CHAPTER 12

サイト間 VPN

この章の各トピックでは、サイト間 VPN 設定画面および VPN 設計ガイド画面について説明します。

VPN 設計ガイド

VPN ネットワークを設定する管理者は、VPN 設計ガイドを使用して、設定する VPN のタイプを決定することができます。ユーザのタイプ、ルータが VPN 接続を確立する機器の種類、VPN が転送するトラフィックのタイプ、および設定すべきその他の機能について情報を入力します。これらの情報を入力すると、VPN 設計ガイドが推奨 VPN タイプを示し、ウィザードを開始して、このタイプの VPN を設定することができます。

サイト間 VPN の作成

仮想プライベート ネットワーク（VPN）を使用すると、組織によって所有または制御されていない可能性のある回線上で転送されるトラフィックを保護できます。VPN では、このような回線で送信されるトラフィックを暗号化したり、トラフィック送信の前にピアを認証したりできます。

Cisco Configuration Professional（Cisco CP）で VPN アイコンをクリックすると、指示に従って簡単な VPN 設定を行うことができます。［サイト間 VPN の作成］タブのウィザードを使用する場合は、簡単に設定できるように、Cisco CP によって一部の設定パラメータのデフォルト値が用意されます。

VPN 技術の詳細については、「VPN に関する詳細情報」を参照してください。

サイト間 VPN の作成

このオプションでは、2 つのルータを接続する VPN ネットワークを作成できます。

安全な GRE トンネル（GRE over IPSec）を作成する

このオプションでは、ルータとピア システム間にジェネリック ルーティング カプセル化プロトコル（GRE）トンネルを設定できます。

実行する操作

目的	手順
2 つのルータを接続する VPN ネットワークの一部としてルータを設定する。 2 つのルータ間の VPN ネットワークを設定する場合は、リモート ルータの認証方法、トラフィックの暗号化方法、暗号化の対象となるトラフィックを制御できる。	［サイト間 VPN の作成］を選択する。次に、［選択したタスクを実行する］をクリックする。

目的	手順
ルータと別のルータ間に GRE トンネルを設定する。 異なる LAN プロトコルを使用するネットワーク同士を接続する必要がある場合、またはリモート システムへの接続を介してルーティング プロトコルを送信する必要がある場合は、GRE トンネルを設定できる。	[安全な GRE トンネル（GRE over IPSec）を作成する] を選択する。次に、[選択したタスクを実行する] をクリックする。
このウィザードでは説明されていない他の VPN 関連タスクを実行する方法を調べる。	次のリストからトピックを選択する。 • ルータに送信中の IOS コマンドを表示する方法 • 複数のサイトに対して VPN を作成する方法 • VPN の設定後にピア ルータ上で VPN を設定する方法 • 既存の VPN トンネルを編集する方法 • VPN の動作を確認する方法 • VPN に対してバックアップ ピアを設定する方法 • VPN サポート レベルが異なる複数のデバイスを調整する方法 • サポートされていないインターフェイスで VPN を設定する方法 • ファイアウォールの設定後に VPN を設定する方法 • VPN に対して NAT パススルーを設定する方法 • DMVPN を手動で設定する方法

目的	手順
Easy VPN コンセントレータを設定する。 Easy VPN サーバおよびコンセントレータの設定については、www.cisco.com を参照。	次のリンク先には、Cisco VPN 3000 シリーズのコンセントレータを Easy VPN リモート フェーズ II クライアントとともに動作するように設定する場合のガイドライン、およびその他の役立つ情報が提供されています。 http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800a8565.html 次のリンクでは、Cisco VPN 3000 シリーズのドキュメントにアクセスできます。 http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_book09186a00800bbe74.html

サイト間 VPN ウィザード

ほとんどの設定値については、Cisco CP のデフォルト設定を使用できます。または、Cisco CP の指示に従って VPN を設定することもできます。

実行する操作

目的	手順
Cisco CP のデフォルトを使用してサイト間 VPN をすばやく設定する。	［クイック セットアップ］を選択して、［次へ］をクリックする。 認証を管理するデフォルト IKE ポリシー、データの暗号化を制御するデフォルト トランスフォーム セット、ルータとリモート デバイス間のすべてのトラフィックを暗号化するデフォルト IPSec ルールが Cisco CP によって自動的に提供される。 クイック セットアップは、ローカル ルータとリモート システムの両方が Cisco CP を使用する Cisco ルータである場合に最適。 IOS イメージで 3DES 暗号化がサポートされている場合は、3DES がクイック セットアップで設定される。それ以外の場合は、DES 暗号化が設定される。AES または SEAL 暗号化の設定が必要な場合は、［ステップ バイ ステップ ウィザード］をクリックする。
ワンステップの VPN 設定で使用されるデフォルトの IKE ポリシー、トランスフォーム セット、および IPSec ルールを表示する。	［デフォルトの表示］をクリックする。
指定したパラメータを使用してサイト間 VPN を設定する。	［ステップ バイ ステップ ウィザード］を選択し、［次へ］をクリックする。 VPN のカスタム設定を作成し、必要な Cisco CP デフォルトを使用することができる。 ステップ バイ ステップ ウィザードでは、クイック セットアップ ウィザードで設定されるよりも強力な暗号化を指定できる。

デフォルトの表示

このウィンドウでは、Cisco CP がクイック セットアップのサイト間 VPN の設定に使用するデフォルトのインターネット キー交換（IKE）ポリシー、トランスフォーム セット、および IPSec ルールが表示されます。このウィンドウの表示内容と異なる設定が必要な場合は、設定値を定義できる［ステップ バイ ステップ ウィザード］を選択します。

VPN 接続情報

このウィンドウを使用して、設定している VPN トンネルを終端するリモート サイトの IP アドレスまたはホスト名の識別、使用するルータ インターフェイスの指定、および両方のルータがお互いの認証に使用する事前共有キーの入力を実行することができます。

この VPN 接続に対するインターフェイスの選択

このルータで、リモート サイトに接続するインターフェイスを選択します。設定中のルータは、ユース ケース シナリオ図でローカル ルータとして表示されています。

ピア ID

設定中の VPN トンネルを終端するリモート IP セキュリティ（IPSec）ピアの IP アドレスを入力します。リモート IPSec ピアは、別のルータ、VPN コンセントレータ、IPSec をサポートしているその他のゲートウェイ デバイスなどです。

ダイナミック IP アドレスを持つピア

ルータの接続先のピアが、ダイナミックに割り当てられた IP アドレスを使用している場合は、このオプションを選択します。

スタティック IP アドレスを持つピア

ルータの接続先のピアが、固定した IP アドレスを使用している場合はこのオプションを選択します。

リモート ピアの IP アドレスを入力

［スタティック IP アドレスを持つピア］を選択した場合に有効です。リモート ピアの IP アドレスを入力します。

認証

VPN ピアが事前共有キーを使用して相手からの接続を認証する場合は、このボタンをクリックします。このキーは、VPN 接続の両側で同じでなければなりません。

事前共有キーを入力し、確認のためにキーを再入力します。暗号化された電子メール メッセージなどの安全で便利な手段を使用して、リモート サイトの管理者と事前共有キーを交換します。事前共有キーでは、疑問符（?）およびスペースを使用できません。事前共有キーの最大長は 128 文字です。

（注）

- 事前共有キーとして入力した文字は、フィールドには表示されません。キーを入力する前に、リモート システムの管理者に伝えることができるようにメモしておくと便利です。
- 事前共有キーは、安全なトンネルを確立する必要がある IPSec ピアの各ペア間で交換する必要があります。この認証方法は、限られた数の IPSec ピアとの安定したネットワークに適しています。IPSec ピアが多いネットワーク、またはピアの数が増えたネットワークでは、スケーラビリティの問題が生じることがあります。

デジタル証明書

VPN ピアが認証にデジタル証明書を使用する場合は、このボタンをクリックします。

（注） ルータは、自身を認証するために、認証機関（CA）によって発行されたデジタル証明書を保持していなければなりません。ルータに対してデジタル証明書を設定していない場合は、VPN コンポーネントに移動してデジタル証明書ウィザードを使用し、デジタル証明書を登録します。

暗号化するトラフィック

クイック セットアップでサイト間 VPN 接続を設定している場合は、このウィンドウで送信元と宛先のサブネットを指定する必要があります。

送信元

この VPN 接続のトラフィックの送信元になるルータ上のインターフェイスを選択します。このインターフェイスを通過するトラフィックのうち、宛先 IP アドレスが［宛先］エリアで指定したサブネットにあるものは、すべて暗号化されます。

詳細

このボタンをクリックすると、選択したインターフェイスの詳細を取得できます。詳細ウィンドウには、インターフェイスに関連付けられているすべてのアクセス ルール、IPSec ポリシー、ネットワーク アドレス変換（NAT）ルール、またはインスペクション ルールが表示されます。これらのルールの詳細については、［追加タスク］、［ACL エディタ］の順にクリックして、ルールのウィンドウを参照してください。

宛先

［IP アドレス］と［サブネット マスク］。このトラフィックの宛先の IP アドレスとサブネット マスクを入力します。これらのフィールドに値を入力する方法の詳細については、「IP アドレスとサブネット マスク」を参照してください。

宛先は、メインの VPN ウィザード ウィンドウのユース ケース シナリオ図にリモート ルータとして表示されます。

IKE プロポーザル

このウィンドウには、ルータに設定されているすべてのインターネット キー交換（IKE）ポリシーのリストが表示されます。ユーザ定義のポリシーが設定されていない場合、ウィンドウには Cisco CP のデフォルト IKE ポリシーが表示されます。IKE ポリシーは、VPN 上のデバイスが自身を認証する方法を管理します。

ローカル ルータは、このウィンドウに表示される IKE ポリシーを使用して、リモート ルータとの認証をネゴシエートします。

ローカル ルータとピア デバイスは、どちらも同じポリシーを使用していなければなりません。VPN 接続を開始するルータは、優先順位が最下位のポリシーを最初に提示します。リモート システムがそのポリシーを拒否した場合、ローカル ルータは、次に優先順位が低いポリシーを提示し、リモート システムの許可が得られるまで提示を続けます。両方のルータに同じポリシーを設定できるように、ピア システムの管理者と事前に綿密な調整をしておく必要があります。

Easy VPN 接続の場合、IKE ポリシーは Easy VPN サーバでのみ設定されます。Easy VPN クライアントがプロポーザルを送信し、設定済みの IKE ポリシーに従ってサーバが応答します。

優先順位

ネゴシエーション中にポリシーが提示される順序です。

暗号化

Cisco CP は、さまざまなタイプの暗号化をサポートしています。これらは安全性が高い順にリスト表示されています。暗号化タイプが安全であるほど、処理時間が長くなります。

（注）

- すべてのルータがすべての暗号化タイプをサポートしているわけではありません。サポートされていないタイプは、画面に表示されません。
- Cisco CP がサポートしている暗号化タイプには、IOS イメージでサポートしていないものもあります。IOS イメージでサポートされていないタイプは、画面に表示されません。
- ハードウェア暗号化が有効になっている場合は、ハードウェア暗号化でサポートされている暗号化タイプだけが画面に表示されます。

Cisco CP では、次のタイプの暗号化がサポートされています。

- DES — データ暗号化標準。この暗号化形式は、56 ビットの暗号化をサポートします。
- 3DES — トリプル DES。これは、DES よりも強力な暗号化形式で、168 ビットの暗号化をサポートします。
- AES-128 — 128 ビットのキーを使用する Advanced Encryption Standard（AES）暗号化。AES は、DES よりも強力なセキュリティを提供し、3DES よりも計算効率が高くなります。
- AES-192 — 192 ビットのキーを使用する AES 暗号化。
- AES-256 — 256 ビットのキーを使用する AES 暗号化。

ハッシュ

ネゴシエーションに使用される認証アルゴリズムです。Cisco CP では、次のアルゴリズムがサポートされています。

- SHA_1 — Secure Hash Algorithm。パケット データの認証に使用されるハッシュ アルゴリズム。
- MD5 — Message Digest 5。パケット データの認証に使用されるハッシュ アルゴリズム。

D-H グループ

Diffie-Hellman グループ — Diffie-Hellman は、2 つのルータ間で、安全でない通信チャネルを使用して秘密情報を共有できるようにするパブリック キー暗号プロトコルです。Cisco CP では、次のグループがサポートされています。

- グループ 1 — D-H グループ 1。768 ビットの D-H グループ。
- グループ 2 — D-H グループ 2。1,024 ビットの D-H グループ。このグループは、グループ 1 よりも強力なセキュリティを提供しますが、処理時間が長くなります。
- グループ 5 — D-H グループ 5。1,536 ビットの D-H グループ。このグループは、グループ 2 よりも強力なセキュリティを提供しますが、処理時間が長くなります。

認証

使用される認証方式です。次の値がサポートされています。

- PRE_SHARE — 認証は事前共有キーを使用して実行されます。
- RSA_SIG — 認証はデジタル証明書を使用して実行されます。

（注） VPN 接続に使用するインターフェイスを指定したときに指定した認証タイプを選択する必要があります。

タイプ

［Cisco CP デフォルト］または［ユーザ定義］のいずれかになります。ルータでユーザ定義のポリシーが作成されていない場合、このウィンドウにはデフォルト IKE ポリシーが表示されます。

IKE ポリシーを追加または編集するには

このリストに含まれていない IKE ポリシーを追加する場合は、［追加］をクリックし、表示されるウィンドウでポリシーを作成します。既存のポリシーを編集する場合は、ポリシーを選択し、［編集］をクリックします。Cisco CP デフォルト ポリシーは読み取り専用で編集できません。

ポリシー リストをそのまま使用するには

IKE ポリシー リストをそのまま使用して作業を続けるには、［次へ］をクリックします。

トランスフォーム セット

このウィンドウには、このルータに設定されている Cisco CP のデフォルト トランスフォーム セットとその他のトランスフォーム セットのリストが表示されます。これらのトランスフォーム セットは、VPN または DMVPN で使用できるようになります。トランスフォーム セットは、セキュリティ プロトコルとアルゴリズムの特定の組み合わせです。IPSec セキュリティ アソシエーションのネゴシ

エート時に、ピアは特定のデータ フローを保護するために使用するトランスフォーム セットについて合意します。トランスフォームには、特定のセキュリティ プロトコルが、対応するアルゴリズムとともに記述されています。

このウィンドウで選択できるトランスフォーム セットは 1 つだけですが、［VPN の編集］タブまたは［DMVPN の編集］タブを使用して、VPN または DMVPN 接続に追加のトランスフォーム セットを割り当てることができます。

トランスフォーム セットの選択

このリストから使用するトランスフォーム セットを選択します。

選択したトランスフォーム セットの詳細

このエリアには、選択したトランスフォーム セットに関する次の詳細情報が表示されます。すべての暗号化、認証、および圧縮のタイプを設定する必要はないので、場合によっては値が含まれていないカラムがあります。

各カラムに含めることができる値については、「トランスフォーム セットの追加 / 編集」を参照してください。

名前

このトランスフォーム セットに付けられている名前です。

ESP 暗号化

使用されている ESP（Encapsulating Security Protocol）暗号化のタイプです。トランスフォーム セットに対して ESP 暗号化が設定されていない場合、このカラムは空です。

ESP 認証

使用される ESP 認証のタイプです。トランスフォーム セットに対して ESP 認証が設定されていない場合、このカラムは空です。

AH 認証

使用される認証ヘッダー（AH）認証のタイプです。トランスフォーム セットに対して AH 認証が設定されていない場合、このカラムは空です。

IP 圧縮

トランスフォーム セットに対して IP 圧縮が設定されていない場合、このフィールドには値 COMP-LZS が含まれます。

（注） IP 圧縮をサポートしていないルータもあります。

モード

このカラムには、次のいずれかが含まれます。

- ［トランスポート］— データのみ暗号化します。トランスポート モードは、両方のエンドポイントが IPsec をサポートしている場合に使用されます。トランスポート モードは、オリジナルの IP ヘッダーの後に認証ヘッダーまたは ESP（encapsulated security payload）を配置します。したがって、IP ペイロードだけが暗号化されます。この方法を使用すると、ユーザは Quality Of-Service（QoS）コントロールなどのネットワーク サービスを暗号化したパケットに適用できます。
- ［トンネル］— データと IP ヘッダーを暗号化します。トンネル モードでは、トランスポート モードより強力に防御できます。IP パケット全体を AH または ESP 内にカプセル化して新しい IP ヘッダーを加えることによって、データグラム全体をカプセル化できるからです。トンネル モードでは、ルータなどのネットワーク デバイスを複数の VPN ユーザの IPsec プロキシとして機能させることができます。

タイプ

［ユーザ定義］または［Cisco CP デフォルト］のいずれかになります。

実行する操作

目的	手順
使用する VPN のトランスフォーム セットを選択する。	トランスフォーム セットを選択し、［次へ］をクリックする。
ルータの設定にトランスフォーム セットを追加する。	［追加］をクリックし、［トランスフォーム セットの追加］ウィンドウでトランスフォーム セットを作成する。次に［次へ］をクリックして、VPN 設定を続ける。
既存のトランスフォーム セットを編集する。	トランスフォーム セットを選択し、［編集］をクリックする。次に、［トランスフォーム セットの編集］ウィンドウでトランスフォーム セットを編集する。トランスフォーム セットを編集したら、［次へ］をクリックして、VPN 設定を続ける。ただし、Cisco CP デフォルト トランスフォーム セットは読み取り専用で編集できない。
追加のトランスフォーム セットをこの VPN に関連付ける。	このウィンドウでトランスフォーム セットを 1 つ選択し、VPN ウィザードを終了する。次に、［編集］タブで他のトランスフォーム セットを VPN に関連付ける。

保護するトラフィック

このウィンドウでは、この VPN が保護するトラフィックを定義します。VPN は、指定したサブネット間のトラフィック、または選択した IPSec ルールで指定されたトラフィックを保護できます。

以下のサブネット間のすべてのトラフィックを保護する

このオプションを使用して、アウトバウンド トラフィックを暗号化する送信元サブネット（LAN 上のサブネット）を 1 つと、［VPN 接続］ウィンドウで指定したピアでサポートされている宛先サブネットを 1 つ指定します。

他の送信元と宛先ペア間のすべてのトラフィックは暗号化されずに送信されます。

送信元

アウトバウンド トラフィックを保護するサブネットのアドレスを入力し、サブネット マスクを指定します。詳細については、「使用可能なインターフェイス設定」を参照してください。

この送信元サブネットから発信されるトラフィックで、宛先サブネットの宛先 IP アドレスを持つトラフィックはすべて保護されます。

宛先

宛先サブネットのアドレスを入力し、そのサブネットのマスクを指定します。リストからサブネット マスクを選択するか、カスタム マスクを入力できます。前の例のように、サブネット番号およびマスクは、ドット（.）で区切った 10 進表記で指定する必要があります。

このサブネット上のホストに送られるすべてのトラフィックは保護されます。

IPSec トラフィックのアクセス リストを作成 / 選択する

複数の送信元および宛先を指定する必要がある場合や、特定のタイプのトラフィックを暗号化する場合は、このオプションを使用します。IPSec ルールは、複数のエントリで設定され、各エントリにはそれぞれ異なるトラフィック タイプや送信元および宛先を指定できます。

フィールドの横のボタンをクリックし、暗号化するトラフィックを定義している既存の IPSec ルールを指定するか、この VPN で使用する IPSec ルールを作成します。IPSec ルールの番号がわかっている場合は、右のボックスに入力します。ルールの番号がわからない場合は、[...] ボタンをクリックして、ルールを参照します。ルールを選択すると、番号がボックスに表示されます。

（注） トラフィック タイプ、および送信元と宛先の両方を指定できるので、IPSec ルールは拡張ルールです。標準ルールの番号または名前を入力した場合、名前または番号が標準ルールであることを通知する警告メッセージが表示されます。

IPSec ルールの条件と一致しないパケットはすべて暗号化されずに送信されます。

設定の要約

このウィンドウには、作成した VPN または DMVPN 設定が表示されます。このウィンドウで設定を確認し、必要な場合は、［戻る］ボタンをクリックして変更できます。

スポーク設定

DMVPN ハブを設定している場合は、自分や他の管理者が DMVPN スポークを設定するときに役立つ手順を Cisco CP で生成できます。この手順は、ウィザードで選択するオプションとスポーク設定ウィンドウで入力する情報について説明するものです。この情報を自分や他の管理者が使用できるテキスト ファイルに保存できます。

設定後の接続テスト

設定が終わった VPN 接続をクリックしてテストします。テストの結果は、別のウィンドウに表示されます。

この設定をルータの実行コンフィギュレーションに保存してウィザードを終了するには

［完了］をクリックします。設定の変更がルータの実行コンフィギュレーションに保存されます。変更はすぐに有効になりますが、ルータの電源を切ると失われます。

Cisco CP の［設定］ウィンドウで［コマンドをルータに配信する前にプレビューする］チェック ボックスを選択した場合は、［配信］ウィンドウが表示されます。このウィンドウで、ルータに配信する CLI コマンドを確認できます。

スポーク設定

このウィンドウに表示されている情報を使用して、設定済みの DMVPN ハブと互換性のある設定をスポーク ルータに設定できます。このウィンドウには、作業が必要なウィンドウのリストが表示され、そのウィンドウ内で入力しなければならないデータが示されます。スポークは、これらのデータを使用してハブと通信します。

スポーク設定に入力しなければならないデータとして、次のデータが表示されます。

- ハブのパブリック IP アドレス。これは、mGRE トンネルをサポートするハブ インターフェイスの IP アドレスです。
- ハブの mGRE トンネルの IP アドレス。
- DMVPN のすべてのトンネル インターフェイスで使用しなければならないサブネット マスク。
- 詳細トンネル設定情報。
- 使用するルーティング プロトコルと、自律システム番号（EIGRP の場合）や OSPF プロセス ID など、そのプロトコルに関連付けられているすべての情報。
- ハブが使用する IKE ポリシーのハッシュ、暗号化、DH グループ、および認証タイプ。これらにより、互換性のある IKE ポリシーをスポークに設定できます。
- ハブが使用するトランスフォーム セットの ESP およびモードについての情報。スポークに同じトランスフォーム セットが設定されていない場合は、この情報を使用して設定できます。

GRE トンネル（GRE over IPSec）の保護

ジェネリック ルーティング カプセル化（GRE）は、Cisco が開発したトンネリング プロトコルです。IP トンネル内のさまざまなタイプのプロトコル パケットをカプセル化し、IP インターネットワーク上にリモートの Cisco ルータへの仮想ポイントツーポイント リンクを確立できます。シングルプロトコルのバックボーン環境にマルチプロトコル サブネットワークを接続して、GRE を使用した IP トンネリングを利用すれば、シングルプロトコルのバックボーン環境にまたがるネットワーク拡張が可能になります。

このウィザードでは、IPSec 暗号化を使用する GRE トンネルを作成できます。GRE トンネル設定を作成するときは、トンネルのエンドポイントを記述する IPSec ルールも作成します。

GRE トンネル情報

この画面には全般的な GRE トンネル情報が表示されます。

トンネルの送信元

トンネルが使用するインターフェイスのインターフェイス名または IP アドレスを選択します。インターフェイスの IP アドレスは、トンネルのもう一方の端からこのインターフェイスに到達できる必要があります。したがって、このインターフェイスには、ルート指定可能なパブリック IP アドレスが必要です。設定済みのインターフェイスに関連付けられていない IP アドレスを入力すると、エラーが表示されます。

（注） ［インターフェイス］リストには、スタティック IP アドレスを持つインターフェイスとアンナンバードとして設定されているインターフェイスがリスト表示されます。ループバック インターフェイスは、このリストには含まれません。

詳細

クリックすると、選択したインターフェイスの詳細を取得できます。詳細ウィンドウには、インターフェイスに関連付けられているすべてのアクセス ルール、IPSec ポリシー、NAT ルール、またはインスペクション ルールが表示されます。NAT ルールがこのインターフェイスに適用されている場合はアドレスが到達不可能になるので、トンネルは適切に動作しません。これらのルールの詳細については、［追加タスク］、［ACL エディタ］の順にクリックして、［ルール］ウィンドウを検査してください。

トンネルの宛先

トンネルのもう一方の端にあるリモート ルータ上のインターフェイスの IP アドレスを入力します。これは、トンネルのもう一方の端から見た場合、送信元インターフェイスになります。

ping コマンドを使用して、このアドレスに到達できることを確認します。**ping** コマンドは、［ツール］メニューから利用できます。宛先アドレスに到達できない場合は、トンネルが適切に作成されていません。

GRE トンネルの IP アドレス

トンネルの IP アドレスを入力します。トンネルの両端の IP アドレスは、同じサブネット上にある必要があります。トンネルには、必要な場合はプライベート アドレスにできるように個別の IP アドレスが与えられます。

IP アドレス

トンネルの IP アドレスをドット（.）で区切った 10 進表記で入力します。詳細については、「IP アドレスとサブネット マスク」を参照してください。

サブネット マスク

トンネルのサブネット マスクをドット（.）で区切った 10 進表記で入力します。

VPN 認証情報

VPN ピアは、相手からの接続を認証するために事前共有キーを使用します。このキーは、VPN 接続の両側で同じでなければなりません。

事前共有キー

VPN ピアが認証に事前共有キーを使用する場合は、このボタンをクリックして事前共有キーを入力し、その後、確認のためキーを再入力します。暗号化された電子メール メッセージなどの安全で便利な手段を使用して、リモート サイトの管理者と事前共有キーを交換します。事前共有キーでは、疑問符（?）およびスペースを使用できません。

（注）
- 事前共有キー用に入力した文字は、フィールドには表示されません。キーを入力する前に、リモート システムの管理者に伝えることができるようにメモしておくと便利です。
- 事前共有キーは、安全なトンネルを確立する必要がある IPSec ピアの各ペア間で交換する必要があります。この認証方法は、限られた数の IPSec ピアとの安定したネットワークに適しています。IPSec ピアが多いネットワーク、またはピアの数が増えたネットワークでは、スケーラビリティの問題が生じることがあります。

デジタル証明書

VPN ピアが認証にデジタル証明書を使用する場合は、このボタンをクリックします。

ルータは、自身を認証するために、認証機関（CA）によって発行されたデジタル証明書を保持していなければなりません。ルータに対してデジタル証明書を設定していない場合は、VPN コンポーネントに移動してデジタル証明書ウィザードを使用し、デジタル証明書を登録します。

（注）デジタル証明書を使用して認証する場合は、IKE ネゴシエーション中にアクセスされる CA サーバに、証明書失効リスト（CRL）要求に応答するための設定がないと、VPN トンネルが作成されない可能性があります。この問題を修正するには、［デジタル証明書］ページに移動して設定されているトラストポイントを選択し、［取り消しの確認］で［なし］を選択します。

バックアップ GRE トンネル情報

プライマリ トンネルで問題が発生した場合に、ルータが使用できるバックアップ GRE-over-IPSec トンネルを設定できます。このトンネルでは、プライマリ トンネル用に設定したものと同じインターフェイスを使用しますが、バックアップ VPN ルータをピアとして使用して設定する必要があります。プライマリ GRE-over-IPSec トンネルのルーティングが設定されている場合は、ルーティング

プロトコルが送信するキープアライブ パケットを使用して、トンネルがまだアクティブかどうかを確認します。ルータがプライマリ トンネルでのキープアライブ パケットの受信を停止した場合、トラフィックはバックアップ トンネルを経由して送信されます。

バックアップ用の安全な GRE トンネルを作成する

バックアップ トンネルを作成する場合はこのボックスを選択します。

バックアップ GRE トンネルの宛先 IP アドレス

トンネルのもう一方の端にあるリモート ルータ上のインターフェイスの IP アドレスを入力します。これは、トンネルのもう一方の端から見た場合の送信元インターフェイスです。

ping コマンドを使用して、このアドレスに到達できることを確認します。**ping** コマンドは、［ツール］メニューから利用できます。［Ping］ダイアログ ボックスで指定して確認した宛先アドレスが到達できないアドレスだった場合は、トンネルが適切に作成されません。

トンネル IP アドレス

トンネルの IP アドレスを入力します。トンネルの両端の IP アドレスは、同じサブネット上にある必要があります。トンネルには、必要な場合はプライベート アドレスにできるように個別の IP アドレスが与えられます。

IP アドレス

トンネルの IP アドレスをドット（.）で区切った 10 進表記で入力します。詳細については、「IP アドレスとサブネット マスク」を参照してください。

サブネット マスク

トンネルのサブネット マスクをドット（.）で区切った 10 進表記で入力します。

ルーティング情報

このウィンドウでは、トンネル トラフィックのルーティングを設定できます。このウィンドウで追加する情報は、［ルーティング］ウィンドウに表示されます。［ルーティング］ウィンドウで行った変更は、VPN トラフィックのルーティングに適用される可能性があります。ルーティングを設定すると、GRE-over-IPSec VPN　に関与するネットワークを指定できます。さらに、バックアップの GRE-over-IPSec トンネルを設定する場合、ルータは、ルーティング プロトコルによって送信されるキープアライブ パケットを使用して、プライマリ トンネルで障害が発生しているかどうかを判断できます。

このルータが GRE over IPSec VPN に多数のネットワークを含む大規模な VPN 展開で使用されている場合は、ダイナミック ルーティング プロトコルを選択します。VPN に関与するネットワークの数が少ない場合は、スタティック ルーティングを選択します。

EIGRP

Enhanced Interior Gateway Routing Protocol（EIGRP）を使用してトラフィックのルーティングを行う場合は、このボックスを選択します。次に、［次へ］をクリックし、［ルーティング情報］ウィンドウで GRE-over-IPSec VPN に関与するネットワークを指定します。

OSPF

Open Shortest Path First プロトコル（OSPF）を使用してトラフィックのルーティングを行う場合は、このボックスを選択します。次に、［次へ］をクリックし、［ルーティング情報］ウィンドウで GRE-over-IPSec VPN に関与するネットワークを指定します。

RIP

ルーティング情報プロトコル（RIP）を使用してトラフィックのルーティングを行う場合は、このボックスを選択します。次に、［次へ］をクリックし、［ルーティング情報］ウィンドウで GRE-over-IPSec VPN に関与するネットワークを指定します。

（注）　このオプションは、バックアップ GRE-over-IPSec トンネルを設定している場合は利用できません。

スタティック ルーティング

スタティック ルーティングは、少数のプライベート ネットワークのみが GRE-over-IPSec VPN に関与する、小規模な VPN 導入で使用できます。リモート ネットワーク宛てのトラフィックが適切なトンネルを通過するように、各リモート ネットワークにスタティック ルートを設定することができます。

スタティック ルーティング情報

リモート ネットワーク宛てのトラフィックが適切なトンネルを通過するように、各リモート ネットワークにスタティック ルートを設定することができます。［スタティック ルーティング情報］ウィンドウで 1 つめのスタティック ルートを設定します。さらにスタティック ルートを設定する必要がある場合は、［ルーティング］ウィンドウで設定できます。

トンネルのスタティック ルートを指定する場合は、このボックスを選択し、次のいずれかを選択します。

- ［すべてのトラフィックをトンネルする］— すべてのトラフィックはトンネル インターフェイスを経由してルーティングされ、暗号化されます。Cisco CP は、ネクスト ホップとしてトンネル インターフェイスを持つデフォルトのスタティック ルート エントリを作成します。

  すでにデフォルト ルートが存在する場合、Cisco CP は、元々あったインターフェイスの代わりにトンネル インターフェイスをネクスト ホップとして使用するようにそのルートを変更します。次に、トンネルの終端ネットワークへの新しいスタティック エントリを作成して、元のデフォルト ルートのインターフェイスをネクスト ホップとして指定します。

次の例では、トンネルのもう一方の端にあるネットワークが、宛先ネットワーク フィールドで指定された 200.1.0.0 であるとしています。

```
! 元のエントリ
ip route 0.0.0.0  0.0.0.0 FE0
! SDM によって変更されたエントリ
ip route 0.0.0.0  0.0.0.0 Tunnel0
! SDM によって追加されたエントリ
ip route 200.1.0.0  255.255.0.0 FE0
```

デフォルト ルートがない場合、Cisco CP は、単にネクスト ホップとしてトンネル インターフェイスを使用するルートを作成します。次に例を示します。

```
ip route 0.0.0.0  0.0.0.0 Tunnel0
```

- ［スプリット トンネリングを実施］— スプリット トンネリングを行うと、［IP アドレス］フィールドと［ネットワーク マスク］フィールドで指定されたネットワーク宛てのトラフィックが暗号化され、トンネル インターフェイスを経由してルーティングされます。その他のすべてのトラフィックは暗号化されません。このオプションを選択すると、Cisco CP は、IP アドレスとネットワーク マスクを使用してネットワークへのスタティック ルートを作成します。

  次の例は、ネットワーク アドレス 10.2.0.0/255.255.0.0 が宛先アドレスのフィールドに入力されたと想定しています。

  ```
  ip route 10.2.0.0 255.255.0.0 Tunnel0
  ```

  スプリット トンネリングを選択すると、［IP アドレス］フィールドと［サブネット マスク］フィールドが表示されます。ここに宛先ピアの IP アドレスとサブネット マスクを入力する必要があります。［GRE トンネル情報］ウィンドウの［トンネルの宛先］フィールドに入力した宛先 IP アドレスに到達できることを確認する必要があります。到達できない場合、トンネルは確立されません。

IP アドレス

スプリット トンネリングを行う場合に有効になります。トンネルのもう一方の端にあるネットワークの IP アドレスを入力します。Cisco CP は、このネットワークの宛先アドレスを持つパケットのスタティック ルート エントリを作成します。このフィールドは、［すべてのトラフィックをトンネルする］が選択されている場合は無効です。

このオプションを設定する前に、このフィールドに入力した IP アドレスに到達できることを確認する必要があります。到達できない場合、トンネルは確立されません。

ネットワーク マスク

スプリット トンネリングを行う場合に有効になります。トンネルのもう一方の端にあるネットワークで使用されるネットワーク マスクを入力します。このフィールドは、［すべてのトラフィックをトンネルする］が選択されている場合は無効です。

ルーティング プロトコルの選択

このウィンドウを使用して、このルータの背後にある他のネットワークを、他のルータに通知する間隔を指定します。次のいずれかを選択します。

- ［EIGRP］— Extended Interior Gateway Routing Protocol。
- ［OSPF］— Open Shortest Path First。
- ［RIP］— Routing Information Protocol。
- スタティック ルーティング。このオプションは、GRE over IPSec トンネルを設定している場合に使用できます。

（注） RIP は、DMVPN のハブ アンド スポーク トポロジではサポートされていませんが、DMVPN のフル メッシュ トポロジでは利用できます。

設定の要約

この画面には、完了した GRE 設定の概要が表示されます。この画面で情報を確認します。［戻る］ボタンをクリックして、変更する画面に戻ることもできます。設定を保存する場合は、［完了］をクリックします。

GRE トンネル設定は、GRE トラフィックがどのホスト間のフローを許可されるかを指定する IPSec ルールを作成します。この IPSec ルールが要約に表示されます。

この設定をルータの実行コンフィギュレーションに保存してウィザードを終了するには

［完了］をクリックします。設定の変更がルータの実行コンフィギュレーションに保存されます。変更はすぐに有効になりますが、ルータの電源を切ると失われます。

Cisco CP の［設定］ウィンドウで［コマンドをルータに配信する前にプレビューする］チェック ボックスを選択した場合は、［配信］ウィンドウが表示されます。このウィンドウで、ルータに配信する CLI コマンドを確認できます。

サイト間 VPN の編集

仮想プライベート ネットワーク（VPN）では、トラフィックを暗号化して同じパブリック ネットワークを使用する他のユーザが読み取れないようにすることによって、ルータとリモート システム間のデータを保護できます。これによって、他の組織も使用する可能性がある公衆回線上のプライベート ネットワークを実質的に保護します。

このウィンドウを使用して、リモート システムへの VPN 接続を作成および管理します。ここでは、VPN 接続の作成、編集、削除、および既存の接続のリセットができます。また、このウィンドウを使用して、ルータを 1 つ以上の Easy VPN サーバまたはコンセントレータに接続する Easy VPN クライアントとして設定できます。

ウィンドウ内で、ヘルプを表示したい部分のリンクをクリックします。

サイト間 VPN 接続

*トンネル*と呼ばれることもある VPN 接続は、［VPN 接続］ボックスで作成および管理します。VPN 接続は、IP セキュリティ（IPSec）ポリシーで定義された暗号マップによって指定されている 1 つ以上のピアにルータ インターフェイスをリンクします。このリストで VPN 接続の表示、追加、編集、および削除を行えます。

ステータス カラム

接続のステータスが次のアイコンで示されます。

 　接続されています。

 　接続は切断されています。

 　接続を確立中です。

インターフェイス

この VPN 接続でリモート ピアに接続されているルータ インターフェイスです。1 つのインターフェイスに関連付けられる IPSec ポリシーは 1 つだけです。この接続で使用されている IPSec ポリシーに複数の暗号マップが定義されている場合は、同じインターフェイスが複数の回線に表示されます。

説明

この接続についての簡単な説明です。

IPSec ポリシー

この VPN 接続で使用されている IPSec ポリシーの名前です。IPSec ポリシーでは、データの暗号方法、暗号化対象のデータ、およびデータの送信先を指定します。詳細については、「VPN 接続と IPSec ポリシーに関する詳細情報」を参照してください。

シーケンス番号

この接続のシーケンス番号です。IPSec ポリシーは複数の接続で使用されることがあるので、シーケンス番号と IPSec ポリシー名の組み合わせで、この VPN 接続を一意に識別します。シーケンス番号は、VPN 接続に優先順位を付けるものではありません。ルータは、シーケンス番号にかかわらず、設定済みのすべての VPN 接続を確立しようとします。

ピア

VPN 接続のもう一方の端にあるデバイスの IP アドレスまたはホスト名です。接続に複数のピアが含まれている場合は、それらの IP アドレスまたはホスト名がカンマで区切られます。複数のピアは、VPN 接続の代替ルーティング パスを提供する目的で設定されている可能性があります。

トランスフォーム セット

これは、この VPN 接続で使用されているトランスフォーム セットの名前です。複数のトランスフォーム セット名はカンマで区切られます。トランスフォーム セットでは、データの暗号化、データの整合性の保証、データ圧縮の提供に使用

するアルゴリズムを指定します。両方のピアが、同じトランスフォーム セットを使用する必要があります。ピアはネゴシエートして使用するセットを決定します。ネゴシエートしているピアが使用に同意したトランスフォーム セットをルータで提供できるようにするために、複数のトランスフォーム セットを定義することもあります。トランスフォーム セットは、IPSec ポリシーのコンポーネントです。

IPSec ルール

この接続で暗号化するトラフィックを決定するルールです。IPSec ルールは、IPSec ポリシーのコンポーネントです。

タイプ

次のタイプがあります。

- ［スタティック］— スタティックなサイト間 VPN トンネルです。VPN トンネルはスタティック暗号マップを使用します。
- ［ダイナミック］— ダイナミックなサイト間 VPN トンネルです。VPN トンネルはダイナミック暗号マップを使用します。

追加ボタン

VPN 接続を追加する場合にクリックします。

削除ボタン

選択した VPN 接続を削除する場合にクリックします。

トンネルのテスト ... ボタン

選択した VPN トンネルをテストする場合にクリックします。テストの結果は、別のウィンドウに表示されます。

接続のクリア ボタン

リモート ピアとの間に確立している接続をリセットする場合にクリックします。ダイナミック サイト間 VPN トンネルを選択している場合は、このボタンは無効です。

ミラーの生成 ... ボタン

ローカル ルータの VPN 設定を取得するテキスト ファイルを作成する場合にクリックします。リモート ルータは、このファイルを基に VPN を設定し、ローカル ルータへの VPN 接続を確立できます。ダイナミック サイト間 VPN トンネルを選択している場合は、このボタンは無効です。

（注） ISAKMP 暗号マップを使用しない VPN 接続が以前設定されていたことを Cisco CP が検出した場合、その接続は、VPN 接続テーブルに編集不可の読み取り専用エントリとして表示されます。

新しい接続の追加

このウィンドウを使用して、ローカル ルータと *ピア*と呼ばれるリモート システムの間に、新しい VPN 接続を追加します。VPN 接続を作成するには、IPSec ポリシーにインターフェイスを関連付けます。

VPN 接続を作成するには

ステップ 1　VPN に使用するインターフェイスを［インターフェイスの選択］リストから選択します。このリストには、他の VPN 接続で使用されていないインターフェイスだけが表示されます。

ステップ 2　［IPSec ポリシーの選択］リストからポリシーを選択します。［OK］をクリックして、［VPN 接続］ウィンドウに戻ります。

暗号マップの追加

このウィンドウを使用して、新しい暗号マップを既存の IPSec ポリシーに追加します。このウィンドウには、［VPN 接続］ウィンドウで選択した VPN 接続に関連付けられているインターフェイス、そのインターフェイスに関連付けられている IPSec ポリシー、およびそのポリシーにすでに含まれている暗号マップが表示されます。

暗号マップでは、シーケンス番号、接続のもう一方の端にあるピア デバイス、トラフィックを暗号化するトランスフォームのセット、および暗号化対象のトラフィックを決定する IPSec ルールを指定します。

（注） 既存の VPN 接続で使用されているインターフェイスに VPN トンネルを追加する方法は、既存の IPSec ポリシーに暗号マップを追加する方法だけです。

インターフェイス

この VPN 接続で使用されているインターフェイスの名前です。

IPSec ポリシー

VPN 接続を制御する IPSec ポリシーの名前です。このフィールドの下のリストには、IPSec ポリシーを設定する暗号マップが表示されます。詳細については、「VPN 接続と IPSec ポリシーに関する詳細情報」を参照してください。

実行する操作

目的	手順
暗号マップを自分で設定する。	［新しい暗号マップの追加］をクリックし、［暗号マップの追加］ウィンドウで新しい暗号マップを作成する。作成したら、［OK］をクリックする。次に、このウィンドウで［OK］をクリックする。
Cisco Configuration Professional（Cisco CP）を使ってこの接続に暗号マップを追加する。	［追加ウィザードの使用］チェック ボックスを選択し、［OK］をクリックする。Cisco CP の指示に従って、新しい暗号マップを作成すると、IPSec ポリシーにマップが関連付けられる。

暗号マップ ウィザード：ようこそ

このウィザードでは、指示に従って暗号マップを作成できます。暗号マップは、VPN 接続のもう一方の端にあるピア デバイスの指定、トラフィックの暗号化方法の決定、暗号化対象のトラフィックの識別を行います。

［次へ］をクリックして、暗号マップの作成を開始します。

暗号マップ ウィザード：設定の要約

暗号マップ ウィザードの要約ページに、ウィザードのウィンドウで入力したデータが表示されます。データを確認し、必要に応じて［戻る］をクリックして前の画面で変更を行い、その後で要約ウィンドウに戻ることができます。［完了］をクリックすると、暗号マップ設定をルータに配信できます。

接続の削除

このウィンドウでは VPN トンネルを削除できます。また、インターフェイスとの関連付けの解除だけを行って、再使用できるように定義を保持することもできます。

IPSec ポリシー < *ポリシー名* > からシーケンス番号 <*n*> の暗号マップを削除する

このボタンをクリックして［OK］をクリックし、VPN トンネル定義を削除します。このとき、インターフェイス、IPSec ポリシー、およびピア デバイス間に作成された関連付けは失われます。複数のインターフェイスがこのトンネル定義に関連付けられていた場合は、その関連付けも同様に削除されます。

ダイナミック暗号マップ セット < *セット名* > からシーケンス番号 <*n*> のダイナミック暗号マップを削除する

ダイナミック サイト間 VPN トンネルを選択した場合に、このボタンが表示されます。このボタンをクリックして［OK］をクリックし、VPN トンネル定義を削除します。このとき、インターフェイス、IPSec ポリシー、およびピア デバイス間に作成された関連付けは失われます。複数のインターフェイスがこのトンネル定義に関連付けられていた場合は、その関連付けも同様に削除されます。

インターフェイス < *インターフェイス名* > から IPSec ポリシー < *ポリシー名* > の関連付けを解除し、再利用できるように IPSec ポリシーを保存する

このボタンをクリックして［OK］をクリックすると、トンネル定義を保持したまま、そのインターフェイスとの関連付けを解除できます。必要に応じて、この定義を別のルータ インターフェイスに関連付けることができます。

Ping

このウィンドウではピア デバイスに対して ping を実行できます。ping 操作の送信元と宛先の両方を選択します。VPN トンネルをリセットした後に、リモート ピアに対する ping の実行が必要になる場合があります。

送信元

ping の送信元の IP アドレスを選択または入力します。使用するアドレスがリストにない場合は、フィールドに別のアドレスを入力できます。ping はルータの任意のインターフェイスから発行できます。デフォルトでは、**ping** コマンドはリモート デバイスに接続する外部インターフェイスから発行されます。

宛先

ping の送信先の IP アドレスを選択します。使用するアドレスがリストにない場合は、フィールドに別のアドレスを入力できます。

リモート ピアに ping を実行するには

送信元と宛先を指定し、［Ping］をクリックします。**ping** コマンドの出力で、ping が成功したかどうかを判断できます。

ping コマンドの出力をクリアするには

［クリア］をクリックします。

ミラーの生成 ...

このウィンドウには、選択したピアへの VPN トンネルに使用される IPSec ポリシーが表示されます。また、ピア デバイスで VPN 接続を設定するときに使用できるポリシーをテキスト ファイルに保存できます。

ピア デバイス

ピア デバイスの IP アドレスまたはホスト名を選択すると、そのデバイスへのトンネルに設定されている IPSec ポリシーを参照できます。ピア IP アドレスの下のボックスにポリシーが表示されます。

IPSec ポリシーのテキスト ファイルを作成するには

［保存］をクリックして、テキスト ファイルの名前と場所を指定します。ルータに作成したポリシーのミラー ポリシーをピア デバイス側でも作成できるように、このテキスト ファイルをピア デバイスの管理者に渡します。テキスト ファイルを使用してミラー ポリシーを作成する方法については、「VPN の設定後にピア ルータ上で VPN を設定する方法」を参照してください。

注意　生成したテキスト　ファイルはリモート　システムのコンフィギュレーション ファイルにコピーしないでください。このテキスト ファイルは、リモート デバイスを互換性のある方法で設定する目的でローカル ルータの設定内容を参照する場合にのみ使用します。IPSec ポリシー、IKE ポリシー、およびトランスフォーム セットには、リモート ルータで同じ名前を使用できますが、ポリシーとトランスフォーム セットは異なる名前にすることもできます。テキスト ファイルを単純にリモート コンフィギュレーション ファイルにコピーした場合、設定エラーが発生する可能性が高くなります。

Cisco CP 警告：ACL を使用する NAT ルール

このウィンドウは、アクセス ルールを使用する NAT ルールに関連付けられているインターフェイスを使用して VPN を設定するときに表示されます。このタイプの NAT ルールは、パケットが LAN を出入りする前にパケット内の IP アドレスを変更する可能性があります。このため、NAT ルールが送信元 IP アドレスを変更したことによって VPN 接続用に設定された IPSec ルールと一致しなくなった場合、VPN 接続は適切に機能しません。これを防ぐために、Cisco CP はこれらのルールを、ルート マップを使用する NAT ルールに変換できます。ルート マップで、変換してはならないサブネットを指定します。

ウィンドウには、VPN 接続が適切に機能するために変更する必要がある NAT ルールが表示されます。

元のアドレス

NAT が変換する IP アドレスです。

変換後のアドレス

NAT が元のアドレスと置き換える IP アドレスです。

ルール タイプ

NAT ルールのタイプです。値は［スタティック］または［ダイナミック］のどちらかになります。

リストされている NAT ルールでルート マップを使用するには

［OK］をクリックします。

その他の手順

ここでは、ウィザードで設定できないタスクの手順を示します。

複数のサイトに対して VPN を作成する方法

Cisco CP を使用して、ルータの 1 つのインターフェイスに複数の VPN トンネルを作成できます。各 VPN トンネルは、ルータで選択した、宛先ルータ上の異なるサブネットへのインターフェイスに接続されます。接続する宛先ルータのインターフェイスが同じで、サブネットが異なる VPN トンネルを複数設定することができます。また、宛先ルータ上の別のインターフェイスに接続する VPN トンネルを複数設定することもできます。

まず、最初の VPN トンネルを作成する必要があります。次の手順では最初の VPN トンネルを作成する方法を説明します。すでに 1 つめの VPN トンネルを作成済みで、同じインターフェイスにトンネルを追加する必要がある場合は、最初の手順を省略して、このヘルプ トピックの次の手順に従います。

最初の VPN トンネルを作成する

ステップ 1　機能バーで、［設定］>［セキュリティ］>［VPN］>［サイト間 VPN］の順に選択します。

ステップ 2　［サイト間 VPN を作成する］を選択します。

ステップ 3　［選択したタスクを実行する］をクリックします。

VPN ウィザードが起動します。

ステップ 4　［クイック セットアップ］をクリックします。

ステップ 5　［次へ >］をクリックします。

ステップ 6　［この VPN 接続に対するインターフェイスの選択］フィールドで、VPN トンネルを作成する送信元ルータのインターフェイスを選択します。これは、ユース ケース シナリオ図のローカル システム上のインターネットに接続されているインターフェイスです。

ステップ 7　［ピア ID］フィールドに、宛先ルータ インターフェイスの IP アドレスを入力します。

ステップ 8　認証のフィールドに、2 つの VPN ピアが使用する事前共有キーを入力し、その後、キーを再入力します。

ステップ 9　［送信元］フィールドで、IP トラフィックを保護するサブネットに接続するインターフェイスを選択します。これは、ユース ケース シナリオ図のローカル ルータで、通常は LAN に接続されているインターフェイスです。

ステップ 10［宛先］フィールドに、宛先ルータの IP アドレスとサブネット マスクを入力します。

ステップ 11［次へ >］をクリックします。

ステップ 12［完了］をクリックします。

同じ送信元インターフェイスからさらにトンネルを作成する

最初の VPN トンネルを作成したら、次の手順に従って、同じ送信元インターフェイスから異なる宛先インターフェイスまたは宛先サブネットへのトンネルをさらに作成します。

ステップ 1　機能バーで、［設定］>［セキュリティ］>［VPN］>［サイト間 VPN］の順に選択します。

ステップ 2　［サイト間 VPN を作成する］を選択します。

ステップ 3　［選択したタスクを実行する］をクリックします。

VPN ウィザードが起動します。

ステップ 4　［クイック セットアップ］をクリックします。

ステップ 5　［次へ >］をクリックします。

ステップ 6　［この VPN 接続に対するインターフェイスの選択］フィールドで、最初の VPN 接続の作成に使用したものと同じインターフェイスを選択します。

ステップ 7　［ピア ID］フィールドに、宛先ルータ インターフェイスの IP アドレスを入力します。最初の VPN 接続の作成で入力したときと同じ IP アドレスを入力できます。これにより、2 つめの VPN 接続でも、宛先ルータの最初の VPN 接続と同じインターフェイスを使用することになります。両方の VPN 接続で同じ宛先インターフェイスを使用しない場合は、宛先ルータ上の別のインターフェイスの IP アドレスを入力します。

ステップ 8　認証のフィールドに、2 つの VPN ピアが使用する事前共有キーを入力し、その後、キーを再入力します。

ステップ 9　［送信元］フィールドで、最初の VPN 接続の作成に使用したものと同じインターフェイスを選択します。

ステップ 10　宛先のフィールドには、次のオプションがあります。

- ［ピア ID］フィールドで、宛先ルータ上の異なるインターフェイスの IP アドレスを入力し、特定のサブネットからの IP トラフィックを保護する場合は、サブネットの IP アドレスとサブネット マスクを適切なフィールドに入力します。
- ［ピア ID］フィールドに、最初の VPN 接続で使用したものと同じ IP アドレスを入力し、この VPN トンネルが最初の VPN トンネルと同じルータ インターフェイスを使用することを指定した場合は、保護する新しいサブネットの IP アドレスとサブネット マスクを適切なフィールドに入力します。

ステップ 11　［次へ >］をクリックします。

ステップ 12［完了］をクリックします。

VPN の設定後にピア ルータ上で VPN を設定する方法

Cisco CP は、ルータに VPN 設定を生成します。Cisco CP には、設定のテキスト ファイルを生成する機能があります。これは、VPN トンネルの接続先となるピア ルータの VPN 設定を作成するためのテンプレートとして使用できます。このテキスト ファイルは、設定が必要なコマンドを示すテンプレートとしてのみ使用できます。このファイルの情報は、設定したローカル ルータだけに有効であるため、使用するには編集する必要があります。

ピア VPN ルータのテンプレート設定を生成するには

ステップ 1　機能バーで、［設定］>［セキュリティ］>［VPN］>［サイト間 VPN］の順に選択します。

ステップ 2　［サイト間 VPN の編集］をクリックします。

ステップ 3　テンプレートとして使用する VPN 接続を選択し、［ミラーの生成］をクリックします。

Cisco CP で［ミラーの生成］画面が表示されます。

ステップ 4　［ピア デバイス］フィールドで、推奨される設定を生成するピア デバイスの IP アドレスを選択します。

ピア デバイスに対して推奨される設定が［ミラーの生成］画面に表示されます。

ステップ 5　［保存］をクリックして、Windows の［ファイルの保存］ダイアログ ボックスを表示し、ファイルを保存します。

注意　編集していないミラー設定をピア　デバイスに適用しないでください。この設定は、手動の追加設定を必要とするテンプレートです。このテンプレートは、新しく VPN ピアの設定を作り直すときにのみ使用します。

ステップ 6　ファイルを保存した後、テキスト　エディタを使用してテンプレート設定に必要な変更を行います。編集が必要となる可能性があるコマンドを次に示します。

- ピア IP アドレスのコマンド
- トランスフォーム ポリシーのコマンド
- 暗号マップ IP アドレスのコマンド
- ACL のコマンド
- インターフェイス IP アドレスのコマンド

ステップ 7　ピア コンフィギュレーション ファイルの編集が終わったら、TFTP サーバを使用して、ピア ルータに配信します。

既存の VPN トンネルを編集する方法

既存の VPN トンネルを編集するには

ステップ 1　機能バーで、［設定］>［セキュリティ］>［VPN］>［サイト間 VPN］の順に選択します。

ステップ 2　［サイト間 VPN の編集］をクリックします。

ステップ 3　編集する接続をクリックします。

ステップ 4　［追加］をクリックします。

ステップ 5　［< ポリシー名 > へのスタティック暗号マップ］を選択します。

ステップ 6　［スタティック暗号マップの追加］ウィンドウで、VPN 接続に暗号マップを追加できます。

ステップ 7　IPSec ポリシーや既存の暗号マップなど、接続のコンポーネントを変更する必要がある場合は、VPN ウィンドウ内のそのコンポーネントの名前を記録し、［VPN コンポーネント］の下の適切なウィンドウに移動して変更します。

VPN の動作を確認する方法

VPN 接続の動作は、Cisco CP の監視モードを使用して確認できます。VPN 接続が機能している場合は、送信元と宛先のピア IP アドレスを特定することによって、監視モードで VPN 接続が表示されます。VPN 接続が IPSec トンネルか、インターネット キー交換（IKE）セキュリティ アソシエーション（SA）かによって、監視モードでは、その接続で転送されたパケット数、または接続の現在の状態のいずれかが表示されます。VPN 接続の現在の状態を表示するには

ステップ 1　機能バーで、［監視］>［セキュリティ］の順に選択します。

ステップ 2　［VPN ステータス］を選択します。

ステップ 3　［IPSec トンネル］または［IKE SA］を選択します。

設定されている個々の VPN 接続が画面に行として表示されます。

IPSec トンネル情報を表示している場合は、次の情報で、その VPN 接続が機能していることを確認できます。

- ローカル ピアおよびリモート ピアの IP アドレスが正しい。これは、適切なサイトおよびルータ インターフェイス間に VPN 接続が存在することを示します。

- トンネルのステータスが「稼働」になっている。もし、トンネルのステータスが「停止」または「設定上停止」になっている場合は、VPN 接続はアクティブではありません。
- カプセル化されたパケットおよび非カプセル化パケットの数がゼロではない。これは、データが接続を介して転送されたこと、および送受信されたエラーが多くないことを示します。

IKE SA 情報を表示している場合は、送信元と宛先の IP アドレスが正しいこと、および接続が認証され、データ転送が可能であることを示す「QM_IDLE」状態になっていることを確認することにより、VPN 接続が機能していることを確認できます。

VPN に対してバックアップ ピアを設定する方法

1 つの暗号マップに複数の VPN ピアを設定するには

ステップ 1　機能バーで、［設定］>［セキュリティ］>［VPN コンポーネント］>［IPSec］の順に選択します。

ステップ 2　［IPSec ポリシー（暗号マップ セット）］を選択します。

ステップ 3　［IPSec ポリシー］テーブルで、別の VPN ピアを追加する IPSec ポリシーをクリックします。

ステップ 4　［編集］をクリックします。

［IPSec ポリシーの編集］ダイアログ ボックスが表示されます。

ステップ 5　［追加］をクリックします。

ステップ 6　［暗号マップの追加］ダイアログ ボックスが表示され、新しい暗号マップの値を設定できます。ダイアログ ボックスの 4 つのタブすべてを使用して、新しい暗号マップの値を設定します。［ピア情報］タブの［ピアの指定］フィールドには、追加するピアの IP アドレスを入力できます。

ステップ 7　値の入力を終えたら、［OK］をクリックします。

新しいピア IP アドレスを設定した暗号マップが［この IPSec ポリシー内の暗号マップ］テーブルに表示されます。

ステップ 8　さらにピアを追加する場合は、手順 3 ～ 7 を繰り返します。

VPN サポート レベルが異なる複数のデバイスを調整する方法

1 つの暗号マップに複数のトランスフォーム セットを追加するには

ステップ 1　機能バーで、［設定］>［セキュリティ］>［VPN コンポーネント］>［IPSec］の順に選択します。

ステップ 2　［IPSec ポリシー（暗号マップ セット）］を選択します。

ステップ 3　［IPSec ポリシー］テーブルで、別のトランスフォーム セットを追加する暗号マップを含む IPSec ポリシーをクリックします。

ステップ 4　［編集］をクリックします。

［IPSec ポリシーの編集］ダイアログ ボックスが表示されます。

ステップ 5　［この IPSec ポリシー内の暗号マップ］テーブルで、別のトランスフォーム セットを追加する暗号マップをクリックします。

ステップ 6　［編集］をクリックします。

［暗号マップの編集］ダイアログ ボックスが表示されます。

ステップ 7　［トランスフォーム セット］タブをクリックします。

ステップ 8　［使用可能なトランスフォーム セット］フィールドで、暗号マップに追加するトランスフォーム セットをクリックします。

ステップ 9　［>>］をクリックし、選択したトランスフォーム セットを暗号マップに追加します。

ステップ 10　この暗号マップにさらにトランスフォーム　セットを追加する場合は、すべてのトランスフォーム セットを追加し終えるまで手順 8 および 9 を繰り返します。

ステップ 11　［OK］をクリックします。

サポートされていないインターフェイスで VPN を設定する方法

Cisco CP では、サポートされていないタイプのインターフェイスに VPN を設定できます。VPN 接続を設定する前に、ルータ CLI を使用して、インターフェイスを設定する必要があります。インターフェイスには、少なくとも IP アドレスを設定する必要があり、また、機能していなければなりません。接続が機能していることを確認するには、インターフェイスのステータスが［稼働］になっていることを確認します。

CLI を使用してサポートされていないインターフェイスを設定した後で、Cisco CP を使用して VPN 接続を設定できます。サポートされていないインターフェイスは、VPN 接続用のインターフェイスを選択するフィールドに表示されます。

ファイアウォールの設定後に VPN を設定する方法

ファイアウォールが設定された環境で VPN を機能させるには、ローカルおよびリモート ピアの IP アドレス間のトラフィックを許可するようにファイアウォールを設定する必要があります。この設定は、ファイアウォールを設定した後で VPN を設定するときに、Cisco CP においてデフォルトで作成されます。

VPN に対して NAT パススルーを設定する方法

NAT を使用して自分のネットワーク外のネットワークからのアドレスを変換する場合で、VPN を介して自分のネットワーク外の特定のサイトにも接続している場合は、VPN トラフィックでネットワーク アドレスの変換が行われないように、VPN 接続に対して NAT パススルーを設定する必要があります。すでに NAT を設定したルータに、Cisco CP を使用して新しい VPN 接続を設定する場合は、NAT が VPN トラフィックを変換しないように設定されることを通知する警告メッセージが表示されます。このメッセージを受け入れると、Cisco CP で必要な ACL が作成されて VPN トラフィックが変換されないように保護されます。

すでに VPN 接続を設定している場合に、Cisco CP を使用して NAT を設定するときは、次の手順を実行して ACL を作成します。

ステップ 1　機能バーで、［設定］>［セキュリティ］>［ACL エディタ］の順に選択します。

ステップ 2　ルール ツリーで、［アクセス ルール］を選択します。

ステップ 3　［追加］をクリックします。

［ルールの追加］ダイアログ ボックスが表示されます。

ステップ 4　［名前 / 番号］フィールドに、新しいルールの一意の名前または番号を入力します。

ステップ 5　［タイプ］フィールドから［拡張ルール］を選択します。

ステップ 6　［説明］フィールドに、新しいルールについての簡単な説明を入力します。

ステップ 7　［追加］をクリックします。

［拡張ルール エントリの追加］ダイアログ ボックスが表示されます。

ステップ 8　［アクション］フィールドで、［許可］を選択します。

ステップ 9　［送信元ホスト / ネットワーク］グループの［タイプ］フィールドで、［ネットワーク］を選択します。

ステップ 10［IP アドレス］および［ワイルドカード マスク］フィールドに、VPN の送信元ピアの IP アドレスとサブネット マスクを入力します。

ステップ 11［宛先ホスト / ネットワーク］グループの［タイプ］フィールドで、［ネットワーク］を選択します。

ステップ 12［IP アドレス］および［ワイルドカード マスク］フィールドに、VPN の宛先ピアの IP アドレスとサブネット マスクを入力します。

ステップ 13［説明］フィールドに、ネットワークまたはホストについての簡単な説明を入力します。

ステップ 14［OK］をクリックします。

新しいルールが［アクセス ルール］テーブルに表示されます。