Comprensión de los Contadores Crypto ACL en los Túneles VPN Basados en Políticas

Contenido

Introducción

Este documento describe el comportamiento de los contadores de la lista de control de acceso (ACL) criptográfica dentro de los túneles VPN basados en políticas.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- VPN de sitio a sitio basada en políticas en la plataforma Cisco IOS® /Cisco IOS® XE
- Listas de control de acceso en la plataforma Cisco IOS/Cisco IOS XE

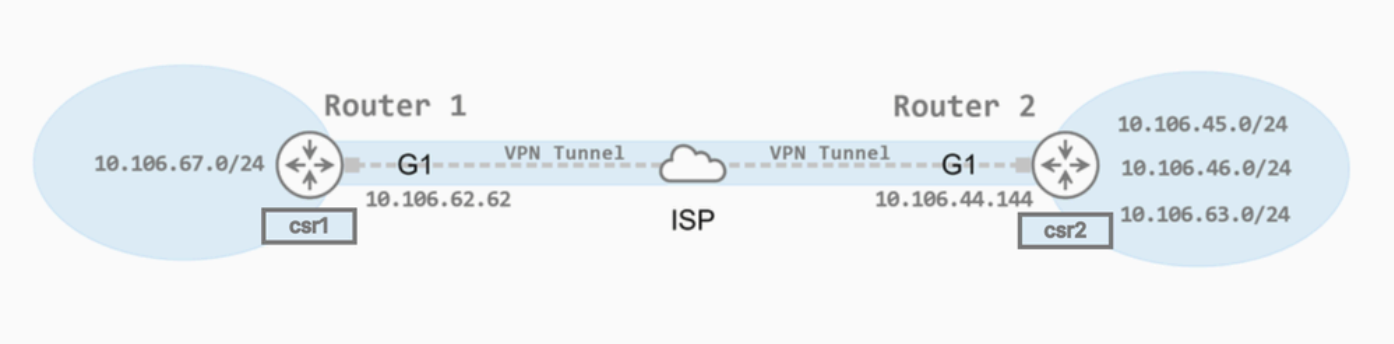
Componentes Utilizados

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

- Cisco C8kv, versión 17.12.04(MD)

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Topología



Topología

Escenarios

Al examinar dos escenarios distintos, nuestro objetivo es comprender cómo se ven afectados los recuentos de visitas de ACL cuando se inicia el tráfico desde diferentes pares y cuando se restablecen los túneles.

1. Escenario uno: Tráfico iniciado desde el Router1 mientras el Túnel VPN está Inactivo

   En esta situación, los cambios en los recuentos de visitas de ACL se analizan cuando el túnel VPN está inicialmente inactivo y el tráfico se inicia desde el Router1. Este análisis ayuda a comprender la configuración inicial y cómo reaccionan los contadores de ACL criptográfica al primer intento de flujo de tráfico.

2. Situación 2: Tráfico iniciado desde el Router 2 mientras el Túnel VPN está Activo

   En esta situación, el túnel VPN ya está establecido y se explora el tráfico iniciado desde el Router 2. Este escenario proporciona información sobre cómo se comportan los contadores de ACL cuando el túnel está activo y el tráfico se introduce desde un peer diferente.

Al comparar estos escenarios, podemos obtener una comprensión integral de la dinámica de los contadores ACL en los túneles VPN en condiciones variables.

Configuración

Hemos configurado un túnel VPN de sitio a sitio basado en políticas entre dos routers Cisco C8kv, designados como peers. El router 1 se denomina "csr1" y el router 2 "csr2".

Configuración criptográfica en el router 1

```
csr1#sh ip int br
Interface              IP-Address      OK?   Method   Status  Protocol
GigabitEthernet1       10.106.62.62    YES   NVRAM    up      up
GigabitEthernet2       10.106.67.27    YES   NVRAM    up      up
```

```
csr1#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.44.144
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr1#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
   20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
   30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
```

```
csr1#sh run int GigabitEthernet1
Building configuration...

Current configuration : 162 bytes
!
interface GigabitEthernet1
ip address 10.106.62.62 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Configuración criptográfica en el router 2

```
csr2#sh ip int br
```

```
Interface              IP-Address        OK?     Method       Status     Protocol
GigabitEthernet1       10.106.44.144     YES     NVRAM        up         up
GigabitEthernet2       10.106.45.145     YES     NVRAM        up         up
GigabitEthernet3       10.106.46.146     YES     NVRAM        up         up
GigabitEthernet4       10.106.63.13      YES     NVRAM        up         up
```

```
csr2#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.62.62
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr2#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
   20 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
   30 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
```

```
csr2#sh run int GigabitEthernet1
Building configuration...

Current configuration : 163 bytes
!
interface GigabitEthernet1
ip address 10.106.44.144 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Análisis del comportamiento de los contadores de la lista de control de acceso criptográfico dentro de los túneles VPN

Inicialmente, ambos dispositivos tienen un conteo de aciertos ACL de cero en sus respectivas listas de acceso crypto.

La Lista de control de acceso alcanzó el conteo de cero en sus respectivas listas de acceso crypto en ambos dispositivos pares.

Escenario uno: Tráfico iniciado desde el Router1 mientras el Túnel VPN está

Inactivo

Estado inicial:

Túnel VPN que conecta el Router 1 (IP: 10.106.67.27) y Router2 (IP: 10.106.45.145) está actualmente inactivo.

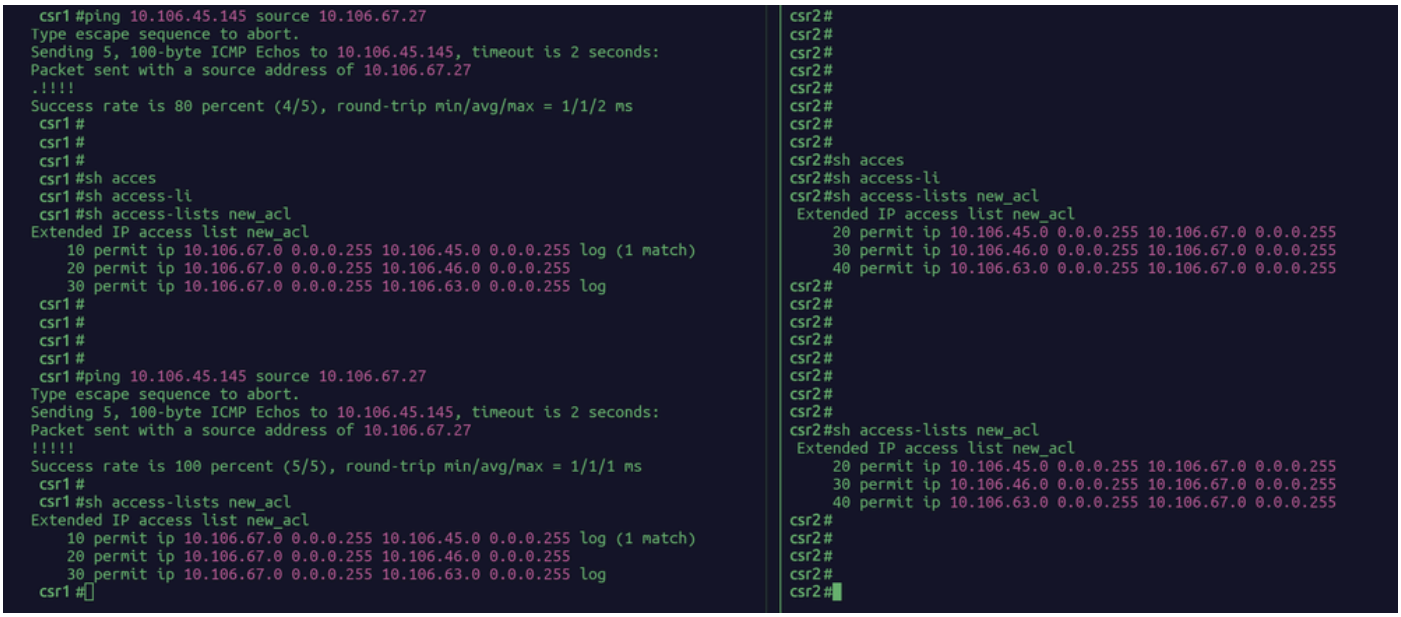
Acción realizada:

El tráfico se inicia desde el Router1, con la intención de establecer comunicación con el Router2.

Observaciones:

1. Comportamiento del Contador ACL:
   a. Al iniciar el tráfico desde el Router1, se produce un aumento notable en el contador de la lista de control de acceso (ACL) en el Router1. Este aumento se produce sólo una vez en el momento en que el túnel intenta establecer la lista.
   b. El aumento en el contador ACL se observa exclusivamente en el router de inicio, que es el Router1 en este escenario. El Router 2 no refleja ningún cambio en su contador ACL en esta etapa.
2. Establecimiento del túnel:
   a. Después del incremento inicial correspondiente a la iniciación del tráfico, el túnel entre el primero y el Router2 se establece correctamente.
   b. Después del establecimiento del túnel, el contador ACL en el Router1 se estabiliza y no exhibe incrementos adicionales, lo que indica que la regla ACL se ha igualado y ahora permite de manera consistente el tráfico a través del túnel establecido.
3. Reinicio del túnel:
   El contador ACL en el Router1 experimenta otro incremento sólo si el túnel cae y requiere el restablecimiento. Esto sugiere que la regla ACL es activada por la iniciación de tráfico inicial que intenta establecer el túnel, en lugar de por la transferencia de datos en curso una vez que el túnel está activo.

En resumen, este escenario demuestra que el contador ACL en el Router1 es sensible a los intentos de tráfico iniciales para la creación del túnel, pero permanece estático una vez que el túnel VPN está activo y en funcionamiento.



Situación 1:

Situación 2: Tráfico iniciado desde el Router 2 mientras el Túnel VPN está Activo

Estado inicial:

Túnel VPN que conecta el Router 1 (IP: 10.106.67.27) y Router2 (IP: 10.106.45.145) está activo y en funcionamiento.

Acción realizada:

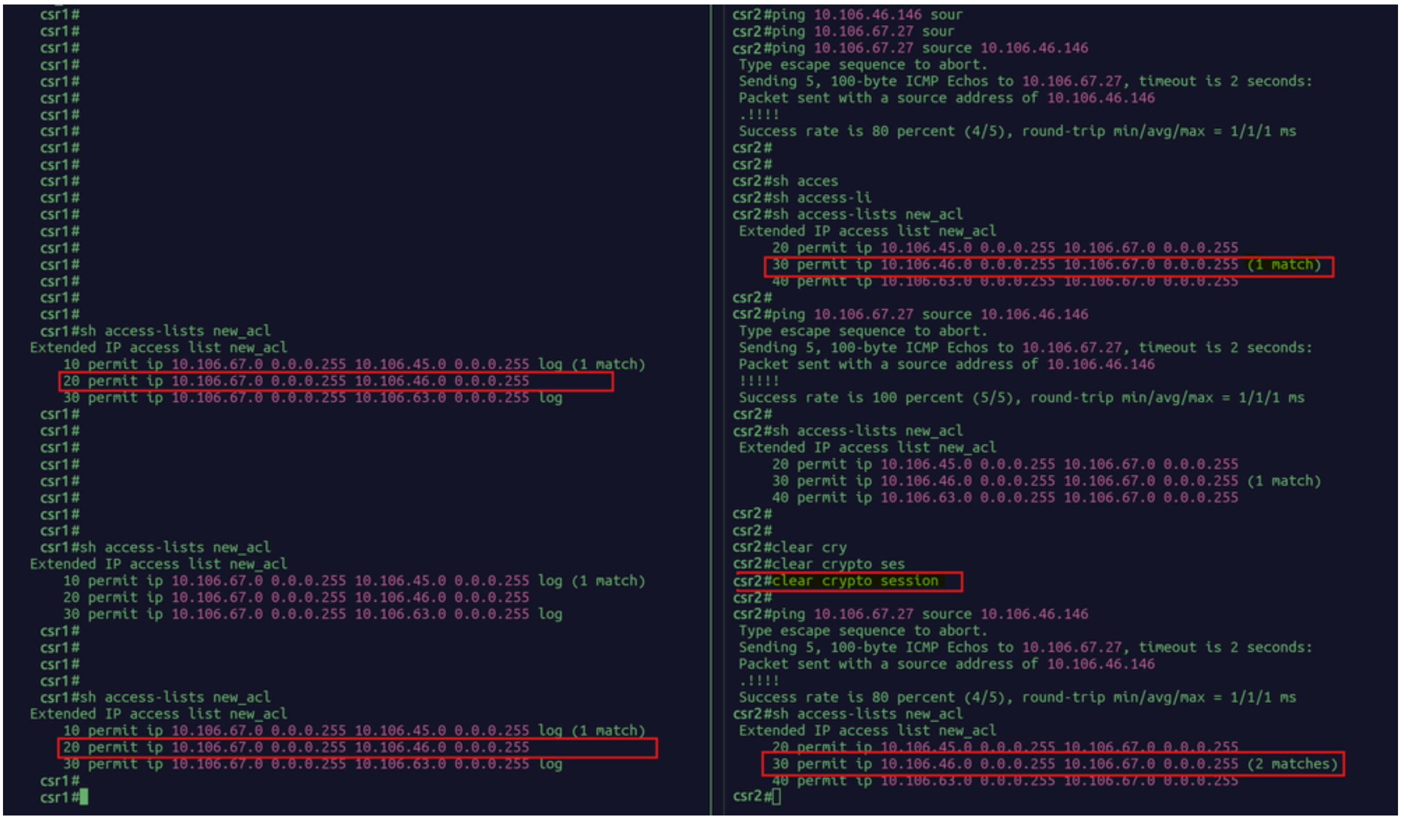
1. El tráfico se inicia desde el Router2 hacia el Router1 mientras el túnel está activo.
2. Posteriormente, el túnel se borra (o reinicia) deliberadamente.
3. Una vez borrado el túnel, el Router2 inicia el tráfico nuevamente para restablecer la conexión.

Observaciones:

1. Inicio del tráfico inicial:
   a. Cuando el tráfico se inicia por primera vez desde el Router2 mientras el túnel ya está establecido, no hay ningún cambio inmediato en el contador de la Lista de control de acceso (ACL).
   b. Esto indica que el tráfico en curso dentro de un túnel ya establecido no activa el incremento del contador ACL.
2. Borrado y Reinicio del Túnel:
   a. Al despejar el túnel, la conexión establecida entre el primero y el Router 2 se interrumpe temporalmente. Esto requiere un proceso de restablecimiento para cualquier tráfico posterior.
   b. Cuando el tráfico se reinicia desde el Router2 después de que el túnel ha sido despejado, hay un incremento observable en el contador ACL en el Router2. Este incremento significa que las reglas ACL se están activando una vez más para facilitar la creación del túnel.
3. Especificidad del contador ACL:
   El incremento en el contador ACL ocurre solamente en el lado que inicia el tráfico, que en

este caso es el Router2. Este comportamiento resalta el rol de la ACL en el monitoreo y control de los procesos de iniciación del tráfico en el lado de origen, mientras que el contador ACL del Router1 no se ve afectado durante esta fase.

En resumen, este escenario ilustra que el contador ACL en el Router2 responde a la iniciación del tráfico cuando se restablece un túnel VPN. El contador no aumenta con el flujo de tráfico regular dentro de un túnel activo, sino que reacciona ante la necesidad de restablecer el túnel, lo que garantiza un seguimiento preciso de los eventos de inicio del túnel.



Escenario 2

Conclusión:

El comportamiento de los contadores de ACL criptográficas revela que registran los recuentos de visitas exclusivamente durante la fase de inicio del túnel VPN.

Incremento Específico del Iniciador: Cuando el túnel se inicia desde el Router1, el aumento en el conteo de aciertos se observa solamente en el Router1. De manera similar, si la iniciación ocurre desde el Router2, el conteo de aciertos aumenta solamente en el Router2. Esto resalta el papel de la ACL en el monitoreo del proceso de iniciación del tráfico en el origen.

Estabilidad después del establecimiento: Una vez que el túnel se establece con éxito, los contadores de ACL en ambos peers permanecen sin cambios, lo que indica que no hay más aciertos. Esta estabilidad persiste hasta que el túnel se borra o se reinicia, y se intenta de nuevo el inicio del tráfico.
Este comportamiento subraya la funcionalidad de las listas de control de acceso en el seguimiento y control de la fase inicial de creación del túnel, asegurándose de que el flujo de

datos subsiguiente dentro del túnel establecido no afecte a los recuentos de visitas.

Puntos clave:

Comportamiento del Contador ACL: Los contadores ACL registran incrementos exclusivamente en el lado del iniciador durante el proceso de inicio del túnel. Esto indica que los contadores están diseñados para monitorear el tráfico inicial que dispara el establecimiento del túnel.

Contadores estáticos después del establecimiento: Una vez que el túnel está activo y establecido, los contadores de ACL permanecen sin cambios. No reflejan ninguna actividad adicional a menos que se reinicie el túnel y deba reiniciarse, lo que subraya el foco en los eventos de tráfico iniciales.

Especificidad de inicio de tráfico: Los conteos de aciertos de ACL son específicos del peer que inicia el túnel. Esta especificidad garantiza un seguimiento preciso de qué lado es responsable de iniciar la conexión VPN, lo que permite una supervisión y un control precisos.

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).