SSL d'AnyConnect au-dessus d'IPv4+IPv6 à la configuration ASA

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour l'appliance de sécurité adaptable Cisco (ASA) pour permettre au Client à mobilité sécurisé Cisco AnyConnect (désigné sous le nom de « AnyConnect » dans le reste de ce document) pour établir un tunnel de VPN SSL au-dessus d'un réseau d'ipv4 ou d'IPv6.

En outre, cette configuration permet au client pour passer le trafic d'ipv4 et d'IPv6 au-dessus du tunnel.

Conditions préalables

Conditions requises

Afin d'établir avec succès un tunnel SSLVPN au-dessus d'IPv6, répondez à ces exigences :

- La Connectivité de bout en bout d'IPv6 est exigée
- La version d'AnyConnect doit être 3.1 ou plus tard
- La version de logiciel ASA doit être 9.0 ou plus tard

Cependant, si l'un de ces exigences ne sont pas répondues, la configuration discutée dans ce document permettra toujours au client pour se connecter au-dessus de l'ipv4.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA 5505 avec la version de logiciel 9.0(1)

- Client sécurisé 3.1.00495 de mobilité d'AnyConnect sur le professionnel de Microsoft Windows XP (sans support d'IPv6)
- Client sécurisé 3.1.00495 de mobilité d'AnyConnect sur l'entreprise de Microsoft Windows 7 de 32 bits

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration

D'abord hors fonction, définissez un groupe d'adresses IP desquelles vous assignerez un à chaque client qui se connecte.

Si vous voulez que le client porte également le trafic d'IPv6 au-dessus du tunnel, vous aurez besoin d'un groupe d'adresses d'IPv6. Les deux groupes sont mis en référence plus tard dans la stratégie de groupe.

```
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
```

Pour la Connectivité d'IPv6 à l'ASA, vous avez besoin d'un ipv6 addres sur l'interface à la laquelle les clients se connecteront (typiquement l'interface extérieure).

Pour la Connectivité d'IPv6 au-dessus du tunnel aux hôtes internes, vous avez besoin de l'IPv6 sur l'interface interne aussi bien.

```
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
```

Pour l'IPv6, vous avez besoin également d'un default route indiquant le routeur du prochain saut vers l'Internet.

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

Afin de s'authentifier aux clients, l'ASA doit avoir un certificat d'identité. Les instructions sur la façon dont créer ou importer un tel certificat sont hors de portée de ce document, mais peuvent être facilement trouvées dans d'autres documents comme

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

La configuration en résultant devrait sembler semblable à ce qui suit :

```
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
```

Puis, demandez à l'ASA pour utiliser ce certificat pour le SSL :

```
ssl trust-point testCA
```

Est ensuite la configuration de base du webvpn (SSLVPN) où la caractéristique est activée sur l'interface extérieure. Des modules de client qui sont disponibles pour le téléchargement sont définis, et nous définissent un profil est définis (plus sur ceci plus tard) :

```
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
```

Dans cet exemple de base, l'ipv4 et des groupes d'ipv6 addres sont configurés, les informations de serveur de DNS (qui seront poussées au client) et un profil dans la stratégie de groupe par défaut (DfltGrpPolicy). Beaucoup plus d'attributs peuvent être configurés ici, et sur option vous pouvez définir différentes stratégies de groupe pour différents ensembles d'utilisateurs.

Note: L'attribut « passerelle-FQDN » est nouveau dans la version 9.0 et définit le FQDN de l'ASA car on le connaît dans les DN. Le client apprend ce FQDN de l'ASA et l'utilisera en errant d'un ipv4 à un réseau d'IPv6 ou vice versa.

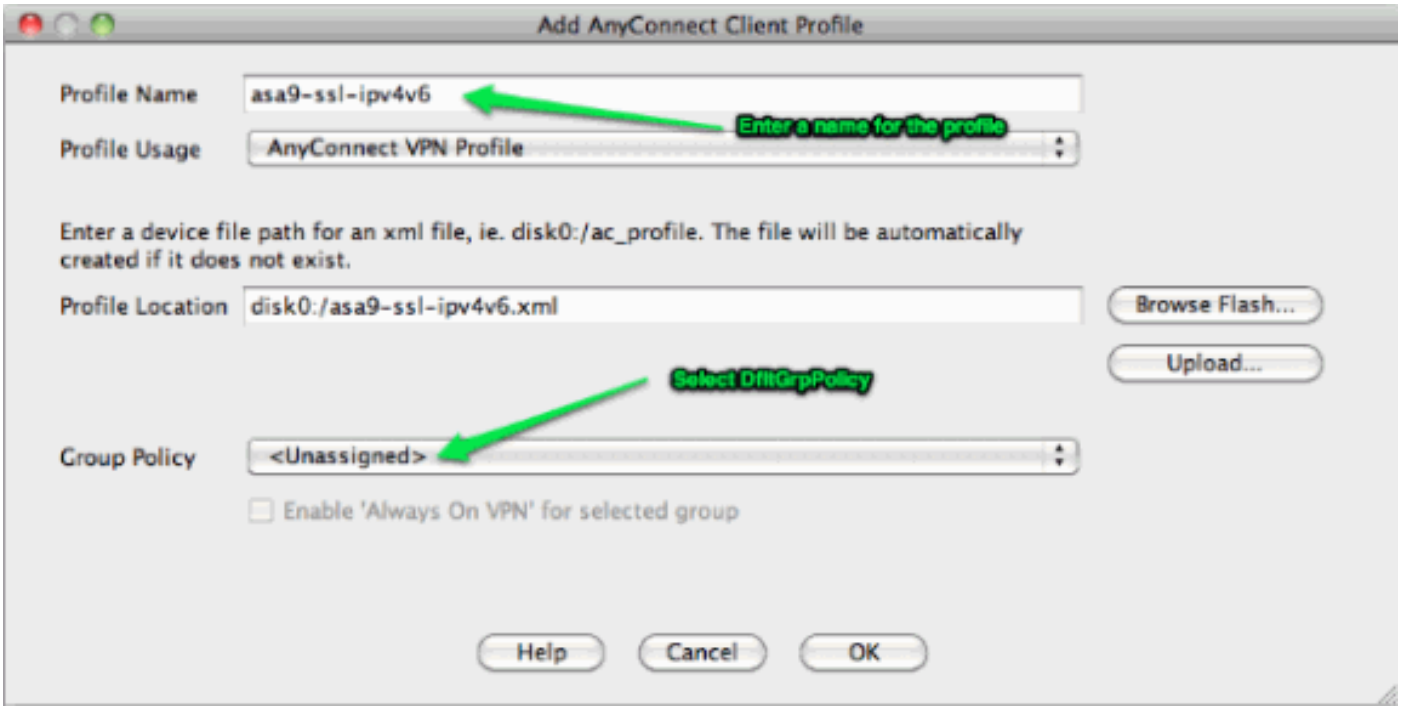
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

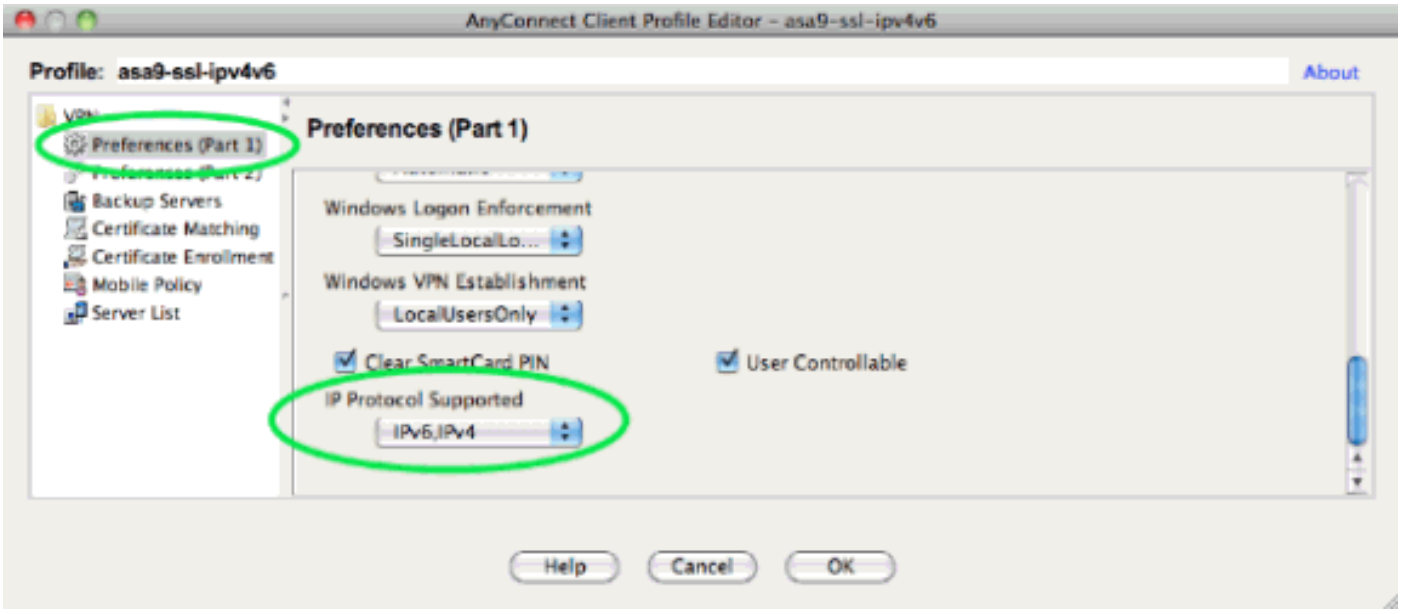
Ensuite, configurez un ou plusieurs groupes de tunnels. Le par défaut (DefaultWEBVPNGroup) est utilisé pour cet exemple, et le configure pour exiger de l'utilisateur d'authentifier utilisant un certificat :

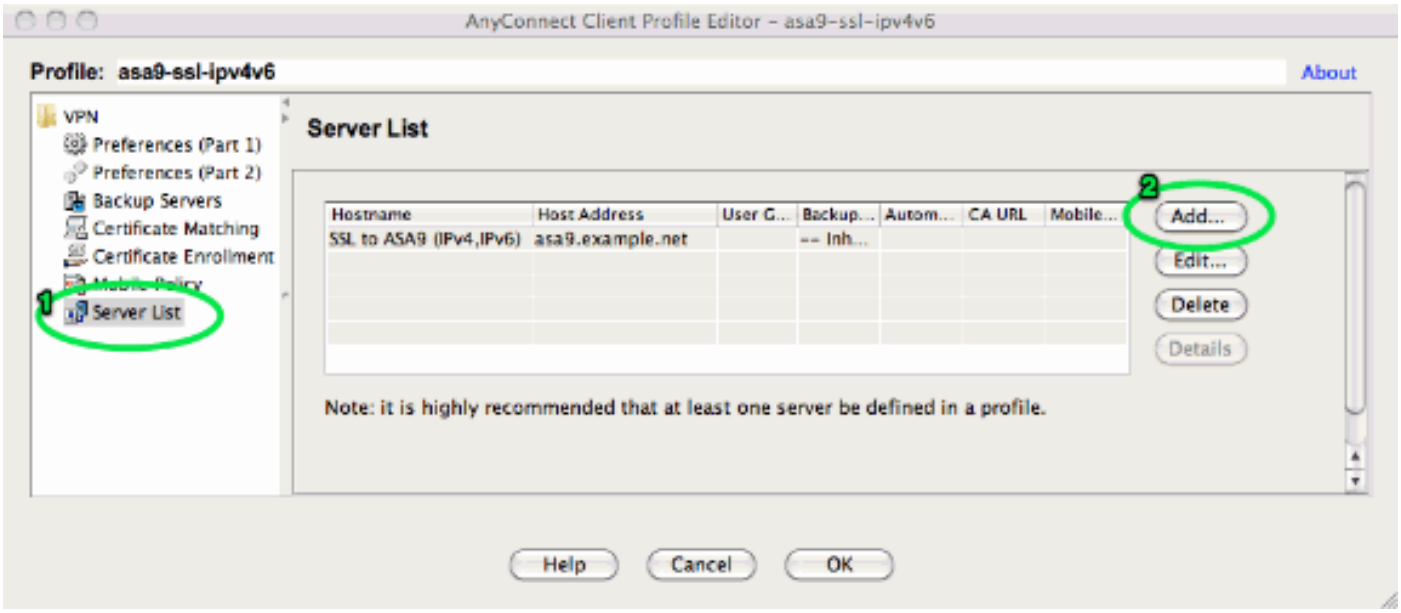
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

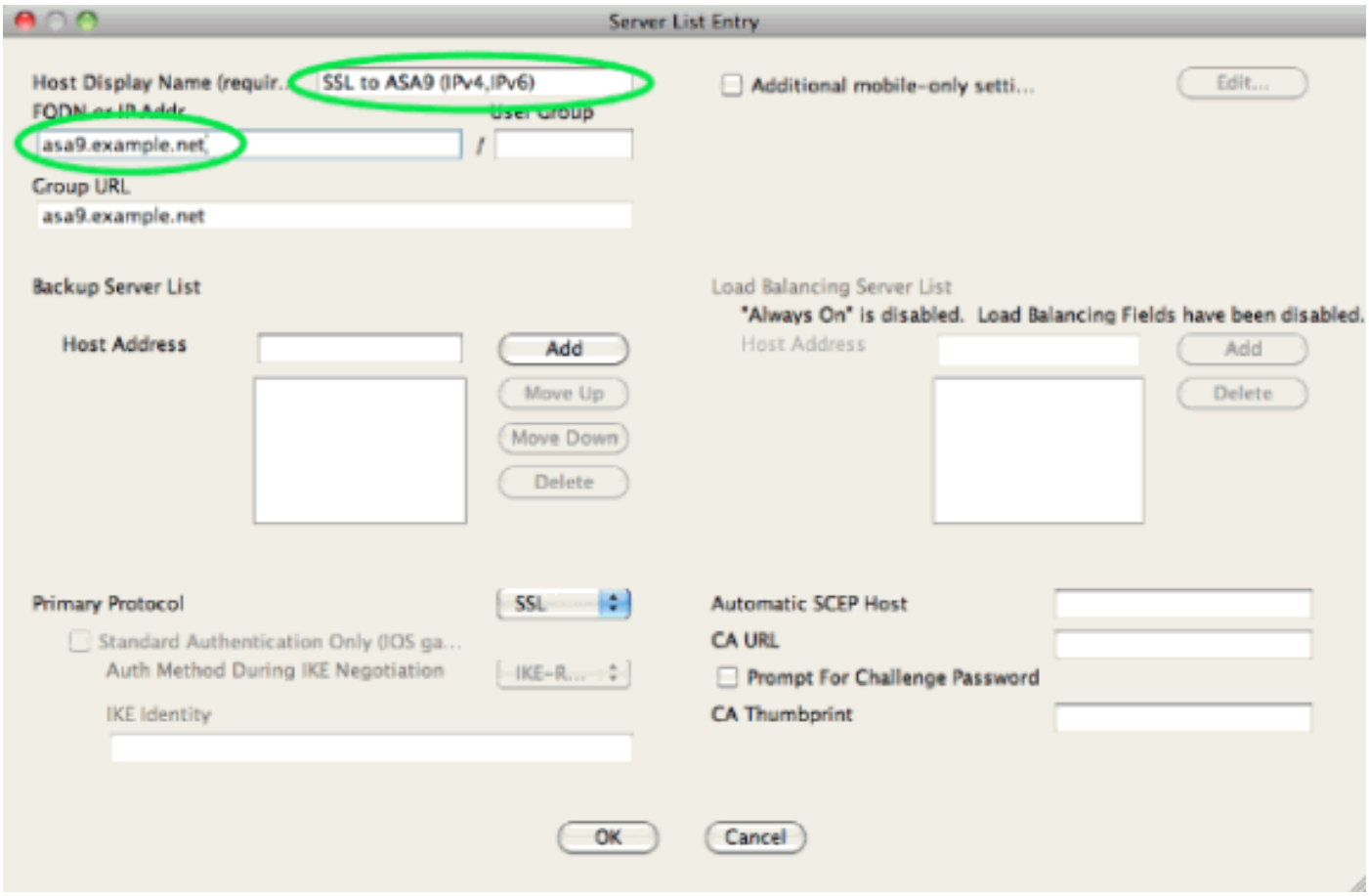
Par défaut, les tentatives de client d'AnyConnect de se connecter au-dessus de l'ipv4 et, seulement si ceci échoue, lui tente de se connecter au-dessus de l'IPv6. Cependant, ce

comportement peut être changé par une configuration dans le profil XML. Le "asa9-SSL-ipv4v6.xml" de profil d'AnyConnect qui est mis en référence dans la configuration ci-dessus, a été généré utilisant l'éditeur de profil dans ASDM (configuration - réseau VPN d'Accès à distance (client) profil de client d'Acccess - d'AnyConnect).









Le profil en résultant XML (avec la majeure partie de la partie par défaut omise par souci de concision) :

```
<?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>
```

Dans le profil ci-dessus une adresse Internet est également définie (qui peuvent être quelque chose, elle n'a pas besoin d'apparier l'adresse Internet réelle de l'ASA), et un host address (qui est typiquement le FQDN de l'ASA).

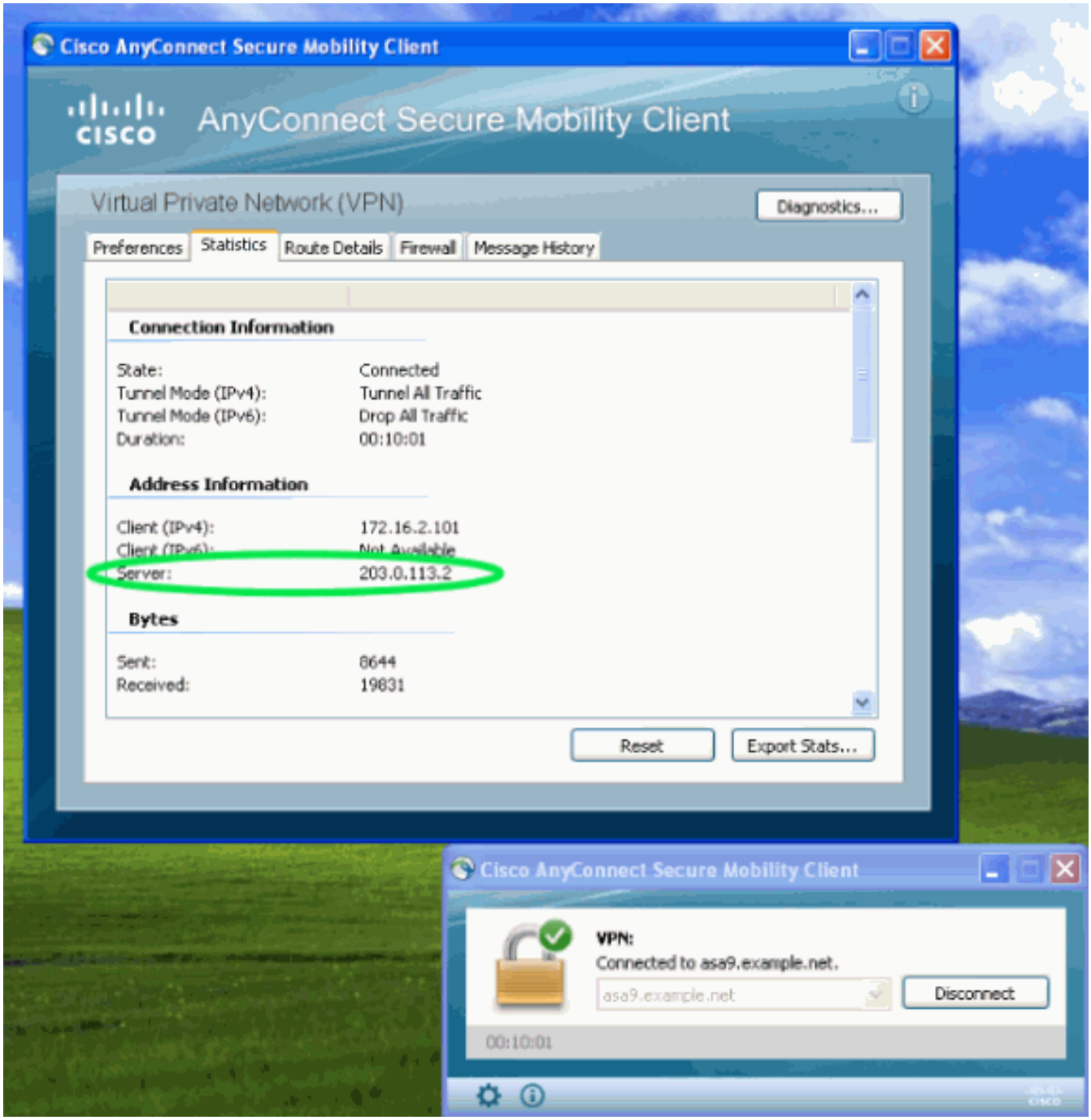
Note: Le champ de host address peut être parti vide, mais le champ d'adresse Internet doit contenir le FQDN de l'ASA.

Note: À moins que le profil soit déployé à l'avance, la première connexion exige de l'utilisateur de saisir le FQDN de l'ASA. Cette connexion initiale préférera l'ipv4. Après la connexion réussie, le profil sera téléchargé. De là, les paramètres de profil seront appliqués.

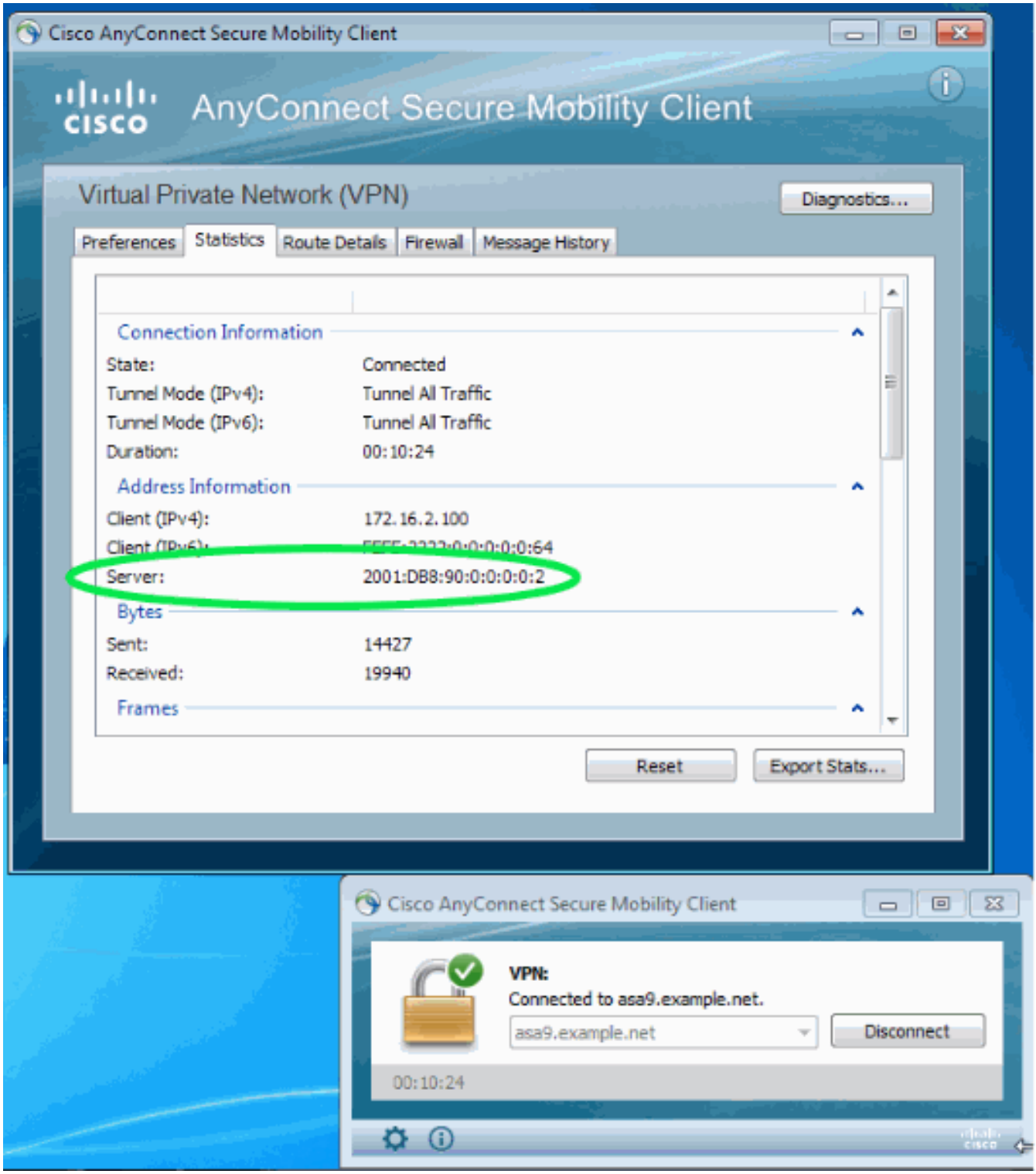
Vérifiez

Afin de vérifier si un client est connecté au-dessus de l'ipv4 ou de l'IPv6, vérifiez le GUI de client ou le DB de session VPN sur l'ASA :

- Sur le client, ouvrez la fenêtre avancée, allez à l'onglet de statistiques et vérifiez l'adresse IP du « serveur ».Cet premier utilisateur se connecte d'un système Windows XP sans support d'IPv6
  :



Cet deuxième utilisateur se connecte d'un hôte de Windows 7 à la Connectivité d'IPv6 à l'ASA :



- Sur l'ASA, du contrôle CLI « IP de public » dans la sortie « d'anyconnect de VPN-sessiondb d'exposition ». Dans cet exemple vous pouvez voir les mêmes deux connexions comme ci-dessus : un du XP au-dessus de l'ipv4 et un du Windows 7 au-dessus de l'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
```

Informations connexes

- Support et documentation techniques - Cisco Systems