Comprender las diferencias de recuperación de SPI en SD-WAN y túneles tradicionales

Contenido

Introducción

Este documento describe cómo recuperar túneles SD-WAN y de terceros del error %RECVD_PKT_INV_SPI.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software (SD-WAN) Cisco Catalyst
- Seguridad de protocolo de Internet (IPSec).
- Detección de reenvío bidireccional (BFD).

Componentes Utilizados

La información de este documento se basa en:

- Cisco IOS® XE Catalyst SD-WAN Edges.

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.

Problema

El concepto de asociación de seguridad (SA) es fundamental para IPSec. Una SA es una relación entre dos terminales que describe cómo los terminales utilizan los servicios de seguridad para comunicarse de forma segura.

Un índice de parámetros de seguridad (SPI) es un número de 32 bits que se elige para identificar de forma exclusiva una SA determinada para cualquier dispositivo conectado que utilice IPSec.

Uno de los problemas más comunes de IPsec es que las SA pueden perder la sincronización debido a un valor SPI no válido, lo que, en consecuencia, provoca que un túnel IPSEC pierda el estado a medida que el par descarta los paquetes y se reciben mensajes de syslog en el router.

Túneles de terceros:

```
Jan  8 15:00:23.723 EDT: : %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
```

Para túneles SD-WAN:

```
Jan 10 12:18:43.404 EDT: : %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
```

Estos registros van acompañados de caídas en el procesador Quantum Flow Processor (QFP) que pertenece al procesador de reenvío (FP).

<#root>

```
Router#
show platform hardware qfp active feature ipsec datapath drops

----------------------------------------------------------------------
Drop Type Name                                                Packets
----------------------------------------------------------------------
1 IN_V4_PKT_HIT_INVALID_SA                                          1
4 IN_US_V4_PKT_SA_NOT_FOUND_SPI 9393888 <-- sub code error

19 IN_OCT_ANTI_REPLAY_FAIL                                        342
```

Solución

Recuperación para túneles IPSec tradicionales

Para recuperar los túneles IPSec tradicionales, es necesario forzar manualmente la renegociación

de la relación de valores SAs actuales; esto se realiza borrando las SAs IPSec con el comando de modo EXEC:

```
<#root>

Router#

clear crypto sa peer 10.20.20.1
```

Recuperación de túneles SD-WAN: situación 1

El comando EXEC clear crypto sa peer sólo funciona para los túneles IPSec tradicionales debido a la existencia de Intercambio de claves de Internet (IKE), que negocia automáticamente la asociación y genera un nuevo valor SPI. Sin embargo, no es posible utilizar ese comando en un túnel SD-WAN. Esto se debe a que en los túneles SD-WAN no se utiliza IKE.

Debido a esto, se utiliza un comando homólogo para los túneles SD-WAN:

```
<#root>

Router#

request platform software sdwan security ipsec-rekey
```

El comando request platform software sdwan security ipsec-rekey genera una nueva clave inmediatamente y, a continuación, aparece el túnel. De la manera opuesta, el comando no afecta a un túnel IPSec tradicional si existe.

Nota: El comando request platform software sdwan security ipsec-rekey este comando tiene efecto en todos los túneles SD-WAN existentes opuestos al clear crypto sa peer que tiene efecto solamente en la SA especificada.

Recuperación de túneles SD-WAN: situación 2

Si por error se utiliza el comando clear crypto sa peer para eliminar una de las SA de túneles SD-WAN, la eliminación se realiza correctamente; sin embargo, no se genera un nuevo valor SPI nuevamente, porque en un túnel SD-WAN, OMP es el que desencadena esa acción no IKE. Una vez en este estado, incluso si el comando request platform software sdwan security ipsec-rekey se ejecuta después del clear crypto sa peer, el túnel no se activa. Las encapsulaciones y desencapsulaciones de SA permanecen en cero, por lo tanto, la sesión BFD permanece en un estado inactivo.

```
Router#clear crypto sa peer 10.20.20.1
Router#show crypto ipsec sa peer 10.20.20.1
interface: Tunnel10001
Crypto map tag: Tunnel10001-vesen-head-0, local addr 10.10.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/12346)
remote ident (addr/mask/prot/port): (10.20.20.1/255.255.255.255/0/12366)
current_peer 10.20.20.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

La única opción de recuperación después de la eliminación de SA es con CUALQUIERA DE ESTOS tres comandos EXEC:

<#root>

```
Router#
```

clear sdwan omp all

El comando clear sdwan omp all aletea todas las sesiones BFD presentes en el dispositivo.

<#root>

```
Router#
```

request platforms software sdwan port_hop

El comando clear sdwan control connections hace que el TLOC utilice el siguiente número de puerto disponible en el color local especificado, lo que causa una inestabilidad no sólo de todas las sesiones BFD de ese color, sino también de las conexiones de control de ese color.

<#root>

```
Router#
```

clear sdwan control connections

El último comando también ayuda en la recuperación, sin embargo, el impacto de la misma es en todas las conexiones de control y sesiones BFD presentes en el dispositivo.

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).