ASDM 6.4:使用IKEv2的站點到站點VPN隧道配置示例

目錄

簡介

本文說明如何使用Internet金鑰交換(IKE)版本2在兩個Cisco Adaptive Security Appliance(ASA)之間配置站點到站點VPN隧道。本文檔介紹了使用自適應安全裝置管理器(ASDM)GUI嚮導配置VPN隧道的步驟。

必要條件

需求

確保Cisco ASA已配置了基本設定。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本8.4及更高版本的Cisco ASA 5500系列自適應安全裝置
- Cisco ASDM軟體6.4版及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

IKEv2是對現有IKEv1協定的增強，包括以下優點：

- IKE對等體之間的消息交換更少
- 單向驗證方法
- 內建對失效對等體檢測(DPD)和NAT遍歷的支援
- 使用可擴展身份驗證協定(EAP)進行身份驗證
- 使用防堵塞cookie消除簡單DoS攻擊的風險

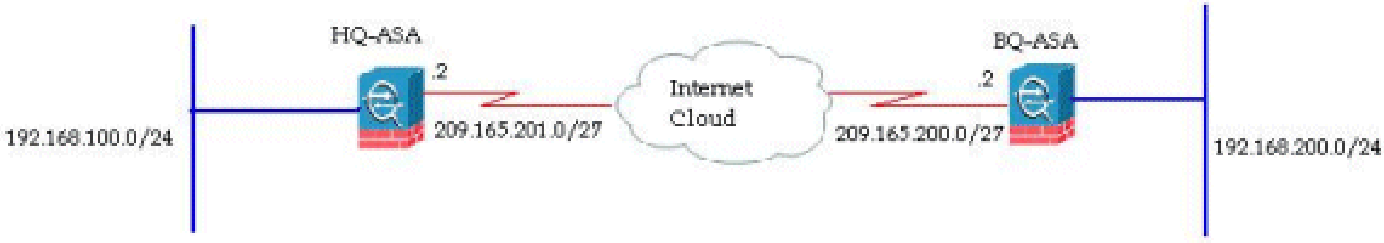
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



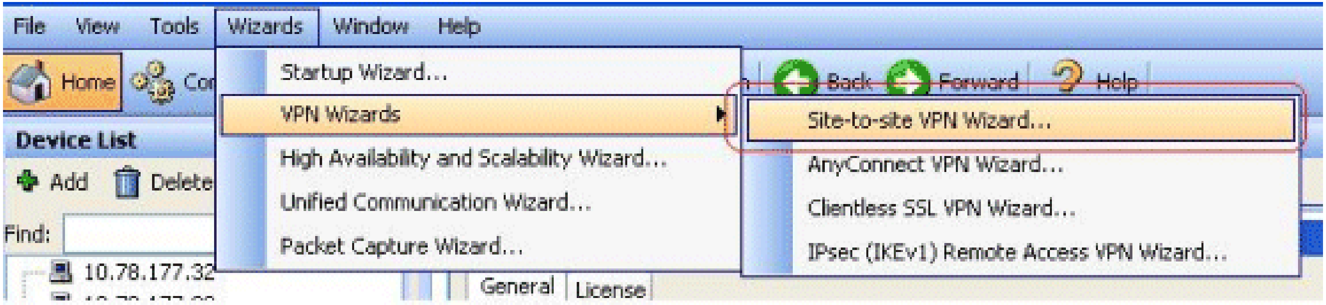
本文檔顯示HQ-ASA上的站點到站點VPN隧道的配置。在BQ-ASA上，同一事件可以作為映象執行。

HQ-ASA上的ASDM配置

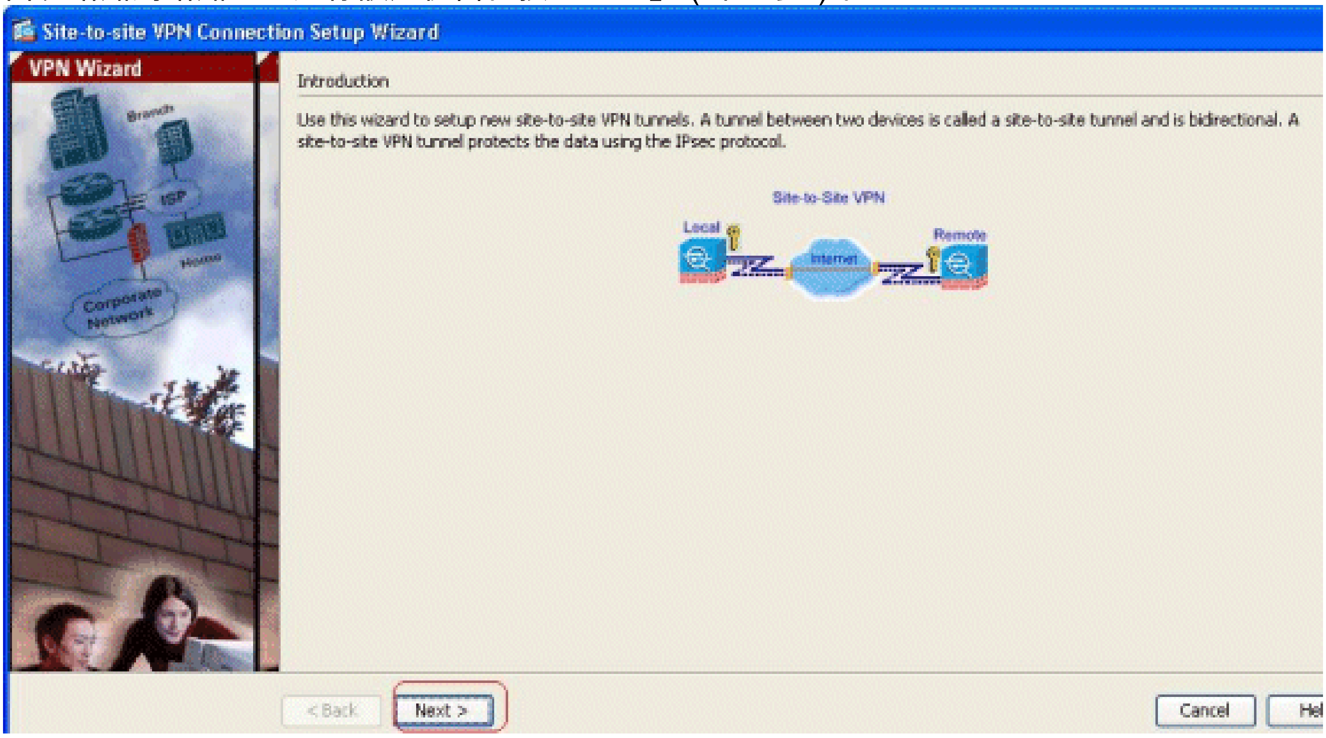
可以使用易於使用的GUI嚮導配置此VPN隧道。

請完成以下步驟：

1. 登入到ASDM，然後轉到**Wizards** > **VPN Wizards** > **Site-to-site VPN Wizard**。



2. 出現站點到站點VPN連線設定視窗。按「**Next**」（下一步）。



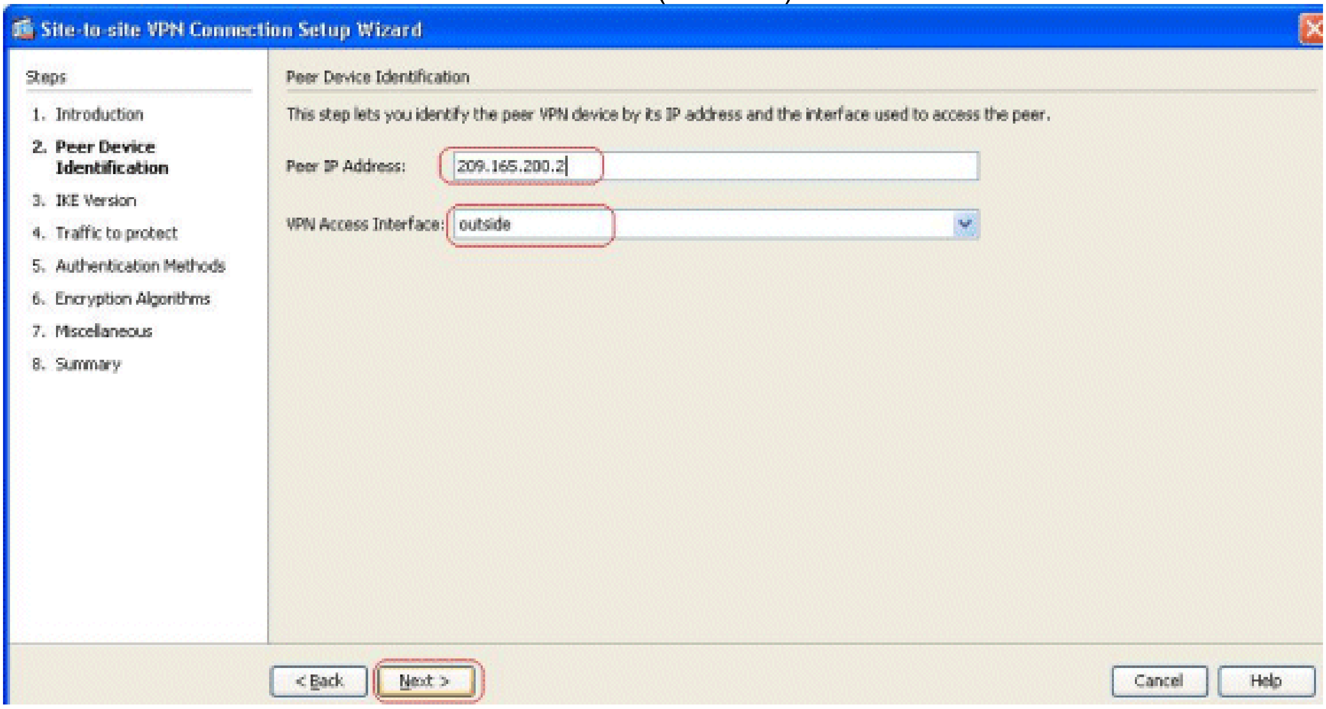
Site-to-site VPN Connection Setup Wizard

VPN Wizard

Introduction

Use this wizard to setup new site-to-site VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol.

3. 指定對等IP地址和VPN訪問介面。按「**Next**」（下一步）。



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. **Peer Device Identification**
3. IKE Version
4. Traffic to protect
5. Authentication Methods
6. Encryption Algorithms
7. Miscellaneous
8. Summary

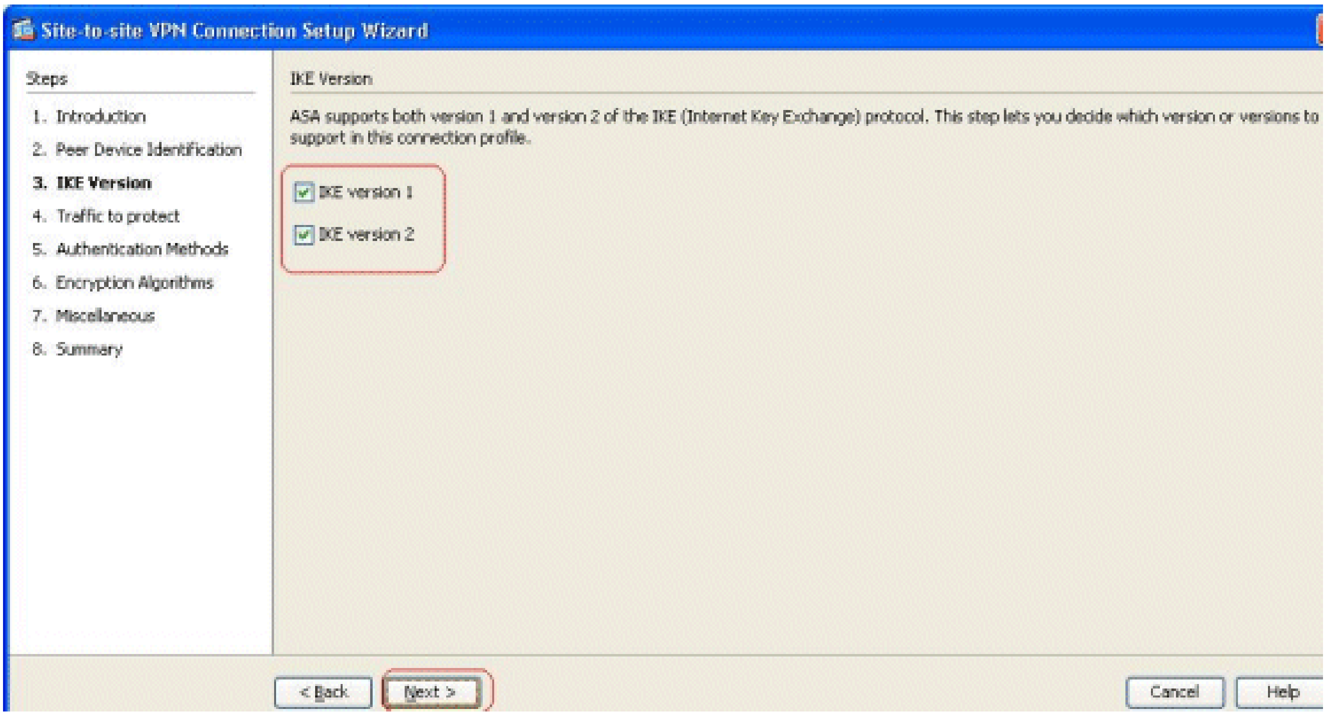
Peer Device Identification

This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address: 209.165.200.2

VPN Access Interface: outside

4. 選擇兩個IKE版本，然後按一下**下一步**。



Site-to-site VPN Connection Setup Wizard

IKE Version

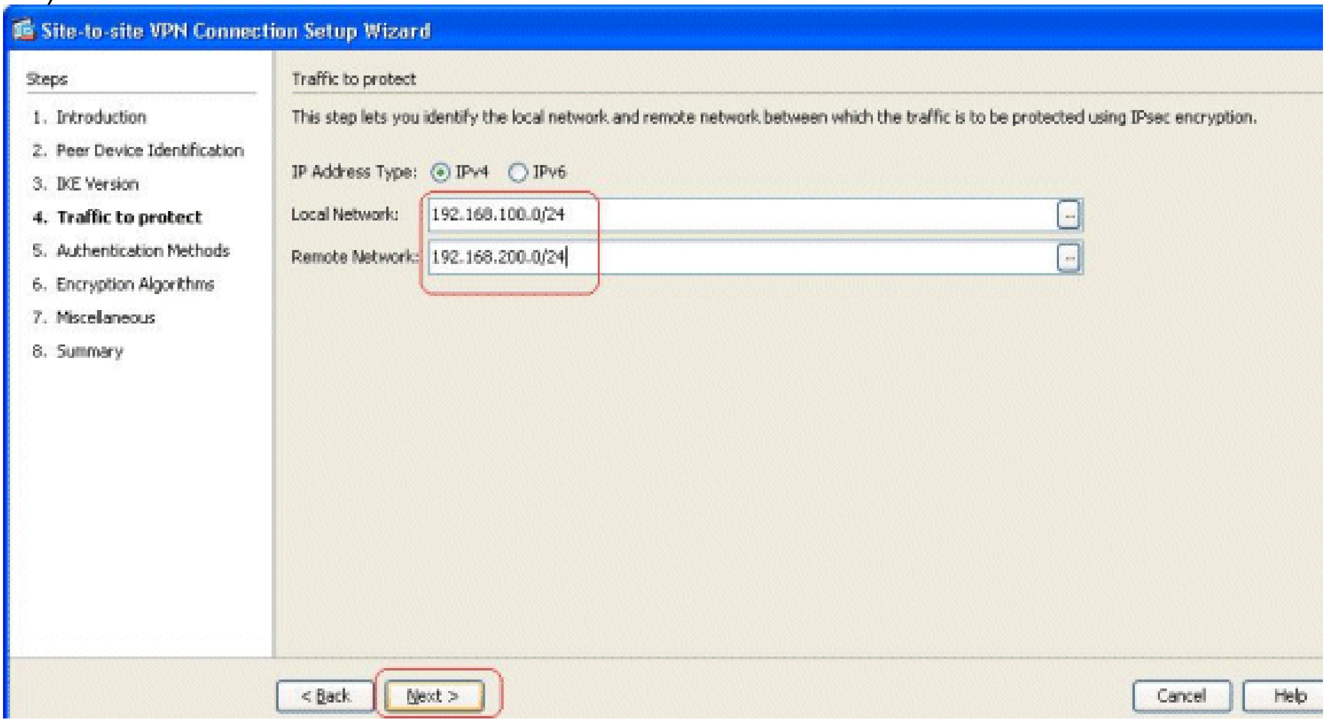
ASA supports both version 1 and version 2 of the IKE (Internet Key Exchange) protocol. This step lets you decide which version or versions to support in this connection profile.

☑ IKE version 1

☑ IKE version 2

注意：此處配置了IKE的兩個版本，因為當IKEv2失敗時，啟動器可以從IKEv2備份到IKEv1。

5. 指定本地網路和遠端網路，以便加密這些網路之間的流量並通過VPN隧道。按「**Next**」（下一步）。



Site-to-site VPN Connection Setup Wizard

Traffic to protect

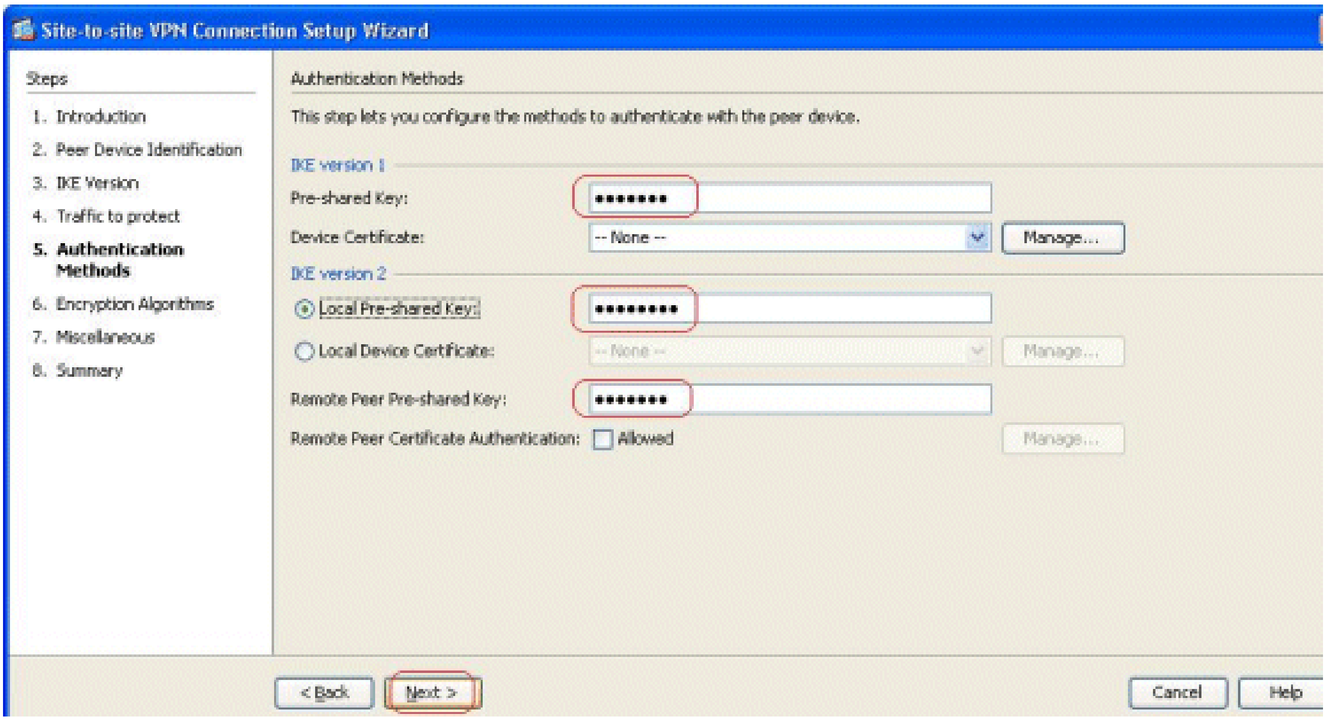
This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

IP Address Type: ● IPv4 ○ IPv6

Local Network: 192.168.100.0/24

Remote Network: 192.168.200.0/24

6. 為兩個版本的IKE指定預共用金鑰。



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. IKE Version
4. Traffic to protect
5. **Authentication Methods**
6. Encryption Algorithms
7. Miscellaneous
8. Summary

Authentication Methods

This step lets you configure the methods to authenticate with the peer device.

IKE version 1

Pre-shared Key: ********

Device Certificate: -- None --

IKE version 2

● Local Pre-shared Key: *********

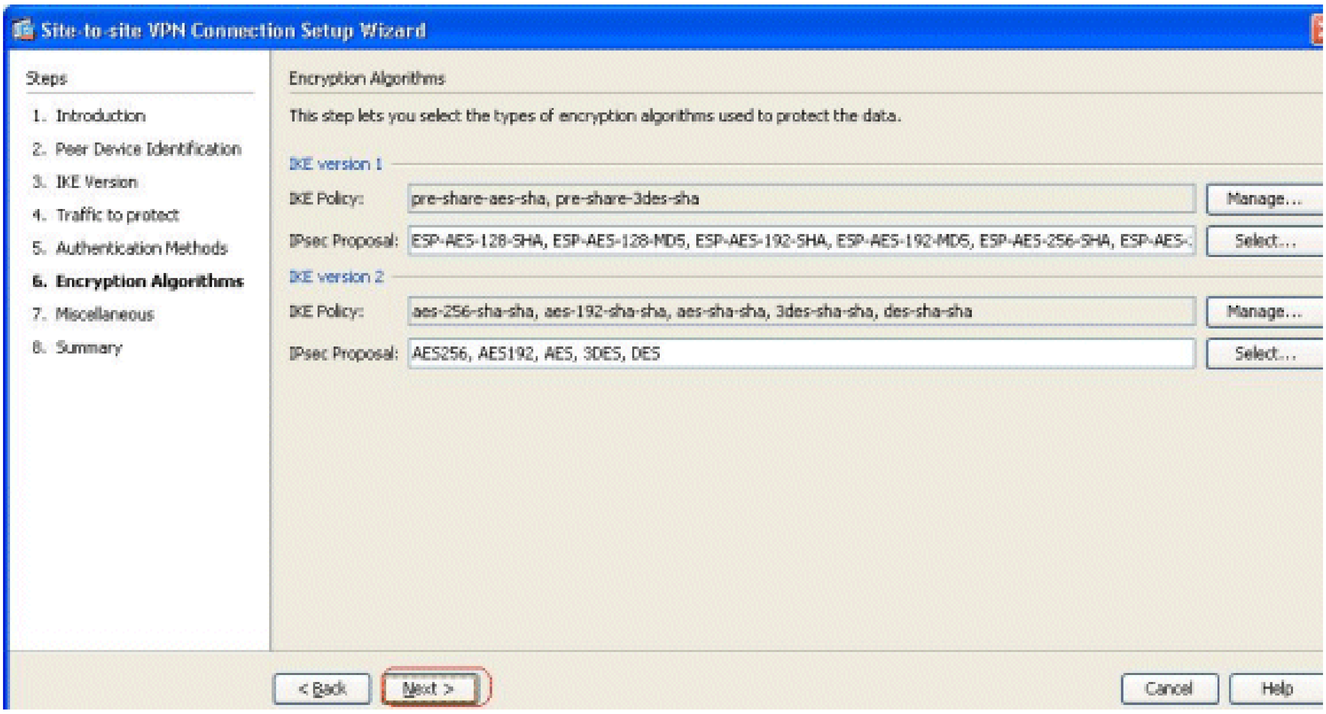
○ Local Device Certificate: -- None --

Remote Peer Pre-shared Key: ********

Remote Peer Certificate Authentication: □ Allowed

IKE版本1和2之間的主要區別在於它們允許的身份驗證方法。IKEv1在VPN的兩端僅允許一種型別的驗證（即預共用金鑰或憑證）。 但是，IKEv2允許使用單獨的本地和遠端身份驗證CLI配置非對稱身份驗證方法（即發起方的預共用金鑰身份驗證，但響應方的證書身份驗證）。此外，您可以在兩端使用不同的預共用金鑰。HQ-ASA端的本地預共用金鑰將成為BQ-ASA端的遠端預共用金鑰。同樣，HQ-ASA端的Remote Pre-shared key將變為BQ-ASA端的Local Pre-shared key。

7. 為IKE版本1和2指定加密演算法。此處接受預設值
：



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. IKE Version
4. Traffic to protect
5. Authentication Methods
6. **Encryption Algorithms**
7. Miscellaneous
8. Summary

Encryption Algorithms

This step lets you select the types of encryption algorithms used to protect the data.

IKE version 1

IKE Policy: pre-share-aes-sha, pre-share-3des-sha

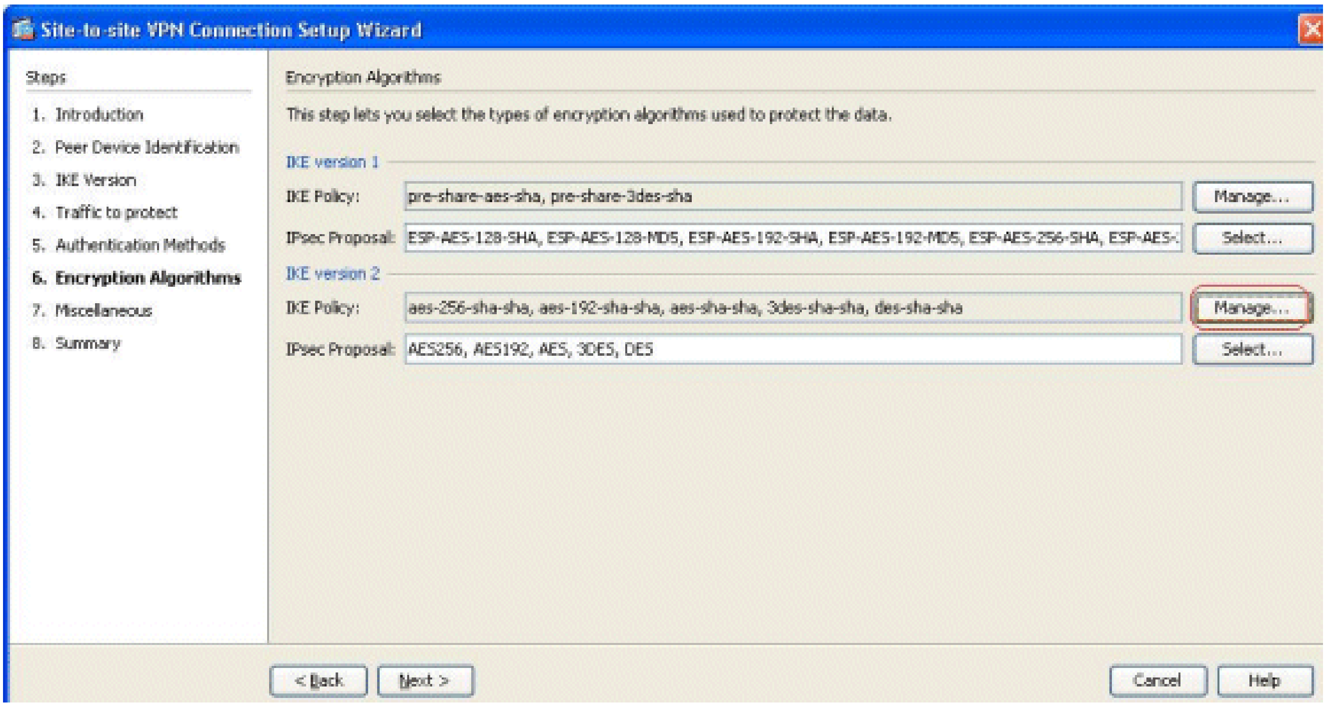
IPsec Proposal: ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-

IKE version 2

IKE Policy: aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha

IPsec Proposal: AES256, AES192, AES, 3DES, DES

8. 按一下**Manage...**以修改IKE策略。



Site-to-site VPN Connection Setup Wizard

Steps
1. Introduction
2. Peer Device Identification
3. IKE Version
4. Traffic to protect
5. Authentication Methods
6. **Encryption Algorithms**
7. Miscellaneous
8. Summary

Encryption Algorithms

This step lets you select the types of encryption algorithms used to protect the data.

IKE version 1

IKE Policy: pre-share-aes-sha, pre-share-3des-sha

IPsec Proposal: ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-

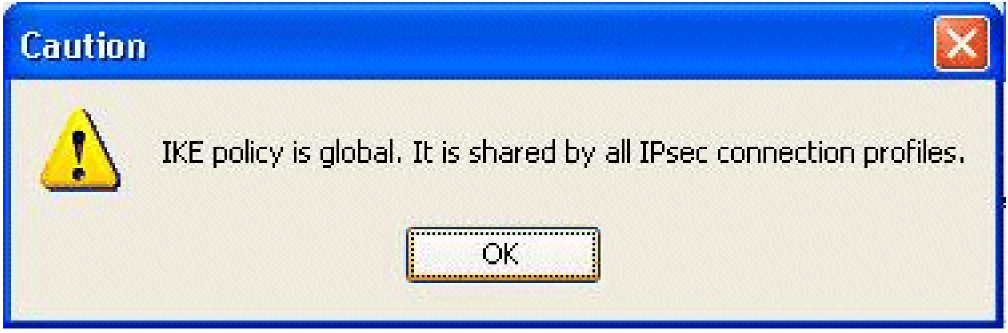
IKE version 2

IKE Policy: aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha

IPsec Proposal: AES256, AES192, AES, 3DES, DES

附註： IKEv2中的IKE策略與IKEv1中的**ISAKMP策**略同義。**IKEv2中**的IPsec建議與IKEv1中**的轉換**集同義。

9. 當您嘗試修改現有策略時，出現以下消息：

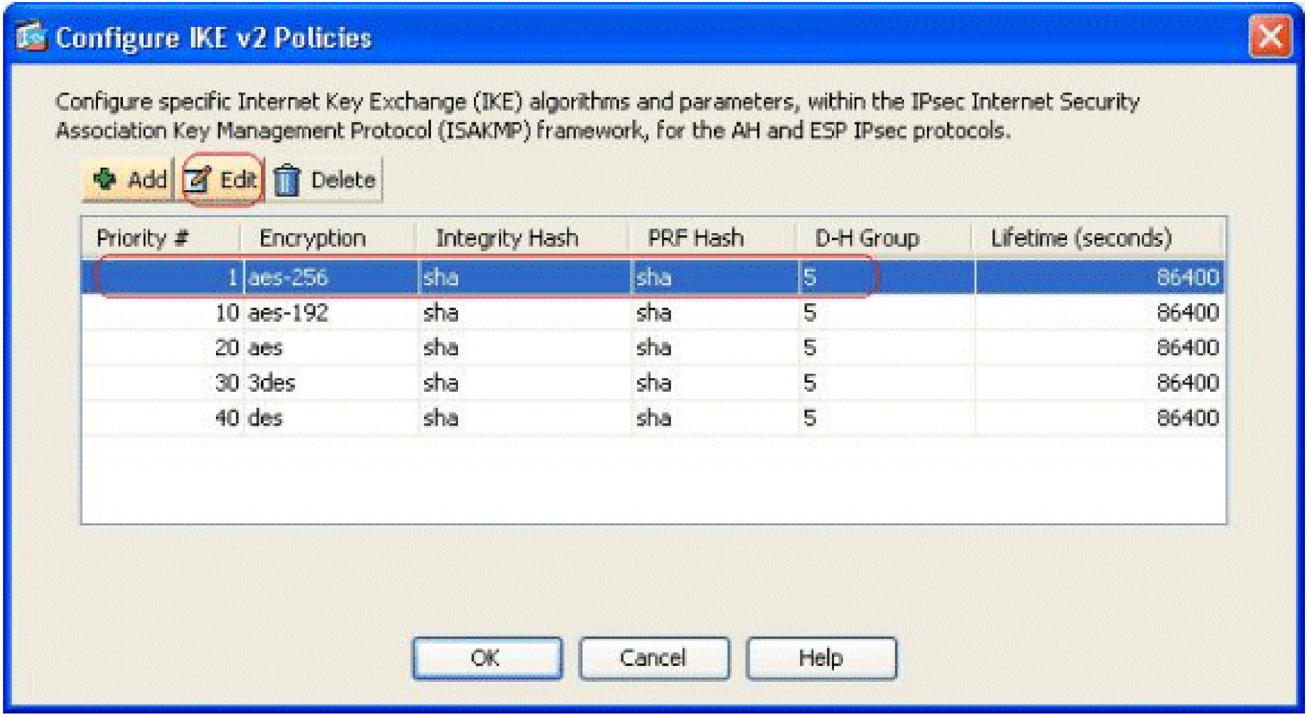


Caution

IKE policy is global. It is shared by all IPsec connection profiles.

按一下「**OK**」以繼續。

10. 選擇指定的IKE策略，然後按一下**Edit**。

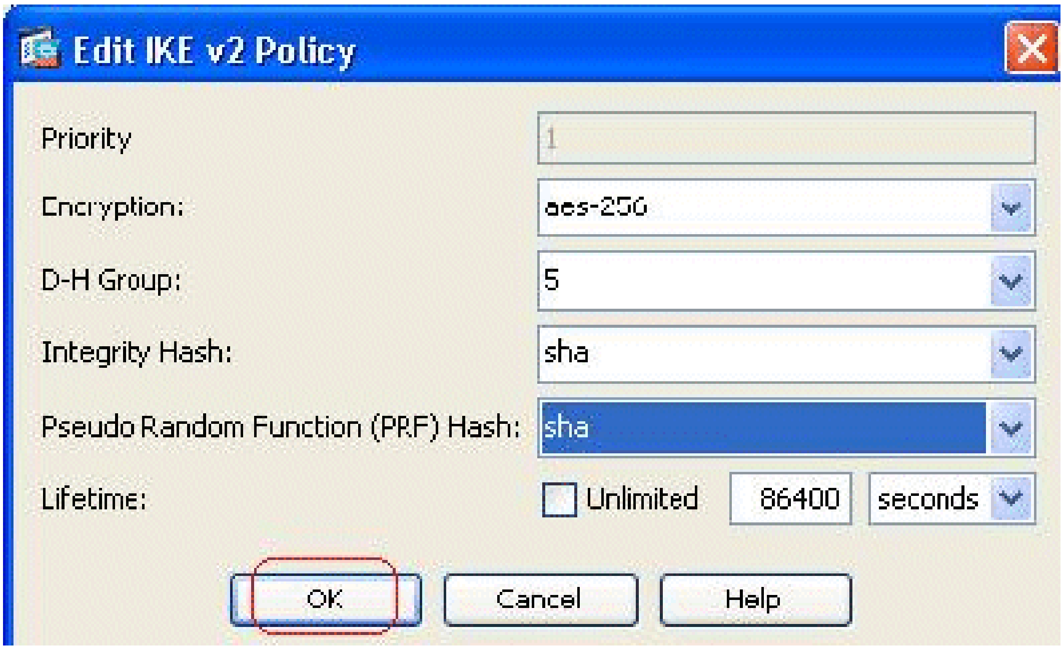


Configure IKE v2 Policies

Configure specific Internet Key Exchange (IKE) algorithms and parameters, within the IPsec Internet Security Association Key Management Protocol (ISAKMP) framework, for the AH and ESP IPsec protocols.

Priority #	Encryption	Integrity Hash	PRF Hash	D-H Group	Lifetime (seconds)
1	aes-256	sha	sha	5	86400
10	aes-192	sha	sha	5	86400
20	aes	sha	sha	5	86400
30	3des	sha	sha	5	86400
40	des	sha	sha	5	86400

11. 您可以修改引數，例如Priority、Encryption、D-H Group、Integrity Hash、PRF Hash和Lifetime值。完成後按一下**OK**。



Edit IKE v2 Policy

Priority: 1

Encryption: aes-256

D-H Group: 5

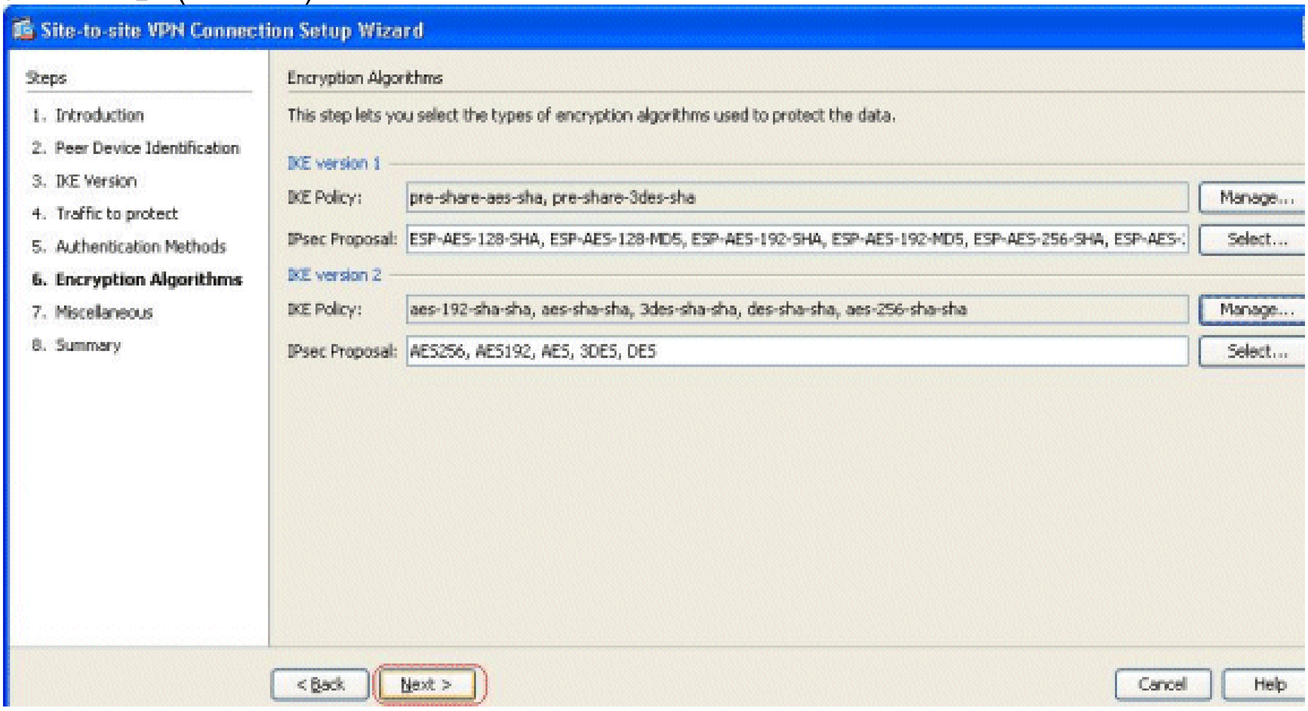
Integrity Hash: sha

Pseudo Random Function (PRF) Hash: sha

Lifetime: □ Unlimited 86400 seconds

IKEv2允許將完整性演算法與偽隨機函式(PRF)演算法分開協商。這可以在IKE策略中配置，當前可用選項為SHA-1或MD5。不能修改預設定義的IPsec建議引數。按一下IPsec Proposal欄位旁邊的**Select**以新增新引數。就IPsec提議而言，IKEv1和IKEv2之間的主要區別在於，IKEv1接受加密和身份驗證演算法組合的轉換集。IKEv2單獨接受加密和完整性引數，並最終生成這些引數的所有可能的OR組合。您可以在此嚮導的末尾的「摘要」幻燈片中檢視這些內容。

12. 按「**Next**」（下一步）。



Site-to-site VPN Connection Setup Wizard

Steps
1. Introduction
2. Peer Device Identification
3. IKE Version
4. Traffic to protect
5. Authentication Methods
6. **Encryption Algorithms**
7. Miscellaneous
8. Summary

Encryption Algorithms

This step lets you select the types of encryption algorithms used to protect the data.

IKE version 1

IKE Policy: pre-share-aes-sha, pre-share-3des-sha

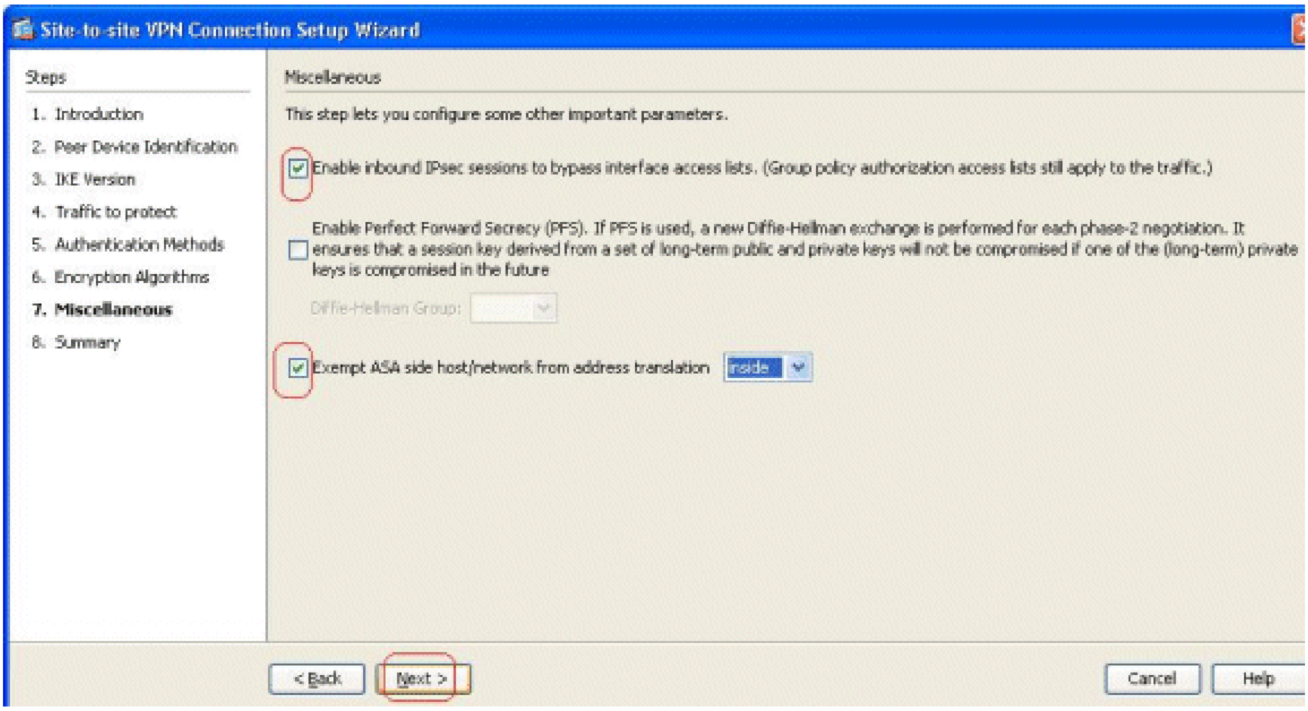
IPsec Proposal: ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-:

IKE version 2

IKE Policy: aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha, aes-256-sha-sha

IPsec Proposal: AES256, AES192, AES, 3DES, DES

13. 指定詳細資訊，例如NAT免除、PFS和介面ACL繞過。選擇**Next**。



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. IKE Version
4. Traffic to protect
5. Authentication Methods
6. Encryption Algorithms
7. **Miscellaneous**
8. Summary

Miscellaneous

This step lets you configure some other important parameters.

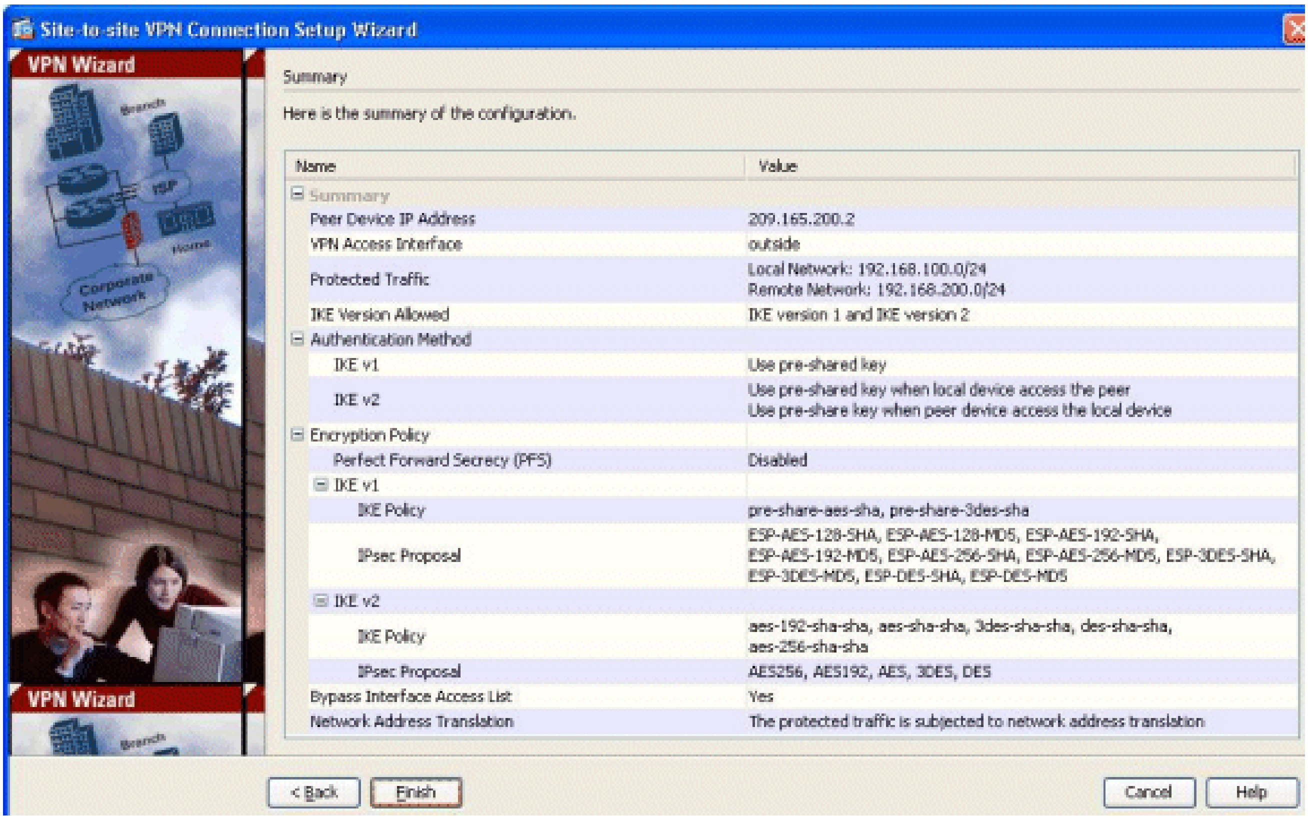
☑ Enable inbound IPsec sessions to bypass interface access lists. (Group policy authorization access lists still apply to the traffic.)

□ Enable Perfect Forward Secrecy (PFS). If PFS is used, a new Diffie-Hellman exchange is performed for each phase-2 negotiation. It ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future

Diffie-Hellman Group:

☑ Exempt ASA side host/network from address translation: inside

14. 配置摘要可在此處檢視
：



Site-to-site VPN Connection Setup Wizard

Summary

Here is the summary of the configuration.

Name	Value
⊟ Summary	
Peer Device IP Address	209.165.200.2
VPN Access Interface	outside
Protected Traffic	Local Network: 192.168.100.0/24 Remote Network: 192.168.200.0/24
IKE Version Allowed	IKE version 1 and IKE version 2
⊟ Authentication Method	
IKE v1	Use pre-shared key
IKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
⊟ Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
⊟ IKE v1	
IKE Policy	pre-share-aes-sha, pre-share-3des-sha
IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5
⊟ IKE v2	
IKE Policy	aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha, aes-256-sha-sha
IPsec Proposal	AES256, AES192, AES, 3DES, DES
Bypass Interface Access List	Yes
Network Address Translation	The protected traffic is subjected to network address translation

按一下**Finish**以完成站點到站點VPN隧道嚮導。使用配置的引數建立新的連線配置檔案。

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **show crypto ikev2 sa** — 顯示IKEv2運行時SA資料庫。

- show vpn-sessiondb detail l2l — 顯示有關站點到站點VPN會話的資訊。

疑難排解

疑難排解指令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- debug crypto ikev2 — 顯示IKEv2的**debug消息。**

相關資訊

- Cisco ASA 5500系列裝置技術支援
- 技術支援與文件 - Cisco Systems