ASDM 6.4: Site-to-Site VPN Tunnel with IKEv2 Configuration Example

Contents

Introduction

This document describes how to configure a site-to-site VPN tunnel between two Cisco Adaptive Security Appliances (ASAs) using Internet Key Exchange (IKE) version 2. It describes the steps used to configure the VPN tunnel using an Adaptive Security Device Manager (ASDM) GUI wizard.

Prerequisites

Requirements

Make sure that the Cisco ASA has been configured with the basic settings.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA 5500 Series Adaptive Security Appliances running software version 8.4 and later
- Cisco ASDM software version 6.4 and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

IKEv2, is an enhancement to the existing IKEv1 protocol which includes these benefits:

- Fewer message exchanges between IKE peers
- Unidirectional authentication methods
- Built-in support for Dead Peer Detection (DPD) and NAT-Traversal
- Use of Extensible Authentication Protocol (EAP) for authentication
- Eliminates the risk of simple DoS attacks using anti-clogging cookies

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:

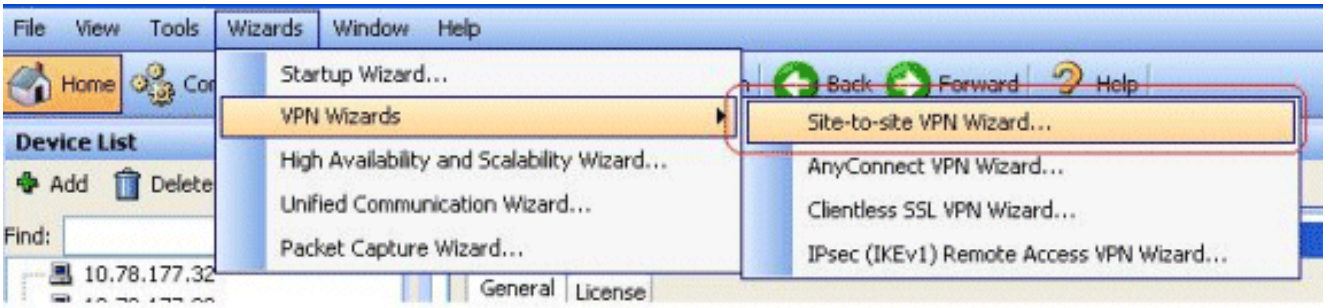
This document shows the configuration of site-to-site VPN tunnel on HQ-ASA. The same could be followed as a mirror on the BQ-ASA.

ASDM Configuration on HQ-ASA

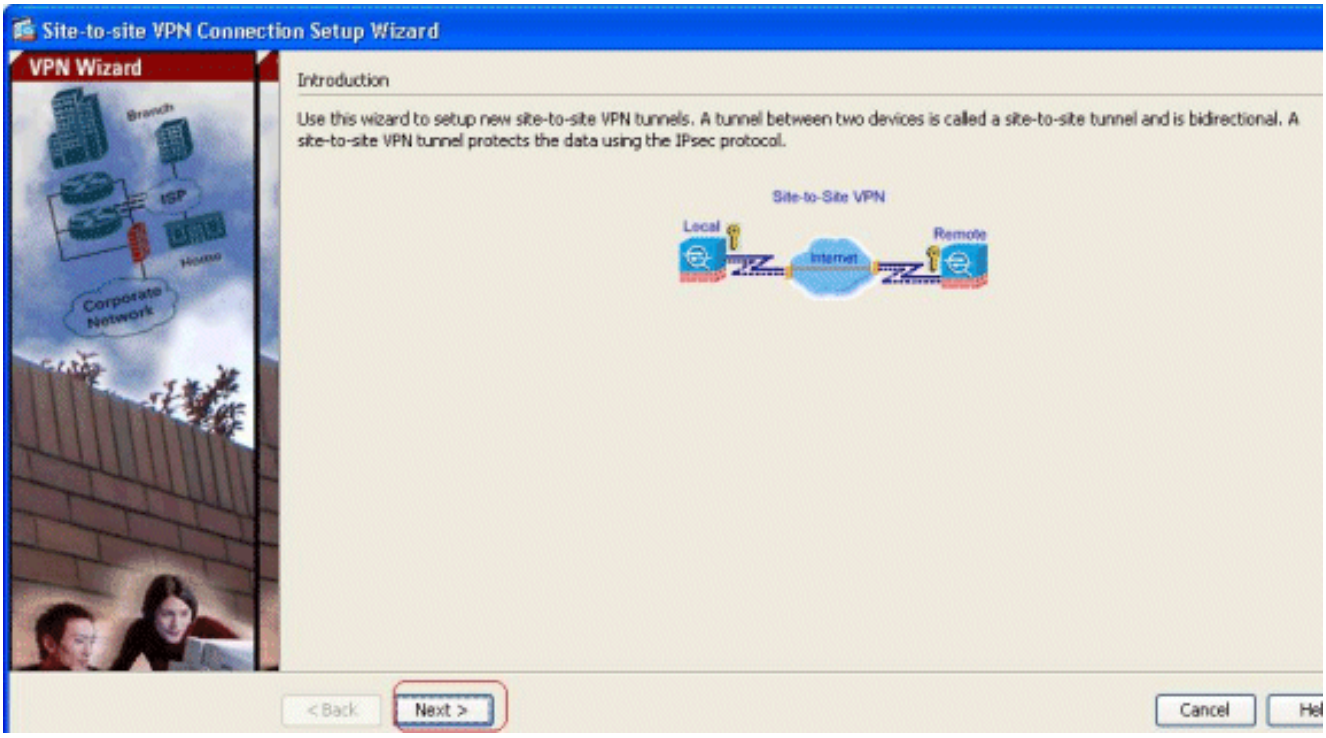
This VPN tunnel could be configured using an easy-to-use GUI wizard.

Complete these steps:

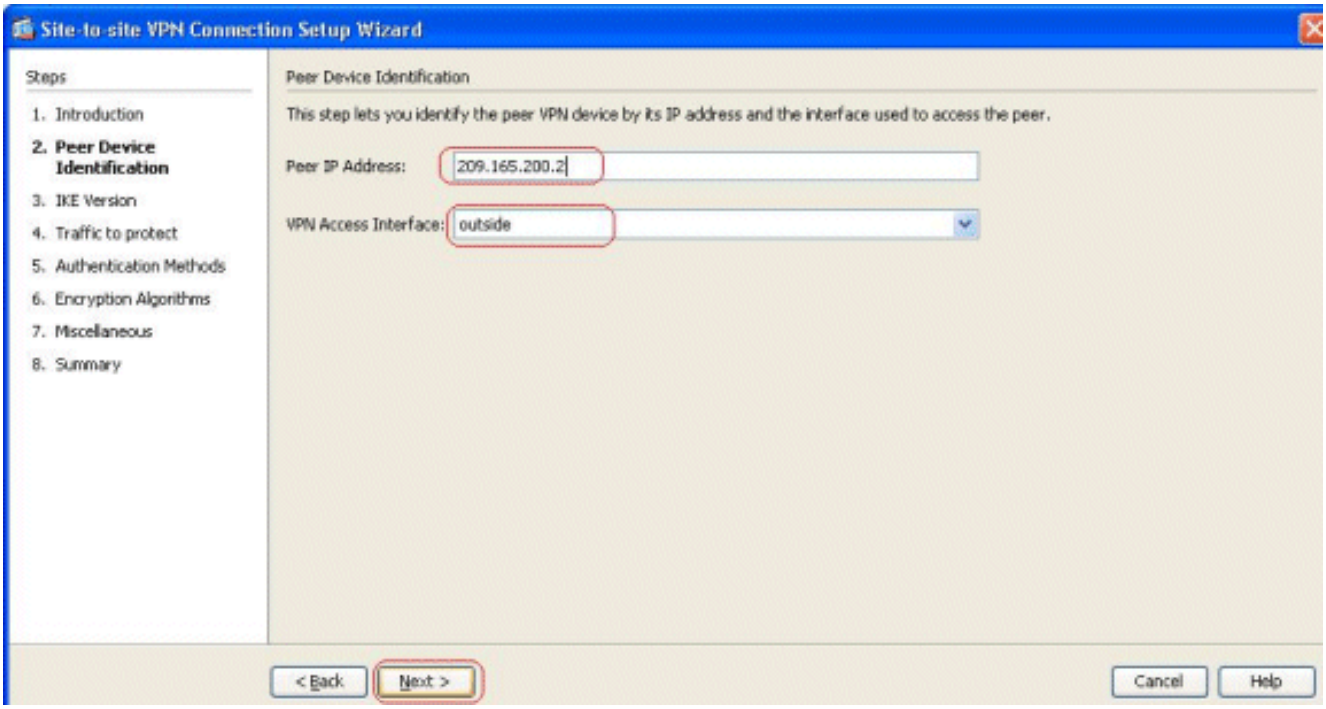
1. Log in to the ASDM, and go to **Wizards** > **VPN Wizards** > **Site-to-site VPN Wizard**.



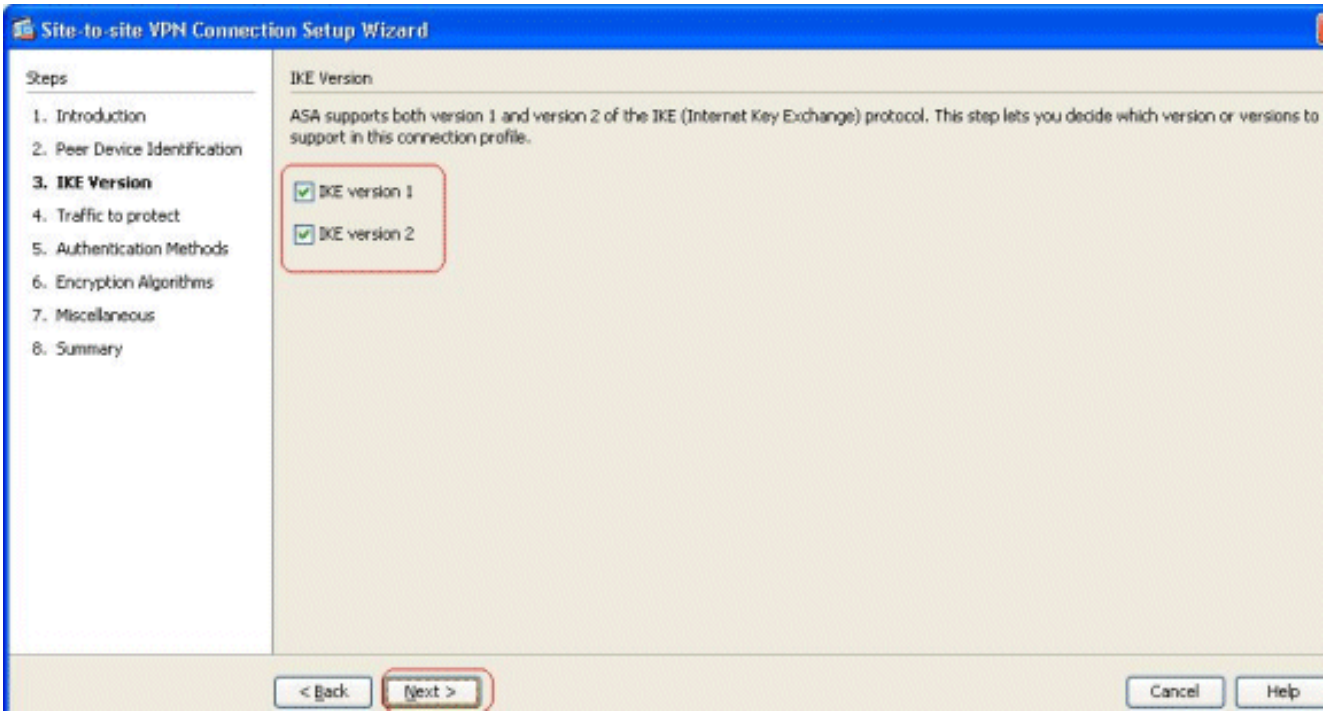
2. A site-to-site VPN Connection setup window appears. Click **Next**.



3. Specify the Peer IP Address and VPN Access Interface. Click **Next**.

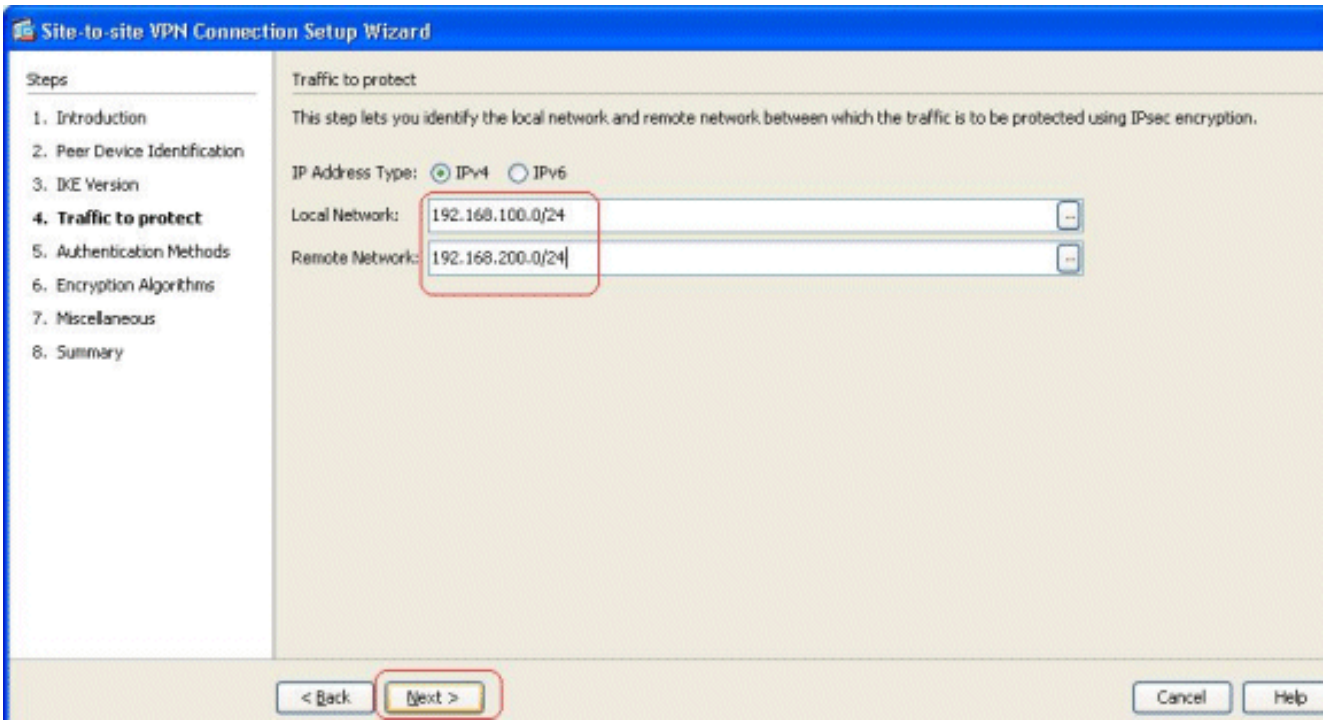


4. Select both IKE versions, and click **Next**.

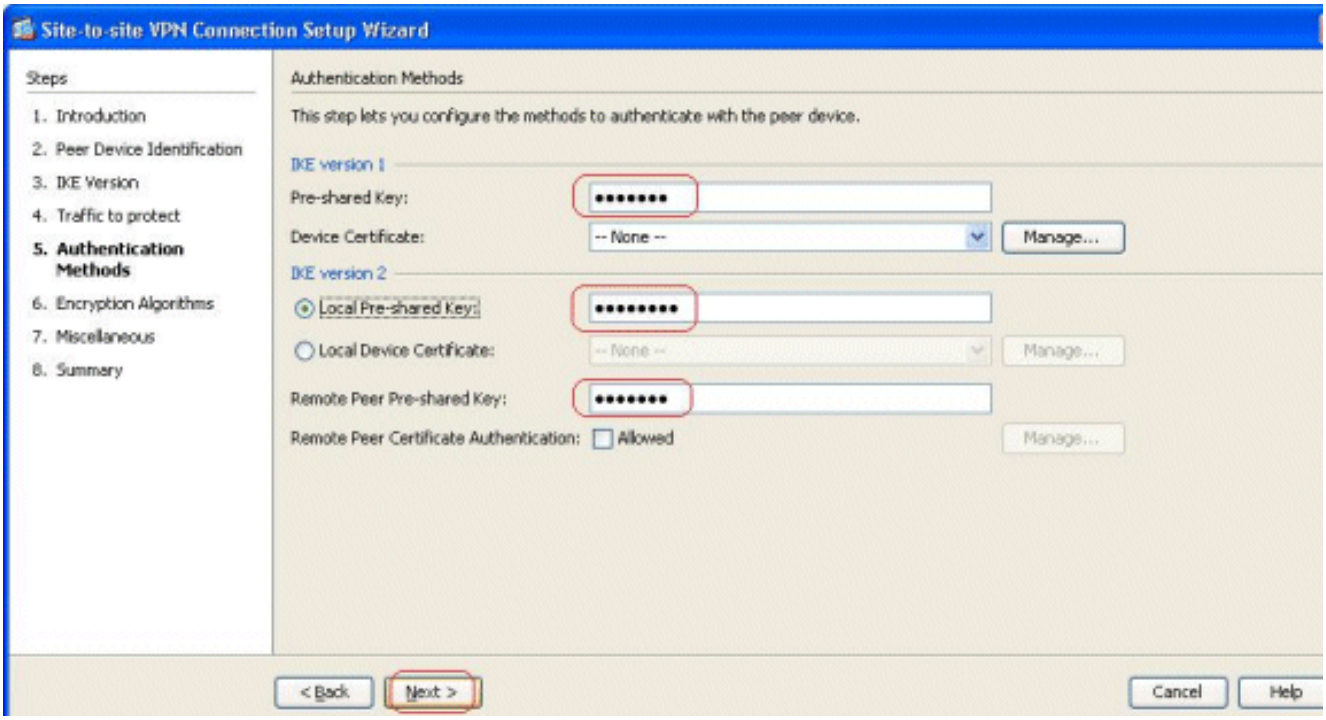


Note: Both versions of IKE are configured here because the initiator could have a backup from IKEv2 to IKEv1 when IKEv2 fails.

5. Specify the Local Network and Remote Network so that the traffic between these networks are encrypted and passed through the VPN tunnel. Click **Next**.

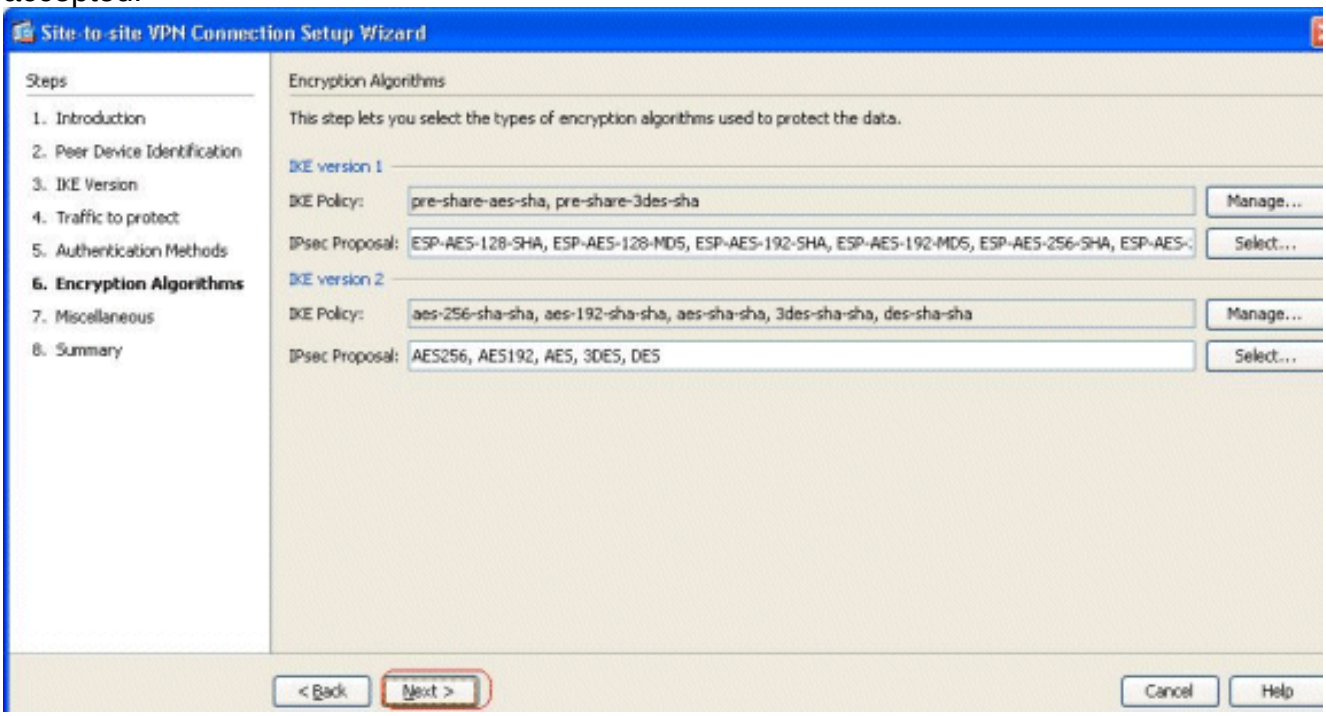


6. Specify the Pre-shared Keys for both versions of IKE.

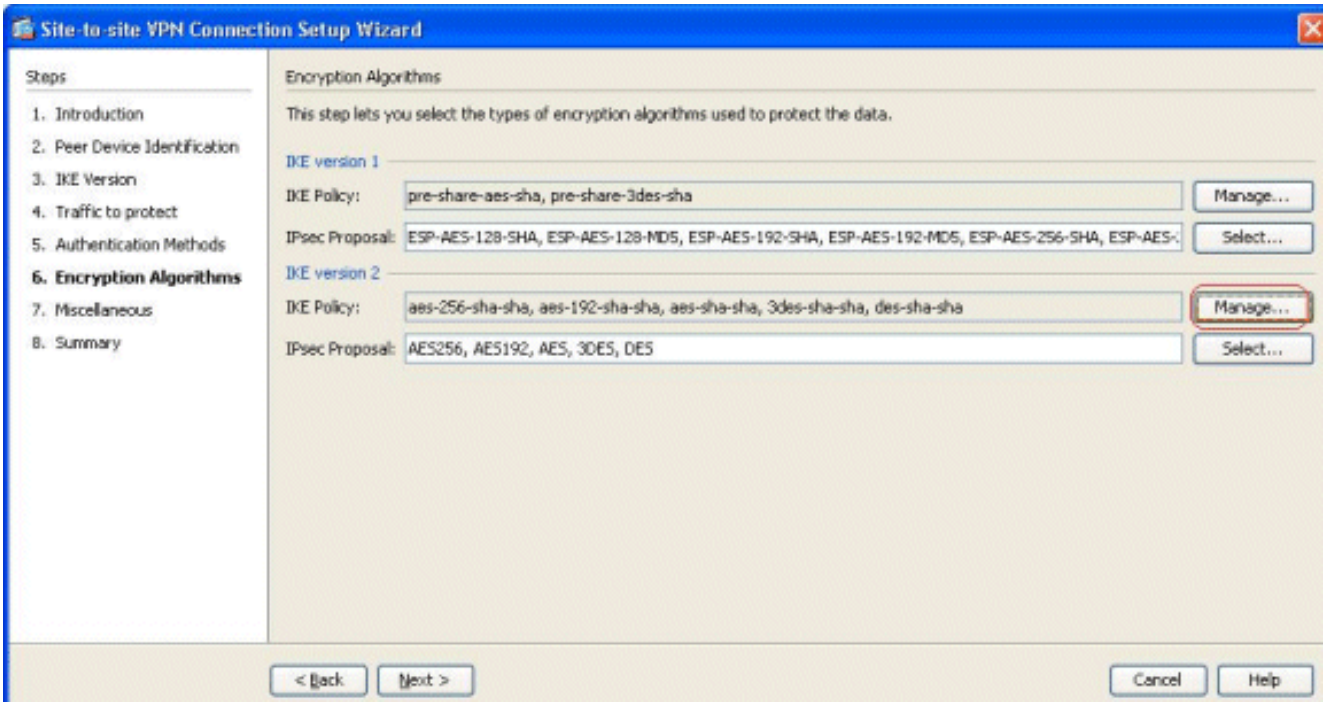


The major difference between IKE versions 1 and 2 lies in terms of the authentication method they allow. IKEv1 allows only one type of authentication at both VPN ends (that is, either pre-shared key or certificate). However, IKEv2 allows asymmetric authentication methods to be configured (that is, pre-shared-key authentication for the originator, but certificate authentication for the responder) using separate local and remote authentication CLIs.Further, you can have different pre-shared keys at both ends. The Local Pre-shared key at the HQ-ASA end becomes the Remote Pre-shared key at the BQ-ASA end. Likewise, the Remote Pre-shared key at the HQ-ASA end becomes the Local Pre-shared key at the BQ-ASA end.

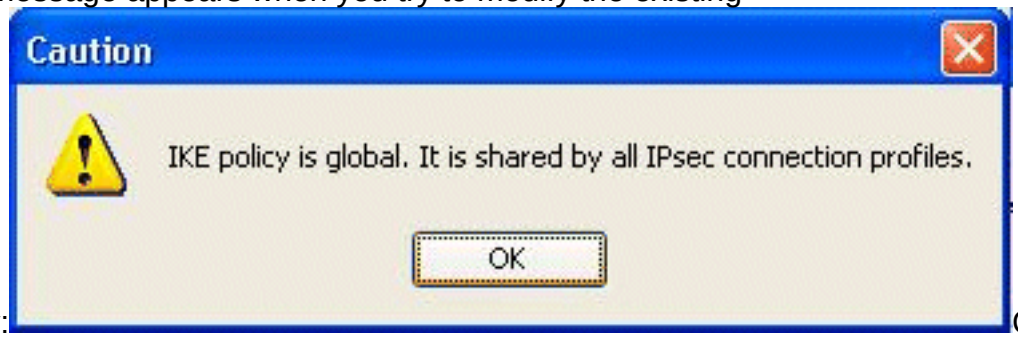
7. Specify the encryption algorithms for both IKE versions 1 and 2. Here, the default values are accepted:



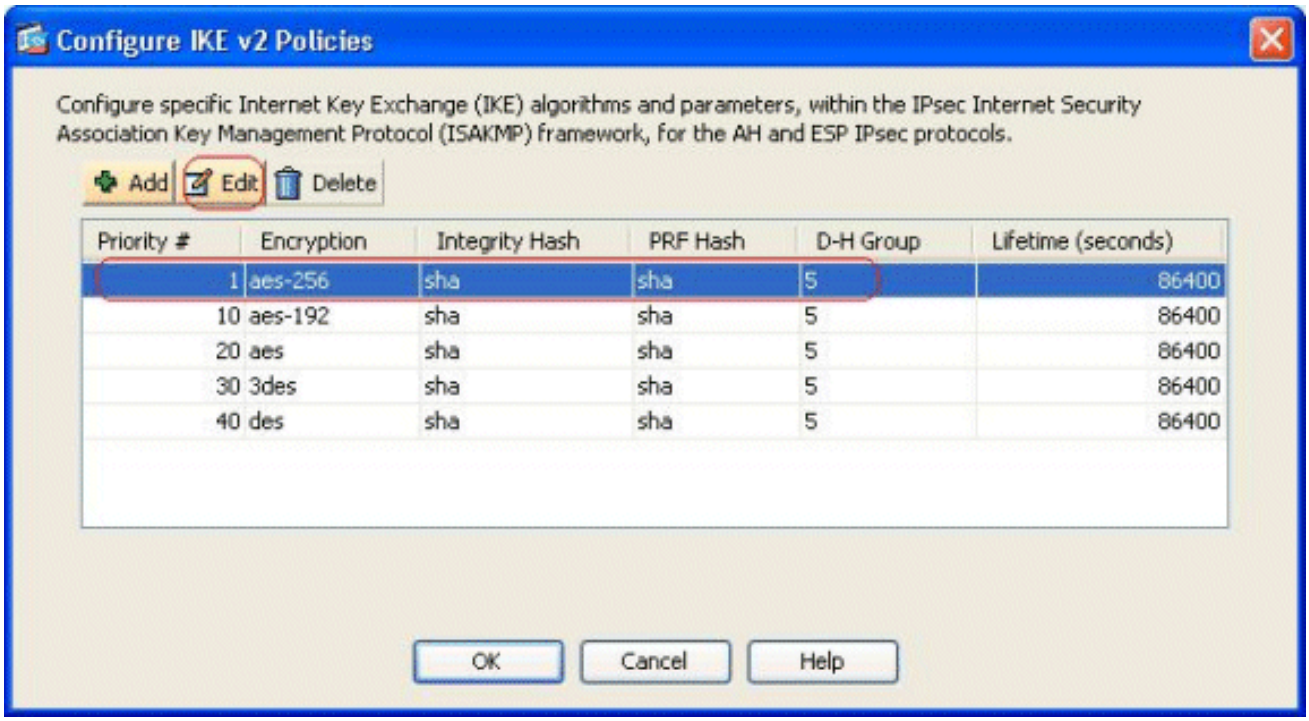
8. Click **Manage...** in order to modify the IKE policy.



Note: IKE Policy in IKEv2 is synonymous to the **ISAKMP Policy** in IKEv1.**IPsec Proposal** in IKEv2 is synonymous to the **Transform Set** in IKEv1.

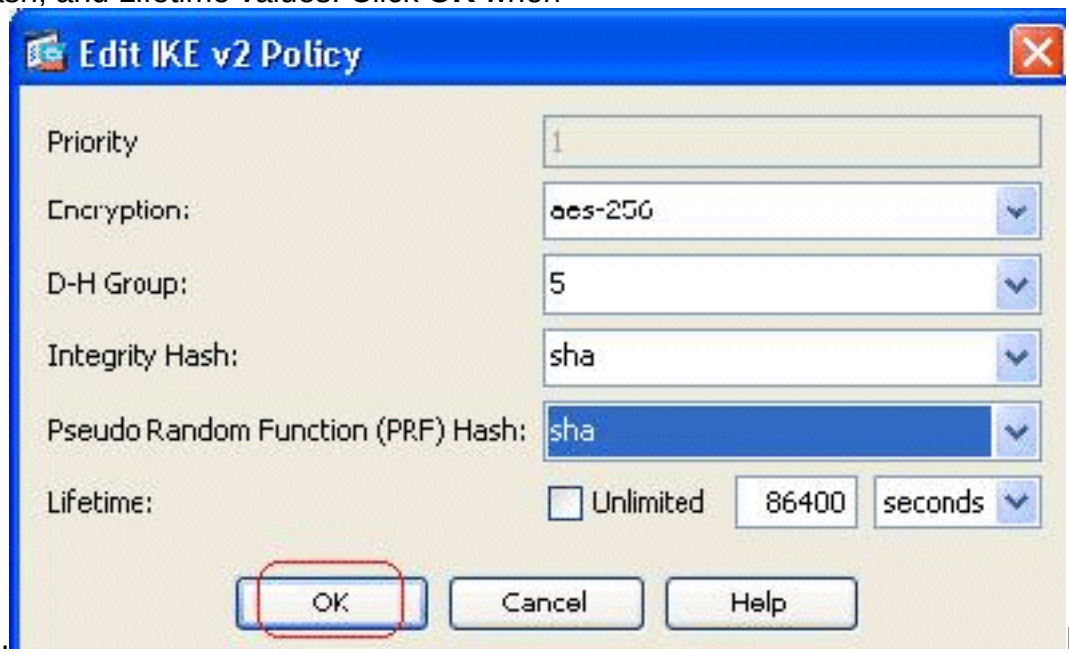
9. This message appears when you try to modify the existing policy: 

Click **OK** in order to proceed.
10. Select the specified IKE policy, and click **Edit**.



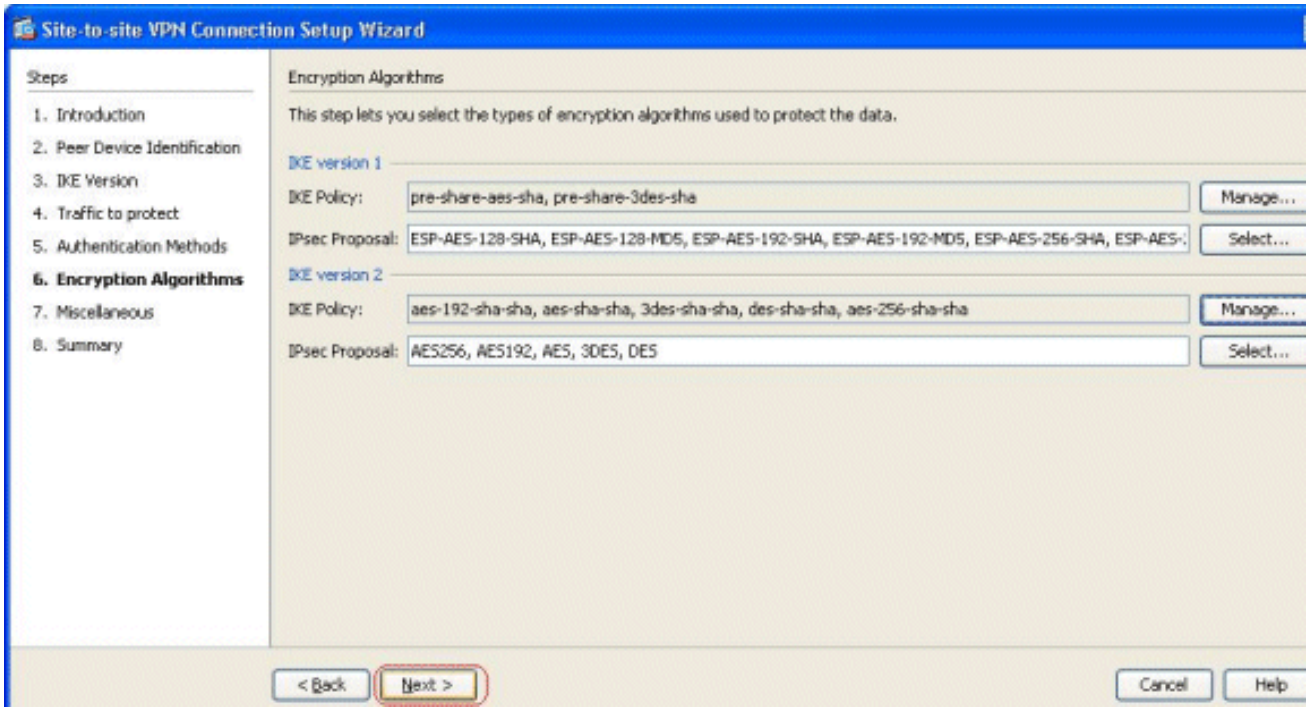
11. You can modify the parameters such as Priority, Encryption, D-H Group, Integrity Hash,

PRF Hash, and Lifetime values. Click **OK** when finished.

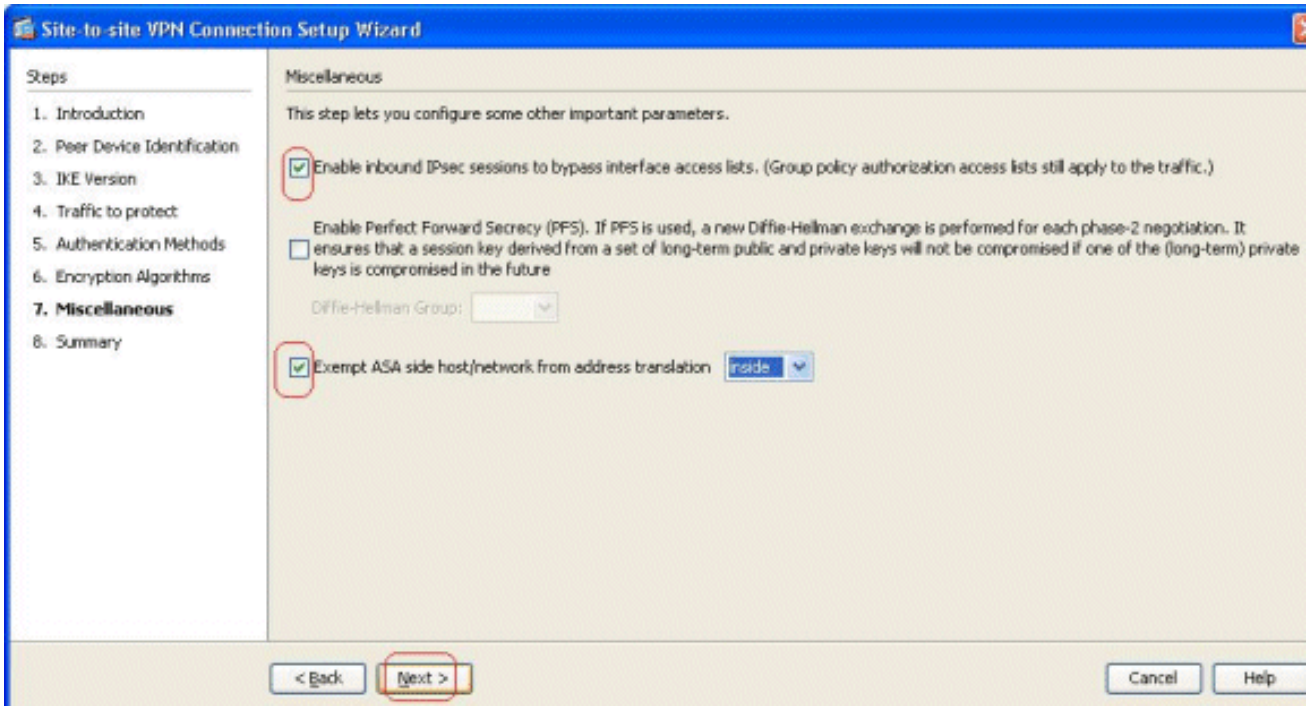


IKEv2 allows for the Integrity algorithm to be negotiated separately from the Pseudo Random Function (PRF) algorithm. This could be configured in the IKE policy with current available options being SHA-1 or MD5.You can not modify the IPsec proposal parameters that are defined by default. Click **Select** next to the IPsec Proposal field in order to add new parameters. The major difference between IKEv1 and IKEv2, in terms of the IPsec proposals, is that IKEv1 accepts the transform set in terms of combinations of encryption and authentication algorithms. IKEv2 accepts the encryption and integrity parameters individually, and finally makes all possible OR combinations of these. You could view these at the end of this wizard, in the Summary slide.

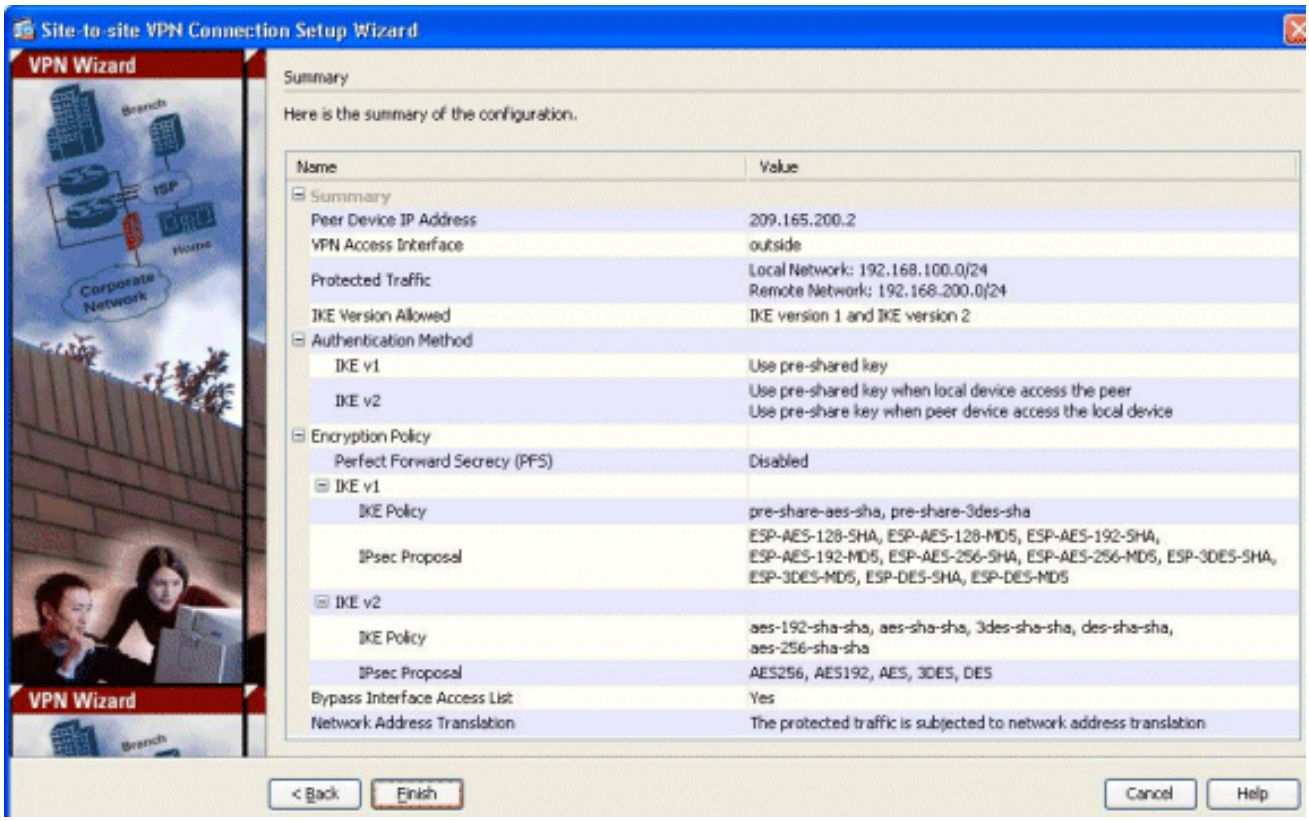
12. Click **Next**.



13. Specify the details, such as NAT exemption, PFS, and Interface ACL Bypassing. Choose **Next**.



14. A summary of the configuration can be seen here:



Click **Finish** in order to complete the site-to-site VPN tunnel wizard. A new Connection Profile is created with the configured parameters.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto ikev2 sa** - Displays the IKEv2 runtime SA database.
- **show vpn-sessiondb detail l2l** - Displays the information about site-to-site VPN sessions.

Troubleshoot

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ikev2** - Shows **debug** messages for IKEv2.

Related Information

- **Cisco ASA 5500 Series Appliances Technical Support**
- **Technical Support & Documentation - Cisco Systems**