ASDM 6.4: Site-to-Site VPN-tunnel met IKEv2 configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u een site-to-site VPN-tunnel tussen twee Cisco adaptieve security applicaties (ASA's) kunt configureren met behulp van Internet Key Exchange (IKE) versie 2. Het beschrijft de stappen die worden gebruikt om de VPN-tunnel te configureren met behulp van een ASDM-wizard (Adaptieve Security Apparaat Manager).

Voorwaarden

Vereisten

Zorg dat Cisco ASA is geconfigureerd met de basisinstellingen.

Gebruikte componenten

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

- Cisco ASA 5500 Series adaptieve security applicaties voor gebruik van softwareversie 8.4 en hoger
- Cisco ASDM-softwareversie 6.4 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

IKEv2 is een versterking van het bestaande IKEv1-protocol dat deze voordelen omvat:

- Minder berichtuitwisseling tussen IKE-peers
- Unidirectionele authenticatiemethoden
- Ingebouwde ondersteuning voor DID (Dead Peer Detection) en NAT-Traversal
- Gebruik van Extensible Authentication Protocol (EAP) voor authenticatie
- Vermijd het risico van eenvoudige DoS-aanvallen met behulp van antiblokkeerkoekjes

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

Dit document toont de configuratie van site-to-site VPN-tunnel op HQ-ASA. Hetzelfde kan worden gevolgd als een spiegel op de BQ-ASA.

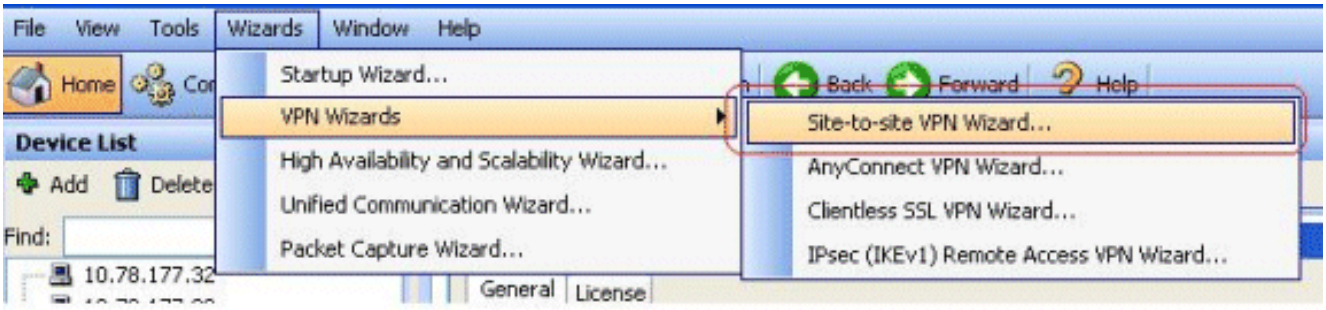
ASDM-configuratie op hoofdkwartier-ASA

Deze VPN-tunnel kon worden geconfigureerd met behulp van een gebruikersvriendelijke GUI-wizard.

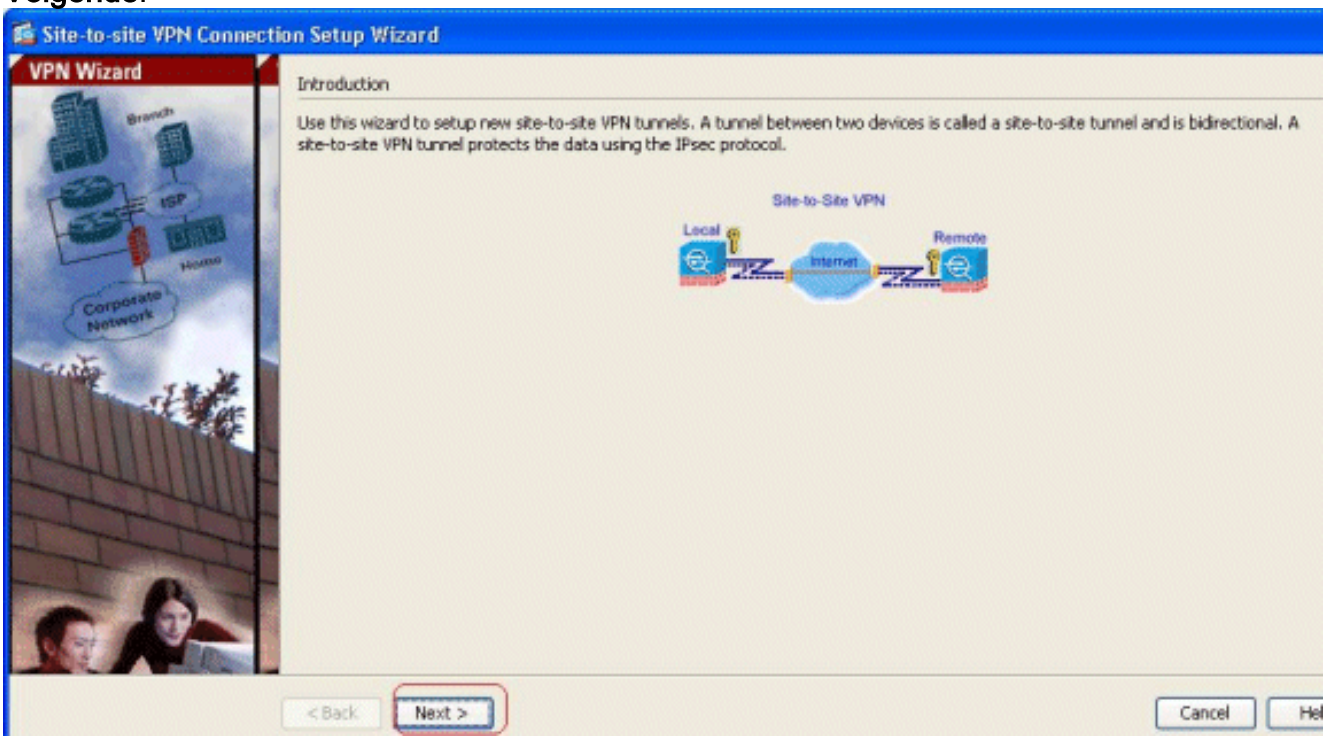
Voer de volgende stappen uit:

1. Meld u aan bij ASDM en ga naar de **Wizard > VPN-wizard > Site-to-site VPN-**

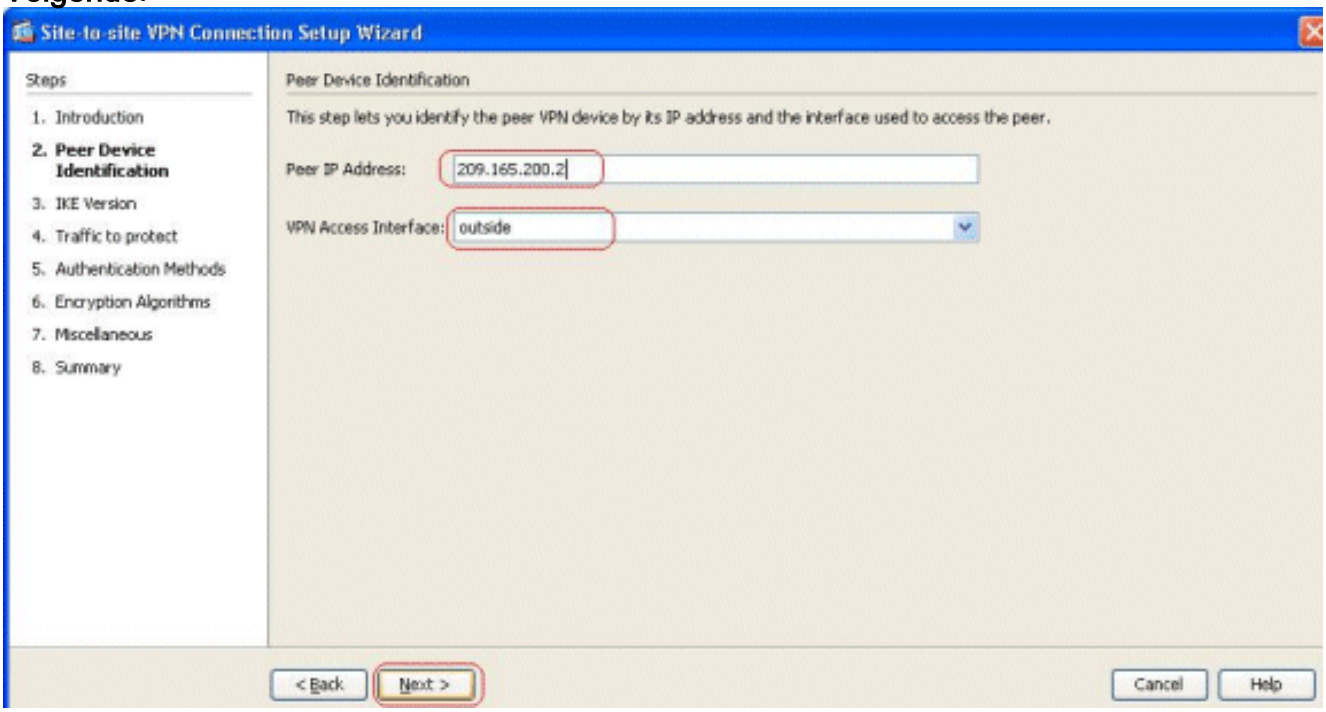
wizard.



2. Er verschijnt een setup-venster van de site-to-site VPN-verbinding. Klik op **Volgende**.

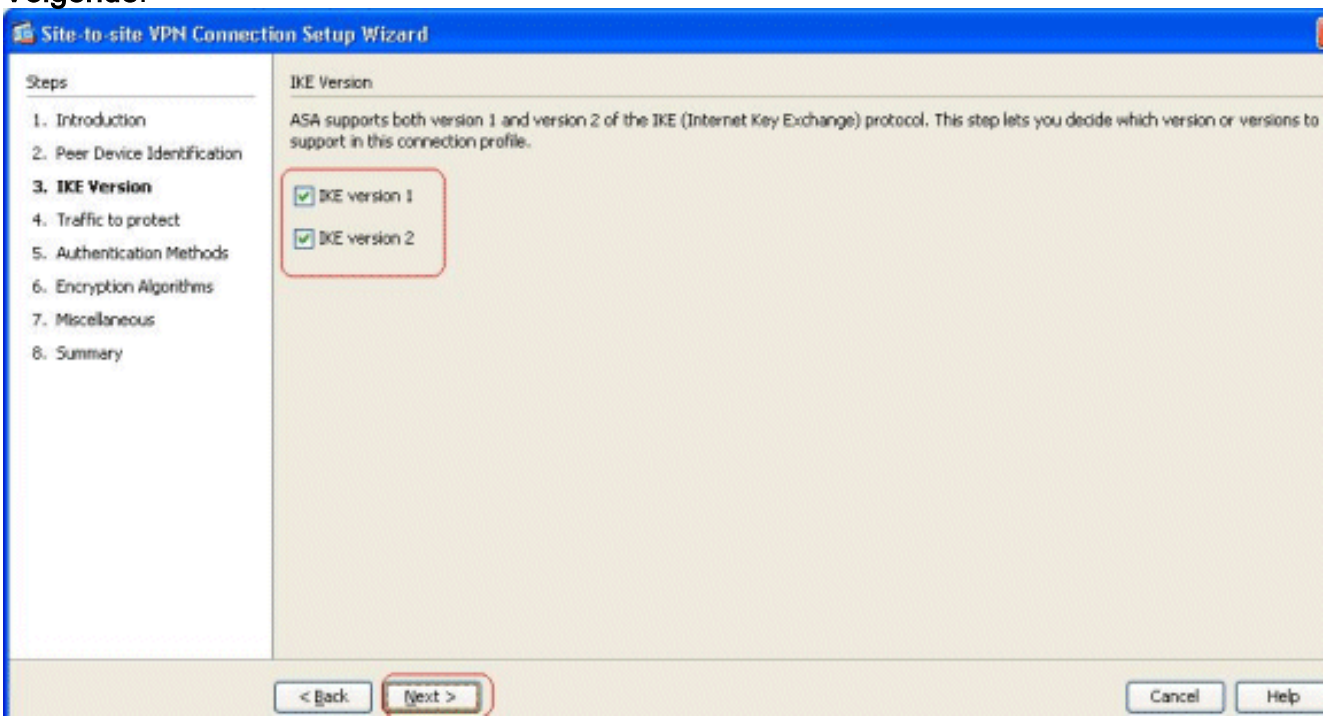


3. Specificeer het peer IP-adres en VPN-toegangsinterface. Klik op **Volgende**.



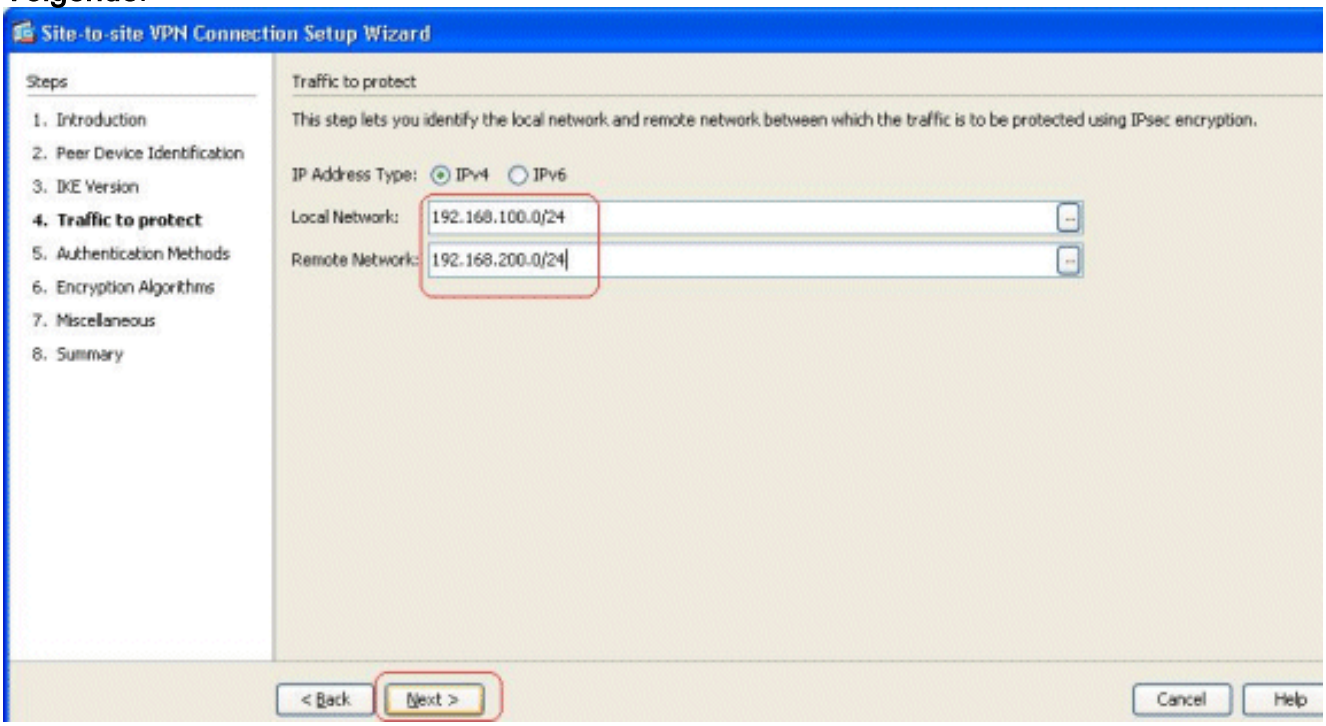
4. Selecteer beide IKE-versies en klik op

Volgende.

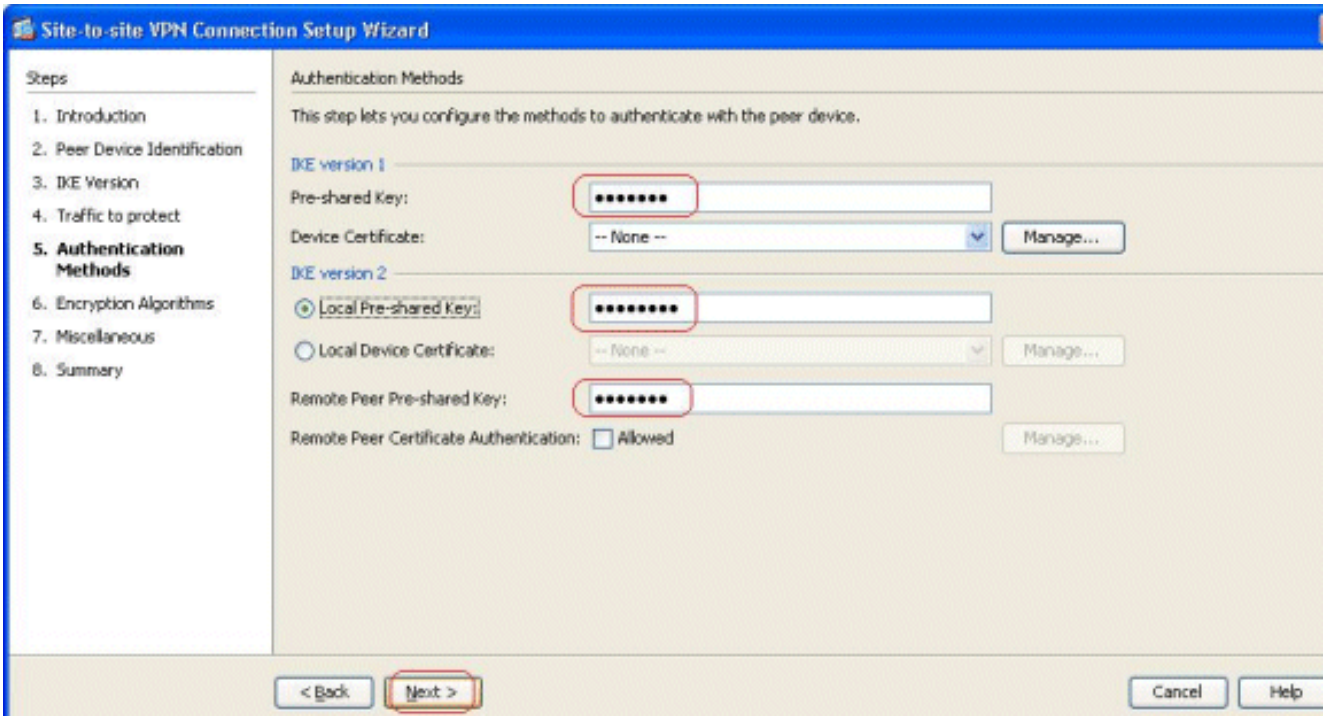


Opmerking: Beide versies van IKE zijn hier ingesteld omdat de initiatiefnemer een back-up kan maken van IKEv2 naar IKEv1 wanneer IKEv2 uitvalt.

5. Specificeer het Local Network en Remote Network zodat het verkeer tussen deze netwerken versleuteld en via de VPN-tunnel wordt doorgegeven. Klik op Volgende.

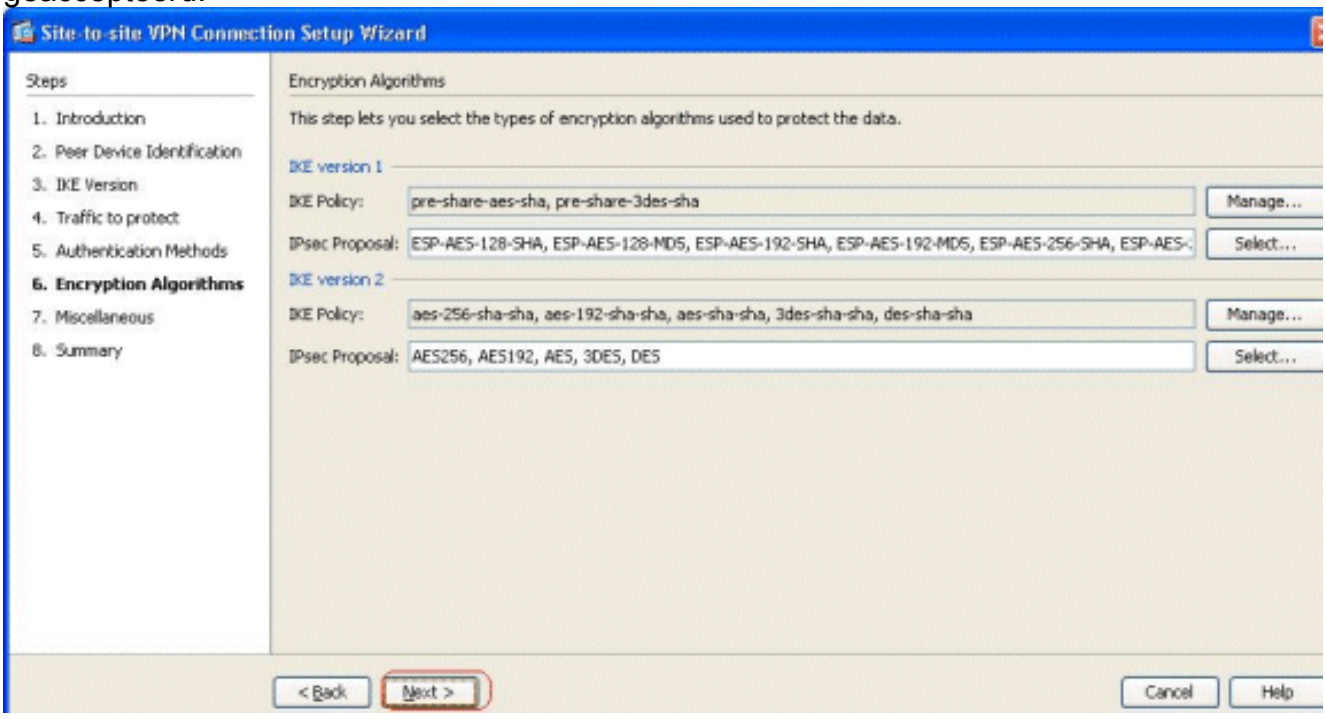


6. Specificeer de vooraf gedeelde toetsen voor beide versies van IKE.



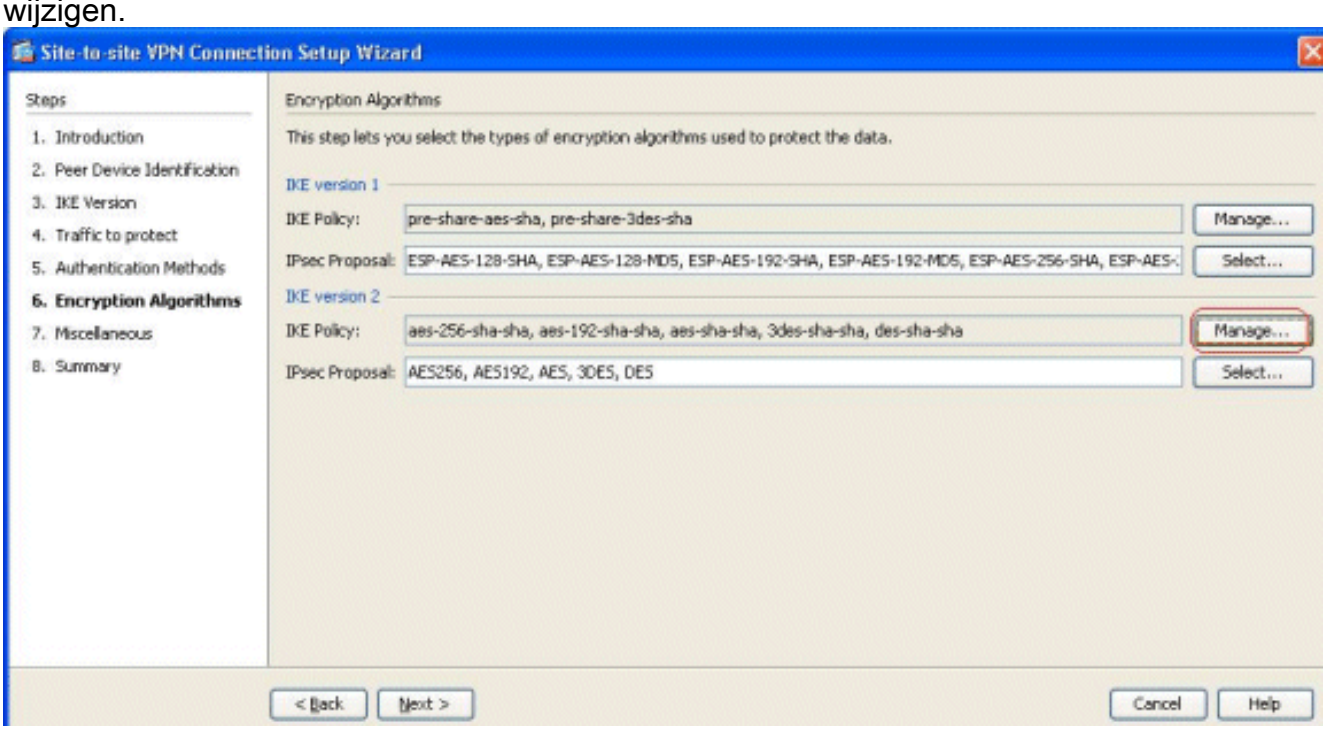
Het belangrijkste verschil tussen IKE-versies 1 en 2 ligt in termen van de door hen toegestane authenticatiemethode. IKEv1 biedt slechts één type verificatie aan beide VPN-eindes (dat wil zeggen, vooraf gedeelde sleutel of certificaat). IKEv2 laat echter toe dat asymmetrische authenticatiemethoden worden geconfigureerd (dat wil zeggen, pre-gedeelde-key authenticatie voor de originator, maar certificatie voor de responder) door middel van aparte lokale en externe authenticatie CLI's.Verder kun je aan beide uiteinden verschillende pre-gedeelde sleutels hebben. De lokale pre-gedeelde sleutel aan het HQ-ASA eind wordt de pre-gedeelde sleutel van Remote aan het BQ-ASA eind. Op dezelfde manier wordt de vooraf gedeelde sleutel op afstand aan het HQ-ASA-eind de lokale Pre-gedeeld sleutel aan het BQ-ASA-eind.

7. Specificeer de coderingsalgoritmen voor zowel IKE versies 1 als 2. Hier worden de standaardwaarden
geaccepteerd:



8. Klik op **Manager...** om het IKE-beleid te

wijzigen.

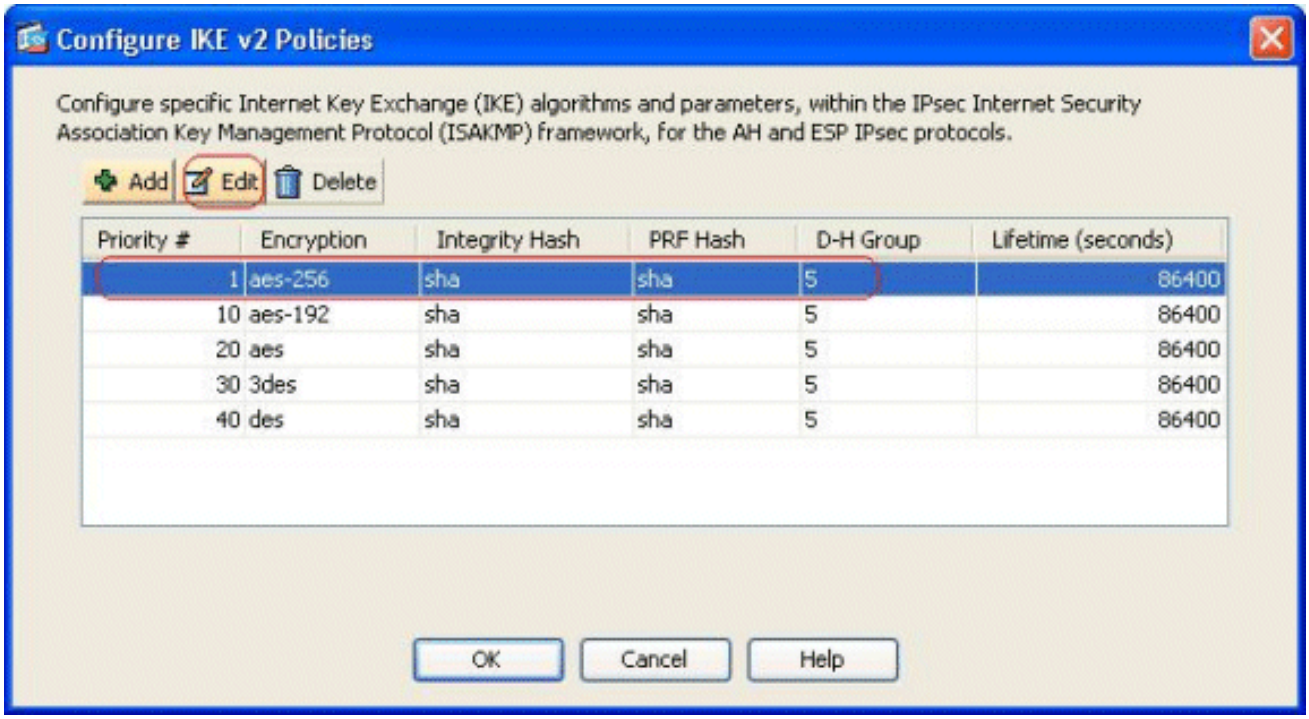


Opmerking: IKE-beleid in IKEv2 is synoniem voor het **ISAKMP-beleid** in IKEv1.**IPsec Proposal** in IKEv2 is synoniem voor de **Omzetten die** in IKEv1 **is ingesteld**.

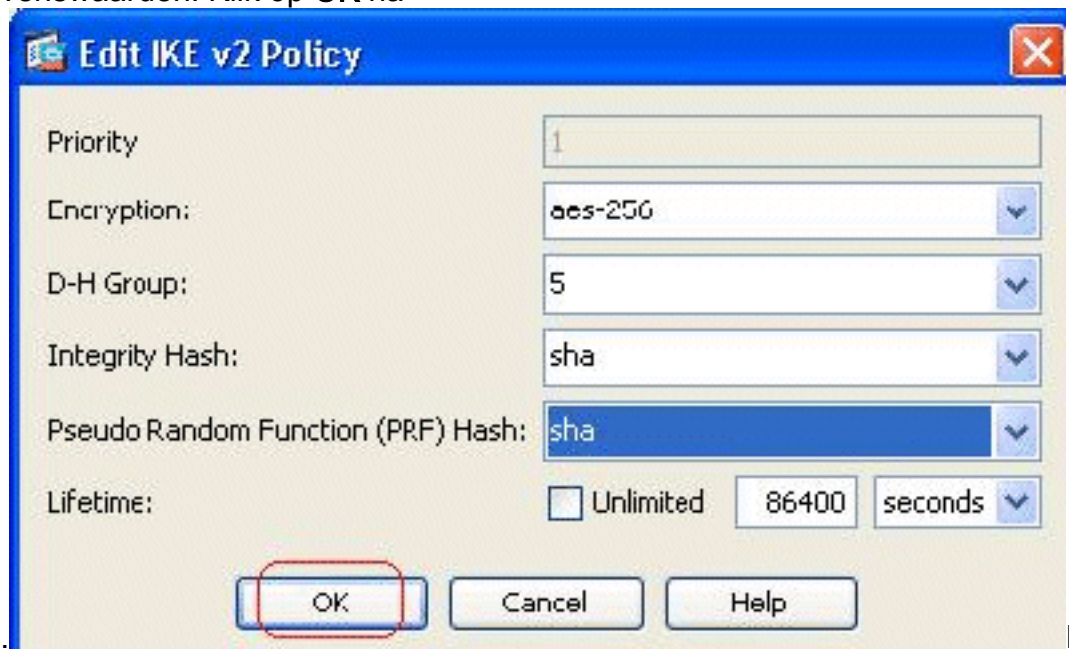
9. Dit bericht verschijnt wanneer u het bestaande beleid wilt wijzigen:

Klik op **OK** om verder te gaan.

10. Selecteer het gespecificeerde IKE-beleid en klik op **Bewerken**.

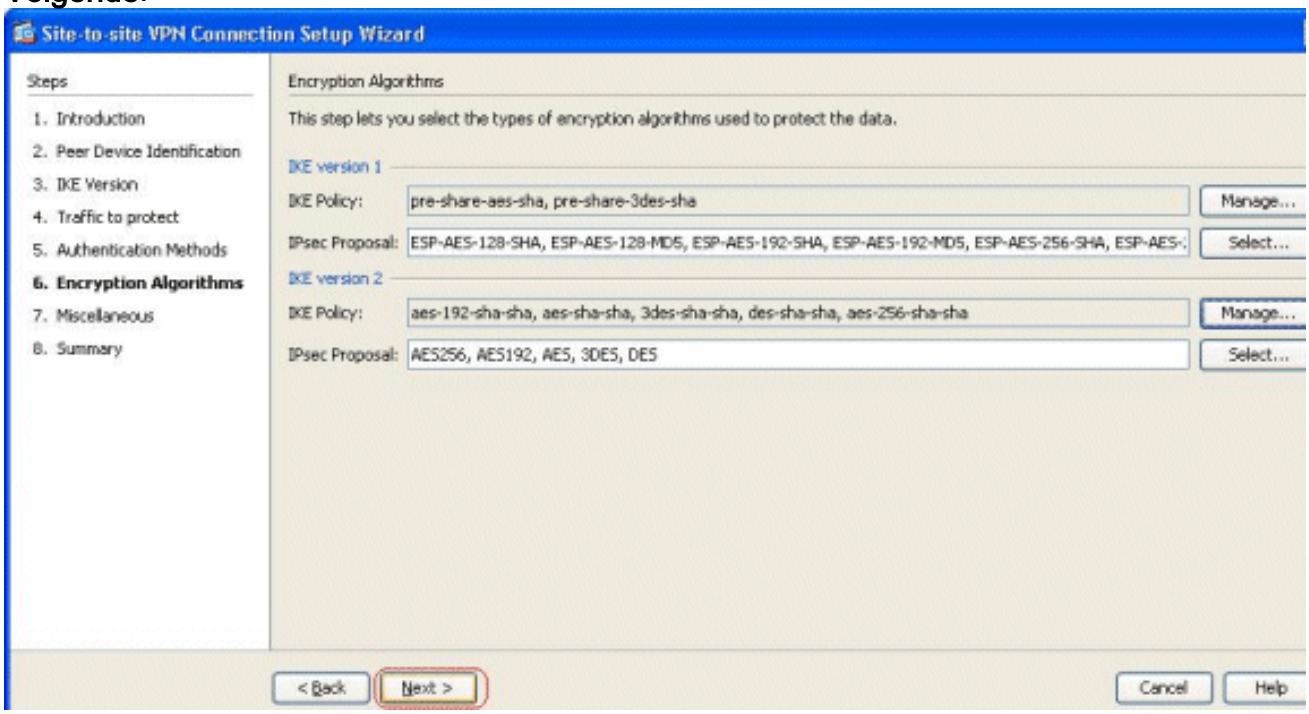


11. U kunt de parameters wijzigen, zoals prioriteit, encryptie, D-H groep, integriteitshash, PRF was en levenswaarden. Klik op **OK** na voltooiing.

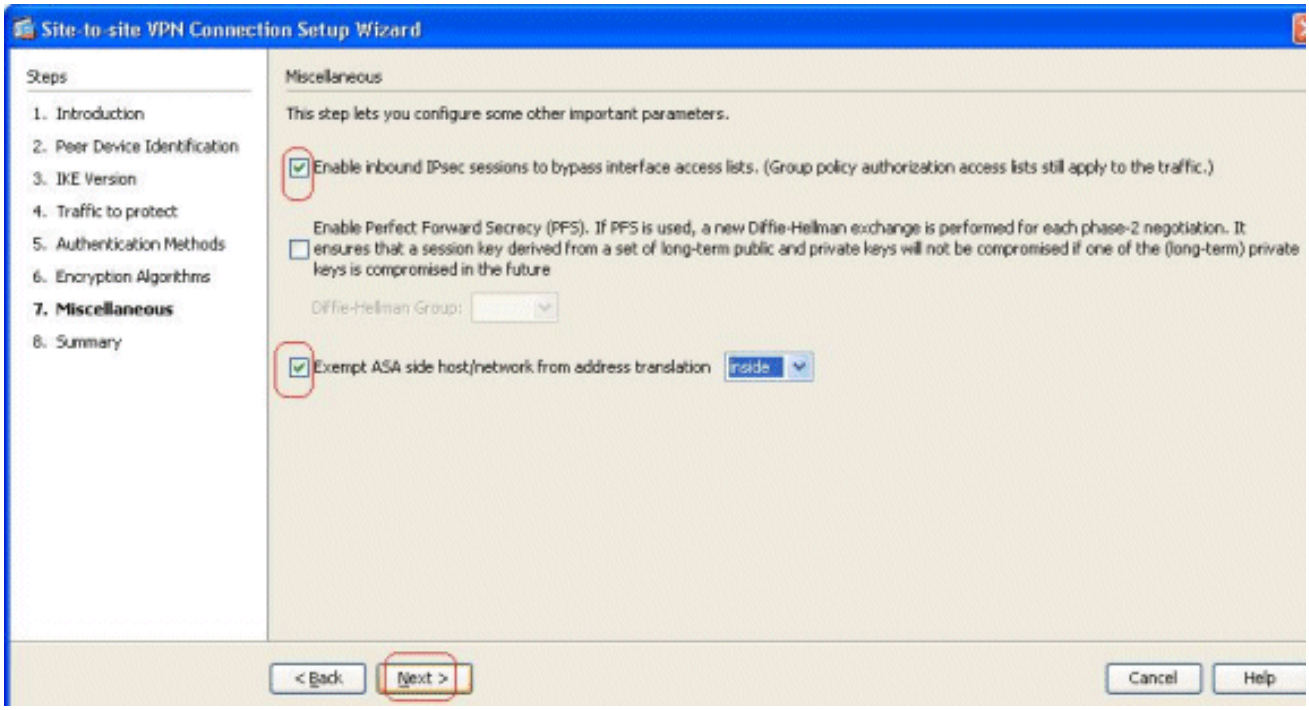


IKEv2 laat toe dat het Integrity algoritme afzonderlijk van het Pseudo Random Functie (PRF) algoritme wordt onderhandeld. Dit zou in het IKE-beleid kunnen worden geconfigureerd met de huidige beschikbare opties in SHA-1 of MD5.U kunt de IPsec voorstel parameters niet wijzigen die standaard gedefinieerd worden. Klik op **Selecteren** naast het veld IPsec Proposal om nieuwe parameters toe te voegen. Het belangrijkste verschil tussen IKEv1 en IKEv2 is in termen van de IPsec-voorstellen dat IKEv1 de transformatie accepteert in termen van combinaties van encryptie- en authenticatie-algoritmen. IKEv2 accepteert de encryptie- en integratieparameters afzonderlijk en maakt tenslotte alle mogelijke OR combinaties van deze. U kunt deze aan het einde van deze wizard bekijken in de Samenvatting-dia.

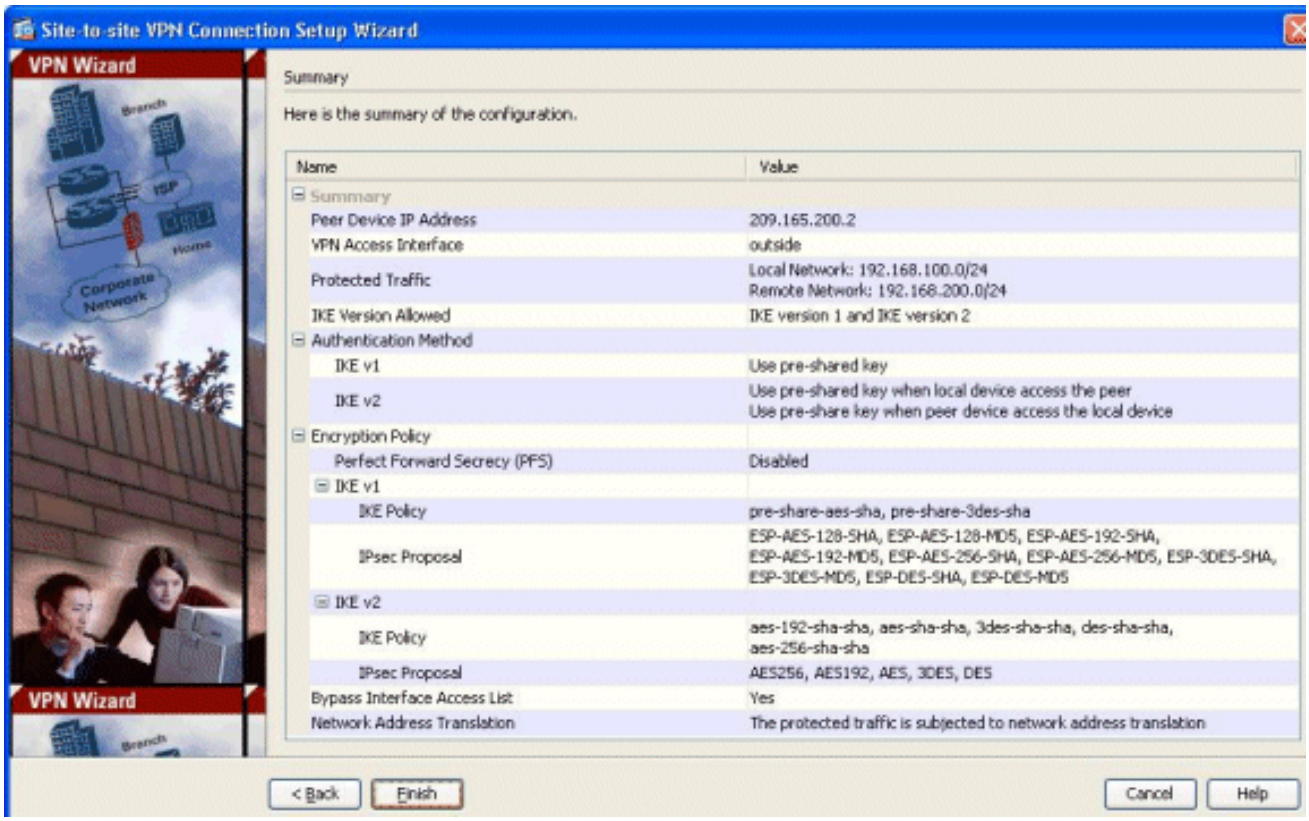
12. Klik op **Volgende**.



13. Specificeer de details, zoals NAT-vrijstelling, PFS en ACL-omzeiling (interface). Kies **Volgende**.



14. U kunt hier een samenvatting van de configuratie zien:



Klik op **Voltooien** om de site-to-site VPN-tunnelwizard te voltooien. Er wordt een nieuw verbindingsprofiel gemaakt met de ingestelde parameters.

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.

- toont crypto ikev2 sa - Toont de IKEv2 run SA database.
- vpn-sessiondb detail l2l - Hier wordt de informatie weergegeven over site-to-site VPN-sessies.

Problemen oplossen

Opdrachten voor probleemoplossing

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

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug**-opdrachten gebruikt.

- debug crypto ikev2 - **Geeft debug**-berichten voor IKEv2 weer.

Gerelateerde informatie

- Cisco ASA 5500 Series applicaties voor technische ondersteuning
- Technische ondersteuning en documentatie – Cisco Systems