IPv4+IPv6 を介して ASA コンフィギュレーションに対する AnyConnect SSL

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[コンフィギュレーション](#)
[確認](#)
[関連情報](#)

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス (ASA) で、Cisco AnyConnect セキュア モビリティ クライアント (以降は「AnyConnect」と表記) が、IPv4 または IPv6 ネットワークを介した SSL VPN トンネルを確立できるようにするための設定例を示します。

さらに、この設定によりクライアントは、トンネルを介して IPv4 および IPv6 トラフィックを渡すことができるようになります。

前提条件

要件

IPv6 を介した SSLVPN トンネルを正常に確立できるようにするには、以下の要件を満たすようにします。

- IPv6 エンドツーエンド接続が必要です。
- AnyConnect のバージョンは、3.1 以降である必要があります。
- ASA ソフトウェアのバージョンは、9.0 以降である必要があります。

これらの要件のいずれかが満たされていない場合でも、このドキュメントで説明されている設定により、クライアントは IPv4 を介した接続が可能です。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASA-5505 ソフトウェアのバージョン 9.0(1)

- Microsoft Windows XP Professional 上の AnyConnect セキュア モビリティ クライアント 3.1.00495（IPv6 サポートなし）
- Microsoft Windows 7 Enterprise 32 ビット上の AnyConnect セキュア モビリティ クライアント 3.1.00495

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

コンフィギュレーション

まず、接続する各クライアントへの IP アドレスの割り当て元になる、IP アドレスのプールを定義します。

クライアントにトンネルを介して IPv6 トラフィックを送信させる場合は、IPv6 アドレスのプールが必要になります。どちらのプールも、後からグループ ポリシー内で参照されます。

```
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
```

ASA への IPv6 接続の場合、クライアントが接続するインターフェイス（通常は外部インターフェイス）上に IPv6 アドレスが必要です。

トンネルを介した内部ホストへの IPv6 接続の場合には、内部インターフェイス上の IPv6 も必要です。

```
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
```

IPv6 では、インターネットへのネクストホップ ルータを指すデフォルト ルートも必要です。

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

クライアントでの認証のために、ASA にはアイデンティティ証明書が必要です。そのような証明書の作成やインポートの手順はこのドキュメントの対象外ですが、次のような他のドキュメントの中に簡単に見つけることができます。

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

結果の設定は次のようになります。

```
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
```

次に、SSL 用にこの証明書を使用するように ASA に指示します。

```
ssl trust-point testCA
```

次に、外部インターフェイスで機能が有効になっている基本 webvpn（SSLVPN）設定を示します。ダウンロードできるクライアントのパッケージが定義されており、プロファイルを定義します（詳細については後述します）。

```
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
```

この基本例では、デフォルト グループ ポリシー（DfltGrpPolicy）内に、IPv4 と IPv6 のアドレス プール、DNS サーバ情報（クライアントにプッシュされる）、およびプロファイルが設定されています。 ここではさらに多くの属性が設定できます。オプションで、異なるユーザのセットに対して異なるグループ ポリシーを定義できます。

注：「gateway-fqdn」属性はバージョン9.0で新しく追加され、DNSで認識されているASAのFQDNを定義します。クライアントはこの FQDN を ASA から取得し、IPv4 ネットワークと IPv6 ネットワークとの間でのローミングに使用します。

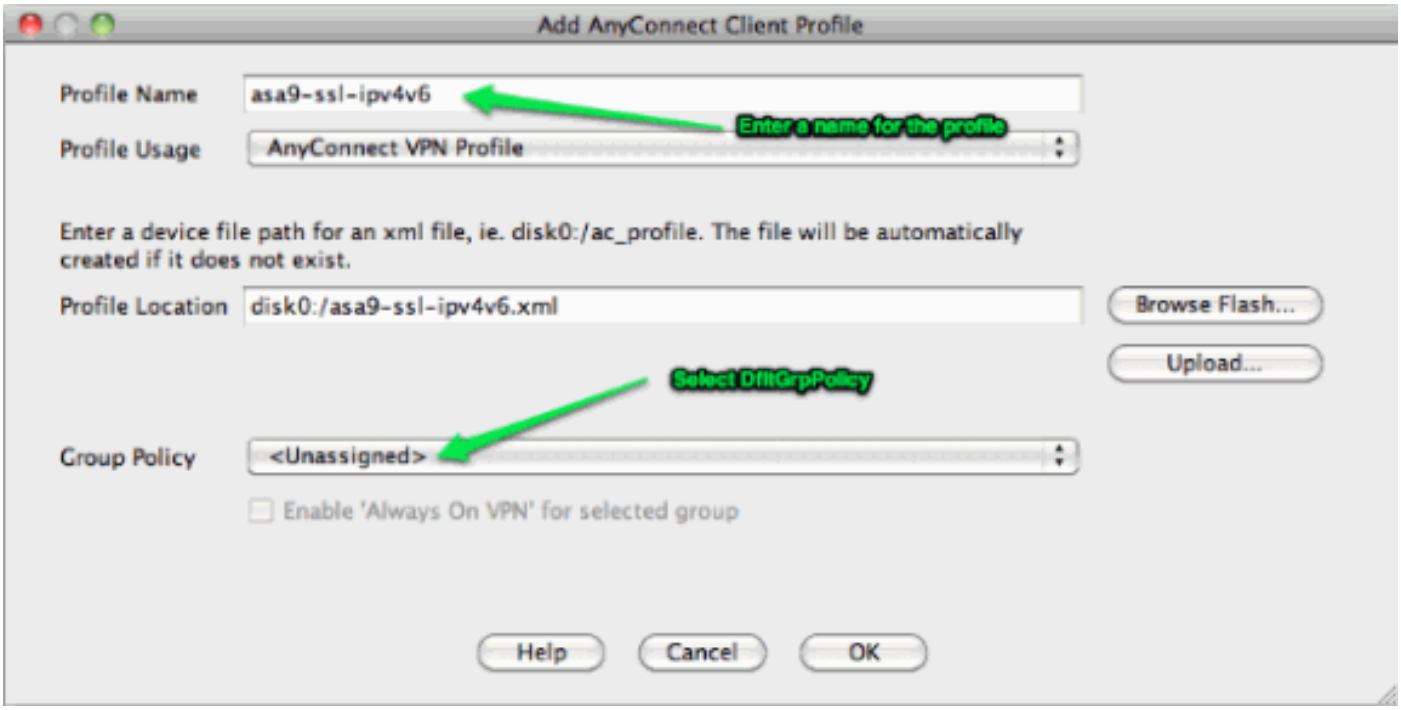
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

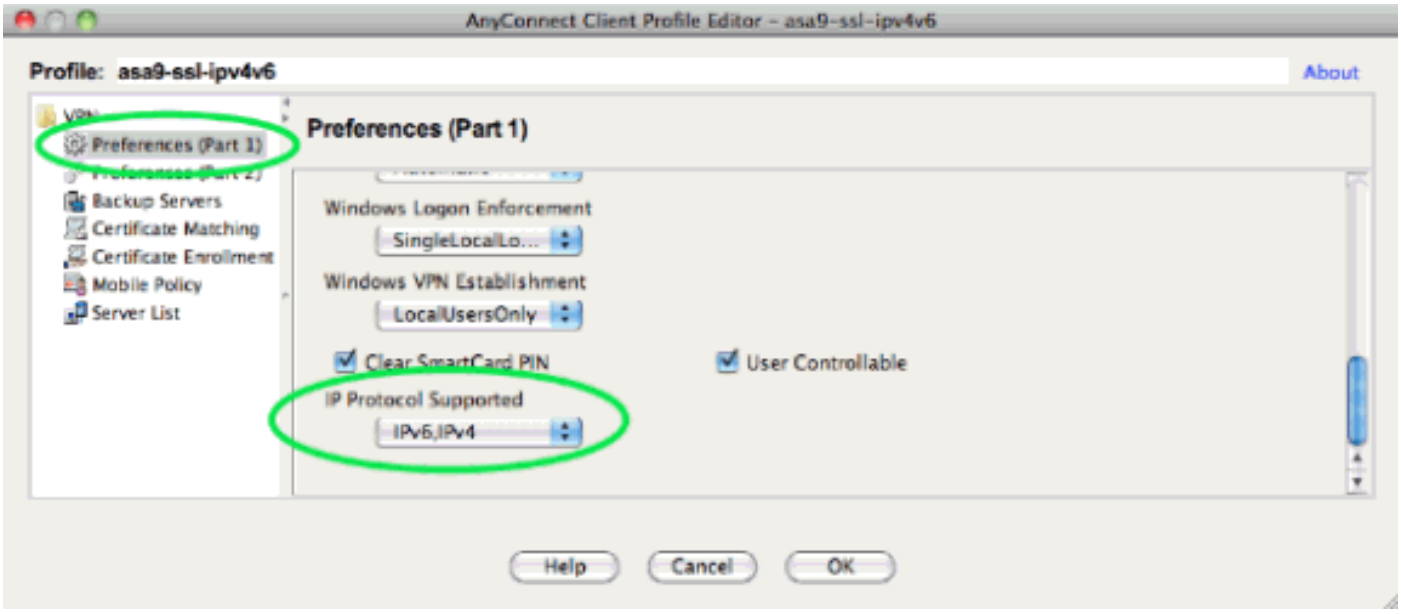
次に、1 つ以上のトンネル グループを設定します。この例では、デフォルトのグループ（DefaultWEBVPNGroup）を使用しており、そのグループを、証明書を使用した認証をユーザに要求するように設定します。

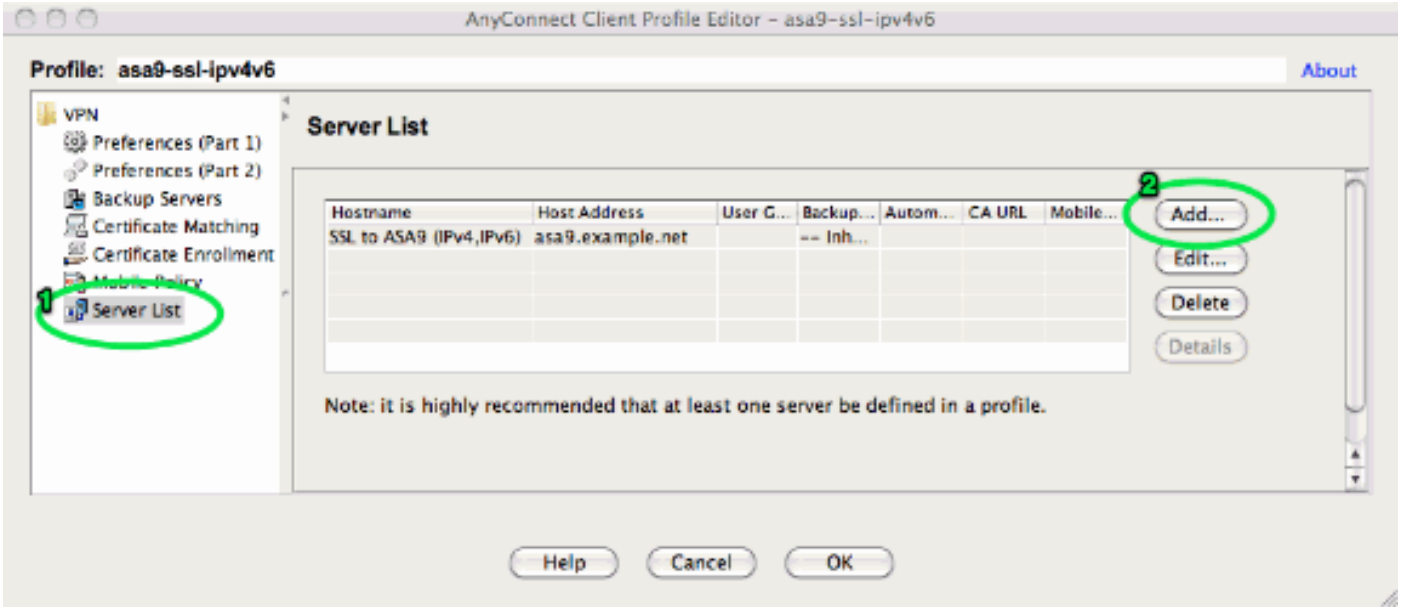
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

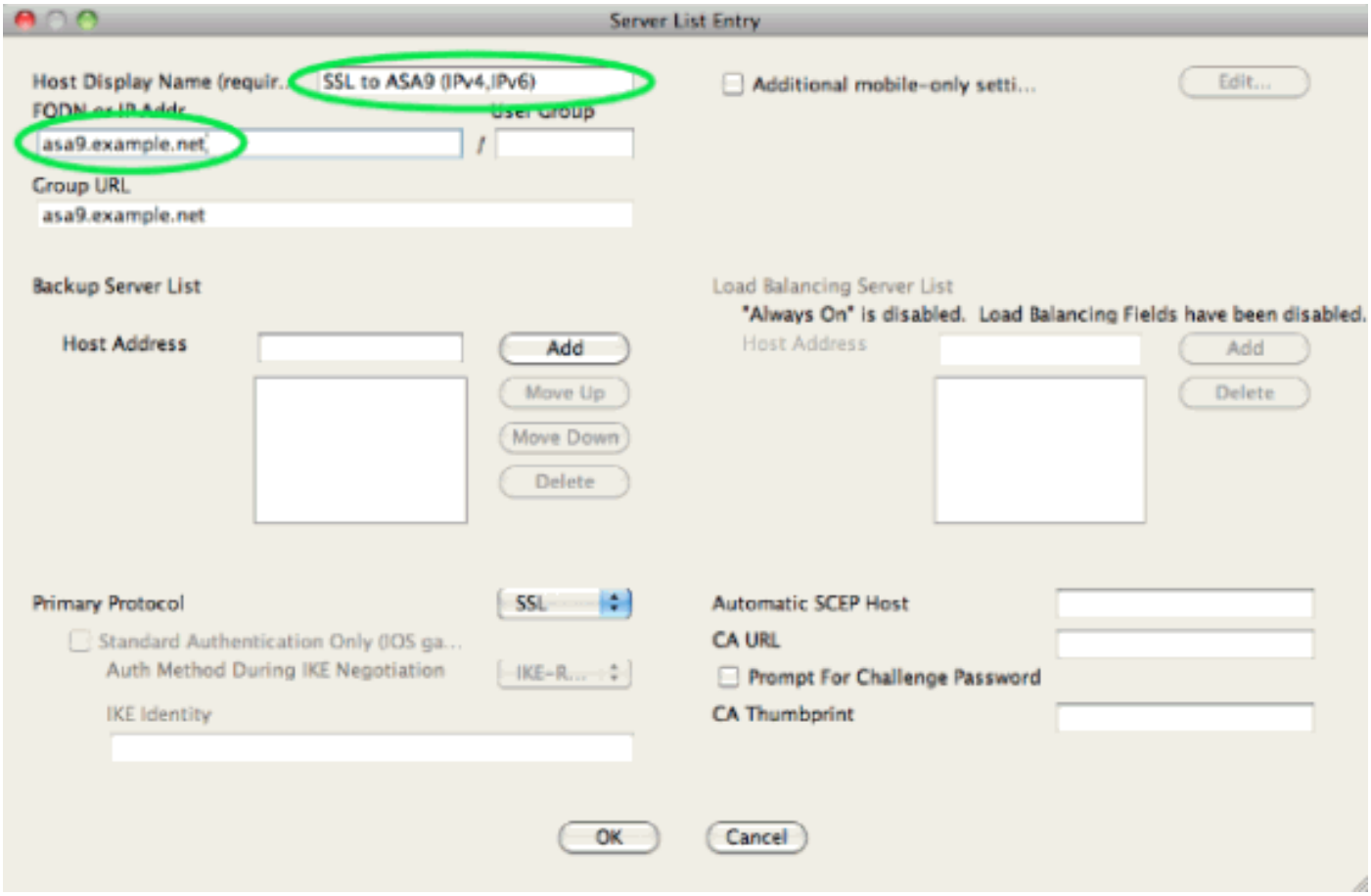
デフォルトでは、AnyConnectクライアントはIPv4経由で接続を試行し、失敗した場合にのみIPv6経由で接続を試行します。ただし、この動作はXMLプロファイルの設定によって変更できます。上記の設定で参照されている AnyConnect プロファイル「asa9-ssl-ipv4v6.xml」は、ASDM のプロファイル エディタを使用して生成されました（[Configuration] > [Remote Access VPN] >

[Network (Client) Acccess] > [AnyConnect Client Profile]) 。









結果の XML プロファイル（デフォルト部分のほとんどを省略して簡略化しています）：

```
<?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>
```

上記のプロファイルでは、HostName（ASA の実際のホスト名と一致する必要はなく、任意の値を使用可能）と HostAddress（通常は ASA の FQDN）も定義されています。

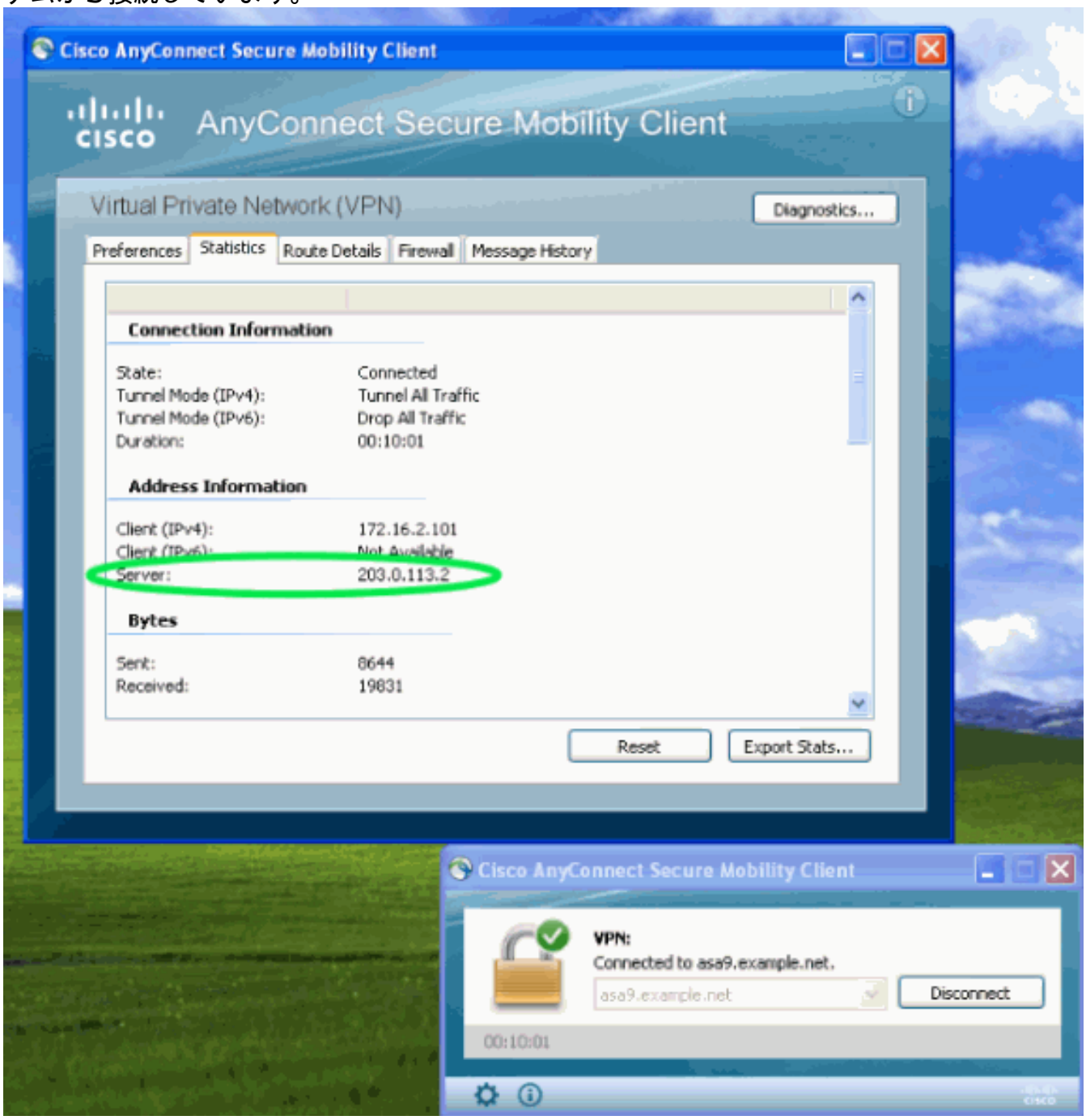
注：HostAddressフィールドは空のままにできますが、HostNameフィールドにはASAのFQDNを含める必要があります。

注：プロファイルが事前に配備されていない限り、最初の接続ではユーザがASAのFQDNを入力する必要があります。この初期接続では、IPv4が優先されます。接続が成功すると、プロファイルがダウンロードされます。そこから、プロファイル設定が適用されます。

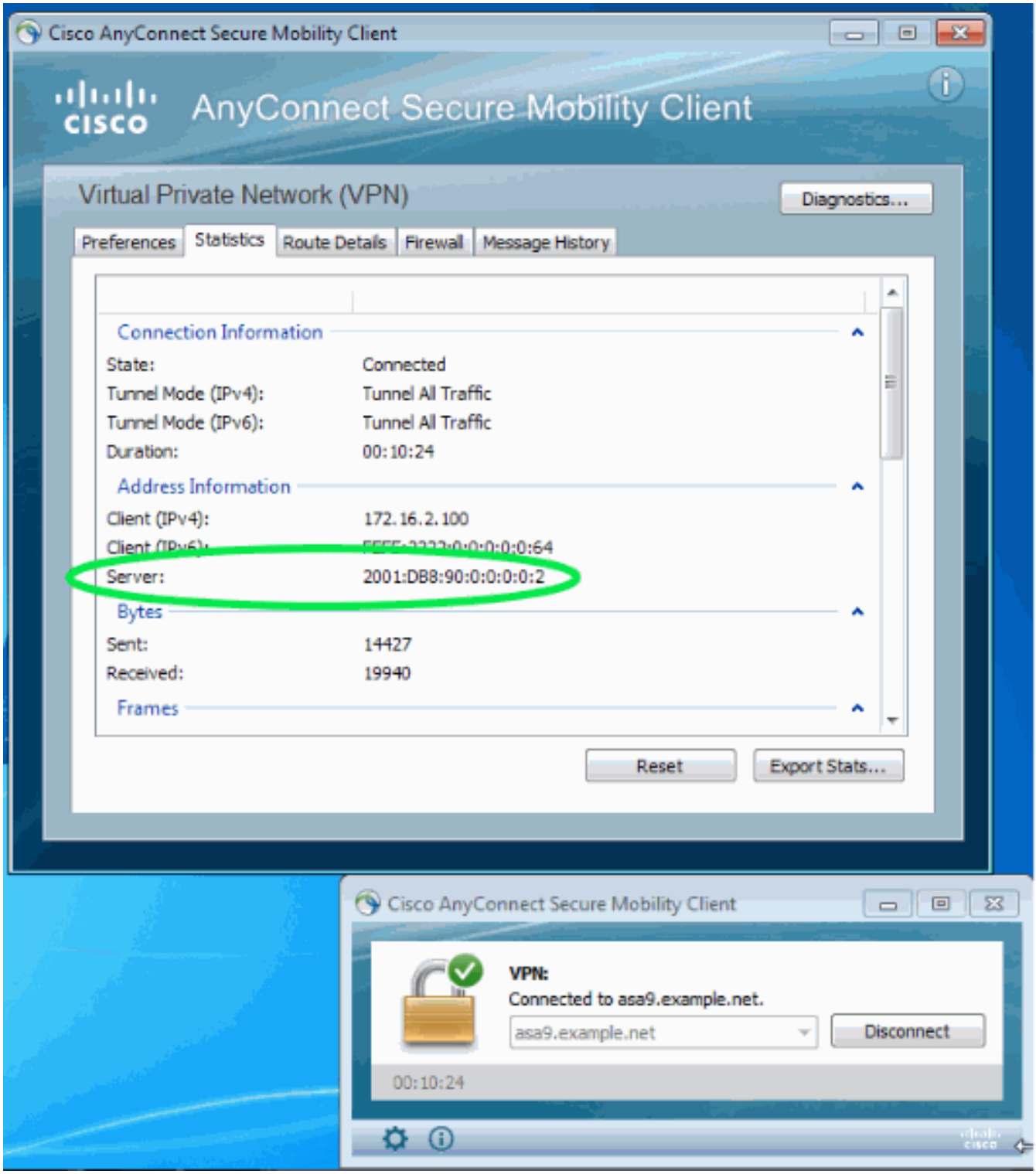
確認

クライアントが IPv4 と IPv6 のどちらを介して接続されているのかを確認するには、クライアント GUI または ASA の VPN セッション DB をチェックします。

- クライアントで、[Advanced] ウィンドウを開き、[Statistics] タブに移動して、「Server」の IP アドレスを確認します。この最初のユーザは、IPv6 をサポートしない Windows XP システムから接続しています。



この 2 番目のユーザは、IPv6 接続がある Windows 7 ホストから ASA に接続しています。



- ASA で、CLI から「show vpn-sessiondb anyconnect」出力の「Public IP」をチェックします。この例では、上記と同じ 2 つの接続を確認できます。1 つは IPv4 を介した XP からの接続であり、もう 1 つは IPv6 を介した Windows 7 からの接続です。

```
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
```

関連情報

- テクニカル サポートとドキュメント – Cisco Systems