Ejemplo de Configuración de SSL VPN Client (SVC) en ASA con ASDM

Contenido

Introducción

La tecnología del Red privada virtual (VPN) de Secure Socket Layer (SSL) permite conectar con seguridad desde cualquier ubicación con una red corporativa interna mediante uno de estos métodos:

- **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 ejemplo de configuración ASA 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 protocolo Post Office Protocol (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).Refiera al cliente "liviano" SSL VPN (WebVPN) en el ASA con el ejemplo de la Configuración de ASDM para aprender más sobre el cliente "liviano" SSL VPN.**Note**: El User Datagram Protocol (UDP) no se soporta.
- **Cliente VPN SSL (modo túnel)** — 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 el (SVC) del cliente VPN SSL a una estación de trabajo remota permanentemente, o usted puede quitar al cliente una vez que la sesión segura es cerrada.

Este documento describe cómo configurar SVC en un dispositivo de seguridad adaptante (ASA) usando el Administrador de dispositivos de seguridad adaptante (ASDM). Las líneas de comando que resultan de esta configuración se enumeran en la sección de los resultados.

prerrequisitos

Requisitos

Antes de utilizar esta configuración, asegúrese de que cumple con los siguientes requisitos:

- Soporte del comienzo de SVC de la versión de software adaptante 7.1 del dispositivo de seguridad de Cisco y posterior
- Privilegios administrativos locales en todas las estaciones de trabajo remotas
- Javas y controles ActiveX en la estación de trabajo remota
- El puerto 443 no se bloquea dondequiera a lo largo del trayecto de conexión

Componentes Utilizados

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

- Versión de software adaptante del dispositivo de seguridad de Cisco 7.2(1)
- Cisco Adaptive Security Device Manager 5.2(1)
- 5510 Series adaptantes del dispositivo de seguridad de Cisco
- Microsoft Windows XP SP2 profesional

La información en este documento fue desarrollada en un ambiente de laboratorio. Todos los dispositivos usados en este documento comenzado fueron reajustados a su configuración predeterminada. Si su red está viva, aseegurese le entender el impacto potencial del comando any. Todos los IP Addresses usados en esta configuración fueron seleccionados de los direccionamientos del RFC 1918 en un ambiente de laboratorio; estos IP Addresses no son routable en Internet y están para las para pruebas solamente.

Diagrama de la red

Este documento utiliza la configuración de red descrita en esta sección.

Un usuario remoto conecta con la dirección IP del ASA con un buscador Web SSL-habilitado. Después de la autenticación satisfactoria, SVC se descarga a la computadora cliente, y el usuario puede utilizar una sesión segura cifrada para el acceso total a todos los recursos permitidos en la red corporativa.

Tareas de Preconfiguración

Antes de que usted comience, complete estas tareas:

- Consulte Cómo Permitir el Acceso HTTPS para el ASDM para que el ASA sea configurado por el ASDM.Para acceder la aplicación ASDM, de su estación de administración, utiliza a un buscador Web SSL-habilitado y ingresa el IP Address del dispositivo ASA. Por ejemplo: ***inside_ip_address de https://,*** donde están el direccionamiento los *inside_ip_address del* ASA. Una vez que se carga el ASDM, usted puede comenzar la configuración de SVC.
- Descargue el paquete del cliente VPN SSL (sslclient-win*.package) del sitio web de la descarga de software de Cisco (clientes registrados solamente) a la unidad de disco duro local de la estación de administración de la cual usted accede la aplicación ASDM.

El WebVPN y el ASDM no se pueden habilitar en la misma interfaz ASA a menos que cambie los números del puerto. Si usted quisiera que las dos Tecnologías utilizaran el mismo puerto (puerto 443) en el mismo dispositivo, usted puede habilitar el ASDM en la *interfaz interior* y habilitar el WebVPN en la *interfaz exterior*.

Convenciones

Para más información sobre las convenciones sobre documentos, consulte Convenciones sobre Consejos Técnicos de Cisco.

Configure al cliente VPN SSL en un ASA

Para configurar al cliente VPN SSL en un ASA, complete estos pasos:

1. Habilite el acceso del WebVPN en el ASA
2. Instale y habilite al cliente VPN SSL en el ASA
3. Habilite la instalación de SVC en los clientes
4. El permiso reintroduce los parámetros

Paso 1. Acceso del WebVPN del permiso en el ASA

Para habilitar el acceso del WebVPN en el ASA, complete estos pasos:

1. Dentro de la aplicación ASDM, haga clic la **configuración**, y después haga clic el **VPN**.
2. Amplíe el **WebVPN**, y elija el **acceso del WebVPN**.
3. Seleccione la interfaz para la cual usted quiere habilitar el WebVPN, y el **permiso del** tecleo**.**

Paso 2. Instale y habilite al cliente VPN SSL en el ASA

Para instalar y habilitar al cliente VPN SSL en el ASA, complete estos pasos:

1. Haga clic la **configuración**, y después haga clic el **VPN**.
2. En el SCR_INVALID, amplíe el **WebVPN**, y elija al **cliente VPN SSL**.
3. Haga clic en Add (Agregar).El cuadro de diálogo de la imagen del cliente VPN del agregar SSL aparece.
4. Haga clic el botón de la **carga**.El cuadro de diálogo de la imagen de la carga aparece.
5. Haga clic los **archivos locales de la ojeada** abotonan para localizar un archivo en su computadora local, o hacen clic el botón del **Flash de la ojeada** para localizar un archivo en el sistema de archivos Flash.
6. Localice el archivo de imagen del cliente para cargar, y haga clic la **AUTORIZACIÓN**.
7. Haga clic el **archivo de la carga**, y después haga clic **cerca**.
8. Una vez que la imagen del cliente se carga para contellear, marque la casilla de verificación del **cliente VPN del permiso SSL**, y después haga clic **se aplican**.**Note**: Si usted recibe un mensaje de error, verifique que el acceso del WebVPN esté habilitado. En el SCR_INVALID, amplíe el **WebVPN**, y elija el **acceso del WebVPN**. Seleccione la interfaz para la cual usted quiere configurar el acceso, y el **permiso del** tecleo.
9. Haga clic la **salvaguardia**, y después haga clic **sí** para validar los cambios.

Paso 3. Instalación de SVC del permiso en los clientes

Para habilitar la instalación de SVC en los clientes, complete estos pasos:

1. En el SCR_INVALID, amplíe la **administración de IP Address**, y elija a las **agrupaciones IP**.
2. El tecleo **agrega**, ingresa los valores en el nombre, comenzando el IP Address, terminando los campos del IP Address, y de la máscara de subred. Los IP Addresses que usted ingresa para el IP Address que comienza y terminar los campos del IP Address deben venir de las subredes en su red interna.
3. El Haga Click en OK, y entonces hace clic **se aplica**.
4. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.
5. En el SCR_INVALID, amplíe la **administración de IP Address**, y elija la **asignación**.
6. Marque la casilla de verificación de los **pools de la dirección interna del uso**, y entonces desmarque al **servidor de autenticación del uso** y **utilice las** casillas de verificación del **DHCP**.
7. Haga clic en Apply (Aplicar).
8. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.
9. En el SCR_INVALID, amplíe al **general**, y elija al **grupo de túnel**.
10. Seleccione al grupo de túnel que usted quiere manejar, y el tecleo **edita**.
11. Haga clic la lengueta de la **asignación de dirección cliente**, y seleccione el pool creado recientemente de la dirección IP de la lista disponible de los pools.

12. El tecleo **agrega**, y después hace clic la **AUTORIZACIÓN**.
13. En la ventana de la aplicación ASDM, el tecleo **se aplica**.
14. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.

Paso 4. El permiso reintroduce el parámetro

Para habilitar reintroduzca los parámetros:

1. En el SCR_INVALID, amplíe al **general**, y elija la **directiva del grupo**.
2. Seleccione la directiva que usted quiere aplicarse a este grupo de clientes, y el tecleo **edita**.
3. Conforme a la ficha general, desmarque los **protocolos de túneles heredan la** casilla de verificación, y marcan la casilla de verificación del **WebVPN**.
4. Haga clic la lengueta del **WebVPN**, haga clic la lengueta del **cliente SSLVPN**, y elija estas opciones:Para la opción del Cliente VPN del uso SSL, desmarque la casilla de verificación de la **herencia**, y haga clic el botón de radio **opcional**.Esta opción permite que el cliente remoto elija independientemente de si descargar SVC. *El siempre* bien escogido se asegura de que SVC esté descargado a la estación de trabajo remota durante cada conexión VPN SSL.Para la opción Keep Installer on Client System, desmarque la casilla de selección **Inherit**, y haga clic en el **botón de opción Yes**.Esta acción permite que el software de SVC permanezca en la máquina del cliente; por lo tanto, el ASA no se requiere para descargar el software de SVC al cliente cada vez que se hace una conexión. Esta opción es una buena opción para los usuarios remotos que suelen acceder a la red corporativa.Para la opción Intervalo de Renegociación, desmarque la casilla **Inherit**, desmarque la casilla de selección **Unlimited**, e ingrese el número de minutos hasta la generación de la nueva clave.La seguridad se ve aumentada al establecer los límites durante el tiempo que una clave es válida.Para la opción Método de Renegociación, desmarque la casilla de selección **Inherit**, y haga clic el botón de opción **SSL**. La renegociación puede utilizar el túnel SSL actual o un túnel nuevo creado expresamente para la renegociación.Sus atributos del cliente VPN SSL se deben configurar tal y como se muestra en de esta imagen:
5. El Haga Click en OK, y entonces hace clic **se aplica**.
6. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.

Resultados

El ASDM crea estas configuraciones de la línea de comandos:

ciscoasa

```
ciscoasa(config)#show run
ASA Version 7.2(1)
!
hostname ciscoasa
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
```

```
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask
255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
!
!--- Group Policy Statements group-policy GroupPolicy1
internal group-policy GroupPolicy1 attributes vpn-
tunnel-protocol IPSec l2tp-ipsec webvpn !--- Enable the
SVC for WebVPN webvpn svc enable svc keep-installer
installed svc rekey time 30 svc rekey method ssl !
username cisco password 53QNetqK.Kqqfshe encrypted
privilege 15 ! http server enable http 10.2.2.0
255.255.255.0 inside ! no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart !--- Tunnel
Group and Group Policy using the defaults here tunnel-
group DefaultWEBVPNGroup general-attributes address-pool
CorporateNet default-group-policy GroupPolicy1 ! no vpn-
addr-assign aaa no vpn-addr-assign dhcp ! telnet timeout
5 ssh 172.22.1.0 255.255.255.0 outside ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp !
service-policy global_policy global !--- Enable webvpn
and the select the SVC client webvpn enable outside svc
image disk0:/sslclient-win-1.1.1.164.pkg 1 svc enable !-
-- Provide list for access to resources url-list
ServerList "E-Commerce Server1" http://10.2.2.2 1 url-
list ServerList "BrowseServer" cifs://10.2.2.2 2 tunnel-
group-list enable prompt hostname context
```

```
Cryptochecksum:80a1890a95580dca11e3aee200173f5f : end
```

Personalice su configuración

Los procedimientos descritos adentro configuran al cliente VPN SSL en un uso ASA los nombres predeterminados ASA para la directiva del grupo (*GroupPolicy1*) y el grupo de túnel (*DefaultWebVPNGroup*) tal y como se muestra en de esta imagen:

Este procedimiento describe cómo crear sus propias directivas y grupos de túnel de encargo del grupo y conectarlos juntos de acuerdo con las políticas de seguridad de su organización.

Para personalizar su configuración, complete estos pasos:

1. Cree una directiva de encargo del grupo
2. Cree a un grupo de túnel de encargo
3. Cree a un usuario y agregue a ese usuario a su directiva de encargo del grupo

Paso 1. Cree una directiva de encargo del grupo

Para crear una directiva de encargo del grupo, complete estos pasos:

1. Haga clic la **configuración**, y después haga clic el **VPN**.
2. Amplíe al **general**, y elija la **directiva del grupo**.
3. El tecleo **agrega**, y elige el **Internal group policy (política grupal interna)**.
4. En el campo de nombre, ingrese un nombre para su directiva del grupo.En este ejemplo, el nombre de la directiva del grupo se ha cambiado a *SalesGroupPolicy*.
5. Conforme a la ficha general, desmarque los **protocolos de túneles heredan la** casilla de verificación, y marcan la casilla de verificación del **WebVPN**.
6. Haga clic la lengueta del **WebVPN**, y después haga clic la lengueta del **cliente SSLVPN**.En este cuadro de diálogo, usted puede también tomar las decisiones para el comportamiento del cliente VPN SSL.
7. El Haga Click en OK, y entonces hace clic **se aplica**.
8. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.

Paso 2. Cree a un grupo de túnel de encargo

Para crear a un grupo de túnel de encargo, complete estos pasos:

1. Haga clic el botón de la **configuración**, y después haga clic el **VPN**.
2. Amplíe al **general**, y elija al **grupo de túnel**.
3. El tecleo **agrega**, y elige el **acceso del WebVPN**.
4. En el campo de nombre, ingrese un nombre para su grupo de túnel.En este ejemplo, el nombre de grupo de túnel se ha cambiado a *SalesForceGroup*.
5. Haga clic la flecha desplegable de la **directiva del grupo**, y elija su directiva creada recientemente del grupo.Ahora conectan su directiva y grupo de túnel del grupo.
6. Haga clic la lengueta de la **asignación de dirección cliente**, y ingrese la información del servidor DHCP o selecciónela de una agrupación IP localmente creada.
7. El Haga Click en OK, y entonces hace clic **se aplica**.

8. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.

Paso 3. Cree a un usuario y agregue a ese usuario a su directiva de encargo del grupo

Para crear a un usuario y agregar a ese usuario a su directiva de encargo del grupo, complete estos pasos:

1. Haga clic la **configuración**, y después haga clic el **VPN**.
2. Amplíe al **general**, y elija a los **usuarios**.
3. El tecleo **agrega**, y ingresa el Nombre de usuario y la información de contraseña.
4. Haga clic la lengueta de la **política del VPN**. Asegúrese de que sus visualizaciones creadas recientemente de la directiva del grupo en la directiva del grupo coloquen.Este usuario hereda todas las características de la nueva directiva del grupo.
5. El Haga Click en OK, y entonces hace clic **se aplica**.
6. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Autenticación

La autenticación para los clientes VPN SSL es realizada usando uno de estos métodos:

- Servidor del Cisco Secure ACS (radio)
- Dominio de NT
- Active Directory
- Contraseñas de USO único
- Certificados digitales
- Tarjetas inteligentes
- Autenticación AAA local

Esta documentación utiliza una cuenta local creada en el dispositivo ASA.

Note: Si un dispositivo de seguridad adaptante tiene trustpoints múltiple que comparte mismo CA, sólo uno de este trustpoints que comparte CA se puede utilizar para validar los Certificados de usuario.

Configuración

Para conectar con el ASA con un cliente remoto, ingrese **https://ASA_outside_address** en el campo de dirección de un buscador Web SSL-habilitado. *ASA_outside_address* es el IP Address externo de su ASA. Si su configuración es acertada, la ventana del cliente VPN de Cisco Systems SSL aparece.

Note: La ventana del cliente VPN de Cisco Systems SSL aparece solamente después que usted valida el certificado del ASA y después de que descargan al cliente VPN SSL a la estación remota. Si no aparece la ventana, aseegurese la no se minimiza.

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 información detallada sobre los **comandos show**, refiera a verificar las configuraciones del 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.

Error de SVC

Problema

Usted puede ser que reciba este mensaje de error durante la autenticación:

```
ciscoasa(config)#show run
ASA Version 7.2(1)
!
hostname ciscoasa
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
!
!--- Group Policy Statements group-policy GroupPolicy1 internal group-policy GroupPolicy1
attributes vpn-tunnel-protocol IPSec l2tp-ipsec webvpn !--- Enable the SVC for WebVPN webvpn svc
enable svc keep-installer installed svc rekey time 30 svc rekey method ssl ! username cisco
password 53QNetqK.Kqqfshe encrypted privilege 15 ! http server enable http 10.2.2.0
255.255.255.0 inside ! no snmp-server location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart !--- Tunnel Group and Group Policy using the
defaults here tunnel-group DefaultWEBVPNGroup general-attributes address-pool CorporateNet
default-group-policy GroupPolicy1 ! no vpn-addr-assign aaa no vpn-addr-assign dhcp ! telnet
timeout 5 ssh 172.22.1.0 255.255.255.0 outside ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map global_policy class inspection_default inspect
dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp
inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp ! service-policy global_policy global !--- Enable webvpn and the select the
SVC client webvpn enable outside svc image disk0:/sslclient-win-1.1.1.164.pkg 1 svc enable !---
Provide list for access to resources url-list ServerList "E-Commerce Server1" http://10.2.2.2 1
url-list ServerList "BrowseServer" cifs://10.2.2.2 2 tunnel-group-list enable prompt hostname
context Cryptochecksum:80a1890a95580dca11e3aee200173f5f : end
```

Solución

Si a servicio de firewall se está ejecutando en su PC, puede interrumpir la autenticación. Pare el servicio y vuelva a conectar al cliente.

¿SVC ha establecido una sesión segura con el ASA?

Para asegurar al cliente VPN SSL ha establecido una sesión segura con el ASA:

1. **Supervisión del** tecleo.
2. Amplíe los **VPN statistics (Estadísticas de la VPN)**, y elija las **sesiones**.
3. Del filtro por el menú desplegable, elija al **cliente VPN SSL**, y haga clic el botón del **filtro**.Su configuración debe aparecer en la lista de las sesiones.

¿Las sesiones seguras se están estableciendo y se están terminando con éxito?

Usted puede ver los registros en tiempo real para asegurarse que las sesiones se están estableciendo y que se están terminando con éxito. Para ver los registros de la sesión:

1. **La supervisión del** tecleo, y entonces hace clic el **registro**.
2. Elija el **Log Viewer** o el **búfer del registro en tiempo real**, y después haga clic la **visión**.**Note**: Para visualizar solamente las sesiones de una dirección específica, filtro por el direccionamiento.

Marque a la agrupación IP en el perfil del WebVPN

```
ciscoasa(config)#show run
ASA Version 7.2(1)
!
hostname ciscoasa
```

```
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
!
!--- Group Policy Statements group-policy GroupPolicy1 internal group-policy GroupPolicy1
attributes vpn-tunnel-protocol IPSec l2tp-ipsec webvpn !--- Enable the SVC for WebVPN webvpn svc
enable svc keep-installer installed svc rekey time 30 svc rekey method ssl ! username cisco
password 53QNetqK.Kqqfshe encrypted privilege 15 ! http server enable http 10.2.2.0
255.255.255.0 inside ! no snmp-server location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart !--- Tunnel Group and Group Policy using the
defaults here tunnel-group DefaultWEBVPNGroup general-attributes address-pool CorporateNet
default-group-policy GroupPolicy1 ! no vpn-addr-assign aaa no vpn-addr-assign dhcp ! telnet
timeout 5 ssh 172.22.1.0 255.255.255.0 outside ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map global_policy class inspection_default inspect
dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp
inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp ! service-policy global_policy global !--- Enable webvpn and the select the
SVC client webvpn enable outside svc image disk0:/sslclient-win-1.1.1.164.pkg 1 svc enable !---
Provide list for access to resources url-list ServerList "E-Commerce Server1" http://10.2.2.2 1
url-list ServerList "BrowseServer" cifs://10.2.2.2 2 tunnel-group-list enable prompt hostname
context Cryptochecksum:80a1890a95580dca11e3aee200173f5f : end
```

No hay direccionamientos disponibles asignar a SVC la conexión. Por lo tanto, asigne el direccionamiento de la agrupación IP en el perfil.

Si usted crea el perfil de la nueva conexión, después configure un alias o un grupo-URL para acceder este perfil de la conexión. Si no, todas las tentativas SSL golpearán el perfil

predeterminado de la conexión WebVPN que no tenía una agrupación IP atada a él. Fije esto hasta uso el perfil de la conexión predeterminado y ponga a una agrupación IP en él.

Consejos

- Aseegurese los trabajos de la encaminamiento correctamente con el pool de la dirección IP que usted asigna a sus clientes remotos. Este pool de la dirección IP debe venir de una subred en su LAN. Usted puede también utilizar un servidor DHCP o a un servidor de autenticación para asignar los IP Addresses.
- El ASA crea un grupo de túnel predeterminado (*DefaultWebVPNGroup*) y una directiva del grupo predeterminado (*GroupPolicy1*). Si usted crea los nuevos grupos y directivas, aseegurese le aplicar los valores de acuerdo con las políticas de seguridad de su red.
- Si usted quiere habilitar el archivo de Windows que hojea con CIFS, ingrese un servidor de los TRIUNFOS (NBNS) bajo la **configuración > el VPN > el WebVPN > los servidores y los URL**. Esta tecnología utiliza la selección CIFS.

Comandos

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

- Clientless SSL VPN (WebVPN) en el ejemplo de configuración ASA
- Cliente “liviano” SSL VPN (WebVPN) en el ASA con el ejemplo de la Configuración de ASDM
- Ejemplo de Configuración de ASA con WebVPN y Single Sign-on con ASDM y NTLMv1
- Cisco ASA 5500 Series Adaptive Security Appliances
- Soporte Técnico y Documentación - Cisco Systems