ASA/PIX: Remote VPN-server met Ininkomend NAT voor VPN-clientverkeer met CLI en ASDM-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco 5500 Series adaptieve security applicatie (ASA) kunt configureren om op te treden als een externe VPN-server met behulp van Adaptieve Security Devices Manager (ASDM) of CLI en NAT in het inkomende VPN-clientverkeer. De ASDM levert veiligheidsbeheer en controle van wereldklasse door middel van een intuïtieve, makkelijk te gebruiken web-gebaseerde beheerinterface. Nadat de Cisco ASA-configuratie is voltooid, kan deze via de Cisco VPN-client worden geverifieerd.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de ASA volledig operationeel en geconfigureerd is om Cisco ASDM of CLI in staat te stellen configuratiewijzigingen door te voeren. De ASA wordt ook verondersteld te zijn geconfigureerd voor uitgaande NAT. Raadpleeg Inside Hosts Toegang tot Outside Networks met het gebruik van PAT voor meer informatie over het configureren van uitgaande NAT.

Opmerking: Raadpleeg HTTPS-toegang voor ASDM of PIX/ASA 7.x: SSH in het Voorbeeld van de configuratie van binnen en buiten om het apparaat extern te kunnen configureren door de ASDM of Secure Shell (SSH).

Gebruikte componenten

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

- Cisco adaptieve security applicatie, versie 7.x en hoger
- Adaptieve Security Adapter Manager versie 5.x en hoger
- Cisco VPN-clientversie 4.x 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.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco PIX security applicatie versie 7.x en hoger.

Conventies

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

Achtergrondinformatie

Remote-toegangsconfiguraties bieden beveiligde externe toegang voor Cisco VPN-clients, zoals mobiele gebruikers. Een VPN-toegang op afstand stelt externe gebruikers in staat om veilig toegang te krijgen tot gecentraliseerde netwerkbronnen. De Cisco VPN-client voldoet aan het IPSec-protocol en is specifiek ontworpen om met het security apparaat te werken. Het security apparaat kan echter wel IPSec-verbindingen maken met veel klanten die aan het protocol voldoen. Raadpleeg de ASA Configuration Guides voor meer informatie over IPSec.

Groepen en gebruikers zijn kernconcepten in het beheer van de beveiliging van VPN's en in de configuratie van het security apparaat. Ze specificeren eigenschappen die de toegang van gebruikers tot en het gebruik van VPN bepalen. Een groep is een verzameling gebruikers die als één entiteit worden behandeld. Gebruikers krijgen hun eigenschappen van groepsbeleid. Tunnelgroepen identificeren het groepsbeleid voor specifieke verbindingen. Als u geen bepaald groepsbeleid aan gebruikers toewijst, is het standaard groepsbeleid voor de verbinding van toepassing.

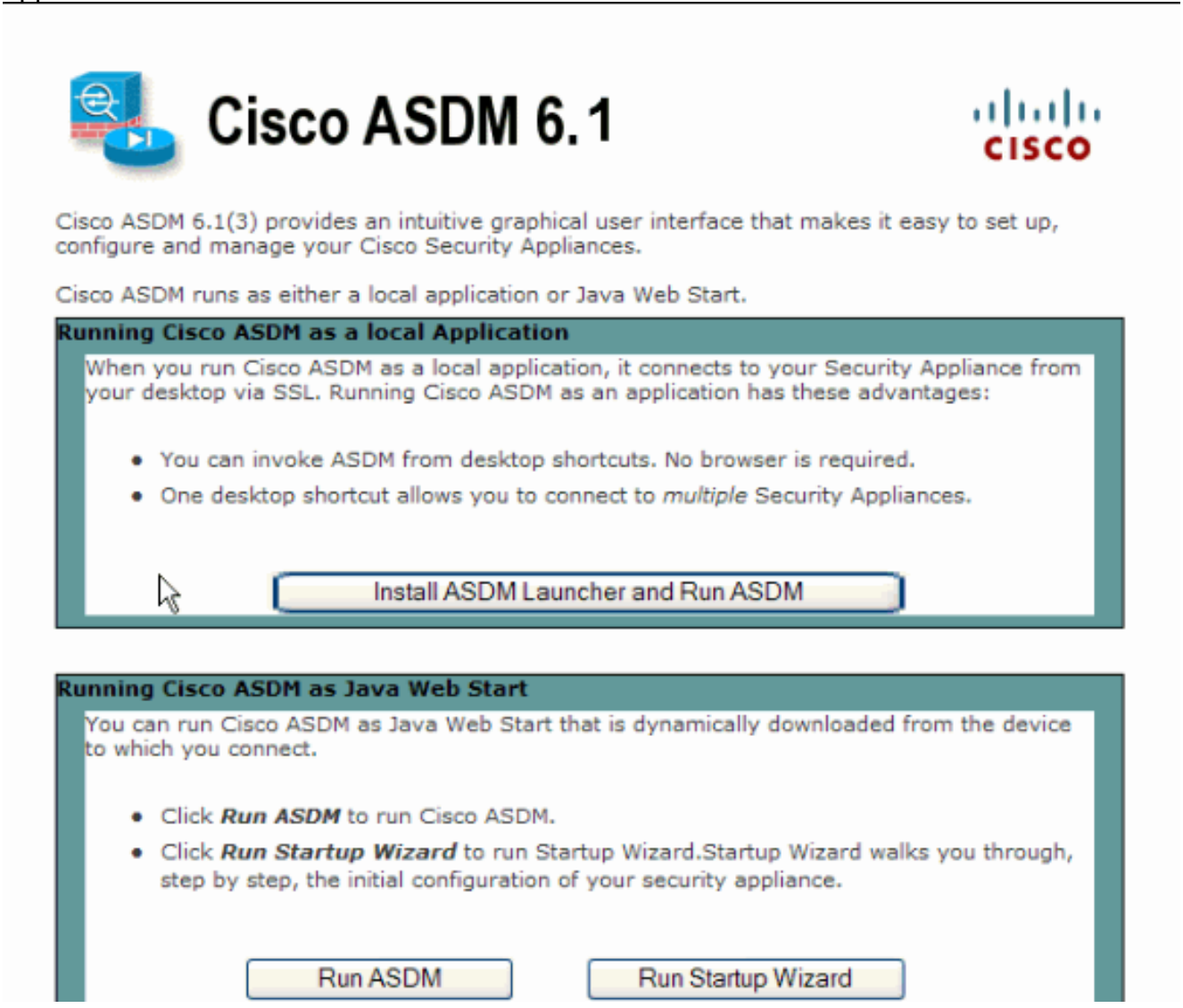
Een tunnelgroep bestaat uit een reeks records die tunnelverbindingsbeleid bepalen. In deze registers worden de servers geïdentificeerd waarop de tunnelgebruikers zijn geauthentiseerd, evenals de eventuele boekhoudkundige servers waarop de verbindingsinformatie wordt verzonden. Ze identificeren ook een standaardgroepsbeleid voor de verbindingen, en ze bevatten protocol-specifieke verbindingsparameters. Tunnelgroepen omvatten een klein aantal eigenschappen die verband houden met de totstandbrenging van de tunnel zelf. Tunnelgroepen bevatten een muiswijzer op een groepsbeleid dat gebruikersgeoriënteerde eigenschappen definieert.

Configuraties

ASA/PIX configureren als een externe VPN-server met ASDM

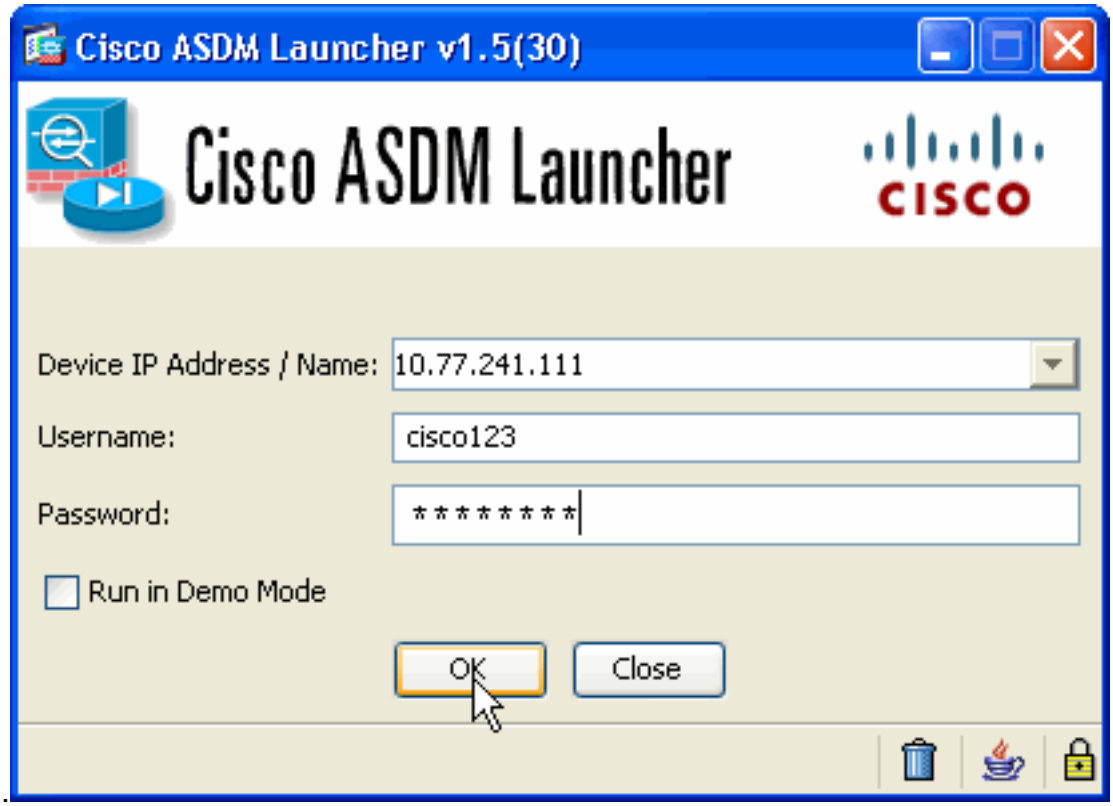
Voltooi deze stappen om Cisco ASA als een externe VPN-server met ASDM te configureren:

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.

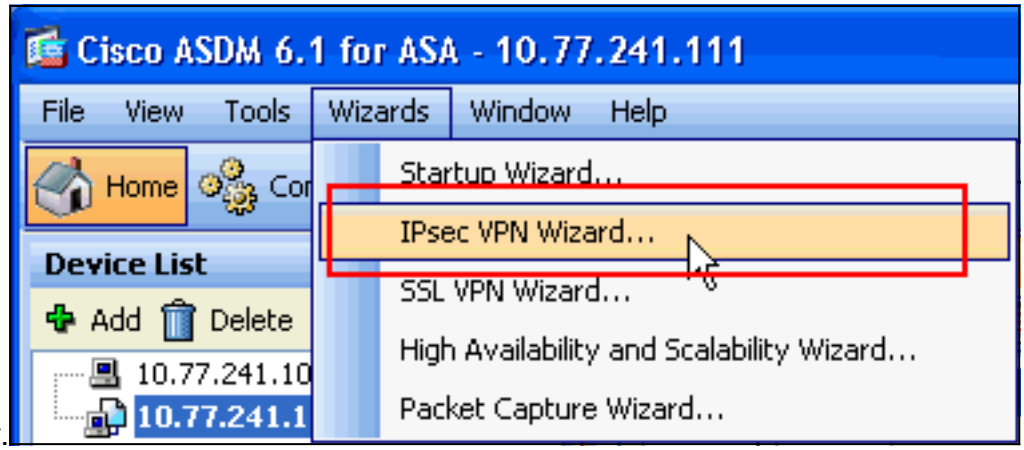


2. Klik op **Download ASDM Launcher en Start ASDM** om de installateur voor de ASDM-toepassing te downloaden.
3. Voltooi na het downloaden van de ASDM Launcher de stappen die door de aanwijzingen zijn geleid om de software te installeren en de Cisco ASDM Launcher uit te voeren.
4. Voer het IP-adres in 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** als de gebruikersnaam en **cisco123** als het

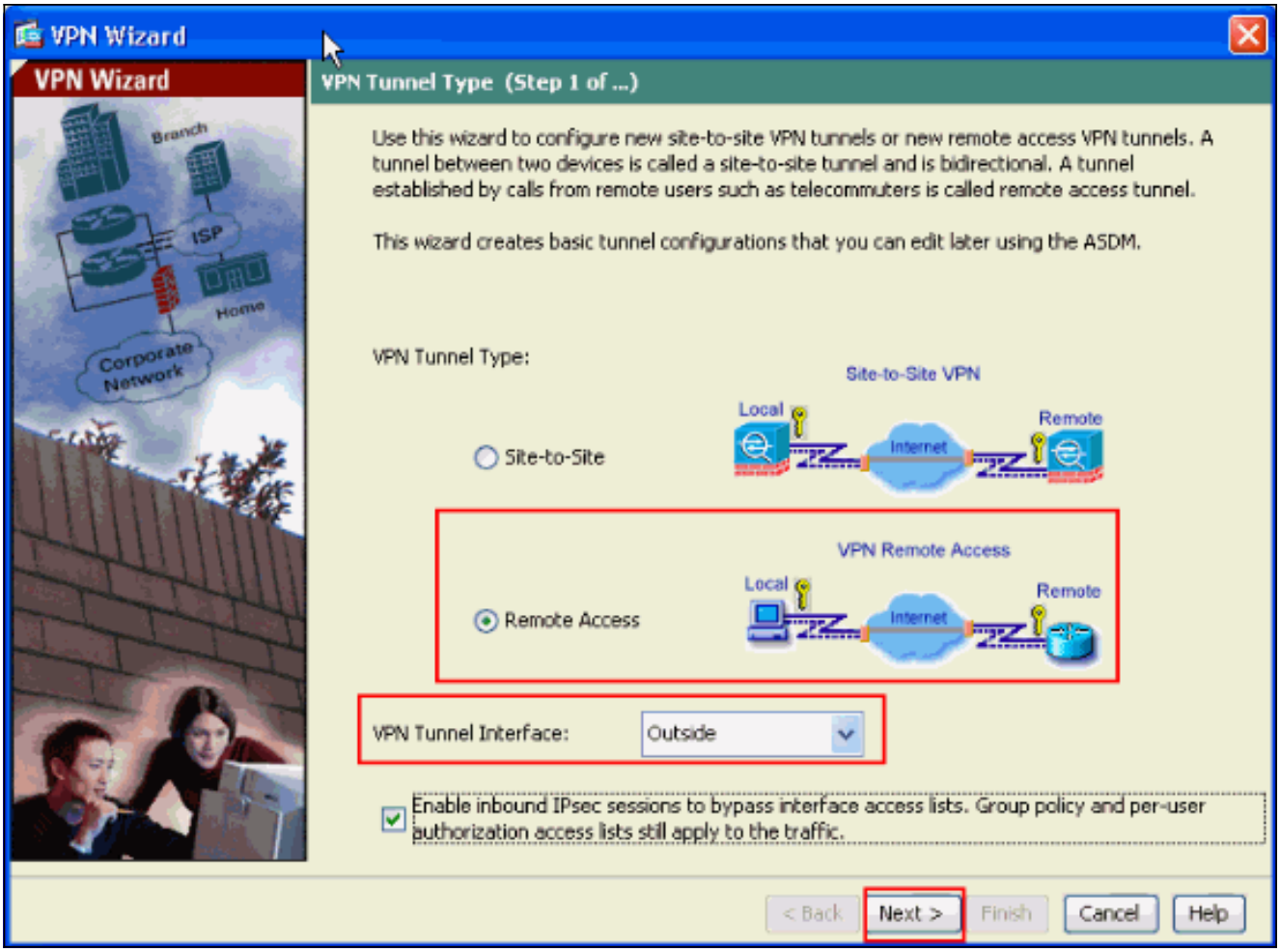
wachtwoord.



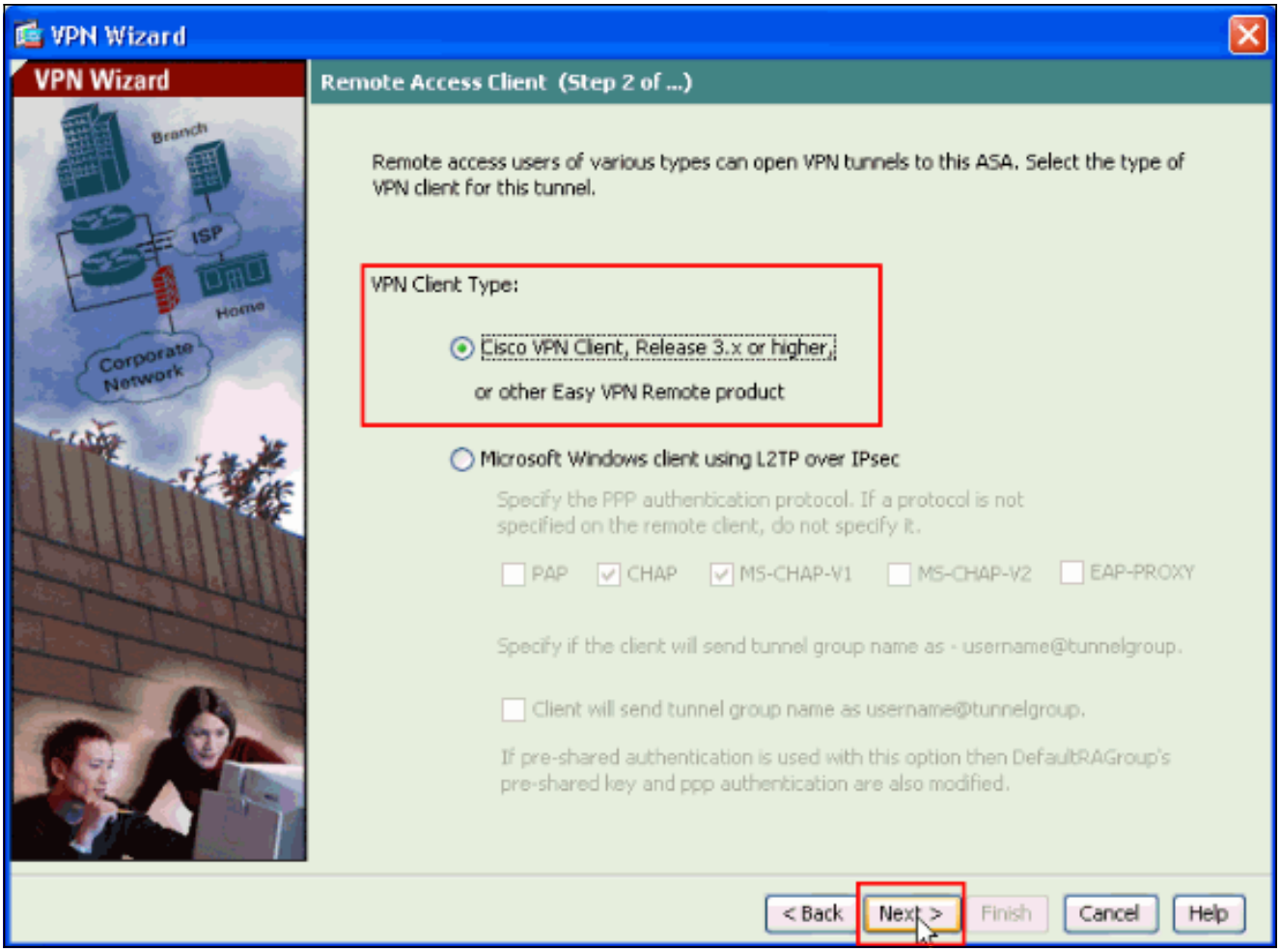
5. Selecteer **Wizard > IPsec VPN-wizard** in het Home venster.



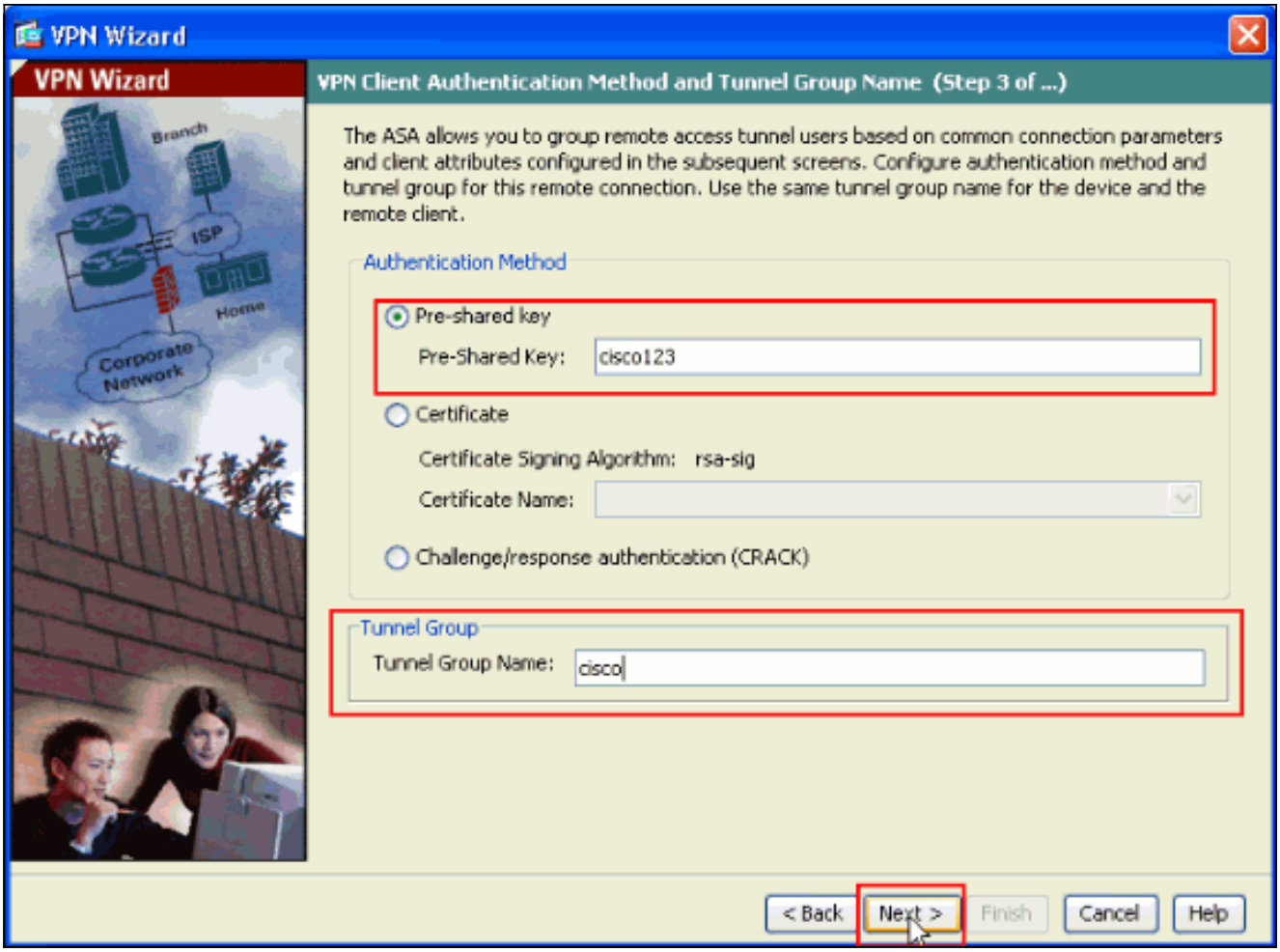
6. Selecteer het tunneltype **Remote Access** VPN en zorg ervoor dat de VPN-tunnelinterface naar wens wordt ingesteld en klik op **Volgende** zoals hier wordt weergegeven.



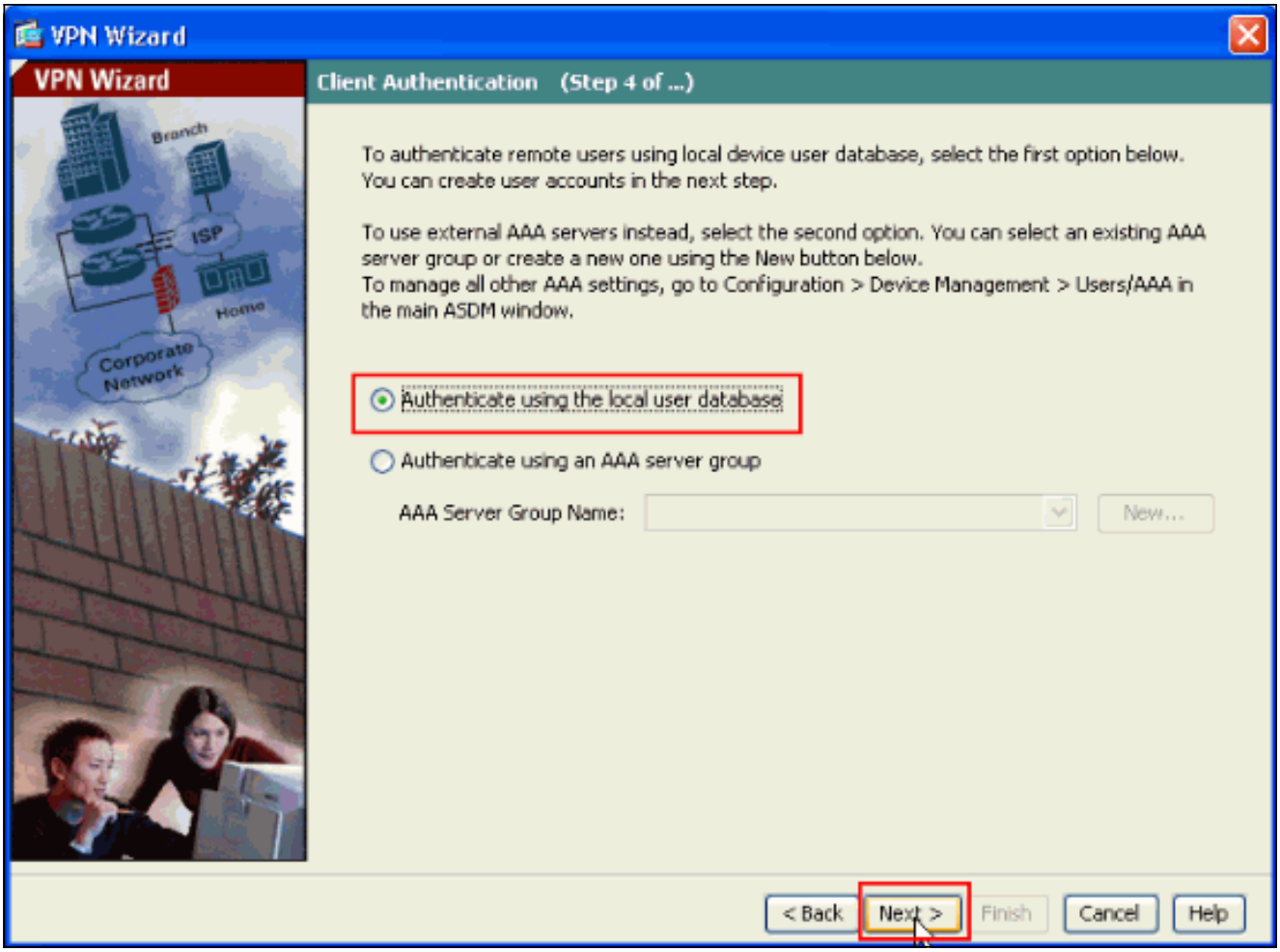
7. Het VPN-clienttype is geselecteerd, zoals wordt weergegeven. **Cisco VPN-client** is hier geselecteerd. Klik op **Volgende**.



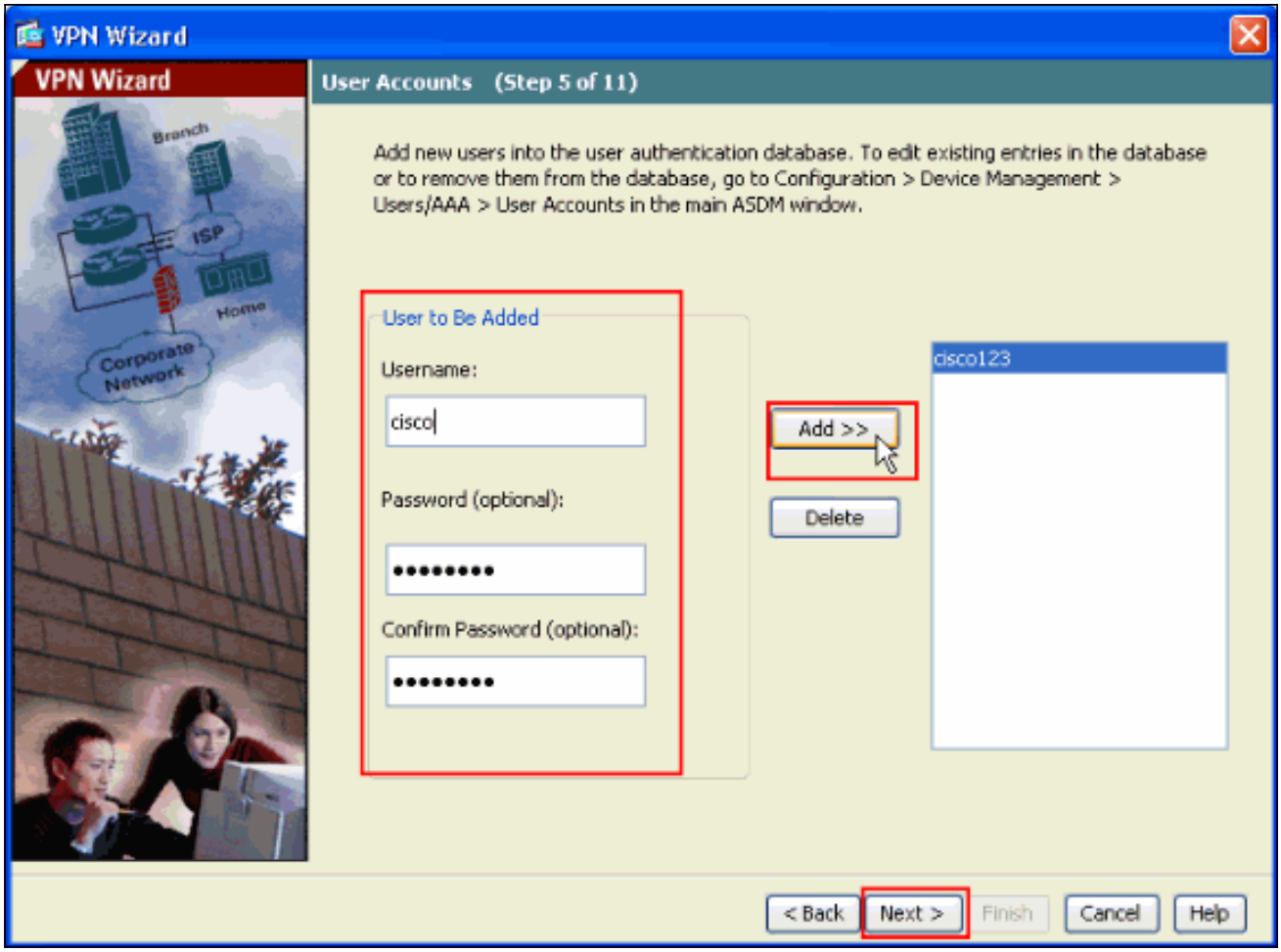
8. Voer een naam in voor de **naam** van de **tunnelgroep**. Voer de te gebruiken authenticatie-informatie in, de **vooraf gedeelde sleutel** in dit voorbeeld. De pre-gedeelde sleutel die in dit voorbeeld wordt gebruikt is **cisco123**. De naam van de Tunnelgroep die in dit voorbeeld wordt gebruikt is **cisco**. Klik op **Volgende**.



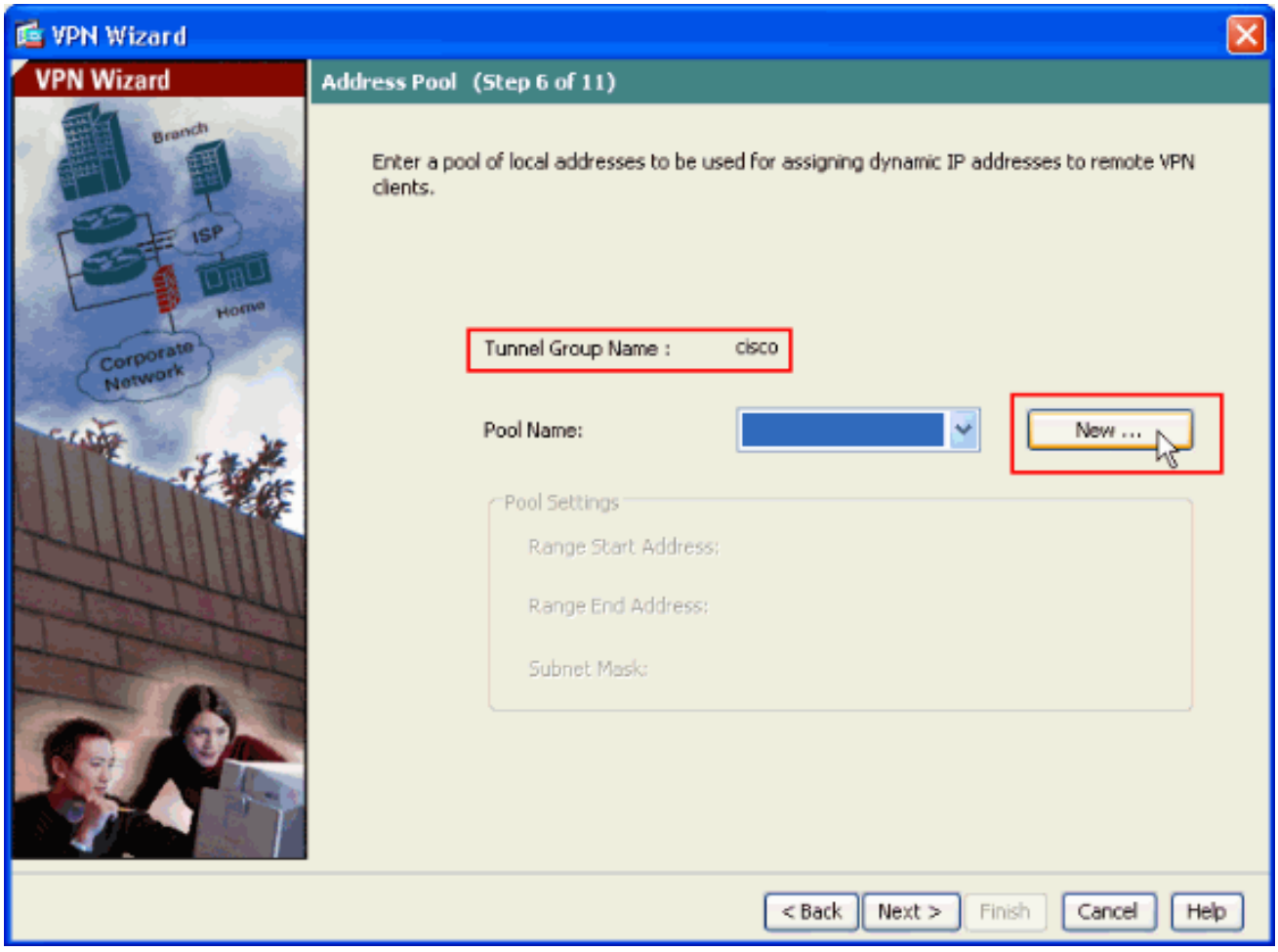
9. Kies of u externe gebruikers wilt geauthentiseerd worden naar de lokale gebruikersdatabase of naar een externe AAA server groep.**Opmerking:** U voegt gebruikers in stap 10 toe aan de lokale gebruikersdatabase.**Opmerking:** Raadpleeg PIX/ASA 7.x-groepen voor verificatie en autorisatie van VPN-gebruikers via het ASDM Configuration Voorbeeld voor informatie over de configuratie van een externe AAA-servergroep met
ASDM.



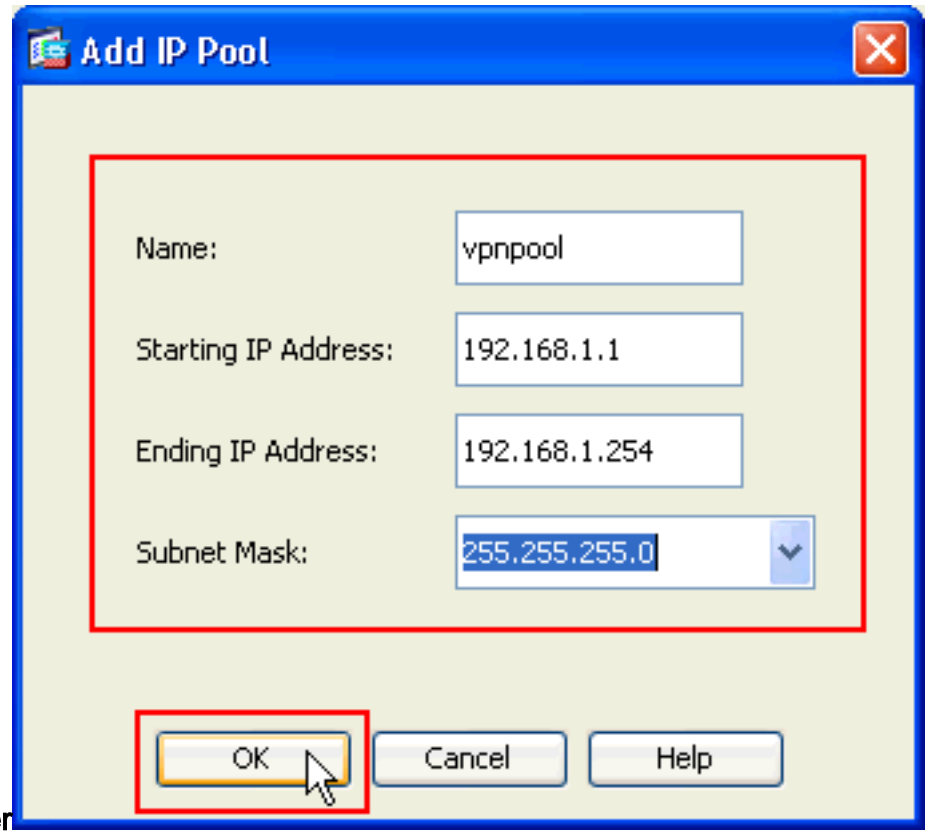
10. Geef een **gebruikersnaam** en optioneel **wachtwoord op** en klik op **Toevoegen** om nieuwe gebruikers toe te voegen aan de gebruikersverificatiedatabase. Klik op **Volgende**.**N.B.:** Verwijder bestaande gebruikers niet uit dit venster. Selecteer **Configuratie > Apparaatbeheer > Gebruikers/AAA > Gebruikersrekeningen** in het hoofdvenster van ASDM om bestaande items in de database te bewerken of deze uit de database te verwijderen.



11. Om een pool van lokale adressen te definiëren die dynamisch aan externe VPN-clients moet worden toegewezen, klikt u op **Nieuw** om een nieuwe **IP-pool** te maken.

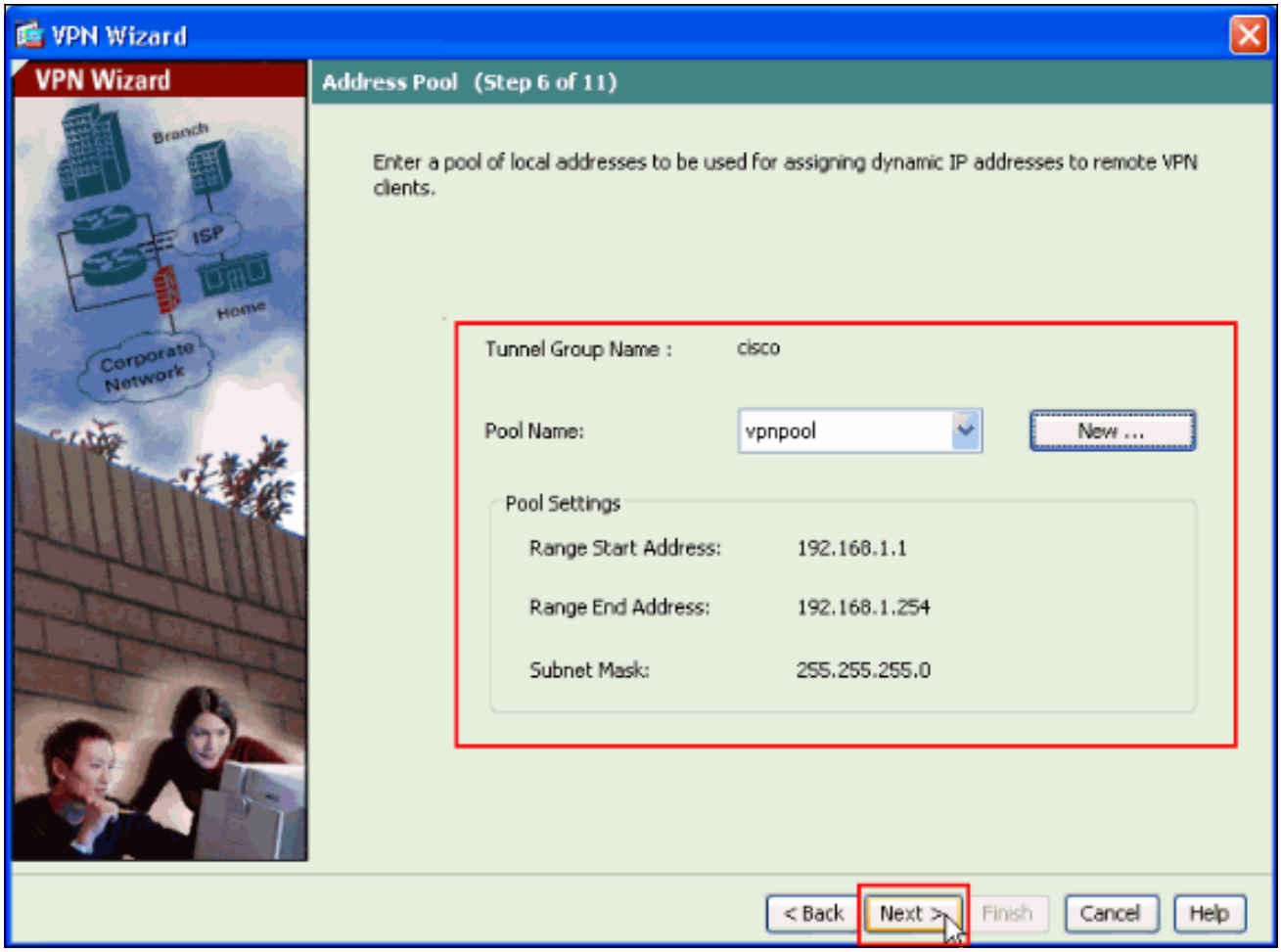


12. Typ deze informatie in het nieuwe venster **Add IP Pool** en klik op **OK**.**Naam van de IP-poolIP-adres start**en**IP-adres**

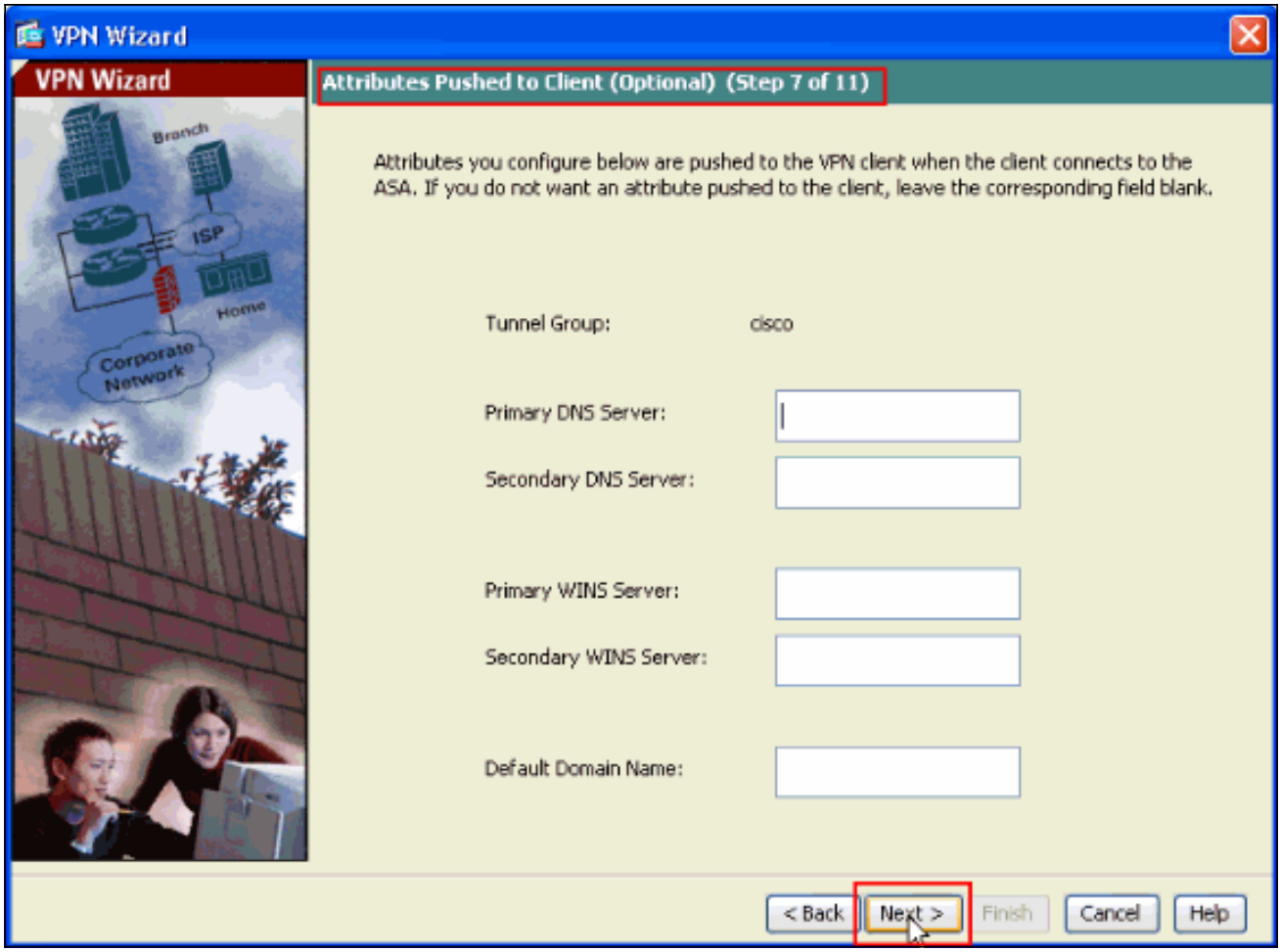


beëindigenSubnetmasker

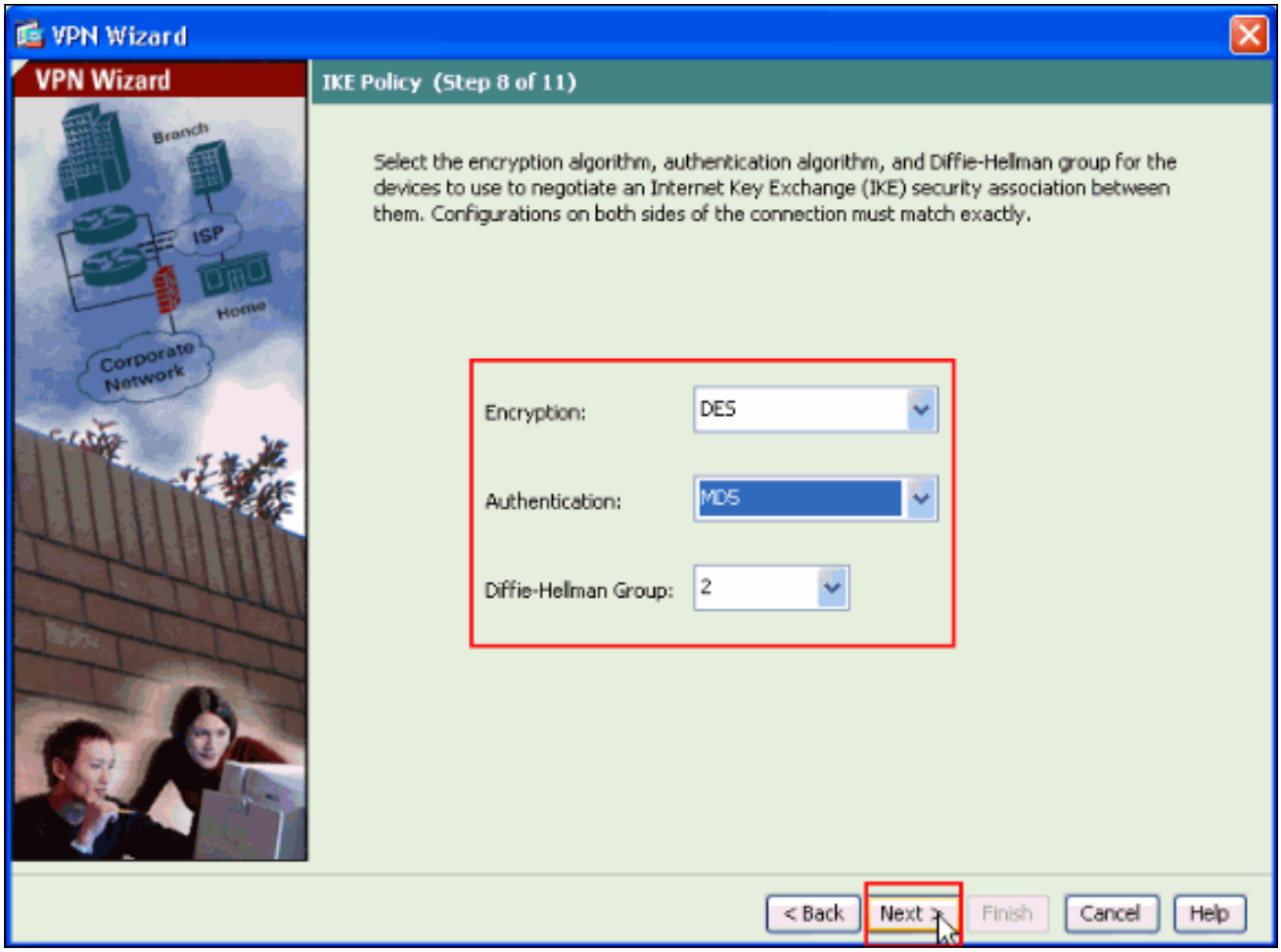
13. Nadat u de pool van lokale adressen definieert die dynamisch aan externe VPN-clients moeten worden toegewezen wanneer ze worden aangesloten, klikt u op **Volgende.**



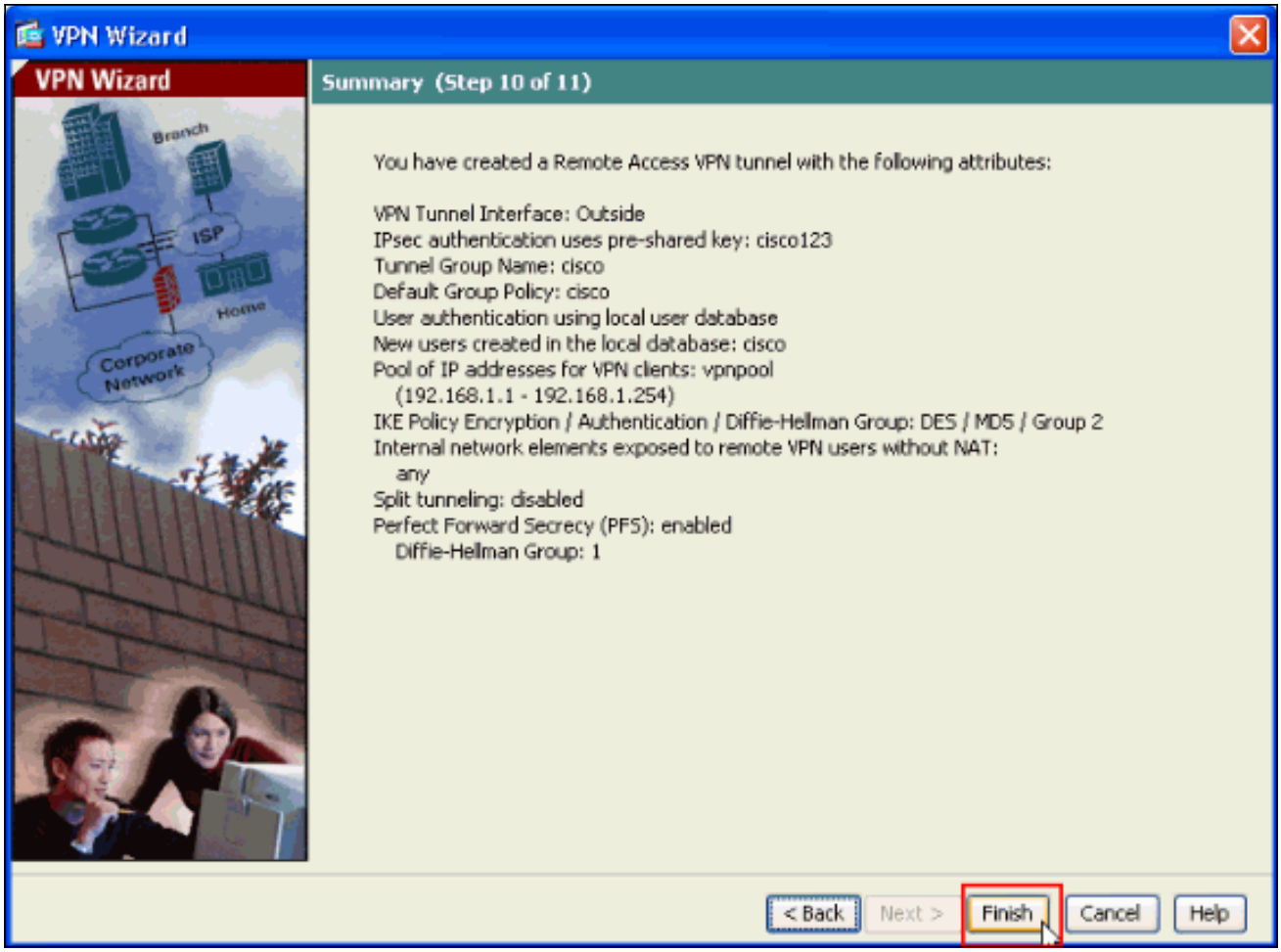
14. *Optioneel:* Specificeer de DNS- en WINS-serverinformatie en een standaardnaam voor domeinen die naar externe VPN-clients moet worden geduwd.



15. Specificeer de parameters voor IKE, ook bekend als IKE Fase 1.De configuraties aan beide zijden van de tunnel moeten precies overeenkomen. Maar de Cisco VPN-client selecteert automatisch de juiste configuratie voor zichzelf. Daarom is geen IKE-configuratie nodig op de client-
pc.



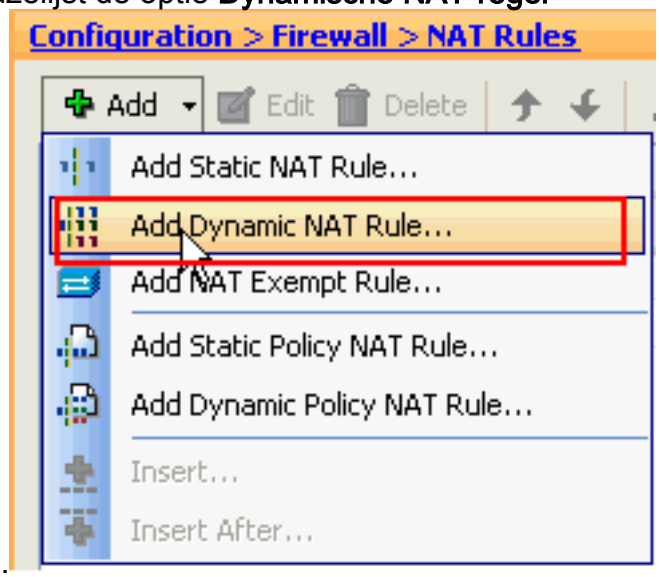
16. Dit venster geeft een samenvatting van de maatregelen die u hebt genomen. Klik op **Voltooien** als u tevreden bent met de configuratie.



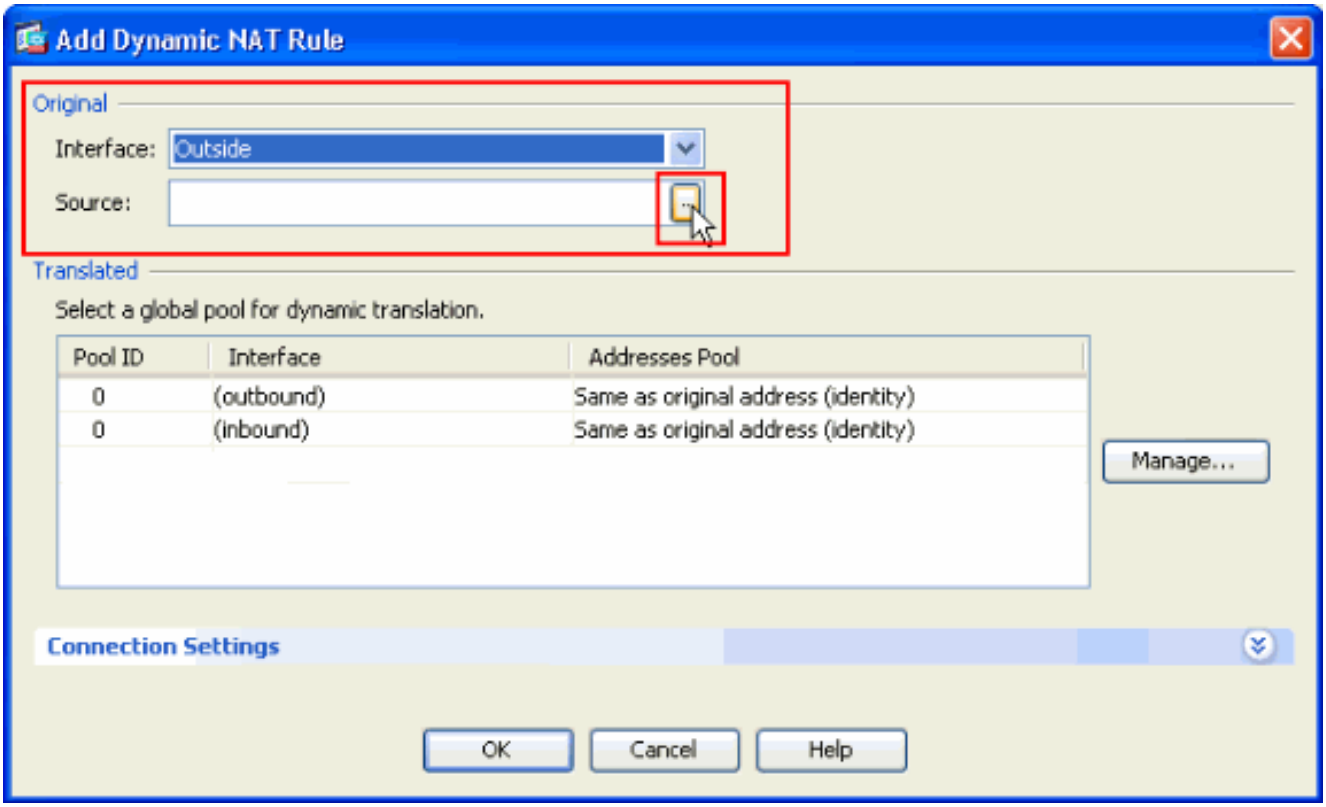
Configureer de ASA/PIX met NAT inkomend VPN-clientverkeer met ASDM

Voltooi deze stappen om Cisco ASA aan NAT inkomend VPN-clientverkeer met ASDM te configureren:

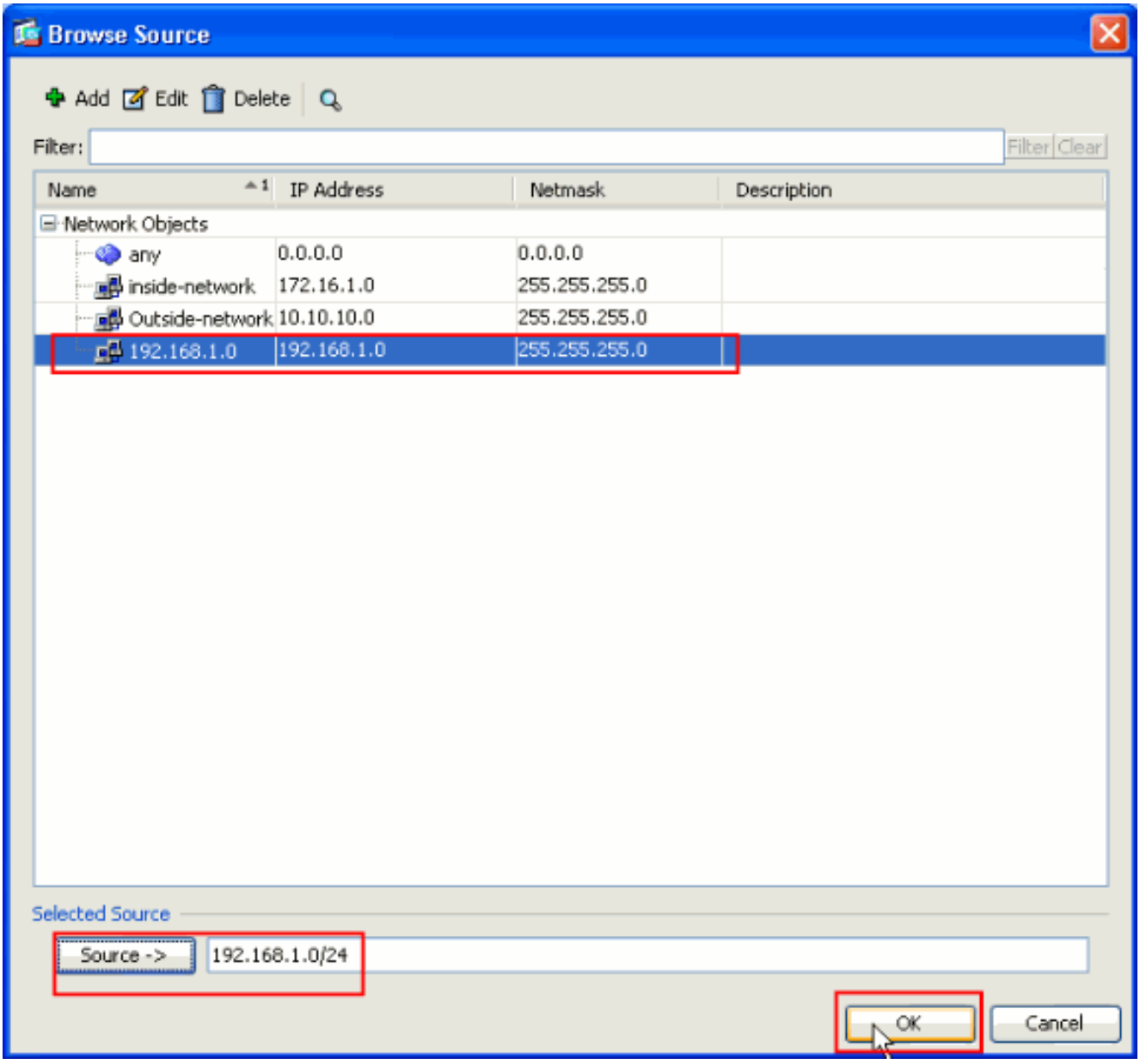
1. Kies **Configuratie > Firewall > NAT-regels** en klik op **Toevoegen**. Selecteer in de vervolgkeuzelijst de optie **Dynamische NAT-regel toevoegen**.



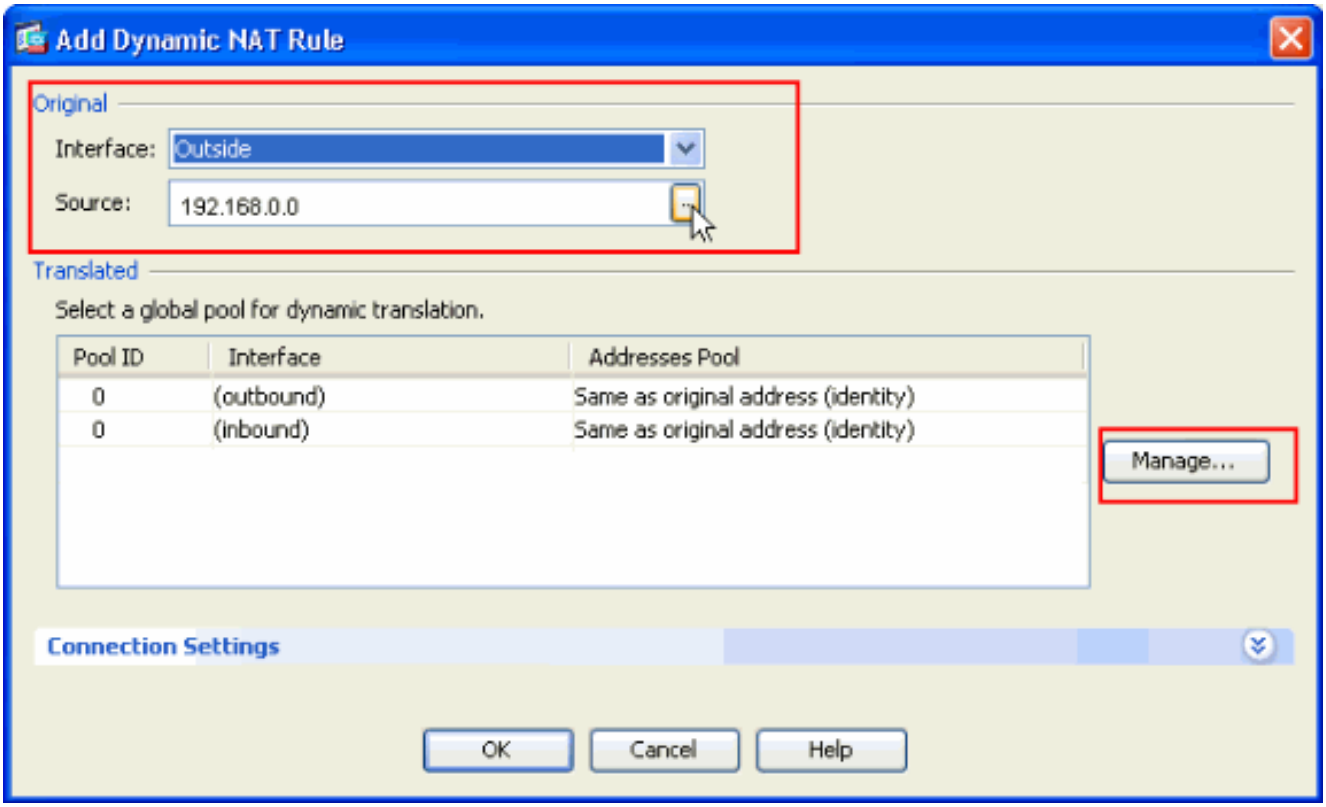
2. In het venster **Dynamische NAT-regel toevoegen**, kiest u **Buitenkant** als de interface en klikt u op de knop Bladeren naast het vak **Bron**.



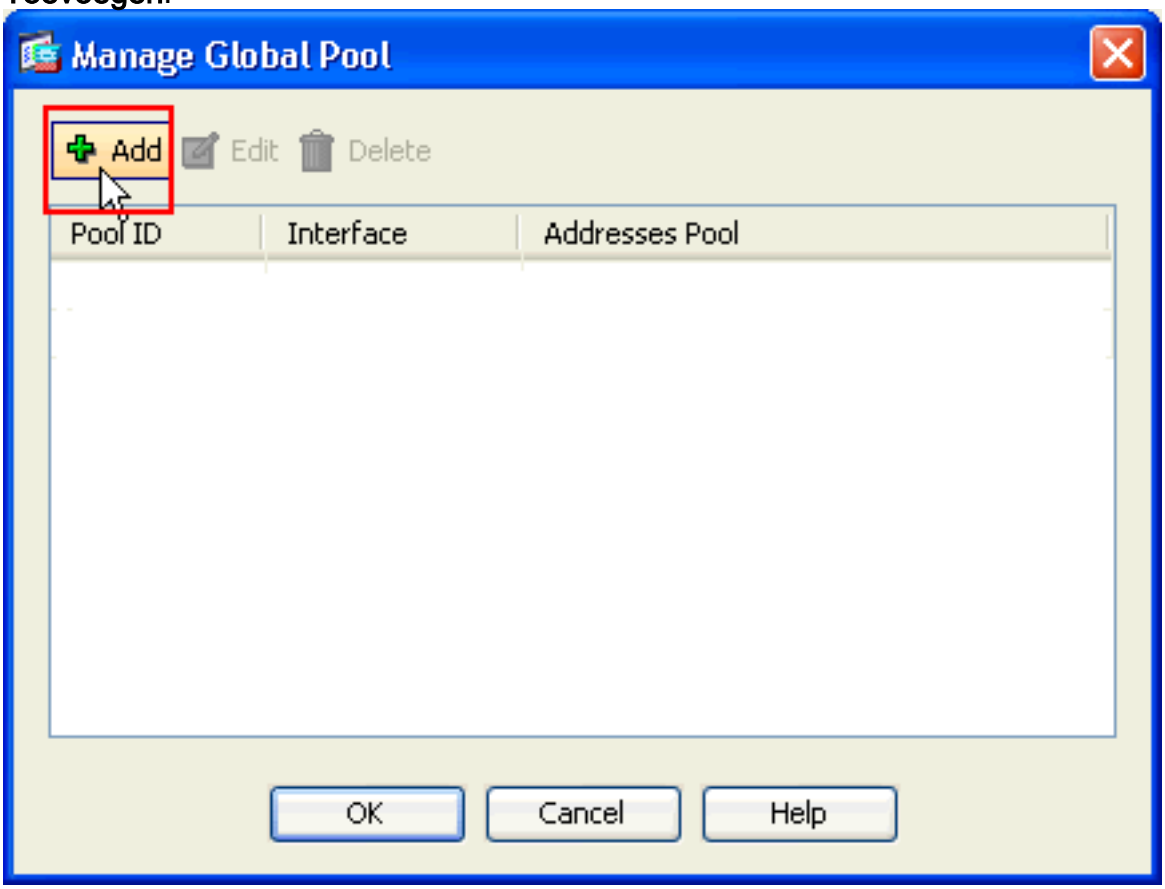
3. Selecteer in het venster Bladeren Bron de juiste netwerkobjecten en kies ook de **bron** onder de sectie Geselecteerde Bron en klik op **OK**. Hier wordt de netwerkobject 192.168.1.0 geselecteerd.



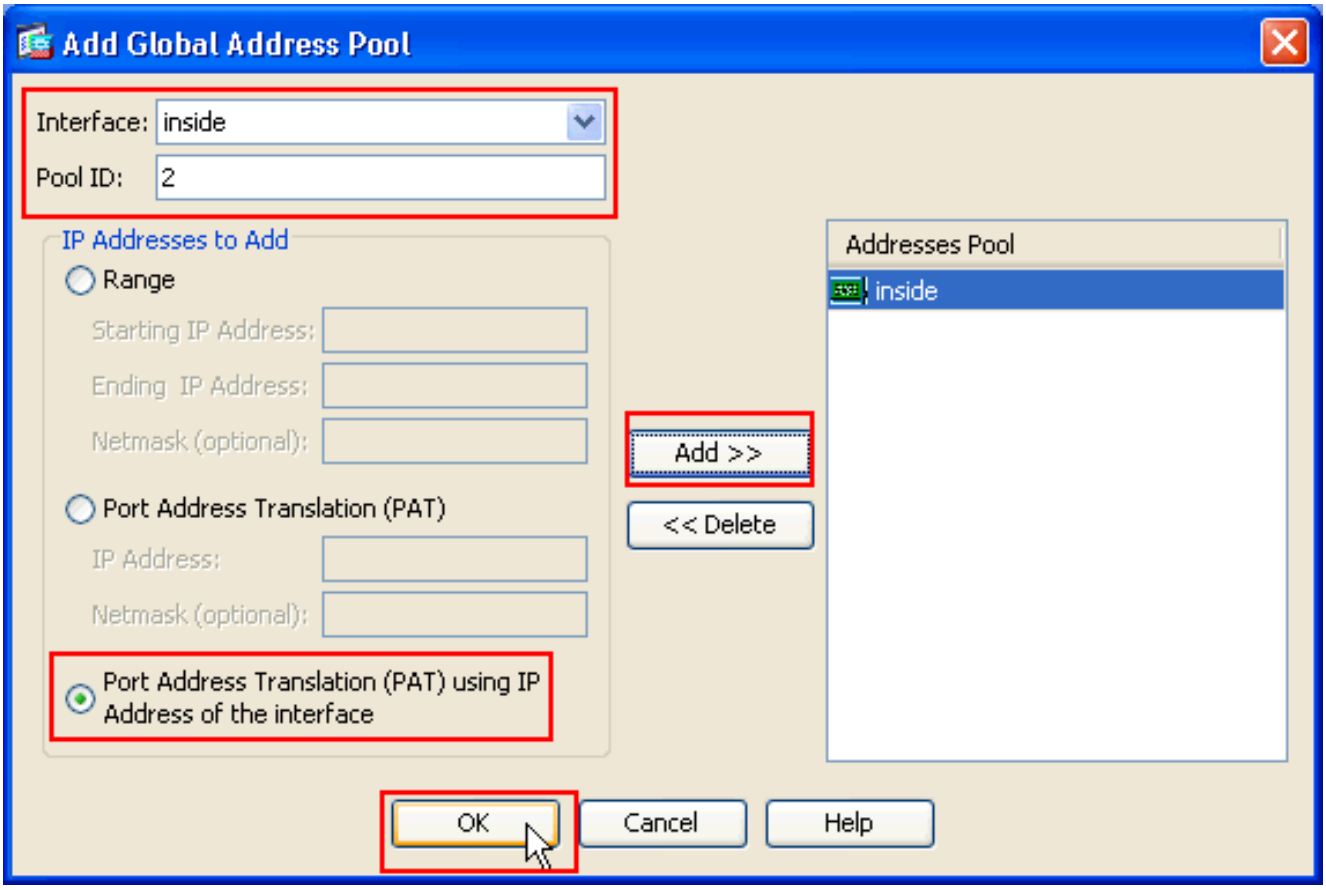
4. Klik op **beheren**.



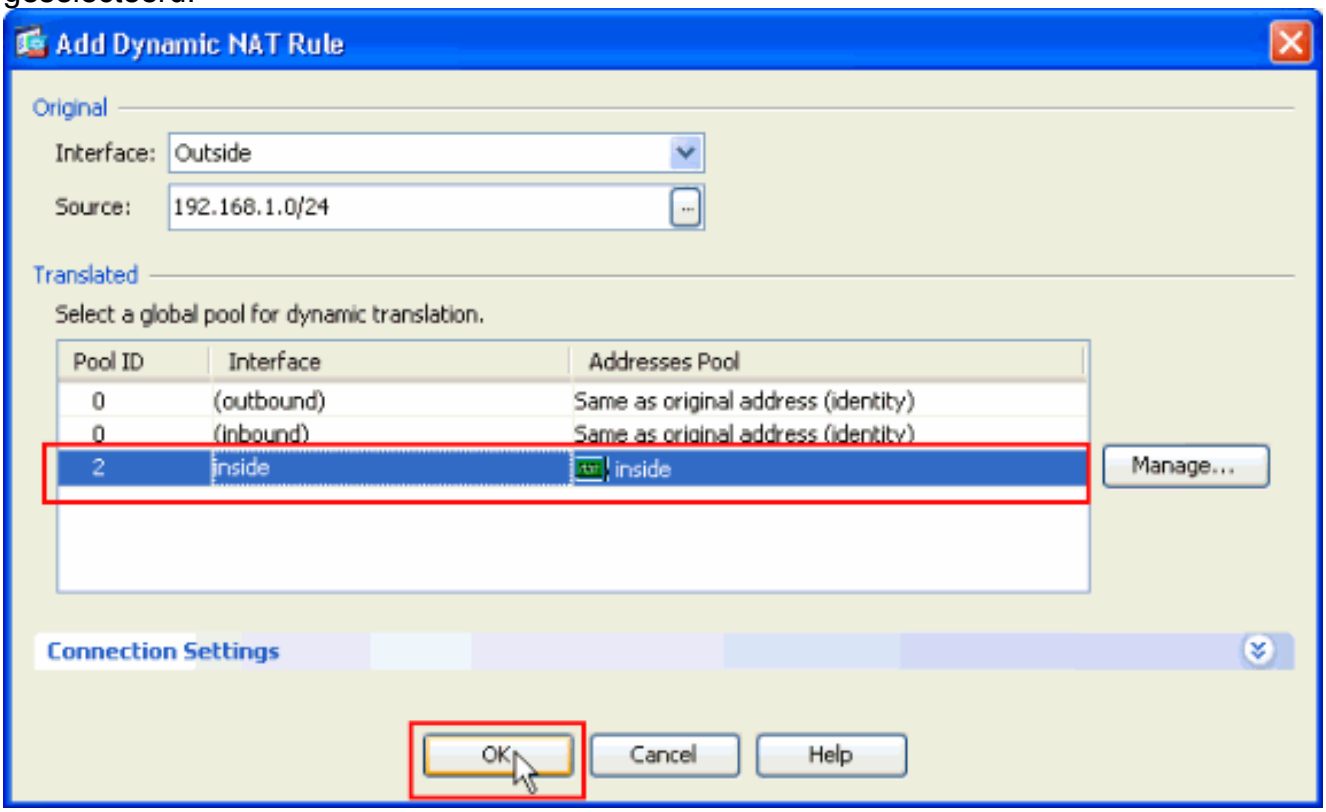
5. Klik in het venster Global Pool beheren op **Toevoegen**.



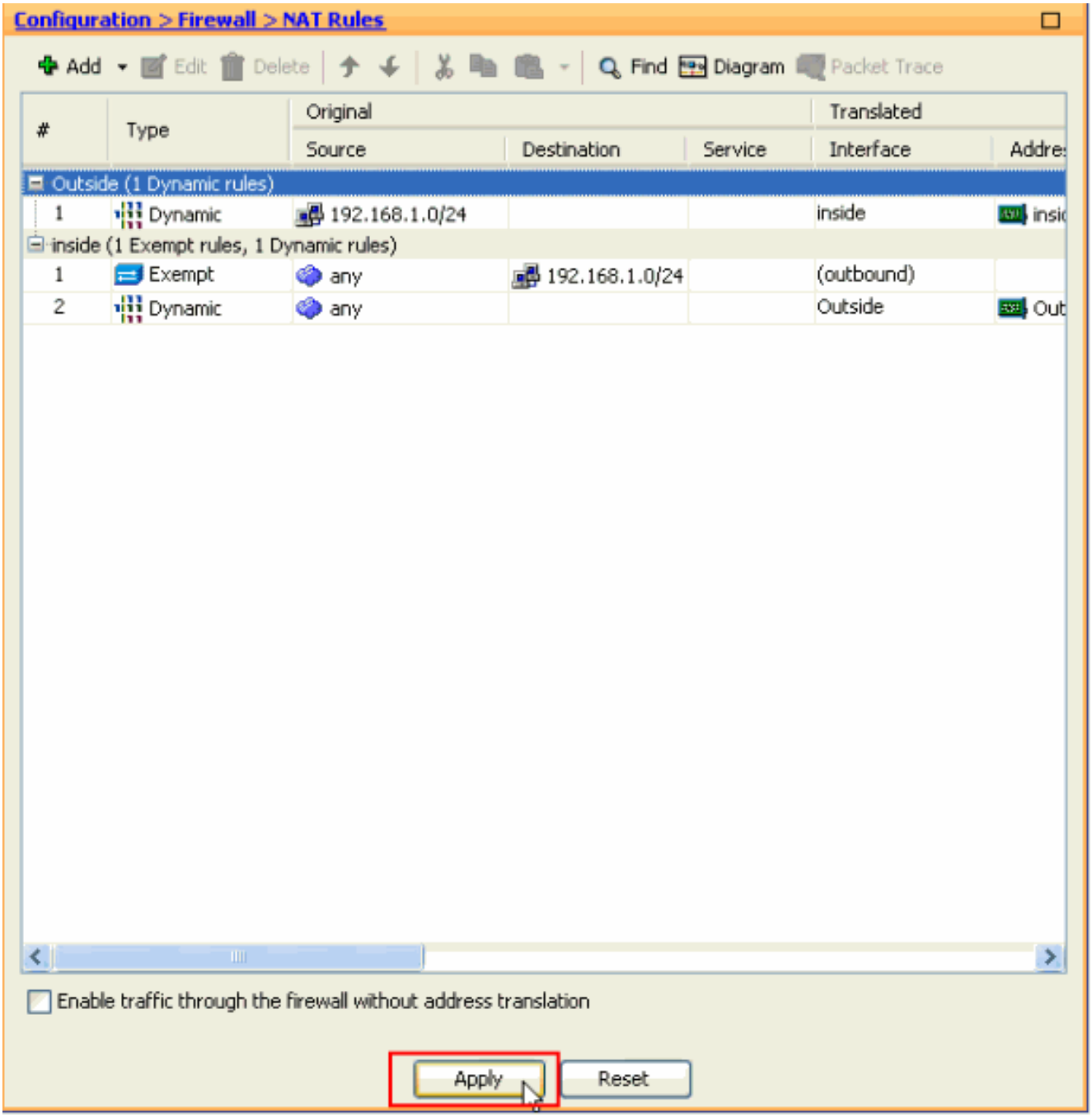
6. Kies in het venster Global Address Pool **binnendringen** als de interface en **2** als de **Pool ID**. Zorg er ook voor dat de radioknop naast **PAT met IP-adres van de interface** is geselecteerd. Klik op **Add>>** en vervolgens op **OK**.



7. Klik op **OK** nadat u de globale pool met de **Pool ID 2** in de vorige stap hebt geselecteerd.



8. Klik nu op **Toepassen** zodat de configuratie wordt toegepast op de ASA. Dit voltooit de configuratie.



ASA/PIX configureren als een externe VPN-server en voor inkomende NAT met CLI

Config op het ASA-apparaat uitvoeren

```
ciscoasa#show running-config

: Saved
ASA Version 8.0(3)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 10.10.10.2 255.255.255.0
!
interface Ethernet0/1
```

```
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa803-k8.bin
ftp mode passive
access-list inside_nat0_outbound extended permit ip any
192.168.1.0 255.255.255
0
pager lines 24
logging enable
mtu Outside 1500
mtu inside 1500
ip local pool vpnpool 192.168.1.1-192.168.1.254 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-615.bin
asdm history enable
arp timeout 14400
nat-control
global (Outside) 1 interface
global (inside) 2 interface
nat (Outside) 2 192.168.1.0 255.255.255.0 outside
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 0.0.0.0 0.0.0.0
route Outside 0.0.0.0 0.0.0.0 10.10.10.3 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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
no snmp-server location
no snmp-server contact

!--- 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 ESP-DES-
SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-
hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
pfs group1
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
transform-set ESP-DES-SH
 ESP-DES-MD5
crypto map Outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
crypto map Outside_map interface Outside
crypto isakmp enable Outside

!--- 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 10
authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 30
 authentication pre-share
 encryption des
 hash md5
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 60
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
group-policy cisco internal
group-policy cisco attributes
 vpn-tunnel-protocol IPSec

!--- Specifies the username and password with their !---
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15
username cisco password ffIRPGpDSOJh9YLq encrypted
privilege 0

username cisco attributes
 vpn-group-policy cisco
tunnel-group cisco type remote-access
tunnel-group cisco general-attributes
 address-pool vpnpool
 default-group-policy cisco

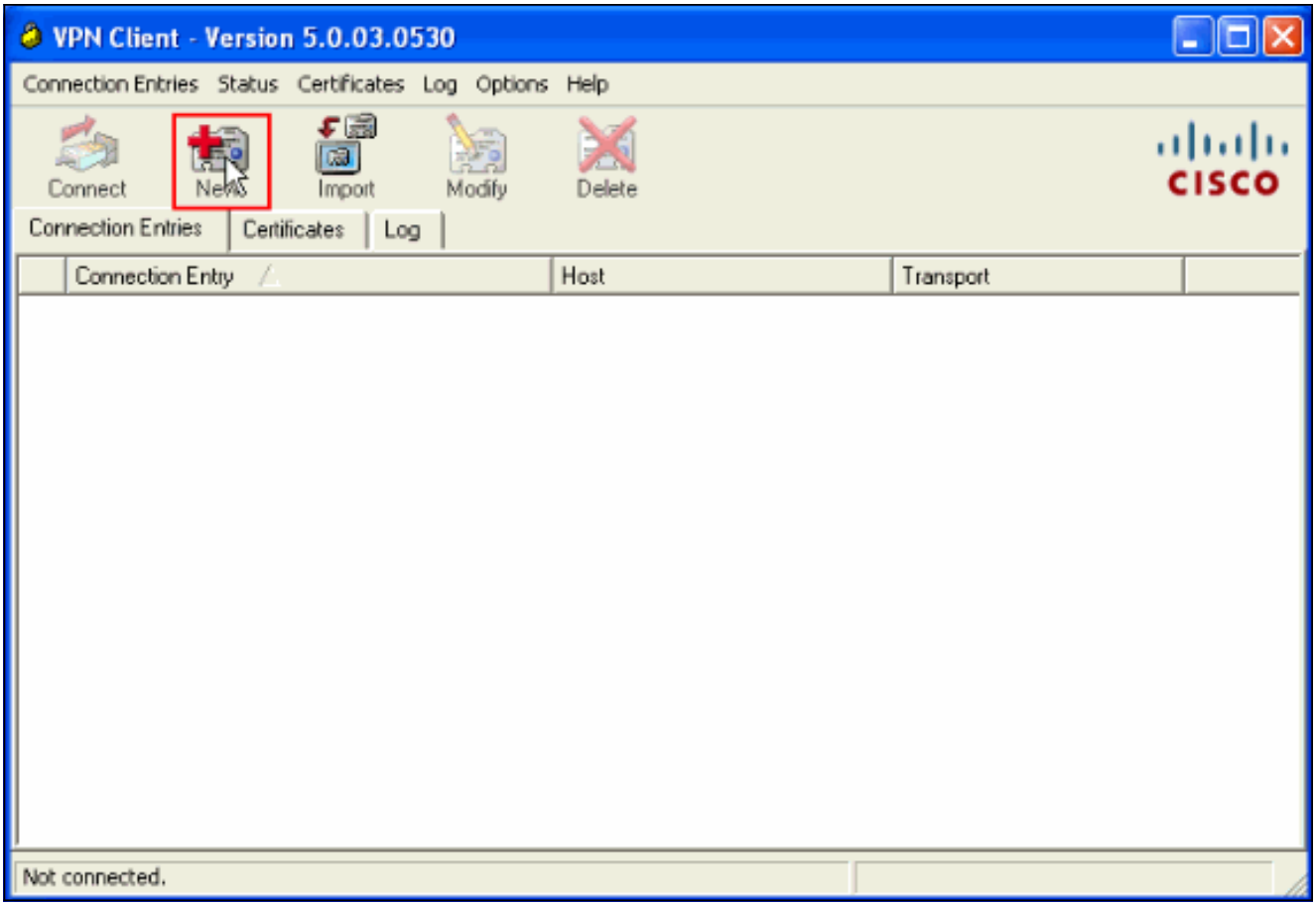
!--- Specifies the pre-shared key "cisco123" which must
!--- be identical at both peers. This is a global !---
configuration mode command. tunnel-group cisco ipsec-
attributes
 pre-shared-key *
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

```
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3
: end
ciscoasa#
```

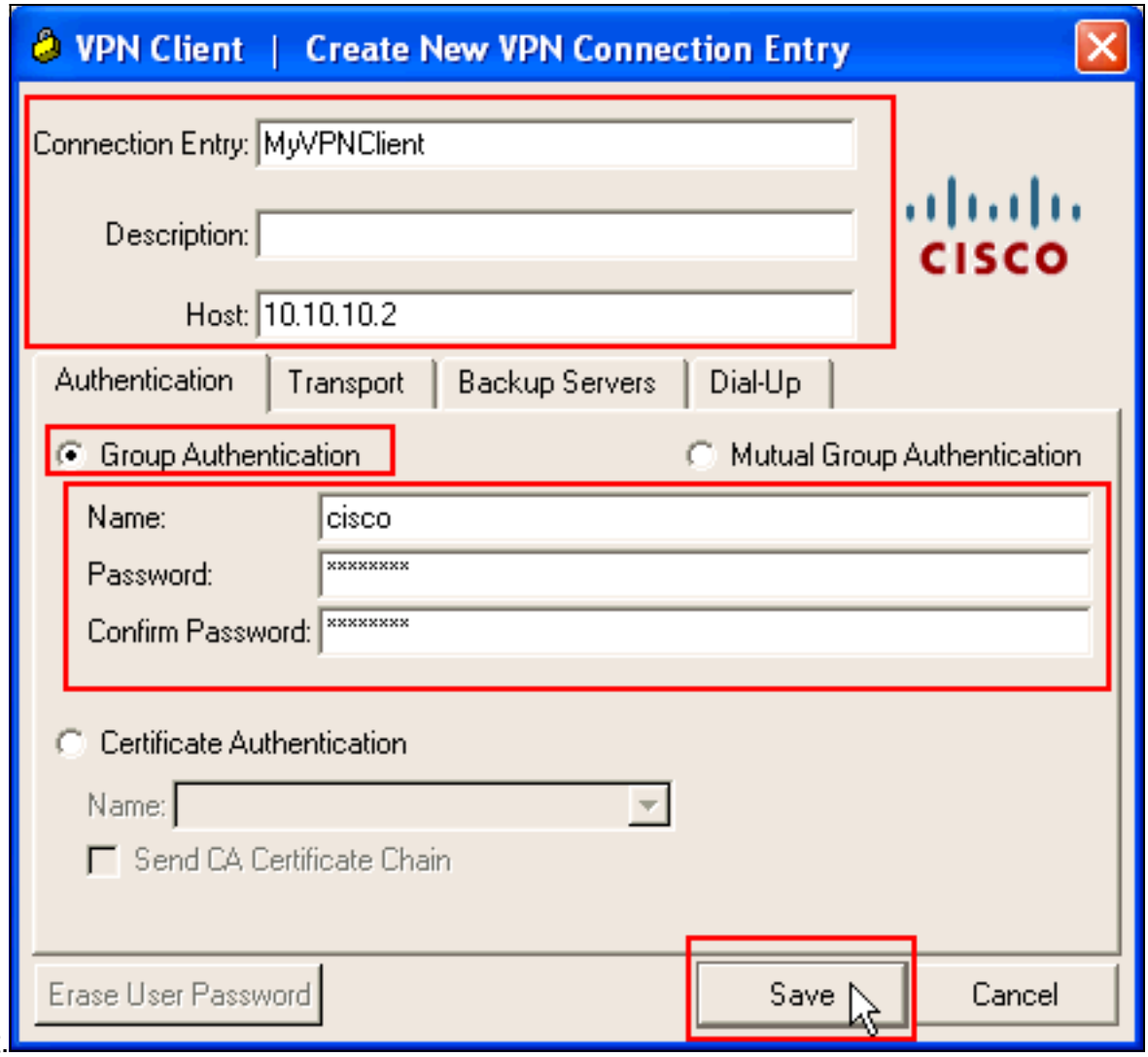
Verifiëren

Probeer via de Cisco ASA-client verbinding te maken met de Cisco ASA om te controleren of de ASA is geconfigureerd.

1. Klik op **Nieuw**.

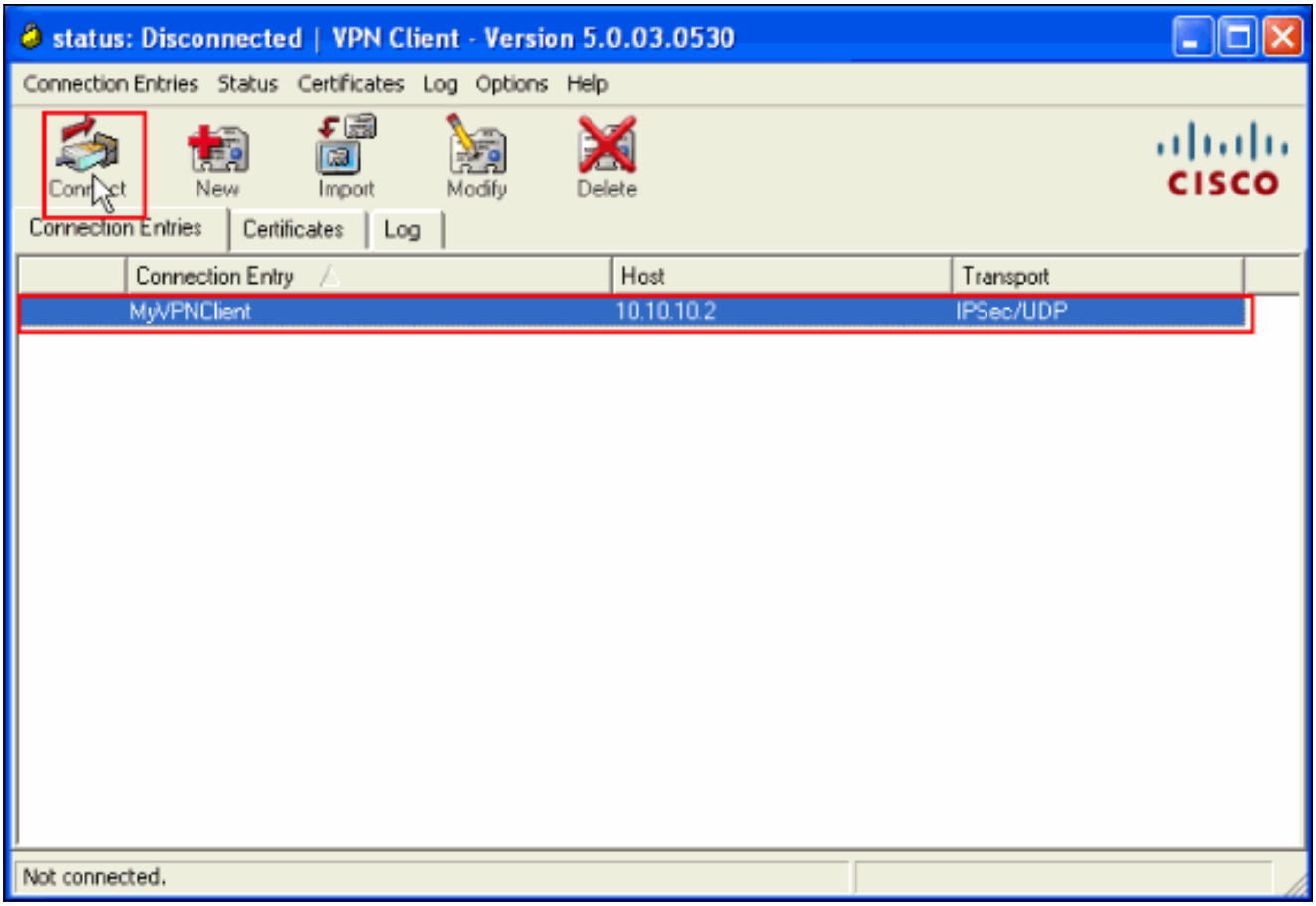


2. Vul de gegevens in van uw nieuwe aansluiting.Het veld Host moet het IP-adres of de hostnaam van de eerder geconfigureerd Cisco ASA bevatten. De informatie over de groepsverificatie moet overeenkomen met de informatie die in **stap 4** wordt gebruikt. Klik op **Opslaan** als u klaar



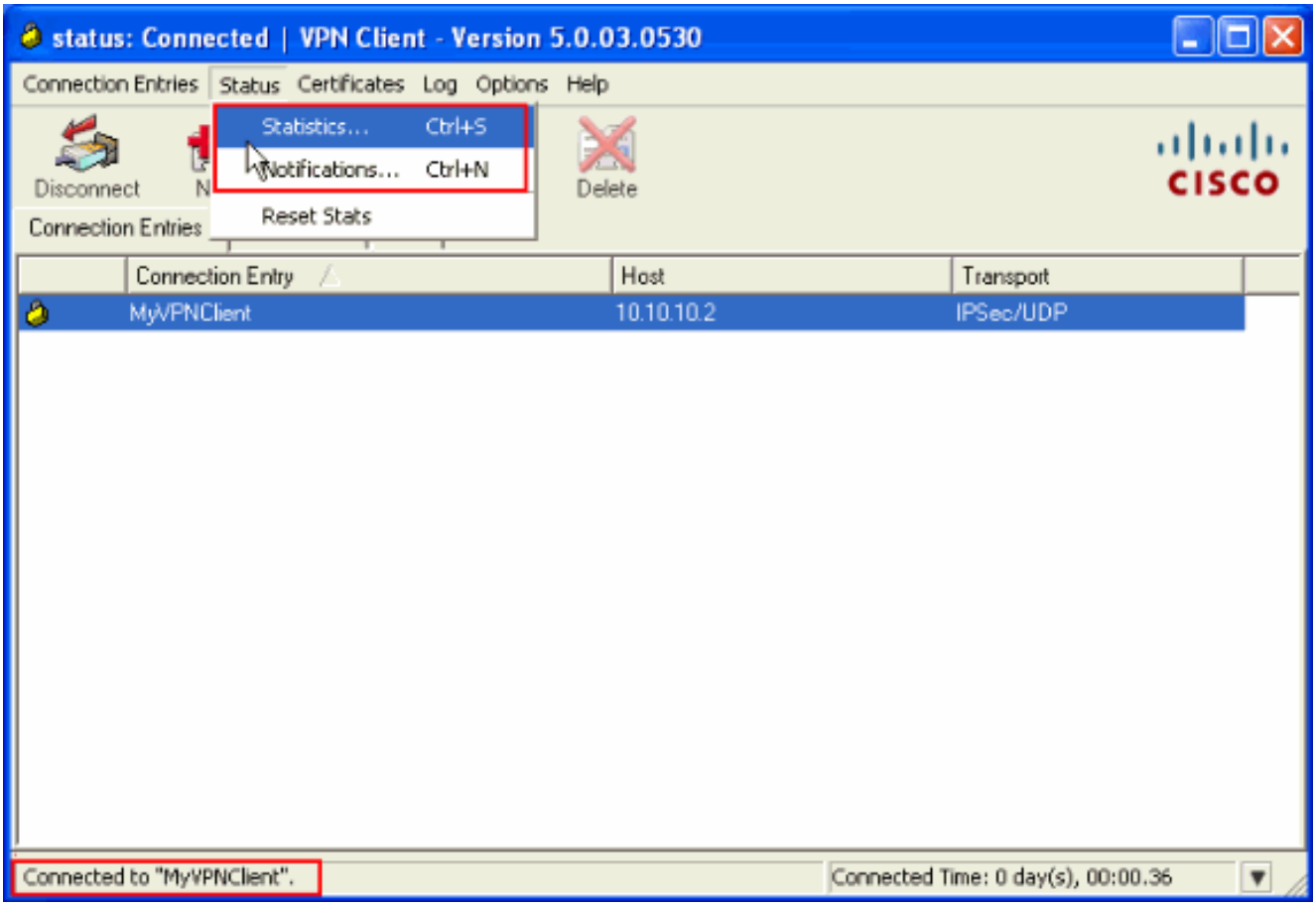
bent.

3. Selecteer de nieuwe verbinding en klik op **Connect**.

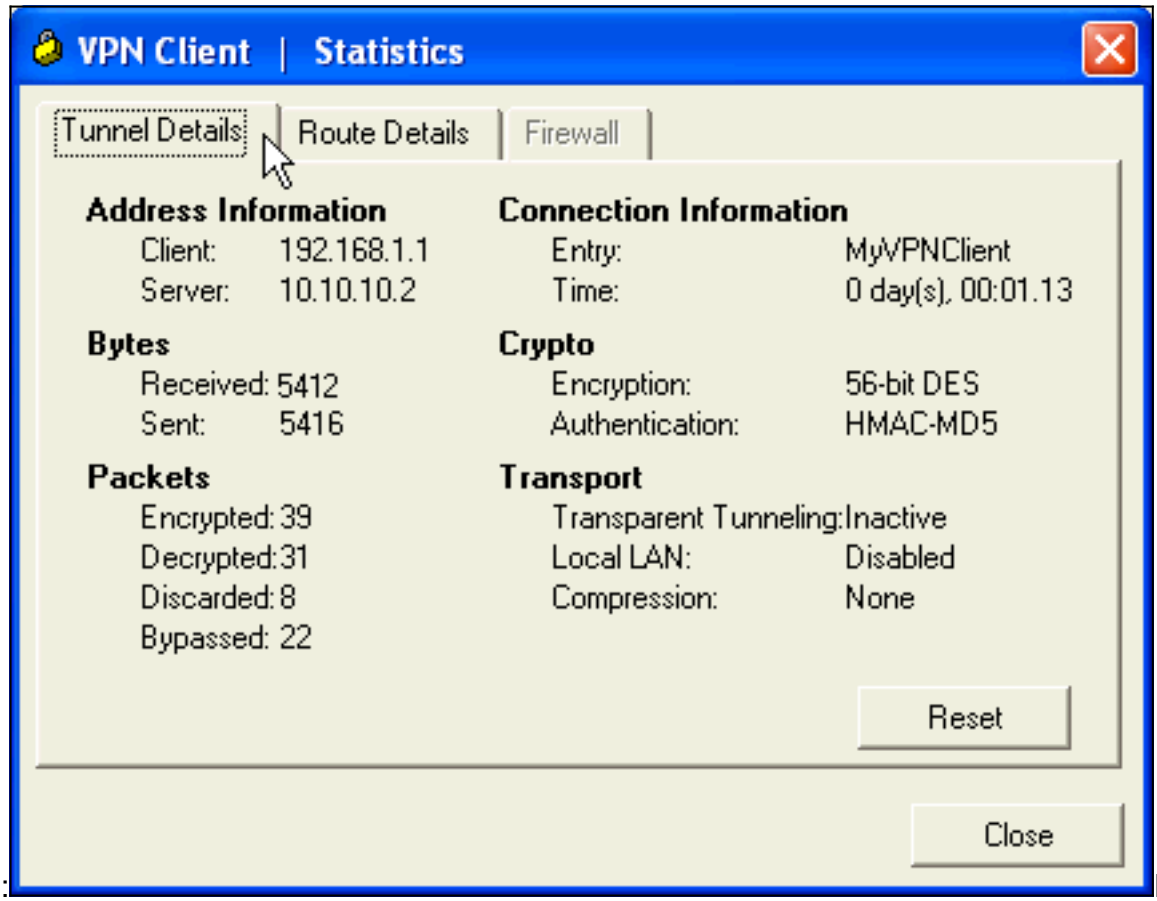


4. Voer een gebruikersnaam en wachtwoord in voor uitgebreide verificatie. Deze informatie moet overeenkomen met de informatie die in **stappen 5 en 6** is gespecificeerd.

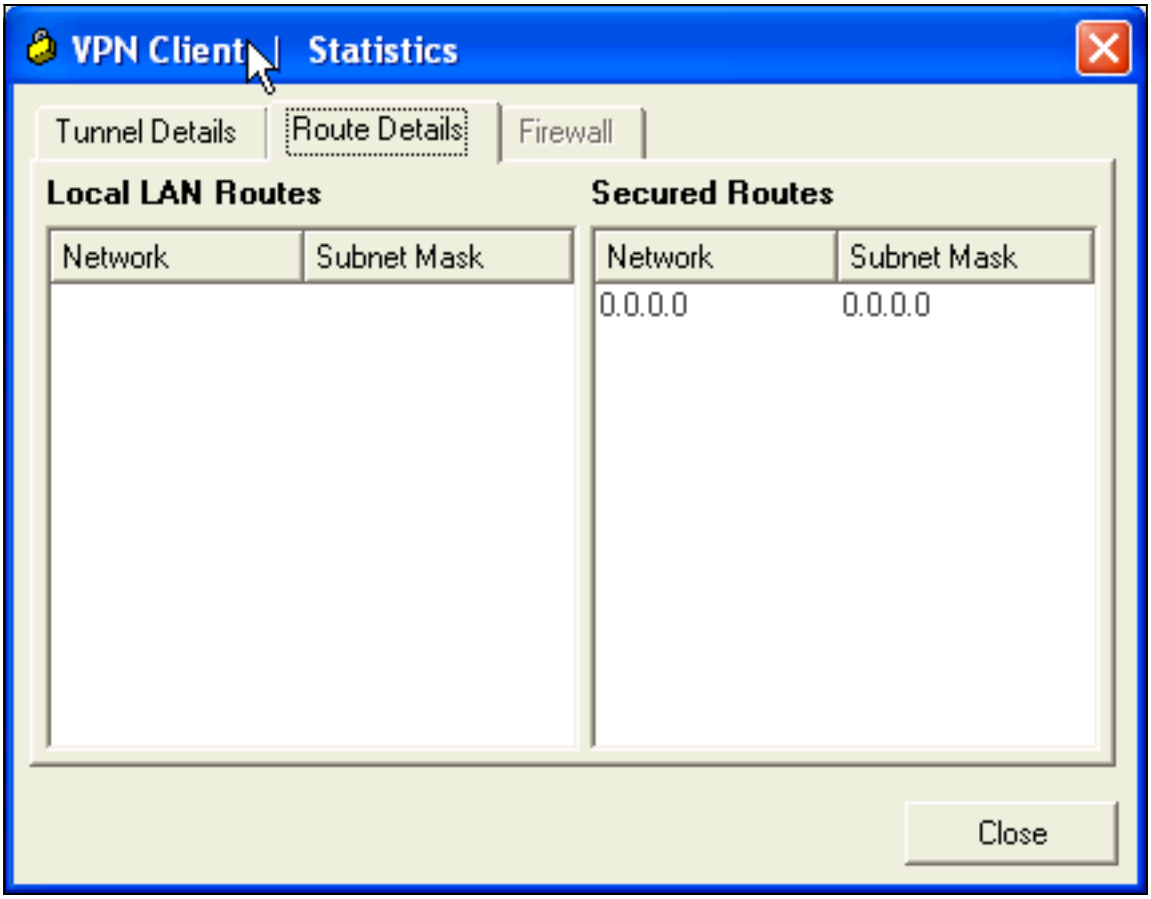
5. Zodra de verbinding met succes is tot stand gebracht, kiest u **Statistieken** uit het menu Status om de details van de tunnel te controleren.



Dit venster toont informatie over verkeer en



crypto: In dit venster wordt informatie over gesplitste tunneling weergegeven:



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: 10.10.10.1
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE
```

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

```
ASA#show crypto ipsec sa
interface: Outside
    Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10
.10.2

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
      current_peer: 10.10.10.1, username: cisco123
      dynamic allocated peer ip: 192.168.1.1

      #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
      #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 20, #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.: 10.10.10.2, remote crypto endpt.: 10.10.10.1
```

```
      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: F49F954C

    inbound esp sas:
      spi: 0x3C10F9DD (1007745501)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 27255
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xF49F954C (4104099148)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 27255
         IV size: 8 bytes
         replay detection support: Y
```

- ```
  ciscoasa(config)#debug icmp trace
  !--- Inbound Nat Translation is shown below for Outside to Inside ICMP echo request
  translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
  ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3
  2
  !--- Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply
  untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
  ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192
  len=32
  ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
  ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3
  2
  ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
  ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32
  ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32
  ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32
  ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32
  ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32
  ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32
  ```

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.

Raadpleeg de meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing voor meer informatie over de oplossing van problemen met de site-site VPN.

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties
- Cisco adaptieve security apparaatbeheer
- Cisco ASA 5500 Series adaptieve security applicaties, probleemoplossing en meldingen
- Technische ondersteuning en documentatie – Cisco Systems
  ```