유효하지 않은 보안 매개변수 인덱스로 인한 터널 플랩 트러블슈팅에 사용되는 EEM 스크립트

목차

소개

이 문서에서는 피어 디바이스 간에 SA(Security Associations)가 동기화되지 않을 수 있다는 가장 일반적인 IPsec 문제 중 하나에 대해 설명합니다.따라서 암호화 디바이스는 피어 암호기가 모르는 SA로 트래픽을 암호화합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS® Release 15.1(4)M4에서 완료된 테스트를 기반으로 합니다. 스크립트 및 구성은 이전 Cisco IOS 소프트웨어 버전에서도 작동해야 합니다. 두 애플릿은 모두 Cisco IOS Release 12.4(22)T 이상에서 지원되는 EEM(Embedded Event Manager) 버전 3.0을 사용하기 때문입니다.그러나 이는 테스트되지 않았습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

문제

패킷은 다음 메시지가 syslog에 로깅되어 피어에서 삭제됩니다.

```
*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
```

잘못된 SPI(보안 매개 변수 인덱스)에 대한 자세한 내용은 IPSec %RECVD_PKT_INV_SPI 오류 및 잘못된 SPI 복구를 참조하십시오.이 문서에서는 간헐적으로 오류가 발생하는 시나리오를 트러블슈팅하는 방법에 대해 설명하며, 이는 트러블슈팅에 필요한 데이터를 수집하기 어렵게 합니다.

이 유형의 문제는 정상적인 VPN 문제 해결과 같지 않습니다. 문제 발생 시 디버그를 가져올 수 있습니다.잘못된 SPI로 인한 간헐적인 터널 플랩의 문제를 해결하려면 먼저 두 헤드엔드가 동기화되지 않은 방법을 확인해야 합니다.다음 정전 발생 시기를 예측하는 것은 불가능하므로 EEM 스크립트가 해결책입니다.

솔루션

이 syslog 메시지가 트리거되기 전에 어떤 일이 발생하는지 아는 것이 중요하므로 라우터에서 조건부 디버그를 계속 실행하고 프로덕션 트래픽에 영향을 주지 않도록 syslog 서버로 전송합니다.대신 스크립트에서 디버그가 활성화되면 syslog 메시지가 트리거된 후 생성되며 유용하지 않을 수 있습니다.이 로그의 발신자와 수신자에서 실행할 수 있는 디버깅 목록은 다음과 같습니다.

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

EEM 스크립트는 다음 두 가지 작업을 수행하도록 설계되었습니다.

1. 첫 번째 syslog 메시지가 생성된 후 18초 동안 수집되면 수신기의 디버그를 끕니다.생성된 디버그/로그의 양에 따라 지연 타이머를 수정해야 할 수 있습니다.
2. 동시에 디버그를 비활성화하고 SNMP 트랩을 피어로 전송하도록 하여 피어 디바이스에서 디버그를 비활성화합니다.

SNMP 컨피그레이션

SNMP(Simple Network Management Protocol) 구성은 다음과 같습니다.

```
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
```

최종 스크립트

수신자 및 발신자에 대한 스크립트는 다음과 같습니다.

```
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 스크립트 로그

EEM 스크립트 로그 메시지 목록은 다음과 같습니다.

```
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
```

확인

문제가 해결되었는지 확인하려면 **show debug** 명령을 입력합니다.

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


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

관련 정보

- 기술 지원 및 문서 – Cisco Systems