Cisco ASA 5500 シリーズ スタートアップ ガイド

For the Cisco ASA 5510, ASA 5520, ASA 5540, and ASA 5550

Software Version 8.0

Customer Order Number: DOC-J-7818002=
Text Part Number: 78-18002-01-J

CONTENTS

CHAPTER 1

始める前に

次の表を使用して、Cisco ASA 5500 シリーズ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設定の手順を確認してください。

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 4 章「ASA 5500、ASA 5510、ASA 5520 および ASA 5540 の設置」
インターフェイス ケーブルの接続	第 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームでのインターフェイス 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 7 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 8 章「シナリオ：DMZ の設定」 第 9 章「シナリオ：IPSec リモートアクセス VPN の設定」 第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」 第 11 章「シナリオ：SSL VPN クライアントレス接続」 第 12 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 4 章「ASA 5500、ASA 5510、ASA 5520 および ASA 5540 の設置」
AIP SSM の取り付け	第 5 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 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームでのインターフェイス 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 7 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「シナリオ：IPSec リモートアクセス VPN 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 4 章「ASA 5500、ASA 5510、ASA 5520 および ASA 5540 の設置」
CSC SSM の取り付け	第 5 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 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームでのインターフェイス 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 7 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 14 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 4 章「ASA 5500、ASA 5510、ASA 5520 および ASA 5540 の設置」
4GE SSM の取り付け	第 5 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 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームでのインターフェイス 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 7 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 5 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*

ASA 5550

作業内容	参照先
シャーシの設置 インターフェイス ケーブルを接続した光ファイバ モジュールの取り付け	第 3 章「ASA 5550 の取り付け」
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 7 章「適応型セキュリティ アプライアンスの設定」
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

ASA 5550 のスループットの最大化

(注) この章は、Cisco ASA 5550 のみに適用されます。

この章で説明されているガイドラインに従って設定すると、Cisco ASA 5550 適応型セキュリティ アプライアンスは、スループットが最大になるように設計されています。

この章は、次の項で構成されています。

組み込みネットワーク インターフェイス

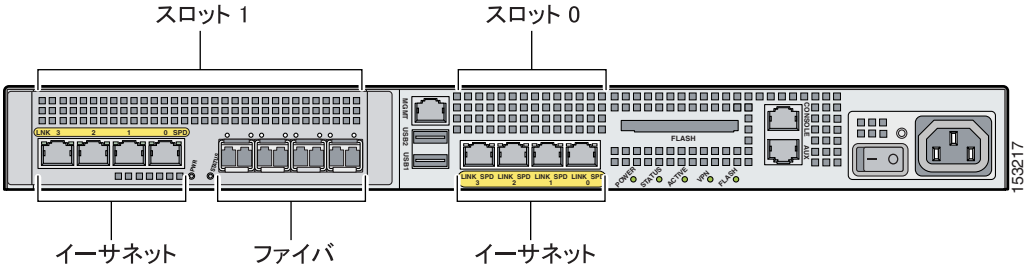
適応型セキュリティ アプライアンスには次の 2 つの内部バスがあり、銅線ギガビット イーサネットとファイバ ギガビット イーサネットを接続できるようになっています。

- スロット 0（バス 0 に対応）には、4 つの組み込み銅線ギガビット イーサネット ポートがある。
- スロット 1（バス 1 に対応）には、4 つの組み込み銅線ギガビット イーサネット ポートと、ファイバ ギガビット イーサネット接続をサポートする 4 つの組み込み SFP がある。

（注） 適応型セキュリティ アプライアンスでファイバ接続を確立するには、使用するファイバ ポートごとに SFP モジュールを注文して設置する必要があります。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。

図 2-1 は、Cisco ASA 5550 の組み込みポートを示しています。

図 2-1　ASA 5550 の組み込みポート



（注） スロット 1 には 4 つの銅線イーサネット ポートと 4 つのファイバ イーサネット ポートがありますが、一度に使用できるのは 4 つの ポートだけです。たとえば、スロット 1 の 2 つの銅線ポートと 2 つのファイバ ポートを使用できますが、すでにスロット 1 の 4 つの銅線ポートをすべて使用している場合、ファイバ ポートは使用できません。

スループットを最大化するためのトラフィックのバランシング

トラフィック スループットを最大化するには、トラフィックが 2 つのバス間で均一に分散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。これを達成するには、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）を通過し、一方のバスから入ってもう一方のバスから出るようにネットワークを配置します。

図 2-2 と 図 2-3 では、すべてのトラフィックがデバイスの両方のバスを通過し、適応型セキュリティ アプライアンスが最大スループットを実現するように、ネットワーク トラフィックが分散されています。

図 2-2　最大スループットのために均一に分散したトラフィック（銅線から銅線）

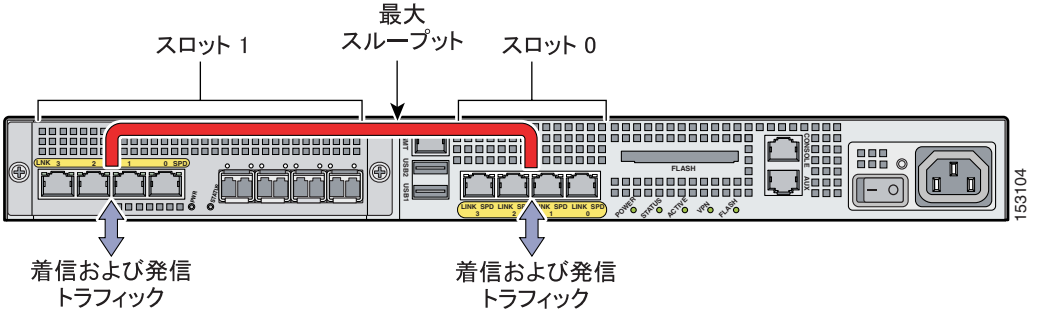


図 2-3　最大スループットのために均一に分散したトラフィック（銅線からファイバ）

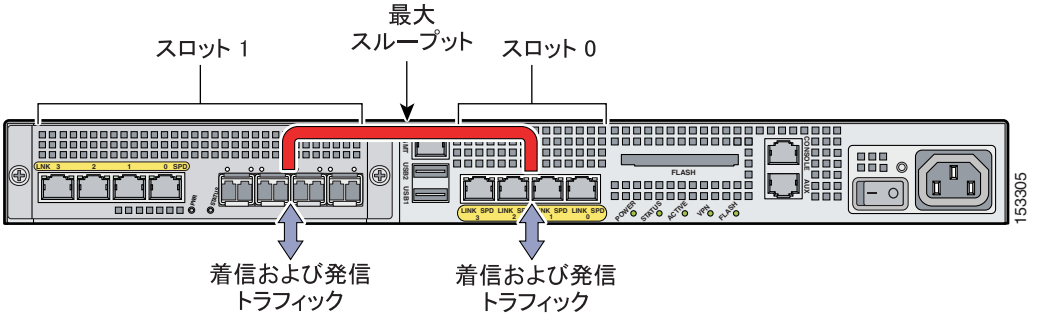
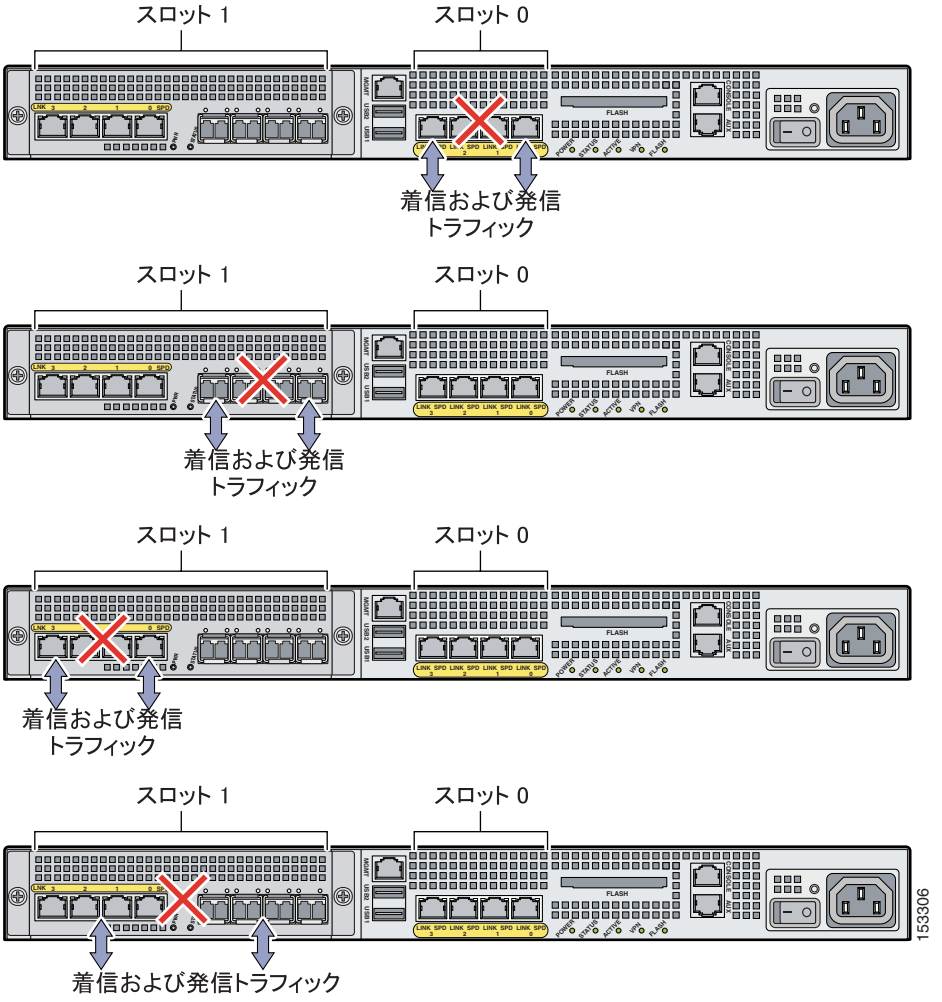


図 2-4 は、ネットワーク トラフィックが 1 つのバスしか通過しないために、適応型セキュリティ アプライアンスが最大スループットを実現できない設定をいくつか示しています。

図 2-4　最大スループットを実現できない設定



(注) **show traffic** コマンドを使用すると、各バス上のトラフィック スループットを確認できます。このコマンドの使用方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「ASA 5550 の取り付け」に進みます。

CHAPTER 3

ASA 5550 の取り付け

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。

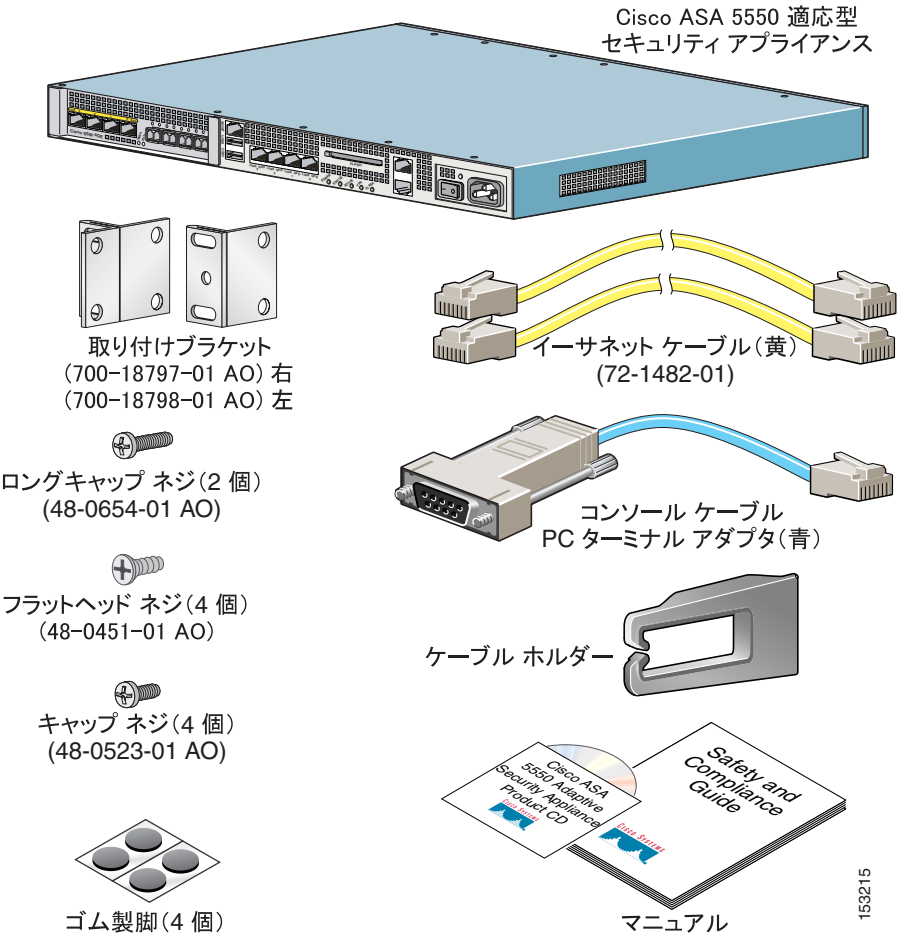
警告 **この機器の設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。ステートメント** 49

この章では、ASA 5550 適応型セキュリティ アプライアンスについて説明し、適応型セキュリティ アプライアンスのラックマウントと設定の手順について示します。この章は、次の項で構成されています。

パッケージ内容の確認

図 3-1 に示すように、梱包箱の内容を確認し、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。

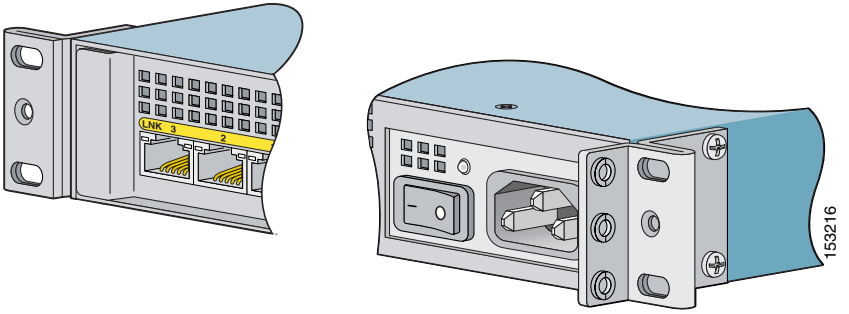
警告　**次のいずれかの手順を実行する前に、電源が切断されていることを確認してください（AC または DC）。電源を DC 回路から確実に切断するには、パネル ボード上で DC 回路に対応している回路ブレーカーを確認して、回路ブレーカーを OFF の位置に切り替え、回路ブレーカーのスイッチ ハンドルを OFF の位置のままテープで固定します。**

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。

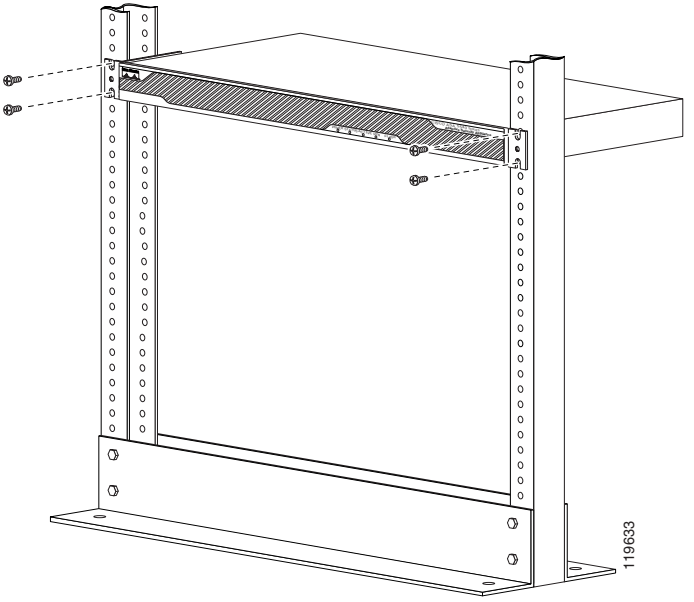
ステップ 1　付属のネジを使用して、シャーシにラックマウント ブラケットを取り付けます。ブラケットを穴に取り付けます（図 3-2 を参照してください）。ブラケットをシャーシに固定すると、ラックマウントできるようになります。

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

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。

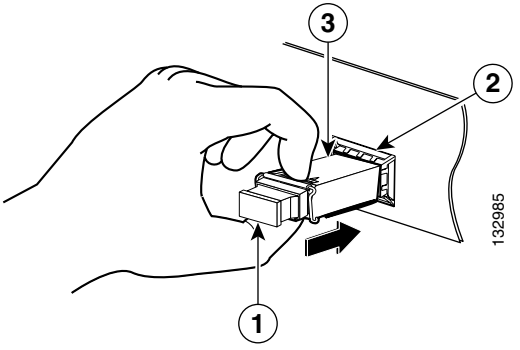
警告　**ケーブルが接続されていない場合、ポートの開口部からは目に見えないレーザー光が放射されている可能性があります。レーザー光に当たらないようにし、開口部をのぞきこまないでください。**ステートメント 70

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、次の手順を実行します。

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 3 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 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 モジュール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。

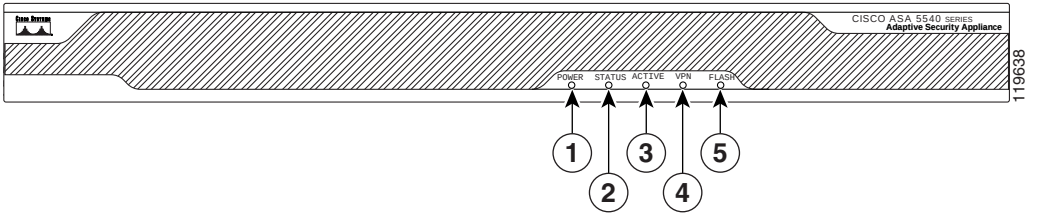
ポートと LED

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。この項では、次のトピックについて取り上げます。

前面パネルの LED

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

図 3-5　前面パネルの LED

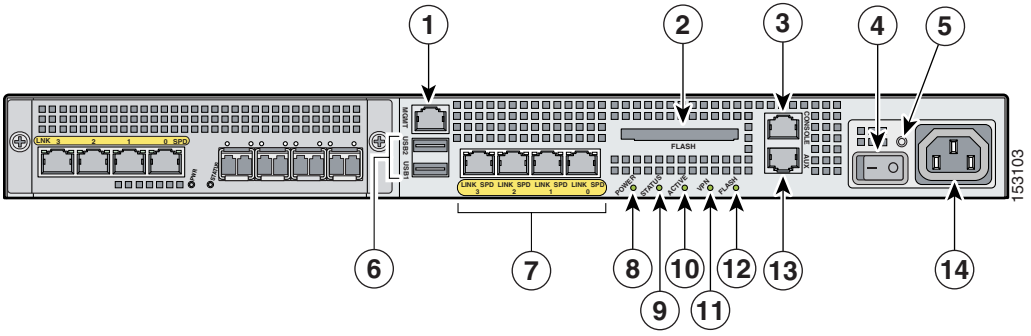


	LED	色	ステート	説明
1	電源	緑	点灯	システムは通電状態です。
2	ステータス	緑	点滅	電源投入診断を実行中か、システムがブート中です。
			点灯	システムは電源投入診断に合格しました。
		オレンジ	点灯	電源投入診断に合格しませんでした。
3	アクティブ	緑	点滅	ネットワーク アクティビティが発生しています。
4	VPN	緑	点灯	VPN トンネルが確立されました。
5	フラッシュ	緑	点灯	CompactFlash がアクセスされています。

背面パネルの LED およびスロット 0 のポート

図 3-6 は、背面パネルの LED およびスロット 0 のポートを示しています。

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）



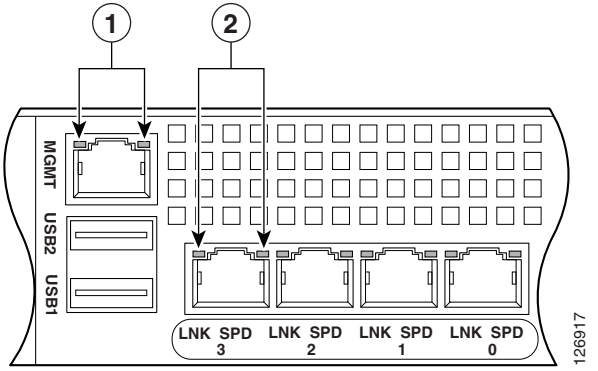
1	管理ポート[1]	**6**	USB 2.0 インターフェイス[2]	**11**	VPN LED
2	外部 CompactFlash スロット	**7**	ネットワーク インターフェイス[3]	**12**	フラッシュ LED
3	シリアル コンソール ポート	**8**	電源インジケータ LED	**13**	補助ポート
4	電源スイッチ	**9**	ステータス インジケータ LED	**14**	電源コネクタ
5	電源インジケータ LED	**10**	アクティブ LED		

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します。
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。

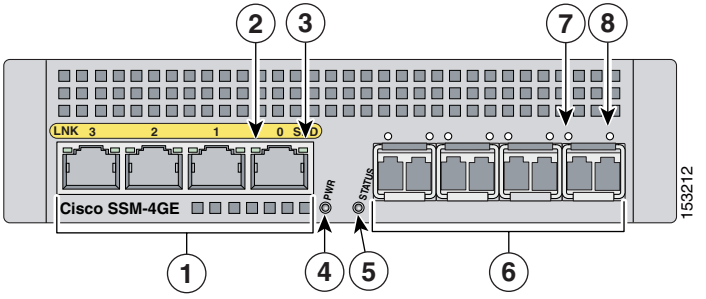
表 3-3　リンクおよび速度の LED

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

ポートおよびスロット 1 の LED

図 3-8 は、ポートおよびスロット 1 の LED を示しています。

図 3-8　ポートおよびスロット 1 の 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、ファイバ 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て取り付ける必要があります。ファイバ ポートおよび 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 は、スロット 1 の LED について説明しています。

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。

インターフェイス ケーブルの接続

この項では、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。

ケーブルをネットワーク インターフェイスに接続するには、次の手順を実行します。

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、デバイス管理のための専用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。

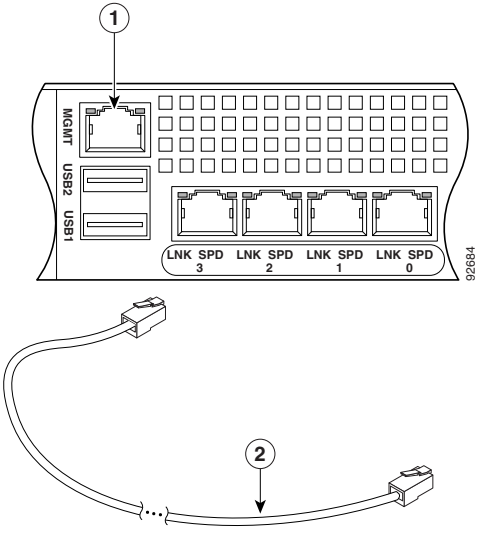
（注）　インターフェイスを管理専用インターフェイスとして設定するには、**management-only** コマンドを使用します。管理インターフェイスの管理専用モードをディセーブルにすることもできます。このコマンドの詳細については、『*Cisco Security Appliance Command Reference*』の **management-only** コマンドの説明を参照してください。

a.　両端に RJ-45 コネクタがついているイーサネット 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 3-9 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、コンピュータのイーサネット ポート、または管理ネットワークに接続します。

図 3-9　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。コンピュータまたはターミナルのボー 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。

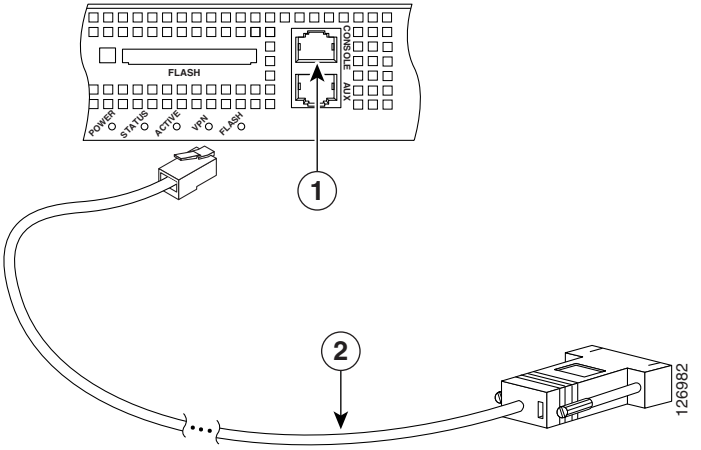
ターミナルの設定は次のとおりです：9600 ボー（デフォルト）、8 データ ビット、パリティなし、1 ストップ ビット、およびフロー制御（FC）= ハードウェア。

b. シリアル コンソール ケーブルを見つけます。シリアル コンソール ケーブルには、一方の端に RJ-45 コネクタがあり、もう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 3-10 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 3-10　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

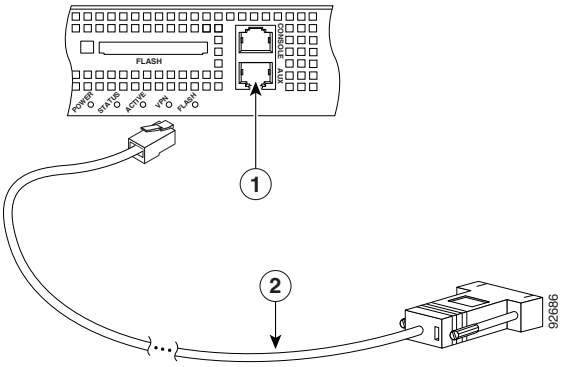
ステップ 4　補助ポート（AUX というレベルがあるポート）に接続します。

a. シリアル コンソール ケーブルを見つけます。シリアル コンソール ケーブルには、一方の端に RJ-45 コネクタがあり、もう一方の端にコンピュータのシリアル ポート用の DB-9 コネクタがあります。

b. ケーブルの　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 3-11 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 3-11　補助ポートへの接続



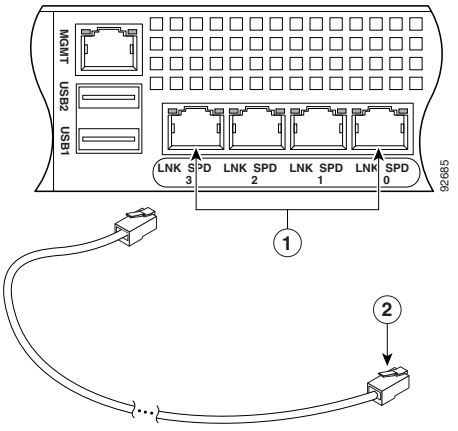
1	RJ-45 補助ポート	**2**	RJ-45/DB-9 コンソール ケーブル

ステップ 5　ネットワーク接続に使用する銅線イーサネット　ポートに接続します。銅線イーサネット ポートは、スロット 0 およびスロット 1 の両方を使用できます。

(注)　内部インターフェイスにはスロット 0 のポートを、外部インターフェイスにはスロット 1 のポートを使用する必要があります。

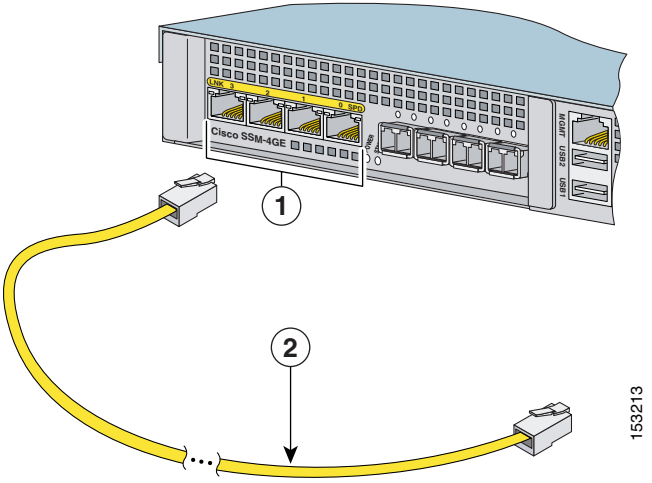
a.　イーサネット ケーブルの一方の端を、銅線イーサネット ポートに接続します（図 3-12 および 図 3-13 を参照してください）。

図 3-12　スロット 0 の銅線イーサネット インターフェイスへの接続



1	銅線イーサネット ポート	**2**	RJ-45 コネクタ

図 3-13　スロット 1 の銅線イーサネット インターフェイスへの接続



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　ネットワーク接続に使用するファイバ イーサネット ポートに接続します。

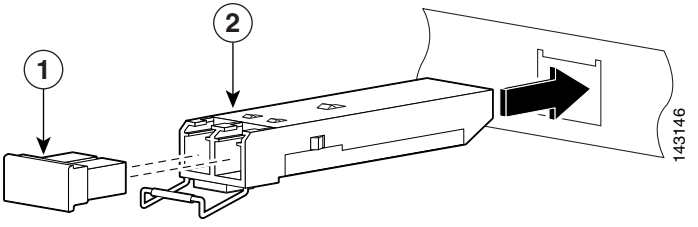
（注） スロット 1 には、4 つの銅線イーサネット ポートと 4 つのファイバ イーサネット ポートがあります。両方のポートを使用できますが、一度に使用できるのは合計で 4 つのスロット 1 ポートだけです。たとえば、2 つの銅線イーサネット ポートと 2 つのファイバ イーサネット ポートを使用できます。

使用するファイバ ポートごとに、次の手順を実行します。

a. SFP モジュールを次の手順で取り付けます。

- 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 3-14 を参照してください）。

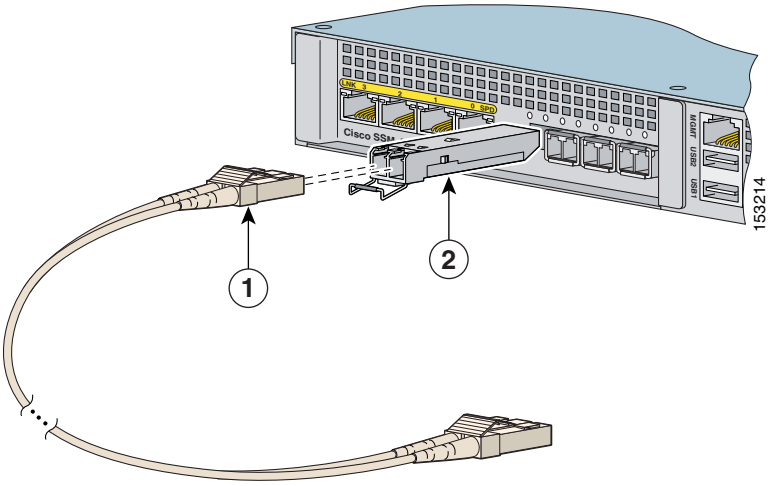
図 3-14　ファイバ ポート プラグの取り外し



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 3-15 を参照してください）。

図 3-15　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 7 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。

CHAPTER 4

ASA 5500、ASA 5510、ASA 5520 および ASA 5540 の設置

（注） この章は ASA 5550 には適用されません。

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。

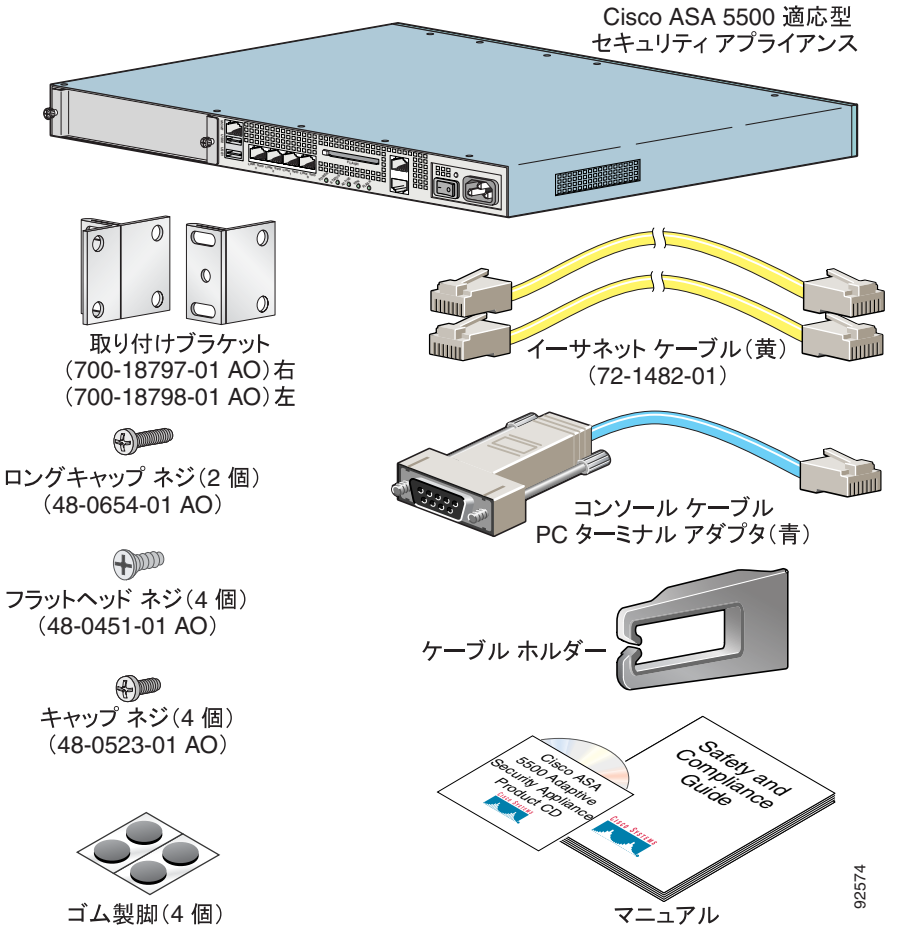
この章では、適応型セキュリティ アプライアンスの製品概要、メモリ要件、およびラックマウントと設置の手順について説明します。この章は、次の項で構成されています。

(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 4-1　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。

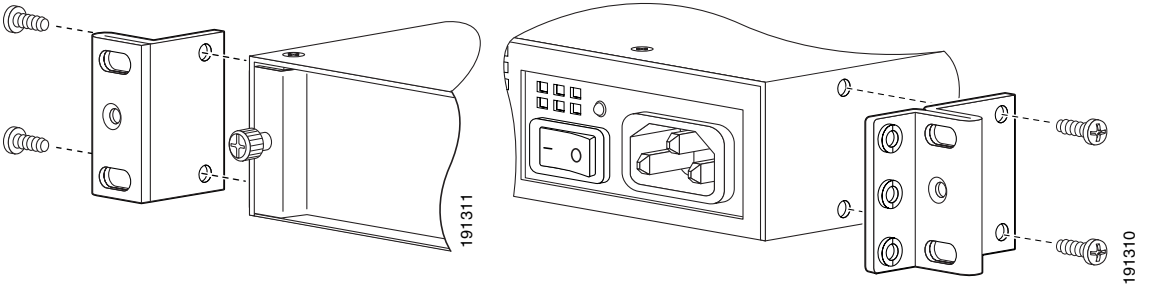
警告　**手順を実行する前に、DC 回路に電気が流れていないことを確認してください。すべての電源を確実に切断するには、パネル ボード上で DC 回路に対応している回路ブレーカーを確認して、回路ブレーカーを OFF の位置に切り替え、回路ブレーカーのスイッチ ハンドルを OFF の位置のままテープで固定します。**

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。

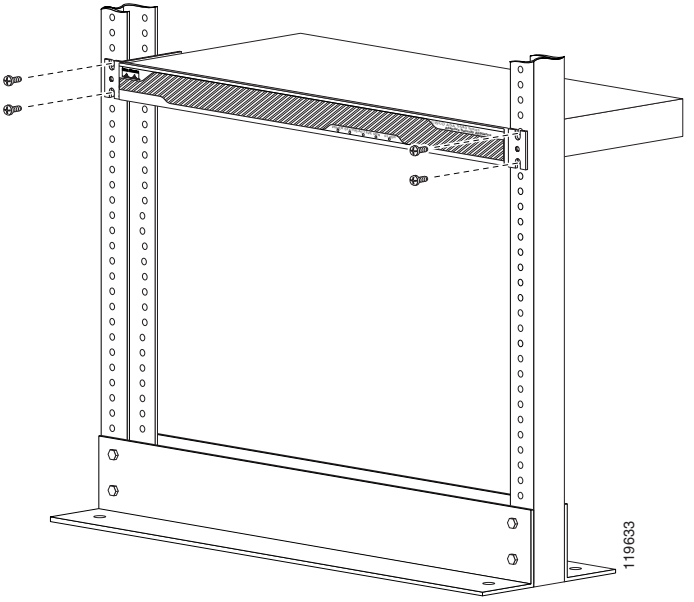
ステップ 1　付属のネジを使用して、シャーシにラックマウント ブラケットを取り付けます。ブラケットを穴に取り付けます（図 4-2 を参照してください）。ブラケットをシャーシに固定すると、ラックマウントできるようになります。

図 4-2　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 4-3 を参照してください）。

図 4-3　　シャーシのラックマウント

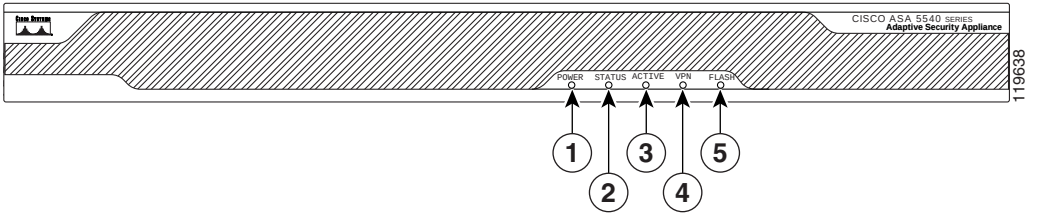


ラックからシャーシを取り外すには、シャーシをラックに取り付けているネジを外してから、シャーシを取り外します。

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 4-4 に前面パネルの LED を示します。

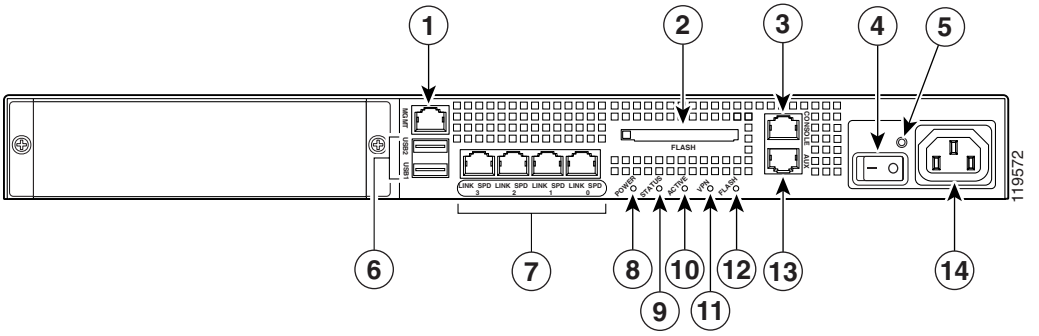
図 4-4　前面パネルの LED



	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 4-5 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 4-5　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）



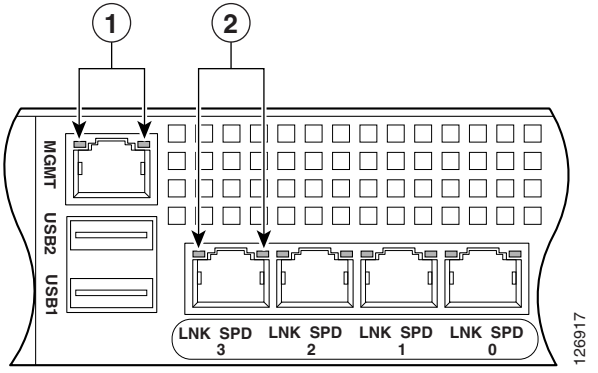
1	管理ポート[1]	**6**	USB 2.0 インターフェイス[2]	**11**	VPN LED
2	外部 CompactFlash スロット	**7**	ネットワーク インターフェイス[3]	**12**	フラッシュ LED
3	シリアル コンソール ポート	**8**	電源インジケータ LED	**13**	補助ポート
4	電源スイッチ	**9**	ステータス インジケータ LED	**14**	電源コネクタ
5	電源インジケータ LED	**10**	アクティブ LED		

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 4-6 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 4-6　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 4-1 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 4-1　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 5 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 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームでのインターフェイス ケーブルの接続」

CHAPTER 5

オプションの SSM の取り付け

(注) この章は ASA 5550 には適用されません。

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

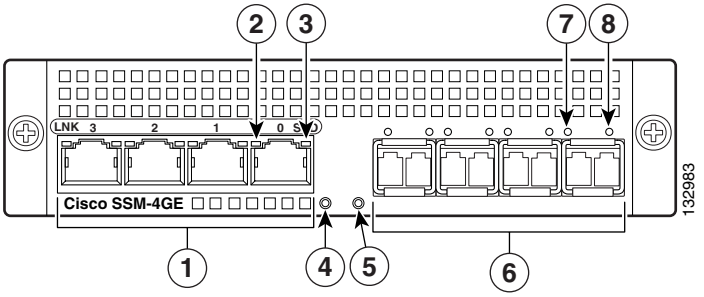
4GE セキュリティ サービス モジュール（SSM）には、8 個のイーサネット ポートがあります。10/100/1000 Mbps 用、銅線の RJ-45 ポートが 4 個、およびオプションの 1000 Mbps 用着脱可能小型フォーム ファクタ（SFP）ファイバ ポートが 4 個です。

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 5-1 に、Cisco 4GE SSM ポートと LED を示します。

図 5-1　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 5-1 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.5-5 の「SFP モジュールの取り付け」を参照してください。

表 5-1 で、Cisco 4GE SSM の LED について説明します。

表 5-1　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	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	100Mbps 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。

Cisco 4GE SSM の取り付け

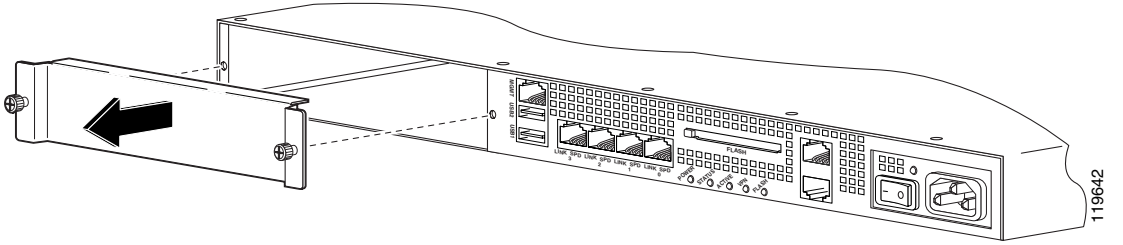
新しい Cisco 4GE SSM を初めて取り付けるには、次の手順に従います。

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。

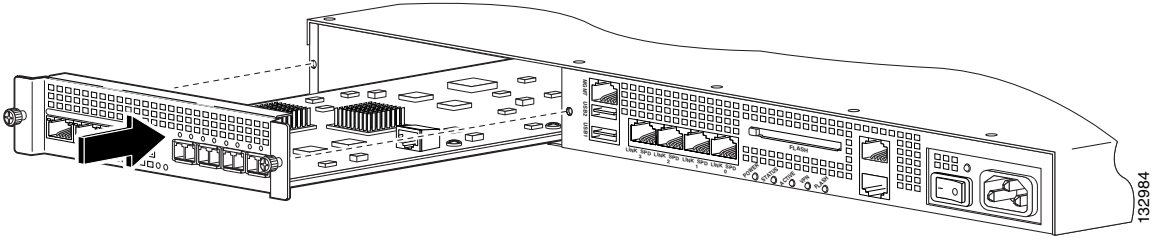
ステップ 3　シャーシ背面左端の 2 個のネジを外して（図 5-2 を参照してください）、スロット カバーを取り外します。

図 5-2　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 5-3 を参照してください）。

図 5-3　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 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームでのインターフェイス 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 5-2 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 5-2　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 5-3 に、ケーブル長の要件を示します。

表 5-3　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。

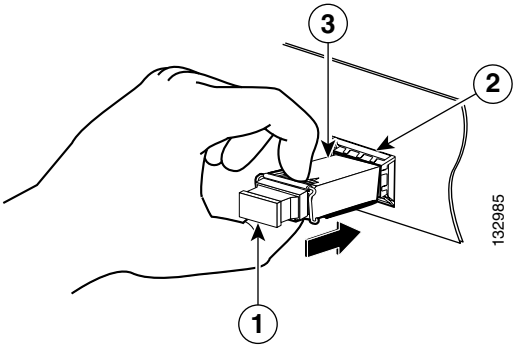
警告 **ケーブルが接続されていない場合、ポートの開口部からは目に見えないレーザー光が放射されている可能性があります。レーザー光に当たらないようにし、開口部をのぞきこまないでください。ステートメント** 70

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 5-4 を参照してください）。

図 5-4　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。

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 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームでのインターフェイス 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 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。

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 5-4 に、AIP SSM 10 と AIP SSM 20 のメモリ仕様を示します。

表 5-4　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 5-5 に、SSM の LED を示します。

図 5-5　SSM の LED

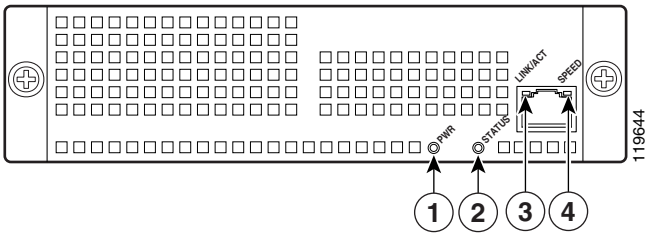


表 5-5 で、SSM の LED について説明します。

表 5-5　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 オレンジ	100 MB	ネットワーク アクティビティが発生しています。
			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

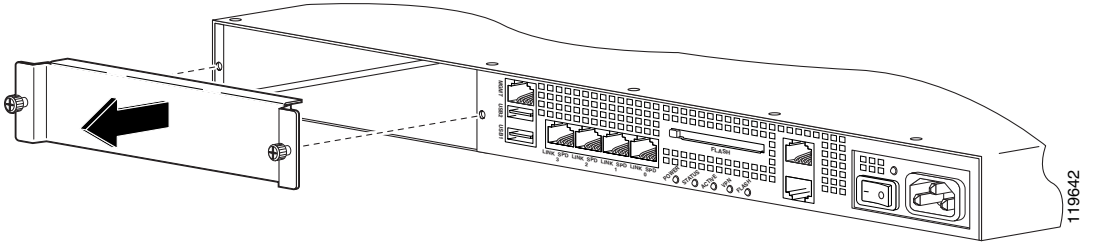
新しい SSM を取り付けるには、次の手順を実行します。

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。

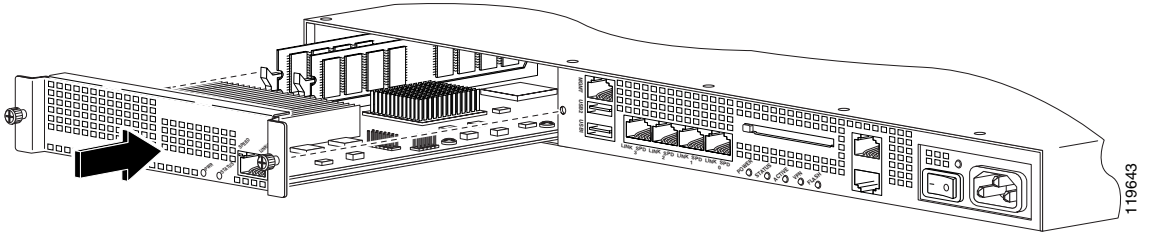
ステップ 3　シャーシ背面左端の 2 個のネジを外して（図 5-6 を参照してください）、スロット カバーを取り外します。

図 5-6　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 5-7 を参照してください）。

図 5-7　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 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームでのインターフェイス ケーブルの接続」に進みます。

次の手順

CHAPTER 6

ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームでのインターフェイス ケーブルの接続

(注) この章は、Cisco ASA 5550 には適用されません。

この章では、コンソール ポート、補助ポート、管理ポート、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。

(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。ご使用の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含まれていない場合は、第 7 章「適応型セキュリティ アプライアンスの設定」に進んでください。

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。

この章は、次の項で構成されています。

インターフェイス ケーブルの接続

この項では、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。

ケーブルをネットワーク インターフェイスに接続するには、次の手順を実行します。

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、デバイス管理のための専用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。

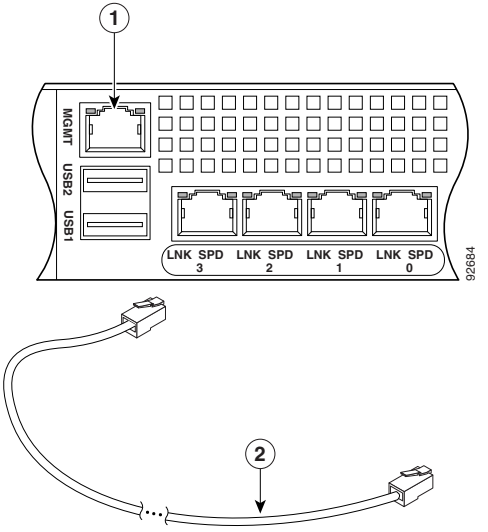
（注）　インターフェイスを管理専用インターフェイスとして設定するには、**management-only** コマンドを使用します。管理インターフェイスの管理専用モードをディセーブルにすることもできます。このコマンドの詳細については、『*Cisco Security Appliance Command Reference*』の **management-only** コマンドの説明を参照してください。

a.　両端に RJ-45 コネクタがついているイーサネット 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 6-1 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、コンピュータのイーサネット ポート、または管理ネットワークに接続します。

図 6-1　　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。

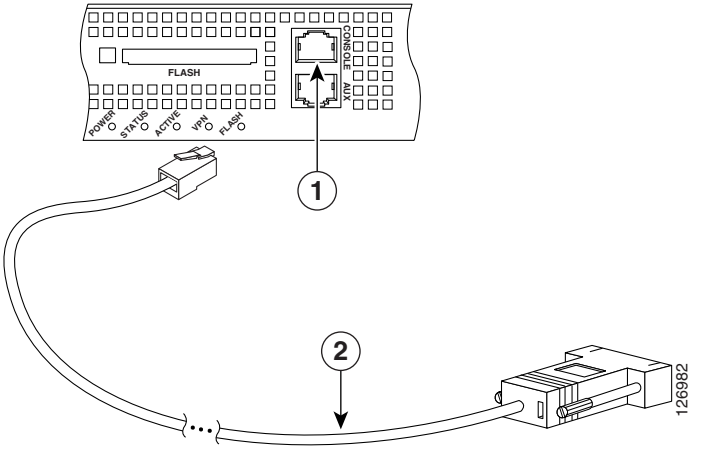
ターミナルの設定は次のとおりです：9600 ボー（デフォルト）、8 データ ビット、パリティなし、1 ストップ ビット、およびフロー制御（FC）= ハードウェア。

b. シリアル コンソール ケーブルを見つけます。シリアル コンソール ケーブルには、一方の端に RJ-45 コネクタがあり、もう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 6-2 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 6-2　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

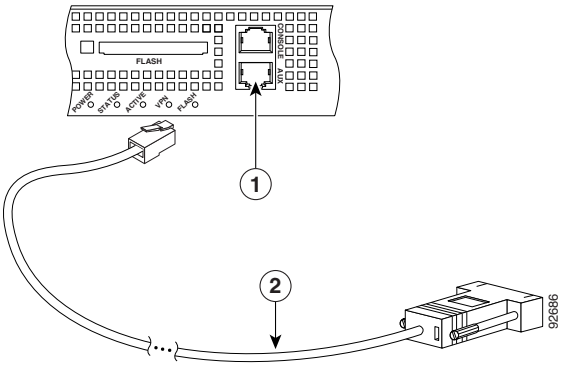
ステップ 4　補助ポート（AUX というレベルがあるポート）に接続します。

a. シリアル コンソール ケーブルを見つけます。シリアル コンソール ケーブルには、一方の端に RJ-45 コネクタがあり、もう一方の端にコンピュータのシリアル ポート用の DB-9 コネクタがあります。

b. ケーブルの　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 6-3 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 6-3　　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

SSM への接続

SSM はオプションです。この手順は、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。

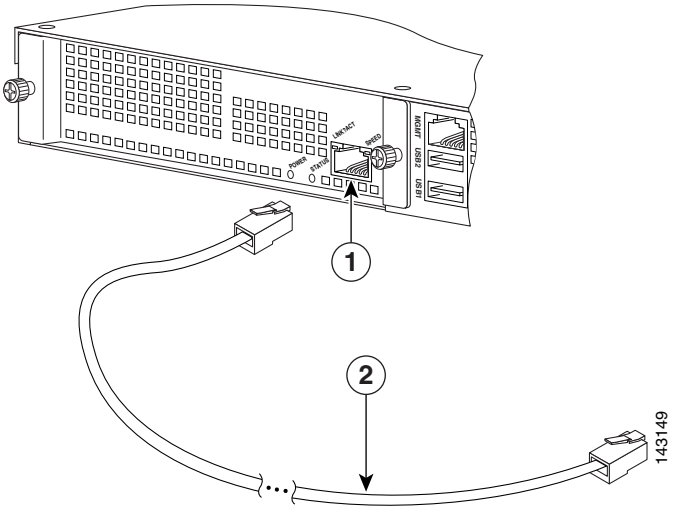
（注） この手順は、4GE SSM には適用されません。4GE SSM への接続方法の詳細については、P.6-10 の「4GE SSM への接続」を参照してください。

SSM に接続するには、次の手順を実行します。

ステップ 1　RJ-45 コネクタの一方を SSM の管理ポートに接続します（図 6-4 を参照してください）。

ステップ 2　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。

図 6-4　SSM 管理ポートへの接続



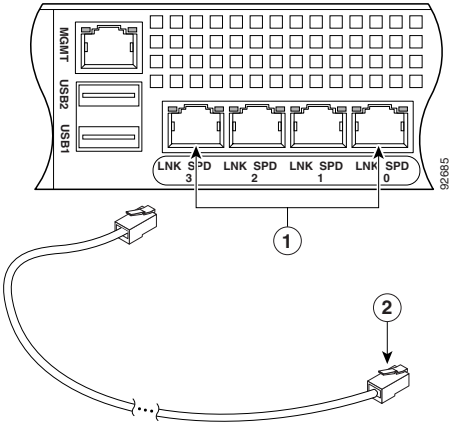
1	SSM 管理ポート	**2**	RJ-45/RJ-45 ケーブル

ステップ 3　ネットワーク接続に使用するイーサネット ポートに接続します。

a. RJ-45 コネクタをイーサネット ポートに接続します。

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。

図 6-5　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

4GE SSM への接続

4GE SSM はオプションです。このため、この手順は、適応型セキュリティ アプライアンスに 4GE SSM を取り付けた場合にのみ必要です。

ステップ 1　ネットワーク接続に使用する銅線イーサネット ポートに接続します。

a. イーサネット　ケーブルの一方の端を銅線イーサネット　ポートに接続します。

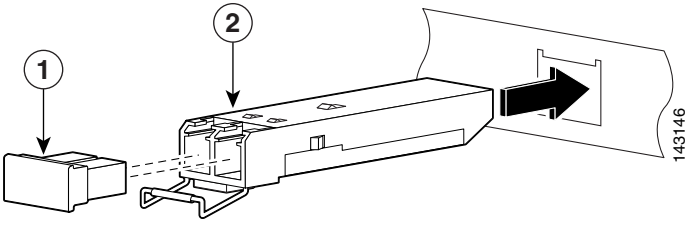
b. イーサネット ケーブルのもう一方の端をネットワーク デバイス（ルータ、スイッチ、ハブなど）に接続します。

ステップ 2　ネットワーク接続に使用するファイバ イーサネット ポートに接続します。使用するファイバ ポートごとに、次の手順を実行します。

a. SFP モジュールを次の手順で取り付けます。

- 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 6-6 を参照してください）。

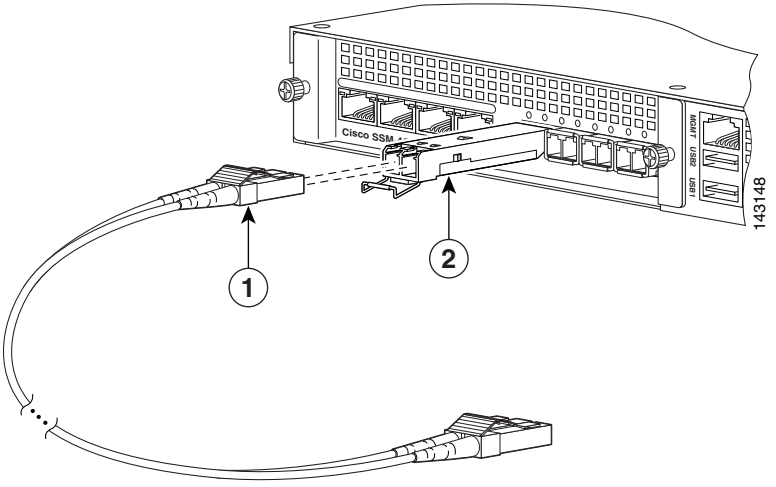
図 6-6　ファイバ ポート プラグの取り外し



1	ポート プラグ	2	SFP モジュール

— LC コネクタを SFP モジュールに接続します（図 6-7 を参照してください）。

図 6-7　LC コネクタの接続



b. 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。

適応型セキュリティ アプライアンスの電源投入

適応型セキュリティ アプライアンスの電源を入れるには、次の手順を実行します。

ステップ 1　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 2　シャーシの電源を入れます。

次の手順

第 7 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。

CHAPTER 7

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。この章の手順では、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。

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。ASA 5500 シリーズ は、次のように事前設定されています。

- 2 つの VLAN：VLAN 1 および VLAN2
- VLAN 1 には次のプロパティがある
  - 名前は「inside」
  - イーサネット 0/1 ～ イーサネット 0/7 のスイッチ ポートが割り当てられている
  - セキュリティ レベルは 100
  - イーサネット 0/1 ～ 0/7 のスイッチ ポートが割り当てられている
  - IP アドレスは 192.168.1.1 255.255.255.0
- VLAN2 には次のプロパティがある
  - 名前は「outside」
  - スイッチ ポート イーサネット 0/0 が割り当てられている
  - セキュリティ レベルは 0
  - DHCP を使用して IP アドレスを取得するように設定されている
- デバイスに接続するための内部インターフェイスで、ASDM を使用して設定を完了する。

デフォルトでは、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。

CLI を使用した設定

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。

vpnsetup ipsec-remote-access steps コマンドおよび **vpnsetup site-to-site steps** コマンドを使用して、基本的なリモートアクセスおよび LAN-to-LAN 接続を CLI で設定する方法を示す段階的な例を参照できます。これらの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。

適応型セキュリティ アプライアンスのすべての機能領域のステップバイステップの設定手順については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

Adaptive Security Device Manager を使用した設定

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。

この項では、次のトピックについて取り上げます。

ASDM を使用するための準備

ASDM を使用する前に、次の手順を実行します。

ステップ 1　まだ実行していない場合は、イーサネット ケーブルを使用して MGMT インターフェイスをスイッチまたはハブに接続します。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 を接続します。

ステップ 2　DHCP を使用するように PC を設定します（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ため）。この操作を行うと、PC が適応型セキュリティ アプライアンスやインターネットと通信でき、ASDM で設定および管理タスクを実行できます。

または、192.168.1.0 サブネットでアドレスを選択して、PC に固定 IP アドレスを割り当てることができます（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）。

他のデバイスを内部ポートのいずれかに接続する場合、デバイスの IP アドレスが同じでないことを確認します。

（注）　デフォルトで、適応型セキュリティ アプライアンスの MGMT 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　MGMT インターフェイスの LINK LED を確認します。

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。

初期セットアップのための情報収集

ASDM Startup Wizard で使用する、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
- ドメイン名
- 外部インターフェイス、内部インターフェイス、および設定するその他のすべてのインターフェイスの IP アドレス
- ASDM 用の HTTPS、SSH、または Telnet を使用してこのデバイスへの管理者アクセス権を持っている必要があるホストの IP アドレス
- 管理者アクセス権用の特権モード パスワード
- NAT または PAT のアドレス変換に使用する IP アドレス
- DHCP サーバの IP アドレス範囲
- WINS サーバの IP アドレス
- 設定するスタティック ルート
- DMZ を作成する場合は、3 つの VLAN を作成し、この VLAN にポートを割り当てる（デフォルトでは、2 つの VLAN が設定されています）
- インターフェイス設定情報：同じセキュリティ　レベルのインターフェイス間でトラフィックが許可されているかどうか、また同じインターフェイス上のホスト間でトラフィックが許可されているかどうか
- Easy VPN ハードウェア クライアントを設定する場合は、プライマリおよびセカンダリ Easy VPN サーバの IP アドレス、Easy VPN ハードウェア クライアントをクライアントまたはネットワーク拡張モードで実行するかどうか、プライマリおよびセカンダリ Easy VPN サーバ上の設定と一致させるためのユーザおよびグループ ログイン認定証

ASDM Launcher のインストール

ASDM は、次の 2 つ方法のどちらかを使用して起動できます。ASDM Launcher ソフトウェアをダウンロードして ASDM を PC 上でローカルに実行する方法と、Web ブラウザで Java と JavaScript を有効にして PC からリモートで ASDM にアクセスする方法です。ここでは、ASDM をローカルに実行するようにシステムを設定する方法について説明します。

ASDM Launcher をインストールするには、次の手順を実行します。

ステップ 1　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。

a. 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。

Cisco ASDM スプラッシュ画面が表示されます。

b. **Install ASDM Launcher and Run ASDM** をクリックします。

c. 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。**OK** をクリックします。

d. **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。

e. File Download ダイアログボックスが開いたら、**Open** をクリックし、直接 ASDM Launcher をインストールします。このインストール プログラムをハードディスクに保存する必要はありません。

f. InstallShield Wizard が表示されたら、指示に従って ASDM Launcher ソフトウェアをインストールします。

ステップ 2　デスクトップから、Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。

ステップ 3　適応型セキュリティ　アプライアンスの　IP　アドレスまたはホスト名を入力します。

ステップ 4　Username および Password フィールドはブランクのままにします。

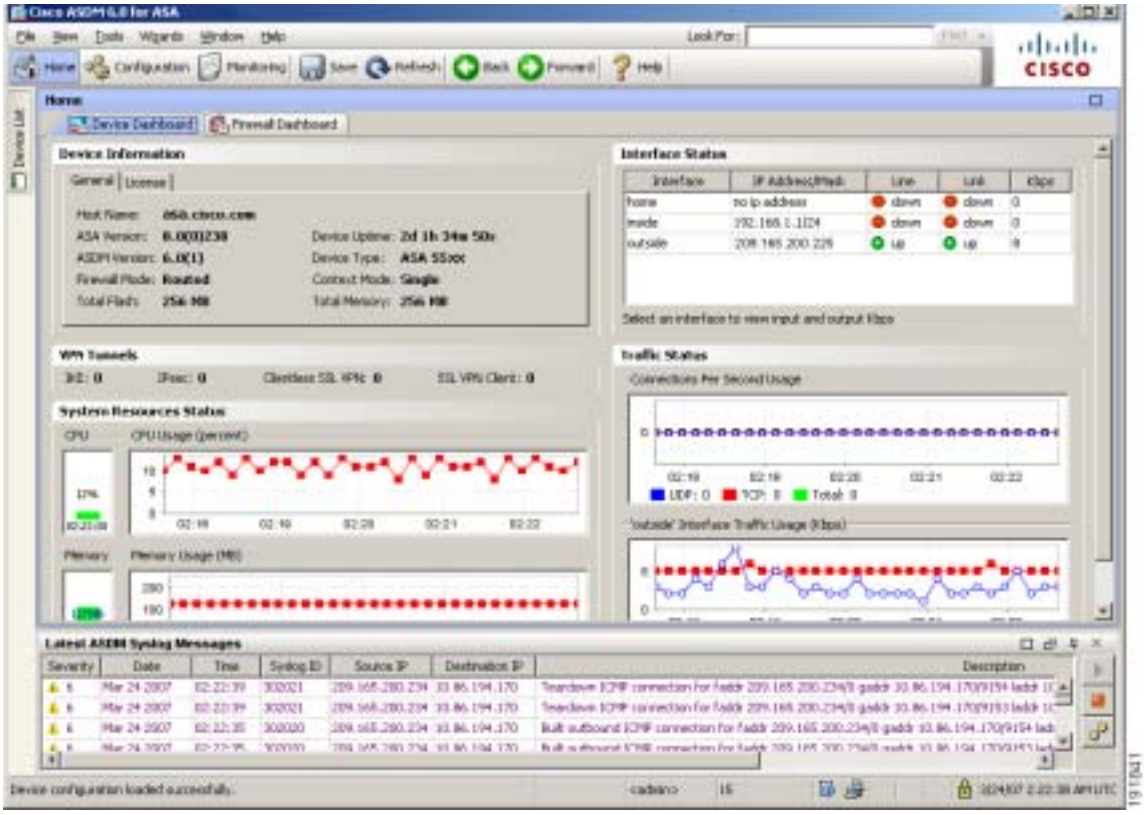
（注）　デフォルトで、Cisco ASDM Launcher には Username および Password は設定されていません。

ステップ 5　OK をクリックします。

ステップ 6　証明書を受け入れるよう要求するセキュリティ警告が表示されたら、**Yes**　をクリックします。

ASA は更新するソフトウェアがあるかどうかを確認し、ある場合は自動的にダウンロードします。

ASDM のメイン ウィンドウが表示されます。



ASDM が起動し、メイン ウィンドウが表示されます。

Web ブラウザを使用した 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。HTTP over SSL（HTTP）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。

ASDM Startup Wizard の実行

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。

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　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 2　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） DES ライセンスまたは 3DES-AES ライセンスを要求するエラーが表示された場合、付録 A「3DES/AES ライセンスの取得」で詳細を確認してください。

（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。このようなアクセス コントロール ポリシーは、ASDM を使用して設定できます。ASDM のメイン ページで、**Configuration > Properties > ICMP Rules** をクリックします。外部インターフェイスのエントリを追加します。IP アドレスを 0.0.0.0 に、ネットマスクを 0.0.0.0 に、Action を deny にそれぞれ設定します。

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 8 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 9 章「シナリオ：IPSec リモートアクセス VPN の設定」
ソフトウェア クライアントを使用した SSL VPN 接続用の適応型セキュリティ アプライアンスの設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」
Web ブラウザを使用した SSL VPN 接続用の適応型セキュリティ アプライアンスの設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
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 12 章「シナリオ：サイトツーサイト VPN の設定」

CHAPTER 8

シナリオ：DMZ の設定

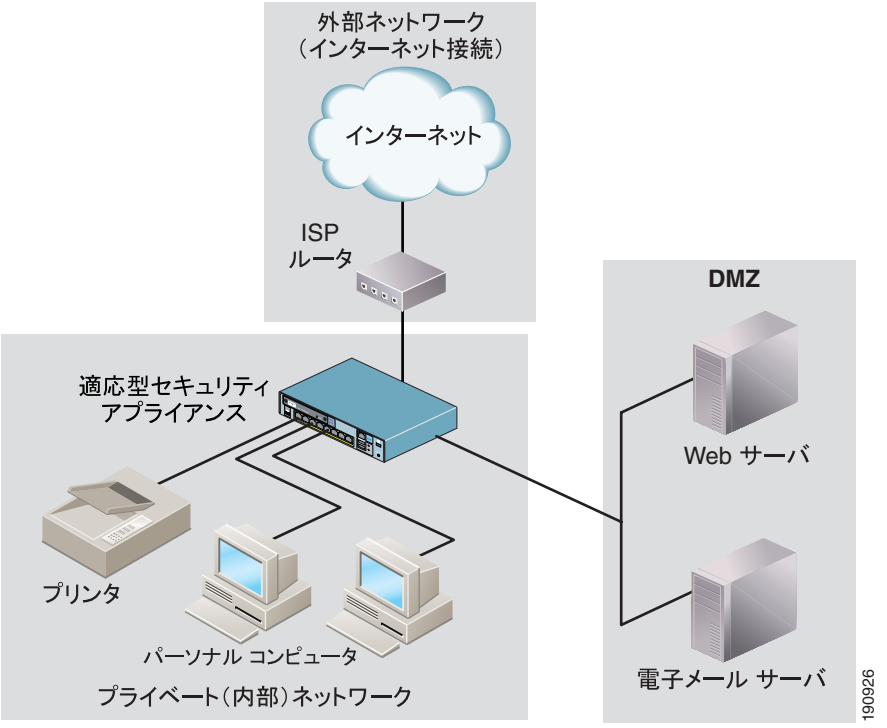
非武装地帯（DMZ）とは、プライベート（内部）ネットワークとパブリック（外部）ネットワークの間の中立ゾーンにある区別されたネットワークです。

この章は、次の項で構成されています。

DMZ 設定用の基本ネットワーク レイアウト

図 8-1 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 実装の代表的なものです。この配置では、Web サーバは DMZ インターフェイス上にあり、HTTP クライアントは内部ネットワークからも外部ネットワークからもこの Web サーバにセキュアにアクセスできます。

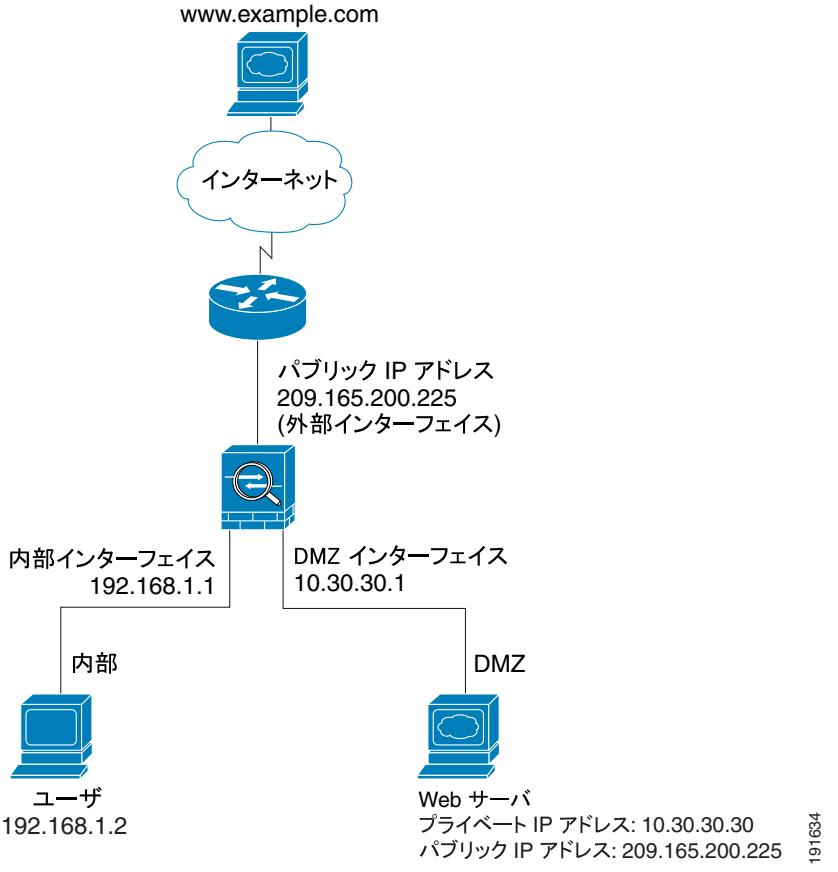
図 8-1　　DMZ を使用したプライベート ネットワーク



DMZ ネットワーク トポロジの例

この章では、適応型セキュリティ アプライアンスの DMZ の配置を設定する方法について説明します（図 8-2 を参照してください）。

図 8-2　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、インターネット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。
- ネットワークには、パブリックに使用可能な IP アドレス、つまり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）があります。このパブリック アドレスは、適応型セキュリティ アプライアンスおよび DMZ Web サーバで共有されます。

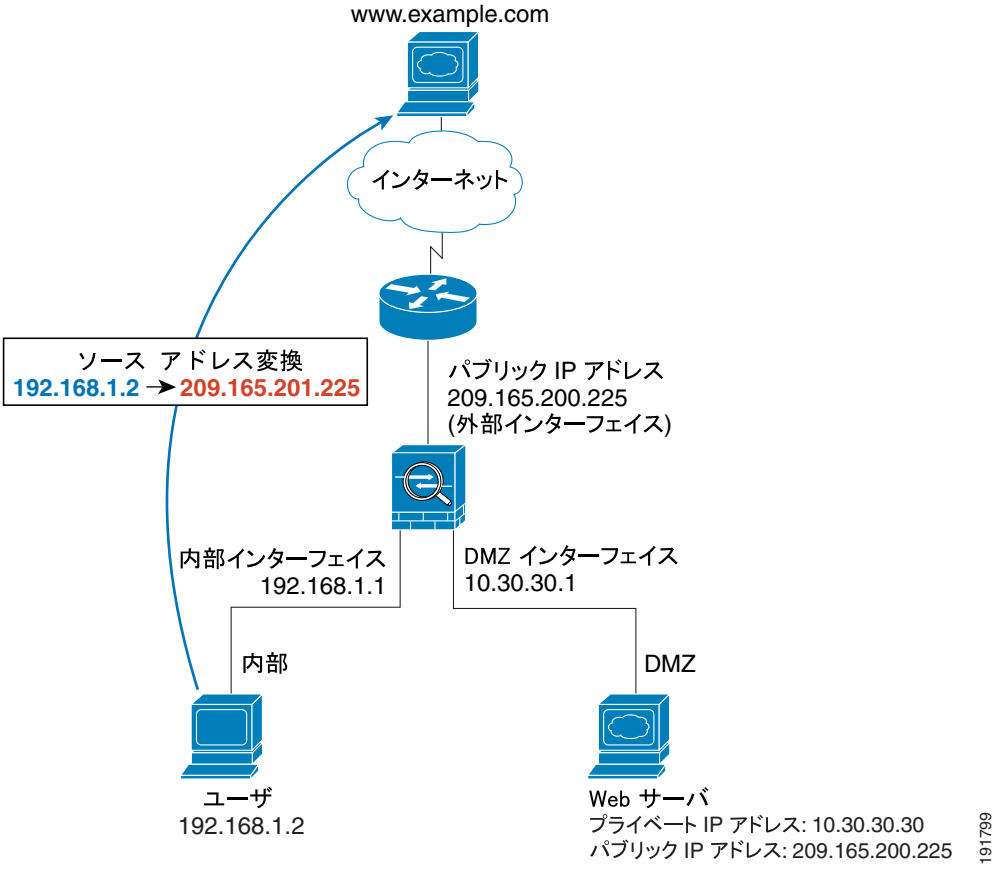
この項では、次のトピックについて取り上げます。

- インターネット上の Web サーバにアクセスする内部ユーザ（P.8-5）
- DMZ Web サーバにアクセスするインターネット ユーザ（P.8-7）
- DMZ Web サーバにアクセスする内部ユーザ（P.8-9）

インターネット上の Web サーバにアクセスする内部ユーザ

図 8-3 は、内部ユーザがインターネット上の Web サーバに HTTP ページを要求したときの、適応型セキュリティ アプライアンスを通るトラフィック フローを示しています。

図 8-3　インターネット上の Web サーバにアクセスする内部ユーザ



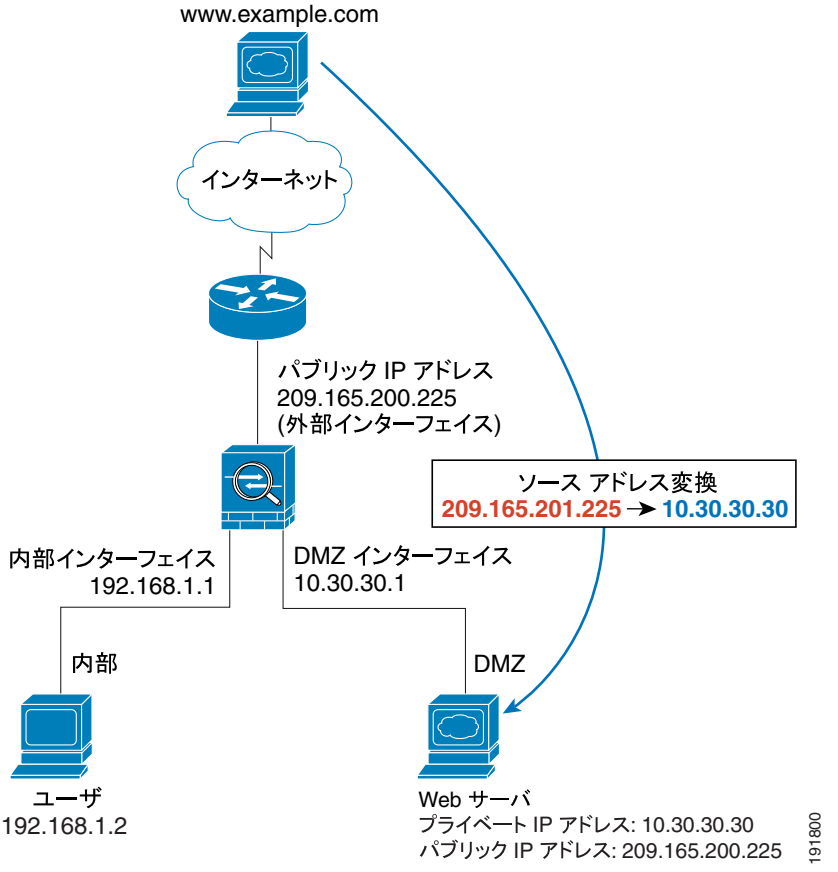
内部ユーザがインターネット上の Web サーバに HTTP ページを要求すると、データは次のように適応型セキュリティ アプライアンスを通じて移動します。

1. 内部ネットワーク上のユーザが www.example.com に Web ページを要求します。
2. 適応型セキュリティ　アプライアンスはパケットを受信します。これは新しいセッションのため、このパケットが許可されていることを確認します。
3. 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）を行い、ローカルの送信元アドレス（192.168.1.2）を外部インターフェイスのパブリック アドレス（209.165.200.225）に変換します。
4. 適応型セキュリティ　アプライアンスはセッションが確立されたことを記録し、外部インターフェイスからこのパケットを転送します。
5. www.example.com が要求に応答すると、パケットは確立されたセッションを使用して適応型セキュリティ アプライアンスを通過します。
6. 適応型セキュリティ アプライアンスは NAT を実行し、パブリックの宛先アドレスをローカル ユーザ アドレス（192.168.1.2）に変換します。
7. 適応型セキュリティ アプライアンスはパケットを内部ユーザに転送します。

DMZ Web サーバにアクセスするインターネット ユーザ

図 8-4 は、インターネット上のユーザが DMZ Web サーバに Web ページを要求したときの、適応型セキュリティ アプライアンスを通るトラフィック フローを示しています。

図 8-4　DMZ Web サーバにアクセスする外部ユーザ



インターネット上のユーザが DMZ Web サーバに HTTP ページを要求すると、トラフィックは次のように適応型セキュリティ アプライアンスを通過します。

1. 外部ネットワーク上のユーザは、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（外部インターフェイスの IP アドレスである 209.165.200.225）を使用して、DMZ Web サーバに Web ページを要求します。
2. 適応型セキュリティ　アプライアンスはパケットを受信します。これは新しいセッションのため、このパケットが許可されていることを確認します。
3. 適応型セキュリティ アプライアンスは、宛先アドレスを DMZ Web サーバのローカル アドレス（10.30.30.30）に変換し、DMZ インターフェイスを通じてパケットを転送します。
4. DMZ Web サーバが要求に応答すると、適応型セキュリティ アプライアンスは、ローカルの送信元アドレスを DMZ Web サーバのパブリック アドレス（209.165.200.225）に変換します。
5. 適応型セキュリティ アプライアンスはパケットを外部ユーザに転送します。

DMZ Web サーバにアクセスする内部ユーザ

図 8-5 は、DMZ Web サーバにアクセスするユーザを示しています。

図 8-5　DMZ 上の Web サーバにアクセスする内部ユーザ

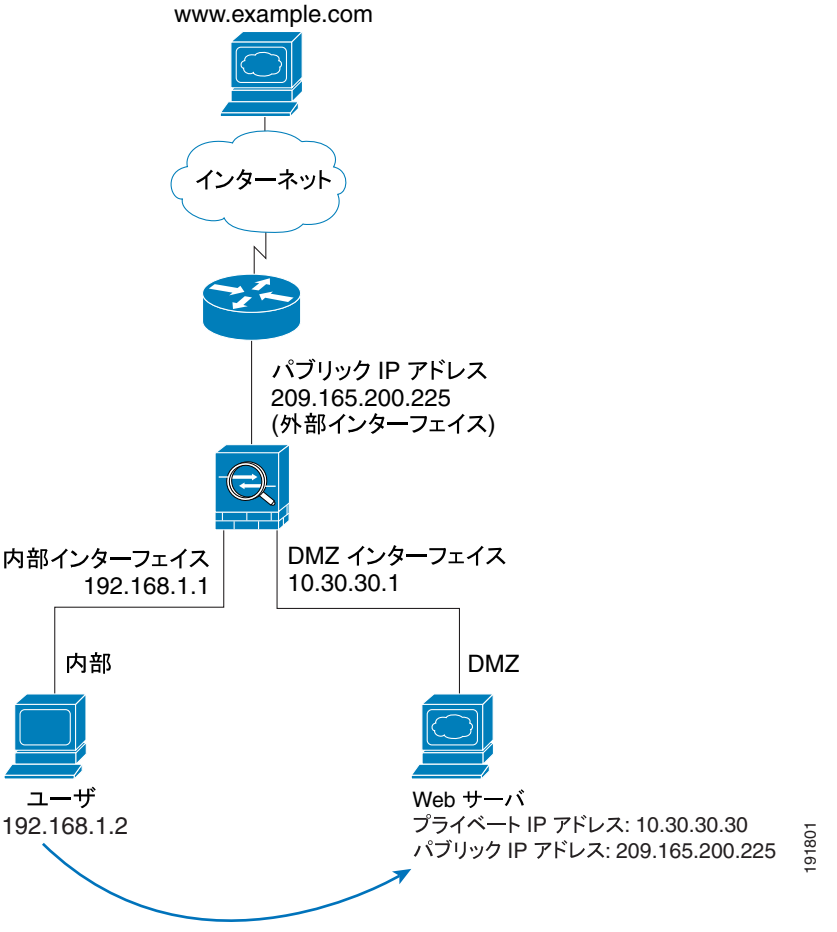


図 8-5 で、適応型セキュリティ アプライアンスは、内部クライアントから発信される DMZ Web サーバ宛の HTTP トラフィックを許可します。内部ネットワークには DNS サーバが存在しないため、内部クライアントの DMZ Web サーバに対する要求は、次のように処理されます。

1. 検索要求は ISP の DNS サーバに送信されます。DMZ Web サーバのパブリック IP アドレスがクライアントに返されます。
2. 内部クライアントは、DMZ Web サーバの IP アドレスに Web ページを要求します。適応型セキュリティ アプライアンスは、内部インターフェイス上でこの要求を受信します。
3. 適応型セキュリティ アプライアンス は DMZ Web サーバの IP アドレスを実アドレス（209.165.200.225 -> 10.30.30.30）に変換し、DMZ インターフェイスから Web サーバに要求を転送します。
4. DMZ Web サーバが要求に応答すると、適応型セキュリティ アプライアンスは DMZ インターフェイス上でデータを受信し、内部インターフェイスからユーザにこのデータを転送します。

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 配置用の適応型セキュリティ アプライアンスの設定

この章では、ASDM を使用して、図 8-2 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、外部インターフェイス、および DMZ 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 7 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。

ここからは、この設定を実装するための手順について説明します。

設定の要件

適応型セキュリティ アプライアンスのこの DMZ 配置には、次の設定規則が必要です。

目的	作成する規則
内部クライアントがインターネット上の Web サーバに情報を要求する	適応型セキュリティ アプライアンスのデフォルト設定では、内部クライアントがインターネット上のデバイスにアクセスすることが許可されています。追加設定は必要ありません。
内部クライアントが DMZ Web サーバに情報を要求する	• DMZ Web サーバの実 IP アドレスをパブリック IP アドレス（10.10.10.30 から 209.165.200.225）に変換する、DMZ および内部インターフェイス間の NAT 規則。 • 内部クライアント ネットワークの実アドレスを変換する、内部および DMZ インターフェイス間の NAT 規則。このシナリオでは、内部ネットワークの実 IP アドレスは自分自身に「変換」されます。つまり、内部クライアントが DMZ Web サーバと通信を行うとき、内部ネットワークの実 IP アドレスが使用されます（10.10.10.0 から 10.10.10.0 に変換）。
外部クライアントが DMZ Web サーバに情報を要求する	• DMZ Web サーバのパブリック IP アドレスをプライベート IP アドレス（209.165.200.225 から 10.10.10.30 に）変換する、外部および DMZ インターフェイス間のアドレス変換規則。 • 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）。

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。

- パブリック ネットワーク上のクライアントが使用できるようにする DMZ 内のサーバ（このシナリオでは Web サーバ）の内部 IP アドレス。
- DMZ 内のサーバ用に使用されるパブリック IP アドレス（パブリック ネットワーク上のクライアントは、このパブリック IP アドレスを使用して DMZ 内のサーバにアクセスします）。
- 発信トラフィックの内部 IP アドレスの代わりになるクライアント IP アドレス（このシナリオでは、外部インターフェイスの IP アドレス）。IP アドレスが公開されないようにするため、発信クライアントの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。

ASDM の起動

この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアをまだインストールしていない場合は、P.7-7 の「ASDM Launcher のインストール」を参照してください。

Web ブラウザまたは Java を使用して直接 ASDM にアクセスする場合は、P.7-10 の「Web ブラウザを使用した ASDM の起動」を参照してください。

ASDM Launcher ソフトウェアを使用して ASDM を起動するには、次の手順を実行します。

ステップ 1　デスクトップから、Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。

ステップ 2　適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 3　Username および Password フィールドはブランクのままにします。

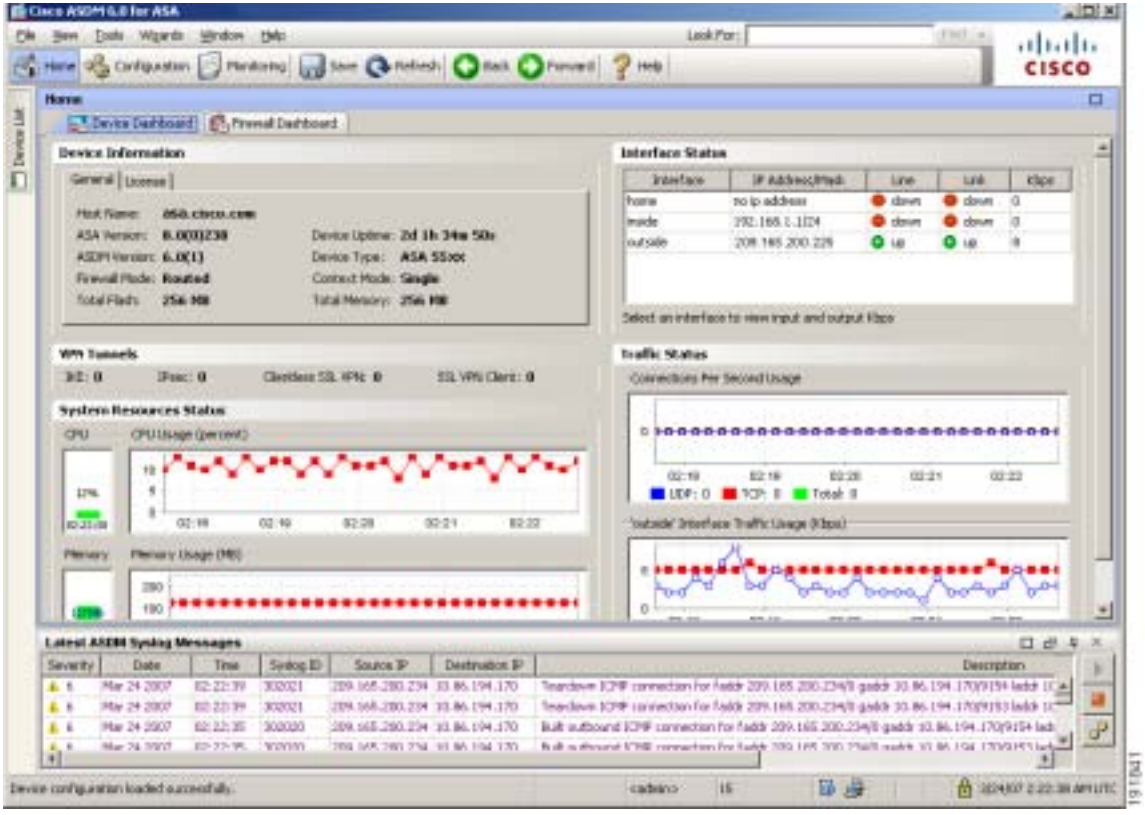
（注）　デフォルトで、Cisco ASDM Launcher には Username および Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書を受け入れるよう要求するセキュリティ警告が表示されたら、**Yes**　をクリックします。

ASA は更新するソフトウェアがあるかどうかを確認し、ある場合は自動的にダウンロードします。

ASDM のメイン ウィンドウが表示されます。



内部クライアントによるインターネット上のデバイスとの通信の許可

内部クライアントがインターネット上のデバイスにコンテンツを要求できるようにするため、適応型セキュリティ アプライアンスは、内部クライアントの実 IP アドレスを外部インターフェイスの外部アドレス（つまり、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）に変換します。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。

適応型セキュリティ アプライアンスでは、必要なアドレス変換規則がデフォルトで設定されています。内部インターフェイスの IP アドレスを変更しない限り、内部クライアントによるインターネットへのアクセスを許可する設定を行う必要はありません。

内部クライアントによる DMZ Web サーバとの通信の許可

この手順では、内部クライアントが DMZ 内の Web サーバとセキュアに通信できるように、適応型セキュリティ アプライアンスを設定します。これを行うには、次の 2 つの規則を設定する必要があります。

- DMZ Web サーバの実 IP アドレスをパブリック IP アドレス（10.30.30.30 から 209.165.200.225）に変換する、DMZ および内部インターフェイス間の NAT 規則。
- DMZ Web サーバのパブリック IP アドレスを実 IP アドレス（209.165.200.225 から 10.30.30.30）に戻す、内部および DMZ インターフェイス間の NAT 規則。

  内部クライアントが DNS 検索要求を送信すると、DNS サーバは DMZ Web サーバのパブリック IP アドレスを返すため、この規則が必要になります。

（注） 内部ネットワーク上に DNS サーバが存在しないため、DNS 要求は適応型セキュリティ アプライアンスを出て、インターネット上の DNS サーバによって解決される必要があります。

この項では、次のトピックについて取り上げます。

- 内部および DMZ インターフェイス間の内部クライアントの IP アドレス変換（P.8-17）
- Web サーバのパブリック アドレスから実アドレスへの変換（P.8-21）

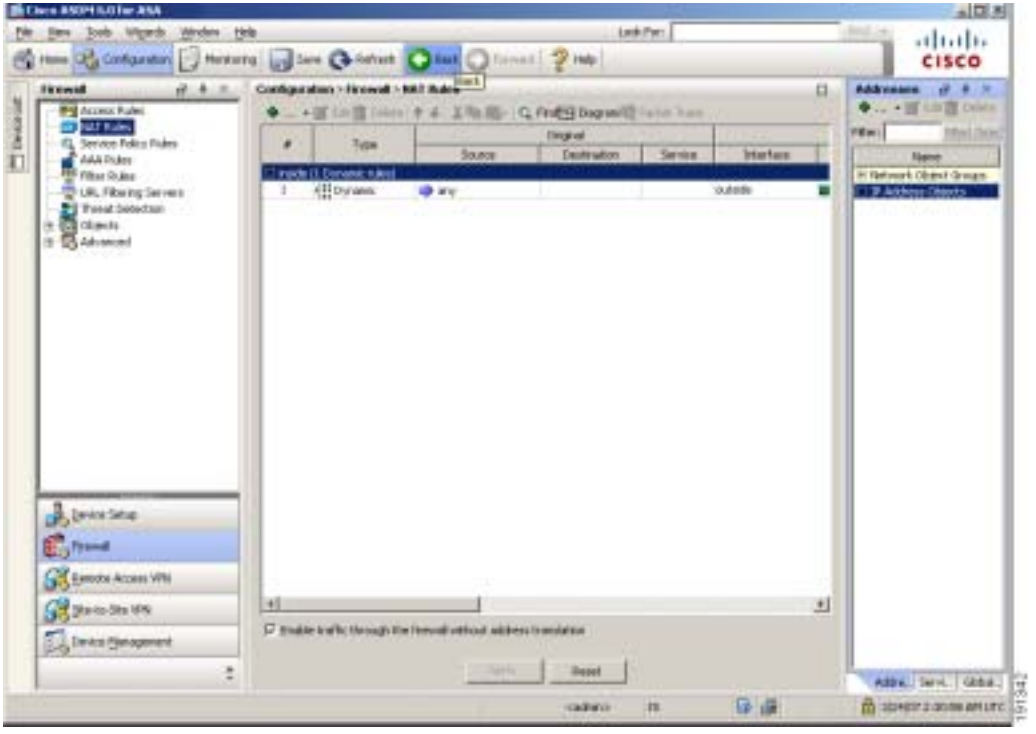
内部および DMZ インターフェイス間の内部クライアントの IP アドレス変換

内部インターフェイスおよび DMZ インターフェイス間で内部クライアントの IP アドレスを変換する NAT 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 のメイン ウィンドウで、**Configuration** ツールをクリックします。

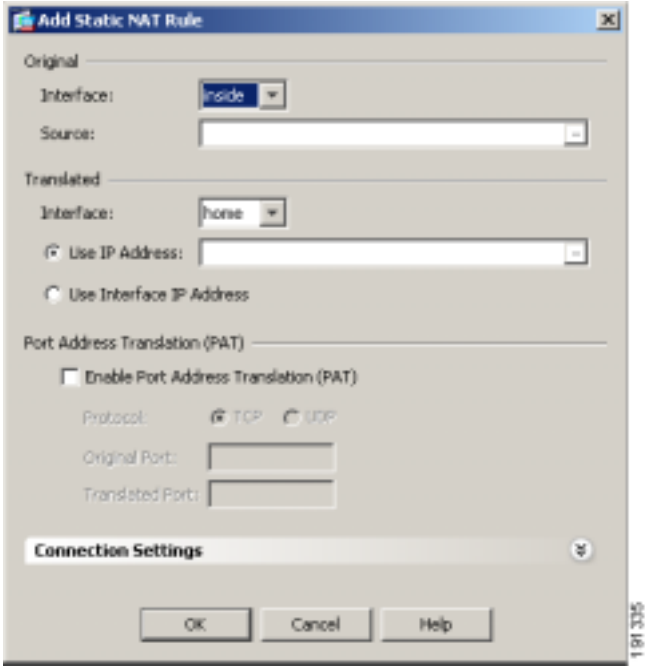
ステップ 2　ASDM ウィンドウの左側にある Device List 領域で、Firewall をクリックします。

ステップ 3　ASDM ウィンドウの左側にある Firewall ペインで、NAT Rules をクリックします。



ステップ 4　緑色のプラス記号（+）のアイコンをクリックし、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 5　Original 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、10.10.10.0 サブネット全体に対して実行されます。

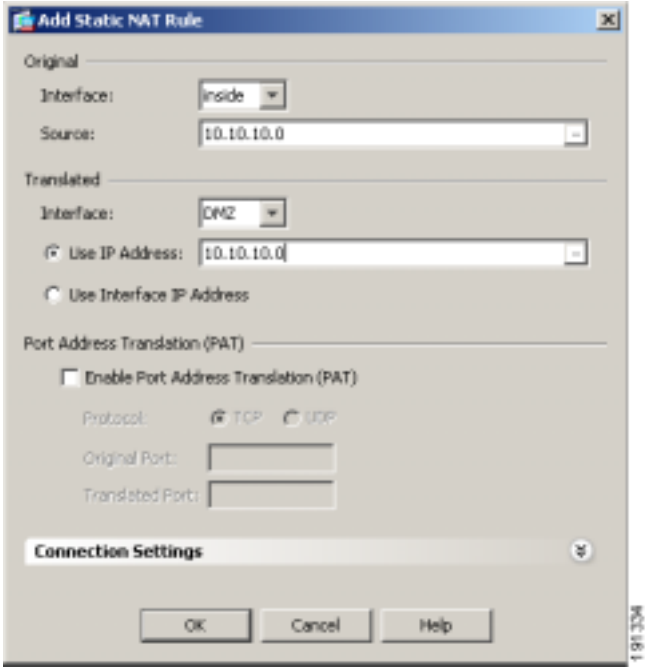
a.　Interface ドロップダウン リストで、inside インターフェイスを選択します。

b.　Source フィールドに、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。

ステップ 6　Translated 領域で、次の手順を実行します。

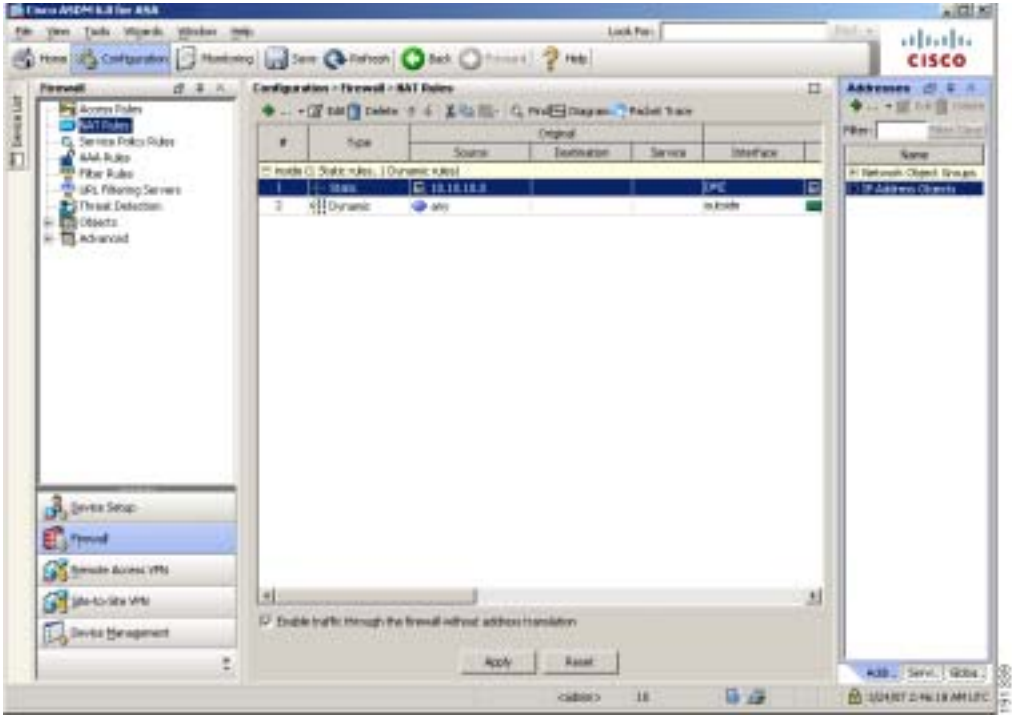
a. Interface ドロップダウン リストで、DMZ インターフェイスを選択します。

b. IP Address フィールドに、内部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. **OK** をクリックして Static NAT Rule を追加し、Configuration > NAT ペインに戻ります。

設定ペインで、変換規則が予想どおりに表示されることを確認します。規則は次のように表示されます。



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。

Web サーバのパブリック アドレスから実アドレスへの変換

Web サーバのパブリック IP アドレスを実 IP アドレスに変換する NAT 規則を設定するには、次の手順を実行します。

ステップ 1　Configuration > Firewall > NAT Rules 画面で、緑色の +（プラス記号）のアイコンをクリックし、Add Static NAT Rule を選択します。

Add Static NAT Rule ダイアログボックスが表示されます。

ステップ 2　Original 領域で、次の手順を実行します。

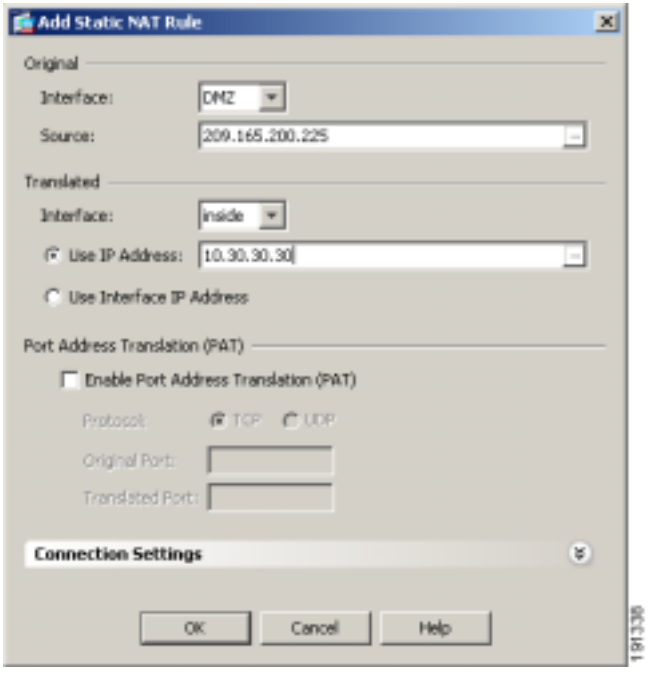
a. Interface ドロップダウン リストで、DMZ を選択します。

b. Source フィールドで、DMZ Web サーバのパブリック アドレスを入力するか、または IP Address ドロップダウン リストから選択します。このシナリオでは、IP アドレスは 209.165.200.225 です。

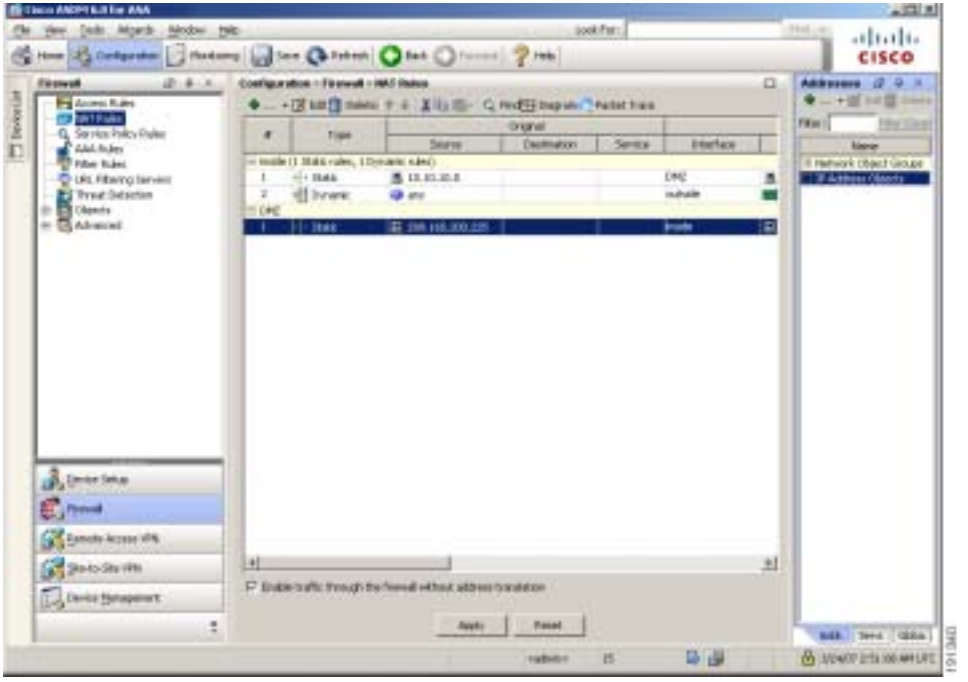
ステップ 3　Translated 領域で、次の手順を実行します。

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

b. DMZ Web サーバの実アドレスを入力するか、または IP Address ドロップダウン リストから選択します。このシナリオでは、IP アドレスは 10.30.30.30 です。


Add Static NAT Rule
Original
Interface:
DMZ
Source:
209.165.200.225
Translated
Interface:
inside
Use IP Address:
10.30.30.30
Use Interface IP Address
Port Address Translation (PAT)
Enable Port Address Translation (PAT)
Protocol:
TCP
UDP
Original Port:
Translated Port:
Connection Settings
OK
Cancel
Help
191330

ステップ 4　**OK** をクリックして、Configuration > NAT ペインに戻ります。表示される設定は、次のようになります。



ステップ 5　**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 アクセス用のスタティック PAT の設定（ポート転送）

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、外部 HTTP クライアントが適応型セキュリティ アプライアンスを意識せずに Web サーバにアクセスできるようにする必要があります。このシナリオでは、DMZ Web サーバは、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）とパブリック IP アドレスを共有しています。

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（209,165,200,225）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　Configuration > Firewall > NAT Rules ペインで、Add ドロップダウン リストから Add Static NAT Rule を選択します。

Add Static NAT Rule ダイアログボックスが表示されます。

ステップ 2　Original 領域で、Web サーバの実 IP アドレスを次のように指定します。

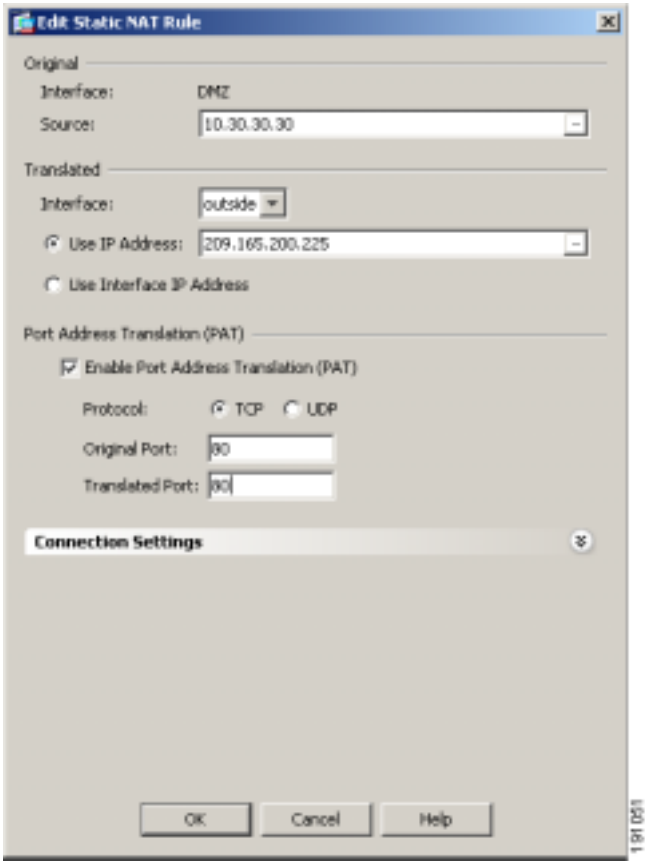
a. Interface ドロップダウン リストで、DMZ インターフェイスを選択します。

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。

ステップ 3　Translated 領域で、Web サーバに使用されるパブリック 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 を選択します。

b. Interface IP オプション ボタンをクリックします。これが指定されたインターフェイス（この場合は外部インターフェイス）の IP アドレスになります。



ステップ 4　ポート アドレス変換を設定します。

パブリック IP アドレスは 1 つしかないため、ポート アドレス変換を使用して、DMZ Web サーバの IP アドレスを、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（外部インターフェイスの IP アドレス）に変換する必要があります。ポート アドレス変換を設定するには、次の手順を実行します。

a.　**Enable Port Address Translation** チェックボックスをオンにします。

b.　TCP Protocol オプション ボタンをクリックします。

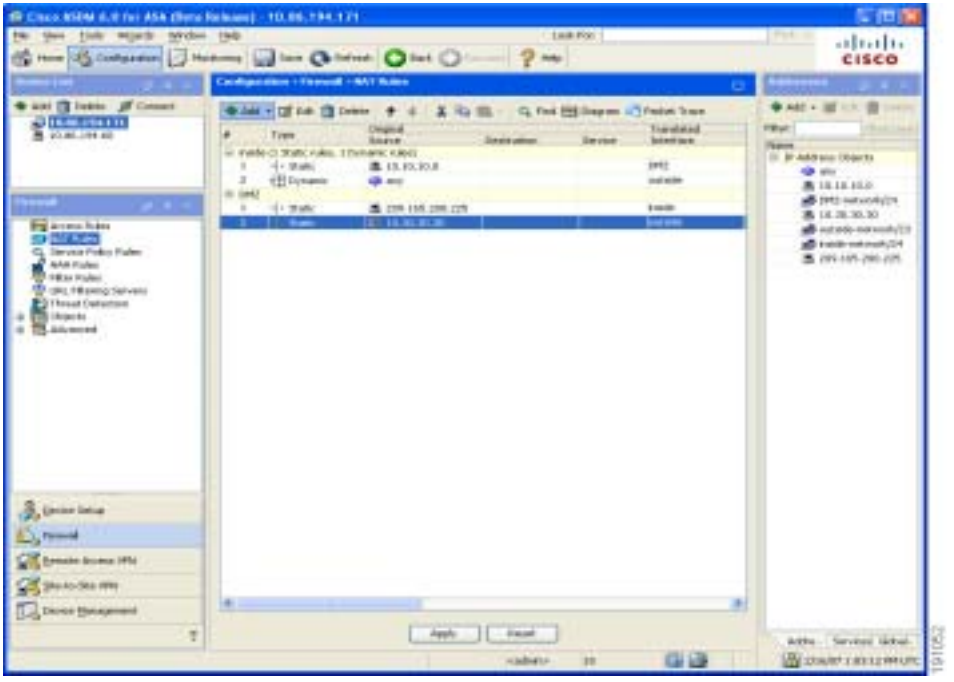
c. Original Port フィールドに 80 を入力します。

d. Translated Port フィールドに 80 を入力します。

e. **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（209,165,200,225）にスタティックにマッピングします。

ステップ 5　規則が予想どおりに作成されたことを確認します。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。

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。インターネットからの着信トラフィックが DMZ Web サーバにアクセスすることを許可するには、DMZ Web サーバ宛の着信 HTTP トラフィックを許可するアクセス コントロールを設定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であること、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 のメイン 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.** Firewall ペインで、**Access Rules** をクリックします。
- **c.** 緑色のプラス記号のアイコンをクリックし、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　Add Access Rule ダイアログボックスで、次の手順を実行します。

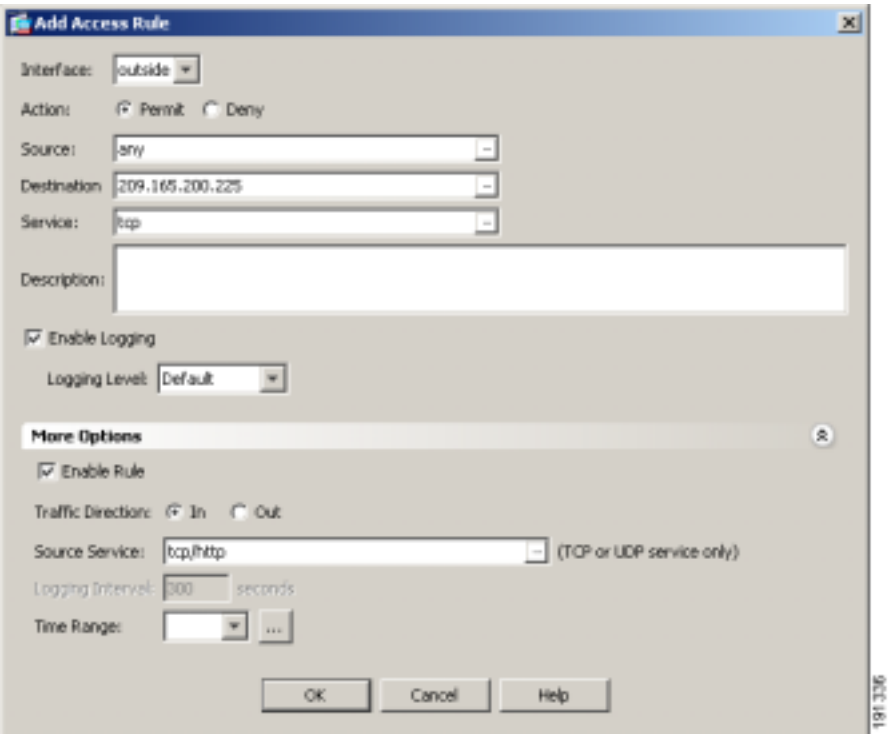
- **a.** Interface プルダウン リストで、outside を選択します。
- **b.** Permit Action オプション ボタンをクリックします。
- **c.** Source フィールドに any を入力します。
- **d.** Destination フィールドで、Web サーバのパブリック IP アドレス（209.165.200.225）を入力します。
- **e.** Service フィールドに tcp を入力します。
- **f.** More Options をクリックします。

g. アクセス コントロール規則をただちにイネーブルにする場合は、Enable Rule チェックボックスをオンにします。

h. Traffic Direction の隣で In をクリックします。

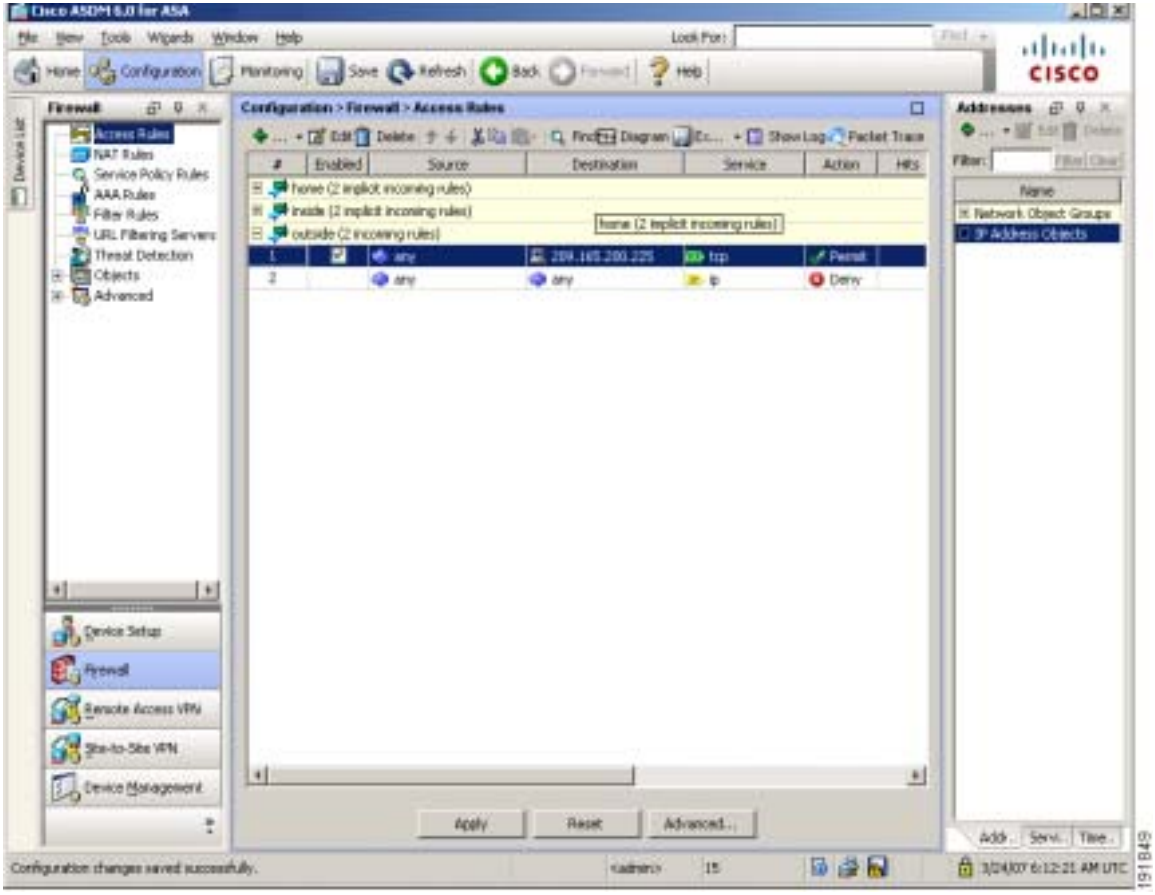
i. Source Service フィールドに tcp/http を入力します。

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。



j. **OK** をクリックし、Security Policy > Access Rules ペインに戻ります。

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。

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、パブリック ネットワーク上のクライアントが、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。

ステップ 3　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*

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 9 章「シナリオ：IPSec リモートアクセス VPN の設定」
Cisco AnyConnect ソフトウェア クライアント用の SSL VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」
ブラウザベースの SSL VPN の設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN の設定」

次の手順

CHAPTER 9

シナリオ：IPSec 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。このタイプの VPN 設定では、リモート ユーザは Cisco VPN クライアントを実行して適応型セキュリティ アプライアンスに接続する必要があります。

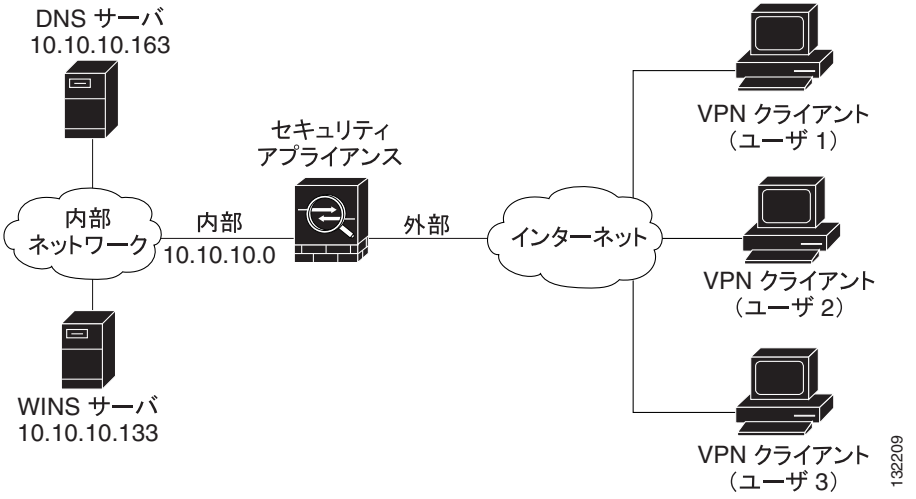
この章では、Easy VPN ソリューションを実装する場合に Easy VPN サーバ（ヘッドエンド デバイスと呼ばれることもあります）を設定する方法について説明します。

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 9-1 は、インターネット経由で VPN クライアント（Cisco Easy VPN ソフトウェアまたはハードウェア 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 9-1　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 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 9-1 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

この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアをまだインストールしていない場合は、P.7-10 の「Web ブラウザを使用した ASDM の起動」を参照してください。

Web ブラウザまたは Java を使用して直接 ASDM にアクセスする場合は、P.7-10 の「Web ブラウザを使用した ASDM の起動」を参照してください。

ASDM Launcher ソフトウェアを使用して ASDM を起動するには、次の手順を実行します。

ステップ 1　デスクトップから、Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。

ステップ 2　適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 3　Username および Password フィールドはブランクのままにします。

（注）　デフォルトで、Cisco ASDM Launcher には Username および Password は設定されていません。

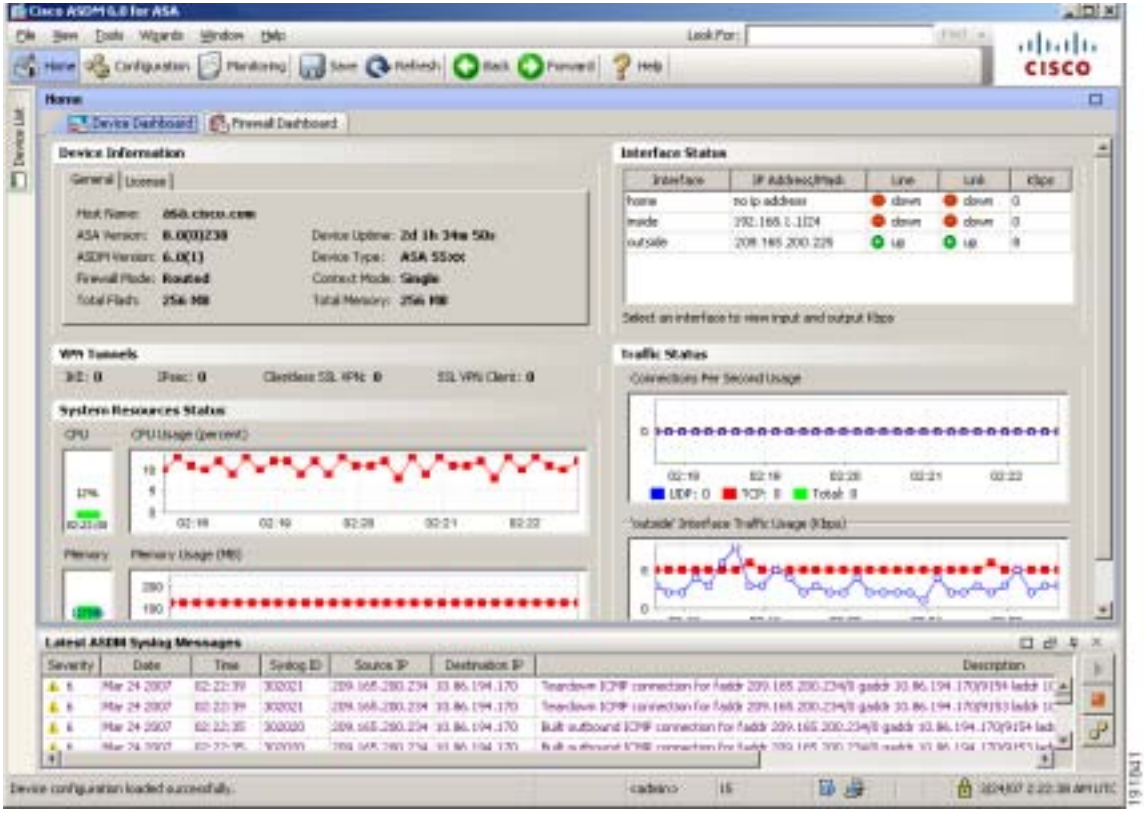
ステップ 4　OK をクリックします。

ステップ 5　証明書を受け入れるよう要求するセキュリティ警告が表示されたら、**Yes** をクリックします。

適応型セキュリティ アプライアンスは更新するソフトウェアがあるかどうかを確認し、ある場合は自動的にダウンロードします。

ASDM のメイン ウィンドウが表示されます。

IPsec リモートアクセス VPN シナリオの実装



IPsec リモートアクセス VPN の設定

リモートアクセス VPN 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、**Ipsec 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** 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。

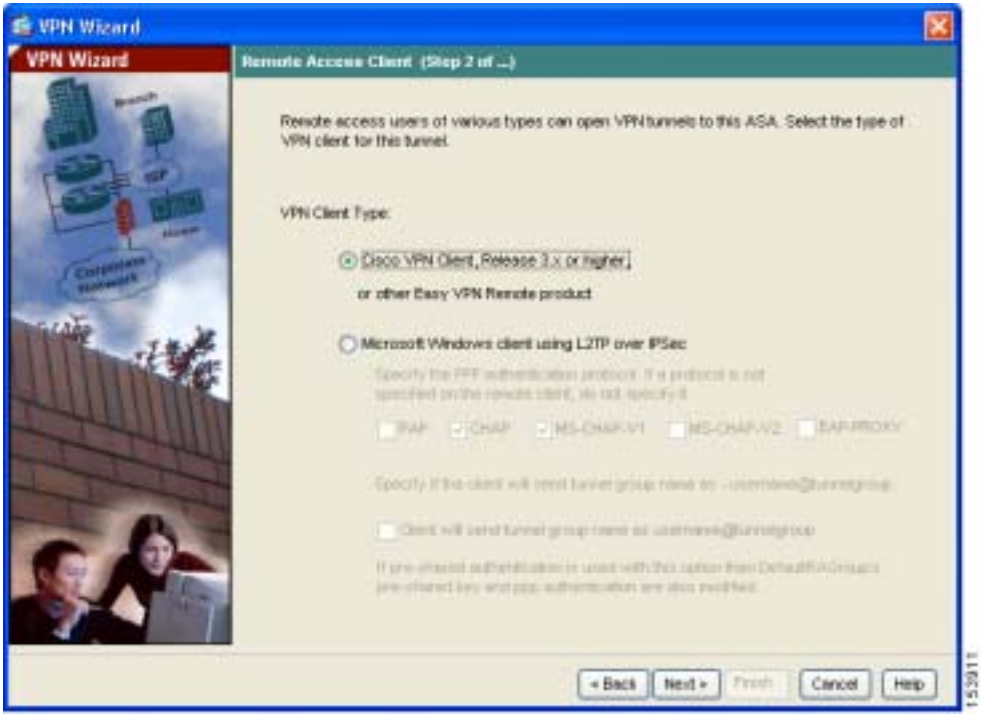
c. **Next** をクリックして続行します。

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。

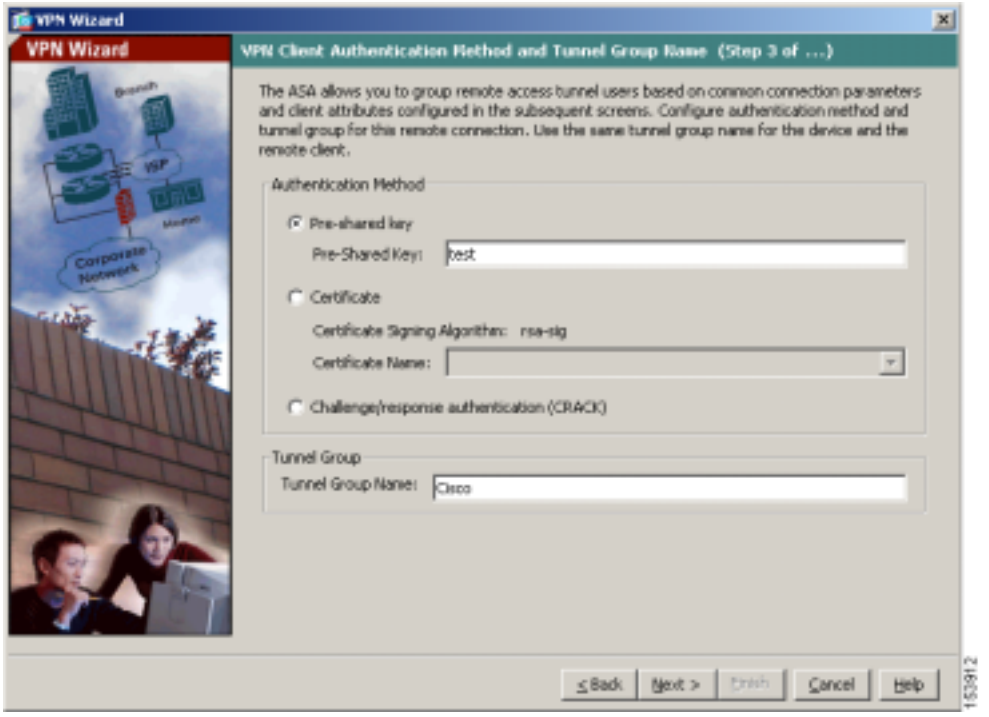
VPN トンネル グループ名と認証方式の指定

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、IPsec ネゴシエーションに使用します。
- 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 ウィンドウを使用して、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。

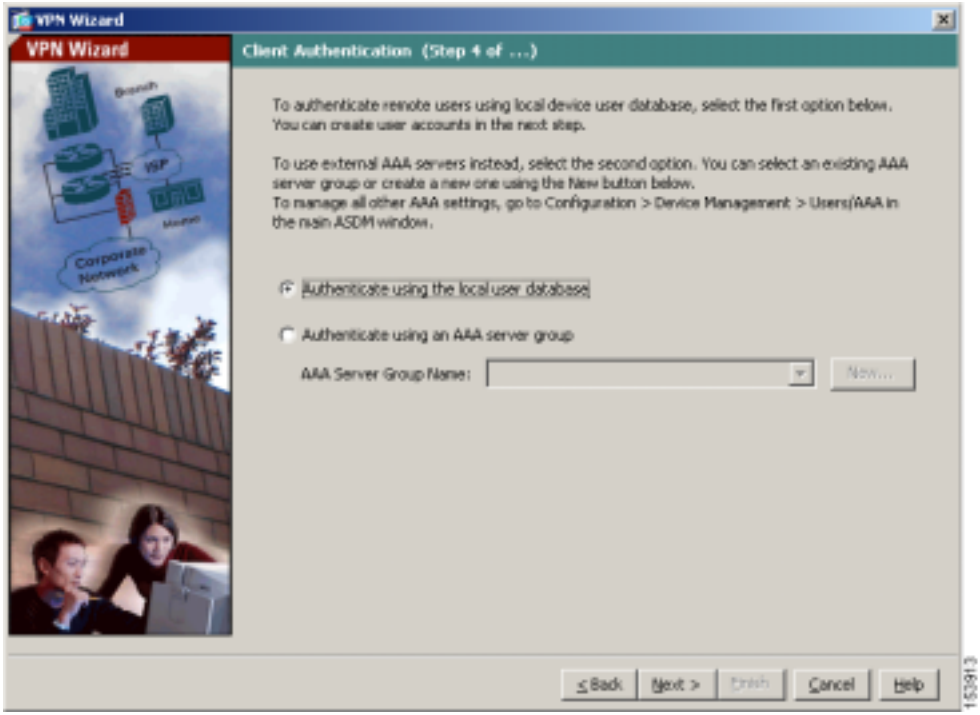
VPN Wizard の Step 4 で、次の手順を実行します。

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. Authenticate using an AAA server group ドロップダウン リストから事前設定済みのサーバ グループを選択するか、または **New** をクリックして、新しい AAA サーバ グループを追加します。



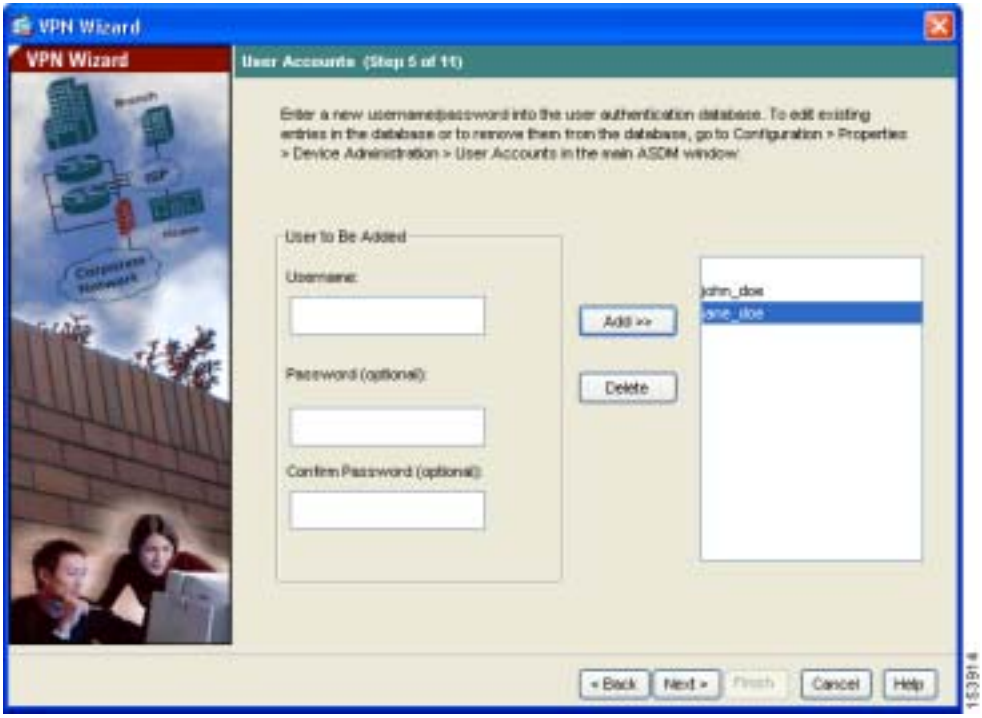
ステップ 3　**Next** をクリックして続行します。

（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。



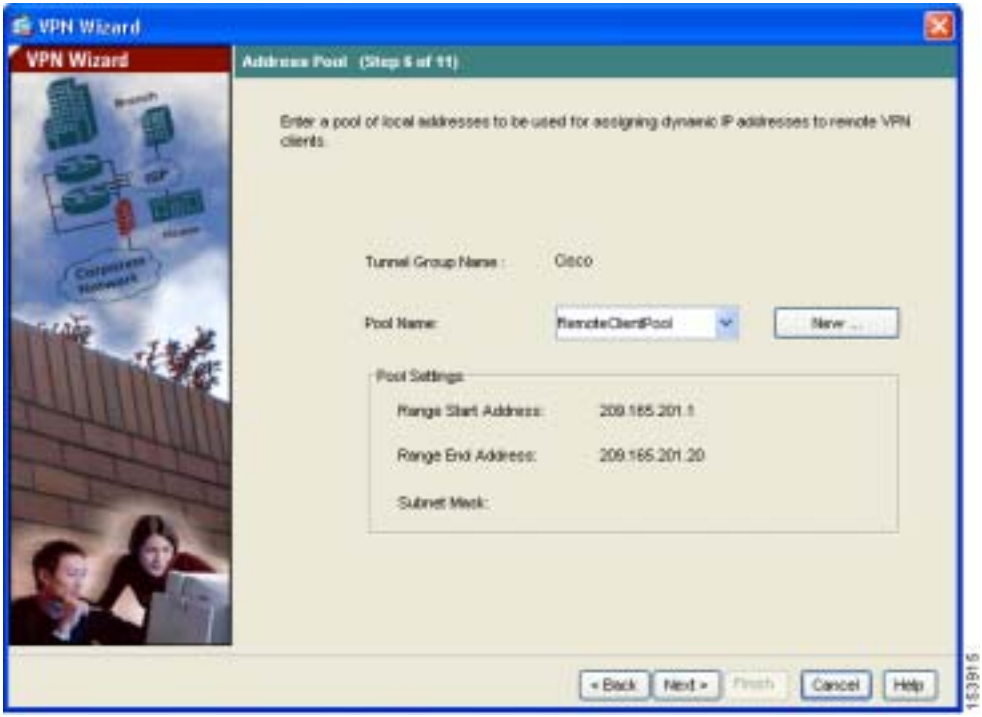
ステップ 2　新しいユーザの追加が終了したら、**Next** をクリックして続行します。

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。

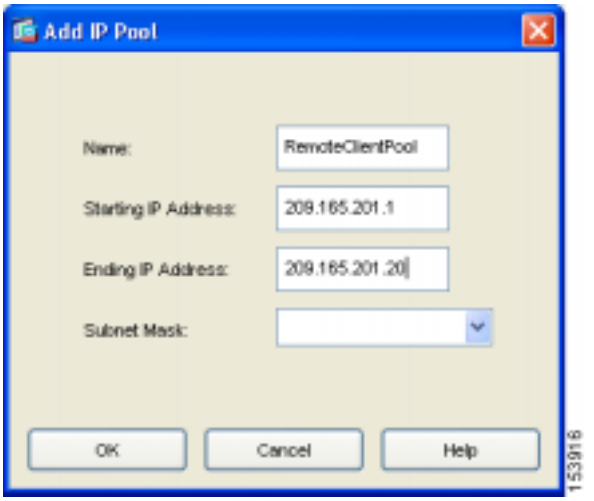
VPN Wizard の Step 6 で、次の手順を実行します。

ステップ 1　Pool Name 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）サブネット マスクを入力するか、または Subnet Mask ドロップダウン リストから、IP アドレスの範囲のサブネット マスクを選択します。

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。

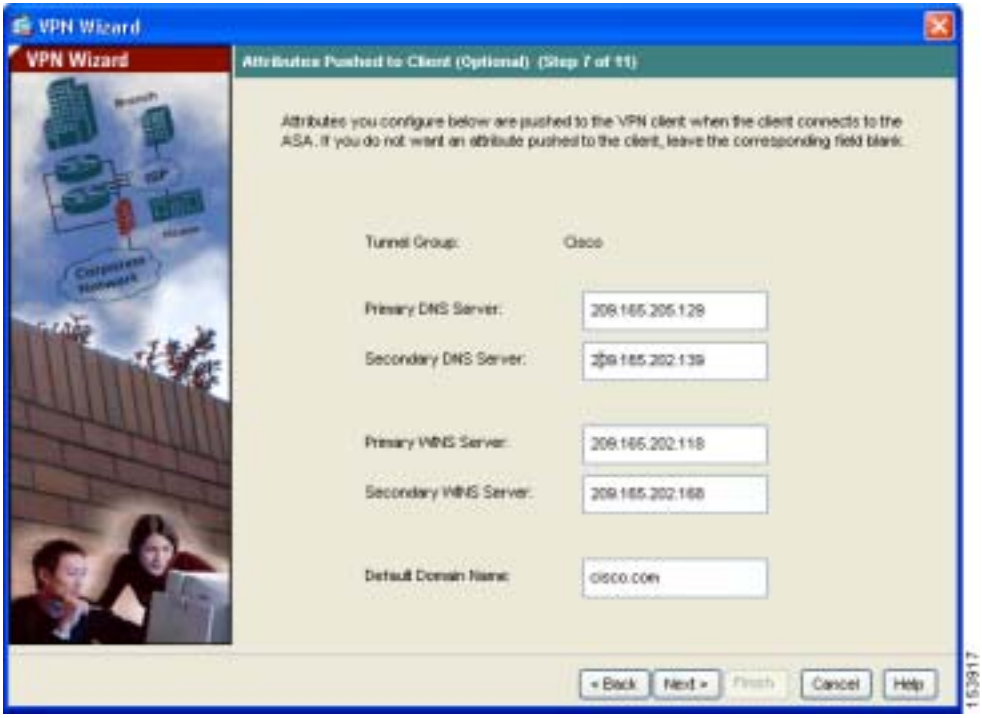
クライアント アトリビュートの設定

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。



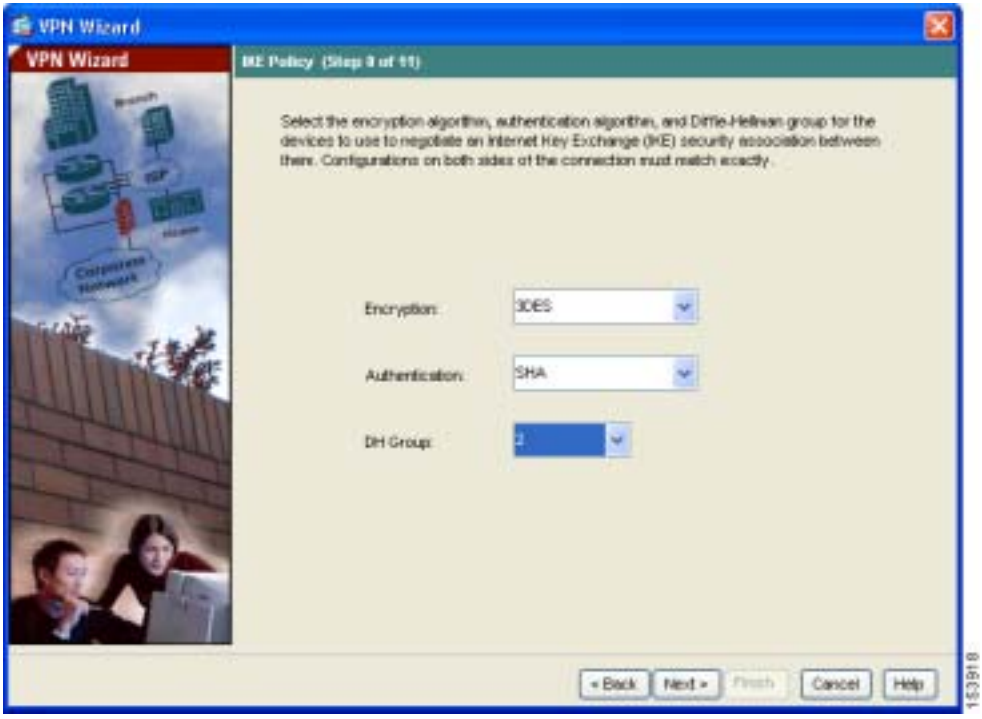
ステップ 2　**Next** をクリックして続行します。

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、または 5）を選択します。

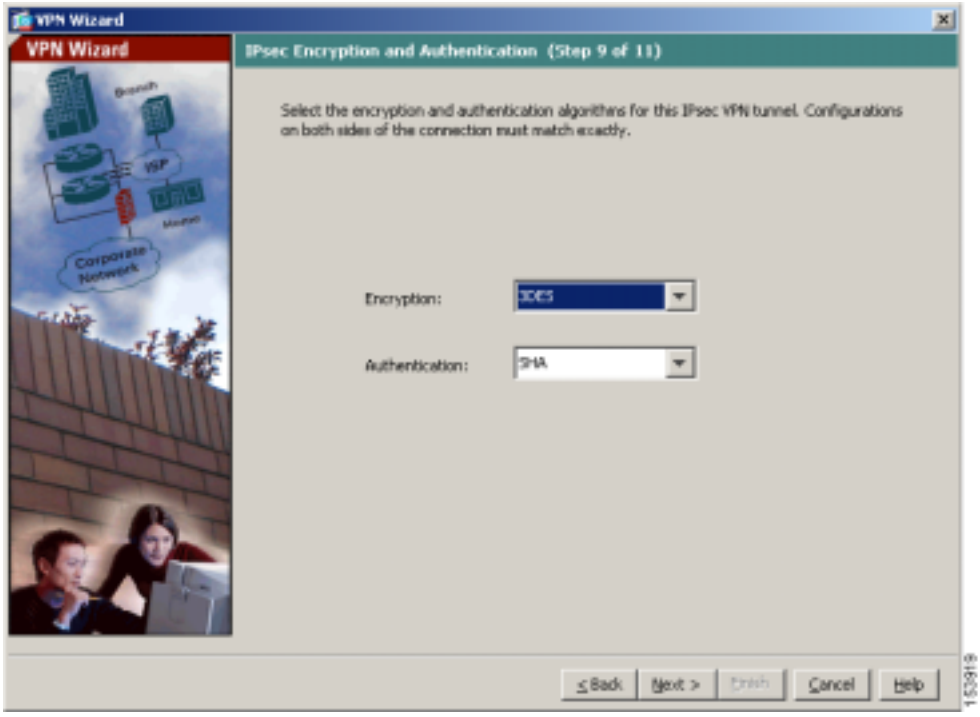


ステップ 2　**Next** をクリックして続行します。

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

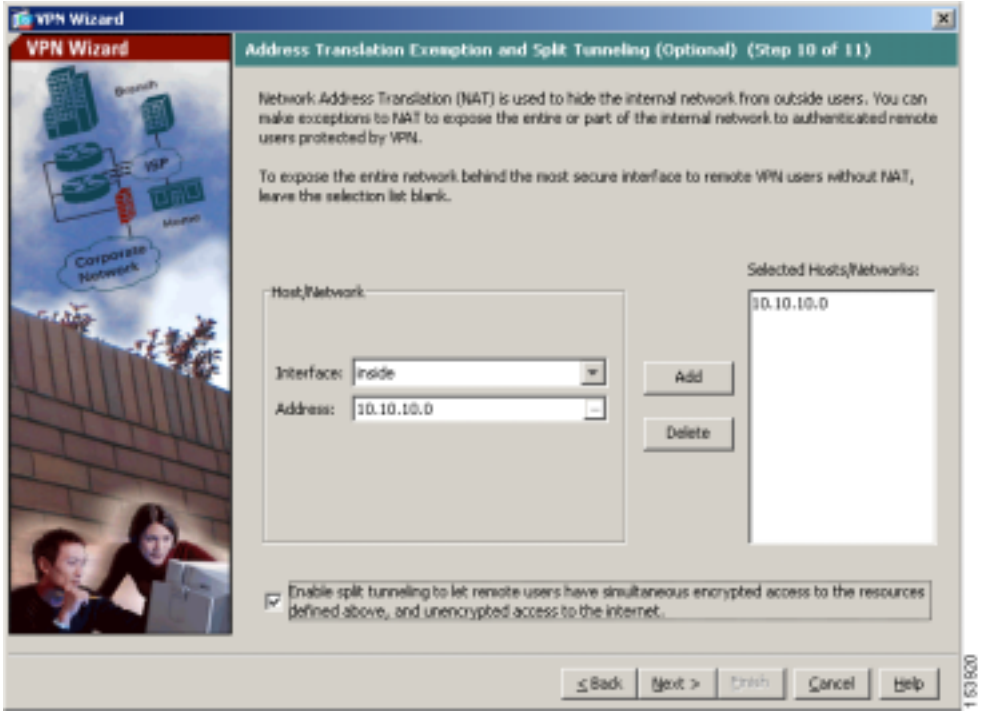
スプリット トンネリングを使用すると、リモートアクセス IPsec クライアントは一定の条件に従い、パケットを暗号化形式で IPsec トンネルに送信したり、テキスト形式でネットワーク インターフェイスに送信したりすることができます。

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

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 領域のホスト、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。

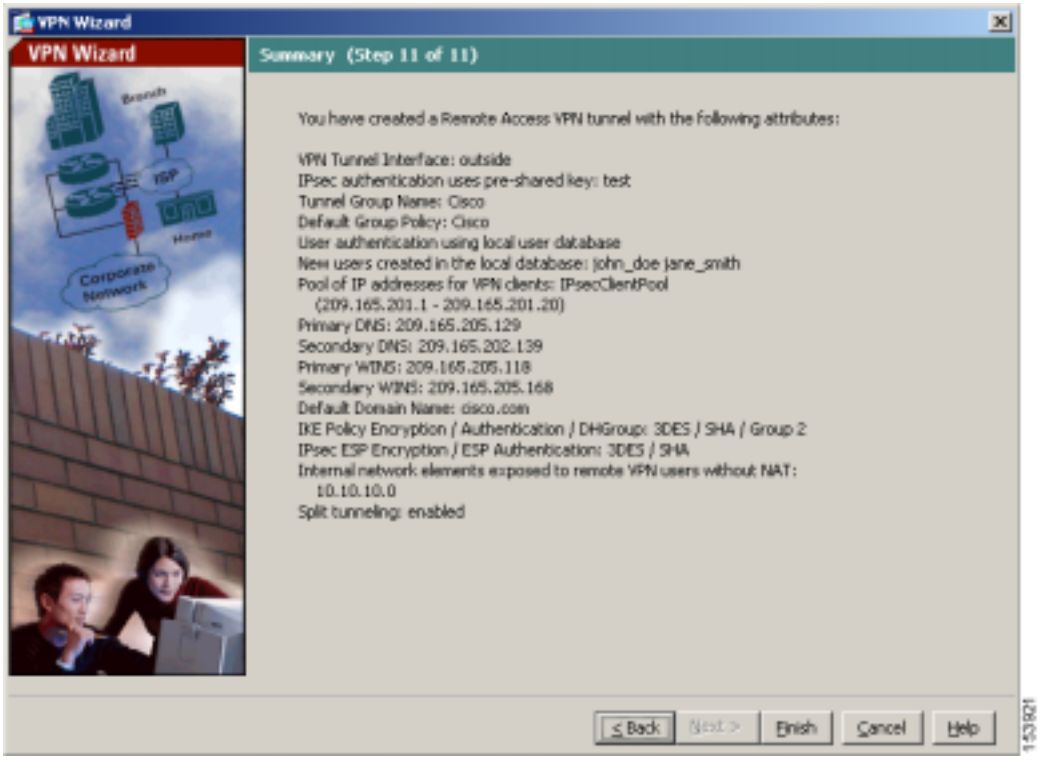


(注)　画面の下部にある **Enable split tunneling...** チェックボックスをオンにして、スプリット トンネリングをイネーブルにします。スプリット トンネリングを使用すると、設定したネットワークの外部のトラフィックを、暗号化された VPN トンネルを使用せずに直接インターネットに送出できるようになります。

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 設定の確認

VPN Wizard の Step 11 で、新しい 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

モバイル ユーザやテレワーカのためのセキュアな接続用のエンドツーエンドの暗号化 VPN トンネルを確立するには、Cisco VPN クライアント ソフトウェアを入手してください。

Cisco Systems VPN クライアントの詳細については、次の URL を参照してください。http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html

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 8 章「シナリオ：DMZ の設定」
Cisco AnyConnect ソフトウェア クライアント用の SSL VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」
クライアントレス（ブラウザベース）SSL VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN の設定」

次の手順

CHAPTER 10

シナリオ：Cisco AnyConnect VPN Client 用の接続の設定

この章では、リモート ユーザが Cisco AnyConnect VPN Client を使用して SSL 接続を確立できるように、適応型セキュリティ アプライアンスを設定する方法ついて説明します。

この章は、次の項で構成されています。

SSL VPN Client 接続について

SSL VPN Client をセットアップすると、ユーザは接続の確立を試行する前に、ソフトウェア クライアントをインストールする必要がなくなります。その代わり、リモート ユーザは Cisco SSL VPN インターフェイスの IP アドレスまたは DNS 名をブラウザに入力します。ブラウザによってこのインターフェイスに接続され、SSL VPN のログイン画面が表示されます。ユーザの認証が成功し、適応型セキュリティ アプライアンスによってユーザがクライアントを要求していることが確認されると、リモート コンピュータのオペレーティング システムに一致するクライアントがプッシュされます。

（注） 初めて Cisco AnyConnect VPN Client をインストールまたはダウンロードするときに、管理権限が必要です。

ダウンロード後、Cisco AnyConnect VPN Client は自動的にインストールおよび設定が行われ、セキュアな SSL 接続が確立されます。接続が終了すると、適応型セキュリティ アプライアンスの設定に応じて、このクライアント ソフトウェアはそのまま残るか、または自動的にアンインストールされます。

リモート ユーザが以前に SSL VPN 接続を確立したことがあり、クライアント ソフトウェアをアンインストールしないよう設定している場合、ユーザ認証のときに、適応型セキュリティ アプライアンスがクライアントのバージョンを調べ、必要に応じてアップグレードします。

Cisco AnyConnect VPN Client ソフトウェアの入手

適応型セキュリティ アプライアンスは、Cisco の Web サイトから AnyConnect VPN Client ソフトウェアを入手します。この章では、コンフィギュレーション ウィザードを使用して SSL VPN を設定する手順について説明します。Cisco SSL VPN ソフトウェアは、設定プロセス中に適応型セキュリティ アプライアンスにダウンロードできます。

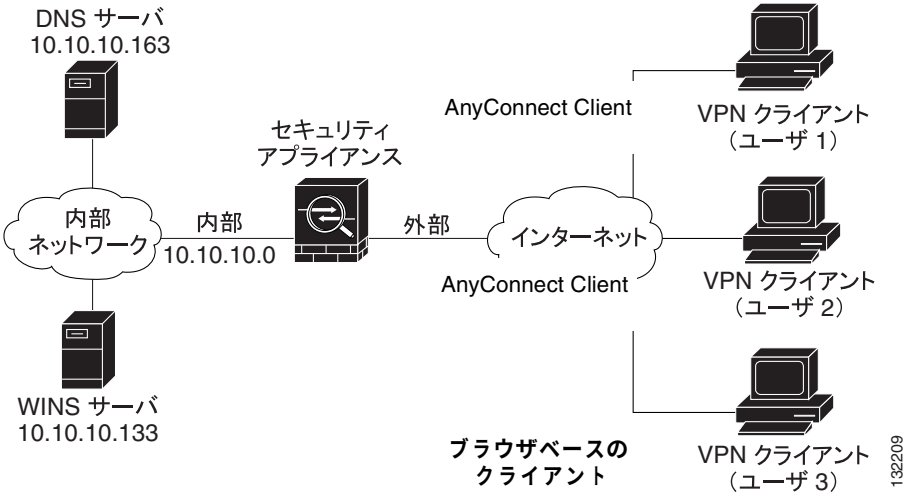
ユーザは、AnyConnect VPN Client を適応型セキュリティ アプライアンスからダウンロードできます。あるいは、システム管理者が手動でリモート PC にインストールできます。このクライアント ソフトウェアのインストールの詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

適応型セキュリティ アプライアンスは、グループ ポリシーまたは接続を確立するユーザのユーザ名アトリビュートに基づいて、クライアント ソフトウェアをプッシュします。ユーザが接続を確立するたびに自動的にクライアントをプッシュ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か、リモート ユーザに対してクライアントをダウンロードするかどうかを指定するように求めるよう設定できます。後者の設定では、ユーザが応答しなかった場合に、タイムアウト後にクライアントをプッシュするか、または SSL VPN のログイン画面を表示するように適応型セキュリティ アプライアンスを設定できます。

AnyConnect SSL VPN Client を使用したトポロジの例

図 10-1 は、AnyConnect SSL VPN ソフトウェアを実行しているクライアントからの要求を受け付け、SSL 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。適応型セキュリティ　アプライアンスは、AnyConnect VPN ソフトウェアを実行しているクライアントおよびブラウザベースのクライアントへの接続をサポートしています。

図 10-1　　SSL VPN シナリオ用のネットワーク レイアウト



Cisco SSL VPN シナリオの実装

この項では、Cisco AnyConnect SSL VPN 接続を受け付けるように適応型セキュリティ アプライアンスを設定する方法について説明します。設定値の例は、図 10-1 で示す SSL VPN 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 AnyConnect SSL 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。

- リモート ユーザの接続先である、適応型セキュリティ アプライアンス上のインターフェイスの名前。
- デジタル証明書。

  適応型セキュリティ アプライアンスは、デフォルトで自己署名証明書を生成します。ただし、より高度なセキュリティのためには、システムを実稼働環境に配置する前に、公式に信頼できる SSL VPN 証明書を購入する必要があります。
- 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 SSL AnyConnect 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）。
- 認証に AAA サーバを使用している場合：

  — AAA サーバ グループ名

- 使用する認証プロトコル（TACACS、SDI、NT、Kerberos、LDAP）
- AAA サーバの IP アドレス
- 認証に使用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
- AAA サーバでの認証を行うための秘密鍵

ASDM の起動

この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアをまだインストールしていない場合は、P.7-7 の「ASDM Launcher のインストール」を参照してください。

Web ブラウザまたは Java を使用して直接 ASDM にアクセスする場合は、P.7-10 の「Web ブラウザを使用した ASDM の起動」を参照してください。

ASDM Launcher ソフトウェアを使用して ASDM を起動するには、次の手順を実行します。

ステップ 1　デスクトップから、Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。

ステップ 2　適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 3　Username および Password フィールドはブランクのままにします。

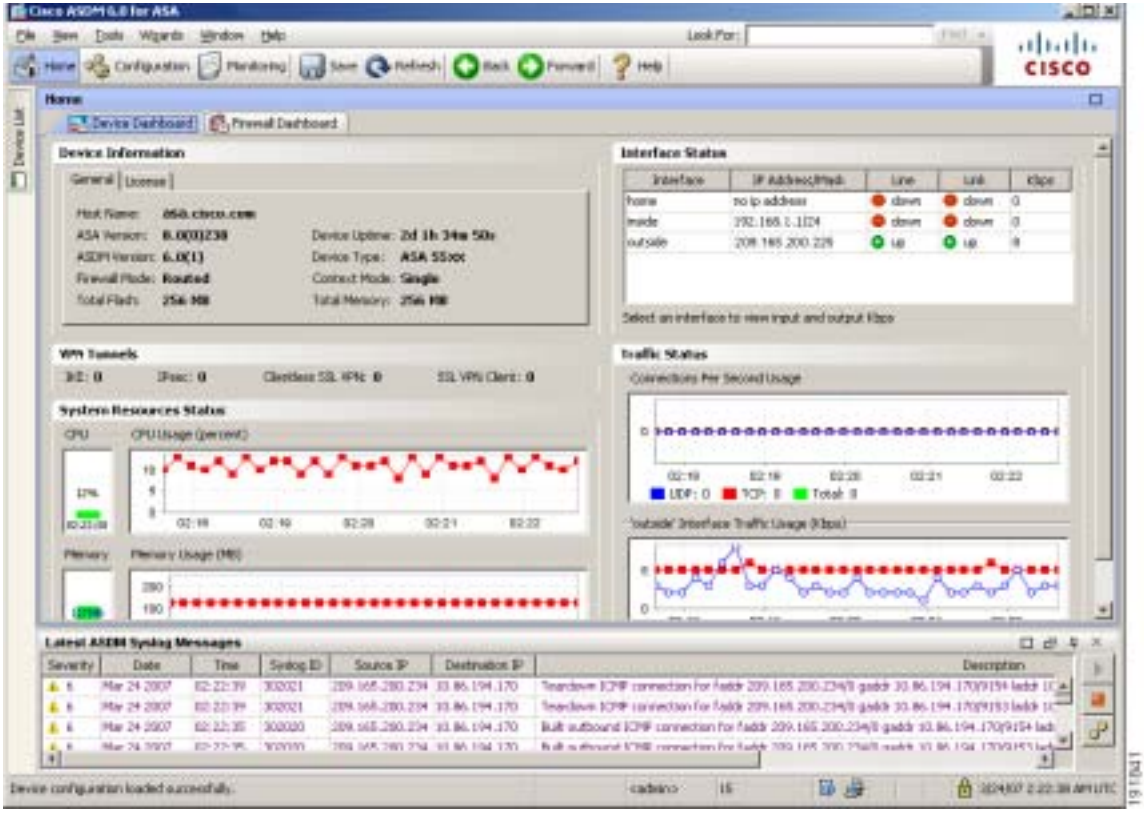
(注)　デフォルトで、Cisco ASDM Launcher には Username および Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書を受け入れるよう要求するセキュリティ警告が表示されたら、**Yes** をクリックします。

ASA は更新するソフトウェアがあるかどうかを確認し、ある場合は自動的にダウンロードします。

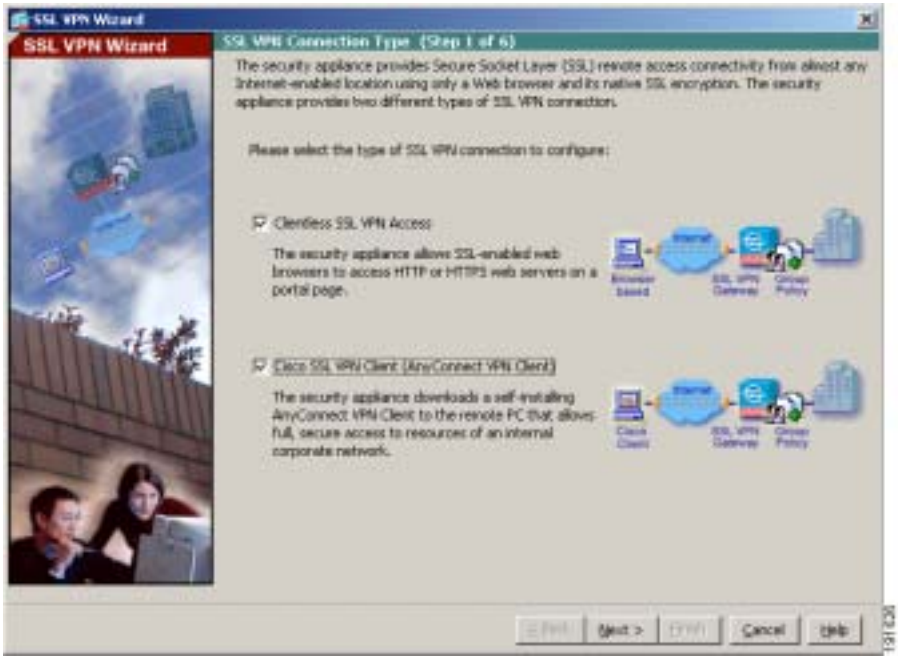
ASDM のメイン ウィンドウが表示されます。


Cisco ASDM 6.0 for ASA
Home
Device Dashboard
Firewall Dashboard
Device Information
Interface Status
VPN Tunnels
Traffic Status
System Resources Status
Latest ASDM Syslog Messages
CISCO

Cisco AnyConnect VPN Client のための適応型セキュリティ アプライアンスの設定

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、**SSL VPN Wizard** を選択します。SSL VPN Wizard の Step 1 画面が表示されます。



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

a. **Cisco SSL VPN Client** チェックボックスをオンにします。
b. **Next** をクリックして続行します。

SSL VPN インターフェイスの指定

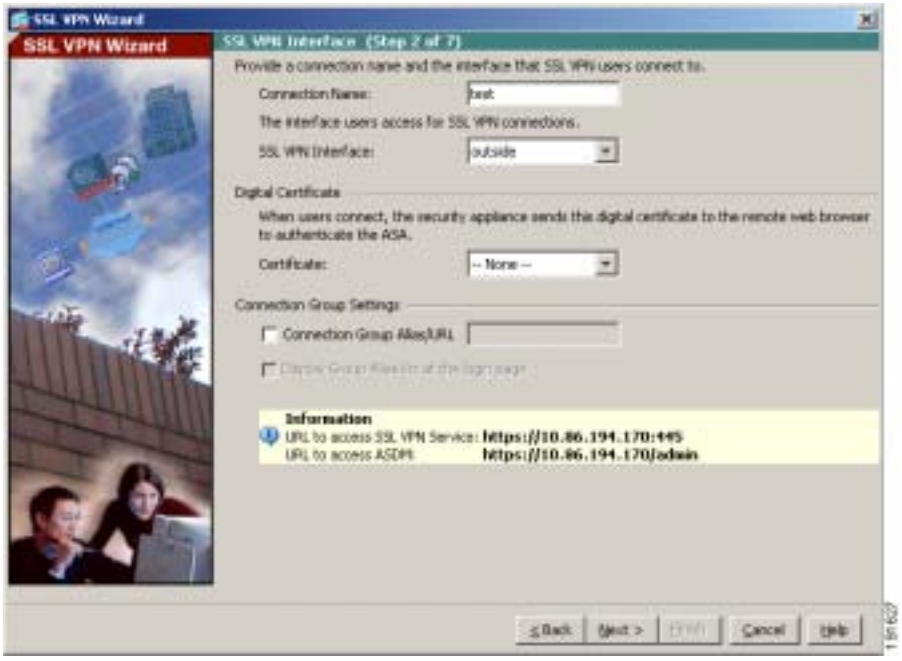
SSL VPN Wizard の Step 2 で、次の手順を実行します。

ステップ 1　リモート ユーザの接続先の接続名を指定します。

ステップ 2　SSL VPN Interface ドロップダウン リストで、リモート ユーザの接続先のインターフェイスを選択します。ユーザがこのインターフェイスへの接続を確立すると、SSL VPN ポータル ページが表示されます。

ステップ 3　Certificate ドロップダウン リストで、ASA が認証のためにリモート ユーザに送信する証明書を選択します。

（注）　適応型セキュリティ アプライアンスは、デフォルトで自己署名証明書を生成します。ただし、より高度なセキュリティのためには、システムを実稼働環境に配置する前に、公式に信頼できる SSL VPN 証明書を購入する必要があります。



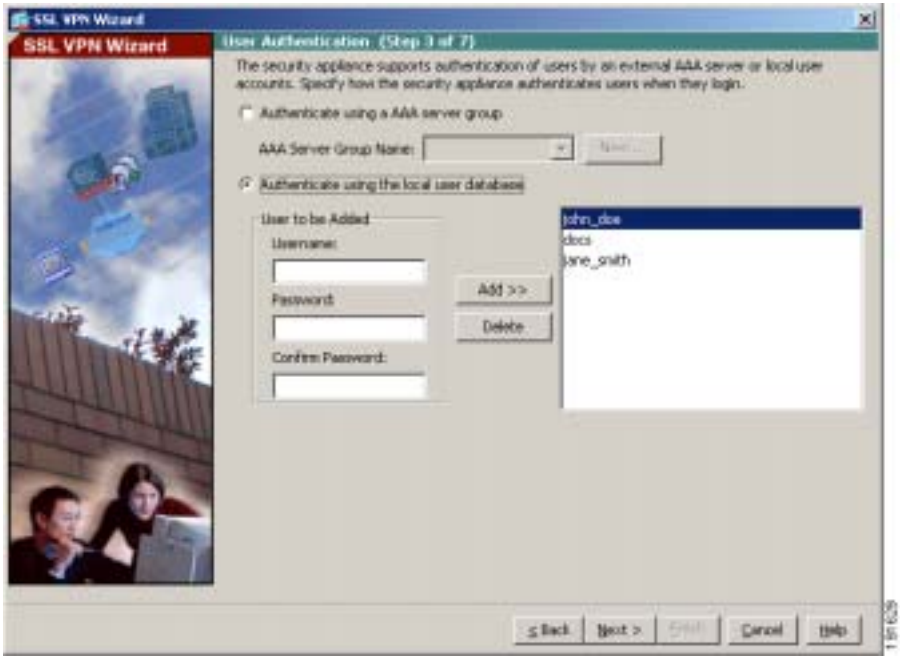
ステップ 4　**Next** をクリックして続行します。

ユーザ認証方式の指定

SSL VPN Wizard の Step 3 で、次の手順を実行します。

ステップ 1　認証に AAA サーバまたはサーバ グループを使用している場合は、次の手順を実行します。

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



b. AAA サーバ グループ名を指定します。

c. 既存の AAA サーバ グループ名をドロップダウン リストから選択するか、または **New** をクリックして、新しいサーバ グループを作成します。

新しい AAA サーバ グループを作成するには、**New** をクリックします。New Authentication Server Group ダイアログボックスが表示されます。

このダイアログボックスで、次のものを指定します。

- サーバ グループ名
- 使用する認証プロトコル（RADIUS、TACACS、SDI、NT、Kerberos、LDAP）
- AAA サーバの IP アドレス
- 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
- AAA サーバとの通信に使用する秘密鍵

OK をクリックします。

ステップ 2　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。

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 3　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。

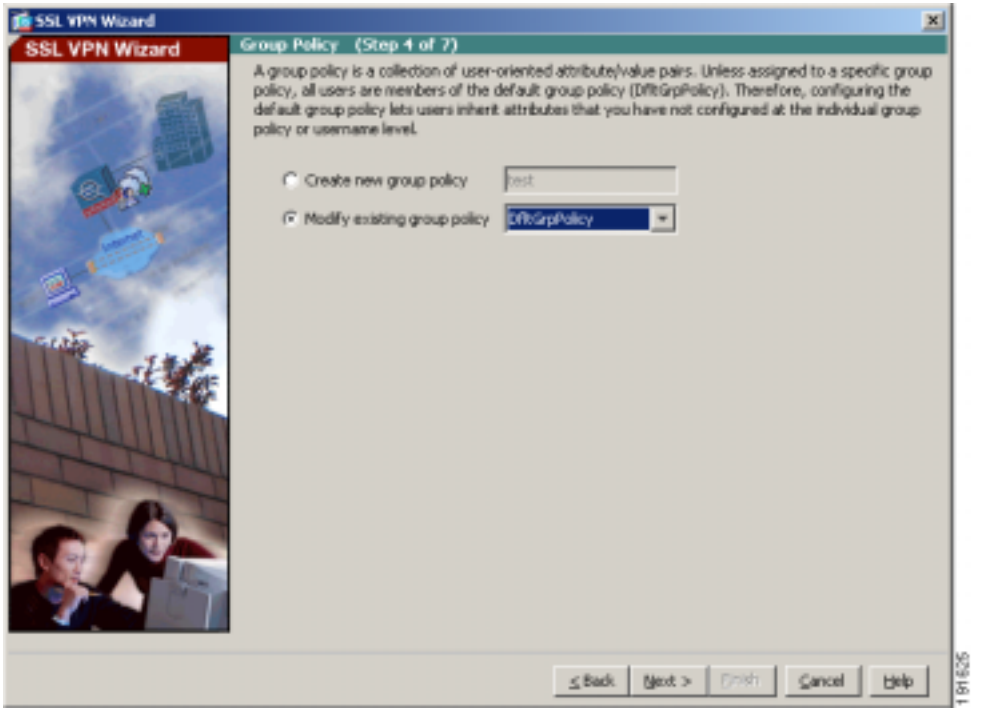
グループ ポリシーの指定

SSL VPN Wizard の Step 4 で、次の手順を実行してグループ ポリシーを指定します。

ステップ 1　**Create new group policy** オプション ボタンをクリックして、グループ名を指定します。

あるいは、

Modify existing group policy オプション ボタンをクリックして、ドロップダウン リストからグループを選択します。



ステップ 2　**Next** をクリックします。

ステップ 3　SSL VPN Wizard の Step 5 が表示されます。このステップは AnyConnect VPN Client 接続には適用されないため、もう一度 **Next** をクリックします。

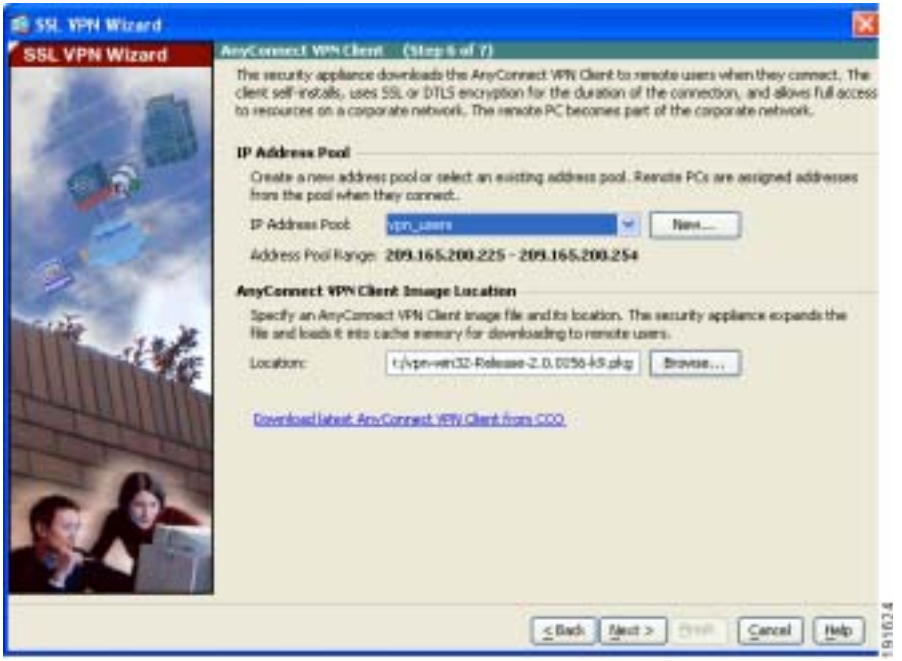
Cisco AnyConnect VPN Client の設定

リモート クライアントが Cisco VPN Client を使用して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。

また、適応型セキュリティ アプライアンスがユーザにプッシュできるようにするため、AnyConnect ソフトウェアのロケーションも指定する必要があります。

SSL VPN Wizard の Step 6 で、次の手順を実行します。

ステップ 1　事前設定済みのアドレス プールを使用するには、IP Address Pool ドロップダウンリストからアドレス プールの名前を選択します。



ステップ 2　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。

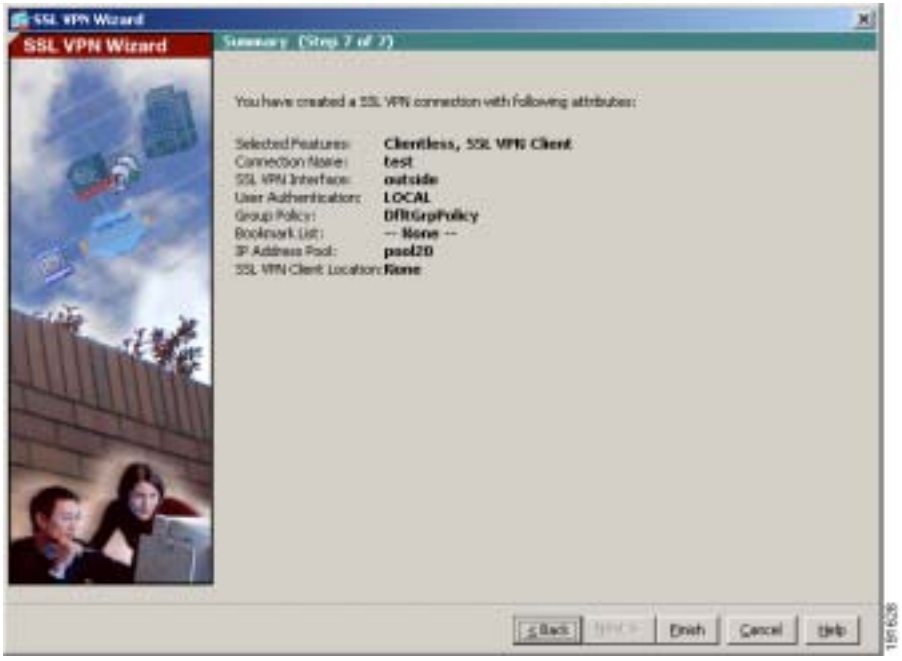
ステップ 3　AnyConnect VPN Client ソフトウェア イメージのロケーションを指定します。

最新バージョンのソフトウェアを入手するには、cisco.com で Download Latest AnyConnect VPN Client をクリックします。この操作により、クライアント ソフトウェアが PC にダウンロードされます。

ステップ 4　**Next** をクリックして続行します。

リモートアクセス VPN 設定の確認

SSL VPN Wizard の Step 7 で、設定を見直して正しいことを確認します。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

AnyConnect VPN 接続をサポートするため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 8 章「シナリオ：DMZ の設定」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN の設定」
リモートアクセス IPSec VPN の設定	第 9 章「シナリオ：IPSec リモートアクセス VPN の設定」
クライアントレス（ブラウザベース）SSL VPN の設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」

CHAPTER 11

シナリオ：SSL VPN クライアントレス接続

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、ソフトウェア クライアントを使用せずに（クライアントレスで）リモートアクセス SSL VPN 接続を受け付ける方法について説明します。クライアントレス SSL VPN を使用すると、Web ブラウザを使用してインターネットを経由するセキュアな接続（トンネル）を作成できます。この方法により、セキュアなアクセスを、ソフトウェア クライアントおよびハードウェア クライアントを持たないオフサイト ユーザに提供できます。

この章は、次の項で構成されています。

クライアントレス SSL VPN について

クライアントレス SSL VPN 接続は、インターネット上のほぼすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションにセキュアにかつ簡単にアクセスできるようにするものです。次のものが含まれます。

- 内部の Web サイト
- Web 対応のアプリケーション
- NT/Active Directory および FTP ファイルの共有資源
- 電子メール プロキシ（POP3S、IMAP4S、および SMTPS など）
- MS Outlook Web アクセス
- MAPI
- アプリケーション アクセス（他の TCP ベースのアプリケーションにアクセスするためのポート転送）およびスマート トンネル

クライアントレス SSL VPN は Secure Sockets Layer Protocol（SSL）およびその後継の Transport Layer Security（TLSI）を使用して、リモート ユーザとサポートされている特定の内部リソース（中央サイトに設定されている）との間にセキュアな接続を提供します。適応型セキュリティ アプライアンスはプロキシする必要のある接続を認識し、HTTP サーバは認証サブシステムとやりとりしてユーザを認証します。

ネットワーク管理者は、クライアントレス SSL VPN のユーザ別にグループ単位でリソースへのアクセスを提供します。

クライアントレス SSL VPN 接続のセキュリティ上の考慮事項

適応型セキュリティ アプライアンス上のクライアントレス SSL VPN 接続は、特に SSL 対応サーバとの通信方法や証明書の検証方法の点で、リモートアクセス IPsec 接続と異なります。

クライアントレス SSL VPN 接続では、適応型セキュリティ アプライアンスは、エンド ユーザの Web ブラウザとターゲット Web サーバとの間のプロキシとして機能します。ユーザが SSL 対応の Web サーバに接続すると、適応型セキュリティ アプライアンスはセキュアな接続を確立し、サーバの SSL 証明書を検証します。エンド ユーザのブラウザが提示された証明書を受信することはないため、証明書を調べたり検証したりはできません。

適応型セキュリティ アプライアンス上の現在のクライアントレス SSL VPN の実装では、有効期限が切れた証明書を提示するサイトとの通信は許可されていません。また、適応型セキュリティ アプライアンスが信頼できる CA 証明書を検証することもありません。このため、ユーザは、SSL 対応の Web サーバとの通信の前に、このサーバが提示する証明書を分析することはできません。

SSL 証明書に含まれるリスクを最小限にするには、次のようにします。

1. クライアントレス SSL VPN アクセスを必要とするすべてのユーザからなるグループ ポリシーを設定し、このグループ ポリシーに対してのみクライアントレス SSL VPN アクセスをイネーブルにします。
2. クライアントレス SSL VPN ユーザのインターネット アクセスを制限します。たとえば、ユーザがクライアントレス SSL VPN 接続を使用してアクセスできるリソースを制限します。これを行うには、まず、ユーザによるインターネット上の一般コンテンツへのアクセスを制限します。次に、クライアントレス SSL VPN のユーザによるアクセスを制限する、内部ネットワーク上の特定のターゲットへのリンクを設定します。
3. ユーザ教育を行います。SSL 対応のサイトがプライベート ネットワーク内に存在しない場合、ユーザはクライアントレス SSL VPN 接続でこのようなサイトにアクセスしてはいけません。ユーザは別のブラウザ ウィンドウを開いてこのようなサイトにアクセスし、ブラウザを使用して提示された証明書を表示します。

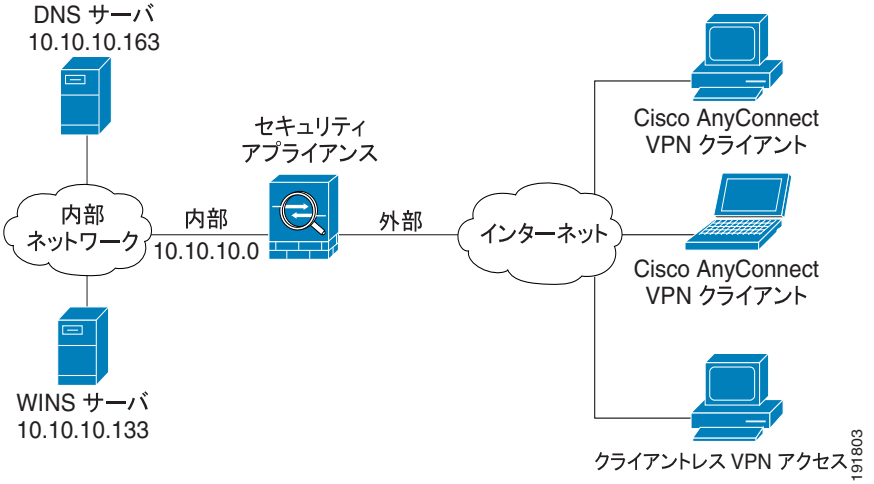
適応型セキュリティ アプライアンスは、クライアントレス SSL VPN 接続に対して次の機能はサポートしていません。

- NAT：グローバルに一意の IP アドレスの必要性を小さくする。
- PAT：複数のアウトバウンド セッションが 1 つの IP アドレスから発信されることを許可する。

ブラウザベースの SSL VPN アクセスを使用したネットワーク例

図 11-1 は、Web ブラウザを使用したインターネット経由での SSL VPN 接続を受け付け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 11-1　SSL VPN 接続のネットワーク レイアウト



クライアントレス SSL VPN シナリオの実装

この項では、Web ブラウザからの SSL VPN 要求を受け付けるように適応型セキュリティ アプライアンスを設定する方法について説明します。設定値の例は、図 11-1 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。

- リモート ユーザの接続先である、適応型セキュリティ アプライアンス上のインターフェイスの名前。リモート ユーザがこのインターフェイスに接続すると、SSL VPN ポータル ページが表示されます。
- デジタル証明書。

  ASA 5500 シリーズは、デフォルトで自己署名証明書を生成します。より高度なセキュリティのために、またブラウザの警告メッセージを表示しないようにするために、システムを実稼働環境に配置する前に、公式に信頼できる SSL VPN 証明書を購入する必要があります。
- 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）。
- 認証に AAA サーバを使用している場合は、AAA サーバ グループ名。
- AAA サーバ上のグループ ポリシーに関する次の情報：

  — サーバ グループ名

- 使用する認証プロトコル（TACACS、SDI、NT、Kerberos、LDAP）
- AAA サーバの IP アドレス
- 認証に使用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
- AAA サーバでの認証を行うための秘密鍵

- リモート ユーザが接続を確立したときに SSL VPN ポータル ページに表示する、内部 Web サイトまたはページのリスト。このページは、ユーザが最初に接続を確立したときに表示されるものであるため、リモート ユーザにとって最もよく使用するターゲットで構成されている必要があります。

ASDM の起動

この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアをまだインストールしていない場合は、P.7-7 の「ASDM Launcher のインストール」を参照してください。

Web ブラウザまたは Java を使用して直接 ASDM にアクセスする場合は、P.7-10 の「Web ブラウザを使用した ASDM の起動」を参照してください。

ASDM Launcher ソフトウェアを使用して ASDM を起動するには、次の手順を実行します。

ステップ 1　デスクトップから、Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。

ステップ 2　適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 3　Username および Password フィールドはブランクのままにします。

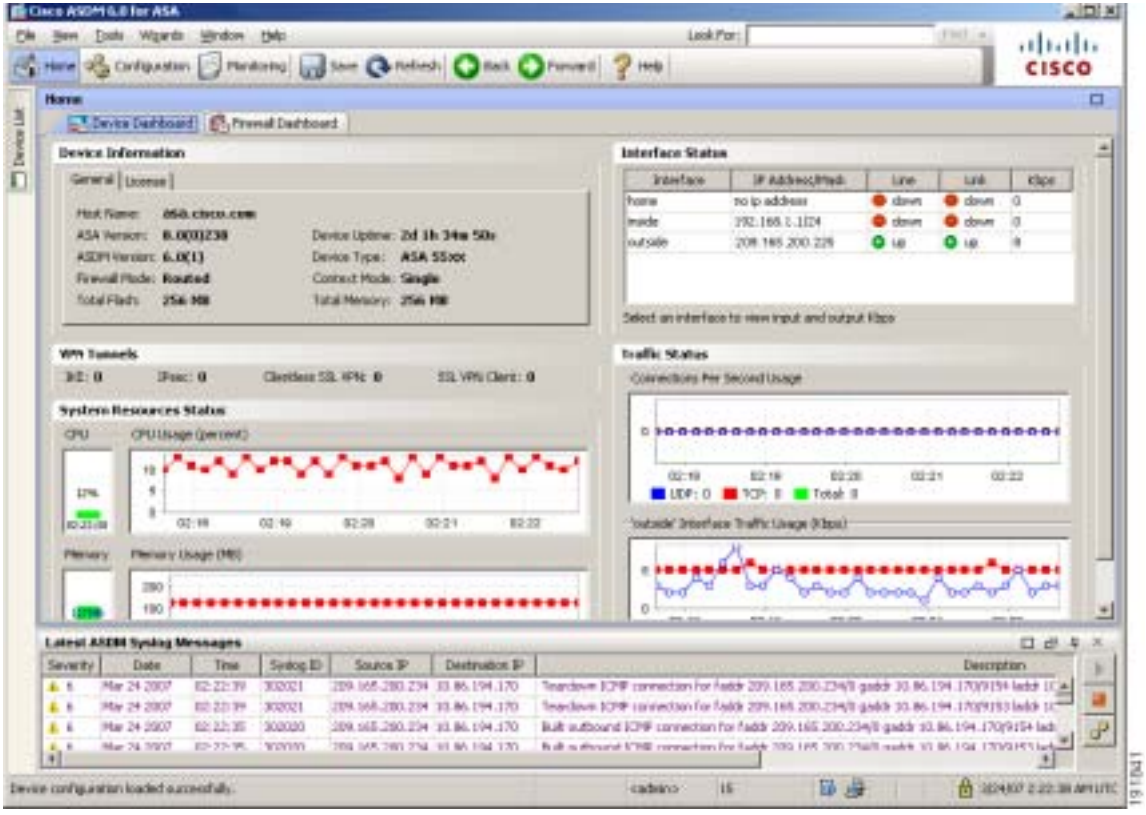
（注）　デフォルトで、Cisco ASDM Launcher には Username および Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書を受け入れるよう要求するセキュリティ警告が表示されたら、**Yes** をクリックします。

適応型セキュリティ アプライアンスは更新するソフトウェアがあるかどうかを確認し、ある場合は自動的にダウンロードします。

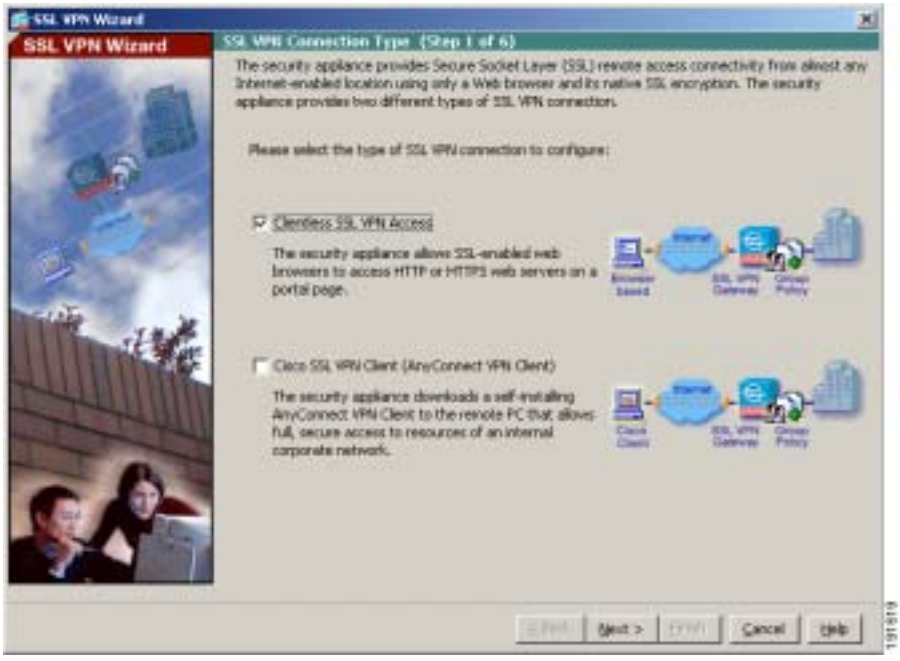
ASDM のメイン ウィンドウが表示されます。


Cisco ASDM 6.0 for ASA
Home
Device Dashboard
Firewall Dashboard
Device Information
Interface Status
VPN Tunnels
Traffic Status
System Resources Status
Latest ASDM Syslog Messages
Device configuration loaded successfully.

ブラウザベースの SSL VPN 接続用の適応型セキュリティ アプライアンスの設定

ブラウザベースの SSL 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、**SSL VPN Wizard** を選択します。SSL VPN Wizard の Step 1 画面が表示されます。



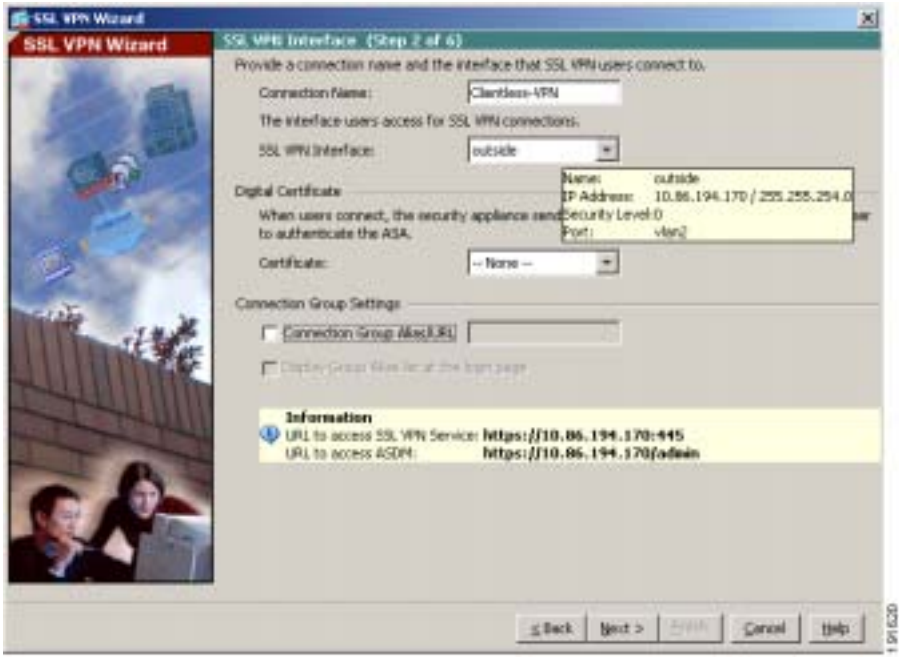
ステップ 2　SSL VPN Wizard の Step 1 で、次の手順を実行します。

a. **Browser-based SSL VPN (Web VPN)** チェックボックスをオンにします。
b. **Next** をクリックして続行します。

SSL VPN インターフェイスの指定

SSL 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 ユーザの接続先の接続名を指定します。



ステップ 2　SSL VPN Interface ドロップダウン リストで、リモート ユーザの接続先のインターフェイスを選択します。ユーザがこのインターフェイスへの接続を確立すると、SSL VPN ポータル ページが表示されます。

ステップ 3　Certificate ドロップダウン リストで、適応型セキュリティ アプライアンスが認証のためにリモート ユーザに送信する証明書を選択します。

（注） ASA 5500 シリーズは、デフォルトで自己署名証明書を生成します。より高度なセキュリティのために、またブラウザの警告メッセージを表示しないようにするために、システムを実稼働環境に配置する前に、公式に信頼できる SSL VPN 証明書を購入する必要があります。

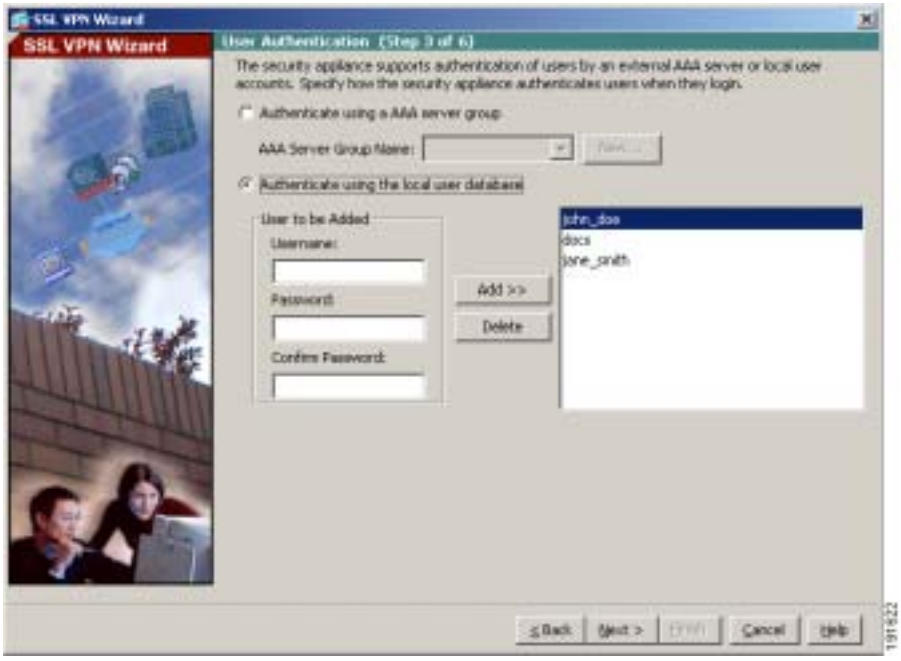
ユーザ認証方式の指定

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。

SSL VPN Wizard の Step 3 で、次の手順を実行します。

ステップ 1　認証に AAA サーバまたはサーバ グループを使用している場合は、次の手順を実行します。

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



b. Authenticate using a AAA server group ドロップダウン リストから事前設定済みのサーバ グループを選択するか、または **New** をクリックして、新しい AAA サーバ グループを追加します。

新しい AAA サーバ グループを作成するには、**New** をクリックします。New Authentication Server Group ダイアログボックスが表示されます。

このダイアログボックスで、次のものを指定します。

- サーバ グループ名
- 使用する認証プロトコル（TACACS、SDI、NT、Kerberos、LDAP）
- AAA サーバの IP アドレス
- 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
- AAA サーバとの通信に使用する秘密鍵

OK をクリックします。

ステップ 2　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。

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 3　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。

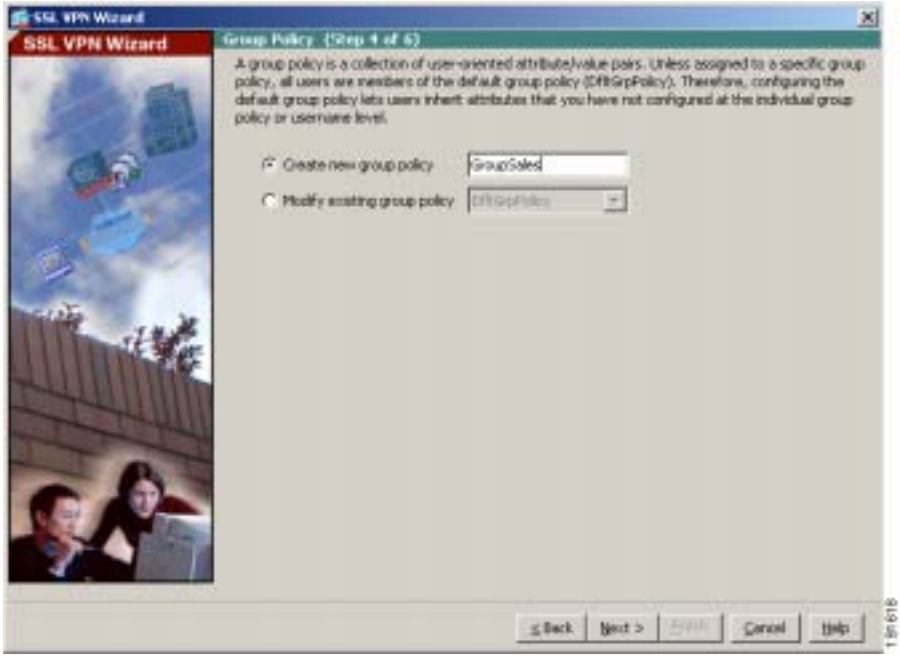
グループ ポリシーの指定

SSL VPN Wizard の Step 4 で、次の手順を実行してグループ ポリシーを指定します。

ステップ 1　**Create new group policy** オプション ボタンをクリックして、グループ名を指定します。

あるいは、

Modify existing group policy オプション ボタンをクリックして、ドロップダウン リストからグループを選択します。



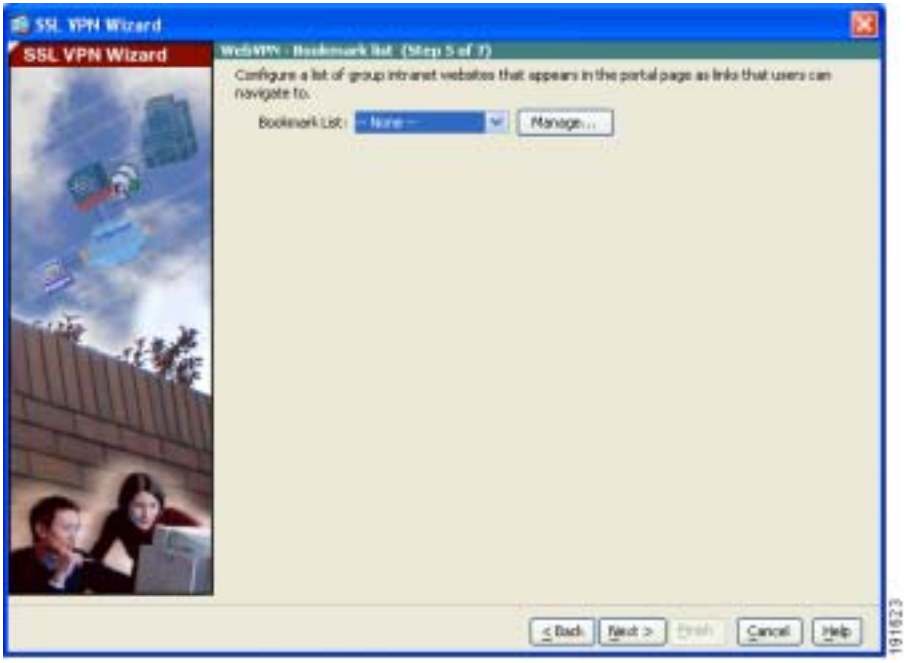
ステップ 2　**Next** をクリックします。

リモート ユーザ用のブックマーク リストの作成

ポータル ページとは、ブラウザベースのクライアントが適応型セキュリティ アプライアンスへの VPN 接続を確立したときに表示される、特別な Web ページです。ポータル ページを作成するには、ユーザが簡単にアクセスできる URL のリストを指定します。

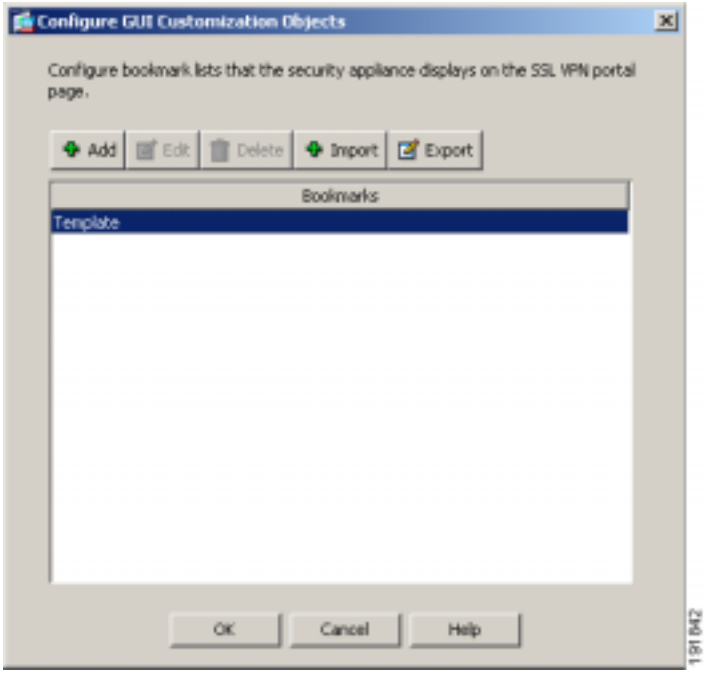
SSL VPN Wizard の Step 5 で、次の手順を実行して、VPN ポータル ページ上に表示する URL を指定します。

ステップ 1　既存のブックマーク　リストを指定するには、ドロップダウンリストからブックマーク リスト名を選択します。



新しいリストの追加または既存のリストの編集を行うには、**Manage** をクリックします。

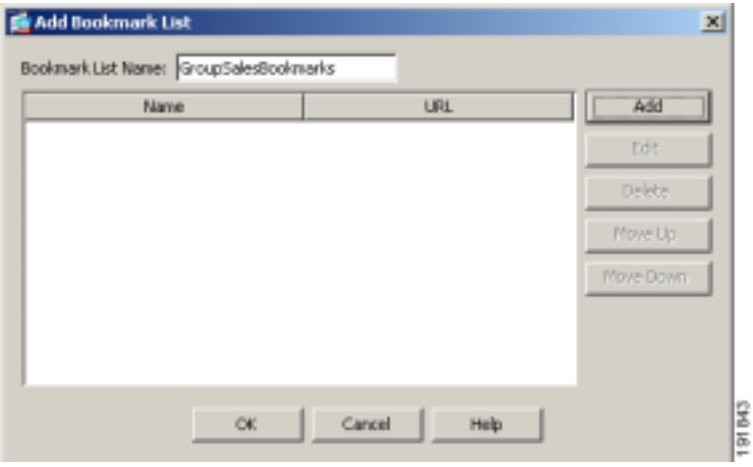
Configure GUI Customization Objects ダイアログボックスが表示されます。



ステップ 2　新しいブックマーク リストを作成するには、**Add** をクリックします。

既存のブックマーク リストを編集するには、**Edit** をクリックします。

Add Bookmark List ダイアログボックスが表示されます。



ステップ 3　Bookmark List Name ボックスに、作成するブックマーク リストの名前を入力します。この名前は、VPN ポータル ページのタイトルとして使用されます。

ステップ 4　**Add** をクリックして、新しい URL をブックマーク リストに追加します。

Add Bookmark Entry ダイアログボックスが表示されます。

ステップ 5　Bookmark Title フィールドに、ブックマーク リストのタイトルを指定します。

ステップ 6　URL Value ドロップダウン リストで、指定する URL のタイプを選択します。たとえば、http、https、ftp などを選択します。

次に、ページの完全な URL を指定します。

ステップ 7　**OK** をクリックして、Add Bookmark List ダイアログボックスに戻ります。

ステップ 8　ブックマーク リストの追加が終了したら、OK をクリックして Configure GUI Customization Objects ダイアログボックスに戻ります。

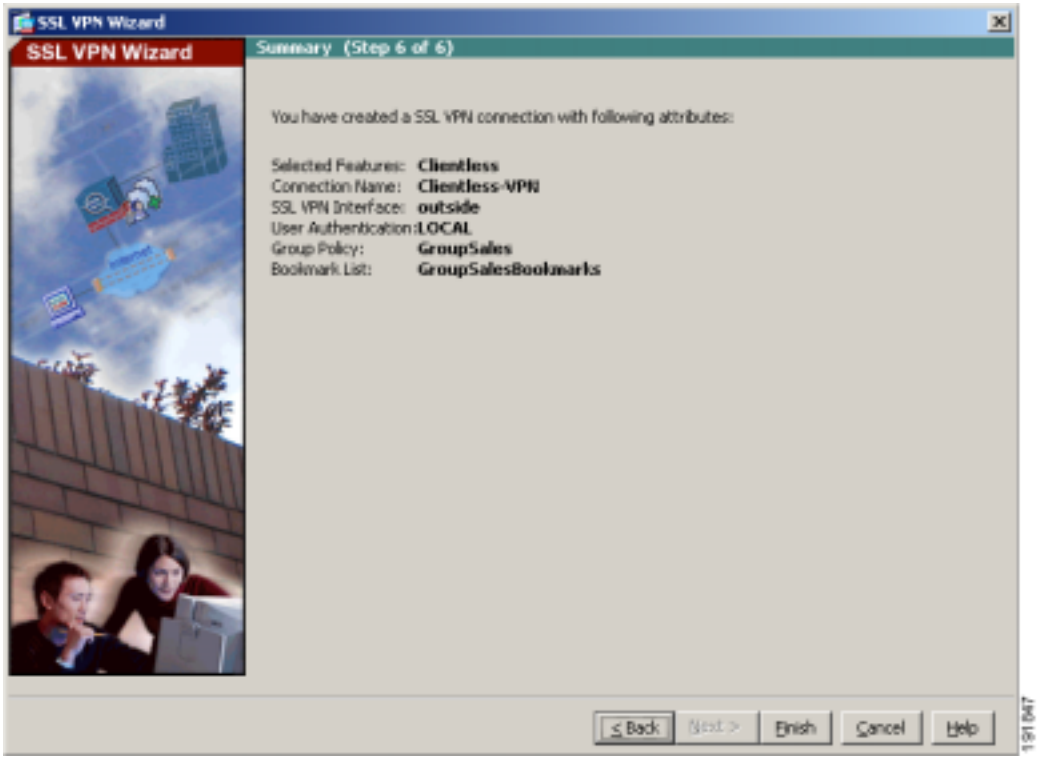
ステップ 9　ブックマーク リストの追加および編集が終了したら、**OK** をクリックして SSL VPN Wizard の Step 5 に戻ります。

ステップ 10　Bookmark List ドロップダウン リストで、この VPN グループのブックマーク リストの名前を選択します。

ステップ 11　**Next** をクリックして続行します。

設定の確認

SSL VPN Wizard の Step 7 で、設定を見直して正しいことを確認します。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

クライアントレス SSL 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 8 章「シナリオ：DMZ の設定」
リモートアクセス VPN の設定	第 9 章「シナリオ：IPSec リモートアクセス VPN の設定」
AnyConnect VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN の設定」

CHAPTER 12

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 12-1 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 12-1　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

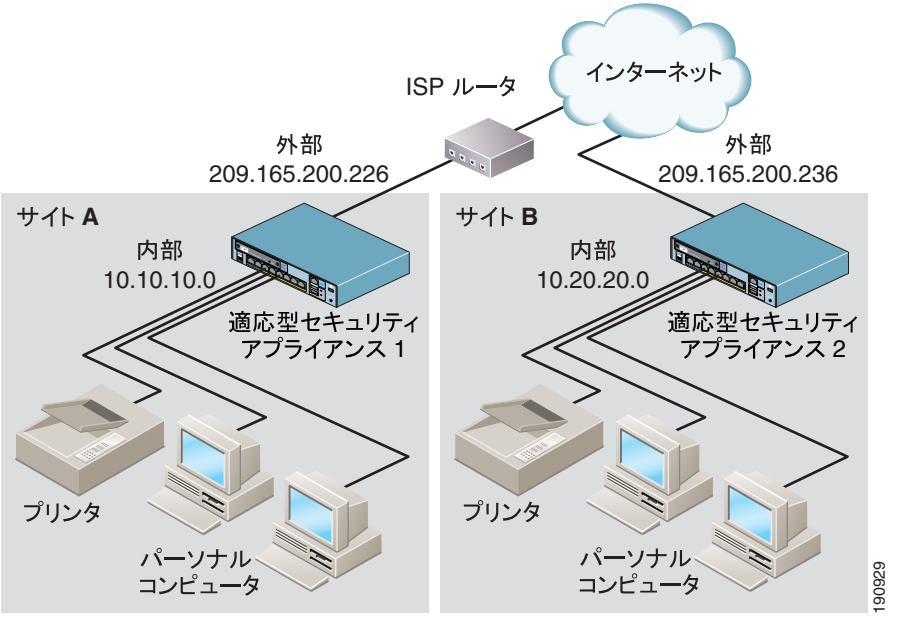


図 12-1 で示すような VPN サイトツーサイト配置の作成では、接続のそれぞれの端で 1 つずつ、合計 2 つの適応型セキュリティ アプライアンスを設定する必要があります。

サイトツーサイトのシナリオの実装

次の項で、図 12-1 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

この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアをまだインストールしていない場合は、P.7-7 の「ASDM Launcher のインストール」を参照してください。

Web ブラウザまたは Java を使用して直接 ASDM にアクセスする場合は、P.7-10 の「Web ブラウザを使用した ASDM の起動」を参照してください。

ASDM Launcher ソフトウェアを使用して ASDM を起動するには、次の手順を実行します。

ステップ 1　デスクトップから、Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。

ステップ 2　適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 3　Username および Password フィールドはブランクのままにします。

（注）　デフォルトで、Cisco ASDM Launcher には Username および Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書を受け入れるよう要求するセキュリティ警告が表示されたら、**Yes**　をクリックします。

ASA は更新するソフトウェアがあるかどうかを確認し、ある場合は自動的にダウンロードします。

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） このシナリオでは、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。

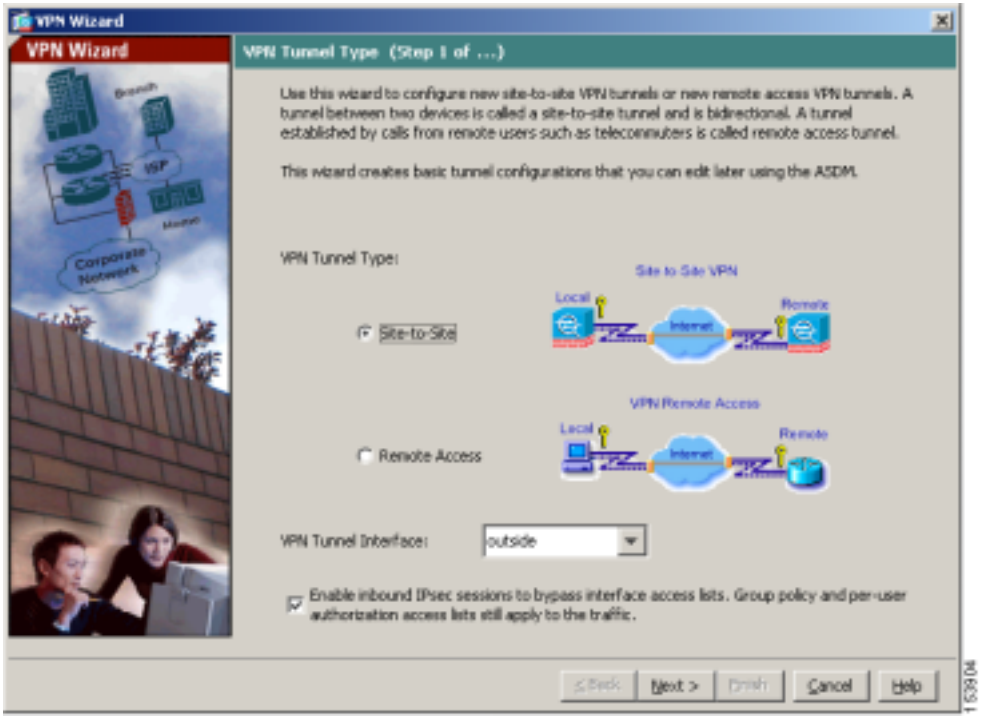
ステップ 1　ASDM のメイン ウィンドウの Wizards ドロップダウン メニューで、IPsec VPN Wizard オプションを選択します。最初の VPN Wizard 画面が表示されます。

VPN Wizard の Step 1 で、次の手順を実行します。

a. VPN Tunnel Type 領域で、**Site-to-Site** 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. VPN Tunnel Interface 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、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 アドレスで、このシナリオでは 209.165.200.236）、および Tunnel Group Name（「Cisco」など）を入力します。

ステップ 2　次の認証方式のいずれかを選択して、使用する認証の種類を指定します。

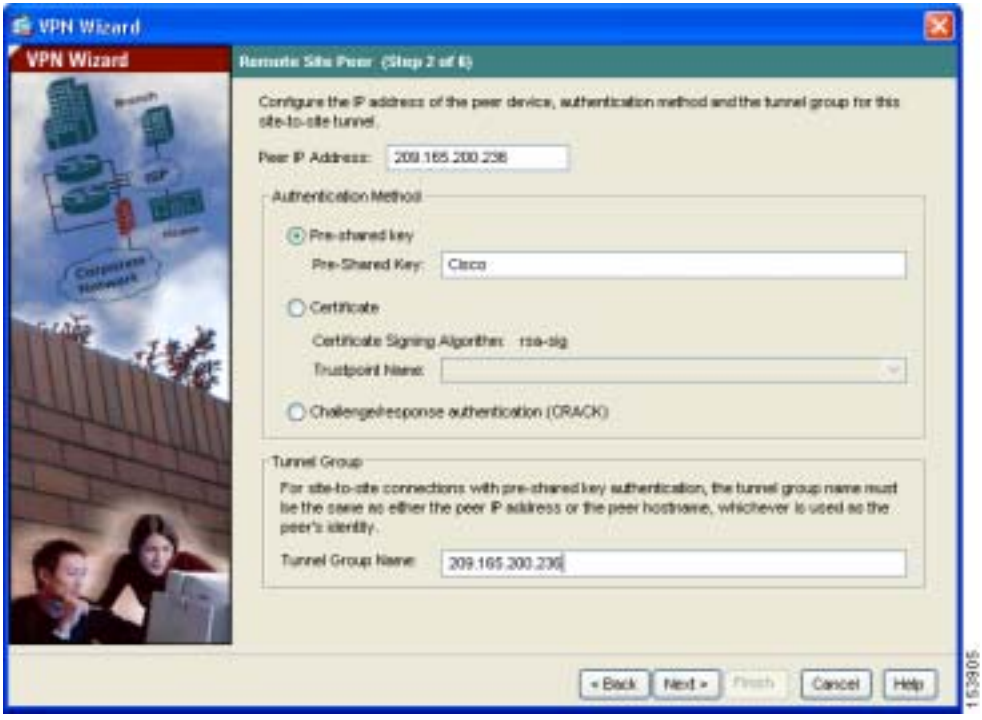
- 認証にスタティックな事前共有キーを使用するには、**Pre-shared key** オプション ボタンをクリックし、事前共有キー（「Cisco」など）を入力します。このキーは、適応型セキュリティ アプライアンス間の IPsec ネゴシエーションに使用されます。

  （注）　事前共有キー認証を使用する場合、Tunnel Group Name はピアの IP アドレスである必要があります。

- 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、Certificate Signing Algorithm ドロップダウン リストで証明書署名アルゴリズムを選択し、Trustpoint Name 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** 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。



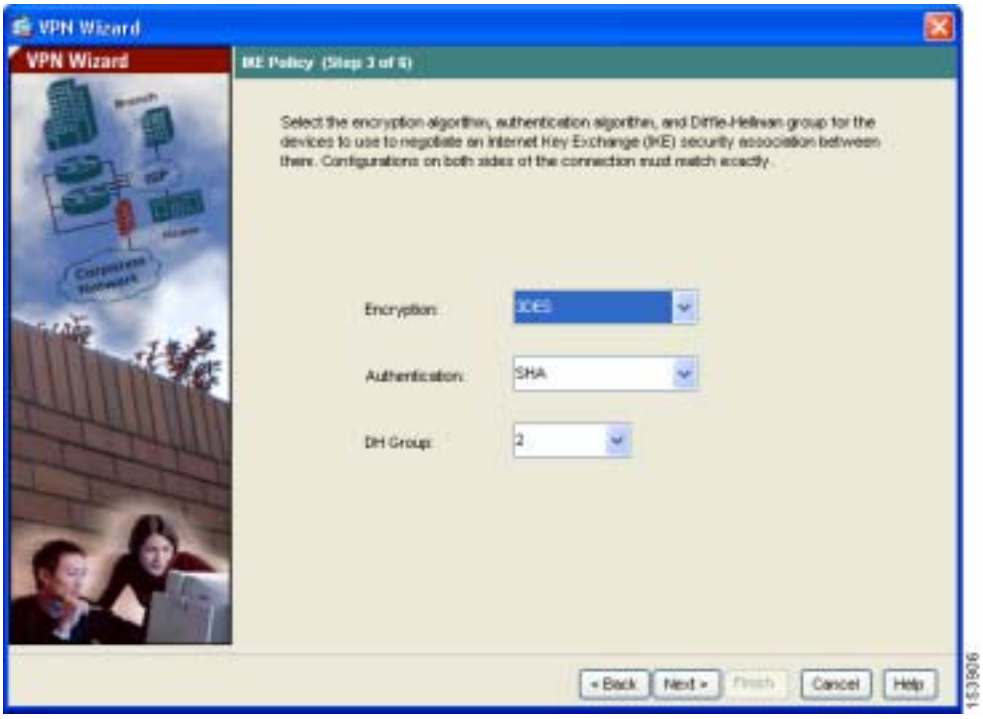
ステップ 3　**Next** をクリックして続行します。

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を保証する認証も提供します。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。



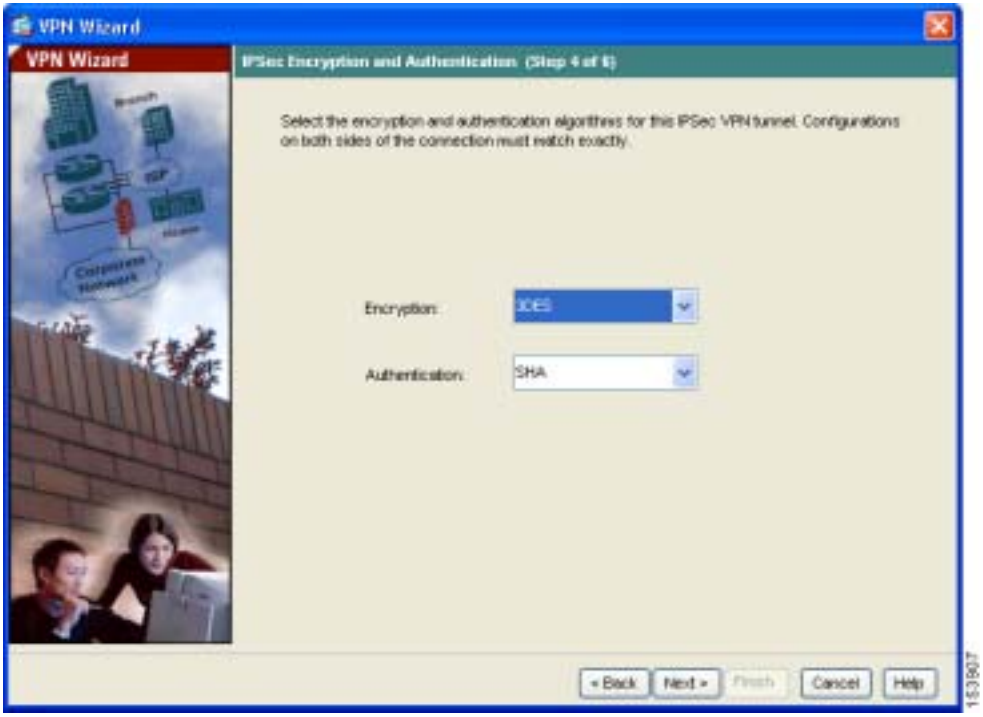
(注)　セキュリティ アプライアンス 2 を設定するときは、セキュリティ アプライアンス 1で選択した各オプションの値を正確に入力する必要があります。暗号化の不一致は、VPN トンネル障害のよくある原因で、設定プロセスを遅らせる原因になります。

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　Encryption ドロップダウン リストで暗号化アルゴリズム（DES、3DES、AES）を選択し、Authentication ドロップダウン リストで認証アルゴリズム（MD5、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トンネルの反対側にあるホストおよびネットワーク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。**Add** または **Delete** をクリックして、トンネルにアクセスできるホストおよびネットワークを指定します。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。

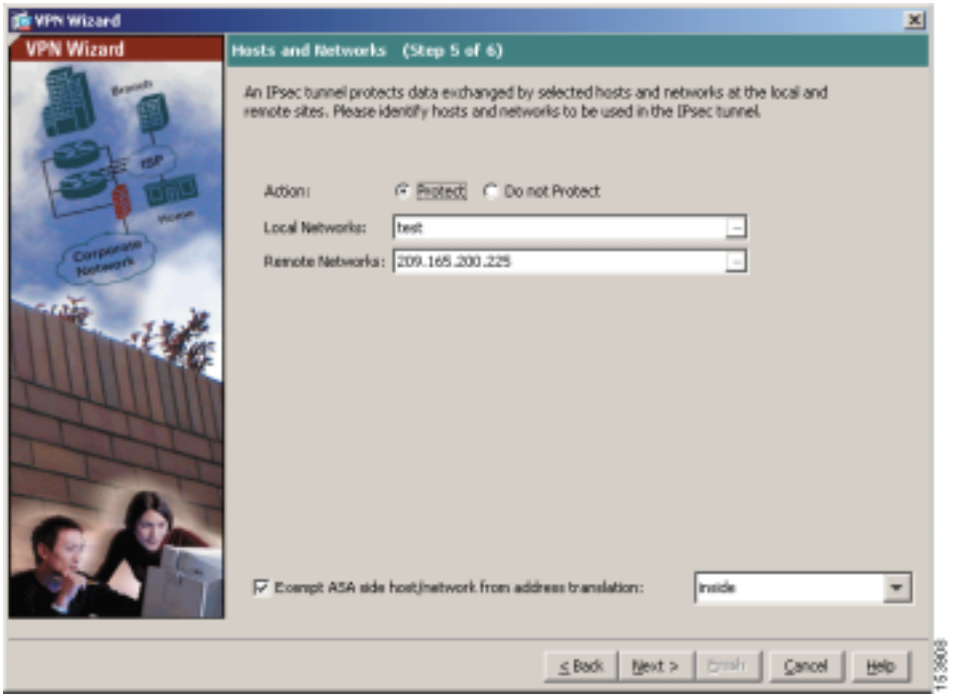
また、この IPSec トンネルを使用してローカル ホストとネットワークにアクセスできるリモート サイトのホストおよびネットワークを指定します。ホストおよびネットワークを動的に追加または削除するには、それぞれ、**Add** または **Delete** をクリックします。このシナリオでは、セキュリティ アプライアンス 1 のリモート ネットワークは Network B（10.20.20.0）なので、このネットワークからの暗号化されたトラフィックは、トンネルを使用できます。

VPN Wizard の Step 5 で、次の手順を実行します。

ステップ 1　Action 領域で、Protect オプション ボタンまたは Do not Protect オプション ボタンをクリックします。

ステップ 2　保護する、または保護しないローカル ネットワークの IP アドレスを入力するか、または省略符号（...）のボタンをクリックして、ホストおよびネットワークのリストから選択します。

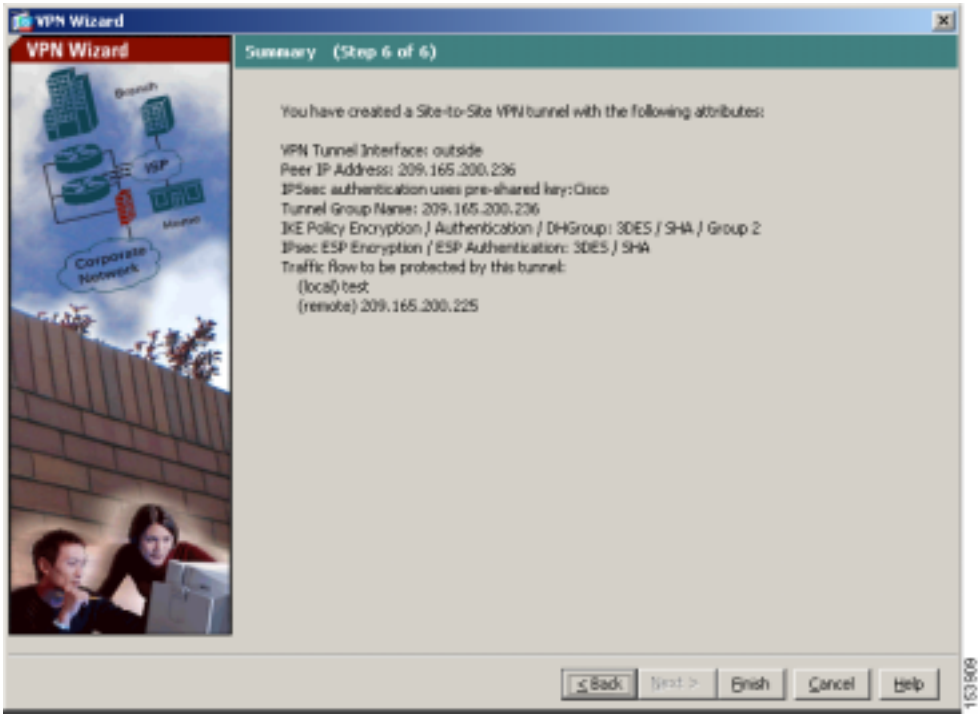
ステップ 3　保護する、または保護しないリモート ネットワークの IP アドレスを入力するか、または省略符号（...）のボタンをクリックして、ホストおよびネットワークのリストから選択します。



ステップ 4　**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

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.12-6 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.12-13 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を設定する場合、セキュリティ アプライアンス 1 に対して選択した各オプションと同じ値を使用してください。ただし、ローカル ホストおよびネットワークの場合は除きます。値が一致しないと、VPN の設定失敗の一般的原因になります。

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 8 章「シナリオ：DMZ の設定」
リモートアクセス VPN の設定	第 9 章「シナリオ：IPSec リモートアクセス VPN の設定」
クライアントレス（ブラウザベース）SSL VPN の設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
Cisco AnyConnect ソフトウェア クライアント用の SSL VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」

CHAPTER 13

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 7.0(1) 以降の ASA ソフトウェアでサポートされます。

AIP SSM は、ASA 5500 シリーズ適応型セキュリティ アプライアンスにインストールできます。AIP SSM は、事前対応型でフル機能の侵入防御サービスを提供する高度な IPS ソフトウェアを実行し、ワームやネットワーク ウイルスなどの悪意のあるトラフィックがネットワークに影響を及ぼす前に、これらを阻止します。この章は、次の項で構成されています。

AIP SSM について

この項では、次のトピックについて取り上げます。

AIP SSM と適応型セキュリティ アプライアンスの連携のしくみ

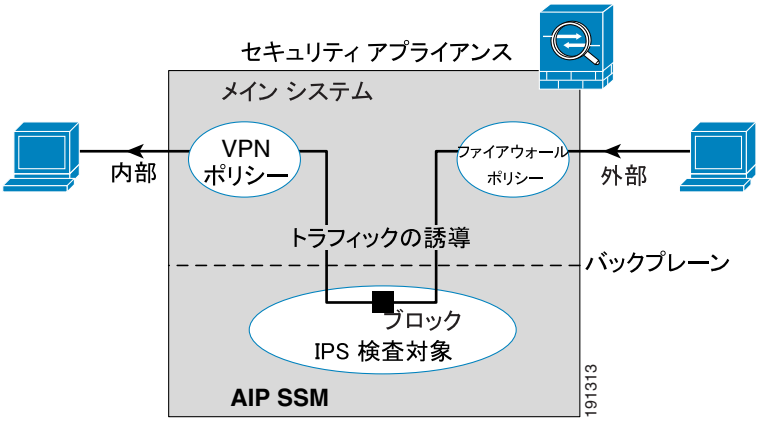
AIP SSM は、適応型セキュリティ アプライアンスとは異なるアプリケーションを実行します。しかし、適応型セキュリティ アプライアンスのトラフィック フローに統合されています。AIP SSM 自体には、管理インターフェイス以外に外部インターフェイスは含まれていません。適応型セキュリティ アプライアンス上で IPS 検査対象のトラフィックが確認されると、トラフィックは、次のように適応型セキュリティ アプライアンスと AIP SSM を流れます。

1. トラフィックが適応型セキュリティ アプライアンスに入ります。
2. ファイアウォール ポリシーが適用されます。
3. トラフィックはバックプレーン経由で AIP SSM に送信されます。

   トラフィックのコピーだけを AIP SSM に送信する場合の詳細については、P.13-3 の「動作モード」を参照してください。
4. AIP SSM はセキュリティ ポリシーをトラフィックに適用し、適切な処理を行います。
5. 有効なトラフィックがバックプレーン経由で適応型セキュリティ　アプライアンスに戻されます。AIP SSM はセキュリティ ポリシーに従ってトラフィックをブロックし、そのようなトラフィックは戻されません。
6. VPN ポリシーが適用されます（設定されている場合）。
7. トラフィックは適応型セキュリティ アプライアンスから出ます。

図 13-1 は、AIP SSM がインライン モードで実行されている場合のトラフィック フローを示しています。この例では、AIP SSM が攻撃と見なしたトラフィックは、自動的にブロックされています。それ以外のトラフィックは、適応型セキュリティ アプライアンスを通って転送されます。

図 13-1　AIP SSM 適応型セキュリティ アプライアンスにおけるトラフィック フロー：インライン モード



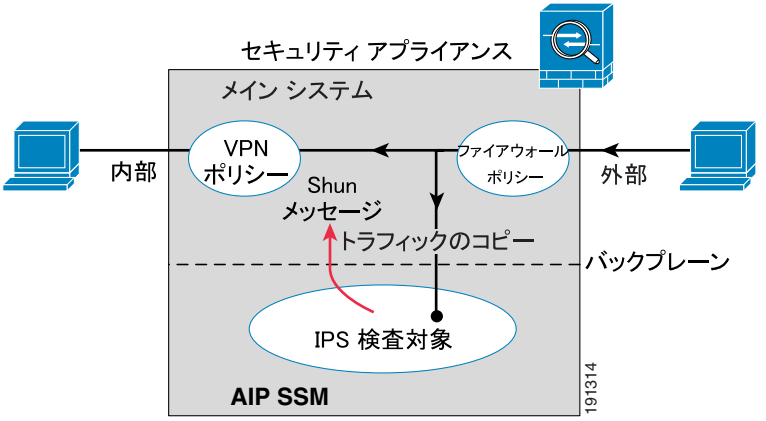
動作モード

次のいずれかのモードを使用して、トラフィックを AIP SSM に送信できます。

- インライン モード：このモードでは、AIP SSM は直接トラフィック フローに配置されます（図 13-1 を参照してください）。IPS 検査対象と認識されたトラフィックは、まず AIP SSM に渡されて検査を受けないと、適応型セキュリティ アプライアンスを通過することはできません。検査対象と認識されたすべてのパケットが分析されてから通過を許可されるため、このモードは最もセキュアです。また、AIP SSM はパケット別にブロッキング ポリシーを実行できます。ただし、このモードはスループットに影響を及ぼす可能性があります。

- 無差別モード：このモードでは、トラフィックの複製ストリームが AIP SSM に送信されます。このモードは、安全性は劣りますが、トラフィック スループットへの影響も小さくなります。インライン モードとは異なり、無差別モードでは、AIP SSM がトラフィックをブロックできるのは、適応型セキュリティ アプライアンスに対してトラフィックの shun を指示するか、適応型セキュリティ アプライアンス上の接続をリセットした場合だけです。また、AIP SSM がトラフィックを分析している間、AIP SSM がトラフィックを shun する前に一部の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することが可能です。図 13-2 は、無差別モードの AIP SSM を示しています。この例では、AIP SSM が脅威と見なしたトラフィックについての shun メッセージを適応型セキュリティ アプライアンスに送信しています。

図 13-2　AIP SSM 適応型セキュリティ アプライアンスにおけるトラフィック フロー：無差別モード



仮想センサーの使用

IPS ソフトウェア バージョン 6.0 以降を実行している AIP SSM では、複数の仮想センサーを実行できます。つまり、複数のセキュリティ ポリシーを AIP SSM に設定できます。各コンテキストまたはシングル モードの適応型セキュリティ アプライアンスを 1 つまたは複数の仮想センサーに割り当てたり、複数のセキュリティ コンテキストを同じ仮想センサーに割り当てたりできます。仮想センサーの詳細（サポートされている最大センサー数など）については、IPS のマニュアルを参照してください。

図 13-3 では、1 つのセキュリティ コンテキストが 1 つの仮想センサー（インライン モード）と対になり、2 つのセキュリティ コンテキストが同じ仮想センサーを共有しています。

図 13-3　セキュリティ コンテキストと仮想センサー

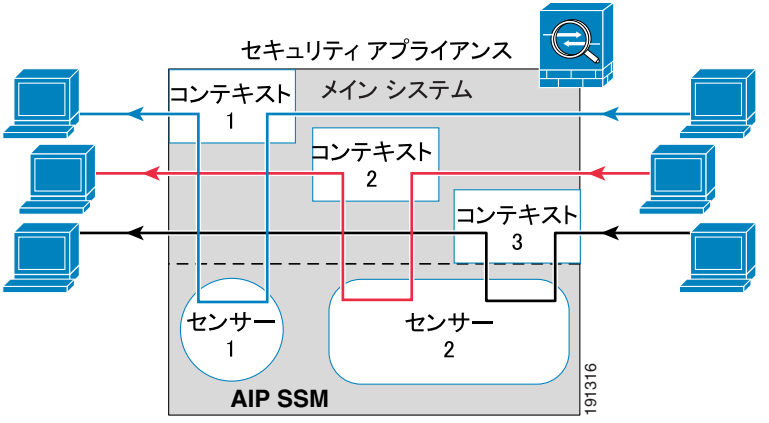
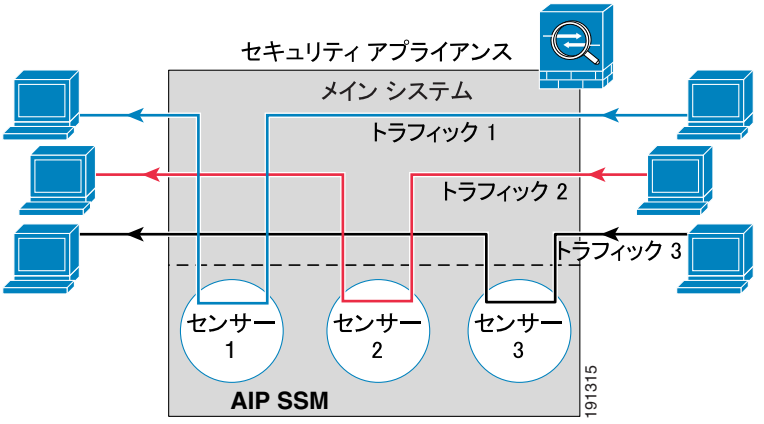


図 13-4 では、シングル モードの適応型セキュリティ アプライアンスが複数の仮想センサー（インライン モード）と対になっています。定義されている各トラフィック フローは、異なるセンサーを進みます。

図 13-4　シングル モードのセキュリティ アプライアンスと複数の仮想センサー



AIP SSM の設定

この項では、次のトピックについて取り上げます。

AIP SSM の手順の概要

AIP SSM の設定は、次に示すように、まず AIP SSM を設定し、次に 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するプロセスからなります。

1. 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。P.13-8 の「AIP SSM へのセッション接続」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。AIP SSM をマルチ センサー モードで実行する場合は、仮想センサーごとに検査と保護ポリシーを設定します。P.13-10 の「AIP SSM でのセキュリティ ポリシーの設定」を参照してください。
3. マルチ コンテキスト モードの ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、各コンテキストに対してどの IPS 仮想センサーが使用可能かを指定します（仮想センサーを設定している場合）。P.13-11 の「セキュリティ コンテキストへの仮想センサーの割り当て」を参照してください。
4. ASA 5500 シリーズ 適応型セキュリティ アプライアンスでは、AIP SSM に誘導するトラフィックを特定します。P.13-14 の「AIP SSM へのトラフィックの誘導」を参照してください。

AIP SSM へのセッション接続

AIP SSM の設定を開始するには、適応型セキュリティ アプライアンスから AIP SSM にセッションを接続します（あるいは、SSH または Telnet を使用して、直接 AIP SSM 管理インターフェイスに接続します）。

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　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するには、次のコマンドを入力します。

```
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「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。

AIP SSM でのセキュリティ ポリシーの設定

AIP SSM で、トラフィックの検査方法と侵入検出時の対処を決定する、検査と保護ポリシーを設定するには、次の手順を実行します。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、P.13-8 の「AIP SSM へのセッション接続」を参照してください。

ステップ 1　AIP SSM の初期設定のセットアップ ユーティリティを実行するには、次のコマンドを入力します。

```
sensor# setup
```

ステップ 2　IPS セキュリティ ポリシーを設定します。IPS バージョン 6.0 以降で仮想センサーを設定する場合は、センサーのうちの 1 つをデフォルトとして指定します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの設定時に仮想センサー名を指定しなかった場合、デフォルト センサーが使用されます。

AIP SSM で実行される IPS ソフトウェアはこのマニュアルの対象ではないため、詳細な設定情報については、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*
- *Command Reference for Cisco Intrusion Prevention System*

ステップ 3　AIP SSM の設定が完了したら、次のコマンドを入力して IPS ソフトウェアを終了します。

```
sensor# exit
```

適応型セキュリティ アプライアンスから AIP SSM へセッションを接続した場合は、適応型セキュリティ アプライアンスのプロンプトに戻ります。

セキュリティ コンテキストへの仮想センサーの割り当て

適応型セキュリティ アプライアンスがマルチ コンテキスト モードの場合は、1 つまたは複数の IPS 仮想センサーを各コンテキストに割り当てることができます。この方法を行うと、トラフィックを AIP SSM に送信するようにコンテキストを設定するときに、そのコンテキストに割り当てられているセンサーを指定できます。コンテキストに割り当てられていないセンサーを指定することはできません。コンテキストにセンサーを割り当てなかった場合、AIP SSM に設定されているデフォルト センサーが使用されます。複数のコンテキストに同じセンサーを割り当てることができます。

（注） 仮想センサーを使用するために、マルチ コンテキスト モードにする必要はありません。シングル モードでも、トラフィック フローごとに異なるセンサーを使用できます。

1 つまたは複数のセンサーをセキュリティ コンテキストに割り当てるには、次の手順を実行します。

ステップ 1　コンテキスト コンフィギュレーション モードに入るには、システム実行スペースで次のコマンドを入力します。

```
hostname(config)# context name
hostname(config-ctx)#
```

ステップ 2　コンテキストに仮想センサーを割り当てるには、次のコマンドを入力します。

```
hostname(config-ctx)# allocate-ips sensor_name [mapped_name] [default]
```

このコマンドは、コンテキストに割り当てる仮想センサーごとに入力します。

sensor _name 引数は、AIP SSM に設定されているセンサー名です。AIP SSM に設定されているセンサーを表示するには、**allocate-ips ?** を入力します。使用可能なすべてのセンサーが一覧表示されます。また、**show ips** コマンドを入力することもできます。システム実行スペースで **show ips** コマンドを入力すると、使用可能なすべてのセンサーが一覧表示されます。コンテキストでこのコマンドを入力すると、コンテキストに割り当て済みのセンサーが表示されます。まだ AIP SSM に存在しないセンサー名を指定した場合、エラーになりますが、**allocate-ips** コマンドはそのまま入力されます。指定した名前のセンサーを AIP SSM に作成するまで、コンテキストはそのセンサーはダウンしていると見なします。

mapped_name 引数は、実際のセンサー名の代わりにコンテキストで使用可能なセンサー名のエイリアスとして使用します。mapped name を指定しなかった場合、センサー名がコンテキストで使用されます。セキュリティのためには、コンテキストでどのセンサーが使用されているかをコンテキスト管理者に知らせない方がいいでしょう。あるいは、コンテキスト設定をジェネリクス化します。たとえば、すべてのコンテキストで「sensor1」および「sensor2」という名前のセンサーを使用する場合、コンテキスト A では「highsec」および「lowsec」センサーを sensor1 および sensor2 にそれぞれマッピングし、コンテキスト B では「medsec」および「lowsec」センサーを sensor1 および sensor2 にそれぞれマッピングします。

default キーワードは、コンテキストごとに 1 つのセンサーを設定するものです。コンテキスト設定でセンサー名が指定されていない場合、コンテキストではこのデフォルト センサーが使用されます。コンテキストごとに設定できるデフォルト センサーは、1 つだけです。デフォルト センサーを変更する場合は、**no allocate-ips** *sensor_name* コマンドを入力し、現在のデフォルト センサーを削除してから新しいデフォルト センサーを割り当てます。デフォルト センサーを指定せず、コンテキスト設定にセンサー名が含まれていない場合、トラフィックでは AIP SSM のデフォルト センサーが使用されます。

ステップ 3　ステップ 1 および ステップ 2 をコンテキストごとに繰り返します。

ステップ 4　コンテキスト IPS ポリシーを設定するには、次のコマンドを使用して、コンテキスト実行スペースに切り替えます。

```
hostname(config-ctx)# changeto context context_name
```

ここで、*context_name* 引数は、設定するコンテキストの名前です。IPS セキュリティ ポリシーを設定するように各コンテキストを変更します（P.13-14 の「AIP SSM へのトラフィックの誘導」を参照してください）。

次の例では、sensor1 と sensor2 がコンテキスト A に割り当てられ、sensor1 と sensor3 がコンテキスト B に割り当てられています。どちらのコンテキストでも、これらのセンサー名を「ips1」と「ips2」にマッピングしています。コンテキスト A では、sensor1 がデフォルト センサーに設定されていますが、コンテキスト B では、デフォルト センサーが設定されていないため、AIP SSM でデフォルトに設定されているセンサーが使用されます。

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface
gigabitethernet0/0.110-gigabitethernet0/0.115 int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url
ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface
gigabitethernet0/1.230-gigabitethernet0/1.235 int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1
hostname(config-ctx)# allocate-ips sensor3 ips2
hostname(config-ctx)# config-url
ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver

hostname(config-ctx)# changeto context A
...
```

AIP SSM へのトラフィックの誘導

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。マルチ コンテキスト モードで、各コンテキスト実行スペースで次の手順を実行します。

ステップ 1　AIP SSM で検査を行うトラフィックを特定するには、**class-map** コマンドを使用して 1 つまたは複数のクラス マップを追加します。

たとえば、すべてのトラフィックを一致させるには、次のコマンドを使用します。

```
hostname(config)# class-map IPS
hostname(config-cmap)# match any
```

特定のトラフィックを一致させるには、アクセスリストを一致させます。

```
hostname(config)# access list IPS extended permit ip any 10.1.1.1
255.255.255.255
hostname(config)# class-map IPS
hostname(config-cmap)# match access-list IPS
```

ステップ 2　AIP SSM にトラフィックを誘導するアクションを設定するポリシーマップを追加または編集するには、次のコマンドを入力します。

```
hostname(config)# policy-map name
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

ここで、*class_map_name* は ステップ 1 のクラス マップです。

次の例を参考にしてください。

```
hostname(config)# policy-map IPS
hostname(config-pmap)# class IPS
```

ステップ 3　トラフィックを AIP SSM に誘導するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |
fail-open} [sensor {sensor_name | mapped_name}]
```

inline キーワードおよび ***promiscuous*** キーワードは、AIP SSM の動作モードを制御します。詳細については、P.13-3 の「動作モード」を参照してください。

fail-close キーワードは、AIP SSM が使用不能の場合に、すべてのトラフィックをブロック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。

fail-open キーワードは、AIP SSM が使用不能の場合に、すべてのトラフィックが検査なしで通過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。

AIP SSM で仮想センサーを使用する場合、**sensor** *sensor_name* 引数を使用してセンサー名を指定できます。使用可能なセンサー名を表示するには、**ips ... sensor ?** コマンドを入力します。使用可能なセンサーが一覧表示されます。また、**show ips** コマンドも使用できます。適応型セキュリティ アプライアンスでマルチ コンテキスト モードを使用する場合、指定できるセンサーはコンテキストに割り当てられているセンサーだけです（P.13-11 の「セキュリティ コンテキストへの仮想センサーの割り当て」を参照してください）。コンテキストで設定されている場合は、*mapped_name* を使用します。センサー名を指定しなかった場合、トラフィックではデフォルト センサーが使用されます。マルチ コンテキスト モードでは、デフォルト センサーをコンテキストに指定できます。マルチ モードでデフォルト センサーを指定しなかった場合またはシングル モードの場合は、AIP SSM で設定されているデフォルト センサーがトラフィックで使用されます。まだ AIP SSM に存在しない名前を入力した場合、エラーになり、コマンドは拒否されます。

ステップ 4　（オプション）他のクラスのトラフィックを AIP SSM に誘導し、IPS ポリシーを設定するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# class class_map_name2
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |
fail-open} [sensor sensor_name]
```

ここで、*class_map_name2* 引数は、IPS 検査を行う別のクラス マップの名前です。コマンド オプションの詳細については、ステップ 3 を参照してください。

トラフィックを同じアクション タイプの複数のクラス マップに一致させることはできません。そのため、ネットワーク A を sensorA に誘導し、それ以外のすべてのトラフィックは sensorB に誘導する場合、まずネットワーク A に対して **class** コマンドを入力してから、すべてのトラフィックに対して **class** コマンドを入力します。この方法をとらないと、すべてのトラフィック（ネットワーク A を含む）が最初の **class** コマンドに一致し、sensorB には送信されません。

ステップ 5　1 つまたは複数のインターフェイスでポリシーマップをアクティブにするには、次のコマンドを入力します。

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

ここで、*policy_map_name* は、ステップ 2 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。

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-ips-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
```

次の例では、10.1.1.0 ネットワークおよび 10.2.1.0 ネットワーク宛のすべての IP トラフィックが AIP SSM にインライン 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、すべてのトラフィックの通過が許可されます。my-ips-class トラフィックには sensor1 が使用され、my-ips-class2 トラフィックには sensor2 が使用されます。

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0
255.255.255.0
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0
255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
hostname(config)# class-map my-ips-class2
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface
outside
```

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 8 章「シナリオ：DMZ の設定」
リモートアクセス VPN の設定	第 9 章「シナリオ：IPSec リモートアクセス VPN の設定」
ソフトウェア クライアント用のリモートアクセス SSL 接続の設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」
ブラウザベースのリモートアクセス用の SSL 接続の設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN の設定」

次の手順

CHAPTER 14

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 バージョン 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。

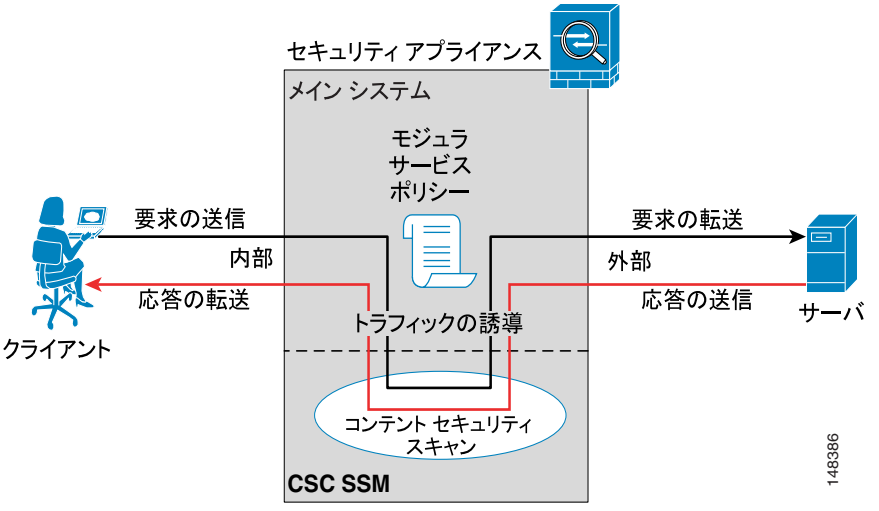
CSC SSM を使用するセキュリティ アプライアンスの配置について

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 14-1 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 14-1 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 14-1　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。

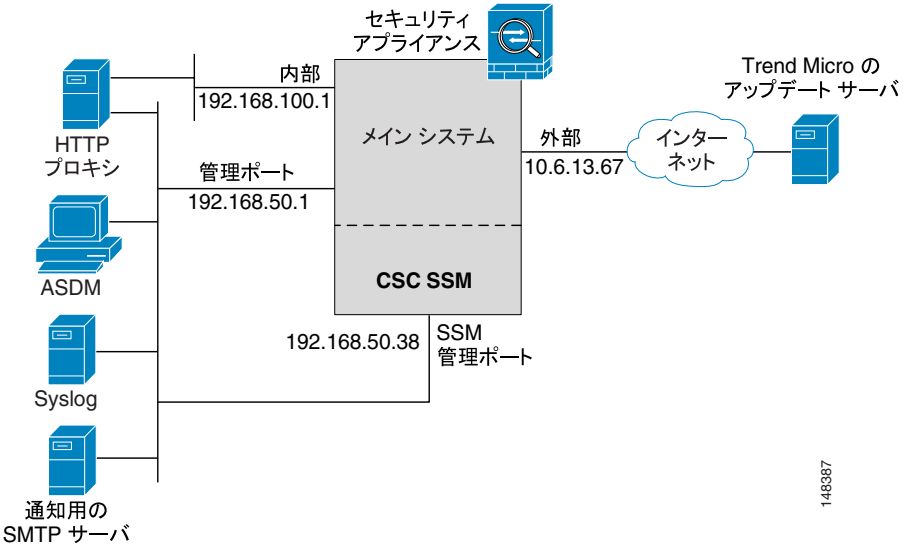
1. クライアントが要求を開始する。
2. 適応型セキュリティ　アプライアンスが要求を受信し、インターネットに転送する。
3. 要求されたコンテントを適応型セキュリティ　アプライアンスが取得し、このコンテント タイプが CSC SSM に誘導し、スキャンする対象としてサービス ポリシーで定義されているかどうかを判別する。定義されている場合は、CSC SSM に誘導する。
4. CSC SSM が適応型セキュリティ アプライアンスからコンテントを受信し、スキャンし、Trend Micro コンテント フィルタの最新アップデートと比較する。
5. コンテントが疑わしい場合、CSC SSM はコンテントをブロックし、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 14-2 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。

図 14-2　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ありませんが、セキュリティの理由により、使用することが推奨されます。
- 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 の管理ポートです。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ります。

- 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ます。
- 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ます。

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 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ます。
- 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 キーを取得します。
2. CSC SSM の設定に必要な情報を収集します。
3. 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 を開きます。
4. 時間設定を確認します。

5. CSC セットアップ ウィザードを実行して、CSC SSM を設定します。
6. 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します。

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.14-11 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、付録 A「3DES/AES ライセンスの取得」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

この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアをまだインストールしていない場合は、P.7-7 の「ASDM Launcher のインストール」を参照してください。

Web ブラウザまたは Java を使用して直接 ASDM にアクセスする場合は、P.7-10 の「Web ブラウザを使用した ASDM の起動」を参照してください。

ASDM Launcher ソフトウェアを使用して ASDM を起動するには、次の手順を実行します。

ステップ 1　デスクトップから、Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。

ステップ 2　適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 3　Username および Password フィールドはブランクのままにします。

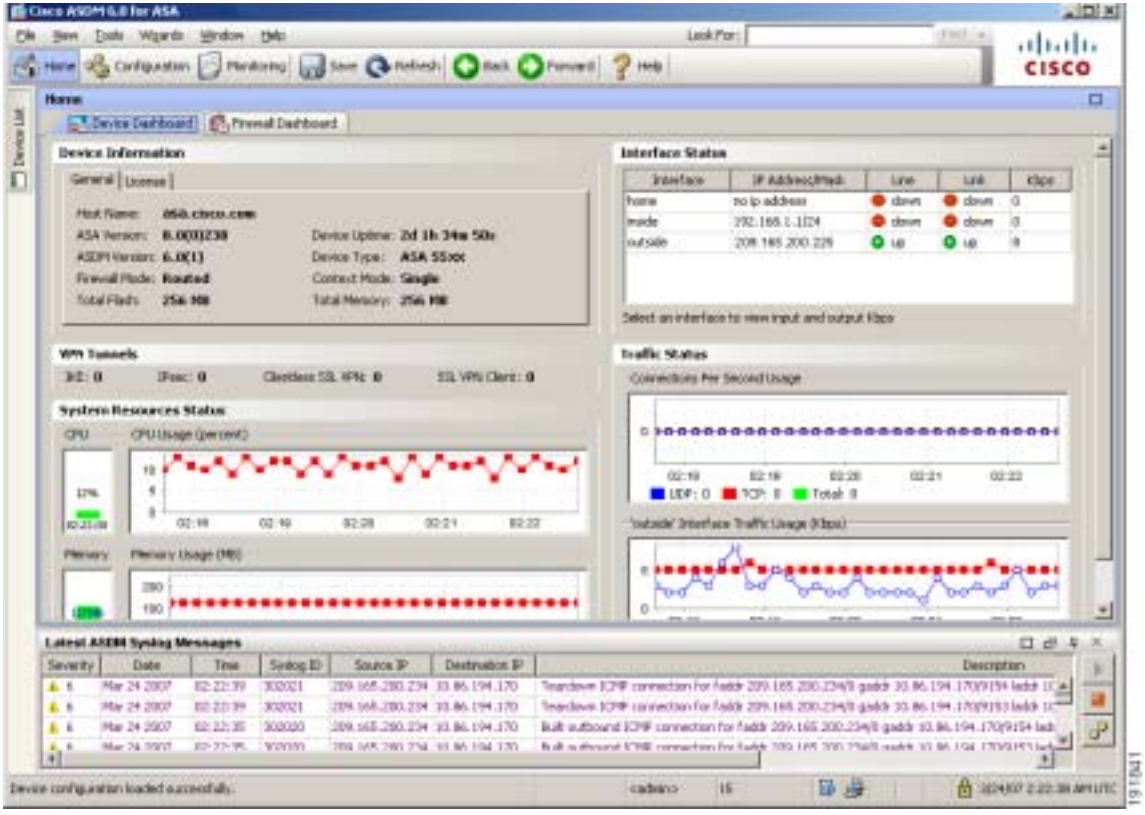
(注)　デフォルトで、Cisco ASDM Launcher には Username および Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書を受け入れるよう要求するセキュリティ警告が表示されたら、**Yes** をクリックします。

ASA は更新するソフトウェアがあるかどうかを確認し、ある場合は自動的にダウンロードします。

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、**Device Setup** > **System Time** > **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、**Device Setup > System Type > 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。

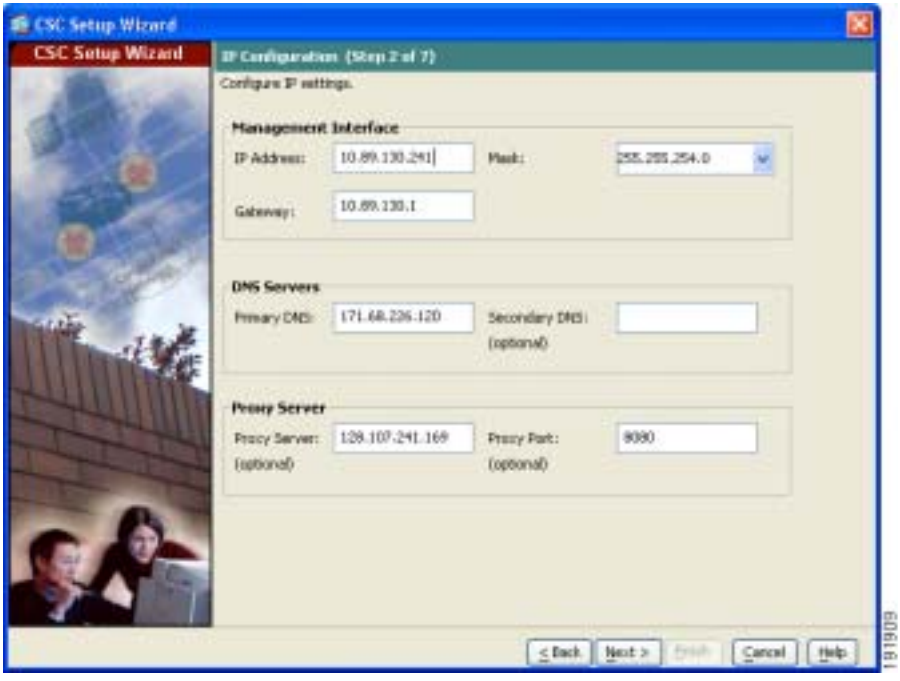
ステップ 3　CSC Wizard の Step 1 で、Base License の **Activation Code** を入力します。オプションで、Plus License のアクティベーション コードを入力します。

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）



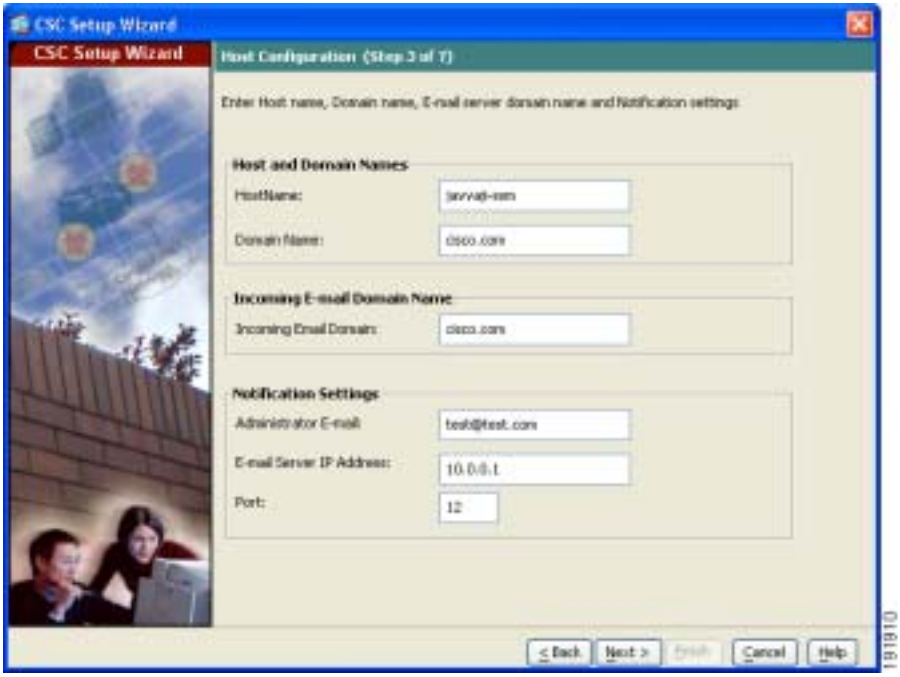
ステップ 6　**Next** をクリックします。

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** および **Domain Name**
- **Domain Name** 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。

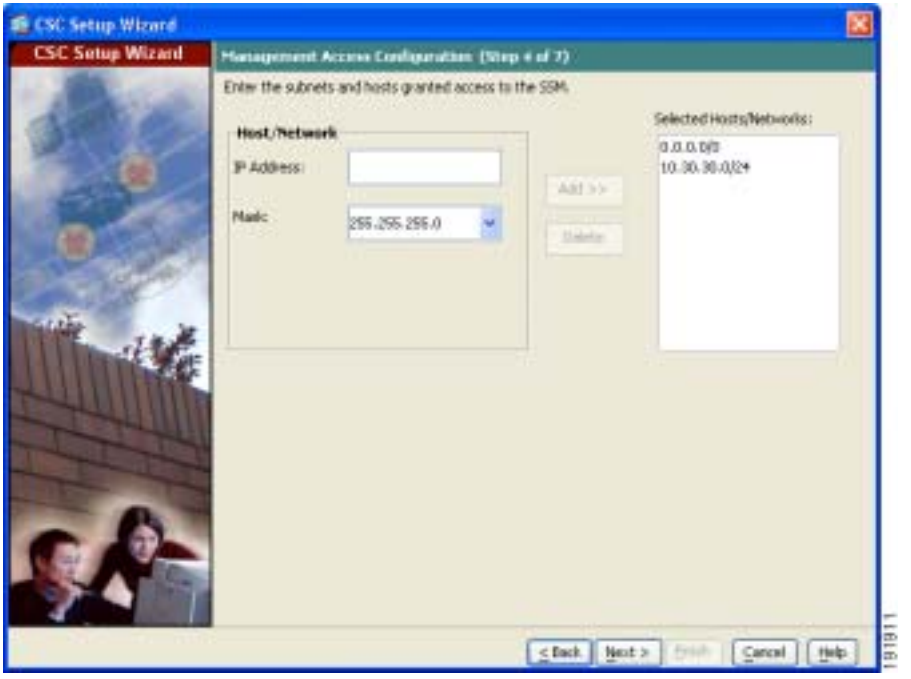
- 通知に使用する管理者の電子メール アドレスと、電子メール サーバの IP アドレスおよびポート



ステップ 8　**Next** をクリックします。

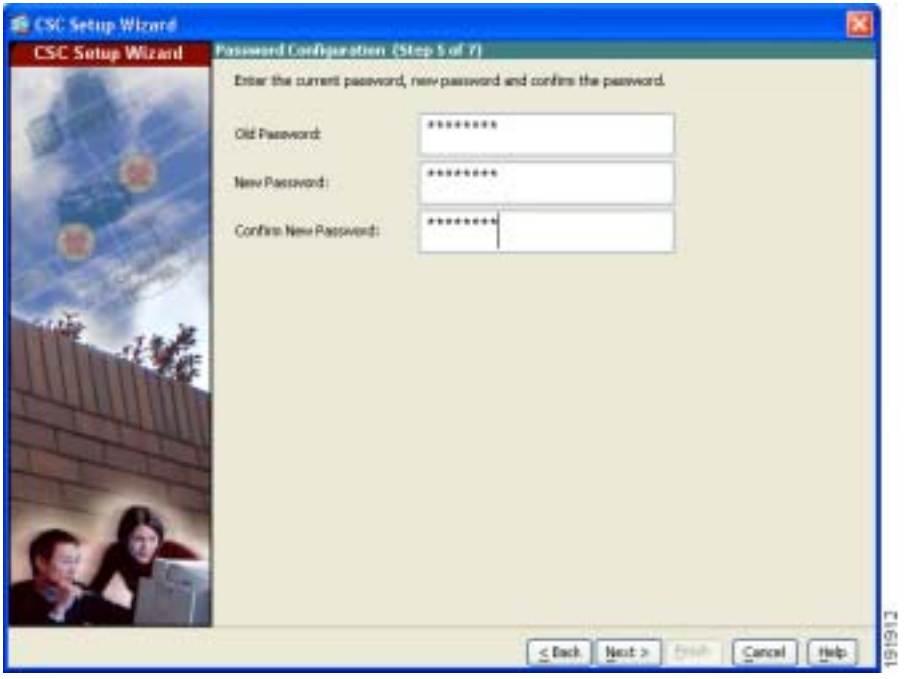
ステップ 9　CSC Setup Wizard の Step 4 で、CSC SSM への管理アクセスが必要な各サブネットおよびホストの、IP アドレスとマスクを入力します。

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、スキャンするトラフィックのタイプを指定します。

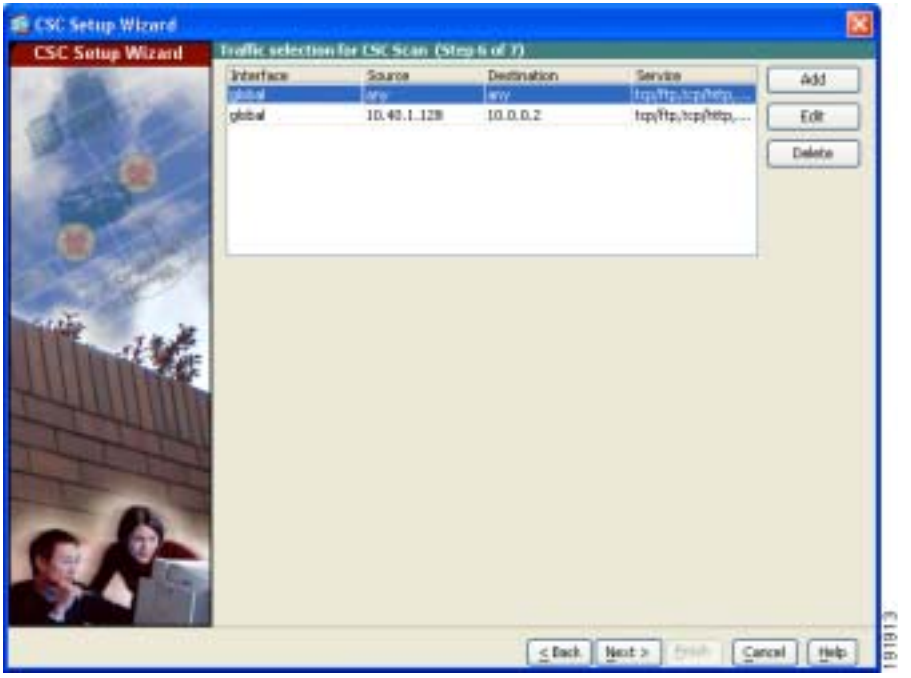
適応型セキュリティ アプライアンスは、ファイアウォール ポリシーを適用した後、出力インターフェイスから出る前に、パケットを CSC SSM に誘導します。たとえば、アクセスリストによってブロックされたパケットは、CSC SSM に転送されません。

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。

a. 新しいトラフィック タイプを追加するには、**Add** をクリックします。



Traffic Selection for CSC Scan ダイアログボックスが表示されます。

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

c. Source および Destination フィールドの設定は Any のままにします。

d. Service 領域で、省略符号（...）オプション ボタンをクリックします。このダイアログボックスで、事前定義済みのサービスを選択するか、または **Add** をクリックして新しいサービスを定義します。

e. **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。

f. **OK** をクリックし、Traffic Selection for CSC Scan ウィンドウに戻ります。

g. **Next** をクリックします。

ステップ 14 CSC Setup Wizard の Step 7 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。

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 8 章「シナリオ：DMZ の設定」
リモートアクセス VPN の設定	第 9 章「シナリオ：IPSec リモートアクセス VPN の設定」
ソフトウェア クライアント用のリモートアクセス SSL 接続の設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」
ブラウザベースのリモートアクセス用の SSL 接続の設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN の設定」

CHAPTER 15

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 Version 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。

(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

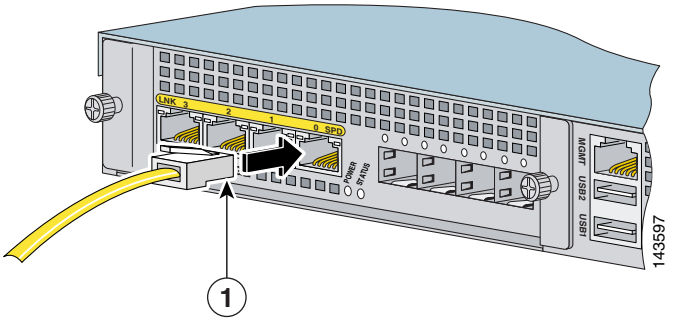
4GE SSM インターフェイスをケーブル接続するには、ネットワーク デバイスに接続するポートごとに、次の手順を実行します。

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 15-1 を参照してください）。

図 15-1　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 15-2 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。

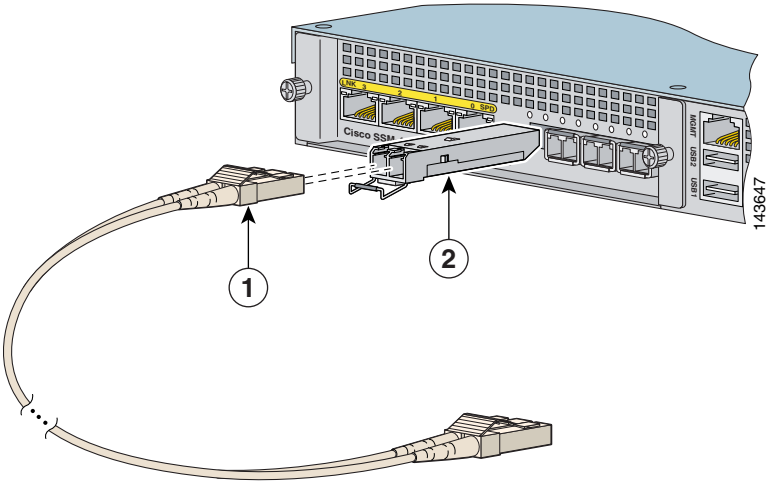
a. SFP モジュールを、カチッという音が聞こえるまで SFP ポートに差し込み、スライドさせます。カチッという音は、SFP モジュールがポートにロックされたことを示します。

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 15-2　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*

次の手順

APPENDIX A

3DES/AES ライセンスの取得

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスには、暗号化を提供する DES ライセンスが同梱されています。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 3DES-AES ライセンスを入手できます。この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。

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。

INDEX

W

か

こ

し

せ

て

ね

は

ほ