

ASA 7.2(2): (SVC) del cliente VPN SSL para el Internet pública VPN en un ejemplo de configuración del palillo

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones ASA 7.2\(2\) usando el ASDM 5.2\(2\)](#)

[Configuración CLI ASA 7.2\(2\)](#)

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

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo configurar Adaptive Security Appliance (ASA) 7.2.2 para realizar SSL VPN en un solo sentido. Esta configuración se aplica a un caso específico en el que ASA no permite tunelización dividida y los usuarios se conectan directamente al ASA antes de que se les permita entrar a Internet.

Note: En la Versión de ASA 7.2.2, la palabra clave de la intra-*interfaz del* comando configuration mode del **permiso del trafico de seguridad igual** permite que todo el tráfico ingrese y salga la misma interfaz (no apenas tráfico IPSec).

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El dispositivo de seguridad del concentrador ASA necesita funcionar con la versión 7.2.2
- (SVC) 1.x del Cliente Cisco SSL VPN**Note:** 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 en el ASA. SVC 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 del comando line configuration del dispositivo del Cisco Security, versión 7.2](#) para más información.

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
- PC que ejecuta Windows 2000 Professional o Windows XP
- 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 el usuario satisface el login y la autenticación, y el dispositivo de seguridad identifica al usuario como requerir SVC, el dispositivo de seguridad descarga SVC a la computadora remota. Si el dispositivo de seguridad identifica al usuario como teniendo la opción para utilizar SVC, el dispositivo de seguridad descarga SVC a la computadora remota mientras que presenta un link en la pantalla del usuario para saltar la instalación de SVC.

Después de descargar, el SVC instala y se configura, y después el SVC permanece o se desinstala (dependiendo de la configuración) de la computadora remota cuando la conexión termina.

Configurar

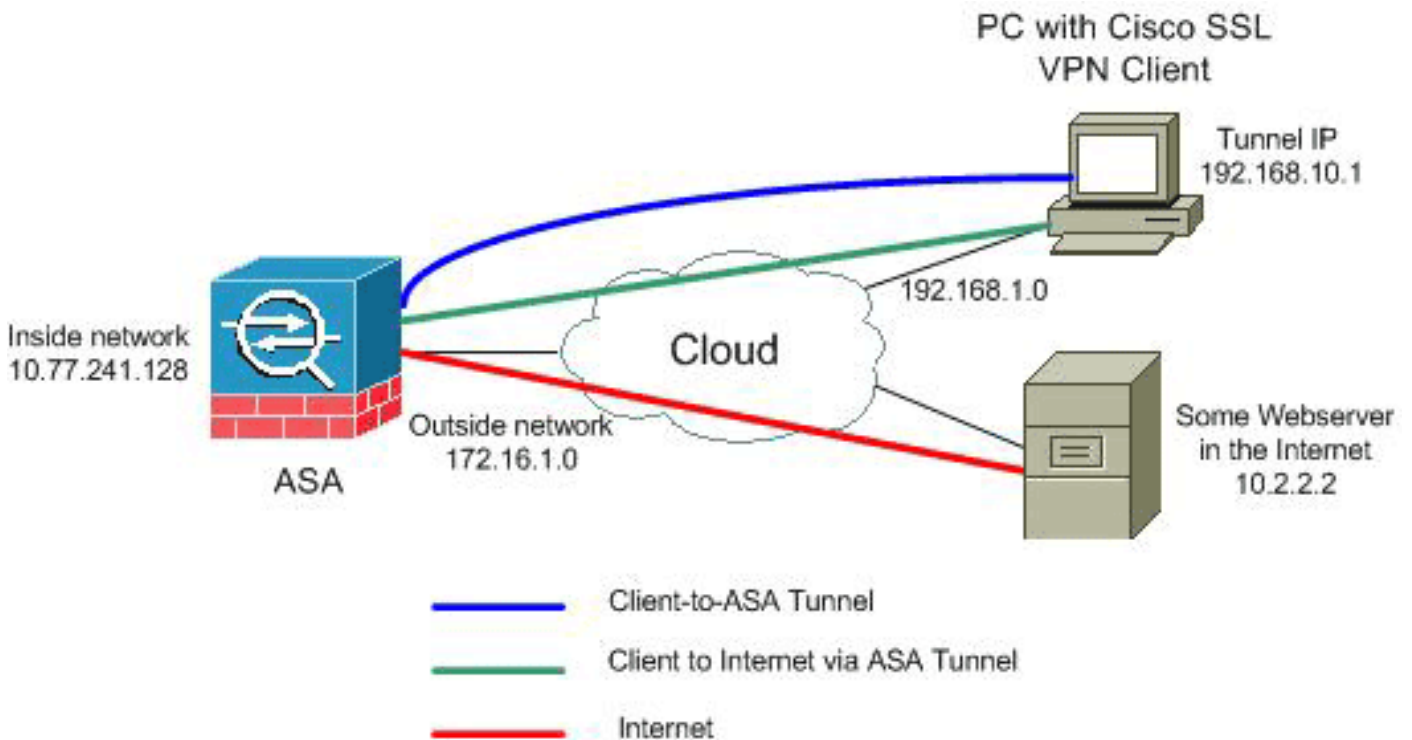
En esta sección encontrará la información para configurar las funciones descritas en este

documento.

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

[Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



Note: 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 7.2\(2\) usando el ASDM 5.2\(2\)](#)

Este documento asume las configuraciones básicas, tales como configuración de la interfaz, es hecho ya y de trabajo correctamente.

Note: Consulte [Cómo Permitir el Acceso HTTPS para el ASDM](#) para que el ASA sea configurado por el ASDM.

Note: 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.

Complete estos pasos para configurar el SSL VPN en un palillo en el ASA:

1. Elija el **Configuration (Configuración) > Interfaces (Interfaces)**, y marcan el **tráfico del habilitar entre dos o más host conectados con el mismo rectángulo de comprobaciones de interfaz** para permitir que el tráfico SSL VPN ingrese y salga lo mismo interconecte.
2. Haga clic en Apply


(Aplicar).

Configuration > Interfaces

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask
Ethernet0/0	inside	Yes	100	10.77.241.142	255.255.255.192
Ethernet0/1	outside	Yes	0	172.16.1.1	255.255.255.0
Ethernet0/2		No			
Ethernet0/3		No			
Management0/0		No			

Please wait...

Please wait while ASDM is delivering the command(s) to the device...



Parsing running configuration...

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

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

Apply Reset

Note: Aquí está el comando de configuración CLI equivalente:

3. Elija la configuración > el VPN > la administración de IP Address > a las agrupaciones IP > Add para crear un pool de la dirección IP nombrado

Add IP Pool

Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

OK Cancel Help

vpnpool.

4. Haga clic en Apply (Aplicar). **Note:** Aquí está el comando de configuración CLI equivalente:
5. WebVPN del permiso: Elija la **configuración > el VPN > el WebVPN > el acceso del WebVPN**, y seleccione la interfaz exterior. 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 permitir que los usuarios elijan a sus grupos correspondientes de la página de registro.

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

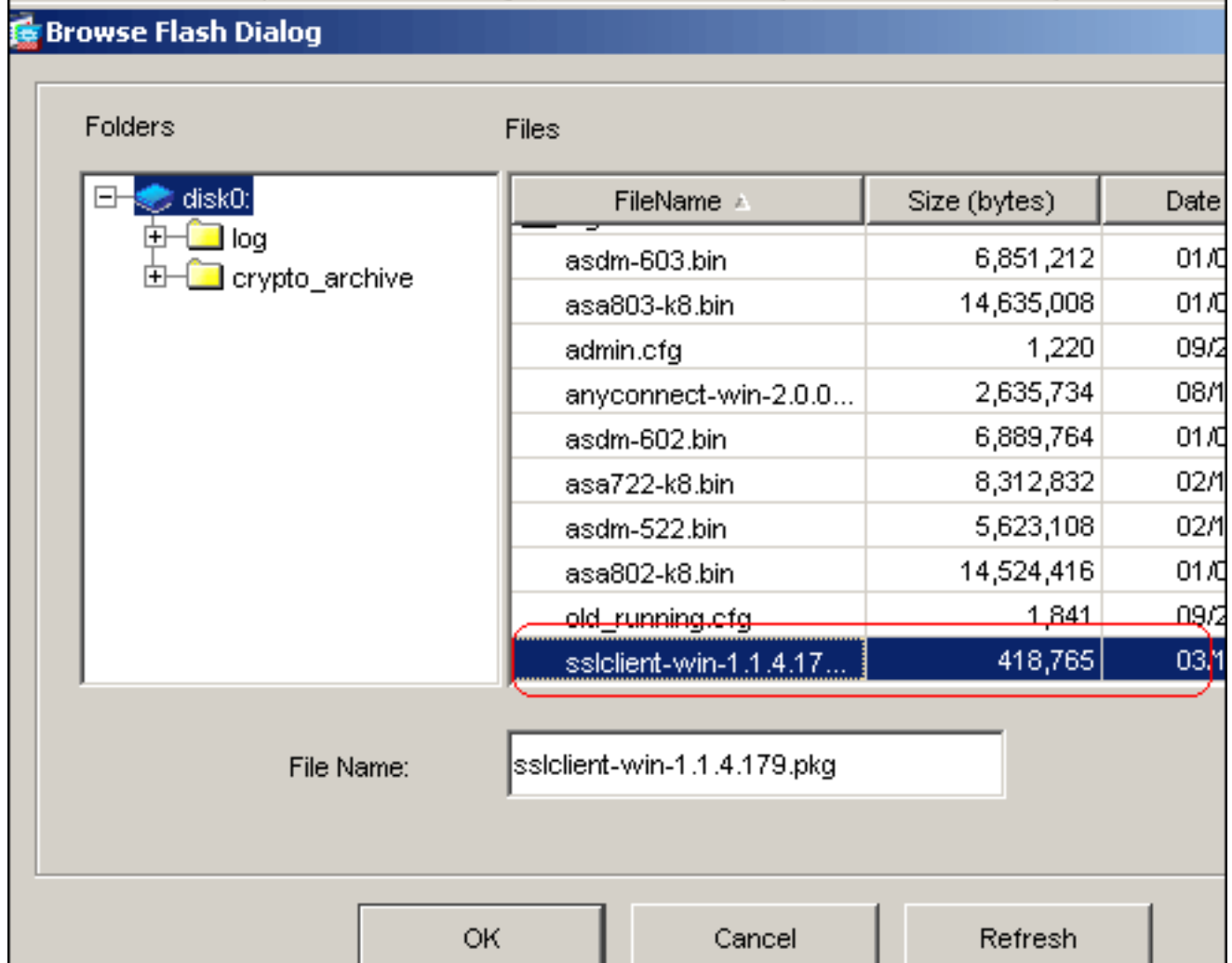
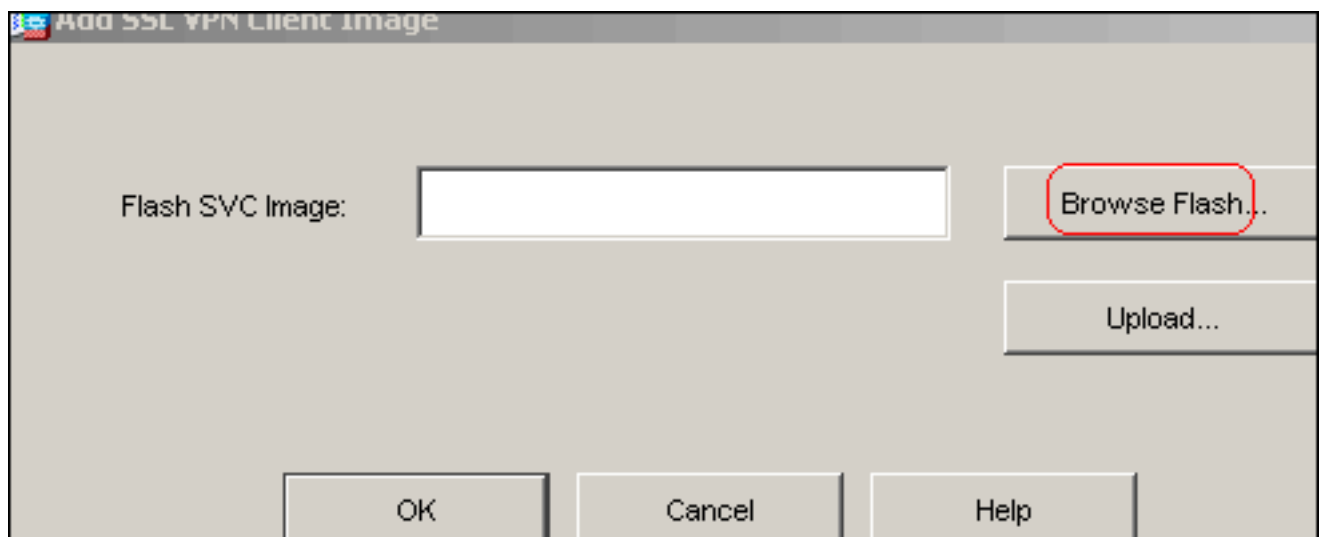
Max. Sessions Limit:

WebVPN Memory Size: % of total physical memory

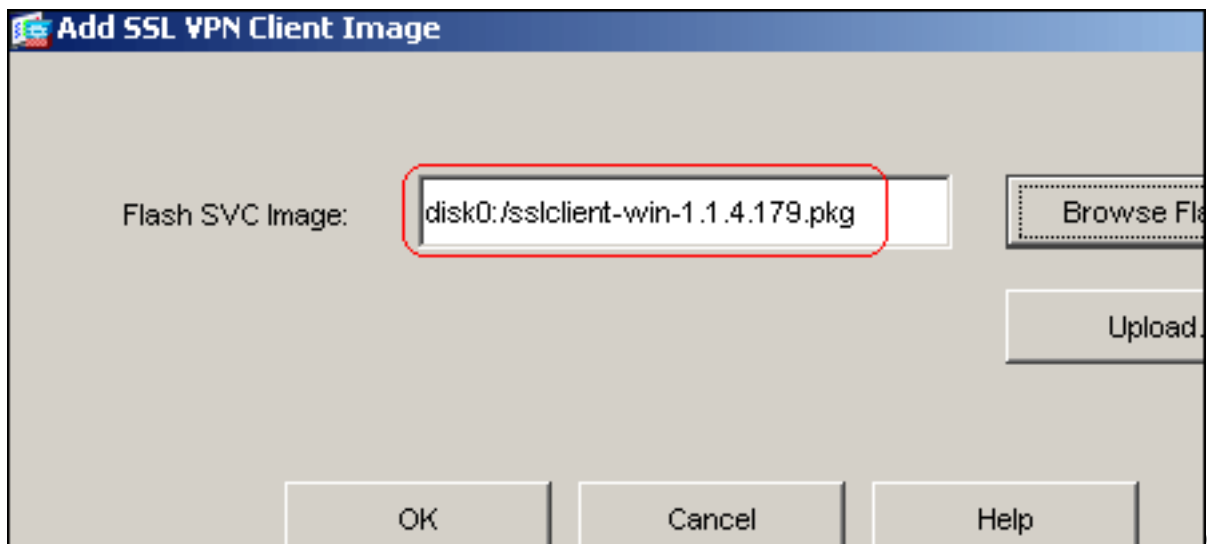
Enable Tunnel Group Drop-down List on WebVPN Login Page

Apply Reset

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

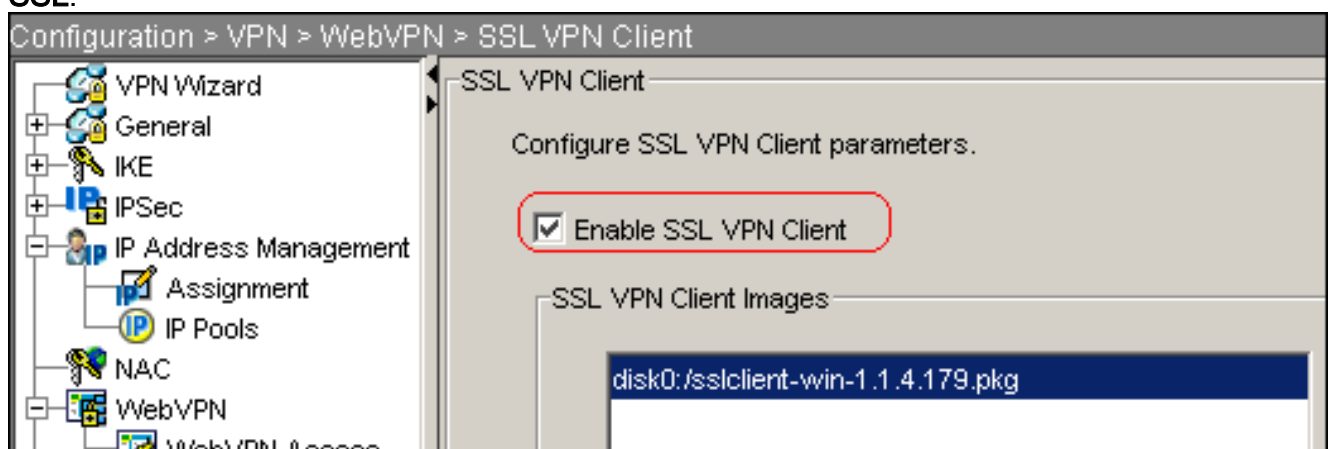


Click



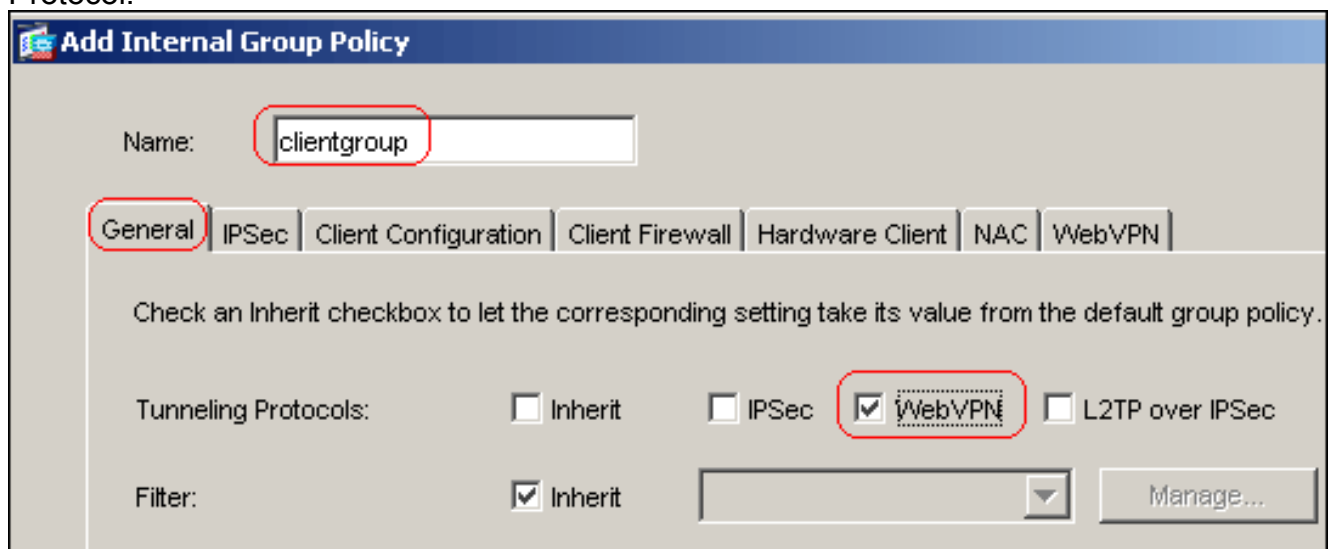
OK. Clic

k OK. Casilla de verificación del **cliente VPN del teclado SSL**.



Note: Aquí están los comandos de configuración CLI equivalentes:

6. Configure la directiva del grupo: Elija la **configuración > el VPN > la directiva del general > del grupo > Add (Internal group policy (política grupal interna))** para crear una directiva interna del grupo nombrada *clientgroup*. Haga clic la **ficha general**, y seleccione la casilla de verificación del **WebVPN** para habilitar el WebVPN como Tunneling Protocol.



Haga clic la lengüeta de la **configuración del cliente**, y después haga clic la lengüeta de **general Client Parameters**. Elija el **túnel todas las redes** de la lista desplegable de la directiva del túnel dividido para hacer que todos los paquetes viajan de la PC remota a través de un

túnel
seguro.

Add Internal Group Policy

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

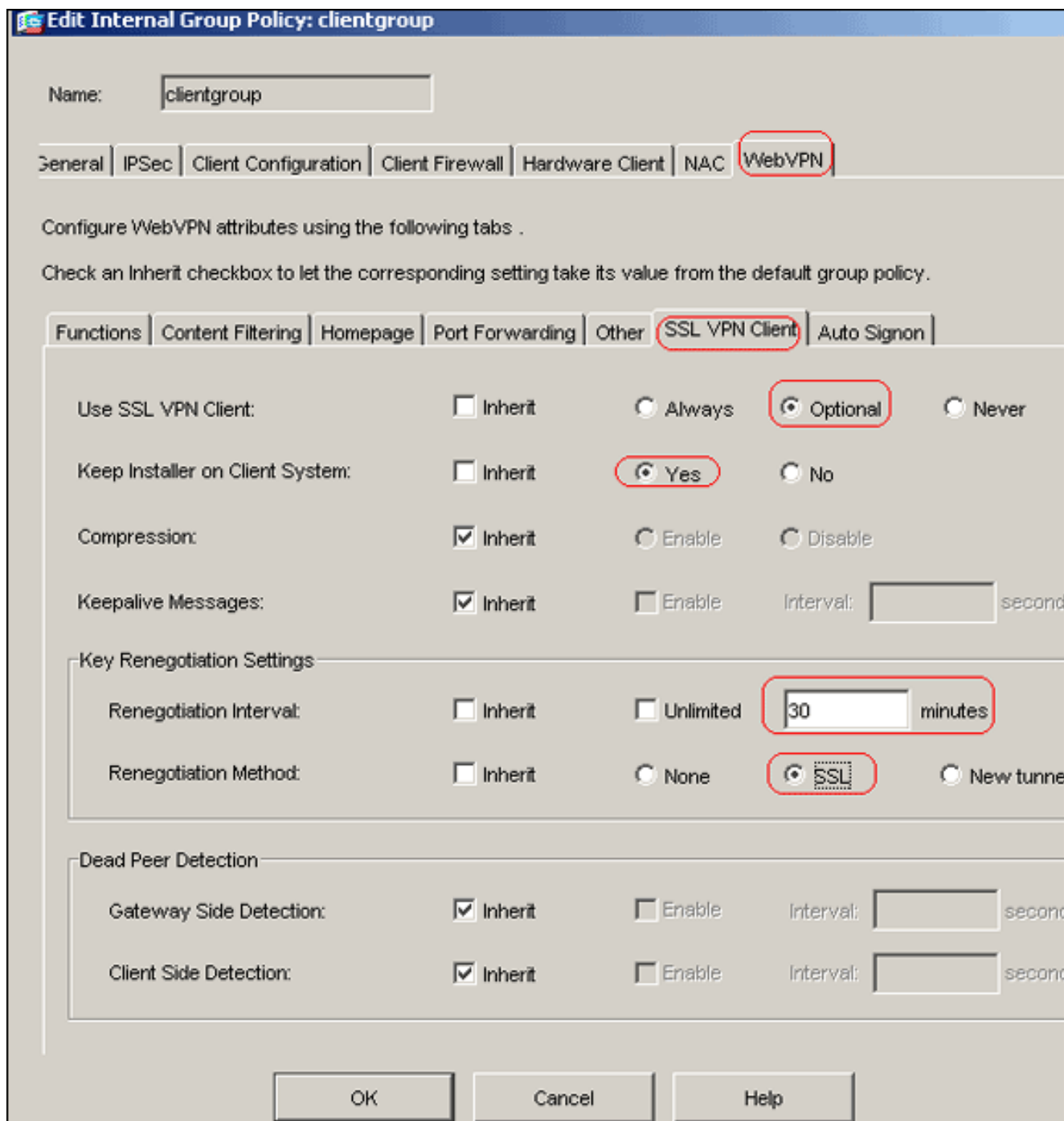
Split Tunnel DNS Names (space delimited): Inherit

Split Tunnel Policy: Inherit

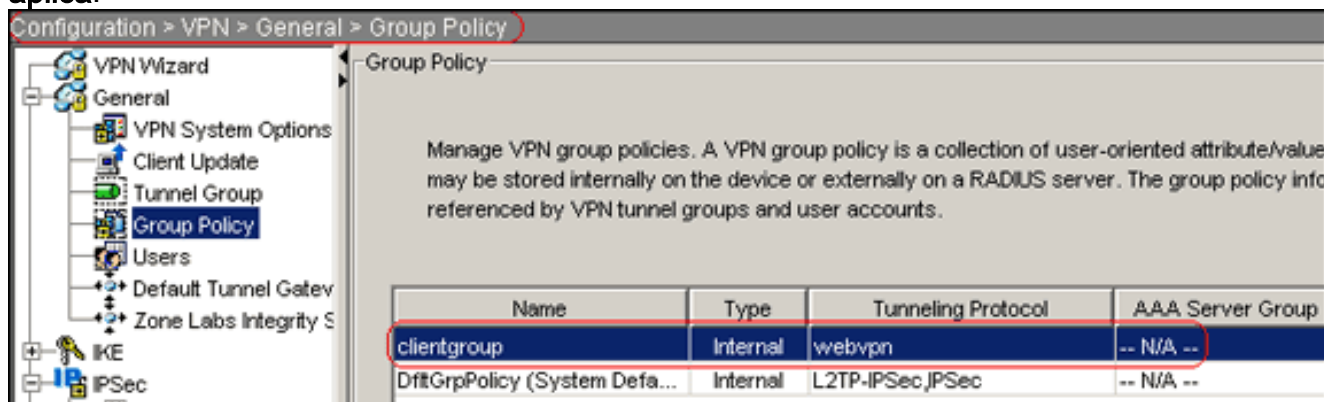
Split Tunnel Network List: Inherit

Address pools: Inherit

Haga clic la lengüeta del **WebVPN > del cliente SSLVPN**, y elija estas opciones: 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 independientemente de si descargar SVC. El siempre bien escogido se asegura de que SVC esté descargado a la estación de trabajo remota durante cada conexión VPN SSL. Para el instalador de la custodia en la opción del sistema del cliente, desmarque la casilla de verificación de la **herencia**, y haga clic el **botón Yes Radio Button**. Esta opción permite que el software de 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. **Note:** 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**. **Note:** La renegociación puede utilizar el actual túnel SSL o un nuevo túnel creado específicamente para la renegociación. Sus atributos del cliente VPN SSL se deben configurar tal y como se muestra en de esta imagen:



El Haga Click en OK, y entonces hace clic se aplica.



Note: Aquí están los comandos de configuración CLI equivalentes:

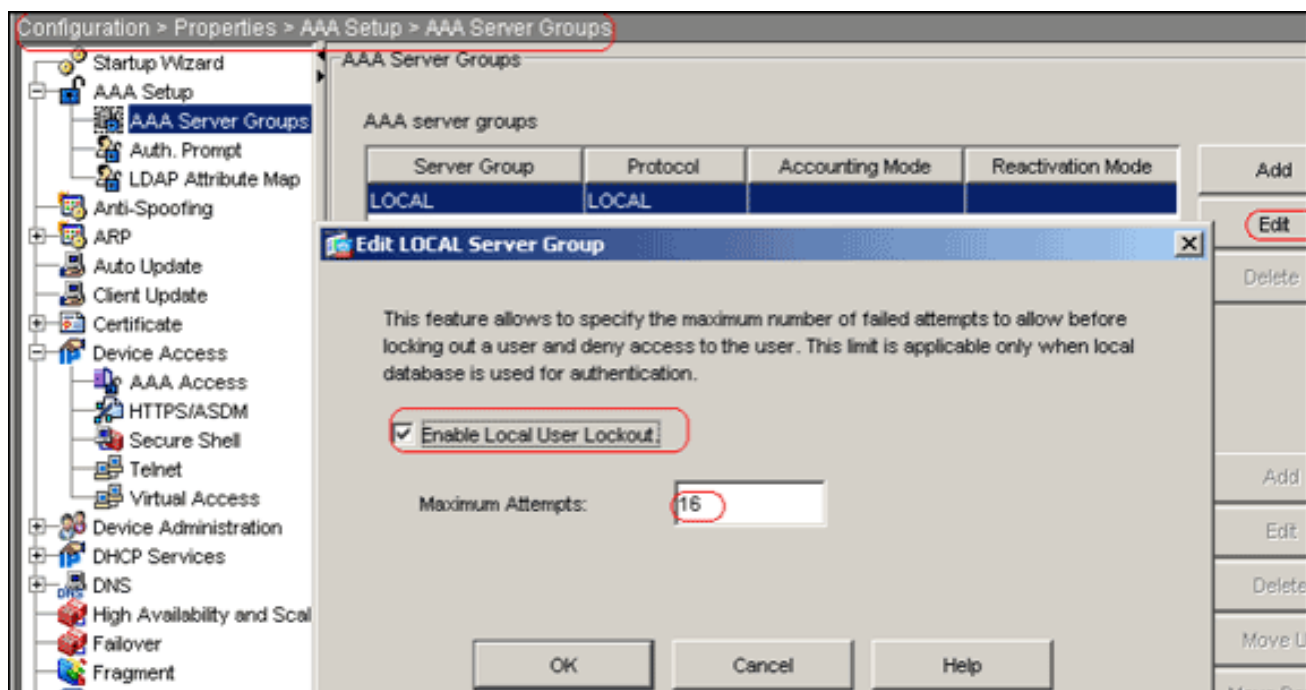
7. Elija la configuración > el VPN > al general > Users > Add para crear una cuenta de usuario nuevo *ssluser1*.

8. El Haga Click en OK, y entonces hace clic **se aplica**.

The image shows a screenshot of the 'Add User Account' dialog box. The 'Identity' tab is selected and highlighted with a red circle. The 'Username' field contains 'ssluser1' and is also highlighted with a red circle. The 'Password' and 'Confirm Password' fields contain '*****'. There is an unchecked checkbox for 'User authenticated using MSCHAP'. The 'Privilege Level' dropdown menu is set to '2' and is highlighted with a red circle. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

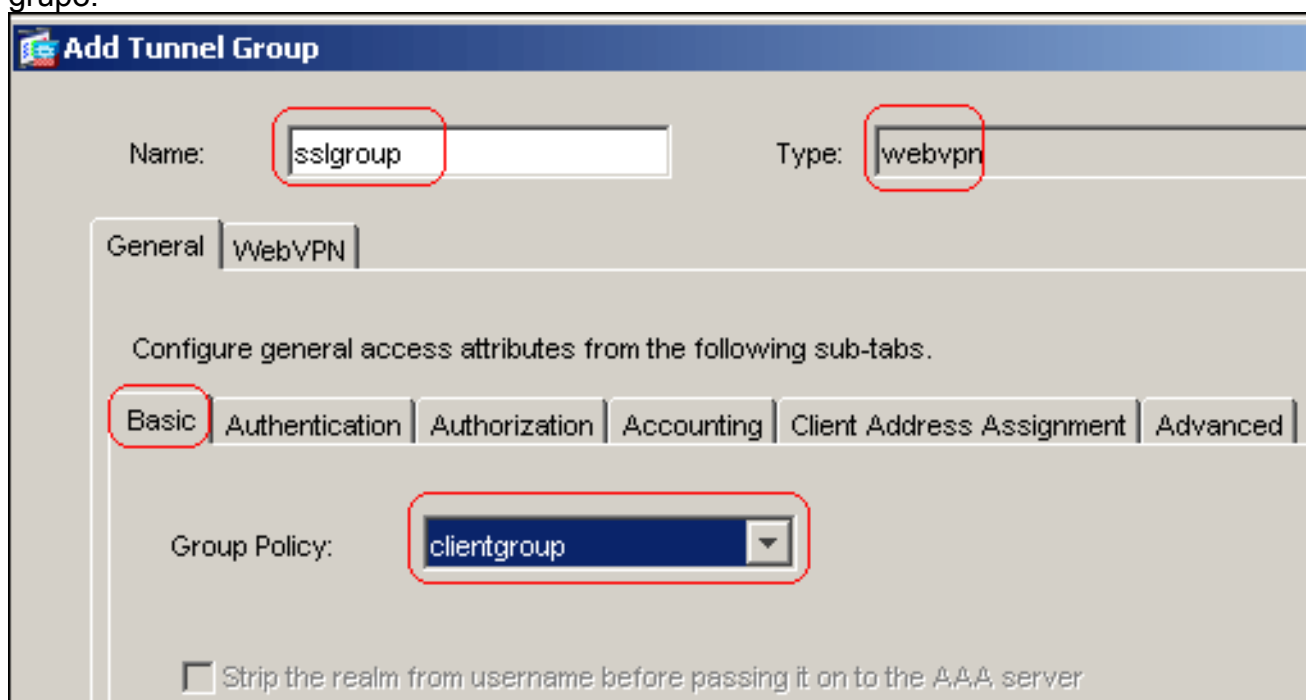
ote: Aquí está el comando CLI equivalente:

9. Elija la **configuración > las propiedades >AAA ponen >AAA los grupos de servidores > editan**.
10. Seleccione el *LOCAL* predeterminado del grupo de servidores, y el tecleo **edita**.
11. En el cuadro de diálogo del grupo de servidor local del editar, haga clic la casilla de verificación del **cierre del usuario local del habilitar**, y ingrese 16 en el cuadro de texto máximo de las tentativas.
12. Click
OK.



Note: Aquí está el comando CLI equivalente:

- Configure al grupo de túnel: Elija la **configuración > el VPN > el general > al grupo de túnel > Add (acceso del WebVPN)** para crear a un nuevo grupo de túnel nombrado *sslgrou*. Haga clic la **ficha general**, y después haga clic la lengüeta **básica**. Elija el **clientgroup** de la lista desplegable de la directiva del grupo.



Haga clic la lengüeta de la **asignación de dirección cliente**, y después haga clic **agregan** 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

Haga clic la lengüeta del **WebVPN**, y después haga clic la lengüeta de los **alias y URL del grupo**. Teclee el nombre de alias en el cuadro del parámetro, y el tecleo **agrega** para agregarlo a 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
sslgroun_users	enable

El Haga Click en OK, y entonces hace clic **se aplica**. **Note:** Aquí están los comandos de configuración CLI equivalentes:

- Configuración NAT: Elija la **configuración > la regla dinámica NAT > Add > Add NAT** para

permitir el tráfico que viene de la red interna que se traducirá con el uso del IP Address

Add Dynamic NAT Rule

Real Address

Interface: inside

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Dynamic Translation

Interface: outside

+ Add Edit Delete

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

NAT Options...

OK Cancel Help

externo 172.16.1.5.

Click

OK. Elija la configuración > la regla dinámica NAT > Add > Add NAT para permitir el tráfico que viene de la red externa 192.168.10.0 que se traducirá con el uso del IP Address

Add Dynamic NAT Rule

Real Address

Interface:

IP Address: ...

Netmask:

Dynamic Translation

Interface:

+ Add Edit Delete

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

NAT Options...

OK Cancel Help

externo 172.16.1.5.
OK.

Click

No	Type	Real		Translated	
		Source	Destination	Interface	Address
inside					
1	Dynamic	any	any	outside	172.16.1.5
outside					
1	Dynamic	192.168.10.0/24	any	outside	172.16.1.5

Haga clic en Apply (Aplicar). **Note:** Aquí están los comandos de configuración CLI equivalentes:

Configuración CLI ASA 7.2(2)

Cisco ASA 7.2(2)

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjYt7RRXU24 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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter
!--- and exit the same interface. access-list 100
extended permit icmp any any 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) 1 0.0.0.0 0.0.0.0

!--- The NAT statement to define what to encrypt !---
(the addresses from vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

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 tunnelall

!--- Encrypt all the traffic coming from the SSL VPN
Clients. 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, 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. 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

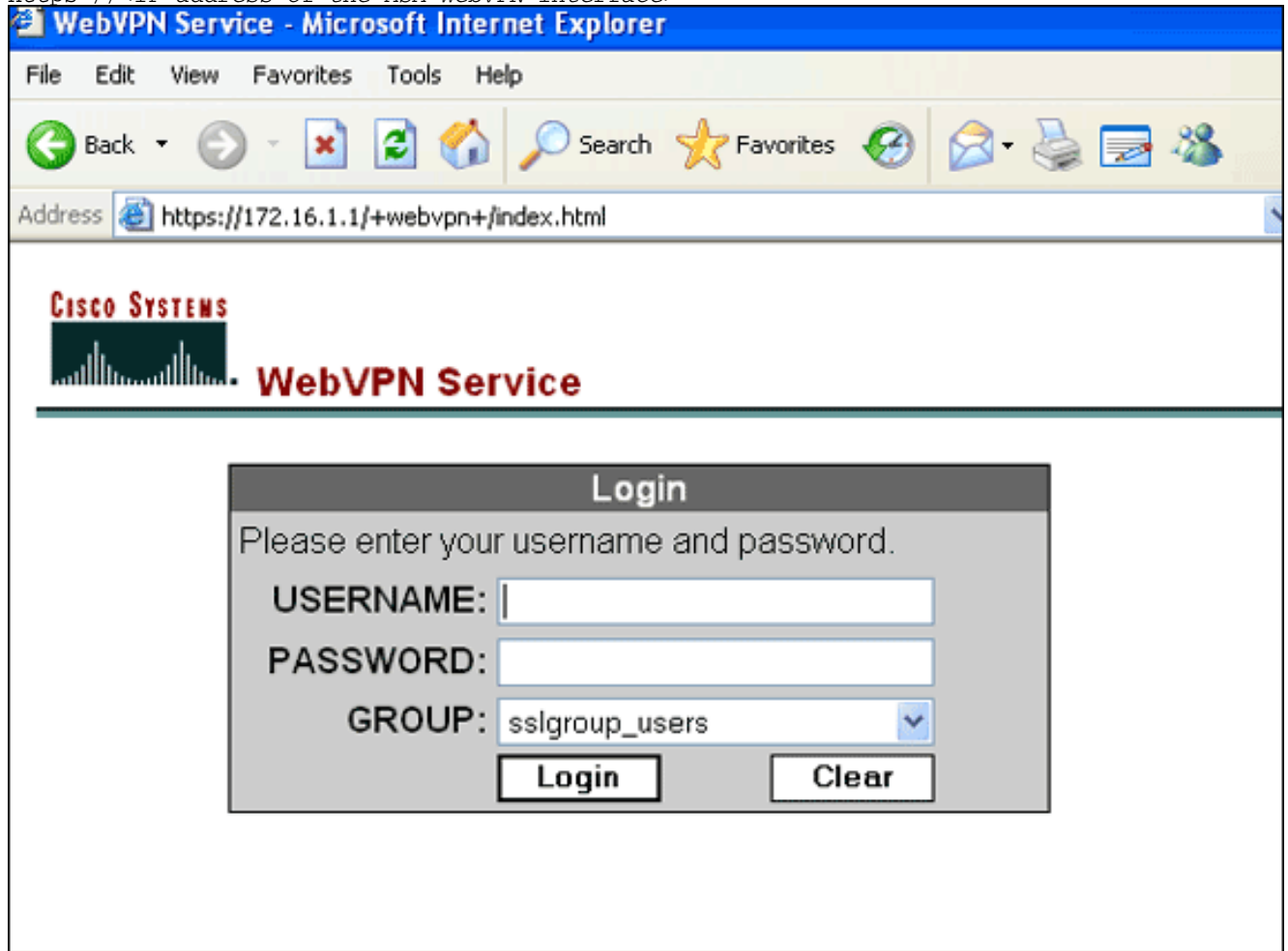
!--- Enable the display of the tunnel-group list on the
WebVPN Login page. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#
```

Establezca la Conexión VPN SSL con el SVC

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

1. Teclee adentro el campo de dirección de su buscador Web el URL o la dirección IP para la interfaz del WebVPN del ASA. Por ejemplo:

<https://<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 desplegable del

Login

Please enter your username and password.

USERNAME:

PASSWORD:

GROUP: ▼

grupo.

Note: El

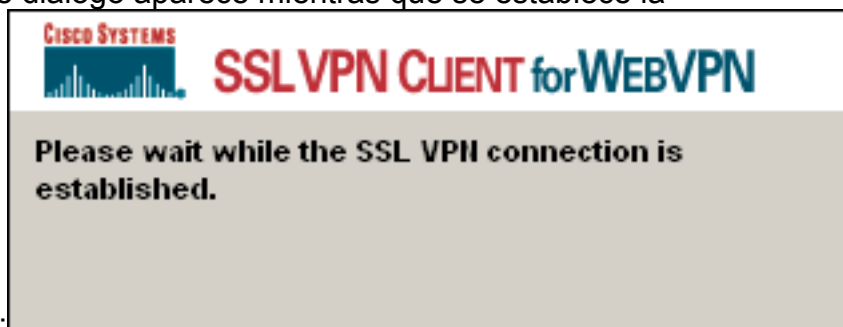
software de ActiveX se debe instalar en su ordenador antes de que usted descargue al cliente VPN



SSL.

Este

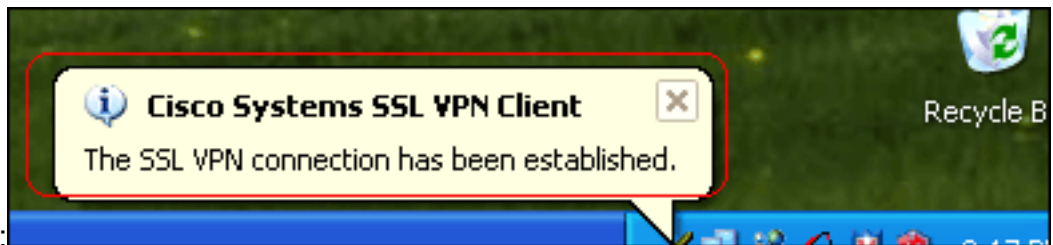
cuadro de diálogo aparece mientras que se establece la



conexión:

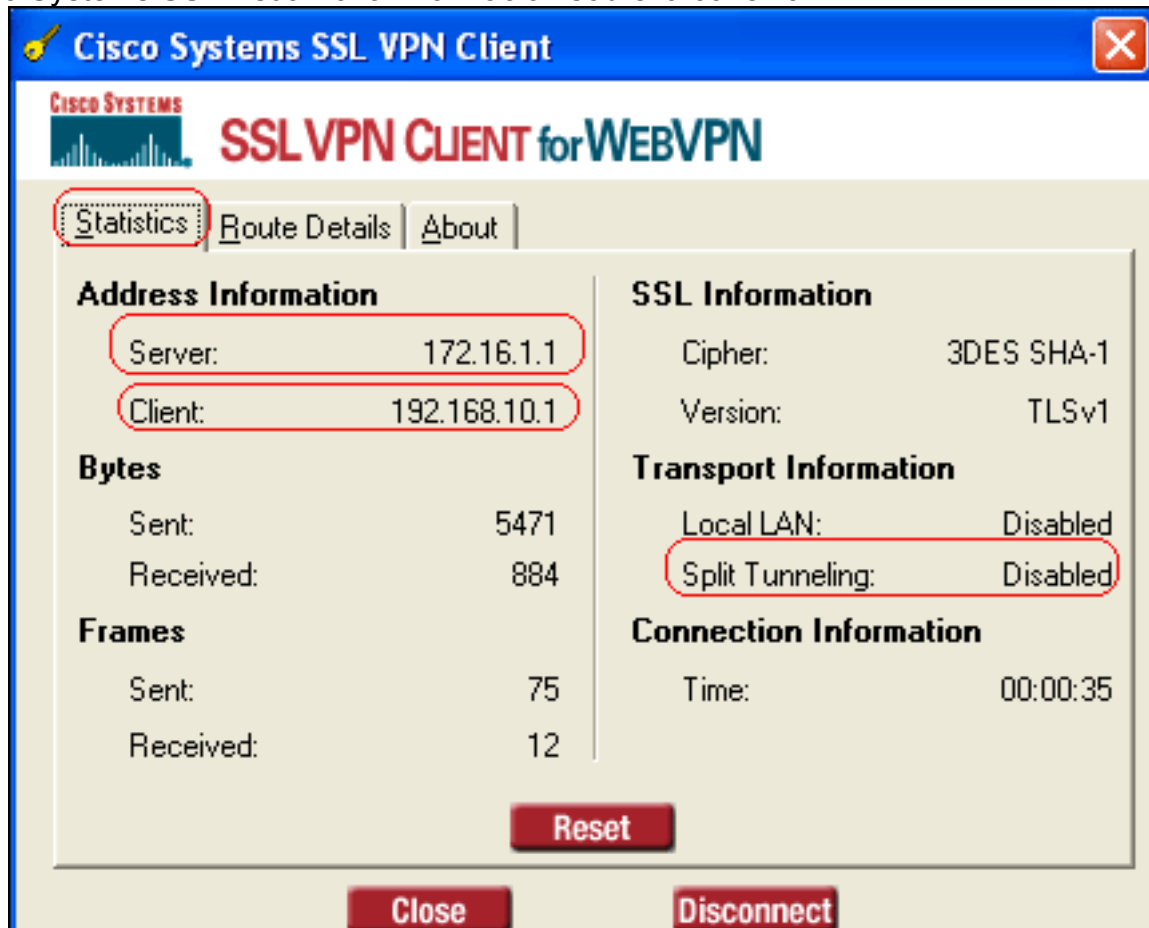
Este mensaje aparece

una vez que se establece la

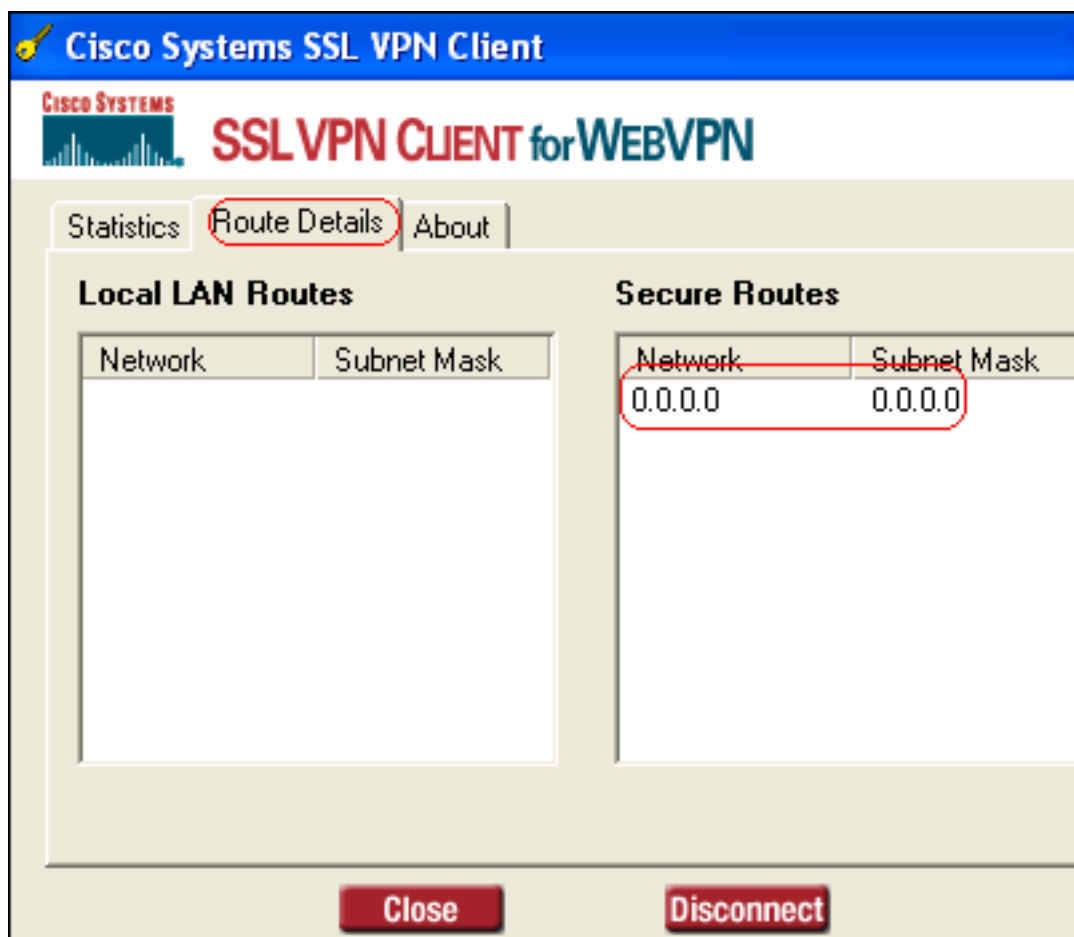


conexión:

3. Una vez que se establece la conexión, haga doble clic el icono dominante amarillo que aparece en la barra de tareas de su ordenador. El cuadro de diálogo del cliente VPN de Cisco Systems SSL visualiza la información sobre la conexión



SSL.



Verificación

Utilize esta sección para confirmar que su configuración funcione 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 ver la información sobre las sesiones WebVPN actuales en el ASA.

The screenshot shows the ASDM interface for monitoring VPN statistics. The left sidebar shows the navigation tree with 'Sessions' selected under 'VPN Statistics'. The main area displays a summary table and a detailed table of sessions.

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	Group Policy	Protocol	Login Time	Details
IP Address	Tunnel Group	Encryption	Duration	
ssluser1	clientgroup	WebVPN	08:48:52 UTC Thu Mar 20 2008	Logout
192.168.1.1	sslgroup	3DES	0h:08m:14s	Ping

Troubleshooting

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

- <username> del nombre del cierre de sesión de VPN-sessiondb — Permite que usted termine

una sesión a la sesión de VPN SSL para el nombre de usuario especificado.

```
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
```

Semejantemente, usted puede utilizar el **cierre de sesión svc de VPN-sessiondb** del comando para terminar todas las sesiones de SVC. **Note:** 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
```

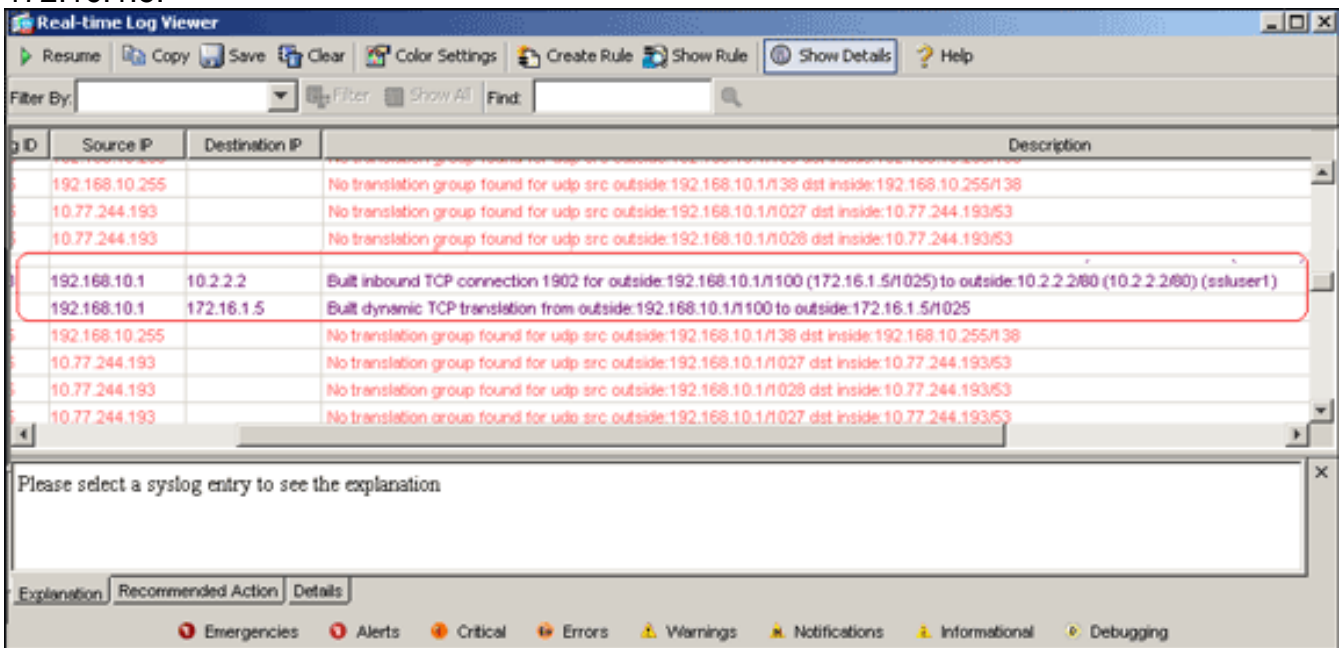
- **Webvpn svc <1-255> del debug** — Proporciona los eventos en tiempo real del WebVPN para establecer la sesión.

```
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@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2'
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
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
```

- En el ASDM, elija la **supervisión > el registro > Log Viewer > visión en tiempo real** para ver los eventos en tiempo real. Estos ejemplos muestran la información de la sesión entre SVC 192.168.10.1 y web server 10.2.2.2 en Internet vía ASA 172.16.1.5.



Información Relacionada

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