Split-tunneling configureren voor VPN-clients op de ASA

Inhoud

Inleiding

Dit document beschrijft het proces om VPN-clients toegang tot internet te geven terwijl u een tunneling maakt in een Cisco ASA 5500 Series security applicatie.

Voorwaarden

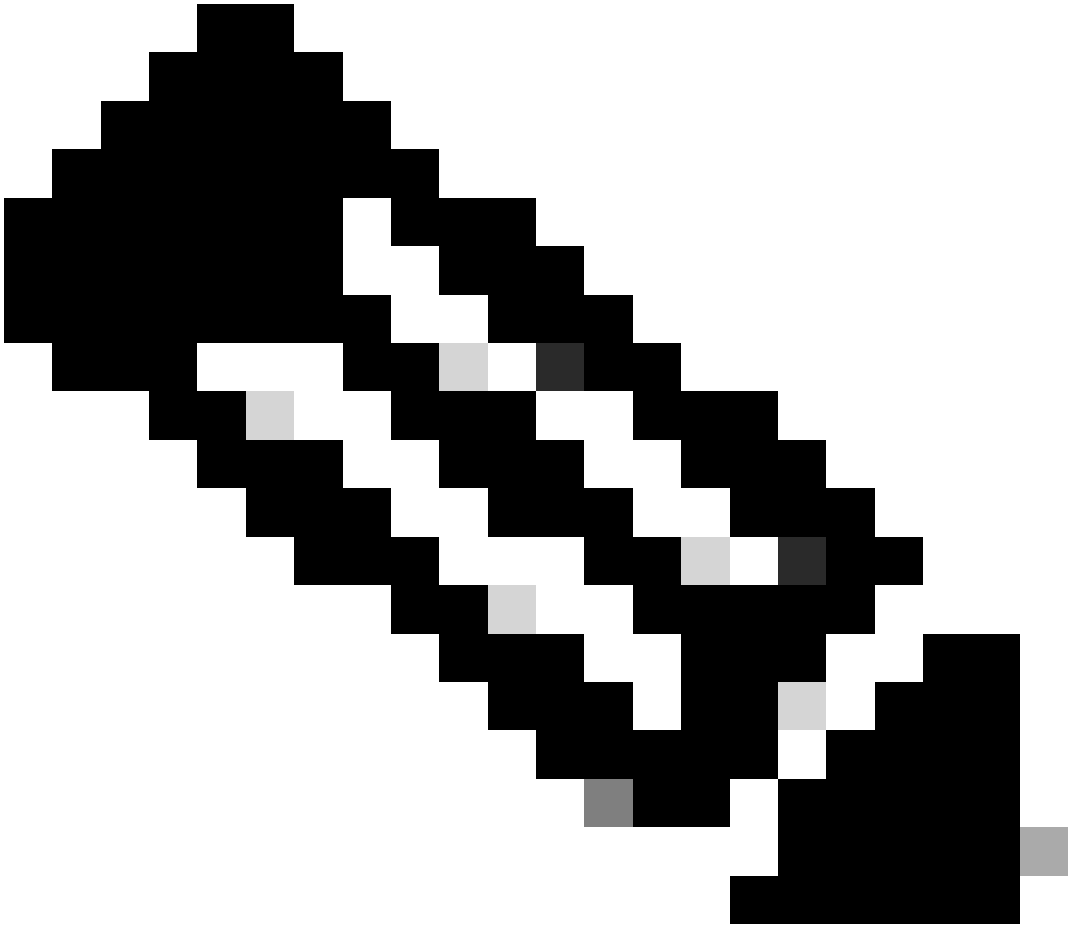
Vereisten

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 Remote VPN-server met ASDM Configuration Voorbeeld als een nog niet is geconfigureerd.

Gebruikte componenten

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

- Software voor Cisco ASA 5500 Series security applicatie, versie 7.x en hoger
- Cisco Systems VPN-clientversie 4.0.5
- Adaptieve security apparaatbeheer (ASDM)

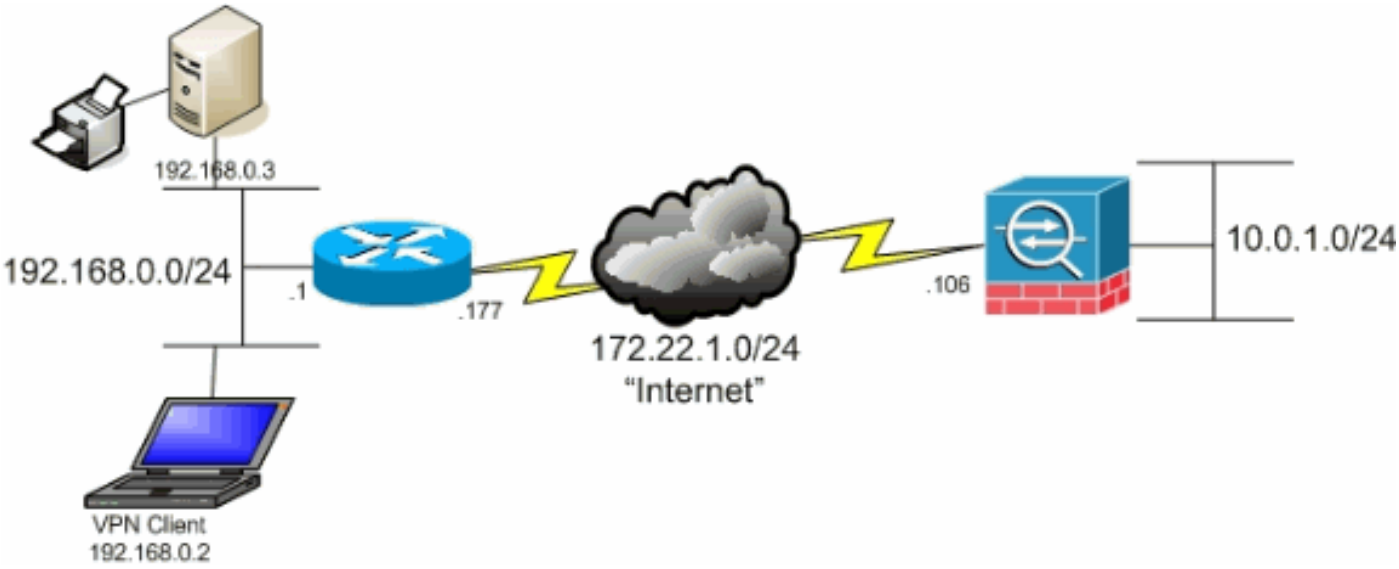


> Opmerking: dit document bevat ook de PIX 6.x CLI-configuratie die compatibel is voor de Cisco VPN-client 3.x.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Netwerkdiagram

De VPN-client bevindt zich op een typisch SOHO-netwerk en maakt via het internet verbinding met het hoofdkantoor.



Netwerkdiagram

Verwante producten

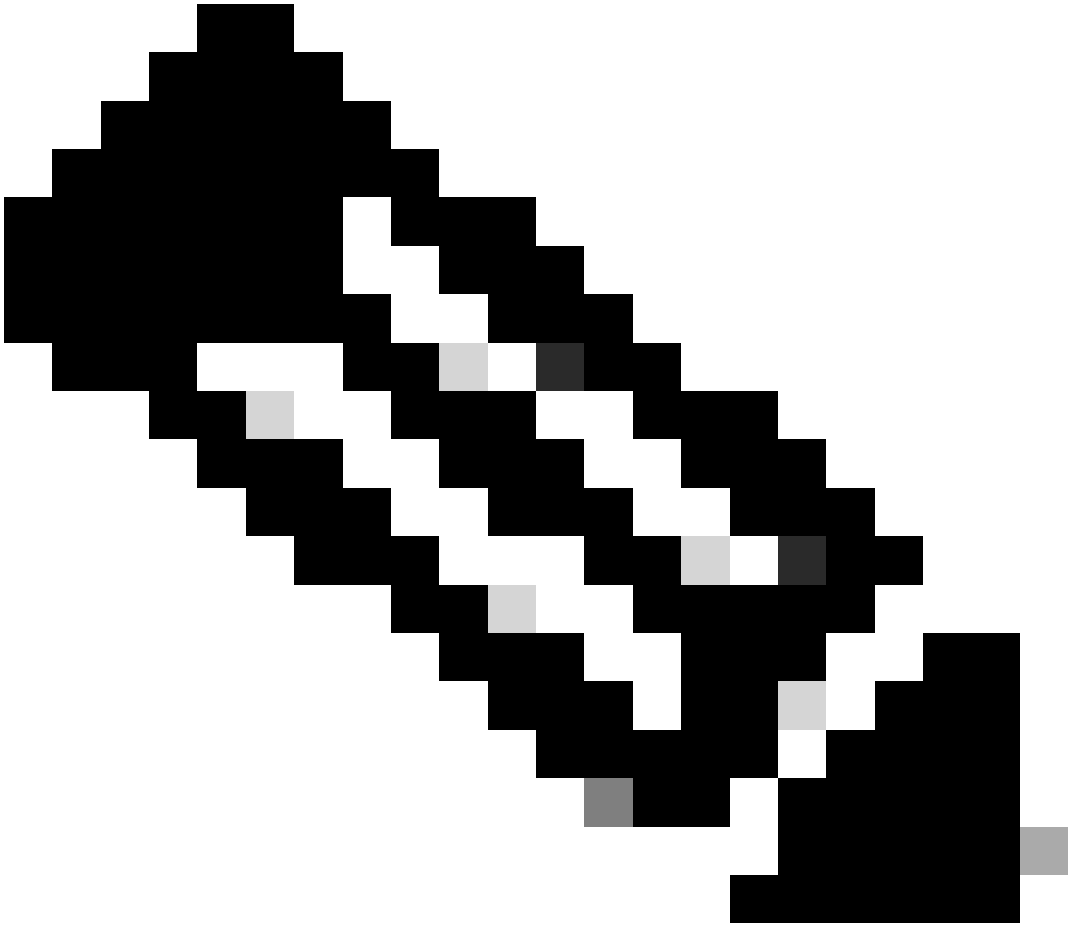
Deze configuratie kan ook worden gebruikt met Cisco PIX 500 Series security applicatie softwareversie 7.x.

Conventies

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

Achtergrondinformatie

Dit document bevat stap-voor-stap instructies hoe u VPN-clients toegang tot internet kunt geven terwijl ze een tunnel zijn gegraven in een Cisco adaptieve security applicatie (ASA) 5500 Series security applicatie. Deze configuratie biedt VPN-clients beveiligde toegang tot bedrijfsbronnen via IPsec terwijl ze onbeveiligde toegang tot het internet geven.



Opmerking: volledige tunneling wordt beschouwd als de best beveiligde configuratie omdat het apparaat geen gelijktijdige toegang tot zowel internet als het LAN van het bedrijf mogelijk maakt. Een compromis tussen volledige tunneling en gesplitste tunneling biedt alleen lokale LAN-toegang voor VPN-clients. Zie PIX/ASA 7.x: Local LAN Access for VPN Clients Configuration Voorbeeld voor meer informatie.

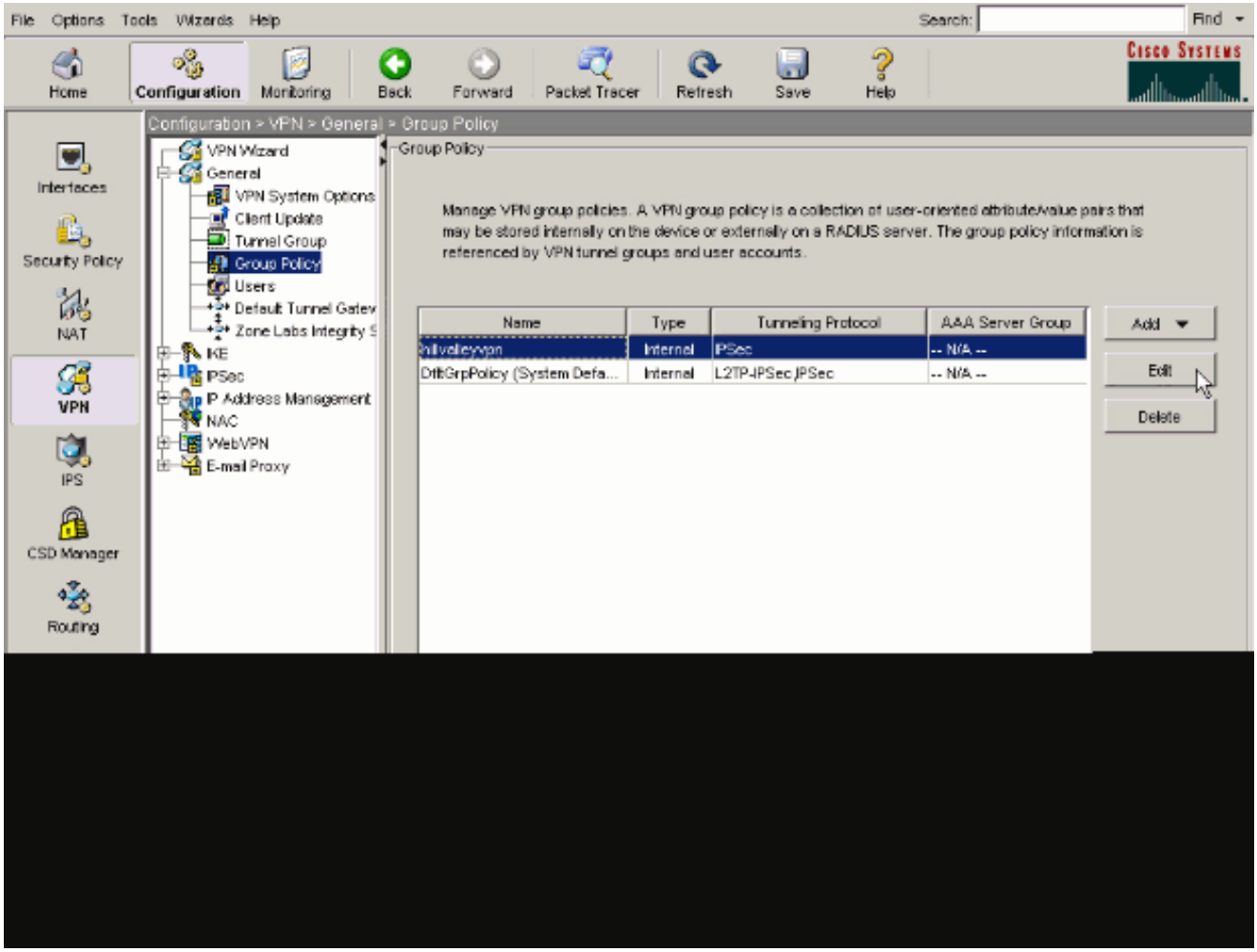
In een basis-VPN-client naar ASA-scenario wordt al het verkeer vanaf de VPN-client versleuteld en naar de ASA verzonden, ongeacht wat de bestemming is. Gebaseerd op uw configuratie en het aantal gebruikers dat wordt ondersteund, kan een dergelijke installatie bandbreedte-intensief worden. Split-tunneling kan werken om dit probleem te verlichten omdat het gebruikers in staat stelt alleen dat verkeer te verzenden dat is bestemd voor het bedrijfsnetwerk over de tunnel. Al het andere verkeer, zoals instant messaging, e-mail of willekeurig browsen, wordt via het lokale LAN van de VPN-client naar het internet verzonden.

Split-tunneling op de ASA configureren

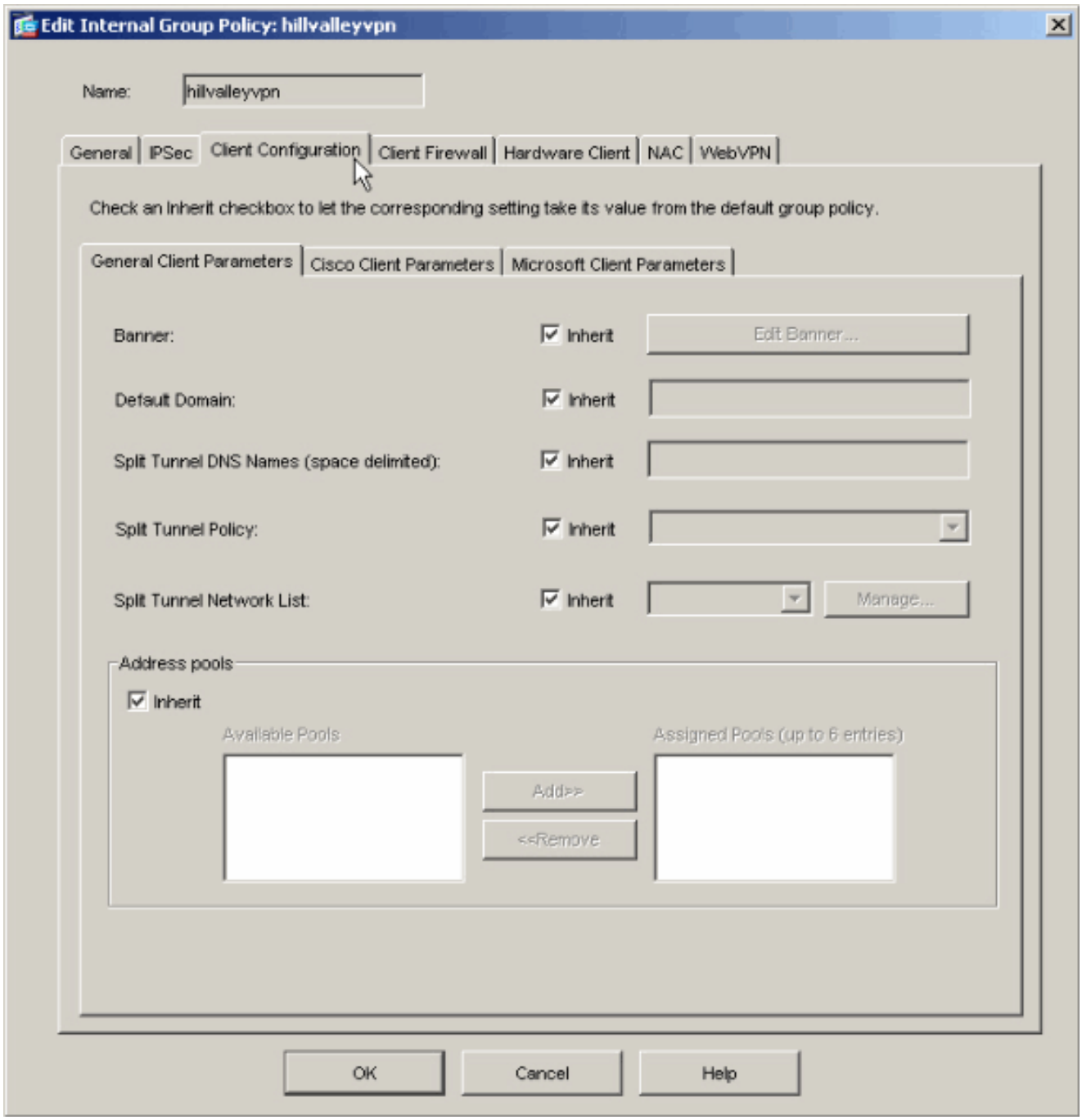
De ASA 7.x configureren met Adaptieve Security Device Manager (ASDM) 5.x

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

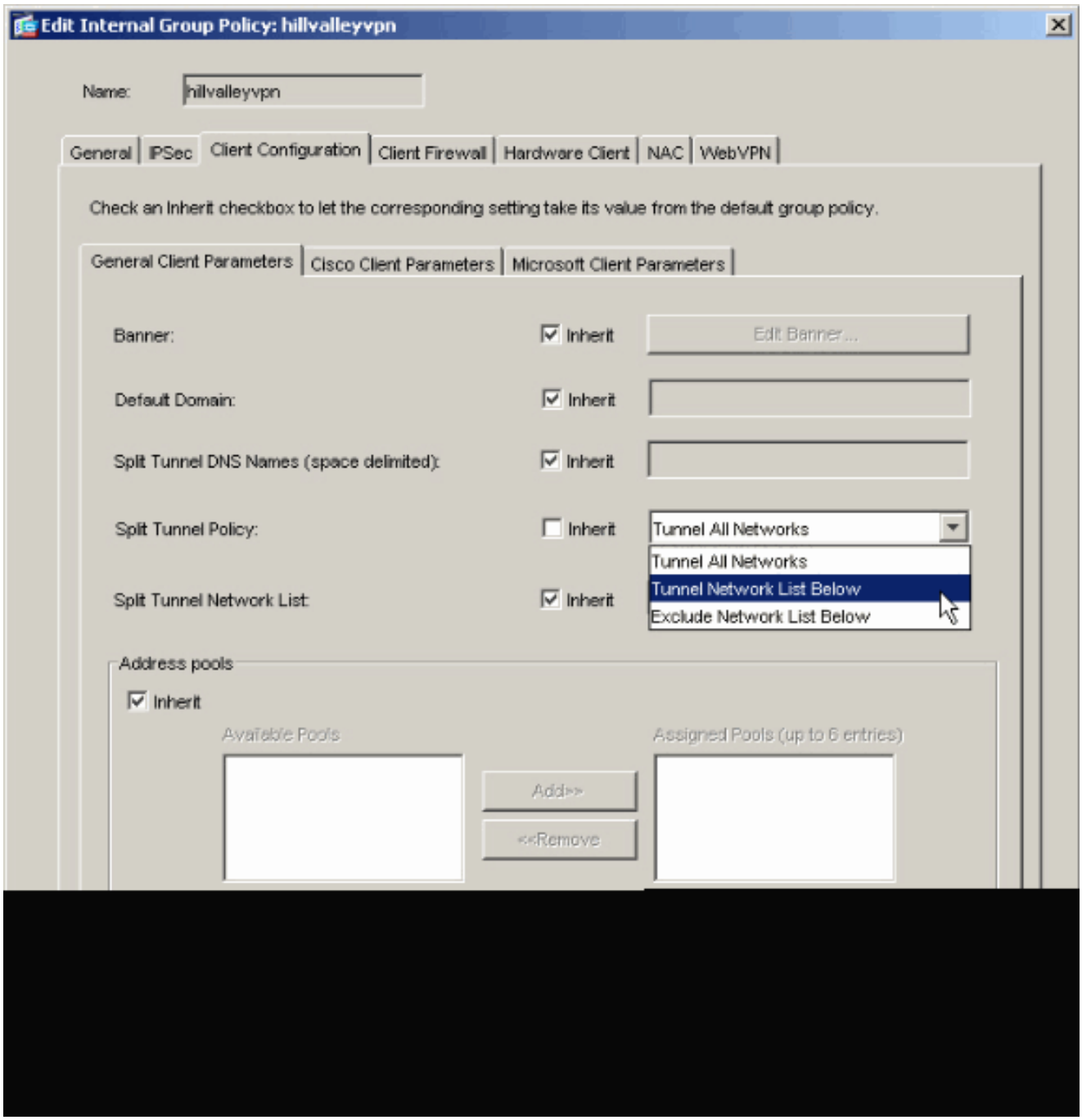
1. Kies Configuratie > VPN > Algemeen > Groepsbeleid en selecteer het Groepsbeleid waarin u lokale LAN-toegang wilt inschakelen. Klik vervolgens op Edit (Bewerken).



2. Ga naar het tabblad Clientconfiguratie.

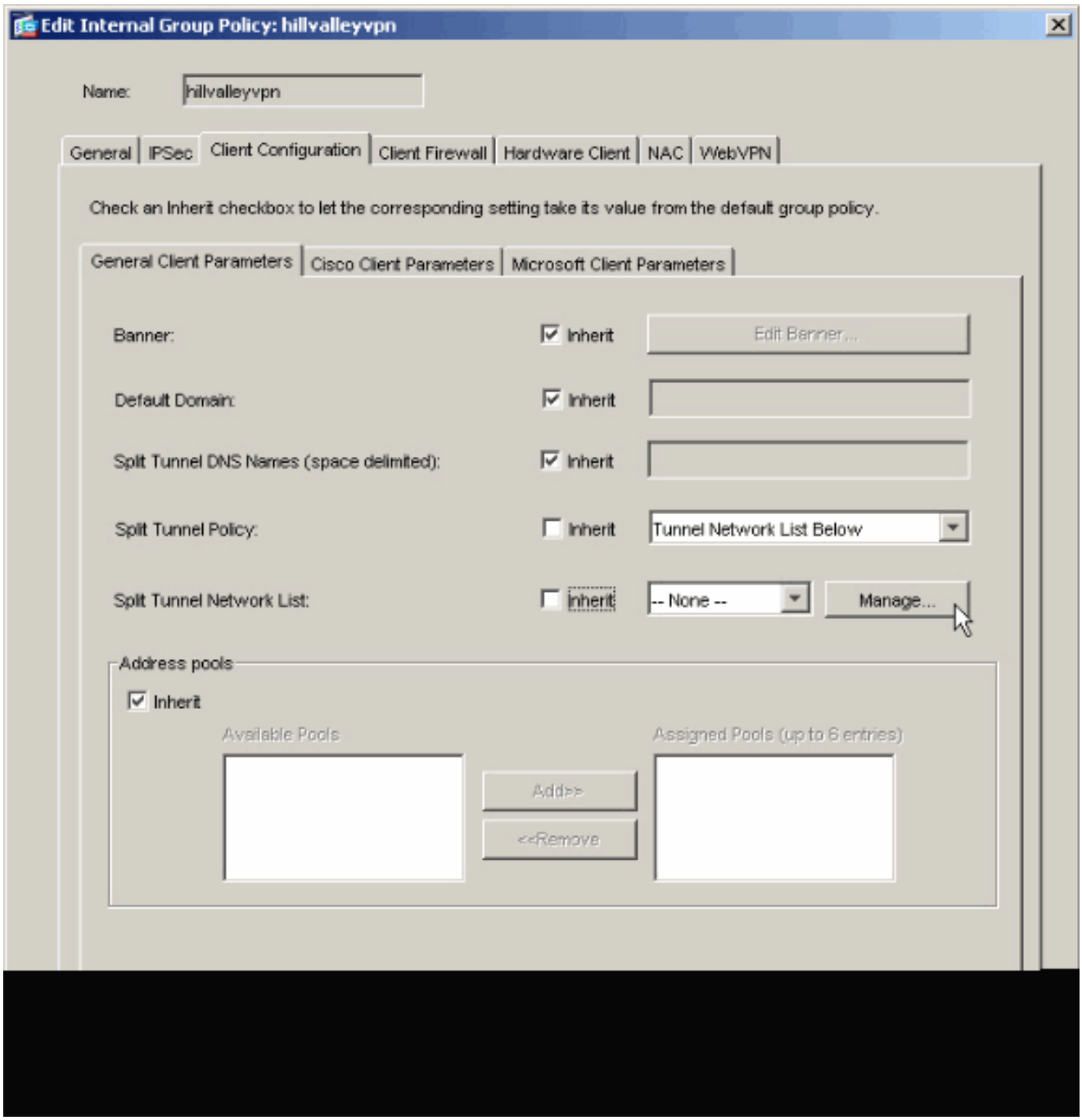


3. Schakel het vakje Inherit voor het beleid voor de Split-tunnel uit en kies Tunnel Network List Below ..



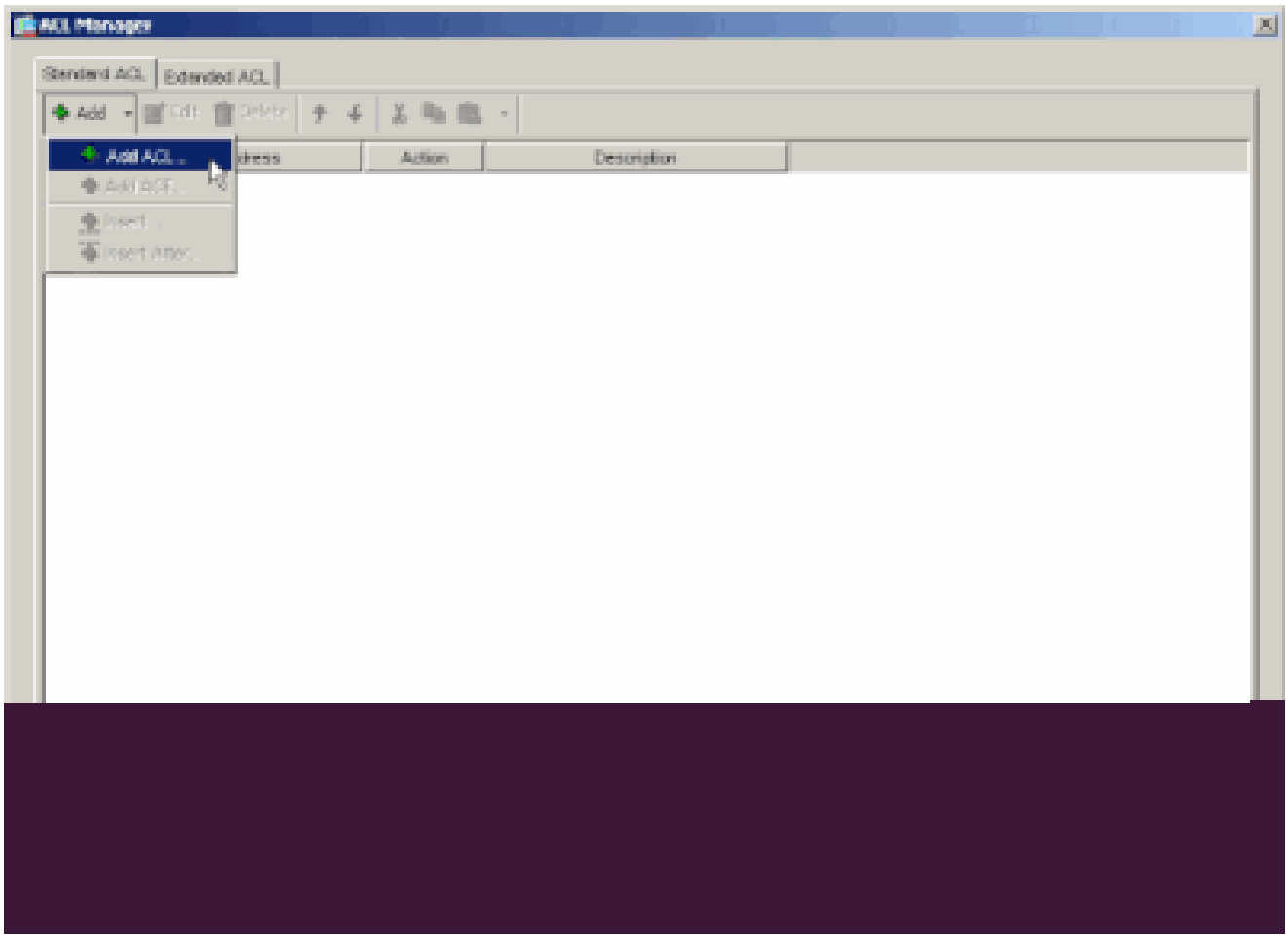
•

Schakel het vakje **Inherit** voor de netwerklijst van de Split-tunnel uit en klik vervolgens op **Beheren** om de ACL-beheer te starten.



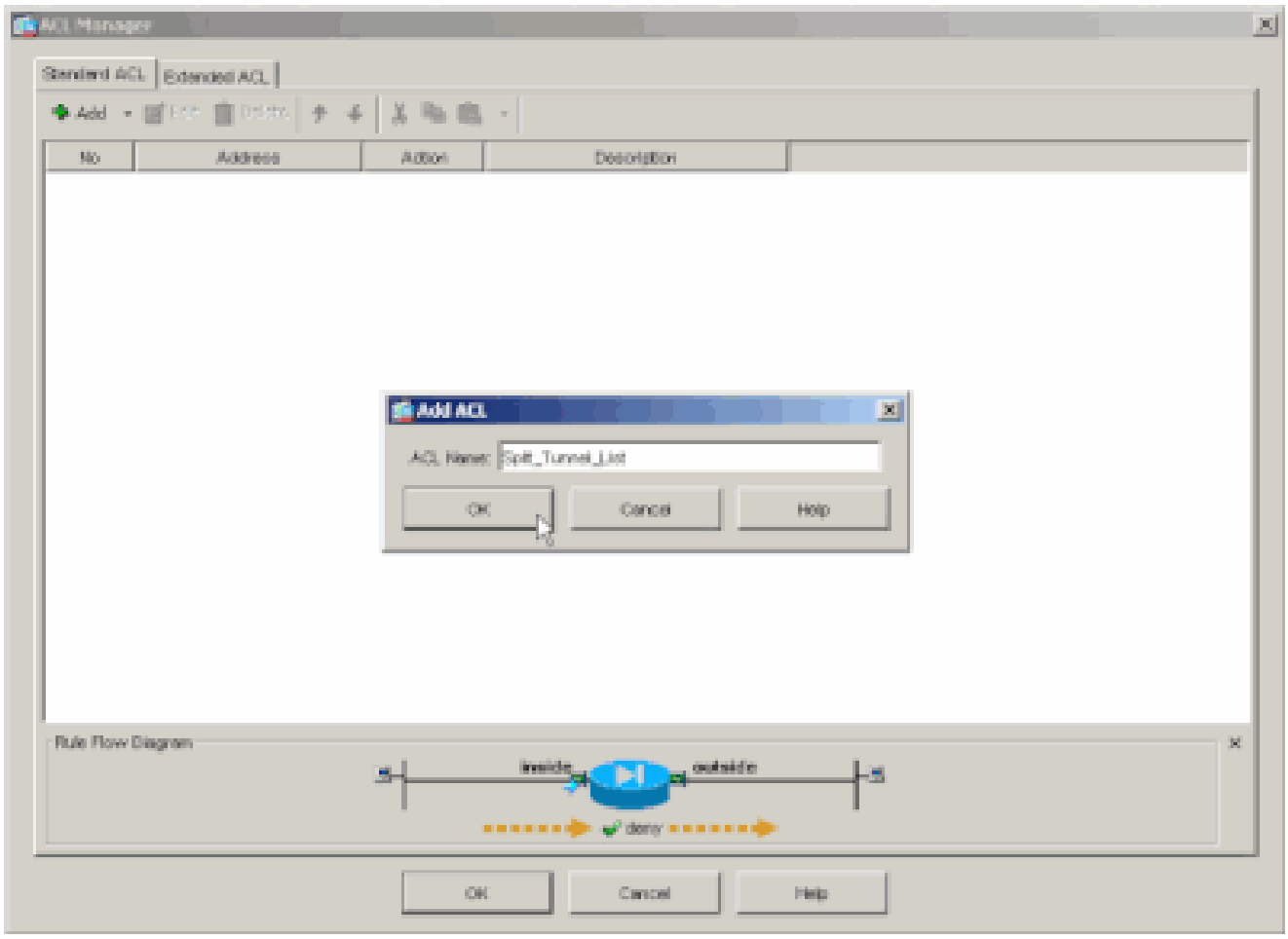
•

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



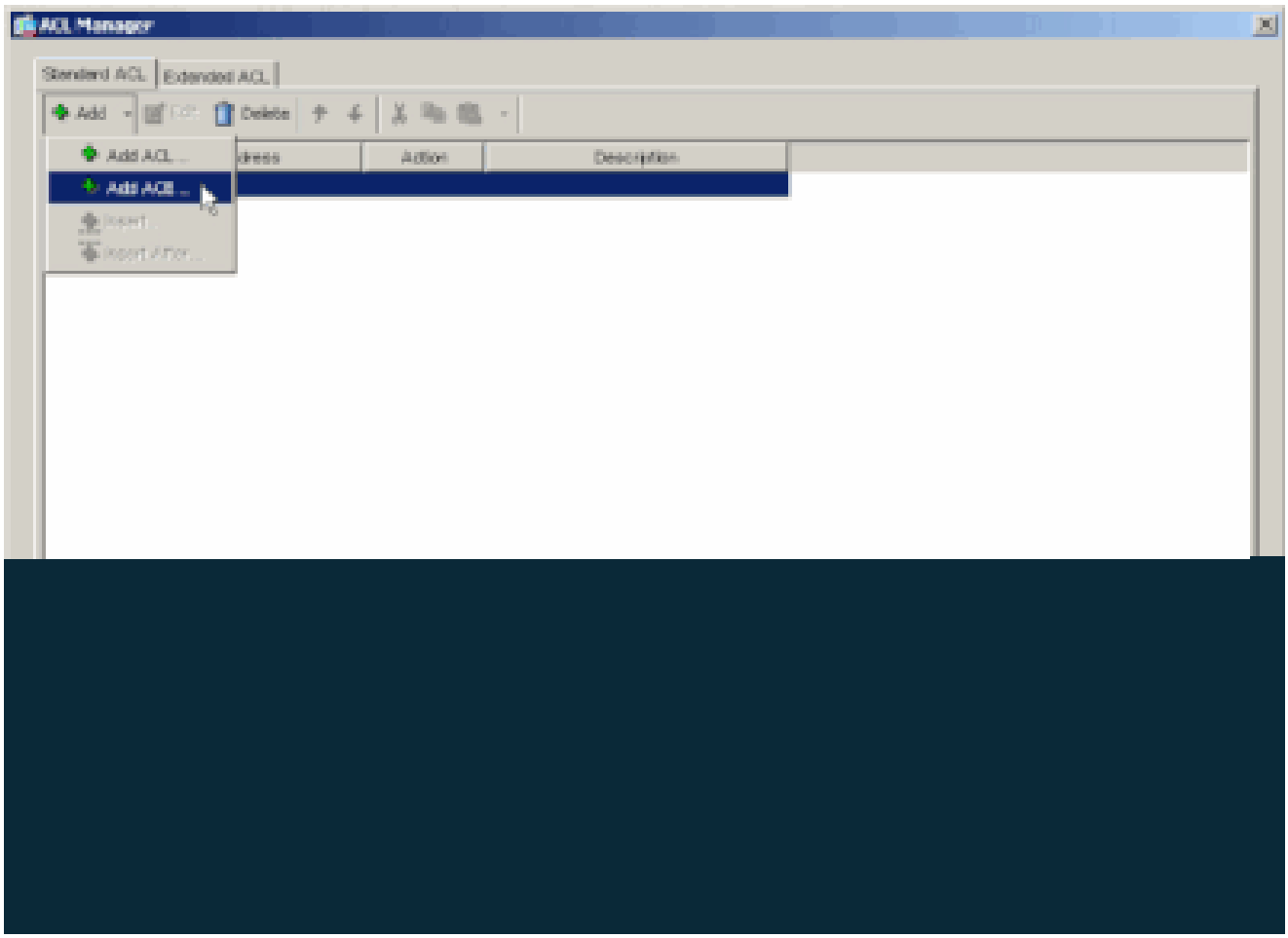
•

Typ een naam voor de ACL en klik op OK.



•

Zodra de ACL is gemaakt, kiest u **Toevoegen > ACE toevoegen. .**om een Access Control Entry (ACE) toe te voegen.



•

Bepaal het ACE dat aan LAN achter ASA beantwoordt. In dit geval is het netwerk 10.0.1.0/24.

a.

Selecteer Permit (Toestaan).

b.

Kies IP-adres 10.0.1.0.

c.

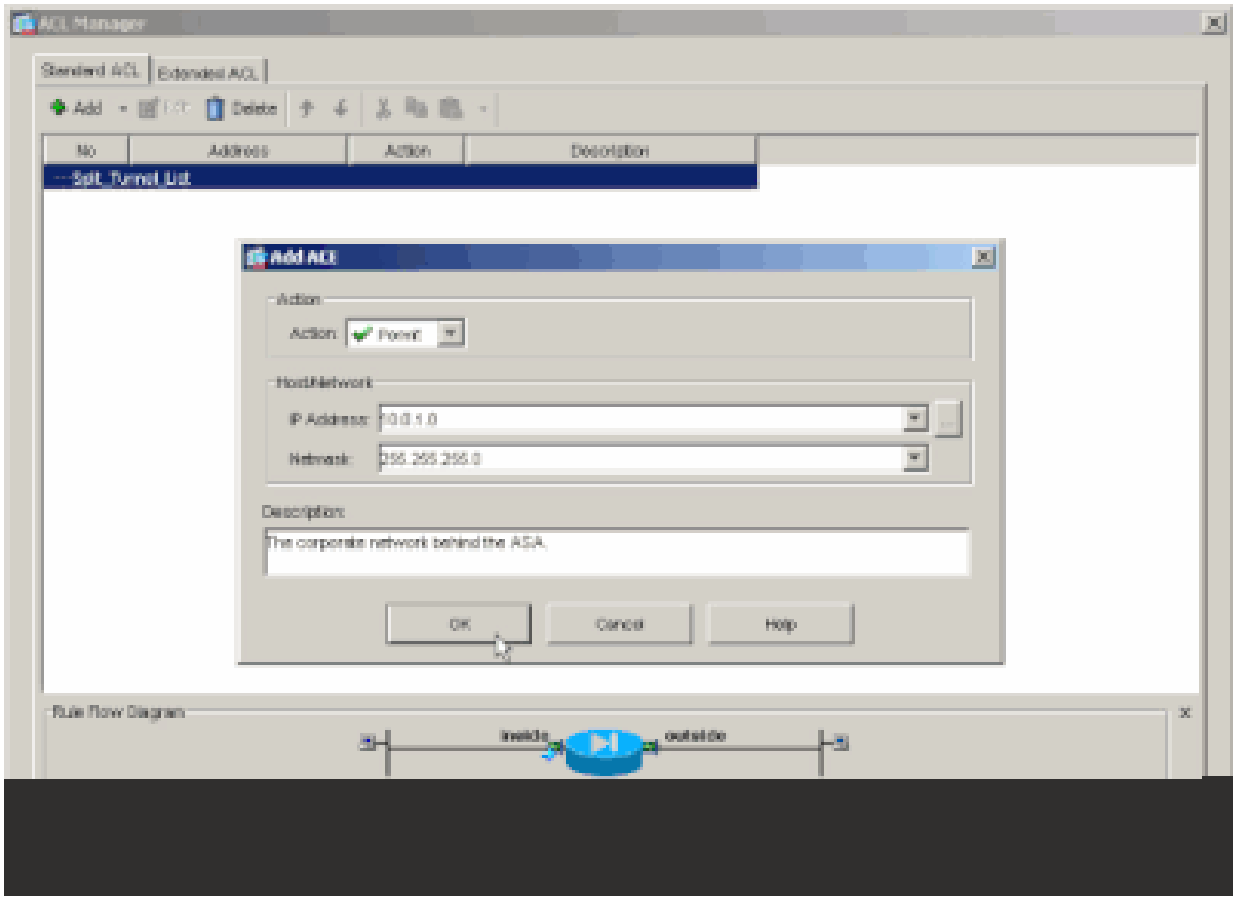
Kies een Netmasker van **255.255.255.0**.

d.

*(Optioneel)*Geef een beschrijving.

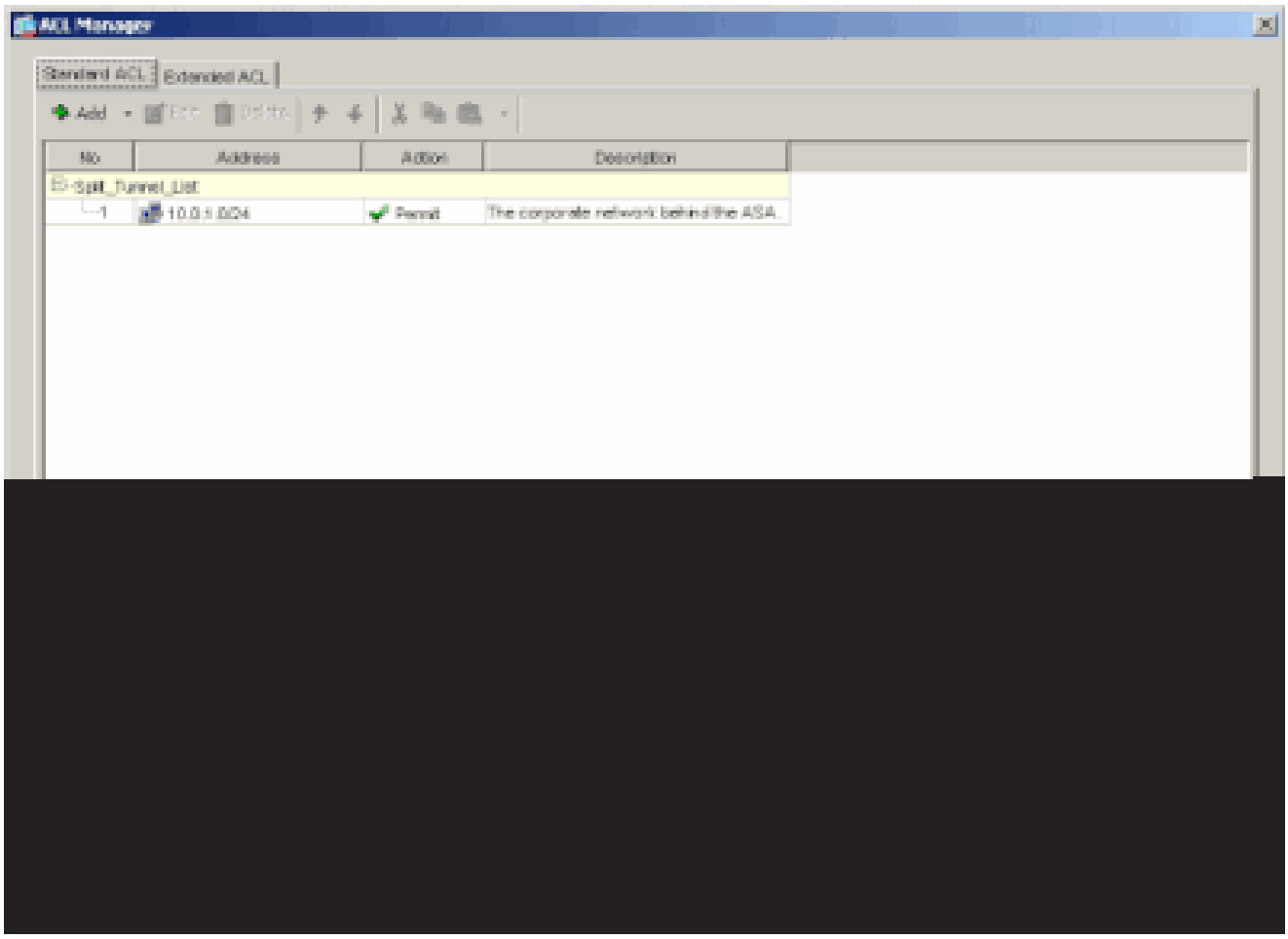
e.

Klik op > **OK**.



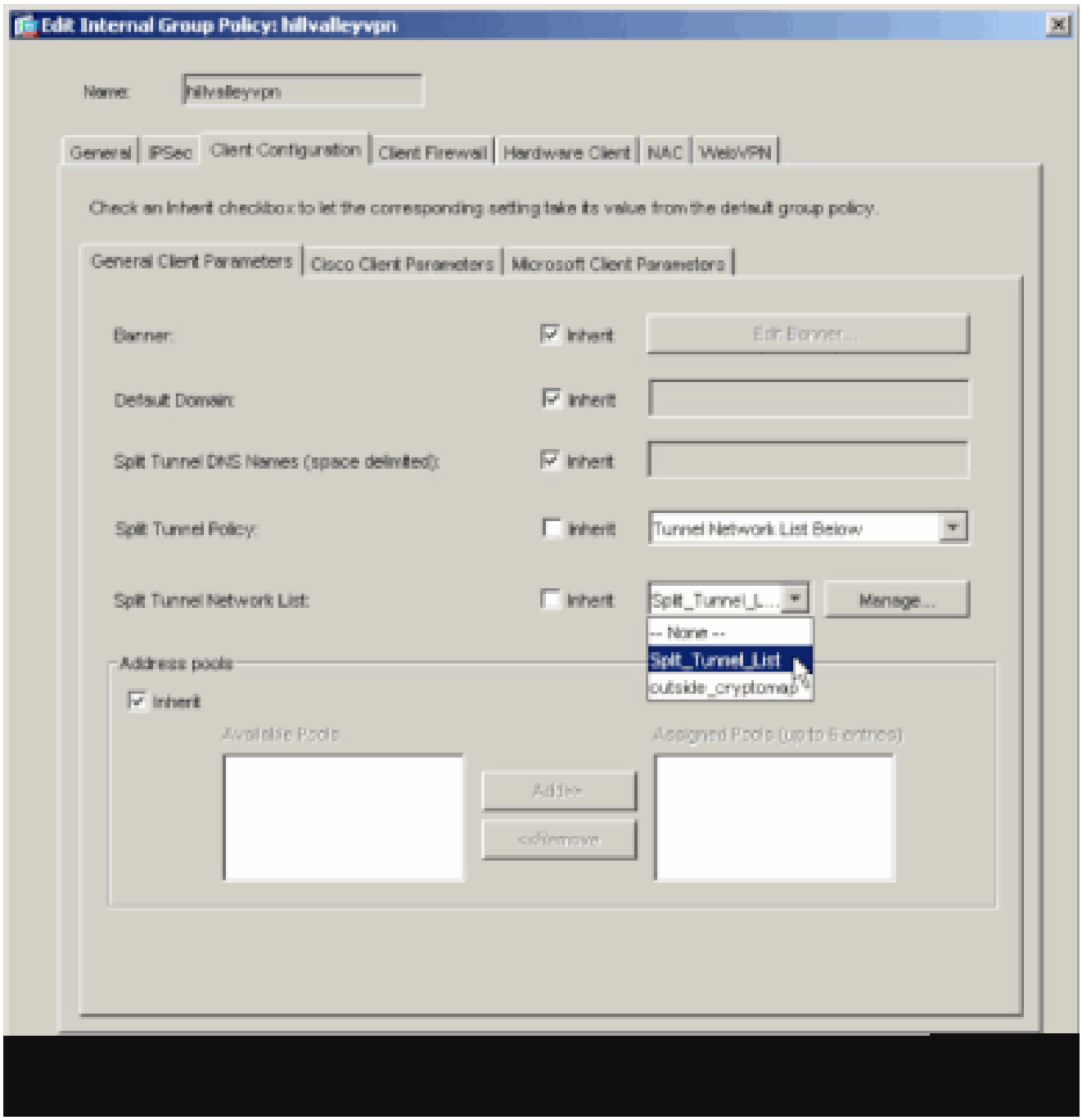
•

Klik op OK om ACL Manager af te sluiten.



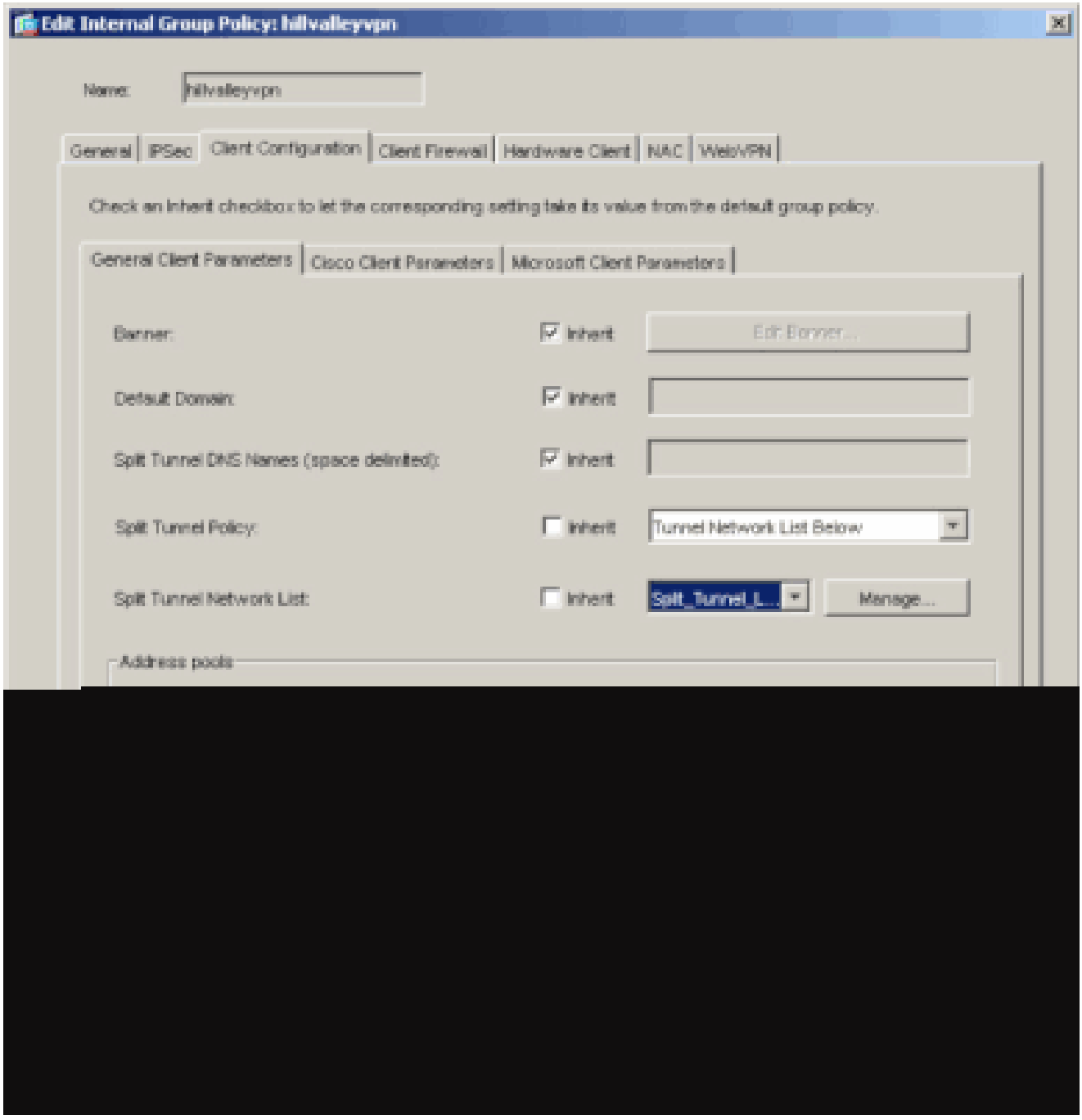
•

Zorg ervoor dat de ACL die u zojuist hebt gemaakt, is geselecteerd voor de netwerklijst van splitste tunnels.



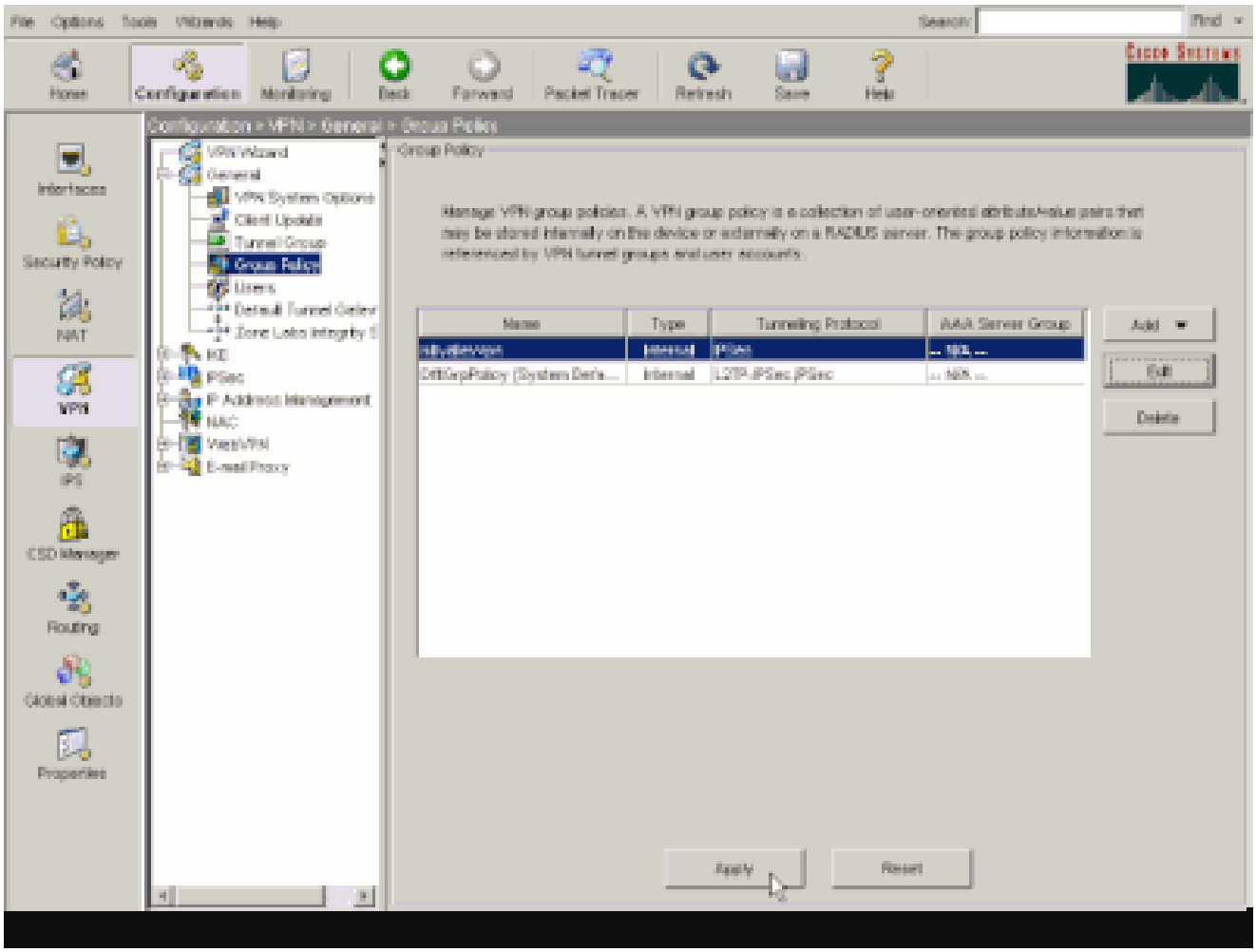
•

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



•

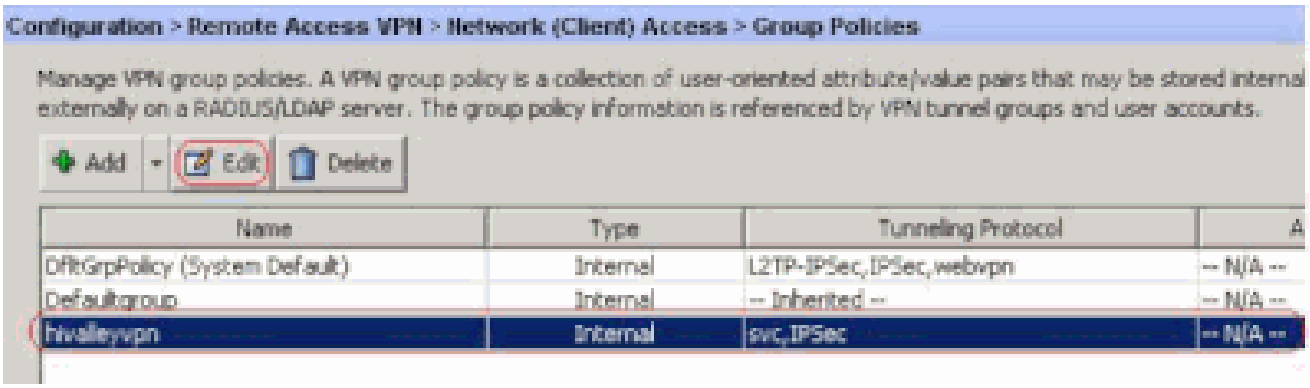
Klik op Apply (Toepassen) en vervolgens op Send (Verzenden) (waar vereist) om de opdrachten naar de ASA te sturen.



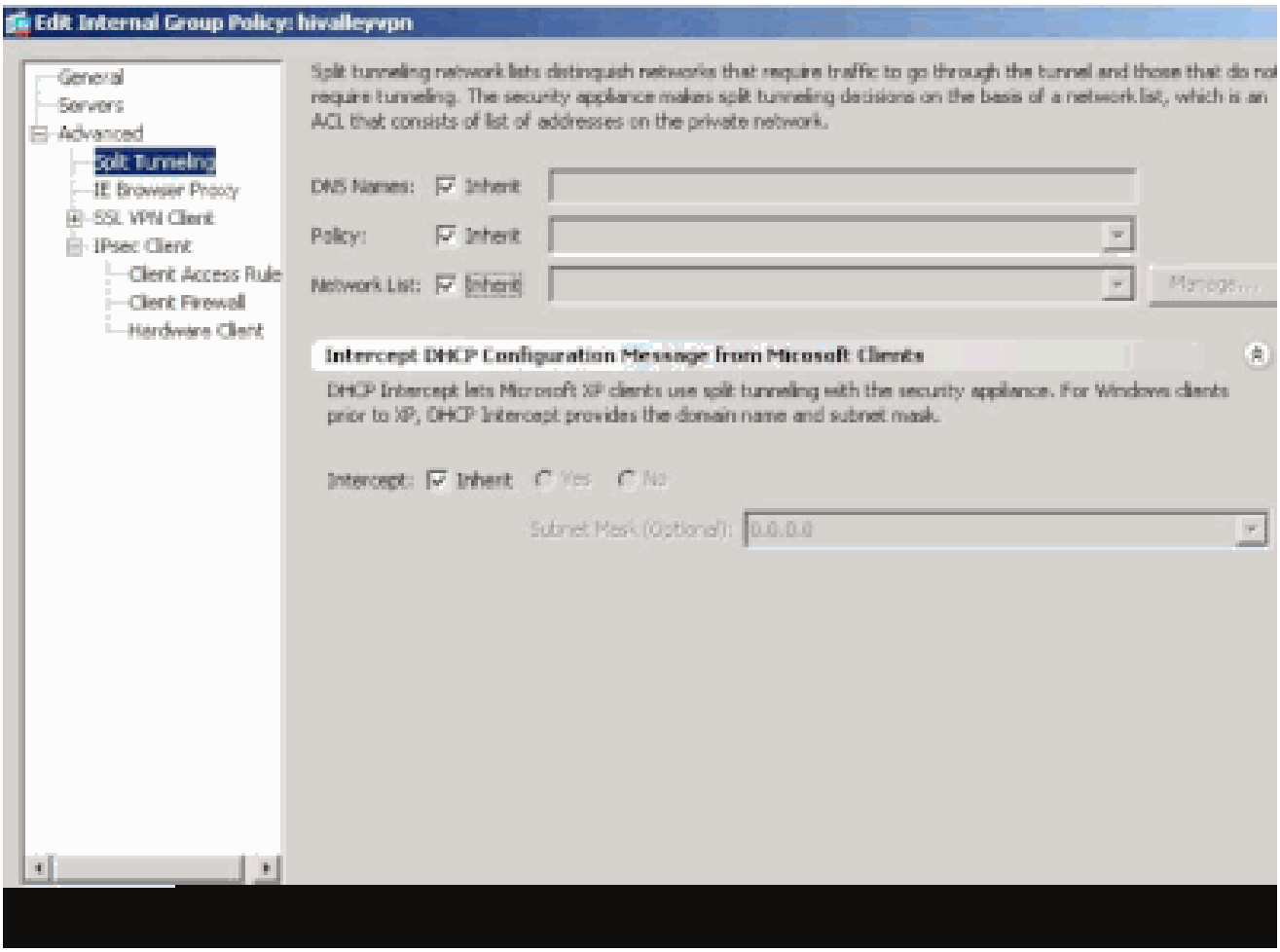
De ASA 8.x configureren met ASDM 6.x

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

- Kies **Configuratie > Externe toegang VPN > Netwerktoegang (client) > Groepsbeleid** en kies het Groepsbeleid waarin u lokale LAN-toegang wilt inschakelen. Klik vervolgens op Edit (Bewerken).

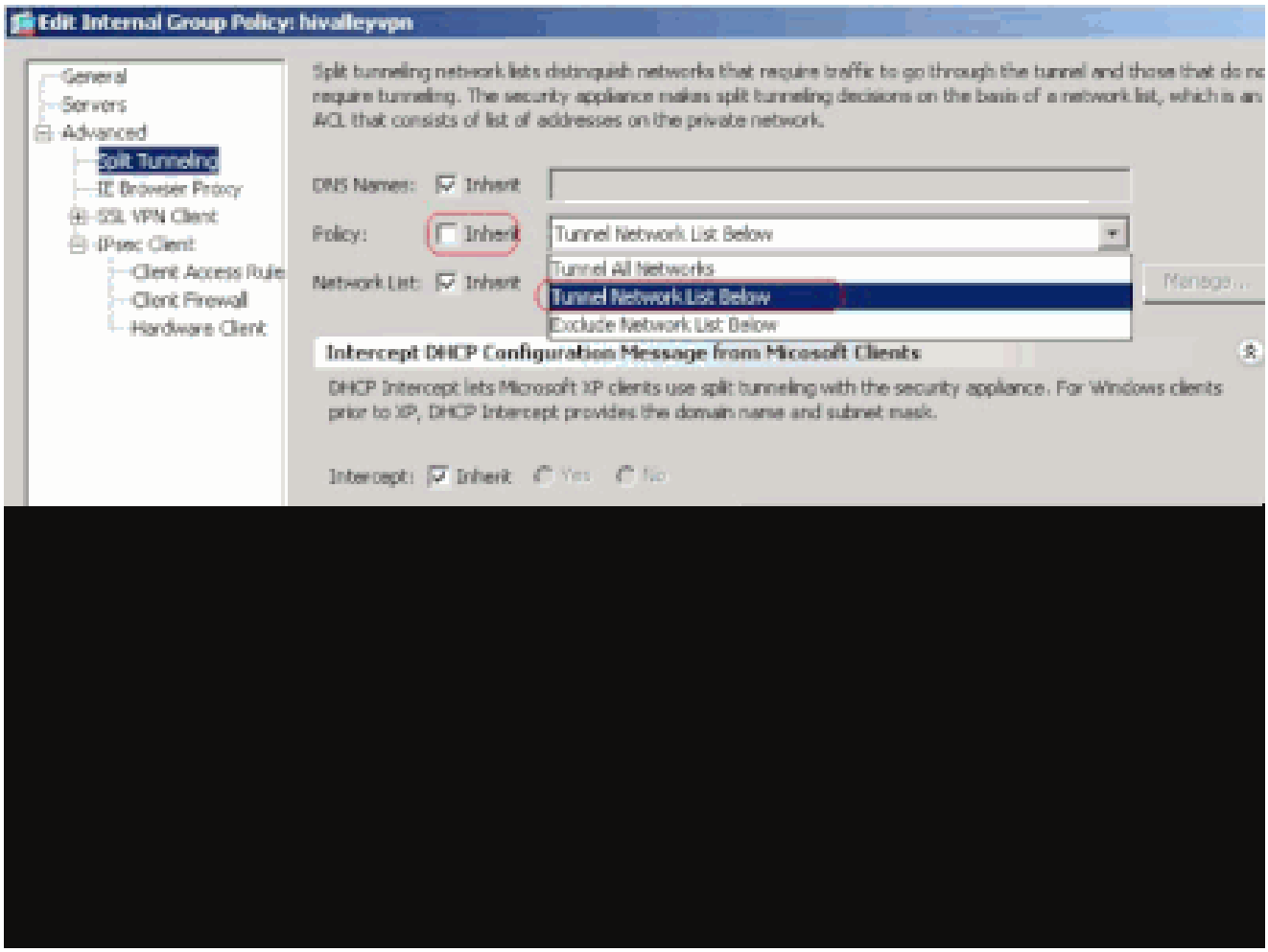


- Klik op **Split-tunneling**.



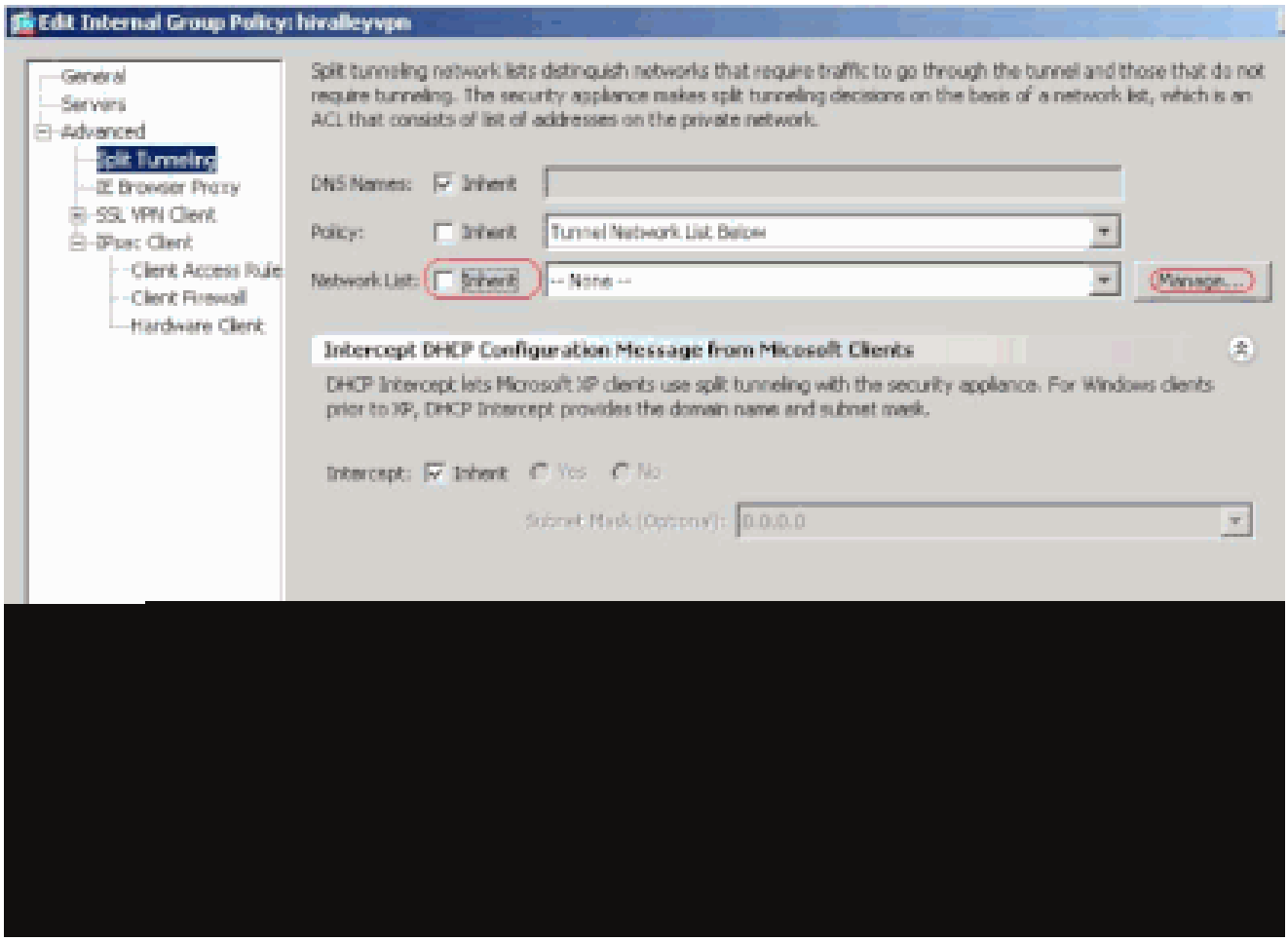
-

Schakel het vakje **Inherit** voor het Split-tunnelbeleid uit en kies **hieronder de lijst met tunnelnetwerken**.



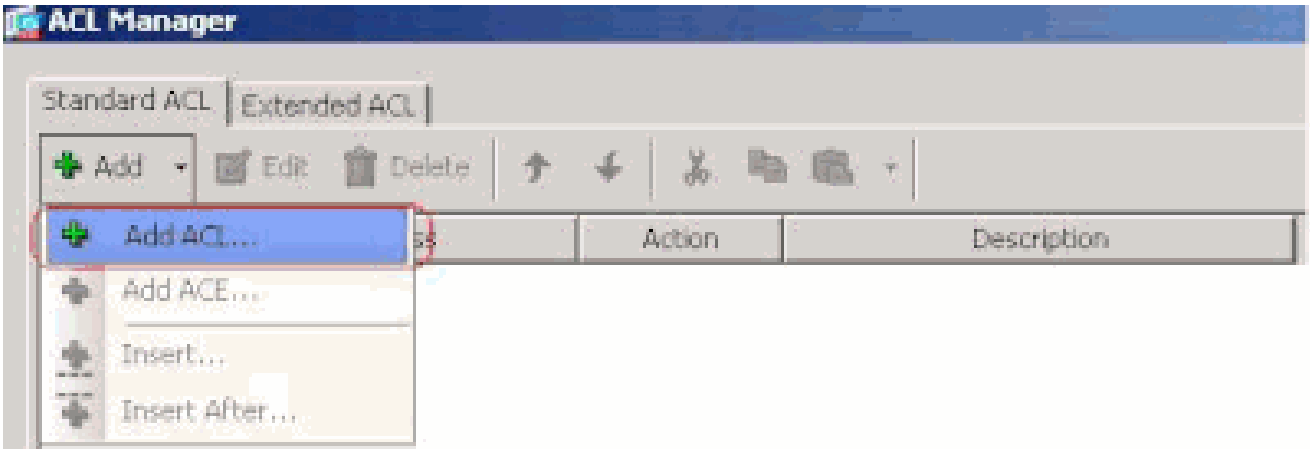
•

Schakel het vakje **Inherit** voor de netwerklijst van de Split-tunnel uit en klik vervolgens op **Beheren** om de ACL-beheer te starten.



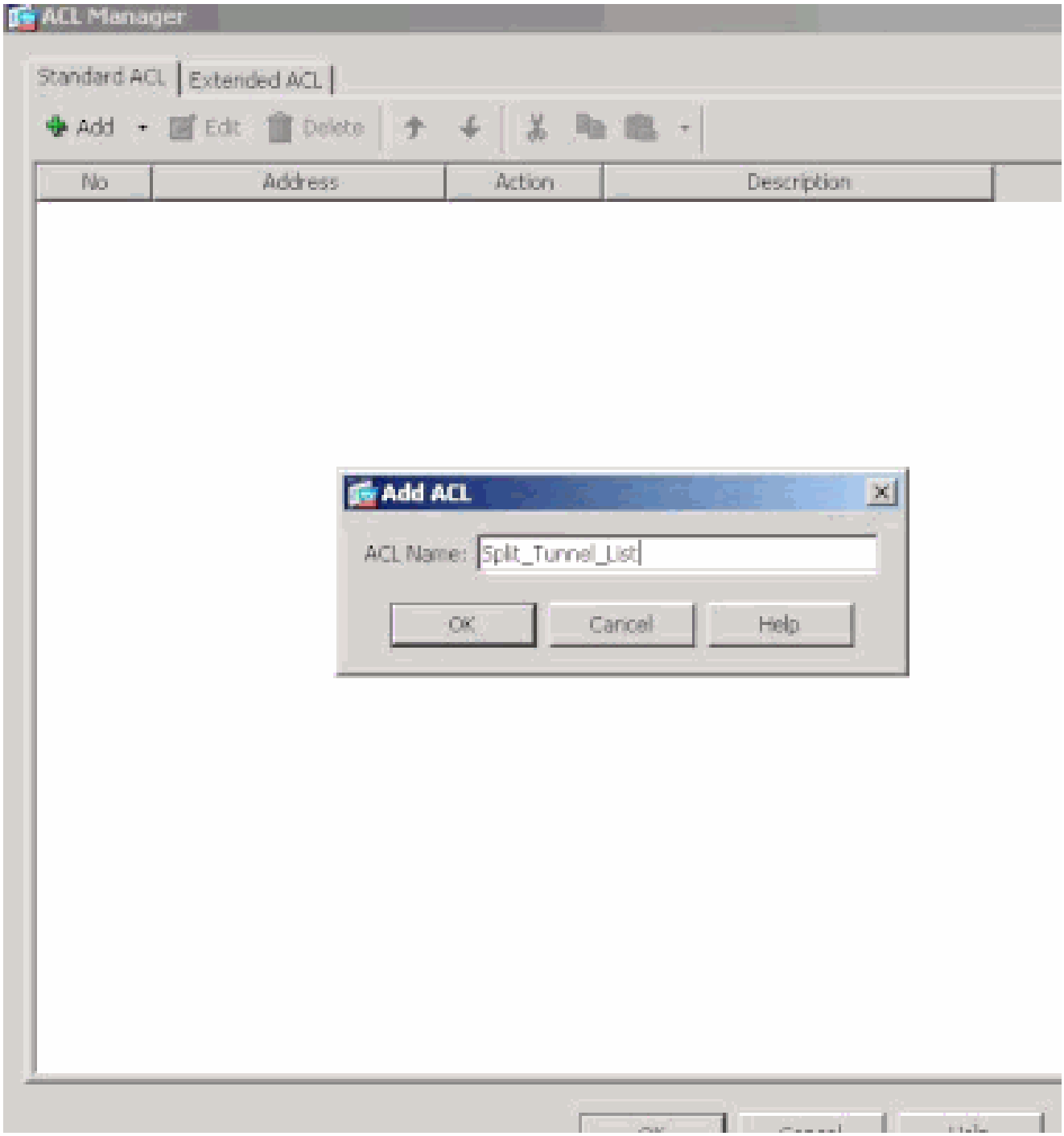
•

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



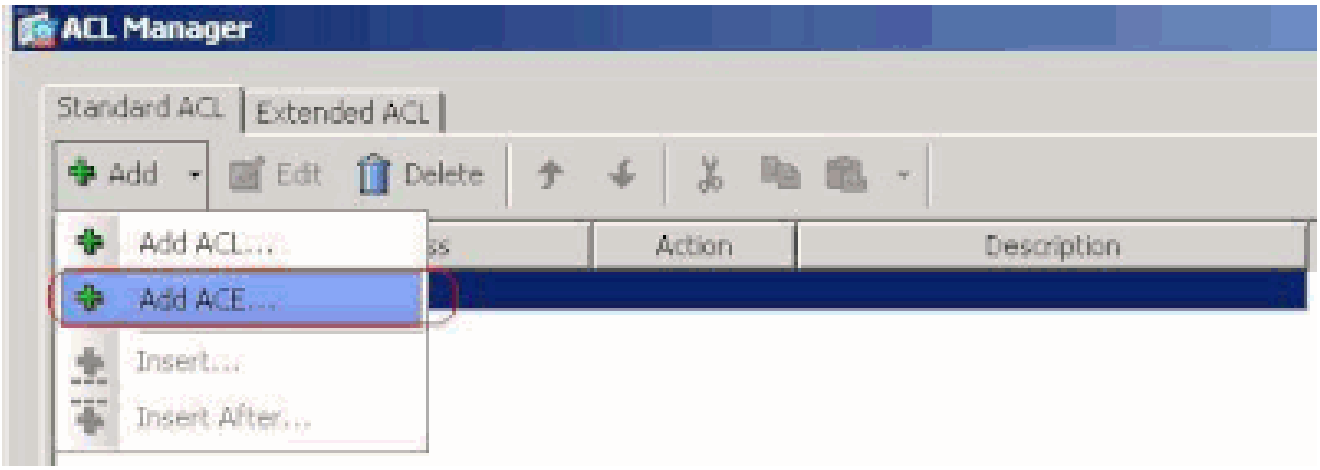
•

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



•

Zodra de ACL is gemaakt, kiest u **Add** > **Add ACE...** om een Access Control Entry (ACE) toe te voegen.



-

Bepaal het ACE dat aan LAN achter ASA beantwoordt. In dit geval is het netwerk 10.0.1.0/24.

a.

Klik op de radioknop **Toestaan**.

b.

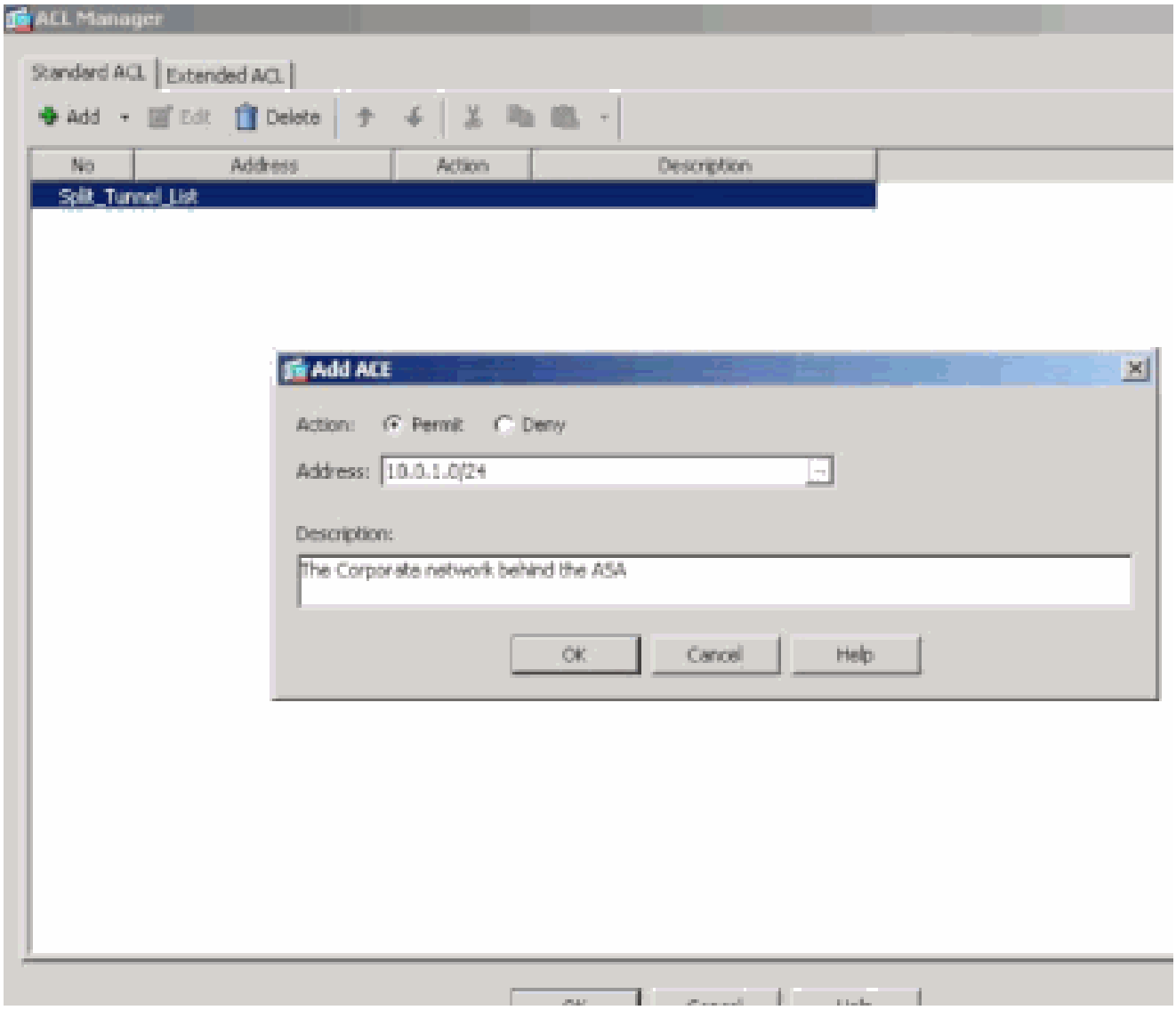
Kies het netwerkadres met masker **10.0.1.0/24**.

c.

(Optioneel) Geef een beschrijving op.

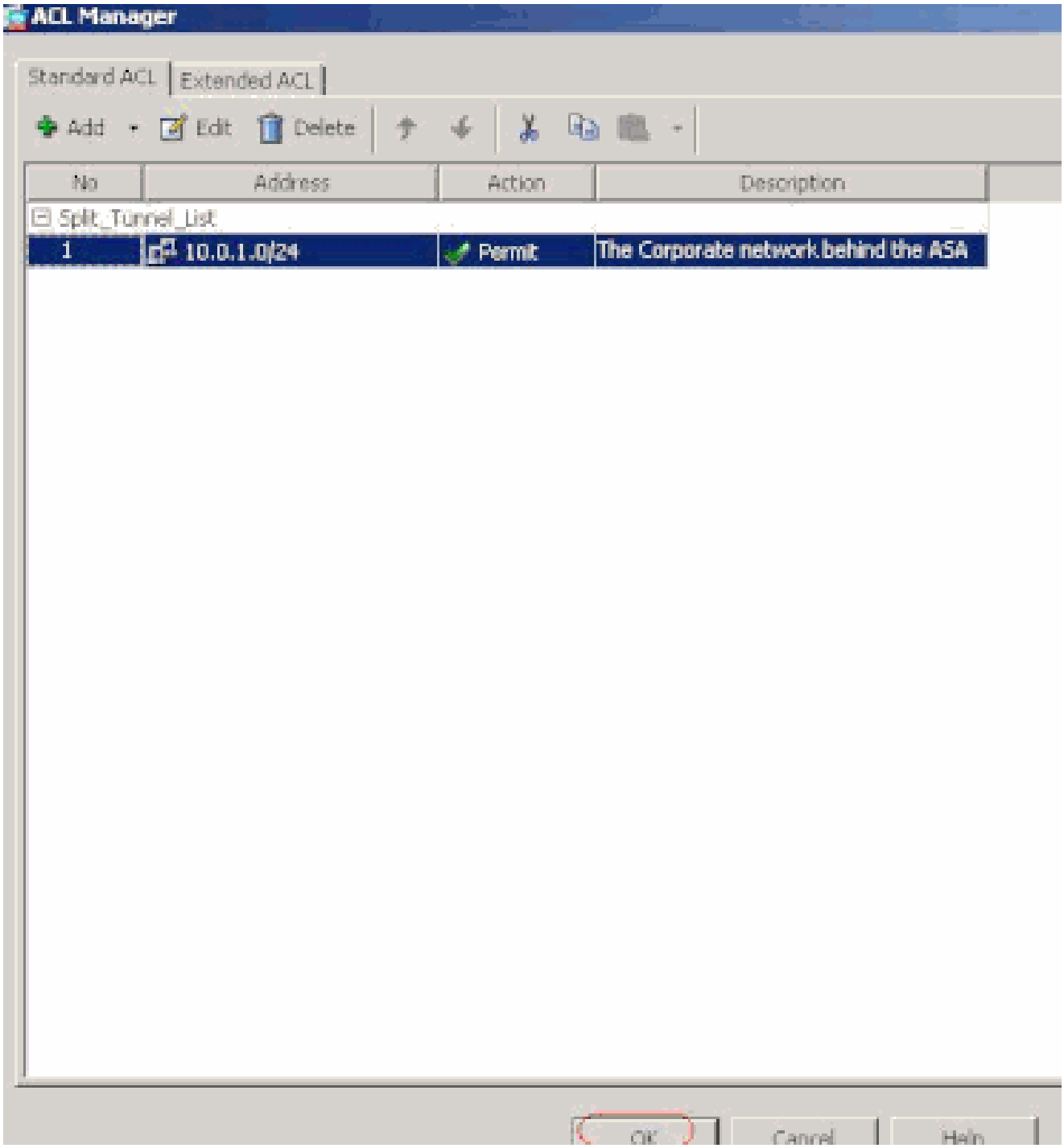
d.

Klik op OK.



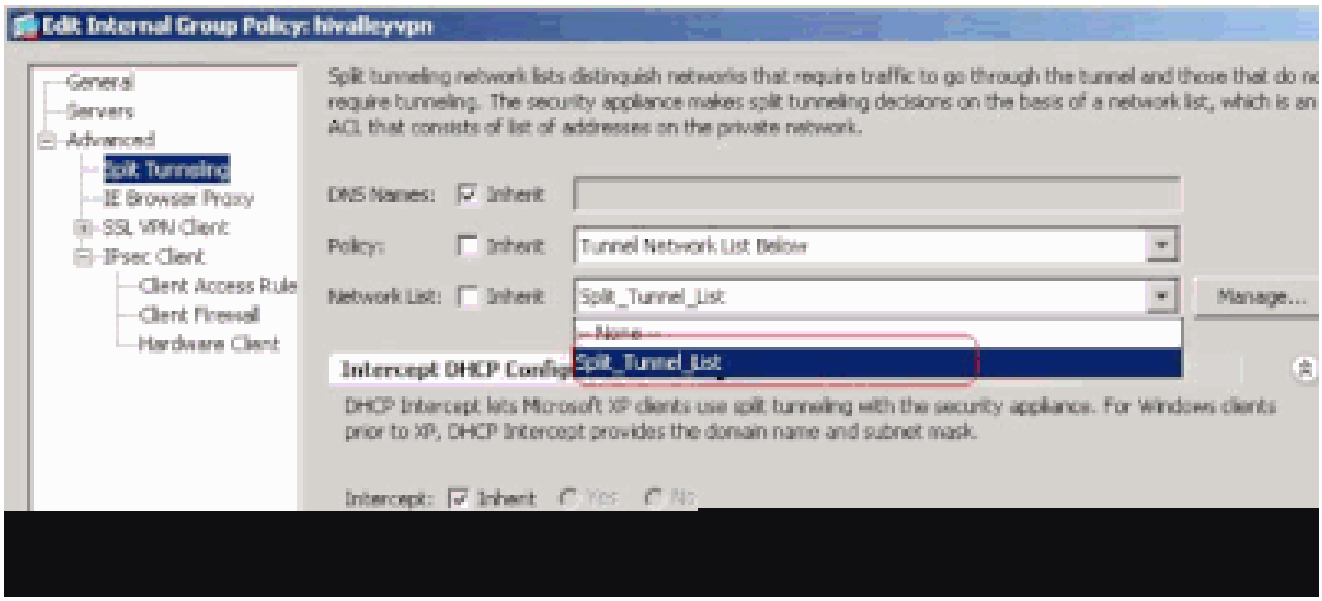
•

Klik op OK om ACL Manager af te sluiten.



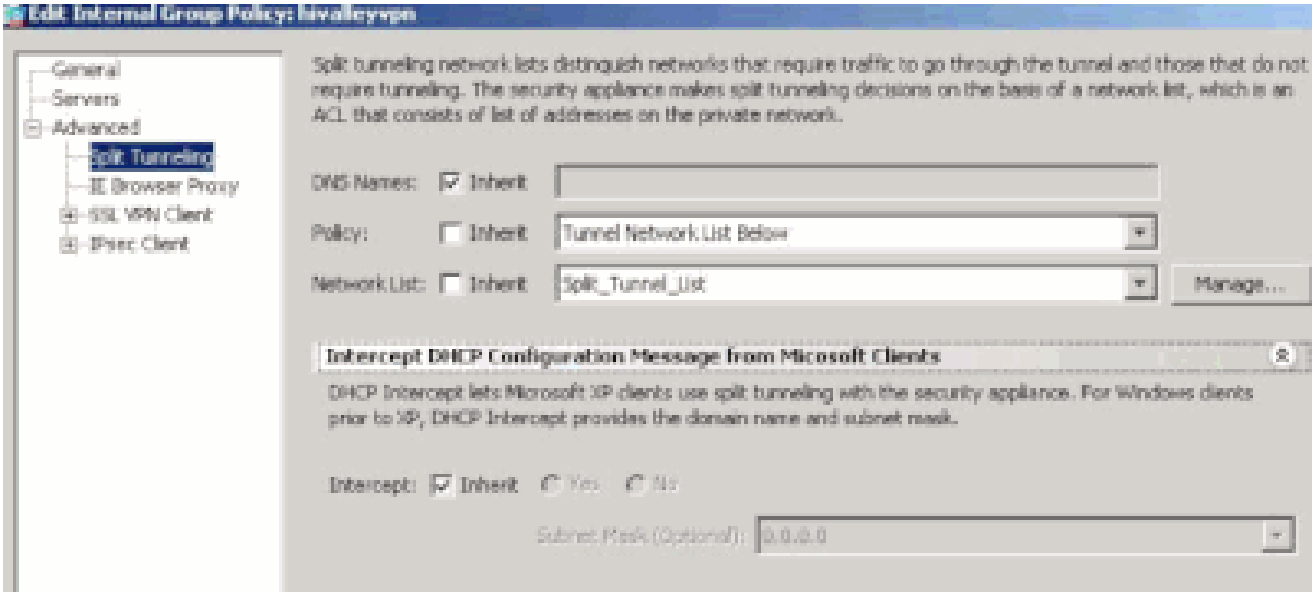
•

Zorg ervoor dat de ACL die u zojuist hebt gemaakt, is geselecteerd voor de netwerklijst van splitste tunnels.



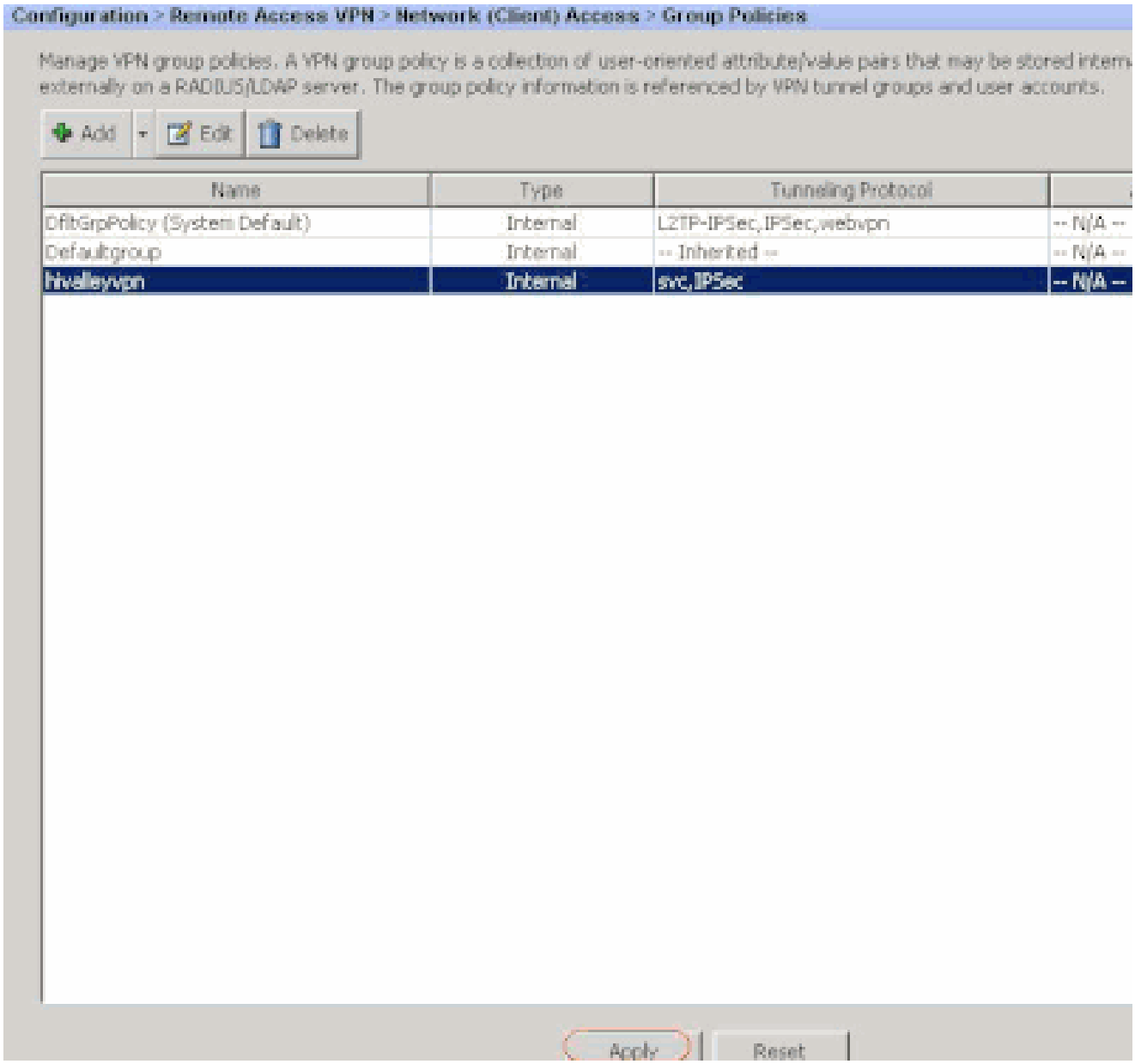
•

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



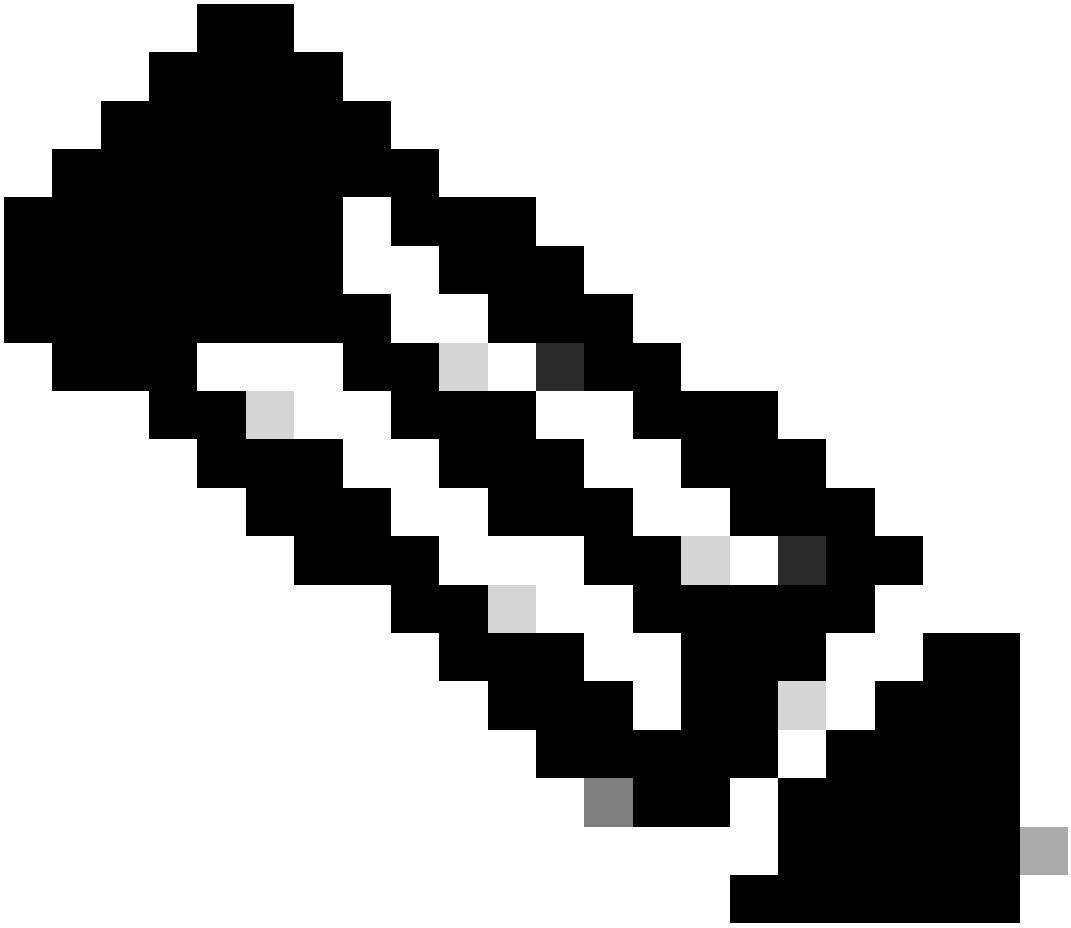
•

Klik op Apply (Toepassen) en vervolgens op Send (Verzenden) (waar vereist) om de opdrachten naar de ASA te sturen.



De ASA 7.x en hoger via CLI configureren

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



Opmerking: de configuratie van de CLI Split-tunneling is hetzelfde voor zowel ASA 7.x als 8.x.

-

Geef de configuratiemodus op.

```
<#root>

ciscoasa>
```

```
enable
```

```
Password: ********
ciscoasa#
```

```
configure terminal
```

```
ciscoasa(config)#
```

-

Maak de toegangslijst die het netwerk achter de ASA definieert.

```
<#root>
```

```
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
```

-

Voer de configuratiemodus voor groepsbeleid in voor het beleid dat u wilt wijzigen.

```
<#root>
```

```
ciscoasa(config)#
```

```
 group-policy hillvalleyvpn attributes
```

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

-

Geef het beleid voor split-tunneling op. In dit geval wordt het beleid **tunnelgespecificeerd**.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-policy tunnelspecified
```

-

Geef de toegangslijst voor split-tunneling op. In dit geval is de lijst **Split_Tunnel_List**.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-network-list value Split_Tunnel_List
```

-

Voer de volgende opdracht uit:

<#root>

```
ciscoasa(config)#
```

tunnel-group hillvalleyvpn general-attributes

-

Koppel het groepsbeleid aan de tunnelgroep

<#root>

```
ciscoasa(config-tunnel-ipsec)#
```

default-group-policy hillvalleyvpn

-

Sluit de twee configuratiemodi af.

<#root>

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

exit

```
ciscoasa(config)#
```

exit

```
ciscoasa#
```

- Sla de configuratie op in niet-vluchtig RAM (NVRAM) en druk op Enter wanneer u wordt gevraagd om de naam van het bronbestand op te geven.

```
<#root>

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 de CLI

Voer de volgende stappen uit:

- Maak de toegangslijst die het netwerk achter de PIX definieert.

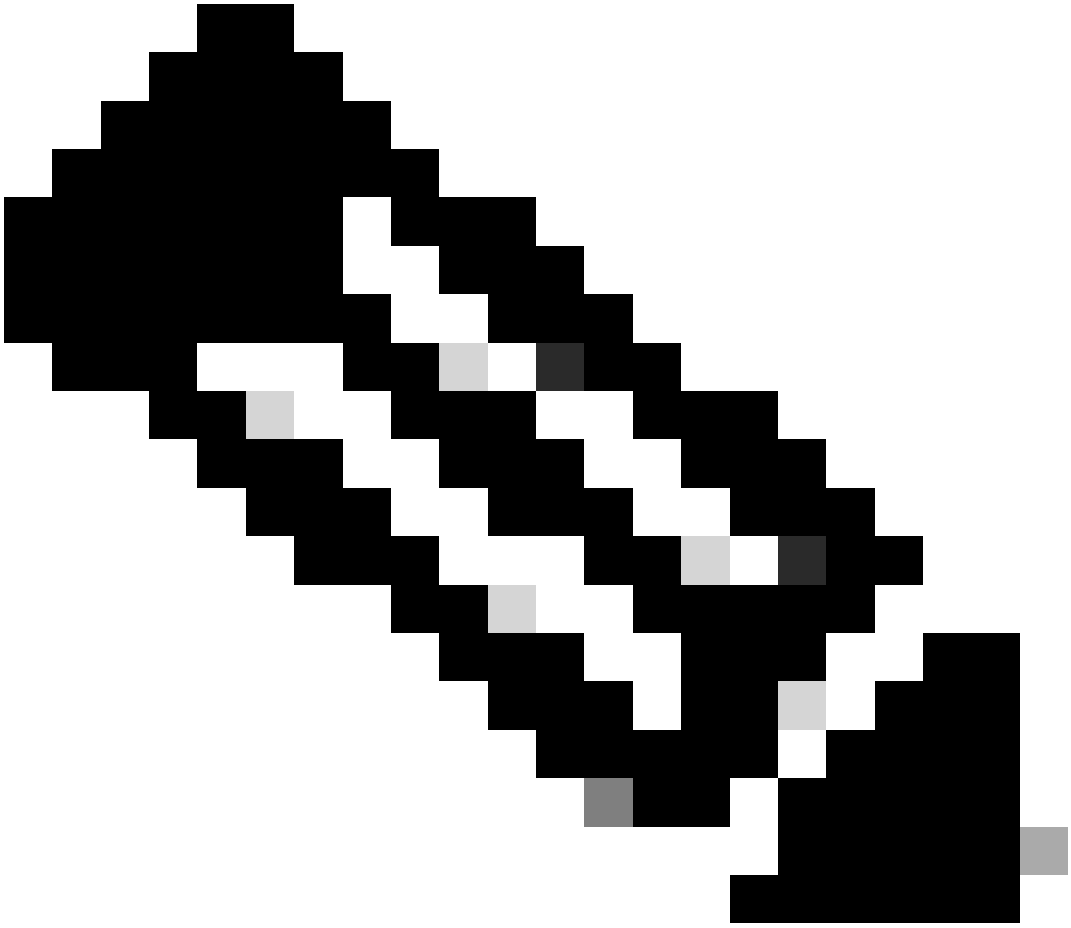
```
<#root>

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

- Maak een VPN-groep **vpn3000** en specificeer de gesplitste tunnelACL zoals aangegeven:

<#root>

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 externe VPN-configuratie voor PIX 6.x.

Verifiëren

Volg de stappen in deze secties om de configuratie te verifiëren.

- Verbinding maken met de VPN-client

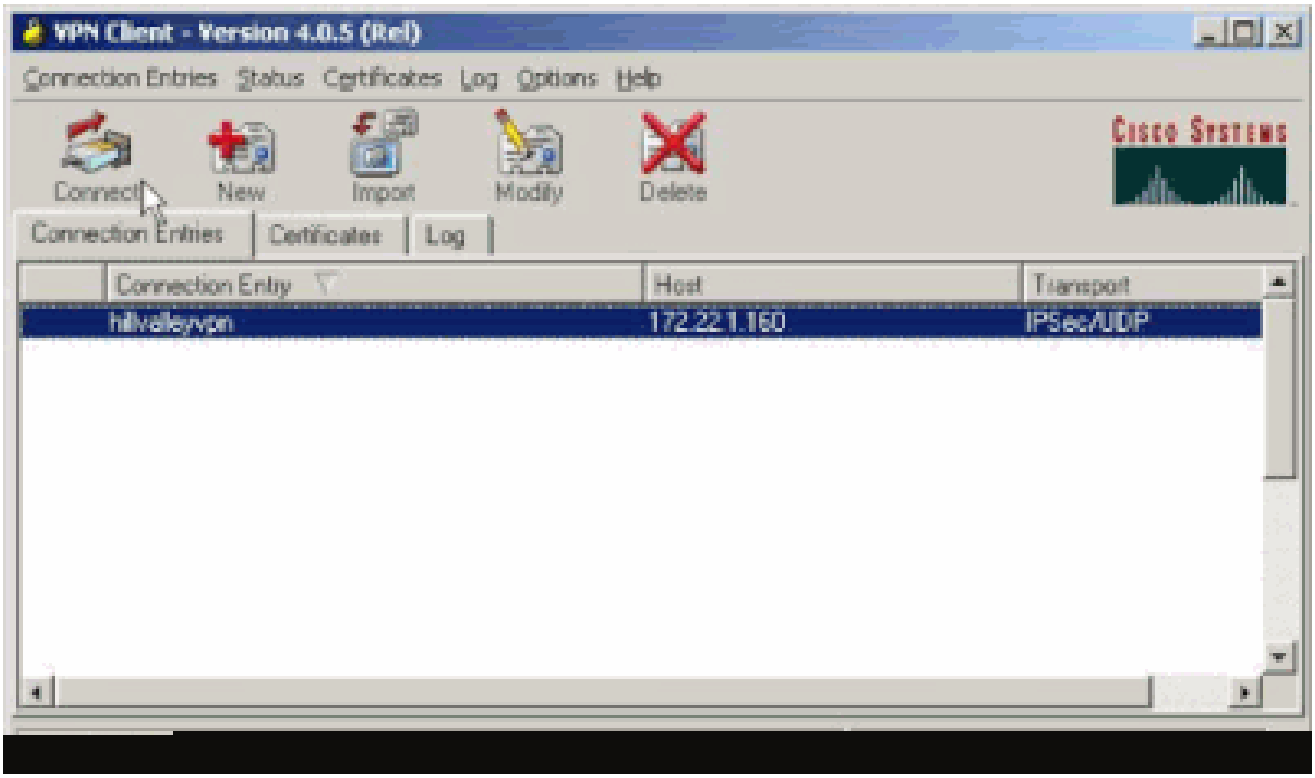
- Het VPN-clientlogboek bekijken

- Lokale LAN-toegang testen met ping

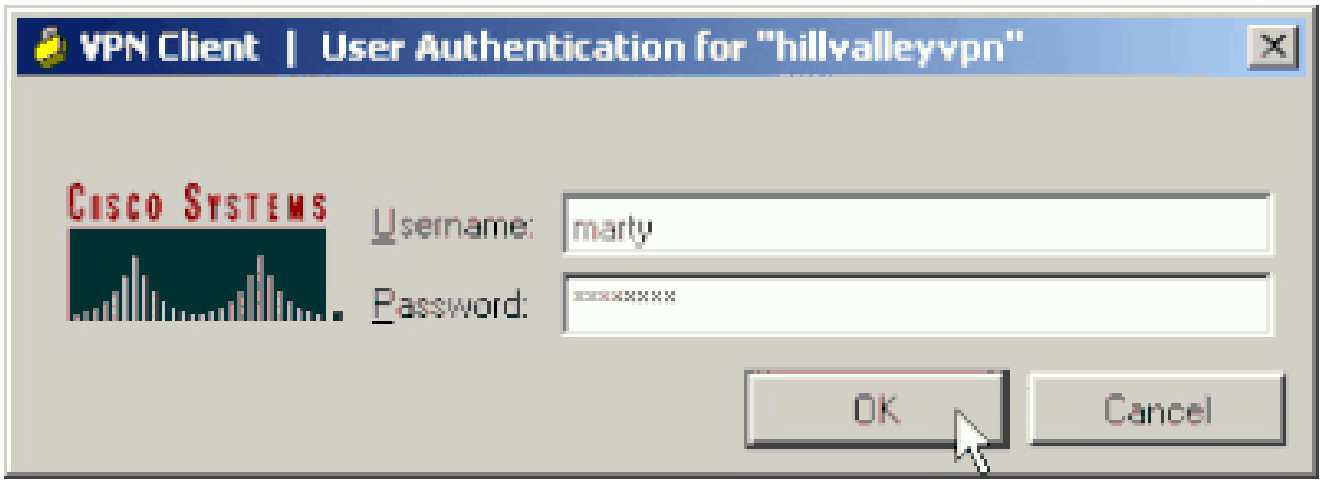
Verbinding maken met de VPN-client

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

- Kies uw verbindingsitem in de lijst en klik op **Verbinden**.

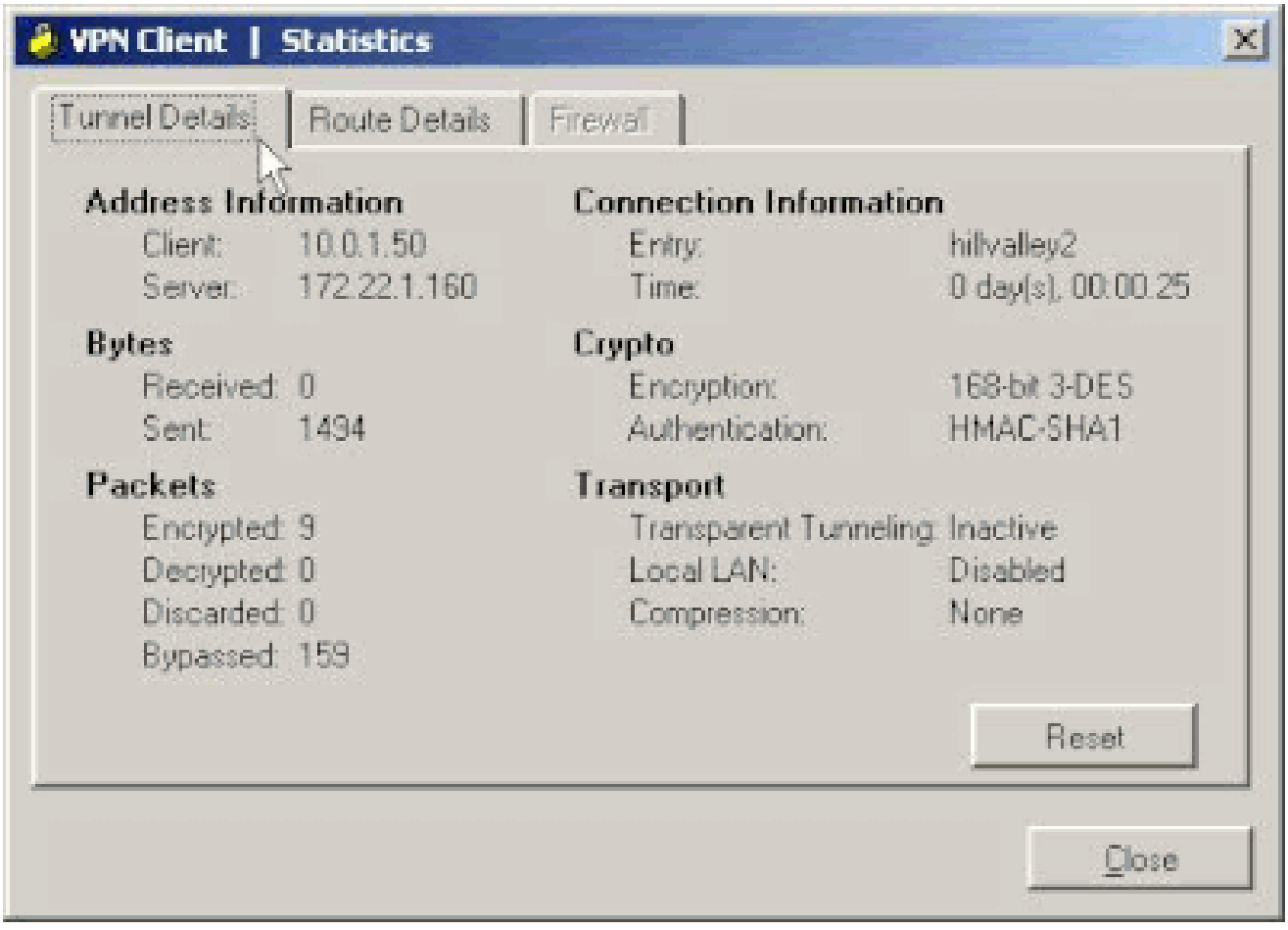


- Voer uw referenties in.



•

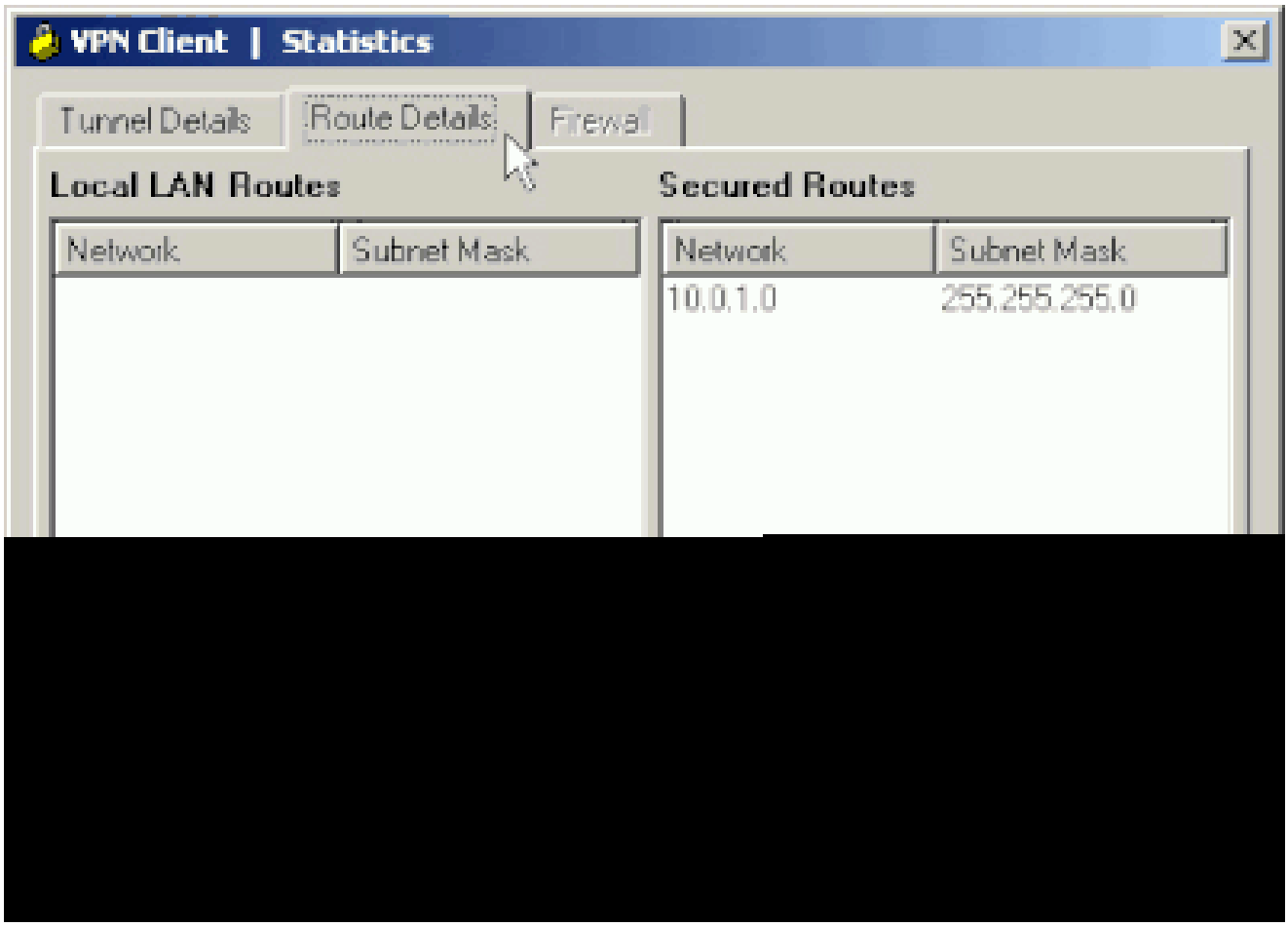
Kies **Status > Statistieken...** om het venster Tunneldetails weer te geven, waar u de gegevens van de tunnel kunt bekijken en het verkeer kunt zien stromen.



•

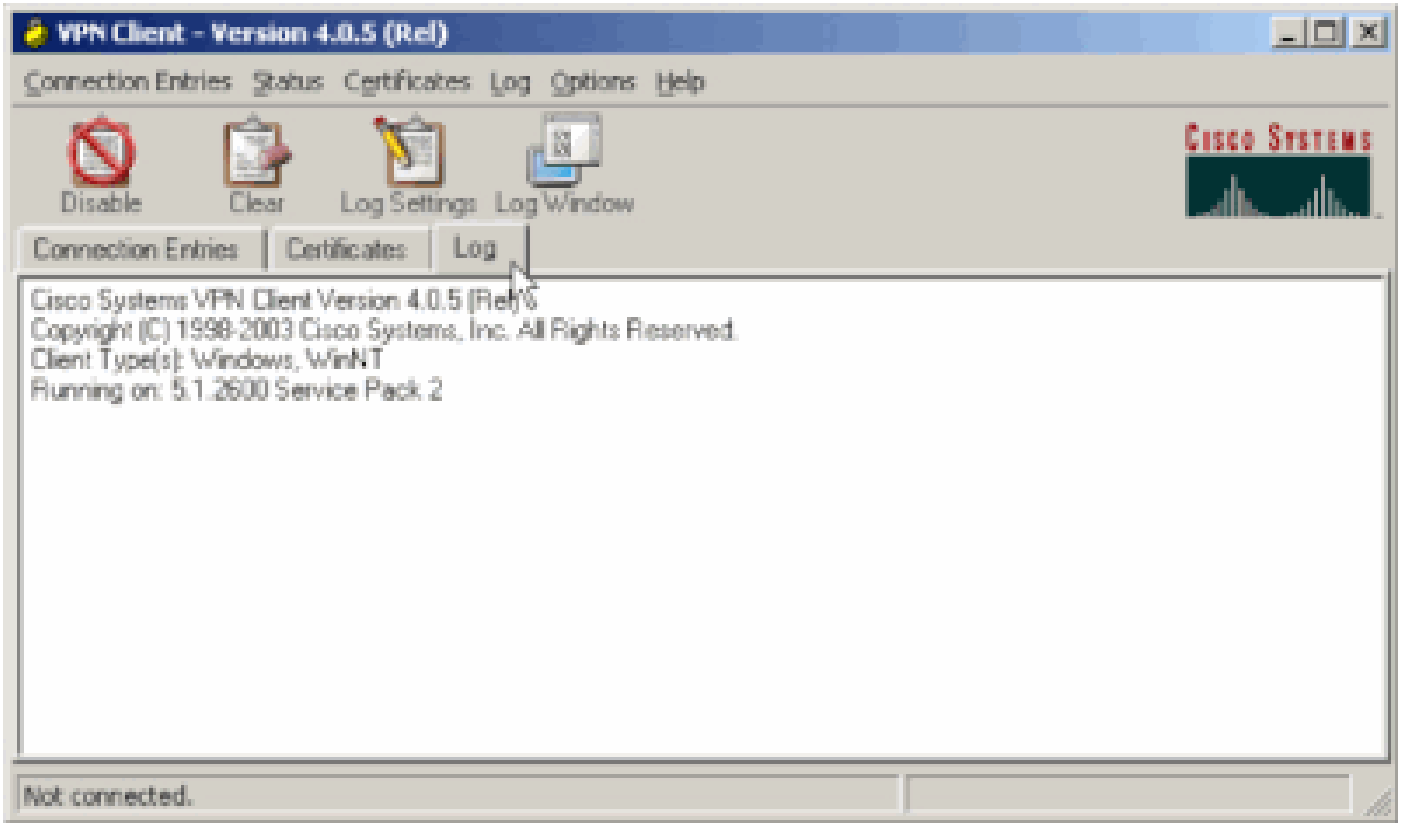
Ga naar het tabblad Routedetails om de routes te zien die de VPN-client voor de ASA beveiligt.

In dit voorbeeld, de VPN-client is het beveiligen van toegang tot 10.0.1.0/24 terwijl al het andere verkeer niet is versleuteld en niet over de tunnel is verzonden.



Het VPN-clientlogboek bekijken

Wanneer u het VPN-clientlogboek onderzoekt, kunt u bepalen of de parameter die gesplitste tunneling specificeert, is ingesteld. Als u het logbestand wilt weergeven, gaat u naar het tabblad Log in de VPN-client. Klik vervolgens op **Log Settings** om aan te passen wat er is vastgelegd. In dit voorbeeld is IKE ingesteld op **3 - High**, terwijl alle andere log elementen ingesteld zijn op **1 - Low**.




```
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/6    IKE/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 er een tunnel wordt gegraven naar de ASA, is om de **ping-**opdracht op de opdrachtregel van Windows te gebruiken. Het lokale LAN van de VPN-client is 192.168.0.0/24 en er is een andere host aanwezig op het netwerk met een IP-adres van 192.168.0.3.

```
   <#root>

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 Split-tunnelACL

Er is een beperking met het aantal ingangen in een ACL die voor gesplitste tunnel wordt gebruikt. Het wordt aanbevolen niet meer dan 50-60 ACE-waarden te gebruiken voor een bevredigende functionaliteit. U wordt geadviseerd om de subnetting eigenschap uit te voeren om een waaier van IP adressen te behandelen.

Gerelateerde informatie

- **PIX/ASA 7.x as a Remote VPN Server using ASDM Configuration Example (Configuratievoorbeeld van PIX/ASA 7.x als externe VPN-server via ASDM)**
- **Adaptieve security applicaties van Cisco ASA 5500 Series**
- **Cisco Technical Support en downloads**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.