AnyConnect SSL over IPv4+IPv6 to ASA Configuration

Document ID: 115735

Contributed by Herbert Baerten and Marcin Latosiewicz, Cisco TAC Engineers.
Jan 18, 2013

Contents

Introduction

This document provides a sample configuration for the Cisco Adaptive Security Appliance (ASA) to allow the Cisco AnyConnect Secure Mobility Client (referred to as "AnyConnect" in the remainder of this document) to establish an SSL VPN tunnel over an IPv4 or IPv6 network.

In addition, this configuration allows the client to pass IPv4 and IPv6 traffic over the tunnel.

Prerequisites

Requirements

In order to successfully establish an SSLVPN tunnel over IPv6, meet these requirements:

- End−to−end IPv6 connectivity is required
- The AnyConnect version needs to be 3.1 or later
- The ASA software version needs to be 9.0 or later

However, if any of these requirements are not met, the configuration discussed in this document will still allow the client to connect over IPv4.

Components Used

The information in this document is based on these software and hardware versions:

- ASA−5505 with software version 9.0(1)
- AnyConnect Secure Mobility Client 3.1.00495 on Microsoft Windows XP Professional (without IPv6 support)
- AnyConnect Secure Mobility Client 3.1.00495 on Microsoft Windows 7 Enterprise 32−bit

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configuration

First off, define a pool of IP addresses from which you will assign one to each client that connects.

If you want the client to also carry IPv6 traffic over the tunnel, you will need a pool of IPv6 addresses. Both pools are referenced later in the group−policy.

```
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
```

For IPv6 connectivity to the ASA, you need an IPv6 address on the interface that the clients will connect to (typically the outside interface).

For IPv6 connectivity over the tunnel to inside hosts, you need IPv6 on the inside interface(s) as well.

```
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
```

For IPv6, you also need a default route pointing to the next−hop router towards the Internet.

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

In order to authenticate itself to the clients, the ASA needs to have an identity certificate. Instructions on how to create or import such a certificate are beyond the scope of this document, but can be easily found in other documents such as

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808b3cff.shtml

The resulting configuration should look similar to the following:

```
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
```

Then, instruct the ASA to use this certificate for SSL:

```
ssl trust-point testCA
```

Next is the basic webvpn (SSLVPN) configuration where the feature is enabled on the outside interface. Client packages that are available for download are defined, and we define a profile is defined (more on this later):

```
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
```

In this basic example, the IPv4 and IPv6 address pools are configured, DNS server information (that will be pushed to the client) and a profile in the default group−policy (DfltGrpPolicy). Many more attributes can be configured here, and optionally you can define different group−policies for different sets of users.

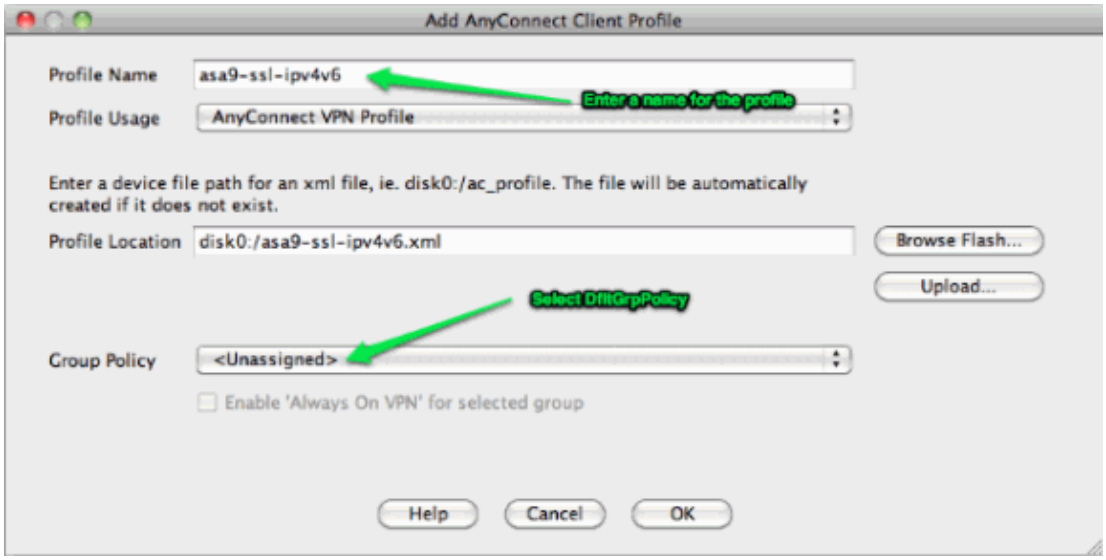
Note: The "gateway−fqdn" attribute is new in version 9.0 and defines the FQDN of the ASA as it is known in the DNS. The client learns this FQDN from the ASA and will use it when roaming from an IPv4 to an IPv6 network or vice versa.

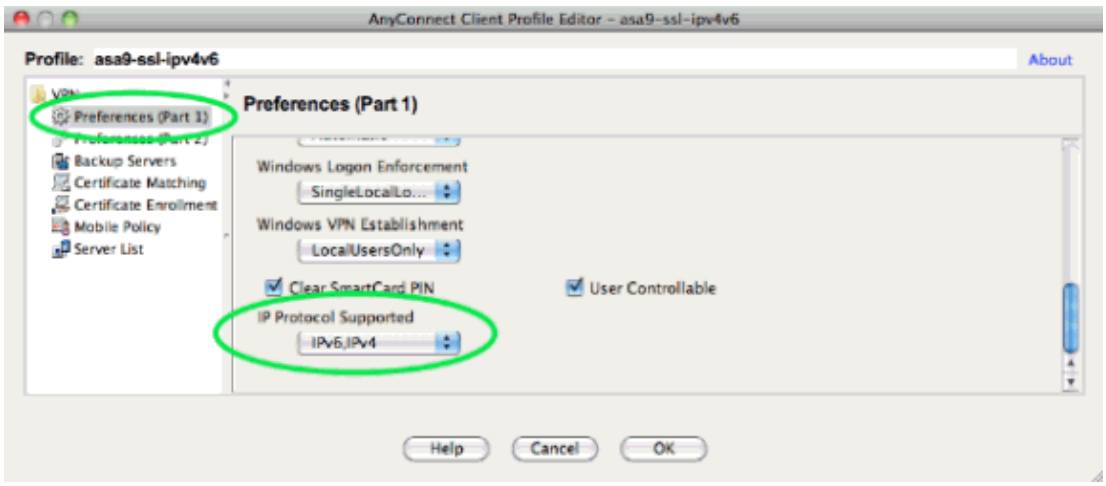
```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

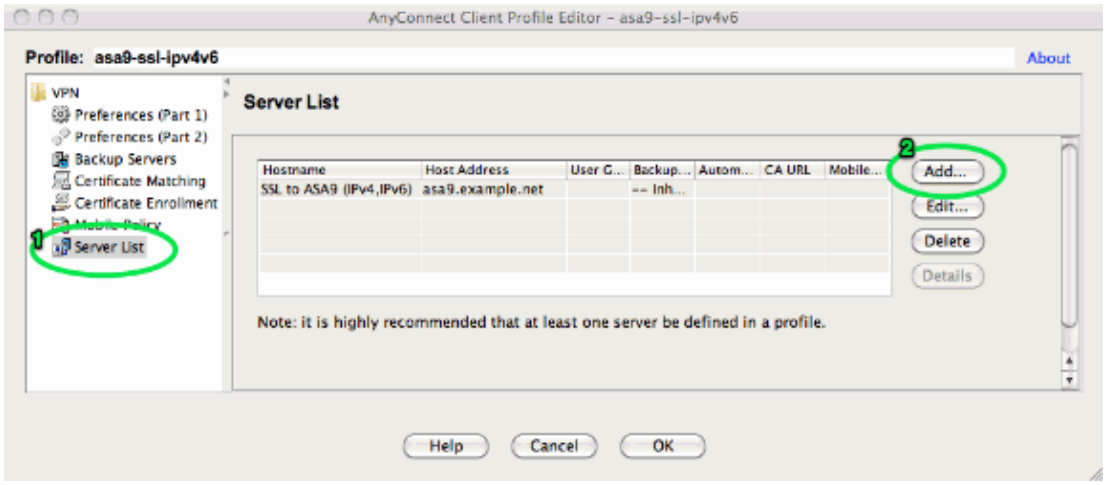
Next, configure one or more tunnel−groups. The default one (DefaultWEBVPNGroup) is used for this example, and configure it to require the user to authenticate using a certificate:

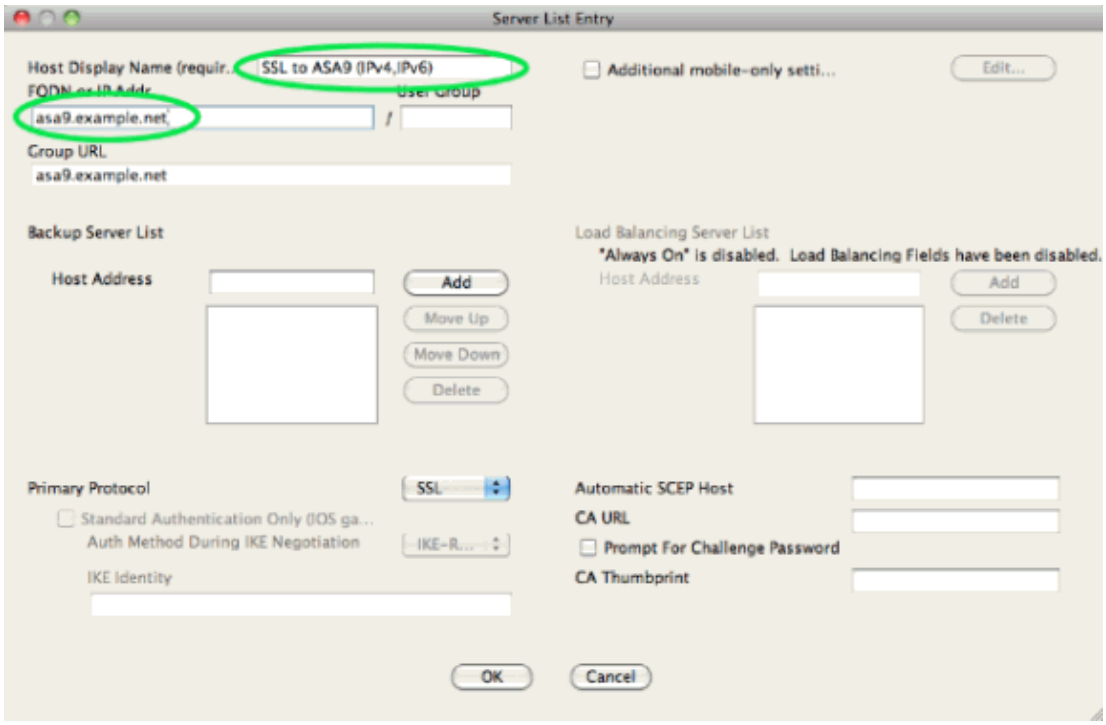
```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

By default, the AnyConnect client attempts to connect over IPv4 and, only if this fails, it attempts to connect over IPv6. However, this behavior can be changed by a setting in the XML profile. The AnyConnect profile "asa9−ssl−ipv4v6.xml" that is referenced in the configuration above, was generated using the Profile Editor in ASDM (Configuration − Remote Access VPN − Network (Client) Acccess − 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
2
Hostname
Host Address
User G...
Backup...
Autom...
CA URL
Mobile...
SSL to ASA9 (IPv4,IPv6)
asa9.example.net
-- Inh...
Add...
Edit...
Delete
Details
Note: it is highly recommended that at least one server be defined in a profile.
Help
Cancel
OK



The resulting XML profile (with most of the default part omitted for brevity):

```
<?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>
```

In the above profile a HostName is also defined (which can be anything, it does not need to match the ASA's actual hostname), and a HostAddress (which is typically the ASA's FQDN).

Note: The HostAddress field can be left empty, but tthe HostName field must contain the ASA's FQDN.

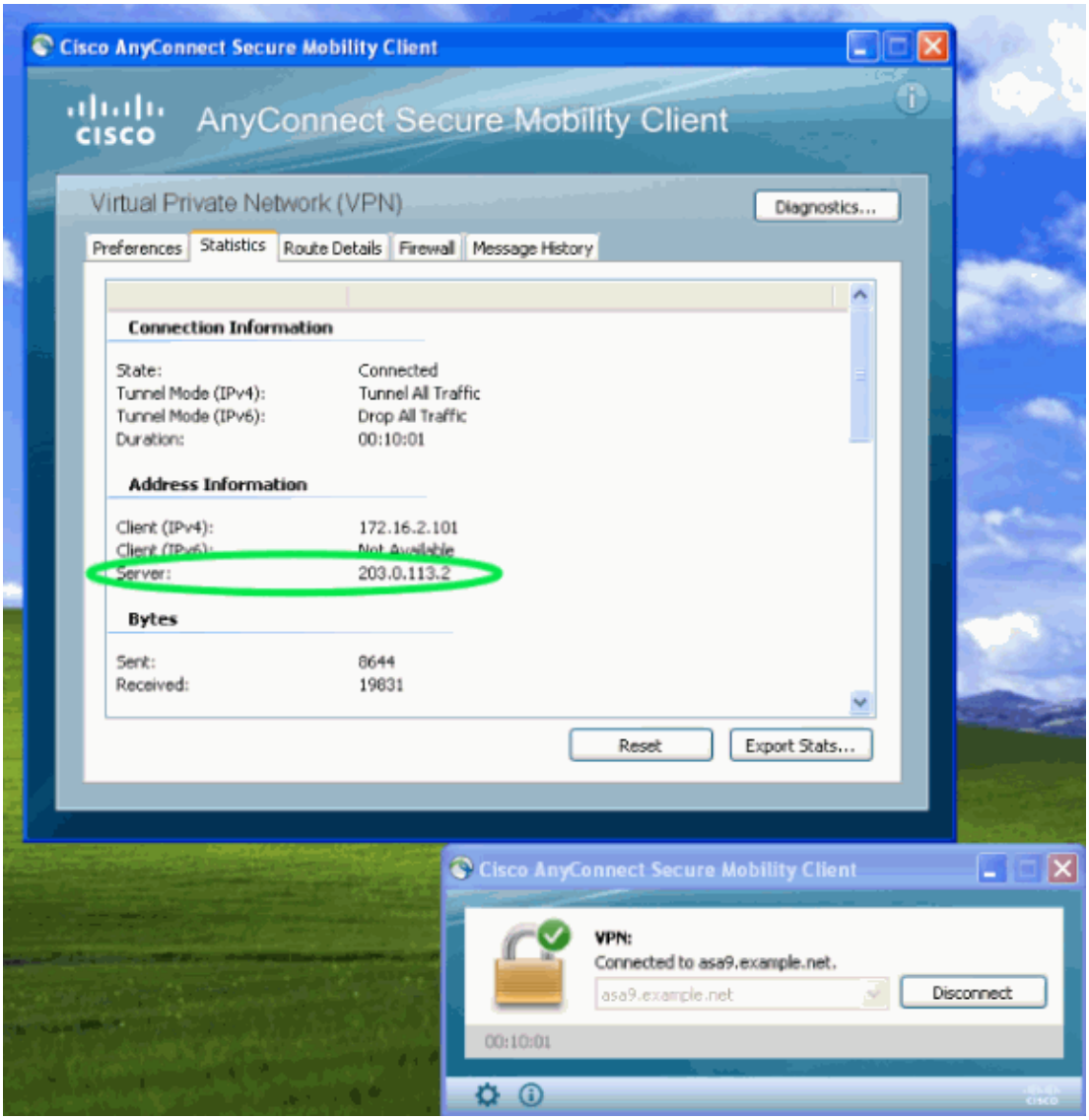
Note: Unless the profile is pre−deployed, the first connection requires the user to type in the FQDN of the ASA. This initial connection will prefer IPv4. After successful connection, the profile will be downloaded. From there, the profile settings will be applied.

Verify

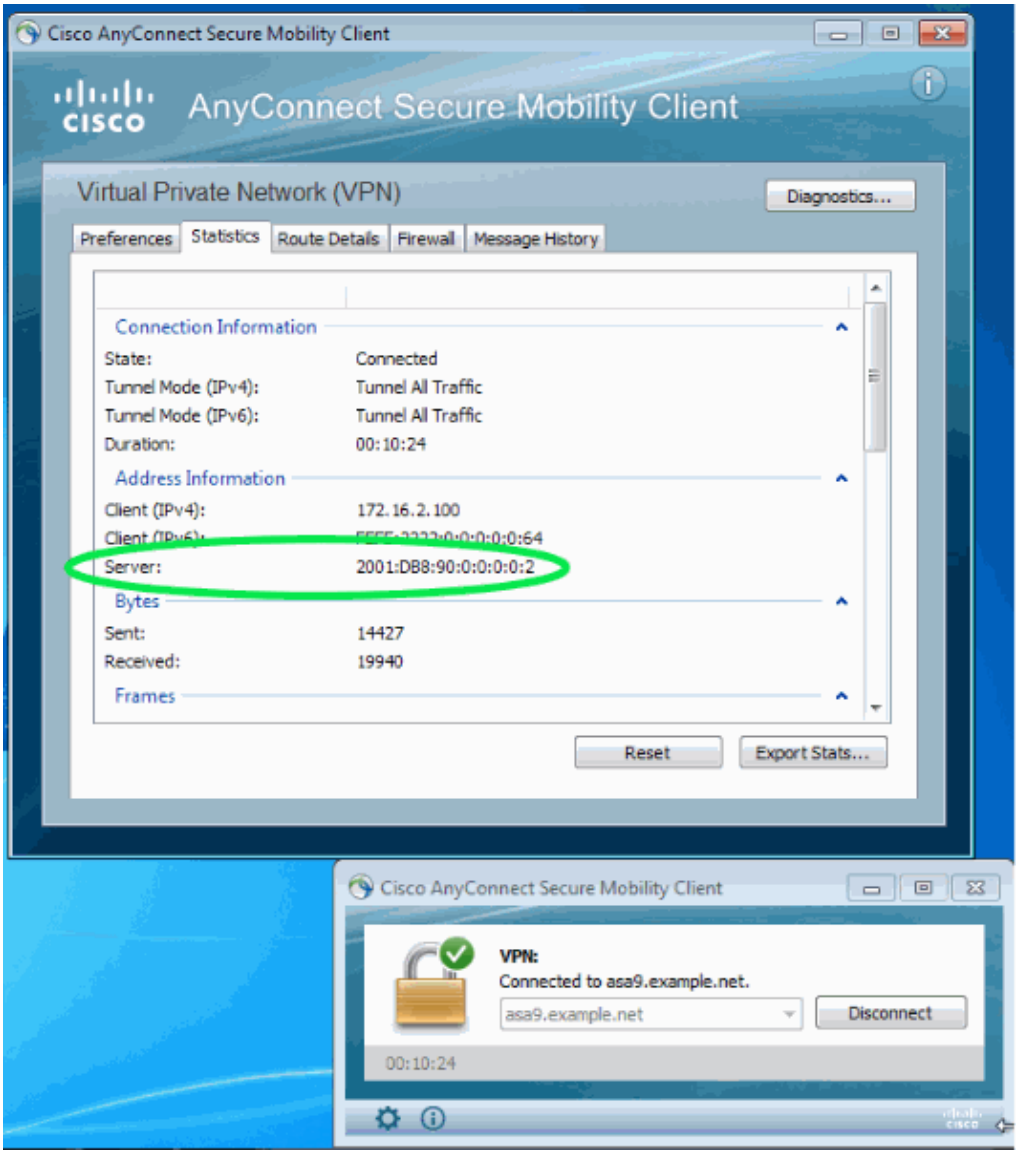
In order to verify whether a client is connected over IPv4 or IPv6, check either the client GUI or the VPN session DB on the ASA:

- On the client, open the Advanced window, go to the Statistics tab and verify the IP address of the "Server".

This first user is connecting from a Windows XP system without IPv6 support:



This second user connects from a Windows 7 host with IPv6 connectivity to the ASA:



- On the ASA, from the CLI check the "Public IP" in the "show vpn−sessiondb anyconnect" output. In this example you can see the same two connections as above: one from XP over IPv4 and one from Windows 7 over 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
```

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Jan 18, 2013 Document ID: 115735