

PIX/ASA en VPN-client voor publiek internet

VPN op een tick Configuration-voorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Helling of U-bocht](#)

[Configuraties](#)

[Netwerkdigram](#)

[CLI-configuratie van PIX/ASA](#)

[ASA/PIX configureren met ASDM](#)

[VPN-clientconfiguratie](#)

[Verifiëren](#)

[VPN-clientverificatie](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document beschrijft hoe u een ASA security applicatie 7.2 kunt instellen en later IPsec op een stick. Deze instelling is van toepassing op een specifiek geval waarin de ASA geen gesplitste tunneling toestaat en gebruikers direct verbinding maken met de ASA voordat ze naar internet mogen.

Opmerking: In PIX/ASA versie 7.2 en later [staat](#) het [intra-interface](#) sleutelwoord al verkeer toe om dezelfde interface in te gaan en te verlaten en niet alleen IPsec-verkeer.

Raadpleeg [Router en VPN-client voor publiekelijk internet op een voorbeeld van de configuratie van de](#) stok om een soortgelijke configuratie op een centrale site router te voltooien.

Raadpleeg [PIX/ASA 7.x Enhanced Spoke-to-Client VPN met het Configuratievoorbeeld van TACACS+ Verificatie](#) om meer te weten te komen over het scenario waarin de hub PIX het verkeer van de VPN-client naar de opgenomen PIX omwijst.

Opmerking: om overlapping van IP-adressen in het netwerk te voorkomen, moet u een volledig andere pool van IP-adressen aan de VPN-client toewijzen (bijvoorbeeld 10.x.x, 172.16.x.x en 192.168.x.x). Deze IP-adresseringsregeling is behulpzaam bij het oplossen van uw netwerk.

Voorwaarden

Vereisten

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

- De hub PIX/ASA security applicatie moet versie 7.2 of hoger uitvoeren
- Cisco VPN-clientversie 5.x

Gebruikte componenten

De informatie in dit document is gebaseerd op versie 8.0.2 van het PIX- of ASA-beveiligingsapparaat en versie 5.0 van Cisco VPN-client.

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 7.2 en hoger.

Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Achtergrondinformatie

Helling of U-bocht

Deze optie is handig voor VPN-verkeer dat een interface invoert maar vervolgens uit dezelfde interface wordt routeerd. Bijvoorbeeld, als u een netwerk van hub en sprak VPN, waar het veiligheidsapparaat de hub is, en de afgelegen VPN-netwerken zijn spaken, zodat de één sprak met een ander gesproken, moet het verkeer in het security apparaat gaan en dan weer naar de ander uitgezocht.

Gebruik de opdracht **Dezelfde security-traffic** om verkeer in te voeren en dezelfde interface te verlaten.

```
securityappliance(config)#same-security-traffic permit intra-interface
```

N.B.: Helling of U-bocht is ook van toepassing voor VPN-client voor VPN-communicatie.

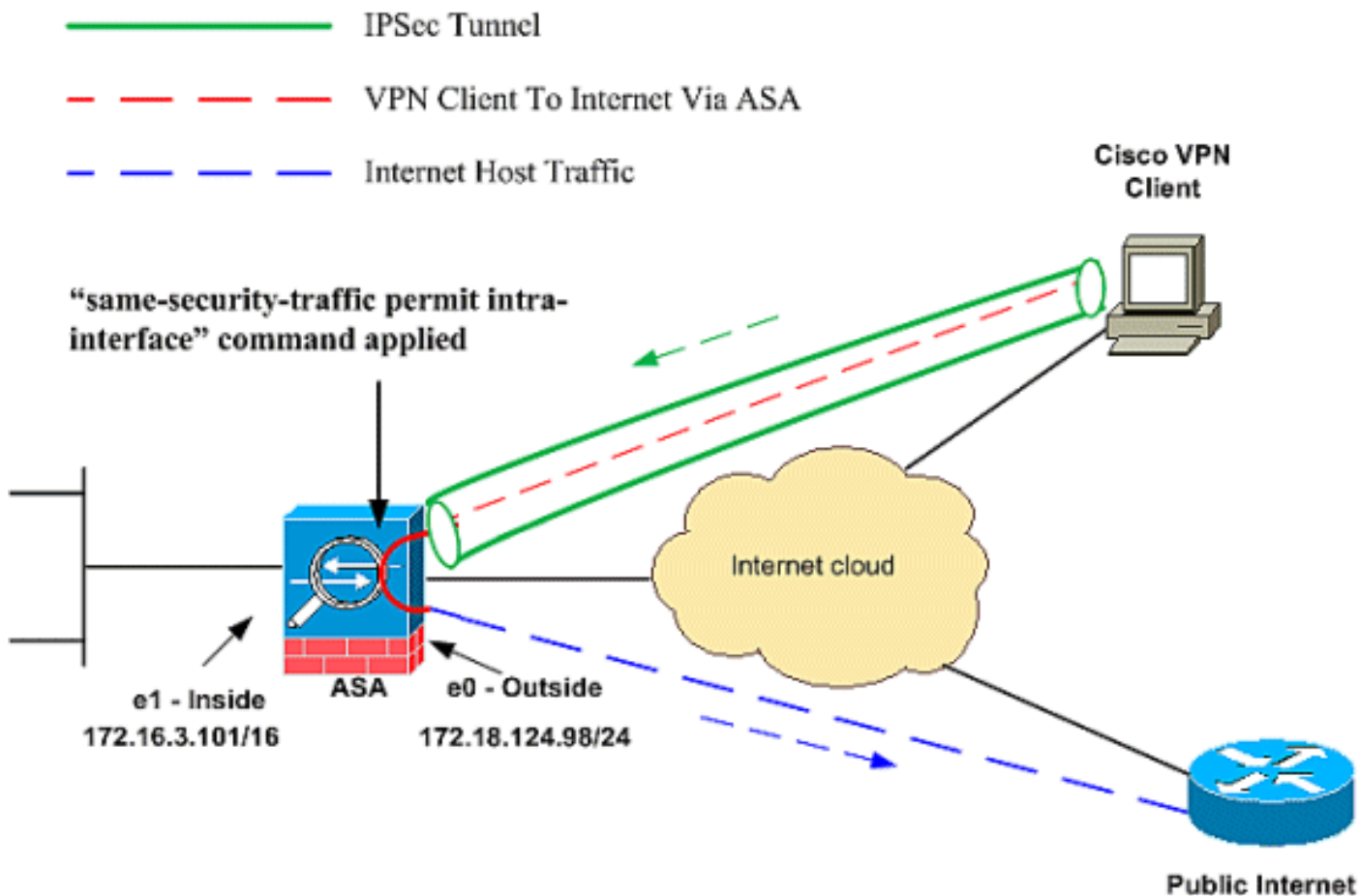
Configuraties

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

Opmerking: Gebruik het [Opname Gereedschap](#) ([alleen geregistreeerde](#) klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



CLI-configuratie van PIX/ASA

- [PIX/ASA](#)

Configuratie uitvoeren op PIX/ASA

```
PIX Version 8.0(2)
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.98 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
```

```
!  
interface Ethernet2  
shutdown  
no nameif  
no security-level  
no ip address  
!  
interface Ethernet3  
shutdown  
no nameif  
no security-level  
no ip address  
!  
interface Ethernet4  
shutdown  
no nameif  
no security-level  
no ip address  
!  
interface Ethernet5  
shutdown  
no nameif  
no security-level  
no ip address  
!  
enable password 8Ry2YjIyt7RRXU24 encrypted  
passwd 2KFQnbNIdI.2KYOU encrypted  
hostname pixfirewall  
ftp mode passive  
!--- Command that permits IPsec traffic to enter and  
exit the same interface. same-security-traffic permit  
intra-interface  
access-list 100 extended permit icmp any any echo-reply  
pager lines 24  
logging enable  
logging buffered debugging  
mtu outside 1500  
mtu inside 1500  
  
ip local pool vpnpool  
192.168.10.1-192.168.10.254 mask 255.255.255.0  
  
no failover  
monitor-interface outside  
monitor-interface inside  
icmp permit any outside  
no asdm history enable  
arp timeout 14400  
nat-control!!--- The address pool for the VPN Clients. !-  
-- The global address for Internet access used by VPN  
Clients. !--- Note: Uses an RFC 1918 range for lab  
setup. !--- Apply an address from your public range  
provided by your ISP.  
  
global (outside) 1 172.18.124.166  
  
!--- The NAT statement to define what to encrypt (the  
addresses from the vpn-pool). nat (outside) 1  
192.168.10.0 255.255.255.0  
  
nat (inside) 1 0.0.0.0 0.0.0.0  
static (inside,outside) 172.16.3.102 172.16.3.102  
netmask 255.255.255.255  
access-group 100 in interface outside
```

```
route outside 0.0.0.0 0.0.0.0 172.18.124.98 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

!--- The configuration of group-policy for VPN Clients.
group-policy clientgroup internal
group-policy clientgroup attributes
vpn-idle-timeout 20

!--- Forces VPN Clients over the tunnel for Internet
access. split-tunnel-policy tunnelall

no snmp-server location
no snmp-server contact
snmp-server enable traps snmp

!--- Configuration of IPsec Phase 2. crypto ipsec
transform-set myset esp-3des esp-sha-hmac

!--- Crypto map configuration for VPN Clients that
connect to this PIX. crypto dynamic-map rtpdynmap 20 set
transform-set myset

!--- Binds the dynamic map to the crypto map process.
crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap

!--- Crypto map applied to the outside interface. crypto
map mymap interface outside

!--- Enable ISAKMP on the outside interface. isakmp
identity address
isakmp enable outside

!--- Configuration of ISAKMP policy. isakmp policy 10
authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0

!--- Configuration of tunnel-group with group
information for VPN Clients. tunnel-group rtptacvpn type
ipsec-ra

!--- Configuration of group parameters for the VPN
Clients. tunnel-group rtptacvpn general-attributes
address-pool vpnpool

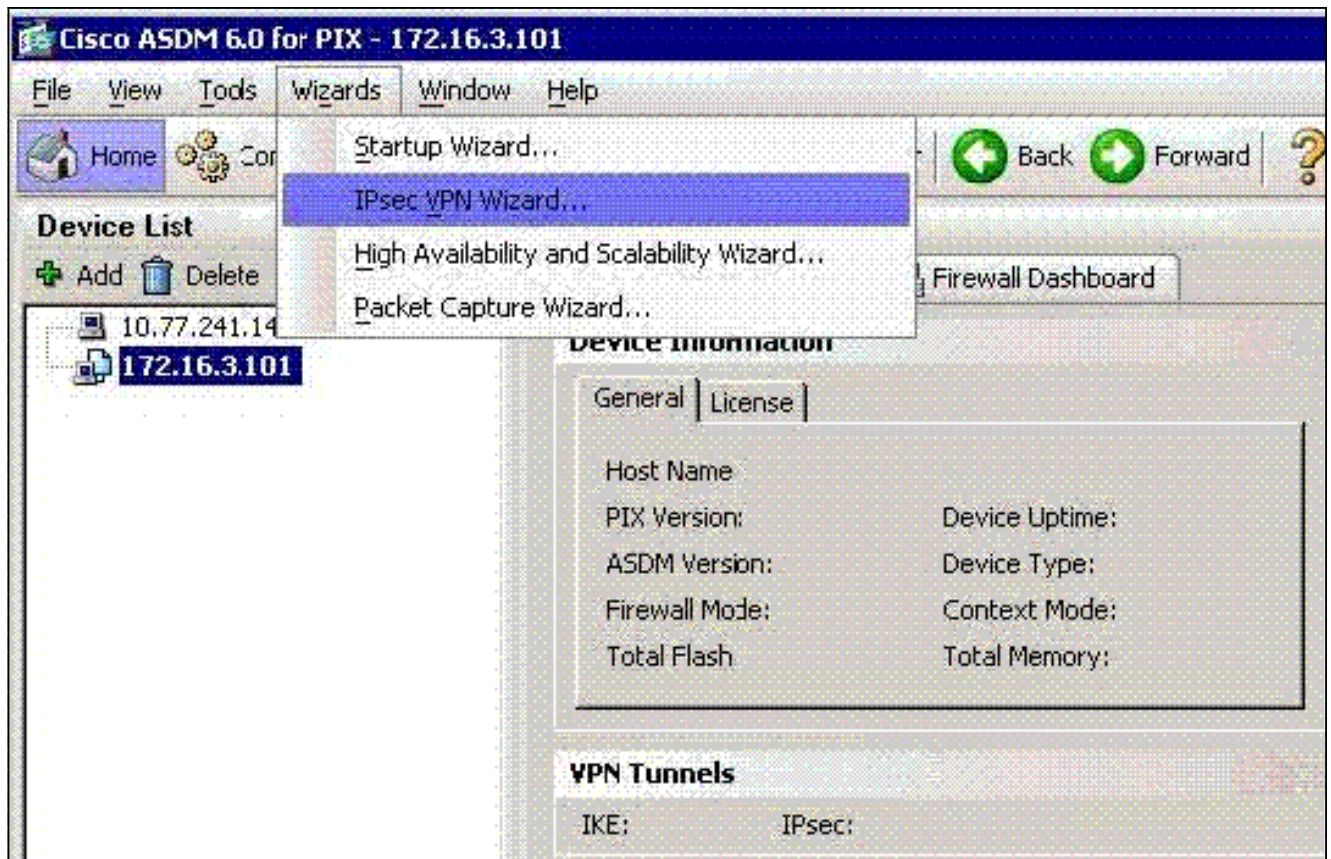
!--- Disable user authentication. authentication-server-
group none
```

```
!--- Bind group-policy parameters to the tunnel-group
for VPN Clients. default-group-policy clientgroup
tunnel-group rtptacvpn ipsec-attributes
pre-shared-key *
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
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
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0
: end
```

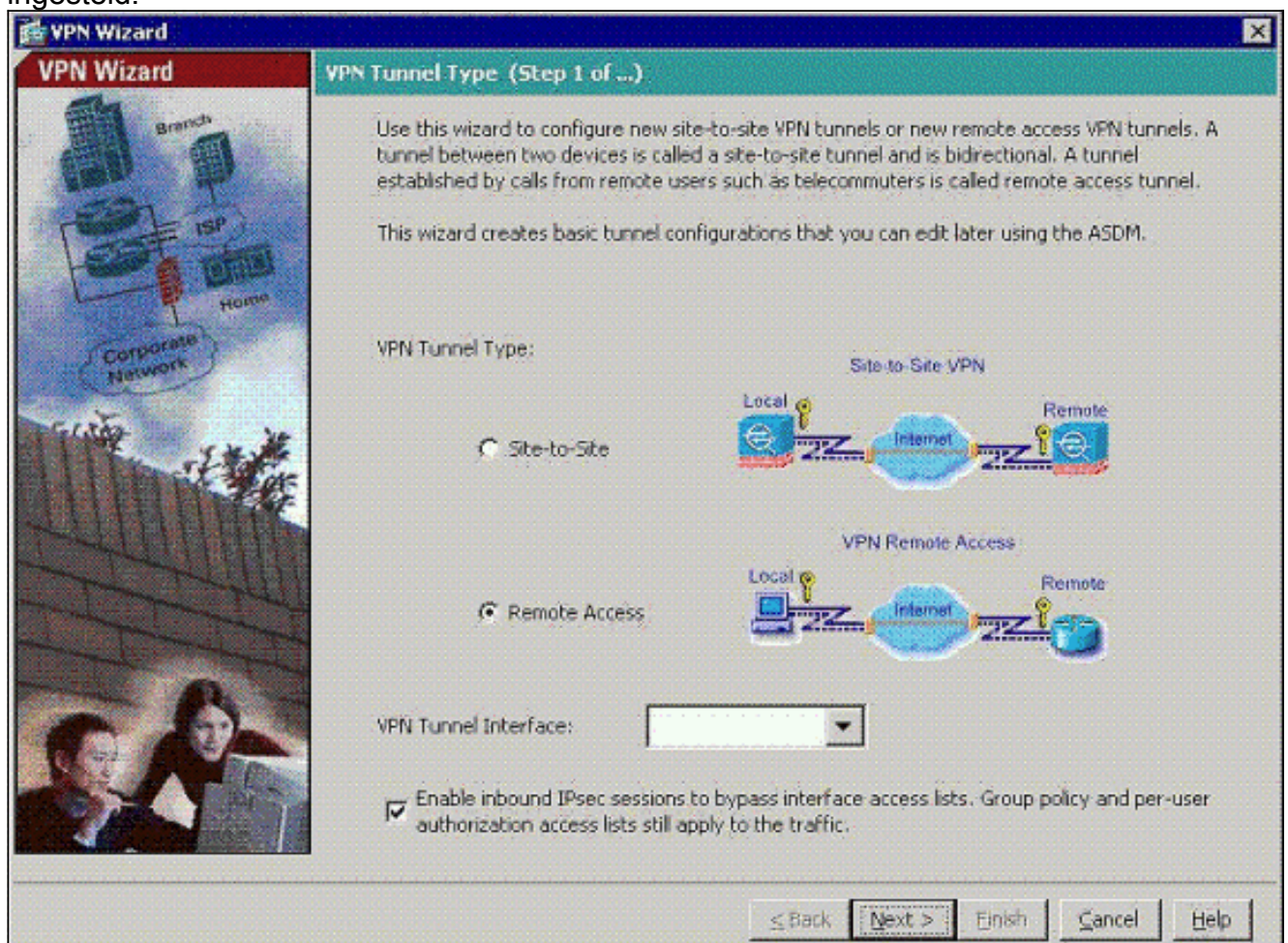
[ASA/PIX configureren met ASDM](#)

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

1. Kies **Wizard > IPsec VPN-wizard** in het startvenster.

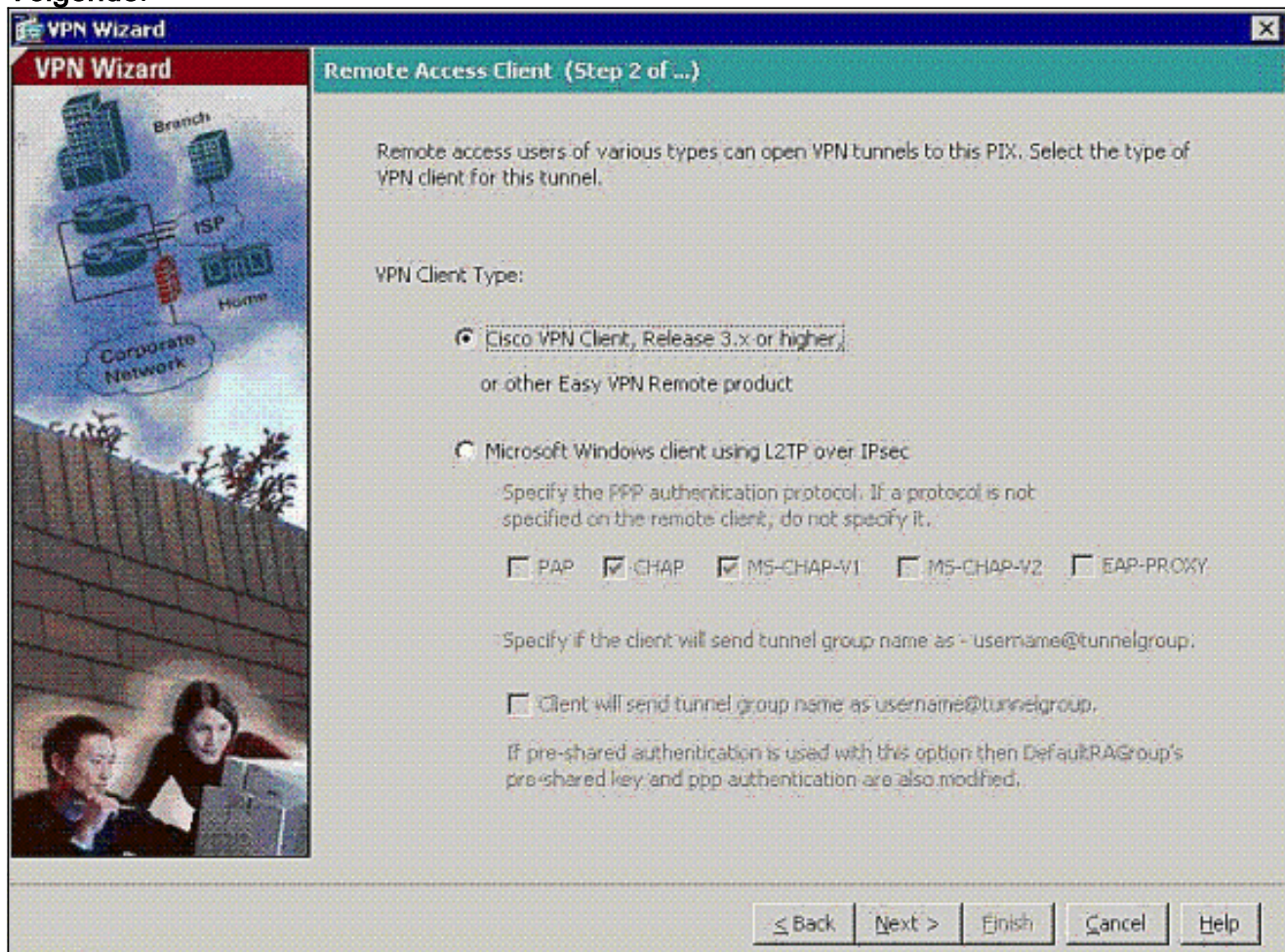


2. Kies het tunneltype **Remote Access VPN** en controleer of de VPN-tunnelinterface naar wens is ingesteld.

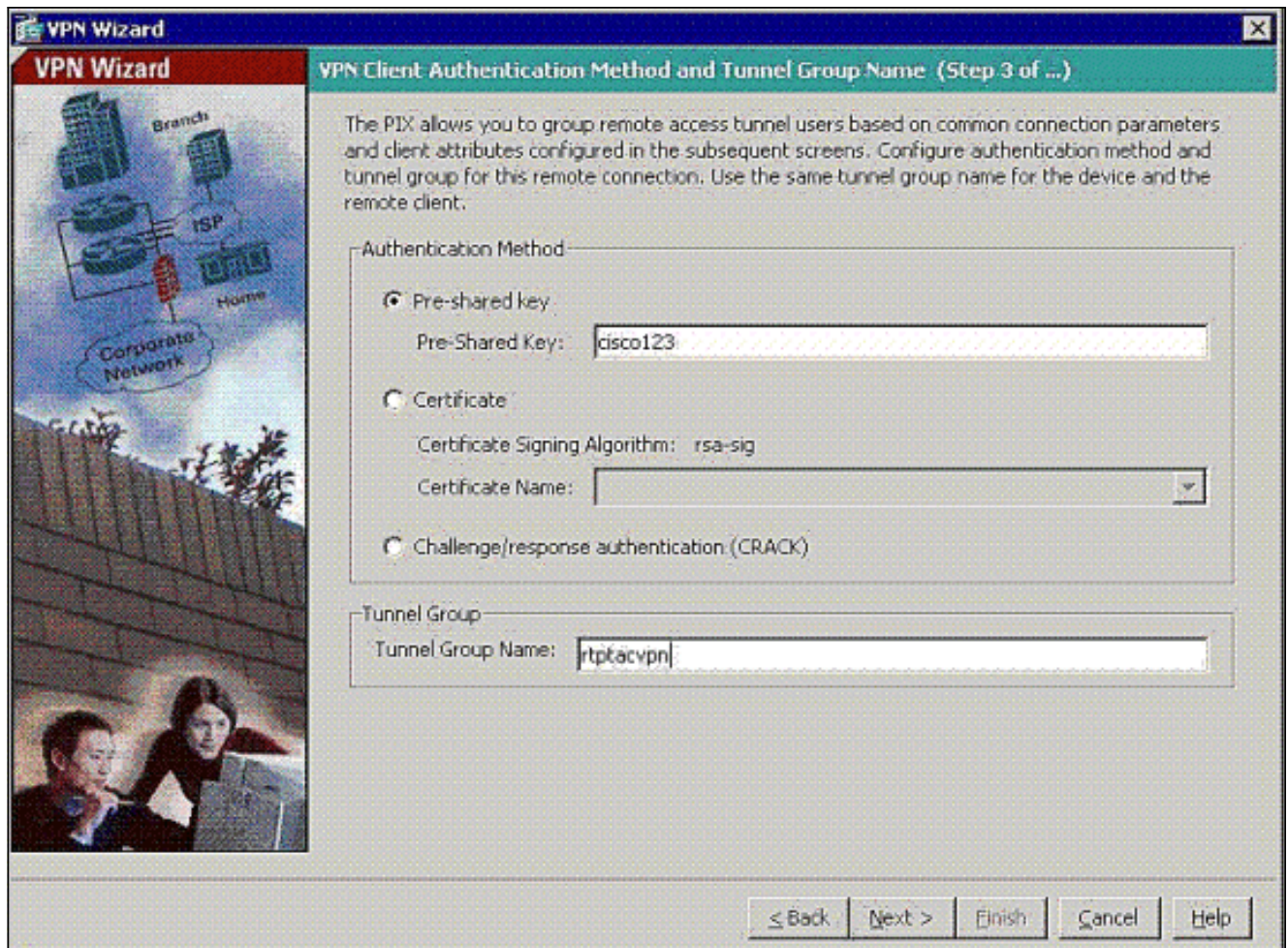


3. Het enige beschikbare VPN-clienttype is al geselecteerd. Klik op

Volgende.

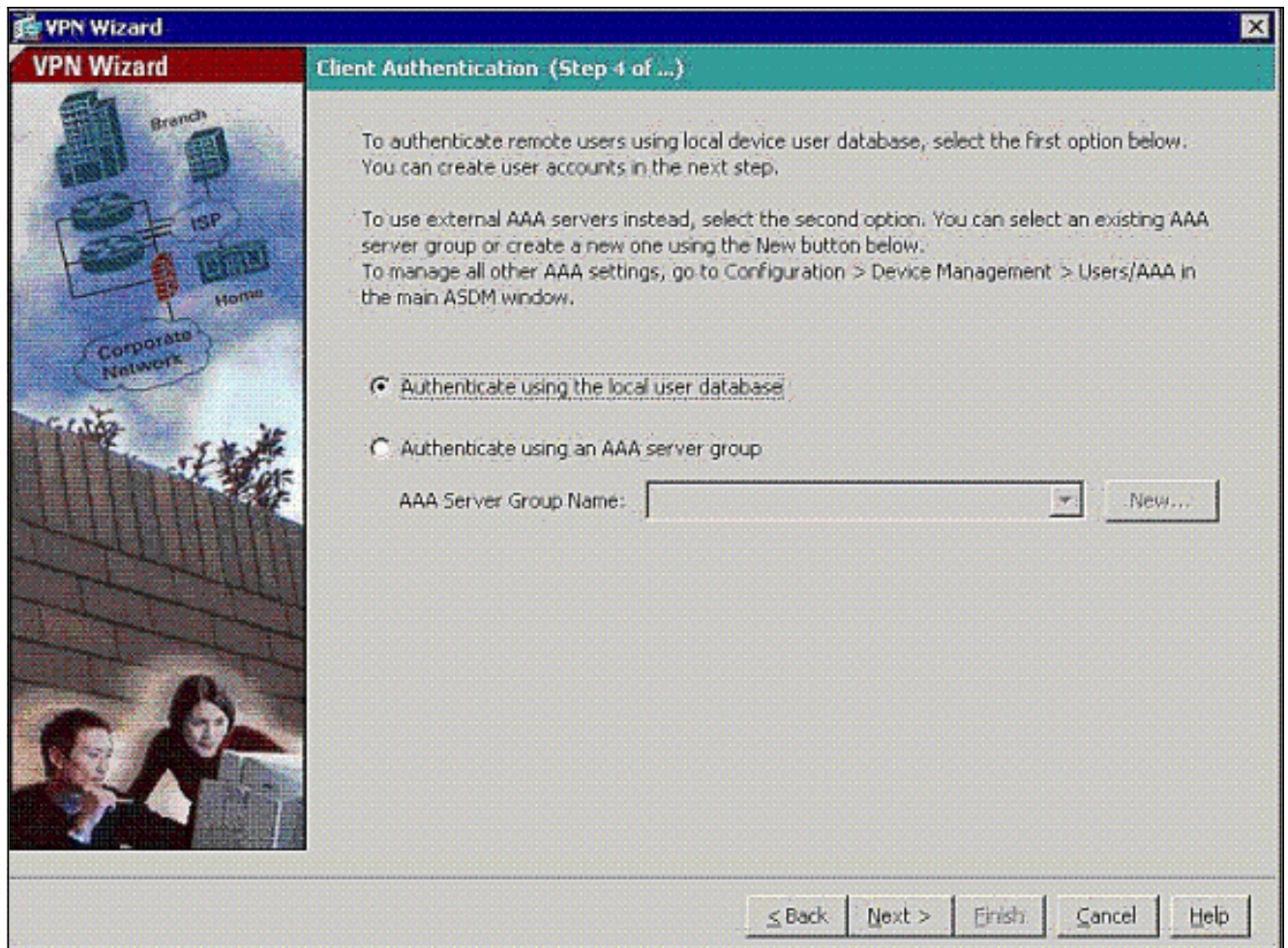


4. Voer een naam in voor de naam van de tunnelgroep. Verstrek de te gebruiken authenticatie informatie. **Vooraf gedeelde sleutel** is in dit voorbeeld geselecteerd.

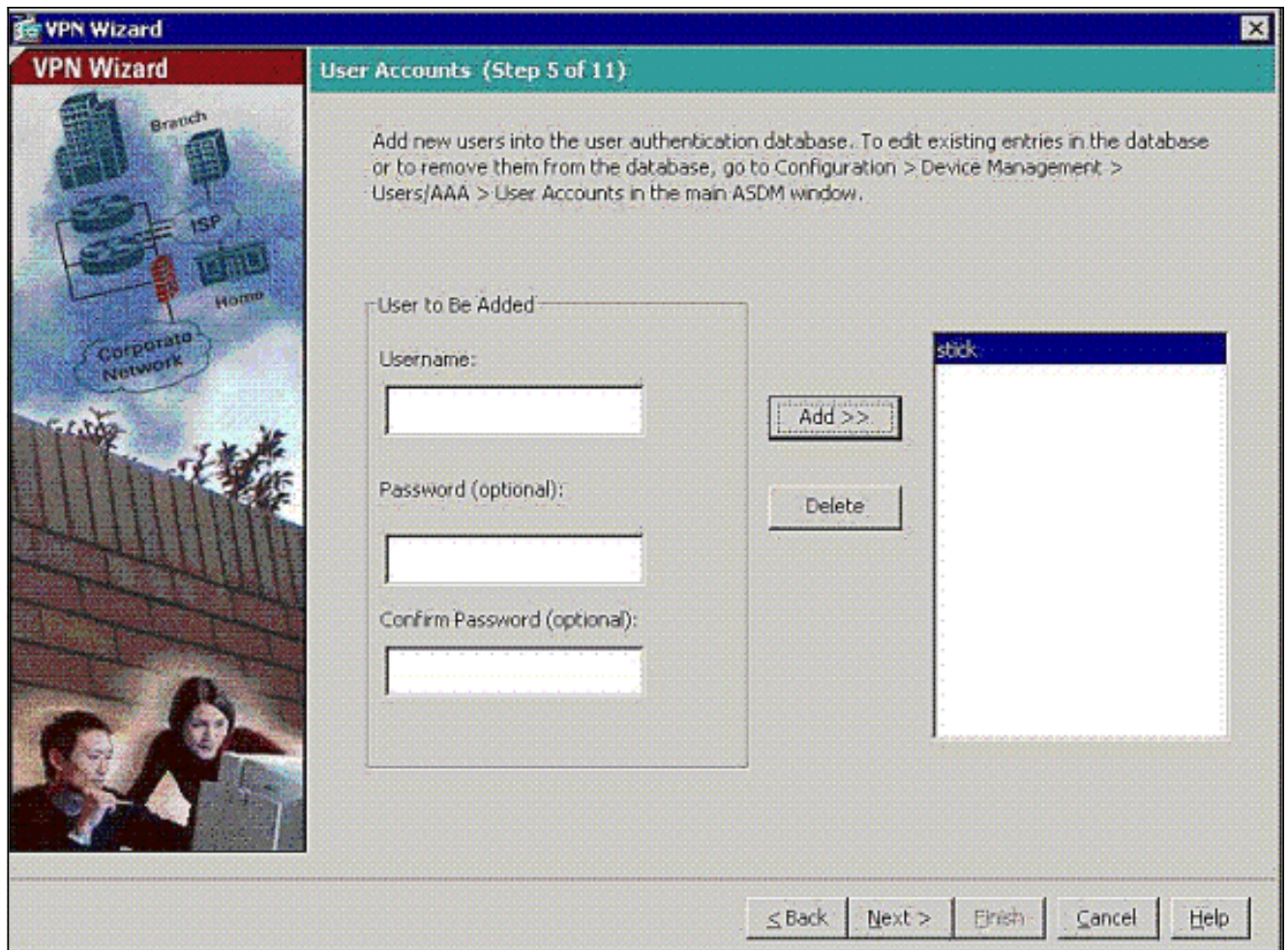


N.B.: Er is geen manier om de voorgedeelde toets op de ASDM te verbergen of te versleutelen. De reden is dat ASDM alleen gebruikt mag worden door mensen die de ASA configureren of door mensen die de klant bijstaan met deze configuratie.

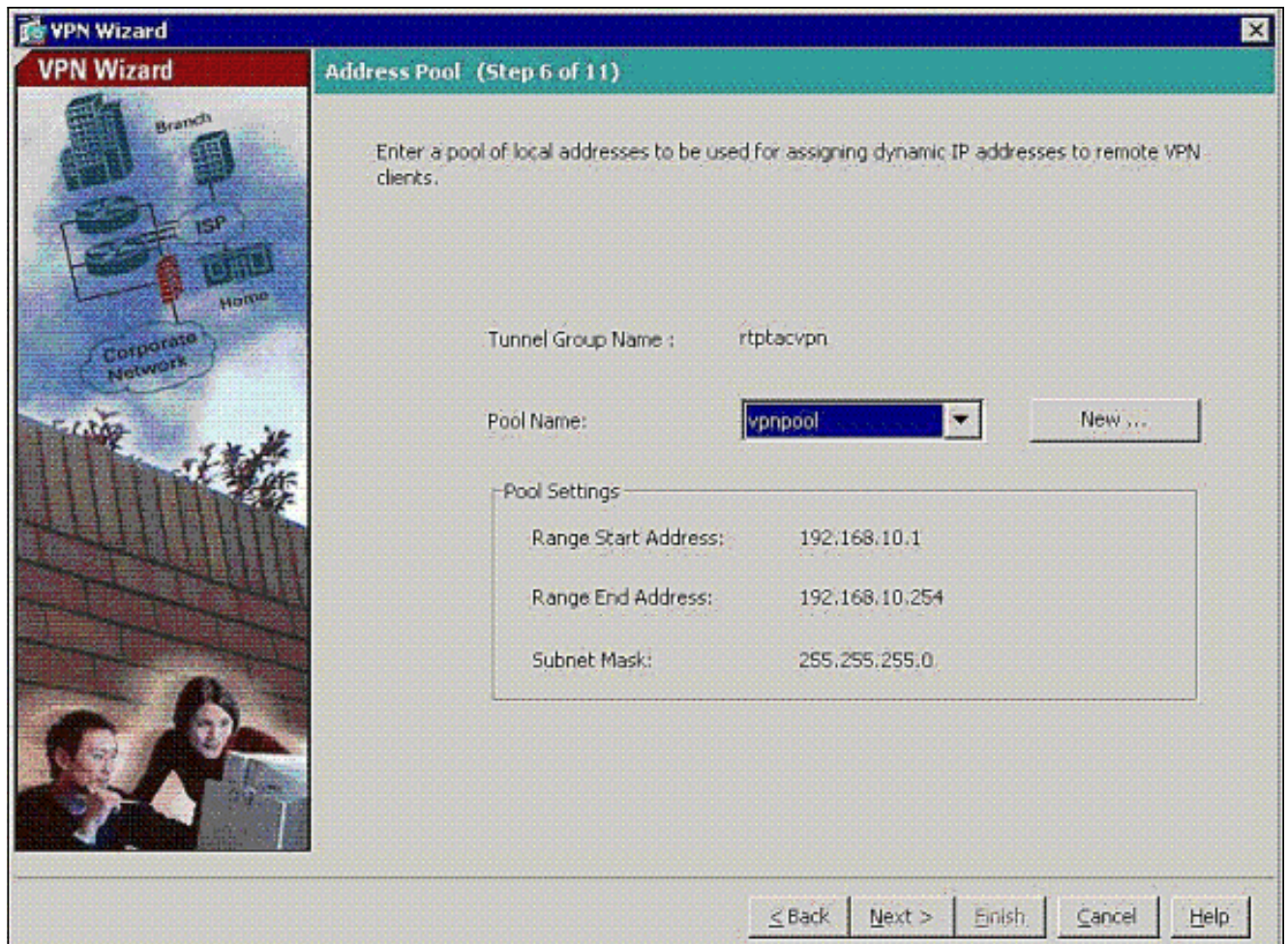
5. Kies of u externe gebruikers wilt geauthentiseerd worden naar de lokale gebruikersdatabase of naar een externe AAA server groep. **Opmerking:** U voegt in stap 6 gebruikers toe aan de lokale gebruikersdatabase. **Opmerking:** Raadpleeg [PIX/ASA 7.x-groepen voor VPN-gebruikers via het ASDM Configuration Voorbeeld](#) voor informatie over de configuratie van een externe AAA-servergroep via ASDM.



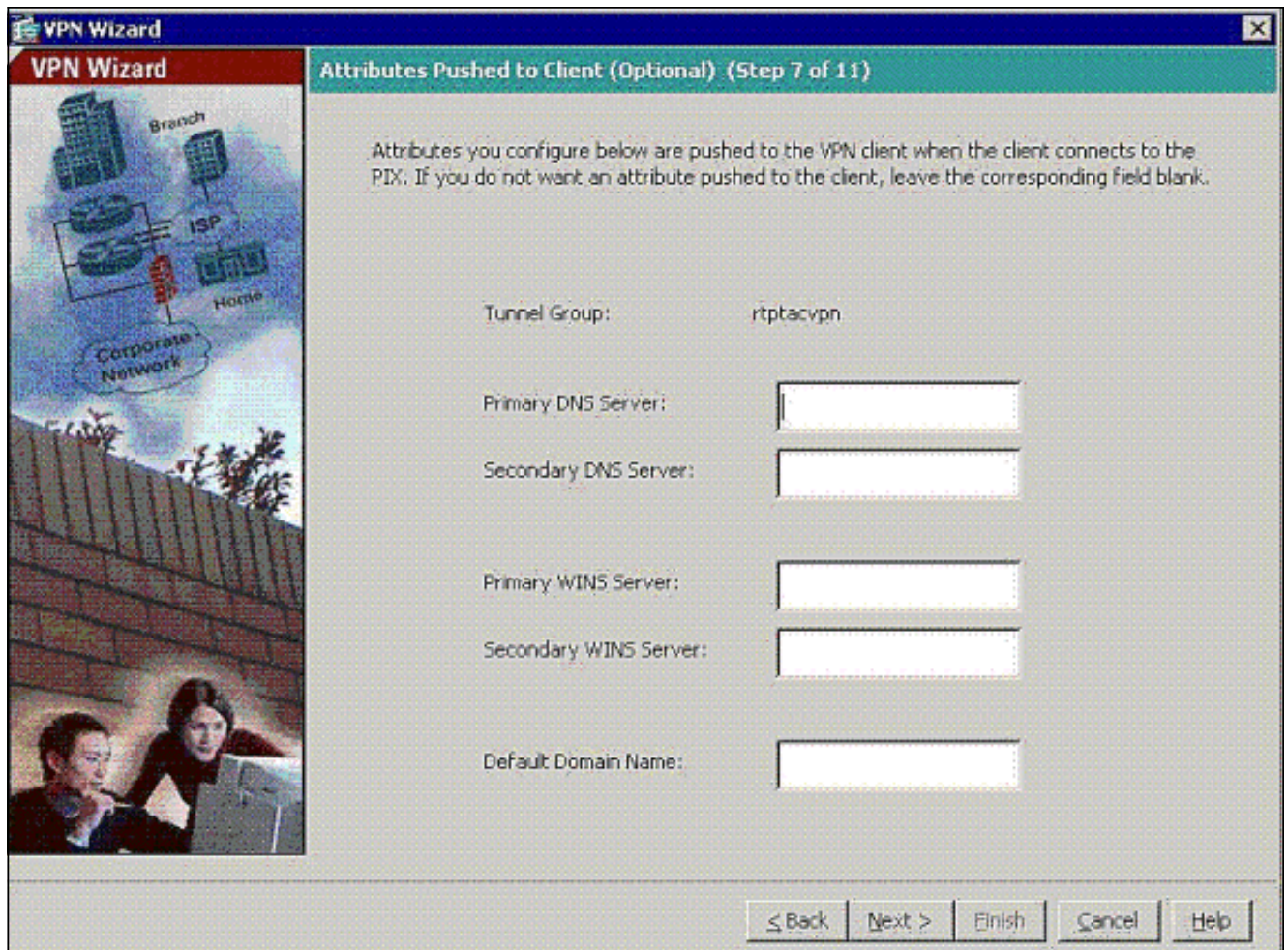
6. Voeg indien nodig gebruikers toe aan de lokale database. **N.B.:** Verwijder de huidige gebruikers niet uit dit venster. Kies **Configuratie > Apparaatbeheer > Administratie > Gebruikersrekeningen** in het hoofdvenster van ASDM om bestaande items in de database te bewerken of deze uit de database te verwijderen.



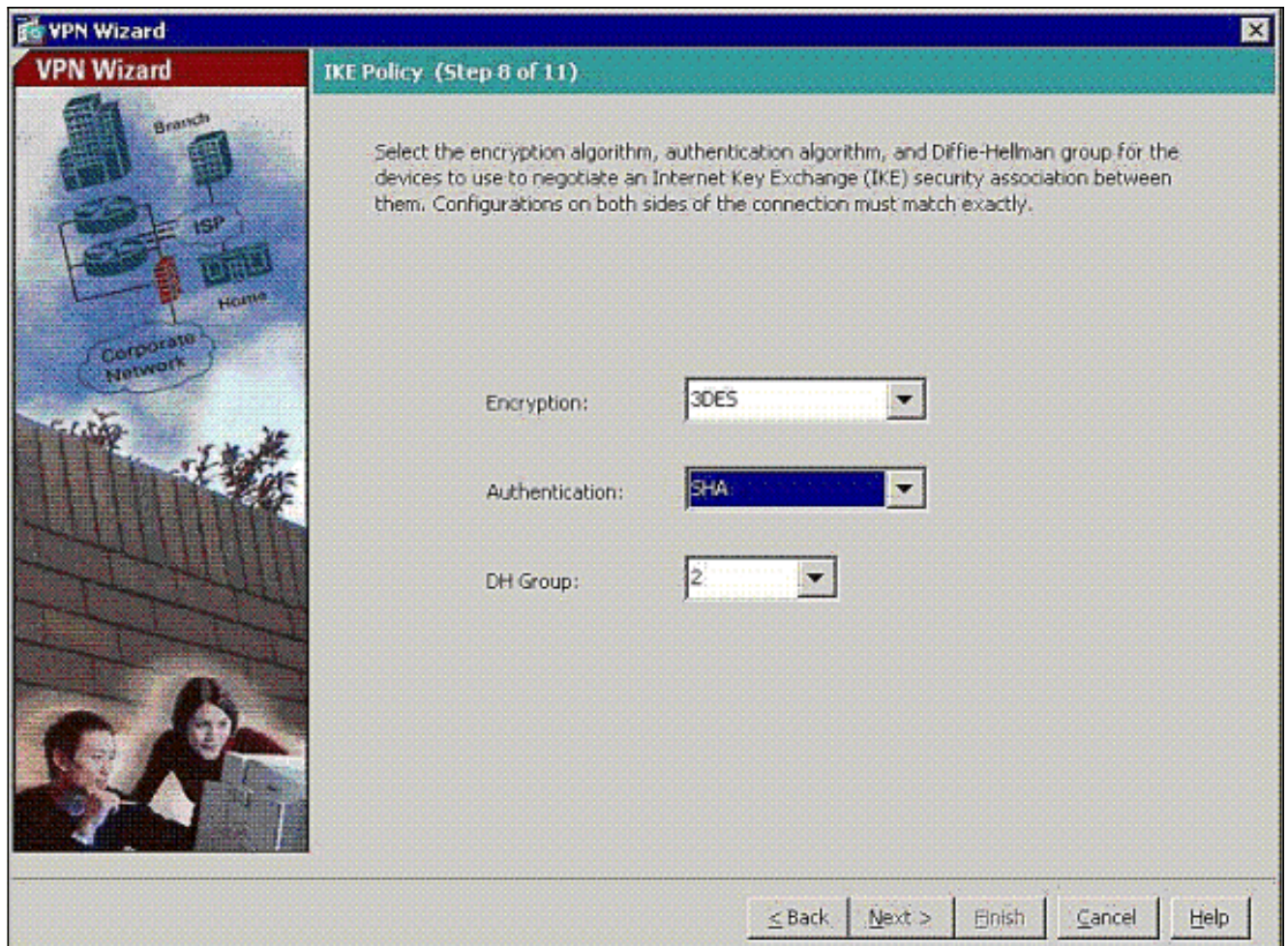
7. Definiert eine Pool von lokalen Adressen, die dynamisch an externe VPN-Clients zugeteilt werden müssen, wenn sie eine Verbindung herstellen.



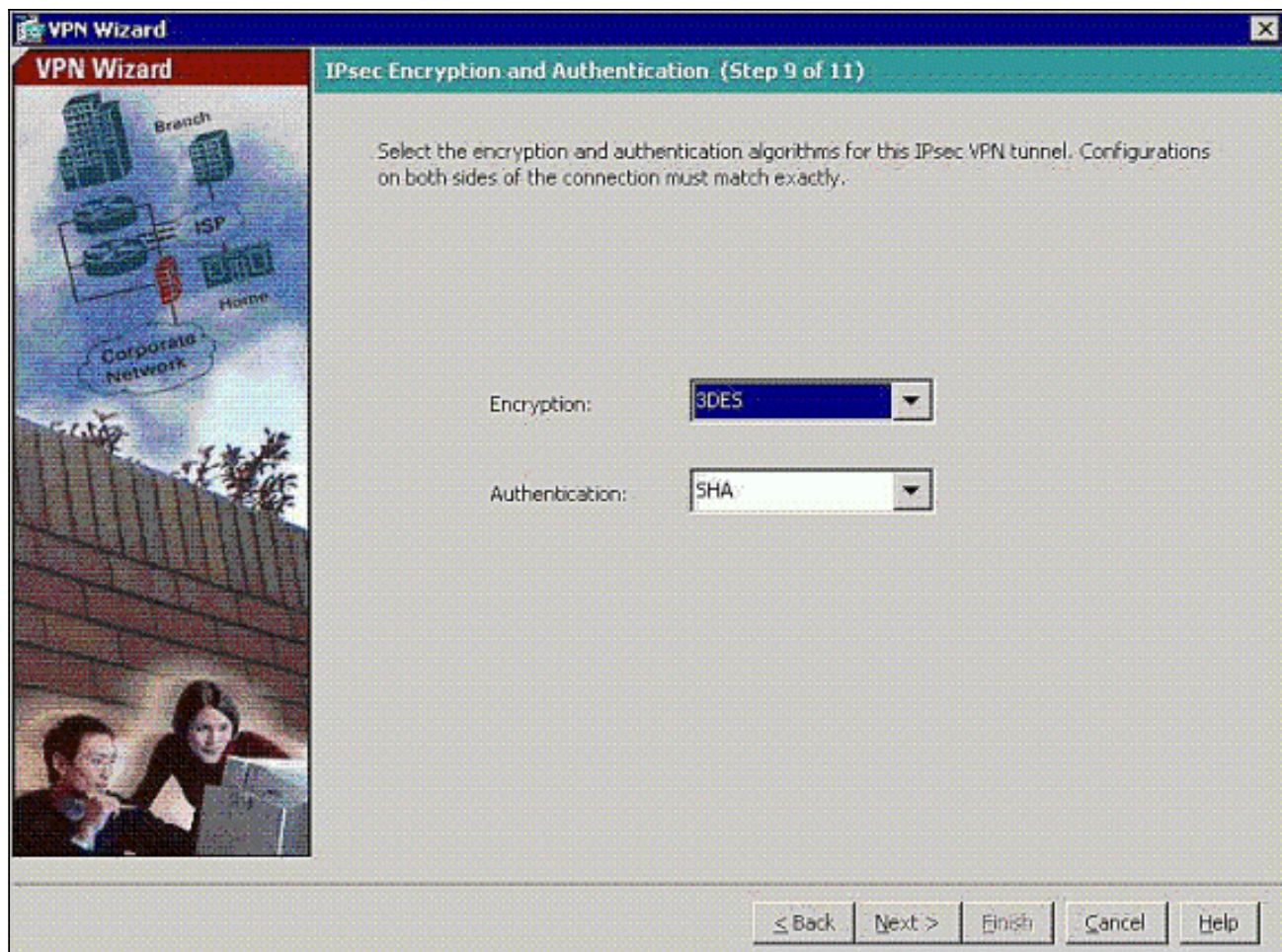
8. *Optioneel*: Specificeer de DNS- en WINS-serverinformatie en een standaardnaam voor domeinen die naar externe VPN-clients moet worden geduwd.



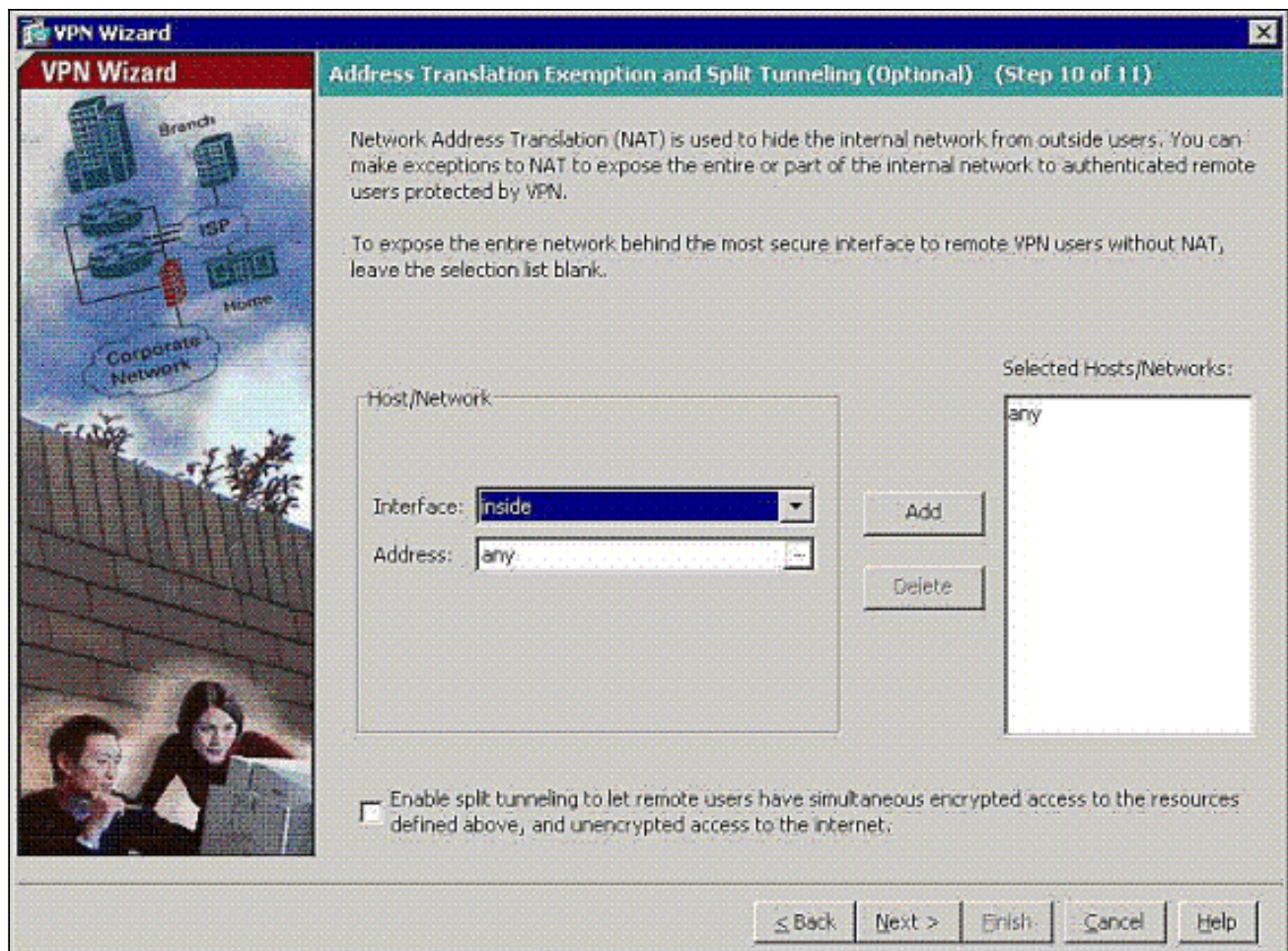
9. Specificeer de parameters voor IKE, ook bekend als IKE Fase 1. De configuraties aan beide zijden van de tunnel moeten precies overeenkomen, maar de Cisco VPN-client kiest automatisch de juiste configuratie voor zichzelf. Er is geen IKE-configuratie nodig op de client-pc.



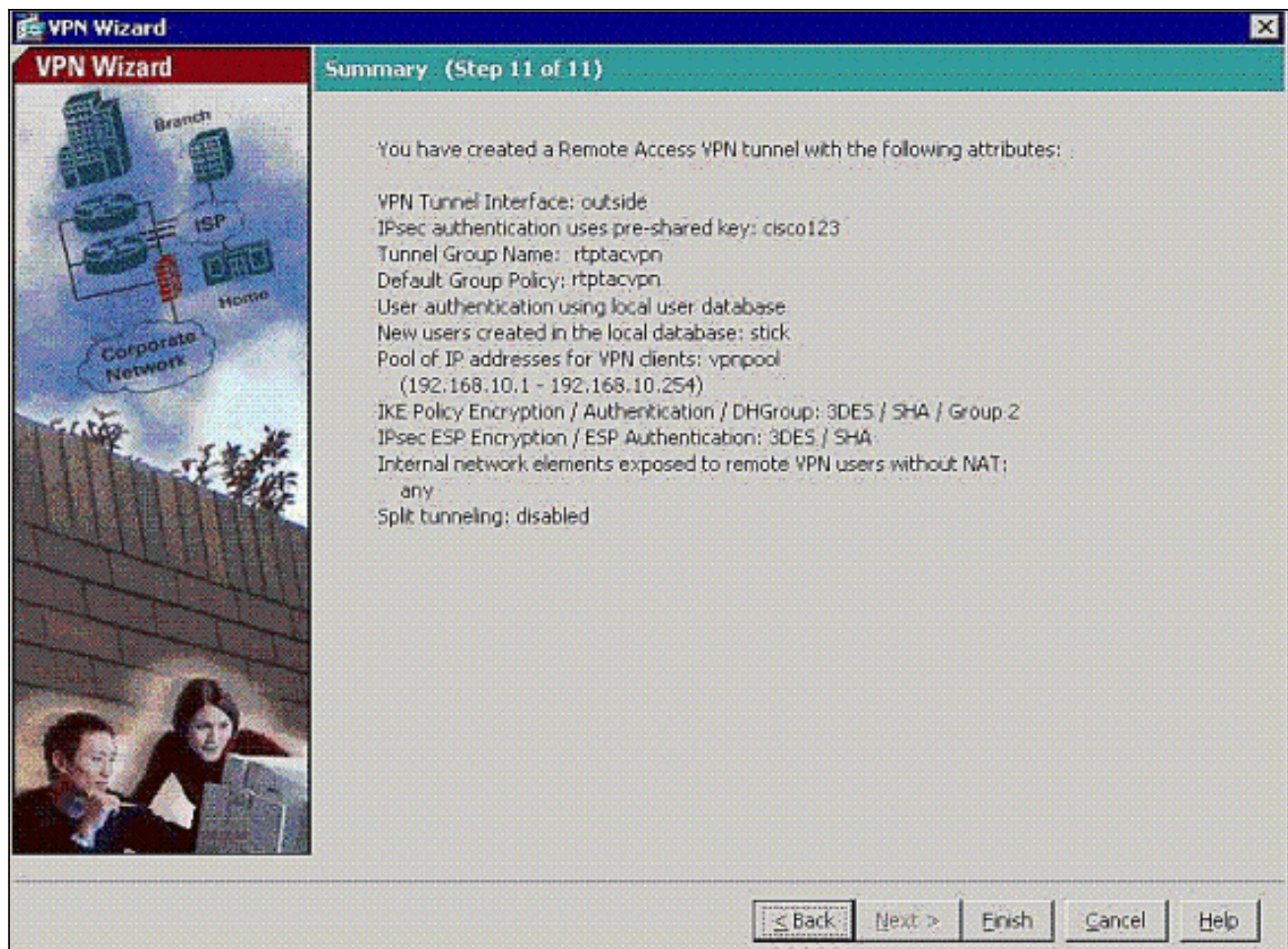
10. Specificeer de parameters voor IPSec, ook bekend als IKE fase 2. De configuraties aan beide zijden van de tunnel moeten precies overeenkomen, maar de Cisco VPN-client kiest automatisch de juiste configuratie voor zichzelf. Er is geen IKE-configuratie nodig op de client-pc.



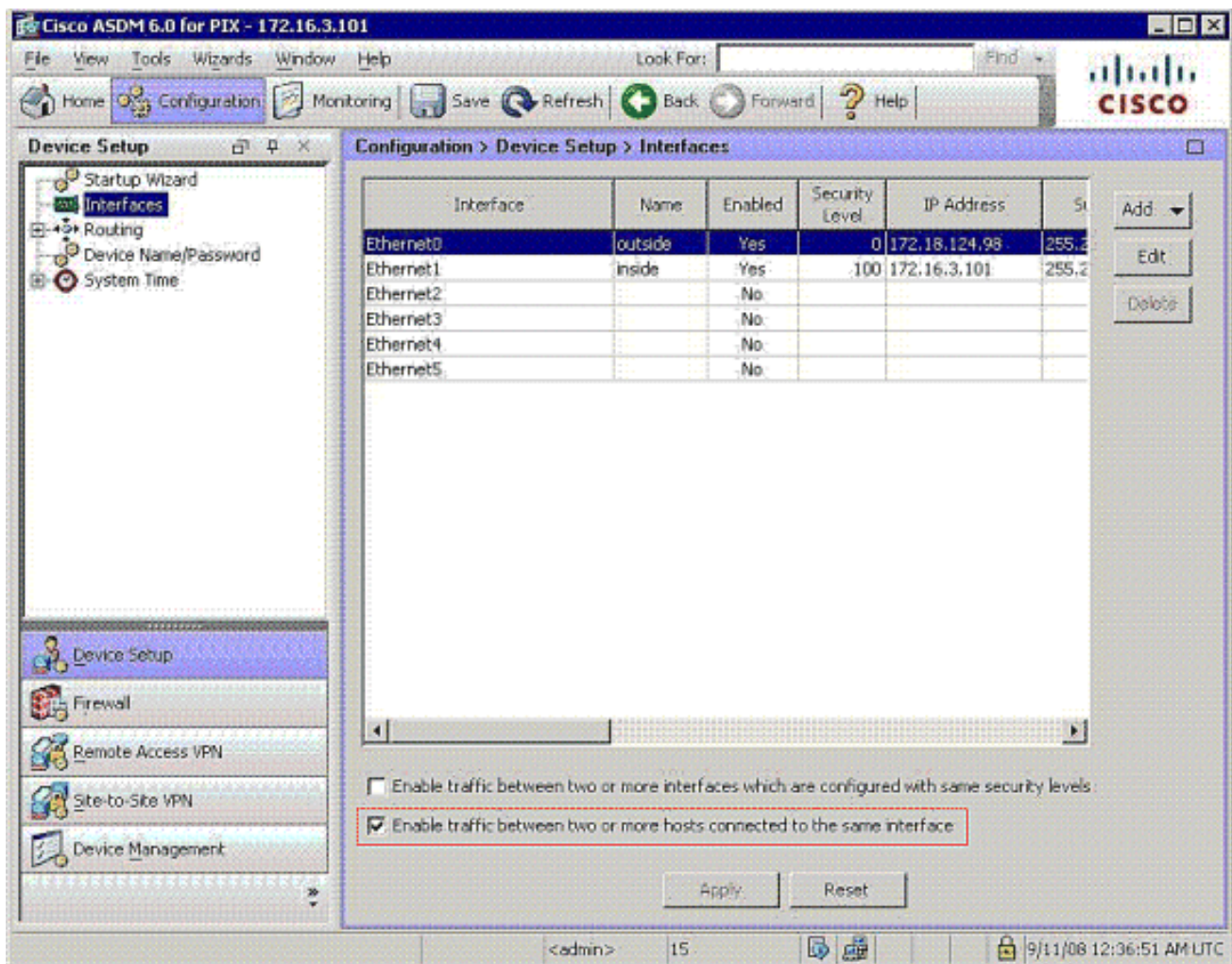
11. Specificeer welke, als om het even welke, interne hosts of netwerken kunnen worden blootgesteld aan externe VPN-gebruikers. Als u deze lijst leeg laat, staat het externe VPN-gebruikers toe om toegang te krijgen tot het gehele binnennetwerk van de ASA. U kunt ook gesplitste tunneling in dit venster inschakelen. Split-tunneling versleutelt het verkeer naar de bronnen die eerder in deze procedure zijn gedefinieerd en geeft onversleutelde toegang tot internet in het algemeen door dat verkeer niet uit te schakelen. Als gesplitste tunneling *niet* ingeschakeld is, wordt al het verkeer van externe VPN-gebruikers naar de ASA gekanaliseerd. Dit kan zeer bandbreedte en processor intensief worden, gebaseerd op uw configuratie.



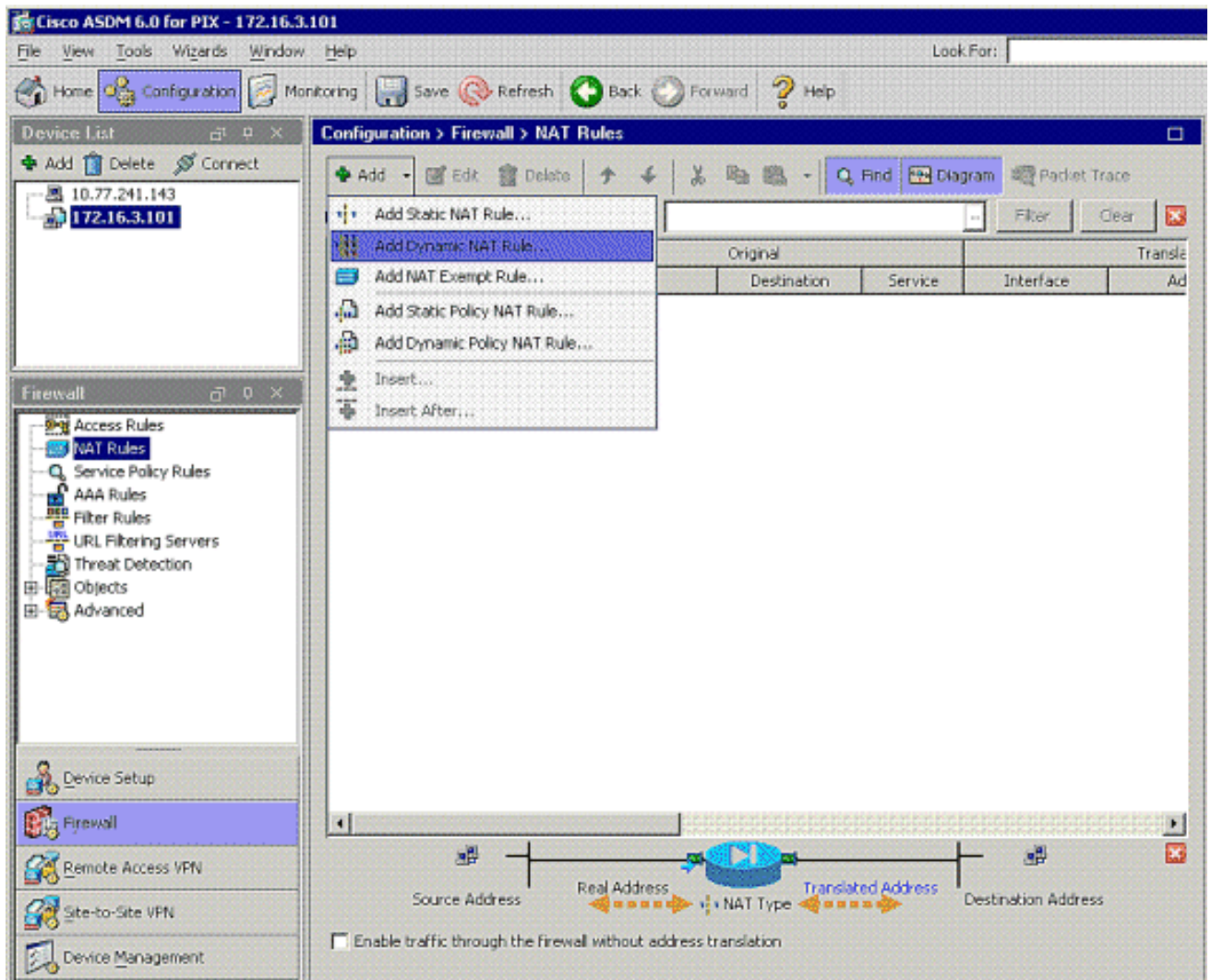
12. Dit venster geeft een samenvatting van de maatregelen die u hebt genomen. Klik op **Voltoeien** als u tevreden bent met de configuratie.



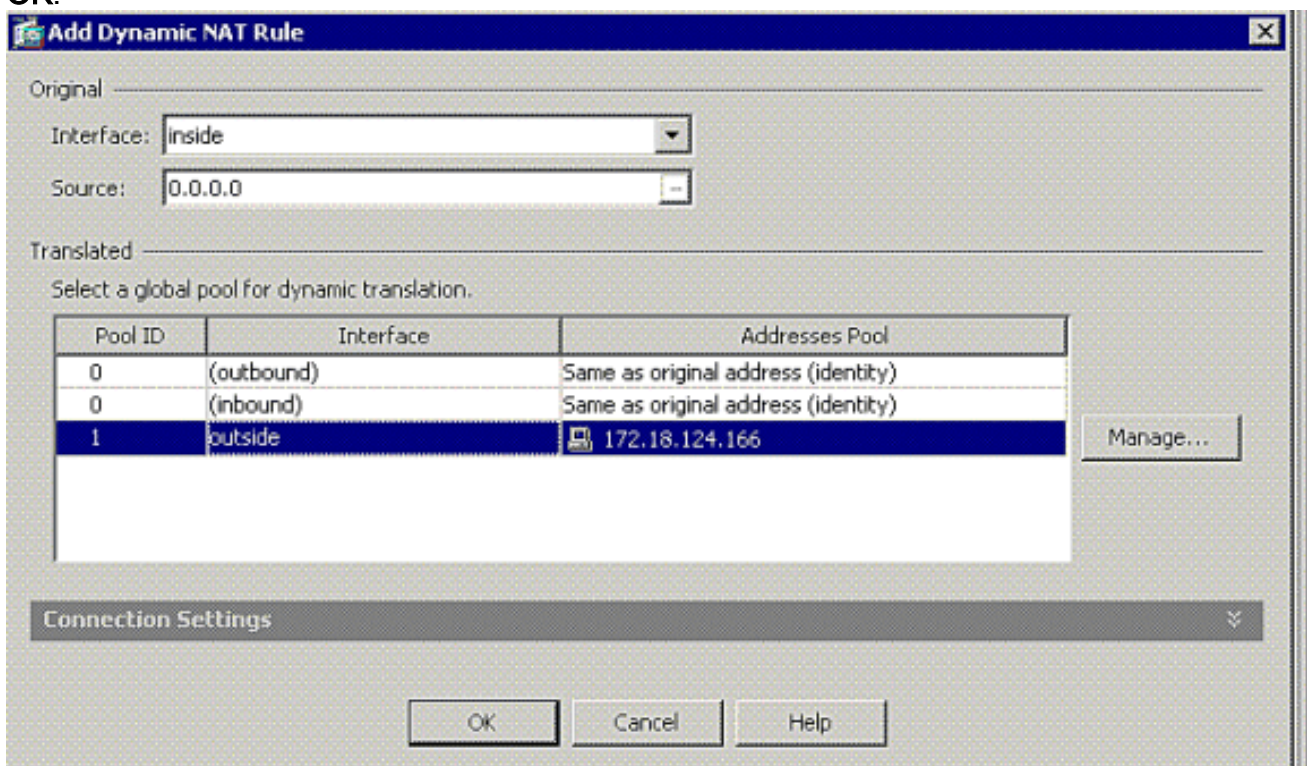
13. Configureer het commando **verkeer met dezelfde beveiliging** om verkeer mogelijk te maken tussen twee of meer hosts die met dezelfde interface zijn verbonden wanneer u op het selectieteken klikt zoals aangegeven in de afbeelding:



14. Kies **Configuratie > Firewall > NAT Regels** en klik op **Dynamische NAT Regel toevoegen** om deze dynamische vertaling met het gebruik van ASDM te maken.

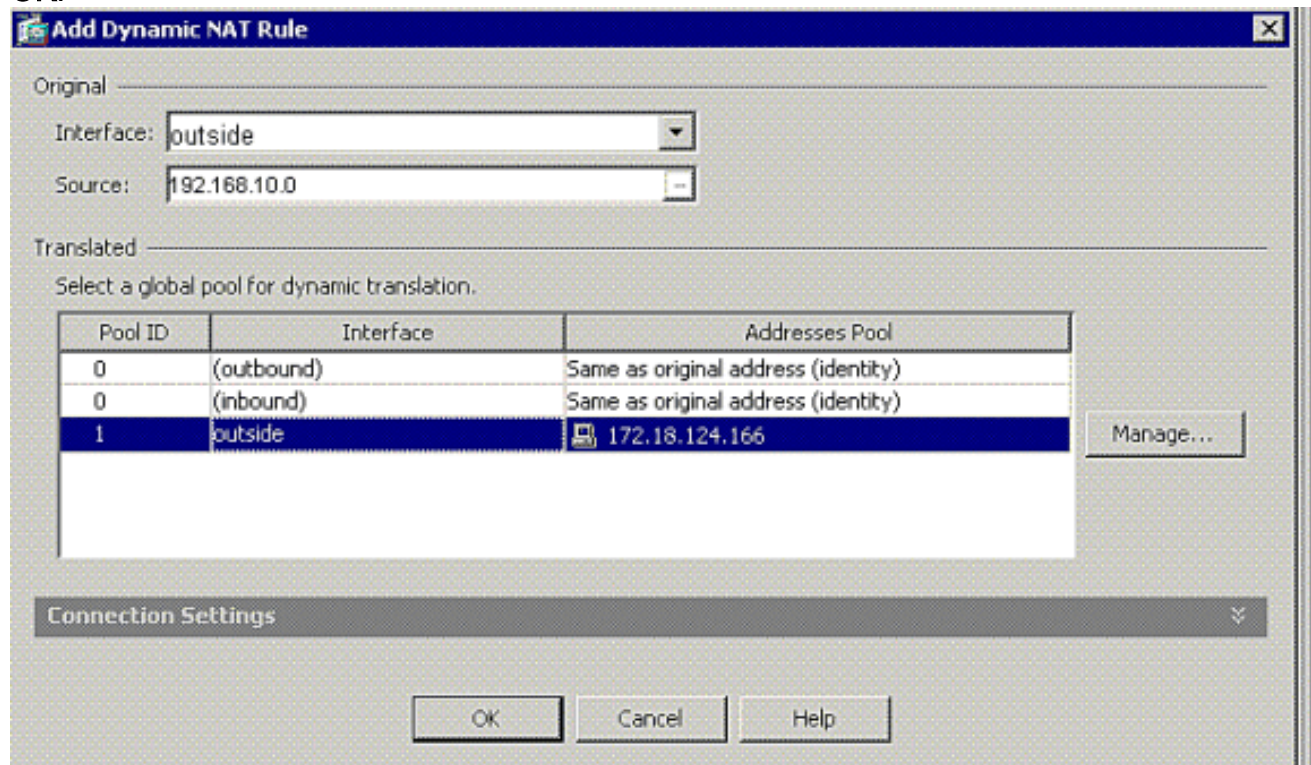


15. Kies **binnen** als de broninterface en voer de adressen in die u wilt NAT. Kies **buiten** voor het **vertaaladres** op de interface en klik op **OK**.

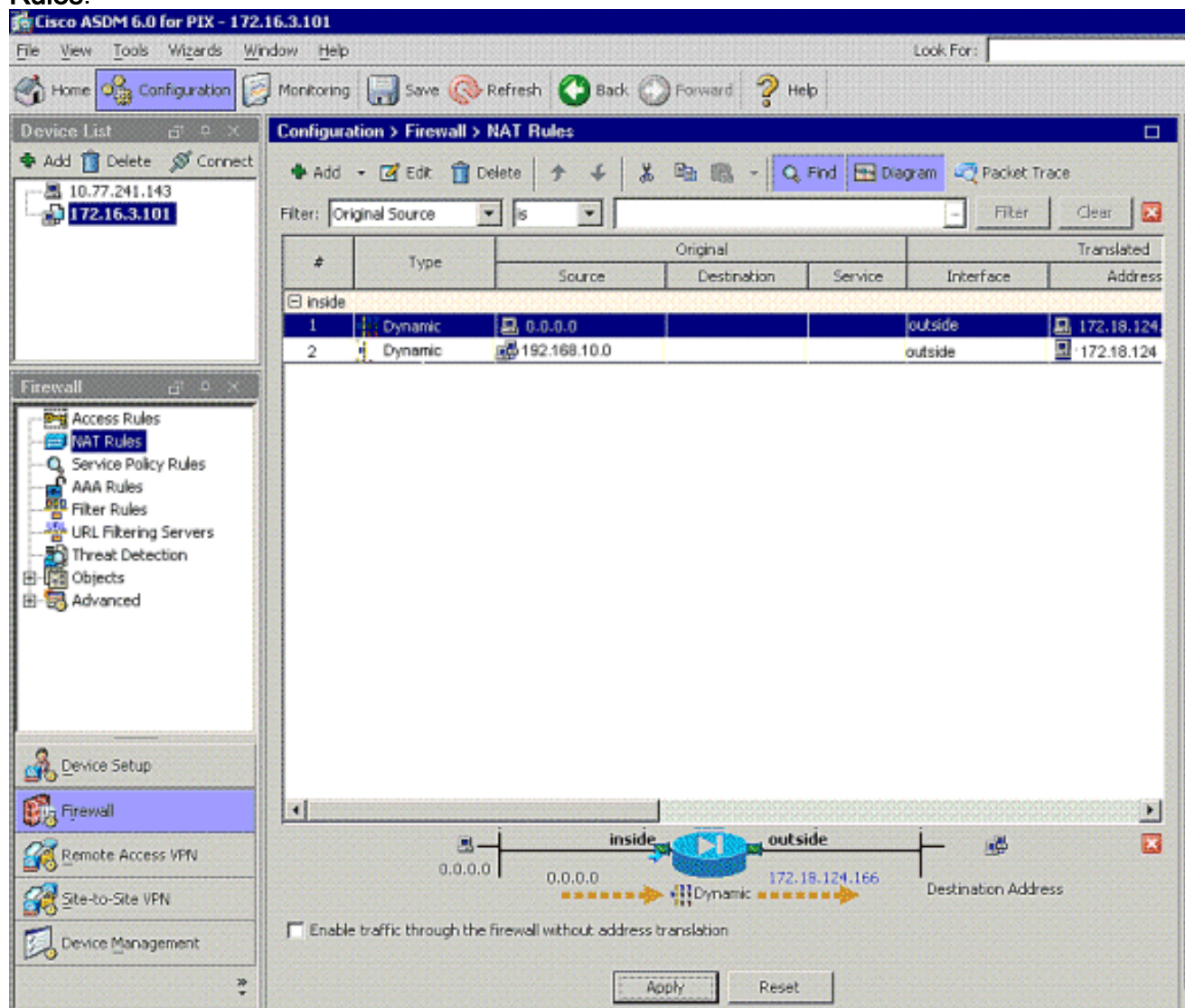


16. Kies **buiten** als de broninterface en voer de adressen in die u wilt NAT. Kies **buiten** voor het **vertaaladres** op de interface en klik op

OK.



17. De vertaling verschijnt in de vertaalregels bij **Configuration > Firewall > NAT Rules**.



Opmerking 1: De opdracht [voor de systeemverbinding](#) moet worden geconfigureerd. Het [tonen in werking stellen-enig systeem](#) bevel verifieert of het wordt gevormd.

Noot 2: Voeg deze output voor het optionele UDP transport toe:

```
group-policy clientgroup attributes vpn-idle-timeout 20  
ipsec-udp enable ipsec-udp-port 10000  
split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel
```

Noot 3: Configureer deze opdracht in de mondiale configuratie van het PIX-apparaat zodat VPN-clients via IPsec over TCP kunnen worden aangesloten:

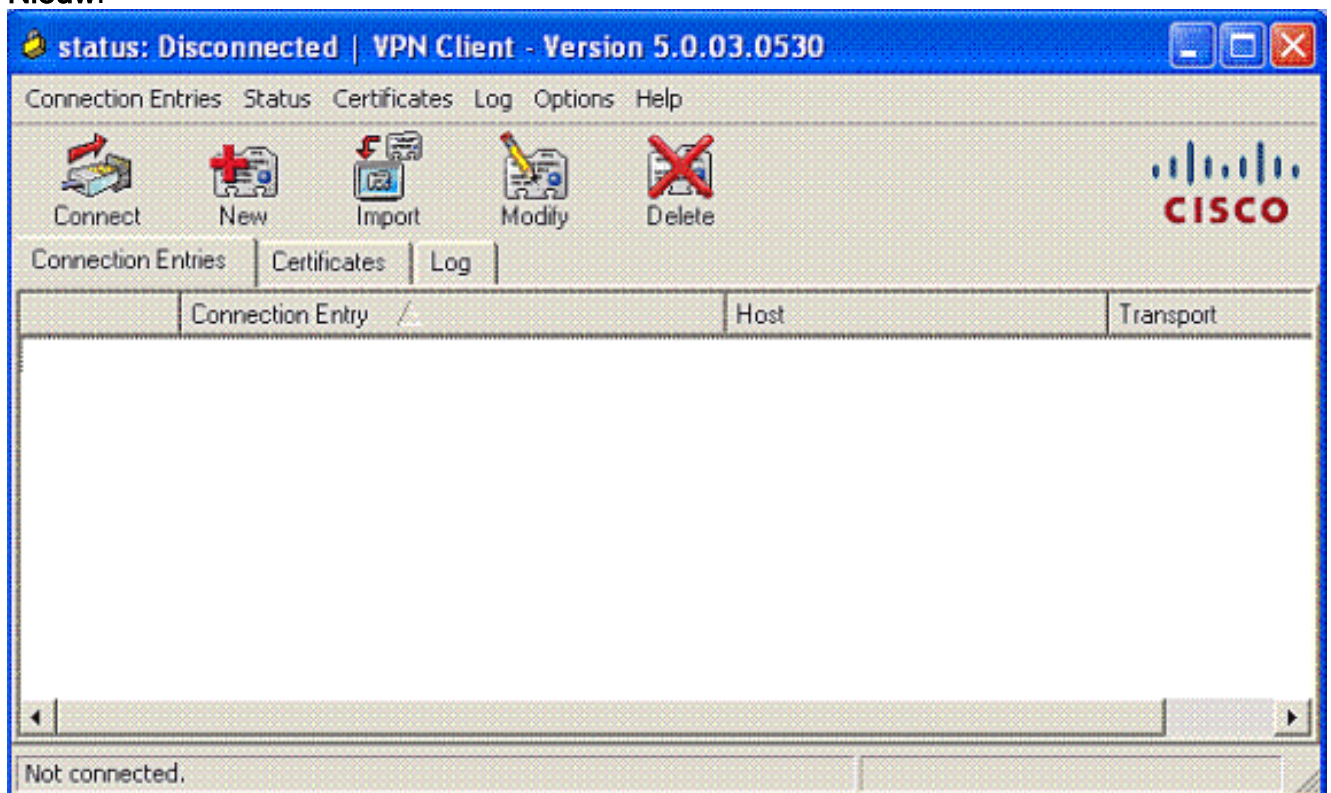
```
isakmp ipsec-over-tcp port 10000
```

Opmerking: Raadpleeg het [Hair-Pinning op Cisco ASA](#) -video voor meer informatie over verschillende scenario's waar haarspelden kunnen worden gebruikt.

VPN-clientconfiguratie

Volg deze stappen om de VPN-client te configureren:

1. Kies **Nieuw**.




2. Voer de PIX-externe interface-ip-adres en tunnelgroepnaam in samen met het wachtwoord voor

VPN Client | Create New VPN Connection Entry

Connection Entry:

Description:

Host:



Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name:

Password:

Confirm Password:

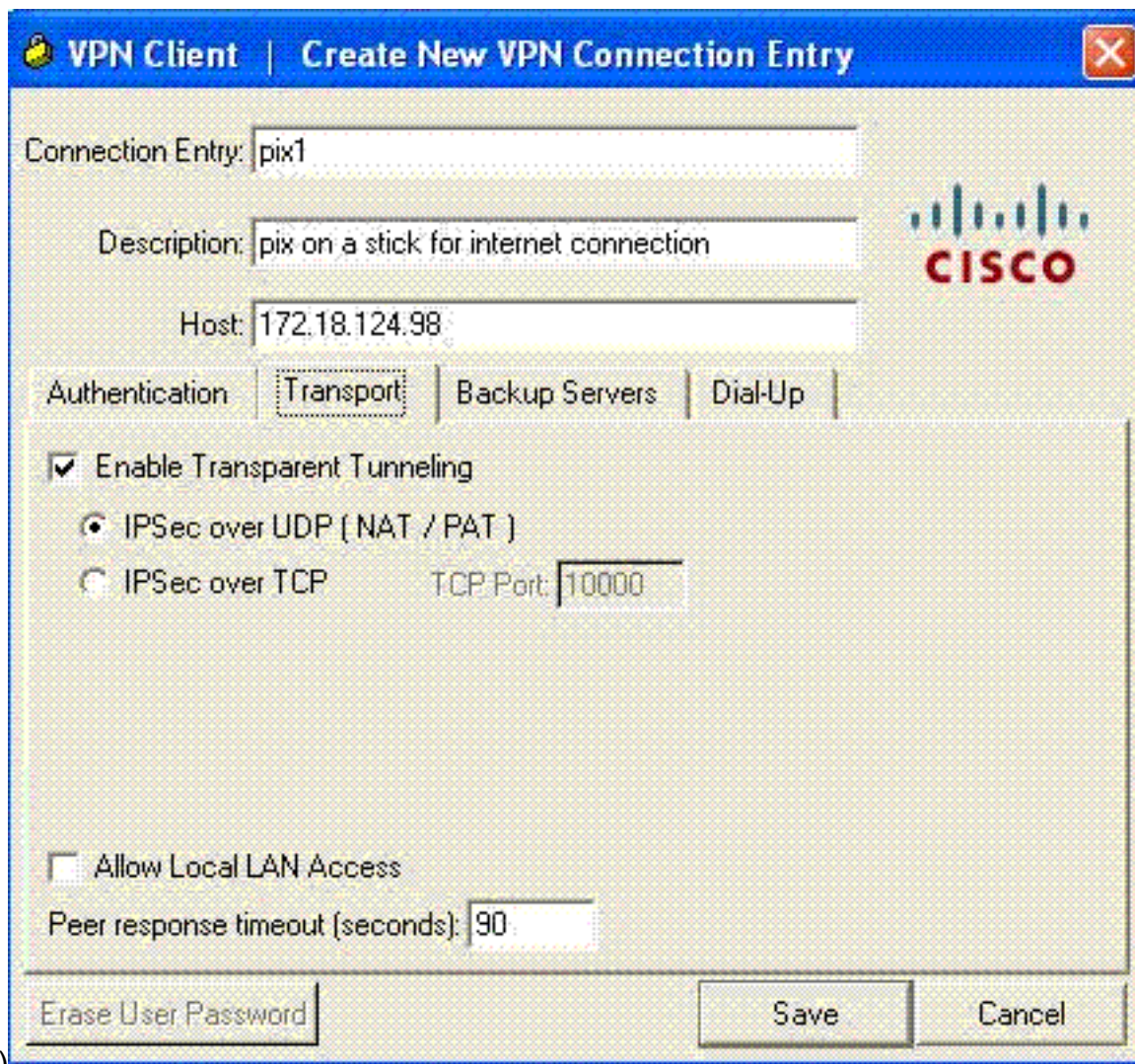
Certificate Authentication

Name:

Send CA Certificate Chain

verificatie.

3. (Optioneel) Klik op **Transparent Tunneling** inschakelen onder het tabblad Transport. (Dit is optioneel en vereist de extra PIX/ASA-configuratie die in [aantekening 2](#) is



vermeld.)

4. Het profiel opslaan.

Verifiëren

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

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

- [toon crypto isakmp sa](#)-Toont alle huidige IKE security associaties (SAs) bij een peer.
- [Laat crypto ipsec sa](#)-displays alle huidige SA's zien. Zoek naar encryptie en decrypteer pakketten op de SA die het verkeer van de VPN client bepalen.

Probeer aan een openbaar IP-adres van de client te pingelen of te bladeren (bijvoorbeeld www.cisco.com).

Opmerking: De interne interface van de PIX kan niet worden ingesloten voor de samenstelling van een tunnel tenzij de [opdracht beheertoegang](#) is ingesteld in de wereldwijde bevestigingsmodus.

```
PIX1(config)#management-access inside
PIX1(config)#show management-access
```

```
management-access inside
```

[VPN-clientverificatie](#)

Voltooi deze stappen om de VPN-client te controleren.

1. Klik met de rechtermuisknop op het pictogram van het clientslot van VPN dat aanwezig is in het systeemvak na een succesvolle verbinding en kies de optie voor **statistieken** om versleutelingen en decrypts te bekijken.
2. Klik op het tabblad Route Details om de niet-gesplitste tunnellijst van het apparaat te controleren.

[Problemen oplossen](#)

N.B.: Raadpleeg voor meer informatie over hoe u problemen met VPN-problemen kunt oplossen [VPN-oplossingen voor probleemoplossing](#).

[Gerelateerde informatie](#)

- [Enhanced Spoke-to-Client VPN-configuratievoorbeeld voor PIX security applicatie versie 7.0](#)
- [Cisco VPN-client](#)
- [IPsec-onderhandeling/IKE-protocollen](#)
- [Cisco PIX-firewallsoftware](#)
- [Opdrachtreferenties van Cisco Secure PIX-firewall](#)
- [Security meldingen uit het veld \(inclusief PIX\)](#)
- [Hair-draaien op Cisco ASA](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)