Detecção de fluxo de elefante em dispositivos Firepower

Contents

Introdução

Este documento descreve como executar a detecção de fluxo de elefante em um ambiente de Defesa contra ameaças (FTD) do Cisco Firepower.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes produtos:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- Netflow

Componentes Utilizados

As informações neste documento são baseadas em um FMC que executa a versão 7.1 do software ou posterior. As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste documento começaram com uma configuração limpa (padrão). Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A detecção de fluxo de elefantes no Cisco Firepower é crucial para identificar e gerenciar fluxos

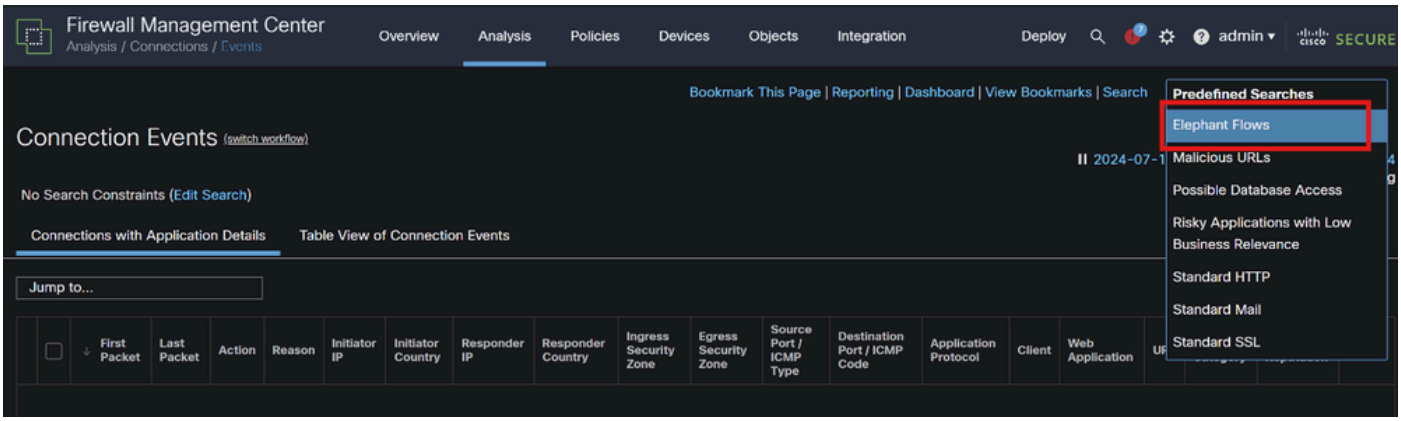
grandes e de longa duração que podem consumir recursos de rede significativos e afetar o desempenho. Os fluxos de elefantes podem ocorrer em aplicativos com grande volume de dados, como transmissão de vídeo, transferências de arquivos grandes e replicação de bancos de dados. Isso pode ser identificado usando estes métodos:

Métodos

1. Utilização do CVP

A detecção de fluxo de elefantes foi introduzida na versão 7.1. A versão 7.2 permite uma personalização mais fácil e a opção de contornar ou até mesmo acelerar fluxos de elefantes. O Intelligent Application Bypass (IAB) foi preterido a partir da versão 7.2.0 para dispositivos Snort 3.

A detecção do fluxo do elefante pode ser feita em Analysis > Connections > Events > Predefined Searches > Elephant Flows.



Eventos de conexão

Este documento fornece o processo passo a passo para configurar o Elephant Flow na política de controle de acesso

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. Usando CLI

a. O pico de CPU da instância de Snort também pode indicar que a rede está lidando com o fluxo Elephant, que pode ser identificado usando o seguinte comando:

show asp inspect-dp snort

Aqui está um exemplo para a saída do comando.

> show asp inspect-dp snort

Pid de Id de Informações de Status da Instância de Inspeção de SNORT

Conns Segs/Pkts Status tot (usr) de Uso da Cpu | sys)

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

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

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

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

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

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

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

6 16458 6% (5%| 0%) 2,2 K 1 PRONTO

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

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

9 16455 100% (100%| 0%) 2,2 K 5 PRONTO **<<<<** Alta utilização da CPU

10 16460 7% (6%| 0%) 2,2 K 0 PRONTO

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

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

b. Além disso, a saída do comando "top" do modo raiz também pode ajudar a verificar qualquer instância do Snort que esteja aumentando.

c. Exporte os detalhes da conexão usando esse comando para verificar o tráfego superior que passa pelo firewall.

show asp inspect-dp snort

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

O arquivo pode ser encontrado em "/mnt/disk0" no modo Linux. Copie o mesmo para **/ngfw/var/common** para fazer o download do FMC.

cp especialista

/mnt/disk0/<nome do arquivo> /ngfw/var/common/

Aqui está um exemplo para a saída dos detalhes da conexão.

UDP dentro: 10.x.x.x/137 dentro: 10.x.x.43/137, flags - N1, 0s ociosos, **uptime 6D2h**, timeout 2m0s, **bytes 123131166926** <<< 123 GB e uptime parece ser de 6 dias 2 horas

ID da chave de pesquisa de conexão: 2255619827

UDP interno: 10.x.x.255/137 interno: 10.x.x.42/137, flags - N1, 0s ociosos, tempo de atividade 7D5h, tempo limite 2m0s, bytes 116338988274

ID da chave de pesquisa de conexão: 1522768243

UDP interno: 10.x.x.255/137 interno: 10.x.x.39/137, sinalizadores - N1, 0s ociosos, tempo de atividade 8D1h, tempo limite 2m0s, bytes 60930791876

ID da chave de pesquisa de conexão: 1208773687

UDP interno: 10.x.x.255/137 interno: 10.x.x0.34/137, sinalizadores - N1, 0s ociosos, tempo de atividade 9D5h, tempo limite 2m0s, bytes 59310023420

ID da chave de pesquisa de conexão: 597774515

3. Usando o Netflow

Os fluxos de elefantes são fluxos de tráfego de alto volume que podem afetar o desempenho da rede. A detecção desses fluxos envolve o monitoramento do tráfego de rede para identificar padrões que indicam fluxos grandes e persistentes. O Cisco Firepower fornece ferramentas e recursos para detectar e analisar o tráfego de rede, incluindo fluxos de elefantes. A ferramenta NetFlow ajuda a coletar informações de tráfego IP para monitoramento.

Este documento fornece o processo passo a passo para configurar a política do NetFlow no 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

Use um coletor e analisador NetFlow (por exemplo: Cisco Stealthwatch, SolarWinds ou qualquer outra ferramenta de análise NetFlow) para analisar os dados coletados. Depois que os fluxos de elefantes são identificados, você pode tomar medidas para atenuar seu impacto:

- Modelagem de tráfego e QoS: Implemente políticas de Qualidade de Serviço (QoS) para priorizar o tráfego e limitar a largura de banda dos fluxos de elefantes.
- Políticas de controle de acesso: crie políticas de controle de acesso para gerenciar e restringir fluxos de elefantes.
- Segmentação: use a segmentação de rede para isolar fluxos de alto volume e minimizar seu impacto no restante da rede.
- Balanceamento de carga: implemente o balanceamento de carga para distribuir o tráfego de forma mais uniforme entre os recursos da rede.

4. Monitoramento e ajuste contínuos

Monitore regularmente o tráfego da sua rede para detectar novos fluxos de elefantes e ajustar suas políticas e configurações conforme necessário.

Com esse processo, você pode detectar e gerenciar com eficiência os fluxos de elefantes na implantação do Cisco Firepower, garantindo melhor desempenho da rede e utilização de recursos.

Informações Relacionadas

Guia de configuração de dispositivos do Cisco Secure Firewall Management Center, 7.2

Configurar o NetFlow no FMC

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.