AnyConnect SSL sobre IPv4+IPv6 a la configuración ASA

Contenido

Introducción

Este documento proporciona una configuración de muestra para el dispositivo de seguridad adaptante de Cisco (ASA) para permitir que el Cliente de movilidad Cisco AnyConnect Secure (designado “AnyConnect” en el recordatorio de este documento) establezca un túnel SSL VPN sobre una red del IPv4 o del IPv6.

Además, esta configuración permite que el cliente pase el tráfico del IPv4 y del IPv6 sobre el túnel.

prerrequisitos

Requisitos

Para establecer con éxito un túnel SSLVPN sobre el IPv6, cumpla estos requisitos:

- Se requiere la Conectividad de punta a punta del IPv6
- La versión de AnyConnect necesita ser 3.1 o más adelante
- La versión de software ASA necesita ser 9.0 o más adelante

Sin embargo, si ninguno de estos requisitos no se cumplen, la configuración discutida en este documento todavía permitirá que el cliente conecte sobre el IPv4.

Componentes Utilizados

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

- ASA-5505 con la versión de software 9.0(1)

- Cliente seguro 3.1.00495 de la movilidad de AnyConnect en el profesional del Microsoft Windows XP (sin el soporte del IPv6)
- Cliente seguro 3.1.00495 de la movilidad de AnyConnect en la empresa de Microsoft Windows 7 de 32 bits

Convenciones

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

Configuración

Primero apagado, defina un pool de los IP Addresses de las cuales usted asigne uno a cada cliente que conecte.

Si usted quisiera que el cliente también llevara el tráfico del IPv6 sobre el túnel, usted necesitará un pool de los direccionamientos del IPv6. Ambos pools se refieren más adelante a la grupo-directiva.

```
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 del IPv6 al ASA, usted necesita un direccionamiento del IPv6 en la interfaz con la cual los clientes conectarán (típicamente la interfaz exterior).

Para la Conectividad del IPv6 sobre el túnel a los host interiores, usted necesita el IPv6 en la interfaz interior también.

```
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 el IPv6, usted también necesita una ruta predeterminado que señala al Next Hop Router 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 a los clientes, el ASA necesita tener un certificado de identidad. Las instrucciones en cómo crear o importar tal certificado están fuera del alcance de este documento, pero se pueden encontrar fácilmente en otros documentos por ejemplo

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

La configuración resultante debe parecer similar al 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
```

Entonces, dé instrucciones el ASA para utilizar este certificado para el SSL:

```
ssl trust-point testCA
```

Está después la configuración básica del webvpn (SSLVPN) donde la característica se habilita en la interfaz exterior. Se definen se definen los paquetes del cliente que están disponibles para la descarga, y nosotros definen un perfil (más en esto 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 configura el IPv4 y las agrupaciones de direcciones del IPv6, la información del servidor DNS (que será avanzado al cliente) y un perfil en la grupo-directiva predeterminada (DfltGrpPolicy). Muchos más atributos se pueden configurar aquí, y usted puede definir opcionalmente diversas grupo-directivas para diversos conjuntos de los usuarios.

Note: El atributo “gateway-FQDN” es nuevo en la versión 9.0 y define el FQDN del ASA pues se sabe en el DNS. El cliente aprende este FQDN del ASA y lo utilizará al vagar por de un IPv4 a una red del IPv6 o vice versa.

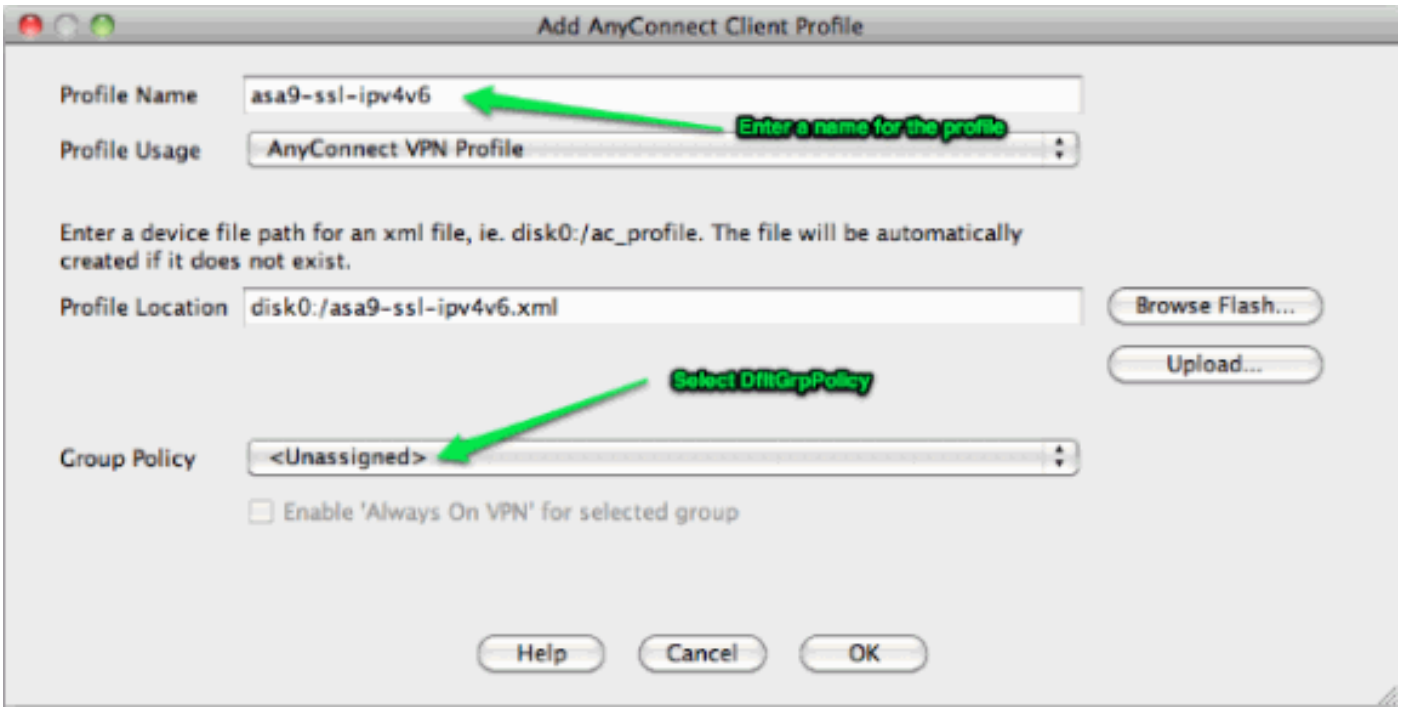
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

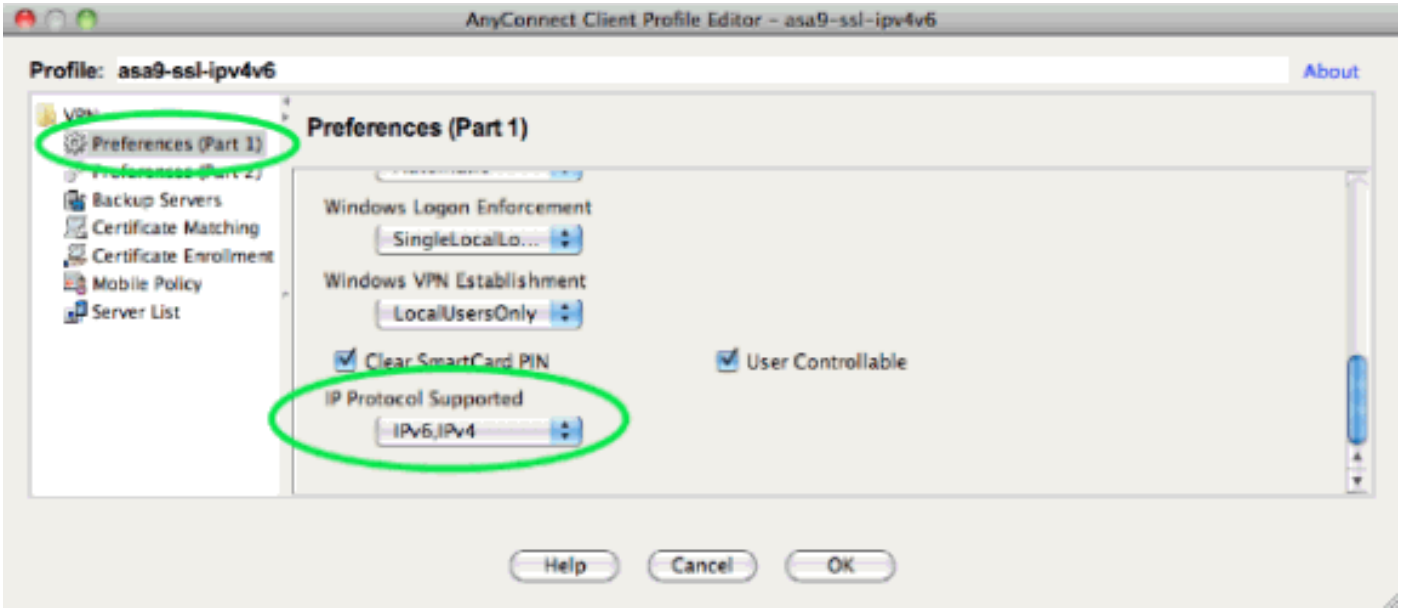
Después, configure a uno o más grupos de túnel. El predeterminado (DefaultWEBVPNGroup) se utiliza para este ejemplo, y lo configura para requerir al usuario autenticar usando un certificado:

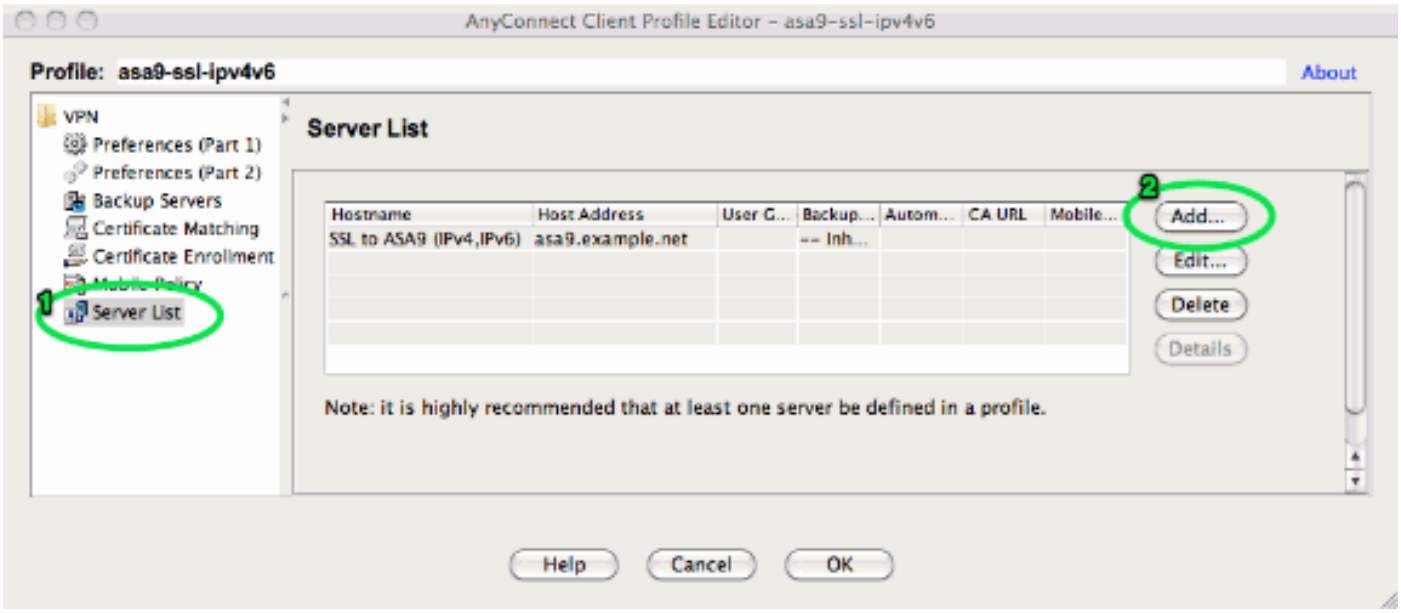
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

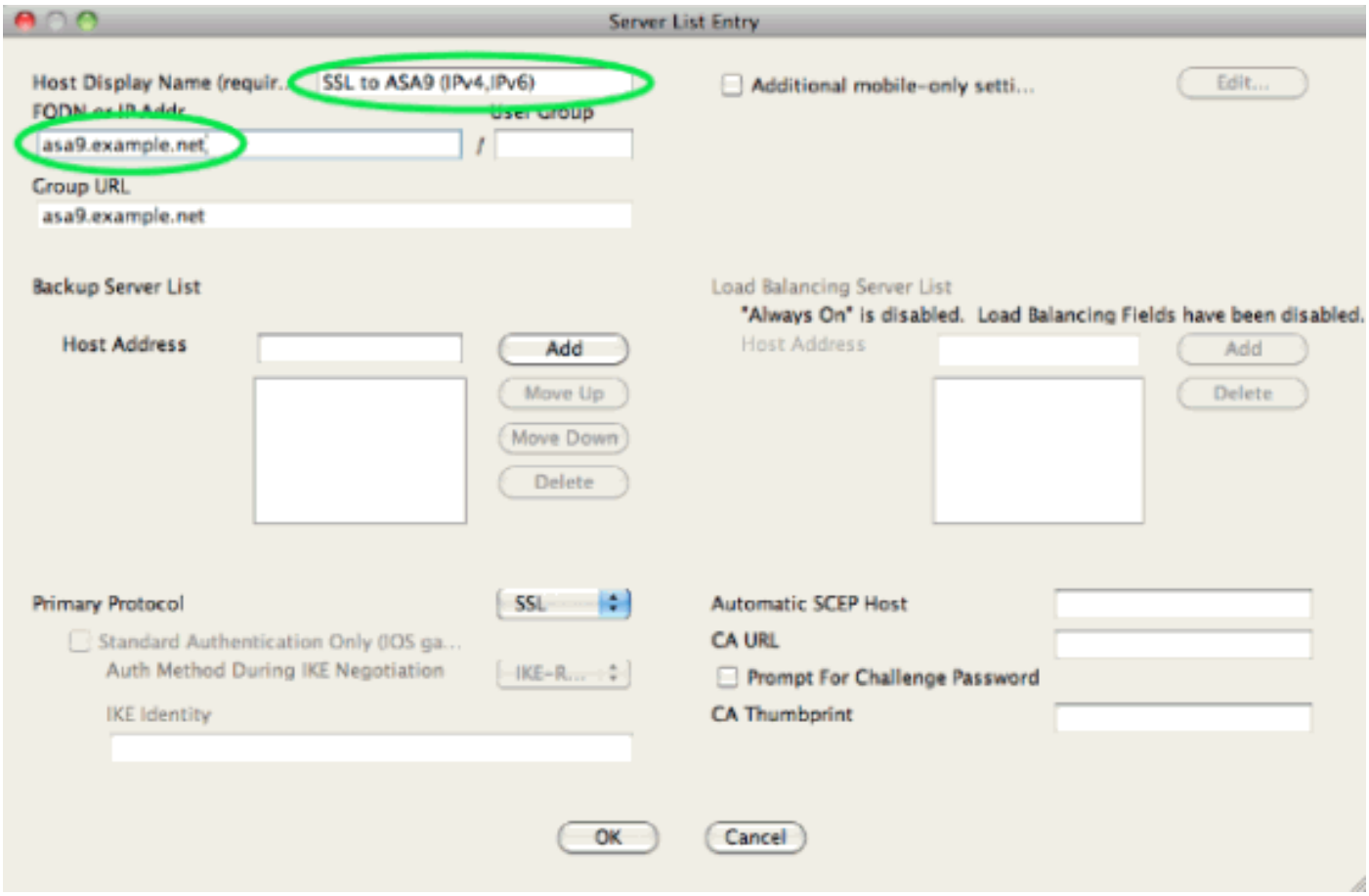
Por abandono, el cliente de AnyConnect intenta conectar sobre el IPv4 y, sólo si éste falla, intenta conectar sobre el IPv6. Sin embargo, este comportamiento se puede cambiar por una configuración en el perfil XML. El perfil "asa9-SSL-ipv4v6.xml" de AnyConnect que se refiere a la

configuración arriba, fue generado usando el editor del perfil en el ASDM (configuración - VPN de acceso remoto - red (cliente) perfil del cliente de Acccess - de AnyConnect).









El perfil resultante XML (con la mayor parte de la parte 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>
 ...

 <IPProtocolSupport>IPv6,IPv4</IPProtocolSupport>
 ...
</ClientInitialization>
```

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

En el perfil antedicho un nombre de host también se define (que pueden ser cualquier cosa, no necesita hacer juego el nombre del host real ASA), y un host address (que sea típicamente el FQDN ASA).

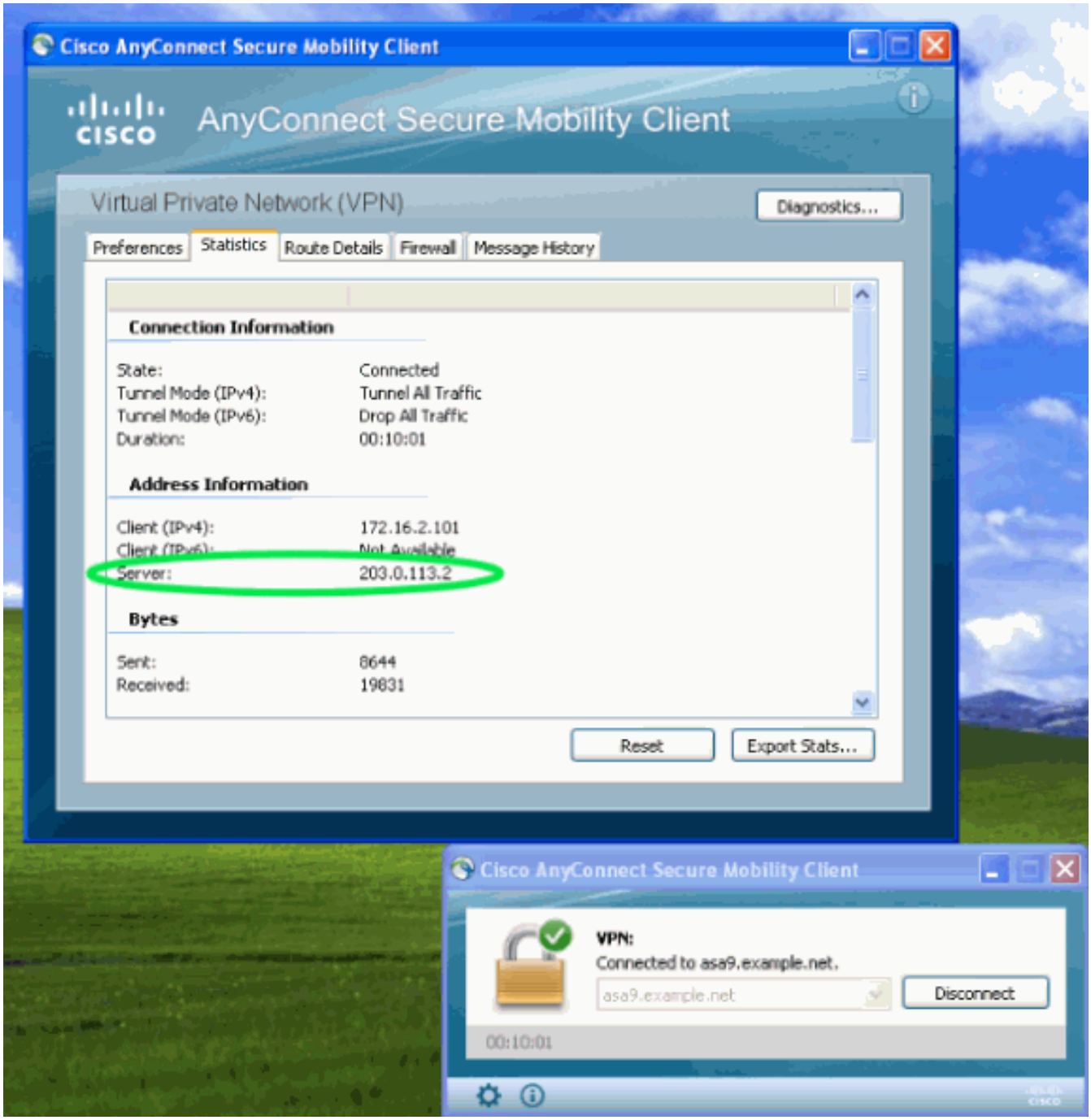
Note: El campo del host address se puede dejar vacío, pero el campo del nombre de host debe contener el FQDN ASA.

Note: A menos que se predespliegue el perfil, la primera conexión requiere al usuario teclear adentro el FQDN del ASA. Esta conexión inicial preferirá el IPv4. Después de la conexión satisfactoria, el perfil será descargado. De allí, las configuraciones del perfil serán aplicadas.

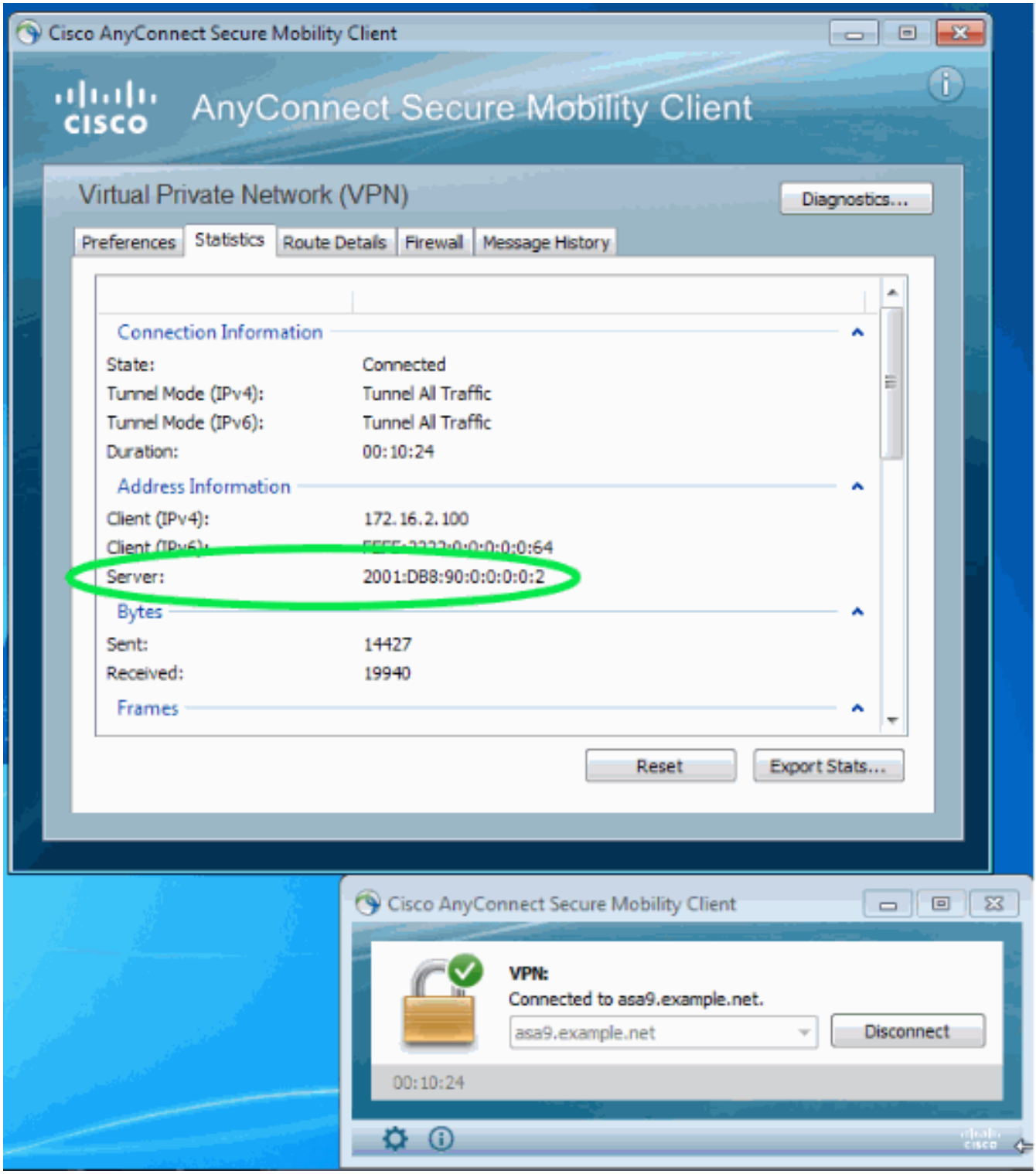
Verificación

Para verificar si un cliente esté conectado sobre el IPv4 o el IPv6, marque el cliente GUI o a la sesión de VPN DB en el ASA:

- En el cliente, abra la ventana avanzada, vaya a la lengueta de las estadísticas y verifique la dirección IP del “servidor”.Este primer usuario está conectando de un sistema de Windows XP sin el soporte del
  IPv6:



Este segundo usuario conecta de un host de Windows 7 con la Conectividad del IPv6 con el ASA:



- En el ASA, del control CLI “IP del público” en “la salida del anyconnect de VPN-sessiondb de la demostración”. En este ejemplo usted puede ver las mismas dos conexiones que arriba: uno de XP sobre el IPv4 y uno de Windows 7 sobre el 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