CHAPTER 18

IP Security

IP Security（IPSec）は、ピア間のデータの機密性、データの整合性、およびデータ認証を提供するオープン スタンダードのフレームワークです。これらのセキュリティ サービスは IP 層で提供されます。IPSec では、IKE を使用して、ローカル ポリシーに基づいてプロトコルとアルゴリズムのネゴシエーションを処理し、IPSec で使用する暗号キーと認証キーを生成します。

Cisco CP では、IPSec のトランスフォーム セット、ルール、およびポリシーを設定できます。

使用する IPSec 設定ウィンドウに移動するには、［IPSec］ツリーを使用します。

IPSec ポリシー

このウィンドウには、ルータに設定されている IPSec ポリシーと、各ポリシーに関連付けられている暗号マップが表示されます。IPSec ポリシーは VPN 接続の定義に使用されます。IPSec ポリシー、暗号マップ、および VPN 接続の関係の詳細については、「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。

アイコン

このアイコンが IPSec ポリシーの横に表示されている場合は読み取り専用なので、編集できません。IPSec ポリシーが読み取り専用になるのは、Cisco CP でサポートされていないコマンドが含まれている場合です。

名前

この IPSec ポリシーの名前です。

タイプ

次のタイプがあります。

- ［ISAKMP］— IKE を使用して、この暗号マップ エントリで指定されたトラフィックを保護するための IPSec セキュリティ アソシエーションを確立します。Cisco CP では、ISAKMP（Internet Security Association and Key Management Protocol）の暗号マップがサポートされています。
- ［手動］— IKE を使用せずに、この暗号マップ エントリで指定されたトラフィックを保護するための IPSec セキュリティ アソシエーションを確立します。

  Cisco CP では、手動の暗号マップの作成はサポートされていません。CLI（コマンドライン インターフェイス）を使用して作成された手動の暗号マップは、読み取り専用とみなされます。
- ［ダイナミック］— この暗号マップ エントリが、既存のダイナミック暗号マップを参照するように指定します。ダイナミック暗号マップは、ピアの IPSec デバイスからのネゴシエーション要求を処理するときに使用されるポリシー テンプレートです。

Cisco CP では、ダイナミック暗号マップの作成はサポートされていません。CLI を使用して作成されたダイナミック暗号マップは、読み取り専用とみなされます。

この IPSec ポリシー内の暗号マップ

名前

暗号マップが含まれている IPSec ポリシーの名前です。

シーケンス番号

IPSec ポリシーが VPN 接続で使用されている場合は、シーケンス番号と IPSec ポリシー名の組み合わせでこの接続を一意に識別します。

ピア

このカラムには、暗号マップで指定されているピア デバイスの IP アドレスまたはホスト名が表示されます。複数のピアはカンマで区切られます。

トランスフォーム セット

このカラムには、暗号マップで使用されているトランスフォーム セットが表示されます。

この IPSec ポリシー内のダイナミック暗号マップ セット

ダイナミック暗号マップ セット名

このダイナミック暗号マップ セットの名前です。管理者は、この名前によって暗号マップ セットの用途を把握できます。

シーケンス番号

このダイナミック暗号マップ セットのシーケンス番号です。

タイプ

タイプは常に［ダイナミック］です。

実行する操作

目的	手順
IPSec ポリシーを設定に追加する。	［追加］をクリックする。
既存の IPSec ポリシーを編集する。	ポリシーを選択して［編集］をクリックする。
ポリシーから暗号マップ エントリを削除する。	ポリシーを選択して［編集］をクリックする。ウィンドウで、削除する暗号マップを選択して［削除］をクリックする。次に、［OK］をクリックしてこのウィンドウに戻る。
IPSec ポリシーを削除する。	ポリシーを選択して［削除］をクリックする。

IPSec ポリシーの追加 / 編集

このウィンドウでは、IPSec ポリシーを追加または編集します。

名前

この IPSec ポリシーの名前です。英数字を組み合わせた名前を指定できます。ポリシー名にピア名やその他の有用な情報を含めると役に立つ場合があります。

この IPSec ポリシー内の暗号マップ

このボックスには、この IPSec ポリシー内の暗号マップのリストが表示されます。リストには、この暗号マップを設定する名前、シーケンス番号、およびトランスフォーム セットが含まれます。暗号マップを選択して、それを編集したり IPSec ポリシーから削除したりできます。

暗号マップを追加するには、［追加］をクリックします。Cisco CP の指示に従ってプロセスを実行するには、［追加ウィザードの使用］を選択してから［追加］をクリックします。

アイコン

暗号マップが読み取り専用の場合は、このカラムに読み取り専用アイコンが表示されます。暗号マップが読み取り専用になるのは、Cisco CP でサポートされていないコマンドが含まれている場合です。

この IPSec ポリシー内のダイナミック暗号マップ セット

このボックスには、この IPSec ポリシー内のダイナミック暗号マップ セットのリストが表示されます。既存のダイナミック暗号マップ セットをポリシーに追加するには、［追加］ボタンを使用します。選択したダイナミック暗号マップ セットをポリシーから削除するには、［削除］ボタンを使用します。

実行する操作

目的	手順
このポリシーに暗号マップを追加する。	［追加］をクリックし、［暗号マップの追加］パネルで暗号マップを作成する。または、［追加ウィザードの使用］を選択してから［追加］をクリックする。 **（注）** ウィザードでは、暗号マップに 1 つのトランスフォーム セットしか追加できない。暗号マップに複数のトランスフォーム セットを追加する必要がある場合は、ウィザードを使用しないこと。
このポリシー内の暗号マップを編集する。	暗号マップを選択し、［編集］をクリックして、［暗号マップの編集］パネルで暗号マップを編集する。
このポリシーから暗号マップを削除する。	暗号マップを選択し、［削除］をクリックする。

暗号マップの追加 / 編集：全般

このウィンドウでは、暗号マップの全般的なパラメータを変更します。このウィンドウには次のフィールドがあります。

IPSec ポリシー名

この暗号マップが使用されているポリシーの名前が表示される読み取り専用フィールドです。暗号マップ ウィザードを使用している場合、このフィールドは表示されません。

説明

このフィールドでは、暗号マップの説明を入力または編集します。この説明は VPN 接続リストに表示され、この暗号マップを同じ IPSec ポリシー内の別の暗号マップと識別するのに役立ちます。

シーケンス番号

IPSec ポリシー名と一緒に表示される番号は、接続の識別に使用されます。Cisco CP は、自動的にシーケンス番号を生成します。手動でシーケンス番号を入力することもできます。

SA ライフタイム

IPSec セキュリティ アソシエーションでは、共有キーを使用します。これらのキーとセキュリティ アソシエーションは同時にタイムアウトになります。ライフタイムには、時間的なライフタイムとトラフィック ボリュームによるライフタイムがあります。セキュリティ アソシエーションは、これらのライフタイムのいずれかに到達したときに期限が切れます。

このフィールドを使用して、この暗号マップに、グローバルに指定されるライフタイムとは異なるセキュリティ アソシエーション ライフタイムを指定できます。［キロバイト］フィールドでは、ライフタイムを送信するキロバイト数で指定できます。最大値は 4,608,000 です。［HH:MM:SS］フィールドでは、ライフタイムを時、分、秒単位で指定できます。また、時間的なライフタイムとトラフィック ボリュームによるライフタイムの両方を指定することも可能です。両方が指定されている場合、ライフタイムは最初の条件が満たされた時点で期限が切れます。

完全転送秘密

セキュリティ キーを以前生成したキーから派生させると、1 つのキーが漏洩した場合に他のキーも同様に漏洩する可能性があるので、セキュリティの点で問題があります。完全転送秘密（PFS）では、個々のキーが独立して派生されることが保証されます。このため、PFS を有効化すれば、1 つのキーが漏洩してもそれ以外のキーが漏洩することはありません。PFS を有効にする場合は、Diffie-Hellman グループ 1、グループ 2、またはグループ 5 のどの方式を使用するか指定できます。

（注）　ルータでグループ 5 がサポートされていない場合は、グループ 5 はこのリストには表示されません。

Reverse Route Injection の有効化

Reverse Route Injection（RRI）は、リモート VPN クライアントまたは LAN 間セッションで Open Shortest Path First（OSPF）プロトコルまたはルーティング インフォメーション プロトコル（RIP）を実行する内部ルータのルーティング テーブルにデータを挿入するために使用されます。

RRI は、Easy VPN サーバに接続されたクライアントにスタティック ルートをダイナミックに追加します。

暗号マップの追加 / 編集：ピア情報

暗号マップには、セキュリティ アソシエーションに関与するピアのホスト名または IP アドレスが含まれます。この画面では、この暗号マップに関連付けられるピアの追加と削除ができます。複数のピアは、暗号化されたデータのための複数のルートをルータに提供します。

目的	手順
［現在のリスト］にピアを追加する。	ピアの IP アドレスまたはホスト名を入力し、［追加］をクリックする。
［現在のリスト］からピアを削除する。	ピアを選択して［削除］をクリックする。

暗号マップの追加 / 編集：トランスフォーム セット

このウィンドウを使用して、暗号マップで使用するトランスフォーム セットを追加し、編集します。暗号マップには、セキュリティ アソシエーションに関与するピアのホスト名または IP アドレスが含まれます。複数のピアは、暗号化されたデータのための複数のルートをルータに提供します。ただし、VPN 接続の両端にあるデバイスは、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。

ルータに、トランスフォーム セットを 1 つ持つ暗号マップを提供すれば十分である場合は、暗号マップ ウィザードを使用します。

複数のトランスフォーム セットを持つ暗号マップを手動で設定する際に、ネゴシエート中のピアが受け入れるトランスフォーム セットをルータが提供できるようにする場合は、[追加ウィザードの使用] の選択を解除し、[新しい暗号マップの追加] を使用します。すでに暗号マップ ウィザードで作業している場合は、このウィザードを終了し、[追加ウィザードの使用] の選択を解除してから [新しい暗号マップの追加] をクリックします。

複数のトランスフォーム セットを持つ暗号マップを手動で設定する場合、トランスフォーム セットの順番を指定することもできます。ルータはトランスフォーム セットをこの順番で使用して、ネゴシエーションを行います。

使用可能なトランスフォーム セット

暗号マップで使用できる設定済みのトランスフォーム セットです。暗号マップ ウィザードでは、使用可能なトランスフォーム セットは、[トランスフォーム セットの選択] ドロップダウン リストに表示されます。

ルータにトランスフォーム セットが設定されていない場合は、Cisco CP のデフォルト トランスフォーム セットのみ表示されます。

（注）

- すべてのルータがすべてのトランスフォーム　セット（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トランスフォーム セットは、ウィンドウに表示されません。
- Cisco CP がサポートしているすべてのトランスフォーム セットをすべての IOS イメージがサポートしているわけではありません。IOS イメージでサポートされていないトランスフォーム セットは、ウィンドウに表示されません。
- 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と IOS イメージの両方でサポートされているトランスフォーム セットだけがウィンドウに表示されます。

選択したトランスフォーム セットの詳細（暗号マップ ウィザードのみ）

選択した暗号マップの名前、暗号、認証の属性、その他のパラメータが表示されます。

このアイコンがトランスフォーム セットの横に表示されている場合は読み取り専用で、編集はできません。

選択したトランスフォーム セットの優先順位（暗号マップの手動設定のみ）

この暗号マップ用に選択されたトランスフォーム セットが使用される順に表示されます。ルータは、ピアとのネゴシエート時にこのリストの順番でトランスフォーム セットを提供します。リストを並べ替えるには、上矢印と下矢印ボタンを使用します。

実行する操作（暗号マップ ウィザードのみ）

目的	手順
選択したトランスフォーム セットを暗号マップに使用する。	［次へ］をクリックする。
既存の別のトランスフォーム セットを使用する。	［トランスフォーム セットの選択］リストでトランスフォーム セットを選択し、［次へ］をクリックする。
新しいトランスフォーム セットを使用する。	［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。その後、このウィンドウに戻って、［次へ］をクリックする。
選択したトランスフォーム セットを編集する。	［編集］をクリックし、［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。
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。これでピアが使用に同意するトランスフォーム セットをルータが確実に提供できる。	暗号マップ ウィザードを終了して［追加ウィザードの使用］の選択を解除し、［暗号マップの追加］をクリックする。［トランスフォーム セット］タブでは、トランスフォーム セットの追加と並べ替えができる。

実行する操作（暗号マップの手動設定のみ）

目的	手順
［選択されたトランスフォーム セット］ボックスにトランスフォーム セットを追加する。	［使用可能なトランスフォーム セット］ボックスでトランスフォーム セットを選択し、右矢印ボタンをクリックする。
［選択されたトランスフォーム セット］ボックスからトランスフォーム セットを削除する。	削除するトランスフォーム セットを選択して左矢印ボタンをクリックする。
選択したトランスフォーム セットの優先順位を変更する。	トランスフォーム セットを選択し、上矢印または下矢印ボタンをクリックする。
［使用可能なトランスフォーム セット］リスト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 セットを設定する。
［使用可能なトランスフォーム セット］リストのトランスフォーム セットを編集する。	［編集］をクリックし、［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 セットを設定する。

暗号マップの追加 / 編集：トラフィックの保護

すべてのトラフィックを保護するように暗号マップを設定したり（暗号マップ ウィザードのみ）、IPSec ルールを選択して指定したトラフィックを保護するように暗号マップを設定したりすることができます。

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（暗号マップ ウィザードのみ）

このオプションを使用して、暗号化するトラフィックを発信する送信元サブネット（LAN 上のサブネット）を 1 つと、［ピア］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。他の送信元と宛先サブネット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。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。サブネット番号およびマスクは、ドット（.）で区切った 10 進表記で入力する必要があります。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。

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暗号化されます。

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。サブネット番号およびマスクは、ドット（.）で区切った 10 進表記で入力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暗号化されます。

IPSec ルール（IPSec トラフィックのアクセスリストを作成 / 選択する）

この暗号マップで使用される IPSec ルールを追加または変更できます。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。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。

（注） トンネル インターフェイスを使用する VPN 接続の IPSec ルールを追加する場合は、そのルールで、トンネル設定として同じ送信元と宛先のデータを指定する必要があります。

暗号マップの IPSec ルールを追加または変更するには、［IPSec ルール］フィールドの右側にある［...］ボタンをクリックし、次のいずれかを選択します。

- ［既存のルール（ACL）を選択する］— 作成済みのルールを使用する場合は、そのルールを選択して［OK］をクリックします。
- ［新しいルールを作成して選択する］— 必要なルールがまだ作成されていない場合は、そのルールを作成して［OK］をクリックします。
- ［なし］— ルールの関連付けを解除する場合に選択します。［IPSec ルール］フィールドには使用中の IPSec ルール名が表示されていますが、［なし］を選択すると、このフィールドは空白になります。

［IPSec ルール］フィールドに直接、IPSec ルールの番号を入力して、暗号マップに IPSec ルールを追加、または変更することもできます。

（注） IPSec　ルールは、標準ルールではなく拡張ルールにする必要があります。標準ルールの番号または名前を入力した場合は、［OK］をクリックすると警告メッセージが表示されます。

ダイナミック暗号マップ セット

このウィンドウには、ルータに設定されているダイナミック暗号マップ セットが表示されます。

追加 / 編集 / 削除ボタン

これらのボタンを使用して、ウィンドウに表示された暗号マップを管理します。IPSec ポリシーに関連付けられている暗号マップ セットを削除しようとしても、Cisco CP によって許可されません。削除する前に、暗号マップとポリシーの関連付けを解除する必要があります。関連付けの解除は、［IPSec ポリシー］ウィンドウで実行できます。

名前

ダイナミック暗号マップの名前です。

タイプ

常に［ダイナミック］です。

ダイナミック暗号マップ セットの追加 / 編集

このウィンドウでは、ダイナミック暗号マップ セットを追加または編集します。

名前

ダイナミック暗号マップを追加する場合は、このフィールドに名前を入力します。暗号マップ セットを編集する場合は、このフィールドは無効になり、名前を変更できません。

この IPSec ポリシー内の暗号マップ

このエリアには、このセットで使用される暗号マップのリストが表示されます。このリスト内の暗号マップを追加、削除、または変更するには、［追加］、［編集］、または［削除］ボタンを使用します。

この IPSec ポリシーに暗号マップを関連付ける

シーケンス番号

この暗号マップ セットを識別するシーケンス番号を入力します。他の暗号マップ セットで使用されている番号は指定できません。

ダイナミック暗号マップ セットを選択してください

追加するダイナミック暗号マップ セットをこのリストから選択します。

この暗号マップ セット内の暗号マップ

このエリアには、選択したダイナミック暗号マップ セットに含まれている名前、シーケンス番号、およびピアのリストが表示されます。

IPSec プロファイル

このウィンドウには、ルータに設定されている IPSec プロファイルのリストが表示されます。IPSec プロファイルは、1 つ以上の設定済みトランスフォーム セットで設定されています。プロファイルは mGRE トンネルに適用され、トンネル トラフィックを暗号化する方法を定義します。

名前

IPSec プロファイルの名前です。

トランスフォーム セット

このプロファイルで使用されるトランスフォーム セットです。

説明

IPSec プロファイルに関する説明です。

追加

新しい IPSec プロファイルを追加する場合にクリックします。

編集

既存のプロファイルを選択し、［編集］をクリックしてプロファイルの設定を変更します。

削除

選択した IPSec プロファイルを削除する場合にクリックします。削除するプロファイルが現在 DMVPN トンネルで使用されている場合は、別の IPSec プロファイルを使用するように DMVPN トンネルを設定する必要があります。

IPSec プロファイルの詳細

このエリアには、選択した IPSec プロファイルの設定が表示されます。このエリアに表示される情報の詳細については、「IPSec プロファイルの追加 / 編集」を参照してください。

IPSec プロファイルの追加 / 編集

このダイアログには、IPSec プロファイルを作成するための情報を入力します。IPSec プロファイルは、使用するトランスフォーム セット、セキュリティ アソシエーション（SA）ライフタイムの特定方法などの情報を指定します。

トランスフォーム セット カラム

ダイアログの上部にある 2 つのカラムを使用して、プロファイルに追加するトランスフォーム セットを指定します。左側のカラムには、ルータに設定されているトランスフォーム セットが表示されます。設定されているトランスフォーム セットをプロファイルに追加するには、そのセットを選択して、［>>］ボタンをクリックします。左側のカラムにトランスフォーム セットが表示されていない場合や、まだ作成されていないトランスフォーム セットが必要な場合は、［追加］をクリックして、表示されるダイアログでトランスフォーム セットを作成します。

IKE プロファイル関連付け

IKE プロファイルを対象の IPSec プロファイルに関連付ける場合は、リストから既存のプロファイルを選択します。IKE プロファイルがすでに関連付けられている場合、このフィールドは読み取り専用になります。

時間ベースの IPSec SA ライフタイム

一定時間が経過したら新しい SA が確立されるようにする場合は、［時間ベースの IPSec SA ライフタイム］をクリックします。右側の［HH:MM:SS］フィールドに時間を入力します。

トラフィック量ベースの IPSec SA ライフタイム

指定した量のトラフィックが IPSec トンネルを通過したら新しい SA が確立されるようにする場合は、［トラフィック量ベースの IPSec SA ライフタイム］をクリックします。既存の SA が解除されて新しい SA が確立するまでに、トンネルを通過するトラフィックのキロバイト数（KB）を入力します。

IPSec SA アイドル タイム

指定した期間ピアがアイドル状態だった場合に新しい SA が確立されるようにする場合は、［IPSec SA アイドル タイム］をクリックします。右側の［HH:MM:SS］フィールドにアイドル時間を入力します。

完全転送秘密

IPSec がこの仮想テンプレート インターフェイスに新しいセキュリティ アソシエーションを要求する際に PFS（perfect forward secrecy; 完全転送秘密）を求める必要がある場合、またはピアから受信する要求に PFS が必要な場合は、［完全転送秘密］をクリックします。指定できる値は次のとおりです。

- グループ 1 — PFS 要求の暗号化に、768 ビットの Diffie-Hellman プライム モジュラス グループが使用されます。
- グループ 2 — PFS 要求の暗号化に、1,024 ビットの Diffie-Hellman プライム モジュラス グループが使用されます。
- グループ 5 — PFS 要求の暗号化に、1,536 ビットの Diffie-Hellman プライム モジュラス グループが使用されます。

IPSec プロファイルの追加 / 編集とダイナミック暗号マップの追加

このウィンドウでは、IPSec プロファイルの追加と編集、またはダイナミック暗号マップの追加を行います。

名前

このプロファイルの名前を入力します。

使用可能なトランスフォーム セット

このカラムには、このルータに設定されているトランスフォーム セットが表示されます。このリスト内のトランスフォーム セットを［選択されたトランスフォーム セット］カラムに追加するには、トランスフォーム セットを選択して右矢印（>>）ボタンをクリックします。

新しいトランスフォーム セットを設定する必要がある場合は、［IPSec］ツリーの［トランスフォーム セット］ノードをクリックして［トランスフォーム セット］ウィンドウに移動します。そのウィンドウで［追加］をクリックし、新しいトランスフォーム セットを作成します。

選択されたトランスフォーム セット

このカラムには、このプロファイルで使用されているトランスフォーム セットが表示されます。設定中のルータとトンネル先のルータが使用するトランスフォーム セットについてネゴシエートできるように、複数のトランスフォーム セットを選択できます。

トランスフォーム セット

この画面では、トランスフォーム セットの表示、新しいトランスフォーム セットの追加、および既存のトランスフォーム セットの編集または削除を行うことができます。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。

複数のトランスフォーム セットを作成して、1 つの暗号マップ エントリで、これらのトランスフォーム セットを 1 つ以上指定できます。暗号マップ エントリで定義されたトランスフォーム セットは、その暗号マップ エントリのアクセス リストによって指定されたデータ フローを保護するための IPSec セキュリティ アソシエーションのネゴシエーションで使用されます。

IKE との IPSec セキュリティ アソシエーションのネゴシエート時に、ピアは両方のピアに設定されているトランスフォーム セットを探します。そのようなトランスフォーム セットが見つかると、そのトランスフォーム セットが選択され、両方のピアの IPSec セキュリティ アソシエーションの要素として、保護するトラフィックに適用されます。

名前

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

Cisco CP では、次の ESP 暗号化タイプが認識されます。

- ESP_DES — DES（Data Encryption Standard）を使用する ESP（Encapsulating Security Payload）。DES は、56 ビットの暗号化をサポートします。
- ESP_3DES — トリプル DES を使用する ESP。これは、DES よりも強力な暗号形式で、168 ビットの暗号化をサポートします。
- ESP_AES_128 — AES（Advanced Encryption Standard）を使用する ESP。暗号化には 128 ビットのキーが使用されます。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。
- ESP_AES_192 — 192 ビット キーの AES 暗号化を使用する ESP。
- ESP_AES_256 — 256 ビット キーの AES 暗号化を使用する ESP。

- ESP_NULL — Null 暗号化アルゴリズム。ただし、暗号化トランスフォームが使用されます。
- ESP_SEAL — 160 ビット暗号キーに基づく SEAL（Software Encryption Algorithm）暗号化アルゴリズムを使用する ESP。SEAL（Software Encryption Algorithm）は、ソフトウェアベースの DES（Data Encryption Standard）、3DES（トリプル DES）、および AES（Advanced Encryption Standard）に代わるアルゴリズムです。SEAL 暗号化では、160 ビットの暗号キーが使用され、他のソフトウェアベースのアルゴリズムを使用する場合よりも CPU に与える影響は小さくなります。

ESP 整合性

使用されている整合性アルゴリズムを示します。このカラムに値が表示されるのは、データの整合性と暗号化の両方を提供するようにトランスフォーム セットが設定されている場合です。このカラムには、次のいずれかの値が含まれます。

- ESP-MD5-HMAC — Message Digest 5 に基づく HMAC（ハッシュベースのメッセージ認証コード）を使用する ESP。
- ESP-SHA-HMAC — Security Hash Algorithm に基づく HMAC を使用する ESP。

AH 整合性

使用されている整合性アルゴリズムを示します。このカラムに値が表示されるのは、データの整合性を提供して暗号化を提供しないようにトランスフォーム セットが設定されている場合です。このカラムには、次のいずれかの値が含まれます。

- AH-MD5-HMAC — Message Digest 5 を使用する AH。
- AH-SHA-HMAC — Security Hash Algorithm を使用する AH。

IP 圧縮

IP データ圧縮が使用されるかどうかを示します。

（注） ルータで IP 圧縮がサポートされていない場合は、このボックスは無効になります。

モード

このカラムには、次のいずれかの値が含まれます。

- ［トンネル］— ヘッダーとデータの両方が暗号化されます。このモードは VPN 設定で使用されます。
- ［トランスポート］— データのみ暗号化されます。このモードは、暗号化のエンドポイントと通信のエンドポイントが同じ場合に使用されます。

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
ルータの設定に新しいトランスフォーム 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。
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。 **（注）** 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ません。
既存のトランスフォーム セットを削除する。	トランスフォーム セットを選択し、［削除］をクリックする。 **（注）** 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削除できません。

トランスフォーム セットの追加 / 編集

このウィンドウでは、トランスフォーム セットを追加または編集します。

許容されるトランスフォームの組み合わせおよびトランスフォームの説明については、「許容されるトランスフォームの組み合わせ」を参照してください。

（注）

- すべてのルータがすべてのトランスフォーム　セット（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トランスフォーム セットは、画面に表示されません。
- Cisco CP がサポートしているすべてのトランスフォーム セットをすべての IOS イメージがサポートしているわけではありません。IOS イメージでサポートされていないトランスフォーム セットは、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と IOS イメージの両方でサポートされているトランスフォーム セットだけが画面に表示されます。
- Easy VPN サーバでは、トンネル モードのみサポートされています。トランスポート モードはサポートされていません。
- Easy VPN サーバでは、ESP 暗号化を使用するトランスフォーム セットのみサポートされています。AH アルゴリズムはサポートされていません。
- Easy VPN サーバでは、ESP-SEAL 暗号化はサポートされていません。

このトランスフォーム セットの名前

どのような名前でも指定できます。この名前は、ピアが使用するトランスフォーム セットの名前と一致する必要はありませんが、同じ名前にしておくと便利です。

データ整合性と暗号化（ESP）

ESP（Encapsulating Security Payload）のデータ整合性と暗号化を提供する場合に選択します。

整合性アルゴリズム

次のいずれかを選択します。

- ［ESP_MD5_HMAC］。Message Digest 5 を使用する ESP
- ［ESP_SHA_HMAC］Security Hash Algorithm を使用する ESP

暗号化

Cisco CP では、次の ESP 暗号化タイプが認識されます。

- ESP_DES。DES（Data Encryption Standard）を使用する ESP（Encapsulating Security Payload）。DES は、56 ビットの暗号化をサポートします。
- ESP_3DES。トリプル DES を使用する ESP。これは、DES よりも強力な暗号形式で、168 ビットの暗号化をサポートします。
- ESP_AES_128。AES（Advanced Encryption Standard）を使用する ESP。暗号化には 128 ビットのキーが使用されます。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。
- ESP_AES_192。192 ビット キーの AES 暗号化を使用する ESP。
- ESP_AES_256。256 ビット キーの AES 暗号化を使用する ESP。
- ESP_SEAL。160 ビット暗号キーに基づく Software Encryption Algorithm（SEAL）暗号化アルゴリズムを使用する ESP。SEAL（Software Encryption Algorithm）は、ソフトウェアベースの DES（Data Encryption Standard）、3DES（トリプル DES）、および AES（Advanced Encryption Standard）に代わるアルゴリズムです。SEAL 暗号化では、160 ビットの暗号キーが使用され、他のソフトウェアベースのアルゴリズムを使用する場合よりも CPU に与える影響は小さくなります。
- ESP_NULL。Null 暗号化アルゴリズム。ただし、暗号化トランスフォームが使用されます。

（注） 使用可能な ESP 暗号化タイプは、ルータによって異なります。設定するルータのタイプによっては、これらのタイプの 1 つ以上が使用できない場合があります。

暗号化なしのデータとアドレスの整合性（AH）

［詳細の表示］をクリックすると、このチェック ボックスとその下のフィールドが表示されます。

ルータで AH（認証ヘッダー）データとアドレスの整合性を提供する場合に選択します。認証ヘッダーは暗号化されません。

整合性アルゴリズム

次のいずれかを選択します。

- ［AH_MD5_HMAC］— Message Digest 5 を使用する AH。
- ［AH_SHA_HMAC］— Security Hash Algorithm を使用する AH。

モード

暗号化するトラフィック部分を選択します。

- ［トランスポート（データのみ暗号化）］— 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、オリジナルの IP ヘッダーの後に AH または ESP 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。トランスポート モードは、データの宛先が常にリモート VPN ピアである場合のみ使用してください。
- ［トンネル（データと IP ヘッダーの暗号化）］— トンネル モードでは、トランスポート モードより強力な防御ができます。IP パケット全体を AH または ESP 内にカプセル化するので、新しい IP ヘッダーを添付して、データグラム全体をカプセル化できます。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。このモードはそのような設定でのみ使用してください。

IP 圧縮（COMP-LZS）

データ圧縮を使用する場合に選択します。

（注）　IP 圧縮をサポートしていないルータもあります。ルータで IP 圧縮がサポートされていない場合は、このボックスは無効になります。

IPSec ルール

このウィンドウには、このルータに設定されている IPSec ルールが表示されます。IPSec ルールでは、IPSec で暗号化するトラフィックを定義します。ウィンドウの上部には、定義されているアクセス ルールのリストが表示されます。下の部分には、ルール リストで選択されているアクセス ルールのエントリが表示されます。

IPSec ルールには、IP アドレスとサービスタイプ情報が含まれます。ルールで指定された条件に一致するパケットは暗号化されます。条件に一致しないパケットは暗号化されません。

名前 / 番号

このルールの名前または番号です。

使用元

このルールが使用される暗号マップです。

タイプ

IPSec ルールでは、送信元と宛先の両方を指定する必要があり、パケットに含まれているトラフィック タイプも指定できなければなりません。したがって、IPSec ルールは拡張ルールです。

説明

ルールの説明が入力されている場合はそれが表示されます。

アクション

［許可］または［拒否］のいずれかになります。［許可］の場合、このルールの条件に一致するパケットは暗号化によって保護されます。［拒否］の場合、条件に一致しないパケットは暗号化されません。詳細については、「キーワード「許可」と「拒否」の意味」を参照してください。

送信元

トラフィックの送信元を示す IP アドレスまたはキーワードです。any は、送信元がどのような IP アドレスでもよいことを示します。このカラムには、IP アドレスだけが表示されることもあれば、後ろにワイルドカード マスクが表示されることもあります。ワイルドカード マスクは、送信元 IP アドレスが一致しなければならない IP アドレス部分を示します。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。

宛先

トラフィックの宛先を示す IP アドレスまたはキーワードです。any は、宛先がどのような IP アドレスでもよいことを示します。このカラムには、IP アドレスだけが表示されることもあれば、後ろにワイルドカード マスクが表示されることもあります。ワイルドカード マスクは、宛先 IP アドレスが一致しなければならない IP アドレス部分を示します。

サービス

パケットに含まれなければならないトラフィックのタイプです。

実行する操作

目的	手順
特定のルールのアクセス ルール エントリを表示する。	ルール リストからルールを選択する。そのルールのエントリが下のボックスに表示される。
IPSec ルールを追加する。	［追加］をクリックし、表示されたルール ウィンドウでルールを作成する。
IPSec ルールを削除する。	ルール リストでルールを選択して［削除］をクリックする。
特定のルール エントリを削除する。	ルール リストでルールを選択して［編集］をクリックする。表示されたルール ウィンドウでエントリを削除する。
インターフェイスに IPSec ルールを適用する。	［インターフェイス設定］ウィンドウでルールを適用する。