Erreurs d'IPsec %RECVD_PKT_INV_SPI et informations non valides de caractéristique de reprise SPI

Contenu

Introduction

Ce document décrit la question d'IPsec quand les associations de sécurité (SAS) deviennent hors du sync entre les périphériques de pair.

Problème

Une des questions d'IPsec les plus communes est que SAS peut devenir hors du sync entre les périphériques de pair. En conséquence, un périphérique chiffrant chiffre le trafic avec SAS que son pair ne connaît pas. Ces paquets sont lâchés par le pair et ce message apparaît dans le 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
```

> **Note**: Avec NAT-T, des messages **RECVD_PKT_INV_SPI** n'ont pas été correctement signalés jusqu'à ce que l'ID de bogue Cisco CSCsq59183 ait été réparé. (IPsec ne signale pas des messages **RECVD_PKT_INV_SPI** avec NAT-T.)

> **Note**: Sur la plate-forme des Routeurs de services d'agrégation de Cisco (ASR), les messages **%CRYPTO-4-RECVD_PKT_INV_SPI** n'ont pas été mis en application jusqu'à ce que la version 2.3.2 (12.2(33)XNC2) du Cisco IOS® XE. Également la note avec la plate-forme ASR, cette cette baisse particulière est enregistrée sous chacun des deux le compteur global de baisse du processeur d'écoulement de Quantum (QFP) aussi bien que dans le compteur de baisse de caractéristique d'IPsec, suivant les indications des exemples suivants.

```
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
```

Il est important de noter que ce message particulier est débit-limité dans le Cisco IOS à un taux d'un par minute pour les raisons de sécurité évidentes. Si ce message pour un flux particulier (SRC, DST, ou SPI) apparaît seulement une fois dans le log, alors ce pourrait seulement être un état passager qui est présent en même temps que le rekey d'IPsec où un pair pourrait commencer à utiliser nouvelle SA alors que le périphérique de pair n'est pas tout à fait prêt à employer même SA. Ce n'est normalement pas un problème, car il est seulement provisoire et affecterait seulement quelques paquets. Cependant, il y a eu des bogues où ceci peut être un problème.

> **Conseil** : Pour des exemples, voir s'il vous plaît l'ID de bogue Cisco CSCsl68327 (perte de paquets pendant le rekey), l'ID de bogue Cisco CSCtr14840 (ASR : pertes de paquets pendant le rekey de la phase 2 dans certaines conditions), ou ID de bogue Cisco CSCty30063 (l'ASR utilise le nouveau SPI avant que des finitions QM).

Alternativement, il y a un problème si on observe plus d'un exemple du même message pour signaler le même SPI pour le même écoulement, tel que ces messages :

```
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
```

C'est une indication que le trafic noir-est troué et ne pourrait pas récupérer jusqu'à ce que SAS expirent sur le périphérique de envoi ou jusqu'à ce que Dead Peer Detection (DPD) est lancé.

Solution

Cette section fournit les informations que vous pouvez employer afin de résoudre le problème qui est décrit dans la section précédente.

Reprise non valide SPI

Afin de résoudre ce problème, Cisco recommande que vous activiez la caractéristique non valide de reprise SPI. Par exemple, sélectionnez la commande de **crypto isakmp invalid-spi-recovery**. Voici quelques informations importantes qui décrivent l'utilisation de cette commande :

- D'abord, la reprise non valide SPI sert seulement de mécanisme de reprise quand SAS sont hors de sync. Il aide à récupérer de cette condition, mais il n'aborde pas la question de racine qui a fait devenir SAS hors du sync en premier lieu. Afin de comprendre mieux la cause principale, vous devez permettre à l'ISAKMP et IPsec met au point sur chacun des deux points d'extrémité de tunnel. Si le problème se pose souvent, alors obtenez met au point et tentative d'adresser la cause principale (et masquer pas simplement le problème).

- Il y a une fausse idée commune au sujet du but et de la fonctionnalité de la commande de **crypto isakmp invalid-spi-recovery**. Même sans cette commande, le Cisco IOS exécute déjà

un type de fonctionnalité non valide de reprise SPI quand il envoie une notification d'EFFACEMENT au pair de envoi pour SA qui est reçue si elle a déjà IKE SA avec ce pair. De nouveau, ceci se produit indépendamment de si la commande de **crypto isakmp invalid-spi-recovery** est lancée.

- Les tentatives de commande de **crypto isakmp invalid-spi-recovery** d'adresser la condition où un routeur reçoit le trafic d'IPsec avec le SPI non valide, et lui n'a pas IKE SA avec ce pair. Dans ce cas, il essaye d'établir une nouvelle session d'IKE avec le pair et envoie une notification d'EFFACEMENT au-dessus d'IKE de création récente SA. Cependant, cette commande ne fonctionne pas pour toutes les crypto-configurations. Les seules configurations pour lesquelles cette commande fonctionne sont les crypto map statiques où le pair est explicitement défini et les pairs statiques qui sont dérivés des crypto map instanciés, tels que VTI. Voici un résumé des crypto-configurations utilisées généralement et si la reprise non valide SPI fonctionne avec cette configuration :

Crypto-configuration	Reprise non valide SPI ?
Crypto map statique	Oui
Crypto-carte dynamique	Non
P2P GRE avec le tunnel protection	Oui
tunnel protection de mGRE qui l'utilise avec le mappage statique de NHRP	Oui
tunnel protection de mGRE qui l'utilise avec le mappage dynamique de NHRP	Non
sVTI	Oui
Client d'EzVPN	S/O

Dépannez les messages d'erreur non valides intermittents SPI

Beaucoup de fois le message d'erreur non valide SPI se produit par intermittence. Ceci le rend difficile à dépanner, pendant qu'il devient très difficile de collecter l'approprié met au point. Les scripts inclus du gestionnaire d'événement (EEM) peuvent être très utiles dans ce cas.

> **Note**: Pour plus de détails, référez-vous aux scripts EEM utilisés pour dépanner des instabilités de tunnel provoquées par le document Cisco non valide d'index de paramètre de Sécurité.