在ASA 9.X上配置AnyConnect VPN客戶端U-turn流量

目錄

簡介

本文檔介紹如何設定思科自適應安全裝置(ASA)版本9.X以允許其轉發VPN流量。它涵蓋以下設定案例：從遠端訪問客戶端調轉流量。

> **附註**： 為了避免網路中IP地址重疊，請為VPN客戶端分配完全不同的IP地址池（例如，10.x.x.x、172.16.x.x和192.168.x.x）。 此IP位址方案有助於排除網路疑難問題。

髮夾或U形轉彎

此功能對於進入介面但隨後從該介面路由出去的VPN流量非常有用。例如，如果您有一個中心輻射型VPN網路，其中安全裝置是中心，遠端VPN網路是輻射型，為了使一個輻射型與另一個輻射型流量通訊，必須轉到安全裝置，然後再次轉到另一個輻射型。

輸入 **same-security-traffic** 命令，以允許流量進入和退出同一介面。

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

必要條件

需求

思科建議您在嘗試此設定之前符合以下要求：

- 中心ASA安全裝置需要運行9.x版。
- Cisco AnyConnect VPN使用者端3.x**附註**：下載AnyConnect VPN客戶端軟體包(anyconnect-win*.pkg)從Cisco Software Download(僅限註冊客戶)網站下載。 將AnyConnect VPN客戶端複製到Cisco ASA快閃記憶體，該快閃記憶體將下載到遠端使用者電腦，以便與ASA建立SSL VPN連線。有關詳細資訊，請參閱ASA配置指南的AnyConnect VPN客戶端連線部分。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5500系列ASA(運行軟體版本9.1(2))
- 適用於Windows 3.1.05152的Cisco AnyConnect SSL VPN客戶端版本
- 根據受支援的VPN平台Cisco ASA系列運行受支援的OS的PC。
- 思科調適型安全裝置管理員(ASDM)版本7.1(6)

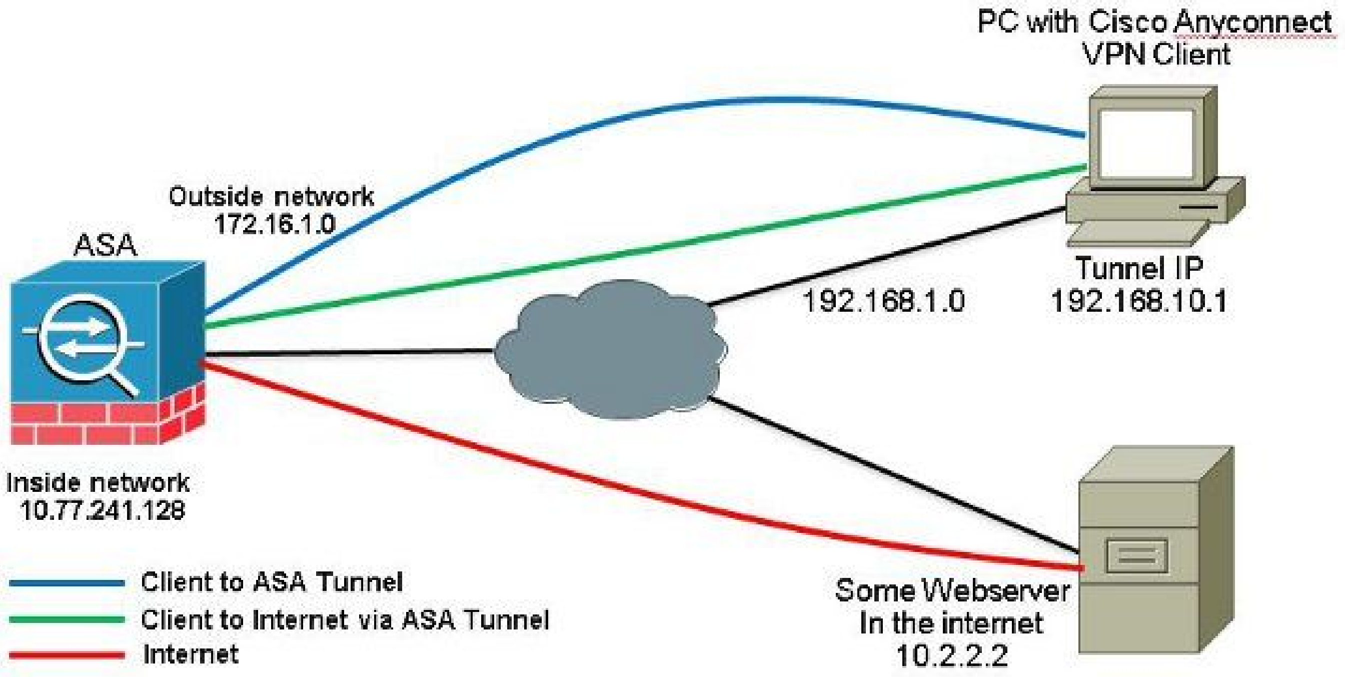
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco AnyConnect VPN客戶端為遠端使用者提供到安全裝置的安全SSL連線。如果沒有先前安裝的客戶端，遠端使用者在其瀏覽器中輸入配置為接受SSL VPN連線的介面的IP地址。除非安全裝置配置為重定向 **http://** 請求 **https://**，使用者必須在表單中輸入URL **https://**

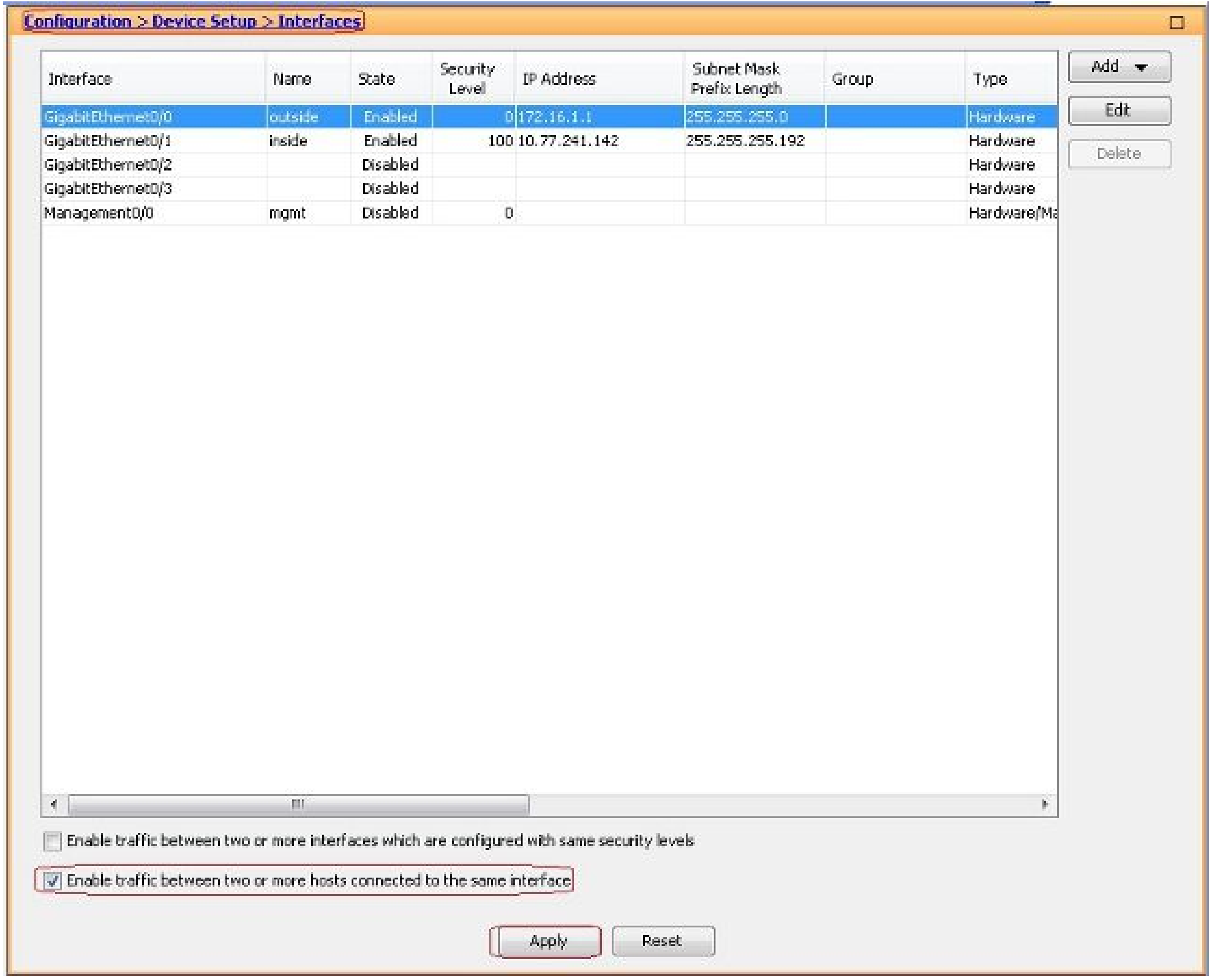
*.輸入URL後，瀏覽器會連線到該介面並顯示登入螢幕。如果使用者滿足登入和身份驗證要求，且安全裝置將使用者識別為需要客戶端，則它將下載與遠端電腦的作業系統匹配的客戶端。下載後，客戶端將自行安裝和配置，建立安全SSL連線，並在連線終止時自行保留或解除安裝（這取決於安全裝置配置）。如果是以前安裝的客戶端，當使用者進行身份驗證時，安全裝置會檢查客戶端的修訂版本，並根據需要升級客戶端。當客戶端與安全裝置協商SSL VPN連線時，它會與傳輸層安全(TLS)連線，並且還會使用資料包傳輸層安全(DTLS)。DTLS可避免與某些SSL連線相關的延遲和頻寬問題，並提高對資料包延遲敏感的即時應用的效能。AnyConnect客戶端可以從安全裝置下載，也可以由系統管理員手動安裝在遠端PC上。有關如何手動安裝客戶端的詳細資訊，請參閱Cisco AnyConnect安全移動客戶端管理員指南。安全裝置根據建立連線的使用者的組策略或使用者名稱屬性下載客戶端。您可以將安全裝置配置為自動下載客戶端，也可以將其配置為提示遠端使用者是否下載客戶端。在後一種情況下，如果使用者沒有響應，您可以將安全裝置配置為在超時時間後下載客戶端或顯示登入頁面。**附註**：本文檔中使用的示例使用IPv4。對於IPv6 U型流量，步驟相同，但使用IPv6地址而不是IPv4。***配置翻轉的遠端訪問流量*****本節提供用於設定本文件中所述功能的資訊。附註：使用命令參考指南可獲取本節所用命令的詳細資訊。用於單臂公共網際網路VPN的AnyConnect VPN客戶端配置示例網路圖表本檔案會使用以下網路設定**

：*


PC with Cisco Anyconnect VPN Client
Outside network 172.16.1.0
ASA
Tunnel IP 192.168.10.1
192.168.1.0
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 9.1(2)版配置與ASDM 7.1(6)版本檔案假設基本設定（例如介面組態）已完成後能正常運作。附註：請參閱配置管理訪問以允許ASDM配置ASA。附註：在8.0(2)及更高版本中，ASA在外部介面的埠443上同時支援無客戶端SSL VPN(WebVPN)會話和ASDM管理會話。在低於8.0(2)的版本中，除非更改埠號，否則不能在同一ASA介面上啟用WebVPN和ASDM。有關詳細資訊，請參閱在同一介面ASA上啟用ASDM和WebVPN。完成以下步驟，以便在ASA中配置單臂上的SSL VPN:

1. 選擇 **Configuration > Device Setup > Interfaces** 並檢查 **Enable traffic between two or more hosts connected to the same interface** 覈取方塊，以允許SSL VPN流量進入和退出同一介面。按一下 **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

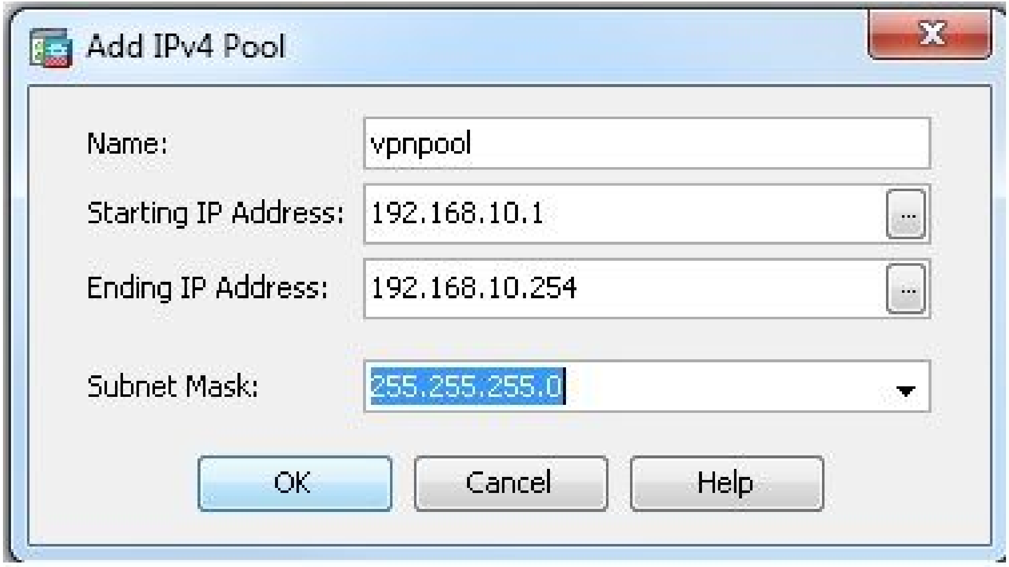
□ Enable traffic between two or more interfaces which are configured with same security levels

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

等效的CLI配置：

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

2. *選擇* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add** *以便建立IP地址池* **vpnpool**.



Add IPv4 Pool

Name: vpnpool

Starting IP Address: 192.168.10.1

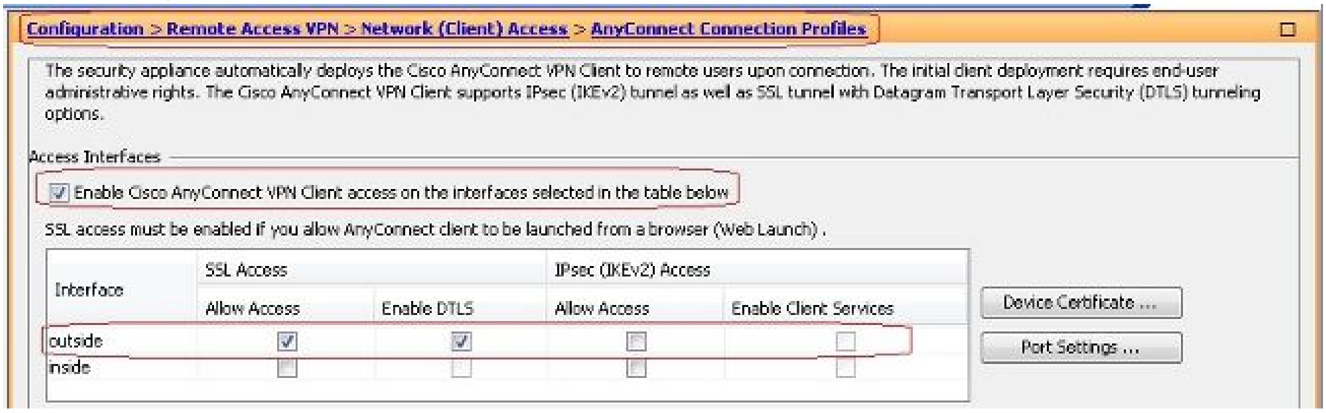
Ending IP Address: 192.168.10.254

Subnet Mask: 255.255.255.0

3. *按一下* **Apply**. ***等效的CLI配置：***

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

4. *啟用WebVPN。 選擇* **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** *和* **Access Interfaces**，*按一下覈取方塊* **Allow Access** *和* **Enable DTLS** *用於外部介面。此外，請檢查* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *覈取方塊以在外部介面上啟用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.

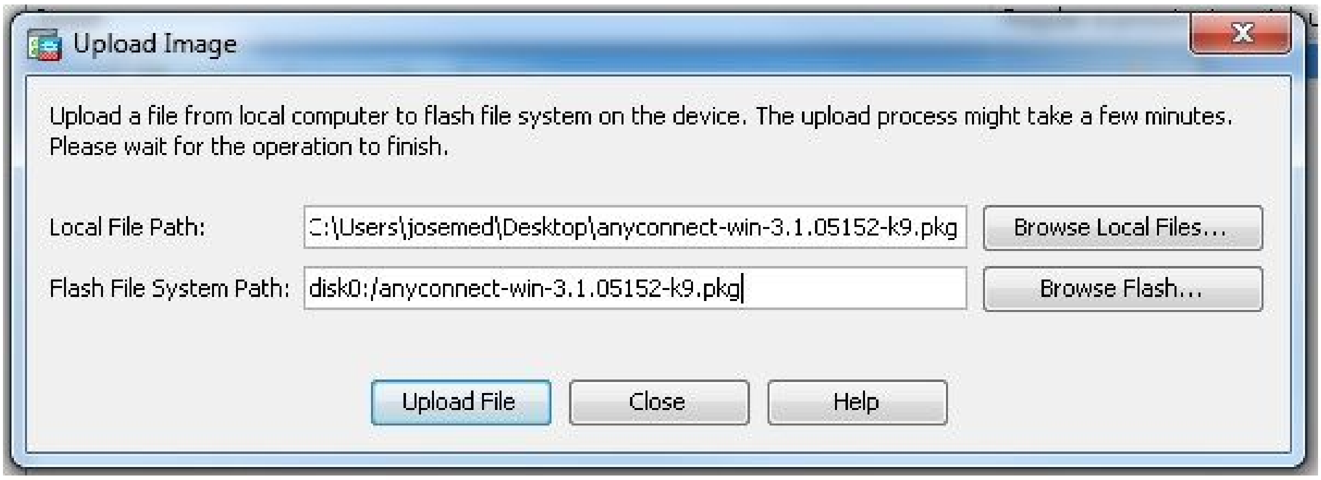
Access Interfaces

☑ 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	□	□	□	□

按一下 **Apply**.*選擇* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** *以便從ASA的快閃記憶體中新增Cisco AnyConnect VPN客戶端映像，如下所示。*

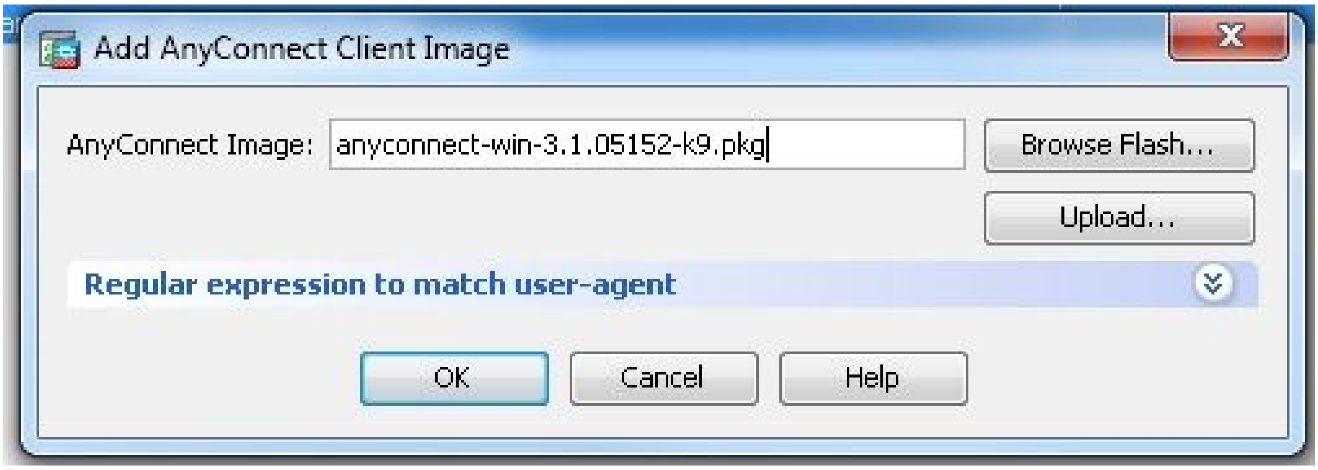


Upload Image

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



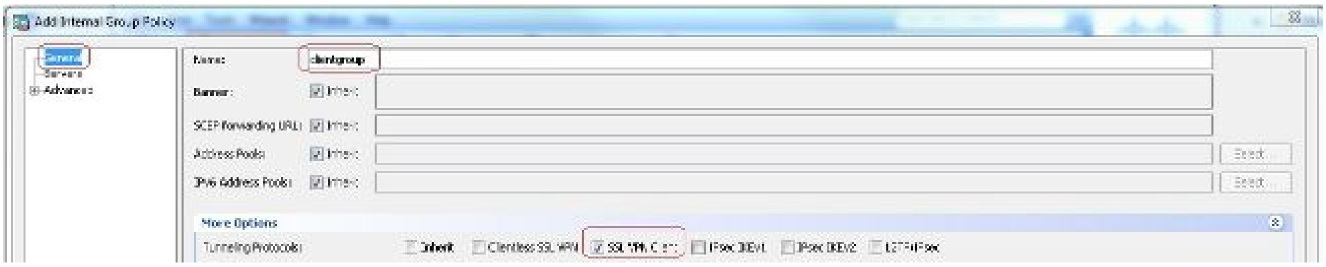
Add AnyConnect Client Image

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

等效的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. *配置組策略。 選擇* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *建立內部組策略* **clientgroup**. *在* **General** *頁籤，選擇* **SSL VPN Client** *覈取方塊以啟用WebVPN作為隧道協定。*



Add Internal Group Policy

Name: clientgroup

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

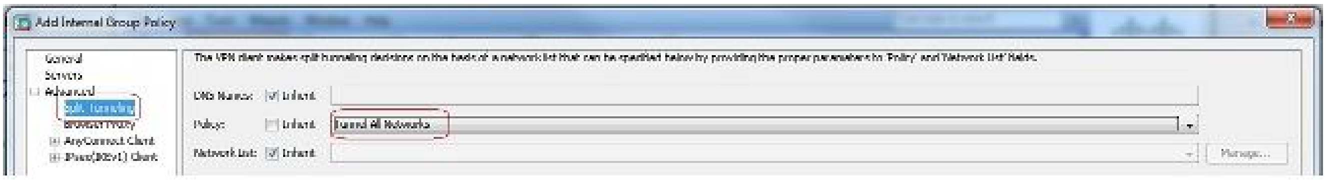
Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

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

在 **Advanced > Split Tunneling** *頁籤，選擇* **Tunnel All Networks** *從策略的Policy下拉選單中，使來自遠端PC的所有資料包通過安全隧道。*



Add Internal Group Policy

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

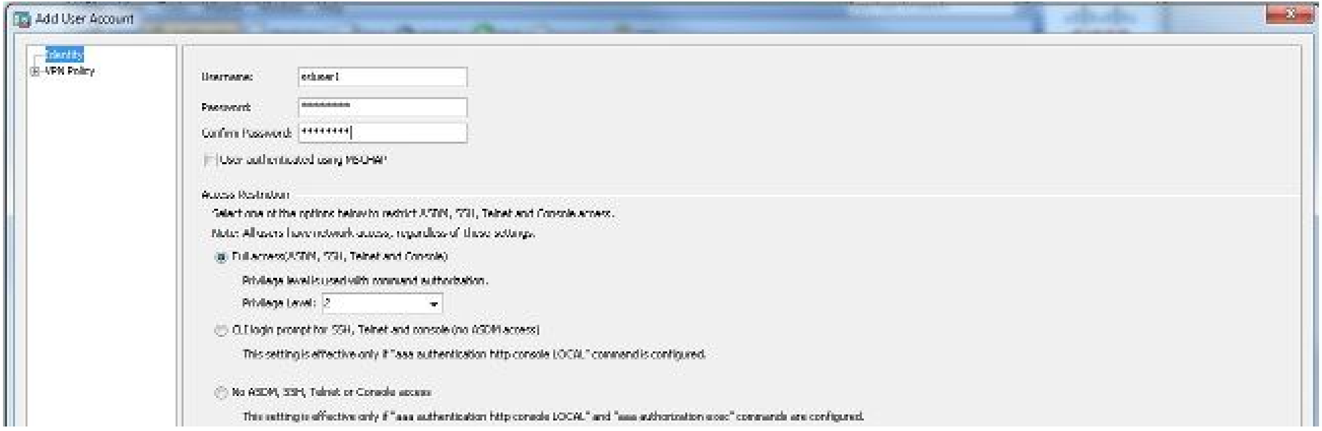
Policy: □ Inherit Tunnel All Networks

Network List: ☑ Inherit

等效的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. *選擇* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *建立新使用者帳戶* **ssluser1**. *按一下* **OK** *然後* **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.

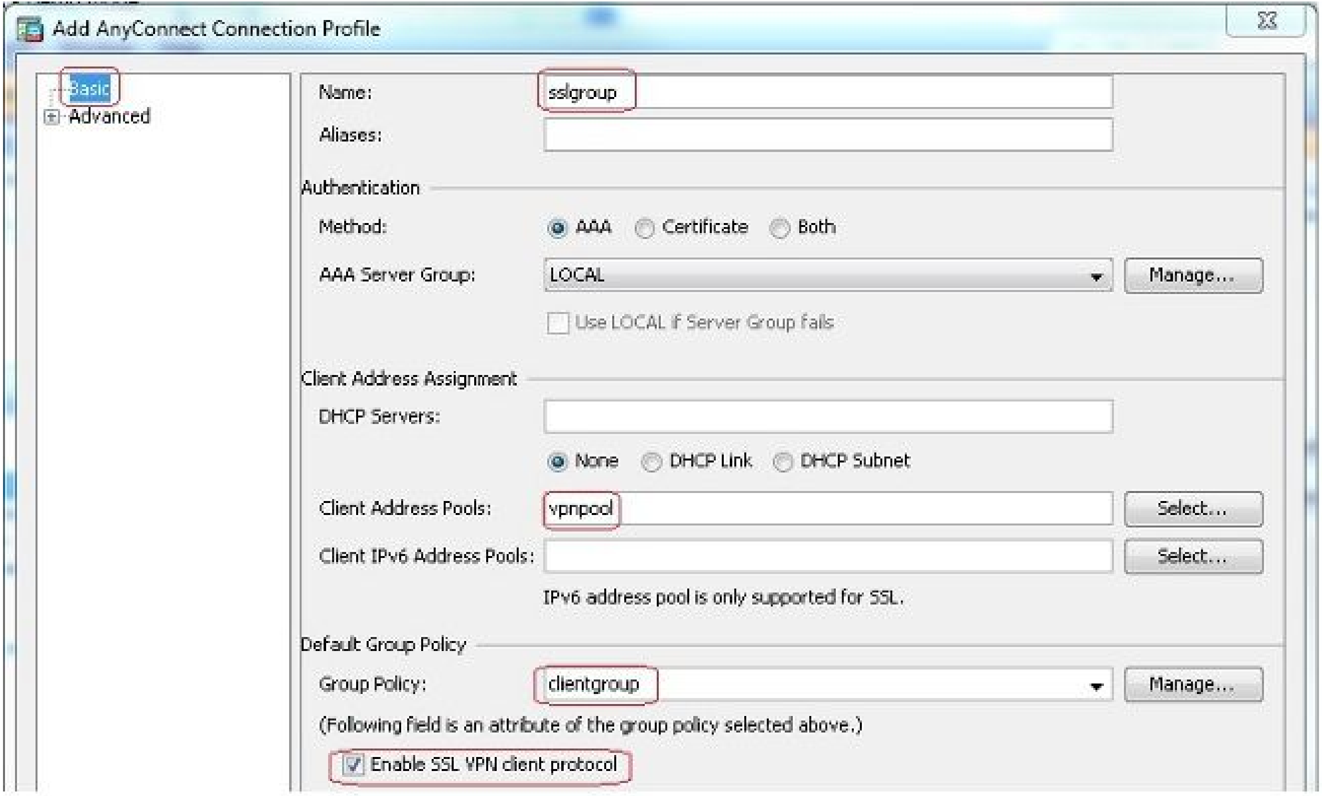
○ No ASDM, SSH, Telnet or Console access

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

等效的CLI配置：

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

7. *配置隧道組。 選擇* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *以建立新的隧道組* **sslgroup**.*在* **Basic** *頁籤中，您可以執行以下配置清單： 將隧道組命名為* **sslgroup**.*在* **Client Address Assignment**，*選擇地址池* **vpnpool** *從* **Client Address Pools** *下拉選單。在* **Default Group Policy**，*選擇組策略* **clientgroup** *從* **Group Policy** *下拉選單。*



Add AnyConnect Connection Profile

Basic

⊞ Advanced

Name: sslgroup

Aliases:

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL ▾ Manage...

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: vpnpool Select...

Client IPv6 Address Pools: Select...

IPv6 address pool is only supported for SSL.

Default Group Policy

Group Policy: clientgroup ▾ Manage...

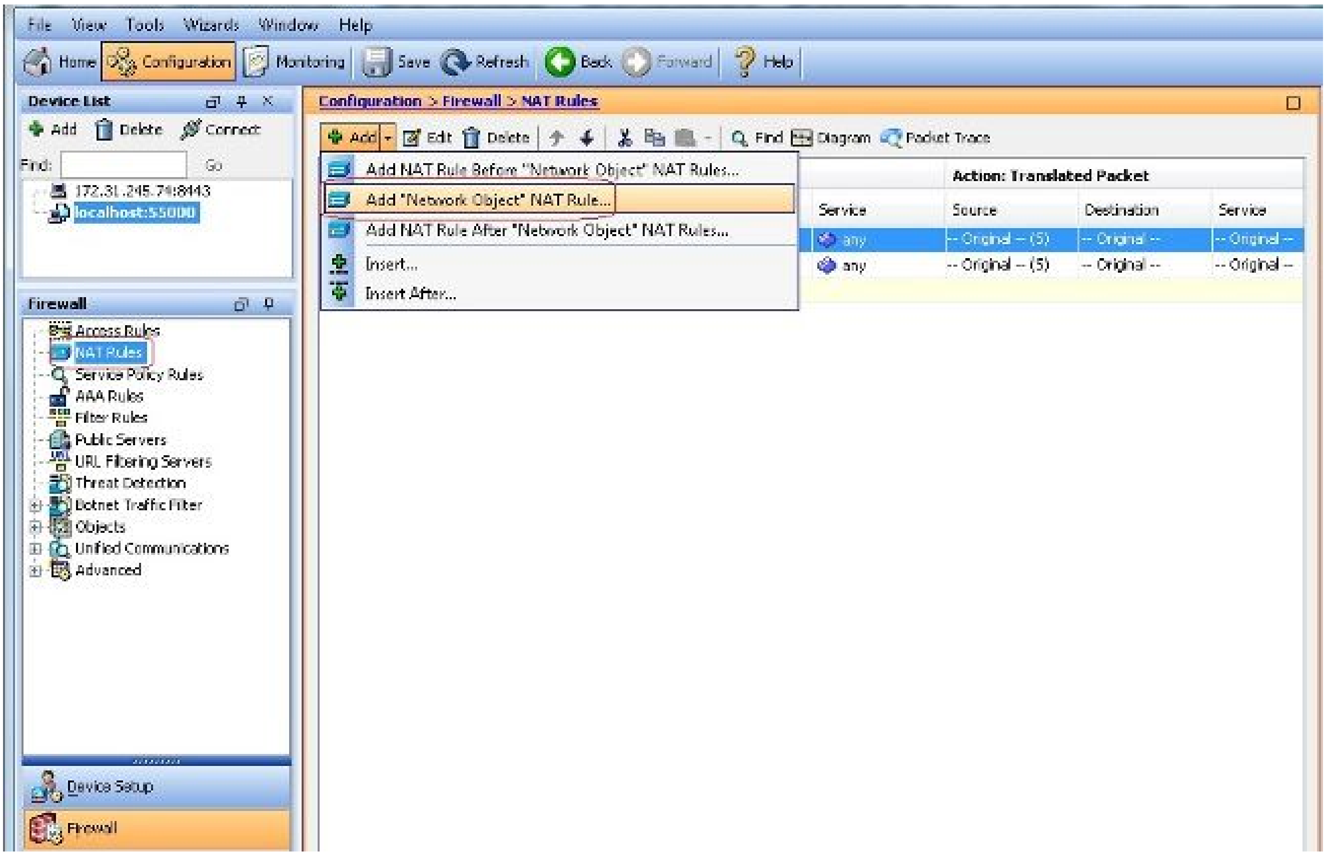
(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN client protocol

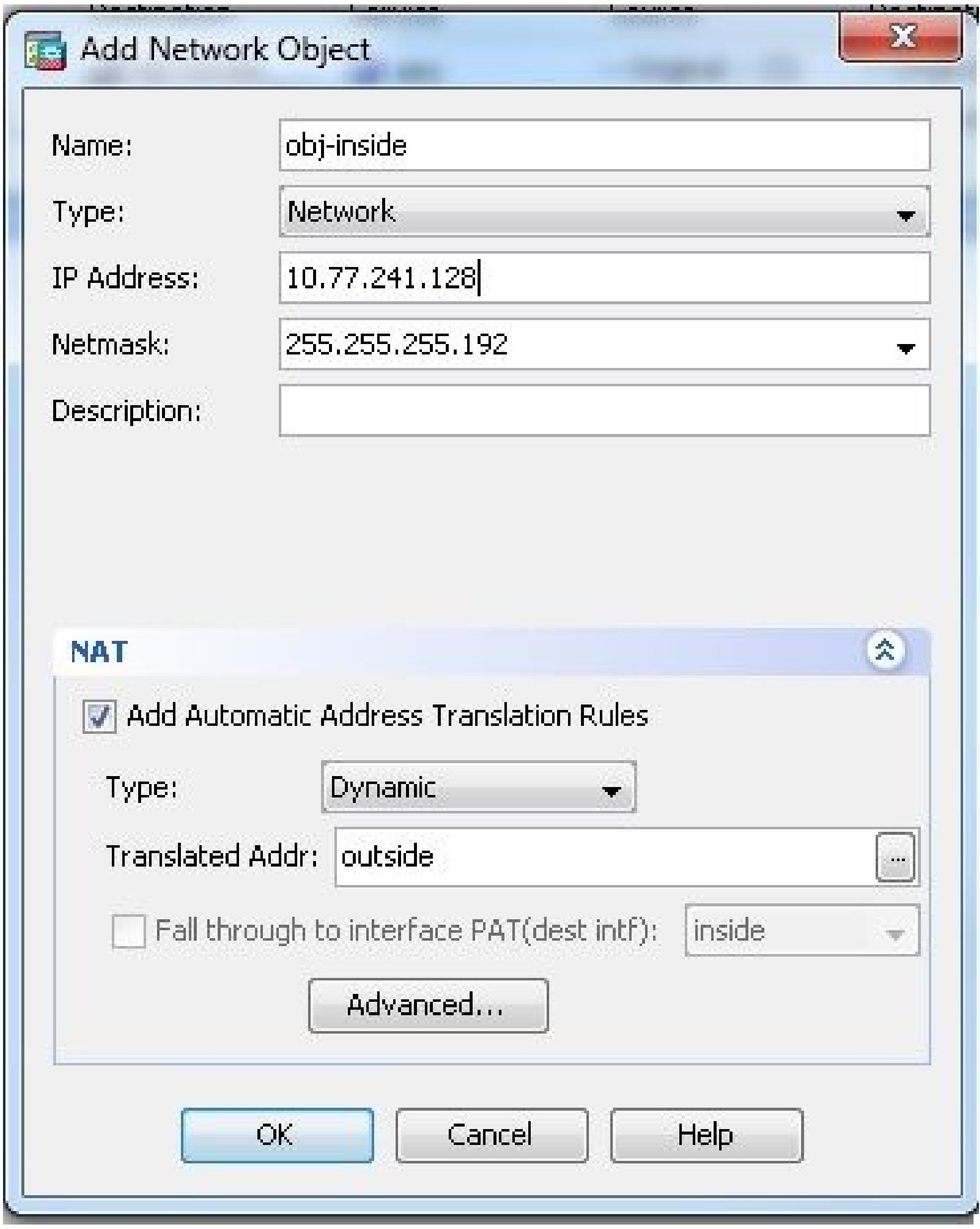
在 **Advanced > Group Alias/Group URL** *頁籤，將組別名指定為* **sslgroup_users** *然後按一下* **OK**. ***等效的CLI配置：***

```
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 選擇* **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *因此，來自內部網路的流量可以使用外部IP地址172.16.1.1進行轉換。*


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
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
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 -- (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

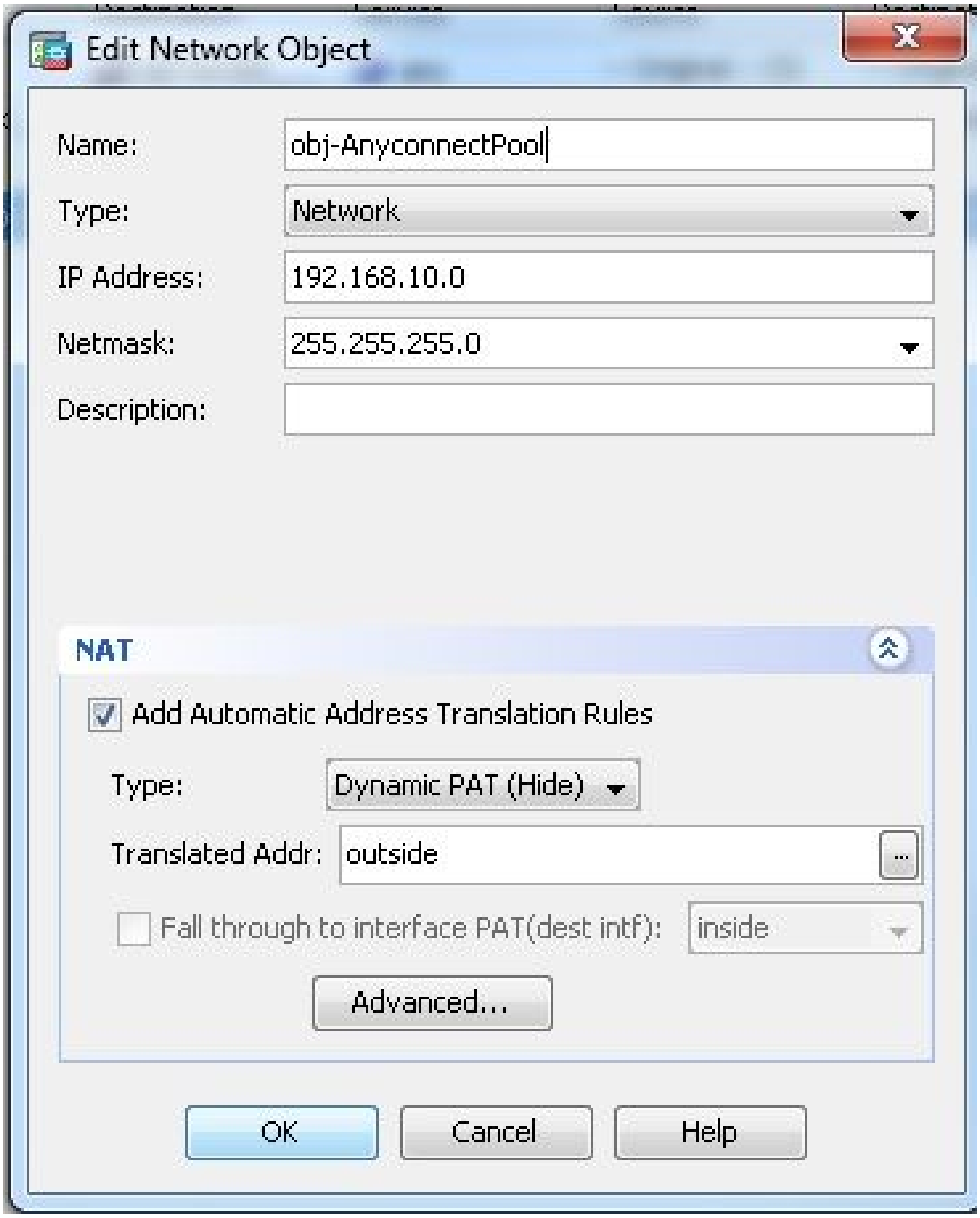
☑ Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: outside

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

選擇 **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** 因此，來自外部網路的VPN流量可以用外部IP地址172.16.1.1進行轉換。



Name: obj-AnyconnectPool

Type: Network

IP Address: 192.168.10.0

Netmask: 255.255.255.0

Description:

☑ Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide)

Translated Addr: outside

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

等效的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

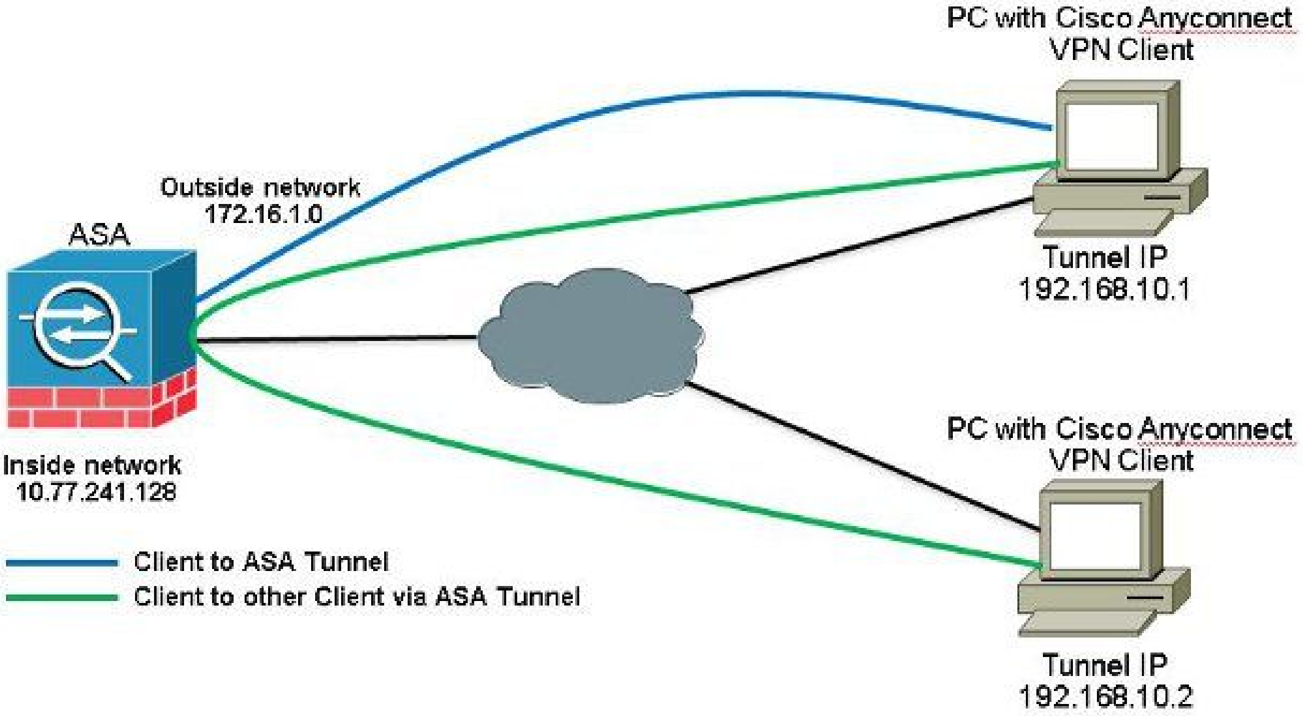
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1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

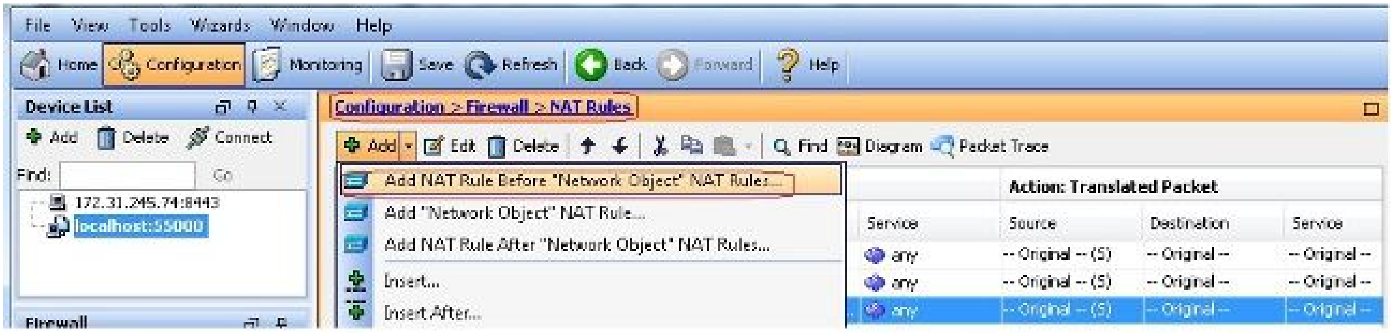
```
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection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

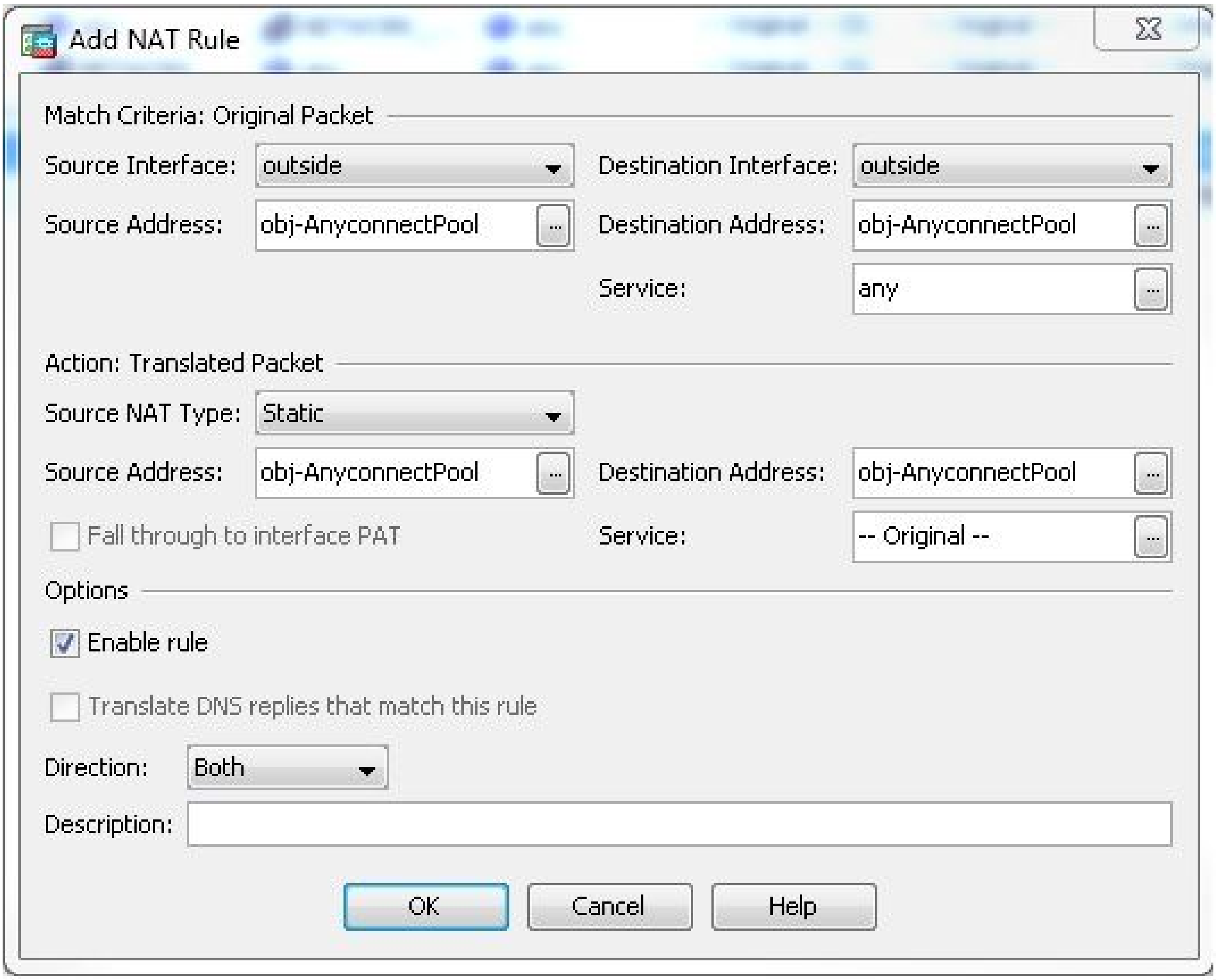
允許使用隧道全部配置在AnyConnect VPN客戶端之間進行通訊網路圖表



如果Anyconnect客戶端之間需要通訊，並且單臂公共網際網路的NAT已經就位；還需要手動NAT以允許雙向通訊。這是Anyconnect客戶端使用電話服務並且必須能夠相互呼叫時的常見情況。ASA 9.1(2)版配置與ASDM 7.1(6)版選擇 Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules 因此，來自外部網路（Anyconnect池）且目的地為來自同一池的另一個Anyconnect客戶端的流量不會使用外部IP地址172.16.1.1進行轉換。



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



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:

等效的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

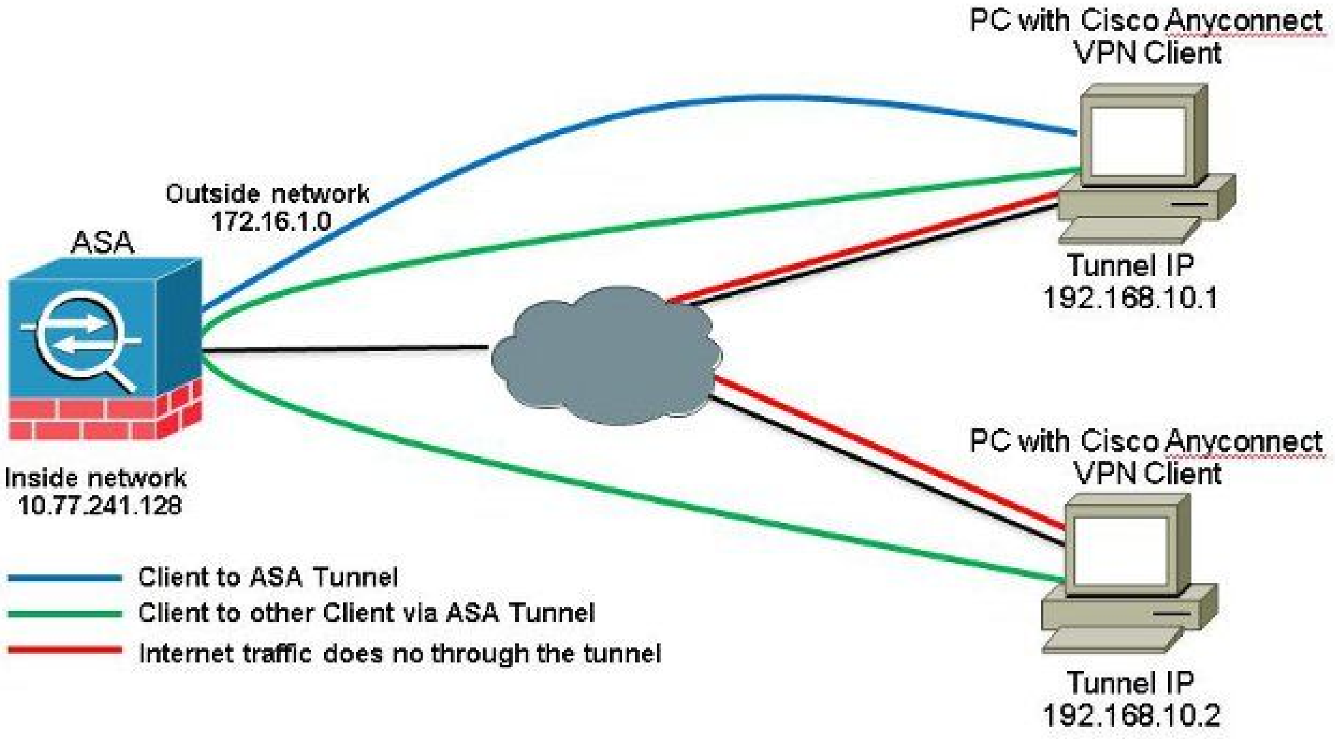
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1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

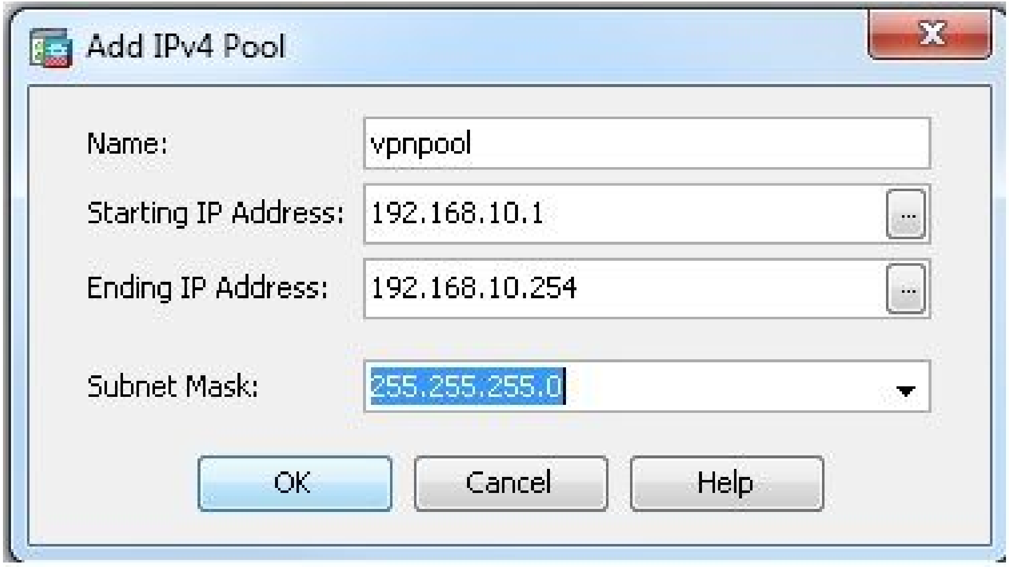
允許使用拆分隧道的AnyConnect VPN客戶端之間進行通訊

網路圖表


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

如果需要在Anyconnect客戶端之間進行通訊且使用分割隧道；無需手動NAT即可允許雙向通訊，除非存在影響已配置此流量的NAT規則。但是，拆分隧道ACL中必須包含Anyconnect VPN池。這是Anyconnect客戶端使用電話服務並且必須能夠相互呼叫時的常見情況。ASA 9.1(2)版配置與ASDM 7.1(6)版

1. *選擇* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment> Address Pools > Add** *以便建立IP地址池* **vpnpool**.



Name: vpnpool

Starting IP Address: 192.168.10.1

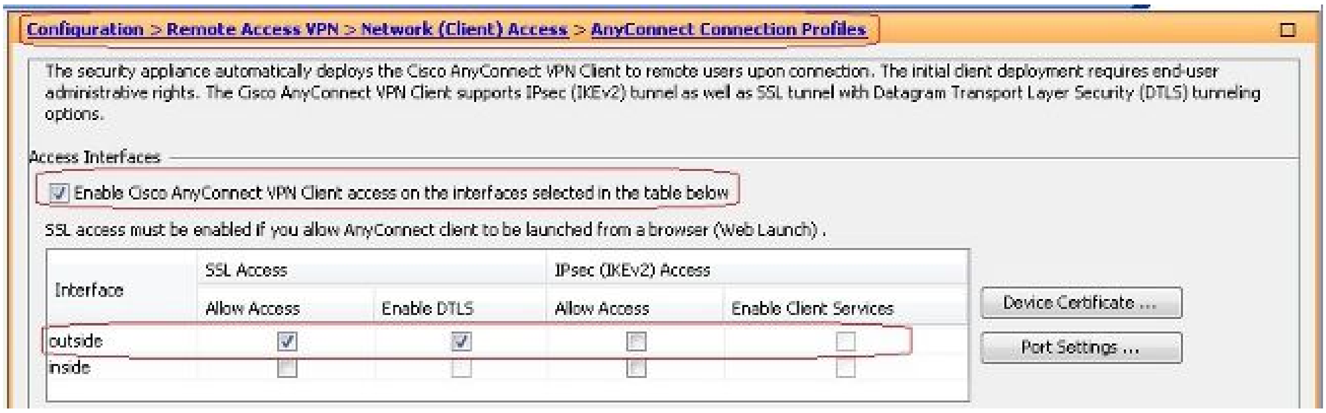
Ending IP Address: 192.168.10.254

Subnet Mask: 255.255.255.0

2. *按一下* **Apply**. ***等效的CLI配置：***

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

3. *啟用WebVPN。 選擇* **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** *和* **Access Interfaces** *，按一下覈取方塊* **Allow Access** *和* **Enable DTLS** *用於外部介面。此外，請檢查* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *覈取方塊以在外部介面上啟用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.

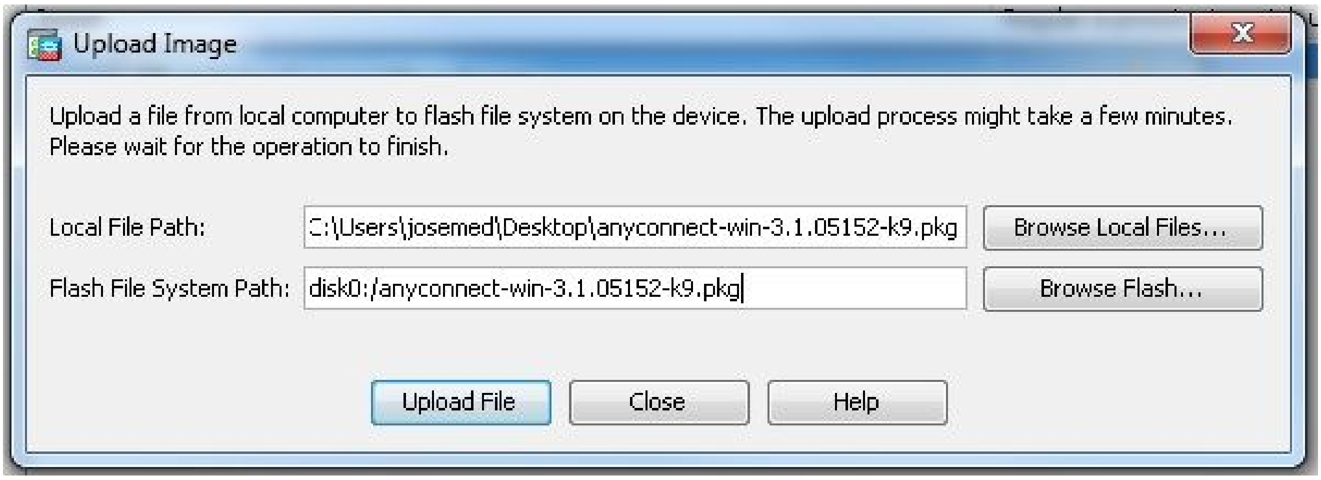
Access Interfaces

☑ 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	☐	☐	☐	☐

按一下 **Apply**.*選擇* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** *以便從ASA的快閃記憶體中新增Cisco AnyConnect VPN客戶端映像，如下所示。*

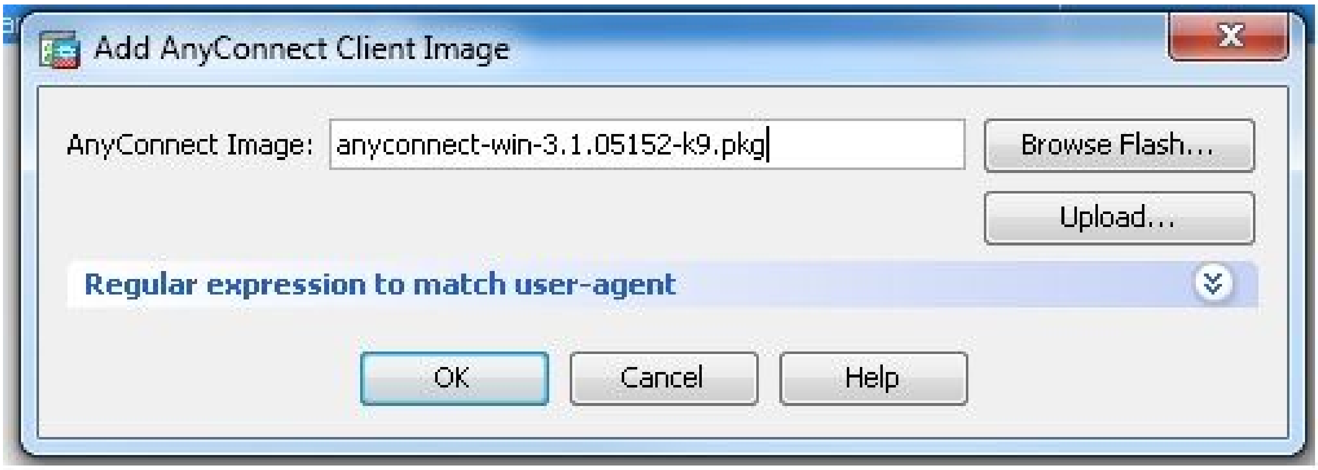


Upload Image

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



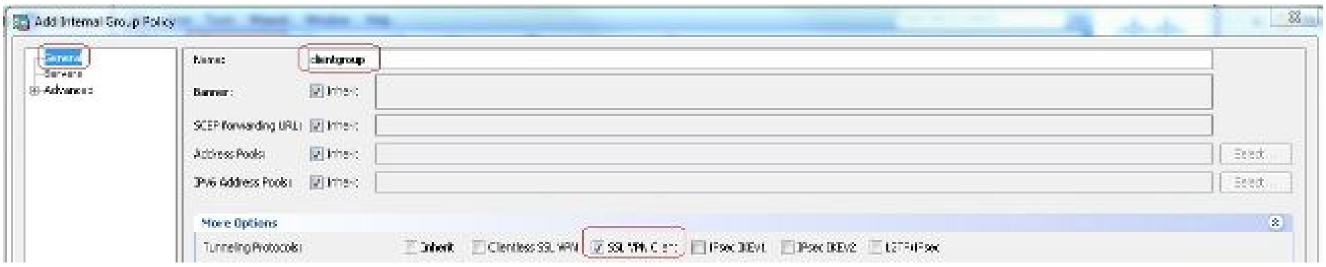
Add AnyConnect Client Image

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

等效的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. *配置組策略。 選擇* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *建立內部組策略* **clientgroup**.*在* **General** *頁籤，選擇* **SSL VPN Client** *覈取方塊以啟用WebVPN作為允許的隧道協定。*



Add Internal Group Policy

Name: clientgroup

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

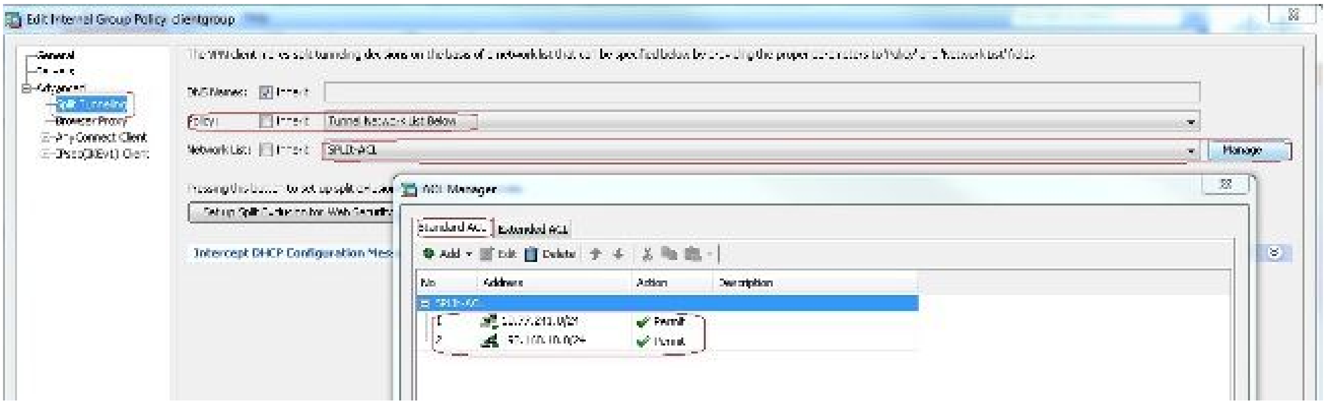
Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

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

在 **Advanced > Split Tunneling** *頁籤，選擇* **Tunnel Network List Below** *從策略下拉選單中，使來自遠端PC的所有資料包通過安全隧道。*



Edit Internal Group Policy: clientgroup

DNS Names: ☑ Inherit

Policy: □ Inherit Tunnel Network List Below

Network List: □ Inherit SPLIt-ACL

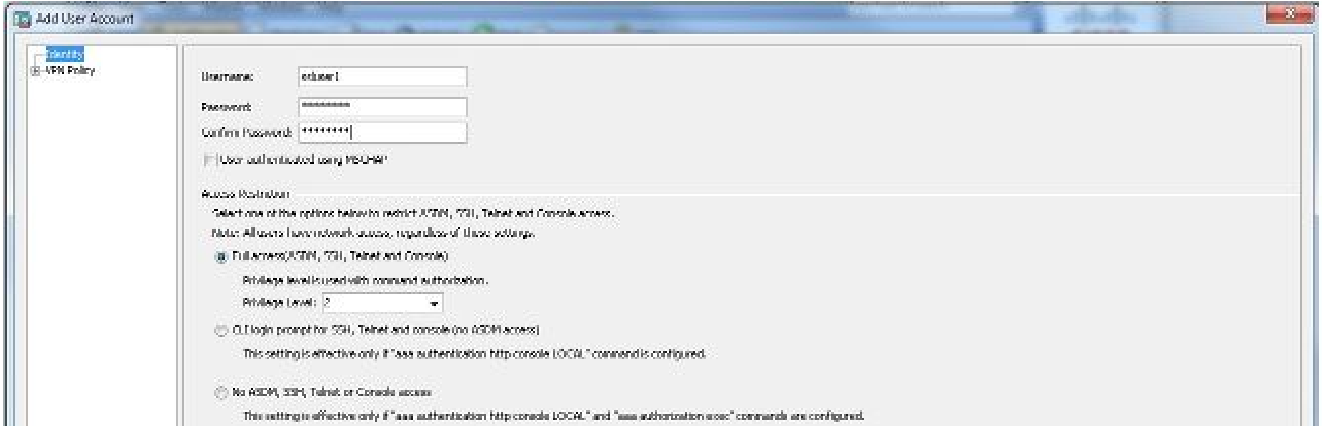
ACL Manager

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

等效的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. *選擇* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *建立新使用者帳戶* **ssluser1**.*按一下* **OK** *然後* **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.

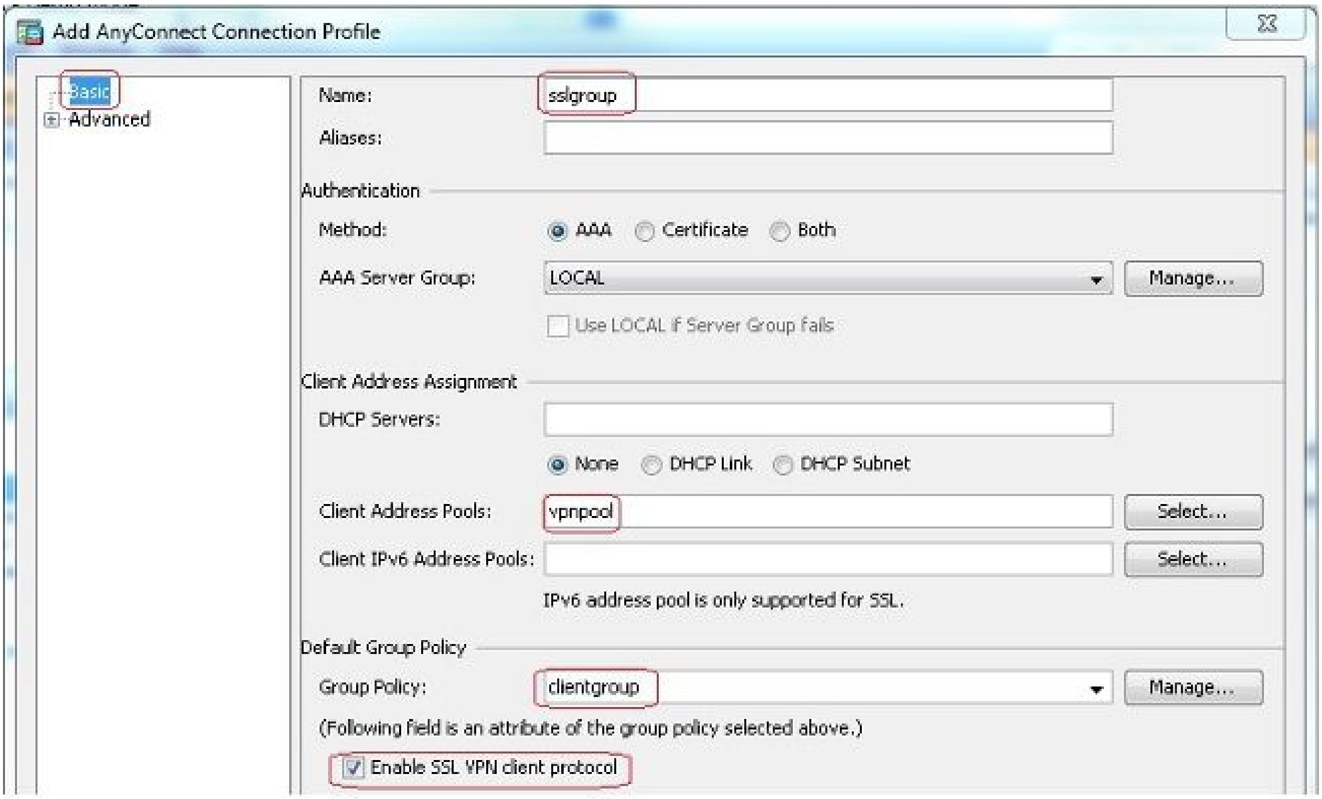
○ No ASDM, SSH, Telnet or Console access

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

等效的CLI配置：

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

6. *配置隧道組。 選擇* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *以建立新的隧道組* **sslgroup**.*在* **Basic** *頁籤中，您可以執行以下配置清單： 將隧道組命名為* **sslgroup**.*在* **Client Address Assignment**，*選擇地址池* **vpnpool** *從* **Client Address Pools** *下拉選單。在* **Default Group Policy**，*選擇組策略* **clientgroup** *從* **Group Policy** *下拉選單。*



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** 頁籤，將組別名指定為 **sslgroup_users** 然後按一下 **OK**. **等效的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)#
```

驗證

使用本節內容，確認您的組態是否正常運作。

- **show vpn-sessiondb svc** — 顯示有關當前SSL連線的資訊。

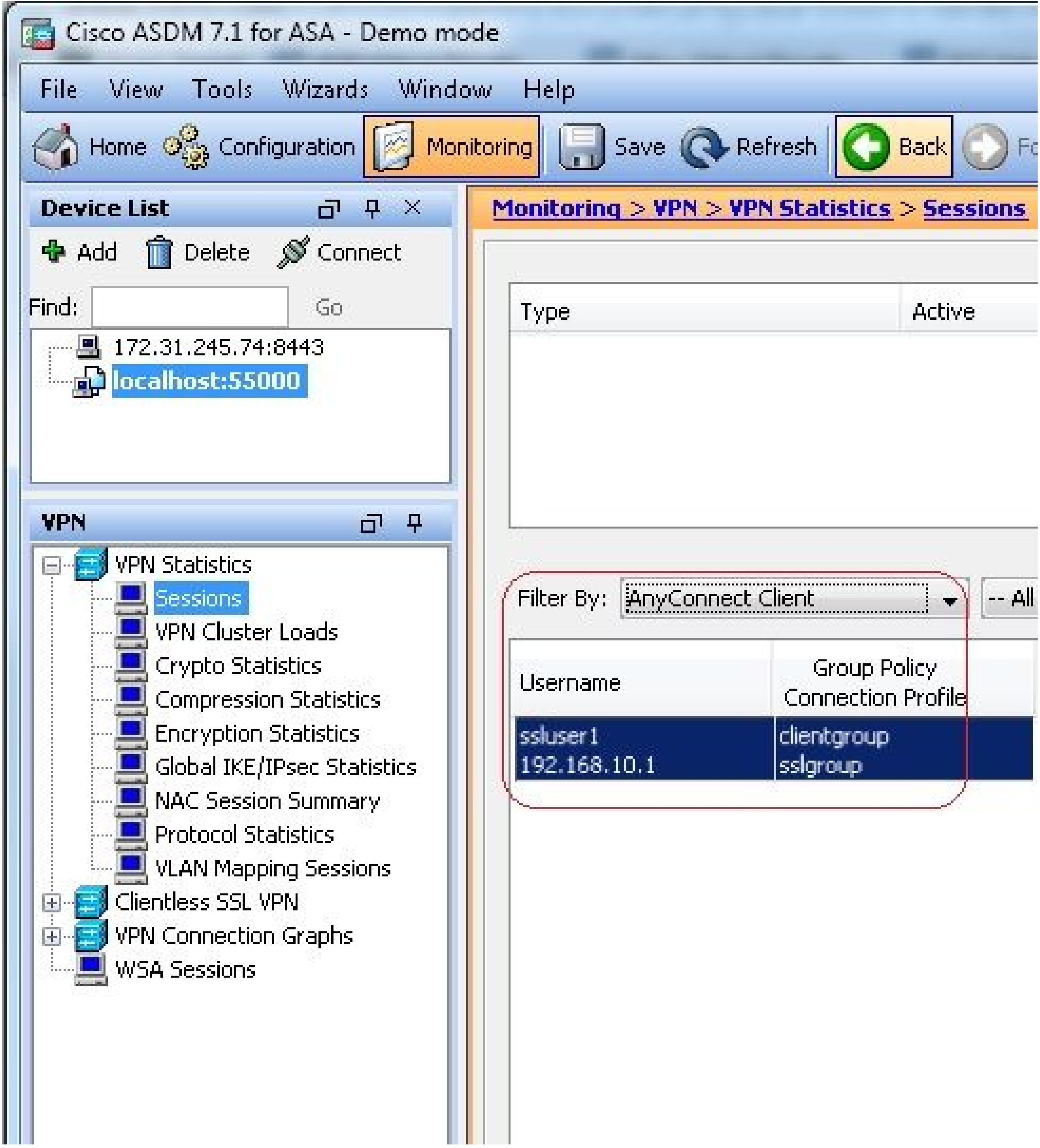
```
ciscoasa#show vpn-sessiondb anyconnect

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** — *顯示各種組的已配置別名。*

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

- *在ASDM中，選擇* **Monitoring > VPN > VPN Statistics > Sessions** *以便瞭解ASA中的當前會話。*



Filter By: AnyConnect Client

Username	Group Policy Connection Profile
ssluser1 192.168.10.1	clientgroup sslgroup

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- **vpn-sessiondb logoff name** — *用於註銷特定使用者名稱的SSL VPN會話的命令。*

```
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)
```

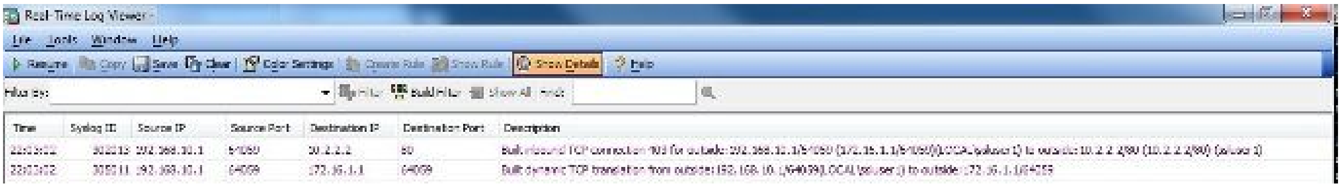
同樣，您可以使用 **vpn-sessiondb logoff anyconnect** *命令以終止所有AnyConnect會話。*

- **debug webvpn anyconnect <1-255>** — *提供即時webvpn事件以建立會話。*

```
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，選擇 **Monitoring > Logging > Real-time Log Viewer > View** 以便檢視即時事件。此範例顯示透過ASA 172.16.1.1在Internet中的AnyConnect 192.168.10.1和Telnet Server10.2.2.2之間的作業階段資訊。



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

相關資訊

- Cisco ASA 5500-X系列防火牆
- 單臂公共網際網路VPN的PIX/ASA和VPN客戶端配置示例
- 帶ASDM的ASA上的SSL VPN客戶端(SVC)配置示例
- 技術支援與文件 - Cisco Systems

關於此翻譯