# تكوين AnyConnect SSL عبر IPv4+IPv6 إلى ASA

## المحتويات



## المقدمة

يقدم هذا المستند نموذجا لتكوين جهاز الأمان القابل للتكيف (ASA) من Cisco للسماح ل Cisco AnyConnect Secure Mobility Client (المشار إليه باسم "AnyConnect" في باقي هذا المستند) بإنشاء نفق SSL VPN عبر شبكة IPv4 أو IPv6.

وبالإضافة إلى ذلك، يتيح هذا التكوين للعميل تمرير حركة مرور بيانات IPv4 و IPv6 عبر النفق.

## المتطلبات الأساسية

### المتطلبات

من أجل إنشاء نفق SSLVPN بنجاح عبر IPv6، يلبي هذه المتطلبات:

- يلزم توفر اتصال شامل عبر بروتوكول IPv6
- يلزم أن يكون إصدار AnyConnect 3.1 أو إصدارا أحدث
- يلزم أن يكون إصدار برنامج ASA 9.0 أو إصدار أحدث

ومع ذلك، إذا لم يتم الوفاء بأي من هذه المتطلبات، سيظل التكوين الذي تمت مناقشته في هذا المستند يسمح للعميل بالاتصال عبر IPv4.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ASA-5505 مع برنامج صيغة 9.0(1)
- AnyConnect Secure Mobility Client 3.1.00495 على نظام التشغيل Microsoft Windows XP Professional (بدون دعم IPv6)
- AnyConnect Secure Mobility Client 3.1.00495 على نظام التشغيل Microsoft Windows 7

Enterprise إصدار 32 بت

## الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

# التكوين

أولا، حدد تجمع عناوين IP الذي ستقوم من خلاله بتعيين عنوان لكل عميل يتصل.

إذا كنت تريد أن يحمل العميل أيضا حركة مرور IPv6 عبر النفق، ستحتاج إلى مجموعة من عناوين IPv6. وتتم الإشارة إلى كلا الصندوقين لاحقا في نهج المجموعة.

```
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
```

لاتصال IPv6 ب ASA، يلزمك عنوان IPv6 على الواجهة التي سيتصل بها العملاء (عادة الواجهة الخارجية).

بالنسبة لاتصال IPv6 عبر النفق بالأجهزة المضيفة الداخلية، تحتاج إلى IPv6 على الواجهة (الواجهات) الداخلية كذلك.

```
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
```

بالنسبة ل IPv6، تحتاج أيضا إلى مسار افتراضي يشير إلى موجه الخطوة التالية باتجاه الإنترنت.

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

للمصادقة على نفسه للعملاء، يحتاج ASA إلى الحصول على شهادة هوية. التعليمات حول كيفية إنشاء أو إستيراد مثل تلك الشهادة تقع خارج نطاق هذا المستند، ولكن يمكن العثور عليها بسهولة في وثائق أخرى مثل

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

يجب أن يبدو التكوين الناتج مماثلا لما يلي:

```
crypto ca trustpoint testCA
 keypair testCA
 crl configure
...
crypto ca certificate chain testCA
 certificate ca 00
308201fa a0030201 02020100 300d0609 2a864886 f70d0101 05050030 30820312
...
 quit
```

```
certificate 04
3082032c 30820214 a0030201 02020104 300d0609 2a864886 f70d0101 05050030
...
quit
```

بعد ذلك، قم بإصدار تعليمات إلى ASA لاستخدام هذه الشهادة ل SSL:

```
ssl trust-point testCA
```

التالي هو تكوين WebVPN الأساسي (SSLVPN) حيث يتم تمكين الميزة على الواجهة الخارجية. يتم تحديد حزم العميل المتوفرة للتنزيل، ونقوم بتعريف توصيف محدد (المزيد على هذا لاحقا):

```
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
```

في هذا المثال الأساسي، يتم تكوين تجمعات عناوين IPv4 و IPv6 ومعلومات خادم DNS (التي سيتم دفعها إلى العميل) وملف تعريف في نهج المجموعة الافتراضي (DfltGrpPolicy). يمكن تكوين العديد من السمات الإضافية هنا، ويمكنك بشكل إختياري تحديد سياسات مجموعات مختلفة لمجموعات مختلفة من المستخدمين.

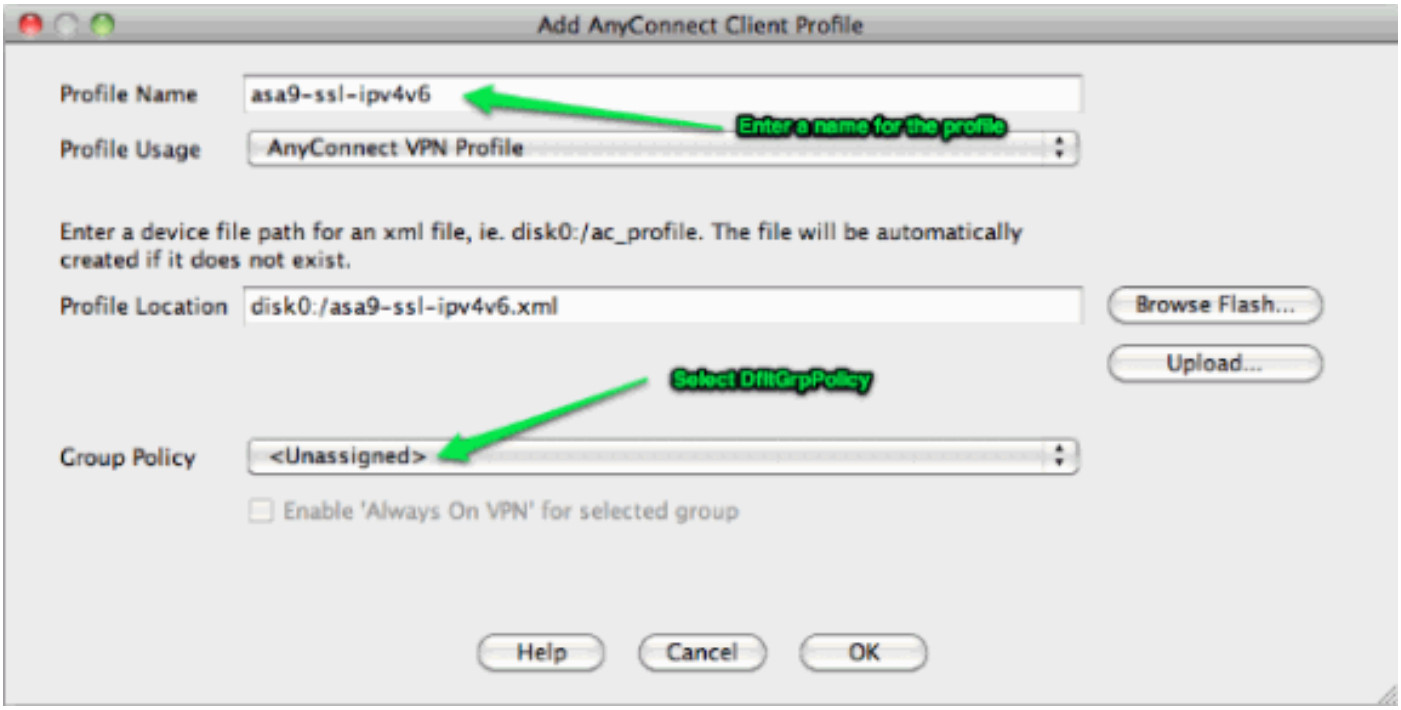
**ملاحظة:** السمة "gateway-fqdn" جديدة في الإصدار 9.0 وتعرف FQDN الخاص ب ASA كما هو معروف في DNS. يعلم العميل FQDN هذا من ASA وسيستخدمه عند التجوال من شبكة IPv4 إلى شبكة IPv6 أو العكس.

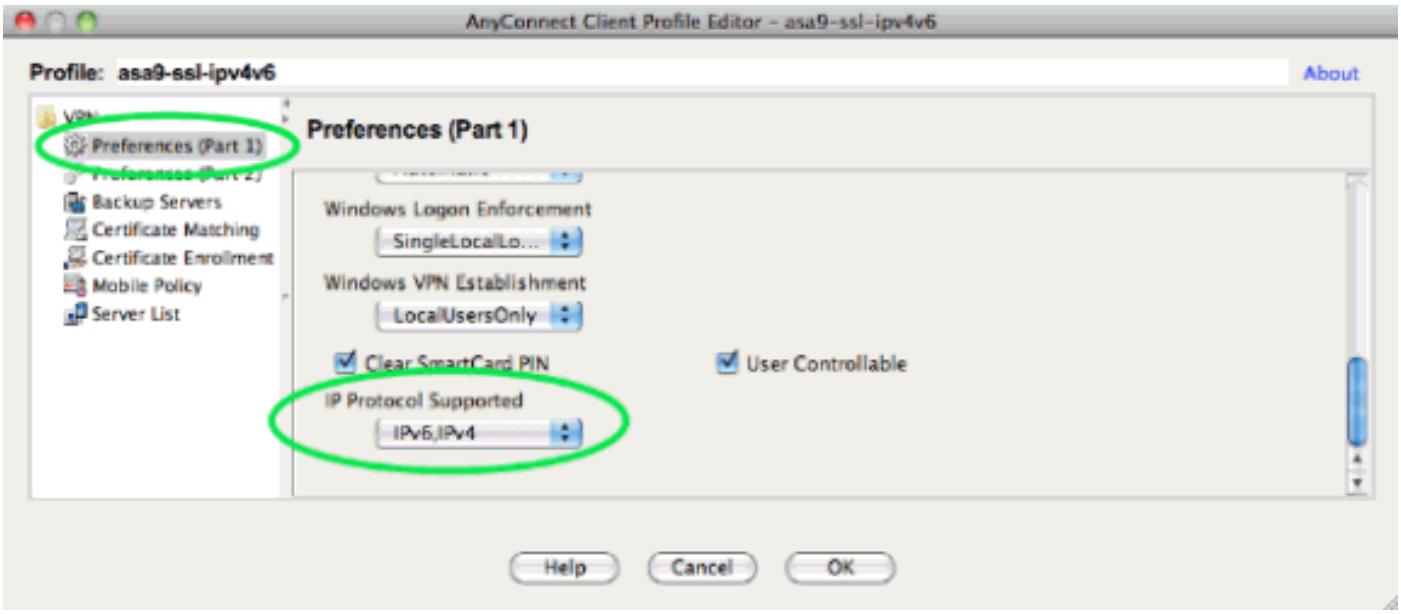
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
  anyconnect profiles value asa9-ssl-ipv4v6 type user
```

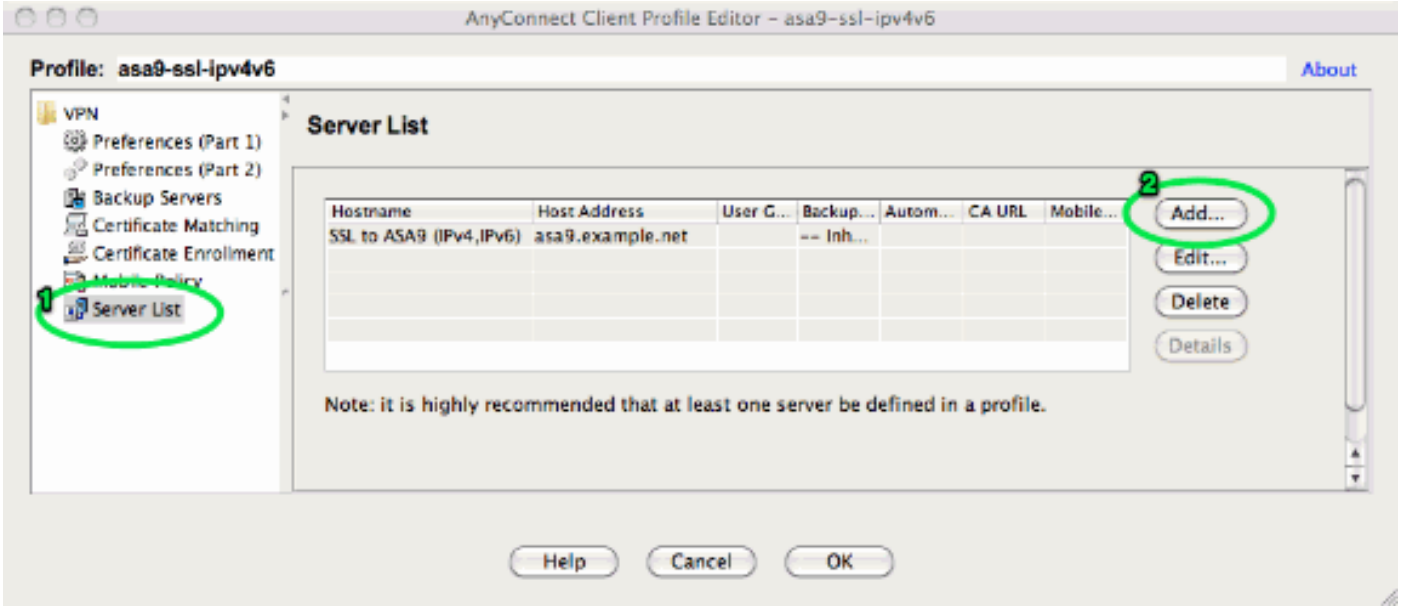
بعد ذلك، قم بتكوين مجموعة نفق واحدة أو أكثر. يتم إستخدام المثال الافتراضي (DefaultWEBVPNGgroup) لهذا المثال، وتكوينه لمطالبة المستخدم بالمصادقة باستخدام شهادة:

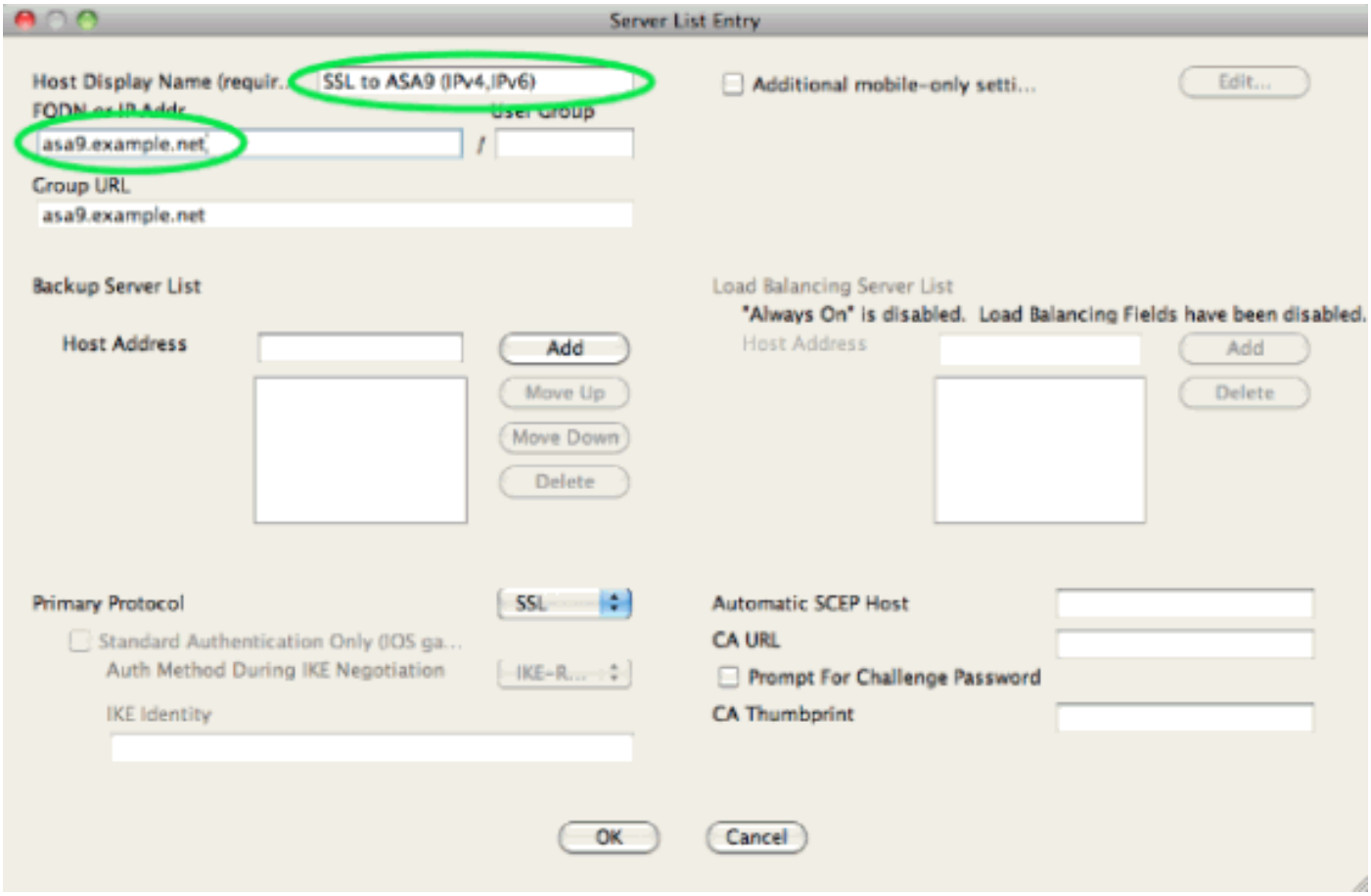
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

بشكل افتراضي، يحاول عميل AnyConnect الاتصال عبر IPv4، وفي حالة فشل هذا فقط، يحاول الاتصال عبر IPv6. ومع ذلك، يمكن تغيير هذا السلوك بإعداد في ملف تعريف XML. تم إنشاء ملف تعريف AnyConnect "asa9-ssl-ipv4v6.xml" الذي تتم الإشارة إليه في التكوين أعلاه، باستخدام محرر ملف التعريف في ASDM (التكوين - الوصول عن بعد VPN - الشبكة (العميل) - ملف تعريف عميل 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




ملف تعريف XML الناتج (مع حذف معظم الجزء الافتراضي للإيجاز):

```
<?"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/>
```

في ملف التعريف أعلاه، يتم أيضا تحديد HostName (والذي يمكن أن يكون أي شيء، ولا يلزم أن يطابق اسم المضيف الفعلي ل ASA)، وعنوان HostAddress (الذي يكون عادة FQDN ل ASA).

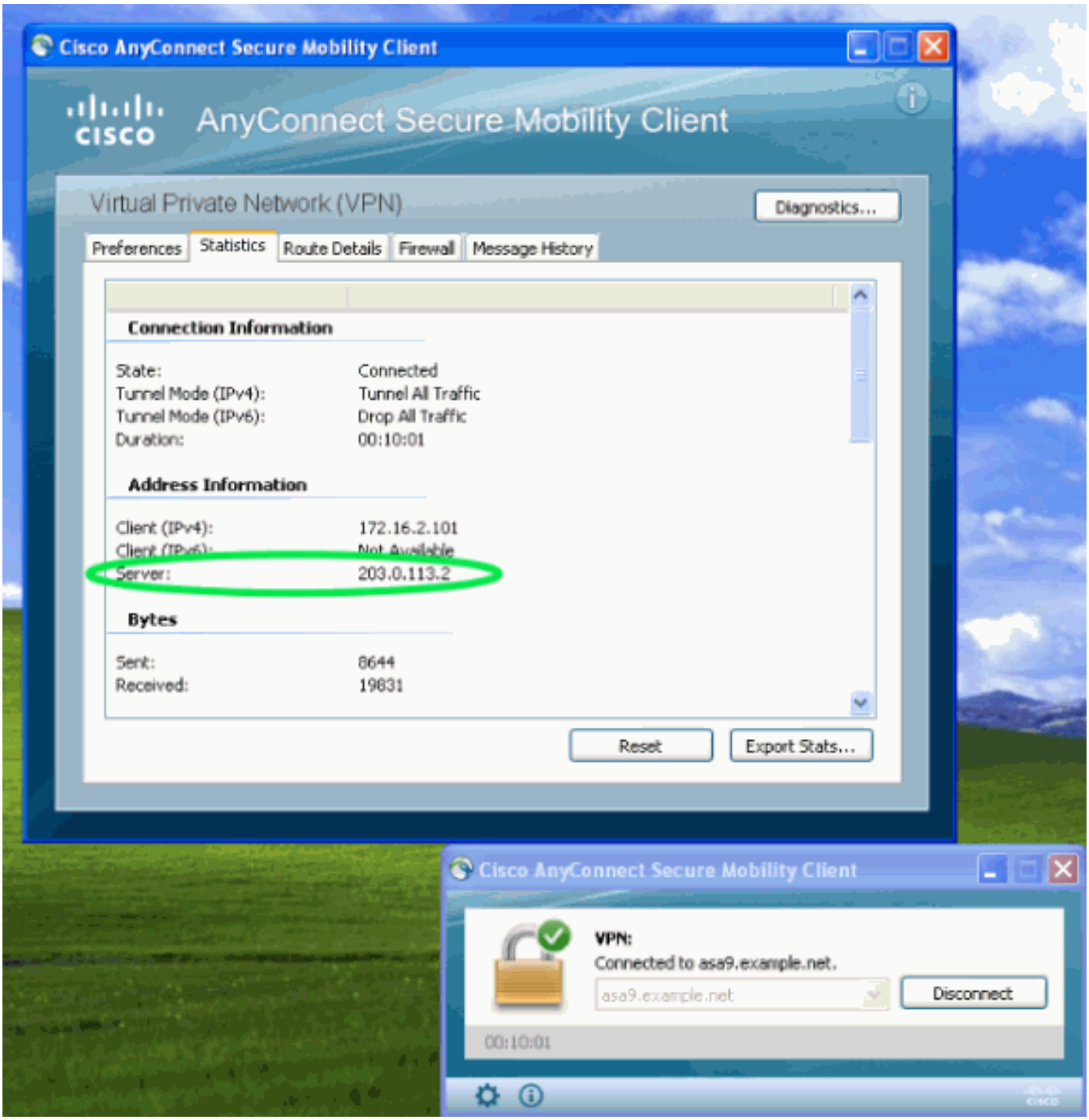
**ملاحظة:** يمكن ترك حقل HostAddress فارغا، ولكن يجب أن يحتوي حقل HostName على FQDN الخاص ب ASA.

**ملاحظة:** ما لم يكن ملف التعريف قد تم نشره مسبقا، يتطلب الاتصال الأول من المستخدم الكتابة في FQDN الخاصة ببروتوكول ASA. يفضل هذا الاتصال الأولي IPv4. بعد نجاح التوصيل، يتم تنزيل التوصيف. من هناك، سيتم تطبيق إعدادات التوصيف.

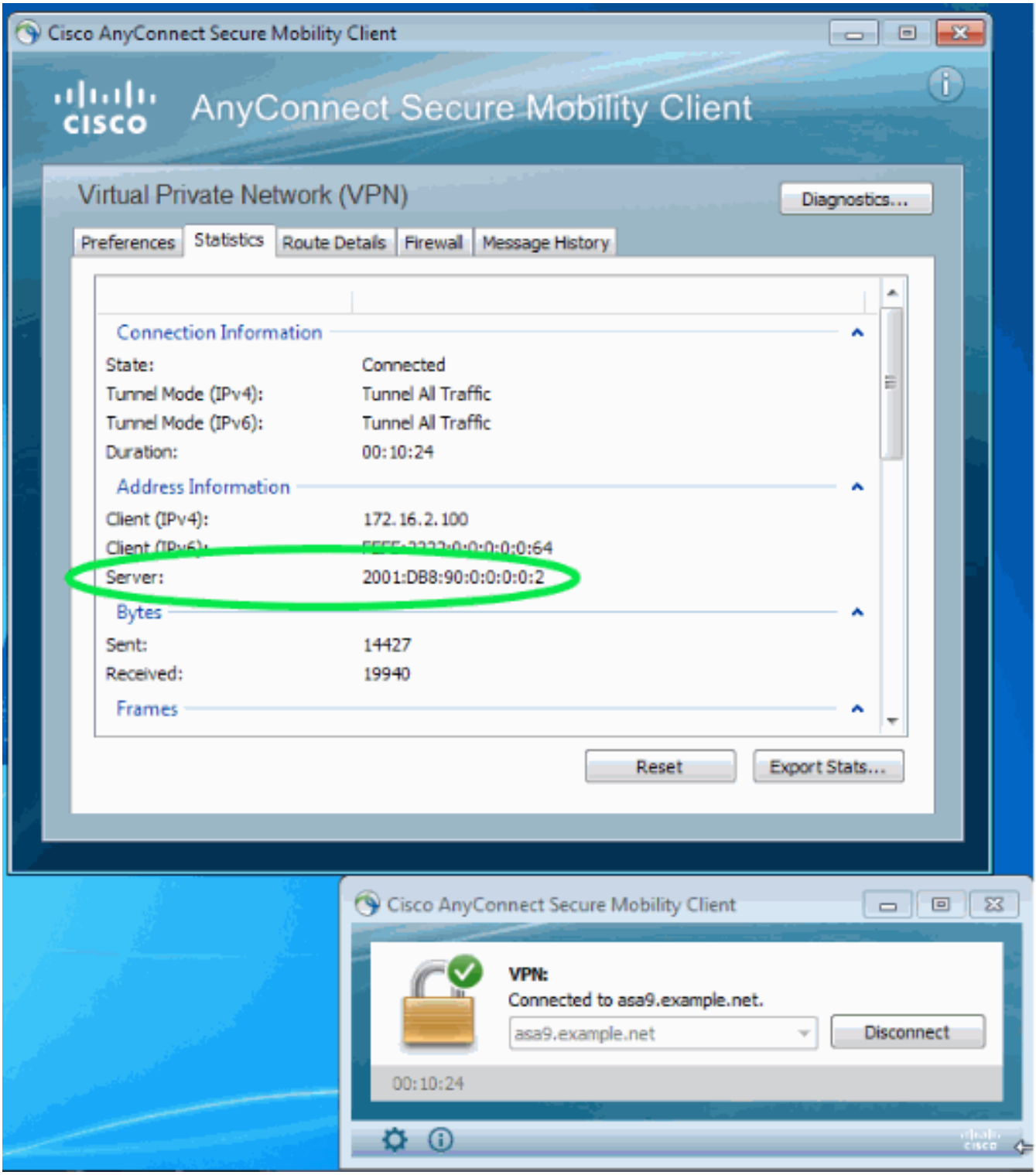
## التحقق من الصحة

للتحقق من ما إذا كان العميل متصلا عبر IPv4 أو IPv6، تحقق من واجهة المستخدم الرسومية (GUI) للعميل أو قاعدة بيانات جلسة عمل VPN على ASA:

- على العميل، افتح نافذة "خيارات متقدمة"، انتقل إلى علامة التبويب "إحصائيات" وتحقق من عنوان IP الخاص ب "الخادم".يقوم هذا المستخدم الأول بالاتصال من نظام Windows XP بدون دعم IPv6:




يتصل هذا المستخدم الثاني من مضيف نظام التشغيل Windows 7 باستخدام اتصال IPv6 بالمحول ASA:




- على ال ASA، من ال CLI فحصت ال "عام ip" في "العرض AnyConnect vpn-sessionDB" إنتاج. في هذا المثال، يمكنك مشاهدة نفس التوصيتين المذكورتين أعلاه: واحدة من XP عبر IPv4 والأخرى من Windows 7 عبر 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
```

## معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).