驗證IPsec %RECVD_PKT_INV_SPI錯誤和無效的SPI恢復功能資訊

目錄

簡介

本文檔介紹當對等裝置之間的安全關聯(SA)不同步時的IPsec問題。

問題

最常見的IPsec問題之一是SA可能在對等裝置之間變得不同步。因此，加密端點使用對等體不知道的SA對流量進行加密。對等體會丟棄這些資料包，並且系統日誌中會顯示以下消息：

```
Sep  2 13:27:57.707: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
destaddr=10.10.1.2, prot=50, spi=0xB761863E(3076621886), srcaddr=10.1.1.1
```

> 注意：在Cisco IOS® XE路由平台(例如，Cisco Aggregation Services Routers (ASR)和Cisco Catalyst 8000系列路由器)上，此特定丟棄在全局量子流處理器(QFP)丟棄計數器和IPsec功能丟棄計數器下註冊，如下例所示。

```
Router# show platform hardware qfp active statistics drop | inc Ipsec
  IpsecDenyDrop                              0              0
  IpsecIkeIndicate                           0              0
  IpsecInput                                 0              0     <======
  IpsecInvalidSa                             0              0
  IpsecOutput                                0              0
  IpsecTailDrop                              0              0
  IpsecTedIndicate                           0              0



Router# show platform hardware qfp active feature ipsec datapath drops all | in SPI
        4   IN_US_V4_PKT_SA_NOT_FOUND_SPI                          64574    <======
```

```
  7  IN_TRANS_V4_IPSEC_PKT_NOT_FOUND_SPI                          0
 12  IN_US_V6_PKT_SA_NOT_FOUND_SPI                                0
```

必須注意的是，出於明顯的安全原因，此特定消息在Cisco IOS®中以每分鐘1的速率受速率限制。如果特定流（SRC、DST或SPI）的此消息在系統日誌中只出現一次，則很可能是IPsec金鑰更新同時出現的臨時情況，在該臨時情況下，對等裝置尚未完全準備好使用同一SA，一個對等裝置可以開始使用新SA。這通常不是問題，因為它只是暫時的，而且只會影響一些資料包。

但是，如果相同的流和SPI編號仍存在相同的消息，則表明對等體之間的IPSec SA不同步。舉例來說：

```
Sep  2 13:36:47.287: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
destaddr=10.10.1.2, prot=50, spi=0x1DB73BBB(498547643), srcaddr=10.1.1.1
Sep  2 13:37:48.039: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
destaddr=10.10.1.2, prot=50, spi=0x1DB73BBB(498547643), srcaddr=10.1.1.1
```

這表示流量被黑洞，在傳送裝置上的SA過期或啟用失效對等體檢測(DPD)之前無法恢復。

解決方案

本節提供的資訊可用於解決上一節中所述的問題。

無效的SPI復原

為了解決此問題，Cisco建議您啟用無效的SPI恢復功能。例如，輸入crypto isakmp invalid-spi-recovery 命令。以下是一些說明此命令用法的重要注意事項：

- 首先，無效的SPI恢復僅在SA不同步時用作恢復機制。它有助於從此情況恢復，但不會解決導致SA最初不同步的根問題。為了更好地瞭解根本原因，您必須在兩個隧道終點啟用ISAKMP和IPSec調試。如果問題經常發生，請取得偵錯並嘗試解決根本原因（而不僅僅是掩蓋問題）。

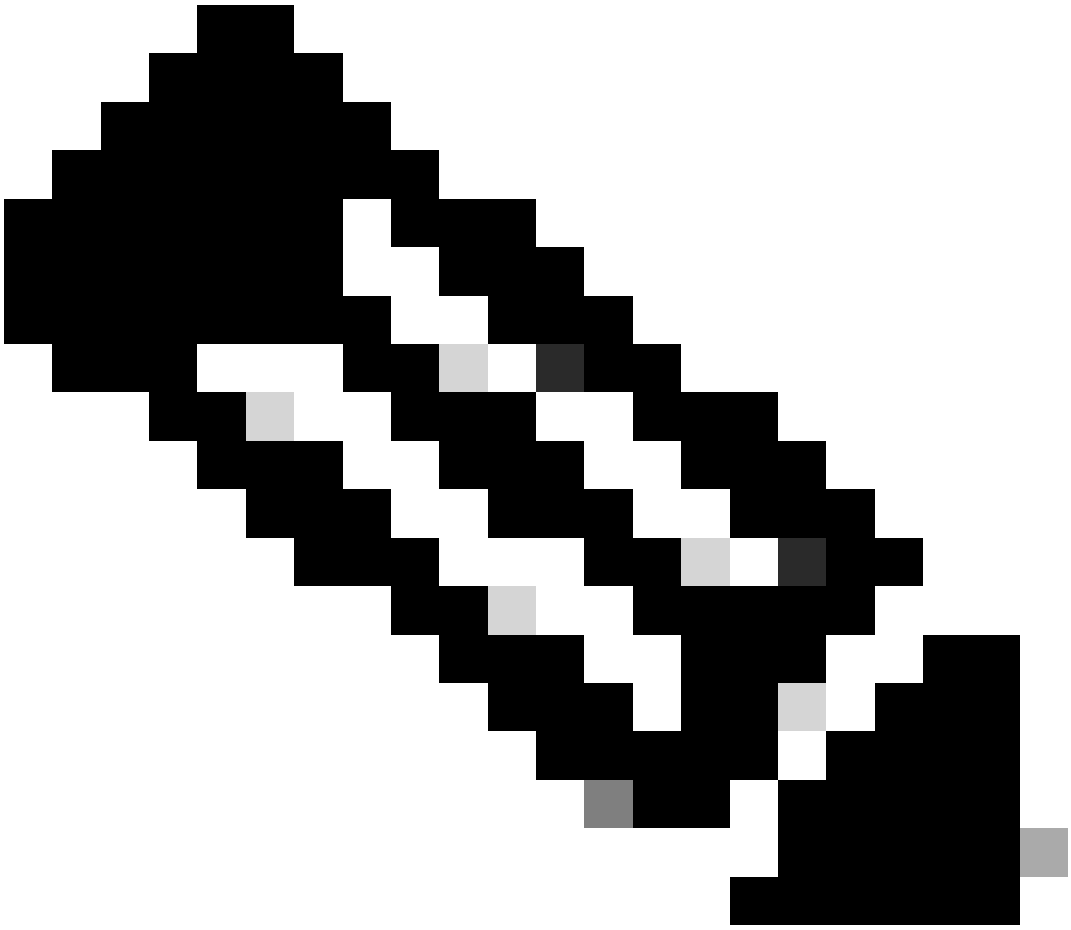
- 對於crypto isakmp invalid-spi-recovery命令的用途和功能，存在一種常見的誤解。即使沒有此命令，Cisco IOS也會在將DELETE通知傳送到所接收的SA的傳送對等體時，執行一種無效的SPI恢復功能，前提是該對等體已具有IKE SA。同樣，無論是否啟用crypto isakmp invalid-spi-recovery命令，都會出現這種情況。

- crypto isakmp invalid-spi-recovery命令可嘗試解決以下情況：路由器接收具有無效SPI的IPsec流量，但該對等體沒有IKE SA。在這種情況下，它將嘗試與對等體建立新的IKE會話，並透過新建立的IKE SA傳送DELETE通知。但是，此命令不適用於所有加密配置。此命令唯一適用的配置是靜態加密對映，其中對等體被顯式定義，靜態對等體派生自例項化加密對映，例如VTI。以下是常用加密配置的摘要以及無效SPI恢復是否適用於該配置：

加密配置	無效的SPI復原
靜態加密對映	是
動態加密對映	否
含通道保護的P2P GRE	是
使用靜態NHRP對映的mGRE隧道保護	是
使用動態NHRP對映的mGRE隧道保護	否
sVTI	是
EzVPN客戶端	不適用

排除間歇性無效SPI錯誤消息故障

許多時候，無效的SPI錯誤訊息會間歇地出現。由於收集相關的調試資訊非常困難，因此很難排除故障。在這種情況下，嵌入式事件管理器(EEM)指令碼可能非常有用。



注意：有關詳細資訊，請參閱Cisco文檔中用於解決由無效安全引數索引引起的隧道抖動的EEM指令碼。

已知的Bug

此清單顯示可能導致IPsec SA不同步或與無效SPI恢復相關的錯誤：

- 思科漏洞ID CSCvn31824 Cisco IOS XE ISAKMP會在完成安裝前刪除新的SPI（逐個SPI資料包）
- 思科漏洞ID CSCvd40554 IKEv2：思科IOS無法解析具有SPI大小0的INV_SPI通知-傳送INVALID_SYNTAX
- Cisco bug ID CSCvp16730 SPI值以0xFF開頭的傳入ESP資料包由於Invalid SPI錯誤而被丟棄

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）。