

ASA 7.1/7.2: Ejemplo de Configuración de Permitir Tunelización Dividida para SVC en ASA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones ASA con ASDM 5.2\(2\)](#)

[Configuración de ASA 7.2\(2\) mediante CLI](#)

[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 a Internet de los clientes VPN de capa de socket seguro (SSL) mientras se tunelizan en un Cisco Adaptive Security Appliance (ASA). Esta configuración permite el acceso seguro de SVC a los recursos corporativos a través de SSL y proporciona acceso no seguro a Internet con el uso de tunelización dividida.

La capacidad de transmitir tráfico seguro y no seguro en la misma interfaz se conoce como tunelización dividida. La tunelización dividida requiere que especifique exactamente qué tráfico está protegido y cuál es el destino de ese tráfico, de modo que sólo el tráfico especificado entre en el túnel, mientras que el resto se transmite sin cifrar a través de la red pública (Internet).

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Privilegios administrativos locales en todas las estaciones de trabajo remotas
- Controles Java y ActiveX en la estación de trabajo remota
- El puerto 443 (SSL) no está bloqueado en ninguna parte a lo largo de la ruta de conexión

Componentes Utilizados

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

- Cisco 5500 Series Adaptive Security Appliance (ASA) que ejecuta la versión de software 7.2(2)
- Cisco SSL VPN Client versión para Windows 1.1.4.179**Nota:** Descargue el paquete SSL VPN Client (sslclient-win*.pkg) de la [descarga de software de Cisco \(sólo clientes registrados\)](#) . Copie el SVC a la memoria flash del ASA, que se descargará a los equipos de usuario remotos para establecer la conexión SSL VPN con ASA. Refiérase a [la sección Instalación del Software SVC](#) de la Guía de Configuración de ASA para obtener más información.
- PC que ejecuta Windows 2000 Professional SP4 o Windows XP SP2
- Versión 5.2(2) 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. 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 SSL VPN Client (SVC) es una tecnología de tunelización VPN que ofrece a los usuarios remotos las ventajas de un cliente VPN IPsec sin necesidad de que los administradores de red instalen y configuren clientes VPN IPsec en equipos remotos. El SVC utiliza el cifrado SSL que ya está presente en el equipo remoto, así como el inicio de sesión WebVPN y la autenticación del dispositivo de seguridad.

Para establecer una sesión SVC, el usuario remoto ingresa la dirección IP de una interfaz WebVPN del dispositivo de seguridad en el navegador y el navegador se conecta a esa interfaz y muestra la pantalla de inicio de sesión WebVPN. Si satisface el inicio de sesión y la autenticación, y el dispositivo de seguridad lo identifica como que necesita el SVC, el dispositivo de seguridad descarga el SVC en el equipo remoto. Si el dispositivo de seguridad lo identifica con la opción de utilizar el SVC, el dispositivo de seguridad descarga el SVC en el equipo remoto mientras presenta un link en la ventana para saltar la instalación del SVC.

Después de descargar, el SVC se instala y configura a sí mismo y, a continuación, el SVC permanece o se desinstala, lo que depende de la configuración, del equipo remoto cuando finaliza la conexión.

Configurar

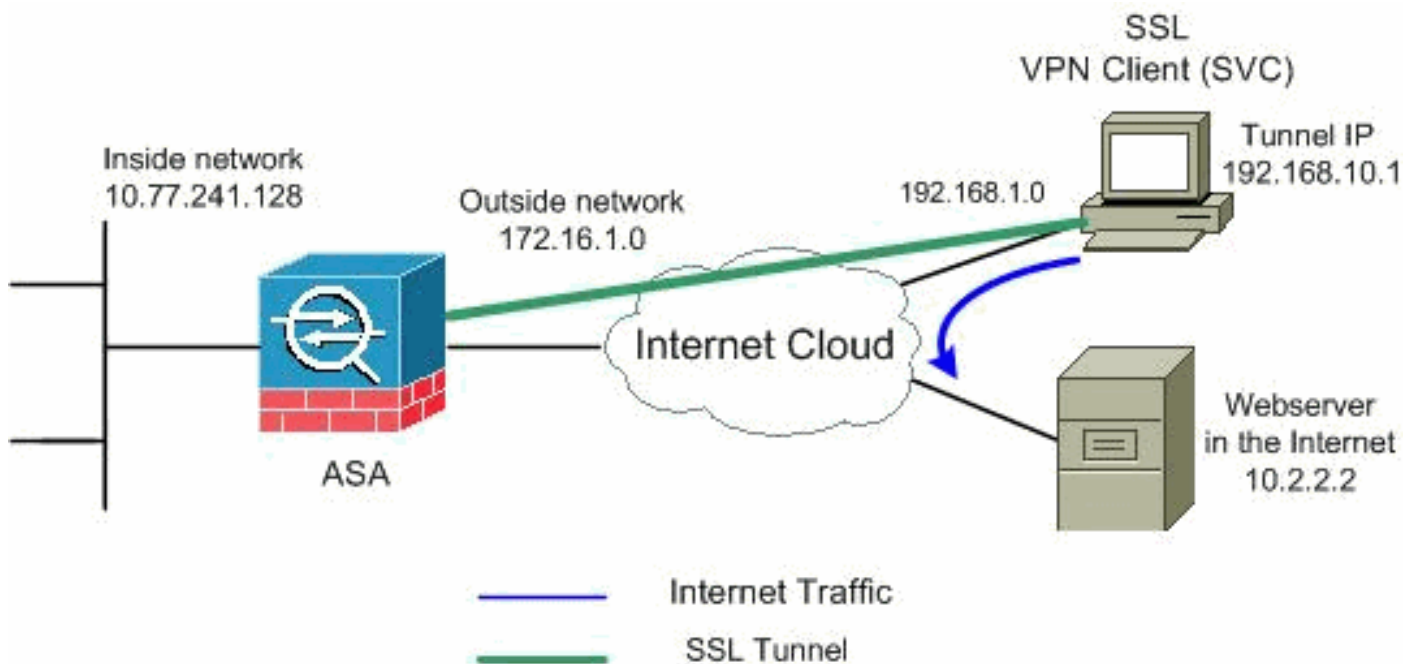
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use el [Command Lookup Tool](#) (únicamente clientes registrados) para obtener más

información sobre los comandos que se utilizan 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.

Configuraciones ASA con ASDM 5.2(2)

Complete estos pasos para configurar SSL VPN en ASA con Tunelización Dividida como se muestra:

1. El documento asume que la configuración básica, como la configuración de la interfaz, etc., ya está hecha 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](#).
2. Elija **Configuration > VPN > IP Address Management > IP Pools** para crear un pool de direcciones IP: `vpnpool` para clientes

Add IP Pool

Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

OK Cancel Help

VPN.

Haga clic en Apply (Aplicar).

3. **Habilite WebVPN** Elija **Configuration > VPN > WebVPN > WebVPN Access** y resalte la interfaz exterior con el mouse y haga clic en **Enable**. Marque la casilla de verificación **Enable Tunnel Group Drop-down List on WebVPN Login Page** para habilitar la lista desplegable que aparece en la página de inicio de sesión para los usuarios, para elegir sus respectivos grupos.

Configuration > VPN > WebVPN > WebVPN Access

WebVPN Access

Configure access parameters for WebVPN.

Interface	WebVPN Enabled
inside	No
outside	Yes

Enable Disable

Port Number:

Default Idle Timeout: seconds

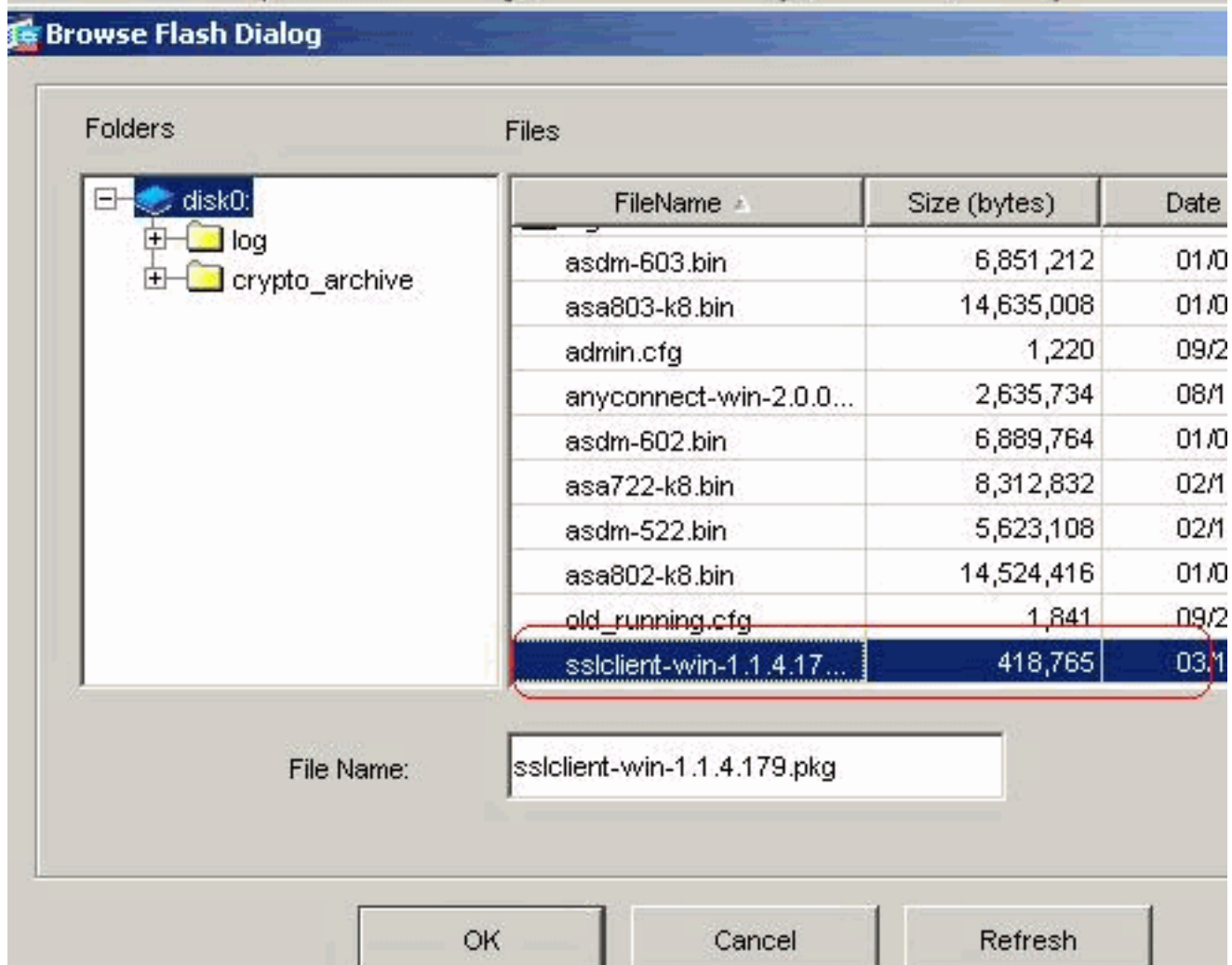
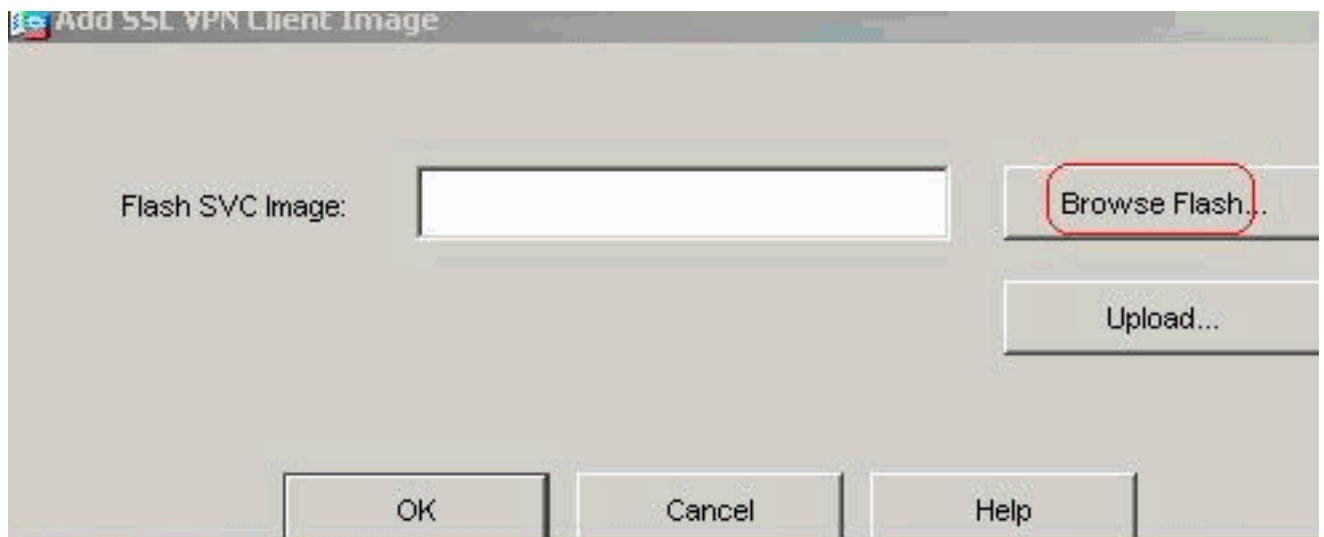
Max. Sessions Limit:

WebVPN Memory Size: % of total physical memory

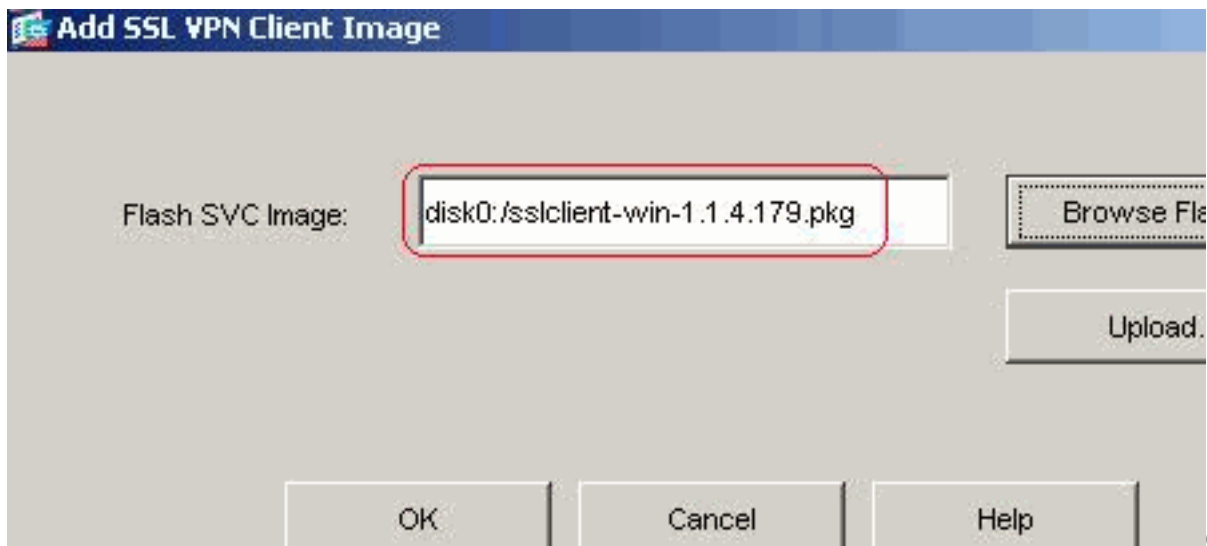
Enable Tunnel Group Drop-down List on WebVPN Login Page

Apply Reset

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

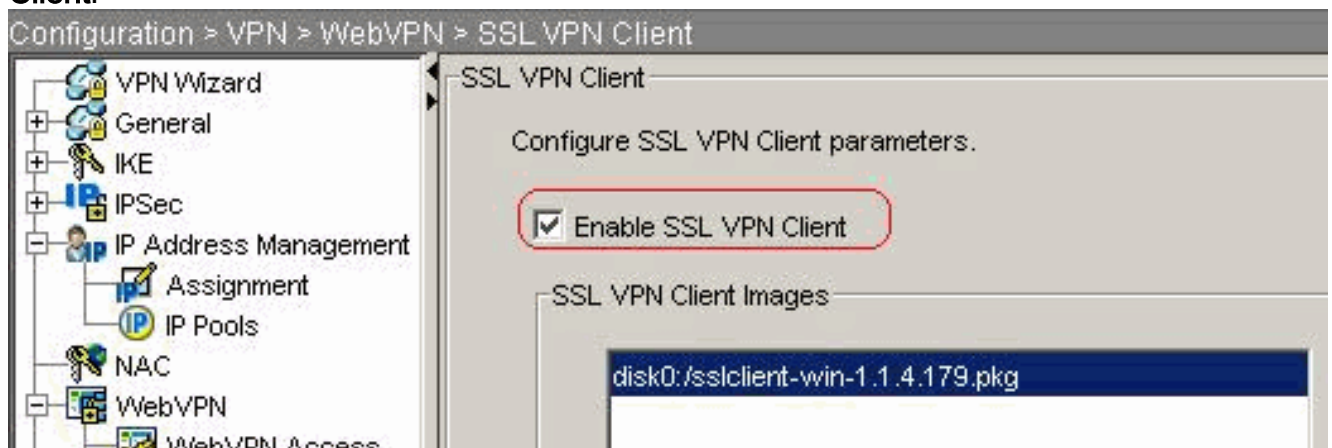


Click



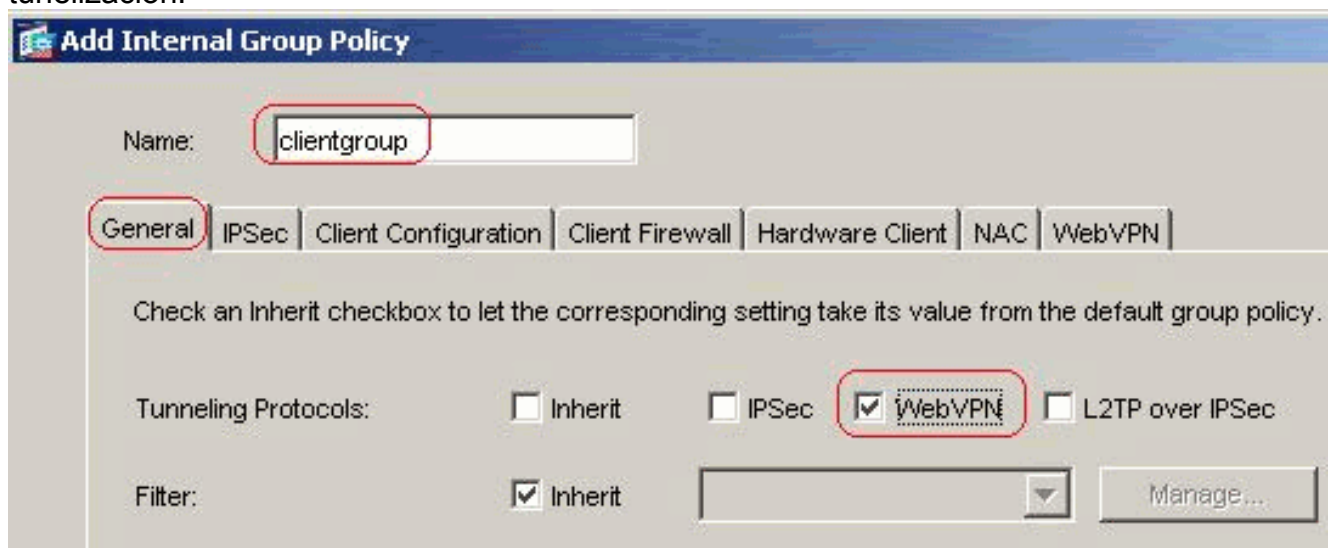
OK.

Haga clic en la casilla de verificación **SSL VPN Client**.



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

4. **Configure la Política de Grupo** Elija **Configuration > VPN > General > Group Policy > Add (Internal Group Policy)** para crear una política interna de grupo **clientgroup**. Bajo **General**, elija la casilla de verificación **WebVPN** para habilitar el WebVPN como protocolo de tunelización.



En la pestaña **Configuración del Cliente > Parámetros Generales del Cliente**, desmarque el cuadro **Heredar** para la Política de Túnel Dividido y elija **Lista de Red de Túnel Debajo** de la lista desplegable. Desmarque la casilla **Heredar** para **Lista de Red de Túnel Dividido** y luego haga clic en **Administrar** para iniciar el Administrador de

ACL.

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

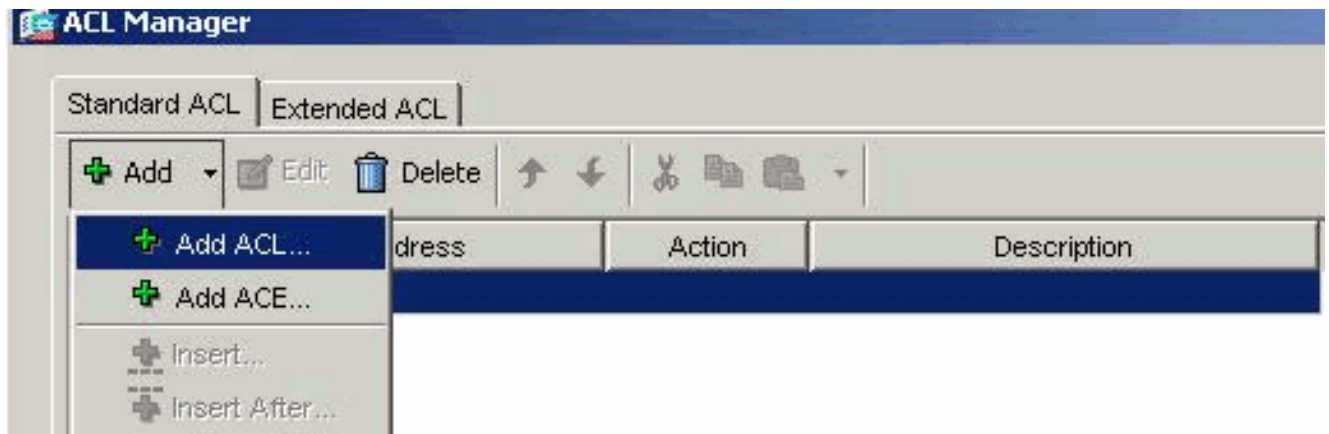
Address pools

Inherit

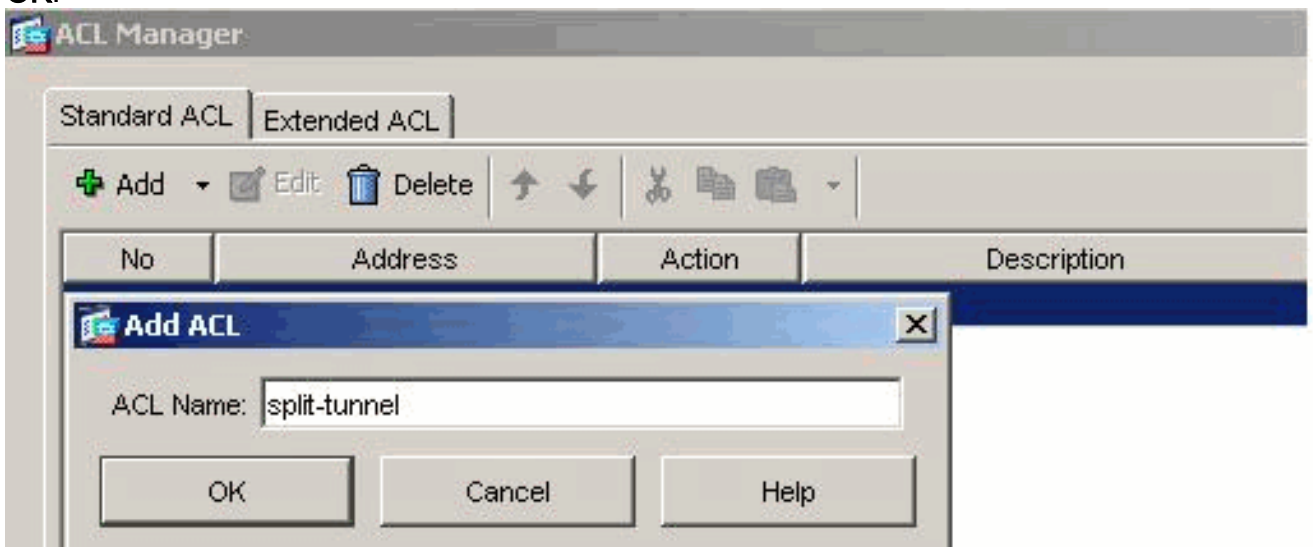
Available Pools

Assigned Pools (up to 6 entries)

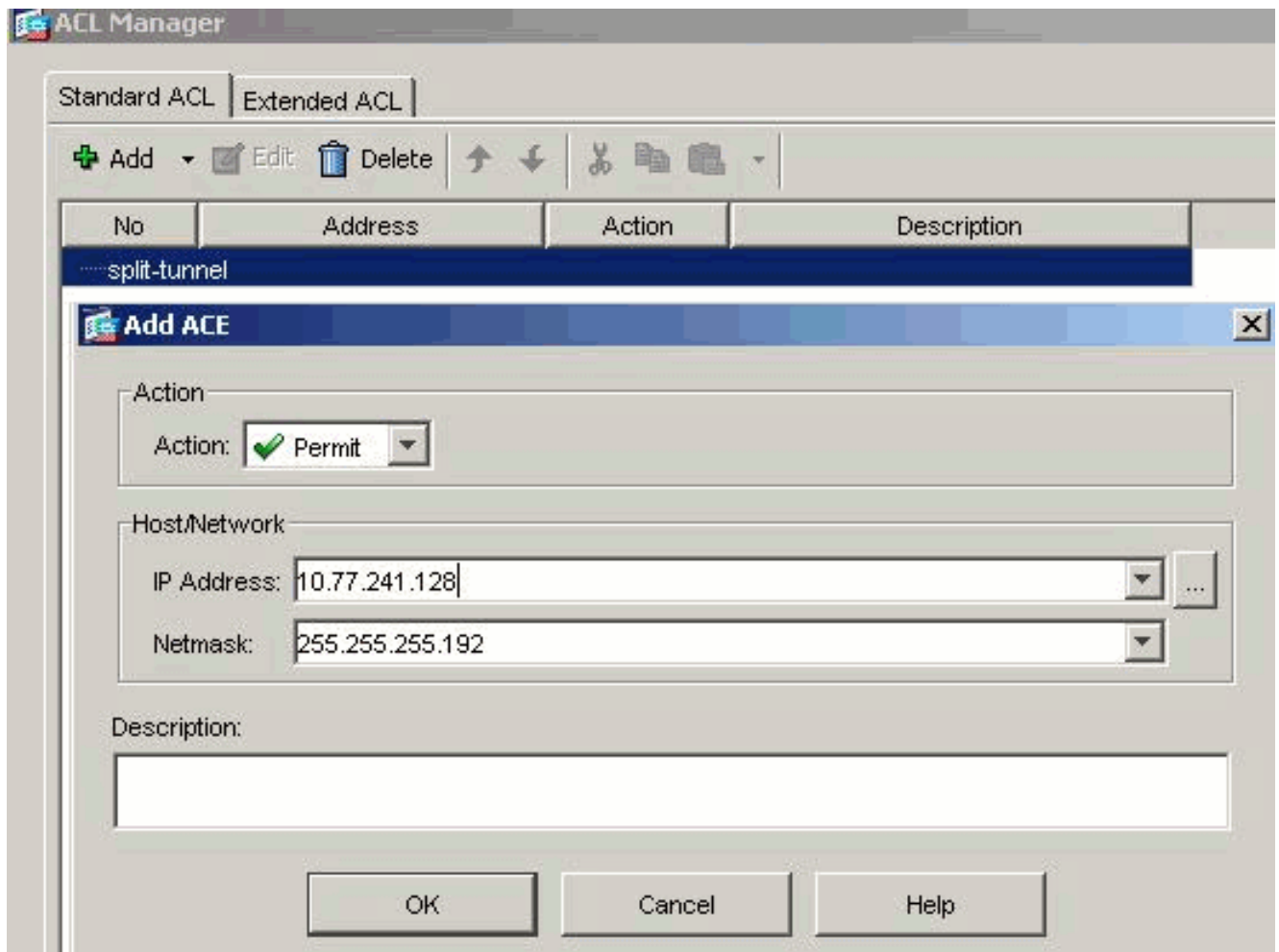
Dentro del Administrador de ACL, elija **Add > Add ACL...** para crear una nueva lista de acceso.



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 elija **Permit**. Haga clic en OK para salir del Administrador de ACL.



Asegúrese de que la ACL que acaba de crear esté seleccionada para la Lista de Red de 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, haga clic en **Aplicar** y luego **Enviar** (si es necesario) para enviar los comandos al ASA. Para la opción Use SSL VPN Client, desmarque la casilla de verificación **Inherit** y haga clic en el botón de opción **Opcional**. Esta opción permite al cliente remoto elegir si hacer clic en la pestaña **WebVPN > SSLVPN Client** y elegir estas opciones: No descargue el SVC. La opción Always (Siempre) garantiza que el SVC se descargue 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 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. Para la opción Intervalo de Renegociación, desmarque la casilla

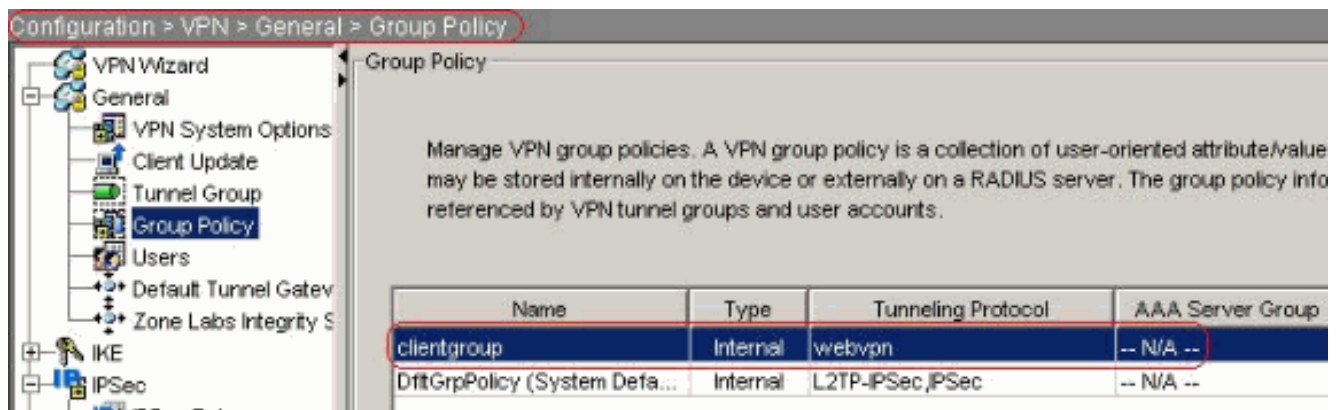
Inherit, desmarque la casilla de selección Unlimited, e ingrese el número de minutos hasta la generación de la nueva clave. La seguridad se mejora al establecer los límites en el tiempo que una clave es válida. Para la opción Método de Renegociación, desmarque la casilla de selección Inherit, y haga clic el botón de opción SSL. La renegociación puede utilizar el túnel SSL actual o un túnel nuevo creado expresamente para la renegociación. Los atributos de SSL VPN Client deben configurarse como se muestra en esta imagen:

The screenshot shows the 'Edit Internal Group Policy: clientgroup' window. The 'Name' field contains 'clientgroup'. The 'WebVPN' tab is selected. Below the tabs, there is a section for 'Configure WebVPN attributes using the following tabs'. The 'SSL VPN Client' sub-tab is selected. The settings are as follows:

Setting	Inherit	Option 1	Option 2	Option 3
Use SSL VPN Client:	<input type="checkbox"/>	<input type="radio"/> Always	<input checked="" type="radio"/> Optional	<input type="radio"/> Never
Keep Installer on Client System:	<input type="checkbox"/>	<input checked="" type="radio"/> Yes	<input type="radio"/> No	
Compression:	<input checked="" type="checkbox"/>	<input type="radio"/> Enable	<input type="radio"/> Disable	
Keepalive Messages:	<input checked="" type="checkbox"/>	<input type="checkbox"/> Enable	Interval: <input type="text"/>	seconds
Key Renegotiation Settings				
Renegotiation Interval:	<input type="checkbox"/>	<input type="checkbox"/> Unlimited	<input type="text" value="30"/> minutes	
Renegotiation Method:	<input type="checkbox"/>	<input type="radio"/> None	<input checked="" type="radio"/> SSL	<input type="radio"/> New tunnel
Dead Peer Detection				
Gateway Side Detection:	<input checked="" type="checkbox"/>	<input type="checkbox"/> Enable	Interval: <input type="text"/>	seconds
Client Side Detection:	<input checked="" type="checkbox"/>	<input type="checkbox"/> Enable	Interval: <input type="text"/>	seconds

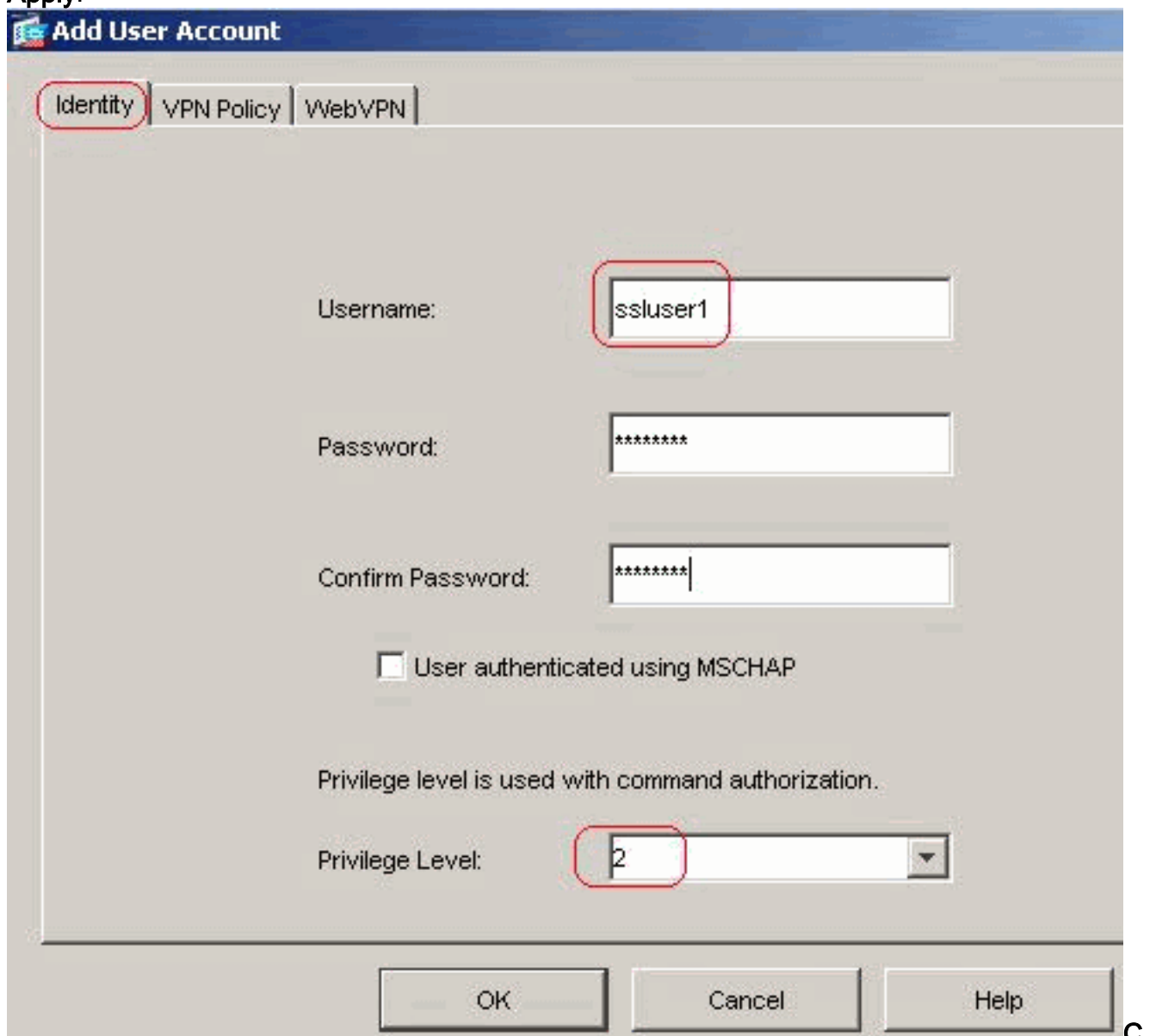
At the bottom of the window, there are three buttons: 'OK', 'Cancel', and 'Help'.

Haga clic en OK y en Apply.



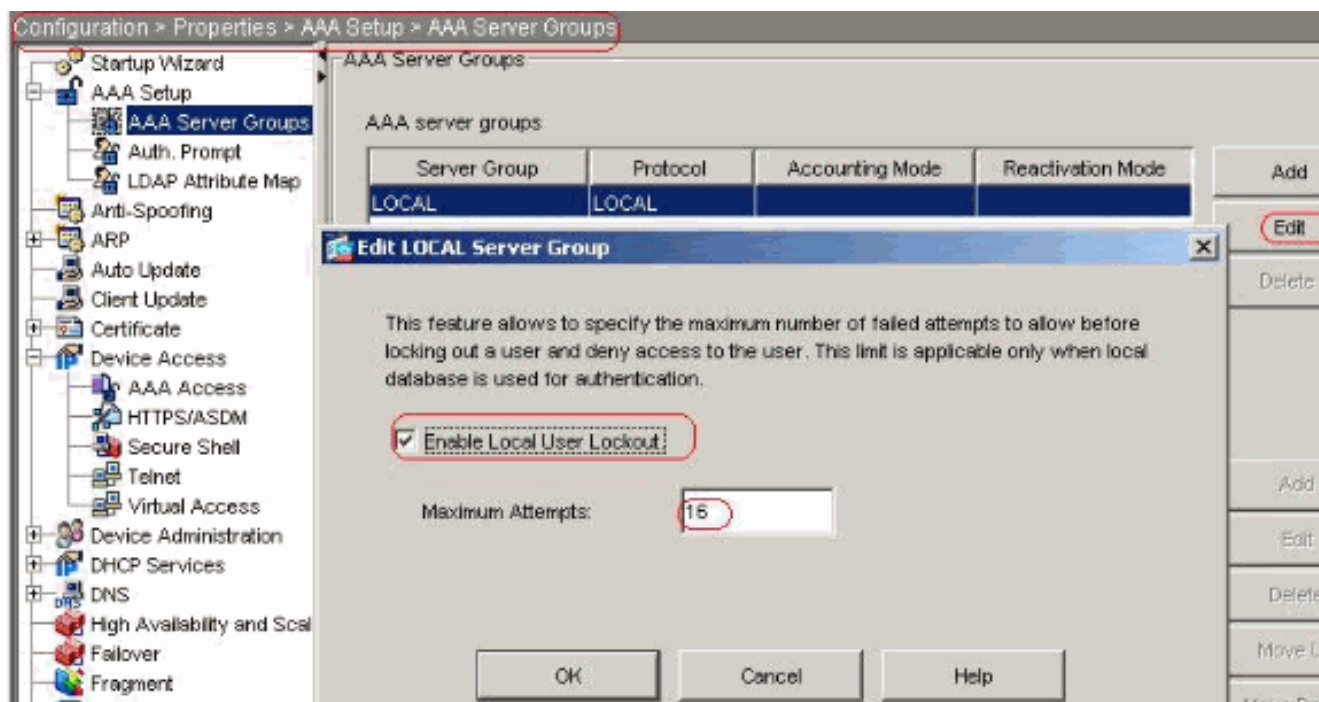
Configuración CLI Equivalente:

5. Elija **Configuration > VPN > General > Users > Add** para crear una nueva cuenta de usuario **ssluser1**. Haga clic en **OK** y en **Apply**.



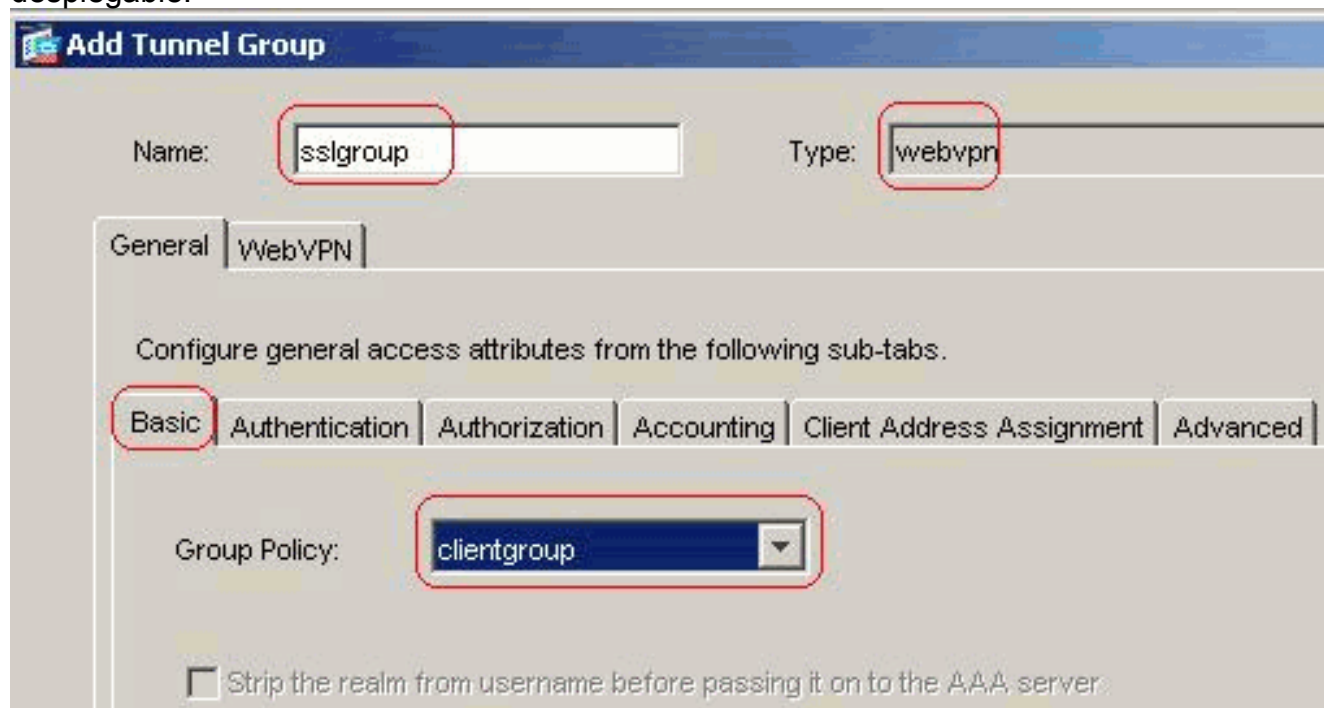
Configuración CLI Equivalente:

6. Elija **Configuration > Properties > AAA Setup > AAA Servers Groups > Edit** para modificar el grupo de servidores predeterminado **LOCAL** y elija la casilla de verificación **Enable Local User Lockout** con el valor máximo de intentos como **16**.



Configuración CLI Equivalente:

- Configure el Grupo de Túnel. Elija Configuration > VPN > General > Tunnel Group > Add (WebVPN access) para crear un nuevo grupo de túnel `sslgroup`. En la ficha General > Básica, elija la Directiva de grupo como grupo de clientes de la lista desplegable.



En General > ficha Client Address Assignment, en Address Pools, haga clic en Add >> para asignar el conjunto de direcciones disponible vpnpool.

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 la ficha **WebVPN > Alias de grupo y URLs**, escriba el nombre de alias en el cuadro de parámetros y haga clic en **Agregar >>** para que aparezca en la lista de nombres de grupo en la página de inicio de sesión.

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:

- Configure el NAT Elija Configuration > NAT > Add > Add Dynamic NAT Rule para el tráfico

que viene de la red interna que se puede traducir con la dirección IP externa

Select	Pool ID	Addresses Pool
<input checked="" type="checkbox"/>	1	172.16.1.5

172.16.1.5.

Haga clic en

Aceptar y haga clic en **Aplicar** en la página principal. **Configuración CLI Equivalente:**

9. 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 de ASA 7.2\(2\) mediante 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 0:05:00
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

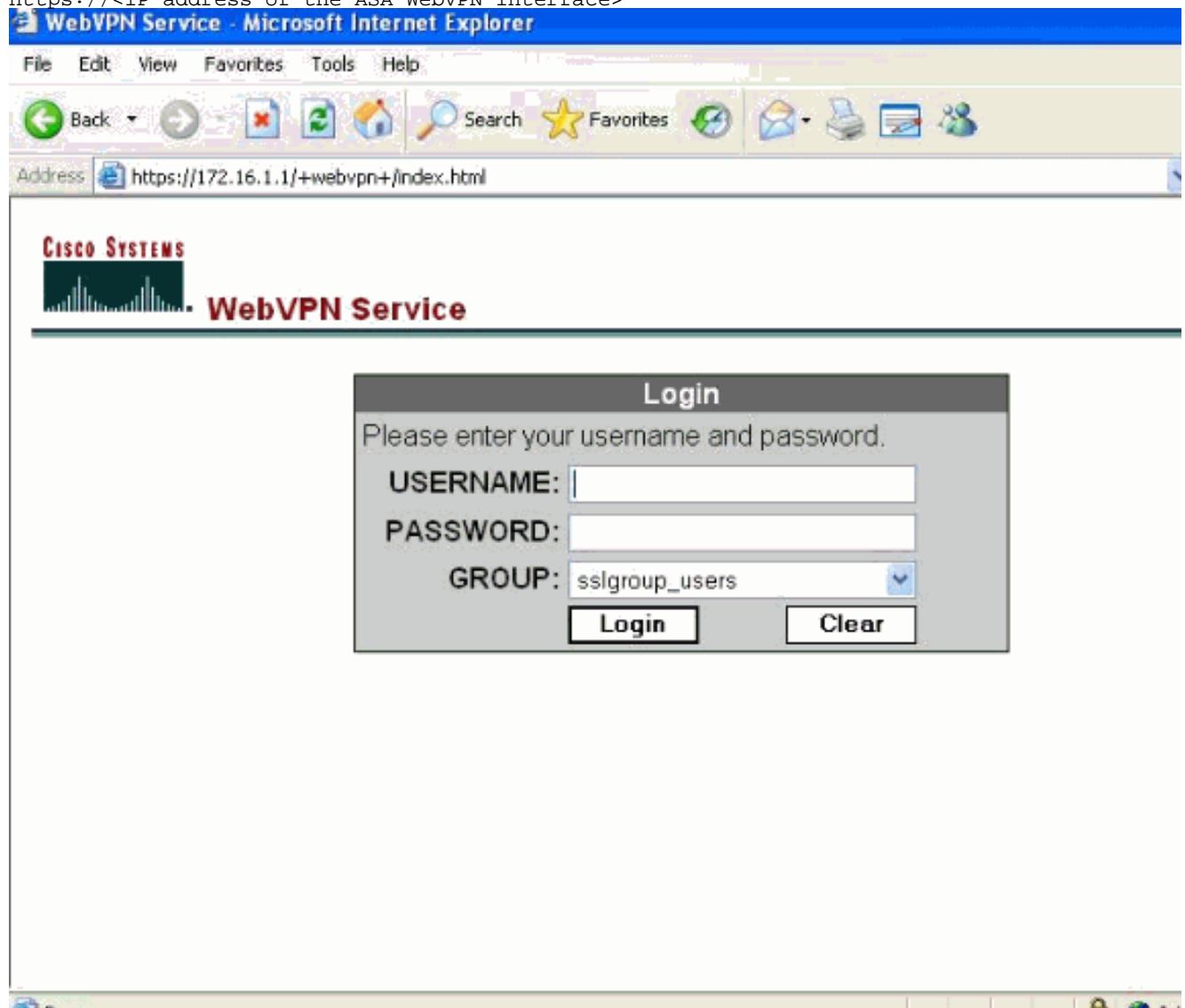
Siga estos pasos para establecer una conexión VPN SSL con el ASA.

1. Escriba la dirección URL o IP de la interfaz WebVPN del ASA en el explorador Web en el formato que se muestra.

https://url

O

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



2. Introduzca su nombre de usuario y contraseña y, a continuación, elija su grupo respectivo en la lista desplegable como se

Login

Please enter your username and password.

USERNAME:

PASSWORD:

GROUP: ▼

muestra.

3. El software ActiveX debe estar instalado en el equipo antes de descargar el



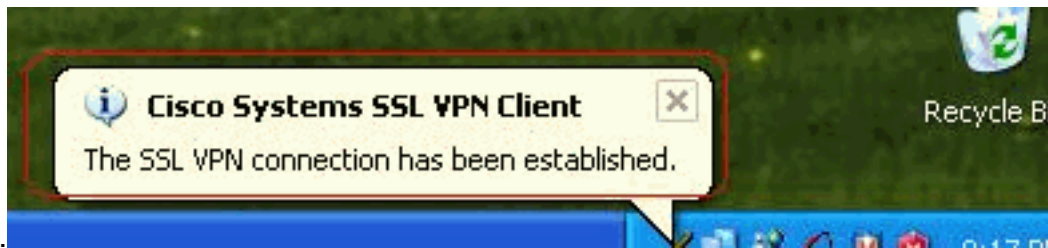
SVC.

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



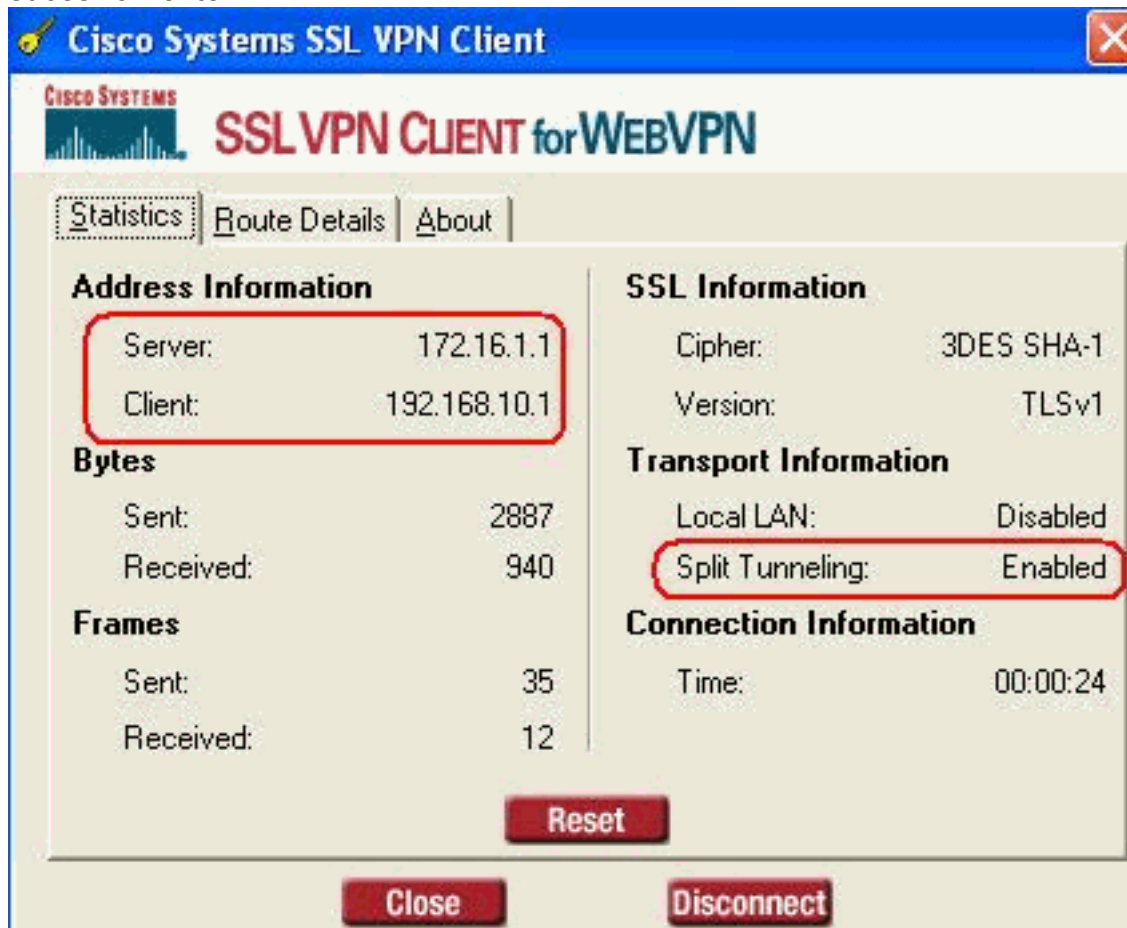
SSL.

5. Puede obtener estas ventanas una vez establecida la



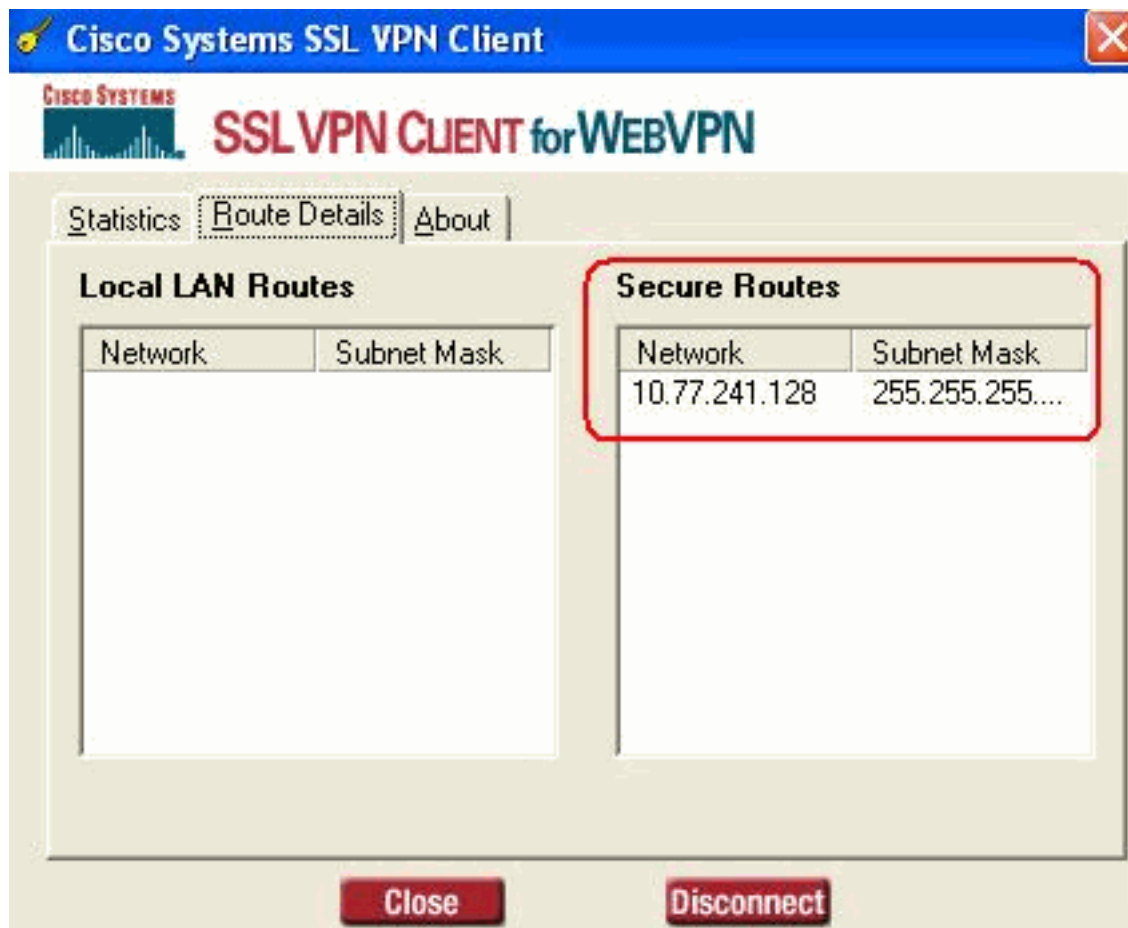
conexión.

- Haga clic en la tecla amarilla que aparece en la barra de tareas del equipo. Aparecen estas ventanas que proporcionan información sobre la conexión SSL. Por ejemplo, **192.168.10.1** es la IP asignada para la dirección IP del cliente y del servidor es 172.16.1.1, la **tunelización dividida está habilitada**, y así sucesivamente.



También

puede verificar la red segura que será cifrada por SSL, la lista de red se descarga de la lista de acceso de túnel dividido configurada en ASA. En este ejemplo, SSL VPN Client asegura el acceso a 10.77.241.128/24 mientras que el resto del tráfico no está cifrado 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

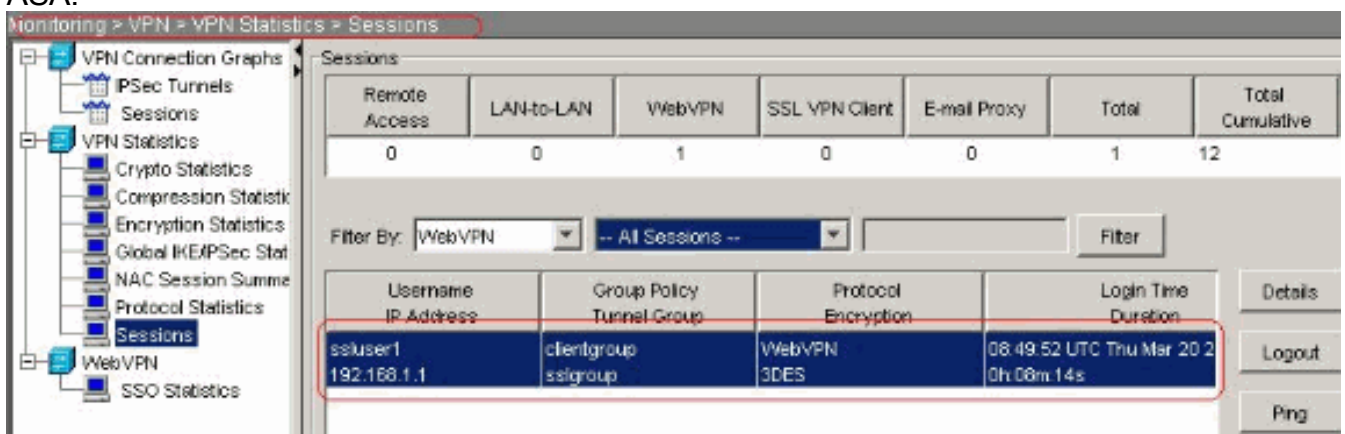
Session Type: SVC

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



The screenshot shows the ASDM interface for monitoring VPN sessions. The left sidebar shows a tree view with 'Sessions' selected under 'VPN Statistics'. The main panel displays a summary table and a detailed session table.

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

Filter By: WebVPN -- All Sessions -- Filter

Username	IP Address	Group Policy	Tunnel Group	Protocol	Encryption	Login Time	Duration	Details
ssluser1	192.168.1.1	clientgroup	sslgroup	WebVPN	3DES	08:49:52 UTC Thu Mar 20 2008	0h:08m:14s	Logout Ping

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
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
INFO: 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.

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, 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
```

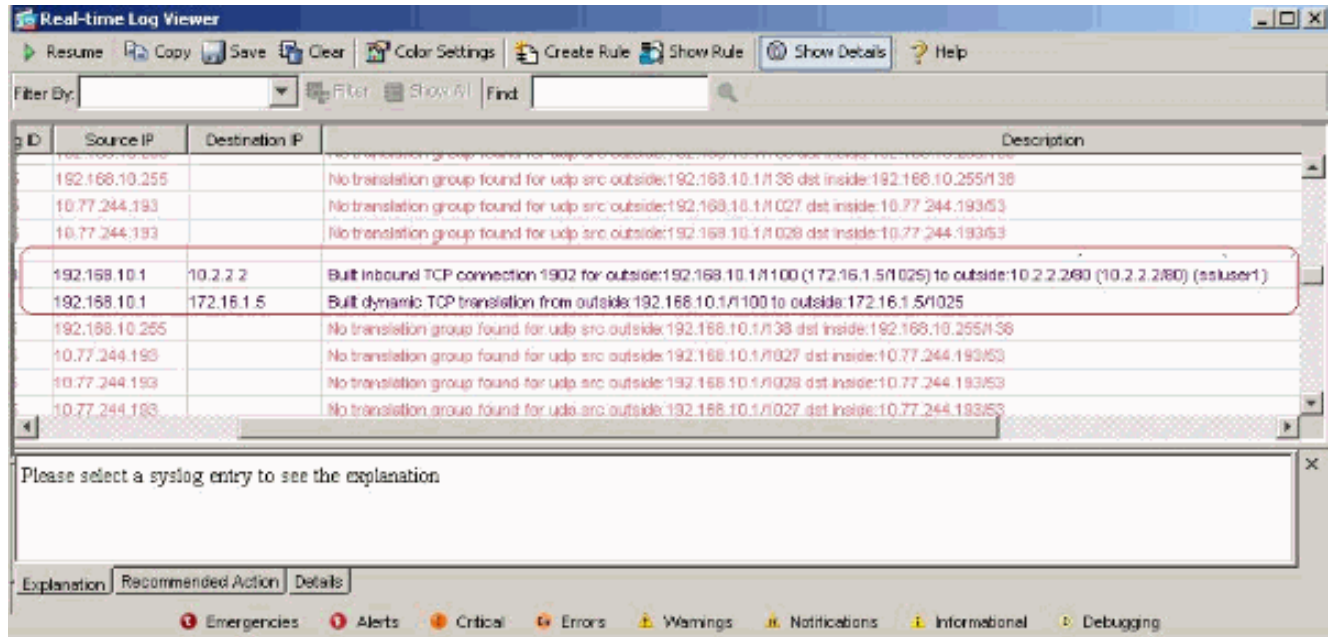
3. **debug webvpn svc <1-255>:** proporciona los eventos webvpn en tiempo real para establecer la sesión.

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

```
ATTR_CISCO_AV_PAIR: got SVC ACL: -1
webvpn_rx_data_tunnel_connect
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 Systems SSL VPN Client 1, 1, 4, 179'
Processing CSTP 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-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: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5BC554D2'
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5BC554D2'
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
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
CSTP state = CONNECTED
```

4. En ASDM, elija **Monitoring > Logging > Real-time Log Viewer > View** para ver los eventos en tiempo real. Este ejemplo muestra información sobre la sesión entre el SVC 192.168.10.1 y el Webserver 10.2.2.2 en Internet a través de ASA 172.16.1.5.



[Información Relacionada](#)

- [Soporte de producto de Cisco 5500 Series Adaptive Security Appliance](#)
- [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](#)