用于排除由无效安全参数索引引起的隧道抖动故障的EEM脚本

目录

简介
先决条件
要求
使用的组件
规则
问题
解决方案
SNMP配置
最终脚本
EEM脚本日志
确认
相关信息

简介

本文档介绍最常见的IPsec问题之一，即安全关联(SA)可能会在对等设备之间不同步。因此，加密设备将使用对等加密器不知道的SA加密流量。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的此信息基于Cisco IOS® 15.1(4)M4版完成的测试。脚本和配置也应与早期的Cisco IOS软件版本配合使用，因为两个小程序都使用Cisco IOS 12.4(22)T版或更高版本支持的嵌入式事件管理器(EEM)版本3.0。但是，这尚未经过测试。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

问题

数据包在对等体上被丢弃，并且此消息记录到系统日志：

```
*Mar 12 18:22:10.706: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
   has invalid spi for destaddr=213.163.222.7, prot=50, spi=0x68842105(1753489669),
   srcaddr=11.1.1.3, input interface=Ethernet0/0
```

有关无效安全参数索引(SPI)的详细信息，请参阅IPSec %RECVD_PKT_INV_SPI错误和无效SPI恢复。本文档介绍如何对间歇性错误发生的场景进行故障排除，这使收集必要数据进行故障排除变得困难。

此类问题与正常VPN故障排除不同，在正常VPN故障排除中，您可以在问题发生时获得调试。为了排除由无效SPI导致的间歇性隧道抖动故障，您必须首先确定两个头端是如何失步的。由于无法预测下一次停机的发生时间，因此EEM脚本是解决方案。

解决方案

由于了解触发此系统日志消息之前发生的情况非常重要，请继续在路由器上运行条件调试并将其发送到系统日志服务器，以便不影响生产流量。如果在脚本中启用调试，则在触发系统日志消息后生成调试，这可能不有用。以下是您可能希望在此日志的发送方和接收方上运行的调试列表：

```
debug crypto condition peer ipv4 <peer IP address> debug crypto isakmp debug crypto ipsec debug
crypto engine
```

EEM脚本旨在执行两项操作：

1. 在生成第一个系统日志消息后收集18秒后，关闭接收方上的调试。可能需要修改延迟计时器，这取决于生成的调试/日志数量。
2. 同时，它禁用调试，让它向对等设备发送SNMP陷阱，然后禁用对等设备上的调试。

SNMP配置

简单网络管理协议(SNMP)配置如下所示：

```
Receiver:
========

snmp-server enable traps event-manager
snmp-server host 11.1.1.3 public event-manager
snmp-server manager



Sender:
=======

snmp-server enable traps event-manager
snmp-server host 213.163.222.7 public event-manager
snmp-server manager
```

最终脚本

接收方和发送方的脚本如下所示：

```
Receiver:
========
!--- To test if this output gets logged to the file called "hub" sh ip int bri | tee /append
disk0:hub.txt conf t ! event manager applet command_hub event syslog pattern "CRYPTO-4-
RECVD_PKT_INV_SPI.*srcaddr=11.1.1.3" action 1 cli command "enable" action 2 syslog msg
"command_hub is running ..." priority informational action 3 cli command "show crypto sockets |
append disk0:hub.txt" action 4 cli command "show crypto isa sa | append disk0:hub.txt" action 5
cli command "show crypto ipsec sa detail | append disk0:hub.txt" action 6 cli command "show
dmvpn detail | append disk0:hub.txt" action 7 wait 18 action 8 cli command "undebug all" action
8.1 snmp-trap intdata1 2323232 strdata "" action 9 syslog priority informational msg "DONE ON
HUB" ! end

Sender:
=======

conf t
!
event manager applet spoke_app
 event snmp-notification oid 1.3.6.1.4.1.9.10.91.1.2.3.1.9.
    oid-val "2323232" op eq src-ip-address 213.163.222.7 maxrun 35
 action 1.0 syslog msg "Received trap from Hub..."
 action 2.0 cli command "enable"
 action 3.0 cli command "undebug all"
 action 4.0 syslog msg "DONE ON SPOKE"
!
end
```

EEM脚本日志

EEM脚本日志消息列表如下所示：

```
Receiver:
=======

*Mar 12 18:22:10.706: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
    has invalid spi for destaddr=213.163.222.7, prot=50, spi=0x68842105(1753489669),
    srcaddr=11.1.1.3, input interface=Ethernet0/0
*Mar 12 18:22:10.727: %HA_EM-6-LOG: command_hub: command_hub is running ...
hub#
*Mar 12 18:22:30.026: %HA_EM-6-LOG: command_hub: DONE ON HUB



Sender:
=======

spoke#
*Mar 12 18:22:30.542: %HA_EM-6-LOG: spoke_app: Received trap from Hub...
*Mar 12 18:22:30.889: %HA_EM-6-LOG: spoke_app: DONE ON SPOKE
```

确认

要验证问题是否已解决，请输入**show debug**命令。

```
Receiver:
=========
```

```
hub# show debug


Sender:
=======
spoke# show debug
```

相关信息

- 技术支持和文档 - Cisco Systems