Detecta el flujo de elefantes en dispositivos Firepower

Contenido

Introducción

Este documento describe cómo realizar Elephant Flow Detection en un entorno Cisco Firepower Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que conozca estos productos:

- Centro de administración Firepower (FMC)
- Firepower Threat Defense (FTD)
- Netflow

Componentes Utilizados

La información de este documento se basa en un FMC que ejecuta la versión de software 7.1 o posterior. 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 iniciaron con una configuración sin definir (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La detección de elefantes en Cisco Firepower es crucial para identificar y gestionar flujos de gran

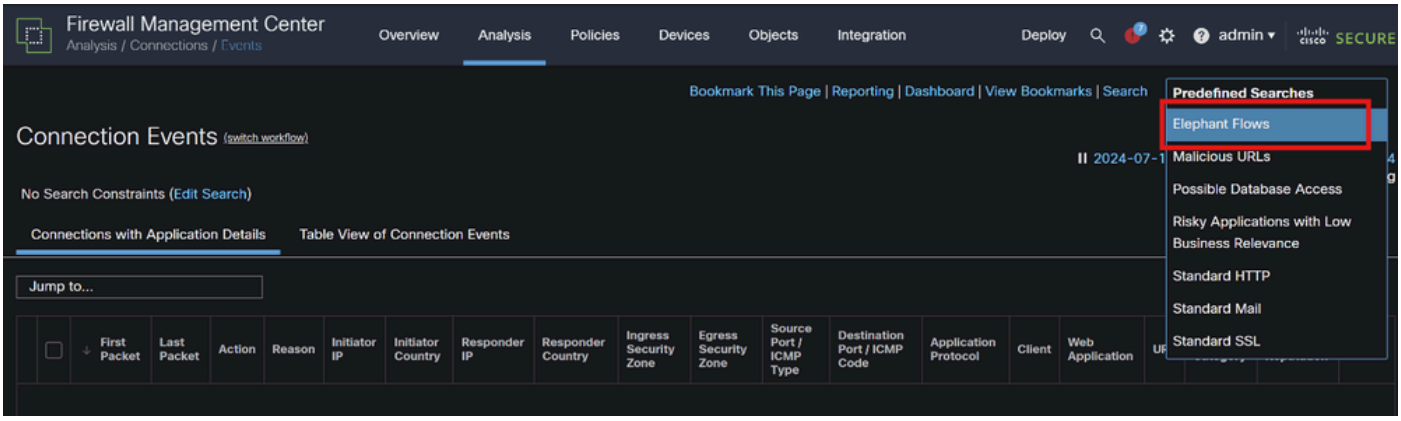
tamaño y de larga duración que pueden consumir recursos de red significativos y afectar al rendimiento. Los flujos elefantes pueden producirse en aplicaciones que generan grandes volúmenes de datos, como la transmisión de vídeo, las transferencias de archivos de gran tamaño y la replicación de bases de datos. Esto se puede identificar mediante los siguientes métodos:

Métodos

1. Utilización de CSP

La detección de flujo de elefante se introdujo en la versión 7.1. La versión 7.2 permite una personalización más sencilla y la opción de omitir o incluso regular los flujos de elefante. El Intelligent Application Bypass (IAB) ha quedado obsoleto a partir de la versión 7.2.0 para los dispositivos Snort 3.

La detección del flujo de elefante se puede realizar en Análisis > Conexiones > Eventos > Búsquedas predefinidas > Flujos de elefante.



Eventos de conexión

Este documento proporciona el proceso paso a paso para configurar Elephant Flow en la política de control de acceso

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/elephant-flow.html#task_sxp_h2d_jsb

2. Uso de CLI

a. El pico de CPU de la instancia de Snort también puede indicar que la red está tratando con el flujo de Elephant que se puede identificar usando el siguiente comando:

show asp inspect-dp snort

Este es un ejemplo del resultado del comando.

> show asp inspect-dp snort

Pid De Información de Estado de Instancia de Inspección de SNORT

Cpu-Usage Conns Segs/Pkts Status tot (usr | sys)

— ----- ---------- ---------- ---------- ----------

0 16450 8% (7%| 0%) 2,2 K 0 PREPARADO

1 16453 9% (8%| 0%) 2,2 K 0 PREPARADO

2 16451 6% (5%| 1%) 2,3 K 0 PREPARADO

3 16454 5% (%)| 0%) 2,2 K 1 PREPARADO

4 16456 6% (%)| 0%) 2,3 K 0 PREPARADO

5 16457 6% (%)| 0%) 2,3 K 0 PREPARADO

6 16458 6% (%)| 0%) 2,2 K 1 PREPARADO

7 16459 4% (4%| 0%) 2,3 K 0 PREPARADO

8 16452 9% (8%| 1%) 2,2 K 0 PREPARADO

9 16455 100% (100%| 0%) 2.2 K 5 READY <<<< Alta utilización de la CPU 10 16460 7% (6%| 0%) 2,2 K 0 PREPARADO

— ----- ---------- ---------- ---------- ----------

Resumen 15% (14%| 0%) 24,6 K 7

b. Además, la salida del comando "top" del modo root también puede ayudar a verificar cualquier instancia de Snort que se eleve.

c. Exporte los detalles de conexión mediante este comando para comprobar el tráfico principal que pasa a través del firewall.

show asp inspect-dp snort

show conn detail | redirect disk0:/con-detail.txt

El archivo se puede encontrar en "/mnt/disk0" desde el modo Linux. Copie el mismo a **/ngfw/var/common** para descargarlo de FMC.

Expert CP

/mnt/disk0/<nombre de archivo> /ngfw/var/common/

A continuación se muestra un ejemplo de la salida de detalles de conexión.

UDP interno: 10.x.x.x/137 interno: 10.x.x.43/137, indicadores - N1, inactivo 0s, tiempo de actividad 6D2h, tiempo de espera 2m0s, bytes 123131166926 << 123 GB y el tiempo de actividad parece ser de 6 días 2 horas

Id. de clave de búsqueda de conexión: 2255619827

UDP interno: 10.x.x.255/137 interno: 10.x.x.42/137, indicadores - N1, inactivo 0s, tiempo de actividad 7D5h, tiempo de espera 2m0s, bytes 116338988274

Id. de clave de búsqueda de conexión: 1522768243

UDP interno: 10.x.x.255/137 interno: 10.x.x.39/137, indicadores - N1, inactivo 0s, tiempo de actividad 8D1h, tiempo de espera 2m0s, bytes 60930791876

Id. de clave de búsqueda de conexión: 1208773687

UDP interno: 10.x.x.255/137 interno: 10.x.x0.34/137, indicadores - N1, inactivo 0s, tiempo de actividad 9D5h, tiempo de espera 2m0s, bytes 59310023420

Id. de clave de búsqueda de conexión: 597774515

3. Uso de Netflow

Los flujos Elephant son flujos de tráfico de gran volumen que pueden afectar al rendimiento de la red. La detección de estos flujos implica la supervisión del tráfico de red para identificar patrones que indiquen flujos persistentes y de gran tamaño. Cisco Firepower proporciona herramientas y funciones para detectar y analizar el tráfico de red, incluidos los flujos de elefantes. La herramienta NetFlow ayuda a recopilar la información del tráfico IP para la supervisión.

Este documento proporciona el proceso paso a paso para configurar la política de NetFlow en FMC

https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-management-center-virtual/221612-htz-01-2024-configure-netflow-in-fmc.html

Utilice un recopilador y analizador de NetFlow (por ejemplo: Cisco StealthWatch, SolarWinds o cualquier otra herramienta de análisis de NetFlow) para analizar los datos recopilados. Una vez identificados los flujos de elefantes, puede tomar medidas para mitigar su impacto:

- Modelado de tráfico y QoS: implemente políticas de calidad de servicio (QoS) para priorizar el tráfico y limitar el ancho de banda de los flujos de elefantes.

- Políticas de control de acceso: cree políticas de control de acceso para administrar y restringir los flujos de elefantes.

- Segmentación: utilice la segmentación de la red para aislar flujos de gran volumen y minimizar su impacto en el resto de la red.

- Equilibrio de carga: implemente el equilibrio de carga para distribuir el tráfico de forma más uniforme entre los recursos de red.

4. Supervisión y ajuste continuos

Supervise regularmente el tráfico de red para detectar nuevos flujos de elefantes y ajuste las políticas y configuraciones según sea necesario.

Con este proceso, puede detectar y administrar eficazmente los flujos de elefantes en su implementación de Cisco Firepower, lo que garantiza un mejor rendimiento de la red y una mejor utilización de los recursos.

Información Relacionada

Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.2

Configuración de NetFlow en FMC

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).