ASA 8.x/ASDM 6.x: Hinzufügen neuer VPN-Peer-Informationen in einem vorhandenen Site-to-Site-VPN mithilfe von ASDM

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Hintergrundinformationen
ASDM-Konfiguration
Erstellen eines neuen Verbindungsprofils
Bearbeiten der vorhandenen VPN-Konfiguration
Überprüfen
Fehlerbehebung
IKE Initiator kann die Richtlinie nicht finden: Intf test_ext, Src: 172.16.1.103, Dst: 10.1.4.251
Zugehörige Informationen

Einführung

Dieses Dokument enthält Informationen zu Konfigurationsänderungen, die vorgenommen werden müssen, wenn der vorhandenen Site-to-Site-VPN-Konfiguration mithilfe des Adaptive Security Device Manager (ASDM) ein neuer VPN-Peer hinzugefügt wird. Dies ist in folgenden Szenarien erforderlich:

- Der Internet Service Provider (ISP) wurde geändert, und es wird ein neuer öffentlicher IP-Bereich verwendet.
- Umgestaltung des Netzwerks am Standort
- Das Gerät, das als VPN-Gateway an einem Standort verwendet wird, wird auf ein neues Gerät mit einer anderen öffentlichen IP-Adresse migriert.

In diesem Dokument wird davon ausgegangen, dass das Site-to-Site-VPN bereits richtig konfiguriert ist und einwandfrei funktioniert. Dieses Dokument enthält die Schritte zum Ändern von VPN-Peer-Informationen in der L2L-VPN-Konfiguration.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in diesem Bereich zu verfügen:

- ASA Site-to-Site-VPN-Konfigurationsbeispiel

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adapative Security Appliance der Serie 5500 mit Softwareversion 8.2 und höher
- Cisco Adaptive Security Device Manager ab Softwareversion 6.3

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Das Site-to-Site-VPN funktioniert zwischen der HQASA und der BQASA einwandfrei. Angenommen, die BQASA verfügt über ein vollständiges Netzwerkdesign und das IP-Schema wurde auf ISP-Ebene geändert, aber alle internen Subnetzwerkdetails bleiben unverändert.

In dieser Beispielkonfiguration werden folgende IP-Adressen verwendet:

- Externe BQASA-IP-Adresse - 200.200.200.200
- Neue externe BQASA-IP-Adresse - 209.165.201.2

Hinweis: Hier werden nur die Peer-Informationen geändert. Da es keine andere Änderung im internen Subnetz gibt, bleiben die Krypto-Zugriffslisten unverändert.

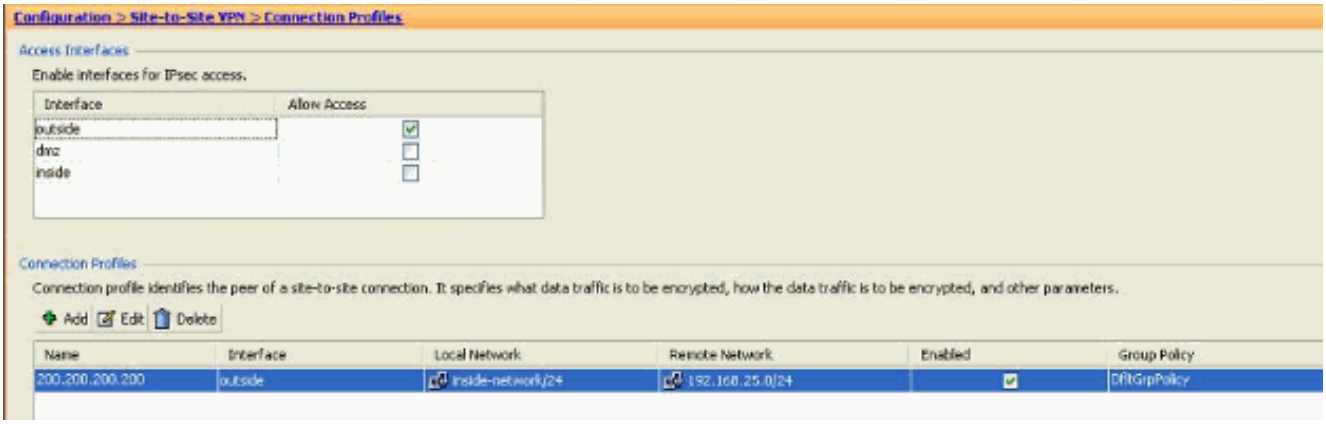
ASDM-Konfiguration

Dieser Abschnitt enthält Informationen zu den möglichen Methoden zum Ändern von VPN-Peer-Informationen auf HQASA mithilfe des ASDM.

Erstellen eines neuen Verbindungsprofils

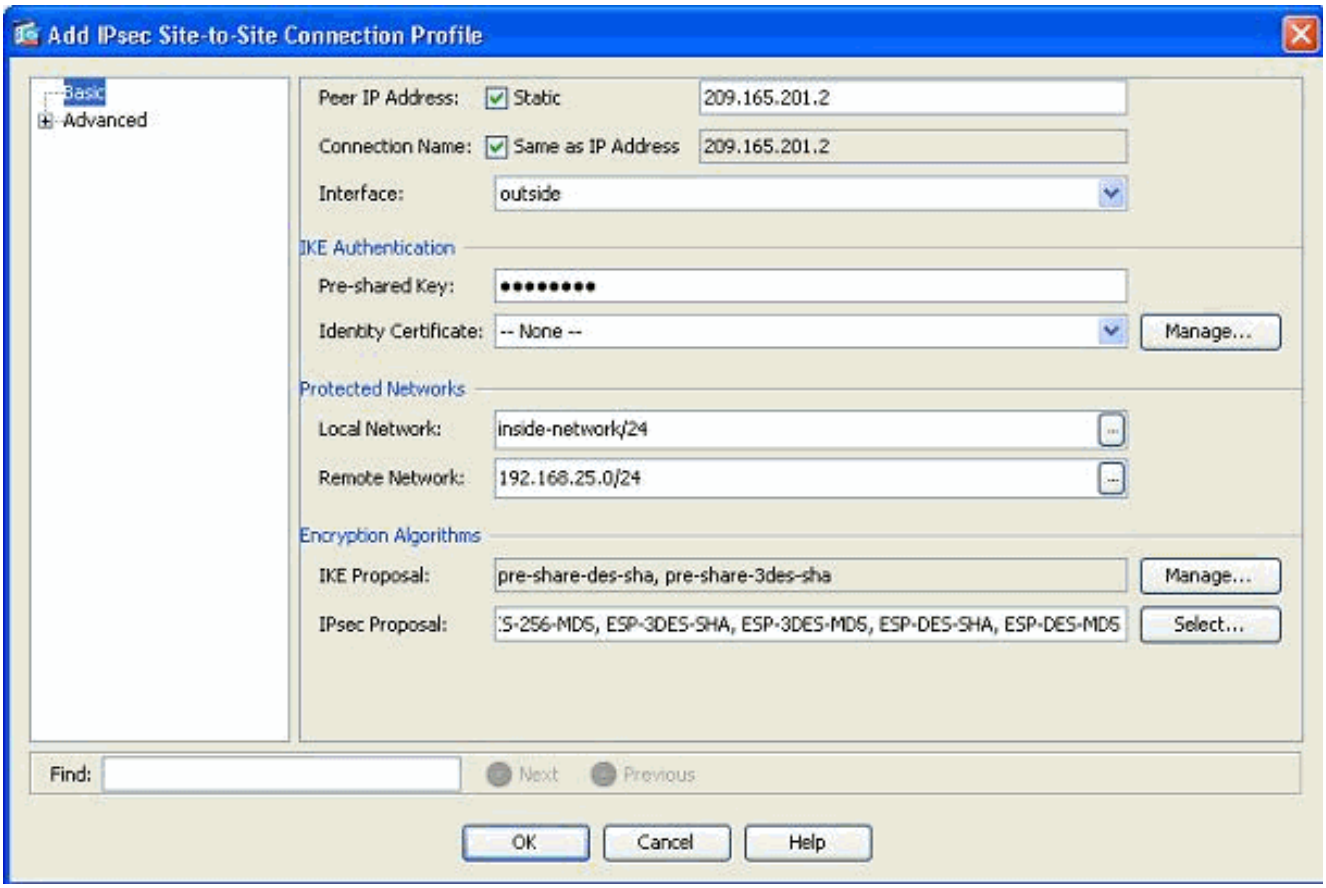
Dies kann die einfachere Methode sein, da sie die bestehende VPN-Konfiguration nicht stört und ein neues Verbindungsprofil mit den neuen VPN-Peer-Informationen erstellen kann.

1. Gehen Sie zu *Konfiguration > Site-to-Site-VPN > Verbindungsprofile,* und klicken Sie im Bereich Verbindungsprofile auf *Hinzufügen*.

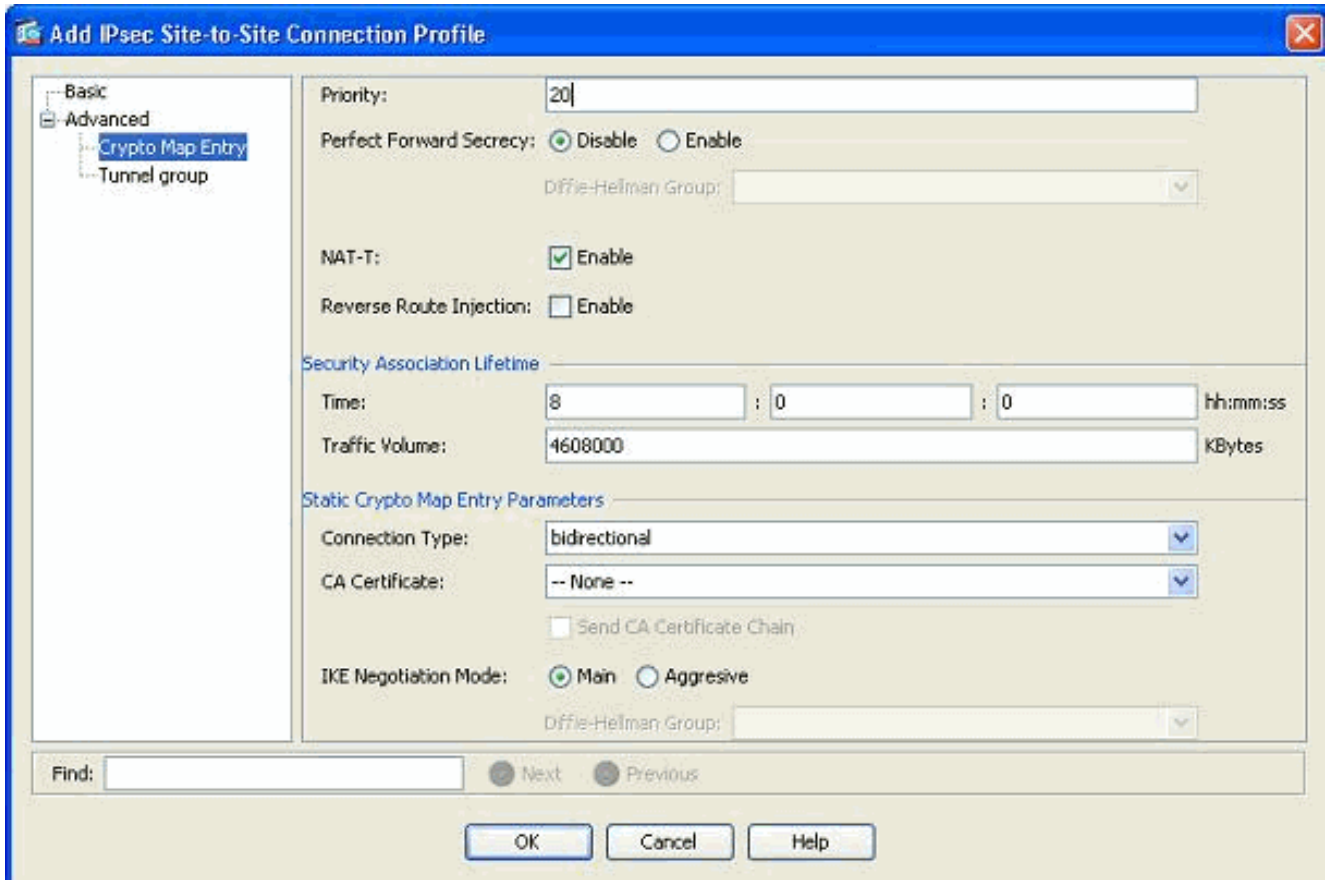


Das Fenster *IPSec Site-to-Site-Verbindungsprofil hinzufügen* wird geöffnet.

2. Geben Sie auf der Registerkarte Basic (Grundlegend) Details für die *Peer-IP-Adresse*, den *vorinstallierten Schlüssel* und *geschützte Netzwerke an*. Verwenden Sie mit Ausnahme der Peer-Informationen dieselben Parameter wie das vorhandene VPN. Klicken Sie auf *OK*.



3. Klicken Sie im Menü Erweitert auf *Crypto Map Entry (Crypto Map-Eintrag)*. Weitere Informationen finden Sie auf der Registerkarte *Priorität*. Diese Priorität entspricht der Sequenznummer in der entsprechenden CLI-Konfiguration. Wenn eine geringere Zahl als der vorhandene Crypto Map-Eintrag zugewiesen wird, wird dieses neue Profil zuerst ausgeführt. Je höher die Prioritätsnummer, desto geringer ist der Wert. Mit diesem Befehl wird die Reihenfolge geändert, in der eine bestimmte Crypto Map ausgeführt wird. Klicken Sie auf *OK*, um das Erstellen des neuen Verbindungsprofils abzuschließen.



Dadurch wird automatisch eine neue Tunnelgruppe zusammen mit einer zugeordneten Crypto Map erstellt. Stellen Sie sicher, dass Sie das BQASA mit der neuen IP-Adresse erreichen können, bevor Sie dieses neue Verbindungsprofil verwenden.

Bearbeiten der vorhandenen VPN-Konfiguration

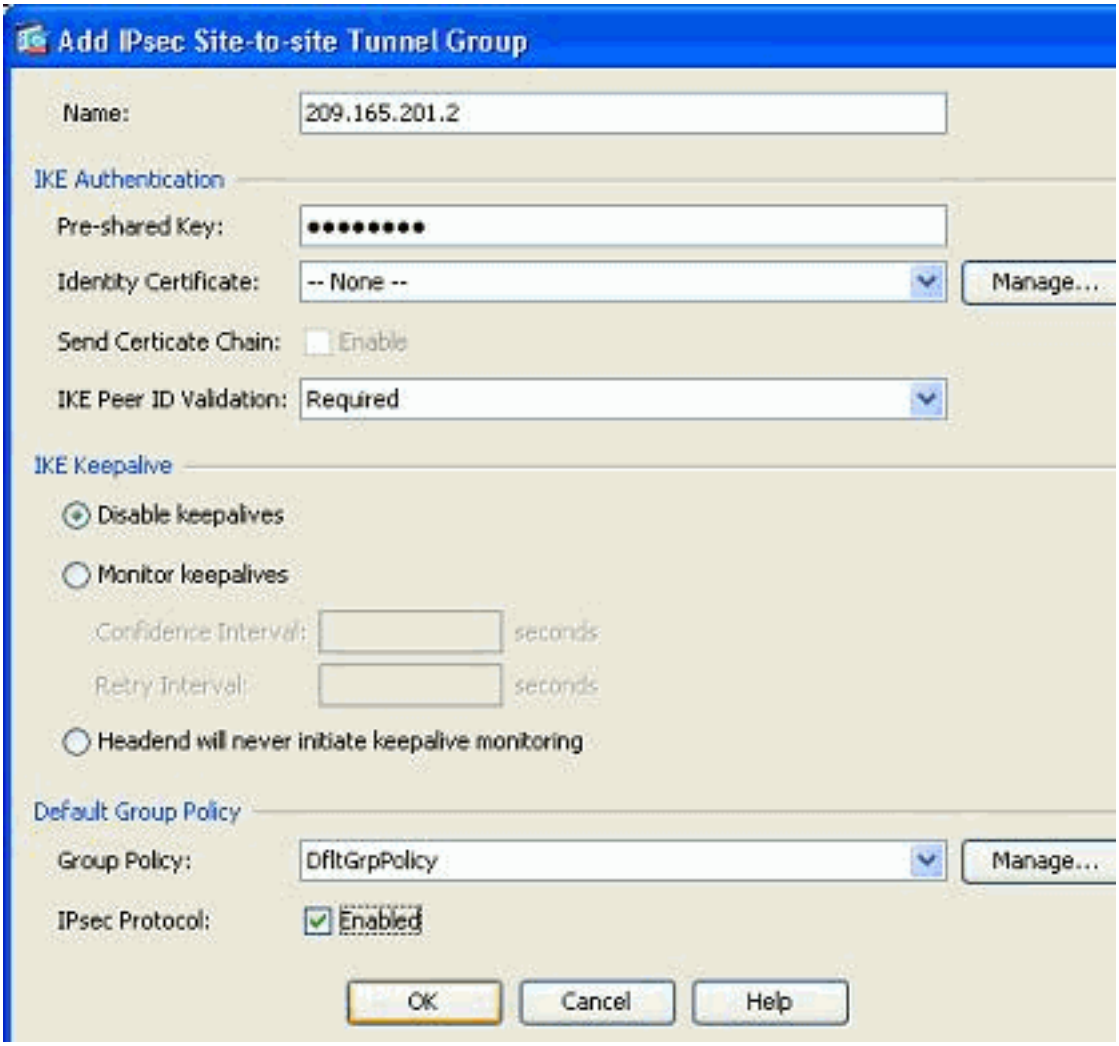
Eine andere Möglichkeit zum Hinzufügen eines neuen Peers besteht darin, die vorhandene Konfiguration zu ändern. Das vorhandene Verbindungsprofil kann für die neuen Peer-Informationen nicht bearbeitet werden, da es an einen bestimmten Peer gebunden ist. Um die vorhandene Konfiguration zu bearbeiten, müssen Sie die folgenden Schritte ausführen:

1. Neue Tunnelgruppe erstellen
2. Bearbeiten der vorhandenen Crypto Map

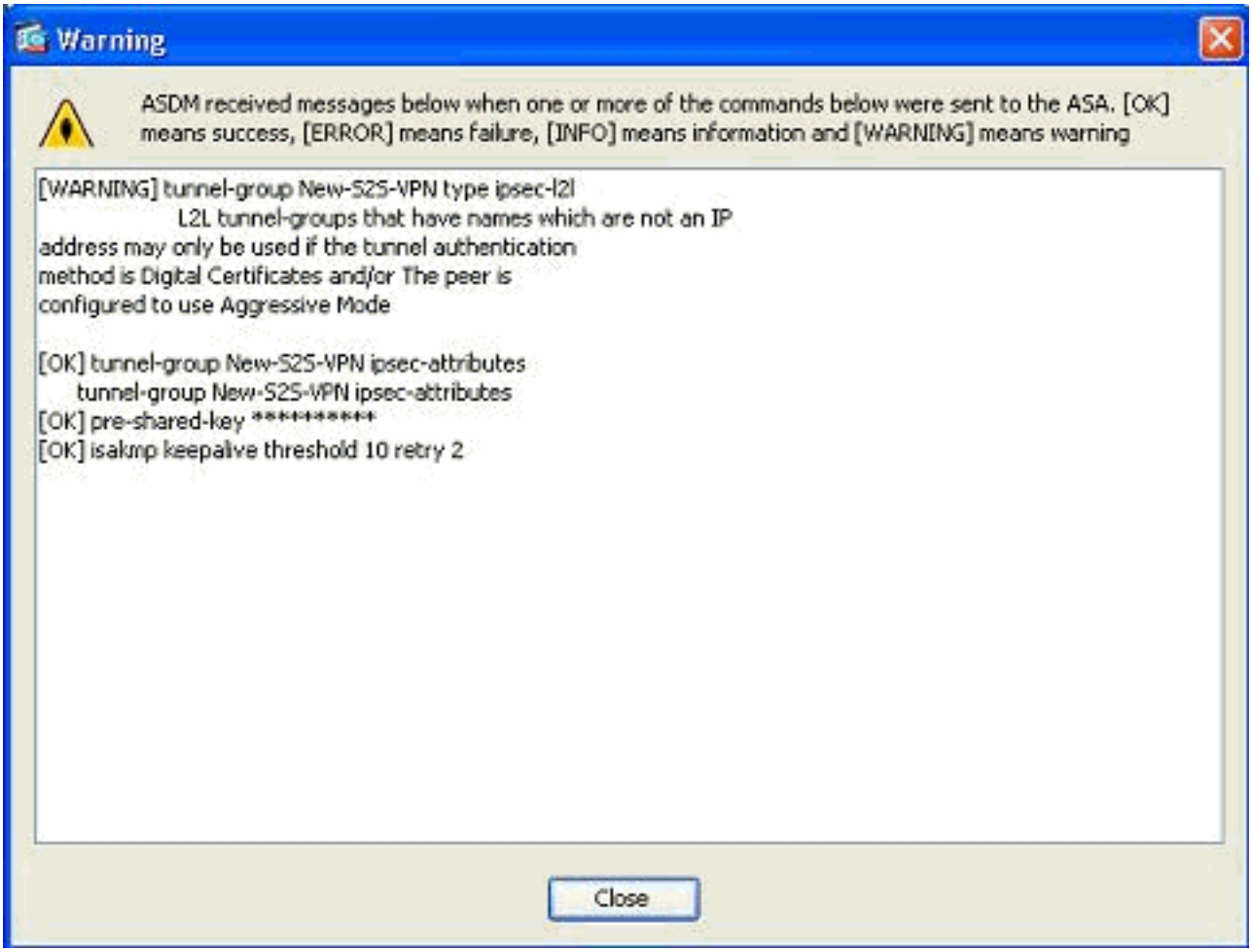
Neue Tunnelgruppe erstellen

Gehen Sie zu *Konfiguration > Site-to-Site-VPN > Erweitert > Tunnel-Gruppen,* und klicken Sie auf *Hinzufügen*, um eine neue Tunnelgruppe zu erstellen, die die neuen VPN-Peer-Informationen enthält. Geben Sie die Felder *Name* und *Vorinstallierter Schlüssel* an, und klicken Sie dann auf *OK*.

Hinweis: Vergewissern Sie sich, dass der Pre-shared Key mit dem anderen Ende des VPN übereinstimmt.



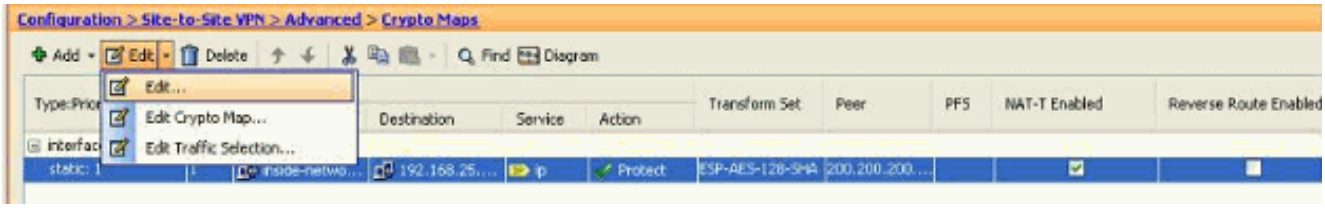
Hinweis: Im Feld Name sollte nur die IP-Adresse des Remote-Peers eingegeben werden, wenn es sich bei dem Authentifizierungsmodus um vorinstallierte Schlüssel handelt. Jeder Name kann nur verwendet werden, wenn die Authentifizierungsmethode über Zertifikate verfügt. Dieser Fehler wird angezeigt, wenn im Feld Name ein Name hinzugefügt wird und die Authentifizierungsmethode vorab freigegeben wurde:



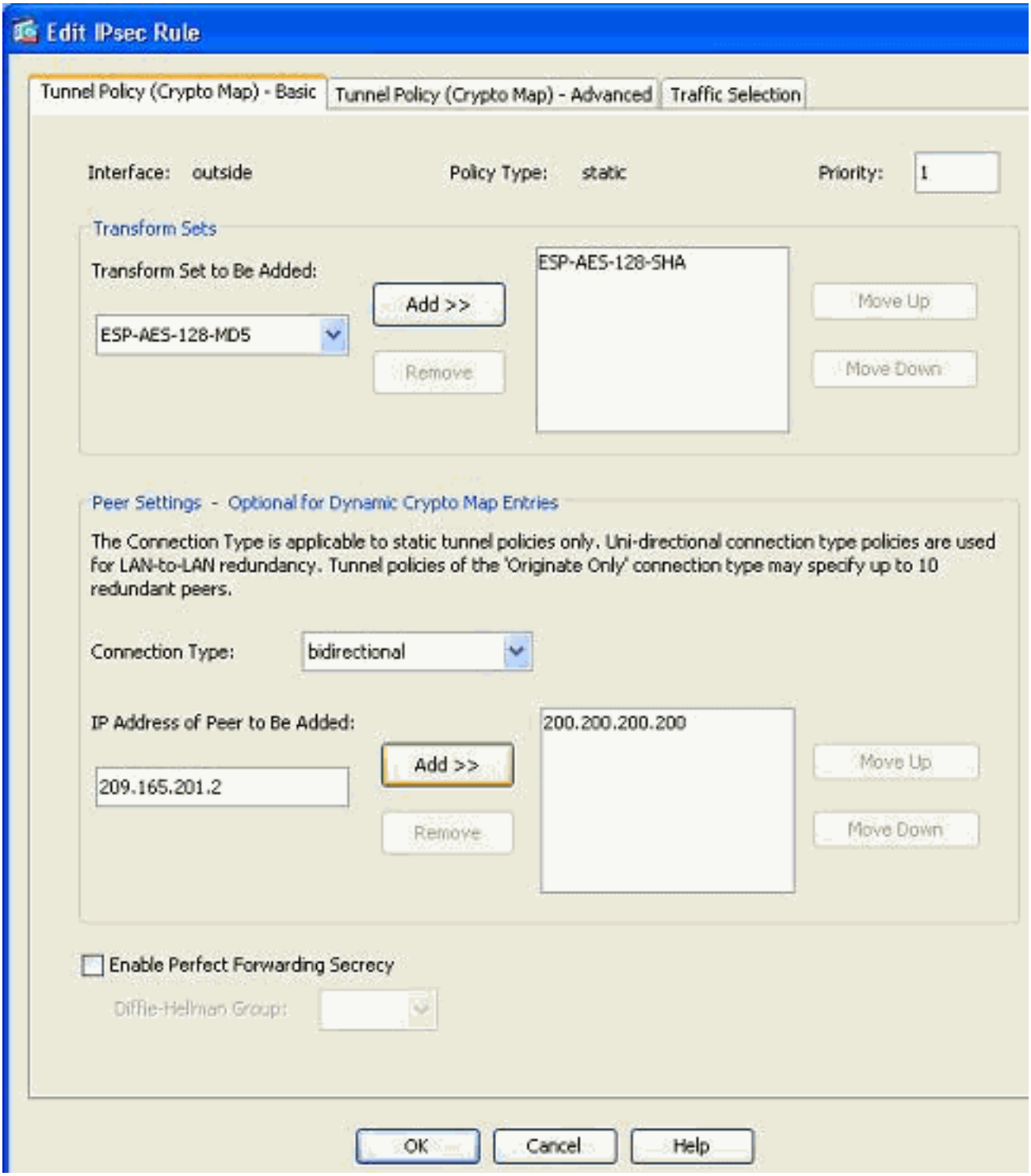
Bearbeiten der vorhandenen Crypto Map

Die vorhandene Crypto Map kann bearbeitet werden, um die neuen Peer-Informationen zuzuordnen.

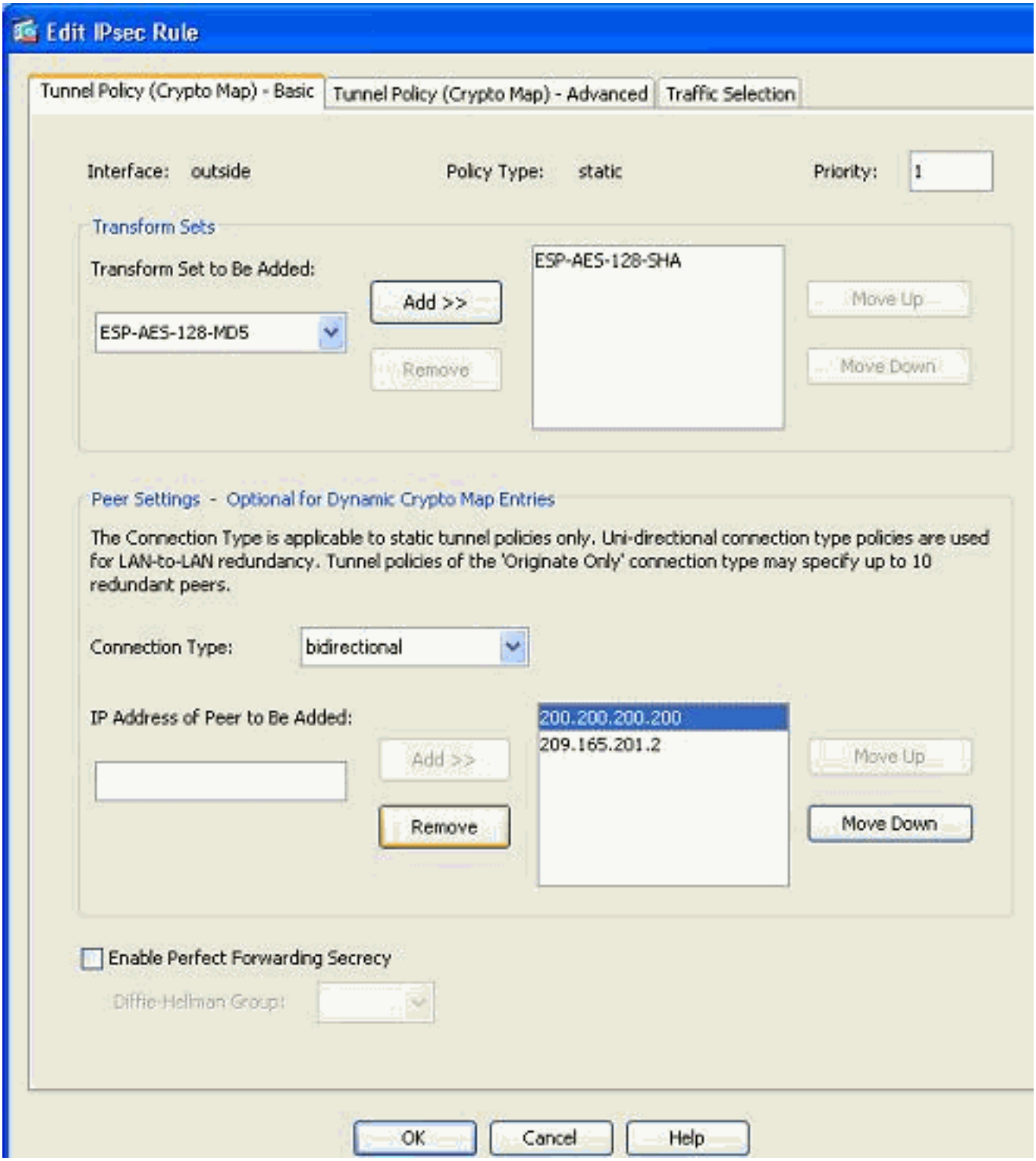
Gehen Sie wie folgt vor:

1. Gehen Sie zu *Konfiguration > Site-to-Site-VPN > Erweitert > Crypto Maps*, wählen Sie die gewünschte Crypto Map aus, und klicken Sie auf *Edit*.


Das Fenster *IPSec-Regel bearbeiten* wird angezeigt.
2. Geben Sie auf der Registerkarte "Tunnel Policy (Basic)" (Tunnelrichtlinie (Grundlegend)) im Bereich Peer Settings (Peereinstellungen) den neuen Peer im Feld IP Address of Peer to be added (IP-Adresse des Peers, das hinzugefügt werden soll) an. Klicken Sie anschließend auf *Hinzufügen*.

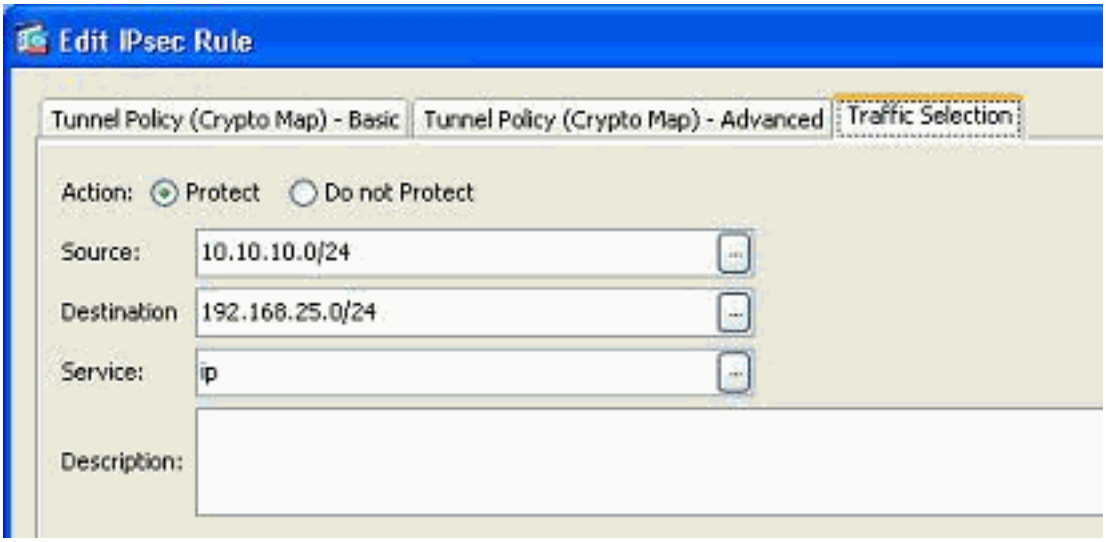


3. Wählen Sie die vorhandene Peer-IP-Adresse aus, und klicken Sie auf *Entfernen*, um die neuen Peer-Informationen beizubehalten. Klicken Sie auf *OK*.

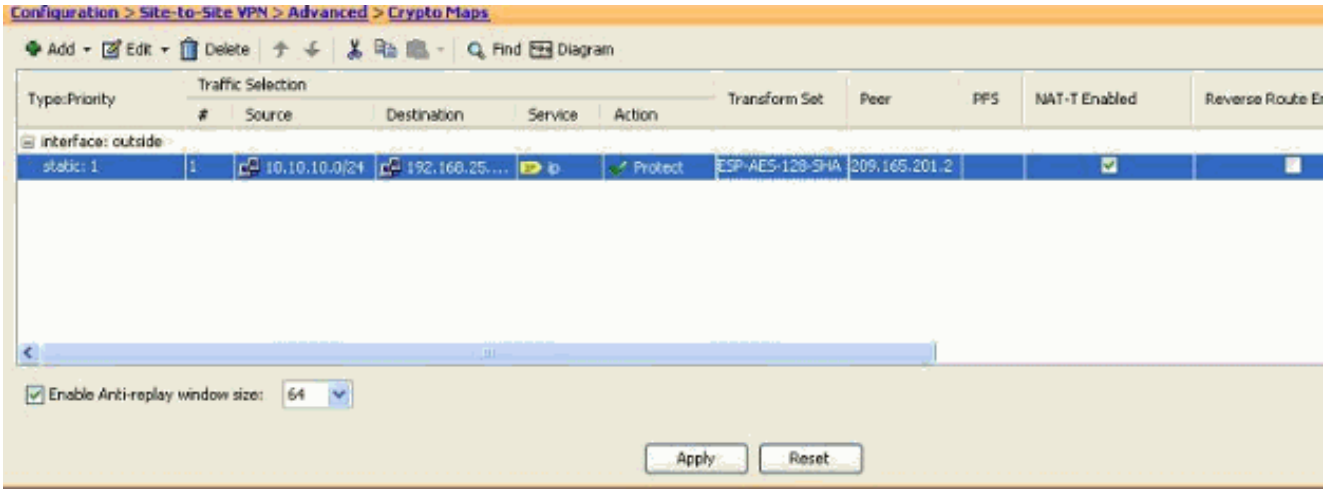


Hinweis: Nachdem Sie die Peerinformationen in der aktuellen Crypto Map geändert haben, wird das dieser Crypto Map zugeordnete Verbindungsprofil im ASDM-Fenster sofort gelöscht.

4. Die Details der verschlüsselten Netzwerke bleiben unverändert. Wenn Sie diese ändern müssen, gehen Sie zur Registerkarte *Traffic Selection (Datenverkehrsauswahl)*.



5. Öffnen Sie den Bereich *Konfiguration > Site-to-Site VPN > Erweitert > Crypto Maps*, um die geänderte Crypto Map anzuzeigen. Diese Änderungen finden jedoch erst statt, wenn Sie auf *Übernehmen* klicken. Wenn Sie auf *Übernehmen* klicken, gehen Sie zum Menü *Konfiguration > Site-to-Site VPN > Erweitert > Tunnelgruppen*, um zu überprüfen, ob eine zugeordnete Tunnelgruppe vorhanden ist oder nicht. Wenn ja, wird ein zugeordnetes *Verbindungsprofil* erstellt.



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- Verwenden Sie diesen Befehl, um die für einen einzelnen Peer spezifischen Sicherheitsparameter anzuzeigen:**show crypto ipsec sa peer <Peer-IP-Adresse>**

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

IKE Initiator kann die Richtlinie nicht finden: Intf test_ext, Src: 172.16.1.103, Dst: 10.1.4.251

Dieser Fehler wird in den Protokollmeldungen angezeigt, wenn versucht wird, den VPN-Peer von einem VPN-Konzentrator zu ASA zu ändern.

Lösung:

Dies kann auf unsachgemäße Konfigurationsschritte während der Migration zurückzuführen sein. Stellen Sie sicher, dass die Kryptobindung an die Schnittstelle entfernt wird, bevor Sie einen neuen Peer hinzufügen. Stellen Sie außerdem sicher, dass Sie die IP-Adresse des Peers in der Tunnelgruppe, jedoch nicht den Namen verwendet haben.

Zugehörige Informationen

- Site-to-Site-VPN (L2L) mit ASA
- Häufigste VPN-Probleme
- ASA Seite für technischen Support
- Technischer Support und Dokumentation - Cisco Systems