Detect Elephant Flow on Firepower Devices

Contents

Introduction

This document describes how to perform Elephant Flow Detection in a Cisco Firepower Threat Defense (FTD) environment.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these products:

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

Components Used

The information in this document is based on an FMC that runs software Version 7.1 or later. The information in this document was created from the devices in a specific lab environment. All the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

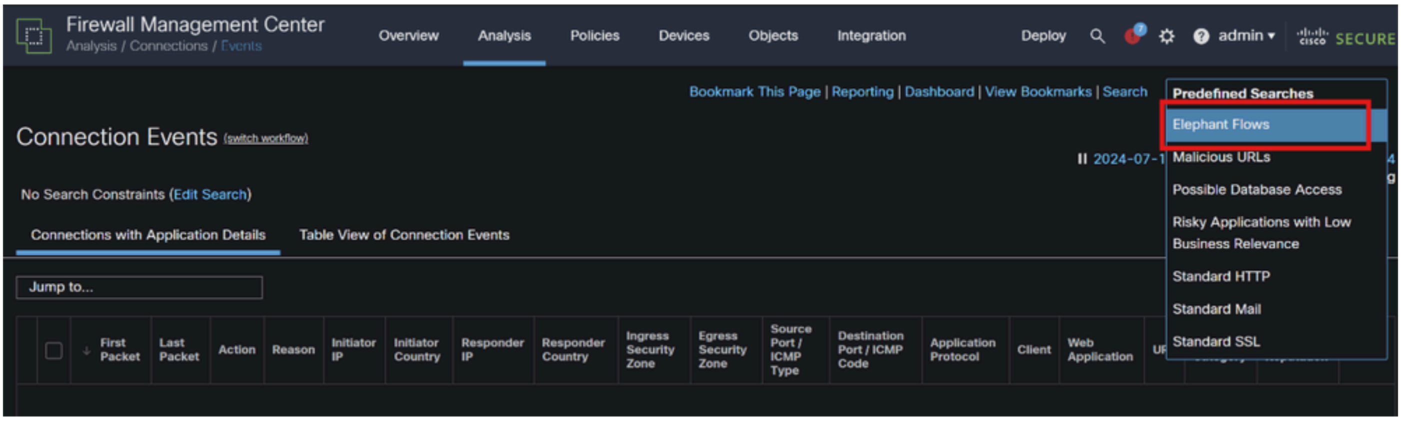
Elephant Flow Detection in Cisco Firepower is crucial for identifying and managing large, long-lived flows that can consume significant network resources and affect performance. Elephant flows can occur in data-heavy applications like video streaming, large file transfers, and database replication. This can be identified using these methods:

Methods

1. Using FMC

Elephant flow detection was introduced in release 7.1. Release 7.2 allows easier customization and the option to bypass or even throttle elephant flows. Intelligent Application Bypass (IAB) is deprecated from version 7.2.0 onwards for Snort 3 devices.

Detection of the Elephant flow can be done under **Analysis > Connections > Events > Predefined Searches > Elephant Flows**.



Connection Events

This document provides Step-by-Step process for configuring Elephant Flow on 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. Using CLI

a. Snort instance CPU spiking can also indicate that the network is dealing with the Elephant flow which can be identified using folllowing command:

show asp inspect-dp snort

Here is an example for the command output.

> show asp inspect-dp snort

```
SNORT Inspect Instance Status Info Id Pid

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

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

0  16450   8% (  7%|  0%)   2.2 K      0        READY

1  16453   9% (  8%|  0%)   2.2 K      0        READY

2  16451   6% (  5%|  1%)   2.3 K      0        READY

3  16454   5% (  5%|  0%)   2.2 K      1        READY

4  16456   6% (  6%|  0%)   2.3 K      0        READY
```

```
5  16457   6% (  6%|  0%)   2.3 K      0       READY

6  16458   6% (  5%|  0%)   2.2 K      1       READY

7  16459   4% (  4%|  0%)   2.3 K      0       READY

8  16452   9% (  8%|  1%)   2.2 K      0       READY

9  16455 100% (100%|  0%)   2.2 K   5     READY       <<<< High CPU utilization

10 16460   7% (  6%|  0%)   2.2 K      0       READY

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

Summary   15% ( 14%|  0%)  24.6 K      7
```

b. Also, "**top**" command output from root mode can also help to check any Snort instance going high.

c. Export the connection detail using this command to check for the top traffic passing through the firewall.

```
show asp inspect-dp snort

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

The file can be found under "/mnt/disk0" from Linux mode. Copy the same to **/ngfw/var/common** to get it downloaded from FMC.

```
expert cp

/mnt/disk0/<file name> /ngfw/var/common/
```

Here is an example for the connection detail output.

```
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 and uptime seems to be 6 days 2 hours

Connection lookup keyid: 2255619827

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

Connection lookup keyid: 1522768243

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

Connection lookup keyid: 1208773687

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

Connection lookup keyid: 597774515
```

3. Using Netflow

Elephant flows are high-volume traffic flows that can impact network performance. Detecting these flows involves monitoring network traffic to identify patterns indicating large, persistent flows. Cisco Firepower provides tools and features to detect and analyze network traffic, including elephant flows. NetFlow tool helps collecting the IP traffic information for monitoring.

This document provides Step-by-Step process for configuring NetFlow policy on 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 a NetFlow collector and analyzer (for example: Cisco Stealthwatch, SolarWinds, or any other NetFlow analysis tool) to analyze the collected data. Once elephant flows are identified, you can take steps to mitigate their impact:

- Traffic Shaping and QoS: Implement Quality of Service (QoS) policies to prioritize traffic and limit the bandwidth of elephant flows.
- Access Control Policies: Create access control policies to manage and restrict elephant flows.
- Segmentation: Use network segmentation to isolate high-volume flows and minimize their impact on the rest of the network.
- Load Balancing: Implement load balancing to distribute traffic more evenly across network resources.

4. Continuous Monitoring and Adjustment

Regularly monitor your network traffic to detect new elephant flows and adjust your policies and configurations as needed.

With this process, you can effectively detect and manage elephant flows in your Cisco Firepower deployment, ensuring better network performance and resource utilization.

Related Information

Cisco Secure Firewall Management Center Device Configuration Guide, 7.2

Configure NetFlow in FMC