

# ASA 8.x: Ejemplo de Configuración de Allow Split Tunneling for AnyConnect VPN Client en ASA

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de ASA con ASDM 6.0\(2\)](#)

[Configuración CLI ASA](#)

[Establezca la Conexión VPN SSL con el SVC](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento proporciona instrucciones paso a paso sobre cómo permitir el acceso de Cisco AnyConnect VPN client a Internet mientras son tunelados en un Cisco Adaptive Security Appliance (ASA) 8.0.2. Esta configuración permite al cliente el acceso seguro a recursos corporativos a través de la SSL y otorga acceso no seguro a Internet con la tunelización dividida.

## [Prerequisites](#)

### [Requirements](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El ASA Security Appliance debe ejecutar la versión 8.x
- Cisco AnyConnect VPN Client 2.x **Nota:** Descargue el paquete AnyConnect VPN Client (anyconnect-win\*.pkg) de Cisco [Software Download \(sólo clientes registrados\)](#) . Copie el AnyConnect VPN client en la memoria flash ASA, que será descargada a los equipos de los usuarios remotos para establecer la conexión SSL VPN con el ASA. Consulte la sección [Instalación de AnyConnect Client de la guía de configuración 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 8.0(2)
- Cisco AnyConnect SSL VPN Client versión para Windows 2.0.0343
- PC que ejecuta Microsoft Vista, Windows XP SP2 o Windows 2000 Professional SP4 con Microsoft Installer versión 3.1
- Cisco Adaptive Security Device Manager (ASDM) versión 6.0(2)

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

## Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

## 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 se configure para redireccionar las solicitudes de http:// a https://, los usuarios deben ingresar el URL en la forma https://<dirección>.

Después de ingresar el URL, el navegador se conecta con dicha interfaz y visualiza la pantalla de login. Si el usuario satisface el login y la autenticación, y el dispositivo de seguridad identifica que el usuario solicita el cliente, descarga el cliente que corresponde según el sistema operativo del equipo remoto. Una vez finalizada la descarga, el cliente se instala y se configura, establece una conexión SSL segura y se mantiene o se desinstala (según 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 Capa de Transporte (TLS), y opcionalmente, la Seguridad de Capa de Transporte de Datagrama (DTLS). La DTLS evita la latencia y los problemas de ancho de banda asociados con algunas conexiones SSL, y mejoran el funcionamiento de las aplicaciones en tiempo real que son sensibles a los retrasos 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. Consulte [Guía del Administrador de Cisco AnyConnect VPN Client](#) para obtener más información sobre cómo instalar el cliente manualmente.

El dispositivo de seguridad descarga el cliente en función de los atributos de la política de grupo o 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.

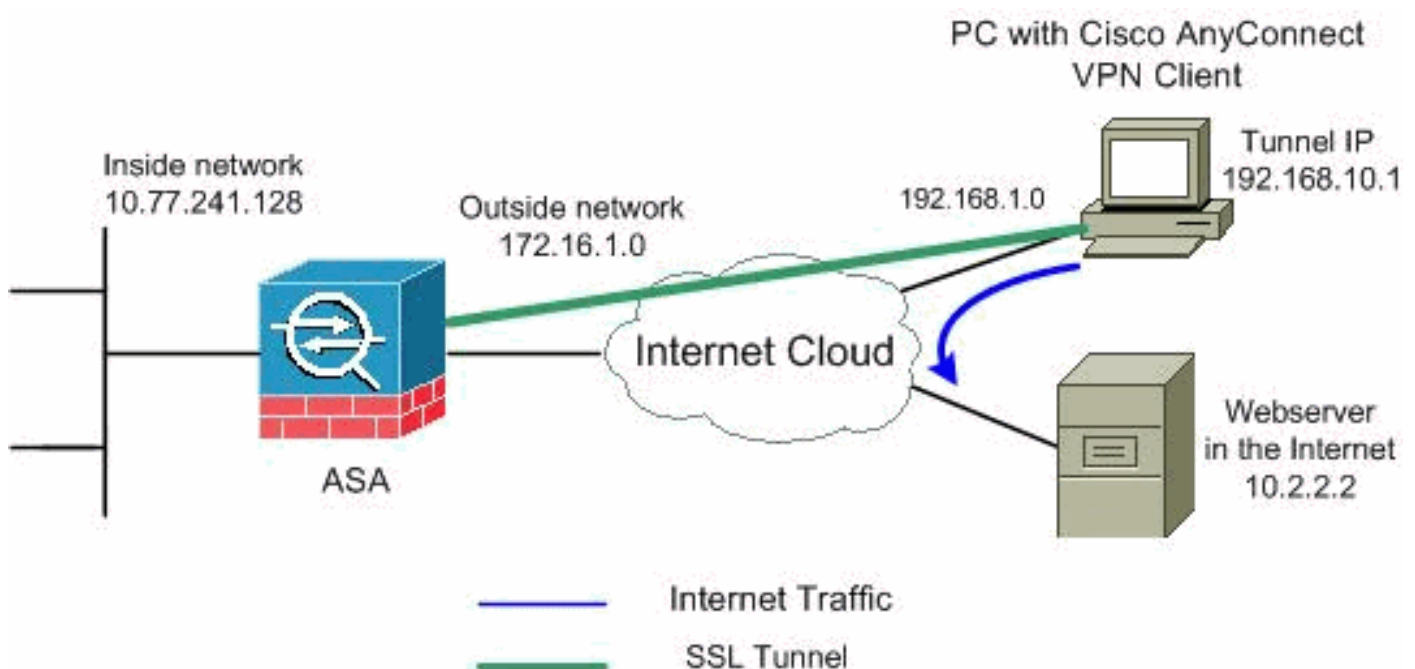
## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Utilice la herramienta [Command Lookup](#) (sólo para clientes [registrados](#)) para obtener más información sobre los comandos utilizados en esta sección.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



**Nota:** Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Son [direcciones RFC 1918](#) que se han utilizado en un entorno de laboratorio.

## Configuración de ASA con ASDM 6.0(2)

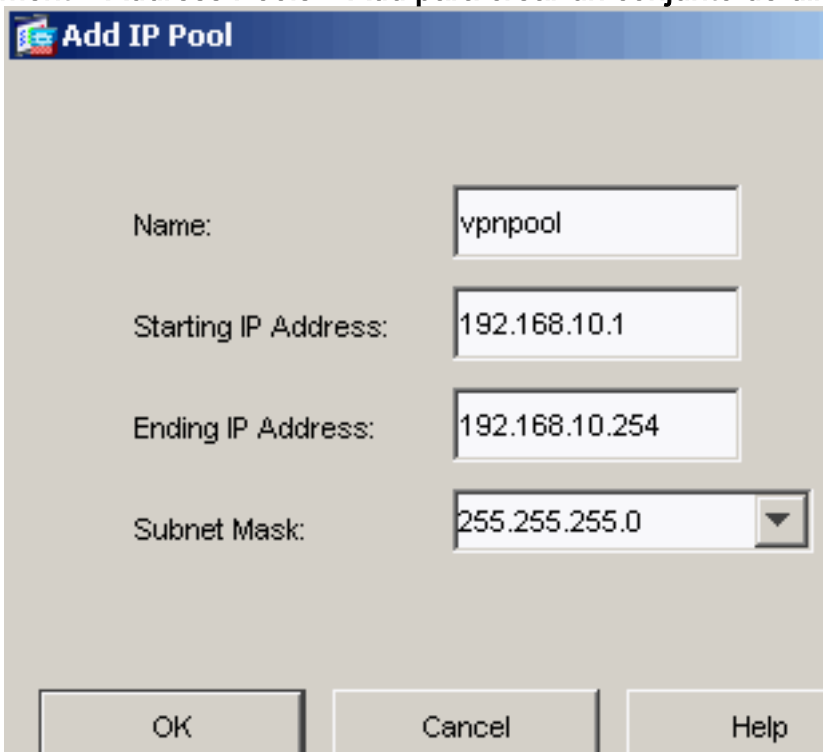
Este documento supone que la configuración básica, tal como la configuración de la interfaz, ya fue realizada y funciona correctamente.

**Nota:** Consulte [Permiso de Acceso HTTPS para ASDM](#) para permitir que el ASA sea configurado por el ASDM.

**Nota:** 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](#).

Siga estos pasos para configurar el SSL VPN en el ASA con la tunelización dividida:

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



**Add IP Pool**

Name: vpnpool

Starting IP Address: 192.168.10.1

Ending IP Address: 192.168.10.254

Subnet Mask: 255.255.255.0

OK Cancel Help

vpnpool.

2. Haga clic en Apply (Aplicar). Configuración CLI Equivalente:
3. Habilite WebVPN. Elija **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** y, debajo de **Access Interfaces**, haga clic en los cuadros de verificación **Allow Access and Enable DTLS** para la interfaz externa. También verifique la Casilla de Selección **Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interface selected in the table below** para habilitar SSL VPN en la interfaz exterior.

**Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles**

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at [Client Settings](#))

**Access Interfaces**

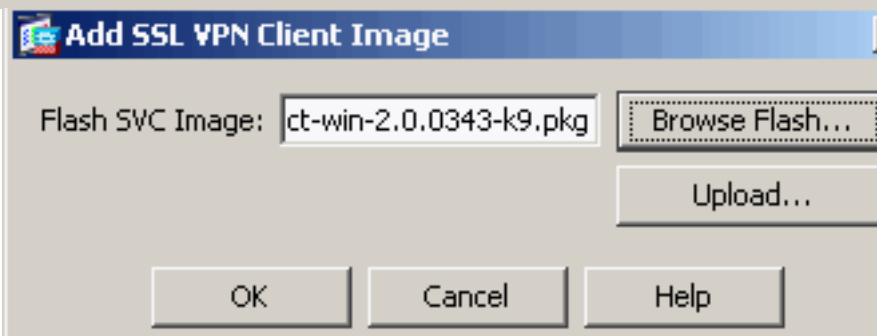
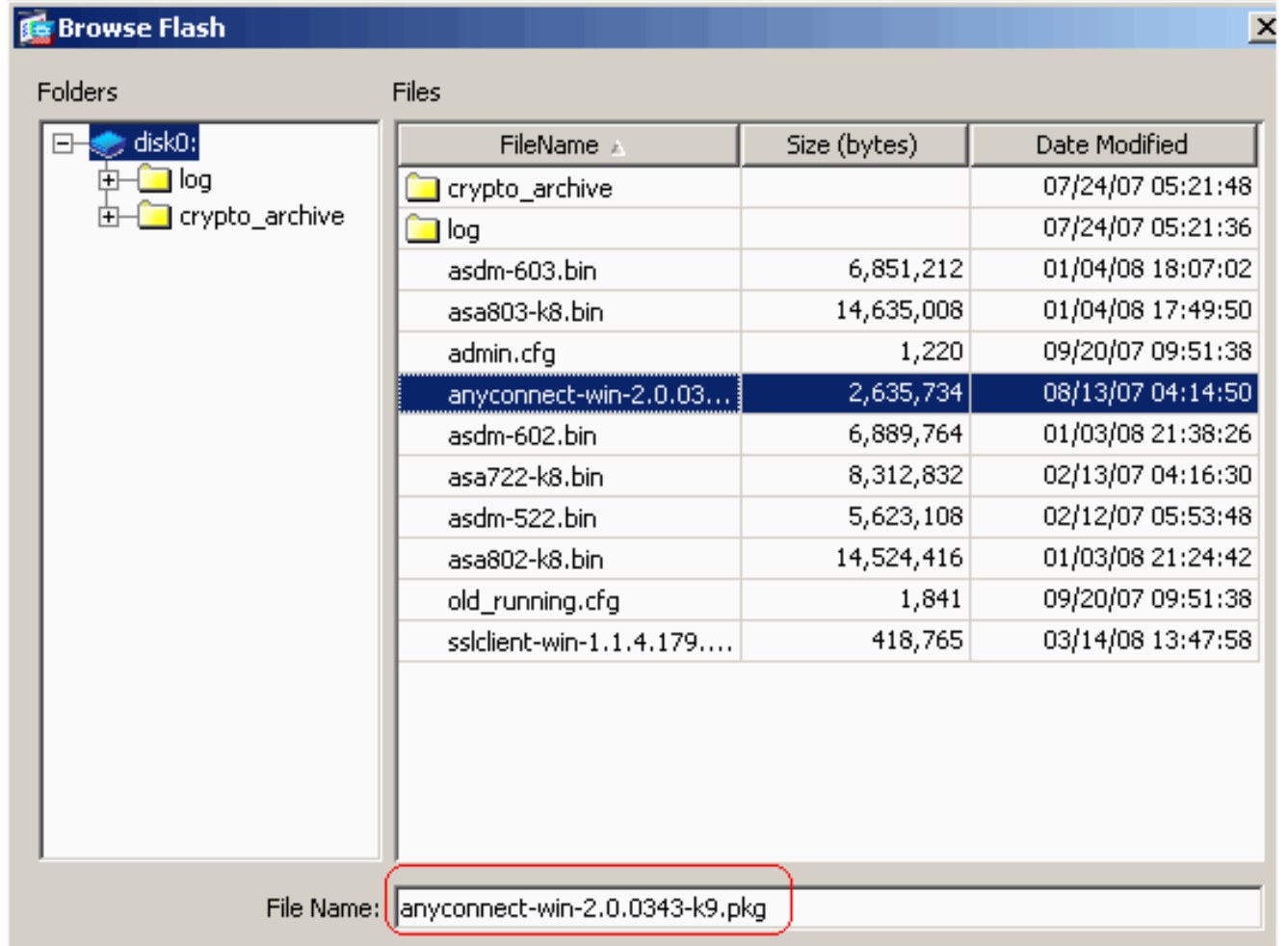
Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the

Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Access Port:  DTLS Port:

Click here to [Assign Certificate to Interface](#).

Haga clic en Apply (Aplicar). Elija **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings > Add** para agregar la imagen de Cisco AnyConnect VPN client de la memoria flash de ASA como se muestra.



Click OK.  
(Agregar).

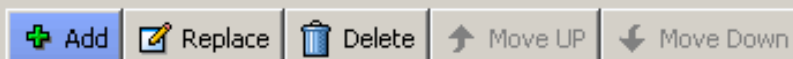
Haga clic en Add

**Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings**

Identify SSL VPN Client (SVC) related files.

#### SSL VPN Client Images

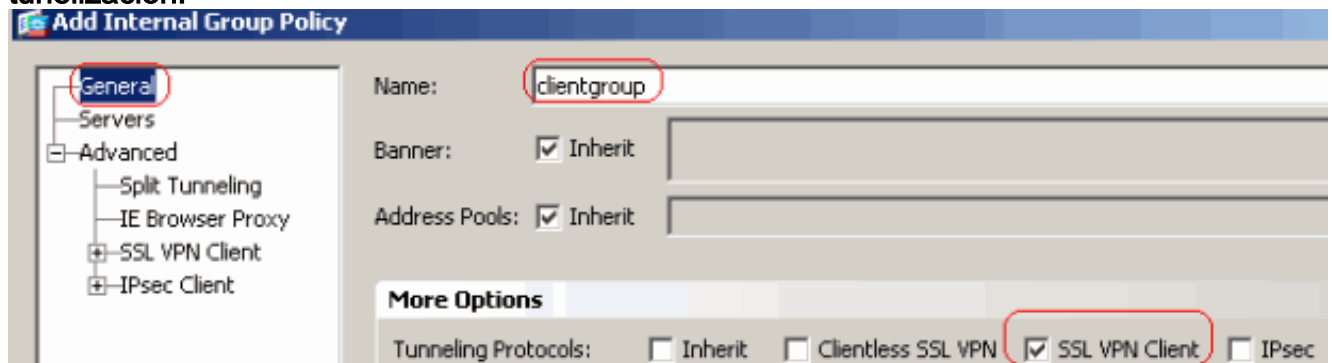
Minimize connection setup time by moving the image used by the most commonly encountered operation system to t



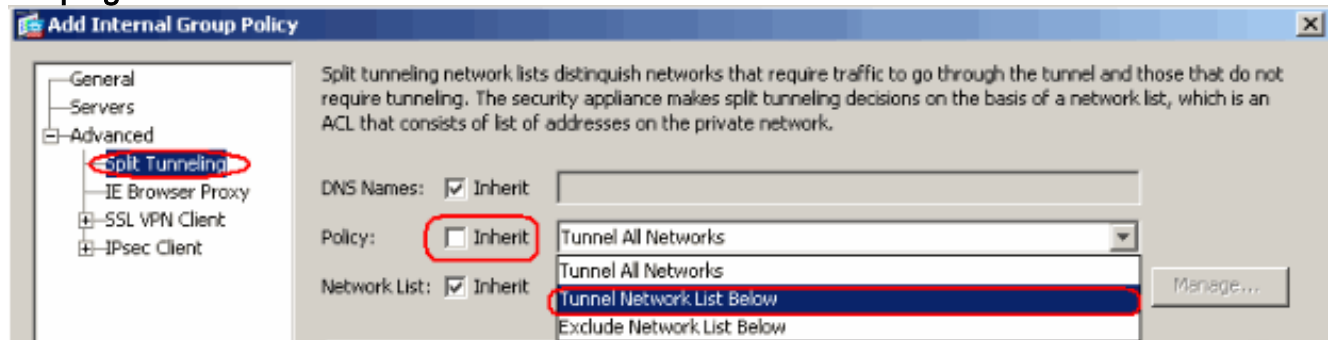
disk0:/anyconnect-win-2.0.0343-k9.pkg

### Configuración CLI Equivalente:

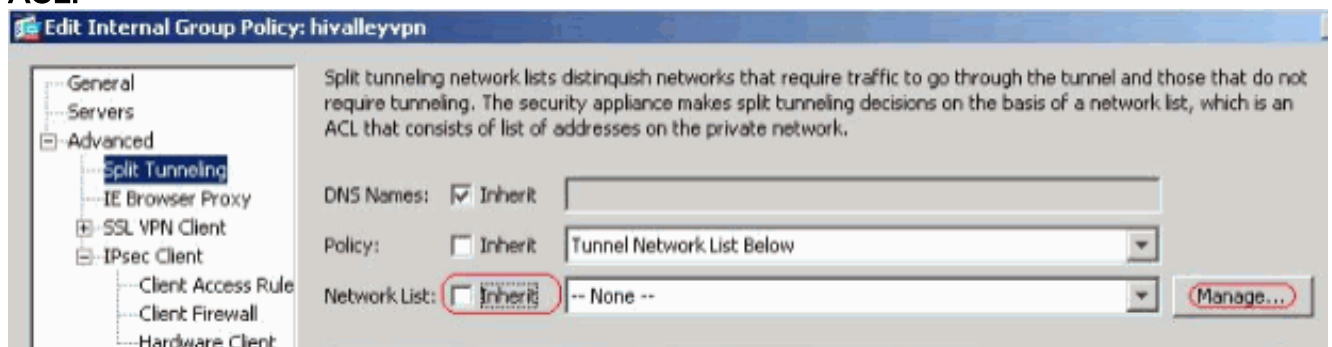
4. Configure la Política de Grupo. Elija **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** para crear una política de grupo interna clientgroup. Debajo de la ficha General, seleccione la casilla de selección SSL VPN Client para habilitar el WebVPN como protocolo de tunelización.



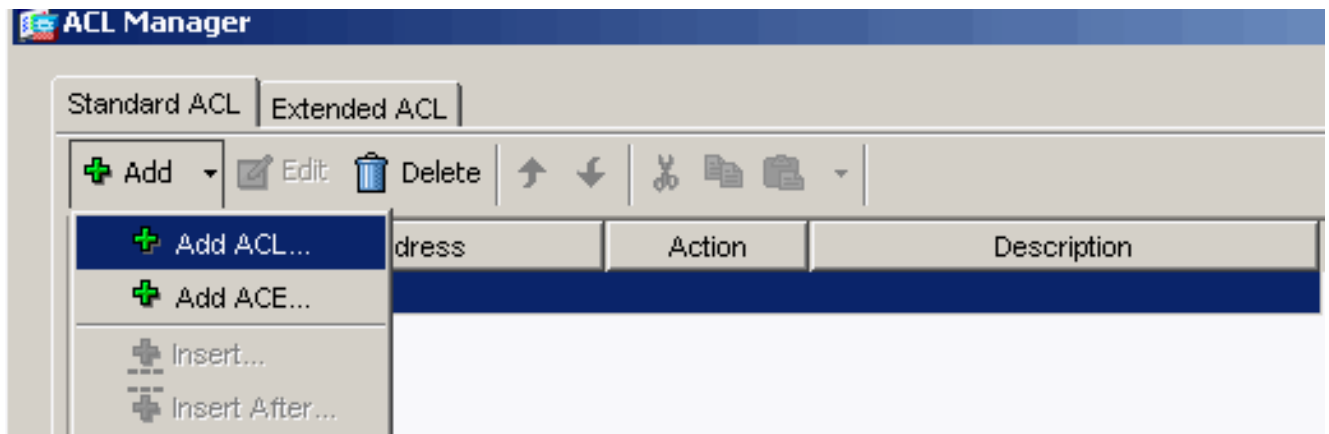
- En la pestaña **Advanced > Split Tunneling**, desmarque la casilla de selección **Inherit** para la Política de Túnel Dividido y elija la **Lista de Red de Túnel** de la lista desplegable.



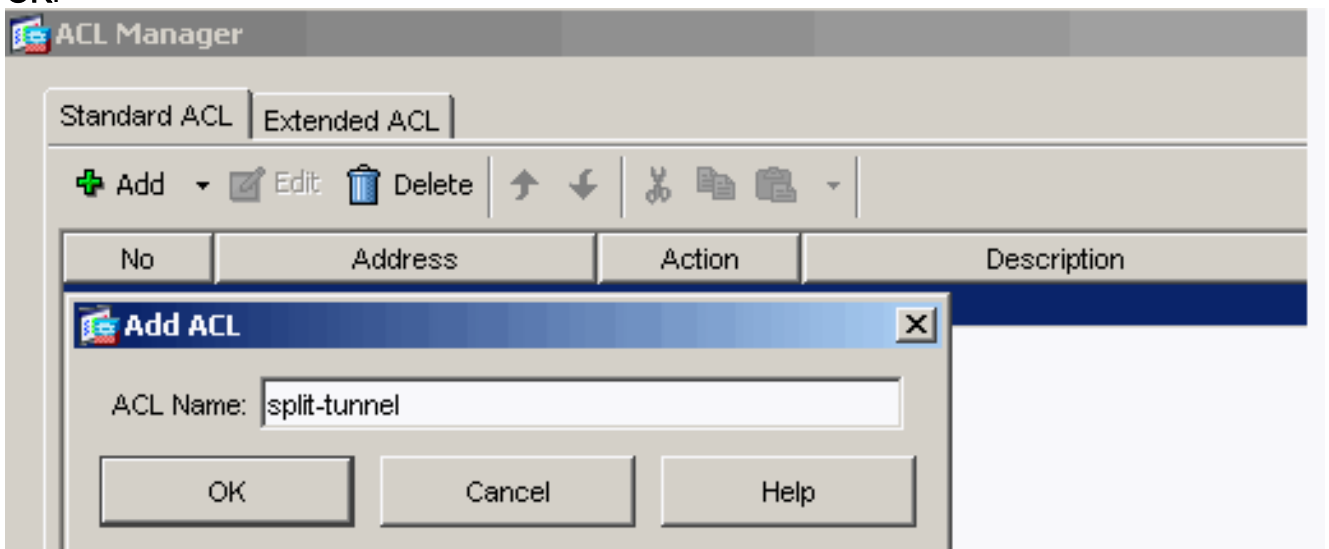
- Desmarque la casilla de selección **Inherit** para la **Lista de Red de Túnel Dividido** y haga clic en **Manage** para iniciar el **Administrador de ACL**.



- Dentro del **Administrador de ACL**, elija **Add > Add ACL...** para crear una nueva lista de acceso.

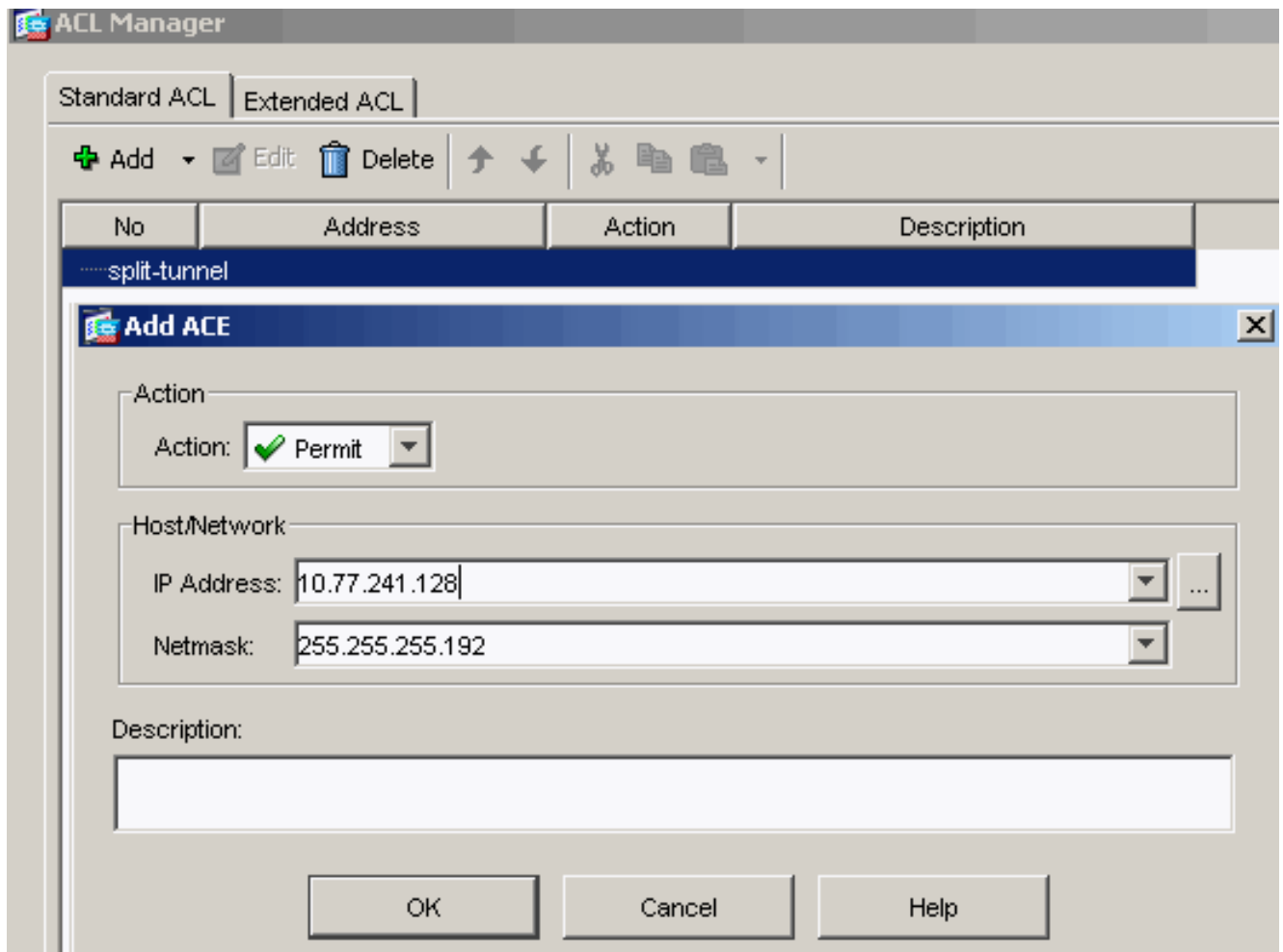


Asigne un nombre al ACL y haga clic en OK.

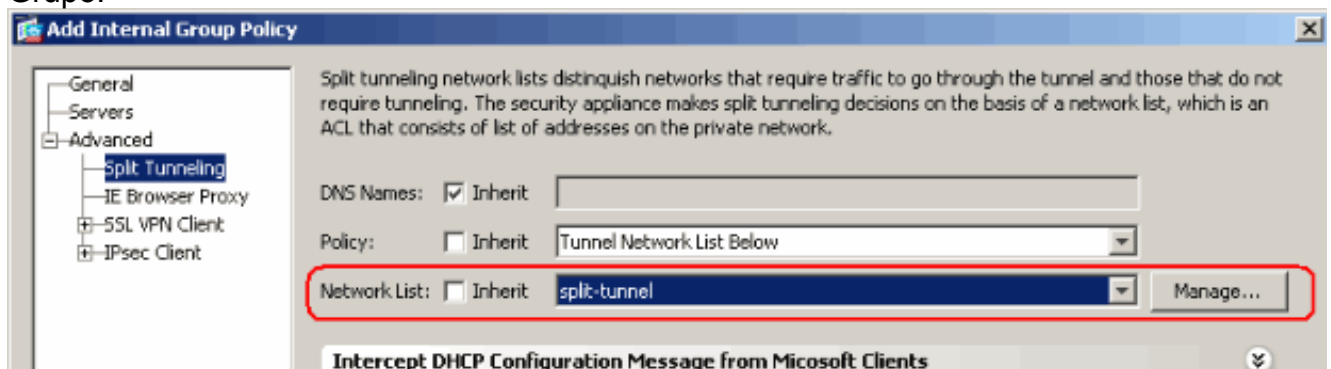


Una vez asignado el nombre ACL, elija **Add > Add ACE** para agregar una **Entrada de Control de Acceso (ACE)**. Defina el ACE que corresponde al LAN detrás del ASA. En este caso, la red es 10.77.241.128/26 y seleccione **Permit** como la **Acción**. Haga clic en OK para salir del Administrador de ACL.

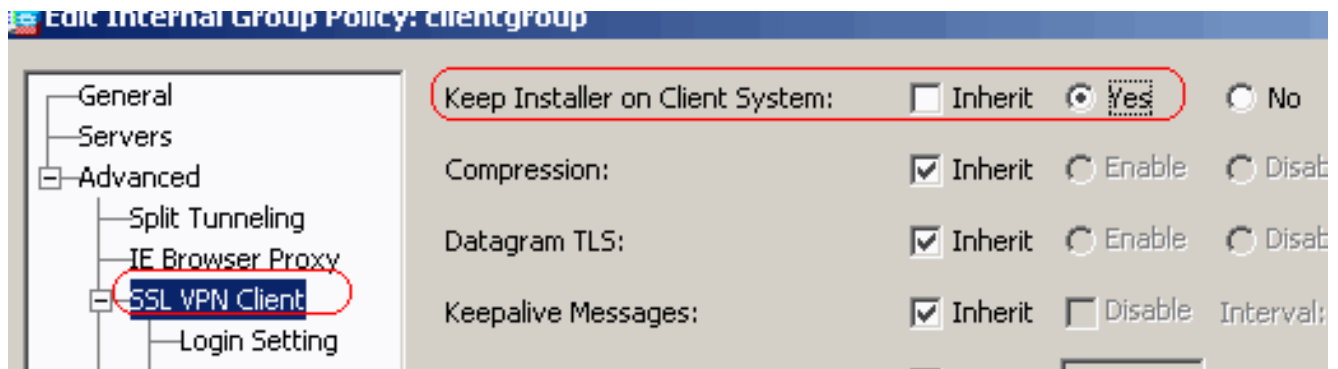




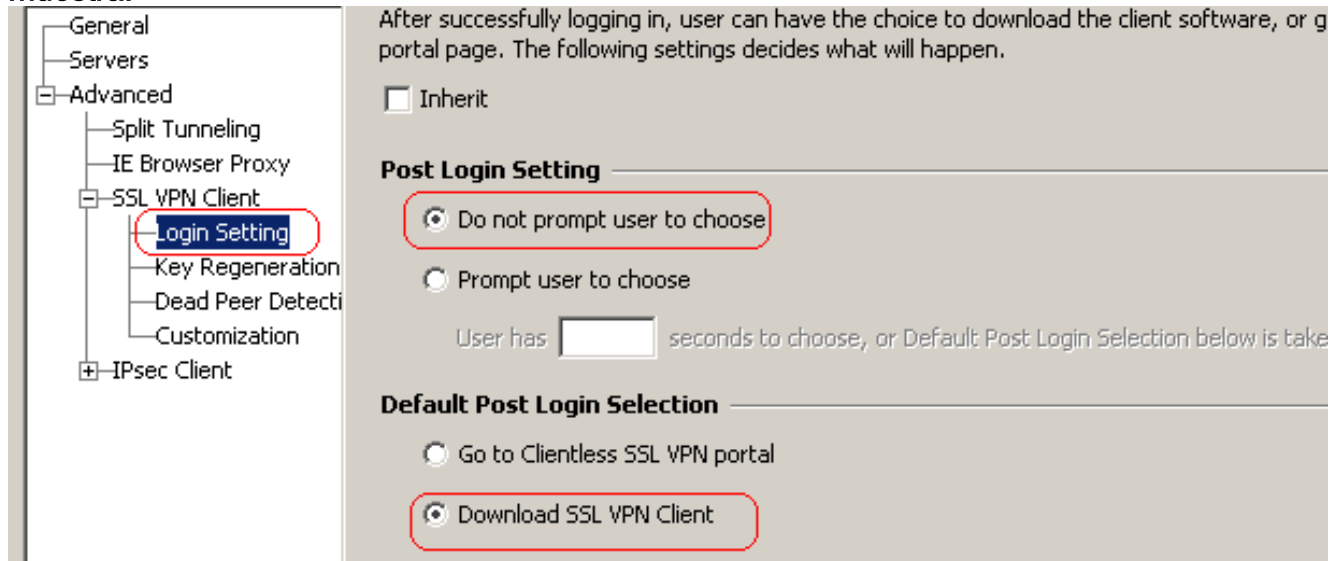
Asegúrese de que el ACL que acaba de crear esté seleccionado para la Lista de Red del túnel dividido. Haga clic en OK para volver a la configuración de la Política de Grupo.



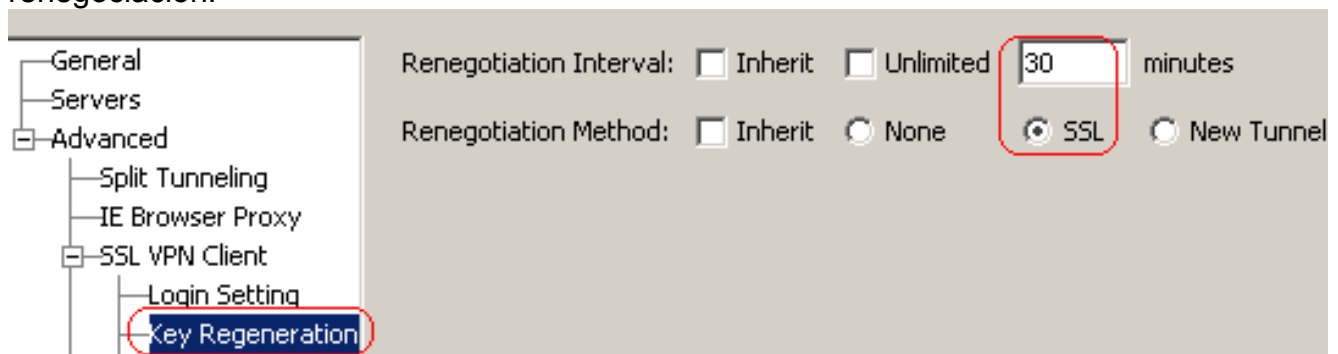
En la página principal, haga clic en **Apply** y luego en **Send** (de ser necesario) para enviar los comandos al ASA. Establezca las configuraciones SSL VPN debajo del módulo política de Grupo. Para la opción Keep Installer on Client System, desmarque la casilla de selección **Inherit**, y haga clic en el botón de opción **Yes**. Esta acción permite que el software SVC permanezca en la máquina del cliente. Por lo tanto, no es necesario que el ASA descargue el software SVC al cliente cada vez que se hace una conexión. Esta opción es una buena opción para los usuarios remotos que suelen acceder a la red corporativa.



Haga clic en **Login Setting** para establecer la Configuración Posterior a Login y Selección Predeterminada Posterior al Login como se muestra.






Para la opción Intervalo de Renegociación, desmarque la casilla **Inherit**, **desmarque la casilla de selección Unlimited**, e ingrese el número de minutos hasta la generación de la nueva clave. La seguridad se ve aumentada al establecer los límites durante el tiempo que una clave es válida. Para la opción Método de Renegociación, desmarque la casilla de selección **Inherit**, y haga clic el botón de opción **SSL**. La renegociación puede utilizar el túnel SSL actual o un túnel nuevo creado expresamente para la renegociación.



Haga clic en **OK** y en **Apply**.

**Configuration > Remote Access VPN > Network (Client) Access > Group Policies**

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

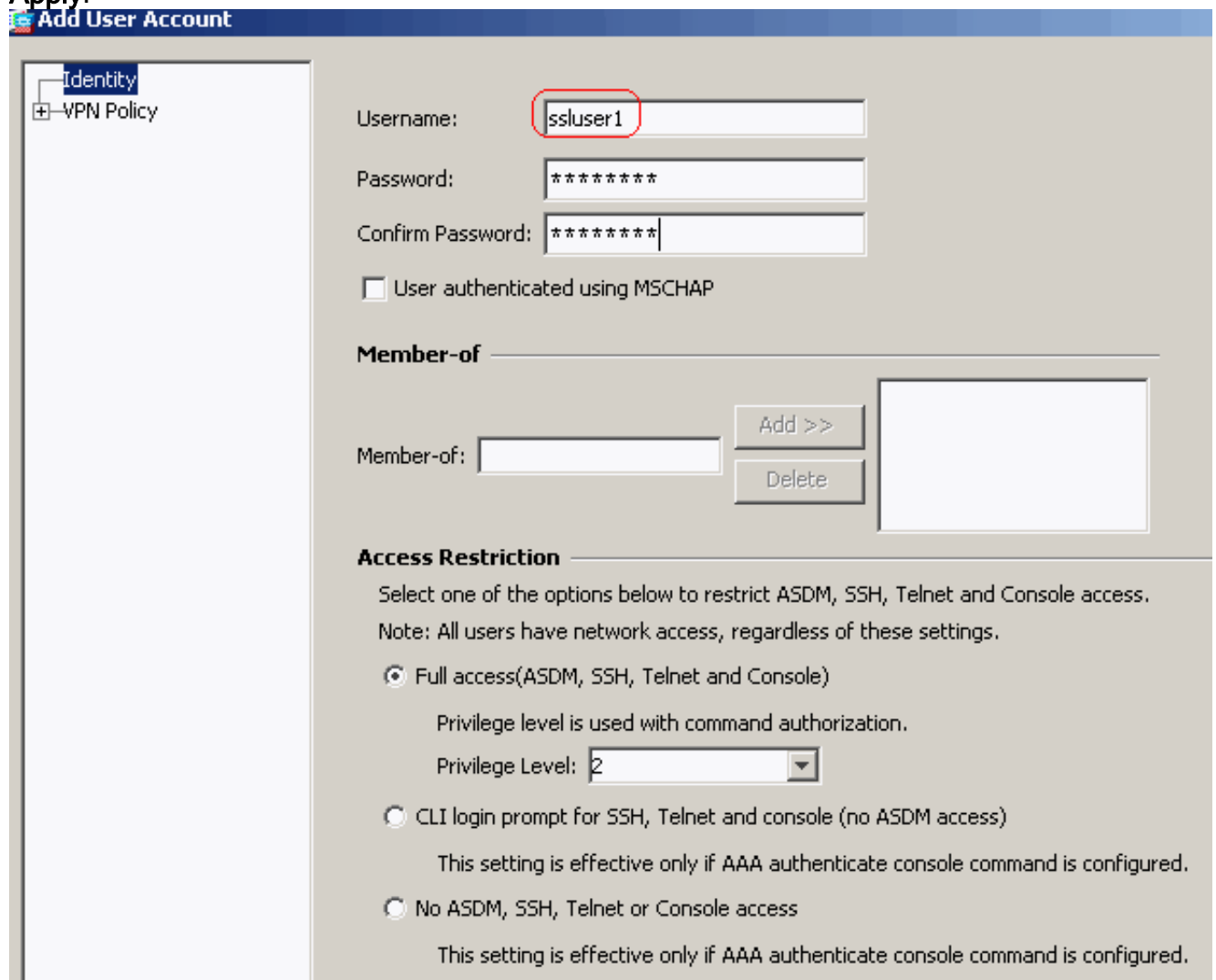
 Add  Edit  Delete

Name	Type	Tunneling Protocol	
clientgroup	Internal	svc	-- N/A -
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec,IPSec,webvpn	-- N/A -

**Configuración CLI Equivalente:**

5. Elija **Configuration > Remote Access VPN > AAA Setup > Local Users > Add** para crear una cuenta de usuario nuevo **ssluser1**. Haga clic en **OK** y en

**Apply.**



**Add User Account**

**Identity**

- VPN Policy

Username:

Password:

Confirm Password:

User authenticated using MSCHAP

**Member-of**

Member-of:

**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:

CLI login prompt for SSH, Telnet and console (no ASDM access)  
This setting is effective only if AAA authenticate console command is configured.

No ASDM, SSH, Telnet or Console access  
This setting is effective only if AAA authenticate console command is configured.

**Configuración CLI Equivalente:**

6. Elija **Configuration > Remote Access VPN > AAA Setup > AAA Servers Groups > Edit** para modificar el grupo de servidor predeterminado **LOCAL** al marcar la casilla de selección **Enable Local User Lockout** con un valor de intentos máximos de **16**.

Configuration > Remote Access VPN > AAA Setup > AAA Server Groups

### AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		

#### Edit LOCAL Server Group

This feature allows you to specify the maximum number of failed attempts to allow before locking out and denying access to the user. This limit is applicable only when the local database is used for authentication.

Enable Local User Lockout

Maximum Attempts:

OK

Cancel

Help

7. Haga clic en OK y en **Apply**. Configuración CLI Equivalente:

8. Configure el Grupo de Túnel. Elija **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles Connection Profiles > Add** para crear un grupo de túnel **sslgroup**. En la pestaña **Basic**, puede confeccionar la lista de configuraciones como se muestra: Asigne el grupo de Túnel como **sslgroup**. Debajo de la Asignación de Dirección de Cliente, elija el conjunto de direcciones **vpnpool** de la lista desplegable. Debajo de Política de Grupo Predeterminado, elija la política de grupo **clientgroup** de la lista desplegable.

#### Add SSL VPN Connection Profile

Basic  
Advanced

Name:

Aliases:

#### Authentication

Method:  AAA  Certificate  Both

AAA Server Group:

Use LOCAL if Server Group fails

#### Client Address Assignment

DHCP Servers:

Client Address Pools:

#### Default Group Policy

Group Policy:

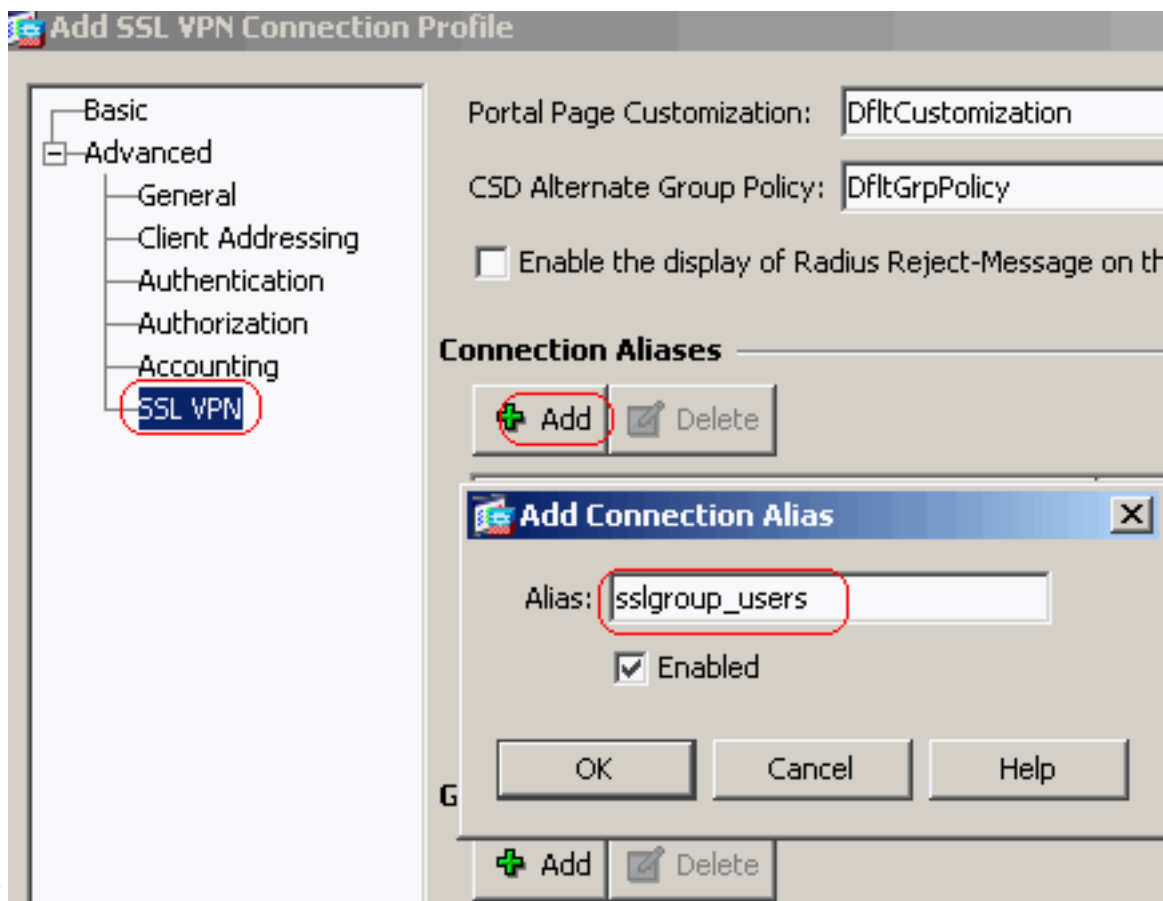
SSL VPN Client Protocol:  Enabled

OK

Cancel

Help

Debajo de la pestaña **SSL VPN > Connection Aliases**, especifique el alias del grupo **sslgroup\_users** y haga clic en

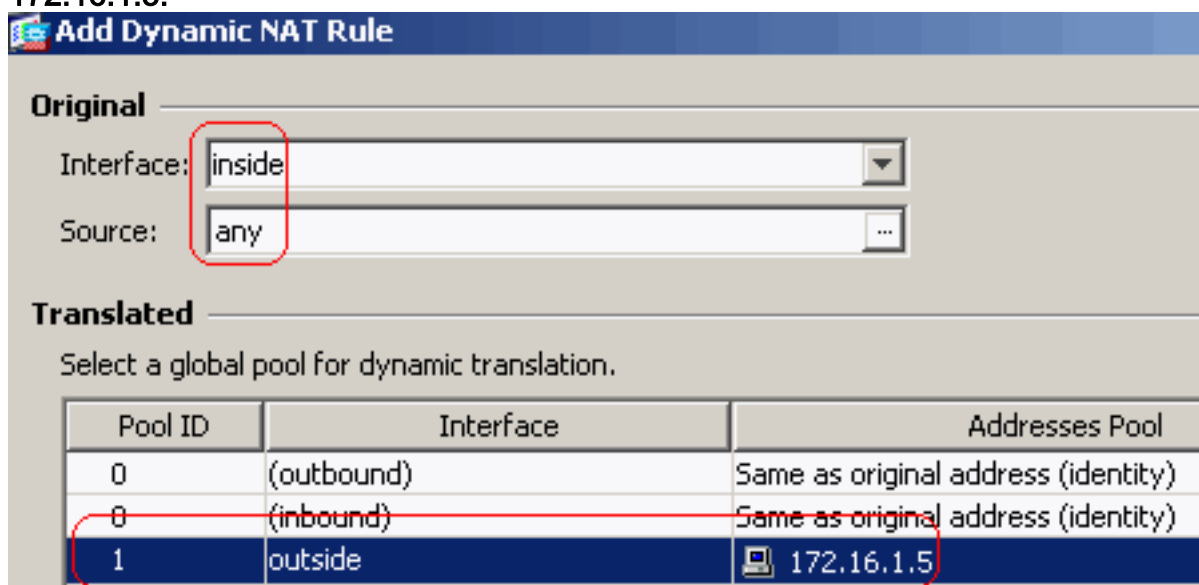


OK.

Haga

clic en OK y en Apply. Configuración CLI Equivalente:

- Configure el NAT. Elija Configuration > Firewall > NAT Rules > Add Dynamic NAT Rule de manera que el tráfico que proviene de la red interna puede traducirse con la dirección IP externa 172.16.1.5.



Click

OK. Click

OK.

Configuration > Firewall > NAT Rules						
#	Type	Original			Interface	
		Source	Destination	Service		
[-] inside (1 Dynamic rules)						
1	Dynamic	any			outside	

Haga clic en Apply (Aplicar). Configuración CLI Equivalente:

10. Configure la exención nat para el tráfico de retorno desde la red interna al cliente VPN.

```
ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0
ciscoasa(config)#nat (inside) 0 access-list nonat
```

## Configuración CLI ASA

### Cisco ASA 8.0(2)

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
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
access-list split-tunnel standard permit 10.77.241.128
255.255.255.192
!--- ACL for Split Tunnel network list for encryption.
access-list nonat permit ip 10.77.241.0 192.168.10.0
access-list nonat permit ip 192.168.10.0 10.77.241.0 !---
- ACL to define the traffic to be exempted from NAT.
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 global (outside) 1 172.16.1.5

!--- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP. nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 0.0.0.0 0.0.0.0

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 svc image
disk0:/anyconnect-win-2.0.0343-k9.pkg 1

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

  !--- Specify SSL as a permitted VPN tunneling protocol
split-tunnel-policy tunnelspecified
  split-tunnel-network-list value split-tunnel

  !--- Encrypt the traffic specified in the split tunnel
ACL only webvpn
  svc keep-installer installed

  !--- When the security appliance and the SVC perform a
rekey, they renegotiate !--- the crypto keys and
initialization vectors, increasing the security of the
connection. svc rekey time 30

  !--- Command that specifies the number of minutes from
the start of the !--- session until the rekey takes
place, from 1 to 10080 (1 week). svc rekey method ssl

  !--- Command that specifies that SSL renegotiation takes
place during SVC rekey. svc ask none default svc

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)#
```

## Establezca la Conexión VPN SSL con el SVC

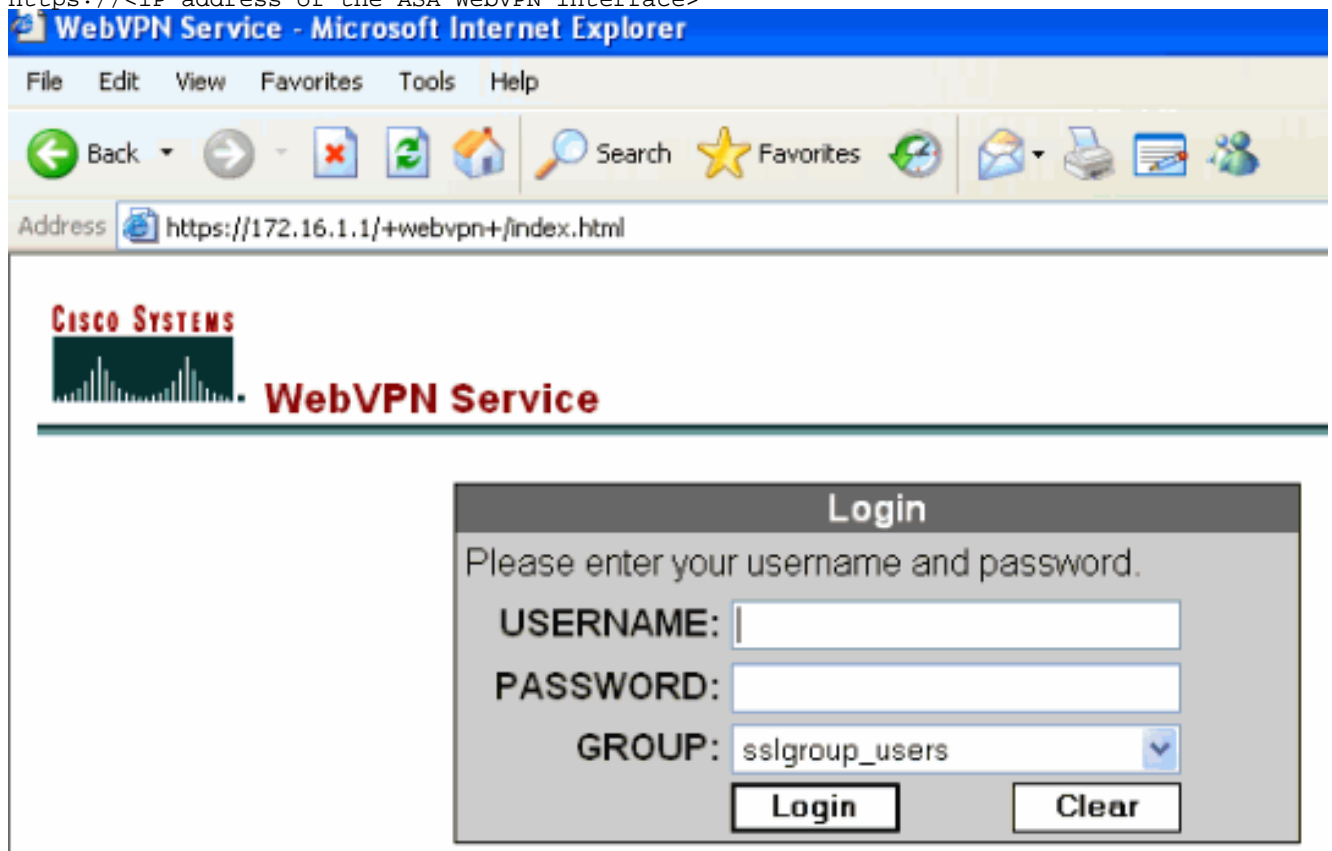
Siga estos pasos para establecer una conexión VPN SSL con el ASA:

1. Ingrese el URL o la dirección IP de la interfaz de WebVPN ASA en su navegador web en el formato como se muestra.

https://url

O

https://<IP address of the ASA WebVPN interface>



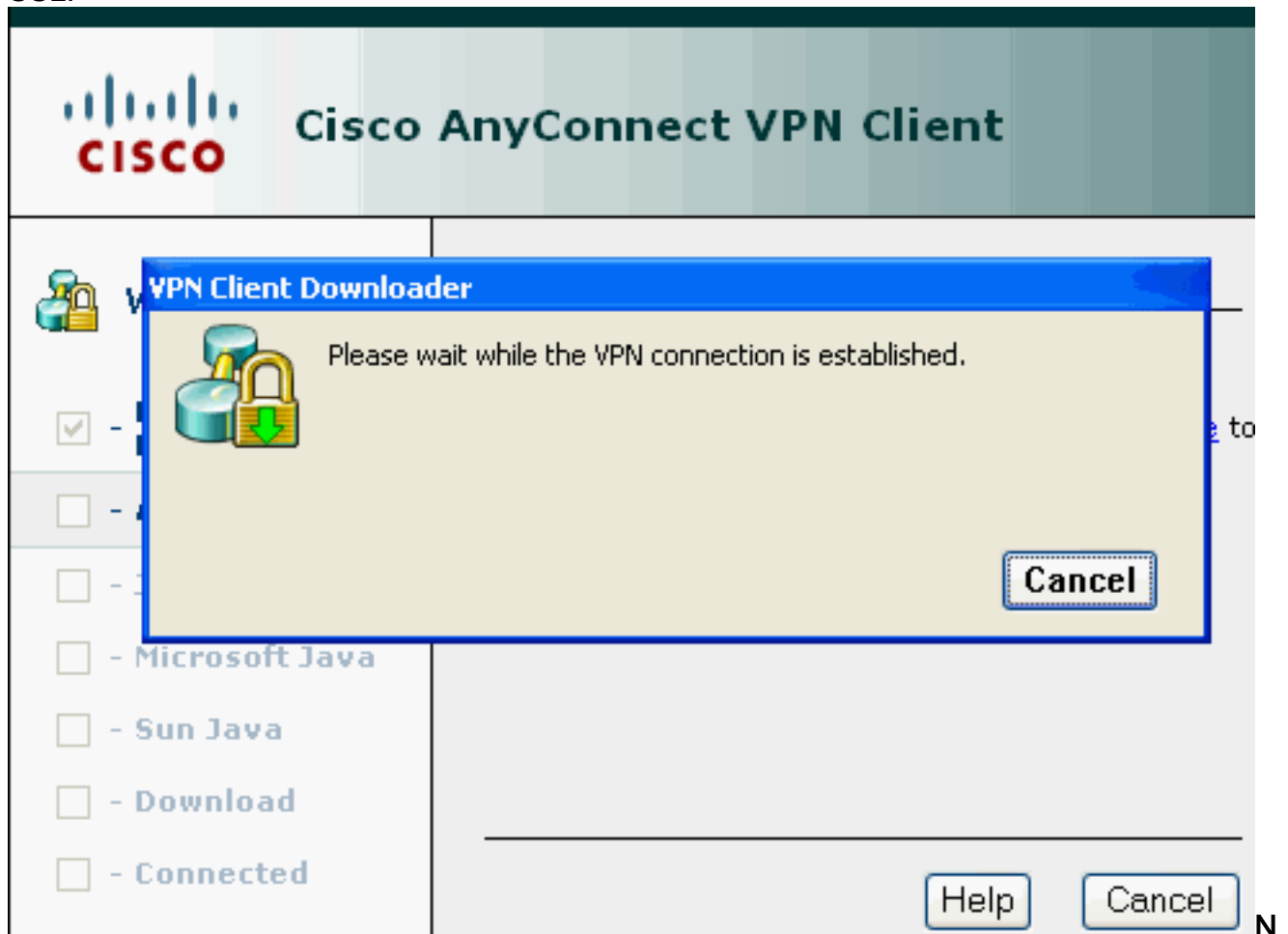
2. Ingrese su nombre de usuario y contraseña. También, elija a su grupo correspondiente de la lista desplegable como se

muestra.

aparece antes de que se establezca la conexión VPN

Esta ventana

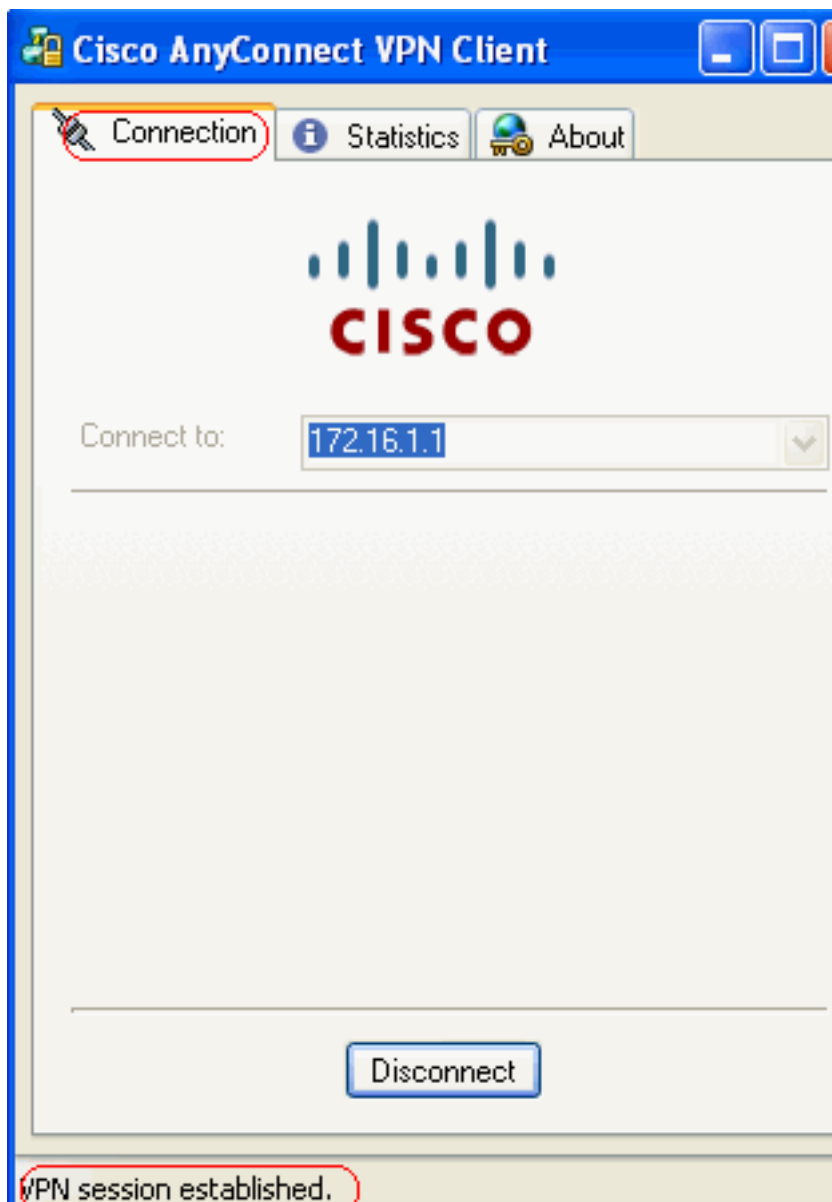
SSL.



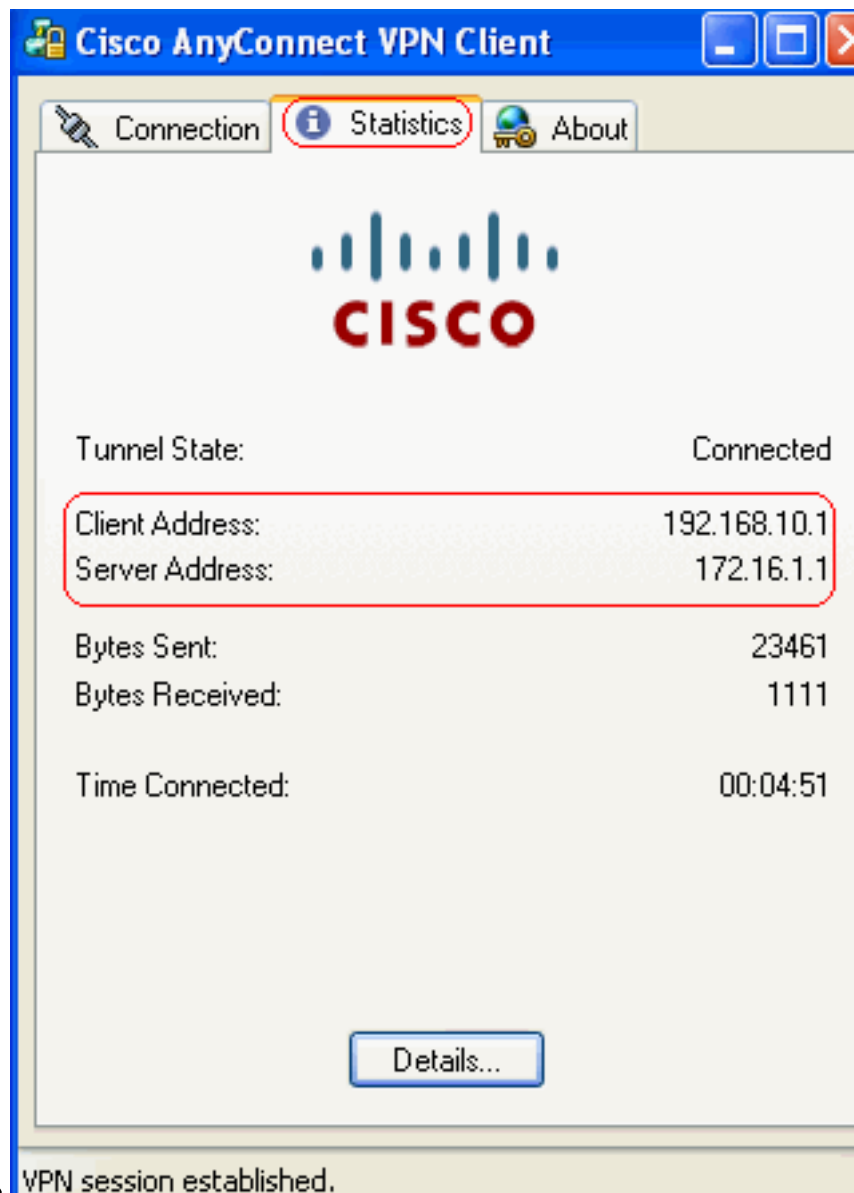
**Nota:** El software ActiveX debe estar instalado en el equipo antes de descargar el SVC. Recibe esta ventana una vez que se establece la conexión.



3. Haga clic en el bloqueo que aparece en la barra de tareas de su



equipo. **VPN session established.** Esta ventana aparece y proporciona información sobre la conexión SSL. Por ejemplo, **192.168.10.1** es la IP asignada



por el ASA, etc.

VPN session established.

Esta ventana

muestra la información de la Versión de Cisco AnyConnect VPN



Client: VPN session established

## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

- **show webvpn svc:** muestra las imágenes SVC almacenadas en la memoria flash ASA.

```
ciscoasa#show webvpn svc
1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1
  CISCO STC win2k+
  2,0,0343
  Mon 04/23/2007 4:16:34.63

1 SSL VPN Client(s) installed
```

- **show vpn-sessiondb svc:** muestra la información acerca de las conexiones SSL actuales.

```
ciscoasa#show vpn-sessiondb svc

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 WebVPN actuales en ASA.

Remote Access	Site-to-Site	SSL VPN			E-mail Proxy	VPN Load Balancing
		Clientless	With Client	Total		
0	0	0	0	0	0	

Filter By: **SSL VPN Client** -- All Sessions -- Filter

Username IP Address	Group Policy Connection	Protocol Encryption	Login Time Duration	Byt Byt
ssluser1 192.168.10.1	clientgroup sslgroup	Clientless SSL-Tunnel DT... RC4 AES128	17:12:23 IST Mon Mar 24 2008 0h:03m:31s	194118 192474

## Troubleshoot

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

1. **vpn-sessiondb logoff name <username>:** comando que se usa para finalizar la sesión SSL VPN para el nombre de usuario.

```

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 comando **vpn-sessiondb logoff svc** para finalizar las sesiones SVC.

2. **Nota:** Si la PC pasa al modo de espera o hibernación, la conexión SSL VPN puede terminar.

```

webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, e
tc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL

```

```
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xA000)
```

```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

### 3. debug webvpn svc <1-255>: proporciona los eventos webvpn en tiempo real para establecer la sesión.

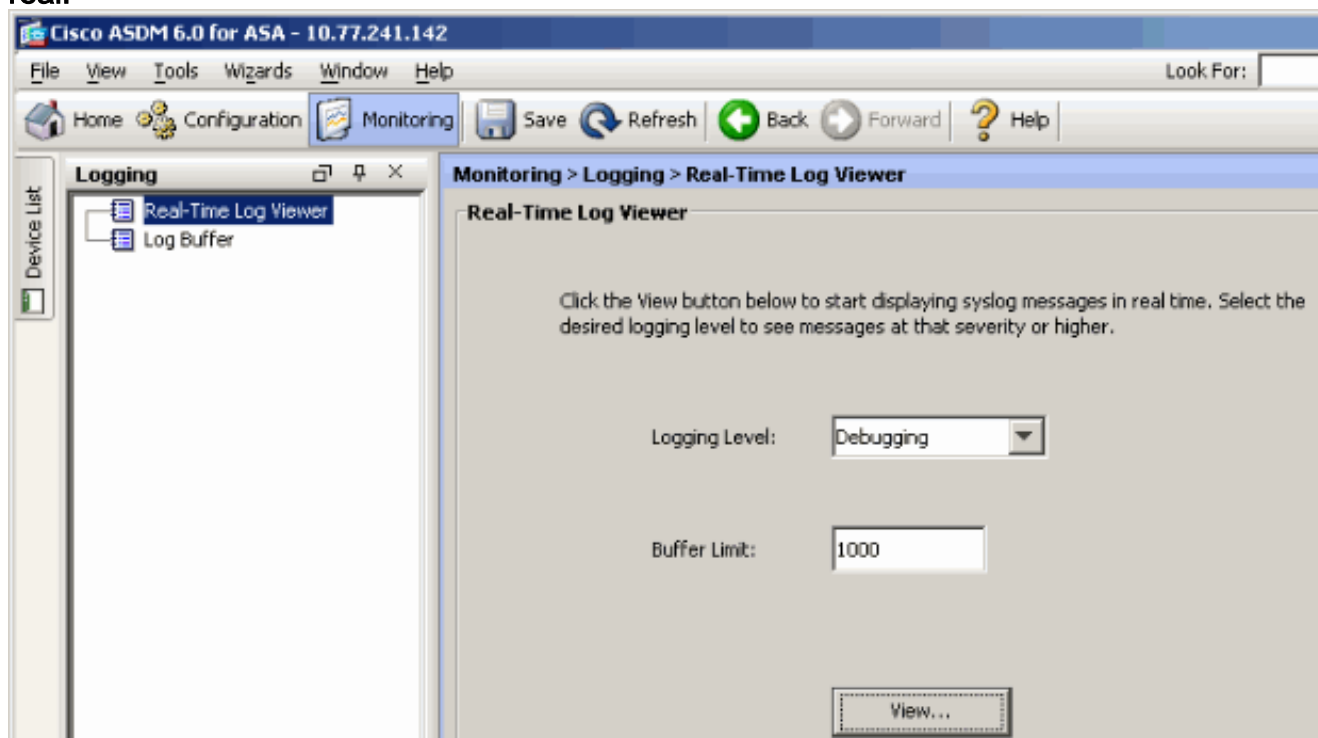
```
Ciscoasa#debug webvpn svc 7
```

```
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343'
'
Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
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: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693'
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693'
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'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
```



```
SVC: NP setup
np_svc_create_session(0x3000, 0xD41611E8, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
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
```

4. En ASDM, elija **Monitoring > Logging > Real-time Log Viewer > View** para ver los eventos en tiempo real.



Este ejemplo muestra que se ha establecido la sesión SSL con el dispositivo del centro distribuidor.

Real-Time Log Viewer - 10.77.241.142

File Tools Window Help

Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help

Filter By: Filter Show All Find:

Severity	Date	Time	Syslog ID	Source IP	Destination IP	
6	Mar 21 2008	20:03:36	725007	10.77.233.74		SSL session with client inside:10.77.233.74/1026 terminated.
6	Mar 21 2008	20:03:35	106015	10.77.233.74	10.77.241.142	Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44:
6	Mar 21 2008	20:03:35	302014	10.77.233.74	10.77.241.142	Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Identit
6	Mar 21 2008	20:03:35	605005	0.0.0.0	0.0.0.0	Login permitted from 0.0.0.0/1026 to inside:0.0.0.0/https for user "enabl
6	Mar 21 2008	20:03:35	725002	10.77.233.74		Device completed SSL handshake with client inside:10.77.233.74/1026
6	Mar 21 2008	20:03:35	725003	10.77.233.74		SSL client inside:10.77.233.74/1026 request to resume previous session.
6	Mar 21 2008	20:03:35	725001	10.77.233.74		Starting SSL handshake with client inside:10.77.233.74/1026 for TL5v1 se
6	Mar 21 2008	20:03:35	302013	10.77.233.74	10.77.241.142	Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.23

%ASA-6-725002: Device completed SSL handshake with remote\_device\_interface\_name:IP\_address/port

The SSL handshake has completed successfully with the remote device.

## Información Relacionada

- [Página de Soporte de Cisco 5500 Series Adaptive Security Appliance](#)
- [Notas de Versión para AnyConnect VPN Client, Release 2.0](#)
- [ASA/PIX: Ejemplo de Configuración Cómo habilitar la Tunelización Dividida para los Clientes VPN en ASA](#)
- [Ejemplo de Configuración Router Permite que los Clientes VPN se Conecten a IPsec e Internet con Tunelización Dividida](#)
- [Ejemplo de Configuración de PIX/ASA 7.x y VPN Client para Public Internet VPN en un Solo Sentido](#)
- [Ejemplo de Configuración de SSL VPN Client \(SVC\) en ASA con ASDM](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)