

El examen del link agregó el tráfico de Sourcefire FirePOWER y dispositivos virtuales

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Soporte de la agregación del link](#)

[Puntos a considerar](#)

[Problema conocido](#)

[Documento relacionado](#)

Introducción

La agregación del link ha sido estandarizada por IEEE en 802.3ad a 802.3ax. Las implementaciones frecuentes de la agregación del link son EtherChannel, el protocolo link aggregation control (LACP), Port Aggregation Protocol (PAgP), etc. Este artículo describe cómo el link de la manija de los dispositivos de Sourcefire agregó el tráfico.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento en los modelos del dispositivo de Sourcefire FirePOWER, dispositivo virtual modela, el protocolo link aggregation control (LACP), EtherChannel, y Port Aggregation Protocol (PAgP).

Soporte de la agregación del link

Un dispositivo de Sourcefire puede trabajar con cualquier implementación estándar de la agregación del link, porque un protocolo de la agregación del link no agrega ningunos datos adicionales al paquete sí mismo. No hay problemas conocidos entre la implementación de los dispositivos de Sourcefire y ninguno conecta los protocolos de la agregación.

Puntos a considerar

Las puntas siguientes necesitan ser consideradas cuando usted despliega un dispositivo de

Sourcefire en el despliegue agregado link:

1. Si un dispositivo de Sourcefire está en el modo pasivo y todos los links del EtherChannel están siendo monitoreados por el mismo motor de la detección, después la configuración de la agregación del link no importa.
2. Si un solo motor de la detección monitorea solamente algunos de los links o el dispositivo se está desplegando como dispositivo en línea, después se recomienda que la agregación del link está configurada para utilizar ambos MAC Address de origen y destino. Esto evitará los problemas de rendimiento relacionados con la encaminamiento asíncrona.
3. El Snort es capaz de procesar el tráfico agregado link sin el problema. Sin embargo, el Snort no podrá decodificar los paquetes de control de la agregación del link enviados entre el Switches.
4. Los métodos del Equilibrio de carga en el EtherChannel se basan en cada flujo de tráfico y no en cada trama o paquete, así que los flujos son que consigue la carga equilibrada. La configuración del "IP de la fuente y del IP de destino" en el EtherChannel puede afectar al Equilibrio de carga a través de los casos del snort de Sourcefire. Éste es solamente si desmenuza los resultados realizados en un más conjunto limitado de IP para elegir de. El uso del "MAC de origen y del MAC de destino" puede ayudar con la distribución de carga.

Problema conocido

El problema conocido siguiente en el LACP está señalado sobre todas las versiones antes de e incluir 5.3.1.1:

En algunos casos, la aplicación cambia a su directiva del control de acceso, a la directiva de la intrusión, a la directiva de la detección de red, o a la configuración del dispositivo, o instalar una actualización de la regla de la intrusión o la actualización de la base de datos de la vulnerabilidad (VDB) hace el sistema experimentar una interrupción en el tráfico que utiliza el protocolo link aggregation control (LACP) en el modo rápido. Como solución alternativa, la configuración LACP conecta en el modo lento. (112070)

Documento relacionado

- [Release Note de 5.3.1.1 de la versión del sistema de FireSIGHT](#)