AnyConnect SSL over IPv4+IPv6 to ASA 컨피그레이션

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)의 샘플 컨피그레이션을 통해 Cisco AnyConnect Secure Mobility Client(이하 이 문서의 나머지 부분에서는 "AnyConnect"라 함)가 IPv4 또는 IPv6 네트워크를 통해 SSL VPN 터널을 설정할 수 있도록 합니다.

또한 이 컨피그레이션을 통해 클라이언트가 터널을 통해 IPv4 및 IPv6 트래픽을 전달할 수 있습니다.

사전 요구 사항

요구 사항

IPv6를 통해 SSLVPN 터널을 성공적으로 설정하려면 다음 요구 사항을 충족해야 합니다.

- 엔드 투 엔드 IPv6 연결이 필요합니다.
- AnyConnect 버전은 3.1 이상이어야 합니다.
- ASA 소프트웨어 버전은 9.0 이상이어야 합니다.

그러나 이러한 요구 사항 중 하나라도 충족되지 않으면 이 문서에서 설명한 컨피그레이션을 통해 클라이언트가 IPv4를 통해 계속 연결할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 9.0(1)이 포함된 ASA-5505
- Microsoft Windows XP Professional의 AnyConnect Secure Mobility Client 3.1.00495(IPv6를 지원하지 않음)

- Microsoft Windows 7 Enterprise 32비트의 AnyConnect Secure Mobility Client 3.1.00495

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

먼저 연결되는 각 클라이언트에 IP 주소 풀을 지정합니다.

클라이언트가 터널을 통해 IPv6 트래픽을 전달하도록 하려면 IPv6 주소 풀이 필요합니다.두 풀 모두 나중에 그룹 정책에서 참조됩니다.

```
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
```

ASA에 대한 IPv6 연결의 경우 클라이언트가 연결할 인터페이스(일반적으로 외부 인터페이스)에 IPv6 주소가 필요합니다.

터널을 통해 내부 호스트로의 IPv6 연결의 경우 내부 인터페이스에서도 IPv6가 필요합니다.

```
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
```

IPv6의 경우 인터넷을 향해 next-hop 라우터를 가리키는 기본 경로가 필요합니다.

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

클라이언트에 자신을 인증하려면 ASA에 ID 인증서가 있어야 합니다.이러한 인증서를 만들거나 가져오는 방법에 대한 지침은 이 문서의 범위를 벗어납니다. 그러나 다른 문서(예:

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

결과 컨피그레이션은 다음과 비슷해야 합니다.

```
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
```
그런 다음 ASA에 이 인증서를 SSL에 사용하도록 지시합니다.

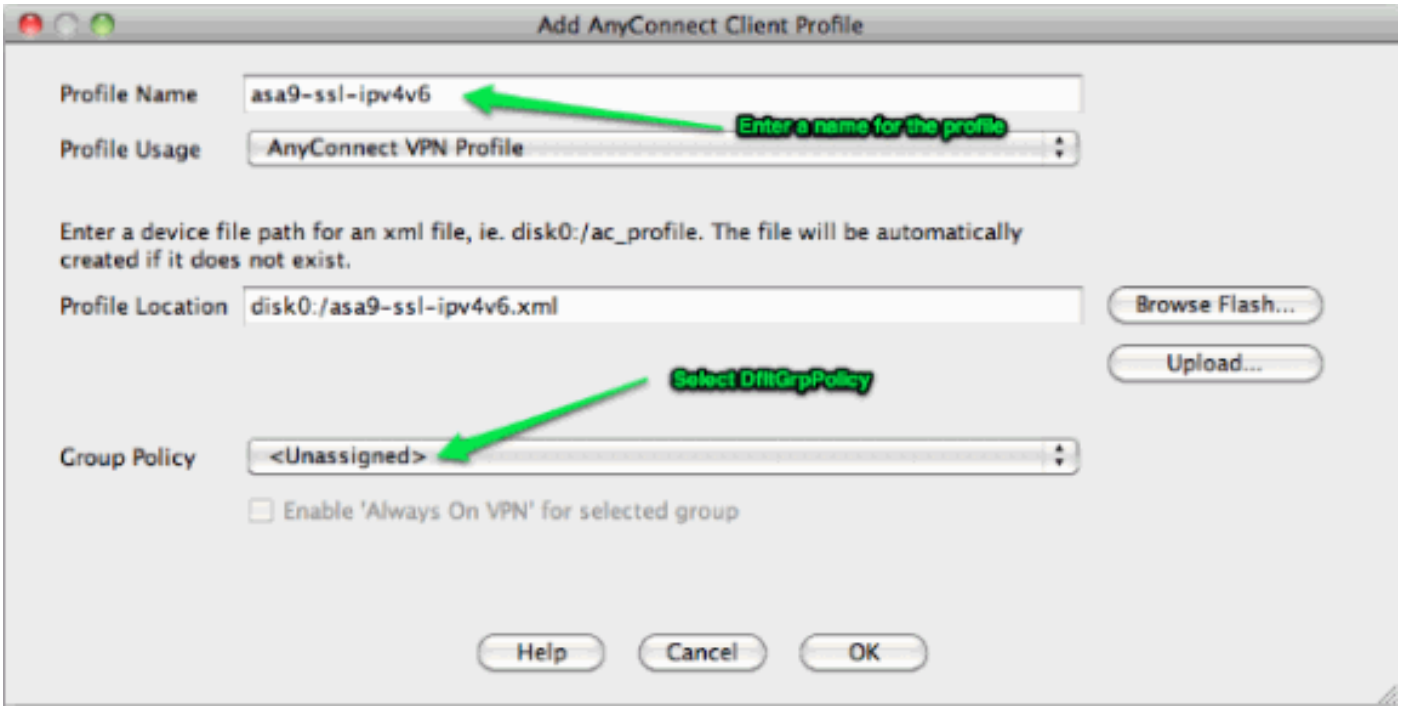
```
ssl trust-point testCA
```
다음은 기본 SSLVPN(webvpn) 컨피그레이션입니다. 이 컨피그레이션은 외부 인터페이스에서 활성화됩니다.다운로드할 수 있는 클라이언트 패키지가 정의되고, 프로파일이 정의됨(이 다음에 자세히 설명):

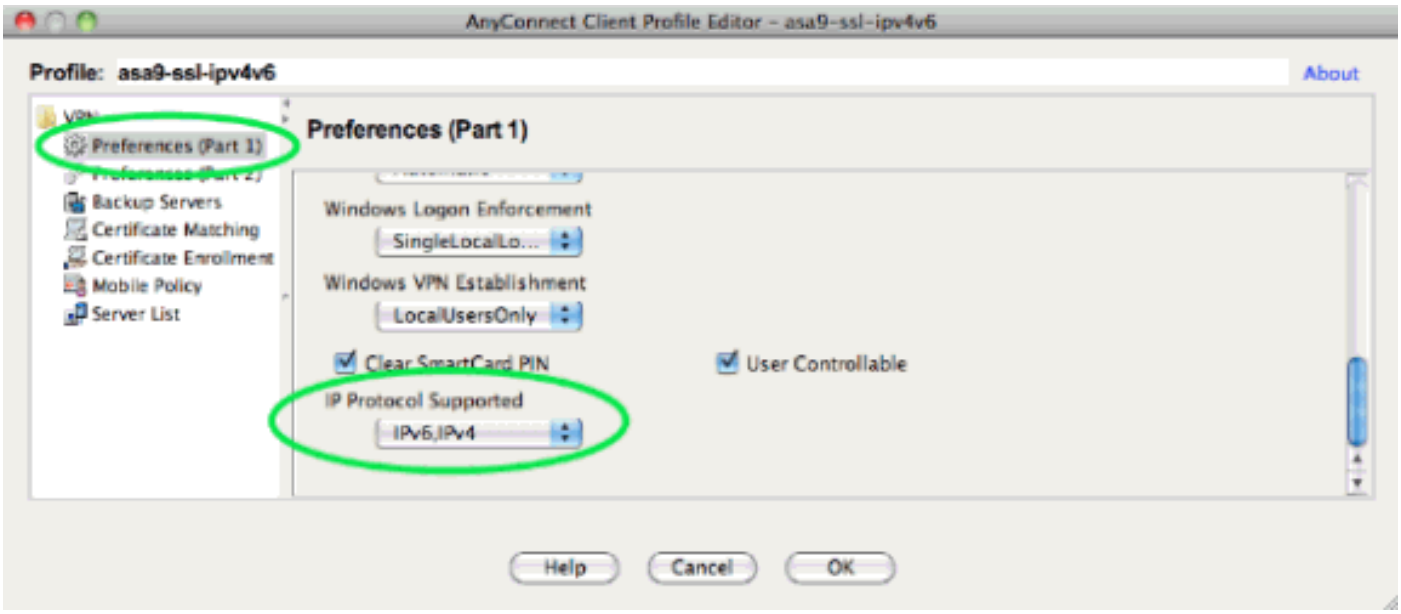
```
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
 anyconnect profiles asa9-ssl-ipv4v6 disk0:/asa9-ssl-ipv4v6.xml
 anyconnect enable
```
이 기본 예에서는 IPv4 및 IPv6 주소 풀이 구성되고, DNS 서버 정보(클라이언트에 푸시됨) 및 기본 그룹 정책(DfltGrpPolicy)의 프로필이 구성됩니다. 여기에서 더 많은 특성을 구성할 수 있으며, 선택적으로 여러 사용자 집합에 대해 다른 그룹 정책을 정의할 수 있습니다.

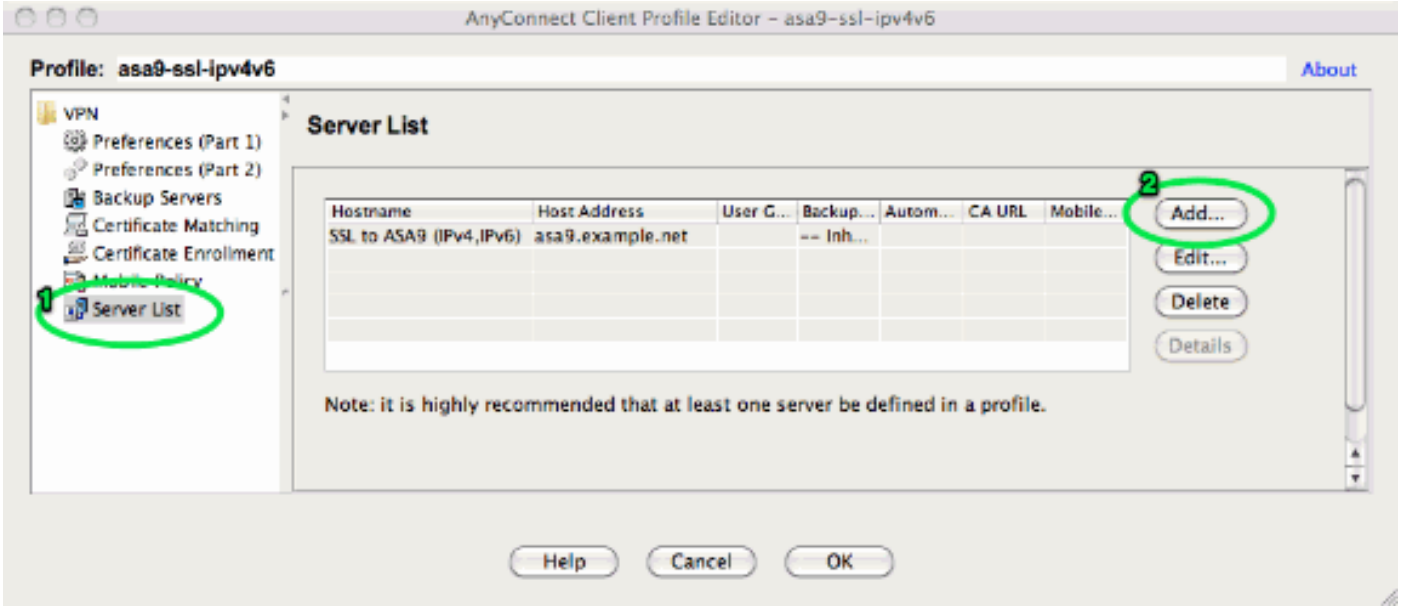
참고: "gateway-fqdn" 특성은 버전 9.0에 새로 추가되었으며 ASA의 FQDN을 DNS에 알려진 대로 정의합니다.클라이언트는 ASA에서 이 FQDN을 학습하고 IPv4에서 IPv6 네트워크로 또는 그 반대로 로밍할 때 이를 사용합니다.

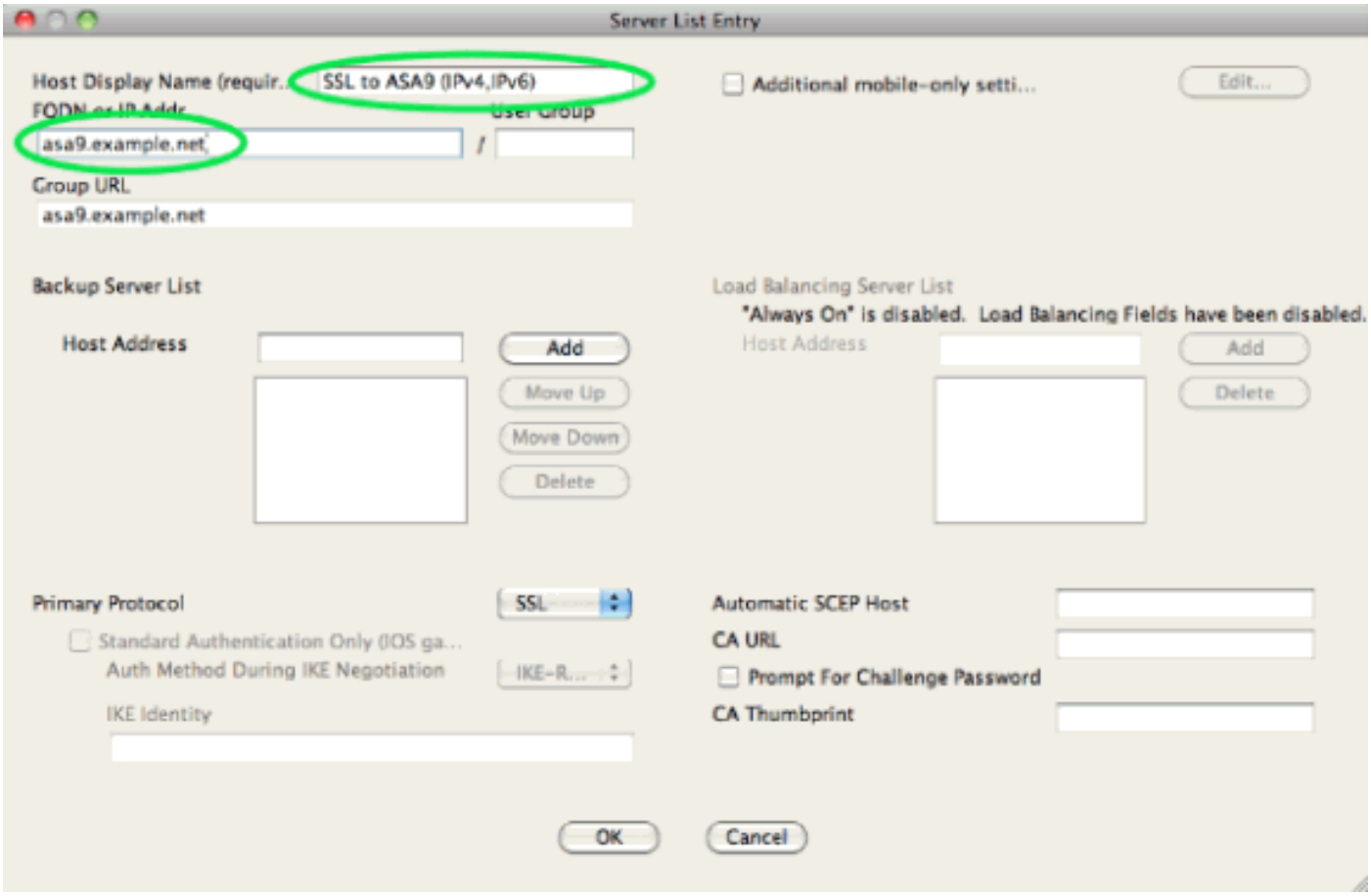
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```
그런 다음 하나 이상의 터널 그룹을 구성합니다.이 예에서는 기본(DefaultWEBVPNGroup)이 사용되며 사용자가 인증서를 사용하여 인증하도록 구성합니다.

```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```
기본적으로 AnyConnect 클라이언트는 IPv4를 통해 연결을 시도하며, 이 오류가 발생한 경우에만 IPv6를 통해 연결을 시도합니다. 그러나 XML 프로파일의 설정으로 이 동작을 변경할 수 있습니다 .위의 구성에서 참조되는 AnyConnect 프로파일 "asa9-ssl-ipv4v6.xml"은 ASDM의 프로파일 편집기(구성 - 원격 액세스 VPN - 네트워크(클라이언트) 액세스 - AnyConnect 클라이언트 프로파일)를 사용하여 생성되었습니다.


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



결과 XML 프로파일(대부분의 기본 부품은 생략됨):

```
<?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>
```

위의 프로필에서 HostName도 정의됩니다(무엇이든 될 수 있으며 ASA의 실제 호스트 이름과 일치하지 않아도 됨). HostAddress(일반적으로 ASA의 FQDN임).

참고: HostAddress 필드는 비워 둘 수 있지만 HostName 필드는 ASA의 FQDN을 포함해야 합니다.

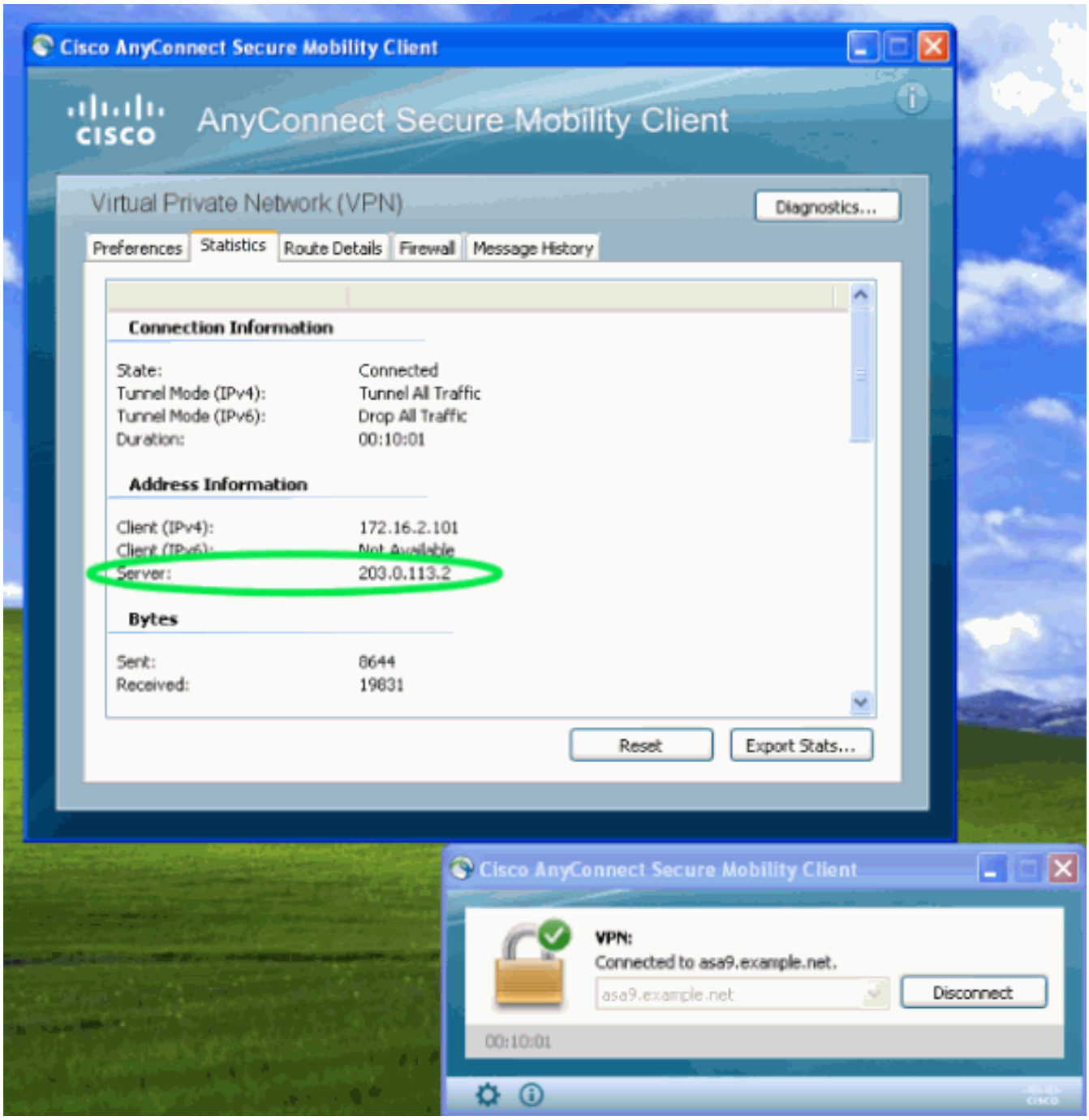
참고: 프로파일이 사전 구축되지 않은 경우 첫 번째 연결에서는 사용자가 ASA의 FQDN을 입력해야 합니다.이 초기 연결은 IPv4를 선호합니다. 연결이 성공하면 프로파일이 다운로드됩니다.여기에서 프로파일 설정이 적용됩니다.

다음을 확인합니다.

클라이언트가 IPv4 또는 IPv6를 통해 연결되었는지 확인하려면 ASA의 클라이언트 GUI 또는 VPN 세션 DB를 확인합니다.

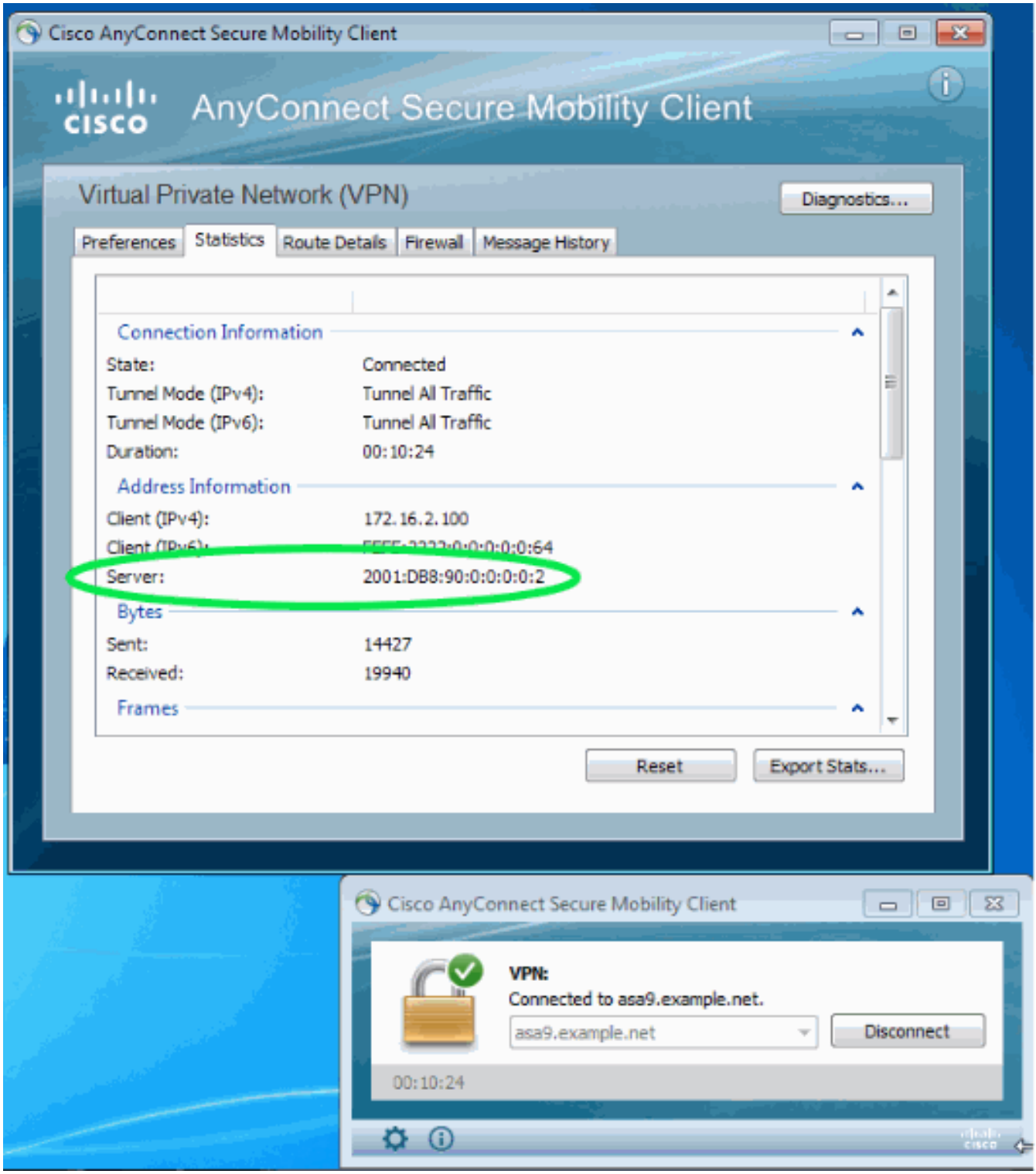
- 클라이언트에서 고급 창을 열고 통계 탭으로 이동하여 "서버"의 IP 주소를 확인합니다.이 첫 번째 사용자는 IPv6를 지원하지 않고 Windows XP 시스템에서 연결합니다

.



이 두 번째 사용자는 IPv6 연결이 설정된 Windows 7 호스트에서 ASA에 연결합니다

.



- ASA의 CLI에서 "show vpn-sessiondb anyconnect" 출력의 "Public IP"를 확인합니다.이 예에서는 위와 동일한 두 개의 연결을 볼 수 있습니다.IPv4를 통한 XP와 IPv6를 통한 Windows 7에서 하나씩

```
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
```

관련 정보

- 기술 지원 및 문서 – Cisco Systems