

ASA/PIX: Split-tunneling voor VPN-clients toestaan in het ASA Configuration-voorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Verwante producten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Split-tunneling op ASA configureren](#)

[ASA 7.550x configureren met adaptieve security applicatie Manager \(ASDM\) 5.x](#)

[ASA 8.500x configureren met adaptieve security applicatie Manager \(ASDM\) 6.x](#)

[ASA 7.x en hoger configureren via CLI](#)

[PIX 6.x configureren via CLI](#)

[Verifiëren](#)

[Connect met VPN-client](#)

[Bekijk het VPN-clientlogboek](#)

[Lokale LAN-toegang testen met Ping](#)

[Problemen oplossen](#)

[Beperking met aantal ingangen in een splitter-tunnelleiding](#)

[Gerelateerde informatie](#)

Inleiding

Dit document bevat stap-voor-stap instructies over hoe u VPN-clients toegang tot het internet kunt geven terwijl ze in een Cisco adaptieve security applicatie (ASA) 5500 Series security applicatie zijn verbonden. Deze configuratie maakt VPN-clients veilig toegang tot bedrijfsmiddelen via IPsec mogelijk terwijl u onbeveiligde toegang tot het internet hebt.

Opmerking: Een volledige tunneling wordt gezien als de meest beveiligde configuratie omdat geen gelijktijdige toegang tot zowel internet als LAN door het apparaat mogelijk is. Een compromis tussen een volledige tunneling en een gesplitste tunneling maakt de lokale LAN-toegang van VPN-clients alleen mogelijk. Raadpleeg [PIX/ASA 7.x: Lokaal LAN-toegang voor VPN-clients toestaan. Configuratievoorbeeld](#) voor meer informatie.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat er al een werkende VPN-configuratie voor externe toegang op de ASA bestaat. Raadpleeg [PIX/ASA 7.x als een externe VPN-server met ASDM Configuration Voorbeeld](#) als deze niet al is geconfigureerd.

Gebruikte componenten

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

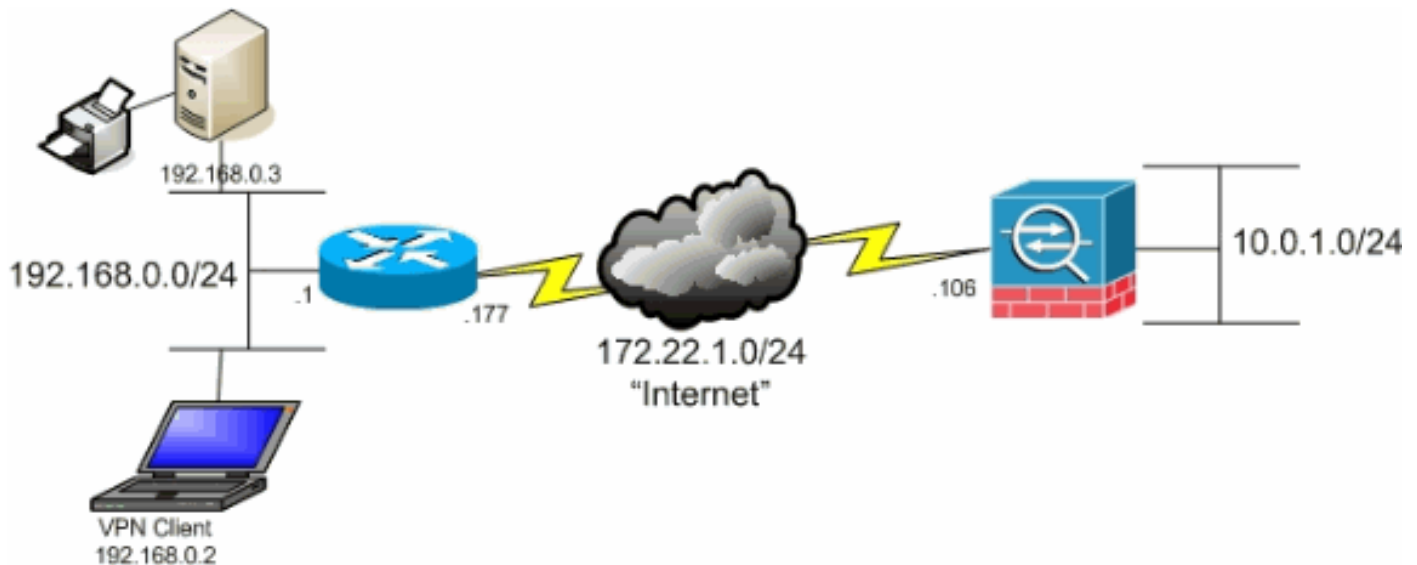
- Cisco ASA 5500 Series security applicatie, versie 7.x en hoger
- Cisco Systems VPN-clientversie 4.0.5

Opmerking: Dit document bevat ook de PIX 6.x CLI-configuratie die compatibel is voor Cisco VPN-client 3.x.

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.

Netwerkdigram

De VPN-client is gevestigd op een typisch SOHO-netwerk en sluit zich via het internet aan op het hoofdkantoor.



Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco PIX 500 Series security applicatie, versie 7.x.

Conventies

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

Achtergrondinformatie

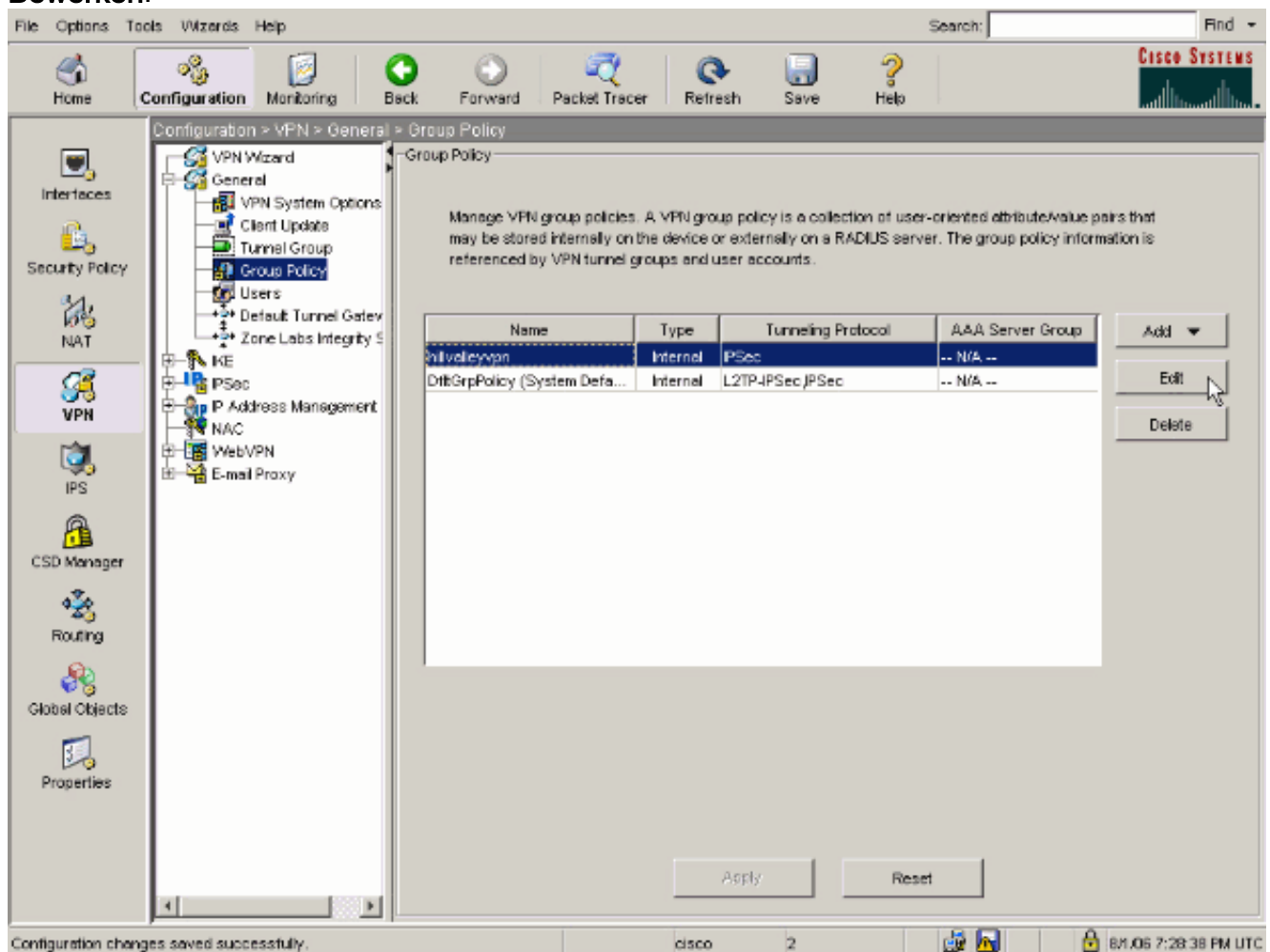
In een basisscenario van VPN-client naar ASA wordt al het verkeer van de VPN-client versleuteld en naar de ASA verzonden, ongeacht de bestemming ervan. Op basis van uw configuratie en het aantal ondersteunde gebruikers kan een dergelijke installatie bandbreedte-intensief worden. Split-tunneling kan dit probleem helpen verminderen aangezien het gebruikers alleen dat verkeer dat voor het bedrijfsnetwerk over de tunnel bestemd is, laat verzenden. Al het andere verkeer, zoals onmiddellijk overseinen, e-mail of willekeurig bladeren, wordt naar het internet verzonden via het lokale LAN van de VPN-client.

Split-tunneling op ASA configureren

ASA 7.550x configureren met adaptieve security applicatie Manager (ASDM) 5.x

Voltooi deze stappen om uw tunnelgroep te configureren om een gesplitste tunneling voor de gebruikers in de groep toe te staan.

1. Kies **Configuratie > VPN > Algemeen > Groepsbeleid** en selecteer het groepsbeleid dat u lokale LAN-toegang in wilt schakelen. Klik vervolgens op **Bewerken**.

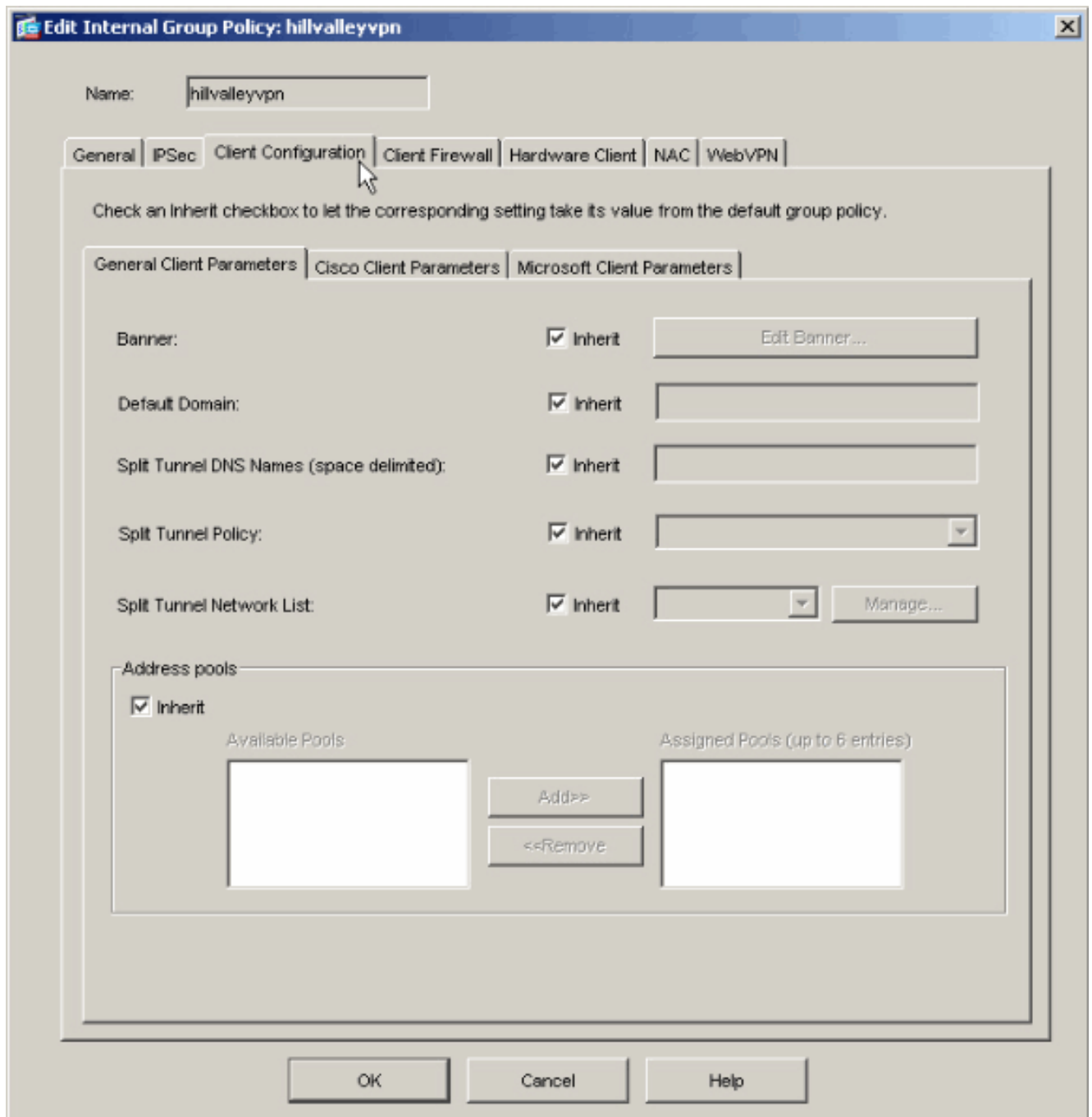


The screenshot shows the Cisco ASDM 5.x configuration interface. The navigation pane on the left is set to **VPN > Algemeen > Groepsbeleid**. The main configuration area displays the **Group Policy** configuration page. A table lists the configured policies:

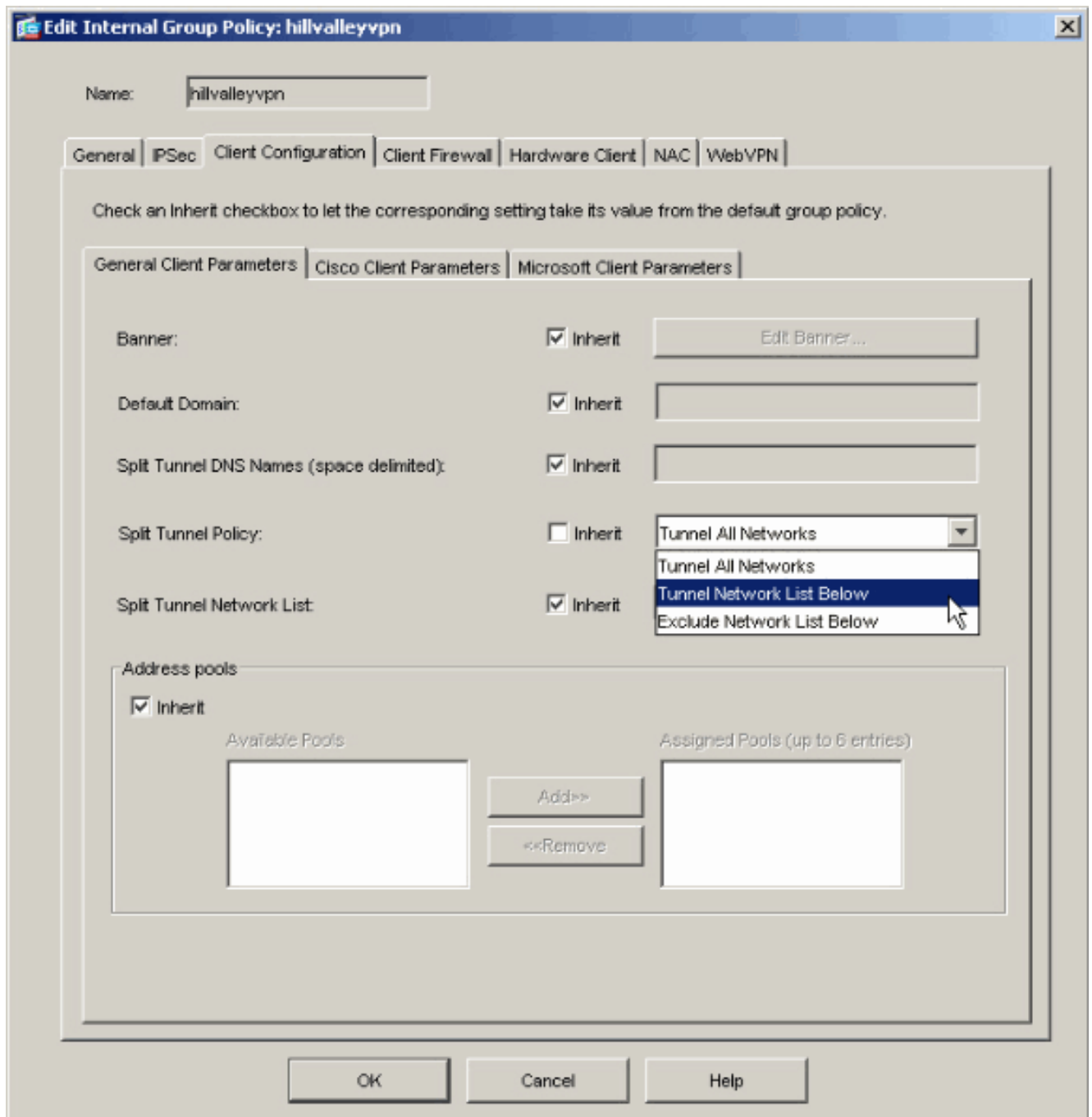
Name	Type	Tunneling Protocol	AAA Server Group
invalleyvpn	Internal	IPSec	-- N/A --
DfltGrpPolicy (System Defa...	Internal	L2TP/IPSec/JPsec	-- N/A --

Buttons for **Add**, **Edit**, and **Delete** are visible to the right of the table. The **Edit** button is highlighted by the mouse cursor. At the bottom of the configuration area, there are **Apply** and **Reset** buttons. The status bar at the bottom indicates "Configuration changes saved successfully."

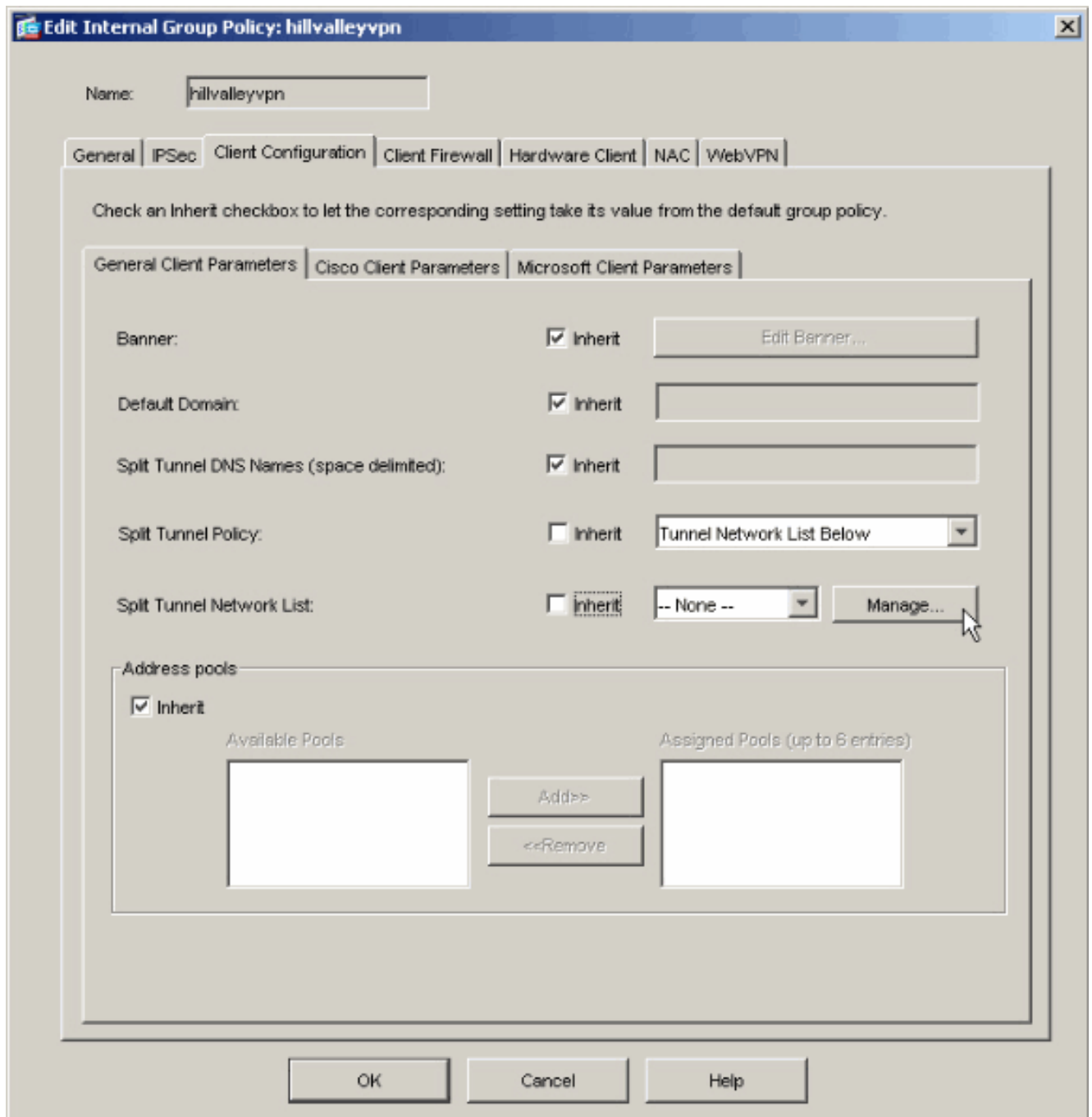
2. Ga naar het tabblad **Clientconfiguratie**.



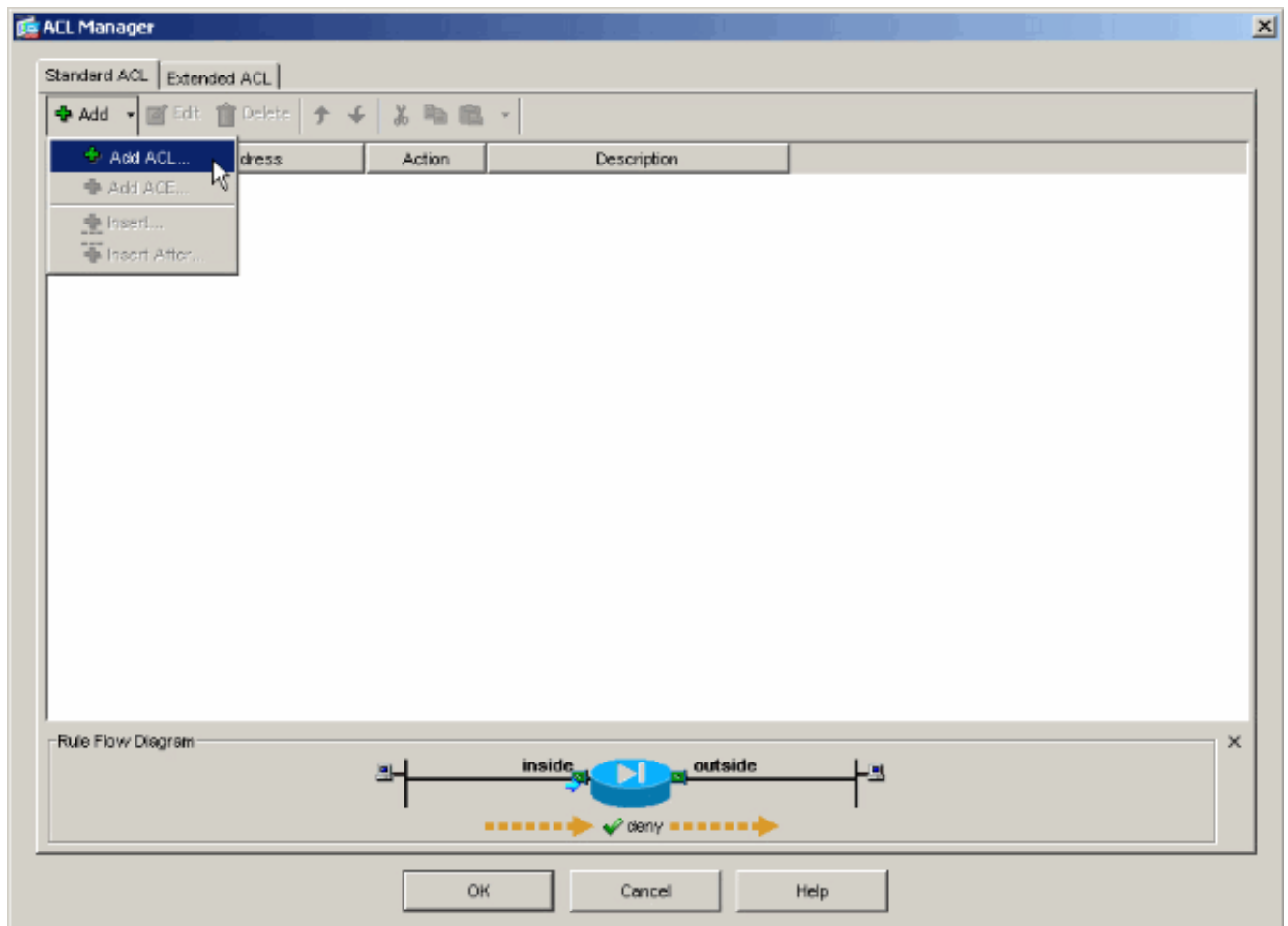
- Schakel het vakje **Inherit** voor Split Tunnel Policy uit en kies **de onderstaande** lijst met tunnelnetwerken.



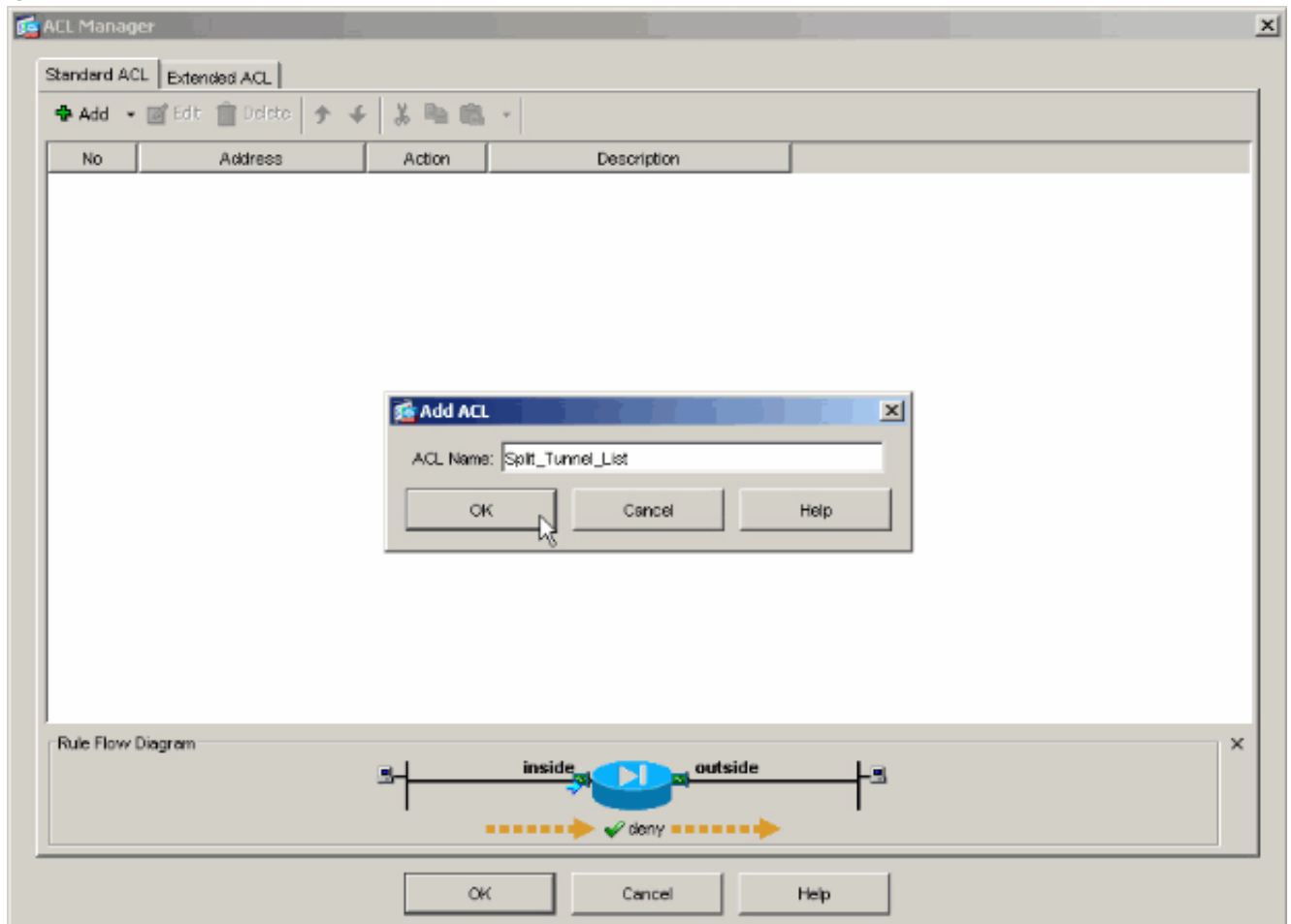
4. Schakel het vakje Inherit uit voor de netwerklijst met splitter en klik vervolgens op **Bewerken** om de ACL-Manager te starten.



5. Kies in de ACL Manager **Add > Add ACL...** om een nieuwe toegangslijst te maken.

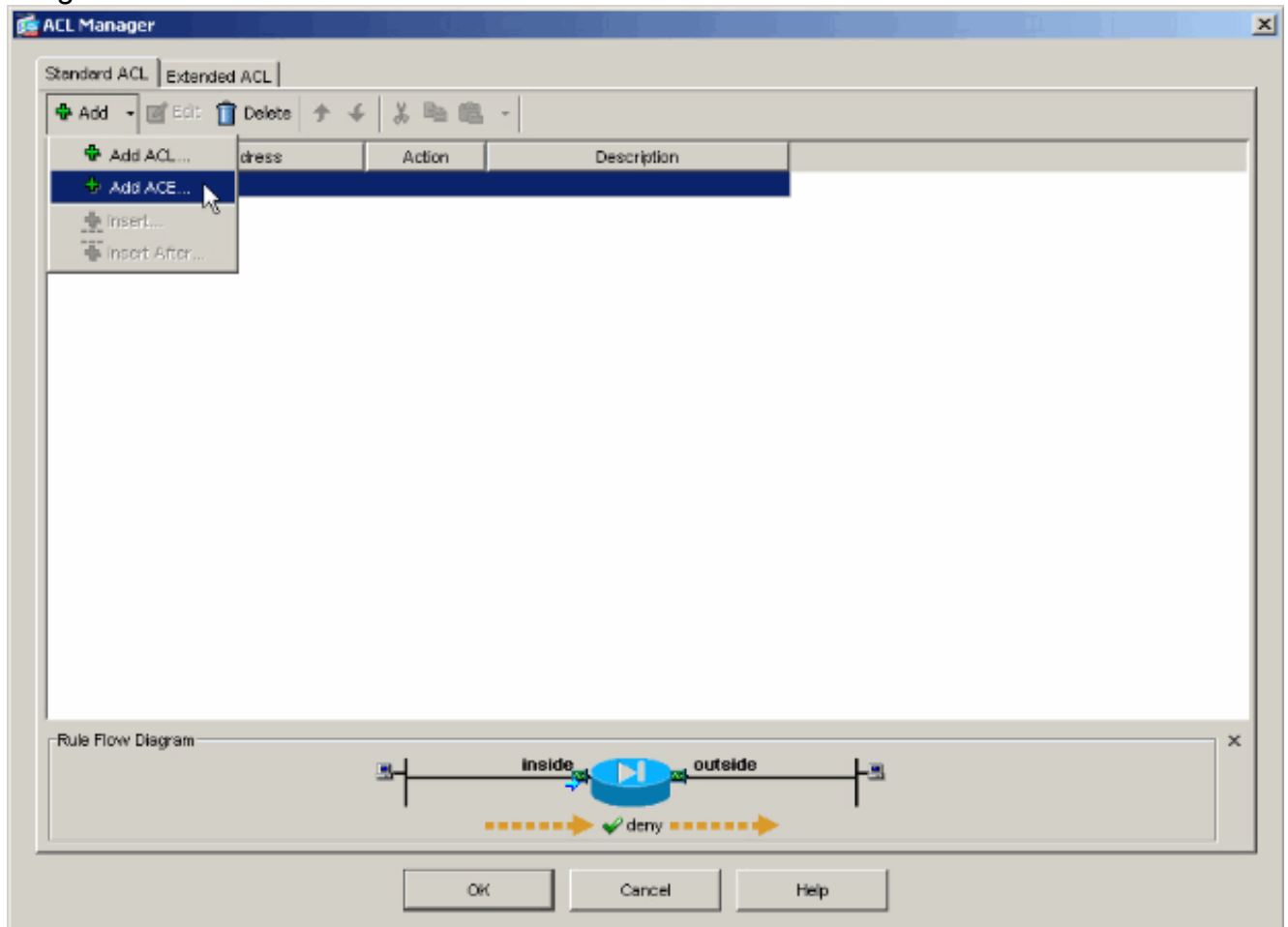


6. Typ een naam voor ACL en klik op OK.

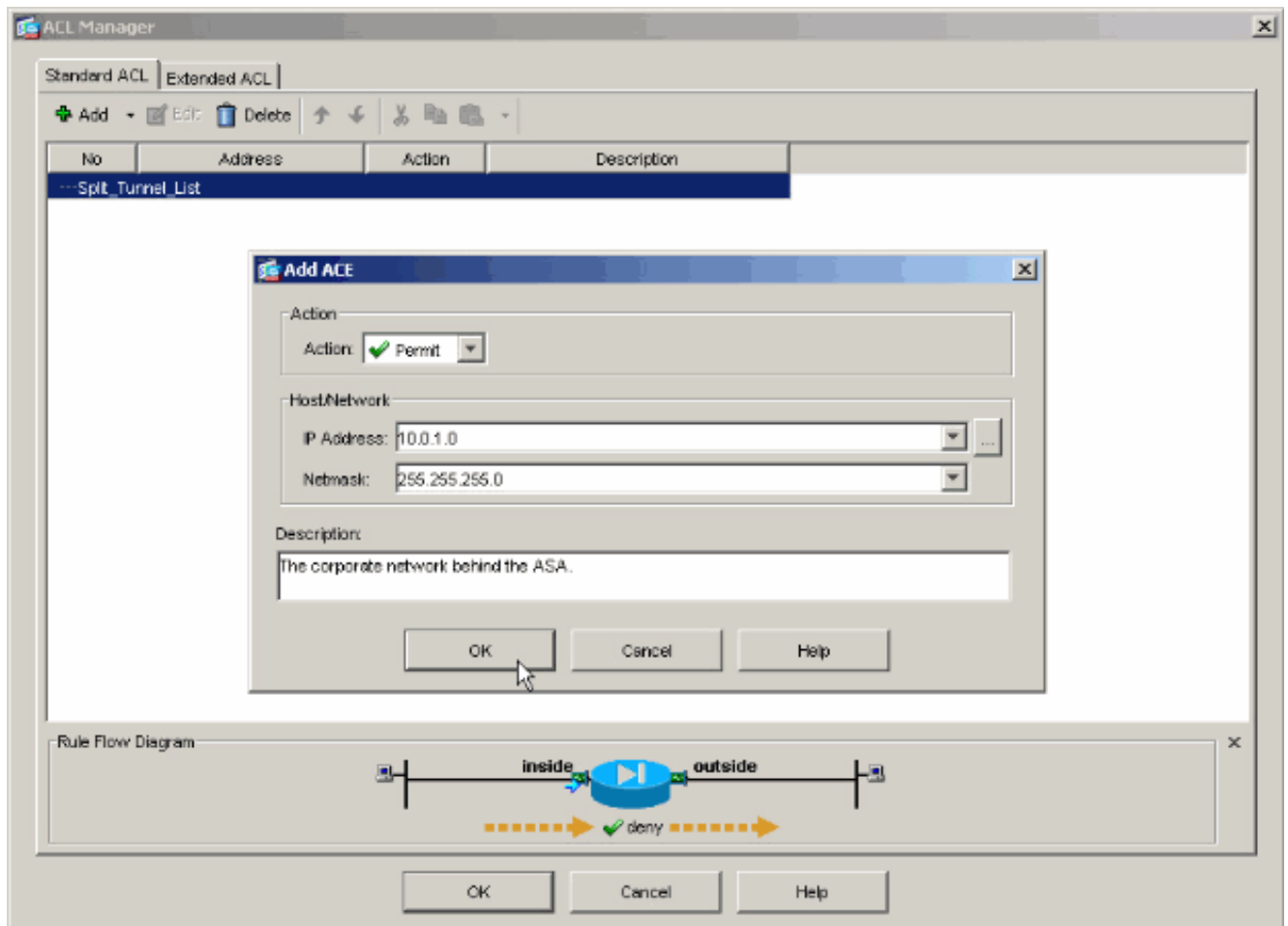


7. Zodra ACL wordt gecreëerd, kies **Add > Add ACE...** om een Access Control Entry (ACE) toe

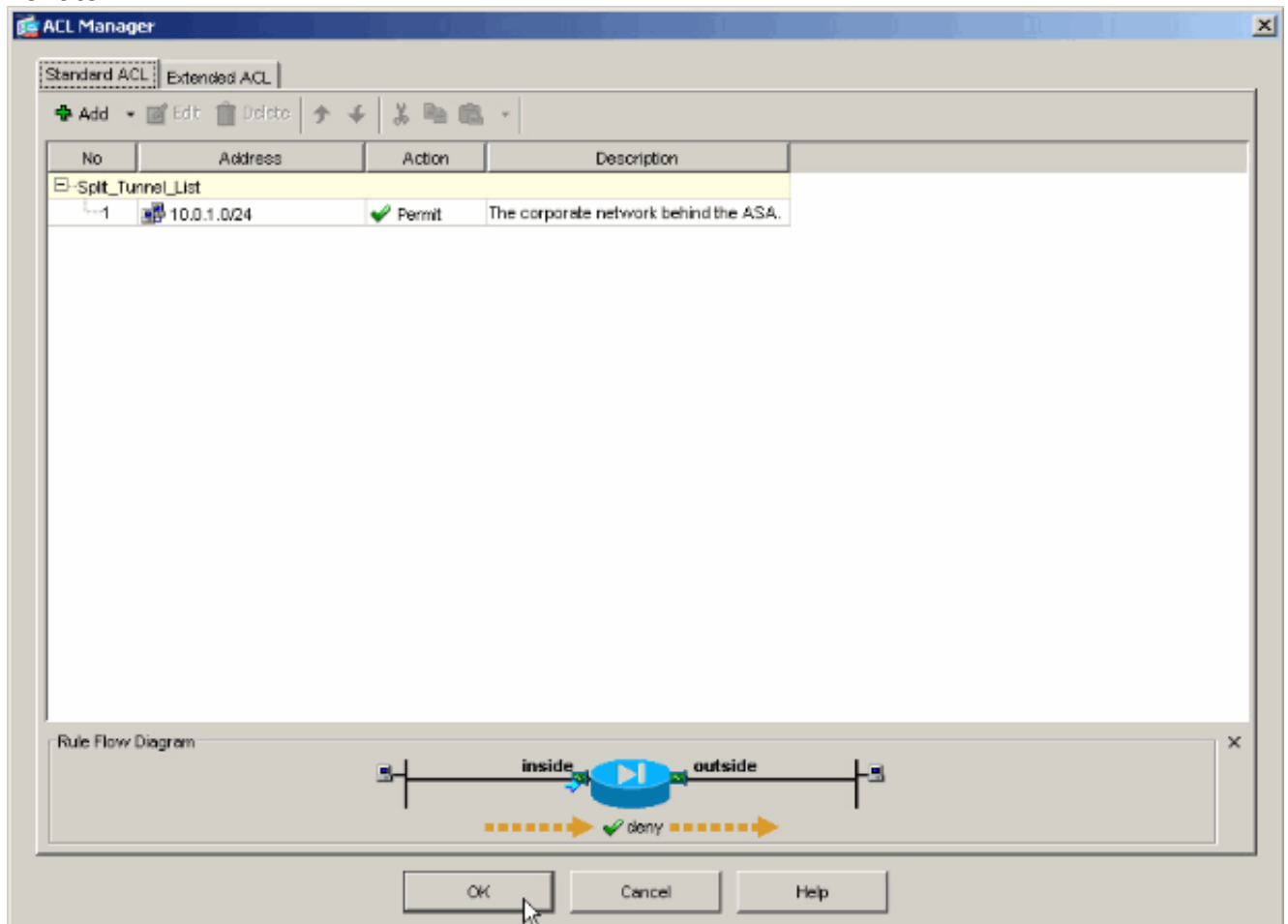
te
voegen.



8. Definieer de ACE die overeenkomt met het LAN achter de ASA. In dit geval is het netwerk 10.0.1.0/24. Kies **Toestemming**. Kies een IP-adres van 10.0.1.0. Kies een netwerkmasker van 255.255.255.0. (Optioneel) Geef een beschrijving. Klik op OK.

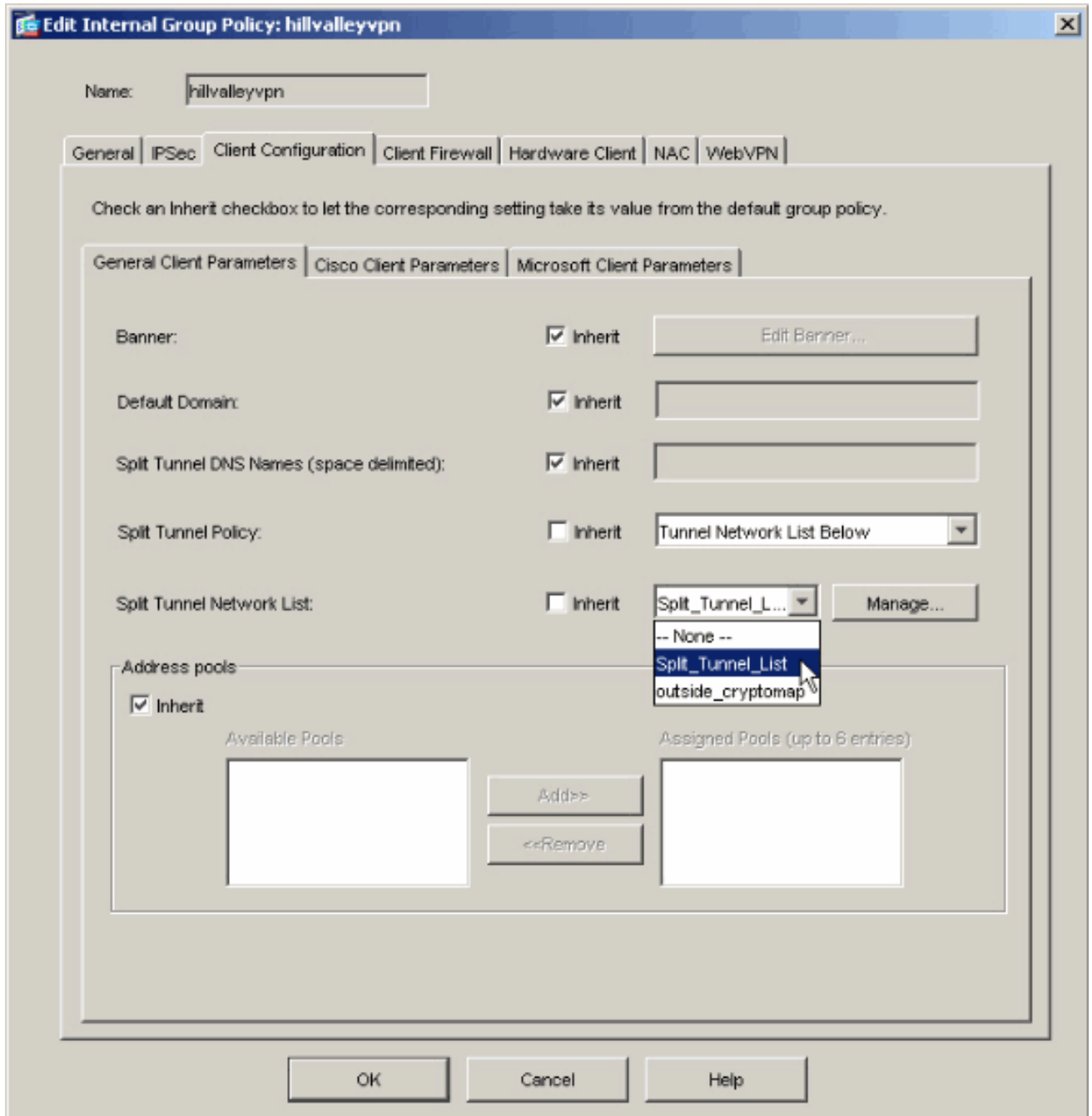


9. Klik op OK om de ACL-Manager te verlaten.

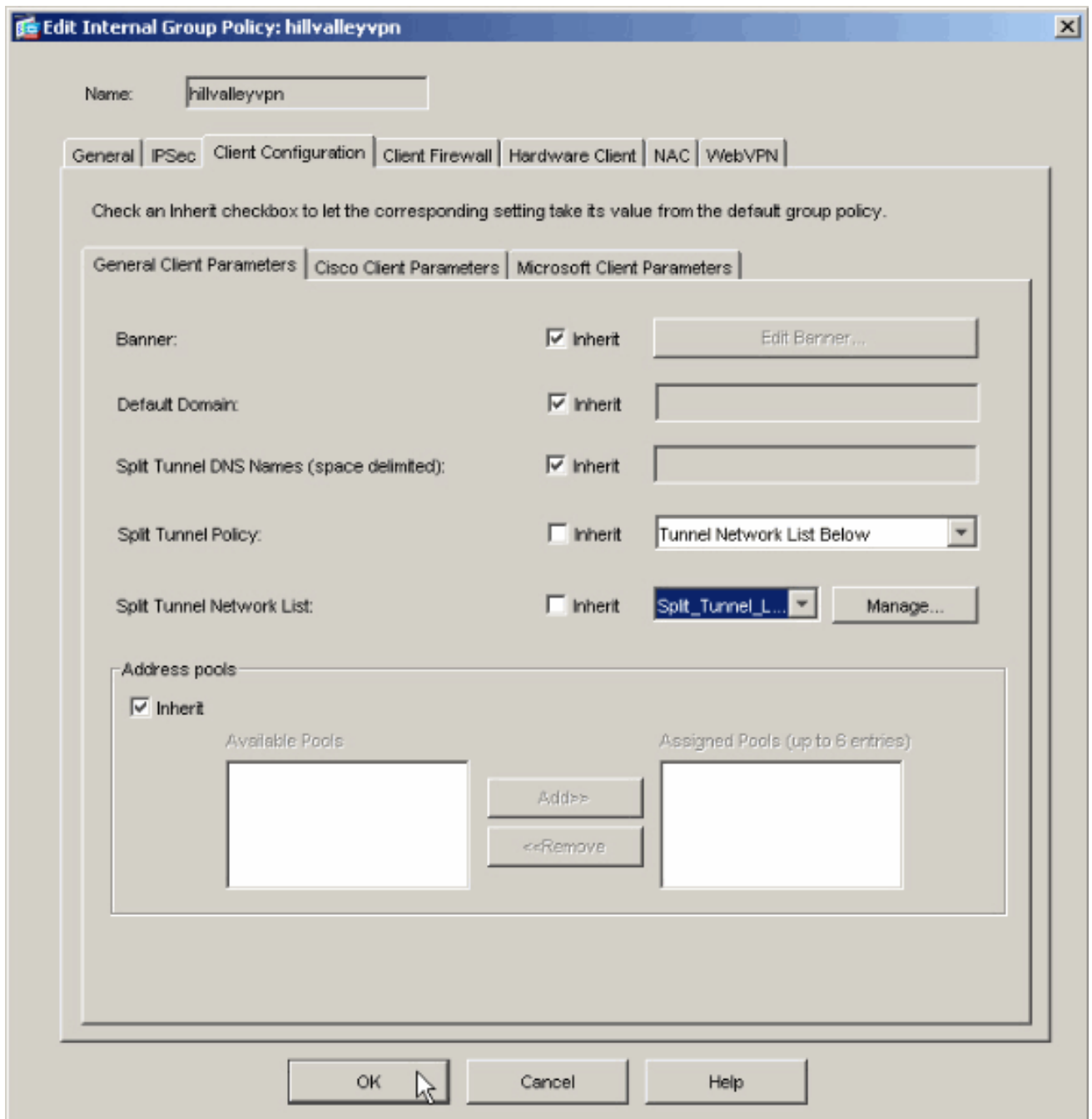


10. Verzeker u dat ACL die u zojuist hebt gemaakt, is geselecteerd voor Split Tunnel Network

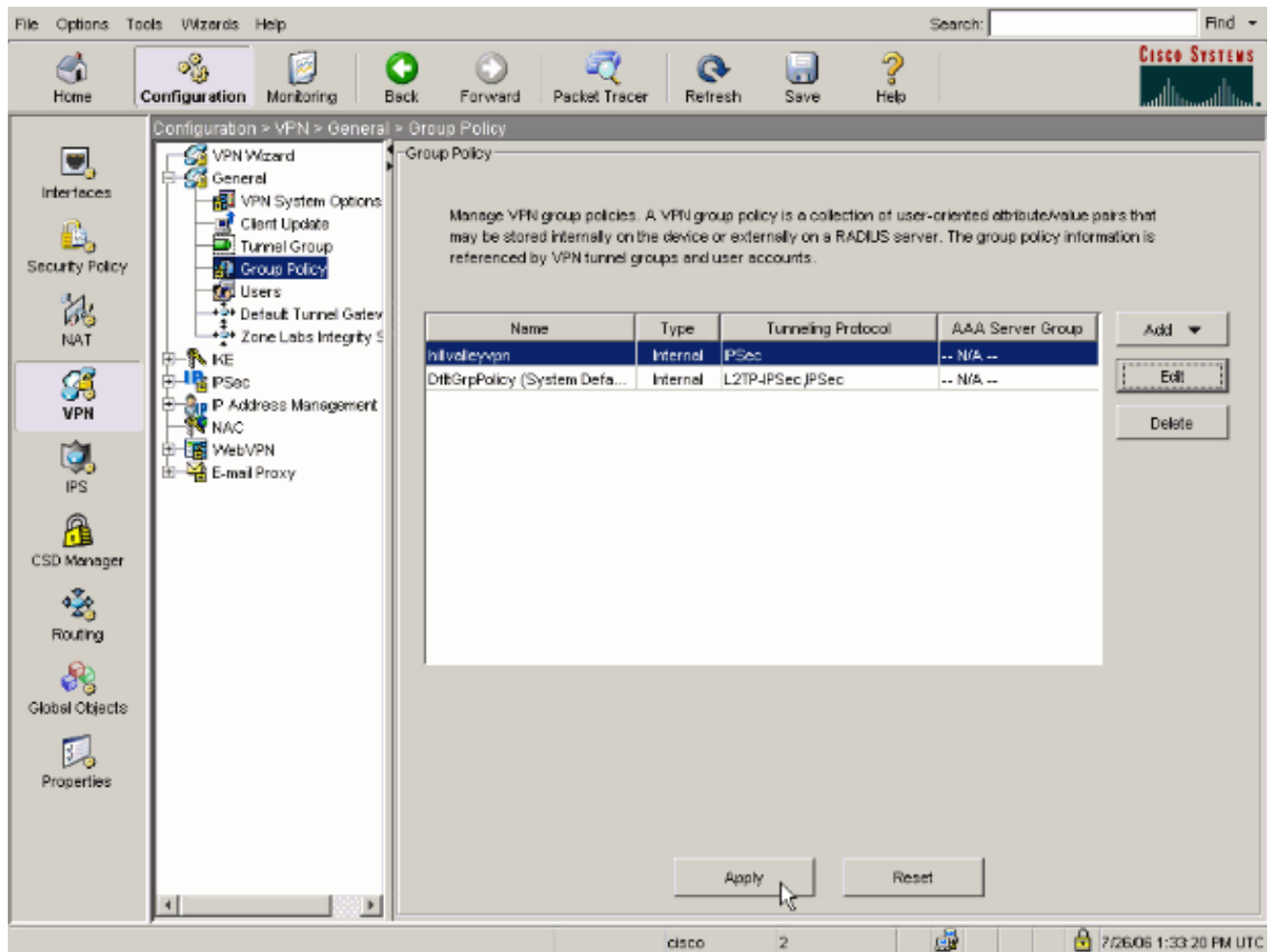
List.



11. Klik op **OK** om naar de configuratie van het groepsbeleid terug te keren.



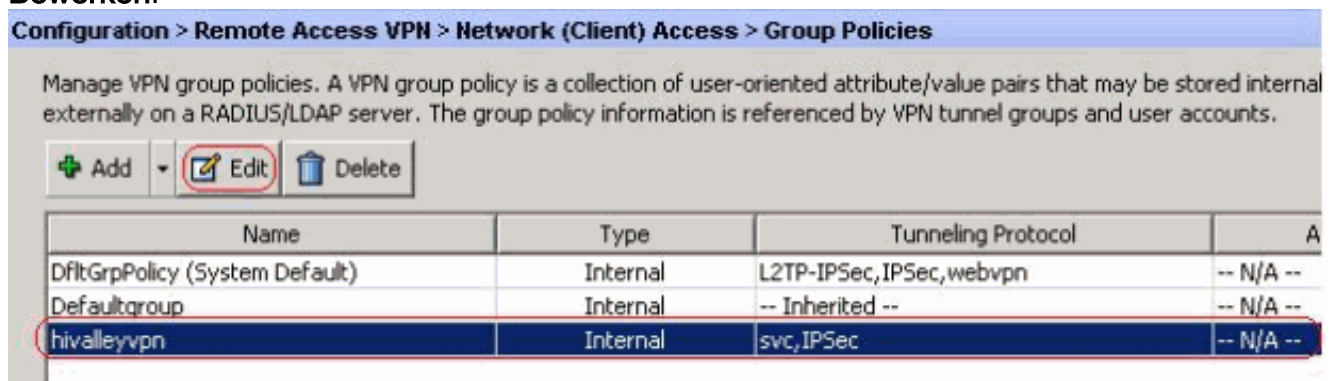
12. Klik op **Toepassen** en **Verzend** (indien nodig) om de opdrachten naar de ASA te sturen.



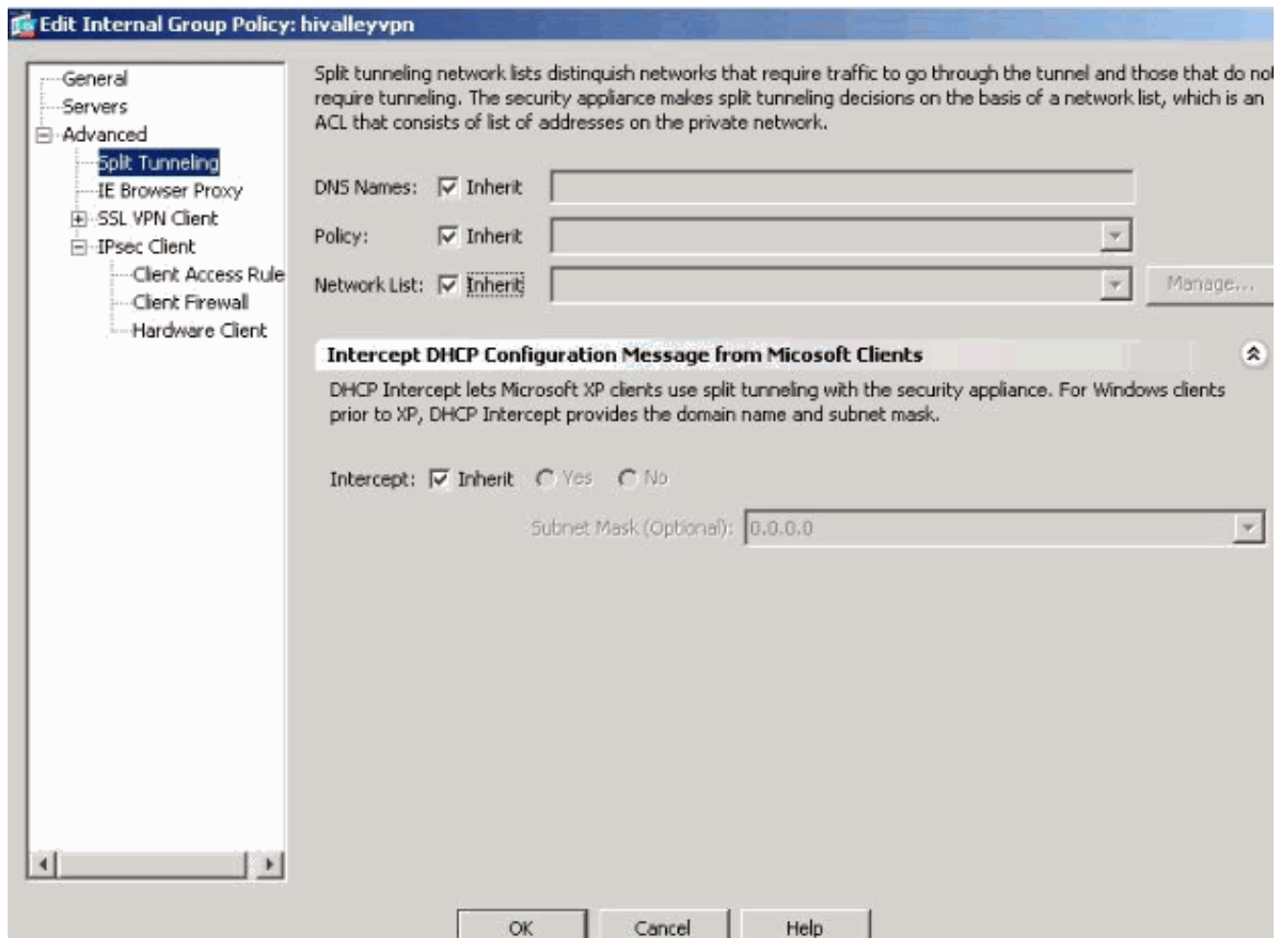
[ASA 8.500x configureren met adaptieve security applicatie Manager \(ASDM\) 6.x](#)

Voltooi deze stappen om uw tunnelgroep te configureren om een gesplitste tunneling voor de gebruikers in de groep toe te staan.

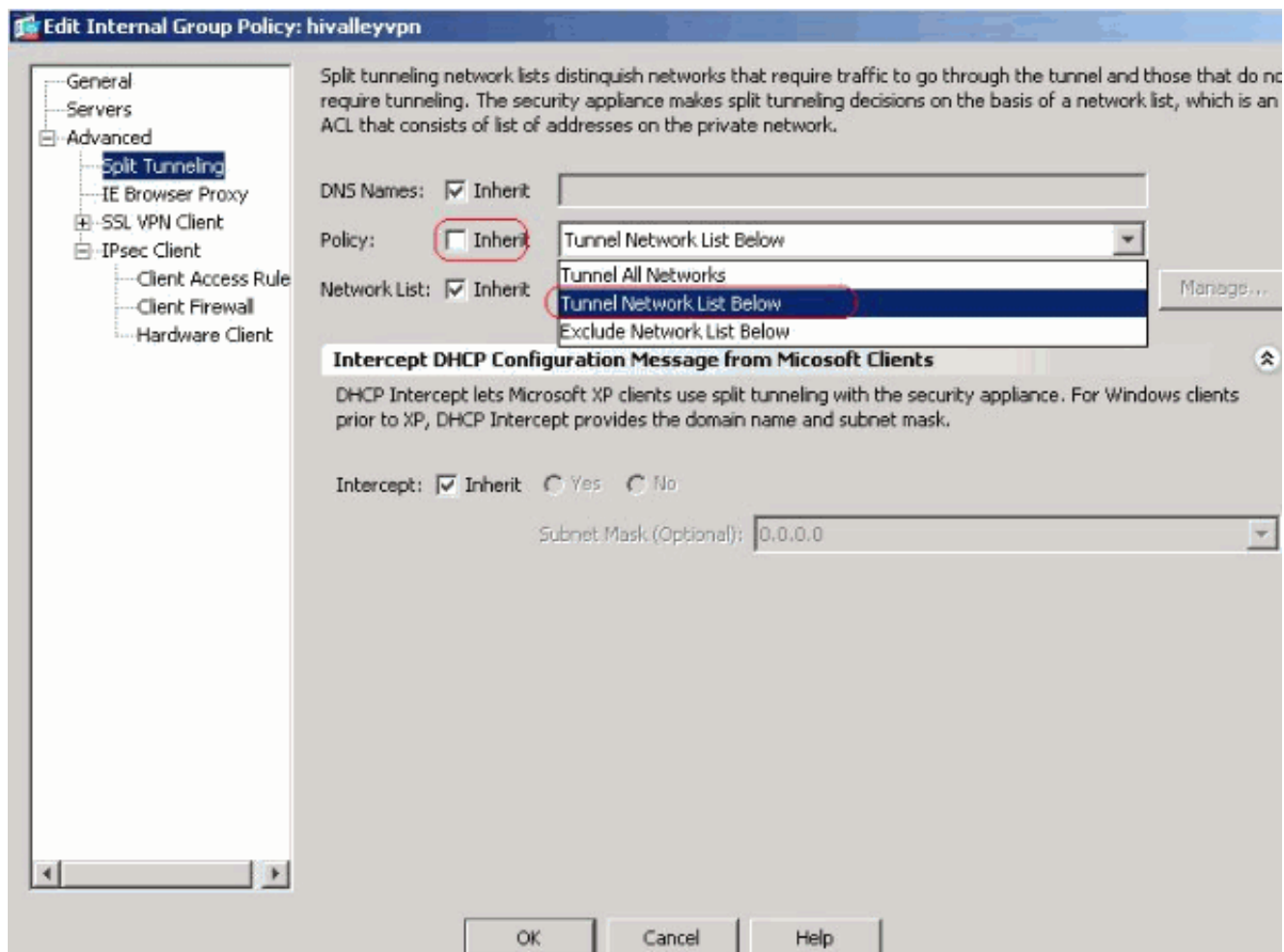
1. Kies **Configuration > Remote Access VPN > Network (Client) Access > Group Policy** en kies het groepsbeleid waarin u lokale LAN-toegang wilt inschakelen. Klik vervolgens op **Bewerken**.



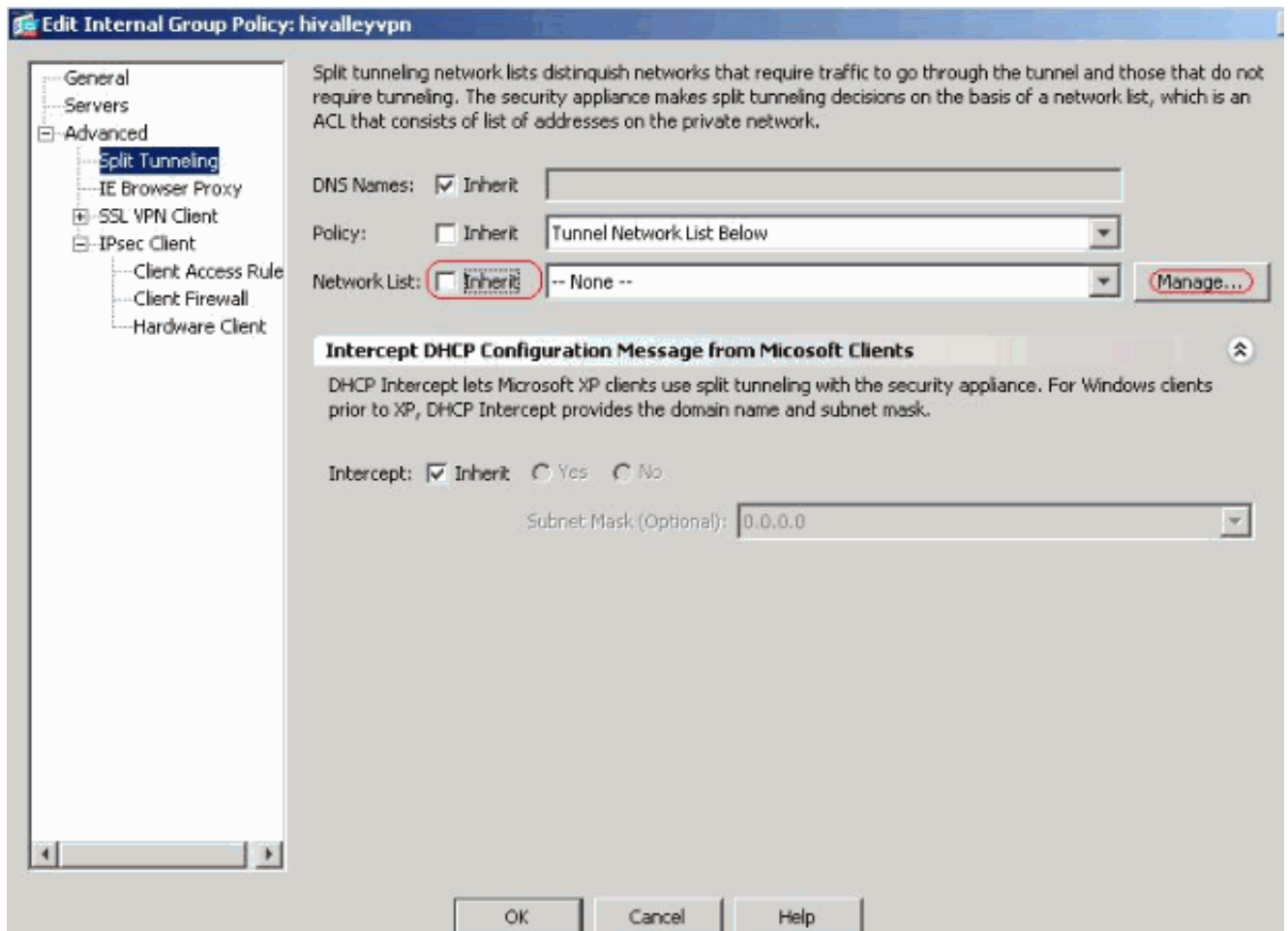
2. Klik op **Tunneling splitsen**.



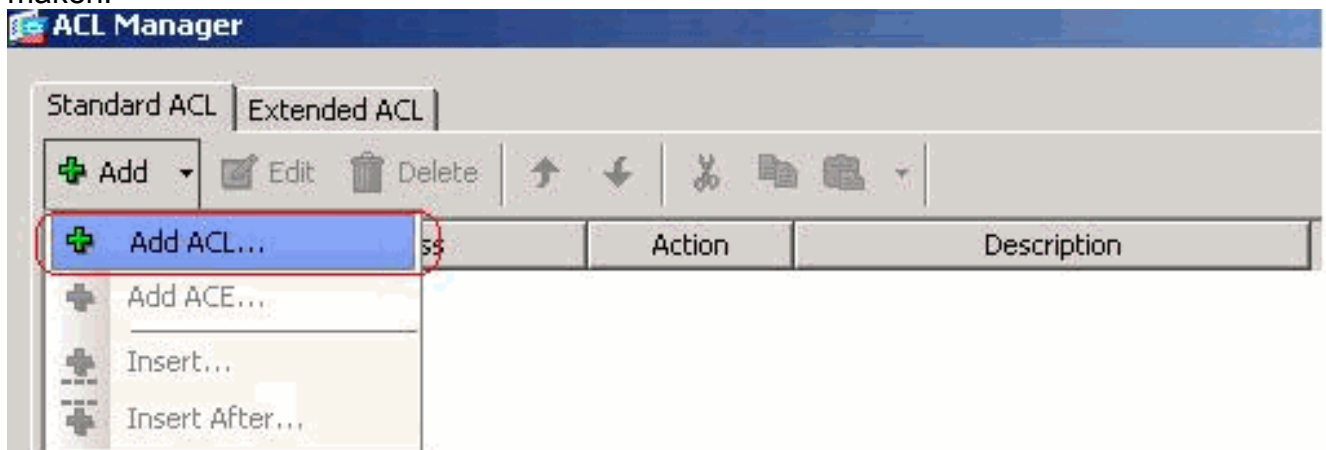
- Schakel het vakje **Inherit** voor Split Tunnel Policy uit en kies **de onderstaande lijst met tunnelnetwerken**.



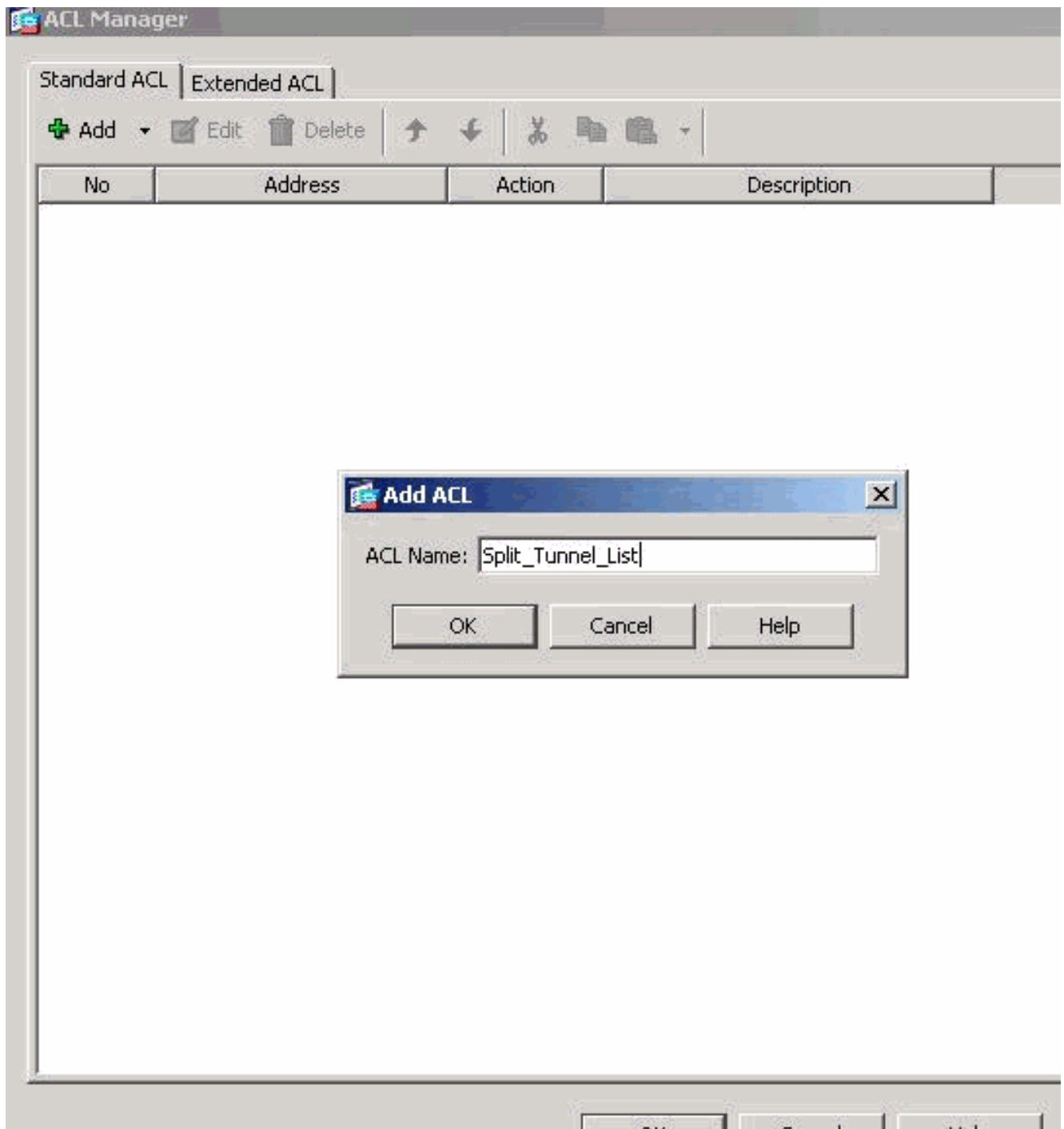
4. Schakel het vakje **Inherit** uit voor de netwerklijst Split Tunnel en klik vervolgens op **Bewerken** om de ACL Manager te starten.



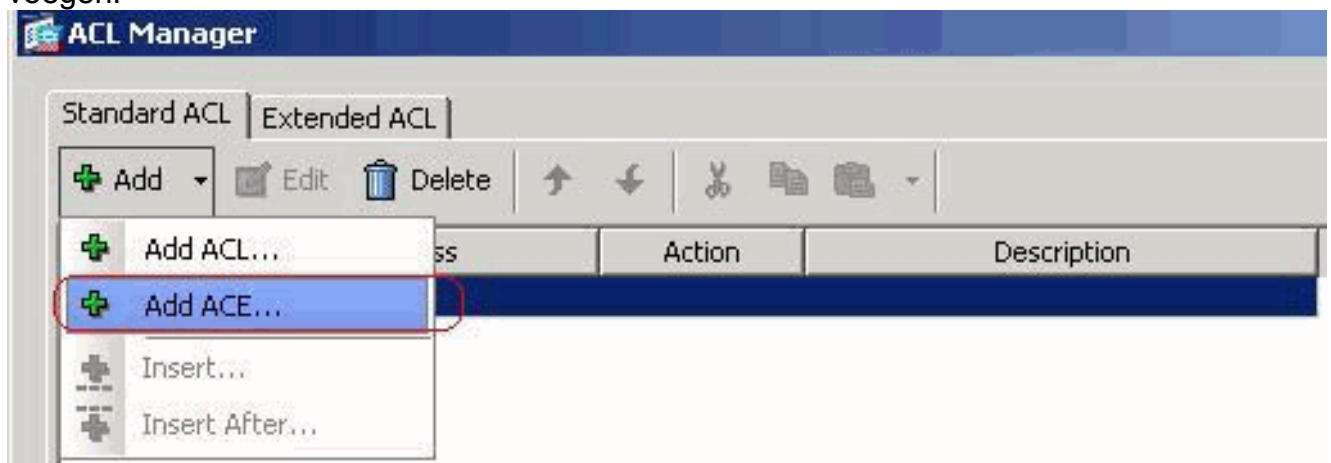
5. Kies in de ACL Manager **Add > Add ACL...** om een nieuwe toegangslijst te maken.



6. Typ een naam voor ACL en klik op **OK**.

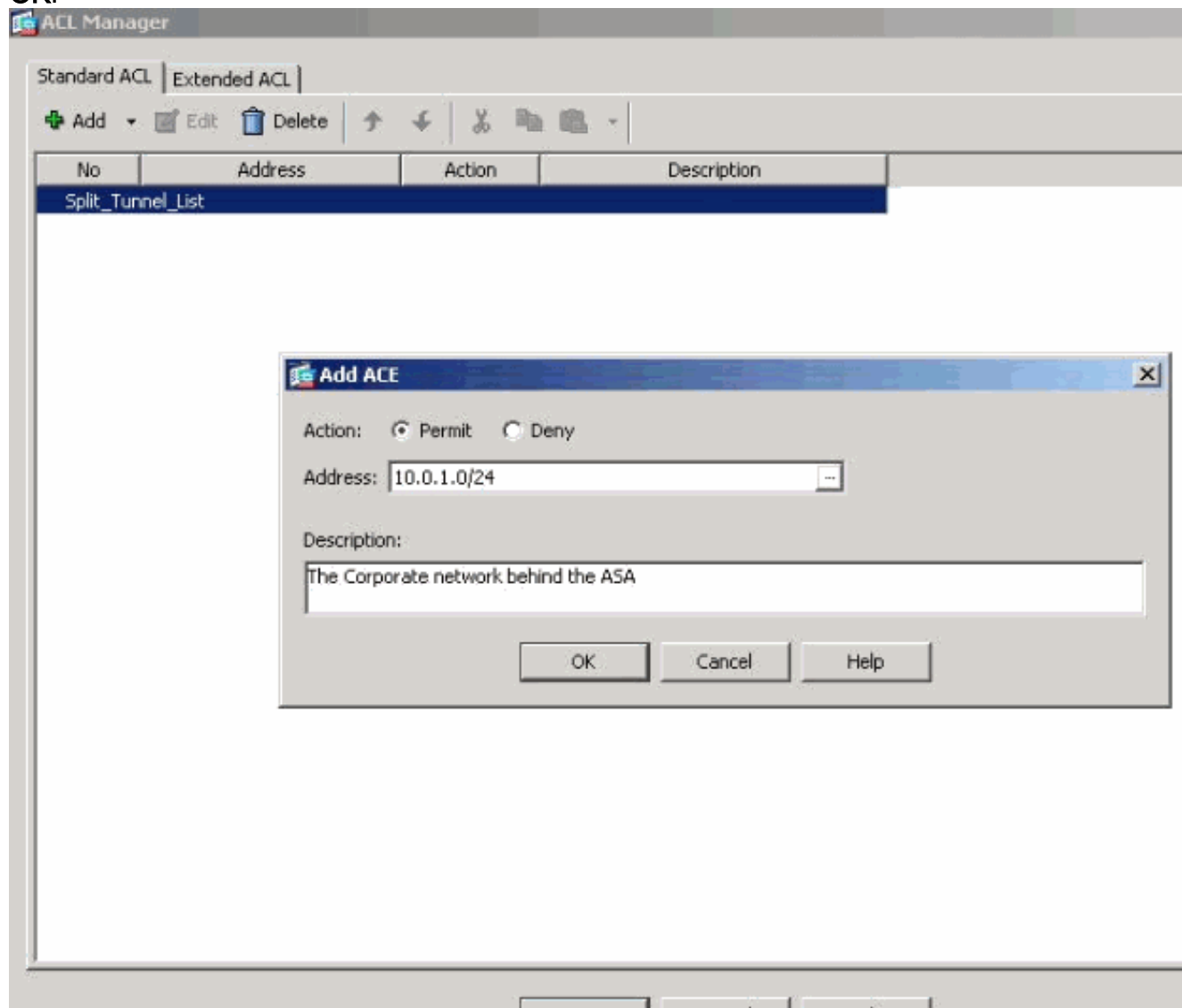


7. Zodra ACL wordt gecreëerd, kies **Add > Add ACE...** om een Access Control Entry (ACE) toe te voegen.

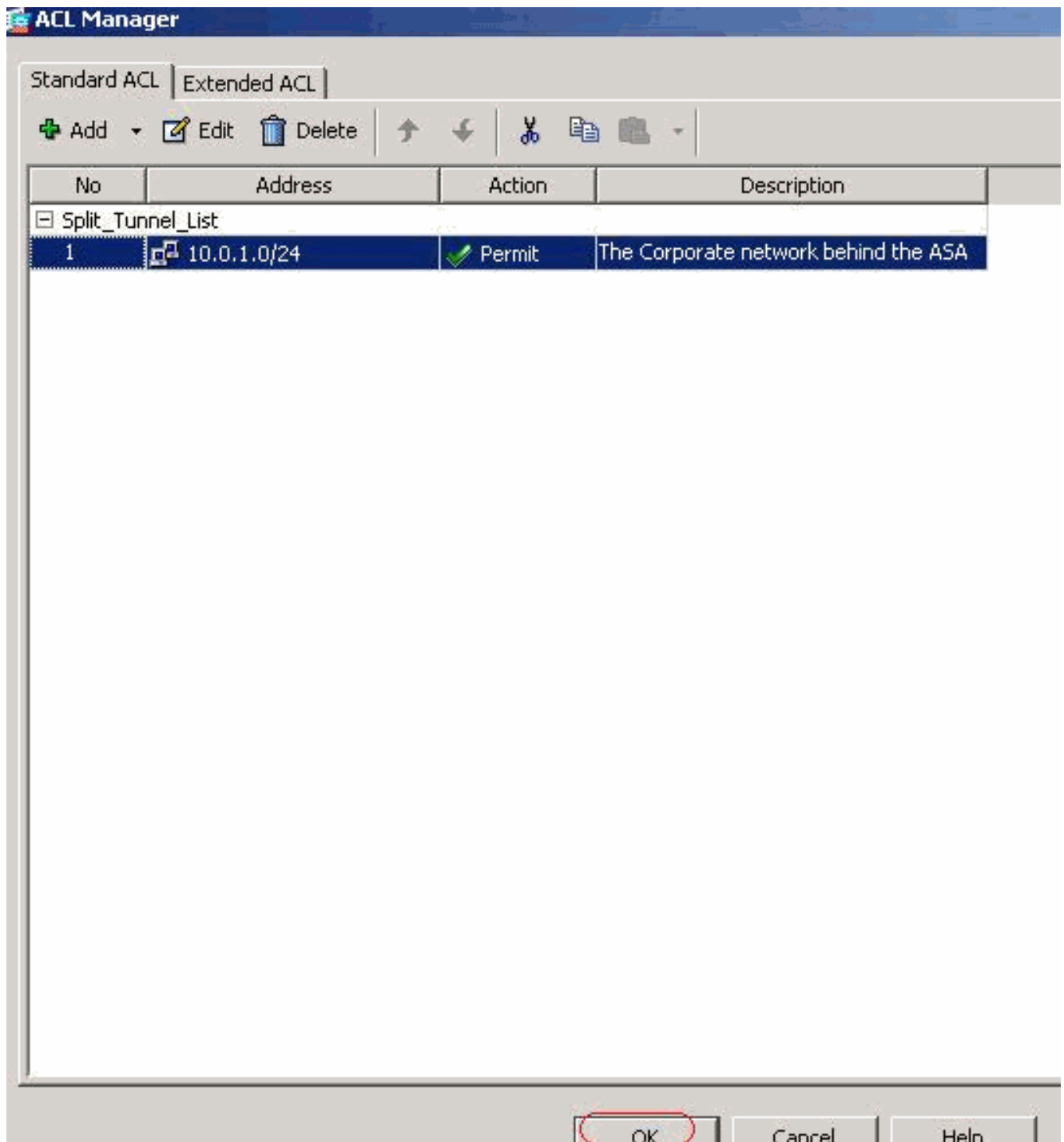


8. Definieer de ACE die overeenkomt met het LAN achter de ASA. In dit geval is het netwerk

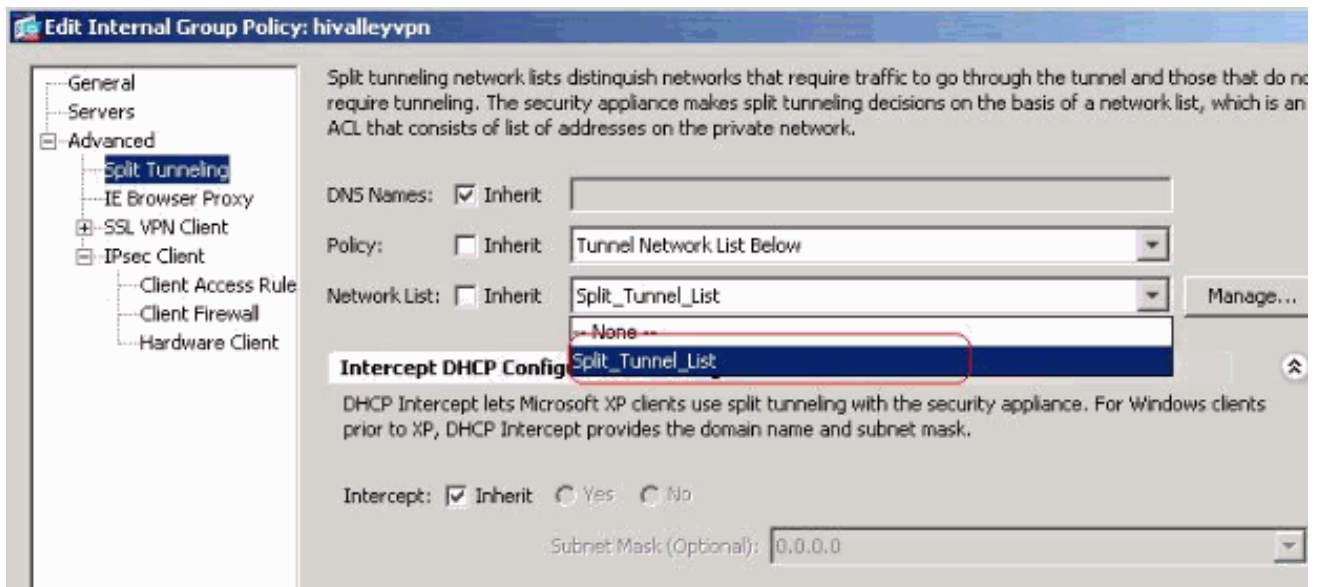
10.0.1.0/24. Klik op de radioknop **Toestemming**. Kies het netwerkadres met masker **10.0.1.0/24**. (Optioneel) Geef een beschrijving. Klik op **OK**.



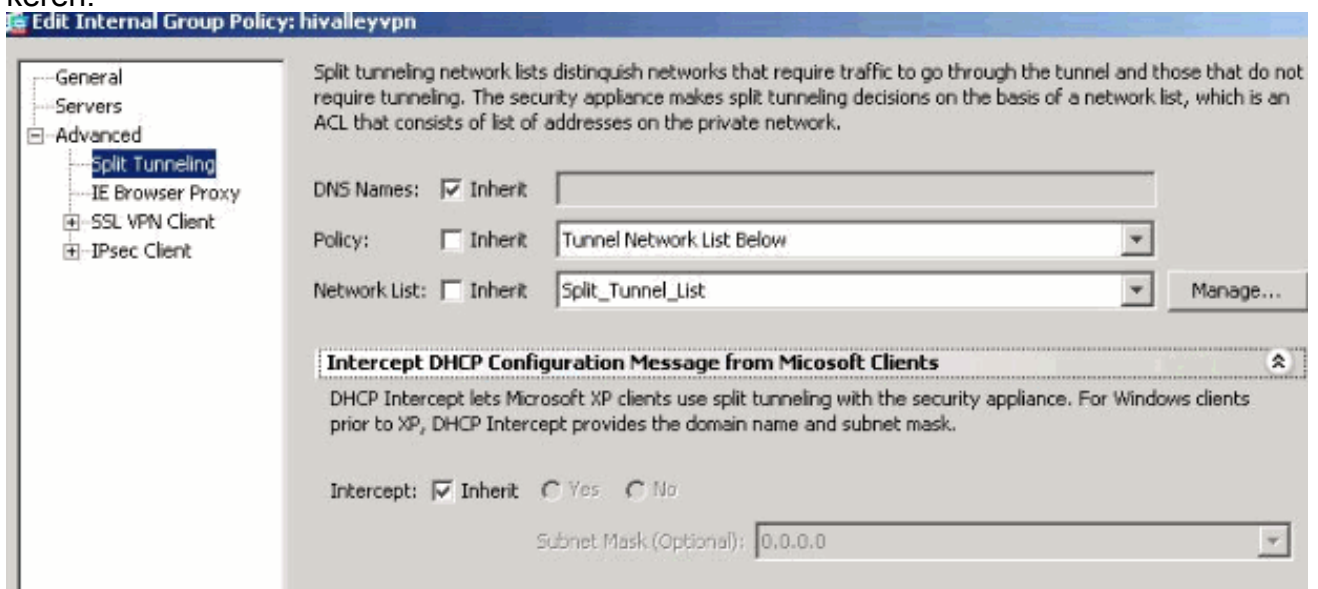
9. Klik op **OK** om de ACL-Manager te verlaten.



10. Verzeker u dat ACL die u zojuist hebt gemaakt, is geselecteerd voor Split Tunnel Network List.



11. Klik op **OK** om naar de configuratie van het groepsbeleid terug te keren.



12. Klik op **Toepassen** en **Verzend** (indien nodig) om de opdrachten naar de ASA te sturen.

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Type	Tunneling Protocol	
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec,IPSec,webvpn	-- N/A --
Defaultgroup	Internal	-- Inherited --	-- N/A --
hivalleyvpn	Internal	svc,IPSec	-- N/A --

[ASA 7.x en hoger configureren via CLI](#)

In plaats van de ASDM te gebruiken, kunt u deze stappen in de ASA CLI voltooien om gesplitste tunneling op de ASA toe te staan:

Opmerking: De CLI Split Tunneling-configuratie is hetzelfde voor zowel ASA 7.x als 8.x.

1. Geef de configuratie op.

```
ciscoasa>enable
Password: *****
ciscoasa#configure terminal
ciscoasa(config)#
```

2. Maak de toegangslijst die het netwerk achter de ASA definieert.

```
ciscoasa(config)#access-list Split_Tunnel_List remark The corporate network behind the ASA.
ciscoasa(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

3. Geef de configuratiemodus voor het groepsbeleid op voor het beleid dat u wilt wijzigen.

```
ciscoasa(config)#group-policy hivalleyvpn attributes
ciscoasa(config-group-policy)#
```

4. Specificeer het gesplitste tunnelbeleid. In dit geval wordt het beleid aangegeven.

```
ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified
```

5. Specificeer de gesplitste tunneltoeganglijst. In dit geval is de lijst **Split_Tunnel_List**.

```
ciscoasa(config-group-policy)#split-tunnel-network-list value Split_Tunnel_List
```

6. Deze opdracht geven:

```
ciscoasa(config)#tunnel-group hillvalleyvpn general-attributes
```

7. Associeer het groepsbeleid met de tunnelgroep

```
ciscoasa(config-tunnel-ipsec)# default-group-policy hillvalleyvpn
```

8. Sluit de twee configuratie-modi.

```
ciscoasa(config-group-policy)#exit
ciscoasa(config)#exit
ciscoasa#
```

9. Sla de configuratie op in niet-vluchtige RAM (NVRAM) en druk op **ENTER** wanneer u wordt gevraagd om de bronbestandsnaam te specificeren.

```
ciscoasa#copy running-config startup-config
```

```
Source filename [running-config]?
Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a
```

```
3847 bytes copied in 3.470 secs (1282 bytes/sec)
ciscoasa#
```

[PIX 6.x configureren via CLI](#)

Voer de volgende stappen uit:

1. Maak de toeganglijst die het netwerk achter de PIX definieert.

```
PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

2. Maak een VPN groep *vpn3000* en specificeer de gesplitste tunnel ACL naar deze zoals wordt weergegeven:

```
PIX(config)#vpngroup vpn3000 split-tunnel Split_Tunnel_List
```

Opmerking: Raadpleeg [Cisco Secure PIX Firewall 6.x en Cisco VPN-client 3.5 voor Windows met Microsoft Windows 2000 en 2003 IAS RADIUS-verificatie](#) voor meer informatie over VPN-configuratie voor externe toegang voor PIX 6.x.

[Verifiëren](#)

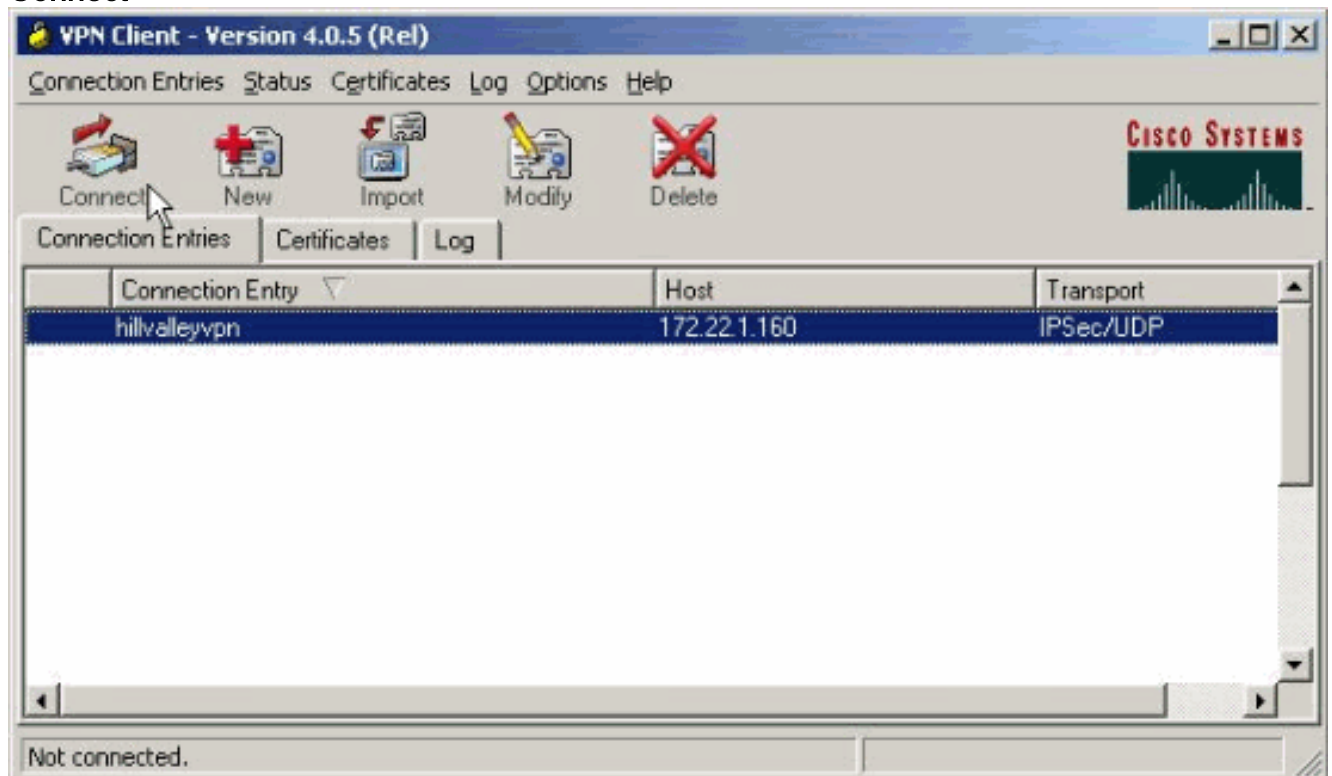
Volg de stappen in deze secties om uw configuratie te controleren.

- [Connect met VPN-client](#)
- [Bekijk het VPN-clientlogboek](#)
- [Lokale LAN-toegang testen met Ping](#)

[Connect met VPN-client](#)

Sluit uw VPN-client aan op de VPN-centrator om uw configuratie te controleren.

1. Kies uw verbindingssingang van de lijst en klik op **Connect**.

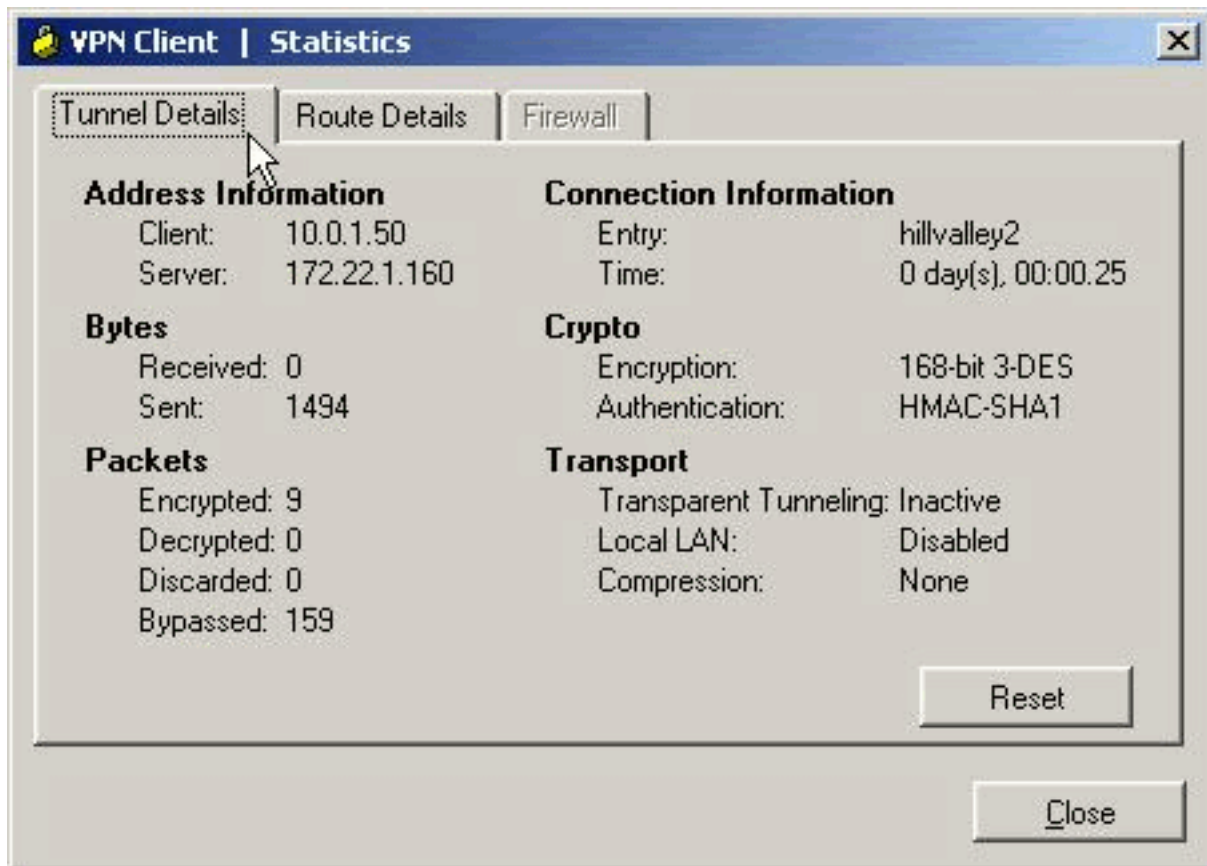


2. Voer je geloofsbriefen

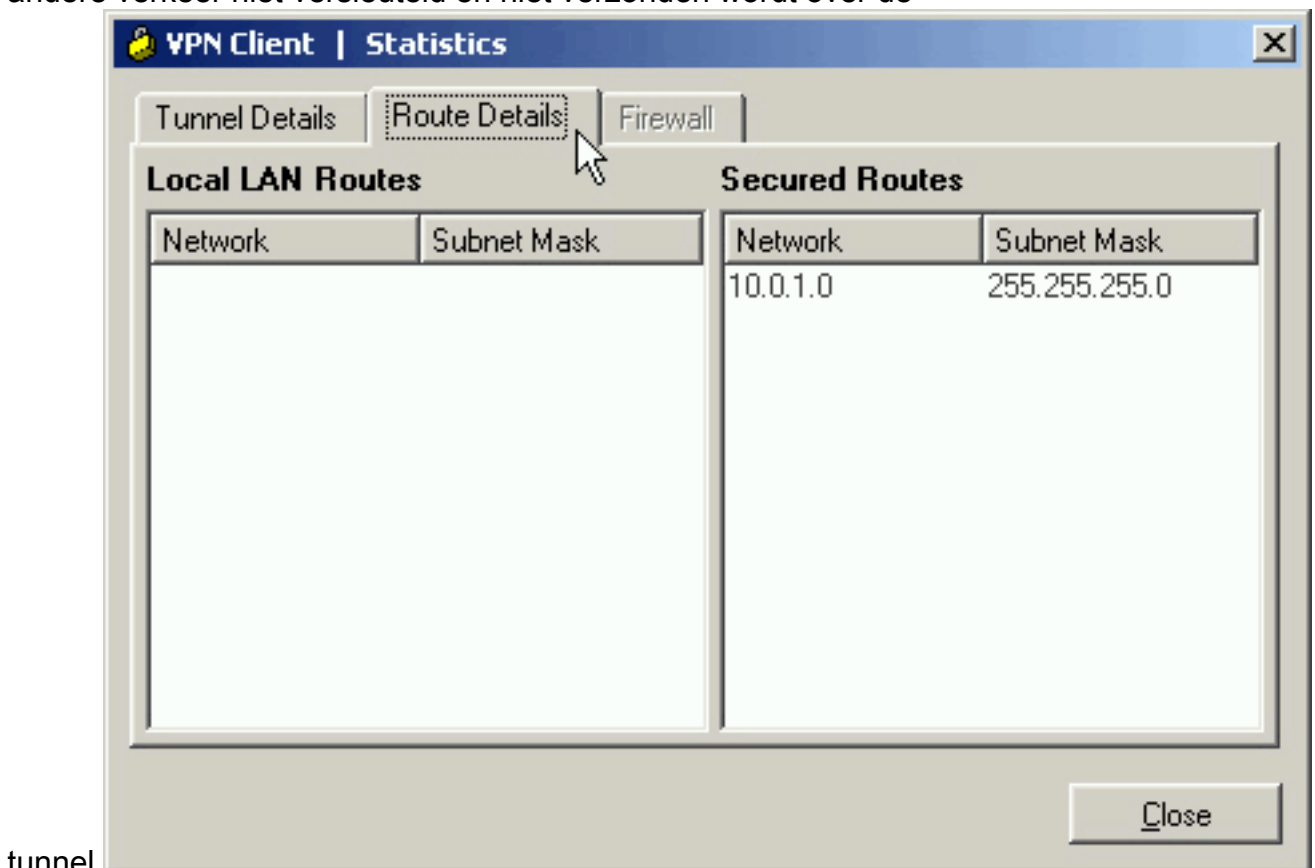


in.

3. Kies **Status > Statistieken...** om het venster met tunneldetails weer te geven, waar u de gegevens van de tunnel kunt inspecteren en verkeer kunt zien stromen.



4. Ga naar het tabblad Route Details om de routes te zien die de VPN-client aan de ASA heeft beveiligd. In dit voorbeeld, waarborgt de client van VPN toegang tot 10.0.1.0/24 terwijl al het andere verkeer niet versleuteld en niet verzonden wordt over de

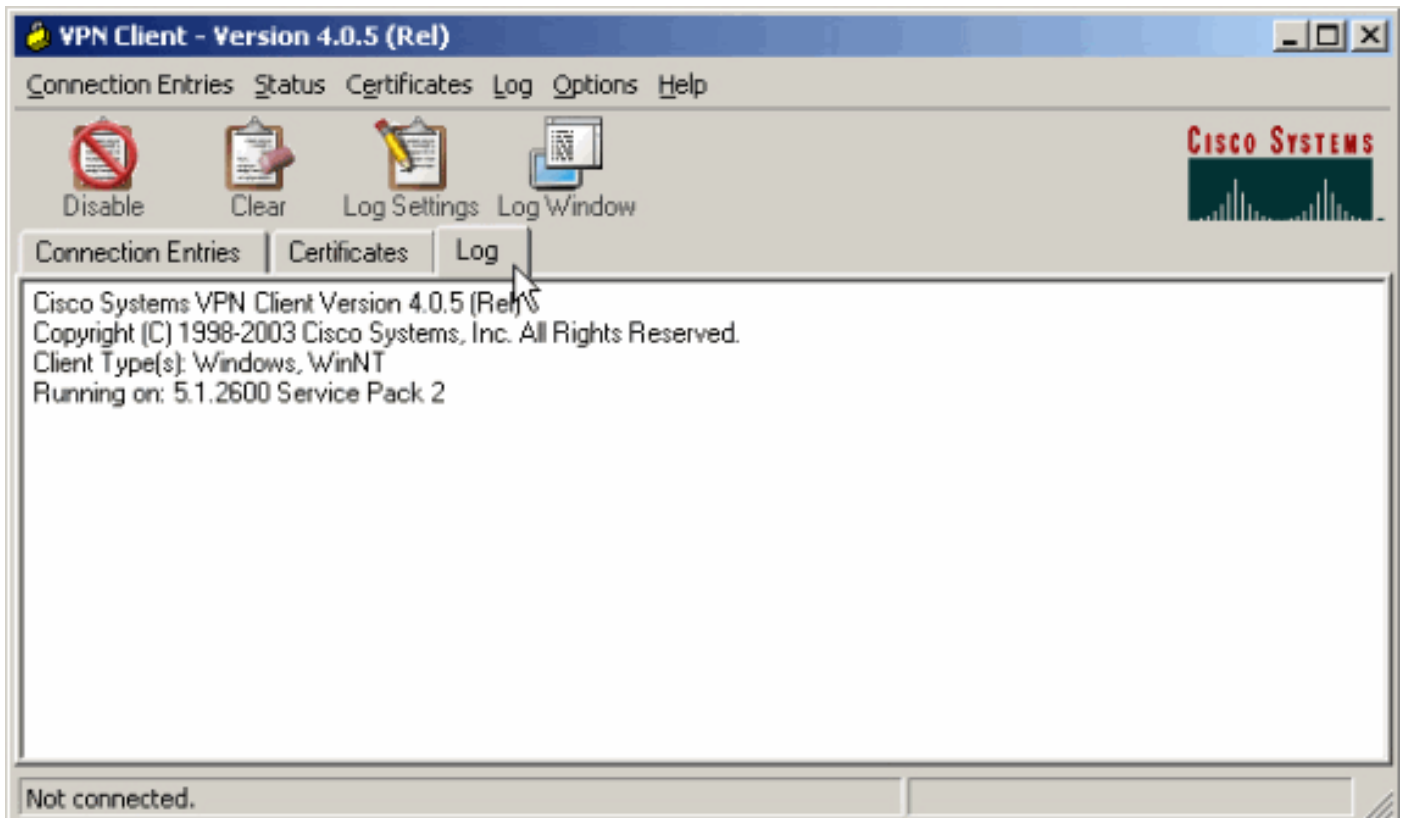


tunnel.

[Bekijk het VPN-clientlogboek](#)

Wanneer u het logbestand van VPN-client onderzoekt, kunt u bepalen of de parameter die

gesplitste tunneling specificeert, al dan niet is ingesteld. Ga naar het tabblad Log in de VPN-client om het logbestand te bekijken. Klik vervolgens op **loginstellingen** om aan te passen wat is vastgelegd. In dit voorbeeld is IKE ingesteld op **3 - Hoog** terwijl alle andere logelementen zijn ingesteld op **1 - Laag**.



```
Cisco Systems VPN Client Version 4.0.5 (Rel)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
```

```
1      14:20:09.532 07/27/06 Sev=Info/6IKE/0x6300003B
Attempting to establish a connection with 172.22.1.160.
```

```
!--- Output is supressed 18 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005D Client sending a
firewall request to concentrator 19 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall
Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 20
14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion
Prevention Security Agent, Capability= (Are you There?). 21 14:20:14.208 07/27/06 Sev=Info/4
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.160 22 14:20:14.208
07/27/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.160 23 14:20:14.208
07/27/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
172.22.1.160 24 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute =
INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 25 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 26 14:20:14.208
07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value =
0x00000000 27 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
MODECFG_UNITY_PFS: , value = 0x00000000 28 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc ASA5510 Version
7.2(1) built by root on Wed 31-May-06 14:45 !--- Split tunneling is permitted and the remote LAN
is defined. 29 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value = 0x00000001 30 14:20:14.238 07/27/06
Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0 mask = 255.255.255.0 protocol = 0 src
port = 0 dest port=0 !--- Output is supressed.
```

[Lokale LAN-toegang testen met Ping](#)

Een extra manier om te testen dat de VPN-client is geconfigureerd voor gesplitste tunneling terwijl deze is aangesloten op de ASA, is door de ping-opdracht in de Windows-opdrachtregel te gebruiken. Het lokale LAN van de VPN-client is 192.168.0.0/24 en er is een andere host op het netwerk aanwezig met een IP-adres van 192.168.0.3.

```
C:\>ping 192.168.0.3
```

```
Pinging 192.168.0.3 with 32 bytes of data:
```

```
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
```

```
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
```

```
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
```

```
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 192.168.0.3:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

[Problemen oplossen](#)

[Beperking met aantal ingangen in een splitter-tunnelleiding](#)

Er is een beperking met het aantal ingangen in een ACL die voor splitsingen tunnel wordt gebruikt. Aanbevolen wordt niet meer dan 50-60 ACE-items te gebruiken voor een bevredigende functionaliteit. U wordt geadviseerd om de subnetting optie uit te voeren om een bereik van IP adressen te bestrijken.

[Gerelateerde informatie](#)

- [PIX/ASA 750x als externe VPN-server met ASDM-configuratievoorbeeld](#)
- [Cisco ASA 5500 Series adaptieve security applicaties](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)