RV180 および RV180W の VPN ポリシー 設定

目的

この資料は Cisco スモール ビジネス RV180 および RV180W VPN ファイアウォールの VPN ポリシーを設定 するためにプロシージャを展示したものです。

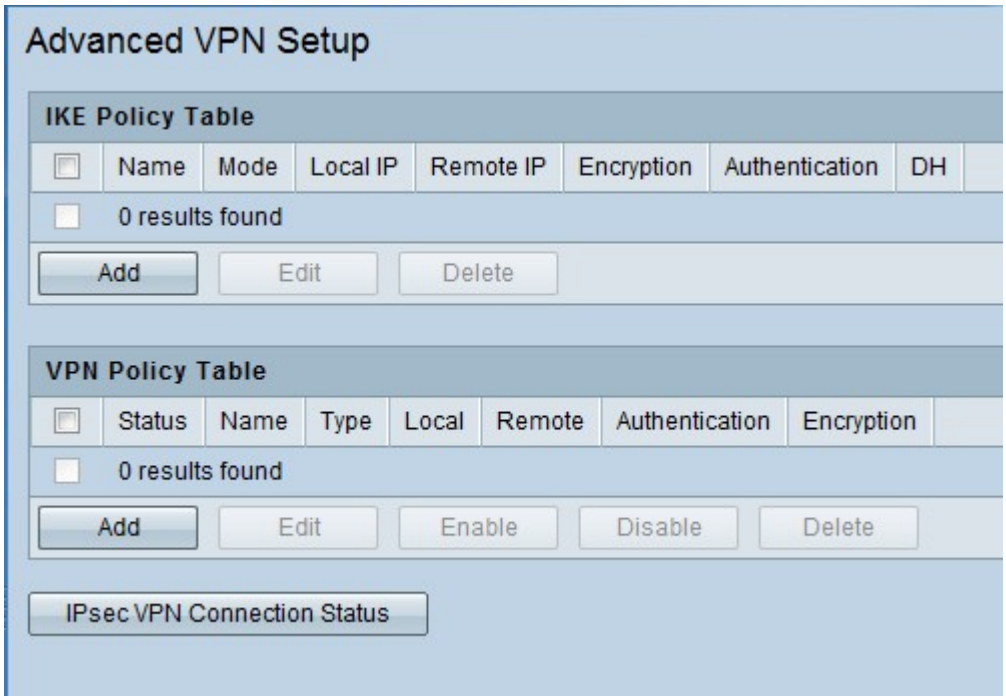
VPN ポリシー機能は自動ポリシーの VPN 設定を、手動ポリシーおよび暗号化および統合アルゴリズム行うことを可能にします。

適当なデバイス

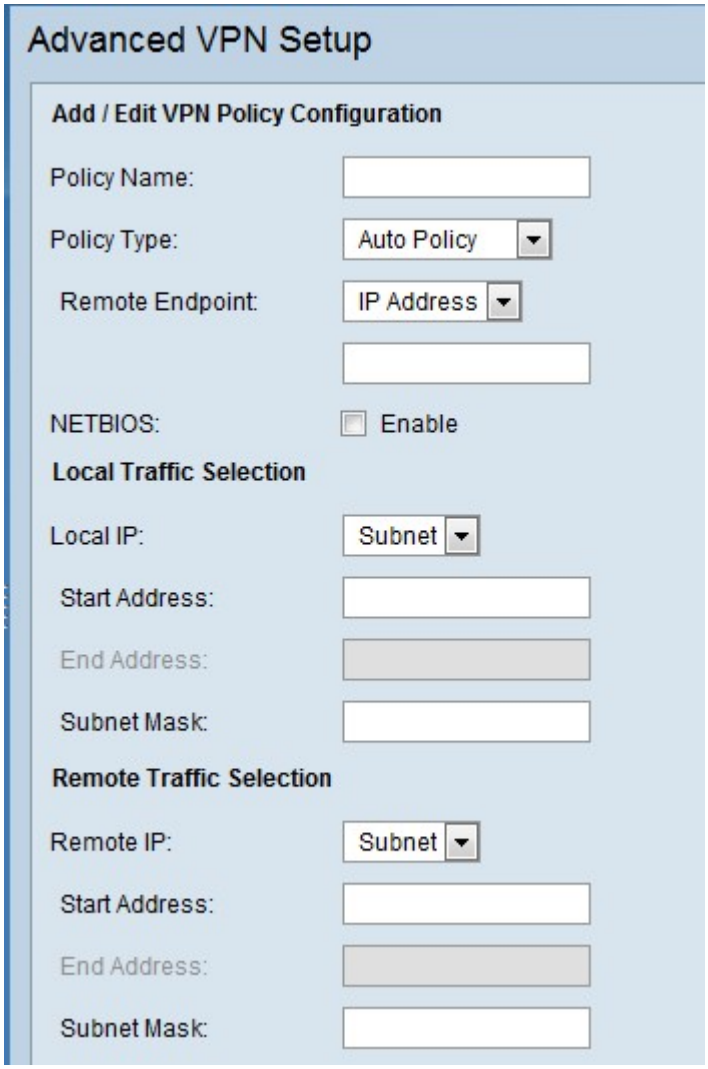
- RV180
- RV180W

VPN ポリシー 設定

ステップ 1： コンフィギュレーションユーティリティを使用する、**> IPSec > 進めました VPN のセットアップを**『VPN』 を選択 して下さい。 *高度 VPN のセットアップ* ページは開きます。



呼び出します。 VPN ポリシー 表 セクションで、『Add』 をクリック して下さい。



ステップ 3.固有の名前をです設定 されるべきポリシーのための Policy Name フィールド入力して下さい。

ステップ 4.**ポリシーの種類**ドロップダウン リストから適切なポリシーの種類を選択して下さい。

- オートは policy — パラメータ自動的に設定できます。 この場合 IKE （ Internet Key Exchange （ IKE ））プロトコルが 2 つの VPN エンドポイントの間でネゴシエートすることがポリシーに加えて必要となります。

- マニュアル policy —この場合 VPN のキーの設定が含まれているすべての設定が各エンドポイントのために手動で入力されるトンネル伝送する。

ステップ 5.**リモートエンドポイント** ドロップダウン リストからのリモートエンドポイントでゲートウェイを識別する IP 識別子の種類を選択して下さい。

- ip address — リモートエンドポイントのゲートウェイの IP アドレス。
- FQDN （ 完全修飾ドメイン ネーム ） — remore エンドポイントのゲートウェイの完全修飾ドメイン ネームを挿入して下さい。

ステップ 6 NetBIOS ブロードキャストが VPN を渡って移動することを可能にするために **Enable チェックボックスを**トンネル伝送して下さい、チェックして下さい。

ローカル トラフィック選択およびリモート トラフィック選択

ステップ 1： 両方のエリアに関しては次の設定を行って下さい:

• ローカル/リモートIP —エンドポイントに提供したいと思う識別子の種類を選択して下さい:

• これがトラフィックを規定 するどの-でもある特定のエンドポイントからあります（ローカルか遠隔）。 両方とも選択することができません。
• 単一-は 1 ホストにこれポリシーを制限します。開始する IP address フィールドの VPN の一部であるホストの IP アドレスを挿入して下さい。
• 範囲-はこれ指定IPアドレス 範囲内のコンピュータが VPN に接続するようにします。開始する IP アドレスを挿入し、適切なフィールドの IP アドレスを終了して下さい。
• これが IPアドレス範囲内のコンピュータが VPN に接続するようにする-をサブネット化して下さい。 開始する IP アドレスを挿入し、適切なフィールドの IP アドレスを終了して下さい。 またサブネット マスク フィールドでネットワークのサブネット マスクを挿入して下さい。

スプリット DNS

分割DNS は RV120W がインターネットを通過しないでリモート エンドポイントの DNS を得るようにします。

ステップ 1： 分割DNS を有効に するために **Enable チェックボックスを**チェックして下さい。

呼び出します。 Domain Name Server 1 フィールドでは、Domain Name Server IP アドレスを挿入して下さい。 この IP アドレスがドメイン名 1 フィールドで挿入されたドメインしか解決しないのに使用されます。

ステップ 3 Domain Name Server 2 フィールドでは、Domain Name Server IP アドレスを挿入して下さい。 この IP アドレスがドメイン名 2 フィールドで挿入されたドメインしか解決しないのに使用されます。

手動ポリシー パラメータ

ステップ 1. SPI 着信および SPI 発信フィールドで 3 と 8 間の 16進値を挿入して下さい。

ステップ 2.**暗号化アルゴリズム** ドロップダウン リストから適切な暗号化アルゴリズムを選択して下さい。

ステップ 3. SPI 着信および SPI 発信フィールドで 3 と 8 間の 16進値を挿入して下さい。

ステップ 4.フィールド キーのでインバウンドポリシーの暗号化キーを挿入して下さい。

ステップ 5.キー フィールドでアウトバウンドポリシーの暗号化キーを挿入して下さい。

ステップ 6.**統合 アルゴリズム** ドロップダウン リストから適切な統合 アルゴリズムを選択して下さい。 このアルゴリズムはデータの統合を検証します。

ステップ 7.フィールド キーのでインバウンドポリシーの統合 キーを挿入して下さい。

ステップ 8.キー フィールドでアウトバウンドポリシーの統合 キーを挿入して下さい。

オート ポリシー パラメータ

ステップ 1： SA ライフタイム フィールドでセキュリティ結合の期間に入って下さい。 ド

ロップダウン リストの SA ライフタイム フィールドのための適切なユニットを選択して下さい。

- 秒—デフォルト値は 3600 秒です。 最小値は 300 秒です。
- K バイト—このフィールドの K バイトのある値の後で SA は再取り決めされます。最小値は 1920000 KB です。

ステップ 2.**暗号化アルゴリズム** ドロップダウン リストから適切な暗号化アルゴリズムを選択して下さい。

ステップ 3.**統合 アルゴリズム** ドロップダウン リストから適切な統合 アルゴリズムを選択して下さい。 このアルゴリズムはデータの統合を検証します。

ステップ 4 完全転送秘密がセキュリティを向上することを可能にするために **Enable チェックボックスを**チェックして下さい。 **PFS キー Group フィールド**から適切な Diffie-Hellmanキー交換を選択して下さい。 選択します。

ステップ 5. **『IKE』 を選択 ポリシー** ドロップダウン リストから適切な IKE ポリシーを選択して下さい。