Kennenlernen von SD-WAN und traditionellen Tunneln SPI Recover Differences

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Problem

Lösung

- Recovery für herkömmliche IPSec-Tunnel
- Wiederherstellung für SD-WAN-Tunnel - Szenario 1
- Wiederherstellung für SD-WAN-Tunnel - Szenario 2

Einleitung

Dieses Dokument beschreibt die Wiederherstellung von SD-WAN- und Drittanbietertunneln nach dem Fehler %RECVD_PKT_INV_SPI.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Catalyst Software-Defined Wide Area Network (SD-WAN)
- Internetprotokollsicherheit (IPSec).
- Bidirectional Forwarding Detection (BFD)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Cisco IOS® XE Catalyst SD-WAN-Edges.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

Das Konzept einer Security Association (SA) ist grundlegend für IPSec. Ein SA ist eine Beziehung zwischen zwei Endpunkten, in der beschrieben wird, wie die Endpunkte Sicherheitsdienste für die sichere Kommunikation nutzen.

Ein Security Parameter Index (SPI) ist eine 32-Bit-Nummer, die ausgewählt wird, um eine bestimmte Sicherheitszuordnung für ein angeschlossenes Gerät mit IPSec eindeutig zu identifizieren.

Eines der häufigsten IPsec-Probleme ist, dass SAs aufgrund eines ungültigen SPI-Werts nicht synchronisiert sind. Dies führt zu einem IPSEC-Tunnelausfall, da die Pakete vom Peer verworfen werden und Syslog-Meldungen auf dem Router empfangen werden.

Drittanbieter-Tunnel:

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

Für SD-WAN-Tunnel:

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

Diese Protokolle werden von Löschungen im Quantum Flow Processor (QFP) begleitet, der zum Forwarding Processor (FP) gehört.

<#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
```

Lösung

Recovery für herkömmliche IPSec-Tunnel

Um herkömmliche IPSec-Tunnel wiederherzustellen, muss die Neuverhandlung der aktuellen SAs-Wertbeziehung manuell erzwungen werden. Hierzu müssen die IPSec-SAs mit dem Befehl "EXEC mode" gelöscht werden:

```
<#root>

Router#

clear crypto sa peer 10.20.20.1
```

Wiederherstellung für SD-WAN-Tunnel - Szenario 1

Der Befehl clear crypto sa peer EXEC funktioniert nur für traditionelle IPSec-Tunnel, da es Internet Key Exchange (IKE) gibt, das die Zuordnung automatisch aushandelt und einen neuen SPI-Wert generiert. Es ist jedoch nicht möglich, diesen Befehl in einem SD-WAN-Tunnel zu verwenden. Der Grund dafür ist, dass in SD-WAN-Tunneln kein IKE verwendet wird.

Aus diesem Grund wird ein einheitlicher Befehl für SD-WAN-Tunnel verwendet:

```
<#root>

Router#

request platform software sdwan security ipsec-rekey
```

Der Befehl request platform software sdwan security ipsec-rekey generiert sofort einen neuen Schlüssel und der Tunnel wird gestartet. Umgekehrt wirkt sich der Befehl nicht auf einen herkömmlichen IPSec-Tunnel aus, wenn dieser vorhanden ist.

Hinweis: Die Anforderungsplattform-Software sdwan security ipsec-rekey dieses Befehls wird in allen vorhandenen SD-WAN-Tunneln wirksam, gegenüber dem Clear Crypto sa Peer, der nur in der angegebenen SA wirksam wird.

Wiederherstellung für SD-WAN-Tunnel - Szenario 2

Wenn versehentlich der Befehl clear crypto sa peer verwendet wird, um eine der SAs des SD-WAN-Tunnels zu löschen, erfolgt das Löschen erfolgreich. Es wird jedoch kein neuer SPI-Wert generiert, da OMP in einem SD-WAN-Tunnel diejenige ist, die diese Aktion auslöst, nicht IKE. Einmal in diesem Status, auch wenn der Befehl Anforderungsplattformen Software sdwan Sicherheit ipsec-rekey nach der klaren Crypto als Peer ausgegeben wird, der Tunnel kommt nicht. Die Kapselungen und Entkapselungen des SAs verbleiben bei Null, sodass die BFD-Sitzung nicht verfügbar bleibt.

```
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
```

Die einzige Wiederherstellungsoption nach dem Löschen des SA ist mit IRGENDEINEM DER FOLGENDEN drei EXEC-Befehle:

<#root>

```
Router#

clear sdwan omp all
```

Mit dem Befehl clear sdwan omp all werden alle im Gerät vorhandenen BFD-Sitzungen als Flaps angezeigt.

<#root>

```
Router#

request platforms software sdwan port_hop
```

Der Befehl clear sdwan control connections veranlasst den TLOC, die nächste verfügbare Port-Nummer auf der angegebenen lokalen Farbe zu verwenden, was zu einem Flapping nicht nur aller BFD-Sitzungen dieser Farbe, sondern auch der Steuerverbindungen dieser Farbe führt.

<#root>

```
Router#

clear sdwan control connections
```

Der letzte Befehl unterstützt ebenfalls die Wiederherstellung, allerdings wirkt sich dieser Befehl auf alle Steuerungsverbindungen und BFD-Sitzungen im Gerät aus.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.