Comprendere le differenze tra SD-WAN e tunnel tradizionali SPI Recover

Sommario

Introduzione

In questo documento viene descritto come ripristinare SD-WAN e tunnel di terze parti dall'errore %RECVD_PKT_INV_SPI.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Software Cisco Catalyst Defined Wide Area Network (SD-WAN)
- IPSec (Internet Protocol Security).
- Rilevamento inoltro bidirezionale (BFD).

Componenti usati

Le informazioni fornite in questo documento si basano su:

- Bordi Cisco IOS® XE Catalyst SD-WAN.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Il concetto di associazione di sicurezza (SA, Security Association) è fondamentale per IPSec. Un'associazione di sicurezza è una relazione tra due endpoint che descrive il modo in cui gli endpoint utilizzano i servizi di sicurezza per comunicare in modo sicuro.

Un indice SPI (Security Parameter Index) è un numero a 32 bit scelto per identificare in modo univoco un'associazione di protezione specifica per qualsiasi dispositivo connesso che utilizza IPSec.

Uno dei problemi più comuni di IPSec è che le associazioni di protezione possono non essere sincronizzate a causa di un valore SPI non valido. Questa situazione causa uno stato di inattività del tunnel IPSEC quando i pacchetti vengono scartati dal peer e i messaggi syslog vengono ricevuti nel router.

Tunnel di terze parti:

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

Per tunnel SD-WAN:

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

Questi log sono accompagnati da cadute nel Quantum Flow Processor (QFP) che appartiene al Forwarding Processor (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
```

Soluzione

Ripristino per tunnel IPSec tradizionali

Per ripristinare i tunnel IPSec tradizionali, è necessario forzare manualmente la rinegoziazione della relazione corrente dei valori delle SA. Questa operazione viene eseguita cancellando le SA IPSec con il comando EXEC mode:

```
<#root>

Router#

clear crypto sa peer 10.20.20.1
```

Ripristino per tunnel SD-WAN - Scenario 1

Il comando clear crypto sa peer EXEC funziona solo sui tunnel IPSec tradizionali a causa dell'esistenza di Internet Key Exchange (IKE), negozia automaticamente l'associazione e genera un nuovo valore SPI. Tuttavia, non è possibile usare questo comando su un tunnel SD-WAN. Ciò si verifica perché nei tunnel SD-WAN non viene utilizzato lo standard IKE.

Per questo motivo, viene usato un comando omologo per i tunnel SD-WAN:

```
<#root>

Router#

request platform software sdwan security ipsec-rekey
```

Il comando request platform software sdwan security ipsec-rekey genera immediatamente una nuova chiave, quindi il tunnel si attiva. Al contrario, il comando non influisce su un tunnel IPSec tradizionale, se esistente.

Nota: il software della piattaforma di richiesta sdwan security ipsec-rekey. Questo comando ha effetto su tutti i tunnel SD-WAN esistenti opposti al peer clear crypto sa che ha effetto solo nell'associazione di sicurezza specificata.

Ripristino per tunnel SD-WAN - Scenario 2

Se per errore viene usato il comando clear crypto sa peer per eliminare una delle associazioni di protezione dei tunnel SD-WAN, l'eliminazione ha esito positivo. Tuttavia, non viene generato nuovamente un nuovo valore SPI, perché in un tunnel SD-WAN, OMP è quello che attiva quell'azione e non IKE. In questo stato, anche se il comando request platform software sdwan security ipsec-rekey viene emesso dopo che il peer clear crypto sa, il tunnel non compare. Gli incapsulamenti e i decapsulamenti dell'associazione di protezione rimangono a zero, di conseguenza la sessione BFD rimane nello stato inattivo.

```
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
```

L'unica opzione di ripristino dopo l'eliminazione dell'associazione di protezione è con uno dei tre comandi EXEC seguenti:

<#root>

```
Router#
```

clear sdwan omp all

Il comando clear sdwan omp all esegue il flap di tutte le sessioni BFD presenti nel dispositivo.

<#root>

```
Router#
```

request platforms software sdwan port_hop

Il comando clear sdwan control connections fa in modo che il TLOC utilizzi il successivo numero di porta disponibile sul colore locale specificato, il che provoca un flap non solo di tutte le sessioni BFD di quel colore, ma anche delle connessioni di controllo di quel colore.

<#root>

```
Router#
```

clear sdwan control connections

Anche l'ultimo comando aiuta nel ripristino, tuttavia il suo impatto è su tutte le connessioni di controllo e le sessioni BFD presenti nel dispositivo.

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).