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 el FTP o el protocolo HTTP 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 consume 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 la medida el rendimiento máximo de un dispositivo por el tráfico del Equilibrio de carga a varios diversos procesos en ejecución para el snort - un proceso del snort para cada CPU en el dispositivo. Sin embargo, el tráfico de la balanza de la carga de servicios de la potencia de fuego uniformemente en a por la base al paquete a través de todos los casos del Snort. El Snort necesita poder volver a montar las conexiones. Si el doesnot del Snort vuelve a montar estas sesiones, un sistema de la prevención de intrusiones podría ser evadido haciendo fragmentos de los paquetes de una manera tal que una regla del Snort pueda ser menos probable hacer juego. Para que cada caso individual del Snort pueda volver a montar el tráfico, el servicio de la potencia de fuego debe enviar todo el tráfico de cualquier conexión al mismo caso del Snort. Por lo tanto, el algoritmo del Equilibrio de carga se basa en la información de conexión que puede identificar únicamente una conexión dada.

el algoritmo 3-Tuple en la versión de software 5.3 o baja

En todas las versiones anteriores (5.3 o bajan), el Snort 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 la versión 5.4, 6.0 o mayor, la potencia de fuego mantiene las aplicaciones 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 basa en la capacidad combinada de todos los casos del snort que trabajan a su capacidad más máxima. Usted puede estimar el grado de funcionamiento de un caso individual del Snort tomando el grado del dispositivo y dividiendo eso por el número de casos del Snort que se estén ejecutando.

Por ejemplo, un dispositivo 8250 es clasificado en el 10 Gbps para el IPS y tiene 22 casos del funcionamiento del Snort. Por lo tanto, el solo umbral de rendimiento del Snort sería caso 10,000 Mbps/22 = 454 Mbps por el caso del Snort. Ahora algunos de los dispositivos pueden subestimado levemente, por lo tanto un solo caso del Snort puede procesar levemente más que este algoritmo le daría. El dispositivo 8250 es uno de ellos, él enarbola generalmente en el 500 Mbps por el caso del Snort.

Otro ejemplo sería un ASA 5516 con los servicios de la potencia de fuego. El ASA 5516 es clasificado en un rendimiento máximo del 450 Mbps con 1500 paquetes de bytes para la visibilidad de la aplicación y el control (AVC) e IPS. El ASA 5516 tiene 3 casos del funcionamiento del snort. El máximo por la producción del caso sería aproximadamente 150 Mbps.

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 generalmente con las transferencias de archivos grandes, por ejemplo, los respaldos, la réplica de base de datos, el etc. Muchas de estas transferencias de archivos no se pueden beneficiar del examen. Para evitar los problemas con las transferencias de archivos 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 el Snort pase esos flujos sin inspeccionar, y que no sea limitado 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