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](#)
[排除故障断断续续无效的SPI错误消息](#)

简介

当安全关联(SA)变得不同步在对等设备之间时，本文描述IPsec问题。

问题

其中一个最普通的IPsec问题是SAS能变得不同步在对等设备之间。结果，一个加密的设备加密与其对等体不知道的SAS的流量。这些数据包由对等体丢弃，并且此消息在Syslog出现：

```
Sep  2 13:27:57.707: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
has invalid spi for destaddr=20.1.1.2, prot=50, spi=0xB761863E(3076621886),
srcaddr=10.1.1.1
```

> **Note**:使用NAT-T， **RECVD_PKT_INV_SPI**消息未正确地报告，直到Cisco Bug ID CSCsq59183修复。(IPsec不报告与NAT-T的**RECVD_PKT_INV_SPI**消息。)

> **Note**:在思科聚合服务路由器(ASR)平台上， **%CRYPTO-4-RECVD_PKT_INV_SPI**消息未实现直到Cisco IOS XE版本2.3.2 (12.2(33)XNC2)。并且注意用ASR平台，该此特定的丢弃注册在两个下全局Quantum流处理器(QFP)如以下的示例所显示，丢弃计数器以及在IPsec功能丢弃计数器。

```
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
```

请注意此特定消息是速率限制在Cisco IOS以一个的速率每明显的安全原因的分钟。如果特定的流量的(SRC、DST或者SPI)此消息在日志一次只出现，则它也许只是存在的临时状态，在IPsec重新生

成密钥的同时一对等体也许开始使用新的SA的地方，而对等设备不是相当立即可用的同样SA。因为只是临时的，并且只影响一些数据包，这通常不是问题。然而，有这可以是问题的Bug。

> **提示**：关于示例，请参阅Cisco Bug ID CSCsl68327 (包丢失在期间重新生成密钥)， Cisco Bug ID CSCtr14840 (ASR ：在第2阶段期间的在一定条件下丢包重新生成密钥)，或者Cisco Bug ID CSCty30063 (在QM完成前的ASR用途新建的SPI)。

或者，有一问题，如果超过同一个消息的一个实例被观察报告同一个流的同样SPI，例如这些消息：

```
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
```

这是暗示流量黑洞，并且也许不恢复，直到SAS在发送设备超时或，直到对端死机检测(DPD)激活。

解决方案

此部分提供您能使用为了解决问题在前面部分描述的信息。

无效的SPI恢复

为了解决此问题，思科建议您启用无效的SPI恢复功能。例如，请输入**crypto isakmp无效SPI恢复**命令。这是描述使用此命令的一些重要提示：

- 首先，当SAS是不同步的时，无效的SPI恢复只担当恢复机制。它帮助从此情况恢复，但是不解决造成SAS变得不同步首先的根问题。为了改善请了解根本原因，您必须启用ISAKMP和IPsec调试在两个通道端点。如果问题经常发生，则请得到调试并且尝试寻址根本原因(和不仅屏蔽问题)。

- 有关于**crypto isakmp无效SPI恢复**命令的目的和功能的一种常见的误解。不用此命令， Cisco IOS已经执行无效的SPI恢复功能的类型，当发送删除通知给接收SA的时的发送的对等体，如果已经有与该对等体的一IKE SA。再次，这发生不管**crypto isakmp无效SPI恢复**命令是否被启动。

- **crypto isakmp无效SPI恢复**命令尝试寻址路由器收到与无效的SPI的IPSec数据流的情况，并且没有与该对等体的一IKE SA。在这种情况下，它设法建立有对等体的一个新的IKE会话并且发送在新建立的IKE SA的一个删除通知。然而，此命令不为所有加密配置作用。此命令运作的唯一的配置是对等体明确地定义和静态对等体从例示的加密映射派生的静态加密映射，例如VTI。这是常用的加密配置的摘要，并且无效的SPI恢复是否与该配置一起使用：

加密配置	**无效的SPI恢复？**
静态加密映射	是
动态加密映射	无
与通道保护的P2P GRE	是
使用与静态NHRP映射的mGRE通道保护	是
使用与动态NHRP映射的mGRE通道保护	无

sVTI	是
EzVPN客户端	不适用

排除故障断断续续无效的SPI错误消息

许多时间无效的SPI错误消息间歇地出现。当收集相关调试，变得非常难这使困难排除故障。嵌入式活动管理器(EEM)脚本可以在这种情况下是非常有用的。

> **Note**:欲了解更详细的信息，参考用于的EEM脚本排除故障无效安全参数索引Cisco文档造成的通道飘荡。