在IPv4+IPv6的AnyConnect SSL对ASA配置

目录

简介

本文为思科可适应安全工具(ASA)提供一配置示例允许Cisco AnyConnect安全移动客户端(指“AnyConnect”在本文档的剩余部分)设立在IPv4或IPv6网络的一个SSL VPN通道。

另外，此配置允许客户端通过IPv4和IPv6流量在通道。

先决条件

要求

为了成功设立在IPv6的一个SSLVPN通道，请符合这些要求：

- 端到端IPv6连接要求
- AnyConnect版本需要3.1或以后
- ASA软件版本需要9.0或以后

然而，如果这些需求中的任一个没有符合，在本文讨论的配置将允许客户端在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：

- 与软件版本的ASA-5505 9.0(1)
- AnyConnect Microsoft Windows XP专业人员的安全移动性客户端3.1.00495 (没有IPv6支持)
- AnyConnect 32位Microsoft Windows 7的企业的安全移动性客户端3.1.00495

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

首先，请定义您将分配一到每个客户端连接IP地址的池。

如果希望客户端也运载在通道的IPv6流量，您将需要IPv6地址的池。两个池是被参考的以后在组政策。

```
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
```

对于对ASA的IPv6连接，您需要在客户端将连接的接口的一个IPv6地址(典型地外部接口)。

对于在通道的IPv6连接对内部主机，您需要在内部接口的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，您也需要指向往互联网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
```

为了验证对客户端， ASA需要有身份证书。关于如何的说明创建或导入这样证书是超出本文的范围之外，但是可以在其他文档容易地找到例如

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

导致的配置应该看似类似于以下：

```
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，请指示ASA使用此证书SSL ：

```
ssl trust-point testCA
```

其次基本(SSLVPN)的WebVPN配置功能在外部接口启用。可以下载的客户端包定义和我们定义了配置文件定义(更多在此以后) ：

```
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
```

在本例中基本示例， IPv4和IPv6地址池配置，将推送给客户端)的DNS服务器信息(和在默认组政策(DfltGrpPolicy)的一配置文件。许多属性可以配置此处，并且或者您能定义不同的套的不同的组政策用户。

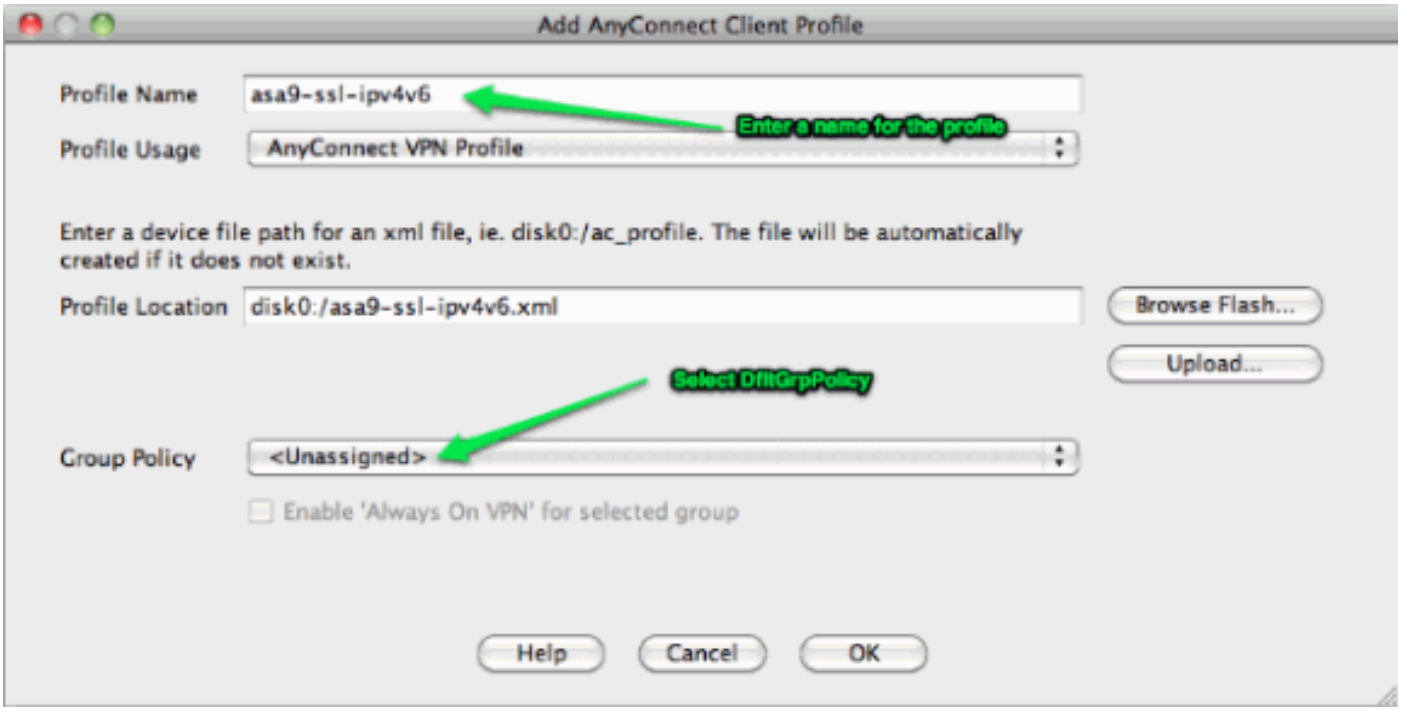
注意： 当在DNS，知道“网关FQDN”属性在版本9.0新建并且定义了ASA的FQDN。当漫游从IPv4到IPv6网络或反之亦然时，客户端学习从ASA的此FQDN，并且使用它。

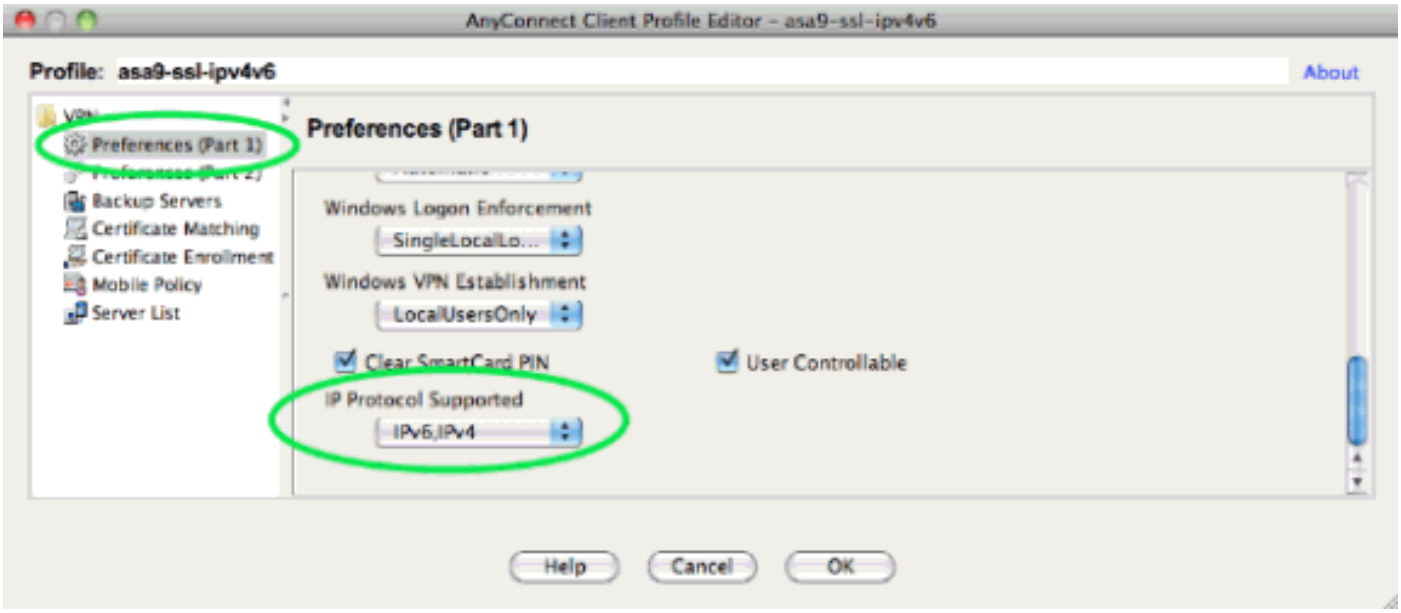
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

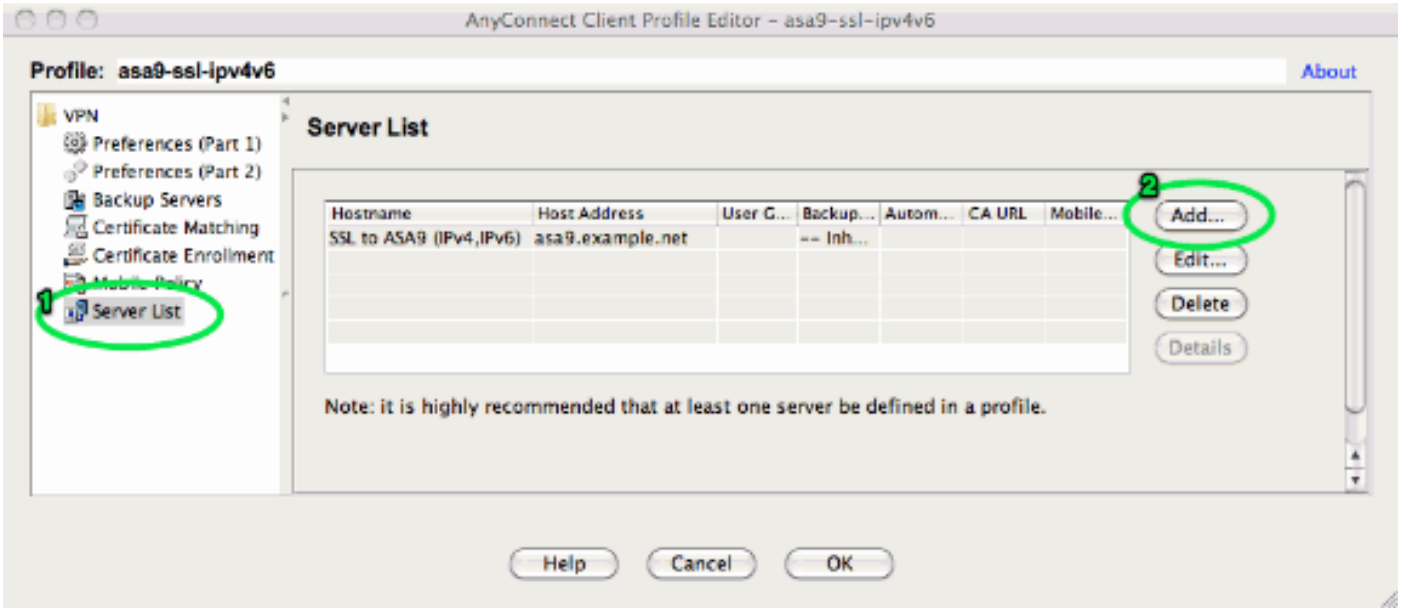
其次，请配置一个或更多隧道群。默认一(DefaultWebVPNGroup)使用证书，使用此示例，并且配置它要求用户验证：

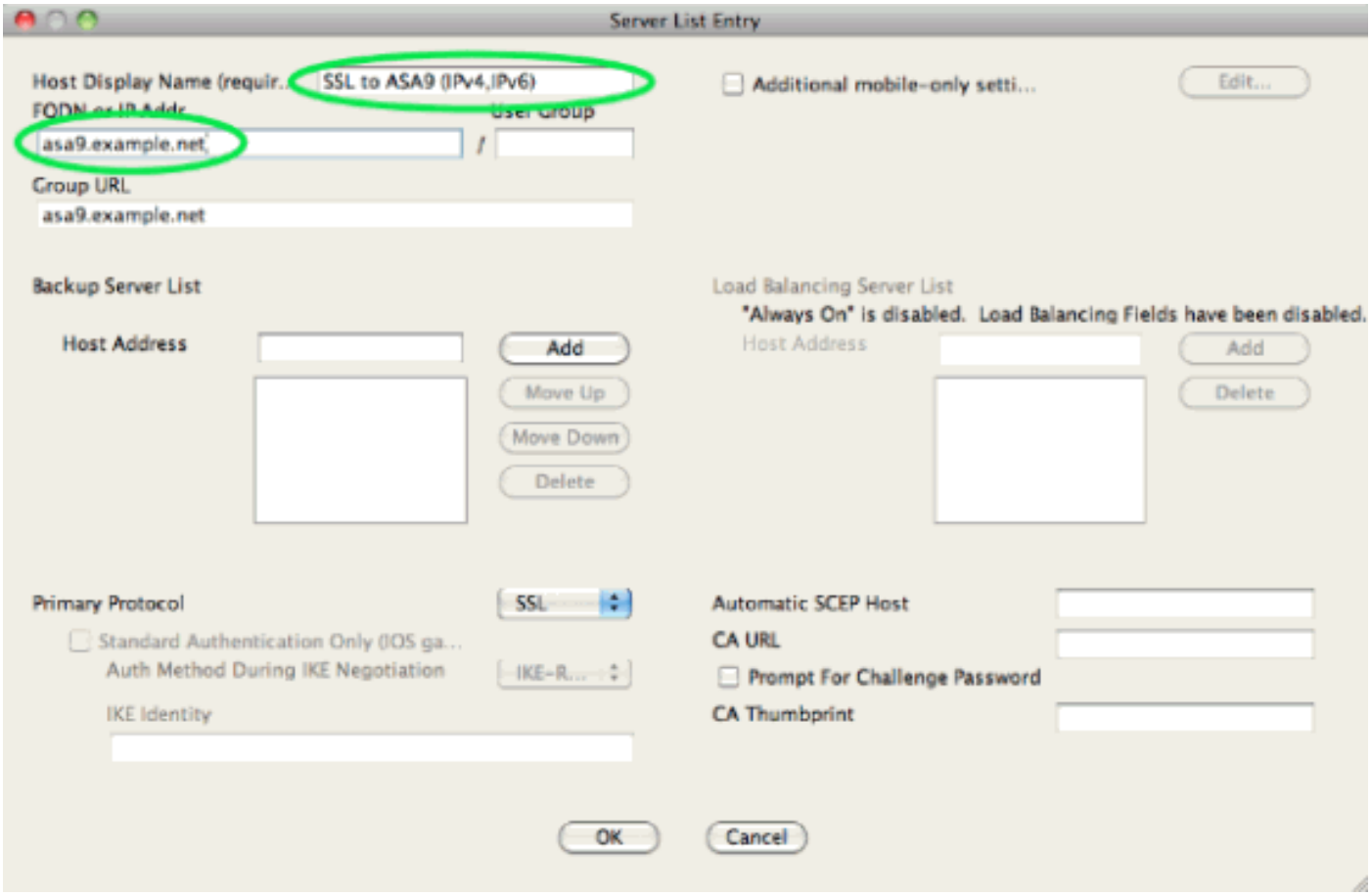
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

默认情况下， AnyConnect客户端尝试在IPv4连接，并且，只有当这发生故障，尝试在IPv6连接。然而，此行为可以由在XML配置文件的一设置更改。AnyConnect配置文件"asa9 SSLipv4v6.xml"，生成使用在ASDM (配置的配置文件编辑器-远程访问VPN -网络(被参考以上配置的客户端) Acccess - AnyConnect客户端配置文件)。




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



发生的XML配置文件(与大多数默认零件为简要起见省略) ：

```
<?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>
 ...


 <IPProtocolSupport>IPv6,IPv4</IPProtocolSupport> ... </ClientInitialization> <ServerList>
<HostEntry> <HostName>SSL to ASA9 (IPv4,IPv6)</HostName>
<HostAddress>asa9.example.net</HostAddress> </HostEntry> </ServerList> </AnyConnectProfile>
```

在上述配置文件主机名也定义(可以是的任何，不需要匹配ASA的实际主机名)和(典型地是ASA的FQDN)的主机地址。

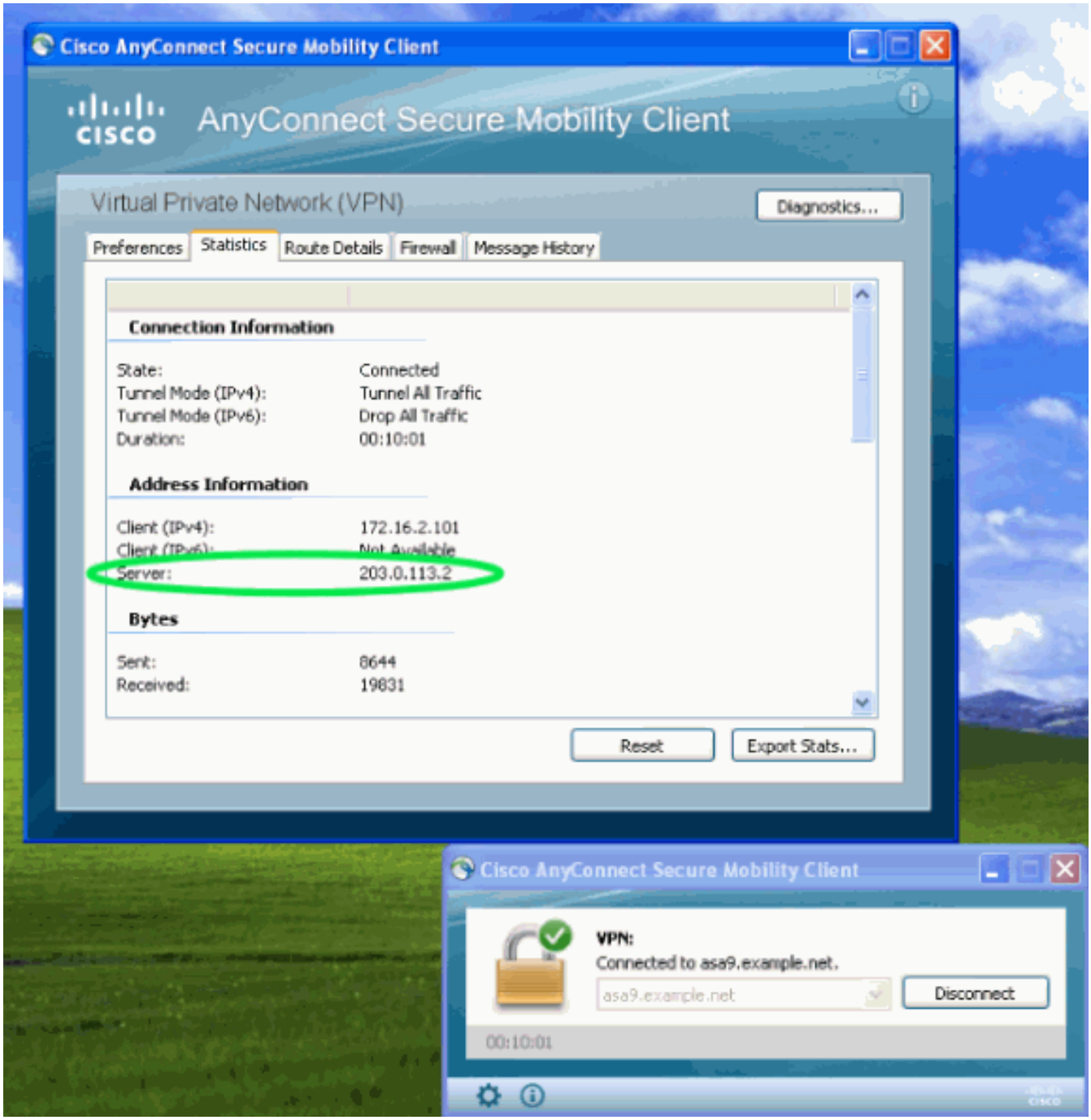
注意： 主机地址字段可以被离开空，但是Hostname Field必须包含ASA的FQDN。

注意： 除非配置文件PRE部署，第一个连接要求用户输入ASA的FQDN。此初始连接将更喜欢IPv4。在成功的连接以后，配置文件将下载。从那里，配置文件设置将应用。

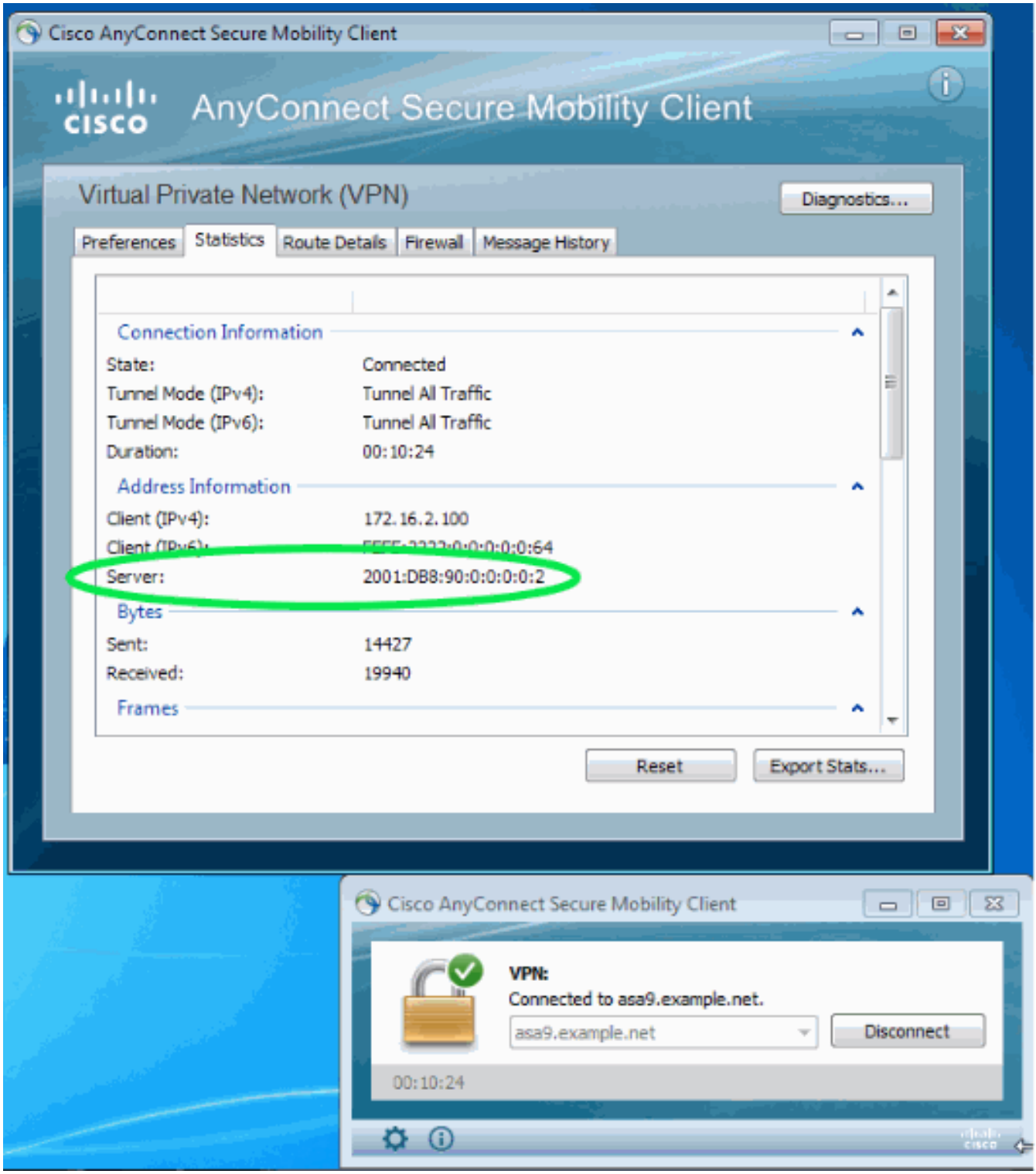
验证

为了验证客户端是否在IPv4或IPv6连接，请检查客户端GUI或VPN会话DB在ASA ：

- 在客户端，请打开Advanced窗口，去统计信息选项卡并且验证“服务器的” IP地址。此第一个用户从Windows XP系统连接，不用IPv6支持
  ：



此第二个用户从有IPv6连接的一台Windows 7主机连接对ASA
：



- 在ASA，从CLI检查“公有IP”在“显示vpn-sessiondb anyconnect”输出中。在本例中您能看到两连接和上述一样：一从在IPv4的XP和一个从在IPv6的Windows 7 ：`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