Easy VPN

Easy VPN は、さまざまなルータ、PIX、および ASA デバイスで使用できるハブアンドスポーク VPN トポロジです。ほとんどのポリシーはハブで定義され、リモート スポーク VPN デバイスにプッシュされるため、クライアントには、セキュアな接続を確立する前に確実に最新のポリシーが配置されます。

この章は次のトピックで構成されています。

Easy VPN について

Easy VPN を使用すると、リモート オフィスの VPN 展開が容易になります。Easy VPN では、ヘッドエンドに定義されたセキュリティ ポリシーがリモート VPN デバイスにプッシュされるため、クライアントには、セキュアな接続を確立する前に確実に最新のポリシーが配置されます。

Security Manager では、ハブアンドスポーク VPN トポロジにおける Easy VPN ポリシーの設定がサポートされています。このような設定では、ほとんどの VPN パラメータは、ハブ デバイスとして機能する Easy VPN サーバに定義されます。集中管理された IPsec ポリシーは、サーバによって Easy VPN クライアント デバイスにプッシュされるため、リモート（スパイク）デバイス設定を最小限に抑えることができます。

Easy VPN サーバーは、Cisco IOS ルータ、PIX ファイアウォール、または ASA 5500 シリーズ デバイスです。Easy VPN クライアントは、PIX 6.3 を実行する PIX 501、506、506E Firewall、Cisco 800 ～ 3900 シリーズ ルータ、および ASA ソフトウェア リリース 7.2 以降を実行する ASA 5505 デバイスでサポートされます。

バージョン 4.17 以降、Cisco Security Manager は BVI による Easy VPN のサポートを提供します。通常、Easy VPN は、ASA の起動時に最高および最低のセキュリティレベルのインターフェイスを判別します。最も低いセキュリティレベルのインターフェイスは、VPN クライアントが

ヘッドエンドへのトンネリングを開始する外部インターフェイスとして使用され、最も高いセキュリティレベルのインターフェイスは、内部のセキュリティで保護されたインターフェイスとして使用されます。

ASA5506 プラットフォームでは、デフォルト設定に、最高セキュリティ レベル インターフェイスを示す 100 に設定された BVI（そのメンバーインターフェイスもレベル 100 に設定）と、セキュリティレベルが 0 の外部インターフェイスが含まれます。VPN クライアントは、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を拒否します。Easy VPN によって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、VPN クライアントが無効になります。

この問題を解決するために、ASA 9.9(2) 以降のすべての ASA 5506、5508、および 5512 [x/h/w] デバイスに vpnclient secure interface CLI が導入されました。そのため、Cisco Security Manager で CLI をサポートするために、バージョン 4.17 以降、新しいコンポーネント「VPN クライアント インターフェイス」がタイプ（Easy VPN）のハブアンドスポークトポロジに導入されました。

（注） Easy VPN トポロジで使用されるポリシーの中には、リモート アクセス VPN で使用されるポリシーに類似しているものもあります。リモート アクセス VPN では、ポリシーはサーバと VPN クライアント ソフトウェアを実行するモバイル リモート PC との間に設定されますが、サイト間 Easy VPN トポロジでは、クライアントはハードウェア デバイスです。

ここでは、次の内容について説明します。

Easy VPN とダイヤル バックアップ

Easy VPN のダイヤル バックアップを使用すると、リモート クライアント デバイスにダイヤル バックアップ トンネル接続を設定できます。このバックアップ機能は、実際のトラフィックの送信準備が完了したときにだけアクティブになります。これにより、トラフィックがない場合に高価なダイヤルアップまたは ISDN リンクを作成および維持する必要がなくなります。

（注） Easy VPN ダイヤル バックアップは、IOS バージョン 12.3(14)T 以降を実行するルータであるリモート クライアントにだけ設定できます。

Easy VPN 設定では、リモート デバイスがサーバへの接続を試み、追跡された IP がアクセスできない場合には、プライマリ接続がティアダウンされて、Easy VPN バックアップ トンネル経由でサーバへの新しい接続が確立されます。プライマリ ハブに到達できない場合は、プライマリ設定が、バックアップ設定ではなく、同じプライマリ設定を持つフェールオーバー ハブに切り替えられます。

各プライマリ Easy VPN 設定では、1 つのバックアップ設定だけがサポートされています。各内部インターフェイスでは、プライマリおよびバックアップの Easy VPN 設定を指定する必要があります。Easy VPN リモート デバイスでダイヤル バックアップが動作するためには、IP スタティック ルート トラッキングが設定されている必要があります。オブジェクト トラッキング設定は、Easy VPN リモート ダイヤル バックアップ設定とは独立しています。オブジェクト トラッキングの詳細は、スポークの [エンドポイントの編集（Edit Endpoints）] ダイアログボックスで指定します。

ダイヤル バックアップの詳細については、ダイヤル バックアップの設定を参照してください。

ハイ アベイラビリティ Easy VPN

Easy VPN トポロジ内のデバイスにハイ アベイラビリティ（HA）を設定できます。LAN 上で IP を実行する Cisco IOS ルータまたは Catalyst 6500/7600 デバイスに High Availability（HA; ハイ アベイラビリティ）を設定すると、自動デバイス バックアップ機能を使用できます。Easy VPN に、Hot Standby Routing Protocol（HSRP）を使用して透過的な自動デバイス フェールオーバーを提供する 2 つ以上のハブ デバイスで構成された HA グループを作成できます。詳細については、VPN トポロジにおけるハイ アベイラビリティの設定を参照してください。

Easy VPN とダイナミック仮想トンネル インターフェイス

IPsec Virtual Tunnel Interface（VTI; 仮想トンネル インターフェイス）機能を使用すると、IPsec によって保護する必要がある、リモート アクセス リンク用の GRE トンネルの設定が簡素化されます。VTI は、IPsec トンネリングをサポートするインターフェイスです。VTI を使用すると、IPsec トンネルに直接インターフェイス コマンドを適用できます。仮想トンネル インターフェイスの設定では、クリプトマップが適用されている特定の物理インターフェイスに対する IPsec セッションのスタティック マッピングが不要であるため、オーバーヘッドが低減されます。

IPsec VTI では、任意の物理インターフェイスにおいて、ユニキャストとマルチキャストの両方の暗号化されたトラフィックがサポートされます（複数のパスがある場合など）。トラフィックは、トンネル インターフェイスから転送されるときに暗号化され、トンネル インターフェイスに転送されると復号化されます。また、IP ルーティング テーブルによって管理されます。ダイナミックまたはスタティック IP ルーティングを使用して、仮想トンネル インターフェイスにトラフィックをルーティングできます。IP ルーティングを使用してトンネル インターフェ

イスにトラフィックを転送することによって、アクセス コントロール リスト（ACL）とクリプト マップを使用する複雑なプロセスと比較して IPsec VPN 設定が簡素化されます。ダイナミック VTI は、他のすべての実際のインターフェイスと同様に機能するため、トンネルがアクティブになるとすぐに Quality of Service（QoS）、ファイアウォール、およびその他のセキュリティ サービスを適用できます。

ダイナミック VTI では、IPsec インターフェイスの動的なインスタンス化および管理のために、仮想テンプレート インフラストラクチャが使用されます。Easy VPN トポロジでは、Security Manager によって暗黙的にデバイスに仮想テンプレートインターフェイスが作成されます。デバイスがハブの場合、ユーザは、ハブに仮想テンプレートインターフェイスとして使用される IP アドレスを指定する必要があります。この IP アドレスには、サブネット（アドレスのプール）、既存のループバック インターフェイス、または既存の物理インターフェイスを指定できます。スポークでは、仮想テンプレートインターフェイスは IP アドレスなしで作成されます。

Security Manager では、[Easy VPN IPsec Proposal] ページでダイナミック VTI を設定します。Easy VPN に対するダイナミック VTI の設定 （17 ページ）を参照してください。

注記

- ダイナミック VTI は、ハブアンドスポーク VPN トポロジにおいて、IOS バージョン 12.4(2)T 以降を実行する 7600 デバイスを除くルータでだけ設定できます。PIX ファイアウォール、ASA デバイス、または Catalyst 6000 シリーズ スイッチではサポートされていません。
- 検出またはプロビジョニング中に、すべてのハブおよびスポークにダイナミック VTI 設定が必要なわけではありません。（dVTI をサポートしていないルータを含む）既存の Easy VPN トポロジを拡張して、dVTI をサポートするルータを追加できます。
- ダイナミック VTI は、サーバのみ、クライアントのみ（サーバが dVTI をサポートしていない場合）、およびクライアントとサーバの両方でサポートされます。
- dVTI が設定されたハブ（サーバ）には、ハイ アベイラビリティを設定できません。
- リモート アクセス VPN でもダイナミック VTI を設定できます。詳細については、リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス）を参照してください。

Easy VPN コンフィギュレーション モード

Easy VPN は、Client、Network Extension、および Network Extension Plus の 3 つのモードで設定できます。

- Client モード：クライアント サイトのデバイスがセントラル サイトのリソースにアクセスできるデフォルトの設定です。ただし、セントラル サイトからクライアント サイトのリソースへはアクセスできません。Client モードでは、VPN 接続が確立されると、単一の IP アドレスがサーバからリモート クライアントにプッシュされます。通常、このアドレスは、お客様のネットワークのプライベート アドレス空間内でルーティング可能なアドレスです。Easy VPN トンネルを通過するすべてのトラフィックでは、そのプッシュされた単一の IP アドレスへのポート アドレス変換（PAT）が実行されます。

- Network Extension モード：セントラル サイトのユーザは、クライアント サイトのネットワーク リソースにアクセスできます。また、クライアント PC およびホストは、セントラル サイトの PC およびホストに直接アクセスできます。Network Extension モードでは、宛先ネットワークで完全にルーティング可能で、宛先ネットワークから到達可能な IP アドレスを VPN トンネルのクライアント側終端にあるホストに設定することが指定されます。接続の両端のデバイスは、一体となって 1 つの論理ネットワークを形成します。PAT は使用されないため、クライアント側終端のホストは、宛先ネットワークのホストに直接アクセスできます。つまり、ルーティング可能なアドレスが Easy VPN サーバ（ハブ）から Easy VPN クライアント（スポーク）に設定され、クライアントの背後にある LAN において PAT は実行されません。
- Network Extension Plus モード：Network Extension モードを機能拡張したもので、IOS ルータにだけ設定できます。モード設定を介して受信した IP アドレスを、使用可能なループバック インターフェイスに自動的に割り当てることができます。この IP アドレスを使用してルータに接続し、リモート管理およびトラブルシューティング（ping、Telnet、およびセキュア シェル）を行うことができます。このオプションの選択時に一部のクライアントが IOS ルータでない場合、それらのクライアントは Network Extension モードで設定されません。

（注） すべての動作モードで、スプリット トンネリングをサポートすることもできます。スプリット トンネリングを使用すると、VPN トンネル経由で企業リソースに安全にアクセスできることに加えて、ISP などのサービスへの接続を使用したインターネット アクセスも可能となります（そのため、Web アクセス用のパスから企業ネットワークを除外できます）。

Easy VPN のクライアント接続特性の設定 （9 ページ）の説明に従って、Client Connection Characteristics ポリシー内のモードを設定します。

関連項目

- Easy VPN 設定に関する重要事項 （8 ページ）
- Easy VPN について （1 ページ）

Easy VPN および IKE 拡張認証（Xauth）

Easy VPN 設定で IPsec トンネルを確立するためのトンネル パラメータをネゴシエートする場合、IKE Extended Authentication（Xauth; 拡張認証）によって、IPsec 接続を要求するユーザを識別する、追加の認証レベルが追加されます。VPN サーバに Xauth が設定されている場合、IKE Security Association（SA; セキュリティ アソシエーション）の確立後、クライアントは「ユーザ名/パスワード」チャレンジを待機します。エンド ユーザがチャレンジに応答すると、その応答は IPsec ピアに転送され、さらに上のレベルの認証が行われます。

入力された情報は、RADIUS や TACACS+ などの認証、許可、アカウンティング（AAA）プロトコルを使用して認証エンティティに照らしてチェックされます。トークン カードは、AAA プロキシを介して使用することもできます。Xauth 中、ユーザのクレデンシャルが RADIUS を介して検証される場合に、そのユーザに固有の属性を取得できます。

（注） リモート クライアントを処理するように設定されている VPN サーバは、ユーザ認証を実行するように常に設定されている必要があります。

Security Manager では、Easy VPN トンネルを確立するたびにこれらのクレデンシャルを手動で入力する必要がないように、デバイス自体に Xauth ユーザ名およびパスワードを保存できます。情報は、デバイスの設定ファイルに保存され、トンネルが確立されるたびに使用されます。クレデンシャルをデバイスの設定ファイルに保存する方法は、一般的に、デバイスを複数の PC で共有し、VPN トンネルを常にアップ状態にする場合や、送信するトラフィックがある場合は常に自動的にデバイスでトンネルを確立する場合に使用します。

ただし、デバイスの設定ファイルにクレデンシャルを保存すると、デバイス設定にアクセスできるすべてのユーザーがこの情報を入手できるため、セキュリティ上のリスクとなる可能性があります。Xauth 認証のもう 1 つの方法として、Xauth が要求されるたびにユーザ名とパスワードを手動で入力する方法があります。クレデンシャルの入力に Web ブラウザ ウィンドウまたはルータ コンソールのどちらを使用するかを選択できます。Web ベースの対話形式を使用すると、ログインページが表示され、そのページで VPN トンネルを認証するためのクレデンシャルを入力できます。VPN トンネルが確立されると、このリモートサイトの背後のすべてのユーザは、再度ユーザ名とパスワードを求められることなく企業 LAN にアクセスできます。または、VPN トンネルを迂回して、インターネットにだけ接続することもできます。この場合、パスワードは必要ありません。

Easy VPN トンネル アクティベーション

デバイスのクレデンシャル（Xauth ユーザ名とパスワード）がデバイス自体に保存されている場合は、IOS ルータ クライアントのトンネルのアクティベーション方法を選択する必要があります。2 つのオプションから選択できます。

- [Auto]：Easy VPN トンネルは、Easy VPN 設定がデバイス設定ファイルに配信されると自動的に確立されます。トンネルでタイムアウトまたは障害が発生した場合、トンネルは自動的に再接続し、無制限に再試行します。これがデフォルトのオプションです。
- [Traffic Triggered Activation]：Easy VPN トンネルは、発信ローカル（LAN 側）トラフィックが検出されるたびに確立されます。トンネル経由で送信するトラフィックがある場合にだけバックアップ トンネルがアクティブになるように、Easy VPN ダイヤル バックアップ設定では [Traffic Triggered Activation] を使用することを推奨します。このオプションを使用している場合は、「対象の」トラフィックを定義するアクセスコントロールリスト（ACL）を指定する必要があります。

（注） Xauth パスワードを対話形式で設定することを選択した場合は、手動によるトンネルのアクティベーションが暗黙的に設定されます。この場合、デバイスは、Easy VPN リモート接続の確立を試みる前にコマンドを待機します。トンネルでタイムアウトまたは障害が発生した場合は、後続の接続においてもコマンドを待機する必要があります。

Easy VPN のクライアント接続特性の設定 （9 ページ）の説明に従って、Client Connection Characteristics ポリシー内の xauth およびトンネル アクティベーション モードを設定します。

関連項目

- Easy VPN 設定に関する重要事項 （8 ページ）
- Easy VPN について （1 ページ）
- クレデンシャル ポリシー オブジェクトの設定 （12 ページ）

Easy VPN の設定の概要

リモート クライアントから VPN サーバに接続が開始されると、IKE を使用したピア間でのデバイス認証、IKE Extended Authentication（Xauth; 拡張認証）を使用したユーザ認証、VPN ポリシーのプッシュ（Client、Network Extension、または Network Extension Plus モード）、および IPsec Security Association（SA; セキュリティ アソシエーション）の作成が順に実行されます。

次に、このプロセスの概要を示します。

1. 認証に事前共有キーが使用される場合はアグレッシブ モードを、デジタル証明書が使用される場合はメイン モードを使用して、クライアントによって IKE フェーズ 1 が開始されます。クライアントが自身を事前共有キーによって識別する場合は、付随するユーザ グループ名（設定時に定義されます）を使用して、このクライアントに関連付けられているグループ プロファイルが特定されます。デジタル証明書が使用される場合は、Distinguished Name（DN; 識別名）の Organizational Unit（OU; 組織ユニット）フィールドを使用してユーザ グループ名が特定されます。[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブを参照してください。

（注） クライアントで、IKE アグレッシブ モードが開始される事前共有キー認証が設定される可能性があるため、管理者は、crypto isakmp identity hostname コマンドを使用して、VPN デバイスのアイデンティティを変更する必要があります。この操作は、IKE メイン モードを使用した証明書認証には影響しません。

1. クライアントは、クライアントのパブリック IP アドレスと VPN サーバのパブリック IP アドレスとの間で IKE SA の確立を試みます。クライアントに手動で設定する作業量を減らすために、暗号化アルゴリズム、ハッシュ アルゴリズム、認証方式、および D-H グループ サイズのあらゆる組み合わせが提案されます。

2. IKE ポリシー設定に応じて、VPN サーバはどのプロポーザルを受け入れてフェーズ 1 のネゴシエーションを続行するかを判断します。

（注） この時点でデバイス認証が終了し、ユーザ認証が開始されます。

1. IKE SA が正常に確立され、VPN サーバーに Xauth が設定されている場合、クライアントは「ユーザー名/パスワード」チャレンジを待機して、ピアのチャレンジに応答します。入力された情報は、RADIUS や TACACS+ などの認証、許可、アカウンティング（AAA）プロトコルを使用して認証エンティティに照らしてチェックされます。トークンカードは、AAA プロキシを介して使用することもできます。Xauth 中、ユーザのクレデンシャルが RADIUS を介して検証される場合に、そのユーザに固有の属性を取得できます。

（注） リモート クライアントを処理するように設定されている VPN サーバは、ユーザ認証を実行するように常に設定されている必要があります。

1. サーバから認証が成功したことを通知されると、クライアントはさらにピアから設定パラメータを要求します。残りのシステム パラメータ（IP アドレス、DNS、スプリット トンネル属性など）が、Client モードまたは Network Extension モード設定を使用してクライアントにプッシュされます。

（注） （Rivest, Shamir, and Adelman（RSA）の署名が使用されていない場合）IP アドレス プールおよびグループ事前共有キーだけがグループ プロファイルで必要なパラメータです。その他すべてのパラメータはオプションです。

1. モード設定を介して各クライアントに内部 IP アドレスが割り当てられたあと、Reverse Route Injection（RRI; 逆ルート注入）によってデバイスの各クライアント内部 IP アドレスに対してスタティック ルートが作成されます（RRI が設定されている場合）。
2. IKE クイック モードが開始されて、IPsec SA のネゴシエーションおよび作成が行われます。

これで、接続が完了します。

Easy VPN 設定に関する重要事項

トポロジに Easy VPN ポリシーを設定する前に、次の事項を把握しておく必要があります。

- Easy VPN トポロジ設定では、リモート クライアント デバイスとして 72xx シリーズ ルータが使用されていると展開に失敗します。Easy VPN クライアントは、PIX 6.3 を実行する

PIX 501、506、506E Firewall、Cisco 800 ～ 3900 シリーズ ルータ、および ASA ソフトウェア リリース 7.2 以降を実行する ASA 5505 デバイスでサポートされます。

- Easy VPN トポロジ設定において PIX 6.3 リモート クライアントに Public Key Infrastructure（PKI）ポリシーの設定を試みると、展開に失敗します。このデバイスに正常に展開するには、最初に CA サーバに PKI 証明書を発行してから、再度デバイスの展開を試みます。PKI ポリシーの詳細については、Public Key Infrastructure ポリシーについてを参照してください。
- 外部インターフェイスではなく NAT（または PAT）内部インターフェイスにクリプトマップが設定されている場合は、Easy VPN クライアントとして機能するデバイスで展開が失敗する場合があります。一部のプラットフォームでは、内部インターフェイスと外部インターフェイスが固定されています。たとえば、Cisco 1700 シリーズルータでは、VPN インターフェイスはデバイスの FastEthernet0 インターフェイスである必要があります。Cisco 800 シリーズルータでは、VPN インターフェイスは設定に応じてデバイスの Ethernet0 インターフェイスまたは Dialer1 インターフェイスのいずれかです。Cisco uBR905 および uBR925 ケーブル アクセス ルータでは、VPN インターフェイスは Ethernet0 インターフェイスである必要があります。

Easy VPN のクライアント接続特性の設定

[Client Connection Characteristics] ページを使用して、Easy VPN トポロジにおけるトラフィックのルーティング方法、および VPN トンネルの確立方法を指定します。このポリシーで定義する特性は、リモート クライアントに対して設定されます。このポリシーを設定する前に、次のトピックを参照してください。

- Easy VPN コンフィギュレーション モード （4 ページ）
- Easy VPN および IKE 拡張認証（Xauth） （5 ページ）

ナビゲーション パス

- （[Site-to-Site VPN Manager] ウィンドウ）VPN セレクタで Easy VPN トポロジを選択して、ポリシーセレクタで [クライアント接続特性（Client Connection Characteristics）] を選択します。
- （ポリシービュー）[サイト間VPN（Site-to-Site VPN）] > [クライアント接続特性（Client Connection Characteristics）] を選択して新しいポリシーを作成するか、既存のポリシーを編集します。

関連項目

- Easy VPN について （1 ページ）
- アクセス コントロール リスト オブジェクトの作成
- Easy VPN 設定に関する重要事項 （8 ページ）

フィールド リファレンス

表 *1 : [Easy VPN Client Connection Characteristics]* ページ

要素	説明
[モード（Mode）]	リモート デバイスのコンフィギュレーション モード： • [クライアント（Client）]：リモートクライアントの内部ネットワークからのすべてのトラフィックに対して、接続時にヘッドエンドサーバーによってデバイスに割り当てられた単一 IP アドレスへのポートアドレス変換（PAT）を実行することを指定します。 • [ネットワーク拡張（Network Extension）]：宛先ネットワークで完全にルーティング可能で、宛先ネットワークから到達可能な IP アドレスを VPN トンネルのクライアント側終端にある PC およびその他のホストに設定することを指定します。PAT は使用されないため、クライアント PC およびホストは、宛先ネットワークの PC およびホストに直接アクセスできます。 • [ネットワーク拡張プラス（Network Extension Plus）]：ネットワーク拡張モードを機能拡張したもので、モード設定を介して受信した IP アドレスを、使用可能なループバック インターフェイスに自動的に割り当てることができます。この IP アドレスの IPsec SA は、Easy VPN クライアントによって自動的に作成されます。通常、IP アドレスは、（ping、Telnet、およびセキュア シェルを使用した）トラブルシューティングに使用されます。 [Network Extension Plus] を選択する場合、このモードは IOS ルータに対してのみ設定されます。PIX デバイスまたは ASA デバイスであるクライアントは、Network Extension モードで設定されます。 詳細については、 Easy VPN コンフィギュレーション モード （4 ページ）を参照してください。
Xauth Credentials Source	サーバとの VPN 接続を確立する場合にユーザ認証用の Xauth クレデンシャルを入力する方法を次のように選択します。 • [デバイスに保存されたクレデンシャル（Device Stored Credentials）]（デフォルト）：ユーザ名とパスワードはデバイス自体のデバイスの設定ファイルに保存され、トンネルが確立されるたびにこの情報が使用されます。 • [Interactive Entered Credentials]：Web ブラウザのウィンドウまたはルータ コンソールで、Xauth が要求されるたびに手動でユーザ名とパスワードを入力できます。 詳細については、 Easy VPN および IKE 拡張認証（Xauth） （5 ページ）を参照してください。

要素	説明
Xauth Credentials	[Xauthクレデンシャルソース（Xauth Credentials Source）] として [デバイスに保存されたクレデンシャル（Device Stored Credentials）] を選択した場合にだけ使用できます。 デフォルトの Xauth クレデンシャルを定義するクレデンシャル ポリシー オブジェクトです。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。詳細については、クレデンシャル ポリシー オブジェクトの設定 （12 ページ）を参照してください。 （注） リモートクライアントに異なる Xauth クレデンシャルを設定する場合は、オーバーライドを許可するようにクレデンシャル ポリシー オブジェクトを設定する必要があります（オブジェクト定義で [デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択します）。
Tunnel Activation（IOS）	Xauth パスワードソースに対して [デバイスに保存されたクレデンシャル（Device Stored Credentials）] オプションを選択した場合にのみ使用できます。 IOS ルータ クライアントについて、トンネルのアクティベーション方法を選択します。 • [自動（Auto）]（デフォルト）：Easy VPN トンネルは、Easy VPN 設定がデバイス設定ファイルに配信されると自動的に確立されます。トンネルでタイムアウトまたは障害が発生した場合、トンネルは自動的に再接続し、無制限に再試行します。 • [トラフィックトリガーアクティベーション（Traffic Triggered Activation）]：Easy VPN トンネルは、発信ローカル（LAN 側）トラフィックが検出されるたびに確立されます。[Traffic Triggered Activation] を選択する場合は、トンネルをアクティブにするトラフィックを定義するアクセス コントロール リスト（ACL）ポリシーオブジェクトの名前も入力します。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。 トンネル経由で送信するトラフィックがある場合にだけバックアップ トンネルがアクティブになるように、Easy VPN ダイヤル バックアップ設定では [Traffic Triggered Activation] を使用することを推奨します。 （注） Xauth パスワードを対話形式で設定することを選択した場合は、手動によるトンネルのアクティベーションが暗黙的に設定されます。

要素	説明
User Authentication Method（IOS）	Xauth クレデンシャルソースに対して [インタラクティブに入力されたクレデンシャル（Interactive Entered Credentials）] オプションを選択した場合にのみ使用できます。このオプションは、リモート IOS ルータにのみ適用されます。 Xauth 認証が要求されるたびに対話形式で Xauth ユーザ名とパスワードを入力するための方法として、次のいずれかを選択します。 • [Web Browser]（デフォルト）：Web ブラウザ ウィンドウで手動で入力します。 • [ルータコンソール（Router Console）]：ルータのコマンド行から手動で入力します。

クレデンシャル ポリシー オブジェクトの設定

[Credentials] ダイアログボックスを使用して、クレデンシャル オブジェクトを作成、コピー、および編集します。

クレデンシャル オブジェクトは、認証ユーザがネットワークおよびネットワーク サービスにアクセスする場合の IKE Extended Authentication（Xauth; 拡張認証）中に、Easy VPN 設定で使用されます。Easy VPN 設定で IPsec トンネルを確立するためのトンネル パラメータをネゴシエートする場合、Xauth によって IPsec 接続を要求するユーザが識別されます。VPN サーバーに Xauth が設定されている場合、IKE SA の確立後、クライアントは「ユーザー名/パスワード」チャレンジを待機します。エンドユーザがチャレンジに応答すると、その応答は IPsec ピアに転送され、さらに上のレベルの認証が行われます。Xauth クレデンシャル（ユーザ名とパスワード）はデバイス自体に保存できるため、Easy VPN トンネルが確立されるたびに Xauth クレデンシャルを手動で入力する必要はありません。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [ログイン情報（Credentials）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- Easy VPN および IKE 拡張認証（Xauth） （5 ページ）
- Easy VPN のクライアント接続特性の設定 （9 ページ）
- Policy Object Manager

フィールド リファレンス

表 2 : [Credentials] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）最大 1024 文字のオブジェクトの説明。
ユーザー名	Xauth 認証時にユーザの識別に使用される名前。
パスワード 確認（Confirm）	両方のフィールドに入力される、ユーザのパスワード。パスワードは、英数字で、最大 128 文字である必要があります。スペースは使用できません。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

Easy VPN での IPsec プロポーザルの設定

[Easy VPN IPsec Proposal] ページを使用して、Easy VPN トポロジの IKE フェーズ 2 ネゴシエーション中に使用される IPsec プロポーザルを設定します。IPsec プロポーザルは [IPSec Proposal] タブで設定されます。オプションについては、以下に説明されています。

Easy VPN トポロジでは、[Dynamic VTI] タブでダイナミック仮想インターフェイスを設定することもできます。dVTI 設定の説明については、Easy VPN に対するダイナミック VTI の設定（17 ページ）を参照してください。

（注） このトピックでは、サイト間 VPN テクノロジーが Easy VPN である場合の [IPsec Proposal] ページを説明します。サイト間 VPN テクノロジーが異なる場合の [IPsecプロポーザル（IPsec Proposal）] ページの説明については、サイト間 VPN での IPsec プロポーザルの設定を参照してください。

ナビゲーション パス

- （[Site-to-Site VPN Manager] ウィンドウ）VPN セレクタで Easy VPN トポロジを選択して、ポリシーセレクタで [IPsecプロポーザル（IPsec Proposal）] を選択します。[IPsecプロポーザル（IPsec Proposal）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）]>[簡単なIPsecプロポーザル（Easy IPsec Proposal）] を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。[IPsecプロポーザル（IPsec Proposal）] タブをクリックします。

関連項目

- Easy VPN について （1 ページ）
- Easy VPN での IPsec プロポーザルの設定 （13 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて
- IPsec プロポーザルについて

フィールド リファレンス

表 3 : [Easy VPN IPsec Proposal] タブ

要素	説明
IKEv1 トランスフォーム セット	トンネル ポリシーで使用するトランスフォーム セット。トランスフォーム セットは、トンネル内のトラフィックの確立に使用される認証アルゴリズムおよび暗号化アルゴリズムを指定します。最大11個のトランスフォーム セットを選択できます。詳細については、トランスフォーム セットの概要を参照してください。 トランスフォーム セットでは、トンネル モードの IPsec 動作だけを使用できます。 選択したトランスフォーム セットの 2 つ以上が両方のピアでサポートされている場合は、最も高いセキュリティを提供するトランスフォーム セットが使用されます。 [選択（Select）] をクリックして、トポロジで使用する IPsec トランスフォーム セット ポリシー オブジェクトを選択します。必要なオブジェクトがまだ定義されていない場合、選択ダイアログボックスの使用可能なオブジェクト リストの下にある [作成（Create）]（+）ボタンをクリックして、新しいオブジェクトを作成できます。詳細については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定を参照してください。

要素	説明
Reverse Route	ASA 5500 シリーズ デバイス、PIX 7.0+ デバイス、および 7600 デバイス以外の Cisco IOS ルータでサポートされます。 リバース ルート インジェクション（RRI）により、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。詳細については、逆ルート注入についてを参照してください。 次のいずれかのオプションを選択して、クリプト マップで RRI を設定します。 • [なし（None）]：クリプトマップで RRI の設定を無効にします。 • [標準（Standard）]（ASA、PIX 7.0+、IOS デバイス）：クリプトマップアクセス制御リスト（ACL）に定義された宛先情報に基づいてルートを作成します。これがデフォルトのオプションです。 • [リモートピア（Remote Peer）]（IOS デバイスのみ）：リモートエンドポイント用に 1 つ、クリプトマップが適用されるインターフェイス経由でのリモートエンドポイントへのルート再帰用に 1 つ、合計 2 つのルートを作成します。 • [リモートピア IP（Remote Peer IP）]（IOS デバイスのみ）：アドレスをリモート VPN デバイスへの明示的なネクストホップとして指定します。IP アドレス、またはアドレスを指定するネットワーク/ホストオブジェクトを入力します。あるいは、[選択（Select）] をクリックして、リストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） ネットワークまたはホストオブジェクトを使用する場合は、オブジェクトで [デバイスごとの値のオーバーライドを許可（Allow Value Override per Device）] オプションを選択し、必要に応じて、このオブジェクトを使用する特定のデバイスの IP アドレスをオーバーライドできます。
Enable Network Address Translation Traversal	PIX 7.0+ および ASA 5500 シリーズ デバイスでサポートされます。 ネットワーク アドレス変換（NAT）通過を許可するかどうか。 NAT 通過は、VPN 接続されたハブとスポークの間に、IPsec トラフィックに対してネットワーク アドレス変換（NAT）を実行するデバイスがある場合に使用します。NAT 通過については、VPN での NAT についてを参照してください。

要素	説明
Group Policy Lookup/AAA Authorization Method	Cisco IOS ルータでだけサポートされます。 グループ ポリシーを検索する順序を定義するために使用される AAA 認可方式リスト。グループ ポリシーは、ローカル サーバまたは外部 AAA サーバ上に設定できます。リモート ユーザはグループ化され、リモート クライアントから VPN サーバに接続が正常に確立されたときに、その特定のユーザ グループのグループ ポリシーがユーザ グループに属するすべてのクライアントにプッシュされます。 [選択（Select）] をクリックすると、使用可能なすべての AAA グループサーバーを表示したダイアログボックスが開き、そこで、AAA グループ サーバー オブジェクトを作成できます。該当する項目をすべて選択し、上矢印ボタンと下矢印ボタンを使用してプライオリティ順に並べ替えます。
User Authentication (Xauth)/AAA Authentication Method	Cisco IOS ルータおよび PIX 6.3 ファイアウォールのみでサポートされます。 ユーザ アカウントの検索順序を定義するために使用される AAA または Xauth ユーザ認証方式。 Xauth では、すべての AAA 認証方式で、IKE 認証フェーズ 1 の交換後に別のフェーズでユーザ認証を実行できます。ユーザ認証が実行されるためには、AAA 設定リスト名が Xauth 設定リスト名と一致する必要があります。 デバイスに Xauth が設定されている場合、クライアントは、IKE SA が正常に確立されたあとで、「ユーザ名/パスワード」チャレンジを待機して、ピアのチャレンジに応答します。入力された情報は、RADIUS や TACACS+ などの認証、許可、アカウンティング（AAA）プロトコルを使用して認証エンティティに照らしてチェックされます。 [選択（Select）] をクリックすると、使用可能なすべての AAA グループサーバーを表示したダイアログボックスが開き、そこで、AAA グループ サーバー オブジェクトを作成できます。該当する項目をすべて選択し、上矢印ボタンと下矢印ボタンを使用してプライオリティ順に並べ替えます。

Easy VPN に対するダイナミック VTI の設定

[Easy VPN IPSec Proposal] ポリシーの [Use the Dynamic VTI] タブを使用して、ハブアンドスポーク Easy VPN トポロジ内のデバイスにダイナミック仮想トンネル インターフェイスを設定します。詳細については、Easy VPN とダイナミック仮想トンネル インターフェイス （3 ページ）を参照してください。

（注） ダイナミック VTI は、IOS バージョン 12.4(2)T 以降を実行する 7600 デバイスを除く IOS ルータでだけ設定できます。

ナビゲーション パス

- （[Site-to-Site VPN Manager] ウィンドウ）VPN セレクタで Easy VPN トポロジを選択して、ポリシーセレクタで [IPsecプロポーザル（IPsec Proposal）] を選択します。[ダイナミック VTI（Dynamic VTI）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）]>[簡単なIPsecプロポーザル（Easy IPsec Proposal）] を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。[ダイナミックVTI（Dynamic VTI）] タブをクリックします。

関連項目

- Easy VPN について （1 ページ）
- Easy VPN での IPsec プロポーザルの設定 （13 ページ）

フィールド リファレンス

表 4 : [Easy VPN IPSec Proposal]、[Dynamic VTI] タブ

要素	説明
Enable Dynamic VTI	選択されている場合、Security Manager は、デバイスにダイナミック仮想テンプレート インターフェイスを暗黙的に作成できます。 デバイスが、ダイナミック VTI をサポートしないハブ サーバである場合は、警告メッセージが表示されて、ダイナミック VTI なしでクリプト マップが展開されます。クライアント デバイスの場合は、エラー メッセージが表示されます。
Virtual Template IP	トポロジのハブにダイナミック VTI を設定している場合は、サブネット アドレスまたはインターフェイス ロールを指定します。 • [サブネット（Subnet）] : アドレスのプールから取得された IP アドレスを使用します。サブネット マスクを含むプライベート IP アドレスを入力します（たとえば 10.1.1.0/24）。 • [インターフェイスロール（Interface Role）] : デバイスの物理インターフェイスまたはループバックインターフェイスを使用します。必要に応じて、[選択（Select）] をクリックしてインターフェイスセレクタを開きます。そこで、目的のインターフェイスを識別するインターフェイス ロール オブジェクトを選択できます。適切なオブジェクトがまだ存在していない場合は、選択ダイアログボックスで作成できます。 トポロジのスポークにダイナミック VTI を設定している場合は、[なし（None）] を選択します。

Easy VPN における Connection Profile ポリシーの設定

接続プロファイルは、IPsec トンネル接続ポリシーを含むレコードのセットで構成されます。接続プロファイル、またはトンネル グループは、特定の接続のグループ ポリシーを示しており、ユーザ指向の属性を含んでいます。ユーザーに対して特定のグループ ポリシーを割り当てない場合は、接続のデフォルト グループ ポリシーが適用されます。正常に接続するためには、リモート クライアントのユーザ名がデータベースに存在している必要があります。データベースに存在しない場合は、接続が拒否されます。

サイト間 VPN では、Easy VPN サーバ（PIX ファイアウォール バージョン 7.0+ デバイスまたは ASA 5500 シリーズ デバイス）に Connection Profile ポリシーを設定します。Easy VPN Connection Profile ポリシーは、リモート アクセス VPN で使用されるプロファイルに類似しています。どの Easy VPN サーバも ASA デバイスまたは PIX 7.0+ デバイスでない場合、Connection Profile ポリシーを割り当て解除できます。

Connection Profile ポリシーの作成には、次の指定が含まれます。

- グループ ポリシー：デバイス内部または外部の RADIUS サーバや LDAP サーバに保存されるユーザ指向の属性の集合。
- グローバル AAA 設定：認証、許可、アカウンティング サーバ。
- クライアント アドレスの割り当てに使用される DHCP サーバ、および IP アドレスの割り当て元となるアドレス プール。
- Internet Key Exchange（IKE; インターネット キー交換）および IPsec の設定（事前共有キーなど）。

[PIX7.0+/ASA Connection Profiles] ページで、Easy VPN サーバ上の接続プロファイルを設定できます。

関連項目

- VPN トポロジの作成または編集
- IPsec テクノロジーおよびポリシーについて
- Easy VPN について　（1 ページ）

ステップ 1 次のいずれかを実行します。

- （[Site-to-Site VPN Manager] ウィンドウ）VPN セレクタで Easy VPN トポロジを選択し、ポリシー セレクタで [接続プロファイル（PIX7.0/ASA）（Connection Profiles (PIX 7.0/ASA)）] を選択します。
- （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）] > [接続プロファイル（PIX7.0/ASA）（Connection Profiles (PIX 7.0/ASA)）] を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

ポリシーについては、[Connection Profiles] ページを参照してください。

ステップ 2 [全般（General）] タブで、接続プロファイル名およびグループポリシーを指定して、使用するアドレス割り当て方式を選択します。使用可能なプロパティの詳細については、[General] タブ（[Connection Profiles]）を参照してください。

ステップ 3 [AAA] タブをクリックして、接続プロファイルの AAA 認証パラメータを指定します。タブの要素の詳細については、[AAA] タブ（[Connection Profiles]）を参照してください。

ステップ 4 [IPsec] タブをクリックして、接続プロファイルの IPsec および IKE パラメータを指定します。タブの要素の詳細については、[IPSec] タブ（[Connection Profiles]）を参照してください。

Easy VPN における User Group ポリシーの設定

[User Group Policy] ページを使用して、Easy VPN サーバの User Group ポリシーを作成または編集します。Easy VPN サーバを設定するときに、リモート クライアントが属するユーザ グループを作成します。Easy VPN ユーザ グループ ポリシーは、Cisco IOS セキュリティ ルータ、PIX 6.3 Firewall、または Catalyst 6500/7600 デバイスに設定できます。どの Easy VPN サーバも、IOS ルータ、Catalyst 6500/7600 デバイス、または PIX 6.3 ファイアウォールでない場合、ユーザ グループ ポリシーを割り当て解除できます。

リモート クライアントは、サーバ デバイスに接続するためには、サーバに設定されているユーザ グループと同じグループ名を持っている必要があります。同じグループ名を持たない場合、接続は確立されません。リモート クライアントから VPN サーバに接続が正常に確立されたときに、その特定のユーザ グループのグループ ポリシーがユーザ グループに属するすべてのクライアントにプッシュされます。

[Available User Groups] リストで、ポリシーで使用するユーザ グループ ポリシー オブジェクトを選択します。[作成（Create）]（+）ボタンをクリックして、新しいユーザー グループ オブジェクトを作成できます。また、既存のグループを選択し、[編集（Edit）]（鉛筆アイコン）ボタンをクリックして既存のグループを編集できます。ユーザ グループ オブジェクトの設定については、[Add User Group]/[Edit User Group] ダイアログボックスを参照してください。

ナビゲーション パス

- （[Site-to-Site VPN Manager] ウィンドウ）VPN セレクタで Easy VPN トポロジを選択して、ポリシーセレクタで [ユーザーグループポリシー（User Group Policy）] を選択します。
- （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）]>[ユーザーグループポリシー（User Group Policy）] を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

関連項目

- Easy VPN について （1 ページ）

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。