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. Puede configurar el acceso usuario por usuario o puede crear diferentes contextos WebVPN en los que coloque 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

Puede configurar la tecnología SSL VPN en estos modos:

- Clientless SSL VPN (WebVPN): proporciona un cliente remoto que requiere un navegador web habilitado para SSL para acceder a los servidores web HTTP o HTTPS en una red de

área local (LAN) corporativa. Además, la VPN SSL sin cliente proporciona acceso para la exploración de archivos de Windows a través del protocolo CIFS (sistema común de archivos de Internet). Outlook Web Access (OWA) es un ejemplo de acceso HTTP.

Consulte Ejemplo de Configuración de Clientless SSL VPN (WebVPN) en Cisco IOS con SDM para obtener más información sobre Clientless SSL VPN.

- Thin-Client SSL VPN (reenvío de puertos): proporciona un cliente remoto que descarga un pequeño applet basado en Java y permite el acceso seguro para aplicaciones de protocolo de control de transmisión (TCP) que utilizan números de puerto estáticos. El punto de presencia (POP3), el protocolo simple de transferencia de correo (SMTP), el protocolo de acceso a mensajes de Internet (IMAP), el shell seguro (ssh) y Telnet son ejemplos de acceso seguro. Dado que los archivos del equipo local cambian, los usuarios deben tener privilegios administrativos locales para utilizar este método. Este método de VPN SSL no funciona con aplicaciones que utilizan asignaciones de puertos dinámicos, como algunas aplicaciones de protocolo de transferencia de archivos (FTP).

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

  Nota: El protocolo de datagramas de usuario (UDP) no es compatible.

- SSL VPN Client (SVC Full Tunnel Mode): descarga un cliente pequeño a la estación de trabajo remota y permite un acceso totalmente seguro a los recursos de una red corporativa interna. Puede descargar el SVC a una estación de trabajo remota permanentemente, o puede quitar el cliente una vez que se cierre la sesión segura.

Este documento demuestra la configuración de un router Cisco IOS para su uso por parte de un SSL VPN Client.

Prerequisites

Requirements

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 de los routers enumerados en la Introducción con una imagen de Seguridad avanzada (12.4(6)T o posterior)
- Cisco Security Device Manager (SDM) versión 2.3

  Si 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 router

  Puede utilizar un certificado autofirmado persistente o una autoridad de certificación (CA) externa para cumplir este requisito. Para obtener más información sobre los certificados autofirmados persistentes, consulte Certificados Autofirmados Persistentes.

Componentes Utilizados

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

- Cisco IOS Router serie 3825 con 12.4(9)T
- Administrador de dispositivos de seguridad (SDM) versión 2.3.1

Nota: La información de este documento se creó a partir de dispositivos en un entorno de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Tareas de Preconfiguración

1. Configure el router para SDM. (Opcional)

   Los routers con la licencia de paquete de seguridad adecuada ya tienen la aplicación SDM cargada en flash. Consulte Descarga e Instalación del Router de Cisco y el Administrador del Dispositivo de Seguridad (SDM) para obtener y configurar el software.

2. Descargue una copia del SVC en el PC de administración.

   Puede obtener una copia del archivo del paquete SVC en Descarga de Software: Cisco SSL VPN Client (sólo para clientes registrados) . Debe tener una cuenta CCO válida con un contrato de servicio.

3. Establezca la fecha, hora y zona horaria correctas y, a continuación, 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

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

Configuración de SVC en IOS

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

Complete estos pasos para configurar el SVC en el router IOS:

1. Instalación y activación del software SVC en el router IOS
2. Configuración de un Contexto WebVPN y un Gateway WebVPN con el Asistente SDM
3. Configuración de la Base de Datos de Usuarios para Usuarios SVC
4. Configure los Recursos para Mostrar a los Usuarios

Paso 1. Instalación y activación del software SVC en el router IOS

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

1. Abra la aplicación SDM, haga clic en Configure y, a continuación, haga clic en VPN.
2. Amplíe WebVPN, y elija Paquetes.
3. Dentro del área Cisco WebVPN Client Software, haga clic en el botón Browse.

   Aparecerá el cuadro de diálogo Seleccionar ubicación de SVC.
4. Haga clic en el botón de opción Mi PC y, a continuación, haga clic en Examinar para localizar el paquete SVC en el PC de administración.
5. Haga clic en Aceptar y, a continuación, haga clic en el botón Instalar.
6. Haga clic en Yes y luego en OK.

   En esta imagen se muestra una instalación exitosa del paquete SVC:

Paso 2. Configuración de un Contexto WebVPN y un Gateway WebVPN con el Asistente SDM

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

1. Una vez que el SVC esté instalado en el router, haga clic en Configure y luego en VPN.
2. Haga clic en WebVPN, y haga clic en la pestaña Create WebVPN.
3. Marque el botón de opción Create a New WebVPN y, a continuación, haga clic en Launch the selected task.

   Aparecerá el cuadro de diálogo Asistente para WebVPN.
4. Haga clic en Next (Siguiente).
5. Introduzca la dirección IP del nuevo gateway WebVPN e introduzca un nombre único para este contexto WebVPN.

   Puede crear contextos WebVPN diferentes para la misma dirección IP (gateway 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. Configuración de la Base de Datos de Usuarios para Usuarios 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 SVC:

1. Después de completar el Paso 2, haga clic en el botón de opción Locally on this router ubicado en el cuadro de diálogo WebVPN Wizard User Authentication.

   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 Mostrar a los Usuarios

El cuadro de diálogo Configurar sitios Web de intranet Asistente para WebVPN le permite seleccionar los recursos de intranet que desea exponer a los clientes SVC.

Complete estos pasos para configurar los recursos que se expondrán a los usuarios:

1. Después de completar el Paso 3, haga clic en el botón Add ubicado en el cuadro de diálogo Configure Intranet Websites.
2. Escriba un nombre de lista de direcciones URL y, a continuación, un encabezado.

3. Haga clic en Agregar y elija Sitio web para agregar los sitios web que desea exponer a este cliente.

4. Introduzca la URL y la información de enlace y, a continuación, haga clic en Aceptar.

5. Para agregar acceso a OWA Exchange Servers, haga clic en Add y elija E-mail.

6. Marque la casilla de verificación Outlook Web Access, escriba la etiqueta de la dirección URL y la información del vínculo y, a continuación, haga clic en Aceptar.

7. Después de agregar los recursos deseados, haga clic en Aceptar y, a continuación, haga clic en Siguiente.

   Aparecerá el cuadro de diálogo de túnel completo del Asistente de WebVPN.

8. Verifique que la casilla de verificación Enable Full Tunnel esté activada.

9. Cree un conjunto de direcciones IP que los clientes de este contexto WebVPN puedan utilizar. El conjunto de direcciones debe corresponder a las direcciones disponibles y ruteables en su Intranet.

10. Haga clic en los puntos suspensivos (...) junto al campo IP Address Pool y elija Create a new IP Pool.

11. En el cuadro de diálogo Add IP Local Pool, ingrese un nombre para el pool y haga clic en Add.

12. En el cuadro de diálogo Add IP address range, ingrese el rango de conjunto de direcciones para los clientes SVC y haga clic en OK.

    Nota: El conjunto de direcciones IP debe estar en un rango de una interfaz conectada directamente al router. Si desea utilizar un intervalo de conjunto diferente, puede crear una dirección de bucle invertido asociada a su nuevo conjunto para satisfacer este requisito.

13. Click OK.

14. Si desea que sus clientes remotos almacenen permanentemente una copia del SVC, haga clic en la casilla de verificación Keep the Full Tunnel Client Software installed on client's PC. Desactive esta opción para solicitar al cliente que descargue el software SVC cada vez que un cliente se conecte.

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:

    a. Haga clic en el botón Advanced Tunnel Options.

    b. Haga clic en la pestaña DNS and WINS Servers e ingrese las direcciones IP

principales para los servidores DNS y WINS.

c. Para configurar la tunelización dividida y los ajustes de proxy del explorador, haga clic en la pestaña Tunelización dividida o Configuración de proxy del explorador.

16. Después de que configure la opción necesaria, haga clic en Next.

17. Personalice la página del portal WebVPN o seleccione los valores predeterminados.

    La página Personalizar el portal WebVPN le permite personalizar la forma en que la página WebVPN Portal se muestra a sus clientes.

18. Después de configurar la página del portal WebVPN, haga clic en Next, haga clic en Finish y luego haga clic en OK.

    El asistente de WebVPN envía comandos tour al router.

19. Haga clic en Aceptar para guardar la configuración.

    Nota: Si recibe un mensaje de error, es posible que la licencia de WebVPN sea incorrecta. En esta imagen se muestra un ejemplo de mensaje de error:

    Para corregir un problema de licencia, siga estos pasos:

    a. Haga clic en Configure, y luego en VPN.

    b. Expanda WebVPN y haga clic en la pestaña Edit WebVPN.

    c. Resalte su contexto creado recientemente, y haga clic en el botón Edit.

    d. En el campo Maximum Number of users, ingrese el número correcto de usuarios para su licencia.

    e. Haga clic en OK, y luego haga clic en OK.

       Sus comandos se escriben en el archivo de configuración.

    f. 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
<#root> 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 explorador Web cliente habilitado para SSL.

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.

Nota: La herramienta Output Interpreter Tool (sólo clientes registrados) (OIT) admite ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshoot

Use esta sección para resolver problemas de configuración.

Problema de Conectividad SSL

Problema: Los clientes SSL VPN no pueden conectar el router.

Solución: Este problema puede deberse a que las direcciones IP del grupo de direcciones IP no son suficientes. 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.

Nota: El uso de los comandos debug puede afectar negativamente a su dispositivo 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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).