Configuración de Clientless SSL VPN (WebVPN) en Cisco IOS con SDM

Contenido

Introducción **Prerequisites** Requirements Componentes Utilizados Diagrama de la red **Convenciones** Tareas de Preconfiguración Configure el WebVPN en el Cisco IOS Paso 1. Configure el Gateway del WebVPN Paso 2. Configure los Recursos Permitidos para el Grupo de Políticas Paso 3. Configure al Grupo de Políticas del WebVPN y Seleccione los Recursos Paso 4. Configure el Contexto del WebVPN Paso 5. Configure la Base de datos del Usuario y el Método de Autenticación **Resultados** Verificación Procedimiento Comandos Troubleshoot Procedimiento Comandos Información Relacionada

Introducción

Clientless SSL VPN (WebVPN) le permite al usuario acceder de forma segura a los recursos en la LAN corporativa desde cualquier lugar con un navegador web con SSL habilitado. El usuario primero autentica con un gateway del WebVPN que le permite luego acceder a los recursos de red preconfigurados. Los gateways WebVPN se pueden configurar en los routers Cisco IOS[®], Cisco Adaptive Security Appliances (ASA), Cisco VPN 3000 Concentrators y Cisco WebVPN Services Module para los routers Catalyst 6500 y 7600.

La tecnología Secure Socket Layer (SSL) Virtual Private Network (VPN) se puede configurar en dispositivos Cisco de tres maneras principales: Clientless SSL VPN (WebVPN), Thin-Client SSL VPN (Reenvío de Puerto), y modo SSL VPN Client (SVC). Este documento demuestra la configuración de theWebVPN en los routers de Cisco IOS.

Nota: No cambie ni el nombre de dominio IP ni el nombre de host del router, ya que esto

desencadenará una regeneración del certificado autofirmado y anulará el punto de confianza configurado. La regeneración del certificado autofirmado causa problemas de conexión si el router se ha configurado para el WebVPN. El WebVPN une el nombre de trustpoint SSL a la configuración de gateway de WebVPN. Por lo tanto, si se ejecuta un nuevo certificado autofirmado, el nuevo nombre del trustpoint no corresponde con la configuración del WebVPN y los usuarios no se pueden conectar.

Nota: Si ejecuta el comando **ip https-secure server** en un router WebVPN que utiliza un certificado autofirmado persistente, se genera una nueva clave RSA y el certificado se vuelve inválido. Se crea un nuevo trustpoint, que interrumpe el WebVPN SSL. Si el router que usa el certificado autofirmado se reinicia después de que ejecuta el comando **ip https-secure server, se produce el mismo problema.**

Consulte Ejemplo de Configuración de <u>Thin-Client SSL VPN (WebVPN) IOS con SDM para</u> obtener más información sobre la thin-client SSL VPN.

Consulte el Ejemplo de Configuración de <u>SSL VPN Client (SVC) en IOS con SDM para obtener</u> más información sobre <u>SSL VPN Client</u>.

SSL VPN ejecuta estas plataformas del Cisco Router:

- Routers Cisco series 870, 1811, 1841, 2801, 2811, 2821 y 2851
- Routers Cisco series 3725, 3745, 3825, 3845, 7200 y 7301

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Una imagen avanzada del Cisco IOS Software Release 12.4(6)T o posterior
- Una de las plataformas del router de Cisco enumeradas en la introducción

Componentes Utilizados

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

- Cisco 3825 router
- Imagen avanzada de Enterprise software Cisco IOS Software Release 12.4(9)T
- Cisco Router y Security Device Manager (SDM) versión 2.3.1

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. Las direcciones IP utilizadas en este ejemplo se extraen de las direcciones RFC 1918 que son privados y no es legal utilizarlas en Internet.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Tareas de Preconfiguración

Antes de comenzar, complete estas tareas:

- 1. Configure un nombre de host y un nombre de dominio.
- 2. Configure el router para el SDM. Cisco envía algunos routers con una copia instalada previamente de SDM.Si Cisco SDM no está cargado en su router, puede obtener una copia gratuita del software de la página de <u>Descarga de Software (sólo clientes registrados)</u>. Debe tener una cuenta CCO con un contrato de servicio. Para obtener información detallada sobre la instalación y la configuración del SDM, consulte <u>Cisco Router y Security Device Manager</u>.
- 3. Configure la fecha, la hora, y el huso horario correctos para su router.

Configure el WebVPN en el Cisco IOS

Puede tener más de un gateway de WebVPN asociado a un dispositivo. Cada gateway de WebVPN se conecta a una sola dirección IP en el router. Puede crear más de un contexto de WebVPN para un gateway determinado del WebVPN. Para identificar los contextos individuales, proporcione cada contexto con un nombre único. Un grupo de políticas puede ser asociado a solamente un contexto del WebVPN. El grupo de políticas describe qué recursos están disponibles en un contexto determinado del WebVPN.

Siga estos pasos para configurar el WebVPN en el Cisco IOS:

- 1. Configure el Gateway del WebVPN
- 2. Configure los Recursos Permitidos para el Grupo de Políticas
- 3. Configure al Grupo de Políticas del WebVPN y Seleccione los Recursos
- 4. Configure el Contexto del WebVPN

5. Configure la Base de datos del Usuario y el Método de Autenticación

Paso 1. Configure el Gateway del WebVPN

Siga estos pasos para configurar el gateway del WebVPN:

- 1. Dentro de la aplicación de SDM, haga clic en Configure, y luego haga clic en VPN.
- 2. Amplie el WebVPN, y elija los Gateways del



3. Haga clic en Add (Agregar). Aparece el cuadro de diálogo Add Gateway

Add WebVPN Gat	eway				
Gateway Name:	WidgetSSLVPNGW1				
🔽 Enable Gatewa	y				
IP Address					
WebVPN clients will use this IP address and port number to connect to the WebVPN gateway.					
IP Address:	192.168.0.37	Port: 443			
Hostname:	ausnml-3825-01	(Optional)			
Enable secure	e SDM access through 192.1	168.0.37			
Digital Certifica	ate				
Digital Certificate	configured under this trustp hentication.	point will be sent to the			
Trustpoint:	ausnml-3825-01_Certifica	te 💌			
Redirect HTTP Traffic (Optional) Configure HTTP redirect so that clients accessing the portal page using HTTP will be automatically redirected to the secure HTTPS service that WebVPN uses.					
HTTP Port:	80				
	OK Cancel	Help			

Gateway.

- 4. Ingrese los valores en los campos Gateway Name e IP Address, y luego active la casilla de verificación **Enable Gateway.**
- 5. Active la casilla de verificación Redirect HTTP Traffic, y luego haga clic en OK.
- 6. Haga clic en **Guardar** y, a continuación, haga clic en **Sí** para aceptar los cambios.

Paso 2. Configure los Recursos Permitidos para el Grupo de Políticas

Para facilitar la adición de recursos a un grupo de políticas, puede configurar los recursos antes de que cree el grupo de políticas.

Siga estos pasos para configurar los recursos permitidos para el grupo de políticas:

1. Haga clic en **Configure**, y luego en **VPN**.



2. Elija **WebVPN**, y después haga clic en la pestaña **Edit WebVPN.Nota:** WebVPN le permite configurar el acceso para HTTP, HTTPS, la exploración de archivos de Windows a través del protocolo CIFS y

Citrix.



3. Haga clic en Add (Agregar). Aparece el cuadro de diálogo Add del WebVPN Context.

🚰 Cisco Router a	and Security Device	e Manager (SDM): 10.89	9.129.170					
File Edit View	Tools Help							ICCO SVETSME
🔥 Home	Configure	Monitor Refre	sh Save	C Search	P Help		Ĭ	dlussdlu.
Tasks	🐔 VPN							
Interfaces and Connections Frewal and ACL VPN Security Rudt Routing NRT NRT Dutrusion Prevention Cusity of Service NRC	VPN Ste-to-Si Easy VPN Gynamic WebVPN Packa VPN Con	Add WebVPN Context Add WebVPN Context Group Policie HTML Display NetBIOS Nam Port Forward URL Lists Cisco Secure	WebVPN Er	dit WebVPN Name: Associated Ga Domain: Authentication Authentication Finable Cont Maximum Num VRF Name: Default Group	teway: List: Domain: text hber of users: Policy:	 None 10000 <none></none>		
Additional Tasks				ок	Cancel	Help		
Configuration delive	ered to router.					15:50	11 UTC Wed Ju	1 26 2006 👩

4. Amplíe el **Contexto de WebVPN**, y elija las **Listas URL**.

Add WebVPN Context		
WebVPN Context Group Policies HTML Display Settings NetBIOS Name Server Lis Port Forward Lists URL Lists Cisco Secure Desktop	Group policies use URL Lists to expose through the portal page. URL List URL List Name	corporate URLs to the WebVPN users
	Item Name	Item Value
	OK Cancel Help	

5. Haga clic en Add (Agregar).El cuadro de diálogo AddURL

Add URL List	me: InternalWebServers WidgetWebServers	(This will appear	on Portal pag
Label	URL Link	Outlook Web Acces	Adr ⊽ Website E-mail
4	OK Cancel	Help	

- 6. Ingrese los valores en los campos URL List Name y Heading.
- 7. Haga clic en Add, y elija

Add URL List				
URL List Nar	me: InternalWebServers			
Heading:	WidgetWebServers	(This will appear on Portal page		
List of URLs:	:			
Label	URL Link	Outlook Web Acces Add 🗸		
WidgetWeb http://172.22.1.30				
OWA	http://172.22.1.50/exchang	Enabled Edit		
		Delete		
4				
	OK Cancel	Help		

Website.

sta lista contiene todos los servidores Web HTTP y HTTPS que desea que estén disponibles para esta conexión WebVPN.

- 8. Para agregar el acceso para Outlook Web Access (OWA), haga clic en Add, elija el E-mail, y luego haga clic en OK una vez que ha completado todos campos deseados.
- Para permitir que el archivo de Windows explore CIFS, puede designar un servidor de Servicio de Nombre NetBIOS (NBNS) y configurar las partes apropiadas en el dominio de Windows en orden.De la lista de Contexto WebVPN, elija las Listas del Servidor de Nombre de

NetBIOS.

Add WebVPN Context			
WebVPN Context Group Policies HTML Display Settings NetBIOS Name Server Lis Port Forward Lists URL Lists Cisco Secure Desktop	The Common Internet File System feature uses NetBIOS name server the corporate Microsoft Windows File System to WebVPN users. Li: Add Edit Server Name		OS name servers to expose PN users.
	IP Address	Retry	Timeout
<	OK Cancel	Help	

Haga clic en Add (Agregar). Aparece el cuadro de diálogo Add NBNS Server List. Ingrese un nombre para la lista, y haga clic en AddAparece el cuadro de diálogo NBNS Server.

Sa Cisco Router and Security Device Manager (SDM): 10.89.129.170	
File Edit View Tools Help	
Home Configure State Save Search Help	CO SYSTEMS
Tesk Add WebVPN Context	
Image: Second of Contrast The Common Informat File System feature uses NetBIOS name servers to expose the corporate Microsoft Windows File System to WebVPN users. Edit: Image: Ed	Disable twe Status
	36. 300.6 .00

Si corresponde, active **el cuadro de diálogo Make This the Master Server.**Haga clic en OK, y luego haga clic en OK.

Paso 3. Configure al Grupo de Políticas del WebVPN y Seleccione los Recursos

Siga estos pasos para configurar el grupo de políticas del WebVPN y seleccionar los recursos:

- 1. Haga clic en **Configure**, y luego en **VPN**.
- 2. Amplíe el WebVPN, y elija el Contexto del WebVPN.



3. Elija las **Políticas del Grupo**, y haga clic en AddAparece el cuadro de diálogo Add Group Policy.

Add Group Policy			
General Clientless Thin Client SSL VPN Client (Full Tunnel)			
Name: Indicy 1			
Make this the default aroun policy for context			
- Nimeouts			
Client's WebVPN session will be disconnected if the client is connected longer than the session timeout or if the client is idle longer than the idle timeout.			
Idle Timeout 2100 (sec) Session Timeout: 43200 (sec)			
OK Cancel Help			

- 4. Ingrese un nombre para la nueva política, y active **la casilla de verificación Make this the default group policy for context.**
- 5. Haga clic en la pestaña policy for context situada en la parte superior del cuadro de diálogo.

eral Clientles	ss Thin Client SSL VPN Client (Full Tunnel)
- Clientless We	eb Browsing
Select a list of U	JRLs from the global list of URLs configured in this WebVPN context. The URLs
in this list appea	ar to the webypy client in the webypy portal page.
Action	URL List View
Select	InternalWebServers
	Add V
Hide URL ba	ar in the portal page 🔽 Enable Citrix
Enable Cl	IFS
Common Interr	IFS net File System(CIFS) allows users to view, create, or edit files on servers of Windows operating systems using a web browser. Use this feature to
Common Interr running Microso access shared	IFS net File System(CIFS) allows users to view, create, or edit files on servers oft Windows operating systems using a web browser. Use this feature to files in the corporate network from any public network using WebVPN. Specify
Common Interr running Microso access shared the WINS serve	IFS net File System(CIFS) allows users to view, create, or edit files on servers oft Windows operating systems using a web browser. Use this feature to I files in the corporate network from any public network using WebVPN. Specify er list.
Common Interr running Microso access shared the WINS serve	IFS net File System(CIFS) allows users to view, create, or edit files on servers oft Windows operating systems using a web browser. Use this feature to I files in the corporate network from any public network using WebVPN. Specify er list.
Common Interr running Microso access shared the WINS serve Read	IFS net File System(CIFS) allows users to view, create, or edit files on servers oft Windows operating systems using a web browser. Use this feature to I files in the corporate network from any public network using WebVPN. Specify ar list.
Enable Cl Common Interr running Microso access shared the WINS serve Read Write	IFS net File System(CIFS) allows users to view, create, or edit files on servers oft Windows operating systems using a web browser. Use this feature to I files in the corporate network from any public network using WebVPN. Specify er list.
Common Interr running Microso access shared the WINS serve Read Write NBNS Server L	IFS net File System(CIFS) allows users to view, create, or edit files on servers oft Windows operating systems using a web browser. Use this feature to I files in the corporate network from any public network using WebVPN. Specify er list.
Common Interr running Microso access shared the WINS serve Read Write NBNS Server L	IFS net File System(CIFS) allows users to view, create, or edit files on servers oft Windows operating systems using a web browser. Use this feature to I files in the corporate network from any public network using WebVPN. Specify ar list.
Common Interr running Microso access shared the WINS serve Read Write NBNS Server L	IFS net File System(CIFS) allows users to view, create, or edit files on servers oft Windows operating systems using a web browser. Use this feature to I files in the corporate network from any public network using WebVPN. Specify ar list.

- 6. Active la casilla de verificación Select para la lista URL deseada.
- 7. Si sus clientes utilizan clientes Citrix que necesitan el acceso a los servidores Citrix, active la casilla de verificación **Enable Citrix.**
- 8. Active las casillas de verificación, Enable CIFS y Read y Write.
- 9. Haga clic en la flecha desplegable NBNS Server List, y elija la lista de servidores NBNS que creó para la exploración del archivo de Windows en el Paso 2.
- 10. Click OK.

Paso 4. Configure el Contexto del WebVPN

Para conectar el gateway del WebVPN, el grupo de políticas, y los recursos, debe configurar el contexto del WebVPN. Para configurar el contexto del WebVPN, siga estos pasos:

1. Elija el **contexto del WebVPN**, e ingrese un nombre para el contexto.

Add WebVPN Context			 X
WebVPN Context Group Policies HTML Display Settings NetBIOS Name Server Lis Port Forward Lists URL Lists Cisco Secure Desktop	Name: Associated Gateway: Domain: Authentication List: Authentication Domain: I Enable Context Maximum Number of users: VRF Name: Default Group Policy:	SalesContext WidgetSSLVPNGW1 None	
	OK Cancel	Help	

- 2. Haga clic en la flecha desplegable Gateway, y elija un gateway asociado.
- 3. Si se pretende crear más de un contexto, ingrese un nombre único en el campo del dominio para identificar este contexto. Si deja en blanco el campo Dominio, los usuarios deben acceder al WebVPN con https://IPAddress. Si ingresa un nombre de dominio (por ejemplo, *Ventas*), los usuarios deben conectarse con https://IPAddress/Sales.
- 4. Active la casilla de verificación Enable Context.
- 5. En el campo Maximum Number of Users, ingrese la cantidad máxima de usuarios permitida por la licencia del dispositivo.
- 6. Haga clic en la flecha desplegable **Default Group policy y seleccione la política del grupo para asociarse a este contexto.**
- 7. Haga clic en OK, y luego haga clic en OK.

Paso 5. Configure la Base de datos del Usuario y el Método de Autenticación

Puede configurar las sesiones del Clientless SSL VPN (WebVPN) para autenticar con Radius, el Cisco AAA Server, o la base de dato local Este ejemplo utiliza la base de datos local.

Siga estos pasos para configurar la base de datos de usuarios y el método de autenticación:

- 1. Haga clic en Configuration, y luego en Additional Tasks.
- 2. Amplie el Acceso al Router, y elija las Cuentas de Usuario/Ver.

🚰 Cisco Router	🔂 Cisco Router and Security Device Manager (SDM): 10.89.129.170				
File Edit View	Tools Help				
🔥 Home	Configure S Monitor	Refresh Save	C 🌮 Search Help		CISCO SYSTEMS
Tesks	Additional Tasks				
-	P - Router Properties P - Router Access	User Accounts/View			Add Edit Delete
Interfaces and	- VTY	Usemame	Password	Privilege Level	View Name
	- Management Access	admin austin		15	<none></none>
S1.	SSH	ausnml	*******	15	<none></none>
Firewall and RCL	Secure Device Provisioning	fallback	*********	15	<none></none>
~~					I
- 👘	Dynamic DNS Methods				
UPN	B-ACL Editor				
C 20	Port to Application Mapping	8			
	B- AAA				
Security Audit	Local Pools				
<u>↓</u>	Router Provisioning Configuration Management				
Routing					
6.4					
Cart and					
NRT					
Q					
Indusion Prevencion					
1007					
Quality of Service					
2					
NRC					
(7)					
Additional Tasks	•				
Additional Tasks				17:12:15	5 UTC Wed Jul 26 2006 👩

3. 'Haga clic en el botón Add (Agregar).'Aparece el cuadro de diálogo Add an

dd an Account	
Enter the username and password	
Username:	sales_user1
Password	
Password	<none></none>
New Password:	****
Confirm New Password:	****
Encrypt password using MD5 has	sh algorithm
Privilege Level:	5
Associate a View with the use	er
View Name : SDM_Administrator((root) 💌 View Details
OK Cancel	Help
	dd an Account Enter the username and password Username: Password Password New Password: Confirm New Password: ✓ Encrypt password using MD5 has Privilege Level: ✓ Associate a View with the use View Name : SDM_Administrator

- 4. Ingrese una cuenta de usuario y una contraseña.
- 5. Haga clic en OK, y luego haga clic en OK.
- 6. Haga clic en Guardar y, a continuación, haga clic en Sí para aceptar los cambios.

Resultados

El ASDM crea estas configuraciones de línea de comandos:

ausnml-3825-01
Building configuration
Current configuration : 4190 bytes ! ! Last configuration change at 17:22:23 UTC Wed Jul 26 2006 by ausnml

```
NVRAM config last updated at 17:22:31 UTC Wed Jul 26
2006 by ausnml
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname ausnml-3825-01
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
no logging buffered
enable secret 5 $1$KbIu$508qKYAVpWvyv9rYbrJLi/
aaa new-model
1
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization exec default local
1
aaa session-id common
resource policy
1
ip cef
ip domain name cisco.com
voice-card 0
no dspfarm
1
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 29312730 2506092A 864886F7 0D010902
16186175 736E6D6C 2D333832 352D3031 2E636973 636F2E63
6F6D301E 170D3036 30373133 32333230 34375A17 0D323030
31303130 30303030 305A3029 31273025 06092A86 4886F70D
01090216 18617573 6E6D6C2D 33383235 2D30312E 63697363
6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281 8100C97D 3D259BB7 3A48F877 2C83222A
A1E9E42C 5A71452F 9107900B 911C0479 4D31F42A 13E0F63B
E44753E4 0BEFDA42 FE6ED321 8EE7E811 4DEEC4E4 319C0093
C1026C0F 38D91236 6D92D931 AC3A84D4 185D220F D45A411B
09BED541 27F38EF5 1CC01D25 76D559AE D9284A74 8B52856D
BCBBF677 0F444401 D0AD542C 67BA06AC A9030203 010001A3
78307630 0F060355 1D130101 FF040530 030101FF 30230603
551D1104 1C301A82 18617573 6E6D6C2D 33383235 2D30312E
63697363 6F2E636F 6D301F06 03551D23 04183016 801403E1
5EAABA47 79F6C70C FBC61B08 90B26C2E 3D4E301D 0603551D
0E041604 1403E15E AABA4779 F6C70CFB C61B0890 B26C2E3D
4E300D06 092A8648 86F70D01 01040500 03818100 6938CEA4
2E56CDFF CF4F2A01 BCD585C7 D6B01665 595C3413 6B7A7B6C
F0A14383 4DA09C30 FB621F29 8A098FA4 F3A7F046 595F51E6
7C038112 0934A369 D44C0CF4 718A8972 2DA33C43 46E35DC6
5DCAE7E0 B0D85987 A0D116A4 600C0C60 71BB1136 486952FC
55DE6A96 1135C9D6 8C5855ED 4CD3AE55 BDA966D4 BE183920
```

```
88A8A55E quit username admin privilege 15 secret 5
$1$jm6N$2xNfhupbAinq3BQZMRzrW0 username ausnml privilege
15 password 7 15071F5A5D292421 username fallback
privilege 15 password 7 08345818501A0A12 username austin
privilege 15 secret 5 $1$3xFv$W0YUsKDx1adDc.cVQF2Ei0
username sales_user1 privilege 5 secret 5
$1$2/SX$ep4fsCpodeyKaRji2mJkX/ ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! ip route
0.0.0.0 0.0.0.0 172.22.1.1 ! ip http server ip http
authentication local ip http timeout-policy idle 600
life 86400 requests 100 ! control-plane ! line con 0
stopbits 1 line aux 0 stopbits 1 line vty 0 4 exec-
timeout 40 0 privilege level 15 password 7
071A351A170A1600 transport input telnet ssh line vty 5
15 exec-timeout 40 0 password 7 001107505D580403
transport input telnet ssh ! scheduler allocate 20000
1000 ! !--- WebVPN Gateway webvpn gateway
WidgetSSLVPNGW1 hostname ausnml-3825-01 ip address
192.168.0.37 port 443 http-redirect port 80 ssl
trustpoint ausnml-3825-01_Certificate inservice ! webvpn
context SalesContext ssl authenticate verify all ! !---
Identify resources for the SSL VPN session url-list
"InternalWebServers" heading "WidgetWebServers" url-text
"WidgetWeb" url-value "http://172.22.1.30" url-text
"OWA" url-value "http://172.22.1.50/exchange" ! nbns-
list NBNSServers nbns-server 172.22.1.30 ! !--- Identify
the policy which controls the resources available policy
group policy_1 url-list "InternalWebServers" nbns-list
"NBNSServers" functions file-access functions file-
browse functions file-entry hide-url-bar citrix enabled
default-group-policy policy_1 gateway WidgetSSLVPNGW1
max-users 2 inservice ! end
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Procedimiento

Siga estos procedimientos para confirmar que su configuración funciona correctamente:

 Pruebe su configuración con un usuario. Ingrese https://WebVPN_Gateway_IP_Address en un explorador Web con SSL habilitado; donde WebVPN_Gateway_IP_Address es la dirección IP del servicio WebVPN. Después de que valide el certificado e ingrese un Nombre de usuario y una contraseña, una pantalla similar a esta imagen debe aparecer.

WebVPN Service			? • 6 ×	
If the Floating Toolbar does not open, click here to open it.				
Websites				
Tacacs Enter Web Add	ress (URL)	Go		
Thttps://192.168.0.37 - WebVPN Service Toolbar	Browse Network			
Websites				
Tececs Go				
Go Go				
2 Streemet				

- Verifique la sesión de VPN SSL. Dentro de la aplicación SDM, haga clic en el botón Monitor, y después haga clic en VPN Status. Amplíe el WebVPN (todos los contextos), amplíe el contexto apropiado, y elija los usuarios.
- Verifique los mensajes de error. Dentro de la aplicación de SDM, haga clic el botón Monitor, haga clic en Logging, y luego haga clic en la pestaña Syslog.
- Vea la configuración en ejecución para el dispositivo. Dentro de la aplicación de SDM, haga clic en el **botón Configure, y después haga clic en Additional Tasks**. Amplíe la **Administración de la Configuración**, y elija el **Editor de Configuración**.

Comandos

Varios **comandos show se asocian a WebVPN.** Puede ejecutar estos comandos en command-line interface (CLI) para mostrar las estadísticas y otra información. Para obtener información detallada sobre los **comandos show, consulte** <u>Verificar la Configuración WebVPN</u>.

Nota: La <u>Herramienta Output Interpreter</u> (<u>sólo</u> clientes registrados) (OIT) admite determinados comandos <u>show</u>. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshoot

Use esta sección para resolver problemas de configuración.

Nota: No interrumpa el comando **Copy File to Server** ni navegue a una ventana diferente mientras la copia está en curso. La interrupción de la operación puede hacer que un archivo incompleto sea guardado en el servidor.

Nota: Los usuarios pueden cargar y descargar los nuevos archivos mediante el cliente WebVPN, pero no se permite que el usuario sobrescriba los archivos en el sistema de archivos comunes de Internet (CIFS) en WebVPN mediante el comando **Copy File to Server**. El usuario recibe este mensaje cuando el usuario intenta substituir un archivo en el servidor:

Procedimiento

Siga estos pasos para resolver problemas con su configuración:

- 1. Asegúrese de que los clientes inhabilitaron los bloqueadores emergentes.
- 2. Asegúrese de que los clientes habiliten las cookies.
- 3. Asegúrese de que los clientes usen Netscape, Internet Explorer, Firefox, o los exploradores Web de Mozilla.

Comandos

Varios **comandos debug se asocian a WebVPN.** Consulte <u>Uso de los Comandos Debug del</u> <u>WebVPN para obtener información detallada sobre estos comandos.</u>

Nota: El uso de los comandos **debug** puede afectar negativamente a su dispositivo Cisco. Antes de que utilice los **comandos debug, consulte** <u>Información Importante sobre los Comandos Debug</u>.

Información Relacionada

- <u>Cisco IOS SSLVPN</u>
- Preguntas Y Respuestas de Cisco IOS SSLVPN
- Ejemplo de la Configuración IOS de Thin-Client SSL VPN (WebVPN) con SDM
- Ejemplo de Configuración de SSL VPN Client (SVC) en IOS con SDM
- Soporte Técnico y Documentación Cisco Systems