Elefantenfluss auf FirePOWER-Geräten erkennen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die Elephant Flow Detection in einer Cisco Firepower Threat Defense (FTD)-Umgebung durchgeführt wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit den folgenden Produkten vertraut sind:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem FMC, das die Softwareversion 7.1 oder höher ausführt. Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle in diesem Dokument verwendeten Geräte begannen mit einer gelöschten (Standard-)Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Elephant Flow Detection in Cisco FirePOWER ist entscheidend für die Identifizierung und

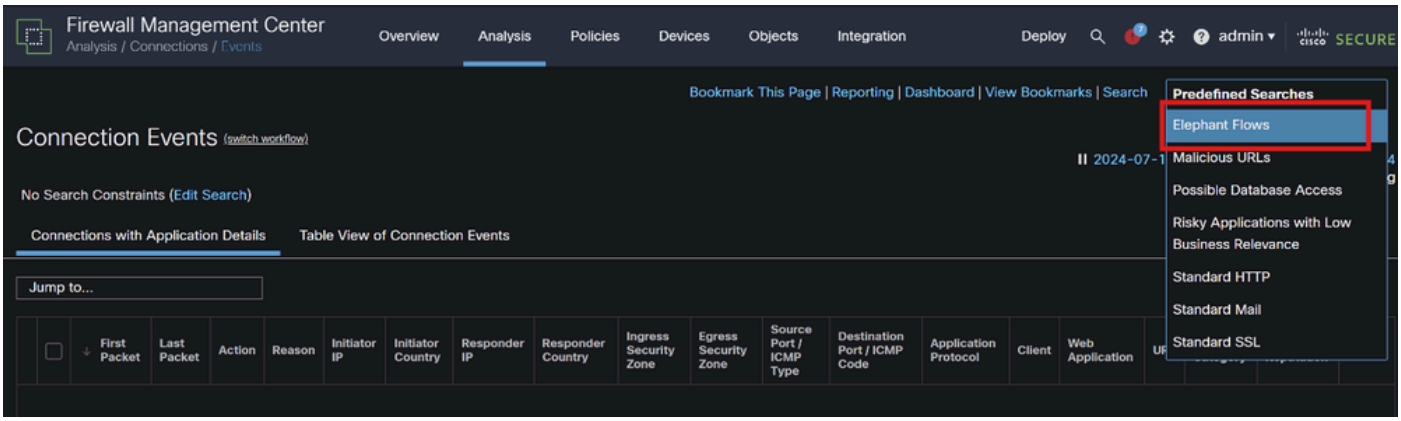
Verwaltung großer, langlebiger Datenströme, die erhebliche Netzwerkressourcen belegen und die Leistung beeinträchtigen können. Elephant-Datenflüsse können in datenintensiven Anwendungen wie Video-Streaming, Übertragungen großer Dateien und Datenbankreplikation auftreten. Dies lässt sich anhand der folgenden Methoden feststellen:

Methoden

1. Verwendung von FMC

Die Elefantenflussdetektion wurde in Version 7.1 eingeführt. Release 7.2 ermöglicht eine einfachere Anpassung und die Option, Elefantenflüsse zu umgehen oder sogar zu drosseln. Intelligent Application Bypass (IAB) ist seit Version 7.2.0 für Snort 3-Geräte veraltet.

Die Erkennung des Elefantenflusses kann unter Analyse > Verbindungen > Ereignisse > Vordefinierte Suchen > Elefantenflüsse erfolgen.



Verbindungsereignisse

Dieses Dokument enthält detaillierte Anweisungen zur Konfiguration der Richtlinie für die Elephant Flow-Zugriffskontrolle.

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. Verwenden der CLI

a. Snort-Instanz-CPU-Spiking kann auch anzeigen, dass das Netzwerk mit dem Elephant-Fluss zu tun hat, der mit dem folgenden Befehl identifiziert werden kann:

asp inspect-dp snort anzeigen

Hier ist ein Beispiel für die Befehlsausgabe.

> asp inspect-dp snort anzeigen

SNORT Inspection-Instanzstatus-Info-ID PID

CPU-Nutzung verbindet Segmente/Pakete mit Status tot (Benutzer) | sys)

- ----- ---------- ---------- ---------- ----------

0 16450 8 % (7 %) 0 %) 2.200 0 BEREIT

1 16453 9 % (8 %) 0 %) 2.200 0 BEREIT

2 16451 6 % (5 %) 1 %) 2,3.000 BEREIT

3 16454 5 % (5 %) 0 %) 2.200 1 BEREIT

4 16456 6 % (6 %) 0 %) 2,3.000 BEREIT

5 16457 6 % (6 %) 0 %) 2,3.000 BEREIT

6 16458 6 % (5 %) 0 %) 2.200 1 BEREIT

7 16459 4 % (4 %) 0 %) 2,3.000 BEREIT

8 16452 9 % (8 %) 1 %) 2.200 0 BEREIT

9 16455 100 % (100 %) 0 %) 2.200 5 BEREIT **<<<<<** Hohe CPU-Auslastung 10 16460 7 % (6 %| 0 %) 2.200 0 BEREIT

- ----- ---------- ---------- ---------- ----------

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

b. Außerdem kann die "top"-Befehlsausgabe aus dem Root-Modus auch helfen, jede Snort-Instanz zu überprüfen, die hoch geht.

c. Exportieren Sie die Verbindungsdetails mit diesem Befehl, um zu überprüfen, ob der meiste Datenverkehr die Firewall passiert.

asp inspect-dp snort anzeigen

Verbindungsdetails anzeigen | disk0:/con-detail.txt umleiten

Die Datei ist unter "/mnt/disk0" im Linux-Modus zu finden. Kopieren Sie das gleiche in **/ngfw/var/common**, um es von FMC herunterzuladen.

Experte CP

/mnt/disk0/<Dateiname> /ngfw/var/common/

Hier ein Beispiel für die Ausgabe der Verbindungsdetails.

UDP inside: 10.x.x.x/137 inside: 10.x.x.43/137, flags - N1, idle 0s, uptime 6D2h, timeout 2m0s, bytes 123131166926 <<<<< 123 GB und uptime scheint 6 days 2 hours zu sein

Schlüsselkennung für Verbindungsueberwachung: 2255619827

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

Schlüsselkennung für Verbindungsueberwachung: 1522768243

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

Schlüsselkennung für Verbindungsueberwachung: 1208773687

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

Schlüsselkennung für Verbindungsueberwachung: 597774515

3. Verwendung von NetFlow

Bei Elephant-Datenströmen handelt es sich um Datenverkehrsströme mit hohem Volumen, die die Netzwerkleistung beeinträchtigen können. Zur Erkennung dieser Datenströme wird der Netzwerkverkehr überwacht, um Muster für große, persistente Datenströme zu identifizieren. Cisco FirePOWER bietet Tools und Funktionen zum Erkennen und Analysieren von Netzwerkverkehr, einschließlich Elefantenflüssen. Das NetFlow-Tool hilft bei der Erfassung der IP-Datenverkehrsinformationen für die Überwachung.

Dieses Dokument enthält detaillierte Anweisungen zur Konfiguration der NetFlow-Richtlinie auf 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

Verwenden Sie einen NetFlow-Collector und -Analyzer (z. B. Cisco Stealthwatch, SolarWinds oder ein anderes NetFlow-Analyse-Tool), um die erfassten Daten zu analysieren. Sobald Elefantenströme erkannt wurden, können Sie Schritte ergreifen, um ihre Auswirkungen zu mildern:

- Traffic Shaping und QoS: Implementieren von QoS-Richtlinien (Quality of Service), um den Datenverkehr zu priorisieren und die Bandbreite von Elefantenflüssen zu begrenzen.

- Zugriffskontrollrichtlinien: Erstellen Sie Zugriffskontrollrichtlinien, um Elefantenflüsse zu verwalten und einzuschränken.

- Segmentierung: Isolieren Sie Datenströme mit hohem Volumen mithilfe der Netzwerksegmentierung, und minimieren Sie deren Auswirkungen auf den Rest des Netzwerks.

- Load Balancing: Implementieren Sie Load Balancing, um den Datenverkehr gleichmäßiger auf die Netzwerkressourcen zu verteilen.

4. Kontinuierliche Überwachung und Anpassung

Überwachen Sie regelmäßig den Netzwerkverkehr, um neue Elefantenströme zu erkennen und Ihre Richtlinien und Konfigurationen nach Bedarf anzupassen.

Mit diesem Prozess können Sie Elefantenflüsse in Ihrer Cisco FirePOWER-Bereitstellung effektiv erkennen und verwalten und so eine bessere Netzwerkleistung und Ressourcenauslastung sicherstellen.

Zugehörige Informationen

Gerätekonfigurationsanleitung für Cisco Secure Firewall Management Center, 7.2

Konfigurieren von NetFlow in FMC

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.