Contenido

Introducción

Un sistema de FireSIGHT genera los eventos cuando detecta un nuevo host en su segmento de red monitoreado. Puede detectar un sistema operativo o un servicio incorrectamente, o con menos confianza. Si un evento se marca como *desconocido*, significa que el tráfico está analizado, pero los sistemas operativos no hacen juego las huellas dactilares sabidas unas de los. Este documento proporciona una lista de verificación y las recomendaciones de minimizar los *eventos desconocidos*.

Prerrequisitos

La información que contiene este documento se basa en estas versiones de software y hardware.

- Sistema de FireSIGHT, dispositivos de la potencia de fuego, y dispositivos virtuales NGIPS
- Versión de software 5.2 o más adelante

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.

Listas de Verificación de Resolución de Problemas

Si su sistema de FireSIGHT está generando los eventos que están en el estado pendiente o en desconocido, usted puede seguir los pasos abajo para comenzar a resolver problemas este problema:

> Nota: Los host *no identificados* no son lo mismo que los *host desconocidos*. Los host *no identificados* son los host sobre quienes un sistema todavía no ha recopilado bastante información para identificar sus sistemas operativos.

Lista de verificación del Troubleshooting	Recomendaciones
1. ¿Qué versión VDB está instalada en el centro de administración de FireSIGHT?	La última versión VDB tiene más información de la huella dactilar. Se recomienda siempre para tener la última versión instalada en el centro administración de FireSIGHT.
2. ¿Cuál es el límite del host de su licencia de FireSIGHT? ¿Cuántos host han sido detectados por FireSIGHT?	Si el límite del host se excede, un sistema de FireSIGHT poda los más viejos datos mientras que vienen los nuevos datos adentro. Usted pue configurar la política del sistema para caer los nuevos host cuando el del host alcanzó.
3. ¿Cuántos saltos lejos los host están situados del dispositivo administrado de FireSIGHT?	Cuanto más alto es el conteo saltos entre los host y un dispositivo administrado, más lejos el host es del dispositivo, y la probabilidad as creciente el tráfico se ha modificado y no permitirá la identificación exa
4. ¿Hay dispositivos en línea entre los host y el dispositivo administrado?	La presencia de cualquier dispositivo en línea; por ejemplo el Firewall dispositivo NAT, el balanceador de la carga y el servidor proxy pueden modificar la información original TCP o de encabezado IP que puede también ser las causas de la recopilación de información mala o no identificada de los host.
5. ¿Los dispositivos administrados están monitoreando el tráfico en red asíncrona de la encaminamiento?	Si un tráfico asíncrono de la encaminamiento de los monitores de sist de FireSIGHT, él puede no poder considerar la sesión completa.
6. ¿Hay puertos no estándar usados para servicios? ¿Hay decodificadores de encargo configurados para dirigir los puertos no estándar?	Un decodificador de encargo incorrectamente configurado puede esta conflicto con los decodificadores predeterminados.

Datos adicionales

Si se siguen todas las recomendaciones antedichas, pero hay desconocido, pendiente o los host no identificados encontrados, después nosotros necesitaremos analizar el data&colon siguiente;

1. Tráfico de sesión completo

Tráfico de sesión completo de los host que se identifican incorrectamente, o se marcan como desconocido o pendiente.

2. Resolver problemas los archivos

El resolver problemas clasifía del centro de administración y del dispositivo administrado de FireSIGHT. La correlación de la red o la topología que muestra la ubicación del dispositivo

administrado sería útil.

3. Captura de paquetes (PCAP)

Los paquetes recibidos por el dispositivo administrado pueden ser diferentes que los paquetes originados en los host. Sucede si cualquier encabezado que modifica el dispositivo en línea existe entre los host y el dispositivo administrado. Por lo tanto, es mejor capturar PCAP de los ambos extremos - los host y los dispositivos administrados, que permite comparar las encabezados de los dos PCAPs. Cualquier discordancía entre los paquetes puede causar la identificación errónea de los servicios o de los host.