Inzicht in verschillen tussen SD-WAN en traditionele tunnels voor SPI-herstel

Inhoud

Inleiding

Dit document beschrijft hoe u SD-WAN- en third party tunnels kunt herstellen van een fout met %RECVD_PKT_INV_SPI.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Catalyst softwaregedefinieerde Wide Area Network (SD-WAN)
- Internet Protocol Security (IPSec).
- Detectie van bidirectioneel doorsturen (BFD).

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Cisco IOS® XE Catalyst SD-WAN randen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

Het concept van een Security Association (SA) is fundamenteel voor IPSec. Een SA is een relatie tussen twee endpoints die beschrijft hoe de endpoints security services gebruiken om veilig te communiceren.

Een Security Parameter Index (SPI) is een 32-bits getal dat wordt gekozen om een bepaalde SA voor een aangesloten apparaat uniek te identificeren met behulp van IPSec.

Een van de meest voorkomende IPsec-problemen is dat SA's niet meer kunnen worden gesynchroniseerd vanwege een ongeldige SPI-waarde. Dat veroorzaakt dan ook een IPSEC-tunnelstatus omdat de pakketten door de peer worden gedropt en syslogberichten in de router worden ontvangen.

Tunnels van derden:

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

Voor SD-WAN tunnels:

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

Deze logboeken gaan gepaard met druppels in de Quantum Flow Processor (QFP) die tot de Forwarding Processor (FP) behoort.

<#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
```

Oplossing

Herstel voor traditionele IPSec-tunnels

Om traditionele IPSec-tunnels te herstellen is het nodig de heronderhandeling van de huidige SAs-waardenrelatie handmatig af te dwingen; dit wordt uitgevoerd door de IPSec SAs met de opdracht EXEC-modus te wissen:

```
<#root>

Router#

clear crypto sa peer 10.20.20.1
```

Herstel voor SD-WAN tunnels - scenario 1

De duidelijke crypto als peer EXEC-opdracht werkt alleen voor traditionele IPSec-tunnels vanwege het bestaan van Internet Key Exchange (IKE), die onderhandelt automatisch over de vereniging en genereert een nieuwe SPI-waarde. Het is echter niet mogelijk om dat commando op een SD-WAN Tunnel te gebruiken. De reden hiervoor is dat in SD-WAN tunnels IKE niet wordt gebruikt.

Daarom wordt een homologe opdracht voor SD-WAN tunnels gebruikt:

```
<#root>

Router#

request platform software sdwan security ipsec-rekey
```

Het verzoek platform software sdwan security ipsec-rekey commando genereert onmiddellijk een nieuwe sleutel, dan komt de tunnel omhoog. Op de tegenovergestelde manier heeft de opdracht geen invloed op een traditionele IPSec-tunnel als deze bestaat.

Opmerking: de request platform software sdwan security ipsec-rekey deze opdracht wordt uitgevoerd in alle bestaande SD-WAN tunnels tegenover de duidelijke crypto sa peer die alleen in de opgegeven SA van kracht wordt.

Herstel voor SD-WAN tunnels - scenario 2

Als de duidelijke crypto als peer opdracht wordt gebruikt om een van de SD-WAN tunnels SAs te verwijderen, gebeurt de verwijdering succesvol; echter, een nieuwe SPI waarde wordt niet opnieuw gegenereerd, omdat in een SD-WAN Tunnel, OMP is degene die die actie niet IKE veroorzaakt. Eenmaal in deze status, zelfs of de opdrachtaanvraag platformen software sdwan security ipsec-rekey wordt uitgegeven na de duidelijke crypto als peer, komt de Tunnel niet omhoog. De inkapseling en decapsulaties van de SA blijven in nul, als gevolg daarvan blijft de BFD sessie in een down staat.

```
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
```

De enige hersteloptie na de verwijdering van de SA is met OM HET EVEN WELK VAN DEZE drie EXEC bevelen:

<#root>

```
Router#
```

clear sdwan omp all

De duidelijke sdwan omp alle commando flaps alle BFD sessies aanwezig in het apparaat.

<#root>

```
Router#
```

request platforms software sdwan port_hop

De opdracht clear Sdwan control connections zorgt ervoor dat de TLOC het volgende beschikbare poortnummer op de lokale kleur gebruikt die is opgegeven. Hierdoor wordt een flap veroorzaakt van niet alleen alle BFD-sessies van die kleur, maar ook de besturingsverbindingen van die kleur.

<#root>

```
Router#
```

clear sdwan control connections

De laatste opdracht helpt ook bij het herstel, maar de impact ervan is op alle besturingsverbindingen en BFD-sessies aanwezig in het apparaat.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.