Olifantstroom op FirePOWER-apparaten detecteren

Inhoud

Inleiding

Dit document beschrijft hoe u Elephant Flow Detection kunt uitvoeren in een Cisco Firepower Threat Defence (FTD)-omgeving.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze producten:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op een VCC dat de software Versie 7.1 of hoger uitvoert. De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, zijn gestart met een uitgeschakelde (standaard) configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Olifant Flow Detection in Cisco Firepower is cruciaal voor het identificeren en beheren van grote,

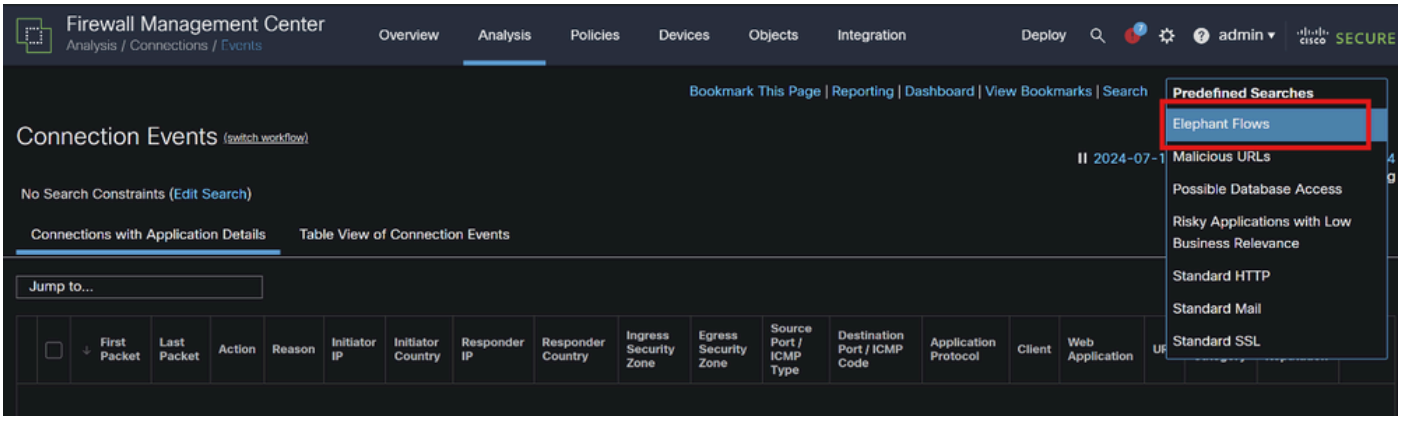
langdurige stromen die aanzienlijke netwerkresources kunnen verbruiken en de prestaties kunnen beïnvloeden. Olifantstromen kunnen voorkomen in gegevensintensieve toepassingen zoals videostreaming, grote bestandsoverdrachten en databasereplicatie. Dit kan met behulp van de volgende methoden worden vastgesteld:

Methoden

1. Gebruik van VCC

De detectie van olifantenstromen werd geïntroduceerd in release 7.1. Release 7.2 maakt een eenvoudiger aanpassing mogelijk en biedt de mogelijkheid om olifantenstromen te omzeilen of zelfs te verstikken. Intelligent Application Bypass (IAB) wordt vanaf versie 7.2.0 afgekeurd voor Snort 3-apparaten.

Detectie van de olifantenstroom kan worden gedaan onder Analyse > Verbindingen > Gebeurtenissen > Vooraf gedefinieerde zoekopdrachten > Olifantstromen.



Verbindingsgebeurtenissen

Dit document biedt stap voor stap een proces voor het configureren van Olifant Flow op Access Control Policy

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 gebruiken

a. Snortinstantie CPU spiking kan ook aangeven dat het netwerk de olifantenstroom verwerkt die met de volgende opdracht kan worden geïdentificeerd:

aanwijzen als 'inspect-dp'-snort

Hier is een voorbeeld voor de opdrachtoutput.

> toon asp inspect-dp snort

SNORT Inspect Instance Status Info ID PID

Status voor CPU-gebruik van segmenten/PKTS-overzichten (USR) | sys)

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

0 16450 8% (7%)| 0%) GEREED VOOR 2,2 K 0

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

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

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

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

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

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

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

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

9 16455 100% (100%)| 0%) 2.2 K 5 KLAAR <<<<<< Hoge CPU-benutting 10 16460 7% (6%| 0%) GEREED VOOR 2,2 K 0

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

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

b. Ook, "top" opdrachtoutput van root mode kan ook helpen om elke Sort instantie te controleren die hoog gaat.

c. Exporteer de verbindingsgegevens met deze opdracht om te controleren of het bovenste verkeer door de firewall loopt.

aanwijzen als 'inspect-dp'-snort

Conn-details weergeven | redirect disk0:/con-detail.txt

Het bestand is te vinden onder "/mnt/disk0" van Linux-modus. Kopieer hetzelfde naar **/ngfw/var/common** om het gedownload te krijgen van FMC.

expert-cp

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

Hier is een voorbeeld voor de uitvoer van het verbindingsdetail.

UDP binnenin: 10.x.x.x/137 binnenin: 10.x.x.43/137, vlaggen - N1, idle 0s, uptime 6D2h, time-out 2m0s, bytes 123131166926 << 123 GB en uptime lijkt 6 dagen 2 uur te zijn

Toets voor opzoeken verbinding: 2255619827

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

Toets voor opzoeken verbinding: 1522768243

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

Toets voor opzoeken verbinding: 1208773687

UDP binnen: 10.x.x.255/137 binnen: 10.x.x0.34/137, vlaggen - N1, stationair 0s, uptime 9D5h, timeout 2m0s, bytes 59310023420

Toets voor opzoeken verbinding: 597774515

3. Gebruik van NetFlow

Olifantstromen zijn verkeersstromen met een hoog volume die van invloed kunnen zijn op de netwerkprestaties. Het detecteren van deze stromen impliceert het bewaken van netwerkverkeer om patronen te identificeren die grote, persistente stromen aangeven. Cisco Firepower biedt tools en functies om netwerkverkeer, waaronder olifantenstromen, te detecteren en te analyseren. NetFlow-tool helpt bij het verzamelen van IP-verkeersinformatie voor bewaking.

Dit document biedt stapsgewijze procedures voor het configureren van NetFlow-beleid op 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

Gebruik een NetFlow Collector en analyzer (bijvoorbeeld Cisco Stealthwatch, SolarWinds of een ander NetFlow-analyseprogramma) om de verzamelde gegevens te analyseren. Zodra de olifantenstromen zijn geïdentificeerd, kunt u stappen nemen om hun effect te verlichten:

- Traffic Shaping en QoS: implementeren van QoS-beleid (Quality of Service) om prioriteit te geven aan verkeer en de bandbreedte van olifantenstromen te beperken.

- Toegangsbeheer Beleid: Maak toegangscontrole beleid om olifantenstromen te beheren en te beperken.

- Segmentatie: gebruik netwerksegmentatie om stromen met een hoog volume te isoleren en hun impact op de rest van het netwerk te minimaliseren.

- Taakverdeling: implementeer taakverdeling om verkeer evenwichtiger over netwerkbronnen te verdelen.

4. Continue bewaking en aanpassing

Controleer regelmatig uw netwerkverkeer om nieuwe olifantenstromen te detecteren en pas uw beleid en configuraties aan als dat nodig is.

Met dit proces kunt u effectief olifantenstromen detecteren en beheren in uw Cisco Firepower-implementatie, waardoor u verzekerd bent van betere netwerkprestaties en een beter gebruik van bronnen.

Gerelateerde informatie

Handleiding voor configuratie van apparaat in Cisco Secure Firewall Management Center, 7.2

NetFlow configureren in VCC

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.