Configuración de AnyConnect SSL sobre IPv4+IPv6 a ASA

Contenido

Introducción

Este documento proporciona una configuración de ejemplo para Cisco Adaptive Security Appliance (ASA) para permitir que Cisco AnyConnect Secure Mobility Client (denominado "AnyConnect" en el resto de este documento) establezca un túnel SSL VPN a través de una red IPv4 o IPv6.

Además, esta configuración permite al cliente pasar tráfico IPv4 e IPv6 por el túnel.

Prerequisites

Requirements

Para establecer correctamente un túnel SSLVPN sobre IPv6, cumpla estos requisitos:

- Se requiere conectividad IPv6 de extremo a extremo
- La versión de AnyConnect debe ser 3.1 o posterior
- La versión del software ASA debe ser 9.0 o posterior

Sin embargo, si no se cumple alguno de estos requisitos, la configuración que se describe en este documento seguirá permitiendo que el cliente se conecte a través de IPv4.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA-5505 con versión de software 9.0(1)
- AnyConnect Secure Mobility Client 3.1.00495 en Microsoft Windows XP Professional (sin

compatibilidad con IPv6)
- AnyConnect Secure Mobility Client 3.1.00495 en Microsoft Windows 7 Enterprise de 32 bits

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configuración

En primer lugar, defina un conjunto de direcciones IP desde el que asignará una a cada cliente que se conecte.

Si desea que el cliente también transporte tráfico IPv6 a través del túnel, necesitará un conjunto de direcciones IPv6. A ambos grupos se hace referencia más adelante en la 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 la conectividad IPv6 al ASA, necesita una dirección IPv6 en la interfaz a la que se conectarán los clientes (normalmente la interfaz externa).

Para la conectividad IPv6 a través del túnel a los hosts internos, también necesita IPv6 en las interfaces internas.

```
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, también necesita una ruta predeterminada que apunte al router de salto siguiente hacia 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 autenticarse en los clientes, el ASA necesita tener un certificado de identidad. Las instrucciones sobre cómo crear o importar un certificado están fuera del alcance de este documento, pero pueden encontrarse fácilmente en otros documentos como

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

La configuración resultante debe ser similar a la siguiente:

```
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
```

A continuación, indique al ASA que utilice este certificado para SSL:

```
ssl trust-point testCA
```

A continuación, se encuentra la configuración básica de webvpn (SSLVPN), donde la función está activada en la interfaz externa. Se definen los paquetes de cliente disponibles para su descarga y se define un perfil (más adelante):

```
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
```

En este ejemplo básico, se configuran los conjuntos de direcciones IPv4 e IPv6, la información del servidor DNS (que se enviará al cliente) y un perfil en la política de grupo predeterminada (DfltGrpPolicy). Aquí se pueden configurar muchos atributos más y, opcionalmente, puede definir diferentes políticas de grupo para diferentes conjuntos de usuarios.

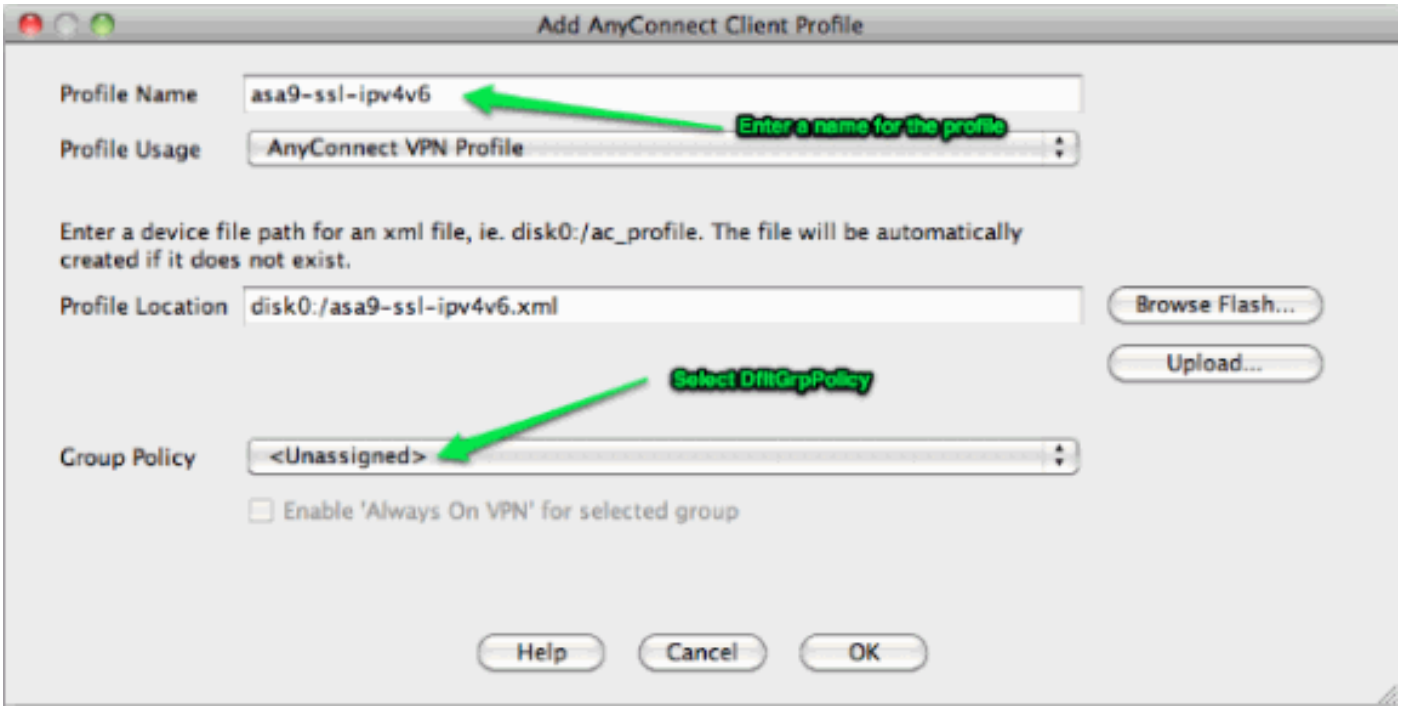
Nota: El atributo "gateway-fqdn" es nuevo en la versión 9.0 y define el FQDN del ASA como se conoce en el DNS. El cliente aprende este FQDN del ASA y lo utilizará cuando se desplace de una red IPv4 a una red IPv6 o viceversa.

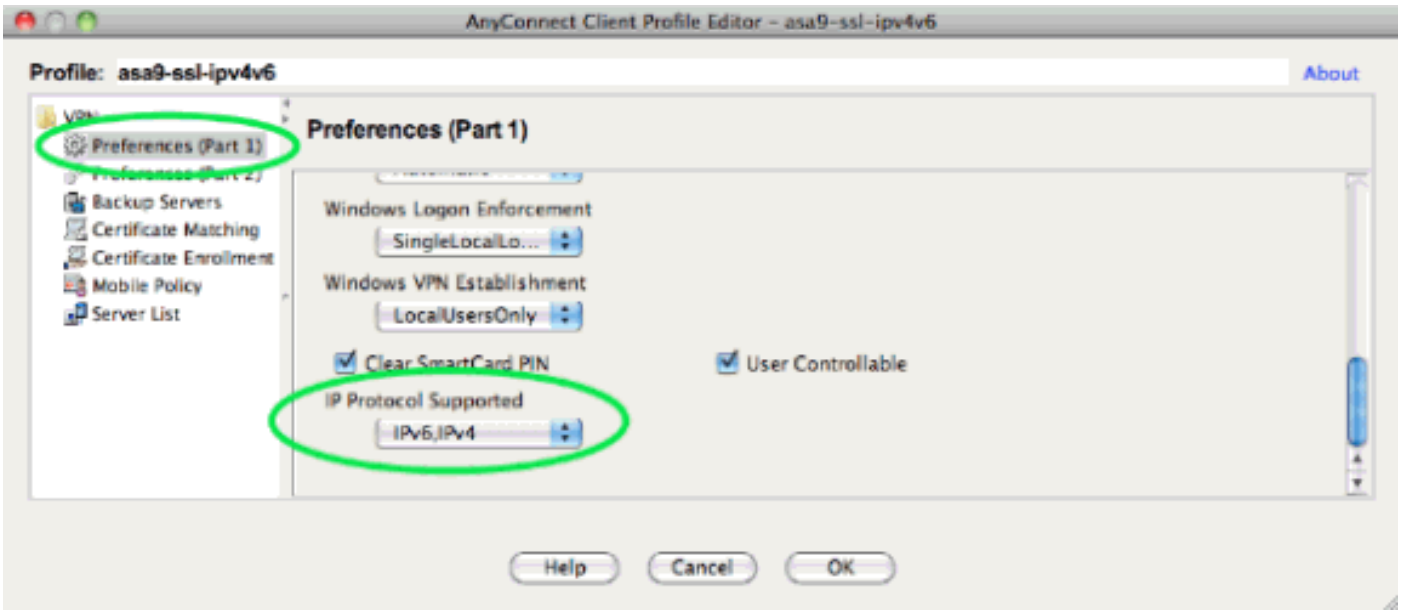
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

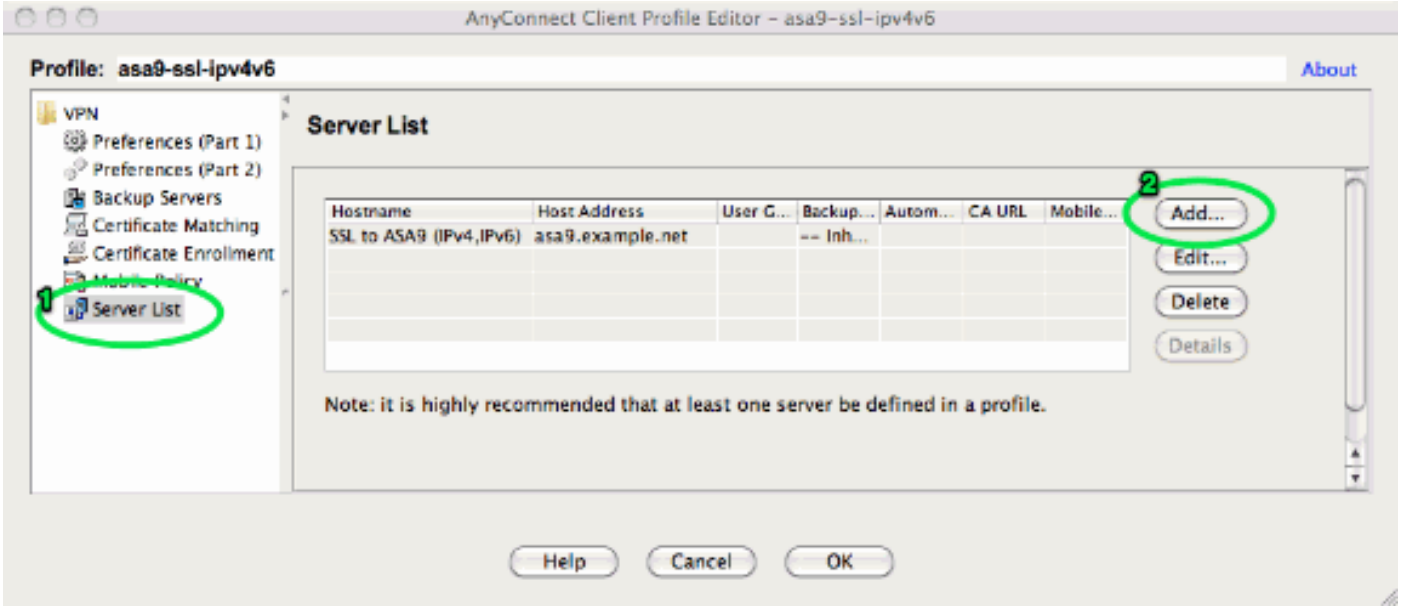
A continuación, configure uno o varios grupos de túnel. El valor predeterminado (DefaultWEBVPNGroup) se utiliza para este ejemplo, y configúrelo para que el usuario requiera la autenticación mediante un certificado:

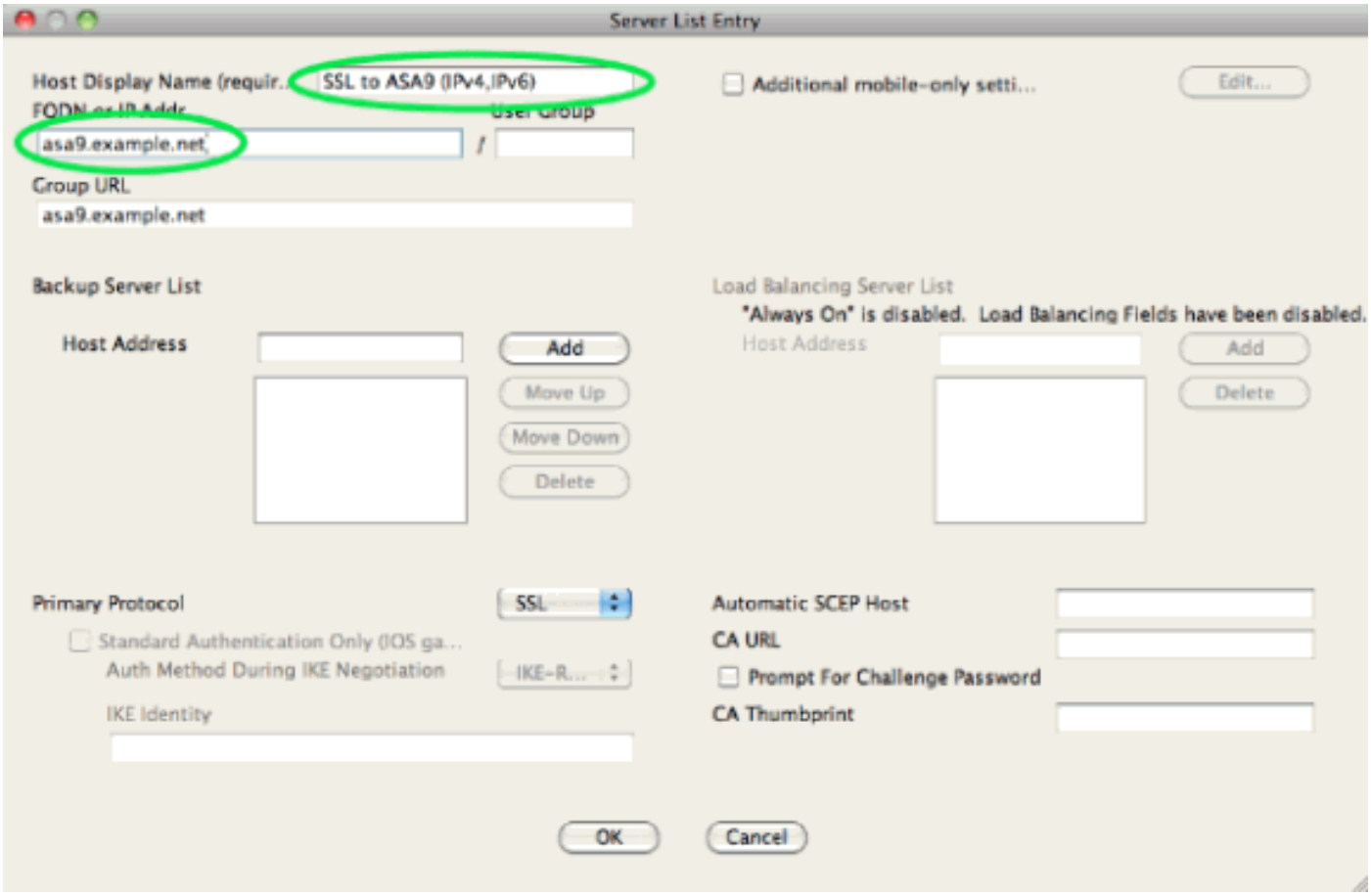
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

De forma predeterminada, el cliente AnyConnect intenta conectarse a través de IPv4 y, sólo si esto falla, intenta conectarse a través de IPv6. Sin embargo, este comportamiento se puede cambiar mediante una configuración en el perfil XML. El perfil de AnyConnect "asa9-ssl-ipv4v6.xml" al que se hace referencia en la configuración anterior, se generó mediante el Editor de perfiles en ASDM (Configuración - VPN de acceso remoto - Acceso de red (cliente) - Perfil de cliente de 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



El perfil XML resultante (con la mayoría de la pieza predeterminada omitida para la brevedad):

```
<?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>
```

En el perfil anterior también se define un HostName (que puede ser cualquier cosa, no necesita coincidir con el nombre de host real del ASA) y un HostAddress (que normalmente es el FQDN del ASA).

Nota: El campo HostAddress se puede dejar vacío, pero el campo HostName debe contener el

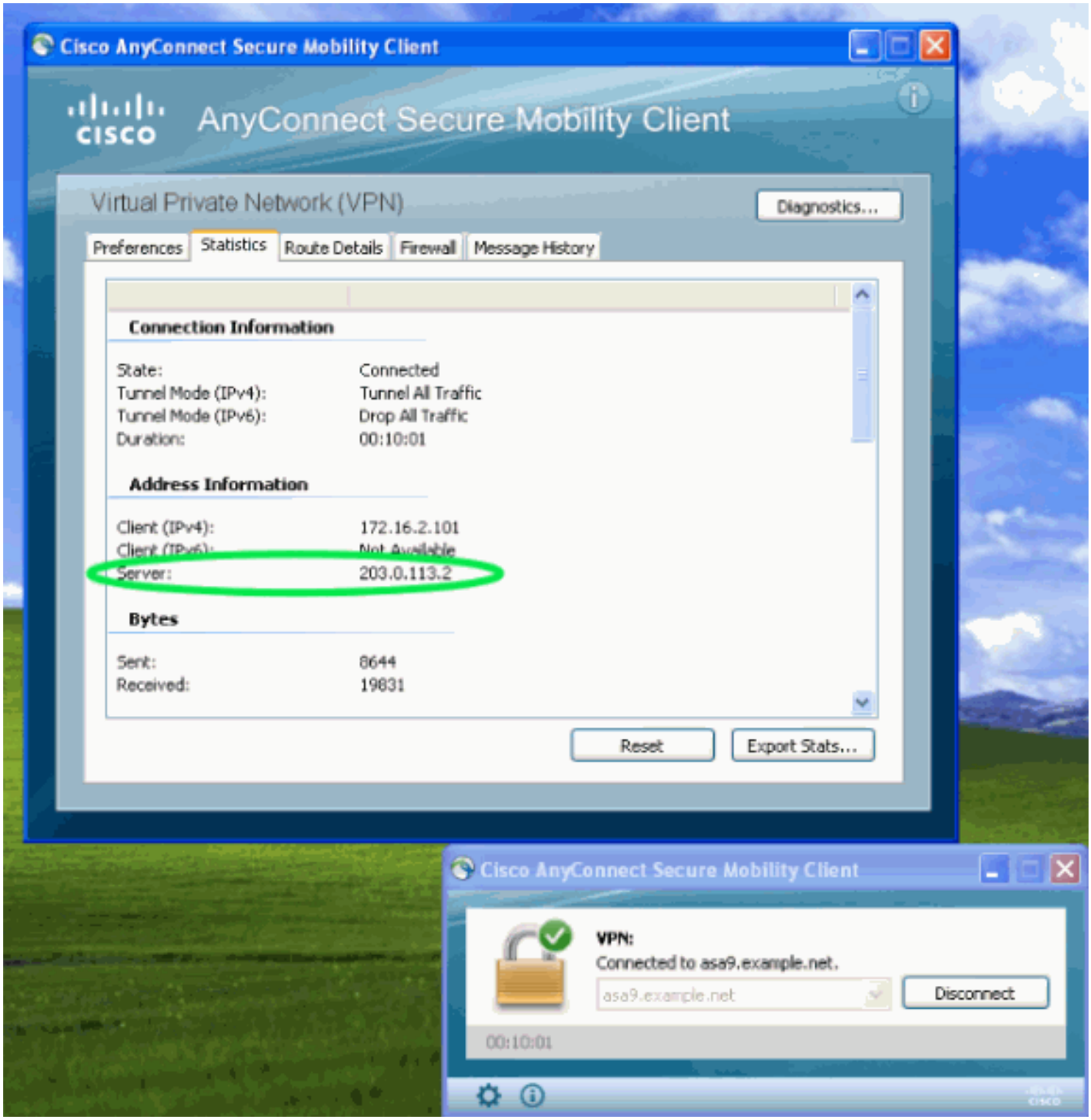
FQDN del ASA.

Nota: A menos que el perfil esté preimplementado, la primera conexión requiere que el usuario escriba el FQDN del ASA. Esta conexión inicial preferirá IPv4. Después de una conexión correcta, el perfil se descargará. A partir de ahí, se aplicará la configuración del perfil.

Verificación

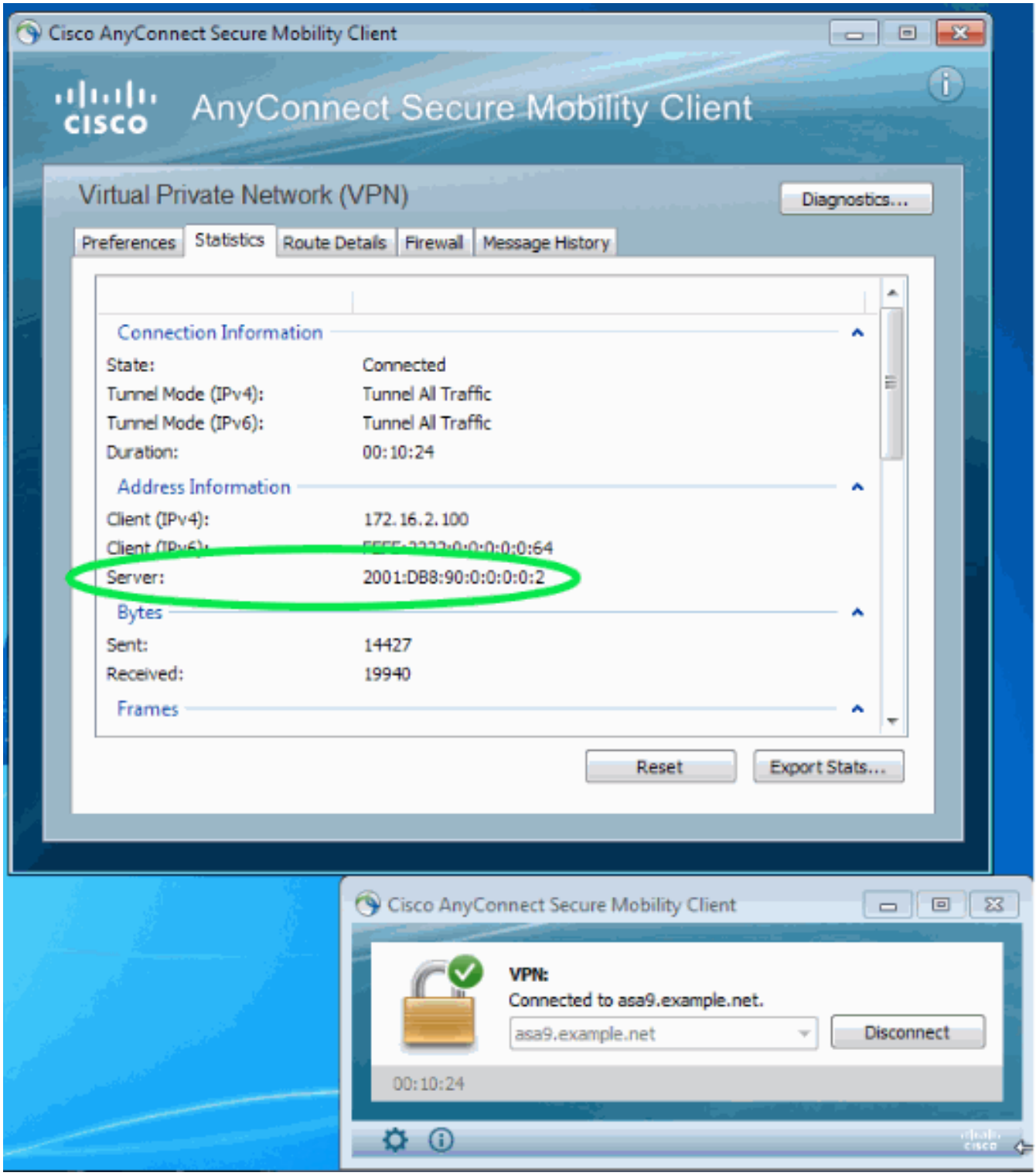
Para verificar si un cliente está conectado a través de IPv4 o IPv6, verifique la GUI del cliente o la base de datos de la sesión VPN en el ASA:

- En el cliente, abra la ventana Avanzadas, vaya a la ficha Estadísticas y verifique la dirección IP del "Servidor".Este primer usuario se conecta desde un sistema Windows XP sin compatibilidad con
  IPv6:



Este segundo usuario se conecta desde un host Windows 7 con conectividad IPv6 al

ASA:



- En el ASA, desde la CLI, verifique la "IP pública" en el resultado "show vpn-sessiondb anyconnect". En este ejemplo puede ver las mismas dos conexiones como las anteriores: uno de XP sobre IPv4 y uno de 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
```

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems