

Catalyst 9500和Nexus 9000之間的MACSec XPN流量失敗，無效資料包和FCS錯誤增加

目錄

問題

在Catalyst 9500-28C8D和Nexus N9K-C93180YC-FX之間啟用MACSec XPN時，MKA會話成功建立，但沒有資料流量通過鏈路。Catalyst 9500報告物理介面上的SA統計資訊和FCS輸入錯誤下增加了「Notvalid pkts」。具體來說，可以觀察到以下症狀：

- 啟用MACSec後無連線
- MKA會話顯示為已建立，但Catalyst 9500端顯示的SA統計資訊中「Notvalid pkts 118」增加且「Valid pkts:0」
- Catalyst 9500物理介面上的FCS輸入錯誤增加
- 刪除MACSec配置會立即恢復連線並停止FCS錯誤

MKA會話在兩個裝置上建立，並成功協商了GCM-AES-XPN-256密碼。Nexus端顯示加密處於活動狀態，但Catalyst 9500已收到加密資料包並由於驗證不匹配而將其拒絕，導致接受零個有效資料包。

環境

- 執行Cisco IOS®的Catalyst 9500-28C8D
- Nexus N9K-C93180YC-FX
- 使用GCM-AES-XPN-256密碼套件的MACSec XPN配置
- 400 Gigabit乙太網路介面 (Catalyst上的400GigE 1/0/15, Nexus上的Ethernet1/52)
- Catalyst 9500配置為金鑰伺服器優先順序1, Nexus配置為金鑰伺服器優先順序100

- 用於預共用金鑰的AES-256-CMAC加密演算法

解析

此問題通過實施一種變通方法解決，該方法更改了裝置之間的關鍵伺服器角色分配。建議的解決方案涉及以下步驟：

步驟 1:確定關鍵伺服器配置問題

檢驗兩台裝置上的當前金鑰伺服器優先順序配置。有問題的配置顯示：

Catalyst 9500組態：

```
mka policy MEHEALTH-ORG-XPN
  key-server priority 1
  macsec-cipher-suite gcm-aes-xpn-256
```

Nexus配置

```
macsec policy MEHEALTH-ORG-XPN
  key-server-priority 100
```

步驟 2:實施金鑰伺服器角色解決方法

將Nexus裝置配置為MACSec金鑰伺服器而不是Catalyst 9500。這包括調整金鑰伺服器優先順序值，以便Nexus承擔金鑰伺服器角色。

修改Nexus配置，使其具有較低的金鑰伺服器優先順序值（較低的值具有更高的優先順序）：

```
macsec policy MEHEALTH-ORG-XPN
  key-server-priority 1
```

修改Catalyst 9500配置以具有更高的金鑰伺服器優先順序值：

```
mka policy MEHEALTH-ORG-XPN
key-server priority 100
macsec-cipher-suite gcm-aes-xpn-256
```

步驟 3:驗證MACSec操作

實施金鑰伺服器角色更改後，請驗證：

- 在兩台裝置上成功建立MKA會話
- 資料流量通過啟用MACSec的鏈路
- Catalyst 9500 SA統計資訊上沒有遞增的「Notvalid pkts」
- 物理介面上未發生FCS輸入錯誤

此解決方法允許MACSec XPN配置正常運作，直到平台調查和軟體升級計畫可以完成為止。

原因

此問題的根本原因與Cisco錯誤ID CSCvs00410有關，該錯誤描述的情況是，在與Nexus裝置之間的特定互操作性條件下，當使用AES-256-XPB和Catalyst 9500作為關鍵伺服器角色時，MKA會話建立成功，但資料無法通過鏈路。該行為表現為驗證不匹配，其中Catalyst 9500拒絕來自Nexus的加密資料包，導致無效資料包計數和FCS錯誤增加。在針對此缺陷將Cisco IOS列為固定版本方面，存在明顯差異，要求Catalyst平台團隊進行進一步調查。

相關內容

- 思科錯誤ID CSCvs00410 - MKA會話已啟動，但在使用具有Catalyst 9500金鑰伺服器角色的AES-256-XPB時，無法通過鏈路傳遞資料

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）。