Ejemplo de Configuración de ASA con WebVPN y Single Sign-on con ASDM y NTLMv1

Contenido

Introducción prerrequisitos Requisitos Componentes Utilizados **Convenciones** Configurar Agregue a un servidor de AAA para la autenticación del Dominio de Windows Cree un certificado autofirmado Habilite el WebVPN en la interfaz exterior Configure una lista url para sus servidores internos Configure un Internal group policy (política grupal interna) Configure a un grupo de túnel Configure el Auto-anuncio del comienzo de las emisiones para un servidor Configuración final de ASA Verificación Pruebe un login del WebVPN Sesiones de monitoreo Haga el debug de a una sesión WebVPN Troubleshooting Información Relacionada

Introducción

Este documento describe cómo configurar Cisco Adaptive Security Appliance (ASA) para pasar automáticamente credenciales de login de usuario WebVPN, así como la autenticación secundaria, a los servidores que requieren validación de login adicional respecto a Windows Active Directory que ejecuta NT LAN Manager versión 1 (NTLMv1). Esta función se conoce como Inicio único de sesión (SSO). Proporciona a los links configurados para un grupo WebVPN específico la capacidad de pasar esta información de autenticación de usuarios, eliminando así las indicaciones de autenticación múltiples. Esta función también se puede utilizar en el nivel global o en el nivel de configuración de usuarios.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

• Asegúrese de que el NTLMv1 y los permisos de Windows para los usuarios de VPN de la blanco estén configurados. Consulte su documentación de Microsoft para más información sobre los derechos de acceso del Dominio de Windows.

Componentes Utilizados

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

- Cisco ASA 7.1(1)
- Cisco Adaptive Security Device Manager (ASDM) 5.1(2)
- Servicios de Internet Information Server de Microsoft (IIS)

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 <u>Convenciones de Consejos Técnicos de Cisco</u> para obtener más información sobre las convenciones sobre documentos.

<u>Configurar</u>

En esta sección, le presentan con la información para configurar el ASA como servidor WebVPN con el SSO.

Nota: Utilice la herramienta <u>Command Lookup Tool</u> (<u>clientes registrados solamente</u>) para obtener más información sobre los comandos utilizados en esta sección.

Agregue a un servidor de AAA para la autenticación del Dominio de Windows

Complete estos pasos para configurar el ASA para utilizar un controlador de dominio para la autenticación.

 Seleccione la configuración > las propiedades >AAA ponen >AAA los servidores y el haga click en Add Proporcione un nombre para el grupo de servidores, tal como Windows_NT, y elija el dominio de NT como el protocolo.

G Claco ASDM 2	5.1 for ASA - 172.16.172.57	7	
File Rules Be	arch Options Tools Wizards	is Halp	
Harra C	antiquestion Mediadae	C C C C C C C C C C C C C C C C C C C	
inite (s	Configuration + Proceedies + A	AAA Setus - AAA Setuaris	
Ξ,	● 金 平 ■1前13.0	12 호 등 집 ()	
Interfaces	Startup Witeard	AVA Servers	
Encarta Bolica	AAA Song	Server Groups	
54	Auth, Prompt Set DAP Athlburs Mag.	Server Group Protocol Accounting Node Reactivation Mode Add	
NAT	- SANI-Spoofing	Edit	
8	Auto Upcate	Decla	
VIN	B- Confinance B- Confinance Device Access		
	與 第Device Administration 回 督DHCP Services	Parameter Salarand Comm	
121	- BDNS Clent	Server Name or IP Address Interface Timeout Add	
PS -	- Eragment	Edi	
- <u>*</u>	History Metrics	Deide	
Routing	由·歌 IF Audt 回·题 Logging	Minya az	
Re alle alle alle alle alle alle alle al		70, 99 (20+9)	
		Tes:	
Properties	-∰TCP Options -⊗TTimeoute	🖬 Add AAA Server Group	3
	🖵 🚰 URL Filtering	Apply Reset Configure AAA server group. The Accounting Mode ath buts is only applicable for RACIUS and TACACE+ protocols.	
		orison (NACIO) 😡 🛃 📋 Server Group: (Windows_N1	
		Protocol MT Domein	
		Asservation bracks — Cl Constitution on — St Consta	
		raccinitedizensi Contenanecea (Contena	
		Reactivation Mode: O Depletion	
		Dead Time 10 minutes	
		Nas Failed Attempts: 3	
		DK Canzel Help	

2. Agregue a un Servidor Windows.Seleccione el grupo creado recientemente y el haga click en Add Seleccione la interfaz donde se localiza el servidor y ingrese el IP Address y el nombre del controlador de dominio. Esté seguro que el nombre del controlador de dominio está ingresado en todas las letras mayúsculas. Haga Click en OK cuando le hacen.

🖆 Cisco ASDM	5.1 for ASA -	172.16.172.5	2					1		
Fie Rulas Ga	anth Options	Tools Wizard	is Help							
i dia amin'ny fiana amin'ny fi	Configuration	[] Montoring	C Dack	O Forward	Q (Search Re	💽 🔚 fresh Save	? Hela	Cisco Sr	allu.	
interfacese	Sentiputeter 9 (2) T - P Startu D AAA S - C Startu D AAA S - C Startu - C Startu	n - Properties - × I III 1 1 2 1 p Wizand stup A Carvers th. Prompt	AAA Setu AAAA S - Se S	pin AAA Berverie Re Kall © I Servers Inter Groups erver Groups	Protocol	Accounting Mod	ie Reactivation	Mode Add		
NAT SAT	- Seco -	MP Adribute Map poofing Jodate	UC [77]	CAL ndows_NT	LOCAL NT Domai		Depleti	nn Edit Delete		
VFN CSD Monager	E Certifi E Certifi E Societa E Conce E Conce	cate e Access e Administration ? Services Client	Se	wers in Selector	d Group			>		
irs Racha	Failow FSFragm FSF FSFragm	er vent v Metrics HTTPS	8	erver Name or I	P Address	Interface	Timeout	Add Edit Delete		
Ginbal Objects	E E Loggi F Priorit F SEL F SUNR	ng y Queue IPC Server						Move up biove down		
Properties	는 쇼라TCP C OTimed - 쨜URL P	Dations Inits Fitering				Apply	Rese Server	AA Server Group:	Windows_NT	X
	,				cisco	NA (15)	interfa Server	te Name: Name or IP Address:	inside 10.1.1.200	
							Timed NT Do Servi	ut: main Parameters er Port: en Dontraler.	10 139 Esc.e2200	seconds
								ок	Cancel	Help

Esta ventana muestra la configuración AAA completada:



Cree un certificado autofirmado

Complete estos pasos para configurar el ASA para utilizar un certificado autofirmado.

Nota: En este ejemplo un certificado autofirmado se utiliza para la simplicidad. Para otras opciones de la inscripción del certificado, tales como alistar con un Certificate Authority externo, refiera a <u>configurar los Certificados</u>.

- 1. Seleccione la **configuración > las propiedades > el certificado > el trustpoint > la configuración** y el haga click en Add
- 2. En la ventana que aparece ingrese un nombre del trustpoint tal como Local-TP y control generan un certificado autofirmado en la inscripción. Las otras opciones se pueden dejar con sus configuraciones predeterminadas. Haga Click en OK cuando le hacen.



Esta ventana muestra la configuración completada del trustpoint:



WebVPN del permiso en la interfaz exterior

Complete estos pasos para permitir que los usuarios fuera de su red conecten usando el WebVPN.

- 1. Seleccione la configuración > el VPN > el WebVPN > el acceso del WebVPN.
- 2. Seleccione la interfaz deseada, haga clic el permiso, y marque la lista desplegable del grupo de túnel del permiso en la página de registro del WebVPN.Nota: Si la misma interfaz se utiliza para el WebVPN y el acceso del ASDM, usted debe cambiar el puerto predeterminado para el acceso del ASDM del puerto 80 a un nuevo puerto tal como 8080. Esto se hace bajo la configuración > las propiedades > acceso del dispositivo > HTTPS/ASDM.Nota: Usted puede reorientar automáticamente a un usuario al puerto 443 en caso que un usuario navegue a http:// <ip_address> en vez de https:// <ip_address>. Seleccione la configuración > las propiedades > en vez de https:// <ip_address>. Seleccione la configuración > las propiedades > en vez de https:// <ip_address>. Seleccione la configuración > las propiedades > en vez de https:// <ip_address>. Seleccione la configuración > las propiedades > en vez de https:// <ip_address>. Seleccione la configuración > las propiedades > en vez de https:// <ip_address>.

Cisco ASDM	5.1 for ASA - 172.16.171.51		
File Rules Se	arch Options Tools Wizards	Help	
in the second se	Configuration Monitoring	Sack Forward Search Refresh Save Help	STENS Allana
	Configuration > VPN > WebVPN	> WebVPN Access	
Ξ,	●金革 ■ 前 炎暭	8. 免 筋 ()	
Interfaces	(마 Material Proxy 📃	WebVPN Access	
<u>6</u>	General		
Security Policy	- B Client Update	Configure access parameters for WebVPN. (Note: The WebVPN features in this software release are currently provided as a free trial, and future major software releases will require the purchase and	6
24	Group Policy	installation of a WebVPN feature license.)	
NAT	- 💭 Tunnel Group		
13	- SIVPN System Opt	Interface WebVPN Enabled Enable	
<u>88</u>	E Address Manager	outside Yes Disable	
VPN	🕀 🥵 IPSec		- 1
<u> </u>			
CSD Manager			
۵.	-JAPCF		
IPS	- BCSD Setup	Port Number: 443	
4≩⊳	- Cache	Defaultiple Times de 1900	
Routing	- The Encoding	Default ldie Timeout: Tabu seconds	
(A)	- Sport Forwarding	Max. Sessions Limit: 2	
Clabel Objects	- Proxies	WebVPN Nemory Size: 50 % of Intel Integral memory	
Gibbal Objects	- 39 Proxy Bypass		
3	SSO Servers	Enable Tunnel Group Drop-down List on WebYPN Login Page	
Properties	Servers and URL		
	WebvPN Access	Apply Reset	
	<		
Configuration cha	anges saved successfully.	cisco 🛛 NA (15) 🛛 🛃 🖬 🔹 3/30/06 2:37:41 PM	UTC

Configure una lista url para sus servidores internos

Complete estos pasos para crear una lista que contenga los servidores para los cuales usted quiere conceder su acceso de usuarios de WebVPN.

- 1. Seleccione la **configuración > VPN > WebVPN > los servidores y los URL** y haga click en Add
- 2. Ingrese un nombre para la lista url. Este nombre no es visible a los usuarios finales. Haga clic en Add (Agregar).
- 3. Ingrese el nombre de la visualización URL pues debe ser visualizado a los usuarios. Ingrese la información del URL del servidor. Éste debe ser cómo usted accede normalmente el servidor.

Cisco ASDM 5 File Rules Se	5.1 for ASA - 172.16.172.5; arch Options Tools Wizard	s Help	
G Home C	Configuration Monitoring	O O Q Reference Search Reference Save Help	Cisco Systems
Interfaces	Contiguiation - VPN - WebVP	N - Servers and URLs	Adte
VPN CSD Manager	PBec		Edt Delde
PS PS Routing	- Content Rewrite - Port Forwarding - Proxy Bypass - Stroky Bypass - S	Add Server and URL List List Name: Webserver URL Display Name URL	Add
Global Objects	- WebyPN Access	erver or UKL	Edit Defete Mova Up
	URL	https v 10.1.1.200	Move Down:

4. El Haga Click en OK, AUTORIZACIÓN, y entonces se aplica.



Configure un Internal group policy (política grupal interna)

Complete estos pasos para configurar una directiva del grupo para sus usuarios de WebVPN.

- 1. Seleccione la **configuración > el VPN > la directiva del general > del grupo**, el tecleo **agrega**, y selecciona el **Internal group policy (política grupal interna)**.
- En la ficha general, especifique un nombre de la directiva, tal como Internal-Group_POL_WEBVPN. Entonces desmarque heredan al lado de los protocolos de túneles y del WebVPN del control.

🖆 Add Internal Group Policy						
Name: mal-GRP_POL_WEBVPN						
General IPSec Client Configuration Cl	General IPSec Client Configuration Client Firewall Hardware Client WebVPN					
Check an Inherit checkbox to let the corre	esponding setting take its value from the default group policy.					
Tunneling Protocols: 📃 Inherit	IPSec VebVPN					
Filter: 🔽 Inherit	Manage					
Connection Settings						
Access Hours: 🗹 Inherit	New					
Simultaneous Logins: 🗹 Inherit						
Maximum Connect Time: 🔽 Inherit	Unlimited minutes					
Idle Timeout: 🗹 Inherit	Unlimited minutes					
Servers						
DNS Servers: 🗹 Inherit	Primany: Secondary:					
WINS Servers: 🔽 Inherit	Primary: Secondary:					
DHCP Scope: 🔽 Inherit						
OK	Cancel Help					

3. En la lengueta del WebVPN seleccione la **otra sub-**lengueta. Desmarque **heredan** al lado de los servidores y de las listas url y seleccionan la lista url que usted configuró de la lista desplegable. Haga Click en OK cuando le hacen.

📬 Add Internal Group Policy
Name: mal-GRP_POL_WEBVPN
General IPSec Client Configuration Client Firewall Hardware Client WebVPN
Configure WebVPN attributes using the following tabs . Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.
Functions Content Filtering Homepage Port Forwarding Other SSL VPN Client
Servers and URL Lists: Inherit webserver New
Web-Type ACL ID: VInherit Manage
SSO Server: Vinherit New
HTTP Compression: Inherit O Enable O Disable
Keepalive Ignore
Specify upper limit of the HTTP/HTTPS traffic, per transaction to ignore.
Transaction Size: Inherit KB
Deny Message
✓ Inherit
UK Cancel Heip

Configure a un grupo de túnel

Complete estos pasos para configurar a un grupo de túnel para sus usuarios de WebVPN.

 Seleccione la configuración > el VPN > el general > al grupo de túnel, el tecleo agrega y acceso selecto del WebVPN...



2. Ingrese un nombre para el grupo de túnel, tal como WEB_VPN-GRP. En la lengueta básica seleccione la directiva del grupo que usted creó y verifiquela que el Tipo de grupo es **webvpn**.

📧 Edit Tunnel Group 🛛 🔀
Name: WEB_VPN-GRP Type: webvpn
General WebVPN
Configure general access attributes from the following cub take
Basic AAA Client address Assignment Advanced
Group Policy: Internal-GRP_POL
DftGrpPolicy
outpute realm from userialite before passing it on to the Ave server
Strip the group from username before passing it on to the AAA server
OK Cancel Help

3. Vaya a la lengueta AAA.Para el grupo de servidor de autenticación, elija al grupo que usted configuró para habilitar la autenticación del NTLMv1 con su controlador de dominio.Opcional: Marque el LOCAL del uso si el grupo de servidores no puede habilitar el uso de la base de datos de usuarios locales en caso que el grupo configurado AAA falle. Esto puede ayudarle a resolver problemas en otro momento.

🖆 Edit Tunnel Group 🛛 🔀					
Name: WEB_VPN-GRP Type: webvpn					
General WebVPN					
Configure general access attributes from the following sub-tabs.					
Basic AAA Client Address Assignment Advanced					
To set authentication server group per interface, go to the Advanced tab.					
Authentication Server Group: Windows_NT					
Use LOCAL if Server Gra					
Authorization Server Group: LOCAL					
 Users must exist in the authorization database to connect 					
Accounting Server Group: None 💙					
Authorization Settings					
 Use the entire DN as the username 					
 Specify individual DN fields as the username 					
Primary DN Field: CN (Common Name)					
Secondary DN Field: OU (Organization Unit)					
Password Management					
Override account-disabled indication from AAA server					
Enable notification upon password expiration to allow user to change password					
Enable notification prior to expiration Notify days prior to expiration					
OK Cancel Help					

- 4. Vaya a la lengueta del WebVPN y después vaya a la sub-lengueta de los **alias y URL del grupo**.
- 5. Ingrese un alias bajo los alias y el haga click en Add del grupo Este alias aparece en la lista desplegable presentada a los usuarios de WebVPN en el login.

🖆 Edit Tunnel Group
Name: WEB_VPN-GRP Type: webvpn
General WebVPN
Configure WebVPN access attributes from the following sub-tabs.
Basic NetBIOS Servers Oroup Anases and Orics Web Page
Alias Status
Alias: Add >> Group-Selection enable
<< Remove
✓ Enable
URL Status
URL (http or https): Add >>
<< Remove
✓ Enable
OK Cancel Help

6. Haga clic en OK y en Apply.

Auto-anuncio del comienzo de las emisiones de la configuración para un servidor

Switch a la línea de comando para habilitar el SSO para sus servidores internos.

Nota: Este paso no se puede completar en el ASDM y debe ser realizado usando la línea de comando. Refiera a <u>acceder la interfaz de la línea de comandos</u> para más información.

Utilice el **comando auto-signon** de especificar al recurso de red, tal como un servidor, que usted quiere dar su acceso de usuarios a. Una dirección IP del servidor único se configura aquí, pero un rango de red tal como **10.1.1.0** /24 puede también ser especificado. Refiera al <u>comando auto-</u><u>signon</u> para más información.

```
ASA#configure terminal
ASA(config)#webvpn
ASA(config-webpvn)#auto-signon allow ip 10.1.1.200 255.255.255.255 auth-type ntlm
ASA(config-webvpn)#quit
ASA(config)#exit
ASA#write memory
```

En esta salida de ejemplo, configuran al **comando auto-signon** para el WebVPN global. Este comando se puede también utilizar en el modo de la configuración de grupo del WebVPN o el modo de configuración del nombre de usuario de WebVPN. El uso de este comando en el modo de la configuración de grupo del WebVPN lo limita a un grupo determinado. Asimismo, el uso de este comando en el modo de configuración del nombre de usuario de usuario de WebVPN lo limita a un grupo determinado. Asimismo, el uso de este comando en el modo de configuración del nombre de usuario de WebVPN lo limita a un grupo determinado. Refiera al <u>comando auto-signon</u> para más información.

Configuración final de ASA

Este documento usa esta configuración:

Versión de ASA 7.1(1) ASA# show running-config : Saved ASA Version 7.1(1) ! terminal width 200 hostname ASA domain-name cisco.com enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface GigabitEthernet0/0 nameif outside security-level 0 ip address 172.16.171.51 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0 interface GigabitEthernet0/2 shutdown no nameif no security-level no ip address interface GigabitEthernet0/3 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 dns server-group DefaultDNS domain-name cisco.com pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image disk0:/asdm512.bin no asdm history enable arp timeout 14400 route outside 0.0.0.0 0.0.0.0 172.16.171.1 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 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute !--- AAA server configuration aaa-server Windows_NT protocol nt aaa-server Windows_NT host 10.1.1.200 ntauth-domain-controller ESC-SJ-7800 !--- Internal group policy configuration group-policy Internal-GRP_POL_WEBVPN internal group-policy Internal-GRP_POL_WEBVPN attributes vpn-tunnel-protocol webvpn webvpn url-list value webserver username cisco password Q/odgwmtmVIw4Dcm encrypted privilege 15 aaa authentication http console LOCAL aaa authentication ssh console LOCAL aaa authentication enable console LOCAL http server enable 8181 http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart !--- Trustpoint/certificate configuration crypto ca trustpoint Local-TP enrollment self crl configure crypto ca certificate chain Local-TP certificate 31 308201b0 30820119 a0030201 02020131 300d0609 2a864886 f70d0101 04050030 le311c30 la06092a 864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30 1e170d30 36303333 30313334 3930345a 170d3136 30333237 31333439 30345a30 le311c30 la06092a 864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30 819f300d 06092a86 4886f70d 01010105 0003818d 00308189 02818100 e47a29cd 56becf8d 99d6d919 47892f5a 1b8fc5c0 c7d01ea6 58f3bec4 a60b2025 03748d5b 1226b434 561e5507 5b45f30e 9d65a03f 30add0b5 81f6801a 766c9404 9cabcbde 44b221f9 b6d6dc18 496fe5bb 4983927f adabfb17 68b4d22c cddfa6c3 d8802efc ec3af7c7 749f0aa2 3ea2c7e3 776d6d1d 6ce5f748 e4cda3b7 4f007d4f 02030100 01300d06 092a8648 86f70d01 01040500 03818100 c6f87c61 534bb544 59746bdb 4e01680f 06a88a15 e3ed8929 19c6c522 05ec273d 3e37f540 f433fb38 7f75928e 1b1b6300 940b8dff 69eac16b af551d7f 286bc79c e6944e21 49bf15f3 c4ec82d8 8811b6de 775b0c57 e60a2700 fd6acc16 a77abee6 34cb0cad 81dfaf5a f544258d cc74fe2d 4c298076 294f843a edda3a0a 6e7f5b3c quit !--- Tunnel group configuration tunnel-group WEB_VPN-GRP type webvpn tunnel-group WEB_VPN-GRP general-attributes authentication-server-group Windows_NT default-grouppolicy Internal-GRP_POL_WEBVPN tunnel-group WEB_VPN-GRP webvpn-attributes group-alias Group-Selection enable telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspectiontraffic ! ! policy-map global_policy class inspection_default inspect dns maximum-length 512 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				
<pre>sip inspect xdmcp ! service-policy global_policy global</pre>				
! WebVPN Configuration webvpn enable outside url-list				
webserver "Internal Server" https://10.1.1.200 1 tunnel-				
group-list enable auto-signon allow ip 10.1.1.200				
255.255.255.255 auth-type ntlm				
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6				
: end				

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.

Pruebe un login del WebVPN

Inicie sesión como usuario para probar su configuración.

 Intente iniciar sesión al ASA con la información del usuario de su dominio de NT. Seleccione al grupo alias configurado en el paso 5 debajo <u>configuran a un grupo de</u> túnel

WebVPN Service - Microsoft Internet Explorer	
Ele Edit Vew Fgyorites Icols Help	a shi kata ka ka sa sa 🖉
😋 Back 🔹 🐑 📓 😭 🔎 Search 🤺 Favorites 🤣 🎯 - 嬦 🚍 🖓	
Address 💩 https://172.16.171.51/+webvpr+/index.html	💙 🔂 Go Unks 🎽
CISCO SYSTEMS wellingen tillingen WebVPN Service	
Login	
Please enter your usemame and password.	
USERNAME: test	
PASSWORD:	
GROUP: Group-Selection	
Login Clear	
	8
a Done	🔒 🔮 Internet

2. Busque los links configurados a los servidores internos. Haga clic en el link para verificar.

WebVPN Service - Microsoft Internet	et Explorer	
Elle Edit Yew Favorites Icols Help		<u></u>
Ġ Back = 🛞 - 💌 🖻 🏠 🍃	🔎 Search 🧏 Favorites 🥝 🔗 🍓 🚍 🥸	
Address 🍓 https://172.16.171.51/+webvpn+/	-/portal.html 🔽 💽	Go Links »
S Pop-up blocked. To see this pop-up or addition	onal options dick here	×
Cisco Systems automatilities WebVPN Servi	rice	
	<u>Click here to open the Floating Toolbar</u> 🖓 🖉	
WEB APPLICATIONS	Web Bookmarks	
Enter Web Address (URL)	Internal Server	
Go		
Web Bookmarks 🛛 👻		
		-
iavascript:top.doWebUrl("https://10.1.1.200")	1) 🔂 🕒 🗿 Internet	<u>۲</u>

Sesiones de monitoreo

Seleccione la **supervisión > el VPN > los VPN statistics (Estadísticas de la VPN) > las sesiones** y busque a una sesión WebVPN que pertenezca al grupo configurado en este documento.

🚰 Cisco ASDM 5.1 for ASA - 172.16.171.51		
File Rules Search Options Tools Wizards Help		
G Home C	Sontiguration Monitoring	O O Q Q Q Q Cisco Systems Back Forward Search Refresh Save Help Image: Cisco Systems
Hiterfaces	Monitoring > VPN > VPN Statust P P VPN Connection Grapt P P Sec Tunnels WebVPN/SVC VPN Statistics P VPN Statistics P Compression Statistics P Compression Statistics P Compression Statistics P Robool Statistics P Robool Statistics P Sessions P Sessions P So Statistics P So Statistics	Sessions Remote LAN-to-LAN WebVPN SSL VPN Client E-mail Proxy Total Cumulative 0 0 1 0 0 1 3 Filter By: WebVPN - All Sessions Filter Filter Username Group Policy Protocol Login Ti Details IP Address Tunnel Group Encryption Duration Logout 121 Intemal-GRP_POLVebVPN 15:03:36 UTC Thut Logout 171 <s9.86.116< td=""> ViceB_VPN-GRPSDE3 0h.01m-18s Ping ViceB_VPN-GRPSDE3 Intemal-GRP_POL VebVPN 15:03:36 UTC Thut Logout Intemal-GRP_POL VebVPNSDE3 0h.01m-18s Ping ViceB_VPN-GRP SDE3 Codent from popup menu. Logout Bessions Logout By: All Sessions Logout Sessions Last Updated: 3/30/06 2:31:30 PM</s9.86.116<>
Data Refeshed Successfully. Cisco INA (15) 📑 🖬 🐼 🖄 3/30/06 3:05:21 PM UT		

Haga el debug de a una sesión WebVPN

Esta salida es un debug de la muestra de una sesión WebVPN exitosa.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

```
ASA#debug webvpn 255
INFO: debug webvpn enabled at level 255
ASA#
ASA# webvpn_portal.c:ewaFormServe_webvpn_login[1570]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286]
WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782]
!--- Begin AAA WebVPN: calling AAA with ewsContext (78986968) and nh (78960800)! WebVPN: started
user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422]
WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_auth.c:http_webvpn_post_authentication[1095]
WebVPN: user: (test) authenticated.
!--- End AAA webvpn_auth.c:http_webvpn_auth_accept[2093]
webvpn_session.c:http_webvpn_create_session[159] webvpn_session.c:http_webvpn_find_session[136]
```

WebVPN session created!

```
webvpn_session.c:http_webvpn_find_session[136]
webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202]
traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421]
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
!--- Output supressed webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn auth.c:webvpn auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
```

Troubleshooting

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

- Si la casilla desplegable del grupo no está presente en la página de registro del WebVPN, esté seguro que usted ha completado el paso 2 bajo el <u>WebVPN del permiso en la interfaz</u> <u>exterior</u> y el paso 5 debajo <u>configura a un grupo de túnel</u>. Si estos pasos no se completan y el descenso-abajo falta, la autenticación baja bajo grupo predeterminado y falla probablemente.
- Aunque usted no pueda asignar los derechos de acceso al usuario en el ASDM o en el ASA, usted puede restringir a los usuarios con los derechos de acceso de Microsoft Windows en su controlador de dominio. Agregue los permisos necesarios del grupo de NT para la página web que el usuario autentica a. Una vez los registros de usuario en el WebVPN con los permisos del grupo, acceso a las páginas especificadas se conceden o se niegan por consiguiente. El ASA actúa solamente como host de la autenticación de representación en nombre del controlador de dominio y todas las comunicaciones aquí son NTLMv1.
- Usted no puede configurar el SSO para Sharepoint sobre el WebVPN porque el servidor de Sharepoint no soporta la autenticación basada las formas. Como consecuencia, los marcadores con el poste o el procedimiento plug-in del poste son no corresponde aquí.

Información Relacionada

- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- Soporte Técnico y Documentación Cisco Systems