Ejemplo de Configuración de SSL VPN Client (SVC) en IOS con SDM

Contenido

Introducción

SSL VPN Client (SVC) proporciona un túnel completo para las comunicaciones seguras a la red interna corporativa. Usted puede configurar el acceso en un usuario por la base del usuario, o usted puede crear diversos contextos del WebVPN en los cuales usted coloque a uno o más usuarios.

La SSL VPN o la tecnología WebVPN es soportada en estas plataformas del router IOS:

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

Usted puede configurar la tecnología VPN SSL en estos modos:

- **Clientless SSL VPN (WebVPN)** — Proporciona a un cliente remoto que requiera a un buscador Web SSL-habilitado acceder a los servidores Web HTTP o HTTPS en un red de

área local (LAN) corporativo. Además, el clientless SSL VPN proporciona el acceso para el archivo de Windows que hojea con el protocolo del Common Internet File System (CIFS). El Acceso Web de la perspectiva (OWA) es un acceso del ejemplo de HTTP.Refiera al clientless SSL VPN (WebVPN) en el Cisco IOS con el ejemplo de la configuración de SDM para aprender más sobre el clientless SSL VPN.

- **El cliente "liviano" SSL VPN (expedición del puerto)** — proporciona a un cliente remoto que descargue un pequeño applet de la Java basada y permite el acceso seguro para las aplicaciones del Transmission Control Protocol (TCP) que utilizan los números del puerto estático. El Point of Presence (POP3), el Simple Mail Transfer Protocol (SMTP), el Internet Message Access Protocol (IMAP), el Secure Shell (SSH), y Telnet son ejemplos del acceso seguro. Porque los archivos en la máquina local cambian, los usuarios deben tener privilegios administrativos locales de utilizar este método. Este método de SSL VPN no trabaja con las aplicaciones que utilizan las asignaciones de puerto dinámico, tales como algunas aplicaciones del File Transfer Protocol (FTP).Consulte Ejemplo de Configuración de Thin-Client SSL VPN (WebVPN) IOS con SDM para obtener más información sobre la thin-client SSL VPN.**Note**: El User Datagram Protocol (UDP) no se soporta.
- **Cliente VPN SSL (modo túnel completo de SVC)** — descarga a un pequeño cliente a la estación de trabajo remota y permite el acceso seguro completo a los recursos en una red corporativa interna. Usted puede descargar SVC a una estación de trabajo remota permanentemente, o usted puede quitar al cliente una vez que la sesión segura es cerrada.

Este documento demuestra la configuración de un router del Cisco IOS para uso de un cliente VPN SSL.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Microsoft Windows 2000 o XP
- Navegador Web con SUN JRE 1.4 o una versión posterior o un navegador controlado ActiveX
- Privilegios administrativos locales en el cliente
- Uno del Routers enumerado en la introducción con una imagen de la Seguridad avanzada (12.4(6)T o más adelante)
- Versión 2.3 del (SDM) del administrador de dispositivo Security de CiscoSi Cisco SDM no está cargado en su router, puede obtener una copia gratuita del software de la página de Descarga de Software (sólo clientes registrados). Debe tener una cuenta CCO con un contrato de servicio. Para obtener información detallada sobre la instalación y la configuración del SDM, consulte Cisco Router y Security Device Manager.
- Un certificado digital en el routerUsted puede utilizar un certificado autofirmado persistente o un Certificate Authority (CA) externo para satisfacer este requisito. Para más información sobre los certificados autofirmados persistentes, refiera a los certificados autofirmados persistentes.

Componentes Utilizados

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

hardware.

- 3825 Series del router del Cisco IOS con 12.4(9)T
- Versión 2.3.1 del (SDM) del Administrador de dispositivos de seguridad

Note: La información de este documento se originó a partir de dispositivos dentro de 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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Tareas de Preconfiguración

1. Configure el router para el SDM. (Opcional)El Routers con la licencia apropiada del conjunto de la Seguridad tiene ya la aplicación del SDM cargada en el flash. Refiera a la transferencia y a instalar el (SDM) de Router de Cisco y Administrador de dispositivo de seguridad para obtener y para configurar el software.
2. Descargue una copia de SVC a su Administración PC.Usted puede obtener una copia del archivo de paquete de SVC de la descarga del software: Cliente Cisco SSL VPN (clientes registrados solamente). Usted debe tener una cuenta válida CCO con un contrato de servicio.
3. Fije la fecha, la hora, y el huso horario correctos, y después configure un certificado digital en el router.

Convenciones

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

Antecedentes

SVC se carga inicialmente sobre el router de gateway del WebVPN. Cada vez que el cliente conecta, una copia de SVC se descarga dinámicamente sobre el PC. Para cambiar este comportamiento, configure al router para permitir al software para permanecer permanentemente en la computadora cliente.

Configure SVC en el IOS

En esta sección, se presentan los pasos necesarios para configurar las funciones descritas en este documento. Este ejemplo de configuración utiliza al Asisitente del SDM para habilitar la operación de SVC en el router IOS.

Complete estos pasos para configurar SVC en el router IOS:

1. Instale y habilite el software de SVC en el router IOS
2. Configure un contexto del WebVPN y un gateway del WebVPN con el Asisitente del SDM

3. Configure la base de datos de usuarios para los usuarios de SVC
4. Configure los Recursos para Mostrar a los Usuarios

Paso 1. Instale y habilite el software de SVC en el router IOS

Complete estos pasos para instalar y habilitar el software de SVC en el router IOS:

1. Abra la aplicación del SDM, haga clic la **configuración**, y después haga clic el **VPN**.
2. Amplíe el **WebVPN**, y elija los **paquetes**.
3. Dentro del área del software de cliente del WebVPN de Cisco, haga clic el **botón Browse**.El cuadro de diálogo selecto de la ubicación de SVC aparece.
4. Haga clic el botón de radio del **mi PC**, y después haga clic **hojean** para localizar el paquete de SVC en su Administración PC.
5. El Haga Click en OK, y entonces hace clic el **botón Install Button**.
6. Haga clic en **Yes** y luego en **OK**.Un acertado instala del paquete de SVC se muestra en esta imagen:

Paso 2. Configure un contexto del WebVPN y un gateway del WebVPN con el Asisitente del SDM

Complete estos pasos para configurar un contexto del WebVPN y un gateway del WebVPN:

1. Después de que SVC esté instalado en el router, haga clic la **configuración**, y después haga clic el **VPN**.
2. Haga clic el **WebVPN**, y haga clic la lengueta del **WebVPN del crear**.
3. Marque el **crear un nuevo** botón de radio del **WebVPN**, y después haga clic el **lanzamiento la tarea seleccionada**.El cuadro de diálogo del Asisitente del WebVPN aparece.
4. Haga clic en Next (Siguiente).
5. Ingrese el IP Address del nuevo gateway del WebVPN, y ingrese un nombre único para este contexto del WebVPN.Usted puede crear diversos contextos del WebVPN para la misma dirección IP (gateway del WebVPN), pero cada nombre debe ser único. Este ejemplo utiliza esta Dirección IP: *https://192.168.0.37/sales*
6. Haga clic en **Next** y continúe con el Paso 3.

Paso 3. Configure la base de datos de usuarios para los usuarios de SVC

Para la autenticación, puede utilizar un Servidor AAA, los usuarios locales, o ambos. Este ejemplo de configuración utiliza los usuarios creados localmente para la autenticación.

Complete estos pasos para configurar la base de datos de usuarios para los usuarios de SVC:

1. Después de que usted complete el paso 2, haga clic **localmente encendido el este** botón de radio del **router** situado en el cuadro de diálogo de la autenticación de usuario del Asisitente del WebVPN.Este cuadro de diálogo le permite agregar usuarios a las bases de datos locales.
2. Haga clic en **Add** e ingrese la información de usuario.
3. Haga clic en OK y agregue usuarios adicionales, de ser necesario.
4. Una vez que agregue la cantidad necesaria de usuarios, haga clic en **Next** y continúe con el

Paso 4.

Paso 4. Configure los recursos para exponer a los usuarios

El cuadro de diálogo del Asisitente del WebVPN de los sitios web del Intranet de la configuración permite que usted seleccione los recursos del intranet que usted quiere para exponer a su SVC a los clientes.

Complete estos pasos para configurar los recursos para exponer a los usuarios:

1. Después de que usted complete el paso 3, haga clic el **botón Add** situado en el cuadro de diálogo de los sitios web del Intranet de la configuración.
2. Ingrese un nombre de la lista url, y después ingrese un título.
3. El tecleo **agrega**, y elige el **sitio web** para agregar los sitios web que usted quiere exponer a este cliente.
4. Ingrese el URL y la información de link, y después haga clic la **AUTORIZACIÓN**.
5. Para agregar el acceso a los servidores Exchange OWA, el tecleo **agrega** y elige el **email**.
6. Marque la casilla de verificación del **Acceso Web de la perspectiva**, ingrese la escritura de la etiqueta URL y la información de link, y después haga clic la **AUTORIZACIÓN**.
7. Después de que usted agregue los recursos deseados, haga clic la **AUTORIZACIÓN**, y después haga clic **después**.El cuadro de diálogo lleno del túnel del Asisitente del WebVPN aparece.
8. Verifique que la casilla de verificación **Enable Full Tunnel** esté activada.
9. Cree un pool de los IP Addresses que los clientes de este contexto del WebVPN puedan utilizar. El conjunto de direcciones debe corresponder a las direcciones disponibles y ruteables en su Intranet.
10. Haga clic las elipses (**…**) al lado de la dirección IP reúna el campo, y elija **crean a una nueva agrupación IP**.
11. En el cuadro de diálogo de la agrupación local IP del agregar, ingrese un nombre para el pool, y el haga click en Add
12. En el cuadro de diálogo del alcance del IP Address del agregar, ingrese el rango de la agrupación de direcciones para los clientes SVC, y haga clic la **AUTORIZACIÓN**.**Note**: El pool de la dirección IP debe estar en un rango de una interfaz conectada directamente con el router. Si usted quiere utilizar un diverso rango del pool, usted puede crear un Loopback Address asociado a su nuevo pool para satisfacer este requisito.
13. Click OK.
14. Si usted quisiera que sus clientes remotos salvaran permanentemente una copia del tecleo de SVC la **custodia el software de cliente completo del túnel instaló en la** casilla de verificación **PC del cliente**. Borre esta opción para requerir al cliente descargar el software de SVC cada vez que un cliente conecta.
15. Configure las opciones de túnel avanzadas, como tunelización dividida, DNS dividido, configuraciones proxy del navegador y servidores DNS y WNS. Cisco le recomienda configurar al menos servidores DNS y WINS.Para configurar opciones avanzadas de túnel, siga estos pasos:Haga clic en el botón **Advanced Tunnel Options**.Haga clic en la pestaña **DNS and WINS Servers** e ingrese las direcciones IP principales para los servidores DNS y WINS.Para configurar las configuraciones de representación del Túnel dividido y del navegador, haga clic la lengueta de las **configuraciones de representación del Túnel dividido** o del **navegador**.

16. Después de que configure la opción necesaria, haga clic en **Next**.
17. Personalice la página porta del WebVPN o seleccione los valores predeterminados.La página porta del WebVPN del personalizar permite que usted personalice cómo la página porta del WebVPN aparece a sus clientes.
18. Después de que usted configure la página porta del WebVPN, el tecleo **después**, el clic en Finalizar, y entonces hacen clic la **AUTORIZACIÓN**.El Asisitente del WebVPN somete los comandos del viaje al router.
19. Haga Click en OK para salvar su configuración.**Note**: Si usted recibe un mensaje de error, la licencia del WebVPN puede ser incorrecta. Un mensaje de error de ejemplo se muestra en esta imagen:Para corregir un problema de licencia, siga estos pasos:Haga clic en **Configure**, y luego en **VPN**.Amplíe el **WebVPN**, y haga clic la lengueta del **WebVPN del editar**.Resalte su contexto creado recientemente, y haga clic en el botón **Edit**.En el campo Maximum Number of users, ingrese el número correcto de usuarios para su licencia.Haga clic en OK, y luego haga clic en **OK**.Sus comandos se escriben en el archivo de configuración.**La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.

Resultados

El ASDM crea estas configuraciones de la línea de comandos:

ausnml-3825-01

```
ausnml-3825-01#show run
Building configuration...

Current configuration : 4393 bytes
!
! Last configuration change at 22:24:06 UTC Thu Aug 3
2006 by ausnml
! NVRAM config last updated at 22:28:54 UTC Thu Aug 3
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
!
aaa new-model
!
!--- Added by SDM for local aaa authentication. aaa
authentication login sdm_vpn_xauth_ml_1 local aaa
authentication login sdm_vpn_xauth_ml_2 local aaa
authentication login sdm_vpn_xauth_ml_3 local aaa
authentication login sdm_vpn_xauth_ml_4 local ! aaa
session-id common ! resource policy ! ip cef ! ip domain
name cisco.com ! voice-card 0 no dspfarm !--- Digital
certificate information. crypto pki trustpoint TP-self-
signed-577183110 enrollment selfsigned subject-name
```

```
cn=IOS-Self-Signed-Certificate-577183110 revocation-
check none rsakeypair TP-self-signed-577183110 ! crypto
pki certificate chain TP-self-signed-577183110
certificate self-signed 01 3082024E 308201B7 A0030201
02020101 300D0609 2A864886 F70D0101 04050030 30312E30
2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
43657274 69666963 6174652D 35373731 38333131 30301E17
0D303630 37323731 37343434 365A170D 32303031 30313030
30303030 5A303031 2E302C06 03550403 1325494F 532D5365
6C662D53 69676E65 642D4365 72746966 69636174 652D3537
37313833 31313030 819F300D 06092A86 4886F70D 01010105
0003818D 00308189 02818100 F43F6DD9 32A264FE 4C5B0829
698265DC 6EC65B17 21661972 D363BC4C 977C3810 !--- Output
suppressed. quit username wishaw privilege 15 secret 5
$1$r4CW$SeP6ZwQEAAU68W9kbR16U. username ausnml privilege
15 password 7 044E1F505622434B username sales privilege
15 secret 5 $1$/Lc1$K.Zt41zF1jSdKZrPgNK1A. username
newcisco privilege 15 secret 5
$1$Axlm$7k5PWspXKxUpoSReHo7IQ1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
ip virtual-reassembly duplex auto speed auto media-type
rj45 no keepalive ! interface GigabitEthernet0/1 ip
address 172.22.1.151 255.255.255.0 duplex auto speed
auto media-type rj45 !--- Clients receive an address
from this pool. ip local pool Intranet 172.22.1.75
172.22.1.95 ip route 0.0.0.0 0.0.0.0 172.22.1.1 ! ip
http server ip http authentication local ip http secure-
server 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 ! scheduler allocate
20000 1000 !--- Identify the gateway and port. webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint TP-self-signed-577183110
inservice !--- SVC package file. webvpn install svc
flash:/webvpn/svc.pkg ! !--- WebVPN context. webvpn
context sales title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all ! !---
Resources available to this context. url-list
"WebServers" heading "Intranet Web" url-text "SalesSite"
url-value "http://172.22.1.10" url-text "OWAServer" url-
value "http://172.22.1.20/exchange" ! nbns-list NBNS-
Servers nbns-server 172.22.1.15 master !--- Group policy
for the context. policy group policy_1 url-list
"WebServers" functions svc-enabled svc address-pool
"Intranet" svc default-domain "cisco.com" svc keep-
client-installed svc dns-server primary 172.22.1.100 svc
wins-server primary 172.22.1.101 default-group-policy
policy_1 aaa authentication list sdm_vpn_xauth_ml_4
gateway gateway_1 domain sales max-users 2 inservice ! !
end
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Procedimiento

Para probar su configuración, ingrese *http://192.168.0.37/sales* en un buscador Web SSL-habilitado del cliente.

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 Verificar la Configuración WebVPN.

Note: 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.

Troubleshooting

Use esta sección para resolver problemas de configuración.

Problema de Conectividad SSL

Problema: Los clientes VPN SSL no pueden conectarse con el router.

Solución: El número insuficiente de direcciones IP en el conjunto de direcciones IP puede causar este problema. Aumente el número de direcciones IP en el conjunto de direcciones IP en el router para resolver este problema.

Comandos para resolución de problemas

Varios **comandos clear se asocian a** WebVPN. Para obtener información detallada sobre estos comandos, consulte Uso de los Comandos Clear de WebVPN.

Varios **comandos debug se asocian a** WebVPN. Para obtener información detallada sobre estos comandos, consulte Uso de los Comandos Debug de WebVPN.

Note: El uso de los **comandos debug** puede afectar negativamente su dispositivo de Cisco. Antes de que utilice los **comandos debug**, consulte Información Importante sobre los Comandos Debug.

Información Relacionada

- Cisco IOS SSLVPN
- SSL VPN - WebVPN
- Ejemplo de Clientless SSL VPN (WebVPN) en Cisco IOS con la Configuración de SDM
- Ejemplo de la Configuración IOS de Thin-Client SSL VPN (WebVPN) con SDM
- Guía de Implementación y Convergencia de WebVPN y DMVPN
- Soporte Técnico y Documentación - Cisco Systems