AnyConnect SSL su IPv4+IPv6 su configurazione ASA

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per Cisco Adaptive Security Appliance (ASA) in modo da consentire a Cisco AnyConnect Secure Mobility Client (indicato come "AnyConnect" nel prosieguo del documento) di stabilire un tunnel VPN SSL su una rete IPv4 o IPv6.

Inoltre, questa configurazione consente al client di passare il traffico IPv4 e IPv6 sul tunnel.

Prerequisiti

Requisiti

Per stabilire correttamente un tunnel SSLVPN su IPv6, soddisfare i seguenti requisiti:

- Connettività IPv6 end-to-end necessaria
- La versione di AnyConnect deve essere 3.1 o successiva
- La versione del software ASA deve essere 9.0 o successiva

Tuttavia, se uno di questi requisiti non viene soddisfatto, la configurazione descritta in questo documento consentirà al client di connettersi su IPv4.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA-5505 con software versione 9.0(1)
- AnyConnect Secure Mobility Client 3.1.00495 su Microsoft Windows XP Professional (senza

supporto IPv6)
- AnyConnect Secure Mobility Client 3.1.00495 su Microsoft Windows 7 Enterprise a 32 bit

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

Definire innanzitutto un pool di indirizzi IP da cui assegnarne uno a ogni client che si connette.

Se si desidera che il client trasporti anche il traffico IPv6 sul tunnel, sarà necessario un pool di indirizzi IPv6. In seguito, nei criteri di gruppo viene fatto riferimento a entrambi i pool.

```
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
```

Per la connettività IPv6 all'appliance ASA, è necessario un indirizzo IPv6 sull'interfaccia a cui si connetteranno i client, in genere l'interfaccia esterna.

Per la connettività IPv6 tramite il tunnel verso gli host interni, è necessario utilizzare anche IPv6 sulle interfacce interne.

```
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
```

Per IPv6 è inoltre necessario un percorso predefinito che punti al router dell'hop successivo verso Internet.

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

Per autenticarsi sui client, l'ASA deve avere un certificato di identità. Le istruzioni su come creare o importare un certificato di questo tipo esulano dall'ambito del presente documento, ma possono essere facilmente trovate in altri documenti, ad esempio

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

La configurazione risultante dovrebbe essere simile alla seguente:

```
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
```

Quindi, chiedere all'ASA di usare questo certificato per SSL:

```
ssl trust-point testCA
```

Di seguito viene riportata la configurazione base della webvpn (SSLVPN) con la funzionalità abilitata sull'interfaccia esterna. Vengono definiti i pacchetti client disponibili per il download e viene definito un profilo (ulteriori informazioni in merito sono disponibili più avanti):

```
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
```

In questo esempio di base vengono configurati i pool di indirizzi IPv4 e IPv6, le informazioni sul server DNS (che verranno inviate al client) e un profilo in Criteri di gruppo predefiniti (DfltGrpPolicy). In questa finestra è possibile configurare molti altri attributi e, facoltativamente, definire criteri di gruppo diversi per gruppi di utenti diversi.

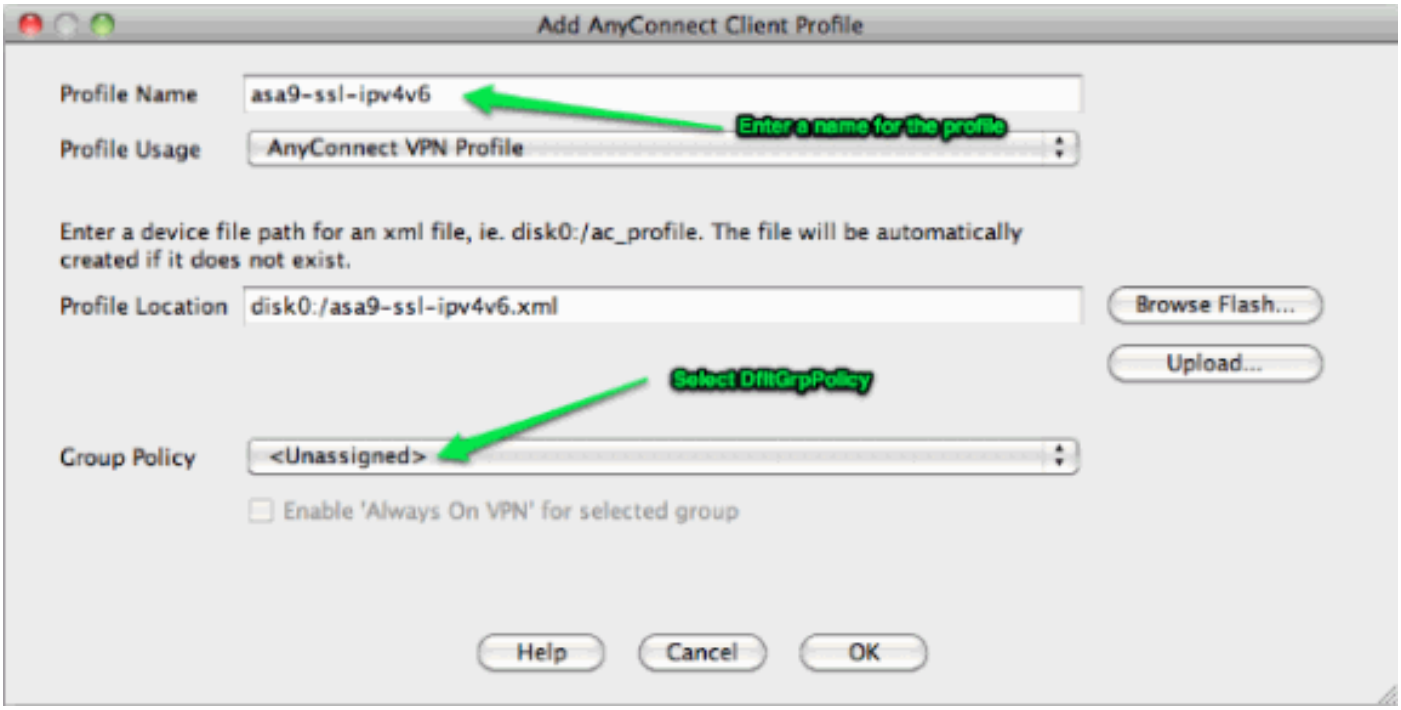
Nota: l'attributo "gateway-fqdn" è stato introdotto nella versione 9.0 e definisce il nome di dominio completo (FQDN) dell'ASA come è noto nel DNS. Il client apprende questo FQDN dall'ASA e lo utilizzerà durante il roaming da una rete IPv4 a una rete IPv6 o viceversa.

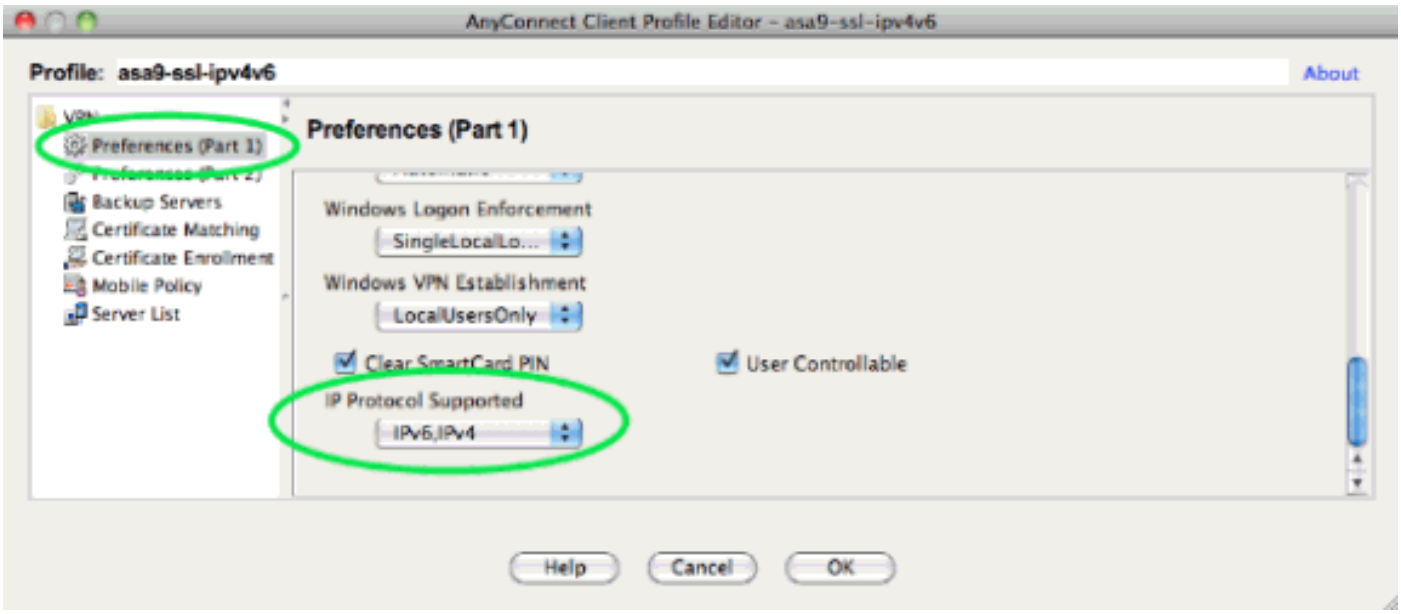
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

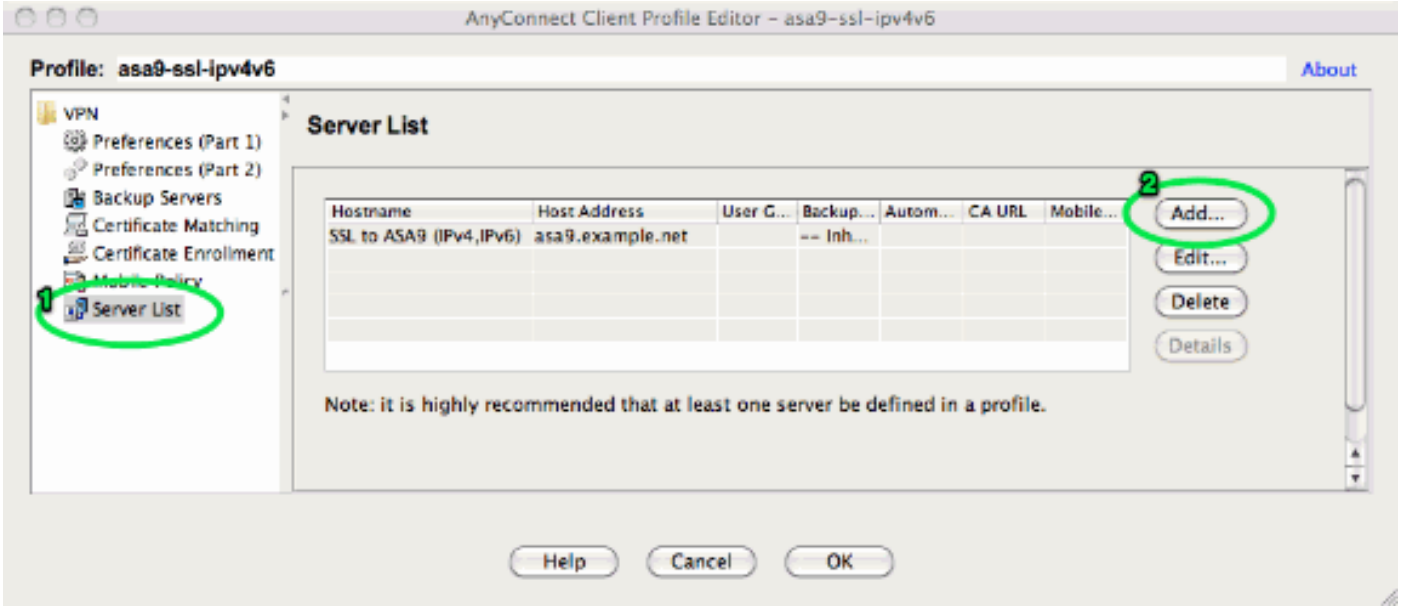
Configurare quindi uno o più gruppi di tunnel. Per questo esempio viene utilizzato quello predefinito (DefaultWEBVPNGroup) che viene configurato in modo da richiedere all'utente l'autenticazione tramite un certificato:

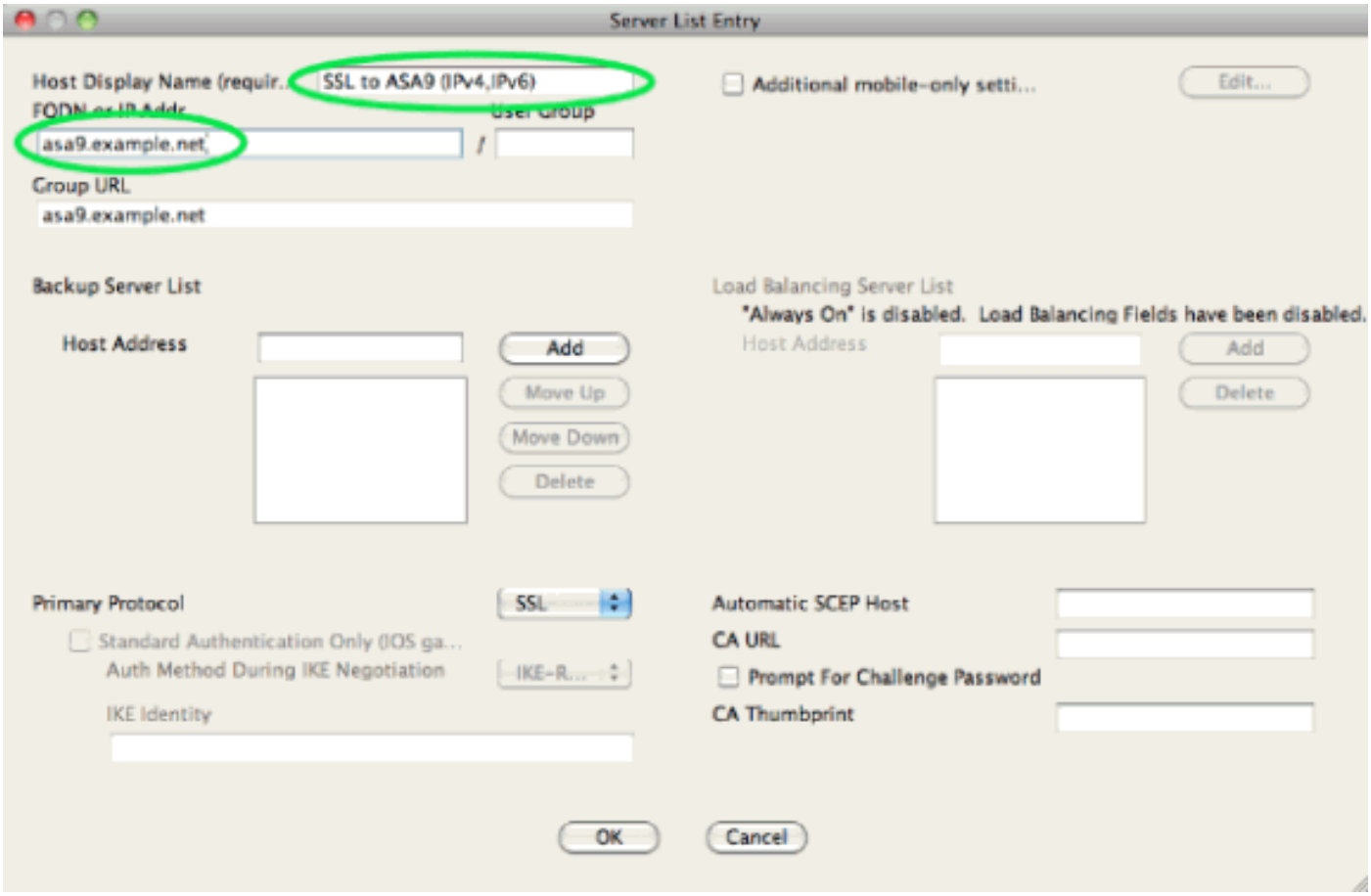
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

Per impostazione predefinita, il client AnyConnect tenta di connettersi tramite IPv4 e, solo se l'operazione non riesce, tenta di connettersi tramite IPv6. Tuttavia, questo comportamento può essere modificato da un'impostazione nel profilo XML. Il profilo AnyConnect "asa9-ssl-ipv4v6.xml" a cui si fa riferimento nella configurazione precedente, è stato generato utilizzando l'Editor profili in ASDM (Configurazione - VPN ad accesso remoto - Accesso di rete (client) - Profilo client 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



Profilo XML risultante (con la maggior parte della parte predefinita omessa per brevità):

```
<?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>
```

Nel profilo precedente vengono definiti anche un HostName (che può essere qualsiasi cosa, non deve necessariamente corrispondere al nome host effettivo dell'ASA) e un HostAddress (che in genere è il nome di dominio completo dell'ASA).

Nota: il campo HostAddress può essere lasciato vuoto, ma il campo HostName deve contenere il

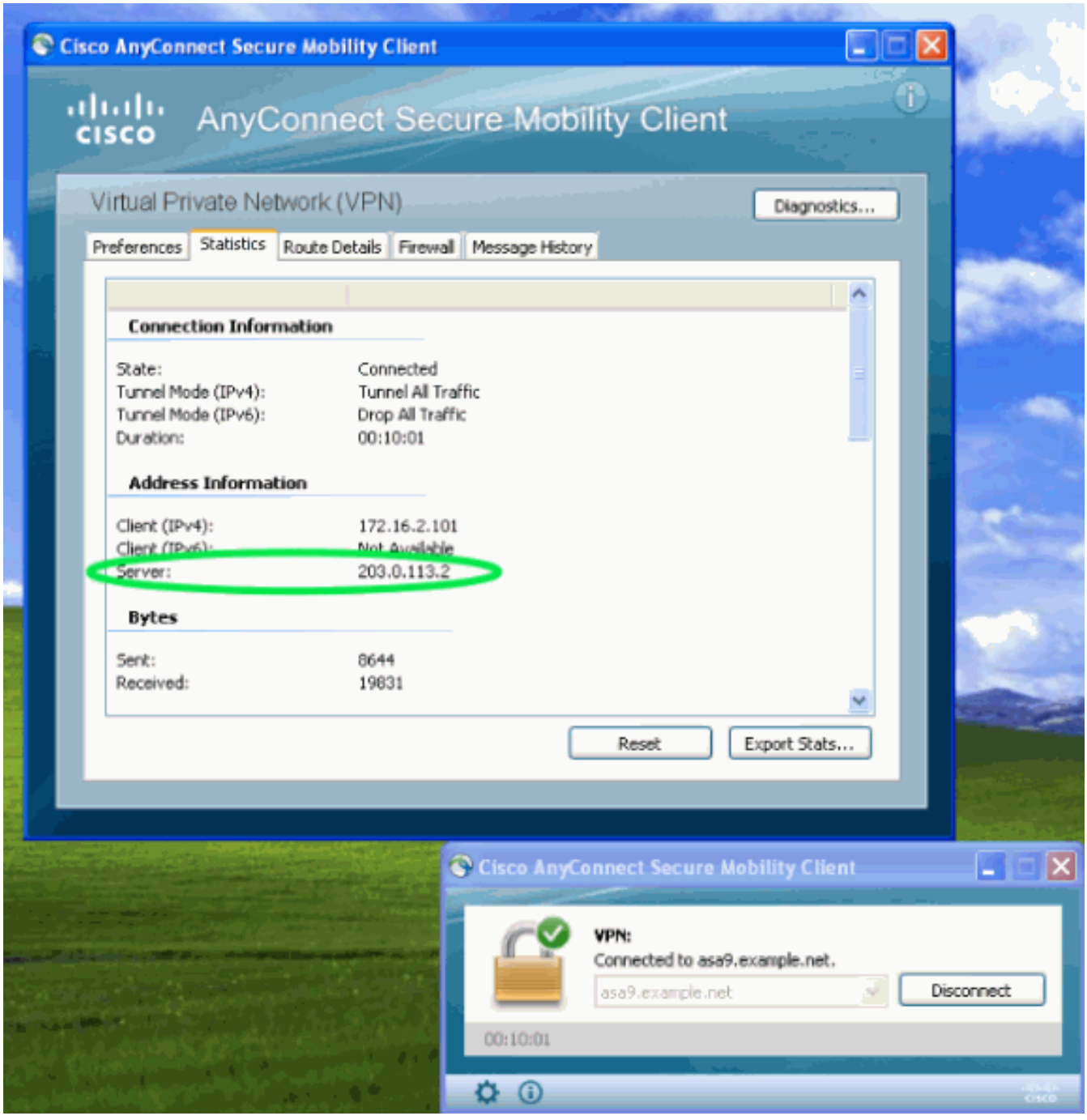
nome di dominio completo (FQDN) dell'ASA.

Nota: a meno che il profilo non sia pre-distribuito, la prima connessione richiede l'immissione del nome di dominio completo (FQDN) dell'ASA. Questa connessione iniziale preferirà IPv4. Dopo la connessione, il profilo verrà scaricato. Le impostazioni del profilo verranno quindi applicate.

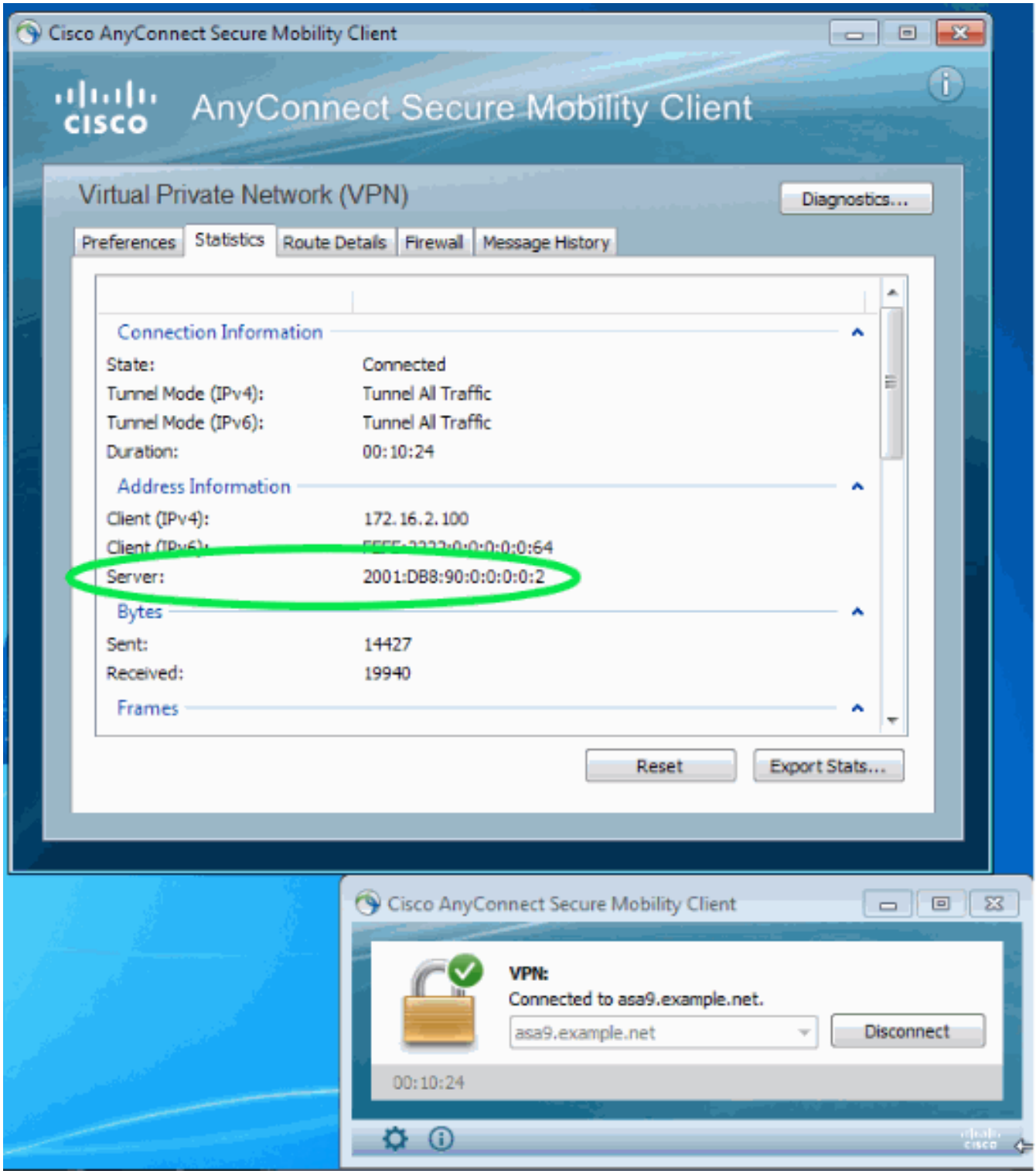
Verifica

Per verificare se un client è connesso tramite IPv4 o IPv6, controllare l'interfaccia utente del client o il database della sessione VPN sull'appliance ASA:

- Sul client, aprire la finestra Avanzate, andare alla scheda Statistiche e verificare l'indirizzo IP del "Server".Questo primo utente si connette da un sistema Windows XP senza supporto per IPv6:



Questo secondo utente si connette da un host Windows 7 con connettività IPv6 all'appliance ASA:



- Sull'appliance ASA, dalla CLI selezionare "Public IP" nell'output "show vpn-sessiondb anyconnect". In questo esempio vengono visualizzate le stesse due connessioni descritte sopra: una da XP su IPv4 e una da Windows 7 su 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
```

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems