Vérification des erreurs IPsec %RECVD_PKT_INV_SPI et des informations de fonctionnalité de récupération SPI non valides

Contenu

Introduction

Ce document décrit le problème IPsec lorsque les associations de sécurité (SA) ne sont plus synchronisées entre les périphériques homologues.

Problème

L'un des problèmes les plus courants liés à IPsec est que les associations de sécurité peuvent devenir désynchronisées entre les périphériques homologues. Par conséquent, un périphérique chiffré chiffre le trafic avec des SA que son homologue ne connaît pas. Ces paquets sont abandonnés par l'homologue 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=10.10.1.2, prot=50, spi=0xB761863E(3076621886),
srcaddr=10.1.1.1
```

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

> **Note**: Sur la plate-forme Cisco Aggregation Services Routers (ASR), les messages **%CRYPTO-4-RECVD_PKT_INV_SPI n'**ont pas été mis en oeuvre avant Cisco IOS® XE version 2.3.2 (12.2(33)XNC2). Notez également avec la plate-forme ASR que cette suppression particulière est enregistrée à la fois dans le compteur de suppression QFP (Quantum Flow Processor) global et dans le compteur de suppression de fonctionnalité IPsec, comme indiqué dans les 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 limité en débit dans Cisco IOS à un débit d'une par minute pour des raisons évidentes de sécurité. Si ce message pour un flux particulier (SRC, DST ou SPI) n'apparaît qu'une seule fois dans le journal, alors il ne peut s'agir que d'une condition transitoire qui est présente en même temps que la nouvelle clé IPsec où un homologue peut commencer à utiliser la nouvelle SA alors que le périphérique homologue n'est pas tout à fait prêt à utiliser la même SA. Ce n'est normalement pas un problème, car il n'est que temporaire et n'affecterait que quelques paquets. Cependant, il y a eu des bogues où cela peut être un problème.

> **Astuce** : Pour obtenir des exemples, consultez l'ID de bogue Cisco CSCsl68327 (Perte de paquets lors d'une nouvelle clé), l'ID de bogue Cisco CSCtr14840 (ASR : abandons de paquets lors de la phase 2 (nouvelle clé dans certaines conditions) ou ID de bogue Cisco CSCty30063 (ASR utilise un nouveau SPI avant la fin de QM).

Il existe également un problème si plusieurs instances du même message sont observées pour signaler le même SPI pour le même flux, par exemple les messages suivants :

```
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
```

Cela indique que le trafic est bloqué et ne peut pas être récupéré tant que les SA n'expirent pas sur le périphérique qui envoie ou tant que la détection d'homologue mort (DPD) n'est pas activée.

Solution

Cette section fournit des informations que vous pouvez utiliser pour résoudre le problème décrit dans la section précédente.

Récupération SPI non valide

Pour résoudre ce problème, Cisco recommande d'activer la fonctionnalité de récupération SPI non valide. Par exemple, entrez la commande **crypto isakmp invalid-spi-recovery**. Voici quelques remarques importantes qui décrivent l'utilisation de cette commande :

- Tout d'abord, la récupération SPI non valide sert de mécanisme de récupération uniquement lorsque les SA ne sont pas synchronisées. Il permet de récupérer à partir de cette condition, mais il ne résout pas le problème racine qui a causé la désynchronisation des SA en premier lieu. Afin de mieux comprendre la cause première, vous devez activer les débogages ISAKMP et IPsec sur les deux points d'extrémité du tunnel. Si le problème se produit souvent, obtenez les débogages et essayez de résoudre la cause première (et pas seulement de masquer le

problème).

- Il y a une idée fausse commune sur le but et la fonctionnalité de la commande **crypto isakmp invalid-spi-recovery**. Même sans cette commande, Cisco IOS exécute déjà un type de fonctionnalité de récupération SPI non valide lorsqu'il envoie une notification DELETE à l'homologue expéditeur pour l'association de sécurité qui est reçue s'il a déjà une association de sécurité IKE avec cet homologue. Encore une fois, cela se produit indépendamment du fait que la commande **crypto isakmp invalid-spi-recovery** soit activée.

- La commande **crypto isakmp invalid-spi-recovery** tente de résoudre la condition dans laquelle un routeur reçoit du trafic IPsec avec un SPI non valide, et il n'a pas d'association de sécurité IKE avec cet homologue. Dans ce cas, il tente d'établir une nouvelle session IKE avec l'homologue et envoie une notification DELETE sur la SA IKE nouvellement créée. Cependant, cette commande ne fonctionne pas pour toutes les configurations de chiffrement. Les seules configurations pour lesquelles cette commande fonctionne sont les crypto-cartes statiques où l'homologue est explicitement défini et les homologues statiques qui sont dérivés de crypto-cartes instanciées, telles que VTI. Voici un résumé des configurations de chiffrement couramment utilisées et si la récupération SPI non valide fonctionne avec cette configuration :

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

Dépanner les messages d'erreur SPI non valides intermittents

Souvent, le message d'erreur SPI non valide apparaît par intermittence. Cela rend le dépannage difficile, car il devient très difficile de collecter les débogages appropriés. Les scripts EEM (Embedded Event Manager) peuvent être très utiles dans ce cas.

> **Note**: Pour plus de détails, référez-vous au document Cisco Scripts EEM utilisés pour dépanner les failles de tunnel provoquées par des index de paramètres de sécurité non valides.

Bogues connus

Cette liste montre les bogues qui peuvent provoquer la désynchronisation des SA IPsec ou liés à la récupération SPI non valide :

- ID de bogue Cisco CSCvn31824 Cisco IOS-XE ISAKMP supprime le nouveau SPI si rx nouveau paquet SPI avant l'installation
- ID de bogue Cisco CSCvd4054 IKEv2 : Cisco IOS ne peut pas analyser la notification INV_SPI avec SPI taille 0 - envoie INVALID_SYNTAX

- ID de bogue Cisco CSCvp16730 Les paquets ESP entrants dont la valeur SPI commence par 0xFF sont abandonnés en raison d'une erreur SPI non valide

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.