Cisco ASA 5580 スタート ガイド

Software Version 8.1

Customer Order Number: DOC-J-7818101=
Text Part Number: 78-18101-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco ASA 5580 スタート ガイド

CONTENTS

CHAPTER 1

始める前に

次の表を使用して、Cisco ASA 5580 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。

作業内容	参照先
シャーシの設置	第 3 章「ASA 5580 の取り付け」
インターフェイス ケーブルの接続	第 3 章「ASA 5580 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 4 章「適応型セキュリティ アプライアンスの設定」 *Cisco ASDM User Guide*
実装のシナリオに応じた適応型セキュリティ アプライアンスの設定	第 5 章「シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定」 第 6 章「シナリオ：SSL VPN クライアントレス接続」 第 7 章「シナリオ：サイトツーサイト VPN の設定」 第 8 章「シナリオ：IPsec リモート アクセス 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*

作業内容	参照先
システムの日常のオペレーション	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages* *Cisco ASDM User Guide*

CHAPTER 2

ASA 5580 のスループットの最大化

Cisco ASA 5580 適応型セキュリティ アプライアンスは、この章で説明するガイドラインに従って設定された場合に最大のスループットを発揮するように設計されています。

この章には、次の項があります。

ネットワーク インターフェイス

ASA 5580 には、2 個の組み込みギガビット イーサネット ネットワーク ポートと 9 個の拡張スロットがあります。ネットワーク ポートには、上から下に向かって 0 ～ 4 の番号が付けられています。拡張スロットの番号は、右から左に向かって増えていきます。

2 個の組み込みギガビット イーサネット ポートは管理に使用され、管理 0/0 および管理 0/1 と呼ばれます。

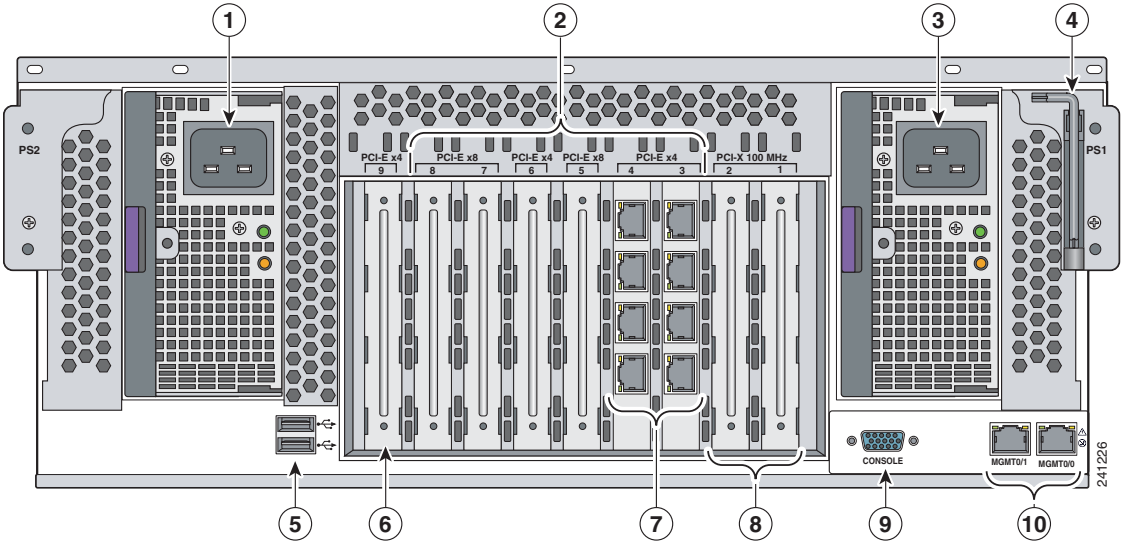
ASA 5580 には 9 個のインターフェイス拡張スロットがあります。スロット 1、2、および 9 は予約されています。スロット 1 は、暗号アクセラレータが実装されるため、ネットワーク インターフェイス カードに使用することはできません。スロット 2 は、将来の使用のために予約されています。

スロット 3 ～ 8 に、サポートされるネットワーク インターフェイス カードを実装できます。

アプライアンスには 2 個の I/O ブリッジがあり、I/O スロットは 2 個のバスのいずれか一方に接続します。管理ポートとスロット 3、スロット 4、スロット 5、スロット 6 のアダプタは I/O ブリッジ 1 上にあり、スロット 7 とスロット 8 は I/O ブリッジ 2 上にあります。

図 2-1 に、ASA 5580 の組み込みポートとスロットを示します。

図 2-1　ASA 5580 の組み込みポートとスロット



1	電源モジュール	**2**	インターフェイス拡張スロット
3	電源モジュール	**4**	T-15 トルクス ドライバ
5	USB ポート	**6**	予備スロット
7	実装されたスロットの例	**8**	予備スロット
9	コンソール ポート	**10**	管理ポート

拡張ボード

スロット 1、スロット 2、およびスロット 9 は予約されています。スロット 3 ～ 9 は PCI-Express スロットです。

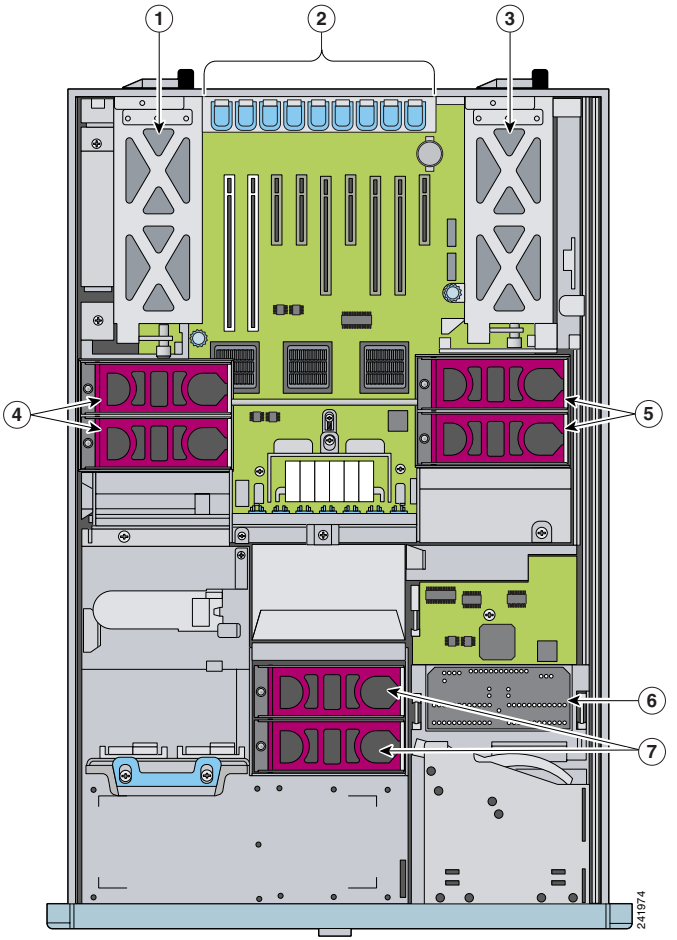
適応型セキュリティ アプライアンスは、次の 2 種類の内部 I/O ブリッジによって、銅線ギガビット イーサネットとファイバ ギガビット イーサネットの接続性を提供します。

スロット 5、スロット 7、およびスロット 8 は大容量バス（PCIe x8）を使用し、スロット 3、スロット 4、およびスロット 6 はスロット用の PCIe x4 バスを使用します。

図 2-2 に、ASA 5580 で使用可能なインターフェイス拡張スロットを示します。

スロット	説明
1	PCI-X 非ホットプラグ予備スロット、64 ビット /100 MHz
2	PCI-X 非ホットプラグ予備スロット、64 ビット /100 MHz
3	PCI Express x4 非ホットプラグ拡張スロット
4	PCI Express x4 非ホットプラグ拡張スロット
5	PCI Express x8 非ホットプラグ拡張スロット
6	PCI Express x4 非ホットプラグ拡張スロット
7	PCI Express x8 非ホットプラグ拡張スロット
8	PCI Express x8 非ホットプラグ拡張スロット
9	PCI Express x4 非ホットプラグ予備スロット

図 2-2　インターフェイス拡張スロット



1, 3	電源モジュール
4, 5, 7	ファン
6	診断パネル

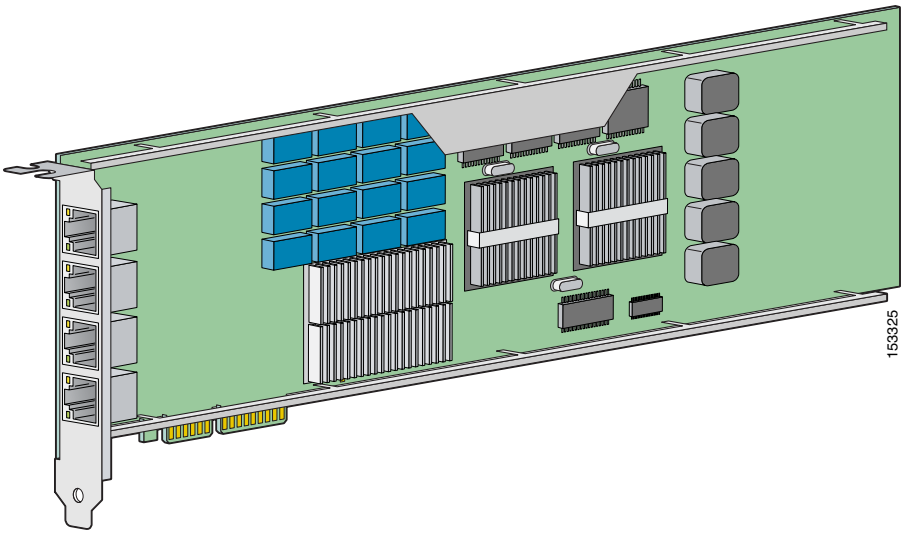
サポートされる PCI カード

ASA 5580 は、次の PCI カードをサポートします。

- 4 ポート ギガビット イーサネット銅線 PCI カード

  4 個の 10/100/1000BASE-T インターフェイスを提供します。これらのインターフェイスは、合計で最大 24 個のギガビット イーサネット インターフェイスを許容します。図 2-3 に、ギガビット イーサネット インターフェイス カードを示します。

図 2-3　4 ポート ギガビット イーサネット銅線 PCI カード

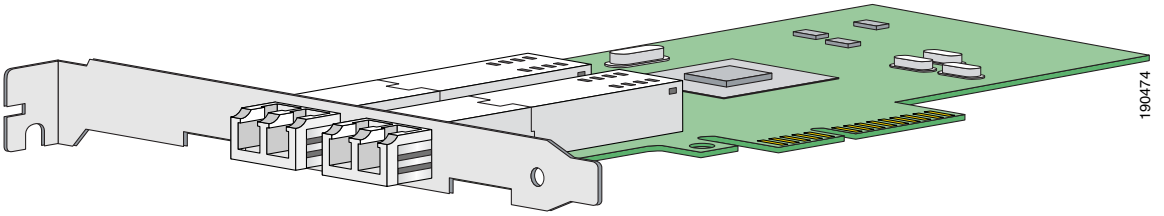


- 2 ポート 10 ギガビット イーサネット ファイバ PCI カード

  2 個の 10000BASE-SX（ファイバ）インターフェイスを提供します（完全に実装された状態のシャーシでは、合計で最大 12 個の 10 ギガビット イーサネット ファイバ インターフェイスを許容します）。

  カード ポートには、センサーの SX インターフェイスに接続するために、LC コネクタを持つマルチモード ファイバ ケーブルが必要です。図 2-4 に、2 ポート 10 ギガビット イーサネット ファイバ PCI カードを示します。

図 2-4　2 ポート 10 ギガビット イーサネット ファイバ PCI カード



- 4 ポート ギガビット イーサネット ファイバ PCI カード

  4 個の 10000BASE-SX（ファイバ）インターフェイスを提供します（完全に実装された状態のシャーシでは、合計で最大 24 個のギガビット イーサネット ファイバ インターフェイスを許容します）。

  カード ポートには、センサーの SX インターフェイスに接続するために、LC コネクタを持つマルチモード ファイバ ケーブルが必要です。

パフォーマンスの最適化

トラフィックのスループットを最大化するには、適応型セキュリティ アプライアンスのトラフィック フローとハードウェア構成が次のガイドラインを満たしている必要があります。

- 望ましいパフォーマンスが実現するのは、同一アダプタ上のポート、または同一 I/O ブリッジによってサービスが行われているポートをトラフィックが出入りする場合です。

  ASA 5580 には 2 個の I/O ブリッジがあり、I/O スロットは 2 個の I/O ブリッジのいずれか一方に接続します。スロット 3、スロット 4、スロット 5、スロット 6 のアダプタは一方の I/O ブリッジ上にあり、スロット 7 とスロット 8 はもう一方の I/O ブリッジ上にあります。

  最適なパフォーマンスが実現するのは、トラフィックが両方の I/O ブリッジを通過しない場合です。具体的には、同一バスのアダプタ上のポート間をトラフィックが流れる必要があります。

  スロット 7 と 8 のアダプタ上のポートをトラフィックが通過するように設定します。この設定により、そのトラフィックの最適なパフォーマンスが得られます。スロット 3 ～ 6 のアダプタ上のポートにトラフィックがとどまるように設定します。大容量 I/O ブリッジ（PCIe x8）上のスロット 7 とスロット 8 のポートをトラフィックが通過するように設定した例については、図 2-5 を参照してください。

- アダプタから最適なパフォーマンスを得るために 10 ギガビット イーサネットのアダプタを使用する場合は、大容量 I/O ブリッジ（PCIe x8）上のスロット（スロット 5、スロット 7、およびスロット 8）にアダプタを設置します。

  （注） 10 ギガビット イーサネットのアダプタとポートを使用すると、正しいトラフィック プロファイルが割り当てられた 1 つのポート上で 10 ギガビット イーサネット全二重を実現できます。バス帯域幅により、同一アダプタ上の 10 ギガビット イーサネット 2 ポート パフォーマンスは 16 Gbps 未満の全二重に制限されます。

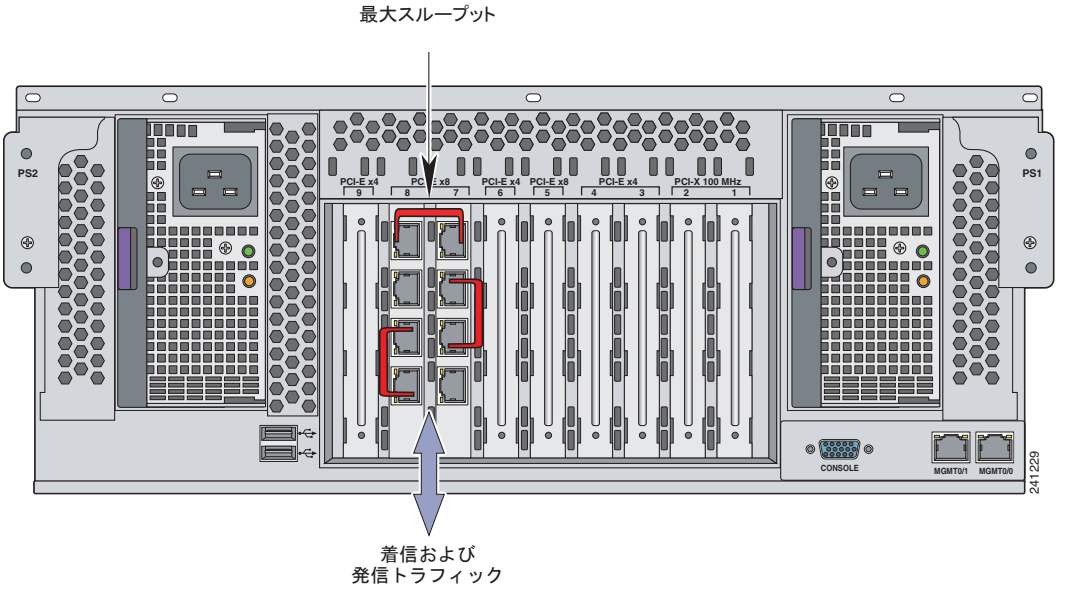
- 4 ポート アダプタは、どのスロットにも設置できます。ただし、各ポートに 1 ギガビット全二重相当のトラフィックがある場合は、バスがボトルネックになる可能性があります。通常速度のバスの帯域幅により、1 つのアダプタの集約帯域幅は 8 Gbps 未満に制限されます。

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

- 管理ポートは、**management-only** コマンドを削除することで、通過トラフィックに対応できます。ただし、管理専用のポートは、データ トラフィックの通過に関して最適化されていません。また、アダプタ上のポートと同様の機能もありません。

図 2-5 に、大容量 I/O ブリッジ（PCIe x8）上のスロット 7 とスロット 8 のポートをトラフィックが通過するように設定した例を示します。

図 2-5　最適なパフォーマンスを実現するトラフィック フローの例



次の手順

第 3 章「ASA 5580 の取り付け」に進みます。

CHAPTER 3

ASA 5580 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 5580 Adaptive Security Appliance*』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、適応型セキュリティ アプライアンスおよびラックマウントについて説明し、適応型セキュリティ アプライアンスの設置手順を示します。この章には、次の項があります。

パッケージ内容の確認

梱包箱の内容が 図 3-1 と同じかどうかを調べて、ASA 5580 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 5580 パッケージの内容

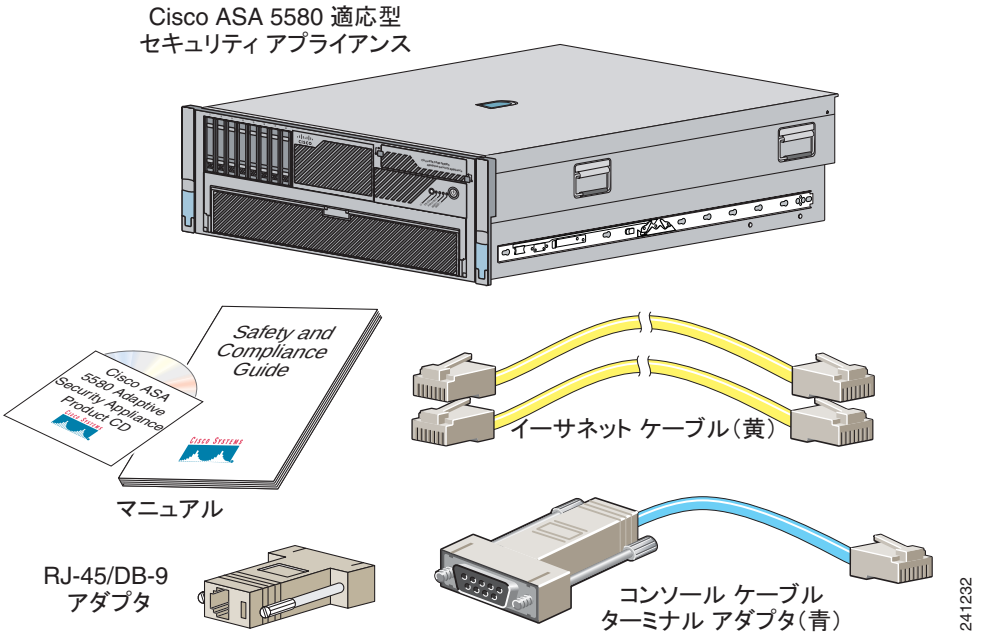


図 3-1 の内容に加え、ASA 5580 パッケージにはレール システム キットも含まれています。レール システム キットを構成する品目は次のとおりです。

- スライド アセンブリ 2 個
- シャーシ レール 2 個
- マジックテープ ストラップ 4 本
- ケーブル タイ 6 本
- ケーブル管理アーム 1 個
- 各種部品のパッケージ（ネジなど）
- ケーブル管理アーム ストッパ ブラケット 1 個

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。

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

次の情報は、ラックへの機器の取り付けを計画する場合に役立ちます。

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

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

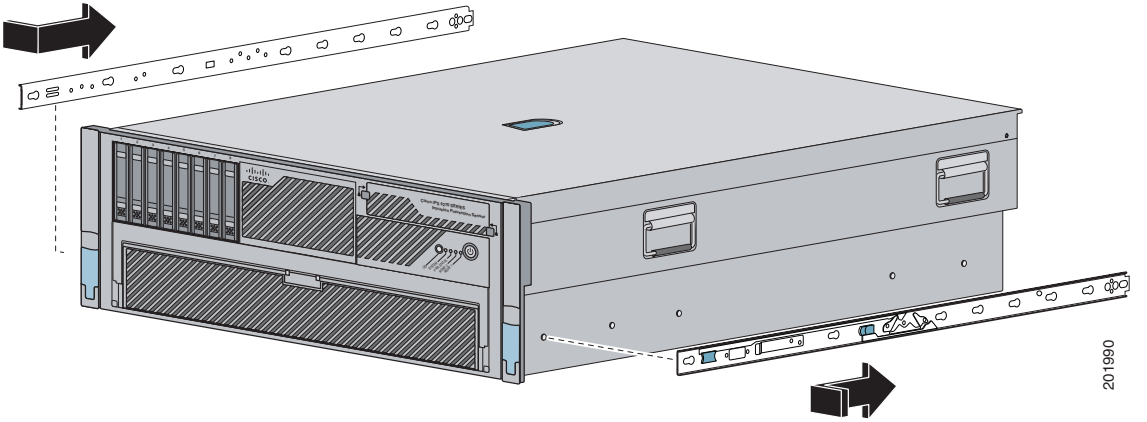
シャーシのラックマウント

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。**
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。
すでに別の装置が取り付けられているラックに装置をマウントする場合は、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。ステートメント 1006
適応型セキュリティ アプライアンスをスライド アセンブリに置いてからラックに収めるため、この手順は 2 人以上で行う必要があります。

ラックに適応型セキュリティ アプライアンスを取り付けるには、次の手順を実行します。

ステップ 1　シャーシ サイド レールを適応型セキュリティ アプライアンスに取り付けます。取り付けるには、シャーシ サイド レールを適応型セキュリティ アプライアンスの突起に合せて押し込み、ラッチのはまる音が聞こえるまで、シャーシ サイド レールを後ろにスライドさせます。図 3-2 を参照してください。

図 3-2　シャーシ サイド レールの取り付け

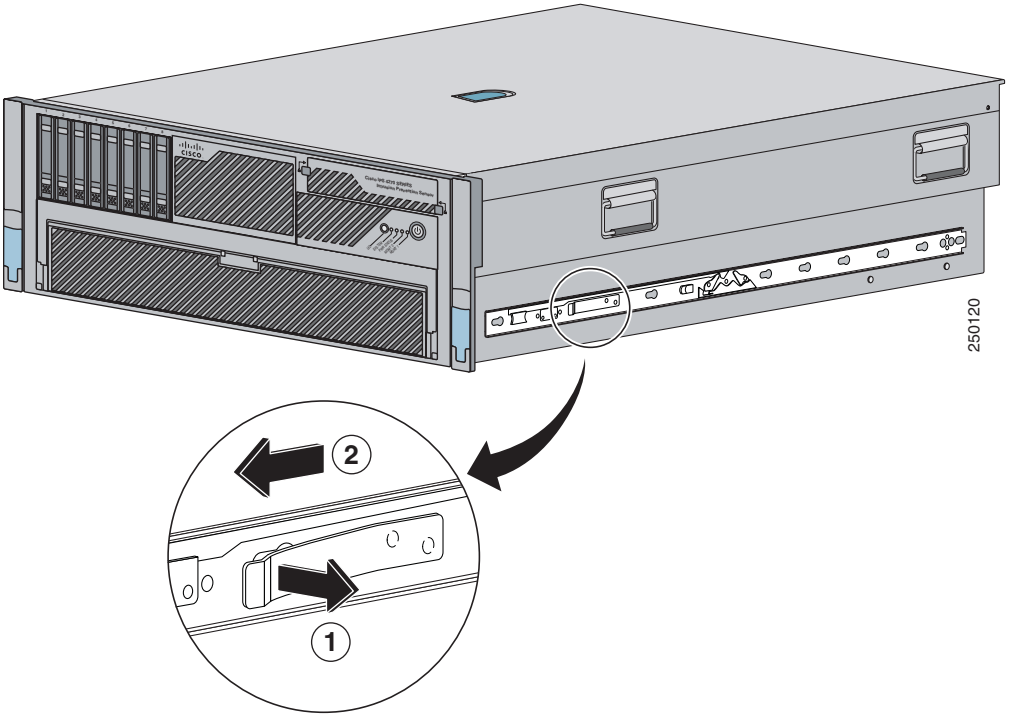


(注) シャーシ サイド レールの細い方の端が適応型セキュリティ アプライアンスの後部になるようにしてください。シャーシ サイド レールは、内側のラッチで所定の位置に固定されます。

ステップ 2　各シャーシ サイド レールについてステップ 1 を繰り返します。

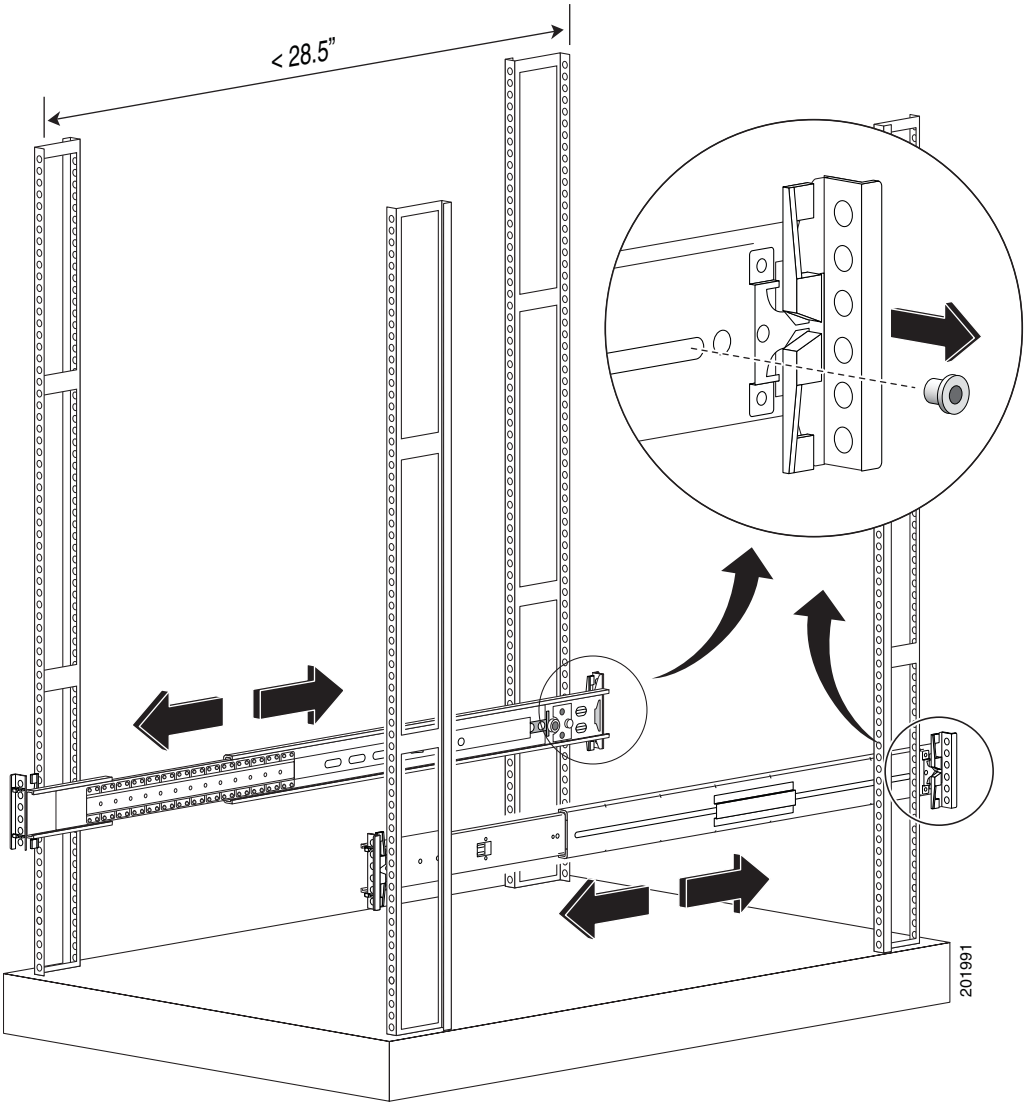
ステップ 3　シャーシ サイド レールを取り外すには、ラッチを上げ、レールを前にスライドさせます。図 3-3 を参照してください。

図 3-3　シャーシ サイド レールからの取り外し



ステップ 4　奥行きのないラック（28.5 インチ（72.39 cm）未満のラック）に適応型セキュリティ アプライアンスを取り付ける場合は、スライド アセンブリの内側からネジを取り外した後に、ステップ 5 に進みます。図 3-4 を参照してください。

図 3-4　スライド アセンブリの内側のネジ



ステップ 5　スライド アセンブリをラックに取り付けます。図 3-5 を参照してください。

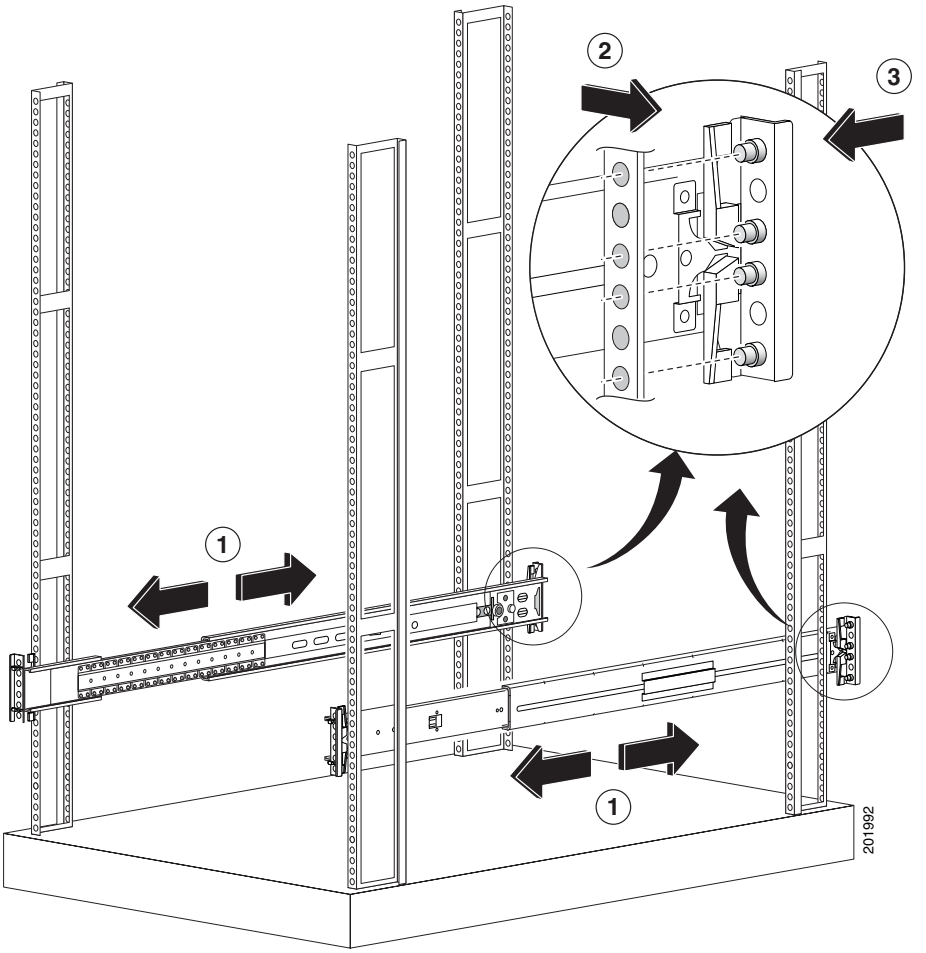
丸穴ラックおよび角穴ラックの場合：

a. ラックの内側にある穴にスライド　アセンブリの突起を合せ、所定の位置にはめ込みます。

b. スライド アセンブリを縦方向に調節して、ラックに取り付けます。

スプリング ラッチでスライド アセンブリを所定の位置にロックします。

図 3-5　スライド アセンブリの取り付け



c. 各スライド アセンブリについて同じ作業を繰り返します。

ラック内で 2 つのスライド アセンブリの取り付け位置が揃っていることを確認します。

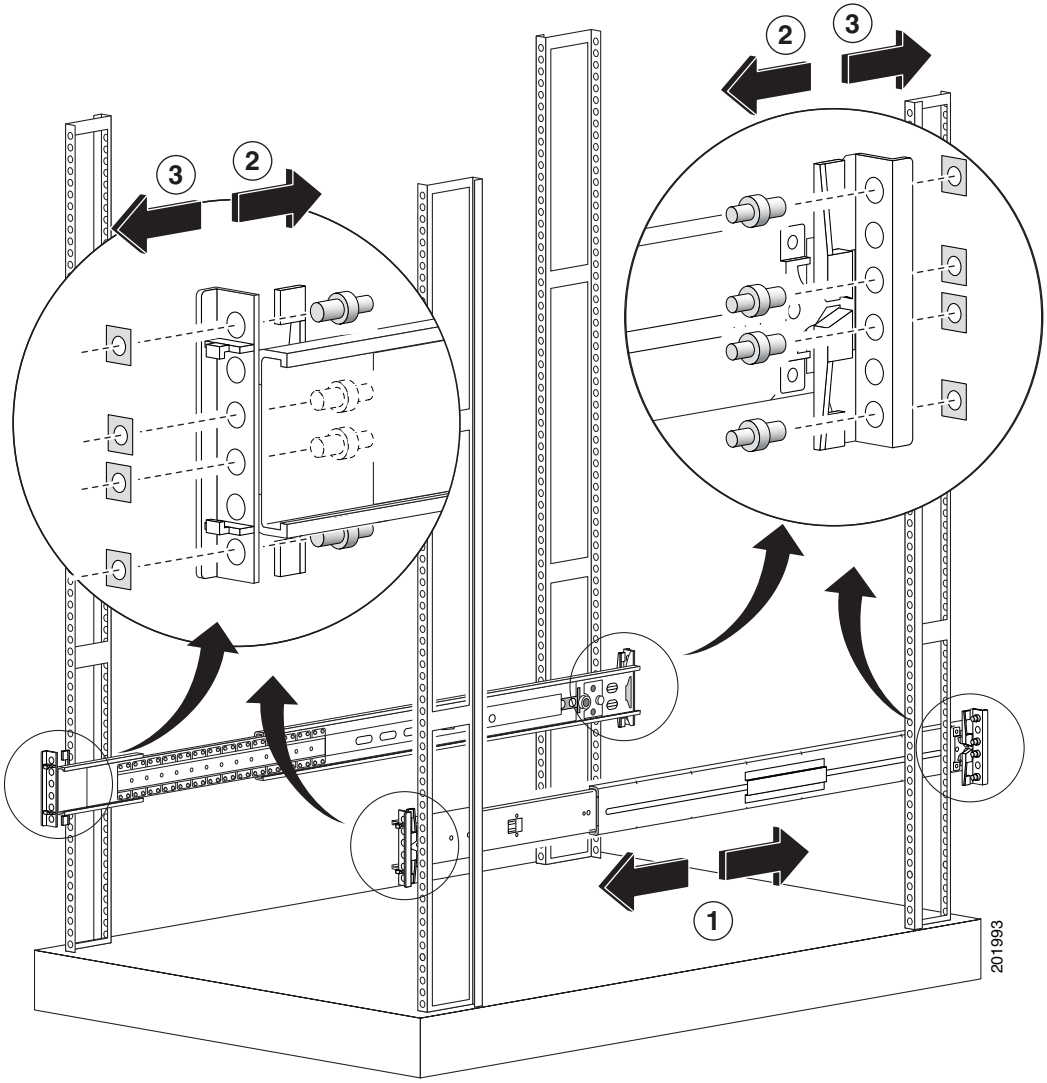
d. 位置を修正する必要がある場合は、スプリング ラッチを上げてスライド アセンブリを外します。

ネジ穴ラックの場合：

a. 各スライド　アセンブリの丸穴または角穴の突起を通常のドライバで取り外します。図 3-6 を参照してください。

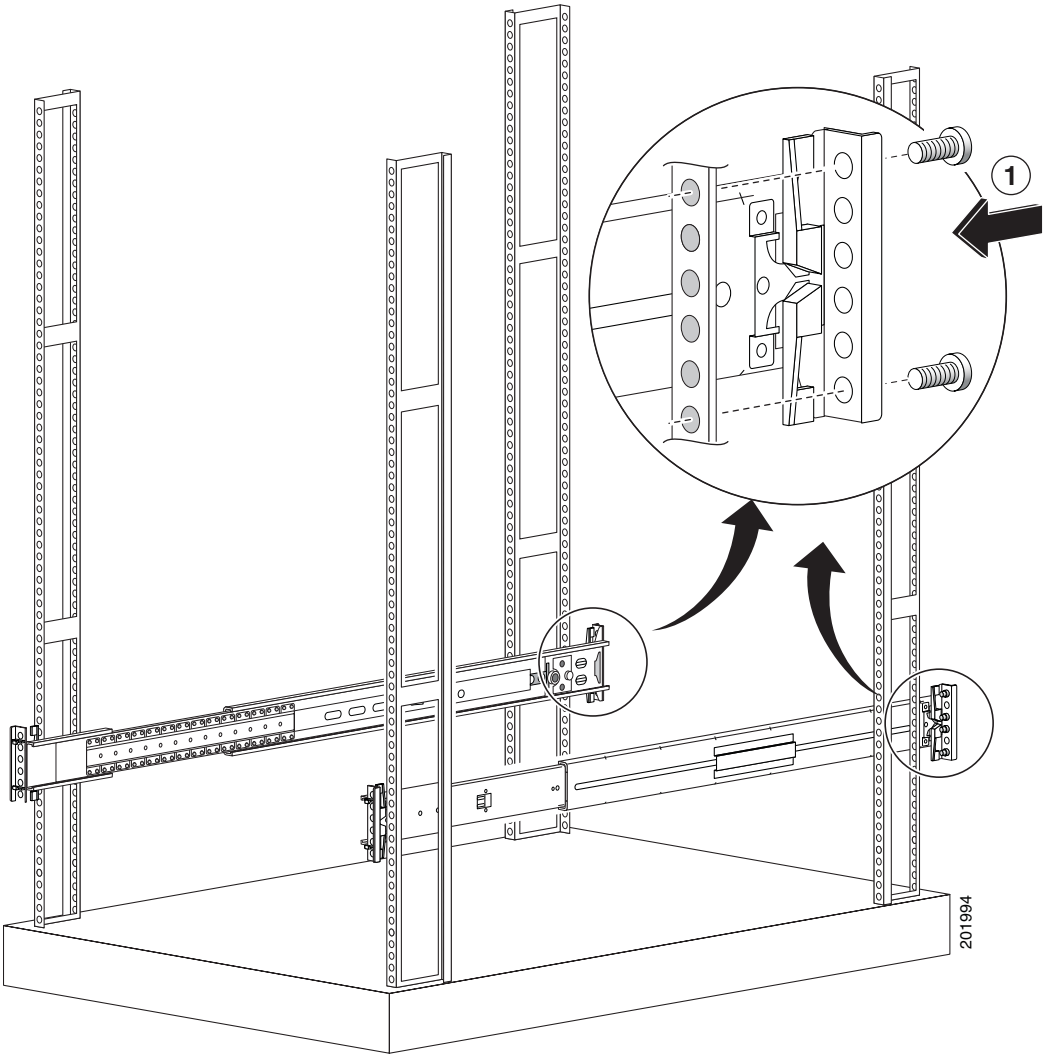
（注） 保持ナットを留めるために、プライヤが必要になる場合があります。

図 3-6　ネジ穴のラックの取り付け



b. ラックの穴にスライド アセンブリのブラケットを合せ、スライド アセンブリの各端に 2 つのネジ（上下）を取り付けます。図 3-7 を参照してください。

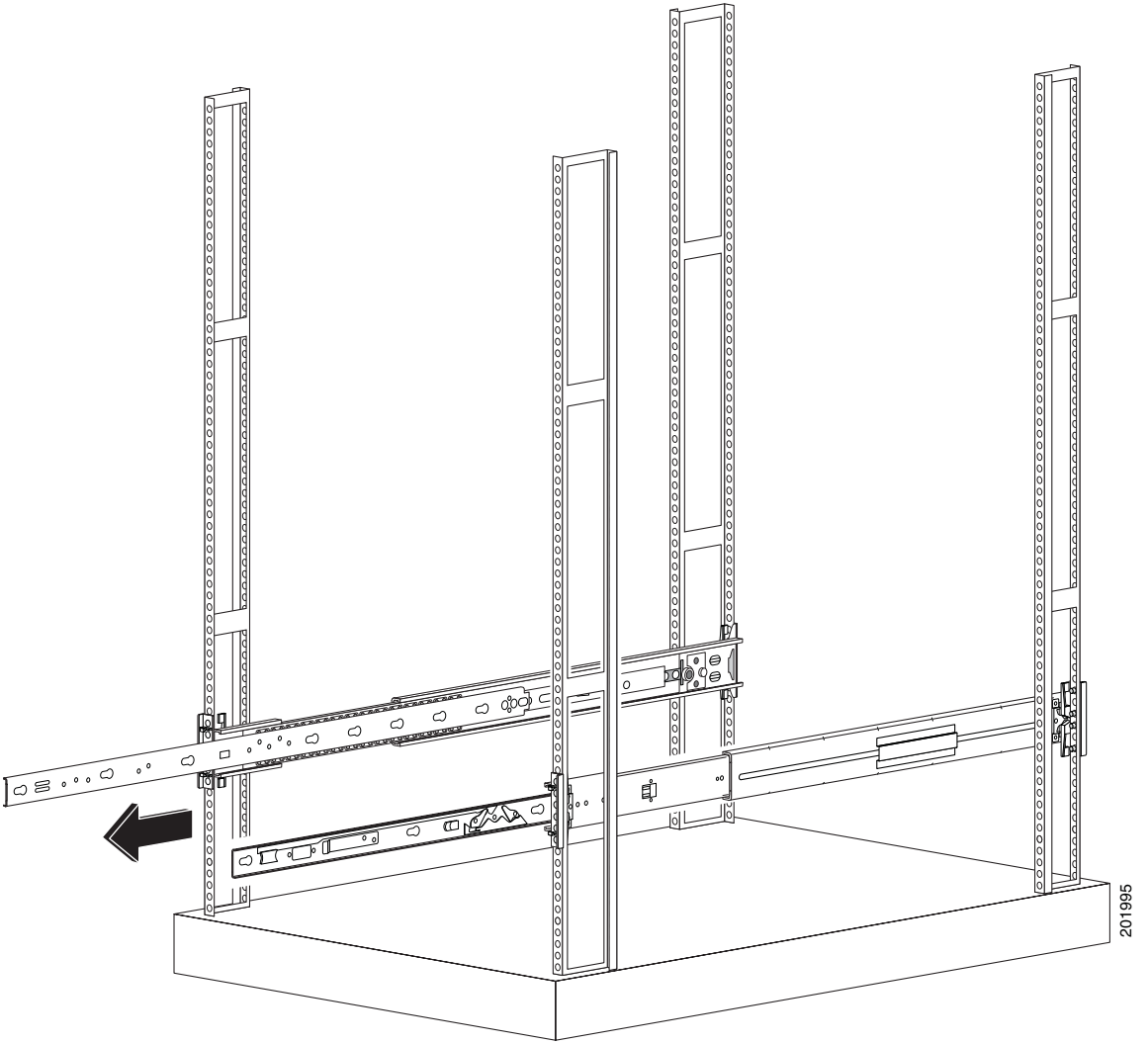
図 3-7　ブラケットの位置合せ



c. 各スライド アセンブリについて同じ作業を繰り返します。

ステップ 6　スライド アセンブリをラックから引き出します。図 3-8 を参照してください。

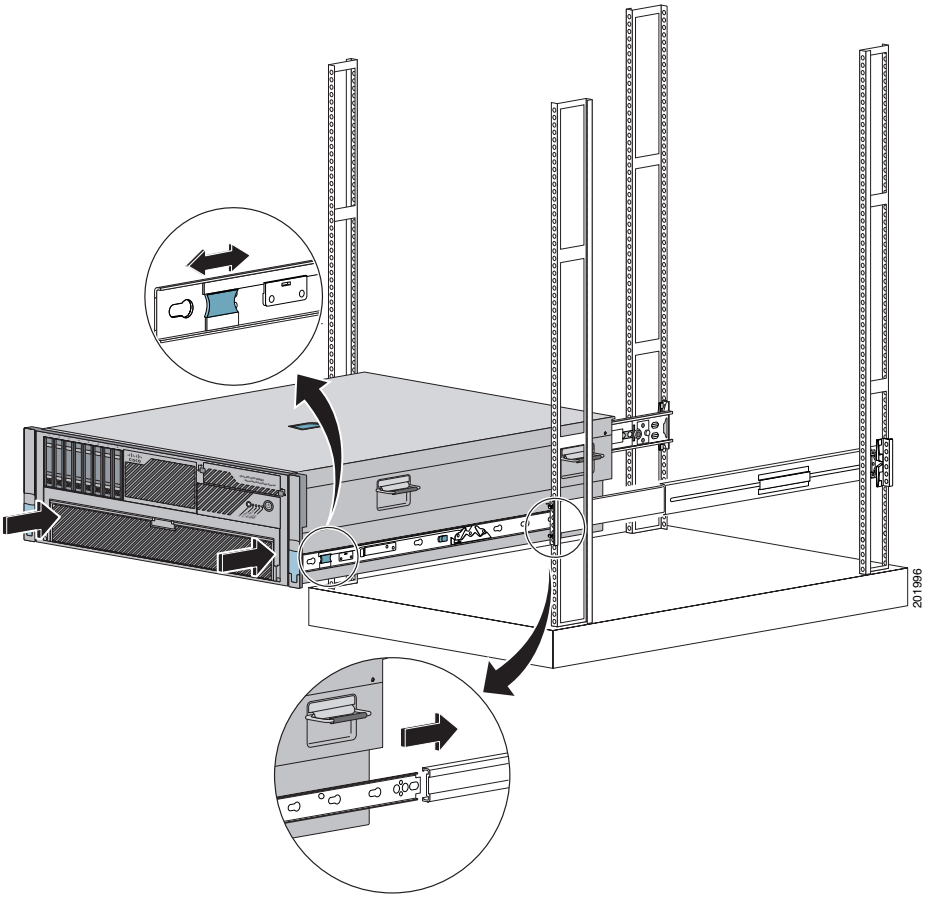
図 3-8　引き出された状態のスライド アセンブリ



ステップ 7　適応型セキュリティ アプライアンスのシャーシ サイド レールをラック両側のスライド アセンブリに合せ、青いスライドつまみを外します（つまみを前に引っ張るか、後ろへ押します）。その後、慎重に適応型セキュリティ アプライアンスを所定の位置に押し込みます。図 3-9 を参照してください。

警告　**適応型セキュリティ アプライアンスを空のラックに取り付ける場合は、適応型セキュリティ アプライアンスが青いスライドつまみにはまり、完全にラックに収まるまで、適応型セキュリティ アプライアンスを前から支える必要があります。支えないと、ラックが転倒する恐れがあります。**

図 3-9　シャーシ サイド レールの位置合せ



注意　適応型セキュリティ アプライアンスを床と平行にしたまま、レールにスライドさせてください。適応型セキュリティ アプライアンスを上下に傾けると、スライド レールが損傷する恐れがあります。

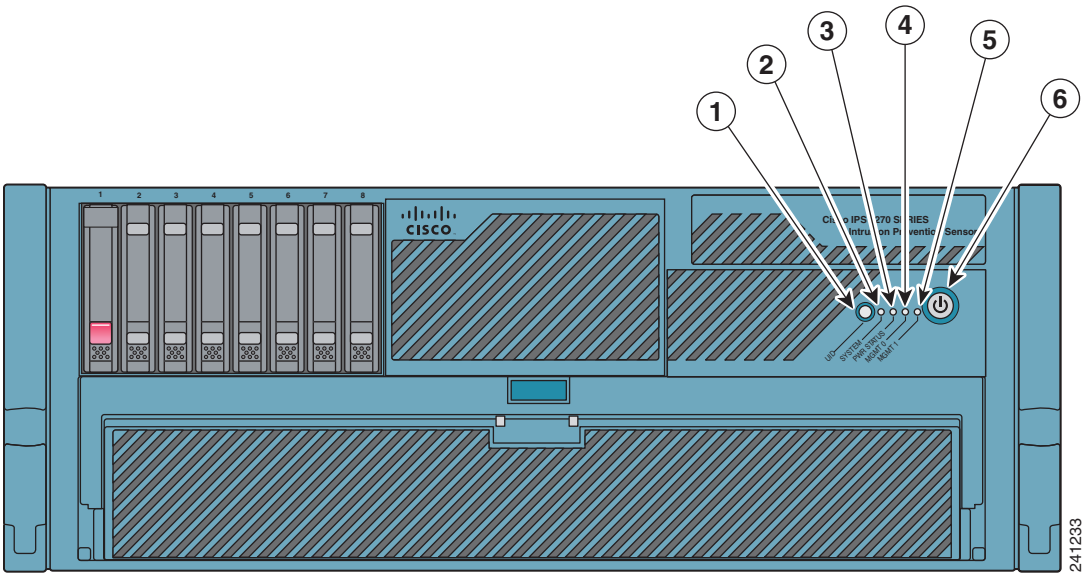
ポートと LED

この項では、前面パネルと背面パネルについて説明します。次のトピックについて取り上げます。

前面パネルの LED

図3-10 に、適応型セキュリティ アプライアンスの前面パネルの LED を示します。

図 3-10　正面図



1	アクティブ LED	2	システム LED
3	電源ステータス LED	4	管理 0/0 LED
5	管理 0/1 LED	6	電源

表 3-1 で、ASA 5580 の前面パネルにあるスイッチとインジケータについて説明します。

表 3-1　前面パネルのスイッチとインジケータ

インジケータ	説明
アクティブ	シャーシのアクティブ / スタンバイ フェールオーバー ステータスを切り替えます。 • 点灯：フェールオーバーがアクティブです。 • 消灯：スタンバイ ステータスです。
システム インジケータ	内部システム ヘルスを示します。 • 緑色：システムが稼働しています。 • オレンジ色の点滅：システム　ヘルスが低下しています。 • 赤色の点滅：システム　ヘルスが危機的状況にあります。 • 消灯：システムが停止しています。
電源ステータス インジケータ	電源ステータスを示します。 • 緑色：電源が入っています。 • オレンジ色の点滅：電源ヘルスが低下しています。 • 赤色の点滅：電源ヘルスが危機的状況にあります。 • 消灯：電源が切れています。
管理 0/0 インジケータ	管理ポートのステータスを示します。 • 緑色：ネットワークに接続されています。 • 緑色の点滅：接続されたネットワーク上でアクティビティが発生しています。 • 消灯：ネットワークに接続されていません。

表 3-1　前面パネルのスイッチとインジケータ（続き）

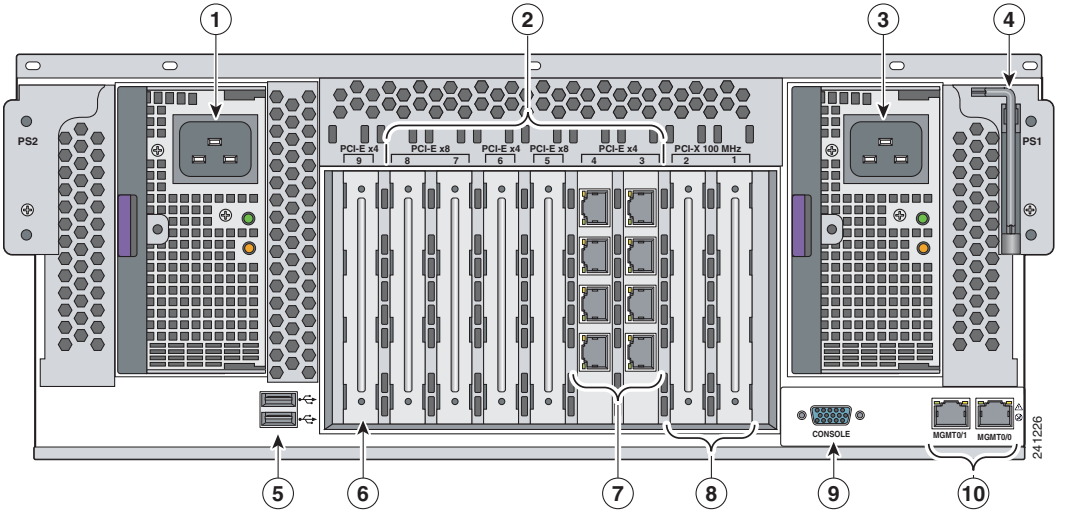
インジケータ	説明
管理 0/1 インジケータ	管理ポートのステータスを示します。 • 緑色：ネットワークに接続されています。 • 緑色の点滅：接続されたネットワーク上でアクティビティが発生しています。 • 消灯：ネットワークに接続されていません。
電源スイッチとインジケータ	電源の投入 / 切断を行います。 • オレンジ色：システムは AC 電源が入っており、スタンバイ モードになっています。 • 緑色：システムは AC 電源が入っており、稼働しています。 • 消灯：システムの AC 電源が入っていません。

管理ポートの詳細については、『*Cisco Security Appliance Command Reference*』の **management-only** コマンドの説明を参照してください。

背面パネルの LED とポート

図 3-11 に、背面パネルの LED とポートを示します。

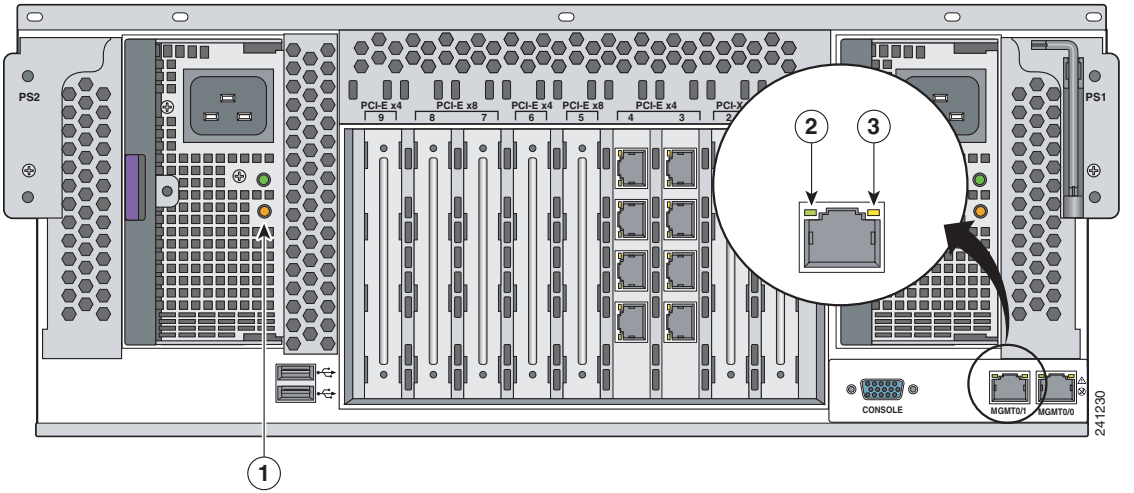
図 3-11　背面パネルの外観



1	電源モジュール	**2**	インターフェイス拡張スロット
3	電源モジュール	**4**	T-15 トルクス ドライバ
5	USB ポート	**6**	予備スロット
7	実装されたスロットの例	**8**	予備スロット
9	コンソール ポート	**10**	管理ポート

図 3-12 に、イーサネット ポートのアクティビティ インジケータを示します。アクティビティ インジケータには、ポートごとに 2 つのインジケータと電源モジュールのインジケータがあります。

図 3-12　背面パネルの LED



1	電源インジケータ	2	接続インジケータ
3	アクティビティ インジケータ		

表 3-2 で、イーサネット ポート インジケータについて説明します。ポート インジケータの動作は、ポートのタイプ（管理ポート、ギガビット イーサネット インターフェイス カードのポート、10 ギガビット イーサネット ファイバ インターフェイス カードのポート、またはギガビット イーサネット ファイバ インターフェイス カードのポート）によって異なります。

表 3-2　イーサネット ポート インジケータ

インジケータ	説明
ギガビット イーサネット	緑色（上）：ネットワークに接続されています。 緑色の点滅（上）：接続されたネットワーク上でアクティビティが発生しています。 オレンジ色（下）：速度 1000 緑色（下）：速度 100 消灯（下）：速度 10
10 ギガビット イーサネット ファイバ（1 つの LED）	緑色：ネットワークに接続されています。 緑色の点滅:接続されたネットワーク上でアクティビティが発生しています。
ギガビット イーサネット ファイバ（1 つの LED）	緑色：ネットワークに接続されています。 緑色の点滅:接続されたネットワーク上でアクティビティが発生しています。
管理ポート	緑色（右）：ネットワークに接続されています。 緑色の点滅（左）：接続されたネットワーク上でアクティビティが発生しています。 **（注）** 管理ポートのインジケータは、ネゴシエートされた速度（10/100/1000）にかかわらず、緑色になります。これに対し、ギガビット イーサネット インターフェイス カードは、1000 Mbps 接続がネゴシエートされた場合、オレンジ色の LED になります。

表 3-3 で、電源モジュールのインジケータについて説明します。

表 3-3　電源モジュールのインジケータ

故障インジケータ 1 オレンジ色	電源インジケータ 2 緑色	説明
消灯	消灯	すべての電源モジュールの AC 電源が入っていません。
点滅	消灯	電源モジュールが故障しています（過電流）。
点灯	消灯	この電源モジュールの AC 電源が入っていません。
消灯	点滅	• AC 電源が入っています。 • スタンバイ モードです。
消灯	点灯	正常です。

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、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、デバイスを管理するための専用の管理インターフェイスがあります。管理ポート（管理 0/0 ポートと管理 0/1 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。管理ポートはコンソール ポートと類似していますが、（through-the-box のトラフィックとは対照的な）to-the-box 宛のトラフィックのみを受け入れます。管理 0/0（MGMT0/0）は、コマンド制御ポートです。

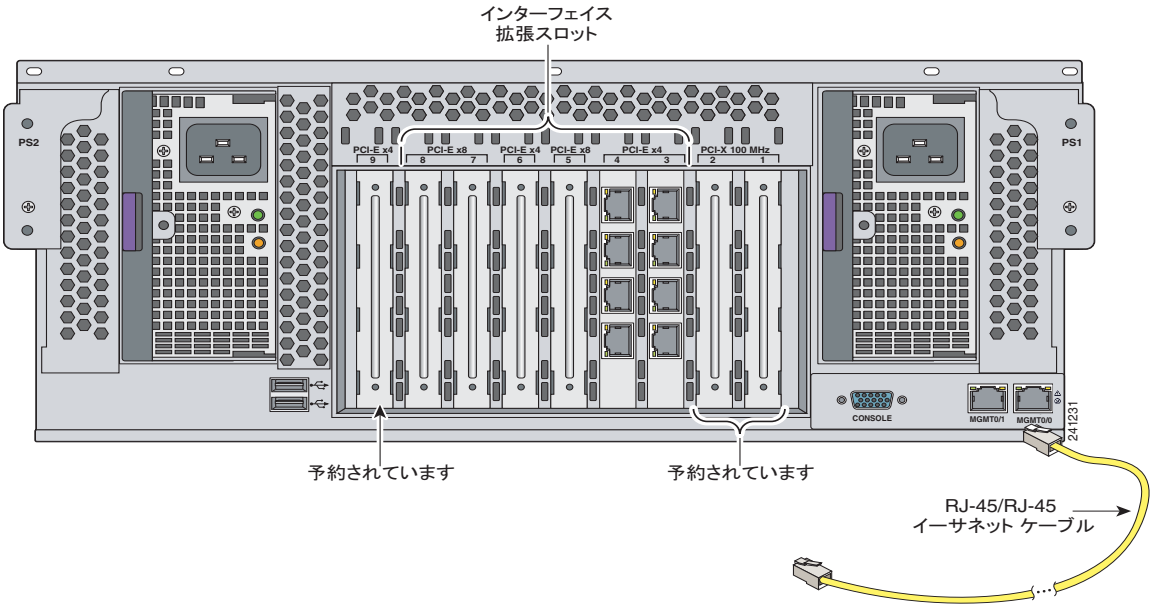
（注）　インターフェイスを管理専用インターフェイスとして設定するには、**management-only** コマンドを使用します。管理インターフェイス上の管理専用の設定モードをディセーブルにすることもできます。このコマンドの詳細については、『*Cisco Security Appliance Command Reference*』の **management-only** コマンドの説明を参照してください。

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

b.　RJ-45 コネクタの一方を管理 0/0 ポートに接続します。図 3-13 を参照してください。

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

図 3-13　管理ポートへの接続



注意　管理ポートとコンソール ポートは、特権付きの管理用ポートです。これらのポートを非信頼ネットワークに接続すると、セキュリティ上の問題が発生する可能性があります。

ステップ 3　コンソール ポートに接続します。設定コマンドを入力するには、コンソール ポートを使用してコンピュータに接続します。

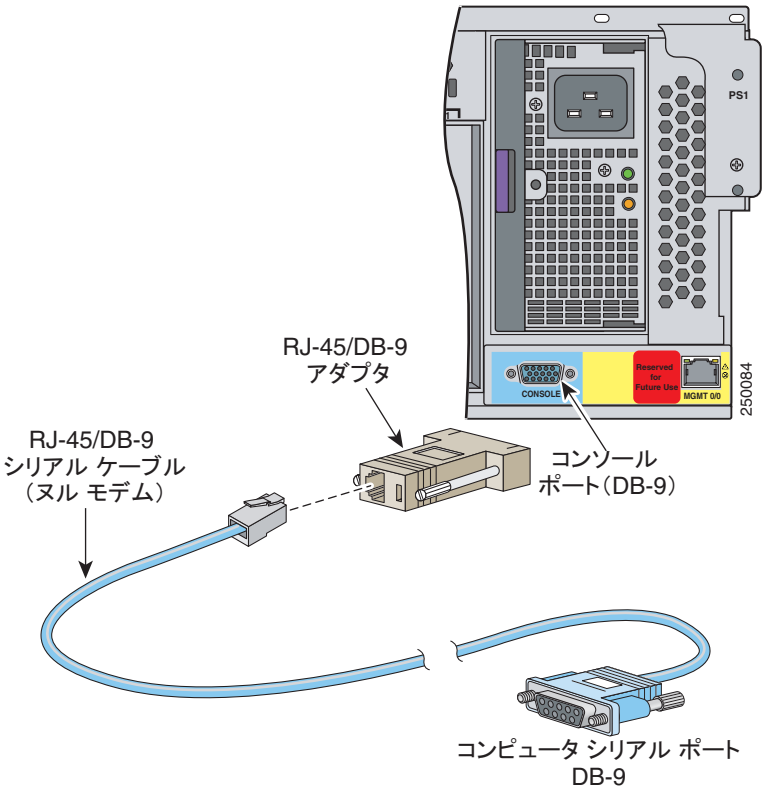
a. コンピュータまたはターミナルを任意のポートに接続する前に、シリアル ポートのボー レートを確認します。コンピュータまたはターミナルのボー レートは、適応型セキュリティ アプライアンスのコンソール ポートのデフォルト ボー レート（9600 ボー）と一致している必要があります。

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. RJ-45/DB-9 アダプタのコネクタをコンソール ポートに接続し、もう一方の端をコンピュータの DB-9 コネクタに接続します。図 3-14 を参照してください。

（注） 180/ ロールオーバーまたはストレート型パッチ　ケーブルを使用して、RJ-45 またはヒドラ ケーブル アセンブリ接続で、アプライアンスをターミナル サーバのポートに接続できます。適切なケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。

図 3-14　RJ-45/DB-9 アダプタの接続

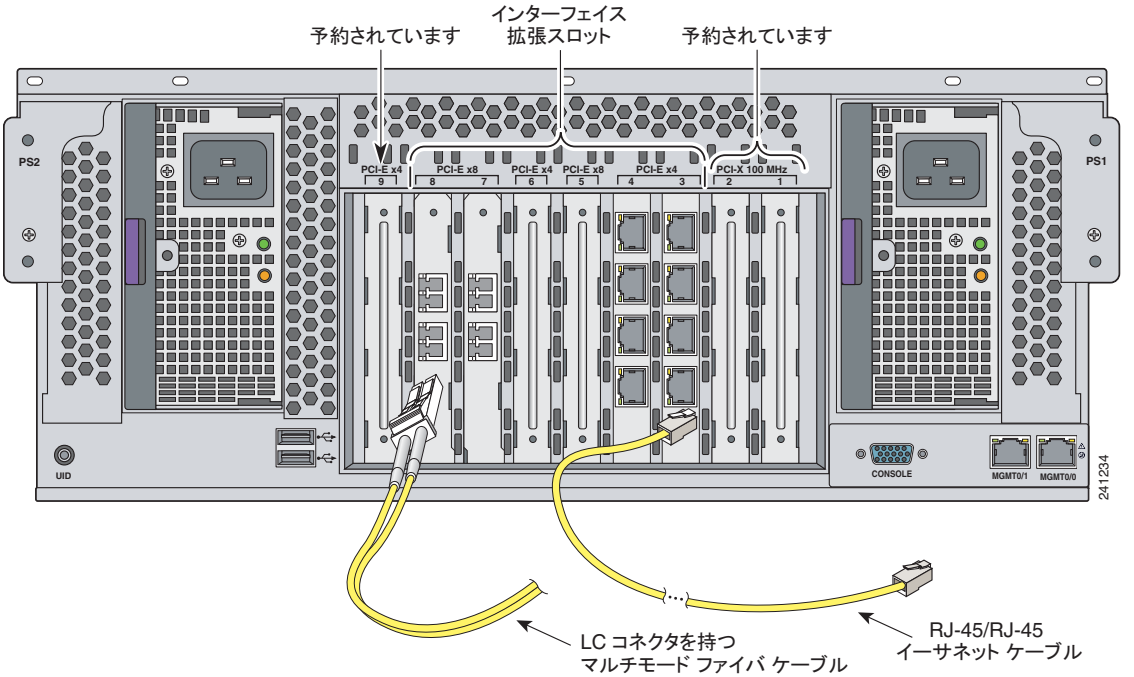


ステップ 4　ネットワーク接続用の銅線およびファイバ イーサネット ポートを接続します。銅線およびファイバ イーサネット ポートはスロット 3 ～スロット 8 で使用できます。

デフォルトでは、使用可能なスロット 3 ～スロット 8 が ASA 5580 に付属しています。I/O アダプタ オプションのバンドルを購入することもできます。第 2 章「ASA 5580 のスループットの最大化」の「*パフォーマンスの最適化*」を参照してください。

a.　イーサネット ケーブルの一方の端をスロット 3 ～ 8 のイーサネット ポートに接続します。図 3-15 を参照してください。

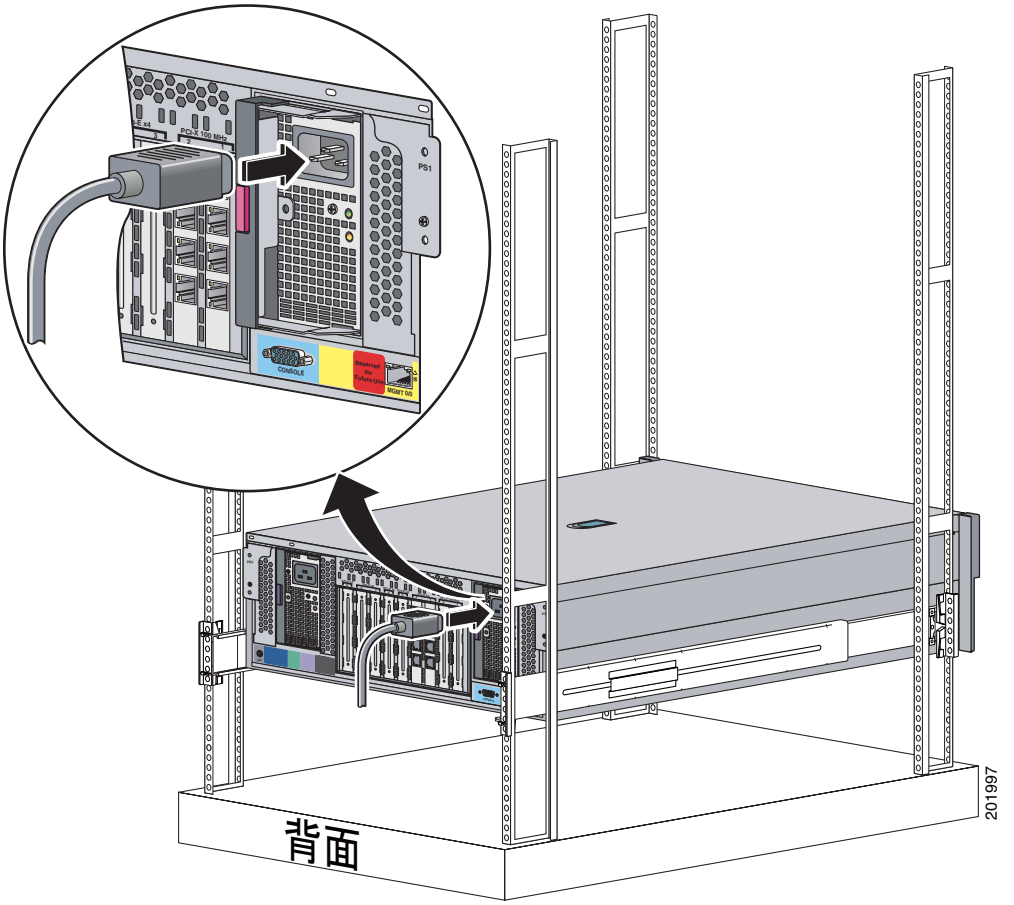
図 3-15　銅線イーサネットまたはファイバ イーサネット インターフェイス



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、スイッチなど）に接続します。

ステップ 5　適応型セキュリティ アプライアンスの背面に電気ケーブルを取り付けます。電源コードを取り付け、電源に差し込みます（電源には UPS を推奨します）。図 3-16 を参照してください。

図 3-16　電気ケーブルの取り付け



ステップ 6　シャーシの電源を入れます。

次の手順

第 4 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

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を示します。

この章には、次の項があります。

工場出荷時のデフォルト設定について

シスコの適応型セキュリティ アプライアンスは、すぐにスタートアップできるように、工場出荷時のデフォルト設定が設定されて出荷されます。ASA 5580 適応型セキュリティ アプライアンスの工場出荷時のデフォルト設定は、次のとおりです。

- 管理インターフェイスの管理 0/0。**configure factory-default** コマンドで IP アドレスを設定しなかった場合、IP アドレスとマスクは 192.168.1.1 と 255.255.255.0 になります。
- DHCP サーバは適応型セキュリティ アプライアンスでイネーブルになっているため、インターフェイスに接続している PC は 192.168.1.2 ～ 192.168.1.254 のアドレスを受信します。
- HTTP サーバは ASDM に対してイネーブルになっており、192.168.1.0 ネットワーク上でユーザにアクセスできます。

この設定は、次のコマンドで構成されています。

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

CLI による設定

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。

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に関する詳細な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 による設定

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。

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（P.4-4）
- 初期セットアップ用の設定情報の収集（P.4-5）
- ASDM Launcher のインストール（P.4-5）
- Web ブラウザでの ASDM の起動（P.4-8）

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　イーサネット ケーブルを使用して管理 0/0 インターフェイスをスイッチまたはハブに接続します（まだ接続していない場合）。適応型セキュリティ アプライアンスを設定するには、このスイッチに 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自動的に IP アドレスを受信できます）。この設定により、PC は適応型セキュリティ アプライアンスおよびインターネットとの通信が可能になり、設定や管理の作業のために ASDM を実行できます。

あるいは、192.168.1.0 サブネット内のアドレスを選択して、固定 IP アドレスを PC に割り当てます（有効なアドレスは、255.255.255.0 のマスクと 192.168.1.1 のデフォルト ルートを持つ 192.168.1.2 ～ 192.168.1.254 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は、同一の IP アドレスを設定しないようにしてください。

（注）　適応型セキュリティ アプライアンスの管理 0/0 インターフェイスは、デフォルトで 192.168.1.1 に割り当てられます。したがって、このアドレスは使用できません。

ステップ 3　管理 0/0 インターフェイスの LINK LED を確認します。

接続が確立されている場合は、適応型セキュリティ アプライアンスの LINK LED インターフェイスおよび対応するスイッチまたはハブの LINK LED が緑色に点灯します。

初期セットアップ用の設定情報の収集

ASDM Startup Wizard で使用される、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、およびその他のすべてのこれから設定するインターフェイスの IP アドレス。
- ASDM の HTTPS、SSH、または Telnet を使用して、このデバイスに管理アクセスできるホストの IP アドレス。
- 管理アクセス用の特権モードのパスワード。
- NAT または PAT アドレス変換に使用する IP アドレス（存在する場合）。
- 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 つ目の VLAN を作成し、その VLAN にポートを割り当てる必要があります（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（同一セキュリティ　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るかどうか、および同一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 アドレスが必要です。また、クライアントを実行するモード（クライアント モードまたはネットワーク拡張モード）、プライマリおよびセカンダリ Easy VPN サーバに設定されたユーザとグループのログイン クレデンシャルも必要です。

ASDM Launcher のインストール

ASDM を起動するには、2 つの方法があります。ASDM Launcher ソフトウェアをダウンロードして、PC 上で ASDM をローカルで実行する方法、および Web ブラウザで Java と JavaScript をイネーブルにして 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 をローカルで実行するようにシステムをセットアップ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、次の URL を入力します。
https://192.168.1.1/admin

(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 の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入れます。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** をクリックしてインストール プログラムを直接実行します。インストール ソフトウェアをハードドライブ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 フィールドと Password フィールドを空のままにします。

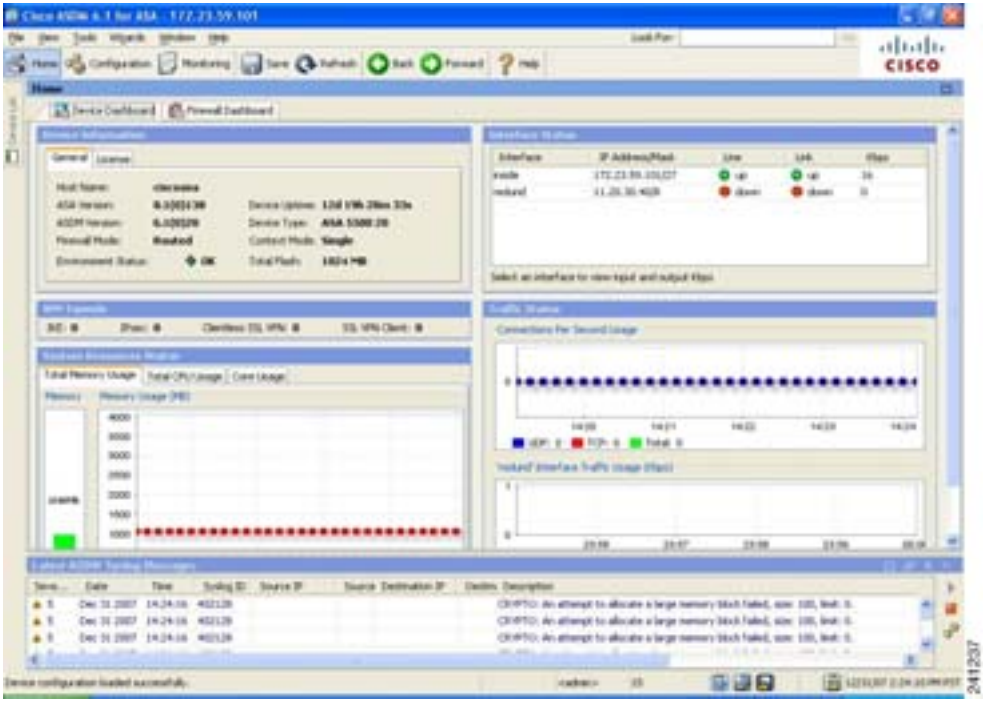
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

ステップ 5　OK をクリックします。

ステップ 6　証明書の受け入れを求めるセキュリティ警告が表示された場合は、**Yes** をクリックします。

適応型セキュリティ アプライアンスは最新ソフトウェアが存在するかどうかを調べ、存在す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。



Web ブラウザでの ASDM の起動

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

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

ASDM のメイン ウィンドウが表示されます。

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 ウィンドウの上部にあるウィザードのメニューから、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、ウィンドウの下部にある **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は、付録 A「3DES/AES ライセンスの取得」を参照してください。

（注）　ネットワーク セキュリティ ポリシーに基づき、外部インターフェイスまたは必要なその他の任意のインターフェイスを経由するすべての ICMP トラフィックを拒否するように、適応型セキュリティ アプライアンスを設定することを検討する必要があります。このアクセス コントロール ポリシーは、ASDM を使用して設定できます。ASDM のメインページから、**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

次に示す 1 つ以上の章を参照し、適応型セキュリティ アプライアンスを設定して配置します。

作業内容	参照先
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 5 章「シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定」
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 6 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 7 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 VPN 用の適応型セキュリティ アプライアンスの設定	第 8 章「シナリオ：IPsec リモート アクセス VPN の設定」

CHAPTER 5

シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定

この章では、リモート ユーザが Cisco AnyConnect VPN クライアントを使用して 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について説明します。

この章には、次の項があります。

SSL VPN クライアント接続について

SSL VPN クライアントがセットアップされている場合、リモート ユーザは、接続を確立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はありません。代わりに、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。ブラウザは、そのインターフェイスに接続し、SSL VPN ログイン画面を表示します。ユーザが正常に認証された後、適応型セキュリティ アプライアンスは、そのユーザがクライアントを必要としていると認識すると、リモート コンピュータのオペレーティング システムに適合するクライアントをプッシュします。

（注） Cisco AnyConnect VPN クライアントを初めてインストールまたはダウンロードする場合は、管理者権限が必要です。

ダウンロード後、クライアント自身がインストールと設定を行ってから、セキュアな SSL 接続を確立します。接続が終了すると、クライアント ソフトウェアは適応型セキュリティ アプライアンスの設定方法に応じてそのまま残るか、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 ソフトウェア自身がアンインストールするよう指示されていない場合は、ユーザ認証時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を行います。

Cisco AnyConnect VPN クライアント ソフトウェアの取得

適応型セキュリティ アプライアンスは、シスコの Web サイトから AnyConnect VPN クライアント ソフトウェアを取得します。この章では、設定ウィザードを使用して SSL VPN を設定する方法について説明します。Cisco SSL VPN ソフトウェアは、設定プロセス中にダウンロードできます。

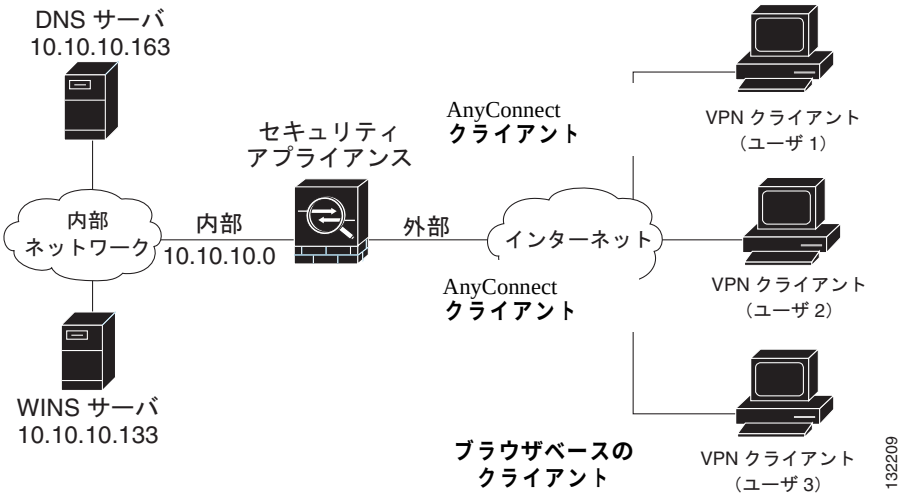
AnyConnect VPN クライアントは、ユーザが適応型セキュリティ アプライアンスからダウンロードするか、システム管理者がリモート PC に手動でインストールすることができます。このクライアント ソフトウェアを手動でインストールする方法の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

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。適応型セキュリティ アプライアンスでは、ユーザが接続を確立するたびにクライアントを自動的にプッシュするように設定するか、クライアントをダウンロードするかどうかの確認をリモート ユーザに求めるように設定することができます。後者の場合、ユーザからの応答がないときに、適応型セキュリティ アプライアンスでは、タイムアウト時間の経過後にクライアントをプッシュするように設定するか、SSL VPN ログイン画面を表示するように設定することができます。

AnyConnect SSL VPN クライアントを使用したトポロジの例

図 5-1 に、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 SSL 接続要求を受け入れ、SSL 接続を確立するように設定されている適応型セキュリティ アプライアンスを示します。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とブラウザベースのクライアントの両方への接続をサポートすることができます。

図 5-1　SSL VPN シナリオのネットワーク レイアウト



Cisco SSL VPN シナリオの実装

この項では、Cisco AnyConnect SSL VPN 接続を受け入れ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。設定内容の値の例は、図 5-1 に示した SSL VPN シナリオから使用しています。

次のトピックについて取り上げます。

必要な情報

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

- リモート ユーザが接続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の名前。
- デジタル証明書。

  ASA 5580 は、デフォルトで自己署名証明書を生成します。ただし、セキュリティを強化するために、システムを実稼働環境に設置する前に、公的に信頼されている SSL VPN 証明書を購入することもできます。
- IP プールに使用する IP アドレスの範囲。これらのアドレスは、正常に接続されると、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を作成するときに使用するユーザのリスト（認証に AAA サーバを使用している場合を除く）。
- 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 ソフトウェアがインストールされていない場合は、P.4-5 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 ASDM に直接アクセスする場合は、P.4-8 の「Web ブラウザでの 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 フィールドと Password フィールドを空のままにします。

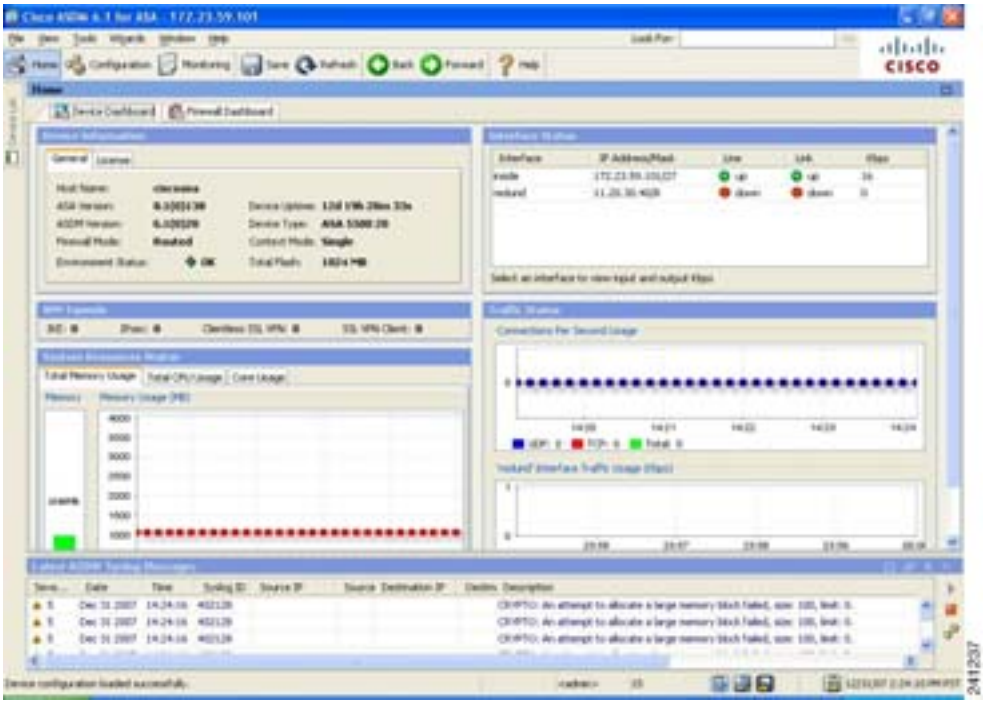
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書の受け入れを求めるセキュリティ警告が表示された場合は、**Yes** をクリックします。

ASA 5580 は最新ソフトウェアが存在するかどうかを調べ、存在する場合は自動的にダウンロードします。

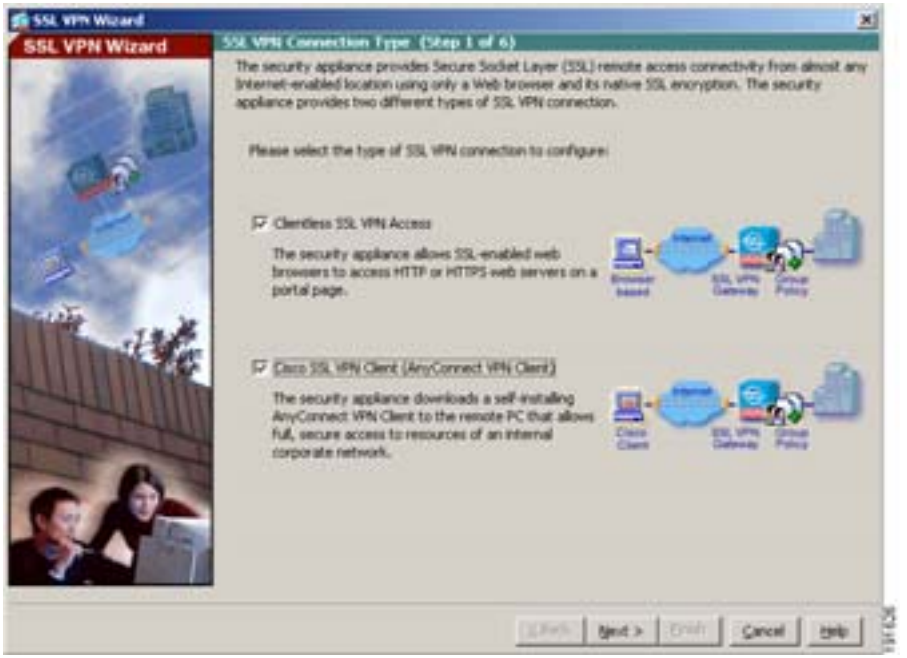
ASDM のメイン ウィンドウが表示されます。


CISCO
241237

Cisco AnyConnect VPN クライアント用の ASA 5580 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 ウィンドウで、Wizards ドロップダウン メニューから **SSL VPN Wizard** を選択します。SSL VPN Wizard 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。

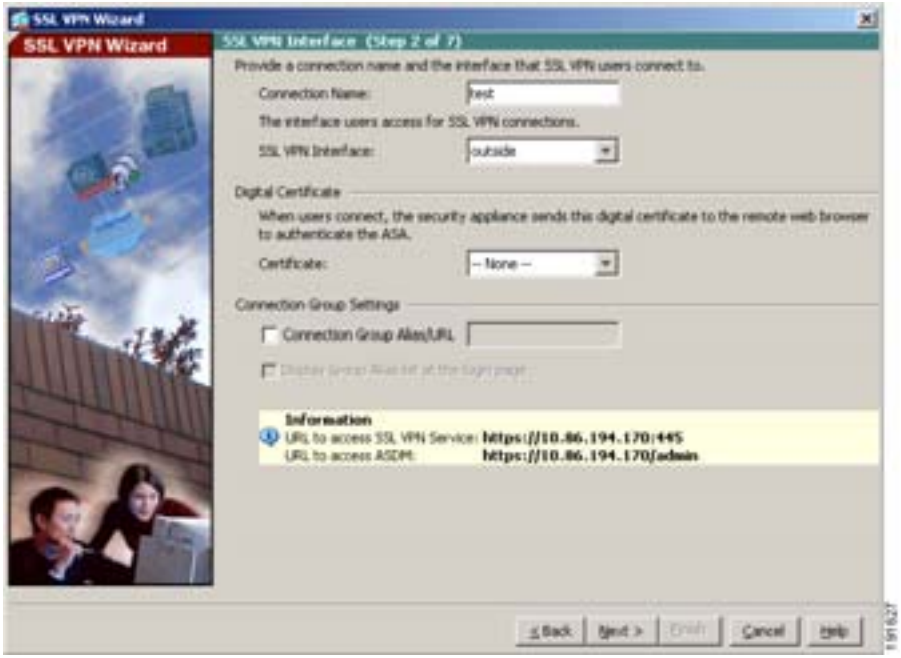
SSL VPN インターフェイスの指定

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 ユーザが接続する接続名を指定します。

ステップ 2　SSL VPN Interface ドロップダウン リストから、リモート ユーザが接続する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 リストから、ASA 5580 を認証するために ASA 5580 がリモート ユーザに送信する証明書を選択します。



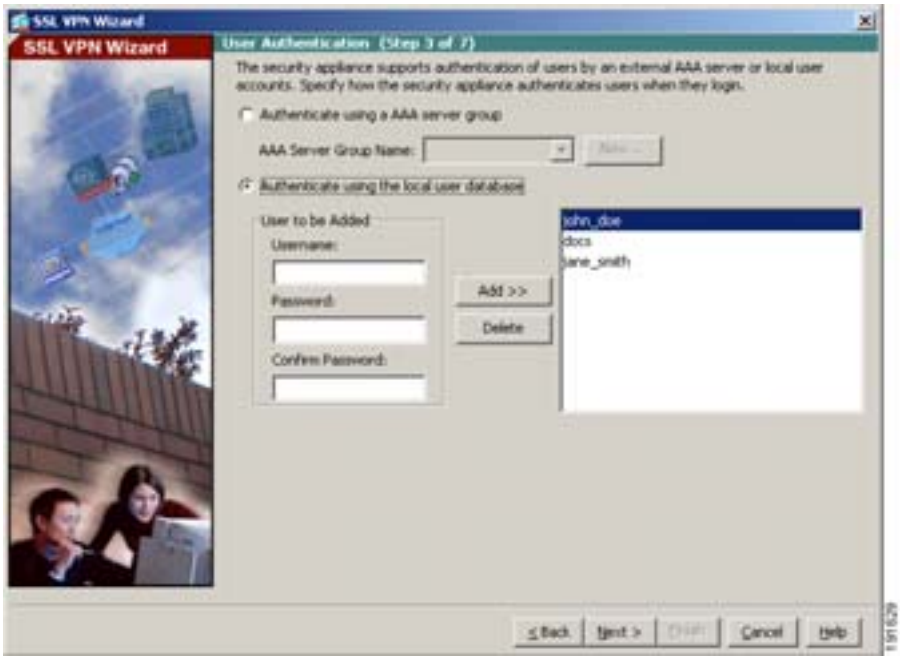
ステップ 4　**Next** をクリックして続行します。

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　AAA サーバまたはサーバ グループを認証に使用している場合、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. ドロップダウン リストから既存の AAA サーバ グループ名を選択するか、**New** をクリックして新しいサーバ グループを作成することができます。

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、次の内容を指定します。

- 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 サーバと通信するときに使用する秘密鍵

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。

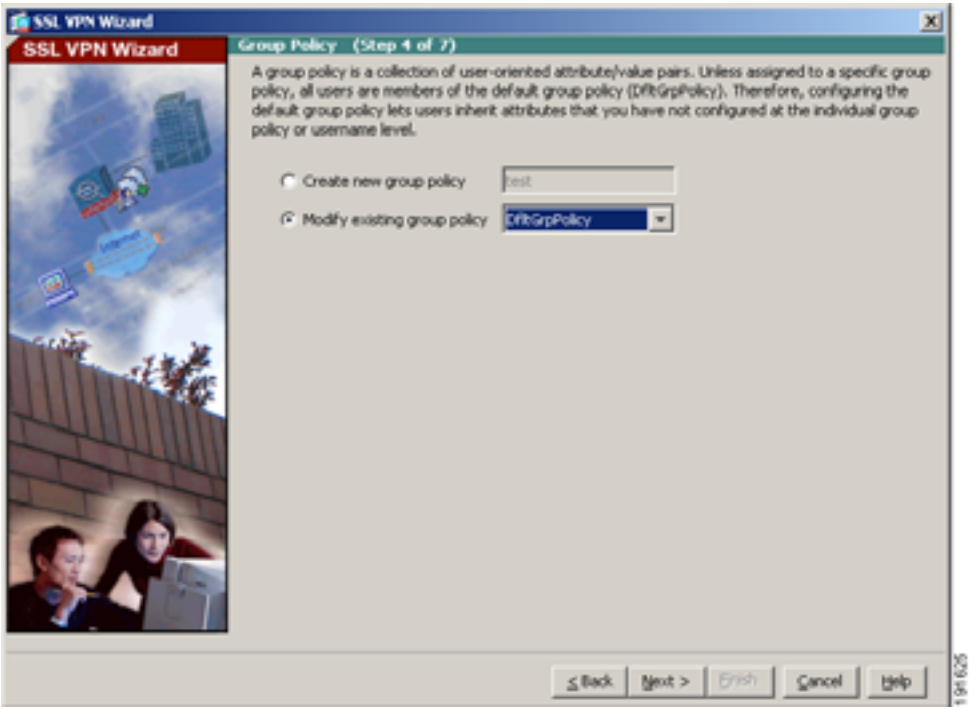
グループ ポリシーの指定

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、グループ名を指定します。

または

ステップ 2　**Modify existing group policy** オプション ボタンをクリックし、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 3　**Next** をクリックします。

ステップ 4　SSL VPN Wizard の Step 5 が表示されます。この手順は AnyConnect VPN クライアント接続には適用されないので、もう一度 **Next** をクリックします。

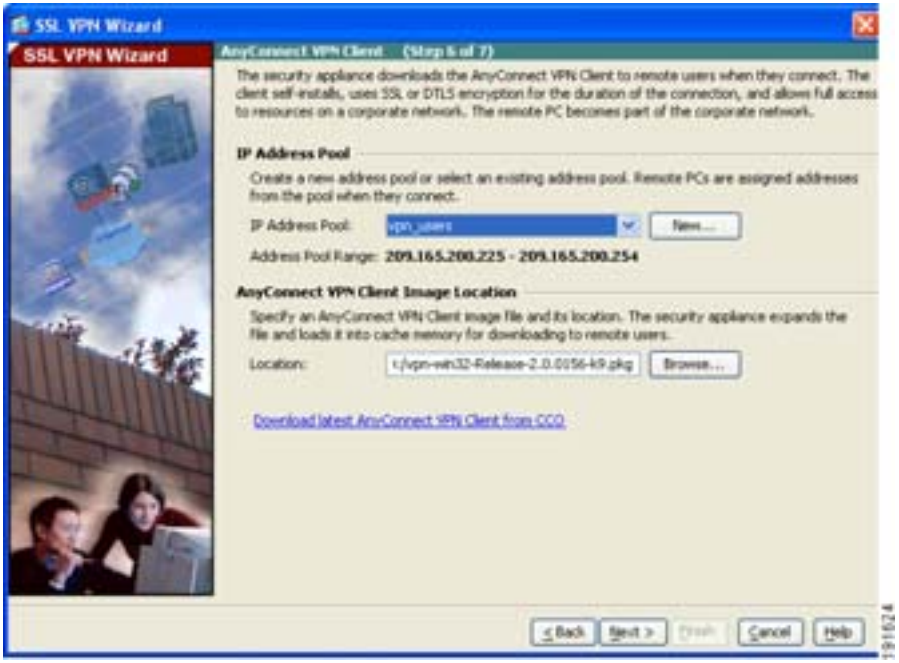
Cisco AnyConnect VPN クライアントの設定

リモート クライアントが Cisco AnyConnect VPN クライアント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。

適応型セキュリティ アプライアンスが AnyConnect ソフトウェアをユーザにプッシュできるように、AnyConnect ソフトウェアの場所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プールの名前を選択します。



ステップ 2　または、**New** をクリックして新しいアドレス プールを作成します。

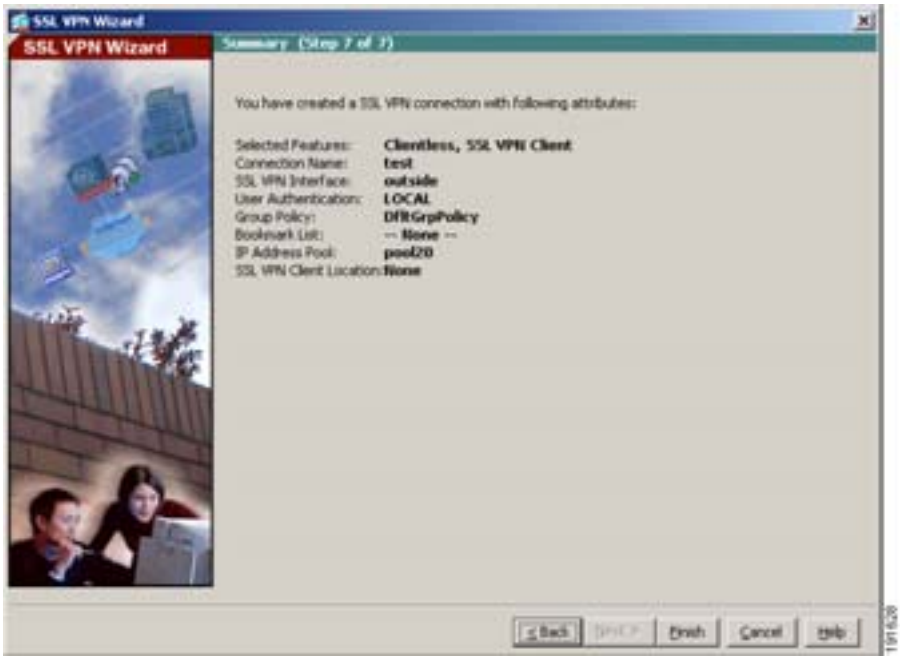
ステップ 3　AnyConnect VPN クライアント ソフトウェア イメージの場所を指定します。

このソフトウェアの最新バージョンを取得するには、Download latest AnyConnect VPN Client from CCO をクリックします。この操作を行うと、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 の設定の確認

SSL VPN Wizard の Step 7 で、設定内容が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。

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

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

次の手順

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了です。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
クライアントレス（ブラウザベース）SSL VPN の設定	第 6 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 7 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 8 章「シナリオ：IPsec リモート アクセス VPN の設定」

次の手順

CHAPTER 6

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 クライアントなしで（クライアントレス）リモート アクセス SSL VPN 接続を受け入れる方法について説明します。クライアントレス SSL VPN では、Web ブラウザを使用して、インターネットを介したセキュアな接続（トンネル）を作成できます。このため、オフサイトのユーザにソフトウェア クライアントまたはハードウェア クライアントを使用せずに、セキュアなアクセスを提供できます。

この章には、次の項があります。

クライアントレス SSL VPN について

クライアントレス SSL VPN 接続を使用すると、インターネット上のほぼすべてのコンピュータから、豊富な Web リソースと Web 対応アプリケーションにセキュアかつ簡単にアクセスできます。アクセスできるものは次のとおりです。

- 内部 Web サイト
- Web 対応アプリケーション
- NT/Active Directory および FTP ファイル共有
- POP3S、IMAP4S、SMTPS などの電子メール プロキシ
- MS Outlook Web Access
- 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）とスマート トンネル

クライアントレス SSL VPN は、Secure Sockets Layer Protocol（SSL）とその後継プロトコルである Transport Layer Security（TLSI）を使用して、中央サイトで設定するサポート対象の特定内部リソースとリモート ユーザとの間で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で処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ネットワーク管理者は、グループ単位でクライアントレス SSL VPN のユーザにリソースへのアクセス権限を付与します。

クライアントレス SSL VPN 接続のセキュリティに関する検討事項

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 対応サーバとの対話方法および証明書の検証に関して、リモート アクセス IPsec 接続とは異なります。

クライアントレス SSL VPN 接続では、適応型セキュリティ アプライアンスがエンドユーザの Web ブラウザとターゲット Web サーバとの間でプロキシとして機能します。ユーザが SSL 対応 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は、提示される証明書を受け取ることはありません。したがって、エンドユーザのブラウザでは証明書の検査および検証はできません。

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したサイトとの通信は許可されません。また、適応型セキュリティ アプライアンスでは、信頼されている CA 証明書の検証は行われません。そのため、ユーザは、SSL 対応 Web サーバと通信する前に、SSL 対応 Web サーバが提供する証明書を解析することはできません。

SSL 証明書に関するリスクを最小限に抑えるには、次の方法があります。

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で構成されるグループ ポリシーを設定し、そのグループ 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。これを実行すると、インターネット上の一般的なコンテンツへのユーザによるアクセスが制限されることがあります。その場合は、クライアントレス SSL VPN ユーザがアクセスできる内部ネットワーク上の特定ターゲットへのリンクを設定できます。
3. ユーザを教育します。SSL 対応サイトがプライベート ネットワーク内部にない場合、ユーザはクライアントレス SSL VPN 接続を介してそのサイトにアクセスすべきではありません。そのようなサイトにアクセスするには、別のブラウザ ウィンドウを開く必要があります。そのブラウザを使用して、提示された証明書を参照します。

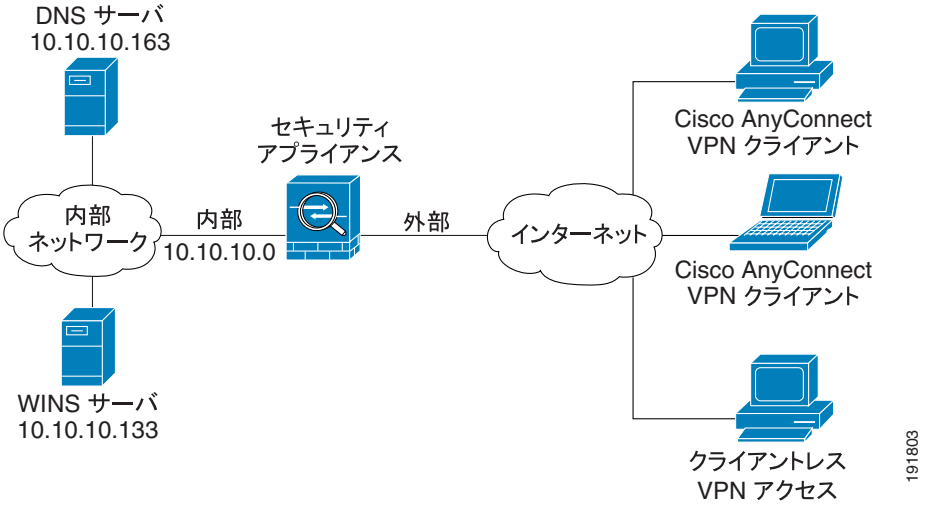
適応型セキュリティ アプライアンスは、クライアントレス SSL VPN 接続に対して、次の機能をサポートしません。

- NAT（グローバルに一意の IP アドレスの必要性を低減する機能）
- PAT（複数のアウトバウンド セッションが単一の IP アドレスから発信されているように見せることを許可する機能）

ブラウザベースの SSL VPN アクセスを使用するネットワークの例

図 6-1 に、Web ブラウザを使用してインターネット経由で SSL VPN 接続要求を受け入れるように設定されている適応型セキュリティ アプライアンスを示します。

図 6-1　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 要求を受け入れ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。設定内容の値の例は、図 6-1 に示したリモート アクセスのシナリオから使用しています。

次のトピックについて取り上げます。

必要な情報

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

- リモート ユーザが接続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 5580 は、デフォルトで自己署名証明書を生成します。セキュリティを強化し、かつブラウザの警告メッセージが表示されないようにするために、システムを実稼働環境に設置する前に、公的に信頼されている SSL VPN 証明書を購入することもできます。
- ローカル認証データベースを作成するときに使用するユーザのリスト（認証に AAA サーバを使用している場合を除く）。
- AAA サーバ グループ名（認証に AAA サーバを使用している場合）。
- 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。これは、ユーザが初めて接続を確立したときに表示されるページなので、リモート ユーザが最も頻繁に使用するターゲットを含める必要があります。

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 ソフトウェアがインストールされていない場合は、P.4-5 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 ASDM に直接アクセスする場合は、P.4-8 の「Web ブラウザでの 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 フィールドと Password フィールドを空のままにします。

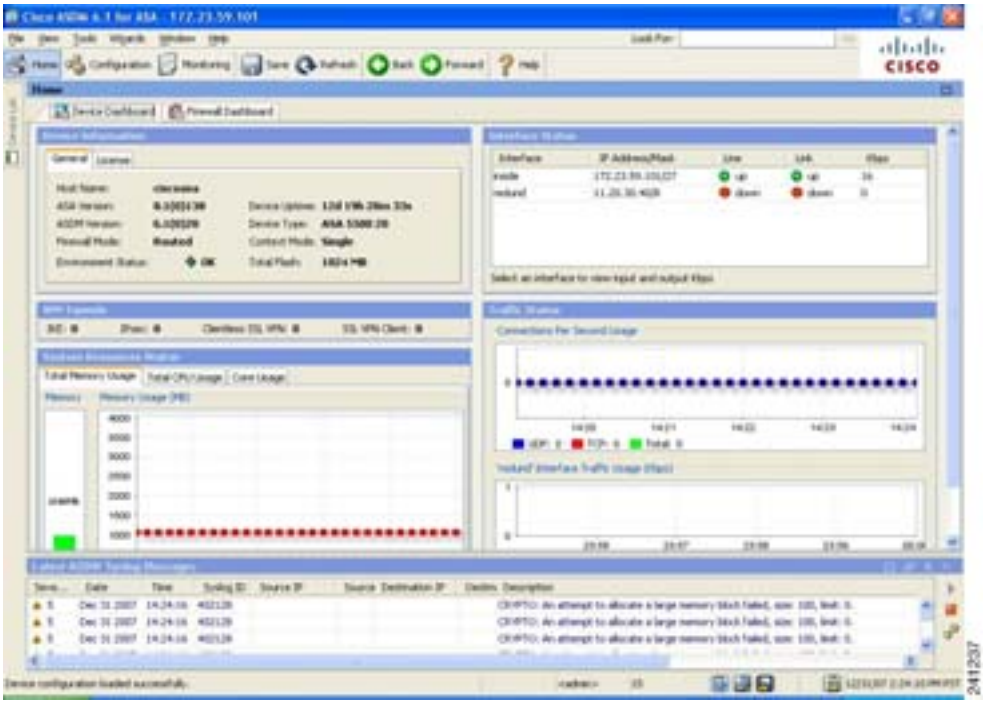
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書の受け入れを求めるセキュリティ警告が表示された場合は、**Yes** をクリックします。

ASA 5580 は最新ソフトウェアが存在するかどうかを調べ、存在する場合は自動的にダウンロードします。

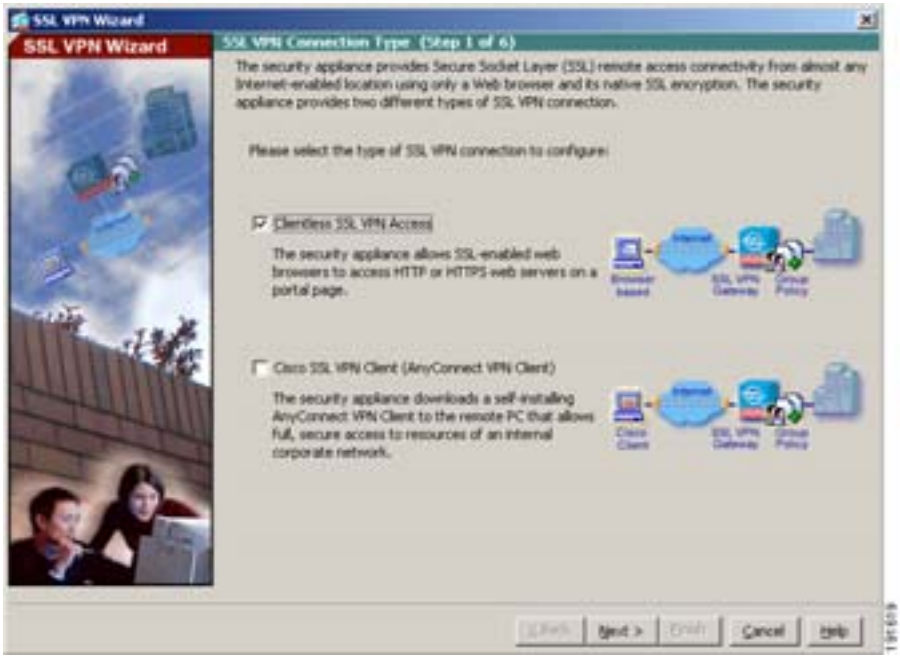
ASDM のメイン ウィンドウが表示されます。


241237

ブラウザベースの SSL VPN 接続用の ASA 5580 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 ウィンドウで、Wizards ドロップダウン メニューから **SSL VPN Wizard** を選択します。SSL VPN Wizard 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。

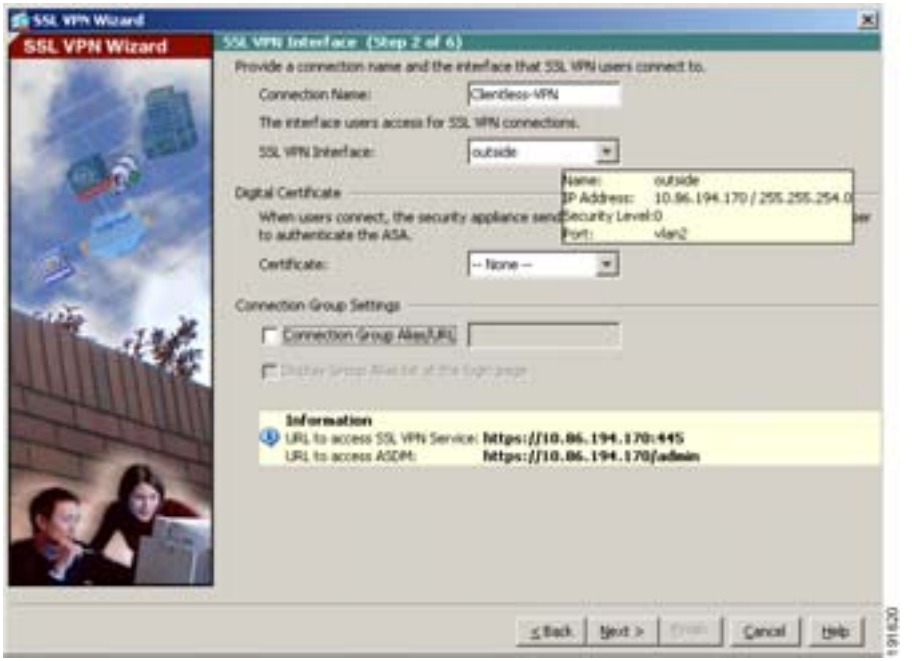
a. **Clientless SSL VPN Access** チェックボックスをオンにします。

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 ユーザが接続する接続名を指定します。



ステップ 2　SSL VPN Interface ドロップダウン リストから、リモート ユーザが接続する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 リストから、ASA 5580 を認証するために ASA 5580 がリモート ユーザに送信する証明書を選択します。

（注） ASA 5580 は、デフォルトで自己署名証明書を生成します。セキュリティを強化し、かつブラウザの警告メッセージが表示されないようにするために、システムを実稼働環境に設置する前に、公的に信頼されている SSL VPN 証明書を購入することもできます。

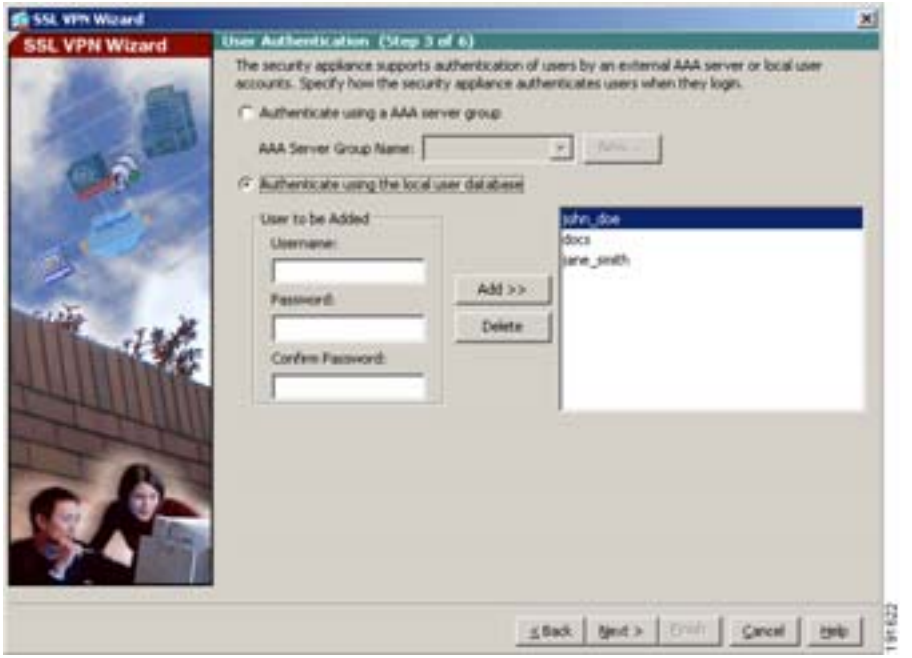
ユーザ認証方式の指定

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　AAA サーバまたはサーバ グループを認証に使用している場合、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 Server Group Name 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、**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、次の内容を指定します。

- 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 サーバと通信するときに使用する秘密鍵

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。

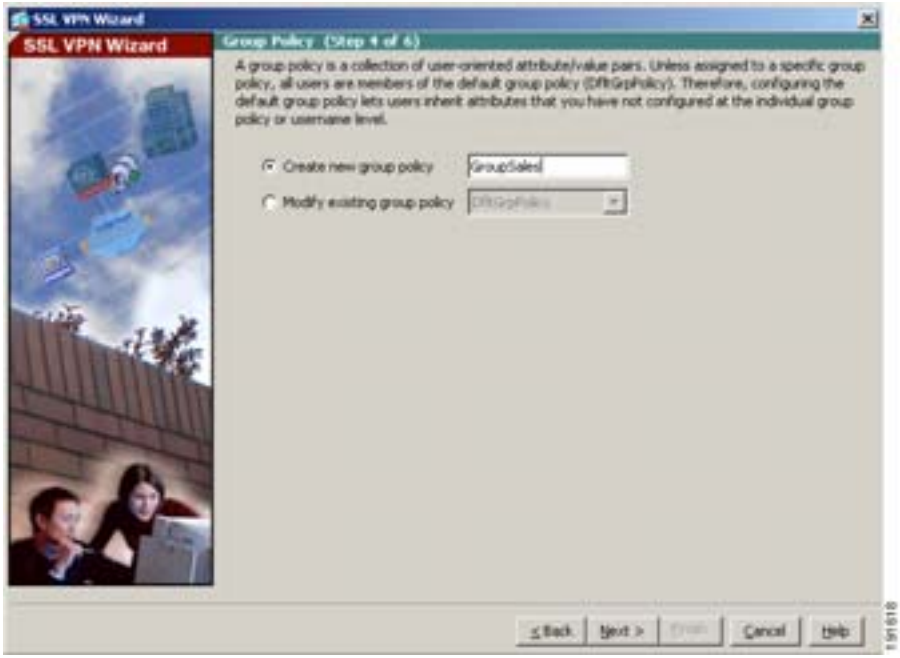
グループ ポリシーの指定

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、グループ名を指定します。

または

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



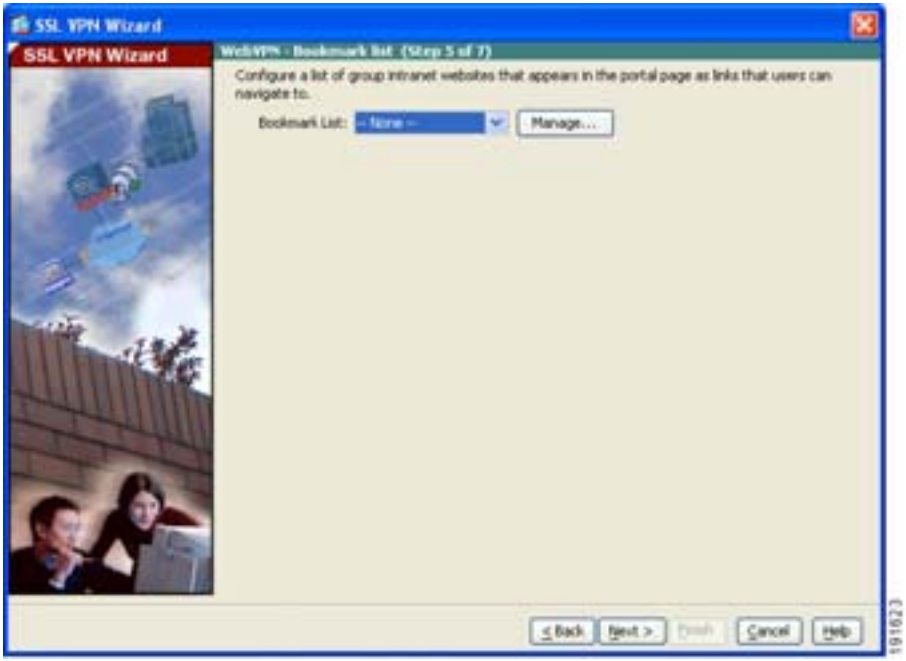
ステップ 2　**Next** をクリックします。

リモート ユーザ用のブックマーク リストの作成

ユーザが簡単にアクセスできるように URL のリストを指定して、ポータル ページ（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）を作成できます。

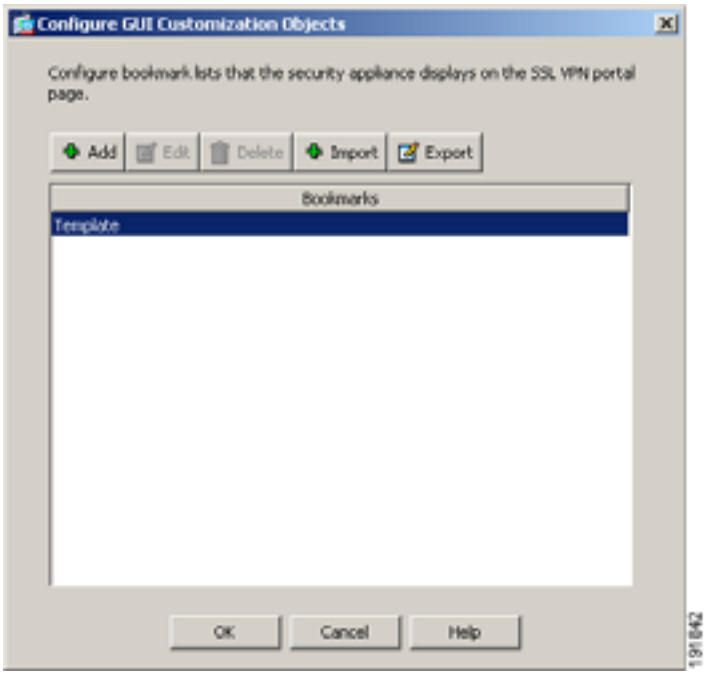
SSL VPN Wizard の Step 5 で、次の手順を実行して、VPN ポータル ページに表示する URL を指定します。

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。



新しいリストを追加するか、既存のリストを編集するには、**Manage** をクリックします。

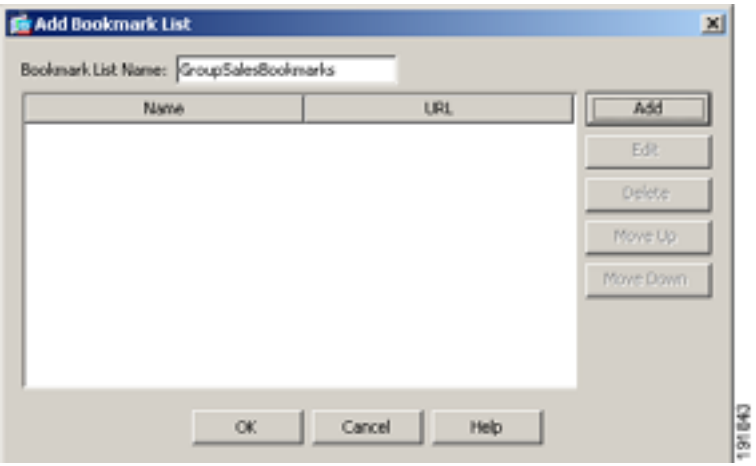
Configure GUI Customization Objects ダイアログボックスが表示されます。



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、リストを選択し、**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 フィールドで、作成するブックマーク リストの名前を指定します。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 フィールドで、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 リストから、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。

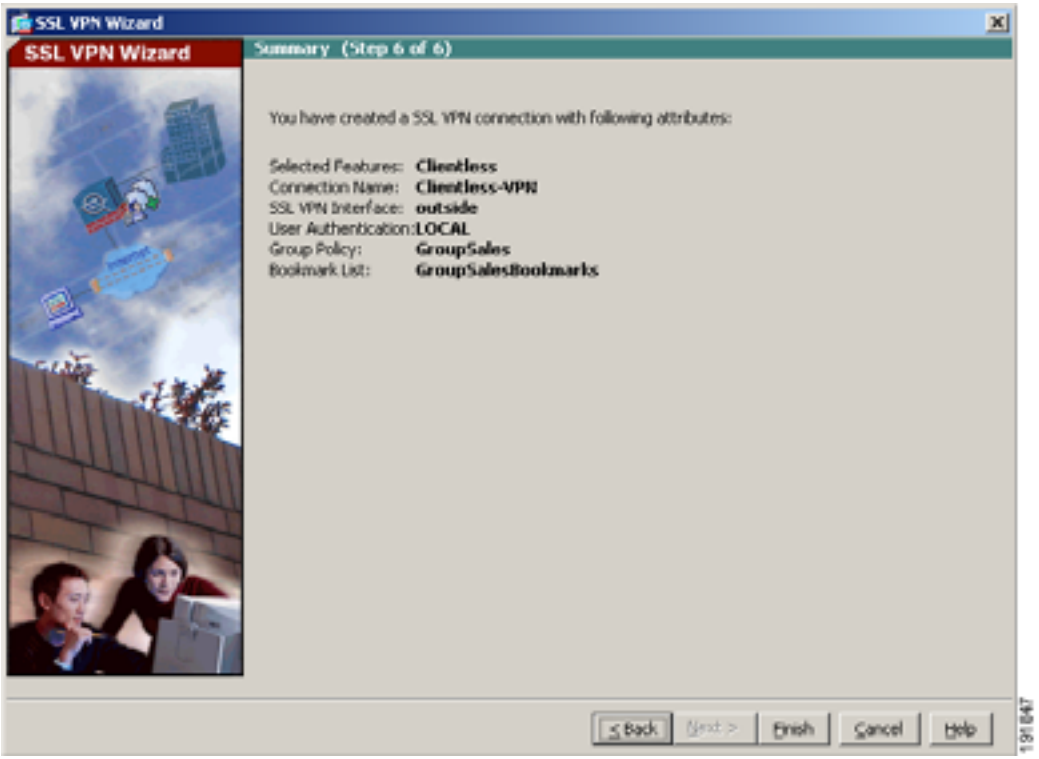
ステップ 9　ブックマーク リストの追加および編集が終了したら、**OK** をクリックして SSL VPN Wizard の Step 5 に戻ります。

ステップ 10　Bookmark List ドロップダウン リストから、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 6 で、設定内容が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。

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

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

次の手順

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了です。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
AnyConnect VPN の設定	第 5 章「シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定」
サイトツーサイト VPN の設定	第 7 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 VPN の設定	第 8 章「シナリオ：IPsec リモート アクセス VPN の設定」

CHAPTER 7

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。

この章には、次の項があります。

サイトツーサイト VPN ネットワーク トポロジの例

図 7-1 に、2 台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 7-1　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

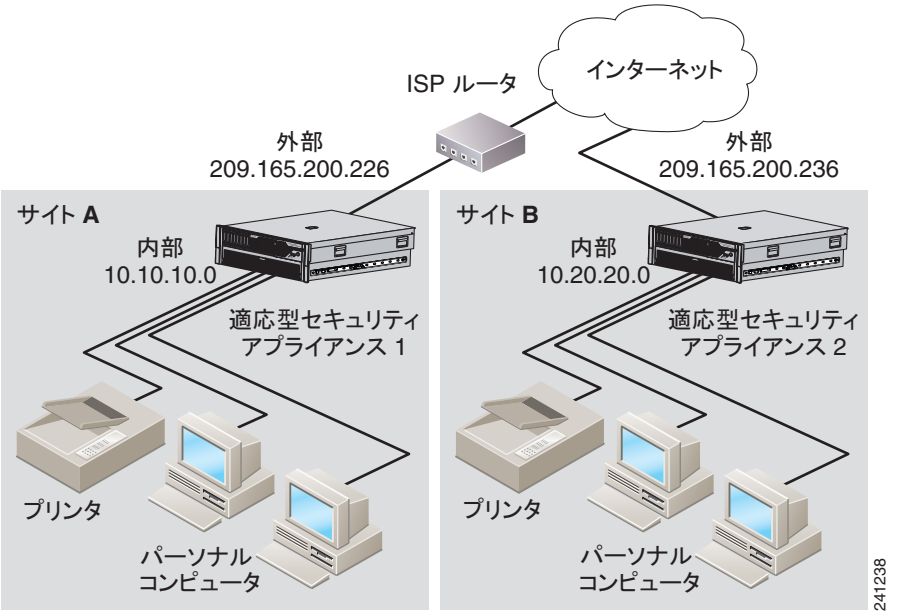


図 7-1 のような VPN サイトツーサイト配置を作成にするには、2 台の適応型セキュリティ アプライアンスを設定する必要があります（接続のそれぞれの側に 1 台ずつ）。

サイトツーサイトのシナリオの実装

この項では、図 7-1 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について説明します。

次のトピックについて取り上げます。

必要な情報

設定手順を開始する前に、次の情報を取得します。

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

サイトツーサイト VPN の設定

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

次のトピックについて取り上げます。

次の項では、各設定手順の実行方法について詳しく説明します。

ASDM の起動

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 ソフトウェアがインストールされていない場合は、P.4-5 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 ASDM に直接アクセスする場合は、P.4-8 の「Web ブラウザでの 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 フィールドと Password フィールドを空のままにします。

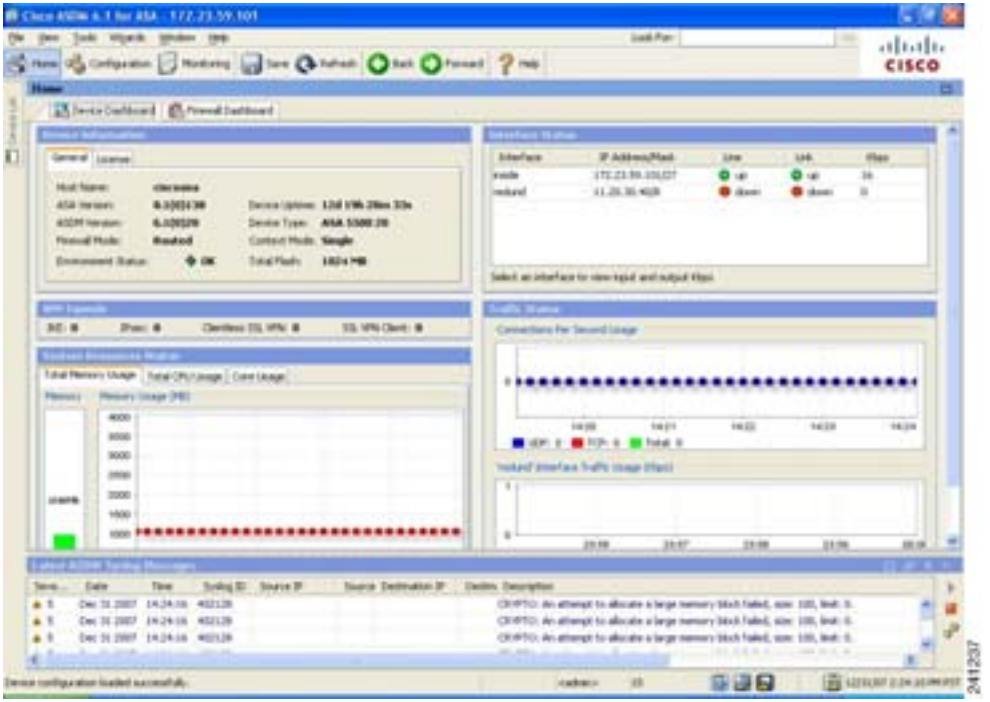
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書の受け入れを求めるセキュリティ警告が表示された場合は、**Yes** をクリックします。

ASA 5580 は最新ソフトウェアが存在するかどうかを調べ、存在す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 サイトでの適応型セキュリティ 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。

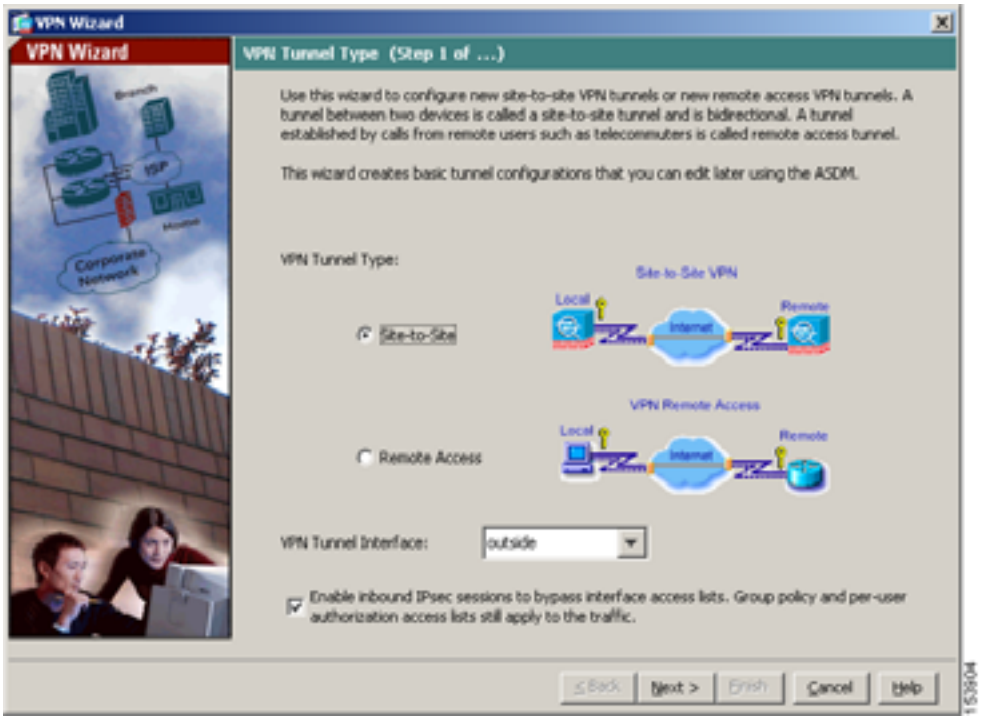
ステップ 1　ASDM のメイン ウィンドウで、Wizards ドロップダウン リストから **IPsec VPN Wizard** オプションを選択します。最初の VPN Wizard 画面が表示されます。

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 リストから、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。このシナリオでは 209.165.200.236）と、Tunnel Group Name（「Cisco」など）を入力します。

ステップ 2　次のいずれかの手順を選択して、使用する認証の種類を指定します。

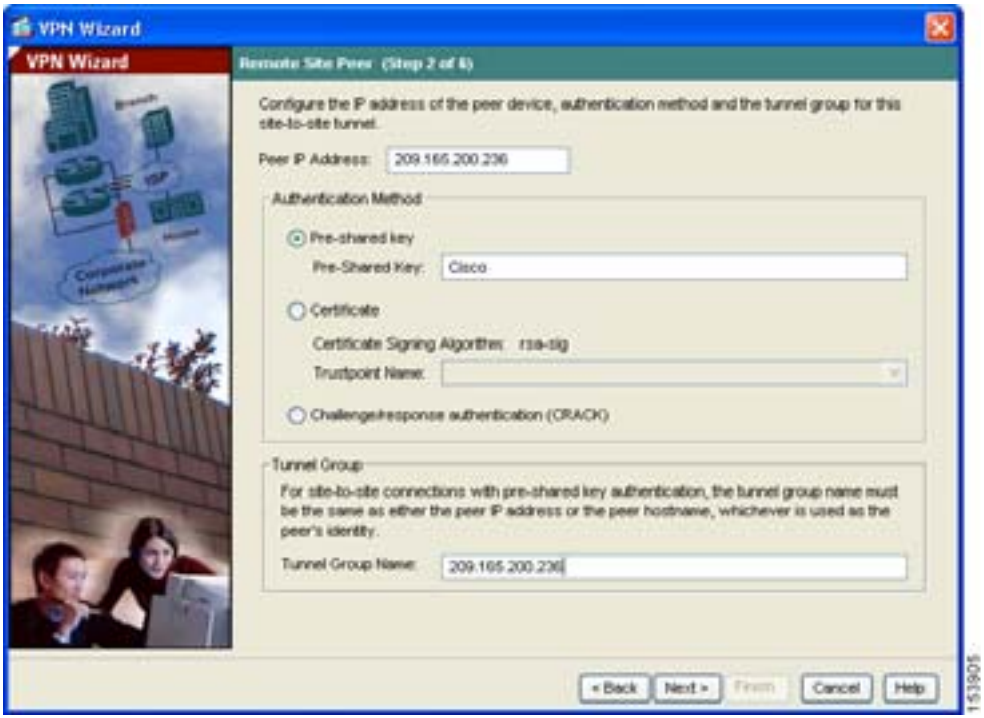
- 認証にスタティックな事前共有キーを使用するには、**Pre-Shared Key** オプション ボタンをクリックし、事前共有キー（「Cisco」など）を入力します。このキーは、適応型セキュリティ アプライアンス間の IPsec ネゴシエーションに使用されます。

  （注）　事前共有キーの認証を使用する場合、トンネル グループ名はピアの IP アドレスにする必要があります。

- 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 リストから証明書署名アルゴリズムを選択し、次に Trustpoint Name ドロップダウン リストから事前設定済みのトラストポイント名を選択します。

  デジタル証明書を認証に使用するがトラストポイント名をまだ設定していない場合は、他の 2 つのオプションのいずれかを使用して Wizard を続行できます。認証方式の設定は、標準の ASDM 画面を使用して後で変更できます。

- **Challenge/response authentication (CRACK)** オプション ボタンをクリックすると、この方法で認証されます。



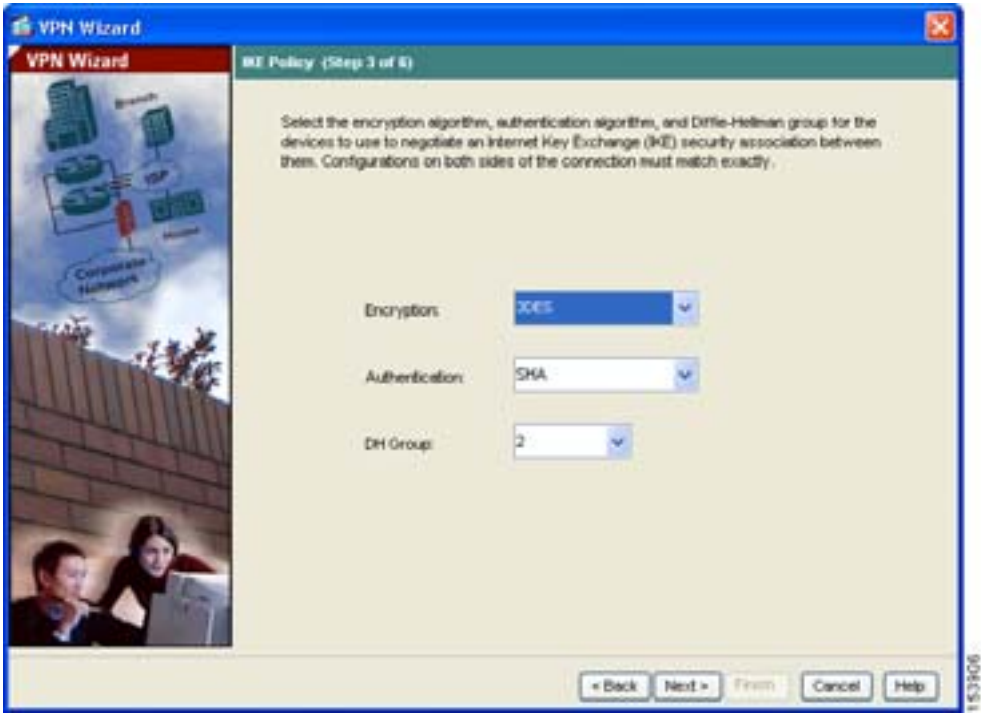
ステップ 3　**Next** をクリックして続行します。

IKE ポリシーの設定

IKE は、データを保護しプライバシーを保証する暗号化方式を含むネゴシエーション プロトコルで、ピアの ID を確認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。



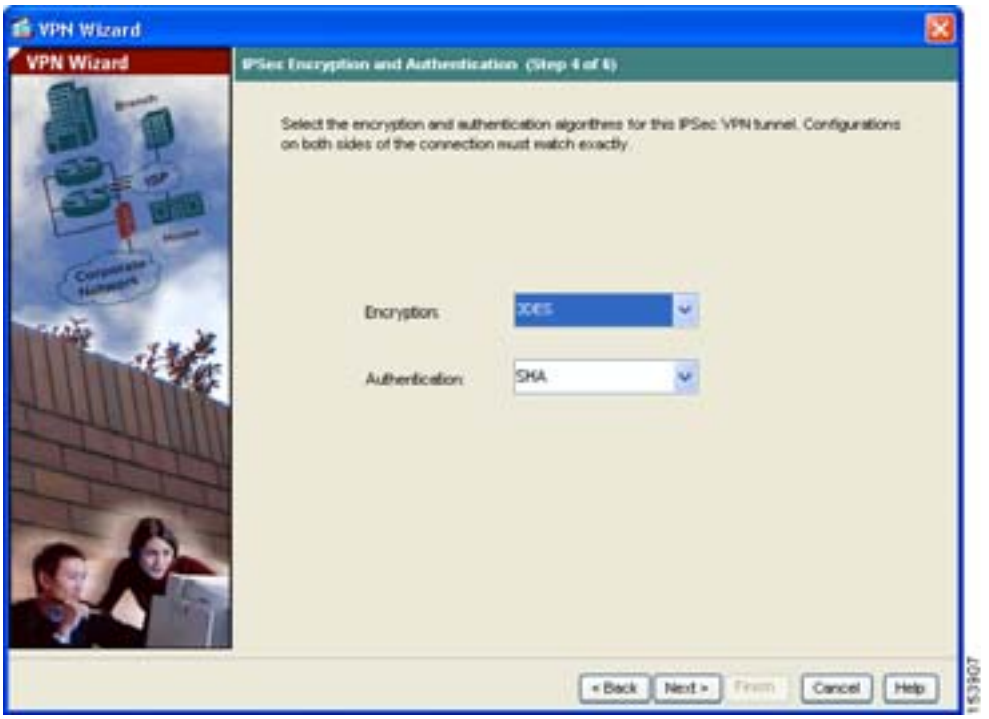
（注）　セキュリティ アプライアンス 2 を設定するときは、セキュリティ アプライアンス 1で選択した各オプションの値を正確に入力する必要があります。暗号化の不一致は、VPN トンネル障害の一般的な原因であり、設定プロセスの遅れにつながります。

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 リストから暗号化アルゴリズム（DES、3DES、または AES）を選択し、Authentication ドロップダウン リストから認証アルゴリズム（MD5 または SHA）を選択します。



ステップ 2　**Next** をクリックして続行します。

ホストおよびネットワークの指定

この IPsec トンネルを使用してトンネルの反対側の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。

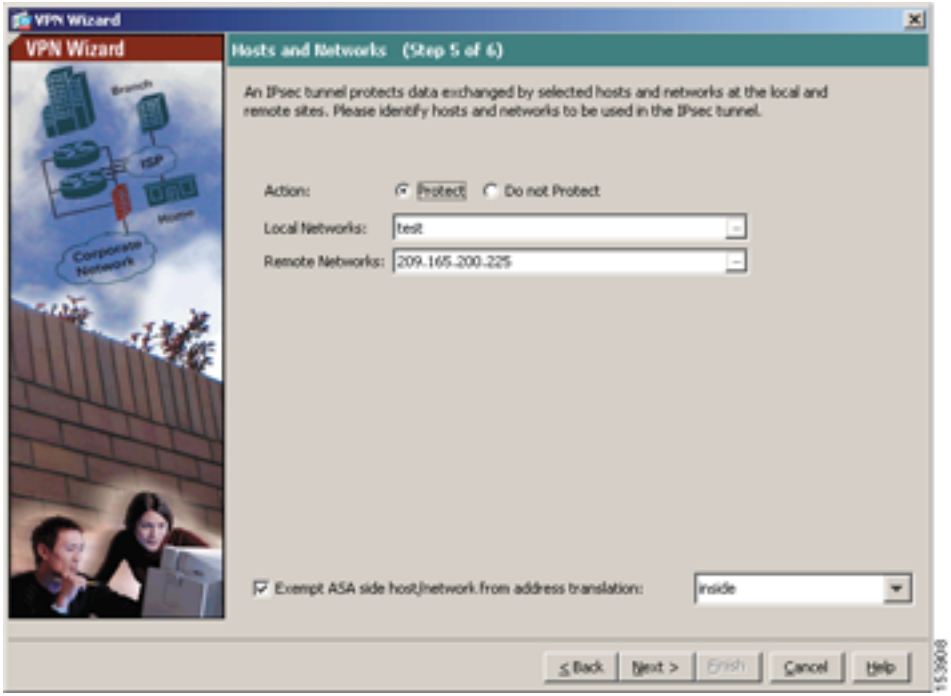
さらに、この IPsec トンネルを使用してローカル ホストおよびネットワークにアクセスできるリモート サイトのホストおよびネットワークを指定します。ホストおよびネットワークを動的に追加または削除するには、それぞれ、**Add** または **Delete** をクリックします。このシナリオでは、セキュリティ アプライアンス 1 のリモート ネットワークは Network B（10.20.20.0）なので、このネットワークからの暗号化されたトラフィックは、トンネルを使用できます。

VPN Wizard の Step 5 で、次の手順を実行します。

ステップ 1　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、または保護を解除するローカル ネットワークの IP アドレスを入力するか、省略（**...**）ボタンをクリックしてホストとネットワークのリストから選択します。

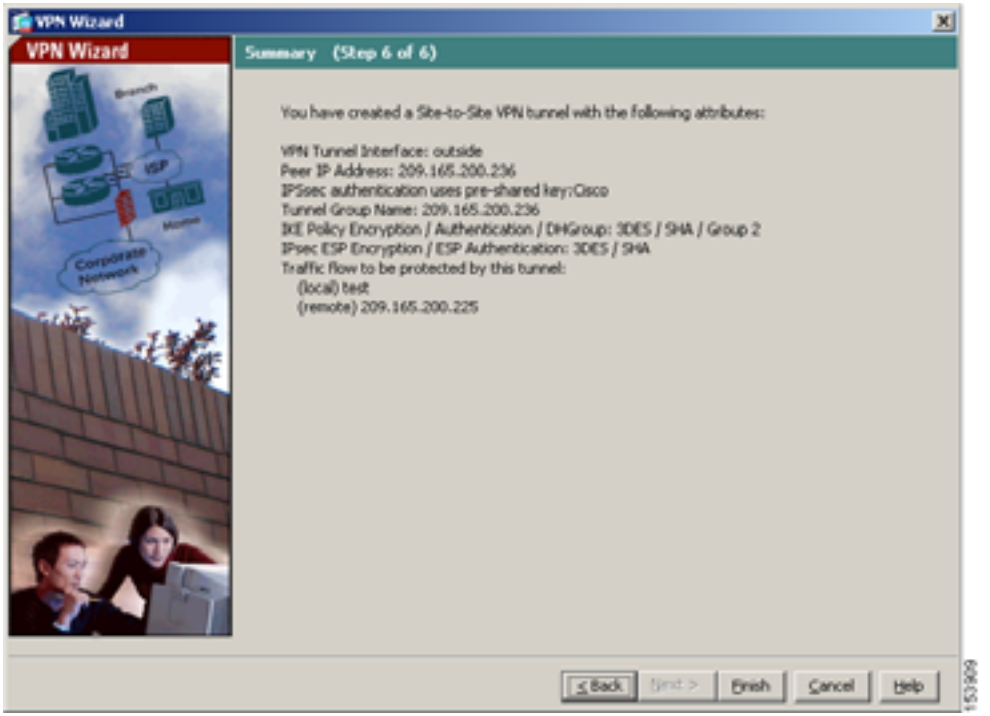
ステップ 3　保護する、または保護を解除するリモート ネットワークの IP アドレスを入力するか、省略（**...**）ボタンをクリックしてホストとネットワークのリストから選択します。



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。

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

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

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

これで、セキュリティ アプライアンス 1 の設定プロセスは終了です。

VPN 接続の反対側の設定

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

リモート サイトでは、VPN ピアとして機能するように、2 番目の適応型セキュリティ アプライアンスを設定します。ローカルな適応型セキュリティ アプライアンスの設定手順のうち、P.7-6 の「ローカル サイトでの適応型セキュリティ アプライアンスの設定」から P.7-14 の「VPN アトリビュートの確認とウィザードの完了」までを使用します。

（注） セキュリティ アプライアンス 2 を設定するときは、セキュリティ アプライアンス 1 で選択した各オプション（ローカル ホストおよびネットワークは除く）と同じ値を使用する必要があります。VPN の設定が失敗する一般的な原因は、不整合です。

次の手順

サイトツーサイト VPN 環境に適応型セキュリティ アプライアンスを配置するだけの場合は、これで初期設定は終了です。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
Cisco AnyConnect ソフトウェア クライアント用の SSL VPN の設定	第 5 章「シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定」
クライアントレス（ブラウザ ベース）SSL VPN の設定	第 6 章「シナリオ：SSL VPN クライアントレス接続」
リモート アクセス VPN の設定	第 8 章「シナリオ：IPsec リモート アクセス VPN の設定」

CHAPTER 8

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

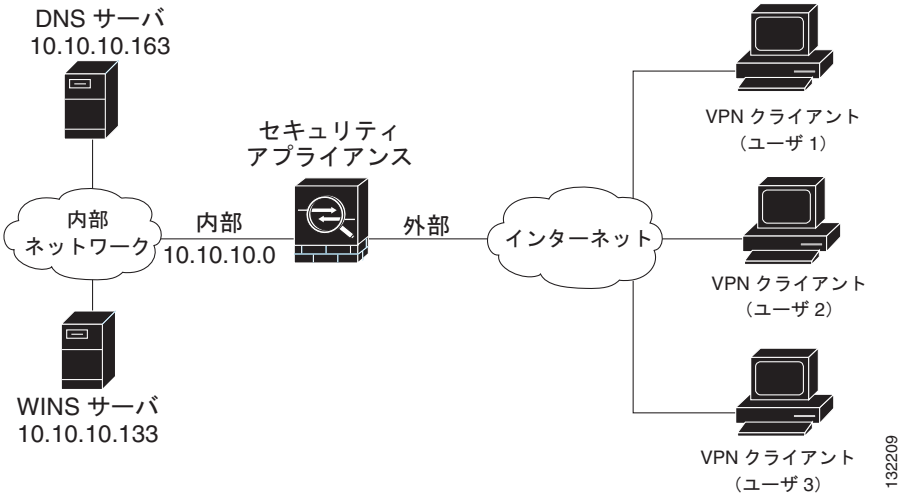
Easy VPN ソリューションを実装している場合は、この章で Easy VPN サーバ（ヘッドエンド デバイスと呼ばれる場合もあります）の設定方法を参照できます。

この章には、次の項があります。

IPsec リモート アクセス VPN ネットワーク トポロジの例

図 8-1 に、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）からの要求を受け入れ、IPsec 接続を確立するように設定されている適応型セキュリティ アプライアンスを示します。

図 8-1　リモート アクセス VPN のシナリオのネットワーク レイアウト



IPsec リモート アクセス VPN のシナリオの実装

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

設定内容の値の例は、図 8-1 に示したリモート アクセスのシナリオから使用しています。

次のトピックについて取り上げます。

必要な情報

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

- IP プールに使用する IP アドレスの範囲。これらのアドレスは、接続に成功したときにリモート VPN クライアントに割り当てられます。
- ローカル認証データベースを作成するときに使用するユーザのリスト（認証に AAA サーバを使用している場合を除く）。

- VPN との接続時にリモート クライアントで使用する次のネットワーキング情報。
  - プライマリおよびセカンダリ DNS サーバの IP アドレス
  - プライマリおよびセカンダリ WINS サーバの IP アドレス
  - デフォルト ドメイン名
  - 認証されたリモート　クライアントにアクセスできるようにするローカル ホスト、グループ、およびネットワークの IP アドレスのリスト

ASDM の起動

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 ソフトウェアがインストールされていない場合は、P.4-8 の「Web ブラウザでの 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 ASDM に直接アクセスする場合は、P.4-8 の「Web ブラウザでの 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 フィールドと Password フィールドを空のままにします。

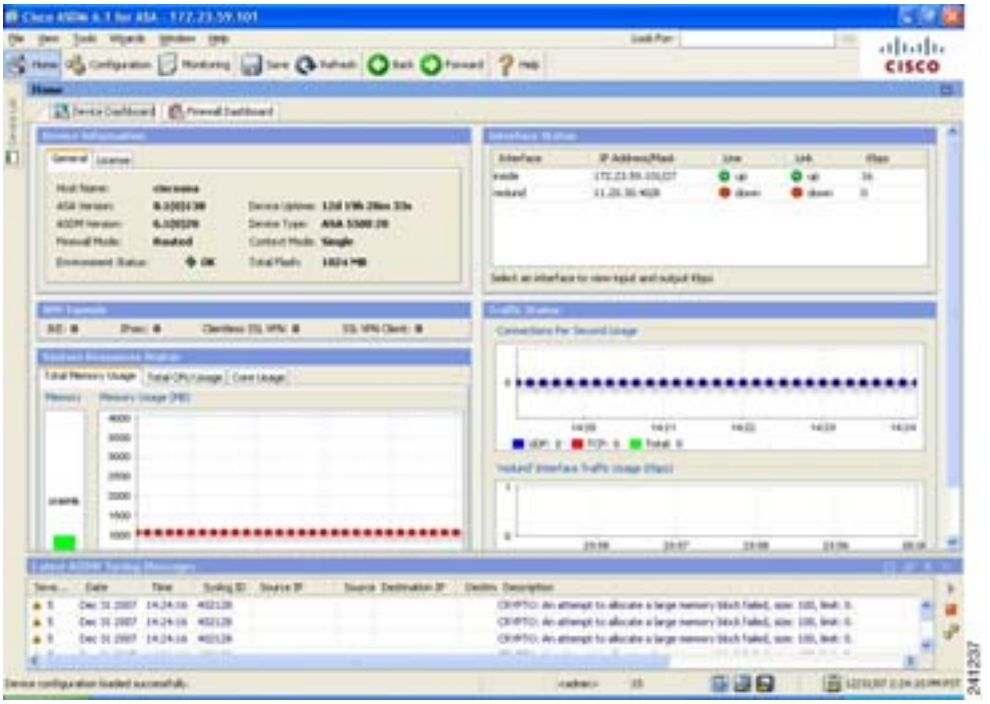
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

ステップ 4　**OK** をクリックします。

ステップ 5　証明書の受け入れを求めるセキュリティ警告が表示された場合は、**Yes** をクリックします。

適応型セキュリティ アプライアンスは最新ソフトウェアが存在するかどうかを調べ、存在する場合は自動的にダウンロードします。

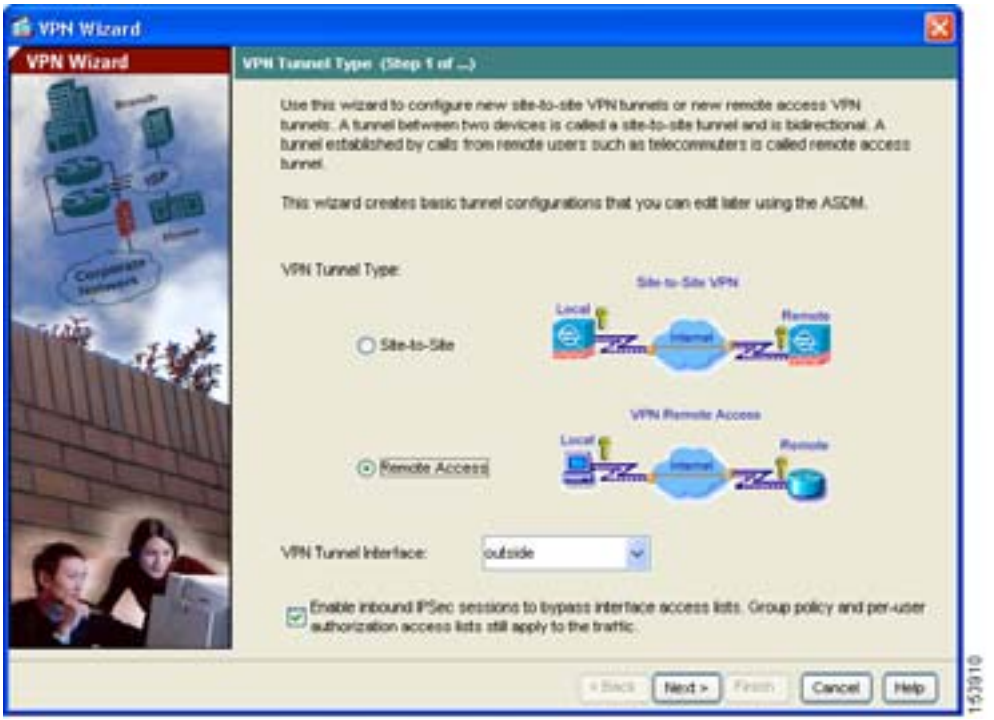
ASDM のメイン ウィンドウが表示されます。



IPSec リモート アクセス VPN 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 ウィンドウで、Wizards ドロップダウン メニューから **IPsec VPN Wizard** を選択します。VPN Wizard 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 リストから、着信 VPN トンネルに対してイネーブルにするインターフェイスとして **outside** を選択します。

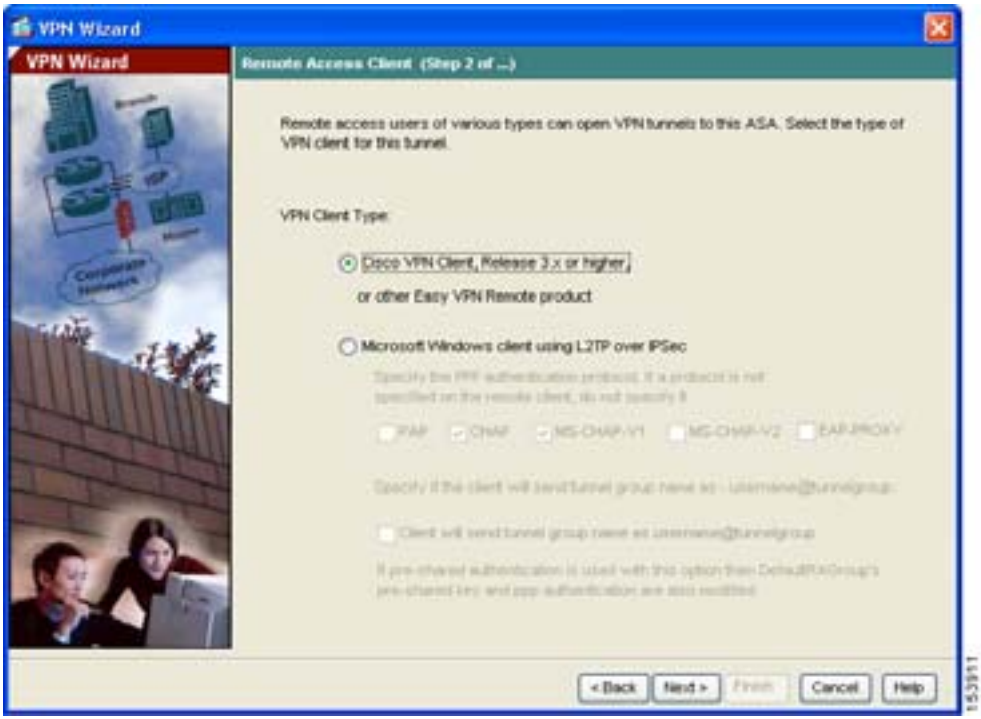
c. **Next** をクリックして続行します。

VPN クライアントの種類の選択

VPN Wizard の Step 2 で、次の手順を実行します。

ステップ 1　リモート ユーザをこの適応型セキュリティ アプライアンスに接続できるようにする VPN クライアントの種類を指定します。このシナリオでは、**Cisco VPN Client** オプション ボタンをクリックします。

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



ステップ 2　**Next** をクリックして続行します。

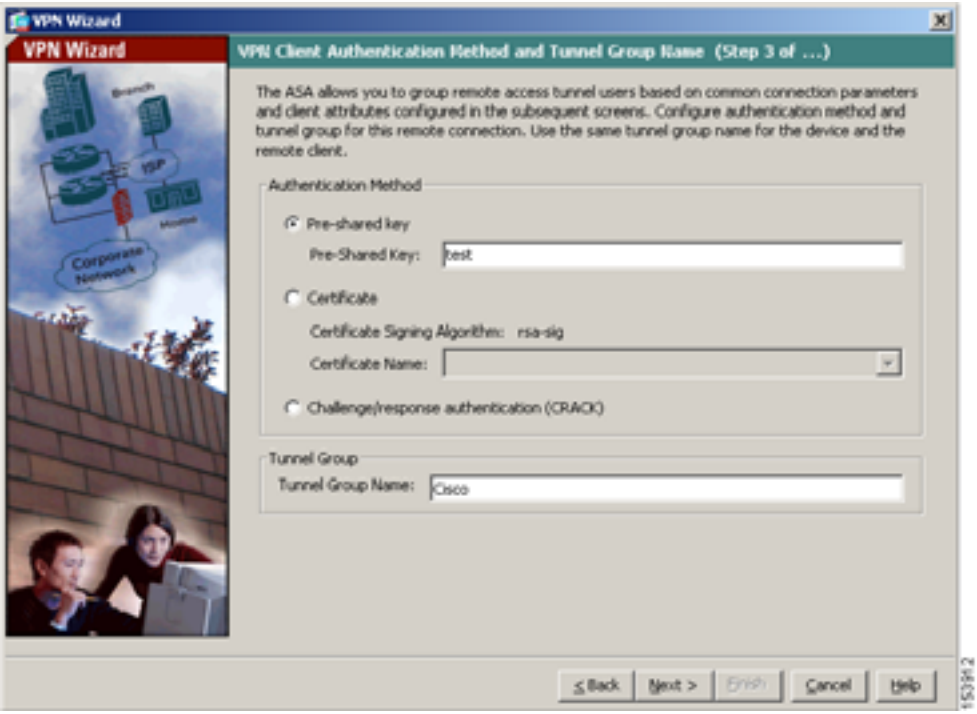
VPN トンネル グループ名と認証方式の指定

VPN Wizard の Step 3 で、次の手順を実行します。

ステップ 1　次のいずれかの手順を実行して、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されます。
- 認証にデジタル証明書を使用するには、**Certificate** オプション ボタンをクリックし、ドロップダウン リストから Certificate Signing Algorithm を選択し、次のドロップダウン リストから事前設定済みのトラスト ポイント名を選択します。

  デジタル証明書を認証に使用するがトラストポイント名をまだ設定していない場合は、他の 2 つのオプションのいずれかを使用して Wizard を続行できます。認証方式の設定は、標準の ASDM ウィンドウを使用して後で変更できます。
- **Challenge/response authentication (CRACK)** オプション ボタンをクリックすると、この方法で認証されます。



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

ステップ 3　**Next** をクリックして続行します。

ユーザ認証方式の指定

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

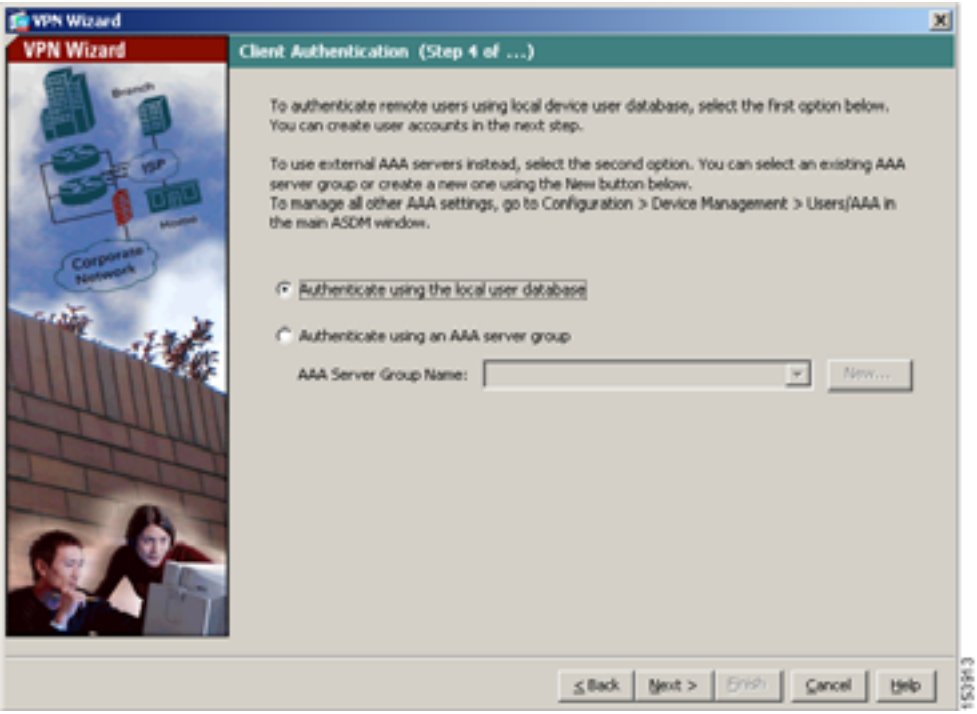
VPN Wizard の Step 4 で、次の手順を実行します。

ステップ 1　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. AAA Server Group Name 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、**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。



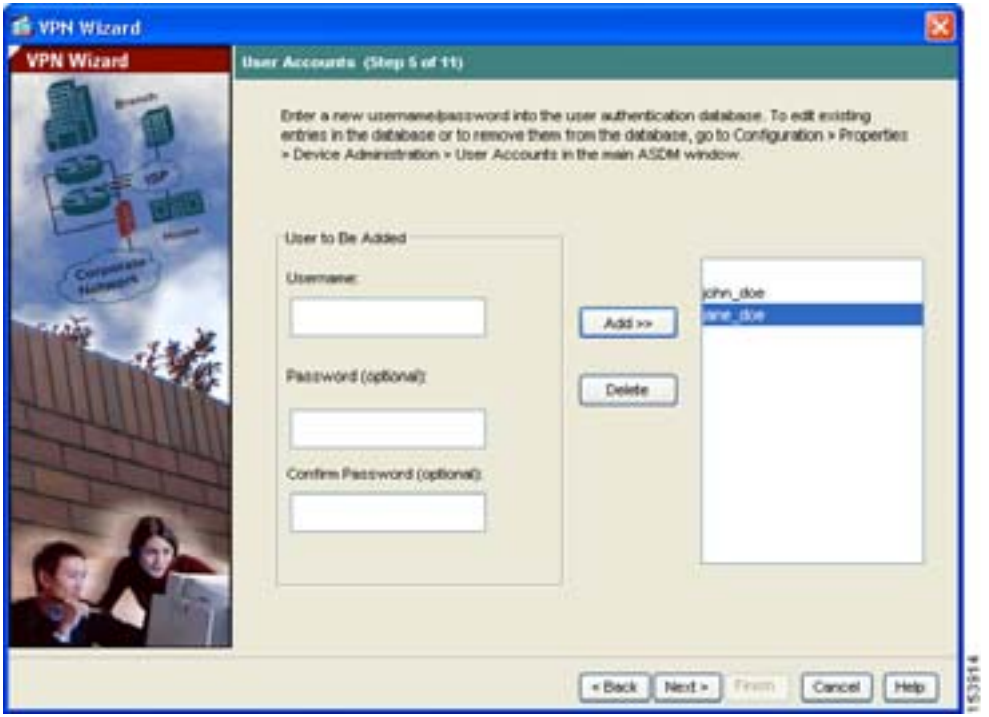
ステップ 3　**Next** をクリックして続行します。

ユーザ アカウントの設定（オプション）

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

VPN Wizard の Step 5 で、次の手順を実行します。

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



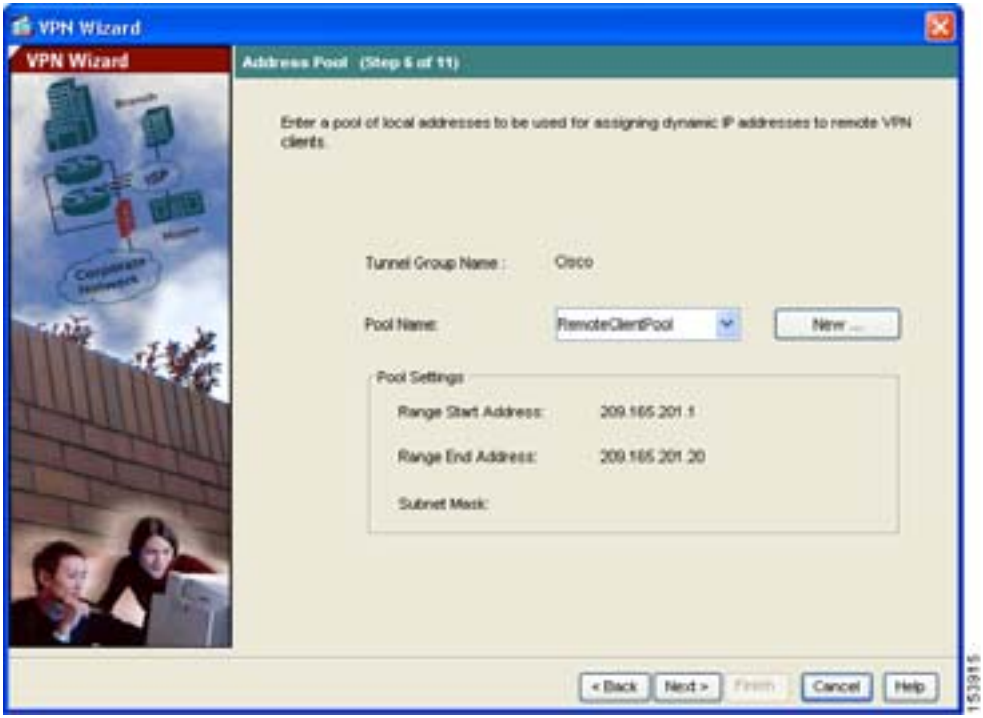
ステップ 2　新しいユーザの追加が終了したら、**Next** をクリックして続行します。

アドレス プールの設定

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

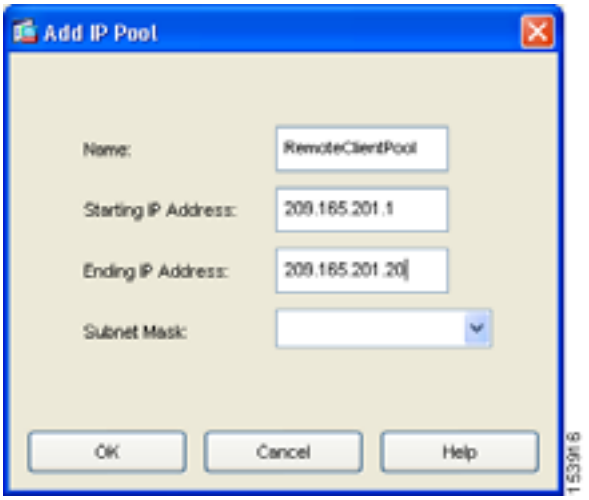
VPN Wizard の Step 6 で、次の手順を実行します。

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



または、**New** をクリックして新しいアドレス プールを作成します。

Add IP Pool ダイアログボックスが表示されます。



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

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

b. （オプション）サブネット マスクを入力するか、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。

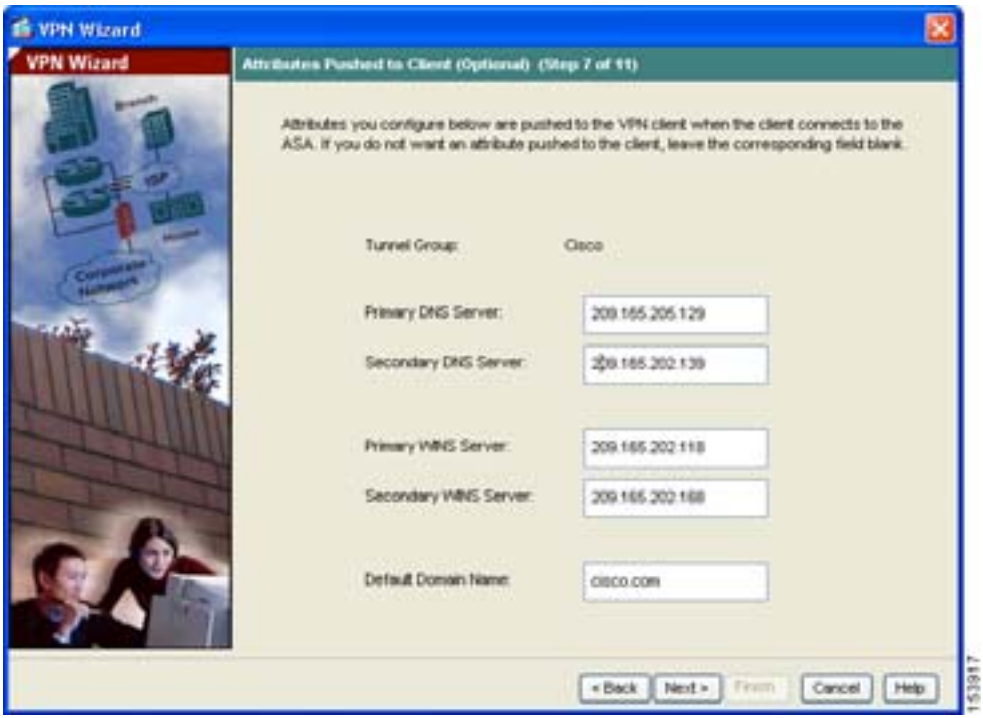
クライアント アトリビュートの設定

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。



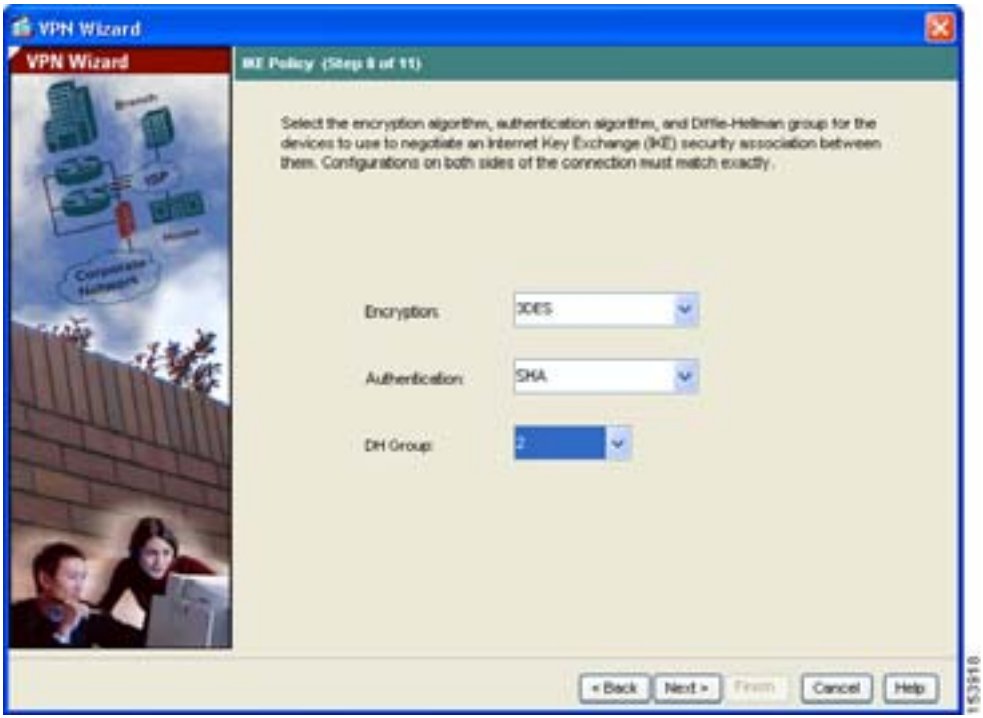
ステップ 2　**Next** をクリックして続行します。

IKE ポリシーの設定

IKE は、データを保護しプライバシーを保証する暗号化方式を含むネゴシエーション プロトコルで、ピアの ID を確認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、セキュアな VPN トンネルを確立できます。

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

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

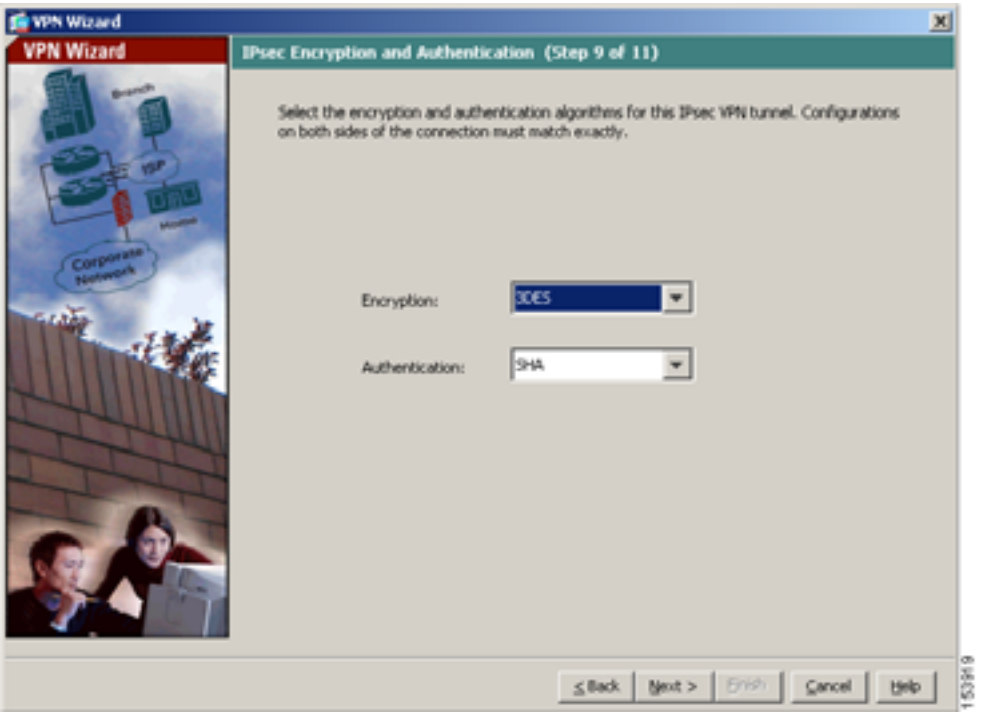


ステップ 2　**Next** をクリックして続行します。

IPSec 暗号化および認証パラメータの設定

VPN Wizard の Step 9 で、次の手順を実行します。

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



ステップ 2　**Next** をクリックして続行します。

アドレス変換の例外とスプリット トンネリングの指定

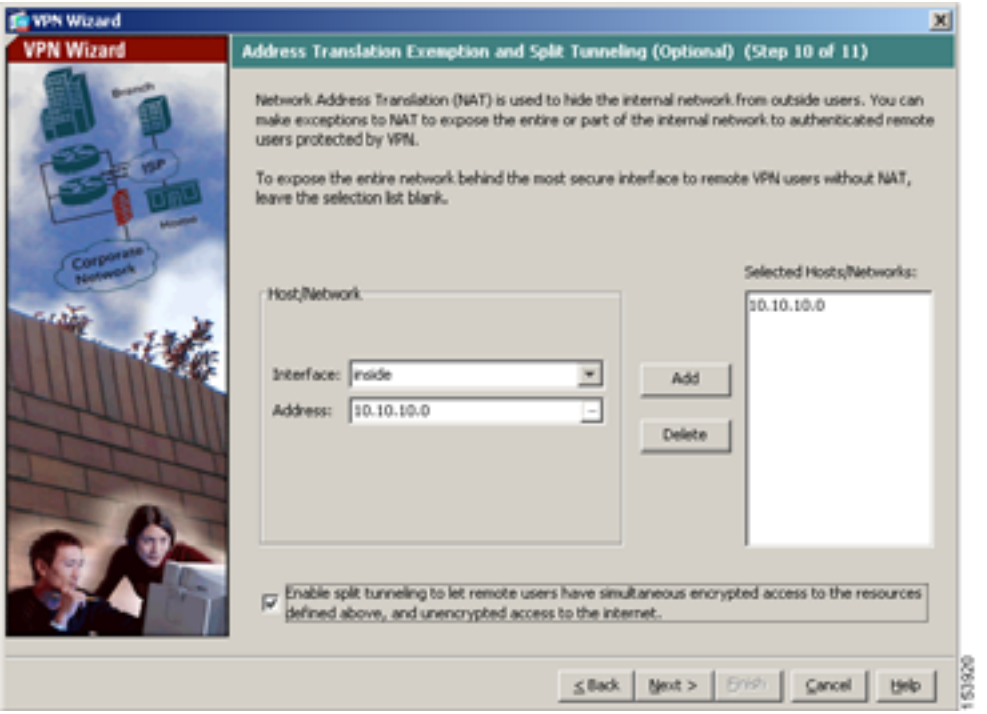
スプリット トンネリングを使用すると、リモート アクセス IPsec クライアントは、IPsec トンネル経由での暗号化形式のパケット、またはネットワーク インターフェイスへのテキスト形式のパケットを、条件付きで送信できます。

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 ユーザのアクセスを可能にする必要があるローカル ホストおよびネットワークを特定して、このネットワーク保護の例外を作成できます。

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。

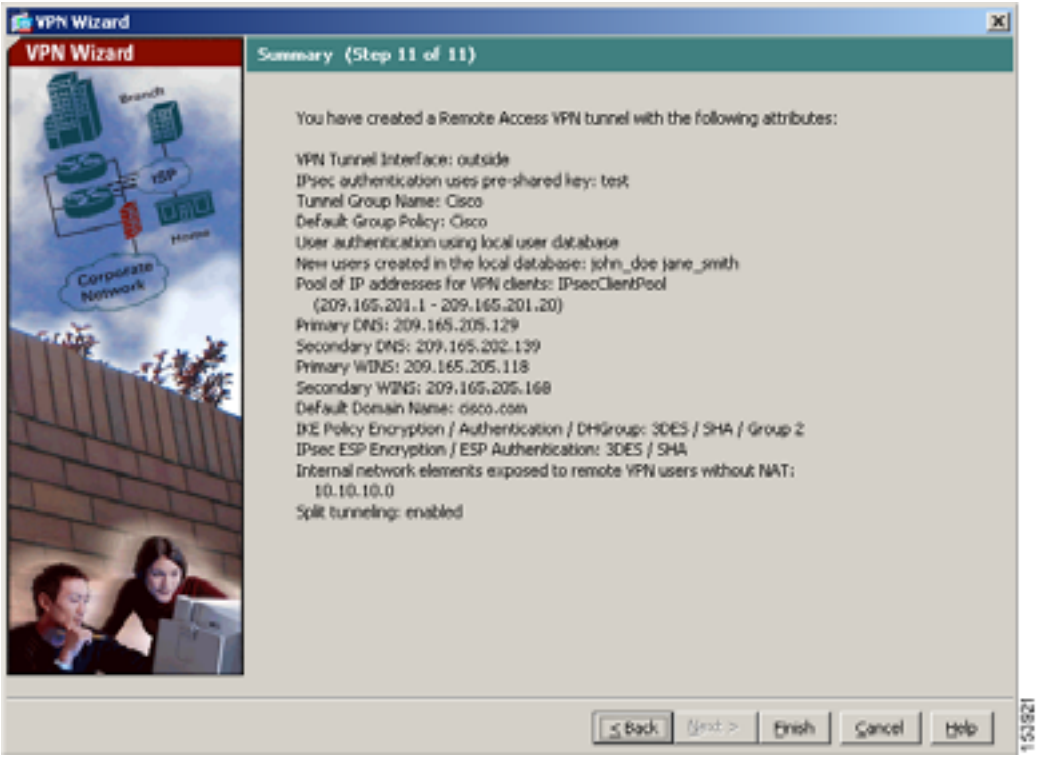


（注） 画面の下部にある **Enable split tunneling** チェックボックスをオンにして、スプリット トンネリングをイネーブルにします。スプリット トンネリングを使用すると、設定したネットワークの外部のトラフィックを、暗号化された VPN トンネルを使用せずに直接インターネットに送出できるようになります。

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 の設定の確認

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。

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

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

次の手順

エンドツーエンドの暗号化された VPN トンネル（外勤社員や在宅勤務者向けにセキュアな接続を提供）を確立するには、Cisco VPN クライアント ソフトウェアを取得します。

シスコシステムズの VPN クライアントの詳細については、http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html を参照してください。

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了です。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
Cisco AnyConnect ソフトウェア クライアント用の SSL VPN の設定	第 5 章「シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定」
クライアントレス（ブラウザ ベース）SSL VPN の設定	第 5 章「シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定」
サイトツーサイト VPN の設定	第 7 章「シナリオ：サイトツーサイト VPN の設定」

APPENDIX **A**

3DES/AES ライセンスの取得

Cisco ASA 5580 には、暗号化を提供する DES ライセンスが付属しています。暗号化技術を提供する 3DES/AES ライセンスを取得して、セキュア リモート管理（SSH、ASDM など）、サイトツーサイト VPN、リモート アクセス VPN などの特定の機能をイネーブルにすることができます。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 3DES または AES 暗号化ライセンスを取得するには、次の Web サイトを参照してください。

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

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

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

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

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

アクティベーション キーの例やソフトウェアのアップグレードに関する詳細については、『*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# activation-key` *`activation-5-tuple-key`*	*activation-5-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 つの要素からなる 16 進文字列です。各要素は 1 つのスペースで区切られます。たとえば、0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e 0x1234abcd のようになります。「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。 **（注）** 設定をリロードする必要があるのは、ライセンスされた機能をダウングレードする場合だけです。

INDEX

こ

せ

て

ら

れ