ASA 8.X: Permitir que la Aplicación de Usuario se Ejecute con el Restablecimiento del Túnel VPN L2L

Contenido

Introducción

Este documento proporciona información sobre la función Flujos Tunelizados IPSec Persistentes y cómo conservar el flujo TCP a través de la interrupción de un túnel VPN.

Prerequisites

Requirements

Los lectores de este documento deben tener conocimientos básicos sobre cómo funciona la VPN. Si desea más información, consulte estos documentos:

- Ejemplo de configuración de VPN L2L
- VPN L2L con ASA

Componentes Utilizados

La información de este documento se basa en Cisco Adaptive Security Appliance (ASA) con la versión 8.2 y posteriores.

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.

Convenciones

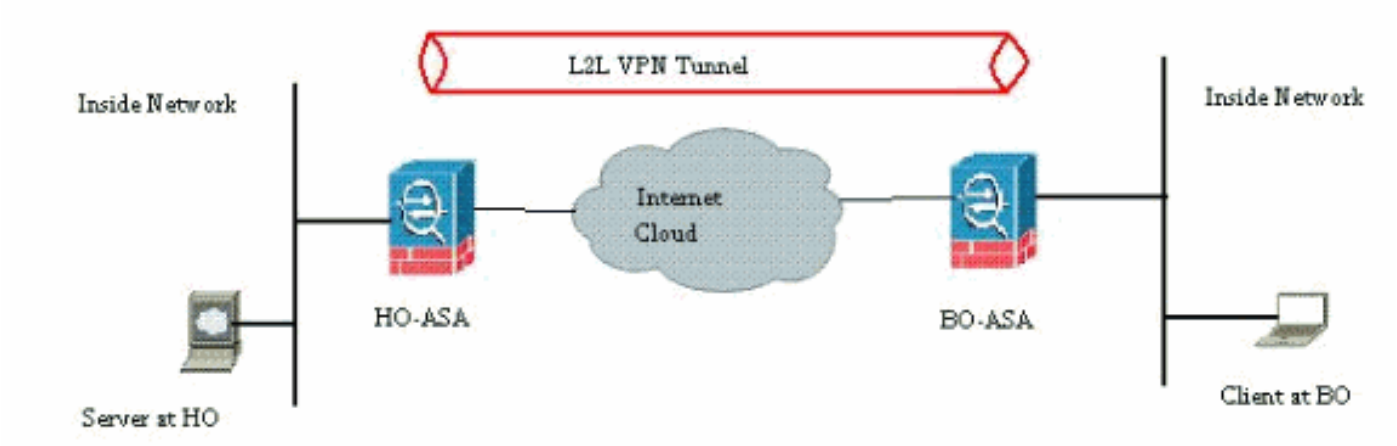
Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

Como se muestra en el diagrama de red, la sucursal (BO) está conectada a la sede central (HO) a través de la VPN de sitio a sitio. Considere un usuario final de la sucursal que intenta descargar un archivo grande del servidor situado en la sede central. La descarga dura horas. La transferencia de archivos funciona bien hasta que la VPN funcione correctamente. Sin embargo, cuando se interrumpe la VPN, se cuelga la transferencia de archivos y el usuario debe reiniciar la solicitud de transferencia de archivos de nuevo desde el principio después de que se haya establecido el túnel.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Este problema surge debido a la funcionalidad integrada sobre cómo funciona ASA. El ASA monitorea cada conexión que lo atraviesa y guarda una entrada en su tabla de estado según la característica de inspección de la aplicación. Los detalles del tráfico encriptado que pasan por la VPN se mantienen bajo la forma de base de datos de asociación de seguridad (SA). Para el escenario de este documento, mantiene dos flujos de tráfico diferentes. Uno es el tráfico cifrado entre los gateways VPN y el otro es el flujo de tráfico entre el servidor en la sede central y el usuario final en la sucursal. Cuando la VPN se desactiva, los detalles del flujo para este SA determinado se borran. Sin embargo, la entrada de la tabla de estado guardada por el ASA para esta conexión TCP queda desactualizada debido a la falta de 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 perderán y expirarán una vez que haya transcurrido el tiempo de caducidad de TCP.

Este problema ha sido resuelto introduciendo una característica llamada Flujos de túnel de IPSec persistentes. Se ha integrado un nuevo comando en Cisco ASA para 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 defecto, este comando está desactivado. Al habilitar esto, Cisco ASA mantendrá la información de la tabla de estado TCP cuando la VPN L2L se recupere de la interrupción y restablezca el túnel.

En este escenario, este comando debe estar habilitado en ambos extremos del túnel. Si se trata de un dispositivo que no es de Cisco en el otro extremo, habilitar este comando en Cisco ASA debería ser suficiente. Si el comando se habilita cuando los túneles ya estaban activos, los túneles deben ser borrados y restablecidos para que este comando surta efecto. Para obtener más detalles sobre el despeje y restablecimiento de los túneles, consulte Despejar las asociaciones de seguridad.

Detalles de compatibilidad para esta función

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

- Túneles LAN a LAN
- Túneles de acceso remoto en modo de extensión de red (NEM)

Esta función no se soporta para estos tipos de VPN:

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

Esta función no existe en estas plataformas:

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

La activación de esta función no crea ninguna sobrecarga adicional en el procesamiento interno de la CPU del ASA porque va a mantener las mismas conexiones TCP que el dispositivo cuando el túnel está activo.

Nota: Este comando sólo se aplica a conexiones TCP. No tiene ningún efecto en el tráfico UDP. Las conexiones UDP agotarán el tiempo de espera según el período de tiempo de espera configurado.

Configuraciones

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) 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

Este es un ejemplo de resultado de configuración en ejecución del firewall 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
```

Habilitar esta función

De forma predeterminada, esta función está desactivada. Esto se puede habilitar utilizando este comando en la 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 utilizar el ASDM, esta función se puede habilitar siguiendo esta ruta:

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options.

A continuación, verifique la *opción Preserve stateful VPN flows cuando el túnel cae para la opción Network Extension Mode (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.

- **show asp table vpn-context detail** —Muestra el contenido del contexto de VPN de la trayectoria de seguridad acelerada, que podría ayudarle a resolver un problema. A continuación se muestra un ejemplo de salida del comando **show asp table vpn-context** cuando se habilita la función IPSec tunelizada flows persistente. Tenga en cuenta que contiene un indicador **PRESERVE** específico.

```
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
```

Troubleshoot

En esta sección, se presentan algunas soluciones alternativas para evitar la inestabilidad de los túneles. También se detallan los pros y los contras de las soluciones alternativas.

Establezca el valor de duración IKE en cero

Puede hacer que un túnel VPN permanezca activo por un tiempo infinito, pero no para volver a negociar, manteniendo el valor de vida de IKE como cero. Los peers VPN conservan la información sobre la SA hasta que caduque la vida útil. Al asignar un valor como cero, puede hacer que esta sesión IKE dure para siempre. A través de esto, puede evitar los problemas de desconexión de flujo intermitente durante la recodificación 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 comprometer el nivel de seguridad del túnel VPN. El reajuste de la sesión IKE en intervalos de tiempo especificados

proporciona más seguridad al túnel VPN en términos de claves de cifrado modificadas cada vez y se hace difícil para cualquier intruso descodificar la información.

Nota: La inhabilitación de la vida útil de IKE no significa que el túnel no vuelva a activar la llave en absoluto. Aun así, la SA IPSec volverá a introducir la clave en el intervalo de tiempo especificado porque no se puede establecer en cero. El valor de duración mínimo permitido para una SA IPSec es de 120 segundos y el máximo es de 214783647 segundos. Para obtener más información sobre esto, refiérase a vida útil de SA IPSec.

Mensaje de error cuando el túnel falla

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

```
%ASA-6-302014: Conexión TCP de cierre 57983 para afuera:XX.XX.XX.XX/80 a adentro:10.0.0.100/1135
duración 0:00:36 bytes El túnel 53947 ha sido derribado
```

Puede ver que la razón es que el **túnel ha sido derribado**.

Nota: El registro de nivel 6 debe estar habilitado para ver este mensaje.

Cómo se diferencia esta función con la opción reclassify-vpn

La opción preserve-vpn-flow se utiliza cuando se rebota un túnel. Esto permite que un flujo TCP anterior permanezca abierto para que cuando el túnel vuelva a funcionar, se pueda utilizar el mismo flujo.

Cuando se utiliza el comando **sysopt connection reclassify-vpn**, borra cualquier flujo anterior que pertenezca al tráfico tunelizado y clasifica el flujo para pasar a través del túnel. La opción reclassify-vpn se utiliza en una situación en la que ya se creó un flujo TCP que no está relacionado con VPN. Esto crea una situación en la que el tráfico no fluye a través del túnel después de que se establece la VPN. Para obtener más información sobre esto, refiérase a sysopt reclassify-vpn.

Información Relacionada

- VPN de sitio a sitio (L2L) con ASA
- Página de documentación de Cisco ASA
- Soporte Técnico y Documentación - Cisco Systems