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。

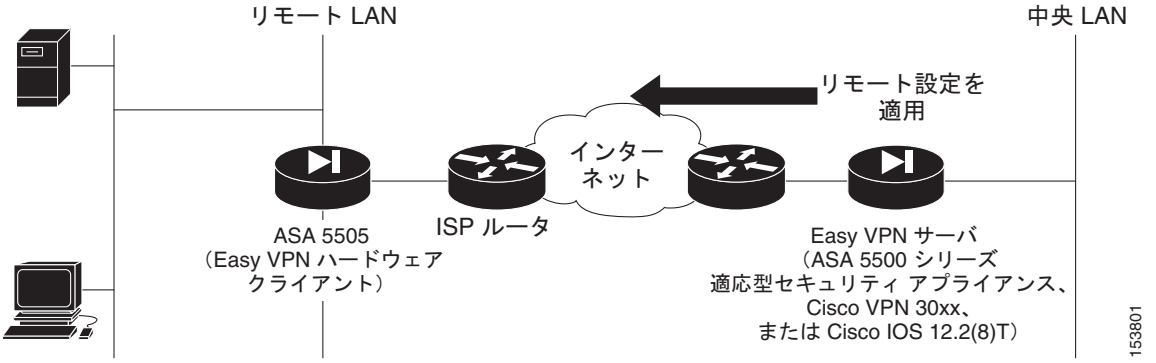
Cisco ASA 5505 は、Cisco Easy VPN ハードウェア クライアントまたは Cisco Easy VPN サーバ（別名、「ヘッドエンド デバイス」）として機能することができますが、同時に両方の役割を果たすことはできません。

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。

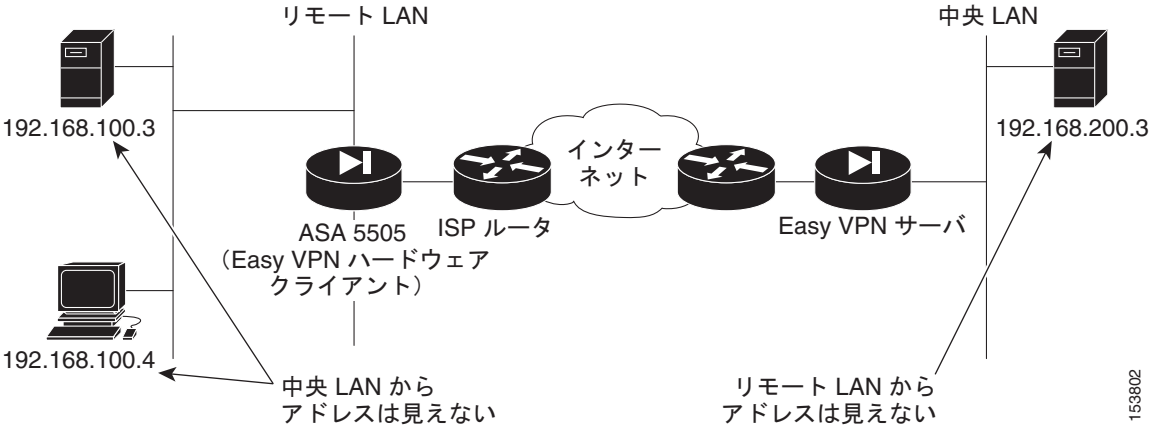
NEM では、内部インターフェイスとすべての内部ホストは、トンネルを経由してエンタープライズ ネットワークにルーティングできます。内部ネットワークのホストは、スタティック IP アドレスが事前に設定されたアクセス可能なサブネットから（スタティックに、または DHCP を使用して）IP アドレスを取得します。NEM では、PAT は VPN トラフィックに適用されません。このモードでは、各クライアントに VPN を設定する必要がありません。NEM モードに設定された ASA 5505 は、トンネルの自動開始をサポートしています。この設定には、グループ名、ユーザ名、およびパスワードが保存される必要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

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

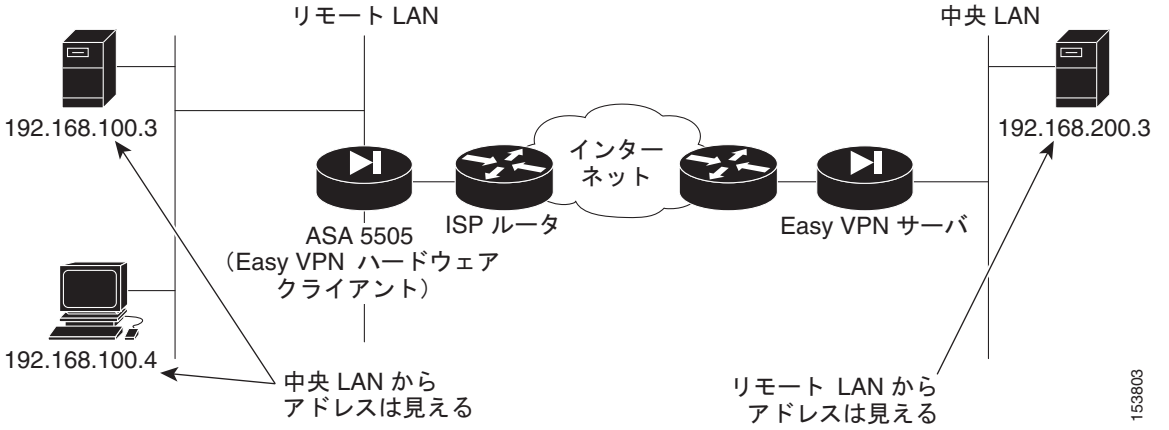


Easy VPN NEM に設定している場合、ASA 5505 は、パブリック IP アドレスを代用することにより、ローカル ホストの IP アドレスを隠蔽しません。したがって、VPN 接続の反対側のホストは、ローカル ネットワーク上のホストと直接通信できます。

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。

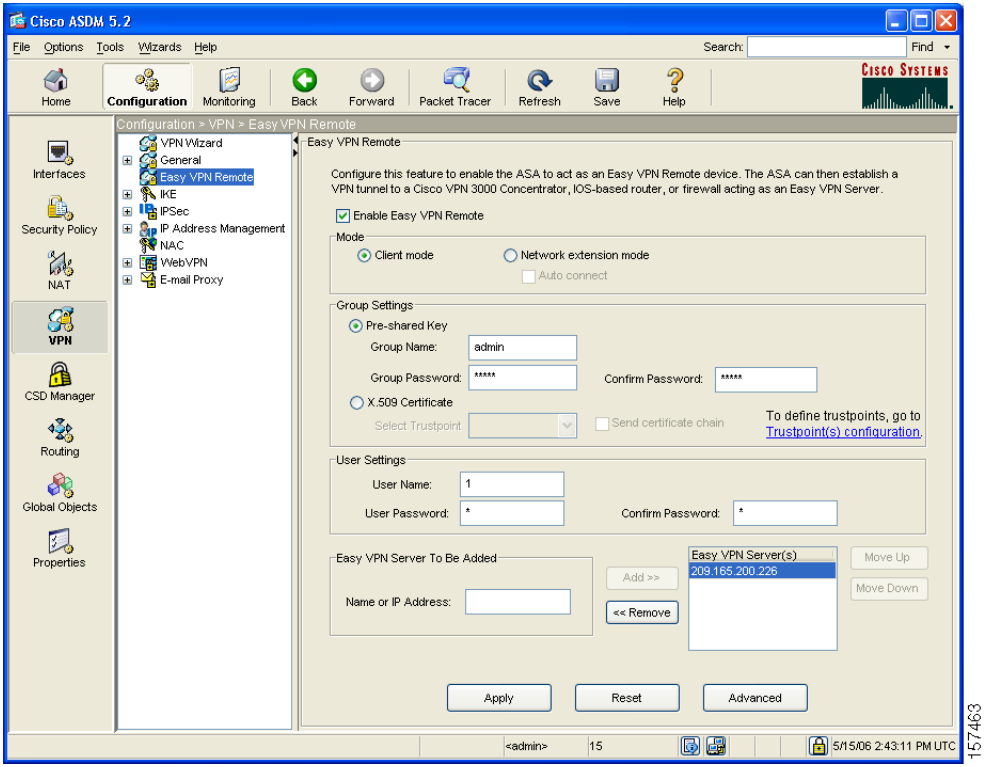
c. ASDM ソフトウェアを実行するのに使用する方法を選択するウィンドウで、ASDM Launcher をダウンロードするか、ASDM ソフトウェアを Java アプレットとして実行するかを選択します。

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