Easy VPN

この章では、Easy VPN サーバーとして任意の 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 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 サーバーで大部分の 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 サーバーへの 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 サーバーとして、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 サーバー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。ASDM で ASA を Easy VPN リモート ハードウェア クライアントとして設定するには、**[Configuration] > [VPN] > [Easy VPN Remote]** に移動します。Easy VPN サーバーでグループ ポリシー属性を設定する

には、 **[Configuration] > [Remote Access] > [Network (Client) Access] > [Group Policies] > [Advanced] > [IPsec (IKEv1) Client] > [Hardware Client]** に移動します。

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 サーバー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 サーバー 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 サーバーを使用する場合は、それらの設定をプライマリ サーバー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 サーバーの 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）サーバーを設定します。プライマリ サーバー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 サーバーへの接続を試み、次に VPN サーバー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 サーバー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 サーバー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 サーバー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ーは IPSec をユーザー 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ーを設定します。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 サーバー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 サーバーは、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ー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 サーバー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 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 サーバーはデフォルトでクライアント モードになります。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。

（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 ユーザー認証

ASA Easy VPN リモートは、自動ログイン用にユーザー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 サーバー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ー名およびパスワードを無視して、ユーザー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、Easy VPN サーバーで SUA をイネーブルにします。
- 個別ユーザー認証（IUA）：Easy VPN リモートの背後にいるユーザーは、企業 VPN ネットワークへのアクセス権限を得るために、ユーザー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、Easy VPN サーバーで 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）が個々のユーザー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 サーバーで IP Phone Bypass を指定し、Easy VPN リモートで MAC アドレス免除を指定します。

  さらに、Easy VPN サーバーは、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。

ユーザー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 サーバーは HTTP トラフィックを代行受信し、ユーザー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 サーバー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。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。

（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、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

Easy VPN リモート ハードウェア クライアントとして ASA を設定します。

（注） Cisco ASA with FirePOWER- 5506-X、5506W-X、5506H-X、および 5508-X モデルのみを、Easy VPN リモート ハードウェア クライアントとして設定できます。

はじめる前に

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 サーバーのアドレスと、セカンダリ サーバーのアドレスのアドレス（セカンダリ サーバーを使用できる場合）。
- 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 サーバー 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 サーバーに設定されている、VPN トンネルの使用を許可されたユーザー。

[Configuration] > [VPN] > [Easy VPN Remote]

[Enable Easy VPN Remote]：Easy VPN Remote 機能をイネーブルにして、このダイアログボックスの残りのフィールドを設定できるようにします。

[モード（Mode）] : [クライアントモード（Client mode）] または [ネットワーク拡張モード（Network extension mode）] を選択します。

- [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に企業ネットワークからアクセスできるようにします。

（注） Easy VPN リモートが NEM を使用しており、セカンダリ サーバーに接続している場合は、各ヘッドエンドへの ASDM 接続を確立し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Crypto Maps] で作成した暗号マップの [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。

- [Auto connect]：ネットワーク拡張モードがローカルに設定され、かつ Easy VPN リモートにプッシュされたグループ ポリシーに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 リモートは自動 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、この属性をオンにすると、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、この属性をオフにした場合、この属性は無視されます。

[Group Settings]：事前共有キーまたは X.509 証明書をユーザー認証に使用するかどうかを指定します。

- [Pre-shared key]：認証での事前共有キーの使用をイネーブルにして、以降の [Group Name]、[Group Password]、[Confirm Password] の各フィールドで、そのキーを含むグループ ポリシー名とパスワードを指定できるようにします。
  - [グループ名（Group Name）]：認証に使用するグループポリシーの名前を指定します。
  - [Group Password]：特定のグループ ポリシーで使用するパスワードを指定します。
  - [Confirm Password]：入力したグループ パスワードの確認を必須にします。
- [X.509 Certificate]：認証に対して、認証局から提供された X.509 デジタル証明書の使用を指定します。
  - [Select Trustpoint]：ドロップダウン リストからトラストポイントを選択できます。トラストポイントは IP アドレスまたはホスト名です。トラストポイントを定義するには、この領域の下部にある [Trustpoint(s) configuration] リンクをクリックします。
  - [証明書チェーンを送信（Send certificate chain）]：証明書だけでなく、証明書チェーンの送信もイネーブルにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。

[User Settings]：ユーザー ログイン情報を設定します。

- [ユーザー名（User Name）]：Easy VPN リモートの接続用 VPN ユーザー名を設定します。Xauth には、TACACS+ または RADIUS を使用して IKE 内のユーザーを認証する機能があります。Xauth は、RADIUS または別のサポートされているユーザー認証プロトコルを使用して、ユーザーを認証します（この場合、Easy VPN ハードウェア クライアント）。セキュア ユニット認証がディセーブルになっており、サーバーが Xauth クレデンシャルを要

求する場合には、Xauthユーザー名とパスワードパラメータが使用されます。セキュアユニット認証がイネーブルの場合、これらのパラメータは無視され、ASA によって、ユーザー名とパスワードの入力を求めるプロンプトが表示されます。

- [User Password] および [Confirm Password]：Easy VPN リモートの接続用 VPN ユーザー パスワードを設定して確認します。

[追加するEasy VPNサーバー（Easy VPN Server To Be Added）]：Easy VPN サーバーを追加または削除します。どの ASA も Easy VPN サーバーとして動作できます。接続を確立する前にサーバーを設定する必要があります。ASA は、IPv4 アドレス、名前データベース、または DNS 名をサポートしており、この順序でアドレスを解決します。Easy VPN Server(s) リストの最初のサーバーはプライマリ サーバーです。プライマリ サーバーに加え、最大 10 台のバックアップサーバーを指定できます。

- [Easy VPNサーバー（Easy VPN Server(s)）]：設定されている Easy VPN サーバーを優先順に一覧表示します。
- [Name or IP Address]：リストに追加する Easy VPN サーバーの名前または IP アドレス。
- [Add] および [Remove]：指定したサーバーを [Easy VPN Server(s)] リストに移動、またはリストから削除します。
- [Move Up] および [Move Down]：[Easy VPN Server(s)] リスト内でのサーバーの位置を変更します。これらのボタンは、リストにサーバーが 1 台以上存在する場合にだけ使用できます。

[Secure Client Interface]：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、ドロップダウンの選択肢からインターフェイスを選択します。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。

[Configuration] > [VPN] > [Easy VPN Remote] > [Advanced]

[MAC Exemption]：Easy VPN リモートの接続用デバイス パススルーで使用する MAC アドレスとマスクを設定します。Cisco IP Phone やプリンタなどのデバイスは、認証を実行できないため、個別ユニット認証に追加できません。これらのデバイスに対応するために、Individual User Authentication がイネーブルになっている場合には、MAC Exemption 属性によってイネーブルにされるデバイス パススルー機能が、指定した MAC アドレスを持つデバイスの認証を免除します。

- [MAC Address]：指定した MAC アドレスを持つデバイスの認証を免除します。

  このフィールドでMACアドレスを指定するための形式は3桁の16進数値で、45ab.ff36.9999のようにピリオドで区切られます。MAC アドレスの最初の 24 ビットは、その機器の製造元を示します。最後の 24 ビットは、ユニットの 16 進形式のシリアル番号です。

- [MAC Mask]：このフィールドでMACマスクを指定するときは、ピリオドで区切った3桁の16進数値の形式を使用します。たとえば、ffff.ffff.ffffというMACマスクは特定のMACアドレスとだけ一致します。すべてがゼロの MAC マスクは、いずれの MAC アドレスと

も一致しません。MAC マスク ffff.ff00.0000 は、製造業者が同じであるすべてのデバイスと一致します。

- [Add] および [Remove]：指定した MAC アドレスとマスクのペアを [MAC Address/Mask] リストに追加、またはリストから削除します。

[Tunneled Management]：デバイス管理のための IPsec 暗号化を設定し、トンネル経由での Easy VPN ハードウェア クライアント接続の管理を許可するネットワークを指定します。

- [トンネル化管理の有効化（Enable Tunneled Management）]：すでに管理トンネルに存在する SSH または HTTPS 暗号化に IPsec 暗号化レイヤを追加します。
- [Clear Tunneled Management]：暗号化を追加せず、すでに管理トンネルに存在する暗号化を使用します。[Clear Tunneled Management] を選択しても、IPsec の暗号化レベルが削除されるだけで、SSH や HTTP など、その接続に存在する他の暗号化には影響しません。
- [IPアドレス/マスク（IP Address/Mask）]：この領域の Enable または Clear 機能によって処理される、設定済みの IP アドレスとマスクのペアを一覧表示します。
  - [IP Address]：VPN トンネルを介した Easy VPN ハードウェア クライアントへの管理アクセスを許可するホストまたはネットワークの IP アドレスを指定します。
  - [Mask]：対応する IP アドレスのネットワーク マスクを指定します。
  - [Add/Remove]：指定した IP アドレスとマスクを [IP Address/Mask] リストに移動、またはリストから削除します。

[IPsec Over TCP]：Easy VPN リモートの接続に PCT カプセル化 IPsec を使用するように設定します。

（注） PCT カプセル化 IPsec を使用するように Easy VPN リモートの接続を設定する場合は、大きなパケットを送信するように ASA を設定する必要があります。

[Configuration] > [Remote Access VPN] > [Network （Client） Access] > [Advanced] > [IPsec] > [Fragmentation Policies] に移動し、外部インターフェイスをダブルクリックして、[DF Bit Setting Policy] を [Clear] に設定します。

- [イネーブル（Enable）]：IPsec over TCP をイネーブルにします。
- [Enter Port Number]：IPsec over TCP 接続で使用するポート番号を指定します。

[Server Certificate]：証明書マップで指定された特定の証明書を持つ Easy VPN サーバーとの接続だけを許可するように、Easy VPN リモートの接続を設定します。このパラメータを使用して、Easy VPN サーバー証明書のフィルタリングをイネーブルにします。

Easy VPN サーバーの設定

始める前に

すべてのセカンダリ Easy VPN サーバーに、プライマリ Easy VPN サーバー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 サーバーを設定します。一般的な VPN 設定 を参照してください。

ステップ 2 特定の Easy VPN サーバー属性を設定します。内部グループ ポリシー、IPsec（IKEv1）のハードウェア クライアント属性 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 VPN の使用をサポートし、かつ ASA 550 Easy VPN をサポートします。ASA は、V ドに接続すると VPN ハードウェア クラ 機能します。ASA の背後にある Easy VP バイス（コンピュータ、プリンタなど） 通信できます。個別に VPN クライアン 要はありません。ASA インターフェイス VPN ポートとして機能できます。このポ バイスを接続するには、レイヤ 2 スイッ 上に配置してから、このスイッチにデバ す。 次の画面が導入されました。[Configurati [Easy VPN Remote]

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 セキュアインターフェイスとしてサポート 張され、管理者は新しい **vpnclient secure int** [*interface-name*] コマンドを使用して内部セキ ターフェイスを直接設定できるようになり 物理インターフェイスまたはブリッジ型仮想 フェイスを内部セキュアインターフェイスと てることができます。これが管理者によって いない場合、Easy VPN はそれが独立した物 フェイスまたはBVIかに関わらず、以前と同 ティ レベルを使用してその内部セキュア イ 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 合、**telnet**、**http**、**ssh** などの管理サービスを できるようになりました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、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。