通过IPv4+IPv6的AnyConnect SSL到ASA配置

目录

简介

本文档为思科自适应安全设备(ASA)提供配置示例，以允许思科AnyConnect安全移动客户端（在本文档的其余部分中称为“AnyConnect”）通过IPv4或IPv6网络建立SSL VPN隧道。

此外，此配置允许客户端通过隧道传递IPv4和IPv6流量。

先决条件

要求

要成功建立IPv6上的SSLVPN隧道，请满足以下要求：

- 需要端到端IPv6连接
- AnyConnect版本需要为3.1或更高版本
- ASA软件版本需要为9.0或更高版本

但是，如果这些要求中的任何一项未满足，本文档中讨论的配置仍允许客户端通过IPv4连接。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 软件版本为9.0(1)的ASA-5505
- Microsoft Windows XP Professional上的AnyConnect安全移动客户端3.1.00495（不支持IPv6）
- Microsoft Windows 7企业版32位版上的AnyConnect安全移动客户端3.1.00495

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

首先，定义一个IP地址池，您将从该池为连接的每个客户端分配一个地址。

如果您希望客户端也通过隧道传输IPv6流量，则需要IPv6地址池。两个池稍后在组策略中引用。

```
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
```

对于与ASA的IPv6连接，您需要在客户端要连接的接口（通常是外部接口）上提供IPv6地址。

对于通过隧道到内部主机的IPv6连接，您还需要内部接口上的IPv6。

```
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
```

对于IPv6，您还需要指向通往Internet的下一跳路由器的默认路由。

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

为了向客户端验证自身，ASA需要拥有身份证书。有关如何创建或导入此类证书的说明不在本文档的范围之内，但可以在其他文档中轻松找到，如

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

结果配置应类似于以下内容：

```
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
```

然后，指示ASA将此证书用于SSL:

```
ssl trust-point testCA
```

接下来是基本webvpn(SSLVPN)配置，在该配置中，在外部接口上启用该功能。定义可供下载的客户端软件包，并定义配置文件（稍后将详细介绍）：

```
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
```

在此基本示例中，配置了IPv4和IPv6地址池、DNS服务器信息（将推送到客户端）和默认组策略(DfltGrpPolicy)中的配置文件。 此处可以配置更多属性，或者您可以为不同的用户集定义不同的组策略。

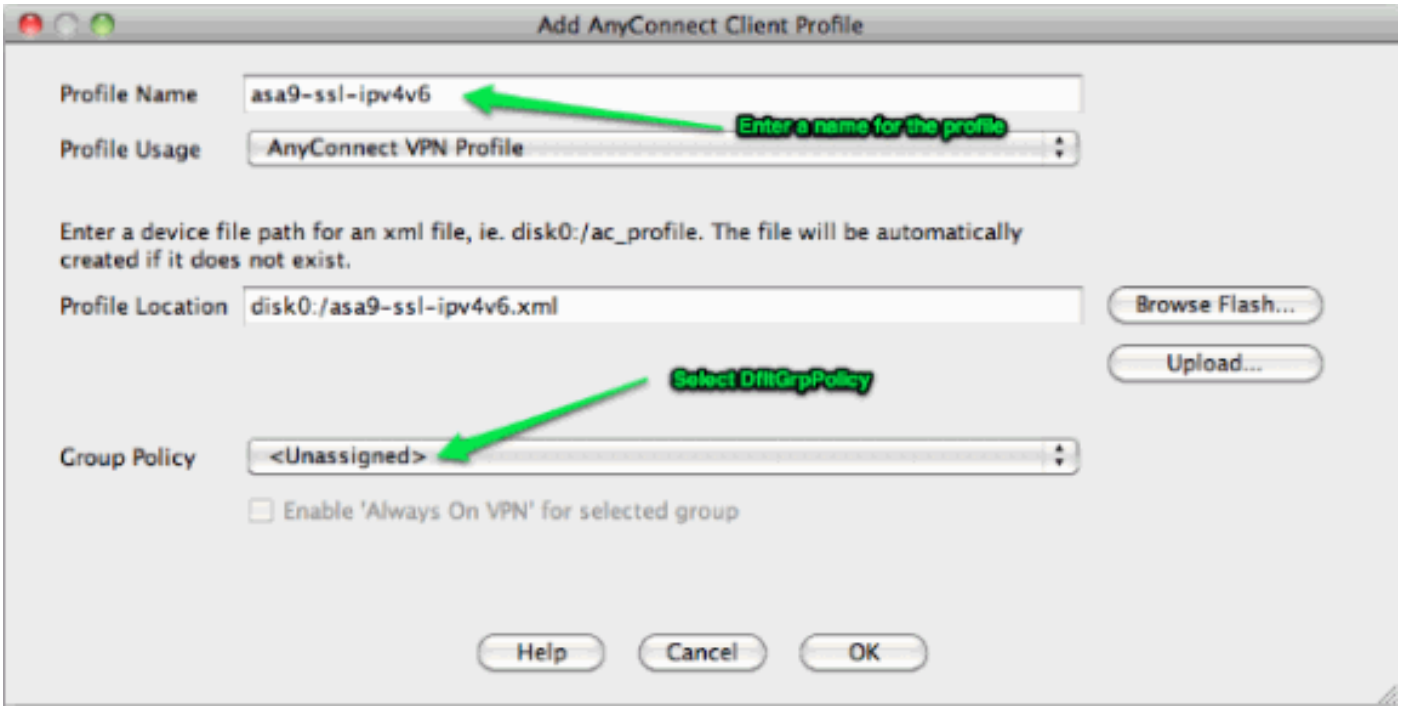
注意：“gateway-fqdn”属性是9.0版中的新属性，定义ASA的FQDN，如DNS中所知。客户端从ASA获取此FQDN，并在从IPv4漫游到IPv6网络时使用，反之亦然。

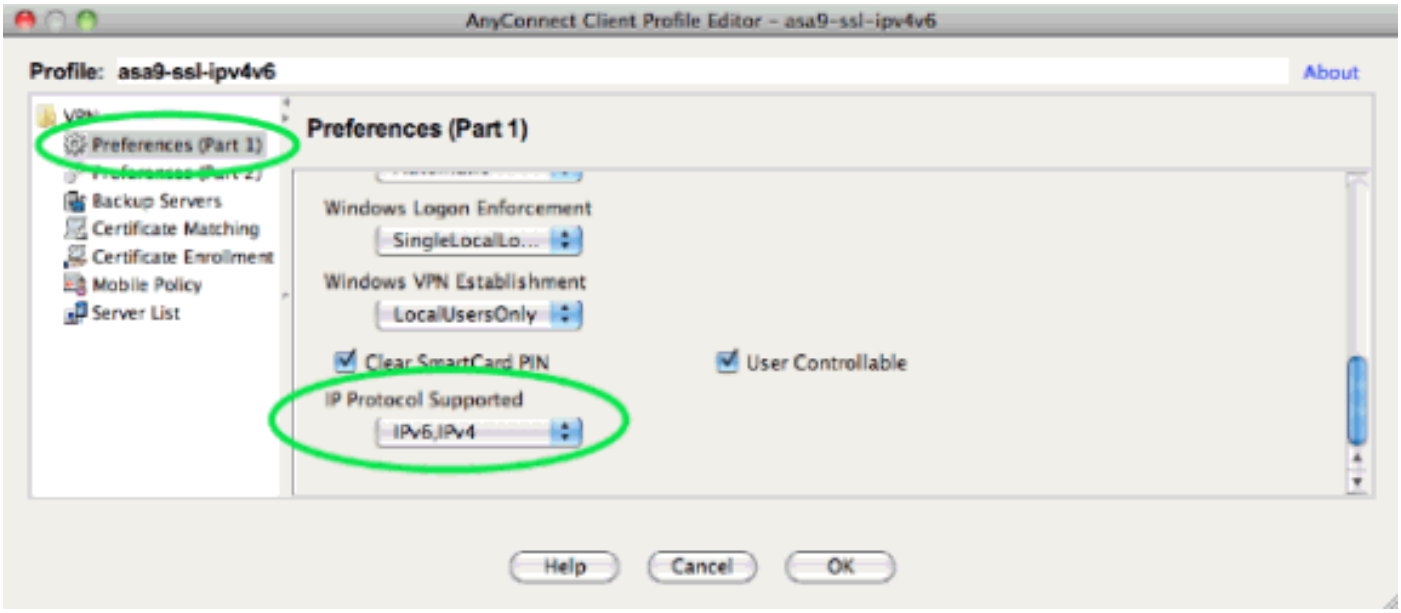
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

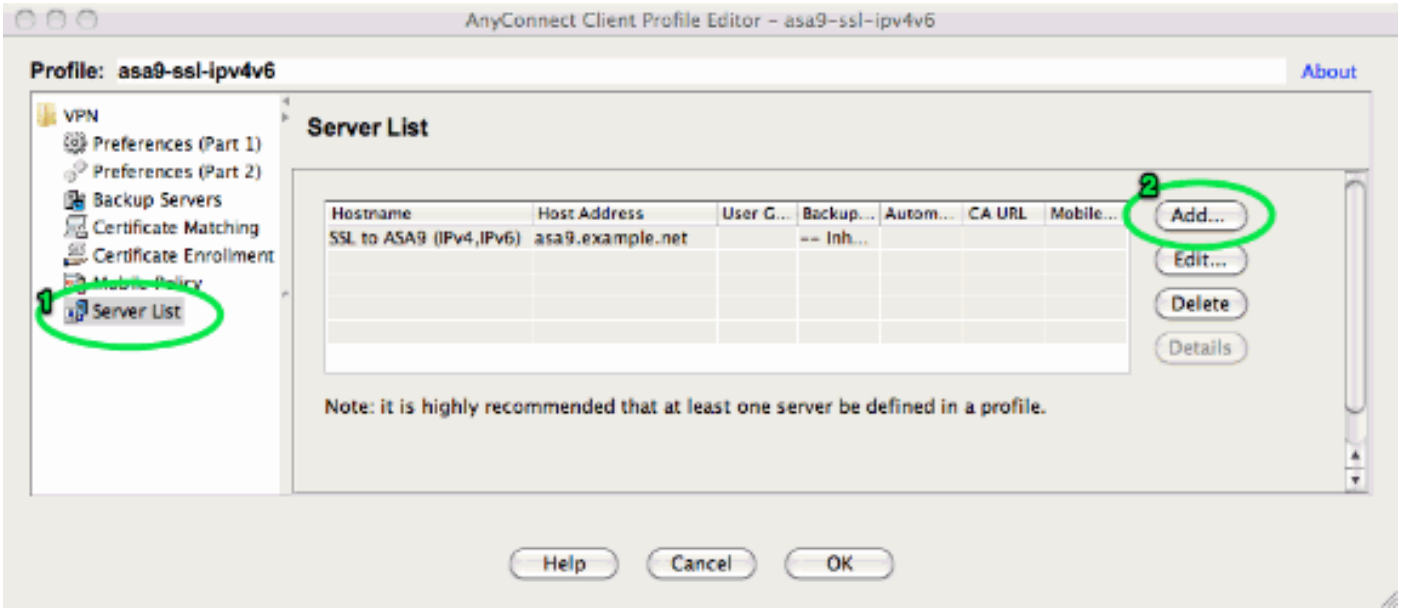
接下来，配置一个或多个隧道组。此示例使用默认组(DefaultWEBVPNGroup)，并将其配置为要求用户使用证书进行身份验证：

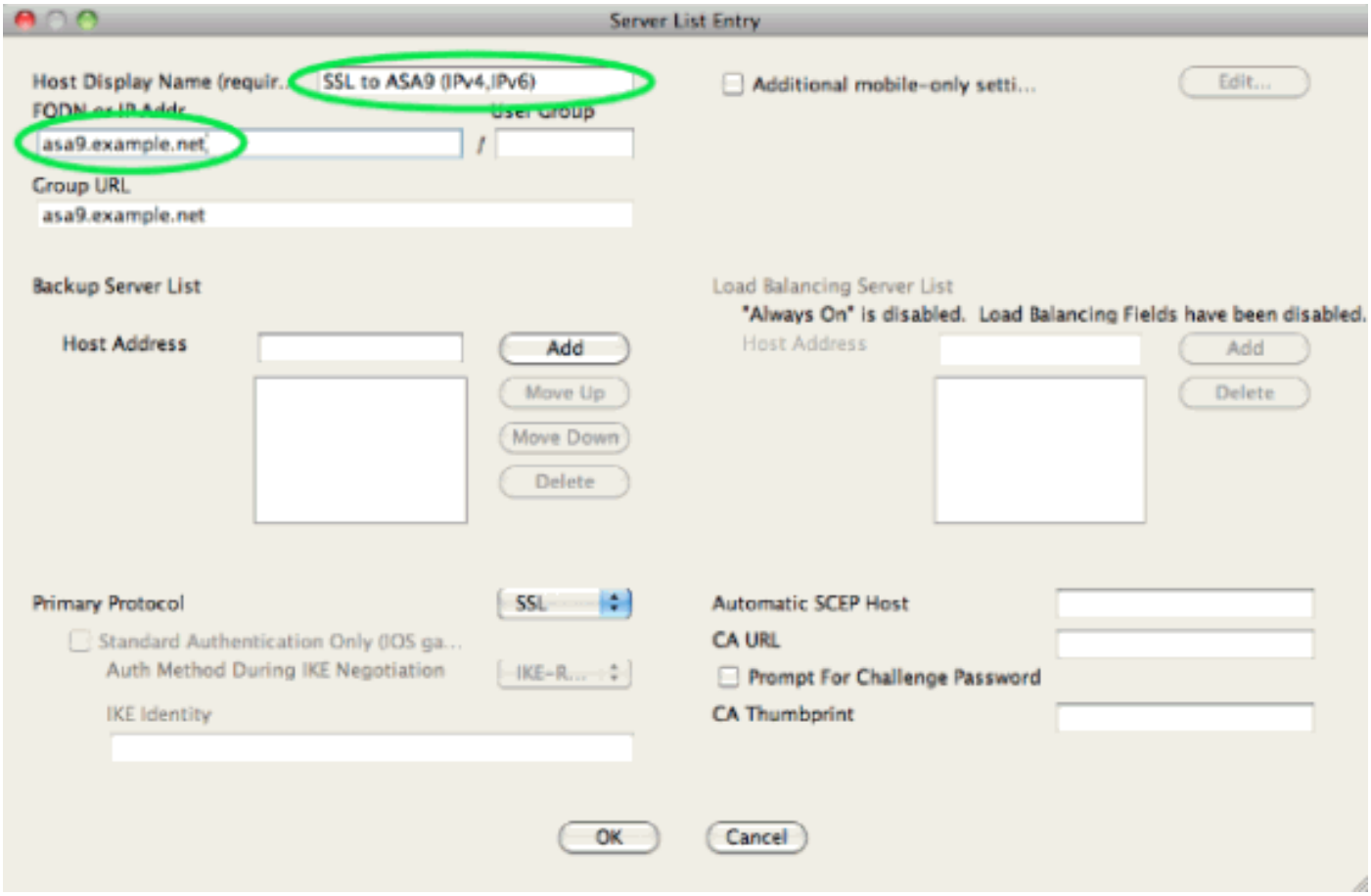
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

默认情况下，AnyConnect客户端尝试通过IPv4连接，并且仅在失败时尝试通过IPv6连接。但是，可以通过XML配置文件中的设置更改此行为。在上述配置中引用的AnyConnect配置文件“asa9-ssl-ipv4v6.xml”是使用ASDM(配置 — 远程访问VPN — 网络（客户端）访问 — AnyConnect客户端配置文件)中的配置文件编辑器生成的。




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



生成的XML配置文件（为简洁起见，省略了大部分默认部分）：

```
<?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>
```

在上述配置文件中，还定义了HostName（可以是任何名称，它不需要与ASA的实际主机名匹配）和HostAddress（通常是ASA的FQDN）。

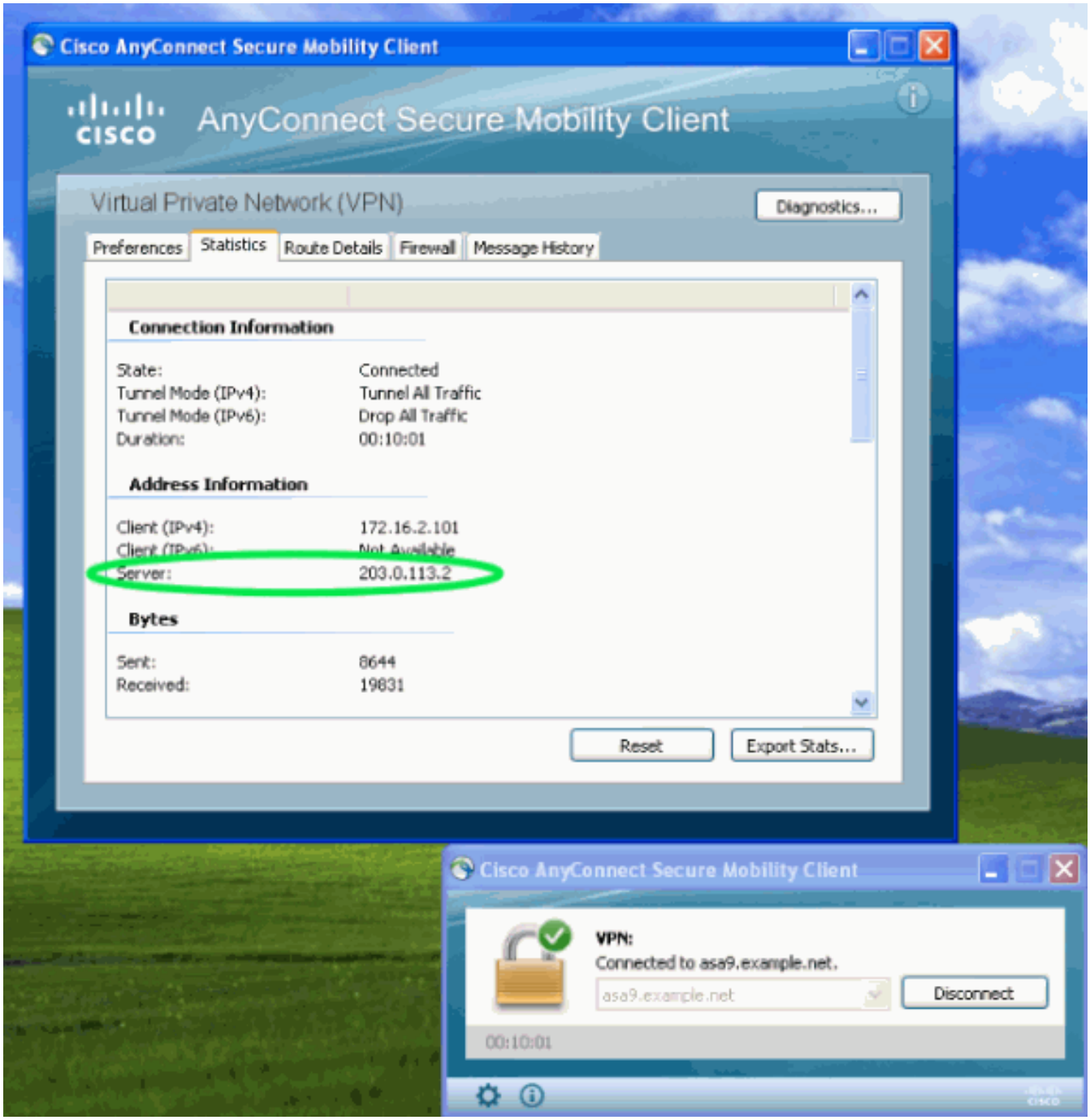
注意： HostAddress字段可以留空，但HostName字段必须包含ASA的FQDN。

注意：除非预部署了配置文件，否则第一个连接要求用户键入ASA的FQDN。此初始连接将首选IPv4。连接成功后，将下载配置文件。从此处，将应用配置文件设置。

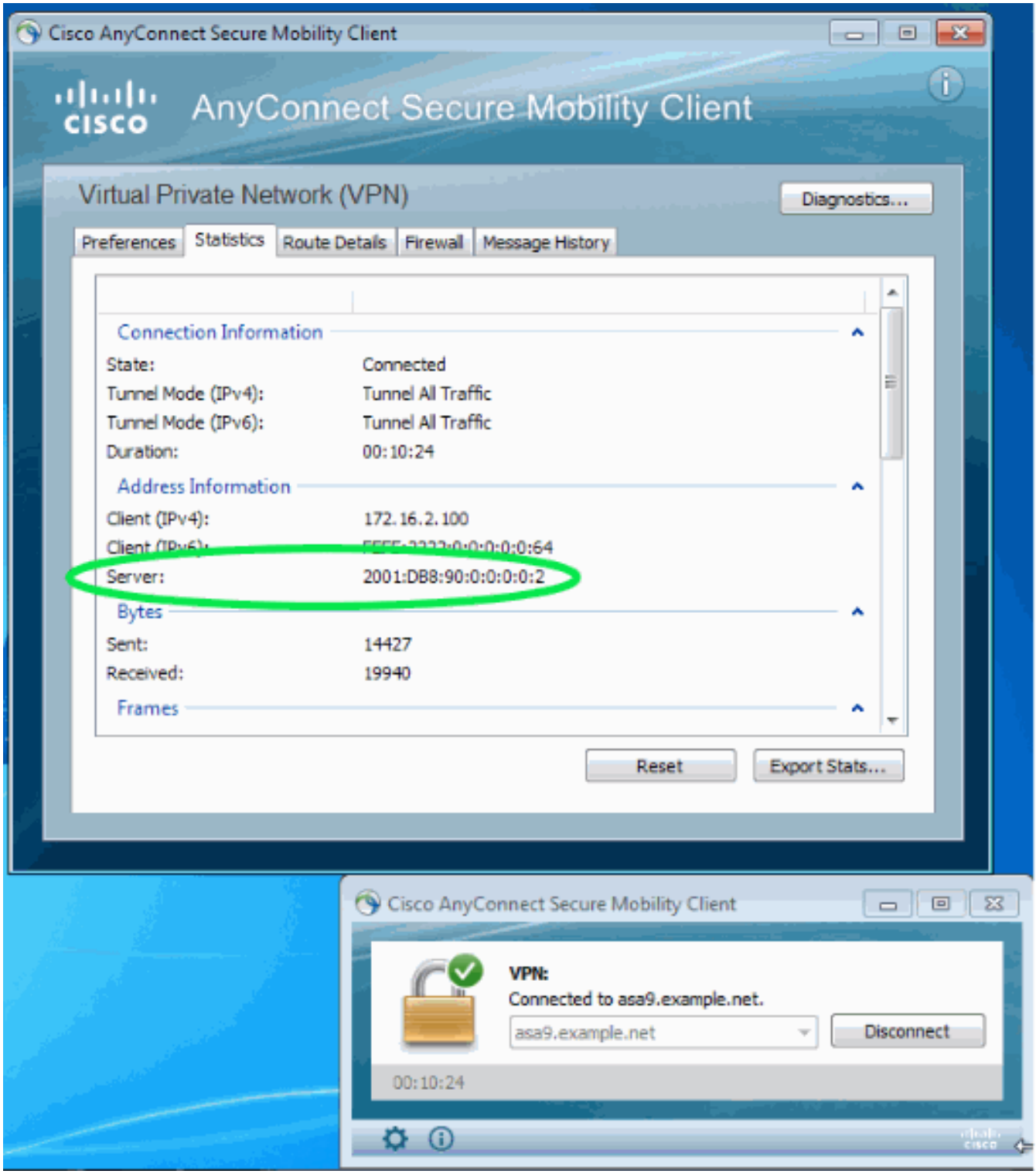
验证

要验证客户端是通过IPv4还是IPv6连接，请检查ASA上的客户端GUI或VPN会话数据库：

- 在客户端上，打开Advanced窗口，转到Statistics选项卡并验证“Server”的IP地址。第一个用户从Windows XP系统连接时不支持
  IPv6:



第二个用户从具有IPv6连接的Windows 7主机连接到
ASA:



- 在ASA上，从CLI中，在“show vpn-sessiondb anyconnect”输出中检查“Public IP”。在本示例中，您可以看到与上面相同的两个连接：一个来自XP over IPv4，另一个来自Windows 7 over 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
```

相关信息

- 技术支持和文档 - Cisco Systems