CISCO SYSTEMS

Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス スタートアップ ガイド

For the Cisco ASA 5510, ASA 5520, and ASA 5540

Customer Order Number: DOC-J-7817611=
Text Part Number: 78-17611-01-J

CONTENTS

CHAPTER 1

始める前に

次の表を使用して、適応型セキュリティ アプライアンスの実装に必要なインストールおよびコンフィギュレーションの手順を検索します。

このマニュアルで扱う適応型セキュリティ アプライアンスの実装は、次のとおりです。

ASA 5500

作業内容	参照先
シャーシの設置	第 2 章「Cisco ASA 5500 の設置」
インターフェイス ケーブルの接続	第 4 章「インターフェイス ケーブルの接続」
適応型セキュリティ アプライアンスの初期セットアップの実行	第 5 章「適応型セキュリティ アプライアンスの設定」
実装に対応した適応型セキュリティ アプライアンスの設定	第 6 章「シナリオ：DMZ の設定」 第 7 章「シナリオ：リモートアクセス VPN の設定」 第 8 章「シナリオ：サイトツーサイト VPN の設定」
オプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のシステムの操作	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*

AIP SSM を使用する ASA 5500

作業内容	参照先
シャーシの設置	第 2 章「Cisco ASA 5500 の設置」
AIP SSM の取り付け	第 3 章「オプションの SSM の取り付け」
インターフェイス ケーブルの接続	第 4 章「インターフェイス ケーブルの接続」
適応型セキュリティ アプライアンスの初期セットアップの実行	第 5 章「適応型セキュリティ アプライアンスの設定」
AIP SSM に対応した適応型セキュリティ アプライアンスの設定	第 9 章「AIP SSM の設定」
侵入防御用 IPS ソフトウェアの設定	*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface* *Cisco Intrusion Prevention System Command Reference*
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide* *Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*

CSC SSM を使用する ASA 5500

作業内容	参照先
シャーシの設置	第 2 章「Cisco ASA 5500 の設置」
CSC SSM の取り付け	第 3 章「オプションの SSM の取り付け」
インターフェイス ケーブルの接続	第 4 章「インターフェイス ケーブルの接続」
適応型セキュリティ アプライアンスの初期セットアップの実行	第 5 章「適応型セキュリティ アプライアンスの設定」
コンテント セキュリティに対応した適応型セキュリティ アプライアンスの設定	第 10 章「CSC SSM の設定」
CSC SSM の設定	*Cisco Content Security and Control SSM Administrator Guide*
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide* *Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*

4GE SSM を使用する ASA 5500

作業内容	参照先
シャーシの設置	第 2 章「Cisco ASA 5500 の設置」
4GE SSM の取り付け	第 3 章「オプションの SSM の取り付け」
インターフェイス ケーブルの接続	第 4 章「インターフェイス ケーブルの接続」
適応型セキュリティ アプライアンスの初期セットアップの実行	第 5 章「適応型セキュリティ アプライアンスの設定」
光ファイバ モジュールの取り付け	第 3 章「オプションの SSM の取り付け」
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide* *Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*

CHAPTER 2

Cisco ASA 5500 の設置

警告 **この装置の設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。**

注意 これらの手順を実行するときは、『*Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*』の安全に関する警告を読み、適切な安全手順に従ってください。

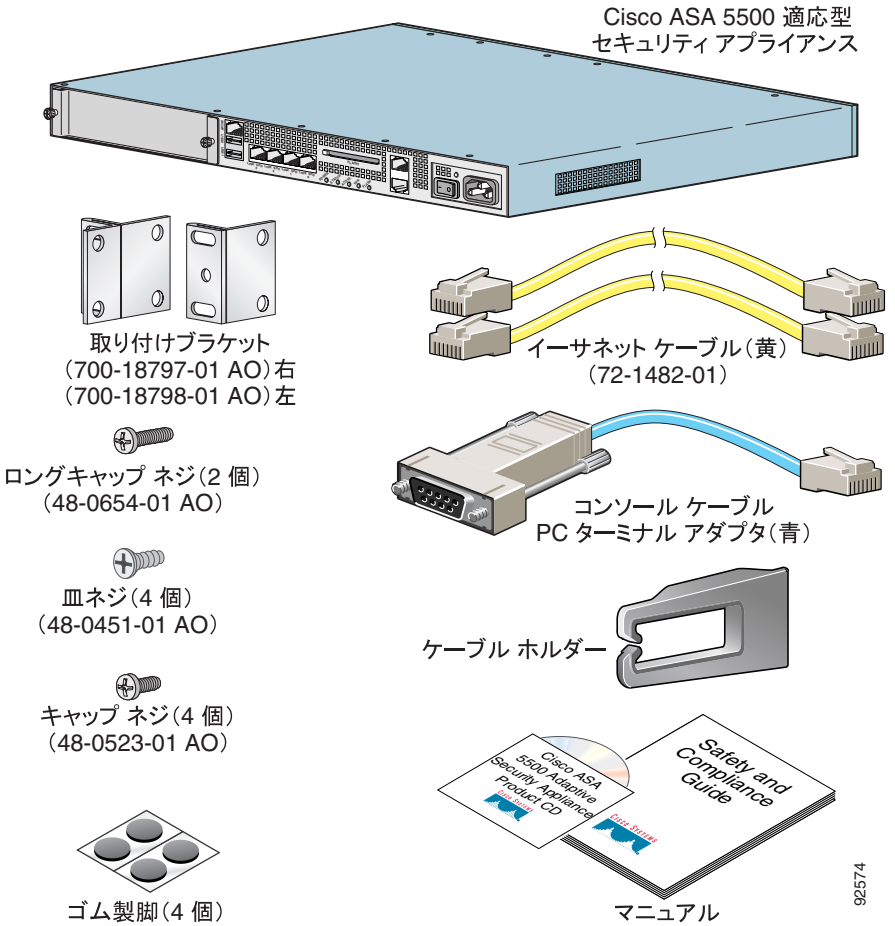
この章では、適応型セキュリティ アプライアンスの製品概要、メモリ要件、およびラックマウントと設置の手順について説明します。この章は、次の項で構成されています。

（注） このマニュアルで示す図は、Cisco ASA 5540 適応型セキュリティ アプライアンスのものです。Cisco ASA 5510 適応型セキュリティ アプライアンスと Cisco ASA 5520 適応型セキュリティ アプライアンスは同一で、背面パネルの機能とインジケータは同じです。

パッケージ内容の確認

梱包箱の内容を確認し、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの設置に必要なすべての品目を受領したことを確認します。図 2-1 を参照してください。

図 2-1　ASA 5500 パッケージの内容



シャーシの設置

ここでは、適応型セキュリティ アプライアンスのラックマウントおよび設置の方法について説明します。適応型セキュリティ アプライアンスは、19 インチラック（17.5 インチまたは 17.75 インチ（約 45 cm）の開口部）にマウントできます。

警告　**ラックにこの装置をマウントしたり、ラック上の装置の作業を行うときは、ケガをしないように、装置が安定した状態に置かれていることを十分に確認してください。安全のために、次のガイドラインに従ってください。**

次の情報は、ラックへの機器の取り付けを計画する場合に役立ちます。

- メンテナンスのためにラックの周囲にすき間を空けます。
- 閉鎖型ラックに装置をマウントする場合は、換気が十分に行われるようにします。閉鎖型ラックに装置を詰め込みすぎないようにしてください。各装置で熱が発生するため、ラック内に装置を詰め込みすぎないように注意が必要です。
- 開放型ラックに装置をマウントする場合は、ラックのフレームで吸気口や排気口をふさがないように注意します。
- ラックに装置を 1 つしか取り付けない場合は、ラックの一番下に装置をマウントします。
- すでに別の装置がこのラックに取り付けられている場合は、最も重い装置をラックの一番下に取り付け、重い順に下から上へと設置するようにします。
- ラックにスタビライザが付属している場合は、スタビライザを取り付けてから、ラックへの装置の取り付けまたはラックでの作業を行います。

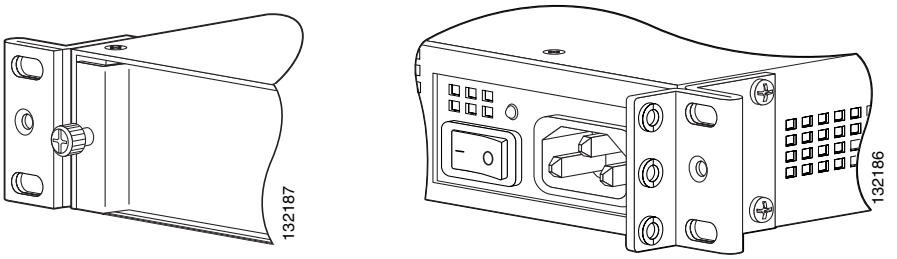
警告　**手順を実行する前に、DC 回路に電気が流れていないことを確認してください。すべての電源を確実に切断するには、パネル ボード上で DC 回路に対応している回路ブレーカーを確認して、回路ブレーカーを OFF の位置に切り替え、回路ブレーカーのスイッチ ハンドルを OFF の位置のままテープで固定します。**

シャーシのラックマウント

シャーシをラックマウントするには、次の手順に従います。

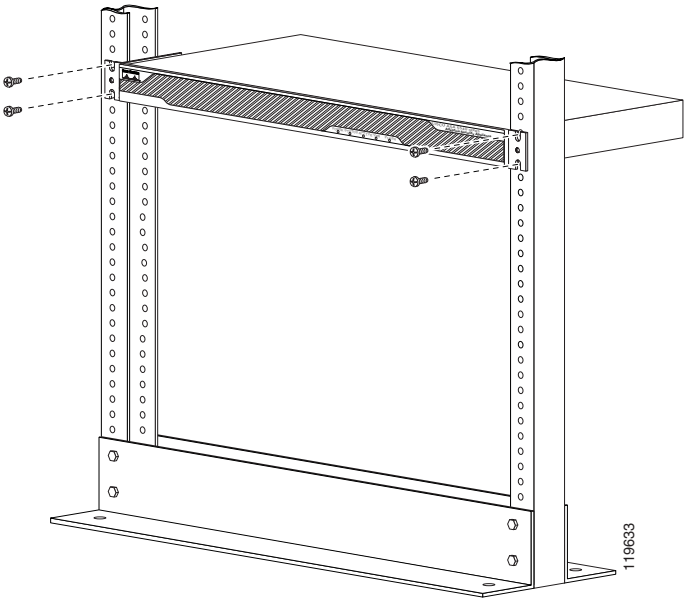
ステップ 1　付属のネジを使用して、シャーシにラックマウント ブラケットを取り付けます。ブラケットを穴に取り付けます（図 2-2 を参照してください）。ブラケットをシャーシに固定すると、ラックマウントできるようになります。

図 2-2　　右ブラケットと左ブラケットの取り付け



ステップ 2　付属のネジを使用して、シャーシをラックに取り付けます（図 2-3 を参照してください）。

図 2-3　　シャーシのラックマウント

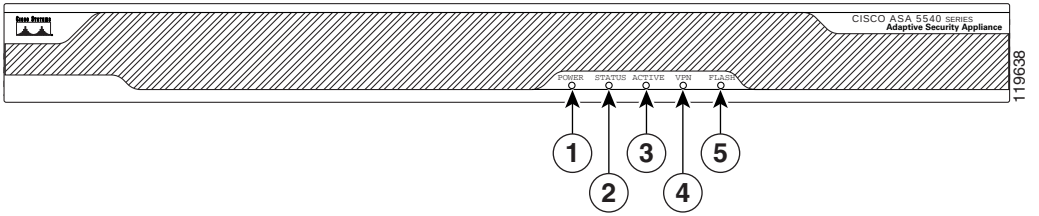


ラックからシャーシを取り外すには、シャーシをラックに取り付けているネジを外してから、シャーシを取り外します。

ポートと LED

ここでは、前面パネルと背面パネルについて説明します。図 2-4 に前面パネルの LED を示します。

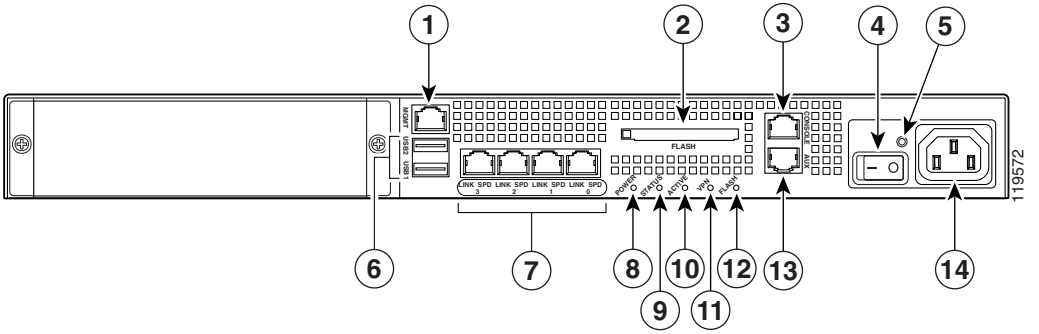
図 2-4　前面パネルの LED



	LED	色	ステート	説明
1	電源	緑	点灯	システムは通電状態です。
2	ステータス	緑	点滅	電源投入診断を実行中か、システムがブート中です。
			点灯	システムは電源投入診断に合格しました。
		オレンジ	点灯	電源投入診断に合格しませんでした。
3	アクティブ	緑	点灯	アクティブ フェールオーバー デバイスです。
		オレンジ	点灯	スタンバイ フェールオーバー デバイスです。
4	VPN	緑	点灯	VPN トンネルが確立されました。
5	フラッシュ	緑	点灯	CompactFlash がアクセスされています。

図 2-5 に適応型セキュリティ アプライアンスの背面パネルの機能を示します。

図 2-5　背面パネルの LED とポート（AC 電源モジュール モデルの場合）



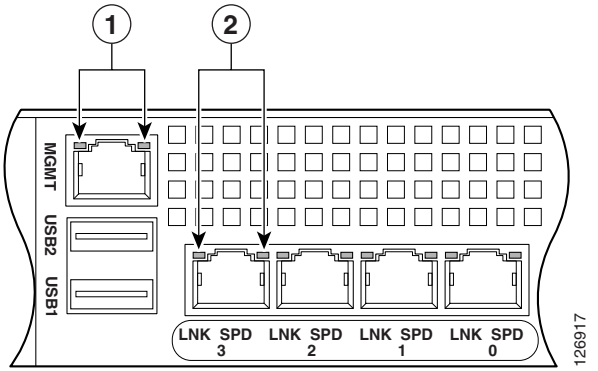
1	管理ポート[1]	**6**	USB 2.0 インターフェイス[2]	**11**	VPN LED
2	外部 CompactFlash スロット	**7**	ネットワーク インターフェイス[3]	**12**	フラッシュ LED
3	シリアル コンソール ポート	**8**	電源インジケータ LED	**13**	補助ポート
4	電源スイッチ	**9**	ステータス インジケータ LED	**14**	電源コネクタ
5	電源インジケータ LED	**10**	アクティブ LED		

1. 管理 0/0 インターフェイスは、管理トラフィックのためだけに設計されたファースト イーサネット インターフェイスです。
2. 現時点ではサポートされていません。
3. ギガビット イーサネット インターフェイス。右から左に、ギガビット イーサネット 0/0、ギガビット イーサネット 0/1、ギガビット イーサネット 0/2、ギガビット イーサネット 0/3 です。

管理ポートの詳細については、『*Cisco Security Appliance Command Reference*』の「Management-Only」の項を参照してください。

図 2-6 に適応型セキュリティ アプライアンスの背面パネルの LED を示します。

図 2-6　背面パネルのリンクおよび速度のインジケータ LED



1	MGMT インジケータ LED	**2**	ネットワーク インターフェイス LED

表 2-1 に、背面の MGMT およびネットワーク インターフェイスの LED を示します。

表 2-1　リンクおよび速度の LED

インジケータ	色	説明
左側	緑（点灯）	物理リンク
	緑（点滅）	ネットワーク アクティビティ
右側	消灯	10 Mbps
	緑	100 Mbps
	オレンジ	1000 Mbps

（注） ASA 5510 適応型セキュリティ アプライアンスがサポートするのは 10BaseTX および 100BaseTX のみです。ASA 5520 適応型セキュリティ アプライアンスおよび ASA 5540 適応型セキュリティ アプライアンスは 1000BaseT をサポートします。

次の手順

次の章のいずれかに進みます。

作業内容	参照先
購入したが取り付けていない SSM の取り付け	第 3 章「オプションの SSM の取り付け」
インターフェイス ケーブルの接続	第 4 章「インターフェイス ケーブルの接続」

次の手順

CHAPTER 3

オプションの SSM の取り付け

この章では、オプションの SSM（セキュリティ サービス モジュール）およびそのコンポーネントの取り付けについて説明します。この章の手順は、オプションの SSM を購入し、取り付けていない場合にのみ実行する必要があります。

この章は、次の項で構成されています。

Cisco 4GE SSM

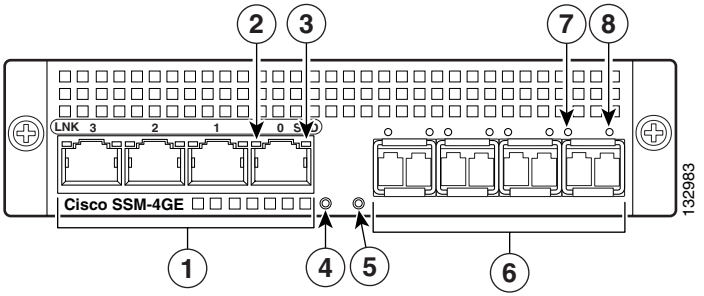
4GE セキュリティ サービス モジュール（SSM）には、8 個のイーサネット ポートがあります。10/100/1000 Mbps 用、銅線の RJ-45 ポートが 4 個、およびオプションの 1000 Mbps 用着脱可能小型フォーム ファクタ（SFP）ファイバ ポートが 4 個です。

この項では、適応型セキュリティ アプライアンスに対する Cisco 4GE SSM の取り付けと交換の方法について説明します。この項では、次のトピックについて取り上げます。

4GE SSM コンポーネント

図 3-1 に、Cisco 4GE SSM ポートと LED を示します。

図 3-1　Cisco 4GE SSM ポートと LED



1	RJ-45 ポート	**5**	ステータス LED
2	RJ-45 リンク LED	**6**	SFP ポート
3	RJ-45 速度 LED	**7**	SFP リンク LED
4	電源 LED	**8**	SFP 速度 LED

（注）　図 3-1 は、ポート スロットに取り付けられている SFP モジュールを示しています。この機能を使用する場合は、SFP モジュールを注文し、取り付ける必要があります。SFP ポートとモジュールの詳細については、P.3-5 の「SFP モジュールの取り付け」を参照してください。

表 3-1 で、Cisco 4GE SSM の LED について説明します。

表 3-1　Cisco 4GE SSM の LED

	LED	色	ステート	説明
2, 7	リンク	緑	点灯	イーサネット リンクがあります。
			点滅	イーサネット アクティビティが発生しています。
3, 8	速度	消灯 緑 オレンジ	10 MB	ネットワーク アクティビティは発生していません。
			100 MB	100 Mbps でネットワーク アクティビティが発生しています。
			1000 MB (GigE)	1000 Mbps でネットワーク アクティビティが発生しています。
4	電源	緑	点灯	システムは通電状態です。
5	ステータス	緑 緑 オレンジ	点滅	システムはブート中です。
			点灯	システムは正常にブートされました。
			点灯	システムの診断が失敗しました。

Cisco 4GE SSM の取り付け

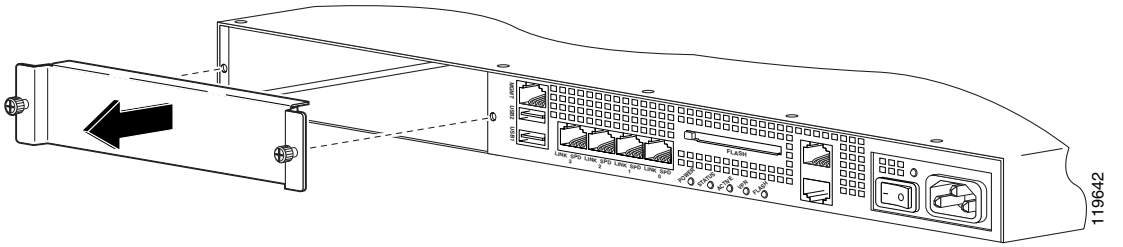
新しい Cisco 4GE SSM を初めて取り付けるには、次の手順に従います。

ステップ 1　適応型セキュリティ アプライアンスの電源を切ります。

ステップ 2　アクセサリ キットからアース ストラップを取り出して、肌に密着するように、ストラップの一端を手首に固定します。もう一方の端をシャーシに接続します。

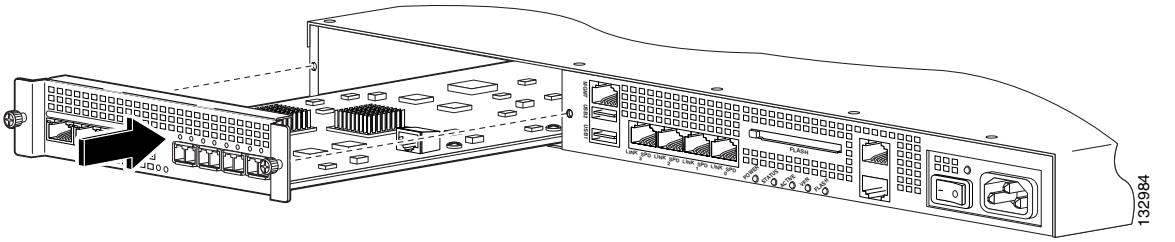
ステップ 3　シャーシ背面左端の 2 個のネジを外して（図 3-2 を参照）、スロット カバーを取り外します。

図 3-2　スロット カバーのネジの取り外し



ステップ 4　スロット開口部に Cisco 4GE SSM を差し込みます（図 3-3 を参照してください）。

図 3-3　スロットへの Cisco 4GE SSM の差し込み



ステップ 5　ネジを取り付けて、Cisco 4GE SSM をシャーシに固定します。

ステップ 6　適応型セキュリティ アプライアンスの電源を入れます。

ステップ 7　LED を確認します。Cisco 4GE SSM が適切に取り付けられると、ステータス LED が点滅（ブート アップ中の場合）、または点灯（操作可能になった場合）します。

ステップ 8　RJ-45 ケーブルの一方の端をポートに接続し、もう一方の端をネットワーク デバイスに接続します。詳細については、第 4 章「インターフェイス ケーブルの接続」を参照してください。

SFP モジュールの取り付け

SFP（着脱可能小型フォーム ファクタ）は、ホットスワップ可能な入力 / 出力デバイスで、SFP ポートに接続されます。次の SFP モジュール タイプがサポートされています。

- 長波長 / ロング ホール 1000BASE-LX/LH (GLC-LH-SM=)
- 短波長 1000BASE-SX (GLC-SX-MM=)

この項では、光ギガビット イーサネット接続を使用できるように、適応型セキュリティ アプライアンスに対する SFP モジュールの取り付けと取り外しの方法について説明します。この項では、次のトピックについて取り上げます。

SFP モジュール

適応型セキュリティ アプライアンスは、現場交換可能な SFP モジュールを使用して、ギガビット接続を確立します。

（注）　スイッチの電源を入れた後で SFP モジュールを取り付ける場合は、適応型セキュリティ アプライアンスをリロードして、SFP モジュールをイネーブルにする必要があります。

表 3-2 に、適応型セキュリティ アプライアンスによってサポートされる SFP モジュールを示します。

表 3-2　サポートされる SFP モジュール

SFP モジュール	接続タイプ	シスコ製品番号
1000BASE-LX/LH	光ファイバ	GLC-LH-SM=
1000BASE-SX	光ファイバ	GLC-SX-MM=

1000BASE-LX/LH と 1000BASE-SX の SFP モジュールは、光ファイバ接続の確立に使用されます。SFP モジュールに接続するには、LC コネクタに光ファイバ ケーブルを使用します。SFP モジュールは、850 ～ 1550 nm の公称波長をサポートします。ケーブルの長さは、信頼できる通信の要件であるケーブル長を超えることはできません。表 3-3 に、ケーブル長の要件を示します。

表 3-3　光ファイバ SFP モジュールのケーブル要件

SFP モジュール	62.5/125 ミクロン マルチモード 850 nm ファイバ	50/125 ミクロン マルチモード 850 nm ファイバ	62.5/125 ミクロン マルチモード 1310 nm ファイバ	50/125 ミクロン マルチモード 1310 nm ファイバ	9/125 ミクロン シングルモード 1310 nm ファイバ
LX/LH	—	—	500 Mhz-km で 550 m	400 Mhz-km で 550 m	10 km
SX	200 Mhz-km で 275 m	500 Mhz-km で 550 m	—	—	—

適応型セキュリティ アプライアンスには、シスコ認定の SFP モジュールのみを使用します。SFP モジュールにはそれぞれ、セキュリティ情報で符号化された内部シリアル EEPROM があります。この符号化によって、SFP モジュールが適応型セキュリティ アプライアンスの要件を満たしていることを、シスコが識別して検証できます。

（注） 適応型セキュリティ アプライアンスでサポートされるのは、シスコによって認定された SFP モジュールのみです。

注意 SFP からケーブルを外した後は、清潔なダスト プラグを SFP に差し込んで SFP モジュールを保護します。別の SFP モジュールの光ボアにファイバ ケーブルを再接続する前に、ケーブルの受光面が汚れていないことを確認してください。SFP モジュールの光ボアが埃などで汚れないようにします。光学機器は、埃が付着すると正しく動作しません。

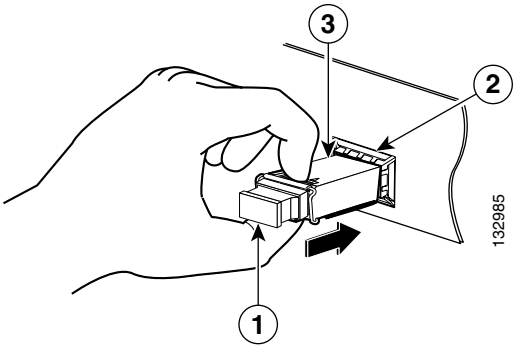
警告 **ケーブルが接続されていない場合、ポートの開口部からは目に見えないレーザー光が放射されている可能性があります。レーザー光に当たらないようにし、開口部をのぞきこまないでください。**ステートメント 70

SFP モジュールの取り付け

SFP モジュールを Cisco 4GE SSM に取り付けるには、次の手順に従います。

ステップ 1　SFP モジュールをポートの位置に合せ、ロックする位置までポート スロット内にスライドさせます（図 3-4 を参照してください）。

図 3-4　SFP モジュールの取り付け



1	光ポート プラグ	**3**	SFP モジュール
2	SFP ポート スロット		

注意　ケーブル接続の準備ができるまでは光ポート プラグを SFP から取り外さないでください。

ステップ 2　光ポート プラグを取り外し、ネットワーク ケーブルを SFP モジュールに接続します。

ケーブルのもう一方の端をネットワークに接続します。ケーブル接続の詳細については、第 4 章「インターフェイス ケーブルの接続」を参照してください。

注意　多くの SFP で使用されているラッチ メカニズムによって、ケーブルが接続されると SPF がロックされます。SFP を取り外す際にはケーブルを引っ張らないようにしてください。

Cisco AIP SSM および CSC SSM

ASA 5500 シリーズ 適応型セキュリティ アプライアンスは、インテリジェント SSM とも呼ばれる AIP SSM（Advanced Inspection and Prevention Security Services Module）および CSC SSM（Content Security Control Security Services Module）をサポートします。

AIP SSM は、セキュリティ検査を提供する高度な IPS ソフトウェアを実行します。AIP SSM には、AIP SSM 10 と AIP SSM 20 の 2 つのモデルがあります。両タイプの外観は同じですが、AIP SSM 20 は AIP SSM 10 よりもプロセッサが高速で、多くのメモリを備えています。スロットに実装できるのは、一度に 1 モジュール（AIP SSM 10 または AIP SSM 20）のみです。

表 3-4 に、AIP SSM 10 と AIP SSM 20 のメモリ仕様を示します。

表 3-4　SSM のメモリ仕様

SSM	CPU	DRAM
AIP SSM 10	2.0 GHz Celeron	1.0 GB
AIP SSM 20	2.4 GHz Pentium 4	2.0 GB

AIP SSM の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の「Managing the AIP SSM」を参照してください。

CSC SSM は、Content Security and Control ソフトウェアを実行します。CSC SSM は、ウイルス、スパイウェア、スパムなど、望ましくないトラフィックからの保護を提供します。CSC SSM の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の「Managing the CSC SSM」を参照してください。

この項では、適応型セキュリティ アプライアンスに対する SSM の取り付けと、交換の方法について説明します。図 3-5 に、SSM の LED を示します。

図 3-5　SSM の LED

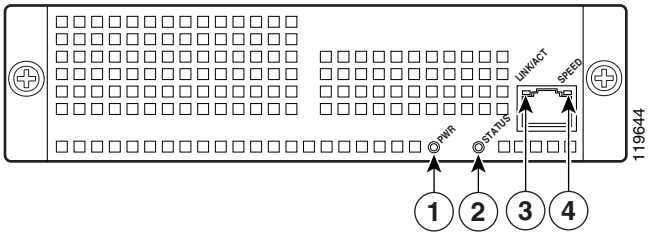


表 3-5 で、SSM の LED について説明します。

表 3-5　SSM の LED

	LED	色	ステート	説明
1	電源	緑	点灯	システムは通電状態です。
2	ステータス	緑	点滅	システムはブート中です。
			点灯	システムは電源投入診断に合格しました。
3	リンク / アクティブ	緑	点灯	イーサネット リンクがあります。
			点滅	イーサネット アクティビティが発生しています。
4	速度	緑	100 MB	ネットワーク アクティビティが発生しています。
		オレンジ	1000 MB (GigE)	ネットワーク アクティビティが発生しています。

SSM の取り付け

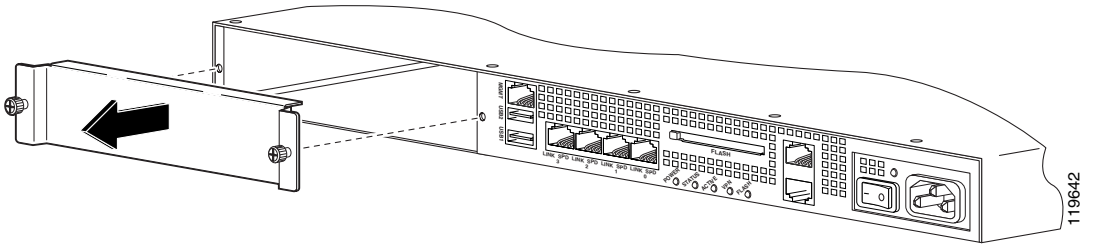
新しい SSM を取り付けるには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスの電源を切ります。

ステップ 2　アクセサリ キットからアース ストラップを取り出して、肌に密着するように、ストラップの一端を手首に固定します。もう一方の端をシャーシに接続します。

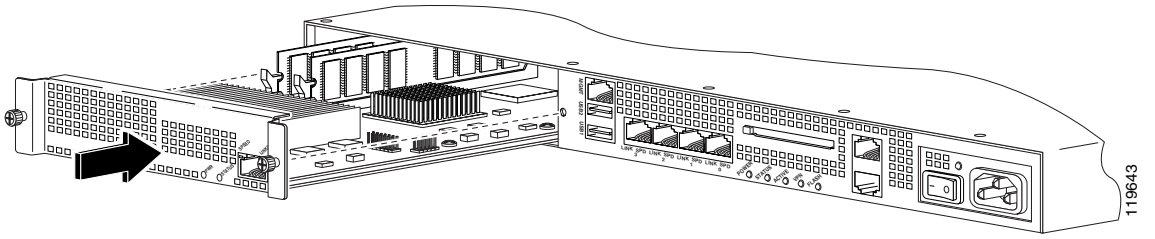
ステップ 3　シャーシ背面左端の 2 個のネジを外して（図 3-6 を参照）、スロット カバーを取り外します。

図 3-6　スロット カバーのネジの取り外し



ステップ 4　スロット開口部に SSM を差し込みます（図 3-7 を参照してください）。

図 3-7　スロットへの SSM の差し込み



ステップ 5　ネジを取り付けて、SSM をシャーシに固定します。

ステップ 6　適応型セキュリティ アプライアンスの電源を入れます。LED を確認します。SSM が適切に取り付けられると、電源 LED が緑色に点灯し、ステータス LED が緑色に点滅します。

ステップ 7　RJ-45 ケーブルの一方の端をポートに接続し、もう一方の端をネットワーク デバイスに接続します。

次の手順

第 4 章「インターフェイス ケーブルの接続」に進みます。

CHAPTER 4

インターフェイス ケーブルの接続

この章では、コンソール ポート、補助ポート、管理ポート、Cisco 4GE SSM のポート、および SSM のポートにケーブルを接続する方法について説明します。このマニュアルでは、SSM はインテリジェント SSM（AIP SSM または CSC SSM）を指します。

この章は、次の項で構成されています。

（注） 4GE SSM、AIP SSM、および CSC SSM は、オプションのセキュリティ サービス モジュールです。使用する適応型セキュリティ アプライアンスにこれらのモジュールがない場合は、これらの手順をスキップします。

警告 **この機器の設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。ステートメント 49**

注意 これらの手順を実行するときは、『*Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*』の安全に関する警告を読み、適切な安全手順に従ってください。

インターフェイスへのケーブルの接続

ケーブルをインターフェイスに接続するには、次の手順に従います。

ステップ 1　シャーシを平坦で安定した場所に置くか、またはラックに設置します（ラックマウントの場合）。

ステップ 2　コンピュータまたはターミナルをポートに接続する前に、シリアル　ポートのボー レートを確認します。ボー レートは、適応型セキュリティ アプライアンスのコンソール ポートのデフォルト ボー レート（9600 ボー）と一致している必要があります。ターミナルの設定は次のとおりです。9600 ボー（デフォルト）、8 データ ビット、パリティなし、1 ストップ ビット、およびフロー制御（FC）= ハードウェア。

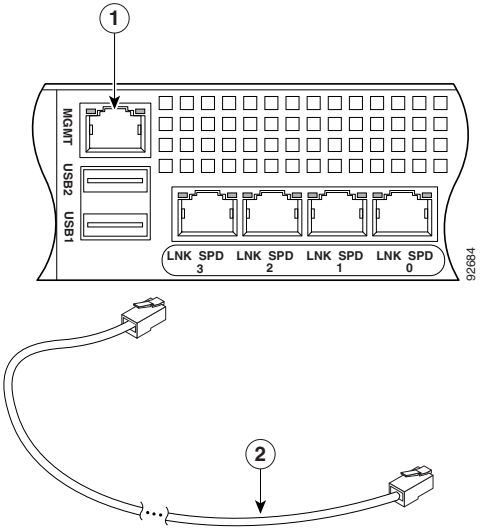
ステップ 3　ケーブルをポートに接続します。

a. 管理ポートの場合：適応型セキュリティ アプライアンスには、管理 0/0 ポートと呼ばれる専用の管理インターフェイスがあります。管理 0/0 ポートは、トラフィック管理にのみ使用される専用ポートとのファースト イーサネット インターフェイスです。コンソール ポートと類似していますが、管理ポートは適応型セキュリティ アプライアンスへの着信トラフィックのみを受け入れます。

（注）　インターフェイスを管理専用インターフェイスとして設定するには、**management-only** コマンドを使用します。管理インターフェイスの管理専用モードをディセーブルにすることもできます。このコマンドの詳細については、『*Cisco Security Appliance Command Reference*』の **management-only** コマンドの説明を参照してください。

- RJ-45 コネクタの一方を管理 0/0 ポートに接続します（図 4-1 を参照してください）。
- イーサネット ケーブルのもう一方の端を、コンピュータのイーサネット ポートに接続します。

図 4-1　　管理ポートへの接続

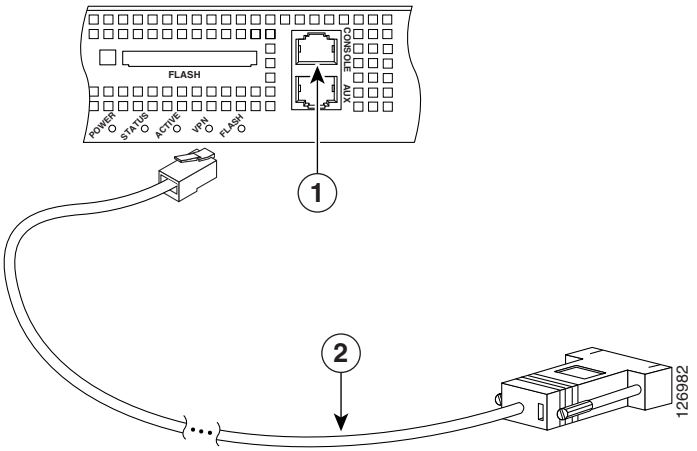


1	管理ポート	**2**	RJ-45/RJ-45 イーサネット ケーブル

b. コンソール ポートの場合

- シリアル コンソール ケーブルを接続します（図 4-2 を参照してください）。コンソール ケーブルには、一方の端にコンピュータのシリアル ポート用の DB-9 コネクタがあり、もう一方の端に RJ-45 コネクタがあります。
- RJ-45　コネクタを適応型セキュリティ　アプライアンスのコンソール ポートに接続します。
- ケーブルのもう一方の端（DB-9 コネクタ）を、コンピュータのコンソール ポートに接続します。

図 4-2　　コンソール ケーブルの接続

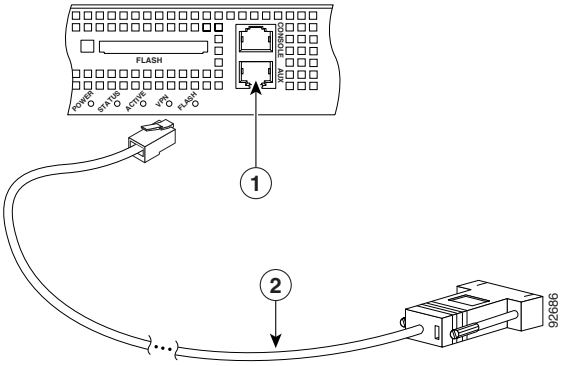


1	RJ-45 コンソール ポート	**2**	RJ-45/DB-9 コンソール ケーブル

c. 補助ポートの場合

- シリアル コンソール ケーブルを接続します（図 4-2 を参照してください）。コンソール ケーブルには、一方の端にコンピュータのシリアル ポート用の DB-9 コネクタがあり、もう一方の端に RJ-45 コネクタがあります。
- RJ-45　コネクタを適応型セキュリティ　アプライアンスの補助ポート（AUX というラベルがあるポート）に接続します（図 4-3 を参照してください）。
- ケーブルのもう一方の端（DB-9　コネクタ）を、コンピュータのシリアル ポートに接続します。

図 4-3　　補助ポートへの接続



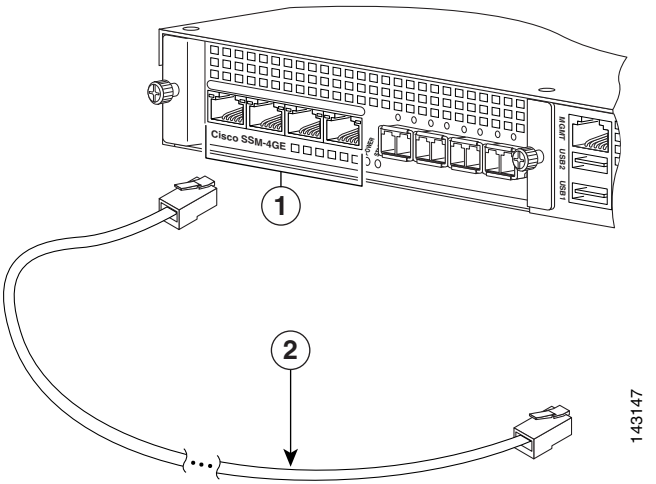
1	RJ-45 補助ポート	**2**	RJ-45/DB-9 コンソール ケーブル

d. Cisco 4GE SSM

- イーサネット ポート
  - RJ-45 コネクタの一方を Cisco 4GE SSM のイーサネット ポートに接続します（図 4-4 を参照してください）。
  - イーサネット ケーブルのもう一方の端をネットワーク デバイス（ルータ、スイッチ、ハブなど）に接続します。

（注） Cisco 4GE SSM はオプションです。この接続は、適応型セキュリティ アプライアンスに Cisco 4GE SSM を取り付けた場合にのみ必要です。

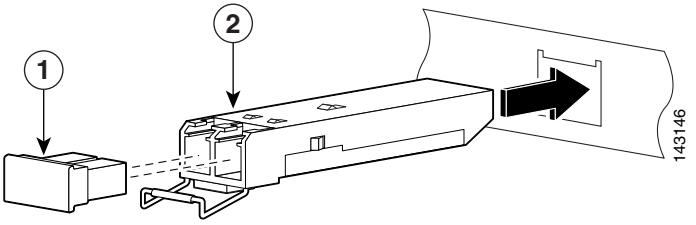
図 4-4　RJ-45 ポートへの接続



1	イーサネット ポート	**2**	RJ-45 コネクタ

- SFP モジュール
  - SFP モジュールを、カチッという音が聞こえるまで SFP ポートに差し込み、スライドさせます。カチッという音は、SFP モジュールがポートにロックされたことを示します。
  - 取り付けた SFP から光ポート プラグを取り外します（図 4-5 を参照してください）。

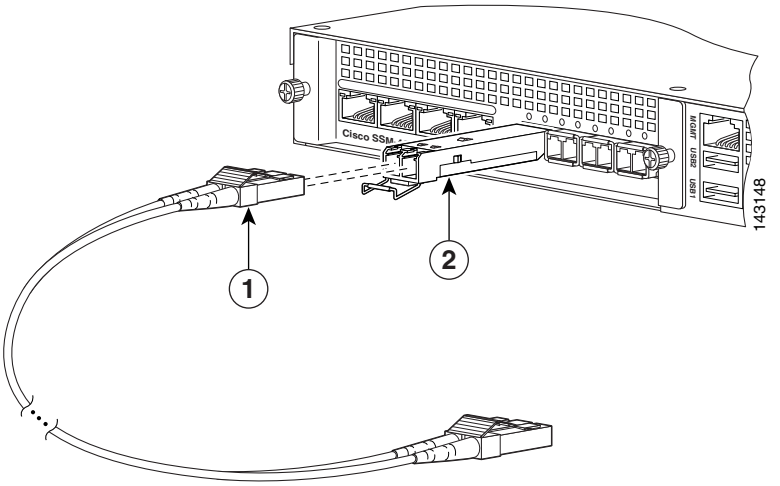
図 4-5　光ポート プラグの取り外し



1	光ポート プラグ	**2**	SFP モジュール

  - LC コネクタを SFP モジュールに接続します（図 4-6 を参照してください）。

図 4-6　　LC コネクタの接続



1	LC コネクタ	**2**	SFP モジュール

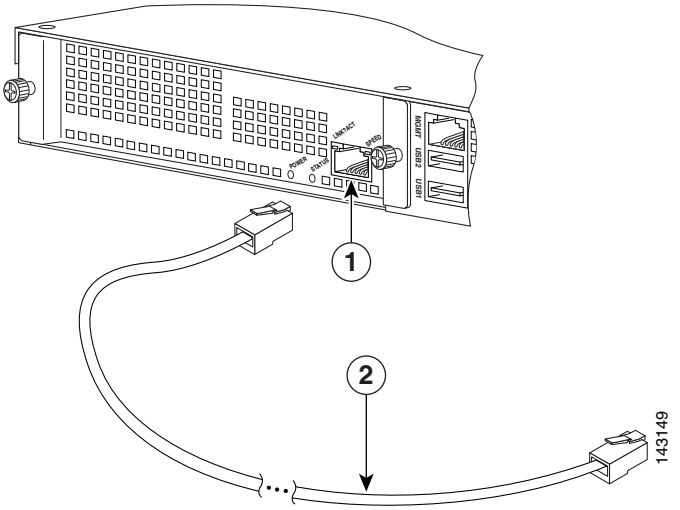
– もう一方の端をネットワーク デバイス（ルータ、スイッチ、ハブなど）に接続します。

e. SSM

- RJ-45 コネクタの一方を SSM の管理ポートに接続します（図 4-7 を参照してください）。
- RJ-45 ケーブルのもう一方の端をネットワーク デバイスに接続します。

（注） SSM はオプションです。この接続は、適応型セキュリティ アプライアンスに SSM を取り付けた場合にのみ必要です。

図 4-7　管理ポートへの接続

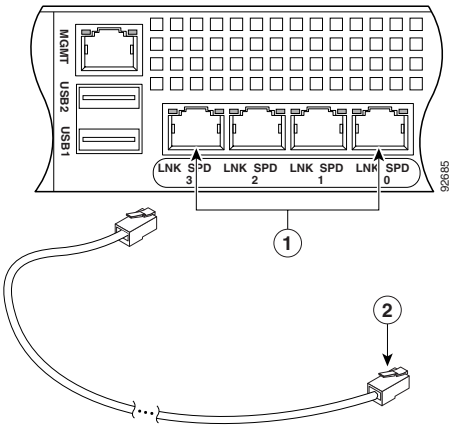


1	SSM 管理ポート	**2**	RJ-45/RJ-45 ケーブル

f. イーサネット ポートの場合

- RJ-45 コネクタをイーサネット ポートに接続します（図 4-8 を参照してください）。
- イーサネット ケーブルのもう一方の端をネットワーク デバイス（ルータ、スイッチ、ハブなど）に接続します。

図 4-8　　ネットワーク インターフェイスへのケーブルの接続



1	RJ-45 イーサネット ポート	**2**	RJ-45 コネクタ

ステップ 4　電源コードを適応型セキュリティ　アプライアンスに接続して、もう一方の端を電源に差し込みます。

ステップ 5　シャーシの電源を入れます。

次の手順

第 5 章「適応型セキュリティ アプライアンスの設定」に進みます。

次の手順

CHAPTER 5

適応型セキュリティ アプライアンスの設定

この章では、適応型セキュリティ アプライアンスの初期設定について説明します。設定の手順は、ブラウザベースの Cisco Adaptive Security Device Manager（ASDM）またはコマンドライン インターフェイス（CLI）で実行できます。ただし、この章の手順では、ASDM を使用する方法を示します。

（注） ASDM を使用するには、DES ライセンスまたは 3DES-AES ライセンスが必要です。詳細については、付録 A「DES ライセンスまたは 3DES-AES ライセンスの取得」を参照してください。

この章は、次の項で構成されています。

工場出荷時のデフォルト設定について

シスコの適応型セキュリティ アプライアンスは、すぐにスタートアップできるように、工場出荷時のデフォルト設定が設定されて出荷されます。この設定は、ほとんどの小規模および中規模のビジネス ネットワーキング環境に適合します。

デフォルトでは、適応型セキュリティ アプライアンスの管理インターフェイスは、デフォルトの DHCP アドレス プールで設定されます。この設定によって、内部ネットワークのクライアントは、適応型セキュリティ アプライアンスから DHCP アドレスを取得し、装置に接続できます。この後、管理者は ASDM を使用して、適応型セキュリティ アプライアンスを設定および管理できます。ネットワーク セキュリティ ポリシーに基づき、外部インターフェイスまたは必要なその他の任意のインターフェイスを経由するすべての ICMP トラフィックを拒否するように、適応型セキュリティ アプライアンスを設定することを検討する必要があります。

Adaptive Security Device Manager について

Adaptive Security Device Manager（ASDM）は、適応型セキュリティ アプライアンスを管理および監視できる、機能が豊富なグラフィカル インターフェイスです。Web ベースの設計によって、Web ブラウザを使用して任意の場所から適応型セキュリティ アプライアンスに接続し、管理できるように、セキュアなアクセスが提供されます。

完全な設定機能および管理機能のほかに、ASDM には、適応型セキュリティ アプライアンスの配置を簡素化し、高速化するインテリジェント ウィザードが含まれています。

ASDM を使用するには、DES ライセンスまたは 3DES-AES ライセンスが必要です。また、Web ブラウザで Java および JavaScript をイネーブルにする必要があります。

ASDM Web 設定ツールのほかに、コマンドライン インターフェイスでも適応型セキュリティ アプライアンスを設定できます。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』および『*Cisco Security Appliance Command Reference*』を参照してください。

Startup Wizard を起動する前に

Startup Wizard を起動する前に、次の手順を実行します。

ステップ 1　DES ライセンスまたは 3DES-AES ライセンスを取得します。

ASDM を実行するには、DES ライセンスまたは 3DES-AES ライセンスが必要です。適応型セキュリティ アプライアンスの購入時にこれらのライセンスを購入していない場合は、取得方法とアクティブ化の方法について、付録 A「DES ライセンスまたは 3DES-AES ライセンスの取得」を参照してください。

ステップ 2　Web ブラウザで Java と Javascript をイネーブルにします。

ステップ 3　次の情報を収集します。

- ネットワークで適応型セキュリティ　アプライアンスを識別する一意のホスト名
- 外部インターフェイス、内部インターフェイス、およびその他のすべてのインターフェイスの IP アドレス
- NAT または PAT の設定に使用する IP アドレス
- DHCP サーバの IP アドレス範囲

Startup Wizard の使用

ASDM には、適応型セキュリティ アプライアンスの初期設定を簡素化する Startup Wizard が含まれています。Startup Wizard を使用すると、内部ネットワーク（GigabitEthernet0/1）と外部ネットワーク（GigabitEthernet0/0）の間でパケットがセキュアに流れるように、わずかな手順で適応型セキュリティ アプライアンスを設定できます。

Startup Wizard を使用して適応型セキュリティ アプライアンスの基本設定をセットアップするには、次の手順を実行します。

ステップ 1　次の手順のいずれかを実行していない場合、実行します。

- ASA 5520 または 5540 の場合、イーサネット ケーブルで内部 GigabitEthernet0/1 インターフェイスをスイッチまたはハブに接続する。同じスイッチに、適応型セキュリティ アプライアンスの設定に使用する PC を接続する。
- ASA 5510 の場合、イーサネット ケーブルで内部 Ethernet 1 インターフェイスをスイッチまたはハブに接続する。同じスイッチに、適応型セキュリティ アプライアンスの設定に使用する PC を接続する。

ステップ 2　DHCP を使用するように（適応型セキュリティ アプライアンスから IP アドレスを自動的に受信するように）、PC を設定します。または、192.168.1.0 ネットワークの外のアドレスを選択して、固定 IP アドレスを PC に割り当てます（有効なアドレスは 192.168.1.2 ～ 192.168.1.254 で、マスクが 255.255.255.0、デフォルト ルートが 192.168.1.1 です）。

（注）　デフォルトで、適応型セキュリティ アプライアンスの内部インターフェイスに 192.168.1.1 が割り当てられているため、このアドレスは使用できません。

ステップ 3　次の手順のいずれかを実行します。

- ASA 5520 または 5540 の場合、GigabitEthernet0/1 インターフェイスの LINK LED を確認する。
- ASA 5510 の場合、Ethernet 1 インターフェイスの LINK LED を確認する。

接続が確立されると、適応型セキュリティ アプライアンスの LINK LED インターフェイスと、スイッチまたはハブの対応する LINK LED が緑色に点灯します。

ステップ 4　Startup Wizard を起動します。

a. スイッチまたはハブに接続された PC で、インターネット ブラウザを起動します。

b. ブラウザのアドレス フィールドに、URL「**https://192.168.1.1/**」を入力します。

（注） 適応型セキュリティ アプライアンスの出荷時のデフォルト IP アドレスは 192.168.1.1 です。「**s**」を追加して「**https**」にすることに注意してください。追加しないと、接続が失敗します。HTTPS（HTTP over SSL）は、ブラウザと適応型セキュリティ アプライアンスとの間でセキュアな接続を提供します。

ステップ 5　ユーザ名とパスワードを要求するダイアログボックスで、両方のフィールドを空のままにします。**Enter** キーを押します。

ステップ 6　**Yes** をクリックして、証明書を受け付けます。すべてのユーザ認証および証明書ダイアログボックスで、**Yes** をクリックします。

ASDM が起動します。

ステップ 7　ASDM ウィンドウの上部の Wizards メニューから、Startup Wizard を選択します。

ステップ 8　Startup Wizard の指示に従い、適応型セキュリティ アプライアンスをセットアップします。

Startup Wizard のフィールドの詳細については、ウィンドウの下部の **Help** をクリックしてください。

次の手順

次の章のいずれか、または複数を使用して、配置用に適応型セキュリティ アプライアンスを設定します。

作業内容	参照先
DMZ Web サーバ保護用の適応型セキュリティ アプライアンスの設定	第 6 章「シナリオ：DMZ の設定」
リモートアクセス VPN 用の適応型セキュリティ アプライアンスの設定	第 7 章「シナリオ：リモートアクセス VPN の設定」
サイトツーサイト VPN 用の適応型セキュリティ アプライアンスの設定	第 8 章「シナリオ：サイトツーサイト VPN の設定」
侵入防御用の AIP SSM の設定	第 9 章「AIP SSM の設定」
コンテント セキュリティ用の CSC SSM の設定	第 10 章「CSC SSM の設定」

CHAPTER 6

シナリオ：DMZ の設定

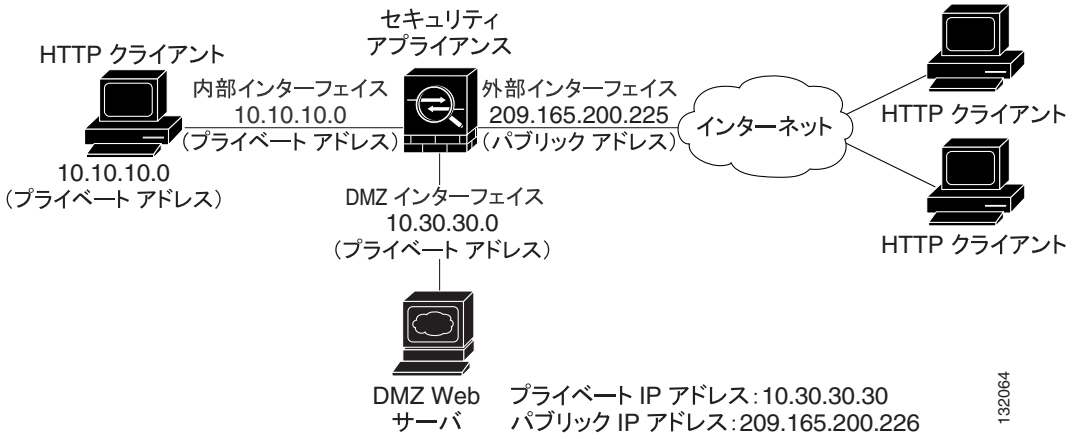
この章では、非武装地帯（DMZ）にあるネットワーク リソースを保護するために適応型セキュリティ アプライアンスが使用される設定シナリオについて説明します。DMZ とは、プライベート（内部）ネットワークとパブリック（外部）ネットワークの間の中立ゾーンにある区別されたネットワークです。

この章は、次の項で構成されています。

DMZ ネットワーク トポロジの例

図 6-1 で示すネットワーク トポロジは、適応型セキュリティ アプライアンスのほとんどの DMZ 実装の代表的な例です。

図 6-1　DMZ の設定シナリオのネットワーク レイアウト



このシナリオの例には、次の特徴があります。

- Web サーバは、適応型セキュリティ アプライアンスの DMZ インターフェイス上にあります。
- プライベート ネットワーク上の HTTP クライアントは、DMZ の Web サーバにアクセスでき、またインターネット上のデバイスとも通信できます。
- インターネット上のクライアントは、DMZ Web サーバへの HTTP アクセスを許可され、その他のトラフィックはすべて拒否されます。
- ネットワークには、パブリックに使用可能な 2 つのルーティング可能 IP アドレスがあります。1 つは適応型セキュリティ アプライアンスの外部インターフェイス（209.165.200.225）で、もう 1 つは DMZ Web サーバのパブリック IP アドレス（209.165.200.226）です。

図 6-2 は、プライベート ネットワークから DMZ Web サーバとインターネットの両方への HTTP 要求の発信トラフィック フローを示しています。

図 6-2　プライベート ネットワークからの発信 HTTP トラフィック フロー

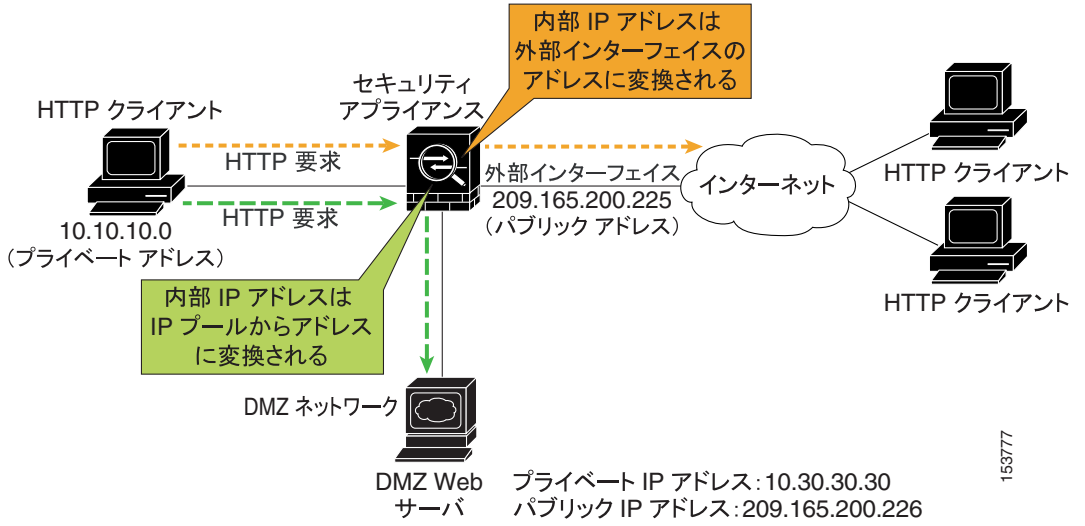


図 6-2 では、内部のクライアントから発信され、DMZ Web サーバとインターネット上のデバイスの両方に送信される HTTP トラフィックが適応型セキュリティ アプライアンスによって許可されます。トラフィックの通過を許可するために、適応型セキュリティ アプライアンス設定には次の要素が含まれています。

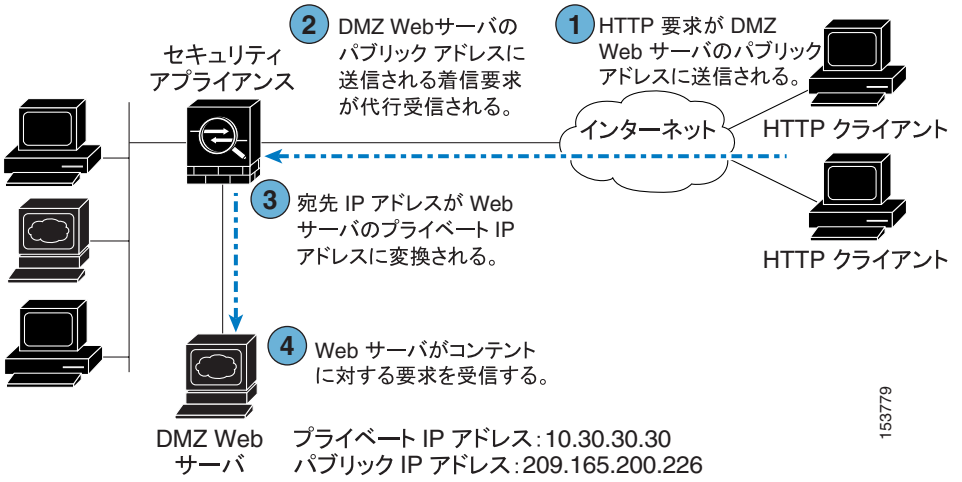
- アクセス コントロール規則（DMZ Web サーバとインターネット上のデバイスに送信されるトラフィックを許可します）
- アドレス変換規則（プライベート IP アドレスをインターネットから見えないように変換します）

  DMZ Web サーバに送信されるトラフィックの場合、プライベート IP アドレスは IP プールからアドレスに変換されます。

  インターネットに送信されるトラフィックの場合、プライベート IP アドレスは適応型セキュリティ アプライアンスのパブリック IP アドレスに変換されます。発信トラフィックは、このアドレスから発信されたように見えます。

図 6-3 は、インターネットから発信され、DMZ Web サーバのパブリック IP アドレスに送信される HTTP 要求を示しています。

図 6-3　インターネットからの着信 HTTP トラフィック フロー



着信トラフィックに DMZ Web サーバへのアクセスを許可するために、適応型セキュリティ アプライアンス設定には次の要素が含まれています。

- アドレス変換規則（DMZ Web サーバのパブリック IP アドレスを DMZ Web サーバのプライベート IP アドレスに変換します）
- アクセス コントロール規則（DMZ Web サーバに送信される着信 HTTP トラフィックを許可します）

この設定の作成手順は、この章の残りの部分で詳しく説明します。

DMZ 配置用のセキュリティ アプライアンスの設定

この章では、ASDM を使用して、図 6-1 で示す設定シナリオの適応型セキュリティ アプライアンスを設定する方法について説明します。手順で使用するサンプル パラメータは、シナリオに基づいています。

この設定手順では、内部インターフェイス、DMZ インターフェイス、および外部インターフェイス用に適応型セキュリティ アプライアンスのインターフェイスがすでに設定されていることを前提としています。適応型セキュリティ アプライアンスのインターフェイスをセットアップするには、ASDM の Startup Wizard を使用します。DMZ インターフェイスのセキュリティ レベルが 0 ～ 100 に設定されていることを確認します（一般的な値は 50 です）。

Startup Wizard の使用方法の詳細については、第 5 章「適応型セキュリティ アプライアンスの設定」を参照してください。

この項では、次のトピックについて取り上げます。

次の各項で、それぞれの手順を実行する方法について詳しく説明します。

設定の要件

この DMZ 配置用に適応型セキュリティ アプライアンスを設定するには、次の設定作業が必要になります。

- DMZ Web サーバへの HTTP アクセスを内部クライアントに提供するために、アドレス変換用の IP アドレスのプールを作成し、そのプールからアドレスを使用するクライアントを特定する必要があります。この作業を完了するには、次の要素を設定する必要があります。
  - DMZ インターフェイス用の IP アドレスのプール。このシナリオでは、IP プールは 10.30.30.50 ～ 10.30.30.60 です。
  - 内部インターフェイス用の動的 NAT 変換規則。この規則には、IP プールからアドレスを割り当てることができるクライアント IP アドレスを指定します。
- 内部クライアントがインターネット上の HTTP リソースおよび HTTPS リソースにアクセスできるようにするために、内部クライアントの実 IP アドレスを、ソース アドレスとして使用できる外部アドレスに変換する規則を作成する必要があります。

  この作業を完了するには、内部 IP アドレスを適応型セキュリティ アプライアンスの外部 IP アドレスに変換する内部インターフェイス用の PAT 変換規則（ポート アドレス変換規則、インターフェイス NAT と呼ばれることもあります）を設定する必要があります。

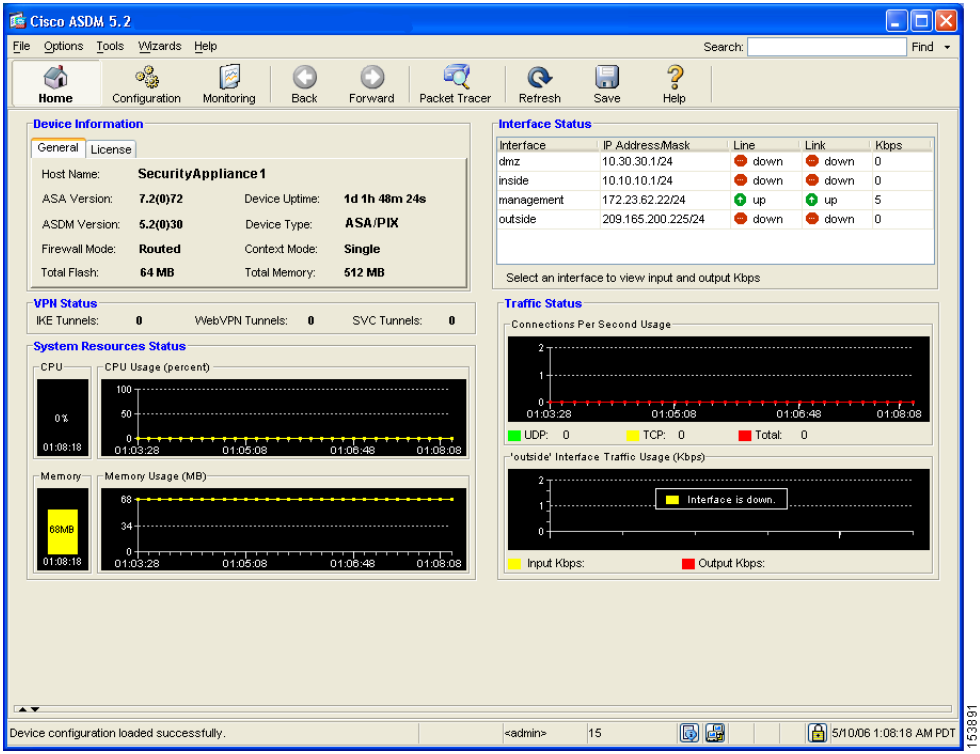
  このシナリオでは、変換される内部アドレスは、プライベート ネットワークのサブネットの内部アドレス（10.10.10.0）です。このサブネットからのアドレスは、適応型セキュリティ アプライアンスのパブリック アドレス（209.165.200.225）に変換されます。
- DMZ Web サーバへの HTTP アクセスを外部クライアントに提供するために、DMZ Web サーバの外部アイデンティティを設定し、またインターネット上のクライアントから発信される HTTP 要求を許可するアクセス規則を設定する必要があります。この作業を完了するには、次の要素を設定する必要があります。
  - 静的 NAT 規則を作成します。この規則は、DMZ Web サーバの実 IP アドレスを単一のパブリック IP アドレスに変換します。このシナリオでは、Web サーバのパブリック アドレスは 209.165.200.226 です。
  - セキュリティ アクセス規則を作成します。この規則は、インターネットからのトラフィックを許可します（DMZ Web サーバのパブリック IP アドレスに送信される HTTP 要求のトラフィックの場合）。

ASDM の起動

ASDM を Web ブラウザで実行するには、アドレス フィールドに、工場出荷時のデフォルト IP アドレス **https://192.168.1.1/admin/** を入力します。

（注） 「**s**」を追加して「**https**」にすることに注意してください。追加しないと、接続が失敗します。HTTPS（HTTP over SSL）は、ブラウザと適応型セキュリティ アプライアンスとの間でセキュアな接続を提供します。

ASDM のメイン ウィンドウが表示されます。



ネットワーク アドレス変換用の IP プールの作成

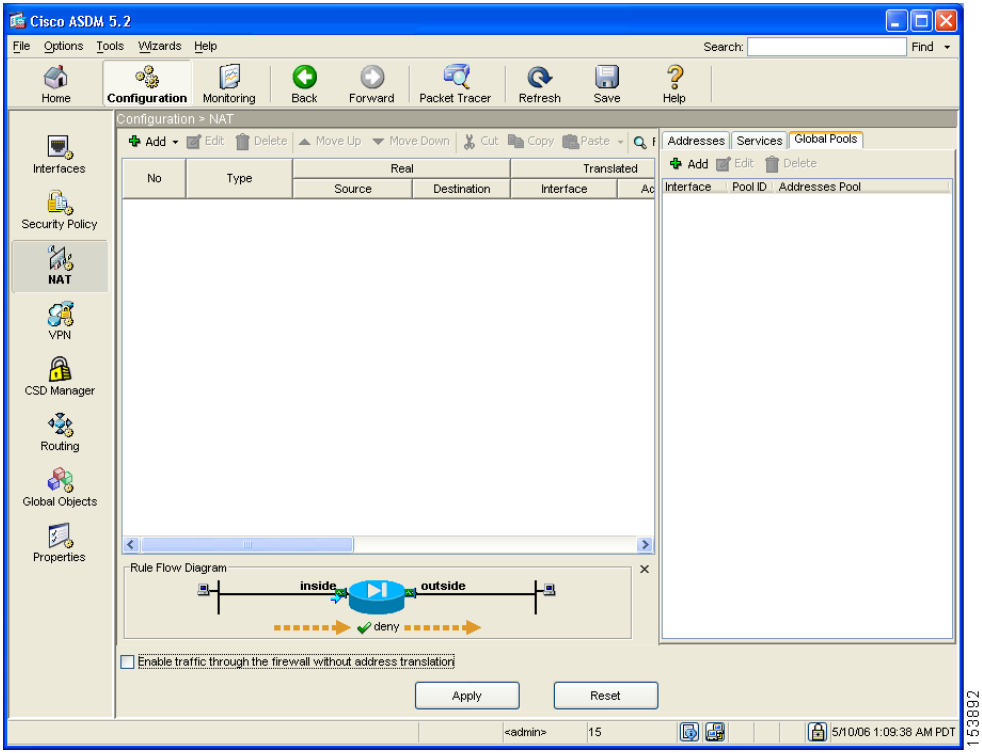
適応型セキュリティ アプライアンスは、ネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）を使用して、内部 IP アドレスが外部に公開されることを防いでいます。この手順では、DMZ インターフェイスおよび外部インターフェイスがアドレス変換に使用できる IP アドレスのプールの作成方法について説明します。

単一の IP プールに NAT と PAT の両方のエントリが含まれることがあり、また複数のインターフェイスのエントリが含まれることもあります。

ネットワーク アドレス変換に使用できる IP アドレスの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　ASDM ウィンドウで、**Configuration** ツールをクリックします。

a. Features ペインで、**NAT** をクリックします。
NAT Configuration 画面が表示されます。

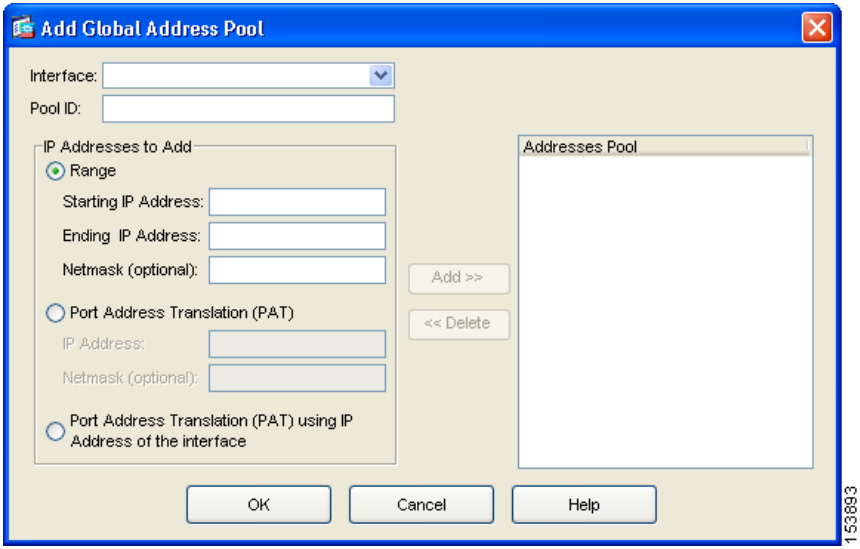


b. 右ペインで、**Global Pools** タブをクリックします。

c. **Add** をクリックして、DMZ インターフェイス用の新しいグローバル プールを作成します。

Add Global Address Pool ダイアログボックスが表示されます。

（注） ほとんどの設定で、IP プールはよりセキュアでない（パブリックな）インターフェイスに追加されます。



d. Interface ドロップダウン リストで、DMZ をクリックします。

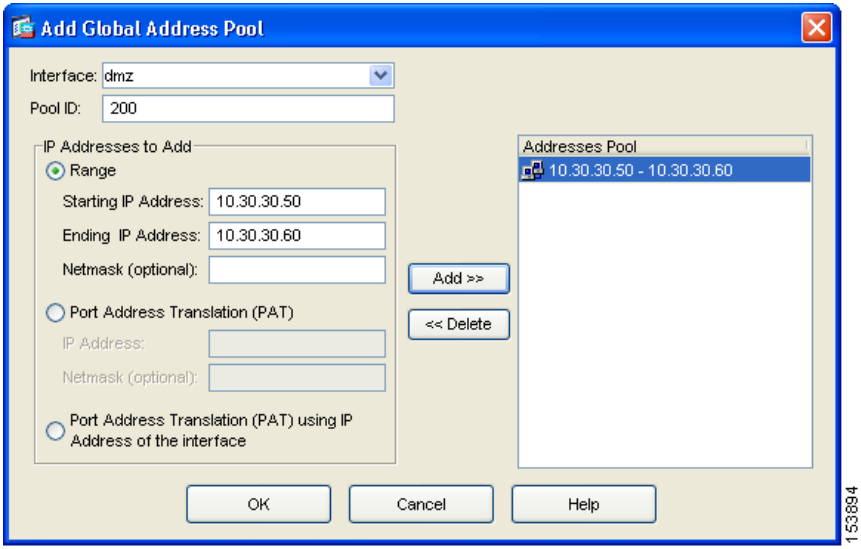
e. 新しい IP プールを作成するには、一意の Pool ID を入力します。このシナリオでは、Pool ID は 200 です。

f. IP Addresses to Add 領域で、DMZ インターフェイスで使用される IP アドレスの範囲を指定します。

- **Range** オプション ボタンをクリックします。
- IP アドレスの範囲の開始値と終了値を入力します。このシナリオでは、IP アドレスの範囲は 10.30.30.50 ～ 10.30.30.60 です。
- （オプション）IP アドレスの範囲のネットマスクを入力します。

g. **Add** をクリックして、この IP アドレスの範囲を Addresses Pool に追加します。

Add Global Pool ダイアログボックスの設定は、次のようになります。



h. **OK** をクリックして、Configuration > NAT ウィンドウに戻ります。

ステップ 2　外部インターフェイスで使用されるアドレスを IP プールに追加します。これらのアドレスはプライベート IP アドレスの変換に使用され、内部クライアントはインターネット上のクライアントとセキュアに通信できます。

このシナリオでは、使用可能なパブリック IP アドレスは制限されています。ポート アドレス変換（PAT）を使用して、次のように多数の内部 IP アドレスを同一のパブリック IP アドレスにマッピングできます。

a. NAT Configuration 画面の右ペインで、**Global Pools** タブをクリックします。

b. Global Pools タブで、**Add** をクリックします。

Add Global Pool Item ダイアログボックスが表示されます。

c. Interface ドロップダウン リストで、Outside を選択します。

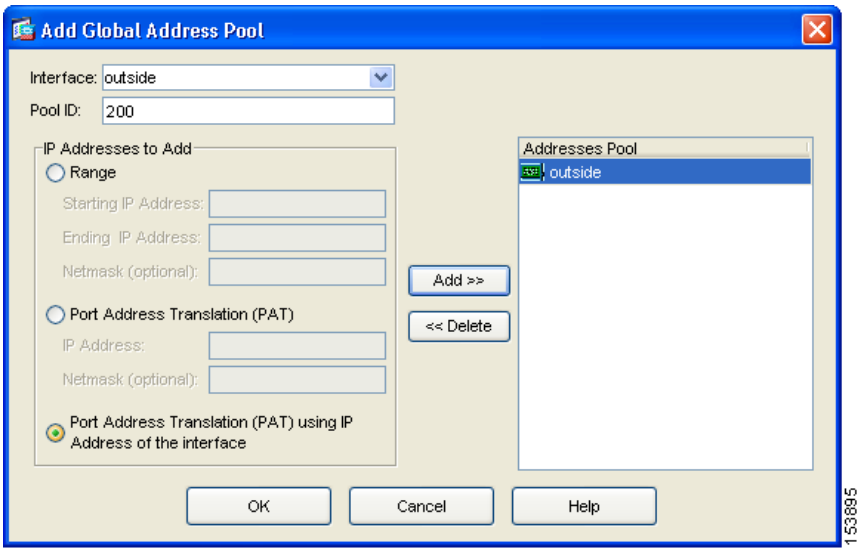
d. 外部インターフェイス用の Pool ID を指定します。

これらのアドレスは、DMZ インターフェイスで使用されるアドレス プールが含まれる同一の IP プールに追加できます（このシナリオでは、Pool ID は 200 です）。

e. **Port Address Translation (PAT) using IP address of the interface** オプション ボタンをクリックします。

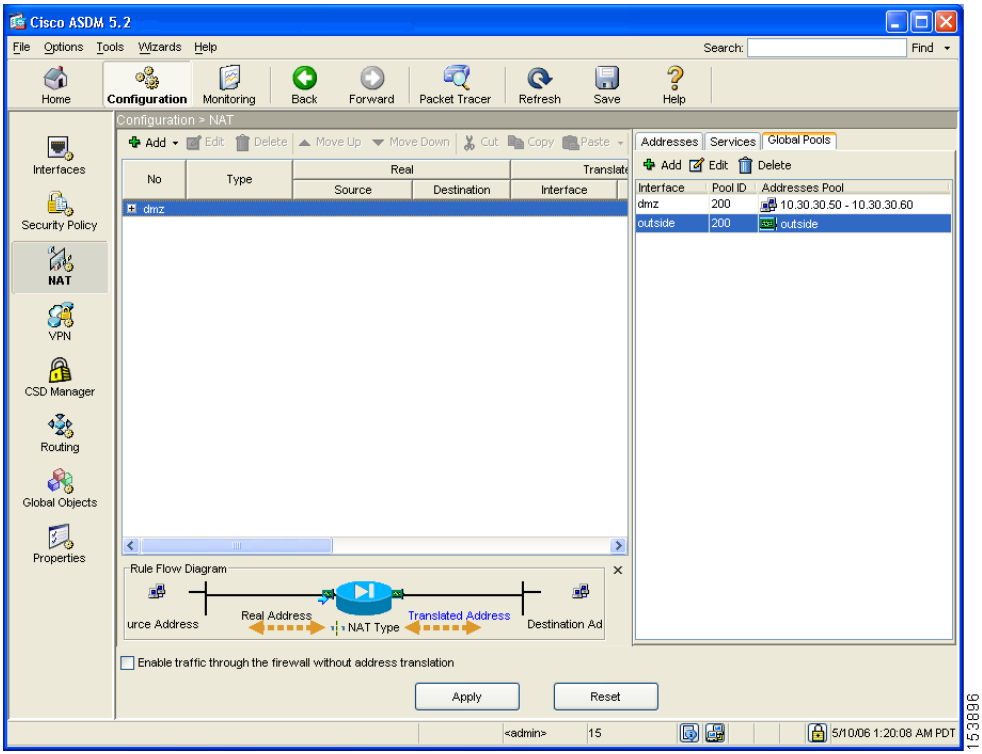
Port Address Translation (PAT) using IP address of the interface オプションを選択した場合、内部ネットワークから発信されたすべてのトラフィックは、外部インターフェイスの IP アドレスを使用して適応型セキュリティ アプライアンスから送出されます。インターネット上のデバイスでは、この 1 つの IP アドレスからすべてのトラフィックが発信されているように見えます。

f. **Add** ボタンをクリックして、この新しいアドレスを IP プールに追加します。



g. **OK** をクリックします。

表示される設定は、次のようになります。



ステップ 3　設定値が正しいことを確認します。

ステップ 4　ASDM のメイン ウィンドウで **Apply** をクリックします。

内部クライアントが DMZ Web サーバと通信するための NAT の設定

前述の手順では、適応型セキュリティ アプライアンスで使用できる IP アドレスのプールを作成して、内部クライアントのプライベート IP アドレスをマスクしました。

この手順では、内部クライアントが DMZ Web サーバとセキュアに通信できるように、このプールからの IP アドレスを内部クライアントに関連付けるネットワーク アドレス変換（NAT）規則を設定します。

内部インターフェイスと DMZ インターフェイスとの間で NAT を設定するには、ASDM のメイン ウィンドウから、次の手順を実行します。

ステップ 1　ASDM のメイン ウィンドウで、**Configuration** ツールをクリックします。

ステップ 2　Features ペインで、**NAT** をクリックします。

ステップ 3　Add ドロップダウン リストで、Add Dynamic NAT Rule を選択します。

Add Dynamic NAT Rule ダイアログボックスが表示されます。

ステップ 4　Real Address 領域で、変換する IP アドレスを指定します。このシナリオの場合、内部クライアントのアドレス変換はサブネットの IP アドレスに従って実行されます。

a. Interface ドロップダウン リストで、Inside インターフェイスを選択します。

b. クライアントまたはネットワークの IP アドレスを入力します。このシナリオでは、ネットワークの IP アドレスは 10.10.10.0 です。

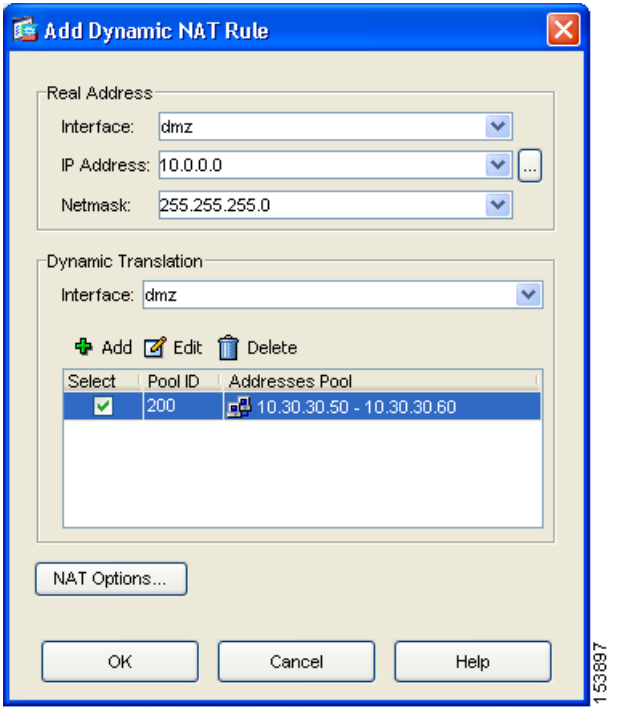
c. Netmask ドロップダウン リストで、ネットマスクを選択します。このシナリオでは、ネットマスクは 255.255.255.0 です。

ステップ 5　Dynamic Translation 領域で、次の手順を実行します。

a. Interface ドロップダウン リストで、DMZ インターフェイスを選択します。

b. この Dynamic NAT 規則に使用されるアドレス プールを指定するには、Global Pool ID の横にある **Select** チェックボックスをオンにします。このシナリオでは、IP プール ID は 200 です。

このシナリオでは、使用する IP プールはすでに作成されています。作成されていない場合は、**Add** をクリックして、新しい IP プールを作成します。



c. **OK** をクリックして Dynamic NAT Rule を追加し、Configuration > NAT ウィンドウに戻ります。

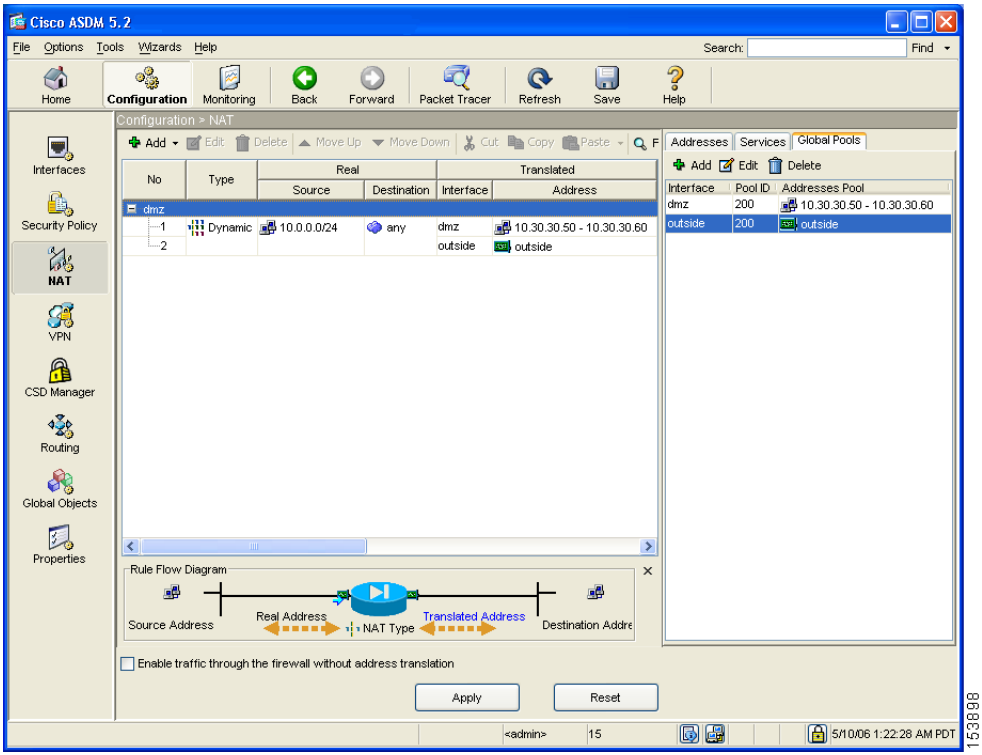
設定画面で、変換規則が予想どおりに表示されることを確認します。

（注） OK をクリックしてこの規則を作成すると、実際には次の 2 つの変換規則が作成されることに注意してください。

- 内部インターフェイスと DMZ インターフェイス間の変換規則。これは、内部クライアントが DMZ Web サーバと通信する際に使用されます。
- 内部インターフェイスと外部インターフェイス間の変換規則。これは、内部クライアントがインターネットと通信する際に使用されます。

変換に使用されるアドレスは両方とも同一の IP プールに存在するので、ASDM は両方の規則を作成できます。

表示される設定は、次のようになります。



ステップ 6　**Apply** をクリックして、適応型セキュリティ アプライアンスの設定変更を完了します。

内部クライアントがインターネット上のデバイスと通信するための NAT の設定

前述の手順では、内部クライアントが DMZ Web サーバとセキュアに通信できるように、IP プールからの IP アドレスを内部クライアントに関連付けるネットワーク アドレス変換（NAT）規則を設定しました。

多くの設定では、内部インターフェイスと外部インターフェイス間の NAT 規則を作成して、内部クライアントがインターネットと通信できるようにする必要もあります。

ただし、このシナリオでは、この規則を明示的に作成する必要はありません。その理由は、アドレス変換に必要な両方のタイプのアドレス（DMZ インターフェイスに使用される IP アドレスと外部インターフェイスに使用される IP アドレスの範囲）が IP プール（プール ID 200）に含まれているためです。したがって、2 番目の変換規則は、ユーザが明示的に作成する代わりに ASDM で作成できます。

DMZ Web サーバの外部アイデンティティの設定

DMZ Web サーバは、インターネット上のすべてのホストからアクセスできる必要があります。この設定では、DMZ Web サーバのプライベート IP アドレスをパブリック IP アドレスに変換して、適応型セキュリティ アプライアンスを認識していない外部 HTTP クライアントにアクセスできるようにする必要があります。Web サーバの実 IP アドレス（10.30.30.30）をパブリック IP アドレス（209.165.200.226）にスタティックにマッピングするには、次の手順を実行します。

ステップ 1　ASDM ウィンドウで、**Configuration** ツールをクリックします。

ステップ 2　Features ペインで、**NAT** をクリックします。

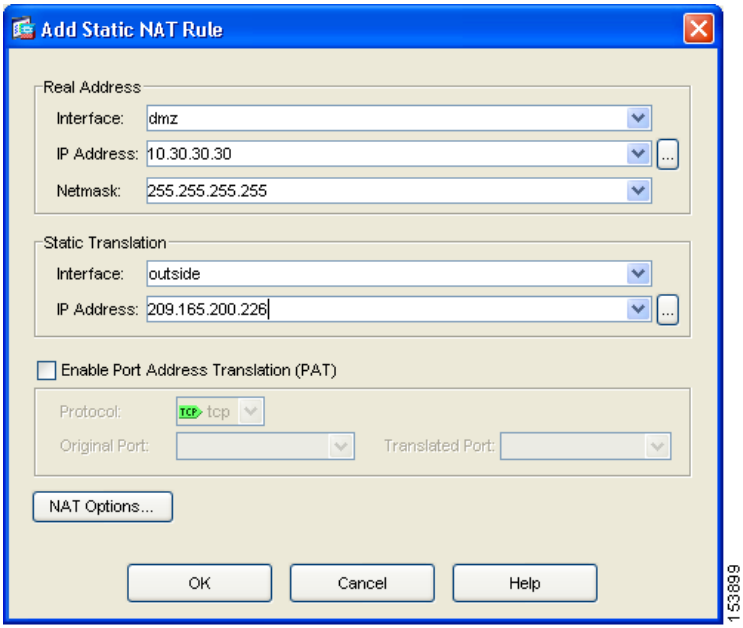
ステップ 3　Add ドロップダウン リストで、Add Static NAT Rule を選択します。Add Static NAT Rule ダイアログボックスが表示されます。

ステップ 4　Real Address 領域で、次のように Web サーバの実 IP アドレスを指定します。

a. Interface ドロップダウン リストで、DMZ インターフェイスを選択します。

b. DMZ Web サーバの実 IP アドレスを入力します。このシナリオでは、IP アドレスは 10.30.30.30 です。

c. Netmask ドロップダウン リストで、ネットマスク 255.255.255.255 を選択します。



ステップ 5　Static Translation 領域で、次のように Web サーバに使用されるパブリック IP アドレスを指定します。

a. Interface ドロップダウン リストで、Outside を選択します。

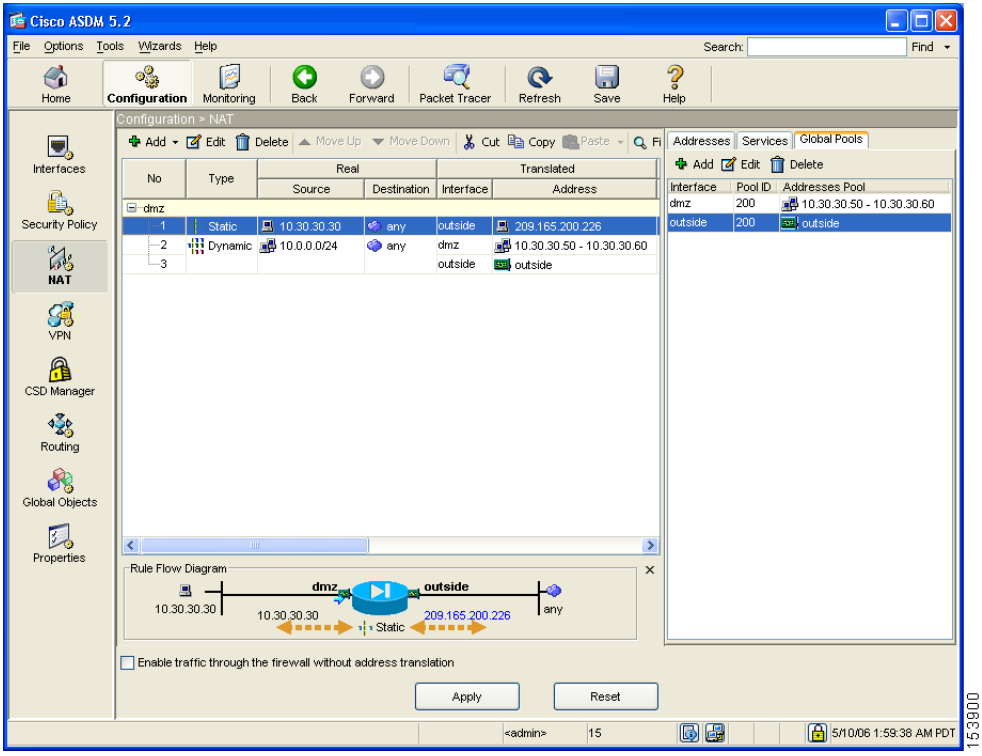
b. IP Address ドロップダウン リストで、DMZ Web サーバのパブリック IP アドレスを選択します。

このシナリオでは、DMZ Web サーバのパブリック IP アドレスは 209.165.200.226 です。

ステップ 6　**OK** をクリックして規則を追加し、Address Translation Rules のリストに戻ります。

この規則は、Web サーバの実 IP アドレス（10.30.30.30）を Web サーバのパブリック IP アドレス（209.165.200.226）にスタティックにマッピングします。

表示される設定は、次のようになります。



ステップ 7　**Apply** をクリックして、適応型セキュリティ アプライアンスの設定変更を完了します。

DMZ Web サーバへのパブリック HTTP アクセスの提供

デフォルトでは、適応型セキュリティ アプライアンスはパブリック ネットワークから発信されたすべてのトラフィックを拒否します。適応型セキュリティ アプライアンスでアクセス コントロール規則を作成して、パブリック ネットワークからの特定の種類のトラフィックが DMZ のリソースに到達できるようにする必要があります。このアクセス コントロール規則には、トラフィックを処理する適応型セキュリティ アプライアンスのインターフェイス、トラフィックが着信か発信かの区別、トラフィックの発信元と宛先、および許可されるトラフィックのプロトコルとサービスの種類を指定します。

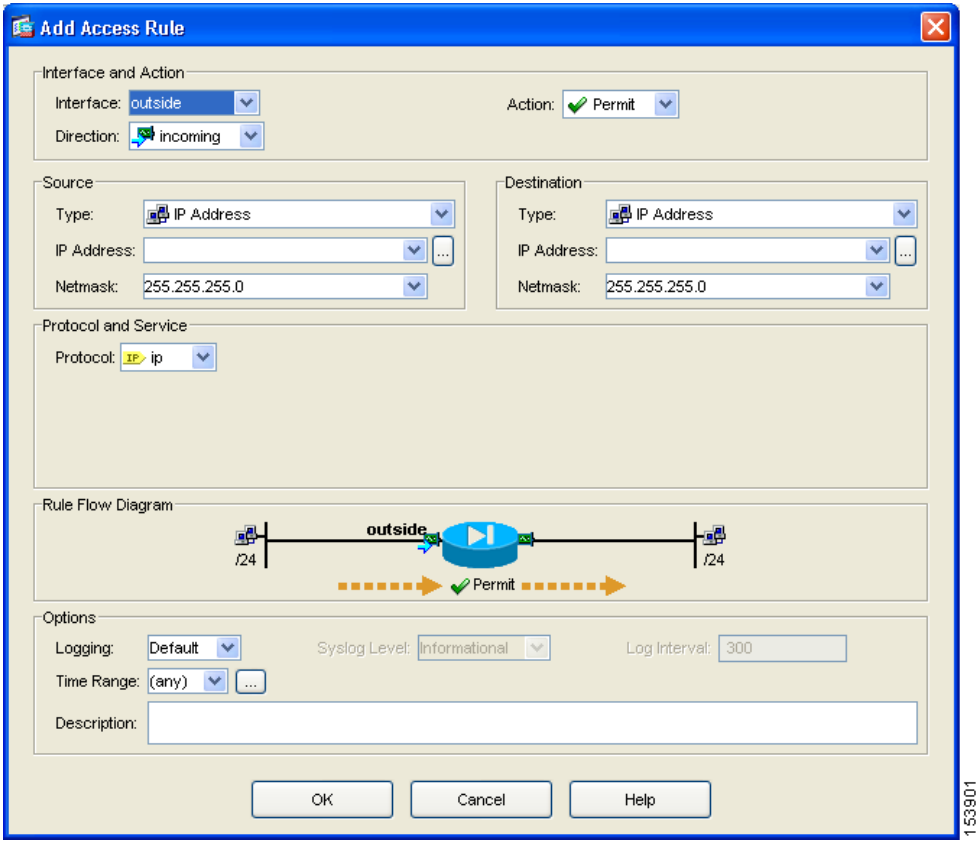
この項では、トラフィックの宛先が DMZ ネットワークの場合に、インターネット上のホストまたはネットワークから発信される着信 HTTP トラフィックを許可するアクセス規則を作成します。パブリック ネットワークから発信されるその他のトラフィックはすべて拒否されます。

アクセス コントロール規則を設定するには、次の手順を実行します。

ステップ 1　ASDM ウィンドウで、次の手順を実行します。

a. **Configuration** ツールをクリックします。
b. Features ペインで、**Security Policy** をクリックします。
c. **Access Rules** タブをクリックし、Add プルダウン リストで Add Access Rule を選択します。

   Add Access Rule ダイアログボックスが表示されます。



ステップ 2　Interface and Action 領域で、次の手順を実行します。

a. Interface ドロップダウン リストで、Outside を選択します。
b. Direction ドロップダウン リストで、Incoming を選択します。
c. Action ドロップダウン リストで、Permit を選択します。

ステップ 3　Source 領域で、次の手順を実行します。

a. Type ドロップダウン リストで、IP Address を選択します。

b. 発信元ホストまたは発信元ネットワークの IP アドレスを入力します（すべてのホストまたはネットワークから発信されたトラフィックを許可するには、0.0.0.0 を使用します）。

あるいは、発信元ホストまたは発信元ネットワークのアドレスが事前設定済みの場合は、IP Address ドロプダウン リストで発信元 IP アドレスを選択します。

c. 発信元 IP アドレスのネットマスクを入力するか、または Netmask ドロップダウン リストで 1 つ選択します。

ステップ 4　Destination 領域で、次の手順を実行します。

a. IP address フィールドに、宛先ホストまたは宛先ネットワーク（Web サーバなど）のパブリック IP アドレスを入力します（このシナリオでは、DMZ Web サーバのパブリック IP アドレスは 209.165.200.226 です）。

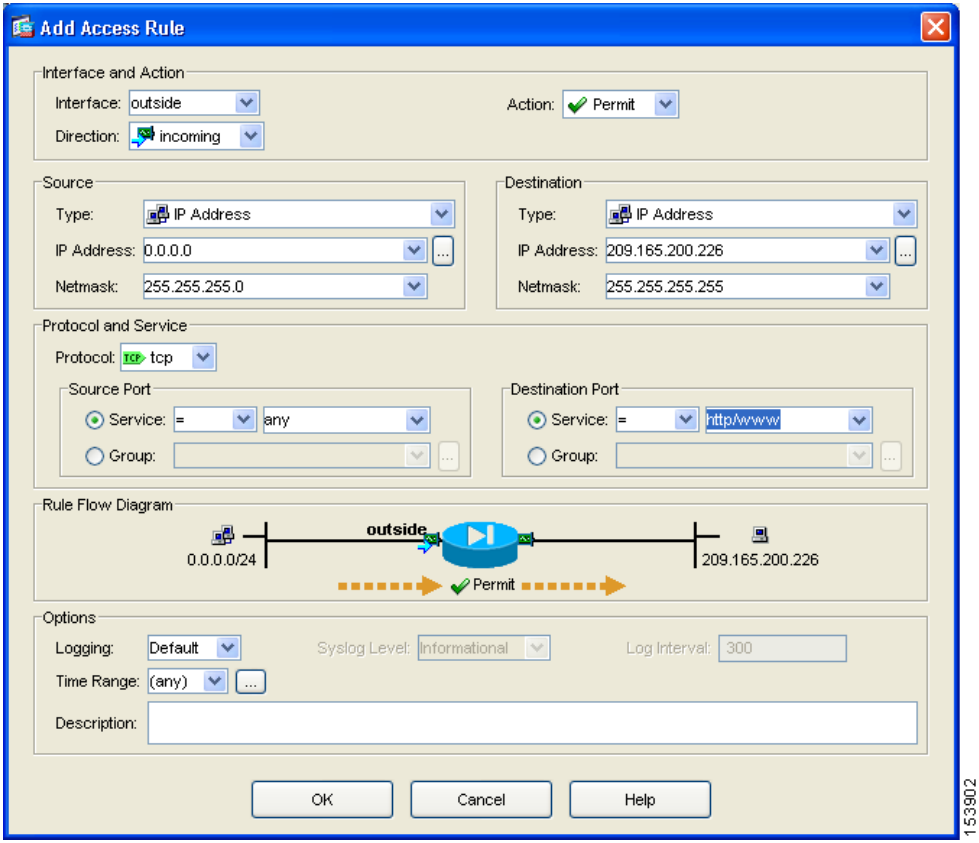
ステップ 5　Protocol and Service 領域で、適応型セキュリティ アプライアンスで許可するトラフィックの種類を指定します。

a. Protocol ドロップダウン リストで、tcp を選択します。

b. Source Port 領域で、**Service** オプション ボタンをクリックし、Service ドロップダウン リストで「=」（等号）を選択し、次のドロップダウン リストで Any を選択します。

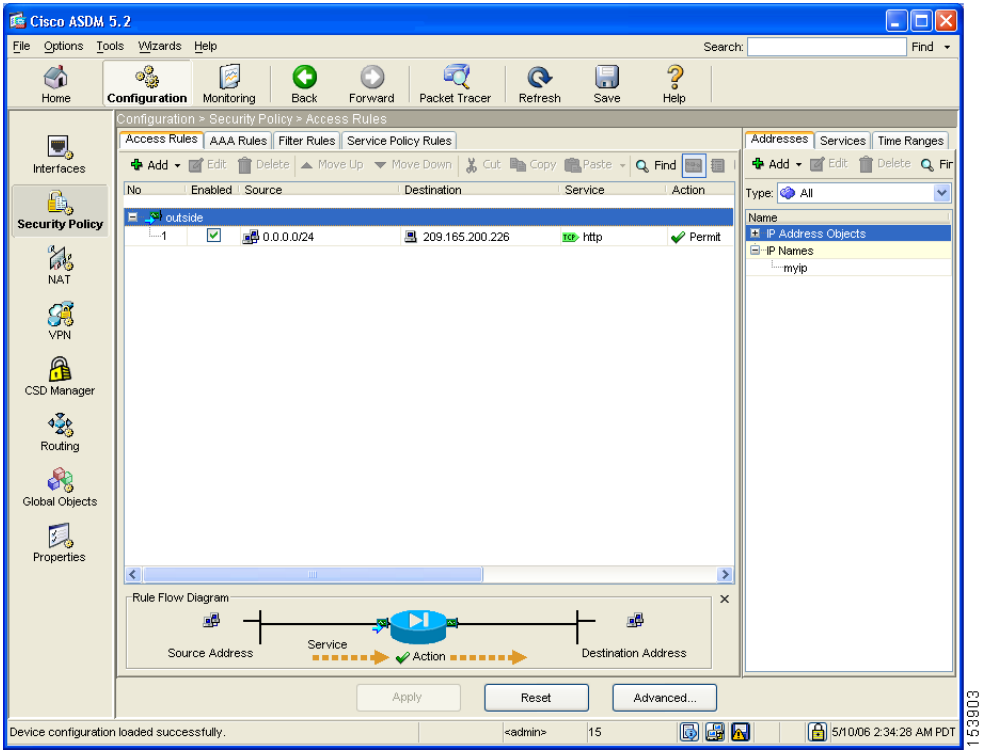
c. Destination Port 領域で、**Service** オプション ボタンをクリックし、Service ドロップダウン リストで「=」（等号）を選択し、次のドロップダウン リストで HTTP/WWW を選択します。

この時点で、Add Access Rule ダイアログボックスのエントリは、次のようになります。



d. **OK** をクリックします。

ステップ 6　表示される設定は、次のようになります。入力した情報が正しいことを確認します。



ステップ 7　**Apply** をクリックして、適応型セキュリティ アプライアンスが現在実行中の設定変更を保存します。

これで、プライベート ネットワークおよびパブリック ネットワークのどちらのクライアントも、プライベート ネットワークをセキュアな状態に保ちながら、DMZ Web サーバからのコンテントに対する HTTP 要求を解決できます。

（注）　指定された宛先アドレスは DMZ Web サーバのプライベート アドレス（10.30.30.30）ですが、パブリック アドレス 209.165.200.226 に送信されたインターネット上のすべてのホストからの HTTP トラフィックが、適応型セキュリティ アプライアンスを通過できます。209.165.200.226 から 10.30.30.30 へのアドレス変換によって、トラフィックが許可されます。変換規則の作成方法の詳細については、P.6-14 の「内部クライアントが DMZ Web サーバと通信するための NAT の設定」を参照してください。

ステップ 8　次回のデバイス起動時に変更が適用されるように、設定変更をスタートアップ設定に保存する場合は、File メニューで **Save** をクリックします。

あるいは、ASDM の終了時に設定変更の保存を要求するプロンプトが表示されます。

設定変更を保存しない場合は、次回のデバイス起動時に以前の設定が有効になります。

次の手順

DMZ 内の Web サーバを保護する目的で適応型セキュリティ アプライアンスを配置するだけの場合は、これで初期設定は終わりです。次の追加の手順について、実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のオペレーションの学習	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	*Cisco ASA 5500 Series Hardware Installation Guide*

適応型セキュリティ アプライアンスは、複数のアプリケーション用に設定できます。次の項で、その他の一般的なアプリケーション用に適応型セキュリティ アプライアンスを設定する手順を説明します。

作業内容	参照先
リモートアクセス VPN の設定	第 7 章「シナリオ：リモートアクセス VPN の設定」
サイトツーサイト VPN の設定	第 8 章「シナリオ：サイトツーサイト VPN の設定」

シナリオ：リモートアクセス VPN の設定

この章では、適応型セキュリティ アプライアンスを使用して、リモートアクセス IPsec VPN 接続を受け付ける方法について説明します。リモートアクセス VPN を使用すると、インターネットを経由するセキュアな接続（トンネル）を作成できるため、セキュアなアクセスをオフサイト ユーザに提供できます。

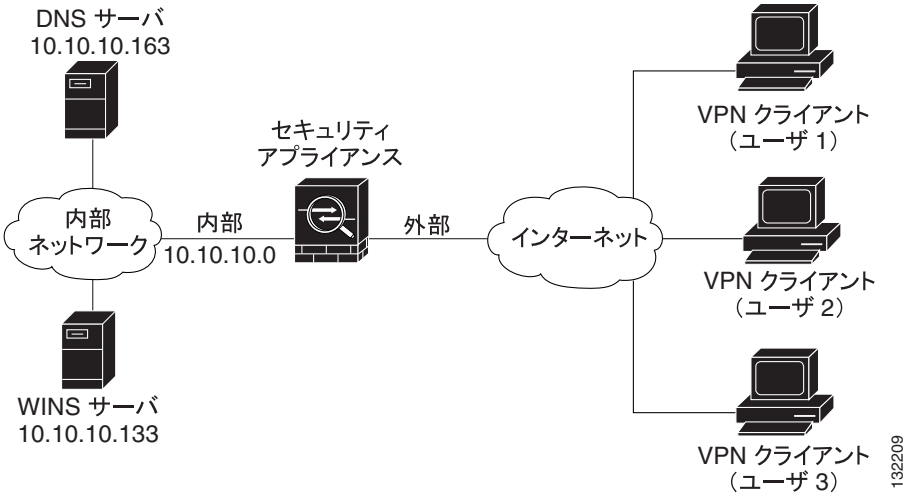
この章では、Easy VPN ソリューションを実装する場合に Easy VPN サーバ（ヘッドエンド デバイスと呼ばれることもあります）を設定する方法について説明します。

この章は、次の項で構成されています。

IPsec リモートアクセス VPN ネットワーク トポロジの例

図 7-1 は、インターネット経由で VPN クライアント（Cisco Easy VPN ハードウェア クライアントなど）からの要求を受け付け、それらのクライアントとの IPsec 接続を確立するように設定された適応型セキュリティ アプライアンスを示しています。

図 7-1　　リモート アクセス VPN のシナリオのネットワーク レイアウト



IPsec リモートアクセス VPN のシナリオの実装

この章では、適応型セキュリティ アプライアンスを設定して、リモート クライアントおよびリモート デバイスから IPsec VPN 接続を受け付ける方法について説明します。この項では、Easy VPN ソリューションを実装する場合に Easy VPN サーバ（ヘッドエンド デバイスと呼ばれることもあります）を設定する方法について説明します。

設定値の例は、図 7-1 で示すリモートアクセスのシナリオから取得されます。

この項では、次のトピックについて取り上げます。

必要な情報

適応型セキュリティ アプライアンスの設定を開始してリモート アクセス IPsec VPN 接続を受け付けるには、事前に必ず次の情報を準備します。

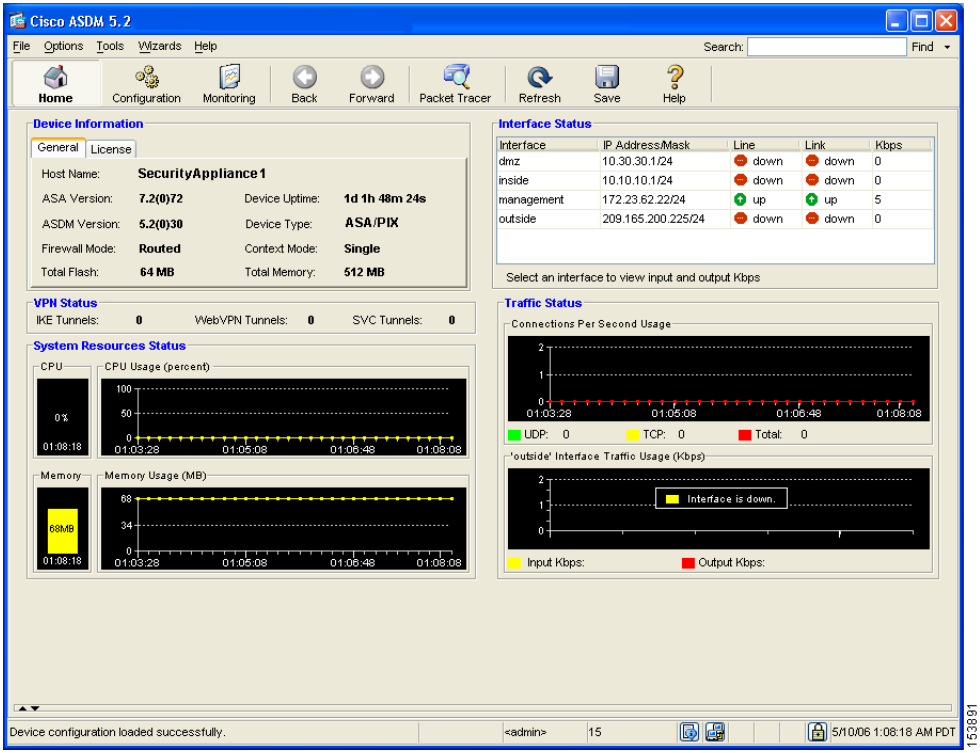
- IP プールで使用される IP アドレスの範囲。これらのアドレスは、接続が成功するとリモート VPN クライアントに割り当てられます。
- ローカル認証データベースの作成に使用されるユーザのリスト（認証に AAA サーバを使用する場合を除く）。
- VPN への接続時にリモート クライアントで使用されるネットワーキング情報。次の情報が含まれます。
  - プライマリおよびセカンダリ DNS サーバの IP アドレス
  - プライマリおよびセカンダリ WINS サーバの IP アドレス
  - デフォルト ドメイン名
  - 認証されたリモート　クライアントにアクセスできるようにするローカル ホスト、グループ、およびネットワークの IP アドレスのリスト

ASDM の起動

ASDM を Web ブラウザで実行するには、アドレス フィールドに、工場出荷時のデフォルト IP アドレス **https://192.168.1.1/admin/** を入力します。

（注） 「**s**」を追加して「**https**」にすることに注意してください。追加しないと、接続が失敗します。HTTPS（HTTP over SSL）は、ブラウザと適応型セキュリティ アプライアンスとの間でセキュアな接続を提供します。

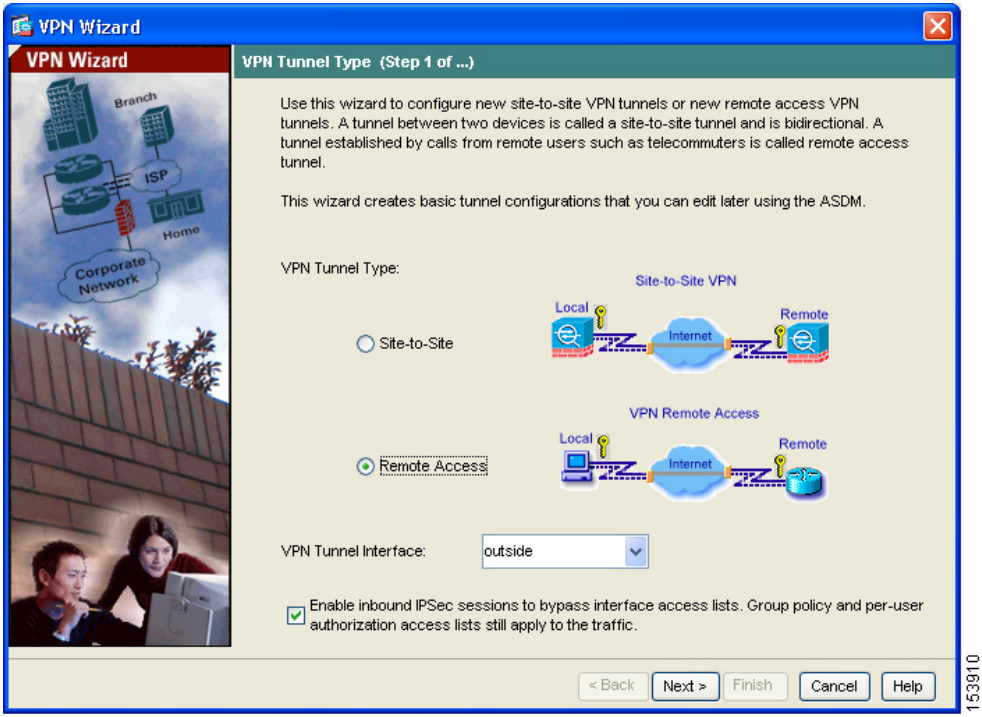
ASDM のメイン ウィンドウが表示されます。


Cisco ASDM 5.2
File Options Tools Wizards Help
Search:
Find
Home
Configuration
Monitoring
Back
Forward
Packet Tracer
Refresh
Save
Help
Device Information
General
License
Host Name: SecurityAppliance1
ASA Version: 7.2(0)72
Device Uptime: 1d 1h 48m 24s
ASDM Version: 5.2(0)30
Device Type: ASA/PIX
Firewall Mode: Routed
Context Mode: Single
Total Flash: 64 MB
Total Memory: 512 MB
Interface Status
Interface IP Address/Mask Line Link Kbps
dmz 10.30.30.1/24 down down 0
inside 10.10.10.1/24 down down 0
management 172.23.62.22/24 up up 5
outside 209.165.200.225/24 down down 0
Select an interface to view input and output Kbps
VPN Status
IKE Tunnels: 0
WebVPN Tunnels: 0
SVC Tunnels: 0
Traffic Status
Connections Per Second Usage
UDP: 0
TCP: 0
Total: 0
'outside' Interface Traffic Usage (Kbps)
Interface is down.
Input Kbps:
Output Kbps:
System Resources Status
CPU
CPU Usage (percent)
Memory
Memory Usage (MB)
Device configuration loaded successfully.
<admin>
15
5/10/06 1:08:18 AM PDT
153891

IPsec リモートアクセス VPN 用の FWSM の設定

リモートアクセス VPN の設定プロセスを開始するには、次の手順を実行します。

ステップ 1　ASDM のメイン ウィンドウの Wizards ドロップダウン メニューで、**VPN Wizard** を選択します。VPN Wizard の Step 1 画面が表示されます。



ステップ 2　VPN Wizard の Step 1 で、次の手順を実行します。

a. **Remote Access VPN** オプション ボタンをクリックします。

b. ドロップダウン リストで、着信 VPN トンネルに対してイネーブルにするインターフェイスとして Outside を選択します。

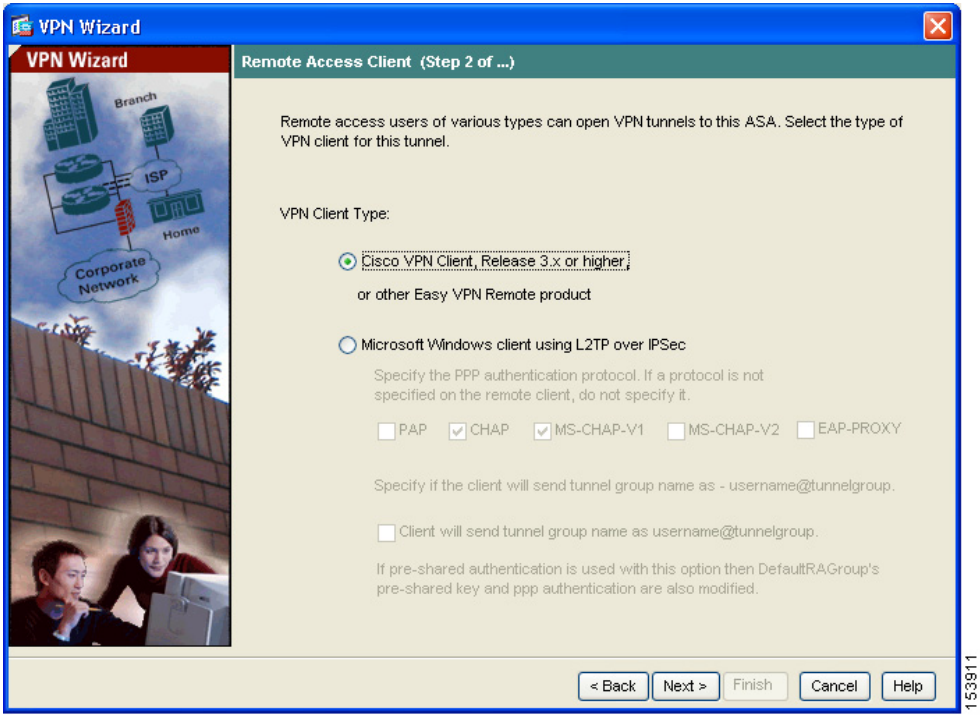
c. **Next** をクリックして続行します。

VPN クライアント タイプの選択

VPN Wizard の Step 2 で、次の手順を実行します。

ステップ 1　この適応型セキュリティ アプライアンスにリモート ユーザが接続できる VPN クライアントのタイプを指定します。このシナリオでは、**Cisco VPN Client** オプション ボタンをクリックします。

その他の Cisco Easy VPN リモート製品もすべて使用することができます。



ステップ 2　**Next** をクリックして続行します。

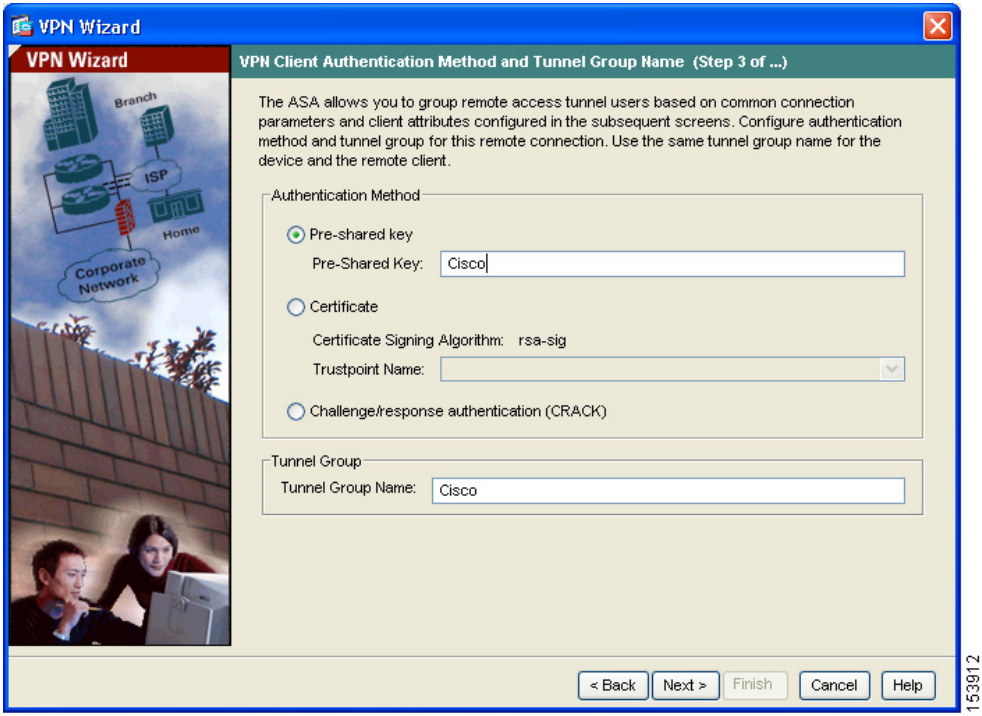
VPN トンネル グループ名と認証方式の指定

VPN Wizard の Step 3 で、次の手順を実行します。

ステップ 1　次の手順のいずれかを実行して、使用する認証の種類を指定します。

- 認証にスタティックな事前共有キーを使用するには、**Pre-Shared key** オプション ボタンをクリックし、事前共有キー（「Cisco」など）を入力します。このキーは、適応型セキュリティ アプライアンス間の IPsec ネゴシエーションに使用されます。
- 認証にデジタル証明書を使用するには、**Certificate** オプション ボタンをクリックし、ドロップダウン リストで Certificate Signing Algorithm を選択し、次のドロップダウン リストで事前設定されたトラストポイント名を選択します。

  認証にデジタル署名を使用する場合でも、トラストポイント名をまだ設定していないときは、他の 2 つのオプションのいずれかを使用して Wizard を続行できます。標準の ASDM 画面を使用して、後で認証設定を変更できます。
- **Challenge/response authentication (CRACK)** オプション ボタンをクリックして、その認証方式を使用します。



ステップ 2　共通の接続パラメータとクライアント アトリビュートを使用するユーザのセットに対してトンネル グループ名（「Cisco」など）を入力して、この適応型セキュリティ アプライアンスに接続します。

ステップ 3　**Next** をクリックして続行します。

ユーザ認証方式の指定

ユーザは、ローカル認証データベース、または外部認証、認可、アカウンティング（AAA）サーバ（RADIUS、TACACS+、SDI、NT、Kerberos、および LDAP）で認証できます。

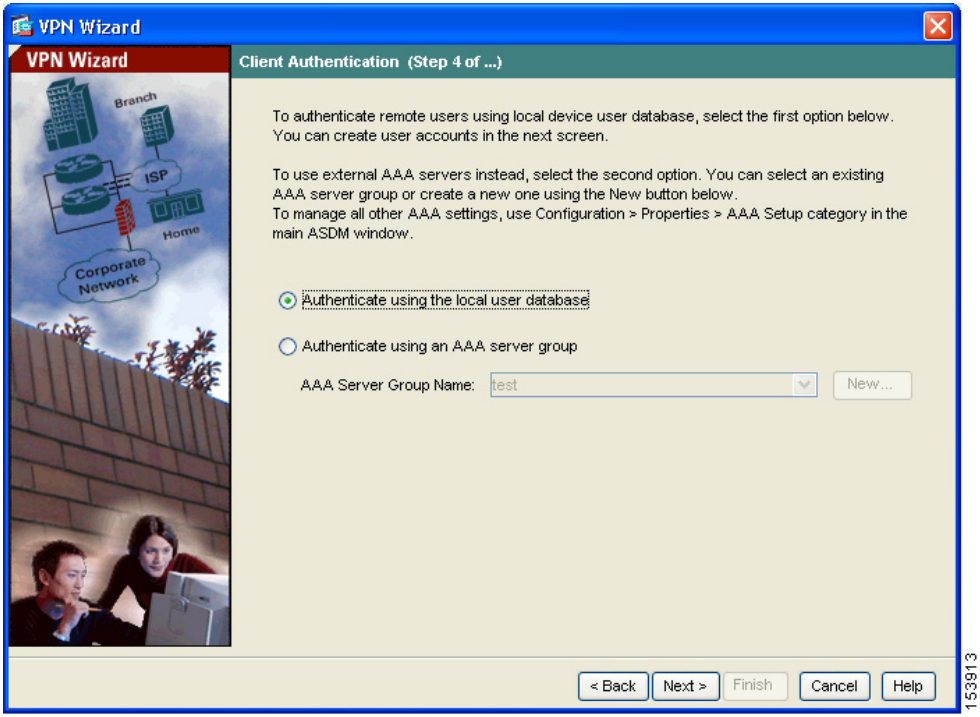
VPN Wizard の Step 4 で、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスにユーザ データベースを作成してユーザを認証する場合は、**Authenticate using the local user database** オプション ボタンをクリックします。

ステップ 2　外部 AAA サーバ グループでユーザを認証する場合は、次の手順を実行します。

a. **Authenticate using an AAA server group** オプション ボタンをクリックします。

b. ドロップダウン リストで、事前設定済みのサーバ グループを選択します。または、**New** をクリックして、新しいサーバ グループを追加します。



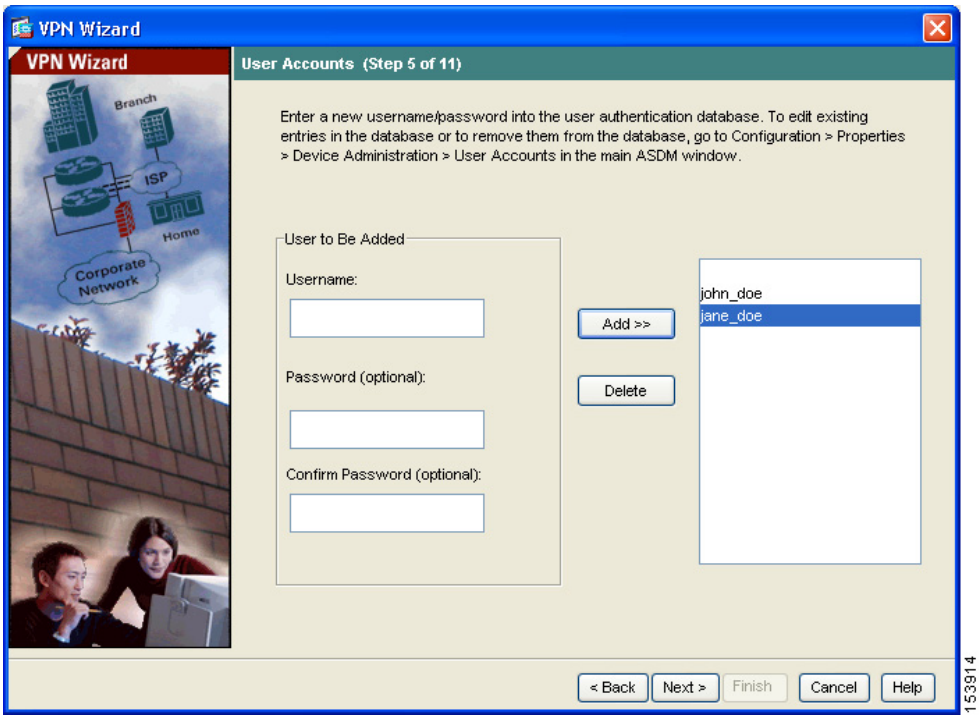
ステップ 3　**Next** をクリックして続行します。

（オプション）ユーザ アカウントの設定

ローカル ユーザ データベースでユーザを認証する場合は、ここで新しいユーザ アカウントを作成できます。ASDM 設定インターフェイスを使用して、後でユーザを追加することもできます。

VPN Wizard の Step 5 で、次の手順を実行します。

ステップ 1　新しいユーザを追加するには、ユーザ名とパスワードを入力し、**Add** をクリックします。



ステップ 2　新しいユーザの追加が終了したら、**Next** をクリックして続行します。

アドレス プールの設定

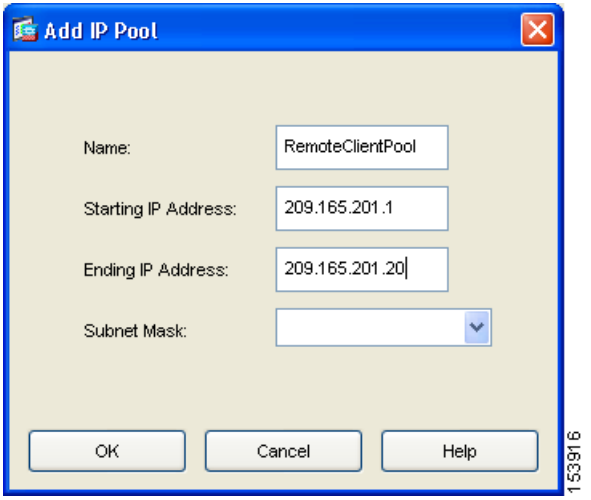
リモート クライアントがネットワークにアクセスできるようにするには、正常に接続したときにリモート VPN クライアントに割り当てることができる IP アドレスのプールを設定する必要があります。このシナリオでは、IP アドレス 209.165.201.1 ～ 209.166.201.20 を使用するようにプールを設定します。

VPN Wizard の Step 6 で、次の手順を実行します。

ステップ 1　ドロップダウン リストで、プール名を入力するか、事前設定済みのプールを選択します。

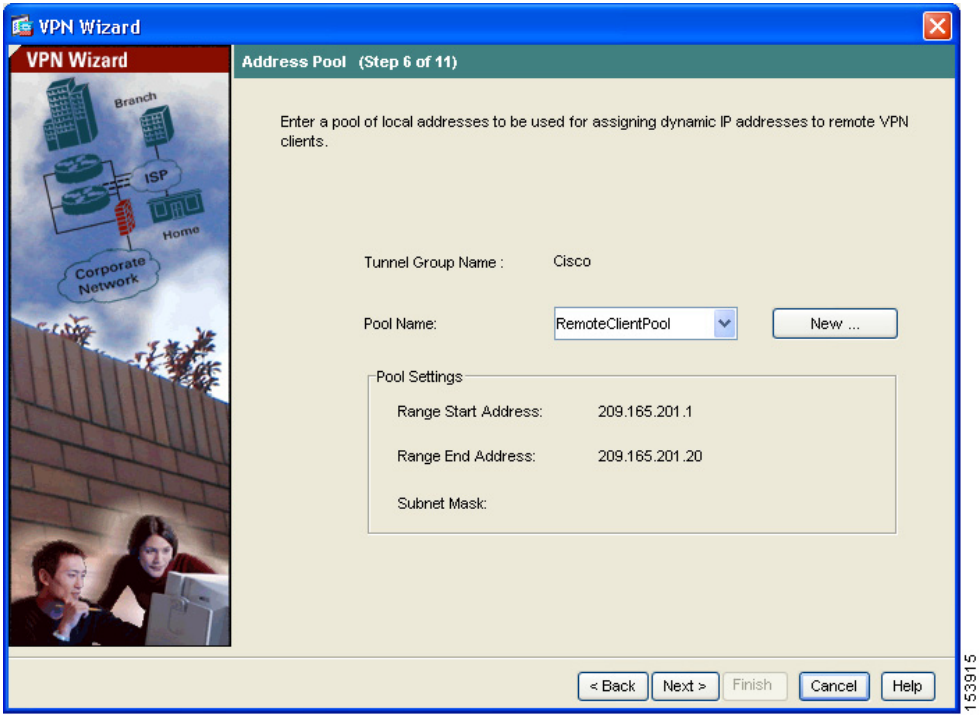
あるいは、**New** をクリックして、新しいアドレス プールを作成します。

Add IP Pool ダイアログボックスが表示されます。



ステップ 2　Add IP Pool ダイアログボックスで、次の手順を実行します。

a. IP アドレスの範囲の開始値と終了値を入力します。
b. （オプション）IP アドレスの範囲のネットマスクを入力します。
c. **OK** をクリックして、VPN Wizard の Step 6 に戻ります。



ステップ 3　**Next** をクリックして続行します。

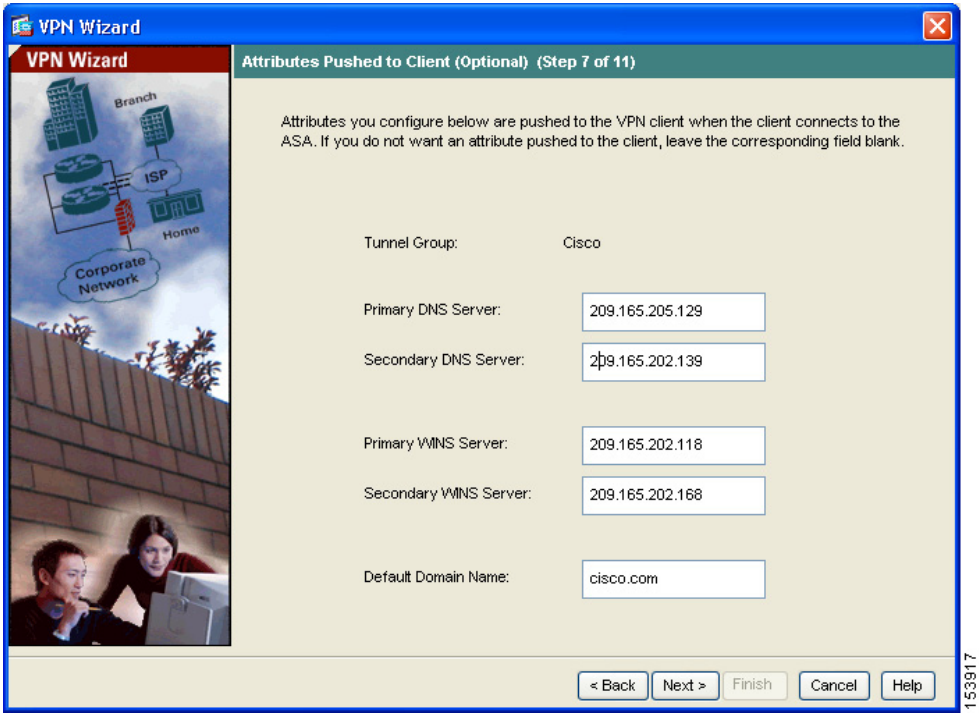
クライアント アトリビュートの設定

ネットワークにアクセスするには、各リモート アクセス クライアントに基本ネットワーク設定情報（使用する DNS サーバおよび WINS サーバ、デフォルト ドメイン名など）が必要です。各リモート クライアントを個別に設定する代わりに、ASDM にクライアント情報を入力できます。適応型セキュリティ アプライアンスは、接続が確立されたときに、この情報をリモート クライアントまたは Easy VPN ハードウェア クライアントにプッシュします。

正しい値を指定したことを確認してください。値が正しくない場合、リモート クライアントは、DNS 名を使用した解決や Windows ネットワーキングの使用ができなくなります。

VPN Wizard の Step 7 で、次の手順を実行します。

ステップ 1　リモート クライアントにプッシュするネットワーク設定情報を入力します。



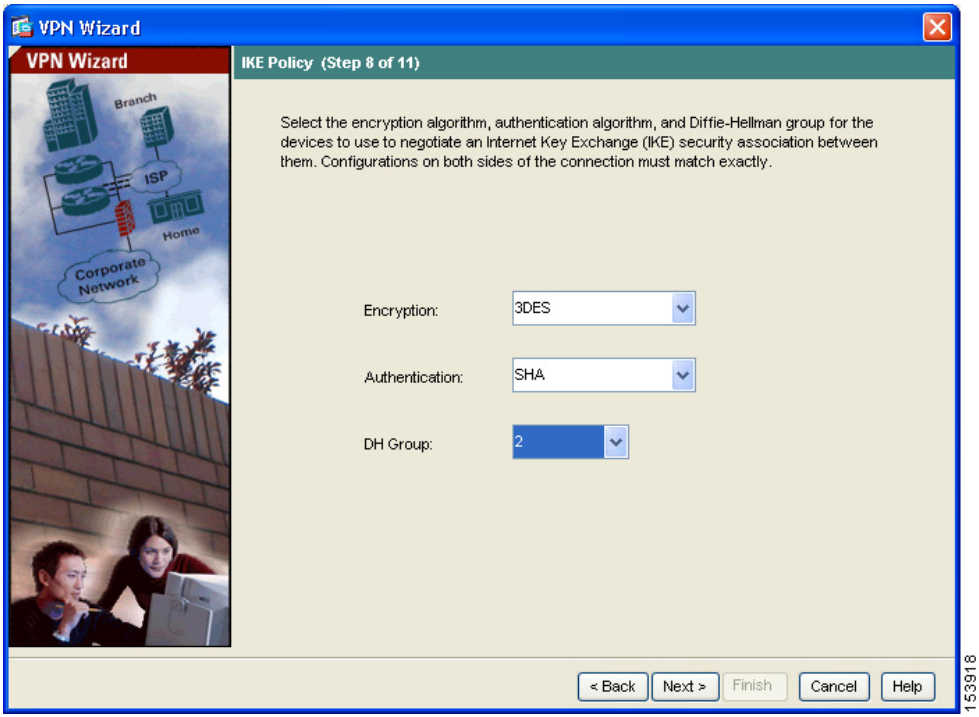
ステップ 2　**Next** をクリックして続行します。

IKE ポリシーの設定

IKE は、暗号化方式を含むネゴシエーション プロトコルで、データを保護し、機密性を保証します。また、ピアのアイデンティティも保証する認証方式でもあります。ほとんどの場合、ASDM のデフォルト値で、セキュアな VPN トンネルを確立できます。

VPN Wizard の Step 8 で IKE ポリシーを指定するには、次の手順を実行します。

ステップ 1　IKE セキュリティ アソシエーションで、適応型セキュリティ アプライアンスが使用する暗号化アルゴリズム（DES、3DES、または AES）、認証アルゴリズム（MD5 または SHA）、および Diffie-Hellman グループ（1、2、5、または 7）をクリックします。

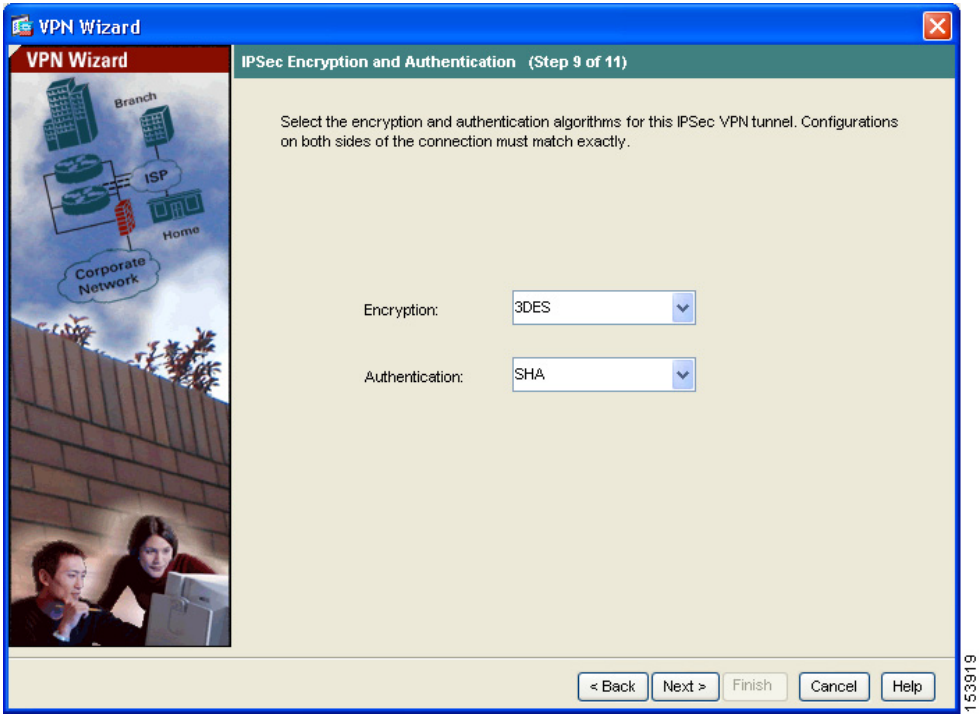


ステップ 2　**Next** をクリックして続行します。

IPsec 暗号化および認証パラメータの設定

VPN Wizard の Step 9 で、次の手順を実行します。

ステップ 1　暗号化アルゴリズム（DES、3DES、または AES）および認証アルゴリズム（MD5 または SHA）をクリックします。



ステップ 2　**Next** をクリックして続行します。

アドレス変換の例外とスプリット トンネリングの指定

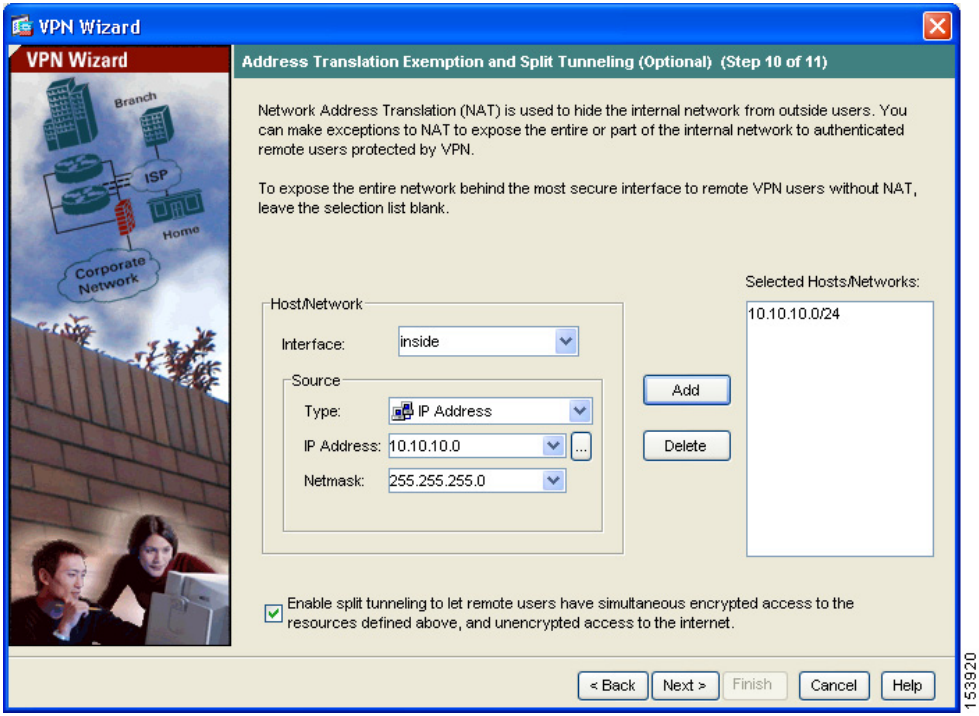
スプリット トンネリングを使用すると、リモートアクセス IPsec クライアントは一定の条件に従い、パケットを暗号化形式で IPsec トンネルに誘導したり、クリア テキスト形式でネットワーク インターフェイスに誘導したりすることができます。

適応型セキュリティ アプライアンスは、ネットワーク アドレス変換（NAT）を使用して、内部 IP アドレスが外部に公開されることを防いでいます。認証されたリモート ユーザにアクセスできるようにする必要があるローカル ホストおよびネットワークを指定して、このネットワーク保護の例外を作成できます（このシナリオでは、内部ネットワーク 10.10.10.0 全体をすべてのリモート クライアントに公開します）。

VPN Wizard の Step 10 で、次の手順を実行します。

ステップ 1　認証されたリモート ユーザがアクセスできるようにする内部リソースのリストに含めるホスト、グループ、およびネットワークを指定します。

Selected Hosts/Networks ペインのホスト、グループ、およびネットワークを動的に追加または削除するには、それぞれ、**Add** または **Delete** をクリックします。

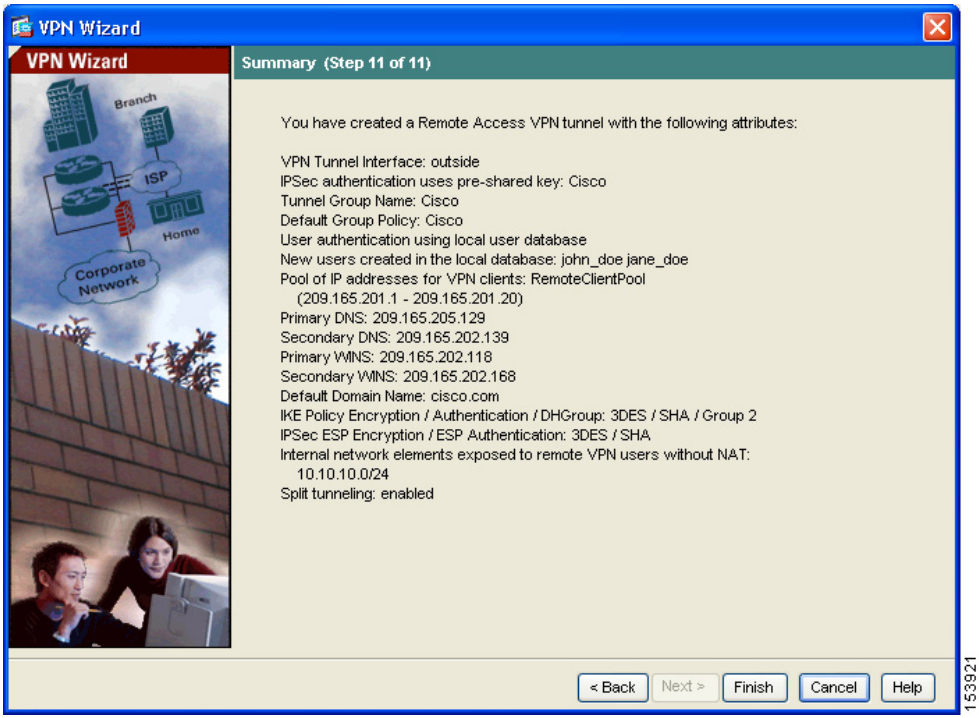


（注）　画面の下部にある **Enable split tunneling** チェックボックスをオンして、スプリット トンネリングをイネーブルにします。スプリット トンネリングを使用すると、設定したネットワークの外部のトラフィックを、暗号化された VPN トンネルを使用せずに直接インターネットに送出できるようになります。

ステップ 2　**Next** をクリックして続行します。

リモートアクセス VPN の設定の確認

VPN Wizard の Step 11 で、ここで作成した VPN トンネルの設定アトリビュートを確認します。表示される設定は、次のようになります。



設定が正しいことを確認したら、**Finish** をクリックして、変更を適応型セキュリティ アプライアンスに適用します。

次回のデバイス起動時に変更が適用されるように、設定変更をスタートアップ設定に保存する場合は、File メニューで **Save** をクリックします。あるいは、ASDM の終了時に設定変更の保存を要求するプロンプトが表示されます。

設定変更を保存しない場合は、次回のデバイス起動時に以前の設定が有効になります。

次の手順

リモートアクセス VPN 環境に適応型セキュリティ アプライアンスを配置するだけの場合は、これで初期設定は終わりです。このほかに、次の手順について、実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のオペレーションの学習	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	*Cisco ASA 5500 Series Hardware Installation Guide*

適応型セキュリティ アプライアンスは、複数のアプリケーション用に設定できます。次の項で、その他の一般的なアプリケーション用に適応型セキュリティ アプライアンスを設定する手順を説明します。

作業内容	参照先
DMZ 内の Web サーバを保護する適応型セキュリティ アプライアンスの設定	第 6 章「シナリオ：DMZ の設定」
サイトツーサイト VPN の設定	第 8 章「シナリオ：サイトツーサイト VPN の設定」

CHAPTER 8

シナリオ：サイトツーサイト VPN の設定

この章では、適応型セキュリティ アプライアンスを使用して、サイトツーサイト VPN を作成する方法について説明します。

適応型セキュリティ アプライアンスが提供するサイトツーサイト VPN 機能を使用すると、ネットワーク セキュリティを維持しながら、低コストな公衆インターネット接続で、ビジネス ネットワークを世界中のビジネス パートナー、およびリモート オフィスに拡張できます。VPN 接続を使用すると、あるロケーションから別のロケーションに、セキュアな接続（トンネル）でデータを送信できます。まず、接続の両端が認証され、次に、2 つのサイト間で送信されるすべてのデータが自動的に暗号化されます。

この章は、次の項で構成されています。

サイトツーサイト VPN ネットワーク トポロジの例

図 8-1 で、2 つの適応型セキュリティ アプライアンス間の VPN トンネルの例を示します。

図 8-1　サイトツーサイト VPN の設定シナリオのネットワーク レイアウト

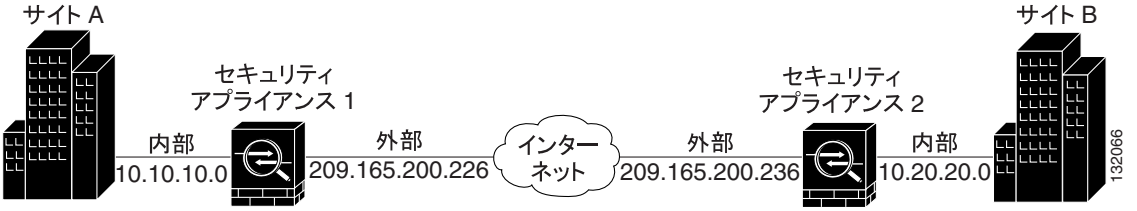


図 8-1 で示すような VPN サイトツーサイト配置の作成では、接続のそれぞれの端で 1 つずつ、合計 2 つの適応型セキュリティ アプライアンスを設定する必要があります。

サイトツーサイトのシナリオの実装

次の項で、図 8-1 で示したリモートアクセスのシナリオのパラメータ例を使用して、サイトツーサイト VPN 配置で適応型セキュリティ アプライアンスを設定する方法を示します。

この項では、次のトピックについて取り上げます。

必要な情報

この設定手順を開始する前に、次の情報を収集します。

- リモート適応型セキュリティ アプライアンス ピアの IP アドレス
- トンネルを使用してリモート サイトのリソースと通信できるローカル ホストおよびネットワークの IP アドレス
- トンネルを使用してローカル リソースと通信できるリモート ホストおよびネットワークの IP アドレス

サイトツーサイト VPN の設定

この項では、ASDM VPN Wizard を使用して、サイトツーサイト VPN の適応型セキュリティ アプライアンスを設定する方法について説明します。

この項では、次のトピックについて取り上げます。

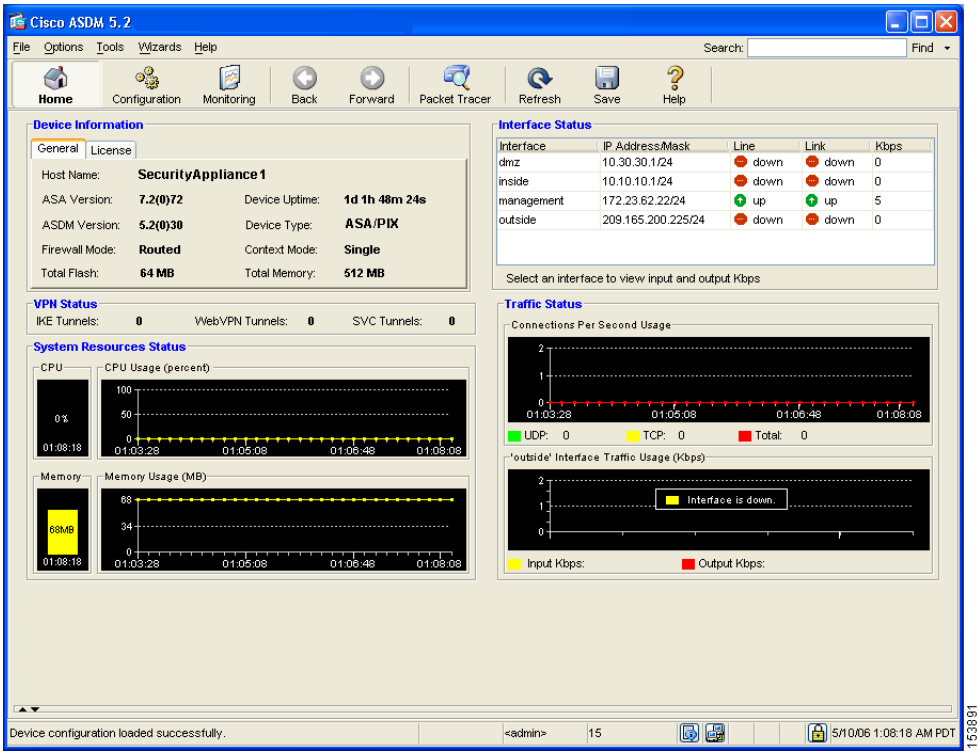
次の各項で、それぞれの設定手順を実行する方法について詳しく説明します。

ASDM の起動

ASDM を Web ブラウザで実行するには、アドレス フィールドに、工場出荷時のデフォルト IP アドレス **https://192.168.1.1/admin/** を入力します。

（注） 「**s**」を追加して「**https**」にすることに注意してください。追加しないと、接続が失敗します。HTTPS（HTTP over SSL）は、ブラウザと適応型セキュリティ アプライアンスとの間でセキュアな接続を提供します。

ASDM のメイン ウィンドウが表示されます。



ローカル サイトでのセキュリティ アプライアンスの設定

（注）　以後、最初のサイトの適応型セキュリティ アプライアンスをセキュリティ アプライアンス 1 と呼びます。

セキュリティ アプライアンス 1 を設定するには、次の手順を実行します。

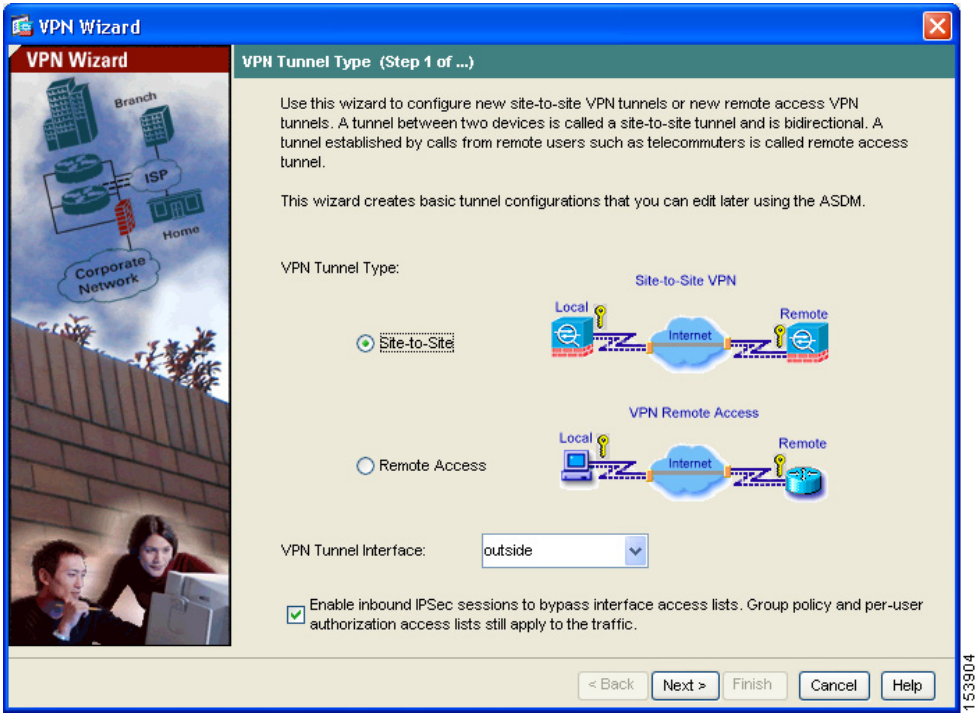
ステップ 1　ASDM のメイン ウィンドウの Wizards ドロップダウン メニューで、VPN Wizard オプションを選択します。最初の VPN Wizard 画面が表示されます。

VPN Wizard の Step 1 で、次の手順を実行します。

a. **Site-to-Site VPN** オプション ボタンをクリックします。

（注）　Site-to-Site VPN オプションは、2 つの IPSec セキュリティ ゲートウェイを接続します。これには、適応型セキュリティ アプライアンス、VPN コンセントレータ、またはサイトツーサイト IPSec 接続をサポートするその他のデバイスが含まれます。

b. ドロップダウン リストで、現在の VPN トンネルに対してイネーブルにするインターフェイスとして Outside を選択します。



c. **Next** をクリックして続行します。

リモート VPN ピアに関する情報の入力

VPN ピアは、設定している接続の反対側にあるシステムで、通常、リモート サイトにあります。

（注） このシナリオでは、以後、リモート VPN ピアをセキュリティ アプライアンス 2 と呼びます。

VPN Wizard の Step 2 で、次の手順を実行します。

ステップ 1　ピア IP アドレス（セキュリティ アプライアンス 2 の IP アドレスで、このシナリオでは 209.165.200.236）およびトンネル グループ名（「Cisco」など）を入力します。

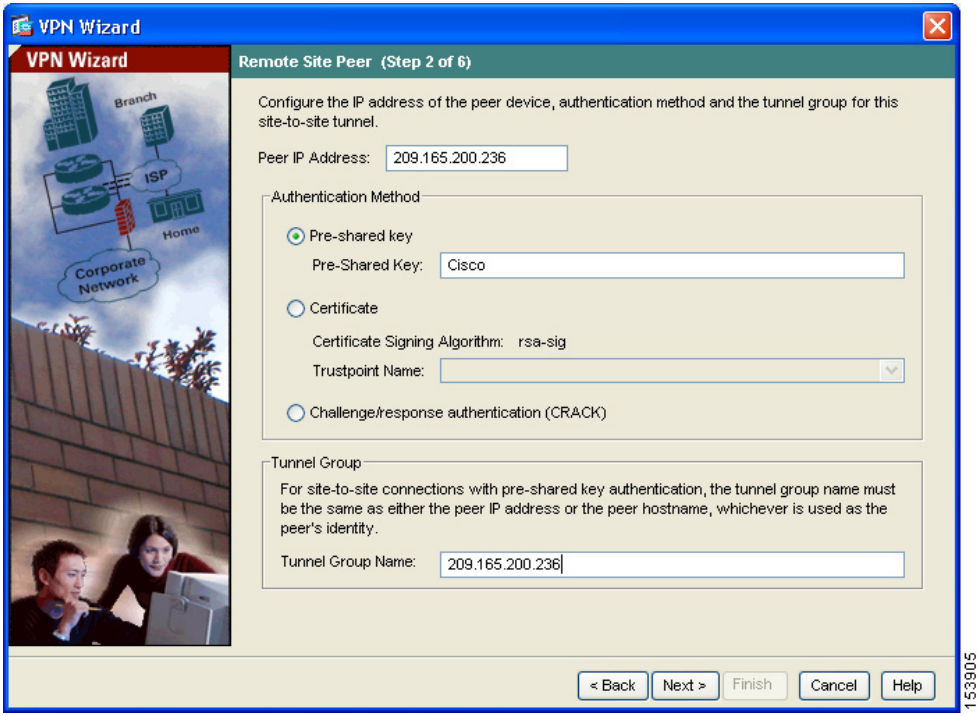
ステップ 2　次の手順のいずれかを実行して、使用する認証の種類を指定します。

- 認証にスタティックな事前共有キーを使用するには、**Pre-Shared key** オプション ボタンをクリックし、事前共有キー（「Cisco」など）を入力します。このキーは、適応型セキュリティ アプライアンス間の IPsec ネゴシエーションに使用されます。

  （注） リモート サイトでセキュリティ アプライアンス 2 を設定するとき、VPN ピアはセキュリティ アプライアンス 1 になります。ここで使用するものと同じ事前共有キー（Cisco）を入力してください。

- **Challenge/response authentication** オプション ボタンをクリックして、その認証方式を使用します。
- 認証にデジタル証明書を使用するには、**Certificate** オプション ボタンをクリックし、ドロップダウン リストで Certificate Signing Algorithm を選択し、次のドロップダウン リストで事前設定されたトラストポイント名を選択します。

  認証にデジタル署名を使用する場合でも、トラストポイント名をまだ設定していないときは、他の 2 つのオプションのいずれかを使用して Wizard を続行できます。標準の ASDM 画面を使用して、後で認証設定を変更できます。



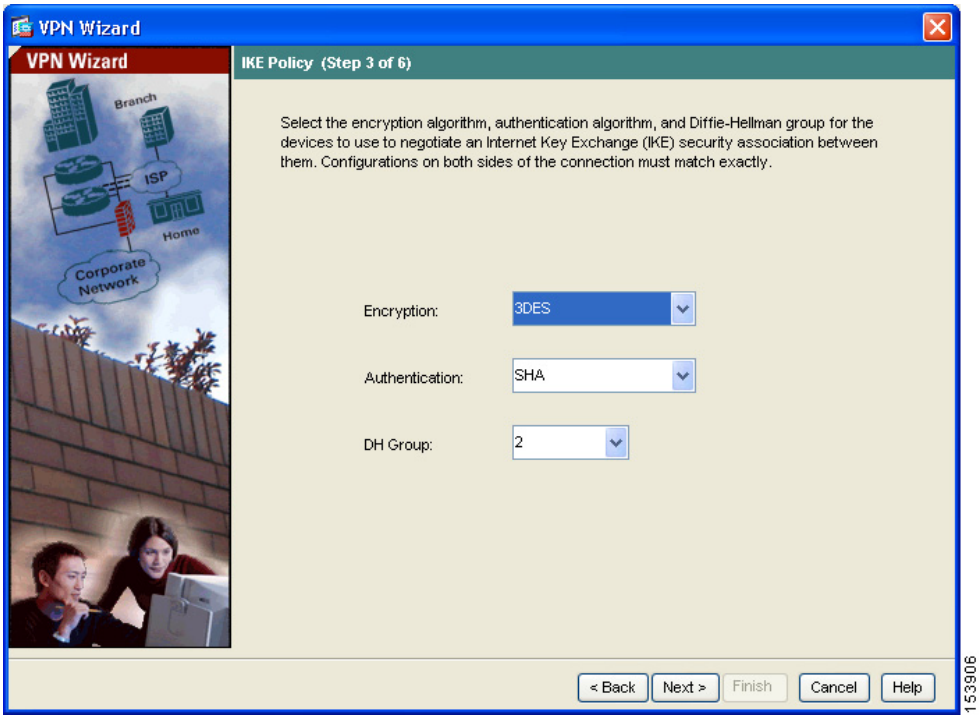
ステップ 3　**Next** をクリックして続行します。

IKE ポリシーの設定

IKE は、暗号化方式を含むネゴシエーション プロトコルで、データを保護し、機密性を保証します。また、ピアのアイデンティティも保証する認証方式でもあります。ほとんどの場合、ASDM のデフォルト値で、2 つのピア間でセキュアな VPN トンネルを確立できます。

VPN Wizard の Step 3 で、次の手順を実行します。

ステップ 1　IKE セキュリティ アソシエーションで、適応型セキュリティ アプライアンスが使用する暗号化アルゴリズム（DES、3DES、または AES）、認証アルゴリズム（MD5 または SHA）、および Diffie-Hellman グループ（1、2、または 5）をクリックします。



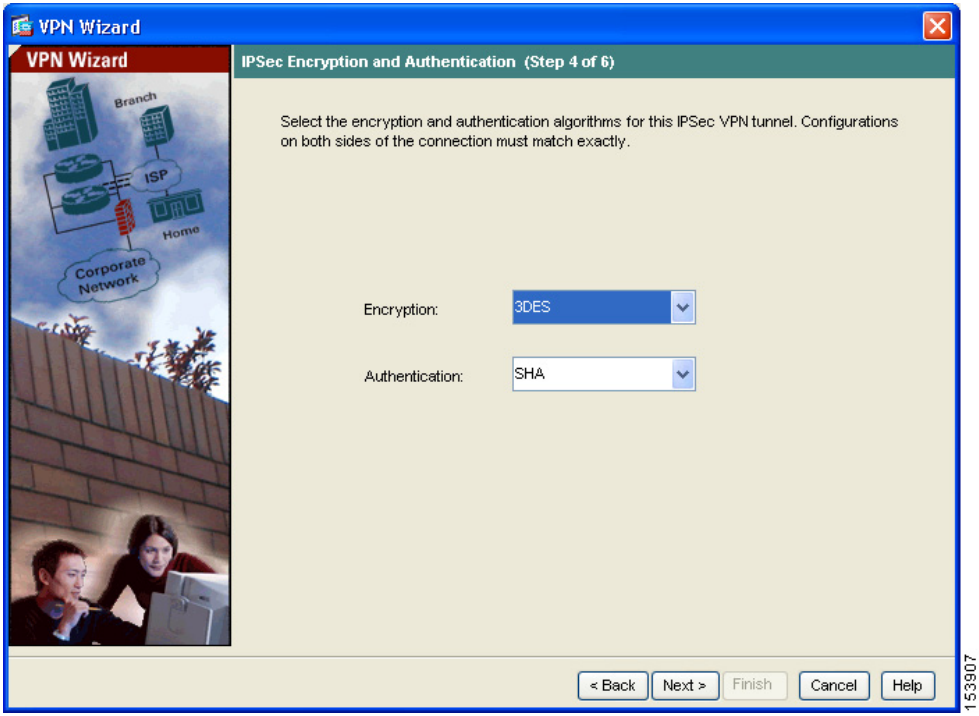
（注） セキュリティ アプライアンス 2 を設定するときは、セキュリティ アプライアンス 1 で選択した各オプションの値を正確に入力する必要があります。暗号化の不一致は、VPN トンネル障害のよくある原因で、設定プロセスを遅らせる原因になります。

ステップ 2　**Next** をクリックして続行します。

IPSec 暗号化および認証パラメータの設定

VPN Wizard の Step 4 で、次の手順を実行します。

ステップ 1　ドロップダウン リストで、暗号化アルゴリズム（DES、3DES、または AES）および認証アルゴリズム（MD5 または SHA）を選択します。



ステップ 2　**Next** をクリックして続行します。

ホストおよびネットワークの指定

この IPSec トンネルを使用してリモートサイト ピアと通信できるローカル サイトのホストおよびネットワークを指定します。ホストおよびネットワークを動的に追加または削除するには、それぞれ、**Add** または **Delete** をクリックします。現在のシナリオでは、Network A（10.10.10.0）からのトラフィックはセキュリティ アプライアンス 1 で暗号化され、VPN トンネルを使用して送信されます。

また、この IPSec トンネルを使用してローカル ホストとネットワークにアクセスできるリモート サイトのホストおよびネットワークを指定します。ホストおよびネットワークを動的に追加または削除するには、それぞれ、**Add** または **Delete** をクリックします。このシナリオでは、セキュリティ アプライアンス 1 のリモート ネットワークは Network B（10.20.20.0）なので、このネットワークからの暗号化されたトラフィックは、トンネルを使用できます。

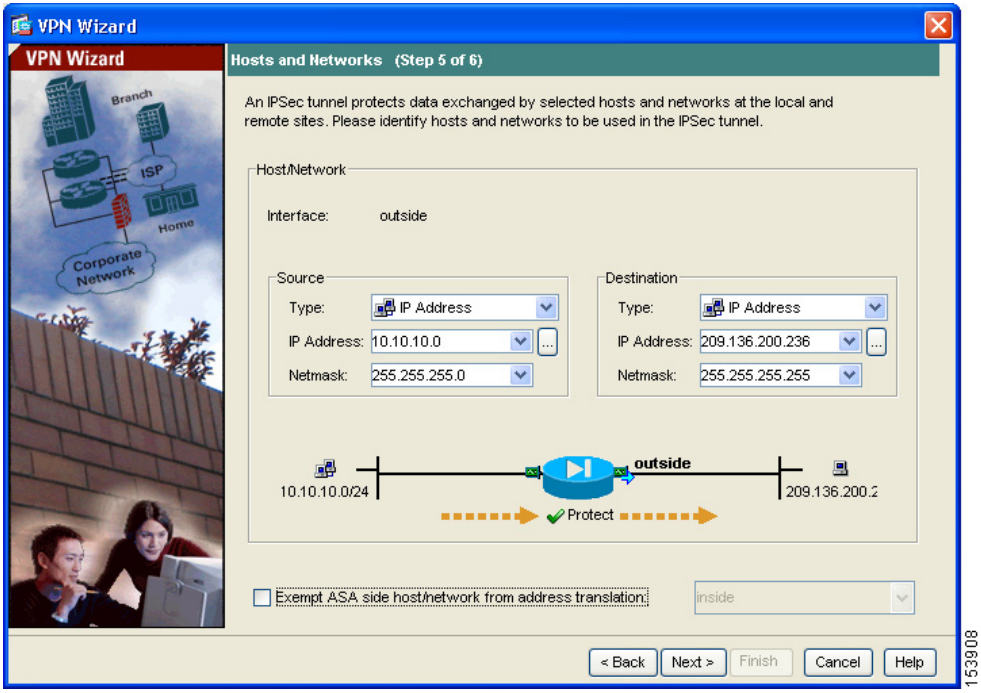
VPN Wizard の Step 5 で、次の手順を実行します。

ステップ 1　Source 領域の Type ドロップダウン リストで、IP アドレスを選択します。

ステップ 2　IP Address フィールドと Netmask フィールドに、ローカル IP アドレスとネットマスクを入力します。

ステップ 3　Destination 領域の Type ドロップダウン リストで、IP アドレスを選択します。

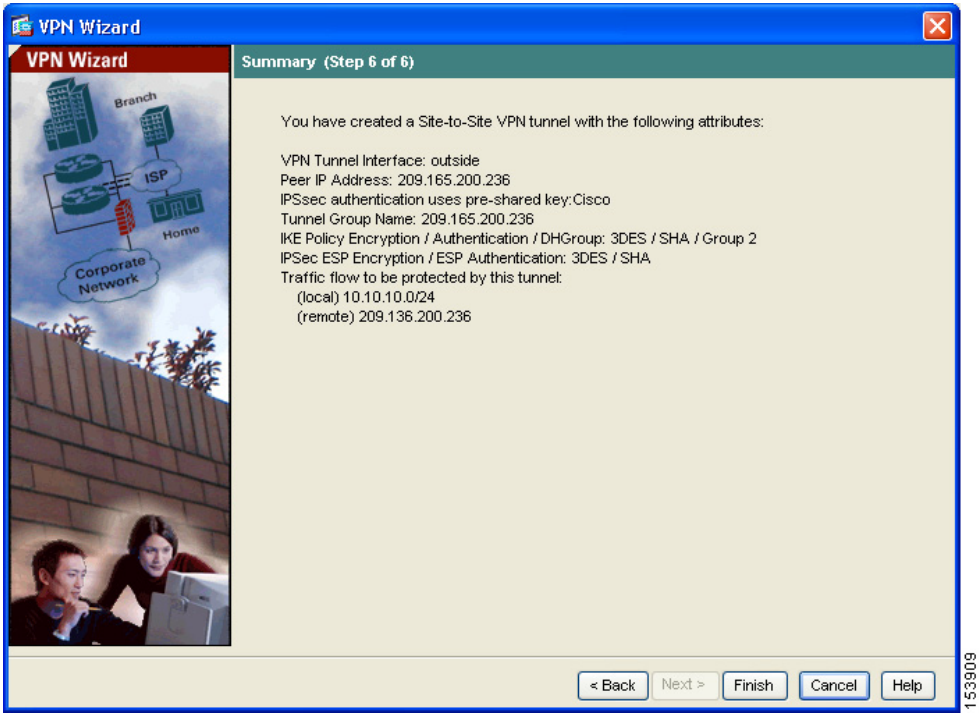
ステップ 4　リモート ホストまたはリモート ネットワークの IP アドレスとネットマスクを入力します。



ステップ 5　**Next** をクリックして続行します。

VPN アトリビュートの確認とウィザードの完了

VPN Wizard の Step 6 で、ここで作成した VPN トンネルの設定リストを確認します。設定が正しいことを確認したら、**Finish** をクリックして、変更を適応型セキュリティ アプライアンスに適用します。



次回のデバイス起動時に変更が適用されるように、設定変更をスタートアップ設定に保存する場合は、File メニューで **Save** をクリックします。

あるいは、ASDM の終了時に設定変更の保存を要求するプロンプトが表示されます。

設定変更を保存しない場合は、次回のデバイス起動時に以前の設定が有効になります。

これで、セキュリテイ アプライアンス 1 の設定プロセスは終わりです。

VPN 接続の反対側の設定

ローカルな適応型セキュリティ アプライアンスは設定されました。次に、リモート サイトの適応型セキュリティ アプライアンスを設定する必要があります。

リモート サイトでは、VPN ピアとして機能するように、2 番目の適応型セキュリティ アプライアンスを設定します。ローカルな適応型セキュリティ アプライアンスの設定手順のうち、P.8-5 の「ローカル サイトでのセキュリティ アプライアンスの設定」から P.8-14 の「VPN アトリビュートの確認とウィザードの完了」までを使用します。

（注） セキュリティ アプライアンス 2 を設定するときは、セキュリティ アプライアンス 1で選択した各オプションと同じ値を正確に入力する必要があります。不一致は、VPN トンネル設定エラーのよくある原因です。

次の手順

サイトツーサイト VPN 環境に、適応型セキュリティ アプライアンスを配置するだけの場合は、これで初期設定は終わりです。このほかに、次の手順について、実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のオペレーションの学習	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	*Cisco ASA 5500 Series Hardware Installation Guide*

適応型セキュリティ アプライアンスは、複数のアプリケーション用に設定できます。次の項で、その他の一般的なアプリケーション用に適応型セキュリティ アプライアンスを設定する手順を説明します。

作業内容	参照先
DMZ 内の Web サーバを保護する適応型セキュリティ アプライアンスの設定	第 6 章「シナリオ：DMZ の設定」
リモートアクセス VPN の設定	第 7 章「シナリオ：リモートアクセス VPN の設定」

AIP SSM の設定

オプションの AIP SSM は、インライン モードまたは無差別モードでセキュリティ検査を強化する、高度な IPS ソフトウェアを実行します。適応型セキュリティ アプライアンスが AIP SSM にパケットを転送するのは、パケットが出力インターフェイスを通過する直前（または VPN 暗号化が設定されている場合は暗号化が行われる前）と、他のファイアウォール ポリシーが適用された後です。たとえば、アクセスリストによってブロックされたパケットは、AIP SSM に転送されません。

AIP SSM を購入した場合は、この章の手順に従って、次の操作を行います。

- AIP SSM に誘導するトラフィックを特定するための適応型セキュリティ アプライアンスの設定
- AIP SSM へのセッションの接続とセットアップの実行

（注） AIP SSM は、バージョン 7.01 以降の ASA ソフトウェアでサポートされます。

この章は、次の項で構成されています。

AIP SSM の設定

この手順では、AIP SSM 用に適応型セキュリティ アプライアンスを設定するために必要な設定手順について説明します。

この項では、次のトピックについて取り上げます。

設定プロセスの概要

AIP SSM の設定は、3 段階に分けられます。まず適応型セキュリティ アプライアンスを設定し、次に AIP SSM を設定し、最後に IPS ソフトウェアを設定します。

1. ASA 5500 シリーズ 適応型セキュリティ アプライアンスでは、AIP SSM に誘導するトラフィックを特定します（P.9-3 の「トラフィックを AIP SSM に誘導するための ASA 5500 の設定」の説明を参照してください）。
2. AIP SSM では、検査と保護ポリシーを設定することにより、トラフィックの検査方法と侵入検出時の対処を決定します。
3. AIP SSM で実行する IPS ソフトウェアを設定します。IPS ソフトウェアについては、このマニュアルでは扱いません。IPS ソフトウェア設定の詳細については、IPS 製品に同梱されている次のマニュアルを参照してください。
   - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
   - *Cisco Intrusion Prevention System Command Reference*

トラフィックを AIP SSM に誘導するための ASA 5500 の設定

MPF（モジュラ ポリシー フレームワーク）コマンドを使用して、トラフィックを AIP SSM に誘導するように、適応型セキュリティ アプライアンスを設定します。この手順では、AIP SSM 配置の単純なポリシー セットを設定するための情報を示します。複雑なポリシー セットを作成する場合は、Modular Policy Framework の概念と一般的なコマンドを説明する『*Cisco Security Appliance Command Line Configuration Guide*』の「Modular Policy Framework」の章を参照してください。

適応型セキュリティ アプライアンスから AIP SSM に誘導するトラフィックを特定するには、次の手順を実行します。

ステップ 1　すべてのトラフィックと一致するアクセス リストを作成します。

```
hostname(config)# access-list acl-name permit ip any any
```

ステップ 2　AIP SSM に誘導するトラフィックを特定するクラスマップを作成します。次のように、**class-map** コマンドを使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

ここで、*class_map_name* は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI は、クラスマップ コンフィギュレーションモードに移行します。

ステップ 3　ステップ 1 で作成したアクセス リストと **match access-list** コマンドを使用して、スキャンするトラフィックを特定します。

```
hostname(config-cmap)# match access-list acl-name
```

ステップ 4　AIP SSM へのトラフィックの送信に使用するポリシーマップを作成するか、既存のポリシーマップを修正します。次のように、**policy-map** コマンドを使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

ここで、*policy_map_name* は、ポリシーマップの名前です。CLI は、ポリシーマップ コンフィギュレーション モードに移行し、プロンプトが変化します。

ステップ 5　スキャンするトラフィックを特定する、ステップ 2 で作成したクラスマップを指定します。次のように、**class** コマンドを使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

ここで、*class_map_name* は、ステップ 2 で作成したクラスマップの名前です。CLI は、ポリシーマップ クラス コンフィギュレーション モードに移行し、プロンプトが変化します。

ステップ 6　クラスマップで特定されたトラフィックを、AIP SSM に送信するトラフィックとして割り当てます。次のように、**ips** コマンドを使用します。

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |
fail-open}
```

inline キーワードおよび ***promiscuous*** キーワードによって、AIP SSM の動作モードを制御します。***fail-close*** キーワードおよび ***fail-open*** キーワードによって、AIP SSM を使用できないときに適応型セキュリティ アプライアンスがトラフィックを処理する方法を制御します。動作モードおよび障害発生時の動作の詳細については、P.9-2 の「AIP SSM の設定」を参照してください。

ステップ 7　**service-policy** コマンドを使用して、ポリシーマップをグローバルに、または特定のインターフェイスに適用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global |
interface interface_ID]
hostname(config)#
```

ここで、*policy_map_name* は、ステップ 4 で設定したポリシーマップです。すべてのインターフェイスのトラフィックにポリシーマップを適用するには、**global** キーワードを使用します。特定のインターフェイスのトラフィックにポリシーマップを適用するには、***interface*** *interface_ID* オプションを使用します。ここで、*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てた名前です。

グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

適応型セキュリティ アプライアンスは、指定されたとおりにトラフィックを AIP SSM に誘導し始めます。

次の例では、すべての IP トラフィックが AIP SSM に無差別モードで誘導され、何らかの理由で AIP SSM カードに障害が発生した場合は、すべての IP トラフィックがブロックされます。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ids-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

AIP SSM へのセッションの接続とセットアップの実行

トラフィックを AIP SSM に誘導するように、ASA 5500 シリーズ 適応型セキュリティ アプライアンスを設定した後、AIP SSM へのセッションを接続し、初期コンフィギュレーション用のセットアップ ユーティリティを実行します。

（注） (**session 1** コマンドを使用して)適応型セキュリティ アプライアンスから SSM へのセッションを接続することも、管理インターフェイスで SSH または Telnet を使用して、SSM に直接接続することもできます。あるいは、ASDM を使用することもできます。

適応型セキュリティ アプライアンスから AIP SSM へのセッションを接続するには、次の手順を実行します。

ステップ 1　**session 1** コマンドを入力して、ASA 5500 シリーズ適応型セキュリティ アプライアンス から AIP SSM へのセッションを接続します。

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

ステップ 2　ユーザ名とパスワードを入力します。デフォルトのユーザ名とパスワードは、どちらも **cisco** です。

（注） 初めて AIP SSM にログインしたときに、デフォルト パスワードの変更を要求するプロンプトが表示されます。パスワードは 8 文字以上で、辞書に載っていない単語にする必要があります。

```
login: cisco
Password:
Last login: Fri Sep  2 06:21:20 from xxx.xxx.xxx.xxx
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
AIP SSM#
```

（注） 上記のライセンスの注意が表示された場合（一部のソフトウェア バージョンでのみ表示されます）、AIP SSM でシグニチャ ファイルをアップグレードする必要がなければ、無視してかまいません。有効なライセンス キーがインストールされるまで、AIP SSM は現在のシグニチャ レベルで動作し続けます。ライセンス キーは後でインストールできます。ライセンス キーは、AIP SSM の現在の機能には影響を与えません。

ステップ 3　**setup** コマンドを入力して、AIP SSM の初期コンフィギュレーション用のセットアップ ユーティリティを実行します。

```
AIP SSM# setup
```

次の手順

これで、侵入防止のために適応型セキュリティ アプライアンスを設定する準備ができました。次のマニュアルを参照して、実装に合せて適応型セキュリティ アプライアンスを設定します。

作業内容	参照先
IPS センサーの設定	*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface* *Cisco Intrusion Prevention System Command Reference*
より効率的なサービス ポリシーの作成によるパフォーマンスの最適化	『*Cisco Security Appliance Command Line Configuration Guide*』の「Managing AIP SSM and CSC SSM」

IPS センサーおよび AIP SSM ソフトウェアを設定した後、次の追加の手順について、実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のオペレーションの学習	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	*Cisco ASA 5500 Series Hardware Installation Guide*

適応型セキュリティ アプライアンスは、複数のアプリケーション用に設定できます。次の項で、その他の一般的なアプリケーション用に適応型セキュリティ アプライアンスを設定する手順を説明します。

作業内容	参照先
DMZ Web サーバの保護の設定	第 6 章「シナリオ：DMZ の設定」
リモートアクセス VPN の設定	第 7 章「シナリオ：リモートアクセス VPN の設定」
サイトツーサイト VPN の設定	第 8 章「シナリオ：サイトツーサイト VPN の設定」

次の手順

CHAPTER 10

CSC SSM の設定

ASA 5500 シリーズ 適応型セキュリティ アプライアンスは、Content Security and Control ソフトウェアを実行する CSC SSM をサポートします。CSC SSM は、ウイルス、スパイウェア、スパムなど、望ましくないトラフィックからの保護を提供します。そのために、適応型セキュリティ アプライアンスで FTP、HTTP、POP3、および SMTP トラフィックを CSC SSM に誘導し、スキャンします。

（注） CSC SSM には、ASA ソフトウェア リリース 7.1.1 以降が必要です。

この章は、次の項で構成されています。

CSC SSM について

CSC SSM は、疑わしいコンテントのシグニチャ プロファイルが含まれるファイルを管理し、Trend Micro のアップデート サーバから定期的にアップデートします。CSC SSM は、適応型セキュリティ アプライアンスから受信したトラフィックをスキャンし、Trend Micro から取得したコンテント プロファイルと比較します。正当なコンテントは適応型セキュリティ アプライアンスに転送してルーティングし、疑わしいコンテントはブロックしてレポートします。

Trend Micro からコンテント プロファイルを取得するほかに、システム管理者は、CSC SSM が追加のトラフィック タイプまたはロケーションをスキャンするように、設定をカスタマイズすることもできます。たとえば、システム管理者は、特定の URL をブロックまたはフィルタリングしたり、FTP や電子メールのパラメータをスキャンするように、CSC SSM を設定できます。

CSC SSM のシステム セットアップおよびモニタリングは、ASDM を使用して実行できます。CSC SSM ソフトウェアのコンテント セキュリティ ポリシーの高度な設定を行うには、ASDM のリンクをクリックして、CSC SSM の Web ベースの GUI にアクセスします。

この章では、配置用に適応型セキュリティ アプライアンスを設定する方法を説明します。CSC SSM GUI の使用方法については、『*Cisco Content Security and Control SSM Administrator Guide*』で説明します。

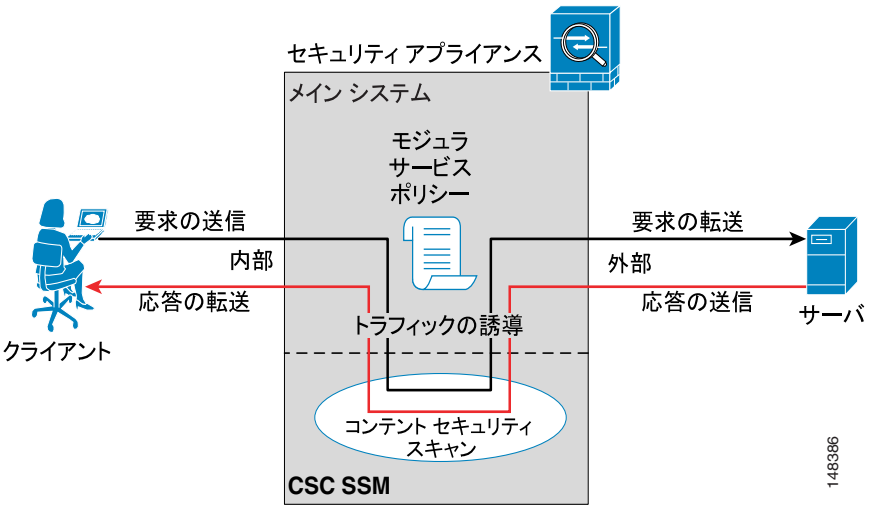
CSC SSM を使用するセキュリティ アプライアンスの配置について

CSC SSM と共に適応型セキュリティ アプライアンスを配置するネットワークでは、スキャンする種類のトラフィックだけを CSC SSM に送信するように、適応型セキュリティ アプライアンスを設定します。

図 10-1 で、企業ネットワーク、適応型セキュリティ アプライアンス、および CSC SSM と、インターネットとの間の基本的なトラフィック フローを示します。図 10-1 で示すネットワークには、次の要素が含まれています。

- CSC SSM が取り付けられ、設定されている適応型セキュリティ アプライアンス
- CSC SSM に誘導してスキャンするトラフィックを指定する、適応型セキュリティ アプライアンスのサービス ポリシー

図 10-1　CSC SSM のトラフィック フロー



この例では、クライアントは Web サイトにアクセスできるネットワーク ユーザ、FTP サーバからファイルをダウンロードできるネットワーク ユーザ、または POP3 サーバからメールを取得できるネットワーク ユーザです。

この設定では、トラフィック フローは次のようになります。

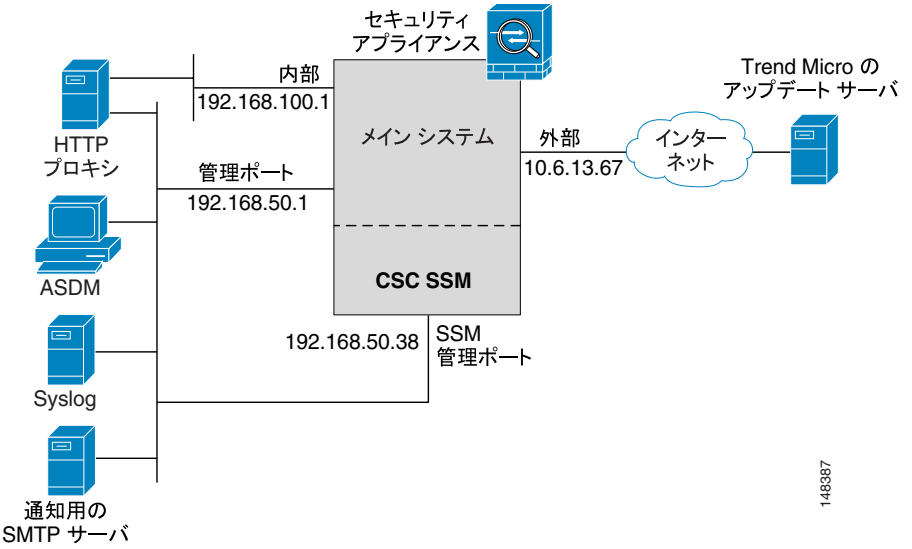
1. クライアントが要求を開始する。
2. 適応型セキュリティ アプライアンスが要求を受信し、インターネットに転送する。
3. 要求されたコンテントを適応型セキュリティ アプライアンスが取得し、このコンテント タイプが CSC SSM に誘導し、スキャンする対象としてサービス ポリシーで定義されているかどうかを判別する。定義されている場合は、CSC SSM に誘導する。
4. CSC SSM が適応型セキュリティ アプライアンスからコンテントを受信し、スキャンし、Trend Micro コンテント フィルタの最新アップデートと比較する。
5. コンテントが疑わしい場合、CSC SSM はコンテントをブロックし、イベントをレポートする。コンテントが疑わしくない場合、CSC SSM は要求されたコンテントを適応型セキュリティ アプライアンスに戻し、ルーティングする。

（注） CSC SSM は、SMTP トラフィックを他のコンテント タイプとは異なる方法で処理します。CSC SSM は、SMTP トラフィックを受信してスキャンしたら、そのトラフィックを適応型セキュリティ アプライアンス に戻してルーティングしません。代わりに、CSC SSM は、適応型セキュリティ アプライアンスで保護されている SMTP サーバに SMTP トラフィックを直接転送します。

シナリオ：コンテント セキュリティ用に配置されている CSC SSM を使用するセキュリティ アプライアンス

図 10-2 で、CSC SSM を使用する適応型セキュリティ アプライアンスの一般的な配置を示します。このシナリオのプロパティは、この章の後半の設定手順で例として使用します。

図 10-2　CSC SSM 配置のシナリオ



このシナリオでは、顧客がコンテント セキュリティ用に CSC SSM を使用する、適応型セキュリティ アプライアンスを配置しています。次の点に注意してください。

- 適応型セキュリティ　アプライアンスが専用管理ネットワークにある。必ずしも専用管理ネットワークを使用する必要はないが、セキュリティの理由により、使用することが推奨される。

- この適応型セキュリティ　アプライアンス設定には、2 つの管理ポートがある。1 つは、適応型セキュリティ アプライアンス自身の管理ポートで、もう 1 つは、CSC SSM の管理ポート。すべての管理ホストが、両方の IP アドレスにアクセスできる必要がある。
- HTTP プロキシ サーバが、内部ネットワークと専用管理ネットワークの両方に接続されている。これによって、CSC SSM は Trend Micro のアップデート サーバから、最新のコンテント セキュリティ フィルタを取得できる。
- 管理ネットワークに SMTP サーバが含まれており、管理者は CSC SSM イベントの通知を受けることができる。管理ネットワークには syslog サーバも含まれており、CSC SSM が生成したログを保管できる。

設定の要件

適応型セキュリティ アプライアンスの配置を計画するときは、ネットワークが次の要件を満たしている必要があります。

- SSM の管理ポートの IP アドレスに、ASDM の実行に使用するホストからアクセスできる。ただし、SSM の管理ポートと適応型セキュリティ アプライアンス管理インターフェイスの IP アドレスは、別のサブネットにできる。
- SSM の管理ポートは、CSC SSM が Trend Micro のアップデート サーバに到達できるように、インターネットに接続できる必要がある。

コンテント セキュリティ用の CSC SSM の設定

適応型セキュリティ アプライアンスと同時にオプションの CSC SSM モジュールを注文した場合、初期設定を完了するために、いくつかの手順を実行する必要があります。設定手順の一部は適応型セキュリティ アプライアンスで実行し、残りの設定手順は CSC SSM で実行するソフトウェアで実行します。

このマニュアルの前の手順を実行していた場合、この時点で、ASA システムはライセンス付きのソフトウェアを実行し、セットアップ ウィザードで基本的なシステム値が入力されています。次に、コンテント セキュリティ配置用に、適応型セキュリティ アプライアンスを設定します。

基本的な手順は、次のとおりです。

1. Cisco.com からソフトウェア アクティベーション キーを取得する。
2. CSC SSM の設定に必要な情報を収集する。

3. Cisco.com からアクティベーション キーを取得する。
4. このセットアップ プロセスのすべての設定作業に使用する ASDM を開く。
5. 時間設定を確認する。
6. CSC セットアップ ウィザードを実行して、CSC SSM を設定する。
7. 適応型セキュリティ アプライアンスを設定して、トラフィックを CSC SSM に誘導してスキャンする。

これらの手順は、次の項で詳しく説明します。

Cisco.com からのソフトウェア アクティベーション キーの取得

CSC SSM を使用して、Product Authorization Key（PAK）を受信します。PAK を使用して、次の URL で CSC SSM を登録します。

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

登録後、電子メールでアクティベーション キーを受信します。このアクティベーション キーは、P.10-10 の「CSC セットアップ ウィザードの実行」で説明する手順で必要になります。

情報の収集

適応型セキュリティ アプライアンス、および CSC SSM の設定を開始する前に、次の情報を収集します。

CSC SSM の管理ポートの IP アドレス ネットマスク、ゲートウェイ IP アドレス、およびネットマスク（適応型セキュリティ アプライアンスの IP アドレスは、第 5 章「適応型セキュリティ アプライアンスの設定」で説明するように、Setup Wizard を実行したときに割り当てられます）

（注）　SSM の管理ポート IP アドレスには、ASDM の実行に使用するホストからアクセスできる必要があります。SSM の管理ポートと、適応型セキュリティ アプライアンス管理インターフェイスの IP アドレスは、別のサブネットにできます。

- CSC SSM で使用するホスト名とドメイン名
- DNS サーバの IP アドレス
- HTTP プロキシ サーバの IP アドレス（ネットワークで、インターネットへの HTTP アクセスにプロキシを使用している場合）
- 電子メール通知に使用する電子メール アドレスと、SMTP サーバの IP アドレスおよびポート番号
- CSC SSM への管理アクセスを許可するホスト、およびネットワークの IP アドレス

ASDM の起動

ASDM を使用して、CSC SSM の設定と管理を行います。CSC SSM ソフトウェアのコンテント セキュリティ ポリシーの高度な設定を行うには、ASDM のリンクをクリックして、CSC SSM の Web ベースの GUI にアクセスします。

ASDM を起動するには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンス、および CSC SSM の管理ポートにアクセスできる PC で、インターネット ブラウザを起動します。

ステップ 2　ブラウザのアドレス フィールドに、URL「**https://*IP_address*/**」を入力します。

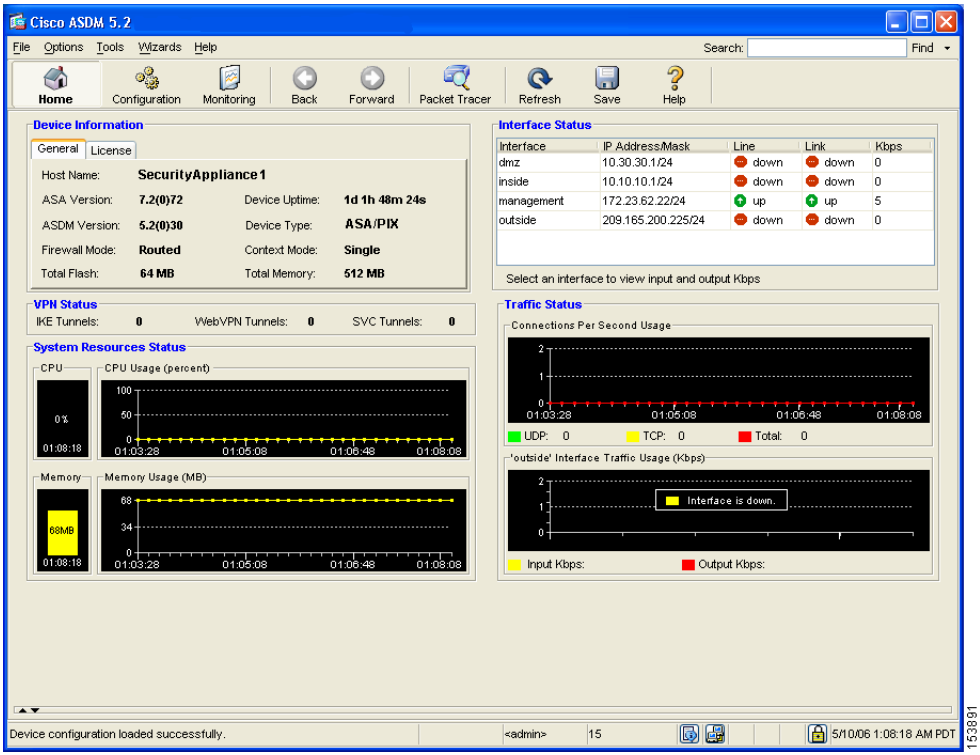
ここで、*IP_address* は、適応型セキュリティ アプライアンスの IP アドレスです。

（注）　適応型セキュリティ アプライアンスの出荷時のデフォルト IP アドレスは 192.168.1.1 です。「**s**」を追加して「**https**」にすることに注意してください。追加しないと、接続が失敗します。HTTPS（HTTP over SSL）は、ブラウザと適応型セキュリティ アプライアンスとの間でセキュアな接続を提供します。

ステップ 3　ユーザ名とパスワードを要求するダイアログボックスで、両方のフィールドを空のままにします。**Enter** キーを押します。

ステップ 4　**Yes** をクリックして、証明書を受け付けます。すべてのユーザ認証および証明書ダイアログボックスで、**Yes** をクリックします。

ASDM のメイン ウィンドウが表示されます。



時間設定の確認

適応型セキュリティ アプライアンスの時間設定が、時間帯を含めて正しいことを確認します。時間は、CSC SSM でのセキュリティ イベントのロギング、およびコンテント フィルタ リストの自動アップデートにとって重要です。また、ライセンスは時間の影響を受けるため、ライセンスにとっても重要です。

- 時間設定を手動で制御する場合は、クロック設定を確認します。ASDM で、**Configuration > Properties > Device Administration > Clock** をクリックします。
- NTP を使用して時間設定を制御する場合は、NTP 設定を確認します。ASDM で、**Configuration > Properties > Device Administration > NTP** をクリックします。

CSC セットアップ ウィザードの実行

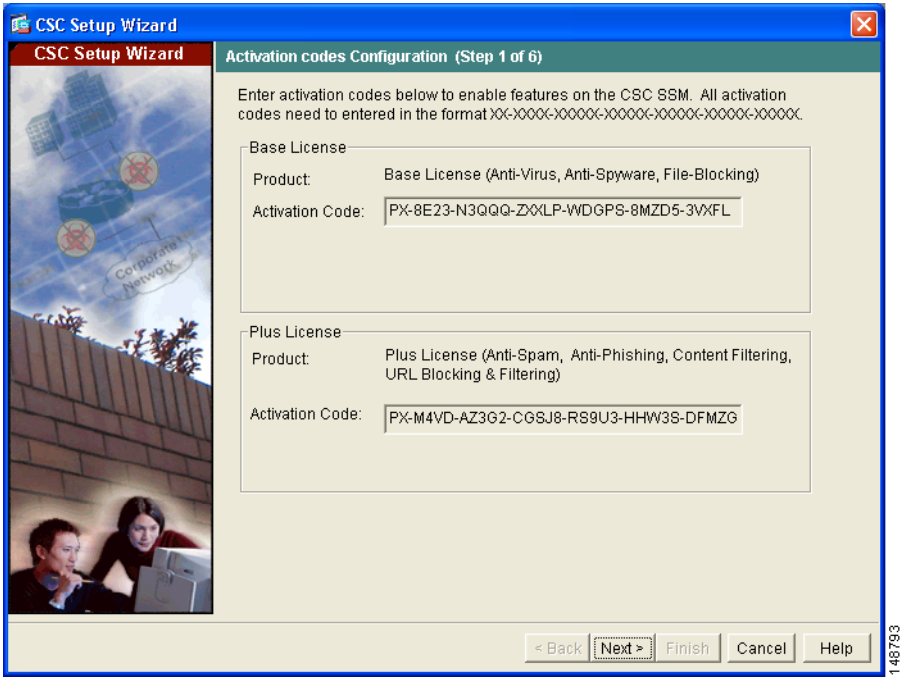
ステップ 1　ASDM のメイン ウィンドウで、**Configuration** タブをクリックします。

ステップ 2　左ペインで、**Trend Micro Content Security** タブをクリックします。

Wizard Setup 画面が表示されます。

ステップ 3　CSC Wizard の Step 1 で、Base License の **Software Activation Codes**（アクティベーション コード）を入力します。オプションで、Plus License のアクティベーション コードを入力します。

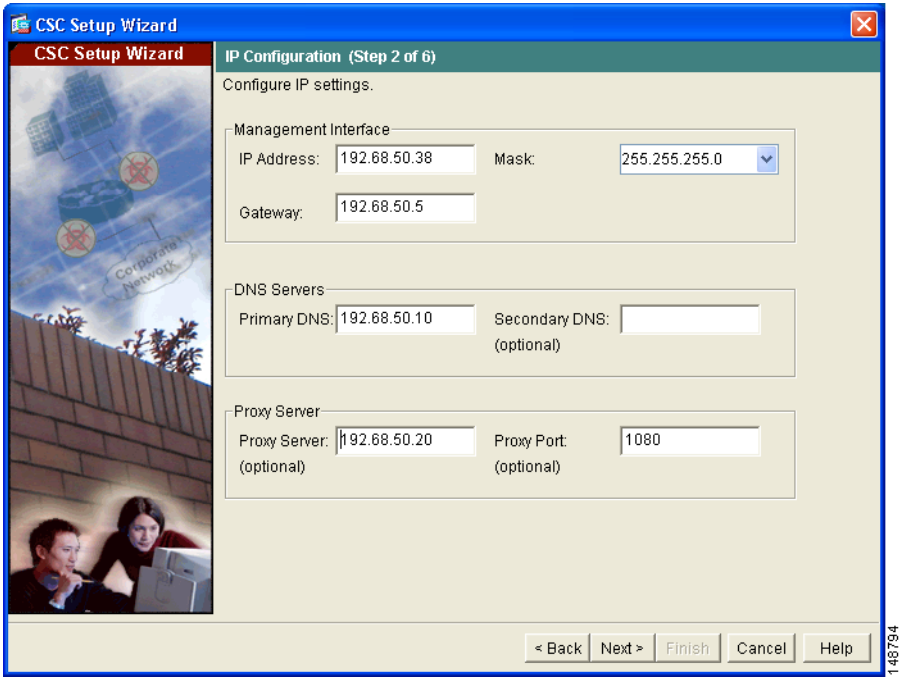
Plus License のアクティベーション コードは、CSC SSM の初期設定の後でも入力できます。



ステップ 4　**Next** をクリックします。

ステップ 5　CSC Wizard の Step 2 で、次の情報を入力します。

- CSC 管理インターフェイスの IP アドレス、ネットマスク、およびゲートウェイ IP アドレス
- プライマリ DNS サーバの IP アドレス
- HTTP プロキシ サーバの IP アドレスおよびプロキシ ポート（ネットワークで HTTP 要求をインターネットに送信するときに、HTTP プロキシを使用している場合のみ）



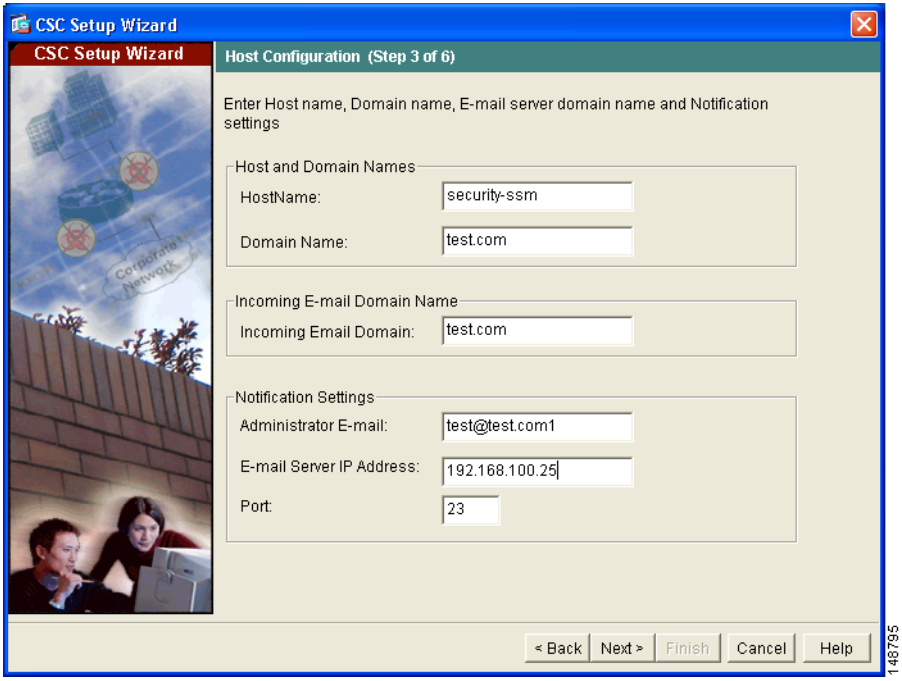
ステップ 6　**Next** をクリックします。

ステップ 7　CSC Setup Wizard の Step 3 で、次の情報を入力します。

- CSC SSM の **Hostname**（ホスト名）および **Domain**（ドメイン名）
- **Domain**（ドメイン名）は、着信ドメインとしてローカル メール サーバで使用します。

（注）　アンチスパム ポリシーは、このドメインに着信した電子メール トラフィックにのみ適用されます。

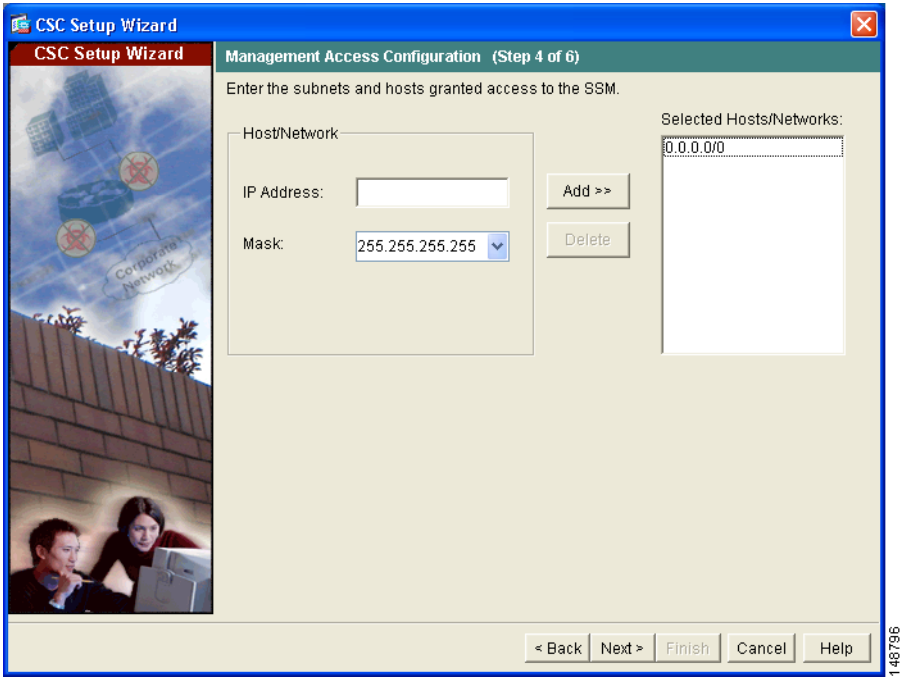
- 通知に使用する管理者の電子メール アドレスと、電子メール サーバの IP アドレスおよびポート



ステップ 8　**Next** をクリックします。

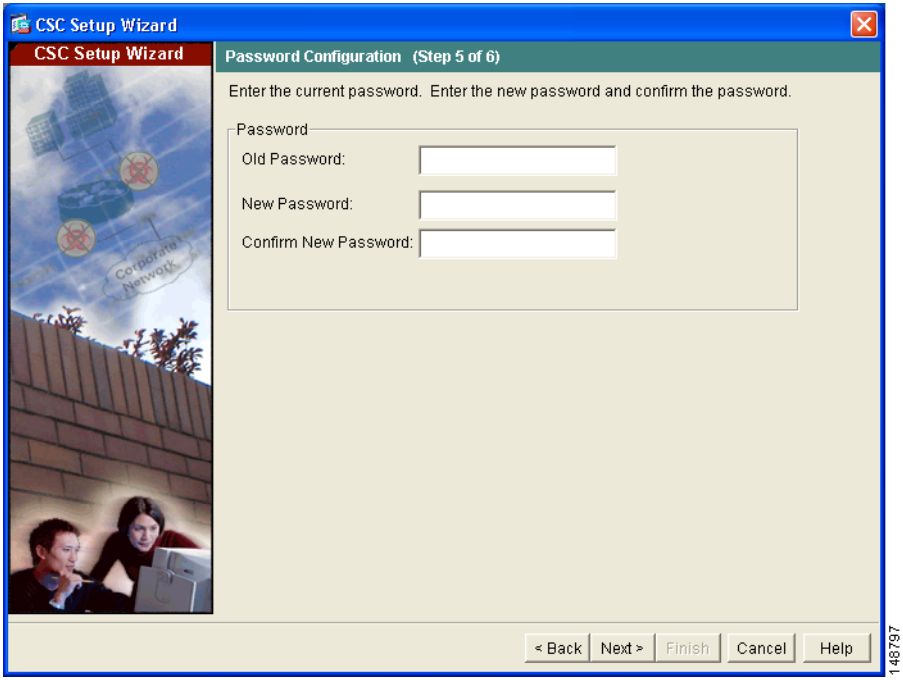
ステップ 9　CSC Setup Wizard の Step 4 で、CSC SSM への管理アクセスが必要な各サブネットおよびホストの、IP アドレスとマスクを入力します。

デフォルトでは、すべてのネットワークが CSC SSM に管理アクセスできます。セキュリティ上の理由により、特定のサブネットまたは管理ホストにアクセスを制限することが推奨されます。



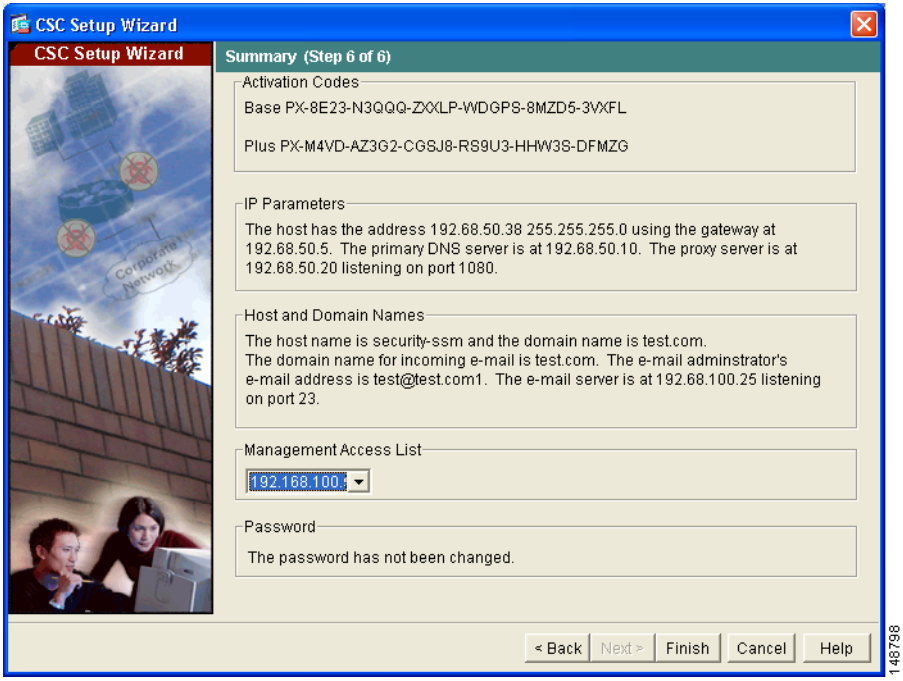
ステップ 10　**Next** をクリックします。

ステップ 11　CSC Setup Wizard の Step 5 で、管理アクセス用の新しいパスワードを入力します。Old Password フィールドに、工場出荷時のデフォルト パスワード「cisco」を入力します。



ステップ 12　**Next** をクリックします。

ステップ 13　CSC Setup Wizard の Step 6 で、CSC SSM に入力したコンフィギュレーション設定値を確認します。



これらの設定が正しいことを確認したら、**Finish** をクリックします。

ASDM に、CSC デバイスがアクティブになったことを示すメッセージが表示されます。

コンテント スキャン用の CSC SSM へのトラフィック誘導

適応型セキュリティ アプライアンスは、ファイアウォール ポリシーを適用した後、出力インターフェイスから出る前に、パケットを CSC SSM に誘導します。たとえば、アクセスリストによってブロックされたパケットは、CSC SSM に転送されません。

適応型セキュリティ アプライアンスで、CSC SSM に誘導するトラフィックを指定するサービス ポリシーを設定します。CSC SSM は、HTTP、POP3、FTP、および SMTP プロトコルの既知のポートに送信された、これらのトラフィックをスキャンできます。

初期設定プロセスを簡素化するために、この手順では、サポートされるプロトコルのすべてのトラフィック（着信および発信）を CSC SSM に誘導する、グローバル サービス ポリシーを作成します。適応型セキュリティ アプライアンスを通過するすべてのトラフィックをスキャンすると、適応型セキュリティ アプライアンス、および CSC SSM のパフォーマンスが低下する可能性があるため、このセキュリティ ポリシーは後で変更できます。たとえば、通常、内部ネットワークからの着信トラフィックは、信頼される発信元から着信しているため、すべてをスキャンする必要はありません。CSC SSM が信頼されない発信元からのトラフィックだけをスキャンするようにサービス ポリシーを調整することによって、セキュリティの目的を達成しながら、適応型セキュリティ アプライアンス、および CSC SSM の最大のパフォーマンスが得られます。

スキャンするトラフィックを特定するグローバル サービス ポリシーを作成するには、次の手順を実行します。

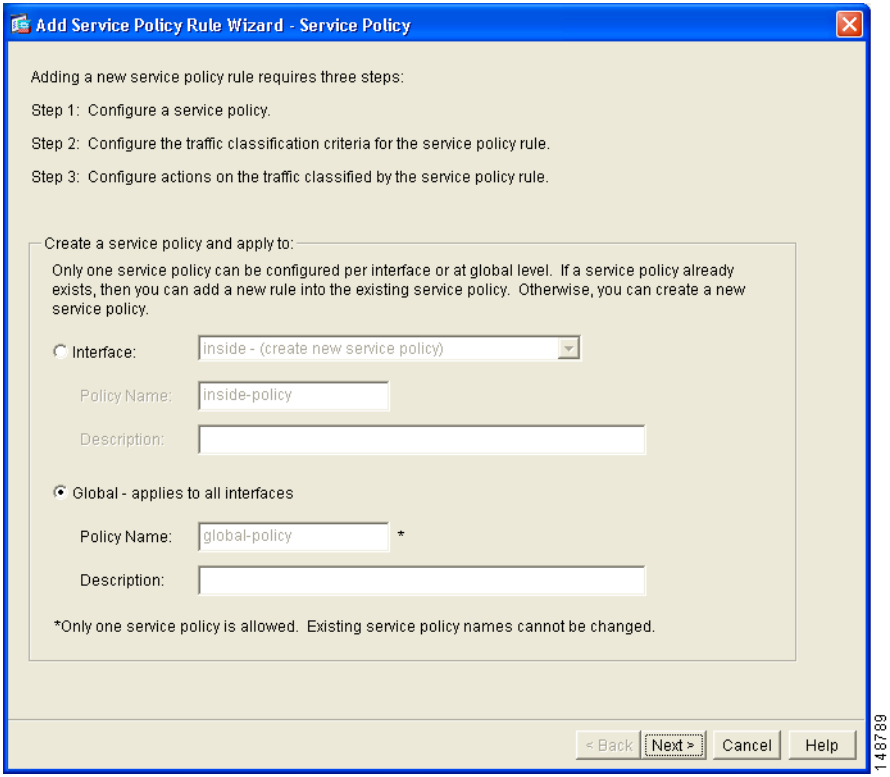
ステップ 1　ASDM のメイン ウィンドウで、**Configuration** タブをクリックします。

ステップ 2　**Security Policies** をクリックし、**Service Policy Rules** オプション ボタンをクリックします。

ステップ 3　**Add** をクリックします。

Add Service Policy Rule が表示されます。

ステップ 4　Service Policy ページで、**Global - applies to all interfaces** オプション ボタンをクリックします。

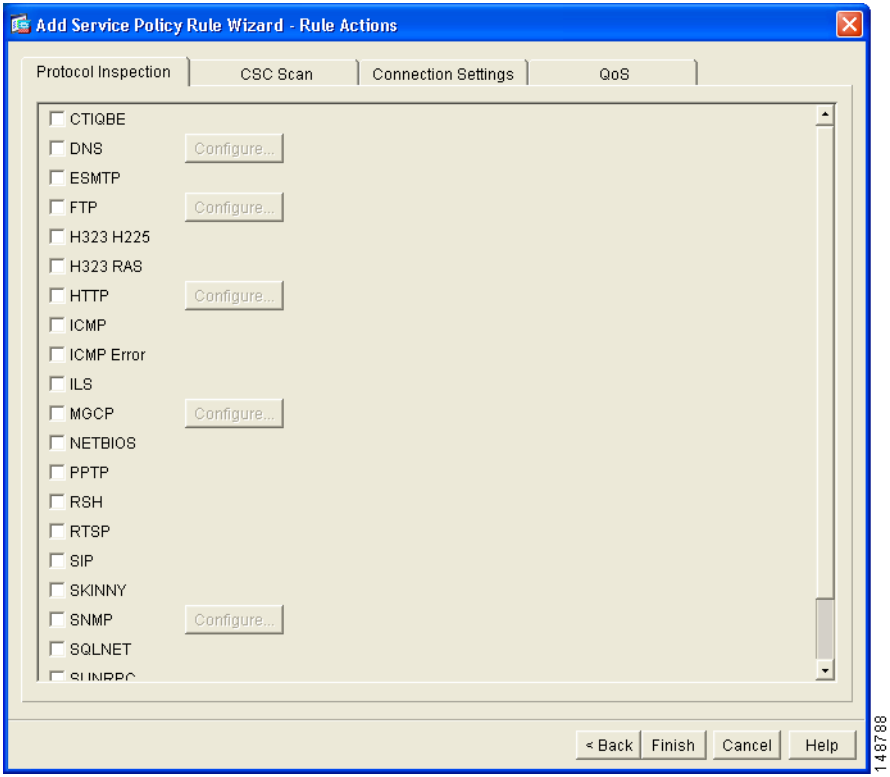


ステップ 5　**Next** をクリックします。Traffic Classification Criteria ページが表示されます。

ステップ 6　Traffic Classification Criteria ページで、**User class-default as the traffic class** オプション ボタンをクリックします。

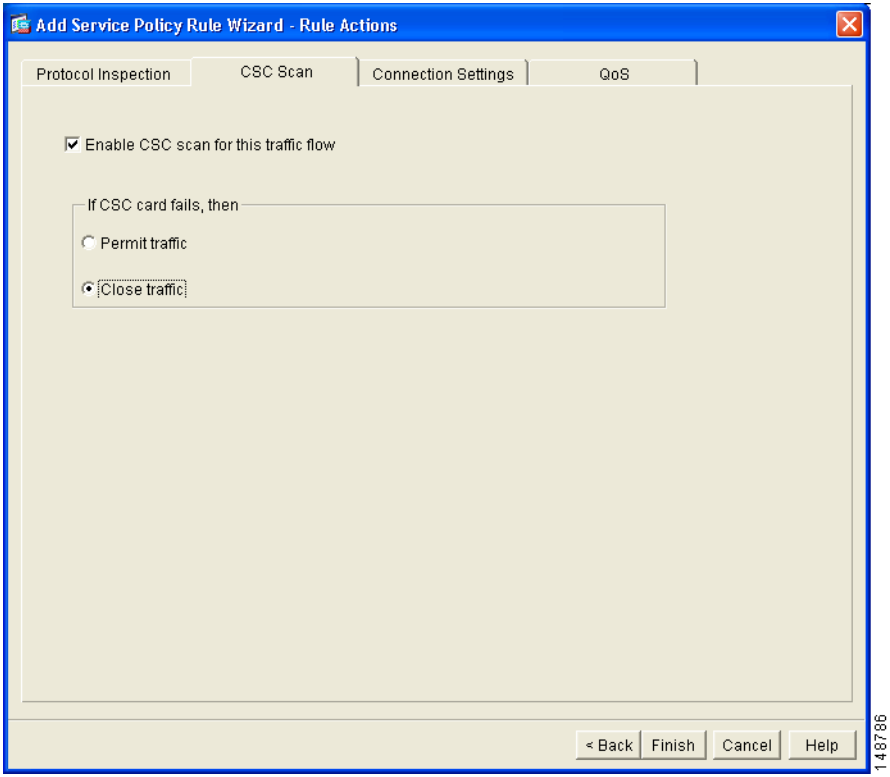
ステップ 7　**Next** をクリックします。Add Service Policy Rule Wizard - Rule Actions ページが表示されます。

ステップ 8　Service Policy Rule Wizard で、**CSC Scan** タブをクリックします。



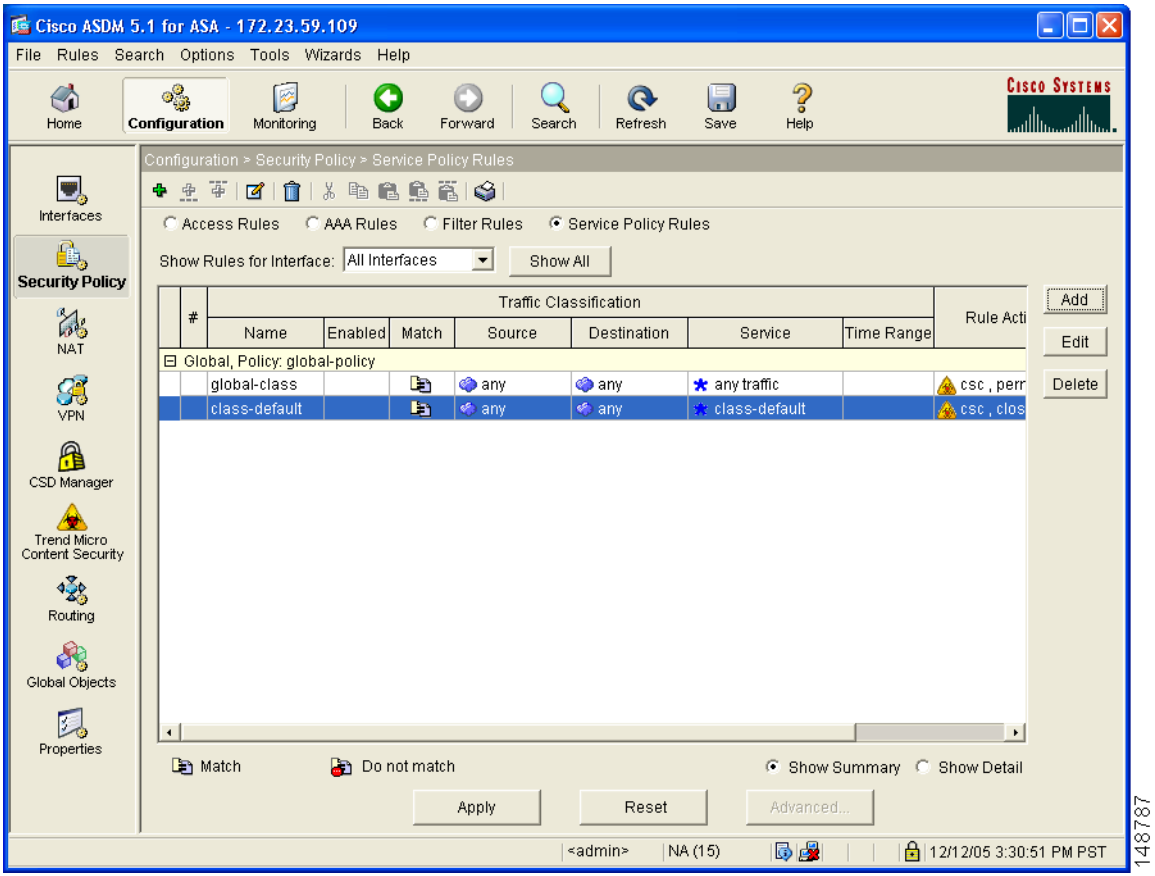
ステップ 9　CSC Scan タブ ページで、**Enable CSC scan for this traffic flow** チェックボックスをオンにします。

If CSC card fails, then 領域で、CSC SSM を使用できないときに選択されたトラフィックを、適応型セキュリティ アプライアンスが許可するか拒否するかを選択します。


Add Service Policy Rule Wizard - Rule Actions
Protocol Inspection
CSC Scan
Connection Settings
QoS
Enable CSC scan for this traffic flow
If CSC card fails, then
Permit traffic
Close traffic
< Back
Finish
Cancel
Help
148786

ステップ 10　**Finish** をクリックします。

新しいサービス ポリシーが Service Policy Rules ペインに表示されます。



ステップ 11　**Apply** をクリックします。

デフォルトでは、CSC SSM は、購入したライセンスでイネーブルになっているコンテント セキュリティ スキャン（アンチウイルス、アンチスパム、アンチフィッシング、コンテント フィルタリングなど）を実行するように設定されています。また、Trend Micro のアップデート サーバから、定期的にアップデートを取得するように設定されています。

購入したライセンスに含まれている場合、URL ブロッキングおよび URL フィルタリング用のカスタム設定や、電子メールおよび FTP のパラメータを作成できます。詳細については、『*Cisco Content Security and Control SSM Administrator Guide*』を参照してください。

次の手順

これで、Trend Micro Interscan for Cisco CSC SSM ソフトウェアを設定する準備ができました。次のマニュアルを参照して、実装に合せて適応型セキュリティ アプライアンスを設定します。

作業内容	参照先
CSC SSM ソフトウェアの設定（高度なセキュリティ ポリシーなど）	*Cisco Content Security and Control SSM Administrator Guide*
ASDM による追加の CSC SSM 機能の設定（コンテント フィルタリングなど）	ASDM のオンライン ヘルプ（**Configuration** または **Monitoring** タブをクリックし、**Trend Micro Content Security** タブをクリック）
より効率的なサービス ポリシーの作成によるパフォーマンスの最適化	『*Cisco Security Appliance Command Line Configuration Guide*』の「Managing AIP SSM and CSC SSM」

CSC SSM ソフトウェアを設定した後、次の追加の手順について、実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のオペレーションの学習	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	*Cisco ASA 5500 Series Hardware Installation Guide*

適応型セキュリティ アプライアンスは、複数のアプリケーション用に設定できます。次の項で、その他の一般的なアプリケーション用に適応型セキュリティ アプライアンスを設定する手順を説明します。

作業内容	参照先
DMZ Web サーバの保護の設定	第 6 章「シナリオ：DMZ の設定」
リモートアクセス VPN の設定	第 7 章「シナリオ：リモートアクセス VPN の設定」
サイトツーサイト VPN の設定	第 8 章「シナリオ：サイトツーサイト VPN の設定」

CHAPTER 11

ファイバ用 4GE SSM の設定

4GE Security Services Module（SSM）には、4 つのイーサネット ポートがあり、各ポートに、SFP（着脱可能小型フォーム ファクタ）ファイバと RJ 35 の 2 つのメディア タイプ オプションがあります。同じ 4GE カードを使用して、銅線ポートとファイバ ポートを混在させることができます。

（注） 4GE SSM には、ASA ソフトウェア リリース 7.04 以降が必要です。

この章は、次の項で構成されています。

（注） デフォルトのメディア タイプ設定はイーサネットなので、使用するイーサネット インターフェイスのメディア タイプ設定は、変更する必要がありません。

4GE SSM インターフェイスのケーブル接続

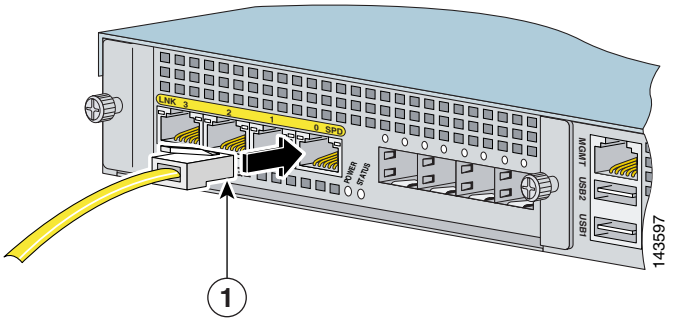
4GE SSM インターフェイスをケーブル接続するには、ネットワーク デバイスに接続するポートごとに、次の手順を実行します。

ステップ 1　RJ-45（イーサネット）インターフェイスをネットワーク デバイスに接続するには、各インターフェイスで次の手順を実行します。

a. アクセサリ キットから黄色のイーサネット ケーブルを見つけます。

b. ケーブルの一方の端を、4GE SSM のイーサネット ポートに接続します（図 11-1 を参照してください）。

図 11-1　イーサネット ポートの接続



1	RJ-45（イーサネット）ポート

c. ケーブルのもう一方の端を、ネットワーク デバイスに接続します。

ステップ 2　（オプション）SFP（光ファイバ）ポートを使用する場合は、図 11-2 で示すように、SFP モジュールを取り付けてケーブル接続します。

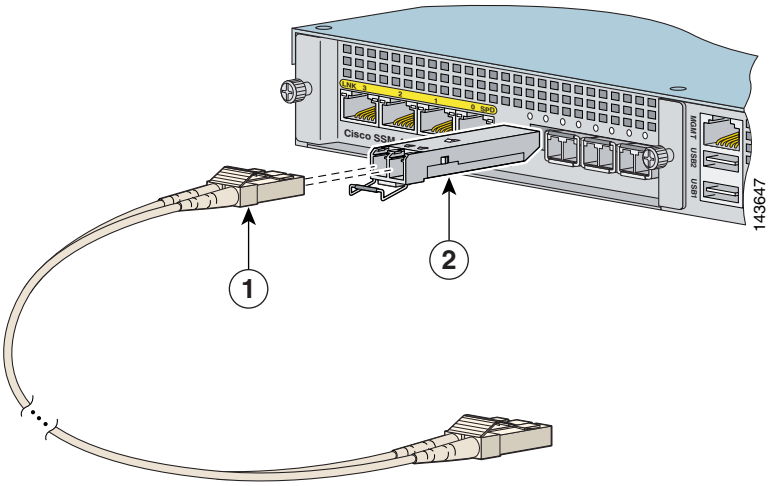
a. SFP モジュールを、カチッという音が聞こえるまで SFP ポートに差し込み、スライドさせます。カチッという音は、SFP モジュールがポートにロックされたことを示します。

b. 取り付けた SFP から光ポート プラグを取り外します。

c. 4GE SSM アクセサリ キットから、LC コネクタ（光ファイバケーブル）を見つけます。

d. LC コネクタを SFP ポートに接続します。

図 11-2　LC コネクタの接続



1	LC コネクタ	**2**	SFP モジュール

e. LC コネクタのもう一方の端を、ネットワーク デバイスに接続します。

SFP ポートをネットワーク デバイスに接続した後、各 SFP インターフェイスのメディア タイプ設定を変更する必要もあります。次の手順、「ファイバ インターフェイスの 4GE SSM メディア タイプ設定（オプション）」に進みます。

ファイバ インターフェイスの 4GE SSM メディア タイプ設定（オプション）

ファイバ インターフェイスを使用する場合、各 SFP インターフェイスで、メディア タイプ設定をデフォルト設定（イーサネット）からファイバ コネクタに変更する必要があります。

（注） デフォルトのメディア タイプ設定はイーサネットなので、使用するイーサネット インターフェイスのメディア タイプ設定は、変更する必要がありません。

ASDM を使用して SFP インターフェイスのメディア タイプを設定するには、ASDM のメイン ウィンドウから次の手順を実行します。

ステップ 1　ASDM ウィンドウの上部で **Configuration** タブをクリックします。

ステップ 2　ASDM ウィンドウの左側で **Interfaces** タブをクリックします。

ステップ 3　**4GE SSM** インターフェイスをクリックし、**Edit** をクリックします。Edit Interface ダイアログボックスが表示されます。

ステップ 4　**Configure Hardware Properties** をクリックします。Hardware Properties ダイアログボックスが表示されます。

ステップ 5　Media Type ドロップダウン リストで、**Fiber Connector** を選択します。

ステップ 6　**OK** をクリックして Edit Interfaces ダイアログボックスに戻り、**OK** をクリックしてインターフェイス設定ダイアログボックスに戻ります。

ステップ 7　各 SFP インターフェイスに対して、この手順を繰り返します。

コマンドラインからメディア タイプを設定することもできます。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の「Configuring Ethernet Settings and Subinterfaces」を参照してください。

次の手順

これで、初期設定が完了しました。次の追加の手順について、実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のオペレーションの学習	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	*Cisco ASA 5500 Series Hardware Installation Guide*

DES ライセンスまたは 3DES-AES ライセンスの取得

Cisco 適応型セキュリティ アプライアンスには、セキュア リモート管理（SSH、ASDM など）、サイトツーサイト VPN、リモート アクセス VPN など、特定の機能をイネーブルにするための暗号化技術を提供する DES または 3DES-AES ライセンスがあります。ライセンスをイネーブルにするには、暗号化ライセンス キーが必要です。

適応型セキュリティ アプライアンスと同時に DES または 3DES-AES ライセンスを注文した場合は、適応型セキュリティ アプライアンスに暗号化ライセンス キーが同梱されています。

Cisco.com の登録ユーザが DES または 3DES/AES 暗号化ライセンスを取得するには、次の Web サイトを参照してください。

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

Cisco.com の登録ユーザ以外の場合は、次の Web サイトを参照してください。

https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet

名前、電子メール アドレス、および適応型セキュリティ アプライアンスのシリアル番号を入力します。シリアル番号は、show version コマンドの出力で表示されます。

（注） 適応型セキュリティ アプライアンスの新しいアクティベーション キーが、ライセンス アップグレードを要求してから 2 時間以内に送信されます。

アクティベーション キーの例、またはソフトウェアのアップグレードの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

アクティベーション キーを使用するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`hostname# **show version**`	ソフトウェア リリース、ハードウェア構成、ライセンス キー、および関連する稼働時間データを表示します。
ステップ 2	`hostname# **configure terminal**`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	`hostname(config)# **activation-key** *activation-5-tuple-key*`	*activation-4-tuple-key* 変数に、新しいライセンスで取得したアクティベーション キーを指定して、暗号化アクティベーション キーをアップデートします。*activation-5-tuple-key* 変数は、5 つのエレメントからなる 16 進文字列です。各エレメントは 1 つのスペースで区切られます。たとえば、0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e です。「0x」は省略できます。値は、すべて 16 進数であると見なされます。
ステップ 4	`hostname(config)# **exit**`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	`hostname# **copy running-config startup-config**`	設定を保存します。
ステップ 6	`hostname# **reload**`	適応型セキュリティ アプライアンスをリブートし、設定をリロードします。

Numerics

A

C

L

M

R

S

か

こ