されています。	**Configuration > Properties > AAA Setup** に移動します。 • サーバ グループを追加します。 • サーバ グループにサーバを追加します。 • 認証プロンプトを設定します。
内部サーバのユーザ データベースの設定 次のユーザ情報を入力します。 • ユーザ名 • パスワード • パスワードの確認 • IP アドレス（ユーザごとにアドレスが割り当てられている場合） • サブネット マスク	**Configuration > Properties > Device Administration > User Accounts** に移動します。 ユーザ アカウントを追加し、次の情報を入力します。 • Identity の項目： ユーザ名 パスワード パスワードの確認 特権レベル • VPN Policy の項目（指定するか、またはグループ ポリシーから継承する場合は選択する）： グループ ポリシー（以前に定義済み） トンネリング プロトコル フィルタ トンネル グループ ロック クライアント システムにパスワードを保存 接続の設定 専用の IP アドレス（オプション）
IPSec グループの設定 • グループ名 • パスワード • 確認	**Configuration > VPN > General > Tunnel Group** に移動します。 IPSec タイプのトンネル グループを追加します。
管理者パスワードの設定	**Configuration > Properties > Device Administration > Password** に移動します。
VPN 接続手順のテスト	

VPN ウィザードを使用した VPN トンネルの設定

VPN ウィザードを使用すると、ASA から別の VPN デバイスまたはリモート クライアント ユーザのいずれかへの VPN トンネルを設定できます。この VPN トンネルは、サイトツーサイト アクセスまたはリモート アクセスに使用します。このウィザードは、新しい VPN 設定を定義する場合にだけ使用できます。このウィザードを使用して設定した VPN トンネルについては、ASDM 機能を使用して（特に **Configuration > Features > VPN** セクションで使用して）編集できます。

情報の収集

VPN ウィザードを起動する前に、VPN トンネルの設定に必要な情報を収集します。設定するトンネル タイプの項を参照してください。

- サイトツーサイト VPN トンネル
- ローカルに保存されたユーザ アカウントを使用したリモート アクセス
- クライアント認証に AAA サーバ グループを使用したリモート アクセス

サイトツーサイト VPN トンネル

VPN ウィザードを使用してサイトツーサイト VPN トンネルを設定する場合は、事前に次の情報を収集する必要があります。

（注） これらの値を記録する場合は、関連付けられている番号をメモしてください。これらの値は、このデータを収集した後で実行する VPN ウィザードに表示されるステップ番号に対応しています。

1. VPN トンネル タイプ

   サイトツーサイト VPN トンネル用のインターフェイス（たとえば、「inside」や「outside」）。VPN トンネルを設定する前に、セキュリティ アプライアンスにインターフェイスを設定します。トンネルを設定する場合は、設定する VPN トンネルに関連付けるインターフェイスを選択します。

2. リモート サイト ピア

   トンネルのもう一方の終端にあるピア デバイスの IP アドレス。

   トンネル グループのオプション名（ピアの IP アドレスのデフォルト）。

   認証タイプ（事前共有鍵またはデジタル証明書）。次のいずれかも必要です。

   - 事前共有鍵の場合は、鍵の名前。
   - デジタル証明書の場合は、証明書署名アルゴリズム（RSA または DSA）、およびトラストポイントの名前。

     RSA アルゴリズムと DSA アルゴリズムの違いについては、「鍵ペア」を参照してください。

     トラストポイントは、CA または ID ペアを示します。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、および 1 つの登録済み ID 証明書とのアソシエーションが含まれています。

     （注） デジタル証明書認証タイプを選択する場合は、VPN ウィザードを実行する前に、トラストポイントを設定します（P.4-4 の「トラストポイントの作成」を参照してください）。

3. トンネルのネゴシエートに使用する IPSec フェーズ 1 Internet Key Exchange Security Association ポリシー。これは、次のもので構成されます。
   - IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）：DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
   - IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）：MD5 または SHA。デフォルトは SHA です。

     Diffie Hellman グループ（両方のデバイスで同じである必要がある）：グループ 1、グループ 2、グループ 5、またはグループ 7。デフォルトはグループ 2 です。
4. VPN トンネルに適用する IPSec フェーズ 2 Encryption and Authentication ポリシー。パラメータとオプションは、次のとおりです。
   - IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）：DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
   - IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）：MD5 または SHA。デフォルトは SHA です。
5. ローカル ホストとネットワーク：IP 接続のローカル サイトのホストとネットワーク。IP 接続のローカル サイトにおけるホストおよびネットワークを指定するには、次のオプションがあります。
   - IP アドレス。このオプションを選択する場合は、次の情報が必要です。

     インターフェイス名：ホストの接続先のインターフェイス、たとえば「inside」や「outside」。

     IP アドレス：any、特定のローカル ホストのアドレス、またはサブネット。any を選択すると、IP アドレスとサブネット マスクが 0.0.0.0 になります。

     サブネット マスク：255.255.255.255 ～ 0.0.0.0 の値。
   - ASA コンフィギュレーションにすでに存在するホストの名前。
   - 保護対象のネットワークまたはホストのリストを含むグループ。このオプションを選択する場合は、次の情報が必要です。

     ASA コンフィギュレーションにすでに存在するホストの名前。

     ASA コンフィギュレーションにすでに存在するグループの名前。

（注） ホストまたはネットワークのグループ名を設定するには、**Configuration > Global Objects > Hosts/Networks** に移動します。

6. リモート ホストとネットワーク：IP 接続のリモート サイトのホストとネットワーク。

   オプションは、ローカル ホストとネットワークのオプションと同じです。

この項で説明した情報を準備した後、「VPN ウィザードの実行」に進みます。

ローカルに保存されたユーザ アカウントを使用したリモート アクセス

リモート アクセス VPN トンネルで ASA コンフィギュレーションにログイン アカウントを保存する必要がある場合は、次の情報を収集します。

（注） これらの値を記録する場合は、関連付けられている番号をメモしてください。これらの番号は、VPN ウィザードに表示されるステップ番号に対応しています。

1. VPN トンネル タイプ

   サイトツーサイト VPN トンネル用のインターフェイス（たとえば、「inside」や「outside」）。VPN トンネルを設定する前に、セキュリティ アプライアンスにインターフェイスを設定します。トンネルを設定する場合は、設定する VPN トンネルに関連付けるインターフェイスを選択します。

2. リモートアクセス クライアント

   デフォルト設定（Cisco VPN Client リリース 3.x 以上、または他の Easy VPN Remote 製品）を使用して、この ASA へのトンネルでサポートされる VPN クライアントのタイプを指定します。このリリースでは、他のオプションはサポートされていません。

3. VPN トンネル グループ名および認証方式

   リモート クライアントと ASA の両方に使用するトンネル グループの名前。このグループ名によって、次のステップで指定する共通の接続設定およびクライアント設定が決まります。

   認証タイプ（事前共有鍵またはデジタル証明書）。次のいずれかも必要です。

   - 事前共有鍵の場合は、鍵の名前。
   - デジタル証明書の場合は、証明書署名アルゴリズム（RSA または DSA）、およびトラストポイントの名前。

     RSA アルゴリズムと DSA アルゴリズムの違いについては、「鍵ペア」を参照してください。

     トラストポイントは、CA または ID ペアを示します。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、および 1 つの登録済み ID 証明書とのアソシエーションが含まれています。

   （注） デジタル証明書認証タイプを選択する場合は、VPN ウィザードを実行する前に、トラストポイントを設定します（Configuration > Properties > Certificate > Trustpoint）。

4. クライアント認証（次のいずれかのオプションを選択できる）

   - ローカル（内部）ユーザ データベースを使用した認証。

     このオプションでは、ASA コンフィギュレーションにユーザ アカウントを入力できます。
   - AAA サーバ グループを使用した認証。

     このオプションでは、クライアント認証を処理するための AAA サーバ グループを選択できます。このオプションを選択した場合は、次の項の同じステップに進みます。

5. ユーザ アカウント

   「Authenticate using the local (internal) user database」を選択した場合は、ローカル データベースに挿入するために、各ユーザのログイン名とそれぞれのパスワードをリストします。

6. アドレス プール

   ASA コンフィギュレーション内にすでに存在する IP アドレス プールの名前を選択することも、新しい IP アドレス プールを指定することもできます。新しい IP アドレス プールを指定する場合は、新しいプールの名前、関連付けられる IP アドレス範囲、およびサブネット マスク（オプション）が必要です。

7. （オプション）クライアントにプッシュするアトリビュート

   VPN クライアントの接続時に、VPN クライアントに次のアトリビュートをプッシュするよう選択できます。

   - プライマリおよびセカンダリ DNS サーバの IP アドレス。
   - プライマリおよびセカンダリ WINS サーバの IP アドレス。
   - デフォルト ドメイン名。

8. トンネルのネゴシエートに使用する IPSec フェーズ 1 Internet Key Exchange Security Association ポリシー。これは、次のもので構成されます。
   - IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）：DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
   - IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）：MD5 または SHA。デフォルトは SHA です。

     Diffie Hellman グループ（両方のデバイスで同じである必要がある）：グループ 1、グループ 2、グループ 5、またはグループ 7。デフォルトはグループ 2 です。
9. VPN トンネルに適用する IPSec フェーズ 2 Encryption and Authentication ポリシー。パラメータとオプションは、次のとおりです。
   - IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）：DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
   - IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）：MD5 または SHA。デフォルトは SHA です。
10. （オプション）アドレス変換免除およびスプリット トンネリング

    VPN の認証済みリモート ユーザに公開される、内部ネットワーク内のホストおよびネットワーク。none を指定してトンネル内の認証済みリモート ユーザに内部ネットワーク全体を公開するか、トンネル内の認証済みリモート ユーザに公開する内部アドレスを指定して、残りのアドレスがネットワーク アドレス変換によって隠蔽されたままになるようにします。IP 接続のローカル サイトにおけるホストおよびネットワークの内部アドレスを指定するには、次のオプションがあります。
    - IP アドレス。このオプションを選択する場合は、次の情報が必要です。

      インターフェイス名：ホストの接続先のインターフェイス、たとえば「inside」や「outside」。

      IP アドレス：any、特定のローカル ホストのアドレス、またはサブネット。any を選択すると、IP アドレスとサブネット マスクが 0.0.0.0 になります。

      サブネット マスク：255.255.255.255 ～ 0.0.0.0 の値。
    - ASA コンフィギュレーションにすでに存在するホストの名前。
    - 保護対象のネットワークまたはホストのリストを含むグループ。このオプションを選択する場合は、次の情報が必要です。

      ASA コンフィギュレーションにすでに存在するホストの名前。

      ASA コンフィギュレーションにすでに存在するグループの名前。

（注） ホストまたはネットワークのグループ名を設定するには、**Configuration > Global Objects > Hosts/Networks** に移動します。

スプリット トンネリング：イネーブルにして VPN ユーザによるインターネットへの暗号化されていないアクセスを可能にするか、またはディセーブルのままにします。

（注） スプリット トンネリングをイネーブルにすると、上記で指定したホストがスプリット トンネル アクセス リストとしても機能します。

この項で説明した情報を準備した後、「VPN ウィザードの実行」に進みます。

クライアント認証に AAA サーバ グループを使用したリモート アクセス

AAA サーバ グループを使用したクライアント認証が必要なリモート アクセス VPN トンネルには、次の情報を収集します。

(注)　これらの値を記録する場合は、関連付けられている番号をメモしてください。これらの番号は、VPN ウィザードに表示されるステップ番号に対応しています。

1. VPN トンネル タイプ

   サイトツーサイト VPN トンネル用のインターフェイス（たとえば、「inside」や「outside」）。VPN トンネルを設定する前に、セキュリティ アプライアンスにインターフェイスを設定します。トンネルを設定する場合は、設定する VPN トンネルに関連付けるインターフェイスを選択します。

2. リモートアクセス クライアント

   デフォルト設定（Cisco VPN Client リリース 3.x 以上、または他の Easy VPN Remote 製品）を使用して、この ASA へのトンネルでサポートされる VPN クライアントのタイプを指定します。このリリースでは、他のオプションはサポートされていません。

3. VPN トンネル グループ名および認証方式

   リモート クライアントと ASA の両方に使用するトンネル グループの名前。このグループ名によって、次のステップで指定する共通の接続設定およびクライアント設定が決まります。

   認証タイプ（事前共有鍵またはデジタル証明書）。次のいずれかも必要です。

   - 事前共有鍵の場合は、鍵の名前。
   - デジタル証明書の場合は、証明書署名アルゴリズム（RSA または DSA）、およびトラストポイントの名前。

     RSA アルゴリズムと DSA アルゴリズムの違いについては、「鍵ペア」を参照してください。

     トラストポイントは、CA または ID ペアを示します。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、および 1 つの登録済み ID 証明書とのアソシエーションが含まれています。

     (注)　デジタル証明書認証タイプを選択する場合は、VPN ウィザードを実行する前に、トラストポイントを設定します（Configuration > Properties > Certificate > Trustpoint）。

4. クライアント認証（次のいずれかのオプションを選択できる）

   - ローカル（内部）ユーザ データベースを使用した認証。

     このオプションでは、ASA コンフィギュレーションにユーザ アカウントを入力できます。このオプションを選択した場合は、前の項のステップ 5 から操作を続けます。

   - AAA サーバ グループを使用した認証。

     このオプションを選択した場合は、コンフィギュレーションに追加済みの AAA サーバ グループの名前を選択するか、または新しい名前を作成します。**Configuration** > **Properties** > **AAA Setup** パスでは、AAA サーバのコンフィギュレーションを確認および管理できます。これらの認証オプションを提供する VPN ウィザードの Client Authentication パネルには、AAA サーバ グループの作成に使用できる **New** ボタンもあります。このオプションを選択した場合は、グループ名の入力、認証プロトコルの選択（RADIUS、TACACS+、SDI、NT、Kerberos のいずれか）、サーバの IP アドレスの指定、インターフェイスの選択（「inside」または「outside」）、およびサーバの秘密鍵の指定を実行できるように準備しておいてください。

5. アドレス プール

   ASA コンフィギュレーション内にすでに存在する IP アドレス プールの名前を選択することも、新しい IP アドレス プールを指定することもできます。新しい IP アドレス プールを指定する場合は、新しいプールの名前、関連付けられる IP アドレス範囲、およびサブネット マスク（オプション）が必要です。

6. （オプション）クライアントにプッシュするアトリビュート

   VPN クライアントの接続時に、VPN クライアントに次のアトリビュートをプッシュするよう選択できます。

   - プライマリおよびセカンダリ DNS サーバの IP アドレス。
   - プライマリおよびセカンダリ WINS サーバの IP アドレス。
   - デフォルト ドメイン名。

7. トンネルのネゴシエートに使用する IPSec フェーズ 1 Internet Key Exchange Security Association ポリシー。これは、次のもので構成されます。

   - IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）：DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
   - IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）：MD5 または SHA。デフォルトは SHA です。

     Diffie Hellman グループ（両方のデバイスで同じである必要がある）：グループ 1、グループ 2、グループ 5、またはグループ 7。デフォルトはグループ 2 です。

8. VPN トンネルに適用する IPSec フェーズ 2 Encryption and Authentication ポリシー。パラメータとオプションは、次のとおりです。

   - IPSec VPN トンネルの暗号化アルゴリズム（両方のデバイスで同じである必要がある）：DES、3DES、AES-128、AES-192、または AES-256。デフォルトは 3DES です。
   - IPSec VPN トンネルの認証アルゴリズム（両方のデバイスで同じである必要がある）：MD5 または SHA。デフォルトは SHA です。

9. （オプション）アドレス変換免除およびスプリット トンネリング

   VPN の認証済みリモート ユーザに公開される、内部ネットワーク内のホストおよびネットワーク。none を指定してトンネル内の認証済みリモート ユーザに内部ネットワーク全体を公開するか、トンネル内の認証済みリモート ユーザに公開する内部アドレスを指定して、残りのアドレスがネットワーク アドレス変換によって隠蔽されたままになるようにします。IP 接続のローカル サイトにおけるホストおよびネットワークの内部アドレスを指定するには、次のオプションがあります。

   - IP アドレス。このオプションを選択する場合は、次の情報が必要です。

     インターフェイス名：ホストの接続先のインターフェイス、たとえば「inside」や「outside」。

     IP アドレス：any、特定のローカル ホストのアドレス、またはサブネット。any を選択すると、IP アドレスとサブネット マスクが 0.0.0.0 になります。

     サブネット マスク：255.255.255.255 ～ 0.0.0.0 の値。
   - ASA コンフィギュレーションにすでに存在するホストの名前。
   - 保護対象のネットワークまたはホストのリストを含むグループ。このオプションを選択する場合は、次の情報が必要です。

     ASA コンフィギュレーションにすでに存在するホストの名前。

     ASA コンフィギュレーションにすでに存在するグループの名前。

（注） ホストまたはネットワークのグループ名を設定するには、**Configuration > Global Objects > Hosts/Networks** に移動します。

スプリット トンネリング：イネーブルにして VPN ユーザによるインターネットへの暗号化されていないアクセスを可能にするか、またはディセーブルのままにします。

（注） スプリット トンネリングをイネーブルにすると、上記で指定したホストがスプリット トンネル アクセス リストとしても機能します。

この項で説明した情報を準備した後、「VPN ウィザードの実行」に進みます。

VPN ウィザードの実行

VPN ウィザードを実行するには、次の手順を実行します。

ステップ 1　**Wizards > VPN Wizard** に移動します。

ステップ 2　設定するトンネルのタイプとして、**Site to Site** または **Remote Access** を選択します。

ステップ 3　VPN Tunnel インターフェイスの横にある **Inside** または **Outside** を選択します。

ステップ 4　**Next** をクリックして、VPN ウィザードの指示に従います。詳細については、**Help** をクリックしてください。

コンフィギュレーションの保存

作業中は、次の手順を使用して、変更内容をフラッシュ メモリに保存して保持することを忘れないようにしてください。

- ASDM の場合：**File** > **Save Running Configuration to Flash** を選択します。
- CLI の場合：**write memory** コマンドを入力します。

コンフィギュレーションの表示

現在のコンフィギュレーション設定を表示するには、次のいずれかのコマンドを入力します。

- hostname# **show config**

  このコマンドを入力すると、フラッシュ メモリに保存されたスタートアップ コンフィギュレーションが表示されます。
- hostname# **show running-config**

  このコマンドを入力すると、オペレーティング コンフィギュレーションが表示されます。
- hostname# **show running config all**

  このコマンドを入力すると、デフォルト値を持つアトリビュートを含むオペレーティング コンフィギュレーションが表示されます。

（注） 最初の 2 つのコマンドは、実行したコンフィギュレーション変更を保存した場合は同じになります。

また、**show run ?** と入力すると、より詳細なリストを取得するために入力する show configuration コマンドの詳細なリストが表示されます。

ASDM の使用による CLI の学習

ASDM の **Options** > **Preferences** ウィンドウには、「Preview commands before sending to the device」オプションが表示されます。このオプションをイネーブルにすると、**Apply** をクリックするたびに、同等の CLI コマンドが Preview CLI Commands ウィンドウに表示されます。

コマンドを表示したら、**OK** をクリックし、次に確認ウィンドウで **Proceed** をクリックすると、実行コンフィギュレーションへの変更が保存されます。

CHAPTER 4

基本的な IPSec VPN トンネルの構築

次の項では、CLI コマンドと ASDM を使用して LAN 間トンネルおよびリモート アクセス トンネルを作成する方法と、事前共有鍵またはデジタル証明書を使用してそれらを認証する方法について説明します。

- デジタル証明書の登録
- LAN 間トンネルの設定
- リモート アクセス トンネルの設定

(注) ASDM には、完全なオンラインヘルプ システムが付属しています。パネルのフィールド定義を参照する場合は、**Help** をクリックしてください。

この章で使用するコマンドの完全なシンタックスについては、『*Cisco Security Appliance Command Reference*』を参照してください。

デジタル証明書の登録

この項では、CLI コマンドと ASDM を使用してデジタル証明書を登録する方法を説明します。登録が完了すると、その証明書を使用して VPN の LAN 間トンネルおよびリモート アクセス トンネルを認証できます。認証に事前共有鍵だけを使用する場合は、この項を読む必要はありません。

鍵ペア

各ピアには、公開鍵と秘密鍵の両方を含む鍵ペアが 1 つあります。これらの鍵は補完的に動作します。一方の鍵で暗号化された通信は、もう一方の鍵で復号化されます。

鍵ペアは RSA 鍵です。ASA では今後は DSA 鍵をサポートしなくなります。RSA 鍵には次の特性があります。

- RSA 鍵は、セキュリティ アプライアンスへの SSH アクセスまたは SSL アクセスをサポートします。
- SCEP 登録は、RSA 鍵の証明書でサポートされます。
- 鍵の生成が目的の場合、RSA 鍵の最大絶対値は 2048 です。デフォルトのサイズは 1024 ビットです。
- シグニチャ操作の場合、サポートされている鍵の最大サイズは RSA 鍵では 4096 ビットです。
- 生成した*汎用目的の* RSA 鍵ペアは、署名と暗号化の両方に使用できます。*特定用途向けの* RSA 鍵ペアの場合は、それぞれの目的に応じて分かれるため、対応する ID ごとに 2 つの証明書が必要です。デフォルトの設定は、汎用目的です。

証明書に鍵ペアを設定するには、生成する鍵ペアを識別するラベルを指定します。次の項では、CLI を使用してデフォルト ラベル付きの RSA 鍵ペアを生成する方法、ASDM を使用して指定のラベル付きの RSA 鍵ペアを生成する方法、およびその他のパラメータのデフォルト設定を使用する方法を説明します。

コンフィギュレーション手順の概要

CA に登録し、トンネルを認証するための ID 証明書を取得するには、次の手順を実行します。

（注） この例では、自動（SCEP）登録を示します。

1. ID 証明書の RSA 鍵ペアを作成します。
2. トラストポイントを作成します。この例のトラストポイントの名前は newmsroot です。
3. 登録 URL を設定します。この例で使用している URL は、http://10.20.30.40/certsrv/mscep/mscep.dll です。
4. CA を認証します。
5. CA に登録し、ID 証明書を ASA 上に取得します。

CLI コマンドを使用した手順

show crypto key mypubkey RSA コマンドを入力すると、現在実行されている鍵ペアを表示できます。

鍵ペアを生成する CLI コマンドの完全なシンタックスは、次のとおりです。

crypto key generate rsa [**usage-keys** | **general-keys**] [**label** *key-pair-label*] [**modulus** *size*]

たとえば、グローバル コンフィギュレーション モードの場合、デフォルト名 <Default-RSA-Key> を持つ RSA 鍵ペアを生成するには、次のコマンドを入力します。

```
hostname(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
```

ASDM を使用した手順

ASDM を使用して RSA 鍵ペアを生成するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Key Pair** パネルで、**Add** 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。

a. **Name**：デフォルト名を使用する場合はクリックします。または、鍵ペアの名前を入力します。この例では、key1 という名前を使用します。

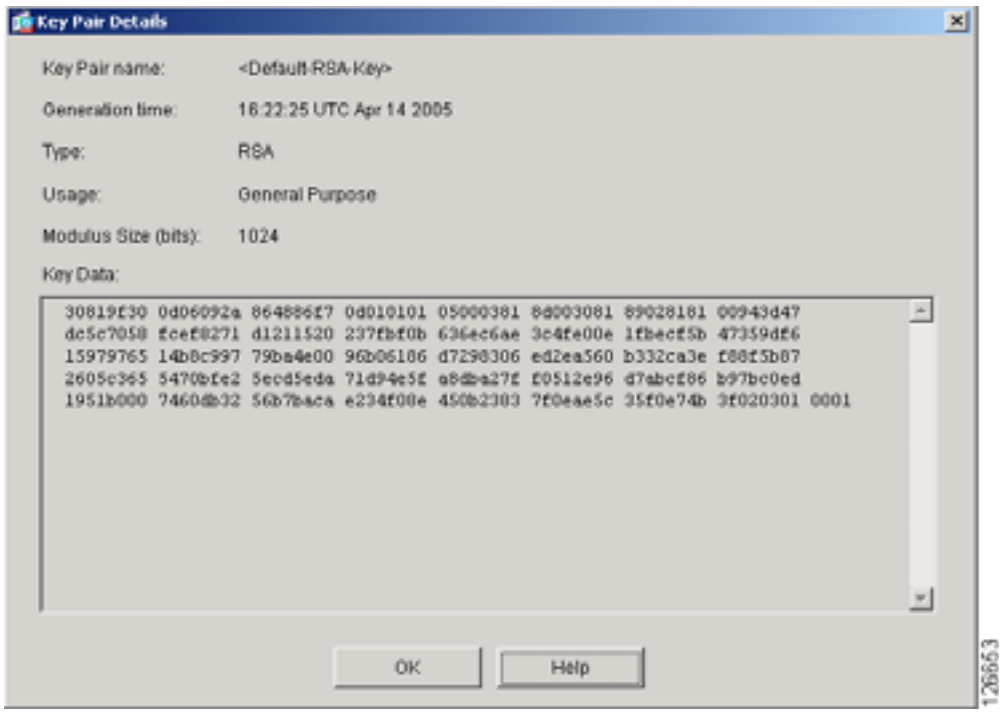
b. **Size** リスト：RSA 鍵ペアの場合、**Size** リストには、オプションとして 512、768、1024、または 2048 が表示されます。デフォルト サイズは 1024 です。この例では、デフォルト設定を受け入れます。

c. **Usage** オプション：Type が RSA の場合だけ使用できます。オプションは、General Purpose（署名および暗号化の両方に 1 つのペアを使用）と Special（機能ごとに 1 つのペアを使用）です。この例では、デフォルト設定（General Purpose）を受け入れます。

ステップ 3　**Generate Now** をクリックします。

ステップ 4　生成された鍵ペアを表示するには、**Show Details** をクリックします。ASDM に、鍵ペアに関する情報が表示されます。図 4-1 に出力例を示します。

図 4-1　鍵ペアの詳細表示



トラストポイントの作成

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。トラストポイントを作成するには、使用するインターフェイスの項を参照してください。

CLI コマンドを使用した手順

トラストポイントの作成には、**crypto ca trustpoint** CLI コマンドを使用します。このコマンドを使用すると、config-ca-trustpoint モードに移行し、トラストポイント情報を管理できるようになります。このコマンドの後に必要なコマンドは、2 つのトラストポイント コマンド **enrollment url** および **subject-name** だけです。

次の手順に従って、コマンド例のシンタックスを使用します。

ステップ 1　グローバル コンフィギュレーション モードから config-ca-trustpoint モードに移行して、新しいトラストポイントを作成します。この例では、トラストポイントの名前は newmsroot です。

```
hostname(config)# crypto ca trustpoint newmsroot
```

ステップ 2　自動登録（SCEP）を指定し、このトラストポイントに登録して登録 URL を設定するには、**enrollment url** コマンドを使用します。次に、証明書の認定者（X.500）の名前を指定するために、**subject-name** コマンドを使用します。これが、この証明書を使用するユーザまたはシステムになります。DN フィールドは、グループ マッチングをサポートしていません。この例では、Common Name（CN; 通常名）と Organizational Unit（OU; 組織ユニット）を使用します。

```
hostname(config-ca-trustpoint)# enrollment url
http://10.20.30.40/certsrv/mscep/mscep.dll
hostname(config-ca-trustpoint)# subject-name CN=Pat, OU=Techpubs
```

ステップ 3　（オプション）トラストポイントの設定（デフォルト パラメータと値など）を表示します。

```
hostname(config-ca-trustpoint)# show run all crypto ca trustpoint newmsroot
crypto ca trustpoint newmsroot
 crl nocheck
 enrollment retry period 1
 enrollment retry count 0
 enrollment url http://10.20.30.40/certsrv/mscep/mscep.dll
 fqdn hostname.ciscopix.com
 no email
 subject-name CN=Pat, OU=Techpubs
 serial-number
 no ip-address
 no password
 id-cert-issuer
 accept-subordinates
 support-user-cert-validation
 crl configure
  policy cdp
  cache-time 60
  enforcenextupdate
  protocol http
  protocol ldap
  protocol scep
```

ASDM を使用した手順

ASDM を使用して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** パネルで、**Add** 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** ボックス：**Trustpoint Name** ボックスにトラストポイントの名前を入力します。この例では、名前は newmsroot です。

b. **Enrollment URL** ボックス：**Enrollment Settings** パネルの **Enrollment Mode** グループ ボックスで、**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。この例では、**10.20.30.40/certsrv/mscep/mscep.dll** と入力します。

ステップ 3　CN と OU の名前を使用して、サブジェクト名を設定します。

a. **Enrollment Settings** パネルの **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鍵ペアを選択します。この例では、鍵ペアは key1 です。

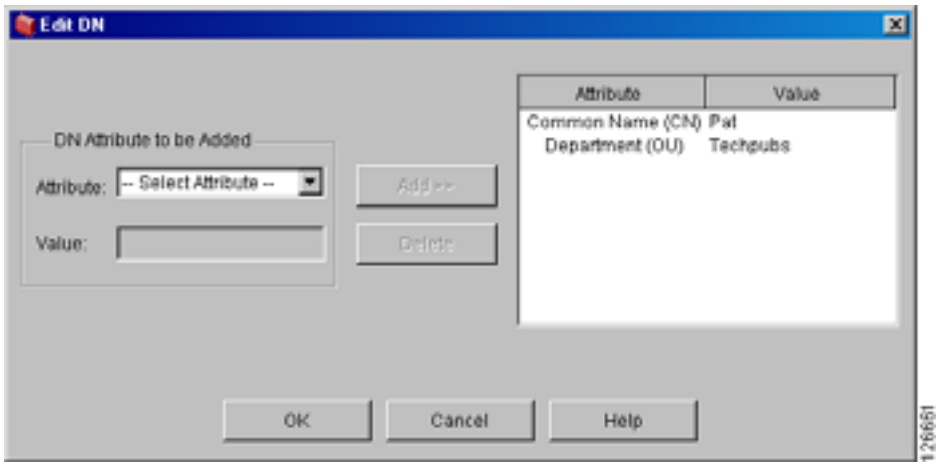
b. **Enrollment Settings** パネルで、**Certificate Parameters** をクリックします。

c. サブジェクト認定者（X.500）の名前の値を追加するには、**Certificate Parameters** ダイアログボックスで **Edit** 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** をクリックします。DN 情報を入力したら **OK** をクリックします。

この例では、まず **Common Name (CN)** を選択し、**Value** ボックスに **Pat** と入力します。次に Add をクリックしてから **Department (OU)** を選択して、**Value** ボックスに **Techpubs** と入力します。図 4-2 は、**Edit DN** ダイアログボックスに入力した内容を示しています。

図 4-2　サブジェクト名のアトリビュートと値



ステップ 4　ダイアログボックスを確認したら **OK** をクリックして、残りの 2 つのダイアログボックスで **OK** をクリックします。

SCEP による証明書の取得

ここでは、SCEP を使用した証明書の設定方法を説明します。自動登録の場合は、設定するトラストポイントごとに手順を繰り返します。各トラストポイントに対する手順が完了すると、ASA は CA 証明書をトラストポイント用に 1 つ、そして署名および暗号化用に 1 つまたは 2 つを受信します。これらの手順を実行しない場合、ASA によって base-64 形式の CA 証明書をテキストボックスに貼り付けるよう求められます。

汎用目的の RSA 鍵を使用する場合、受信した証明書は署名と暗号化を目的としたものです。署名と暗号化に別個の RSA 鍵を使用すると、セキュリティ アプライアンスは目的ごとに別個の証明書を受信します。

CLI コマンドを使用した手順

証明書を取得するには、グローバル コンフィギュレーション モードで **crypto ca authenticate** コマンドを使用します。オプションとして、英数字で構成されたフィンガープリントを ASA に提供し、CA 証明書の認証に使用することもできます。このコマンドを発行すると、対話モードに移行します。証明書のフィンガープリントが表示され、その証明書を受け入れるかどうかを確認するプロンプトが表示されます。この証明書を受け入れるには、**yes**（または **y**）と入力します。

（注） この例では、「フィンガープリント」を使用した証明書の確認方法を示します。ただし、すべての CA でこの確認が必要なわけではありません。

```
hostname(config)# crypto ca authenticate newmsroot
INFO: Certificate has the following attributes:
Fingerprint:     3736ffc2 243ecf05 0c40f2fa 26820675

Do you accept this certificate? [yes/no]: y

Trustpoint 'newmsroot' is a subordinate CA and holds a non self signed cert.
Trustpoint CA certificate accepted.
```

ASDM を使用した手順

ASDM を使用して証明書を取得するには、次の手順を実行します。

ステップ 1　**Configuration >Properties > Certificate > Authentication** パネルに移動します。

ステップ 2　**Trustpoint Name** リストで、トラストポイントの名前を選択します。この例では、**newmsroot** を選択します。

ステップ 3　**Authenticate** をクリックします。

ステップ 4　**Apply** をクリックします。**Authentication Successful** ダイアログが表示されたら、**OK** をクリックします。

認証局への登録

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。

CLI コマンドを使用した手順

show running-config crypto ca certificates *trustpoint_name* コマンドおよび **show running-config crypto ca trustpoint** *trustpoint_name* コマンドを使用すると、特定のトラストポイントの実行コンフィギュレーションを表示できます。

SCEP 登録のためにトラストポイントを設定した場合、次の例に示すように、ASA に CLI プロンプトが表示され、コンソールにステータス メッセージが表示されます。

登録を開始するには、**crypto ca enroll** コマンドを使用します。シンタックスは、**crypto ca enroll** *trustpoint* [**noconfirm**] です。開始する前に、パスワードを決定してください。

(注)　対話型のプロンプトは、参照されるトラストポイントの設定状態によって異なります。

```
hostname(config)# crypto ca enroll newmsroot
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: v$bx8*c

Re-enter password: v$bx8*c
% The subject name in the certificate will be: CN=Pat, OU=Techpubs
% The fully-qualified domain name in the certificate will be: hostname.ciscopix.com

% Include the router serial number in the subject name? [yes/no]: y
% The serial number in the certificate will be: P3000000098

Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
hostname(config)# The certificate has been granted by CA!
```

これで、CA と ID 証明書の両方を入手できました。

ASDM を使用した手順

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** パネルに移動します。

ステップ 2　**Trustpoint Name** リストでトラストポイントを選択します。この例では、**newmsroot** を選択します。

ステップ 3　**Enroll** をクリックします。

ASDM での証明書の管理

証明書を管理するには、**Configuration > Properties > Certificate > Manage Certificates** パネルに移動します。

新しい証明書の追加や証明書の削除には、このパネルを使用します。**Show Details** をクリックすると、証明書に関する情報を表示することもできます。Certificate Details ダイアログには、General、Subject、および Issuer という 3 つのテーブルがあります。

General パネルには、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 または Pending
  - 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：General purpose または Signature
- CRL distribution point (CDP)：証明書を検証するために CRL を取得する URL
- Dates/times within which the certificate is valid：発効日、有効期限

Subject テーブルには、次の情報が表示されます。

- Name：証明書を所有しているユーザまたはエンティティの名前
- Serial number：ASA のシリアル番号
- Distinguished (X.500) name fields for the subject of the certificate：cn、ou、など
- 証明書保有者のホスト名

Issuer テーブルには、証明書を付与したエンティティの認定者名のフィールドが表示されます。

- 通常名（cn）
- 組織ユニットまたは部門（ou）
- 組織（o）
- 地名（l）
- 州（st）
- 国番号（c）
- 発行者の電子メール アドレス（ea）

LAN 間トンネルの設定

ASA とピア デバイスとの間に IPSec LAN 間トンネルを設定する最も容易な方法は、VPN ウィザードを使用することです。このウィザードの使用方法の詳細については、「VPN ウィザードを使用した VPN トンネルの設定」を参照してください。ここでは、ウィザードを実行する前に収集しておく必要のある情報のリストが示されています。

ウィザードを使用しないでトンネルを設定するか、または初期設定の後に変更を行う場合は、この項の手順を使用してください。この項では、CLI と ASDM を使用して LAN 間トンネルを設定する方法を説明します。この項ではさらに、ASA で使用する VPN の用語の一部についても説明します。この用語は、VPN 3000 コンセントレータのものとは異なります。

LAN 間 VPN 接続を構築するには、次のタスクを実行する必要があります。

- インターフェイスの設定
- ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化
- トランスフォーム セットの作成
- ACL の設定
- トンネル グループの定義
- 暗号マップの作成とインターフェイスへの暗号マップの適用
- IPSec トラフィックの許可

設定例

次のコマンドは、LAN 間接続の設定方法を示しています。以降の項では、この接続を設定する方法をステップごとに示します。また、事前共有鍵と証明書を使用した認証方法についても説明します。

```
hostname(config)# interface g0/0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto isakmp policy 1 authentication pre-share
hostname(config)# crypto isakmp policy 1 encryption 3des
hostname(config)# crypto isakmp policy 1 hash sha
hostname(config)# crypto isakmp policy 1 group 2
hostname(config)# crypto isakmp policy 1 lifetime 43200
```

（注） 次のコマンドは、1 回だけ実行します。これは、トンネルごとに実行する必要はありません。

```
hostname(config)# crypto isakmp enable outside
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec_l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
hostname(config)# crypto map abcmap 1 match address xyz
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
```

（注） 別のインターフェイスにトンネルを構築するのでない限り、次の 2 つのコマンドは 1 回だけ実行します。

```
hostname(config)# crypto map abcmap interface outside
hostname(config)# sysopt connection permit-vpn
hostname(config)# write mem
```

インターフェイスの設定

ASA には、少なくとも 4 つのインターフェイスがあり、ここではそのうち 2 つを外部インターフェイスと内部インターフェイスと呼びます。通常、外部インターフェイスはパブリック インターネットに接続され、内部インターフェイスはプライベート ネットワークに接続されてパブリック アクセスから保護されます。

ASA で 2 つのインターフェイスを設定およびイネーブル化し、名前、IP アドレス、およびサブネット マスクを割り当てます。オプションとして、セキュリティ レベル、速度、およびセキュリティ アプライアンスでの二重化操作を設定します（この例では示されていません）。

CLI コマンドを使用した手順

CLI でインターフェイスを設定するには、次の手順を実行します。上記の例のコマンド シンタックスを指針として使用します。

ステップ 1　グローバル コンフィギュレーション モードで、**interface** コマンド、および設定するインターフェイスのデフォルト名を入力します（たとえば g0/0）。この操作により、セッションがインターフェイス コンフィギュレーション モードに移行します。次に例を示します。

```
hostname(config)# interface g0/0
hostname(config-if)#
```

ステップ 2　**ip address** コマンド、およびインターフェイスの IP アドレスとサブネット マスクを入力します。次の例では、IP アドレスは 10.10.4.100、サブネット マスクは 255.255.0.0 です。

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

ステップ 3　インターフェイス名を指定するには、**nameif** コマンドを使用します。最大 48 文字使用できます。この名前は、設定後に変更できません。この例では、g0/0 インターフェイスの名前は outside です。

```
hostname(config-if)# nameif outside
hostname(config-if)##
```

ステップ 4　インターフェイスをイネーブルにするには、**shutdown** コマンドの **no** バージョンを使用します。デフォルトでは、インターフェイスはディセーブルです。

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

ステップ 5　変更内容を保存するには、**write memory** コマンドを使用します。

```
hostname(config-if)# write memory
hostname(config-if)#
```

ステップ 6　2 番目のインターフェイスを設定する場合も、同じ手順を使用します。

ASDM を使用した手順

ASDM がデバイスに送信する CLI コマンドを表示するには、**Options** メニューをクリックし、**Preferences** をクリックして、**Preview commands before sending to the device** を選択します。

ASDM を使用してこの例のインターフェイスを設定するには、次の手順を実行します。

ステップ 1　**Configuration > Interfaces** パネルで、**Add** をクリックします。**Add Interface** ダイアログボックスが開きます。

ステップ 2　**Hardware Port** リストでインターフェイスをクリックします。この例では、**g0/0** を選択します。

ステップ 3　**Enable Interface** をクリックします。

ステップ 4　**Interface Name** ボックスに名前を入力します。この例では、名前は outside です。

ステップ 5　**IP Address** ボックスに IP アドレスを入力します。この例では、IP アドレスは 10.10.4.100 です。

ステップ 6　**Subnet Mask** リストで、サブネット マスクをクリックします。この例では、**255.0.0.0** をクリックします。

ステップ 7　**Use Static IP** をクリックし（この例の場合）、次に **OK** をクリックします。

ステップ 8　コンフィギュレーションを保存するには（定期的に行う必要があります）、ツールバーで **Save** をクリックし、**Yes** をクリックします。

ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化

Internet Security Association and Key Management Protocol（ISAKMP）は IKE とも呼ばれるもので、2 つのホストが IPSec セキュリティ アソシエーションの構築方法について合意するためのネゴシエーション プロトコルです。各 ISAKMP ネゴシエーションは、フェーズ 1 およびフェーズ 2 と呼ばれる 2 つのセクションに分かれています。

フェーズ 1 では、最初のトンネルが作成されます。これは後で ISAKMP ネゴシエーション メッセージを保護します。フェーズ 2 では、データを保護するトンネルが作成されます。

ISAKMP ネゴシエーションの条件を設定するには、ISAKMP ポリシーを作成します。これには、次が含まれます。

- ピアの ID を保証するための認証方式（事前共有鍵または証明書のいずれか）。
- データを保護し、プライバシーを確保するための暗号化方式。
- メッセージと送信者の ID の整合性を確保するための Hashed Message Authentication Code（HMAC; ハッシュ メッセージ認証コード）方式。
- 暗号鍵を決定するアルゴリズムの強度を確立するための Diffie-Hellman グループ。ASA は、このアルゴリズムを使用して暗号鍵とハッシュ鍵を導出します。
- ASA が置換するタイミングを決定するための暗号鍵の期限満了タイマー。

表 4-1 は、IKE ポリシーのキーワードとそれらの値に関する情報を示しています。

表 4-1　フェーズ 1：CLI コマンドの IKE ポリシー キーワード

コマンド	キーワード	意味	説明
crypto isakmp policy authentication	rsa-sig	RSA シグニチャ アルゴリズムによって生成された鍵を持つデジタル証明書	ASA が各 IPSec ピアの ID を保証するために使用する認証方式を指定します。
	pre-share	事前共有鍵	
crypto isakmp policy encryption	des	56 ビットの DES-CBC	2 つの IPSec ピア間で伝送されるデータを保護する対称暗号アルゴリズムを指定します。デフォルトは 56 ビットの DES-CBC で、これは他のアルゴリズムより安全性は劣りますが高速です。
	3des	168 ビットの Triple DES	
	aes aes-192 aes-256		Advanced Encryption Standard では、128 ビット、192 ビット、および 256 ビットの鍵長をサポートしています。
crypto isakmp policy hash	sha	SHA-1（HMAC バリアント）	データ整合性を確保するために使用するハッシュ アルゴリズムを指定します。これは、想定した相手から着信したパケットであることと、そのパケットが中継の間に変更されていないことを保証するものです。デフォルトは SHA-1 です。MD5 は、SHA-1 よりもダイジェストが小さく、わずかに速いとされています。
	md5	MD5（HMAC バリアント）	
crypto isakmp policy group	1	グループ 1（768 ビット）	Diffie-Hellman グループ識別子を指定します。2 つの IPSec ピアは、互いに送信を行うことなく、これを使用して共有秘密鍵を導出します。デフォルトは、グループ 2（1024 ビットの Diffie-Hellman）です。
	2	グループ 2（1024 ビット）	
	5	グループ 5（1536 ビット）	
	7	グループ 7（楕円曲線フィールドのサイズは 163 ビット）	
crypto isakmp policy lifetime	整数値	120 ～ 2147483647 秒	SA ライフタイムを指定します。デフォルトは、86400 秒（24 時間）です。一般的な規則として、ライフタイムが短い方が（ある程度まで）、より安全な IKE ネゴシエーションになります。ただし、ライフタイムが長い方が、ASA は後の IPSec セキュリティ アソシエーションをよりすばやくセット アップします。

CLI コマンドを使用した手順

show run crypto isakmp コマンドを入力すると、現在実行されている ISAKMP コンフィギュレーションを表示できます。システム応答の「policy」の後ろに *優先順位*が表示されます。それに後続するコマンドでは、関連付けられている IKE ポリシーが一意に識別され、そのポリシーに割り当てられている優先順位が表示されます。これは、1 ～ 65,534 の整数になります。1 は優先順位が最も高く、65,534 が最も低くなります。

ISAKMP ポリシーを設定するには、グローバル コンフィギュレーション モードで、さまざまな引数を付けて **crypto isakmp policy** コマンドを使用します。isakmp policy コマンドのシンタックスは、次のとおりです。

crypto isakmp policy *priority* **attribute_name** [**attribute_value** | *integer*]

次の手順を実行します。上記の例のコマンド シンタックスを指針として使用します。

ステップ 1　認証方式を設定します。この例では、認証方式として、RSA シグニチャを指定します。デフォルトの設定は、**pre-share** です。この手順および後続の手順での優先順位は 1 です。

```
hostname(config)# crypto isakmp policy 1 authentication rsa-sig
hostname(config)#
```

ステップ 2　暗号化方式を設定します。この例では、デフォルト設定（**3des**）を示します。

```
hostname(config)# crypto isakmp policy 1 encryption 3des
hostname(config)#
```

ステップ 3　HMAC 方式を設定します。この例では、デフォルト設定（**sha**）を示します。

```
hostname(config)# crypto isakmp policy 1 hash sha
hostname(config)#
```

ステップ 4　Diffie-Hellman グループを設定します。この例ではグループ 2 を設定します。

```
hostname(config)# crypto isakmp policy 1 group 2
hostname(config)#
```

ステップ 5　暗号鍵のライフタイムを設定します。この例では、43,200 秒（12 時間）を設定します。デフォルト設定は、**86400** です。

```
hostname(config)# crypto isakmp policy 1 lifetime 43200
hostname(config)#
```

ステップ 6　outside という名前のインターフェイス上で ISAKMP をイネーブルにします（このアトリビュートには、デフォルト設定がありません）。

```
hostname(config)# crypto isakmp enable outside
hostname(config)#
```

ステップ 7　**write mem** コマンドを使用して、変更内容を保存します。

```
hostname(config)# write mem
hostname(config)#
```

ASDM を使用した手順

ASDM で ISAKMP ポリシーを設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN > IKE > Policies** パネルで、**Add** をクリックします。

ステップ 2　上記の例のコンフィギュレーションから情報を入力します。

a. **Priority** ボックスに **1** と入力します。
b. 事前共有鍵の場合、**Authentication** リストで **pre-share** をクリックします。証明書認証の場合、**rsa-sig** をクリックします。
c. **Encryption** リストで **3des** をクリックします。
d. **Hash** リストで **sha** をクリックします。
e. **D-H group** リストで **2** をクリックします。
f. **Lifetime** ボックスに 43200 と入力し、**Lifetime** リストで **Seconds** をクリックします。

ステップ 3　**OK** をクリックします。

ステップ 4　次に、インターフェイスで ISAKMP をイネーブルにします。**Configuration > Features > VPN > IKE > Global Parameters** パネルで、**Enable IKE** グループ ボックス内で対象のインターフェイスをクリックしてから、**Enable** をクリックします。

ステップ 5　**Apply** をクリックします。

トランスフォーム セットの作成

トランスフォーム セットは、暗号化方式と認証方式を組み合せたものです。ISAKMP との IPSec セキュリティ アソシエーションのネゴシエート中に、ピアは、特定のトランスフォーム セットを使用して特定のデータ フローを保護することに同意します。トランスフォーム セットは、両方のピアで同じである必要があります。

トランスフォーム セットを複数作成して、暗号マップ エントリでそれらのトランスフォーム セットを 1 つまたはそれ以上指定することもできます。ASA はそのトランスフォーム セットを使用して、暗号マップ エントリのアクセス リストで指定されているデータ フローを保護します。

有効な暗号化方式は次のとおりです。

- esp-des
- esp-3des
- esp-aes（128 ビット暗号化）
- esp-aes-192
- esp-aes-256
- esp-null

有効な認証方式は次のとおりです。

- esp-md5-hmac
- esp-sha-hmac

IPSec はトンネル モードで動作します。これは、パブリック インターネットなど、信頼できないネットワークを介して接続されている 2 つの ASA の間に IPSec を実装する方法です。これにはコンフィギュレーションは必要ありません。

CLI コマンドを使用した手順

show run crypto ipsec コマンドを入力すると、現在実行されているトランスフォーム セットのコンフィギュレーションを表示できます。

CLI を使用してトランスフォーム セットを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec transform-set** コマンドを使用します。シンタックスは次のとおりです。

crypto ipsec transform-set *transform-set-name encryption-method authentication-method*

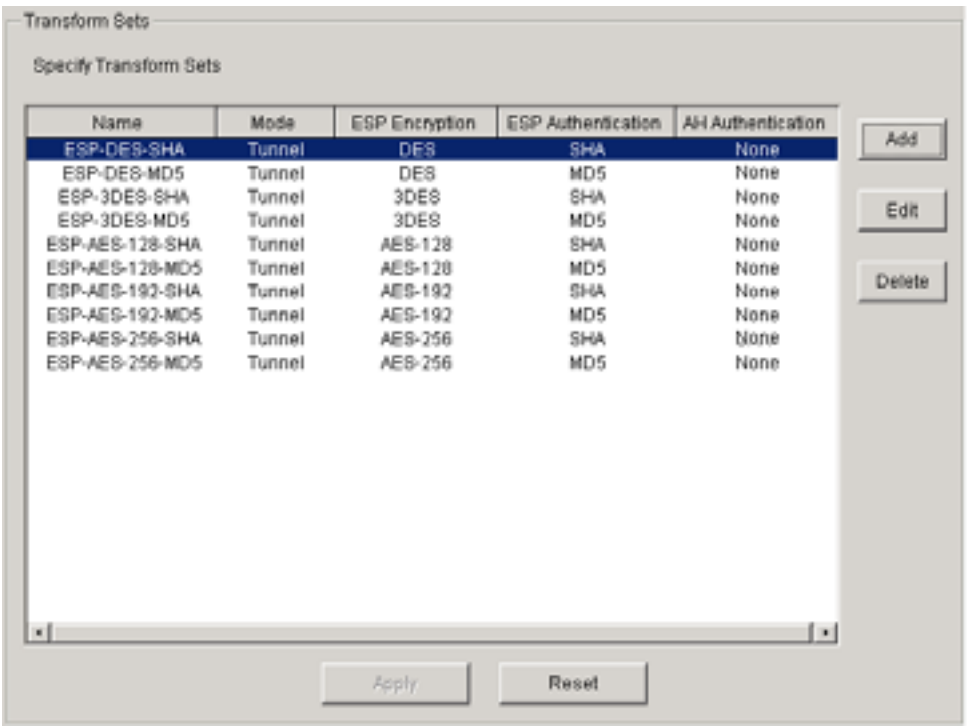
この例では、FirstSet という名前のトランスフォーム セット、esp-3des 暗号化、および esp-md5-hmac 認証を設定しています。

```
hostname(config)# crypto ipsec transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

ASDM を使用した手順

ASDM には、あらかじめ、標準のトランスフォーム セットがすべて設定されています。ほとんどの場合は、リストにトランスフォーム セットを追加する必要はありません。これらのトランスフォーム セットを表示するには、**Configuration** > **VPN** > **IPSec** > **Transform Sets** パネルに移動します。

図 4-3　Transform Sets テーブル



ACL の設定

ASA は Access Control List（ACL; アクセス コントロール リスト）を使用して、ネットワーク アクセスを制御します。デフォルトでは、ASA はすべてのトラフィックを拒否します。トラフィックを許可する ACL を設定する必要があります。

LAN 間 VPN 用に設定する ACL は、送信元および宛先の IP アドレスに基づいて接続を制御します。接続の両側で互いに反映するように ACL を設定します。

CLI コマンドを使用した手順

ステップ 1　ACL を設定するには、**access-list extended** コマンドを使用します。次の例では、l2l_list という名前の ACL を作成します。この ACL は、IP アドレスが 192.168.0.0 のネットワークから 150.150.0.0 のネットワークへのトラフィックの伝送を許可します。シンタックスは、次のとおりです。**access-list** *listname* **extended permit ip** *source-ipaddress source-netmask destination-ipaddress destination-netmask*

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)#
```

ステップ 2　上に示す ACL が反映される接続のもう一方の側で、ASA 用の ACL を設定します。この例では、ピアのプロンプトは hostname2 で、コマンドによってトラフィックを 150.150.0.0 ネットワークから 192.168.0.0 ネットワークに伝送できるようになります。

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0
192.168.0.0 255.255.0.0
hostname2(config)#
```

ASDM を使用した手順

ASDM を使用して ACL を設定するには、次の手順を実行します。

ステップ 1　**Configuration > Security Policy > Access Rules** パネルで、**Add** をクリックします。

ステップ 2　ほとんどのフィールドで、デフォルトを受け入れることができます。次の情報は入力する必要があります。

- 送信元ホストまたはネットワークの IP アドレスとマスク（たとえば、150.150.0.0/255.255.0.0）。
- 宛先ネットワークの IP アドレスとマスク（たとえば、192.168.0.0/255.255.0.0）。

トンネル グループの定義

トンネル グループとは、トンネル接続ポリシーが含まれたレコードのセットです。トンネル グループを設定して AAA サーバを識別し、接続パラメータを指定して、デフォルトのグループ ポリシーを定義します。ASA はトンネル グループを内部に格納します。

ASA システムには、次の 2 つのデフォルト トンネル グループがあります。

- DefaultRAGroup：デフォルトの IPSec リモート アクセス トンネル グループ
- DefaultL2LGroup：デフォルトの IPSec LAN 間トンネル グループ

これらのグループは変更できますが、削除はできません。また、環境に適応させるため、新しいトンネル グループを 1 つ以上作成できます。トンネル ネゴシエーションの間に特定のトンネル グループが識別されない場合、ASA はこれらの新しいトンネル グループを使用して、リモート アクセスおよび LAN 間のトンネル グループ用にデフォルトのトンネル パラメータを設定します。

基本の LAN 間接続を確立するには、トンネル グループに 2 つのアトリビュートを設定する必要があります。

- 接続タイプを IPSec LAN 間に設定します。
- 認証方式を設定します。この例では、事前共有鍵と証明書の両方のコンフィギュレーションが示されています。

CLI コマンドを使用した手順

show run all tunnel コマンドを入力して、現在実行されているトンネル グループ コンフィギュレーションを表示できます。

次の手順のように、**tunnel-group** コマンドを使用して、接続タイプを IPSec LAN 間に設定します。

ステップ 1　接続タイプを IPSec LAN 間に設定するには、**tunnel-group** コマンドを使用します。シンタックスは、**tunnel-group** *name* ***type*** *type* です。ここで、*name* はトンネル グループに割り当てる名前、*type* はトンネルのタイプです。CLI で入力するトンネル タイプは、次のとおりです。

- ipsec_ra（IPSec リモート アクセス）
- ipsec_l2l（IPSec LAN 間）

この例では、トンネル グループの名前は、LAN 間ピアの IP アドレスである 10.10.4.108 です。

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec_l2l
hostname(config)#
```

ステップ 2　認証方式を設定するには、ipsec-attributes モードに移行し、次に **pre-shared-key** コマンドを使用して事前共有鍵を作成します。この LAN 間接続では、両方の ASA に同一の事前共有鍵を使用する必要があります。証明書認証の場合、**trust-point** コマンドを使用します。

事前共有鍵は、1 ～ 127 文字の英数字文字列です。この例では、事前共有鍵は xyzx です。証明書認証の場合、トラストポイント名を指定します。この例では、newmsroot です。

事前共有鍵認証の場合、コマンドは次のとおりです。

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
```

また、デジタル証明書認証の場合、コマンドは次のとおりです。

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# trust-point newmsroot
```

ASDM を使用した手順

この例の情報を使用して ASDM でトンネル 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** > **VPN** > **General** > **Tunnel Group** パネルで、**Add** をクリックします。**Add Tunnel Group** ダイアログボックスが表示されます。これは、VPN 3000 Concentrator Manager の User Management セクションに似ています。

ステップ 2　**Identity** パネルで、**Name** ボックスにトンネル グループの名前を入力し、次に **IPSec for LAN to LAN** オプションをクリックします。この名前には、LAN 間ピアのホスト名または IP アドレス（この例では 10.10.4.108）を使用できます。

ステップ 3　**IPSec** パネルで、事前共有鍵認証の場合は **Pre-shared Key** ボックスに事前共有鍵を入力します。この例では、**xyzx** と入力します。証明書認証の場合、**Trustpoint Name** リストからトラストポイント名（**newmsroot**）を選択します。

暗号マップの作成とインターフェイスへの暗号マップの適用

暗号マップ エントリは、次のような IPSec セキュリティ アソシエーションの各種の要素をまとめたものです。

- IPSec で保護する必要があるトラフィック（アクセス リスト内で定義）
- IPSec によって保護されたトラフィックの送信先（ピアを特定することで指定）
- このトラフィックに適用される IPSec セキュリティ（トランスフォーム セットによって指定）
- IPSec トラフィックのローカル アドレス（インターフェイスに暗号マップを適用することで特定）

IPSec を成功させるには、設定に互換性のある暗号マップ エントリを両方のピアに用意する必要があります。このエントリは、IPSec リモート アクセス（ipsec-ra）または LAN 間（ipsec-l2l）です。2 つの暗号マップ エントリに互換性を持たせるには、少なくとも次の条件を満たす必要があります。

- 暗号マップ エントリに互換性のある暗号アクセス リスト（たとえば、ミラー イメージのアクセス リスト）が含まれている。応答ピアがダイナミック暗号マップを使用している場合、ASA 暗号アクセス リスト内のエントリは、ピアの暗号アクセス リストによって*許可*されている必要があります。
- 暗号マップ エントリはそれぞれ、他のピアを識別する（応答ピアがダイナミック暗号マップを使用していない場合）。
- 各ピアの暗号マップ エントリは、共通のトランスフォーム セットを少なくとも 1 つ持っている。

指定したインターフェイスに複数の暗号マップ エントリを作成する場合、各エントリのシーケンス番号（seq-num）を使用して、順位付けをします。小さいシーケンス番号の方が優先順位は高くなります。暗号マップ セットを持つインターフェイスでは、ASA は優先順位が最も高いマップのエントリから順にトラフィックを評価します。

次の条件のいずれかが存在する場合は、指定のインターフェイスに複数の暗号マップ エントリを作成します。

- 別個のピアが別個のデータ フローを処理する場合。
- 別個の IPSec セキュリティを異なるタイプのトラフィックに適用する場合（同一または別個のピアに対して）。たとえば、あるサブネットのセット間のトラフィックは認証し、別のサブネットのセット間のトラフィックは認証も暗号化も行う場合など。このケースでは、別個のタイプのトラフィックを 2 つの別個のアクセス リストで定義し、それぞれの暗号アクセス リストに別個の暗号マップ エントリを作成します。

CLI コマンドを使用した手順

show run crypto map コマンドを入力すると、現在実行されている暗号マップ コンフィギュレーションを表示できます。

グローバル コンフィギュレーション モードで暗号マップを作成し、その暗号マップを外部インターフェイスに適用するには、いくつかの **crypto map** コマンドを使用します。これらのコマンドではさまざまな引数を使用しますが、シンタックスはすべて **crypto map** *map-name-seq-num* で始まります。このコマンドの例では、マップ名は abcmap、シーケンス番号は 1 です。これらのコマンドをグローバル コンフィギュレーション モードで入力します。

ステップ 1　アクセス リストを暗号マップ エントリに割り当てるには、**crypto map match address** コマンドを使用します。

シンタックスは、**crypto map** *map-name seq-num* **match address** *aclname* です。この例では、マップ名は abcmap、シーケンス番号は 1、アクセス リスト名は xyz です。

```
hostname(config)# crypto map abcmap 1 match address xyz
hostname(config)#
```

ステップ 2　IPSec 接続に対してピア（複数可）を指定するには、**crypto map set peer** コマンドを使用します。

シンタックスは、**crypto map** *map-name seq-num* **set peer** {*ip_address1* | *hostname1*}[... *ip_address10* | *hostname10*] です。この例では、ホスト名は 10.10.4.108 です。

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)#
```

ステップ 3　暗号マップ エントリにトランスフォーム セットを指定するには、**crypto map set transform-set** コマンドを使用します。

シンタックスは、**crypto map** *map-name seq-num* **set transform-set** *transform-set-name* です。この例では、トランスフォーム セットの名前は FirstSet です。

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)#
```

ASDM を使用した手順

このコンフィギュレーション例の情報を使用して ASDM で暗号マップ機能を設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN > IPSec > Tunnel Policy** パネルで、**Add** をクリックします。

ステップ 2　インターフェイスとポリシー タイプを選択します。

a. **Interface** リストで **outside** をクリックします。

b. **Policy Type** リストで **Static** をクリックします。

ステップ 3　**Priority** ボックスに、優先順位（1）を入力します。

ステップ 4　**Transform Set to Be Added** リストでトランスフォーム セットをクリックし、**Add** をクリックします。この例では、**ESP-3DES-MD5** をクリックします。

ステップ 5　接続タイプを選択します。LAN 間の場合は、**Connection Type** リストから **Bidirectional** を選択します。

ステップ 6　ピア デバイスの IP アドレスを入力します。接続タイプが双方向の場合は、入力できるピア デバイスは 1 つだけです。**IP Address of Peer to be Added** ボックスに IP アドレス（この例では 192.168.1.1）を入力し、**Add** をクリックします。

インターフェイスへの暗号マップの適用

CLI インターフェイスを使用している場合は、IPSec トラフィックが経由するインターフェイスそれぞれに暗号マップ セットを適用する必要があります。ASA は、すべてのインターフェイスで IPSec をサポートしています。暗号マップ セットをインターフェイスに適用することにより、ASA はすべてのインターフェイス トラフィックを暗号マップ セットと対照させて評価し、接続中またはセキュリティ アソシエーション ネゴシエーション中に、指定されたポリシーを使用します。ASDM は、これらの操作を自動的に実行します。

インターフェイスに暗号マップをバインドすると、セキュリティ アソシエーション データベースやセキュリティ ポリシー データベースなど、実行時のデータ構造も初期化されます。後でどのように暗号マップを変更しても、ASA はその変更内容を実行コンフィギュレーションに自動的に適用します。この場合、既存の接続はドロップされ、新しい暗号マップが適用された後で再度確立されます。

設定済みの暗号マップを外部インターフェイスに適用するには、**crypto map interface** コマンドを使用します。

シンタックスは、**crypto map** *map-name* **interface** *interface-name* です。

```
hostname(config)# crypto map abcmap interface outside
hostname(config)#
```

IPSec トラフィックの許可

ASA は、デフォルトで IPSec トラフィックを許可します。

IPSec トラフィックがディセーブルの場合は、**sysopt connection permit-vpn** コマンドを使用して IPSec トラフィックを許可します。これは、IPSec トラフィックを受け入れるために、トンネル型トラフィックがインターフェイス ACL をバイパスすることによって実現されます。これは、復号化されたトラフィックがインターフェイス ACL の対象ではないことを意味します。

CLI コマンドを使用した手順

CLI コマンドを使用する場合は、次のようにして、IPSec トラフィックを許可してから、コンフィギュレーションを保存します。

ステップ 1　グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを使用し、ASA で IPSec トラフィックを許可します。

```
hostname(config)# sysopt connection permit-vpn
hostname(config)#
```

ステップ 2　変更内容を保存します。

```
hostname(config)# write mem
hostname(config)#
```

ASDM を使用した手順

ASDM では、IPSec トラフィックをイネーブルにしてから、コンフィギュレーションを保存します。次の手順を実行します。

ステップ 1　**Configuration > VPN > General > VPN System Options** パネルに移動します。

ステップ 2　**Enable IPSec authenticated inbound sessions to bypass interface access lists** オプションをクリックします。

ステップ 3　実行コンフィギュレーションをフラッシュ メモリに保存するには、ツールバーで **Save** をクリックし、確認を求められたら **Yes** をクリックします。

リモート アクセス トンネルの設定

リモート アクセス VPN トンネルを構築するには、次の手順を実行します。

- インターフェイスの設定
- ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化
- アドレス プールの設定
- ユーザの追加
- トランスフォーム セットの作成
- トンネル グループの定義
- ダイナミック暗号マップの作成
- ダイナミック暗号マップを使用するための暗号マップ エントリの作成（CLI のみ）
- IPSec トラフィックの許可

設定例の概要

このマニュアルでは、次の設定を使用して、リモート アクセス接続の設定方法を説明します。以降の項では、手順をステップごとに示します。ここでは、事前共有鍵と証明書を使用した認証方法を説明します。

```
hostname(config)# interface g0/0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# # no shutdown
hostname(config)# crypto isakmp policy 1 authentication pre-share
hostname(config)# crypto isakmp policy 1 encryption 3des
hostname(config)# crypto isakmp policy 1 hash sha
hostname(config)# crypto isakmp policy 1 group 2
hostname(config)# crypto isakmp policy 1 lifetime 43200
hostname(config)# crypto isakmp enable outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type ipsec_ra
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# sysopt connection permit-vpn
hostname(config)# write mem
```

インターフェイスの設定

セキュリティ アプライアンスには、少なくとも 2 つのインターフェイスがありますが、このマニュアルではそれらを外部と内部と呼んでいます。通常、外部インターフェイスはパブリック インターネットに接続され、内部インターフェイスはプライベート ネットワークに接続されてパブリック アクセスから保護されます。

まず、ASA で 2 つのインターフェイスを設定してイネーブルにします。次に、名前、IP アドレス、およびサブネット マスクを割り当てます。オプションとして、セキュリティ レベル、速度、およびセキュリティ アプライアンスでの二重化操作を設定します。

CLI コマンドを使用した手順

インターフェイスを設定するには、次の手順に従って、例に示したコマンド シンタックスを使用します。

(注)　すべてのインターフェイスの設定を表示するには、**show interface** コマンドを入力します。

ステップ 1　インターフェイス コンフィギュレーション モードに移行するには、グローバル コンフィギュレーション モードで、設定するインターフェイスのデフォルト名を使用して **interface** コマンドを実行します。この例では、インターフェイスは g0/0 です。

```
hostname(config)# interface g0/0
hostname(config-if)#
```

ステップ 2　インターフェイスの IP アドレスとサブネット マスクを設定するには、**ip address** コマンドを使用します。この例では、IP アドレスは 10.10.4.200、サブネット マスクは 255.255.0.0 です。

```
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)#
```

ステップ 3　インターフェイス名を指定するには、**nameif** コマンドを使用します。最大 48 文字使用できます。この名前は、設定後に変更できません。この例では、g0/0 インターフェイスの名前は outside です。

```
hostname(config-if)# nameif outside
hostname(config-if)#
```

(注)　インターフェイスに「outside」という名前を付けた場合、ASA はデフォルト設定の g0/0 と Security Level 0 を割り当てます。インターフェイスに「inside」という名前を付けた場合、ASA はデフォルト設定の g0/1 と Security Level 100 を割り当てます。

ステップ 4　インターフェイスをイネーブルにするには、**shutdown** コマンドの **no** バージョンを使用します。デフォルトでは、インターフェイスはディセーブルです。

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

ステップ 5　変更内容を保存するには、**write memory** コマンドを使用します。

```
hostname(config-if)# write memory
```

ステップ 6　同じ手順を使用して、2 番目のインターフェイスを設定します。

ASDM を使用した手順

ASDM を使用してこの例のインターフェイスを設定するには、次の手順を実行します。

ステップ 1　**Configuration > Interfaces** パネルで、**Add** をクリックします。**Add Interface** ダイアログボックスが開きます。

ステップ 2　**Hardware Port** リストでインターフェイスをクリックします。この例では、**g0/0** を選択します。

ステップ 3　**Enable Interface** をクリックします。

ステップ 4　**Interface Name** ボックスに名前を入力します。この例では、名前は outside です。

ステップ 5　**IP Address** ボックスに IP アドレスを入力します。この例では、IP アドレスは 10.10.4.200 です。

ステップ 6　**Subnet Mask** リストで、サブネット マスクをクリックします。この例では、サブネット マスクは 255.0.0.0 です。

ステップ 7　**Use Static IP** をクリックし（この例の場合）、次に **OK** をクリックします。

ステップ 8　コンフィギュレーションを保存するには（定期的に行う必要があります）、ツールバーで **Save** をクリックし、**Yes** をクリックします。

ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化

ISAKMP は、2 つのホストが IPSec セキュリティ アソシエーションの構築方法について合意するためのネゴシエーション プロトコルです。各 ISAKMP ネゴシエーションは、フェーズ 1 およびフェーズ 2 と呼ばれる 2 つのセクションに分かれています。

フェーズ 1 では、後で ISAKMP ネゴシエーション メッセージを保護する最初のトンネルが作成されます。フェーズ 2 では、データを保護するトンネルが作成されます。

ISAKMP ネゴシエーションの条件を設定するには、ISAKMP ポリシーを作成します。これには、次が含まれます。

- ピアの ID を保証するための認証方式。

  この項では、事前共有鍵と証明書の両方のコンフィギュレーションについて説明します。
- データを保護し、プライバシーを確保するための暗号化方式。
- 送信者の ID を保証し、また、中継の間にメッセージが変更されていないことを保証するための HMAC 方式。
- 暗号鍵のサイズを設定するための Diffie-Hellman グループ。セキュリティ アプライアンスは、このアルゴリズムを使用して暗号鍵とハッシュ鍵を導出します。
- 暗号鍵の期限満了タイマー。

その他の情報については、この章の LAN 間トンネルに関する項の表 4-1 を参照してください。

CLI コマンドを使用した手順

ISAKMP ポリシーを設定するには、グローバル コンフィギュレーション モードで、さまざまな引数を付けて **crypto isakmp policy** コマンドを使用します。isakmp policy コマンドのシンタックスは、次のとおりです。

crypto isakmp policy *priority* **attribute_name** [**attribute_value** | *integer*]

次の手順を実行します。上記の例のコマンド シンタックスを指針として使用します。

ステップ 1　認証方式を設定します。デフォルトの設定は、pre-share です。その他のオプションは、RSA シグニチャを認証方式として使用する **rsa-sig** です。

次に例を示します。

```
hostname(config)# crypto isakmp policy 1 authentication pre-share
hostname(config)#
```

ステップ 2　暗号化方式を設定します。この例では 3DES を設定します。

```
hostname(config)# crypto isakmp policy 1 encryption 3des
hostname(config)#
```

ステップ 3　HMAC 方式を設定します。この例では SHA を設定します。

```
hostname(config)# crypto isakmp policy 1 hash sha
hostname(config)#
```

ステップ 4　Diffie-Hellman グループを設定します。この例ではグループ 2 を設定します。

```
hostname(config)# crypto isakmp policy 1 group 2
hostname(config)#
```

ステップ 5　暗号鍵のライフタイムを設定します。この例では、43,200 秒（12 時間）を設定します。

```
hostname(config)# crypto isakmp policy 1 lifetime 43200
hostname(config)#
```

ステップ 6　outside という名前のインターフェイス上で ISAKMP をイネーブルにします。

```
hostname(config)# crypto isakmp enable outside
hostname(config)#
```

ステップ 7　**write mem** コマンドを使用して、変更内容を保存します。

```
hostname(config)# write mem
hostname(config)#
```

ASDM を使用した手順

ASDM で ISAKMP ポリシーを設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN > IKE > Policies** パネルで、**Add** をクリックします。

ステップ 2　上記の例のコンフィギュレーションから情報を入力します。

a. **Priority** ボックスに **1** と入力します。
b. 事前共有鍵の場合、**Authentication** リストで **pre-share** をクリックします。証明書認証の場合、**rsa-sig** をクリックします。
c. **Encryption** リストで **3des** をクリックします。
d. **Hash** リストで **md5** をクリックします。
e. **D-H group** リストで **2** をクリックします。
f. **Lifetime** ボックスに 43200 と入力し、**Lifetime** リストで **Seconds** をクリックします。

ステップ 3　インターフェイスで ISAKMP をイネーブルにするには、**Configuration > Features > VPN > IKE > Global Parameters** パネルに移動し、**Enable IKE** ボックスで対象のインターフェイスをクリックしてから、**Enable** をクリックします。

アドレス プールの設定

セキュリティ アプライアンスでは、ユーザに IP アドレスを割り当てる方式が必要です。一般的な方式は、アドレス プールを使用するというものです。代替方式として、DHCP サーバでアドレスを割り当てるか、または AAA サーバでアドレスを割り当てることもできます。この例では、アドレス プールを使用します。

CLI コマンドを使用した手順

アドレス プールを設定するとき、VPN クライアントに割り当てられている IP アドレスが標準以外のネットワークに所属する場合は、マスク値を入力する必要があります。デフォルト マスクを使用すると、データが正しくルーティングされない可能性があります。一般的な例は、IP ローカル プールに 10.10.10.0/255.255.255.0 というアドレスが含まれている場合です。これはデフォルトでクラス A ネットワークです。そのため、VPN クライアントが別のインターフェイスを介して 10 ネットワーク内の異なるサブネットにアクセスする必要が生じた場合に、ルーティング上の問題が発生することがあります。たとえば、アドレス 10.10.100.1/255.255.255.0 のプリンタがインターフェイス 2 経由で使用可能な一方で、10.10.10.0 ネットワークが VPN トンネル（インターフェイス 1）経由で使用可能である場合、VPN クライアントには、プリンタを宛先とするデータをどこにルーティングするかという混乱が生じます。サブネット 10.10.10.0 と 10.10.100.0 はどちらも 10.0.0.0 クラス A ネットワーク内にあるため、プリンタ データは VPN トンネル経由で送信される可能性があります。

アドレス プールを設定するには、**ip local pool** コマンドを使用します。シンタックスは、**ip local pool** *poolname first_address-last_address* [**mask** *mask*] です。次のコマンド例では、firstpool という名前の IP アドレス プールを設定します。開始アドレスは 10.20.30.40 で、終了アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
hostname(config)#
```

アドレス プール コンフィギュレーションを表示するには、**show running-config ip local pool** コマンドを使用します。

ASDM を使用した手順

ASDM でアドレス プ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 > VPN > IP Address Management > IP Pools** パネルで、**Add** をクリックします。

ステップ 2　名前、開始 IP アドレス、および終了 IP アドレスを入力します。この例では、次のように入力します。

a. **Name** ボックスに、testpool と入力します。
b. **Start IP** ボックスに、**192.168.0.10** と入力します。
c. **End IP** ボックスに、**192.168.0.15** と入力します。

ステップ 3　**Subnet Mask** リストで、標準ネットワーク マスクの 1 つをクリックします。この例では、**255.255.255.0** をクリックします。

ユーザの追加

ASA にリモート アクセス ユーザを設定するには、ユーザ名とパスワードを指定します。

CLI コマンドを使用した手順

各ユーザ用の内部データベースのエントリを設定するには、**username** コマンドを使用します。シンタックスは、**username** *username* **password** *password* です。この例では、ユーザ名は testuser で、パスワードは 12345678 です。外部認証の設定方法の詳細については、「外部サーバを使用する認証」を参照してください。

```
hostname(config)# username testuser password 12345678
hostname(config)#
```

ASDM を使用した手順

ASDM でユーザ名とパスワードを設定するには、次の手順を実行します。

ステップ 1　**Configuration > Properties> Device Administration > User Accounts** パネルで、**Add** をクリックします。

ステップ 2　ユーザ名とパスワードを入力し、パスワードを確認します。オプションとして特権レベルを入力します。この例では、次のように入力します。

a. **Identity** パネルで、**User Name** ボックスに **testuser** と入力します。
b. **Password** ボックスに **12345678** と入力します。
c. **Confirm Password** ボックスにパスワードをもう一度入力します。

トランスフォーム セットの作成

トランスフォーム セットは、暗号化方式と認証方式を組み合せたものです。ISAKMP との IPSec セキュリティ アソシエーションのネゴシエート中に、ピアは、特定のトランスフォーム セットを使用して特定のデータ フローを保護することに同意します。トランスフォーム セットは、両方のピアで同じである必要があります。

異なるアトリビュートを含むトンネルの組み合せをサポートできるようにトランスフォーム セットを複数設定して、暗号マップ エントリでそれらのトランスフォーム セットを 1 つまたはそれ以上指定することもできます。ASA はそのトランスフォーム セットを使用して、暗号マップ エントリのアクセス リストで指定されているデータ フローを保護します。有効な暗号化方式や認証方式など、その他の情報については、LAN 間トンネルに関する項にある「トランスフォーム セットの作成」を参照してください。

CLI コマンドを使用した手順

トランスフォーム セットを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec transform-set** コマンドを使用します。シンタックスは次のとおりです。

crypto ipsec transform-set *transform-set-name encryption-method authentication-method*

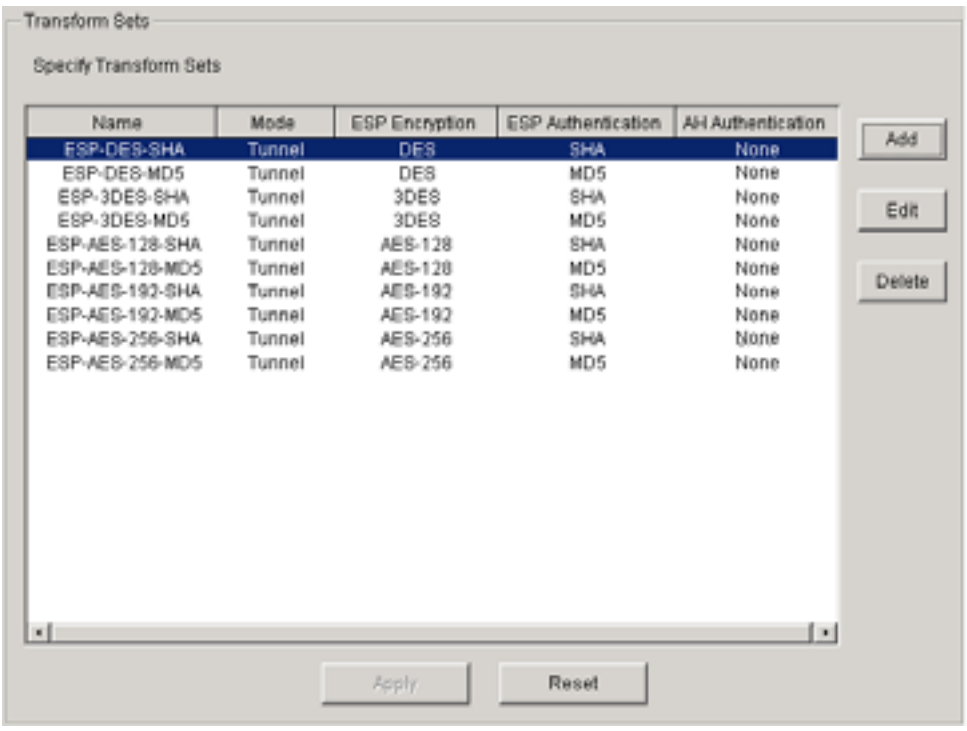
この例では、FirstSet という名前のトランスフォーム セット、esp-3des 暗号化、および esp-md5-hmac 認証を設定しています。

```
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

ASDM を使用した手順

ASDM には、あらかじめ、標準のトランスフォーム セットがすべて設定されています。ほとんどの場合は、リストにトランスフォーム セットを追加する必要はありません。これらのトランスフォーム セットを表示するには、**Configuration > VPN > IPSec > Transform Sets** パネルに移動します。

図 4-4　Transform Sets テーブル



トンネル グループの定義

トンネル グループとは、トンネル接続ポリシーが含まれたレコードのセットです。トンネル グループを設定して AAA サーバを識別し、接続パラメータを指定して、デフォルトのグループ ポリシーを定義します。ASA はトンネル グループを内部に格納します。

ASA システムには 2 つのデフォルト トンネル グループがあります。DefaultRAGroup（デフォルトの IPSec リモート アクセス トンネル グループ）と、DefaultL2LGroup（デフォルトの IPSec LAN 間トンネル グループ）です。これらを変更することはできますが、削除はできません。トンネル ネゴシエーションの間に特定のトンネル グループが識別されない場合、ASA はこれらのトンネル グループを使用してリモート アクセスおよび LAN 間のトンネル グループ用にデフォルトのトンネル パラメータを設定します。

基本のリモート アクセス接続を確立するには、トンネル グループに 3 つのアトリビュートを設定する必要があります。

- 接続タイプを IPSec_RA（リモート アクセス）に設定します。
- アドレス割り当て方式を設定します。次の手順ではアドレス プールを示します。
- 認証方式を設定します。次の手順では事前共有鍵とデジタル証明書を示します。

CLI コマンドを使用した手順

show run all tunnel コマンドを入力して、現在実行されているトンネル グループ コンフィギュレーションを表示できます。

CLI を使用してトンネル 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　接続タイプを IPSec リモート アクセスに設定するには、**tunnel-group** コマンドを使用します。コマンド シンタックスは、**tunnel-group** *name* ***type*** *type* です。ここで、*name* はトンネル グループに割り当てる名前、*type* はトンネルのタイプです。CLI で入力するトンネル タイプは、次のとおりです。

- ipsec_ra（IPSec リモート アクセス）
- ipsec_l2l（IPSec LAN 間）

この例では、トンネル グループの名前は testgroup で、タイプは ipsec_ra です。

```
hostname(config)# tunnel-group testgroup type ipsec_ra
hostname(config)#
```

ステップ 2　トンネル グループのアドレス プールを設定するには、一般アトリビュート モードに移行し、次に **address-pool** コマンドを使用してアドレス プールを作成します。この例では、グループの名前は testgroup で、アドレス プールの名前は testpool です。

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
```

ステップ 3　認証方式を設定するには、ipsec-attributes モードに移行し、次に **pre-shared-key** コマンドを使用して事前共有鍵を作成します。このリモート アクセス接続では、両方のデバイスに同一の事前共有鍵を使用する必要があります。証明書認証の場合、**trust-point** コマンドを使用します。

事前共有鍵は、1 ～ 127 文字の英数字文字列です。この例では、事前共有鍵は xyzx です。証明書認証の場合、トラストポイント名を指定します。この例では、newmsroot です。

事前共有鍵認証の場合、コマンドは次のとおりです。

```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
```

デジタル証明書認証の場合、コマンドは次のとおりです。

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# trust-point newmsroot
```

ASDM を使用した手順

ASDM を使用してトンネル 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 > VPN** > **General** > **Tunnel Group** パネルに移動して、**Add** をクリックします。

ステップ 2　**Identity** パネルで、**Name** ボックスにトンネル グループの名前を入力します。この例では、名前は testgroup です。

ステップ 3　**Type** グループで、**IPSec for Remote Access** オプションをクリックします。

ステップ 4　**Client Address Assignment** パネルの **Address Pool** グループから、追加済みのアドレス プールを選択して、**Add** をクリックします。

ステップ 5　**IPSec** パネルで、事前共有鍵認証の場合は **Pre-shared Key** ボックスに事前共有鍵を入力します。この例では、事前共有鍵は xyzx です。証明書認証の場合は、**Trustpoint Name** リストからトラストポイント名を選択します。この例では、名前は newmsroot です。

ダイナミック暗号マップの作成

ASA では、ダイナミック暗号マップを使用してポリシー テンプレートを定義します。これらのダイナミック暗号マップを使用すると、ASA は IP アドレスが不明な場合でもピアから接続を受信できます。リモートアクセス クライアントは、このカテゴリに入ります。

ダイナミック暗号マップ エントリは、接続のトランスフォーム セットを識別します。また、Reverse Route Injection（RRI）をイネーブルにすると、ASA は接続クライアントのルーティング情報を取得できます。ASA は RIP または OSPF 経由でこの情報をアドバタイズする必要があります。アドレスをすべての方式（AAA、IP プール、および DHCP プロキシ）から取得するクライアントについては、ASA は設定済みのルートを通知します。他のアドレス割り当て方式の場合、ASA はグローバル イネーブル / ディセーブル フラグを使用して、クライアント ルートのアドバタイズメントを決定します。

CLI コマンドを使用した手順

show run all crypto dynamic-map コマンドを入力すると、現在実行されている暗号ダイナミック マップ コンフィギュレーションを表示できます。

このコンフィギュレーション例の情報を使用して CLI でダイナミック暗号マップ機能を設定するには、次の手順を実行します。

ステップ 1　ダイナミック暗号マップ エントリのトランスフォーム セットを指定するには、次のコマンド シンタックスを使用します。

crypto dynamic -map *dynamic-map-name seq-num* **set transform-set** *transform-set-name*

次の例では、ダイナミック マップの名前は dyn1、シーケンス番号は 1、トランスフォーム セットの名前は FirstSet です。

```
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)#
```

ステップ 2　この暗号マップ エントリに基づく任意の接続に対して RRI をイネーブルにするには、次のように **crypto dynamic-map set reverse route** コマンドを使用します。

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)#
```

ステップ 3　変更内容を保存します。

```
hostname(config)# write mem
hostname(config)#
```

ASDM を使用した手順

このコンフィギュレーション例の情報を使用して ASDM でダイナミック暗号マップ機能を設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN > IPSec > Tunnel Policy** パネルで、**Add** をクリックします。

ステップ 2　**Interface** ボックスでインターフェイスをクリックします。この例では、**outside** をクリックします。

ステップ 3　**Policy Type** ボックスで **dynamic** をクリックします。

ASDM は、インターフェイスとポリシー タイプを組み合せてダイナミック マップの名前を付けます。この例では、暗号ダイナミック マップの名前は dyn1 になります。

ステップ 4　**Priority** ボックスに、優先順位（**1**）を入力します。

ステップ 5　**Transform Set to Be Added** リストでトランスフォーム セットをクリックし、**Add** をクリックします。この例では、**ESP-3DES-MD5** をクリックします。

ステップ 6　**Advanced** をクリックします。

ステップ 7　**Enable Reverse Route Injection** オプションをクリックします。

ステップ 8　**OK** をクリックして、**Tunnel Policy Advanced Settings** ダイアログボックスを閉じ、次にもう一度 **OK** をクリックして **Add Tunnel Policy** ダイアログボックスを閉じます。

ステップ 9　**Apply** をクリックします。

図 4-5 は、トンネル ポリシー コンフィギュレーションによって生成された CLI コマンドを示しています。暗号ダイナミック マップ dyn1 を参照する暗号マップ コマンドを ASDM が生成していることに注意してください。

図 4-5　トンネル ポリシー

```
crypto dynamic-map outside_dyn_map 1 set transform-set ESP-3DES-MD5
crypto dynamic-map outside_dyn_map 1 set security-association lifetime seconds 28800 kilobyte
crypto dynamic-map outside_dyn_map 1 set nat-t-disable
crypto dynamic-map outside_dyn_map 1 set reverse-route
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
```

ダイナミック暗号マップを使用するための暗号マップ エントリの作成（CLI のみ）

CLI を使用している場合、ASA がダイナミック暗号マップを使用して IPSec セキュリティ アソシエーションのパラメータを設定できるように、暗号マップ エントリを作成する必要があります。

（注）　ASDM を使用している場合は、ダイナミック暗号マップを使用するための暗号マップを作成する必要はありません。ASDM は暗号マップを自動的に作成します。

このコマンド例では、前の項「ダイナミック暗号マップの作成」で作成したのと同様、暗号マップの名前は mymap、シーケンス番号は 1、ダイナミック暗号マップの名前は dyn1 になります。これらのコマンドをグローバル コンフィギュレーション モードで入力します。

ステップ 1　ダイナミック暗号マップを使用する暗号マップ エントリを作成するには、**crypto map** コマンドを使用します。シンタックスは、**crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name* です。

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)#
```

ステップ 2　暗号マップを外部インターフェイスに適用するには、**crypto map interface** コマンドを使用します。

シンタックスは、**crypto map** *map-name* **interface** *interface-name* です。

```
hostname(config)# crypto map mymap interface outside
hostname(config)#
```

IPSec トラフィックの許可

ASA は、デフォルトで IPSec トラフィックを許可します。

IPSec トラフィックがディセーブルの場合は、**sysopt connection permit-vpn** コマンドを使用して IPSec トラフィックを許可します。これは、IPSec トラフィックを受け入れるために、トンネル型トラフィックがインターフェイス ACL をバイパスすることによって実現されます。これは、復号化されたトラフィックがインターフェイス ACL の対象ではないことを意味します。

CLI コマンドを使用した手順

CLI コマンドを使用する場合は、次のようにして、IPSec トラフィックを許可してから、コンフィギュレーションを保存します。

ステップ 1　グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを使用し、ASA で IPSec トラフィックを許可します。

```
hostname(config)# sysopt connection permit-vpn
hostname(config)#
```

ステップ 2　変更内容を保存します。

```
hostname(config)# write mem
hostname(config)#
```

ASDM を使用した手順

ASDM では、IPSec トラフィックをイネーブルにしてから、コンフィギュレーションを保存します。次の手順を実行します。

ステップ 1　**Configuration > VPN > General > VPN System Options** パネルに移動します。

ステップ 2　**Enable IPSec authenticated inbound sessions to bypass interface access lists** オプションをクリックします。

ステップ 3　実行コンフィギュレーションをフラッシュ メモリに保存するには、ツールバーで **Save** をクリックし、確認を求められたら **Yes** をクリックします。

CHAPTER 5

選択したユーザ管理タスクの実行

この章では、VPN 3000 Concentrator Manager の User Management セクションで設定可能な、いくつかの ASA ユーザ管理機能を設定する方法について説明します。ASA では、以前は基本グループ、グループ、およびユーザ アトリビュートとして設定できたすべての機能を、グループ ポリシーとトンネル グループを使用して設定できます。

この章では、次のユーザ管理タスクについて説明します。

- スプリット トンネリングおよびネットワーク リストの設定
- クライアント ファイアウォールおよび VPN の設定
- 外部サーバを使用する認証

(注) ASDM には、完全なオンラインヘルプ システムが付属しています。パネルのフィールド定義を参照する場合は、**Help** をクリックしてください。
この章で使用するコマンドの完全なシンタックスについては、『*Cisco Security Appliance Command Reference*』を参照してください。

スプリット トンネリングおよびネットワーク リストの設定

スプリット トンネリングは、IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにするものです。IPSec トンネルの反対側の宛先にバインドされていないパケットについては、暗号化してからトンネルを介して送信し、復号化してから最終的な宛先にルーティングする必要はありません。このように、スプリット トンネリングを使用すると、トラフィックの管理が簡単になり、処理負荷が軽減されます。

スプリット トンネリングは、単一ユーザのリモート アクセス IPSec トンネルにだけ適用されます。LAN 間の接続には適用されません。

スプリット トンネリングは、基本的にトラフィック管理機能であり、セキュリティ機能ではありません。実際のところ、最適のセキュリティを得るには、スプリット トンネリングをイネーブルにしないことをお勧めします。しかし、スプリット トンネリングをイネーブルにできるのはセキュリティ アプライアンスだけで、IPSec クライアントはイネーブルにできないので、実装を制御することによりセキュリティを保護できます。デフォルトでは、スプリット トンネリングはセキュリティ アプライアンスおよび IPSec クライアントの両方でディセーブルです。この機能を ASA でイネーブルにして設定すると、機能は ASA により ISAKMP を介して IPSec クライアントにプッシュされ、IPSec クライアントでイネーブルにされます。

この項のコマンド例は、CLI で access-list コマンドを使用するか、ASDM で ACL Manager を使用することによって、ネットワーク リストを設定する方法を示しています。また、ネットワーク リストを使用するスプリット トンネリング用の内部グループ ポリシーを設定する方法と、グループ ポリシーを使用するリモート アクセス トンネル グループを設定する方法も示しています。

コンフィギュレーション手順の概要

スプリット トンネリングを設定する手順は、次のとおりです。

1. 標準のアクセス リストを使用してネットワーク リストを定義します。
2. スプリット トンネリング グループ ポリシーを作成するか、既存のリモート アクセス グループ ポリシーを変更します。
3. スプリット トンネリング用のトンネル グループを作成します。

この項の手順では、次のシナリオを使用します。

- ネットワーク リストの名前は split。
- グループ ポリシーの名前は splitgroup。
- トンネル グループの名前は splittunnel。
- トンネル グループ タイプは IPSec_RA。
- トンネル グループでは、認証に事前共有鍵を使用する。

次に例を示します。

```
hostname(config)# access-list split standard permit 172.16.1.0 255.255.255.0
hostname(config)# access-list split standard permit 192.168.1.0 255.255.255.0
hostname(config)# group-policy splitgroup internal
hostname(config)# group-policy splitgroup attributes
    hostname(config-group-policy)# split-tunnel-policy tunnelspecified
    hostname(config-group-policy)# split-tunnel-network-list value split
hostname(config)# tunnel-group splittunnel type ipsec_ra
hostname(config)# tunnel-group splittunnel general-attributes
    hostname(config-general)# default-group-policy splitgroup
hostname(config)# tunnel-group splittunnel ipsec-attributes
    hostname(config-ipsec)# pre-shared-key v$bx8*c
```

ネットワーク リストの定義

最初に、組織の中央にある特定のネットワークへのセキュアなトラフィック フローを許可するネットワーク リストを定義します。次の項で使用する例では、ネットワーク アドレスは 172.16.1.0 255.255.255.0 および 192.168.1.0 255.255.255.0 で、ネットワーク リストの ID は split です。

CLI コマンドを使用した手順

ネットワーク リストを定義するには、access-list コマンドを使用します。この例で使用するコマンドのシンタックスは、次のとおりです。

access-list *identifier* **standard permit** *ipaddress*

(注) アクセス リストは標準タイプでも拡張タイプでもかまいません。

これらのアドレスへのトラフィックを許可するには、次の **access-list** コマンドを使用します。

```
hostname(config)# access-list split standard permit 172.16.1.0 255.255.255.0
hostname(config)# access-list split standard permit 192.168.1.0 255.255.255.0
```

ASDM を使用した手順

この項では、ASDM を使用してスプリット トンネリング用のネットワーク リストを設定する方法について説明します。ASDM の Group Policy パネルで、グループ ポリシーに名前を付け、ネットワーク リストおよびその他のスプリット トンネリング パラメータを定義します。

ネットワーク リストを定義するには、Group Policy Add/Edit Client Configuration タブからアクセスできる **ACL Manager** を使用します。スプリット トンネリング用のネットワーク リストを追加します（または既存のグループを編集します）。

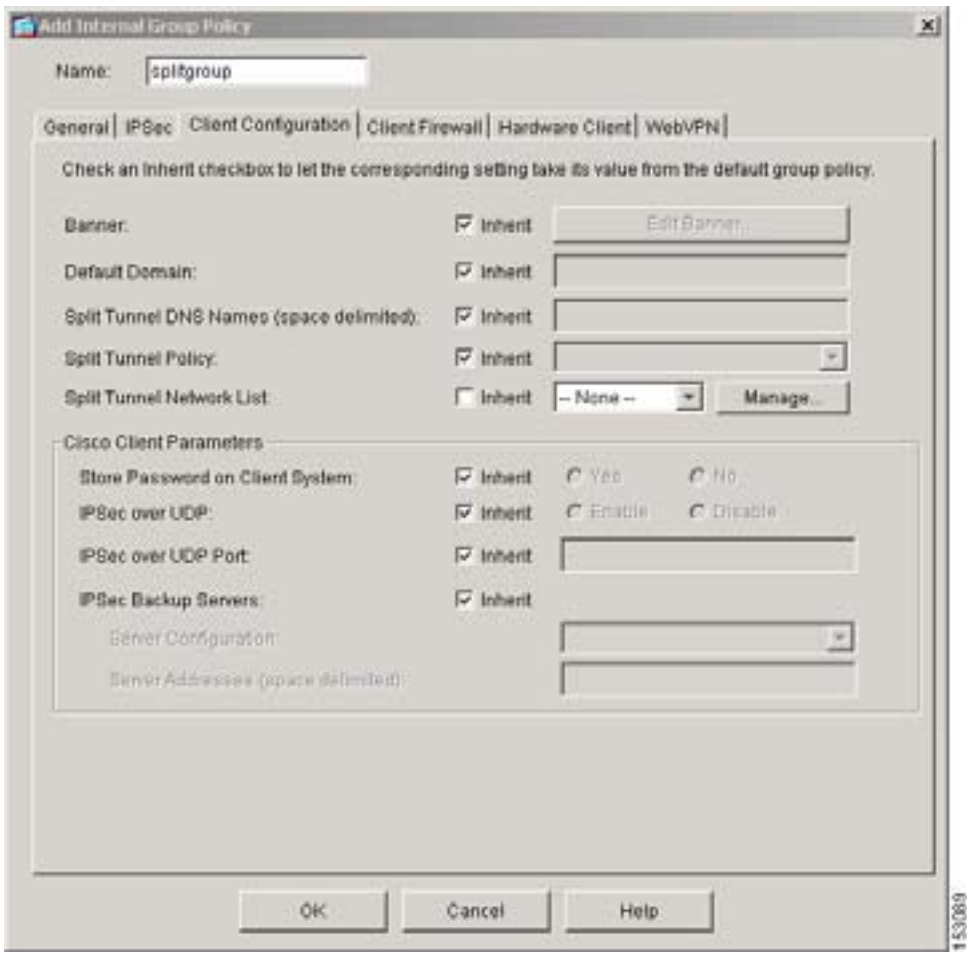
ステップ 1　Configuration > VPN > General > Group Policy パネルで **Add** をクリックし、メニューから **Internal Group Policy** を選択します。Add Internal Group Policy ダイアログボックスが表示され、General タブが示されます。

RADIUS などの外部サーバを選択するには、**External** オプションをクリックして、サーバ情報を入力します。

ステップ 2　新しいグループの名前を Name フィールドに入力します。この例では、名前は splitgroup です。

ステップ 3　**Client Configuration** タブをクリックします。Client Configuration オプションが表示されます（図 5-1 を参照してください）。

図 5-1　Add Internal Group Policy ダイアログボックス：Client Configuration



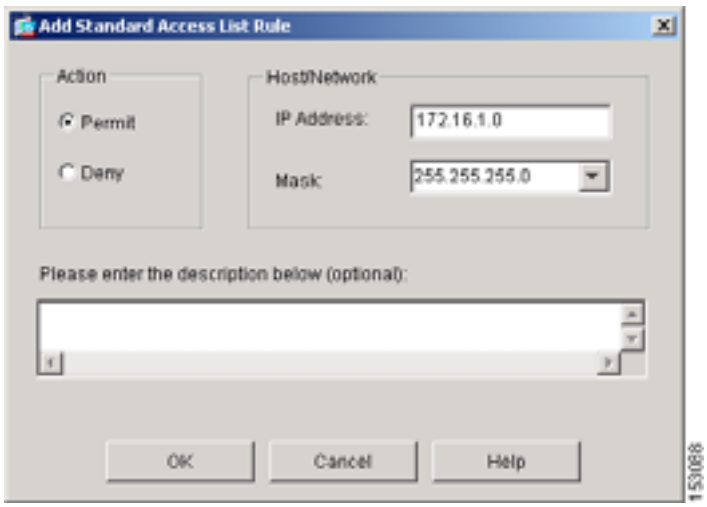
ステップ 4　ネットワーク リストの定義を開始するには、Split Tunnel Network List の横にある **Inherit** チェックボックスをオフにします。

ステップ 5　**Manage** をクリックします。ACL Manager テーブルが表示されます。

ステップ 6　ACL を追加するには、**Add** をクリックします。**ACL ID** フィールドに ACL の ID を入力し、**OK** をクリックします。この例では、名前は split です。

ステップ 7　**Add ACE** をクリックします。Add Standard Access List Rule ダイアログボックスが表示されます（図 5-2 を参照してください）。

図 5-2　スプリット トンネリング用の ACL の追加



ステップ 8　オプションを次のように設定します。

- Action オプション：ネットワーク リストに当該ネットワークを含めるには、**Permit** オプションをクリックします。
- Host/Network 領域：企業ネットワークまでトラフィックをセキュアにトンネリングできるように、含める各ホストまたはネットワークの IP アドレスとサブネット マスクを設定します。
  - IP Address：テキスト フィールドに IP アドレスを入力します。この例では、IP アドレスは 172.16.1.0 です。
  - Mask：リストでサブネット マスクをクリックします。この例では、サブネット マスクは 255.255.255.0 です。

ステップ 9　**OK** をクリックし、新しいグループ ポリシーのために Add Group Policy ダイアログボックスに戻ります。

スプリット トンネリング グループ ポリシーの作成

次の項では、スプリット トンネリング グループ ポリシーを作成する方法、またはデフォルトのグループ ポリシー（DfltGrpPolicy）を変更する方法について説明します。この例のコンフィギュレーション手順では、splitgroup という名前の、スプリット トンネリング用の特定の内部グループ ポリシーを作成します。

CLI コマンドを使用した手順

group-policy コマンドを使用して、config-group-policy モードでスプリット トンネリング ポリシーを設定します。split-tunnel-policy アトリビュートには次のオプションがあります。

- excludespecified：指定したネットワークのみ除外します。ネットワーク リスト内のアドレス宛のデータを除くすべてのデータを、セキュアな IPSec トンネルを介して送信します。この場合は、指定したネットワークまたはホスト宛のトラフィックを除くすべてのトラフィックが ASA のトンネルを通過します。

- tunnelall：すべてをトンネリングします。これがデフォルトのスプリット　トンネリング　ポリシーで、スプリット トンネリングはディセーブルになります。これが設定されている場合、トンネル グループ内のリモート クライアントからのトラフィックはすべて、暗号化された形式でセキュアな IPSec トンネルを通過します。
- tunnelspecified：指定したネットワークのみトンネリングします。セキュアな IPSec トンネルを介して、ネットワーク リスト内のアドレスにデータを送信します。その他のアドレス宛てのデータは、クリア テキストで伝送されます。このオプションを指定すると、リモート ユーザは、企業ネットワークを通じてトンネリングされることなくインターネット ネットワークにアクセスできると同時に、セキュアなトンネルを介して企業ネットワーク上の指定のリソースを使用できます。

次のコマンド例では、**tunnelspecified** オプションを使用して、ステップ 1 で作成したネットワーク リストに含まれるネットワークまでトラフィックをトンネリングします。

```
hostname(config)# group-policy splitgroup internal
hostname(config)# group-policy splitgroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
hostname(config-group-policy)# split-tunnel-network-list value split
```

ASDM を使用した手順

スプリット トンネリング用に既存のグループ ポリシーを編集することも、新しいグループ ポリシーを追加することもできます。スプリット トンネリング用に既存のグループ ポリシーを編集する場合、次の手順を実行します。

ステップ 1　以前に作成したグループの Add Group Policy ダイアログボックスで **Client Configuration** タブを選択します（図 5-1 を参照してください）。この例では、以前に作成したグループ ポリシーは splitgroup です。

ステップ 2　Split Tunnel Policy の横にある **Inherit** チェックボックスをオフにし、次のいずれかをクリックします。

- Tunnel All Networks：デフォルトのスプリット トンネリング ポリシーです。スプリット トンネリングはディセーブルになります。これが設定されている場合、トンネル グループ内のリモート クライアントからのトラフィックはすべて、暗号化された形式でセキュアな IPSec トンネルを通過します。トラフィックがクリア テキストで伝送されたり、ASA 以外の宛先に伝送されたりすることはありません。トンネル グループ内のリモート ユーザは、ローカル ネットワークにはアクセスせず、企業ネットワークを経由してインターネット ネットワークに到達します。
- Tunnel Network List Below：セキュアな IPSec トンネルを介して、ネットワーク リスト内のアドレスにデータを送信します。その他のアドレス宛てのデータは、クリア テキストで伝送されます。このオプションを指定すると、リモート ユーザは、企業ネットワークを通じてトンネリングされることなくインターネット ネットワークにアクセスできると同時に、セキュアなトンネルを介して企業ネットワーク上の指定のリソースを使用できます。
- Exclude Network List Below：ネットワーク リスト内のアドレス宛のデータを除くすべてのデータを、セキュアな IPSec トンネルを介して送信します。この場合は、指定したネットワークまたはホスト宛のトラフィックを除くすべてのトラフィックが ASA のトンネルを通過します。

  Exclude Network List Below オプションを使用すると、トンネル グループ内のすべてのユーザが、ローカル ネットワーク上のすべてのデバイスにアクセスできます。ユーザによるアクセスをローカル ネットワーク上の指定のデバイスに制限するには、トンネル グループ内のリモート ユーザがアクセスするローカル デバイスのアドレスを知っている必要があります。これらのアドレスからネットワーク リストを作成し、Split Tunneling Network List からネットワーク リストを選択します。1 つのトンネル グループには 1 つのネットワーク リストしか適用できません

が、1 つのネットワーク リストには最大 10 個のネットワーク エントリを含めることができます。Cisco VPN クライアントで **Local LAN Access** をイネーブルにする必要もあります。詳細については、『*Cisco VPN Client Administrator Guide*』を参照してください。

この例では、**Tunnel Network List Below** をクリックします。

ステップ 3　Split Tunnel Network List の横にある **Inherit** チェックボックスをオフにし、メニューから ACL を選択します。この例では **split** を選択します。

ステップ 4　**OK** をクリックし、Configuration > VPN > General > Group Policy パネルに戻ります。

ステップ 5　**Apply** をクリックし、新しい ACL とグループ ポリシーを実行コンフィギュレーションに追加します。

スプリット トンネリング用のトンネル グループの設定

最後に、次のいずれかの項の手順を使用して、スプリット トンネリング用のトンネル グループを追加するか、既存のグループを編集します。この手順の例では、splittunnel という名前のリモート アクセス トンネル グループを追加し、そのグループに、スプリット トンネリングを提供するデフォルトのグループ ポリシーを割り当てる方法を示しています。

CLI コマンドを使用した手順

スプリット トンネリング用のトンネリング グループを作成する手順は、次のとおりです。

```
hostname(config)# tunnel-group splittunnel type ipsec_ra
hostname(config)# tunnel-group splittunnel general-attributes
hostname(config-general)# default-group-policy splitgroup
hostname(config)# tunnel-group splittunnel ipsec-attributes
hostname(config-ipsec)# pre-shared-key v$bx8*c
```

ASDM を使用した手順

スプリット トンネリング用のトンネリング グループを作成する手順は、次のとおりです。

ステップ 1　Configuration > VPN > General > Tunnel Group パネルで **Add** をクリックし、トンネル グループのタイプを選択します。この例では **IPSec for Remote Access** を選択します。

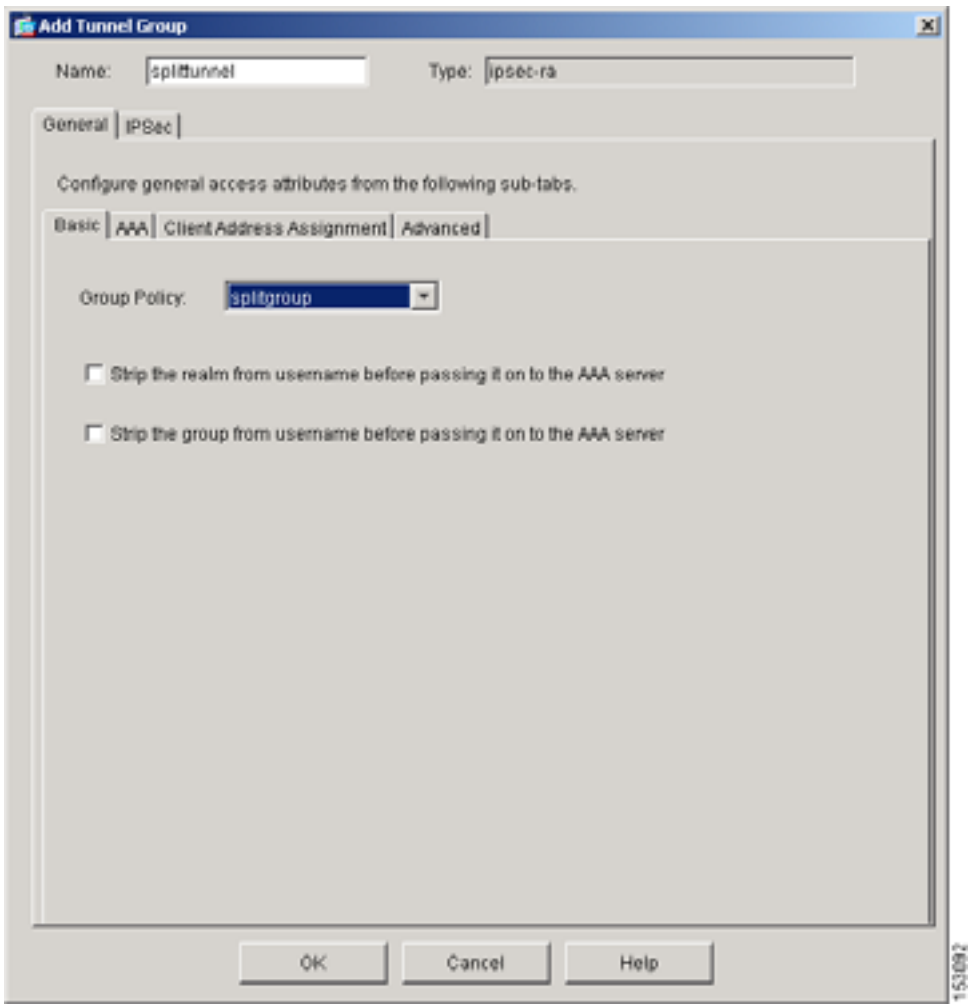
Add Tunnel Group ダイアログボックスが表示されます。

ステップ 2　**Name** フィールドにトンネル グループの名前を入力します。

この例では、名前は splittunnel です。

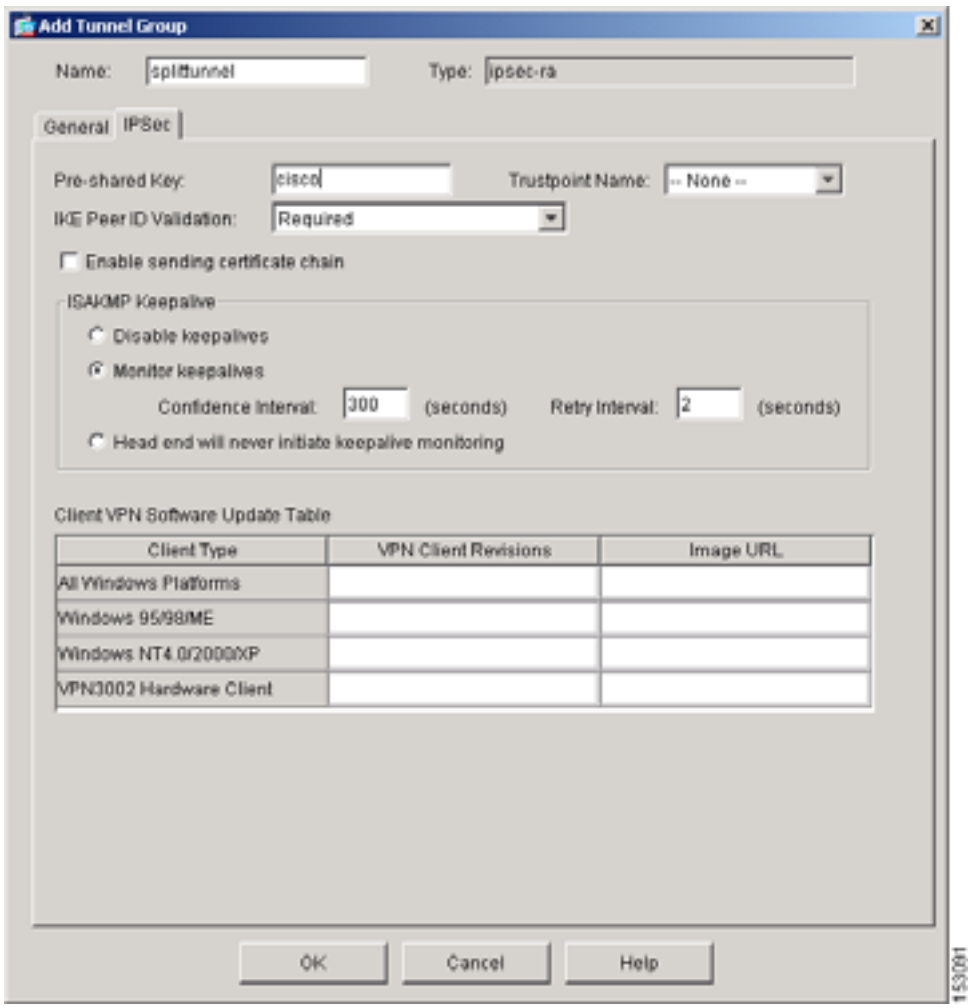
ステップ 3　**General** タブ、**Basic** タブの順にクリックし、次に Group Policy リストからグループ ポリシーを選択します。この例では、前の項で設定したグループ ポリシーである **splitgroup** をクリックします（図 5-3 を参照してください）。

図 5-3　Tunnel Group の追加：General タブと Basic タブ



ステップ 4　**IPSec** タブをクリックし、**Pre-shared Key** フィールドに事前共有鍵を入力します。この例では、**cisco** と入力して **OK** をクリックします。次に **Apply** をクリックします（図 5-4 を参照してください）。

図 5-4　トンネル グループの追加：IPSec タブ



ステップ 5　**OK** をクリックし、Configuration > VPN > General > Tunnel Group パネルに戻ります。

ステップ 6　**Apply** をクリックし、新しいトンネル グループをセキュリティ アプライアンスの実行コンフィギュレーションに追加します。

スプリット DNS 名

スプリット DNS を使用すると、集中定義された*ローカル ドメイン名*を内部 DNS サーバで解決できるようになります。それ以外のすべての DNS 要求は、ISP で割り当てられた DNS サーバによって解決されます。これは、スプリット トンネリング接続用です。トンネルを通過するトラフィックのドメイン名は内部 DNS サーバにより解決され、クリア テキストでインターネットに伝送される DNS 要求は、ISP で割り当てられた DNS サーバにより解決されます。

ASA では、Microsoft VPN クライアントのスプリット DNS はサポートされていません。ただし、Microsoft Windows オペレーティング システムで動作する Cisco VPN クライアントのスプリット DNS はサポートされています。

内部サーバにより解決される各ドメイン名を入力します。名前を区切るために使用できるのはスペースだけです。

クライアント ファイアウォールおよび VPN の設定

(注) これらのファイアウォール機能は、Microsoft Windows を実行している VPN クライアントだけで使用可能です。現在、ハードウェア クライアントまたはその他の（Windows 以外の）ソフトウェア クライアントでは使用できません。

トンネル グループ内のリモート ユーザがスプリット トンネリングを設定すると、クライアント ファイアウォールのセキュリティは強化されます。この場合、ファイアウォールは、インターネットまたはユーザのローカル LAN を経由した侵入からユーザの PC を保護することにより、企業ネットワークを保護します。

VPN クライアントから ASA に接続しているリモート ユーザは、2 つのファイアウォール オプションのいずれかを選択できます。

1 つ目のオプションは、リモート ユーザの PC にパーソナル ファイアウォールをインストールすることです。VPN クライアントは、ローカル ファイアウォールで定義されたファイアウォール ポリシーを強制的に適用し、動作を確認するためにファイアウォールを監視します。ファイアウォールの動作が停止すると、VPN クライアントは ASA への接続をドロップします（このファイアウォール適用メカニズムは *Are You There（AYT）*と呼ばれます。これは、VPN クライアントが「are you there?」というメッセージを定期的に送信することによってファイアウォールを監視するためです。応答がない場合、VPN クライアントはファイアウォールがダウンしていると判断し、セキュリティ アプライアンスへの接続を終了します）。ネットワーク管理者が元々これらの PC ファイアウォールを設定している場合がありますが、この方法を使用すれば、ユーザは独自のコンフィギュレーションをカスタマイズできます。

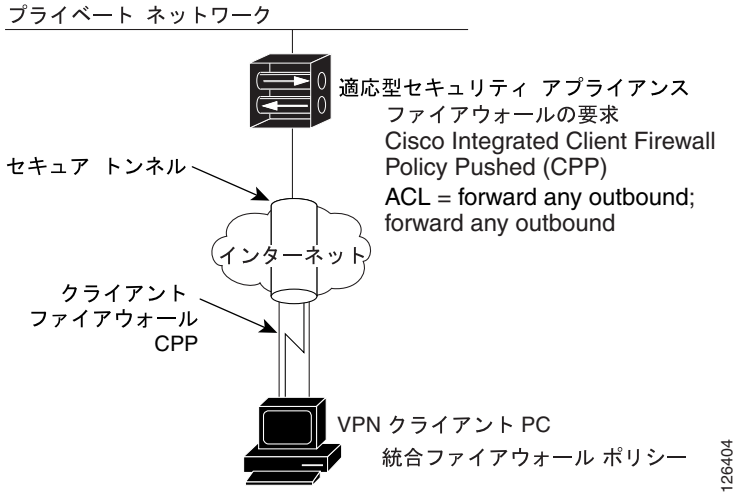
2 つ目のオプションは、パーソナル ファイアウォール用の集中型ファイアウォール ポリシーを VPN クライアント PC に強制的に適用することです。スプリット トンネリングを使用して、トンネル グループ内のリモート PC に対するインターネット トラフィックをブロックすることは、この方法の一般的な例です。この方法では、トンネルが確立されている間、インターネット経由の侵入から PC を保護することにより、中央のサイトを保護します。このファイアウォール シナリオは、*プッシュ ポリシー*または *Central Protection Policy（CPP）*と呼ばれます。ASA で、VPN クライアントに強制的に適用するファイアウォール ポリシーとして CPP を指定し、着信トラフィックおよび発信トラフィック用の ACL を追加します。ASA によってこのポリシーが VPN クライアントにプッシュされます。ポリシーは VPN クライアントによりローカルの Cisco Integrated Client ファイアウォールに渡され、そこで強制適用されます。

デフォルトとして使用するクライアント ファイアウォールの設定

この項の手順では、例として次のシナリオを使用します（図 5-5 を参照してください）。

- ファイアウォールが必要。ファイアウォール タイプは、Cisco Integrated Client Firewall です。
- スプリット トンネリング コンフィギュレーションでデフォルトとして使用できるアクセス リストが 2 つある。1 つ目のアクセス リストは、インターネット（またはトンネルの外側にある他のサイト）から VPN クライアントに着信する非請求トラフィックをすべて拒否します。この ACL は FWBlockIn と呼ばれます。2 つ目のアクセス リストは、VPN クライアントからトンネルの外側にあるサイトへの発信トラフィックを許可します。この ACL は FWAllowAnyOut と呼ばれます。プロトコルはどちらも IP です。

図 5-5　スプリット トンネリング コンフィギュレーション用に Cisco Integrated Client Firewall を使用したシナリオ



クライアント ファイアウォール コンフィギュレーション用のアクセス リストの設定（CLI）

この例で使用するクライアント アクセス リストを設定する CLI コマンドは、次のとおりです。

```
hostname(config)# access-list FWBlockIn deny ip any any
hostname(config)# access-list FWAllowAnyOut permit ip any any
hostname(config)# group-policy GroupPolicy4 attributes
hostname(config-group-policy)# client-firewall req cisco-integrated acl-in FWBlockIn
acl-out FWAllowAnyOut
```

1 つ目の **access-list** コマンドは、VPN クライアントへのすべての着信トラフィックをブロックするためのデフォルトとして動作できます。ACL の ID は FWBlockIn です。アクションは deny、プロトコルは ip です。送信元のアドレス / マスク、および宛先のアドレス / マスクは、両方とも any です（任意の場所から VPN クライアントへのトラフィックをすべてブロックします）。

2 つ目のコマンドは、VPN クライアントまたは VPN クライアントのグループからの発信トラフィックをすべて許可します。この ACL の ID は FWAllowAnyOut です。アクションは permit、プロトコルは ip です。送信元のアドレス / マスク、および宛先のアドレス / マスクは、両方とも any です（送信元から宛先へのトラフィックをすべて許可します）。

グループ ポリシーでのクライアント ファイアウォールの設定

この項では、CLI および ASDM で、グループ ポリシーの一部としてクライアント ファイアウォールを設定するための手順を示します。

CLI コマンドを使用した手順

show running-config group-policy *name* コマンドを使用すると、特定のグループ ポリシーの実行コンフィギュレーションを表示できます。

リモート ユーザ用の VPN クライアントまたは VPN クライアントのグループのファイアウォールを設定するには、**group-policy** コマンドを使用します。この例で使用するコマンドのシンタックスは、次のとおりです。

group-policy *name* **attributes**

client-firewall opt | **req cisco-integrated acl-in** *ACL* **acl-out** *ACL*

次のコマンドは、GroupPolicy4 という名前のグループ ポリシーを作成し、config-group-policy モードに移行して Cisco Integrated Firewall を要求するクライアント ファイアウォールを設定します。着信 ACL は FWBlockIn で、発信 ACL は FWAllowAnyOut です。この例を使用すると、デフォルト ファイアウォール ポリシーの設定を完了できます。

```
hostname(config)# group-policy GroupPolicy4 attributes
hostname(config-group-policy)# client-firewall req cisco-integrated acl-in FWBlockIn
acl-out FWAllowAnyOut
```

ASDM を使用した手順

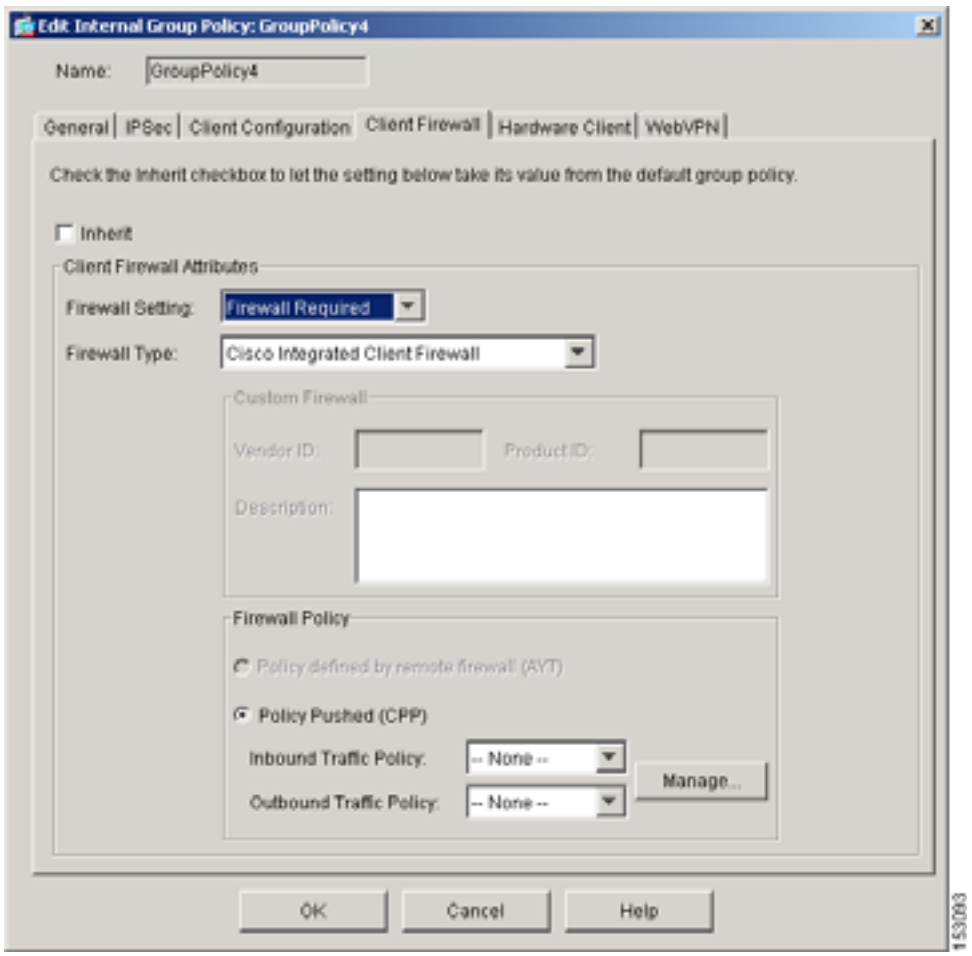
ASDM を使用してクライアント ファイアウォール プロテクションを設定するには、グループ ポリシーを追加するか、既存のグループ ポリシーを編集します。この例では、GroupPolicy4 という名前の既存のポリシーを編集します。

ステップ 1　Configuration > VPN > General > Group Policy パネルで、テーブルからグループ ポリシーを選択し、**Edit** をクリックします。ASDM に Edit Group Policy ダイアログボックスが表示されます。

ステップ 2　**Client Firewall** タブをクリックします。図 5-6 は、この例で設定されているクライアント ファイアウォール オプションを示しています。

- Inherit：オフ（ディセーブル）
- Firewall Setting：Firewall Required
- Firewall Type：Cisco Integrated Client Firewall
- Firewall Policy：Policy Pushed (CPP)

図 5-6　クライアント ファイアウォール オプション



ステップ 3　**Inherit** チェックボックスをオフにします。

ステップ 4　ファイアウォール設定を選択するには、Firewall Setting リストで対象のオプションをクリックします。この例では、Firewall Required を設定します。このリストには、次のオプションが含まれています。

- No Firewall：このトンネル グループ内のリモート ユーザにはファイアウォールが必要ありません。これがデフォルト設定です。
- Firewall Required：このトンネル グループ内のすべてのリモート ユーザは、特定のファイアウォールを使用する必要があります。指定のファイアウォールを使用しているユーザだけが接続できます。

  この例と同じように Firewall Required を選択した場合、トンネル グループ内のすべてのユーザは、指定されたファイアウォールを使用する必要があります。サポートされている指定のファイアウォールがインストールされ動作していない場合、接続を試行するすべてのセッションは ASA によりドロップされます。この場合は、ファイアウォール コンフィギュレーションが一致しないことを ASA が VPN クライアントに通知します。

（注）　トンネル グループ用のファイアウォールが必要な場合は、当該トンネル グループに Windows ベースの VPN クライアント以外のクライアントが含まれていないことを確認してください。トンネル グループに他のクライアントが含まれている場合（ハードウェア クライアントを含む）、それらのクライアントからは接続できません。

- Firewall Optional：このトンネル グループ内のすべてのリモート ユーザが接続できます。指定されたファイアウォールがある場合、ユーザはそれを使用できます。ファイアウォールがないユーザは、警告メッセージを受信します。

  トンネル グループ内のリモート ユーザがファイアウォール機能を使用できない場合は、Firewall Optional をクリックします。Firewall Optional 設定を使用すると、トンネル グループ内のすべてのユーザが接続できます。ファイアウォールがあるユーザは、それを使用できます。ファイアウォールがない状態で接続するユーザは、警告メッセージを受信します。

  この設定は、ファイアウォールがサポートされているユーザとファイアウォールがサポートされていないユーザが混在するトンネル グループを作成する場合に役立ちます。たとえば、トンネル グループを変更しつつあり、グループ内に、ファイアウォール機能の設定が完了したメンバと、ファイアウォールが設定されていないメンバが両方含まれる場合などです。

ステップ 5　Firewall Type リストからファイアウォールを選択します。この例では、Cisco Integrated Client Firewall を指定します。

指定するファイアウォールは使用できるファイアウォール ポリシーと相関関係にあるので注意してください。設定するファイアウォールによって、サポートされるファイアウォール ポリシー オプションが決まります（詳細については 表 5-1 を参照してください）。

次のいずれかをクリックします。

- **Cisco Integrated Client Firewall**：Cisco VPN クライアントに組み込まれているステートフル ファイアウォール。
- **Cisco Security Agent**：Cisco 侵入防御（サーバおよびデスクトップ システムに対する脅威からの保護）。
- **Custom Firewall**：同じベンダーからのファイアウォールの組み合せ、またはリストに含まれていない他のファイアウォール。このオプションを選択した場合、**Custom Firewall** グループ ボックスで独自のファイアウォールのリストを作成する必要があります。カスタム ファイアウォールを設定する手順は、このマニュアルには含まれていません。
- **Network ICE BlackICE Defender**：Network ICE BlackICE Agent または Defender パーソナル ファイアウォール。
- **Sygate Personal Firewall**
- **Sygate Personal Firewall Pro**
- **Sygate Security Agent**：Sygate Security Agent パーソナル ファイアウォール。
- **Zone Labs ZoneAlarm**：Zone Labs ZoneAlarm パーソナル ファイアウォール。
- **Zone Labs ZoneAlarm or ZoneAlarm Pro**：Zone Labs ZoneAlarm パーソナル ファイアウォールまたは Zone Labs ZoneAlarm Pro パーソナル ファイアウォールのいずれか。
- **Zone Labs ZoneAlarm Pro**：Zone Labs ZoneAlarm Pro パーソナル ファイアウォール。

ステップ 6　ファイアウォール ポリシーを選択するには、Firewall Policy グループ ボックスで対象のオプションをクリックします。

設定したファイアウォールに応じて、特定のファイアウォール ポリシー オプションを使用できます（表 5-1 を参照してください）。

表 5-1　各ファイアウォールで使用できるファイアウォール ポリシー オプション

ファイアウォール	Policy Defined by Remote Firewall (AYT)	Policy Pushed (CPP)
Cisco Integrated Client Firewall	使用不可	使用可
Cisco Security Agent	使用可	使用不可
Network ICE BlackICE Defender	使用可	使用不可
Sygate Personal Firewall	使用可	使用不可
Sygate Personal Firewall Pro	使用可	使用不可
Sygate Security Agent	使用可	使用不可
Zone Labs ZoneAlarm	使用可	使用可
Zone Labs ZoneAlarm or Zone Labs ZoneAlarm Pro	使用可	使用可
Zone Labs ZoneAlarm Pro	使用可	使用可

ステップ 7　ファイアウォール ポリシーに関連付けられているオプションから選択します。

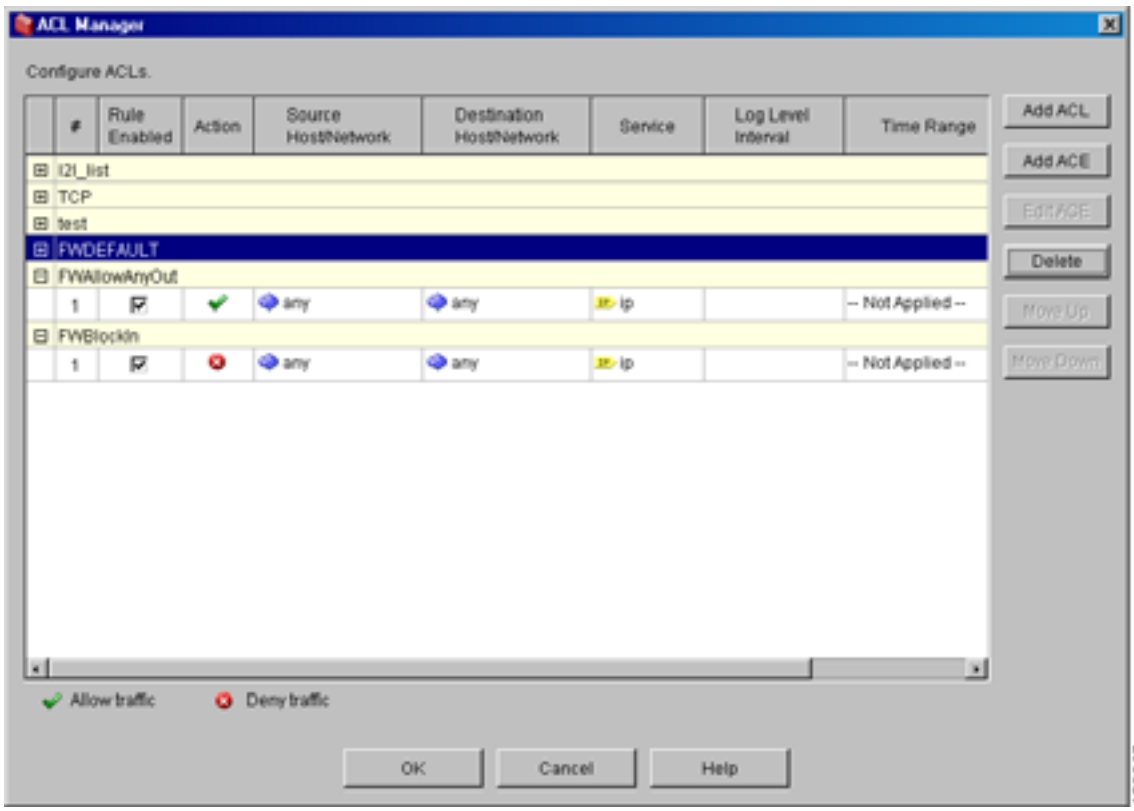
この例では、Policy Pushed (CPP) を指定します。Firewall Policy リストには、次のオプションが含まれています。

- Policy defined by remote firewall (AYT)：このトンネル グループ内のリモート ユーザの PC には、ファイアウォールが配置されています。ローカル ファイアウォールは、VPN クライアントにファイアウォール ポリシーを強制的に適用します。ASA は、指定のファイアウォールが VPN クライアントにインストール済みで動作している場合のみ、VPN クライアントの接続を許可します。指定のファイアウォールが実行されていない場合、接続は失敗します。接続が確立されると、VPN クライアントは、30 秒ごとにファイアウォールにポーリングすることにより、ファイアウォールが動作中であることを確認します。ファイアウォールの動作が停止すると、VPN クライアントはセッションを終了します。
- Policy Pushed (CPP)：ASA は、次の Policy Pushed（CPP）リストでユーザが選択した ACL で定義されているトラフィック管理規則を、VPN クライアントに強制的に適用します。
  - Inbound Traffic Policy：VPN クライアントへの着信トラフィックを制御するための ACL を選択します。
  - Outbound Traffic Policy：VPN クライアントからの発信トラフィックを制御するための ACL を選択します。

  VPN クライアントにローカル ファイアウォールも配置されている場合、ASA からプッシュされたポリシーは、ローカル ファイアウォールのポリシーと共存します。*いずれかの*ファイアウォールの規則によりブロックされたパケットは、ドロップされます。

ステップ 8　CPP を選択した場合、Inbound Traffic Policy リストおよび Outbound Traffic Policy リストで、ACL をクリックします。ASDM では、両方のリストで同じ ACL を選択することはできません。リストに ACL を追加するには、**Manage** をクリックします。ACL Manager テーブルが表示されます。この例では、2 つの ACL を追加します。1 つは着信トラフィック ポリシーとして、もう 1 つは発信トラフィック ポリシーとして使用します（図 5-7 を参照してください）。

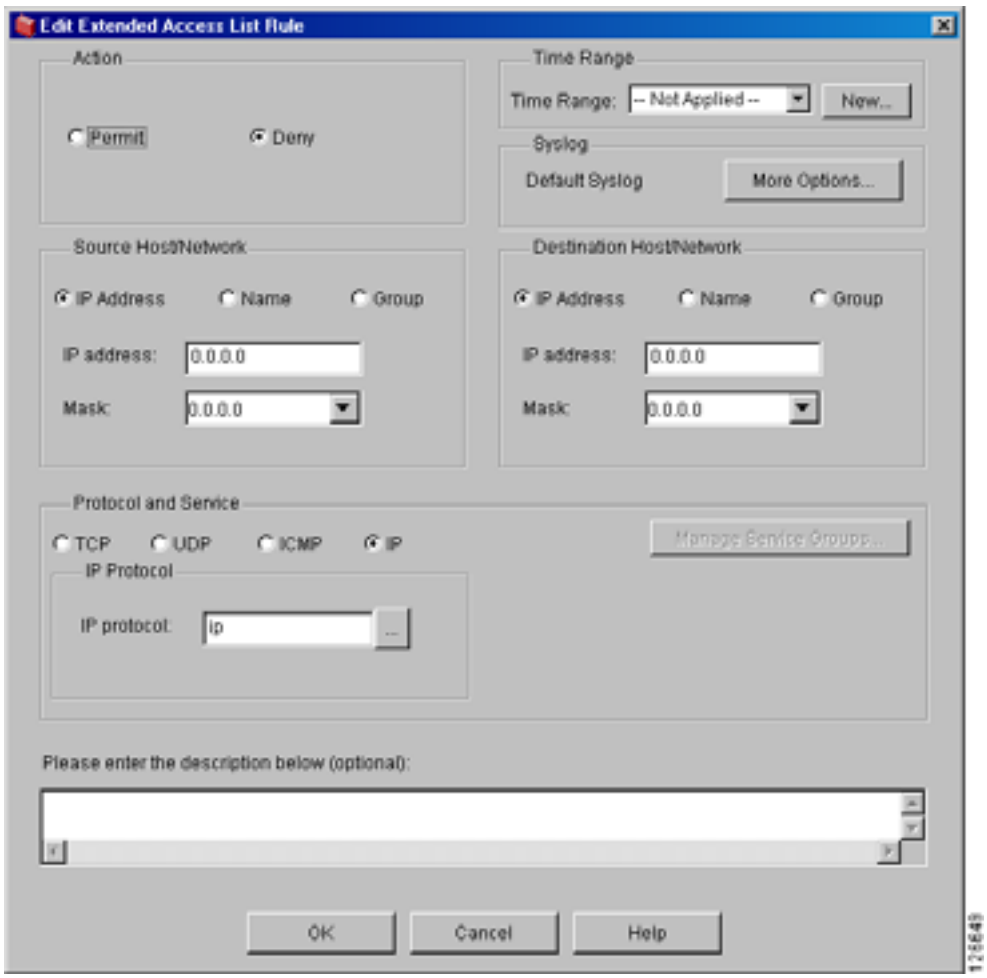
図 5-7　ACL Manager の使用



ステップ 9　ACL を追加するには、**Add ACL** をクリックし、ACL の名前を ACL ID ボックスに入力して **OK** をクリックします。着信 ACL の場合、名前は ID としての FWBlockIn です。

ステップ 10　前のステップで追加した **FWBlockIn** ACL をクリックし、次に **Add ACE** をクリックしてアクセス コントロール エントリを挿入します。Add Extended Access List Rule ダイアログボックスが表示されます。すべてのフィールドの詳細を参照する場合は、**Help** をクリックします（図 5-8 を参照してください）。

図 5-8　アクセス リスト規則の追加



a. CPP ポリシーの場合、非請求ネットワークおよびホストから VPN クライアントまたは VPN クライアントのグループへのすべてのトラフィックを拒否する必要があります。そのように設定するには、**Deny** オプションをクリックします。Source Host/Network および Destination Host/Network で、デフォルトの **0.0.0.0**（任意）を受け入れます。

b. IP をデフォルトのプロトコルとして設定するには、Protocol and Service グループ ボックスで **IP** オプションをクリックします。送信元と宛先の両方で、デフォルトのサービスは any です。これらを変更する場合の詳細については、**Help** をクリックしてください。

c. **OK** をクリックして ACE を追加します。

ステップ 11　同じ手順を実行して、VPN クライアントからのすべての発信トラフィックを許可する 2 つ目の ACL を追加します。

a. ACL ID ボックスに *FWAllowAnyOut* と入力します。

b. **Add ACE** をクリックします。Add/Edit Extended Access List Rule ダイアログボックスが表示されたら、Action では **Permit** をクリックし、Protocol では **IP** をクリックします。

ステップ 12　**OK** をクリックします。ASDM に ACL Manager が表示されるので、ACL が追加されたことを確認します。図 5-7 を参照してください。

ステップ 13　**OK** をもう一度クリックします。ASDM に Client Firewall タブが表示されます。

ステップ 14 Policy Pushed (CPP) オプションで、着信トラフィック ポリシーおよび発信トラフィック ポリシーを設定します。

a. Inbound Traffic Policy リストで **FWBlockIn** をクリックします。

b. Outbound Traffic Policy リストで **FWAllowAnyOut** をクリックします。

c. **OK** をクリックします。ASDM に Group Policy パネルが表示されます。

ステップ 15 **Apply** をクリックしてから、設定を保存します。

HTTP トラフィックを許可するためのクライアント ファイアウォールの設定

HTTP トラフィックの着信を許可し、他の着信トラフィックをすべてブロックするようにクライアント ファイアウォールを設定できます。この例では、発信トラフィック ポリシーとして、前の項で作成した FWAllowAnyOut を使用します。

CLI コマンドを使用した手順

HTTP トラフィックを許可し、他のすべての着信トラフィックを拒否するには、次の **access-list** コマンドをコンフィギュレーション モードで実行します。ACL の名前は FWAllowHTTP、使用するプロトコルは TCP、HTTP トラフィックのポート番号は 80 です。

ステップ 1 ACL を設定します。最初の 2 つのコマンドは着信トラフィック ポリシーを定義し、3 つ目のコマンドは発信トラフィック ポリシーを定義します。

```
hostname(config)# access-list FWAllowHTTP permit tcp any any eq 80
hostname(config)# access-list FWAllowHTTP deny ip any any
hostname(config)# access-list FWAllowAnyOut permit ip any any
```

ステップ 2 group-policy モードで client-firewall コマンドを入力します。この例では、グループ ポリシーの名前は ClientServer です。

```
hostname(config)# group-policy ClientServer internal
hostname(config)# group-policy ClientServer attributes
hostname(config-group-policy)# client-firewall req cisco-integrated acl-in FWAllowHTTP
acl-out FWAllowAnyOut
```

ASDM を使用した手順

ASDM を使用して Cisco Integrated Client Firewall および CPP を設定する手順は、次のとおりです。

（注） 詳細については、「グループ ポリシーでのクライアント ファイアウォールの設定」を参照してください。

ステップ 1　Configuration > VPN > General > Group Policy で、グループ ポリシーを追加または編集します。この例では、新しいポリシーを追加します。

ステップ 2　**Add** をクリックし、**Internal Group Policy** を選択します。

ステップ 3　新しいポリシーの名前を Name フィールドに入力します。この例では、ClientServer という名前のポリシーを追加します。

ステップ 4　**Client Firewall** タブをクリックします。

ステップ 5　**Inherit** オプションをクリックして、オフにします。

ステップ 6　Firewall Setting リストで、**Firewall Required** オプションをクリックします。

ステップ 7　Firewall Type として **Cisco Integrated Client Firewall** を保持します。

この設定では、Firewall Policy グループ ボックスの Policy Pushed (CPP) オプションが自動的にイネーブルになります。

ステップ 8　**Manage** をクリックします。

ステップ 9　**Add ACL** をクリックし、ACL ID ボックスに *FWAllowHTTP* という名前を入力して **OK** をクリックします。

ステップ 10　テーブル内の **FWAllowHTTP** をクリックし、**Add ACE** をクリックします。次のオプションを設定します。

a. Action で、デフォルトのオプション（**Permit**）を使用します。
b. デフォルトの Protocol and Service 設定（**TCP**）を使用します。このオプションを指定すると、その下の Service パラメータがイネーブルになります。
c. 左側でデフォルトの Service 演算子（=）を使用し、**...** をクリックします。表示されるリストで **www/http** をクリックし、**OK** をクリックします。
d. Destination Port の側で、デフォルト設定である **Service = any** を保持します。
e. **OK** をクリックします。

ステップ 11　**OK** をクリックします。

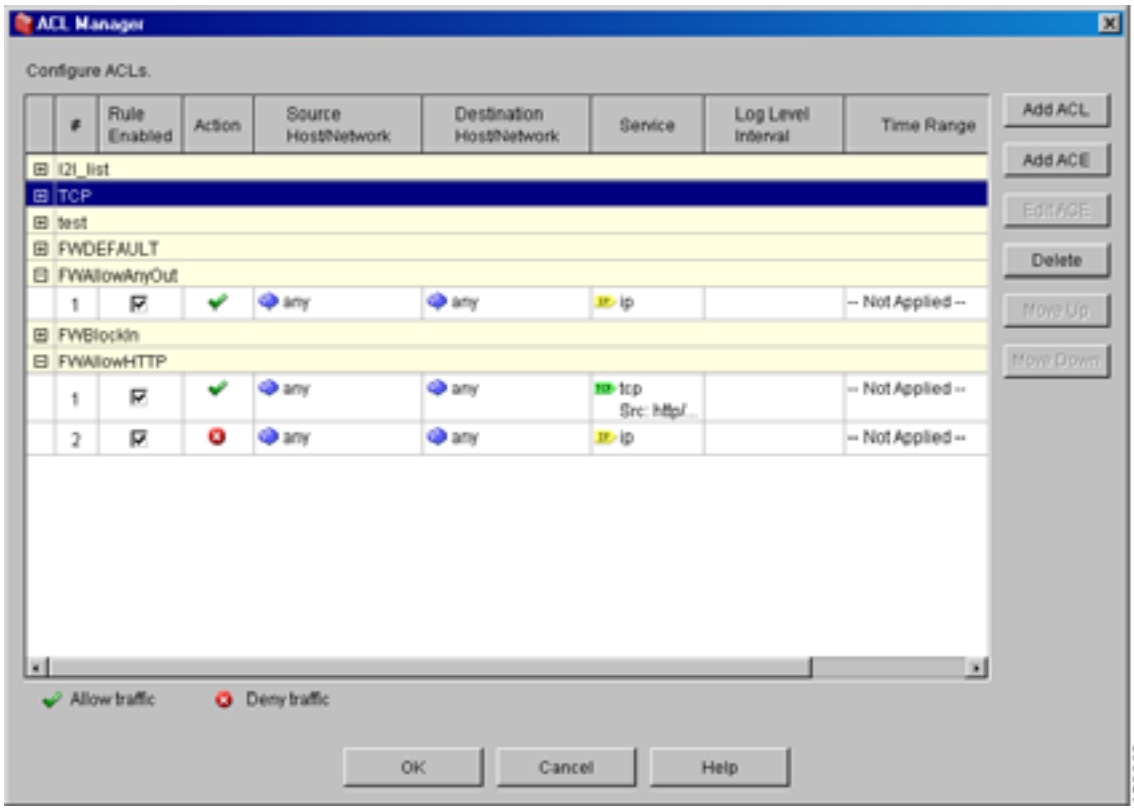
ステップ 12　Client Firewall タブの Firewall Policy および Policy Pushed (CPP) で、Inbound Traffic Policy リストに対して **FWAllowHTTP** をクリックし、Outbound Traffic Policy リストに対して **FWAllowAnyOut** をクリックします。次に **Manage** をクリックします。

ステップ 13　ACL Manager テーブル内の FWAllowHTTP ACL で **Add ACE** をクリックし、2 つ目の規則を追加します。

ここでは、すべてのトラフィックを拒否するように、別の規則を FWAllowHTTP に追加します（この規則は、HTTP トラフィックを許可する規則の後に追加されます）。

ステップ 14 Action で **Deny** を、Protocol and Service で **IP** をクリックし、次に **OK** をクリックします。図 5-9 は、この例での ACL Manager テーブルの最終的なコンフィギュレーションを示しています。FWAllowHTTP ACL に対し、2 つの規則が正しい順序で設定されていることに注意してください。HTTP から VPN クライアントへの着信トラフィックは通過できますが、その他のトラフィックはすべて拒否されます。

図 5-9　VPN クライアントを Web サーバとして使用するためのクライアント ファイアウォール ACL



ステップ 15 ACL Manager で **OK** をクリックします。

ステップ 16 Client Firewall タブで **OK** をもう一度クリックし、次に **Apply** をクリックします。

外部サーバを使用する認証

この例は、リモート アクセス ユーザの外部認証を設定する方法、具体的には RADIUS サーバを設定する方法を示しています。

コンフィギュレーション手順の概要

外部認証を設定するには、次の手順を実行します。

1. 認証用の AAA サーバ グループを作成します。
2. AAA サーバ グループにホストを追加します。
3. 外部認証用のリモート アクセス トンネル グループを追加または編集します。

この例では、次のシナリオを使用します。

- AAA サーバ グループの名前は ACSRadiusServer。
- AAA ホストの IP アドレスは、172.16.0.1、172.16.0.2、および 172.16.0.3。
- リモート アクセス トンネル グループの名前は、ACSRadiusGroup。

IP アドレス プールの作成

最初のステップは、コール インする VPN クライアント用の IP アドレス プールの作成です。別の方法として、DHCP サーバを使用して、IP アドレスをクライアントに配布することもできます。この例では、アドレス プールを使用します。

CLI コマンドを使用した手順

IP アドレス プールを作成するには、**ip local pool** コマンドを使用します。コマンドのシンタックスは、次のとおりです。

ip local pool *poolname first-address—last-address* [***mask*** *mask*]

たとえば、次のコマンドを入力して、名前が IPPool2 で、アドレス範囲が 10.20.30.40 から 10.20.30.60 の IP アドレス プールを作成します。

```
hostname(config)# ip local pool IPPool2 10.20.30.40-10.20.30.60
hostname(config)#
```

ASDM を使用した手順

IP アドレス プールを作成するには、次の手順を実行します。

ステップ 1　Configuration > VPN > IP Address Management > IP Pools で、**Add** をクリックします。ASDM に、Add IP Pool ダイアログボックスが表示されます（図 5-10 を参照してください）。

図 5-10　IP アドレス プールの追加

ステップ 2　**Name** フィールドに IP プールの名前を入力します。この例では、名前は IPpool2 です。

ステップ 3　**Starting IP Address** フィールドに開始 IP アドレスを入力します。この例では、開始 IP アドレスは 10.20.30.40 です。

ステップ 4　**Ending IP Address** フィールドに終了 IP アドレスを入力します。この例では、終了 IP アドレスは 10.20.30.60 です。

ステップ 5　**Subnet Mask** リストで、サブネット マスクをクリックします。ASDM では、サブネット マスクの設定は必須です。

ステップ 6　**OK** をクリックしてから、**Apply** をクリックします。

サーバ グループの追加

認証用に外部サーバ グループを追加します。この例では、次の機能を使用して、RADIUS 認証用に ACSRadiusServers という名前のサーバ グループを追加します。

- RADIUS プロトコル
- single アカウンティング モード
- timed リアクティベーション モード

  このオプションでは、サーバは、ダウン時間が 30 秒経過すると再度有効にされます。デフォルトの設定は、depletion です。この設定では、障害が発生したサーバは、グループ内のすべてのサーバが非アクティブになった後でのみ再度有効にされます。
- サーバが無効になるまでに許容されている試行失敗の回数は 2

  デフォルト値は 3 です。

CLI コマンドを使用した手順

サーバ グループを設定するには、**aaa-server protocol** コマンドを使用します。このサーバ グループを RADIUS サーバ グループとして設定する **aaa-server protocol** コマンドのシンタックスは、次のとおりです。

aaa-server *server-tag* **protocol** *server-protocol*

aaa-server コマンドを入力すると、CLI は、AAA サーバ グループ アトリビュートを設定するための config-aaa-server-group モードに切り替わります。

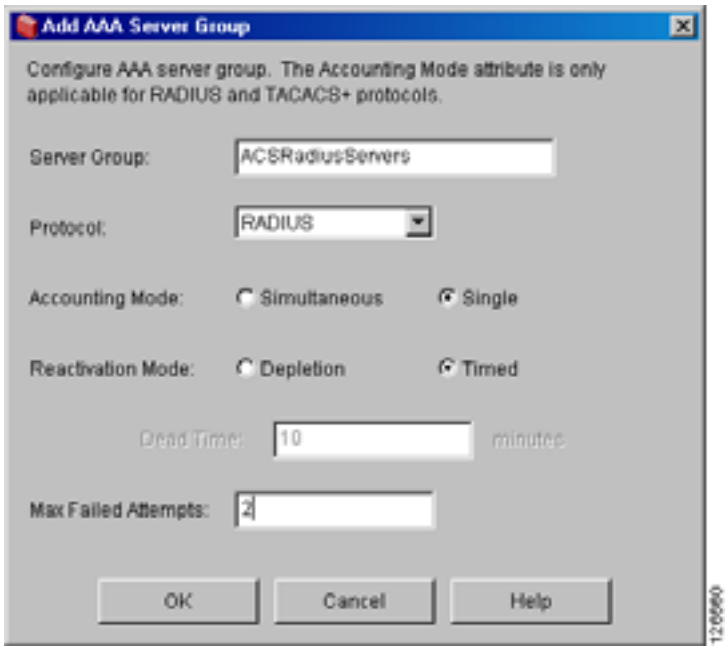
次のコマンドは、RADIUS プロトコルを使用する RadiusServer という名前の AAA サーバ グループを設定します。

```
hostname(config)# aaa-server ACSRadiusServers protocol radius
hostname(config-aaa-server-group)# accounting-mode single
hostname(config-aaa-server-group)# reactivation-mode timed
hostname(config-aaa-server-group)# max-failed-attempts 2
```

ASDM を使用した手順

ステップ 1　認証用のサーバ グループを設定するには、Configuration > Properties > AAA Setup > AAA Servers パネルの Server Groups 領域で **Add** をクリックします。ASDM に、Add AAA Server Group ダイアログボックスが表示されます（図 5-11 を参照してください）。

図 5-11　AAA サーバ グループの追加



ステップ 2　追加するサーバ グループの情報を入力します。

a. Server Group：このサーバ グループの名前を入力します。この例では、名前は ACSRadiusServers です。

Protocol：Protocol リストで、このサーバ グループで使用するプロトコルをクリックします。次のプロトコルから選択できます。この例では、プロトコルは RADIUS です。

- RADIUS
- TACACS+
- NT Domain
- SDI
- Kerberos
- LDAP
- HTTP Form

b. Accounting Mode：RADIUS または TACACS+ の場合、アカウンティング モード オプションとして **Simultaneous** または **Single**（デフォルト）をクリックします。simultaneous モードの ASA では、アカウンティング データがグループ内のすべてのサーバに送信されます。single モードの ASA では、アカウンティング データが 1 つのサーバにだけ送信されます。この例では、デフォルトの Single を受け入れます。

c. Reactivation Mode：障害が発生したサーバを再度有効にする方法として Depletion または Timed を選択します。depletion モードでは、障害が発生したサーバは、グループ内のすべてのサーバが非アクティブになった後でのみ再度有効にされます。timed モードでは、障害が発生したサーバは、ダウン時間が 30 秒経過すると再度有効にされます。これらのオプションのいずれかをクリックします。デフォルトは Depletion です。この例では、timed リアクティベーション モードを使用します。

d. Dead Time：リアクティベーション モードが Depletion の場合、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イネーブルにするまでの経過時間を、分単位で設定する必要があります。デフォルトは 10 です。

e. Max Failed Attempts：応答がないサーバをデッドと宣言するまでに許可されている接続試行失敗の回数。許可する試行回数を入力します。デフォルトは 3 です。この例では、値を 2 に設定します。

ステップ 3　**OK** をクリックしてから、**Apply** をクリックします。

AAA サーバ グループへの AAA ホストの追加

AAA サーバ グループを設定した後は、サーバ グループに追加している各ホストの IP アドレスを識別し、ホストが使用しているインターフェイスを識別することにより（オプション）、サーバ グループに AAA ホスト（この場合は RADIUS サーバ）を追加できます。

CLI コマンドを使用した手順

CLI のこの例では、内部インターフェイス上のサーバ グループ ACSRadiusServers に 3 個のホストを追加します。これらのコマンドは、ホスト IP アドレスを定義し、aaa-server-group モードで設定できるパラメータを示します。

aaa-server host コマンドのシンタックスは、次のとおりです。

aaa-server *server-tag* [(*interface-name*)] **host** *server-ip*

AAA サーバ ホストを追加するために使用する **aaa-server host** コマンドの例では、次のアトリビュートを参照します。

- **retry-interval**：接続を試行するまでに待機する秒数。デフォルト値は 10 です。
- **timeout**：ASA がプライマリ AAA サーバへの要求を断念し、バックアップ サーバ（存在する場合）にその要求を送信するまでの時間（分単位）。デフォルト値は 10 です。
- **key**：暗号鍵。大文字と小文字が区別されます。

```
hostname(config)# aaa-server ACSRadiusServers (inside) host 172.16.0.1
hostname(config-aaa-server-group)# retry-interval 5
hostname(config-aaa-server-group)# timeout 16
hostname(config-aaa-server-group)# key x5*zbrct
hostname(config-aaa-server-group)#
hostname(config)# aaa-server ACSRadiusServers (inside) host 172.16.0.2
hostname(config-aaa-server-group)# retry-interval 5
hostname(config-aaa-server-group)# timeout 16
hostname(config-aaa-server-group)# key x5*zbrct
hostname(config-aaa-server-group)#
hostname(config)# aaa-server ACSRadiusServers (inside) host 172.16.0.3
hostname(config-aaa-server-group)# retry-interval 5
hostname(config-aaa-server-group)# timeout 16
hostname(config-aaa-server-group)# key x5*zbrct
hostname(config-aaa-server-group)#
```

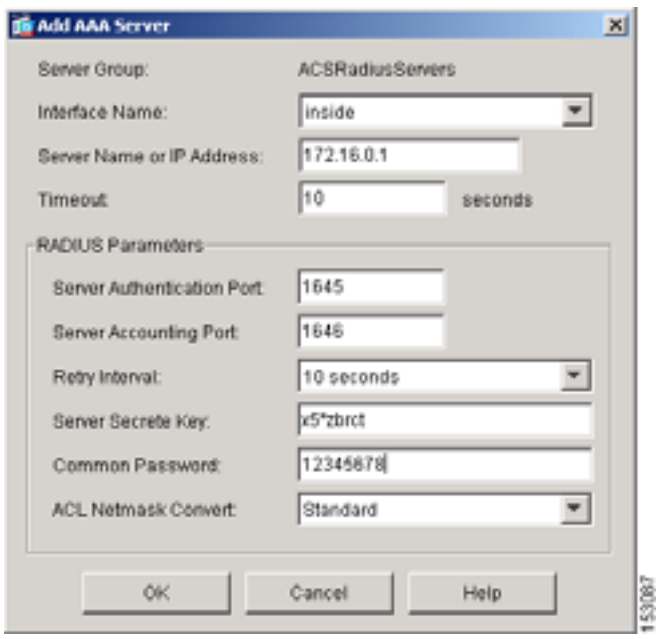
ASDM を使用した手順

ASDM を使用して、認証に RADIUS を使用する AAA サーバ グループに AAA サーバを追加する手順は、次のとおりです。

ステップ 1　Configuration > Properties > AAA Setup > AAA Servers パネルで、AAA サーバの追加先のサーバ グループをクリックします。この例では、**ACSRadiusServers** をクリックします。

ステップ 2　Servers の Selected Group 領域で **Add** をクリックします。ASDM に、Add AAA Server ダイアログボックスが表示されます。図 5-12 は、この例の値を設定するダイアログボックスを示しています。

図 5-12　外部認証用の AAA の追加



ステップ 3　グループ内の最初のホストについて、次の情報を入力します。

a. Interface Name：認証サーバに関連付けられたネットワーク インターフェイスの名前を、Interface Name リストから選択します。この例では、**inside** を選択します。

b. Server IP Address：AAA サーバの IP アドレスを入力します。この例では、追加する最初のホストの IP アドレスは 172.16.0.1 です。

c. Timeout：ASA がプライマリ AAA サーバへの要求を断念し、バックアップ サーバ（存在する場合）にその要求を送信するまでの時間を分単位で入力します。この例では、デフォルト設定の 10 秒を使用します。

d. RADIUS Parameters グループ：このグループ ボックスで各パラメータを設定します。この例では、配置場所のデフォルトを受け入れます。サーバの秘密鍵と共通のパスワードを入力する必要があります。

(注)　共通パスワードを使用するのは、RADIUS サーバだけです。

e. Server Authentication Port：ユーザ認証用のサーバ ポート。デフォルト ポートは、1645 です。

f. Server Accounting Port：ユーザ アカウンティング用のサーバ ポート。デフォルト ポートは、1646 です。

g. Retry Interval：接続を試行するまでに待機する秒数を選択します。デフォルト設定は、10 秒です。この例では、デフォルト設定を使用します。

h. Server Secret Key：暗号鍵を入力します。大文字と小文字が区別されます。この例では、鍵は *x5*zbrct* です。

i. Common Password：RADIUS の共通パスワードを入力します。この例では、パスワードは *12345678* です。

j. ACL Netmask Convert：Detect Automatically、Standard、または Wildcard を選択します。この例では、**Standard** を選択します。

ステップ 4　設定を指定した後、**OK** および **Apply** をクリックします。

同じ手順を実行して、残りの 2 つのホストを AAA サーバ グループに追加します。

外部認証を使用するリモート アクセス用のトンネル グループの追加

最後に、トンネル グループを追加します。この例では、トンネル グループの名前は ACSRadiusGroup です。AAA サーバ グループの名前は、ACSRadiusServers です。

CLI コマンドを使用した手順

次のコマンドは、トンネル グループの名前を指定し、トンネル グループの一般アトリビュート モードにアクセスし、トンネル グループを認証グループに割り当てます。最後の 2 つのコマンドは、IPSec アトリビュート モードに移行し、リモート アクセス認証用の事前共有鍵を設定します。

```
hostname(config)# tunnel-group ACSRadiusGroup type ipsec_ra
hostname(config)# tunnel-group ACSRadiusGroup general-attributes
hostname(config-general)# address-pool IPPool2
hostname(config-general)# authentication-server-group ACSRadiusServers
hostname(config)# tunnel-group ACSRadiusGroup ipsec-attributes
hostname(config-ipsec)# pre-shared k*5$h9s%
```

ASDM を使用した手順

ASDM を使用して、外部認証を使用するリモート アクセス用のトンネル グループを追加する手順は、次のとおりです。

ステップ 1　Configuration > VPN > General > Tunnel Group パネルで **Add** をクリックし、**IPSec for Remote Access** を選択します。ASDM に Add Tunnel Group ダイアログボックスが表示され、General タブと Basic タブが示されます。

ステップ 2　Name フィールドにこのトンネル グループの名前を入力します。この例では、名前は ACSRadiusGroup です。

ステップ 3　General タブで **AAA** タブをクリックします。

ステップ 4　Authentication Server Group リストからサーバ グループを選択します。この例では、サーバ グループの名前は ACSRadiusServers です（「サーバ グループの追加」を参照してください）。

ステップ 5　このリモート アクセス トンネル グループの IPSec アトリビュートを設定するには、**IPSec** タブをクリックし、Pre-shared Key フィールドに暗号鍵を入力します。この例では、事前共有鍵は *k*5$h9s%* です。次に **OK** および **Apply** をクリックします。

CHAPTER 6

トラフィック管理の設定

この章では、次の設定タスクについて説明します。

- ロード バランシングの設定
- VPN トラフィック用の Quality of Service の設定

ロード バランシングの設定

リモート クライアント コンフィギュレーションで、同じネットワーク上に接続された 2 つ以上の ASA を使用してリモート セッションを処理している場合、セッション ロードを共有するようにこれらのデバイスを設定できます。この機能は、*ロード バランシング*と呼ばれます。ロード バランシングを使用すると、ロード量が最小のデバイスにセッション トラフィックが誘導されるため、ロードはすべてのデバイスに分散されます。このロード バランシングにより、システム リソースを効率的に使用し、高いアベイラビリティを実現できます。

ロード バランシングを実装するには、同じサブネット上の 2 つ以上のデバイスを論理的にグループ化して*仮想クラスタ*を形成します。

仮想クラスタ内のすべてのデバイスに、セッション ロードが課せられます。仮想クラスタ内の 1 つの ASA である*仮想クラスタ マスター*は、接続を受け入れ、*バックアップ デバイス*と呼ばれる他のデバイスに着信コールを誘導することができます。仮想クラスタ マスターは、クラスタ内のすべてのデバイスを監視し、各デバイスの通信量を追跡し、それに応じてセッション ロードを分散させます。仮想クラスタ マスターは、1 つの物理デバイスに関連付けられているものではなく、デバイス間を移動してその役割を果たします。たとえば、現在の仮想クラスタ マスターに障害が発生すると、クラスタ内のバックアップ デバイスの 1 つがその役割を引き継ぎ、ただちに新しい仮想クラスタ マスターになります。

外部のクライアントには、仮想クラスタは単一の*仮想クラスタ IP アドレス*として見えます。この IP アドレスは特定の物理デバイスに関連付けられていません。現在の仮想クラスタ マスターに属しています。そのため「仮想」です。接続の確立を試行している VPN クライアントは、最初にこの仮想クラスタ IP アドレスに接続します。次に仮想クラスタ マスターは、クラスタ内で使用可能で、ロード量が最小のパブリック IP アドレスを、クライアントに返送します。2 回目のトランザクション（ユーザには透過）では、クライアントはそのデバイスに直接接続します。このような方法で、仮想クラスタ マスターは、リソース間で均等かつ効率的にトラフィックを誘導します。

クラスタ内のあるデバイスに障害が発生した場合、終了されたセッションは、ただちに仮想クラスタ IP アドレスに再接続できます。次に、仮想クラスタ マスターは、それらの接続をクラスタ内のアクティブ デバイスに誘導します。仮想クラスタ マスター自体に障害が発生した場合、クラスタ内のバックアップ デバイスの 1 つが、ただちに、また自動的に、新しい仮想セッション マスターとして役割を引き継ぎます。クラスタ内の複数のデバイスに障害が発生しても、クラスタ内のいずれか 1 つのデバイスがアップ状態で使用可能であれば、ユーザはクラスタへの接続を継続できます。

（注） WebVPN でロード バランシングが正しく機能するには、クラスタ内のすべてのデバイスが WebVPN をサポートしている必要があります。

前提条件

ロード バランシングは、デフォルトではディセーブルです。明示的に設定してイネーブルにする必要があります。

ロード バランシングを設定できるようにするには、まずパブリック インターフェイスおよびプライベート インターフェイスを設定し、仮想クラスタ IP アドレス用のインターフェイスを定義する必要があります。

クラスタ内のすべてのデバイスは、次の値について、クラスタ固有の同じ値を共有する必要があります。

- 仮想クラスタの IP アドレス
- 暗号化設定（オプション）
- 暗号鍵（暗号化がイネーブルでない場合はオプション）
- ポート ID（デフォルト UDP は 9023）

コンフィギュレーション手順の概要

最小の VPN ロード バランシング スキームを設定するには、次の手順を実行します。

1. 仮想クラスタ IP アドレスを定義します。この IP アドレスは、VPN ロード バランシング クラスタ内のすべてのデバイスで共有されます。アドレスは、デバイスで共有されるパブリック サブネット アドレスの範囲内にする必要があります。
2. ステートフル フェールオーバーを設定する場合、暗号化をイネーブルにし、クラスタ内のすべてのデバイスで共有する暗号鍵を定義します。仮想クラスタ内のデバイスは、IPSec を使用して LAN 間トンネル経由で通信します。暗号化をイネーブルにすると、デバイス間で通信されるすべてのロード バランシング情報の暗号化が保証されます。
3. オプションで、クラスタ内のデバイスのデフォルトの優先順位を変更します。範囲は 1 ～ 10 で、10 が最上位です。優先順位は、起動時または既存のマスターに障害が発生したときに、当該デバイスが仮想クラスタ マスターになる可能性を示すものです。設定する優先順位が高いほど、そのデバイスが仮想クラスタ マスターになる可能性は高くなります。
4. クラスタに含まれる各 ASA で、ロード バランシングをイネーブルにします。

この項の例では、次の値を設定します。

- クラスタ IP アドレスは 209.165.202.224。
- クラスタ暗号鍵は、12345678。
- このクラスタでは暗号化がイネーブル。
- この例の ASA の優先順位は 10。

この項の例では、次の CLI コマンドを使用してロード バランシングを設定します。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# priority 10
hostname(config-load-balancing)# cluster key 12345678
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

CLI コマンドを使用した手順

show running-config vpn load-balancing コマンドを入力すると、特定のグループ ポリシーの実行コンフィギュレーションを表示できます。

CLI を使用してロード バランシングを設定する手順は、次のとおりです。

ステップ 1　**vpn load-balancing** コマンドを実行すると、config-load-balancing モードに移行します。このモードで、クラスタのパラメータを設定します。このモードで **cluster** コマンドを入力して、仮想クラスタ IP アドレスを設定する手順は次のとおりです。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# cluster ip address 209.165.202.224
```

ステップ 2　このコンフィギュレーションで暗号化を使用するには、**cluster** コマンドを使用し、暗号鍵を定義してから暗号化をイネーブルにします。このステップはオプションです。暗号化をイネーブルにする前に、暗号鍵を設定する必要があります。

```
hostname(config-load-balancing)# cluster key 12345678
hostname(config-load-balancing)# cluster encryption
```

ステップ 3　（オプション）ASA のデフォルトの優先順位を変更するには、**priority** コマンドを次のように使用します。

```
hostname(config-load-balancing)# priority 10
```

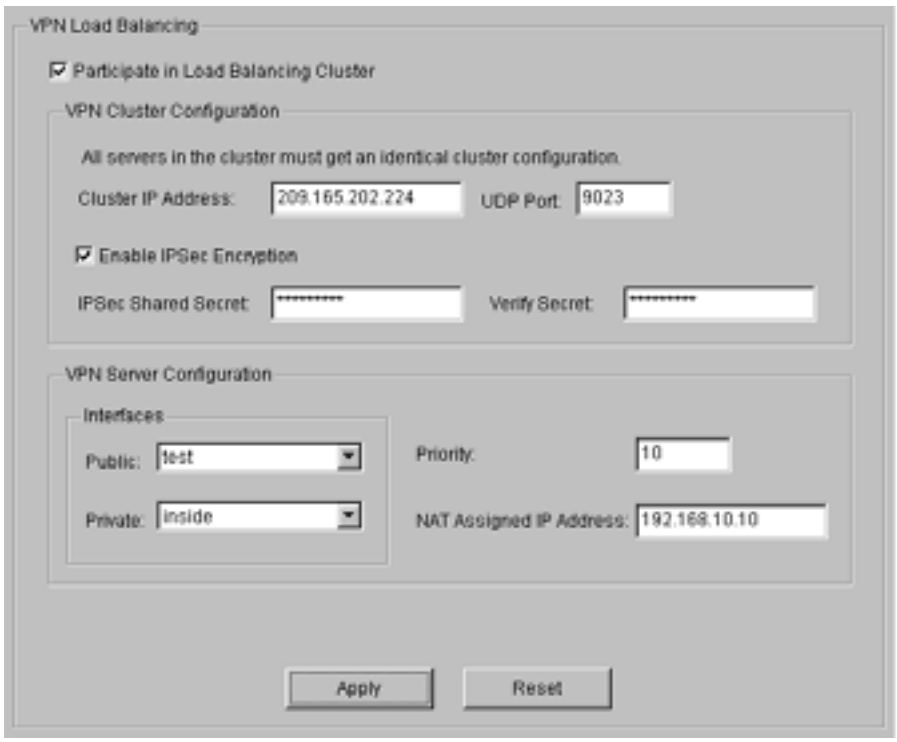
ステップ 4　この ASA でロード バランシングをイネーブルにするには、**participate** コマンドを次のように使用します。

```
hostname(config-load-balancing)# participate
```

ASDM を使用した手順

次の手順は、ASDM を使用してロード バランシングを設定する方法を示しています。この例のパラメータの多くにはデフォルト値があるので、注意してください。

図 6-1　ASDM でのロード バランシングの設定



ステップ 1　VPN ロード バランシングをイネーブルにするには、**Configuration > Features > VPN > Load Balancing** に移動して、**Participate in Load Balancing Cluster** をクリックします。

ステップ 2　**VPN Cluster Configuration** グループ ボックスで、クラスタに参加するすべての ASA 用のパラメータを次のように設定します。

a. **Cluster IP Address** テキスト ボックスにクラスタの IP アドレスを入力します。

b. **Enable IPSec Encryption** オプションをクリックします。

c. **IPSec Shared Secret** テキスト ボックスに暗号鍵を入力し、**Verify Secret** テキスト ボックスにもう一度入力します。

ステップ 3　**VPN Server Configuration** グループ ボックスで次のようにオプションを設定します。

a. **Public** リストで、着信 VPN 接続を受け入れるインターフェイスを選択します。

b. **Private** リストで、プライベート インターフェイスであるインターフェイスを 1 つ選択します。

c. （オプション）**Priority** テキスト ボックスで、ASA でクラスタに対して設定されている優先順位を変更します。

d. このデバイスが、NAT を使用するファイアウォールの背後にある場合は、**NAT Assigned IP Address** に IP アドレスを入力します。この例では、NAT で割り当てられている IP アドレスは 192.168.10.10 です。デバイスが NAT を使用していない場合、または ASA が、NAT を使用するファイアウォールの背後にない場合は、0.0.0.0 と入力します。

VPN トラフィック用の Quality of Service の設定

VPN 3000 コンセントレータには、トラフィック ポリシー管理の一部として帯域幅管理が実装されています。ASA のセキュリティ ポリシー コンフィギュレーションのコンポーネントである Quality of Service（QoS）は、その実装に取って代わるものです。ASA での QoS の実装は、IOS でのその機能の実装に基づいています。

QoS は、ミッション クリティカルなデータと通常のデータの両方にネットワーク リソースを割り振るためのトラフィック管理方針で、この割り振りは、ネットワーク トラフィックのタイプとそのトラフィックに割り当てられた優先順位に基づいて実行されます。簡潔に言うと、QoS は妨害のない優先トラフィックを保証し、レート制限（ポリシング）トラフィック機能を提供します。

QoS は、個々のユーザ トンネルおよびサイトツーサイト トンネルに対して、最大のレート制御またはポリシングを提供します（LAN 間接続では、1 つのトンネル内の個々のユーザ トラフィックは考慮されません）。このリリースでは、最小帯域幅保証（帯域幅予約）は提供されていません。

QoS は大量のリソースを消費し、ASA のパフォーマンスを低下させる可能性があるので、QoS はデフォルトではディセーブルになっています。

次の項では、QoS を使用して、トンネル グループだけの優先トラフィックを設定する方法を簡潔に示します。

（注） QoS の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

コンフィギュレーション手順の概要

ASDM を使用して QoS を設定する手順は、次のとおりです。

1. サービス ポリシーを設定します。

   インターフェイスごとに、またはグローバル レベルで設定できるサービス ポリシーは 1 つだけです。
2. サービス ポリシー規則のトラフィック分類基準を設定します。
3. サービス ポリシー規則で分類されたトラフィックに対するアクションを設定します。

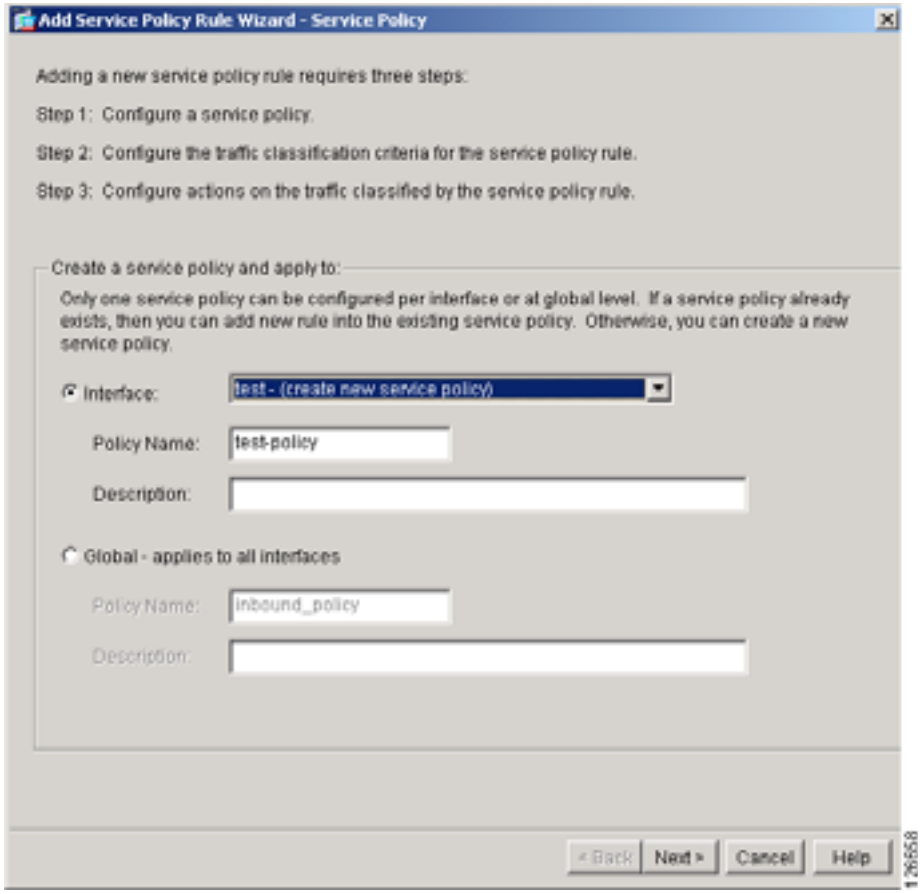
ASDM を使用した手順

ASDM には、QoS の設定手順を紹介するウィザードがあります。この項では、このウィザードを使用してトンネル グループの QoS を設定する方法を示します。ASDM で **Help** ボタンをクリックすると、詳細な情報を参照できます。

ステップ 1　**Configuration > Features > Security policy** パネルで、**Service Policy Rules** をクリックします。

ステップ 2　**Add** をクリックします。ASDM に **Add Service Policy Rule Wizard - Service Policy** 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を使用して、サービス ポリシーを作成または編集します。

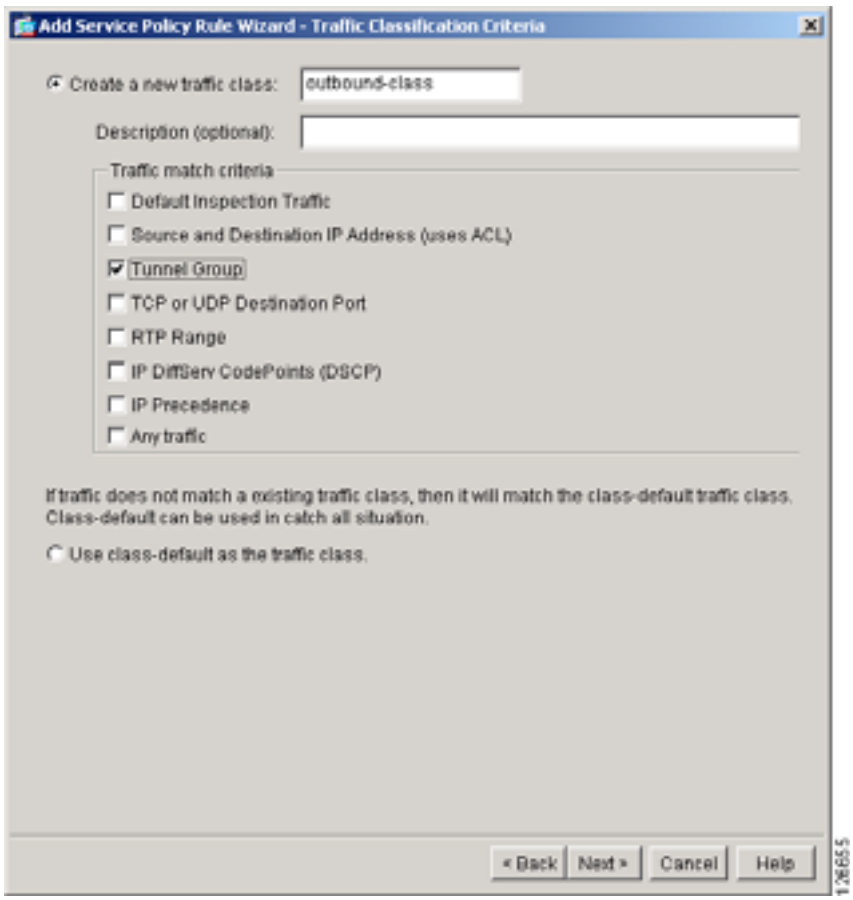
図 6-2　Add Service Policy Rule Wizard - Service Policy ウィザード



ステップ 3　この例では、新しいサービス ポリシーを作成し、そのポリシーをテスト インターフェイスに適用します。開始するには、**Interface** オプションをクリックし、次に **Interface** リストから **test - (create new service policy)** という名前を選択します（インターフェイス名に (create new service policy) というテキストが付加されます）。

ステップ 4　**Policy Name** テキスト ボックスにポリシーの名前を入力します。ASDM では、インターフェイス名に「policy」という言葉を付加したデフォルト名が提供されます。この例では、名前を outbound-policy に変更します。**Next** をクリックします。ASDM に **Add Service Policy Rule Wizard - Traffic Classification Criteria** ダイアログボックスが表示されます。

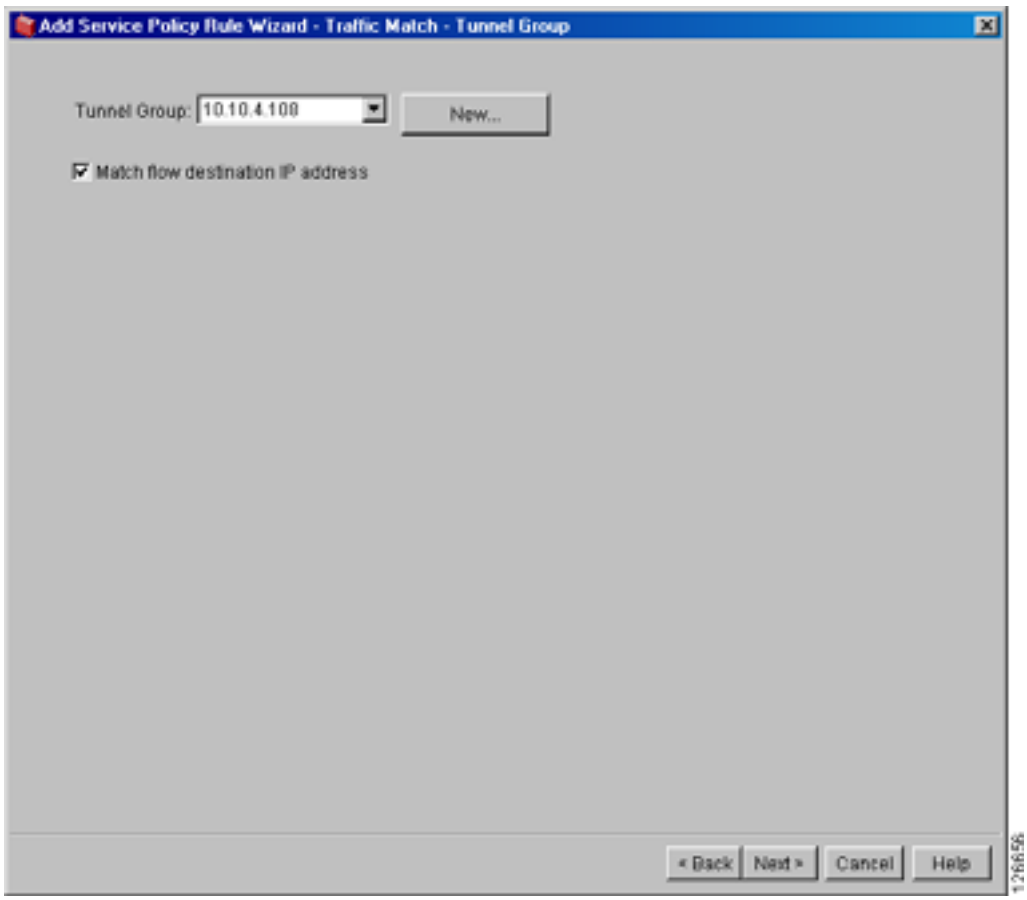
図 6-3　Add Service Policy Rule Wizard - Traffic Classification Criteria



ステップ 5　**Create a new traffic class** オプションをクリックします。ASDM によりインターフェイス名と「class」という言葉が結合されて、テキスト ボックスにデフォルトのポリシー名が作成されます。この例では、名前を outbound-class に変更します。

ステップ 6　**Traffic match criteria** グループ ボックスには、ASA で提供されている一致基準のサブセットが表示されます。この例では、**Tunnel Group** オプションをクリックして、**Next** をクリックします。ASDM に **Add Service Policy Rule Wizard-Traffic Match - Tunnel Group** ダイアログボックスが表示されます。

図 6-4　Add Service Policy Rule Wizard-Traffic Match - Tunnel Group

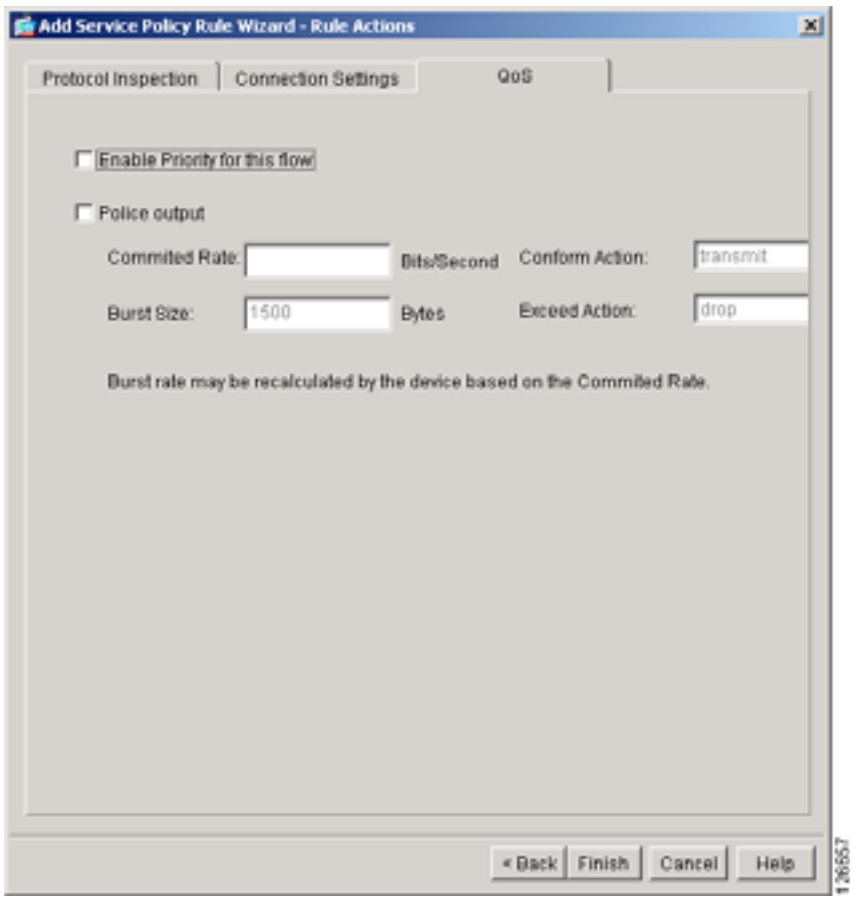


ステップ 7　システムにすでに存在するトンネル グループの IP アドレスを選択するか、**New** をクリックして新しいトンネル グループを設定します。この例では、**Tunnel Group** リストから **10.10.4.108** を選択し、**Match flow destination IP address** をクリックします。このオプションをイネーブルにすると、次のダイアログボックスで選択するトラフィック アクションが、このトンネル グループに適用されます。**Next** をクリックします。

ASDM に **Add Service Policy Rule Wizard - Rule Actions** ダイアログボックスが表示されます。

ステップ 8　**QoS** タブをクリックします。

図 6-5　QoS オプションの設定



QoS タブでは、次の規則アクションの 1 つを選択できます。

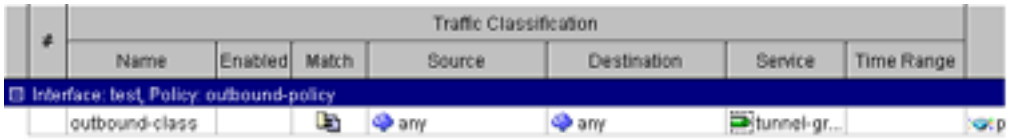
- **Enable Priority for this flow**：このトンネル グループへのトラフィックを優先トラフィックに設定します。
- **Police output**：このトンネル グループに向かうトラフィックをポリシングするための基準を確立します。このオプションをイネーブルにする場合は、認定レート、バースト レート、準拠アクション、および超過アクションの値を変更するか、デフォルト値を受け入れます。これらのパラメータの定義を参照する場合は、**Help** をクリックしてください。

ステップ 9　このトンネル グループのプライオリティ キューイングを確立するには、**Enable Priority for this flow** および **Finish** をクリックします。

ステップ 10　**Apply** をクリックします。

図 6-6 は、この例で設定された QoS セキュリティ ポリシーを示しています。

図 6-6　設定された QoS ポリシー



CLI コマンドを使用した手順

show running-config all service-policy コマンドを入力すると、特定のグループ ポリシーの実行サービス ポリシー コンフィギュレーションを表示できます。

次のコマンド例は、CLI を使用してトンネル グループの優先トラフィックを設定する方法を示しています（コマンド シーケンスが前の項で説明したウィザードと異なるので、注意してください）。

```
class-map outbound-class
  match tunnel-group 10.10.4.108
  match flow-ip destination-address
policy-map outbound policy
  class outbound-class
    priority
service-policy outbound-policy interface test
```

（注） CLI を使用して QoS を設定する方法の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

VPN 3000 シリーズ コンセントレータと ASDM の項目の比較

次の表は、VPN 3000 コンセントレータのタスクを Adaptive Security Device Manager のパスにマッピングしたものを示しています。

- 表 A-1「設定タスクのナビゲーション マップ」
- 表 A-2「管理タスクのナビゲーション マップ」
- 表 A-3「監視タスク」

表 A-1　設定タスクのナビゲーション マップ

VPN 3000 タスク	項目	ASDM パス
VPN 3000 管理アプリケーションの使用	該当なし	ASDM Online Help > About Cisco ASDM
インターフェイスの設定	該当なし	Configuration > Interfaces > Add
	電源	Enable Interface/Dedicate to management only
	イーサネット	Hardware Port
	一般パラメータ	VLAN ID/Sub-interface ID
サーバの設定	AAA サーバ	Configuration > Properties > AAA Setup > AAA Servers Groups
	認証、認可、アカウンティング	Configuration > Security Policy > AAA Rules
	DHCP	Configuration > Properties > DHCP Services > DHCP Server and DHCP Relay
	DNS	Configuration > Properties > DNS Client and Dynamic DNS
	NTP	Configuration > Properties > Device Administration > NTP
	外部サーバ（TACACS および RADIUS）	Configuration > Properties > AAA Setup > AAA Server Groups > Add AAA Server Group（Protocol リスト ボックス）
アドレス管理の設定	該当なし	Configuration > VPN > IP Address Management
	割り当て	Assignment
	プール	IP Pools

表 A-1　設定タスクのナビゲーション マップ（続き）

VPN 3000 タスク	項目	ASDM パス
トンネリングおよび IPSec の設定	PPTP	該当なし
	IPSec サイトツーサイト	Configuration > VPN > IPSec and Configuration > VPN > General > Tunnel Group、Group Policy
	IKE 提案事項	Configuration > VPN > IKE > Policies
	NAT 透過性	Configuration > VPN > IKE > Global Parameters（NAT Transparency グループ ボックス） Configuration > VPN > IPsec > IPSec Rules > Tunnel Policy (Crypto Map) - Advanced タブ > Enable NAT-T チェックボックス
	アラート	Configuration > VPN > IKE > Global Parameters
IP ルーティングの設定	該当なし	Configuration > Routing
	スタティック ルート	Configuration > Routing > Static Route
	デフォルト ゲートウェイ（「トンネル デフォルト ゲートウェイ」）	Configuration > Routing > Static Route
	OSPF	Configuration > Routing > Dynamic Routing > OSPF
	DHCP	Configuration > Properties > DHCP Services
	冗長性	Configuration > Properties > High Availability、Failover
	RIP	Configuration > Routing > Dynamic Routing > RIP
	RRI	Configuration > VPN > IPsec > IPSec Rules > Tunnel Policy (Crypto Map) - Advanced タブ > Enable Reverse Route Injection チェックボックス
管理プロトコルの設定	該当なし	該当なし
	FTP	Tools > File Management > File Transfer
	HTTP/HTTPS	Configuration > Properties > HTTP/HTTPS
	TFTP	Configuration > Properties > Device Administration > TFTP Server
	Telnet	Configuration > Properties > Device Access > Telnet
	SNMP	Configuration > Properties > Device Administration > SNMP
	SSL	Configuration > Properties > SSL
	SSH	Configuration > Properties > Device Access > Secure Shell
	XML	該当なし

表 A-1　設定タスクのナビゲーション マップ（続き）

VPN 3000 タスク	項目	ASDM パス
イベント レポートの設定	イベント クラス リスト イベント セキュリティ レベル リスト イベント ログ	Configuration > Properties > Logging Event Lists Syslog Setup
	イベントの一般またはデフォルトの処理 自動バックアップ用の FTP 情報 特殊処理用のクラス SNMP 管理のトラップ先 Syslog サーバ	Configuration > Properties > Logging > Logging Setup、Syslog Servers、Syslog Setup
	電子メール受信者用の SMTP サーバ	Configuration > Logging > E-Mail Setup
システム情報およびパラメータの設定	該当なし	Configuration > Properties > Device Administration
	識別情報	Configuration > Properties > Device Administration > Device
	日時	Configuration > Properties > Device Administration > Clock
	セッション • アクティブな IPSec 接続の最大数 • 圧縮	Configuration > VPN > General > VPN System Options
	• ヘアピニング（同じインターフェイスに接続された 2 つ以上のホスト間のトラフィックを許可）	Configuration > Interfaces
	認証（グローバル パラメータ）	Configuration > Properties > Device Access > AAA Access
クライアント アップデートの設定	該当なし	Configuration > VPN > General > Client Update
ロード バランシングの設定	該当なし	Configuration > VPN > Load Balancing
ユーザ管理の設定	ユーザ	Configuration > Properties > Device Administration > User Accounts
	基本グループ	該当なし
	グループ	Configuration > VPN > General > Group Policy および Configuration > VPN > General > Tunnel Group

表 A-1　設定タスクのナビゲーション マップ（続き）

VPN 3000 タスク	項目	ASDM パス
ポリシー管理の設定	アクセス時間 トラフィック管理 • ネットワーク リスト • 規則 • SA • フィルタ • 帯域幅	Configuration > Security Policy Access Rules AAA Rules Filter Rules Service Policy Rules
	NAT ポリシー	Configuration > NAT
	証明書グループのマッチング • ポリシー（グループ派生用） • 規則	Configuration > VPN > IKE > Certificate Group Matching • Policy • Rules
	HTTP および HTTPS	Configuration > Properties > HTTP/HTTPS
	SSL	Configuration > Properties > SSL
Web VPN の設定	該当なし	Configuration > VPN > WebVPN
	アクセス	Configuration > VPN > WebVPN > WebVPN Access
	HTTP/HTTPS プロキシ	Configuration > VPN > WebVPN > Proxies
	ホームページ	Configuration > VPN > WebVPN > Webpage Customization
	ロゴ	Configuration > VPN > WebVPN > Webpage Customization
	E メール プロキシ	Configuration > VPN > E-mail Proxy
	サーバと URL	Configuration > VPN > WebVPN > Servers and URLs、Encoding
	ポート転送	Configuration > VPN > WebVPN > Port Forwarding
	NetBIOS ネーム サーバ	Configuration > VPN > Tunnel Group > Add WebVPN Access Tunnel Group > WebVPN タブ > NetBIOS Servers タブ
	SSL VPN Client	Configuration > VPN > WebVPN > SSL VPN Client
	Cisco Secure Desktop、Setup and Manager	Configuration > Properties > Device Administration > CSD Setup Configuration CSD Manager

表 A-2　管理タスクのナビゲーション マップ

VPN 3000 タスク	項目	ASDM パス
すべてのアクティブ セッションの統計情報の表示	該当なし	Monitoring > VPN
	表示のアップデート	**Refresh** をクリック
ASA システム ソフトウェアのアップデート	該当なし	Tools > Upgrade Software > Upload Image From Local PC
VPN クライアント ソフトウェアのアップデート	該当なし	Configuration > VPN > General > Client Update
システムのシャットダウンまたはリブート（あるいは両方）	該当なし	Tools > System Reload
リブート ステータスの表示	該当なし	Tools > System Reload
Ping ユーティリティの使用	該当なし	Tools > Ping
トレースルート	該当なし	Tools > Traceroute
管理者アクセス権の設定および制御	管理者のユーザ名、アクセス権、および権限の設定 管理者用 ACL の設定 アクセス設定値の設定	Configuration > Properties > Device Access > AAA Access
	管理ユーザ用の AAA サーバの設定	Configuration > Properties > AAA Setup > AAA Servers
	デバイスのフラッシュ　メモリ内のファイルの管理	Tools > File Management
	バックアップおよびブート コンフィギュレーション ファイルのスワップ	Tools > Upgrade Software > Upload Image from Local PC
	TFTP を使用したファイル転送	Tools > File Management > File Transfer > TFTP
	HTTP を使用したファイル送信	Tools > File Management > File Transfer > HTTP
	XML ファイルへのコンフィギュレーションのエクスポート	該当なし

表 A-2　管理タスクのナビゲーション マップ（続き）

VPN 3000 タスク	項目	ASDM パス
証明書の登録および管理（PKI）	証明書の登録 SSL 証明書の取得 CRL チェックおよびキャッシングのイネーブル化 リモート アクセス接続用のデジタル証明書のイネーブル化 サイトツーサイト接続用のデジタル証明書のイネーブル化 デジタル証明書の削除 証明書の管理 • ID 証明書および SSL 証明書の登録 • 登録済み証明書のインストール SCEP パラメータの設定 CRL キャッシュの表示 証明書情報の表示 CA 証明書の設定 証明書の更新 登録要求の管理	Configuration > Properties > Certificate Authentication Enrollment Import Certificate Keypair Manage Certificate Trustpoint

表 A-3　監視タスク

VPN 3000 タスク	項目	ASDM パス
ルーティング テーブルの監視（ルートおよびプロトコル）	該当なし	Monitoring > Routing > Routes Monitoring > Routing > OSPF LSAs Monitoring > Routing > OSPF Neighbors
動的フィルタおよび規則の表示	該当なし	Configuration > Security Policy
イベント ログの表示	該当なし	Monitoring > Logging > Real-Time Log Viewer
システム ステータスおよびメモリ ステータスの表示	該当なし	Monitoring > Properties > System Resource Graphs
すべてのアクティブ セッションの情報の表示	該当なし	Monitoring > VPN
統計の収集	該当なし	Monitoring > VPN > VPN Statistics
	アカウンティング	Monitoring > Properties > AAA Servers
	管理 AAA	Monitoring > Properties > AAA Servers
	認証	Monitoring > Properties > Device Access > Authenticated Users
	認可	Monitoring > Properties > AAA Servers
	帯域幅の管理	Monitoring > Properties > System Resource Graphs
	圧縮	Monitoring > VPN > VPN Statistics > Compression Statistics
	暗号	Monitoring > VPN > VPN Statistics > Crypto Statistics
	DHCP	Monitoring > Interfaces > DHCP
	DNS	Monitoring > Properties > DNS Cache
	暗号化	Monitoring > VPN > VPN Statistics > Encryption Statistics
	イベント	Monitoring > Logging > Real-Time Log Viewer
	フィルタリング	該当なし
	グローバル IKE/IPSec	Monitoring > VPN > VPN Statistics > Global IKE/IPSec Statistics
	IPSec トンネル	Monitoring > VPN > VPN Connection Graphs
	L2TP	Monitoring > VPN > VPN Connection Graph
	ロード バランシング	Monitoring > VPN > VPN Statistics > Cluster Loads
	PPTP	該当なし
	SSH	Monitoring > Properties > Device Access > Secure Shell Sessions
	SSL	Monitoring > Device Access > HTTPS/ASDM Sessions
	Telnet	Monitoring > Properties > Device Access > Telnet Sessions
	VRRP	該当なし

VPN 3000 シリーズ コンセントレータと ASA のデバッグ レベルまたはイベント レベルの比較

VPN 3000 シリーズ コンセントレータには、ロギングについて 13 段階の重大度レベルがあります。一方 ASA では、異なるデバッグ レベルを表すため、1 から 11、および 254 と 255 の番号を使用します。どちらのシステムでも、小さい番号ほど高い重大度を表します。たとえば、いずれかのシステムで重大度 3 を選択すると、重大度が上位 3 レベルのイベント メッセージのみが表示されます。表 B-1 は、VPN 3000 コンセントレータでの重大度と ASA での重大度のマッピングを示しています。

表 B-1　　デバッグ レベルのマッピング

VPN 3000 デバッグ レベル	ASA デバッグ レベル
1、2、3	1
4	2
5	3
6	4
7	5
8	6
9	7
10	8
11	9
12	10
13	11、254、255

ASA のデバッグ レベル 254 および 255 には、特殊な意味があります。

- 254 は、IKE パケット デコードを示します。ここには、各 IKE パケットのフィールドおよび値について、スニファ類似のデコードが表示されます。
- 255 は、IKE パケット ダンプを示します。ここには、パケット内のオクテットが表示されます。

より大きい数字のレベルを選択すると、そのレベルのロギング メッセージに加えて、それより数字が小さい（つまり、重大度がより大きい）レベルすべてのロギング メッセージがキャプチャされるため、表示されるデータの量は多くなります。

レベル 254 または 255 を選択すると、デバッグ トレース キューがオーバーフローする場合があります。オーバーフローを避けるには、**capture** コマンドを使用します。このとき、情報を保持するためのメモリ領域の名前と、パケット キャプチャの適用先のインターフェイスの名前を指定します。たとえば次のとおりです。

```
hostname(config)# capture name type isakmp interface interface-name
```

このコマンドを実行すると、メモリ内の 1 つの領域にデータが格納されます。格納されたデータは表示またはファイルへの書き込みが可能で、さらに後処理を行うと情報を抽出できます。**capture** コマンドの使用法の詳細については、このコマンドの説明を参照してください。

Numerics

A

C

D

H

I

K

L

M

O

P

Q

R

S

T

V

W

Z

あ

い

う

お

か

き

く

け

さ

し

す

せ

た

て

と

に

ね

は

ふ

ほ

ま

も

ゆ

ら

り

ろ

わ