Configure AnyConnect VPN Client U-turn Traffic on ASA 9.X

Contents

Introduction

This document describes how to set up a Cisco Adaptive Security Appliance (ASA) Release 9.X to allow it to u-turn VPN traffic.

Components Used

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

- Cisco 5500 Series ASA that runs software version 9.1(2)
- Cisco AnyConnect SSL VPN Client version for Windows 3.1.05152
- PC which runs a supported OS per the Supported VPN Platforms, Cisco ASA Series.
- Cisco Adaptive Security Device Manager (ASDM) version 7.1(6)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Prerequisites

Requirements

Cisco recommends that you meet these requirements before you attempt this configuration:

- The hub ASA Security Appliance needs to run Release 9.x.
- Cisco AnyConnect VPN Client 3.x

> **Note**: Download the AnyConnect VPN Client package (anyconnect-win*.pkg) from the Cisco Software Download (registered customers only). Copy the AnyConnect VPN client to the Cisco ASA flash memory, and download it to the remote user computers in order to establish the SSL VPN connection with the ASA. Refer to the AnyConnect VPN Client Connections section of the ASA configuration guide for more information.

Background Information

> **Note**: In order to avoid an overlap of IP addresses in the network, assign a completely different pool of IP addresses to the VPN Client (for example, 10.x.x.x , 172.16.x.x, and 192.168.x.x). This IP address scheme is helpful in order to troubleshoot your network.

Hairpin or U-turn

This feature is useful for VPN traffic that enters an interface, but is then routed out of that same interface.

For example, if you have a hub-and-spoke VPN network (where the security appliance is the hub and the remote VPN networks are spokes), in order for one spoke to communicate with another, traffic must go first to the security appliance.

Enter the **same-security-traffic** command in order to allow traffic to enter and exit the same interface.

<#root>

```
ciscoasa(config)#

same-security-traffic permit intra-interface
```

The Cisco AnyConnect VPN Client provides secure SSL connections to the security appliance for remote users.

Without a previously installed client, in their browser, remote users enter the IP address of an interface configured to accept SSL VPN connections.

Unless the security appliance is configured to redirect **http://** requests to **https://**, users must enter the URL in the form **https://<address>**.

After the URL is entered, the browser connects to that interface and displays the login screen.

If the user satisfies the log in and authentication, and the security appliance identifies the user as in need of the client, it downloads the client that matches the operating system of the remote computer.

After the download, the client installs and configures itself, establishes a secure SSL connection, and either remains or uninstalls itself (this depends on the security appliance configuration) when the connection terminates.

In the case of a previously installed client, when the user authenticates, the security appliance examines the revision of the client and upgrades the client as necessary.

When the client negotiates an SSL VPN connection with the security appliance, it connects with Transport Layer Security (TLS), and also uses Datagram Transport Layer Security (DTLS).

DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

The AnyConnect client can be downloaded from the security appliance, or it can be installed manually on the remote PC by the system administrator.

For more information on how to install the client manually, refer to the Cisco AnyConnect Secure Mobility Client Administrator Guide.

The security appliance downloads the client based on the group policy or username attributes of the user that establishes the connection.

You can configure the security appliance to automatically download the client, or you can configure it to prompt the remote user about whether to download the client.

In the latter case, if the user does not respond, you can configure the security appliance to either download the client after a timeout period or present the login page.

> **Note**: The examples used in this document use IPv4. For IPv6 U-turn traffic, the steps are the same but use the IPv6 addresses instead of the IPv4.

Configure U-turning Remote Access Traffic

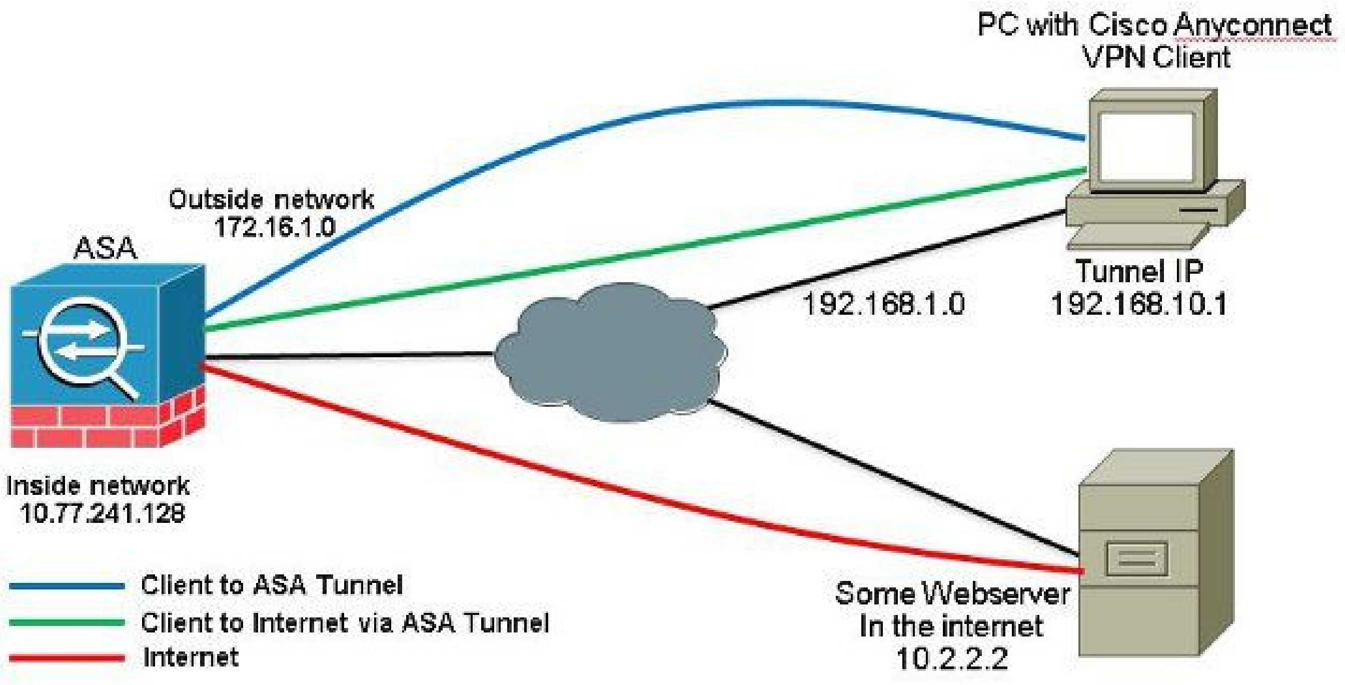
In this section, you are presented with the information to configure the features described in this document.

> **Note**: Use the Command References guides in order to obtain more information on the commands used in this section.

AnyConnect VPN Client for Public Internet VPN on a Stick Configuration Example

Network Diagram

This document uses this network setup:


PC with Cisco Anyconnect VPN Client
Outside network 172.16.1.0
ASA
192.168.1.0
Tunnel IP 192.168.10.1
Inside network 10.77.241.128
Client to ASA Tunnel
Client to Internet via ASA Tunnel
Internet
Some Webserver In the internet 10.2.2.2

ASA Release 9.1(2) Configurations with ASDM Release 7.1(6)

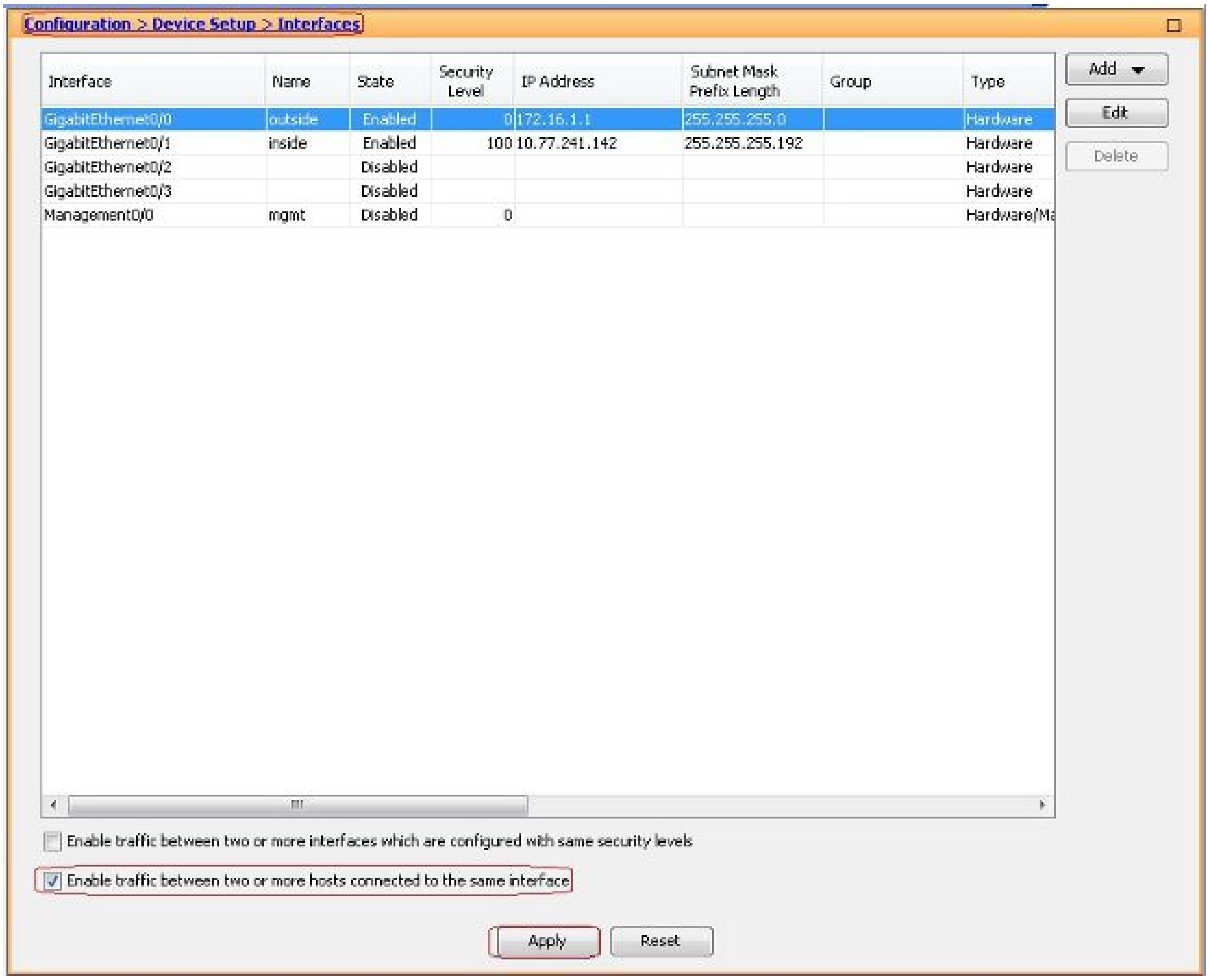
This document assumes that the basic configuration, such as interface configuration, is already completed and works properly.

> **Note**: Refer to Configuring Management Access in order to allow the ASA to be configured by the ASDM.

> **Note**: In Release 8.0(2) and later, the ASA supports both clientless SSL VPN (WebVPN) sessions and ASDM administrative sessions simultaneously on Port 443 of the outside interface. In versions earlier than Release 8.0(2), WebVPN and ASDM cannot be enabled on the same ASA interface unless you change the port numbers. Refer to ASDM and WebVPN Enabled on the Same Interface of the ASA for more information.

Complete these steps in order to configure the SSL VPN on a stick in ASA:

1. Choose **Configuration > Device Setup > Interfaces** and check the **Enable traffic between two or more hosts connected to the same interface** check box in order to allow SSL VPN traffic to enter and exit the same interface. Click **Apply**.



Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type
GigabitEthernet0/0	outside	Enabled	0	172.16.1.1	255.255.255.0		Hardware
GigabitEthernet0/1	inside	Enabled	100	10.77.241.142	255.255.255.192		Hardware
GigabitEthernet0/2		Disabled					Hardware
GigabitEthernet0/3		Disabled					Hardware
Management0/0	mgmt	Disabled	0				Hardware/Ma

☐ Enable traffic between two or more interfaces which are configured with same security levels

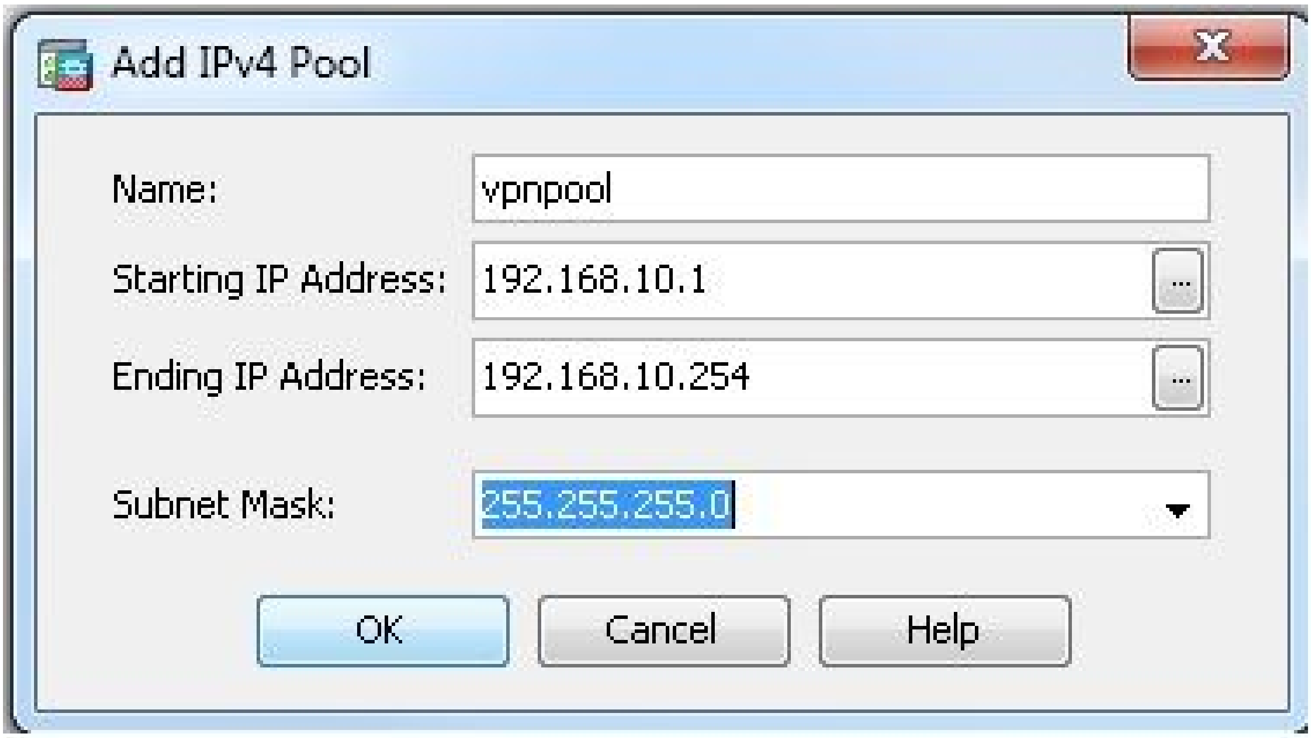
☑ Enable traffic between two or more hosts connected to the same interface

Equivalent CLI Configuration:

<#root>

```
ciscoasa(config)#

same-security-traffic permit intra-interface
```

2. Choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Address Assignment** > **Address Pools** > **Add** in order to create an IP address pool **vpnpool**.



Add IPv4 Pool

Name: vpnpool

Starting IP Address: 192.168.10.1

Ending IP Address: 192.168.10.254

Subnet Mask: 255.255.255.0

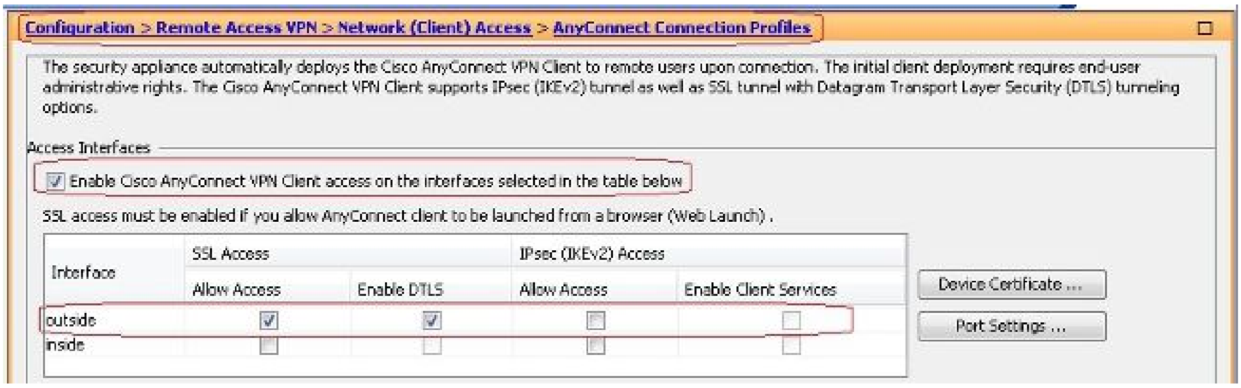
3. Click **Apply**.

   Equivalent CLI Configuration:

   <#root>

   ```
   ciscoasa(config)#
   ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
   ```

4. Enable WebVPN.
   a. Choose **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** and under **Access Interfaces**, click the check boxes **Allow Access** and **Enable DTLS** for the outside interface. Check the **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** check box in order to enable SSL VPN on the outside interface.



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

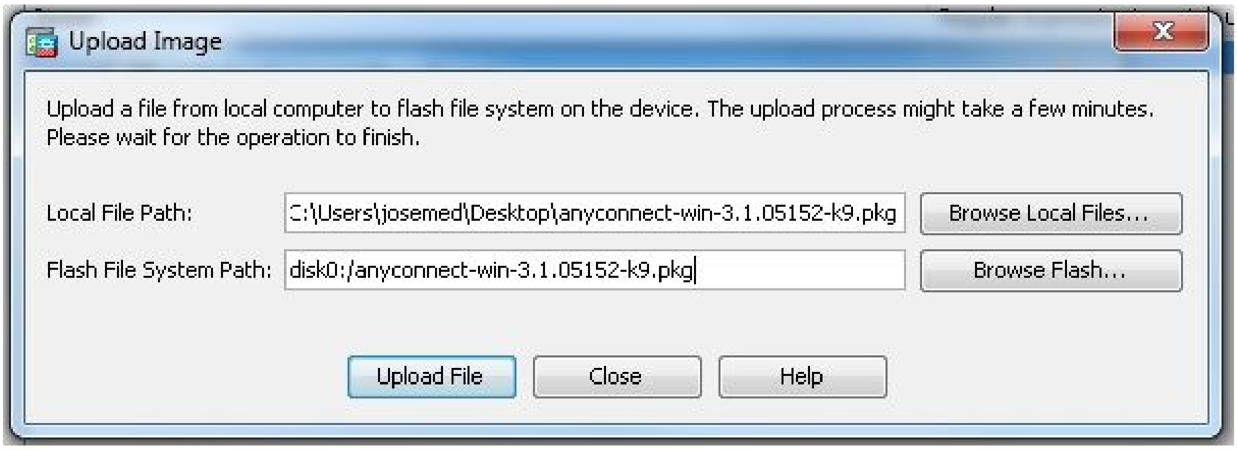
Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	□	□
inside	□	□	□	□

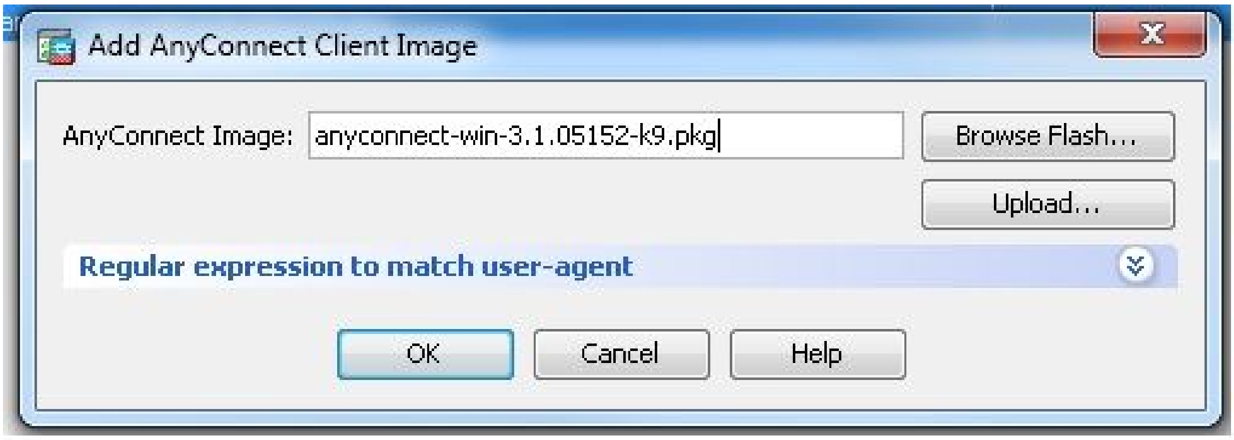
   b. Click **Apply**.
   c. Choose **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** in order to add the Cisco AnyConnect VPN client image from the flash memory of ASA as shown.



Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.

Local File Path: C:\Users\josemed\Desktop\anyconnect-win-3.1.05152-k9.pkg

Flash File System Path: disk0:/anyconnect-win-3.1.05152-k9.pkg



Add AnyConnect Client Image

AnyConnect Image: anyconnect-win-3.1.05152-k9.pkg

Browse Flash...
Upload...
Regular expression to match user-agent
OK
Cancel
Help

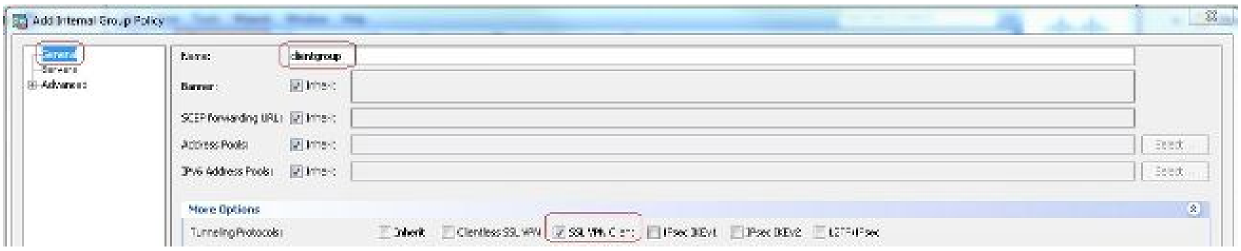
Equivalent CLI Configuration:

<#root>

```
ciscoasa(config)#

webvpn


ciscoasa(config-webvpn)#

enable outside


ciscoasa(config-webvpn)#

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


ciscoasa(config-webvpn)#

tunnel-group-list enable


ciscoasa(config-webvpn)#

anyconnect enable
```

5. Configure Group Policy.
   a. Choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** in order to create an internal group policy **clientgroup**. Under the **General** tab, select the **SSL VPN Client** check box in order

to enable the WebVPN as tunnel protocol.



Add Internal Group Policy

General
Servers
Advanced

Name: clientgroup

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

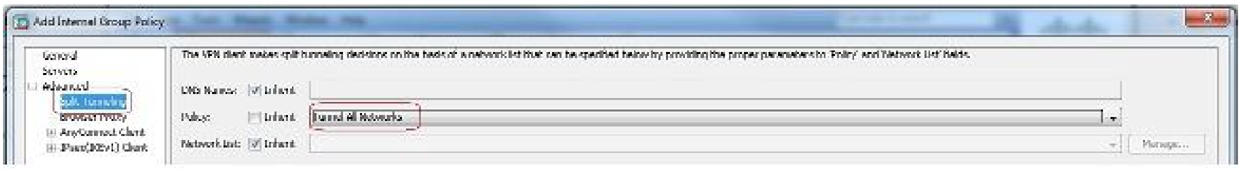
Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit □ Clientless SSL VPN ☑ SSL VPN Client □ IPsec IKEv1 □ IPsec IKEv2 □ L2TP/IPsec

b. In the **Advanced** > **Split Tunneling** tab, choose **Tunnel All Networks** from the Policy drop-down list of the Policy in order to make all the packets from the remote PC through a secure tunnel.



Add Internal Group Policy

General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec(IKEv1) Client

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network List' fields.

DNS Names: ☑ Inherit

Policy: □ Inherit Tunnel All Networks

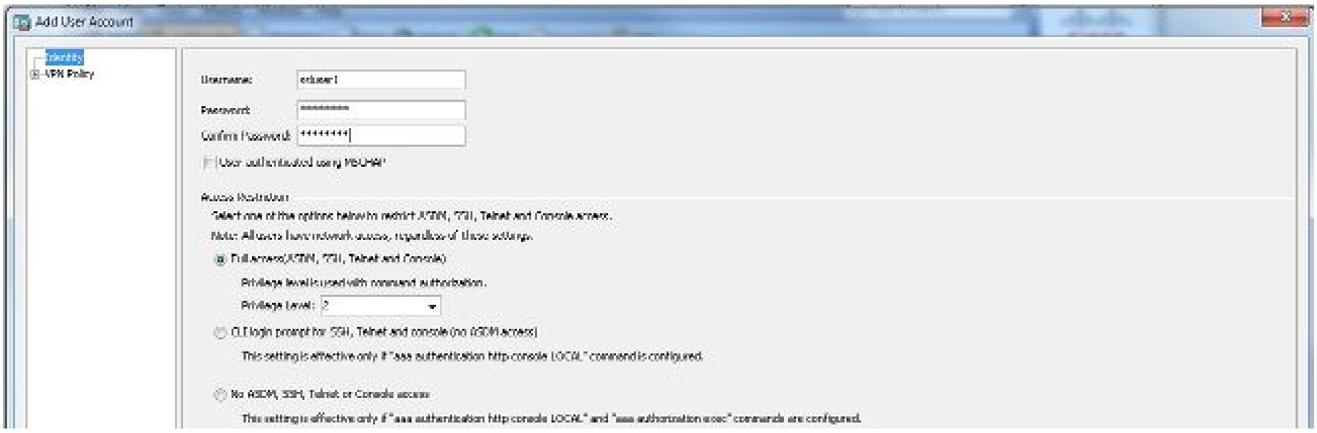
Network List: ☑ Inherit

Equivalent CLI Configuration:

<#root>

```
ciscoasa(config)#

group-policy clientgroup internal


ciscoasa(config)#

group-policyclientgroup attributes


ciscoasa(config-group-policy)#

vpn-tunnel-protocol ssl-client


ciscoasa(config-group-policy)#

split-tunnel-policy tunnelall
```

6. Choose **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **Local Users** > **Add** in order to create a new user account **ssluser1**. Click **OK** and then **Apply**.



Add User Account

Identity
VPN Policy

Username: ssluser1

Password: **********

Confirm Password: ********

□ User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.

Note: All users have network access, regardless of these settings.

● Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 2

○ CLI login prompt for SSH, Telnet and console (no ASDM access)

This setting is effective only if "aaa authentication http console LOCAL" command is configured.

○ No ASDM, SSH, Telnet or Console access

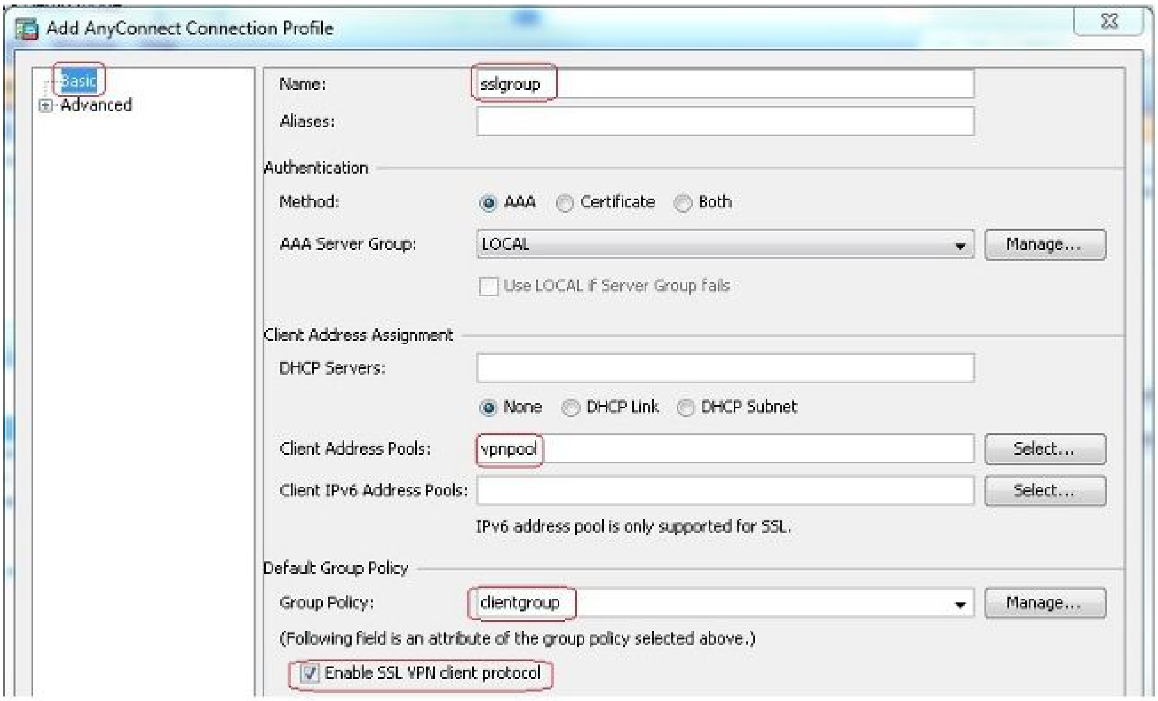
This setting is effective only if "aaa authentication http console LOCAL" and "aaa authorization exec" commands are configured.

Equivalent CLI Configuration:

<#root>

```
ciscoasa(config)#

username ssluser1 password asdmASA@
```

7. Configure Tunnel Group.
   a. Choose **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** in order to create a new tunnel group **sslgroup**.
   b. In the **Basic** tab, you can perform the list of configurations as shown:
      - Name the Tunnel group as **sslgroup**.
      - Under **Client Address Assignment**, choose the address pool **vpnpool** from the **Client Address Pools** drop-down list.
      - Under **Default Group Policy**, choose the group policy **clientgroup** from the **Group Policy** drop-down list.



Add AnyConnect Connection Profile

Basic

Advanced

Name: sslgroup

Aliases:

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: vpnpool

Client IPv6 Address Pools:

IPv6 address pool is only supported for SSL.

Default Group Policy

Group Policy: clientgroup

(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN client protocol

- Under the **Advanced > Group Alias/Group URL** tab, specify the group alias name as **sslgroup_users** and click **OK**.

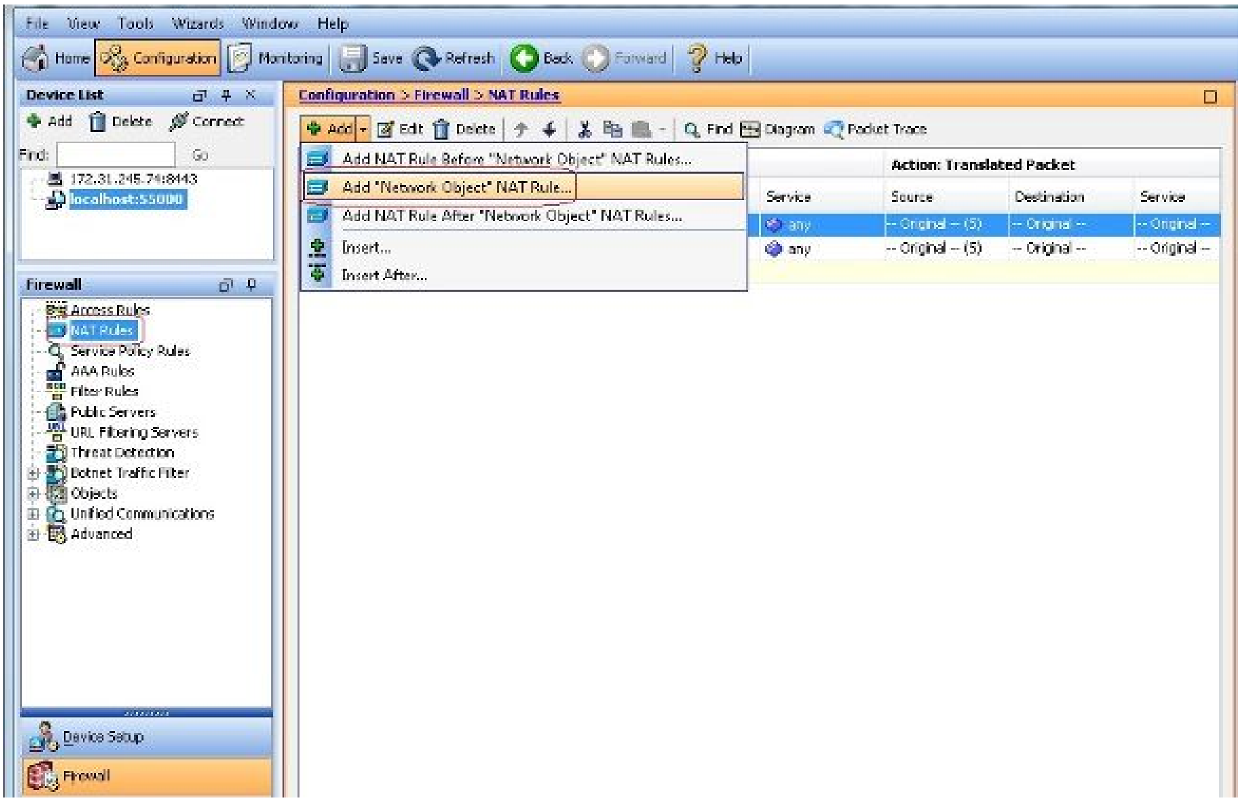
Equivalent CLI Configuration:

<#root>

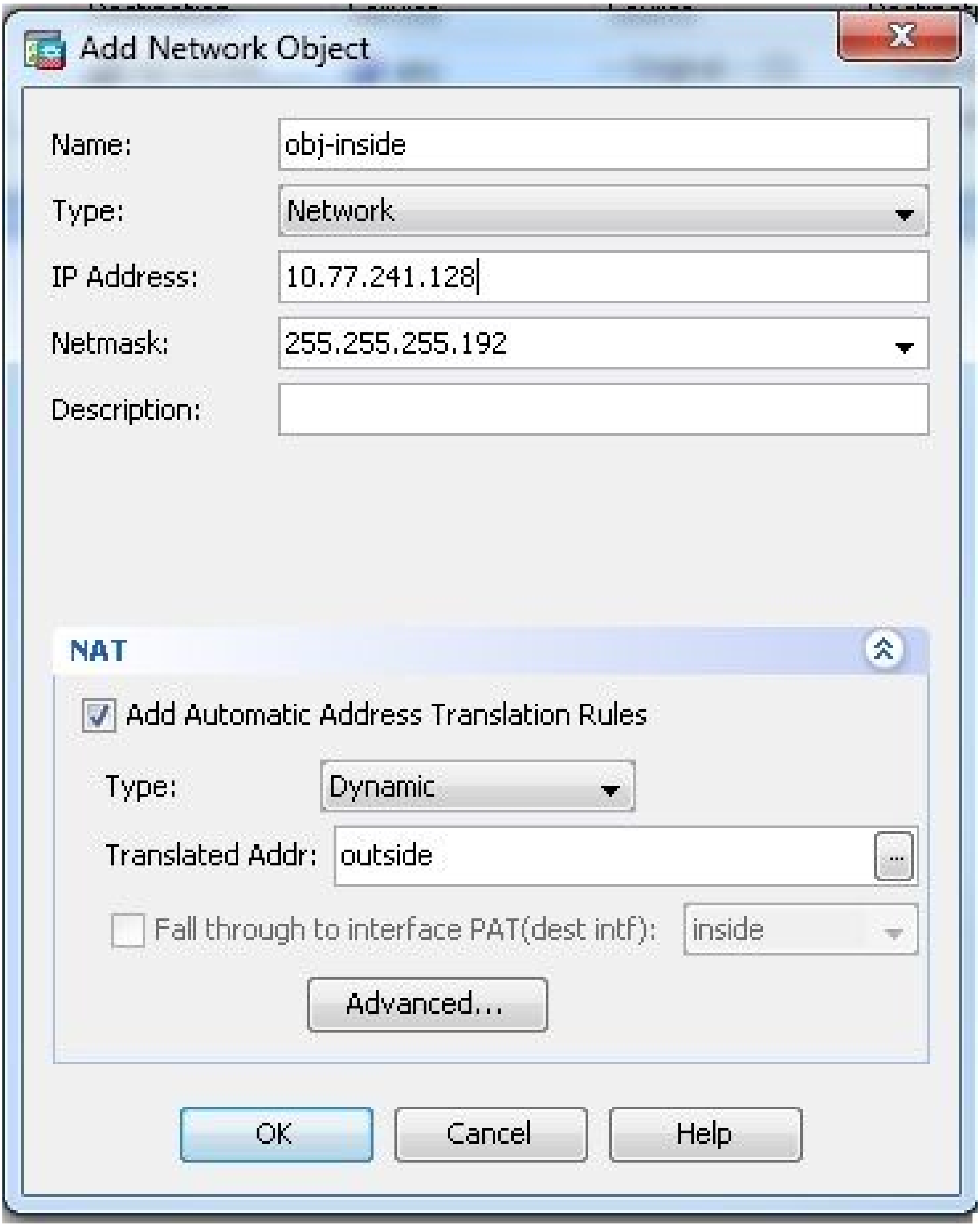
```
ciscoasa(config)#

tunnel-group sslgroup type remote-access


ciscoasa(config)#

tunnel-group sslgroup general-attributes
```

```
ciscoasa(config-tunnel-general)#

address-pool vpnpool

ciscoasa(config-tunnel-general)#

default-group-policy clientgroup

ciscoasa(config-tunnel-general)#

exit

ciscoasa(config)#

tunnel-group sslgroup webvpn-attributes

ciscoasa(config-tunnel-webvpn)#

group-alias sslgroup_users enable
```

8. Configure NAT
    a. Choose **Configuration** > **Firewall** > **NAT Rules** > **Add "Network Object" NAT Rule** so that the traffic from the inside network can be translated with outside IP address 172.16.1.1.



	Action: Translated Packet		
Service	Source	Destination	Service
any	-- Original -- (S)	-- Original --	-- Original --
any	-- Original -- (S)	-- Original --	-- Original --



Name: obj-inside

Type: Network

IP Address: 10.77.241.128

Netmask: 255.255.255.192

Description:

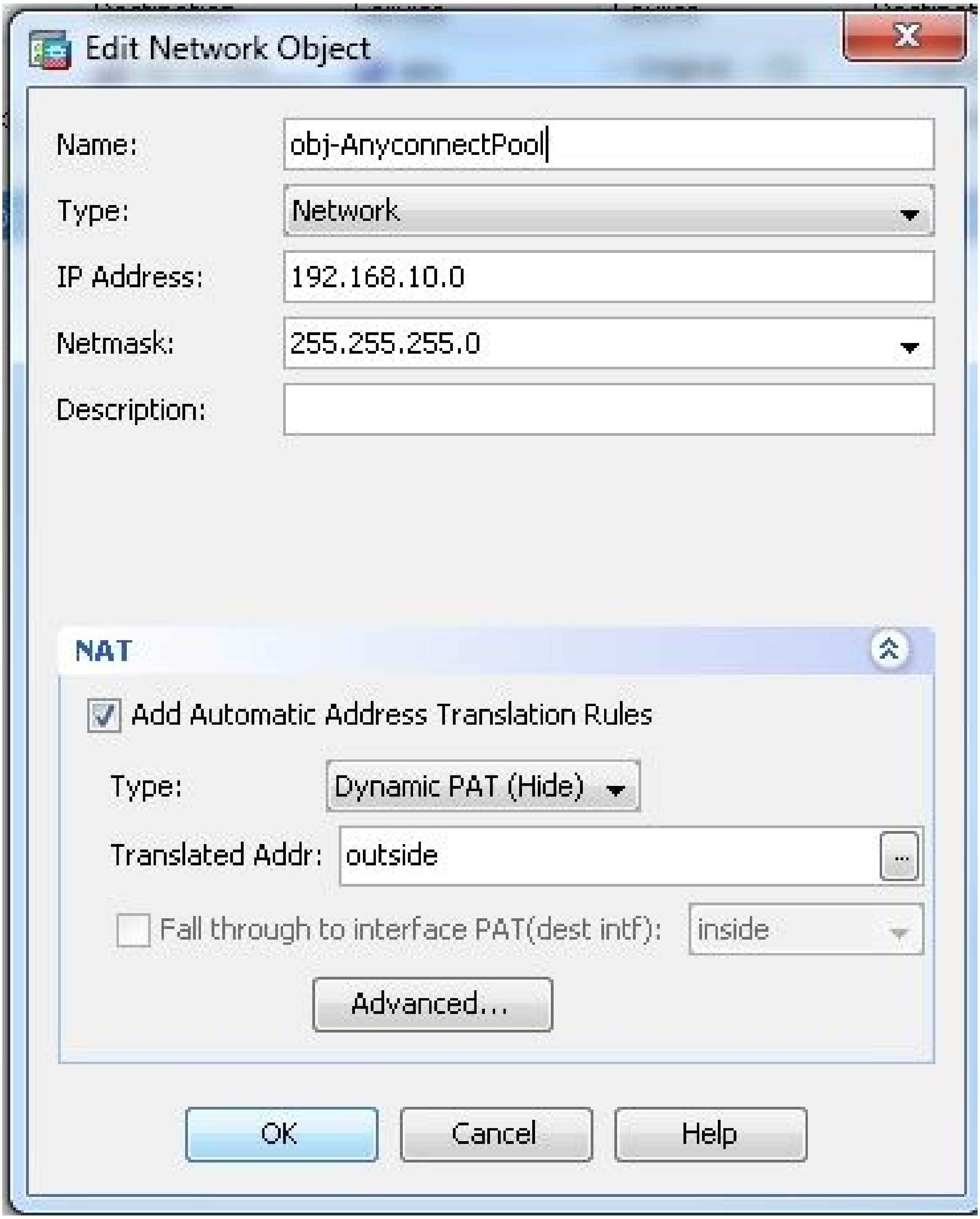
☑ Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: outside

□ Fall through to interface PAT(dest intf): inside

b. Choose **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** so the traffic that VPN traffic that comes from the outside network can be translated with outside IP address 172.16.1.1.



Edit Network Object

Name: obj-AnyconnectPool

Type: Network

IP Address: 192.168.10.0

Netmask: 255.255.255.0

Description:

NAT

☑ Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide)

Translated Addr: outside

□ Fall through to interface PAT(dest intf): inside

Equivalent CLI Configuration:

<#root>

```
ciscoasa(config)#
```

`object network obj-inside`

```
ciscoasa(config-network-object)#
```

`subnet 10.77.241.128 255.255.255.192`

```
ciscoasa(config-network-object)#

nat (inside,outside) dynamic interface
```

```
ciscoasa(config)#

object network obj-AnyconnectPool
```

```
ciscoasa(config-network-object)#

subnet 192.168.10.0 255.255.255.0
```

```
ciscoasa(config-network-object)#

nat (outside,outside) dynamic interface
```

ASA Release 9.1(2) Configuration in the CLI

<#root>

```
ciscoasa(config)#

show running-config
```

```
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address

!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
clock timezone IST 5 30
dns server-group DefaultDNS
```

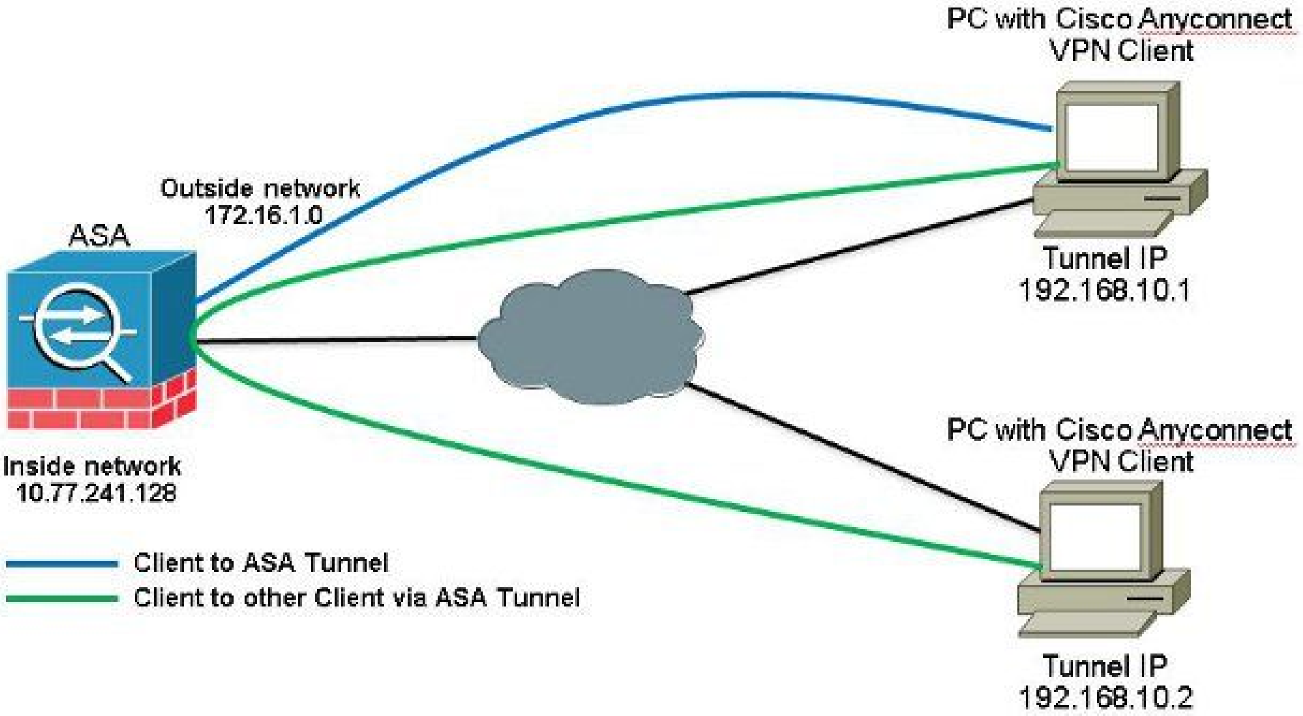
```
 domain-name default.domain.invalid
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool
 subnet 192.168.10.0 255.255.255.0
object network obj-inside
 subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0


!--- The address pool for the Cisco AnyConnect SSL VPN Clients


no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static
 obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated
 when going to the Anyconnect Pool.

object network obj-AnyconnectPool
 nat (outside,outside) dynamic interface
object network obj-inside
 nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and
 Anyconnect Clients.
!--- Note: Uses an RFC 1918 range for lab setup.

route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
```

```
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
webvpn
 enable outside


!--- Enable WebVPN on the outside interface


 anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect enable


!--- Enable the security appliance to download SVC images to remote computers


tunnel-group-list enable


!--- Enable the display of the tunnel-group list on the WebVPN Login page


group-policy clientgroup internal


!--- Create an internal group policy "clientgroup"


group-policy clientgroup attributes
 vpn-tunnel-protocol ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol
```

```
split-tunnel-policy tunnelall


!--- Encrypt all the traffic from the SSL VPN Clients.

username ssluser1 password ZRhW85jZqEaVd5P. encrypted


!--- Create a user account "ssluser1"


tunnel-group sslgroup type remote-access


!--- Create a tunnel group "sslgroup" with type as remote access


tunnel-group sslgroup general-attributes
 address-pool vpnpool


!--- Associate the address pool vpnpool created


 default-group-policy clientgroup


!--- Associate the group policy "clientgroup" created


tunnel-group sslgroup webvpn-attributes
 group-alias sslgroup_users enable


!--- Configure the group alias as sslgroup-users

prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#
```

Allow Communication between AnyConnect VPN Clients with the TunnelAll Configuration in Place

Network Diagram

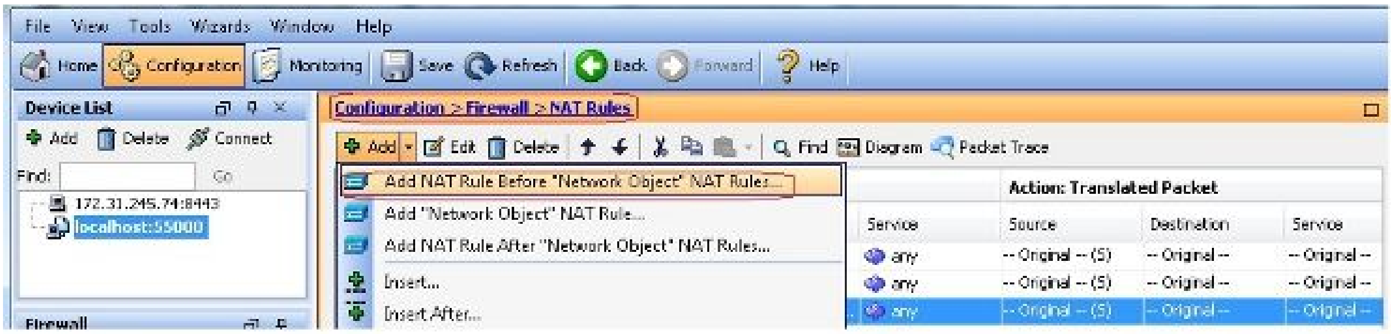

PC with Cisco Anyconnect VPN Client
Outside network 172.16.1.0
ASA
Tunnel IP 192.168.10.1
Inside network 10.77.241.128
PC with Cisco Anyconnect VPN Client
Client to ASA Tunnel
Client to other Client via ASA Tunnel
Tunnel IP 192.168.10.2

If communication between Anyconnect Clients is required and the NAT for Public Internet on a Stick is in place; a manual NAT is also needed to allow bidirectional communication.

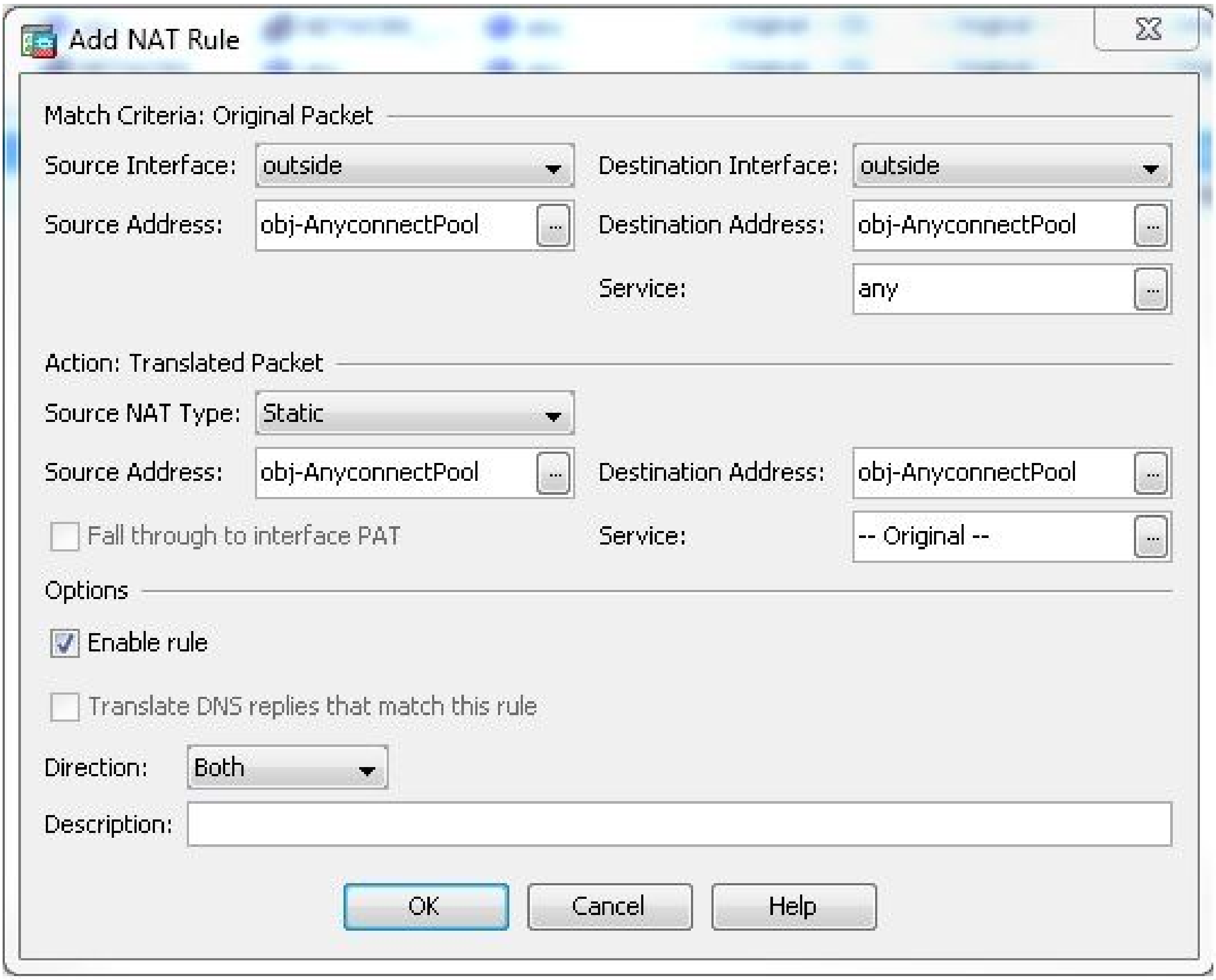
This is a common scenario when Anyconnect Clients use phone services and must be able to call each other.

ASA Release 9.1(2) Configurations with ASDM Release 7.1(6)

Choose **Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules** so that traffic from the outside network (Anyconect Pool) destined to another Anyconnect Client from the same pool does not get translated with outside IP address 172.16.1.1.


File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Add Delete Connect
Find: Go
172.31.245.74:8443
localhost:55000
Firewall
Configuration > Firewall > NAT Rules
Add Edit Delete Find Diagram Packet Trace
Add NAT Rule Before "Network Object" NAT Rules...
Add "Network Object" NAT Rule...
Add NAT Rule After "Network Object" NAT Rules...
Insert...
Insert After...

	Action: Translated Packet		
Service	Source	Destination	Service
any	-- Original -- (S)	-- Original --	-- Original --
any	-- Original -- (S)	-- Original --	-- Original --
any	-- Original -- (S)	-- Original --	-- Original --



Add NAT Rule

Match Criteria: Original Packet

Source Interface: outside

Destination Interface: outside

Source Address: obj-AnyconnectPool

Destination Address: obj-AnyconnectPool

Service: any

Action: Translated Packet

Source NAT Type: Static

Source Address: obj-AnyconnectPool

Destination Address: obj-AnyconnectPool

☐ Fall through to interface PAT

Service: -- Original --

Options

☑ Enable rule

☐ Translate DNS replies that match this rule

Direction: Both

Description:

Equivalent CLI Configuration:

<#root>

```
nat (outside,outside)

source static obj-AnyconnectPool obj-AnyconnectPool destination
 static obj-AnyconnectPool obj-AnyconnectPool
```

ASA Release 9.1(2) Configuration in the CLI

<#root>

```
ciscoasa(config)#

show running-config


: Saved
:
ASA Version 9.1(2)
!
```

```
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address

!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
clock timezone IST 5 30
dns server-group DefaultDNS
 domain-name default.domain.invalid
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool
 subnet 192.168.10.0 255.255.255.0
object network obj-inside
 subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0


!--- The address pool for the Cisco AnyConnect SSL VPN Clients



no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static
 obj-AnyconnectPool obj-AnyconnectPool
nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool
 destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT statements used so that traffic from the inside network
```

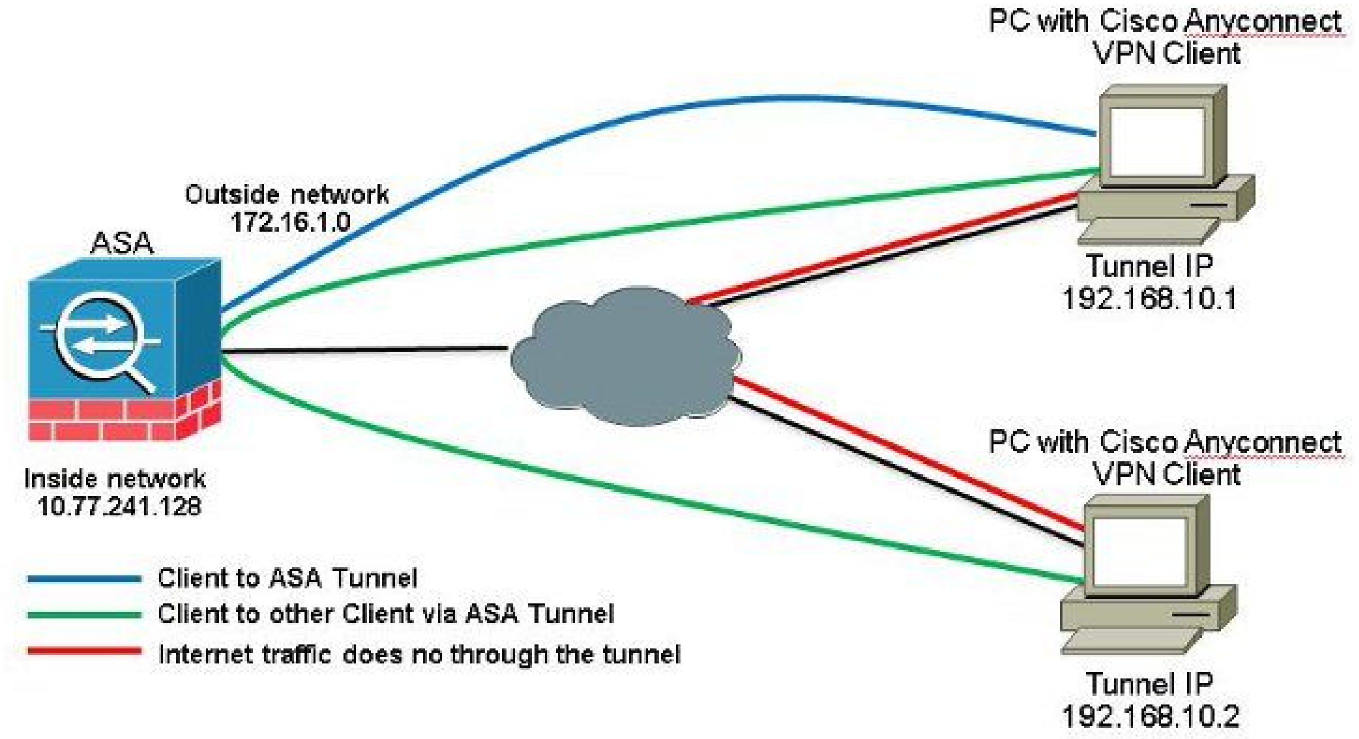
```
 destined to the Anyconnect Pool and traffic from the Anyconnect Pool destined
 to another Client within the same pool does not get translated.

object network obj-AnyconnectPool
 nat (outside,outside) dynamic interface
object network obj-inside
 nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and
 Anyconnect Clients.
!--- Note: Uses an RFC 1918 range for lab setup.

route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
webvpn
 enable outside


!--- Enable WebVPN on the outside interface
```

```
 anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect enable


!--- Enable the security appliance to download SVC images to remote computers


tunnel-group-list enable


!--- Enable the display of the tunnel-group list on the WebVPN Login page


group-policy clientgroup internal


!--- Create an internal group policy "clientgroup"


group-policy clientgroup attributes
 vpn-tunnel-protocol ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol


split-tunnel-policy tunnelall


!--- Encrypt all the traffic from the SSL VPN Clients.

username ssluser1 password ZRhW85jZqEaVd5P. encrypted


!--- Create a user account "ssluser1"


tunnel-group sslgroup type remote-access


!--- Create a tunnel group "sslgroup" with type as remote access


tunnel-group sslgroup general-attributes
 address-pool vpnpool


!--- Associate the address pool vpnpool created


 default-group-policy clientgroup


!--- Associate the group policy "clientgroup" created
```

```
tunnel-group sslgroup webvpn-attributes
 group-alias sslgroup_users enable


!--- Configure the group alias as sslgroup-users

prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#
```

Allow Communication between AnyConnect VPN Clients with Split-Tunnel

Network Diagram


PC with Cisco Anyconnect VPN Client
Outside network 172.16.1.0
ASA
Tunnel IP 192.168.10.1
Inside network 10.77.241.128
PC with Cisco Anyconnect VPN Client
Client to ASA Tunnel
Client to other Client via ASA Tunnel
Internet traffic does no through the tunnel
Tunnel IP 192.168.10.2

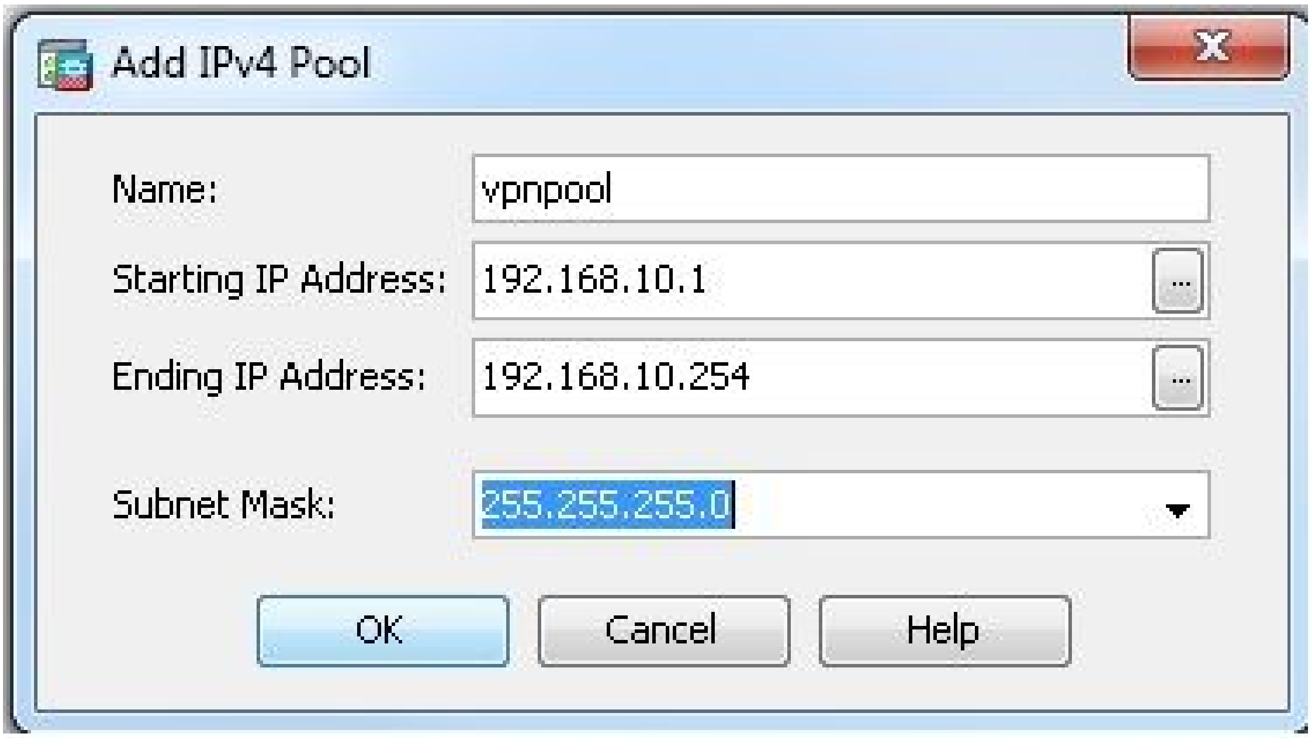
If communication between Anyconnect Clients is required and Split-Tunnel is used, no manual NAT is required in order to allow bidirectional communication unless there is a NAT rule that affects this traffic configured.

However the Anyconnect VPN Pool must be included on the Split-Tunnel ACL.

This is a common scenario when Anyconnect Clients use phone services and must be able to call each other.

ASA Release 9.1(2) Configurations with ASDM Release 7.1(6)

1. Choose **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment> Address Pools > Add** in order to create an IP address pool **vpnpool**.



Add IPv4 Pool

Name: vpnpool

Starting IP Address: 192.168.10.1

Ending IP Address: 192.168.10.254

Subnet Mask: 255.255.255.0

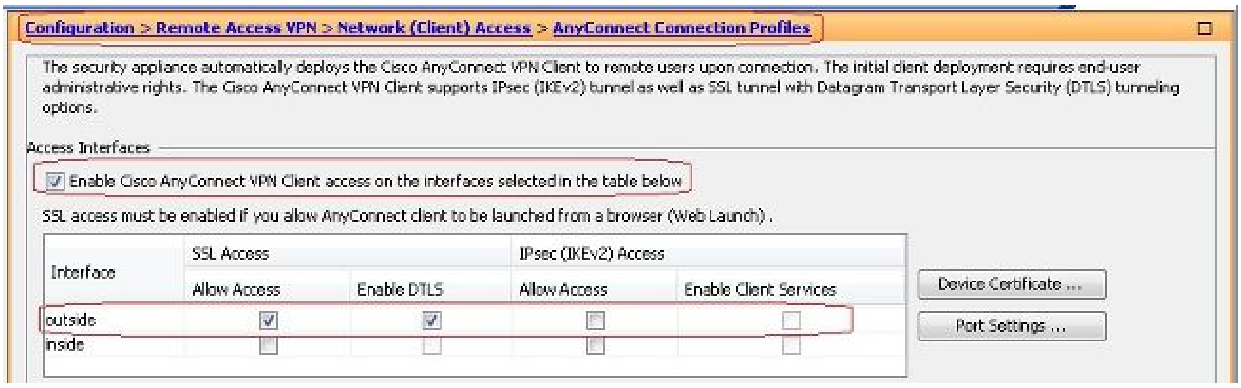
2. Click **Apply**.

Equivalent CLI Configuration:

<#root>

```
ciscoasa(config)#

ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
```

3. Enable WebVPN.
    a. Choose **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** and under **Access Interfaces**, click the check boxes **Allow Access** and **Enable DTLS** for the outside interface. Also, check the **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** check box in order to enable SSL VPN on the outside interface.



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

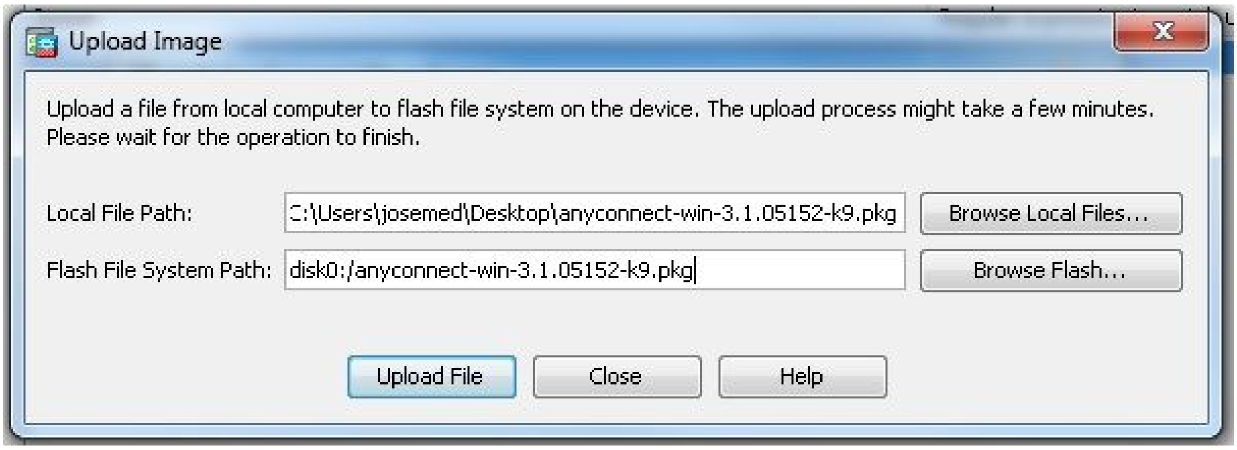
Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	□	□
inside	□	□	□	□

    b. Click **Apply**.
    c. Choose **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** in order to add the Cisco AnyConnect VPN client image from the flash memory of ASA as shown.

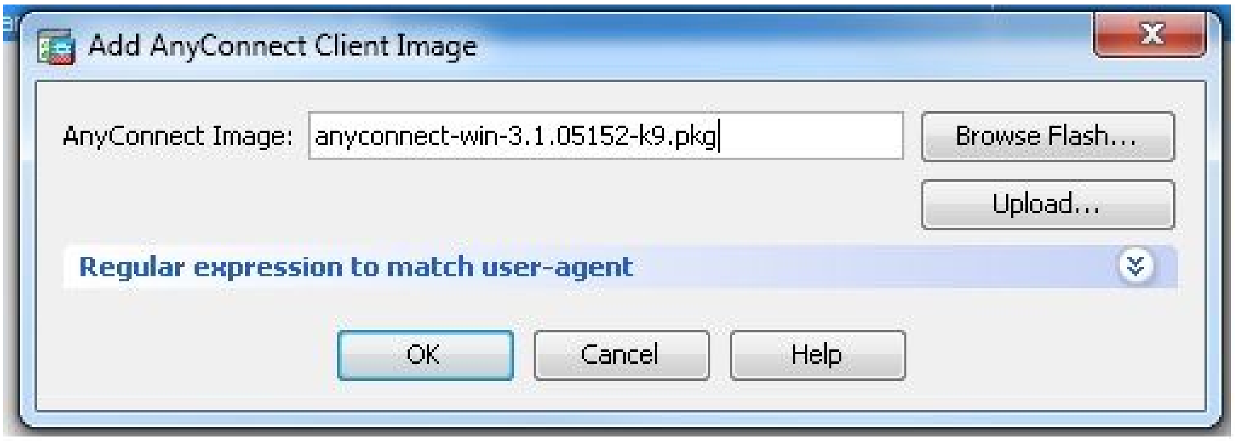


Upload Image

Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.

Local File Path: C:\Users\josemed\Desktop\anyconnect-win-3.1.05152-k9.pkg

Flash File System Path: disk0:/anyconnect-win-3.1.05152-k9.pkg



Add AnyConnect Client Image

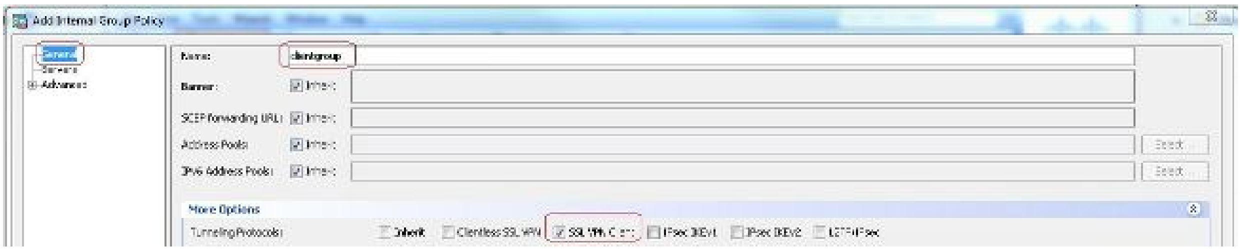
AnyConnect Image: anyconnect-win-3.1.05152-k9.pkg

Equivalent CLI Configuration:

<#root>

```
ciscoasa(config)#

webvpn

ciscoasa(config-webvpn)#

enable outside

ciscoasa(config-webvpn)#

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

ciscoasa(config-webvpn)#

tunnel-group-list enable

ciscoasa(config-webvpn)#

anyconnect enable
```

4. Configure Group Policy.
    a. Choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** in order to create an internal group policy **clientgroup**. Under the **General** tab, select the **SSL VPN Client** check box in order to enable the WebVPN as an allowed tunnel protocol.



Add Internal Group Policy

Name: clientgroup

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

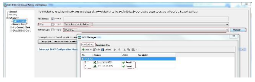
Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit □ Clientless SSL VPN ☑ SSL VPN Client □ IPsec IKEv1 □ IPsec IKEv2 □ L2TP/IPsec

    b. In the **Advanced** > **Split Tunneling** tab, choose **Tunnel Network List Below** from the Policy drop-down list in order to make all the packets from the remote PC through a secure tunnel.

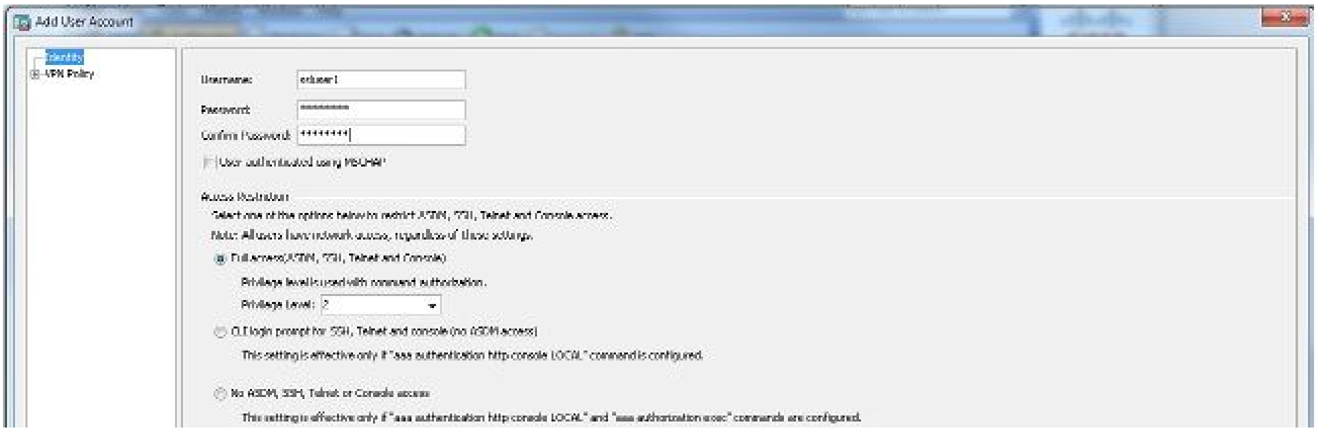


Equivalent CLI Configuration:

<#root>

```
ciscoasa(config)#

access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0


ciscoasa(config)#

access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0


ciscoasa(config)#

group-policy clientgroup internal


ciscoasa(config)#

group-policy clientgroup attributes


ciscoasa(config-group-policy)#

vpn-tunnel-protocol ssl-client


ciscoasa(config-group-policy)#

split-tunnel-policy tunnelspecified


ciscoasa(config-group-policy)#

split-tunnel-network-list SPLIt-ACL
```

5. Choose **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **Local Users** > **Add** in order to create a new user account **ssluser1**. Click **OK** and then **Apply**.



Add User Account

Username: ssluser1

Password: *********

Confirm Password: ********

□ User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.

Note: All users have network access, regardless of these settings.

● Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 2

○ CLI login prompt for SSH, Telnet and console (no ASDM access)

This setting is effective only if "aaa authentication http console LOCAL" command is configured.

○ No ASDM, SSH, Telnet or Console access

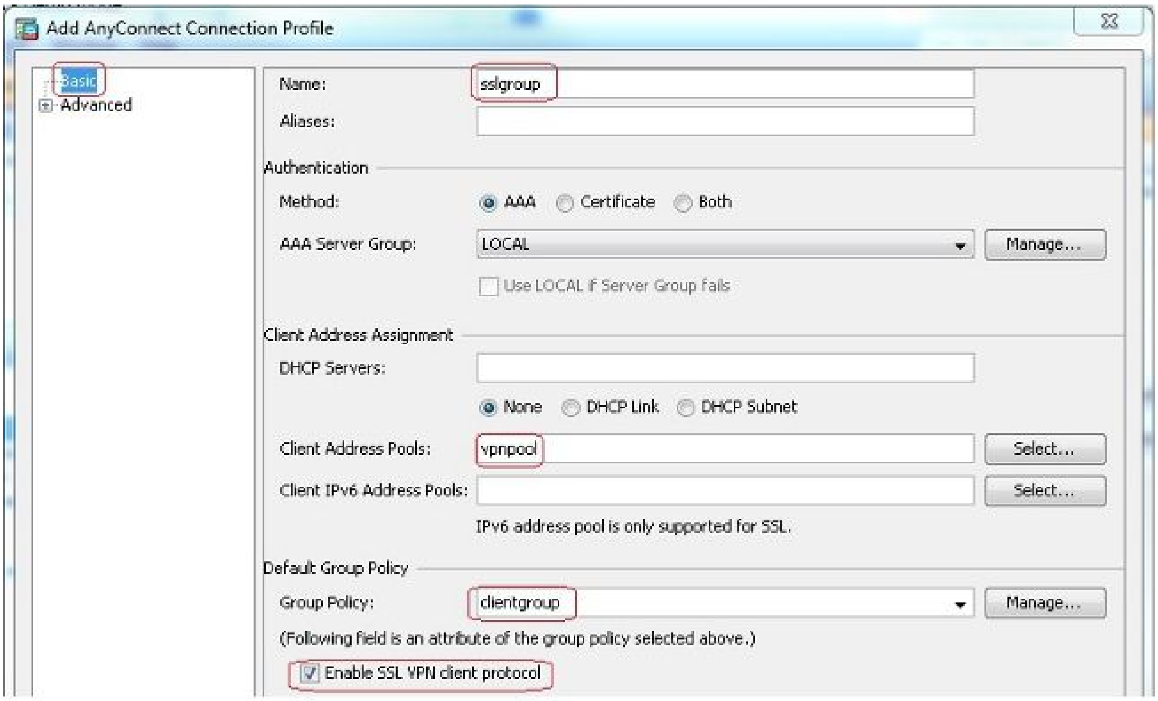
This setting is effective only if "aaa authentication http console LOCAL" and "aaa authorization exec" commands are configured.

Equivalent CLI Configuration:

<#root>

```
ciscoasa(config)#

username ssluser1 password asdmASA@
```

6. Configure Tunnel Group.
   a. Choose **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** in order to create a new tunnel group **sslgroup**.
   b. In the **Basic** tab, you can perform the list of configurations as shown:
      - Name the Tunnel group as **sslgroup**.
      - Under **Client Address Assignment**, choose the address pool **vpnpool** from the **Client Address Pools** drop-down list.
      - Under **Default Group Policy**, choose the group policy **clientgroup** from the **Group Policy** drop-down list.



Add AnyConnect Connection Profile

Name: sslgroup

Aliases:

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: vpnpool

Client IPv6 Address Pools:

IPv6 address pool is only supported for SSL.

Default Group Policy

Group Policy: clientgroup

(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN client protocol

- Under the **Advanced > Group Alias/Group URL** tab, specify the group alias name as **sslgroup_users** and click **OK**.

Equivalent CLI Configuration:

```
<#root>

ciscoasa(config)#

tunnel-group sslgroup type remote-access

ciscoasa(config)#

tunnel-group sslgroup general-attributes

ciscoasa(config-tunnel-general)#

address-pool vpnpool

ciscoasa(config-tunnel-general)#

default-group-policy clientgroup

ciscoasa(config-tunnel-general)#

exit

ciscoasa(config)#

tunnel-group sslgroup webvpn-attributes

ciscoasa(config-tunnel-webvpn)#

group-alias sslgroup_users enable
```

ASA Release 9.1(2) Configuration in the CLI

```
<#root>

ciscoasa(config)#

show running-config

: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
```

```
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address

!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
clock timezone IST 5 30
dns server-group DefaultDNS
 domain-name default.domain.invalid
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-inside
 subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0
access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

!--- Standard Split-Tunnel ACL that determines the networks that should travel the
 Anyconnect tunnel.

pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN Clients

no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static
 obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated when
 going to the Anyconnect Pool

object network obj-inside
 nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users.
!--- Note: Uses an RFC 1918 range for lab setup.

route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
webvpn
 enable outside


!--- Enable WebVPN on the outside interface


 anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect enable


!--- Enable the security appliance to download SVC images to remote computers


tunnel-group-list enable
```

```
!--- Enable the display of the tunnel-group list on the WebVPN Login page


group-policy clientgroup internal


!--- Create an internal group policy "clientgroup"


group-policy clientgroup attributes
 vpn-tunnel-protocol ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol


split-tunnel-policy tunnelspecified


!--- Encrypt  only traffic specified on the split-tunnel ACL coming from the SSL
 VPN Clients.


split-tunnel-network-list value SPLIt-ACL


!--- Defines the previosly configured ACL to the split-tunnel policy.

username ssluser1 password ZRhW85jZqEaVd5P. encrypted


!--- Create a user account "ssluser1"


tunnel-group sslgroup type remote-access


!--- Create a tunnel group "sslgroup" with type as remote access


tunnel-group sslgroup general-attributes
 address-pool vpnpool


!--- Associate the address pool vpnpool created


 default-group-policy clientgroup


!--- Associate the group policy "clientgroup" created


tunnel-group sslgroup webvpn-attributes
 group-alias sslgroup_users enable


!--- Configure the group alias as sslgroup-users

prompt hostname context
```

```
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#
```

Verify

Use this section to confirm that your configuration works properly.

- **show vpn-sessiondb svc** - Displays the information about the current SSL connections.

  <#root>

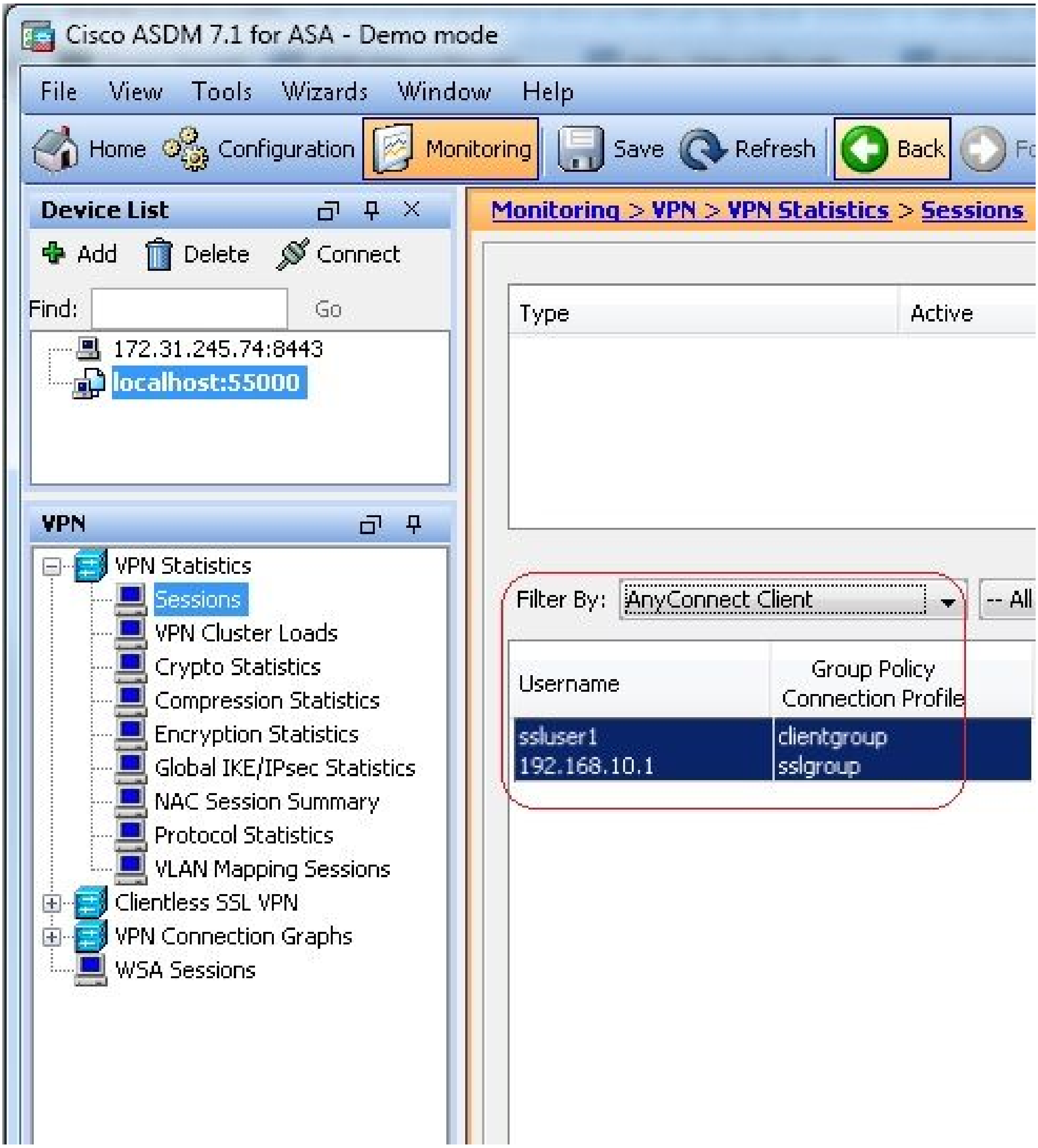
  ```
  ciscoasa#

  show vpn-sessiondb anyconnect



  Session Type: SVC

  Username     :

  ssluser1

                 Index        : 12
  Assigned IP  :

  192.168.10.1

            Public IP    :

  192.168.1.1


  Protocol     :

  Clientless SSL-Tunnel DTLS-Tunnel


  Encryption   :

  RC4 AES128

               Hashing      :

  SHA1


  Bytes Tx     : 194118                Bytes Rx     : 197448
  Group Policy :

  clientgroup

            Tunnel Group :

  sslgroup


  Login Time   : 17:12:23 IST Mon Mar 24 2008
  Duration     : 0h:12m:00s
  NAC Result   : Unknown
  VLAN Mapping : N/A                   VLAN         : none
  ```

- **show webvpn group-alias** - Displays the configured alias for various groups.

  <#root>

  ```
  ciscoasa#
  show webvpn group-alias

  Tunnel Group:
  sslgroup
     Group Alias:
  sslgroup_users enabled
  ```

- In ASDM, choose **Monitoring** > **VPN** > **VPN Statistics** > **Sessions** in order to know the current sessions in the ASA.



Filter By: AnyConnect Client

Username	Group Policy Connection Profile
ssluser1 192.168.10.1	clientgroup sslgroup

Troubleshoot

This section provides information to troubleshoot your configuration.

- **vpn-sessiondb logoff name <username>** - Command to log off the SSL VPN session for the particular username.

  ```
  <#root>

  ciscoasa#

  vpn-sessiondb logoff name ssluser1
  ```

```
Do you want to logoff the VPN session(s)? [confirm]

Y


INFO: Number of sessions with name "ssluser1" logged off : 1


ciscoasa#

Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xB000)
```

Similarly, you can use the **vpn-sessiondb logoff anyconnect** command in order to terminate all the AnyConnect sessions.

- **debug webvpn anyconnect <1-255>** - Provides the real time webvpn events in order to establish the session.

<#root>

```
Ciscoasa#

debug webvpn anyconnect 7


CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.198.16.132'
Processing CSTP header line: 'Host: 10.198.16.132'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.05152'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows
3.1.05152'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.1.05152'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Processing CSTP header line: 'Cookie: webvpn=
146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Found WebVPN cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
WebVPN Cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: WCRSJOW7Pnbc038'
Processing CSTP header line: 'X-CSTP-Hostname: WCRSJOW7Pnbc038'
Setting hostname to: 'WCRSJOW7Pnbc038'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1280'
Processing CSTP header line: 'X-CSTP-MTU: 1280'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
```

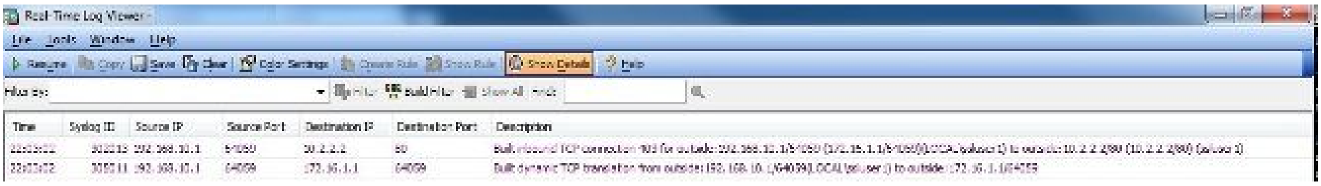
```
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1300'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1300'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0A602CF075972F91EAD1
9BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
Processing CSTP header line: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0
A602CF075972F91EAD19BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3
 -SHA:DES-CBC-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/255.255.255.0
webvpn_cstp_accept_ipv6_address: No IPv6 Address
CSTP state = HAVE_ADDRESS
SVC: Sent gratuitous ARP for 192.168.10.1.
SVC: NP setup
np_svc_create_session(0x5000, 0xa930a180, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.1!
No SVC ACL
Iphdr=20 base-mtu=1300 def-mtu=1500 conf-mtu=1406
tcp-mss = 1260
path-mtu = 1260(mss)
mtu = 1260(path-mtu) - 0(opts) - 5(ssl) - 8(cstp) = 1247
tls-mtu = 1247(mtu) - 20(mac) = 1227
DTLS Block size = 16
mtu = 1300(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1243
mod-mtu = 1243(mtu) & 0xfff0(complement) = 1232
dtls-mtu = 1232(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1210
computed tls-mtu=1227 dtls-mtu=1210 conf-mtu=1406
DTLS enabled for intf=2 (outside)
tls-mtu=1227 dtls-mtu=1210
SVC: adding to sessmgmt

Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state =
```

CONNECTED

```
webvpn_rx_data_cstp
```

```
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy
```

- In ASDM, choose **Monitoring** > **Logging** > **Real-time Log Viewer** > **View** in order to see the real time events. This example shows the session information between the AnyConnect 192.168.10.1 and Telnet Server10.2.2.2 in the Internet via ASA 172.16.1.1.


Real-Time Log Viewer
File Tools Window Help
Resume Copy Save Clear Color Settings Create Rule Show Rule Show Details Help
Filter By:
Filter Build Filter Show All Find:

Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
22:03:02	302013	192.168.10.1	64059	10.2.2.2	80	Built inbound TCP connection 103 for outside:192.168.10.1/64059 (172.16.1.1/64059)(LOCAL\ssluser1) to outside:10.2.2.2/80 (10.2.2.2/80) (ssluser1)
22:03:02	305011	192.168.10.1	64059	172.16.1.1	64059	Built dynamic TCP translation from outside:192.168.10.1/64059(LOCAL\ssluser1) to outside:172.16.1.1/64059

Related Information

- **Cisco ASA 5500-X Series Firewalls**
- **PIX/ASA and VPN Client for Public Internet VPN on a Stick Configuration Example**
- **SSL VPN Client (SVC) on ASA with ASDM Configuration Example**
- **Technical Support & Documentation - Cisco Systems**