

El tráfico XPN de MACSec falla entre Catalyst 9500 y Nexus 9000 y aumenta los paquetes no válidos y los errores FCS

Contenido

Problema

Cuando MACSec XPN se habilita entre un Catalyst 9500-28C8D y un Nexus N9K-C93180YC-FX, la sesión MKA se establece con éxito pero ningún tráfico de datos pasa a través del link. El Catalyst 9500 informa que aumenta el número de "paquetes no válidos" bajo las estadísticas SA y los errores de entrada FCS en la interfaz física. Específicamente, se observaron estos síntomas:

- No hay conectividad después de habilitar MACSec
- La sesión de MKA se muestra tal como se estableció, pero el lado de Catalyst 9500 muestra las estadísticas de SA con "Pkts 118 no válidos" en aumento y "Pkts válidos: 0"
- Incremento de errores de entrada FCS en la interfaz física Catalyst 9500
- La eliminación de la configuración de MACSec restaura inmediatamente la conectividad y detiene los errores de FCS

Las sesiones MKA se establecieron en ambos dispositivos y negociaron con éxito el cifrado GCM-AES-XPN-256. El lado de Nexus mostró el cifrado como activo, pero Catalyst 9500 recibió paquetes cifrados y los rechazó debido a una discordancia de validación, lo que resultó en la aceptación de paquetes válidos cero.

Entorno

- Catalyst 9500-28C8D con Cisco IOS®
- Nexus N9K-C93180YC-FX
- Configuración de MACSec XPN mediante la suite de cifrado GCM-AES-XPN-256

- Interfaz de 400 Gigabit Ethernet (400 GigE1/0/15 en Catalyst, Ethernet1/52 en Nexus)
- Catalyst 9500 configurado como prioridad de servidor de claves 1, Nexus configurado como prioridad de servidor de claves 100
- Algoritmo criptográfico AES-256-CMAC para claves previamente compartidas

Resolución

El problema se resolvió implementando una solución alternativa que cambia la asignación de funciones de servidor de claves entre los dispositivos. La resolución recomendada implica los siguientes pasos:

Paso 1: Identificar el problema de configuración del servidor de claves

Verifique la configuración actual de prioridad del servidor de claves en ambos dispositivos. La configuración problemática mostró:

Configuración de Catalyst 9500:

```
mka policy MEHEALTH-ORG-XPN
  key-server priority 1
  macsec-cipher-suite gcm-aes-xpn-256
```

Configuración de Nexus:

```
macsec policy MEHEALTH-ORG-XPN
  key-server-priority 100
```

Paso 2: Implementar la solución alternativa de rol de servidor clave

Configure el dispositivo Nexus como el servidor de claves MACSec en lugar de Catalyst 9500.

Esto implica ajustar los valores de prioridad del servidor de claves para que Nexus asuma la función de servidor de claves.

Modifique la configuración de Nexus para que tenga un valor de prioridad de servidor de claves inferior (los valores inferiores tienen mayor prioridad):

```
macsec policy MEHEALTH-ORG-XPB
  key-server-priority 1
```

Modifique la configuración de Catalyst 9500 para que tenga un valor de prioridad de servidor de claves más alto:

```
mka policy MEHEALTH-ORG-XPB
  key-server priority 100
  macsec-cipher-suite gcm-aes-xpn-256
```

Paso 3: Verificar el funcionamiento de MACSec

Después de implementar el cambio de función del servidor de claves, compruebe que:

- Sesiones MKA establecidas correctamente en ambos dispositivos
- El tráfico de datos pasa a través del enlace habilitado para MACSec
- No hay "paquetes no válidos" incrementando en las estadísticas de Catalyst 9500 SA
- No se producen errores de entrada FCS en la interfaz física

Esta solución alternativa permite que la configuración de MACSec XPN funcione correctamente hasta que se pueda completar la investigación de la plataforma y la planificación de la actualización del software.

Causa

La causa raíz de este problema está relacionada con el ID de bug de Cisco CSCvs00410, que

describe un escenario donde las sesiones MKA se establecen con éxito pero los datos no pueden pasar a través del link cuando se utiliza AES-256-XPB con un Catalyst 9500 en el rol de servidor de claves bajo ciertas condiciones de interoperabilidad con los dispositivos Nexus. El comportamiento se manifiesta como una discordancia de validación donde el Catalyst 9500 rechaza los paquetes cifrados del Nexus, lo que resulta en un aumento de los recuentos de paquetes no válidos y errores FCS. Se observó una discrepancia en cuanto a que Cisco IOS se listó como corregido para este defecto, lo que requiere una investigación adicional por parte del equipo de la plataforma Catalyst.

Contenido relacionado

- Cisco Bug ID CSCvs00410 - Sesión MKA activa pero no puede pasar datos a través del enlace cuando se utiliza AES-256-XPB con el rol de servidor de claves Catalyst 9500

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).