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 1.1.4.179Nota: 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 saltear 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 <u>direcciones RFC 1918</u> 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:

- El documento asume que la configuración básica, como la configuración de la interfaz, etc., ya está hecha y funciona correctamente. Nota: Consulte <u>Permiso de Acceso HTTPS para</u> <u>ASDM</u> 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 <u>ASDM y WebVPN Habilitados en la Misma Interfaz de ASA para obtener más</u> <u>información.</u>
- 2. Elija Configuration > VPN > IP Address Management > IP Pools para crear un pool de direcciones IP: vpnpool para clientes

Name:	vpnpool	
Starting IP Address:	192.168.10.1	
Ending IP Address:	192.168.10.254	
Subnet Mask:	255.255.255.0	-

Haga clic en Apply (Aplicar).

3. Habilite WebVPNElija Configuration > VPN > WebVPN > WebVPN Access y resulte 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	I > WebVPN Access	
VPN Wizard	-WebVPN Access	
🕀 🚰 General		
Ē-∱ KE	Configure access parameters for WebVPN.	
🔁 📲 IPSec		
E - B P Address Management		
Assignment		
P Pools	Interface WebVPN Enabled	(Enskle)
- INAC	incida kin	
P-LE WebVPN		
WebVPN Access		Disable
Proxies		
APCF		
Auto Signon		
Cache		
Content Rewrite		
Java Trustpoint	Port Number 443	
Proxy Bypass		
Derd Farmendern	Default Me Timeout: 1800 seconde	
Port Forwarding		
Veopage Customiza	May Saccine Lint 2	
- Focosting		
- SSL VPN Client	MishVPNI Memory Sizer 50	
- SSO Servers	webver wenter y daze. Do po or total physical menter y	
E-mail Proxy	Finable Tunnel Group Drop-down List on WebVPN Login Page	
1		
	Apply Reset	
Log Constant		

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.

			sh.
		Upload	
ОК	Cancel	Help	
owse Flash Dialog			
Folders	Files		
🖃 🥏 disk0:	FileName 🔺	Size (bytes)	
🕀 🛄 log	asdm-603.bin	6,851,212	ł
the crypto_archive	asa803-k8.bin	14,635,008	
	admin.cfg	1,220	
	anyconnect-win-2.0.0	2,635,734	
	arrycornicol-min-2.0.0		
	asdm-602.bin	6,889,764	
	asdm-602.bin asa722-k8.bin	6,889,764 8,312,832	
	asdm-602.bin asa722-k8.bin asdm-522.bin	6,889,764 8,312,832 5,623,108	
	asdm-602.bin asa722-k8.bin asdm-522.bin asa802-k8.bin	6,889,764 8,312,832 5,623,108 14,524,416	
	asdm-602.bin asa722-k8.bin asdm-522.bin asa802-k8.bin old_running.cfg	6,889,764 8,312,832 5,623,108 14,524,416 1,841	

Click

🎼 P	dd SSL ¥PN Client In	nage			
	Flash SVC Image:	disk0:/sslcliv	ent-win-1.1.4.179.pkg		Browse Fla
					Upload.
OK.		ок	Cancel	Help	Clic

k OK.Haga clic en la casilla de verificación SSL VPN Client.

Configuration > VPN > WebVPI	N > SSL VPN Client	
VPN Wizard General F Sike F Sec F Sec F Sec F Address Management VebVPN VebVPN WebVPN Access	SSL VPN Client Configure SSL VPN Client parameters.	

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

4. Configure la Política de GrupoElija 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.

🚰 Add Internal Group Policy		
Name: Clientgroup		
General IPSec Client Config	guration Client Fi	rewall │ Hardware Client │ NAC │ Web∨PN │
Check an Inherit checkbox t	to let the correspo	nding setting take its value from the d <mark>efault</mark> group policy.
Tunneling Protocols:	🗖 Inherit	□ IPSec 🔽 WebVPN □ L2TP over IPSec
Filter:	🔽 Inherit	Manage

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		
Neme:		
Internet Internet		
General IPSec Client Configuration Client Fir	rewall Hardware Client	NAC WebVPN
	unding and ting take the control	a fuana flaa ala far ili awar na maliar i
check an innent checkbox to let the correspo	riung setting take its valu	e from the default group policy.
General Client Parameters Cisco Client Para	meters Microsoft Client	Parameters
		a sugar a sugar
Banner:	I⊻ Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Cull Trans I Delive	E lukant	
Split Tunnel Policy:		
Split Tunnel Network List:		None Manage
	C	
Address pools		
🔽 Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	Add>>	
2		
OK	Cancel	Help
	0.000	

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

CL Manager	d ACL		
🗣 Add 👻 💕 Edit 🥤	🕽 Delete 🔶 🛧 🤞	- X = 4 -	
🔂 Add ACL	dress	Action	Description
🔂 Add ACE			
🔹 Insert 🐺 Insert After			

Asigne un nombre al ACL y haga clic en

Add 👻 🛒	Edit <u> </u>	✓ %	
No	Address	Action	Description
Add ACL			×

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.

40	Address	Action	Description	
plit-tunnel				
Add ACE				
Action				
Action:	🖌 Permit 💌			
	• · •···			
Host/Netwo	ork			
IP Addres	s: 10.77.241.128			-
	255 255 255 192			-
Netmask:				
Netmask:				
	255 255 255 192			-

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.

撞 Edit Internal Group Policy: clientgroup		
Name: clientgroup		
General IPSec Client Configuration Client Firewa	all Hardware Client	NAC WebVPN
Check an Inherit checkbox to let the corresponding	g setting take its value	e from the default group policy.
General Client Parameters Cisco Client Paramete	rs Microsoft Client F	Parameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🔲 Inherit	Tunnel Network List Below
Split Tunnel Network List:	🗖 Inherit	split-tunnel Manage
Address pools		
🔽 Inherit		
Available Pools	Add>> < <remove< th=""><th>Assigned Pools (up to 6 entries)</th></remove<>	Assigned Pools (up to 6 entries)
		,
ок	Cancel	Help

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, desmargue 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

Name: cl	ientgroup				
General IPSec	Client Configuration C	lient Firewall Hard	ware Client NAC 🧕	Neb/PN	
Configure Web\	/PN attributes using the f	ollowing tabs .			
Check an Inherit	checkbox to let the corr	esponding setting ta	ake its value from the	default group polic	cy.
Functions Co	ontent Filtering Homepa	ge Port Forwarding	g Other SSL VPN	Client Auto Signo	on
Use SSL VF	PN Client:	🗖 Inherit	C Always	• Optional	C Never
Keep Install	er on Client System:	🗖 Inherit	(Yes	C No	
Compressio	n:	🔽 Inherit	C Enable	$oldsymbol{C}$ Disable	
Keepalive M	lessages:	🔽 Inherit	🗖 Enable	Interval:	secon
Key Renego	otiation Settings				
Renegot	iation Interval:	🗌 Inherit	🗌 Unlimited	30	minutes
Renegot	iation Method:	🗖 Inherit	C None	(55L	C New tunne
Dead Peer [Detection				
Gatewa	y Side Detection:	🔽 Inherit	Enable	Interval:	secon
Client Si	de Detection:	🔽 Inherit	🔽 Enable	Interval:	secon

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



Configuración CLI Equivalente:

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

Username:	ssluser1	
Password:	*****	
Confirm Password:	******	
🔲 User authenti	cated using MSCHAP	
Privilege level is used	with command authorization	e.
Privilege Level:	2	•

onfiguración CLI Equivalente:

 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.

Configuration > Properties > A	AA Setup > AAA Server Gro	ups			
Startup Wizard	AAA Server Groups	-			
🖯 🚽 AAA Setup	1				
AAA Server Groups	AAA server groups				
- Auth. Prompt	Samuel Comm	Destand	A new setting Martin	Beautivelian Maria	
LDAP Attribute Map	Server Group	Protocol	Accounting Mode	Reactivation Mode	Add
Anti-Spoofing	LOCAL	LOCAL			Edit
E - B ARP	🗯 Edit LOCAL Server Gro	oup			×
- 🛃 Auto Update	Sector and the sector of the s				Delete
Gient Update	This facture allows to	onacity the maxim	um number of folloci offen	unto to ollow hotoro	-
Certificate	locking out a user and	I denu access to th	a user. This limit is anning	able only when local	
E Provice Access	database is used for	authentication.	e aser. The line is appro-	able only whethera	
AAA Access					
HTTPS/ASDM	Extended and the	d only at			
Secure Shell	Enduie Local Use	LOCKOUL:			-
Teinet			A		Add
Virtual Access	Maximum Attempt	s: (16)			-
Device Administration					Ealt
The purch services					Delete
Hab Availability and Sad					Deele
Fellower			12		Move I.
Exerment	OF	Ó Í Í	Cancel H	elp	
					Move Dry

Configuración CLI Equivalente:

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

付 Add Tunnel G	roup					
Name:	sslgroup)	_ ,	Type: wet	ovpn	
General V	VebVPN					
Configure	general acce	ss <mark>attribut</mark> es fro	om the followin	ng sub-tabs.		
Basic A	uthentication	Authorization	Accounting	Client Addr	ess Assignmer	nt Advanced
Group	Policy:	clientgroup	•]		
n St	rip the realm fr	om username k	pefore passing	j it on to the	AAA server	

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

Ivame:	Issigroup		туре:	lwepvpn	
eneral	VVebVPN				
Configu	re general acce:	ss attributes from the	following sub	o-tabs.	
Basic	Authentication	Authorization Acco	unting Client	Address Assignmen	t Advanced
т	o specify wheth	ner to use DHCP or ad	Idress pools f	or address assignme	
×	IP Address Mar	nagement > Assignme	ent.		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
	DHCP Servers	8			
				101	
	IP Address:		Add >>	•	
	IP Address:		Add >> Delete	>	
	IP Address:		Add >> Delete	•	
	IP Address:		Add >> Delete	•	
	IP Address:		Add >> Delete		
	IP Address:	nterface-specific add	Add >> Delete	o to the Advanced tal	b.
	IP Address:	nterface-specific add	Add >> Delete	o to the Advanced tal Assigned	b.

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.

Configure MehVPN access	attributes from the following sub-t	ahe	
	an induces from the following sub-t	1	
Jasic NetBIOS Servers	Froup Allases and OKLS Web Pag	ge	
Group Aliases			40
		Alias	Statu:
Alias:	Add >>	Alias sslgroup_users	Statu enable

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

8. Configure el NATElija 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 📻 Add Dynamic NAT Rule Real Address Interface: inside IP Address: 0.0.0.0 0.0.0.0 Netmask: Dynamic Translation Interface: outside 🖶 Add 🗹 Edit 📋 Delete Pool ID Select Addresses Pool 🖳 172.16.1.5 1 ~ NAT Options... OK Cancel Help 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
1
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-
```

DOTICY LUIMETSDECTITED
anlit_tunnol_notwork_ligt walue anlit_tunnol
spiit-tunnei-network-fist value spiit-tunnei
<i>! Encrypt the traffic specified in the split tunnel</i>
ACL only. webvpn
svc required
510 10441104
! Activate the SVC under webvpn mode. svc keep-
installer installed
I then the convictor and the court of the court
! 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 suc rekey time 30
<i>! Command that specifies the number of minutes !</i>
from the start of the session until the rekey takes
place, I from 1 to 10080 (1 week), svc rekey method
SSI
! Command that specifies that SSL renegotiation !
takes place during SVC rekey username ssluser1 password
eakes place during bye lekey. abelinane bblabeli pubbwela
ZRNW85jZqEavd5P. 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 compacerver contact compacerver enable trang
iocacion no simp-server concact simp-server enable craps
snmp authentication linkup linkdown coldstart tunnel-
group sslgroup type webvpn
I Croate a tunnel group "gglgroup" with tune ag
create a tunner group ssigroup with type as
WebVPN. tunnel-group sslgroup general-attributes
address-pool vpnpool
I Accoriate the address peel impreel created
: Associate the address poor vphpoor created.
default-group-policy clientgroup
default-group-policy clientgroup
default-group-policy clientgroup
default-group-policy clientgroup ! Associate the group policy "clientgroup" created.
default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes
default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable </pre>
<pre>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</pre>
<pre>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</pre>
<pre>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 ! !</pre>
<pre>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 time inspect dng proget dng map parameters</pre>
<pre>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</pre>
<pre>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</pre>
<pre>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</pre>
<pre>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 rag inspect</pre>
<pre>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</pre>
<pre>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</pre>
<pre>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 rsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect</pre>
<pre>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 rsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global policy global</pre>
<pre>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 esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global</pre>
<pre>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 esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global webvpn</pre>
<pre>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 esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global webvpn enable outside</pre>
<pre>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 esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global webvpn enable outside</pre>
<pre>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 esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global webvpn enable outside ! Enable WebVPN op the outside interface. svc image</pre>
<pre>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 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.(sslalient-vin-1 1 4 179 phz 1</pre>
<pre>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 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:/sslclient-win-1.1.4.179.pkg 1</pre>
<pre>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 sip 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</pre>

-- Enable the security appliance to download !--- SVC



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		
0		
https:// <ip address="" of="" t<="" th=""><th>ne ASA WebVPN interface></th><th></th></ip>	ne ASA WebVPN interface>	
Sin Site Man Service - Microso		
File Edit View Payorites 1	ools Hep	
🔇 Back 🔹 🕥 🗉 🚺	🖞 🏠 🔎 Search 🤺 Favorites 🤣 🎯 - 璗 🔜 🖄	
Address 🙆 https://172.16.1.1/+w	vebvpn+/index.html	
CISCO STSTENS	N Service	
	Login	
	Please enter your username and password.	
	PASSWORD:	
	GROUP: sslgroup_users	
	Login Clear	
- Dono		A a to

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





5. Puede obtener estas ventanas una vez establecida la



6. 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

atistics Route D	etails About		
ddress Informal	ion	SSL Information	
Server:	172.16.1.1	Cipher:	3DES SHA-1
Client:	192.168.10.1	Version:	TLSv1
ytes		Transport Informal	tion
Sent:	2887	Local LAN:	Disabled
Received:	940	Split Tunneling:	Enabled
ames		Connection Inform	ation
Sent:	35	Time:	00:00:24
Received:	12		

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

1	Cisco System	ns SSL VPN Client	£	X
C	alling alling SS	LVPN CLIENT F	or WEBVPN	
	Statistics Bou	te Details About		
	Local LAN F	loutes	Secure Routes	
	Network	Subnet Mask	Network 10.77.241.128	Subnet Mask 255.255.255
<i>9</i> .		Close	Disconnect	
únel.	o Systems SS	L VPN Client		6
Cisco Svs	SSLV	N CLIENT for W	ebvpn	
Statis	stics Route Del	ails (About)		
Cit	SCO SYSTEMS	SSL VPN CLIE for WEBVPN	ENT Versio	n 1.1.4.179
C		Create a full anywhere ar	y secure connenytime	now.
© Co	opyright 2004-200	6 Cisco Systems, Inc. A	ll rights reserved. Cisco, Ci	sco Systems
and its at	the Cisco System filiates in the Unit	s Logo are registered tra ed States and certain ot	ademarks of Cisco Systems her countries.	, Inc. and/or
		Close	Disconnect	

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.

Session Type: SVC

```
: ssluser1
Username
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

VPN Connection Graphs	Sessions						
PSec Turnels	Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
Crypto Statistics	0 Filter By: Web	O VPN	1 Al Sessions	0	0	1 Fiter	2
NAC Session Summe	Usernam IP Addres	e Gr Se Tu	oup Policy nnel Group	Protocol Encryption	1	Login Time Duration	Detai
Protocol Statistics		and the second se		A A A A A A A A A A A A A A A A A A A	08.40.51	UTC TRUMP 20	

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_uauIth: 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.

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

 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@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

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

iter	By:	•	Filter Stoschil Find
D	Source IP	Destination P	Description
	192.168.10.255		No trainstation group found for udp are outside:192/168.10.1/138 dist inside:192.168.10.255/138
	10.77.244,193		No translation group found for udp site outside:192,168,18.1/I 027 dst inside:10.77 244.193/63
_	10.77.244;393		No transistion group found for usp and outside:192.168.10.1/1028 dat inside:10.77.244.193/63
~	192.168.10.1	10.2.2.2	Bult inbound TCP connection 1902 for outside:192.168.10.1/1100 (172.16.1.5/1025) to outside:10.2.2.2/80 (10.2.2.2/80) (soluser1)
	192.168.10.1	172.16.1.5	Built dynamic TCP translation from outside 192.168.10.1/1100 to outside:172.16.1.5/1025
_	192,166.10.255		No transistion group found for udp arc outside 192.168.10.1/138 dat inside:192.168.10.255/138
	10.77.244.198		No translation group found for udp and outside 192/168/10.1/1027 dist-inside/10/27/.244/193/53
	10:77.244.193		No translation group found for udp. and outside 197.168 10.1/1028 dst-inside:10.77.244.193/53
۹ľ	10.77.244.193		No transiellon group found for ude arc outside 192.168.10.1/1027 dat Inside:10.77.244.193/53
2le	ase select a sys	log entry to see	the explanation

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