Cisco ASA 5505 クイック スタート ガイド

ソフトウェア バージョン 7. 2

Customer Order Number: DOC-J-7817612=
Text Part Number: 78-17612-02-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 5505 クイック スタート ガイド

CONTENTS

CHAPTER 1

始める前に

適応型セキュリティ アプライアンスの実装に必要な設置および設定の手順を確認するには、次の表を使用してください。

実行内容	参照先
ASA 5505 の典型的な構成について	第 2 章「構成のプランニング」
ASA 5505 の VLAN およびポート割り当てについて	第 3 章「VLAN 構成のプランニング」
シャーシの取り付け	第 4 章「ASA 5505 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 5 章「適応型セキュリティ アプライアンスの設定」
各実装内容に応じた適応型セキュリティ アプライアンスの設定	第 6 章「シナリオ：DMZ 設定」
	第 7 章「シナリオ：IPSec リモートアクセス VPN 設定」
	第 8 章「シナリオ：サイトツーサイト VPN 設定」
	第 9 章「シナリオ：Easy VPN ハードウェア クライアント設定」

実行内容	参照先
詳細な設定 オプション機能および拡張機能の設定	『*Cisco Security Appliance Command Line Configuration Guide*』
	『*Cisco Security Appliance Command Reference*』
	『*Cisco Security Appliance Logging Configuration and System Log Messages*』

CHAPTER 2

構成のプランニング

このマニュアルは、ASA 5505 の典型的なカスタマー構成を表す、いくつかのシナリオ例に基づいています。 この章の構成シナリオは、後続の設定の章に対応しています。

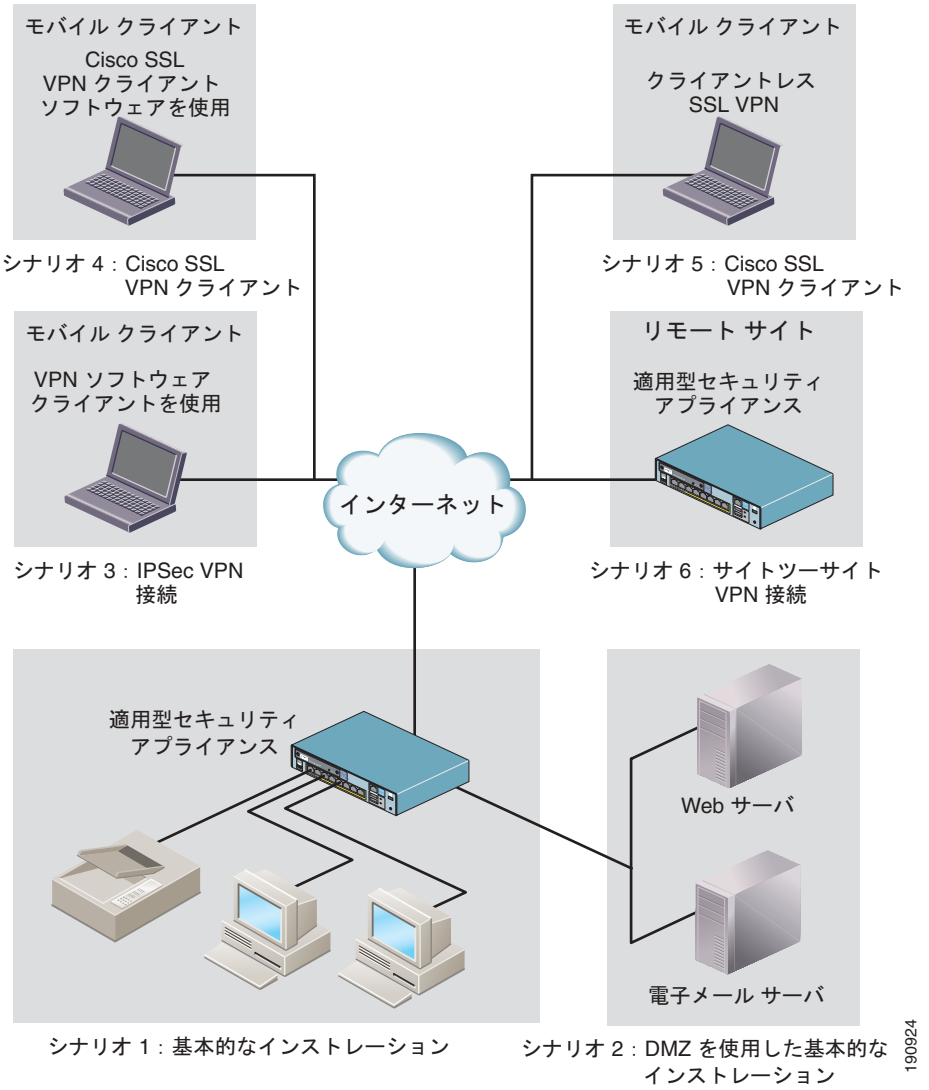
この章には、次の項があります。

構成のプランニングと設定のシナリオ

適応型セキュリティ アプライアンスの拡張構成には、この章で説明する 2 つ以上の異なる構成シナリオを含めることができます。この章の構成シナリオを使用して、ネットワーク上の適応型セキュリティ アプライアンスを構成する方法を決定し、該当する設定の章を判別することができます。

図 2-1 に、このマニュアルに記載されているほとんどの構成シナリオと設定シナリオが含まれる拡張ネットワーク構成を示します。

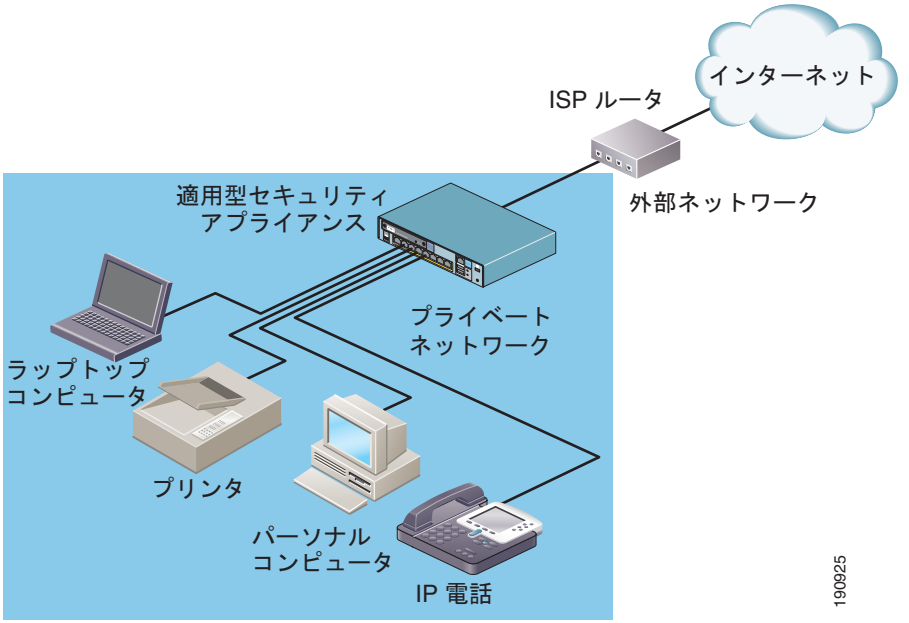
図 2-1　拡張ネットワーク構成



シナリオ 1：外部接続を使用したプライベート ネットワーク

図 2-2 に、小規模なプライベート ネットワークで一般的な基本構成を示します。

図 2-2　外部接続を使用したプライベート（内部）ネットワーク



この例では、適応型セキュリティ アプライアンスを使用することにより、プライベート ネットワーク上のすべてのデバイスが互いに通信を行い、プライベート ネットワーク上のユーザがインターネット上のデバイスと通信を行うことができます。

（注） この構成は PIX 501 を使用するセキュリティ構成に類似しています。 ファイアウォールの背後にあるデバイスが内部および外部で通信できる PIX 501 セキュリティ アプライアンスを使用したセキュリティ構成をすでに使用している場合は、同じ構成をそのまま使用し、PIX 501 デバイスを ASA 5505 デバイスに交換できます。

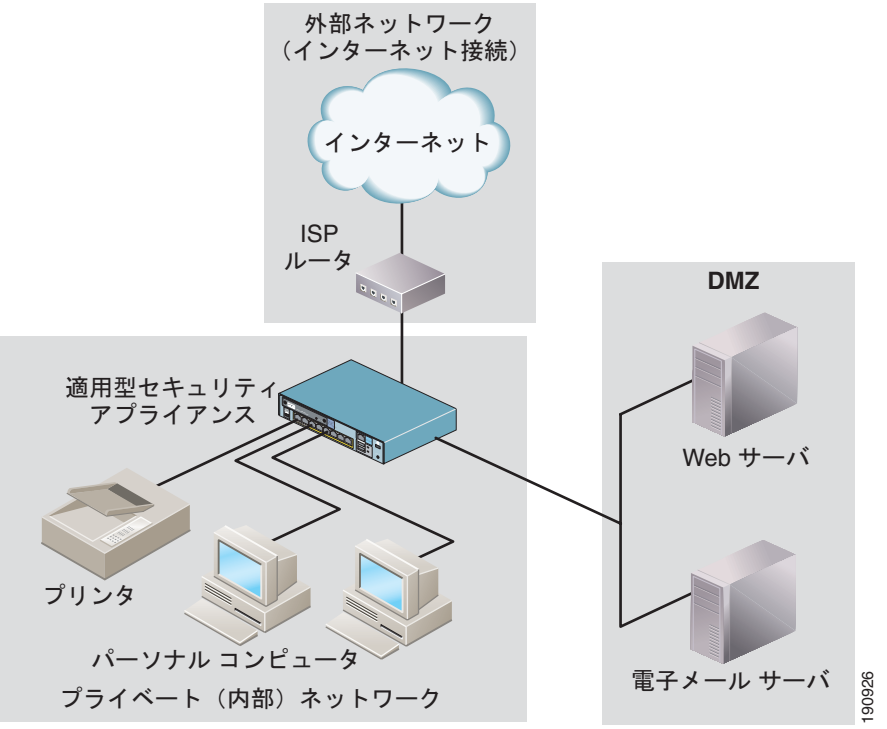
適応型セキュリティ アプライアンスをこの構成用に設定する方法の詳細については、第 5 章「適応型セキュリティ アプライアンスの設定」を参照してください。

シナリオ 2：DMZ を使用した基本的なインストレーション

このシナリオでは、適応型セキュリティ アプライアンスを使用して、内部ネットワークに加えて Demilitarized Zone（DMZ; 非武装地帯）にあるネットワーク リソースを保護します。DMZ は、プライベート（内部）ネットワークとパブリック（外部）ネットワークとの間の中立帯に位置する別個のネットワークです。

プライベート ネットワーク上の HTTP クライアントは、DMZ 内の Web サーバにアクセスでき、インターネット上のデバイスとも通信できます。

図 2-3　DMZ を使用したプライベート ネットワーク

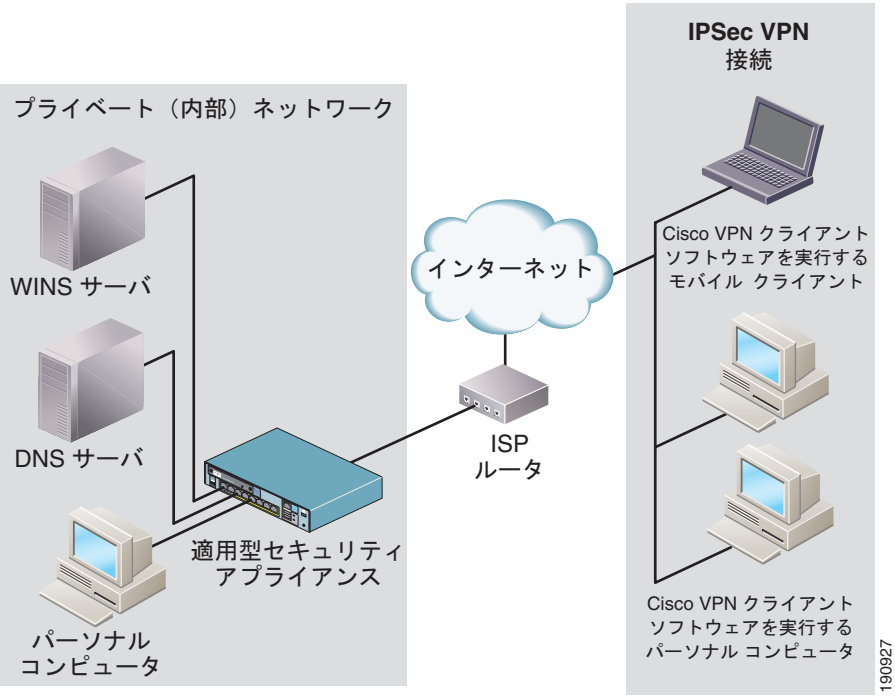


DMZ 構成の設定方法の詳細については、第 6 章「シナリオ：DMZ 設定」を参照してください。

シナリオ 3：IPSec リモートアクセス VPN

このシナリオでは、リモートアクセス IPSec VPN 接続を受け入れるよう、適応型セキュリティ アプライアンスを設定します。リモートアクセス VPN を使用すると、インターネットを越えてセキュアな接続（トンネル）を作成でき、オフサイトのユーザにセキュアなアクセスを提供できます。

図 2-4　IPSec リモートアクセス VPN 接続



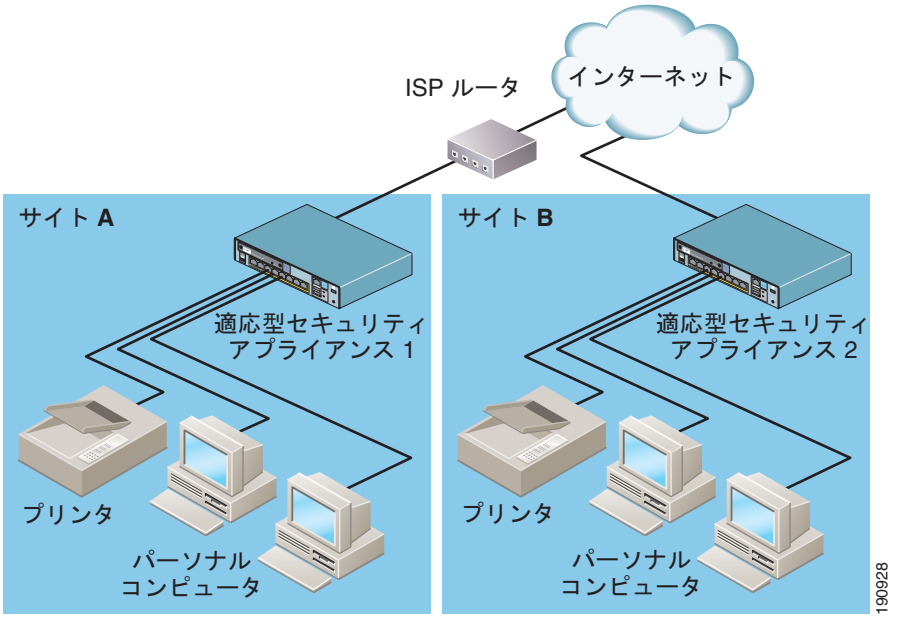
IPSec リモートアクセス VPN 構成の設定方法の詳細については、第 7 章「シナリオ：IPSec リモートアクセス VPN 設定」を参照してください。

シナリオ 4：サイトツーサイト VPN

このシナリオでは、2 つの適応型セキュリティ アプライアンスを設定して、サイトツーサイト VPN を作成します。

サイトツーサイト VPN を構成すると、企業はネットワーク セキュリティを維持したまま、ネットワークを拡張してビジネス パートナーや世界中のリモート オフィスとの間で低コストのパブリック インターネット接続を実現できます。VPN 接続では、セキュアな接続、つまりトンネル経由で 1 つの場所から別の場所へデータを送信できます。これは、まず接続の両端を認証し、次に 2 つのサイト間で送信されるすべてのデータを自動的に暗号化することによって可能になります。

図 2-5　サイトツーサイト VPN 設定シナリオのネットワーク レイアウト



サイトツーサイト VPN 構成の設定方法の詳細については、第 8 章「シナリオ：サイトツーサイト VPN 設定」を参照してください。

シナリオ 5：ハードウェア VPN クライアントとして構成された ASA 5505

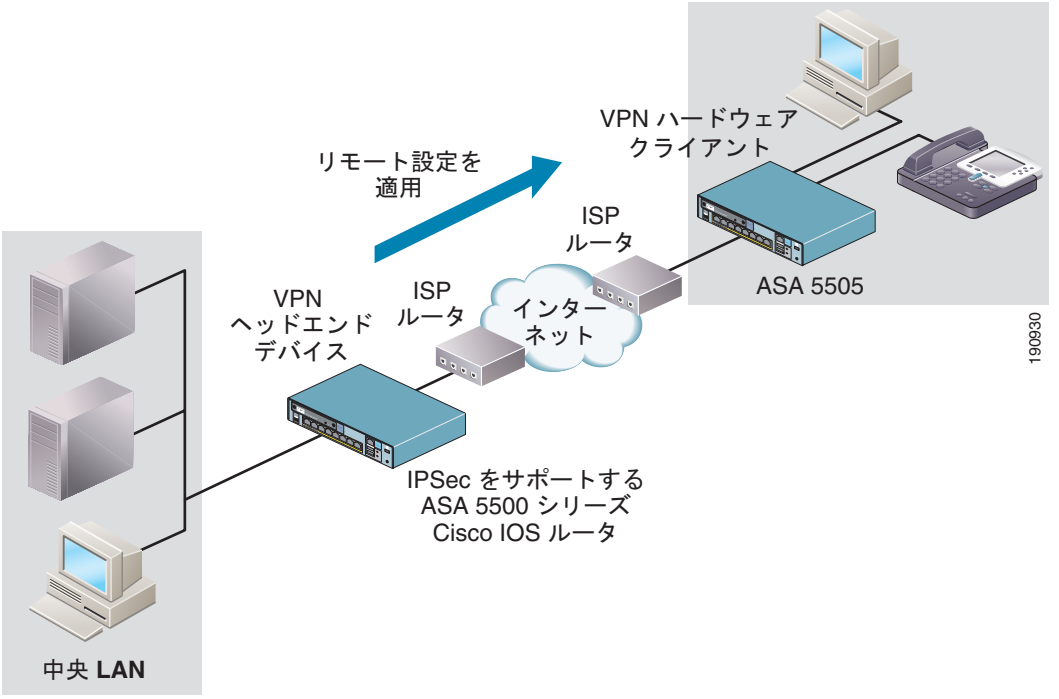
このシナリオでは、ASA 5505 をハードウェア クライアント（リモート デバイスとも呼ばれる）として構成します。VPN ヘッドエンド デバイスを使用して 1 つまたはそれ以上の VPN ハードウェア クライアントを構成すると、複数のサイトを持つ企業は、そのサイト間の安全な通信を確立して、ネットワーク リソースを共有できます。

ハードウェア クライアントを使用して Easy VPN ソリューションを構成すると、次の方法で VPN の構成と管理が簡素化されます。

- リモート サイトのホストが VPN クライアント ソフトウェアを実行する必要がなくなる。
- 中央サーバにセキュリティ ポリシーが常駐し、VPN 接続が確立されると、セキュリティ ポリシーがリモート ハードウェア クライアントに適用される。
- ローカルに設定する必要がある設定パラメータがほとんどないため、オンサイト管理の必要性を最小限に抑えられる。

図 2-6 に、各種 Easy VPN コンポーネントを構成する方法を示します。

図 2-6　VPN ハードウェア クライアントとして設置された ASA 5505



ASA 5505 を VPN ハードウェア クライアントとして設定する方法の詳細については、第 9 章「シナリオ：Easy VPN ハードウェア クライアント設定」を参照してください。

各シナリオに対する設定手順

このマニュアルには、この章の各構成シナリオに対応する設定の章があり、構成タイプに合わせて ASA 5505 を設定する方法が記載されています。

ASA 5505 を設定する構成シナリオ	参照する章
シナリオ 1：外部接続を使用したプライベート ネットワーク	第 5 章「適応型セキュリティ アプライアンスの設定」
シナリオ 2：DMZ を使用した基本的なインストレーション	第 6 章「シナリオ：DMZ 設定」
シナリオ 3：IPSec リモートアクセス VPN	第 7 章「シナリオ：IPSec リモートアクセス VPN 設定」
シナリオ 4：サイトツーサイト VPN	第 8 章「シナリオ：サイトツーサイト VPN 設定」
シナリオ 5：ハードウェア VPN クライアントとして構成された ASA 5505	第 9 章「シナリオ：Easy VPN ハードウェア クライアント設定」

次の作業

第 3 章「VLAN 構成のプランニング」に進みます。

次の作業

CHAPTER 3

VLAN 構成のプランニング

ポートを ASA 5505 上の論理 VLAN にグループ化すると、大規模なプライベート ネットワークをセグメント化でき、サーバ、企業のコンピュータ、および IP 電話などのリソースに対応している可能性がある重要なネットワーク セグメントの保護を強化できます。

この章では、VLAN 構成における ASA 5505 の構成オプションと、必要な VLAN の数を判別する方法を説明します。各 VLAN にポートを割り当てる方法についても説明します。

この章には、次の項があります。

ASA 5505 上の VLAN について

ネットワーク内に ASA 5505 を構成する方法を決定したら、その構成をサポートするのに必要な VLAN の数と、各 VLAN に割り当てるポートの数を決定する必要があります。

この項では、それらを決定できるよう、ASA 5505 上の VLAN がどのように機能するかを説明します。

この項は、次の内容で構成されています。

ASA 5505 上の物理ポートについて

ASA 5505 には、スイッチ ポートと呼ばれる 8 つの Fast Ethernet ポートを備えた内蔵スイッチがあります。8 つの物理ポートのうち 2 つは、Power Over Ethernet（PoE）ポートです。PoE ポートには、PC、IP 電話、DSL モデムなどのユーザ装置を直接接続できます。別のスイッチに接続することもできます。詳細については、「ポートおよび LED」（4-11 ページ）を参照してください。

VLAN について

8 つの物理ポートを、別個のネットワークとして機能する VLAN と呼ばれるグループに分割できます。これによって、企業のセキュリティを向上させることができます。異なる VLAN にあるデバイスは、適切なセキュリティ ポリシーが適用されている適応型セキュリティ アプライアンスを使用してトラフィックを通すことによってのみ、互いに通信できるからです。

ASA 5505 には、VLAN1 と VLAN2 の 2 つの VLAN が事前設定されています。デフォルトでは、イーサネット スイッチ ポート 0/0 は VLAN2 に割り当てられています。他のすべてのスイッチ ポートは、デフォルトで VLAN1 に割り当てられています。

同じ VLAN 上の物理ポートは、ハードウェア スイッチングを使用して互いに通信できます。VLAN は、ルートとブリッジを使用して相互に通信します。たとえば、VLAN1 上のスイッチ ポートが VLAN2 上のスイッチ ポートと通信を行うとき、適応型セキュリティ アプライアンスは設定されているセキュリティ ポリシーをトラフィックに適用し、2 つの VLAN 間でトラフィックをルートまたはブリッジします。

厳密なアクセス コントロールを課して機密デバイスの保護を提供するため、VLAN 間の通信を制限するセキュリティ ポリシーを VLAN に適用できます。セキュリティ ポリシーを個々のポートに適用することもできます。たとえば、同じ VLAN 上に 2 つのポートがあり、互いに通信するのを望まない複数のデバイスが接続されている場合、ポート レベルでセキュリティ ポリシーを適用することができます。

ASA 5505 上のスイッチ ポートは、VLAN に割り当ててからでなければイネーブルにすることはできません。Base プラットフォームでは、各スイッチ ポートを同時に 1 つの VLAN だけに割り当てることができます。Security Plus ライセンスでは、1 つのポートを使用して外部スイッチ上の複数の VLAN 間をトランキングし、組織が大きくなった場合に構成を拡張することができます。

VLAN を作成してポートを割り当てるには、次の方法があります。

VLAN の設定方法	参照先
ASDM Startup Wizard	第 5 章「適応型セキュリティ アプライアンスの設定」
ASDM GUI を使用した設定	ASDM オンライン ヘルプ
コマンドライン インターフェイス	『*Cisco Security Appliance Command Reference*』

VLAN の最大数とタイプ

使用しているライセンスに応じて、ASA 5505 でアクティブにできる VLAN の数が決まります。

ASA 5505 には 2 つの VLAN が事前設定されていますが、使用しているライセンスに応じて最大 20 個の VLAN を作成できます。たとえば、内部、外部、および DMZ ネットワーク セグメント用の VLAN を作成できます。各アクセス スイッチ ポートは、1 つの VLAN に割り当てられます。トランク スイッチ ポートは、複数の VLAN に割り当てることができます。

Base プラットフォームでは、DMZ VLAN と内部 VLAN 間の通信が制限されています。内部 VLAN は DMZ VLAN にトラフィックを送信できますが、DMZ VLAN は内部 VLAN へのトラフィック送信を許可されていません。

Security Plus ライセンスにはこの制限がなく、完全な DMZ 構成を可能にしています。

表 3-1 に、各ライセンスでサポートされている接続数と接続タイプを示します。

表 3-1　アクティブ VLAN のライセンス制限

ライセンス タイプ	モード	接続数
Base プラットフォーム	透過モード	最大 2 つのアクティブ VLAN。
	ルーテッド モード	最大 3 つのアクティブ VLAN。 DMZ VLAN から内部 VLAN へのトラフィックの開始は制限されています。
Security Plus ライセンス	透過モード	最大 3 つのアクティブ VLAN。1 つはフェールオーバー用にする必要があります。
	ルーテッド モード	最大 20 個のアクティブ VLAN。たとえば、各物理ポートに対して、外部、DMZ 1、DMZ 2、エンジリアリング、営業、カスタマーサービス、財務、人事などの個別の VLAN を割り当てることができます。物理ポートは 8 つしかないので、複数の VLAN を 1 つの物理ポートに集約するトランク ポートに追加の VLAN を割り当てる際に役立ちます。

（注） ASA 5505 適応型セキュリティ アプライアンスは、アクティブおよびスタンバイ フェールオーバーをサポートしていますが、ステートフル フェールオーバーはサポートしていません。

VLAN を使用した構成シナリオ

必要な VLAN の数は、適応型セキュリティ アプライアンスにインストールするネットワークの複雑さによって異なります。この項のシナリオをガイドとして使用し、必要な VLAN の数と、それぞれの VLAN に割り当てるポートの数を判別することができます。

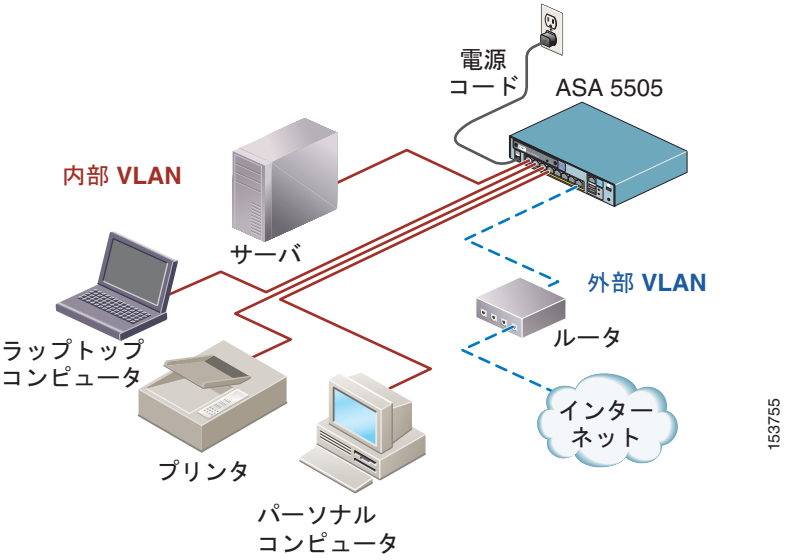
この項は、次の内容で構成されています。

- 2 つの VLAN を使用した基本的な構成（3-6 ページ）
- DMZ 構成（3-8 ページ）
- 3 つの VLAN を使用したテレワーカー構成（3-9 ページ）

2 つの VLAN を使用した基本的な構成

ほとんどの構成では、図 3-1 に示すように、内部 VLAN と外部 VLAN の 2 つの VLAN のみを作成する必要があります。

図 3-1　2 つの VLAN を使用した構成



この例では、ネットワークに内部 VLAN と外部 VLAN が含まれます。内部 VLAN は、互いに通信を行うことを VLAN 内のすべてのデバイスに許可し、外部 VLAN は、インターネット上のデバイスとの通信をユーザに許可します。

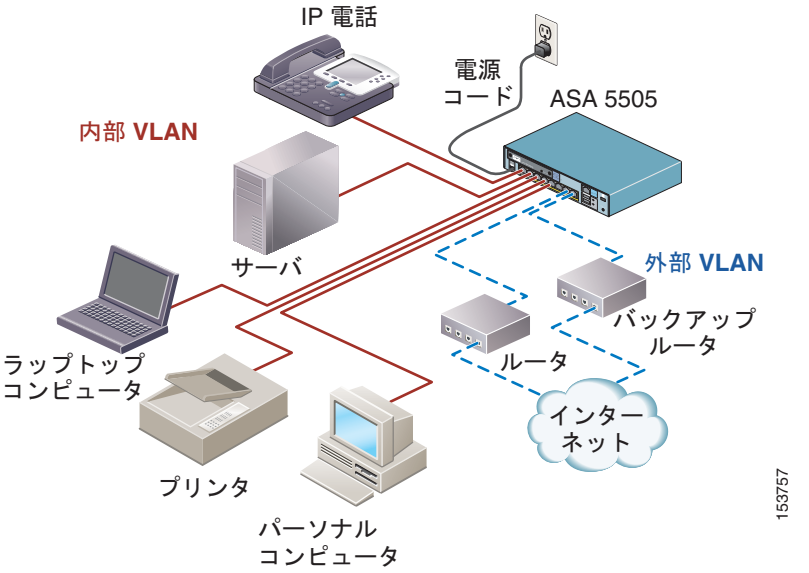
内部 VLAN は、デスクトップ コンピュータ、ネットワーク プリンタ、および他のデバイスを接続する最大 7 つの物理ポートで構成できます。このシナリオでは、外部 VLAN は、外部 WAN ルータを使用するシングル ISP 接続で構成されます。

図 3-1 では、内部 VLAN は ASA 5505 の スイッチ ポートを 4 つ使用し、外部 VLAN は 1 つだけ使用しています。3 つのスイッチ ポートが未使用です。

（注） この構成は PIX 501 を使用するセキュリティ構成に類似しています。 ファイアウォールの背後にあるデバイスが内部および外部で通信できる PIX 501 セキュリティ アプライアンスを使用したセキュリティ構成をすでに使用している場合は、同じ構成をそのまま使用し、PIX 501 デバイスを ASA 5505 デバイスに交換できます。

この同じカスタマーが 2 つのインターネット接続を必要とする場合は、図 3-2 に示すように、外部 VLAN に追加ポートを割り当てることができます。この構成には、内部 VLAN と外部 VLAN が含まれます。外部 VLAN には、一方の接続が切断されたときにリンク冗長性を提供する2つの外部接続が使用されています。

図 3-2　デュアル ISP 接続を使用した内部 VLAN

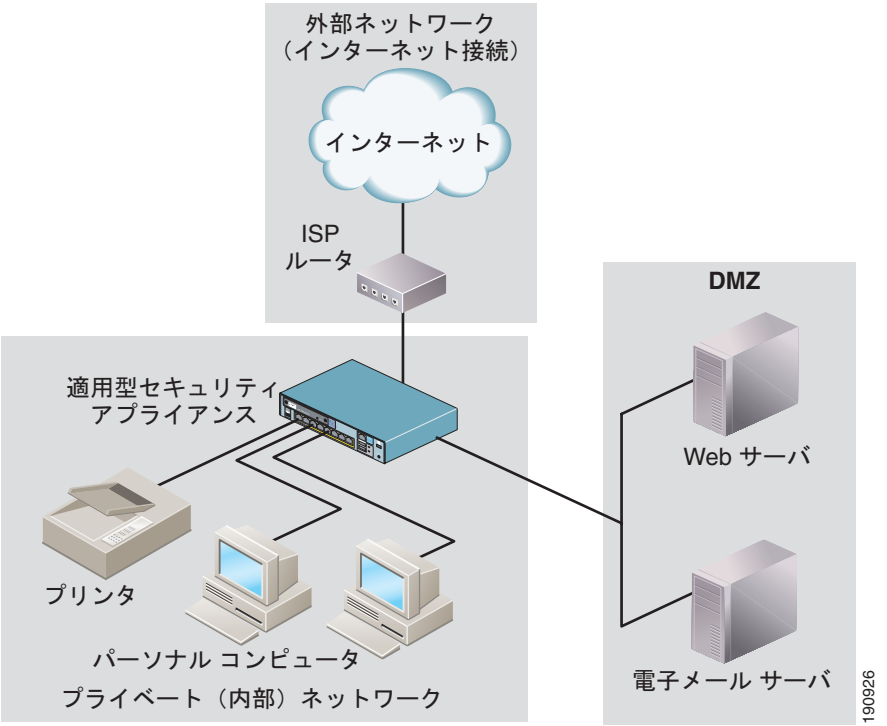


非常に複雑なネットワークの場合でも、内部用と外部用の 2 つの VLAN だけを使用して構成することができます。

DMZ 構成

3 つの VLAN を作成する必要がある唯一の構成は、内部ネットワークに加えて DMZ も保護する必要がある場合です。構成に DMZ がある場合、DMZ は固有の VLAN 上にある必要があります。

図 3-3　3 つの VLAN を必要とする構成



この例では、3 つの物理スイッチ ポートが内部 VLAN に割り当てられ、2 つのスイッチ ポートが DMZ VLAN に割り当てられ、1 つのスイッチ ポートが外部 VLAN に割り当てられています。2 つのスイッチ ポートが未使用です。

3 つの VLAN を使用したテレワーカー構成

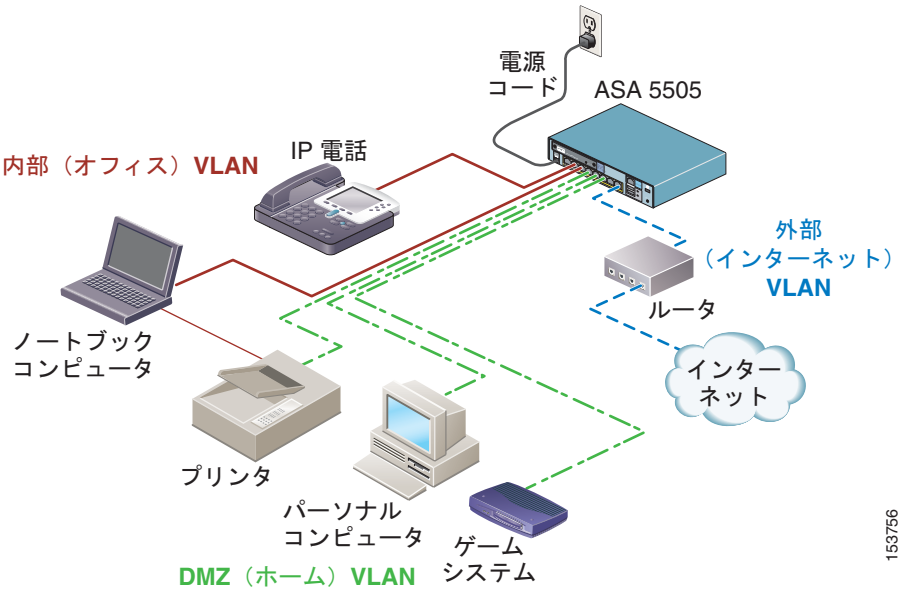
3 つの VLAN の使用は必須ではありませんが、テレワーカーをサポートするためにリモート VPN ハードウェア クライアントを構成する状況などでは、役立つことがあります。

図 3-4 では、ASA 5505 をホーム オフィス環境に設置しており、リモート VPN ハードウェア クライアントとして使用しています。ASA 5505 は、次の 3 つの VLAN に対して設定されています。

- メインの企業ネットワークへのアクセスをサポートするすべてのデバイスで構成されている内部（オフィス）VLAN
- 家族の全員が使用できるデバイスで構成されている DMZ（ホーム）VLAN
- 内部 VLAN と DMZ VLAN の両方にインターネット接続を提供する外部（インターネット）VLAN

この場合、ASA 5505 が内部（オフィス）VLAN 上の重要なアセットを保護するため、これらのデバイスが DMZ（ホーム）VLAN からのトラフィックの影響を受けることはありません。内部（オフィス）VLAN 内のデバイスと企業のヘッドエンド デバイスとの安全な接続を確立するには、Easy VPN ハードウェア クライアント機能をイネーブルにし、内部（オフィス）VLAN からのトラフィックだけが Easy VPN 接続を開始するようにします。この構成では、DMZ（ホーム）VLAN のユーザは内部（オフィス）VLAN とは無関係にインターネットを閲覧でき、内部（オフィス）VLAN のセキュリティが損なわれることはありません。

図 3-4　3 つの VLAN を使用したテレワーカー構成



この例では、ASA 5505 の物理ポートが次のように使用されています。

- 3 つの物理スイッチ ポートで構成される内部（オフィス）VLAN。そのうちの 1 つは Power over Ethernet（PoE）スイッチ ポートで、IP 電話に使用します。
- 3 つの物理スイッチ ポートで構成される DMZ（内部）VLAN。
- 1 つの物理スイッチ ポートで構成される外部（インターネット）VLAN。この物理スイッチ ポートは、外部 WAN ルータまたはブロードバンド モデムを使用するシングル ISP 接続をサポートしています。

プリンタは、内部 VLAN と DMZ VLAN の両方で共有されます。

VLAN の他のシナリオについては、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

次の作業

第 4 章「ASA 5505 の取り付け」に進みます。

次の作業

CHAPTER 4

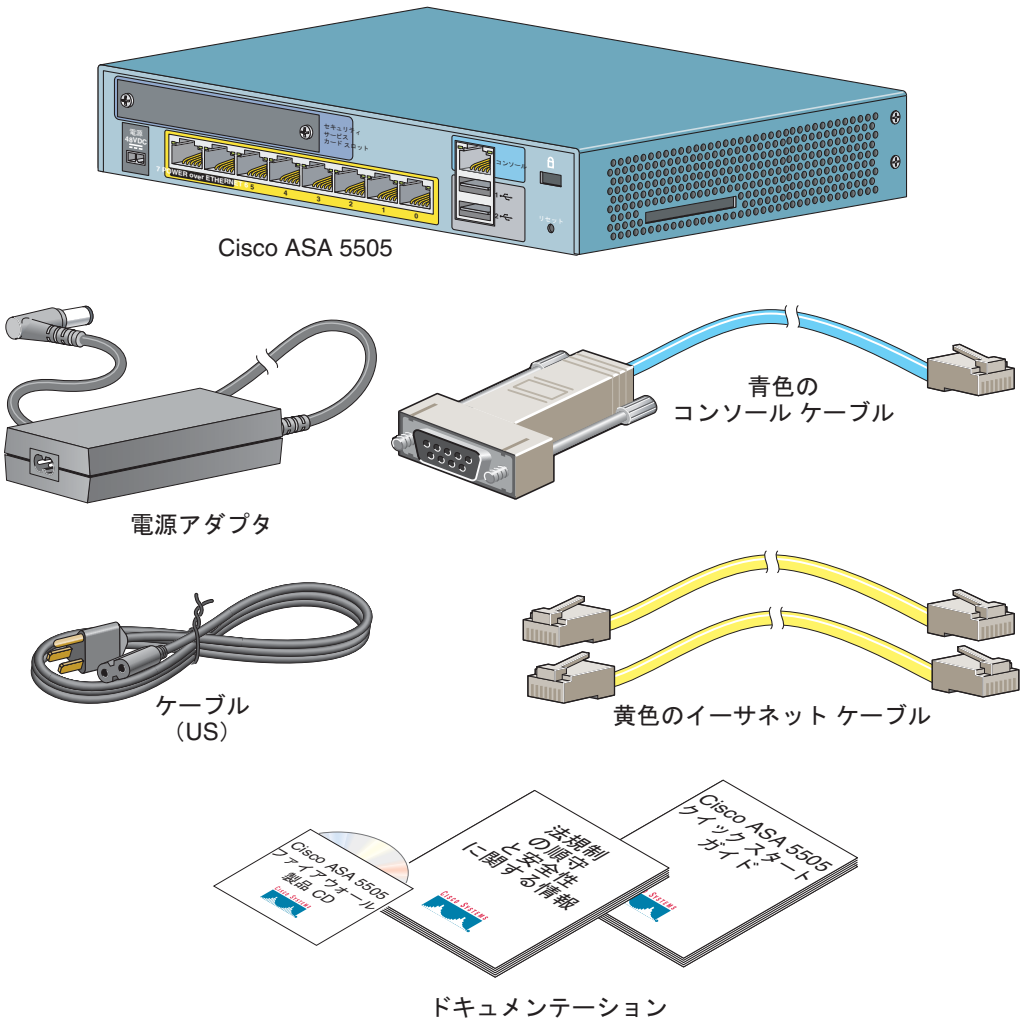
ASA 5505 の取り付け

この章では、ASA 5505 適応型セキュリティ アプライアンスの取り付け方法について説明します。この章には、次の項があります。

パッケージ内容の確認

パッケージの箱の内容をチェックし、図 4-1 に表示されているように、Cisco ASA 5505 適応型セキュリティ アプライアンスを取り付けるために必要な品目がすべてそろっていることを確認します。

図 4-1　ASA 5505 パッケージの内容



PoE ポートおよびデバイス

ASA 5505 では、スイッチ ポート Ethernet 0/6 および Ethernet 0/7 は、IP 電話またはワイヤレス アクセス ポイントなどの IEEE 802.3af 標準に準拠した PoE デバイスをサポートしています。 非 PoE デバイスを取り付ける場合、またはこれらのスイッチ ポートに接続しない場合、適応型セキュリティ アプライアンスはポートに電力を供給しないため、デバイス独自の電源が必要になります。

これらのポートは、IP 電話または他の PoE デバイスに電力を供給できる唯一のポートです。ただし、これらのポートはそれ以外の用途にも使用されます。イーサネット スイッチ ポートとして使用することもできます（イーサネット スイッチ ポートには 0 ～ 5 の番号が割り当てられています）。PoE デバイスが接続されていない場合は、そのポートに電力は供給されません。

PoE デバイスを接続する場合は、次のガイドラインを使用します。

- ストレート　ケーブルだけを使用してください。クロスケーブルを使用した場合、ASA 5505 は電力を PoE ポートに供給しません。
- E0/6 および E0/7 を使用して PoE デバイスに接続する場合、E0/6 および E0/7 のオートネゴシエーション（速度とデュプレックスの強制）をディセーブルにしないでください。オートネゴシエーションがディセーブルの場合、ASA 5505 は PoE デバイスが接続されていることを認識しません。この場合、ポートに電力は供給されません。

（注） Cisco PoE デバイスを非 PoE スイッチ ポート（E0/0 ～ E0/5）に接続するときは注意してください。そのスイッチ ポートでオートネゴシエーションがディセーブルの場合、一部の Cisco Powered Device（PD; 受電装置）モデルでネットワークのループバックが発生する可能性があります。

- Cisco IP Phone 7970 は、ASA 5505 から電力が供給される場合は、常に低電力モードになります。

シャーシの取り付け

ASA 5505 を取り付けるには、次の手順に従います。

ステップ 1　シャーシを安定した平らな面に置きます。このシャーシはラック マウントできません。

ステップ 2　ポート 0 をパブリック ネットワーク（インターネット）に接続します。

a. 黄色のイーサネット ケーブルを使用して、デバイスをスイッチまたはハブに接続します。

b. 黄色のイーサネット ケーブルのうち 1 本を使用して、デバイスをケーブル、DSL、または ISDN モデムに接続します。

（注）　デフォルトでは、スイッチ ポート 0 は外部ポートです。

ステップ 3　イーサネット ケーブルを使用して、ネットワーク デバイスを残りの 7 つのスイッチド ポート（1 ～ 7 番）の 1 つに接続します。

Power over Ethernet（PoE）デバイスを接続する場合は、PoE をサポートしているスイッチ ポート（6 番と 7 番のポート）のいずれかに接続します。

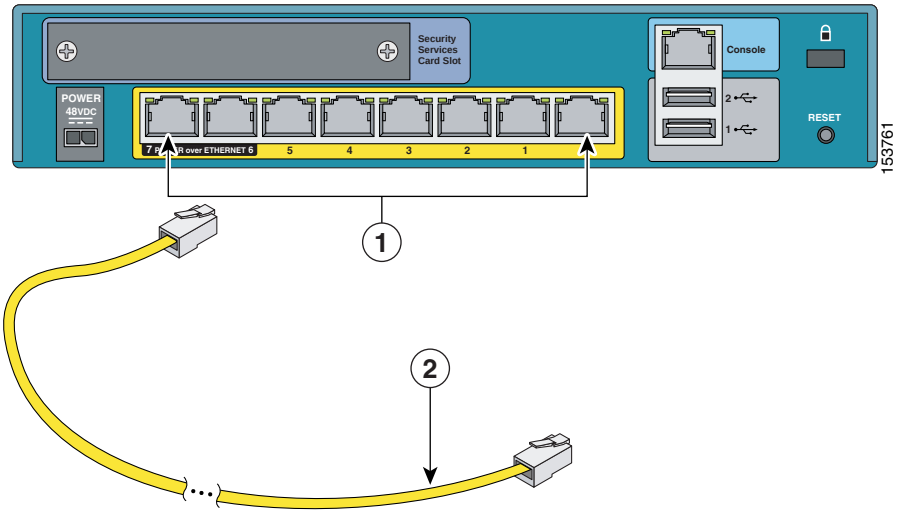
ネットワーク インターフェイスへの接続

ネットワーク インターフェイスに接続するには、次の手順に従います。

ステップ 1　RJ-45 to RJ-45 イーサネット ケーブルを用意します。

ステップ 2　図 4-2 に表示されているように、イーサネット ケーブルの片方の端子をイーサネット ポート（ポート 0 ～ 7）に接続します（通常、イーサネット ポート 0 を使用して、インターネット ルータに接続します）。

図 4-2　イーサネット インターフェイスへの接続



1	イーサネット スイッチ ポート	2	イーサネット ケーブル

ステップ 3　イーサネット ケーブルのもう一方の端子をルータ、デスクトップ コンピュータ、またはプリンタなどのデバイスに接続します。

ASA 5505 の電源投入

ASA 5505 の電源を入れるには、次の手順に従います。

ステップ 1　電源コードを電源に接続します。

ステップ 2　電源コードの小さな四角いコネクタを背面パネルの電源コネクタに接続します。

ステップ 3　電源入力ケーブルの AC 電源コネクタをコンセントに接続します。

（注）　ASA 5505 には、電源スイッチがありません。ステップ 3 を完了すると、デバイスの電源が入ります。

ステップ 4　電源 LED を確認します。緑色に点灯する場合は、デバイスの電源が入っています。

詳細については、「前面パネルのコンポーネント」（4-11 ページ）を参照してください。

システム管理用の PC のセットアップ

わかりやすいグラフィカル ユーザ インターフェイス（GUI）を提供する Adaptive Security Device Manager（ASDM）アプリケーションを使用して、PC からセットアップ、設定、および管理のタスクを実行できます。 設定と管理機能だけでなく、ASDM は、初期設定、VPN 設定、およびハイ アベイラビリティ設定の設定ウィザードも提供します。

ASDM を使用したセットアップおよび設定の詳細については、第 5 章「適応型セキュリティ アプライアンスの設定」 を参照してください。

ASA 5505 を設定および管理できる PC をセットアップするには、次の手順に従います。

ステップ 1　ASA 5505 内部ポートの 1 つに接続する PC インターフェイスの速度がオートネゴシエーションに設定されていることを確認します。この設定は、優れた性能を提供します。

デフォルトでは、ASA 5505 が自動的に内部インターフェイスの速度をネゴシエーションします。オートネゴシエーションを PC インターフェイスのオプションにしない場合は、速度を 10 または 100 Mbps の半二重に設定します。インターフェイスを全二重に設定しないでください。これは、インターフェイスの全体的なスループット機能に大きな影響を与えるデュプレックスの不一致を引き起こす原因となります。

ステップ 2　DHCP を使用するように PC を設定します（ASA 5505 から自動的に IP アドレスを受信するため）。この設定により、PC が ASA 5505 およびインターネットと通信できるようになるだけでなく、ASDM を実行して設定および管理のタスクを行えます。

または、192.168.1.0 サブネットの中からアドレスを選択して、スタティック IP アドレスを使用中の PC に割り当てることもできます 他のデバイスを任意の内部ポートに接続する場合は、同じ IP アドレスが使用されていないことを確認します。

ステップ 3　イーサネット ケーブルを使用して、PC を ASA 5505 の背面パネルにあるスイッチド内部ポート（1 ～ 7 番のポートの 1 つ）に接続します。

ステップ 4　LINK LED を確認し、ASA 5505 との基本的な接続が確立されていることを確認します。

接続が確立されると、ASA 5505 の前面パネルにある LINK LED が緑色に点灯します。

ここまでの作業で、ASDM と ASDM Startup Wizard にアクセスできるようになりました。ASA 5505 の初期セットアップと設定の実行方法の詳細については、第 5 章「適応型セキュリティ アプライアンスの設定」を参照してください。

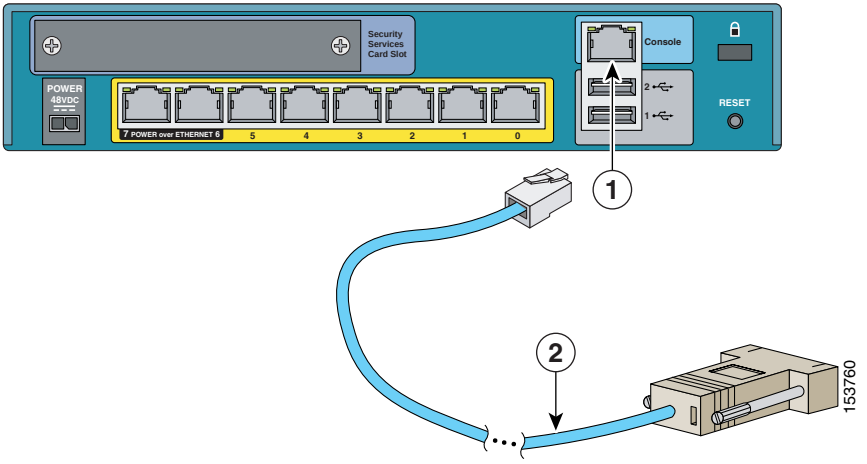
オプションの手順

ここでは、ASA 5505 の初期セットアップでは必須ではないタスクを実行する方法について説明します。この項は、次の内容で構成されています。

コンソールへの接続

ASA 5505 のコンソール ポートを使用して、管理用のコマンドラインにアクセスできます。これには、図 4-3 に表示されているように、PC またはワークステーションのシリアル ターミナル エミュレータを実行する必要があります。

図 4-3　コンソールへの接続



1	コンソール ポート	2	コンソール ケーブル

ローカルのコマンドライン管理アクセス用のコンソールを接続するには、次の手順に従います。

ステップ 1　PC ターミナル アダプタの片方の端子を PC の標準 9 ピン PC シリアル ポートに差し込みます。

ステップ 2　青色のコンソール ケーブルのもう一方の端子をコンソール ポートに差し込みます。

ステップ 3　PC ターミナル エミュレーション ソフトウェアまたはターミナルに 9600 ボー、8 データ ビット、パリティなし、および 1 ストップ ビットを設定します。

ケーブル ロックの取り付け

ASA 5505 には、ラップトップ コンピュータなどの小型のポータブル機器に対して、物理的なセキュリティを提供する標準デスクトップ ケーブル ロックを取り付けるスロットがあります。ケーブル ロックは同梱されていません。

ケーブル ロックを取り付けるには、次の手順に従います。

ステップ 1　メーカーの指示に従って、ケーブルのもう一方の端子を取り付け、適応型セキュリティ アプライアンスの安全を確保します。

ステップ 2　ASA 5505 の背面パネルにあるロック スロットにケーブル ロックを接続します。

ポートおよび LED

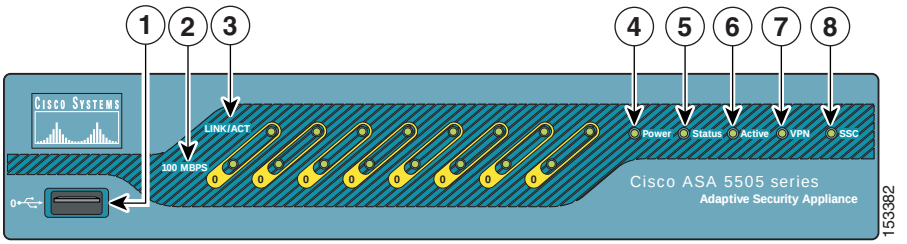
ここでは、ASA 5505 の前面パネルと背面パネルについて説明します。この項は、次の内容で構成されています。

前面パネルのコンポーネント

ASA 5505 の前面パネルにある **LINK/ACT** インジケータは、リンクが確立されたときは通常の緑色の点灯で、ネットワーク アクティビティが発生しているときは緑色の点滅です。各イーサネット インターフェイス（0 ～ 7 番）には、動作速度と物理リンクの確立状況を示す 2 つの LED があります。

図 4-4 に、ASA 5505 の前面パネルを示します。

図 4-4　ASA 5505 前面パネル



	ポート /LED	色	状態	説明
1	USB ポート	—	—	今後のリリース用に確保されています。
2	速度インジケータ	消灯	—	ネットワーク トラフィックが 10 Mbps で流れています。
		緑	点灯	ネットワーク トラフィックが 100 Mbps で流れています。
3	リンク アクティビティ インジケータ	緑	点灯	物理リンクが確立されています。*
		緑	点滅	ネットワーク アクティビティが発生しています。

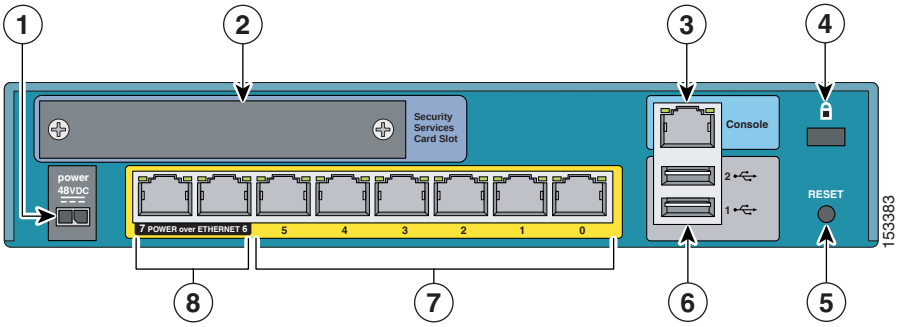
	ポート /LED	色	状態	説明
4	電源	緑	点灯	デバイスの電源が入っています。
		オフ	—	デバイスの電源が入っていません。
5	ステータス	緑	点滅	電源投入診断を実行中か、システムがブート中です。
			点灯	システムが動作可能な状態です。
		オレンジ	点灯	システムで問題が発生しています。
6	アクティブ	緑	点灯	システムがトラフィックを転送しています。 システムがハイ アベイラビリティ セットアップを行っている場合は、緑色の点灯によって、リンクがトラフィックを転送していることが示されます。
		オレンジ	点灯	システムがスタンバイの状態です。 システムがハイ アベイラビリティ セットアップを行っている場合は、オレンジ色の点灯によって、スタンバイユニットであることが示されます。
7	VPN	緑	点灯	VPN トンネルが確立されています。
			点滅	システムが VPN トンネルを開始しています。
		オレンジ	点灯	トンネルの開始が失敗しました。
8	SSC	—	—	SSC スロットに SSC カードが装着されています。 **（注）** 現在のリリースではサポートされていません。

* LINK/ACT LED が点灯していない場合、デュプレックスの不一致が発生していればリンクがダウンしている可能性があります。ASA 5505 側または反対側で設定を変更し、問題を修正できます。オートネゴシエーションがディセーブル（デフォルトでは、イネーブル）の場合は、誤ったタイプのケーブルを使用している可能性があります。

背面パネルのコンポーネント

図 4-5 に、ASA 5505 の背面パネルを示します。

図 4-5　ASA 5505 背面パネル



	ポートまたは LED	目的
1	電源コネクタ	電源コードの接続
2	セキュリティ サービス カード スロット	今後のリリース用に確保されています。
3	シリアル コンソール ポート	コマンドライン インターフェイス（CLI）を使用したデバイスの管理
4	RESET ボタン	今後のリリース用に確保されています。
5	2 つの USB v2.0 ポート	今後のリリース用に確保されています。
6	イーサネット スイッチ ポート 0 ～ 5	柔軟性のあるゾーン設定を提供する、電力の供給されないレイヤ 2 スイッチ ポート。

	ポートまたは LED	目的
7	PoE スイッチ ポート 6 ～ 7	PoE デバイス（IP Phone などのネットワーク インターフェイスで電源投入できるデバイス）に使用できます。 これらのポートは、IP Phone または他の PoE デバイスに使用できる唯一のポートです。ただし、これらのポートはそれ以外の用途にも使用されます。イーサネット スイッチ ポートとして使用することもできます（イーサネット スイッチ ポートには 0 ～ 5 の番号が割り当てられています）。 PoE デバイスが接続されていない場合は、そのポートに電力は供給されないため、デバイス独自の電源が必要になります。

次の作業

第 5 章「適応型セキュリティ アプライアンスの設定」に進みます。

CHAPTER 5

適応型セキュリティ アプライアンスの設定

この章では、適応型セキュリティ アプライアンスの初期設定について説明します。設定手順を実行するには、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）のいずれかを使用します。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説明します。

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

Cisco 適応型セキュリティ アプライアンスは、すぐに使用を開始できるように工場でデフォルト設定されて出荷されます。ASA 5505 は次のように事前設定されています

- 2 つの VLAN：VLAN 1 と VLAN2。
- VLAN 1 のプロパティは次のとおりです。
  - 名前：「inside」
  - 割り当てられているスイッチ ポート：Ethernet 0/1 から Ethernet 0/7
  - セキュリティ レベル：100
  - 割り当てられているスイッチ ポート：Ethernet 0/1 から 0/7
  - IP アドレス：192.168.1.1 255.255.255.0
- VLAN2 のプロパティは次のとおりです。
  - 名前：「outside」
  - 割り当てられているスイッチ ポート：Ethernet 0/0
  - セキュリティ レベル：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
- デバイスに接続し、ASDM　を使用して設定を入力するための内部インターフェイス。

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には、デフォルト DHCP アドレス プールが組み込まれています。この設定により、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 アプライアンスに接続するためにアプライアンスから DHCP アドレスを取得できます。このため、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 設定の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

Adaptive Security Device Manager について

Adaptive Security Device Manager（ASDM）は、適応型セキュリティ アプライアンスを管理および監視できる、豊富な機能を持つグラフィカル インターフェイスです。Web ベースの設計によってセキュアなアクセスが実現されるため、Web ブラウザを使用して、どこからでも適応型セキュリティ アプライアンスに接続し、管理することができます。

設定と管理の機能がそろっているだけでなく、ASDM には適応型セキュリティ アプライアンスの導入を簡素化および促進するインテリジェント ウィザードが搭載されています。

適応型セキュリティ アプライアンスは、ASDM Web コンフィギュレーション ツールだけでなく、コマンドライン インターフェイスを使用しても設定できます。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』および『*Cisco Security Appliance Command Reference*』を参照してください。

Startup Wizard の使用

ASDM には、適応型セキュリティ アプライアンスの初期設定を簡素化する Startup Wizard が用意されています。Startup Wizard を使用すると、わずかな手順で、内部ネットワークと外部ネットワーク間でパケットが安全に流れ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。

この項では、Startup Wizard を使用して基本的な設定パラメータを設定する方法について説明します。この項は、次の内容で構成されています。

Startup Wizard を起動する前に

Startup Wizard を起動する前に、次の手順に従います。

ステップ 1　Web ブラウザの Java と Javascript を有効にします。

ステップ 2　インターネットにアクセスできることを確認します。

ステップ 3　次の情報を取得します。

- ネットワーク上の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。
- 設定する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、3 つ目の VLAN を作成して、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）。
- インターフェイスの設定情報。つまり、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を許可するかどうか、同じインターフェイスのホスト間でトラフィックを許可するかどうか。
- 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の Easy VPN サーバの IP アドレス、クライアントをクライアント モード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の Easy VPN サーバに設定されたユーザおよびグループ ログイン認定証に一致するそれぞれの認定証。

Startup Wizard の実行

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

ステップ 1　まだ PC を ASA 5505 のスイッチ ポートに接続していない場合は、接続します。

a. 両端に RJ-45 コネクタがついているイーサネット ケーブルを用意します。

b. 一方の RJ-45 コネクタをスイッチ ポートに接続します。

c. イーサネット　ケーブルの逆側の端子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。

ステップ 2　ASDM を開始します。

a. ASA 5505 に接続された PC で、Web ブラウザを開きます。

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

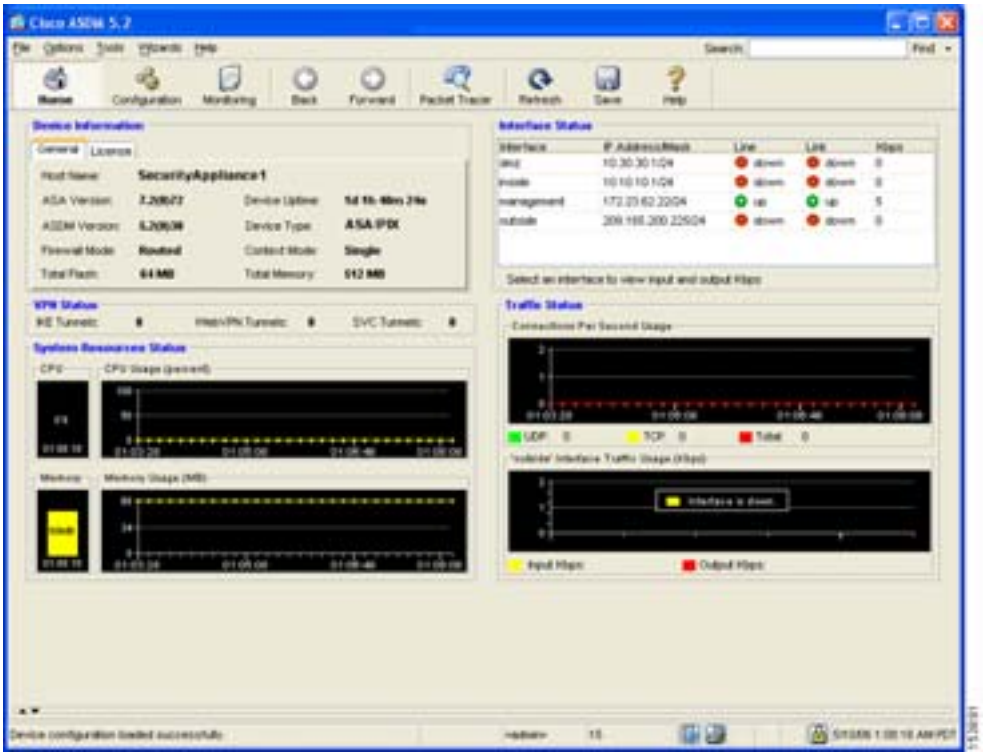
（注） 適応型セキュリティ アプライアンスは、192.168.1.1 のデフォルト IP アドレスが設定されて出荷されます。「**https**」の「**s**」を付け忘れると、接続は失敗します。HTTP over SSL（HTTPS）を使用すると、ブラウザと適応型セキュリティ アプライアンスとの間の安全な接続が可能になります。

c. ASDM ソフトウェアを実行するのに使用する方法を選択するウィンドウで、ASDM Launcher をダウンロードするか、ASDM ソフトウェアを Java アプレットとして実行するかを選択します。

ステップ 3　ユーザ名とパスワードの入力を求めるダイアログボックスで、どちらのフィールドも空のままにします。Enter を押します。

ステップ 4　**Yes** をクリックして、証明書を受け入れます。後続の認証および証明書に関するすべてのダイアログボックスで、**Yes** をクリックします。

ASDM メイン ウィンドウが表示されます。



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

ステップ 6　Startup Wizard の手順に従って、適応型セキュリティ アプライアンスを設定します。

Startup Wizard のフィールドの詳細を確認するには、ウィンドウ下部にある **Help** ボタンをクリックします。

（注） また、ネットワークのセキュリティ ポリシーに基づいて、外部インターフェイス、または必要なその他すべてのインターフェイスを経由する ICMP トラフィックをすべて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もあります。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 メイン ウィンドウで、**Configuration > Properties > Device Administration > ICMP Rules** をクリックします。外部インターフェイス用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 を拒否にそれぞれ設定します。

次の作業

次の 1 つ以上の章を参照して、それぞれの構成に応じた適応型セキュリティ アプライアンスを設定します。

実行内容	参照先
DMZ Web サーバ を保護するための適応型セキュリティ アプライアンスの設定	第 6 章「シナリオ：DMZ 設定」
リモートアクセス VPN 用の適応型セキュリティ アプライアンスの設定	第 7 章「シナリオ：IPSec リモートアクセス VPN 設定」
サイトツーサイト VPN 用の適応型セキュリティ アプライアンスの設定	第 8 章「シナリオ：サイトツーサイト VPN 設定」
Easy VPN リモート デバイスとして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：Easy VPN ハードウェア クライアント設定」

CHAPTER 6

シナリオ：DMZ 設定

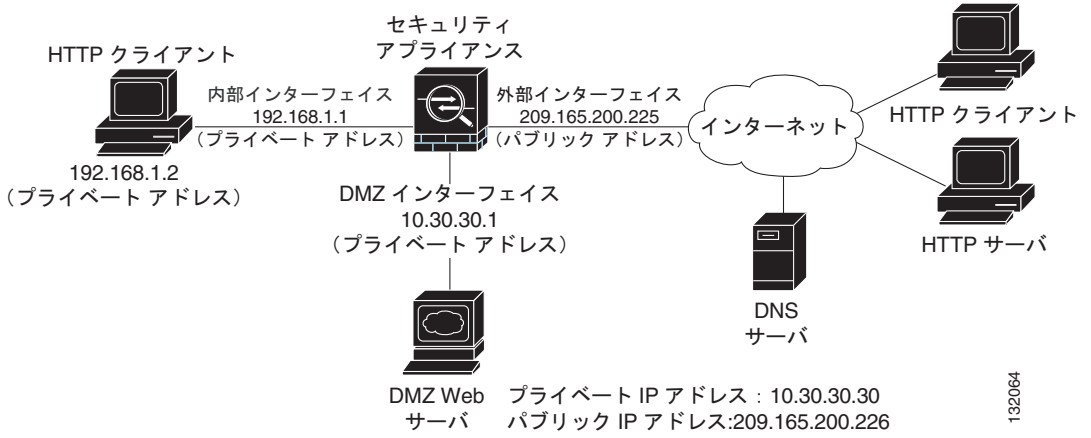
（注） Cisco ASA 5505 の DMZ 設定は、Security Plus ライセンスの場合にだけ可能です。

この章には、次の項があります。

DMZ ネットワーク トポロジの例

図 6-1 のネットワーク トポロジの例は、適応型セキュリティ アプライアンスの DMZ 実装で多く利用されているものです。

図 6-1　DMZ 設定シナリオのネットワーク レイアウト



このシナリオ例には、次の特徴があります。

- Web サーバが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存在します。
- プライベート ネットワーク上の HTTP クライアントは、DMZ 内の Web サーバにアクセスでき、インターネット上のデバイスとも通信できます。
- インターネット上のクライアントは、DMZ Web サーバへの HTTP アクセスが許可され、その他のトラフィックはすべて拒否されます。
- ネットワークには、だれでも使用できるルーティング可能な IP アドレスが 1 つあります。この IP アドレス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です（209.165.200.225）。

図 6-2 に、プライベート ネットワークから、DMZ Web サーバとインターネットへの HTTP 要求の発信トラフィックの流れを示しています。

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

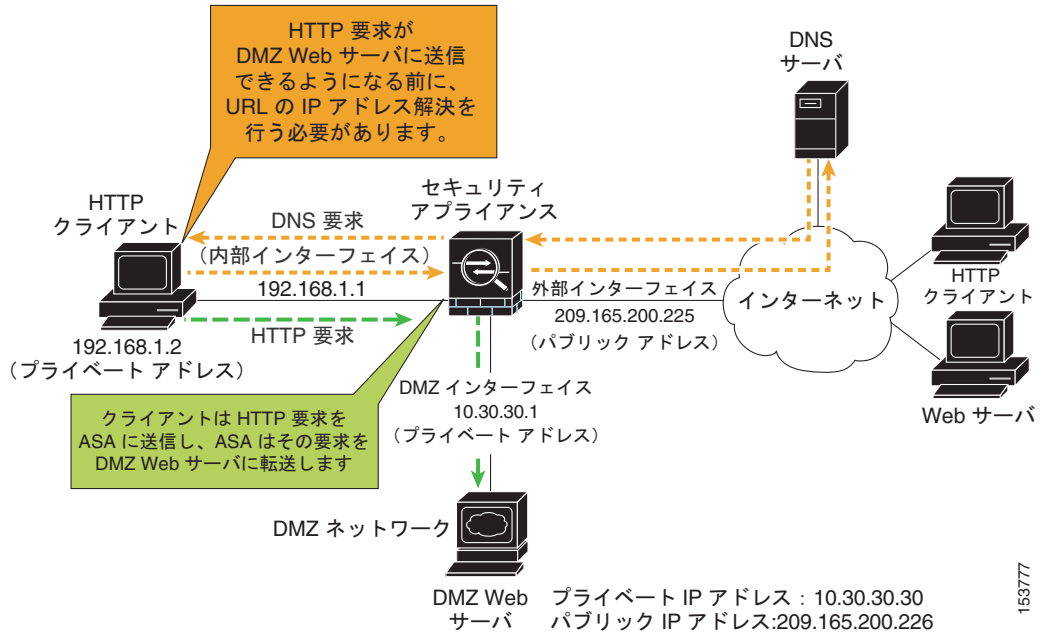


図 6-2 では、適応型セキュリティ アプライアンスは内部クライアントから DMZ Web サーバ宛の HTTP トラフィックを許可します。内部ネットワークには DNS サーバがないので、DMZ Web サーバへの内部クライアントの要求は、次のように処理されます。

1. ルックアップ要求が 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 HTTP 要求を適応型セキュリティ アプライアンスに送信します。
3. 適応型セキュリティ アプライアンスは DMZ Web サーバのパブリック IP アドレスを実際のアドレスに変換し、その要求を Web サーバに転送します。
4. DMZ Web サーバは、内部クライアントの実際の IP アドレスの宛先アドレスとともに HTTP コンテンツを適応型セキュリティ アプライアンスに返します。
5. 適応型セキュリティ アプライアンスは HTTP コンテンツを内部クライアントに転送します。

内部クライアントが DMZ Web サーバから HTTP コンテンツを要求することを許可するには、適応型セキュリティ アプライアンスの設定に次のルールを含める必要があります。

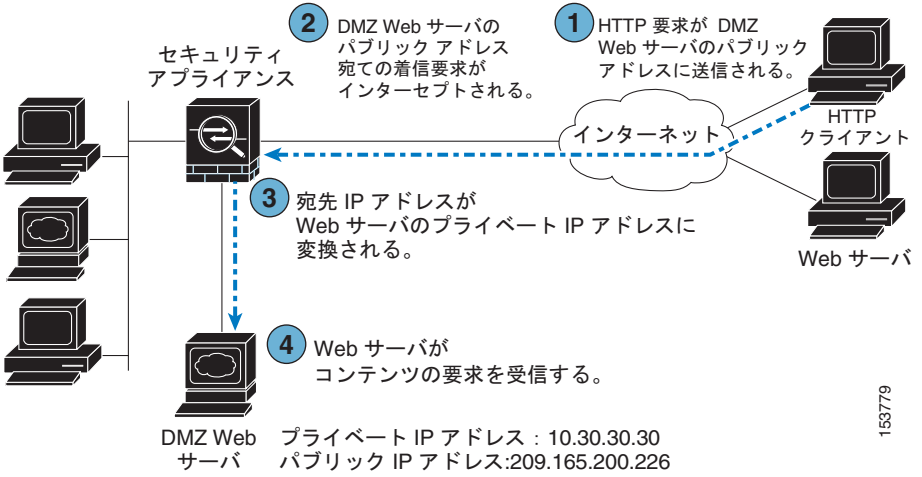
- DMZ Web サーバの実際の IP アドレスを DMZ Web サーバのパブリック IP アドレスに変換する（10.30.30.30 から 209.165.200.225 へ）、DMZ インターフェイスと内部インターフェイス間の NAT ルール。
- 内部クライアント ネットワークの実際のアドレスを変換する、内部インターフェイスと DMZ インターフェイス間の NAT ルール。このシナリオでは、内部クライアントが DMZ Web サーバと通信するとき、内部ネットワークの実際の IP アドレスは同じものに変換されます（10.30.30.30 から 10.30.30.30 へ）。

インターネットから DMZ Web サーバにアクセスするトラフィックを許可するには、適応型セキュリティ アプライアンスの設定に次のものを含めます。

- DMZ Web サーバのパブリック IP アドレスを DMZ Web サーバのプライベート IP アドレスに変換するアドレス変換ルール。
- DMZ Web サーバ宛の着信 HTTP トラフィックを許可するアクセス コントロール ルール。

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

図 6-3　インターネットからの着信 HTTP トラフィックの流れ



この設定を作成する手順については、この章の後半部分で説明します。

DMZ 構成用のセキュリティ アプライアンスの設定

この項では、ASDM を使用して、図 6-1 に示されている設定シナリオ用に適応型セキュリティ アプライアンスを設定する方法について説明します。手順では、シナリオに基づいたサンプル パラメータを使用します。

この設定手順では、適応型セキュリティ アプライアンスにはすでに内部インターフェイス、外部インターフェイス、および DMZ インターフェイスとして設定されているインターフェイスがあることを前提とします。ASDM で Startup Wizard を使用して、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設定します。DMZ インターフェイスのセキュリティ レベルを 0 ～ 100 の間に設定していることを確認します（通常は 50）。

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

この項は、次の内容で構成されています。

次の項では、各手順を実行する方法を詳細に説明します。

設定要件

この DMZ 構成で適応型セキュリティ アプライアンスを設定するには、次の条件が満たされている必要があります。

- 内部クライアントはインターネット上のデバイスと通信ができる必要があります。
- 内部クライアントは DMZ Web サーバと通信できる必要があります。
- 外部クライアントは DMZ Web サーバと通信できる必要があります。

この章の後半部分では、この設定を完了する方法について説明します。

ASDM の起動

Web ブラウザで ASDM を実行するには、アドレス フィールドに次の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) 「https」の「**s**」を付け忘れると、接続は失敗します。HTTP over SSL（HTTPS）を使用すると、ブラウザと適応型セキュリティ アプライアンスとの間の安全な接続が可能になります。

ASDM メイン ウィンドウが表示されます。

内部クライアントとインターネット上のデバイスとの通信を可能にする

内部クライアントによるインターネット上のデバイスからのコンテンツの要求を許可するには、適応型セキュリティ アプライアンスが内部クライアントの実際の 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表示されます。

ASA 5505 のデフォルト設定には、必要なアドレス変換ルールが含まれています。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 アクセスを許可するために何らかの設定を行う必要はありません。

内部クライアントと DMZ Web サーバとの通信を可能にする

この手順では、内部クライアントが DMZ 内の Web サーバと安全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。この手順を実行するには、次の 2 つの変換ルールを設定する必要があります。

- DMZ Web サーバの実際の IP アドレスをパブリック IP アドレスに変換する（10.30.30.30 から 209.165.200.225 へ）、DMZ インターフェイスと内部インターフェイス間の NAT ルール。
- DMZ Web サーバのパブリック IP アドレスを実際の IP アドレスに変換する（209.165.200.225 から 10.30.30.30 へ）、内部インターフェイスと DMZ インターフェイス間の NAT ルール。

  このルールが必要なのは、内部クライアントが DNS ルックアップ要求を送信したときに、DNS サーバが DMZ Web サーバのパブリック IP アドレスを返すためです。

（注） 内部ネットワーク上には DNS サーバがないため、DNS 要求は適応型セキュリティ アプライアンスから出て、インターネット上の DNS サーバによって解決されなければなりません。

この項は、次の内容で構成されています。

内部インターフェイスと DMZ インターフェイス間の内部クライアント IP アドレスの変換

内部インターフェイスと DMZ インターフェイス間で内部クライアント IP アドレスを変換するように NAT を設定するには、次の手順に従います。

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

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

ステップ 3　Add ドロップダウン リストから、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 4　Real Address 領域で、変換する IP アドレスを指定します。このシナリオでは、内部クライアント用のアドレス変換は、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 リストから、Inside インターフェイスを選択します。

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

c.　Netmask ドロップダウン リストから、このシナリオ用の 255.255.255.0 を選択します。

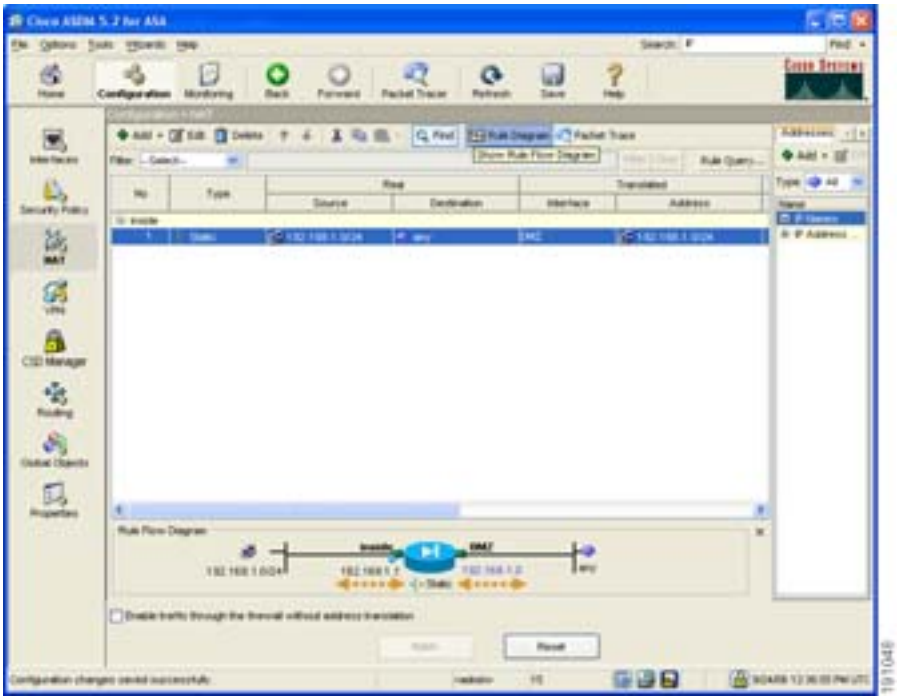
ステップ 5　Static Translation 領域で、次の内容を実行します。

a.　Interface ドロップダウン リストから、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 サブネットの 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 10.10.10.0 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。

ステップ 6　変換ルールが意図したとおりに表示されていることを設定ペインで確認します。ルール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終了します。

Web サーバのパブリック アドレスから実際のアドレスへの変換

Web サーバのパブリック IP アドレスを実際のアドレスに変換する NAT ルールを設定するには、次の手順に従います。

ステップ 1　ASDM メイン ウィンドウで、**Configuration > NAT** を選択します。

ステップ 2　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 3　Real Address 領域で、次の内容を実行します。

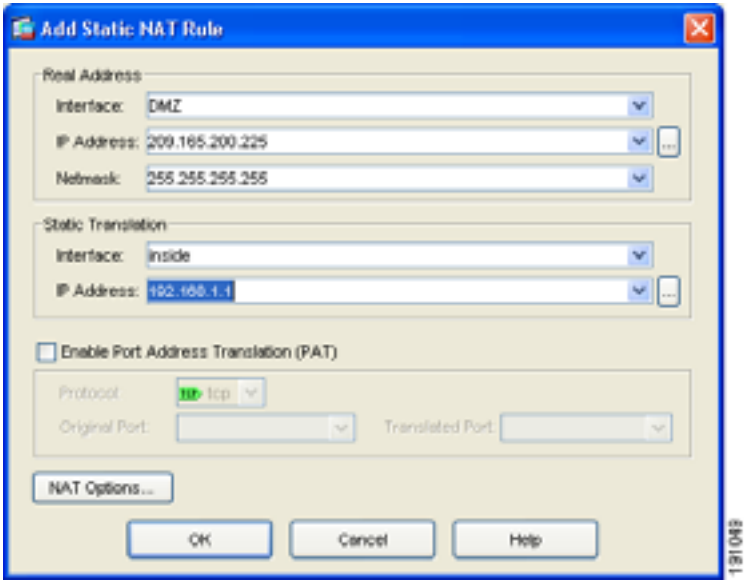
a. Interfaces ドロップダウン リストから、DMZ を選択します。

b. IP Address ドロップダウン リストから、DMZ Web サーバのパブリック アドレスを選択するか、入力します。このシナリオでは、IP アドレスは **209.165.200.225** です。

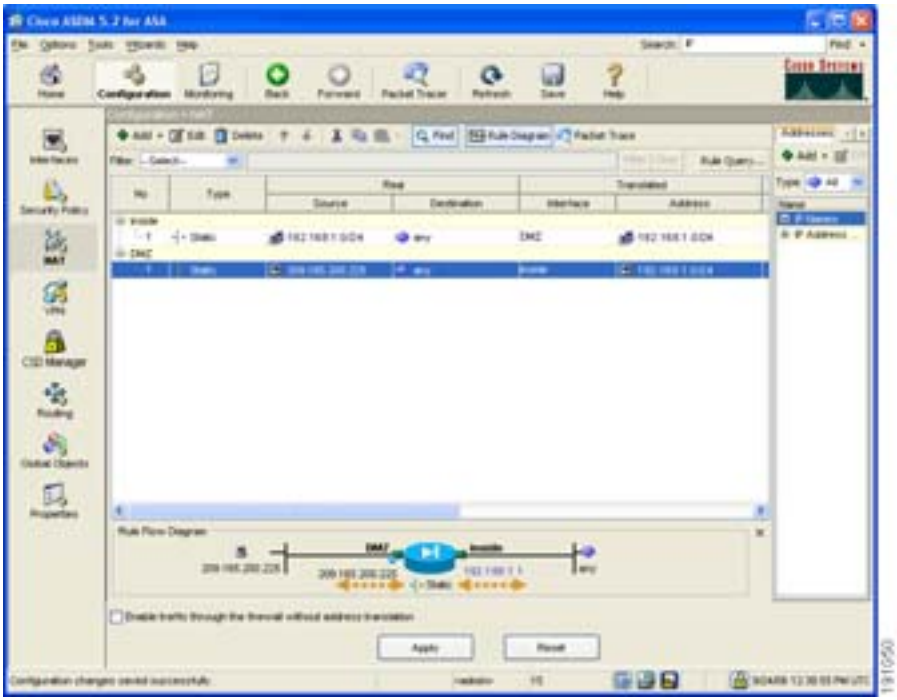
ステップ 4　Static Translation 領域で、次の内容を実行します。

a. Interface ドロップダウン リストから、Inside を選択します。

b. IP Address ドロップダウン リストから、DMZ Web サーバの実際の IP アドレスを選択するか、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。


Add Static NAT Rule
Real Address
Interface: DMZ
IP Address: 209.165.200.225
Netmask: 255.255.255.255
Static Translation
Interface: inside
IP Address: 192.168.1.1
Enable Port Address Translation (PAT)
Protocol: tcp
Original Port:
Translated Port:
NAT Options...
OK
Cancel
Help
191049

ステップ 5　**OK** をクリックして、Configuration > NAT ペインに戻ります。設定は次のように表示されます。



DMZ Web サーバの外部 ID 設定

DMZ Web サーバは、インターネット上のすべてのホストからアクセスできる必要があります。この設定では、DMZ Web サーバのプライベート IP アドレスをパブリック IP アドレスに変換し、外部 HTTP クライアントが適応型セキュリティ アプライアンスを認識せずに Web サーバにアクセスできるようにする必要があります。実際の Web サーバの IP アドレス（10.30.30.30）をパブリック IP アドレス（209.165.200.225）にスタティックにマッピングするには、次の手順に従います。

ステップ 1　ASDM メイン ウィンドウで、**Configuration > NAT** を選択します。

ステップ 2　Add ドロップダウン リストから、Add Static NAT Rule を選択します。

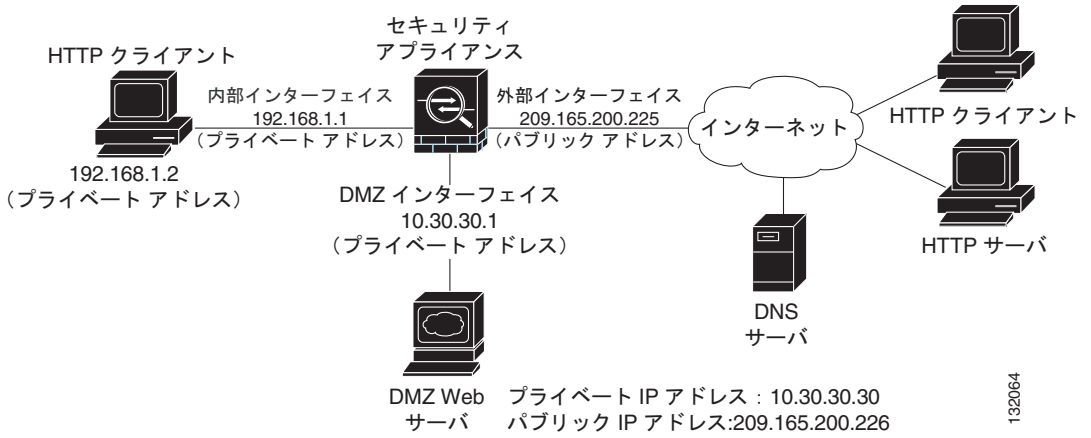
Add Static NAT Rule ダイアログボックスが表示されます。

ステップ 3　Real Address 領域で、次の内容を指定します。

- **a.** Interface ドロップダウン リストから、DMZ インターフェイスを選択します。
- **b.** DMZ Web サーバの実際の IP アドレスを入力します。このシナリオでは、IP アドレスは **10.30.30.30** です。
- **c.** Netmask ドロップダウン リストから、255.255.255.255 を選択します。

ステップ 4　Static Translation 領域で、Web サーバで使用されるパブリック IP アドレスを指定します。

- **a.** Interface ドロップダウン リストから、Outside を選択します。
- **b.** IP Address ドロップダウン リストから、Interface IP キーワード（この場合は、指定した外部インターフェイスの IP アドレス）を選択します。



ステップ 5　Port Address Translation を設定します。

パブリック IP アドレスは 1 つだけなので、Port Address Translation 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外部 IP アドレスに変換する必要があります。Port Address Translation を設定するには、次の手順に従います。

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

b. Protocol ドロップダウン リストから、tcp を選択します。

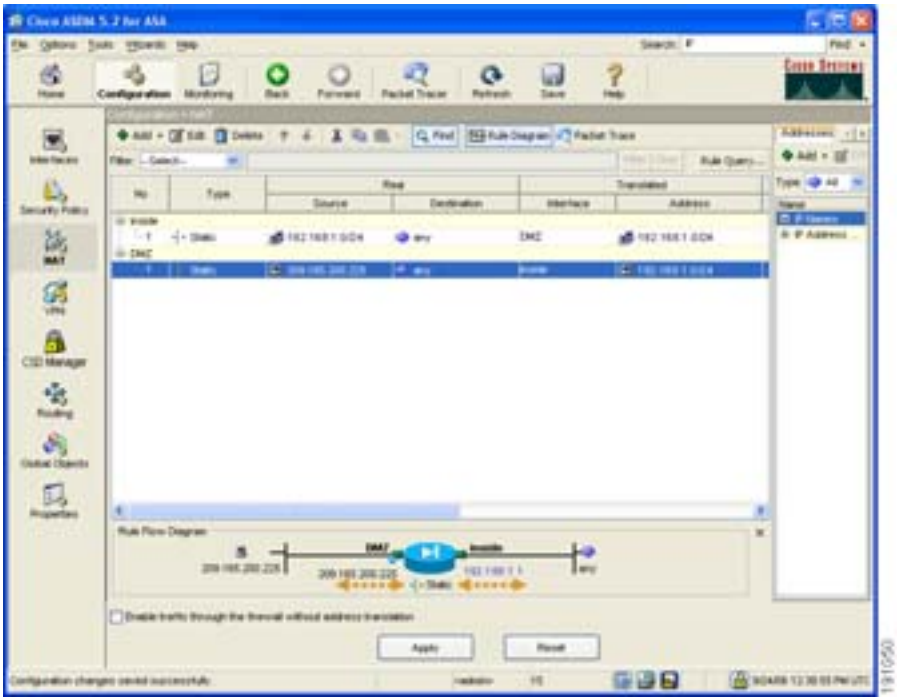
c. Original Port フィールドに **80** と入力します。

d. Translated Port フィールドに **80** と入力します。

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

このルールは、実際の Web サーバの IP アドレス（10.30.30.30）を Web サーバのパブリック IP アドレス（209.165.200.225）にスタティックにマッピングします。

ステップ 6　ルールが、意図したと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 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終了します。

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 ネットワークから着信するトラフィックをすべて拒否します。インターネットから DMZ Web サーバにアクセスするトラフィックを許可するには、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 ル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 ルールは、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に対して、トラフィックが着信されるかどうか、トラフィックの発信元および宛先、および許可するトラフィック プロトコルとサービスのタイプを指定します。

この項では、トラフィックの宛先が DMZ ネットワークの Web サーバである場合に、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 ルールを作成します。パブリック ネットワークから着信する他のすべてのトラフィックは拒否されます。

アクセス コントロール ルールを設定するには、次の手順に従います。

ステップ 1　ASDM メイン ウィンドウで、次の内容を実行します。

a. **Configuration > Security Policy** を選択します。

b. **Access Rules** タブをクリックして、Add プルダウン リストから Add Access Rule を選択します。

Add Access Rule ダイアログボックスが表示されます。

ステップ 2　Interface 領域および Action 領域で、次の内容を実行します。

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

b. Direction ドロップダウン リストから、Incoming を選択します。

c. Action ドロップダウン リストから、Permit を選択します。

ステップ 3　Source 領域で、Type ドロップダウン リストから Any キーワードを選択して、あらゆるホストまたはネットワークから発信されるトラフィックを許可します。

ステップ 4　Destination 領域で、次の内容を実行します。

a. Type ドロップダウン リストから、Interface IP キーワードを選択します。

b. Interface ドロップダウン リストから、Outside を選択します。

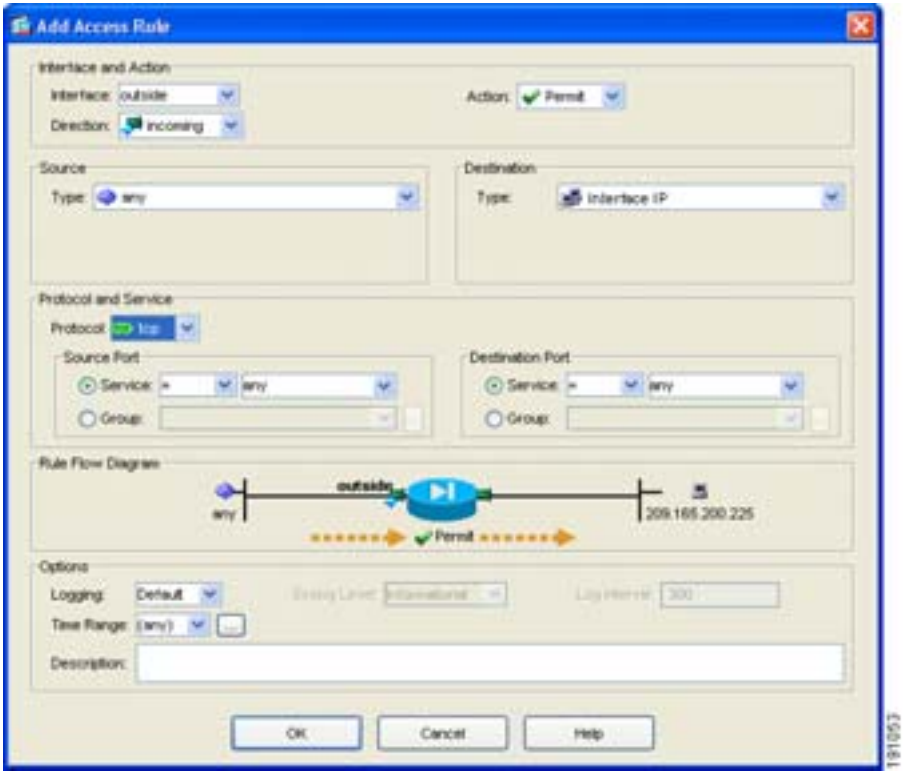
ステップ 5　Protocol 領域および Service 領域で、適応型セキュリティ アプライアンス経由で許可するトラフィックのタイプを指定します。

a. Protocol ドロップダウン リストから、tcp を選択します。

b. Source Port 領域で、Service オプション ボタンが「=」（次と等しい）に設定されていることを確認し、次のドロップダウン リストから Any を選択します。

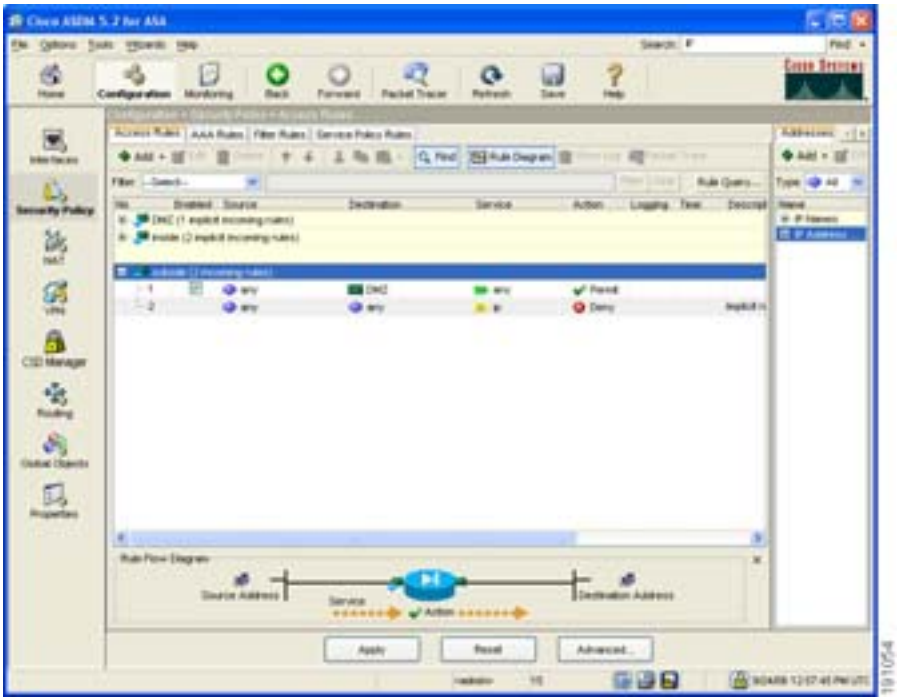
c. Destination Port 領域で、Service オプション ボタンが「=」（次と等しい）に設定されていることを確認し、次のドロップダウン リストから HTTP/WWW を選択します。

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



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

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



ステップ 7　**Apply** をクリックし、適応型セキュリティ アプライアンスを現在実行している設定に変更を保存します。

この設定により、プライベート ネットワークに存在するクライアントは、DMZ Web サーバからのコンテンツに対する HTTP 要求を解決できるだけでなく、プライベート ネットワークの安全性を保持できます。

ステップ 8　次にデバイスを起動するときに適用されるように、設定変更をスタートアップ コンフィギュレーションに保存する場合は、File メニューから **Save** を選択します。

または、ASDM を終了するときに設定変更を半永久的に保存するように求められます。

設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそのまま適用されます。

次の作業

DMZ 内の Web サーバを保護するためだけに適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が完了しました。次の追加の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco Security Appliance Command Line Configuration Guide*』
日常的な運用について	『*Cisco Security Appliance Command Reference*』 『*Cisco Security Appliance Logging Configuration and System Log Messages*』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

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

CHAPTER 7

シナリオ：IPSec リモートアクセス VPN 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 を使用すると、インターネットを越えてセキュアな接続（トンネル）を作成でき、オフサイトのユーザにセキュアなアクセスを提供できます。

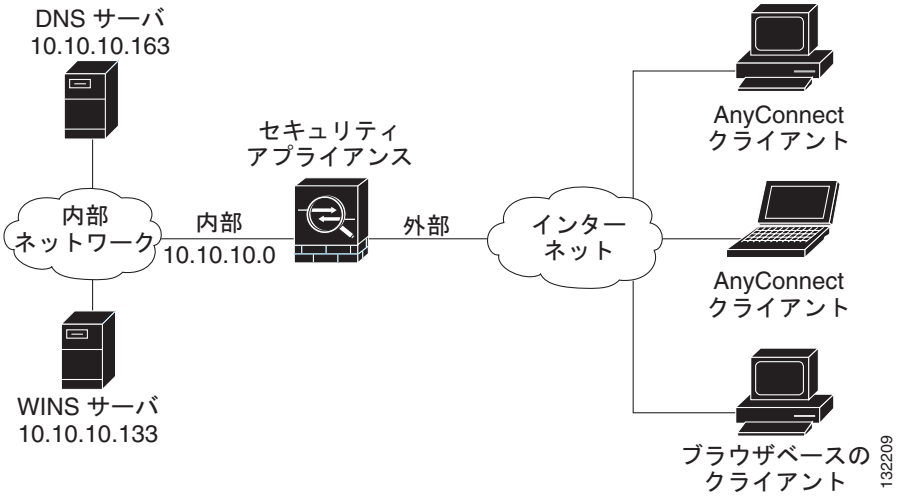
Easy VPN ソリューションを実装する場合、この章では、Easy VPN サーバ（別名、ヘッドエンド デバイス）を設定する方法について説明します。

この章には、次の項があります。

IPSec リモートアクセス VPN ネットワーク トポロジの例

図 7-1 に、インターネットを越えて Cisco Easy VPN ソフトウェア クライアントまたはハードウェア クライアントなどの VPN クライアントからの要求を受け入れ、VPN 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ます。

図 7-1　リモート アクセス VPN 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

ここでは、リモート クライアントおよびデバイスから IPSec 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。Easy VPN ソリューションを実装する場合、この項では、Easy VPN サーバ（別名、ヘッドエンド デバイス）を設定する方法について説明します。

設定内容の例で使われる値は、図 7-1 に示すリモートアクセス シナリオのものです。

この項は、次の内容で構成されています。

収集する情報

リモート アクセス IPSec 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手順を開始する前に、次の情報を手元に用意してください。

- IP プールで使用する 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、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（認証用に AAA サーバを使用している場合を除く）。
- VPN に接続する場合に、リモート クライアントが使用するネットワーキング情報。内容は次のとおりです。
  - プライマリおよびセカンダリの DNS サーバの IP アドレス
  - プライマリおよびセカンダリの WINS サーバの IP アドレス
  - デフォルトのドメイン名
  - 認証されたリモート クライアントにアクセスできるローカル ホスト、グループ、およびネットワークの IP アドレスのリスト

ASDM の起動

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

（注） 「**https**」の「**s**」を付け忘れると、接続は失敗します。HTTP over SSL（HTTPS）を使用すると、ブラウザと適応型セキュリティ アプライアンスとの間の安全な接続が可能になります。

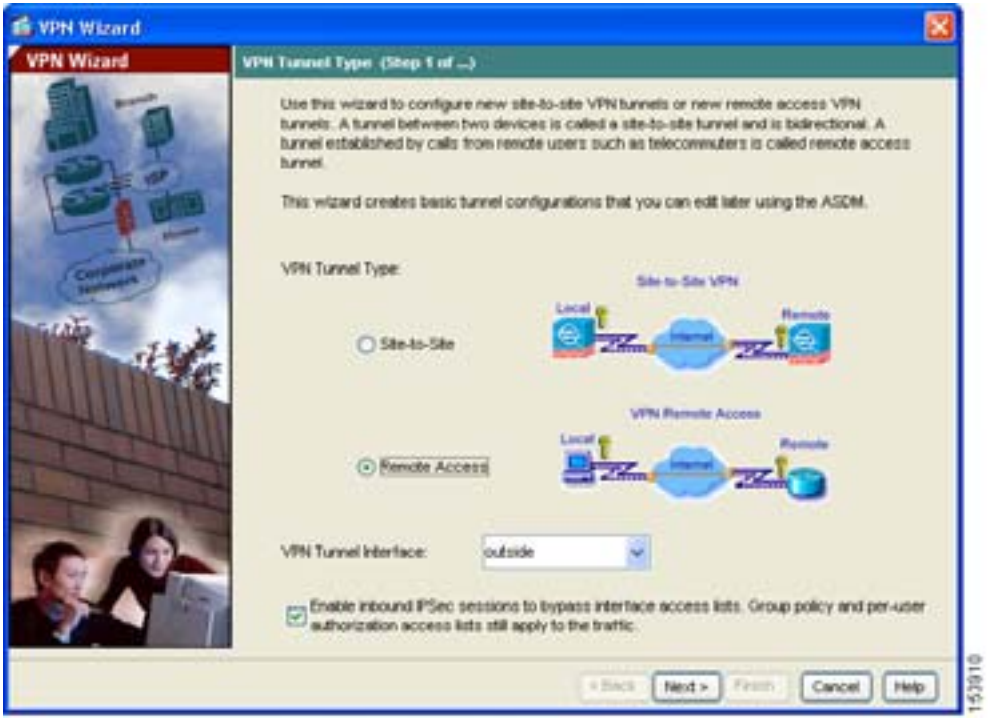
メイン ASDM ウィンドウが表示されます。


Cisco ASDM 5.2
Device Information
SecurityAppliance1
Interface Status
VPN Status
Traffic Status
System Resources Status

IPSec リモートアクセス VPN 用の ASA 5505 の設定

リモートアクセス VPN の設定用のプロセスを開始するには、次の手順に従います。

ステップ 1　ASDM メイン ウィンドウで、Wizards ドロップダウン メニューから **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、次の手順に従います。

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 トンネルで有効なインターフェイスとして **Outside** を選択します。

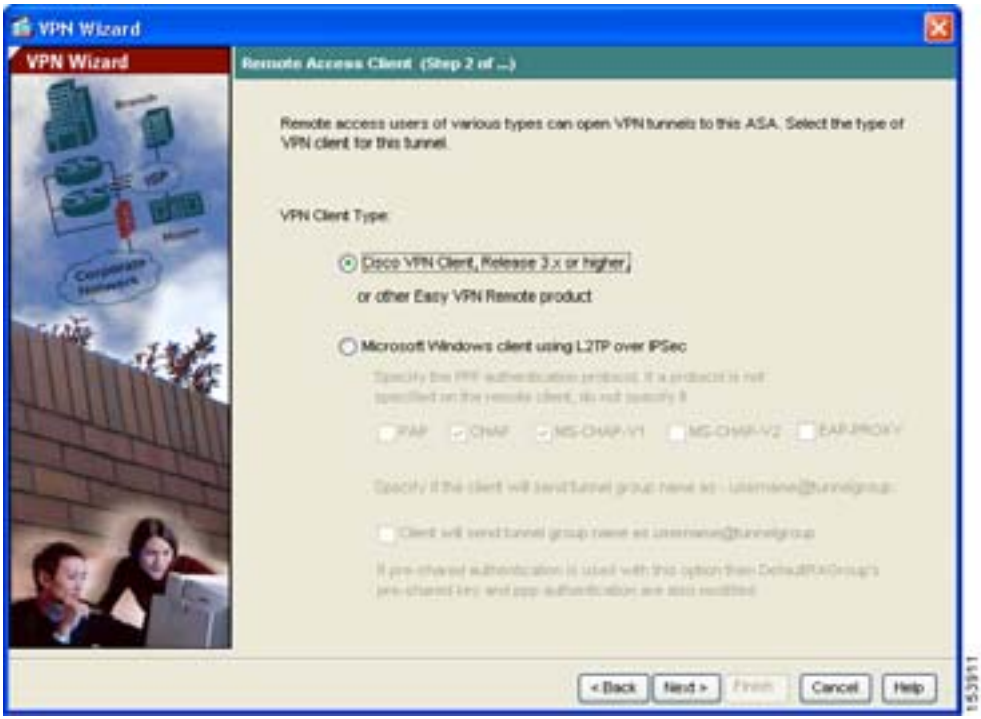
c. **Next** をクリックして続行します。

VPN クライアント タイプの選択

VPN Wizard の Step 2 で、次の手順に従います。

ステップ 1　この適応型セキュリティ アプライアンスに接続するリモート ユーザを有効にする 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。

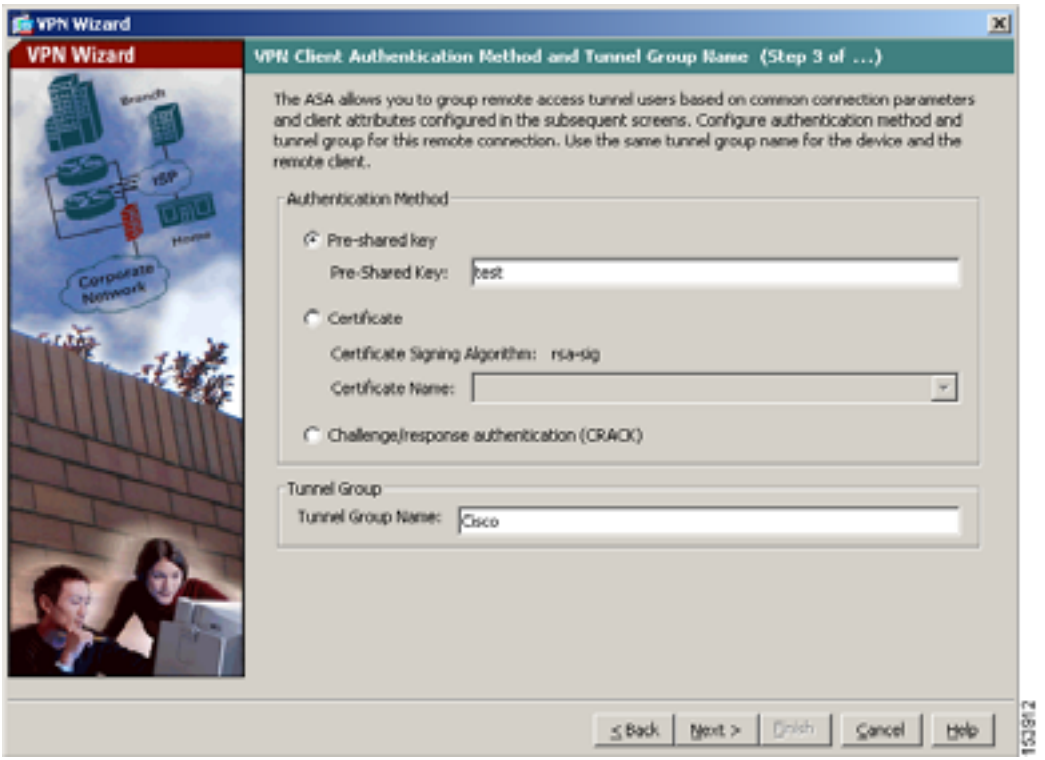
VPN トンネル グループ名と認証方式の指定

VPN Wizard の Step 3 で、次の手順に従います。

ステップ 1　次のいずれかの操作を実行して、使用する認証のタイプを指定します。

- 認証にスタティック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（たとえば、「Cisco」）を入力します。このキーは、適応型セキュリティ アプライアンス間の IPSec ネゴシエーションで使用されます。
- 認証にデジタル証明書を使用するには、**Certificate** オプション ボタンをクリックし、ドロップダウン リストから証明書署名アルゴリズムを選択し、次に、事前設定されているトラストポイント名をドロップダウン リストから選択します。

  認証にデジタル証明書を使用する予定で、まだトラストポイント名を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ウィザードを続行できます。認証設定は、標準 ASDM ウィンドウを使用して後で修正できます。
- **Challenge/Response Authentication (CRACK)** オプション ボタンをクリックすると、この認証方式を使用できます。



ステップ 2　共通の接続パラメータおよびクライアント　アトリビュートを使用して、この適応型セキュリティ アプライアンスに接続する複数ユーザのセットのトンネル グループ名（たとえば、「Cisco」）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

ユーザの認証は、ローカル認証データベース、または外部の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバを使用して実行できます（AAA サーバには RADIUS、TACACS+、SDI、NT、Kerberos、および LDAP があります）。

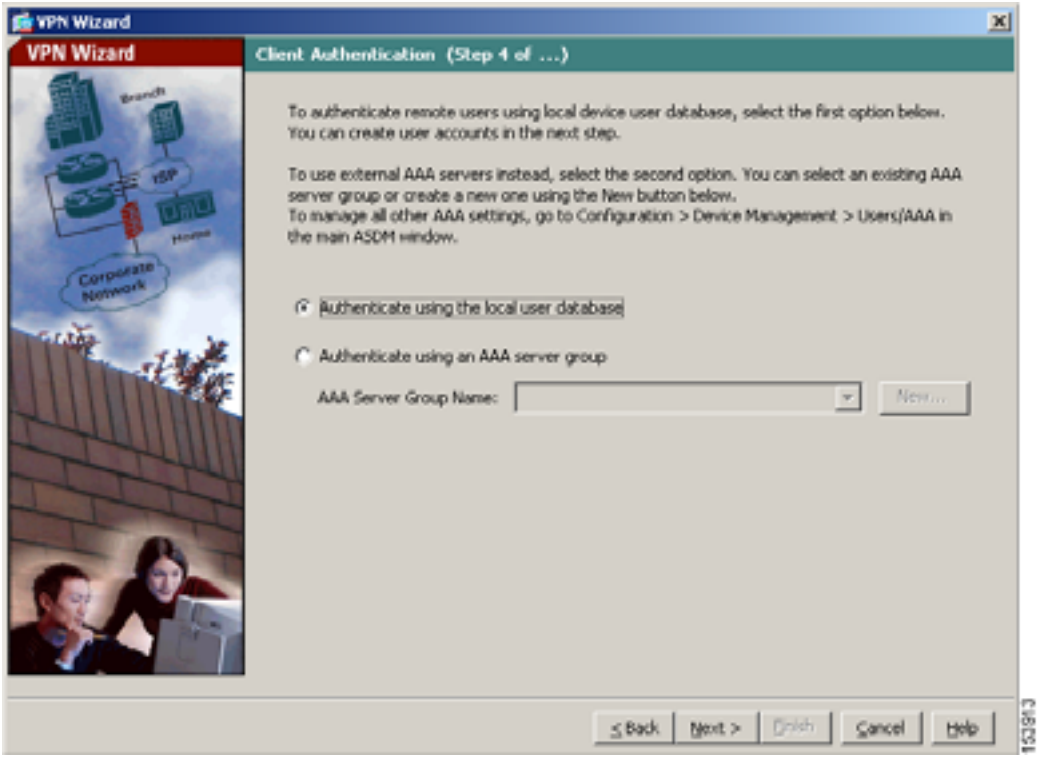
VPN Wizard の Step 4 で、次の手順に従います。

ステップ 1　適応型セキュリティ アプライアンスにユーザ データベースを作成してユーザを認証するには、**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 グループを使用してユーザを認証する場合は、次の手順に従います。

a. **Authenticate Using an AAA Server Group** オプション ボタンをクリックします。

b. 事前設定されているサーバ グループを Authenticate using an AAA Server Group ドロップダウン リストから選択するか、**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。



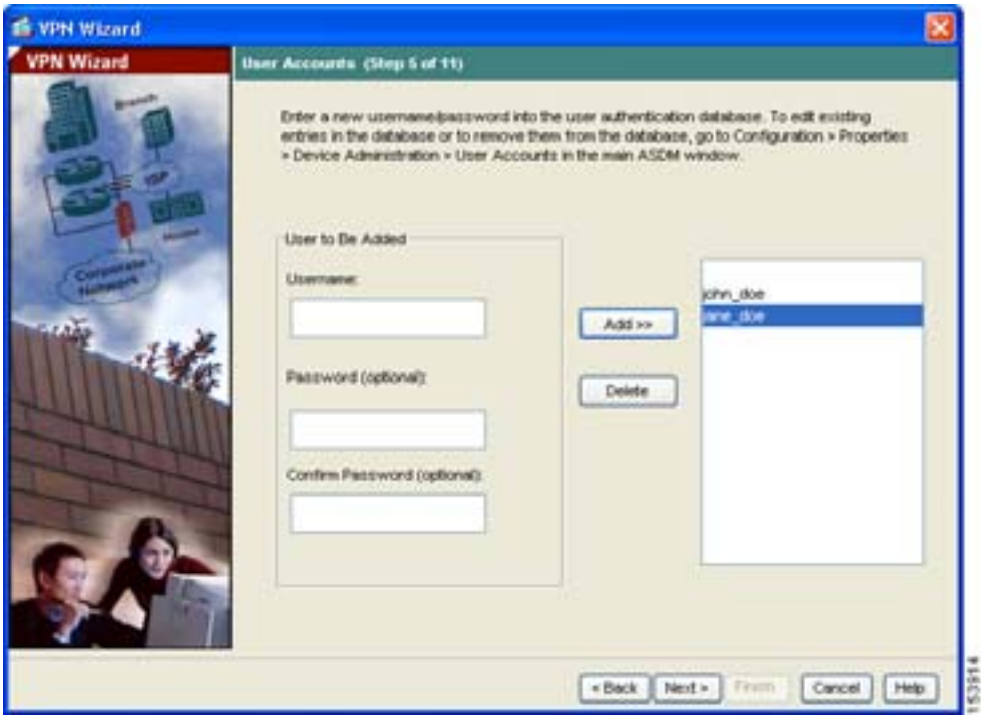
ステップ 3　**Next** をクリックして続行します。

（オプション）ユーザ アカウントの設定

ローカル ユーザ データベースを使用してユーザを認証する場合、次の手順で新しいユーザ 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、次の手順に従います。

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

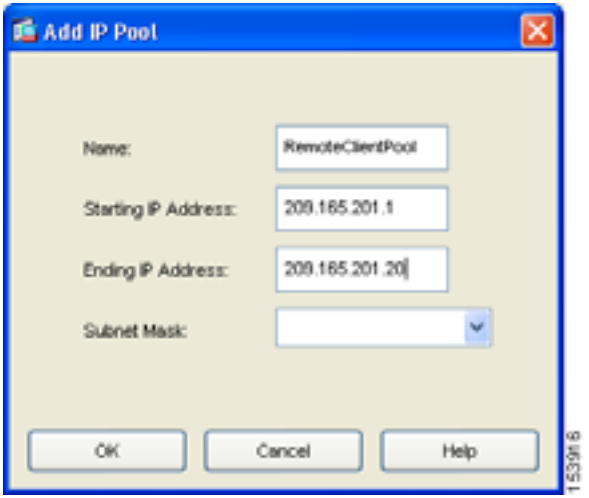
リモート クライアントがネットワークにアクセスするには、接続に成功したときにリモート VPN クライアントに割り当てられる可能性のある IP アドレスのプールを設定する必要があります。このシナリオでは、プールは 209.165.201.1 ～ 209.166.201.20 の範囲の IP アドレスを使用するように設定します。

VPN Wizard の Step 6 で、次の手順に従います。

ステップ 1　プール名を入力するか、事前設定されているプールを Name ドロップダウン リストから選択します。

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。

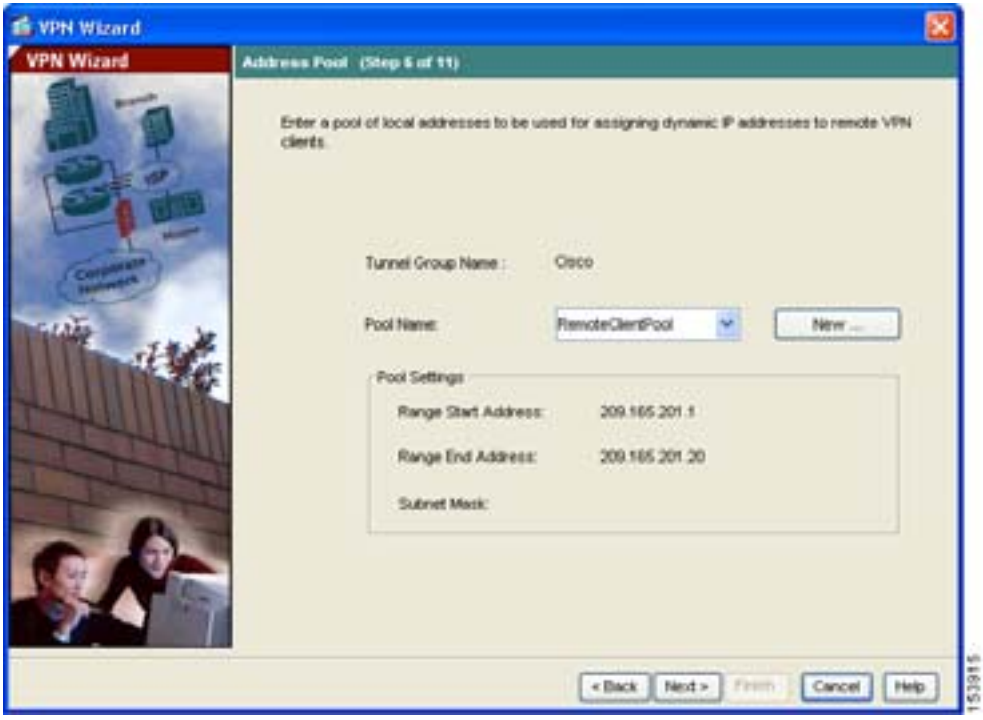


ステップ 2　Add IP Pool ダイアログボックスで、次の内容を実行します。

a. 範囲の開始 IP アドレスと終了 IP アドレスを入力します。

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。

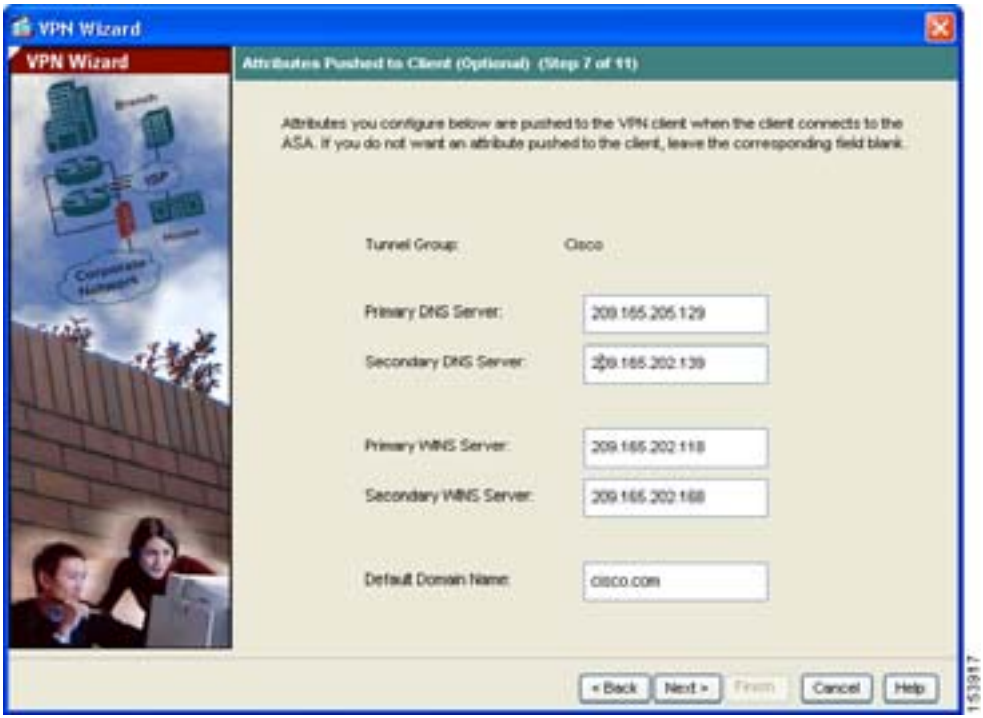
クライアント アトリビュートの設定

各リモート アクセス クライアントがネットワークにアクセスするには、使用する DNS サーバと WINS サーバ、デフォルトのドメイン名などの基本的なネットワーク設定情報が必要です。各リモート クライアントを個々に設定するのではなく、ASDM にクライアント情報を設定できます。接続が確立されると、適応型セキュリティ アプライアンスは、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 クライアントに適用します。

必ず正しい値を指定してください。値が正しくない場合、リモート クライアントが解決に DNS 名を使用できない、または Windows ネットワーキングを使用できないという問題が発生します。

VPN Wizard の Step 7 で、次の手順に従います。

ステップ 1　リモート クライアントに適用するネットワーク設定情報を入力します。



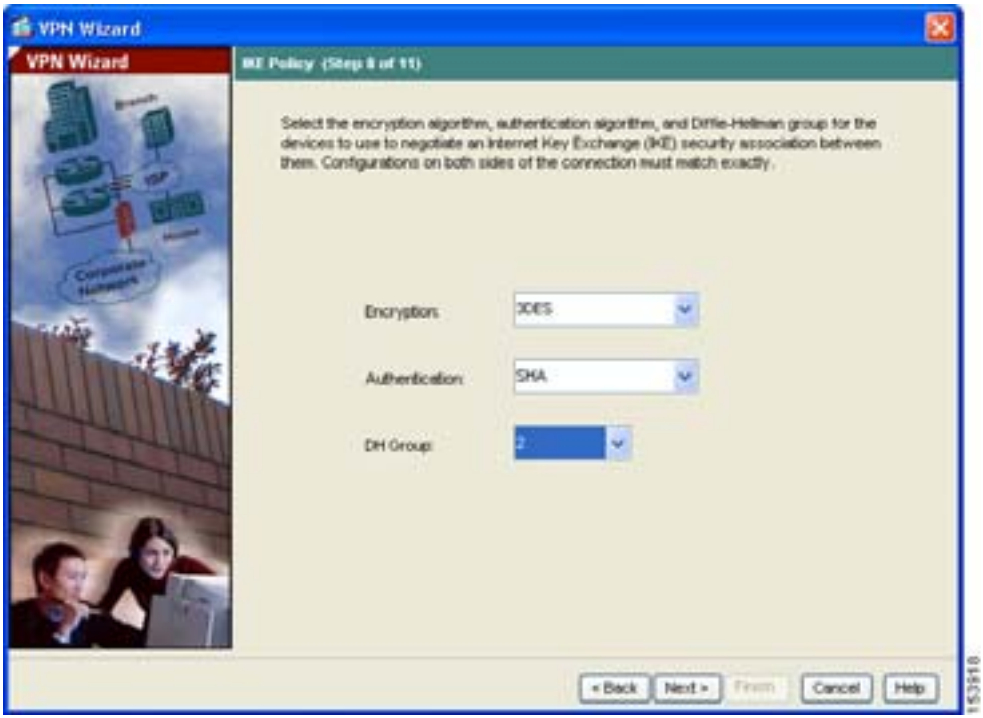
ステップ 2　**Next** をクリックして続行します。

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 を確認する認証方式でもあります。ほとんどの場合、ASDM のデフォルト値を使用すれば、十分にセキュアな 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、次の手順に従います。

ステップ 1　IKE セキュリティ アソシエーションにおいて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）を選択します。

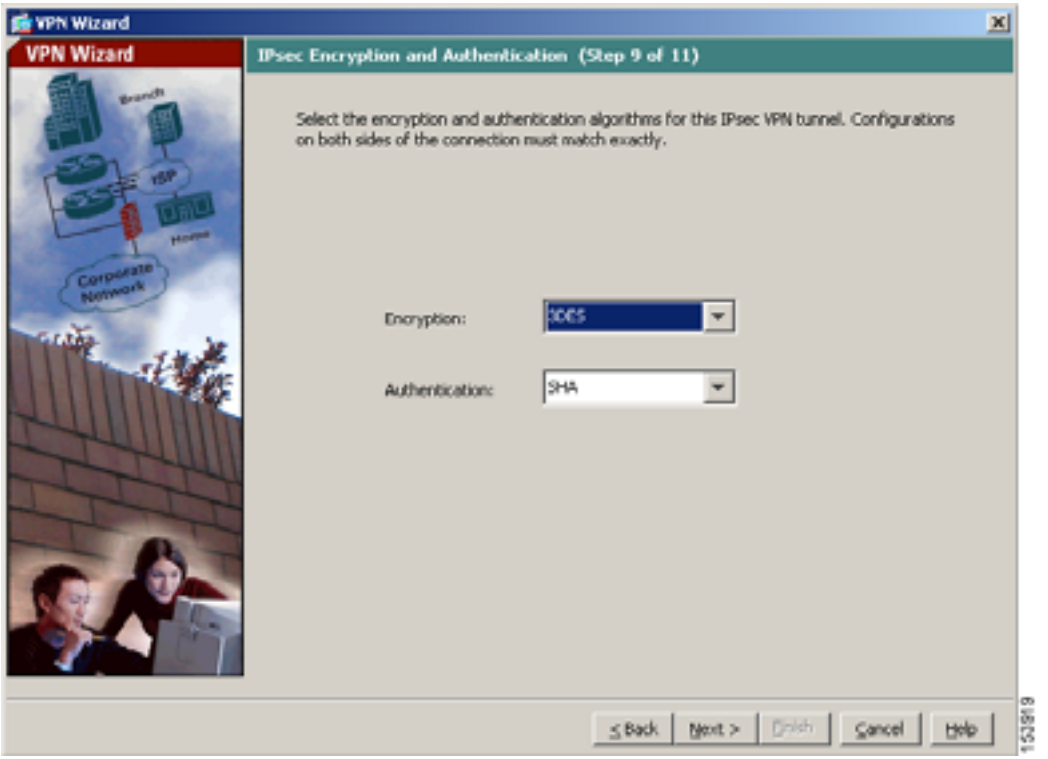


ステップ 2　**Next** をクリックして続行します。

IPSec Encryption パラメータ および Authentication パラメータの設定

VPN Wizard の Step 9 で、次の手順に従います。

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およびスプリット トンネリングの指定

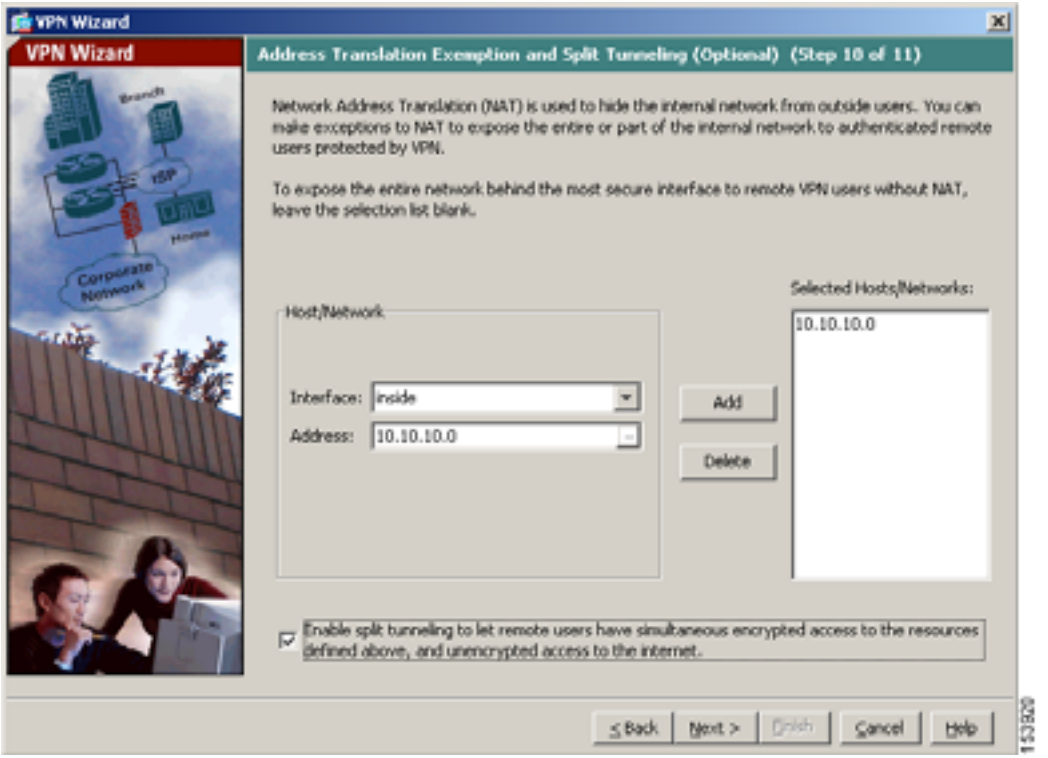
スプリット トンネリングを使用すると、リモートアクセス IPSec クライアントは、パケットを条件によって、IPSec トンネル経由で送信すること（暗号化形式）や、ネットワーク インターフェイスに送信すること（テキスト形式）ができます。

適応型セキュリティ アプライアンスは、Network Address Translation（NAT; ネットワーク アドレス変換）を使用して、内部 IP アドレスが外部に公開されないようにしています。認証されたリモート ユーザにアクセスを許可するローカル ホストおよびネットワークを特定することで、このネットワーク保護に例外を設定できます。

VPN Wizard の Step 10 で、次の手順に従います。

ステップ 1　認証されたリモート ユーザにアクセスを許可する内部リソースのリストに入れるホスト、グループ、およびネットワークを指定します。

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

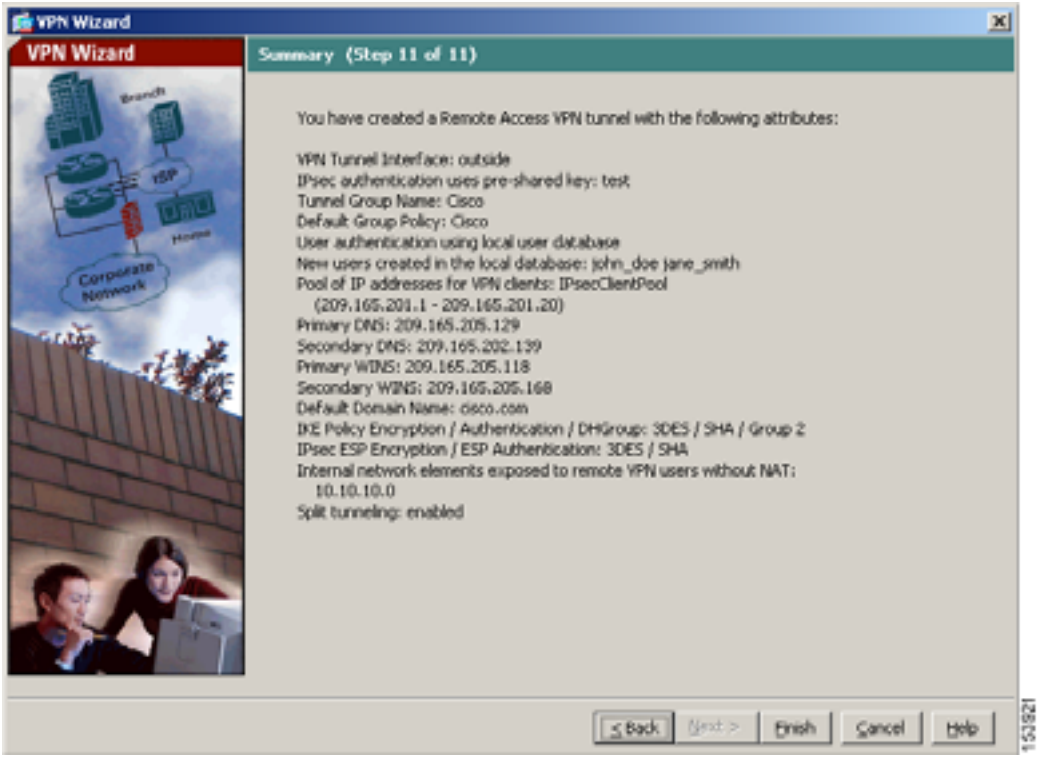


(注)　画面下部の **Enable Split Tunneling ...** チェックボックスをオンにすると、スプリット トンネリングがイネーブルになります。スプリット トンネリングを使用すると、設定したネットワークの外部のトラフィックは、暗号化された VPN トンネルを経由せずにインターネットに直接送信されます。

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。



適切に設定されている場合は **Finish** をクリックして、適応型セキュリティ アプライアンスに変更内容を適用します。

次にデバイスを起動するときに適用されるように、設定変更をスタートアップ コンフィギュレーションに保存する場合は、File メニューから **Save** をクリックします。または、ASDM を終了するときに設定変更を半永久的に保存するように求められます。

設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそのまま適用されます。

次の作業

モバイル従業員またはテレワーカー向けの安全な接続用に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ます。

Cisco Systems 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 環境だけに適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が終了しました。さらに、次の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco Security Appliance Command Line Configuration Guide*』
日常的な運用について	『*Cisco Security Appliance Command Reference*』 『*Cisco Security Appliance Logging Configuration and System Log Messages*』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

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

CHAPTER 8

シナリオ：サイトツーサイト VPN 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 アプライアンスに備わっているサイトツーサイト VPN 機能を使用すると、企業はネットワーク セキュリティを維持したまま、ネットワークを拡張してビジネス パートナーや世界中のリモート オフィスとの間で低コストのパブリック インターネット接続を実現できます。VPN 接続では、セキュアな接続、つまりトンネル経由で 1 つの場所から別の場所へデータを送信できます。これは、まず接続の両端を認証し、次に 2 つのサイト間で送信されるすべてのデータを自動的に暗号化することによって可能になります。

この章には、次の項があります。

サイトツーサイト VPN ネットワーク トポロジの例

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

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

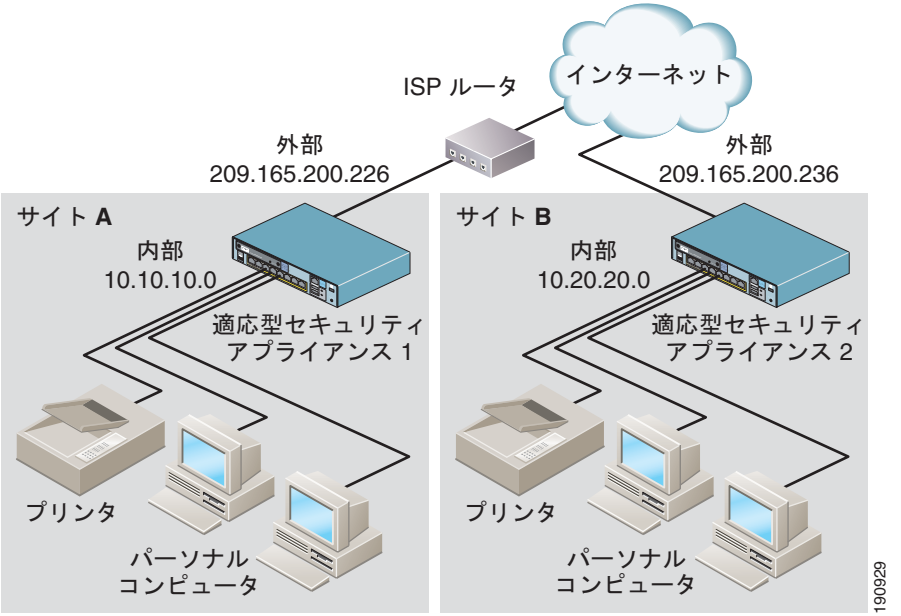


図 8-1 のような VPN サイトツーサイト構成を作成するには、2 台の適応型セキュリティ アプライアンスを設定する必要があります（接続のそれぞれの側に 1 台ずつ）。

サイトツーサイト シナリオの実装

この項では、図 8-1 に表示されているリモートアクセス 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 構成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。

この項は、次の内容で構成されています。

収集する情報

この設定手順を開始する前に、次の情報を取得します。

- リモートの適応型セキュリティ アプライアンス ピアの IP アドレス
- リモート　サイト上のリソースとの通信にトンネルを使用することが許可されたローカル ホストとネットワークの IP アドレス
- ローカル　リソースとの通信にトンネルを使用することが許可されたリモート ホストとネットワークの IP アドレス

サイトツーサイト VPN の設定

ここでは、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。

この項は、次の内容で構成されています。

次の項では、各設定手順を実行する方法を詳細に説明します。

ASDM の起動

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

（注） 「**https**」の「**s**」を付け忘れると、接続は失敗します。HTTP over SSL（HTTPS）を使用すると、ブラウザと適応型セキュリティ アプライアンスとの間の安全な接続が可能になります。

ASDM 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 Security Appliance 1 と呼びます。

Security Appliance 1 を設定するには、次の手順に従います。

ステップ 1　ASDM メイン ウィンドウで、Wizards ドロップダウン メニューから VPN Wizard オプションを選択します。ASDM で、最初の VPN Wizard 画面が開きます。

VPN Wizard の Step 1 で、次の手順に従います。

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

（注） Site-to-Site VPN オプションを選択すると、2 つの IPSec セキュリティ ゲートウェイが接続されますが、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る可能性があります。

b. VPN Tunnel Interface ドロップダウン リストから、現在の VPN トンネルで有効な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もう一方の端にあるシステムで、通常はリモート 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 Security Appliance 2 と呼びます。

VPN Wizard の Step 2 で、次の手順に従います。

ステップ 1　リモートのピアの IP アドレス（209.165.200.236）およびトンネル グループ名（たとえば、「Cisco」）を入力します。

ステップ 2　次のいずれかの認証方式を選択して、使用する認証のタイプを指定します。

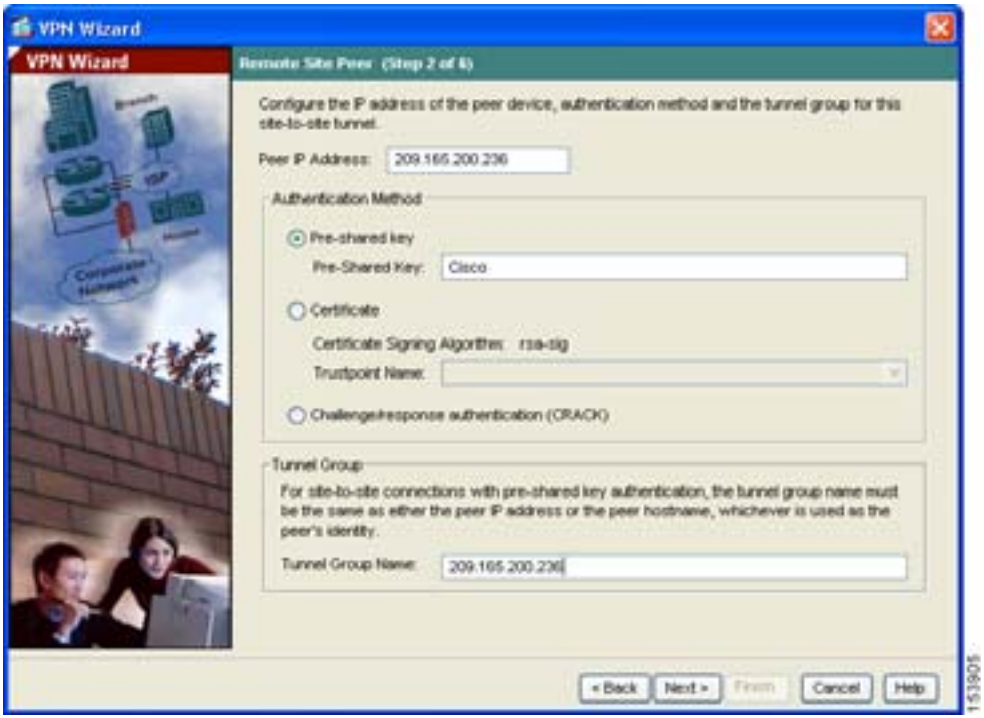
- 認証にスタティック事前共有キーを使用するには、**Pre-Shared Key** オプション ボタンをクリックし、事前共有キー（たとえば、「Cisco」）を入力します。このキーは、適応型セキュリティ アプライアンス間の IPSec ネゴシエーションで使用されます。

  （注） このシナリオのように、事前共有キー認証を使用したサイトツーサイト接続を行う場合、トンネル グループ名は、ピアの IP アドレスとピアのホスト名のうち、ピアの ID として使用されているものと同一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 リストから証明書署名アルゴリズムを選択し、次に、事前設定されているトラストポイント名を Trustpoint Name ドロップダウン リストから選択します。

  認証にデジタル証明書を使用する予定で、まだトラストポイント名を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ウィザードを続行できます。認証設定は、同じ ASDM 画面を使用して後で修正できます。

- **Challenge/Response Authentication** オプション ボタンをクリックして、この認証方式を使用できます。



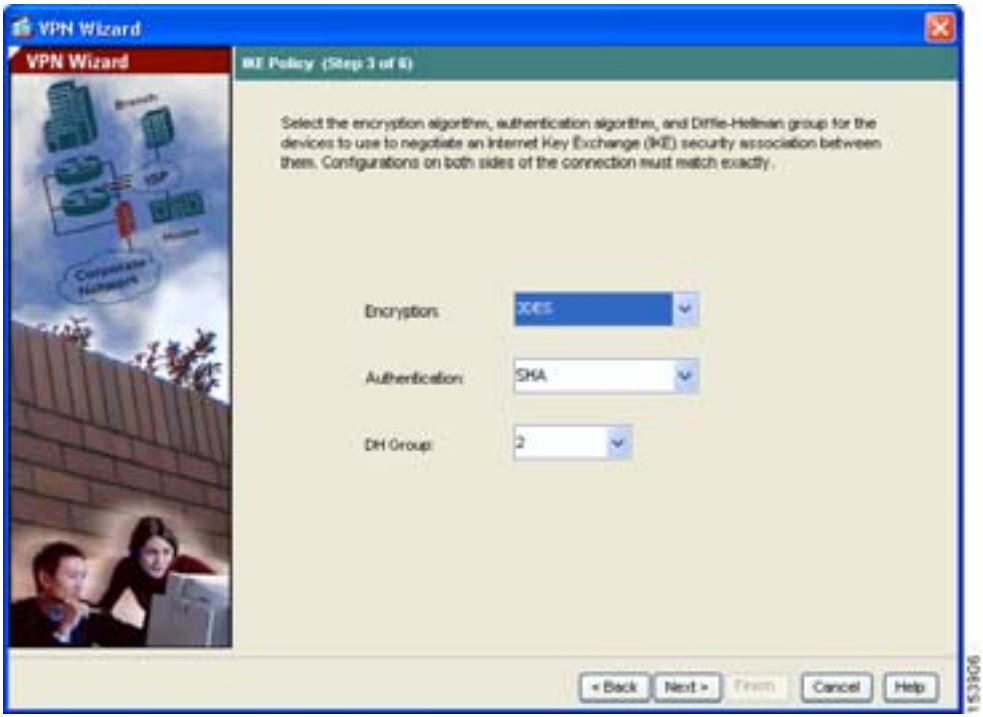
ステップ 3　**Next** をクリックして続行します。

IKE ポリシーの設定

IKE は、セキュアな VPN トンネルを通じてデータの完全性を保護し、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 のデフォルト値を使用すれば、十分にセキュアな VPN トンネルを 2 つのピア間に確立できます。

VPN Wizard の Step 3 で、次の手順に従います。

ステップ 1　IKE セキュリティ アソシエーションにおいて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。



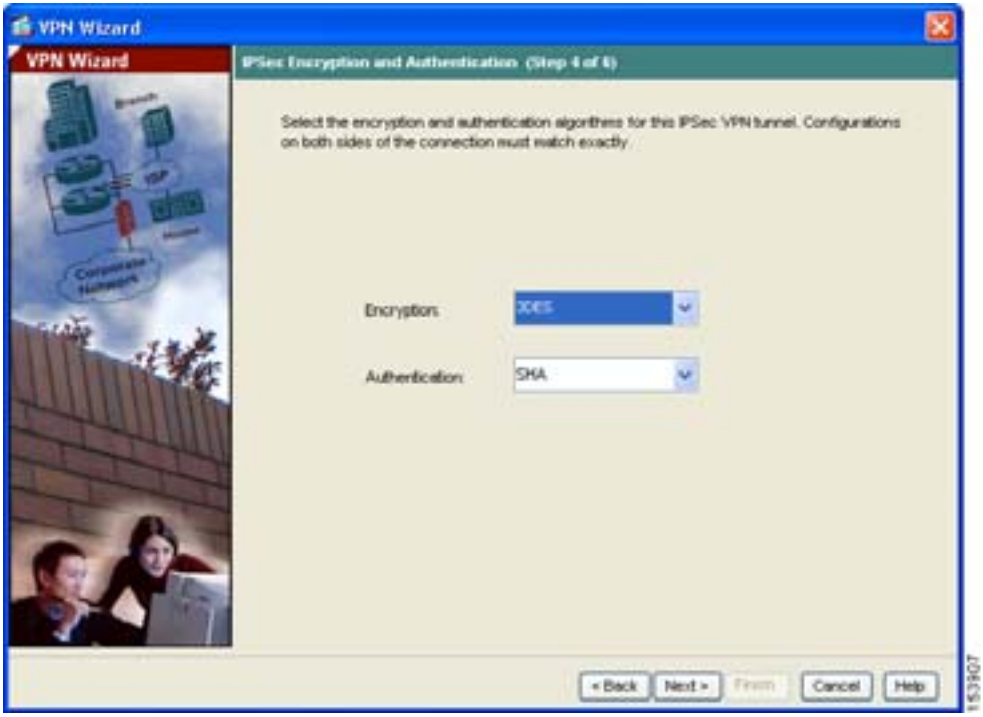
（注） Security Appliance 2 を設定する場合は、Security Appliance 1 で選択した各オプションと同じ値を入力します。VPN トンネルが失敗し、処理速度を低下させる一般的な原因は、暗号化の不整合です。

ステップ 2　**Next** をクリックして続行します。

IPSec Encryption パラメータおよび Authentication パラメータの設定

VPN Wizard の Step 4 で、次の手順に従います。

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、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

トンネルの反対側のホストおよびネットワークとの通信にこの IPSec トンネルを使用することが許可されたローカル 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、トンネルへのアクセスが許可された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、ネットワーク A（10.10.10.0）からのトラフィックは Security Appliance 1 によって暗号化され、VPN トンネル経由で送信されます。

さらに、ローカル ホストおよびネットワークへのアクセスにこの IPSec トンネルを使用することを許可するリモート 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するには **Add**、削除するには **Delete** をクリックします。このシナリオにおいて、Security Appliance 1 では、リモート ネットワークはネットワーク B（10.20.20.0）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経由で許可されます。

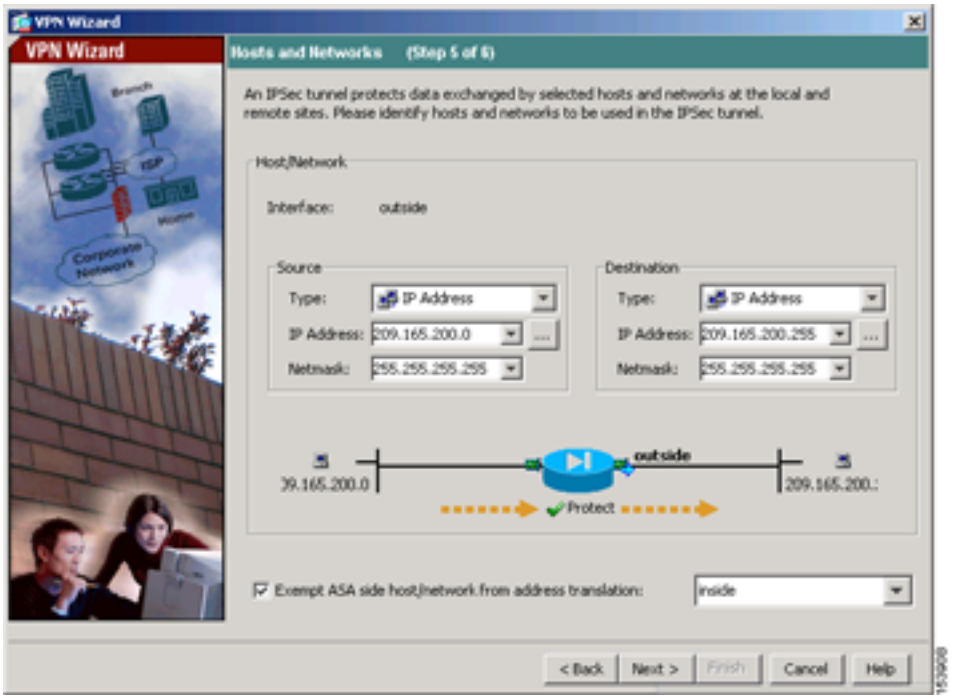
VPN Wizard の Step 5 で、次の手順に従います。

（注） ここでは、暗号化による保護により、セキュアな VPN トンネルを通じて 2 つのホスト間のデータ完全性が保たれます。あるホストから別のホストに、セキュアでない接続で暗号化されずに送信される平文の情報は、保護されていないデータと考えられます。保護されていないデータをセキュアでない接続で送信すると、データが改ざんされる可能性があります。

ステップ 1　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 2　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。

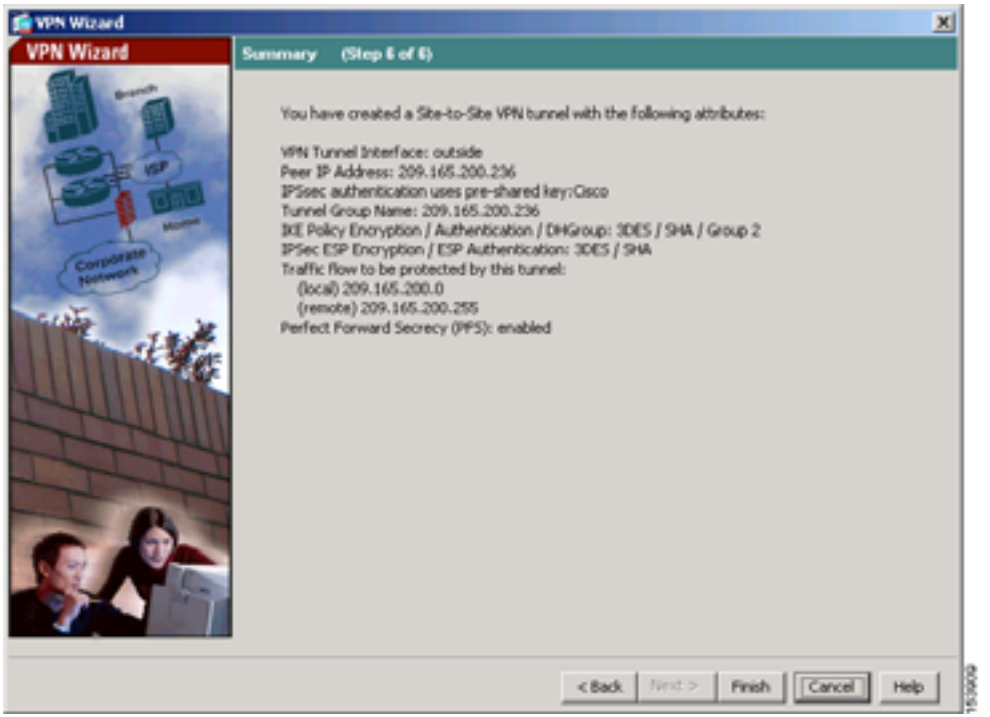
（注） リモートのピアが動的 IP アドレスを持っている場合は、ピアの IP アドレスとしてホスト名を使用できます。



ステップ 3　**Next** をクリックして続行します。

VPN アトリビュートの表示とウィザードの終了

VPN Wizard の手順 6 では、作成した VPN トンネルの設定を確認します。適切に設定されている場合は、**Finish** をクリックして、適応型セキュリティ アプライアンスに変更内容を適用します。



ステップ 4　次にデバイスを起動するときに適用されるように、設定変更をスタートアップ コンフィギュレーションに保存する場合は、File メニューから **Save** をクリックします。

または、ASDM を終了するときに設定変更を半永久的に保存するように求められます。

設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそのまま適用されます。

この操作により、Security Appliance 1 の設定プロセスが終了します。

VPN 接続の反対側の設定

これで、ローカルの適応型セキュリティ アプライアンスの設定は完了しました。次は、リモート サイトで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 ピアとしての役割を果たす 2 つ目の適応型セキュリティ アプライアンスを設定します。ローカルの適応型セキュリティ アプライアンスを設定したときと同じ手順を使用します。「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」（8-5 ページ）から開始し、「VPN アトリビュートの表示とウィザードの終了」（8-14 ページ）で終了します。

（注） Security Appliance 2 を設定する場合、ローカル ホストおよびネットワークを除いて、Security Appliance 1 で選択した各オプションと同じ値を使用します。VPN 構成が失敗する一般的な原因は、不整合です。

次の作業

サイトツーサイト VPN 環境だけに適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が完了しました。さらに、次の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco Security Appliance Command Line Configuration Guide*』
日常的な運用について	『*Cisco Security Appliance Command Reference*』 『*Cisco Security Appliance Logging Configuration and System Log Messages*』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

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

CHAPTER 9

シナリオ：Easy VPN ハードウェア クライアント設定

この章では、Easy VPN ハードウェア クライアントとして機能する ASA 5505 の設定方法について説明します。ASA 5505 は、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を編成する複数のデバイスから成る Easy VPN 構成の一環として使用できます。

この章には、次の項があります。

Easy VPN ハードウェア クライアントとしての ASA 5505 の使用

Cisco Easy VPN ハードウェア クライアント（別名、「Easy VPN リモート デバイス」）を使用すると、複数のサイトを利用している企業はこれらのサイト間の安全な通信を確立して、リソースを共有できます。Cisco Easy VPN ソリューションは、メイン サイトの Easy VPN サーバとリモート オフィスの Easy VPN ハードウェア クライアントで構成されています。

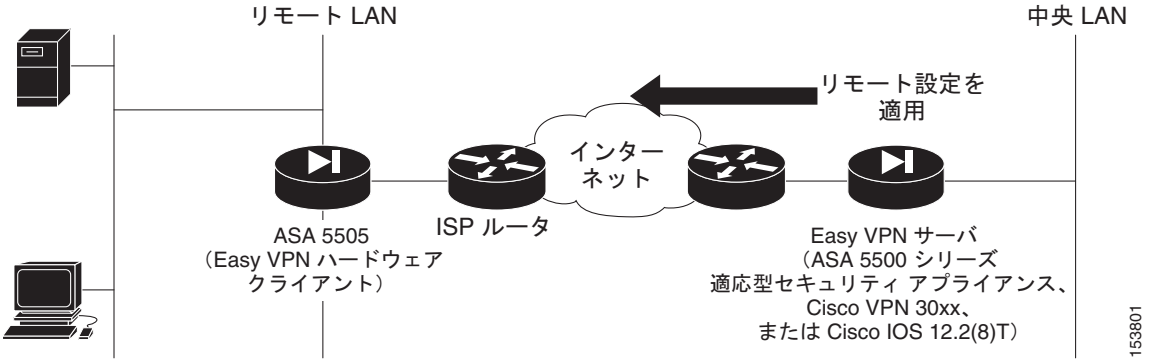
Cisco ASA 5505 は、Cisco Easy VPN ハードウェア クライアントまたは Cisco Easy VPN サーバ（別名、「ヘッドエンド デバイス」）として機能することができますが、同時に両方の役割を果たすことはできません。

Easy VPN ソリューションを使用すると、次の方法で VPN の構成と管理が簡素化されます。

- リモート サイトのホストが VPN クライアント ソフトウェアを実行する必要がなくなる。
- 中央サーバにセキュリティ ポリシーが常駐し、VPN 接続が確立されると、セキュリティ ポリシーがリモート ハードウェア クライアントに適用される。
- ローカルに設定する必要がある設定パラメータがほとんどないため、オンサイト管理の必要性を最小限に抑えられる。

図9-1 に、Easy VPN コンポーネントを展開して、VPN を作成する方法を示します。

図 9-1　VPN の Easy VPN コンポーネント



Easy VPN ハードウェア クライアントとして使用する場合、不正アクセスから DMZ 内のデバイスを保護するなどの基本的なファイアウォール サービスを実行するように ASA 5505 を設定することもできます。ただし、ASA 5505 が Easy VPN ハードウェア クライアントとして機能するように設定されている場合は、他のタイプのトンネルを確立できません。たとえば、ASA 5505 は、Easy VPN ハードウェア クライアントとして機能すると同時に標準ピアツーピア VPN 構成の片方の終端として機能することはできません。

クライアント モードと NEM

Easy VPN ハードウェア クライアントは、クライアント モードまたは Network Extension Mode（NEM; ネットワーク拡張モード）の 2 つの運用モードのいずれかをサポートします。運用モードは、Easy VPN ハードウェア クライアントの背後にあるホストが、トンネルを経由したエンタープライズ ネットワークからアクセス可能かどうかを決定します。

クライアント モードは、Port Address Translation（PAT; ポート アドレス変換）モードとも呼ばれ、Easy VPN クライアント プライベート ネットワークのすべてのデバイスをエンタープライズ ネットワークのデバイスから分離します。Easy VPN クライアントは、内部ホストのすべての VPN トラフィックに対して PAT を実行します。IP アドレスの管理は、Easy VPN クライアントの内部インターフェイスおよび内部ホストのどちらでも必要ありません。

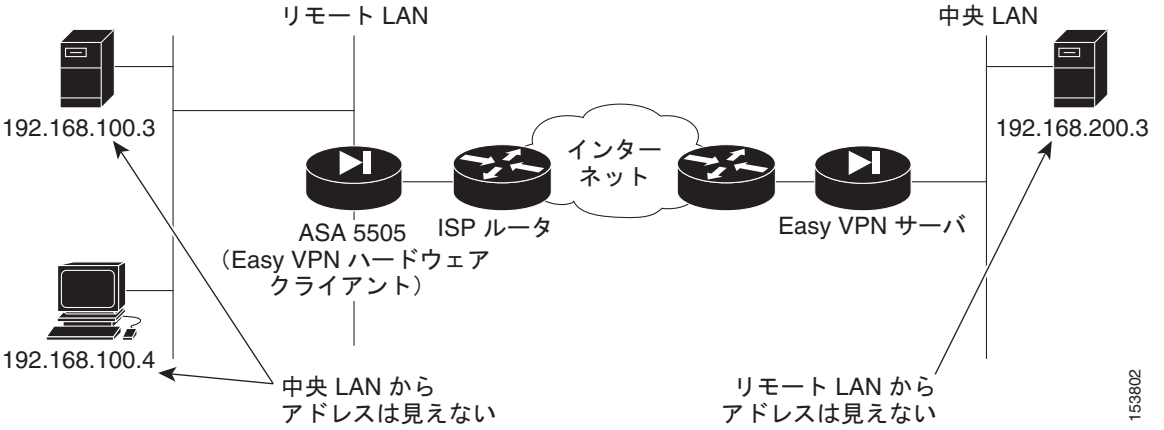
NEM では、内部インターフェイスとすべての内部ホストは、トンネルを経由してエンタープライズ ネットワークにルーティングできます。内部ネットワークのホストは、スタティック IP アドレスが事前に設定されたアクセス可能なサブネットから（スタティックに、または DHCP を使用して）IP アドレスを取得します。NEM では、PAT は VPN トラフィックに適用されません。このモードでは、各クライアントに VPN を設定する必要がありません。NEM モードに設定された ASA 5505 は、トンネルの自動開始をサポートしています。この設定には、グループ名、ユーザ名、およびパスワードが保存される必要があります。

セキュア ユニット認証がイネーブルの場合は、トンネルの自動開始がディセーブルになります。Easy VPN クライアントのプライベート側のネットワークとアドレスは隠蔽され、直接アクセスできません。

Easy VPN ハードウェア クライアントには、デフォルト モードがありません。ただし、ASDM でモードを指定しない場合は、ASDM が自動的にクライアント モードを選択します。CLI を使用して Easy VPN ハードウェア クライアントを設定する場合は、モードを指定する必要があります。

図 9-2 に、Easy VPN クライアント モードで稼働している ASA 5505 のサンプル ネットワーク トポロジを示します。クライアント モードに設定している場合、Easy VPN サーバの背後にあるデバイスは ASA 5505 の内部インターフェイスのデバイスにアクセスできません。

図 9-2　クライアント モードで稼働している ASA 5505 のトポロジ

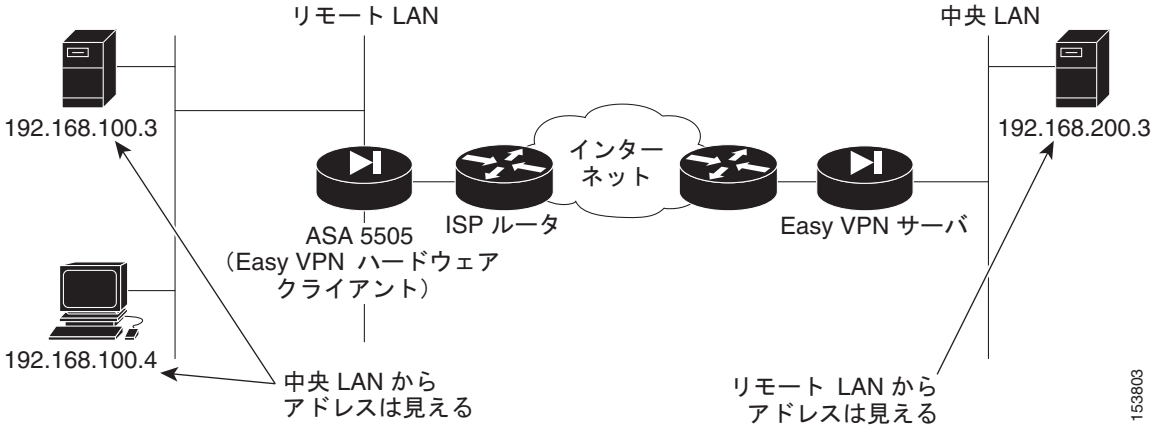


Easy VPN NEM に設定している場合、ASA 5505 は、パブリック IP アドレスを代用することにより、ローカル ホストの IP アドレスを隠蔽しません。したがって、VPN 接続の反対側のホストは、ローカル ネットワーク上のホストと直接通信できます。

NEM を設定する場合、Easy VPN クライアントの背後にあるネットワークが Easy VPN サーバの背後にあるネットワークと重ならないようにする必要があります。

図 9-3 に、NEM で稼働している ASA 5505 のサンプル ネットワーク トポロジを示します。

図 9-3　NEM で稼働している ASA 5505 のネットワーク トポロジ



ASA 5505 を Easy VPN クライアント モードまたは NEM のどちらに設定するかを決めるには、次のガイドラインを使用します。

次の場合は、クライアント モードを使用します。

- Easy VPN ハードウェア クライアントの背後にあるデバイスがエンタープライズ ネットワークのデバイスへのアクセスを試みるときに、VPN 接続を開始する場合。
- エンタープライズ ネットワークのデバイスが Easy VPN ハードウェア クライアントの背後にあるデバイスにアクセスできないようにする場合。

次の場合は、NEM を使用します。

- VPN　接続を自動的に確立し、トラフィックを転送する必要がない場合でも確立された状態を保つ場合。
- リモート デバイスが Easy VPN ハードウェア クライアントの背後にあるホストにアクセスできるようにする場合。

Easy VPN ハードウェア クライアントの設定

Easy VPN サーバは、ASA 5505 Easy VPN ハードウェア クライアントに適用されているセキュリティ ポリシーをコントロールします。ただし、Easy VPN サーバへの初期接続を確立するには、一部の設定をローカルで行う必要があります。

ASDM またはコマンドライン インターフェイスを使用して、この設定手順を実行できます。この項では、ASDM を使用して設定を実行する方法について説明します。

Easy VPN ハードウェア クライアントとして ASA 5505 を設定するには、次の手順に従います。

ステップ 1　ASA 5505 の内部インターフェイスへのアクセスを持つ PC で、ASDM を起動します。

a. Web ブラウザを起動します。

b. ブラウザのアドレス フィールドに工場出荷時のデフォルト IP アドレス **https://192.168.1.1/** を入力します。

（注）「**https**」の「**s**」を付け忘れると、接続は失敗します。HTTP over SSL（HTTPS）を使用すると、ブラウザと適応型セキュリティ アプライアンスとの間の安全な接続が可能になります。

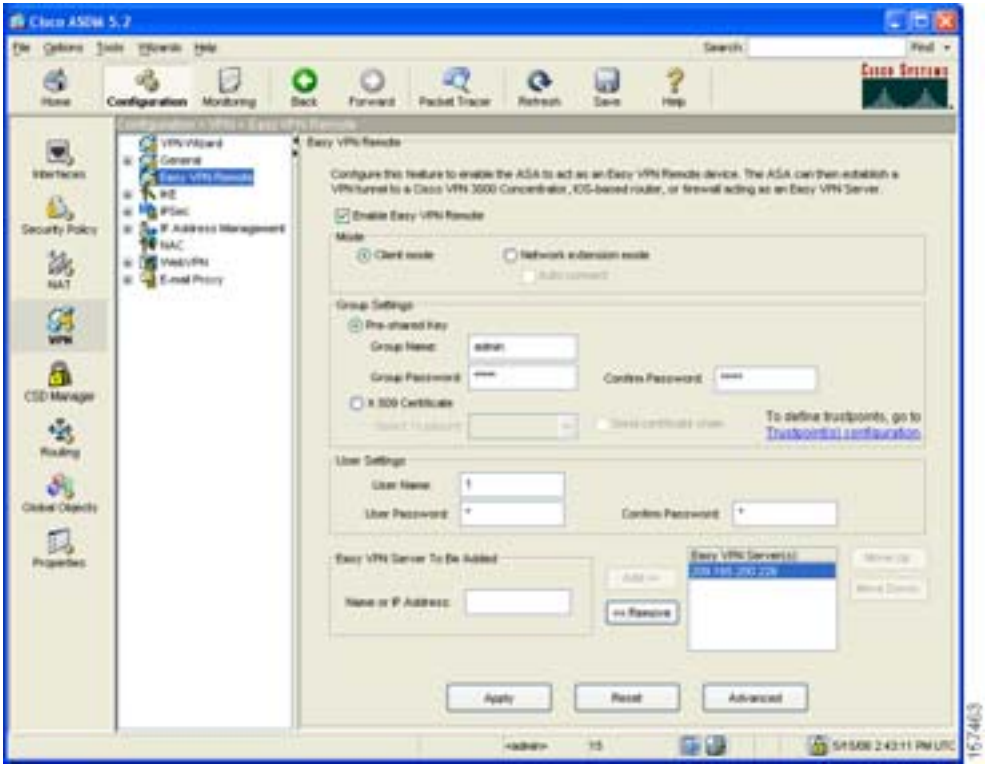
c. ASDM ソフトウェアを実行するのに使用する方法を選択するウィンドウで、ASDM Launcher をダウンロードするか、ASDM ソフトウェアを Java アプレットとして実行するかを選択します。

ステップ 2　ASDM ウィンドウで、**Configuration** ツールをクリックします。

ステップ 3　**VPN** ツールをクリックし、**Enable Easy VPN Remote** チェックボックスをオンにします。

Enable Easy VPN Remote チェックボックスをオンにした場合、Apply をクリックすると、デバイスで Easy VPN がイネーブルになります。チェックボックスをオンにしない場合、設定変更を適用したときに、すべての Easy VPN 設定をクリアするか、一時的に Easy VPN クライアントをディセーブルにするだけかを指定するように求められます。

Easy VPN Remote 設定ペインが表示されます。



ステップ 4　**Enable Easy VPN Remote** チェックボックスをオンにします。

ステップ 5　Easy VPN リモート ハードウェア クライアントで実行するモードを指定するには、**Client Mode** または **Network Extension Mode** オプション ボタンをクリックします。

ステップ 6　Group Settings 領域で、VPN デバイスが使用する認証タイプを指定します。

- VPN デバイスが認証時にテキスト パスワードを使用するように指定するには、**Group Password** オプション ボタンをクリックし、Group Name と Group Password を入力します。

ステップ 7　User Settings 領域で、ASA 5505 が VPN 接続を確立するときに使用する User Name と User Password を指定します。

ステップ 8　このデバイスが VPN セキュリティ ポリシーを取得する Easy VPN サーバを 1 つ以上指定します。

a.　Easy VPN Server To Be Added 領域で、Easy VPN サーバのホスト名または IP アドレスを入力します。

b.　**Add** または **Remove** をクリックして、Easy VPN サーバ リストにサーバを追加するか、Easy VPN サーバ リストからサーバを削除します。

リストに表示される最初のサーバは、プライマリ サーバとして使用されます。リストの他のサーバは、冗長性を提供します。Cisco VPN 3000 シリーズ コンセントレータをヘッドエンド デバイスとして使用している場合は、リストのすべてのサーバの負荷を分散するように、コンセントレータを設定できます。

最大 9 台のバックアップ サーバを指定できます（サーバの合計最大数は 10 台になります）。

ステップ 9　**Apply** をクリックして、適応型セキュリティ アプライアンスに設定を適用します。

設定を保存するには、一番上のツールバーの **Save** ボタンをクリックします。

高度な Easy VPN アトリビュートの設定

使用中のネットワークが次の条件に一致する場合、いくつかの高度な設定タスクを実行しなければならない可能性があります。

- 使用中のネットワークに認証を実行できないデバイスがあり、個々のユニット認証に加えることができない場合。たとえば、Cisco IP Phone、プリンタなどのデバイスが含まれます。

  このようなデバイスに対応するために、デバイスのパススルー機能をイネーブルにすることができます。

- 使用中の ASA 5505 が NAT デバイスの背後で動作している場合。

  この場合、トンネル型管理アトリビュートを使用して、デバイスの管理をトンネル経由で行うかどうか、トンネルを経由して Easy VPN 接続を管理することがネットワークで許可されているかどうかを指定する必要があります。

（注） NAT デバイスにスタティック NAT マッピングを追加する場合を除いて、NAT デバイスの背後にある場合、ASA 5505 のパブリック アドレスにはアクセスできません。

これらのアトリビュートを設定するには、Easy VPN Remote 設定ペインで **Advanced** をクリックします。設定の具体的な内容については、オンライン ヘルプを参照してください。

次の作業

Easy VPN ハードウェア クライアントとしてだけ適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が完了しました。次の追加の手順を実行することもできます。

実行内容	参照先
DMZ Web サーバを保護するための ASA 5505 の設定	第 6 章「シナリオ：DMZ 設定」
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco Security Appliance Command Line Configuration Guide*』
日常的な運用について	『*Cisco Security Appliance Command Reference*』 『*Cisco Security Appliance Logging Configuration and System Log Messages*』

次の作業

APPENDIX A

3DES/AES ライセンスの取得

Cisco ASA 5505 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 ライセンスが付属しています。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 などの特定の機能をイネーブルにする暗号化テクノロジーを提供する 3DES/AES ライセンスを取得できます。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 の登録ユーザの場合、3DES/AES 暗号化ライセンスを入手するには、次の Web サイトにアクセスしてください。

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

Cisco.com の登録ユーザでない場合は、次の Web サイトにアクセスしてください。

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

姓名、電子メールアドレス、および **show version** コマンド出力で表示される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てください。

（注） ライセンス アップグレードを請求すると、2 時間以内に、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、次の手順に従います。

	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 コンフィギュレーション、ライセンス キー、および関連の動作期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* 変数を新しいライセンスで取得したアクティベーション キーに置き換えて、暗号化アクティベーション キーを更新します。*activation-5-tuple-key* 変数は 5 つの要素で構成される 16 進数文字列で、各要素間には 1 つずつスペースがあります。たとえば、0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e です。「0x」はオプションです。すべての値は 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。