用於排除由無效安全引數索引引起的隧道擺動故障的EEM指令碼

目錄

簡介

本文描述最常見的IPsec問題之一，即安全關聯(SA)在對等裝置之間可能變得不同步。因此，加密裝置將加密對等加密器不知道的SA流量。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據使用Cisco IOS®版本15.1(4)M4完成的測試。指令碼和組態也應使用較舊的Cisco IOS軟體版本，因為兩個小程式都使用內嵌式事件管理員(EEM)版本3.0(Cisco IOS版本12.4(22)T或更新版本支援)。但是，這尚未經過測試。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

問題

對等體上的資料包將被丟棄，此消息將記錄到syslog:

```
*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
```

有關無效的安全引數索引(SPI)的詳細資訊，請參閱IPSec %RECVD_PKT_INV_SPI錯誤和無效SPI恢復。本文描述如何對錯誤間歇性發生的場景進行故障排除，這種場景使得收集必要的故障排除資料變得困難。

此類問題不同於正常的VPN故障排除，您可以在出現問題時獲取調試。為了排除由無效SPI引起的間歇性通道翻動的故障，必須首先確定兩個頭端如何不同步。由於無法預測下一次停機何時發生，因此解決方案是EEM指令碼。

解決方案

由於在觸發此syslog消息之前必須瞭解發生的情況，因此請繼續在路由器上運行條件調試，並將它們傳送到syslog伺服器，以便不影響生產流量。如果在指令碼中啟用了調試，則這些調試是在觸發系統日誌消息後生成的，這可能沒有用。以下是您可能希望對此日誌的傳送者和接收者運行的調試清單：

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

EEM指令碼旨在完成兩件事：

1. 在生成第一個syslog消息後18秒內收集接收方上的調試時，關閉它們。可能需要修改延遲計時器，這取決於生成的調試/日誌數量。
2. 在禁用調試的同時，讓其向對等裝置傳送SNMP陷阱，然後對等裝置禁用調試。

SNMP組態

簡單網路管理通訊協定(SNMP)設定如下所示：

```
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
```

最終指令碼

接收者和傳送者的指令碼如下所示：

```
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指令碼日誌

EEM指令碼日誌消息的清單如下所示：

```
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
```

驗證

若要確認問題是否已解決，請輸入**show debug**指令。

```
Receiver:
=========
hub# show debug


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

相關資訊

- 技術支援與文件 - Cisco Systems