CHAPTER 12

ASA 5505 での Easy VPN Services の設定

この章では、ASDM を使用して ASA 5505 を Easy VPN ハードウェア クライアントとして設定する方法について説明します。この章の説明では、スイッチ ポートが設定され、ASA 5505 の VLAN インターフェイスが設定済みであると想定します（『*Cisco Security Appliance Command Line Configuration Guide*』の「Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance」を参照）。

（注） Easy VPN ハードウェア クライアントの設定では、そのプライマリ Easy VPN サーバとセカンダリ（バックアップ）Easy VPN サーバの IP アドレスを指定します。ASA は、ヘッドエンドとして設定されたもう 1 台の ASA 5505、VPN 3000 シリーズのコンセントレータ、IOS ベースのルータ、またはファイアウォールなど、どのような ASA でも Easy VPN サーバとして使用できます。ただし、1 台の ASA 5505 を同時にクライアント兼サーバとして使用することはできません。ASA 5505 をサーバとして設定する方法については、P.12-5 の「Cisco ASA 5505 の役割（クライアントまたはサーバ）の指定」を参照してください。次に、ASA 5505 を他の ASA と同様に設定します。これについては、『*Cisco Security Appliance Command Line Configuration Guide*』の「Getting Started」以降の章を参照してください。

この章には、次の項があります。

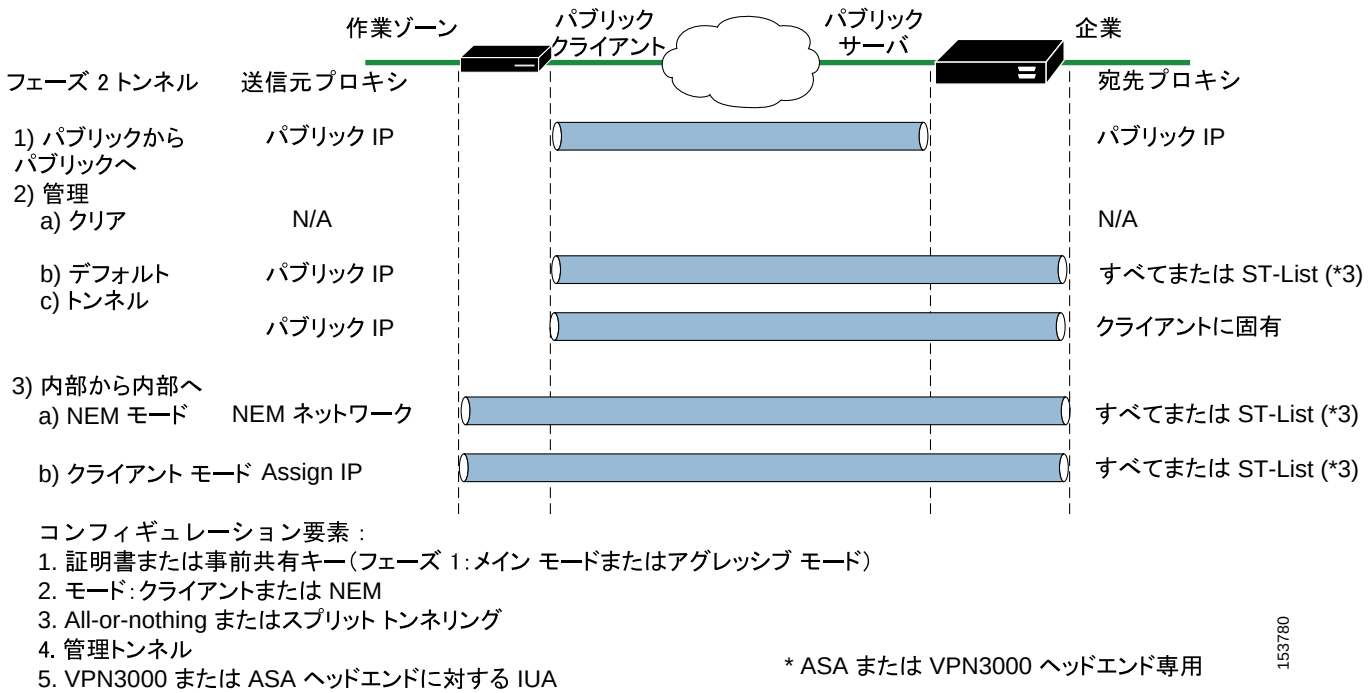
トンネリング オプションの比較

Easy VPN ハードウェア クライアントとして設定された Cisco ASA 5505 が設定するトンネル タイプは、次の要素によって異なります。

- Enable Tunneled Management アトリビュートを使用すると、データ トンネル以外にリモート管理用の IPSec トンネルを自動で確立できます。Clear Tunneled Management アトリビュートを使用すると、通常のルーティングを使用して管理アクセスが可能になります。またどちらのアトリビュートも使用しなければ、ヘッドエンド上でスプリット トンネリングを許可、制限、または禁止する Split Tunnel Policy アトリビュートまたは Split Tunnel Network List アトリビュートに従い、IPSec を使用して管理トンネルが設定されます（Enable Tunneled Management アトリビュートおよび Enable Tunneled Management アトリビュートの設定方法については、P.12-12 の「トンネル管理の設定」を参照してください。ヘッドエンド上で Split Tunnel Policy アトリビュートおよび Split Tunnel Network List アトリビュートを設定する方法については、P.2-32 の「クライアント設定パラメータの設定」を参照）。
- クライアント側から見て内部ホストを企業ネットワークまたはネットワーク拡張モードから隔離する Client Mode アトリビュートを使用すると、企業ネットワークからそれらのアドレスにアクセスできるようになります。

図 12-1 は、Easy VPN ハードウェア クライアントが、複数のアトリビュート設定に基づいて開始するトンネルのタイプを示します。

図 12-1　Cisco ASA 5505 の Easy VPN ハードウェア クライアントのトンネリング オプション



「All-or-nothing」という語は、スプリット トンネリングのアクセス リストが存在または不在であることを意味します。アクセス リストは、トンネリングが必要なネットワークと、必要でないネットワークを区別します。

はじめに（Easy VPN ハードウェア クライアントのみ）

ASA 5505 を Easy VPN ハードウェア クライアントとして設定する前に、次の手順を実行する必要があります。

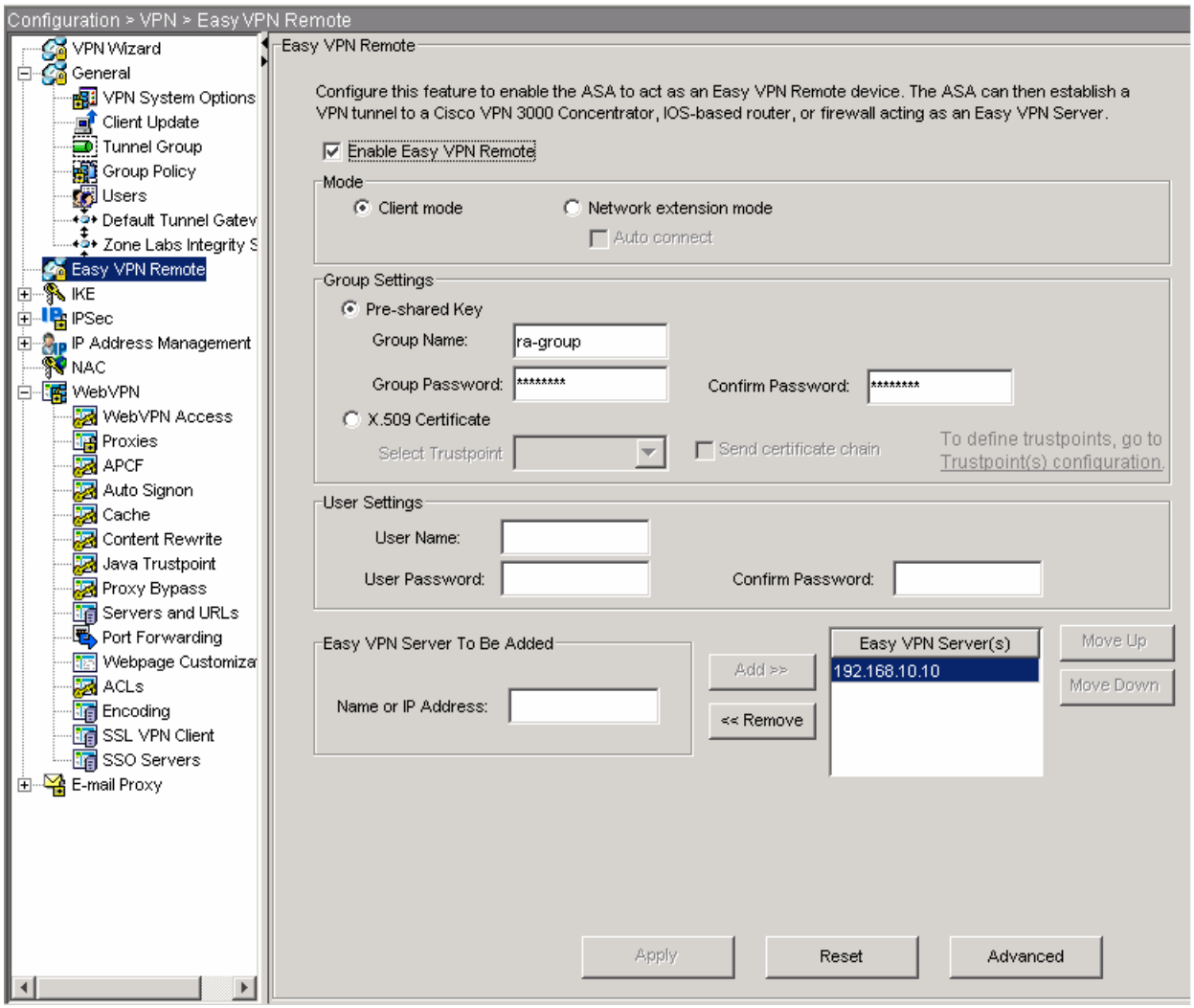
- サーバで必要な認証方式に応じて、次のいずれかの情報を取得します。
  - ヘッドエンドでの認証に事前共有鍵が必要な場合は、トンネルグループ名と事前共有鍵（グループ パスワード）。ヘッドエンドが ASA の場合、そのヘッドエンドに ASDM 接続すると、Configuration > VPN > General > Tunnel Group ウィンドウにトンネル グループ名が表示されます。トンネル グループ名をダブルクリックし、IPSec タブを開くと、事前共有鍵が表示されます。
  - ヘッドエンドでの認証にトラストポイントが必要な場合は、トラストポイント名と証明書チェーンの送信がアクティブかどうかを確認する必要があります。また、Easy VPN ハードウェア クライアントとして使用する ASA 5505 に、トラストポイントを設定する必要があります。ヘッドエンドが ASA の場合、そのヘッドエンドに ASDM 接続すると、Configuration > VPN > General > Tunnel Group > Add or Edit tunnel > IPSec タブにトラストポイント名と証明書チェーン インジケータが表示されます。次の手順に進む前に、P.1-4 の「トラストポイントの作成」の手順に従って、Easy VPN ハードウェア クライアントとして使用する ASA 5505 に、補助的なトラストポイントを設定する必要があります。
- （オプション）Easy VPN ハードウェア クライアントが、サーバからの IKE Extended Authenticate（Xauth; 拡張認証）チャレンジに対して使用するユーザ名とパスワードを取得します。
- Easy VPN サーバの役割を果たすプライマリとバックアップのヘッドエンドの IP アドレス。

基本設定の指定

Cisco ASA 5505 の基本設定では、それが Easy VPN ハードウェア クライアントとして機能するかどうか、また機能する場合は、内部ネットワーク上のホストの IP アドレスを、企業ネットワーク上のホストに公開するか隠蔽するか、ヘッドエンドへの接続の確立に使用されるグループまたはユーザ セキュリティ設定、および接続先のプライマリまたはバックアップ ヘッドエンドを指定します。

基本設定を行うには、Configuration > VPN > Easy VPN Remote を選択します。Easy VPN Remote ウィンドウが表示されます（図 12-2）。

図 12-2　Easy VPN Remote



以下の各項では、このウィンドウに表示される各アトリビュートに設定値を割り当てる方法を説明します。

Cisco ASA 5505 の役割（クライアントまたはサーバ）の指定

Cisco ASA 5505 は、Cisco Easy VPN ハードウェア クライアント（「Easy VPN Remote」）またはサーバ（「ヘッドエンド」）のいずれかとして動作し、同時に両方を兼ねることはできません。

ネットワークにおける ASA 5505 の役割は、次のように指定します。

ステップ 1　ASA 5505 をヘッドエンドとして設定した後、ハードウェア クライアントに変更する場合だけ、次のオブジェクトを削除または無効化します。

- ユーザ定義のトンネル グループをすべて削除するには、Configuration > VPN > General > Tunnel Group を選択し、デフォルト以外の各トンネル グループを選択して、**Delete**、**Apply** の順にクリックします。
- IPSec over TCP グローバル IKE 設定を無効にするには、Configuration > VPN > IKE > Global Parameters を選択し、IPSec over TCP をオフにして、**Apply** をクリックします。
- IKE ポリシーを削除するには、Configuration > VPN > IKE > Policies を選択し、各ポリシーを選択して、**Delete**、**Apply** の順にクリックします。
- IPSec ルールを削除するには、Configuration > VPN > IPSec > IPSec Rules を選択し、各ルールを選択して、**Delete**、**Apply** の順にクリックします。
- WebVPN を無効にするには、Configuration > VPN > WebVPN > WebVPN Access を選択し、各インターフェイスを選択して、**Disable**、**Apply** の順にクリックします。

（注）　設定の中でオブジェクト同士が競合する場合は、ASDM がエラー ウィンドウを表示するので、ASA 5505 を Easy VPN ハードウェア クライアント（以下のステップ 3 の「Easy VPN Remote」）として有効にし、Apply をクリックします。エラー ウィンドウには、設定の中に残っている、削除が必要なオブジェクトのタイプが表示され、これらを削除すると、Easy VPN Remote の設定値を設定に正常に保存できるようになります。

ステップ 2　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 3　次のどちらかを実行します。

- **Easy VPN Remote** をオンにして、ネットワークでの ASA 5505 の役割を Easy VPN ハードウェア クライアントとして指定します。
- **Easy VPN Remote** をオフにして、ネットワークでの ASA 5505 の役割をヘッドエンドとして指定します。

  このアトリビュートをオフにすると、その他のアトリビュートが淡色表示になります。

（注）　このアトリビュートをオフにした場合、**Apply** をクリックしてから、ASA 5505 を他の ASA と同様に設定します。これについては、『*Cisco Security Appliance Command Line Configuration Guide*』の「Getting Started」以降の章を参照してください。この章の残りの部分は無視してください。

User Settings 領域を除き、ASDM では、Easy VPN Remote をオンにした場合、このウィンドウのその他のアトリビュートを設定してから Apply をクリックする必要があります。以下の各項の説明に従ってこれらのアトリビュートを設定し、**Apply** をクリックして変更内容を実行コンフィギュレーションに保存します。

モードの指定

Easy VPN ハードウェア クライアントは、クライアント モードとネットワーク拡張モードの 2 つの操作モードのどちらかをサポートします。操作モードは、Easy VPN ハードウェア クライアントから見た内部ホストの IP アドレスが、企業ネットワークからトンネル経由でアクセス可能にするかどうかを指定します。Easy VPN ハードウェア クライアントにはデフォルト モードがないため、接続するには、その前に操作モードを指定しておくことが必要になります。

Easy VPN ハードウェア クライアントのモードを次のように指定します。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 2　次のいずれかのモード オプションをオンにします。

- **Client mode**：ポート アドレス変換（PAT）モードとも呼ばれます。クライアント モードでは、Easy VPN ハードウェア クライアントのプライベート ネットワークにあるすべてのデバイスが、企業ネットワークのデバイスから隔離されます。Easy VPN ハードウェア クライアントは、その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。

  （注）　IP アドレス管理は、Easy VPN ハードウェア クライアントの内部インターフェイスについても、内部ホストについても必要ありません。

- **Network extension mode**（NEM）：内部インターフェイスおよびすべての内部ホストが、トンネル経由で企業ネットワークにルーティング可能になります。内部ネットワーク上のホストは、スタティック IP アドレスによって事前設定され、（スタティックにまたは DHCP 経由で）アクセス可能なサブネットから IP アドレスを取得します。PAT は、NEM 内の VPN トラフィックには適用されません。このモードでは、各クライアントに VPN 設定を行う必要はありません。NEM 用に設定された Cisco ASA 5505 は、自動トンネル起動をサポートします。設定には、グループ名、ユーザ名、パスワードを保存する必要があります。自動トンネル起動は、セキュアなユニット認証が有効な場合は無効になります。

  ASDM では、Network extension mode をオンにした場合にだけ、Auto connect チェックボックスがオンになります。

ステップ 3　Network extension mode をオンにした場合は、次の手順を実行します。

- **Auto connect**：Network extension mode がローカルに設定され、かつ Easy VPN Remote にプッシュされたグループ ポリシーでスプリットトンネリングが設定されている場合を除き、Easy VPN Remote は、自動 IPSec データ トンネルを確立します。両方の条件を満たしている場合は、このアトリビュートをオンにすると、IPSec データ トンネルの確立が自動化されます。両方の条件を満たしていて、このアトリビュートをオフにした場合、このアトリビュートは無視されます。

ステップ 4　Easy VPN Client の設定が完了し、Easy VPN Remote ウィンドウを開いて、Mode 領域のアトリビュートを変更し終わった場合にだけ、**Apply** をクリックします。そうでない場合は、Easy VPN Remote ウィンドウの残りのセクションを引き続き設定した後で、**Apply** をクリックします。

（注）　Easy VPN ハードウェア クライアントが NEM を使用し、セカンダリ サーバに接続されている場合は、各ヘッドエンドへの ASDM 接続を確立し、その ASDM 接続の Configuration > VPN > IPSec > IPSec Rules > Tunnel Policy (Crypto Map) - Advanced タブを開き、**Enable Reverse Route Injection** をオンにして、RRI を使用したリモート ネットワークのダイナミック アナウンスメントを設定します。

トンネル グループまたはトラストポイントの指定

Cisco ASA 5505 を Easy VPN ハードウェア クライアントとして設定する場合、Easy VPN サーバ上に設定された事前共有鍵またはトラストポイント名を指定できます。Easy VPN サーバとして使用するヘッドエンド上に設定し、認証に使用するオプションの名前の項を参照してください。

- 事前共有鍵の指定
- トラストポイントの指定

事前共有鍵の指定

次の手順に従って、ヘッドエンドの事前共有鍵に合わせて、Easy VPN ハードウェア クライアントの事前共有鍵を指定します。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 2　Group Settings の下の **Pre-shared Key** をクリックします。

以下は、このアトリビュートについての説明です。

- **Pre-shared key**：認証に IKE 事前共有鍵を使用することを指定します。このアトリビュートを指定すると、その後の、Group Name、Group Password、Confirm Password の各フィールドに、その鍵に含まれるグループ ポリシー名とパスワードを指定できるようになります。

ステップ 3　次のアトリビュートに値を割り当てます。

- **Group Name**：ヘッドエンド上に設定される VPN トンネル グループの名前。このトンネル グループは、接続を確立する前に、サーバ上に設定する必要があります。
- **Group Password**：ヘッドエンド上で認証に使用する IKE 事前共有鍵を入力します。

ステップ 4　Easy VPN Client の設定が完了し、Easy VPN Remote ウィンドウを開いて、グループ設定を変更し終わった場合にだけ、**Apply** をクリックします。そうでない場合は、P.12-8 の「自動 Xauth 認証の設定」以降の説明に従い、Easy VPN Remote ウィンドウの残りのセクションを引き続き設定した後で、**Apply** をクリックします。

トラストポイントの指定

次の手順に従って、ヘッドエンドに設定されているトラストポイントと、設定している Easy VPN ハードウェア クライアント上のそれに対応するトラストポイント（P.12-3 の「はじめに（Easy VPN ハードウェア クライアントのみ）」を参照）を指定します。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 2　このウィンドウの Group Settings 領域内の次のアトリビュートに値を割り当てます。

- **X.509 Certificate**：認証用に、認証局から提供された X.509 デジタル証明書の使用をクリックして指定します。
- **Select Trustpoint**：認証に使用する RSA 証明書を識別するトラストポイントを選択します。トラストポイント名には、IP アドレスの形式を使用できます。このドロップダウン リストに入力するトラストポイントを定義するには、右側の **Trustpoint(s) configuration** をクリックします。
- **Send certificate chain**：（オプション）証明書自体だけでなく、証明書チェーンの送信を有効にします。このアクションでは、ルート証明書と下位のすべての CA 証明書が送信されます。

ステップ 3　Easy VPN Client の設定が完了し、Easy VPN Remote ウィンドウを開いて、グループ設定を変更し終わった場合にだけ、**Apply** をクリックします。そうでない場合は、Easy VPN Remote ウィンドウの残りのセクションを引き続き設定した後で、**Apply** をクリックします。

自動 Xauth 認証の設定

次の条件がすべて満たされている場合、Easy VPN ハードウェア クライアントとして設定した ASA 5505 は、Easy VPN への接続時に自動的に認証を行います。

- セキュアなユニット認証が、サーバ上で無効になっている。
- サーバが IKE 拡張認証（Xauth）クレデンシャルを要求している。

  Xauth は、TACACS+ または RADIUS を使用する IKE 内のユーザを認証する機能を提供します。Xauth は、RADIUS やその他のサポートされているユーザ認証プロトコルを使用して、ユーザ（この場合は、Easy VPN ハードウェア クライアント）を認証します。
- クライアント設定には、Xauth ユーザ名とパスワードが含まれています。

したがって、Easy VPN ハードウェア クライアントの Xauth ログイン クレデンシャルの設定はオプションです。

次のように、Xauth ログイン クレデンシャルを設定します。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 2　このウィンドウの Group Settings 領域内の次のアトリビュートに値を割り当てます。

- **User Name**：認証サーバまたはヘッドエンドからの Xauth チャレンジに対応して、Easy VPN ハードウェア クライアントが使用できるユーザ名を入力します。名前は、1 ～ 64 文字の間で、サーバまたはヘッドエンド上に設定する必要があります。

- **User Password** : 認証サーバまたはヘッドエンドからの Xauth チャレンジに対応して、Easy VPN ハードウェア クライアントが使用できるパスワードを入力します。パスワードは、1 ～ 64 文字の間で、サーバまたはヘッドエンド上に設定する必要があります。
- **Confirm Password**：User Password に入力したユーザ パスワードを再度入力します。

ステップ 3　Easy VPN Client の設定が完了し、Easy VPN Remote ウィンドウを開いて、ユーザ設定を変更し終わった場合にだけ、**Apply** をクリックします。そうでない場合は、次の項に進んだ後で、**Apply** をクリックします。

Easy VPN サーバのアドレスの指定

Easy VPN ハードウェア クライアントとの接続を確立する前に、Easy VPN サーバとして動作するヘッドエンドの IP アドレスを少なくとも 1 つ指定する必要があります。ASA は、ヘッドエンドとして設定されたもう 1 台の ASA 5505、VPN 3000 シリーズのコンセントレータ、IOS ベースのルータ、またはファイアウォールなど、どのような ASA でも Easy VPN サーバとして使用できます。

プライマリの Easy VPN サーバと、バックアップとして使用する Easy VPN サーバの IP アドレスを次のように設定します。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 2　次のアトリビュートの説明に従って、このウィンドウの Easy VPN Server To Be Added 領域に値を割り当てます。

Name or IP Address : プライマリ Easy VPN として使用するヘッドエンドの IP アドレスまたは DNS 名を入力し、**Add** をクリックします。この値は、ASDM の Easy VPN Server(s) リストに挿入されます。すべてのバックアップ Easy VPN サーバに対して、この操作を繰り返します。

ステップ 3　エントリを選択し、**Move Up** または **Move Down** をクリックして、関連付けられた Easy VPN サーバへの接続を試みる優先順位を設定します。

ステップ 4　関連付けられた Easy VPN サーバをリストから削除する場合は、エントリを選択して **Remove** をクリックします。

ステップ 5　**Apply** をクリックし、ウィンドウで行った変更を実行コンフィギュレーションに保存します。

（注）　エラー ウィンドウによって、Easy VPN ハードウェア クライアントとしての ASA 5505 の設定と競合するオブジェクトが識別された場合は、ASDM セッションがウィンドウの設定を保持します。エラー ウィンドウには、設定の中に残っている、削除が必要なオブジェクトのタイプが表示され、これらを削除すると、このウィンドウに変更を正常に保存できるようになります。競合するオブジェクトを削除した後、このウィンドウに戻って **Apply** を再度クリックします。

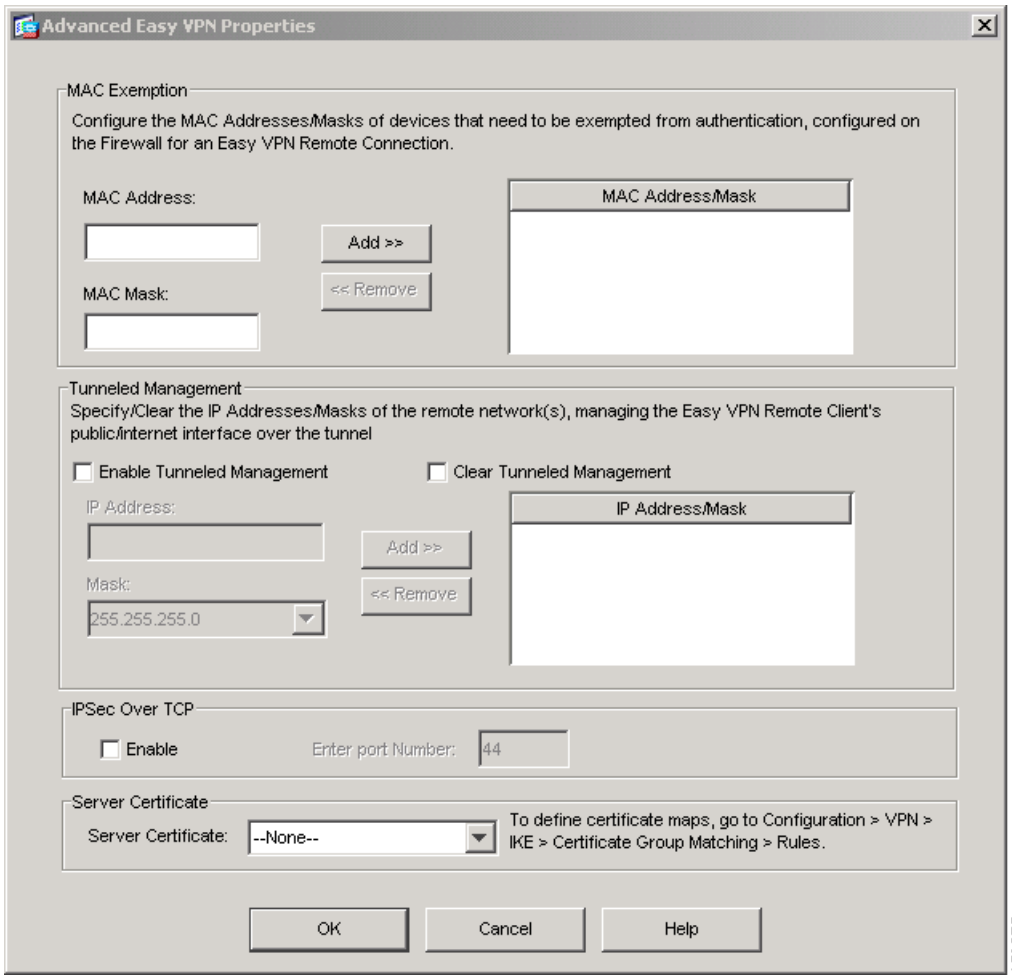
詳細設定の指定

Easy VPN ハードウェア クライアントの詳細設定はオプションです。次の設定が可能です。

- 内部ネットワーク上のデバイスを指定して、個別のユーザ認証を免除する。
- IPSec トンネルを自動的に作成して、企業ネットワークから ASA 5505 の外部インターフェイスへの管理アクセスを提供する。
- IPSec の TCP カプセル化の有効化と無効化。
- 証明書マップを指定し、その証明書マップが識別するデジタル証明書を持つ Easy VPN サーバにだけ、Easy VPN ハードウェア クライアントが接続を許可するように設定します。

Easy VPN ハードウェア クライアントの詳細設定を行うには、Configuration > VPN > Easy VPN Remote を選択し、Easy VPN Remote ウィンドウの下の **Advanced** をクリックします。Advanced Easy VPN Remote Properties ウィンドウが表示されます（図 12-3）。

図 12-3　Advanced Easy VPN Remote Properties



（注）　各領域はオプションで、他の領域から互いに独立しています。このウィンドウの 1 つの領域を設定しても、別の領域を設定する必要は生じません。

以下の各項では、このウィンドウの各アトリビュートに設定値を割り当てる方法を説明します。

デバイス パススルーの設定

Cisco IP Phone、ワイヤレス アクセス ポイント、プリンタなどのデバイスは、認証を実行できません。個々のユーザ認証が有効な場合、次の手順に従って、デバイスをユーザ認証から除外し、そのデバイスにネットワーク アクセスを提供できます。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択し、Easy VPN Remote ウィンドウの下部で **Advanced** をクリックします。

Advanced Easy VPN Remote Properties ウィンドウが表示されます（図 12-3）。このウィンドウ上部の MAC Exemption 領域では、デバイス パススルーを設定できます。

ステップ 2　次のアトリビュートに値を割り当てます。

- **MAC Address**：個々のユーザ認証をバイパスするデバイスの MAC アドレスを、ドット付き 16 進数表記で入力します。
- **MAC Mask**：MAC アドレスに対応するネットワーク マスクを入力します。ffff.ff00.0000 という MAC マスクは、同じ製造元が製造したすべてのデバイスに相当します。ffff.ffff.ffff という MAC マスクは、1 つのデバイスに相当します。

（注）　MAC マスク ffff.ff00.0000 を入力して、同じ製造元のすべてのデバイスを指定する場合、MAC アドレスの最初の 6 文字を入力するだけで済みます。たとえば、Cisco IP phones の製造元 ID が 00036b の場合、MAC アドレスとして `0003.6b00.0000` を入力し、MAC マスク コマンドとして `ffff.ff00.0000` を入力すると、将来追加する Cisco IP phone を含むすべての Cisco IP phone が認証を免除されます。MAC アドレス `0003.6b54.b213` と MAC マスク `ffff.ffff.ffff` を入力することでセキュリティは強化されますが、特定の 1 台の Cisco IP phone の認証を免除するため、柔軟性は低くなります。

ステップ 3　**Add** をクリックします。

MAC Address/Mask リストに MAC アドレスと MAC マスクが挿入されます。

ステップ 4　ユーザ認証を免除するデバイスが他にあれば、それぞれに対してステップ 2 と 3 を繰り返します。

ステップ 5　デバイスをリストから削除する場合は、エントリを選択して **Remove** をクリックします。

ステップ 6　Advanced Easy VPN Properties ウィンドウで他に変更するアトリビュートがない場合は、**OK**、**Apply** の順にクリックします。他に変更するアトリビュートがある場合は、次のセクションに進みます。

トンネル管理の設定

Cisco ASA 5505 は、Easy VPN ハードウェア クライアントとして動作するだけでなく、SSH または HTTPS を使用して、第 2 レイヤの追加暗号機能付きの、またはこの機能のない管理アクセスをサポートします。Easy VPN ハードウェア クライアントを設定することによって、管理セッションにすでに存在する IPSec 暗号化を SSH または HTTPS 暗号内で要求できます。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択し、Easy VPN Remote ウィンドウの下部で **Advanced** をクリックします。

Advanced Easy VPN Remote Properties ウィンドウが表示されます（図 12-3）。

ステップ 2　次のいずれかのオプションを選択します。

- **Enable Tunneled Management** : オンにすると、IPSec トンネルを自動作成して、企業ネットワークから ASA 5505 の外部インターフェイスへの管理アクセスを提供します。Easy VPN ハードウェア クライアントとサーバは、データ トンネルの作成時に管理トンネルを自動的に作成します。
- **Clear Tunneled Management** : オンにすると、通常のルーティングを使用して、企業ネットワークから ASA 5505 の外部インターフェイスへの管理アクセスを提供します（管理パケットの非トンネリング）。このアトリビュートは、NAT デバイスが Easy VPN ハードウェア クライアントとインターネット間で動作している場合にオンにします。
- **Enable Tunneled Management** と **Clear Tunneled Management** の両方のチェックボックスをオフのままにすると、**split-tunnel-policy** コマンドと **split-tunnel-network-list** コマンドに従って、管理トンネルの IPSec が設定されます。

（注）　ステップ 3 ～ 6 を使用するのは、Enable Tunneled Management をオンにした場合だけです。

ステップ 3　説明に従って、次のアトリビュートに値を割り当てます。

- **IP Address**：管理アクセス用の IPSec トンネルを自動作成するリモート ネットワークまたはホストの IP アドレスを入力します。
- **Mask**：入力した IP アドレスのサブネット マスクを選択します。

ステップ 4　**Add** をクリックします。

IP Address/Mask リストに IP アドレスとマスクが挿入されます。

ステップ 5　これ以外のネットワークまたはホストについて、リモート管理アクセス用の IPSec トンネルを自動作成する場合は、それぞれに対してステップ 3 と 4 を繰り返します。

ステップ 6　デバイスをリストから削除する場合は、エントリを選択して **Remove** をクリックします。

ステップ 7　Advanced Easy VPN Properties ウィンドウで他に変更するアトリビュートがない場合は、**OK**、**Apply** の順にクリックします。他に変更するアトリビュートがある場合は、次のセクションに進みます。

IPSec over TCP の設定

デフォルトで、Easy VPN ハードウェアとサーバは、IPSec を UDP（User Datagram Protocol）パケットにカプセル化します。特定のファイアウォール ルールや、NAT、PAT がある環境など、一部の環境では、UDP が使用できません。このような環境で標準の Encapsulating Security Protocol（ESP、Protocol 50）やインターネット キー エクスチェンジ（IKE、UDP 500）を使用するには、TCP パケット内にこれらのパケットをカプセル化してセキュアなトンネリングを行えるように、クライアントとサーバを設定する必要があります。ただし、使用している環境で UDP が利用できる場合は、IPSec over TCP を設定するのは不要なオーバーヘッドを追加するだけです。

IPSec の TCP カプセル化は、次のように有効または無効にします。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択し、Easy VPN Remote ウィンドウの下部で **Advanced** をクリックします。

Advanced Easy VPN Remote Properties ウィンドウが表示されます（図 12-3）。

ステップ 2　次の説明に従って、IPSec Over TCP 領域のアトリビュートを設定します。

- **Enable (IPSec Over TCP)**：オンにすると、TCP を使用して IPSec over UDP パケットがカプセル化されます。オフにすると、UDP だけが使用されます。

  このアトリビュートをオンにすると、Enter port Number ボックスがアクティブになります。
- **Enter port Number**：IPSec over TCP に使用するポート番号を入力します。デフォルトで、Easy VPN ハードウェア クライアントは、ポート 10000 を使用しますが、Enable (IPSec Over TCP) をオンにした場合は、ポート番号を入力する必要があります。10000 を入力するか、ヘッドエンドに割り当てたものと同じポート番号を使用します。

ステップ 3　Advanced Easy VPN Properties ウィンドウで他に変更するアトリビュートがない場合は、**OK**、**Apply** の順にクリックします。他に変更するアトリビュートがある場合は、次のセクションに進みます。

（注）　Easy VPN Remote 接続で、TCP でカプセル化された IPSec を使用する場合は、Configuration > VPN > IPSec > Pre-Fragmentation を選択し、外部インターフェイスをダブルクリックし、DF Bit Setting Policy を Clear に設定します。この処理によって、Don't Fragment（DF）ビットが、カプセル化されたヘッダーからクリアされます。DF ビットは IP ヘッダーの中にあり、パケットのフラグメントが可能かどうかを決定します。このコマンドを使用すると、Easy VPN ハードウェア クライアントは、MTU のサイズを超えるパケットを送信できます。

証明書のフィルタリングの設定

証明書マップを指定し、その証明書マップが識別するデジタル証明書を持つ Easy VPN サーバにだけ、Easy VPN ハードウェア クライアントが接続を許可するように設定できます。それを設定するには、その前に Configuration > VPN > IKE > Certificate Group Matching > Rules メニュー パスを使用して、マップを作成する必要があります。その後、次の手順で証明書マップを割り当てます。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択し、Easy VPN Remote ウィンドウの下部で **Advanced** をクリックします。

Advanced Easy VPN Remote Properties ウィンドウが開きます（図 12-3）。

ステップ 2　次の説明に従って、ウィンドウの下部でアトリビュートを設定します。

- **Server Certificate**：Easy VPN ハードウェア クライアント接続でサポートする証明書の識別に使用する証明書マップを選択します。Configuration > VPN > IKE > Certificate Group Matching > Rules メニュー パスを使用して Rules ウィンドウにアクセスすると、最初のテーブルのマッピング名が、ドロップダウン リストに表示されます。

ステップ 3　**OK**、**Apply** の順にクリックします。

Easy VPN サーバの設定のためのガイドライン

次の各項では、Easy VPN サーバに適用される Easy VPN ハードウェア クライアントについての考慮事項を説明します。

認証オプション

ASA 5505 は、次の認証メカニズムをサポートします。この認証メカニズムは、Easy VPN サーバに格納されているグループ ポリシーから取得されます。次のリストは、Easy VPN ハードウェア クライアントによってサポートされている認証オプションですが、これらは Easy VPN サーバ上で設定が必要です。

- Configuration > VPN General > Group Policy > Add or Edit Internal Group Policy > Hardware Client タブの Require Interactive Client Authentication （セキュアなユニット認証とも呼ばれます）

  このアトリビュートを有効にすると、Xauth ログイン クレデンシャル（P.12-8 の「自動 Xauth 認証の設定」を参照）が無視され、ユーザがパスワードを入力して ASA 5505 を認証する必要があります。
- 同じ Hardware Client タブの Require Individual User Authentication

  このアトリビュートを有効にすると、企業 VPN ネットワークにアクセスする前に、ASA 5505 を使用しているユーザが認証される必要があります。

注意　クライアントが NAT デバイスを持っている可能性がある場合は、IUA を使用しないでください。

- 同じ Hardware Client タブの User Authentication Idle Timeout

  このアトリビュートは、Easy VPN Server がクライアントのアクセスを終了するまでのアイドル タイムアウト期間を設定または解除します。
- Authentication by HTTP redirection

  次のいずれかの場合、Cisco Easy VPN サーバは、HTTP トラフィックを代行受信して、ユーザをログイン ページにリダイレクトします。

  － SUA またはユーザ名とパスワードが Easy VPN ハードウェア クライアント上に設定されていない場合

  － IAU が有効な場合

  HTTP リダイレクションは自動的に行われるため、Easy VPN サーバ上で設定する必要はありません。
- 事前共有鍵、デジタル証明書、トークン、無認証

  ASA 5505 は、ユーザ認証方式として、事前共有鍵、トークンベース（たとえば、SDI ワンタイム パスワード）、および「ユーザ認証なし」をサポートします。**注**：Cisco Easy VPN サーバは、ユーザ認証の一部として、デジタル証明書を使用できます。使用方法については、P.1-1 の「デジタル証明書の登録」を参照してください。

クライアントにプッシュされるグループ ポリシーとユーザ アトリビュート

トンネル確立時に、Easy VPN サーバは、その設定に格納されているグループ ポリシーまたはユーザ アトリビュートの値を Easy VPN ハードウェア クライアントにプッシュします。したがって、Easy VPN ハードウェア クライアントで使用されている一部のアトリビュートを変更するには、プライマリとセカンダリ Easy VPN サーバとして設定されているセキュリティ アプライアンス上でそれらのアトリビュートを変更する必要があります。この項では、Easy VPN ハードウェア クライアントにプッシュされるグループ ポリシー アトリビュートを示します。

（注）　この項は、参考資料として使用してください。グループ ポリシーの設定方法については、P.2-1 の「グループ ポリシーの設定」を参照してください。

Easy VPN サーバ上で変更が必要なグループ ポリシー アトリビュートについては、表 34-2 を参照してください。

表 12-1　EasyVPN ハードウェア クライアントとして設定された Cisco ASA 5505 にプッシュされるグループ ポリシーとユーザ アトリビュート

ASDM Group Policy タブ	アトリビュート	説明
General	Tunneling Protocols	許可されるトンネリング プロトコルを指定します。
General	Filter	VPN トラフィックに適用されます。
General	Access Hours	VPN のアクセス時間を制限します。
General	Simultaneous Logins	同時ログインの最大数を指定します。
General	Maximum Connect Time	VPN 接続の最大分数を指定します。
General	Idle Timeout	セッションがタイムアウトになるまでのアイドル時間を指定します。
General	DNS Servers	プライマリおよびセカンダリ DNS サーバの IP アドレスを指定するか、DNS サーバの使用を禁止します。
General	WINS Servers	プライマリおよびセカンダリ WINS サーバの IP アドレスを指定するか、WINS サーバの使用を禁止します。
General	DHCP Scope	このグループ内で、DHCP サーバがユーザにアドレスを割り当てる IP サブネットワークを指定します。
IPSec	Re-authentication on IKE Re-key	IKE 鍵の再生成時に、Xauth 認証が必要です。 **注**：セキュアなユニット認証が有効な場合は、XAUTH 再認証を無効にします。
IPSec	Perfect Forward Security	VPN クライアントが、perfect forward secrecy（PFS; 完全転送秘密）を使用します。
IPSec	Tunnel Group Lock	トンネル グループによって、ユーザがそのグループに確実に接続されるよう指定します。
IPSec	Client Access Rules	アクセス ルールを適用します。
Client Configuration > General Client Parameters	Banner	トンネル確立後、クライアントにバナーを送信します。
Client Configuration > General Client Parameters	Default Domain	ドメイン名をクライアントに送信します。
Client Configuration > General Client Parameters	Split Tunnel DNS Names	名前解決のためにドメインのリストをプッシュします。

表 12-1　EasyVPN ハードウェア クライアントとして設定された Cisco ASA 5505 にプッシュされるグループ ポリシーとユーザ アトリビュート（続き）

ASDM Group Policy タブ	アトリビュート	説明
Client Configuration > General Client Parameters	Split Tunnel Policy	リモートアクセスの IPSec クライアントが、条件に応じて、パケットを暗号化して IPSec トンネル経由で送信するか、クリアテキストでネットワーク インターフェイスに送信します。オプションは次のとおりです。 • split-tunnel-policy：トンネリング トラフィックのルールを設定していることを示します。 • excludespecified：トラフィックがクリアテキストで送信されるネットワークのリストを定義します。 • tunnelall：クリアテキストで送信するトラフィックも、Easy VPN サーバ以外の宛先に送信するトラフィックも存在しないことを指定します。リモート ユーザは、企業ネットワーク経由でインターネット ネットワークに接続し、ローカル ネットワークにアクセスできません。 • tunnelspecified：指定されたネットワークとの間で送受信されるすべてのトラフィックをトンネリングします。このオプションによって、スプリット トンネリングが有効になります。またトンネルするアドレスのネットワーク リストが作成できます。他のすべてのアドレスに送信されるデータはクリアテキスト形式を取り、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。
Client Configuration > General Client Parameters	Split Tunnel Network List	次のどちらかを指定します。 • スプリット トンネリングのアクセスリストが存在しません。すべてのトラフィックは、トンネル経由で送信されます。 • トンネリングが必要なネットワークと、必要でないネットワークを、セキュリティ アプライアンスが区別するためのアクセス リストを指定します。 スプリット トンネリングでは、リモートアクセスの IPSec クライアントが、条件に応じて、パケットを暗号化して IPSec トンネル経由で送信するか、クリアテキストでネットワーク インターフェイスに送信します。スプリット トンネリングを有効にすると、IPSec トンネルの他端にある宛先以外に送信されるパケットは、暗号化され、トンネル経由で送信され、復号化され、最終宛先にルーティングされます。
Client Configuration > Cisco Client Parameters	Store Password on Client System	VPN ユーザがパスワードをユーザ プロファイルに保存できます。
Client Configuration > Cisco Client Parameters	IPSec over UDP	IPSec トンネルに UDP カプセル化を使用します。
Client Configuration > Cisco Client Parameters	IPSec over UDP Port	IPSec over UDP のポート番号を指定します。
Client Configuration > Cisco Client Parameters	IPSec Backup Servers	プライマリ サーバが応答できない場合に備えて、クライアント上にバックアップ サーバを設定します。
Client Firewall	（このタブ上のすべて）	VPN クライアント上に、ファイアウォール パラメータを設定します。
Hardware Client	Require Interactive Client Authentication	VPN ハードウェア クライアントで、セキュアなユニット認証を有効にします。

表 12-1　EasyVPN ハードウェア クライアントとして設定された Cisco ASA 5505 にプッシュされるグループ ポリシーとユーザ アトリビュート（続き）

ASDM Group Policy タブ	アトリビュート	説明
Hardware Client	Require Individual User Authentication	ハードウェアベースの VPN クライアントで、個別のユーザ認証を有効にします。
Hardware Client	Allow Network Extension Mode	ネットワーク拡張モードを有効または無効にします。

（注）　IPSec NAT-T 接続は、Cisco ASA 5505 の ホーム VLAN 上でサポートされている唯一の IPSec 接続タイプです。IPSec over TCP とネイティブな IPSec 接続はサポートされていません。