Comprendre les différences entre SD-WAN et tunnels traditionnels SPI Recover

Table des matières

Introduction

Ce document décrit comment récupérer les tunnels SD-WAN et tiers à partir de l'erreur %RECVD_PKT_INV_SPI.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) Cisco Catalyst
- Sécurité du protocole Internet (IPSec).
- Détection de transfert bidirectionnel (BFD).

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Périphériques SD-WAN du Catalyst Cisco IOS® XE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Le concept d'association de sécurité (SA) est fondamental pour IPSec. Une association de sécurité est une relation entre deux points d'extrémité qui décrit la manière dont les points d'extrémité utilisent les services de sécurité pour communiquer en toute sécurité.

Un index de paramètres de sécurité (SPI) est un nombre de 32 bits qui est choisi pour identifier de manière unique une association de sécurité particulière pour tout périphérique connecté utilisant IPSec.

L'un des problèmes les plus courants d'IPsec est que les SA peuvent devenir désynchronisées en raison d'une valeur SPI non valide, ce qui entraîne par conséquent un état d'arrêt du tunnel IPSEC lorsque les paquets sont abandonnés par l'homologue et que des messages syslog sont reçus dans le routeur.

Tunnels tiers :

```
Jan  8 15:00:23.723 EDT: : %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
```

Pour les tunnels SD-WAN :

```
Jan 10 12:18:43.404 EDT: : %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
```

Ces journaux sont accompagnés de pertes dans le processeur de flux quantique (QFP) qui appartient au processeur de transfert (FP).

<#root>

```
Router#
show platform hardware qfp active feature ipsec datapath drops

----------------------------------------------------------------------
Drop Type Name                                                Packets
----------------------------------------------------------------------
1 IN_V4_PKT_HIT_INVALID_SA                                          1
4 IN_US_V4_PKT_SA_NOT_FOUND_SPI 9393888 <-- sub code error

19 IN_OCT_ANTI_REPLAY_FAIL                                        342
```

Solution

Récupération des tunnels IPSec traditionnels

Afin de récupérer les tunnels IPSec traditionnels, il est nécessaire de forcer manuellement la renégociation de la relation des valeurs des SA actuelles ; ceci est effectué en effaçant les SA IPSec avec la commande du mode EXEC :

```
<#root>

Router#

clear crypto sa peer 10.20.20.1
```

Récupération pour les tunnels SD-WAN - Scénario 1

La commande EXEC clear crypto sa peer fonctionne uniquement pour les tunnels IPSec traditionnels en raison de l'existence d'Internet Key Exchange (IKE), qui négocie automatiquement l'association et génère une nouvelle valeur SPI. Cependant, il n'est pas possible d'utiliser cette commande sur un tunnel SD-WAN. La raison en est que dans les tunnels SD-WAN, IKE n'est pas utilisé.

Pour cette raison, une commande homologue pour les tunnels SD-WAN est utilisée :

```
<#root>

Router#

request platform software sdwan security ipsec-rekey
```

La commande request platform software sdwan security ipsec-rekey génère une nouvelle clé immédiatement, puis le tunnel s'active. De la manière opposée, la commande n'affecte pas un tunnel IPSec traditionnel s'il existe.

Remarque : le logiciel de plate-forme de requête sdwan security ipsec-rekey cette commande prend effet dans tous les tunnels SD-WAN existants en face de l'homologue clear crypto sa qui prend effet uniquement dans l'association de sécurité spécifiée.

Récupération pour les tunnels SD-WAN - Scénario 2

Si par erreur la commande clear crypto sa peer est utilisée pour supprimer l'une des SA de tunnels SD-WAN, la suppression se produit avec succès ; cependant, une nouvelle valeur SPI n'est pas générée à nouveau, parce que dans un tunnel SD-WAN, OMP est celui qui déclenche cette action pas IKE. Une fois dans cet état, même si la commande request platform software sdwan security ipsec-rekey est émise après le clear crypto sa peer, le tunnel ne s'affiche pas. Les encapsulations et décapsulations de la SA restent à zéro, par conséquent la session BFD reste à l'état down.

```
Router#clear crypto sa peer 10.20.20.1
Router#show crypto ipsec sa peer 10.20.20.1
interface: Tunnel10001
Crypto map tag: Tunnel10001-vesen-head-0, local addr 10.10.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/12346)
remote ident (addr/mask/prot/port): (10.20.20.1/255.255.255.255/0/12366)
current_peer 10.20.20.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

La seule option de récupération après la suppression de l'association de sécurité est avec L'UNE DE CES trois commandes EXEC :

<#root>

```
Router#
clear sdwan omp all
```

La commande clear sdwan omp all fait basculer toutes les sessions BFD présentes dans le périphérique.

<#root>

```
Router#
request platforms software sdwan port_hop
```

La commande clear sdwan control connections amène le TLOC à utiliser le prochain numéro de port disponible sur la couleur locale spécifiée, ce qui provoque un battement non seulement de toutes les sessions BFD de cette couleur, mais aussi des connexions de contrôle de cette couleur.

<#root>

```
Router#
```

```
clear sdwan control connections
```

La dernière commande aide également à la récupération, mais son impact se fait sentir sur toutes les connexions de contrôle et les sessions BFD présentes dans le périphérique.

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.