Configuratievoorbeeld van VPN-client en AnyConnect-client voor lokaal LAN

Inhoud

Inleiding

Dit document beschrijft hoe de Cisco VPN-client of de Cisco AnyConnect Secure Mobility Client **alleen** toegang tot hun lokale LAN kan krijgen wanneer deze is afgestemd op een Cisco adaptieve security applicatie (ASA) 5500 Series of de ASA 5500-X Series. Dankzij deze configuratie kunnen Cisco VPN-clients of Cisco AnyConnect Secure Mobility Client beveiligde toegang tot bedrijfsbronnen via IPsec, Secure Socket Layer (SSL) of Internet Key Exchange versie 2 (IKEv2) en de client nog steeds activiteiten uitvoeren zoals afdrukken waar de client is gevestigd. Als het is toegestaan, wordt het voor het internet bestemde verkeer nog steeds aan de ASA aangepast.

> Opmerking: Dit is geen configuratie voor gesplitste tunneling, waarbij de client geen gecodeerde toegang tot internet heeft terwijl hij verbonden is met de ASA of PIX. Raadpleeg PIX/ASA 7.x: Toestaan Split Tunneling voor VPN-clients in het ASA Configuration Voorbeeld voor informatie over het configureren van gesplitste tunneling op de ASA.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat er al een functionele VPN-configuratie voor externe toegang op de

ASA bestaat.

Raadpleeg PIX/ASA 7.x als een externe VPN-server met ASDM Configuration Voorbeeld voor de Cisco VPN-client als deze niet al is geconfigureerd.

Raadpleeg ASA 8.x VPN-toegang met AnyConnect SSL VPN-clientconfiguratievoorbeeld voor Cisco AnyConnect Secure Mobility Client als deze niet al is ingesteld.

Gebruikte componenten

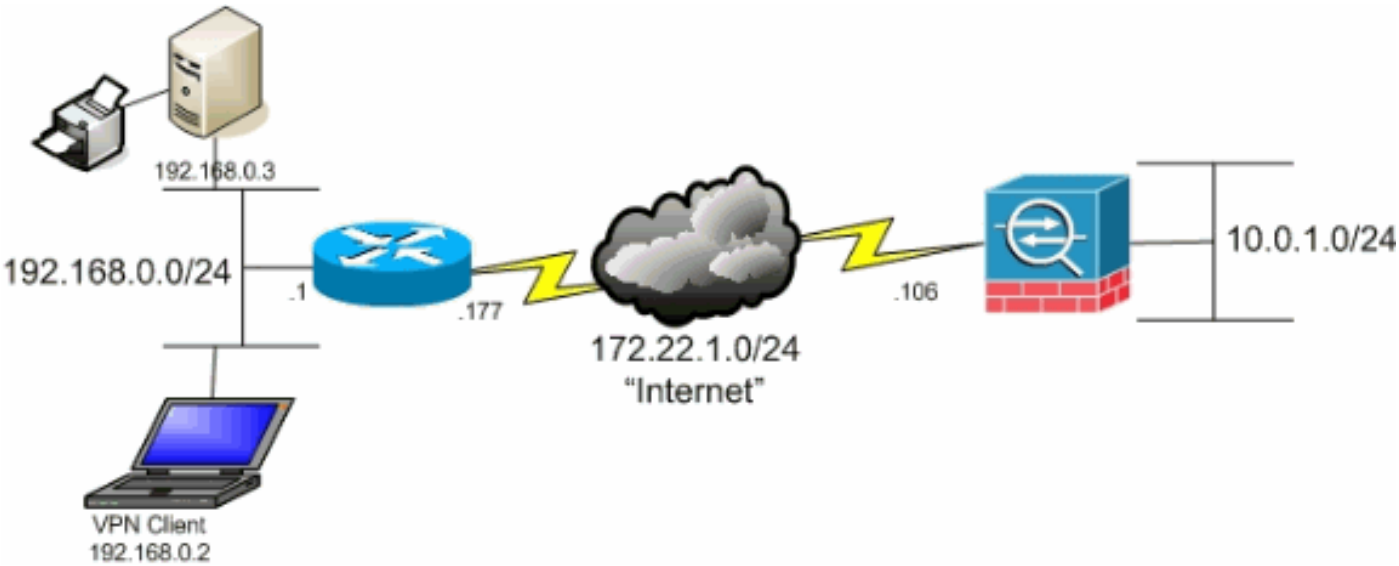
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA 5500 Series versie 9(2)E1
- Cisco Adaptieve Security Devices Manager (ASDM) versie 7.1(6)
- Cisco VPN-clientversie 5.0.07.040
- Cisco AnyConnect Secure Mobility Client versie 3.1.5152

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.

Netwerkdiagram

De client is gevestigd op een typisch netwerk van het Bureau van het Kleine Huis/van het Bureau van het Huis (SOHO) en sluit over het Internet aan op het hoofdbureau.



Achtergrondinformatie

In tegenstelling tot een klassiek gesplitst tunneling scenario waarin al het internetverkeer niet versleuteld wordt, wanneer u lokale LAN-toegang voor VPN-clients toestaat, kunnen deze clients ongeversleuteld communiceren met alleen apparaten op het netwerk waarop ze zich bevinden. Bijvoorbeeld, een client die lokaal LAN toegang terwijl verbonden met de ASA van huis wordt verleend kan aan zijn eigen printer afdrukken maar heeft geen toegang tot het internet zonder eerst het verkeer via de tunnel te verzenden.

Een toegangslijst wordt gebruikt om lokale LAN-toegang op veel dezelfde manier mogelijk te maken als een gesplitste tunneling in de ASA. In plaats van te definiëren welke netwerken versleuteld *zouden moeten worden*, definieert de toegangslijst in dit geval echter welke netwerken *niet* versleuteld *moeten worden*. Ook hoeven de eigenlijke netwerken in de lijst, in tegenstelling tot het scenario voor een gesplitste tunneling, niet bekend te zijn. In plaats daarvan voorziet de ASA in een standaardnetwerk van 0.0.0.0/255.255.255.255, dat wordt begrepen als het lokale LAN van de client.

> Opmerking: Wanneer de client is aangesloten en geconfigureerd voor plaatselijke LAN-toegang, *kunt* u *niet* op het lokale LAN *bij naam afdrukken of bladeren*. U kunt echter ook door het IP-adres bladeren of afdrukken. Zie het gedeelte Problemen oplossen van dit document voor meer informatie en werkpunten voor deze situatie.

Local LAN Access voor VPN-clients of de AnyConnect Secure Mobility Client configureren

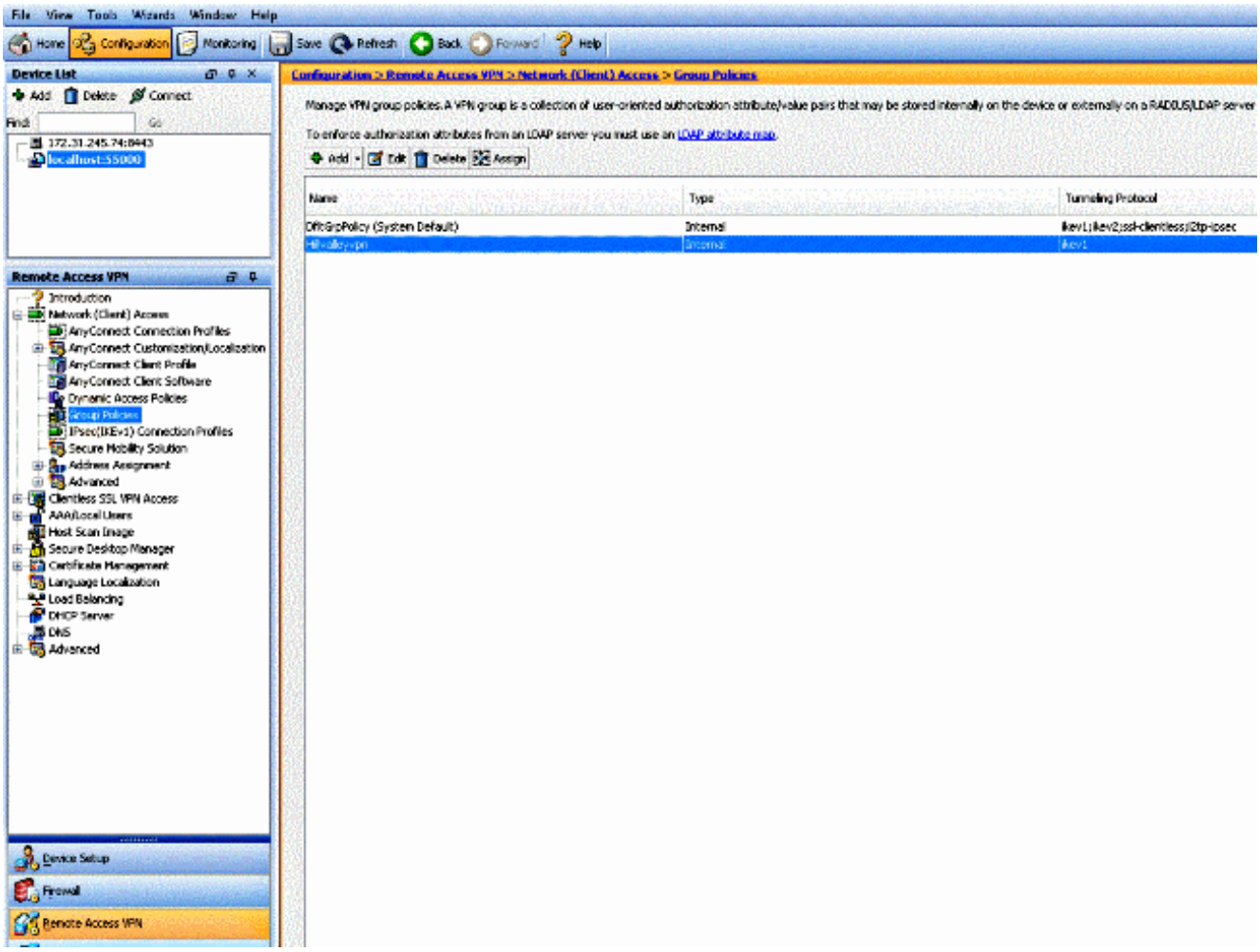
Voltooi deze taken om Cisco VPN-clients of Cisco AnyConnect Secure Mobility Clients toegang te geven tot hun lokale LAN terwijl ze met de ASA zijn verbonden:

- ASA configureren via de ASDM of de ASA configureren via de CLI
- Cisco AnyConnect Secure Mobility Client configureren

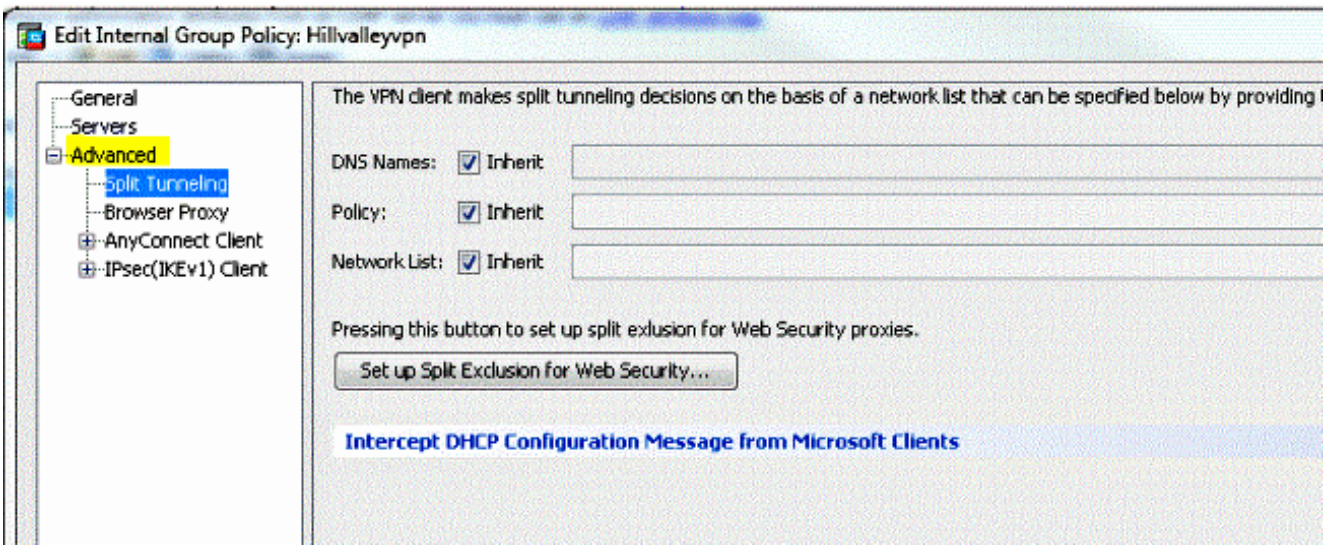
ASA configureren via ASDM

Voltooi deze stappen in de ASDM-modus zodat VPN-clients lokale LAN-toegang hebben terwijl ze met de ASA zijn verbonden:

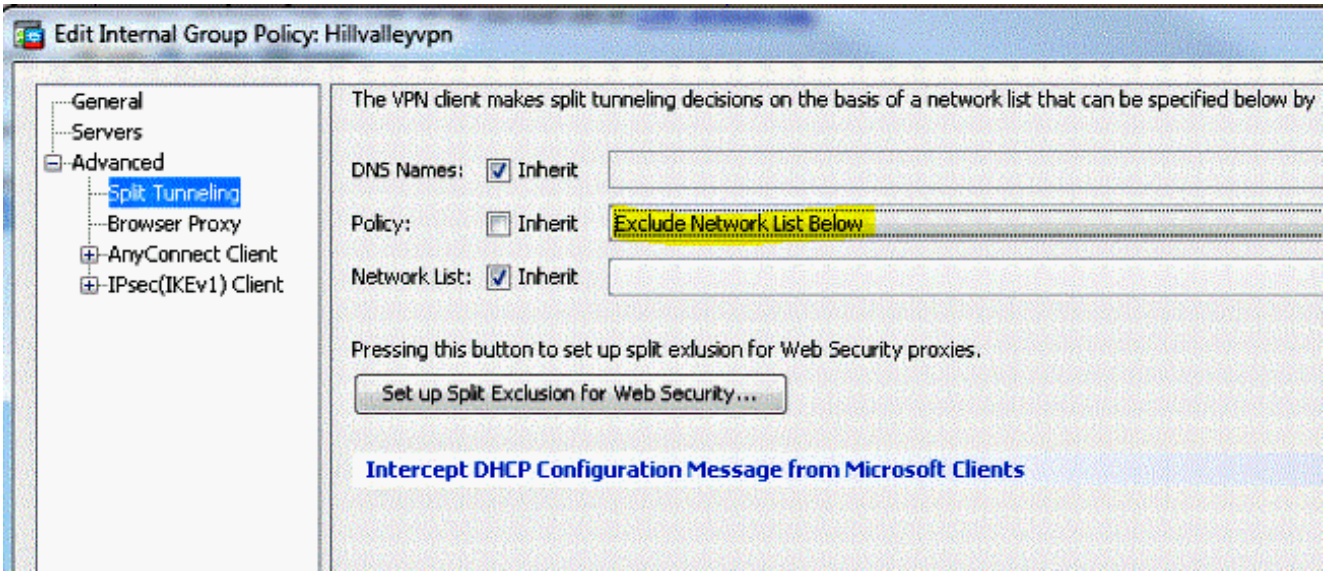
1. Kies **Configuration > Remote Access VPN > Network (Client) Access > Group Policy** en selecteer het groepsbeleid waarin u lokale LAN-toegang wilt inschakelen. Klik vervolgens op **Bewerken**.



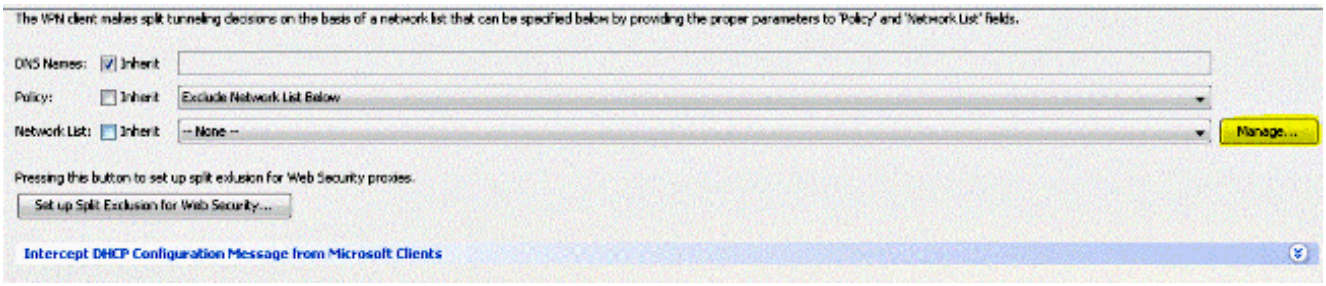
2. Ga naar **Geavanceerd > Split-tunneling**.



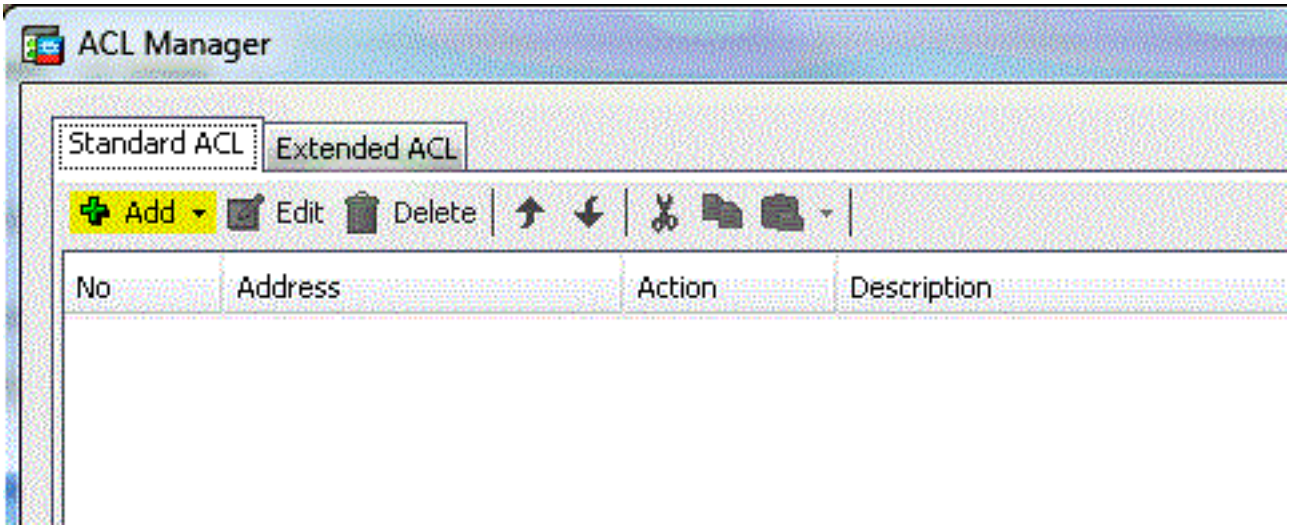
3. Schakel het dialoogvenster **Inherit** voor beleid uit en kies **onderstaande netwerklijst uitsluiten**.



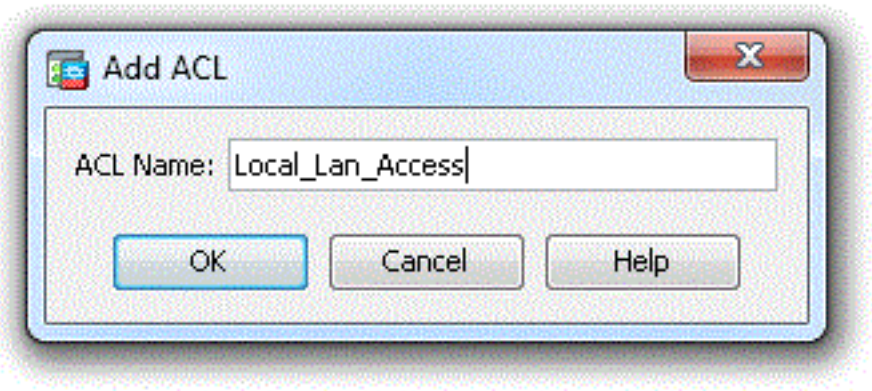
4. Schakel het vakje **Inherit** voor netwerklijst uit en klik vervolgens op **Bewerken** om de Manager Access Control List (ACL) te starten.



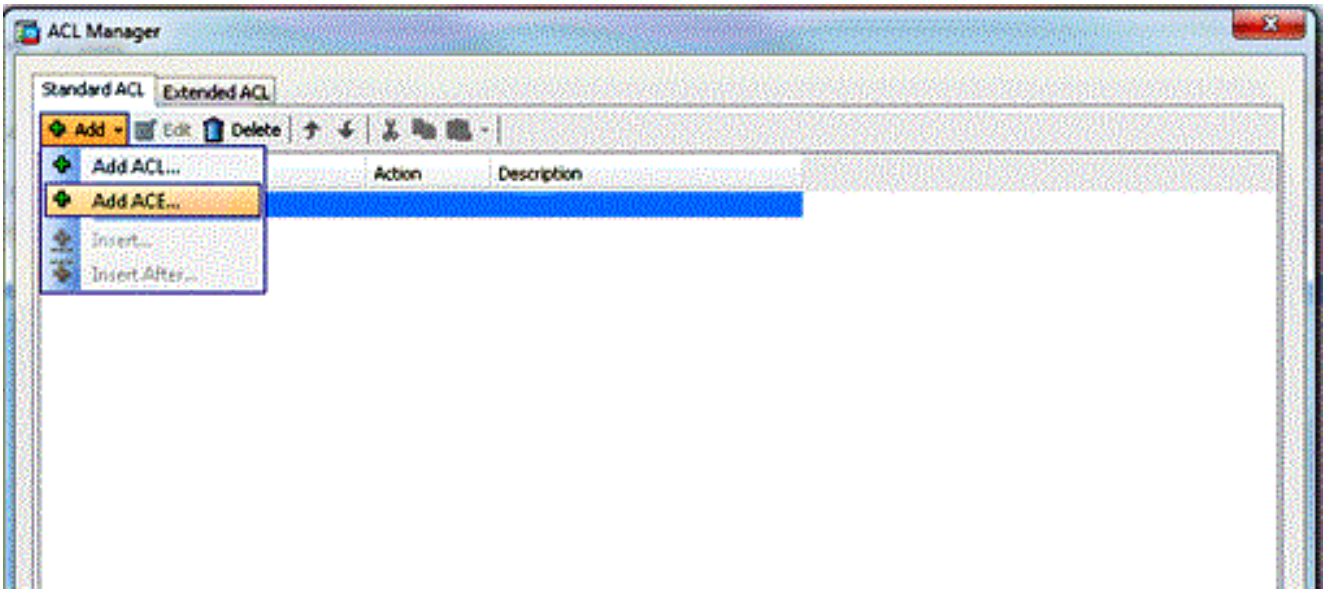
5. Kies in ACL Manager **Add > Add ACL...** om een nieuwe toegangslijst op te stellen.



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

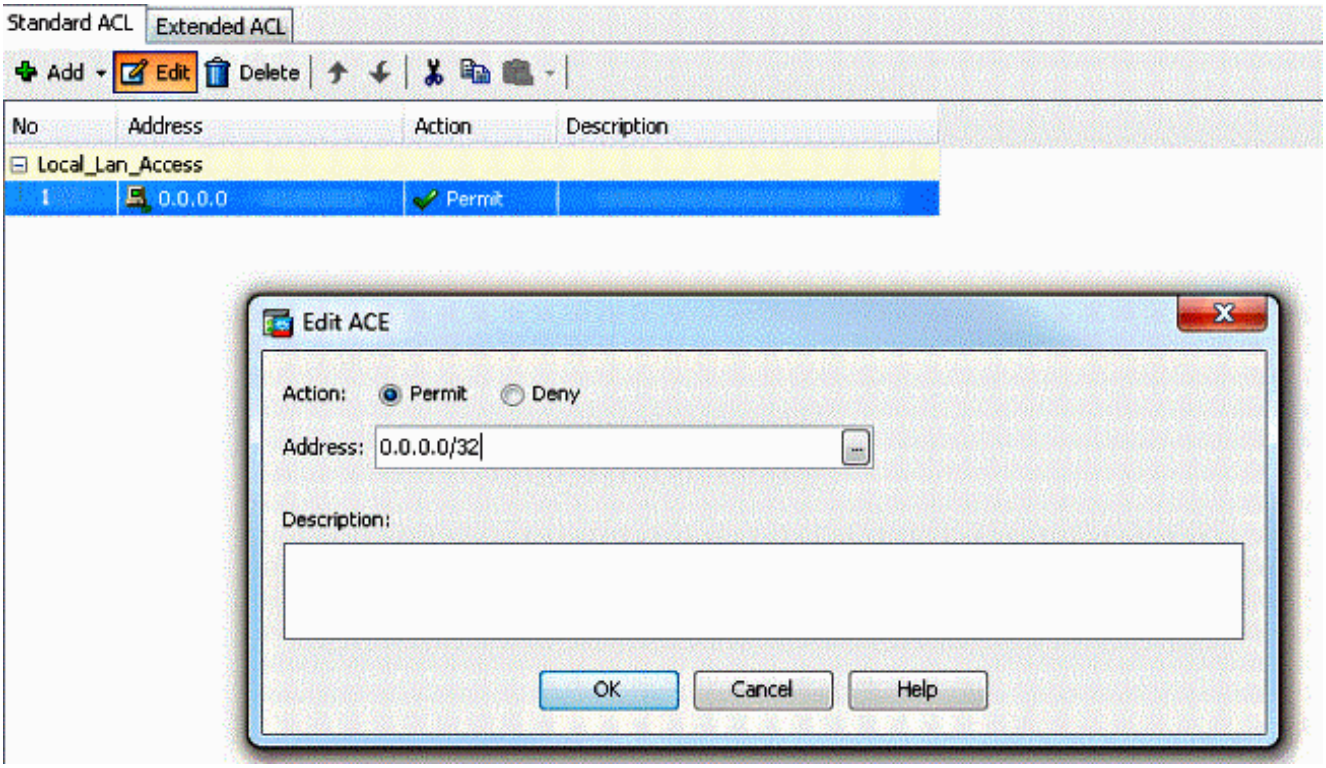


7. Zodra ACL wordt gecreëerd, kies **Add > Add ACE...** om een toegangscontrole-ingang (ACE) toe te voegen.

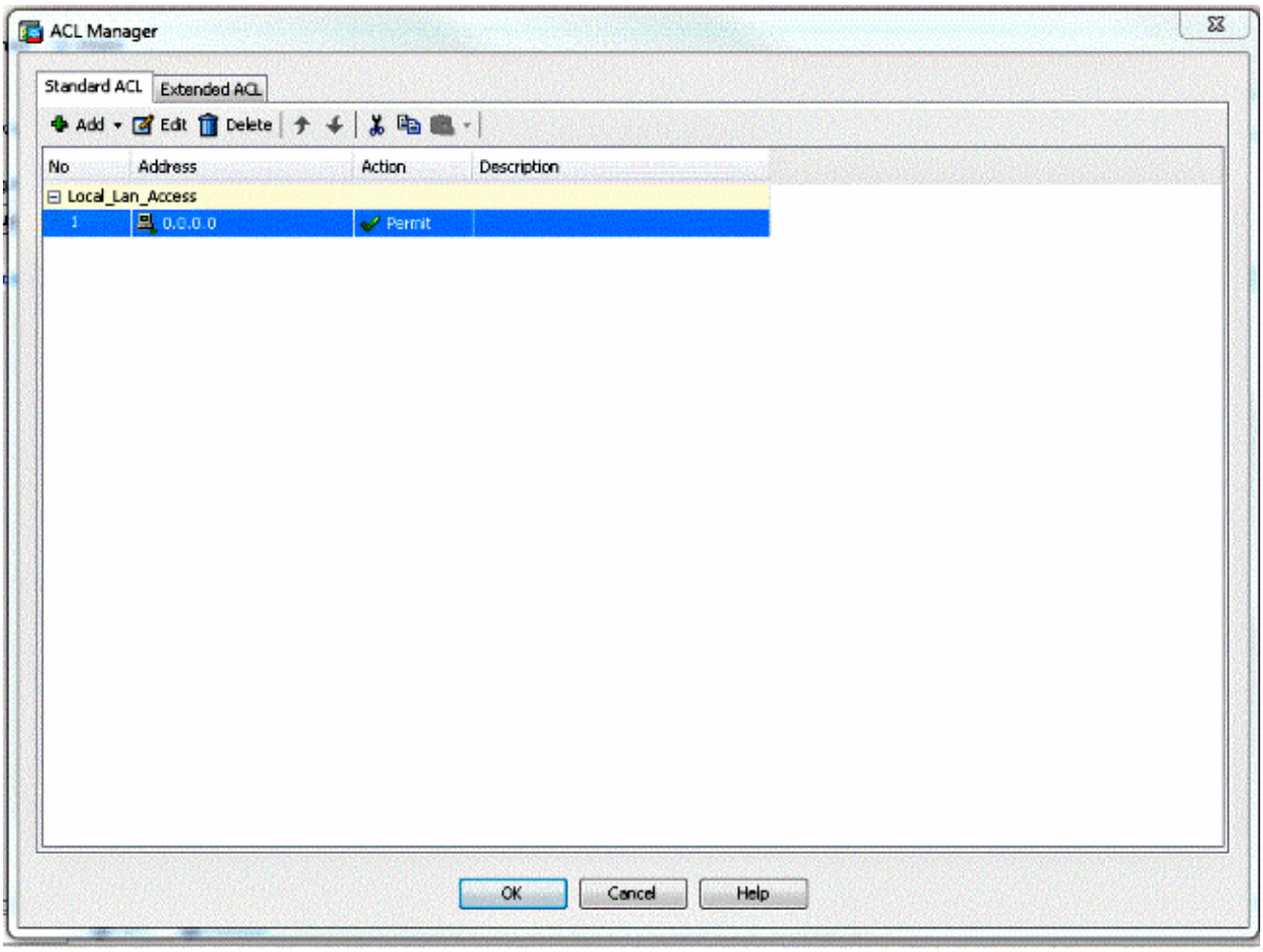


8. Defineer de ACE die overeenkomt met het lokale LAN van de client.

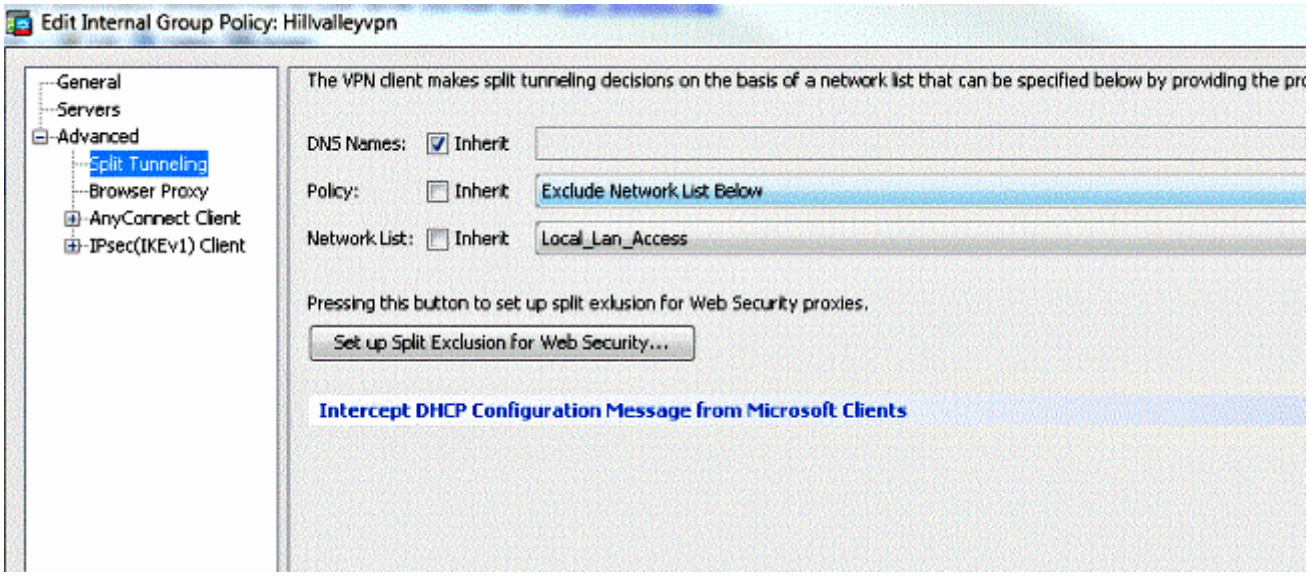
   Kies **Toestemming**.Kies een IP-adres van **0.0.0.0**Kies een netwerkmasker van **2/32**.*(Optioneel)* Geef een beschrijving.Klik op OK.



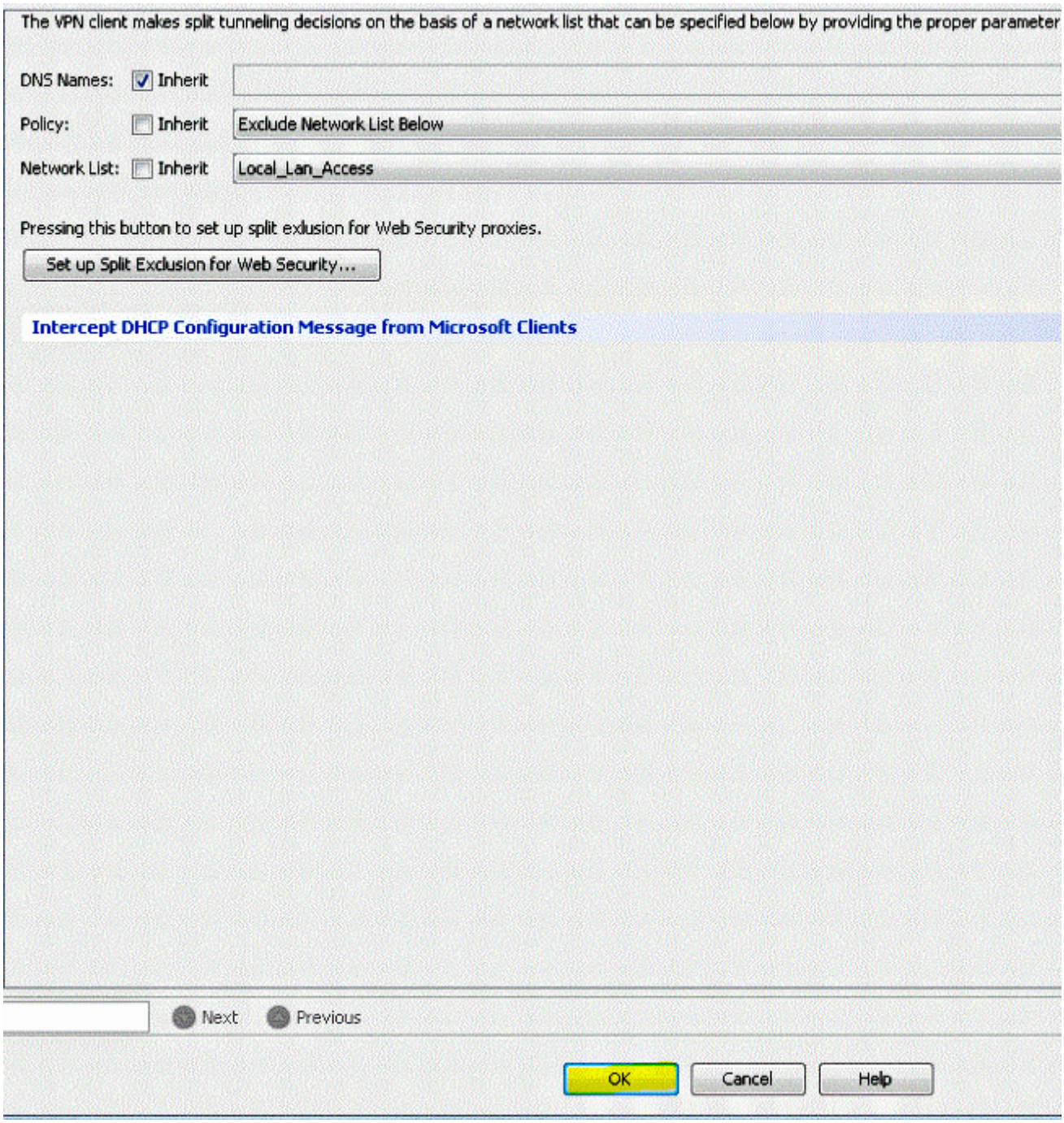
9. Klik op **OK** om de ACL-Manager te verlaten.



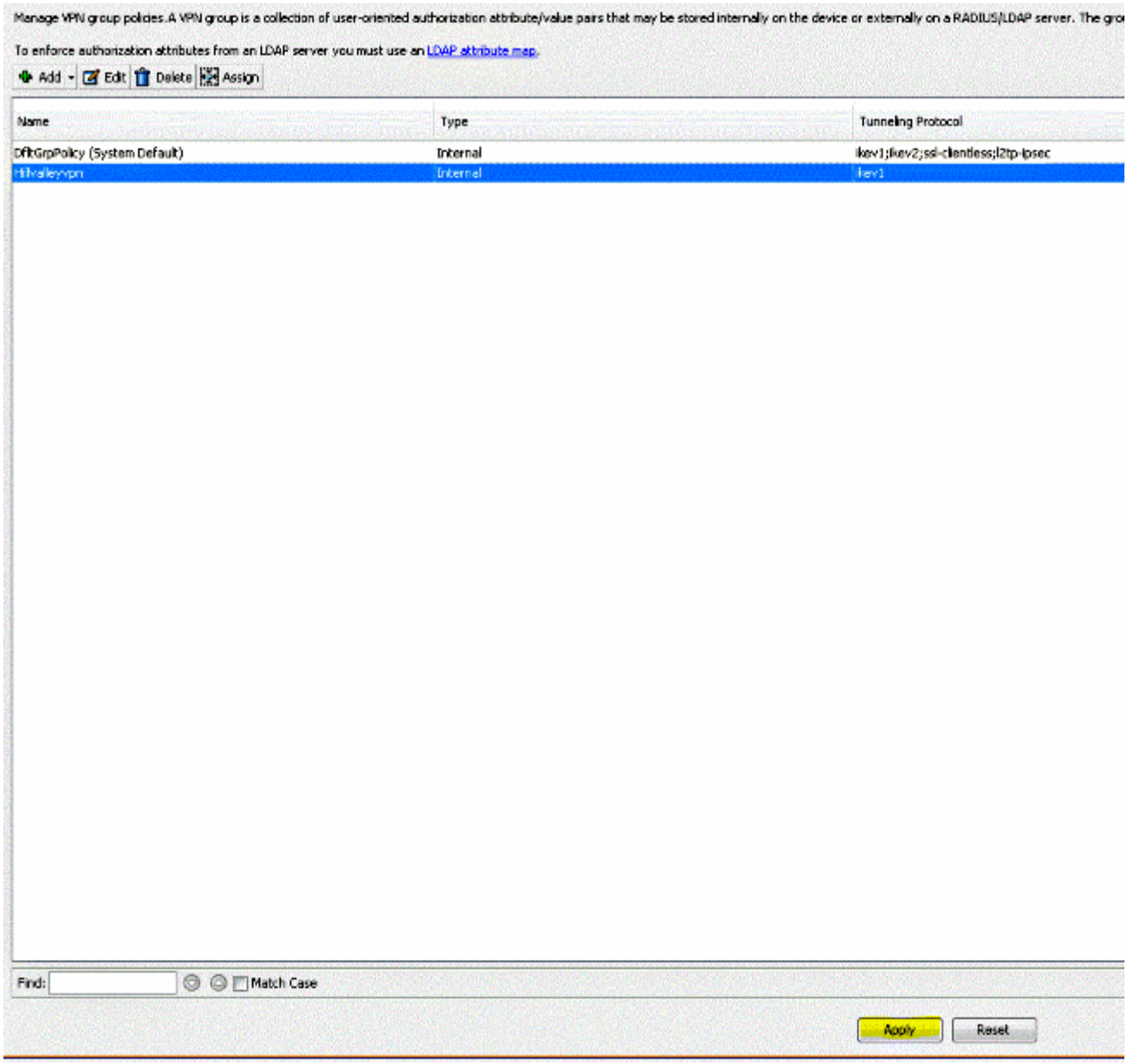
10. Verzeker u dat ACL die u zojuist hebt gemaakt, is geselecteerd voor de netwerklijst Split Tunnel.



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 configureren via de CLI

In plaats van de ASDM te gebruiken, kunt u deze stappen in de ASA CLI voltooien om VPN Clients toe te staan om lokale LAN toegang te hebben terwijl u met de ASA verbonden bent:

1. Geef de configuratie op.

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

2. Maak de toegangslijst om lokale LAN-toegang te verlenen.

```
ciscoasa(config)#access-list Local_LAN_Access remark Client Local LAN Access
ciscoasa(config)#access-list Local_LAN_Access standard permit host 0.0.0.0
```

Voorzichtig: Vanwege veranderingen in de syntaxis van ACL tussen ASA-software versies 8.x tot 9.x, is deze ACL niet langer toegestaan en beheerders zien deze foutmelding

wanneer ze proberen de ACL te configureren:
`rtpvoutbound6 (configuratie)# **access-list teststandaard host 0.0.0.0**`
`FOUT: ongeldig IP-adres`

Het enige wat is toegestaan is:
`rtpv-outbound6 (configuratie)# **access-list teststandaardvergunning any4**`

Dit is een bekend probleem en is aangepakt door Cisco bug-ID CSCut3131. upgrade naar een versie met de oplossing voor dit probleem om lokale LAN-toegang te kunnen configureren.

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

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

4. Specificeer het gesplitste tunnelbeleid. In dit geval wordt het beleid **uitgesloten**.

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

5. Specificeer de gesplitste tunneltoegangslijst. In dit geval is de lijst **Local_LAN_Access**.

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

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#
```

Cisco AnyConnect Secure Mobility Client configureren

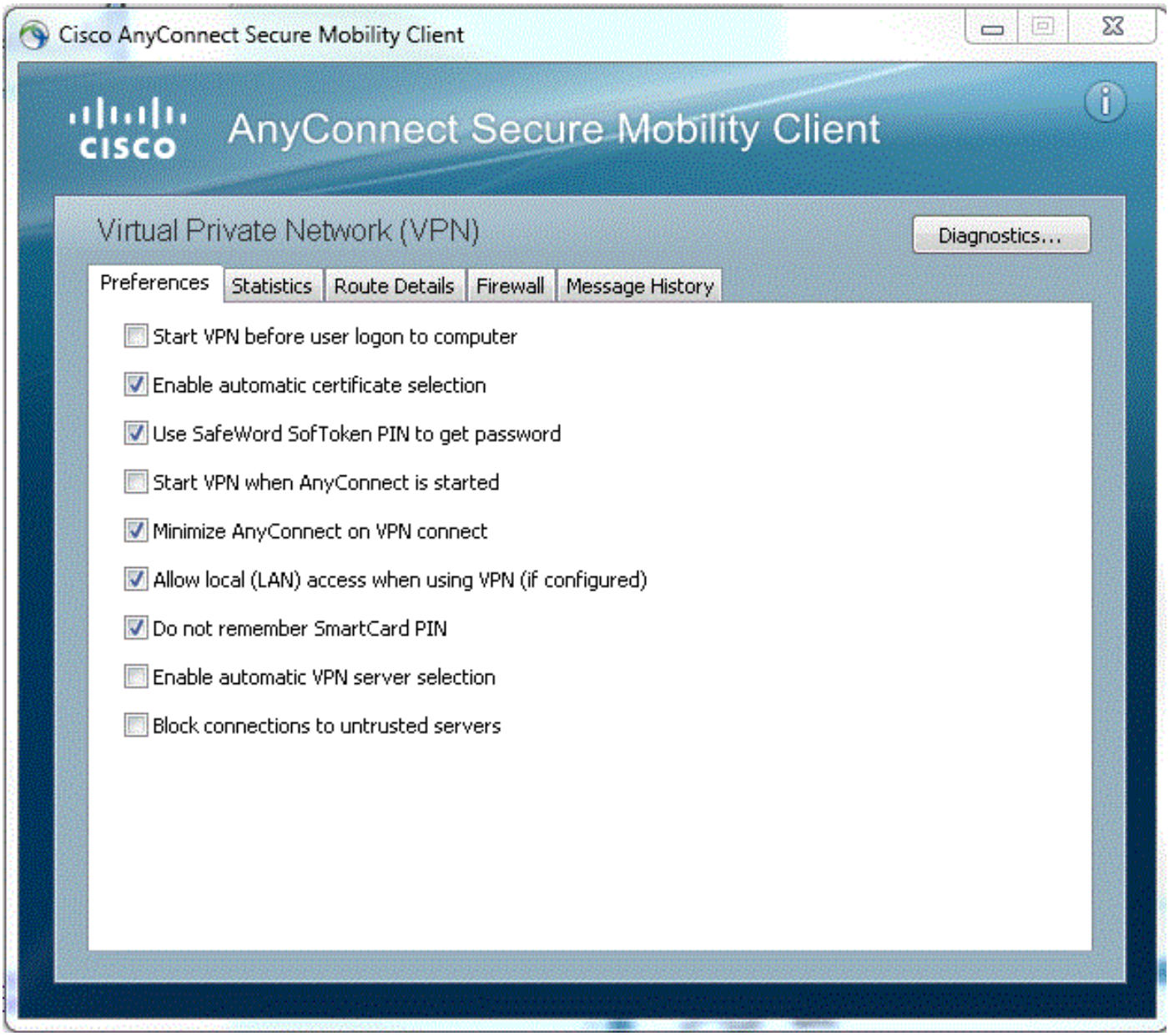
Raadpleeg voor de configuratie van Cisco AnyConnect Secure Mobility Client de SSL VPN-verbinding met SVC van **ASA 8.x: Split-tunneling voor AnyConnect VPN-client toestaan in het ASA Configuration-voorbeeld**.

Voor tunneling via splitter/uitsluiten moet u **LocalLanAccess** toestaan op de AnyConnect-client. Alle tunneling gesplitst wordt beschouwd als een lokale LAN-toegang. Als u de functie Splitsen-tunneling wilt gebruiken, moet u de voorkeur **LocalLAN** Access toestaan in de **voorkeuren** van **AnyConnect VPN-client** inschakelen. Standaard wordt de lokale LAN-toegang uitgeschakeld.

Om lokale LAN-toegang mogelijk te maken en daarom tunneling door splitsingen uit te sluiten, kan een netwerkbeheerder deze in het profiel inschakelen of kunnen gebruikers dit in hun voorkeuren-instellingen inschakelen (zie de afbeelding in de volgende sectie). Om lokale LAN-toegang toe te staan, selecteert een gebruiker het aankruisvakje **Toegang tot** lokaal **LAN toestaan** als een gesplitste tunneling is ingeschakeld op de beveiligde gateway en is geconfigureerd met het **gesplitste-tunnel-beleid exclusief opgegeven** beleid. Daarnaast kunt u het VPN-clientprofiel configureren als lokale LAN-toegang is toegestaan met **<LocalLAN AccessControllable="werkelijk">True</LocalLink LANLANLANLANLANLANLAN LAN LAN** Access **LAN LAN LAN** Access **LAN LAN** Access--LANLANLAN .

Voorkeuren voor gebruikers

Dit zijn de selectie die u moet maken in het tabblad Voorkeuren op de Cisco AnyConnect Secure Mobility Client om lokale LAN-toegang toe te staan.



XML-profiel

Hier is een voorbeeld van hoe je het VPN-clientprofiel met XML kunt configureren.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
```

```
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic
</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
</AnyConnectProfile>
```

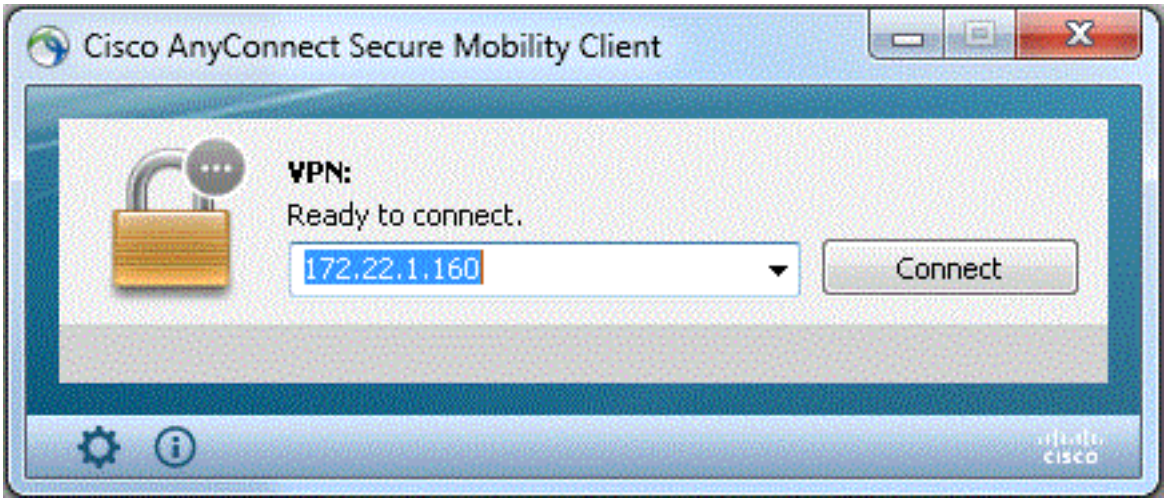
Verifiëren

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

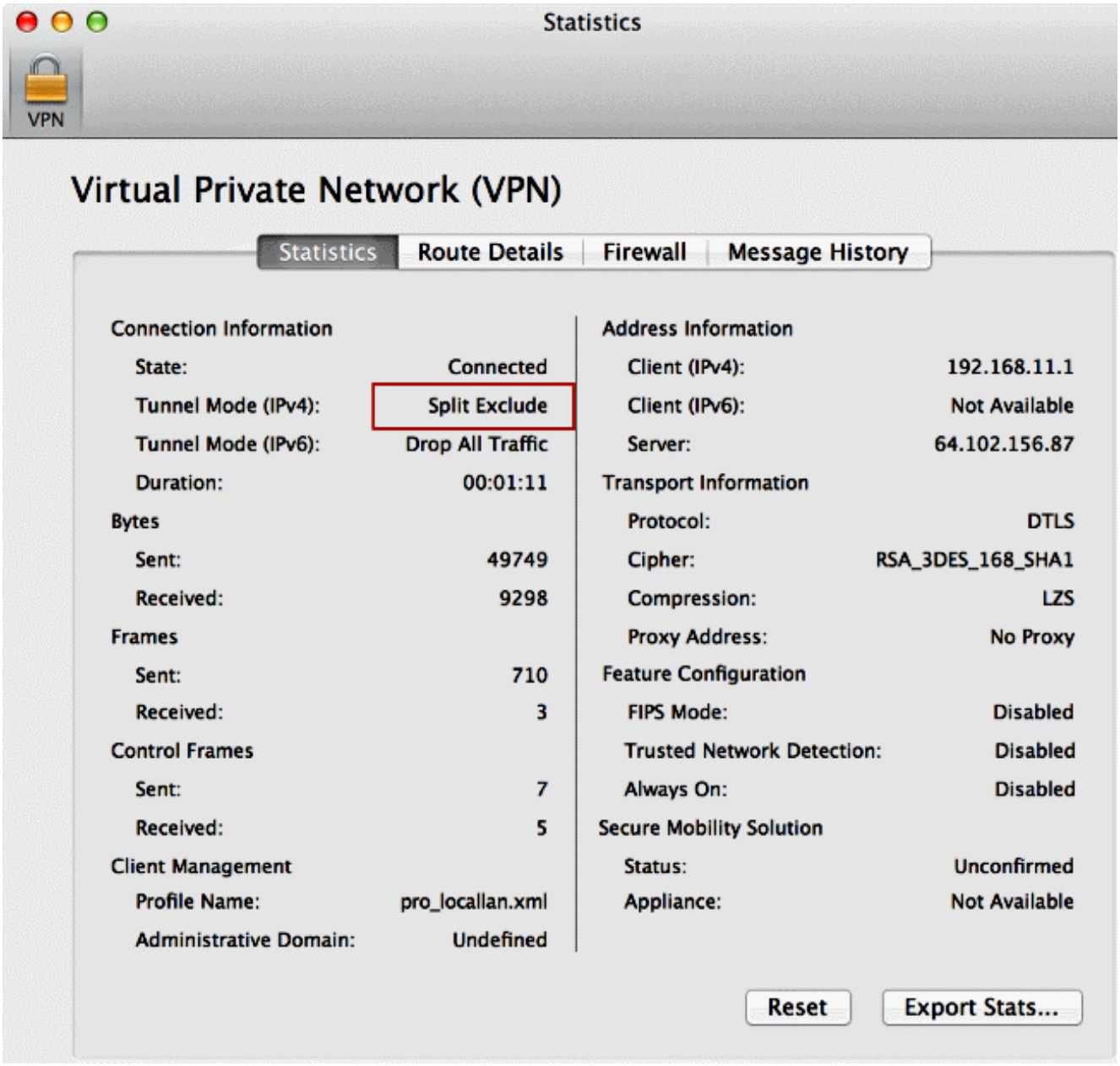
- Bekijk de DART
- Lokale LAN-toegang testen met Ping

Sluit uw Cisco AnyConnect Secure Mobility Client aan op de ASA om uw configuratie te controleren.

1. Kies uw verbindingsingang van de serverlijst en klik op **Connect**.

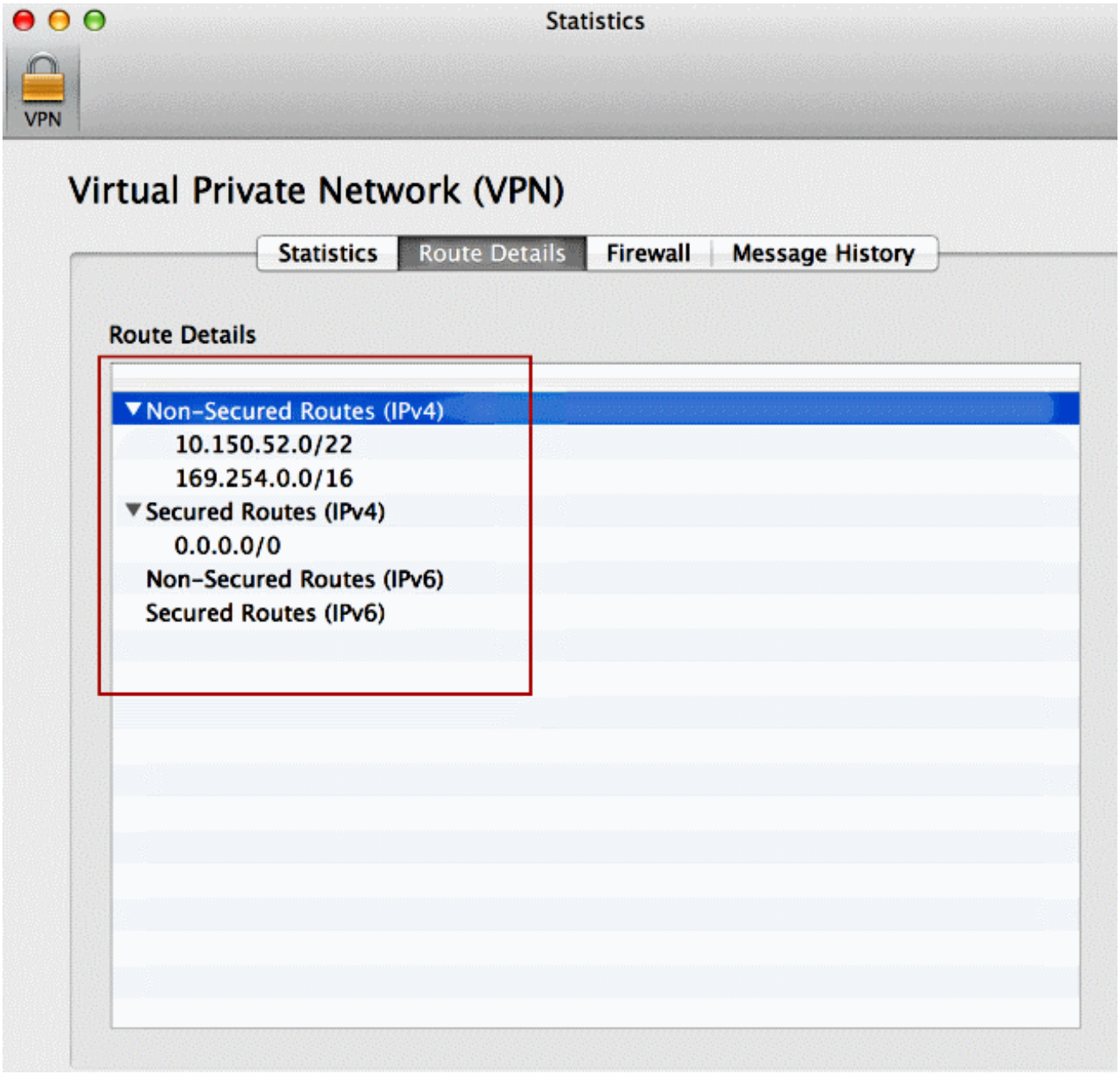


2. Kies **Geavanceerd venster voor alle componenten > Statistieken...** om de tunnelmodus weer te geven.



3. Klik op het tabblad **Routegegevens** om de routes te zien waarop de Cisco AnyConnect Secure Mobility Client nog steeds lokale toegang heeft.

   In dit voorbeeld, wordt de client lokale LAN toegang tot 10.150.52.0/22 en 169.254.0.0/16 verleend terwijl al het andere verkeer versleuteld en over de tunnel verzonden wordt.



Cisco AnyConnect beveiligde mobiliteit-client

Wanneer u de AnyConnect-logbestanden van de bundel Diagnostics en Reporting Tool (DART) onderzoekt, kunt u bepalen of de parameter die plaatselijke LAN-toegang mogelijk maakt, al dan niet is ingesteld.

```
********************************************

Date : 11/25/2011
Time : 13:01:48
Type : Information
Source : acvpndownloader

Description : Current Preference Settings:
ServiceDisable: false
CertificateStoreOverride: false
CertificateStore: All
ShowPreConnectMessage: false
AutoConnectOnStart: false
MinimizeOnConnect: true
```

```
LocalLanAccess: true
AutoReconnect: true
AutoReconnectBehavior: DisconnectOnSuspend
UseStartBeforeLogon: false
AutoUpdate: true
RSASecurIDIntegration: Automatic
WindowsLogonEnforcement: SingleLocalLogon
WindowsVPNEstablishment: LocalUsersOnly
ProxySettings: Native
AllowLocalProxyConnections: true
PPPExclusion: Disable
PPPExclusionServerIP:
AutomaticVPNPolicy: false
TrustedNetworkPolicy: Disconnect
UntrustedNetworkPolicy: Connect
TrustedDNSDomains:
TrustedDNSServers:
AlwaysOn: false
ConnectFailurePolicy: Closed
AllowCaptivePortalRemediation: false
CaptivePortalRemediationTimeout: 5
ApplyLastVPNLocalResourceRules: false
AllowVPNDisconnect: true
EnableScripting: false
TerminateScriptOnNextEvent: false
EnablePostSBLOnConnectScript: true
AutomaticCertSelection: true
RetainVpnOnLogoff: false
UserEnforcement: SameUserOnly
EnableAutomaticServerSelection: false
AutoServerSelectionImprovement: 20
AutoServerSelectionSuspendTime: 4
AuthenticationTimeout: 12
SafeWordSofTokenIntegration: false
AllowIPsecOverSSL: false
ClearSmartcardPin: true
```

```
****************************************
```

Lokale LAN-toegang testen met Ping

Een extra manier om te testen dat de VPN-client nog steeds lokale LAN-toegang heeft terwijl deze naar het VPN-hoofdeinde is getunneld, is om de ping-opdracht in de Microsoft Windows-opdrachtregel te gebruiken. Hier is een voorbeeld waar het lokale LAN van de client 192.168.0.0/24 is en er een andere host op het netwerk aanwezig is 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&colon;

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

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

Kan niet op naam afdrukken of bladeren

Wanneer de VPN-client is aangesloten en geconfigureerd voor plaatselijke LAN-toegang, *kunt* u *niet bij naam* op het lokale LAN *afdrukken of bladeren*. Er zijn twee opties om deze situatie te verbeteren:

- Bladeren of afdrukken op IP-adres.

  Om te bladeren, in plaats van de syntaxis **\\sharname**, gebruikt u de syntax **\\x.x.x.x** waarbij *x.x.x* het IP-adres van de host computer is.

  Wijzig de eigenschappen van de netwerkprinter om een IP-adres in plaats van een naam te gebruiken. Bijvoorbeeld, in plaats van de syntaxis **\\sharename\printername**, gebruik **\\x.x\printernaam**, waar *x.x.x* een IP adres is.
- Maak of wijzig het VPN-clientadapterbestand. Met een LMHOSTS-bestand op een Microsoft Windows-pc kunt u statische afbeeldingen maken tussen hostnamen en IP-adressen. Zo zou een LMHOSTS-bestand bijvoorbeeld als volgt kunnen uitzien:

  ```
  192.168.0.3 SERVER1
  192.168.0.4 SERVER2
  192.168.0.5 SERVER3
  ```

  In Microsoft Windows XP Professional Edition bevindt het LMHOSTS-bestand zich in **%SystemRoot%\System32\Drivers\Etc**. Raadpleeg uw Microsoft documentatie of Microsoft kennisbank artikel 314108 voor meer informatie.

Gerelateerde informatie

- PIX/ASA 750x als externe VPN-server met ASDM-configuratievoorbeeld
- SSL VPN-client (SVC) op IOS met Configuratievoorbeeld
- Cisco ASA 5500 Series adaptieve security applicaties
- Technische ondersteuning en documentatie – Cisco Systems