了解SD-WAN与传统隧道SPI恢复差异

目录

简介

本文档介绍如何从%RECVD_PKT_INV_SPI错误中恢复SD-WAN和第三方隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Catalyst软件定义的广域网(SD-WAN)
- 互联网协议安全(IPSec)。
- 双向转发检测(BFD)。

使用的组件

本文档中的信息基于：

- Cisco IOS® XE Catalyst SD-WAN边缘。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

安全关联(SA)的概念是IPSec的基础。SA是两个端点之间的关系，描述端点如何使用安全服务进行安全通信。

安全参数索引(SPI)是32位数字，选择它来唯一标识使用IPSec的任何已连接设备的特定SA。

最常见的IPsec问题之一是SA可能由于无效的SPI值而失去同步，这将导致IPSEC隧道关闭状态，因为数据包被对等设备丢弃，且路由器中收到系统日志消息。

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
```

对于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
```

这些日志伴有属于转发处理器(FP)的量子流处理器(QFP)中的丢弃。

```
<#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
```

解决方案

恢复传统IPSec隧道

为了恢复传统IPSec隧道，必须手动强制重新协商当前SA值关系；这可通过使用EXEC模式命令清除IPSec SA来执行：

```
<#root>

Router#

clear crypto sa peer 10.20.20.1
```

SD-WAN隧道的恢复 — 场景1

clear crypto sa peer EXEC命令仅对传统IPSec隧道有效，因为存在互联网密钥交换(IKE), 自动协商关联并生成新的SPI值。但是，无法在SD-WAN隧道上使用该命令。原因是在SD-WAN隧道中没有使用IKE。

因此，使用对应的SD-WAN隧道命令：

```
<#root>

Router#

request platform software sdwan security ipsec-rekey
```

request platform software sdwan security ipsec-rekey命令会立即生成新密钥，然后隧道将启动。相反，如果传统IPSec隧道存在，该命令不会对其产生影响。

注:request platform software sdwan security ipsec-rekey此命令在所有现有SD-WAN隧道中生效，与clear crypto sa peer相反，后者仅在指定的SA中生效。

SD-WAN隧道的恢复 — 场景2

如果错误地使用clear crypto sa peer命令删除了某个SD-WAN隧道SA，则删除操作成功；但是，不会再次生成新的SPI值，因为在SD-WAN隧道中，OMP是触发该操作的非IKE值。一旦处于此状态，即使command request platforms software sdwan security ipsec-rekey是在clear crypto sa peer之后发出的，隧道也不会启动。SA的封装和解封保持为零，因此BFD会话保持关闭状态。

```
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
```

删除SA后，唯一的恢复选项是使用以下三种EXEC命令之一：

<#root>

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

clear sdwan omp all命令用于摆动设备中存在的所有BFD会话。

<#root>

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

clear sdwan control connections命令会使TLOC使用指定本地颜色上的下一个可用端口号，这不仅会导致该颜色的所有BFD会话的抖动，而且还会导致该颜色的控制连接。

<#root>

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

最后一个命令也有助于恢复，但它会对设备中存在的所有控制连接和BFD会话产生影响。

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）。