Proceso de la sesión grande de la sola secuencia (flujo del elefante) por los servicios de la potencia de fuego

Contenido

Introducción

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*) puede no exhibir el grado de divulgación de la producción de los dispositivos de la potencia de fuego de Cisco. 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 la potencia de fuego. Ocurre porque el servicio de la potencia de fuego no utiliza un flujo de red única para determinar su rendimiento máximo. Este documento describe porqué un flujo único no puede consumir el caudal nominal entero de un dispositivo de la potencia de fuego de Cisco.

Contribuido por Nazmul Rajib, y Lipkey adoptivo, ingenieros de Cisco TAC.

Proceso del tráfico por el Snort

La tecnología subyacente de la detección del servicio de la potencia de fuego es Snort. La implementación del Snort en el dispositivo de la potencia de fuego de Cisco es un solo proceso del hilo para el procesamiento del tráfico. Un dispositivo es clasificado para un grado específico basado en el caudal útil total de todos los flujos que pasan 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.

La potencia de fuego mantiene el Equilibrio de carga de las aplicaciones del tráfico a vario diverso proceso del Snort con un funcionamiento de proceso del Snort 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 examen NGFW, IPS, y amperio. 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 fue equilibrado a un solo caso del snort, el sistema podría ser evadido partiendo el tráfico de una manera tal que una regla del Snort pueda ser menos probable hacer juego o los pedazos de un archivo no sean contiguos para el examen amperio. 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 la potencia de fuego y NGIPS virtual

En el ASA con la Plataforma de servicio de la potencia de fuego y NGIPS virtual, el tráfico es carga balaned para resoplar usando 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 la potencia de fuego y los dispositivos FTD

En todas las versiones anteriores (5.3 o bajan), el tráfico es carga balaned para resoplar usando 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 la potencia de fuego y los dispositivos FTD

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

- 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. Agregando los puertos, los puertos de origen efímeros de categoría alta deben ser diferentes por el flujo, y deben agregar la entropía adicional que equilibra más uniformemente 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 trabajan a su capacidad más máxima. Las prácticas del estándar de la industria para la producción de medición están para las conexiones HTTP múltiples usando los diversos tamaños de objeto. Por ejemplo, la metodología de prueba NS NGFW mide el caudal útil total del dispositivo usando los objetos 44k, 21k, 10k, 4.4k, y 1.7k. Éstos traducen a un rango de los tamaños promedios de los paquetes alrededor de los bytes 1k 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 tomando el caudal nominal del dispositivo y dividiendo eso por el número de casos del Snort que se estén ejecutando. 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 una 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 **puente Intelligent Application** (IAB). Cuando un dispositivo de la potencia de fuego 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.

> Consejo: Más información sobre configurar el 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.

> Nota: Para identificar los flujos grandes para las reglas de la confianza, entre en contacto

por favor la potencia de fuego TAC de Cisco.

Documentos Relacionados

- Control de acceso usando puente inteligente de la aplicación