Konfiguration von AnyConnect SSL over IPv4+IPv6 auf ASA

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die Cisco Adaptive Security Appliance (ASA), mit der der Cisco AnyConnect Secure Mobility Client (im weiteren Verlauf dieses Dokuments als "AnyConnect" bezeichnet) einen SSL-VPN-Tunnel über ein IPv4- oder IPv6-Netzwerk einrichten kann.

Darüber hinaus ermöglicht diese Konfiguration dem Client die Weiterleitung von IPv4- und IPv6-Datenverkehr über den Tunnel.

Voraussetzungen

Anforderungen

Um einen SSL VPN-Tunnel über IPv6 erfolgreich einzurichten, müssen folgende Voraussetzungen erfüllt sein:

- End-to-End-IPv6-Anbindung erforderlich
- Die AnyConnect-Version muss 3.1 oder höher sein.
- Die ASA-Softwareversion muss Version 9.0 oder höher sein.

Wenn eine dieser Anforderungen jedoch nicht erfüllt wird, ermöglicht die in diesem Dokument beschriebene Konfiguration dem Client weiterhin die Verbindung über IPv4.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA-5505 mit Softwareversion 9.0(1)
- AnyConnect Secure Mobility Client 3.1.00495 unter Microsoft Windows XP Professional (ohne IPv6-Unterstützung)
- AnyConnect Secure Mobility Client 3.1.00495 unter Microsoft Windows 7 Enterprise 32-Bit

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfiguration

Definieren Sie zunächst einen Pool von IP-Adressen, aus dem Sie jedem Client, der eine Verbindung herstellt, eine zuweisen.

Wenn der Client auch IPv6-Datenverkehr über den Tunnel übertragen soll, benötigen Sie einen Pool mit IPv6-Adressen. Auf beide Pools wird später in der Gruppenrichtlinie verwiesen.

```
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
```

Für die IPv6-Anbindung an die ASA benötigen Sie eine IPv6-Adresse auf der Schnittstelle, mit der die Clients verbunden werden (in der Regel die externe Schnittstelle).

Für IPv6-Verbindungen über den Tunnel zu internen Hosts ist auch IPv6 auf der bzw. den internen Schnittstellen erforderlich.

```
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
```

Für IPv6 benötigen Sie außerdem eine Standardroute, die auf den Next-Hop-Router zum Internet verweist.

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

Um sich bei den Clients zu authentifizieren, muss die ASA über ein Identitätszertifikat verfügen. Anweisungen zum Erstellen oder Importieren eines solchen Zertifikats fallen nicht in den Anwendungsbereich dieses Dokuments, sind aber auch in anderen Dokumenten wie

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

Die resultierende Konfiguration sollte ähnlich wie folgt aussehen:

```
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
```

Weisen Sie dann die ASA an, dieses Zertifikat für SSL zu verwenden:

```
ssl trust-point testCA
```

Als Nächstes folgt die grundlegende Webvpn-Konfiguration (SSLVPN), bei der die Funktion auf der externen Schnittstelle aktiviert ist. Client-Pakete, die zum Download verfügbar sind, werden definiert und ein Profil wird definiert (weitere Informationen zu diesem späteren Zeitpunkt):

```
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 diesem einfachen Beispiel werden die IPv4- und IPv6-Adresspools konfiguriert, DNS-Serverinformationen (die an den Client gesendet werden) und ein Profil in der Standardgruppenrichtlinie (DfltGrpPolicy). Hier können viele weitere Attribute konfiguriert werden. Optional können Sie verschiedene Gruppenrichtlinien für verschiedene Benutzergruppen definieren.

Hinweis: Das Attribut "gateway-fqdn" ist neu in Version 9.0 und definiert den FQDN der ASA, wie er im DNS bekannt ist. Der Client erhält diesen FQDN von der ASA und nutzt ihn für das Roaming von einem IPv4- zu einem IPv6-Netzwerk oder umgekehrt.

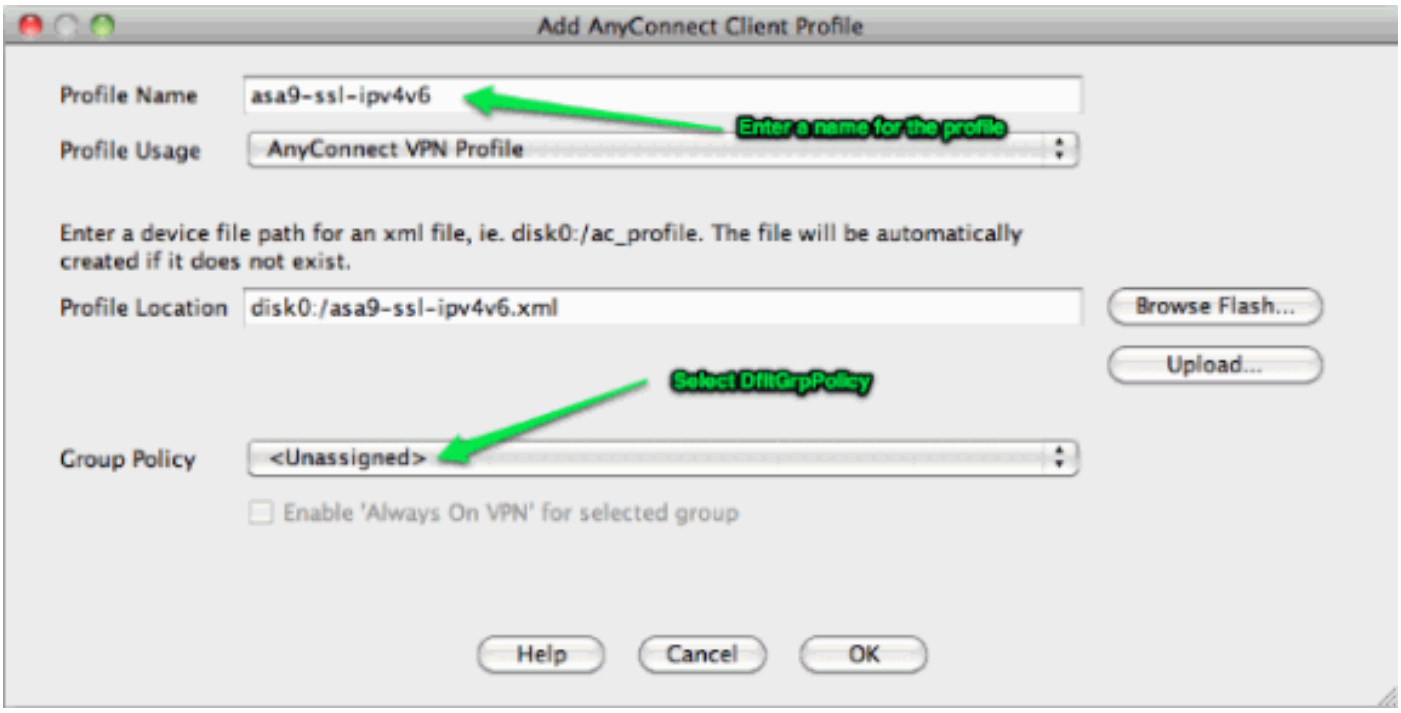
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

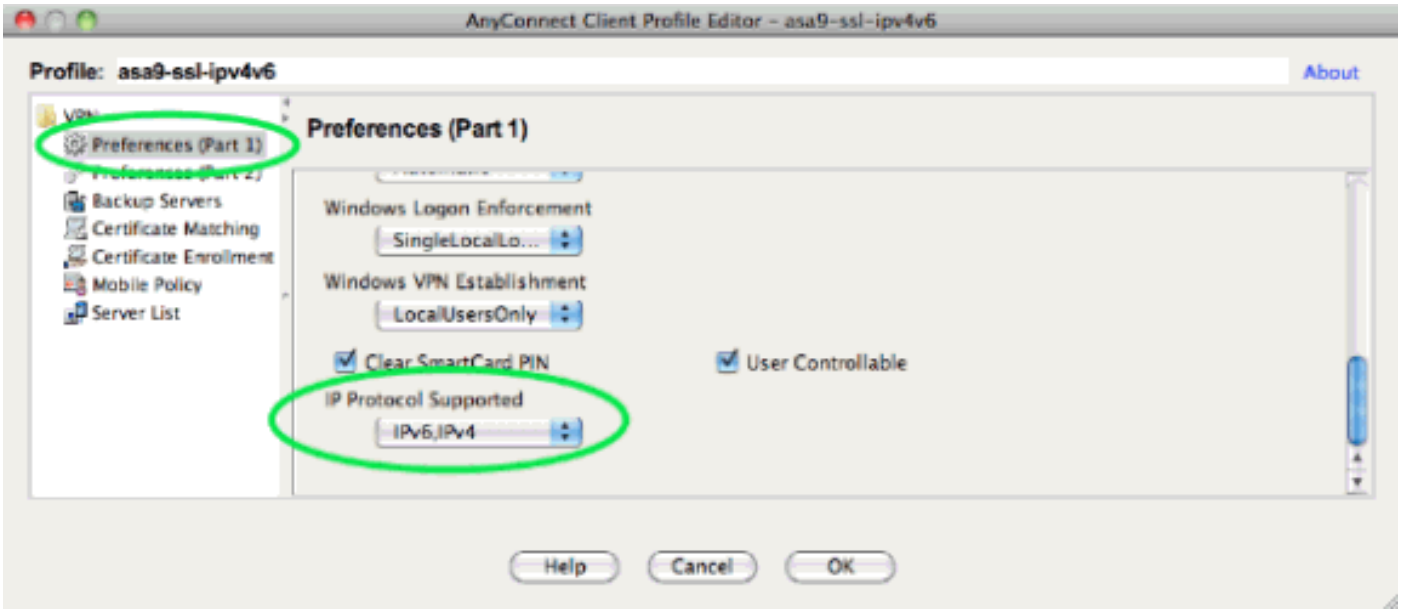
Konfigurieren Sie anschließend eine oder mehrere Tunnelgruppen. In diesem Beispiel wird die Standardgruppe (DefaultWEBVPNGgroup) verwendet, um sie so zu konfigurieren, dass der Benutzer sich anhand eines Zertifikats authentifizieren muss:

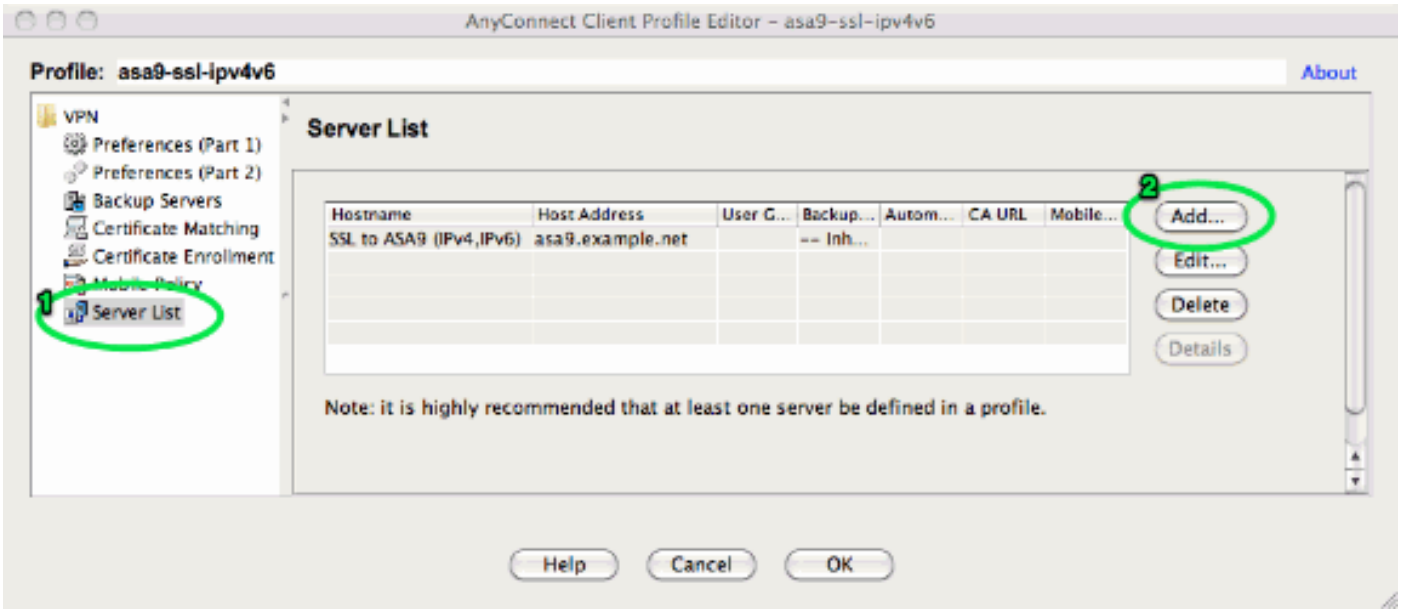
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

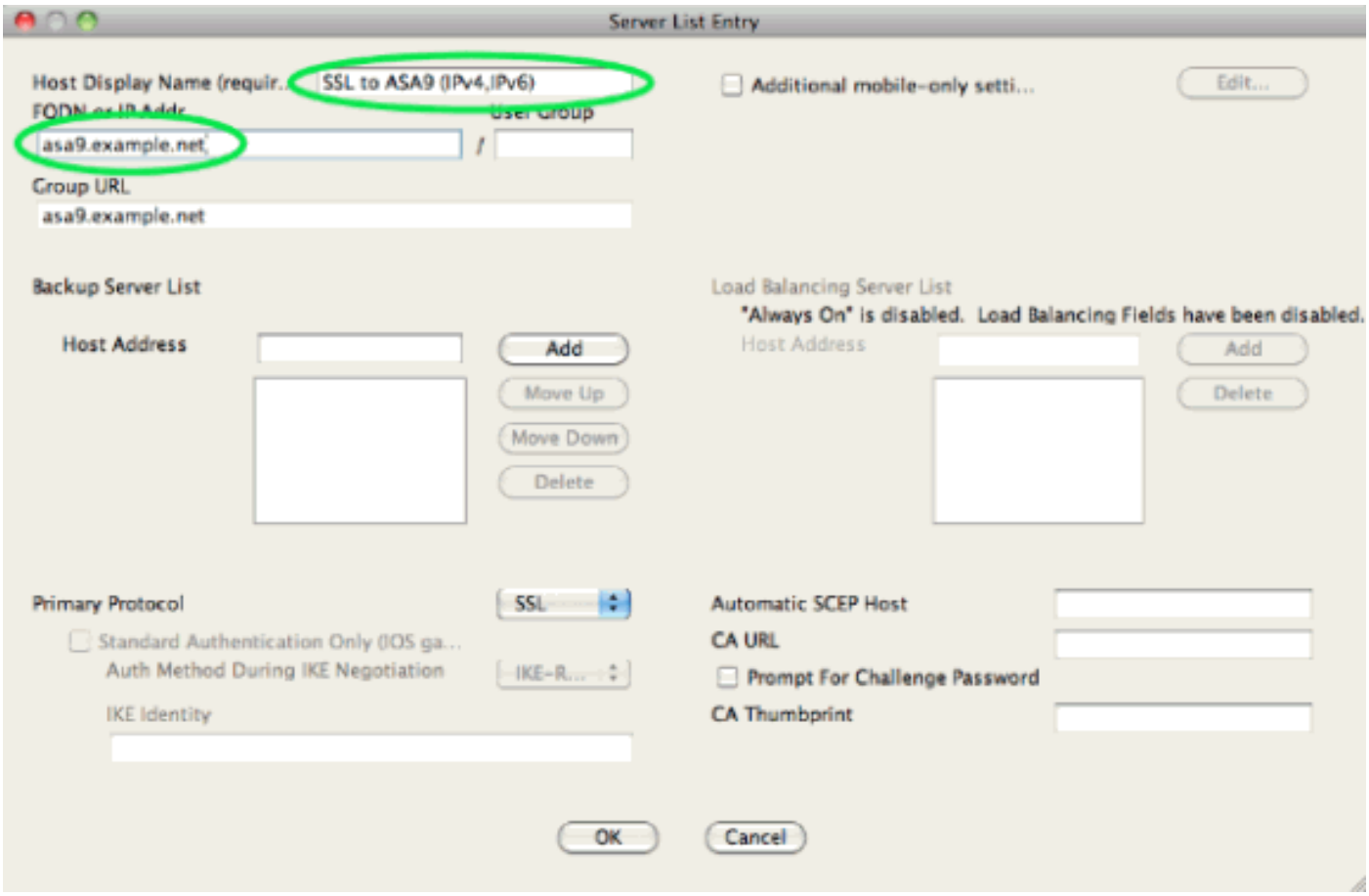
Der AnyConnect-Client versucht standardmäßig, eine Verbindung über IPv4 herzustellen, und versucht nur dann, eine Verbindung über IPv6 herzustellen, wenn dies fehlschlägt. Dieses Verhalten kann jedoch durch eine Einstellung im XML-Profil geändert werden. Das AnyConnect-

Profil "asa9-ssl-ipv4v6.xml", auf das in der obigen Konfiguration verwiesen wird, wurde mit dem Profil-Editor im ASDM (Configuration - Remote Access VPN - Network (Client) Access - AnyConnect Client Profile) erstellt.









Das resultierende XML-Profil (wobei der Großteil des Standardteils aus Gründen der Kürze weggelassen wird):

```
<?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>
```

Im obigen Profil wird auch ein HostName definiert (der beliebig sein kann, aber nicht mit dem tatsächlichen Hostnamen der ASA übereinstimmen muss), und eine HostAddress (normalerweise der FQDN der ASA).

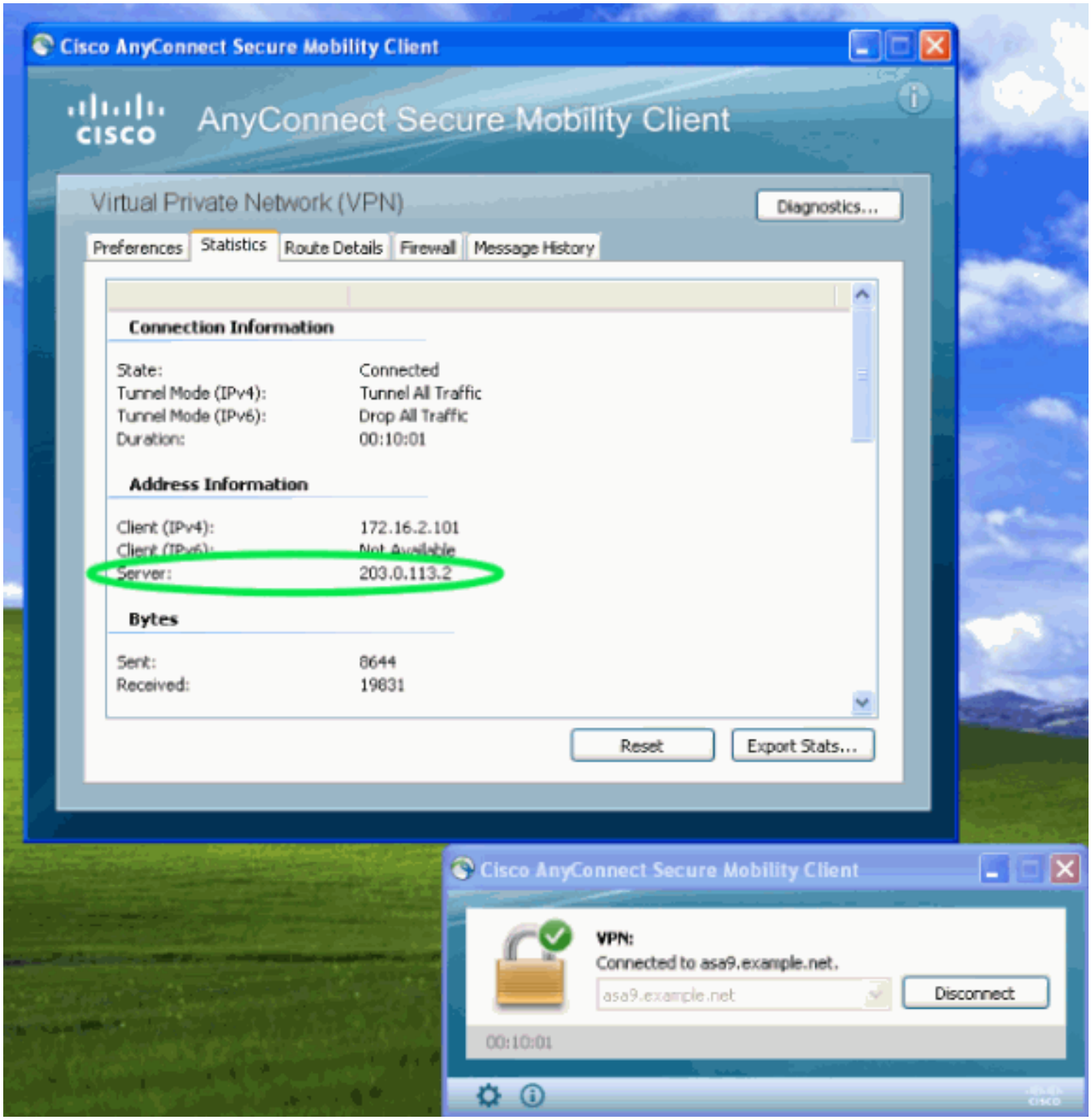
Hinweis: Das Feld HostAddress kann leer gelassen werden, das Feld HostName muss jedoch den FQDN der ASA enthalten.

Hinweis: Wenn das Profil nicht vorinstalliert ist, muss der Benutzer bei der ersten Verbindung den FQDN der ASA eingeben. Diese erste Verbindung bevorzugt IPv4. Nach erfolgreicher Verbindung wird das Profil heruntergeladen. Von dort werden die Profileinstellungen angewendet.

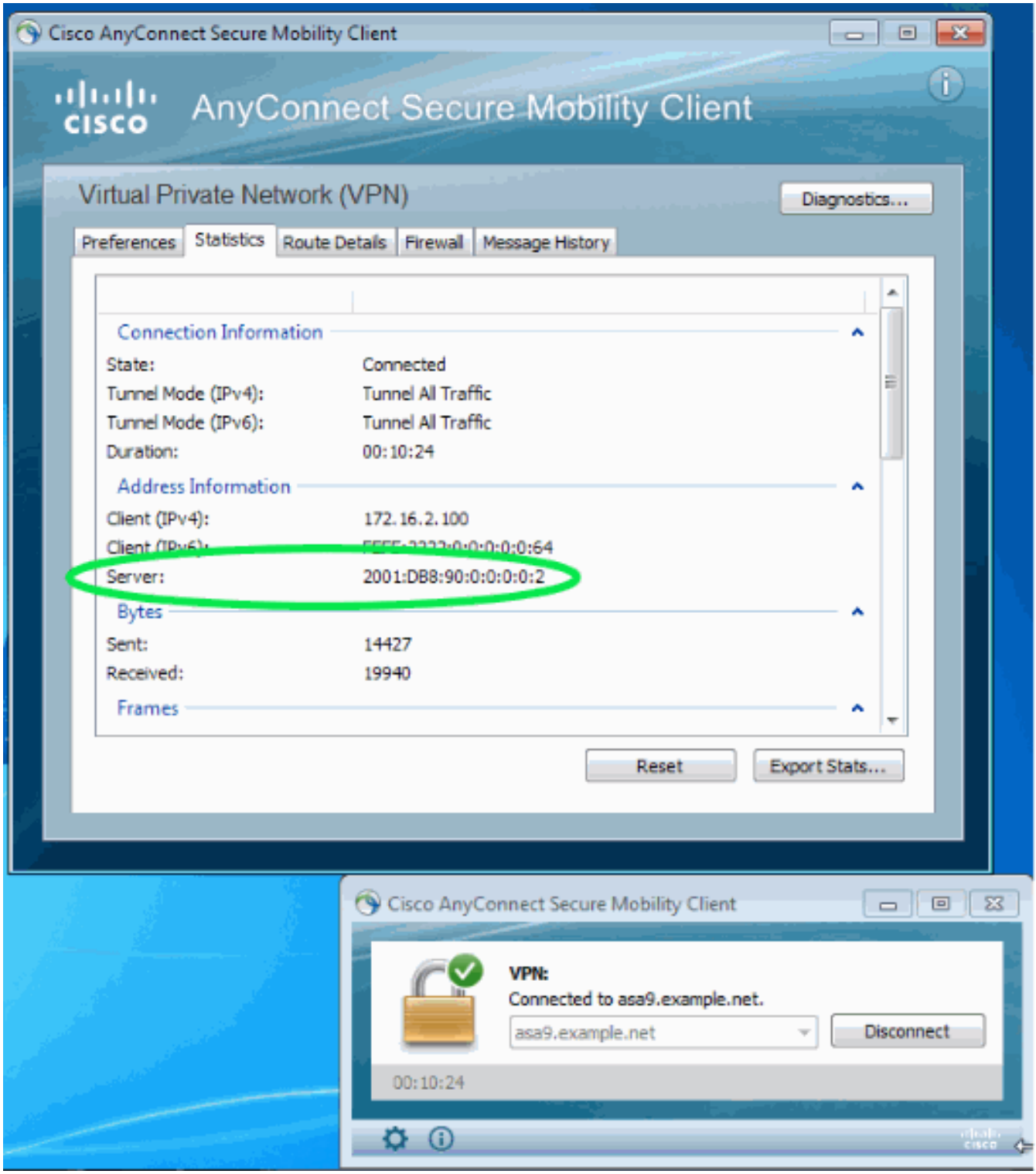
Überprüfen

Um zu überprüfen, ob ein Client über IPv4 oder IPv6 verbunden ist, überprüfen Sie entweder die Client-GUI oder die VPN-Sitzung DB auf der ASA:

- Öffnen Sie auf dem Client das Fenster Erweitert, gehen Sie zur Registerkarte Statistik und überprüfen Sie die IP-Adresse des "Servers".Dieser erste Benutzer stellt eine Verbindung von einem Windows XP-System her, das keine IPv6-Unterstützung unterstützt:



Dieser zweite Benutzer stellt über einen Windows 7-Host mit IPv6-Verbindung eine Verbindung zur ASA
her:



- Aktivieren Sie auf der ASA in der CLI die Option "Public IP" (Öffentliche IP) in der Ausgabe "show vpn-sessiondb anyconnect" (VPN-Sitzung anzeigen). In diesem Beispiel werden die beiden gleichen Verbindungen wie oben angezeigt: eine von XP over IPv4 und eine von Windows 7 über 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
```

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems