在ASA 9.X上配置AnyConnect VPN客户端U-turn流量

目录

简介

本文档介绍如何设置思科自适应安全设备(ASA)版本9.X以允许它回转VPN流量。它涵盖以下配置场景：从远程访问客户端调头流量。

> **注意：** 为了避免网络中的 IP 地址重叠，请为 VPN 客户端分配一个完全不同的 IP 地址池（例如 10.x.x.x、172.16.x.x 和 192.168.x.x）。 此IP地址方案有助于排除网络故障。

发夹或U形转弯

此功能对于进入接口但随后从同一接口路由出去的VPN流量非常有用。例如，如果您有一个中心辐射型VPN网络，其中安全设备是中心，而远程VPN网络是分支，为了使一个分支与另一个分支通信，必须转到安全设备，然后再次转到另一个分支。

输入 **same-security-traffic** 命令，以允许流量进出同一接口。

```
ciscoasa(config)#same-security-traffic permit intra-interface
```

先决条件

要求

Cisco建议您在尝试此配置之前满足以下要求：

- 中心ASA安全设备需要运行版本9.x。
- Cisco AnyConnect VPN客户端3.x**注意：**下载AnyConnect VPN客户端软件包(anyconnect-win*.pkg)下载思科软件(仅限注册客户)。 将AnyConnect VPN客户端复制到Cisco ASA闪存，该闪存将下载到远程用户计算机，以便与ASA建立SSL VPN连接。有关详细信息，请参阅ASA配置指南的AnyConnect VPN客户端连接部分。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 9.1(2) 的 Cisco 5500 系列 ASA
- 用于 Windows 的 Cisco AnyConnect SSL VPN Client 版本 3.1.05152
- PC按照受支持的VPN平台Cisco ASA系列运行受支持的OS。
- Cisco 自适应安全设备管理器 (ASDM) 版本 7.1(6)

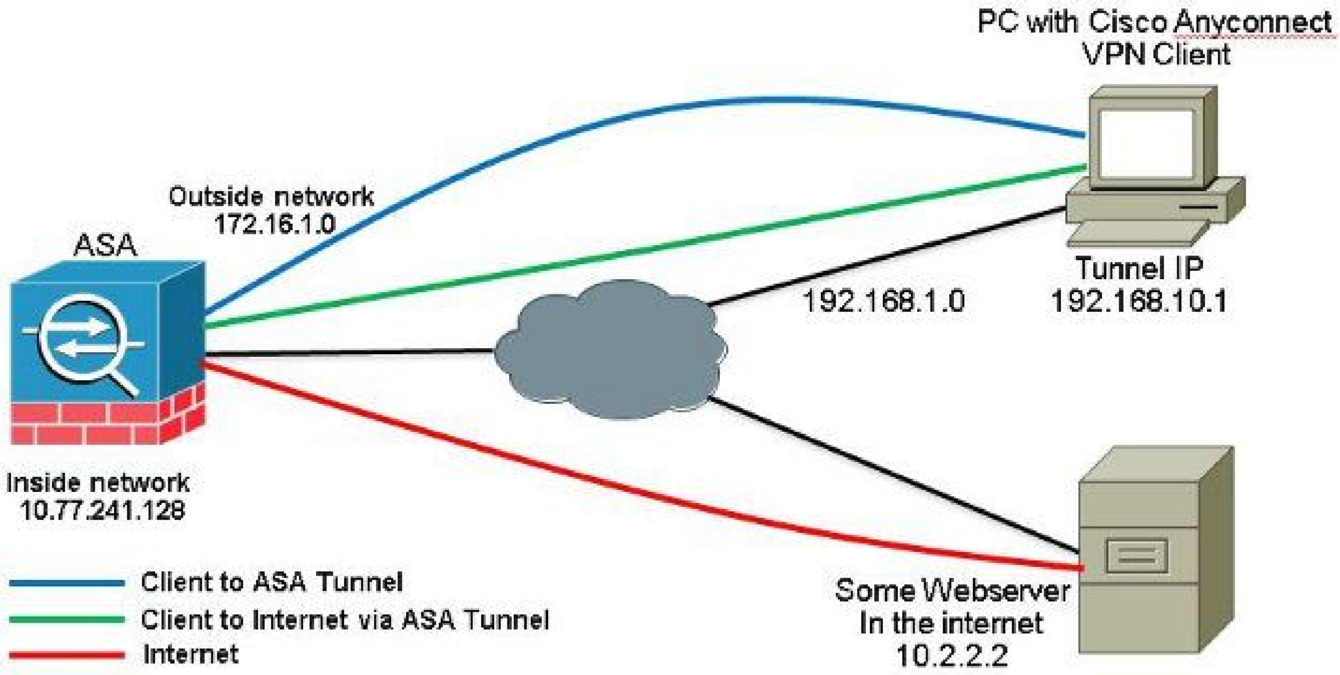
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco AnyConnect VPN Client 为远程用户的安全设备提供了安全的 SSL 连接。如果以前未安装客户端，则远程用户可以在浏览器中输入已配置为接受 SSL VPN 连接的接口的 IP 地址。除非安全设备配置为重定向 **http://** 请求 **https://**，用户必须在表格中输入URL **https://**

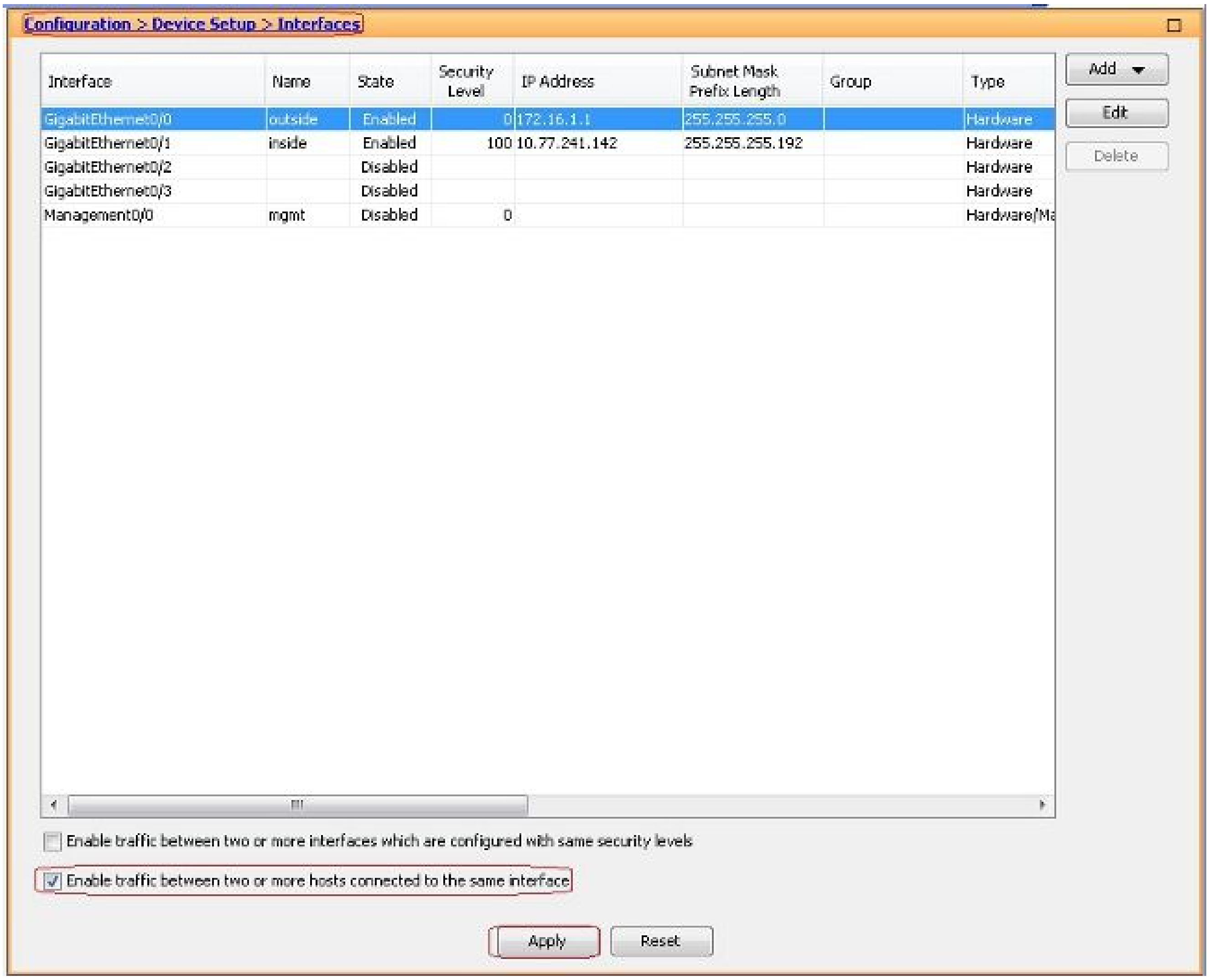
*.输入URL后，浏览器会连接到该接口并显示登录屏幕。如果用户满足登录和身份验证要求，并且安全设备将用户识别为需要客户端，则它会下载与远程计算机的操作系统匹配的客户端。下载后，客户端将自行安装和配置，建立安全SSL连接，并在连接终止时保留或卸载自身（这取决于安全设备配置）。如果以前安装了客户端，则当用户验证身份时，安全设备将会检查客户端的版本，并根据需要升级客户端。当客户端与安全设备协商SSL VPN连接时，它会与传输层安全(TLS)连接，并且还会使用数据报传输层安全(DTLS)。DTLS可避免与某些SSL连接相关的延迟和带宽问题，并提高对数据包延迟敏感的实时应用的性能。AnyConnect 客户端可以从安全设备下载，或者可以由系统管理员手动安装到远程 PC 上。有关如何手动安装客户端的详细信息，请参阅Cisco AnyConnect安全移动客户端管理员指南。安全设备根据建立连接的用户的组策略或用户名属性下载客户端。您可以配置安全设备自动下载客户端，或者将其配置为提示远程用户选择是否下载客户端。在后一种情况下，如果用户不响应，您可以配置安全设备在超时时间后下载客户端或显示登录页。**注意：**本文档中使用的示例使用IPv4。对于IPv6 U-turn流量，步骤相同，但使用IPv6地址而不是IPv4。**配置翻转远程访问流量**本部分提供有关如何配置本文档所述功能的信息。注意：请使用命令参考指南获取有关本节中使用的命令的详细信息。公共 Internet VPN 的单接口 AnyConnect VPN 客户端的配置示例网络图本文档使用以下网络设置*

：



ASA 9.1(2)版本配置与ASDM 7.1(6)版本本文档假设基本配置（如接口配置）已经完成并正常运行。注意：要允许ASDM配置ASA，请参阅配置管理访问。注意：在版本8.0(2)及更高版本中，ASA在外部接口的端口443上同时支持无客户端SSL VPN(WebVPN)会话和ASDM管理会话。在8.0(2)之前的版本中，除非更改端口号，否则不能在同一个ASA接口上启用WebVPN和ASDM。有关详细信息，请参阅在ASA的同一接口上启用ASDM和WebVPN。要在 ASA 的单接口上配置 SSL VPN，请执行以下步骤：

1. *选择* **Configuration > Device Setup > Interfaces** *并查看* **Enable traffic between two or more hosts connected to the same interface** *复选框以允许SSL VPN流量进入和退出同一接口。点击* **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

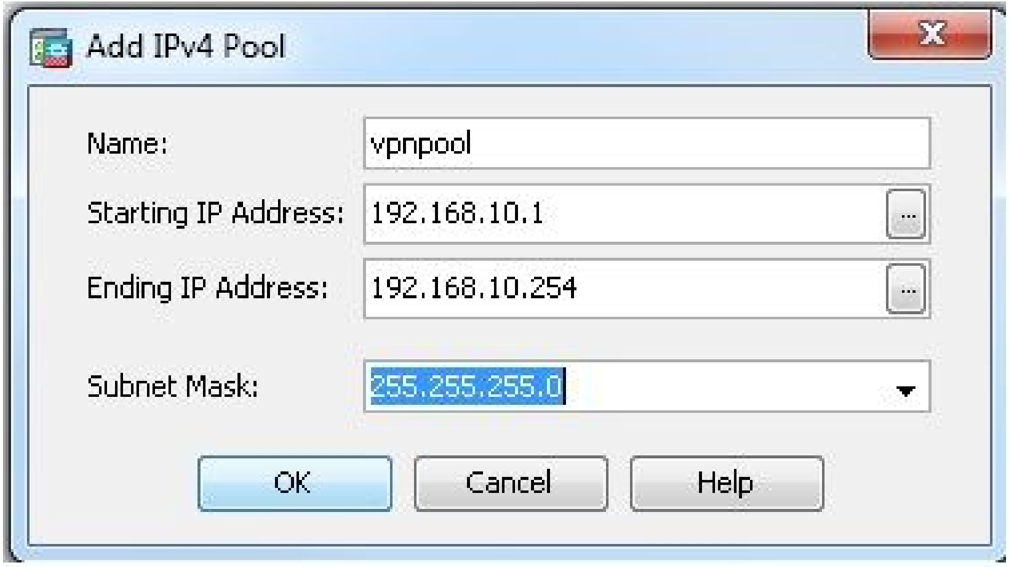
☐ Enable traffic between two or more interfaces which are configured with same security levels

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

等效 CLI 配置：

```
ciscoasa(config)#same-security-traffic permit intra-interface
```

2. *选择* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add** *创建IP地址池* **vpnpool**.



Name: vpnpool

Starting IP Address: 192.168.10.1

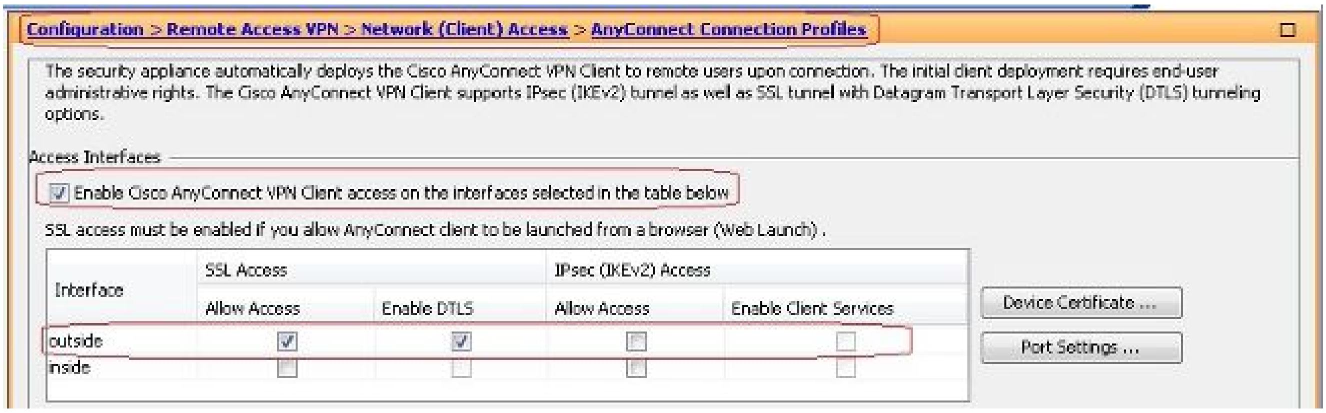
Ending IP Address: 192.168.10.254

Subnet Mask: 255.255.255.0

3. *点击* **Apply**. ***等效 CLI 配置：***

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

4. *启用 Webvpn。 选择* **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** *和* **Access Interfaces** *，单击复选框* **Allow Access** *和* **Enable DTLS** *外部接口。此外，请查看* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *复选框以在外部接口上启用SSL VPN。*



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.

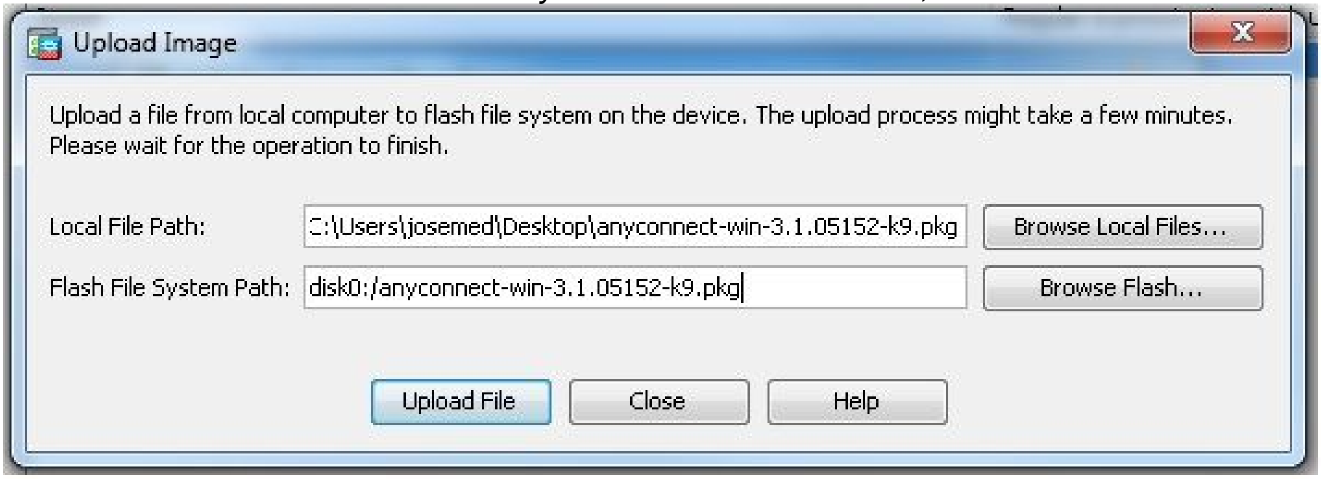
Access Interfaces

☑ 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	□	□	□	□

点击 **Apply**.选择 **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** 以便从ASA的闪存中添加Cisco AnyConnect VPN客户端映像，如下所示。

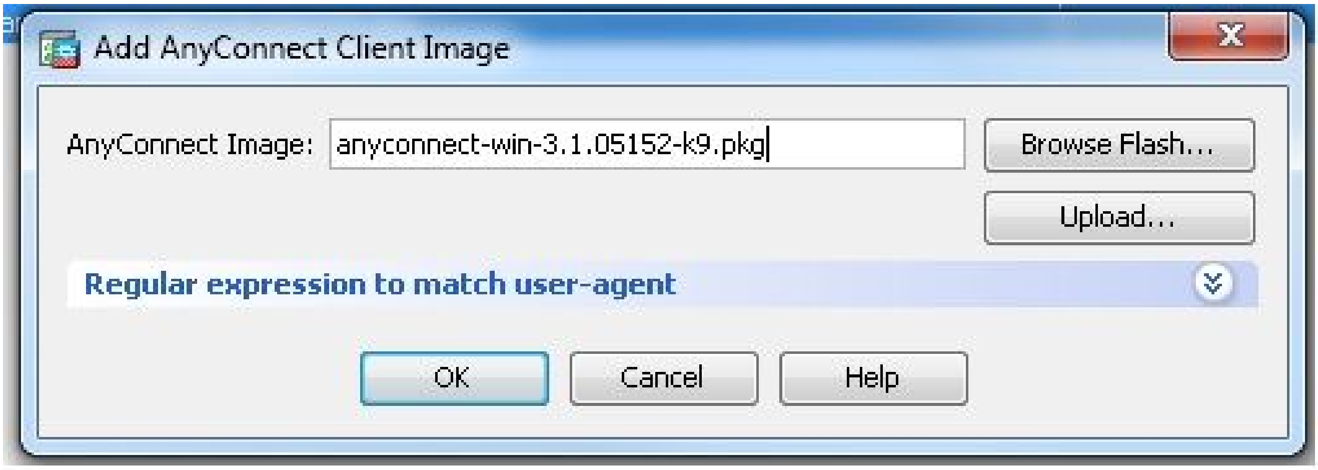


Upload Image

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



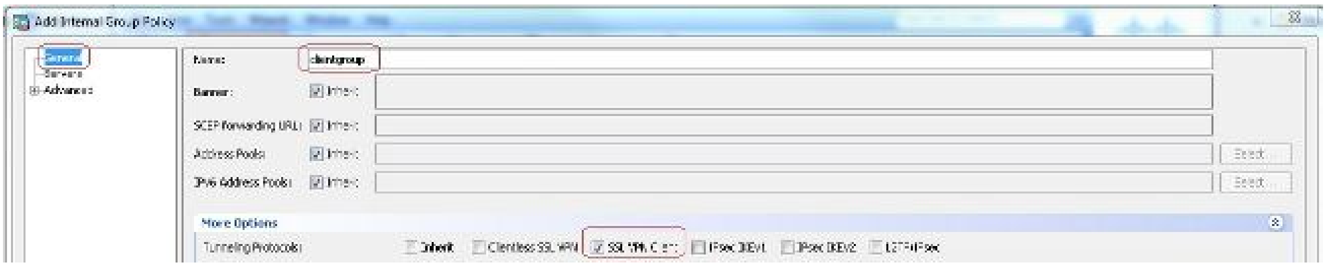
Add AnyConnect Client Image

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

等效 CLI 配置：

```
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. 配置组策略。 选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** 创建内部组策略 **clientgroup**.在 **General** 选项卡，选择 **SSL VPN Client** 复选框以启用WebVPN作为隧道协议。



Add Internal Group Policy

Name: clientgroup

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

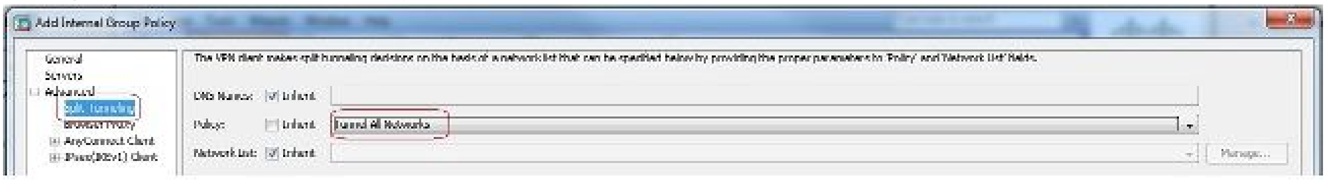
Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

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

如果 **Advanced > Split Tunneling** *选项卡，选择* **Tunnel All Networks** *从策略的Policy下拉列表中，使来自远程PC的所有数据包通过安全隧道。*



Add Internal Group Policy

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

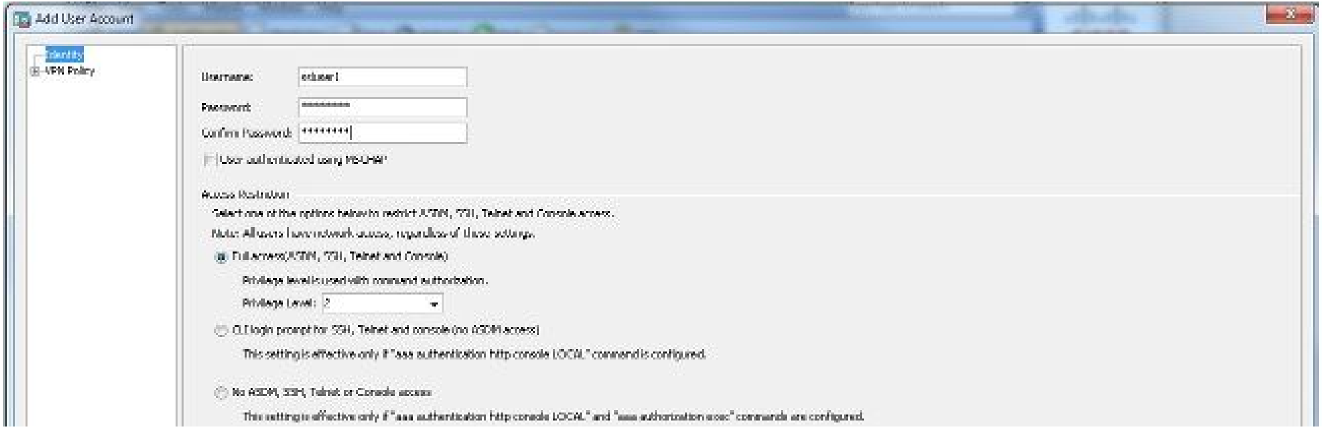
The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network List' fields.

DNS Names: ☑ Inherit
Policy: □ Inherit Tunnel All Networks
Network List: ☑ Inherit

等效 CLI 配置：

```
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. *选择* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *创建新用户帐户* **ssluser1**.*点击* **OK** *然后* **Apply**.



Add User Account

Identity
VPN Policy

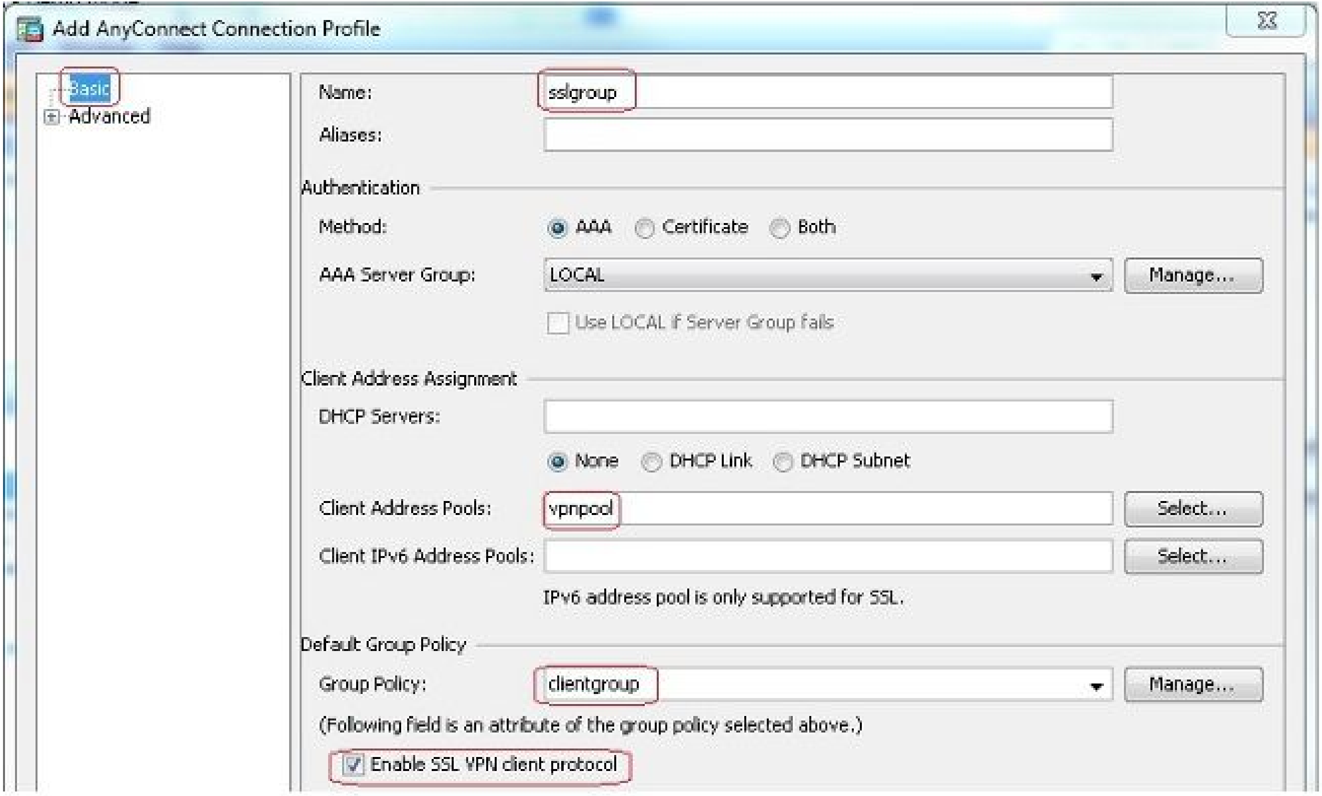
Username: ssluser1
Password: ********
Confirm Password: ********
□ User authenticated using MSCHAP

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.

等效 CLI 配置：

```
ciscoasa(config)#username ssluser1 password asdmASA@
```

7. *配置隧道组。 选择* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *创建新隧道组* **sslgroup**.*如果* **Basic** *选项卡中，您可以按如下所示执行配置列表： 将隧道组命名为* **sslgroup**.*低于* **Client Address Assignment**，*选择地址池* **vpnpool** *从* **Client Address Pools** *下拉列表。低于* **Default Group Policy**，*选择组策略* **clientgroup** *从* **Group Policy** *下拉列表。*



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.

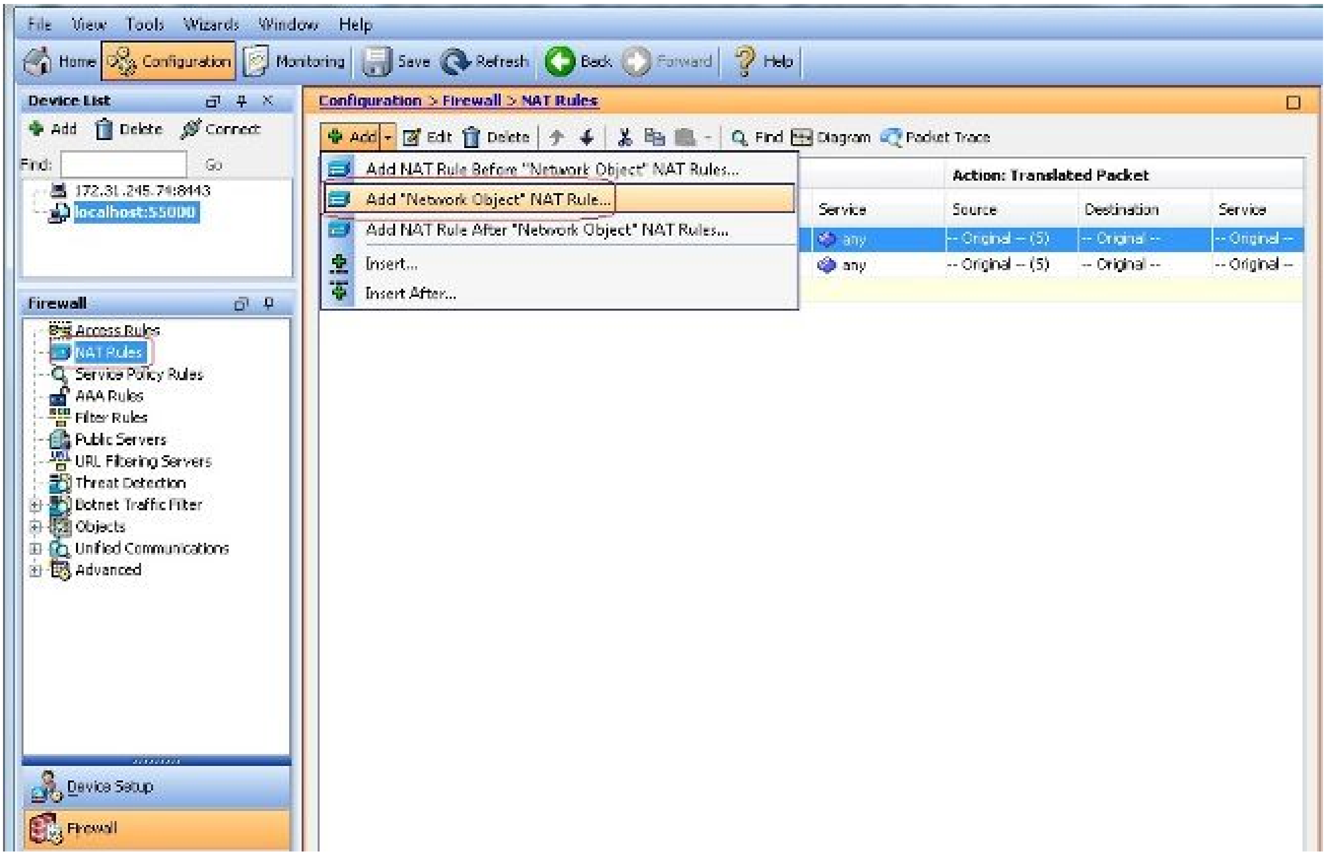
Default Group Policy
Group Policy: clientgroup
(Following field is an attribute of the group policy selected above.)
☑ Enable SSL VPN client protocol

在 **Advanced > Group Alias/Group URL** *选项卡，将组别名指定为* **sslgroup_users** *并点击* **OK**. ***等效 CLI***

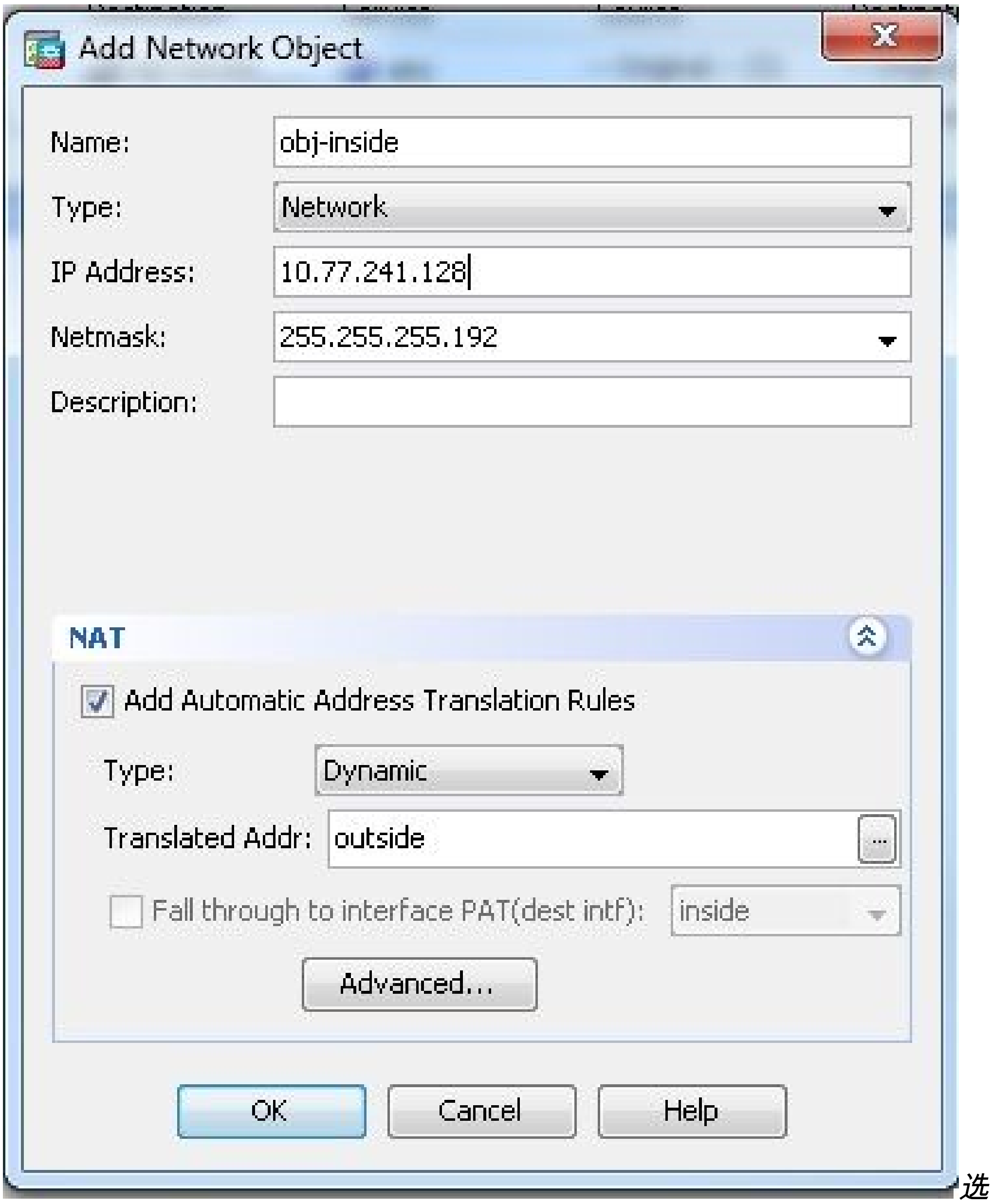
配置：

```
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. *配置 NAT 选择* **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *因此，来自内部网络的流量可以使用外部IP地址172.16.1.1进行转换。*



	Action: Translated Packet		
Service	Source	Destination	Service
any	-- Original -- (5)	-- Original --	-- Original --
any	-- Original -- (5)	-- Original --	-- Original --



Add Network Object

Name: obj-inside

Type: Network

IP Address: 10.77.241.128

Netmask: 255.255.255.192

Description:

NAT

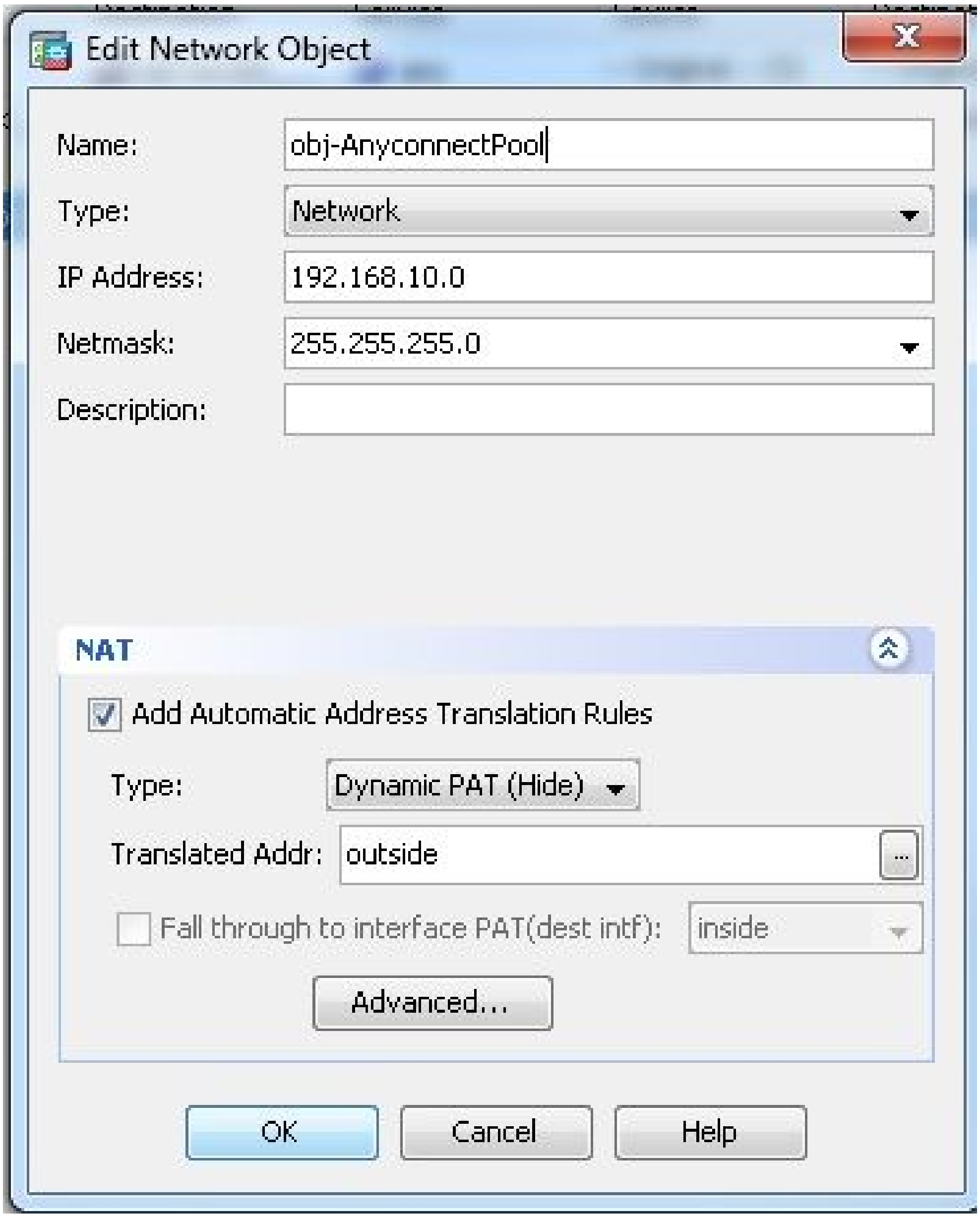
☑ Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: outside

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

选择 **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *因此，来自外部网络的VPN流量可以使用外部IP地址172.16.1.1进行转换。*



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

等效 CLI 配置：

```
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
```

CLI中的ASA 9.1(2)版配置

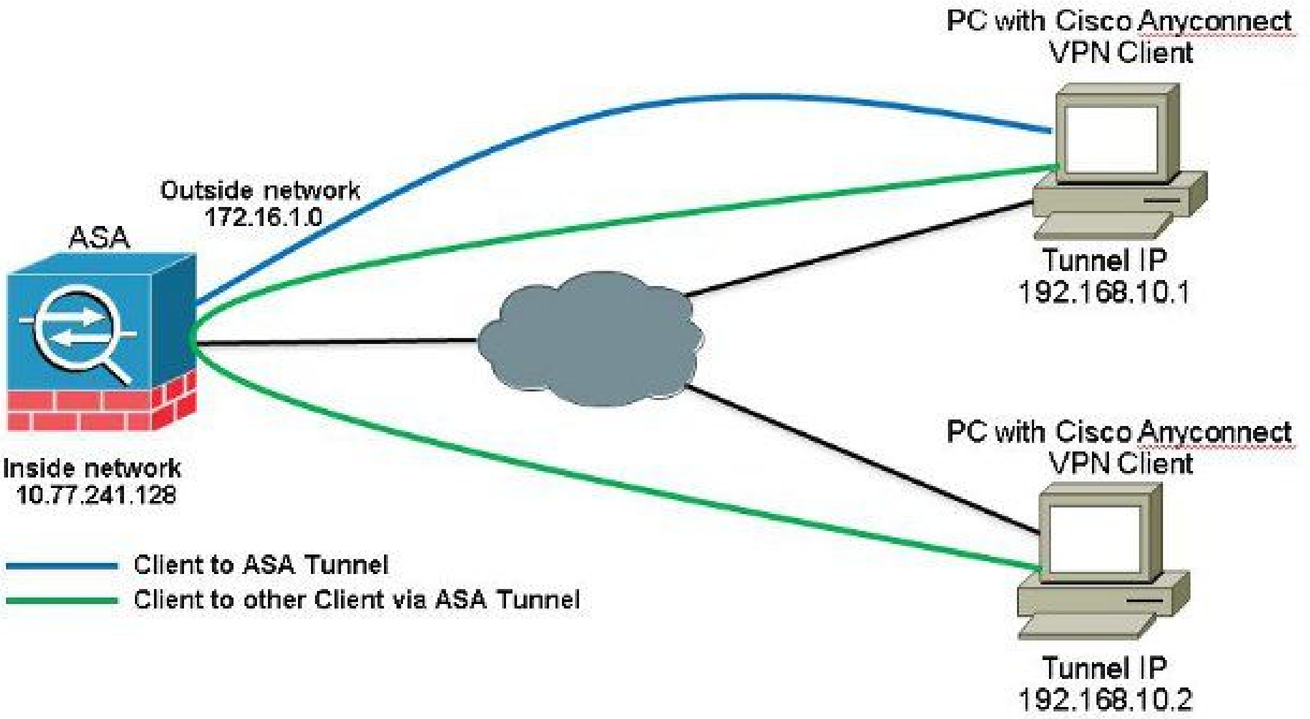
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
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
```

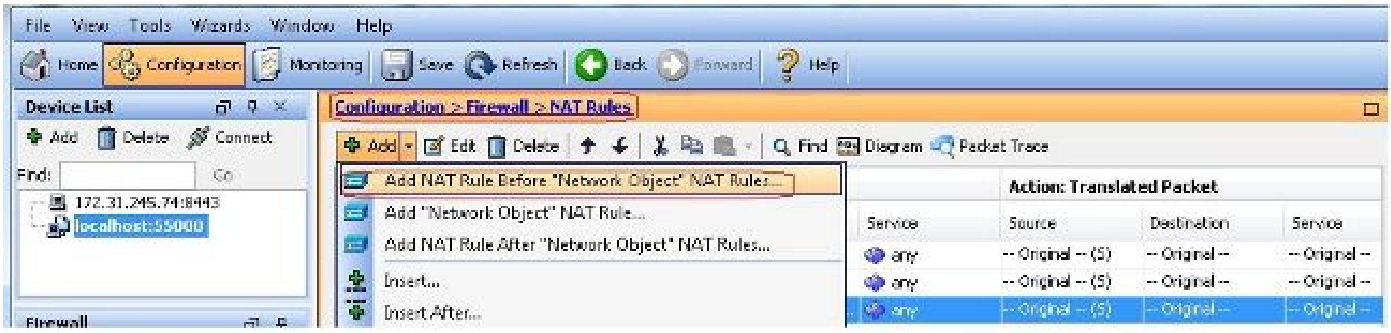
```
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection 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)#
```

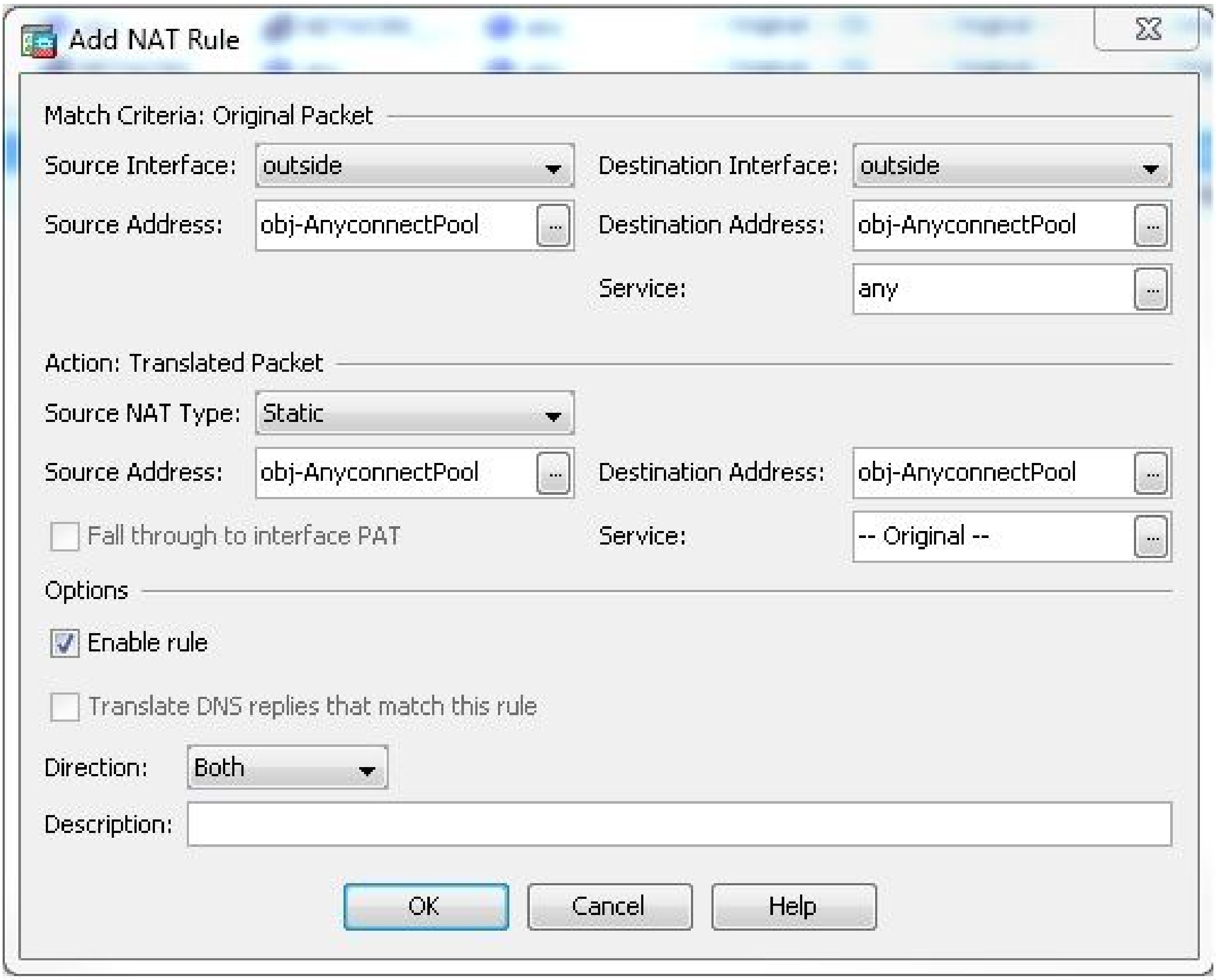
在隧道全部配置就绪的情况下，允许AnyConnect VPN客户端之间的通信网络图



如果Anyconnect客户端之间需要通信，且单臂公共互联网的NAT已建立；还需要手动NAT以允许双向通信。这是Anyconnect客户端使用电话服务且必须能够相互呼叫的常见情况。ASA 9.1(2)版本配置与ASDM 7.1(6)版本选择 Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules 因此，来自外部网络（Anyconnect池）且从同一池发往另一个Anyconnect客户端的流量不会转换为外部IP地址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:

等效 CLI 配置：

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

CLI中的ASA 9.1(2)版配置

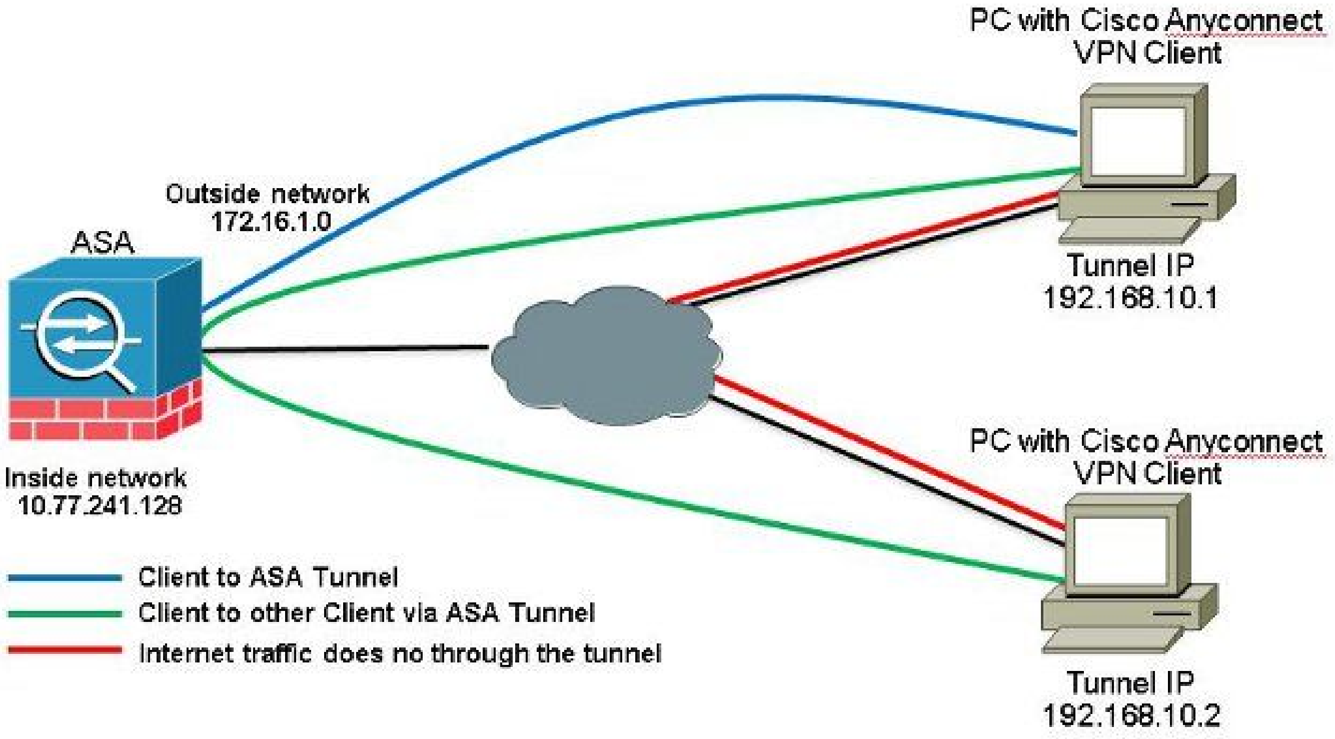
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
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)#
```

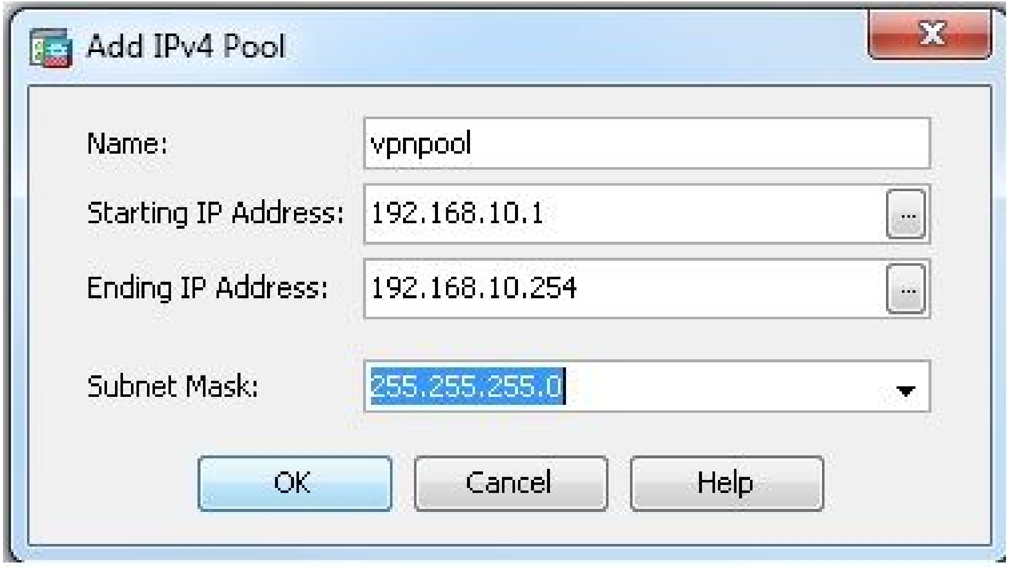
允许使用拆分隧道在AnyConnect VPN客户端之间进行通信

网络图


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

如果需要Anyconnect客户端之间的通信，并且使用拆分隧道；除非配置了影响此流量的NAT规则，否则无需手动NAT即可允许双向通信。但是，Anyconnect VPN池必须包含在分割隧道ACL中。这是Anyconnect客户端使用电话服务且必须能够相互呼叫的常见情况。ASA 9.1(2)版本配置与ASDM 7.1(6)版本

1. *选择* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment> Address Pools > Add** *创建IP地址池* **vpnpool**.


Add IPv4 Pool

Name: vpnpool

Starting IP Address: 192.168.10.1

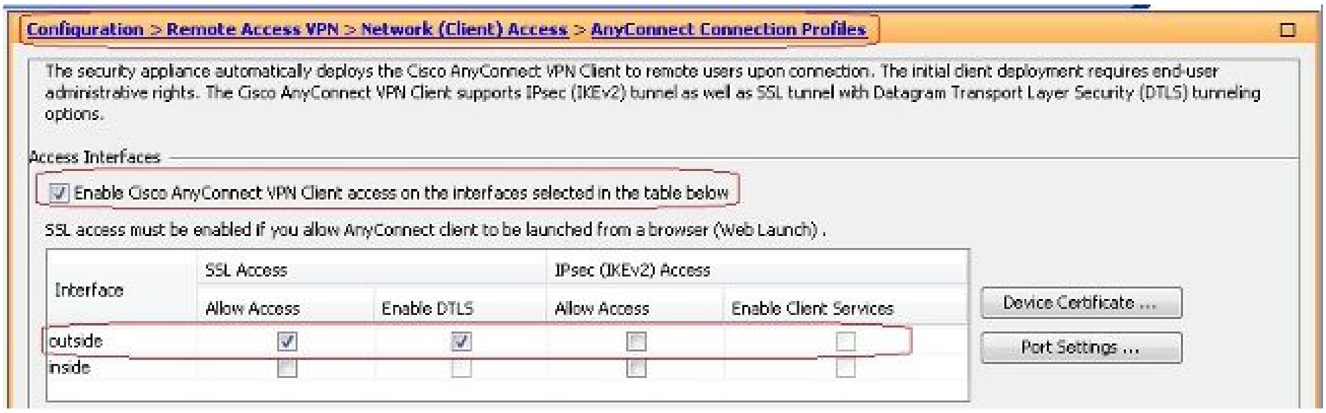
Ending IP Address: 192.168.10.254

Subnet Mask: 255.255.255.0

2. *点击* **Apply**. ***等效 CLI 配置：***

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

3. *启用 Webvpn。 选择* **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** *和* **Access Interfaces**，*单击复选框* **Allow Access** *和* **Enable DTLS** *外部接口。此外，请查看* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *复选框以在外部接口上启用SSL VPN。*



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.

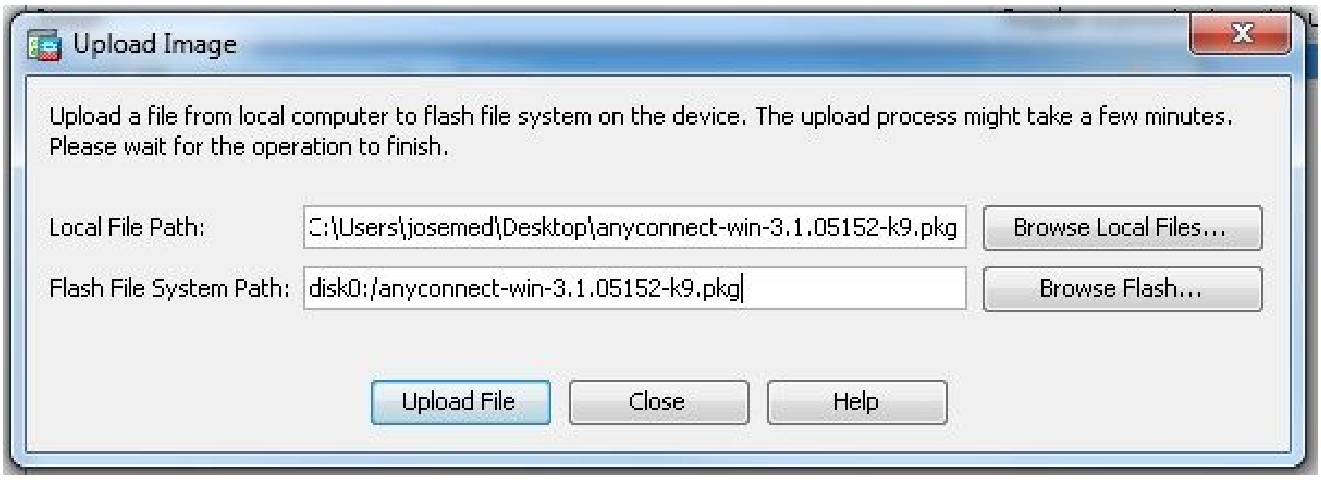
Access Interfaces

☑ 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	□	□	□	□

点击 **Apply**.选择 **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** 以便从ASA的闪存中添加Cisco AnyConnect VPN客户端映像，如下所示。

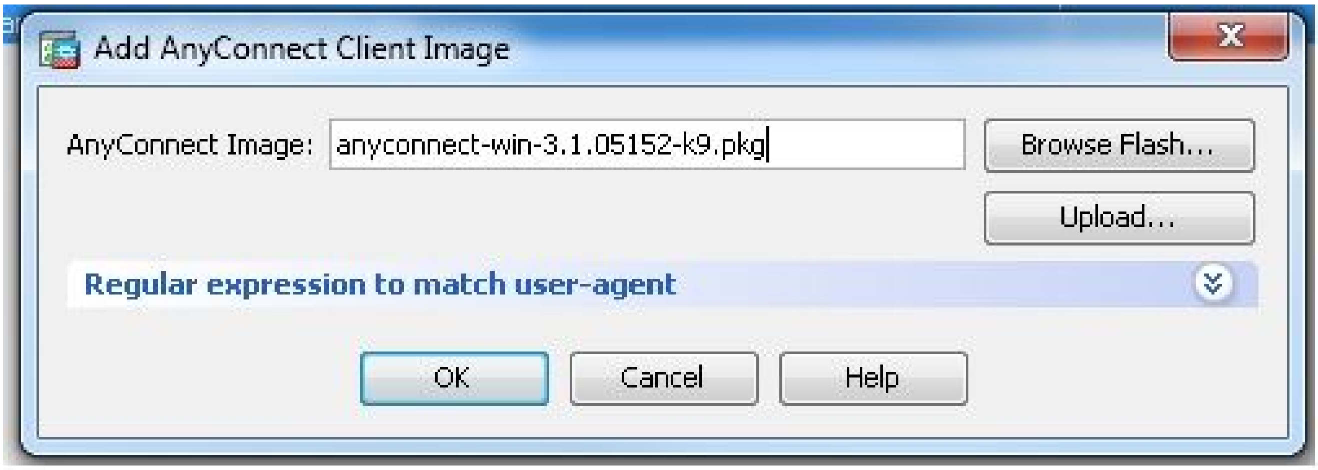


Upload Image

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



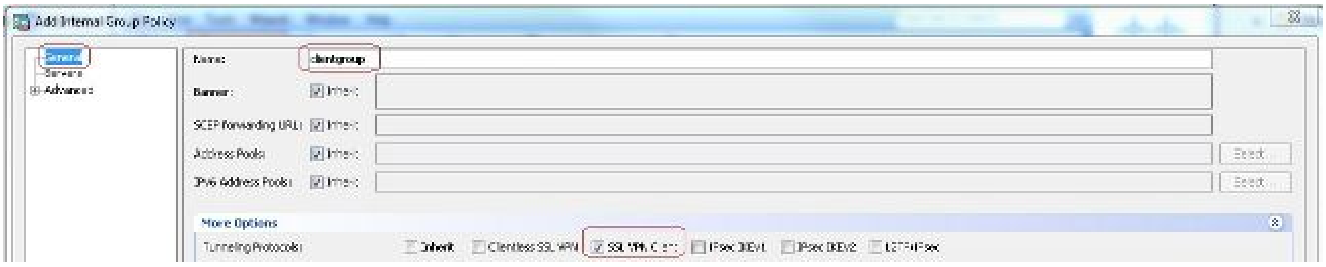
Add AnyConnect Client Image

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

等效 CLI 配置：

```
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. 配置组策略。 选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** 创建内部组策略 **clientgroup**.在 **General** 选项卡，选择 **SSL VPN Client** 复选框以启用WebVPN作为允许的隧道协议。



Add Internal Group Policy

Name: clientgroup

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

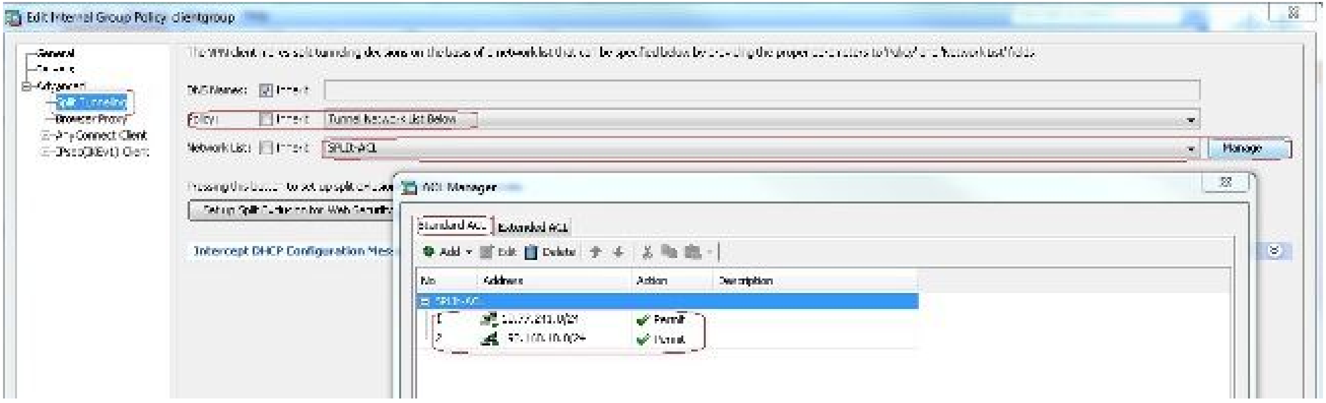
Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

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

如果 **Advanced > Split Tunneling** *选项卡，选择* **Tunnel Network List Below** *从策略(Policy)下拉列表中，使来自远程PC的所有数据包通过安全隧道。*



Edit Internal Group Policy: clientgroup

DNS Names: ☑ Inherit

Policy: □ Inherit Tunnel Network List Below

Network List: □ Inherit SPLIt-ACL

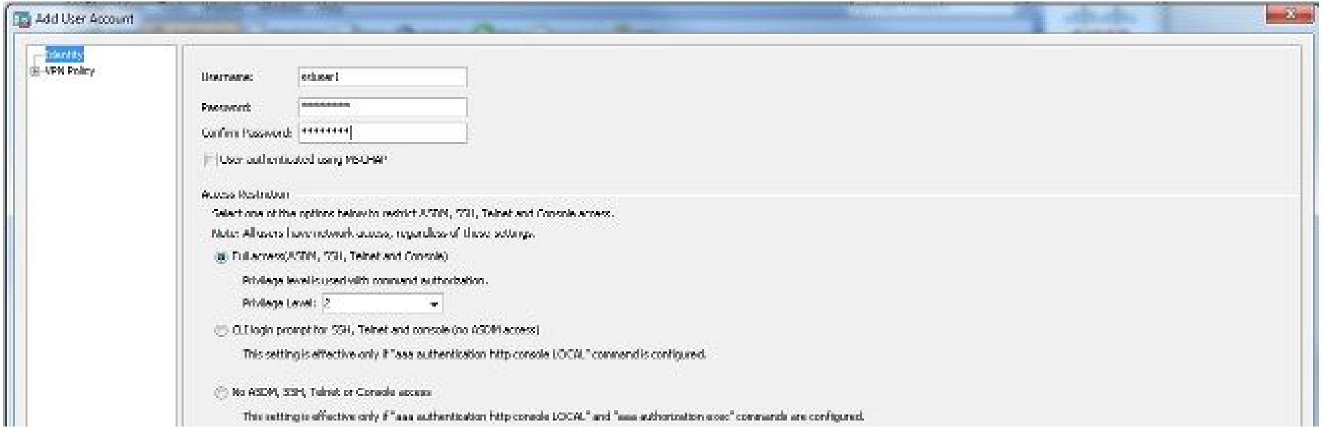
ACL Manager

No	Address	Action	Description
SPLIt-ACL			
1	10.77.241.0/24	Permit	
2	192.168.10.0/24	Permit	

等效 CLI 配置：

```
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. *选择* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *创建新用户帐户* **ssluser1**.*点击* **OK** *然后* **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.

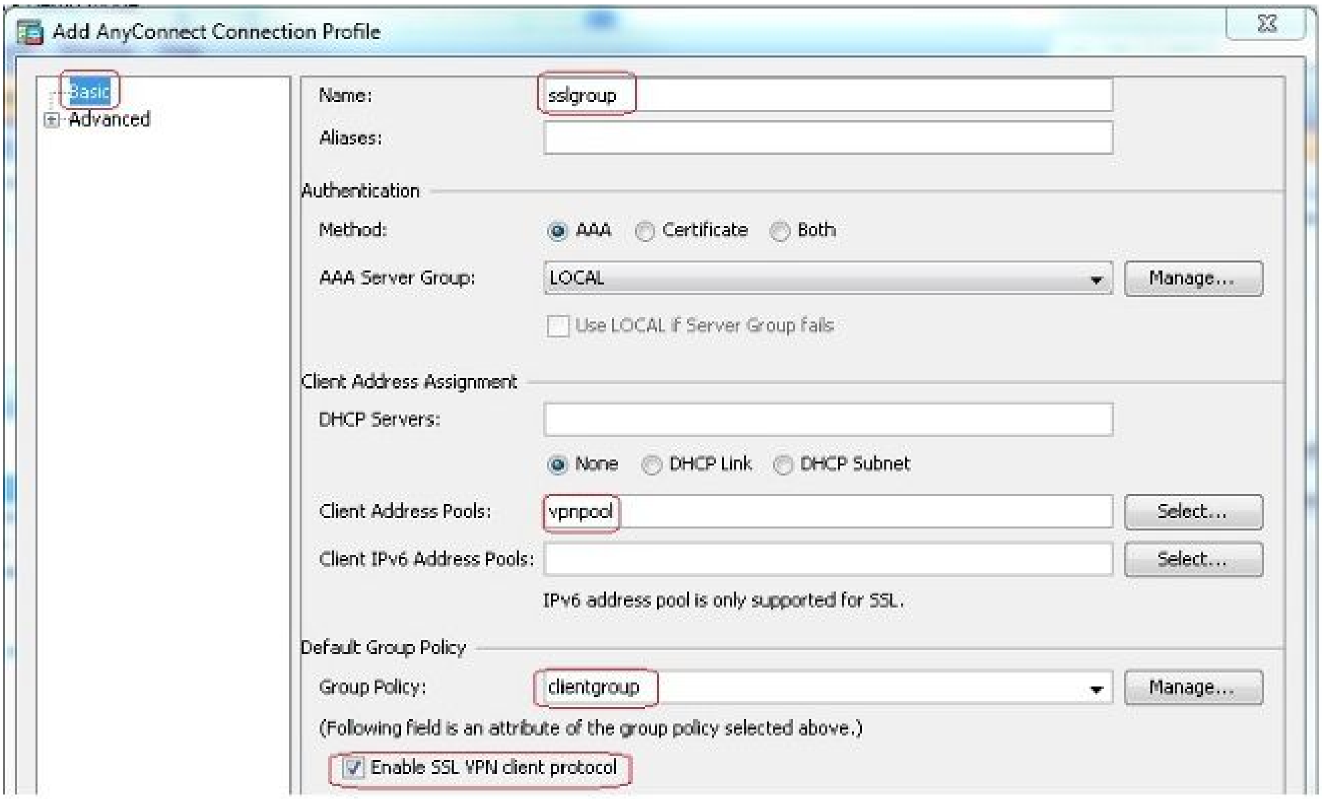
○ No ASDM, SSH, Telnet or Console access

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

等效 CLI 配置：

```
ciscoasa(config)#username ssluser1 password asdmASA@
```

6. *配置隧道组。 选择* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *创建新隧道组* **sslgroup**.*如果* **Basic** *选项卡中，您可以按如下所示执行配置列表： 将隧道组命名为* **sslgroup**.*低于* **Client Address Assignment**，*选择地址池* **vpnpool** *从* **Client Address Pools** *下拉列表。低于* **Default Group Policy**，*选择组策略* **clientgroup** *从* **Group Policy** *下拉列表。*



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

在 **Advanced > Group Alias/Group URL** 选项卡，将组别名指定为 **sslgroup_users** 并点击 **OK**. ***等效 CLI 配置：***

```
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
```

CLI中的ASA 9.1(2)版配置

```
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)#
```

验证

使用本部分可确认配置能否正常运行。

- **show vpn-sessiondb svc** — 显示有关当前SSL连接的信息。

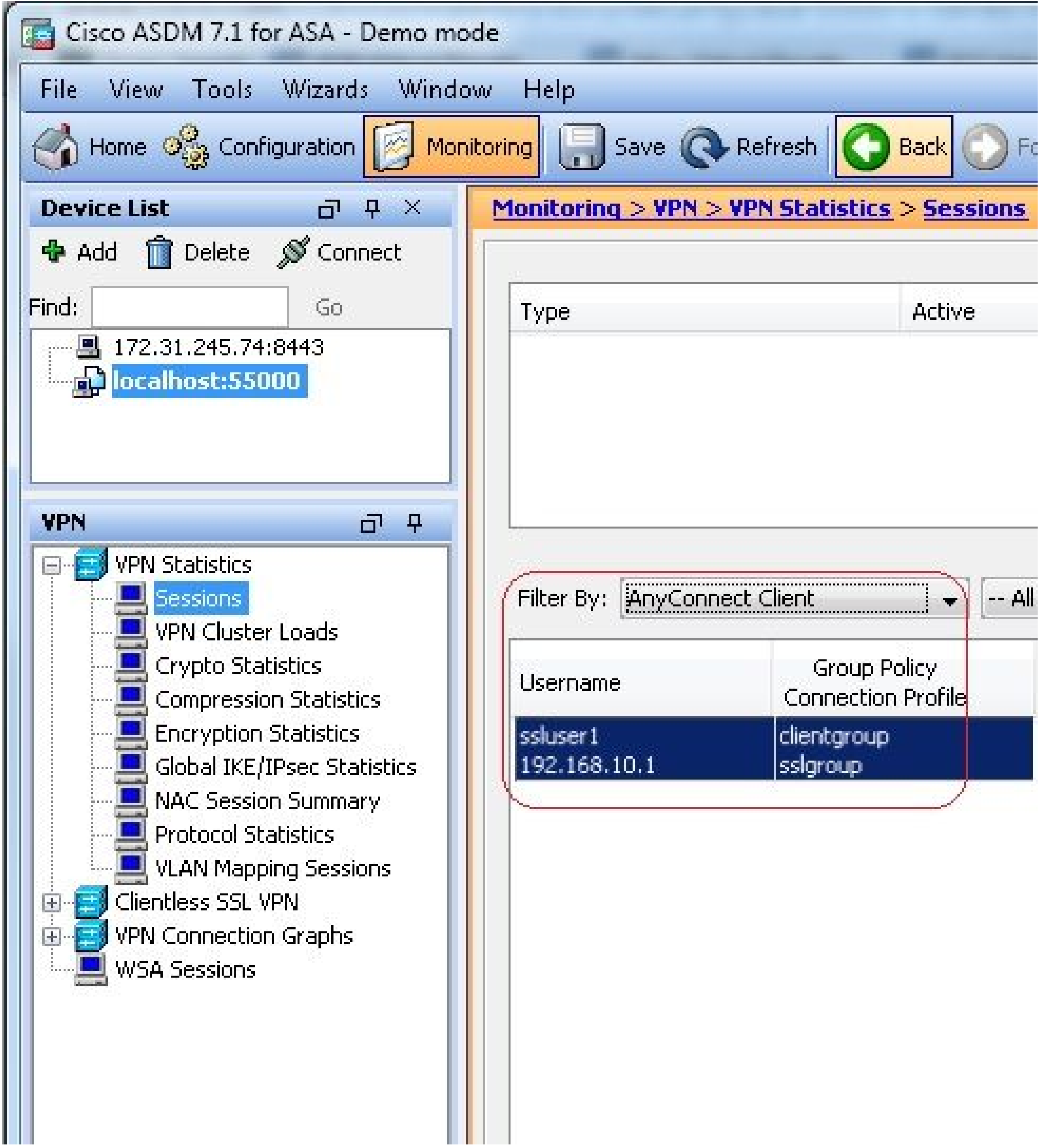
  ```
  ciscoasa#show vpn-sessiondb anyconnect

  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** — 显示各种组的已配置别名。

```
ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup   Group Alias: sslgroup_users enabled
```

- 在ASDM中，选择 **Monitoring > VPN > VPN Statistics > Sessions** 以便了解ASA中的当前会话。



Filter By: AnyConnect Client

Username	Group Policy Connection Profile
ssluser1 192.168.10.1	clientgroup sslgroup

故障排除

本部分提供的信息可用于对配置进行故障排除。

- **vpn-sessiondb logoff name** — 用于注销特定用户名的SSL VPN会话的命令。

```
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)
```

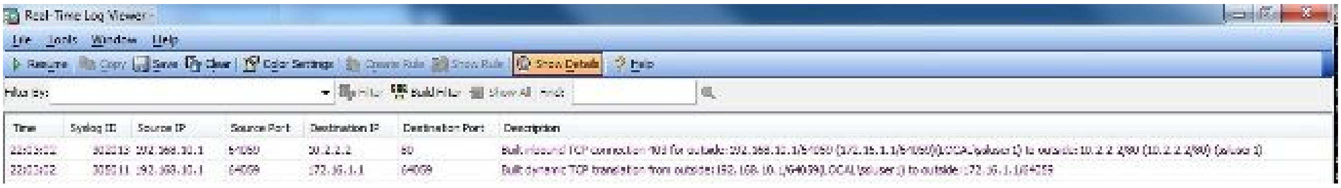
同样，您可以使用 **vpn-sessiondb logoff anyconnect** 命令终止所有AnyConnect会话。

- **debug webvpn anyconnect <1-255>** — 提供实时webvpn事件以建立会话。

```
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
```

- 在ASDM中，选择 **Monitoring > Logging > Real-time Log Viewer > View** 以便查看实时事件。此示例显示通过ASA 172.16.1.1在Internet中的AnyConnect 192.168.10.1和Telnet服务器10.2.2.2之间的会话信息。


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 403 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

相关信息

- Cisco ASA 5500-X系列防火墙
- 单臂路由器上用于公共 Internet 的 PIX/ASA 和 VPN 客户端配置示例
- 在 ASA 上用 ASDM 配置 SSL VPN Client (SVC) 的示例
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。