Verificare gli errori IPsec %RECVD_PKT_INV_SPI e le informazioni sulla funzionalità di ripristino SPI non valide

Sommario

Introduzione

Problema

Soluzione

Ripristino SPI non valido

Risoluzione dei problemi relativi ai messaggi di errore SPI non validi intermittenti

Bug noti

Introduzione

In questo documento viene descritto il problema di IPSec quando le associazioni di sicurezza non sono più sincronizzate tra i dispositivi peer.

Problema

Uno dei problemi più comuni di IPSec è che le associazioni di protezione possono non essere più sincronizzate tra i dispositivi peer. Di conseguenza, un dispositivo crittografato crittografa il traffico con le associazioni di protezione di cui il peer non è a conoscenza. Questi pacchetti vengono scartati dal peer e questo messaggio viene visualizzato nel 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, i messaggi RECVD_PKT_INV_SPI non sono stati segnalati correttamente finché non è stato risolto l'ID bug Cisco CSCsq59183. (IPsec non segnala messaggi RECVD_PKT_INV_SPI con NAT-T.)

Nota: Sulla piattaforma Cisco Aggregation Services Router (ASR), i messaggi %CRYPTO-4-RECVD_PKT_INV_SPI non sono stati implementati fino alla versione 12.2(33)XNC2 di Cisco IOS® XE. Notare inoltre con la piattaforma ASR che questa particolare perdita viene registrata sia nel contatore di perdita QFP (Quantum Flow Processor) globale sia nel contatore di perdita delle funzionalità IPsec, come mostrato negli esempi seguenti.

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</pre>
```

Èimportante notare che questo particolare messaggio ha una velocità limitata in Cisco IOS di uno al minuto per ovvi motivi di sicurezza. Se il messaggio relativo a un particolare flusso (SRC, DST o SPI) viene visualizzato una sola volta nel registro, può trattarsi solo di una condizione transitoria presente contemporaneamente alla reimpostazione della chiave IPsec, in cui un peer può iniziare a utilizzare la nuova SA mentre il dispositivo peer non è ancora pronto a utilizzare la stessa SA. Questo normalmente non è un problema, in quanto è solo temporaneo e influirebbe solo su pochi pacchetti. Tuttavia, ci sono stati bug che potevano rappresentare un problema.

Suggerimento: Per alcuni esempi, vedere l'ID bug Cisco <u>CSCsl68327</u> (perdita di pacchetti durante la reimpostazione della chiave), l'ID bug Cisco <u>CSCtr14840</u> (ASR: il pacchetto viene scartato durante la fase 2 (in alcune condizioni) o l'ID bug Cisco <u>CSCty30063</u> (l'ASR usa il nuovo SPI prima del termine del QM).

In alternativa, si verifica un problema se si osserva più di un'istanza dello stesso messaggio per segnalare lo stesso SPI per lo stesso flusso, ad esempio i messaggi seguenti:

```
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
```

Ciò indica che il traffico è bloccato e non può essere ripristinato finché le SA non scadono sul dispositivo che invia i dati o finché non viene attivato il rilevamento peer inattivi (DPD, Dead Peer Detection).

Soluzione

In questa sezione vengono fornite informazioni che è possibile utilizzare per risolvere il problema descritto nella sezione precedente.

Ripristino SPI non valido

Per risolvere questo problema, Cisco consiglia di abilitare la funzione di ripristino SPI non valida. Ad esempio, immettere il comando **crypto isakmp invalid-spi-recovery**. Di seguito sono riportate alcune note importanti che descrivono l'utilizzo di questo comando:

In primo luogo, il ripristino SPI non valido funge da meccanismo di ripristino solo quando le
associazioni di protezione non sono sincronizzate. Consente il ripristino da questa condizione,
ma non risolve il problema principale che ha causato la mancata sincronizzazione delle
associazioni di protezione. Per comprendere meglio la causa principale, abilitare i debug
ISAKMP e IPsec su entrambi gli endpoint del tunnel. Se il problema si verifica spesso,
eseguire i debug e cercare di risolvere la causa principale (e non solo mascherare il
problema).

- In genere, lo scopo e la funzionalità del comando crypto isakmp invalid-spi-recovery sono
 errati. Anche senza questo comando, Cisco IOS esegue già un tipo di funzionalità di ripristino
 SPI non valida quando invia una notifica DELETE al peer di invio per l'associazione di
 protezione ricevuta se già dispone di un'associazione di protezione IKE con tale peer. Anche
 in questo caso, ciò si verifica indipendentemente dal fatto che il comando crypto isakmp
 invalid-spi-recovery sia attivato.
- Il comando crypto isakmp invalid-spi-recovery tenta di risolvere la condizione in cui un router riceve il traffico IPsec con SPI non valido e non dispone di un'associazione di sicurezza IKE con il peer. In questo caso, tenta di stabilire una nuova sessione IKE con il peer e invia una notifica DELETE sull'associazione di protezione IKE appena creata. Tuttavia, questo comando non funziona per tutte le configurazioni crittografiche. Le uniche configurazioni per cui funziona questo comando sono le mappe crittografiche statiche in cui il peer è definito in modo esplicito e i peer statici derivati dalle mappe crittografiche istanziate, ad esempio VTI. Di seguito è riportato un riepilogo delle configurazioni crittografiche comunemente utilizzate e se il ripristino SPI non valido funziona con tale configurazione:

Configurazione della crittografia	Ripristino SPI non valido?
Mappa crittografica statica	Sì
Mappa crittografica dinamica	No
P2P GRE con protezione tunnel	Sì
Protezione del tunnel GRE con mapping NHRP statico	Sì
Protezione del tunnel GRE che utilizza il mapping NHRP dinamico	No
sVTI	Sì
Client EzVPN	N/D

Risoluzione dei problemi relativi ai messaggi di errore SPI non validi intermittenti

In molti casi il messaggio di errore SPI non valido viene visualizzato in modo intermittente. Ciò rende difficile la risoluzione dei problemi, in quanto diventa molto difficile raccogliere i debug rilevanti. Gli script Embedded Event Manager (EEM) possono essere molto utili in questo caso.

Nota: Per ulteriori informazioni, fare riferimento al documento Cisco sugli script EEM utilizzati per risolvere i problemi di flap del tunnel causati da indici dei parametri di sicurezza non validi.

Bug noti

Nell'elenco vengono mostrati i bug che possono causare il mancato sincronismo delle associazioni di protezione IPsec o essere correlati a un ripristino SPI non valido:

- Cisco ID bug <u>CSCvn31824</u> Cisco IOS-XE ISAKMP elimina il nuovo SPI se prima dell'installazione non viene eseguito l'aggiornamento del pacchetto SPI
- ID bug Cisco <u>CSCvd40554</u> IKEv2: Cisco IOS: impossibile analizzare la notifica INV_SPI con dimensione SPI 0. Invia INVALID_SYNTAX
- ID bug Cisco CSCvp16730 I pacchetti ESP in arrivo con valore SPI che inizia con 0xFF vengono scartati a causa di un errore SPI non valido

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l' accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).