Configuração do AnyConnect SSL sobre IPv4+IPv6 para ASA

Contents

Introduction

Este documento fornece uma configuração de exemplo para o Cisco Adaptive Security Appliance (ASA) para permitir que o Cisco AnyConnect Secure Mobility Client (conhecido como "AnyConnect" no restante deste documento) estabeleça um túnel VPN SSL sobre uma rede IPv4 ou IPv6.

Além disso, essa configuração permite que o cliente passe o tráfego IPv4 e IPv6 pelo túnel.

Prerequisites

Requirements

Para estabelecer com êxito um túnel SSLVPN sobre IPv6, atenda aos seguintes requisitos:

- A conectividade IPv6 de ponta a ponta é necessária
- A versão do AnyConnect precisa ser 3.1 ou posterior
- A versão do software ASA precisa ser 9.0 ou posterior

No entanto, se algum desses requisitos não for atendido, a configuração discutida neste documento ainda permitirá que o cliente se conecte via IPv4.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA-5505 com versão de software 9.0(1)
- AnyConnect Secure Mobility Client 3.1.00495 no Microsoft Windows XP Professional (sem suporte a IPv6)

- AnyConnect Secure Mobility Client 3.1.00495 no Microsoft Windows 7 Enterprise de 32 bits

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configuração

Primeiro, defina um pool de endereços IP dos quais você atribuirá um a cada cliente que se conecta.

Se você quiser que o cliente também transporte tráfego IPv6 pelo túnel, precisará de um pool de endereços IPv6. Ambos os pools são referenciados posteriormente na política de grupo.

```
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
```

Para a conectividade IPv6 com o ASA, você precisa de um endereço IPv6 na interface à qual os clientes se conectarão (geralmente a interface externa).

Para conectividade IPv6 no túnel para hosts internos, você precisa do IPv6 na(s) interface(s) interna(ais) também.

```
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
```

Para IPv6, você também precisa de uma rota padrão apontando para o roteador do próximo salto em direção à Internet.

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

Para se autenticar nos clientes, o ASA precisa ter um certificado de identidade. As instruções sobre como criar ou importar esse certificado estão fora do escopo deste documento, mas podem ser facilmente encontradas em outros documentos, como

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

A configuração resultante deve ser semelhante à seguinte:

```
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
```

Em seguida, instrua o ASA a usar este certificado para SSL:

```
ssl trust-point testCA
```

A seguir, a configuração básica da webvpn (SSLVPN) onde o recurso é ativado na interface externa. Os pacotes de clientes disponíveis para download são definidos e definimos um perfil definido (mais adiante):

```
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
```

Neste exemplo básico, os pools de endereços IPv4 e IPv6 são configurados, as informações do servidor DNS (que serão enviadas ao cliente) e um perfil na política de grupo padrão (DfltGrpPolicy). Muitos outros atributos podem ser configurados aqui e, opcionalmente, você pode definir diferentes políticas de grupo para diferentes conjuntos de usuários.

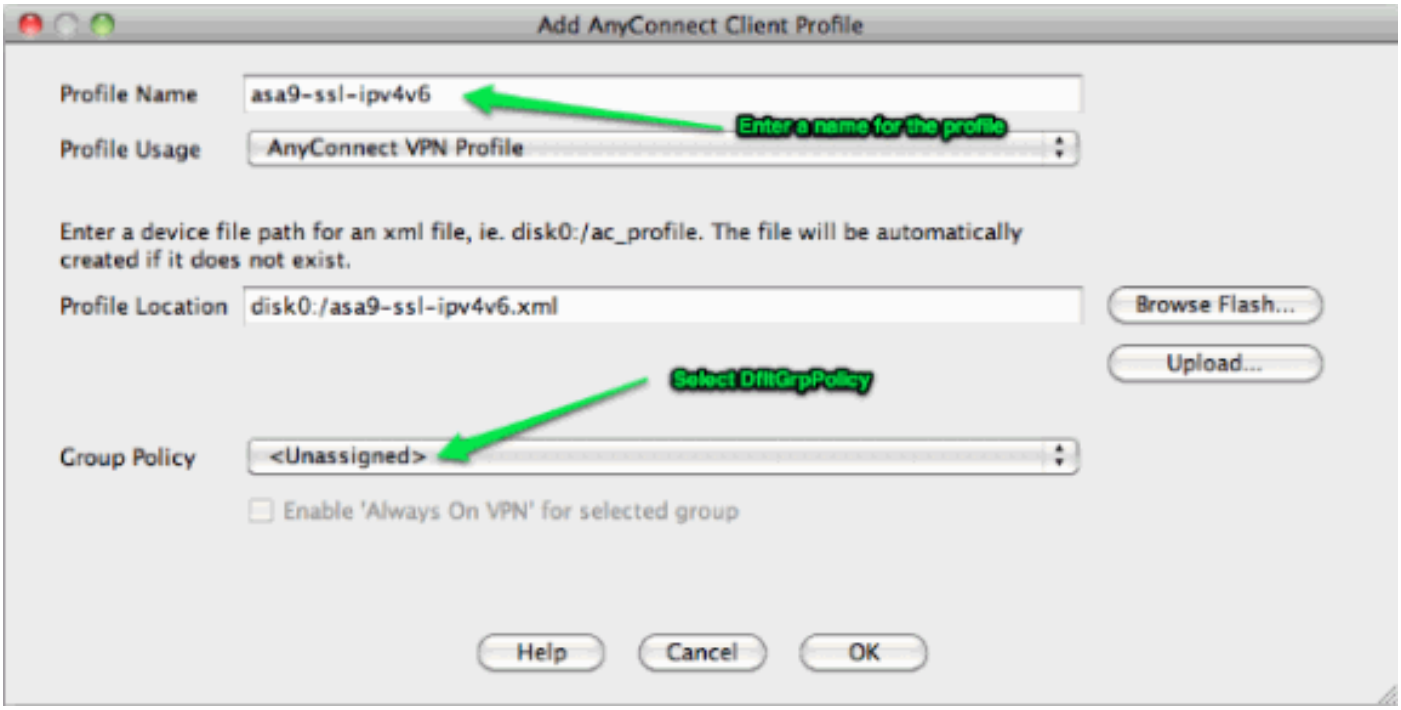
Observação: o atributo "gateway-fqdn" é novo na versão 9.0 e define o FQDN do ASA como é conhecido no DNS. O cliente aprende esse FQDN do ASA e o usará quando estiver em roaming de uma rede IPv4 para uma rede IPv6 ou vice-versa.

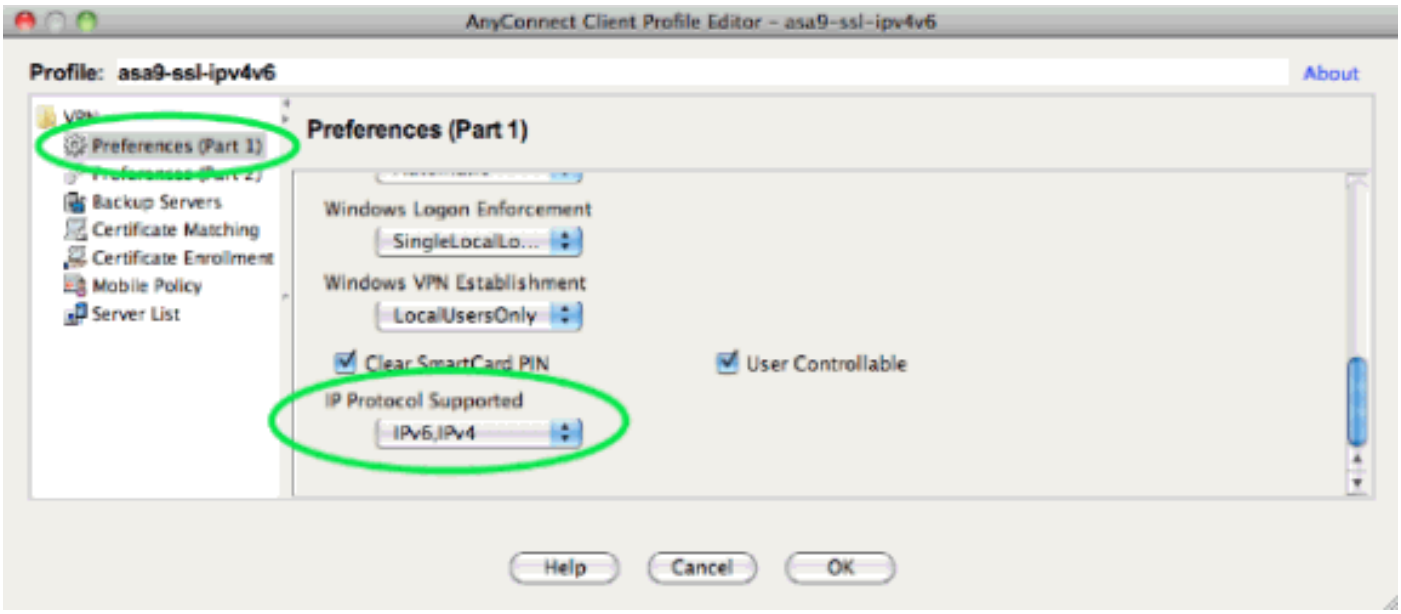
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

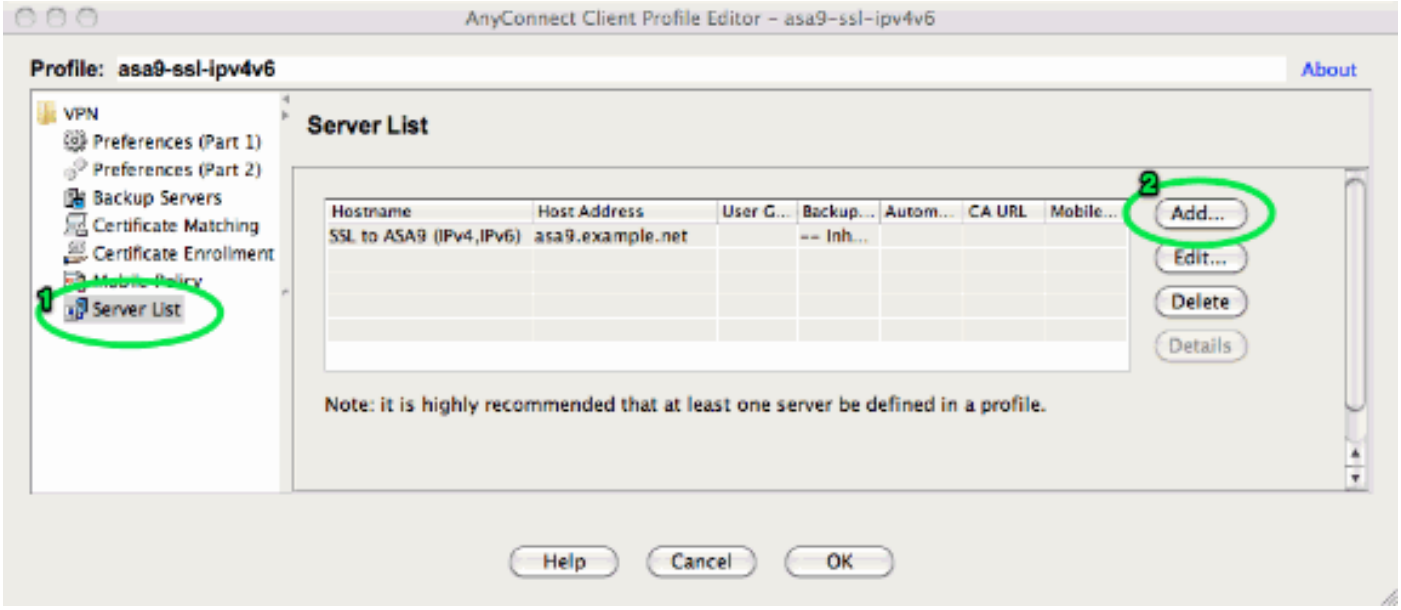
Em seguida, configure um ou mais grupos de túnel. O padrão (DefaultWEBVPNGroup) é usado para este exemplo e o configura para exigir que o usuário faça a autenticação usando um certificado:

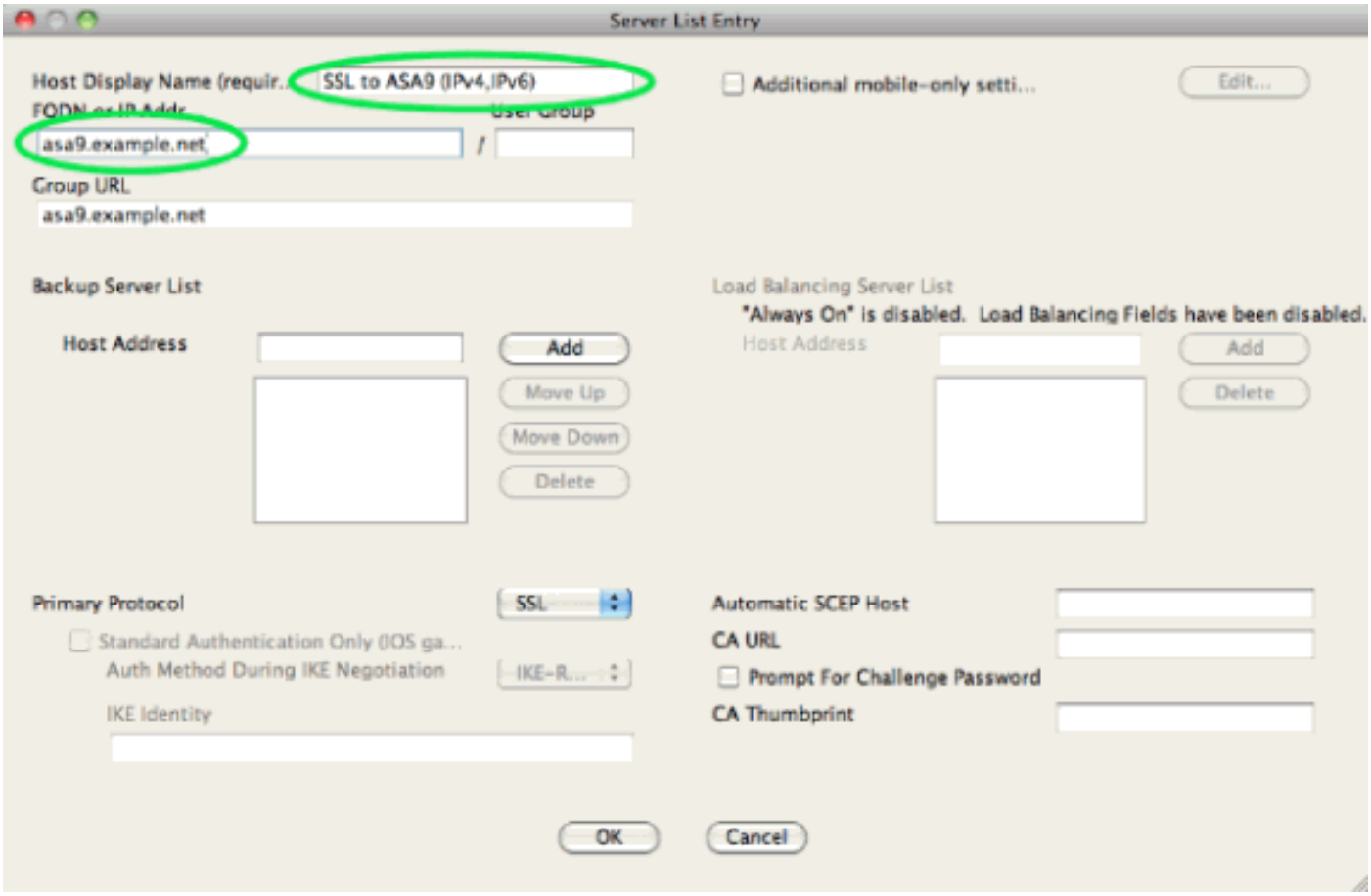
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

Por padrão, o cliente AnyConnect tenta se conectar via IPv4 e, somente se isso falhar, tenta se conectar via IPv6. Entretanto, esse comportamento pode ser alterado por uma configuração no perfil XML. O perfil do AnyConnect "asa9-ssl-ipv4v6.xml" referenciado na configuração acima, foi gerado usando o Editor de perfis no ASDM (Configuração - Acesso remoto VPN - Acesso à rede (cliente) - Perfil do cliente do AnyConnect).


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



O perfil XML resultante (com a maior parte da parte padrão omitida para ser breve):

```
<?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>
```

No perfil acima, um HostName também é definido (o que pode ser qualquer coisa, ele não precisa corresponder ao nome de host real do ASA) e um HostAddress (que geralmente é o FQDN do ASA).

Observação: o campo HostAddress pode ser deixado em branco, mas o campo HostName deve

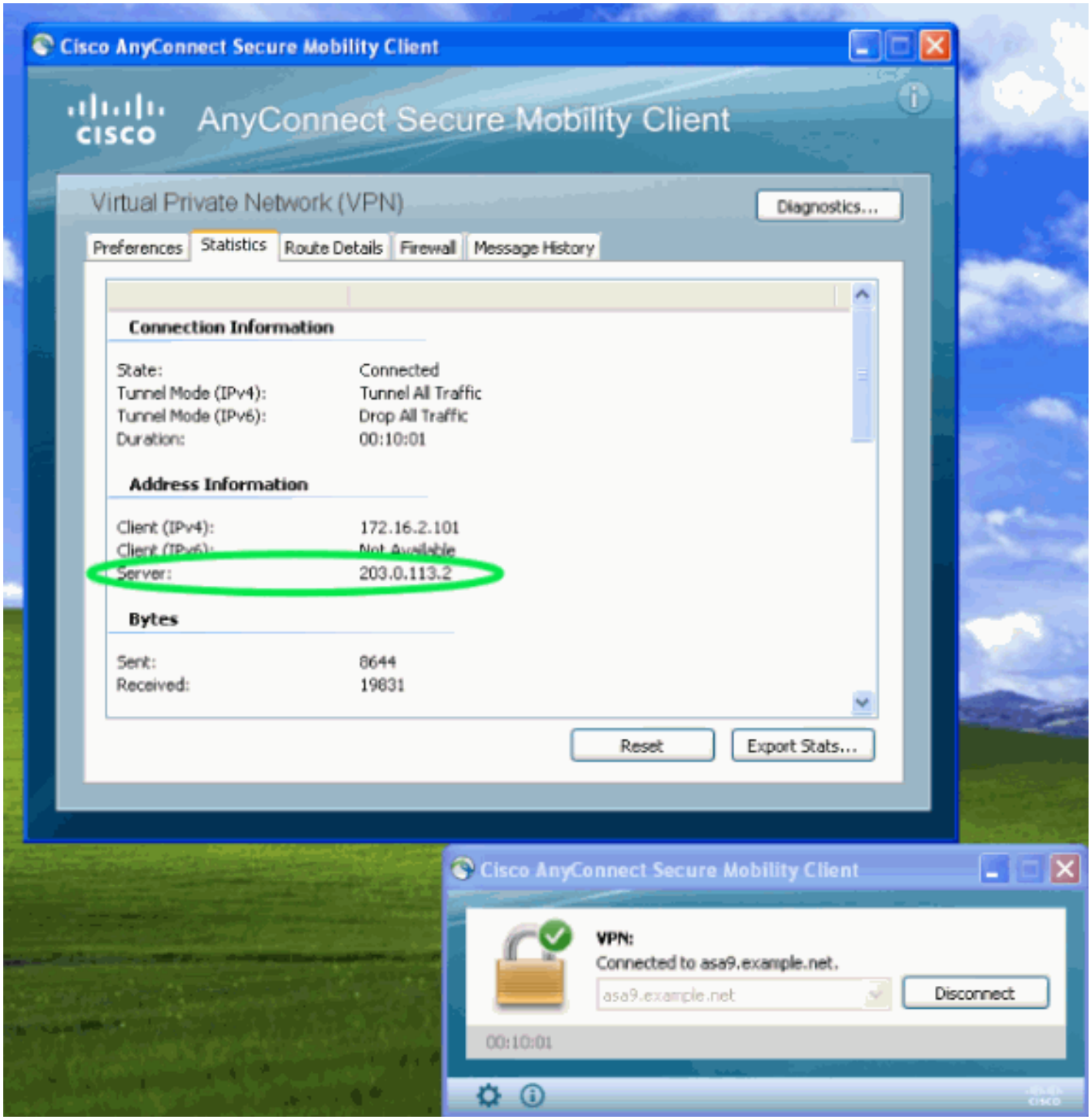
conter o FQDN do ASA.

Observação: a menos que o perfil seja pré-implantado, a primeira conexão exige que o usuário digite o FQDN do ASA. Essa conexão inicial preferirá o IPv4. Após a conexão bem-sucedida, o perfil será baixado. A partir daí, as configurações do perfil serão aplicadas.

Verificar

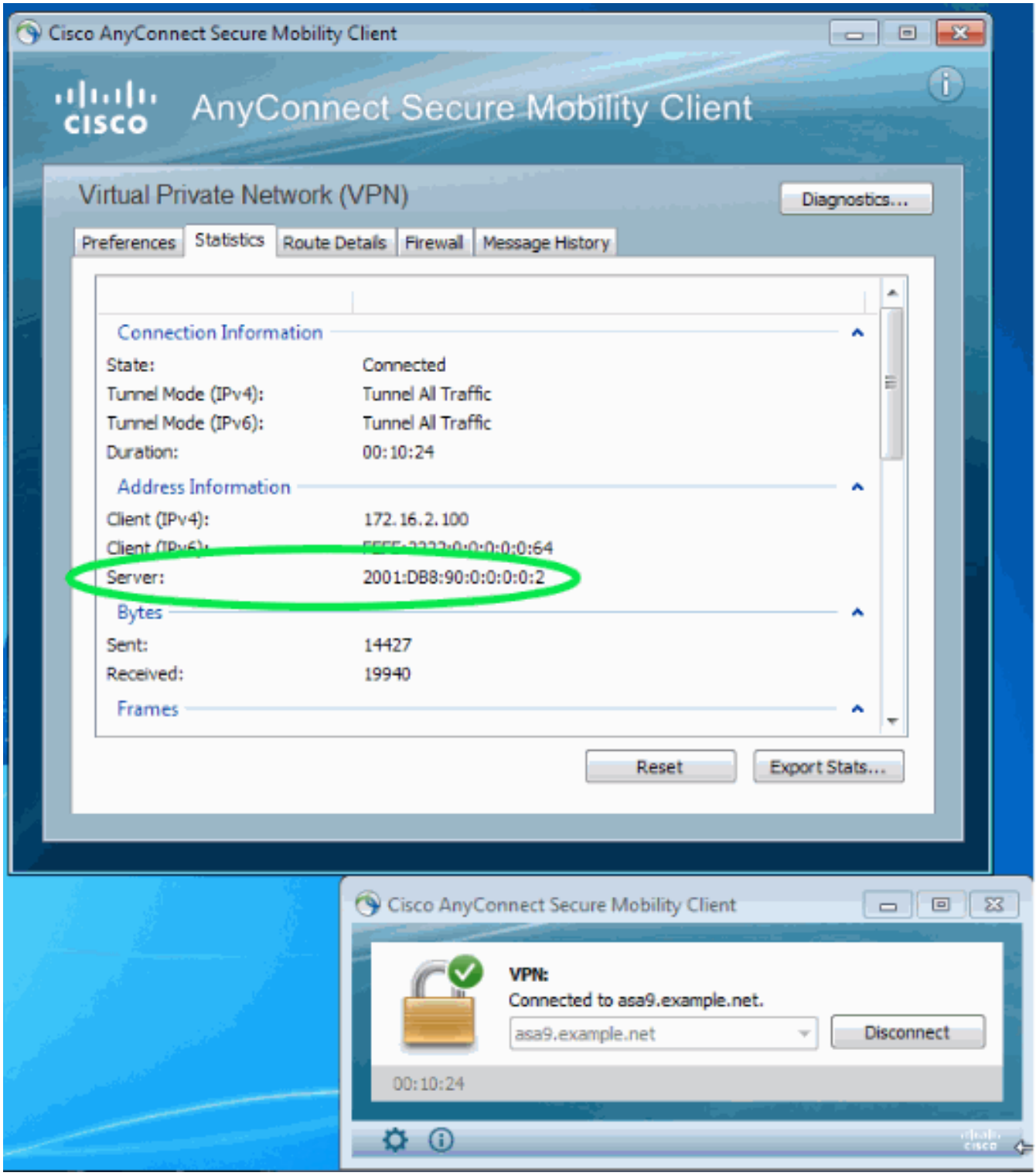
Para verificar se um cliente está conectado por IPv4 ou IPv6, verifique a GUI do cliente ou o banco de dados da sessão VPN no ASA:

- No cliente, abra a janela Avançado, acesse a guia Estatísticas e verifique o endereço IP do "Servidor".Este primeiro usuário está se conectando de um sistema Windows XP sem suporte para
  IPv6:



Este segundo usuário se conecta de um host Windows 7 com conectividade IPv6 ao

ASA:



- No ASA, na CLI, verifique o "IP público" na saída "show vpn-sessiondb anyconnect". Neste exemplo, você pode ver as mesmas duas conexões acima: um do XP sobre IPv4 e um do Windows 7 sobre 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
```

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems