Sesión grande de la sola secuencia de proceso (flujo del elefante) por los servicios de FirePOWER

Contenido

Introducción

Este documento describe porqué un flujo único no puede consumir el caudal nominal entero de un dispositivo de Cisco FirePOWER.

Antecedentes

El resultado de ningún sitio web de la prueba de la velocidad del ancho de banda, o la salida de ninguna herramienta de la medida del ancho de banda (por ejemplo, iperf) no pudo exhibir el grado de divulgación de la producción de los dispositivos de Cisco FirePOWER. Semejantemente, la transferencia de un archivo muy grande sobre ningún Transport Protocol no demuestra el grado de divulgación de la producción de un dispositivo de FirePOWER. Ocurre porque el servicio de FirePOWER no utiliza un flujo de red única para determinar su rendimiento máximo.

Tráfico de proceso por el Snort

La tecnología subyacente de la detección del servicio de FirePOWER es Snort. La implementación del Snort en el dispositivo de Cisco FirePOWER es un solo proceso del hilo para procesar el tráfico. Un dispositivo es clasificado para un grado específico basado en el caudal útil total de todos los flujos que pasa a través del dispositivo. Se espera que los dispositivos estén desplegados en una red corporativa, generalmente cerca del borde y de los trabajos de la frontera con los millares de conexiones.

Equilibrio de carga del uso de los servicios de FirePOWER del tráfico a vario diverso proceso del

Snort con un Snort de proceso que se ejecuta en cada CPU en el dispositivo. Idealmente, la carga del sistema equilibra el tráfico uniformemente a través de todos los procesos del Snort. El Snort necesita poder proporcionar el análisis del contexto apropiado para el Firewall de la última generación (NGFW), el Sistema de prevención de intrusiones (IPS) y el examen avanzado de la protección de Malware (AMP). Para asegurar el Snort es el más eficaz, todo el tráfico de un flujo único es carga equilibrada a un caso del snort. Si todo el tráfico de un flujo único no fuera equilibrado a un solo caso del snort, el sistema podría ser evadido y el tráfico derramado de una manera tal que una regla del Snort pudiera ser menos probable hacer juego o los pedazos de un archivo no sean contiguos para el examen AMP. Por lo tanto, el algoritmo del Equilibrio de carga se basa en la información de conexión que puede identificar únicamente una conexión dada.

algoritmo 2-Tuple en el ASA con los servicios de FirePOWER y NGIPS virtual

En el dispositivo de seguridad adaptante (ASA) con la Plataforma de servicio y el sistema de prevención de intrusiones de la última generación (NGIPS) de FirePOWER virtuales, el tráfico es carga equilibrada para resoplar con el uso de un algoritmo 2-tuple. Los datapoints para este algoritmo son:

- IP de la fuente
- IP de destino

el algoritmo 3-Tuple en la versión de software 5.3 o baja en FirePOWER y los dispositivos FTD

En todas las versiones anteriores (5.3 o bajan), el tráfico es la carga equilibrada para resoplar que utiliza un algoritmo 3-tuple. Los datapoints para este algoritmo son:

- IP de la fuente
- IP de destino
- Protocolo IP

Cualquier tráfico con la misma fuente, destino, y protocolo IP es carga equilibrada a la misma instancia del Snort.

algoritmo 5-Tuple en la versión de software 5.4, 6.0, y mayor en FirePOWER y los dispositivos FTD

En la versión 5.4, 6.0 o mayor, el tráfico es carga balaned para resoplar con un algoritmo 5-tuple. Los datapoints se tienen en cuenta que son:

- IP de la fuente
- Puerto de Origen
- IP de destino
- Puerto de Destino
- Protocolo IP

El propósito de agregar los puertos al algoritmo es equilibrar el tráfico más uniformemente cuando hay los pares específicos de la fuente y del destino que explican las porciones grandes del tráfico. Por la adición de los puertos, los puertos de origen efímeros de categoría alta deben ser diferentes por el flujo, y deben agregar la entropía adicional más uniformemente que equilibra el tráfico a diversos casos del snort.

Caudal útil total

El caudal útil total de un dispositivo se mide basó en el rendimiento total de todos los casos del snort que trabaja a su capacidad más máxima. El estándar de la industria practica para medir la producción está para las conexiones HTTP múltiples con los diversos tamaños de objeto. Por ejemplo, la metodología de prueba NS NGFW mide el caudal útil total del dispositivo con los objetos 44k, 21k, 10k, 4.4k, y 1.7k. Éstos traducen a un radio de acción de tamaños promedios de los paquetes alrededor de 1k y bytes a los bytes 128 debido a los otros paquetes implicados en la conexión HTTP.

Usted puede estimar el grado de funcionamiento de un caso individual del Snort. Tome el caudal nominal del dispositivo y divida eso por el número de casos del Snort que se ejecuten. Por ejemplo, si un dispositivo es clasificado en 10Gbps para el IPS con un tamaño promedio de los paquetes de los bytes 1k, y ese dispositivo tiene 20 casos del Snort, el rendimiento máximo aproximado para una instancia única sería 500 Mbps por el Snort. Diversos tipos de tráfico, los Network Protocol, los tamaños de los paquetes junto con las diferencias en la directiva de seguridad general pueden todo el impacto la producción observada del dispositivo.

Resultado de la prueba de la herramienta del otro vendedor

Cuando usted prueba con cualquier sitio web de la prueba de velocidad, o cualquier herramienta de la medida del ancho de banda, por ejemplo, iperf, un solo flujo grande de la secuencia TCP se genera. Llaman este tipo de flujo grande TCP un flujo del elefante. Un flujo del elefante es una sola sesión, la conexión de red relativamente duradera que consume una cantidad grande o desproporcionada de ancho de banda. Asignan este tipo de flujo a un caso del Snort, por lo tanto el resultado de la prueba visualiza la producción del solo caso del snort, no el grado del rendimiento total del dispositivo.

Correcciones

Puente inteligente de la aplicación (IAB)

La versión de software 6.0 introduce una nueva función llamada IAB. Cuando un dispositivo de FirePOWER alcanza un umbral de rendimiento predefinido, la característica IAB busca los flujos que cumplen los criterios específicos para desviar inteligente que palía la presión sobre los motores de la detección.

> **Tip**: Más información sobre la configuración del IAB se puede encontrar aquí.

Identifique y confíe en los flujos grandes

Los flujos grandes se relacionan a menudo con el tráfico bajo del valor del examen del alto uso por ejemplo, los respaldos, la réplica de base de datos, el etc. Muchas de estas aplicaciones no se pueden beneficiar del examen. Para evitar los problemas con los flujos grandes, usted puede identificar los flujos grandes y crear las reglas de la confianza del control de acceso para ellas. Estas reglas pueden identificar únicamente los flujos grandes, permiten que esos flujos pasen sin inspeccionar, y no sean limitados por el solo comportamiento del caso del snort.

Note: Para identificar los flujos grandes para las reglas de la confianza, entre en contacto Cisco FirePOWER TAC.

Información Relacionada

- Control de acceso usando puente inteligente de la aplicación
- **Soporte Técnico y Documentación - Cisco Systems**