Configuración del tráfico U-turn de AnyConnect VPN Client en ASA 9.X

Contenido

Introducción

Este documento describe cómo configurar un Cisco Adaptive Security Appliance (ASA) Versión 9.X para permitirle activar el tráfico VPN. Cubre este escenario de configuración: Tráfico en U de los clientes de acceso remoto.

> **Nota:** Para evitar una superposición de direcciones IP en la red, asigne un conjunto de direcciones IP completamente diferente al cliente VPN (por ejemplo, 10.x.x.x , 172.16.x.x y 192.168.x.x). Este esquema de direcciones IP es útil para resolver problemas de la red.

Horquilla o giro en U

Esta función es útil para el tráfico VPN que ingresa en una interfaz, pero luego se rutea fuera de esa misma interfaz. Por ejemplo, si tiene una red VPN radial donde el dispositivo de seguridad es el hub y las redes VPN remotas son radios, para que un radio se comunique con otro tráfico radial debe ir al dispositivo de seguridad y luego salir nuevamente al otro radio.

Escriba el **same-security-traffic** para permitir que el tráfico entre y salga de la misma interfaz.

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

Prerequisites

Requirements

Cisco recomienda cumplir estos requisitos antes de intentar realizar esta configuración:

- El dispositivo de seguridad ASA del hub debe ejecutar la versión 9.x.
- Cisco AnyConnect VPN Client 3.x**Nota:** Descargue el paquete AnyConnect VPN Client (anyconnect-win*.pkg) en Cisco Software Download (sólo clientes registrados). Copie el cliente VPN AnyConnect en la memoria flash de Cisco ASA, que se descargará a los equipos de los usuarios remotos para establecer la conexión VPN SSL con el ASA. Consulte la sección Conexiones de AnyConnect VPN Client de la guía de configuración de ASA para obtener más información.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 5500 Series ASA que ejecuta la versión de software 9.1(2)
- Cisco AnyConnect SSL VPN Client versión para Windows 3.1.05152
- PC que ejecuta un sistema operativo compatible según las plataformas VPN compatibles, Cisco ASA Series.
- Versión 7.1(6) de Cisco Adaptive Security Device Manager (ASDM)

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El Cisco AnyConnect VPN Client proporciona conexiones SSL seguras al dispositivo de seguridad para los usuarios remotos. Sin un cliente previamente instalado, los usuarios remotos ingresan la dirección IP en su navegador de una interfaz configurada para aceptar las conexiones VPN SSL. A menos que el dispositivo de seguridad esté configurado para redirigir **http://** solicitudes para **https://**, los usuarios deben introducir la URL en el formulario **https://**

.Una vez introducida la URL, el navegador se conecta a esa interfaz y muestra la pantalla de inicio de sesión. Si el usuario satisface los requisitos de inicio de sesión y autenticación, y el dispositivo de seguridad identifica al usuario como necesitado del cliente, descarga el cliente que coincide con el sistema operativo del equipo remoto. Después de la descarga, el cliente se instala y configura, establece una conexión SSL segura y permanece o se desinstala (esto depende de la configuración del dispositivo de seguridad) cuando la conexión finaliza.En el caso de un cliente previamente instalado, cuando el usuario realiza la autenticación, el dispositivo de seguridad examina la revisión del cliente y actualiza el cliente según sea necesario.Cuando el cliente negocia una conexión VPN SSL con el dispositivo de seguridad, se conecta con la seguridad de

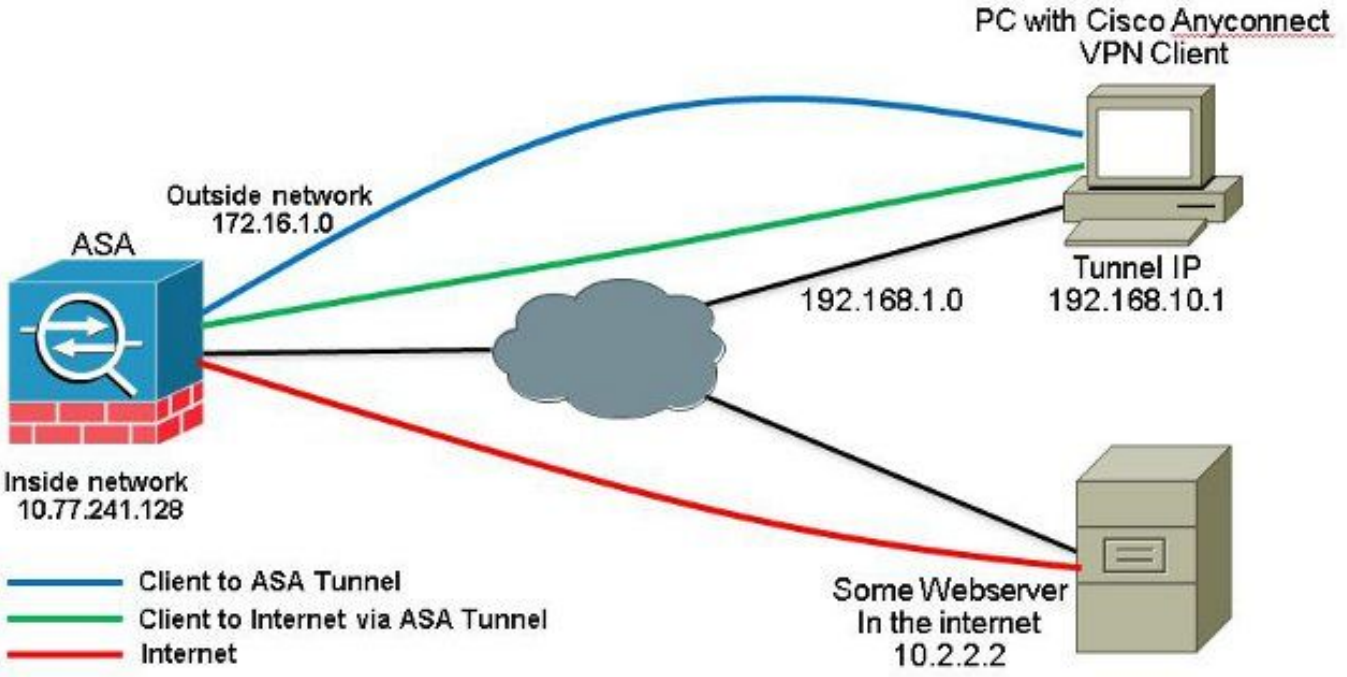
*la capa de transporte (TLS) y también utiliza la seguridad de la capa de transporte del datagrama (DTLS). DTLS evita los problemas de latencia y ancho de banda asociados con algunas conexiones SSL y mejora el rendimiento de las aplicaciones en tiempo real que son sensibles a las demoras de paquetes.El cliente AnyConnect puede ser descargado del dispositivo de seguridad, o puede ser instalado manualmente en el equipo remoto por el administrador del sistema. Para obtener más información sobre cómo instalar el cliente manualmente, consulte la Guía del administrador de Cisco AnyConnect Secure Mobility Client.El dispositivo de seguridad descarga el cliente en función de la política de grupo o los atributos de nombre de usuario del usuario que establece la conexión. Puede configurar el dispositivo de seguridad para descargar automáticamente el cliente, o puede configurarlo para indicarle al usuario remoto si debe descargar el cliente. En este último caso, si el usuario no responde, puede configurar el dispositivo de seguridad para que descargue el cliente después de un determinado tiempo de espera o presentar las páginas de registro.***Nota:*** *Los ejemplos utilizados en este documento utilizan IPv4. Para el tráfico de giro en U IPv6, los pasos son los mismos pero utilizan las direcciones IPv6 en lugar de IPv4.*

Configuración del tráfico de acceso remoto en sentido ascendente

En esta sección encontrará la información para configurar las funciones descritas en este documento.Nota: Utilice las guías Command References para obtener más información sobre los comandos utilizados en esta sección.

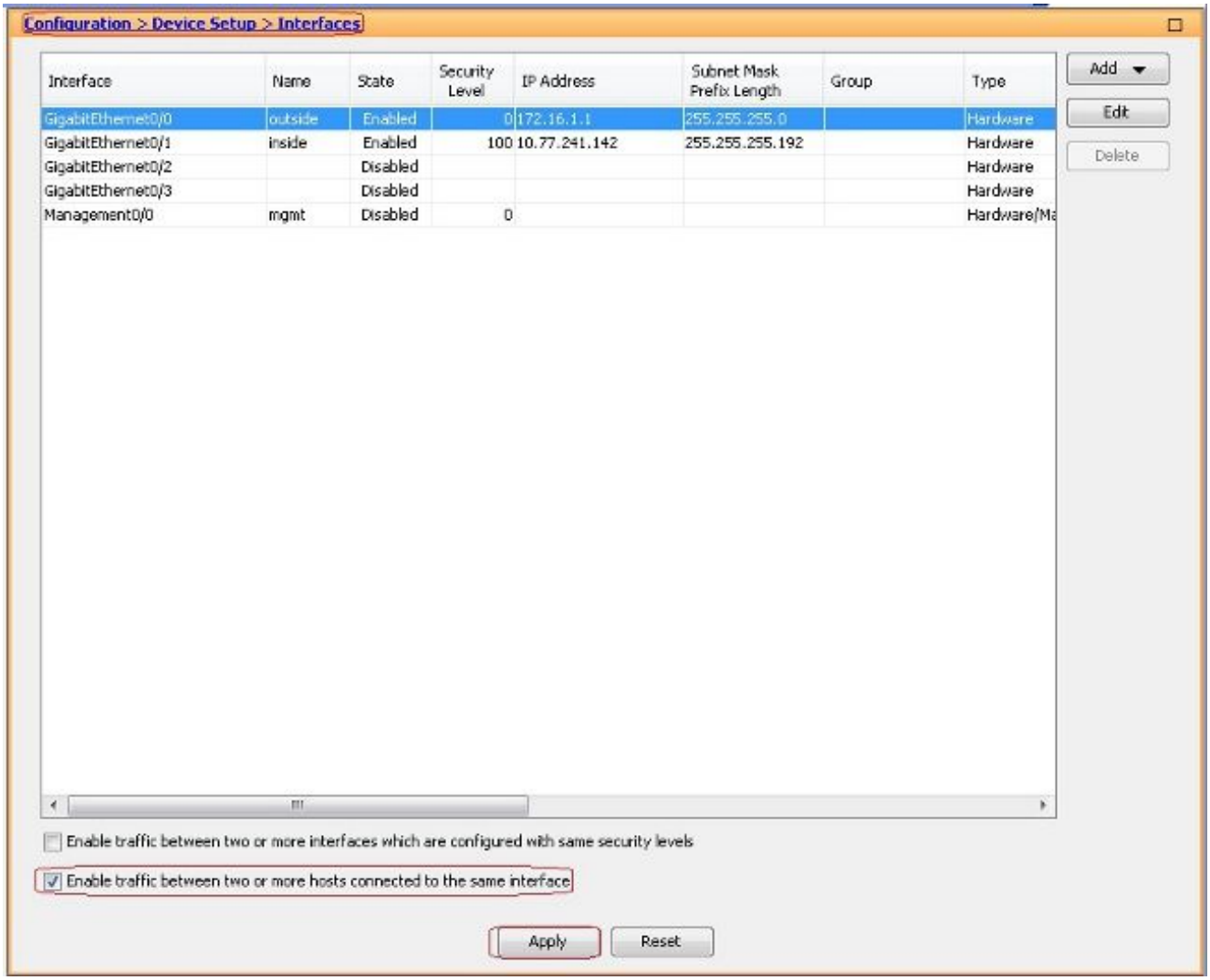
Ejemplo de Configuración de AnyConnect VPN Client for Public Internet VPN on a Stick

Diagrama de la redEn este documento, se utiliza esta configuración de red:



Configuraciones de ASA versión 9.1(2) con ASDM versión 7.1(6)Este documento asume que la configuración básica, tal como la configuración de la interfaz, ya se ha completado y funciona correctamente.Nota: Consulte Configuración del Acceso a la Administración para permitir que el ASA sea configurado por el ASDM.Nota: En la versión 8.0(2) y posteriores, ASA admite sesiones de VPN SSL (WebVPN) sin cliente y sesiones administrativas de ASDM simultáneamente en el puerto 443 de la interfaz externa. En las versiones anteriores a la versión 8.0(2), WebVPN y ASDM no se pueden habilitar en la misma interfaz ASA a menos que cambie los números de puerto. Consulte ASDM y WebVPN Habilitados en la Misma Interfaz de ASA para obtener más información.Complete estos pasos para configurar el SSL VPN en un palo en ASA:

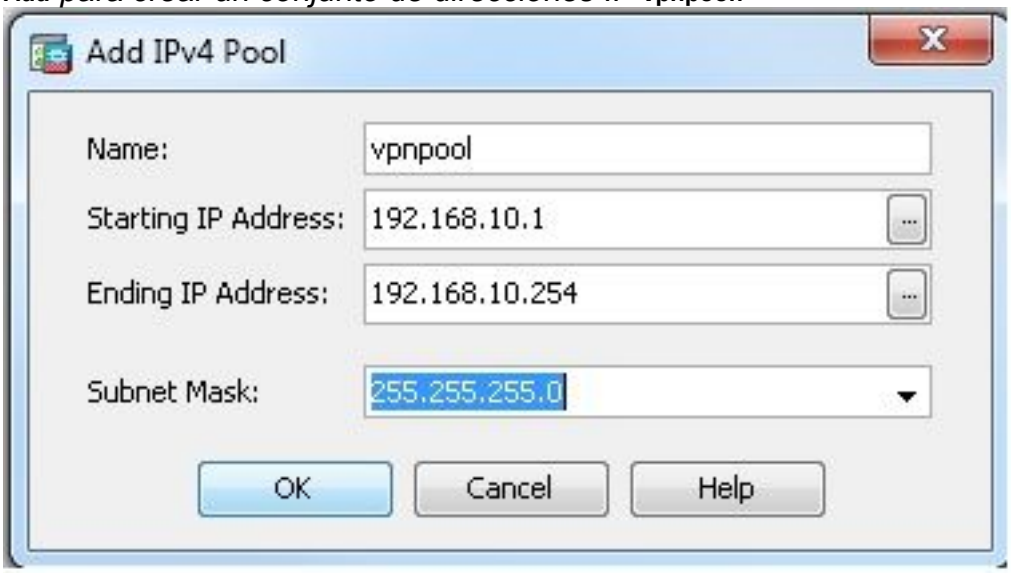
1. *Elegir* **Configuration > Device Setup > Interfaces** *y compruebe la* **Enable traffic between two or more hosts connected to the same interface** *para permitir que el tráfico SSL VPN entre y salga de la misma interfaz. Haga clic* **Apply**.



Configuración CLI Equivalente:

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

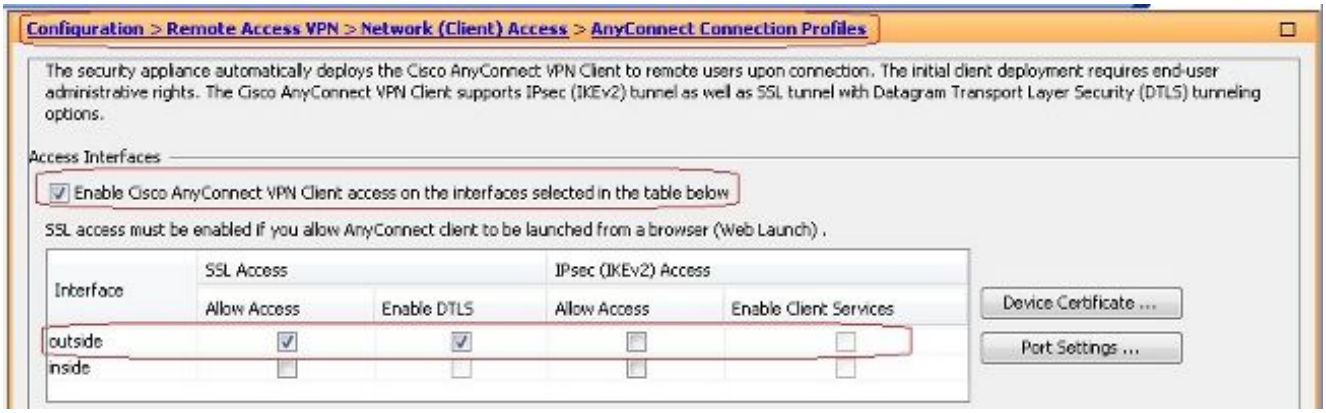
2. *Elegir* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add** *para crear un conjunto de direcciones IP* **vpnpool**.



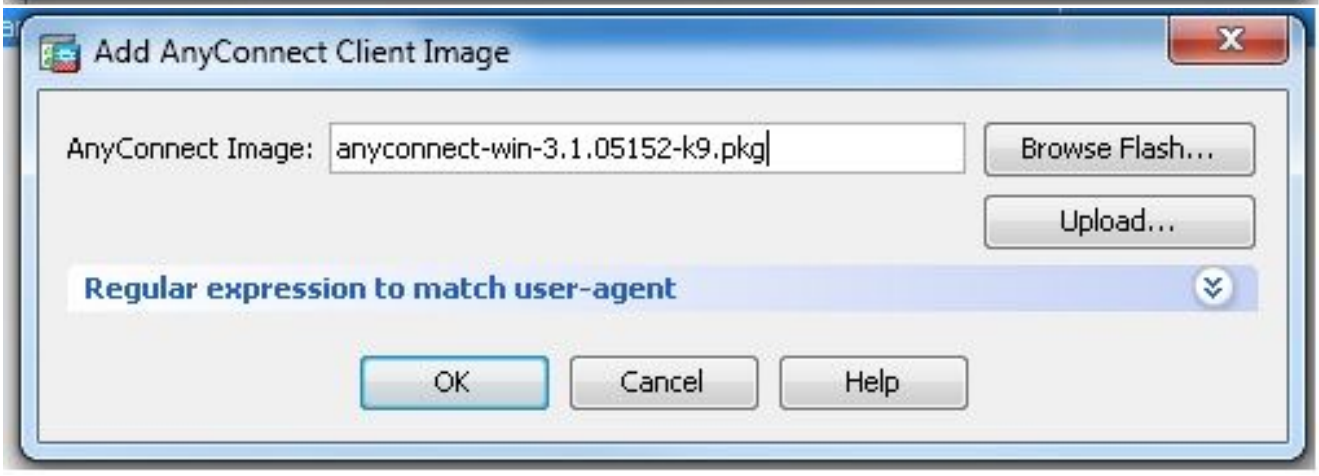
3. *Haga clic* **Apply**. ***Configuración CLI Equivalente:***

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

4. *Habilite WebVPN. Elegir* **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** *y en* **Access Interfaces**, *haga clic en las casillas de verificación* **Allow Access** *y* **Enable DTLS** *para la interfaz externa. Compruebe también el* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *para habilitar SSL VPN en la interfaz externa.*



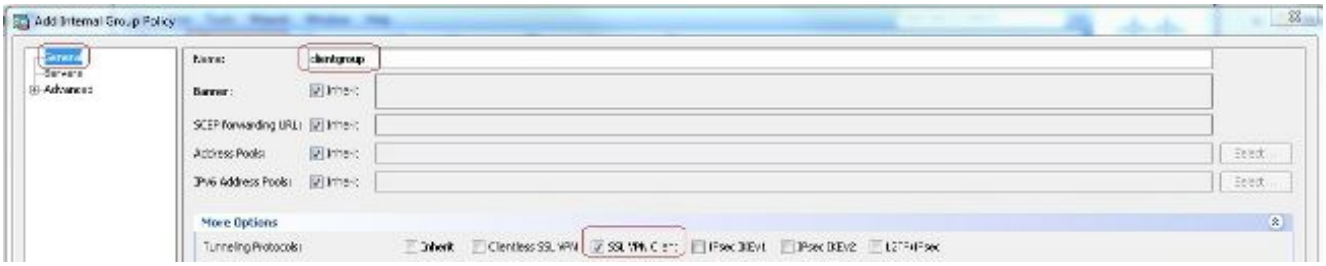
Haga clic **Apply**.*Elegir* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** *para agregar la imagen del cliente Cisco AnyConnect VPN desde la memoria flash de ASA como se muestra.*



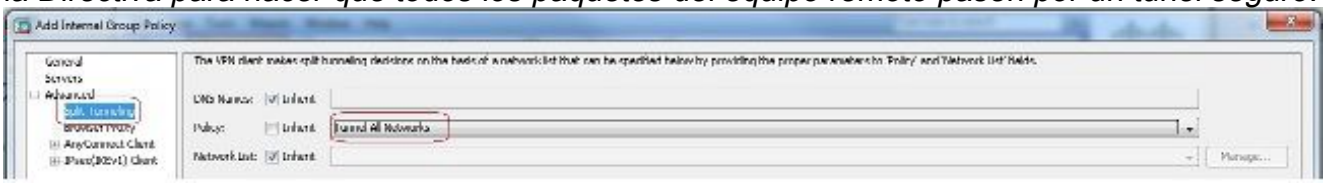
Configuración CLI Equivalente:

```
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 la Política de Grupo. Elegir* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *para crear una política de grupo interna* **clientgroup**. *En la* **General** *seleccione la ficha* **SSL VPN Client** *para habilitar el WebVPN como protocolo de túnel.*



En el **Advanced > Split Tunneling** *ficha, elija* **Tunnel All Networks** *de la lista desplegable Directiva de la Directiva para hacer que todos los paquetes del equipo remoto pasen por un túnel seguro.*



Configuración CLI Equivalente:

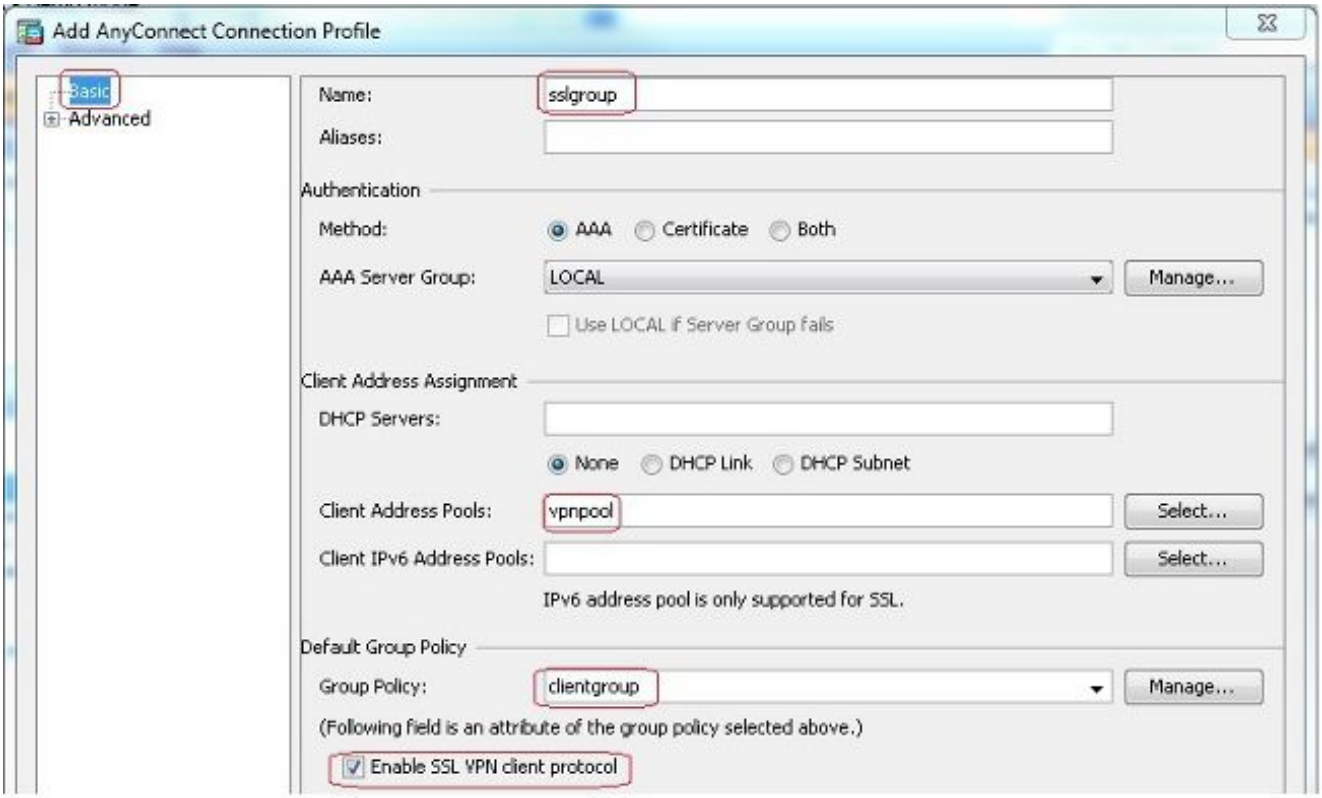
```
ciscoasa(config)#group-policy clientgroup internal
ciscoasa(config)#group-policyclientgroup attributes
ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client
ciscoasa(config-group-policy)#split-tunnel-policy tunnelall
```

6. *Elegir* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *para crear una nueva cuenta de usuario* **ssluser1**. *Haga clic* **OK** *y luego* **Apply**.

Configuración CLI Equivalente:

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

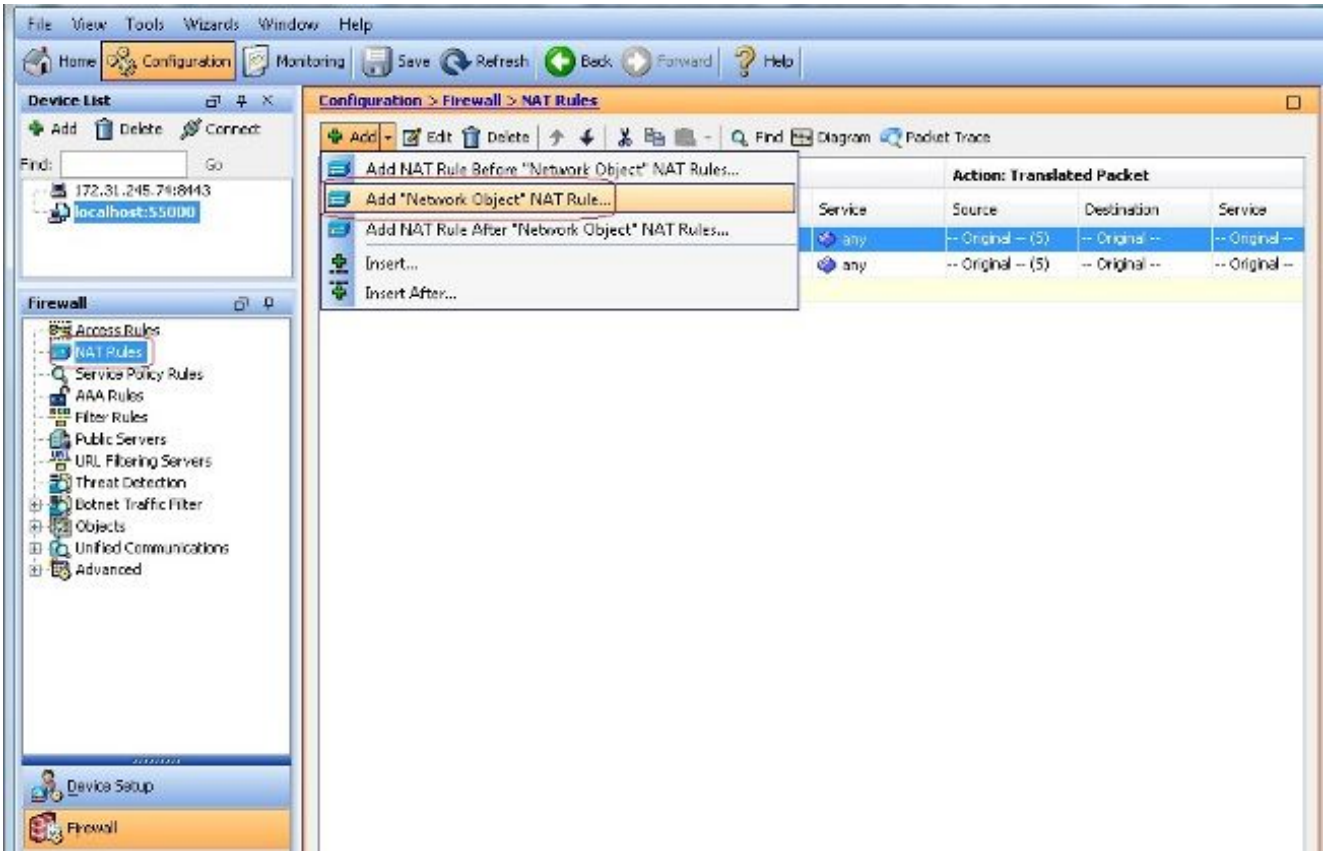
7. *Configure el Grupo de Túnel. Elegir* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *para crear un nuevo grupo de túnel* **sslgroup**.*En el* **Basic** *, puede realizar la lista de configuraciones como se muestra: Nombre el grupo de túnel como* **sslgroup**.*Bajo* **Client Address Assignment**, *elija el conjunto de direcciones* **vpnpool** *desde* **Client Address Pools** *lista desplegable.Bajo* **Default Group Policy**, *elija la política de grupo* **clientgroup** *desde* **Group Policy** *lista desplegable.*

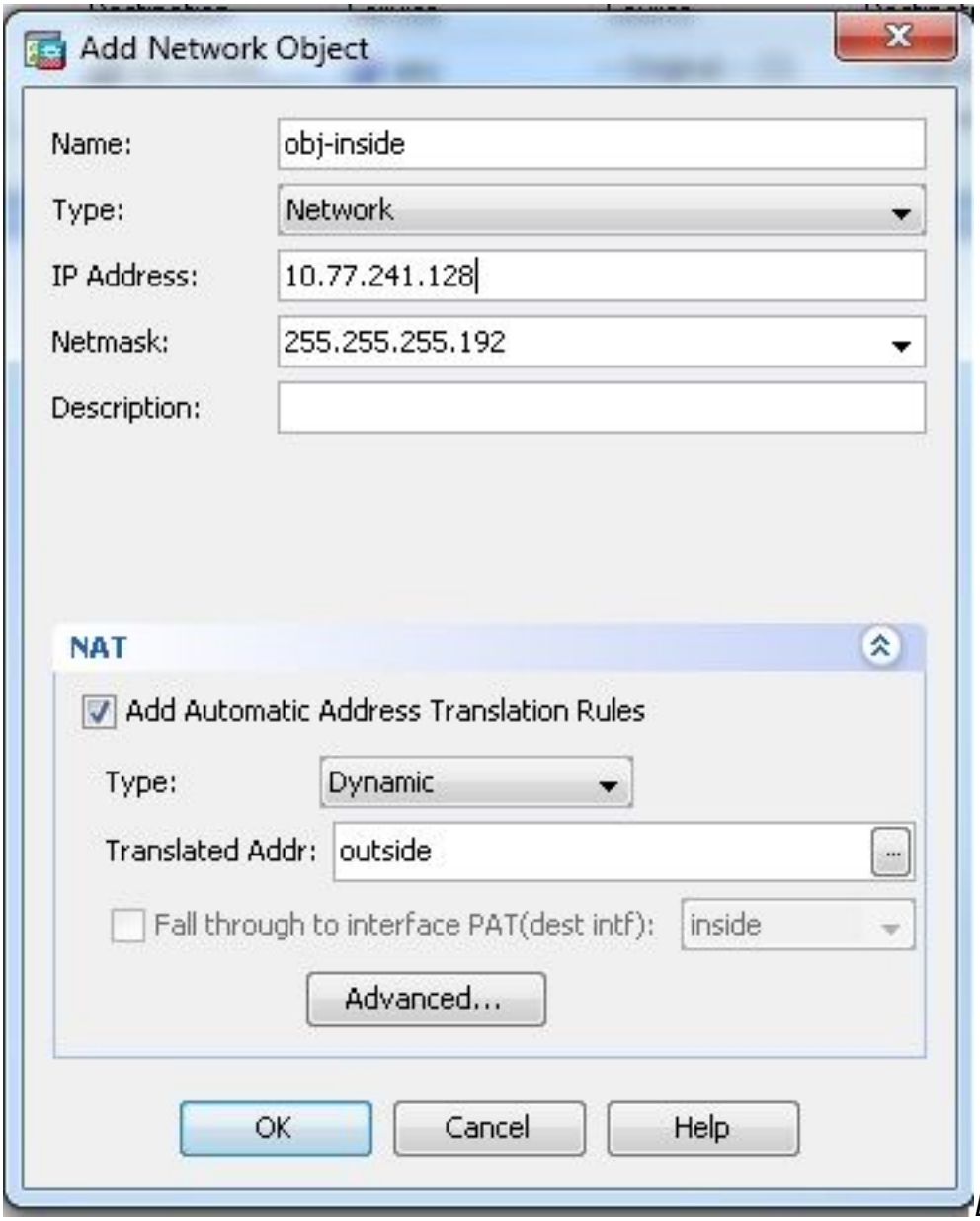


En la **Advanced > Group Alias/Group URL** *, especifique el nombre de alias del grupo como* **sslgroup_users** *y haga clic en* **OK**. ***Configuración CLI Equivalente:***

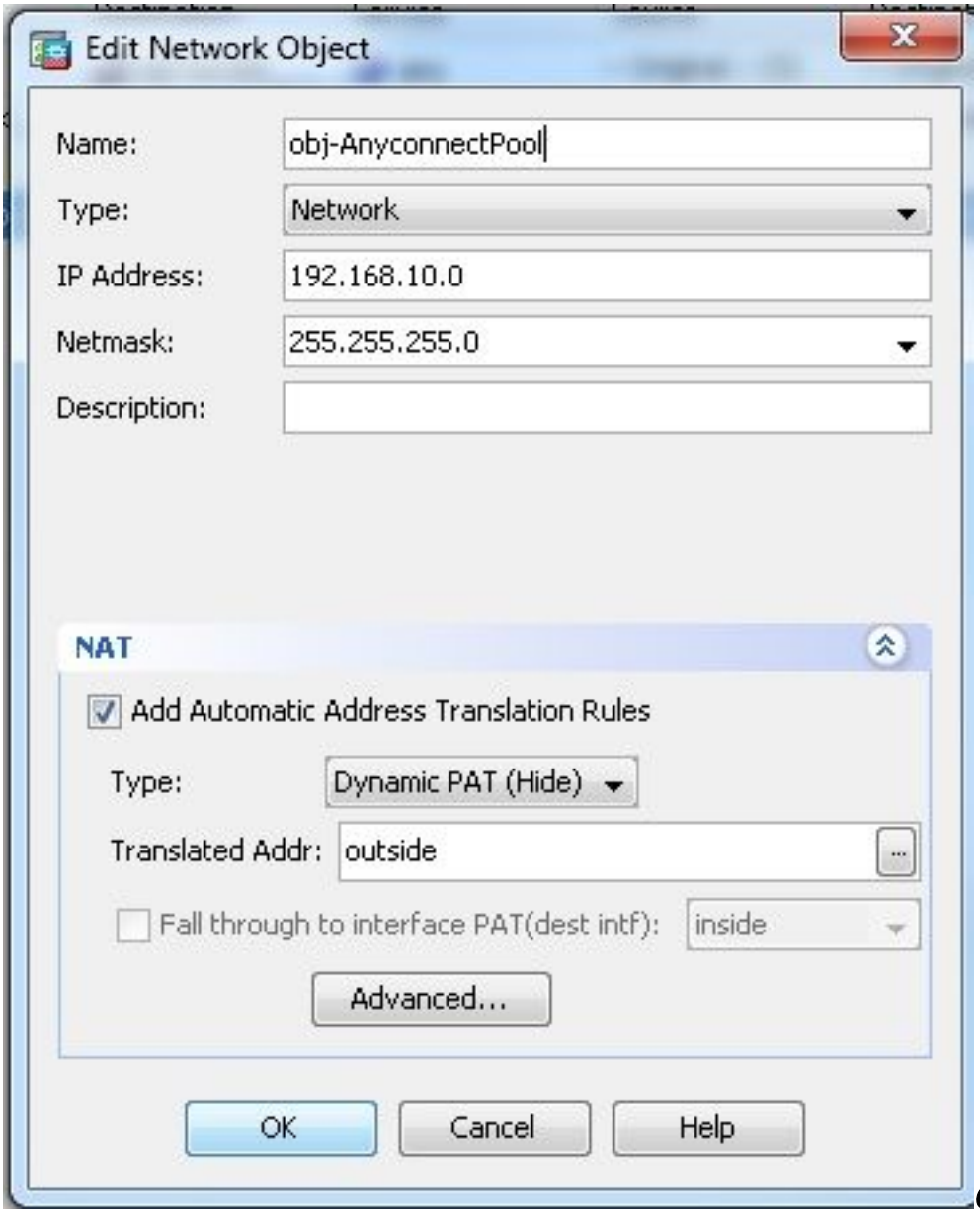
```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

8. *Configure el NAT Elegir* **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *por lo que el tráfico que proviene de la red interna se puede traducir con la dirección IP externa 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
172.31.245.71:8443
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 --



Elegir **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *por lo que el tráfico que el tráfico VPN que proviene de la red externa se puede traducir con la dirección IP externa 172.16.1.1.*



Configuración CLI

Equivalente:

```
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
```

Configuración de ASA versión 9.1(2) en la CLI

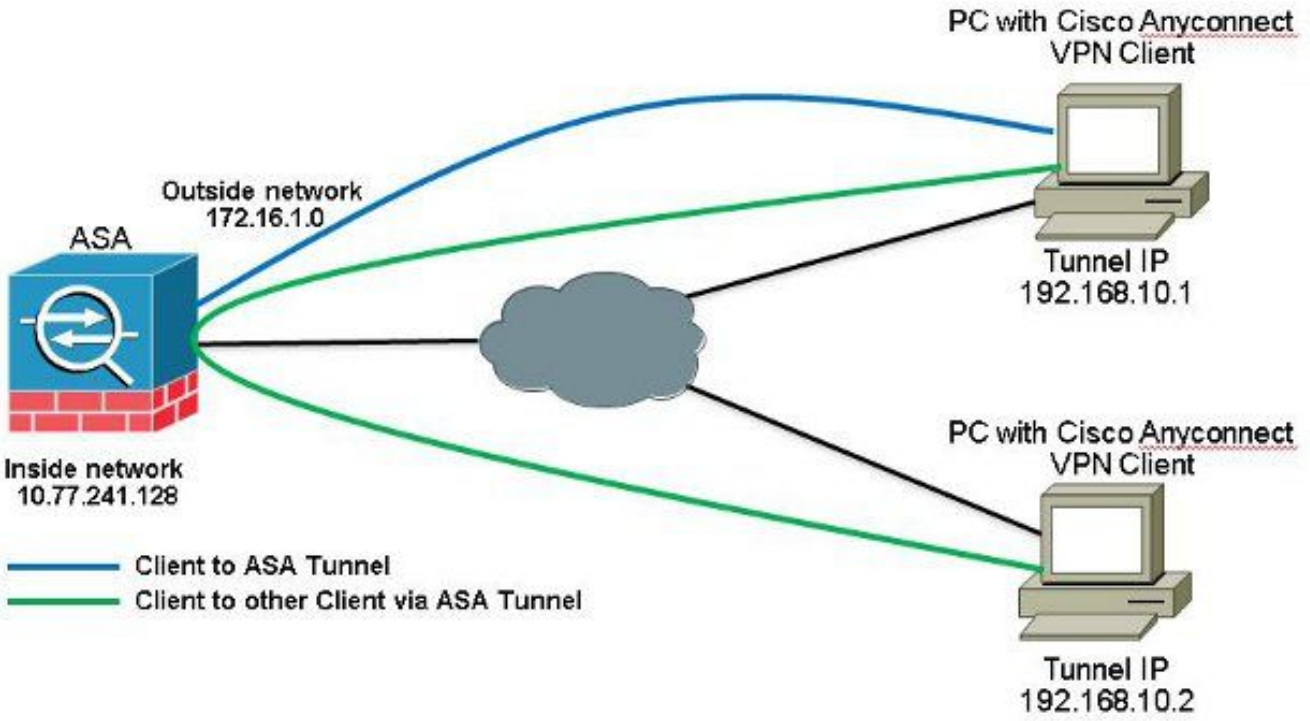
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1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

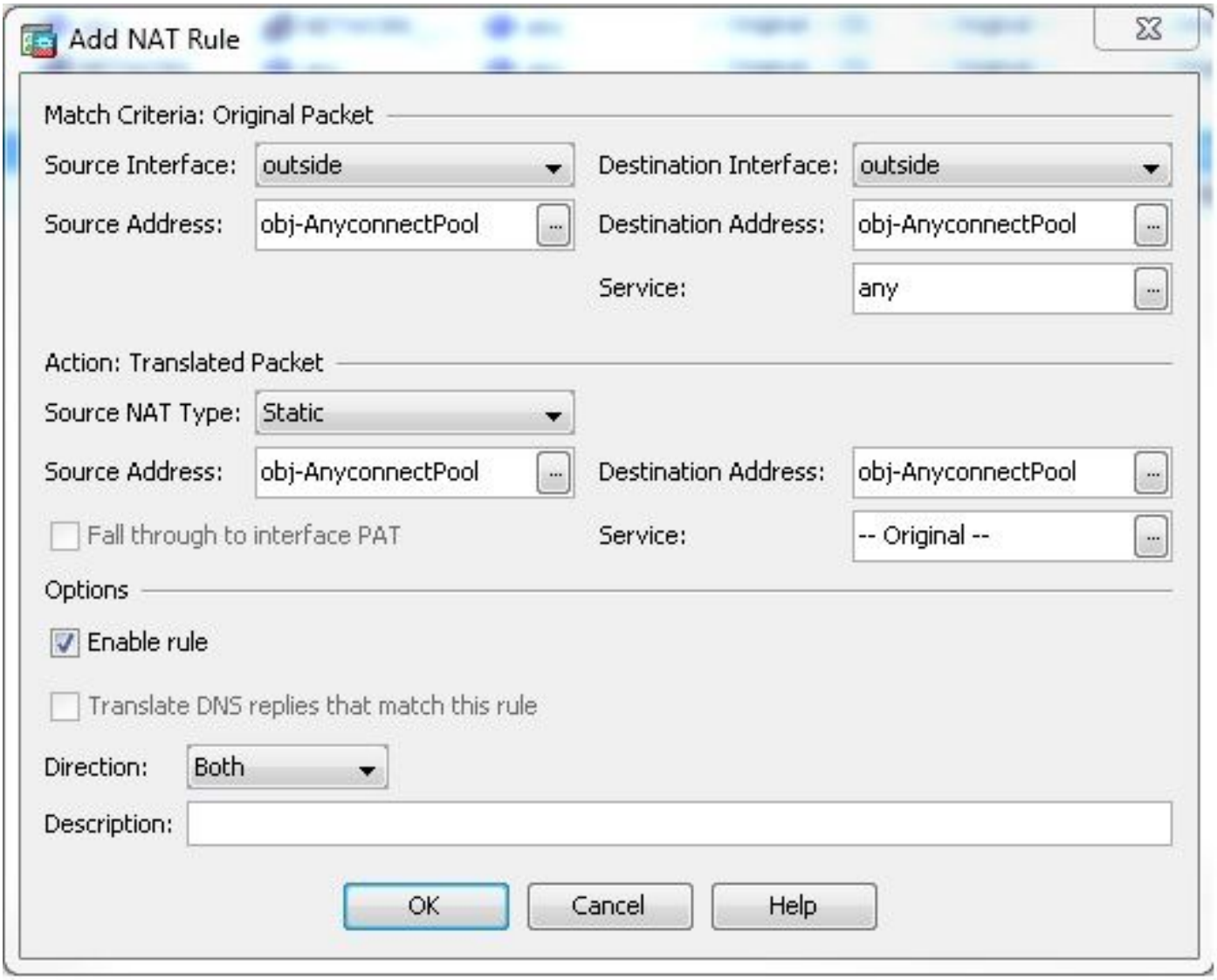
```
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 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)#
```

Permitir la comunicación entre los clientes VPN AnyConnect con la configuración TunnelAll en contextoDiagrama de la red



Si se requiere la comunicación entre los clientes de Anyconnect y la NAT para el Internet público en un dispositivo está en su lugar; también se necesita una NAT manual para permitir la comunicación bidireccional.Este es un escenario común cuando los clientes de Anyconnect utilizan servicios telefónicos y deben poder llamarse entre sí.Configuraciones de ASA versión 9.1(2) con ASDM versión 7.1(6)Elegir Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules por lo tanto, el tráfico que proviene de la red externa (AnyConnect Pool) y está destinado a otro cliente Anyconnect del mismo grupo no se traduce con la dirección IP externa 172.16.1.1.



Configuración CLI Equivalente:

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

Configuración de ASA versión 9.1(2) en la CLI

```
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
```

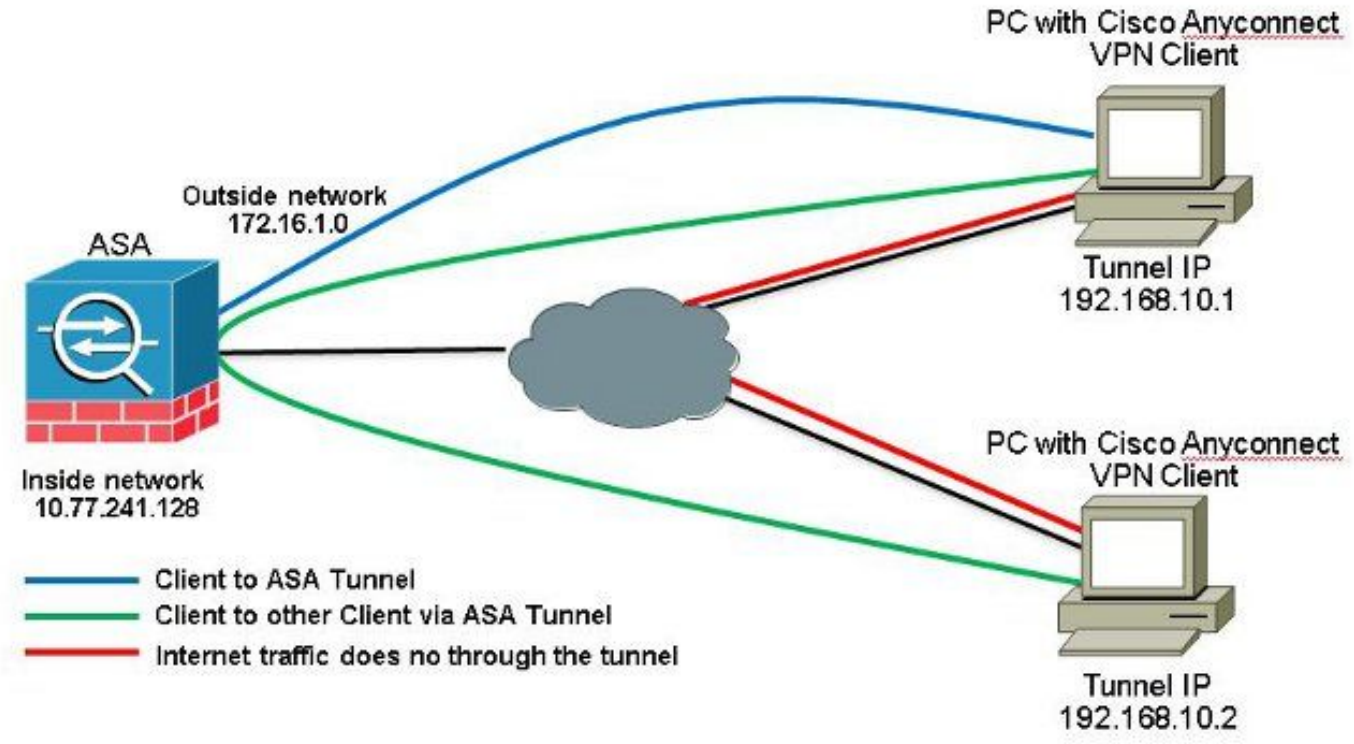
```
no ip address

!
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)#
```

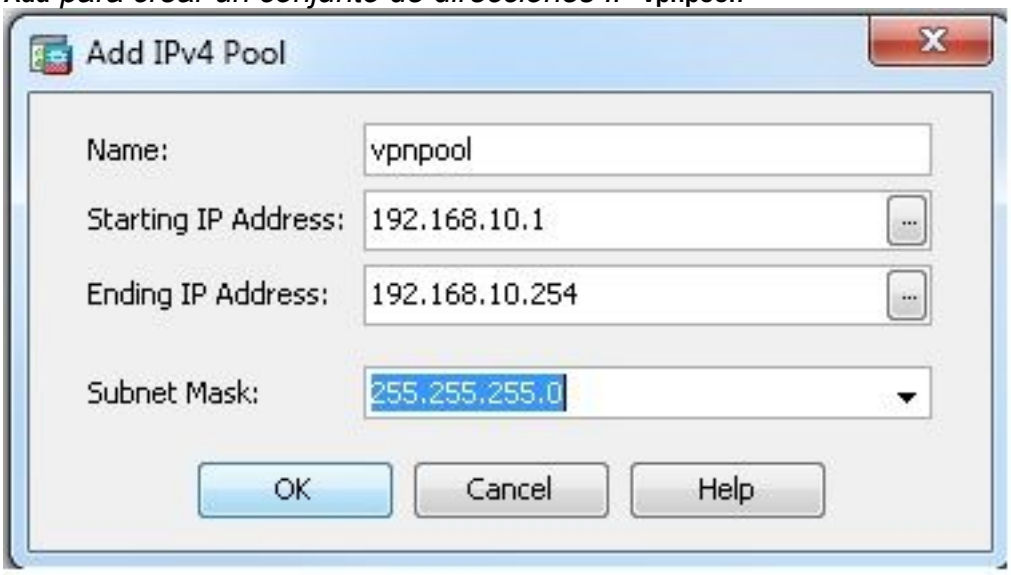
Permitir la comunicación entre clientes VPN AnyConnect con túnel dividido

Diagrama de la red

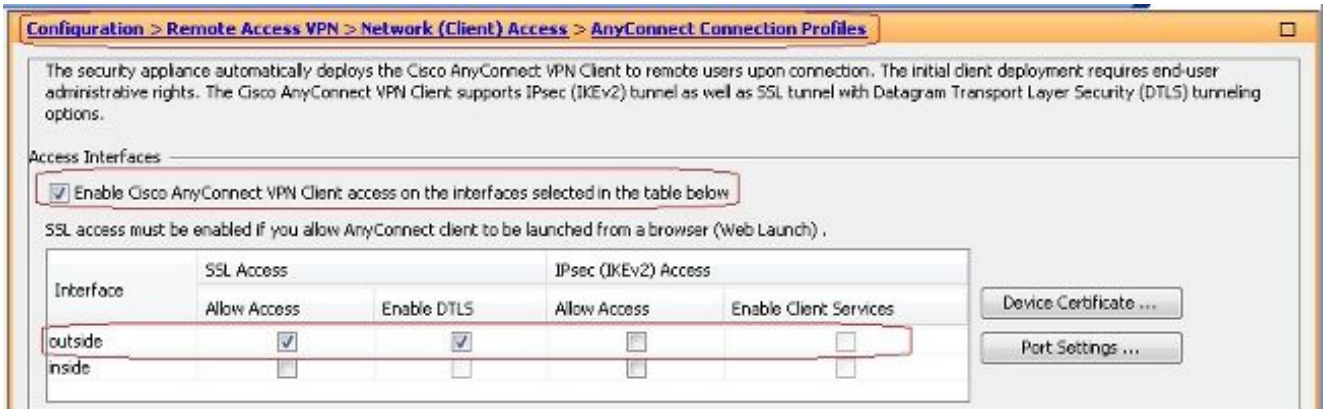


Si se requiere comunicación entre los clientes de Anyconnect y se utiliza el túnel dividido; no se requiere NAT manual para permitir la comunicación bidireccional a menos que haya una regla NAT que afecte a este tráfico configurado. Sin embargo, el conjunto VPN de Anyconnect debe incluirse en la ACL de túnel dividido.Este es un escenario común cuando los clientes de Anyconnect utilizan servicios telefónicos y deben poder llamarse entre sí.Configuraciones de ASA versión 9.1(2) con ASDM versión 7.1(6)

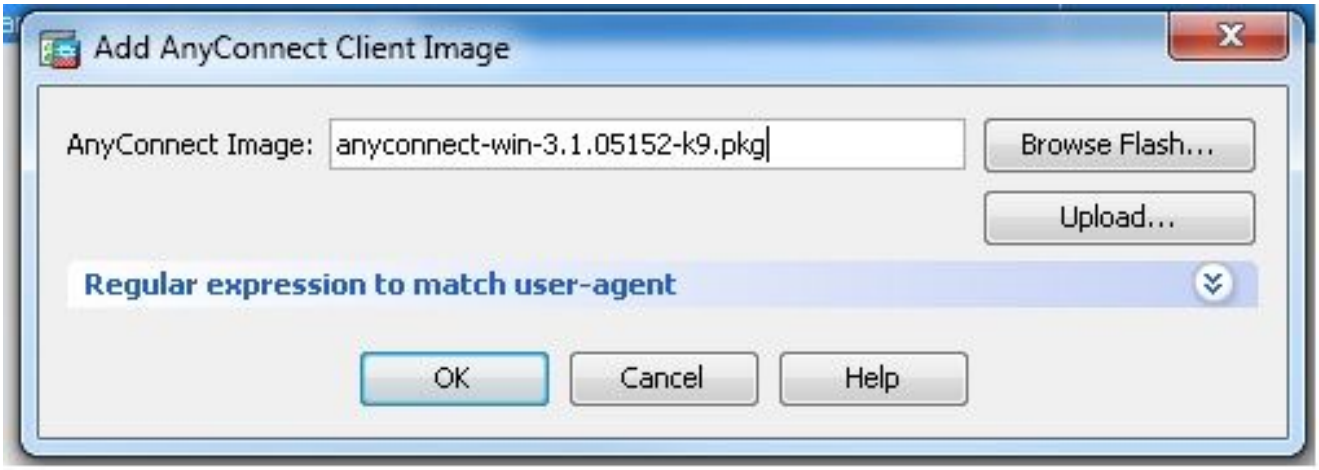
1. *Elegir* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment> Address Pools > Add** *para crear un conjunto de direcciones IP* **vpnpool**.



2. *Haga clic* **Apply**. ***Configuración CLI Equivalente:***
```
ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
```
3. *Habilite WebVPN. Elegir* **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** *y en* **Access Interfaces**, *haga clic en las casillas de verificación* **Allow Access** *y* **Enable DTLS** *para la interfaz externa. Compruebe también el* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *para habilitar SSL VPN en la interfaz externa.*



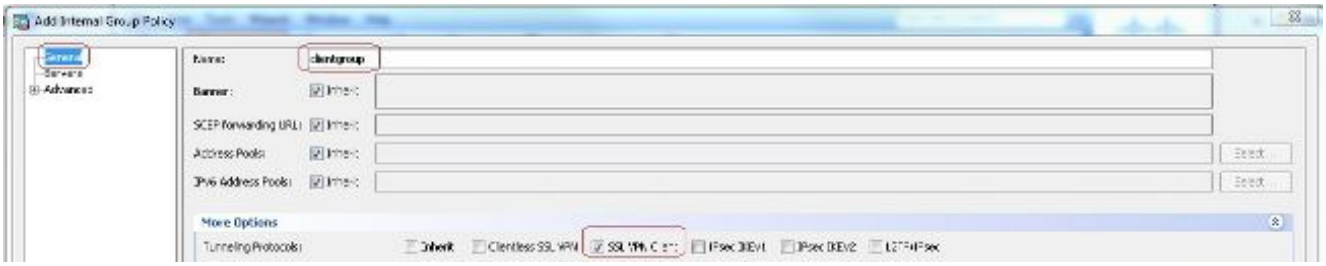
Haga clic **Apply**.*Elegir* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** *para agregar la imagen del cliente Cisco AnyConnect VPN desde la memoria flash de ASA como se muestra.*



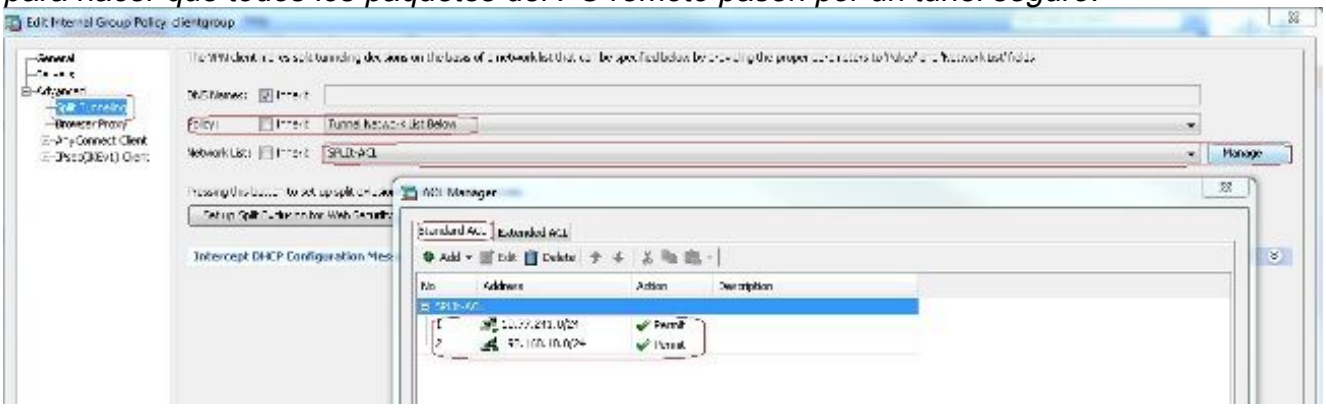
Configuración CLI Equivalente:

```
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 la Política de Grupo. Elegir* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *para crear una política de grupo interna* **clientgroup**. *En la* **General** *seleccione la ficha* **SSL VPN Client** *para habilitar el WebVPN como un protocolo de túnel permitido.*



En el **Advanced > Split Tunneling** *ficha, elija* **Tunnel Network List Below** *de la lista desplegable Policy para hacer que todos los paquetes del PC remoto pasen por un túnel seguro.*



Configuración CLI Equivalente:

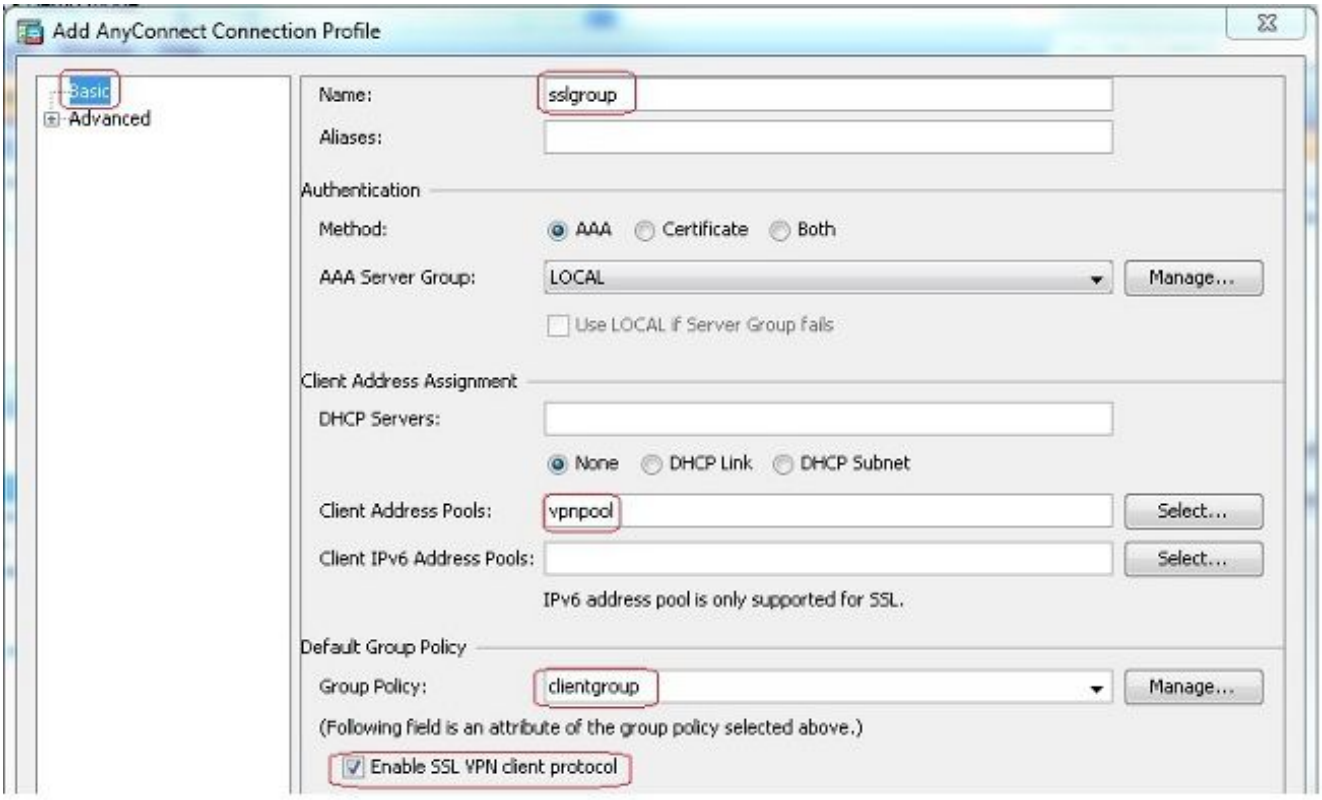
```
ciscoasa(config)#access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0
ciscoasa(config)#access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

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. *Elegir* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *para crear una nueva cuenta de usuario* **ssluser1**. *Haga clic* **OK** *y luego* **Apply**.

Configuración CLI Equivalente:

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

6. *Configure el Grupo de Túnel. Elegir* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *para crear un nuevo grupo de túnel* **sslgroup**.*En el* **Basic** *, puede realizar la lista de configuraciones como se muestra: Nombre el grupo de túnel como* **sslgroup**.*Bajo* **Client Address Assignment**, *elija el conjunto de direcciones* **vpnpool** *desde* **Client Address Pools** *lista desplegable.Bajo* **Default Group Policy**, *elija la política de grupo* **clientgroup** *desde* **Group Policy** *lista desplegable.*



En la **Advanced > Group Alias/Group URL** *, especifique el nombre de alias del grupo como* **sslgroup_users** *y haga clic en* **OK**. ***Configuración CLI Equivalente:***

```
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
```

Configuración de ASA versión 9.1(2) en la CLI

```
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)#
```

Verificación *Use esta sección para confirmar que su configuración funciona correctamente.*

- **show vpn-sessiondb svc** - *Muestra la información sobre las conexiones SSL actuales.*

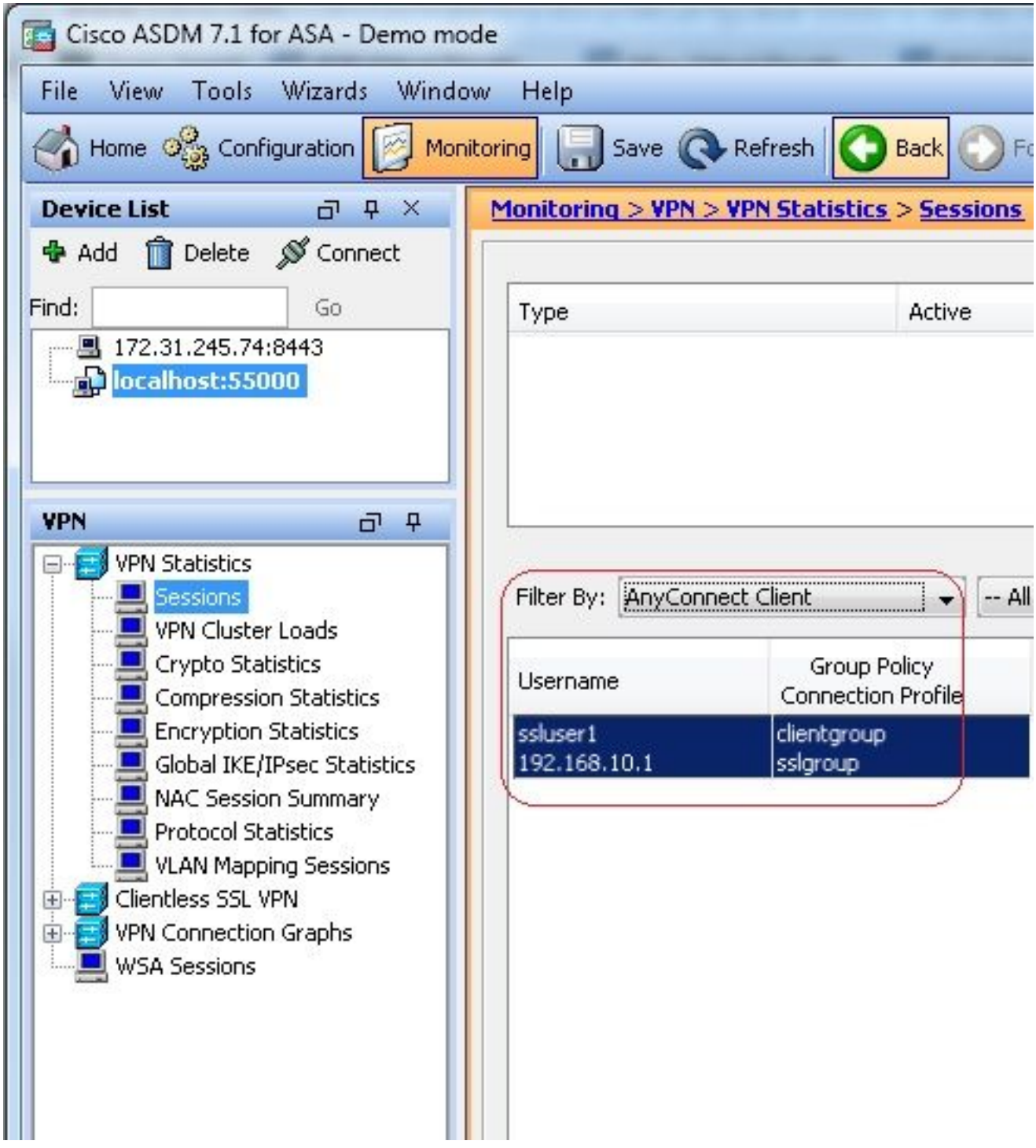
```
ciscoasa#show vpn-sessiondb anyconnect

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** - *Muestra el alias configurado para varios grupos.*

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

- *En ASDM, elija* **Monitoring > VPN > VPN Statistics > Sessions** *para conocer las sesiones actuales en el ASA.*



Troubleshoot *En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.*

- **vpn-sessiondb logoff name** - *Comando para cerrar la sesión VPN SSL para el nombre de usuario específico.*

```
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)
```

De forma similar, puede utilizar el **vpn-sessiondb logoff anyconnect** *para finalizar todas las sesiones de AnyConnect.*

- **debug webvpn anyconnect <1-255>** - *Proporciona los eventos webvpn en tiempo real para establecer la sesión.*

```
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
```

- *En ASDM, elija* **Monitoring > Logging > Real-time Log Viewer > View** *para ver los eventos en tiempo real. Este ejemplo muestra la información de sesión entre AnyConnect 192.168.10.1 y Telnet Server 10.2.2.2 en Internet a través de ASA 172.16.1.1.*

Información Relacionada

- [Firewalls Cisco ASA serie 5500-X]
- [Ejemplo de Configuración de PIX/ASA y Cliente VPN para VPN de Internet Pública en un Sentido]
- [Ejemplo de Configuración de SSL VPN Client (SVC) en ASA con ASDM]
- [Soporte Técnico y Documentación - Cisco Systems]

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).