ASDM 6.4： IKEv2 を使用したサイト間 VPN トンネルの設定例

目次

概要

このドキュメントでは、インターネット キー交換（IKE）バージョン 2 を使用して 2 台の Cisco 適応型セキュリティ アプライアンス（ASA）間のサイト間 VPN トンネルを設定する方法について説明します。 Adaptive Security Device Manager（ASDM）GUI ウィザードを使用して、VPN トンネルを設定する場合に使用する手順について説明します。

前提条件

要件

Cisco ASA が基本設定で設定されていることを確認します。

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くものです。

- ソフトウェア バージョン 8.4 以降を実行する Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco ASDM ソフトウェア バージョン 6.4 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始して

います。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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

IKEv2 は、次のメリットを提供する既存の IKEv1 プロトコルの機能拡張です。

- IKE ピア間のメッセージ交換の低減
- 単方向認証方式
- デッド ピア検出（DPD）および NAT トラバーサルの組み込みサポート
- 認証用の拡張可能認証プロトコル（EAP）の使用
- クロッギング対策の cookie を使用した単純な DoS 攻撃リスクの排除

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

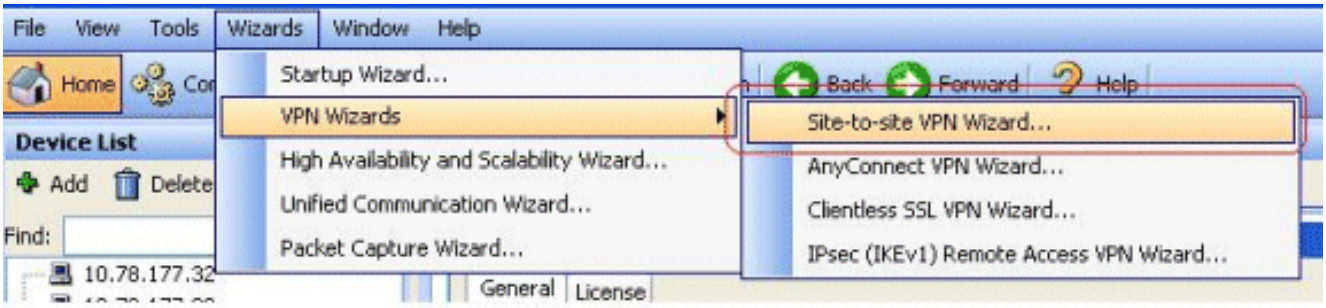
このドキュメントでは、HQ-ASA のサイト間 VPN トンネルの設定について説明します。 BQ-ASA のミラーの場合も同様です。

HQ-ASA での ASDM の設定

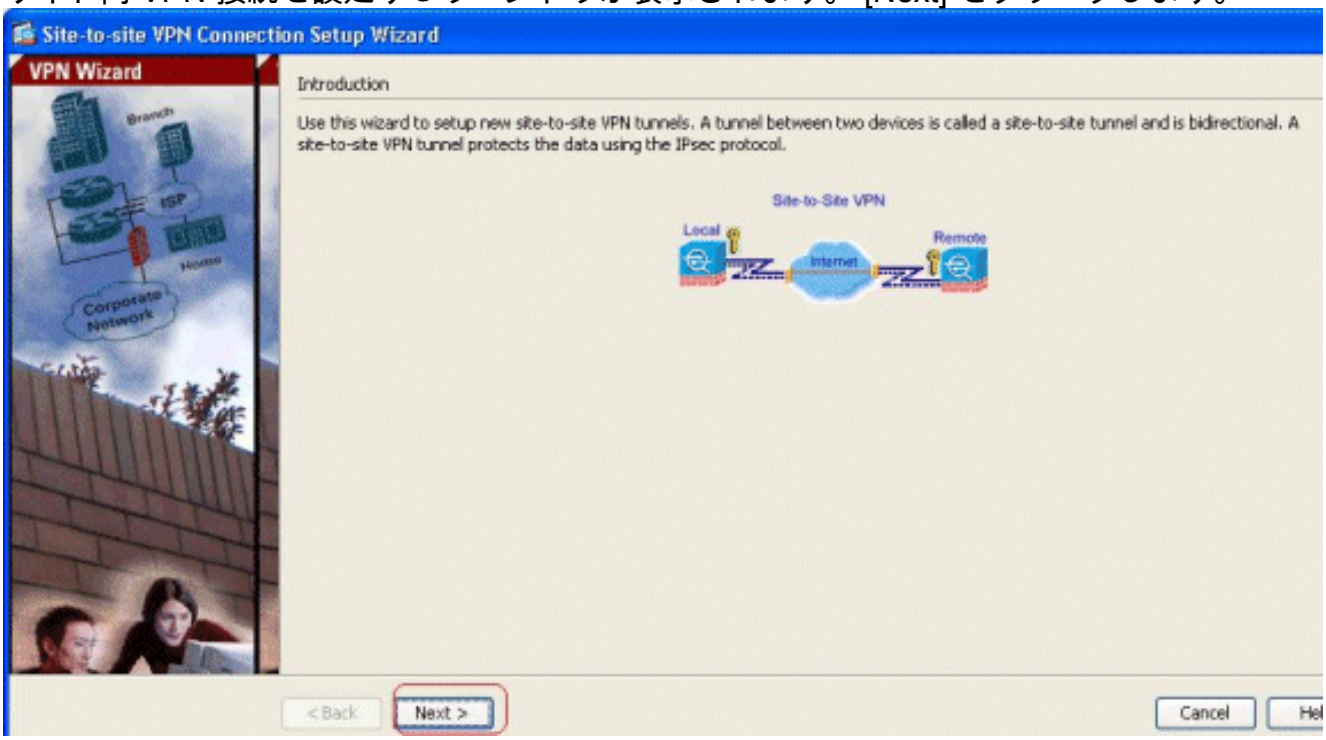
この VPN トンネルは、使いやすい GUI ウィザードを使用して設定できます。

次の手順を実行します。

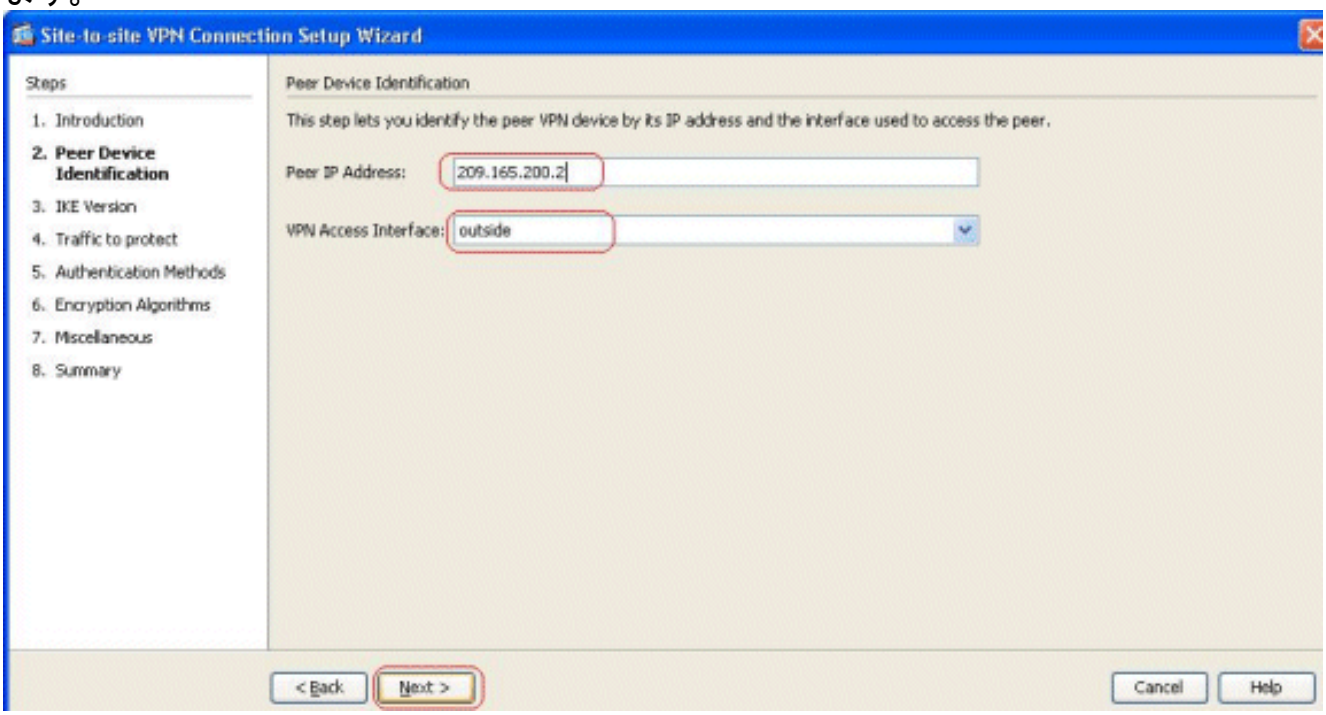
1. ASDM にログインし、[Wizards] > [VPN Wizards] > [Site-to-site VPN Wizard] の順に進みます。



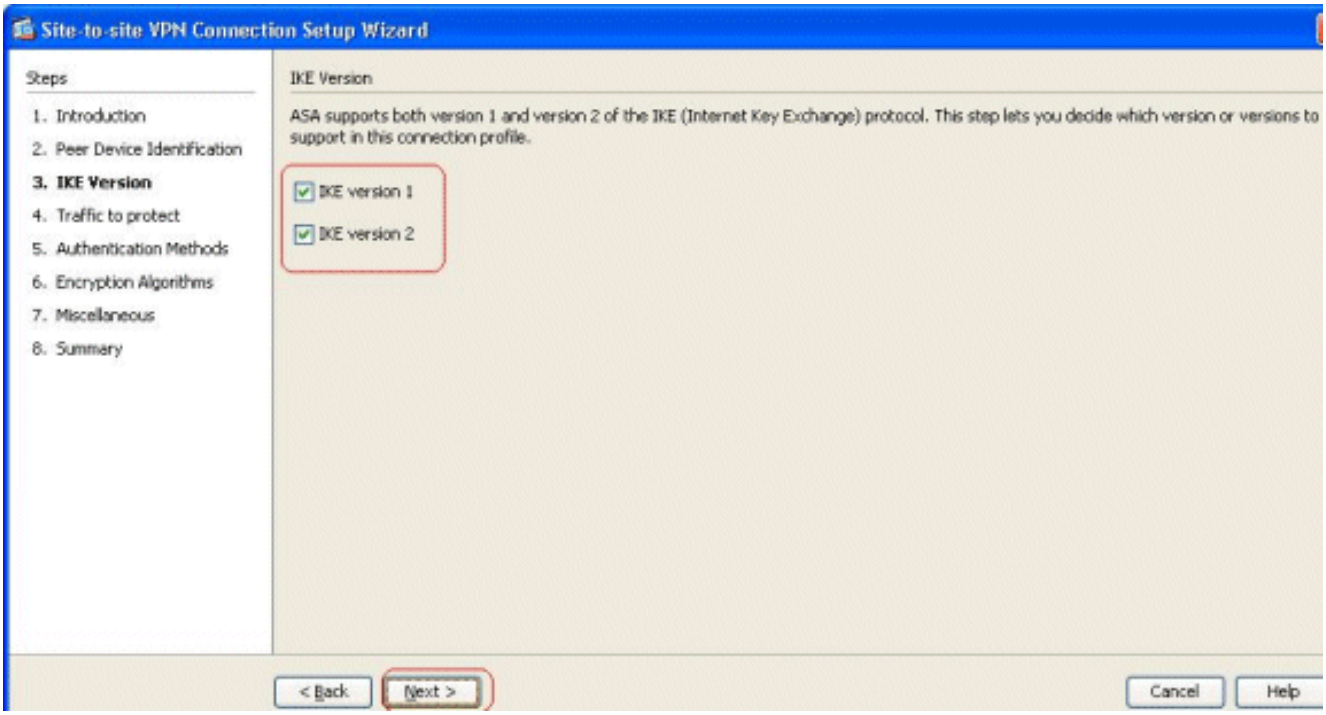
2. サイト間 VPN 接続を設定するウィンドウが表示されます。 [Next] をクリックします。



3. ピア IP アドレスと VPN のアクセス インターフェイスを指定します。 [Next] をクリックします。

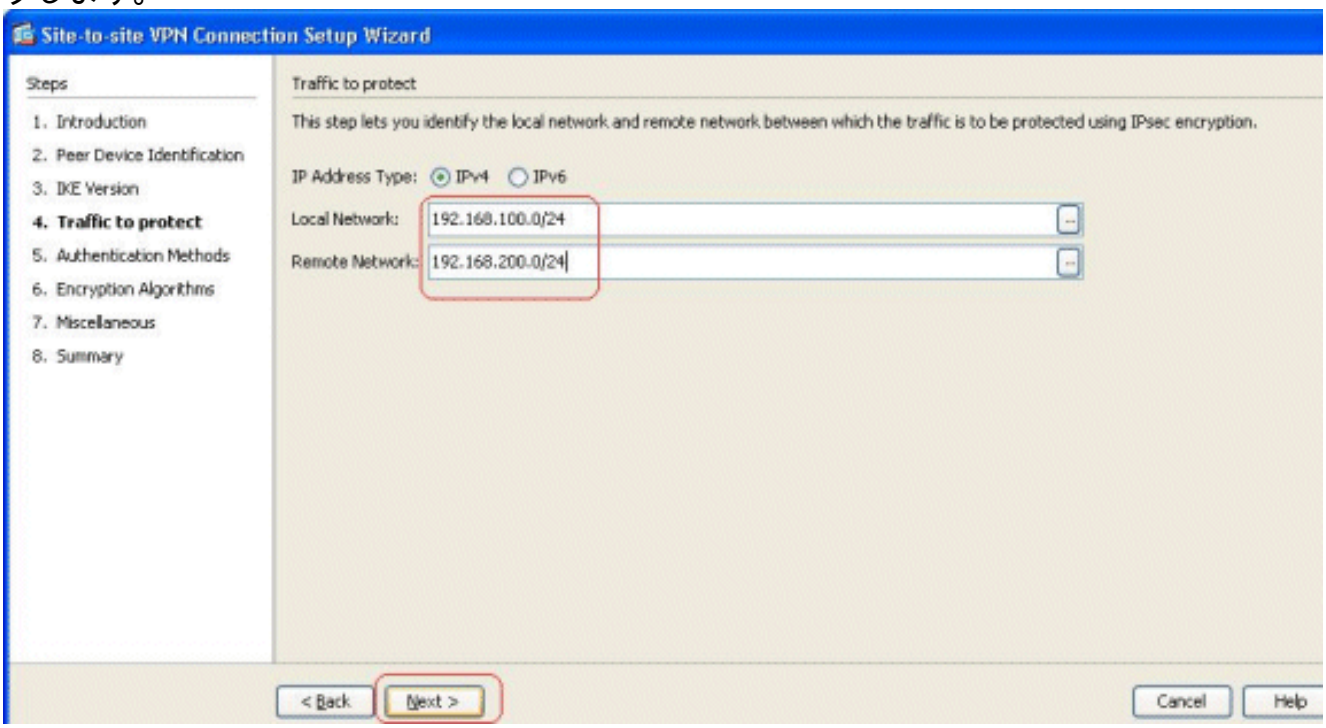


4. 両方の IKE バージョンを選択し、[Next] をクリックします。

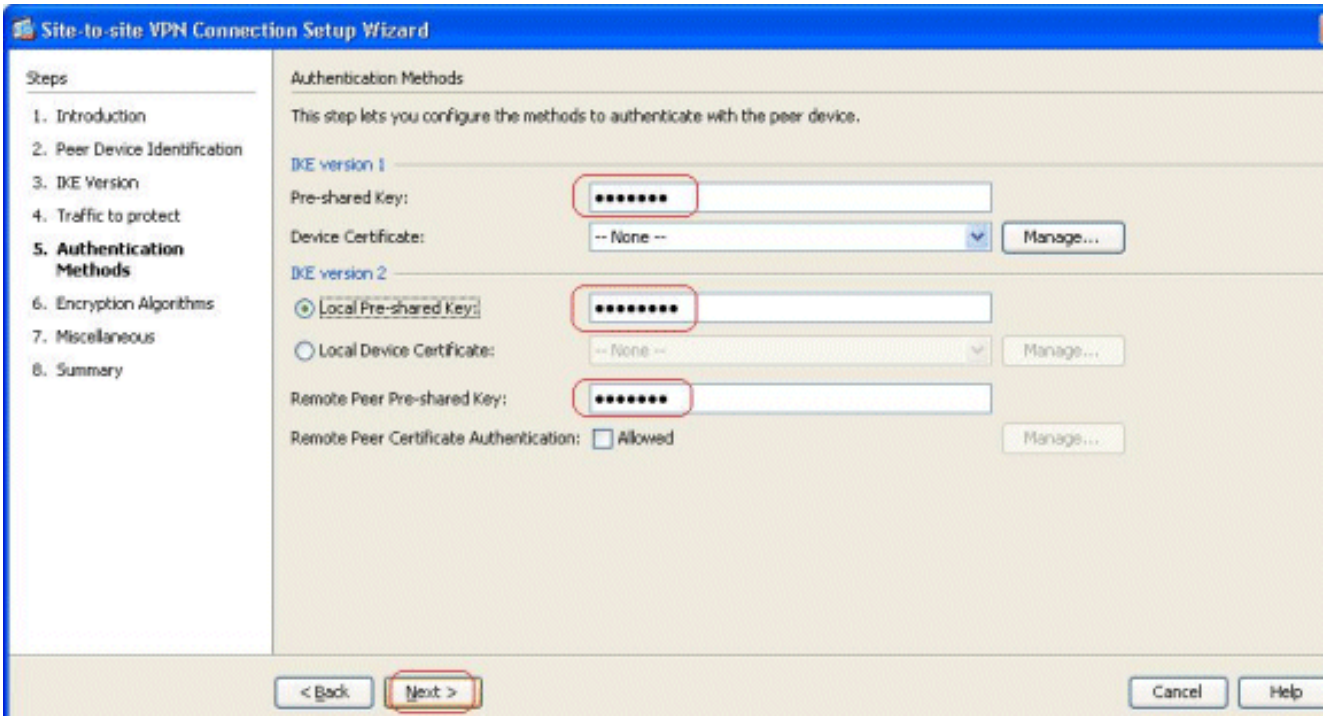


注: 両方のバージョンの IKE をここで設定し、IKEv2 が失敗した場合に発信側が IKEv2 から IKEv1 へバックアップできるようにします。

5. ローカル ネットワークとリモート ネットワークを指定して、これらのネットワーク間のトラフィックが暗号化され、VPN トンネルを通じて渡されるようにします。 [Next] をクリックします。

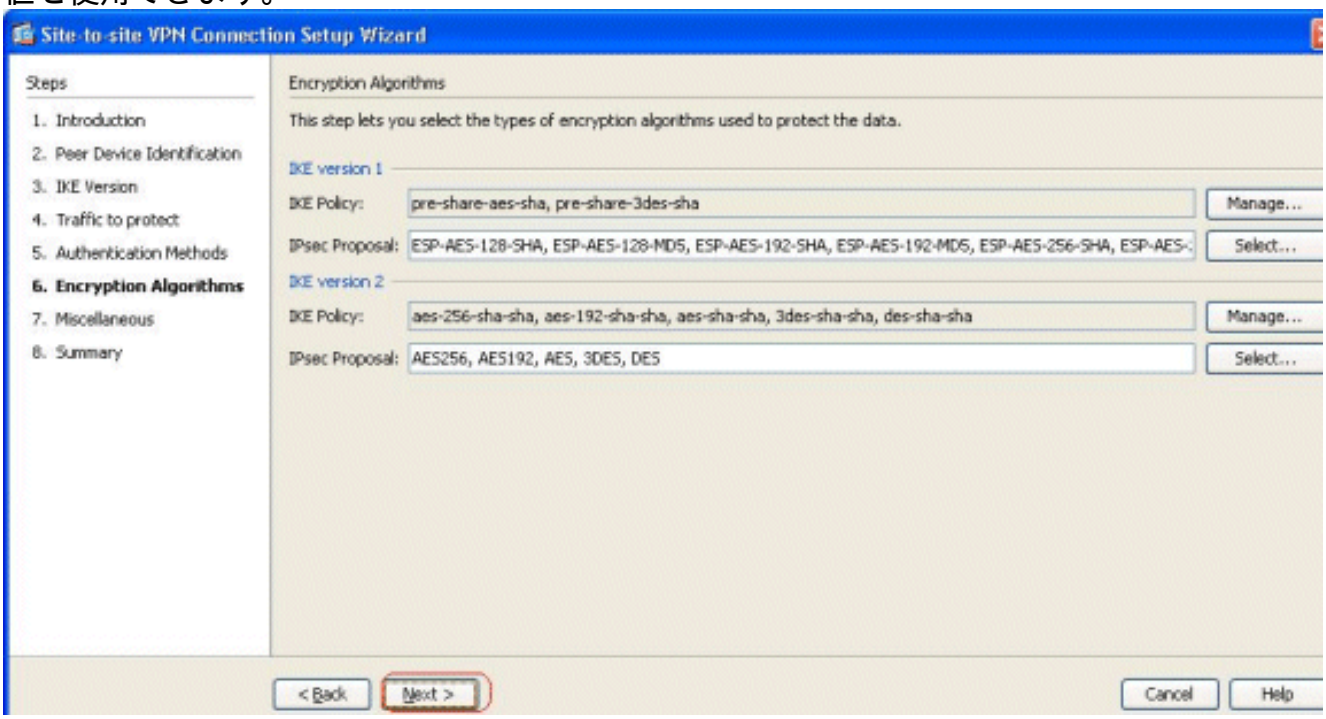


6. 両方のバージョンの IKE に事前共有キーを指定します。

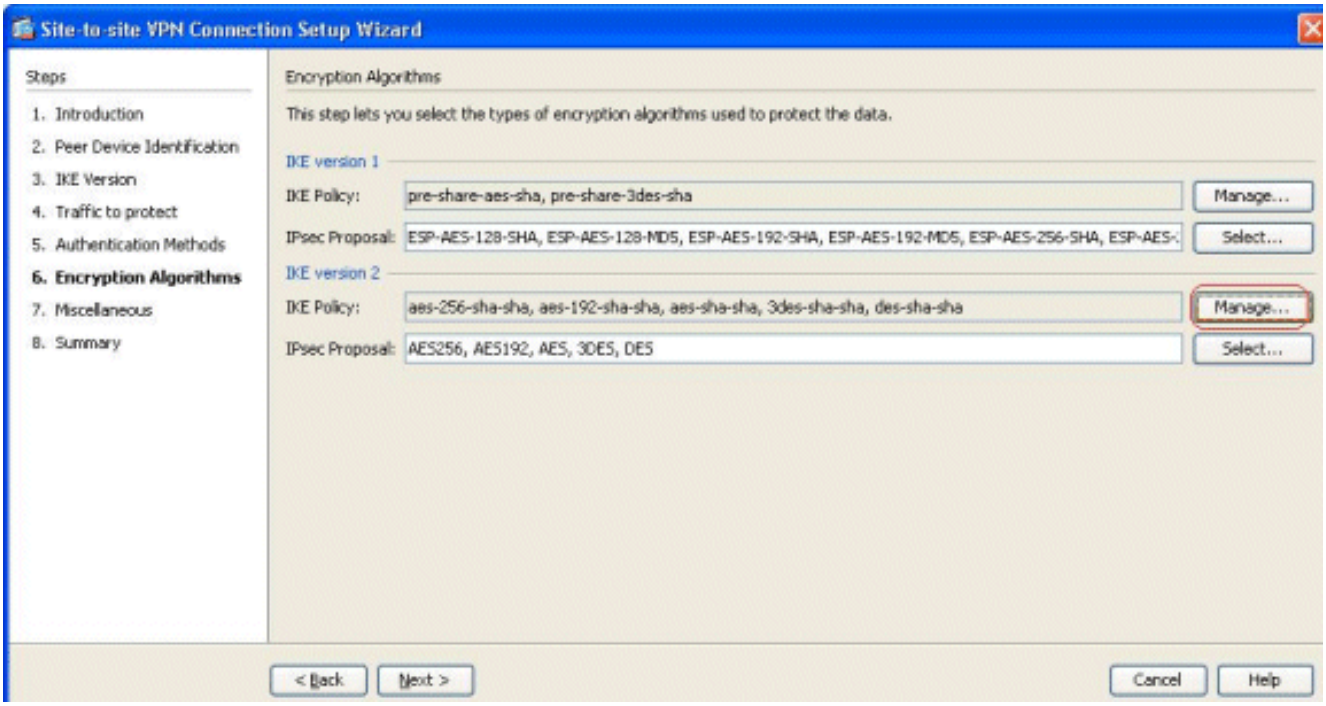


IKE のバージョン 1 と 2 の主な違いは、使用できる認証方式にあります。 IKEv1 では、両方の VPN エンドで 1 つのタイプの認証のみが許可されます (つまり、事前共有キーまたは証明書)。 しかし、IKEv2 では、それぞれローカルおよびリモート認証 CLI を使用して非対称認証方式を設定できます (つまり、発信側に対しては事前共有キー認証を設定し、応答側に対しては証明書認証を設定できます)。さらに、両側に異なる事前共有キーを設定できます。 HQ-ASA 側のローカル事前共有キーが BQ-ASA 側のリモート事前共有キーになります。 同様に、HQ-ASA 側のリモート事前共有キーが BQ-ASA 側のローカル事前共有キーになります。

7. IKE バージョン 1 と 2 の両方の暗号化アルゴリズムを指定します。 ここでは、デフォルト値を使用できます。



8. IKE ポリシーを変更するには、[Manage...] をクリックします。

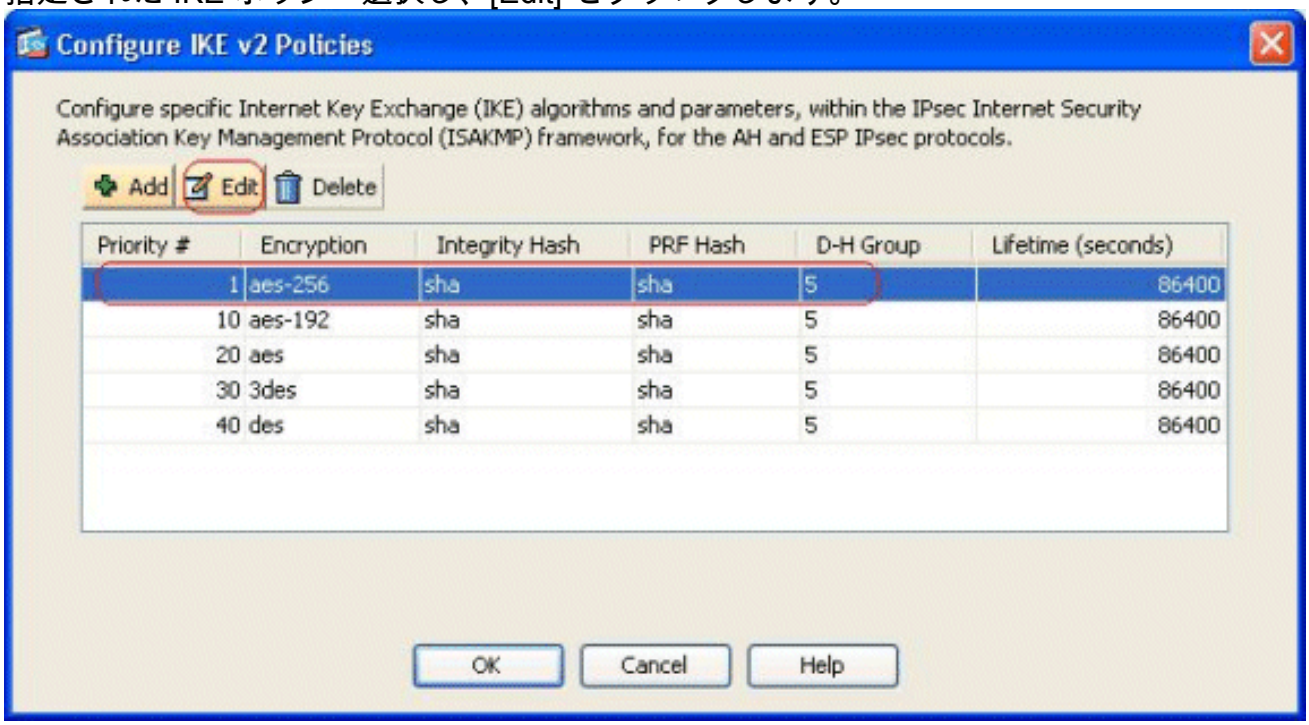


注: IKEv2 の **IKE ポリシー**は、IKEv1 の **ISAKMP ポリシー**と同義です。IKEv2 の **IPsec プロポーザル**は、IKEv1 の**トランスフォーム セット**と同義です。

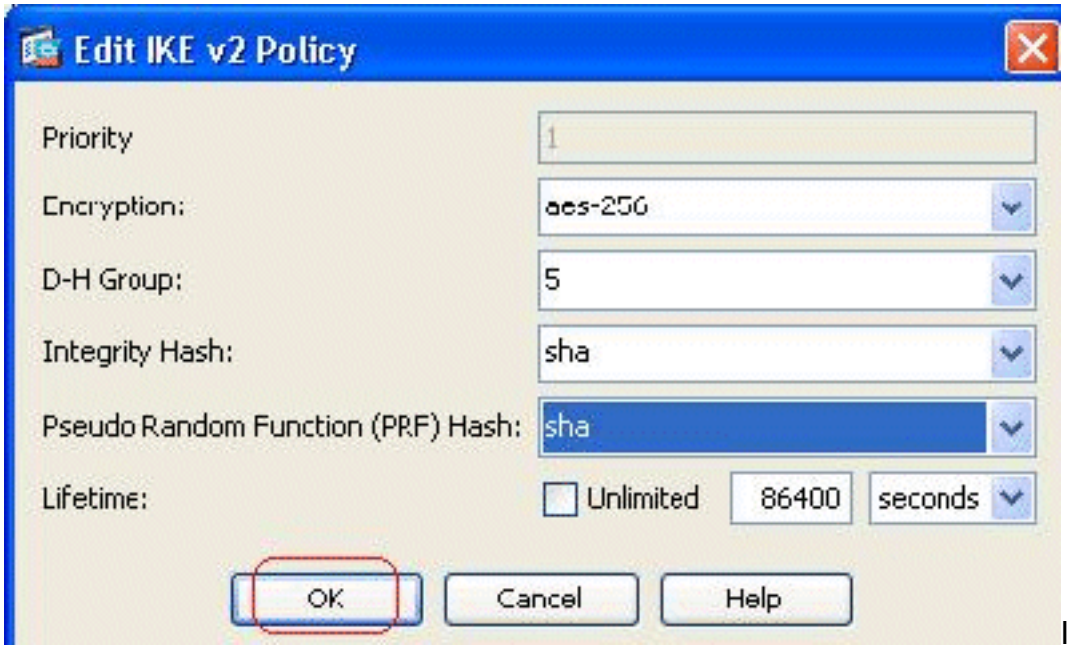
9. 既存のポリシーを変更しようとすると、次のメッセージが表示されます。

先に進むには、[OK] をクリックします。

10. 指定された IKE ポリシー選択し、[Edit] をクリックします。

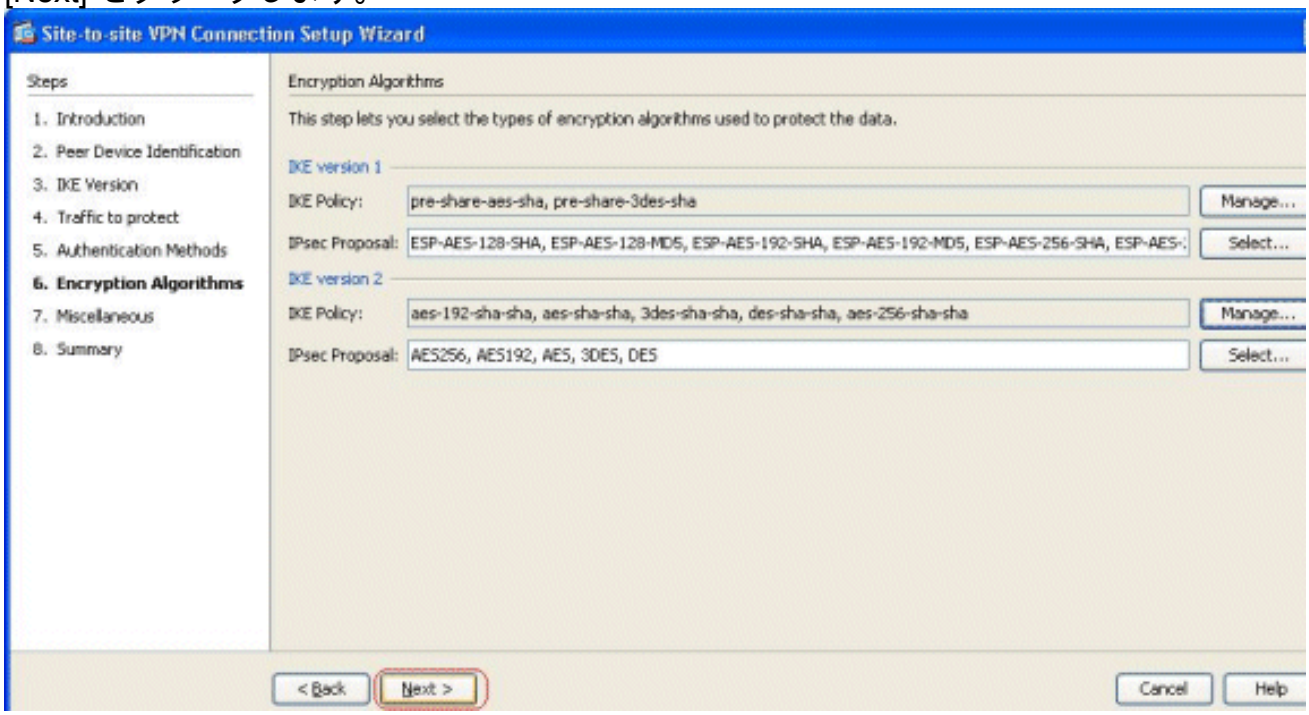


11. [Priority]、[Encryption]、[D-H Group]、[Integrity Hash]、[PRF Hash]、[Lifetime] の値などのパラメータを変更できます。 完了したら、[OK] をクリックします。

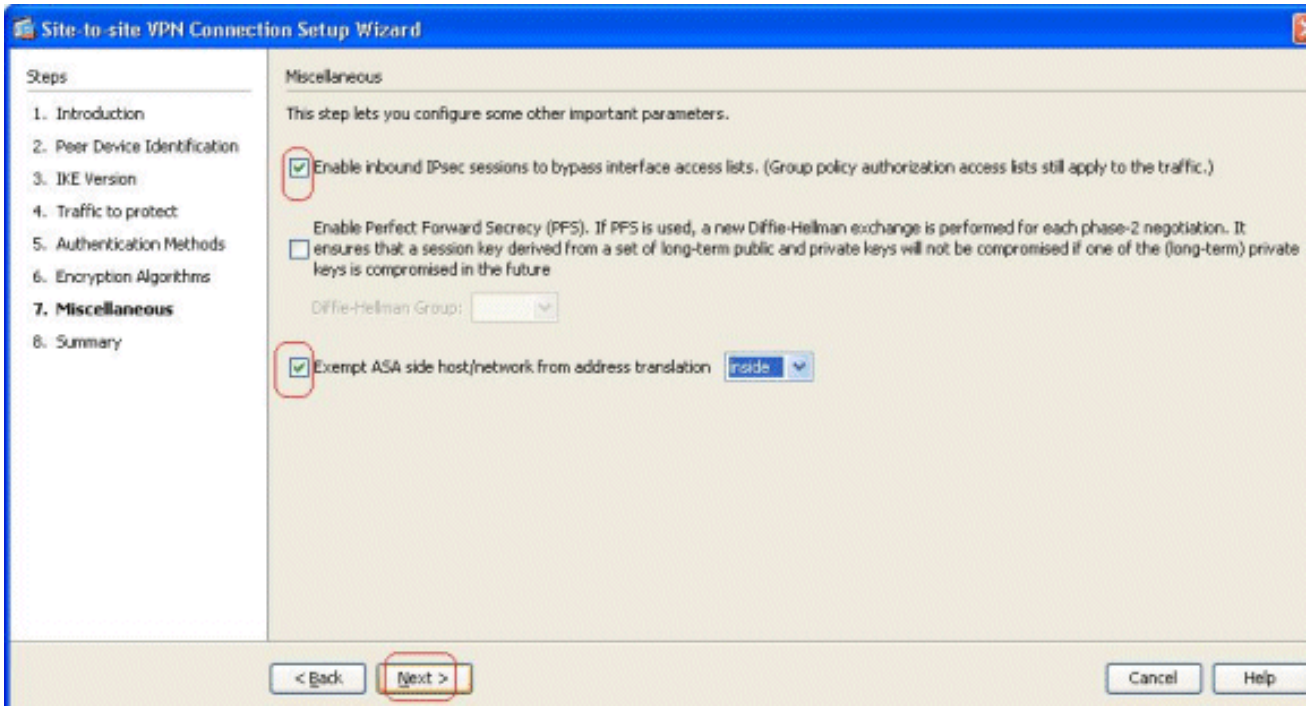


IKEv2 では、擬似ランダム関数（PRF）アルゴリズムとは別の整合性アルゴリズムをネゴシエートできます。 これは、現在利用可能なオプションが SHA-1 または MD5 である IKE ポリシーで設定できます。デフォルトで定義された IPsec プロポーザルのパラメータは変更できません。新しいパラメータを追加するには、[IPsec Proposal] フィールドの横にある [Select] をクリックします。 IPSec プロポーザルについての IKEv1 と IKEv2 の主な違いは、IKEv1 が暗号化と認証のアルゴリズムの組み合わせに関してトランスフォーム セットを受け入れることです。 IKEv2 は暗号化と整合性パラメータを個別に受け入れ、最終的にこれらすべてで可能な OR の組み合わせを行います。 このウィザードの最後の要約スライドでこれらを確認できます。

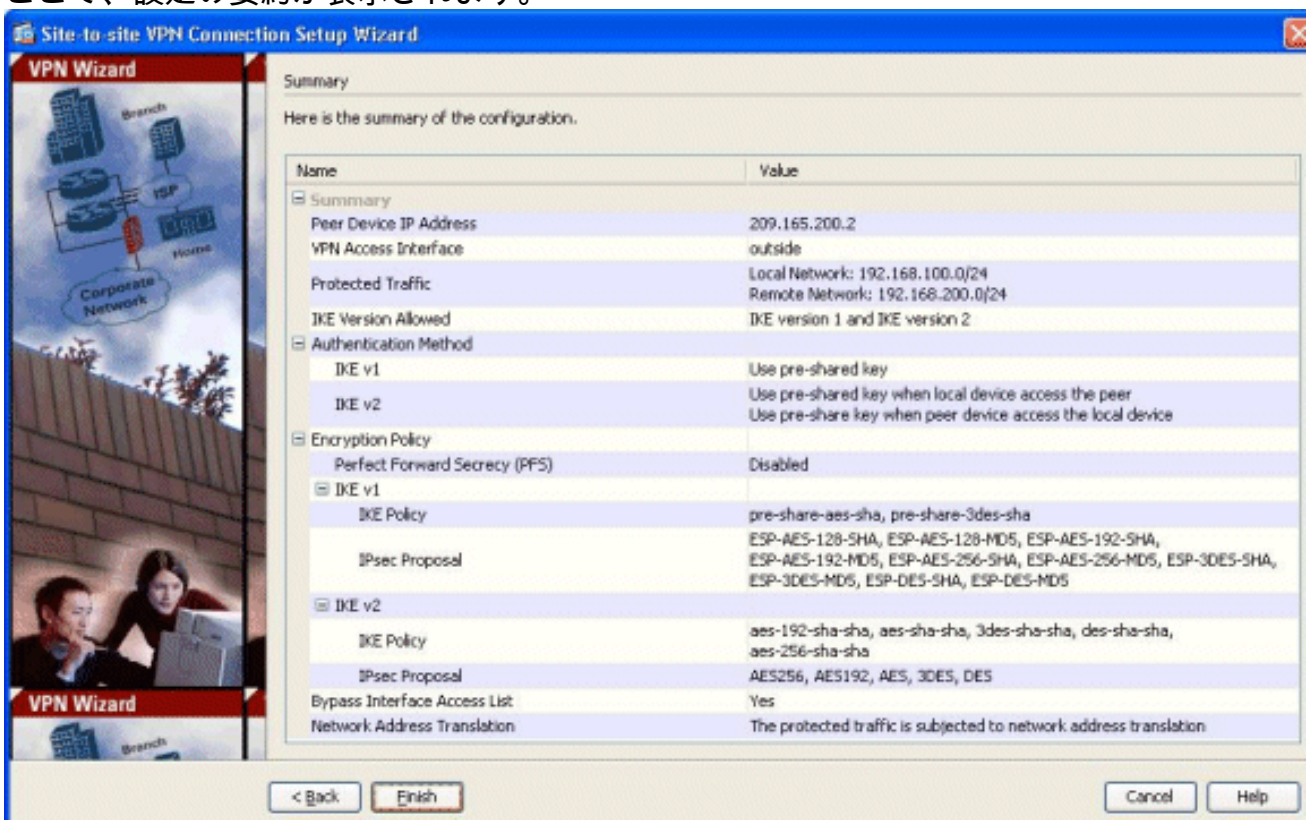
12. [Next] をクリックします。



13. NAT 免除、PFS、インターフェイス ACL のバイパスなどの詳細を指定します。 [Next] を選択します。



14. ここで、設定の要約が表示されます。



サイト間 VPN トンネル ウィザードを終了するには、[Finish] をクリックします。 新しい接続プロファイルが設定済みのパラメータを使用して作成されます。

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- show crypto ikev2 sa - IKEv2 ランタイム SA データベースを表示します。

- show vpn-sessiondb detail l2l - サイト間 VPN セッションに関する情報を表示します。

トラブルシューティング

トラブルシューティングのためのコマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- debug crypto ikev2 - IKEv2 の**デバッグ** メッセージを表示します。

関連情報

- Cisco ASA 5500 シリーズ アプライアンスに関するテクニカル サポート
- テクニカルサポートとドキュメント - Cisco Systems