

# ASA 7.1/7.2: Permita el Túnel dividido para SVC en el ejemplo de configuración ASA

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones ASA usando el ASDM 5.2\(2\)](#)

[Configuración ASA 7.2\(2\) usando el CLI](#)

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

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

## Introducción

Este documento proporciona las instrucciones graduales en cómo no prohibir a los clientes VPN del Secure Socket Layer (SSL) el acceso del (SVC) al Internet mientras que son tunneled en un dispositivo de seguridad adaptante de Cisco (ASA). Esta configuración permite el acceso seguro de SVC a los recursos corporativos con el SSL y da el acceso sin garantía a Internet con el uso del Túnel dividido.

La capacidad de transmitir tráfico seguro y no seguro en la misma interfaz se conoce como tunelización dividida. El Túnel dividido requiere que usted especifique exactamente que el tráfico se asegura y cuál es el destino de ese tráfico, de modo que solamente el tráfico especificado ingrese el túnel, mientras que el resto se transmite unencrypted a través de la red pública (Internet).

## prerrequisitos

### Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Privilegios administrativos locales en todas las estaciones de trabajo remotas
- Javas y controles ActiveX en la estación de trabajo remota

- El puerto 443(SSL) no se bloquea dondequiera a lo largo del trayecto de conexión

## Componentes Utilizados

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

- El dispositivo de seguridad adaptante de las Cisco 5500 Series (el ASA) ese funciona con la versión de software 7.2(2)
- Versión del Cliente Cisco SSL VPN para Windows 1.1.4.179**Nota:** Descargue el paquete del cliente VPN SSL (sslclient-win\*.package) de la [descarga de software de Cisco \(clientes registrados solamente\)](#). Copie SVC a memoria flash del ASA, que debe ser descargado a los ordenadores del usuario remoto para establecer la conexión VPN SSL con el ASA. Refiera a [instalar a la sección del software de SVC de la](#) guía de configuración ASA para más información.
- PC que funciona con el Windows 2000 SP4 profesional o Windows XP SP2
- Versión 5.2(2) del Cisco Adaptive Security Device Manager (ASDM)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

## Antecedentes

El (SVC) del cliente VPN SSL es una tecnología de tunelización VPN que da a usuarios remotos las ventajas de un cliente del IPsec VPN sin la necesidad de los administradores de la red de instalar y de configurar a los clientes del IPsec VPN en las computadoras remotas. SVC utiliza la encriptación de SSL que está ya presente en la computadora remota así como el login del WebVPN y la autenticación del dispositivo de seguridad.

Para establecer una sesión SVC, el usuario remoto ingresa el IP Address de una interfaz del WebVPN del dispositivo de seguridad en el hojeador, y el hojeador conecta con esa interfaz y visualiza a la pantalla de inicio de sesión del WebVPN. Si usted satisface el login y la autenticación, y el dispositivo de seguridad le identifica como requerir SVC, el dispositivo de seguridad descarga SVC a la computadora remota. Si el dispositivo de seguridad le identifica con la opción para utilizar SVC, el dispositivo de seguridad descarga SVC a la computadora remota mientras que presenta un link en la ventana para saltar la instalación de SVC.

Después de que usted descarga, el SVC instale y se configure, y entonces los restos SVC u o se desinstale, que depende de la configuración, de la computadora remota cuando la conexión termina.

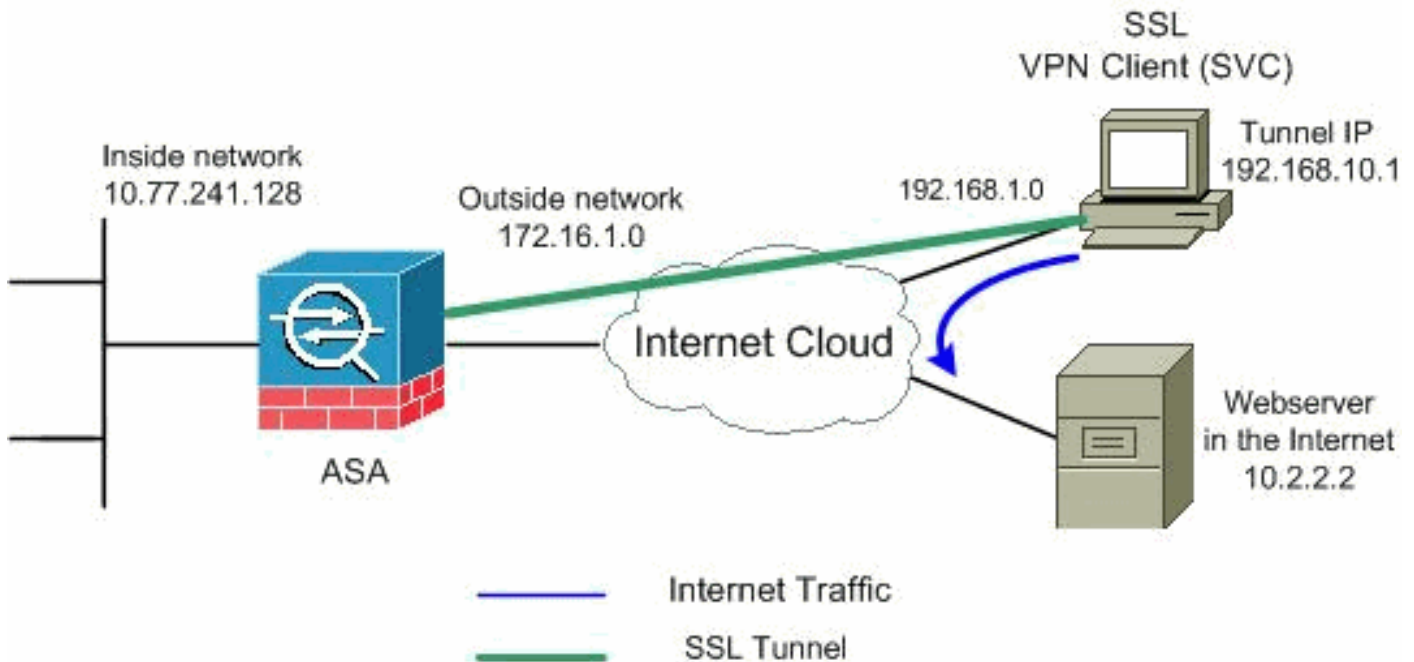
## Configurar

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

**Nota:** Use la [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos usados en esta sección.

## [Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



**Nota:** Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones [RFC1918](#) que se han utilizado en un entorno de laboratorio.

## [Configuraciones ASA usando el ASDM 5.2\(2\)](#)

Complete estos pasos para configurar el SSL VPN en el ASA con el Túnel dividido como se muestra:

1. El documento asume que la configuración básica tal como configuración de la interfaz y así sucesivamente está hecha y que trabaja ya correctamente. **Nota:** Consulte [Cómo Permitir el Acceso HTTPS para el ASDM](#) para que el ASA sea configurado por el ASDM. **Nota:** El WebVPN y el ASDM no se pueden habilitar en la misma interfaz ASA a menos que cambie los números del puerto. Consulte [ASDM y WebVPN Habilitados en la Misma Interfaz de ASA](#) para obtener más información.
2. Elija la configuración > el VPN > la administración de IP Address > a las agrupaciones IP para crear un pool de la dirección IP: `vpnpool` para los clientes

**Add IP Pool**

Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

VPN.

Haga clic en Apply (Aplicar).

3. **WebVPN del permiso** Elija la configuración > el VPN > el WebVPN > el acceso del WebVPN y resalte la interfaz exterior con el ratón y haga clic el permiso. Marque la lista desplegable del grupo de túnel del permiso en la casilla de verificación de la página de registro del WebVPN para habilitar el descenso abajo aparecen en la página de registro para los usuarios, elegir a sus grupos correspondientes.

Configuration > VPN > WebVPN > WebVPN Access

WebVPN Access

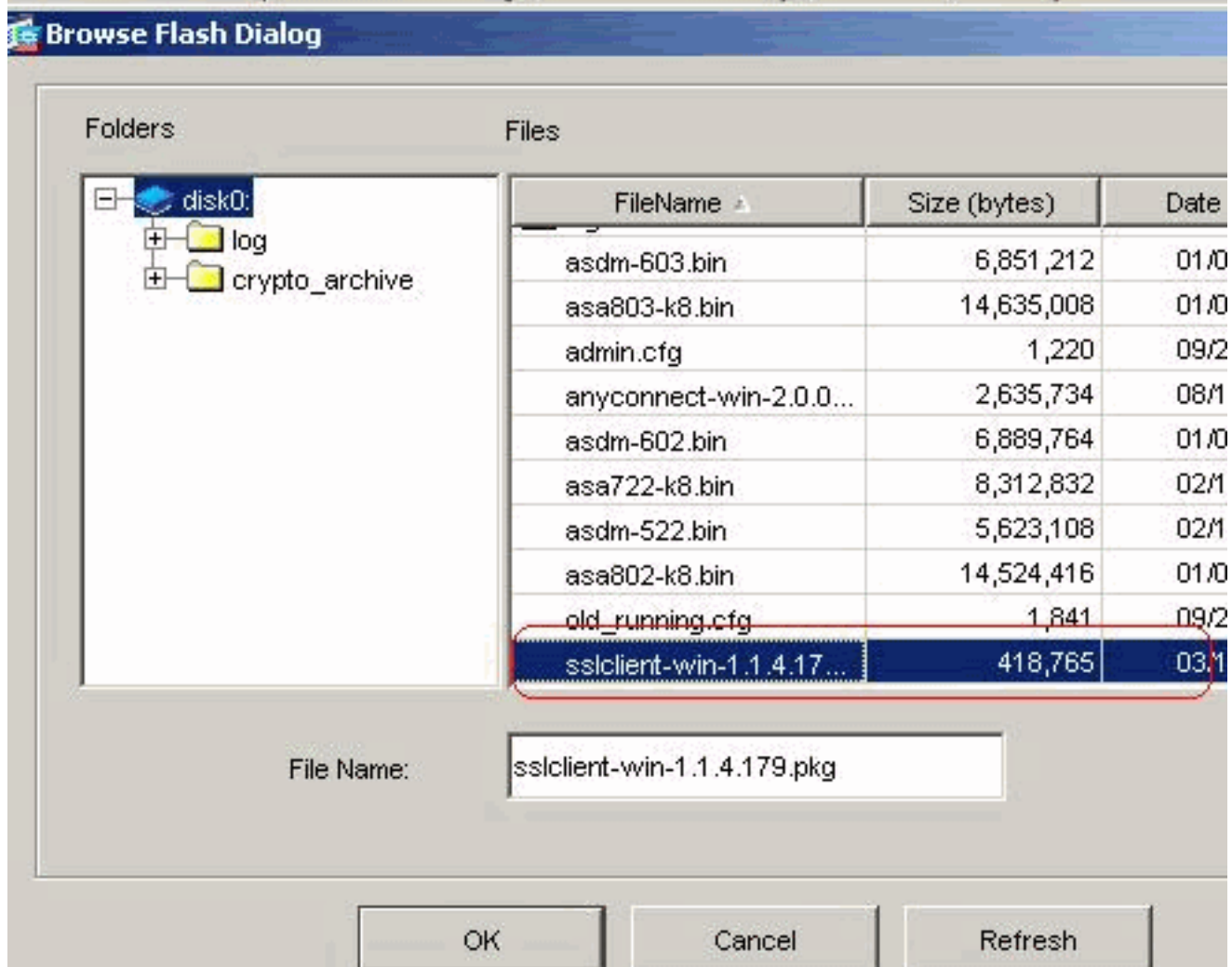
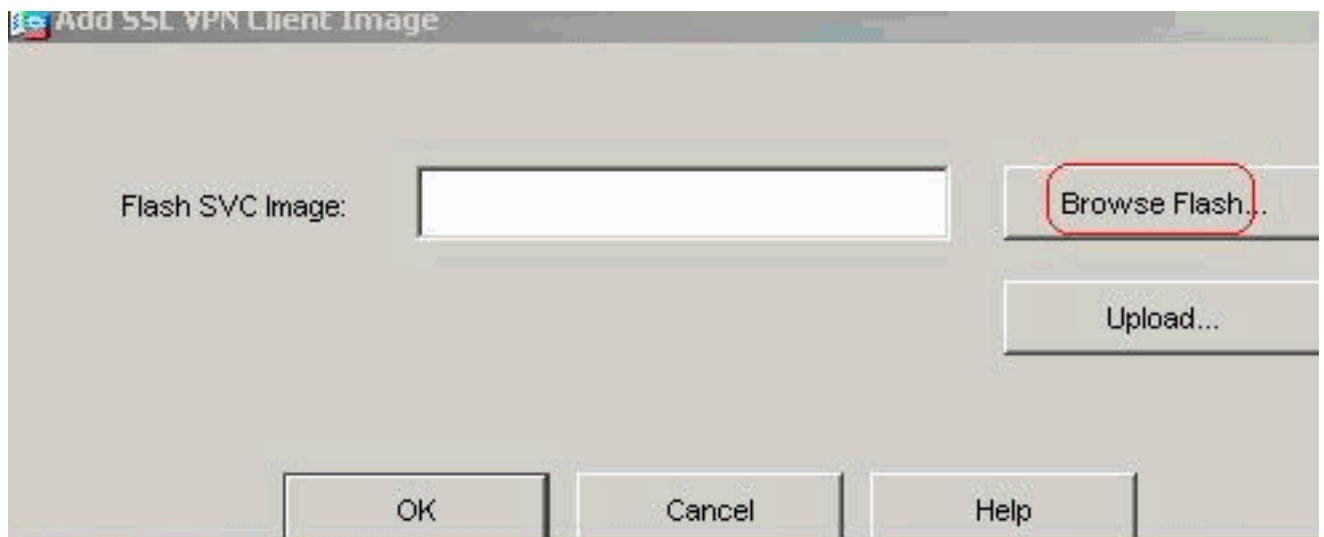
Configure access parameters for WebVPN.

Interface	WebVPN Enabled
inside	No
outside	Yes

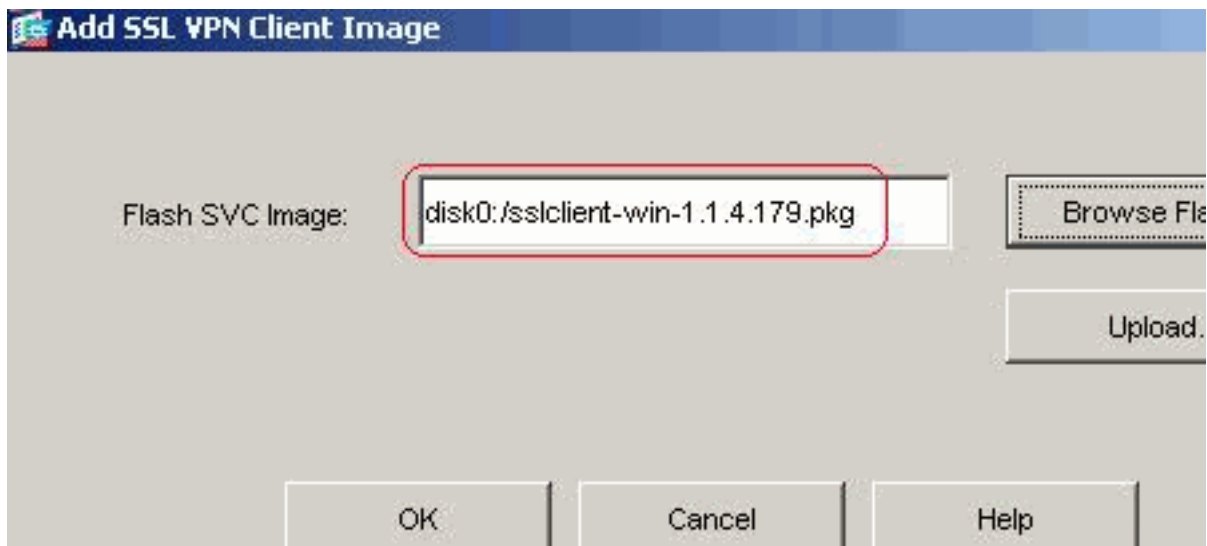
Port Number:   
 Default Idle Timeout:  seconds  
 Max. Sessions Limit:   
 WebVPN Memory Size:  % of total physical memory

Enable Tunnel Group Drop-down List on WebVPN Login Page

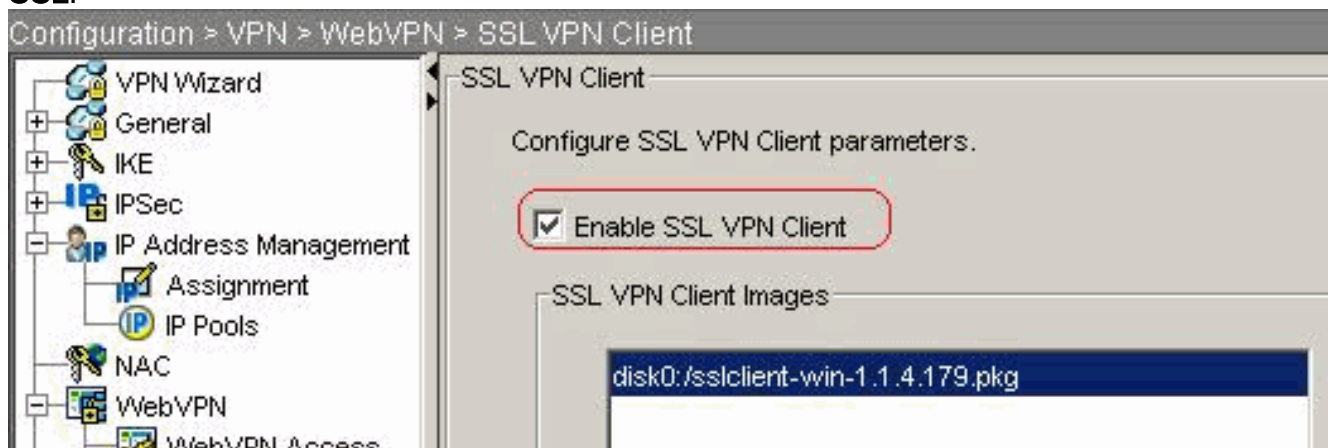
Haga clic en Apply (Aplicar). Elija la configuración > el VPN > el WebVPN > al cliente VPN SSL > Add para agregar la imagen del cliente VPN SSL de memoria flash del ASA como se muestra.



Haga clic en

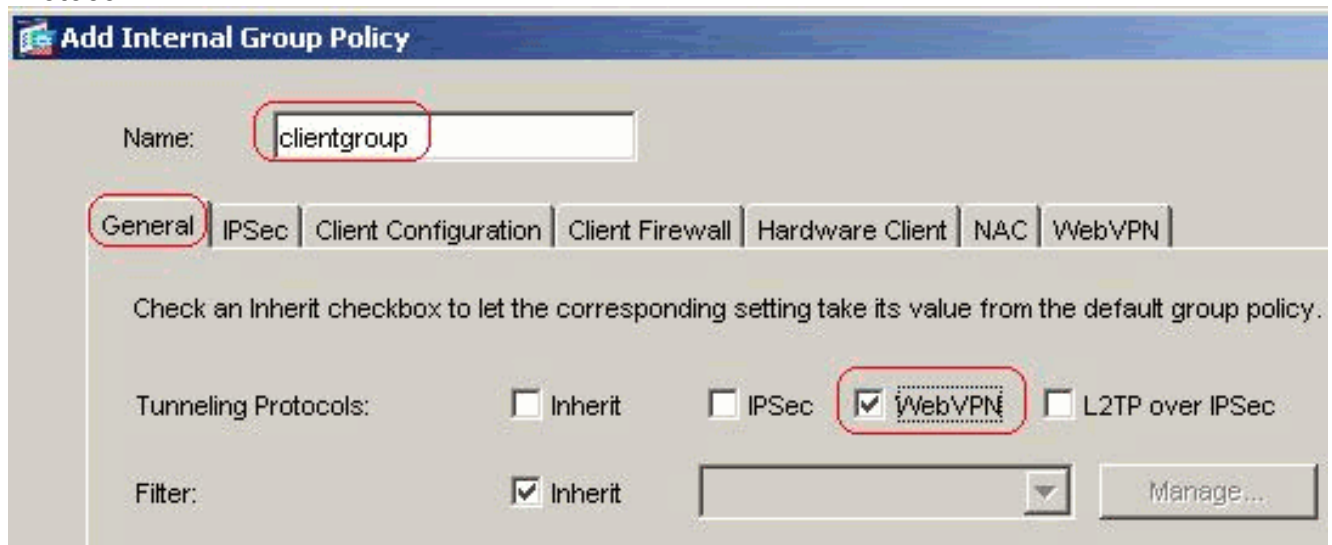


OK. Haga clic en OK. Casilla de verificación del **cliente VPN del teclado SSL**.



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

4. **Directiva del grupo de la configuración** Elija la configuración > el VPN > la directiva del general > del grupo > Add (Internal group policy (política grupal interna)) para crear un **clientgroup** interno de la directiva del grupo. Bajo el **general**, elija la casilla de verificación del **WebVPN** para habilitar el WebVPN como Tunneling Protocol.



En la lengüeta de la **configuración del cliente > de general Client Parameters**, desmarque el cuadro de la **herencia** para la directiva del túnel dividido y elija la **lista de la red de túneles abajo de la lista desplegable**. Desmarque el cuadro de la **herencia** para la lista de red del

túnel dividido y después haga clic **manejar** para iniciar el ACL Manager.

**Edit Internal Group Policy: clientgroup**

Name:

General | IPsec | **Client Configuration** | Client Firewall | Hardware Client | NAC | WebVPN

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

General Client Parameters | Cisco Client Parameters | Microsoft Client Parameters

Banner:  Inherit

Default Domain:  Inherit

Split Tunnel DNS Names (space delimited):  Inherit

Split Tunnel Policy:  Inherit

Split Tunnel Network List:  Inherit

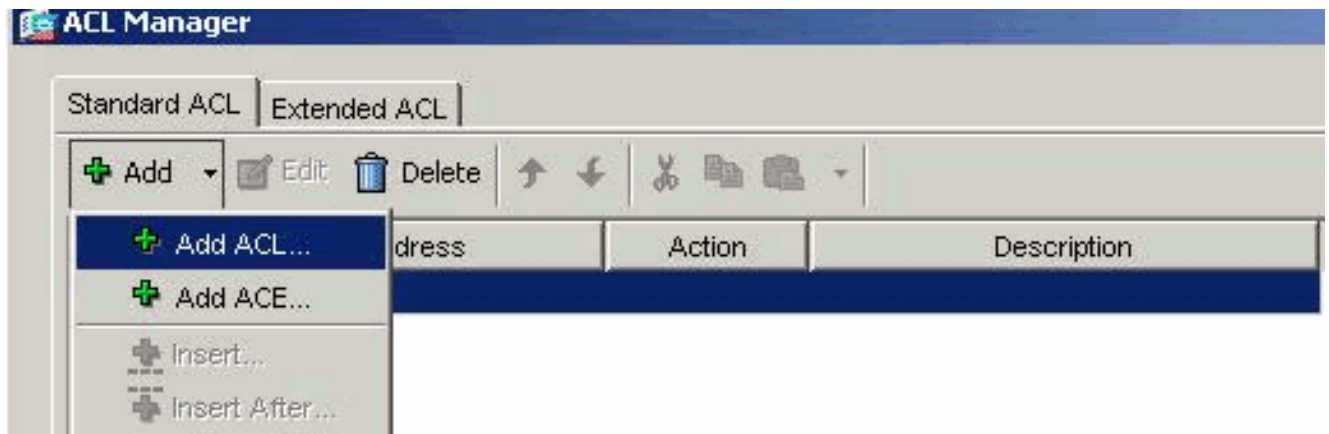
Address pools

Inherit

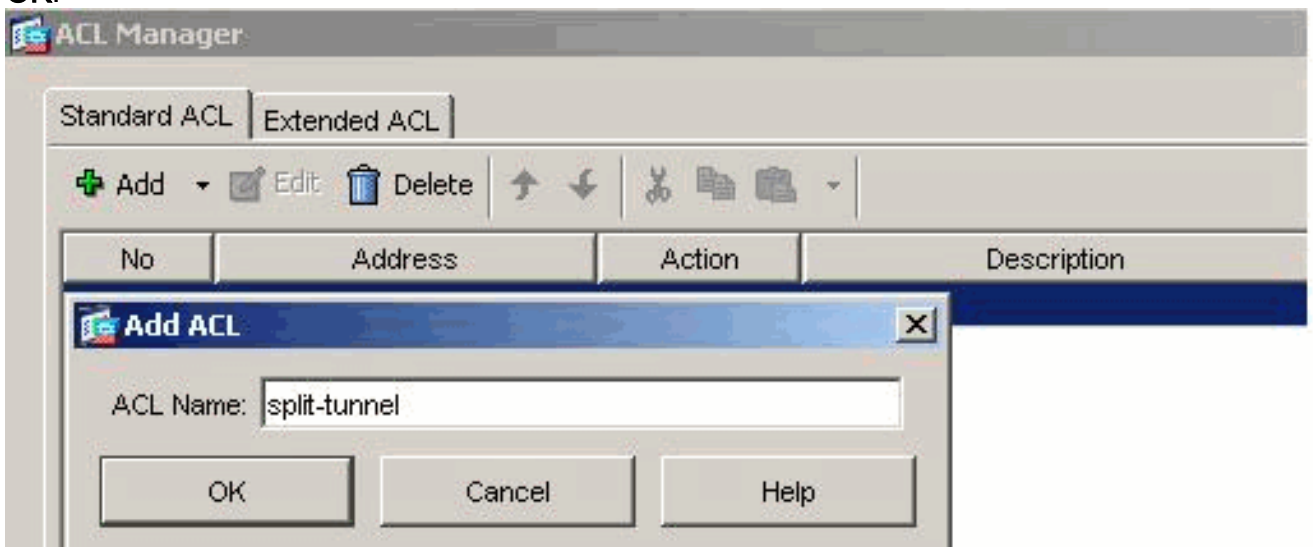
Available Pools:

Assigned Pools (up to 6 entries):

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

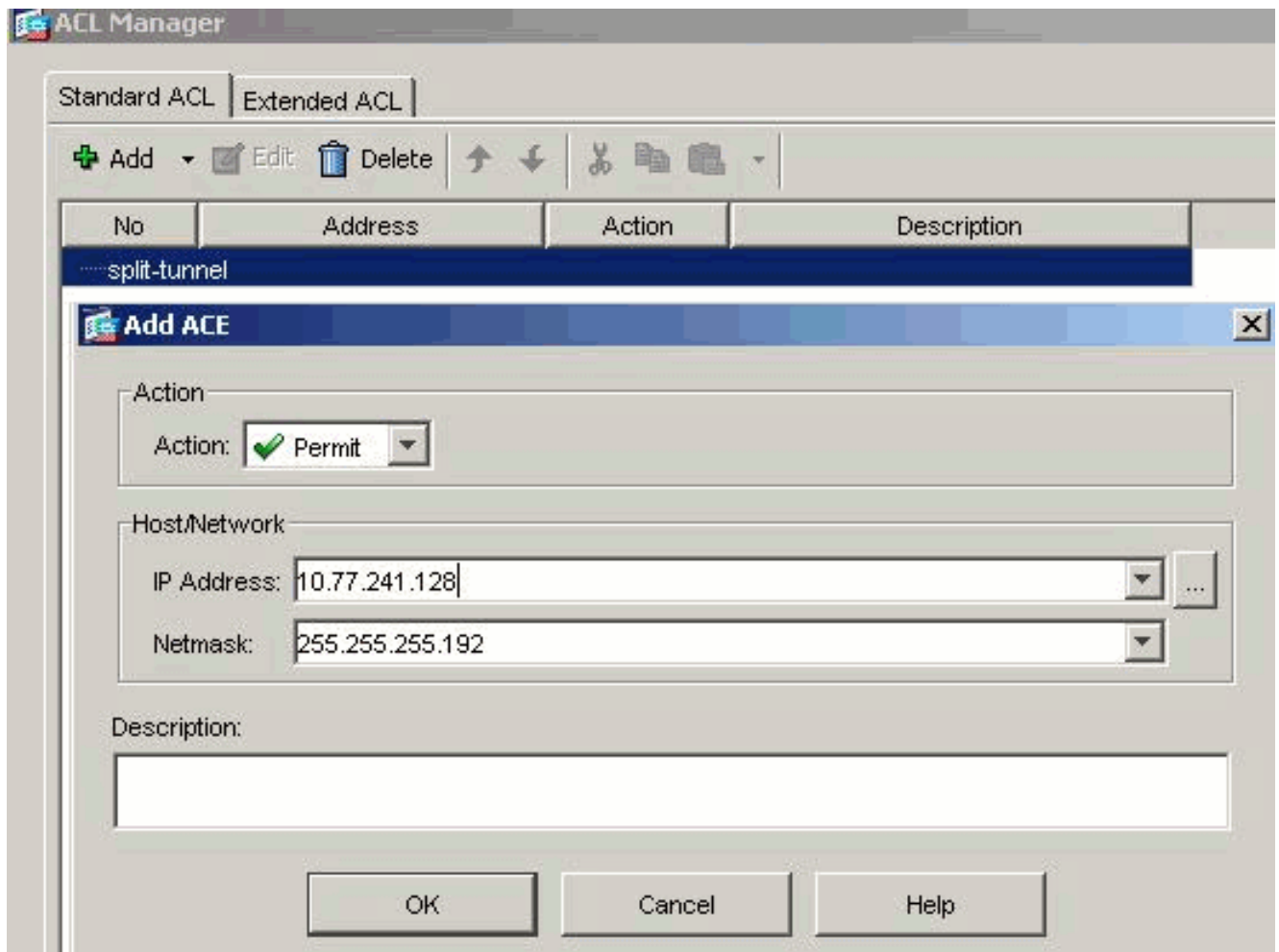


Asigne un nombre al ACL y haga clic en OK.



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 elige el **permiso**. Haga clic en OK para salir del Administrador de ACL.





Esté seguro que el ACL que usted acaba de crear está seleccionado para la lista de red del túnel dividido.Haga clic en OK para volver a la configuración de la Política de Grupo.

**Edit Internal Group Policy: clientgroup**

Name:

General | IPsec | **Client Configuration** | Client Firewall | Hardware Client | NAC | WebVPN

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

General Client Parameters | Cisco Client Parameters | Microsoft Client Parameters

Banner:  Inherit

Default Domain:  Inherit

Split Tunnel DNS Names (space delimited):  Inherit

Split Tunnel Policy:  Inherit

Split Tunnel Network List:  Inherit

Address pools

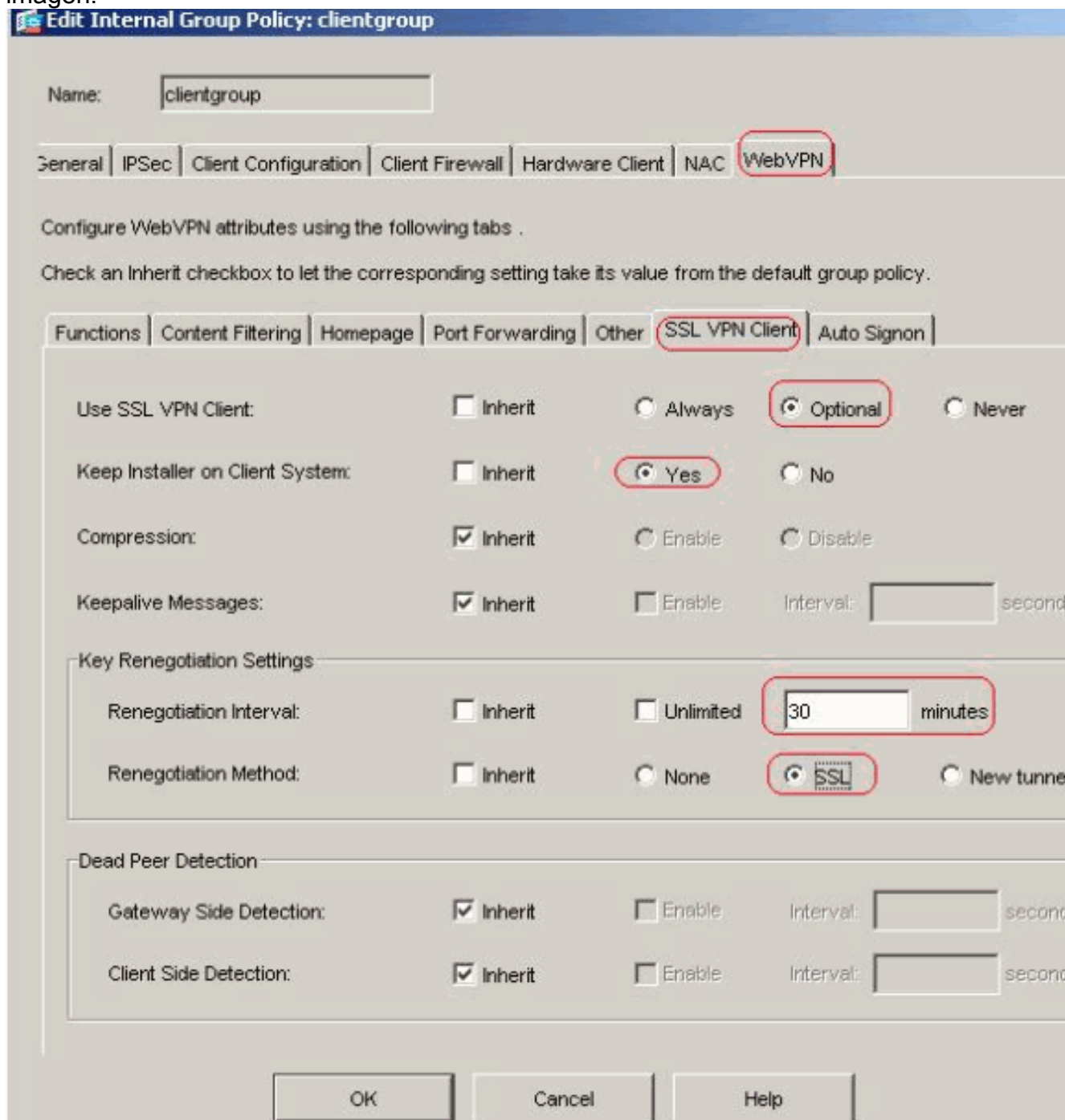
Inherit

Available Pools:

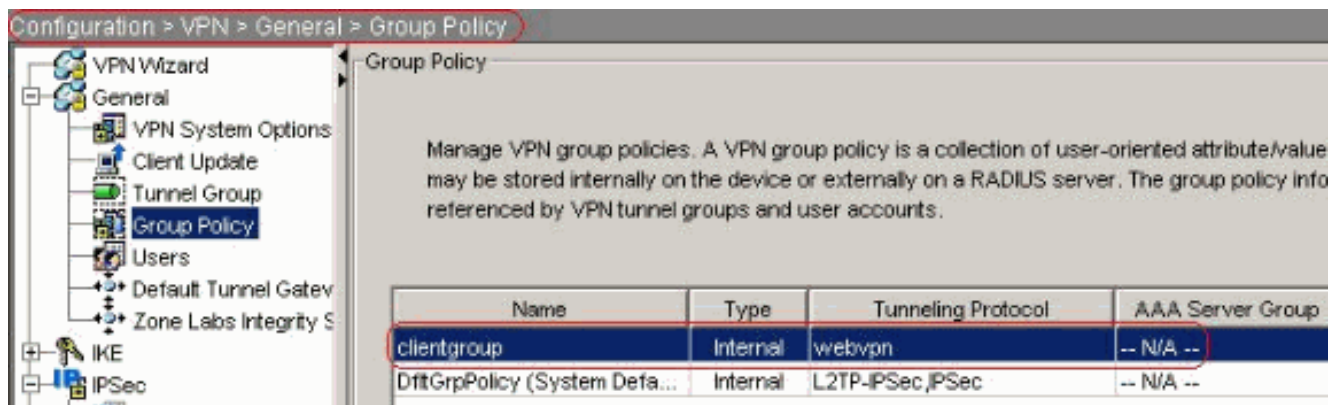
Assigned Pools (up to 6 entries):

En la página principal, el teclado **se aplica** y después **envía** (si procede) para enviar los comandos al ASA. Para la opción del Cliente VPN del uso SSL, desmarque la casilla de verificación de la **herencia** y haga clic el botón de radio **opcional**. Esta opción permite que el cliente remoto elija si hacer clic la lengüeta del **WebVPN > del cliente SSLVPN**, y elegir estas opciones: No descargue SVC. El siempre bien escogido se asegura de que SVC esté descargado a la estación de trabajo remota durante cada conexión VPN SSL. 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 de SVC permanezca en la máquina del cliente; por lo tanto, el ASA no se requiere para descargar el software de 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. 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. Se aumenta la Seguridad cuando usted establece los límites en la longitud del 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. Sus atributos del cliente VPN SSL se deben configurar tal y como se muestra en de esta imagen:



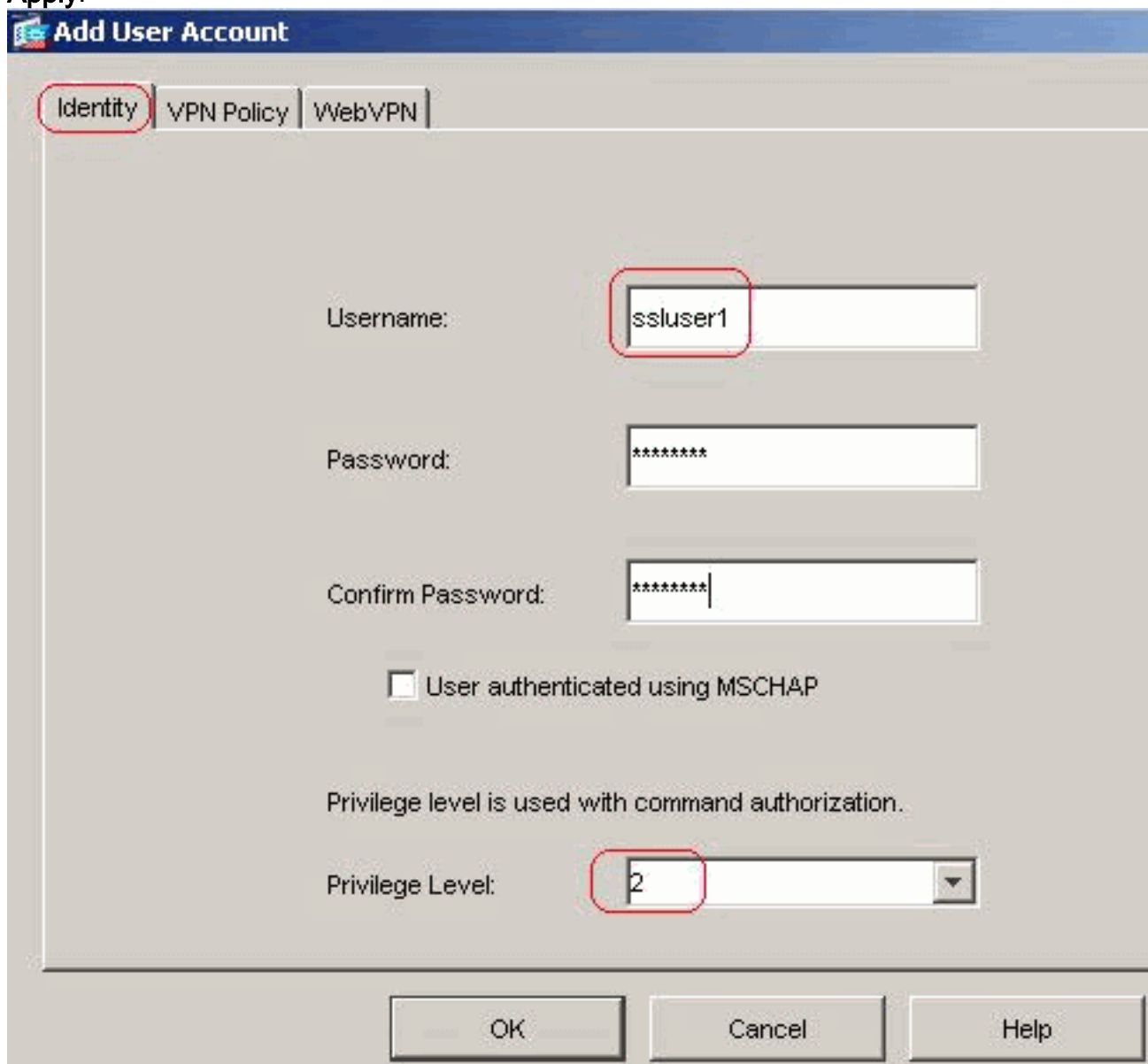
Haga clic en OK y en Apply.



### Configuración CLI Equivalente:

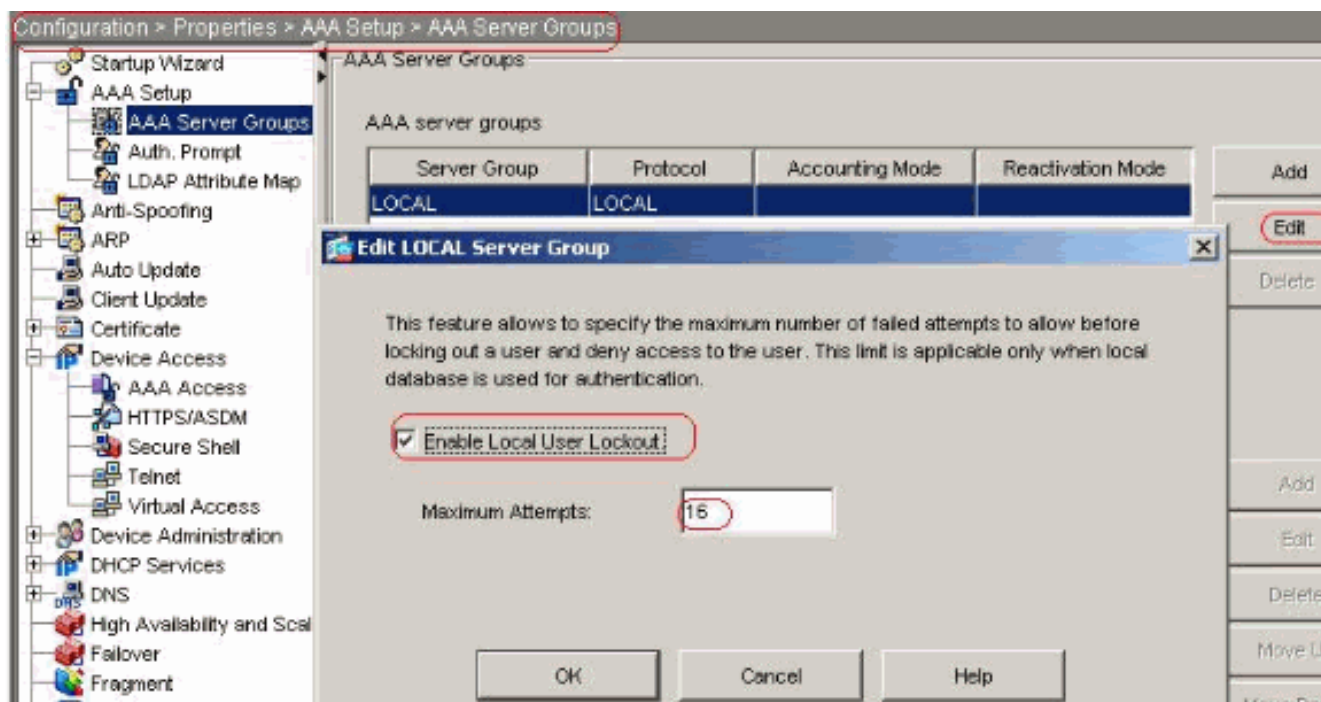
5. Elija la configuración > el VPN > al general > Users > Add para crear una cuenta de usuario nuevo **ssluser1**. Haga clic en OK y en

Apply.



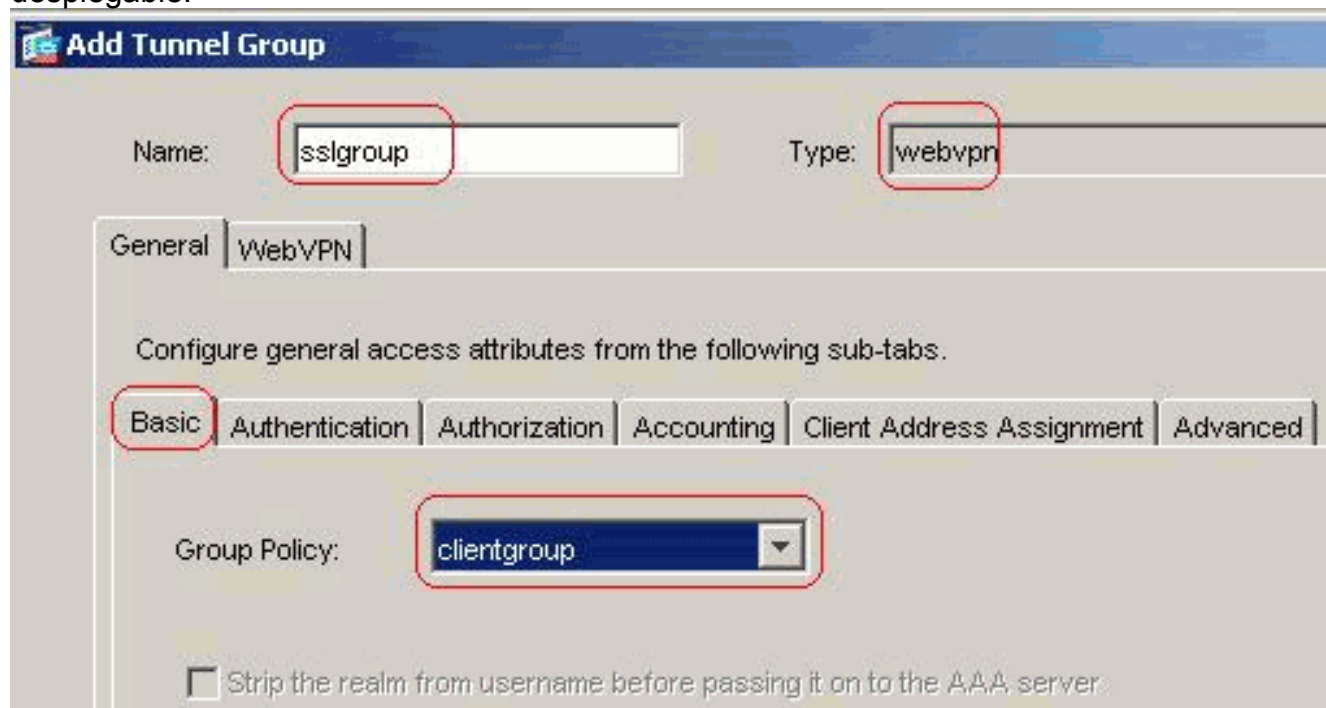
### Configuración CLI Equivalente:

6. Elija la configuración > las propiedades > AAA ponen > AAA los grupos de servidores > editan para modificar el grupo de servidores predeterminado **LOCAL** y elegir la casilla de verificación del **cierre del usuario local del permiso** con el valor de las tentativas del máximo como **16**.



Configuración CLI Equivalente:

- Grupo de túnel de la configuración Elija la configuración > el VPN > el general > al grupo de túnel > Add (acceso del WebVPN) para crear un nuevo sslgroup del grupo de túnel. En la lengüeta general > básica, elija la directiva del grupo como clientgroup de la lista desplegable.



En general la lengüeta de la **asignación de dirección cliente**, bajo agrupaciones de direcciones, tecleo **agrega >>** para asignar el **vpnpool** del pool de la dirección disponible.

**Add Tunnel Group**

Name:  Type:

General | **WebVPN**

Configure general access attributes from the following sub-tabs.

Basic | Authentication | Authorization | Accounting | **Client Address Assignment** | Advanced

To specify whether to use DHCP or address pools for address assignment, go to Configuration > VPN > IP Address Management > Assignment.

DHCP Servers

IP Address:

Address Pools

To configure interface-specific address pools, go to the Advanced tab.

Available Pools

Assigned pools

vpnpool
---------

En el **WebVPN > los alias del grupo y los URL** tabule, teclee el nombre de alias en el cuadro del parámetro y el tecleo **agrega >>** para hacer que aparece en la lista de nombres del grupo en la página de registro.

General | **WebVPN**

Configure WebVPN access attributes from the following sub-tabs.

Basic | NetBIOS Servers | **Group Aliases and URLs** | Web Page

Group Aliases

Alias:

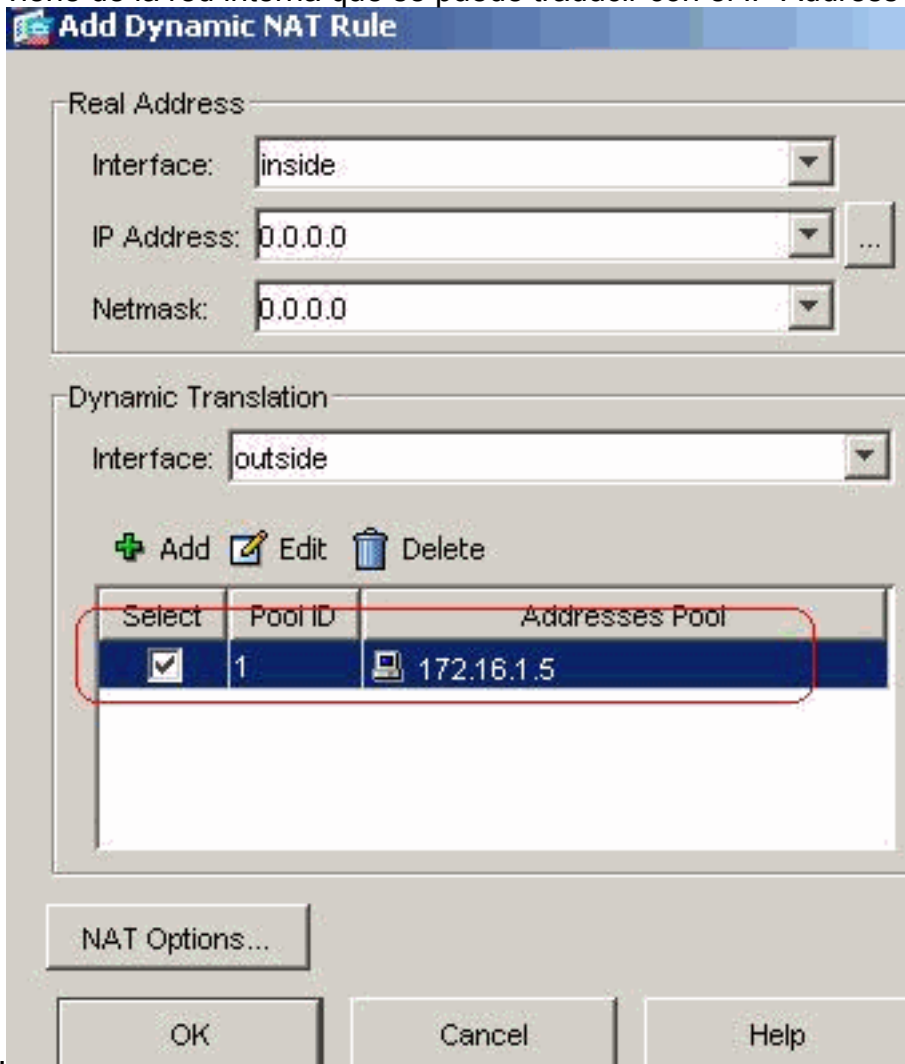
Enable

Alias	Status
sslgroup_users	enable

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

8. Configuración NATElija la configuración > la regla dinámica NAT > Add > Add NAT para el

tráfico que viene de la red interna que se puede traducir con el IP Address externo



172.16.1.5.

El Haga Click en

OK y el tecleo **se aplican** en la página principal.**Configuración CLI Equivalente:**

9. Configure la NAT-exención para el tráfico de retorno por dentro de la red 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 ASA 7.2(2) usando el CLI**

```
Cisco ASA 7.2(2)
ciscoasa#show running-config : Saved : ASA Version
7.2(2) ! hostname ciscoasa 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
ftp mode passive 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 mtu
```

```

inside 1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 !--- The address pool for
the SSL VPN Clients no failover icmp unreachable rate-
limit 1 burst-size 1 asdm image disk0:/asdm-522.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
access-group 100 in interface outside 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 0:05:0 timeout sip 0:30:00
sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02: timeout uauth 0:05:00 absolute group-policy
clientgroup internal !--- Create an internal group
policy "clientgroup". group-policy clientgroup
attributes vpn-tunnel-protocol webvpn !--- Enable webvpn
as 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 required !--- Activate the
SVC under webvpn mode. svc keep-installer installed !---
When the security appliance and the SVC perform a rekey,
!--- they renegotiate the crypto keys and initialization
vectors, !--- and increase 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. username ssluser1 password ZRhW85jZqEaVd5P.
encrypted !--- Create an user account "ssluser1". aaa
local authentication attempts max-fail 16 !--- Enable
the AAA local authentication. 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 tunnel-group
sslgroup type webvpn !--- Create a tunnel group
"sslgroup" with type as WebVPN. 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. telnet
timeout 5 ssh timeout 5 console timeout 0 ! 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
esmtip 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:/sslclient-win-1.1.4.179.pkg
1 !--- Assign an order to the SVC 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

```

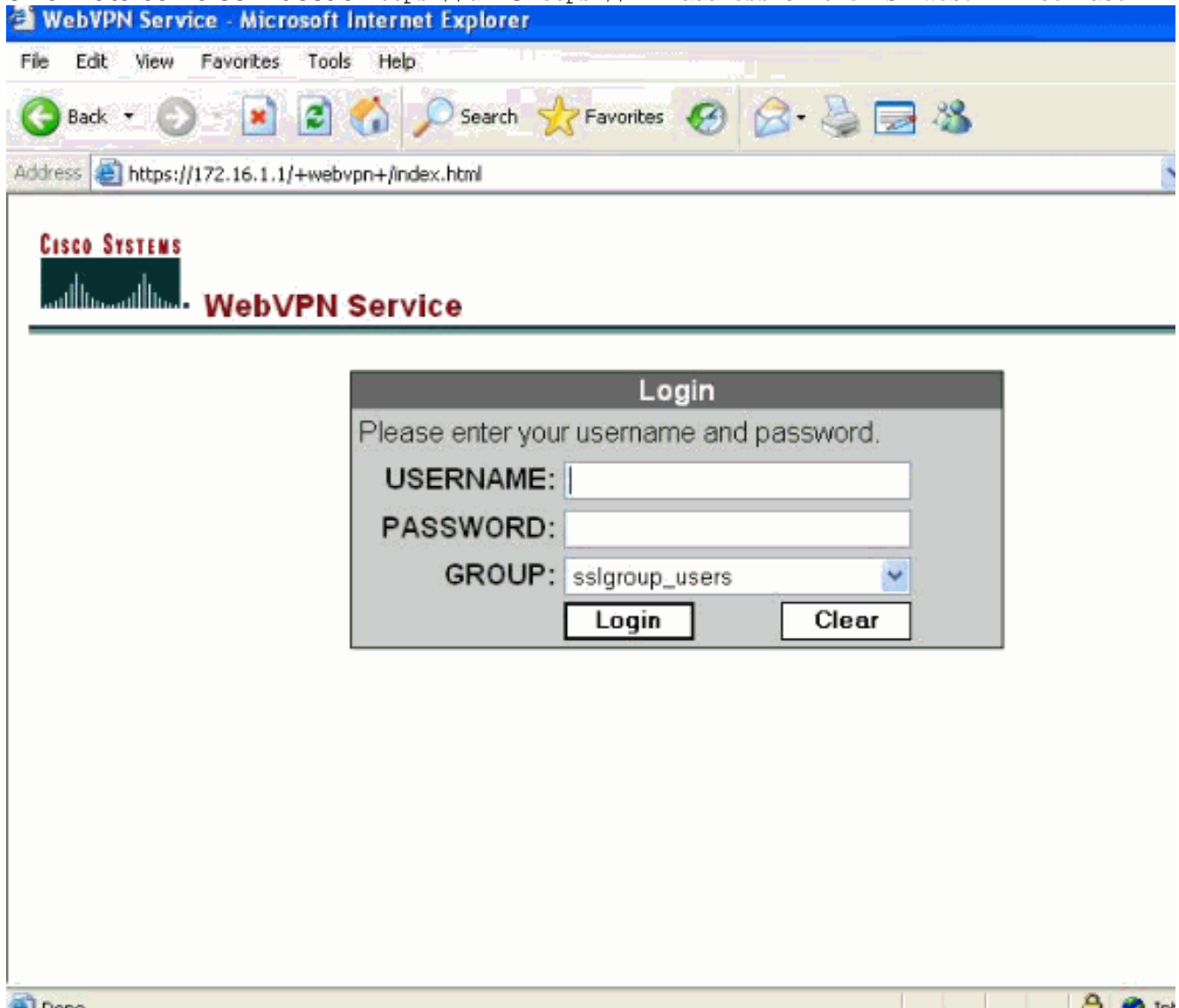


```
the WebVPN Login page. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#
```

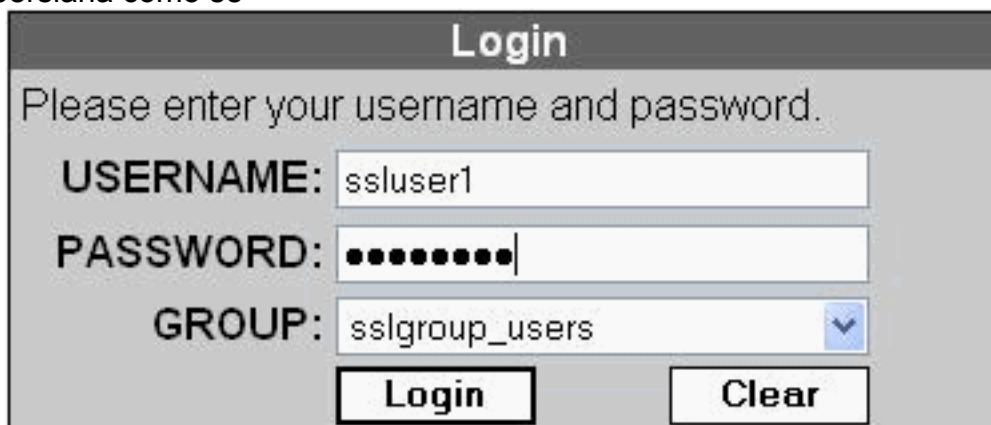
## Establezca la Conexión VPN SSL con el SVC

Complete estos pasos para establecer una conexión VPN SSL con el ASA.

1. Teclee el URL o la dirección IP de la interfaz del WebVPN del ASA en su buscador Web en el formato como se muestra. `https://urlOhttps://<IP address of the ASA WebVPN interface>`



2. Ingrese su nombre de usuario y contraseña y después elija a su grupo correspondiente de la lista de persiana como se



muestra.

3. El software de ActiveX se debe instalar en su ordenador antes de la descarga



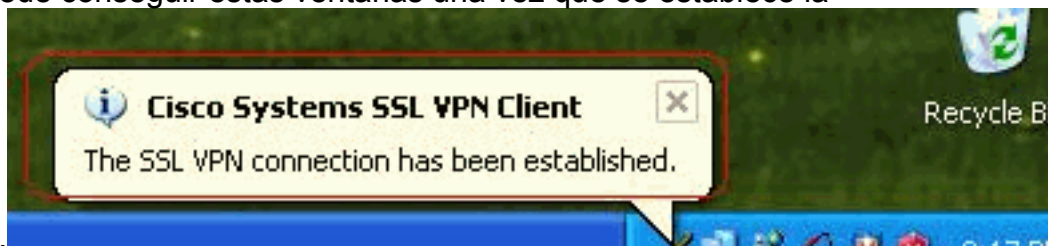
SVC.

4. Estas ventanas aparecen antes de que se establezca la conexión VPN



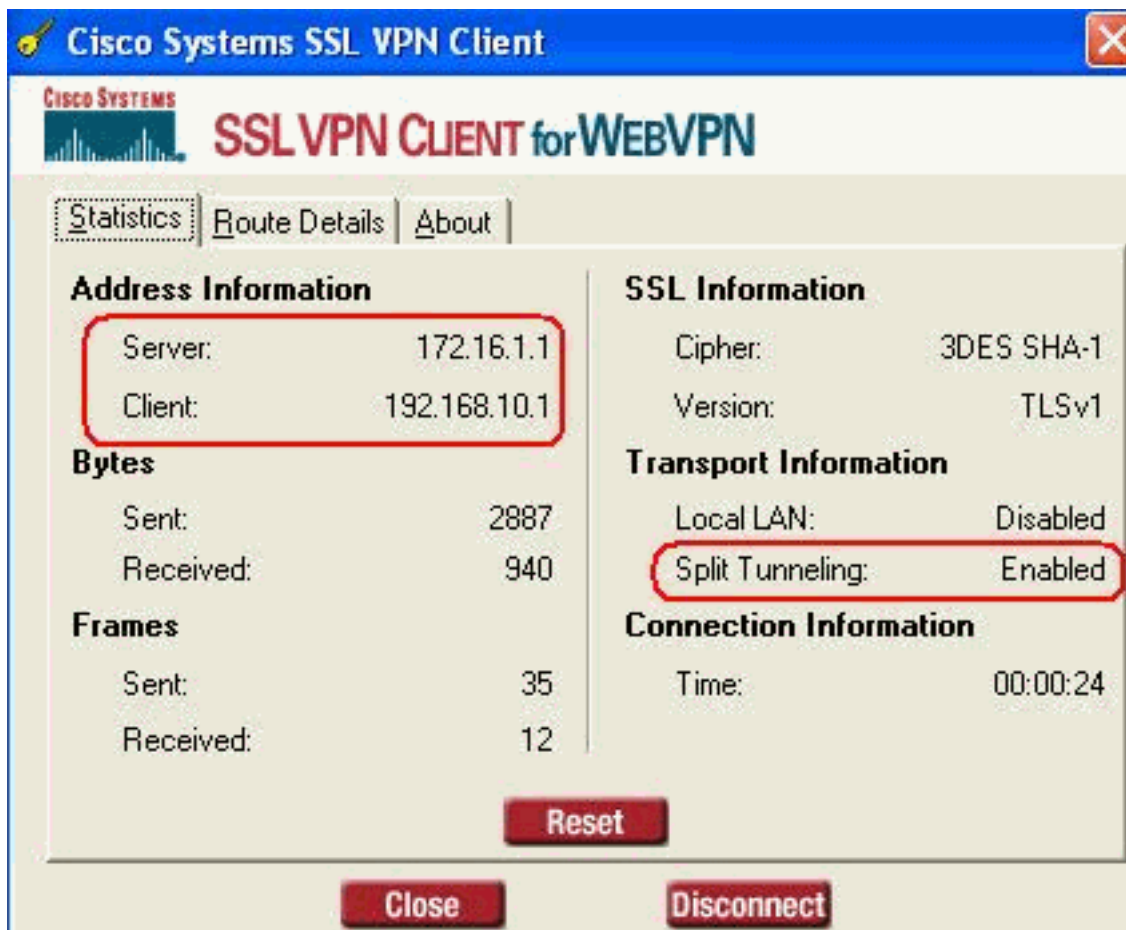
SSL.

5. Usted puede conseguir estas ventanas una vez que se establece la

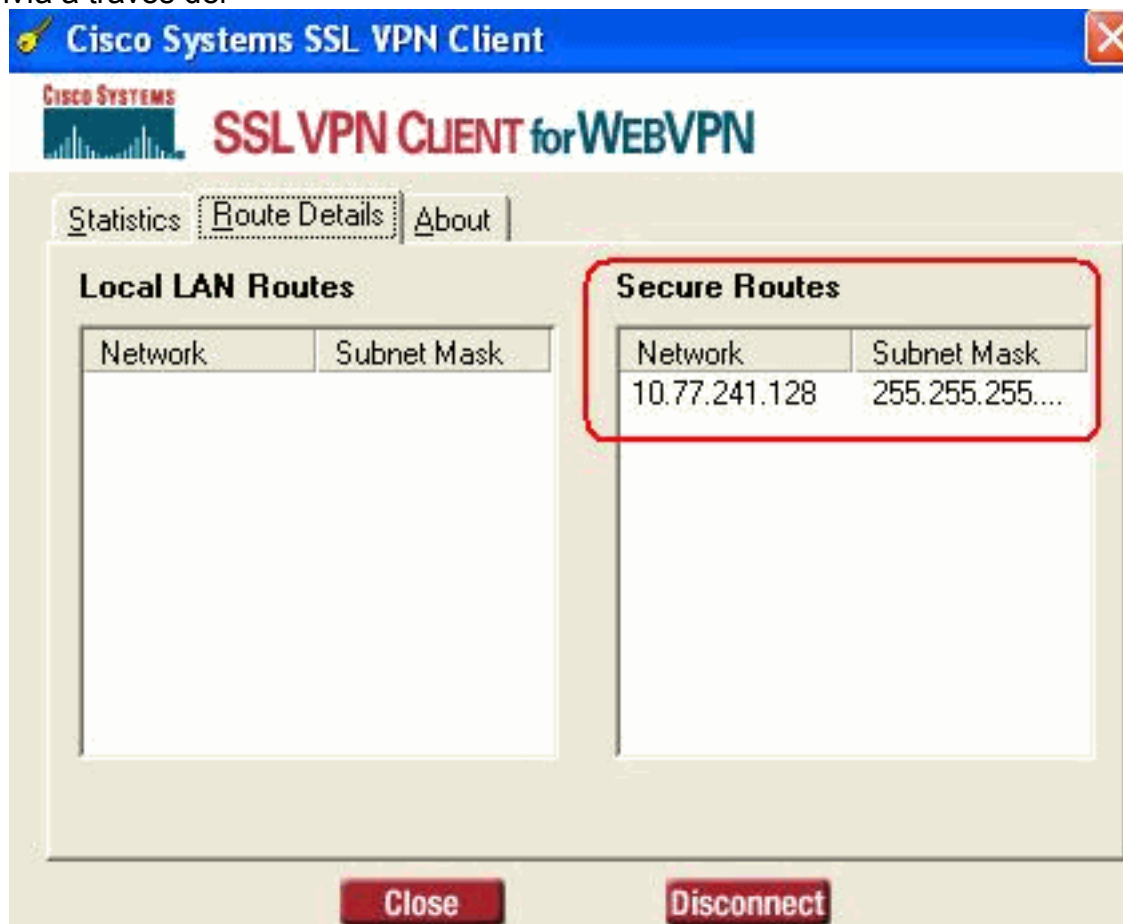


conexión.

6. Haga clic la clave amarilla que aparece en la barra de tareas de su ordenador. Estas ventanas aparecen que da la información sobre la conexión SSL. Por ejemplo, **se habilita 192.168.10.1** es IP asignada para el cliente y servidor que la dirección IP es 172.16.1.1, **Túnel dividido**, y así sucesivamente.



Usted puede también marcar la red segura que debe ser cifrada por el SSL, la lista de red se descarga de la lista de acceso del túnel dividido configurada en el ASA. En este ejemplo, el cliente VPN SSL asegura el acceso a 10.77.241.128/24 mientras que el resto del tráfico no se cifra y no se envía a través del



túnel.



## 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:/sslclient-win-1.1.4.179.pkg 1 CISCO STC win2k+ 1.0.0 1,1,4,179 Fri 01/18/2008 15:19:49.43 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 : 1 Assigned IP : 192.168.10.1 Public IP : 192.168.1.1 Protocol : SVC Encryption : 3DES Hashing : SHA1 Bytes Tx : 131813 Bytes Rx : 5082 Client Type : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Client Ver : Cisco Systems SSL VPN Client 1, 1, 4, 179 Group Policy : clientgroup Tunnel Group : sslgroup Login Time : 12:38:47 UTC Mon Mar 17 2008 Duration : 0h:00m:53s Filter Name :`
- **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 el ASDM, elija la **supervisión > el VPN > los VPN statistics (Estadísticas de la VPN) > las sesiones** para saber sobre las sesiones WebVPN actuales en el ASA.

Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
0	0	1	0	0	1	12

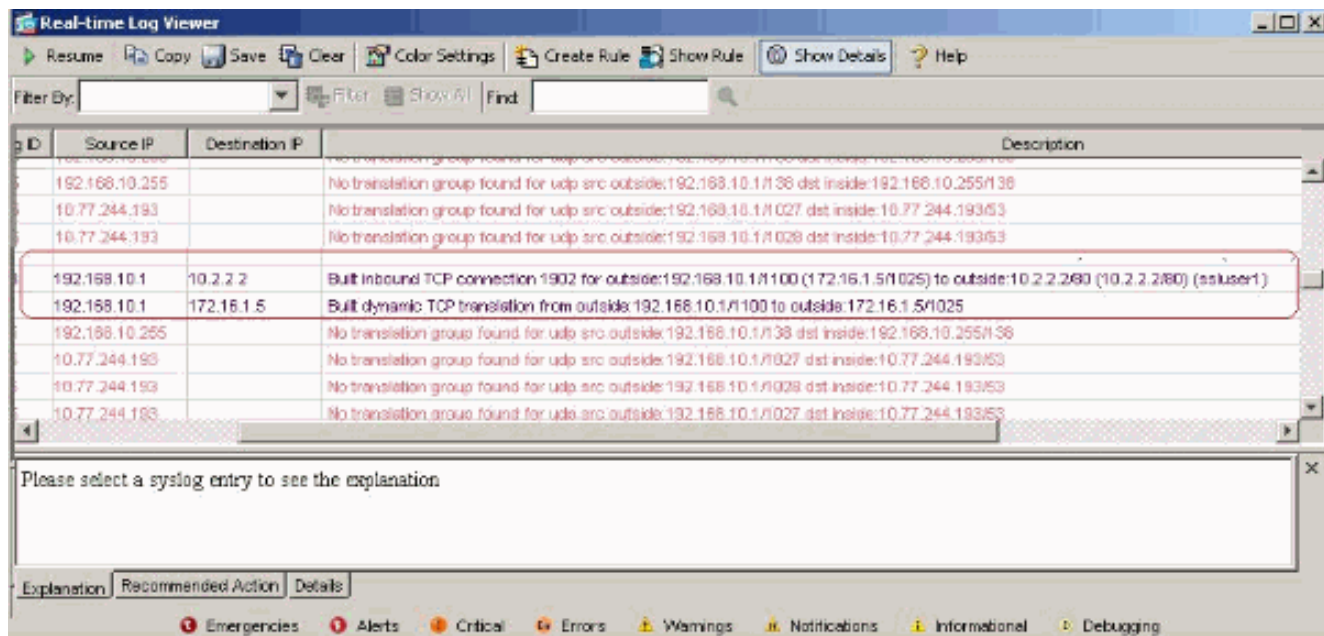
  

Username IP Address	Group Policy Tunnel Group	Protocol Encryption	Login Time Duration	Details
ssluser1 192.168.1.1	clientgroup ssigroup	WebVPN 3DES	08:49:52 UTC Thu Mar 20 2014 0h:08m:14s	Logout Ping

## Troubleshooting

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

- 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 Called vpn\_remove\_uauth: success! webvpn\_svc\_np\_tear\_down: no ACL NFO: Number of sessions with name "ssluser1" logged off : 1* De forma similar, puede utilizar el comando **vpn-sessiondb logoff svc** para finalizar las sesiones SVC.
- Nota:** Si el equipo se encuentra en el modo standby o hibernación, la conexión VPN SSL puede ser terminada.  
*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, etc) Called vpn\_remove\_uauth: success! webvpn\_svc\_np\_tear\_down: no ACL ciscoasa#show vpn-sessiondb svc INFO: There are presently no active sessions*
- debug webvpn svc <1-255>: proporciona los eventos webvpn en tiempo real para establecer la sesión.**  
*ciscoasa#debug webvpn svc 7 ATTR\_CISCO\_AV\_PAIR: got SVC ACL: -1  
webvpn\_rx\_data\_tunnel\_connect CSTEP 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 CSTEP header line: 'Host: 172.16.1.1'  
webvpn\_cstp\_parse\_request\_field() ...input: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179' Processing CSTEP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179' Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'  
webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTEP-Version: 1' Processing CSTEP header line: 'X-CSTEP-Version: 1' Setting version to '1' webvpn\_cstp\_parse\_request\_field()  
...input: 'X-CSTEP-Hostname: tacweb' Processing CSTEP header line: 'X-CSTEP-Hostname: tacweb' Setting hostname to: 'tacweb' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTEP-Accept-Encoding: deflate;q=1.0' Processing CSTEP header line: 'X-CSTEP-Accept-Encoding: deflate;q=1.0' webvpn\_cstp\_parse\_request\_field() ...input: 'Cookie: webvpn=16885952@10@1205757506@d4886d33fbb1cf236db5e8be70b1486d5bc554d2' Processing CSTEP header line: 'Cookie: webvpn=16885952@10@1205757506@d4886d33fbb1cf236db5e8be70b1486d5bc554d2' Found WebVPN cookie: 'webvpn=16885952@10@1205757506@d4886d33fbb1cf236db5e8be70b1486d5bc554d2' WebVPN Cookie: 'webvpn=16885952@10@1205757506@d4886d33fbb1cf236db5e8be70b1486d5bc554d2' Validating address: 0.0.0.0 CSTEP state = WAIT\_FOR\_ADDRESS webvpn\_cstp\_accept\_address: 192.168.10.1/0.0.0.0 CSTEP state = HAVE\_ADDRESS No subnetmask... must calculate it SVC: NP setup webvpn\_svc\_np\_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn\_put\_uauth success! SVC: adding to sessmgmt SVC: Sending response CSTEP state = CONNECTED*
- En ASDM, elija **Monitoring > Logging > Real-time Log Viewer > View** para ver los eventos en tiempo real. Estas demostraciones del ejemplo sobre la información de la sesión entre SVC 192.168.10.1 y web server 10.2.2.2 en Internet con ASA 172.16.1.5.



## Información Relacionada

- [Soporte de productos adaptante del dispositivo de seguridad de las Cisco 5500 Series](#)
- [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](#)