ASA 8.X: Permita la aplicación de usuario para ejecutarse con el reestablecimiento del túnel L2L VPN

Contenido

Introducción

Este documento proporciona la información sobre la característica tunneled de los flujos del IPSec persistente y cómo conservar el flujo TCP sobre la interrupción de un túnel VPN.

prerrequisitos

Requisitos

Los Quien lea este documento deben tener comprensión básica en cómo el VPN trabaja. Si desea más información, consulte estos documentos:

- Muestree la configuración VPN L2L
- L2L VPN con el ASA

Componentes Utilizados

La información en este documento se basa en el dispositivo de seguridad adaptante de Cisco (ASA) con la versión 8.2 y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

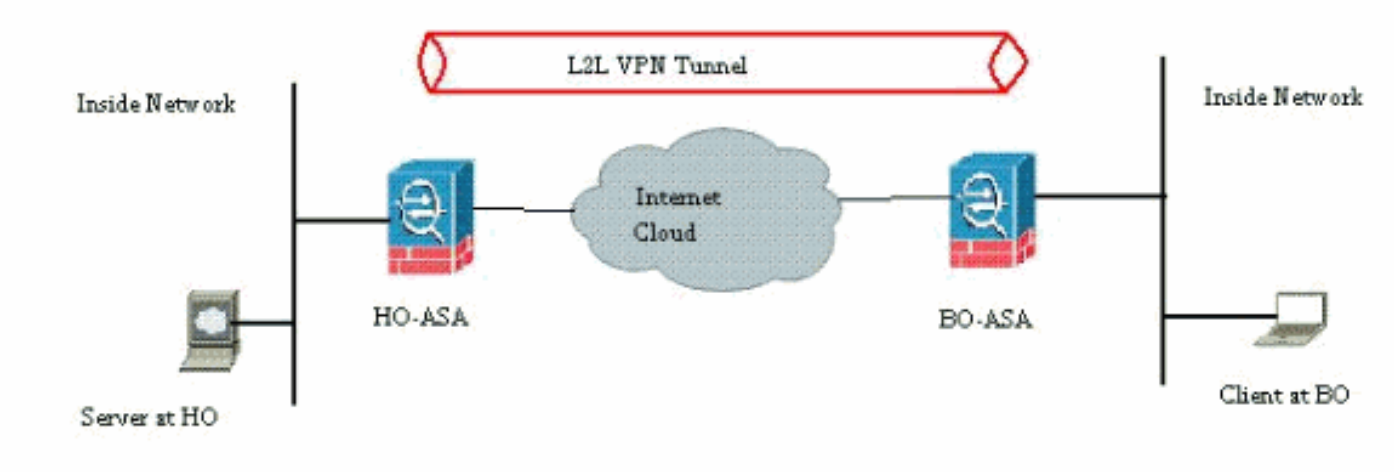
Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

Tal y como se muestra en del diagrama de la red, la sucursal (BO) está conectada con la oficina principal (HO) con el VPN de sitio a sitio. Considere a un usuario final en la sucursal que intenta descargar un archivo grande del servidor situado en la oficina principal. La descarga dura las horas. La transferencia de archivos trabaja muy bien hasta que el VPN trabaje muy bien. Sin embargo, cuando se interrumpe el VPN, se cuelga la transferencia de archivos y el usuario tiene que re-iniciado la petición de la transferencia de archivos otra vez desde el principio después de que se establezca el túnel.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Este problema se presenta debido a las funciones incorporadas en cómo el ASA trabaja. El ASA monitorea cada conexión que los pasos con él y mantengan una entrada en su tabla de estado según la característica de la Inspección de la aplicación. Los detalles del tráfico encriptado que pasan con el VPN se mantienen bajo la forma de base de datos de la asociación de seguridad (SA). Para el escenario de este documento, mantiene dos diversos flujos de tráfico. Uno es el tráfico encriptado entre los gatewayes de VPN y el otro es el flujo de tráfico entre el servidor en la oficina principal y el usuario final en la sucursal. Cuando se termina el VPN, los detalles del flujo para este SA determinado se borran. Sin embargo, la entrada de tabla del estado mantenida por el ASA para esta conexión TCP llega a ser añeja debido a ninguna actividad, que obstaculiza la descarga. Esto significa que el ASA todavía conservará la conexión TCP para ese flujo determinado mientras que la aplicación de usuario termina. Sin embargo, las conexiones TCP se

convertirán en parásito y eventual descanso después de que expire el temporizador ocioso TCP.

Este problema ha sido resuelto introduciendo una característica llamada los flujos tunneled Persistent IPSec. Han integrado a un comando new en Cisco ASA de conservar la información de la tabla de estado en la renegociación del túnel VPN. El comando se muestra aquí:

```
sysopt connection preserve-vpn-flows
```

Por abandono, se inhabilita este comando. Habilitando esto, Cisco ASA mantendrá la información de la tabla de estado TCP cuando el L2L VPN se recupera de la interrupción y restablece el túnel.

En este escenario, este comando tiene que ser habilitado en los ambos extremos del túnel. Si es dispositivo no Cisco en el otro extremo, habilitar este comando en Cisco ASA debe ser suficiente. Si se habilita el comando cuando los túneles eran ya activos, los túneles se deben borrar y restablecer para que este comando tome el efecto. Para más detalles en el claro y el restablecimiento de los túneles, refiera claramente a las asociaciones de seguridad.

Detalles de la compatibilidad para esta característica

Esta característica se ha introducido en la versión de software 8.0.4 de Cisco ASA y posterior. Esto se soporta solamente para estos tipos de VPN:

- LAN a los túneles LAN
- Túneles de acceso remoto en el Modo de ampliación de la red (NEM)

Esta característica no se soporta para estos tipos de VPN:

- Túneles de acceso remoto del IPSec en el modo cliente
- AnyConnect o túneles SSL VPN

Esta característica no existe en estas Plataformas:

- Cisco PIX con la versión de software 6.0
- Concentradores VPN de Cisco
- Plataformas de Cisco IOS®

Habilitar esta característica no crea ninguna sobrecarga adicional en el interno procesamiento de la CPU del ASA porque va a guardar las mismas conexiones TCP que el dispositivo tiene cuando el túnel está para arriba.

Nota: Este comando es aplicable para las conexiones TCP solamente. No tiene ningún efecto sobre el tráfico UDP. Las conexiones UDP quieren el descanso según el período de agotamiento del tiempo de espera configurado.

Configuraciones

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

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Este documento usa esta configuración:

- Ciscoasa

Éste es un resultado de la configuración corriente de la muestra del Firewall de Cisco ASA en un extremo del túnel VPN:

Ciscoasa

```
ASA Version 8.2(1)
!
hostname CiscoASA
domain-name example.com
enable password <removed>
passwd <removed>
names
!
interface Ethernet0/0
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.248
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.224.9.5 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.224.14.10 255.255.255.0
!
boot system disk0:/asa822-k8.bin
ftp mode passive
 !---Output Suppressed ! access-list test extended
permit ip 10.224.228.0 255.255.255.128 any access-list
test extended permit ip 10.224.52.0 255.255.255.128 any
access-list 100 extended permit ip 10.224.228.0
255.255.255.128 any access-list 100 extended permit ip
10.224.52.0 255.255.255.128 any access-list
inside_access_out extended permit ip any 10.224.228.0
255.255.255.1 ! !---Output Suppressed global (outside) 1
interface nat (inside) 0 access-list test nat (inside) 1
10.224.10.0 255.255.255.0 ! !---Output Suppressed route
inside 10.0.0.0 255.0.0.0 10.224.9.1 1 route outside
0.0.0.0 255.255.255.255 209.165.201.1 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 sip-provisional-media 0:02:00
uauth 0:05:00 absolute timeout tcp-proxy-reassembly
0:01:00 dynamic-access-policy-record DfltAccessPolicy !
!---Output Suppressed http server idle-timeout 40 http
10.224.3.0 255.255.255.0 management http 0.0.0.0 0.0.0.0
inside ! snmp-server enable traps snmp authentication
linkup linkdown coldstart ! !--- To preserve and resume
```

```
stateful (TCP) tunneled IPsec LAN-to-LAN traffic within
the timeout period after the tunnel drops and recovers.
sysopt connection preserve-vpn-flows service
resetoutside ! crypto ipsec transform-set ESP-AES-256-
MD5 esp-aes-256 esp-md5-hmac crypto ipsec transform-set
testSET esp-3des esp-md5-hmac crypto map map1 5 match
address 100 crypto map map1 5 set peer 209.165.200.10
crypto map map1 5 set transform-set testSET crypto map
map1 interface outside crypto isakmp enable outside
crypto isakmp policy 5 authentication pre-share
encryption 3des hash sha group 2 lifetime 86400 crypto
isakmp policy 10 authentication pre-share encryption des
hash sha group 2 lifetime 86400 !---Output Suppressed !
telnet timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! !---Output Suppressed ! tunnel-group
209.165.200.10 type ipsec-l2l tunnel-group
209.165.200.10 ipsec-attributes pre-shared-key * !---
Output Suppressed 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 prompt hostname
state Cryptochecksum:5c228e7131c169f913ac8198ecf8427e :
end
```

Habilite esta característica

Por abandono, se inhabilita esta característica. Esto se puede habilitar usando este comando en el CLI del ASA:

```
CiscoASA(config)#sysopt connection preserve-vpn-flows
```

Esto se puede ver usando este comando:

```
CiscoASA(config)#show run all sysopt no sysopt connection timewait sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0 sysopt connection permit-vpn sysopt connection reclassify-vpn
sysopt connection preserve-vpn-flows no sysopt nodnsalias inbound no sysopt nodnsalias outbound
no sysopt radius ignore-secret no sysopt noproxyarp outside
```

Al usar el ASDM, esta característica puede ser habilitada siguiendo esta trayectoria:

La configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzaron > IPSec > las opciones del sistema.

Entonces, marque los *flujos stateful del coto VPN cuando el túnel cae para la* opción del *Modo de ampliación de la red (NEM)*.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **muestre el detalle del VPN-contexto de la tabla ASP** — Muestra el contenido del contexto VPN de la trayectoria acelerada de la Seguridad, que pudo ayudarle a resolver problemas un problema. Lo que sigue es una salida de muestra del comando del VPN-**contexto de la tabla de la demostración ASP** cuando se habilita la característica tunneled de los flujos del IPSec persistente. Observe que contiene un indicador específico del **COTO**.`CiscoASA(config)#show asp table vpn-context VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000, gc=0 VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000, gc=0`

Troubleshooting

En esta sección, ciertas soluciones alternativas se presentan para evitar el cambio de túneles. Los pros - y - contra de las soluciones alternativas también se detallan.

Fije el valor del tiempo de vida de IKE a cero

Usted puede hacer un túnel VPN para permanecer vivo por un tiempo infinito, pero para no renegociar, guardando el valor del tiempo de vida de IKE como cero. La información sobre el SA es conservada por los pares VPN hasta que expire el curso de la vida. Asignando un valor como cero, usted puede hacer este último de la sesión IKE para siempre. Con esto, usted puede evitar los problemas intermitentes de la desconexión del flujo durante la reintroducción del túnel. Esto se puede hacer con este comando:

```
CiscoASA(config)#crypto isakmp policy 50 lifetime 0
```

Sin embargo, esto tiene una desventaja específica en términos de compromiso del nivel de seguridad del túnel VPN. La reintroducción de la sesión IKE dentro de los intervalos de tiempo especificado proporciona más Seguridad al túnel VPN en términos de claves de encripción modificadas cada vez y llega a ser difícil que cualquier intruso decodifique la información.

Nota: Inhabilitar el tiempo de vida de IKE no significa que el túnel no reintroduce en absoluto. No obstante, IPSec SA reintroducirá en el intervalo de tiempo especificado porque eso no se puede fijar a cero. El valor mínimo del curso de la vida permitido para IPSec SA es 120 segundos y el máximo es 214783647 segundos. Para más información sobre esto, refiera al curso de la vida IPSec SA.

Mensaje de error cuando el túnel cae

Cuando esta característica no se utiliza en la configuración, Cisco ASA devuelve este mensaje del registro cuando se interrumpe el túnel VPN:

```
%ASA-6-302014: La conexión TCP 57983 del desmontaje para outside:XX.XX.XX.XX/80
inside:10.0.0.100/1135 al túnel de los bytes 53947 de la duración 0:00:36 se ha derribado
```

Usted puede ver que la razón es que **se ha derribado el túnel**.

Nota: El registro del nivel 6 se debe habilitar para considerar este mensaje.

Cómo esta característica diferencia con la opción de reclasificar-VPN

Se utiliza la opción del coto-VPN-flujo cuando un túnel despide. Esto permite que un flujo anterior TCP permanezca abierto tan cuando viene el túnel salvaguardia, el mismo flujo puede ser

utilizada.

Cuando se utiliza el comando de reclasificar-**VPN de la conexión del sysopt**, borra cualquier flujo anterior que pertenezca al tráfico de túnel y clasifique el flujo para pasar a través del túnel. La opción de reclasificar-VPN se utiliza en una situación cuando un flujo TCP fue creado ya que no es VPN relacionado. Esto crea una situación adonde el tráfico no fluye a través del túnel después de que se establezca el VPN. Para más información sobre esto, refiera al sysopt reclasificar-VPN.

Información Relacionada

- Sitio para localizar VPN (L2L) con el ASA
- Página de documentación de Cisco ASA
- Soporte Técnico y Documentación - Cisco Systems