firepower 장치의 Elephant Flow 탐지

목차

소개

이 문서에서는 Cisco FTD(Firepower 위협 방어) 환경에서 Elephant Flow Detection을 수행하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 제품에 대해 알고 있는 것이 좋습니다.

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

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 7.1 이상을 실행하는 FMC를 기반으로 합니다. 이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된 (기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

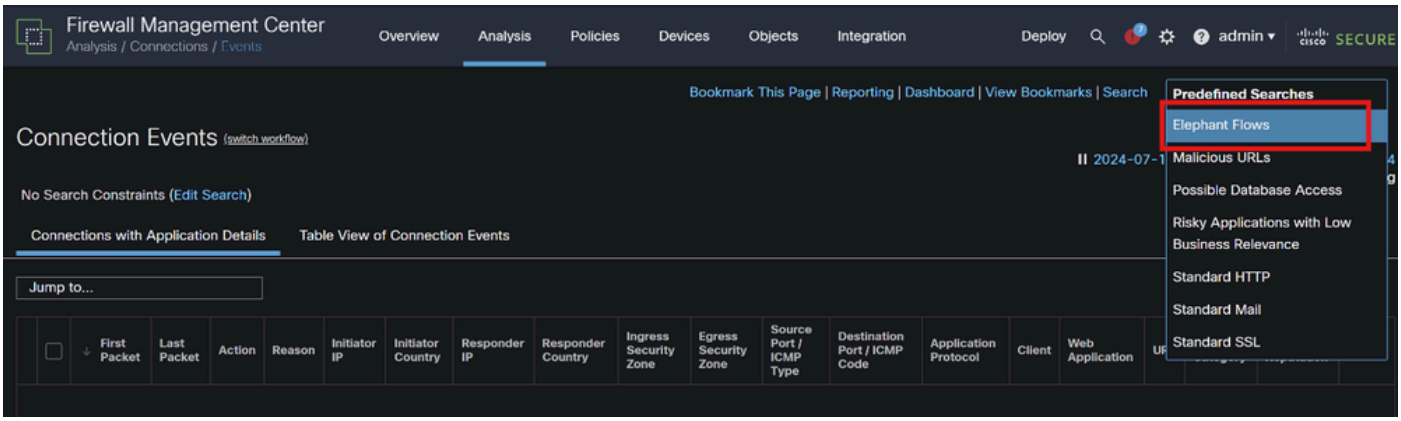
Cisco Firepower의 Elephant Flow Detection은 상당한 네트워크 리소스를 소비하고 성능에 영향을 줄 수 있는 수명이 긴 대규모 플로우를 식별하고 관리하는 데 매우 중요합니다. 엘리펀트 흐름은 비디오 스트리밍, 대용량 파일 전송, 데이터베이스 복제와 같이 데이터 사용량이 많은 애플리케이션에서 발생할 수 있습니다. 이는 다음 방법을 사용하여 식별할 수 있습니다.

방법

1. FMC 사용

Elephant flow detection은 릴리스 7.1에 도입되었습니다. Release 7.2를 사용하면 손쉽게 사용자 지정할 수 있으며, 코끼리 흐름을 우회하거나 심지어 조절할 수도 있습니다. IAB(Intelligent Application Bypass)는 Snort 3 디바이스의 버전 7.2.0부터 더 이상 사용되지 않습니다.

코끼리 흐름 탐지는 Analysis > Connections > Events > Predefined Searches > Elephant Flows에서 수행할 수 있습니다.



연결 이벤트

이 문서에서는 액세스 제어 정책의 Elephant Flow 구성을 위한 단계별 프로세스를 제공합니다

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. CLI 사용

a. Snort 인스턴스 CPU 스파이킹은 또한 네트워크가 다음 명령을 사용하여 식별할 수 있는 Elephant 플로우를 처리하고 있음을 나타낼 수 있습니다.

show asp inspect-dp snort

다음은 명령 출력의 예입니다.

> show asp inspect-dp snort

SNORT 검사 인스턴스 상태 정보 Id Pid

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

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

0 16450 8%(7%| 0%) 2.2 K 0 지원

1 16453 9%(8%| 0%) 2.2 K 0 지원

2 16451 6%(5%| 1%) 2.3 K 0 지원

3 16454 5%(5%| 0%) 2.2 K 1 지원

4 16456 6%(6%| 0%) 2.3 K 0 지원

5 16457 6%(6%| 0%) 2.3 K 0 지원

6164586%(5%| 0%) 2.2 K 1 지원

7 16459 4%(4%| 0%) 2.3 K 0 지원

8 16452 9%(8%| 1%) 2.2 K 0 지원

9 16455 100%(100%| 0%) 2.2 K 5 지원 <<<< 높은 CPU 사용률 10164607%(6%| 0%) 2.2 K 0 지원

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

요약 15%(14%| 0%) 24.6 K7

b. 또한 루트 모드의 "top" 명령 출력도 Snort 인스턴스가 높아지는 것을 확인하는 데 도움이 될 수 있습니다.

c. 방화벽을 통과하는 상위 트래픽을 확인하려면 이 명령을 사용하여 연결 세부사항을 내보냅니다.

show asp inspect-dp snort

conn 세부 정보 표시 | disk0 리디렉션:/con-detail.txt

Linux 모드의 "/mnt/disk0"에서 파일을 찾을 수 있습니다. FMC에서 다운로드하려면 **/ngfw/var/**common에 동일한 내용을 복사합니다.

전문가 cp

/mnt/disk0/<파일 이름> /ngfw/var/common/

다음은 연결 세부 정보 출력의 예입니다.

UDP inside: 10.x.x.x/137 inside: 10.x.x.43/137, flags - N1, idle 0s, uptime 6D2h, timeout 2m0s, bytes 123131166926 <<< 123GB 및 uptime은 6일 2시간인 것 같습니다.

연결 조회 키 ID: 2255619827

UDP 내부: 10.x.x.255/137 내부: 10.x.x.42/137, flags - N1, idle 0s, uptime 7D5h, timeout 2m0s, bytes 116338988274

연결 조회 키 ID: 1522768243

UDP 내부: 10.x.x.255/137 내부: 10.x.x.39/137, flags - N1, idle 0s, uptime 8D1h, timeout 2m0s, bytes 60930791876

연결 조회 키 ID: 1208773687

UDP 내부: 10.x.x.255/137 내부: 10.x.x0.34/137, flags - N1, idle 0s, uptime 9D5h, timeout 2m0s, bytes 59310023420

연결 조회 키 ID: 597774515

3. Netflow 사용

Elephant Flows는 네트워크 성능에 영향을 줄 수 있는 대용량 트래픽 흐름입니다. 이러한 흐름을 탐지하려면 네트워크 트래픽을 모니터링하여 크고 지속적인 흐름을 나타내는 패턴을 식별합니다. Cisco Firepower은 엘리펀트 플로우를 포함하여 네트워크 트래픽을 탐지하고 분석하는 데 필요한 툴과 기능을 제공합니다. NetFlow 툴은 모니터링을 위해 IP 트래픽 정보를 수집하는 데 도움이 됩니다.

이 문서에서는 FMC에서 NetFlow 정책을 구성하는 단계별 프로세스를 제공합니다

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

NetFlow 컬렉터 및 분석기(예: Cisco Stealthwatch, SolarWinds 또는 기타 NetFlow 분석 툴)를 사용하여 수집된 데이터를 분석합니다. 코끼리의 흐름이 확인되면, 그 영향을 완화하기 위한 조치를 취할 수 있습니다.

- 트래픽 셰이핑 및 QoS: QoS(Quality of Service) 정책을 구현하여 트래픽의 우선 순위를 정하고 코끼리 흐름의 대역폭을 제한합니다.

- 액세스 제어 정책: 코끼리 흐름을 관리하고 제한하는 액세스 제어 정책을 생성합니다.

- 세그멘테이션: 네트워크 세그멘테이션을 사용하여 대량의 흐름을 격리하고, 이러한 흐름이 네트워크의 나머지 부분에 미치는 영향을 최소화합니다.

- 로드 밸런싱: 로드 밸런싱을 구현하여 네트워크 리소스 전체에 트래픽을 더 균일하게 분산합니다.

4. 지속적인 모니터링 및 조정

네트워크 트래픽을 정기적으로 모니터링하여 새로운 코끼리 흐름을 탐지하고 필요에 따라 정책 및 컨피그레이션을 조정합니다.

이 프로세스를 통해 Cisco Firepower 구축에서 엘리펀트 흐름을 효과적으로 탐지하고 관리하여 네트워크 성능과 리소스 활용도를 높일 수 있습니다.

관련 정보

Cisco Secure Firewall Management Center Device Configuration Guide, 7.2

FMC에서 NetFlow 구성

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.