ASA 8.x/ASDM 6.x: Voeg nieuwe VPN-peer informatie toe in een bestaande site-to-site VPN met ASDM

Inhoud

Inleiding

Dit document bevat informatie over de configuratie van de wijzigen die moeten worden doorgevoerd wanneer een nieuwe VPN-peer wordt toegevoegd aan de bestaande site-to-site VPN-configuratie met Adaptieve Security Apparaatbeheer (ASDM). Dit is vereist in deze scenario's:

- De Internet Service Provider (ISP) is gewijzigd en er wordt een nieuwe reeks openbare IP-tools gebruikt.
- Een compleet nieuw ontwerp van het netwerk op een site.
- Het apparaat dat als gateway van VPN op een plaats wordt gebruikt wordt gemigreerd naar een nieuw apparaat met een verschillend openbaar IP adres.

Dit document gaat ervan uit dat de site-to-site VPN al correct is geconfigureerd en goed werkt. Dit document bevat de te volgen stappen om een VPN-peer informatie in de L2L VPN-configuratie te wijzigen.

Voorwaarden

Vereisten

Cisco raadt aan dat u kennis hebt van dit onderwerp:

- ASA Site-to-Site VPN-configuratievoorbeeld

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco adaptieve security applicatie 5500 Series met softwareversie 8.2 en hoger
- Cisco Adapter Security apparaat Manager met softwareversie 6.3 en hoger

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Het site-to-site VPN werkt prima tussen de HQASA en de BQASA. Stel dat de BQASA een compleet netwerk opnieuw ontworpen heeft en het IP-schema is aangepast op het niveau van de ISP, maar alle interne subnetwerk details blijven hetzelfde.

Deze voorbeeldconfiguratie gebruikt deze IP-adressen:

- Bestaande BQASA buiten IP-adres - 20.20.200.200.200
- New BQASA Outside IP Address - 209.165.201.2

Opmerking: Hier wordt alleen de peer informatie aangepast. Omdat er geen andere verandering is in interne vorm blijven de crypto toegangslijsten hetzelfde.

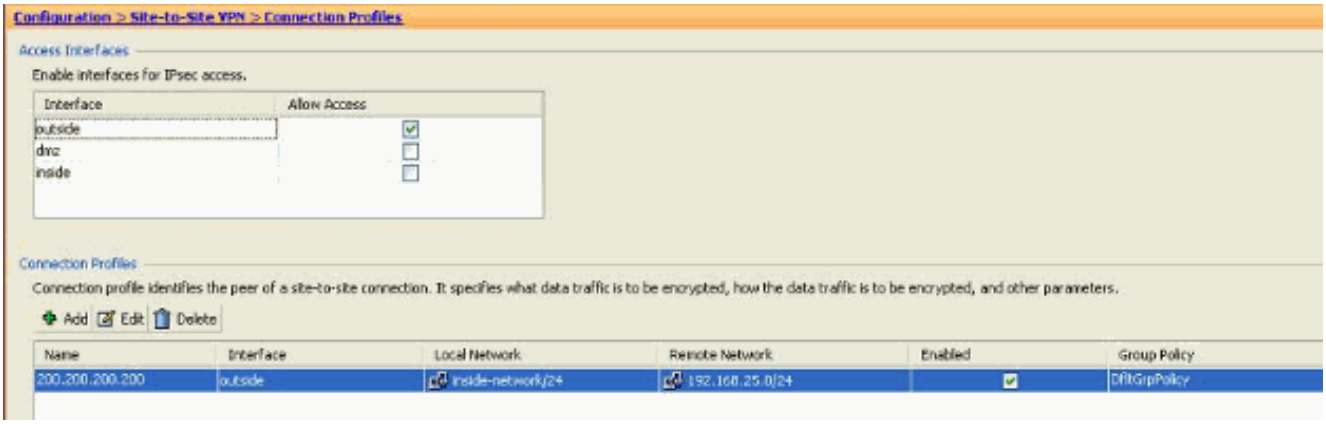
ASDM-configuratie

Deze sectie verschaft informatie over de mogelijke methoden die worden gebruikt om VPN-peer informatie over HQASA te wijzigen met behulp van ASDM.

Een nieuw verbindingsprofiel maken

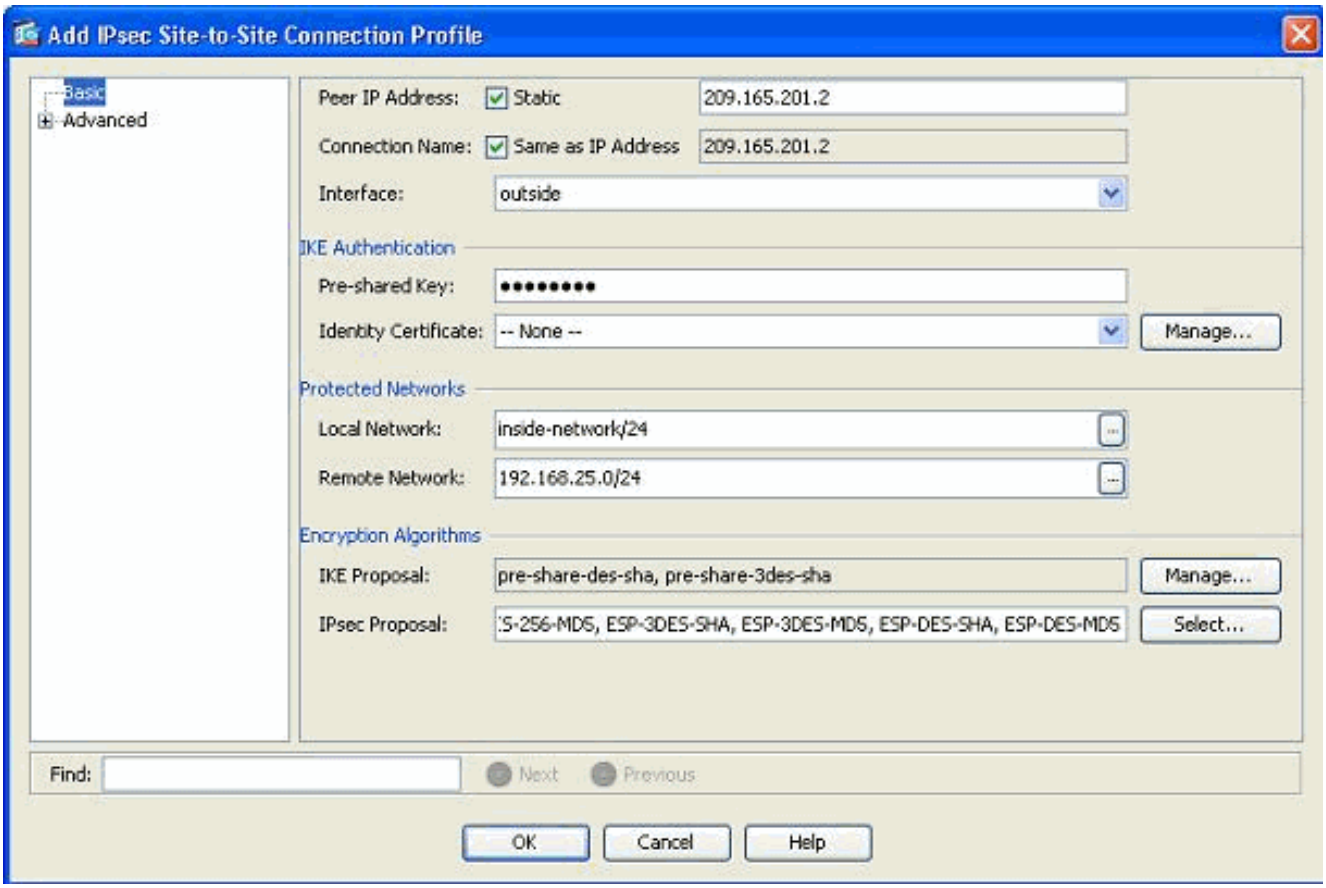
Dit kan de makkelijkste methode zijn omdat de bestaande VPN-configuratie niet wordt verstoord en u kunt een nieuw verbindingsprofiel maken met de nieuwe VPN peer-gerelateerde informatie.

1. Ga naar *Configuration > Site-to-Site VPN > Connection-profielen* en klik op *Add* onder het gebied Connection
   Profile.

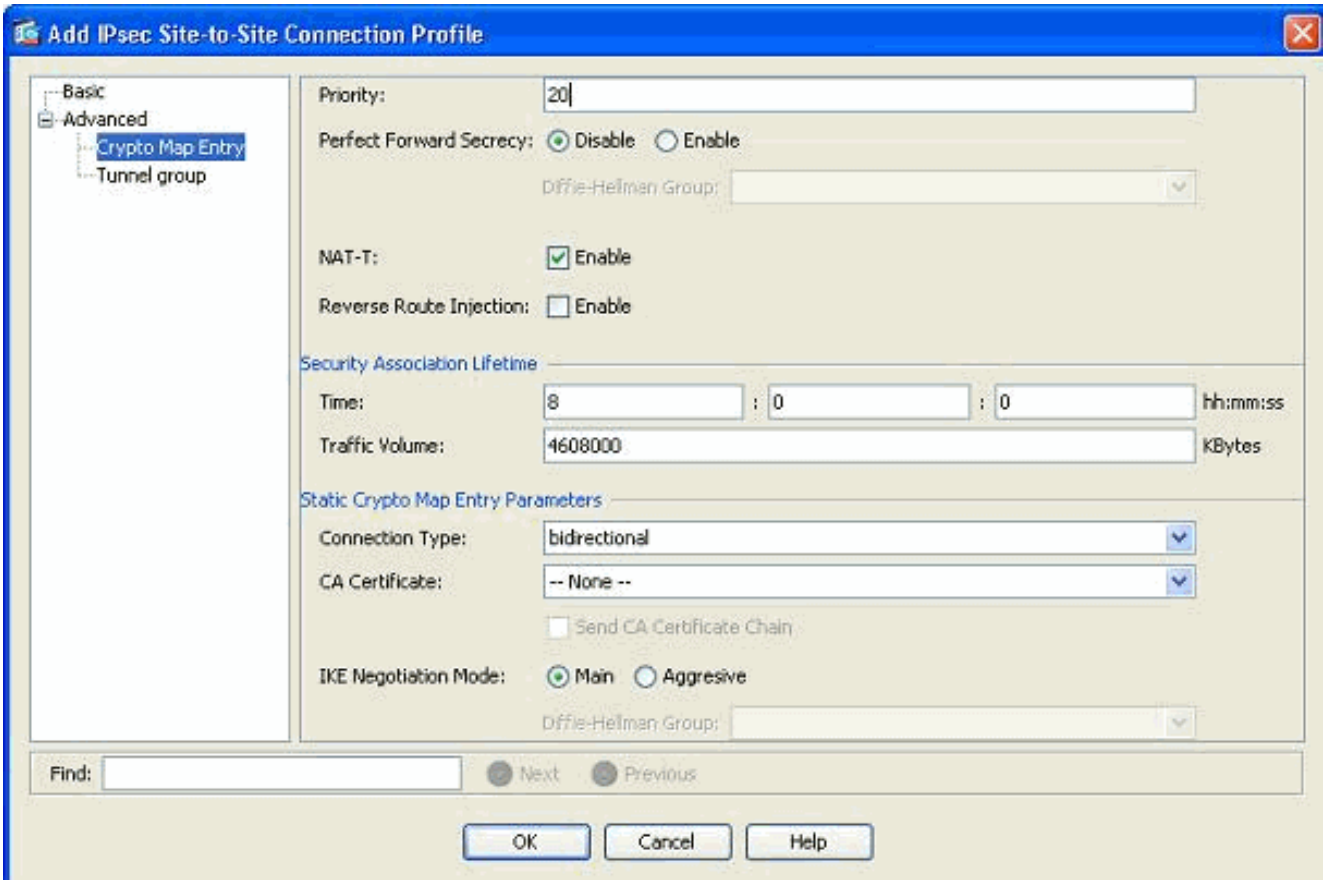


Het venster *Add IPSec Site-to-Site Connection Profile* wordt geopend.

2. Typ onder het tabblad Basic de details voor *peer IP-adres*, *voorgedeelde sleutel* en *beschermde netwerken*. Gebruik alle dezelfde parameters als het bestaande VPN, behalve de peer informatie. Klik op *OK*.



3. Klik onder het menu Geavanceerd op *Crypto Map*. Raadpleeg het tabblad *Prioriteit*. Deze prioriteit is gelijk aan het sequentienummer in zijn equivalente CLI-configuratie. Wanneer een kleiner aantal dan de bestaande crypto map entry is toegewezen, wordt dit nieuwe profiel eerst uitgevoerd. Hoe hoger het prioriteitsnummer, hoe lager de waarde. Dit wordt gebruikt om de volgorde van sequentie te veranderen dat een specifieke crypto kaart zal worden uitgevoerd. Klik op *OK* om het maken van het nieuwe verbindingsprofiel te voltooien.



Dit creëert automatisch een nieuwe tunnelgroep samen met een gekoppelde crypto kaart. Zorg ervoor dat u de BQASA met het nieuwe IP-adres kunt bereiken voordat u dit nieuwe verbindingsprofiel gebruikt.

De bestaande VPN-configuratie bewerken

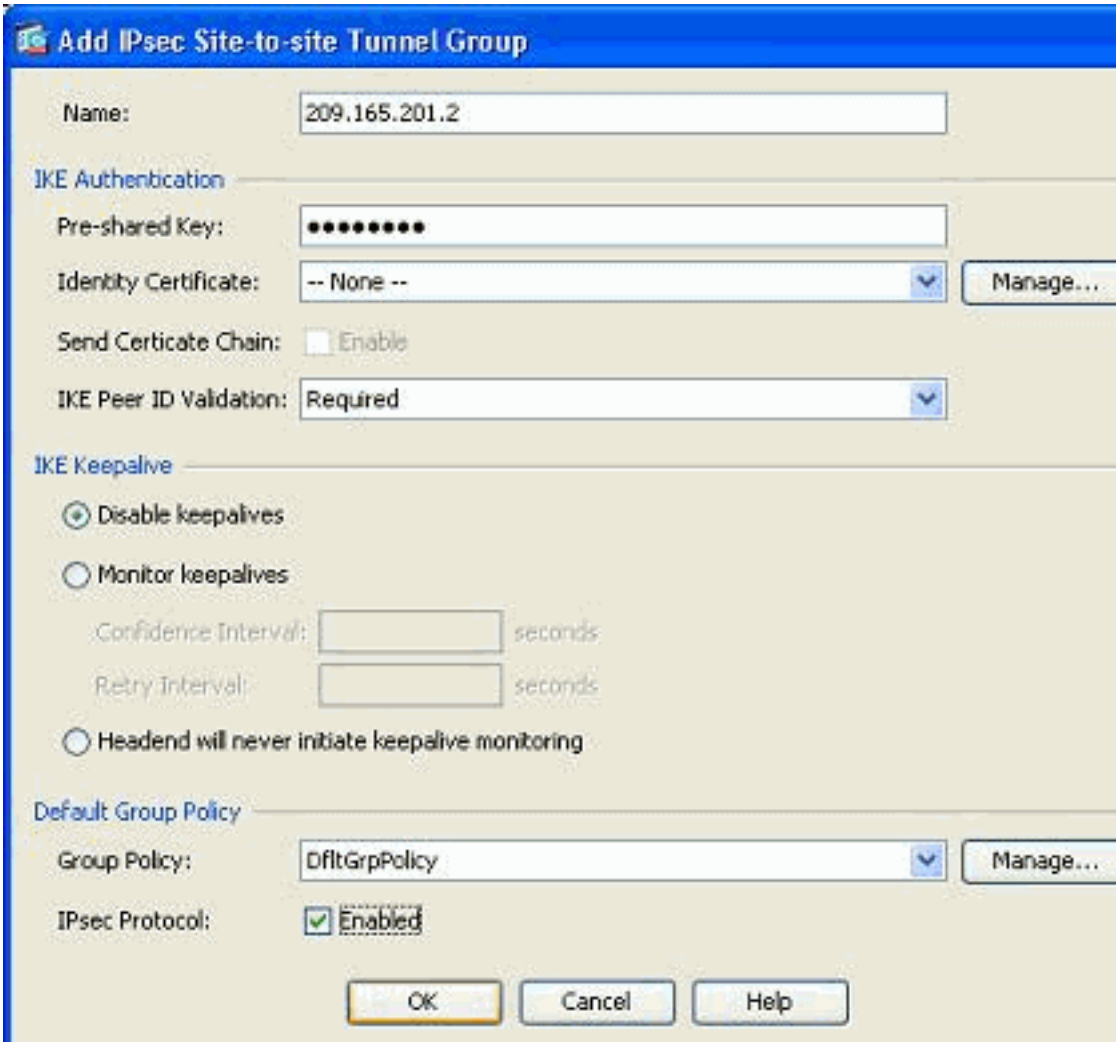
Een andere manier om een nieuw peer toe te voegen is de bestaande configuratie aan te passen. Het bestaande verbindingsprofiel kan niet voor de nieuwe peer informatie worden bewerkt omdat het aan een specifieke peer is gebonden. U moet de volgende stappen uitvoeren om de bestaande configuratie te bewerken:

1. Een nieuwe tunnelgroep maken
2. Bewerk de bestaande encryptie-kaart

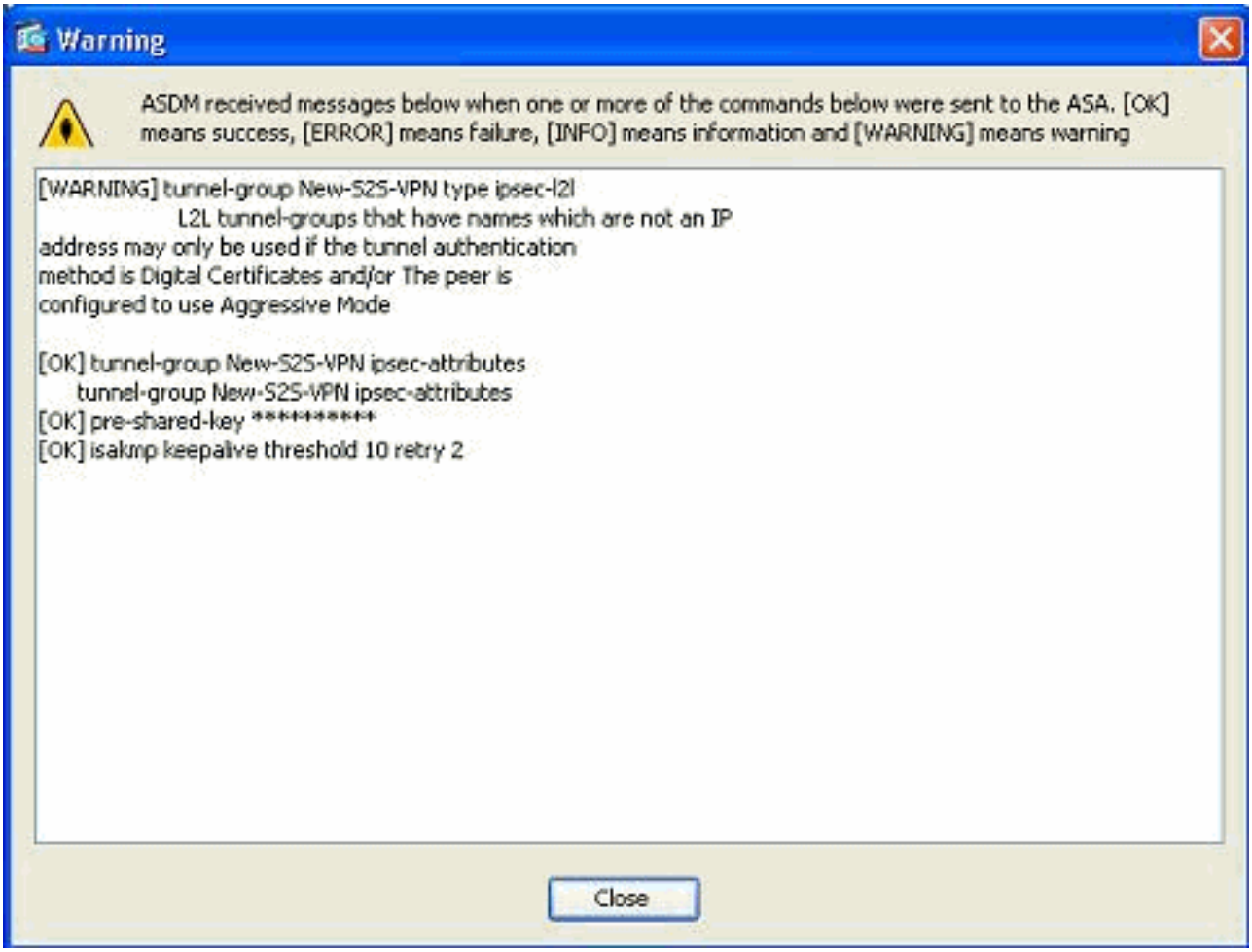
Een nieuwe tunnelgroep maken

Ga naar *Configuratie > Site-to-Site VPN > Geavanceerd > Tunnelgroepen* en klik op *Add* om een nieuwe tunnelgroep te maken die de nieuwe VPN peer informatie bevat. Specificeer de velden *Naam* en *Voorgedeeld sleutel* en klik vervolgens op *OK*.

Opmerking: Controleer of de vooraf gedeelde sleutel overeenkomt met het andere uiteinde van VPN.



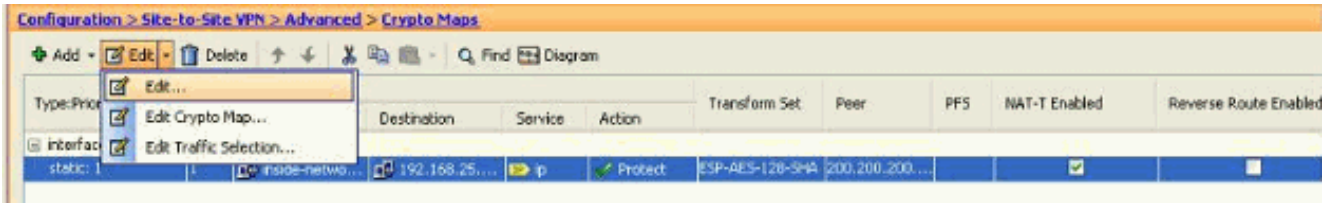
Opmerking: In het veld Naam dient alleen het IP-adres van de externe peer te worden ingevoerd wanneer de verificatiemodus van tevoren gedeelde sleutels is. Elke naam kan alleen worden gebruikt wanneer de echtheidsmethode door middel van certificaten wordt gebruikt. Deze fout verschijnt wanneer een naam wordt toegevoegd in het veld Naam en de verificatiemethode wordt vooraf gedeeld:



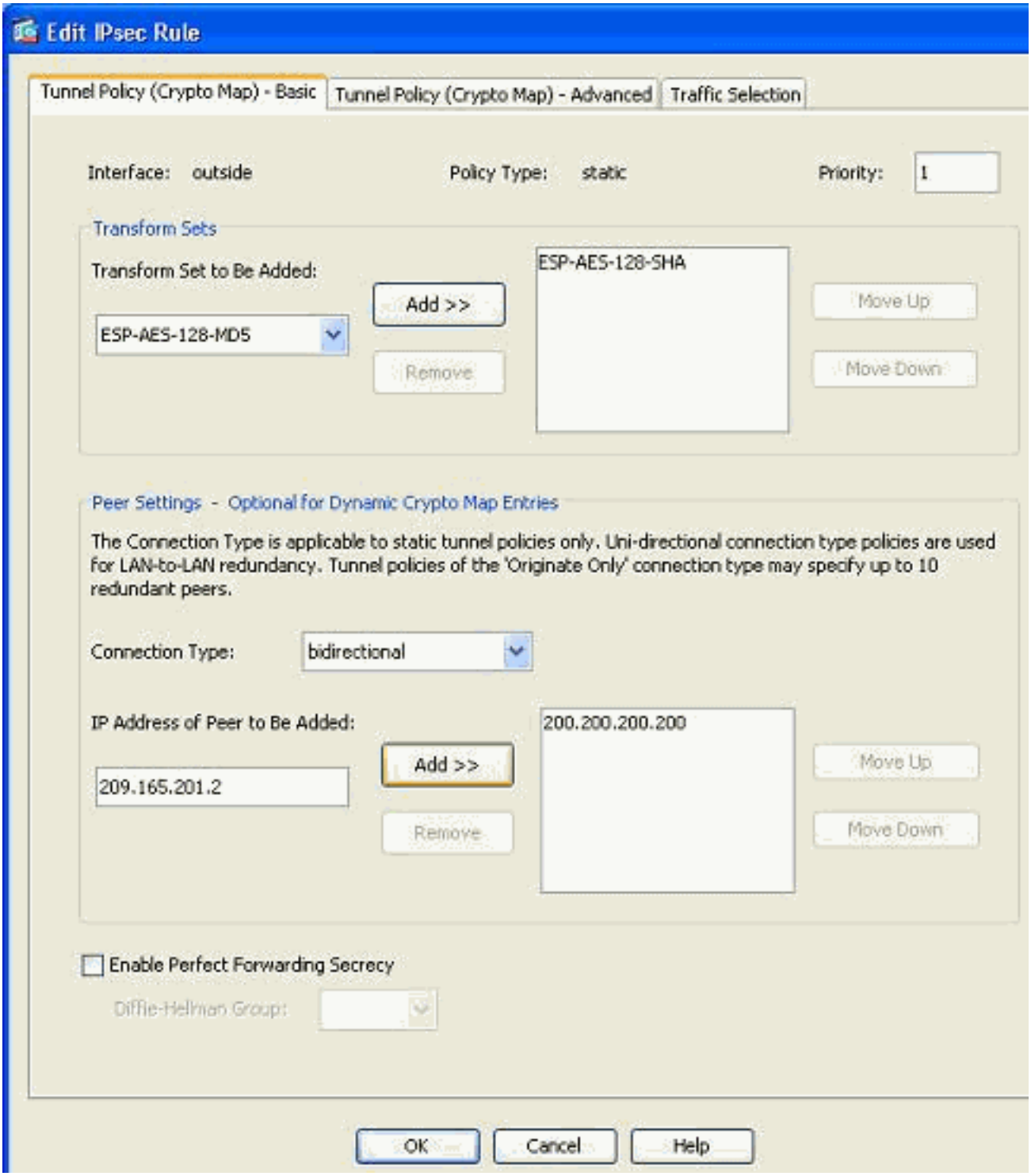
Bewerk de bestaande encryptie-kaart

De bestaande crypto kaart kan worden bewerkt om de nieuwe peer informatie te koppelen.

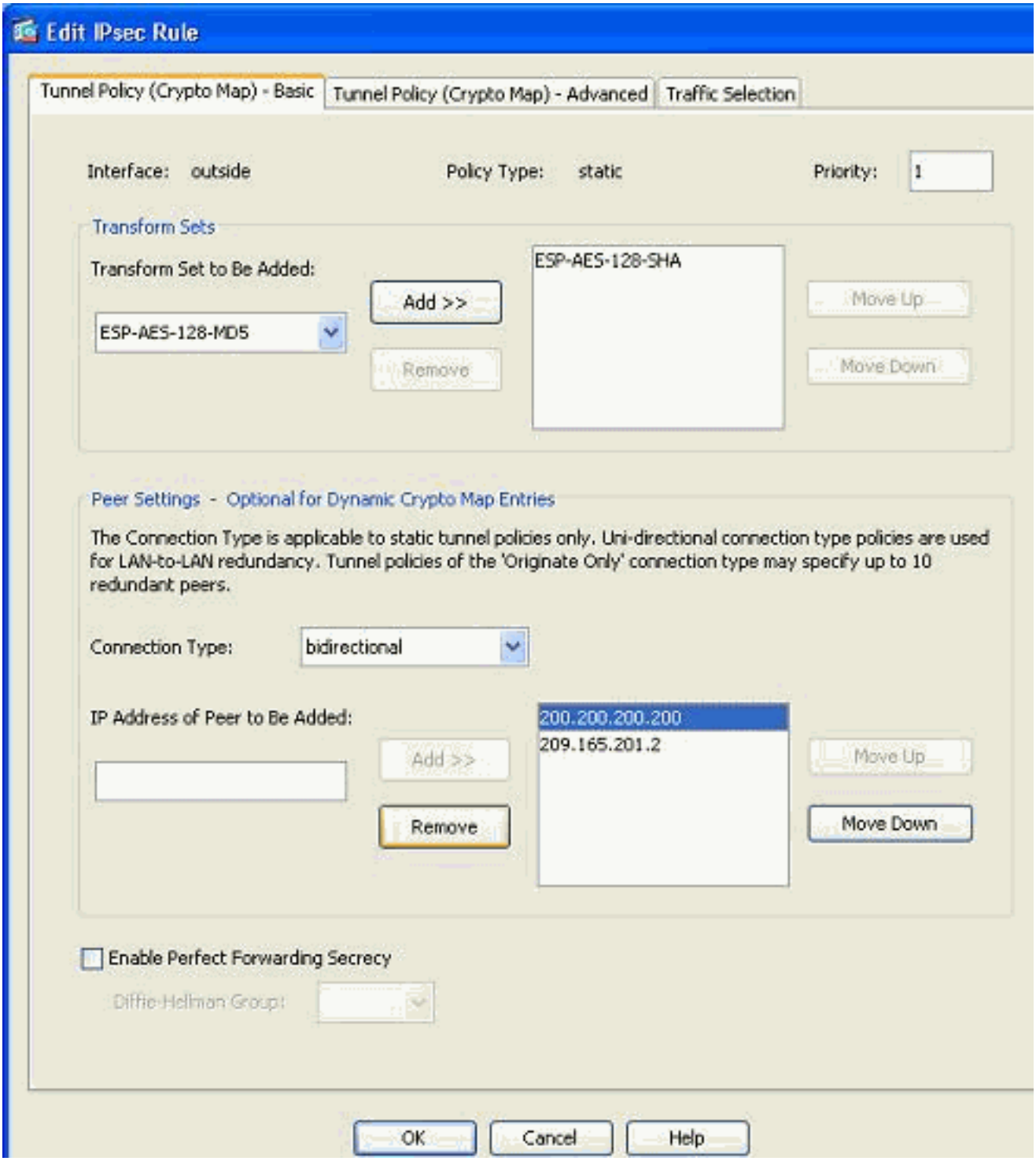
Voer de volgende stappen uit:

1. Ga naar *Configuration > Site-to-Site VPN > Advanced > Crypto Maps*, selecteer de gewenste crypto-kaart en klik op *Bewerken*.


Het venster *IPSec-regel bewerken* verschijnt.
2. Onder het tabblad Tunnel beleid (Basis) specificeert u in het gebied Peer Instellingen de nieuwe peer in het veld IP Adres van peer die wordt toegevoegd. Klik vervolgens op *Add* (Toevoegen).

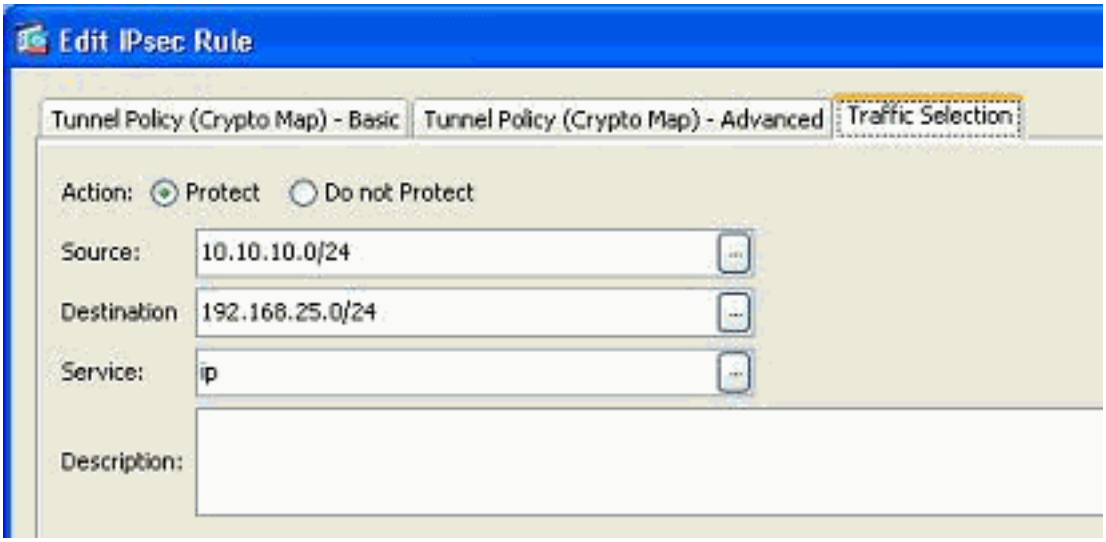


3. Selecteer het bestaande peer IP-adres en klik op *Verwijderen* om alleen de nieuwe peer-informatie te behouden. Klik op
OK.

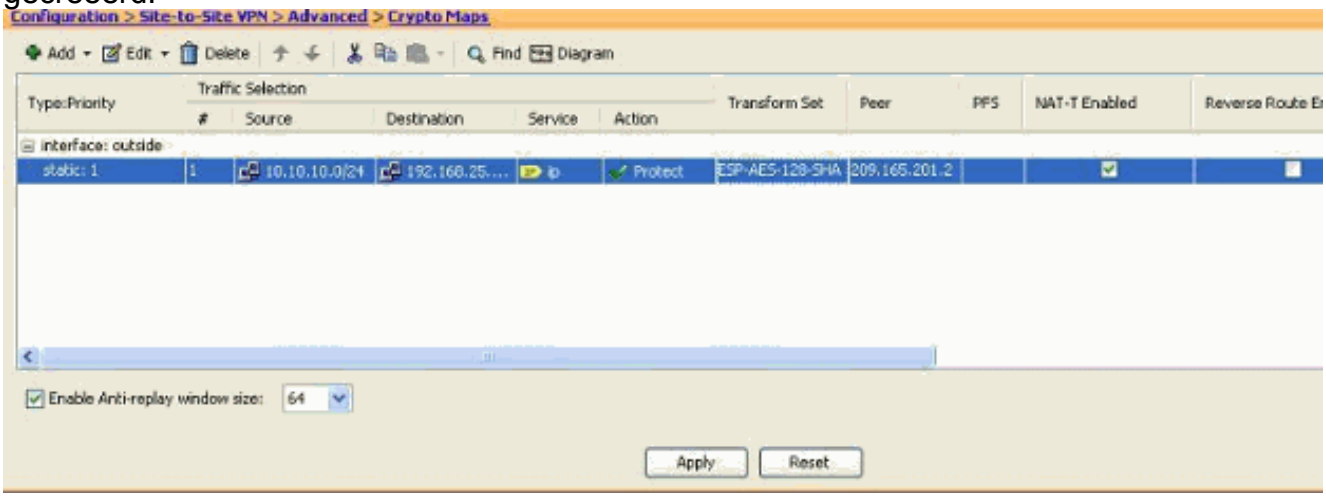


Opmerking: Nadat u de peer informatie in de huidige crypto map hebt gewijzigd, wordt het verbindingsprofiel dat bij deze crypto map hoort direct verwijderd in het ASDM-venster.

4. De details van de versleutelde netwerken blijven hetzelfde. Als u deze instellingen wilt wijzigen, gaat u naar het tabblad *Verkeerselectie*.



5. Kies het *venster Configuration > Site-to-Site VPN > Advanced > Crypto Maps* om de aangepaste crypto-kaart te bekijken. Deze wijzigingen vinden echter niet plaats totdat u op *Toepassen* klikt. Nadat u op *Toepassen* klikt, gaat u naar de *Configuration > Site-to-Site VPN > Advanced > Tunnel Groepen* om te controleren of er een gekoppelde tunnelgroep al dan niet aanwezig is. Als ja, dan wordt een gekoppeld *verbindingsprofiel* gecreëerd.



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- Gebruik deze opdracht om de parameters van de veiligheidsassociatie die specifiek zijn voor één peer, te bekijken:crypto-ipsec als peer <peer IP-adres> tonen

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

IKE-initiator kan geen beleid vinden: Intf test_ext, Src: 172.16.1.103, Dst: 10.1.4.251

Deze fout wordt in de logberichten weergegeven wanneer u de VPN-peer van een VPN-concentrator naar ASA probeert te wijzigen.

Oplossing:

Dit kan een gevolg zijn van ongeschikte configuratiestappen die tijdens de migratie zijn gevolgd. Zorg ervoor dat de crypto binding aan de interface wordt verwijderd voordat u een nieuw peer toevoegt. Zorg er ook voor dat u het IP-adres van de peer in de tunnel-groep gebruikte, maar niet de naam.

Gerelateerde informatie

- Site to Site (L2L) VPN met ASA
- Populairste VPN-problemen
- ASA pagina voor technische ondersteuning
- Technische ondersteuning en documentatie – Cisco Systems