Secuencias de comandos de EEM utilizadas para solucionar problemas de inestabilidad de túnel causados por índices de parámetros de seguridad no válidos

Contenido

Introducción

Este documento describe uno de los problemas más comunes de IPSec, que es que las asociaciones de seguridad (SA) pueden quedar fuera de sincronización entre los dispositivos de peer. Como resultado, un dispositivo de cifrado cifrará el tráfico con las SA que el cifrado de par no conoce.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Esta información en este documento se basa en las pruebas completadas con Cisco IOS® Release 15.1(4)M4. Los scripts y la configuración también deben funcionar con las versiones anteriores del software Cisco IOS, ya que ambos applets utilizan Embedded Event Manager (EEM) versión 3.0, que es compatible con Cisco IOS versión 12.4(22)T o posterior. Sin embargo, esto no se ha probado.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Problema

Los paquetes se descartan en el par con este mensaje registrado en el 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
```

Para obtener información detallada sobre los índices de parámetros de seguridad (SPI) no válidos, consulte Errores IPSec %RECVD_PKT_INV_SPI y Recuperación SPI Inválida. Este documento describe cómo resolver problemas en situaciones en las que el error ocurre de manera intermitente, lo que dificulta la recolección de los datos necesarios para resolver problemas.

Este tipo de problema no es como la resolución de problemas de VPN normal, donde puede obtener las depuraciones cuando ocurre el problema. Para resolver problemas de inestabilidad de túnel intermitente causada por SPI inválidos, primero debe determinar cómo los dos encabezados se salieron de sincronización. Puesto que es imposible predecir cuándo ocurrirá la siguiente interrupción, los scripts EEM son la solución.

Solución

Dado que es importante saber qué sucede antes de que se active este mensaje de syslog, continúe ejecutando las depuraciones condicionales en los routers y envíelas a un servidor syslog para que no afecte el tráfico de producción. Si se habilitan las depuraciones en el script en su lugar, se generan después de que se activa el mensaje syslog, lo que puede no ser útil. Esta es una lista de depuraciones que puede querer ejecutar en el remitente de este registro y en el receptor:

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

La secuencia de comandos EEM está diseñada para hacer dos cosas:

1. Desactive las depuraciones en el receptor cuando se recopilan durante 18 segundos después de que se genere el primer mensaje de syslog. Es posible que sea necesario modificar el temporizador de retraso, que depende de la cantidad de depuraciones/registros generados.
2. Al mismo tiempo inhabilita los debugs, haga que envíe una trampa SNMP al peer, que luego inhabilita los debugs en el dispositivo peer.

Configuración SNMP

Aquí se muestran las configuraciones del protocolo simple de administración de red (SNMP):

```
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
```

Guión final

Las secuencias de comandos para el receptor y el remitente se muestran aquí:

```
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
```

Registros de secuencia de comandos de EEM

Aquí se muestra una lista de mensajes de registro de secuencias de comandos de EEM:

```
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
```

Verificación

Para verificar que el problema se ha resuelto, ingrese el comando **show debug**.

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


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

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems