Verifique los errores %RECVD_PKT_INV_SPI de IPsec y la información de la función de recuperación SPI no válida

Contenido

Introducción

Este documento describe el problema de IPsec cuando las asociaciones de seguridad (SA) no están sincronizadas entre los dispositivos pares.

Problema

Uno de los problemas más comunes de IPsec es que las SA pueden perder la sincronización entre los dispositivos pares. Como resultado, un dispositivo cifrado cifra el tráfico con SA que su par no conoce. El par descarta estos paquetes y aparece este mensaje 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=10.10.1.2, prot=50, spi=0xB761863E(3076621886),
srcaddr=10.1.1.1
```

> **Nota:** Con NAT-T, los mensajes **RECVD_PKT_INV_SPI** no se notificaron correctamente hasta que se corrigió el Id. de bug Cisco CSCsq59183. (IPsec no informa de mensajes **RECVD_PKT_INV_SPI** con NAT-T.)

> **Nota:** En la plataforma Cisco Aggregation Services Routers (ASR), los mensajes **%CRYPTO-4-RECVD_PKT_INV_SPI** no se implementaron hasta Cisco IOS® XE Release 2.3.2 (12.2(33)XNC2). Tenga en cuenta también con la plataforma ASR que esta caída en particular se registra tanto en el contador de caídas del procesador de flujo cuántico (QFP) global como en el contador de caídas de funciones de IPSec, como se muestra en los siguientes 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 0

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
```

Es importante tener en cuenta que este mensaje en particular está limitado por velocidad en Cisco IOS a una velocidad de uno por minuto por las razones de seguridad obvias. Si este mensaje para un flujo determinado (SRC, DST o SPI) solo aparece una vez en el registro, solo puede ser una condición transitoria que esté presente al mismo tiempo que la regeneración de clave IPsec, donde un par puede comenzar a utilizar la nueva SA mientras el dispositivo par no esté listo para utilizar la misma SA. Normalmente, esto no es un problema, ya que es solo temporal y solo afectaría a unos pocos paquetes. Sin embargo, ha habido errores en los que esto puede ser un problema.

> **Consejo:** Para ver ejemplos, consulte Cisco bug ID CSCsl68327 (Packet loss during rekey), Cisco bug ID CSCtr14840 (ASR: caídas de paquetes durante la fase 2 (regeneración de claves en determinadas condiciones) o ID de bug de Cisco CSCty30063 (ASR utiliza el nuevo SPI antes de que finalice QM).

También existe un problema si se observa que más de una instancia del mismo mensaje informa el mismo SPI para el mismo flujo, como estos mensajes:

```
Sep  2 13:36:47.287: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
has invalid spi for destaddr=10.10.1.2, prot=50, spi=0x1DB73BBB(498547643),
srcaddr=10.1.1.1 Sep 2 13:37:48.039: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
has invalid spi for destaddr=10.10.1.2, prot=50, spi=0x1DB73BBB(498547643),
srcaddr=10.1.1.1
```

Esto indica que el tráfico tiene agujeros negros y no se puede recuperar hasta que caduquen las SA en el dispositivo que envía o hasta que se active la detección de punto muerto (DPD).

Solución

Esta sección proporciona información que puede utilizar para resolver el problema descrito en la sección anterior.

Recuperación SPI no válida

Para resolver este problema, Cisco recomienda que habilite la función de recuperación SPI no válida. Por ejemplo, ingrese el comando **crypto isakmp invalid-spi-recovery**. A continuación se indican algunas notas importantes que describen el uso de este comando:

- En primer lugar, la recuperación SPI no válida solo sirve como mecanismo de recuperación cuando las SA no están sincronizadas. Ayuda a recuperarse de esta condición, pero no resuelve el problema raíz que causó que las SA se desincronizaran en primer lugar. Para entender mejor la causa raíz, debe habilitar los debugs ISAKMP e IPsec en ambos extremos del túnel. Si el problema ocurre con frecuencia, obtenga los debugs e intente abordar la causa raíz (y no sólo enmascarar el problema).

- Hay un error común acerca del propósito y la funcionalidad del comando **crypto isakmp invalid-spi-recovery**. Incluso sin este comando, Cisco IOS ya realiza un tipo de funcionalidad de recuperación SPI no válida cuando envía una notificación DELETE al par remitente para la SA que se recibe si ya tiene una SA IKE con ese par. Nuevamente, esto ocurre independientemente de si se activa el comando **crypto isakmp invalid-spi-recovery**.

- El comando **crypto isakmp invalid-spi-recovery** intenta abordar la condición en la que un router recibe tráfico IPsec con SPI no válido y no tiene una SA IKE con ese par. En este caso, intenta establecer una nueva sesión IKE con el par y envía una notificación DELETE sobre la SA IKE recién creada. Sin embargo, este comando no funciona para todas las configuraciones de criptografía. Las únicas configuraciones para las que funciona este comando son mapas criptográficos estáticos donde el par está definido explícitamente y pares estáticos que derivan de mapas criptográficos instanciados, como VTI. A continuación se muestra un resumen de las configuraciones criptográficas utilizadas habitualmente y si la recuperación SPI no válida funciona con esa configuración:

Configuración criptográfica	¿Recuperación SPI no válida?
crypto-map estático	Yes
Mapa criptográfico dinámico	No
GRE P2P con protección de túnel	Yes
Protección de túnel mGRE que utiliza asignación NHRP estática	Yes
Protección de túnel mGRE que utiliza asignación NHRP dinámica	No
sVTI	Yes
cliente EzVPN	N/A

Resolución de problemas de mensajes de error SPI intermitentes no válidos

Muchas veces el mensaje de error SPI inválido ocurre intermitentemente. Esto dificulta la resolución de problemas, ya que se hace muy difícil recopilar las depuraciones relevantes. Las secuencias de comandos de Embedded Event Manager (EEM) pueden ser muy útiles en este caso.

> **Nota:** Para obtener más detalles, consulte el documento de Cisco Scripts EEM utilizados para resolver problemas de inestabilidad de túnel causados por índices de parámetros de seguridad no válidos.

Error de funcionamiento conocido

Esta lista muestra errores que pueden causar que las SAs IPsec se dessincronicen o estén relacionados con la recuperación SPI no válida:

- Cisco bug ID CSCvn31824 Cisco IOS-XE ISAKMP elimina el nuevo SPI si se devuelve un nuevo paquete SPI antes de que se realice la instalación
- Id. de error de Cisco CSCvd40554 IKEv2: Cisco IOS no puede analizar la notificación INV_SPI con el tamaño de SPI 0 - envía INVALID_SYNTAX
- ID de bug de Cisco CSCvp16730 Los paquetes ESP entrantes con valor SPI que comienza con 0xFF se descartan debido a un error SPI no válido

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).