检测Firepower设备上的Elephant Flow

目录

简介

本文档介绍如何在Cisco Firepower威胁防御(FTD)环境中执行大象流检测。

先决条件

要求

思科建议您了解以下产品：

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

使用的组件

本文档中的信息基于运行软件版本7.1或更高版本的FMC。 本文档中的信息都是基于特定实验室环境中的设备编写的。用于本文的所有设备始于初始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

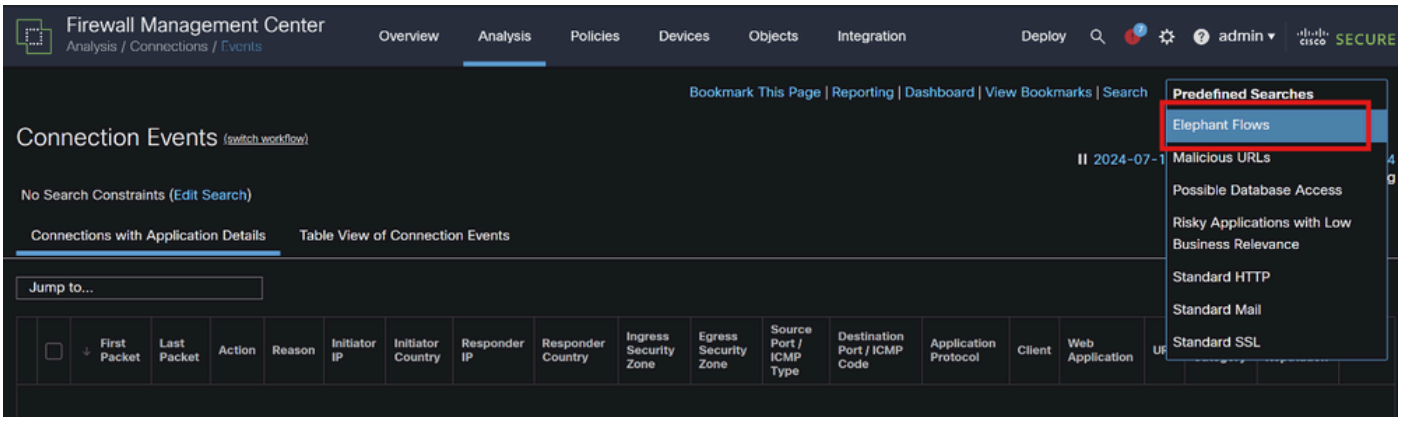
Cisco Firepower中的大流量检测对于识别和管理可能会消耗大量网络资源并影响性能的大型长期流量至关重要。大数据流量可能发生在数据流量较大的应用中，如视频流、大型文件传输和数据库复制。可使用以下方法识别此问题：

方法

1. 使用FMC

大象流检测在版本7.1中引入。版本7.2允许更轻松的自定义和绕过甚至限制大象流的选项。对于Snort 3设备，从版本7.2.0开始，智能应用绕行(IAB)已作废。

可以在分析>连接>事件>预定义搜索>大象流下检测大象流。



连接事件

本文档提供在访问控制策略中配置大象流的分步过程

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. 使用CLI

a. Snort实例CPU尖峰也可能表示网络正在处理Elephant流，可使用以下命令识别此流：

show asp inspect-dp snort

下面是命令输出的示例。

> show asp inspect-dp snort

SNORT检查实例状态信息Id Pid

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

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

0 16450 8% (7%| 0%) 22000就绪

1 16453 9% (8%| 0%) 22000就绪

2 16451 6% (5%| 1%) 23000就绪

3 16454 5% (5%| 0%) 2.2 K 1就绪

4 16456 6% (6%| 0%) 23000就绪

5 16457 6% (6%| 0%) 23000就绪

6 16458 6% (5%| 0%) 2.2 K 1就绪

7 16459 4% (4%| 0%) 23000就绪

8 16452 9% (8%| 1%) 22000就绪

9 16455 100% (100%| 0%) 2.2 K 5就绪<<<< CPU使用率较高

10 16460 7% (6%| 0%) 22000就绪

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

摘要15% (14%| 0%) 2.46万7

b.此外，根模式下的top命令输出也有助于检查任何Snort实例是否变得过高。

c.使用此命令导出连接详细信息，以检查通过防火墙的流量排行榜。

show asp inspect-dp snort

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

可以在Linux模式下的"/mnt/disk0"下找到该文件。将相同内容复制到**/ngfw/var/common**，以便从FMC下载该文档。

专家cp

/mnt/disk0/<文件名> /ngfw/var/common/

以下是连接详细信息输出的示例。

UDP内部：10.x.x.x/137内部：10.x.x.43/137，标志- N1，空闲0，**正常运行时间6D2h**，超时2m0，**字节123131166926 < < 123 GB，正常运行时间似乎为6天2小时**

连接查找关键字ID：2255619827

UDP内部：10.x.x.255/137内部：10.x.x.42/137，标志- N1，空闲0，正常运行时间7D5h，超时2m0，字节116338988274

连接查找关键字ID：1522768243

UDP内部：10.x.x.255/137内部：10.x.x.39/137，标志- N1，空闲0，正常运行时间8D1h，超时2m0，字节60930791876

连接查找关键字ID：1208773687

UDP内部：10.x.x.255/137内部：10.x.x0.34/137，标志- N1，空闲0，正常运行时间9D5h，超时2m0，字节59310023420

连接查找关键字ID：597774515

3. 使用Netflow

大流量是指可能影响网络性能的大流量流量。检测这些流量涉及监控网络流量，以识别指示大型、持续流量的模式。Cisco

Firepower提供检测和分析网络流量（包括大流量）的工具和功能。NetFlow工具可帮助收集IP流量信息以进行监控。

本文档提供在FMC上配置NetFlow策略的分步过程

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

使用NetFlow收集器和分析器（例如：Cisco Stealthwatch、SolarWinds或任何其他NetFlow分析工具）来分析收集的数据。一旦确定了大象流动情况，您就可以采取措施减轻其影响：

- 流量整形和QoS：实施服务质量(QoS)策略，确定流量的优先级并限制大流量的带宽。
- 访问控制策略(Access Control Policies)：创建访问控制策略以管理和限制大象流量。
- 分段：使用网络分段来隔离大流量并将它们对网络其余部分的影响降至最低。
- 负载均衡：实施负载均衡，在网络资源之间更均匀地分配流量。

4. 持续监测和调整

定期监控网络流量以检测新的大流量，并根据需要调整策略和配置。

通过此流程，您可以有效地检测和管理Cisco Firepower部署中的大流量，确保更好的网络性能和资源利用率。

相关信息

Cisco安全防火墙管理中心设备配置指南7.2

在FMC中配置NetFlow

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。