

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Problema](#)

[Solución](#)

[Configuración SNMP](#)

[Script final](#)

[Registros de secuencia de comandos EEM](#)

[Verificación](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe uno de la mayoría de los problemas del IPSec comunes, que es que las asociaciones de seguridad (SA) pueden convertirse fuera de sincronizan entre los dispositivos de peer. Como consecuencia, un dispositivo que cifra cifrará el tráfico con los SA que el encryptor del par no conoce alrededor.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

Esta información en este documento se basa en las pruebas completadas con la versión 15.1(4)M4 de Cisco IOS®. Los scripts y la configuración deben trabajar con versiones del Cisco IOS Software anteriores también, puesto que el uso de ambos applet integró la versión 3.0 del administrador del evento (EEM) que se soporta en el Cisco IOS Release 12.4(22)T o Posterior. Sin embargo, esto no se ha probado.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

Problema

Los paquetes se caen en el par con este mensaje registrado al Syslog:

Para información detallada sobre los índices inválidos del parámetro de seguridad (SPI), refiera a los [errores del IPSec %RECVD_PKT_INV_SPI](#) y a [la recuperación del SPID inválido](#). Este documento describe cómo resolver problemas los escenarios en los cuales el error ocurre intermitentemente, que hace duro recoger los datos necesarios para resolver problemas.

Este tipo de problema no es como el troubleshooting normal VPN, donde usted puede obtener los debugs cuando ocurre el problema. Para resolver problemas las aletas intermitentes del túnel causadas por los SPID inválidos, usted debe primero determinar de cómo los dos headends salieron sincronizan. Puesto que es imposible predecir cuando ocurrirá la caída del sistema próxima, los scripts EEM son la solución.

Solución

Puesto que es importante conocer qué sucede antes de que se accione este mensaje de Syslog, continúe ejecutando los debugs condicionales en los routers y enviándolos a un servidor de Syslog de modo que no afecte al tráfico de producción. Si los debugs se habilitan en el script en lugar de otro, se generan después de que se accione el mensaje de Syslog que puede no ser útil. Aquí está una lista de debugs que usted puede ser que quiera para ejecutarse en el remitente de este registro y el receptor:

El script EEM se diseña para hacer dos cosas:

1. Apague los debugs en el receptor cuando se recogen para 18 segundos después de que el primer mensaje de Syslog se genera. El temporizador del retraso pudo necesitar ser modificado, que es dependiente sobre la cantidad de debugs/de registros generados.
2. Al mismo tiempo inhabilita los debugs, hace que envíe un SNMP trap al par, que entonces inhabilita los debugs en el dispositivo de peer.

Configuración SNMP

Las configuraciones del Simple Network Management Protocol (SNMP) se muestran aquí:

Script final

Los scripts para el receptor y el remitente se muestran aquí:

Registros de secuencia de comandos EEM

Una lista de mensajes de registro de secuencia de comandos EEM se muestra aquí:

Verificación

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

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

Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)