Errores del IPSec %RECVD_PKT_INV_SPI e información de la función de recuperación del SPID inválido

Contenido

Introducción

Este documento describe el problema del IPSec cuando las asociaciones de seguridad (SA) se convierten fuera de sincronizan entre los dispositivos de peer.

Problema

Uno de la mayoría de los problemas del IPSec comunes es que los SA pueden convertirse fuera de sincronizan entre los dispositivos de peer. Como consecuencia, un dispositivo que cifra cifra el tráfico con los SA que su par no conoce alrededor. Estos paquetes son caídos por el par y este mensaje aparece en el Syslog:

```
Sep  2 13:27:57.707: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
has invalid spi for destaddr=20.1.1.2, prot=50, spi=0xB761863E(3076621886),
srcaddr=10.1.1.1
```

> Nota: Con el NAT-T, los mensajes **RECVD_PKT_INV_SPI** no fueron señalados correctamente hasta que el Id. de bug Cisco CSCsq59183 fuera reparado. (El IPSec no señala los mensajes **RECVD_PKT_INV_SPI** con el NAT-T.)

> Nota: En la plataforma del Routers de los servicios de la agregación de Cisco (ASR), los mensajes **%CRYPTO-4-RECVD_PKT_INV_SPI** no fueron implementados hasta la versión 2.3.2 (12.2(33)XNC2) del ® XE del Cisco IOS. También observe con la plataforma ASR, ese este descenso determinado se registra bajo ambos el contador de caídas global del procesador del flujo de Quantum (QFP) así como en el contador de caídas de la característica del IPSec, tal y como se muestra en de los próximos ejemplos.

```
Router# show platform hardware qfp active statistics drop | inc Ipsec
IpsecDenyDrop 0 0
IpsecIkeIndicate 0 0
IpsecInput 0 0 <======
IpsecInvalidSa 0 0
IpsecOutput 0 0
IpsecTailDrop 0 0
IpsecTedIndicate 0 0Router# show platform hardware qfp active feature ipsec datapath drops all |
in SPI
```

```
4 IN_US_V4_PKT_SA_NOT_FOUND_SPI 64574 <======
7 IN_TRANS_V4_IPSEC_PKT_NOT_FOUND_SPI 0
12 IN_US_V6_PKT_SA_NOT_FOUND_SPI 0
```

Es importante observar que este mensaje particular es tarifa limitada en el Cisco IOS hasta una tasa de uno por el minuto por los motivos de seguridad obvios. Si este mensaje para un flujo determinado (SRC, DST, o SPI) aparece solamente una vez en el registro, después puede ser que sea solamente una condición transitoria que está presente al mismo tiempo que el IPSec reintroduce donde un par pudo comenzar a utilizar el nuevo SA mientras que el dispositivo de peer no es muy listo para utilizar el mismo SA. Esto no es normalmente un problema, pues es solamente temporal y afectaría solamente a algunos paquetes. Sin embargo, ha habido los bug donde esto puede ser un problema.

> Consejo: Por los ejemplos, vea por favor el Id. de bug Cisco CSCsl68327 (la pérdida del paquete durante reintroduce), el Id. de bug Cisco CSCtr14840 (ASR: las caídas de paquetes durante la fase 2 reintroducen bajo ciertas condiciones), o el Id. de bug Cisco CSCty30063 (el ASR utiliza nuevo SPI antes de que los finales QM).

Alternativamente, hay un problema si más de un caso del mismo mensaje se observa para señalar mismo SPI para el mismo flujo, tal como estos mensajes:

```
Router# show platform hardware qfp active feature ipsec datapath drops all | in SPI
4 IN_US_V4_PKT_SA_NOT_FOUND_SPI 64574 <======
7 IN_TRANS_V4_IPSEC_PKT_NOT_FOUND_SPI 0
12 IN_US_V6_PKT_SA_NOT_FOUND_SPI 0
```

Esto es una indicación que el tráfico negro-está agujereado y no pudo recuperarse hasta que los SA expiren en el dispositivo remitente o hasta que se activa el Dead Peer Detection (DPD).

Solución

Esta sección proporciona la información que usted puede utilizar para resolver el problema que se describe en la sección anterior.

Recuperación del SPID inválido

Para resolver este problema, Cisco recomienda que usted habilita la función de recuperación del SPID inválido. Por ejemplo, ingrese el comando **crypto de la inválido-SPI-recuperación del isakmp**. Aquí están algunas NOTAS IMPORTANTES que describen el uso de este comando:

- Primero, la recuperación del SPID inválido sirve solamente como mecanismo de recuperación cuando los SA están fuera de sincronizan. Ayuda a recuperarse de esta condición, pero no aborda el problema de la raíz fuera del cual hizo los SA convertirse sincronizan en el primer lugar. Para entender mejor la causa raíz, usted debe permitir al ISAKMP y a los debugs del IPSec en ambos puntos extremos del túnel. Si ocurre el problema a menudo, después obtenga los debugs e intente dirigir la causa raíz (y no apenas enmascarar el problema).

- Hay un concepto erróneo común sobre el propósito y las funciones del comando **crypto de la inválido-SPI-recuperación del isakmp**. Incluso sin este comando, el Cisco IOS realiza ya un tipo de funciones de la recuperación del SPID inválido cuando envía una notificación de la CANCELACIÓN al par de envío para el SA se recibe que si tiene ya IKE SA con ese par. Una vez más esto ocurre sin importar si el comando **crypto de la inválido-SPI-recuperación del**

isakmp está activado.

- El comando **crypto de la inválido-SPI-recuperación del isakmp** intenta dirigir la condición donde un router recibe el tráfico IPSec con el SPID inválido, y no tiene IKE SA con ese par. En este caso, intenta establecer a una nueva sesión IKE con el par y envía una notificación de la CANCELACIÓN sobre IKE creado recientemente SA. Sin embargo, este comando no funciona para todas las configuraciones de criptografía. Las únicas configuraciones para las cuales este comando trabaja son las correspondencias de criptografía estática donde definen al par explícitamente y los peeres estáticos que se derivan de los mapas de criptografía ejemplificados, tales como VTI. Aquí está un resumen de las configuraciones de criptografía de uso general y si la recuperación del SPID inválido trabaja con esa configuración:

Configuración de criptografía	¿Recuperación del SPID inválido?
Correspondencia de criptografía estática	Sí
Correspondencia cifrada dinámica	No
P2P GRE con el TP	Sí
mGRE TP que utiliza con el mapeo NHRP estático	Sí
mGRE TP que utiliza con el mapeo NHRP dinámico	No
sVTI	Sí
Cliente EzVPN	N/A

Mensajes de error intermitentes del SPID inválido del Troubleshooting

Muchas veces el mensaje de error del SPID inválido ocurre intermitentemente. Esto hace difícil resolver problemas, mientras que llega a ser muy duro recoger los debugs relevantes. Los scripts integrados del administrador del evento (EEM) pueden ser muy útiles en este caso.

> Nota: Para más detalles, refiera a los scripts EEM usados para resolver problemas las aletas del túnel causadas por el documento de Cisco inválido de los índices del parámetro de seguridad.