Easy VPN

この章では、Easy VPN サーバとして任意の ASA を設定する方法、および Easy VPN リモート ハードウェア クライアントとして Cisco ASA with FirePOWER- 5506-X、5506W-X、5506H-X、5508-X モデルを設定する方法について説明します。

Easy VPN について

Cisco Ezvpn は、リモート オフィスおよびモバイル ワーカー向けの VPN の設定と導入を大幅に簡素化します。Cisco Easy VPN は、サイト間 VPN とリモート アクセス VPN の両方に対応した柔軟性、拡張性、使いやすさを備えています。Cisco Unity クライアント プロトコルの実装により、管理者は Easy VPN サーバで大部分の VPN パラメータを定義できるので、Easy VPN リモートの設定がシンプルになります。

Cisco ASA with FirePOWER の 5506-X、5506W-X、5506H-X、および 5508-X モデルは、Easy VPN サーバへの VPN トンネルを開始するハードウェア クライアントして Easy VPN リモートをサポートします。Easy VPN サーバとして、別の ASA（任意のモデル）または Cisco IOS ベースのルータを使用できます。ASA は、同時に Easy VPN リモートと Easy VPN サーバの両方として動作することはできません。

（注） Cisco ASA 5506-X、5506W-X、5506H-X、および 5508-X モデルは、L2 スイッチングではなく、L3 スイッチングをサポートしています。内部ネットワーク上で複数のホストやデバイスとともに Easy VPN リモートを使用する場合は、外部スイッチを使用します。ASA の内部ネットワーク上に単一のホストしかない場合、スイッチは必要はありません。

次のセクションでは、Easy VPN のオプションと設定について説明します。

Easy VPN インターフェイス

システムの起動時に、セキュリティ レベルによって Easy VPN の外部および内部インターフェイスが決定されます。最もセキュリティ レベルが低い物理インターフェイスは、Easy VPN サーバへの外部接続に使用されます。最もセキュリティ レベルが高い物理または仮想インターフェイスは、セキュアなリソースへの内部接続に使用されます。Easy VPN で、同じ最高セキュリティ レベルの複数のインターフェイスがあることが特定されると、Easy VPN が無効になります。

必要に応じて、**vpnclient secure interface** コマンドを使用して、内部セキュア インターフェイスを物理インターフェイスから仮想インターフェイスに、あるいは仮想インターフェイスから物理インターフェイスに変更することができます。外部インターフェイスを自動的に選択されたデフォルトの物理インターフェイスから変更することはできません。

たとえば、ASA5506 プラットフォームでは、工場出荷時の設定により、BVI が、最高セキュリティ レベル インターフェイスを示す 100 に設定され（メンバー インターフェイスもレベル 100 に設定）、外部インターフェイスのセキュリティ レベルが 0 になっています。Easy VPN はデフォルトでこれらのインターフェイスを選択します。

仮想インターフェイス（ブリッジ型仮想インターフェイスまたはBVI）が起動時に選択されると、または管理者によって内部のセキュアなインターフェイスとして割り当てられると、次の内容が適用されます。

- すべての BVI メンバー インターフェイスは、自身のセキュリティ レベルに関係なく、内部のセキュアなインターフェイスであるとみなされます。
- ACL および NAT ルールをすべてのメンバー インターフェイスに追加する必要があります。AAA ルールは BVI インターフェイスのみに追加されます。

Easy VPN の接続

Easy VPN は IPsec IKEv1 トンネルを使用します。Easy VPN リモート ハードウェア クライアントの設定は、Easy VPN サーバ ヘッドエンドの VPN の設定と互換性を保つようにする必要があります。セカンダリ サーバを使用する場合は、それらの設定をプライマリ サーバと同じにする必要があります。

ASA Easy VPN リモートはプライマリ Easy VPN サーバの IP アドレスを設定し、必要に応じて、最大 10 台のセカンダリ（バックアップ）サーバを設定します。これらのサーバを設定するには、グローバル コンフィギュレーション モードで **vpnclient server** コマンドを使用します。プライマリ サーバへのトンネルをセットアップできない場合、クライアントは最初のセカンダリ VPN サーバへの接続を試み、次に VPN サーバのリストの上から順に 8 秒間隔で接続を試行します。最初のセカンダリ VPN サーバへのトンネルをセットアップできず、その間にプライマリ サーバがオンライン状態になった場合、クライアントは、引き続き 2 番目のセカンダリ VPN サーバへのトンネルのセットアップを試みます。

デフォルトでは、Easy VPN ハードウェア クライアントとサーバは IPSec をユーザ データグラム プロトコル（UDP）パケット内でカプセル化します。一部の環境（特定のファイアウォール ルールが設定されている環境など）または NAT デバイスや PAT デバイスでは、UDP を使用できません。そのような環境で標準のカプセル化セキュリティ プロトコル（ESP、プロトコル

50）またはインターネット 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 IPsec をカプセル化してセキュアなトンネリングをイネーブルにするようにクライアントとサーバを設定します。**vpnclient ipsec-over-tcp** コマンドを使用してこれを設定します。ただし、UDP が許可されている環境では、IPsec over TCP を設定すると不要なオーバーヘッドが発生します。

Easy VPN トンネル グループ

トンネルの確立後、Easy VPN リモートは Easy VPN サーバで設定されたトンネル グループを指定し、これを接続に使用します。Easy VPN サーバは、トンネルの動作を決定する Easy VPN リモート ハードウェア クライアントにグループ ポリシーまたはユーザ属性をプッシュします。特定の属性を変更するには、プライマリまたはセカンダリ Easy VPN サーバとして設定されている ASA でその属性を変更する必要があります。

Easy VPN リモート クライアントは、**vpnclient vpngroup** コマンドを使用してグループ ポリシーを指定し、その名前と事前共有キーを設定します。または、**vpnclient trustpoint** コマンドを使用して、事前設定されているトラストポイントを指定します。

Easy VPN モードの動作

企業ネットワークからトンネル経由で Easy VPN リモートの背後にあるホストにアクセスできるかどうは、モードによって決まります。

- クライアント モードはポート アドレス変換（PAT）モードとも呼ばれ、Easy VPN リモート プライベート ネットワーク上のすべてのデバイスを、企業ネットワークのデバイスから分離します。Easy VPN リモートは、内部ホストのすべての VPN トラフィックに対してポート アドレス変換（PAT）を実行します。Easy VPN リモートのプライベート側のネットワークとアドレスは非表示になっており、直接アクセスすることはできません。Easy VPN クライアントの内部インターフェイスまたは内部ホストに対して、IP アドレスの管理は必要ありません。
- ネットワーク拡張モード（NEM）は、内部インターフェイスとすべての内部ホストが、トンネルを介して企業ネットワーク全体にルーティングできるようにします。内部ネットワークのホストは、スタティック IP アドレスで事前設定されたアクセス可能なサブネット（スタティックまたは DHCP を介して）から 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、内部ネットワークのホストごとの VPN 設定やトンネルは必要ありません。Easy VPN リモートによってすべてのホストにトンネリングが提供されます。

Easy VPN サーバはデフォルトでクライアント モードになります。NEM モードを設定するには、グループ ポリシー コンフィギュレーション モードで **nem enable** コマンドを使用します。Easy VPN リモートにはデフォルト モードがないため、トンネルを確立する前に、必ず、Easy VPN リモートにいずれかの動作モードを指定する必要があります。PAT または NEM を設定するには、Easy VPN リモートで **vpnclient mode** コマンドを使用します。

（注） NEM モード用に設定された Easy VPN リモート ASA は、自動トンネル起動をサポートしています。自動起動には、トンネルのセットアップに使用するクレデンシャルの設定とストレージが必要です。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。

複数のインターフェイスが設定されているネットワーク拡張モードの Easy VPN リモートは、最もセキュリティレベルが高いインターフェイスからのローカルに暗号化されたトラフィックに対してのみトンネルを構築します。

Easy VPN ユーザ認証

ASA Easy VPN リモートは、**vpnclient username** コマンドを使用して、自動ログイン用にユーザ名とパスワードを保存できます。

セキュリティを強化するために、Easy VPN サーバは以下を要求できます。

- セキュアユニット認証（SUA）：設定されているユーザ名およびパスワードを無視して、ユーザに手動による認証を要求します。デフォルトでは、SUA はディセーブルになっており、**secure-unit-authentication enable** コマンドを使用して、Easy VPN サーバで SUA をイネーブルにします。
- 個別ユーザ認証（IUA）：Easy VPN リモートの背後にいるユーザは、企業 VPN ネットワークへのアクセス権限を得るために、ユーザ認証を受ける必要があります。デフォルトでは、IUA はディセーブルになっており、**user-authentication enable** コマンドを使用して、Easy VPN サーバで IUA をイネーブルにします。

  IUA を使用する場合は、ハードウェア クライアントの背後にある特定のデバイス（Cisco IP Phone やプリンタなど）が個々のユーザ認証をバイパスできるようにする必要があります。これを設定するには、Easy VPN サーバで **ip-phone-bypass** コマンドを使用して IP Phone Bypass を指定し、Easy VPN リモートで **mac-exempt** コマンドを使用して MAC アドレス免除を指定します。

  さらに、Easy VPN サーバは、クライアントのアクセスを終了させるまでのアイドル タイムアウト時間を設定または削除できます。これを行うには、Easy VPN サーバで **user-authentication-idle-timeout** コマンドを使用します。

ユーザ名とパスワードが設定されていない場合、SUA がディセーブルになっている場合、または IUA がイネーブルになっている場合、Cisco Easy VPN サーバは HTTP トラフィックを代行受信し、ユーザをログイン ページにリダイレクトします。HTTP リダイレクションが自動で、Easy VPN サーバ上のコンフィギュレーションが必要ない。

リモート 管理

Easy VPN リモート ハードウェア クライアントとして動作する ASA は、さらに IPsec 暗号化されるかどうかにかかわらず、SSH または HTTPS を使用して管理アクセスをサポートします。

デフォルトでは、管理トンネルは、SSH または HTTPS 暗号化で IPsec 暗号化を使用します。IPsec 暗号化レイヤをクリアすると、VPN トンネルの外部に管理アクセスできます。これを行うには、**vpnclient management clear** コマンドを使用します。トンネル管理をクリアしても、IPsec の暗号化レベルが削除されるだけで、SSH や HTTPS など、その接続に存在する他の暗号化には影響しません。

セキュリティを強化するために、Easy VPN リモートは、IPsec 暗号化および企業側の特定のホストまたはネットワークへの管理アクセスの制限を要求できます。これを行うには、グローバル コンフィギュレーション モードで **vpnclient management tunnel** コマンドを使用します。

デフォルトのリモート管理操作に戻すには、**no vpnclient management** を使用します。

（注） NAT デバイスが ASA Easy VPN リモートとインターネットの間で動作している場合は、ASA Easy VPN リモート上に管理トンネルを設定しないでください。そのような設定では、**vpnclient management clear** コマンドを使用して、リモート管理をクリアしてください。

コンフィギュレーションにかかわらず、DHCP 要求（更新メッセージを含む）は IPSec トンネル上を流れません。vpnclient management tunnel を使用しても、DHCP トラフィックは許可されません。

Easy VPN リモートの設定

始める前に

Easy VPN リモートの設定に必要な次の情報を取得します。

- プライマリ Easy VPN サーバのアドレスと、セカンダリ サーバのアドレスのアドレス（セカンダリ サーバを使用できる場合）。
- Easy VPN リモートを動作させるアドレッシング モード（クライアントまたは NEM）。
- Easy VPN サーバ グループ ポリシーの名前とパスワード（事前共有鍵）、または目的のグループ ポリシーを選択して認証する事前設定されたトラストポイント。
- Easy VPN サーバに設定されている、VPN トンネルの使用を許可されたユーザ。
- リモート管理インターフェイスに対して BVI インターフェイスが使用されている場合、そのインターフェイスで **management-access** を設定する必要があります。

手順

ステップ 1 Easy VPN サーバのアドレスを入力します。

vpnclient server *ip-primary* [*ip-secondary-1... ip-secondary-n*]

- *ip_primary_address*：プライマリ Easy VPN サーバの IP アドレスまたは DNS 名。

- *ip-secondary-n*（任意）：最大 10 台のバックアップ Easy VPN サーバの IP アドレスまたは DNS 名のリスト。スペースを使用して、リスト内の項目を区切ります。

例：

```
asa(config)#vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
```

ステップ 2 （任意） 自動的に選択されたデフォルトのインターフェイスが望ましくない場合は、内部セキュア インターフェイスを再割り当てします。

起動時に最もセキュリティ レベルが高い物理インターフェイスまたはBVIがセキュアなリソースへの内部接続に使用されます。別のインターフェイスを使用する場合は、**vpnclient secure interface** *interface-name* コマンドを使用します。物理または仮想インターフェイスを割り当てることができます。

ステップ 3 動作モードを指定します。

vpnclient mode {**client-mode** | **network-extension-mode**}

- **client-mode**：ポート アドレス変換（PAT）モードを使用して、クライアントに関連する内部ホストのアドレスを企業ネットワークから分離します。
- **network-extension-mode**：内部ホストのアドレスは、企業ネットワークからアクセス可能です。

例：

```
asa(config)#vpnclient mode network-extension-mode
```

ステップ 4 （任意） 必要な場合は、TCP カプセル化 IPsec を使用するように Easy VPN ハードウェア クライアントを設定します。

vpnclient ipsec-over-tcp [**port** *tcp_port*]

指定されていない場合、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。

TCP カプセル化 IPsec を使用するように Easy VPN リモートを設定する場合は、**crypto ipsec df-bit clear-df outside** コマンドを入力して、カプセル化ヘッダーから Don't Fragment（DF）ビットをクリアします。DF ビットは、パケットを断片化できるかどうかを決定する IP ヘッダー内のビットです。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 サイズよりも大きいパケットを送信できます。

例：

ポート 10501 で TCP カプセル化 IPsec を使用するように Easy VPN ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにします。

```
hostname(config)# vpnclient ipsec-over-tcp port 10501
hostname(config)# crypto ipsec df-bit clear-df outside
```

ステップ 5 次のいずれかの方法を使用して、Easy VPN サーバで設定されているトンネル グループを特定します。

- Easy VPN サーバ グループ ポリシーの名前とパスワード（事前共有鍵）を指定します。

vpnclient vpngroup *group_name* **password** *preshared_key*

- *group_name*：Easy VPN サーバ上に設定された VPN トンネル グループの名前。接続を確立する前に、このトンネル グループをサーバ上に設定する必要があります。
- *preshared_key*：Easy VPN サーバで認証に使用される IKE 事前共有キー。

たとえば、次のコマンドを入力して、TestGroup1 と呼ばれる VPN トンネル グループと IKE 事前共有キー my_key123 を指定します。

```
hostname(config)# vpnclient vpngroup TestGroup1 password my_key123
hostname(config)#
```

- グループ ポリシーを選択して認証する事前設定されたトラストポイントを指定します。

  vpnclient trustpoint *trustpoint_name* [**chain**]

  - *trustpoint_name*：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指定します。
  - **chain**（任意）：証明書チェーン全体を送信します。

  たとえば、次のコマンドを入力して central という名前の証明書を指定し、証明書チェーン全体を送信します。

```
hostname(config)# crypto ca trustpoint central
hostname(config)# vpnclient trustpoint central chain
hostname(config)#
```

ステップ 6 グループ ポリシーで NEM とスプリット トンネルが設定されている場合は、自動接続するように VPN トンネルを設定します。

vpnclient nem-st-autoconnect

ステップ 7 （任意） Easy VPN サーバのグループ ポリシーで個別ユーザ認証（IAU）と IP Phone Bypass が設定されている場合は、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には認証機能がないため、それらの認証を免除します。

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]

- アドレスのリストは 15 以下でなければなりません。
- *mac_addr*：個別ユーザ認証をバイパスするデバイスの MAC アドレス（ドット付きの 16 進数で表記）。
- *mac_mask*：対応する MAC アドレスのネットワーク マスク。

  MAC マスク ffff.ff00.0000 は、同一の製造業者が製造したすべてのデバイスに対応します。MAC マスク ffff.ffff.ffff は 1 つのデバイスに対応します。

  同じ製造業者のすべてのデバイスを MAC マスク ffff.ff00.0000 を使用して指定する場合は、特定の MAC アドレスの最初の 6 文字だけが必要です。

例：

Cisco IP Phone には、製造業者 ID として 00036b が設定されています。したがって、次のコマンドは、今後追加される可能性がある Cisco IP Phone も含めてすべての Cisco IP Phone を免除します。

```
hostname(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
hostname(config)#
```

（注） 次のように、個別ユーザ認証と IP Phone Bypass を Easy VPN サーバ グループ ポリシーに設定する必要があります。

```
hostname(config-group-policy)#user-authentication enable
hostname(config-group-policy)#ip-phone-bypass enable
```

ステップ 8 自動 Xauth ユーザ ログイン クレデンシャルを設定します。

vpnclient username *username* **password** *password*

ステップ 9 （任意） Easy VPN リモートのリモート監視を設定します。

デフォルトでは、管理トンネルは、SSH または HTTPS 暗号化で IPsec 暗号化を使用します。IPsec 暗号化を削除するか、またはこの暗号化を保持して特定のホストにのみ ASA の管理を許可するには、次のコマンドのいずれかを使用します。

- **vpnclient management clear**

  IPsec 暗号化レイヤをクリアして、VPN トンネル外部への管理アクセスを許可します。

- **vpnclient management tunnel ip_addr_1 ip_mask_1** [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

例：

次のコマンドを入力して IPSec トンネルの作成を自動化し、IP アドレス 192.168.10.10 のホストに管理アクセス権限を与えます。

```
hostname(config)# vpnclient management tunnel 192.198.10.10 255.255.255.0
```

（注） NAT デバイスが ASA Easy VPN リモートとインターネットの間で動作している場合は、ASA Easy VPN リモート上に管理トンネルを設定しないでください。そのような設定では、**vpnclient management clear** コマンドを使用して、リモート管理をクリアしてください。

ステップ 10 ASA で Easy VPN ハードウェア クライアントをイネーブルにします。

vpnclient enable

Easy VPN リモートをイネーブルにする前に、サーバ アドレス、モード、およびトンネル グループの仕様を設定する必要があります。

ステップ 11 （任意） 構成で Easy VPN トンネルが必要な場合は、手動で Easy VPN トンネルを接続します。

vpnclient connect

Easy VPN サーバの設定

始める前に

すべてのセカンダリ Easy VPN サーバに、プライマリ Easy VPN サーバと同じオプションと設定が指定されていることを確認します。

手順

ステップ 1 IPsec IKEv1 のサポート用に Easy VPN サーバを設定します。接続プロファイル、グループ ポリシー、およびユーザ を参照してください。

ステップ 2 特定の Easy VPN サーバ属性を設定します。VPN ハードウェア クライアントの属性の設定を参照してください。

Easy VPN の機能の履歴

機能名	リリース	機能情報
ASA 5506-X、5506W-X、5506H-X および 5508-X の Cisco Easy VPN クライアント	9.5(1)	このリリースは、ASA 5506-X シリーズでの Cisco Easy VPN の使用をサポートし、かつ ASA 5508-X 用の Cisco Easy VPN をサポートします。ASA は、VPN ヘッドエンドに接続すると VPN ハードウェア クライアントとして機能します。ASA の背後にある Easy VPN ポート上のデバイス（コンピュータ、プリンタなど）は、VPN 経由で通信できます。個別に VPN クライアントを実行する必要はありません。ASA インターフェイス 1 つのみで Easy VPN ポートとして機能できます。このポートに複数のデバイスを接続するには、レイヤ 2 スイッチをこのポート上に配置してから、このスイッチにデバイスを接続します。 次のコマンドが導入されました。**vpnclient enable**、**vpnclient server**、**vpnclient mode**、**vpnclient username**、**vpnclient ipsec-over-tcp**、**vpnclient management**、**vpnclient vpngroup**、**vpnclient trustpoint**、**vpnclient nem-st-autoconnect**、**vpnclient mac-exempt**

機能名	リリース	機能情報
BVI サポートのための Easy VPN 拡張	9.9(2)	Easy VPN は、ブリッジ型仮想インターフェイスを内部セキュア インターフェイスとしてサポートするように拡張され、管理者は新しい **vpnclient secure interface** [*interface-name*] コマンドを使用して内部セキュア インターフェイスを直接設定できるようになりました。 物理インターフェイスまたはブリッジ型仮想インターフェイスを内部セキュア インターフェイスとして割り当てることができます。これが管理者によって設定されていない場合、Easy VPN はそれが独立した物理インターフェイスまたは BVI かに関わらず、以前と同じセキュリティ レベルを使用してその内部セキュア インターフェイスを選択します。 また、管理アクセスがその BVI で有効になっている場合、**telnet**、**http**、**ssh** などの管理サービスを BVI で設定できるようになりました。 新規または変更されたコマンド：**vpnclient secure interface** [*interface-name*]、**https**、**telnet**、**ssh**、**management-access**