ASA 8.x/ASDM 6.x:使用ASDM在現有站點到站點VPN中新增新VPN對等體資訊

目錄

簡介

本文提供有關使用自適應安全裝置管理器(ASDM)將新的VPN對等項新增到現有站點到站點VPN配置時要進行的配置更改的資訊。 以下情況需要如此：

- Internet服務提供商(ISP)已更改，並且使用了一組新的公共IP範圍。
- 對站點中的網路進行全面重新設計。
- 在站點上用作VPN網關的裝置會遷移到具有不同公共IP地址的新裝置。

本文檔假定站點到站點VPN已正確配置且工作正常。本文檔提供了在L2L VPN配置中更改VPN對等資訊要遵循的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- ASA站點到站點VPN配置示例

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Adapative Security Appliance 5500系列，軟體版本8.2及更新版本
- 軟體版本6.3及更高版本的思科自適應安全裝置管理器

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

回退資訊

站點到站點VPN在HQASA和BQASA之間工作正常。假設BQASA已經完成網路重新設計並在ISP級別修改了IP方案，但所有內部子網詳細資訊保持不變。

此示例配置使用以下IP地址：

- 現有BQASA外部IP地址 — 200.200.200.200
- 新的BQASA外部IP地址 — 209.165.201.2

注意：在此僅修改對等體資訊。由於內部子網中沒有其他更改，因此加密訪問清單保持不變。

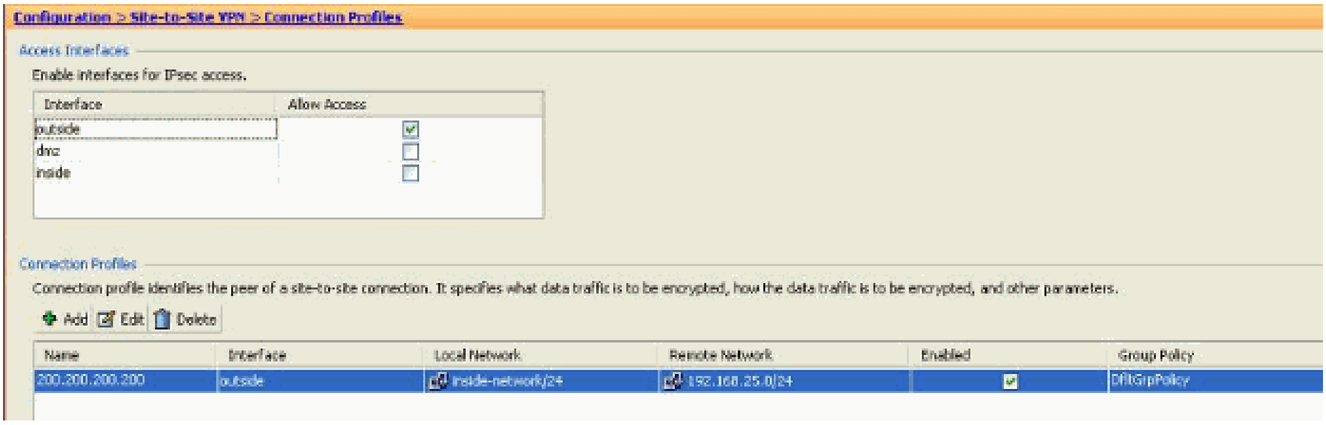
ASDM配置

本節提供有關使用ASDM在HQASA上更改VPN對等資訊的可能方法的資訊。

建立新的連線配置檔案

這種方法比較簡單，因為它不會干擾現有的VPN配置，並且可以使用新的VPN對等體相關資訊建立新的連線配置檔案。

1. 轉到*Configuration > Site-to-Site VPN > Connection Profiles*，然後在Connection Profiles區域下按一下*Add*。



Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
outside	☑
dmz	□
inside	□

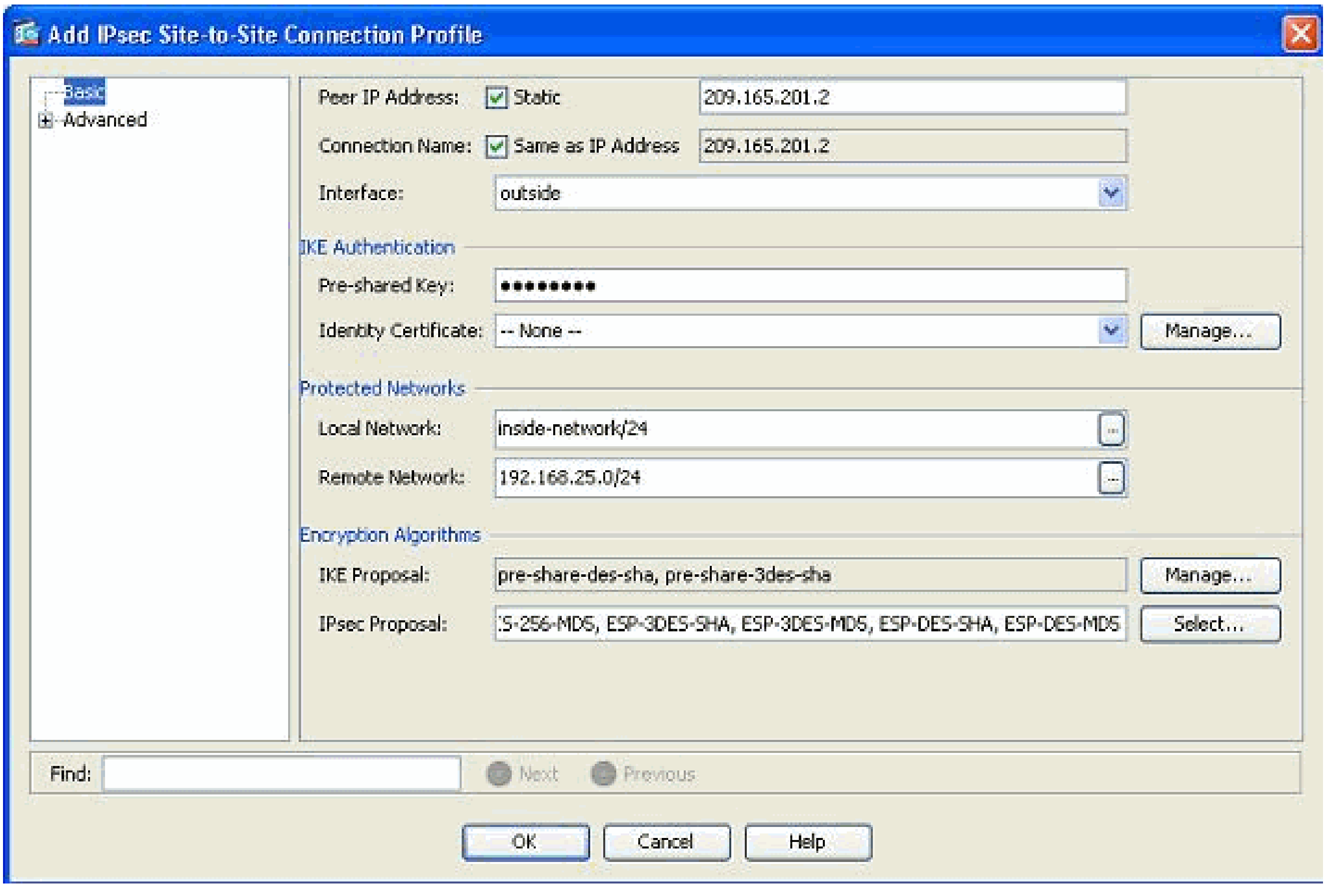
Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters.

Name	Interface	Local Network	Remote Network	Enabled	Group Policy
200.200.200.200	outside	inside-network/24	192.168.25.0/24	☑	DfltGrpPolicy

*Add IPSec Site-to-Site Connection Profile*視窗將開啟。

2. 在Basic頁籤下，提供*對等IP地址*、*預共用金鑰*和*Protected Networks*的詳細資訊。使用與現有VPN相同的所有引數，對等體資訊除外。按一下「*OK*」（確定）。



Add IPsec Site-to-Site Connection Profile

Peer IP Address: ☑ Static 209.165.201.2

Connection Name: ☑ Same as IP Address 209.165.201.2

Interface: outside

IKE Authentication

Pre-shared Key: ••••••••

Identity Certificate: -- None --

Protected Networks

Local Network: inside-network/24

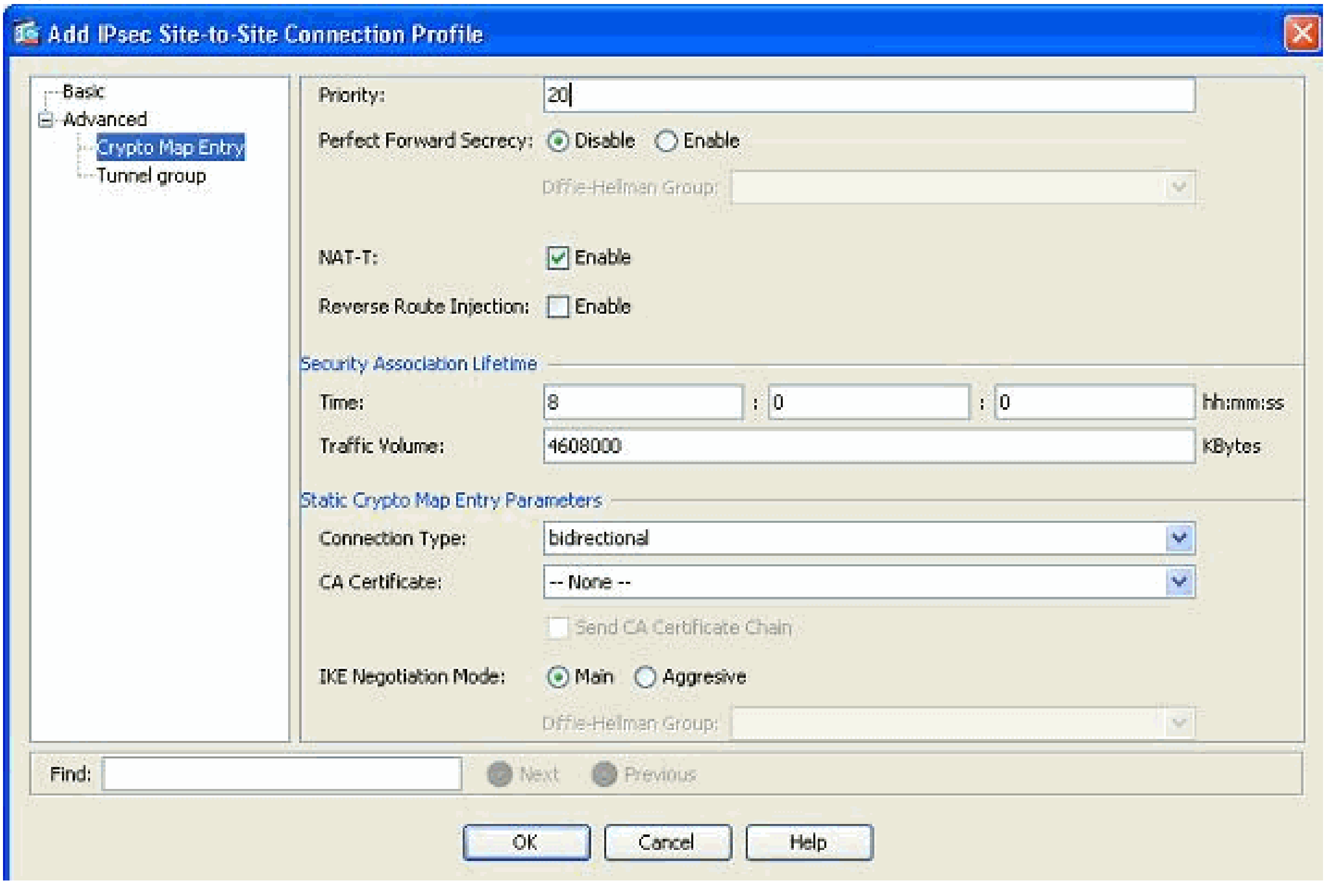
Remote Network: 192.168.25.0/24

Encryption Algorithms

IKE Proposal: pre-share-des-sha, pre-share-3des-sha

IPsec Proposal: S-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5

3. 在「高級」選單下，按一下*加密對映條目*。請參閱*優先順序*索引標籤。此優先順序等於其等效CLI配置中的序列號。當分配的數字小於現有加密對映條目時，將首先執行此新配置檔案。優先順序編號越大，值越小。這用於更改執行特定加密對映的序列順序。按一下*OK*完成新連線配置檔案的建立。



Add IPsec Site-to-Site Connection Profile

Priority: 20

Perfect Forward Secrecy: ● Disable ○ Enable

Diffie-Helman Group:

NAT-T: ☑ Enable

Reverse Route Injection: □ Enable

Security Association Lifetime

Time: 8 : 0 : 0 hh:mm:ss

Traffic Volume: 4608000 KBytes

Static Crypto Map Entry Parameters

Connection Type: bidirectional

CA Certificate: -- None --

□ Send CA Certificate Chain

IKE Negotiation Mode: ● Main ○ Aggresive

Diffie-Helman Group:

這將自動建立新的隧道組以及關聯的加密對映。使用此新的連線配置檔案之前，請確保可以使用新的IP地址訪問BQASA。

編輯現有VPN配置

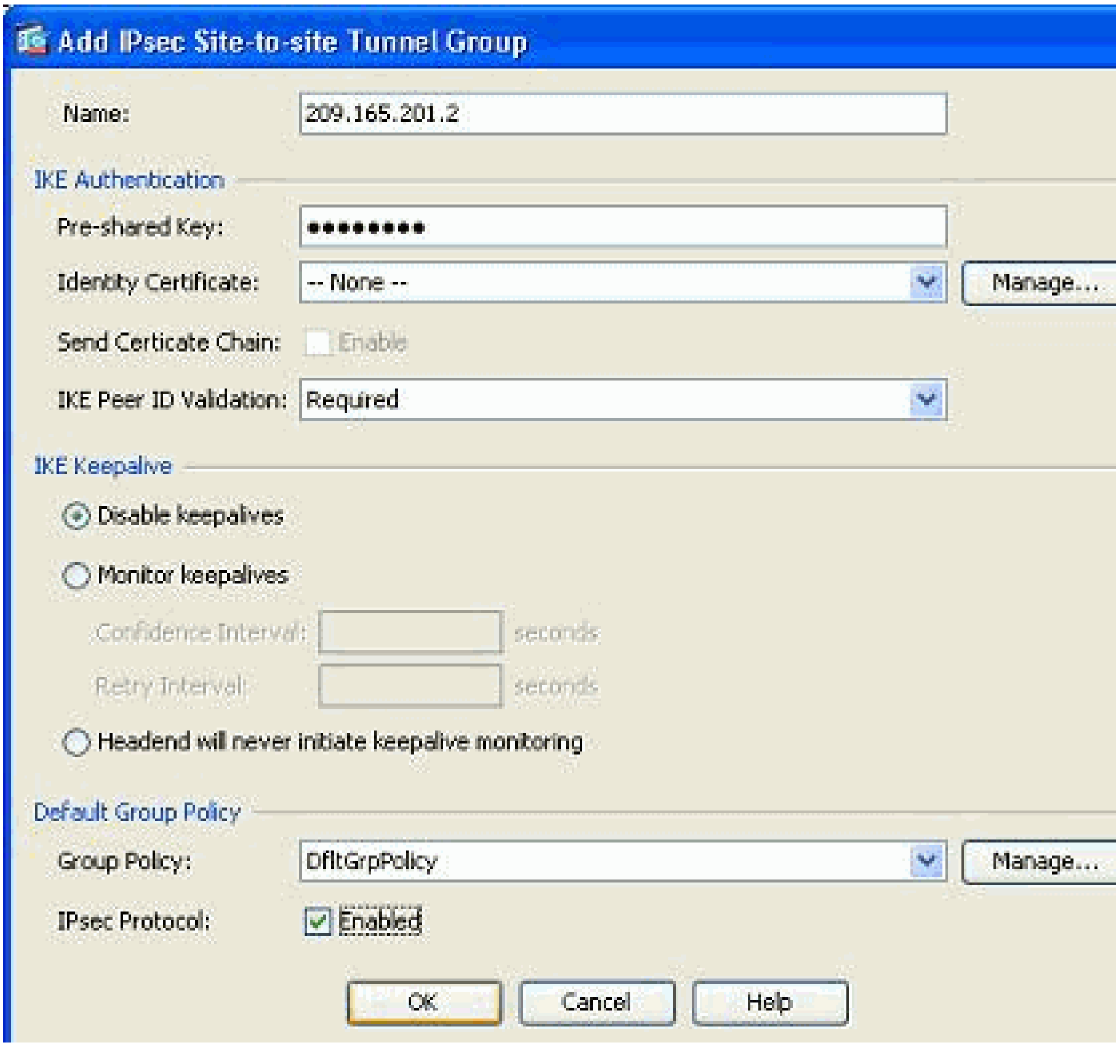
新增新對等體的另一種方法是修改現有配置。無法為新對等體資訊編輯現有連線配置檔案，因為它已繫結到特定對等體。要編輯現有配置，您需要執行以下步驟：

1. 建立新隧道組
2. 編輯現有加密對映

建立新隧道組

轉至*Configuration > Site-to-Site VPN > Advanced > Tunnel groups*，然後按一下*Add*以建立一個包含新VPN對等體資訊的新隧道組。指定*Name*和*Pre-shared Key*欄位，然後按一下*OK*。

注意：確保預共用金鑰與VPN的另一端匹配。



Add IPsec Site-to-site Tunnel Group

Name: 209.165.201.2

IKE Authentication

Pre-shared Key: ●●●●●●●●●

Identity Certificate: -- None --

Send Certicate Chain: □ Enable

IKE Peer ID Validation: Required

IKE Keepalive

● Disable keepalives

○ Monitor keepalives

Confidence Interval: seconds

Retry Interval: seconds

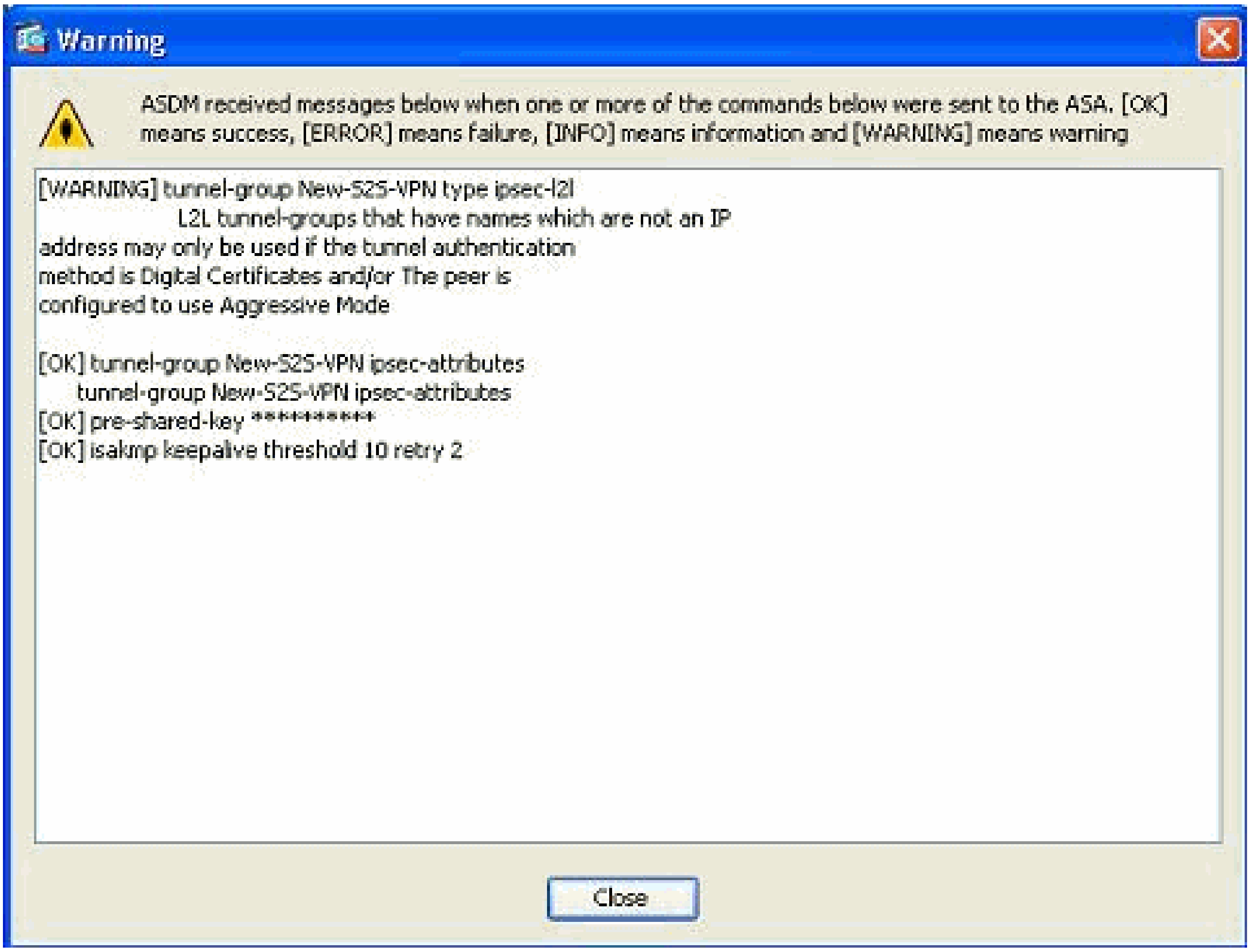
○ Headend will never initiate keepalive monitoring

Default Group Policy

Group Policy: DfltGrpPolicy

IPsec Protocol: ☑ Enabled

注意：在「名稱」欄位中，當身份驗證模式為預共用金鑰時，只應輸入遠端對等體的IP地址。僅當身份驗證方法是通過證書時，才能使用任何名稱。在Name欄位中新增名稱且身份驗證方法為預共用時，將顯示此錯誤：



ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning

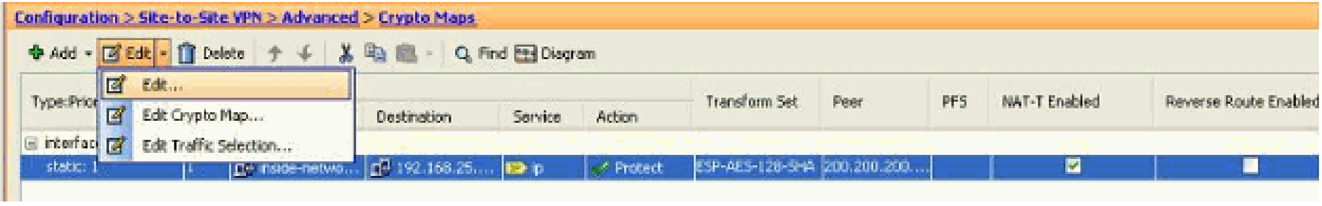
```
[WARNING] tunnel-group New-S2S-VPN type ipsec-l2l
                L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode

[OK] tunnel-group New-S2S-VPN ipsec-attributes
     tunnel-group New-S2S-VPN ipsec-attributes
[OK] pre-shared-key **********
[OK] isakmp keepalive threshold 10 retry 2
```

編輯現有加密對映

可以編輯現有加密對映以關聯新的對等體資訊。

請完成以下步驟：

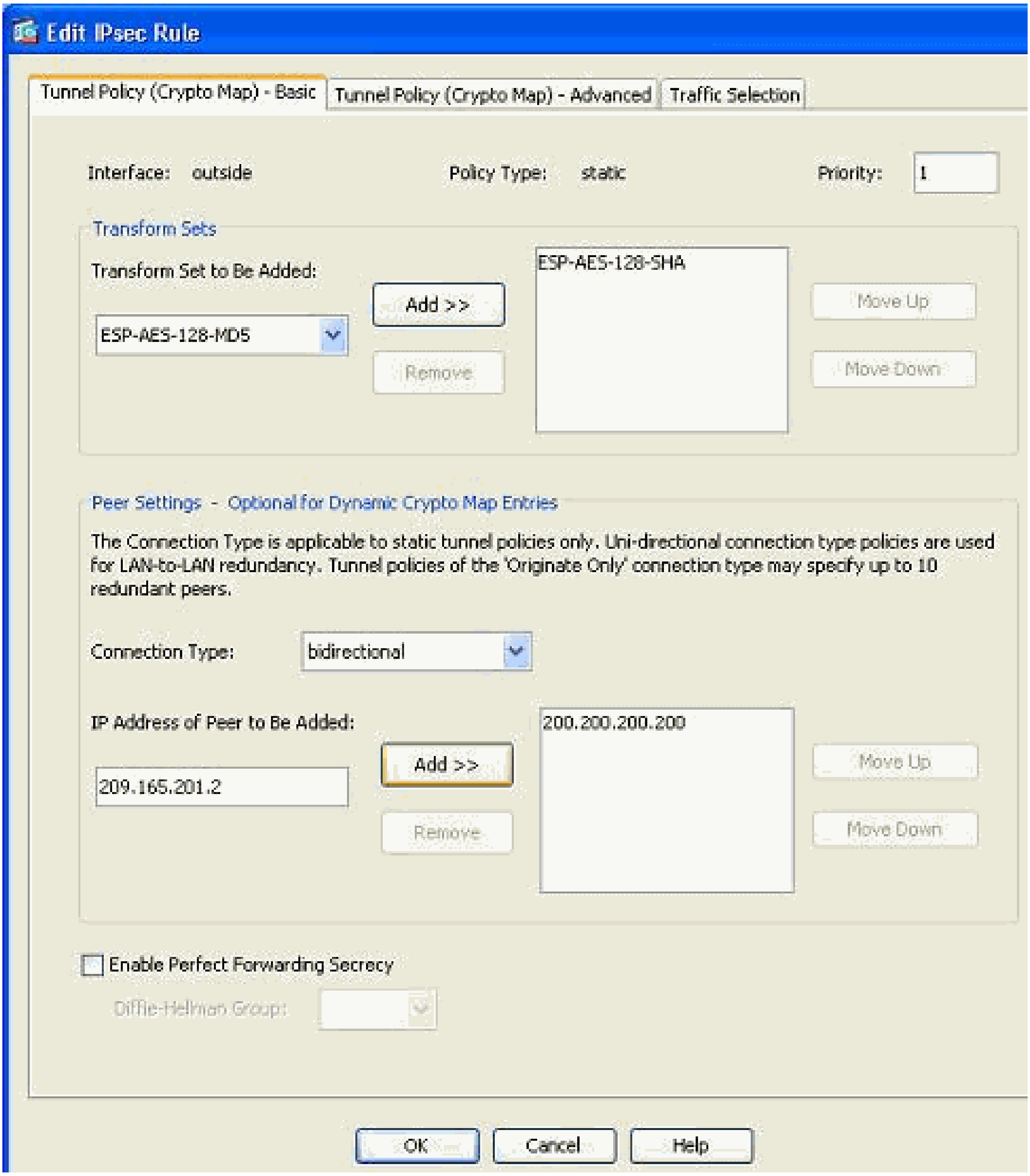
1. 轉到*Configuration > Site-to-Site VPN > Advanced > Crypto Maps*，然後選擇所需的加密對映，然後按一下*Edit*。

   Configuration > Site-to-Site VPN > Advanced > Crypto Maps
Add
Edit
Delete
Find
Diagram
Edit...
Edit Crypto Map...
Edit Traffic Selection...

Type:Prior			Destination	Service	Action	Transform Set	Peer	PFS	NAT-T Enabled	Reverse Route Enabled
⊟ interfac										
static: 1	1	inside-netwo...	192.168.25....	ip	✓ Protect	ESP-AES-128-SHA	200.200.200....		☑	□

   出現*Edit IPSec Rule*視窗。
2. 在Tunnel Policy(Basic)頁籤的Peer Settings區域中，在Peer to be added欄位的IP Address中指定新對等體。然後按一下「*Add*」。



Edit IPsec Rule

Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection

Interface: outside

Policy Type: static

Priority: 1

Transform Sets

Transform Set to Be Added: ESP-AES-128-MD5

Add >>
Remove
Move Up
Move Down

ESP-AES-128-SHA

Peer Settings - Optional for Dynamic Crypto Map Entries

The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.

Connection Type: bidirectional

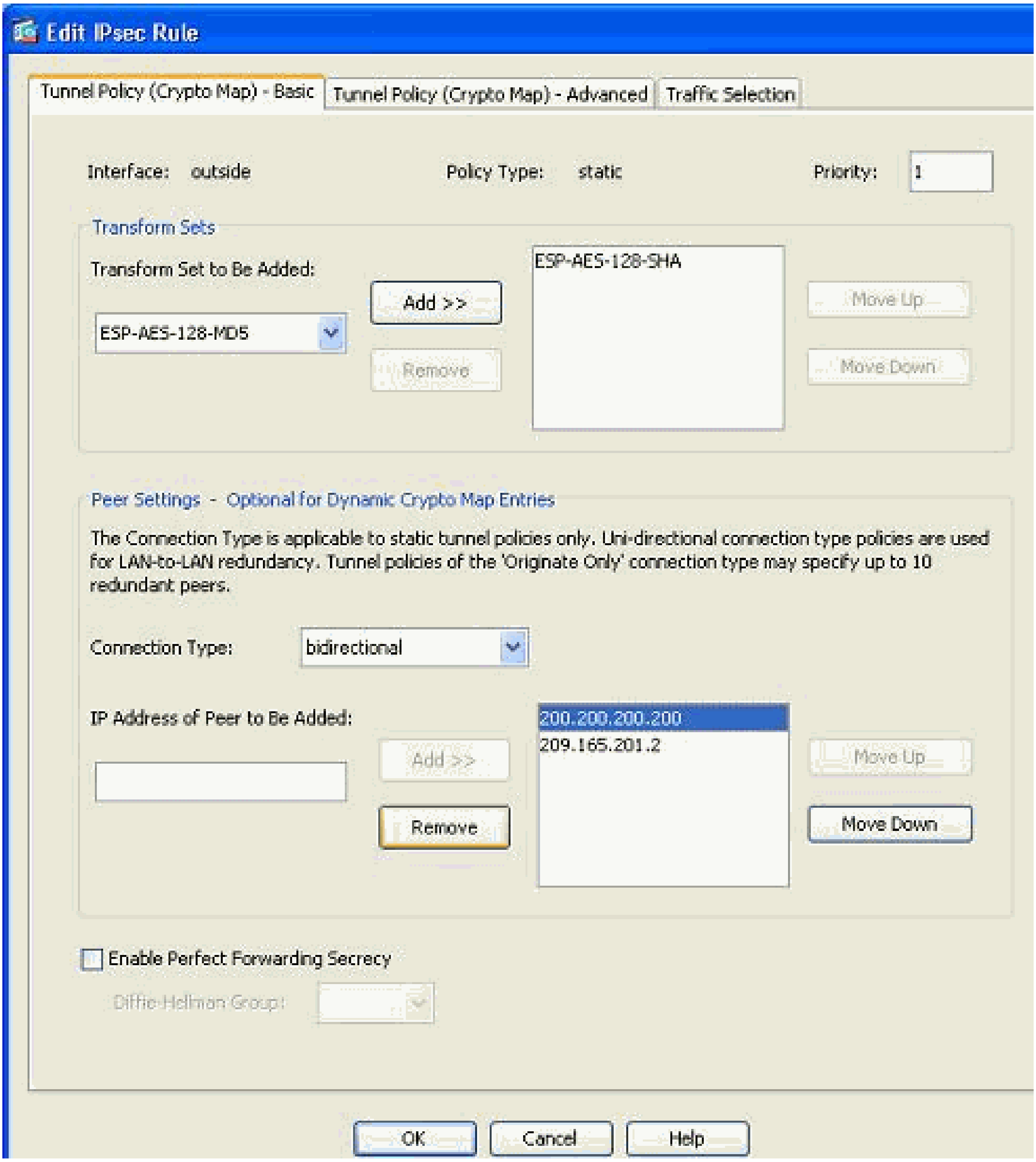
IP Address of Peer to Be Added: 209.165.201.2

200.200.200.200

□ Enable Perfect Forwarding Secrecy

Diffie-Hellman Group:

3. 選擇現有的對等IP地址，然後按一下*Remove*以僅保留新的對等體資訊。按一下「*OK*」（確定）。



Interface: outside

Policy Type: static

Priority: 1

Transform Set to Be Added: ESP-AES-128-MD5

ESP-AES-128-SHA

The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.

Connection Type: bidirectional

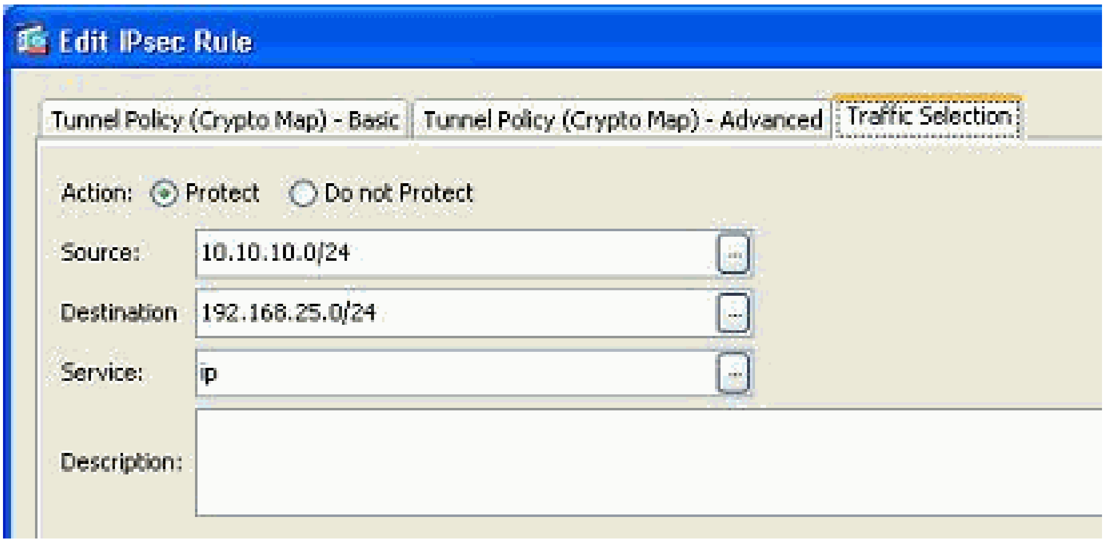
IP Address of Peer to Be Added:

200.200.200.200
209.165.201.2

□ Enable Perfect Forwarding Secrecy

注意：修改當前加密對映中的對等項資訊後，在ASDM視窗中立即刪除與此加密對映關聯的連線配置檔案。

4. 加密網路的詳細資訊保持不變。如果需要修改這些選項，請轉至*Traffic Selection*頁籤。



Edit IPsec Rule

Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection

Action: ● Protect ○ Do not Protect

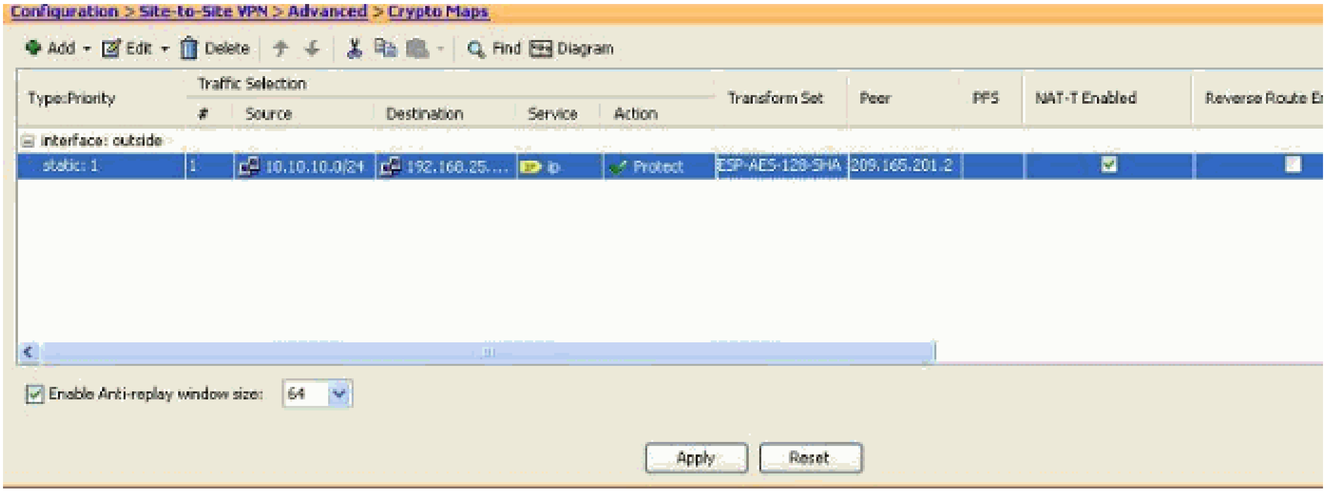
Source: 10.10.10.0/24

Destination 192.168.25.0/24

Service: ip

Description:

5. 轉到*Configuration > Site-to-Site VPN > Advanced > Crypto Maps*窗格以檢視修改的加密對映。但是，這些更改只有在按一下*Apply*後才會發生。按一下*Apply*後，轉到*Configuration > Site-to-Site VPN > Advanced > Tunnel groups*選單以驗證是否存在關聯的隧道組。如果是，則將建立關聯*的連線配*置檔案。



Configuration > Site-to-Site VPN > Advanced > Crypto Maps

Type:Priority	Traffic Selection					Transform Set	Peer	PFS	NAT-T Enabled	Reverse Route E
	#	Source	Destination	Service	Action					
⊟ interface: outside										
static: 1	1	10.10.10.0/24	192.168.25....	ip	✓ Protect	ESP-AES-128-SHA	209.165.201.2		☑	□

☑ Enable Anti-replay window size: 64

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。

- 使用此命令可檢視特定於單個對等體的安全關聯引數：**show crypto ipsec sa peer <Peer IP address>**

疑難排解

使用本節內容，對組態進行疑難排解。

IKE發起程式找不到策略：Intf test_ext， Src:172.16.1.103，夏令時：10.1.4.251

嘗試將VPN對等體從VPN集中器更改為ASA時，日誌消息中會顯示此錯誤。

解決方案：

這可能是在遷移過程中執行的不正確配置步驟的結果。在新增新對等項之前，請確保刪除到介面的加密繫結。此外，請確保使用隧道組中對等體的IP地址，而不是名稱。

相關資訊

- 採用ASA的站點到站點(L2L)VPN
- 最常見的VPN問題
- ASA技術支援頁
- 技術支援與文件 - Cisco Systems