dm: Site-to-Site IPsec VPN tussen ASA/PIX en een IOS routerconfiguratievoorbeeld

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor de LAN-to-LAN (Site-to-Site) IPsec-tunnel tussen Cisco security applicaties (ASA/PIX) en een Cisco IOS-router. Statische routes worden gebruikt voor eenvoud.

Raadpleeg PIX/ASA 7.x security applicatie voor een IOS Router LAN-to-LAN IPsec Tunnel Configuration Voorbeeld om meer te weten te komen over hetzelfde scenario waarin PIX/ASA security applicatie softwareversie *7.x* uitvoert.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- End-to-end IP connectiviteit moet vóór het beginnen van deze configuratie worden vastgesteld.

- De Security Appliance-licentie moet worden ingeschakeld voor Data Encryption Standard (DES) encryptie (op een minimaal coderingsniveau).

Gebruikte componenten

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

- Cisco adaptieve security applicatie (ASA) met versie 8.x en hoger
- ASDM versie 6.x en hoger
- Cisco 1812 router met Cisco IOS® softwarerelease 12.3
- Cisco Security apparaat Manager (DSM) versie 2.5

Opmerking: Raadpleeg HTTPS-toegang voor ASDM om de ASA te kunnen configureren door de ASDM.

Opmerking: Raadpleeg de basisrouterconfiguratie met behulp van een dm om de router door een dm te laten configureren.

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.

Opmerking: Raadpleeg Configuration Professional: Site-to-Site IPsec VPN tussen ASA/PIX en een IOS routerconfiguratievoorbeeld voor een soortgelijke configuratie met Cisco Configuration Professional op de router.

Verwante producten

Deze configuratie kan ook worden gebruikt met de Cisco PIX 500 Series security applicatie, die versie 7.x en hoger uitvoert.

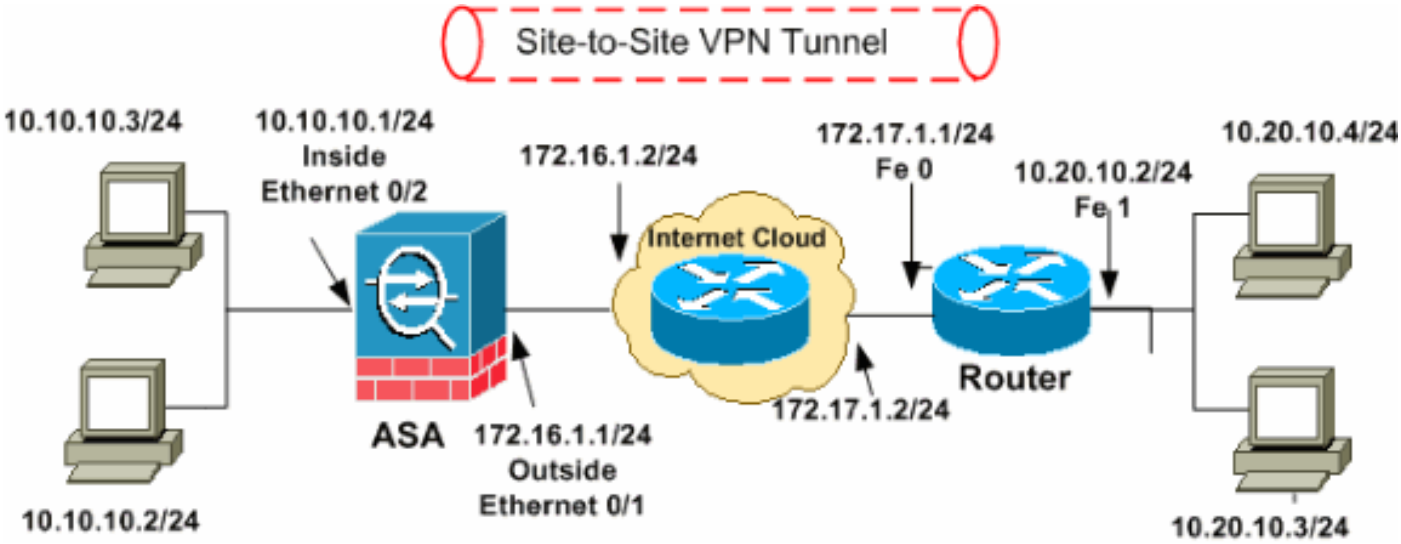
Conventies

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

Configuratie

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven.



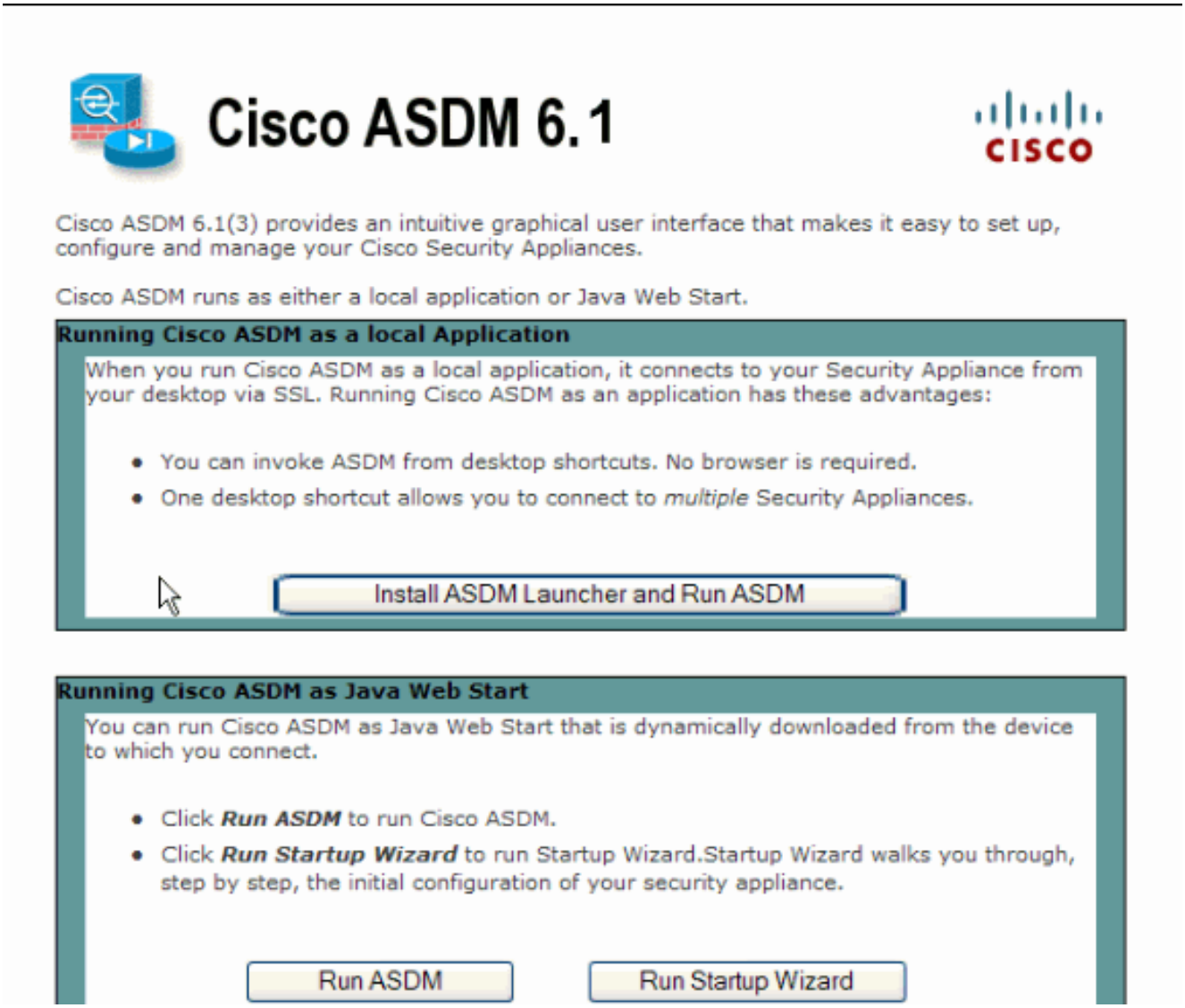
Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918 adressen, die in een labomgeving gebruikt zijn.

- VPN-tunnelconfiguratie ASDM
- Configuratie van routerdm
- ASA CLI-configuratie
- Configuratie van router CLI

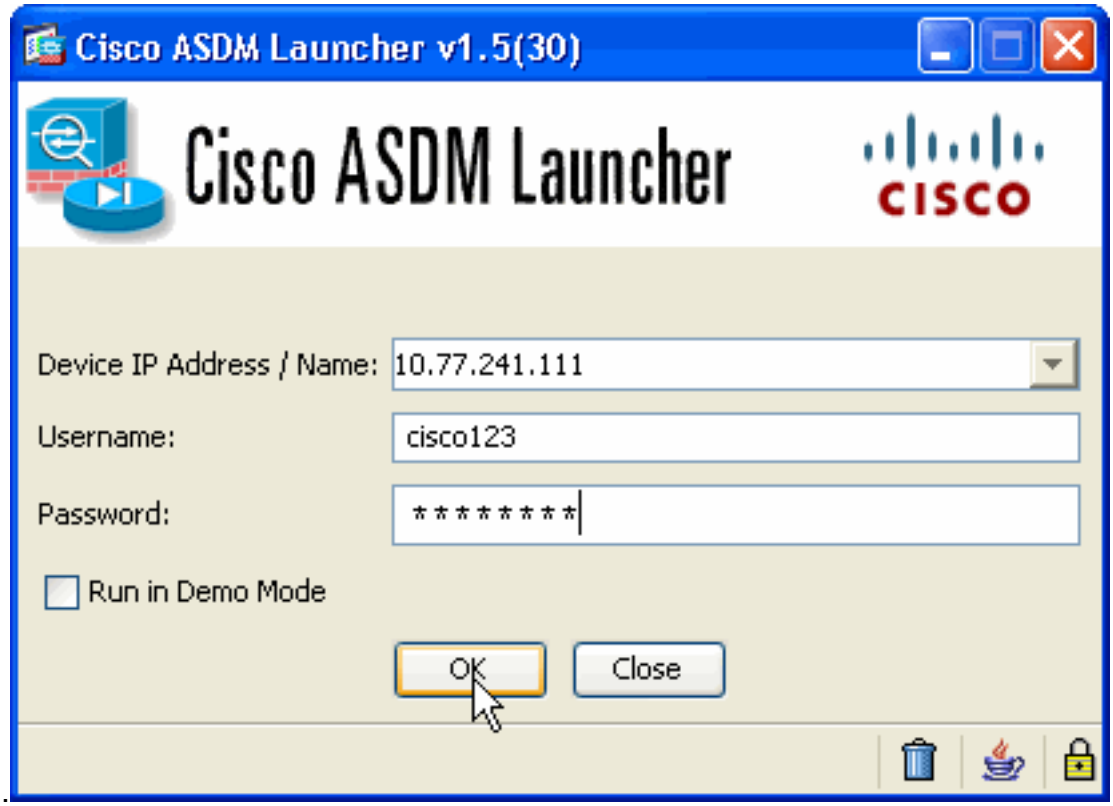
VPN-tunnelconfiguratie ASDM

Voltooi deze stappen om de VPN-tunnel te maken:

1. Open uw browser en voer **https://<IP_Address van de interface van ASA** in **die is geconfigureerd voor ASDM Access>**om toegang te krijgen tot de ASDM in de ASA.Controleer of alle waarschuwingen die uw browser u geeft, behoren tot de SSL-certificatie. De standaard gebruikersnaam en wachtwoord zijn beide leeg.De ASA presenteert dit venster om het downloaden van de ASDM-toepassing mogelijk te maken. Dit voorbeeld laadt de toepassing op de lokale computer en werkt niet in een Java-applet.

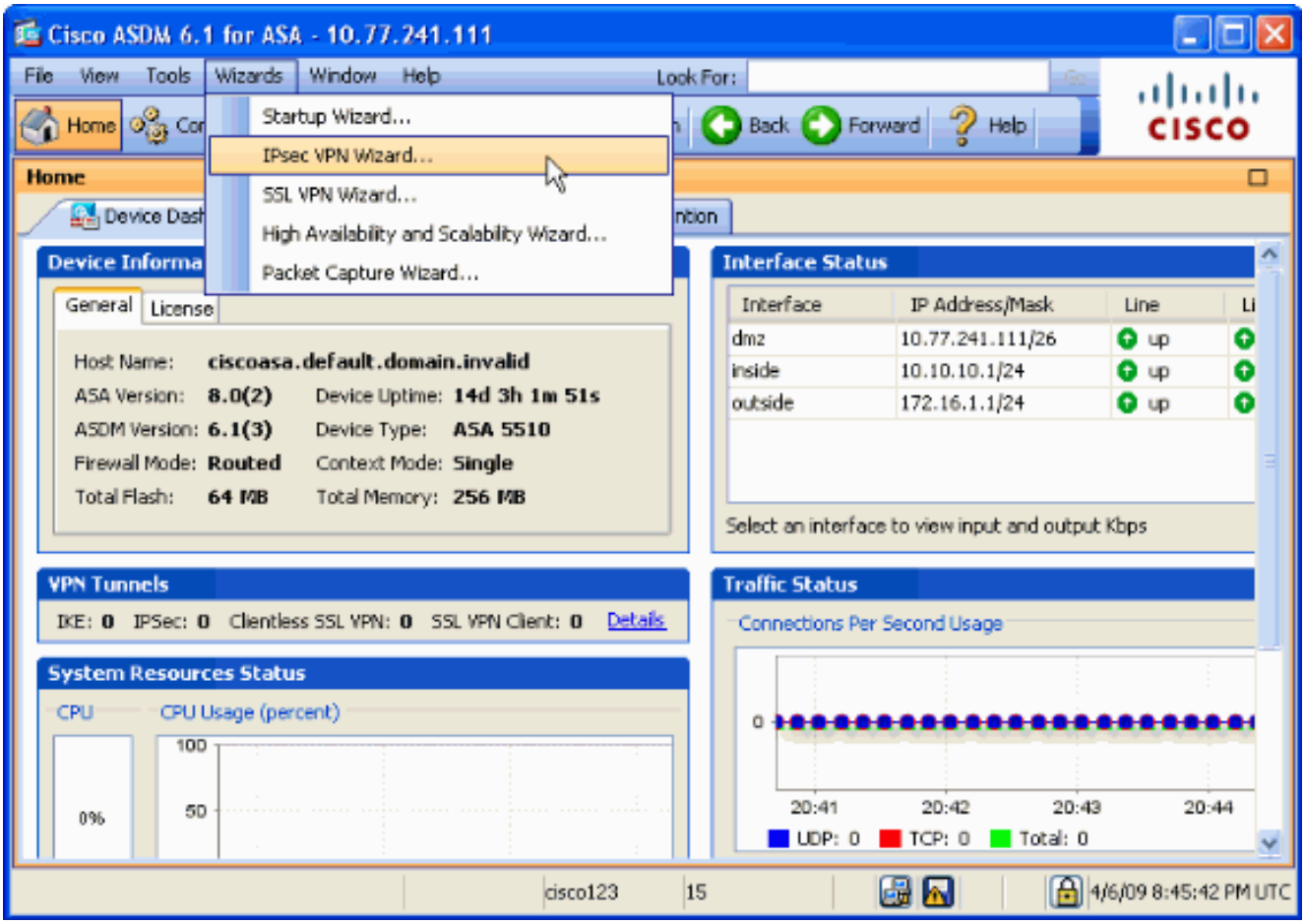


2. Klik op **Download ASDM Launcher en Start ASDM** om de installateur voor de ASDM-toepassing te downloaden.
3. Voltooi na het downloaden van de ASDM Launcher de stappen die door de aanwijzingen zijn geleid om de software te installeren en de Cisco ASDM Launcher uit te voeren.
4. Voer het IP-adres in voor de interface die u met de **http -** opdracht en een gebruikersnaam en wachtwoord hebt ingesteld als u er een hebt opgegeven.Dit voorbeeld gebruikt **cisco123** voor de gebruikersnaam en **cisco123** als het

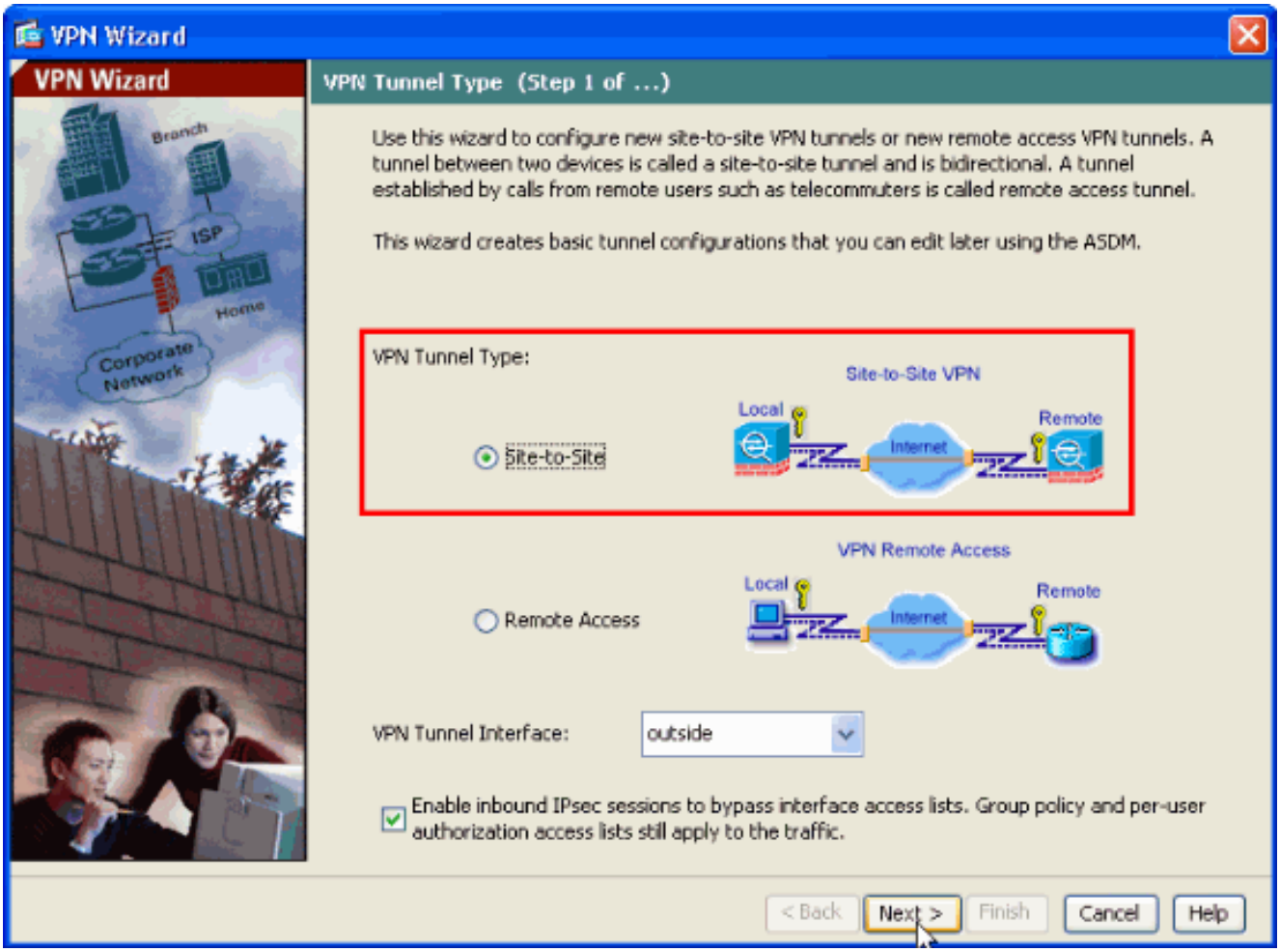


wachtwoord.

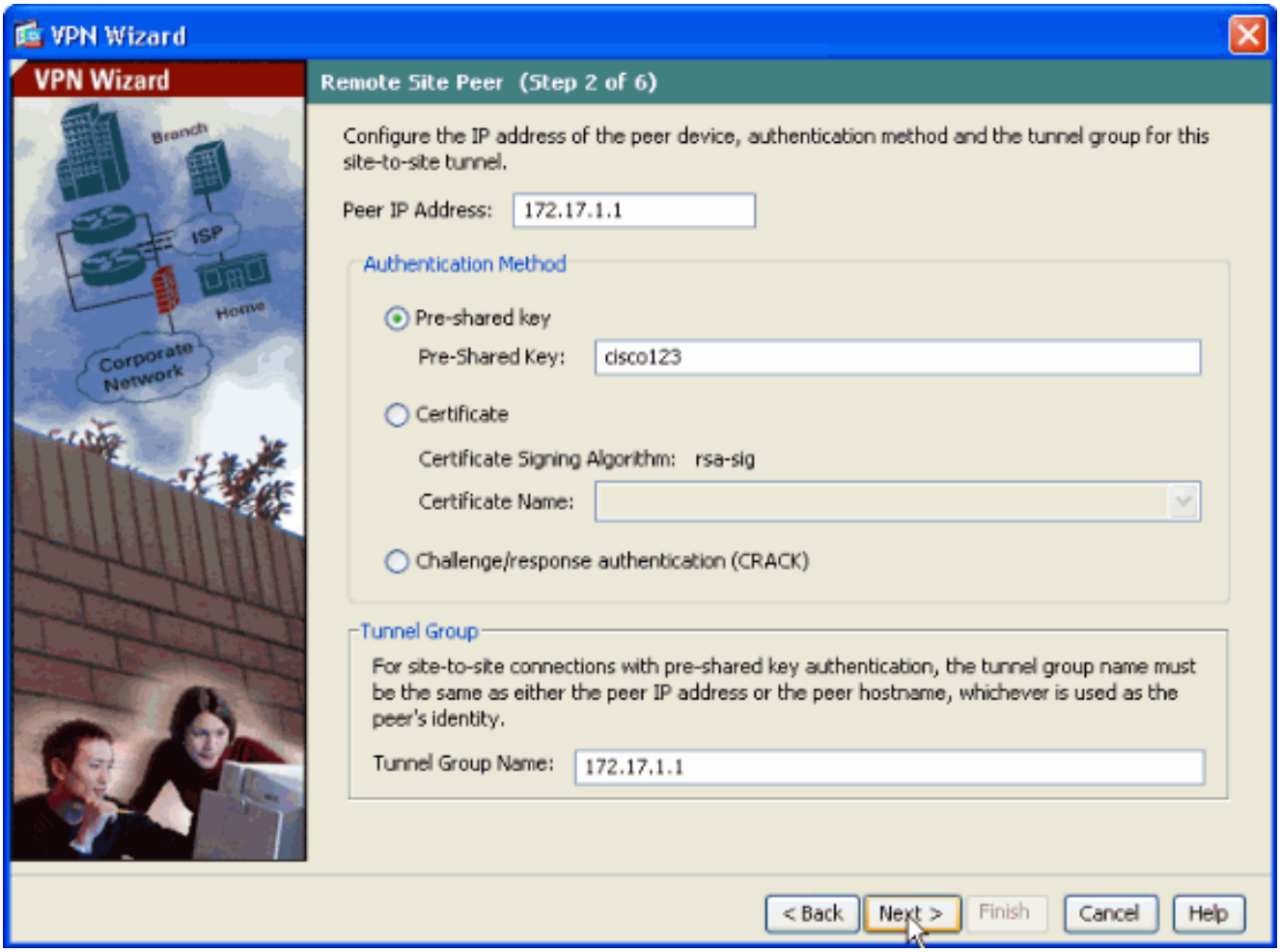
5. Start de **IPsec VPN-wizard** nadat de ASDM-toepassing is aangesloten op de ASA.



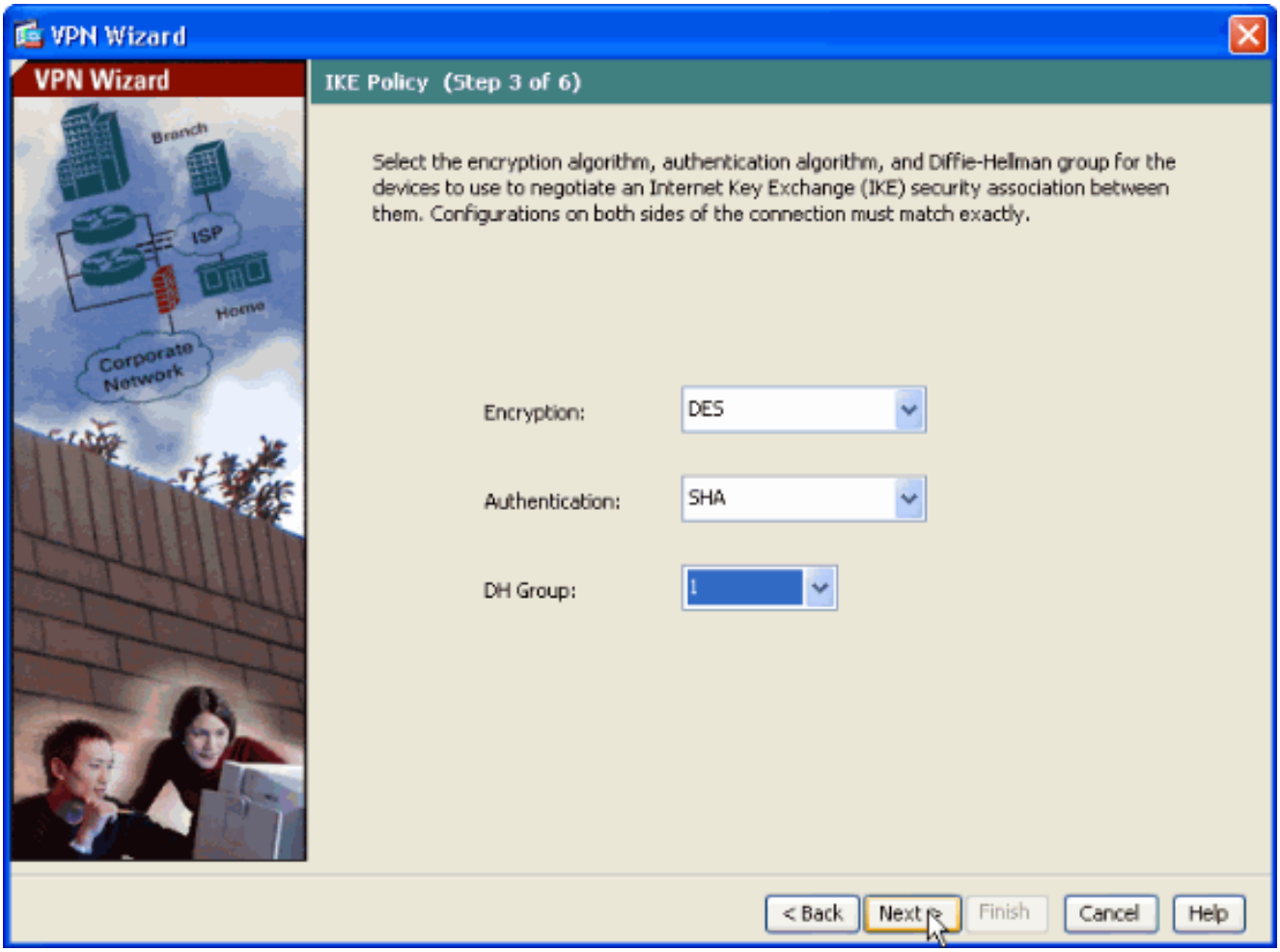
6. Kies het tunneltype **Site-to-Site** IPsec VPN en klik op **Volgende** zoals hier wordt getoond.



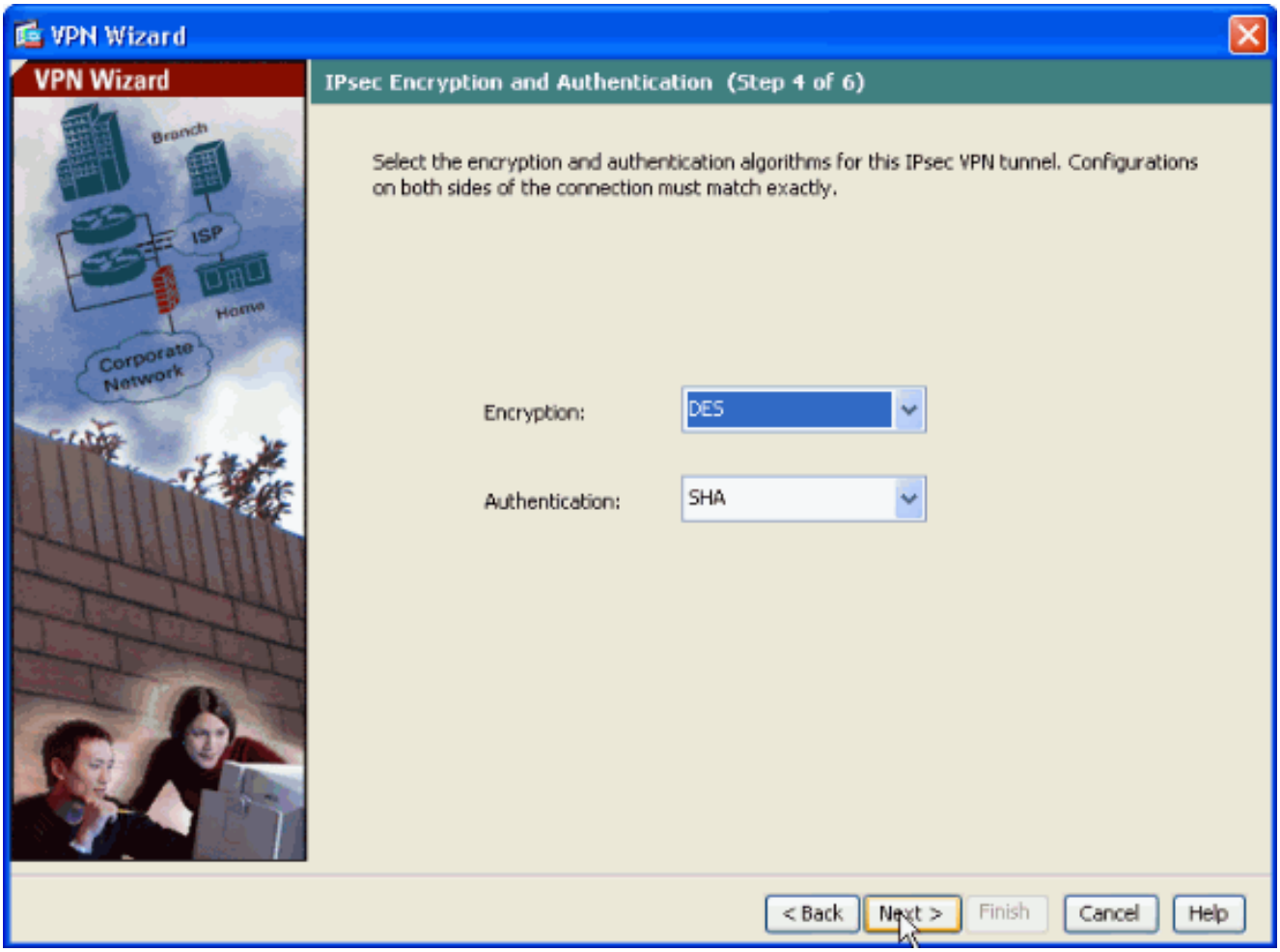
7. Specificeer het externe IP-adres van de externe peer. Voer de te gebruiken verificatieinformatie in, de vooraf gedeelde sleutel in dit voorbeeld. De pre-gedeelde sleutel die in dit voorbeeld wordt gebruikt is **cisco123**. De **Naam van de Tunnel Groep** zal uw buiten IP adres standaard zijn als u L2L VPN configureren. Klik op **Volgende**.



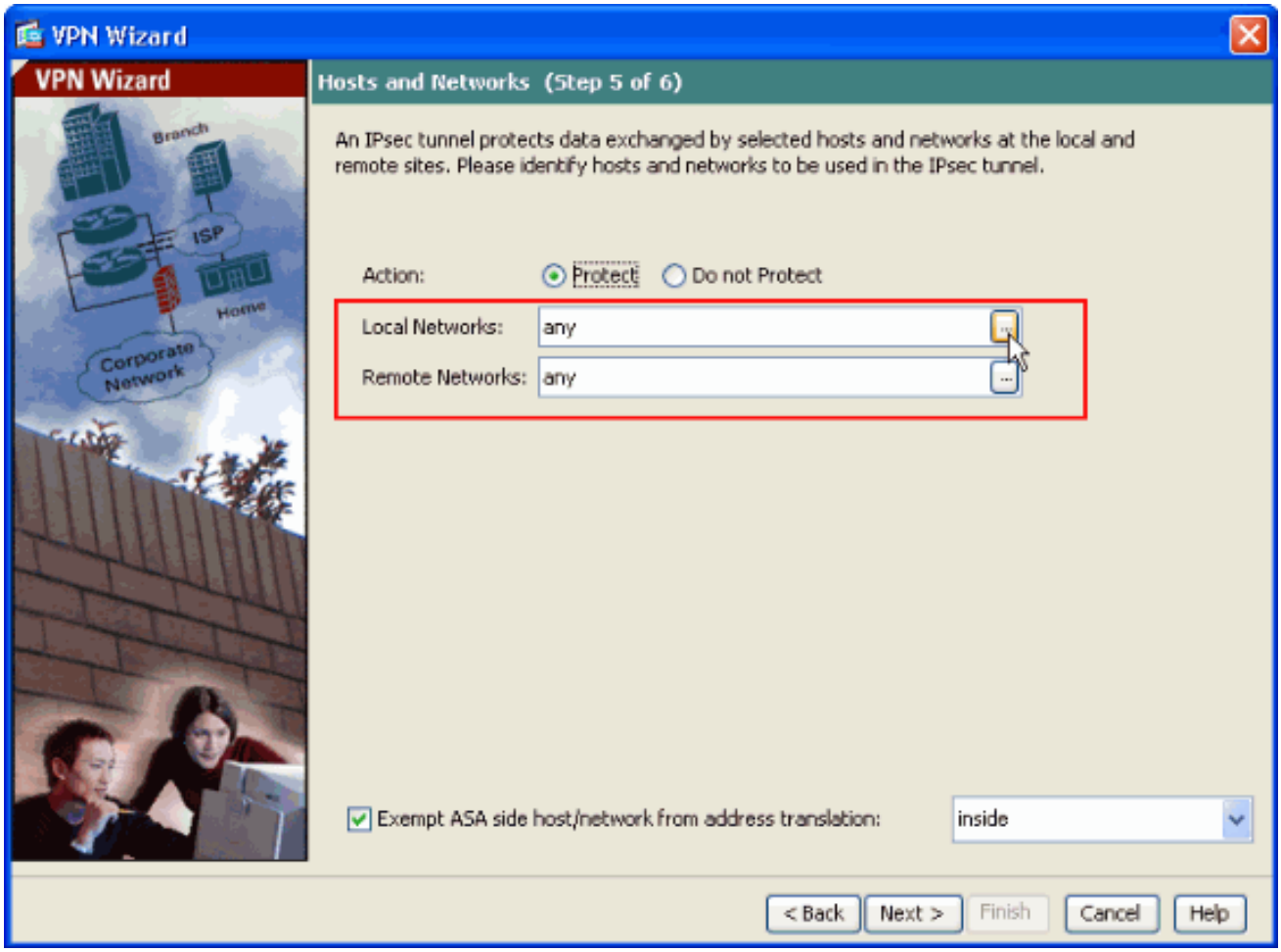
8. Specificeer de eigenschappen die voor IKE moeten worden gebruikt, ook bekend als Fase 1. Deze eigenschappen moeten hetzelfde zijn op zowel de ASA als de IOS Router. Klik op **Volgende**.



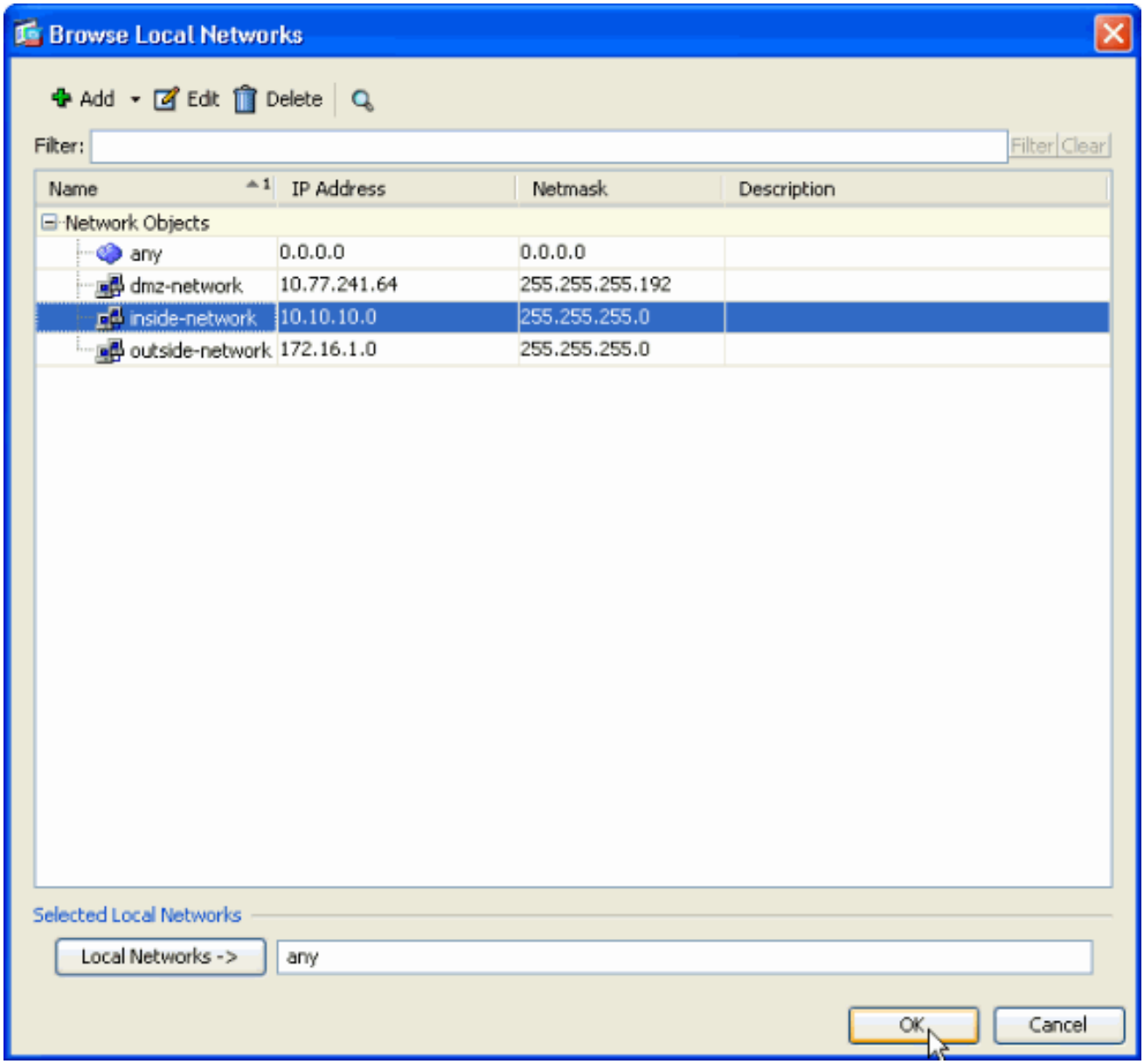
9. Specificeer de eigenschappen die voor IPsec moeten worden gebruikt, ook bekend als Fase 2. Deze eigenschappen moeten op zowel de ASA als de IOS router overeenkomen. Klik op **Volgende**.



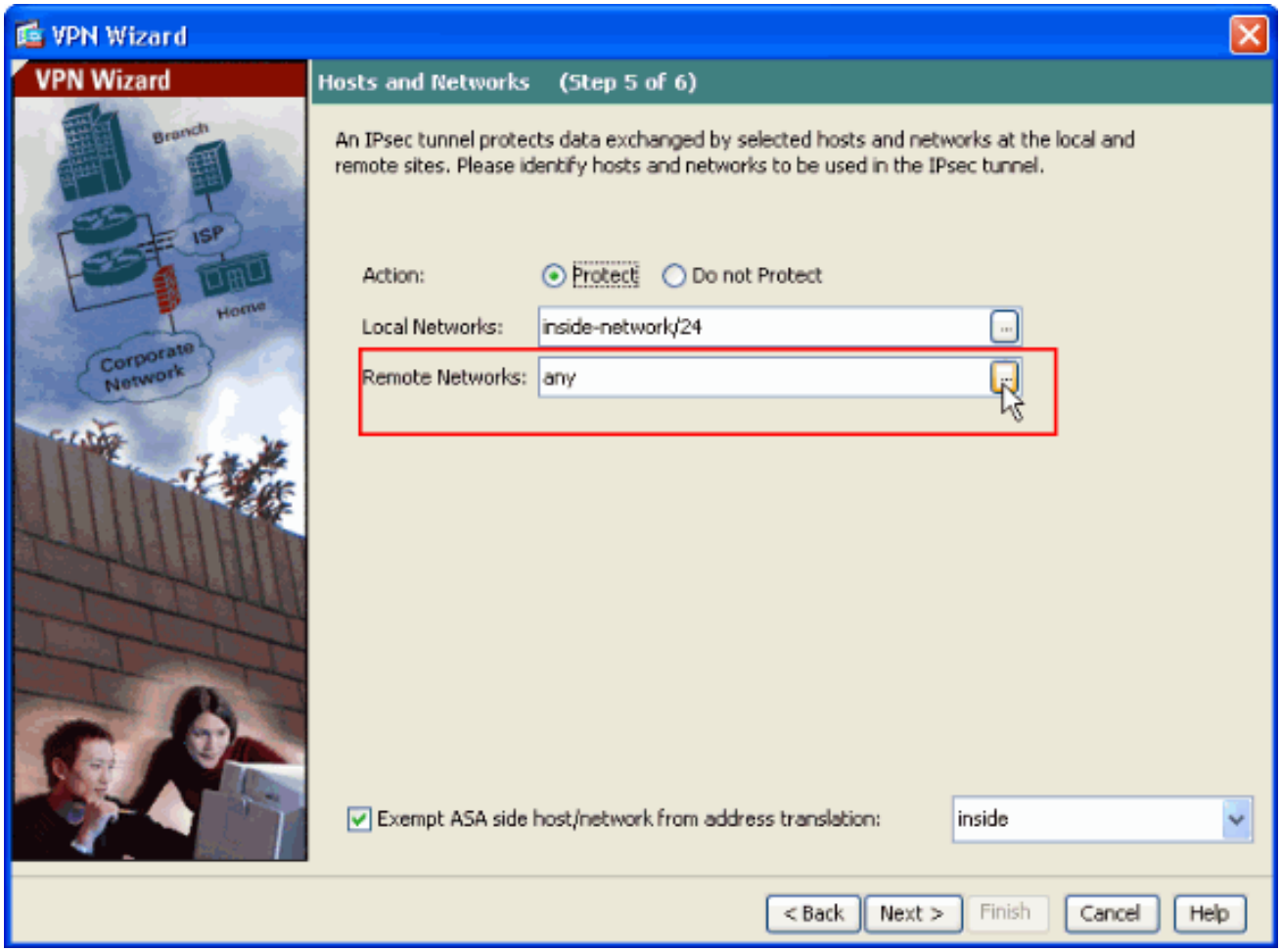
10. Specificeer de hosts waarvan het verkeer door de VPN-tunnel moet kunnen passeren. In deze stap moet u de **lokale** en **afstandsnetwerken** voor de VPN-tunnel beschikbaar stellen. Klik op de knop naast **Local Networks** zoals hier aangegeven om het lokale netwerkadres in de vervolgkeuzelijst te
kiezen.



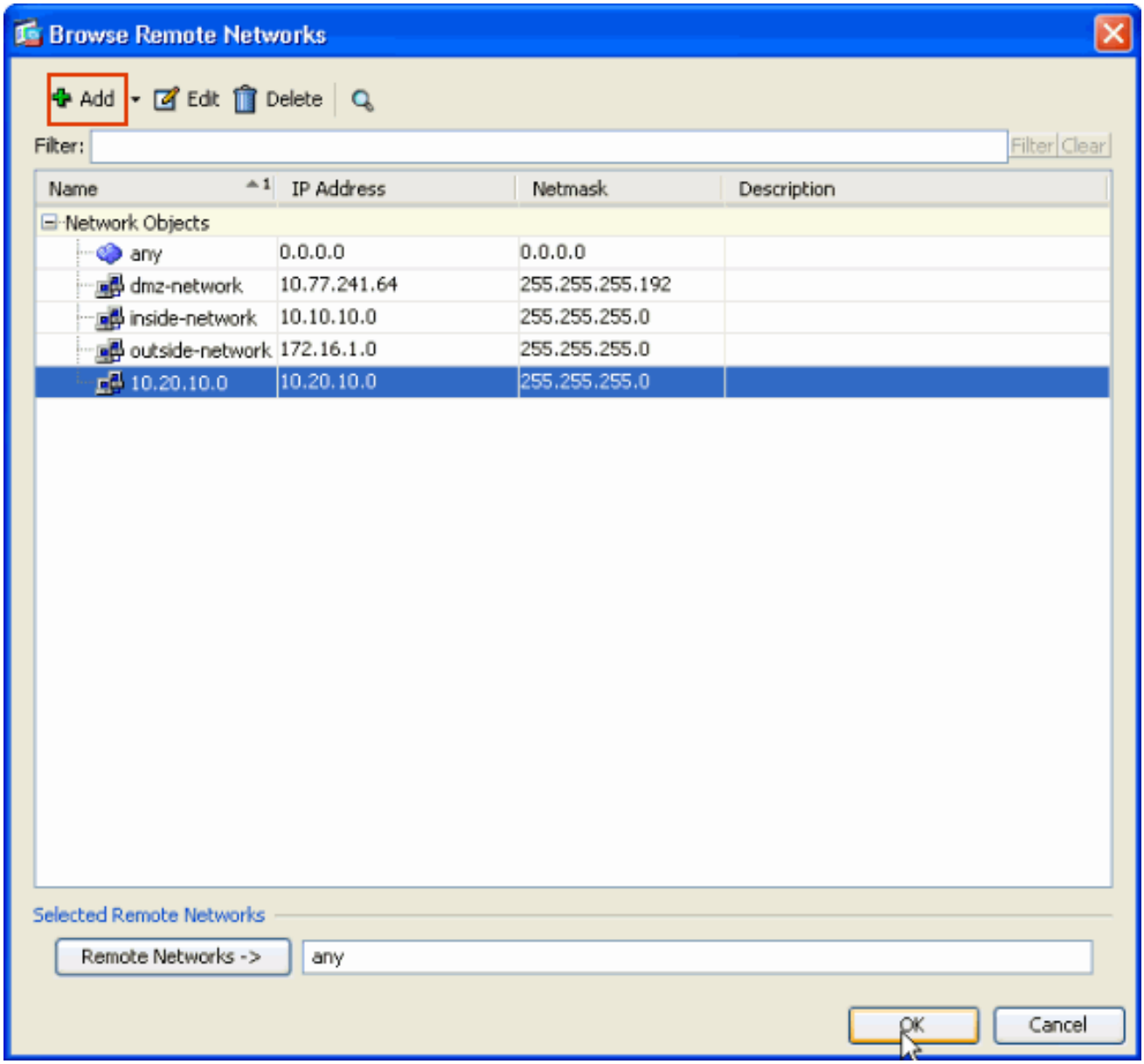
11. Kies het adres **Local Network** en klik vervolgens op **OK** zoals hier wordt weergegeven.



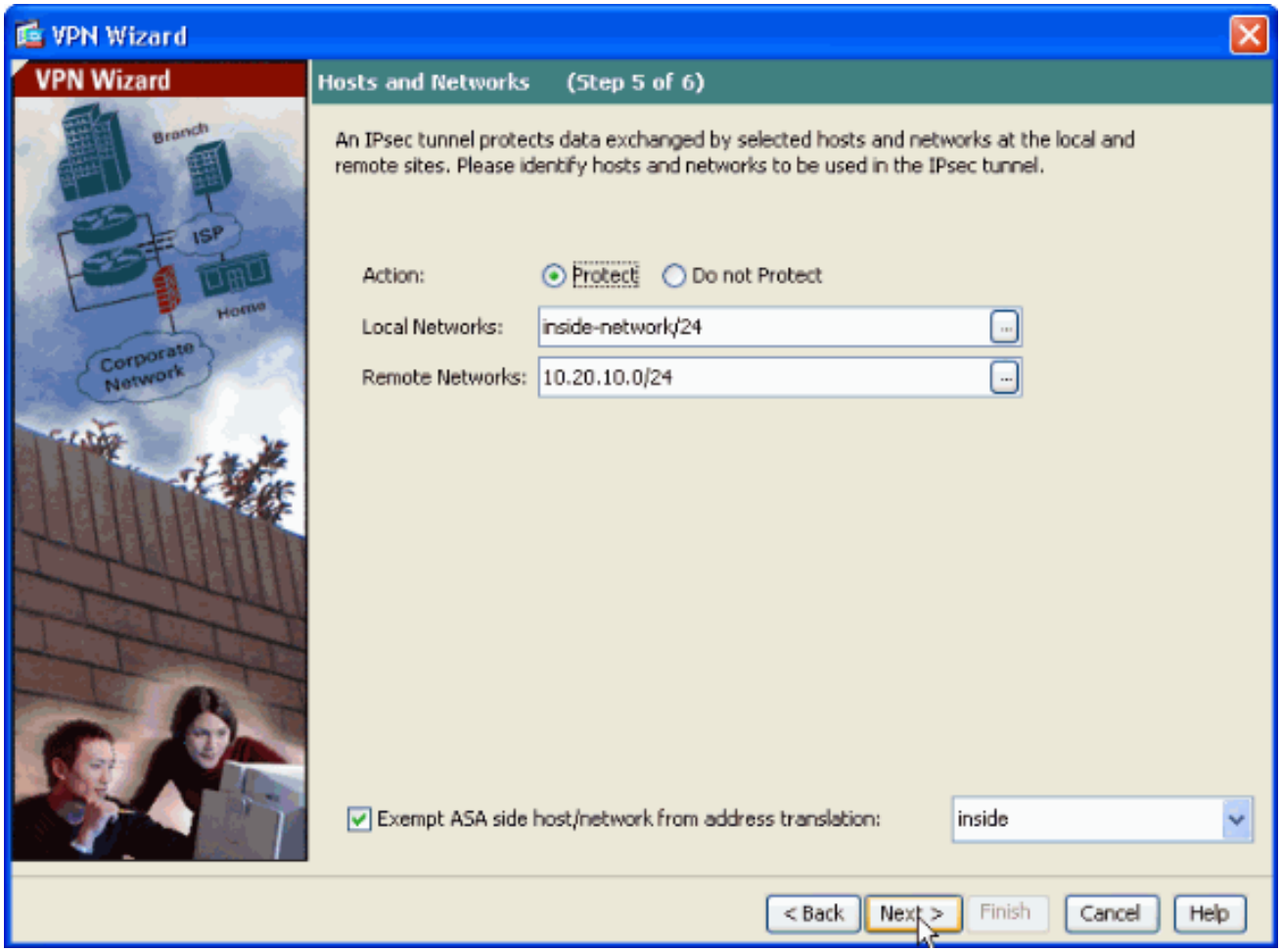
12. Klik op de knop naast **Remote Networks** zoals hieronder aangegeven, om het externe netwerkadres in de vervolgkeuzelijst te kiezen.



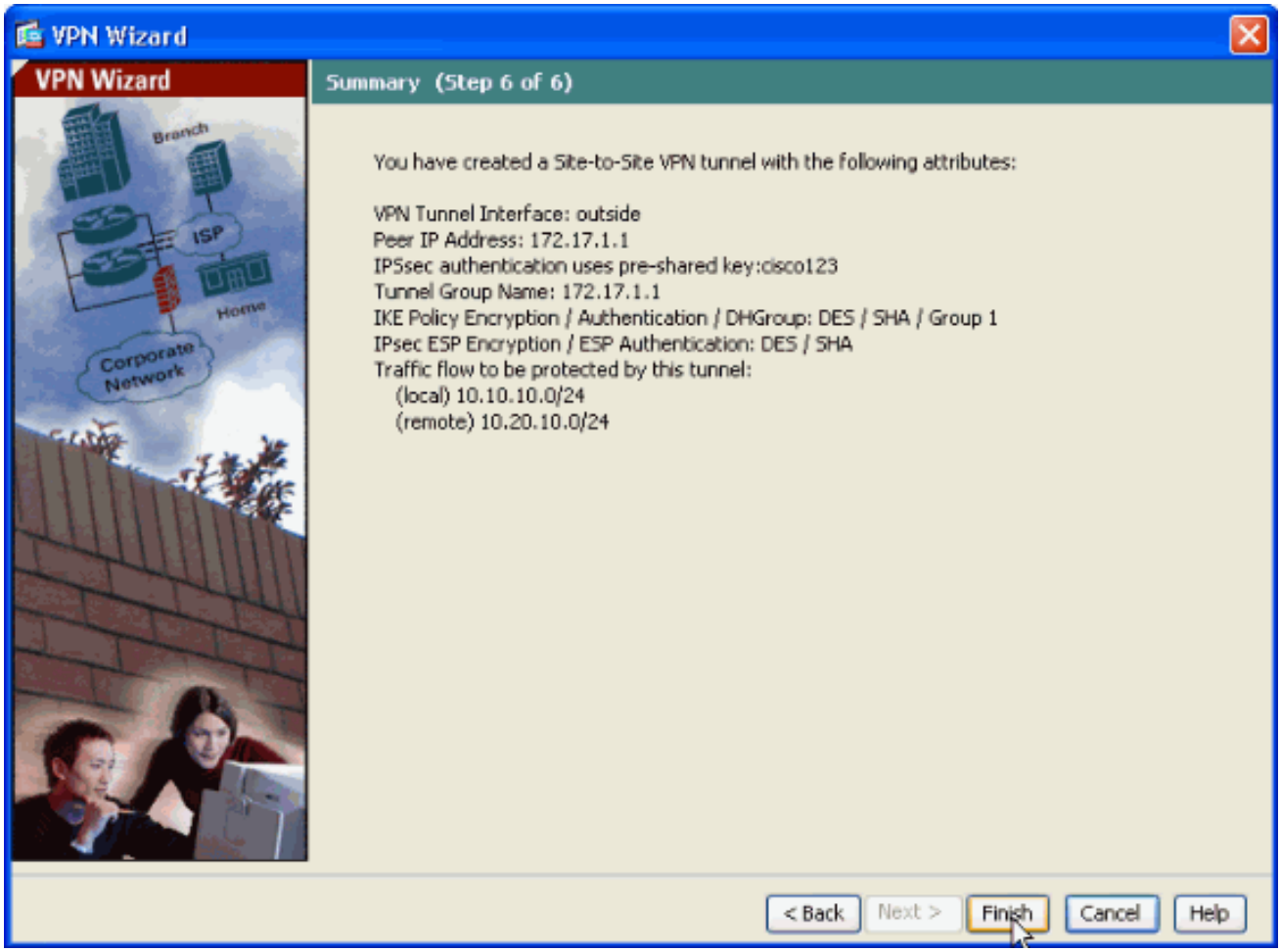
13. Kies het adres **van** het **Remote Network** en klik vervolgens op **OK** zoals hieronder wordt weergegeven.**N.B.:** Als u het Remote Network niet in de lijst hebt staan, moet het netwerk aan de lijst worden toegevoegd door op **Toevoegen** te klikken.



14. Controleer de **vrijstellingsASA side host/network van adresomzetting** selectieteken om te voorkomen dat het tunnelverkeer **netwerkadresomzetting** ondergaat. Klik vervolgens op **Volgende**.



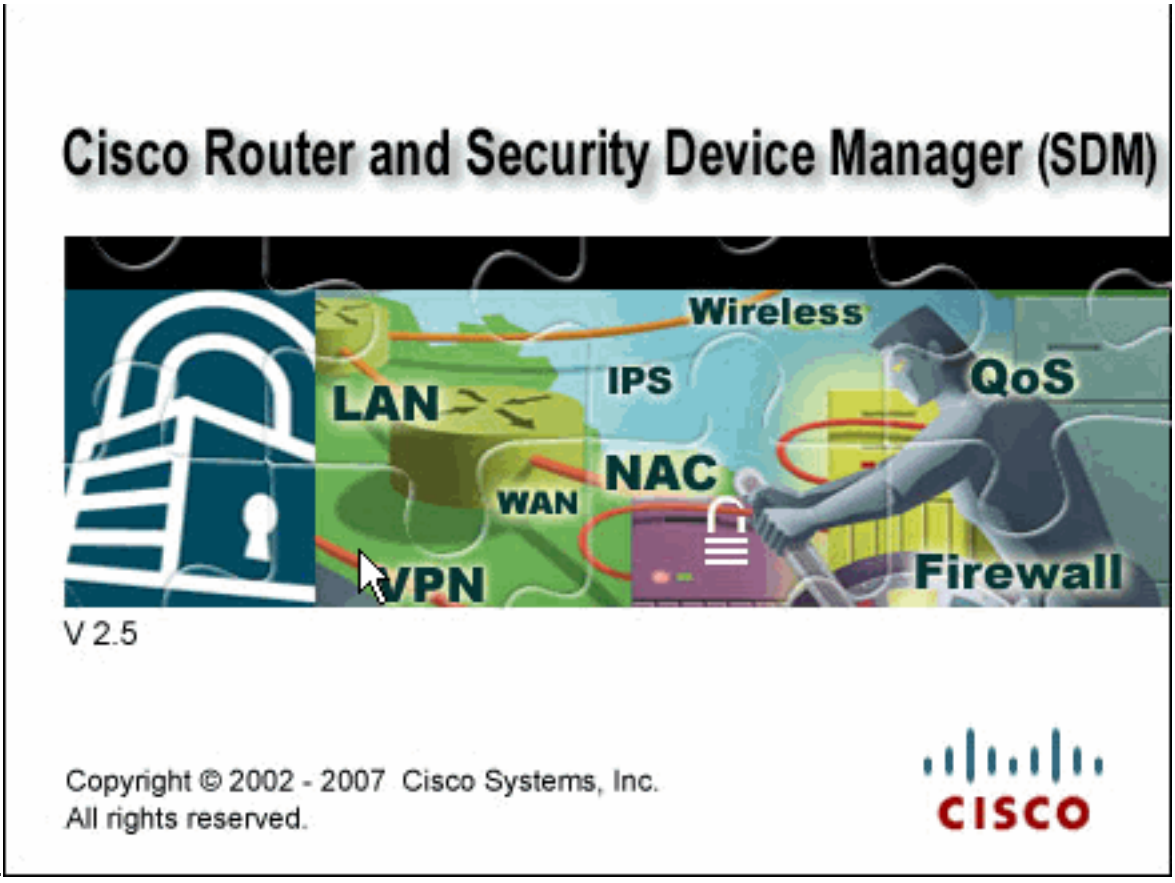
15. De eigenschappen die door de VPN Wizard worden gedefinieerd, worden in deze samenvatting weergegeven. Controleer de configuratie en klik op **Voltooien** wanneer u tevreden bent met de juiste instellingen.



Configuratie van routerdm

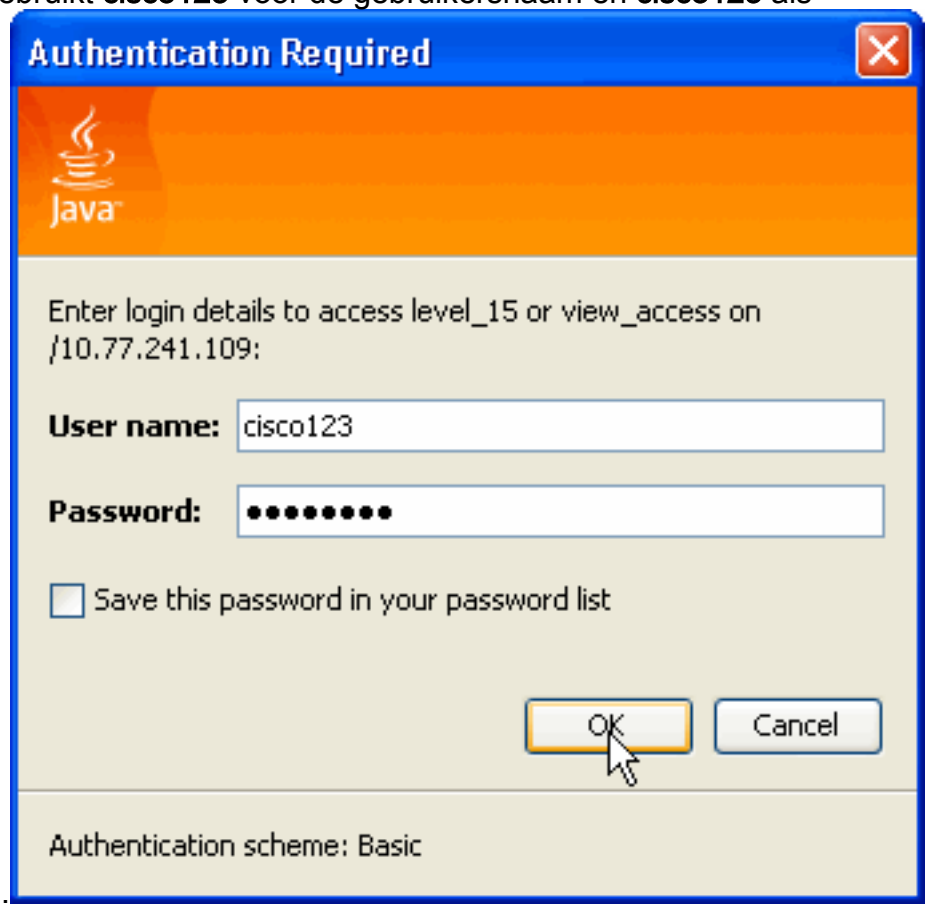
Voltooi deze stappen om site-to-Site VPN-tunnelheid op de Cisco IOS-router te configureren:

1. Open uw browser en voer **https://<IP_Address van de interface van de router** in **die voor** de **Toegang** van **het** Sdm op de router **is gevormd**.Controleer of alle waarschuwingen die uw browser u geeft, behoren tot de SSL-certificatie. De standaard gebruikersnaam en wachtwoord zijn beide leeg.De router stelt dit venster voor om de download van de toepassing te toestaan. Dit voorbeeld laadt de toepassing op de lokale computer en werkt niet in een Java-



applet.

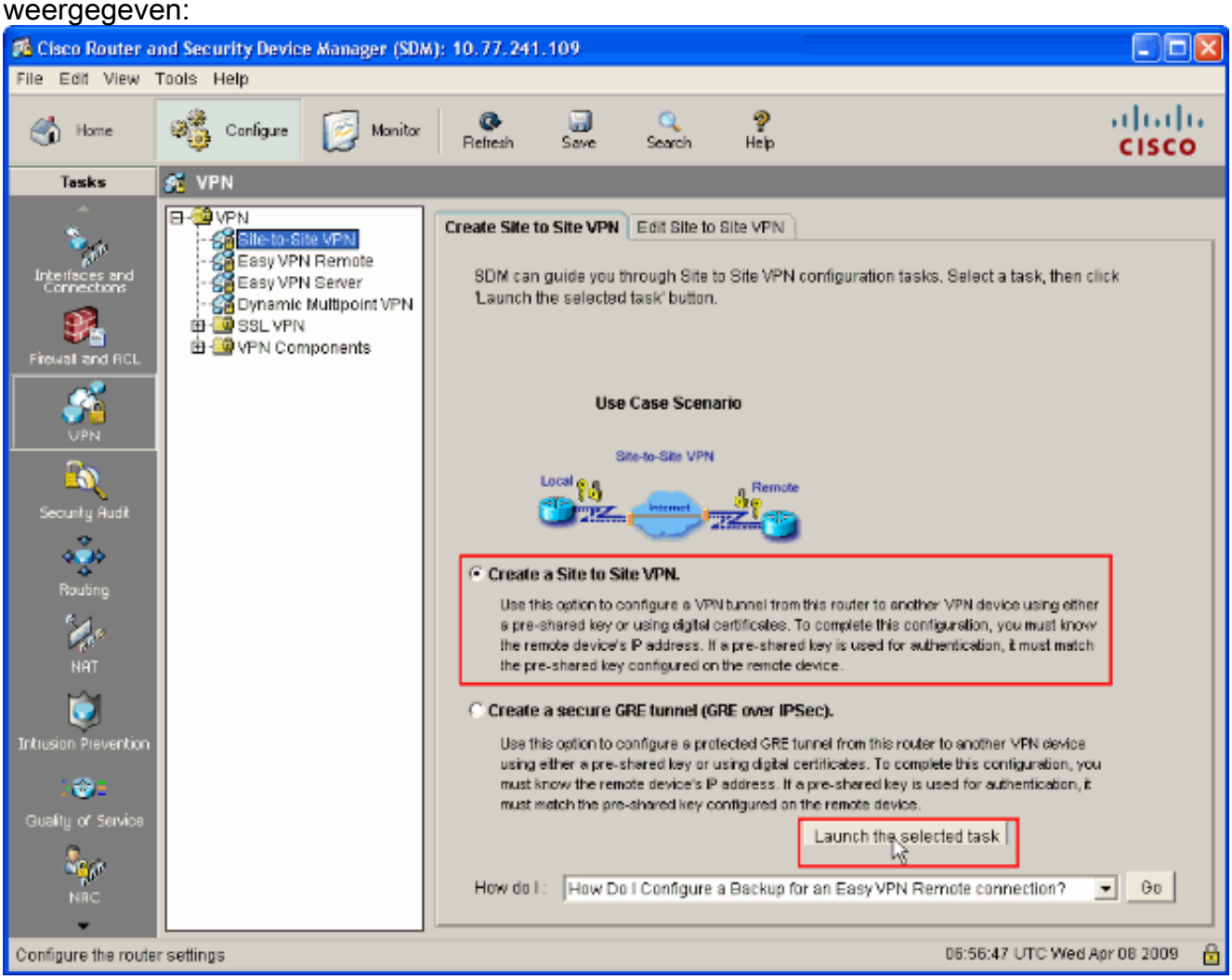
2. De download van het dm begint nu. Zodra de lantaarn van het Sdm wordt gedownload, voltooien de stappen die door de herinnering worden geregisseerd om de software te installeren en de Launcher van Cisco Sdm in werking te stellen.
3. Voer de **gebruikersnaam** en het **wachtwoord in** als u deze hebt ingesteld en klik op **OK**.Dit voorbeeld gebruikt **cisco123** voor de gebruikersnaam en **cisco123** als



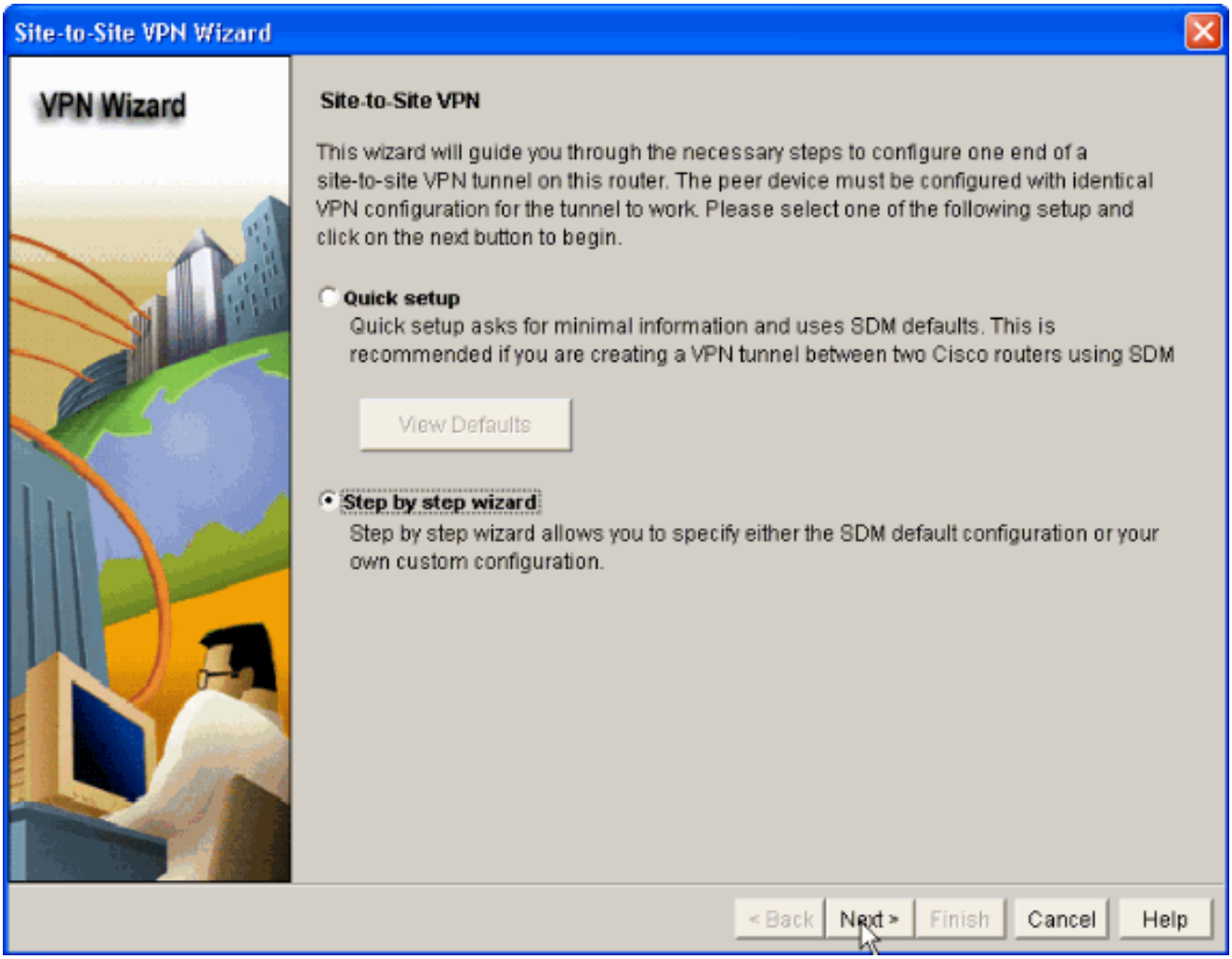
wachtwoord.

4. Kies **Configuration->VPN->**Site-to-Site VPN en klik op de radioknop naast **Een Site-to-Site**

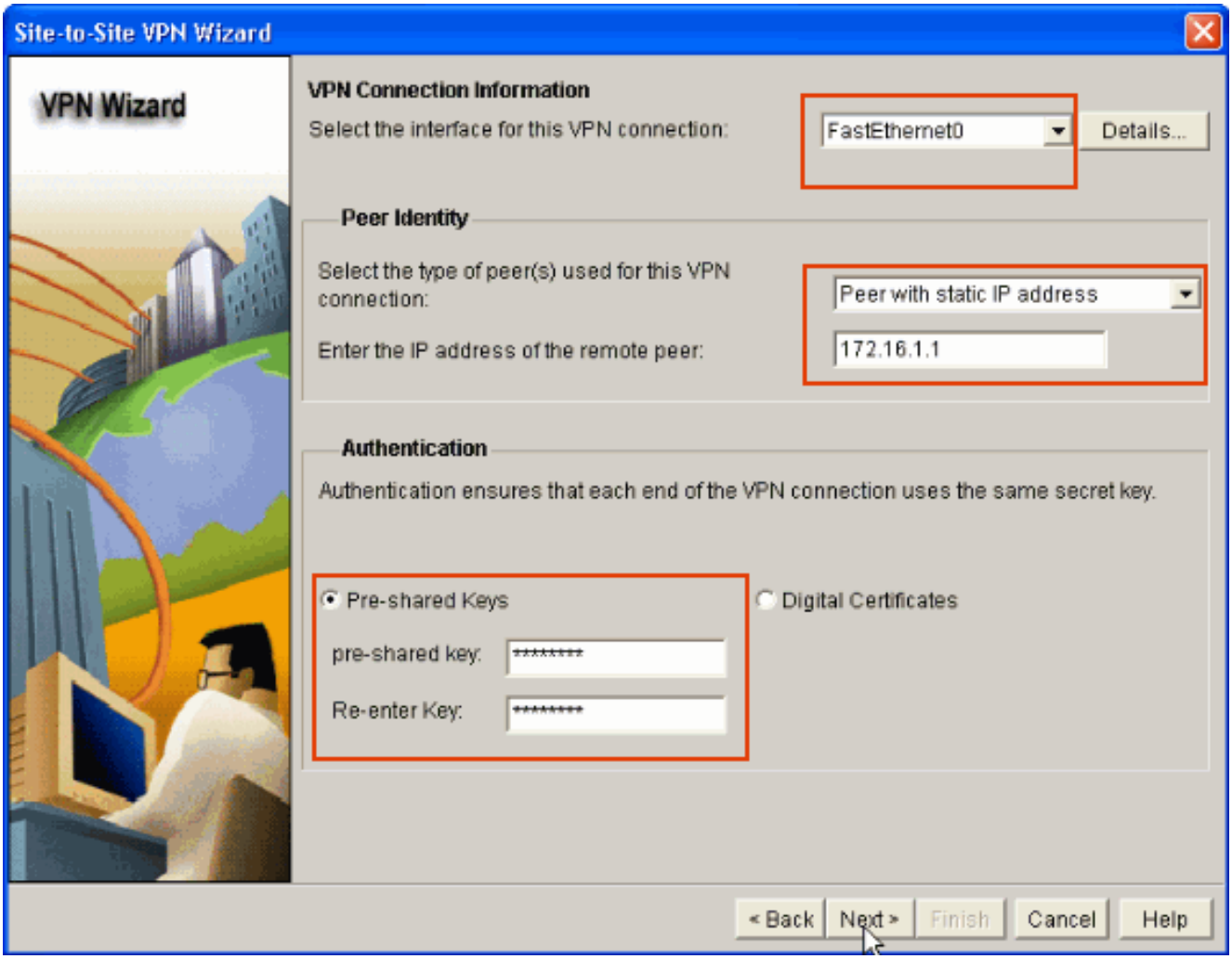
VPN-on-**Site** VPN **maken** op de startpagina **met** SDH. Klik vervolgens op **De geselecteerde taak starten** zoals hieronder wordt weergegeven:



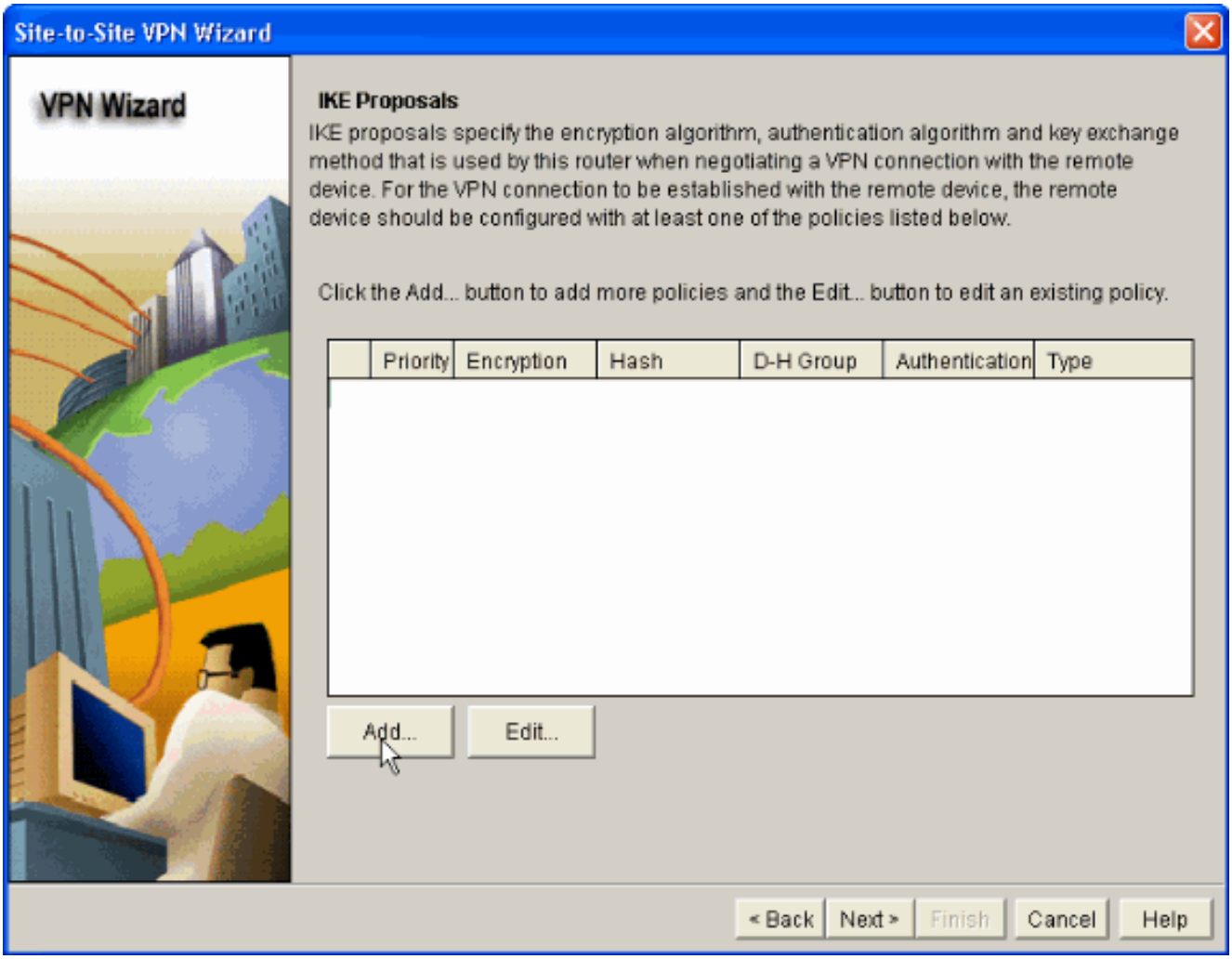
5. Kies **Stap voor stap wizard** om verder te gaan met de configuratie:



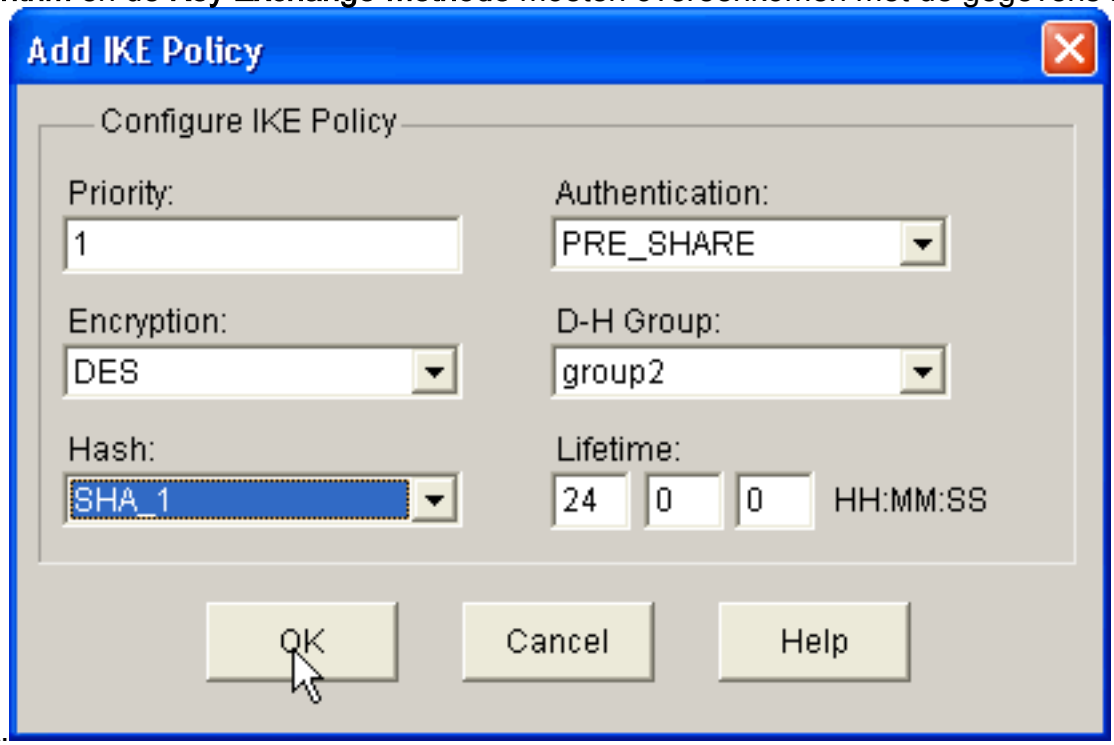
6. Typ in het volgende venster de **VPN-verbindingsinformatie** in de betreffende ruimtes. Selecteer de interface van de VPN-tunnel in de vervolgkeuzelijst. Hier, **FastEthernet0** wordt geselecteerd. Selecteer in het gedeelte **Peer Identity** de optie **Peer met het statische IP-adres** en geef het externe IP-adres op. Typ vervolgens de **Pre-Shared key** (**cisco123** in dit voorbeeld) in de sectie Verificatie zoals getoond. Klik vervolgens op **Volgende**.



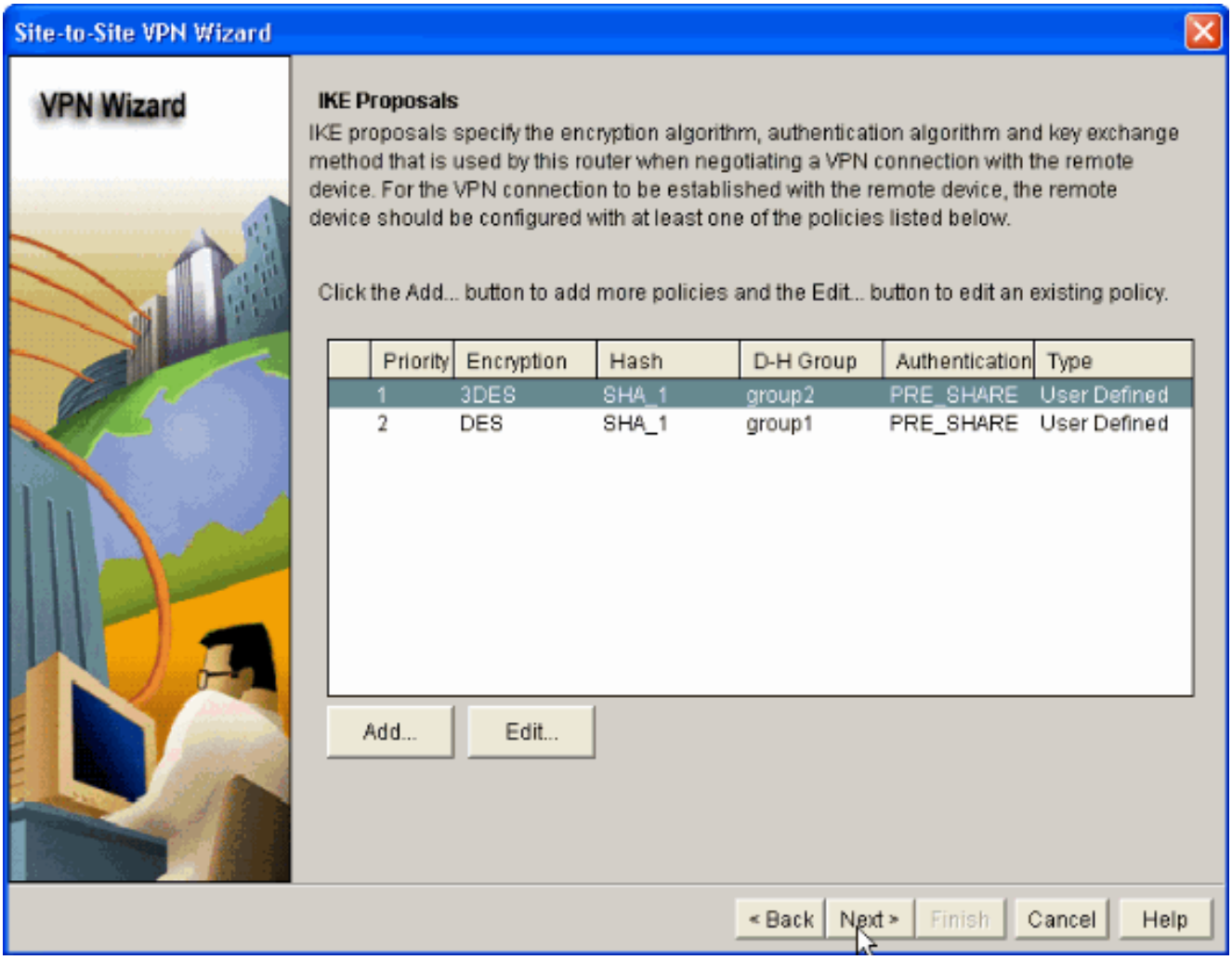
7. Klik op **Add** om IKE-voorstellen toe te voegen die het **Encryption Algorithm, Authentication Algorithm** en de **Key Exchange-methode** specificeren.



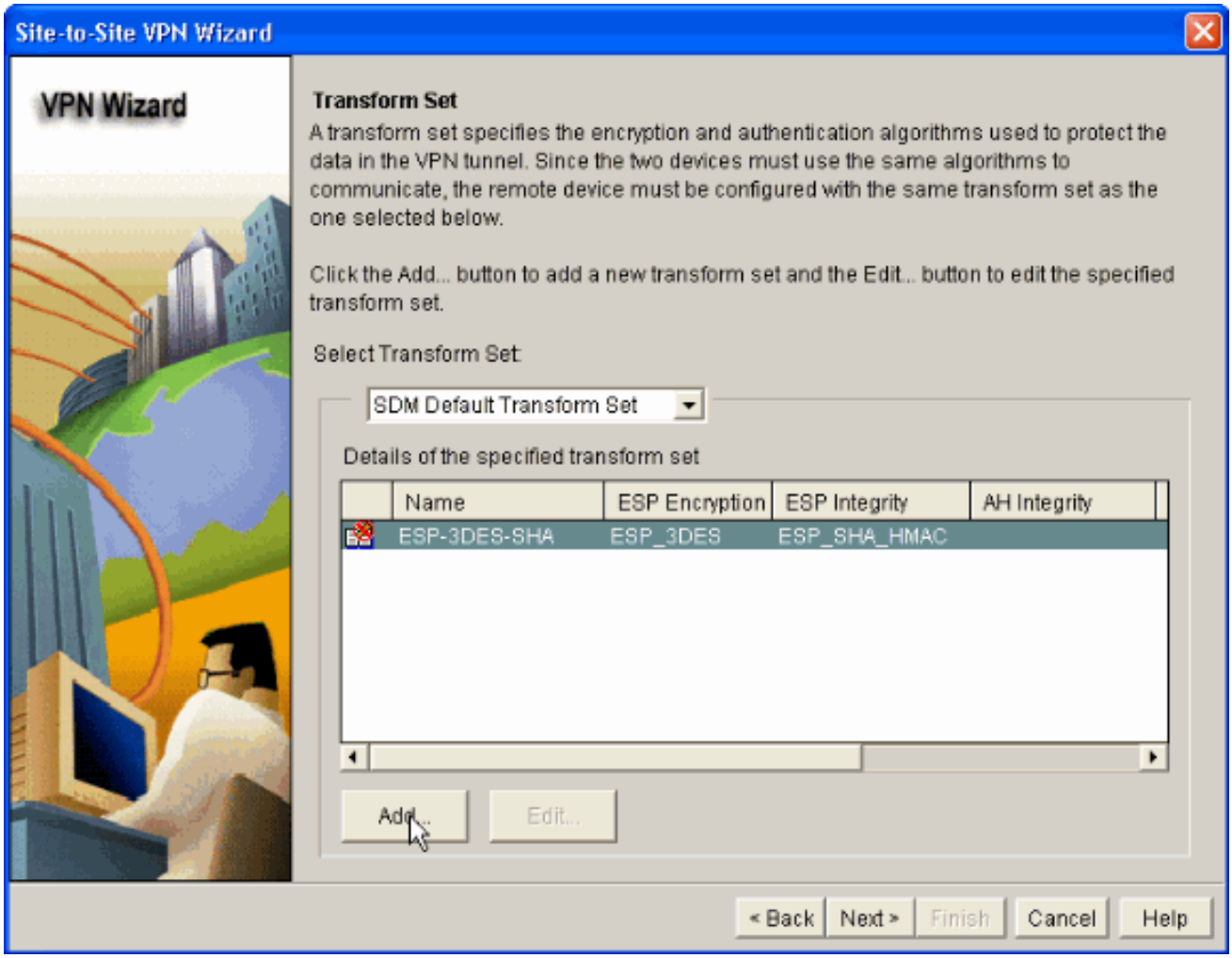
8. Typ **Encryption Algorithm**, **verificatie Algorithm** en de **Key Exchange-methode** zoals hier aangegeven, en klik vervolgens op **OK**. De waarden **Encryption Algorithm**, **Authentication Algorithm** en de **Key Exchange-methode** moeten overeenkomen met de gegevens in de ASA.



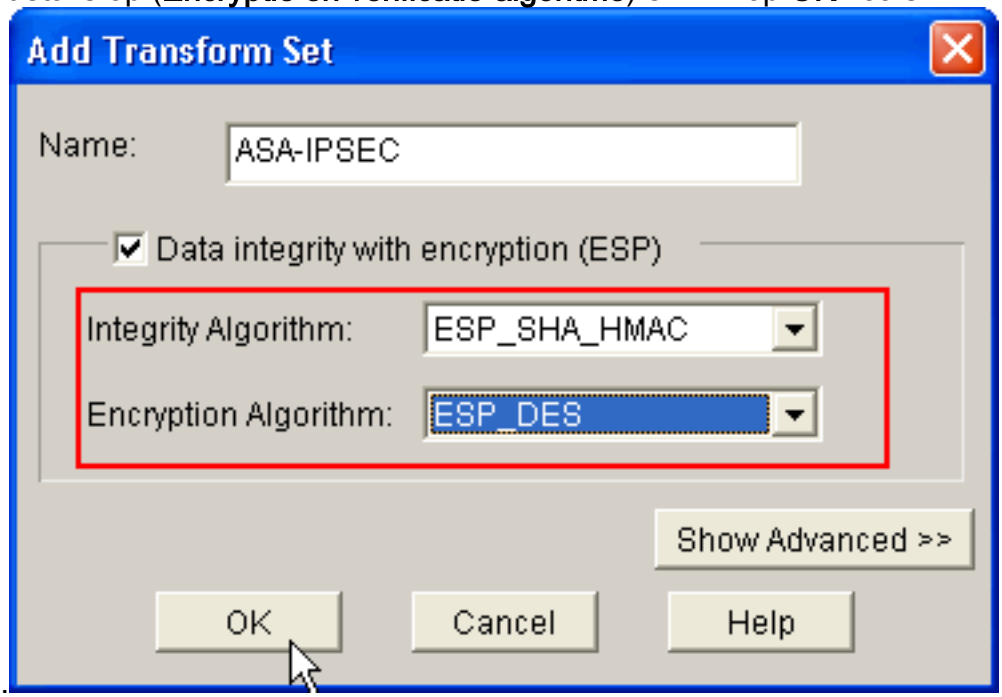
9. Klik op **Volgende** zoals hier wordt weergegeven.



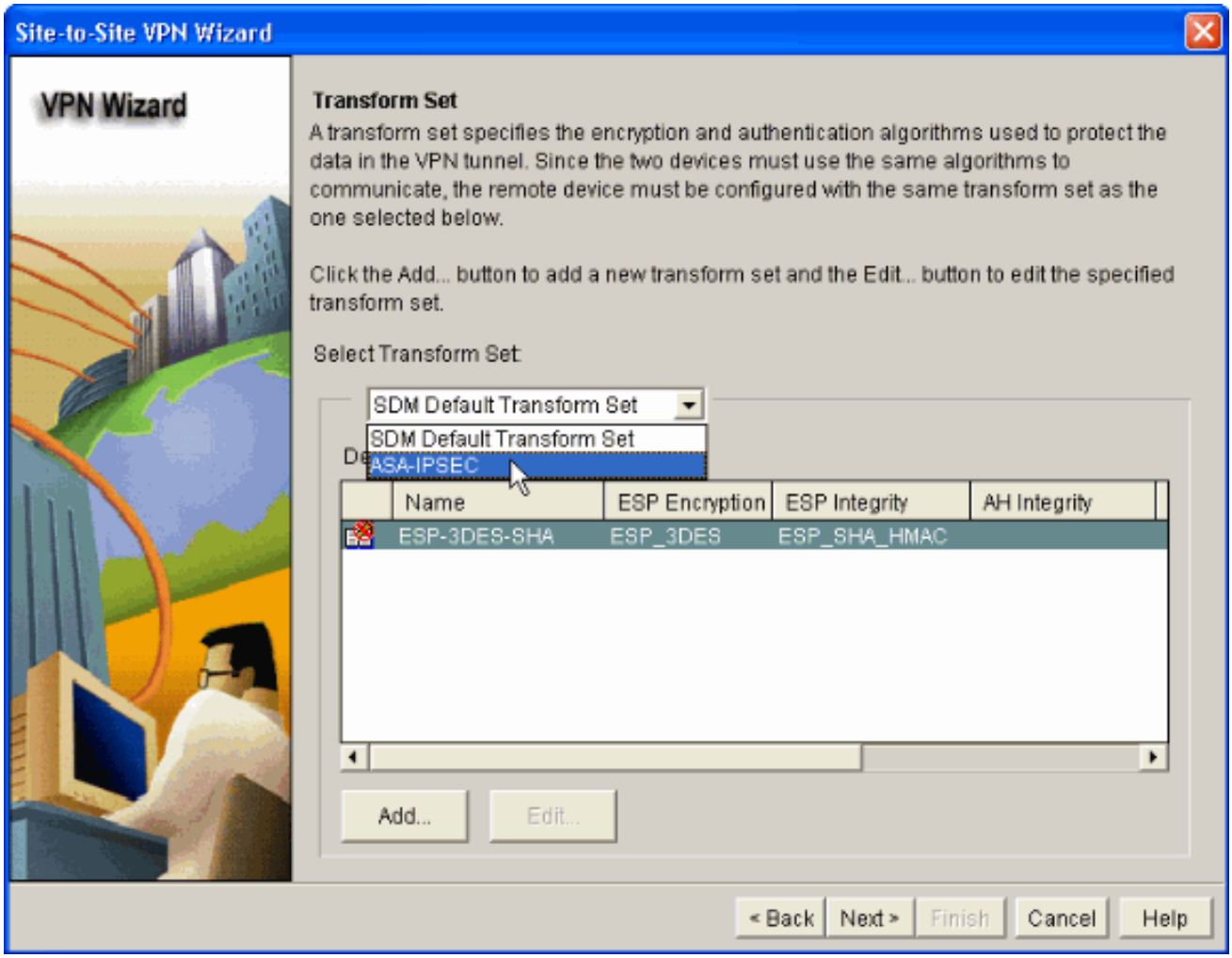
10. In dit nieuwe venster dienen de details **voor het** omzetten van de **instellingen** te worden verstrekt. Met de Instellen Omzetten wordt de **Encryptie** en **verificatie**-algoritmen gespecificeerd die worden gebruikt om **gegevens in VPN-tunnels** te beschermen. Klik vervolgens op **Toevoegen** om deze gegevens te verstrekken. U kunt indien nodig een aantal transformatiesets toevoegen door op **Toevoegen** te klikken en de gegevens te verstrekken.



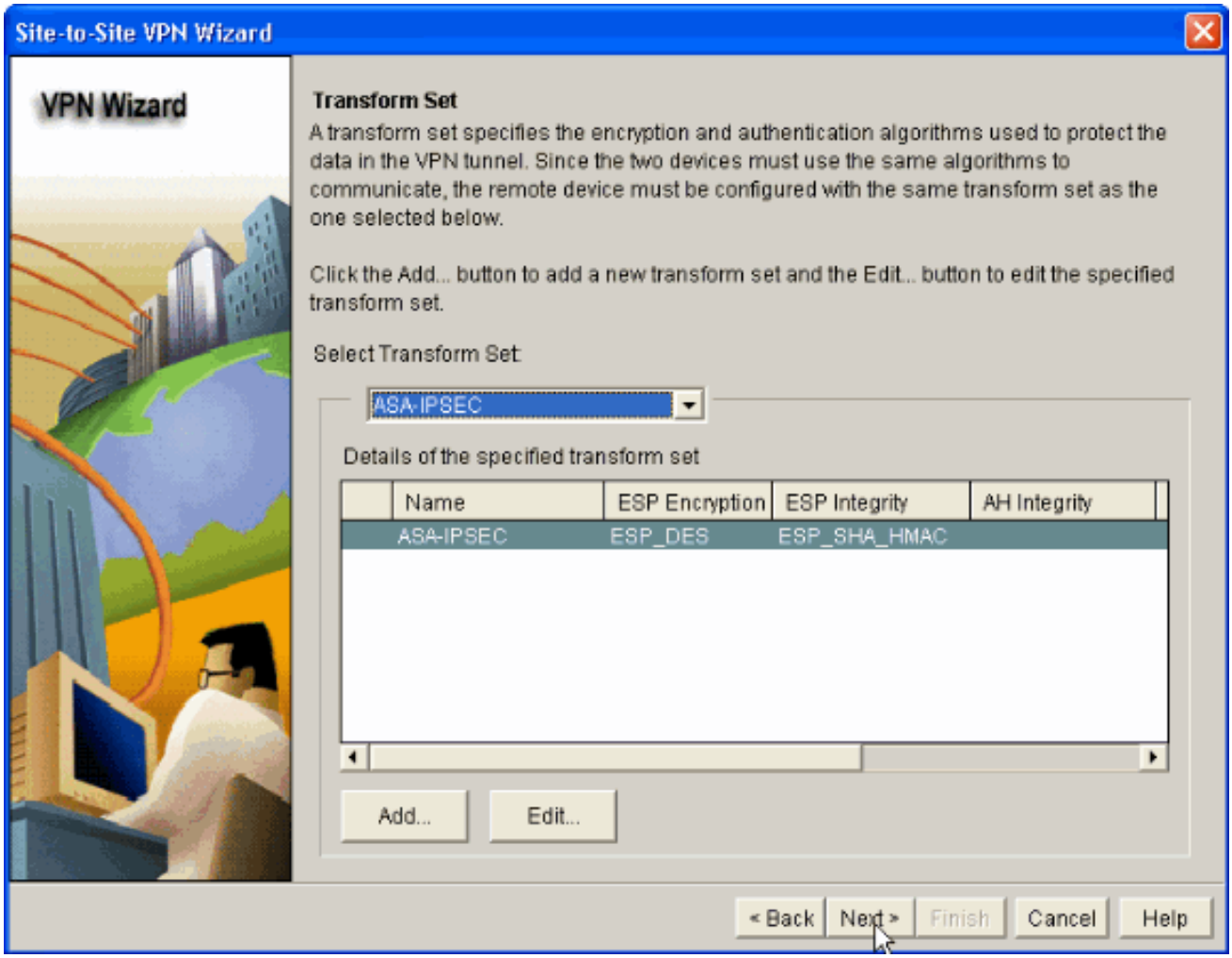
11. Geef de **Set**-details op (**Encryptie en verificatie-algoritme**) en klik op **OK** zoals aangegeven.



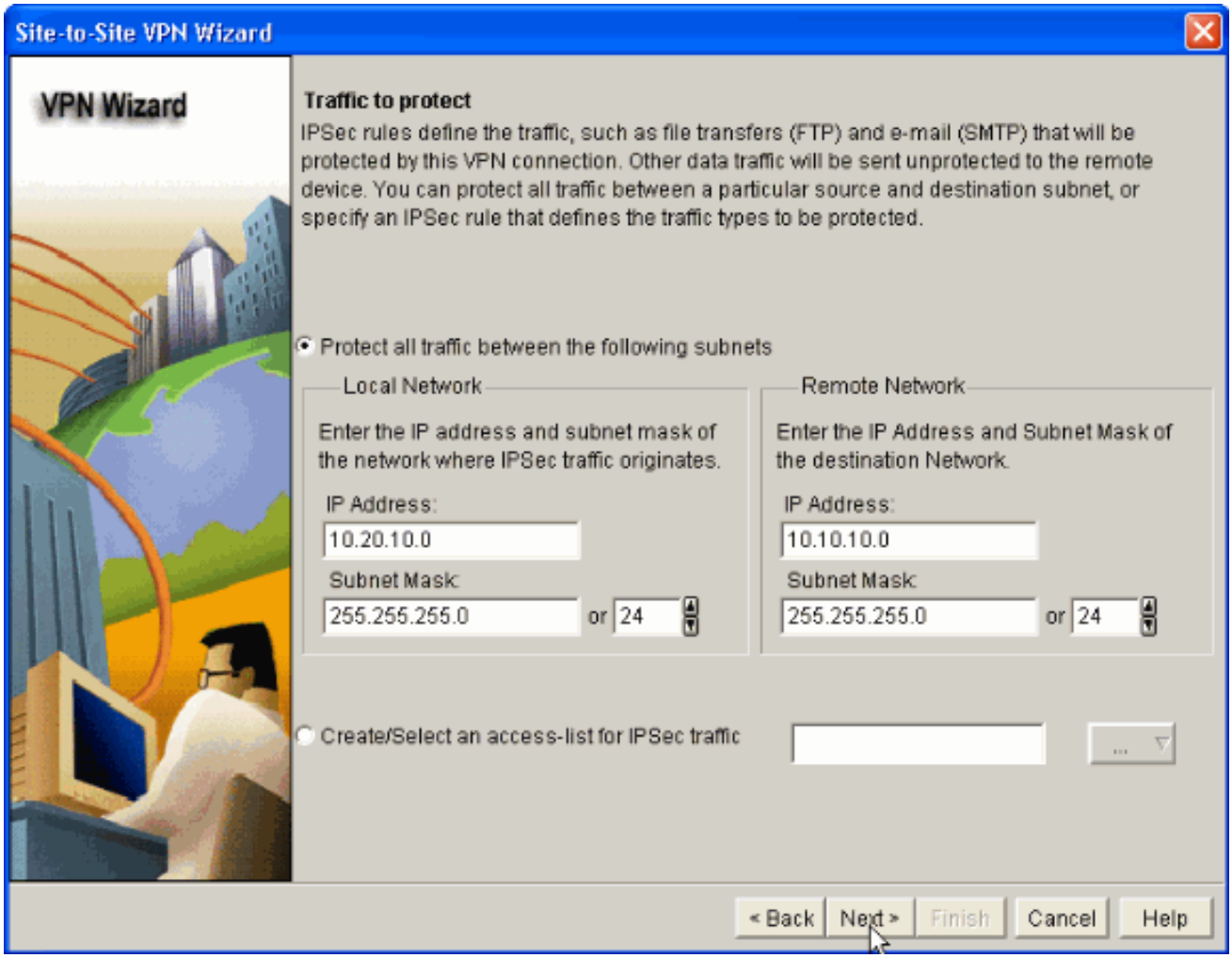
12. Kies de gewenste **transformatie die ingesteld** wordt om gebruikt te worden in de vervolgkeuzelijst zoals weergegeven.



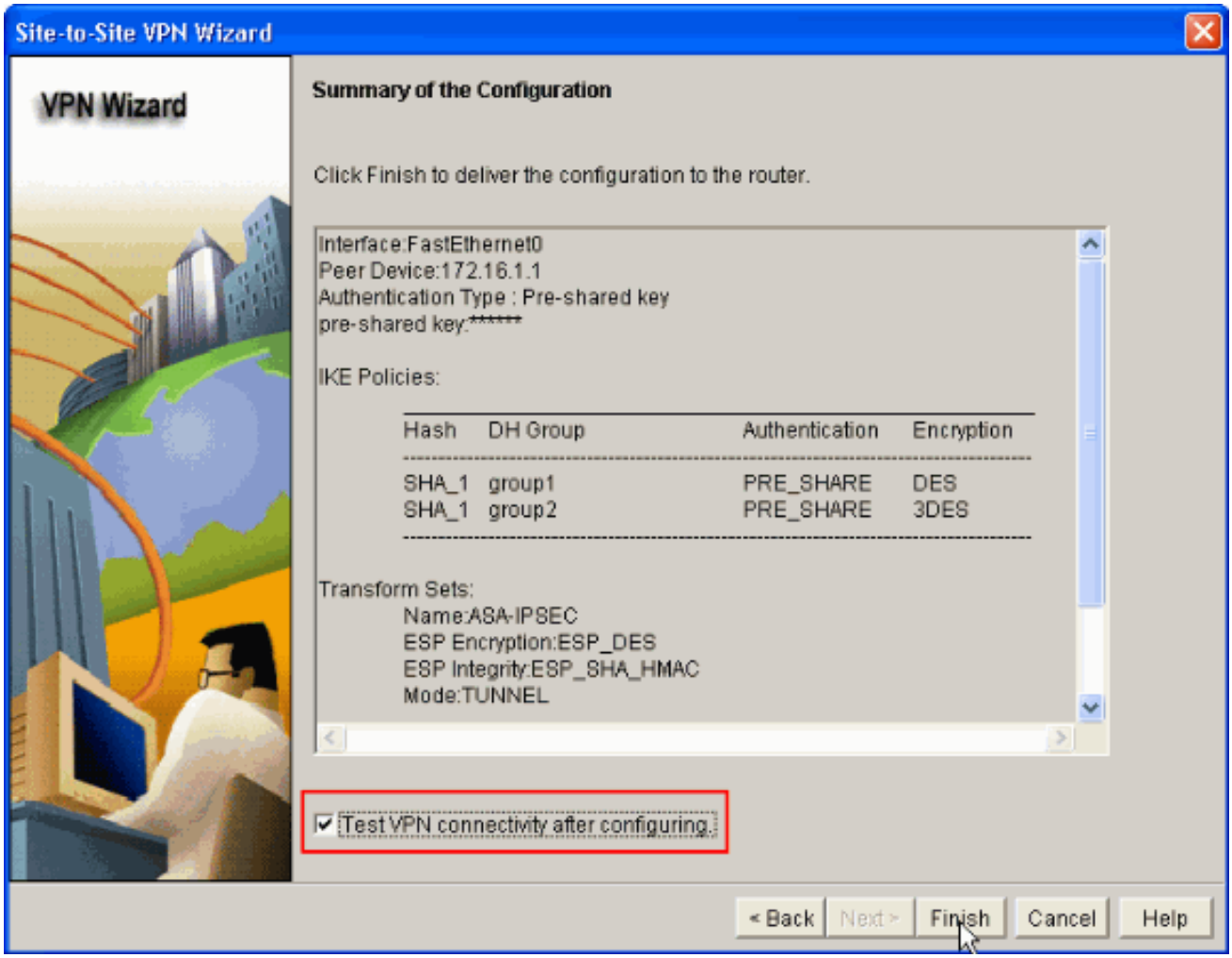
13. Klik op **Volgende**.



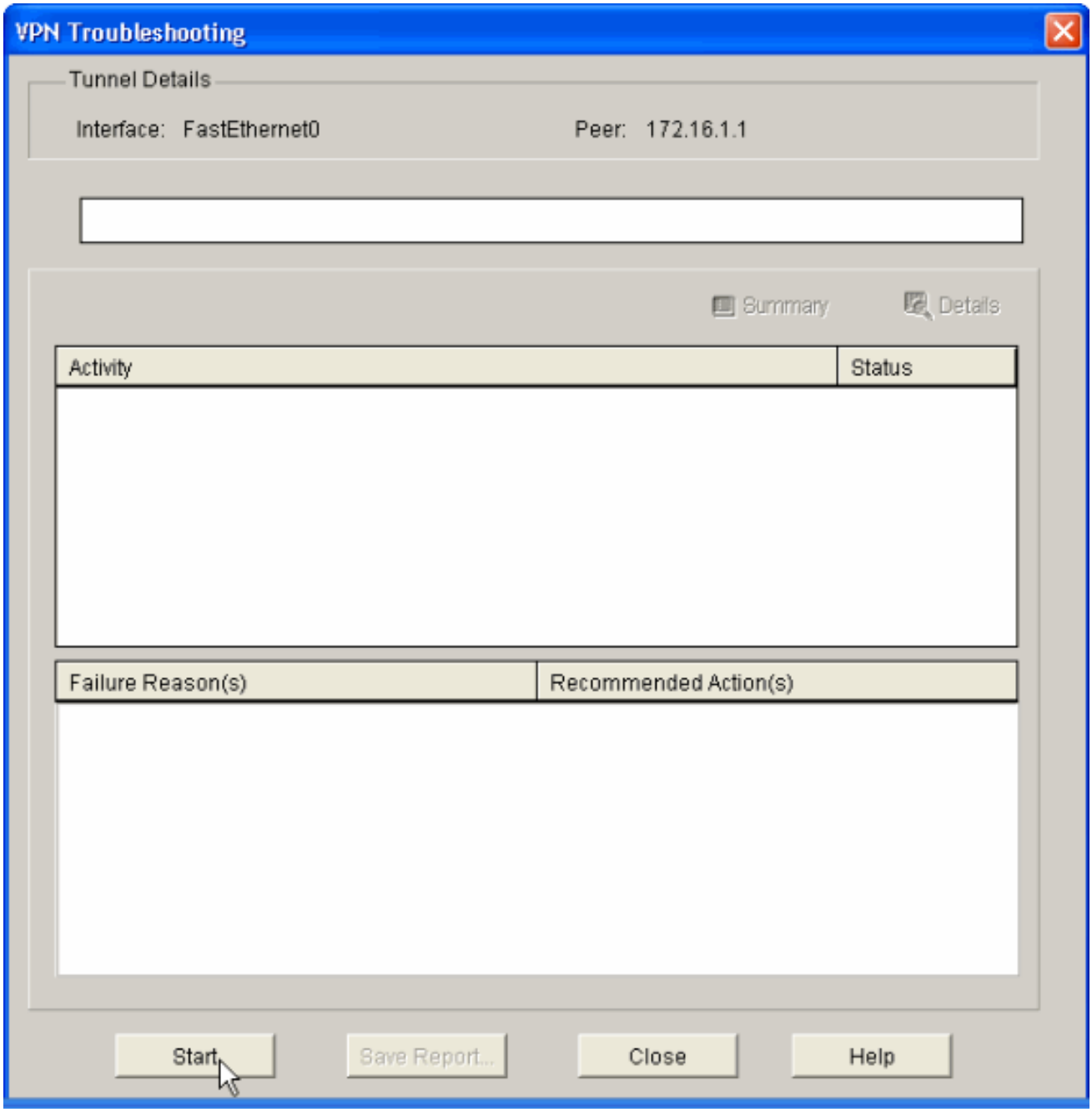
14. Typ in het volgende venster de informatie over het **verkeer dat** door de VPN-tunnelleiding **beschermd moet worden**. Verstrek de **bron- en doelnetwerken** van het te beschermen verkeer zodat het verkeer tussen de gespecificeerde bron- en doelnetwerken wordt beschermd. In dit voorbeeld is het Bron-netwerk 10.20.10.0 en het Bestemingsnetwerk is 10.10.10.0. Klik vervolgens op **Volgende**.



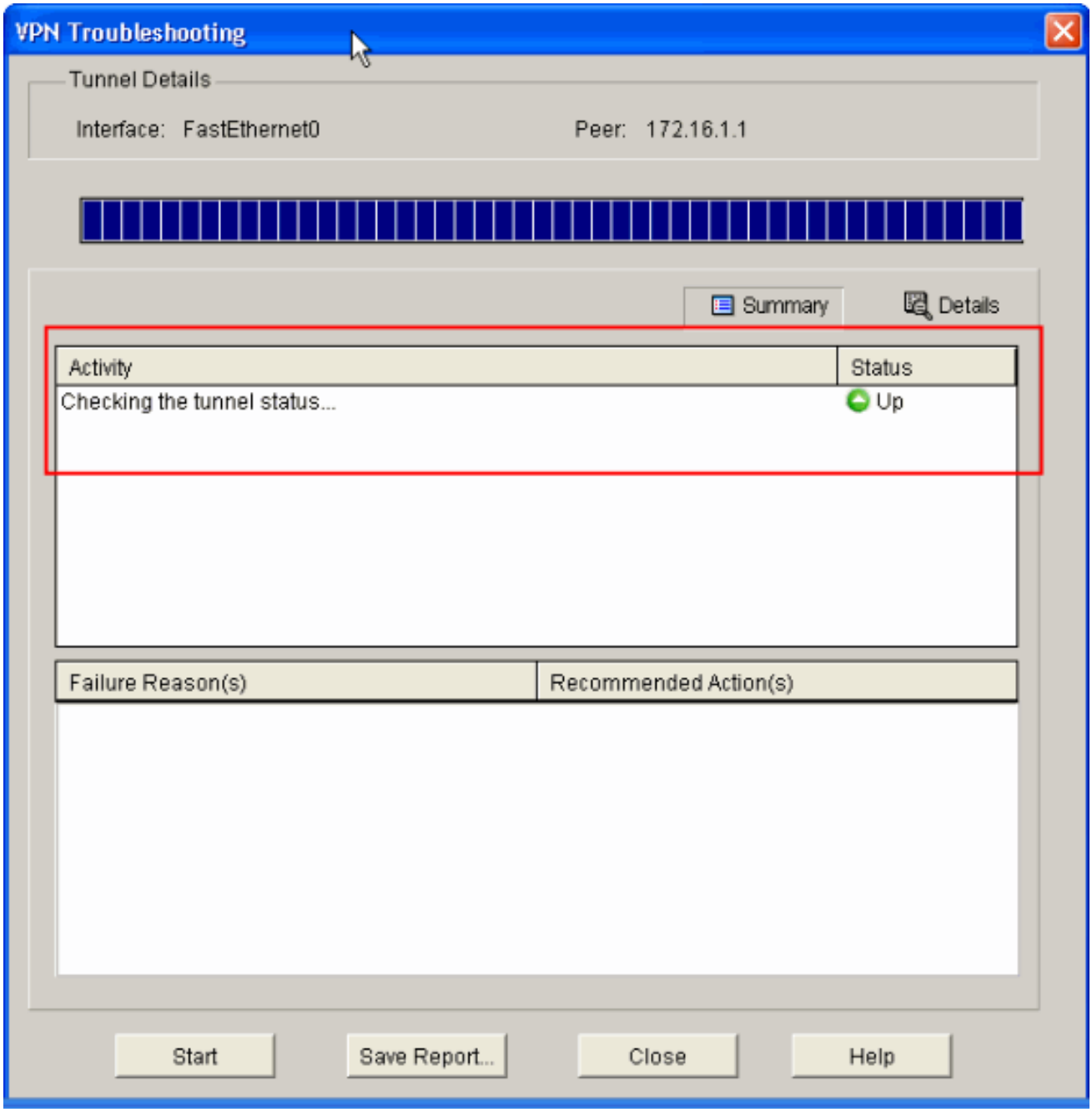
15. Dit venster toont de samenvatting van de Site-to-Site VPN-configuratie uitgevoerd. Controleer de **VPN-connectiviteit testen na het configureren** van het vakje als u de VPN-connectiviteit wilt testen. Hier wordt het vakje ingeschakeld om de aansluitingen te controleren. Klik vervolgens op **Voltooien**.



16. Klik op **Start** zoals wordt getoond om de VPN-connectiviteit te controleren.



17. In het volgende venster wordt het resultaat van de **VPN connectiviteit Test** geleverd. Hier zie je of de tunnel **omhoog** of **omlaag** is. In deze voorbeeldconfiguratie, is de Tunnel **Omhoog** zoals in groen weergegeven.



Dit voltooit de configuratie op de Cisco IOS-router.

ASA CLI-configuratie

ASA

```
ASA#show run
: Saved
ASA Version 8.0(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configure the outside interface. ! interface
Ethernet0/1 nameif outside security-level 0 ip address
172.16.1.1 255.255.255.0 !--- Configure the inside
interface. ! interface Ethernet0/2 nameif inside
security-level 100 ip address 10.10.10.1 255.255.255.0
!-- Output suppressed ! passwd 2KFQnbNIdI.2KYOU
```

```
encrypted ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid access-list 100
extended permit ip any any access-list
inside_nat0_outbound extended permit ip 10.10.10.0
255.255.255.0
10.20.10.0 255.255.255.0
!--- This access list (inside_nat0_outbound) is used !--
- with the nat zero command. This prevents traffic which
!--- matches the access list from undergoing network
address translation (NAT). !--- The traffic specified by
this ACL is traffic that is to be encrypted and !---
sent across the VPN tunnel. This ACL is intentionally !-
-- the same as (outside_1_cryptomap). !--- Two separate
access lists should always be used in this
configuration.

access-list outside_1_cryptomap extended permit ip
10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0
!--- This access list (outside_cryptomap) is used !---
with the crypto map outside_map !--- to determine which
traffic should be encrypted and sent !--- across the
tunnel. !--- This ACL is intentionally the same as
(inside_nat0_outbound). !--- Two separate access lists
should always be used in this configuration.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image disk0:/asdm-613.bin
asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 10.10.10.0 255.255.255.0

nat (inside) 0 access-list inside_nat0_outbound
!--- NAT 0 prevents NAT for networks specified in !---
the ACL inside_nat0_outbound.


access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 dmz
no snmp-server location
no snmp-server contact

!--- PHASE 2 CONFIGURATION ---! !--- The encryption
types for Phase 2 are defined here. crypto ipsec
transform-set ESP-DES-SHA esp-des esp-sha-hmac
!--- Define the transform set for Phase 2. crypto map
outside_map 1 match address outside_1_cryptomap
!--- Define which traffic should be sent to the IPsec
peer. crypto map outside_map 1 set peer 172.17.1.1
!--- Sets the IPsec peer crypto map outside_map 1 set
```

```
transform-set ESP-DES-SHA
!--- Sets the IPsec transform set "ESP-AES-256-SHA" !---
to be used with the crypto map entry "outside_map".
crypto map outside_map interface outside
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. !--- PHASE 1
CONFIGURATION ---! !--- This configuration uses isakmp
policy 10. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. crypto
isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 1
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!



tunnel-group 172.17.1.1 type ipsec-l2l
!--- In order to create and manage the database of
connection-specific !--- records for ipsec-l2l-IPsec
(LAN-to-LAN) tunnels, use the command !--- tunnel-group
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer.



tunnel-group 172.17.1.1 ipsec-attributes
 pre-shared-key *
!--- Enter the pre-shared-key in order to configure the
!--- authentication method. telnet timeout 5 ssh timeout
5 console timeout 0 threat-detection basic-threat
threat-detection statistics access-list ! class-map
inspection_default match default-inspection-traffic ! !
!-- Output suppressed! username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end
```

Configuratie van router CLI

router

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
```

```
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden as the default values are chosen.
crypto isakmp policy 2
 authentication pre-share

!--- Specifies the pre-shared key "cisco123" which
should !--- be identical at both peers. This is a global
!--- configuration mode command. crypto isakmp key
cisco123 address 172.16.1.1
!
!
!--- Configuration for IPsec policies. !--- Enables the
crypto transform configuration mode, !--- where you can
specify the transform sets that are used !--- during an
IPsec negotiation. crypto ipsec transform-set ASA-IPSEC
esp-des esp-sha-hmac
!

!--- !--- Indicates that IKE is used to establish !---
the IPsec Security Association for protecting the !---
traffic specified by this crypto map entry. crypto map
SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to172.16.1.1

!--- !--- Sets the IP address of the remote end. set
peer 172.16.1.1

!--- !--- Configures IPsec to use the transform-set !---
"ASA-IPSEC" defined earlier in this configuration. set
transform-set ASA-IPSEC

!--- !--- Specifies the interesting traffic to be
encrypted. match address 100
!
!
!
!--- Configures the interface to use the !--- crypto map
"SDM_CMAP_1" for IPsec. interface FastEthernet0 ip
address 172.17.1.1 255.255.255.0 duplex auto speed auto
crypto map SDM_CMAP_1
!
interface FastEthernet1
 ip address 10.20.10.2 255.255.255.0
```

```
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!
interface Vlan1
 ip address 10.77.241.109 255.255.255.192
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
!
!
ip nat inside source route-map nonat interface
FastEthernet0 overload
!
ip http server
ip http authentication local
ip http secure-server
!
!--- Configure the access-lists and map them to the
Crypto map configured. access-list 100 remark SDM_ACL
Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
!
!
!
!--- This ACL 110 identifies the traffic flows using
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
!
control-plane
!
!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
!
end
```

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.

- PIX security applicatie - **toon** opdrachten
- Remote IOS-router - **toont** opdrachten

ASA/PIX security applicatie - show Opdrachten

- **toon crypto isakmp sa**-toont alle huidige IKE SAs bij een peer.

```
ASA#show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.17.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

- **toon crypto ipsec sa**-Toont alle huidige IPsec SAs bij een peer.

```
ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
      current_peer: 172.17.1.1

     #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 434C4A7F

    inbound esp sas:
      spi: 0xB7C1948E (3082917006)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x434C4A7F (1129073279)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
```

Remote IOS-router - toont opdrachten

- **toon crypto isakmp sa**-toont alle huidige IKE SAs bij een peer.

```
Router#show crypto isakmp sa

dst             src             state          conn-id slot status
172.17.1.1      172.16.1.1      QM_IDLE              3    0 ACTIVE
```

- **toon crypto ipsec sa**-Toont alle huidige IPsec SAs bij een peer.

```
Router#show crypto ipsec sa
interface: FastEthernet0
    Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
  #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
    #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)

     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3004)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB7C1948E(3082917006)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3002)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

- **tonen de crypto motor verbindingen actief**-toont huidige verbindingen en informatie over gecodeerde en gedecrypteerde pakketten (slechts router).

```
Router#show crypto engine connections active

  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
   3 FastEthernet0        172.17.1.1      set    HMAC_SHA+DES_56_CB        0        0
2001 FastEthernet0        172.17.1.1      set    DES+SHA                   0       59
2002 FastEthernet0        172.17.1.1      set    DES+SHA                  59        0
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

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 en IP security probleemoplossing - Bezig met begrijpen en gebruiken debug Commands voordat u **debug-** opdrachten gebruikt.

- **debug crypto ipsec 7**-displays de IPsec onderhandelingen van fase 2.**debug crypto isakmp 7** — Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.
- **debug crypto ipsec**-displays de IPsec onderhandelingen van fase 2.**debug crypto isakmp** — Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.

Raadpleeg de meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing voor probleemoplossing bij site-site VPN.

Gerelateerde informatie

- Cisco PIX-firewallsoftware
- Cisco adaptieve security apparaatbeheer
- Cisco ASA 5500 Series adaptieve security applicaties
- Configuration Professional: Site-to-Site IPsec VPN tussen ASA/PIX en een IOS routerconfiguratie voorbeeld
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Cisco-router- en beveiligingsapparaatbeheer
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems