ASA 8.x/ASDM 6.x：ASDM を使用した既存のサイト間 VPN での新しい VPN のピア情報の追加

内容

概要

このドキュメントでは、Adaptive Security Device Manager（ASDM）を使用して新しい VPN ピアを既存のサイト間 VPN 設定に追加する場合に行う設定変更について説明します。 これは次のようなシナリオで必要になります。

- インターネット サービス プロバイダー（ISP）が変更され、新しい一連のパブリック IP 範囲が使用される。
- サイトでのネットワークの完全な設計し直し。
- サイトの VPN ゲートウェイとして使用するデバイスを、パブリック IP アドレスが異なる新しいデバイスに移行する。

このドキュメントでは、サイト間 VPN がすでに正しく設定され、正常に機能していることを前提として、L2L VPN 設定で VPN ピア情報を変更するために実行すべき手順を示します。

前提条件

要件

次の項目に関する専門知識があることが推奨されます。

- ASA サイト間 VPN 設定の例

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア バージョン 8.2 以降がインストールされた Cisco Adapative Security Appliance 5500 シリーズ
- ソフトウェア バージョン 6.3 以降がインストールされた Cisco Adaptive Security Device Manager

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

サイト間 VPN が HQASA と BQASA 間で正常に機能しています。BQASA のネットワークが完全に再設計され、IP スキーマが ISP レベルで変更されたが、すべての内部サブネットワークの詳細は変更されていないものとします。

この設定例では、次の IP アドレスが使用されます。

- 既存の BQASA 外部 IP アドレス - 200.200.200.200
- 新しい BQASA 外部 IP アドレス - 209.165.201.2

注：ここでは、ピア情報だけが変更されます。内部サブネットに他の変更は行わないため、暗号アクセス リストは変わりません。

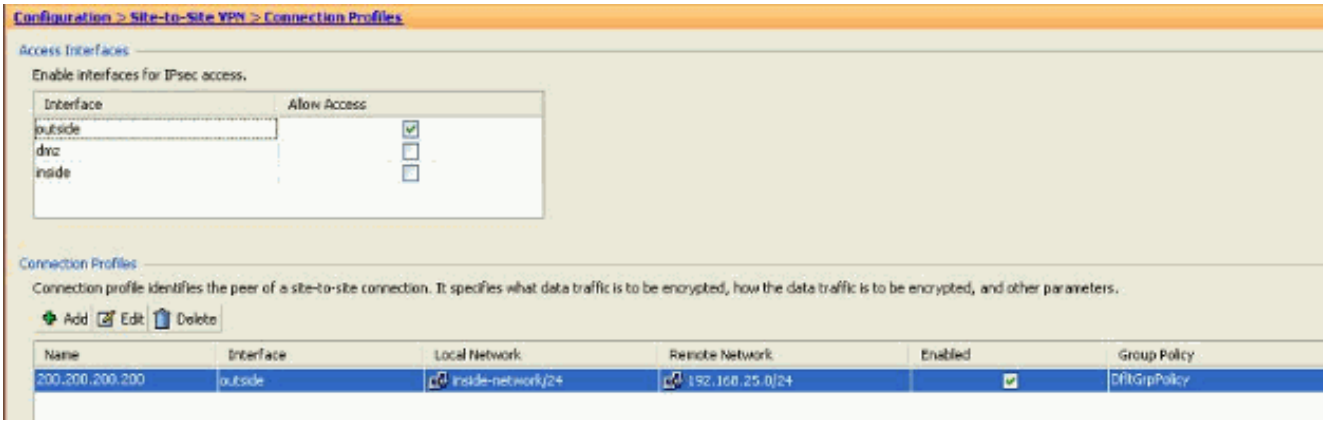
ASDM の設定

この項では、ASDM を使用して HQASA 上の VPN ピア情報を変更する方法について説明します。

新しい接続プロファイルの作成

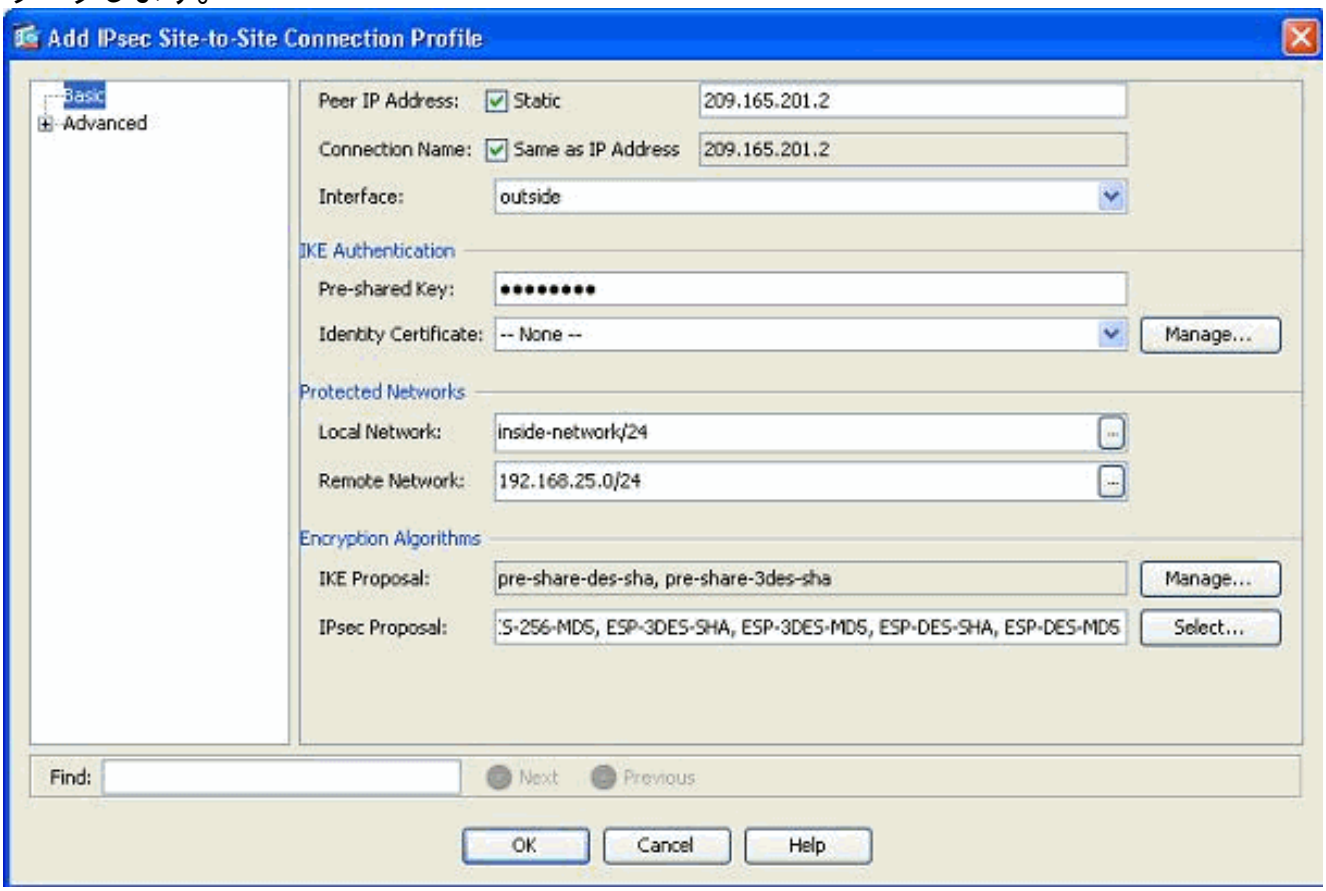
既存の VPN 設定に影響を与えず、新しい VPN ピア関連情報を使用して新しい接続プロファイルを作成できるため、この方法の方が簡単である場合があります。

1. [Configuration] > [Site-to-Site VPN] > [Connection Profiles] *に移動して、[Connection Profiles] 領域で [Add]* をクリックします。

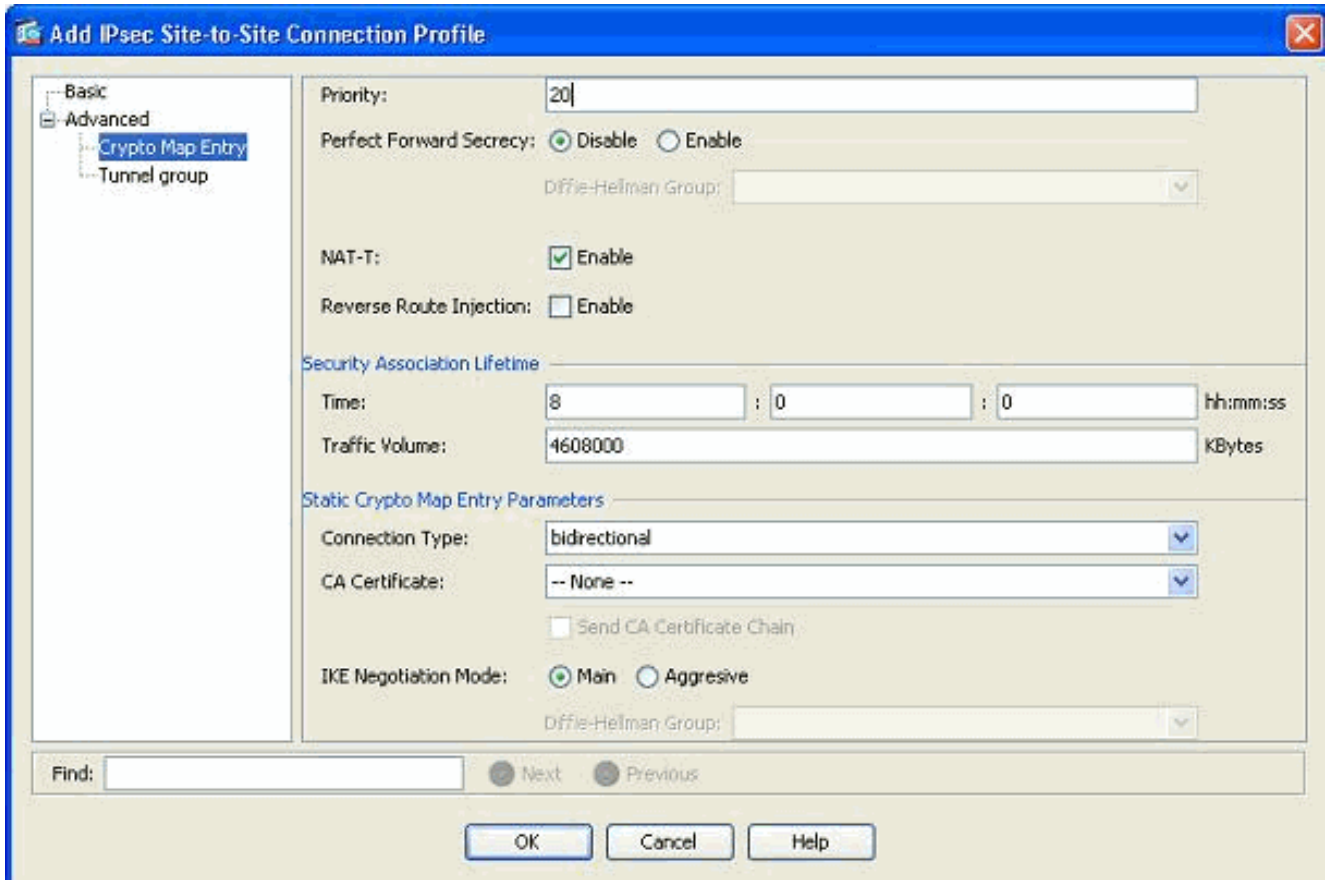


[Add IPsec Site-to-Site Connection Profile] *ウィンドウが表示されます。*

2. [Basic] タブで、[Peer IP Address]、[Pre-shared Key]、および [Protected Networks] の詳細を入力します。ピア情報を除いて、既存の VPN と同じパラメータを使用します。[OK] をクリックします。



3. [Advanced] メニューで、[Crypto Map Entry] をクリックします。[Priority] *タブを参照します*。このプライオリティは、対応する CLI 設定のシーケンス番号と同じです。既存の暗号マップ エントリより小さい番号が割り当てられている場合、この新しいプロファイルが最初に実行されます。プライオリティ番号が大きいほど、値は小さくなります。これは、特定の暗号マップが実行されるシーケンスの順序を変更するために使用されます。[OK] をクリックして、新しい接続プロファイルの作成を完了します。



これにより、関連する暗号マップとともに新しいトンネル グループが自動的に作成されます。この新しい接続プロファイルを使用する前に、新しい IP アドレスで BQASA に到達できることを確認してください。

既存の VPN 設定の編集

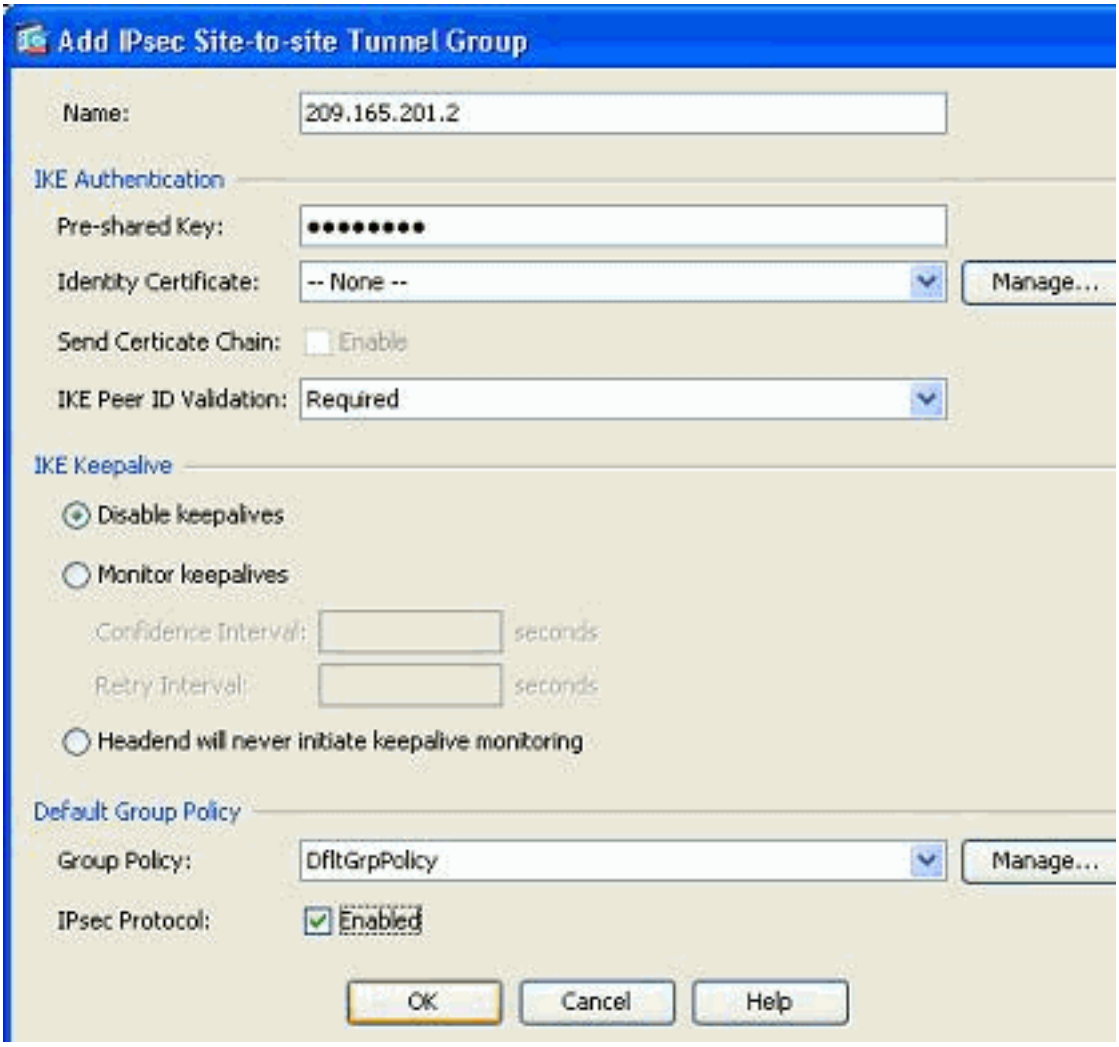
新しいピアを追加するもう 1 つの方法は、既存の設定を変更することです。既存の接続プロファイルは、特定のピアにバインドされているため、新しいピア情報に合わせて編集できません。既存の設定を編集するには、次の手順を実行する必要があります。

1. 新しいトンネル グループの作成
2. 既存の暗号マップの編集

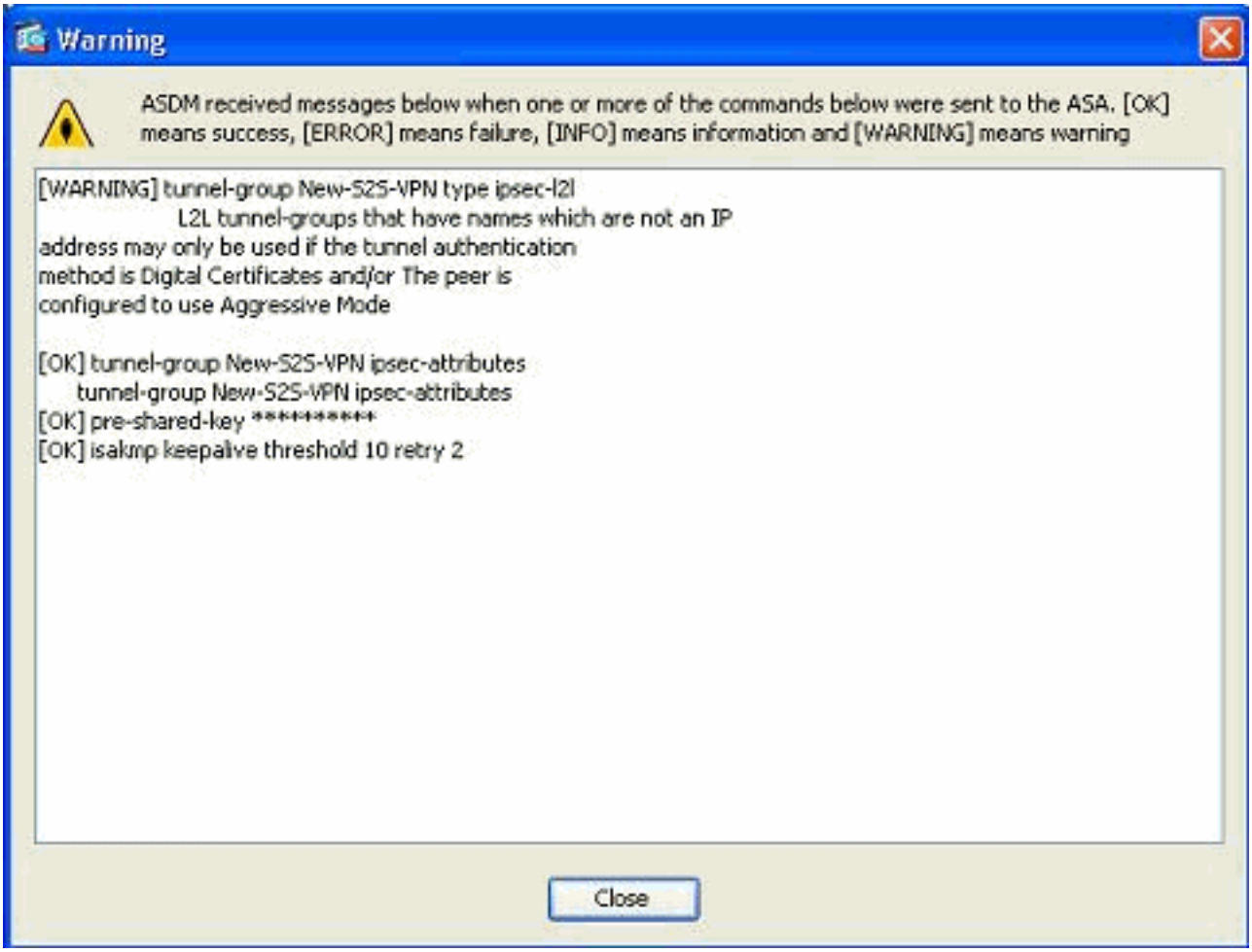
新しいトンネル グループの作成

[Configuration] > [Site-to-Site VPN] > [Advanced] > [Tunnel groups] *に移動して、[Add] をクリックし、*新しい VPN ピア情報を含む新しいトンネル グループを作成します。[Name] *フィールドと [Pre-Shared key] フィールドを指定してから、[OK] をクリックします。*

注：事前共有キーがVPNのもう一方の端と一致していることを確認します。



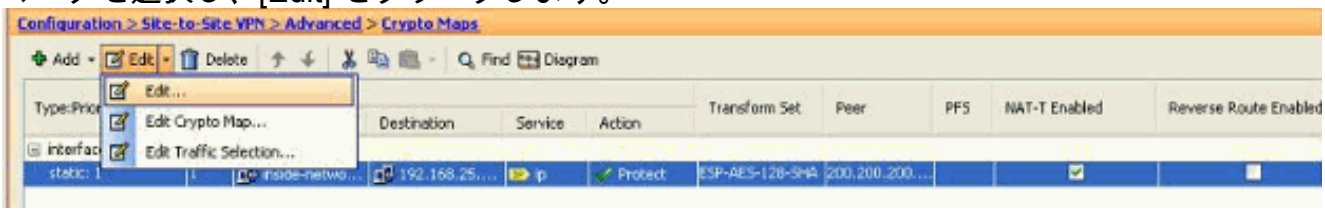
注：[Name]フィールドには、認証モードが事前共有キーの場合にリモートピアのIPアドレスだけを入力する必要があります。名前が使用できるのは、認証方式が証明書経由の場合だけです。[Name] フィールドに名前を追加して、認証方式が事前共有の場合は、次のエラーが表示されます。



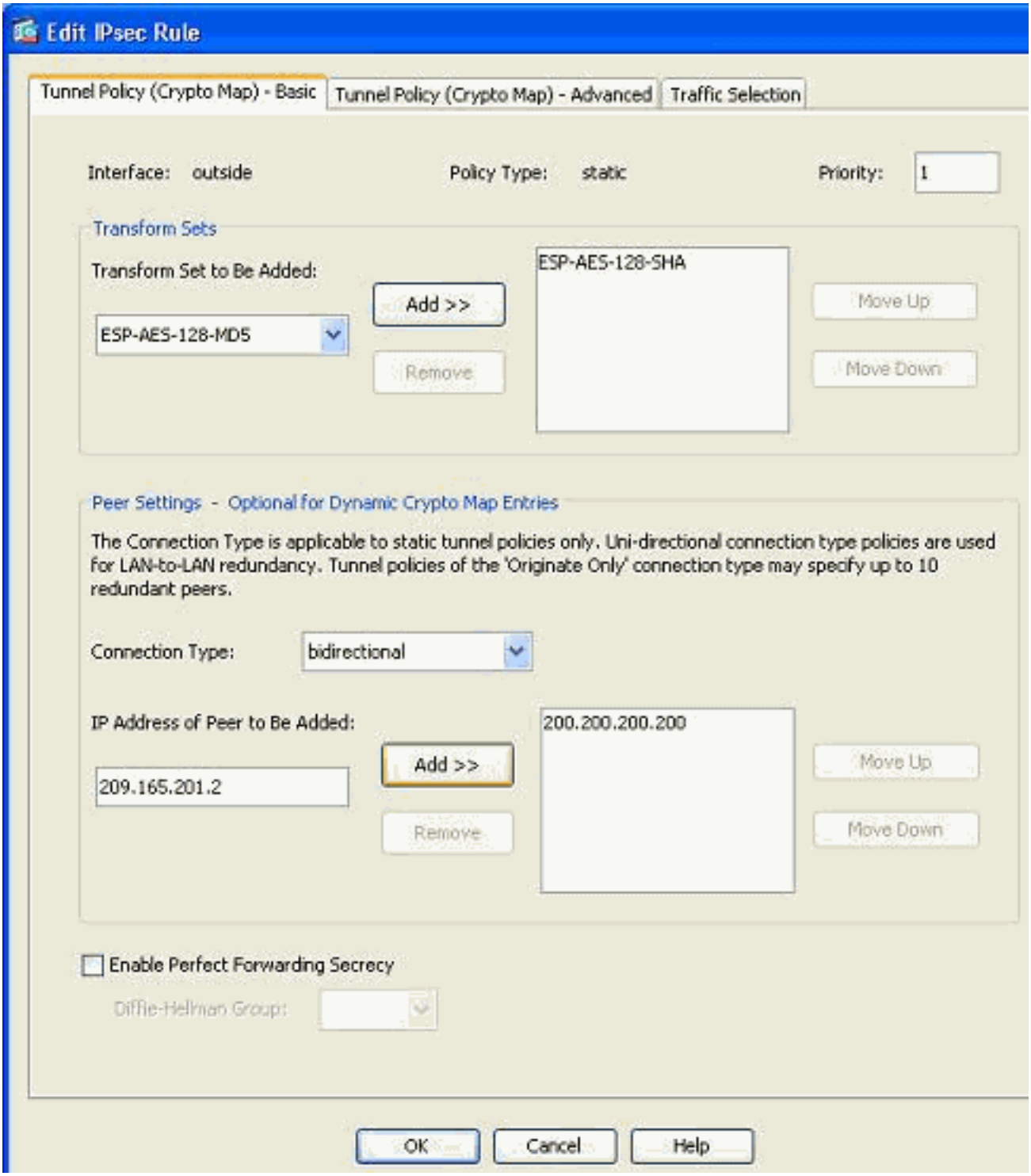
既存の暗号マップの編集

新しいピア情報を関連付けるために既存の暗号マップを編集することができます。

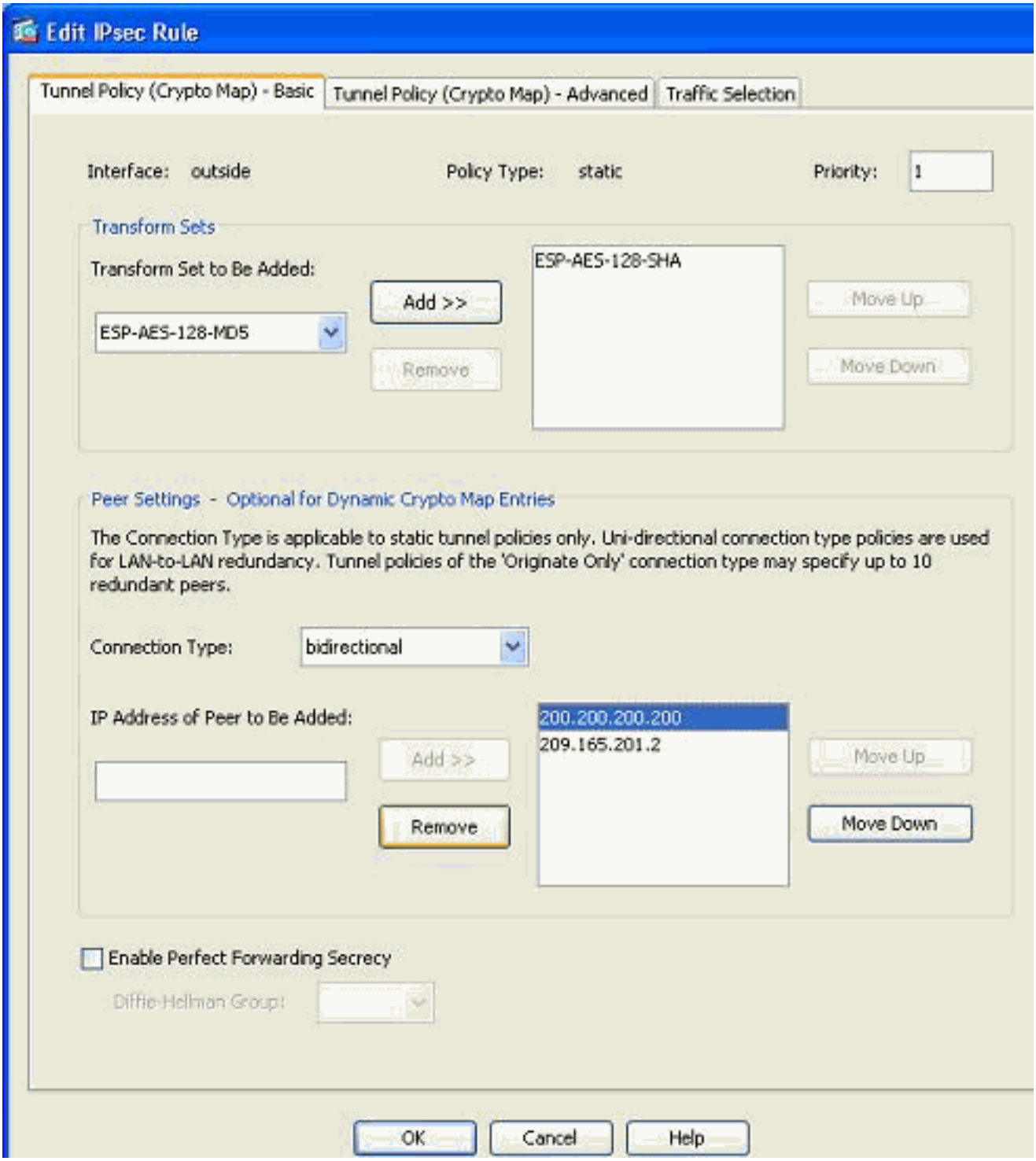
次のステップを実行します。

1. [Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps] に移動して、必要な暗号マップを選択し、[Edit] をクリックします。


[Edit IPSec Rule] *ウィンドウが表示されます。*
2. [Tunnel Policy (Basic)] タブの [Peer Settings] 領域にある [IP Address of Peer to be added] フィールドに新しいピアを指定します。次に、[Add] をクリックします。

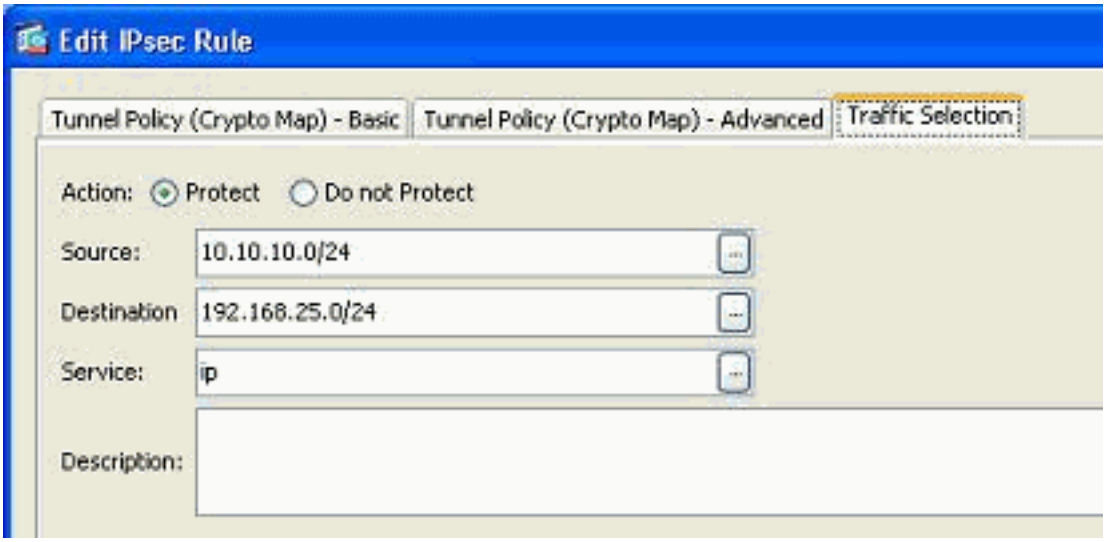


3. 既存のピア IP アドレスを選択して [Remove] をクリックし、新しいピア情報だけを残します。[OK] をクリックします。

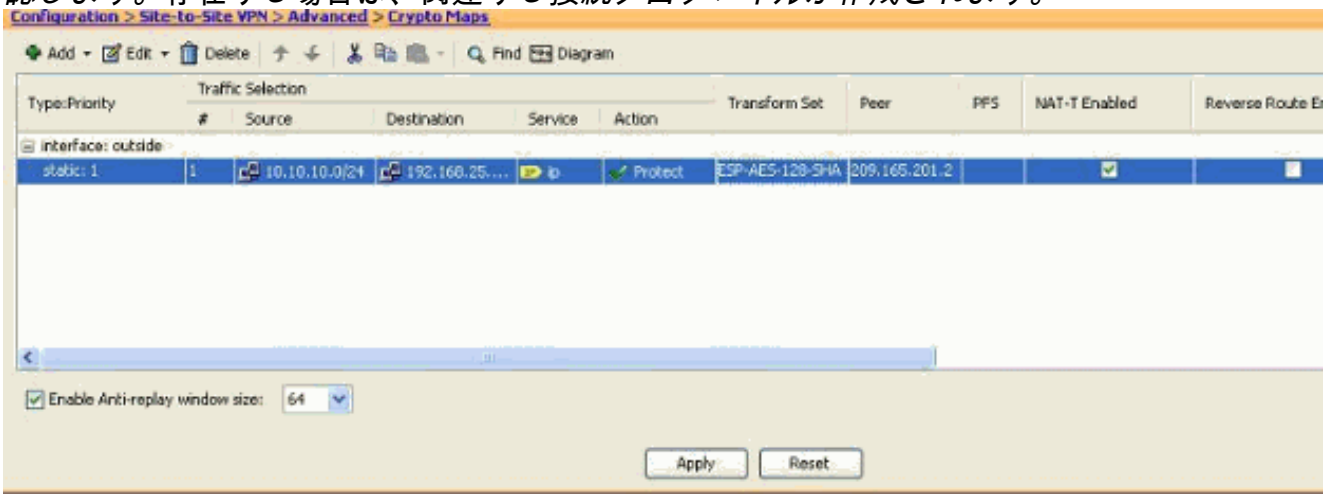


注：現在の暗号マップのピア情報を変更すると、この暗号マップに関連付けられている接続プロファイルがASDMウィンドウで即座に削除されます。

4. 暗号化されたネットワークの詳細は変わりません。これらを変更するには、[Traffic Selection] *タブに移動します。*



5. [Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps] *ペインに移動して、変更した暗号マップを確認します。ただし、これらの変更は* [Apply] をクリックするまで有効になりません。[Apply] *をクリックしたら、[Configuration] > [Site-to-Site VPN] > [Advanced] > [Tunnel groups] メニューに移動して、関連するトンネル グループが存在するかどうかを確認します。存在する場合は、関連する接続プロファイルが作成されます。*



確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- 単一のピアに固有のセキュリティ アソシエーション パラメータを表示するには、次のコマンドを使用します。show crypto ipsec sa peer <Peer IP address>

トラブルシュート

このセクションは、設定のトラブルシューティングを行う際に参照してください。

IKE Initiator unable to find policy:Intf test_ext, Src:172.16.1.103, Dst:10.1.4.251

VPN コンセントレータから ASA に VPN を変更しようとすると、次のエラーがログ メッセージ

に表示されます。

ソリューション：

これは、移行中に不適切な設定手順を実行したためである可能性があります。新しいピアを追加する前に、インターフェイスにバインドしている暗号が削除されていることを確認します。また、トンネル グループ内でピアの名前ではなく IP アドレスが使用されていることを確認します。

関連情報

- ASA とのサイト間（L2L）VPN
- 最も一般的な VPN の問題
- ASA テクニカル サポートページ
- テクニカル サポートとドキュメント – Cisco Systems