ASA 8.x/ASDM 6.x: Add New VPN Peer Information in an Existing Site-to-Site VPN using ASDM

Contents

Introduction

This document provides information about the configurational changes to make when a new VPN peer is added to the existing site-to-site VPN configuration using Adaptive Security Device Manager (ASDM). This is required in these scenarios:

- The Internet Service Provider (ISP) has been changed and a new set of public IP range is used.
- A complete re-design of the network at a site.
- The device used as VPN gateway at a site is migrated to a new device with a different public IP address.

This document assumes that the site-to-site VPN is already configured properly and works fine. This document provides the steps to follow in order to change a VPN peer information in the L2L VPN configuration.

Prerequisites

Requirements

Cisco recommends that you have knowledge of this topic:

- ASA Site-to-Site VPN configuration example

Components Used

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

- Cisco Adaptative Security Appliance 5500 series with software version 8.2 and later
- Cisco Adapative Security Device Manager with software version 6.3 and later

Conventions

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

Backround information

The site-to-site VPN is working fine between the HQASA and the BQASA. Assume that the BQASA has got a complete network re-design and the IP schema has been modified at the ISP level, but all the internal subnetwork details remain the same.

This sample configuration uses these IP addresses:

- Existing BQASA Outside IP address - 200.200.200.200
- New BQASA Outside IP address - 209.165.201.2

Note: Here, only the peer information will be modified. Because there is no other change in internal subnet, the crypto access-lists remain the same.

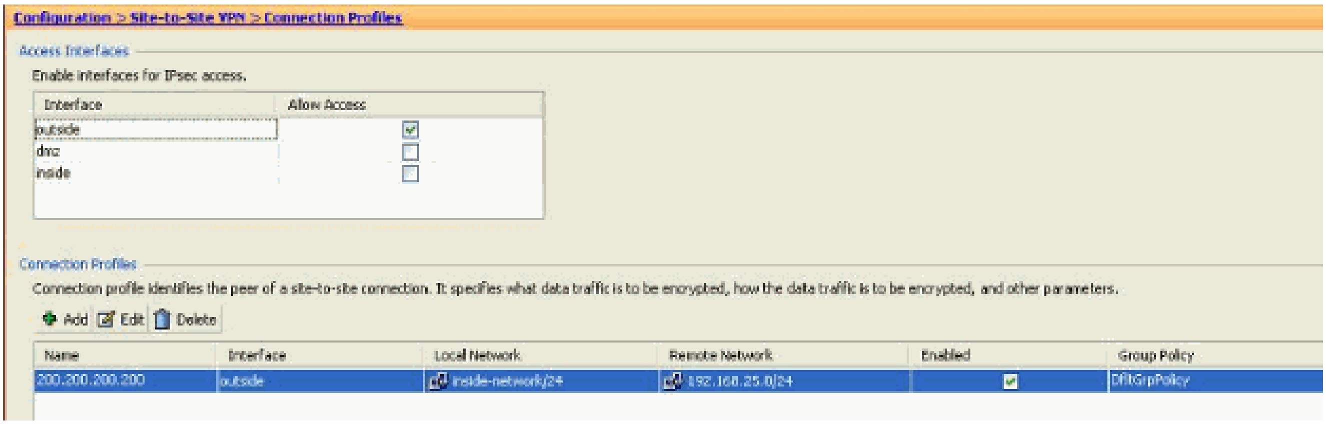
ASDM Configuration

This section provides information about the possible methods used to change VPN peer information on HQASA using the ASDM.

Create a New Connection Profile

This can be the easier method because it does not disturb the existing VPN configuration and can create a new connection profile with the new VPN peer related information.

1. Go to *Configuration* > *Site-to-Site VPN* > *Connection Profiles* and click *Add* under the Connection Profiles
   area.



Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
outside	☑
dmz	□
inside	□

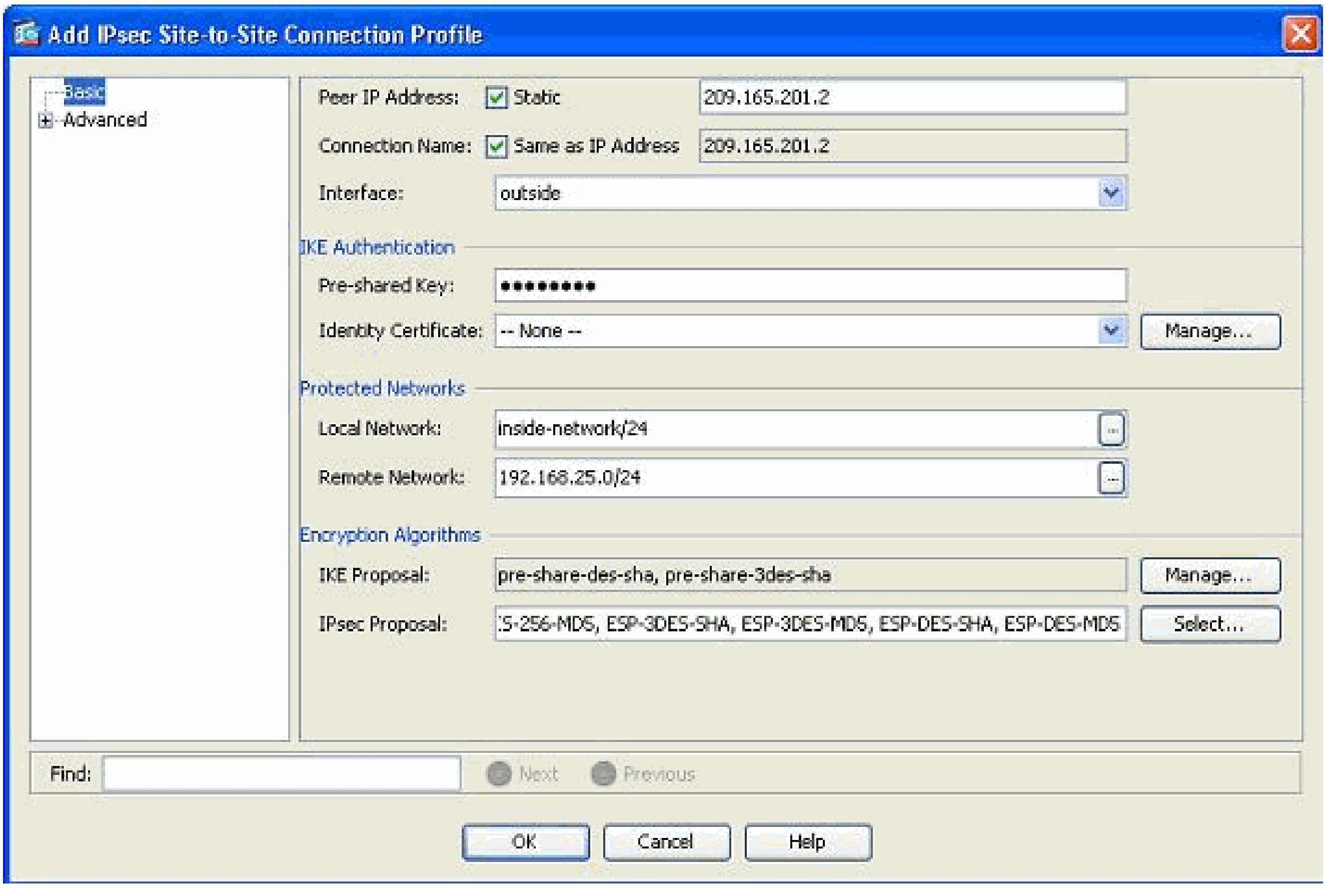
Connection Profiles

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

The *Add IPSec Site-to-Site Connection Profile* window opens up.

2. Under the Basic tab, provide the details for *Peer IP Address*, *Pre-shared Key*, and *Protected Networks*. Use all the same parameters as the existing VPN, except the peer information. Click
OK.



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

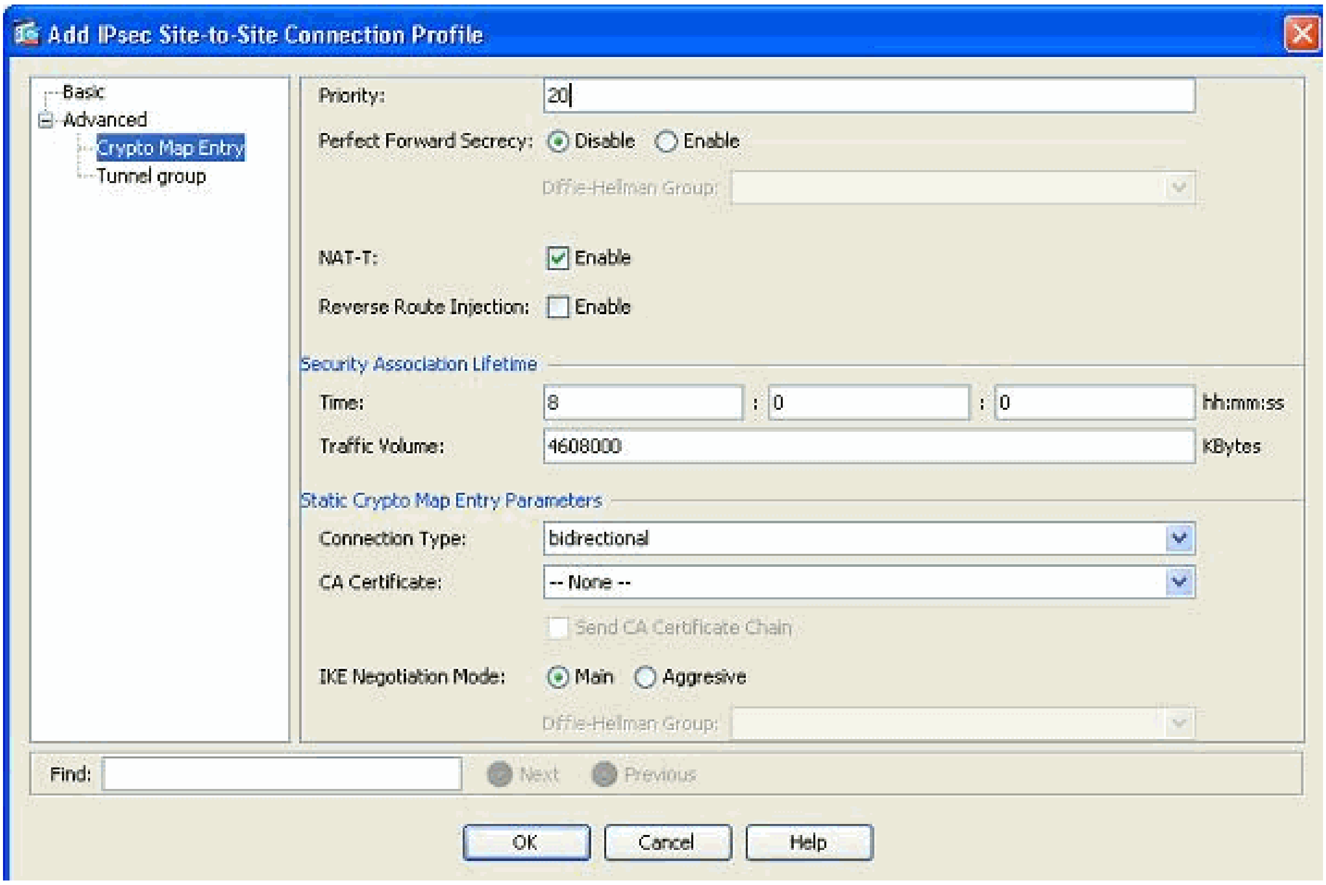
Remote Network: 192.168.25.0/24

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. Under the Advanced menu, click *Crypto Map Entry*. Refer to the *Priority* tab. This Priority is equal to the sequence number in its equivalent CLI configuration. When a lesser number than the existing crypto map entry is assigned, this new profile is executed first. The higher the priority number, the lesser the value. This is used to change the order of sequence that a specific crypto map will be executed. Click *OK* to complete creating the new connection profile.



Priority: 20

Perfect Forward Secrecy: ● Disable ○ Enable

Diffie-Hellman 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-Hellman Group:

This automatically creates a new tunnel-group along with an associated crypto map. Make sure you can reach the BQASA with the new IP address before you use this new connection profile.

Edit the Existing VPN Configuration

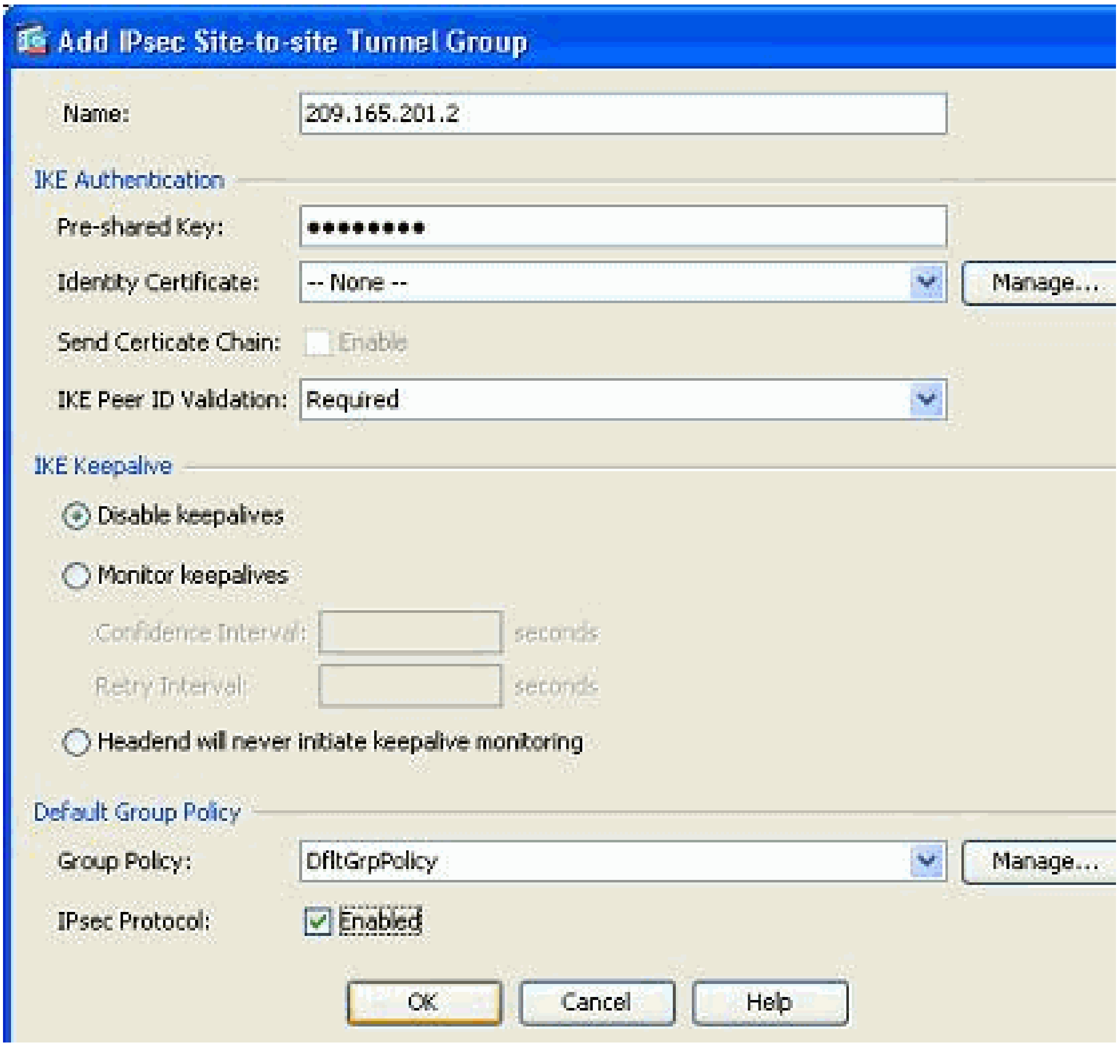
Another way of adding a new peer is to modify the existing configuration. The existing connection profile cannot be edited for the new peer information because it is bound to a specific peer. In order to edit the existing configuration, you need to perform these steps:

1. Create a New Tunnel Group
2. Edit the Existing Crypto Map

Create a New Tunnel Group

Go to *Configuration* > *Site-to-Site VPN* > *Advanced* > *Tunnel groups* and click *Add* to create a new tunnel-group that contains the new VPN peer information. Specify the *Name* and *Pre-shared Key* fields, then click *OK*.

Note: Make sure the Pre-shared Key matches the other end of the VPN.



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

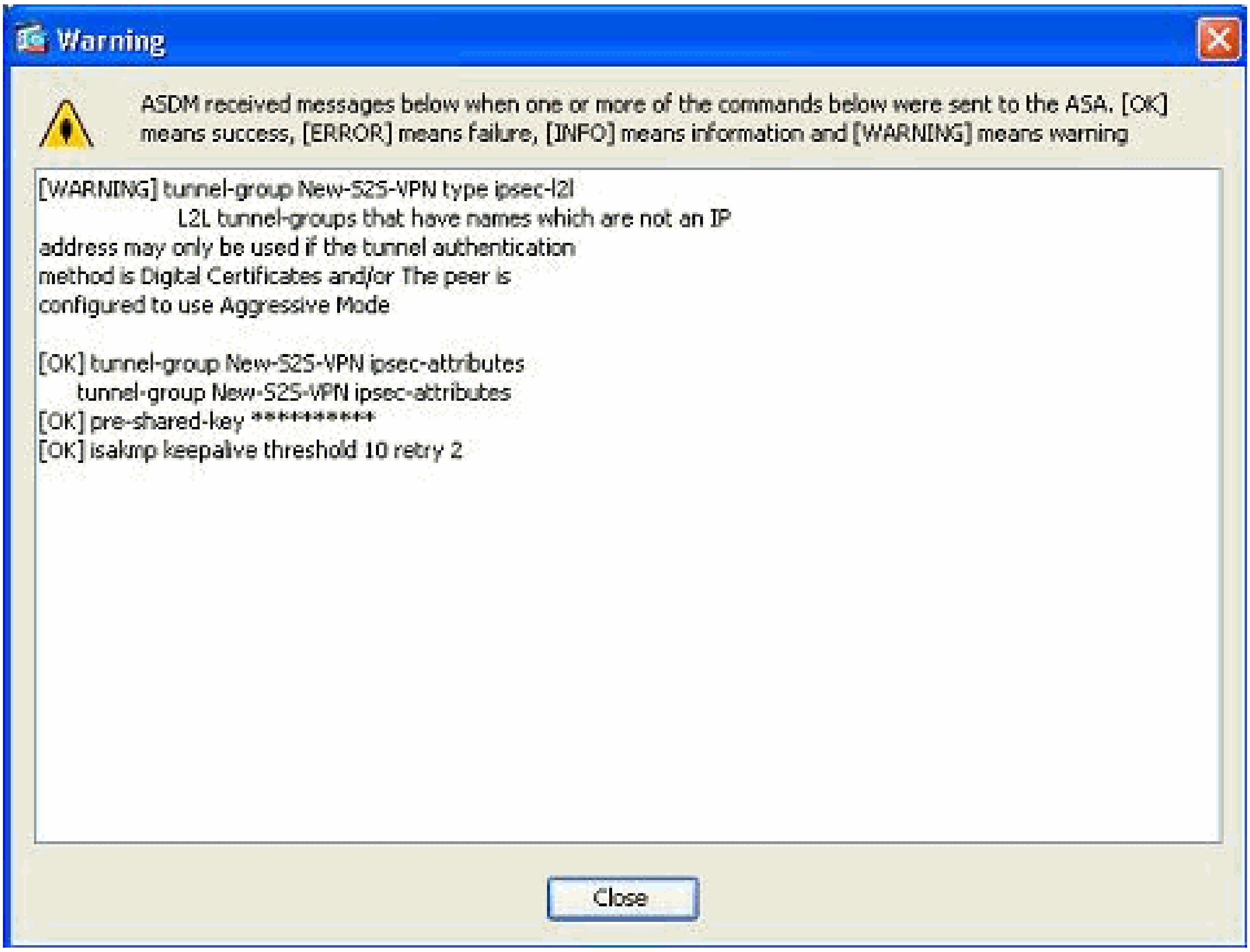
○ Headend will never initiate keepalive monitoring

Default Group Policy

Group Policy: DfltGrpPolicy

IPsec Protocol: ☑ Enabled

Note: In the Name field, only the IP address of the remote peer should be entered when the authentication mode is pre-shared keys. Any name can be used only when the authentication method is through certificates. This error appears when a name is added in the Name field and the authentication method is pre-shared:



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

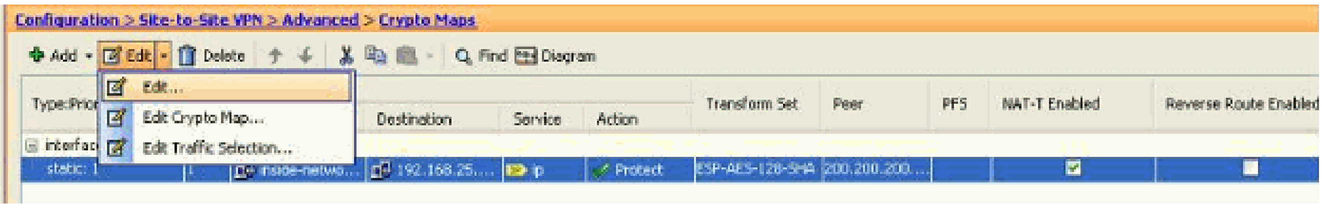
```
[WARNING] tunnel-group New-S2S-VPN type ipsec-l2l
                L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode

[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
```

Edit the Existing Crypto Map

The existing crypto map can be edited in order to associate the new peer information.

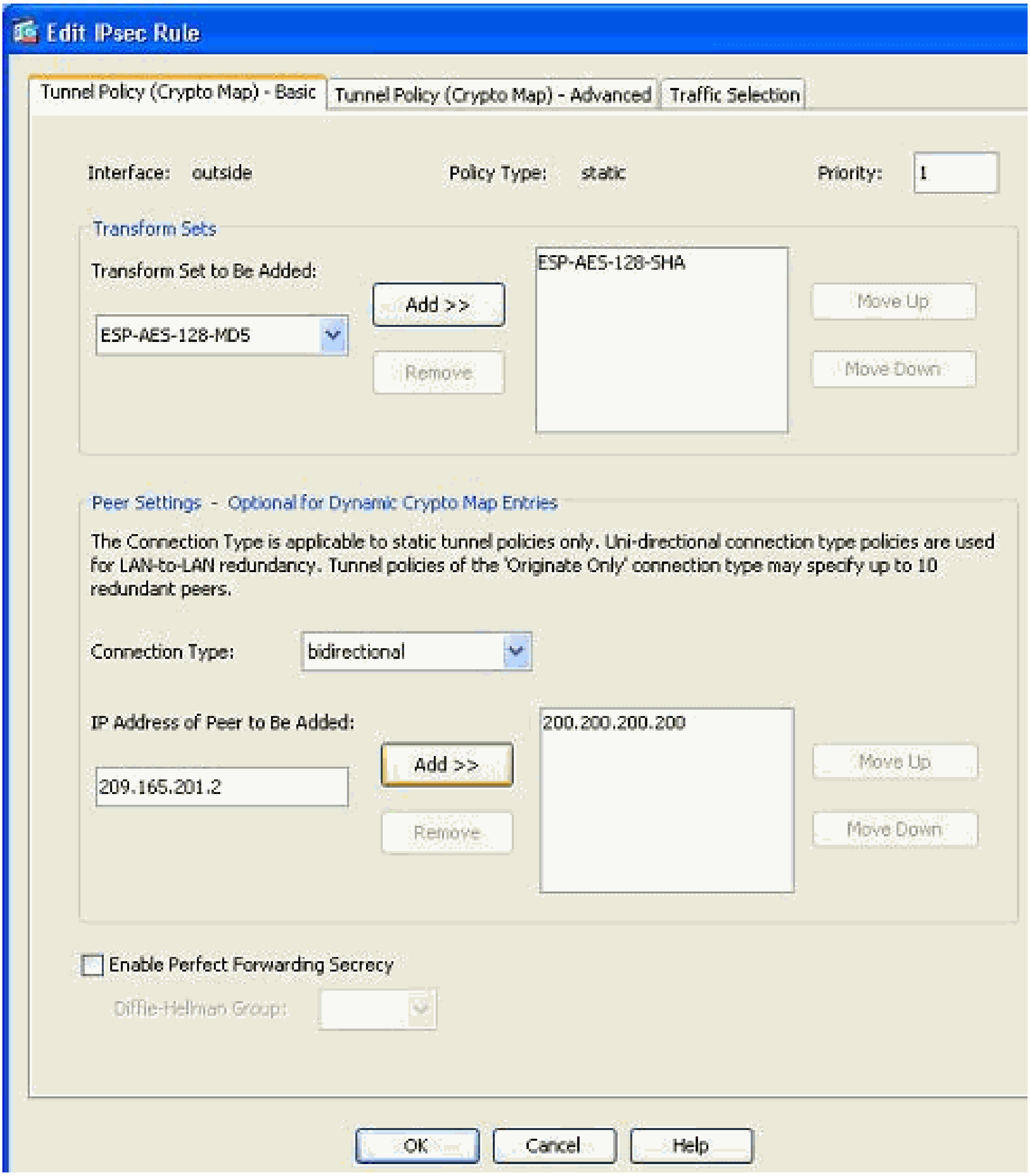
Complete these steps:

1. Go to *Configuration* > *Site-to-Site VPN* > *Advanced* > *Crypto Maps*, then select the required crypto map and click *Edit*.



The *Edit IPSec Rule* window appears.

2. Under the Tunnel Policy (Basic) tab, in the Peer Settings area, specify the new peer in the IP Address of Peer to be added field. Then, click *Add*.


Edit IPsec Rule
Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection
Transform Sets
Add >>
Remove
Move Up
Move Down
Peer Settings - Optional for Dynamic Crypto Map Entries
Add >>
Remove
Move Up
Move Down
OK
Cancel
Help

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

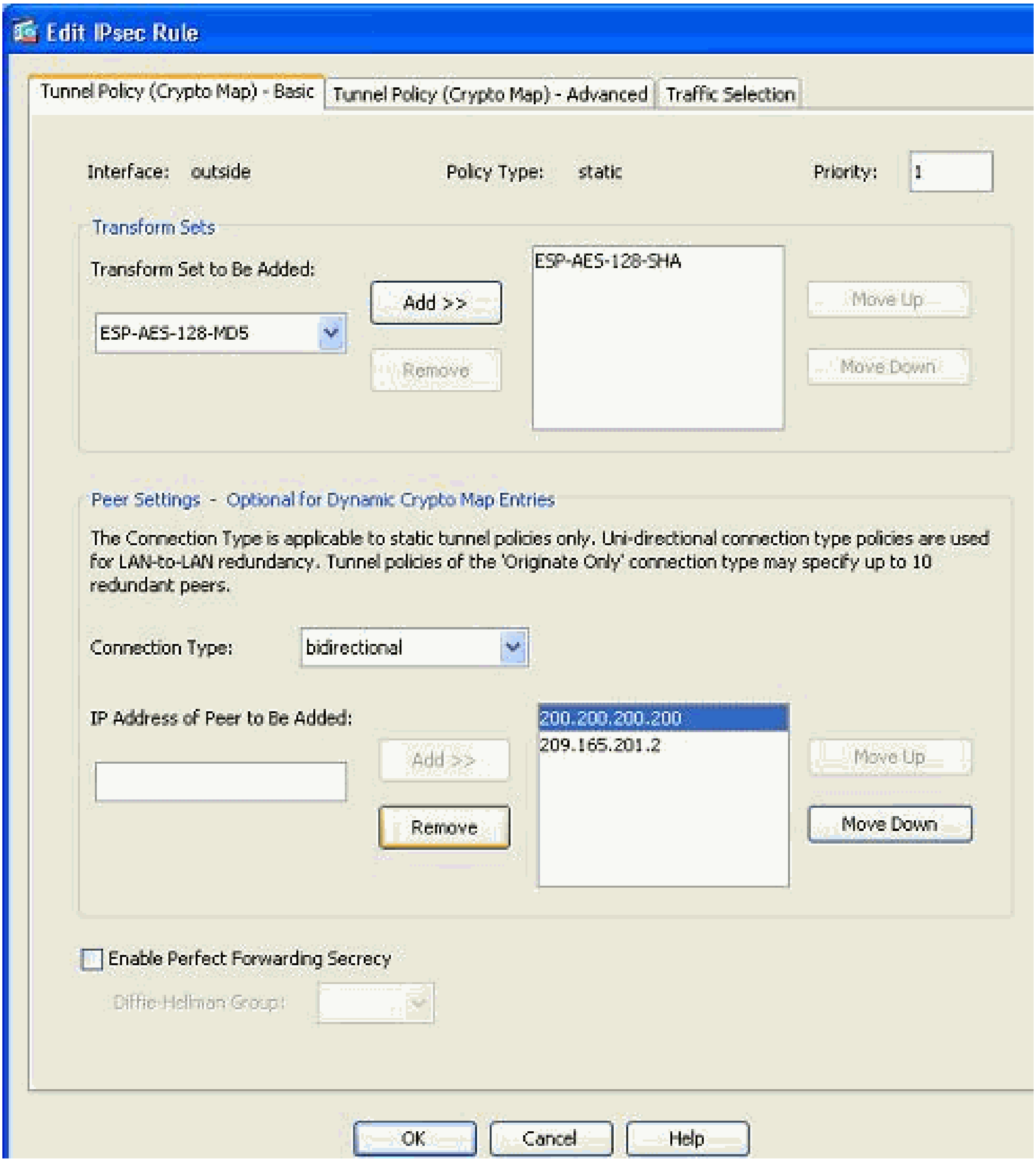
IP Address of Peer to Be Added: 209.165.201.2

200.200.200.200

□ Enable Perfect Forwarding Secrecy

Diffie-Hellman Group:

3. Select the existing peer IP address and click *Remove* to retain the new peer information only. Click
   OK.



Edit IPsec Rule
Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection
Transform Sets
Add >>
Remove
Move Up
Move Down
Peer Settings - Optional for Dynamic Crypto Map Entries
Add >>
Remove
Move Up
Move Down
OK
Cancel
Help

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

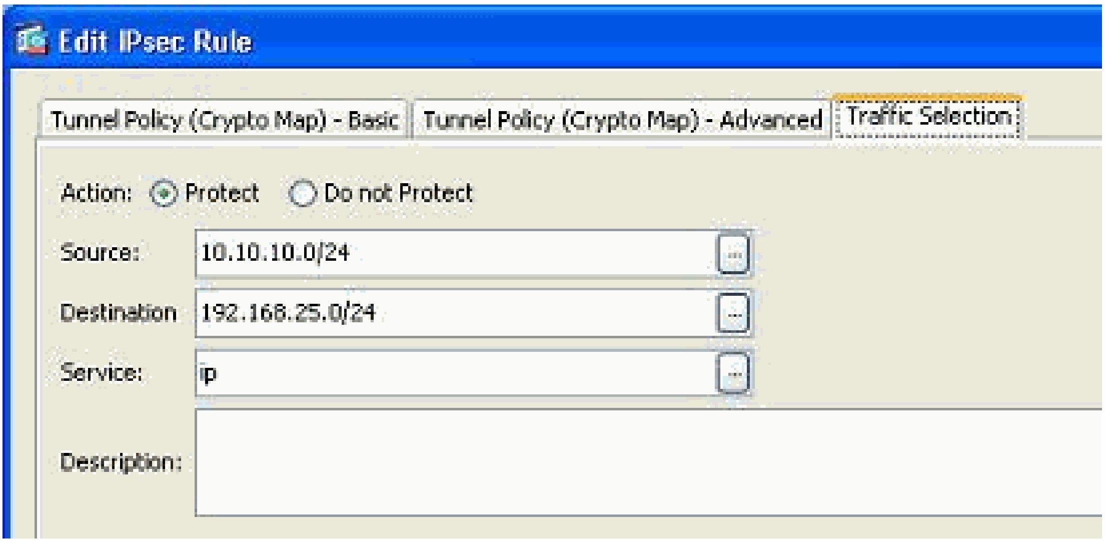
□ Enable Perfect Forwarding Secrecy

Diffie-Hellman Group:

Note: After you modify the peer information in the current crypto map, the Connection Profile associated with this crypto map is deleted instantly in the ASDM window.

4. The details of the encrypted networks remain the same. If you need to modify these, go to the *Traffic Selection*

tab.


Edit IPsec Rule
Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection

Action: ● Protect ○ Do not Protect

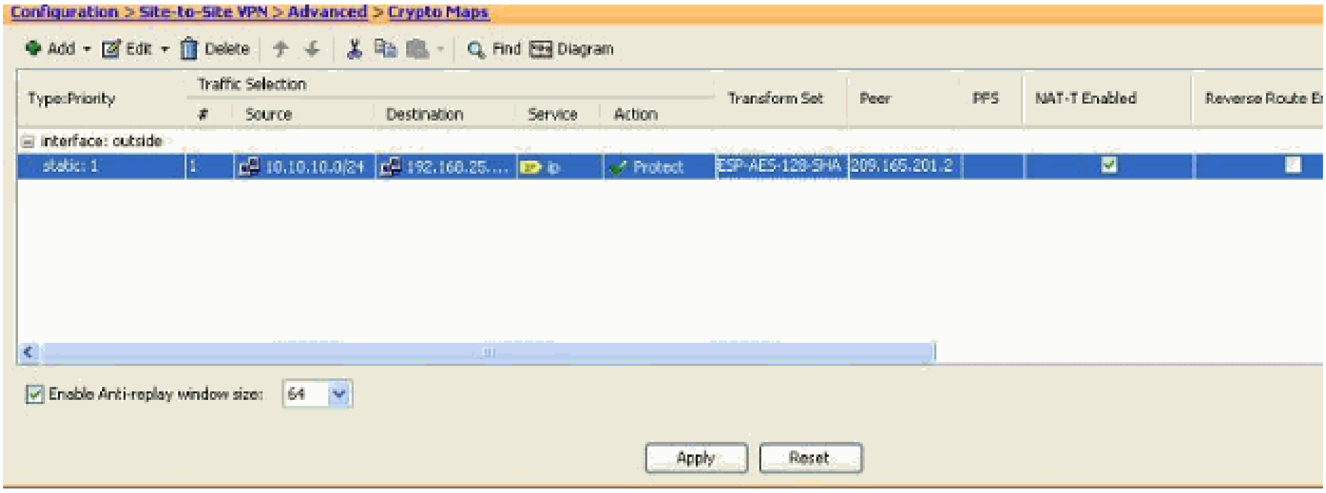
Source: 10.10.10.0/24

Destination 192.168.25.0/24

Service: ip

Description:

5. Go to the *Configuration* > *Site-to-Site VPN* > *Advanced* > *Crypto Maps* pane in order to view the modified crypto map. However, these changes do not take place until you click *Apply*. After you click *Apply*, go to the *Configuration* > *Site-to-Site VPN* > *Advanced* > *Tunnel groups* menu in order to verify if an associated tunnel-group is present or not. If yes, then an associated *Connection Profile* will be created.



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

Verify

Use this section in order 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.

- Use this command to view the security association parameters specific to a single peer:**show crypto ipsec sa peer <Peer IP address>**

Troubleshoot

Use this section to troubleshoot your configuration.

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

This error is displayed in the log messages when trying to change the VPN peer from a VPN concentrator to ASA.

Solution:

This can be a result of improper configuration steps followed during the migration. Ensure that the crypto binding to the interface is removed before you add a new peer. Also, make sure that you used the IP address of the peer in the tunnel-group, but not the name.

Related Information

- **Site to Site (L2L) VPN with ASA**
- **Most Common VPN Problems**
- **ASA Technical Support Page**
- **Technical Support & Documentation - Cisco Systems**