验证IPsec "%RECVD_PKT_INV_SPI"错误和无效的SPI恢复功能信息

目录

简介

问题

解决方案

- 无效的SPI恢复
- 对间歇性无效SPI错误消息进行故障排除
- 已知的 Bug

简介

本文档介绍安全关联 (SA) 在对等设备之间不同步时的 IPsec 问题。

问题

最常见的IPsec问题之一是SA在对等设备之间可能变得不同步。因此，加密终端使用对等体不知道的SA对流量进行加密。这些数据包被对等设备丢弃，系统日志中会显示以下消息：

```
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，思科聚合服务路由器(ASR)和Cisco Catalyst 8000系列路由器)上，此特定丢弃在全局量子流处理器(QFP)丢弃计数器和IPsec功能丢弃计数器下注册，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
```

请注意，出于明显的安全原因，此特定消息在Cisco IOS®中速率受限于每分钟1次。如果特定流（SRC、DST或SPI）的此消息仅在系统日志中出现一次，则很可能是IPsec密钥重新生成同时出现的临时情况，即一个对等体可以开始使用新的SA，而对等体设备尚未完全准备好使用同一SA。这通常不是问题，因为它只是暂时的，并且只会影响几个数据包。

但是，如果相同流和SPI编号仍存在相同消息，则表明对等体之间的IPsec SA已不同步。例如：

```
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
```

这表示流量被黑洞，在发送设备上的SA到期或激活失效对等体检测(DPD)之前无法恢复。

解决方案

本节提供可用于解决上一节中所述问题的信息。

无效的SPI恢复

为了解决此问题，Cisco建议您启用无效的SPI恢复功能。例如，输入crypto isakmp invalid-spi-recovery 命令。下面是一些描述此命令使用的重要说明：

- 首先，无效的SPI恢复仅在SA不同步时用作恢复机制。它有助于从此情况恢复，但不会解决导致SA首先失去同步的根问题。为了更好地了解根本原因，必须在两个隧道终端上启用ISAKMP和IPsec调试。如果问题经常发生，则获取调试并尝试解决根本原因（而不只是掩盖问题）。
- 对于crypto isakmp invalid-spi-recovery命令的用途和功能，存在常见的误解。即使没有此命令，Cisco IOS也会执行一种无效的SPI恢复功能，当它针对收到的SA向发送对等体发送DELETE通知时，如果该SA已经具有该对等体的IKE SA。同样，无论crypto isakmp invalid-spi-recovery命令是否激活，都会出现这种情况。
- crypto isakmp invalid-spi-recovery命令尝试解决路由器接收具有无效SPI的IPsec流量并且它

不具有与该对等体的IKE SA的情况。在这种情况下，它会尝试与对等体建立新的IKE会话，并通过新创建的IKE SA发送DELETE通知。但是，此命令不适用于所有加密配置。此命令唯一适用的配置是静态加密映射（其中明确定义了对等体）和静态对等体（衍生自实例化加密映射，例如VTI）。以下是常用加密配置的摘要以及无效SPI恢复是否适用于该配置：

加密配置	无效的SPI恢复
静态加密映射	Yes
动态加密映射	无
带隧道保护的P2P GRE	Yes
使用静态NHRP映射的mGRE隧道保护	Yes
使用动态NHRP映射的mGRE隧道保护	无
sVTI	Yes
EzVPN客户端	不适用

对间歇性无效SPI错误消息进行故障排除

多次出现无效SPI错误消息。由于收集相关调试变得非常困难，因此很难进行故障排除。在这种情况下，嵌入式事件管理器(EEM)脚本可能非常有用。

注意：有关详细信息，请参阅Cisco文档的EEM脚本，该脚本用于排除由无效安全参数索引引起的隧道摆动故障。

已知的 Bug

此列表显示可能导致IPsec SA不同步或与无效SPI恢复相关的漏洞：

- Cisco Bug ID CSCvn31824 Cisco IOS XE ISAKMP会删除新的SPI（如果在安装之前已收到新的SPI数据包）
- Cisco Bug ID CSCvd40554 IKEv2:Cisco IOS无法解析SPI大小为0的INV_SPI通知 — 发送INVALID_SYNTAX
- Cisco Bug ID CSCvp16730由于SPI错误无效，丢弃了SPI值以0xFF开头的传入ESP数据包

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。