# L2TP-over-IPsec configureren tussen Windows 8 PC en ASA met behulp van een vooraf gedeelde toets

## Inhoud



## Inleiding

Dit document beschrijft hoe u Layer 2 Tunneling Protocol (L2TP) via IPsec kunt configureren met behulp van een vooraf gedeelde sleutel tussen Cisco adaptieve security applicatie (ASA) en Windows 8 native client.

L2TP via Internet Protocol security (IPsec) biedt de mogelijkheid om een L2TP Virtual Private Network (VPN)-oplossing in te stellen en te beheren naast IPsec VPN en firewallservices in één platform.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- IP-connectiviteit van de clientmachine naar de ASA. Probeer om connectiviteit te testen, het

IP adres van de ASA van client eindpunt en vice versa te pingelen
- Zorg ervoor dat het protocol UDP Port 500 en 4500 en Encapsulation Security Payload (ESP) niet ergens langs het pad van de verbinding is geblokkeerd

## Beperkingen

- L2TP via IPsec ondersteunt alleen IKEv1. IKEv2 wordt niet ondersteund.
- L2TP met IPsec op de ASA stelt LNS in staat om te samenwerken met native VPN-clients die in dergelijke besturingssystemen zijn geïntegreerd, zoals Windows, MAC OS X, Android en Cisco IOS. Alleen L2TP met IPsec wordt ondersteund. native L2TP zelf wordt niet ondersteund op ASA.
- De minimale levensduur van IPsec, ondersteund door de Windows client, is 300 seconden. Als de levensduur van de ASA minder dan 300 seconden bedraagt, negeert de Windows client het en vervangt het door een 300 seconden durende levensduur.
- ASA ondersteunt alleen het Point-to-Point Protocol (PPP)-authenticaties met wachtwoordverificatie (PAP) en Microsoft Challenge-Handshake Authentication Protocol (CHAP), versies 1 en 2, op de lokale database. Extensible Authentication Protocol (EAP) en CHAP worden uitgevoerd door proxyverificatieservers. Daarom, als een externe gebruiker tot een tunnelgroep behoort die met de opdrachten **authenticatie-proxy** of **authenticatieschap** wordt ingesteld, en de ASA is ingesteld om de lokale database te gebruiken, kan die gebruiker geen verbinding maken.

Ondersteunde PPP-verificatietypen

L2TP-over-IPsec-verbindingen op ASA ondersteunen alleen de PPP-authenticatietypen die in Tabel worden getoond

*AAA-serverondersteuning en PPP-verificatietypen*

| AAA-servertype | Ondersteunde PPP-verificatietypen |
|---|---|
| LOKAAL | PAP, MSCHAPv1, MSCHAPv2 |
| RADIUS | PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-Proxy |
| TACACS+ | PAP, CHAP, MSCHAPv1 |
| LDAP | PAP |
| NT | PAP |
| Kerberos | PAP |
| SDI | SDI |

Kenmerken PPP-verificatie

| sleutelwoord | Verificatietype | Kenmerken |
|---|---|---|
| **ketting** | CHAP | In antwoord op de serveruitdaging geeft de client de gecodeerde [uitdagin plus wachtwoord] terug met een duidelijke gebruikersnaam. Dit protocol veiliger dan de PAP, maar gegevens worden niet versleuteld. |
| **eap-proxy** | MAART | Hiermee kan EAP worden ingevoerd, waarmee het beveiligingsapparaat h PPP-verificatieproces kan aanpassen aan een externe RADIUS verificatieserver. |
| **ms-chap-v1** | Microsoft CHAP, versie 1 | Gelijkaardig aan CHAP maar veiliger in dat de server slechts gecodeerd wachtwoorden opslaat en vergelijkt in plaats van duidelijke tekstwachtwoorde |
| **ms-chap-v2** | Microsoft CHAP, versie 2 | zoals in CHAP. Dit protocol genereert ook een sleutel voor gegevenscoderin door MPPE. |

| | | |
|---|---|---|
| **pap** | PAP | Duidelijke tekstgebruikersnaam en wachtwoord tijdens verificatie en is ni veilig. |

### Gebruikte componenten

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

- Cisco 5515 Series ASA die versie 9.4(1) van de software uitvoert
- L2TP/IPSec-client (Windows 8)

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

### Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco ASA 5500 Series security applicatie 8.3(1) of hoger.

### Conventies

Raadpleeg de technische Tips van Cisco voor meer informatie over documentconventies

## Achtergrondinformatie

Layer 2 Tunneling Protocol (L2TP) is een VPN-tunneling-protocol dat externe klanten toestaat om het openbare IP-netwerk te gebruiken om veilig met privé-netwerkservers te communiceren. L2TP gebruikt PPP over UDP (poort 1701) om de gegevens te tunnen.

L2TP-protocol is gebaseerd op het client/server-model. De functie is verdeeld tussen de L2TP-netwerkserver (LNS) en de L2TP-toegangscentrator (LAC). LNS loopt in dit geval doorgaans op een netwerkgateway zoals de ASA, terwijl de LAC een inbelnetwerktoegangsserver (NAS) of een endpointapparaat met een gebundelde L2TP-client zoals Microsoft Windows, Apple iPhone of Android kan zijn.

## Configureren

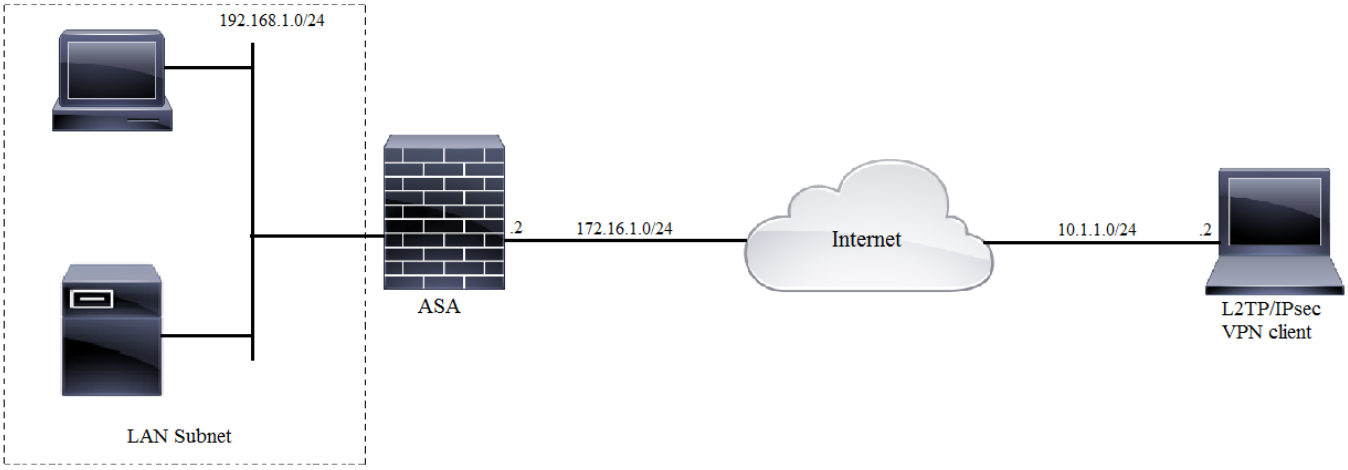
Deze sectie wordt weergegeven met informatie over het configureren van de functies die in dit document worden beschreven.

> Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

> 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 zijn

gebruikt.

## Netwerkdiagram

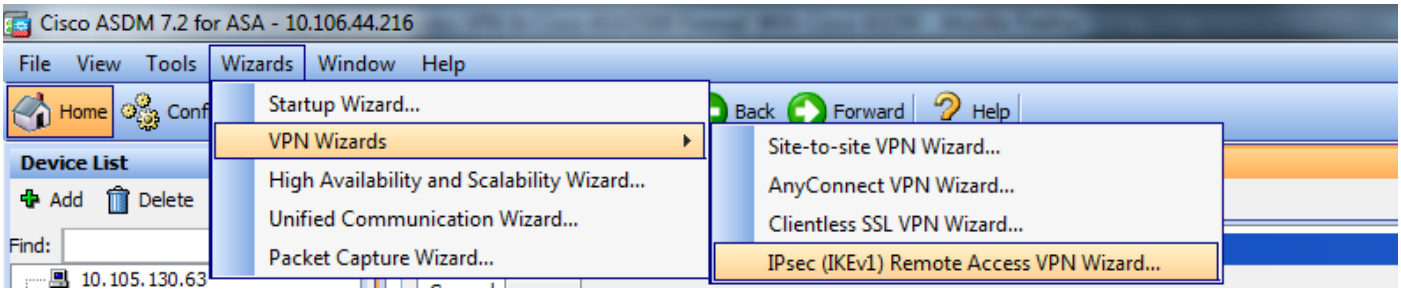



## Volledig tunnelconfiguratie

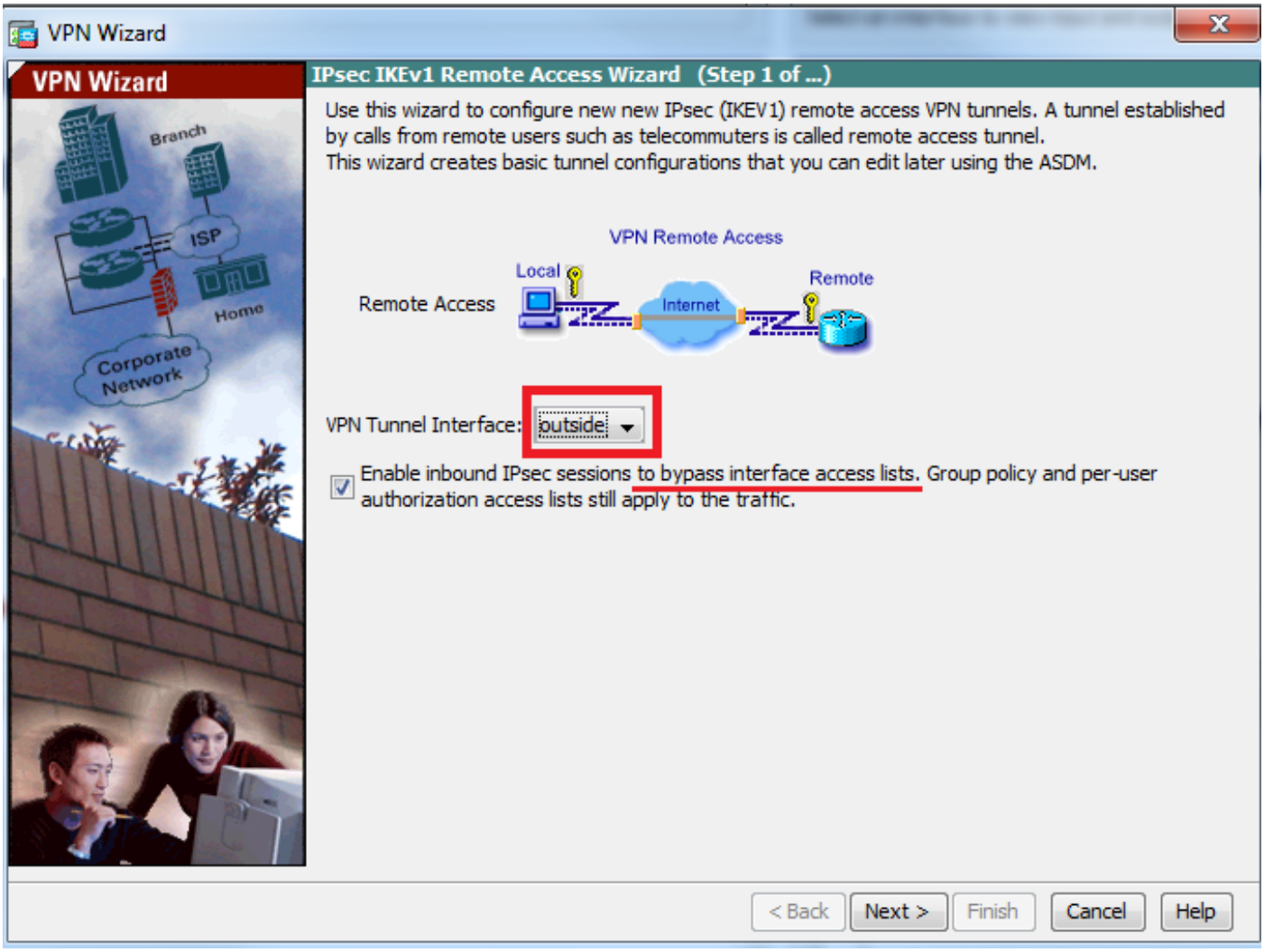
### ASA-configuratie met adaptieve security apparaatbeheer (ASDM)

Voer de volgende stappen uit:

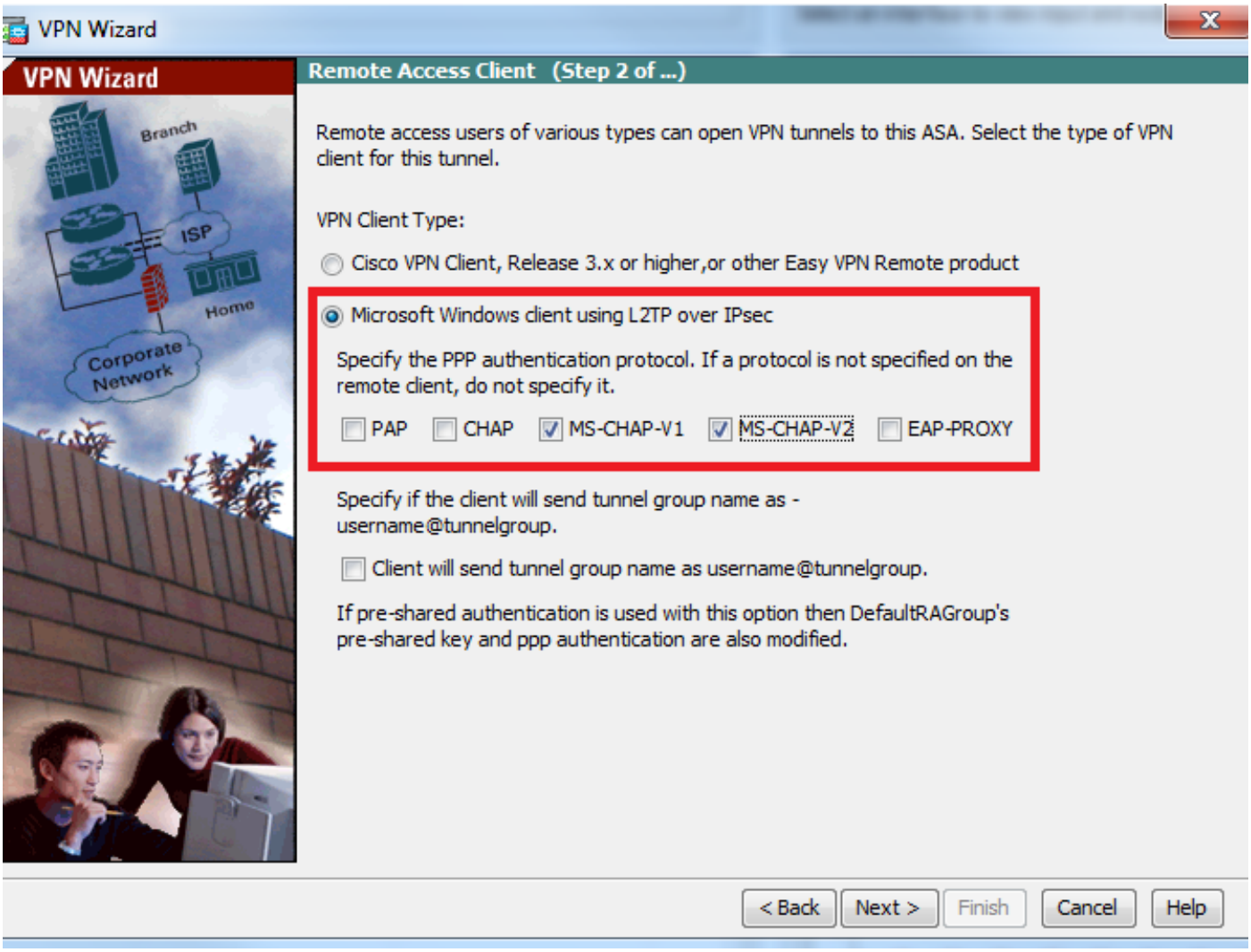
Stap 1. Meld u aan bij ASDM en navigeer naar **Wizard > VPN-wizard > IPsec (IKEv1) externe VPN-toegangswizard**.



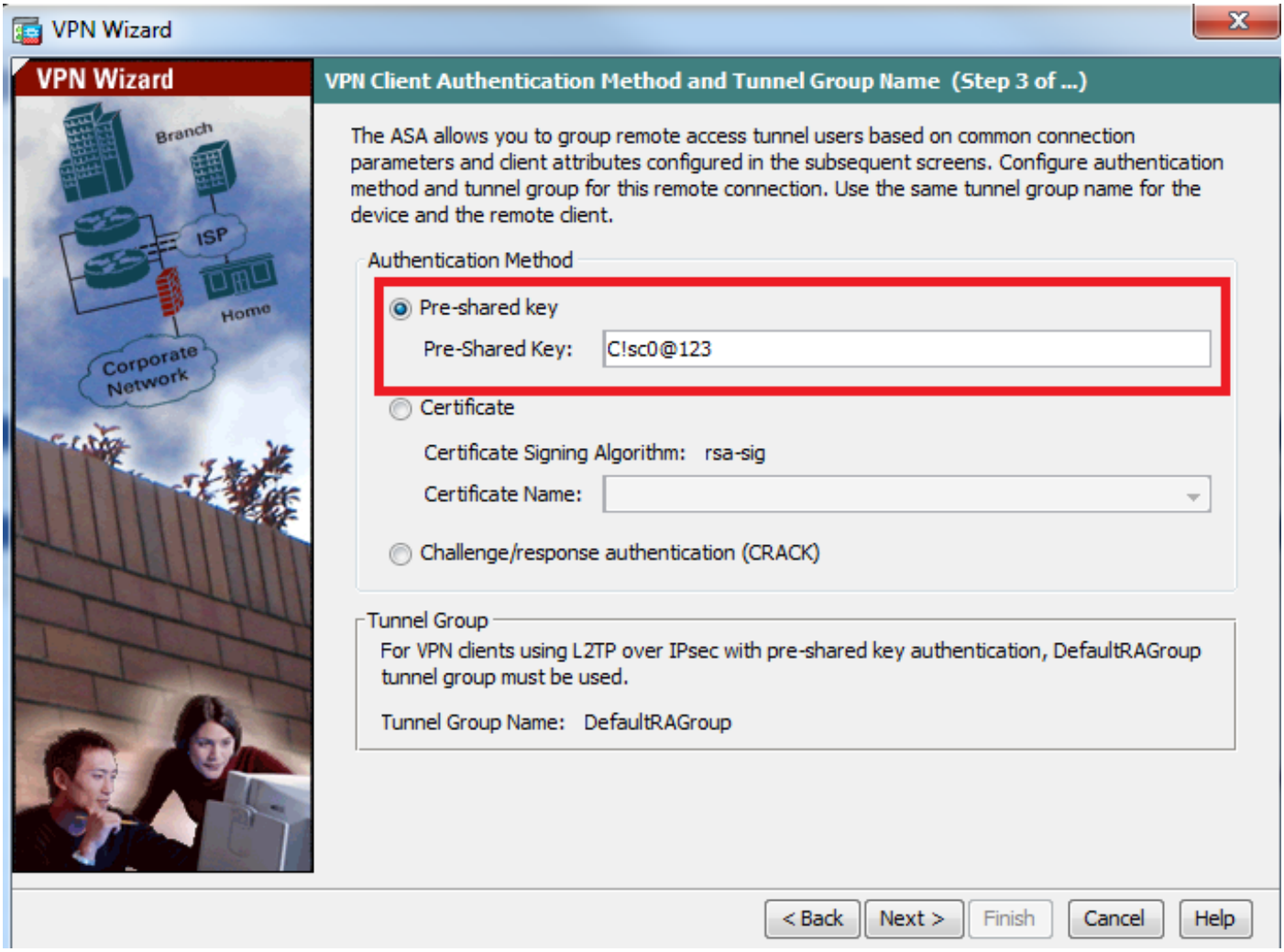

Stap 2. Er verschijnt een setup-venster voor externe toegang VPN. Kies in de vervolgkeuzelijst de interface waarop de VPN-tunnel moet worden afgesloten. In dit voorbeeld wordt de externe interface aangesloten op WAN en zo wordt de tunnels van VPN op deze interface beëindigd. Bewaar het vakje **Toegang van inkomende IPSec sessies om interfacetoegang te omzeilen. Groepsbeleid en toegangslijsten per gebruiker zijn nog steeds van toepassing op het** gecontroleerde **verkeer** zodat de nieuwe toegangslijst niet op externe interface hoeft te worden geconfigureerd om de klanten toegang te geven tot interne bronnen. Klik op **Volgende**.




Stap 3. Zoals in deze afbeelding wordt getoond, kiest u het clienttype als **Microsoft Windows-client met gebruik van L2TP via IPSec** en **MS-CHAP-V1** en **MS-CHAP-V2** als PPP-verificatieprotocol omdat PAP niet veilig is en andere verificatietypen niet worden ondersteund met een LOCAL-database als verificatieserver en klik op **Next**.

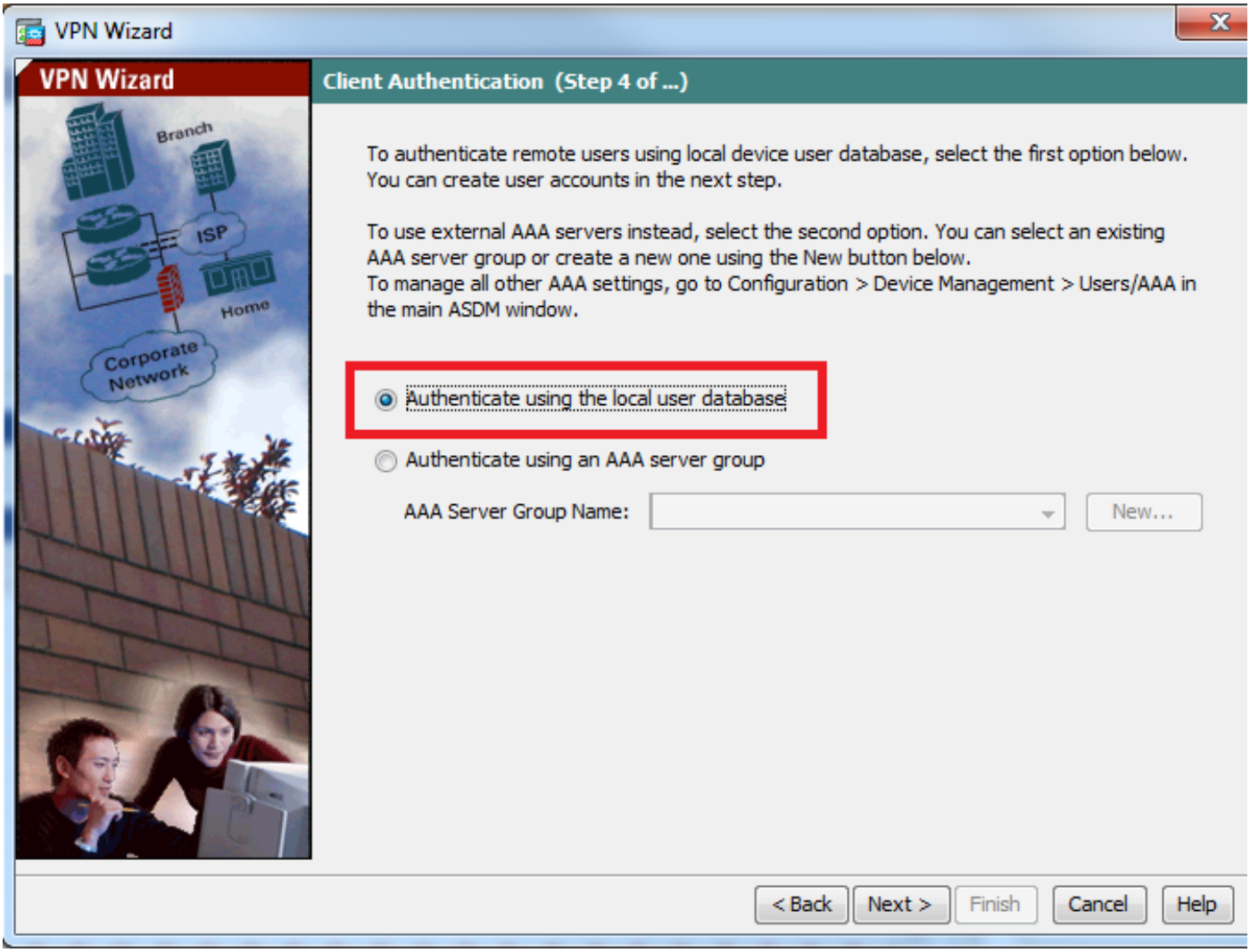



Stap 4. Kies de verificatiemethode als **Pre-gedeeld-toets** en type de vooraf gedeelde-toets die ook aan de clientkant moet staan en klik op **Volgende**, zoals in deze afbeelding.

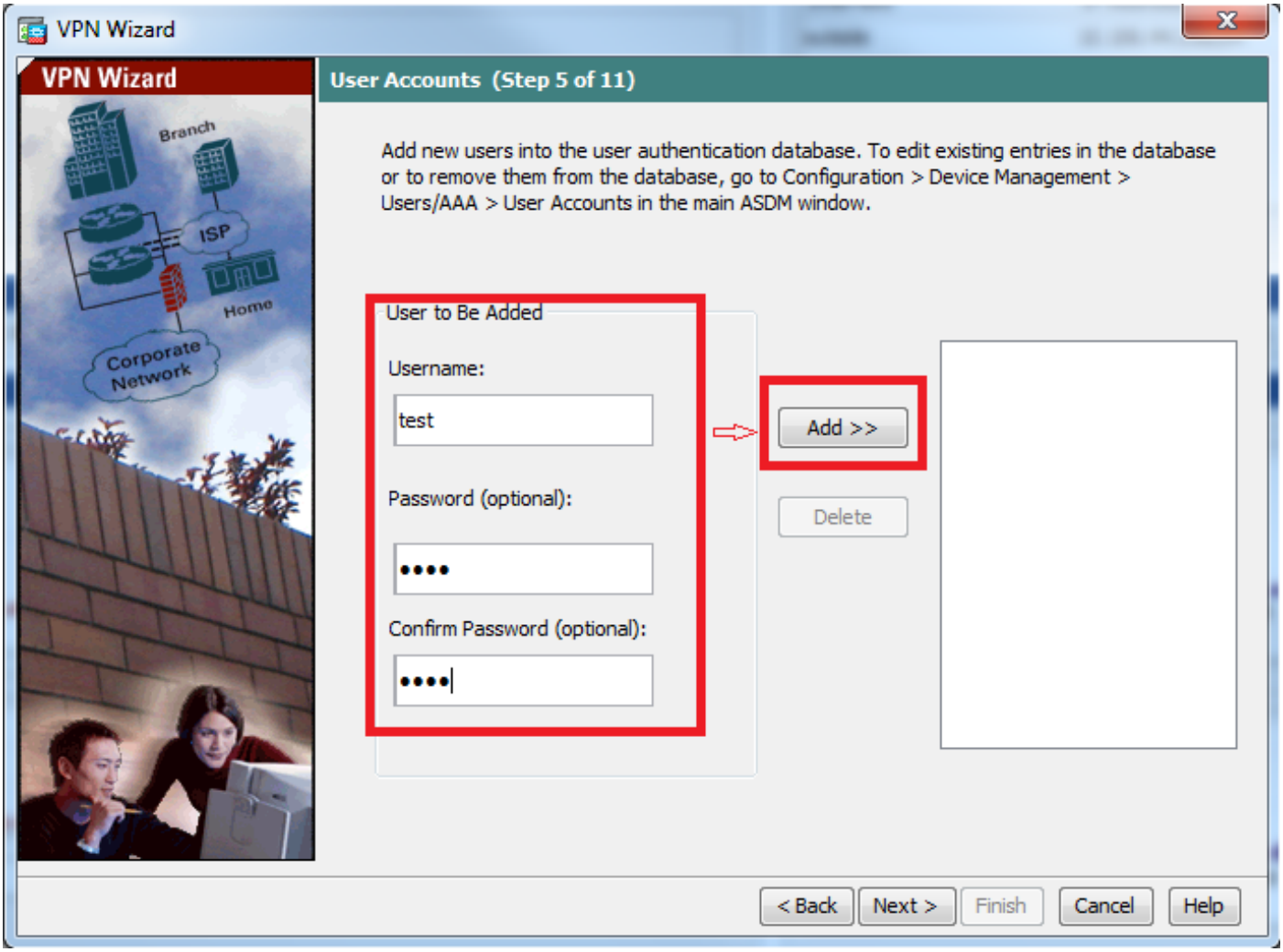



Stap 5. Specificeer een methode om gebruikers die L2TP via IPsec-verbindingen proberen te authenticeren. Ofwel kan een externe AAA-verificatieserver of zijn eigen lokale database worden gebruikt. Kies **Authenticate aan het gebruik van de lokale gebruikersdatabase** als u de clients wilt authenticeren tegen de lokale database van ASA en klik op **Volgende.**

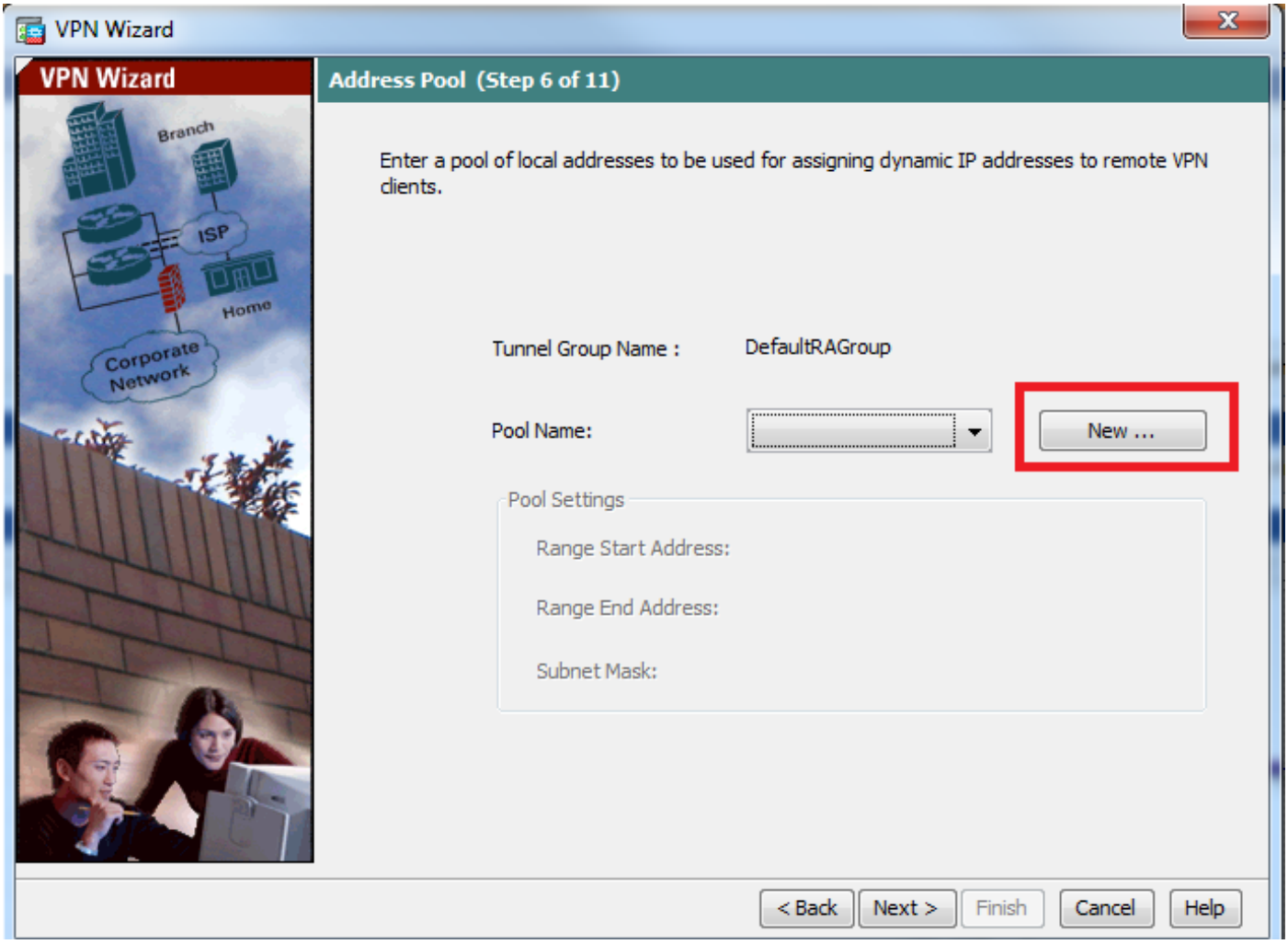
> Opmerking: Raadpleeg RADIUS-verificatie instellen voor VPN-gebruikers om de gebruikers te controleren met behulp van een externe AAA-server.




Stap 6. Om nieuwe gebruikers aan de lokale database voor gebruikersverificatie toe te voegen, voert u de gebruikersnaam en het wachtwoord in en klikt u vervolgens op **ADD** of anders kunnen bestaande gebruikersaccounts in de database worden gebruikt, zoals in deze afbeelding. Klik op **Volgende.**

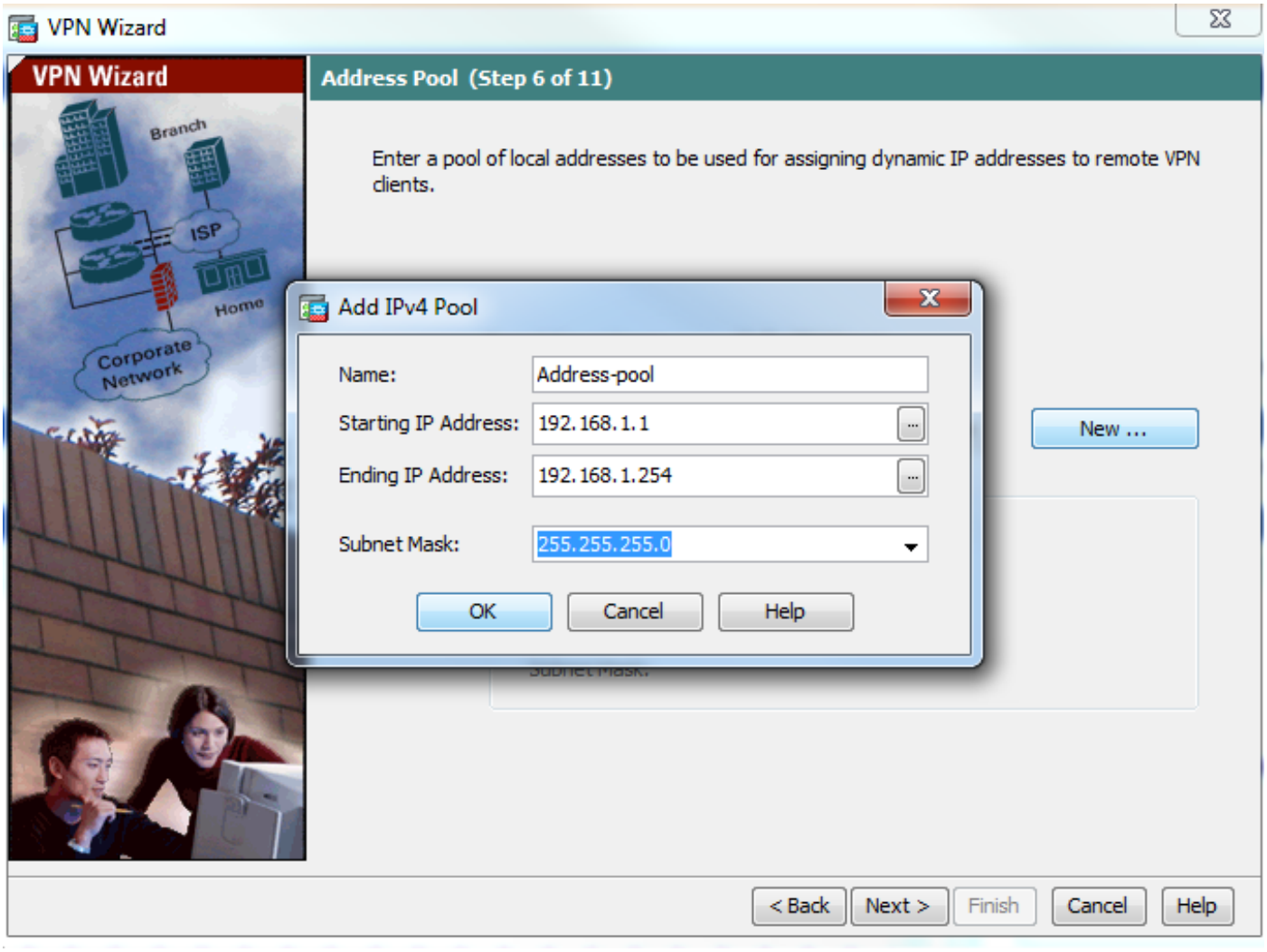



Stap 7. Kies in de vervolgkeuzelijst de adrestoewijzing die moet worden gebruikt voor de toewijzing van IP-adres aan de klanten. Om een nieuwe adrepool te maken, klikt u op **Nieuw** zoals in deze afbeelding.

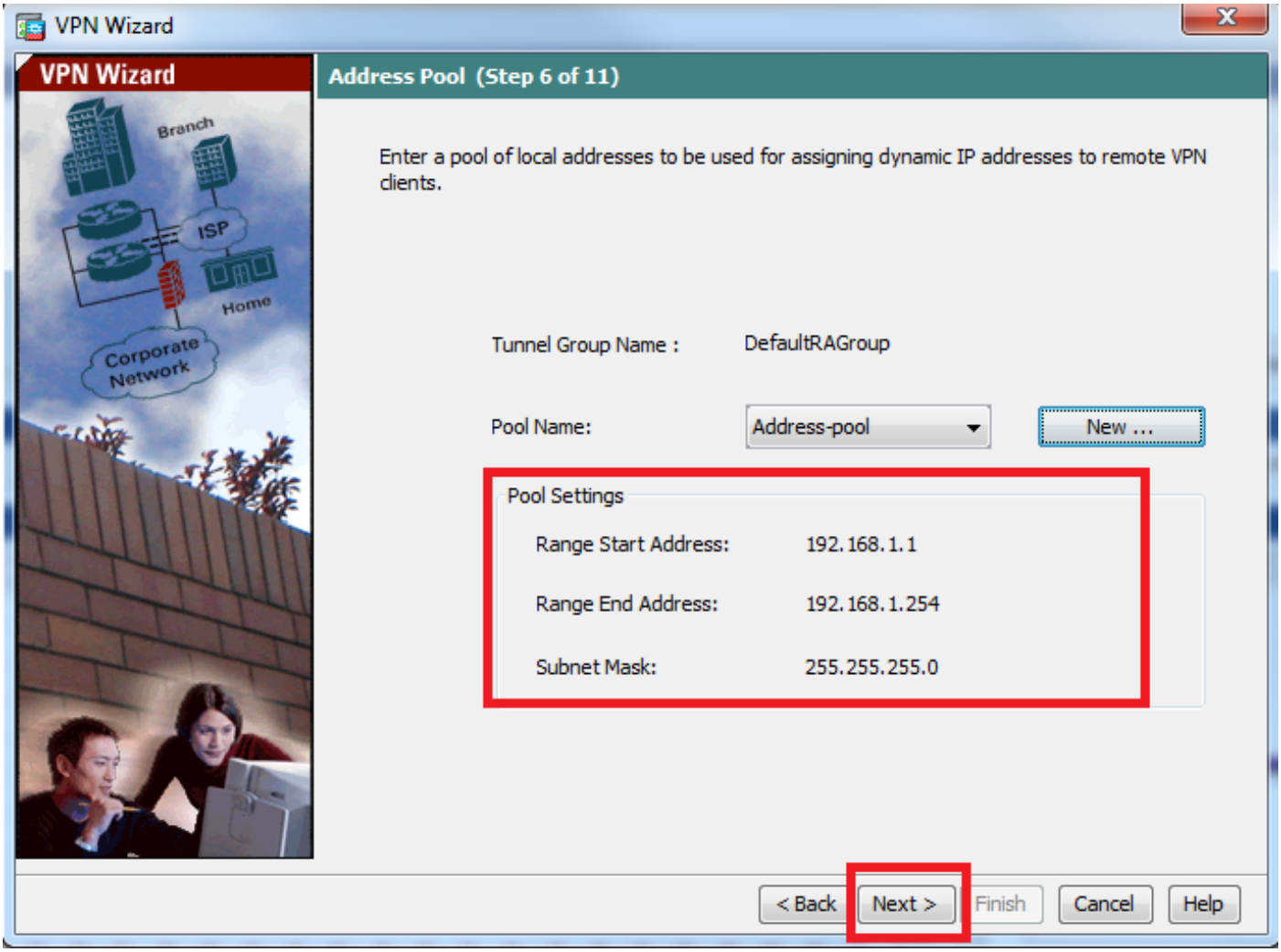



Stap 8. Het dialoogvenster **Add IPv4 Pool** verschijnt.

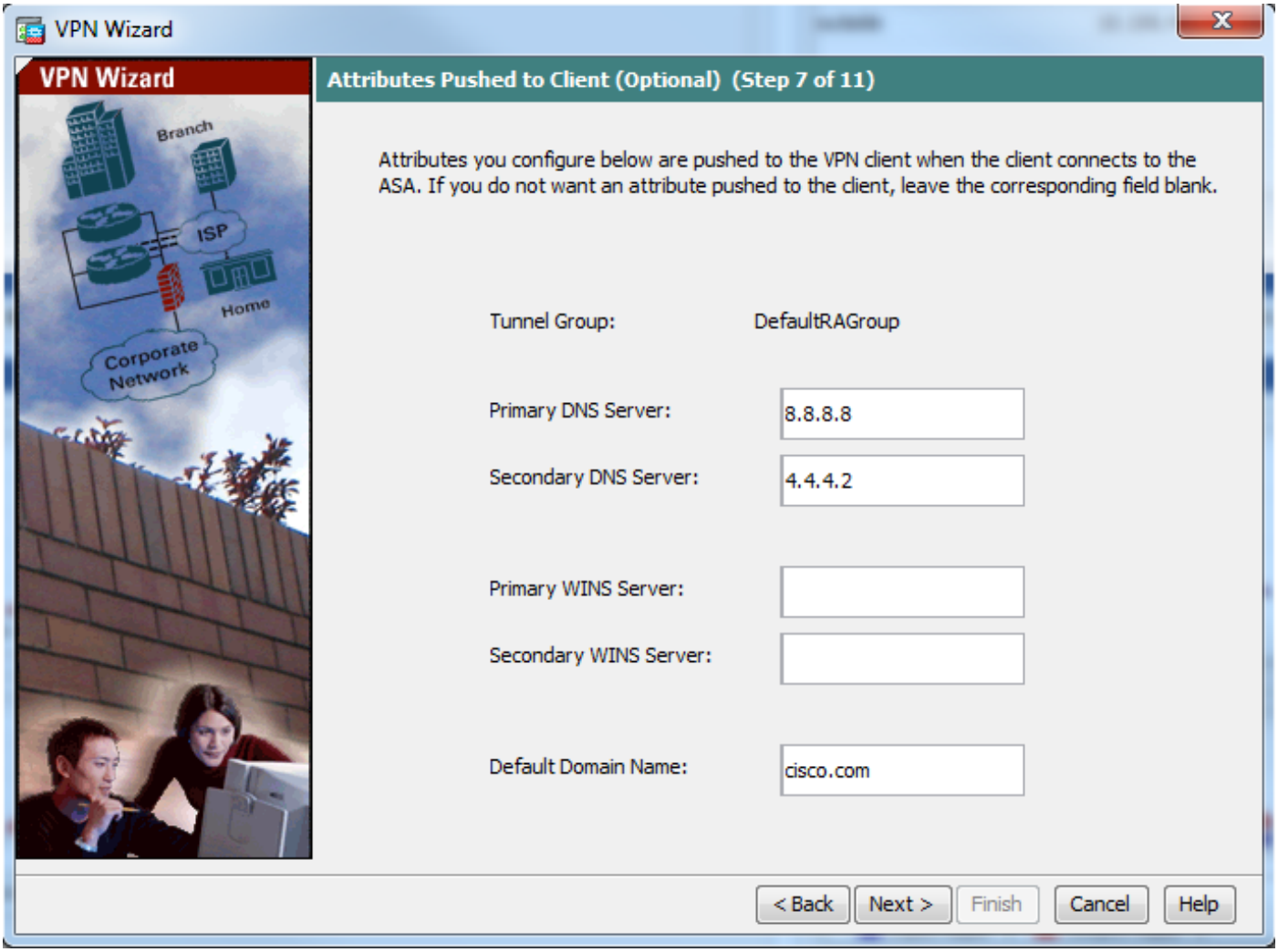
1. Voer de naam van de nieuwe IP-adrespool in.
2. Voer de begin- en eindadressen in.
3. Voer het subnetmasker in en klik op **OK**.



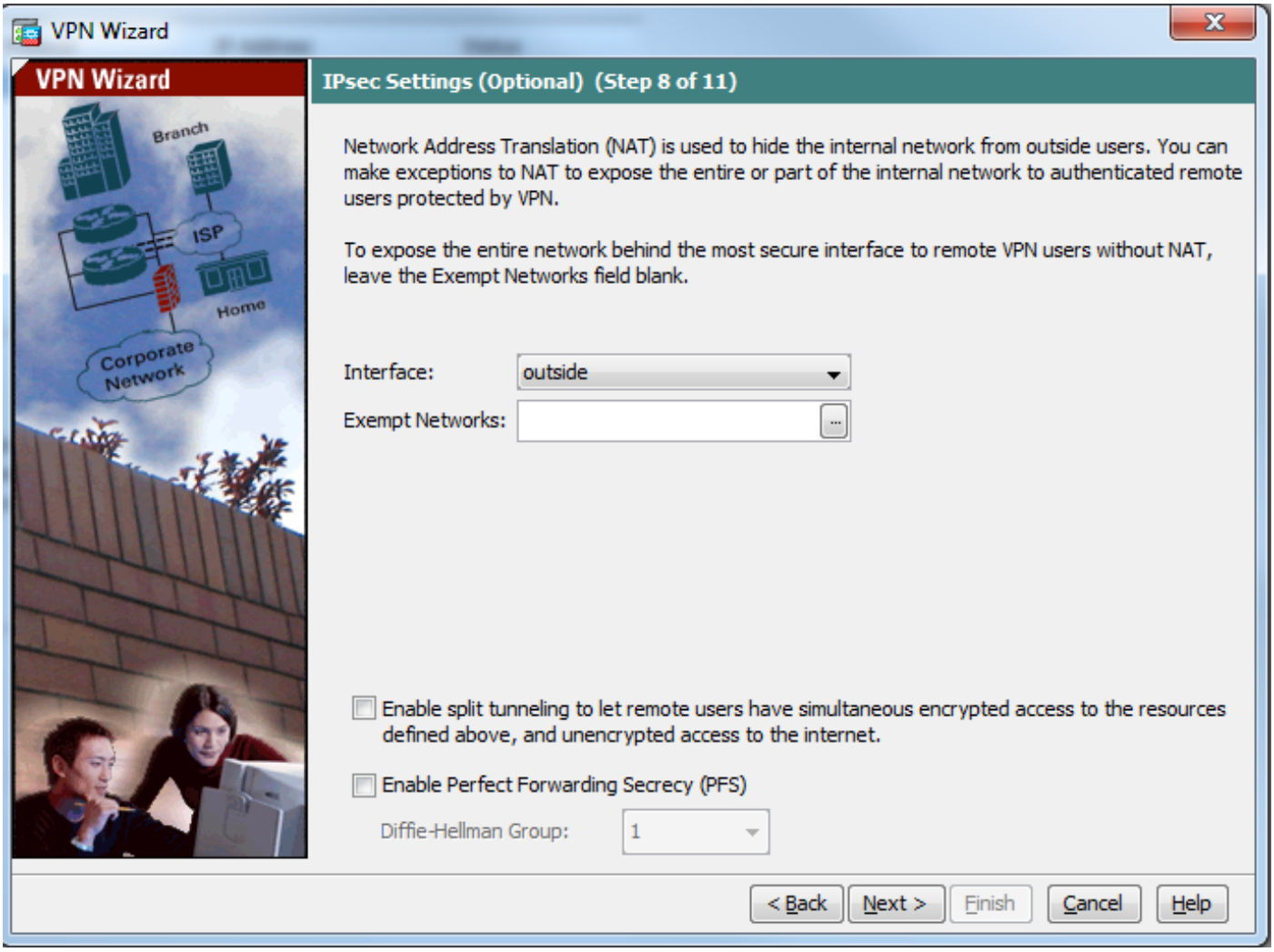

Stap 9. Controleer de poolinstellingen en klik op **Volgende.**



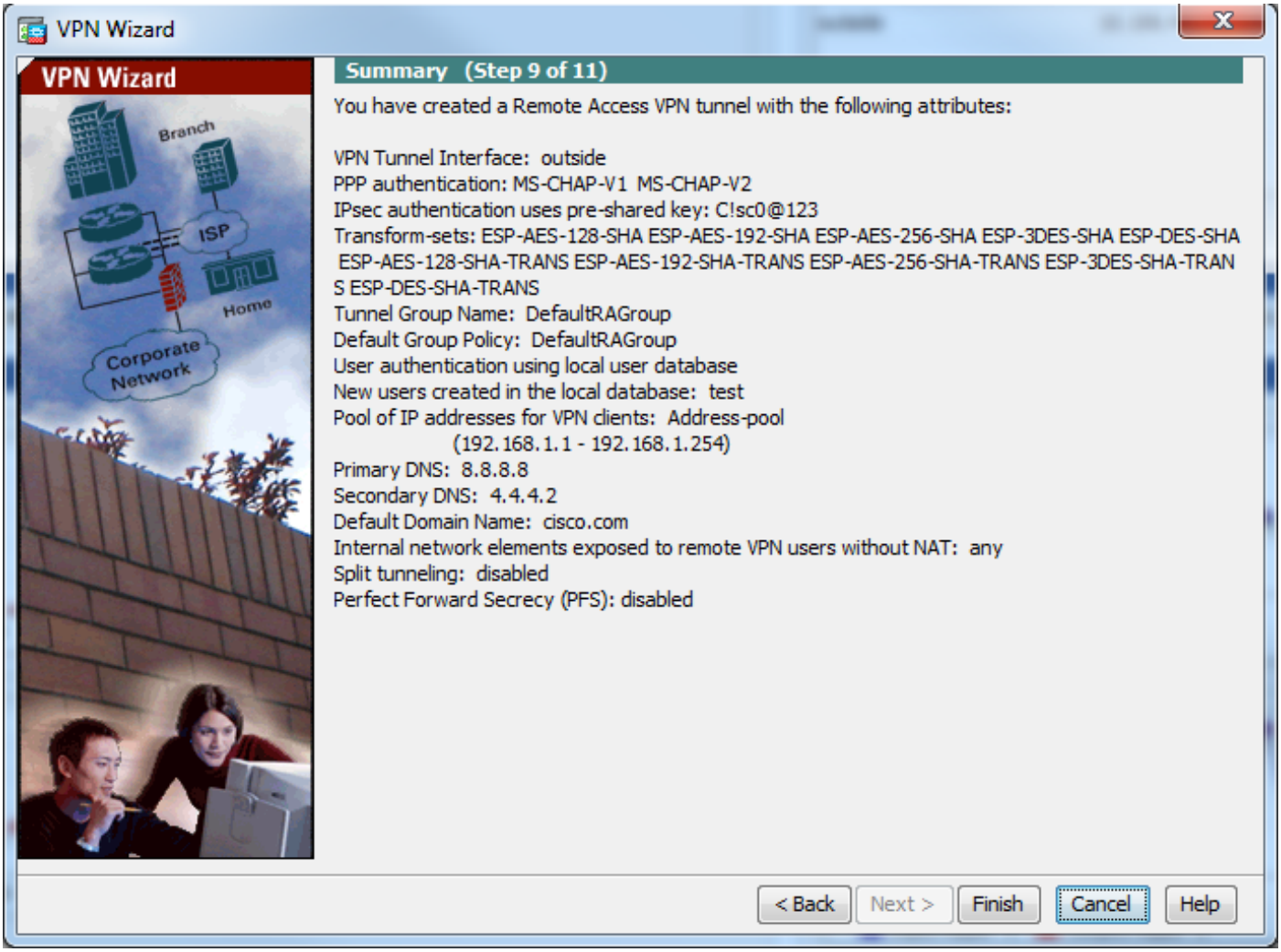

Stap 10. Configuratie van de eigenschappen die aan de cliënten moeten worden geduwd of laat het leeg en klik op **Volgende.**




Stap 11: Zorg ervoor dat het vakje **Perfect Forwarding SecRITY (PFS)** inschakelen niet is ingeschakeld omdat sommige clientplatforms deze optie niet ondersteunen. **Schakel een gesplitste tunneling in om externe gebruikers tegelijkertijd gecodeerde toegang tot de hierboven gedefinieerde bronnen te geven en niet-gecodeerde toegang tot het internet** is ongecontroleerd. Dit betekent dat het volledige tunneling is ingeschakeld waardoor al het verkeer (inclusief internetverkeer) van de client naar de ASA wordt verzonden via de VPN-tunnel. Klik op **Volgende.**




Stap 12. Controleer de beknopte informatie en klik vervolgens op **Voltooien.**




## ASA-configuratie met CLI

**Stap 1. Configuratie van de beleidsparameters van IKE Fase 1.**

Dit beleid wordt gebruikt om het regelverkeer tussen de leeftijdsgenoten te beschermen (dat wil zeggen, het beschermt pre-gedeelde sleutel en de fase 2 onderhandelingen)

```
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#exit
```

**Stap 2. Instellen van transformatie.**

Het bevat beleidsparameters van IKE fase 2 die worden gebruikt om het gegevensverkeer te beschermen. Aangezien de Windows L2TP/IPsec-client IPsec-transportmodus gebruikt, stelt u de modus in om te transporteren. De standaardinstelling is tunnelmodus

```
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport
```

**Stap 3. Configuratie van dynamische kaart.**

Aangezien Windows-clients dynamisch IP-adres voor ISP- of lokale DHCP-server (bijvoorbeeld

modem) krijgen, is ASA niet op de hoogte van het IP-adres van de peer en vormt dit een probleem bij de configuratie van een statisch peer in het ASA-eindstation. Dus moet dynamische cryptoconfiguratie worden benaderd waarin alle parameters niet noodzakelijk worden gedefinieerd en de ontbrekende parameters later dynamisch worden geleerd, als resultaat van IPSec onderhandeling van de klant.

```
ciscoasa(config)#crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-
SHA
```

**Stap 4. Bind dynamische kaart op statische crypto kaart en pas de crypto kaart toe en laat IKEv1 op externe interface toe**

Dynamische crypto kaart kan niet op een interface worden toegepast en bindt het dus aan statische crypto kaart. Dynamische crypto sets dienen de laagste prioriteit te zijn voor crypto kaarten in de crypto map set (dat wil zeggen, ze moeten de hoogste sequentienummers hebben) zodat de ASA eerst andere crypto kaarten evalueert. Het onderzoekt de dynamische crypto kaart die slechts wordt ingesteld wanneer de andere (statische) kaart ingangen niet overeenkomen.

```
ciscoasa(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
ciscoasa(config)#crypto map outside_map interface outside
ciscoasa(config)#crypto ikev1 enable outside
```

**Stap 5. Maak IP-adresgroep**

Maak een pool van adressen waarvan IP-adressen dynamisch aan de externe VPN-clients worden toegewezen. Negeer deze stap om bestaande pool op ASA te gebruiken.

```
ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
```

**Stap 6. Groepsbeleid configureren**

Identificeer het groepsbeleid als intern, wat betekent dat de eigenschappen worden opgenomen in de lokale gegevensbank.

```
ciscoasa(config)#group-policy L2TP-VPN internal
```

> Opmerking: L2TP/IPsec-verbindingen kunnen worden geconfigureerd met of standaard groepsbeleid (DfltGrpPolicy) of een door de gebruiker gedefinieerd groepsbeleid. In beide gevallen moet het groepsbeleid worden ingesteld om het L2TP/IPsec-tunneling protocol te gebruiken. Configureer l2tp-ipsec in de VPN-protocoleigenschap op de standaardgroep-beleid dat geërfd zal worden aan het door de gebruiker ingestelde groepsbeleid als de VPN-protocol eigenschap er niet op is ingesteld.

Configureer de eigenschappen zoals het VPN-tunnelprotocol (in ons geval is het l2tp-ipsec), domeinnaam, DNS- en WINS-server-IP-adres en nieuwe gebruikersrekeningen

```
ciscoasa(config)#group-policy L2TP-VPN attributes
ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2
ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec
ciscoasa(config-group-policy)#default-domain value cisco.com
```

Configureer gebruikersnamen en wachtwoorden op het apparaat naast het gebruik van de AAA. Als de gebruiker een L2TP-client is die Microsoft CHAP versie 1 of versie 2 gebruikt en de ASA is ingesteld om authenticatie aan te vragen tegen de lokale database, moet het trefwoord van het schap worden opgenomen. Bijvoorbeeld, gebruikersnaam <gebruikersnaam> - wachtwoord <wachtwoord> - keurmerk.

```
ciscoasa(config-group-policy)# username test password test mschap
```

**Stap 7. Instellen van een tunnelgroep**

Maak een tunnelgroep met de opdracht **tunnel-groep** en specificeer de naam van de lokale adrestoewijzing die wordt gebruikt om het IP-adres aan de client toe te wijzen. Als de authenticatiemethode vooraf-gedeeld-key is, moet de tunnelgroepnaam DefaultRAGGroup zijn, omdat er geen optie op de client is om de tunnelgroep te specificeren en dus alleen op de standaardinstunnelgroep landt. Bind het groepsbeleid aan tunnel-groep die de standaard-groep-beleid bevel gebruikt

```
ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes
ciscoasa(config-tunnel-general)#address-pool Address-pool
ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN
ciscoasa(config-tunnel-general)#exit
```

> Opmerking: Het standaardverbindingsprofiel (tunnelgroep), DefaultRAGGroup moet worden geconfigureerd, indien vooraf gedeelde key-gebaseerde verificatie wordt uitgevoerd. Indien op certificaat gebaseerde echtheidscontrole wordt uitgevoerd, kan een door de gebruiker bepaald aansluitingsprofiel worden gekozen op basis van certificaathoudkenmerken

Gebruik de opdracht **voor tunnelgroepeigenschappen** om de ipsec-attribuut configuratie-modus in te voeren om de voorgedeelde toets in te stellen.

```
ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes
ciscoasa(config-tunnel-ipsec)#  ikev1 pre-shared-key C!sc0@123
ciscoasa(config-tunnel-ipsec)#exit
```

Configureer het PPP-verificatieprotocol met de opdracht **verificatietype** van de tunnelgroepmodus p-eigenschappen. Schakel CHAP uit dat standaard is ingeschakeld omdat het niet wordt ondersteund als AAA-server is ingesteld als lokale database.

```
ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)#no authentication chap
ciscoasa(config-ppp)#authentication ms-chap-v2
ciscoasa(config-ppp)#exit
```

**Stap 8. NAT-vrijstelling configureren**

NAT-vrijstelling instellen zodat de cliënten toegang hebben tot interne middelen die verbonden zijn met interne interfaces (in dit voorbeeld zijn interne middelen verbonden met interne interface).

```
ciscoasa(config)#object network L2TP-Pool
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#exit
ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-
Pool no-proxy-arp route-lookup
```

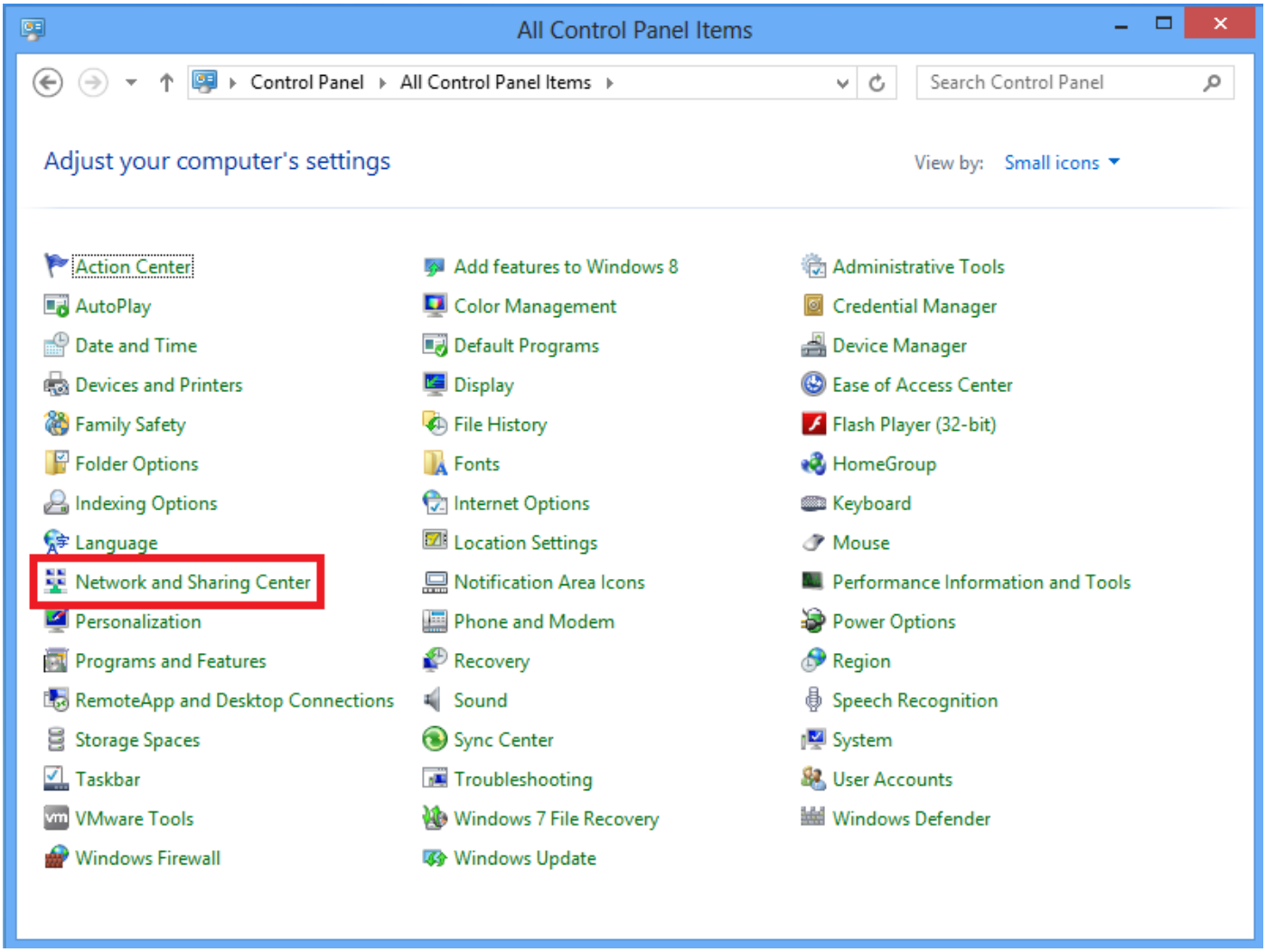
**Configuratie van volledige steekproef**

```
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
```

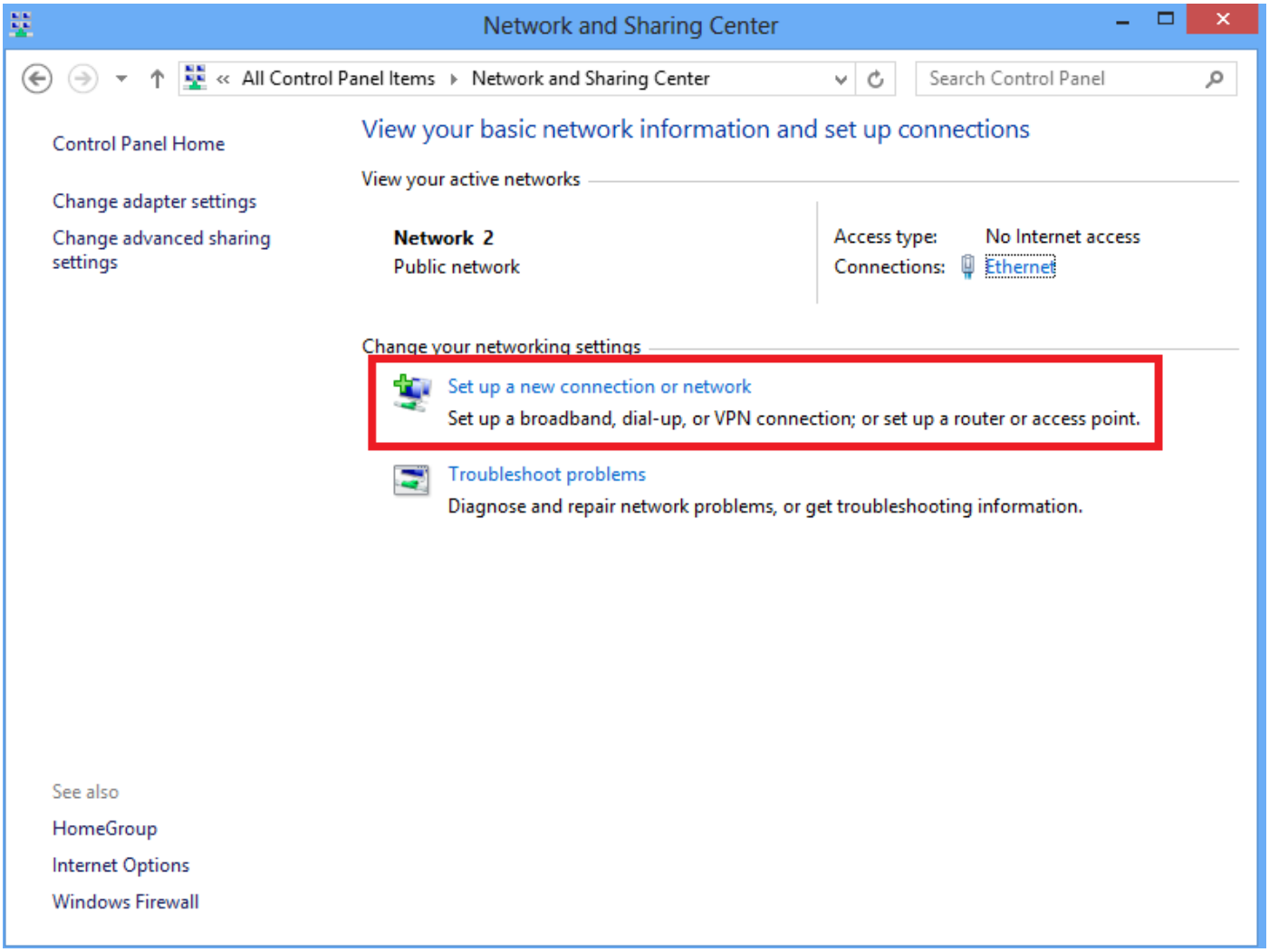
```
exit

crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport

crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
crypto ikev1 enable outside

ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

group-policy L2TP-VPN internal
group-policy L2TP-VPN attributes
vpn-tunnel-protocol l2tp-ipsec
default-domain value cisco.com
username test password test mschap
exit

tunnel-group DefaultRAGroup general-attributes
address-pool Address-pool
default-group-policy L2TP-VPN
exit

tunnel-group DefaultRAGroup ipsec-attributes
ikev1 pre-shared-key C!sc0@123
exit

tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
exit

object network L2TP-Pool
subnet 192.168.1.0 255.255.255.0
exit
nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp
route-lookup
```

## Configuratie van Windows 8 L2TP/IPsec-client

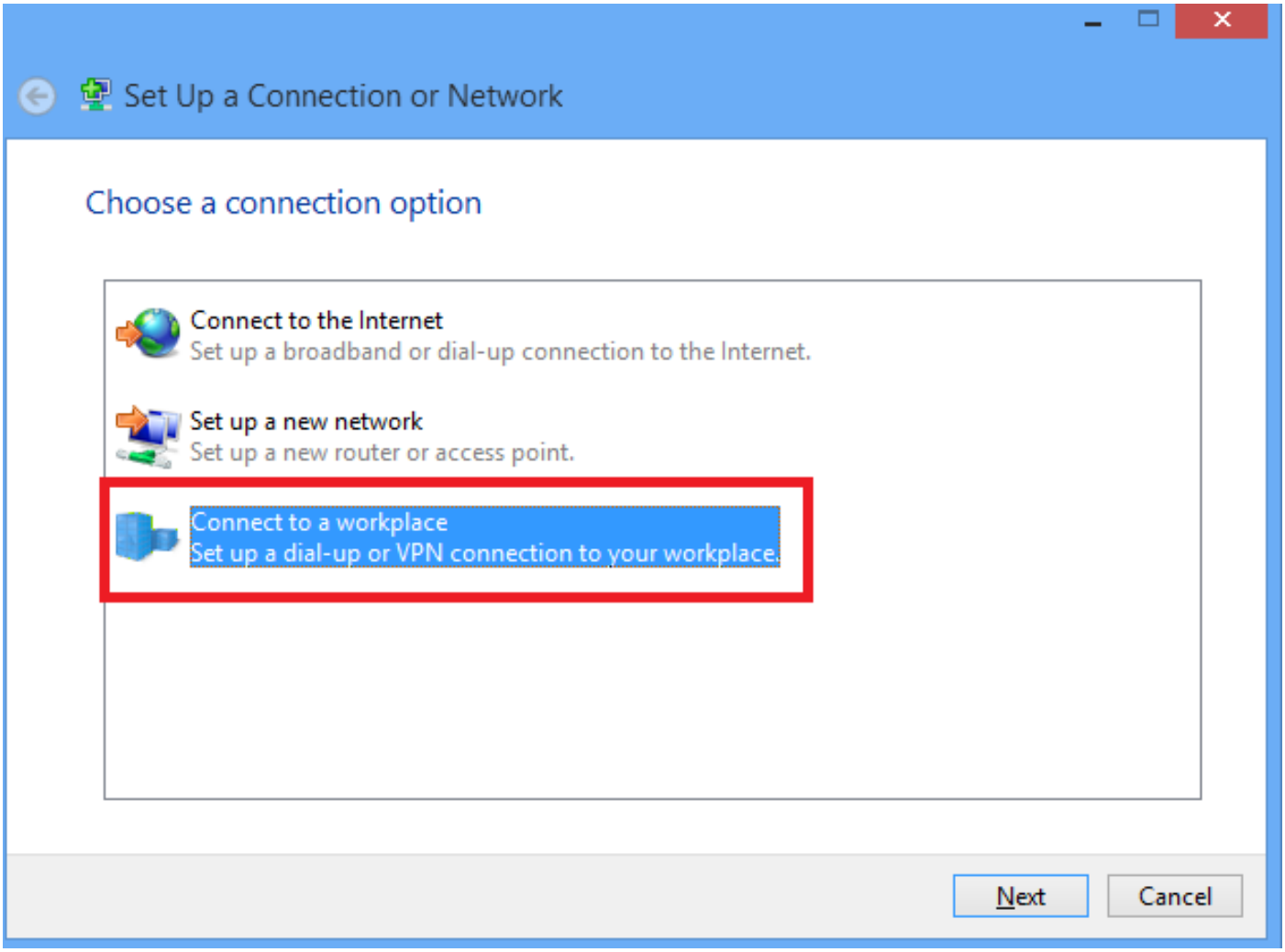
1. Open het bedieningspaneel en selecteer Netwerk en verspreidingscentrum.



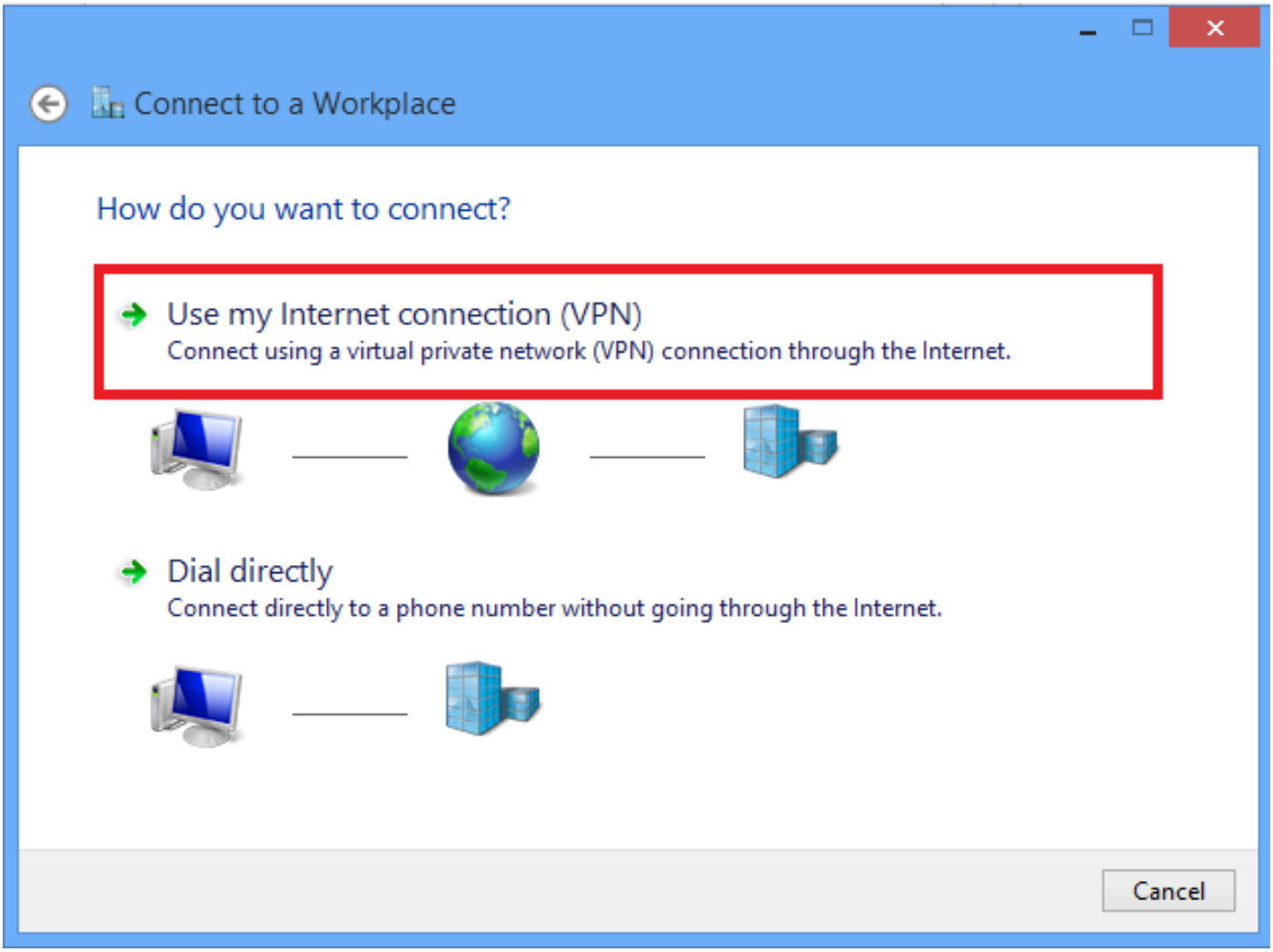

2. Kies **een nieuwe verbinding of** een **netwerkoptie**.



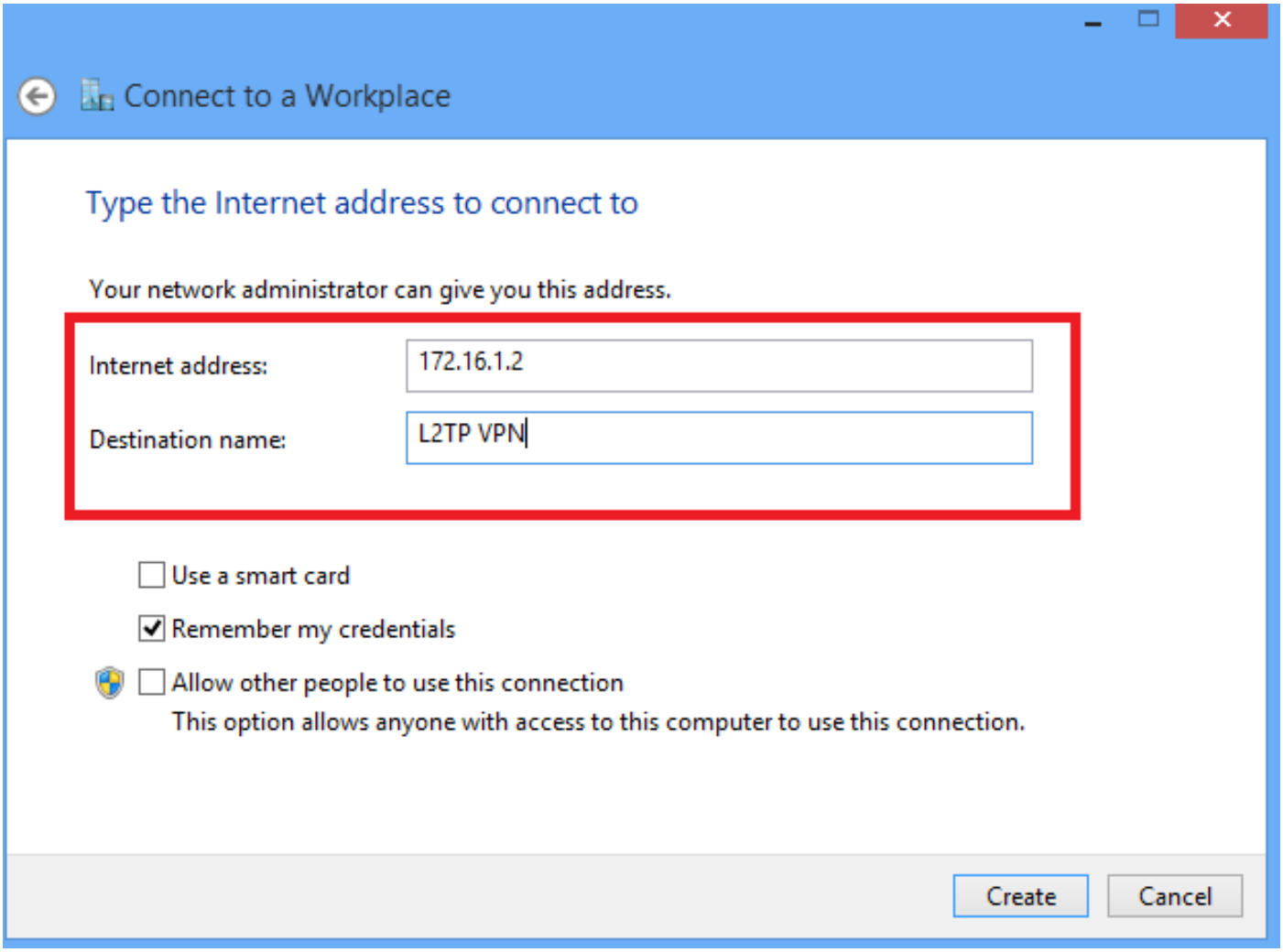

3. Selecteer **Connect met een werkplek** en klik op **Volgende.**



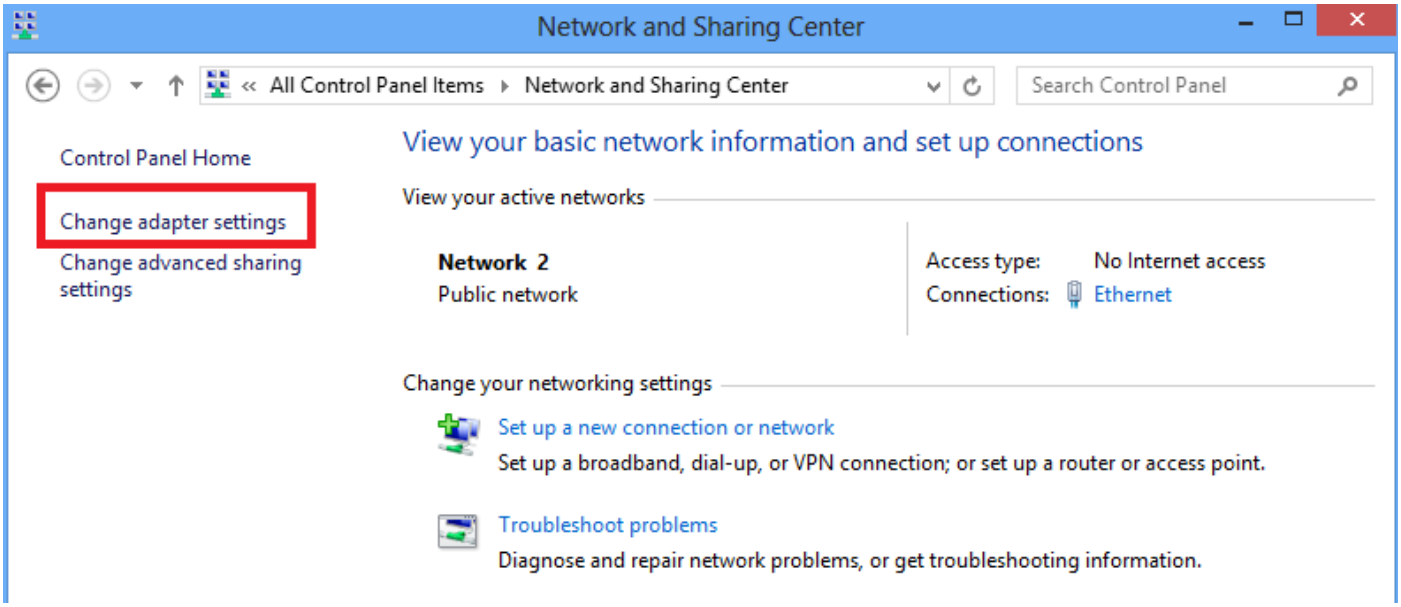

4.Klik op **de** optie **Mijn internetverbinding (VPN)** gebruiken.



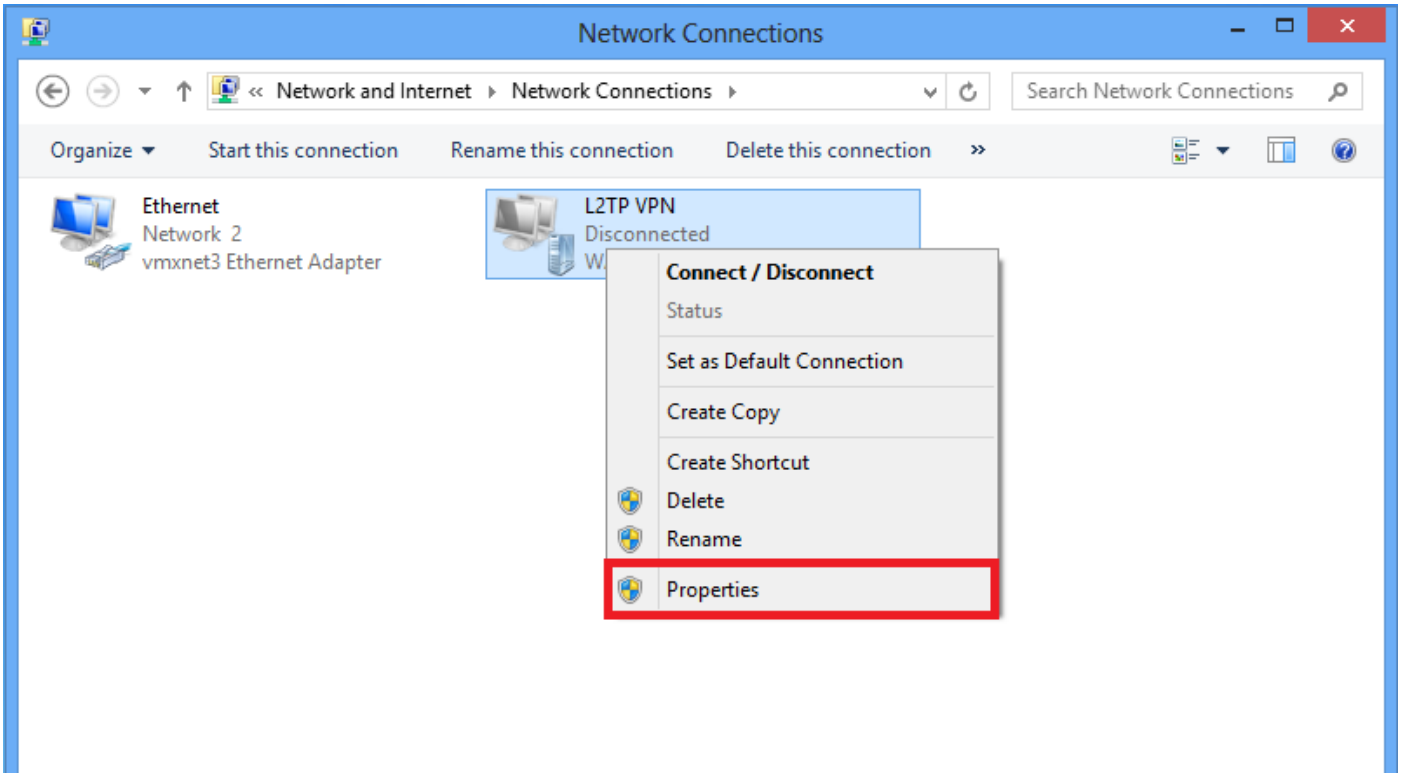

5. Voer IP-adres in van ASA's WAN-interface of FQDN en elke naam voor VPN-adapter die lokaal belangrijk is en klik op **Create.**



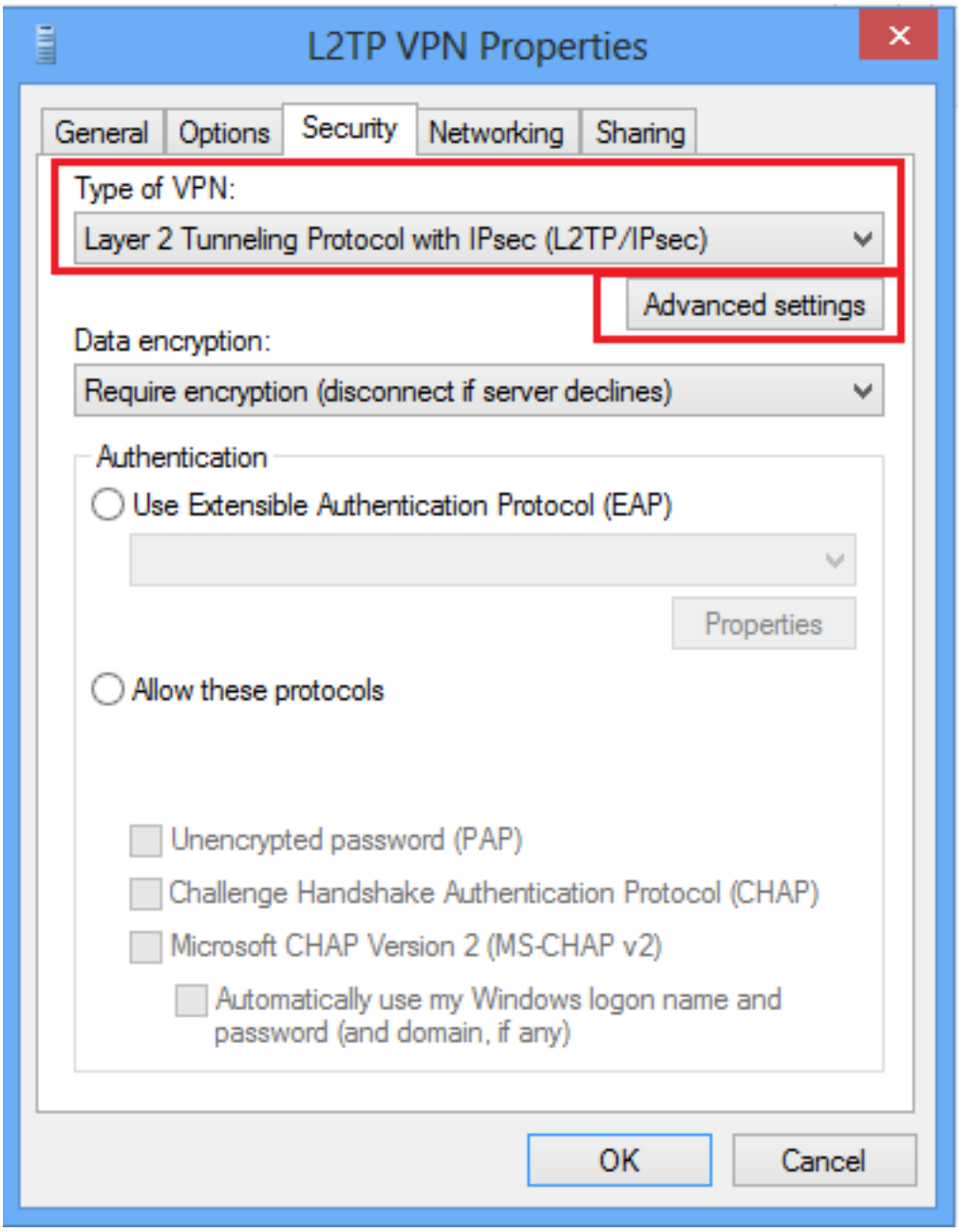

6. Selecteer in het gedeelte Network and Sharing Center de optie **Verander** de **adapterinstellingen** in het linker venster van het venster.



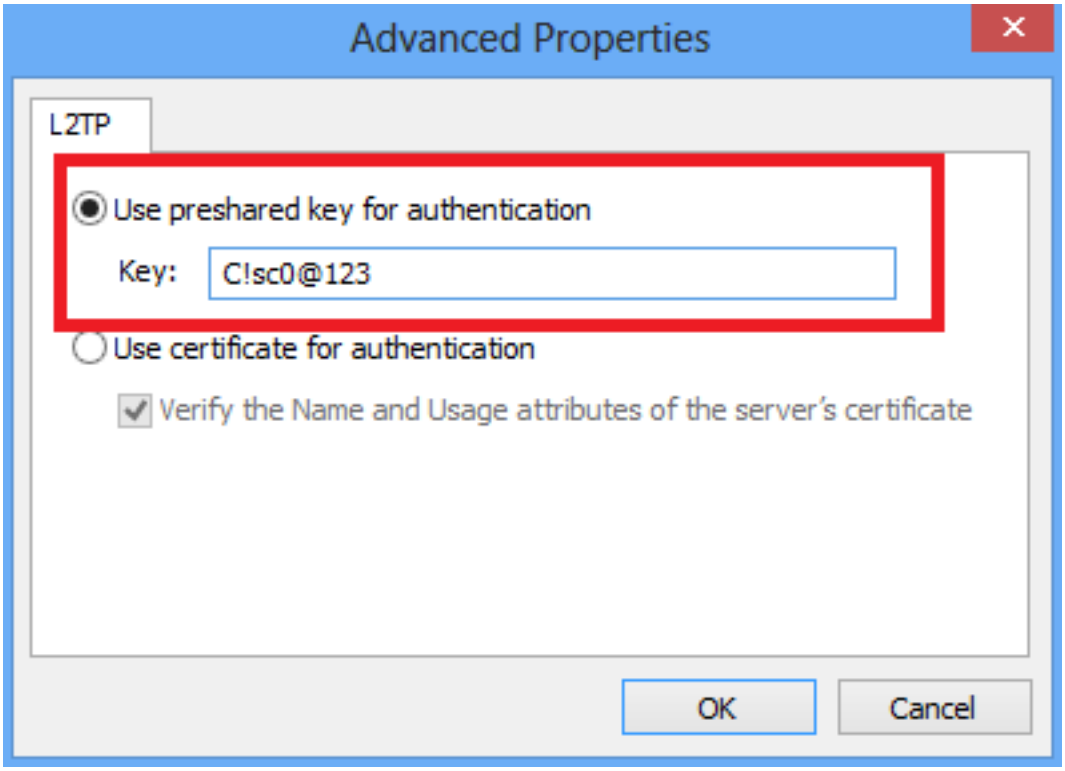

7. Klik met de rechtermuisknop op de recent gemaakte adapter voor L2TP VPN en kies **Eigenschappen.**



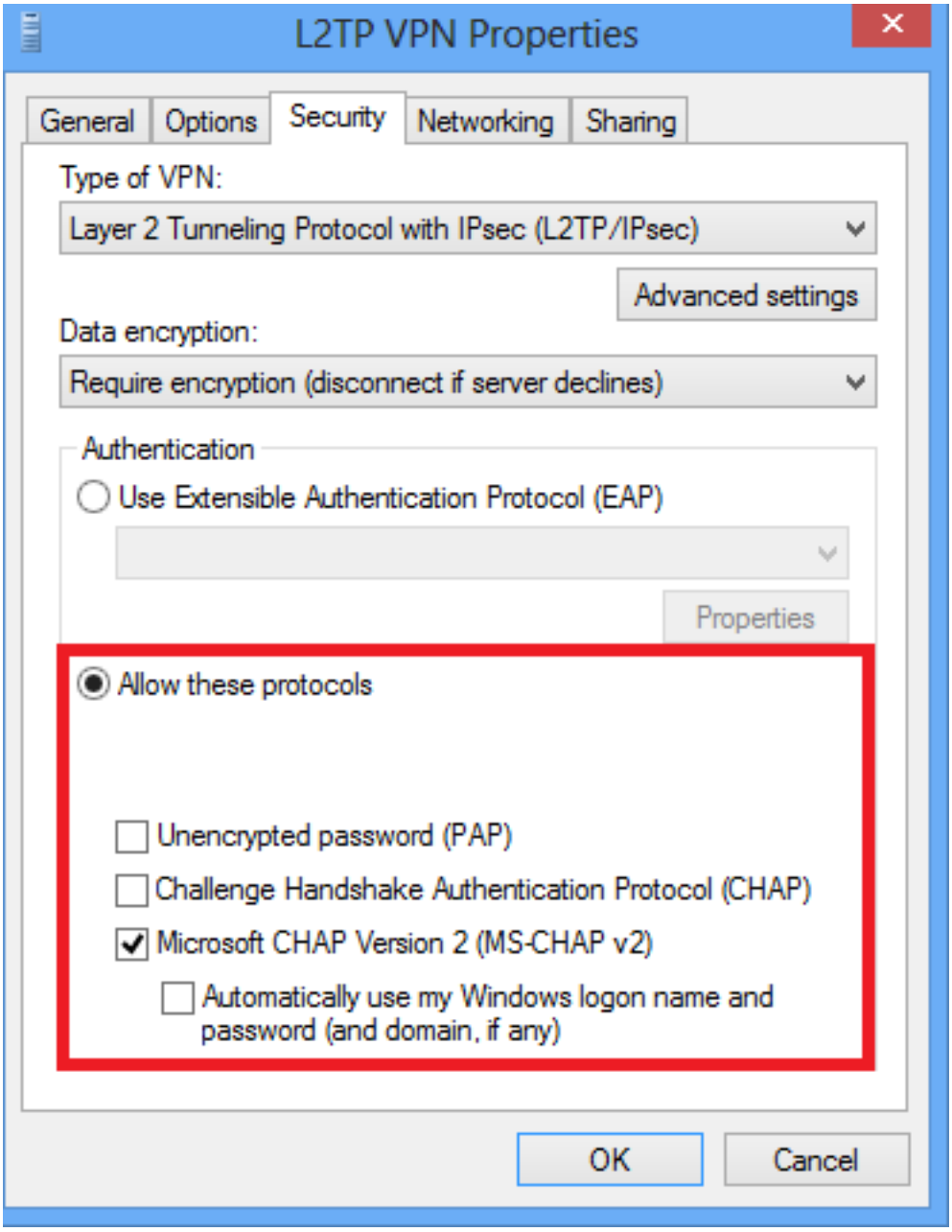

8. Navigeer naar het tabblad **Security**, kies het type VPN als **Layer 2 Tunneling Protocol met IPsec (L2TP/IPsec)** en klik vervolgens op **Geavanceerde instellingen.**



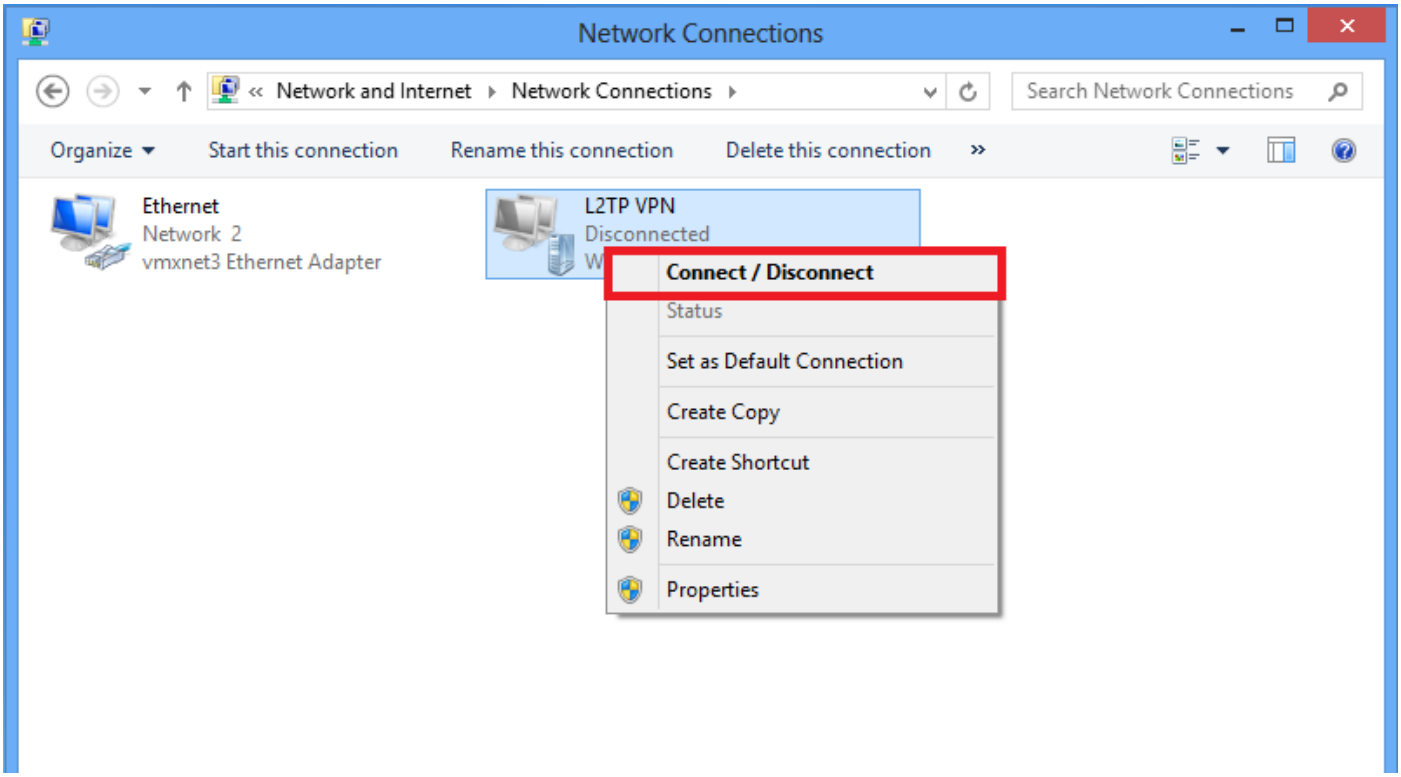

9. Voer de vooraf gedeelde toets in zoals ook wordt vermeld in de **DefaultRAGgroup** van tunnelgroepen en klik op **OK**. In dit voorbeeld wordt C!sc0@123 gebruikt als de vooraf gedeelde toets.



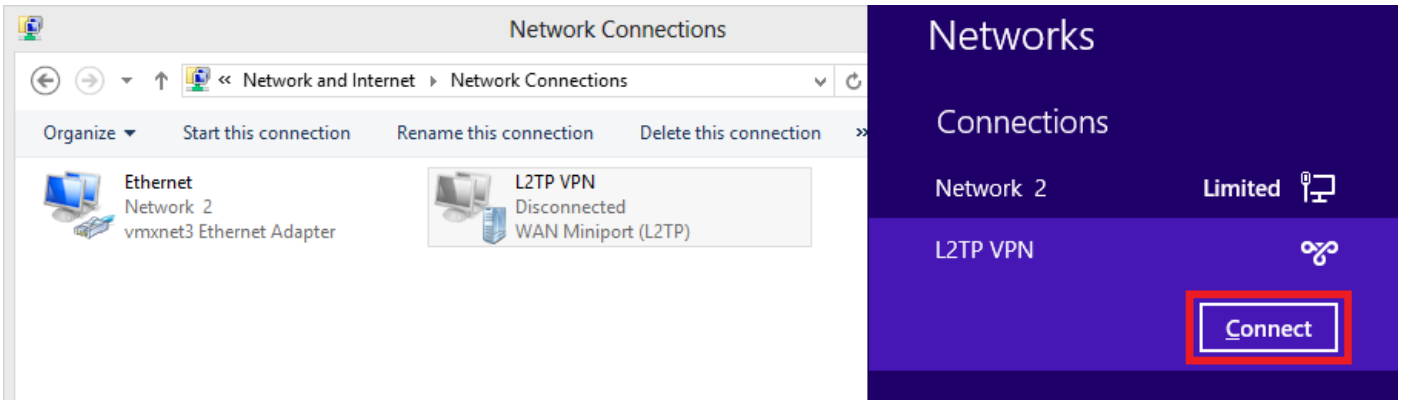

10. Kies de authenticatiemethode zoals Deze protocollen toestaan en zorg ervoor dat alleen de selectieknop '**Microsoft CHAP Versie 2 (MS-CHAP v2)** ingeschakeld is en klik op **OK**.



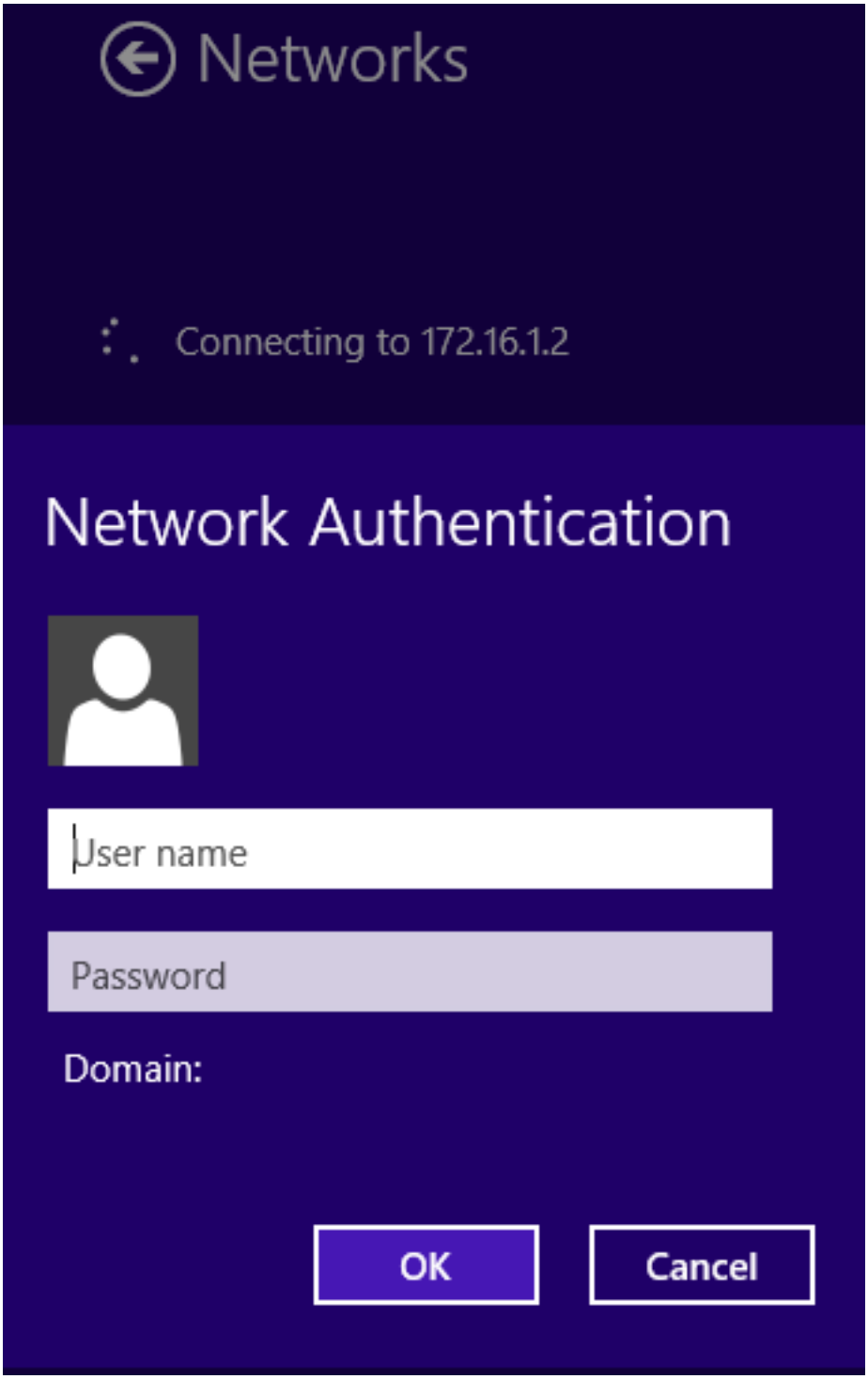

1. Klik met de rechtermuisknop op L2TP VPN-adapter onder netwerkverbindingen en kies **Connect/disconnect.**



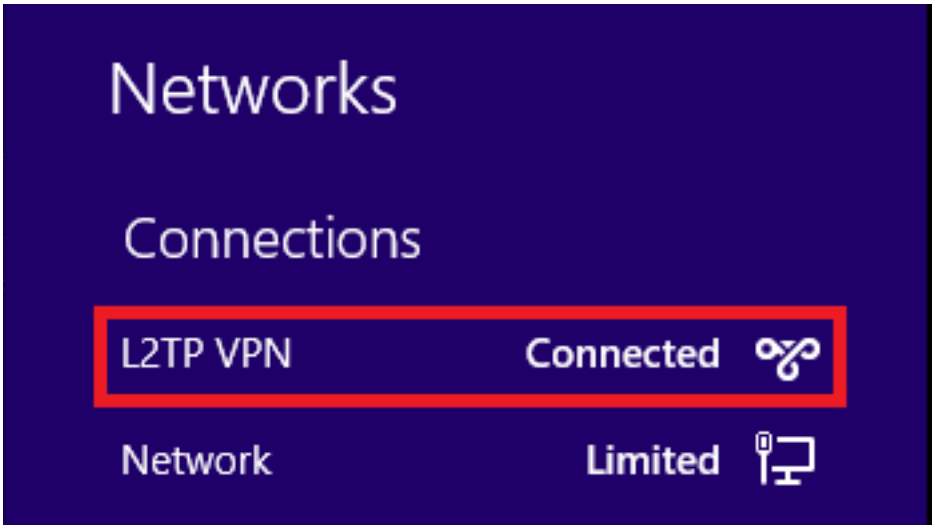

12. Het pictogram netwerken verschijnt en klikt op **Connect** op VPN-verbinding van L2TP.




13. Voer de gebruikersreferenties in en klik op **OK**.




Als de gewenste parameters op beide eindpunten worden afgestemd, wordt de verbinding L2TP/IPsec ingesteld.




## Configuratie Split-tunnelleiding

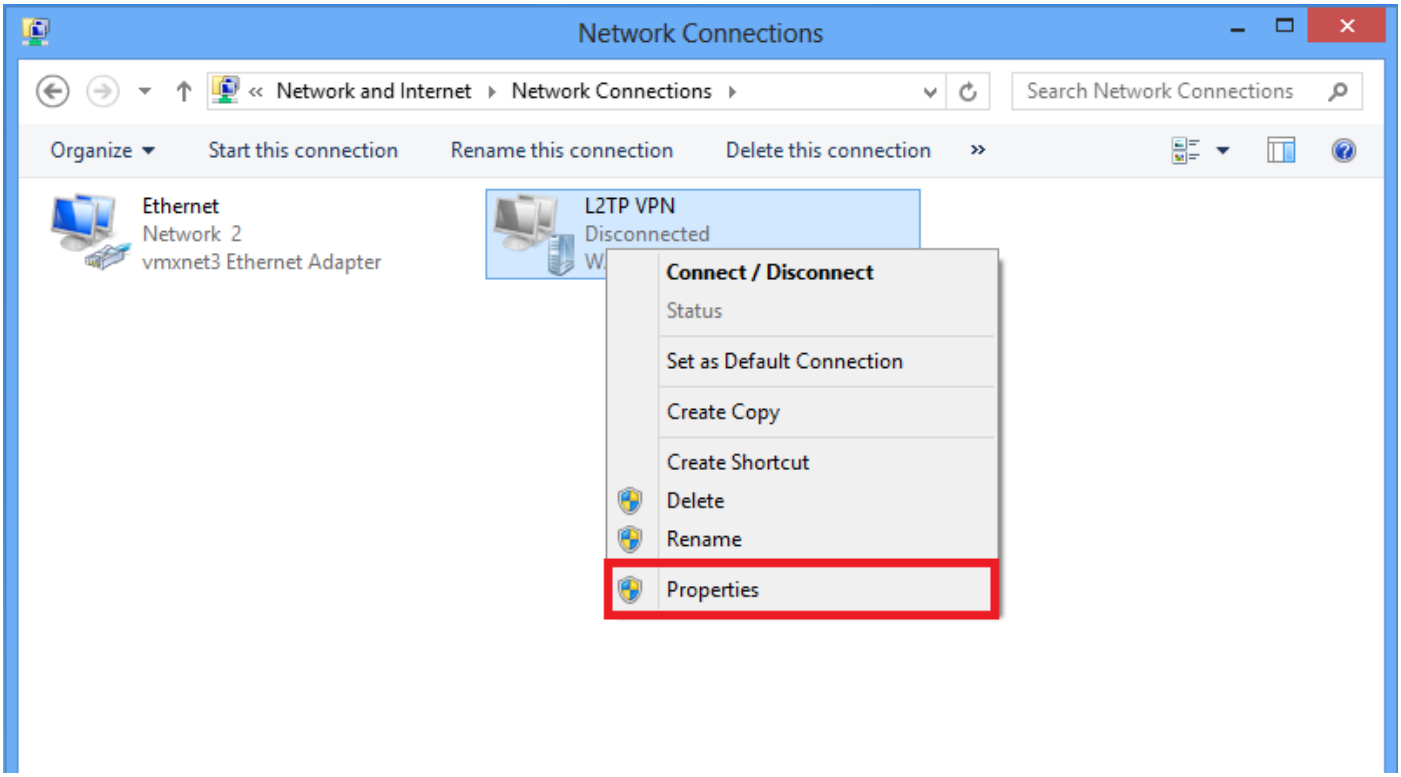
Split-tunneling is een optie die u kunt gebruiken om het verkeer voor de subnetten of hosts te definiëren dat moet worden versleuteld. Dit betreft de configuratie van een toegangscontrolelijst (ACL), die met deze functie is gekoppeld. Het verkeer voor de subnetten of de hosts die op deze ACL wordt gedefinieerd wordt versleuteld via de tunnel van het client-eind, en de routes voor deze subnetten worden geïnstalleerd op de PC die de tabel routeert. ASA onderschept het bericht van DHCPINFORM van een client en reageert met het subnetmasker, de domeinnaam en de klassen van statische routes.

### Configuratie op ASA

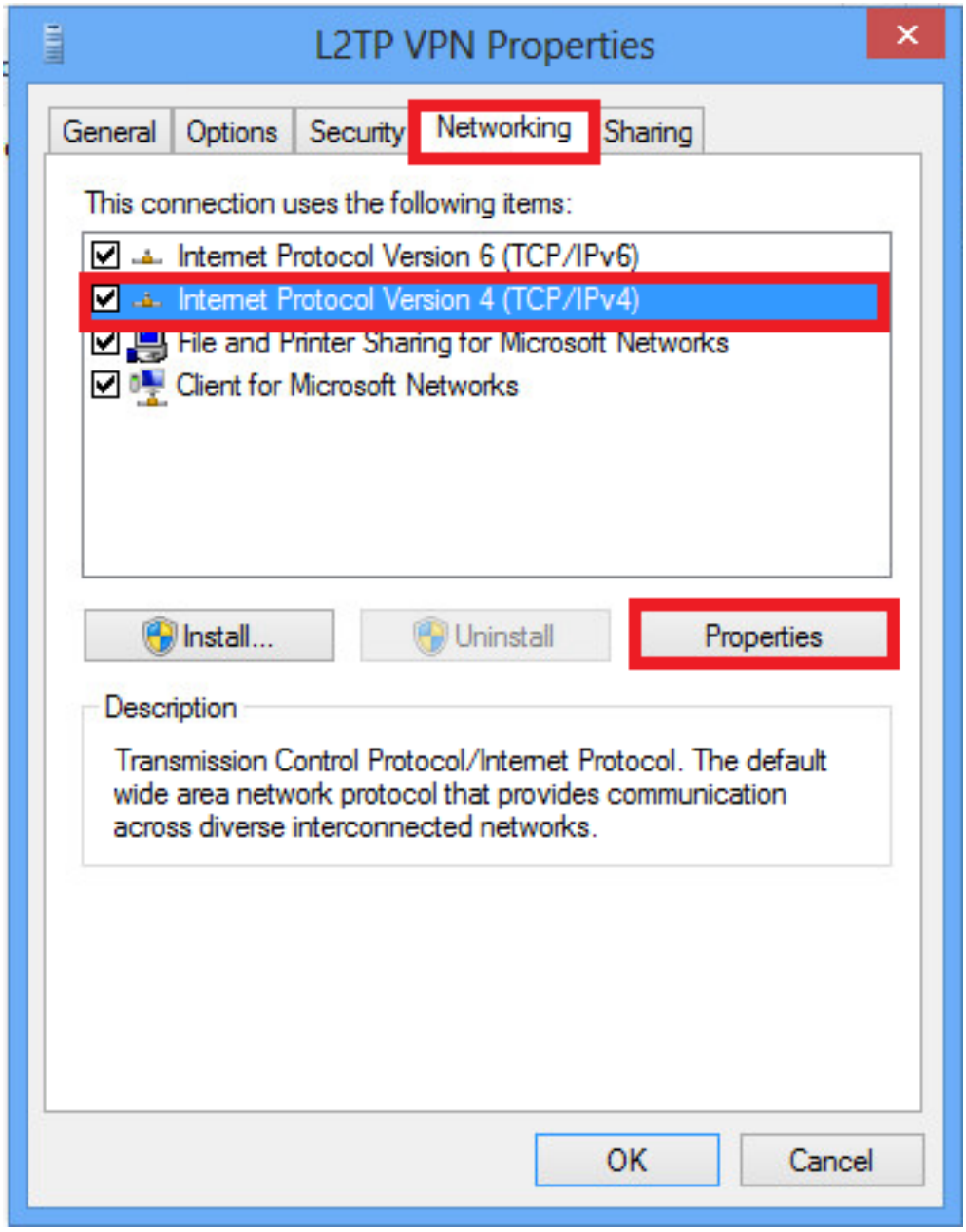
```
ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0

ciscoasa(config)# group-policy DefaultRAGroup attributes
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified
ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT
ciscoasa(config-group-policy)# intercept-dhcp 255.255.255.255 enable
```

### Configuratie op L2TP/IPsec-client

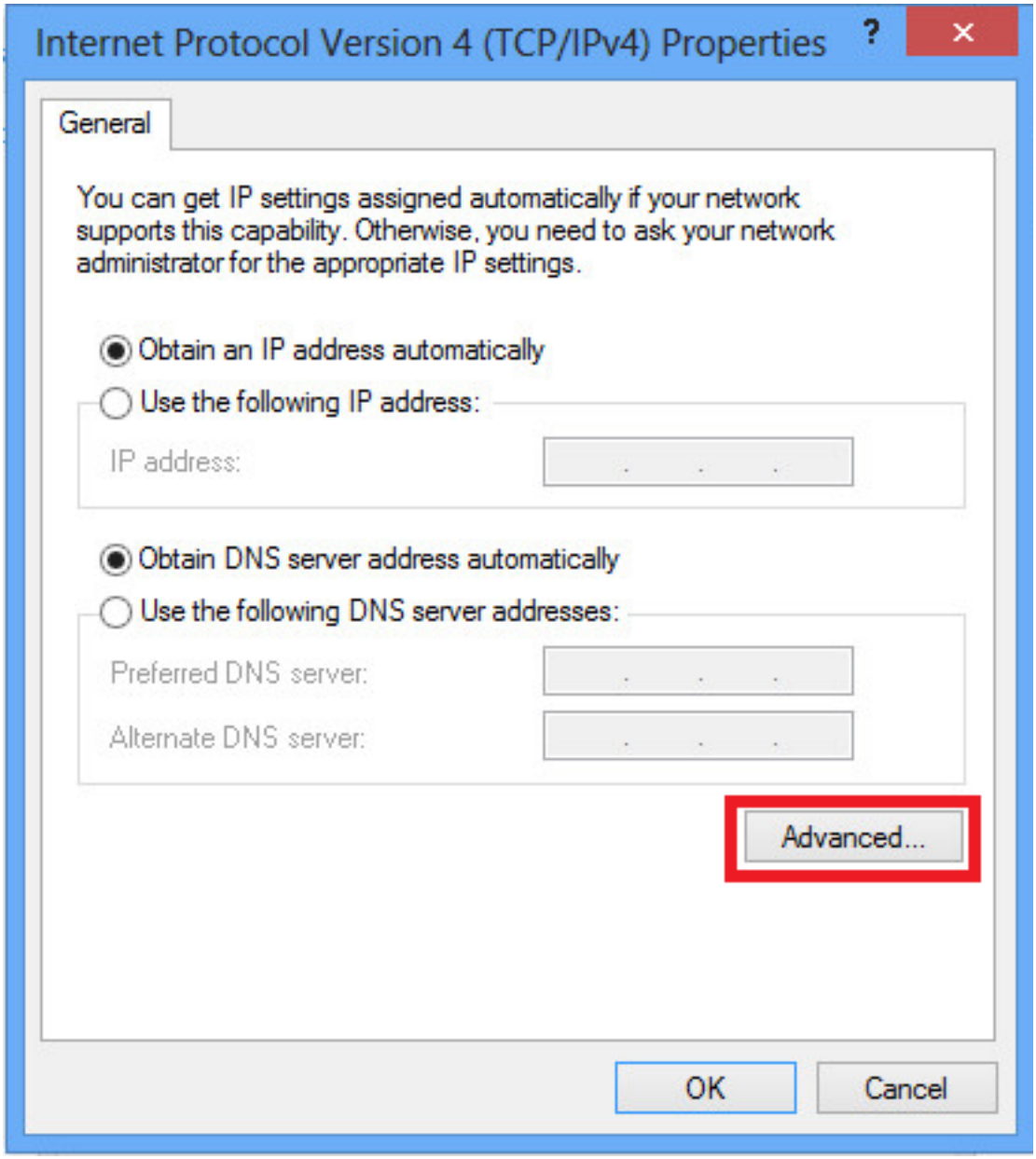
1. Klik met de rechtermuisknop op de L2TP VPN-adapter en kies **Eigenschappen.**



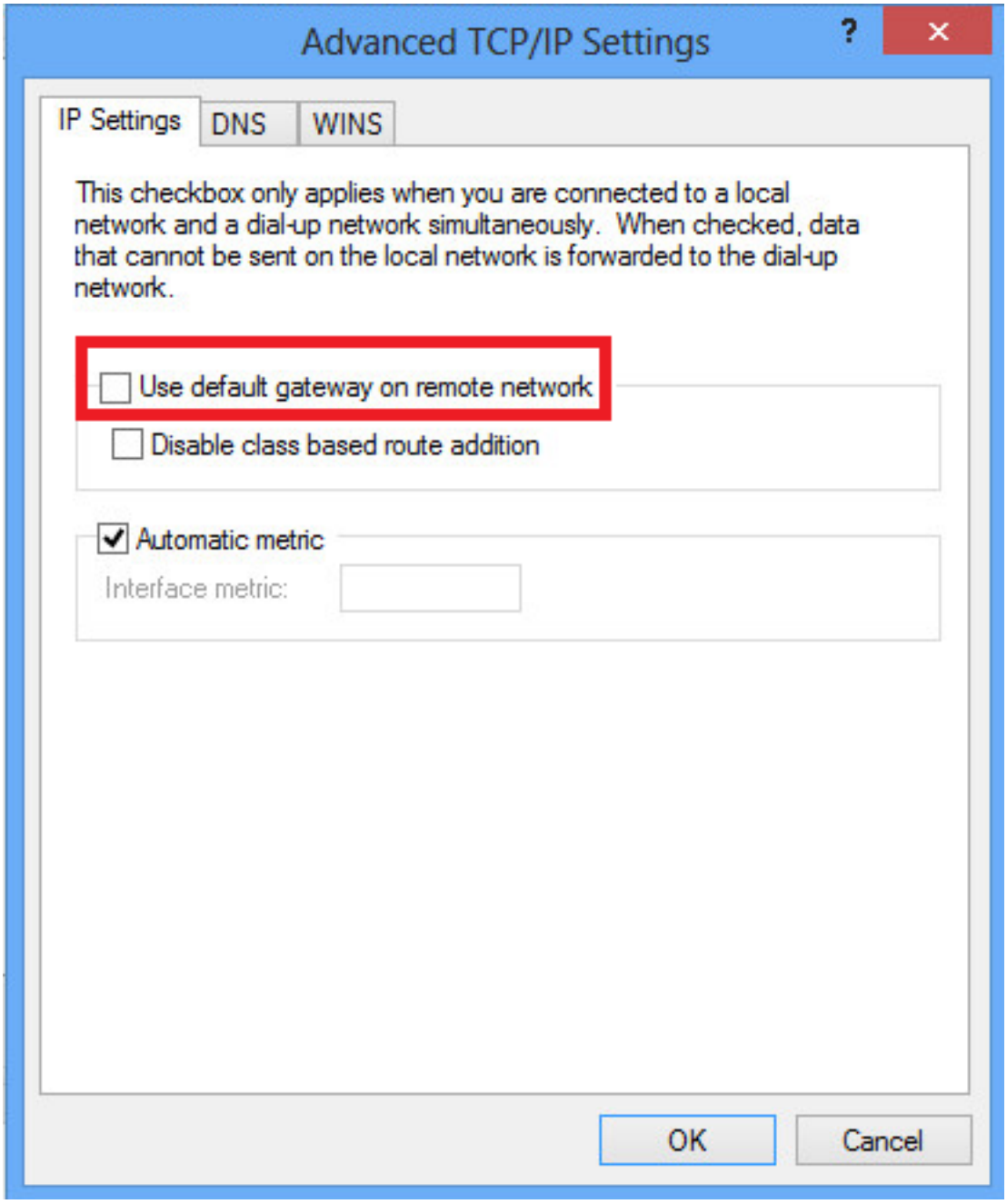

2. Navigeer naar het tabblad Netwerk, kies Internet Protocol, versie 4 (TCP/IPv4) en klik vervolgens op **Properties.**




3. Klik op **de** optie **Geavanceerd**.




4. Schakel de **standaardopening op de** optie **afstandsnetwerk uit** en klik op **OK**.




# Verifiëren

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

> Opmerking: De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

- **toon crypto ikev1 sa** - laat alle huidige IKE SA's bij een peer zien.

```
ciscoasa# show crypto ikev1 sa

IKEv1 SAs:

  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:

10.1.1.2


   Type    : user            Role    : responder
   Rekey   : no

State   : MM_ACTIVE
```

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

```
ciscoasa# show crypto ipsec sa
interface: outside
   Crypto map tag:

outside_dyn_map

, seq num: 10, local addr: 172.16.1.2

     local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/

17/1701

)
     remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/

17/1701

)


current_peer: 10.1.1.2, username: test




dynamic allocated peer ip: 192.168.1.1


     dynamic allocated peer ip(ipv6): 0.0.0.0



#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29




      #pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118


     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
     #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

```
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0
     path mtu 1500, ipsec overhead 58(36), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: E8AF927A
     current inbound spi : 71F346AB

   inbound esp sas:
     spi: 0x71F346AB (1911768747)
        transform: esp-3des esp-sha-hmac no compression
        in use settings ={RA, Transport, IKEv1, }
        slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (237303/3541)
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000003
   outbound esp sas:
     spi: 0xE8AF927A (3903820410)
        transform: esp-3des esp-sha-hmac no compression
        in use settings ={RA, Transport, IKEv1, }
        slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (237303/3541)
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

- **vpn-sessiondb detail ra-ikev1-ipsec filterprotocol l2tpOverIpSec tonen - toont gedetailleerde informatie over L2TP via IPsec-verbindingen.**

```
ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec

Session Type: IKEv1 IPsec Detailed


Username     : test

                  Index        : 1


Assigned IP  : 192.168.1.1           Public IP    : 10.1.1.2


Protocol     : IKEv1 IPsec L2TPOverIPsec
License      : Other VPN
Encryption   : IKEv1: (1)3DES  IPsec: (1)3DES  L2TPOverIPsec: (1)none
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1  L2TPOverIPsec: (1)none
Bytes Tx     : 1574                  Bytes Rx     : 12752
Pkts Tx      : 29                    Pkts Rx      : 118
Pkts Tx Drop : 0                     Pkts Rx Drop : 0


Group Policy : L2TP-VPN              Tunnel Group : DefaultRAGroup


Login Time   : 23:32:48 UTC Sat May 16 2015
```

```
Duration     : 0h:04m:05s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                     VLAN         : none
Audt Sess ID : 0a6a2577000010005557d3a0
Security Grp : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1
L2TPOverIPsec Tunnels: 1
```

**IKEv1:**

```
 Tunnel ID    : 1.1
 UDP Src Port : 500                     UDP Dst Port : 500
 IKE Neg Mode : Main                    Auth Mode    : preSharedKeys
 Encryption   : 3DES                    Hashing      : SHA1
 Rekey Int (T): 28800 Seconds           Rekey Left(T): 28555 Seconds
 D/H Group    : 2
 Filter Name  :
```

**IPsec:**

```
 Tunnel ID    : 1.2
 Local Addr   : 172.16.1.2/255.255.255.255/17/1701
 Remote Addr  : 10.1.1.2/255.255.255.255/17/1701
 Encryption   : 3DES                    Hashing      : SHA1
 Encapsulation: Transport
 Rekey Int (T): 3600 Seconds            Rekey Left(T): 3576 Seconds
 Rekey Int (D): 250000 K-Bytes          Rekey Left(D): 250000 K-Bytes
 Idle Time Out: 30 Minutes              Idle TO Left : 29 Minutes
 Bytes Tx     : 1574                    Bytes Rx     : 12752
 Pkts Tx      : 29                      Pkts Rx      : 118
```

**L2TPOverIPsec:**

```
 Tunnel ID    : 1.3
```

**Username : test**

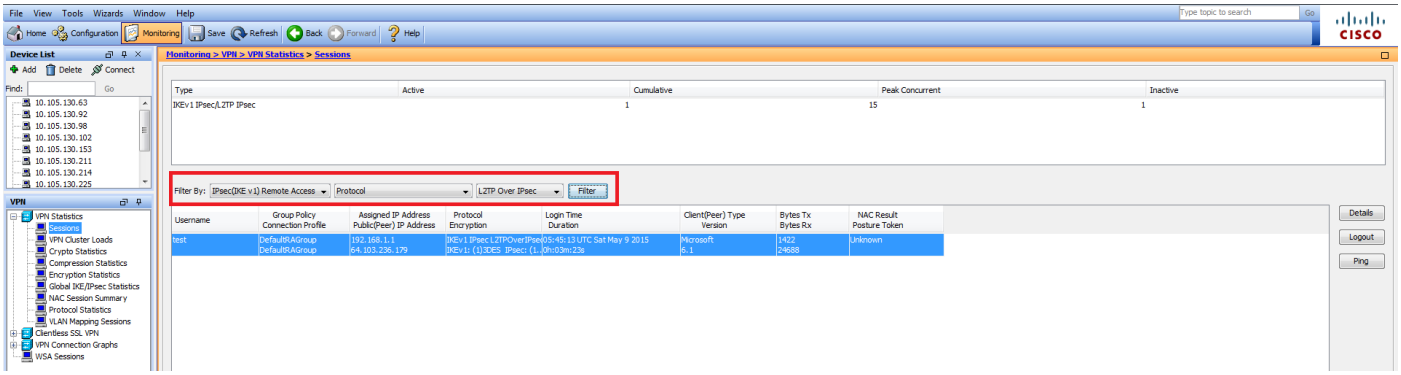
**Assigned IP : 192.168.1.1**

**Public IP : 10.1.1.2**

```
 Encryption   : none                    Hashing      : none
```

```
Auth Mode     : msCHAPV2

Idle Time Out: 30 Minutes            Idle TO Left : 27 Minutes
Client OS     : Microsoft
Client OS Ver: 6.2
Bytes Tx      : 475                  Bytes Rx     : 9093
Pkts Tx       : 18                   Pkts Rx      : 105
```

Op ASDM, onder **Controle > VPN > VPN Statistieken > Sessies** kan de algemene informatie over de VPN-sessie worden gezien. L2TP-over-IPsec sessies kunnen worden gefilterd door **IPsec (IKEv1) externe toegang > Protocol > L2TP via IPsec**.



# Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

> Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

> **Voorzichtig:** Op de ASA kun je verschillende debug-niveaus instellen. standaard wordt niveau 1 gebruikt. Als u het debug-niveau wijzigt, kan de breedtegraad van de insecten toenemen. Doe dit met voorzichtigheid, vooral in productieomgevingen!

Gebruik de volgende **debug-opdrachten** met **voorzichtigheid** om problemen met VPN-tunnelproblemen op te lossen

- **debug crypto ikev1** - toont debug-informatie over IKE
- **debug crypto ipsec** - hiermee wordt debug-informatie over IPsec weergegeven

Hier is de debug uitvoer voor een succesvolle L2TP via een IPSec-verbinding:

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NONE (0) total length : 408
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
```

```
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Oakley proposal is acceptable
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal RFC VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received Fragmentation VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,
```

**IKE SA Proposal # 1, Transform # 5 acceptable  Matches global IKE entry # 2**

```
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended
capabilities payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA_KE payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1]IP = 10.1.1.2,
```

**Connection landed on tunnel_group DefaultRAGroup**

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for
Responder...
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D
(20) + NONE (0) total length : 304
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
```

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 64
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

**Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device**

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel_group DefaultRAGroup
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

**PHASE 1 COMPLETED**

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keep-alives (type = None)
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer: 21600 seconds.
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

**Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701**

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 172.16.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

**Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701**

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

**L2TP/IPSec session detected.**

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

**Static Crypto Map check, map outside_dyn_map, seq = 10 is a successful match**

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside_dyn_map
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPSec SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I

**PSec SA Proposal # 2, Transform # 1 acceptable**

  Matches global IPSec SA entry # 10
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
   Direction: inbound
   SPI      : 0x7AD72E0D
   Session ID: 0x00001000
   VPIF num  : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine: SPI = 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constucting quick mode
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec nonce payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,

**Transmitting Proxy Id:**

  **Remote host: 10.1.1.2  Protocol 17  Port 1701**

  **Local host:  172.16.1.2  Protocol 17  Port 1701**

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd QM pkt: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + NONE (0) total length : 52
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;

```
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x00007fffe1c75c00,
   SCB: 0xE13ABD20,
   Direction: outbound
   SPI      : 0x8C14FD70
   Session ID: 0x00001000
   VPIF num  : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x8C14FD70
IPSEC: Creating outbound VPN context, SPI 0x8C14FD70
   Flags: 0x00000205
   SA   : 0x00007fffe1c75c00
   SPI  : 0x8C14FD70
   MTU  : 1500 bytes
   VCID : 0x00000000
   Peer : 0x00000000
   SCB  : 0x0AC609F9
   Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
   VPN handle: 0x00000000000028d4
IPSEC: New outbound encrypt rule, SPI 0x8C14FD70
   Src addr: 172.16.1.2
   Src mask: 255.255.255.255
   Dst addr: 10.1.1.2
   Dst mask: 255.255.255.255
```

**Src ports**

**Upper: 1701**

**Lower: 1701**

Op   : equal

**Dst ports**

**Upper: 1701**

**Lower: 1701**

Op   : equal

**Protocol: 17**

```
   Use protocol: true
   SPI: 0x00000000
   Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
   Src addr: 172.16.1.2
   Src mask: 255.255.255.255
   Dst addr: 10.1.1.2
   Dst mask: 255.255.255.255
   Src ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Dst ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x8C14FD70
   Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User ()  Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
   Direction: inbound
   SPI      : 0x7AD72E0D
   Session ID: 0x00001000
   VPIF num  : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
   Flags: 0x00000206
   SA   : 0x00007fffe13ab260
   SPI  : 0x7AD72E0D
   MTU  : 0 bytes
   VCID : 0x00000000
   Peer : 0x000028D4
   SCB  : 0x0AC5BD5B
   Channel: 0x00007fffed817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
   VPN handle: 0x0000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
   Flags: 0x00000205
   SA   : 0x00007fffe1c75c00
   SPI  : 0x8C14FD70
   MTU  : 1500 bytes
   VCID : 0x00000000
```

```
   Peer : 0x00004174
   SCB  : 0x0AC609F9
   Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
   VPN handle: 0x00000000000028d4
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c763d0
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c76a00
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   Dst mask: 255.255.255.255
   Src ports
     Upper: 1701
     Lower: 1701
     Op   : equal
   Dst ports
     Upper: 1701
     Lower: 1701
     Op   : equal
   Protocol: 17
   Use protocol: true
   SPI: 0x00000000
   Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe13aba90
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   Dst mask: 255.255.255.255
   Src ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Dst ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x7AD72E0D
   Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe1c77420
IPSEC: New inbound permit rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   Dst mask: 255.255.255.255
   Src ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Dst ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x7AD72E0D
   Use SPI: true
```

```
IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe13abb80
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received
KEY_UPDATE, spi 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer:
3420 seconds.
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

**PHASE 2 COMPLETED**

```
 (msgid=00000001)
May 18 04:17:18 [IKEv1]IKEQM_Active() Add L2TP classification rules: ip <10.1.1.2> mask
<0xFFFFFFFF> port <1701>
May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,
```

**Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1**

Sommige vaak voorkomende VPN-gerelateerde fouten op Windows-client worden in deze tabel weergegeven

| Foutcode | Mogelijke oplossing |
|---|---|
| 691 | Zorg ervoor dat de gebruikersnaam en het wachtwoord juist waren ingevoerd |
| 789,835 | Zorg ervoor dat de vooraf gedeelde toets die op de clientmachine is ingesteld, gelijk is aan die o ASA |
| 800 | 1. Controleer of het VPN-type is ingesteld op "Layer 2 Tunneling Protocol (L2TP)"<br>2. Zorg ervoor dat de voorgedeelde toets correct is geconfigureerd |
| 809 | Zorg ervoor dat UDP-poort 500, 4500 (indien client of server achter NAT-apparaat staat) en dat verkeer niet is geblokkeerd |

# Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties
- Populairste oplossingen voor IPsec gemeenschappelijk L2L en Remote Access IPsec VPN-probleemoplossing
- Technische ondersteuning en documentatie – Cisco Systems