瞭解SD-WAN和傳統隧道SPI恢復差異

目錄

簡介

本文描述如何從%RECVD_PKT_INV_SPI錯誤中恢復SD-WAN和第三方隧道。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Catalyst軟體定義廣域網路(SD-WAN)
- 網際網路通訊協定安全(IPSec)。
- 雙向轉發檢測(BFD)。

採用元件

本檔案中的資訊是根據：

- Cisco IOS® XE Catalyst SD-WAN邊緣。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

安全關聯(SA)的概念是IPSec的基礎。SA是兩個端點之間的關係，描述端點如何使用安全服務進行安全通訊。

安全引數索引(SPI)是32位數，可選擇用於為使用IPSec的任何連線的裝置唯一地標識特定SA。

最常見的IPsec問題之一是SA可能由於無效的SPI值而不同步，從而導致對等路由器丟棄資料包和系統日誌消息在路由器中接收時出現IPSEC隧道關閉狀態。

第三方隧道：

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

對於SD-WAN隧道：

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

這些日誌伴有屬於轉發處理器(FP)的量子流處理器(QFP)中的丟包。

```
<#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
```

解決方案

傳統IPSec通道的復原

為了恢復傳統IPSec隧道，必須手動強制重新協商當前SA值關係；這可通過使用EXEC模式命令清除IPSec SA來執行：

```
<#root>

Router#

clear crypto sa peer 10.20.20.1
```

SD-WAN通道的復原 — 案例1

clear crypto sa peer EXEC命令僅適用於傳統IPSec通道，因為存在網際網路金鑰交換(IKE), 自動協商關聯並生成新的SPI值。但是，無法在SD-WAN隧道上使用該命令。這是因為在SD-WAN通道中，未使用IKE。

因此，使用SD-WAN通道的同源命令：

```
<#root>

Router#

request platform software sdwan security ipsec-rekey
```

request platform software sdwan security ipsec-rekey命令將立即生成新金鑰，然後隧道將啟動。相反，如果傳統IPSec通道存在，該命令不會對其產生影響。

註:request platform software sdwan security ipsec-rekey 此命令在所有現有的SD-WAN隧道中生效，與clear crypto sa peer相反，後者僅在指定的SA中生效。

SD-WAN通道的復原 — 案例2

如果錯誤地使用clear crypto sa peer命令刪除了某個SD-WAN隧道SA，則刪除成功；但是，不會再次生成新的SPI值，因為在SD-WAN隧道中，OMP是觸發該操作的命令，而不是IKE。一旦處於此狀態，即使command request platforms software sdwan security ipsec-rekey在clear crypto sa peer後發出，隧道也不會啟動。SA的封裝和解除封裝保持為零，因此BFD會話保持關閉狀態。

```
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
```

刪除SA後的唯一恢複選項是使用以下三種EXEC命令中的任意一個：

<#root>

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

clear sdwan omp all命令會交換裝置中存在的所有BFD會話。

<#root>

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

clear sdwan control connections命令會使TLOC使用指定本地顏色上的下一個可用埠號，這不僅會導致該顏色的所有BFD會話發生翻動，而且還會導致該顏色的控制連線。

<#root>

```
Router#
clear sdwan control connections
```

最後一個命令也有助於恢復，但是它對裝置中存在的所有控制連線和BFD會話都有影響。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。