CISCO SYSTEMS

Cisco ASA 5550 スタートアップ ガイド

Customer Order Number: DOC-J-7817644=
Text Part Number: 78-17644-01-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。

作業内容	参照先
シャーシの設置	第 3 章「Cisco ASA 5550 適応型アプライアンスの取り付け」
ネットワーク インターフェイスへのケーブルの接続	第 4 章「ネットワーク インターフェイスへのケーブルの接続」
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」
実装のシナリオに応じ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」
設定の調整 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

ASA 5550 適応型セキュリティ アプライアンスのスループットの最大化

Cisco ASA 5550 シリーズ セキュリティ アプライアンスは、この章で説明するガイドラインに従って設定された場合に最大のスループットを発揮するように設計されています。

この章には、次の項があります。

組み込みネットワーク インターフェイス

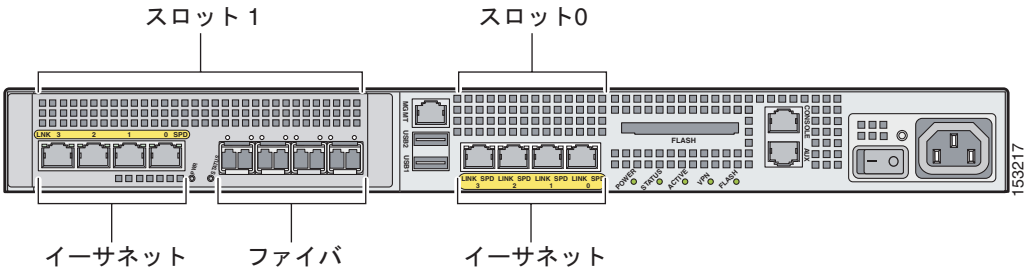
適応型セキュリティ アプライアンスは、次の 2 種類の内部バスによって、銅線ギガビット イーサネットとファイバ ギガビット イーサネットの接続性を提供します。

- 組み込み銅線ギガビット イーサネット ポート 4 個を備えたスロット 0（バス 0 に対応）
- 組み込み銅線ギガビット イーサネット ポート 4 個とファイバ ギガビット イーサネット接続を提供する組み込み SFP 4 個を備えたスロット 1（バス 1 に対応）

（注） 適応型セキュリティ　アプライアンスを使用してファイバ接続を確立するには、使用する各ファイバ ポートごとに SFP モジュールを注文し、取り付ける必要があります。ファイバ ポートと SFP ポートとモジュールの詳細については、P.3-6 の「SFP モジュールの取り付け」を参照してください。

図 2-1 に、FWSM の組み込みポートを示します。

図 2-1　ASA 5550 の組み込みポート



（注） スロット 1 には銅線イーサネット ポート 4 個とファイバ イーサネット ポート 4 個がありますが、スロット 1 で一度に使用可能なのは 4 個のポートのみです。たとえば、スロット 1 で銅線のポート 2 個とファイバ ポート 2 個を使用することはできますが、スロット 1 で 4 個すべての銅線ポートをすでに使用している場合、ファイバ ポートは使えません。

スループットの最大化を図るためのトラフィックの分散

トラフィックのスループットを最大化するためには、デバイスの 2 つのバス間でトラフィックが均等に分散され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。これを実現するには、一方のバスに入ったトラフィックがもう一方のバスから出るようにするため、すべてのトラフィックがバス 0（スロット 0）とバス 1（スロット 1）の両方を通過するネットワーク レイアウトにします。

図 2-2 および 図 2-3 は、ネットワーク トラフィックが分散する様子を示しています。すべてのトラフィックはデバイスの両方のバスを通過するため、適応型セキュリティ アプライアンスは最大のスループットを提供します。

図 2-2　最大スループットのために均等に分散されるトラフィック（銅線から銅線）

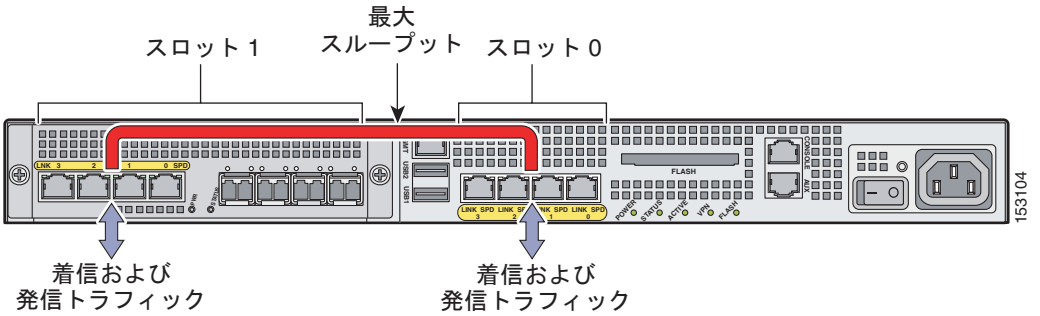


図 2-3　最大スループットのために均等に分散されるトラフィック（銅線からファイバ）

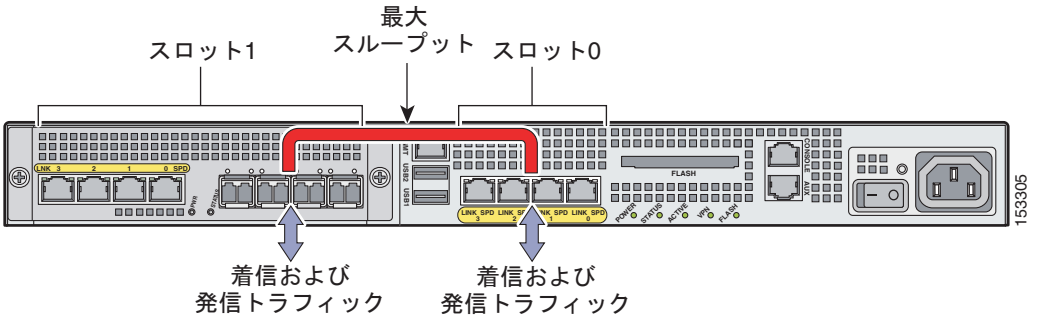
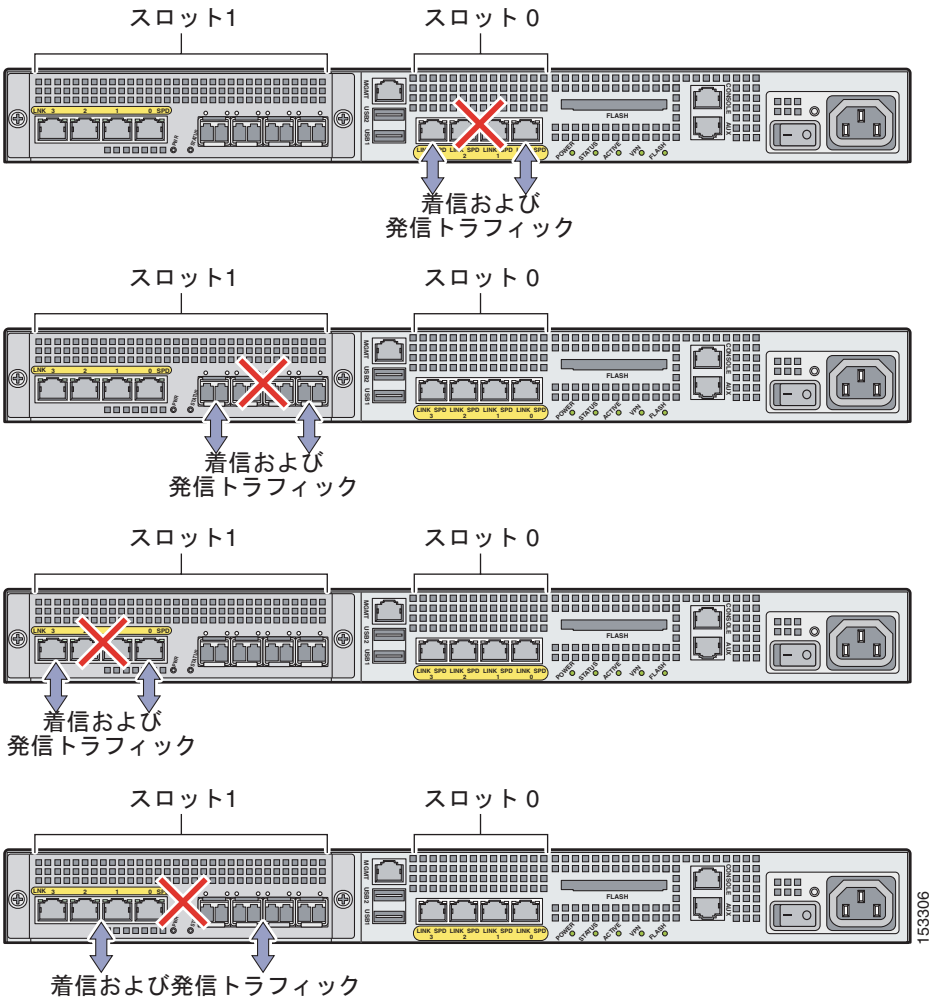


図 2-4 は、ネットワーク トラフィックがデバイスの一方のバスのみ通過するために適応型セキュリティ アプライアンスが最大のスループットを提供できない例を示します。

図 2-4　最大のスループットを提供しない設定



(注) **show traffic** コマンドを使用すると、各バスのトラフィックのスループットを確認できます。コマンドの使用法の詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

次の手順

第 3 章「Cisco ASA 5550 適応型アプライアンスの取り付け」に進みます。

CHAPTER 3

Cisco ASA 5550 適応型アプライアンスの取り付け

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。**

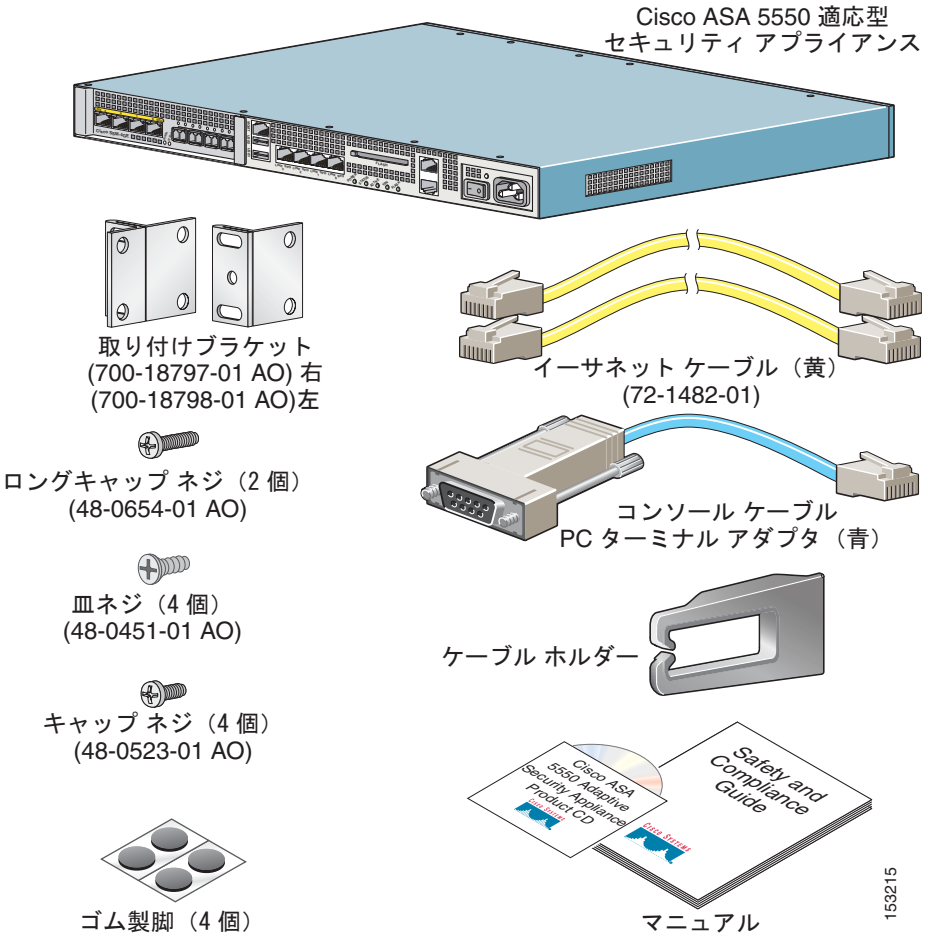
注意 これらの手順を実行するときは、『*Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*』の安全に関する警告を読み、適切な安全手順に従ってください。

この章では、ASA 5500 適応型セキュリティ アプライアンス、ラックマウント、および設置の手順について説明します。この章には、次の項があります。

パッケージ内容の確認

梱包箱の内容が 図 3-1 と同じかどうかを調べて、Cisco ASA 5550 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 3-1　ASA 5550 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。

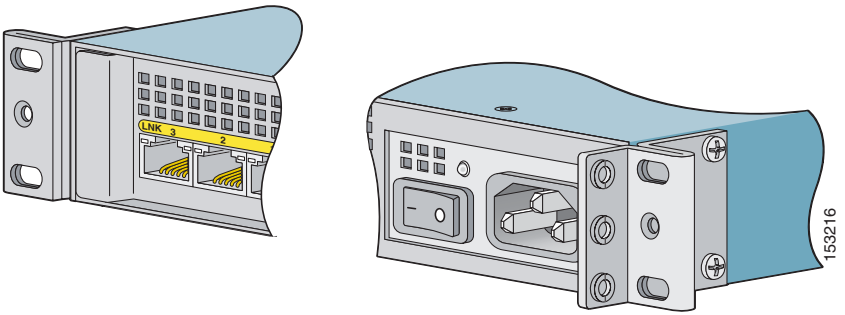
警告　**次の手順を実行する前に、電源が切れていることを確認してください。（AC または DC）。電源が DC 回路から切断されていることを確認するには、パネル ボード上で DC 回路に対応している回路ブレーカーを確認して、回路ブレーカーを OFF の位置に切り替え、回路ブレーカーのスイッチ ハンドルを OFF の位置のままテープで固定します。**

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。

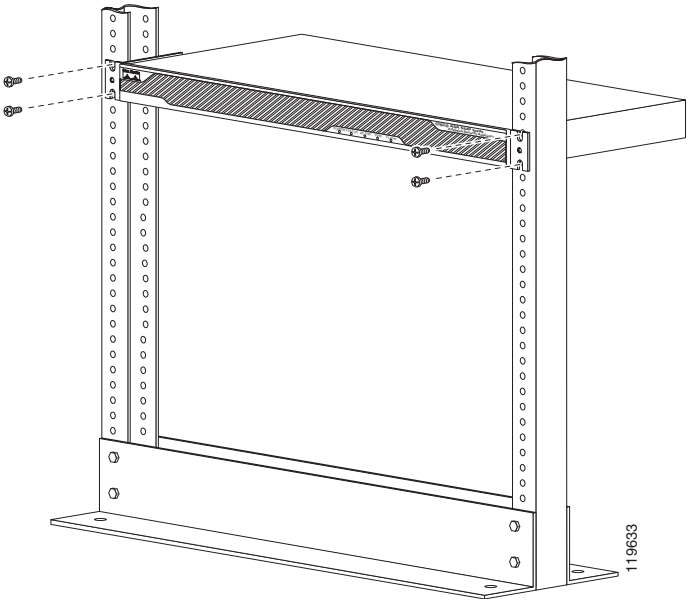
ステップ 1　付属のネジを使用して、シャーシにラックマウント ブラケットを取り付けます。ブラケットを穴に取り付けます（図 3-2 を参照してください）。ブラケットをシャーシに固定すると、ラックマウントできるようになります。

図 3-2　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 3-3 を参照してください）。

図 3-3　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。

SFP モジュールの取り付け

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、ファイバ ギガビット イーサネット接続を確立します。

この項では、適応型セキュリティ アプライアンスの 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。次のトピックについて取り上げます。

SFP モジュール

SFP（着脱可能小型フォーム ファクタ）モジュールは、ホットスワップ可能な入力 / 出力デバイスで、ファイバ ポートに接続されます。

（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 3-1 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 3-1　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	ファイバ	GLC-LH-SM=
1000BASE-SX	ファイバ	GLC-SX-MM=

1000BASE-LX/LH と 1000BASE-SX の SFP モジュールは、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 3-2 に、ケーブル長の要件を示します。

表 3-2　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、清潔なポート 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。

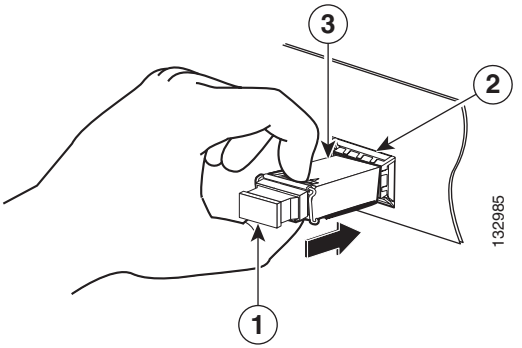
警告 **ケーブルが接続されていない場合、ポートの開口部からは目に見えないレーザー光が放射されている可能性があります。レーザー光に当たらないようにし、開口部をのぞきこまないでください。**ステートメント 70

SFP モジュールの取り付け

SFP モジュールをスロット 1 のファイバ ポートに取り付けるには、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	ポート プラグ	**3**	SFP モジュール
2	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ポート プラグを SFP モジュールから取り外さないでください。

ステップ 2　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。

ステップ 3　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「ネットワーク インターフェイスへのケーブルの接続」を参照してください。

注意　多くの SFP モジュール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 SFP 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。

ポートと LED

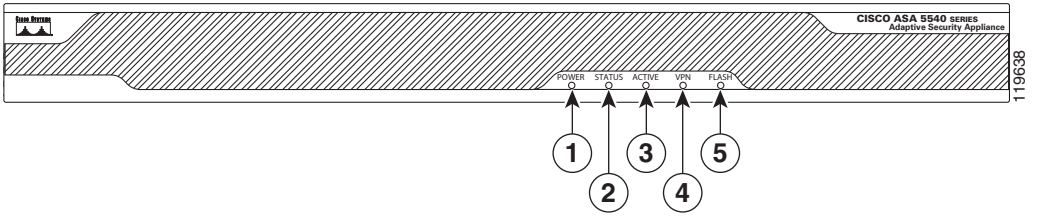
ここでは、前面パネルと背面パネルについて説明します。図 3-5 に前面パネルの LED を示します。次のトピックについて取り上げます。

- 前面パネルの LED（P.3-10）
- 背面パネルの LED とスロット 0 のポート（P.3-11）
- スロット 1 のポートおよび LED（P.3-13）

前面パネルの LED

図 3-5 に適応型セキュリティ アプライアンスの前面パネルの LED を示します。

図 3-5　前面パネルの LED

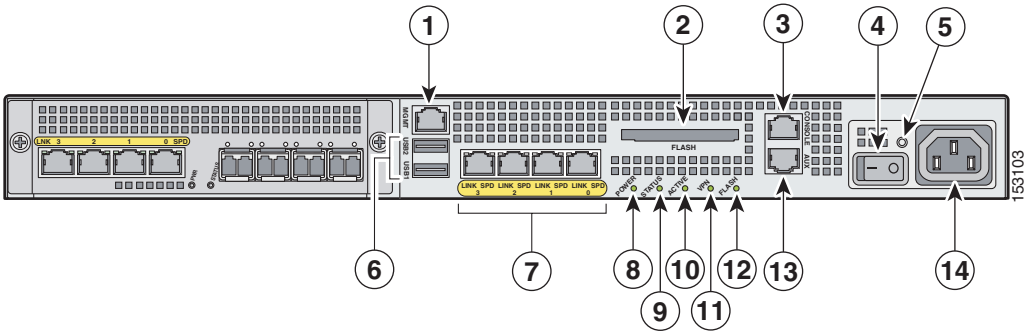


	LED	色	ステート	説明
1	電源	緑	点灯	システムは通電状態です。
2	ステータス	緑	点滅	電源投入診断を実行中か、システムがブート中です。
			点灯	システムは電源投入診断に合格しました。
		オレンジ	点灯	電源投入診断に合格しませんでした。
3	アクティブ	緑	点滅	ネットワーク アクティビティが発生しています。
4	VPN	緑	点灯	VPN トンネルが確立されました。
5	フラッシュ	緑	点灯	CompactFlash がアクセスされています。

背面パネルの LED とスロット 0 のポート

図 3-6 に、背面パネルの LED とスロット 0 のポートを示します。

図 3-6　背面パネルの LED とスロット 0 のポート（AC 電源モジュール モデルの場合）



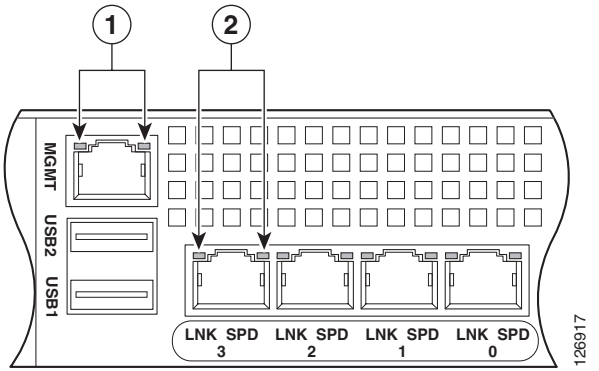
1	管理ポート[1]	**6**	USB 2.0 インターフェイス[2]	**11**	VPN LED
2	外部 CompactFlash スロット	**7**	ネットワーク インターフェイス[3]	**12**	フラッシュ LED
3	シリアル コンソール ポート	**8**	電源インジケータ LED	**13**	補助ポート
4	電源スイッチ	**9**	ステータス インジケータ LED	**14**	電源コネクタ
5	電源インジケータ LED	**10**	アクティブ LED		

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. 今後の使用のために予約されています。
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*** コマンドの説明を参照してください。

図 3-7 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 3-7　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 3-3 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。

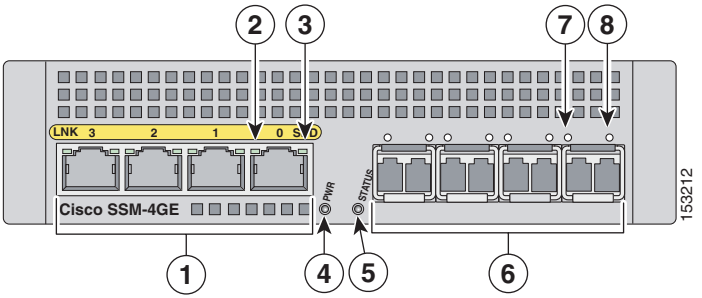
表 3-3　リンクおよび速度の LED

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

スロット 1 のポートおよび LED

図 3-8 に、スロット 1 のポートと LED を示します。

図 3-8　スロット 1 のポートと LED



1	銅線イーサネット ポート	**5**	ステータス LED
2	RJ-45 リンク LED	**6**	ファイバ イーサネット 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 3-8 は、イーサネット ポートに取り付けられている SFP モジュールを示しています。ファイバ イーサネット接続を確立する場合は、SFP モジュールを注文し、取り付ける必要があります。ファイバ ポートと SFP モジュールの詳細については、P.3-6 の「SFP モジュールの取り付け」を参照してください。

表 3-4 に、スロット 1 の LED を示します。

表 3-4　バス G1 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	10 MB	ネットワーク アクティビティは発生していません。
		緑	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。
		オレンジ	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	点滅	システムはブート中です。
		緑	点灯	システムは正常にブートされました。
		オレンジ	点灯	システムの診断が失敗しました。

次の手順

第 4 章「ネットワーク インターフェイスへのケーブルの接続」に進みます。

次の手順

CHAPTER 4

ネットワーク インターフェイスへのケーブルの接続

この章では、コンソール ポート、補助ポート、管理ポート、銅線イーサネット ポート、およびファイバ イーサネット ポートに適切なケーブルを接続する方法について説明します。

この章には、次の項があります。

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 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　管理ポートに接続します。

適応型セキュリティ アプライアンス には、管理 0/0 ポートと呼ばれるデバイスを管理するための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、ファースト イーサネット インターフェイスです。このポートはコンソール ポートと類似していますが、管理 0/0 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。

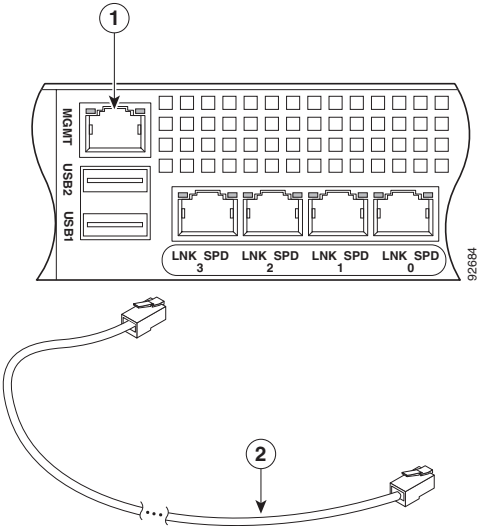
（注）　インターフェイスを管理専用インターフェイスとして設定するには、**management-only** コマンドを使用します。管理インターフェイスの管理専用モードをディセーブルにすることもできます。このコマンドの詳細については、『*Cisco Security Appliance Command Reference*』の **management-only** コマンドの説明を参照してください。

a.　両端に RJ-45 コネクタの付いたイーサネット ケーブルを見つけます。

b.　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）。

c.　イーサネット　ケーブルのもう一方の端を、コンピュータまたは管理ネットワークのイーサネット 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

ステップ 3　コンソール ポートに接続します。

a. コンピュータまたはターミナルを任意の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。

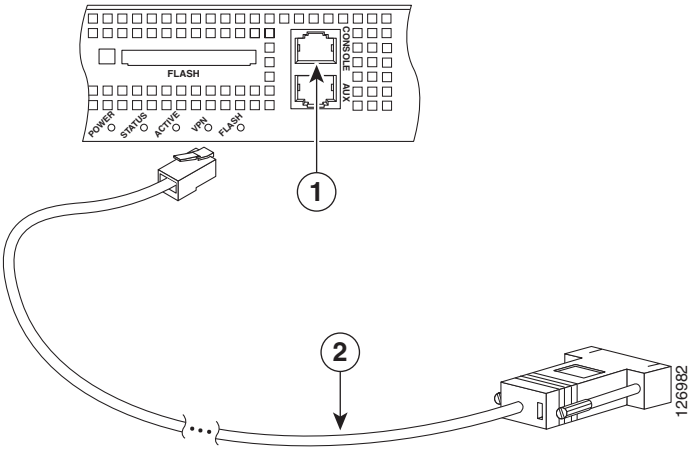
ターミナルの設定は次のとおりです。9600 ボー（デフォルト）、8 データ ビット、パリティなし、1 ストップ ビット、およびフロー制御（FC）= ハードウェア。

b. 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 コネクタがあるコンソール ケーブルを見つけます。

c. 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（図 4-2 を参照してください）。

d. 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

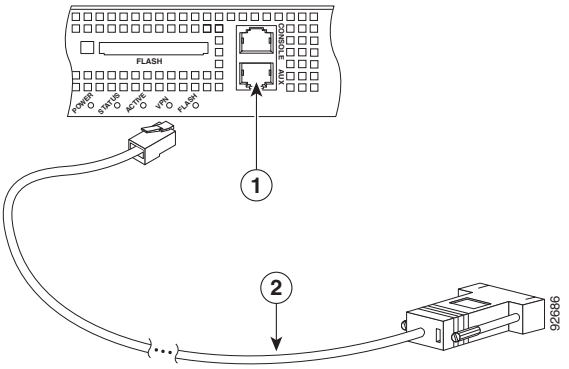
ステップ 4　補助ポート（AUX というラベルがあるポート）に接続します。

a. 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 コネクタがあるコンソール ケーブルを見つけます。

b. 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）。

c. 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



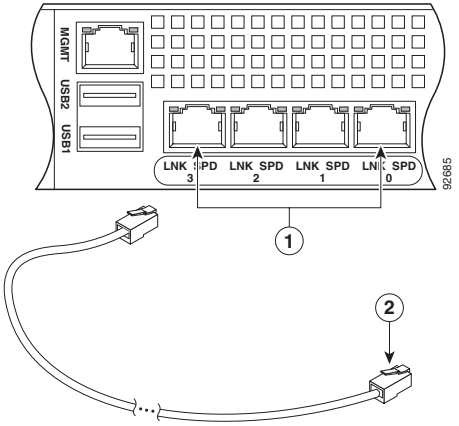
1	RJ-45 補助ポート	**2**	RJ-45/DB-9 コンソール ケーブル

ステップ 5　ネットワーク接続用の銅線のイーサネット　ポートを接続します。銅線のイーサネット ポートはスロット 0 とスロット 1 の両方で使用できます。

（注）　スロット 0 のポートは内部インターフェイス用に、スロット 1 のポートは外部インターフェイス用にそれぞれ使用する必要があります。

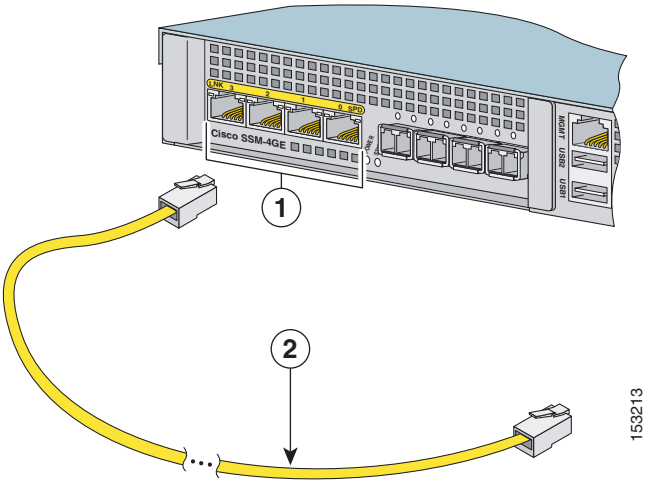
a.　イーサネット ケーブルの一方の端を銅線のイーサネット ポートに接続します（図 4-4 および図 4-5 を参照してください）。

図 4-4　銅線のイーサネット インターフェイスのスロット 0 への接続



1	銅線イーサネット ポート	**2**	RJ-45 コネクタ

図 4-5　銅線のイーサネット インターフェイスのスロット 1 への接続



1	銅線イーサネット ポート	**2**	RJ-45 コネクタ

b. 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。

ステップ 6　ネットワーク接続用のファイバ イーサネット ポートを接続します。

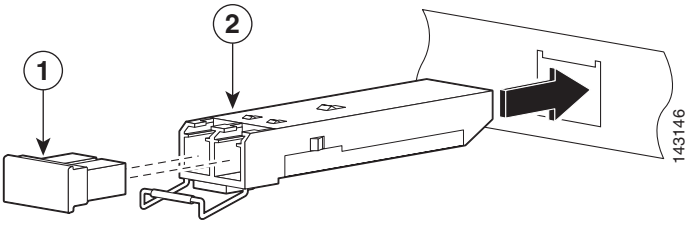
（注） スロット 1 には、銅線イーサネット ポートが 4 個とファイバ イーサネット ポートが 4 個あります。いずれのタイプのポートでも使用できますが、スロット 1 で一度に使用可能なポートは合計 4 個です。たとえば、銅線イーサネット ポート 2 個とファイバ イーサネット ポート 2 個は同時に使用可能です。

使用するファイバ ポートそれぞれに対して、次の手順を実行します。

a. SFP モジュールの取り付け：

- SFP モジュールを、カチッという音が聞こえるまでファイバ 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 からポート プラグを取り外します（図 4-6 を参照してください）。

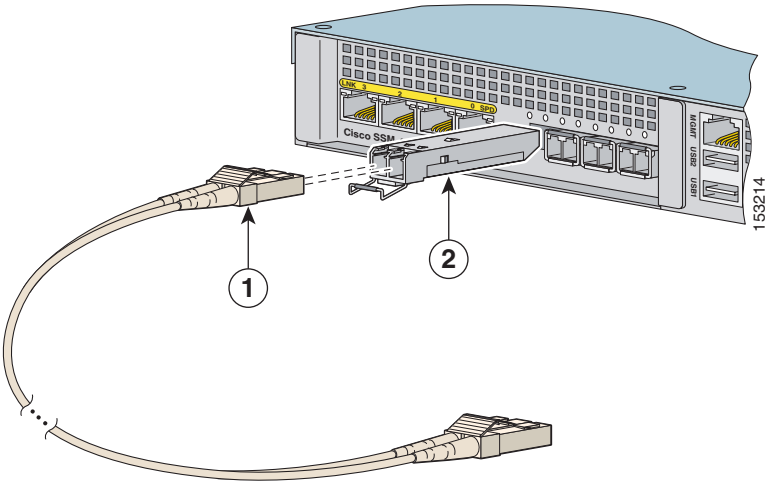
図 4-6　ファイバ ポート プラグの取り外し



1	ポート プラグ	**2**	SFP モジュール

b. LC コネクタを SFP モジュールに接続します（図 4-7 を参照してください）。

図 4-7　LC コネクタの接続



1	LC コネクタ	**2**	SFP モジュール

c. 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。

ステップ 7　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 8　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。

この章には、次の項があります。

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。この工場出荷時のデフォルト設定により、インターフェイスが自動的に設定されるため、デバイスに即時接続して、ASDM で設定を完了することができます。

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。

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 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 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、内部ネットワークと外部ネットワーク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。

（注） スロット 0 のポートは内部インターフェイス用、スロット 1 のポートは外部インターフェイス用として使用する必要があります。

この項では、Startup Wizard を使用した基本的な設定パラメータの設定方法について説明します。次のトピックについて取り上げます。

- Startup Wizard を起動する前に（P.5-4）
- Startup Wizard の実行（P.5-5）

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これから設定する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 の実行

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　管理ポートに接続していない場合は、接続します。

a. 両端に RJ-45 コネクタの付いたイーサネット ケーブルを見つけます。

b. RJ-45 コネクタ 1 個を管理 0/0 ポートに接続します。

c. イーサネット　ケーブルのもう一方の端を、コンピュータまたは管理ネットワークのイーサネット ポートに接続します。

d. 管理ネットワークに接続している場合は、適応型セキュリティ　アプライアンスを設定するための PC を管理ネットワークに接続します。

ステップ 2　Startup Wizard を起動します。

a. スイッチ、ハブ、または管理ネットワークに接続された 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。

c. ASDM ソフトウェアの実行方法を選択するウィンドウで、ASDM ランチャをダウンロードする方法と ASDM ソフトウェアを Java アプレットとして実行する方法のいずれかを選択します。

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 が起動します。

ステップ 5　Wizards メニューから、Startup Wizard を選択します。

ステップ 6　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。

（注）　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。このアクセス コントロール ポリシーは、**icmp** コマンドで設定できます。**icmp** 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。

ファイバ インターフェイスのメディア タイプ設定

スロット 1 でファイバ接続を使用する場合、メディア タイプ設定をデフォルト設定からファイバ 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 タイプ設定は銅線イーサネット ポートなので、使用する銅線イーサネット ポートのメディア タイプ設定は、あらためて設定する必要はありません。

ASDM を使用してファイバ 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 ウィンドウで、**Configuration** をクリックします。

ステップ 2　Features ペインで、**Interfaces** 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　各ファイバ 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

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」

CHAPTER 6

シナリオ：DMZ の設定

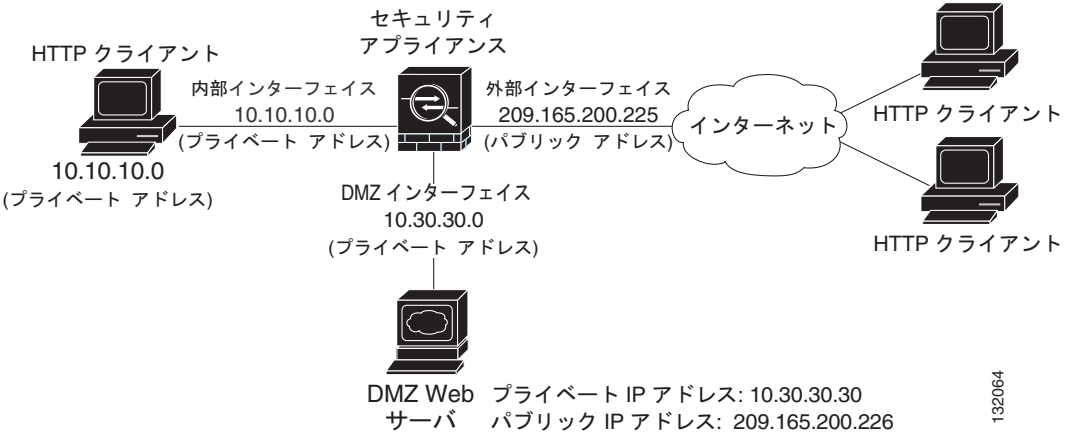
この章では、適応型セキュリティ アプライアンスを使用して非武装地帯（DMZ; demilitarized zone）に置かれたネットワーク リソースを保護するための設定シナリオについて説明します。DMZ とは、プライベート（内部）ネットワークとパブリック（外部）ネットワークの間の中立ゾーンにある区別されたネットワークです。

この章には、次の項があります。

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 トポロジの例は、適応型セキュリティ アプライアンスのほとんどの DMZ 実装の典型的なものです。

図 6-1　DMZ の設定シナリオのネットワーク レイアウト



この例のシナリオには、次の性質があります。

- Web サーバは適応型セキュリティ アプライアンスの DMZ インターフェイスにある
- プライベート ネットワーク上の HTTP クライアントは DMZ にある Web サーバにアクセスでき、インターネット上のデバイスとの通信が可能
- インターネット上のクライアントは DMZ Web サーバへの HTTP アクセスが許可され、他のすべてのトラフィックは拒否される
- ネットワークには、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）と、DMZ Web サーバのパブリック IP アドレス（209.165.200.226）という、パブリックに使用可能な 2 つのルーティング可能 IP アドレスがある

図 6-2 に、DMZ Web サーバとインターネットの両方に対してプライベート ネットワークから出される HTTP 要求の発信トラフィック フローを示します。

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

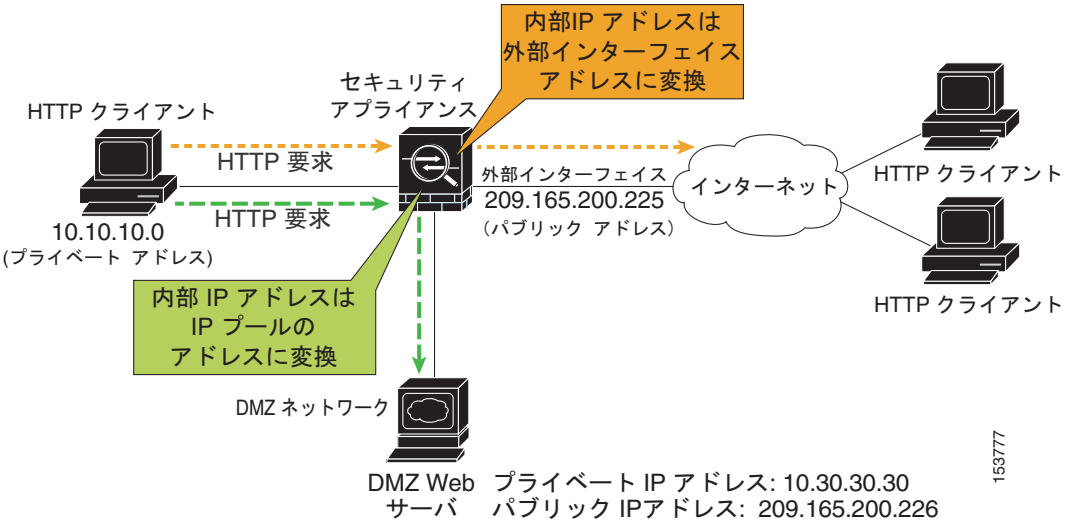


図 6-2 では、DMZ Web サーバとインターネット上のデバイスの両方を宛先として内部クライアントからトラフィックを発信することが適応型セキュリティ アプライアンスによって許可される様子を示します。トラフィックの通過を許可するために、適応型セキュリティ アプライアンスの設定には次のものが含まれます。

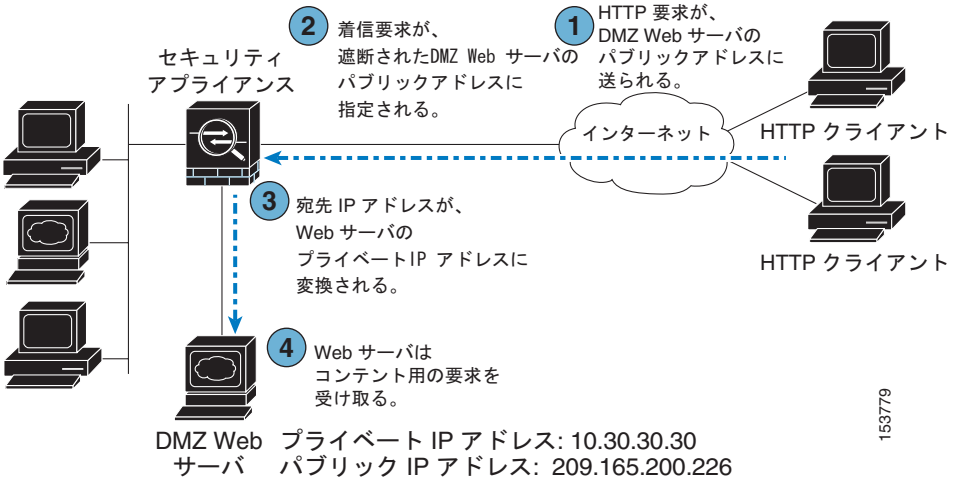
- DMZ Web サーバとインターネット上のデバイスを宛先としたトラフィックを許可するアクセス コントロール規則
- プライベート IP アドレスをプライベート アドレスがインターネットから不可視になるように変換するアドレス変換ルール

  DMZ Web サーバを宛先とするトラフィックには、プライベート IP アドレスは IP プールのアドレスに変換されます。

  インターネットを宛先とするトラフィックには、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送出されると思われます。

図 6-3 に、DMZ Web サーバのパブリック IP アドレスを宛先としてインターネットから発信される HTTP 要求の例を示します。

図 6-3　インターネットからの HTTP トラフィック フローの着信



DMZ Web サーバにアクセスする着信トラフィックを許容するための適応型セキュリティ アプライアンスの設定には次のものが含まれます。

- 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 アドレスに変換するアドレス変換ルール
- DMZ Web サーバを宛先とする HTTP トラフィックの着信を許容するアクセス コントロール規則

この設定を作成するための手順については、この章の以降のページ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

この項では、ASDM を使用して図 6-1 で示した設定シナリオ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について説明します。手順では、このシナリオに基づいたサンプル パラメータを使用します。

この設定手順では、適応型セキュリティ アプライアンスで、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のインターフェイスをすでに設定していることを前提にしています。適応型セキュリティ アプライアンス用に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。

ここでは、次のトピックについて取り上げます。

次の項では、各手順の実行方法について詳しく説明していきます。

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、次の設定タスクが必要です。

- 内部クライアントで DMZ Web サーバに HTTP アクセスできるようにするために、アドレス変換用の IP アドレスのプールを作成する必要があり、このプールのアドレスを使用するクライアントを識別する必要があります。このタスクを実行するには、次のものを設定する必要があります。
  - DMZ インターフェイスの IP アドレスのプール。このシナリオでは、IP アドレスのプールは 10.30.30.50 ～ 10.30.30.60 です。
  - IP プールからのアドレス割り当てが可能なクライアントを指定する、内部インターフェイス用のダイナミック NAT 変換ルール。
- 内部クライアントがインターネット上の HTTP リソースまたは HTTPS リソースにアクセスできるようにするために、インターネット クライアントの実 IP アドレスを送信元アドレスとして使用できる外部アドレスに変換するためのルールを作成する必要があります。

  このためには、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 PAT 変換ルール（ポート アドレス変換ルール、インターフェイス NAT と呼ばれる場合もある）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（10.10.10.0）のサブネットのアドレスです。このサブネットのアドレスは、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。
- 外部クライアントが DMZ Web サーバに HTTP アクセスできるようにするために、DMZ Web サーバの外部アイデンティティと、インターネット上のクライアントから送信される HTTP 要求を許容するアクセス ルールを設定する必要があります。このタスクを実行するには、次のものを設定する必要があります。
  - 静的 NAT ルールを作成します。このルールによって 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）。
  - トラフィックが DMZ Web サーバのパブリック IP アドレスを宛先とする HTTP 要求の場合、インターネットからのアクセスを許容するセキュリティ アクセス規則を作成します。

ASDM の設定

Web ブラウザで ASDM を実行するには、アドレス フィールドに、工場出荷時のデフォルトの 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

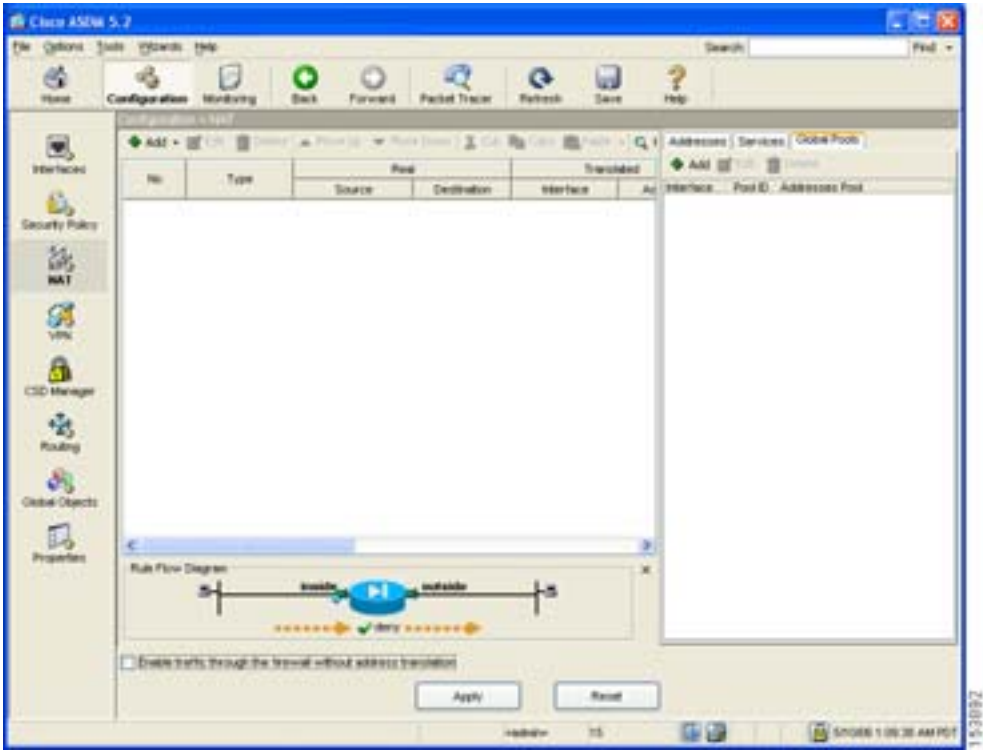
適応型セキュリティ アプライアンスは、ネットワーク アドレス変換（NAT）とポート アドレス変換（PAT）を使用して、内部 IP アドレスが外部に公開されることを防いでいます。ここでは、DMZ インターフェイスと外部インターフェイスがアドレス変換用に使用可能な IP アドレスのプールを作成する方法について説明します。

単一の IP プールに NAT エントリと PAT エントリを両方含めたり、複数のインターフェイスのエントリを含めることができます。

ネットワーク アドレス変換に使用可能な 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。

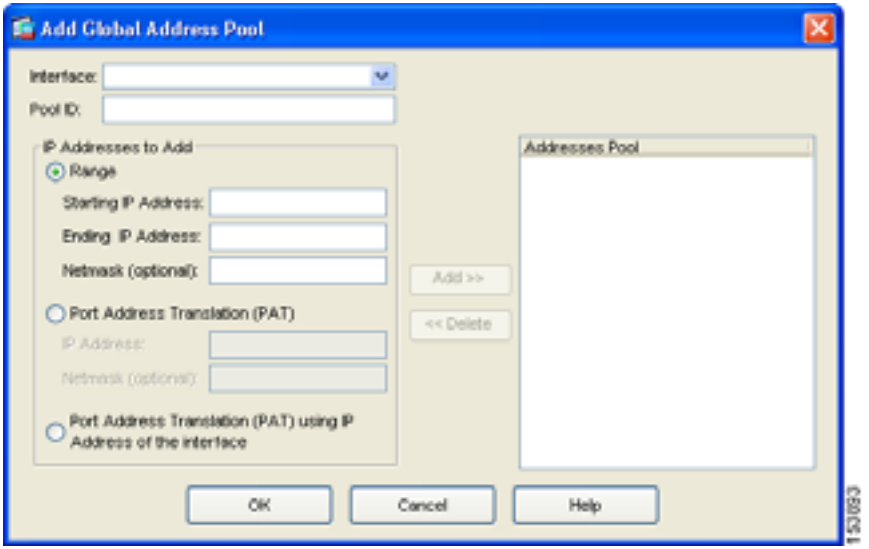


b. 右ペインで、**Global Pools** タブをクリックします。

c. **Add** をクリックして DMZ インターフェイス用のグローバル プールを新規作成します。

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 を選択します。

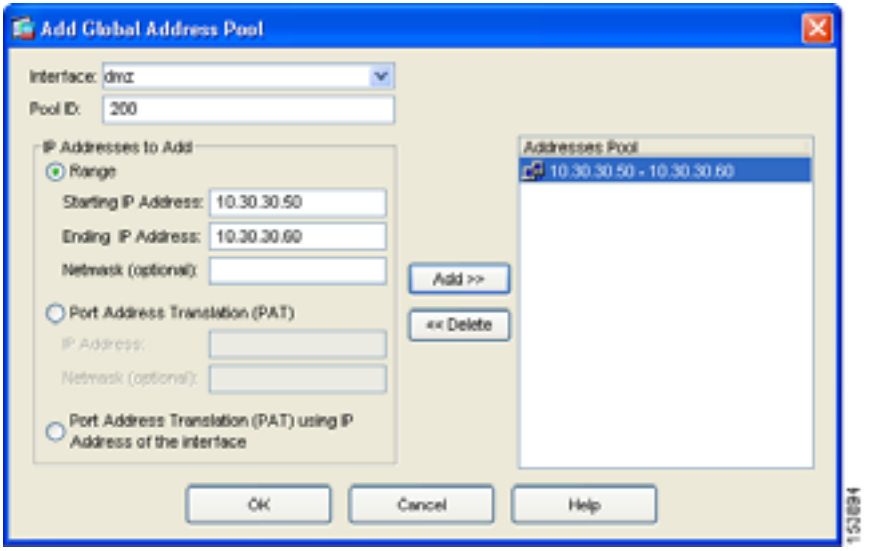
e. 新しい IP プールを作成するには、一意の Pool ID を入力します。このシナリオでは、Pool ID は 200 です。

f. IP Addresses to Add 領域で、DMZ インターフェイスで使用する IP アドレスの範囲を次のように指定します。

- **Range** オプション ボタンをクリックします。
- アドレスの範囲を指定する Starting IP Address と Ending IP Address 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 Netmask 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 Address Pool に追加します。

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



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、内部クライアントが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るように、プライベート IP アドレスを変換する目的で使用します。

このシナリオでは、使用できるパブリック IP アドレスの数が制限されています。次の手順でポート アドレス変換（PAT）を行うことで、多数の内部 IP アドレスが同じパブリック IP アドレスにマッピングできるようにします。

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。

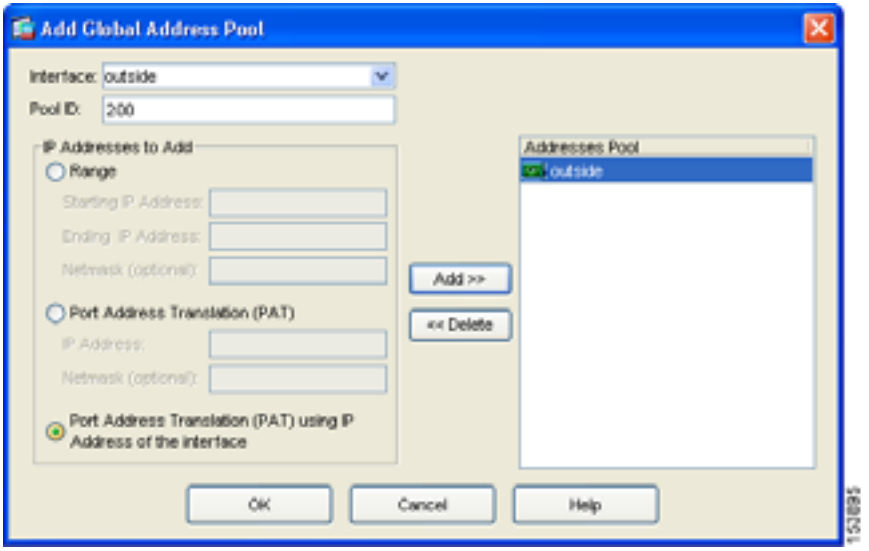
d. outside インターフェイス用の Pool ID を指定します。

DMZ インターフェイスが使用するアドレス プールが含まれる 1 つの IP プール（このシナリオでは Pool ID は 200）に、これら複数のアドレスを追加することができます。

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

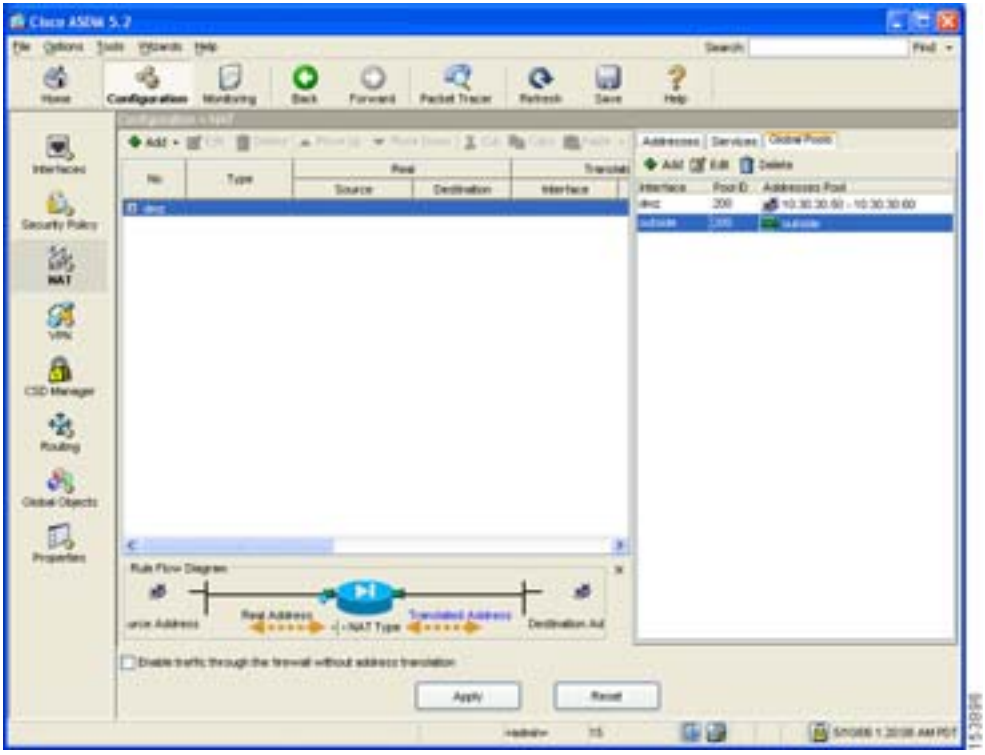
この Port Address Translation（PAT）using the IP address of the interface オプションを選択した場合、内部ネットワークから開始されたすべてのトラフィックは、外部インターフェイスの IP アドレスを使用して適応型セキュリティ アプライアンスを終了します。インターネット上のデバイスにとっては、すべてのトラフィックがこの 1 つの IP アドレスから着信しているように見えます。

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 を設定する

前述した手順では、内部クライアントのプライベート IP アドレスをマスクするために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ました。

この手順では、このプールの IP アドレスと内部クライアントとを関連付けるネットワーク アドレス変換（NAT）ルールを設定して、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。

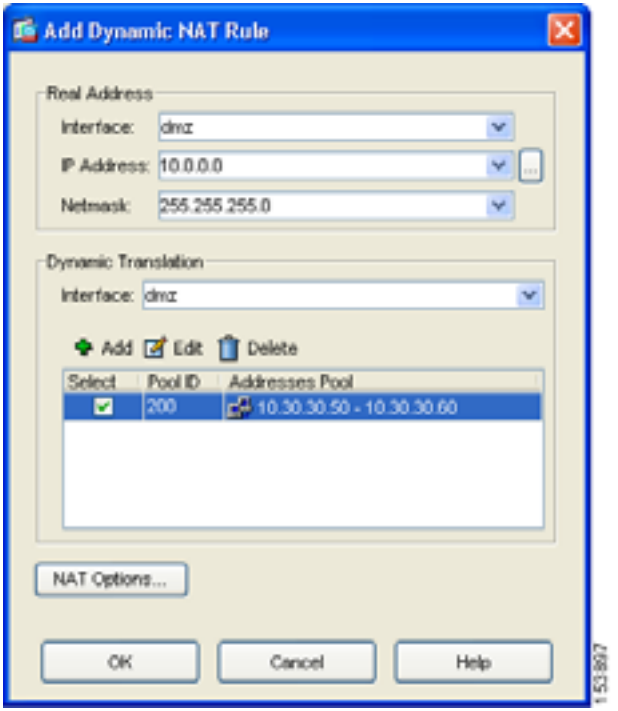
ステップ 4　Real Address 領域で変換する IP アドレスを指定します。このシナリオでは、内部クライアントのアドレス変換はサブネットの IP アドレスに従って行われます。

- **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、Netmask 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 ルールで使用するアドレス プールを指定するには、Global Pool ID の横の **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 プールの ID は 200 です。

  このシナリオでは、使用する予定の IP プールはすでに作成済みです。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 ルールを追加し、Configuration > NAT ウィンドウに戻ります。

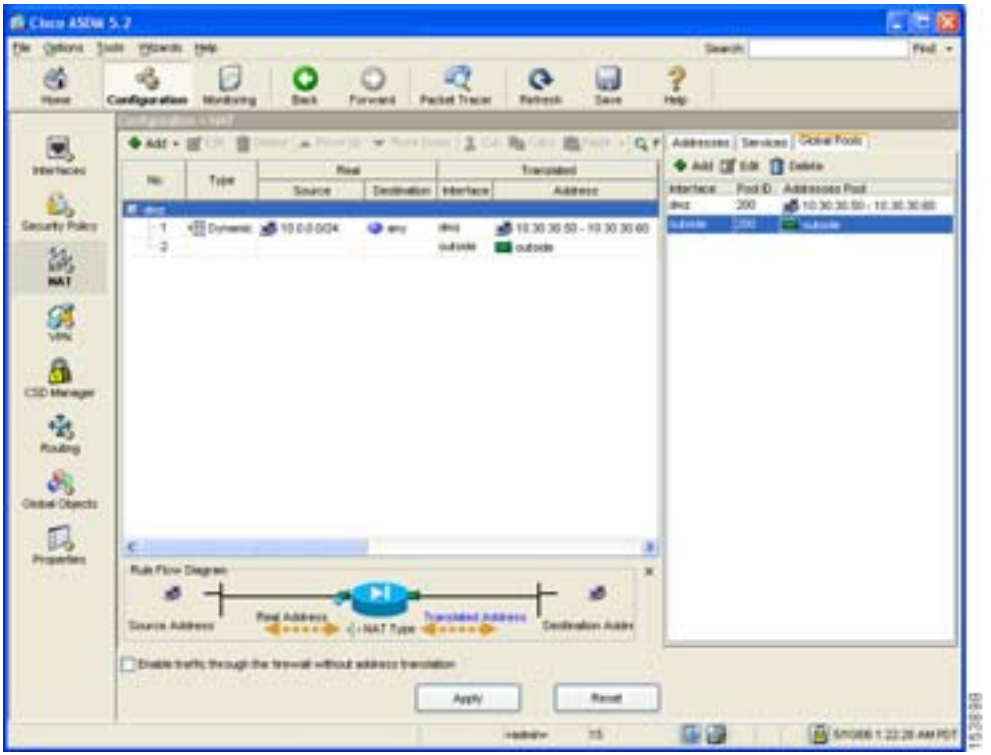
設定画面に変換ルールが予想どおりに表示されることを確認します。

（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 つの変換ルールが作成されていることが分かります。

- 内部クライアントと DMZ Web サーバが通信する場合に使用される、内部インターフェイスと DMZ インターフェイスとの間の変換ルール
- 内部クライアントがインターネットと通信する場合に使用される、内部インターフェイスと外部インターフェイスとの間の変換ルール

変換で使用されるアドレスは両方とも同じ IP プールにあるため、ASDM はこれらの両ルールを作成することができます。

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 を設定する

先ほどの手順では、IP プールの IP アドレスと内部クライアントを関連付けるネットワーク アドレス変換（NAT）ルールを設定して、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しました。

これ以外にも、内部インターフェイスと外部インターフェイスとの間に NAT ルール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多数の設定が必要になります。

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。これは、IP プール（プール ID は 200）に、アドレス変換に必要な両タイプのアドレス、つまり、DMZ インターフェイスで使用される IP アドレスの範囲と、外部インターフェイスで使用される IP アドレスの範囲の 2 種類が含まれているためです。このため、ユーザに代わって ASDM が 2 番目の変換ルールを作成することができます。

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せずに外部の 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。実 Web サーバの 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 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。

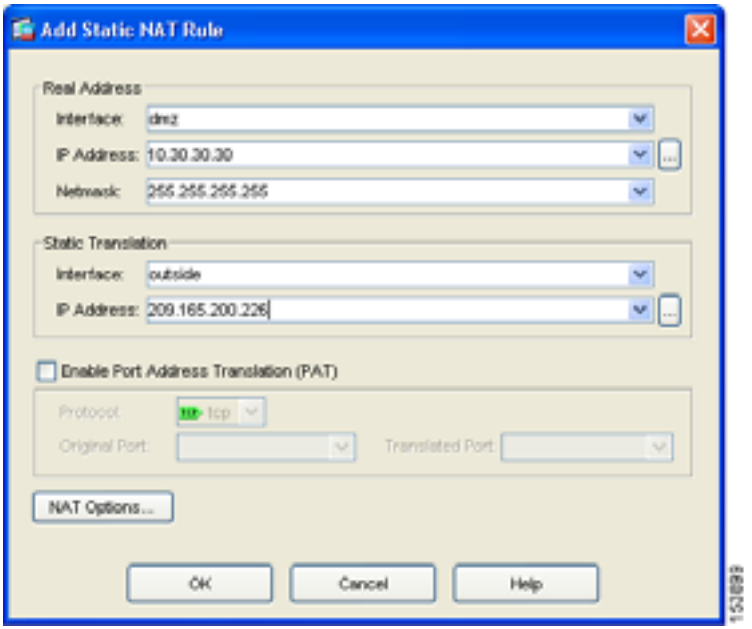
ステップ 3　Add ドロップダウン リストで、Add Static NAT Rule を選択します。Add Static NAT Rule ダイアログボックスが表示されます。

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

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、Web サーバに使用する IP アドレスを次のように指定します。

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

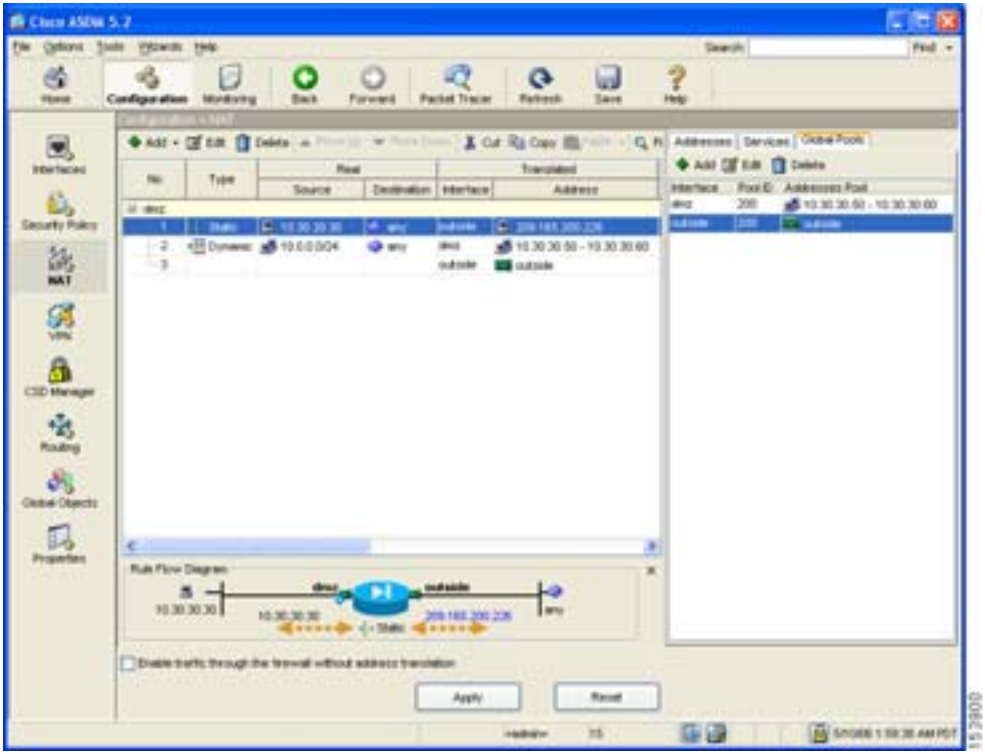
b. IP Address ドロップダウン リストで、DMZ Web サーバのパブリック IP アドレスを選択します。

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** をクリックしてルールを追加し、Address Translation Rules リストに戻ります。

このルールは実 Web サーバの 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プします。

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 のリソースに到達することを許容する必要があります。このアクセス コントロール規則によって、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を指定して、トラフィックが着信と発信のどちらか、トラフィックの発信元と宛先、トラフィック プロトコルの種類、許容すべきサービスなどについて制御します。

この項では、インターネット上の任意のホストまたはネットワークから発信される HTTP トラフィックの宛先が DMZ ネットワークの Web サーバの場合にこのトラフィックの着信を許容するアクセス規則を作成します。パブリック ネットワークからの他のすべてのトラフィックは拒否されます。

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。

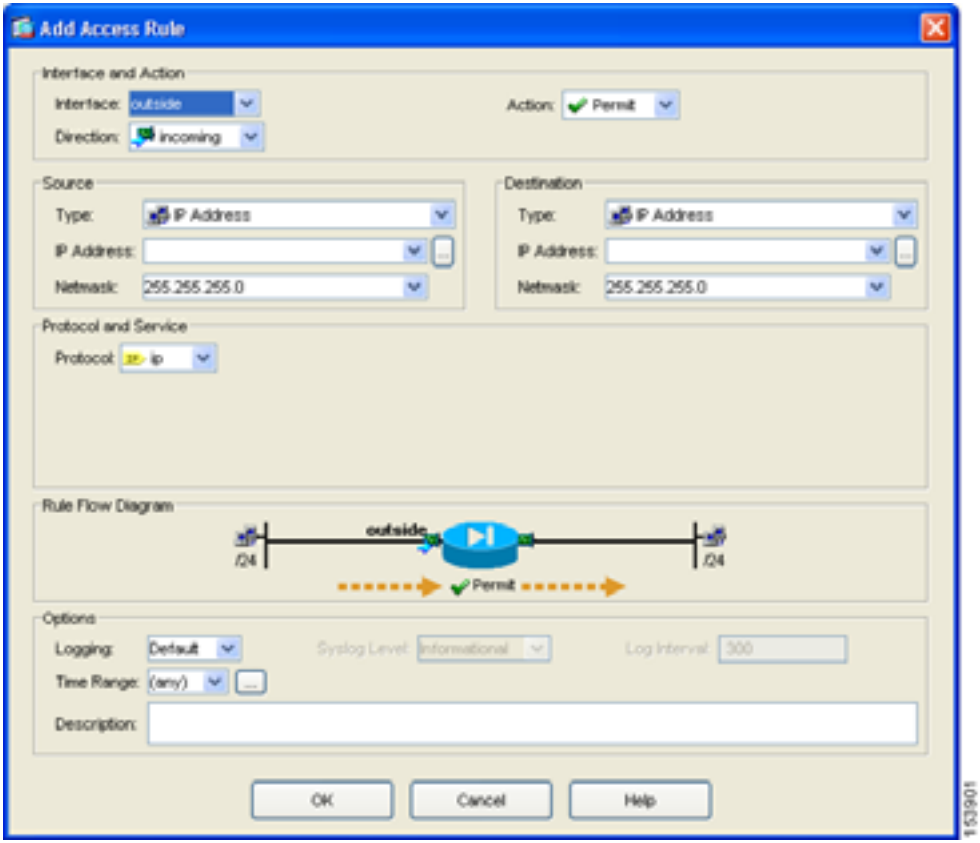
ステップ 1　ASDM ウィンドウで、次の手順を実行します。

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** タブをクリックしてから、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 をクリックします。
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ネットワークが事前設定済みの場合は、IP Address ドロップダウン リストでその発信元の IP アドレスを選択します。

c. 発信元 IP アドレス用のネットマスクを入力するか、Netmask ドロップダウン リストからいずれかを選択します。

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）。

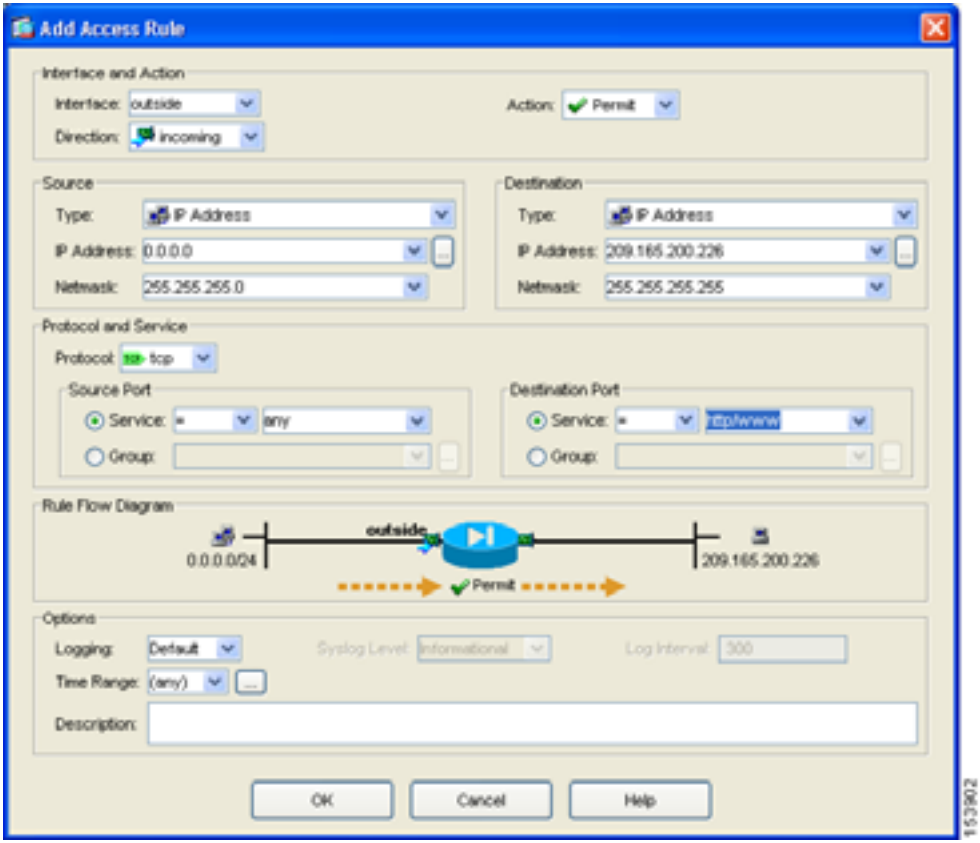
ステップ 5　Protocol and Service 領域で、適応型セキュリティ アプライアンスで許容するトラフィックの種類を指定します。

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 リストから「=」（等号）を選択してから、隣のドロップダウン リストで any を選択します。

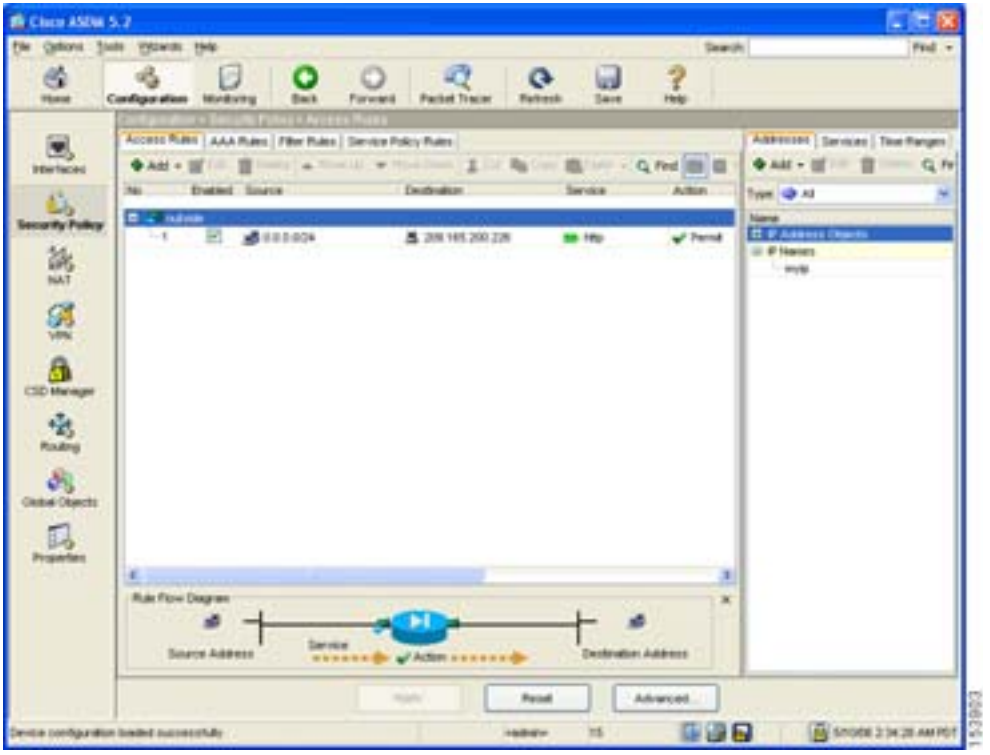
c. Destination Port 領域で、**Service** オプション ボタンをクリックし、Service ドロップダウン リストから「=」（等号）を選択してから、隣のドロップダウン リストで HTTP/WWW を選択します。

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、変更した設定を適応型セキュリティ アプライアンスで現在実行中の設定に保存します。

これで、パブリック ネットワークとプライベート ネットワークの両方のクライアントは、プライベート ネットワークの安全性を維持しながら DMZ Web サーバからのコンテンツに対する HTTP 要求を解決できるようになります。

（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 アドレスの 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。アドレス変換（209.165.200.226 から 10.30.30.30）によって、トラフィックが許可されます。変換ルールの作成の詳細については、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 を設定する」を参照してください。

ステップ 8　設定の変更をスタートアップ設定に保存して、デバイスを次回に起動したときにこの変更が適用されるようにする場合は、File メニューの **Save** をクリックします。

あるいは、ASDM の終了時に、設定の変更を保存するかどうか確認を求めるメッセージが表示されます。

設定の変更を保存しないと、次回にデバイスを起動したときに、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*

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」

CHAPTER 7

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たリモートアクセス IPsec VPN 接続の受け入れ方法について説明します。リモートアクセス VPN では、インターネットを介したセキュアな接続またはトンネルを作成し、オフサイト ユーザにセキュアなアクセスを提供できます。

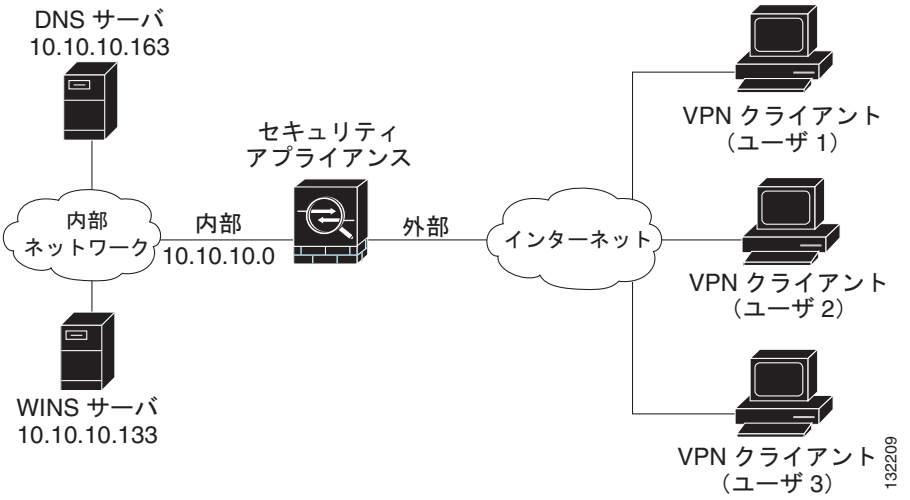
Easy VPN ソリューションを実装している場合は、この章で Easy VPN サーバ（ヘッドエンド デバイスと呼ばれる場合もあります）の設定方法を参照できます。

この章には、次の項があります。

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 で、インターネット経由で Cisco Easy VPN ハードウェア クライアントなどの VPN クライアントからの要求を受け入れ、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

この項では、リモート クライアントおよびデバイスからの IPsec VPN 接続を受け入れるための適応型セキュリティ アプライアンスの設定方法について説明します。Easy VPN ソリューションを実装している場合は、この項で Easy VPN サーバ（ヘッドエンド デバイスと呼ばれる場合もあります）の設定方法を参照できます。

設定内容の値の例は、図 7-1 に示したリモート アクセスのシナリオから使用しています。

次のトピックについて取り上げます。

必要な情報

リモート アクセス IPsec VPN 接続を受け入れるための適応型セキュリティ アプライアンスの設定を開始する前に、次の情報を用意してください。

- IP プールに使用する IP アドレスの範囲。これらのアドレスは、接続に成功したときにリモート 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するユーザのリスト（認証に AAA サーバを使用する場合を除く）
- VPN との接続時にリモート クライアントで使用する次のネットワーキング情報
  - 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

Web ブラウザで ASDM を実行するには、アドレス フィールドに、工場出荷時のデフォルトの 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。

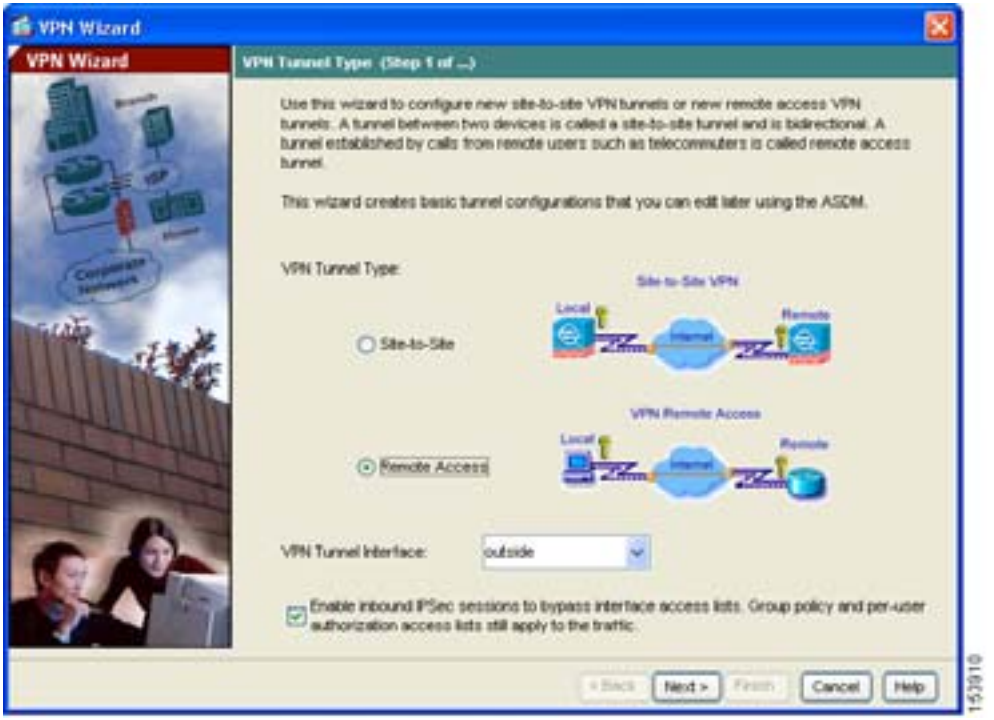
ASDM のメイン ウィンドウが表示されます。


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-IPIX
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
172.23.62.220/24
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

IPSec リモートアクセス VPN 用の ASA 5550 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。

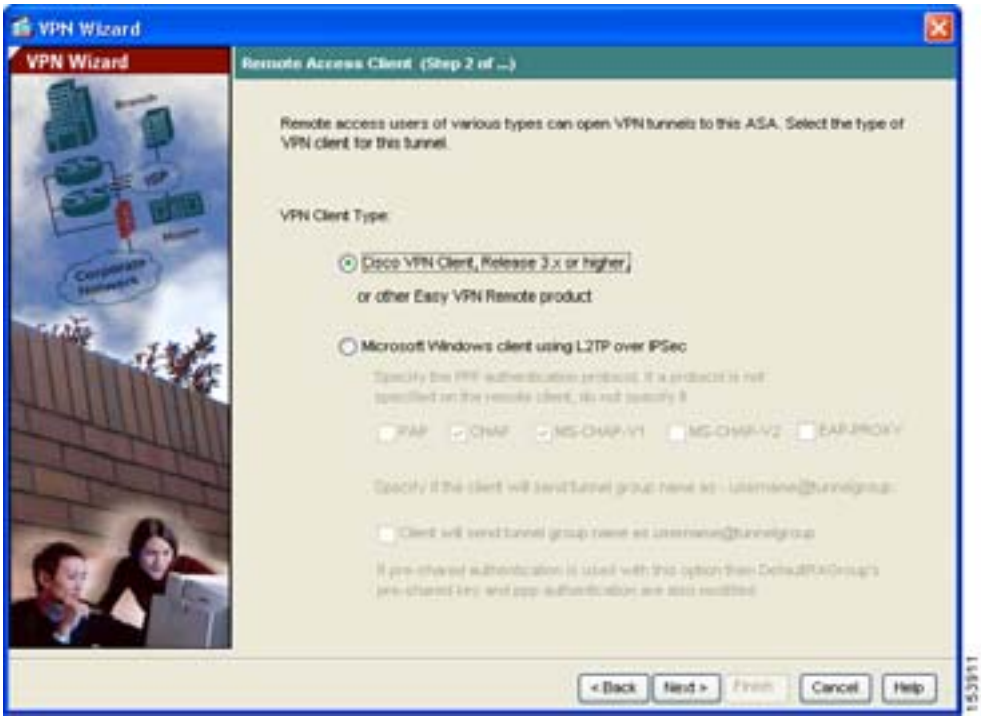
a. **Remote Access VPN** オプション ボタンをクリックします。
b. ドロップダウン リストで、着信 VPN トンネルに対してイネーブルにするインターフェイスとして outside を選択します。
c. **Next** をクリックして続行します。

VPN クライアントの種類の選択

VPN Wizard の Step 2 で、次の手順を実行します。

ステップ 1　リモート ユーザをこの適応型セキュリティ アプライアンスに接続できるようにする VPN クライアントの種類を指定します。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。

他の任意の Cisco Easy VPN Remote 製品も使用できます。



ステップ 2　**Next** をクリックして続行します。

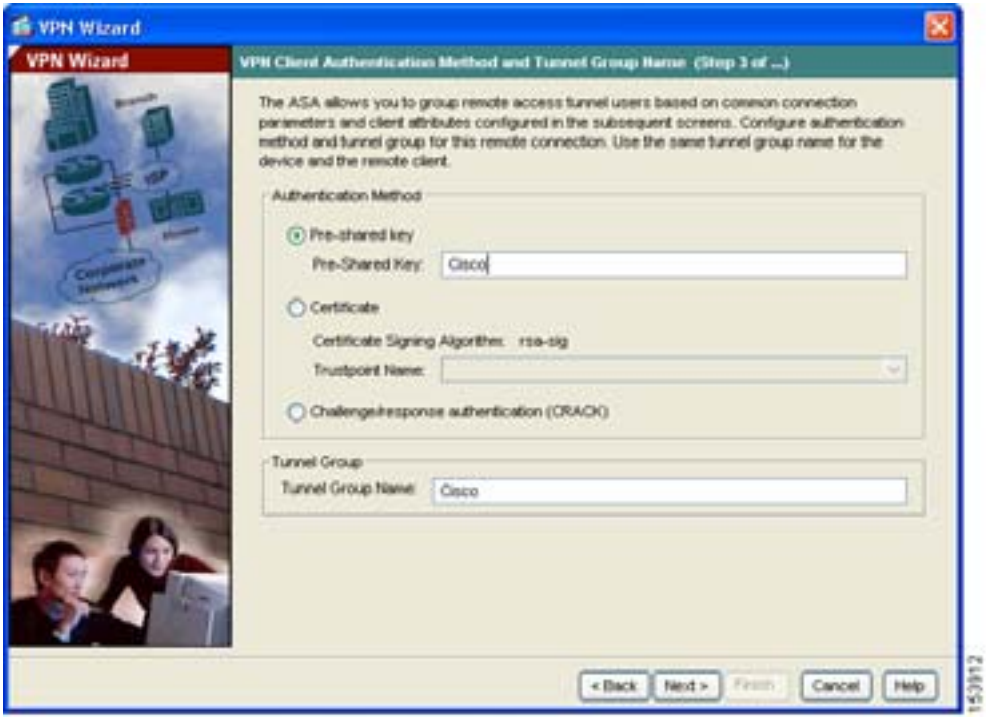
VPN トンネル グループ名と認証方式の指定

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 ネゴシエーションで使用されます。
- 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。

  デジタル証明書を認証に使用するがトラストポイント名をまだ設定していない場合は、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。認証方式の設定は、標準の ASDM 画面を使用して後で変更できます。
- **Challenge/Response Authentication (CRACK)** オプション ボタンをクリックすると、この方法で認証されます。



ステップ 2　この適応型セキュリティ　アプライアンスとの接続で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

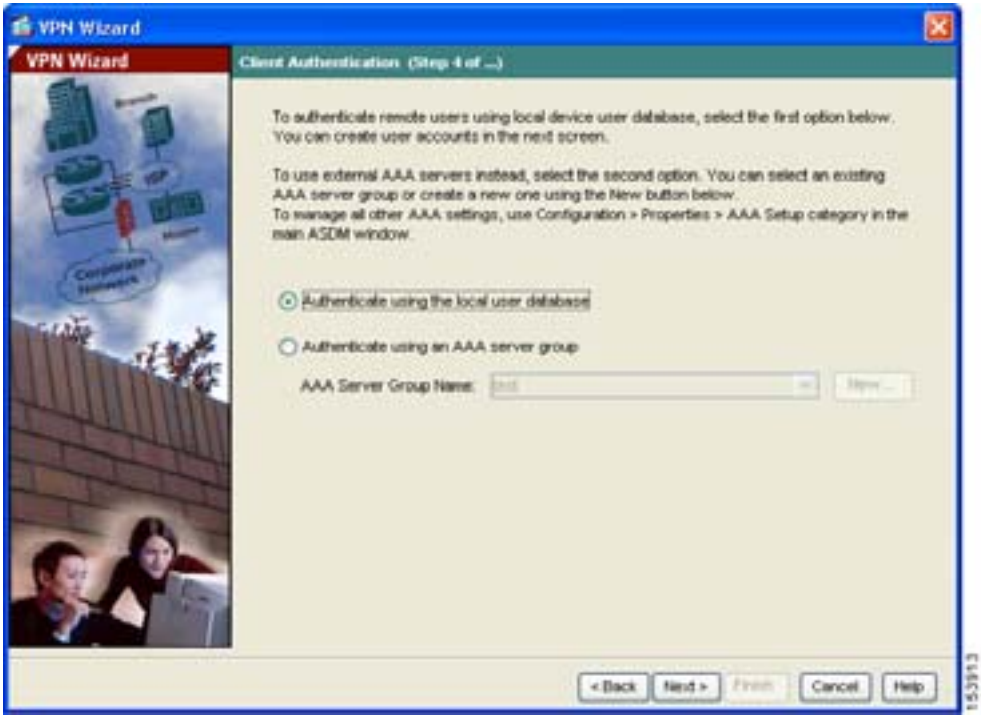
ユーザは、ローカル認証データベース、または外部認証、認可、アカウンティング（AAA）サーバ（RADIUS、TACACS+、SDI、NT、Kerberos、および LDAP）で認証できます。

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。



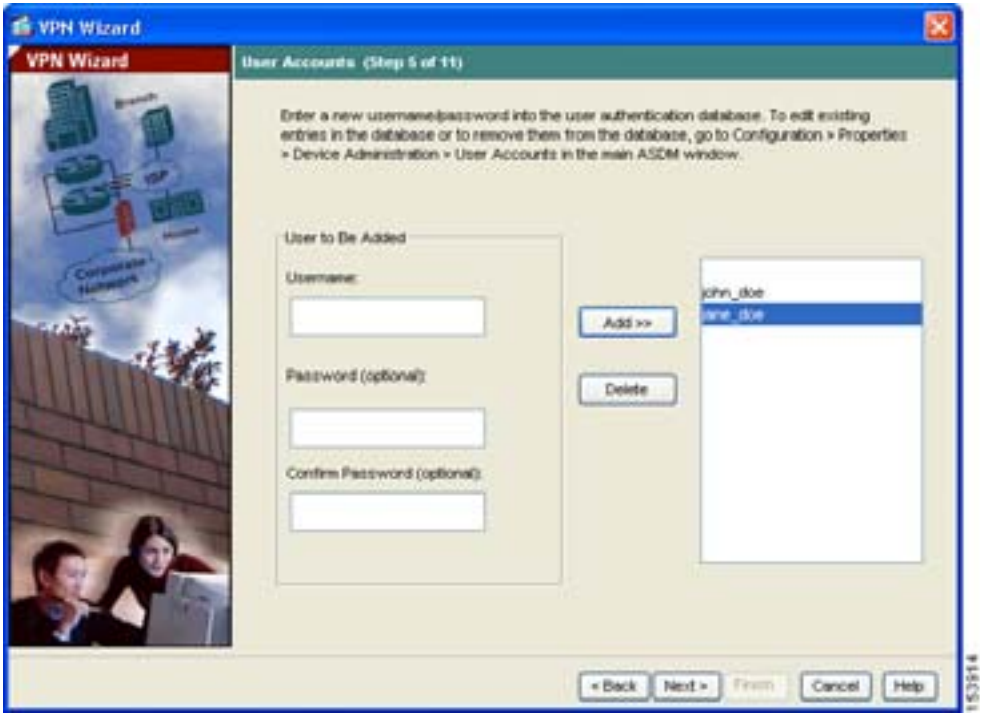
ステップ 3　**Next** をクリックして続行します。

ユーザ アカウントの設定（オプション）

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

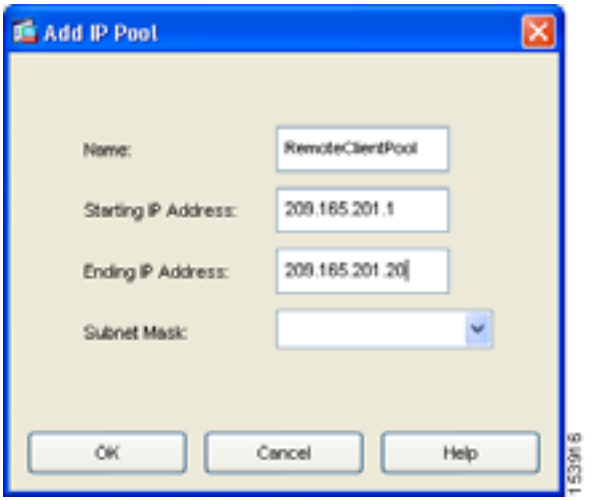
リモート クライアントがネットワークにアクセスできるようにするには、正常に接続したときにリモート VPN クライアントに割り当てることができる IP アドレスのプールを設定する必要があります。このシナリオでは、IP アドレス 209.165.201.1 ～ 209.166.201.20 を使用するようにプールを設定します。

VPN Wizard の Step 6 で、次の手順を実行します。

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

または、**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。

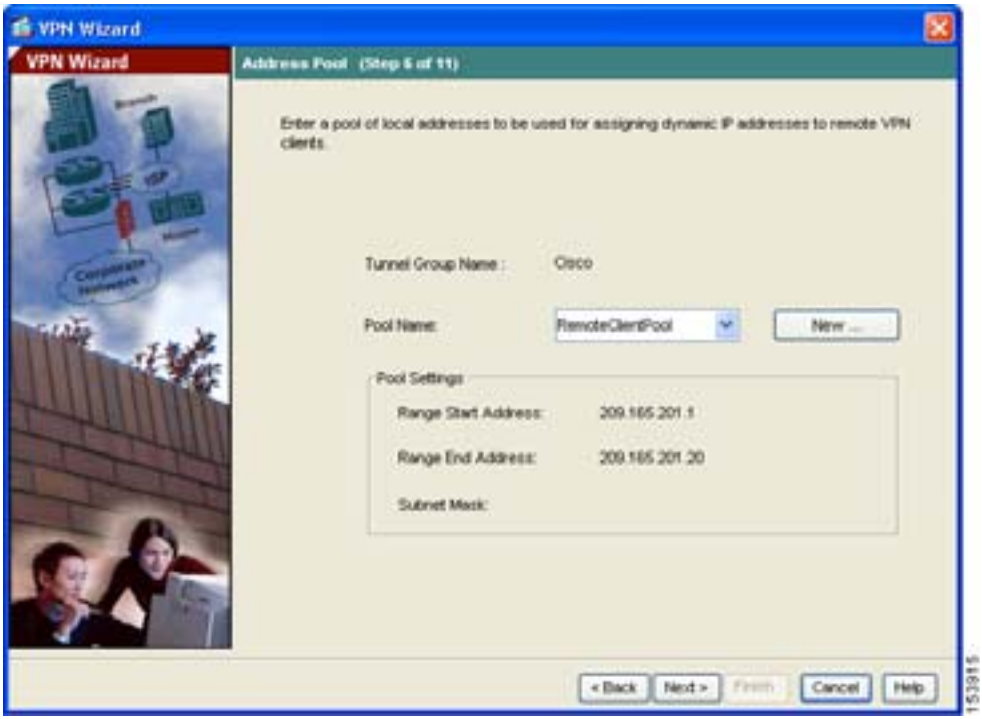


ステップ 2　Add IP Pool ダイアログボックスで、次の手順を実行します。

a.　アドレスの範囲を指定する Starting IP Address と Ending IP Address を入力します。

b. （オプション）IP アドレスの範囲の Netmask 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。

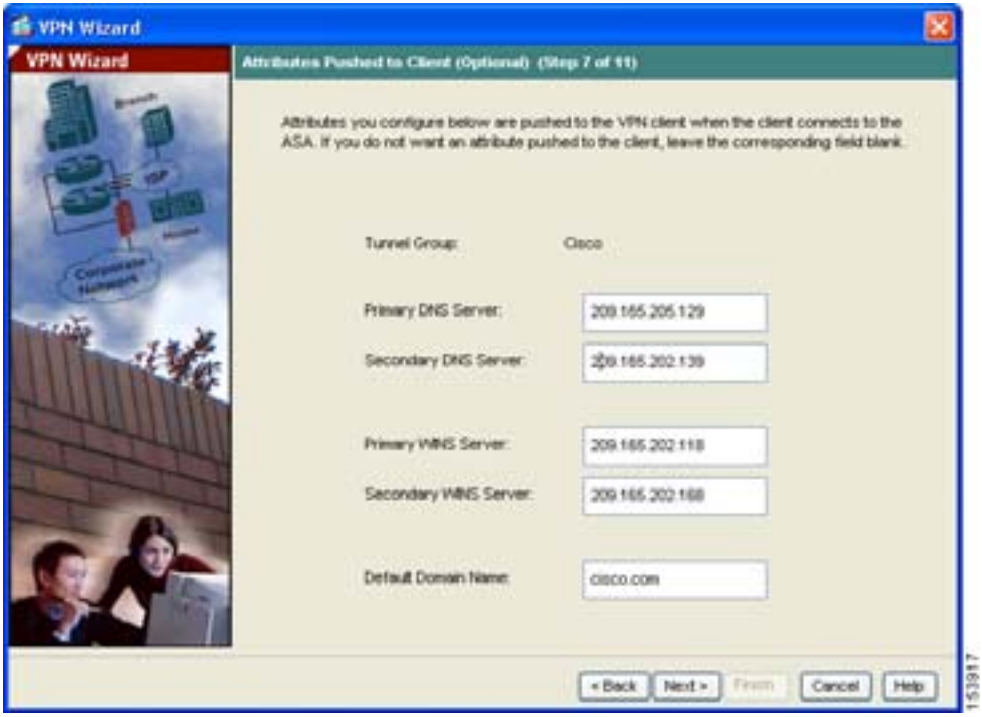
クライアント アトリビュートの設定

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。



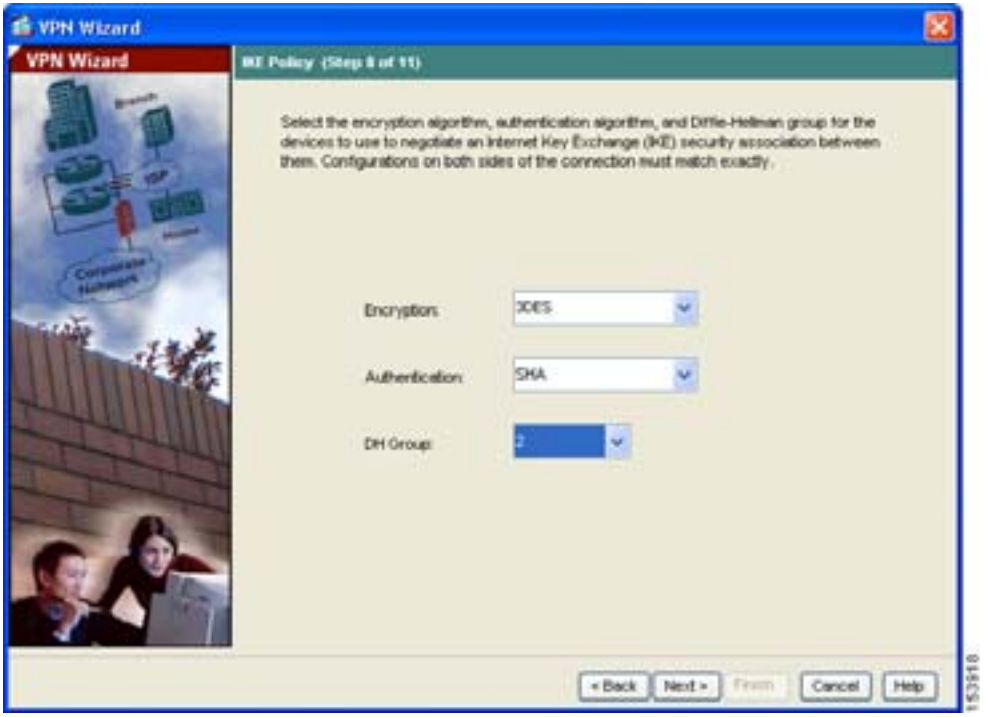
ステップ 2　**Next** をクリックして続行します。

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。

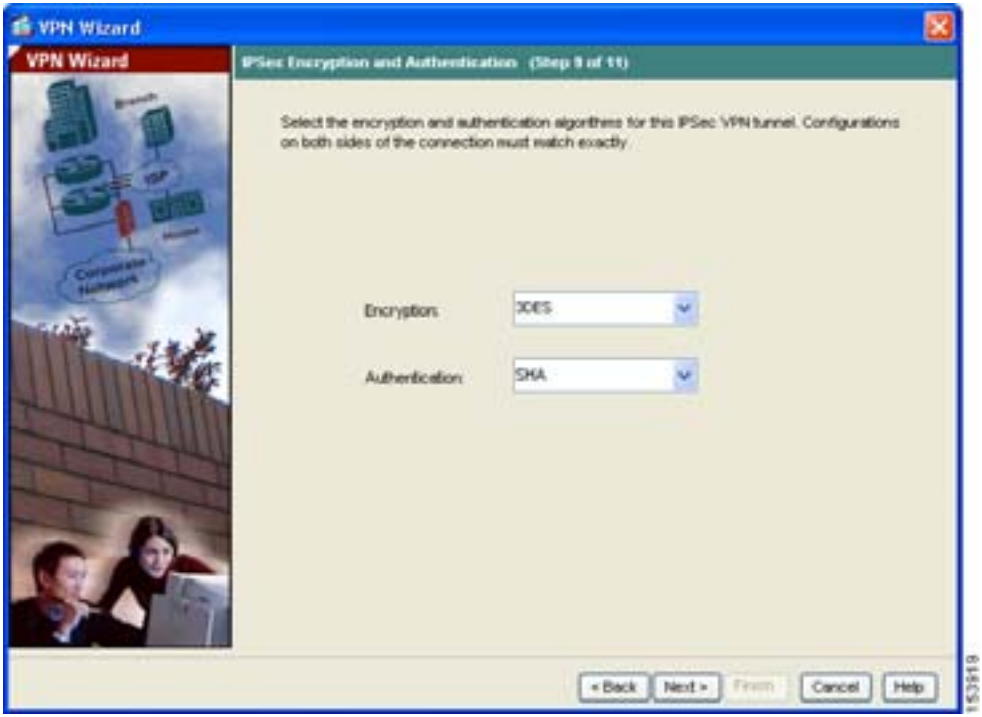


ステップ 2　**Next** をクリックして続行します。

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

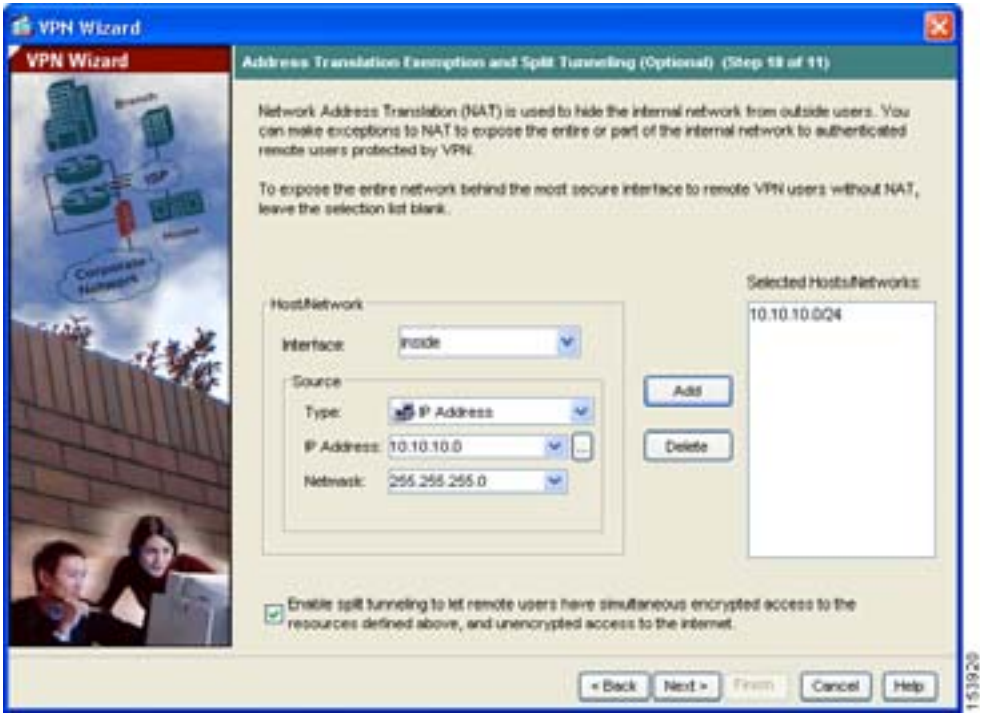
スプリット トンネリングを使用すると、リモートアクセス IPsec クライアントは IPsec トンネルを介して条件付きで暗号化形式のパケットを誘導したり、通常のテキスト形式でネットワーク インターフェイスに誘導します。

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 ユーザのアクセスを可能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特定して、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） 画面の下部の **Enable Split Tunneling** チェックボックスをオンにして、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、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。

設定の変更をスタートアップ設定に保存して、デバイスを次回に起動したときにこの変更が適用されるようにする場合は、File メニューの **Save** をクリックします。あるいは、ASDM の終了時に、設定の変更を保存するかどうか確認を求めるメッセージが表示されます。

設定の変更を保存しないと、次回にデバイスを起動したときに、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*

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たサイトツーサイト VPN の作成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。

この章には、次の項があります。

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

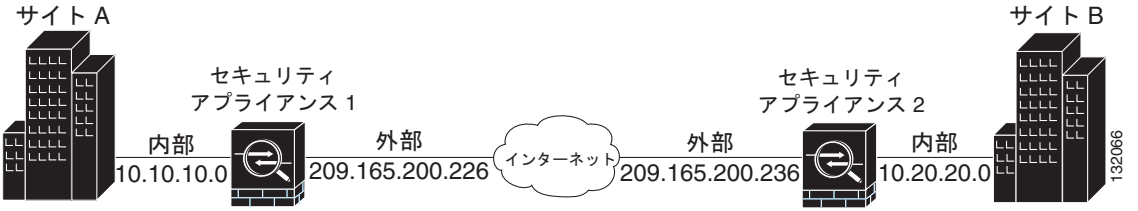


図 8-1 で示すような VPN サイトツーサイト配置の作成では、接続のそれぞれの端で 1 つずつ、合計 2 つの適応型セキュリティ アプライアンスを設定する必要があります。

サイトツーサイトのシナリオの実装

この項では、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を取り上げます。

必要な情報

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 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について説明します。

次のトピックについて取り上げます。

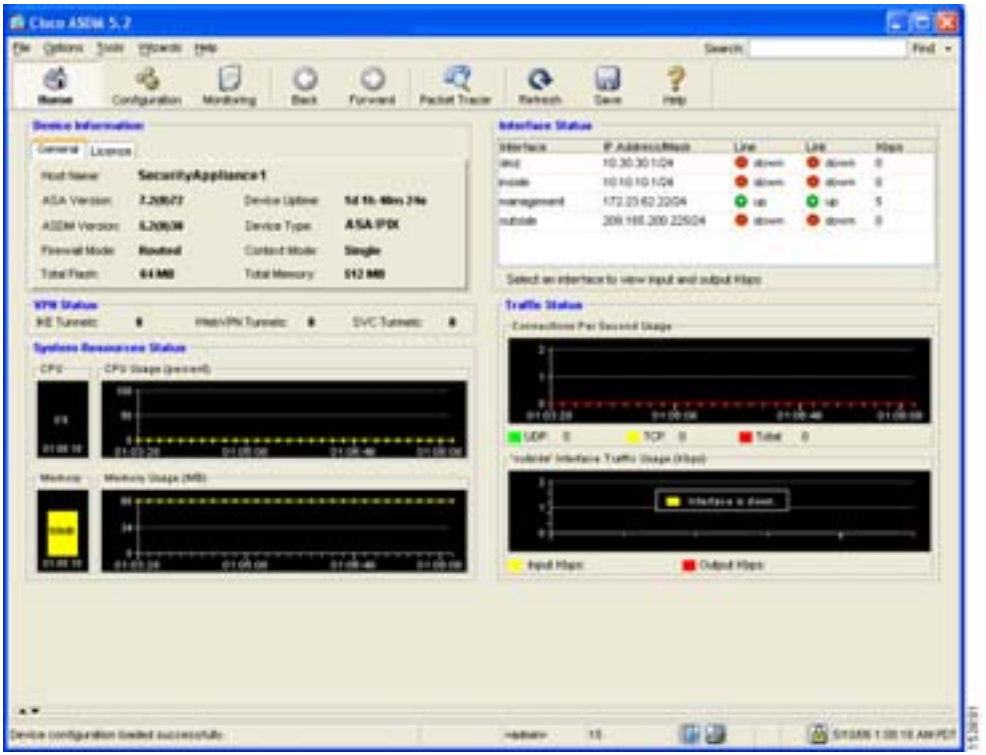
次の項では、各設定手順の実行方法について詳しく説明します。

ASDM の起動

Web ブラウザで ASDM を実行するには、アドレス フィールドに、工場出荷時のデフォルトの 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。

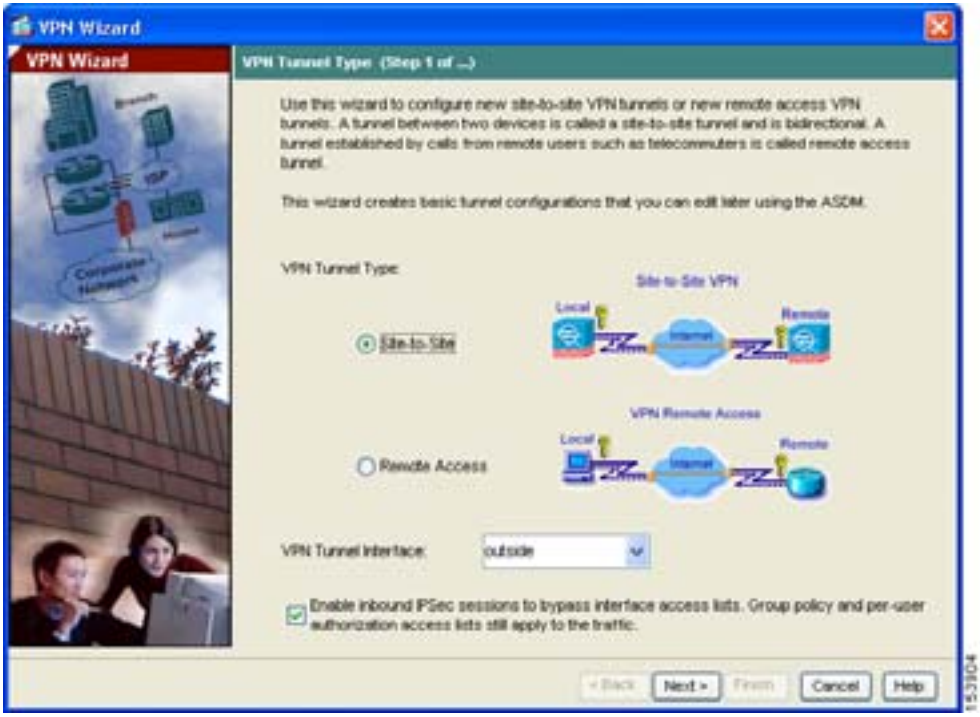
ステップ 1　ASDM のメイン ウィンドウの Wizards ドロップダウン リストで、VPN Wizard オプションを選択します。最初の VPN Wizard 画面が表示されます。

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　Peer IP Address （セキュリティ アプライアンス 2 の IP アドレス。このシナリオでは 209.165.200.236）と、Tunnel Group Name （「Cisco」など）を入力します。

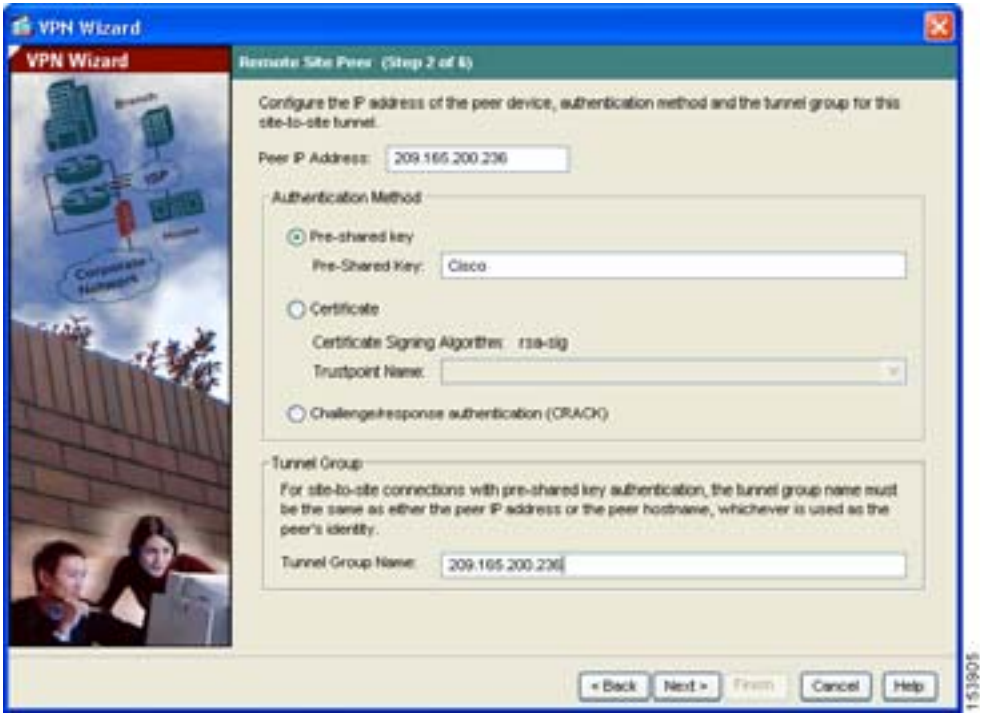
ステップ 2　次の手順のいずれかを実行して、使用する認証の種類を指定します。

- 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 ネゴシエーションで使用されます。

  （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 ボタンをクリックすると、この方法で認証されます。
- 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。

  デジタル証明書を認証に使用するがトラストポイント名をまだ設定していない場合は、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。認証方式の設定は、標準の ASDM 画面を使用して後で変更できます。



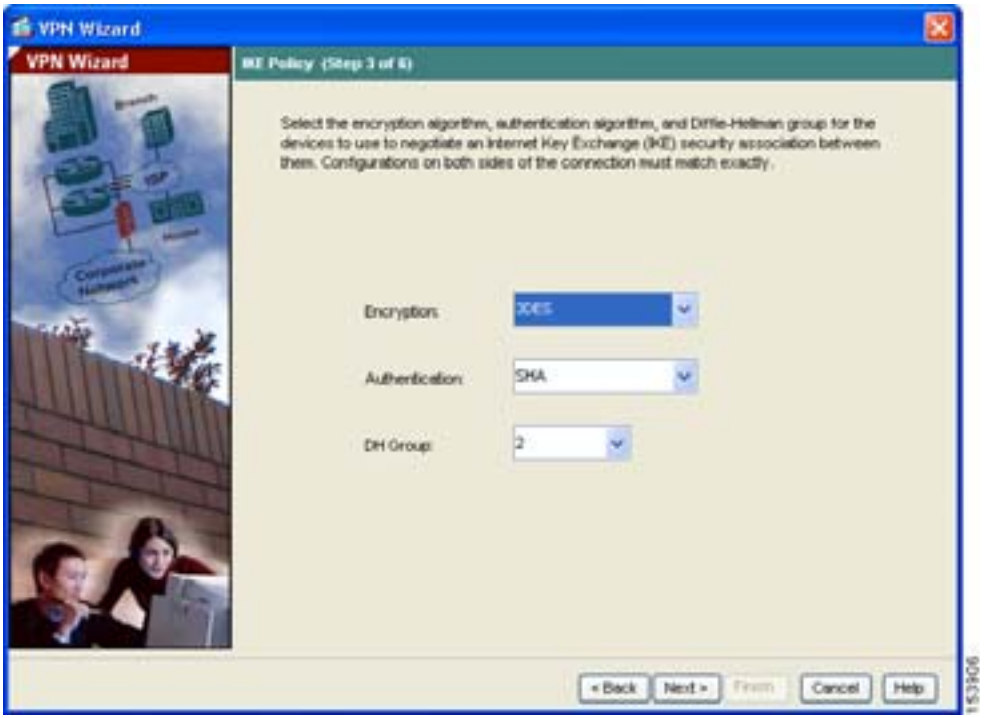
ステップ 3　**Next** をクリックして続行します。

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。



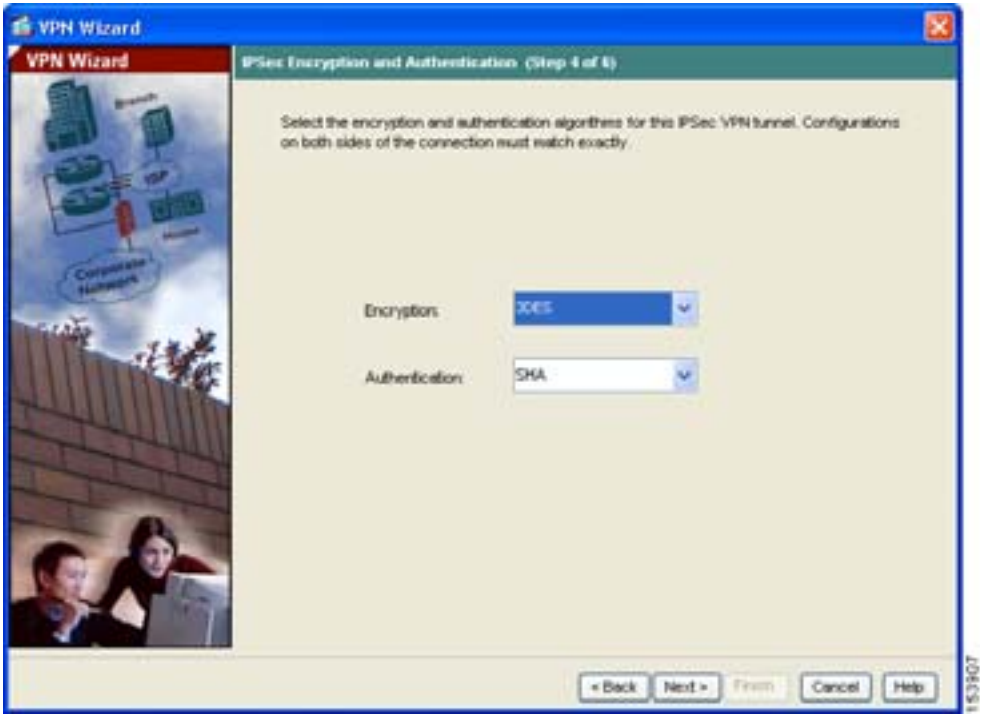
（注）　セキュリティ アプライアンス 2 を設定するときは、セキュリティ アプライアンス 1で選択した各オプションの値を正確に入力する必要があります。暗号化の不一致は、VPN トンネル障害のよくある原因で、設定プロセスを遅らせる原因になります。

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　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）をそれぞれのドロップダウン リストから選択します。



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。

さらに、この IPsec トンネルを使用してローカル ホストおよび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。

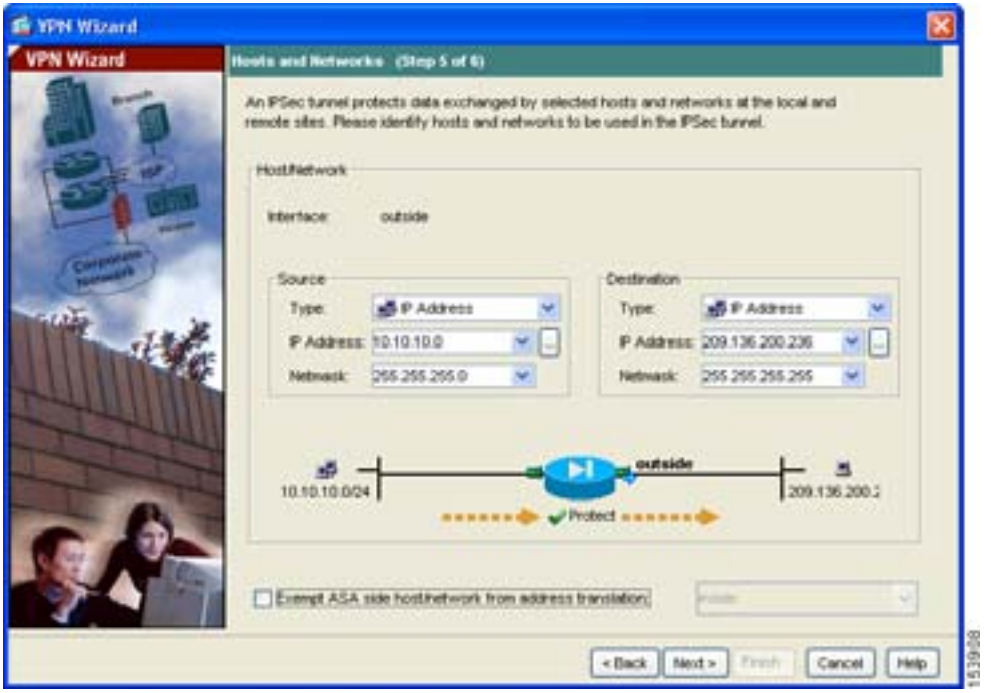
VPN Wizard の Step 5 で、次の手順を実行します。

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

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

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

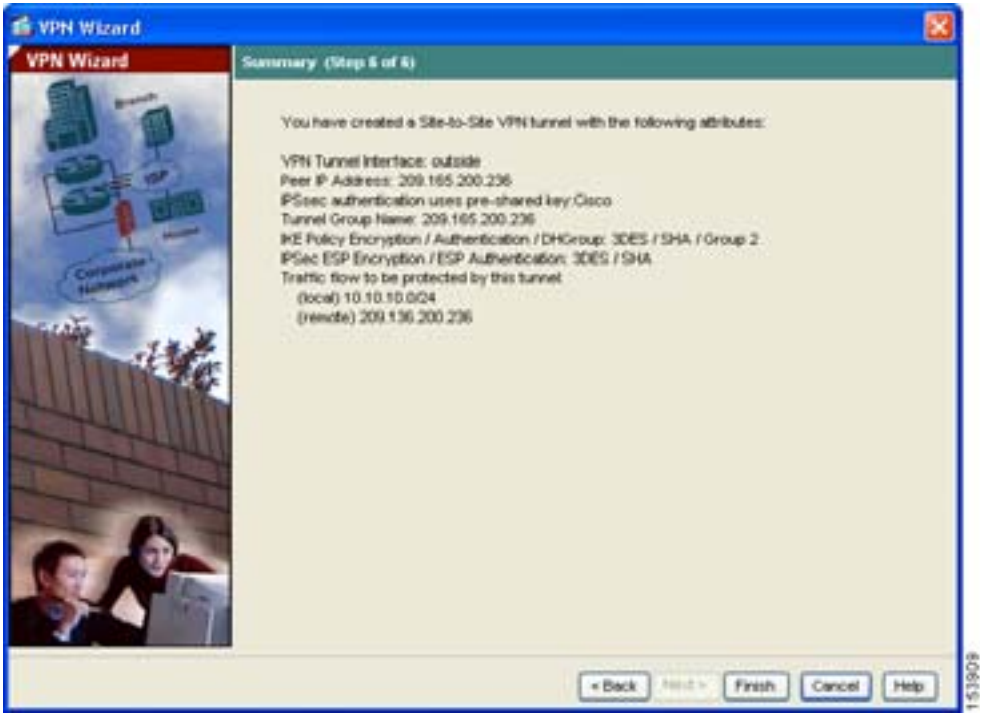
ステップ 4　リモート ホストまたはネットワークの IP アドレスおよびネットマスクを入力します。



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、設定の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。



設定の変更をスタートアップ設定に保存して、デバイスを次回に起動したときにこの変更が適用されるようにする場合は、File メニューの **Save** をクリックします。

あるいは、ASDM の終了時に、設定の変更を保存するかどうか確認を求めるメッセージが表示されます。

設定の変更を保存しないと、次回にデバイスを起動したときに、以前の設定が有効になります。

これで、セキュリティ 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

これで、ローカルな適応型セキュリティ アプライアンスが設定されました。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.8-12 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*

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」

次の手順

APPENDIX A

DES ライセンスまたは 3DES-AES ライセンスの取得

Cisco ASA 5550 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 などの特定の機能をイネーブルにする暗号化技術を提供する、DES または 3DES-AES のライセンスがあります。ライセンスは暗号化ライセンス キーでイネーブルになります。

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 3DES または 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。