Configuration d'AnyConnect SSL sur IPv4+IPv6 vers ASA

Contenu

Introduction

Ce document fournit un exemple de configuration pour le dispositif de sécurité adaptatif Cisco (ASA) afin de permettre au client de mobilité sécurisée Cisco AnyConnect (appelé « AnyConnect » dans le reste de ce document) d'établir un tunnel VPN SSL sur un réseau IPv4 ou IPv6.

En outre, cette configuration permet au client de transmettre le trafic IPv4 et IPv6 via le tunnel.

Conditions préalables

Conditions requises

Afin d'établir avec succès un tunnel SSLVPN sur IPv6, répondez aux conditions suivantes :

- Une connectivité IPv6 de bout en bout est requise
- La version AnyConnect doit être 3.1 ou ultérieure
- La version du logiciel ASA doit être 9.0 ou ultérieure

Cependant, si l'une de ces conditions n'est pas remplie, la configuration décrite dans ce document permettra toujours au client de se connecter via IPv4.

Components Used

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

- ASA-5505 avec la version 9.0(1) du logiciel
- AnyConnect Secure Mobility Client 3.1.00495 sur Microsoft Windows XP Professionnel (sans prise en charge IPv6)

- AnyConnect Secure Mobility Client 3.1.00495 sur Microsoft Windows 7 Entreprise 32 bits

Conventions

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

Configuration

Tout d'abord, définissez un pool d'adresses IP à partir duquel vous attribuerez une adresse à chaque client qui se connecte.

Si vous voulez que le client transporte également le trafic IPv6 via le tunnel, vous aurez besoin d'un pool d'adresses IPv6. Les deux pools sont référencés ultérieurement 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 IPv6 à l'ASA, vous avez besoin d'une adresse IPv6 sur l'interface à laquelle les clients se connecteront (généralement l'interface externe).

Pour la connectivité IPv6 via le tunnel vers les hôtes internes, vous avez également besoin d'IPv6 sur les interfaces internes.

```
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 IPv6, vous avez également besoin d'une route par défaut pointant vers le routeur du tronçon suivant vers Internet.

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

Pour s'authentifier auprès des clients, l'ASA doit disposer d'un certificat d'identité. Les instructions relatives à la création ou à l'importation d'un tel certificat ne relèvent pas de ce document, mais elles peuvent être facilement trouvées dans d'autres documents tels que

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

La configuration résultante doit être similaire à celle-ci :

```
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
```

Ensuite, demandez à l'ASA d'utiliser ce certificat pour SSL :

```
ssl trust-point testCA
```

La configuration de base de WebVPN (SSLVPN) est maintenant activée sur l'interface externe. Les packages clients qui peuvent être téléchargés sont définis, et nous définissons un profil (plus d'informations plus loin) :

```
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, les pools d'adresses IPv4 et IPv6 sont configurés, les informations du serveur DNS (qui seront transmises au client) et un profil dans la stratégie de groupe par défaut (DfltGrpPolicy). De nombreux autres attributs peuvent être configurés ici, et vous pouvez éventuellement définir différentes stratégies de groupe pour différents ensembles d'utilisateurs.

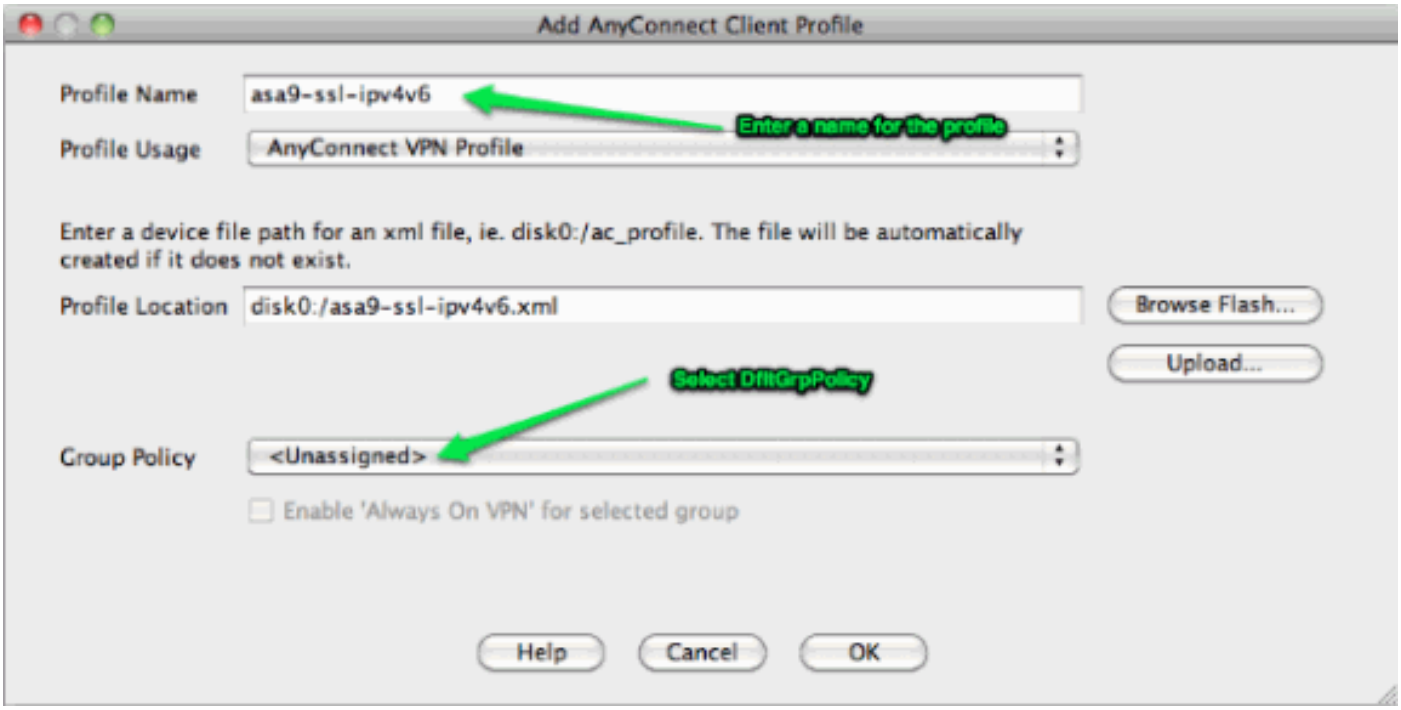
Remarque : L'attribut « gateway-fqdn » est nouveau dans la version 9.0 et définit le nom de domaine complet de l'ASA tel qu'il est connu dans le DNS. Le client apprend ce nom de domaine complet à partir de l'ASA et l'utilisera lors de l'itinérance d'un réseau IPv4 vers un réseau IPv6 ou vice versa.

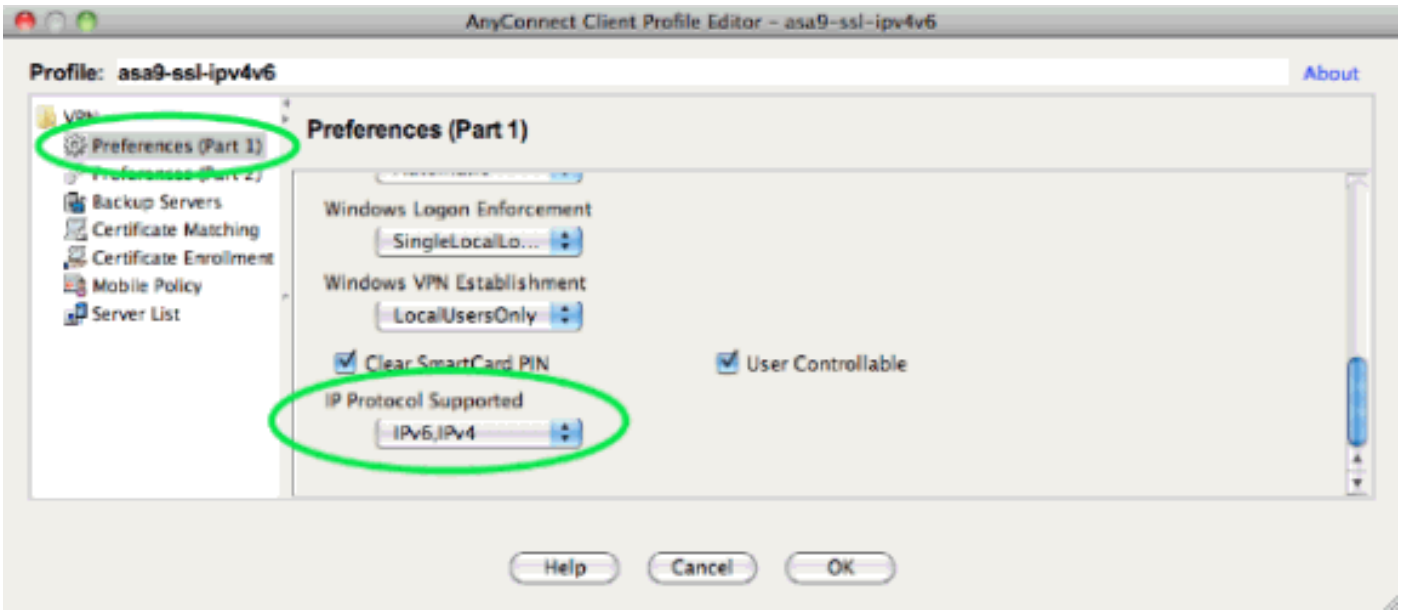
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

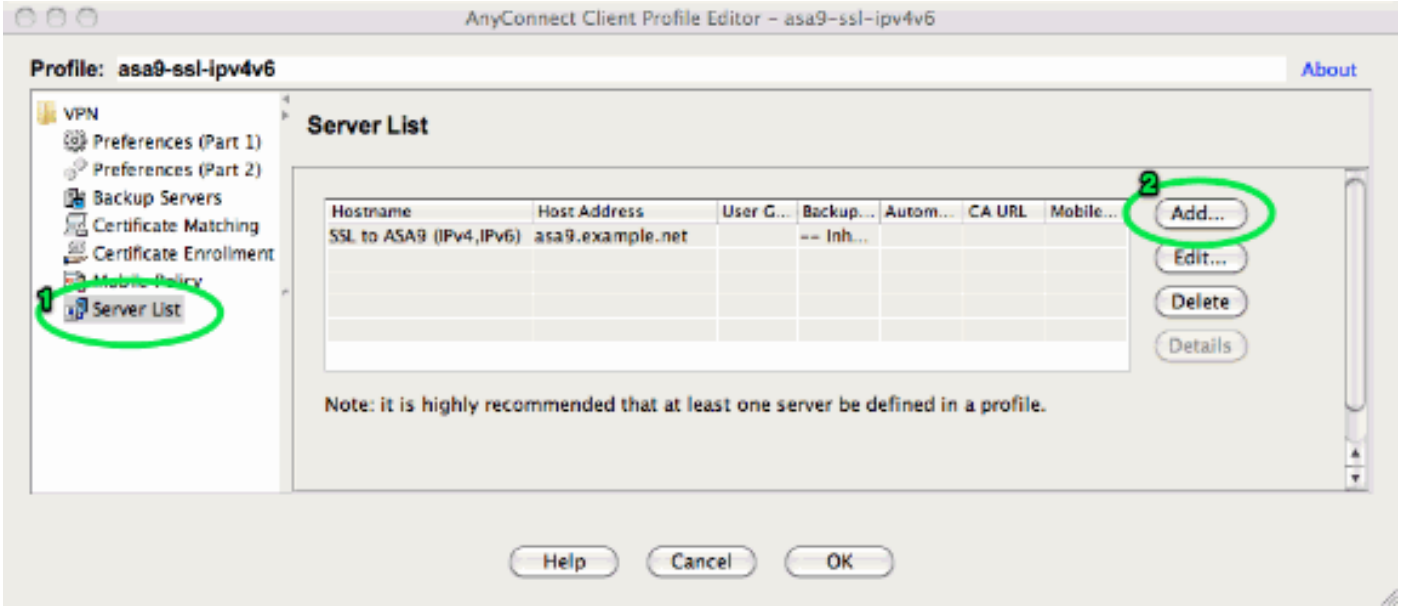
Configurez ensuite un ou plusieurs groupes de tunnels. La valeur par défaut (DefaultWEBVPNGroup) est utilisée pour cet exemple et la configurez pour exiger de l'utilisateur qu'il s'authentifie à l'aide d'un certificat :

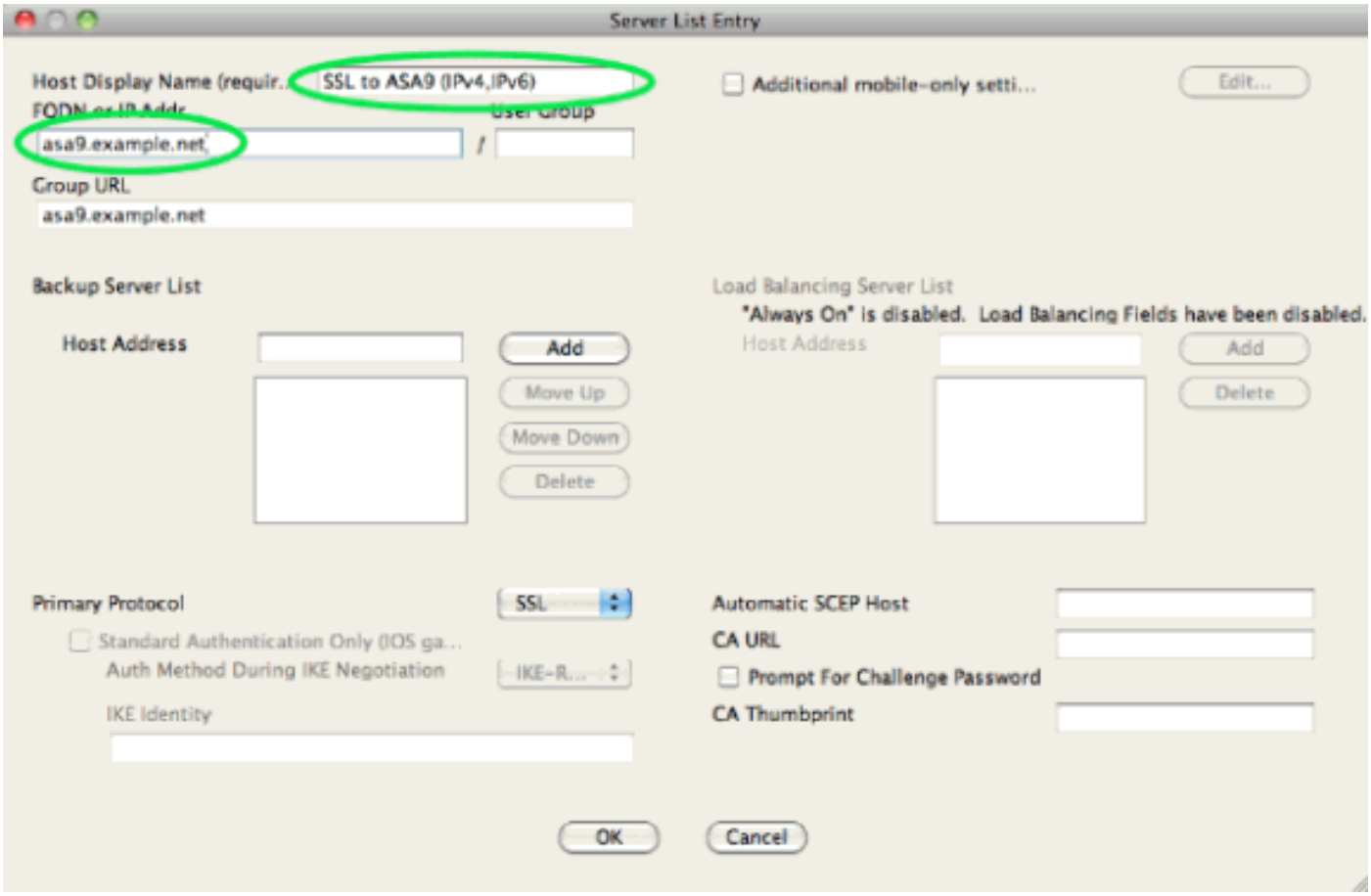
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

Par défaut, le client AnyConnect tente de se connecter sur IPv4 et, si cela échoue, il tente de se connecter sur IPv6. Cependant, ce comportement peut être modifié par un paramètre du profil XML. Le profil AnyConnect « asa9-ssl-ipv4v6.xml » référencé dans la configuration ci-dessus, a été généré à l'aide de l'Éditeur de profil dans ASDM (Configuration - Remote Access VPN - Network (Client) Access - AnyConnect Client Profile).


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



Le profil XML résultant (la plupart de la partie par défaut étant omise pour plus 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>
 ...
```

```
 ...
</ClientInitialization>
 <ServerList>
 <HostEntry>
```

```
       </HostEntry> </ServerList>
</AnyConnectProfile>
```

Dans le profil ci-dessus, un HostName est également défini (qui peut être n'importe quoi, il n'a pas besoin de correspondre au nom d'hôte réel de l'ASA) et un HostAddress (qui est généralement le FQDN de l'ASA).

Remarque : le champ HostAddress peut rester vide, mais le champ HostName doit contenir le

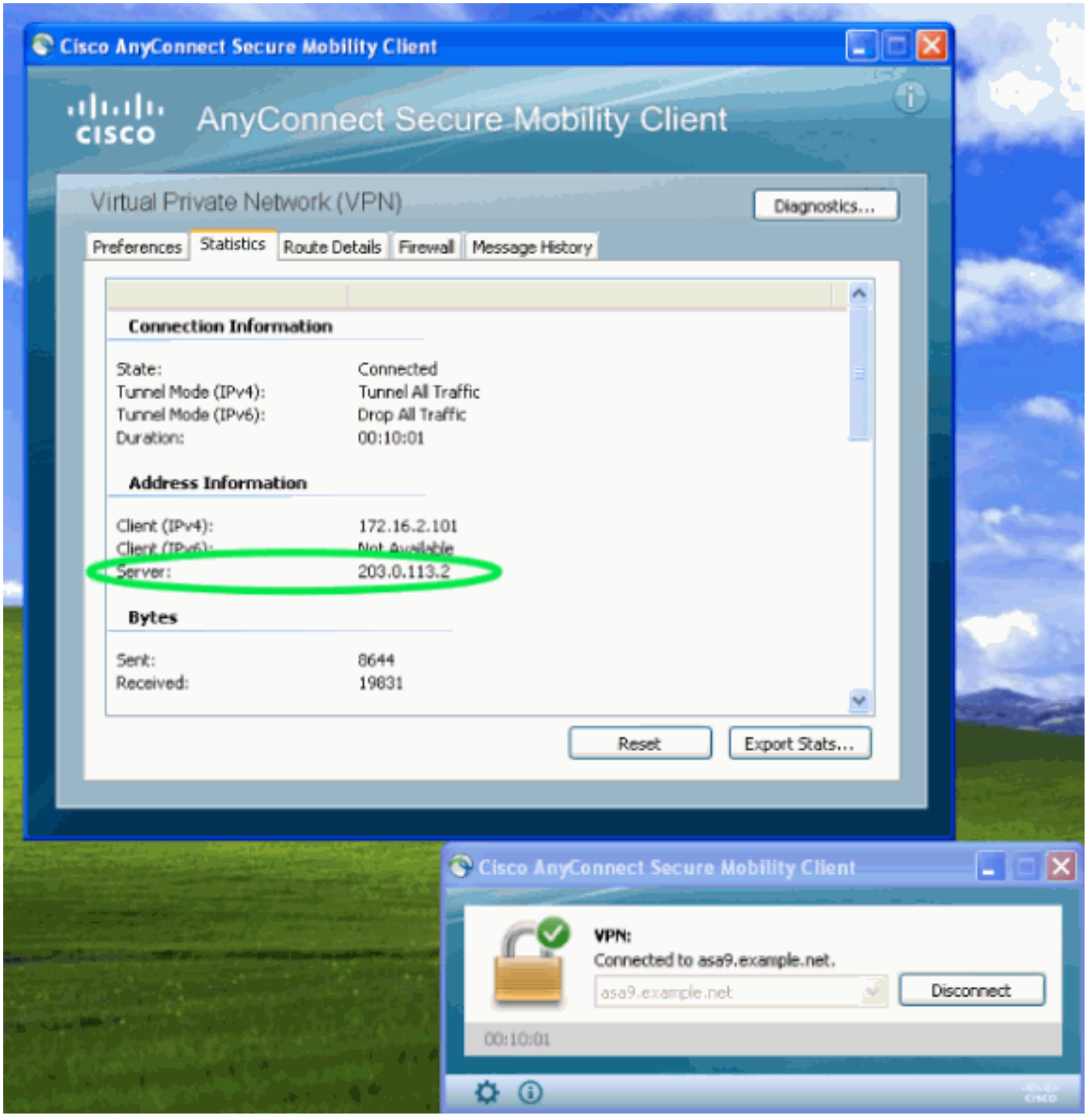
nom de domaine complet de l'ASA.

Remarque : à moins que le profil ne soit pré-déployé, la première connexion nécessite que l'utilisateur saisisse le nom de domaine complet de l'ASA. Cette connexion initiale préfère IPv4. Une fois la connexion établie, le profil est téléchargé. À partir de là, les paramètres de profil seront appliqués.

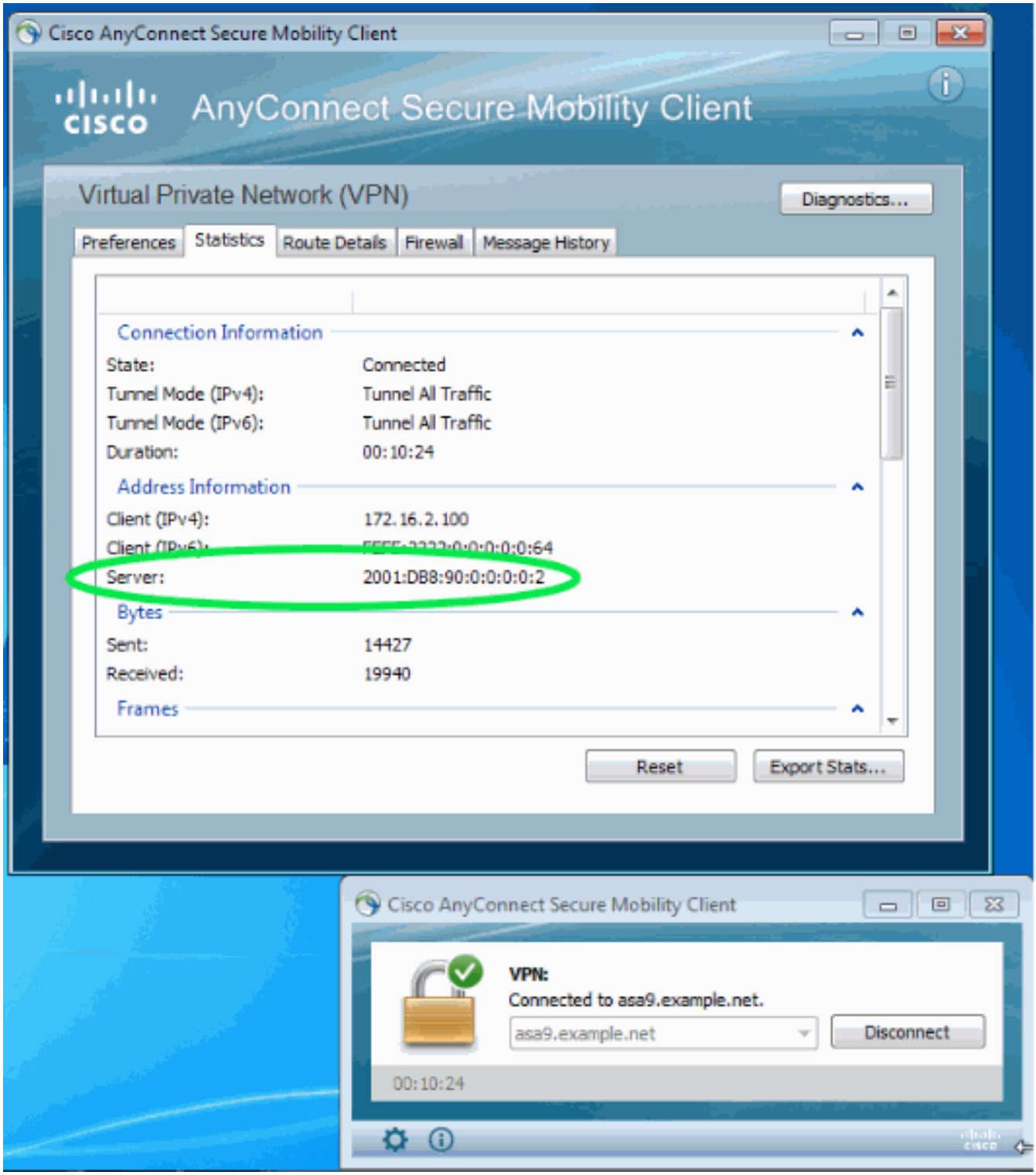
Vérification

Afin de vérifier si un client est connecté sur IPv4 ou IPv6, vérifiez l'interface utilisateur graphique du client ou la base de données de session VPN sur l'ASA :

- Sur le client, ouvrez la fenêtre Avancé, accédez à l'onglet Statistiques et vérifiez l'adresse IP du « Serveur ».Ce premier utilisateur se connecte à partir d'un système Windows XP sans prise en charge IPv6
:



Ce second utilisateur se connecte à partir d'un hôte Windows 7 avec une connectivité IPv6 à l'ASA
:



- Sur l'ASA, à partir de l'interface de ligne de commande, vérifiez l'adresse IP publique dans la sortie « show vpn-sessiondb anyconnect ». Dans cet exemple, vous pouvez voir les deux mêmes connexions que ci-dessus : un de XP sur IPv4 et un de Windows 7 sur 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