# AnyConnect SSL via IPv4+IPv6 naar ASA-configuratie

## Inhoud



## Inleiding

Dit document biedt een voorbeeldconfiguratie voor de Cisco adaptieve security applicatie (ASA) om Cisco AnyConnect Secure Mobility Client (hierna "AnyConnect" genoemd in de rest van dit document) toe te staan om een SSL VPN-tunnel op te zetten via een IPv4- of IPv6-netwerk.

Bovendien stelt deze configuratie de client in staat IPv4- en IPv6-verkeer via de tunnel door te geven.

## Voorwaarden

### Vereisten

Om met succes een SSLVPN-tunnel over IPv6 op te zetten, moet u aan deze vereisten voldoen:

- End-to-end IPv6-connectiviteit is vereist
- De AnyConnect-versie moet 3.1 of hoger zijn
- De ASA-softwareversie moet minimaal 9.0 zijn

Als echter niet aan een van deze vereisten wordt voldaan, zal de configuratie die in dit document wordt besproken, de client nog steeds in staat stellen om verbinding te maken via IPv4.

### Gebruikte componenten

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

- ASA-5505 met softwareversie 9.0(1)
- AnyConnect Secure Mobility Client 3.1.0495 op Microsoft Windows XP Professional (zonder IPv6-ondersteuning)

- AnyConnect Secure Mobility Client 3.1.0495 op Microsoft Windows 7 Enterprise 32-bits

## Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

# Configuratie

Om te beginnen, definieer een pool van IP adressen waarvan u één aan elke client zal toewijzen die verbonden is.

Als u wilt dat de client ook IPv6-verkeer over de tunnel vervoert, hebt u een pool van IPv6-adressen nodig. Beide pools worden later genoemd in het groepsbeleid.

```
ip local pool pool4 172.16.2.100-172.16.2.199 mask 255.255.255.0
ipv6 local pool pool6 fcfe:2222::64/64 128
```

Voor IPv6-connectiviteit met de ASA, hebt u een IPv6-adres nodig op de interface waaraan de klanten zullen verbinden (meestal de externe interface).

Voor IPv6 connectiviteit via de tunnel naar binnen hosts, hebt u ook IPv6 nodig in de interface(s).

```
interface Vlan90
 nameif outside
 security-level 0
 ip address 203.0.113.2 255.255.255.0
 ipv6 address 2001:db8:90::2/64
!
interface Vlan102
 nameif inside
 security-level 100
 ip address 192.168.102.2 255.255.255.0
 ipv6 address fcfe:102::2/64
```

Voor IPv6 hebt u ook een standaardroute nodig die naar de volgende-hop router naar het internet wijst.

```
ipv6 route outside ::/0 2001:db8:90::5
route outside 0.0.0.0 0.0.0.0 203.0.113.5 1
```

Om zich te kunnen authentificeren aan de klanten moet de ASA over een identiteitsbewijs beschikken. Instructies voor het maken of importeren van een dergelijk certificaat vallen buiten het toepassingsgebied van dit document, maar kunnen gemakkelijk worden gevonden in andere documenten zoals

/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98596-asa-8-x-3rdpartyvendorcert.html

De resulterende configuratie zou op het volgende moeten lijken:

```
crypto ca trustpoint testCA
 keypair testCA
 crl configure
```

```
...
crypto ca certificate chain testCA
 certificate ca 00
  30820312 308201fa a0030201 02020100 300d0609 2a864886 f70d0101 05050030
  ...
  quit
 certificate 04
  3082032c 30820214 a0030201 02020104 300d0609 2a864886 f70d0101 05050030
  ...
  quit
```

Vervolgens instrueert u de ASA dit certificaat voor SSL te gebruiken:

```
ssl trust-point testCA
```

Daarna is de basisconfiguratie van VPN (SSLVPN) waar de functie op de externe interface is ingeschakeld. Clientpakketten die kunnen worden gedownload, worden gedefinieerd en we definiëren een profiel (meer op dit later):

```
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
 anyconnect profiles asa9-ssl-ipv4v6 disk0:/asa9-ssl-ipv4v6.xml
 anyconnect enable
```

In dit basisvoorbeeld worden de IPv4- en IPv6-adrespools geconfigureerd, DNS-serverinformatie (die naar de client wordt geduwd) en een profiel in het standaard groepsbeleid (DfltGrpPolicy). Veel meer eigenschappen kunnen hier worden ingesteld en optioneel kunt u verschillende groepen-beleid definiëren voor verschillende groepen gebruikers.

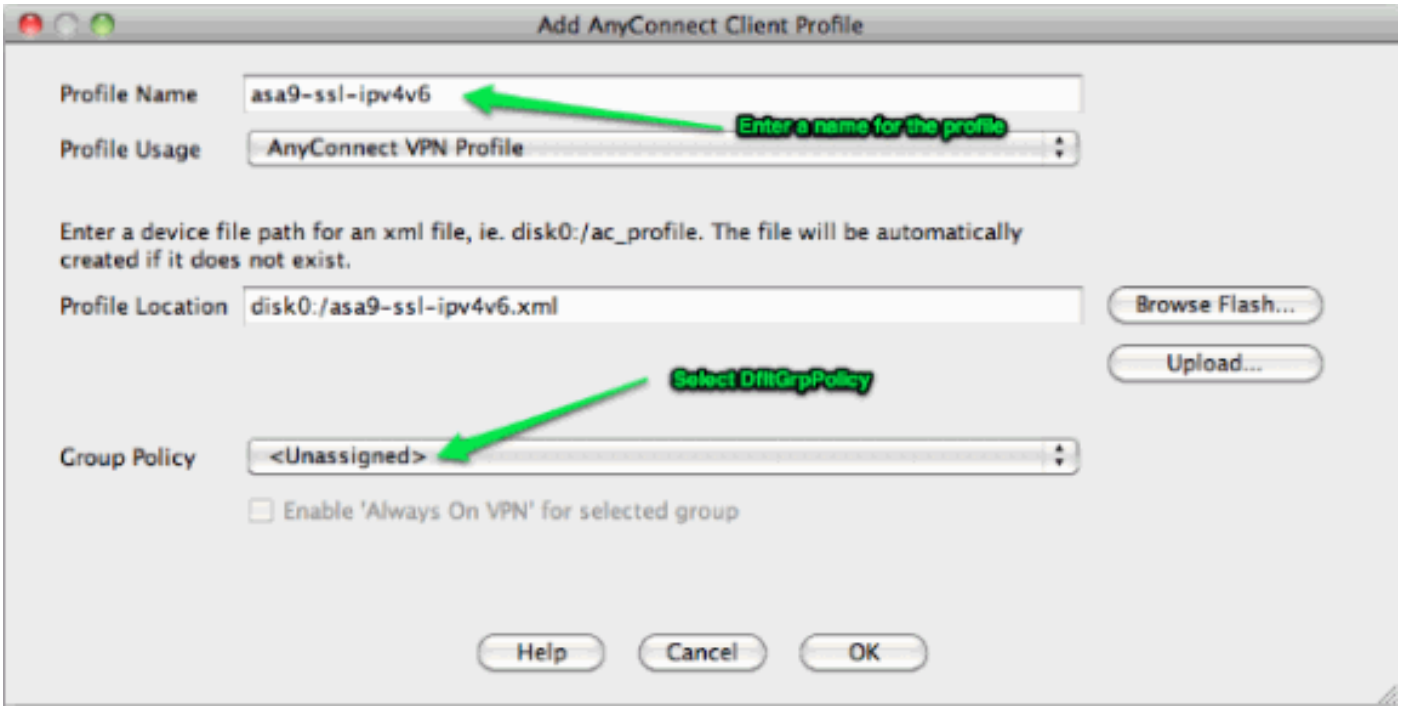
**Opmerking:** Het attribuut "gateway-fqdn" is nieuw in versie 9.0 en definieert de FQDN van de ASA zoals het in de DNS bekend is. De cliënt leert deze FQDN van de ASA en zal het gebruiken wanneer het van een IPv4 aan een IPv6 netwerk of omgekeerd roamt.

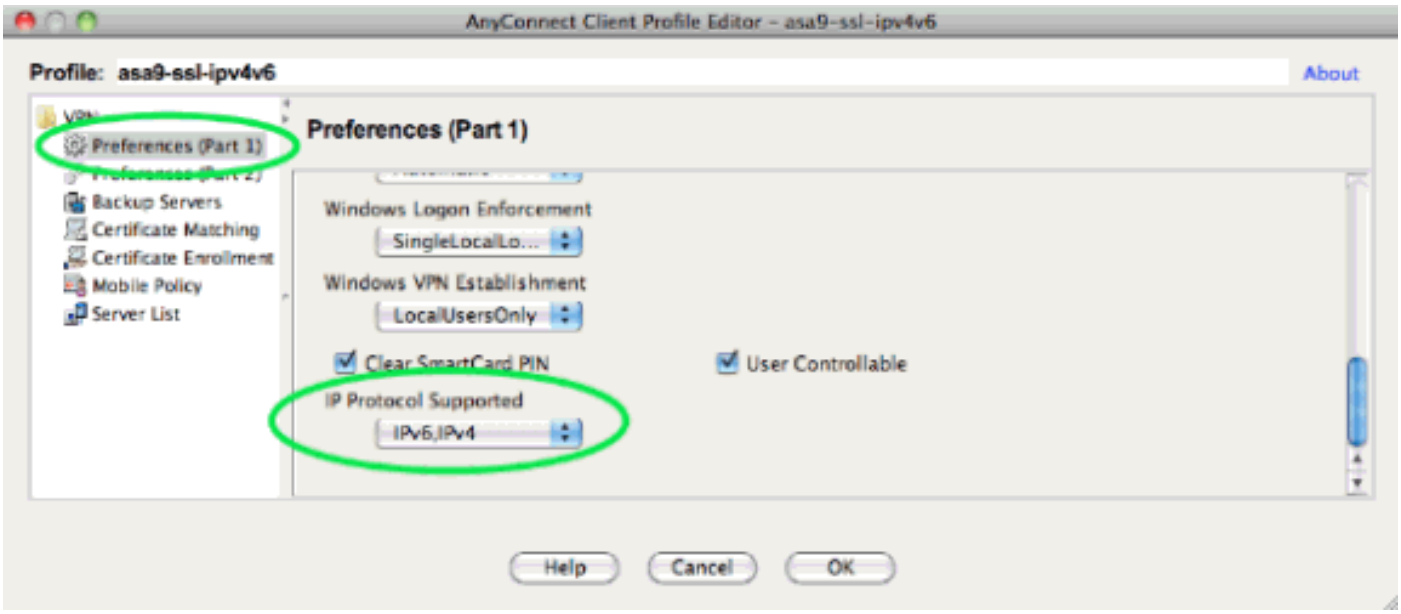
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

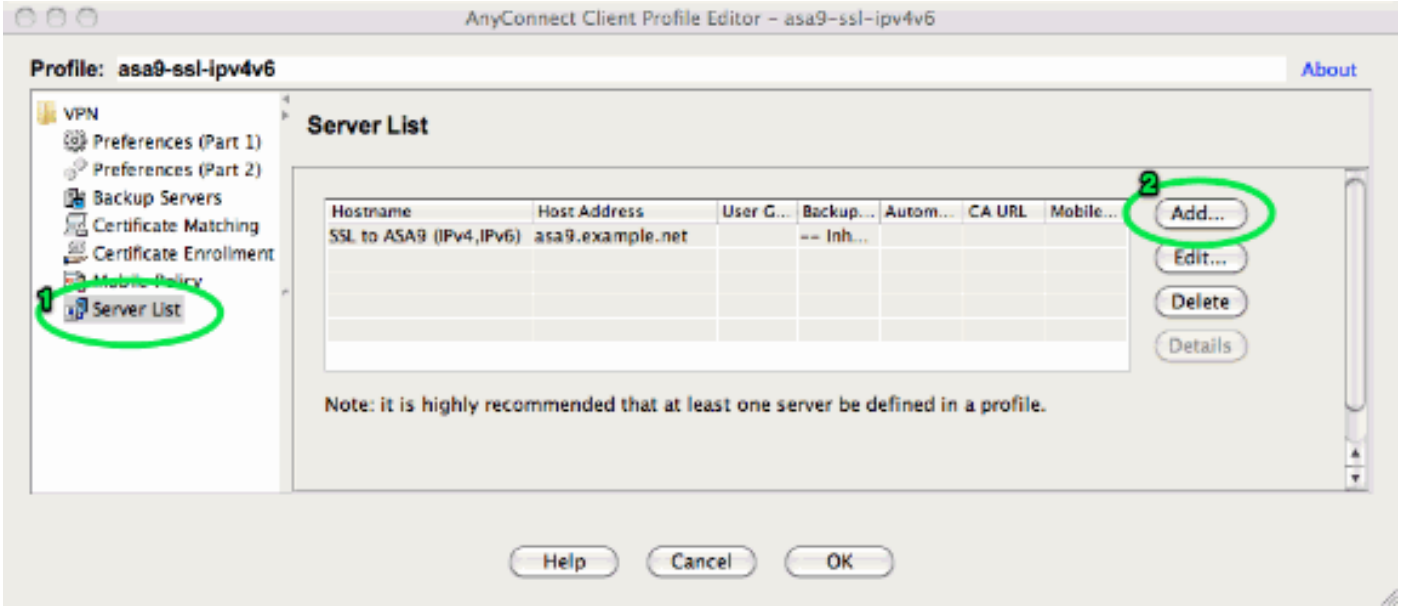
Stel vervolgens een of meer tunnelgroepen in. Standaard wordt één (DefaultWEBVPLroup) gebruikt voor dit voorbeeld en stel de optie in om de gebruiker te verplichten om met behulp van een certificaat te authenticeren:

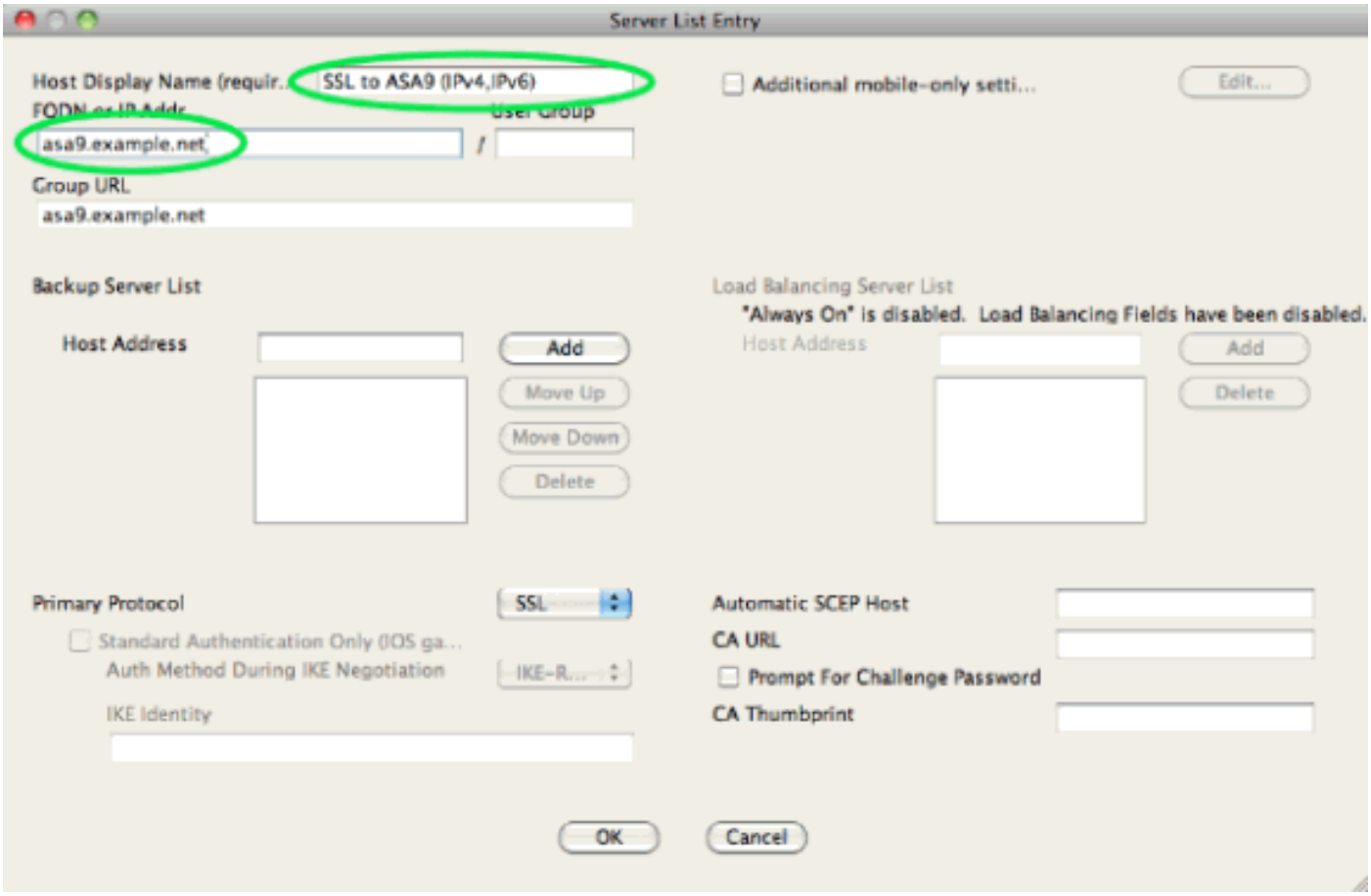
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

Standaard probeert de AnyConnect-client verbinding te maken via IPv4 en alleen als dit mislukt, probeert de client verbinding te maken via IPv6. Dit gedrag kan echter worden gewijzigd door een instelling in het XML-profiel. Het AnyConnect-profiel "asa9-sl-ipv4v6.xml" dat in de bovenstaande configuratie is aangegeven, is gegenereerd met behulp van de Profile Editor in ASDM (Configuration - Remote Access VPN - Network (Client) Access - AnyConnect Profile).


Add AnyConnect Client Profile
Profile Name
asa9-ssl-ipv4v6
Enter a name for the profile
Profile Usage
AnyConnect VPN Profile
Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.
Profile Location
disk0:/asa9-ssl-ipv4v6.xml
Browse Flash...
Upload...
Select DfltGrpPolicy
Group Policy
<Unassigned>
Enable 'Always On VPN' for selected group
Help
Cancel
OK


AnyConnect Client Profile Editor - asa9-ssl-ipv4v6
Profile: asa9-ssl-ipv4v6
About
Preferences (Part 1)
Backup Servers
Certificate Matching
Certificate Enrollment
Mobile Policy
Server List
Preferences (Part 1)
Windows Logon Enforcement
SingleLocalLo...
Windows VPN Establishment
LocalUsersOnly
Clear SmartCard PIN
User Controllable
IP Protocol Supported
IPv6,IPv4
Help
Cancel
OK


AnyConnect Client Profile Editor - asa9-ssl-ipv4v6
Profile: asa9-ssl-ipv4v6
About
VPN
Preferences (Part 1)
Preferences (Part 2)
Backup Servers
Certificate Matching
Certificate Enrollment
Server List
1
Server List
Hostname
Host Address
User G...
Backup...
Autom...
CA URL
Mobile...
SSL to ASA9 (IPv4,IPv6)
asa9.example.net
-- Inh...
2
Add...
Edit...
Delete
Details
Note: it is highly recommended that at least one server be defined in a profile.
Help
Cancel
OK




Het resulterende XML profiel (met het meeste standaard onderdeel weggelaten voor beknoptheid):

```
<?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>
 ...
 ...
</ClientInitialization>
 <ServerList>
 <HostEntry>
       </HostEntry> </ServerList>
</AnyConnectProfile>
```

In het bovenstaande profiel wordt ook een HostName gedefinieerd (wat om het even wat kan zijn, hoeft deze niet overeen te komen met de werkelijke hostname van de ASA) en een HostAddress (wat doorgaans de FQDN van de ASA is).

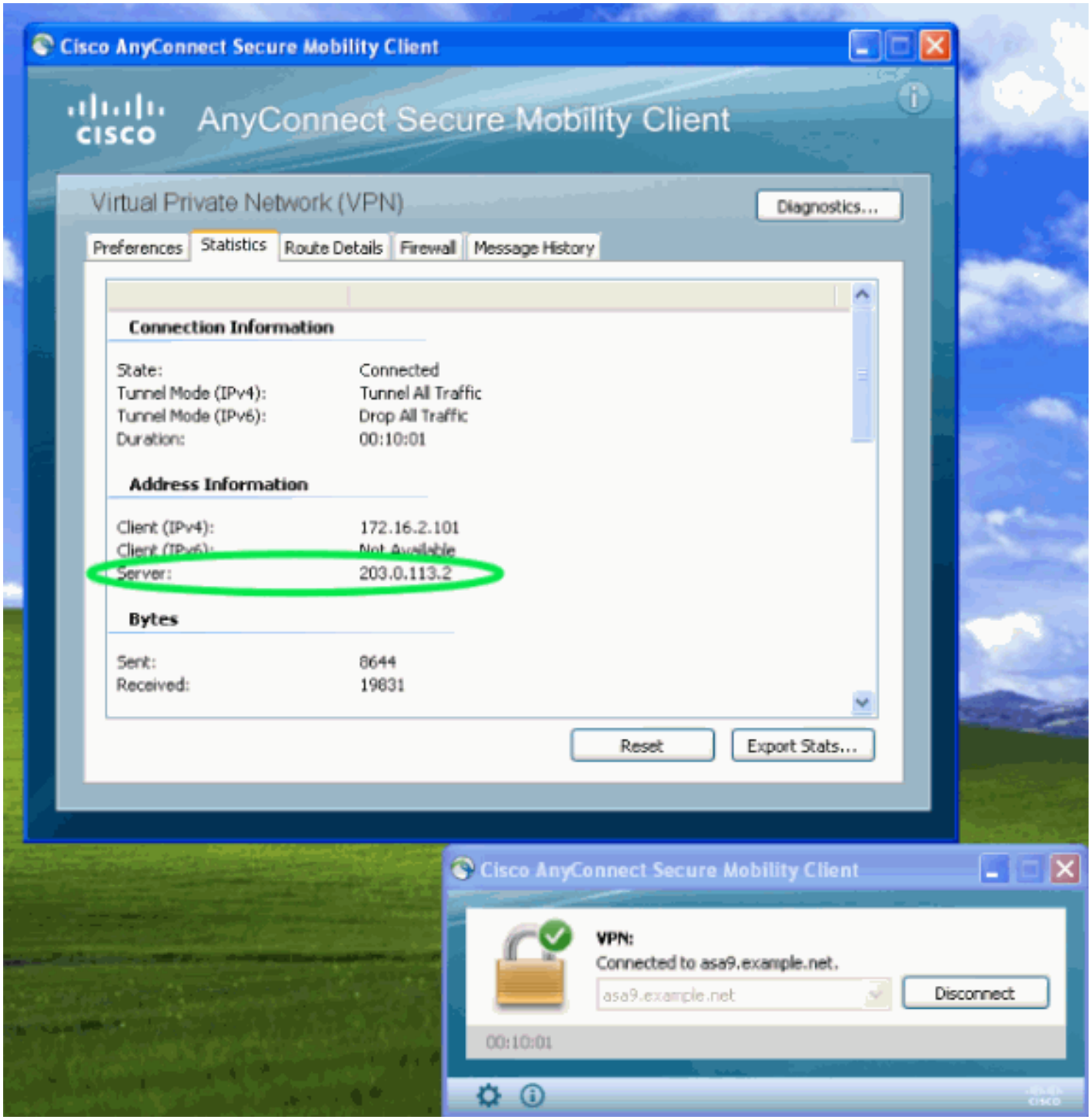
**Opmerking:** Het veld HostAddress kan leeggelaten worden, maar het veld HostName moet de FQDN van de ASA bevatten.

**Opmerking:** Tenzij het profiel vooraf is uitgevoerd, vereist de eerste verbinding dat de gebruiker in de FQDN van de ASA typt. Deze eerste verbinding heeft de voorkeur aan IPv4. Na een succesvolle verbinding wordt het profiel gedownload. Vanaf dat moment worden de profielinstellingen toegepast.

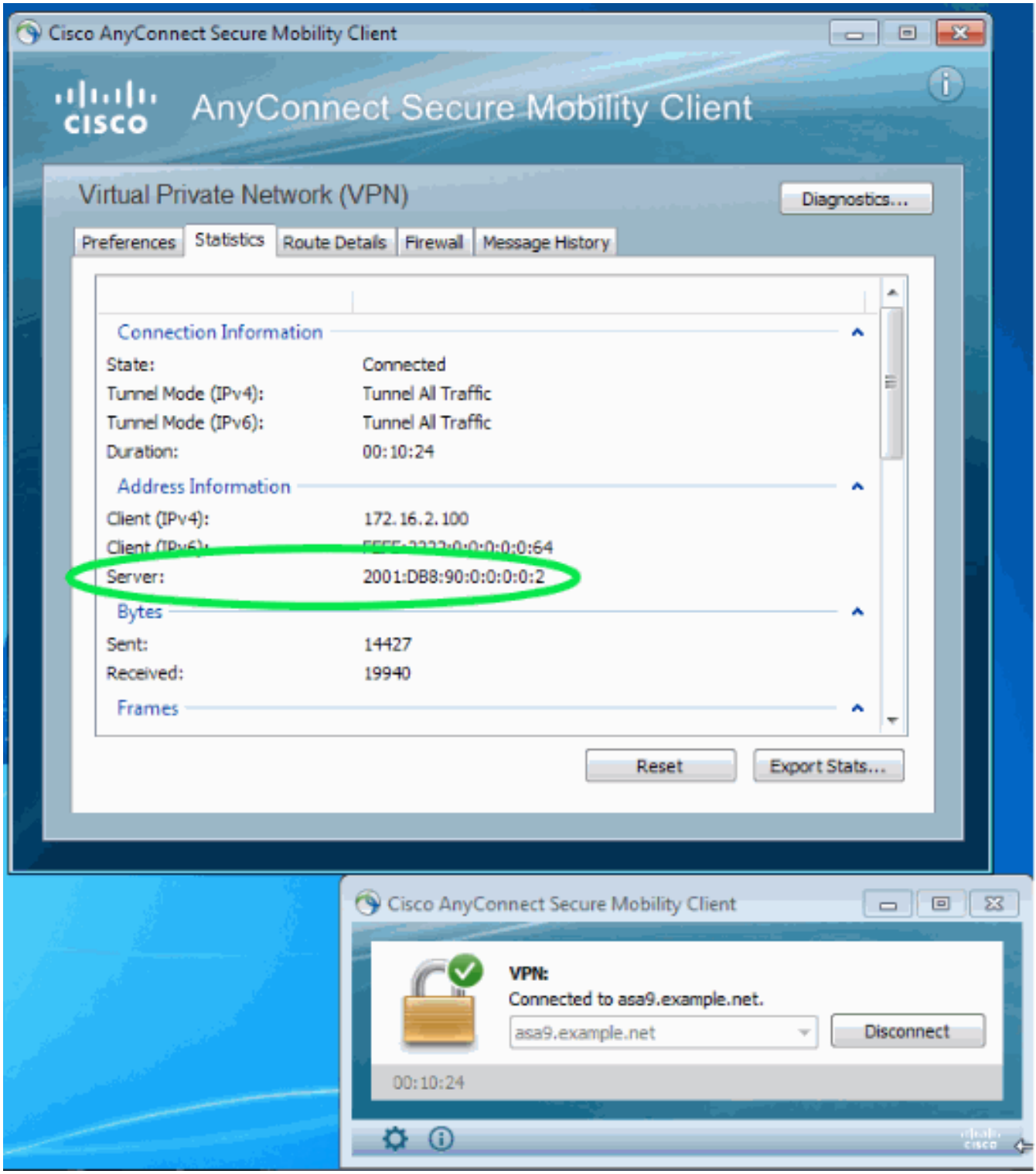
## Verifiëren

Om te controleren of een client via IPv4 of IPv6 is verbonden, controleert u of de client-GUI of de VPN-sessie-DB op de ASA:

- Open in het venster Geavanceerd het tabblad Statistieken en controleer het IP-adres van de "Server".Deze eerste gebruiker maakt een verbinding vanuit een Windows XP-systeem zonder IPv6-
  ondersteuning:




Deze tweede gebruiker sluit zich aan bij een Windows 7-host met IPv6-connectiviteit op de ASA:




- Op de ASA, van de CLI controleer de "Openbare IP" in de "show vpn-sessiondb anyconnect" uitvoer. In dit voorbeeld kunt u dezelfde twee verbindingen zien als hierboven: één vanuit XP over IPv4 en één vanuit Windows 7 via IPv6:

```
asa9# show vpn-sessiondb anyconnect
Session Type: AnyConnect
Username : Nanashi no Gombei Index : 45
Assigned IP : 172.16.2.101 Public IP : 192.0.2.95
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 13138 Bytes Rx : 22656
Group Policy : DfltGrpPolicy Tunnel Group : DefaultWEBVPNGroup
Login Time : 11:14:29 UTC Fri Oct 12 2012
Duration : 1h:45m:14s
```

```
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
Username : Uno Who Index : 48
Assigned IP : 172.16.2.100 Public IP : 2001:db8:91::7
Assigned IPv6: fcfe:2222::64
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11068 Bytes Rx : 10355
Group Policy : DfltGrpPolicy Tunnel Group : DefaultWEBVPNGroup
Login Time : 12:55:45 UTC Fri Oct 12 2012
Duration : 0h:03m:58s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

# Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems