Firepower管理中心显示在错误方向的一些TCP连接事件

Contents

Introduction

本文在发起者IP是TCP连接的服务器IP的反向描述原因和缓解步骤的Firepower管理显示TCP连接事件的Center(FMC)，并且回应者IP是TCP连接的客户端IP。

> **Note**:有出现时间的多个原因的这样事件。本文解释此症状的多数常见原因。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Firepower技术
- 基础知识可适应的安全工具(ASA)
- 对Transmission Control Protocol(TCP)定时机制的了解

Components Used

本文档中的信息基于以下软件和硬件版本：

- ASA Firepower该威胁的防御(5506X/5506H-X/5506W-X、ASA 5508-X， ASA 5516-X)运行软件版本6.0.1及以后
- ASA Firepower该威胁的防御(5512-X,5515-X、ASA 5525-X， ASA 5545-X， ASA 5555-X,FP9300,FP4100)运行软件版本6.0.1及以后
- ASA用该Firepower的模块(5506X/5506H-X/5506W-X、ASA 5508-X， ASA 5516-X,5515-X，ASA 5525-X， ASA 5545-X， ASA 5555-X， ASA 5585-X)运行软件版本6.0.0及以后
- Firepower管理中心(FMC)版本6.0.0和以上

The information in this document was created from the devices in a specific lab environment.用于

本文的所有设备从一种清楚的(默认)配置开始了。If your network is live, make sure that you understand the potential impact of any command.

背景

在TCP连接，**客户端**是指发送初始信息包的IP。Firepower管理中心生成连接事件，当可管理的设备(传感器或FTD)时看到连接的最初的TCP信息包。

跟踪TCP连接的状态的设备有被定义的**空闲超时**确信，没有由终端不正确断开的连接不浪费可利用的内存长的时期。被建立的TCP连接的默认空闲超时在Firepower是**三分钟**。坚持空闲在三分钟或更多的TCP连接，没有由Firepower IPS传感器跟踪。

后续信息包，在超时对待新的TCP流和转发决策后根据匹配此信息包的规则被使用。当信息包是从服务器时，服务器IP被记录作为此新的流发起者。当记录为规则时是启用的，连接事件在Firepower管理中心生成。

> **Note**:根据被配置的策略，来的信息包的转发决策，在超时是与最初的TCP信息包的后决策不同。如果被配置的默认动作是“块”，信息包被丢弃。

此症状示例是根据下面屏幕画面：

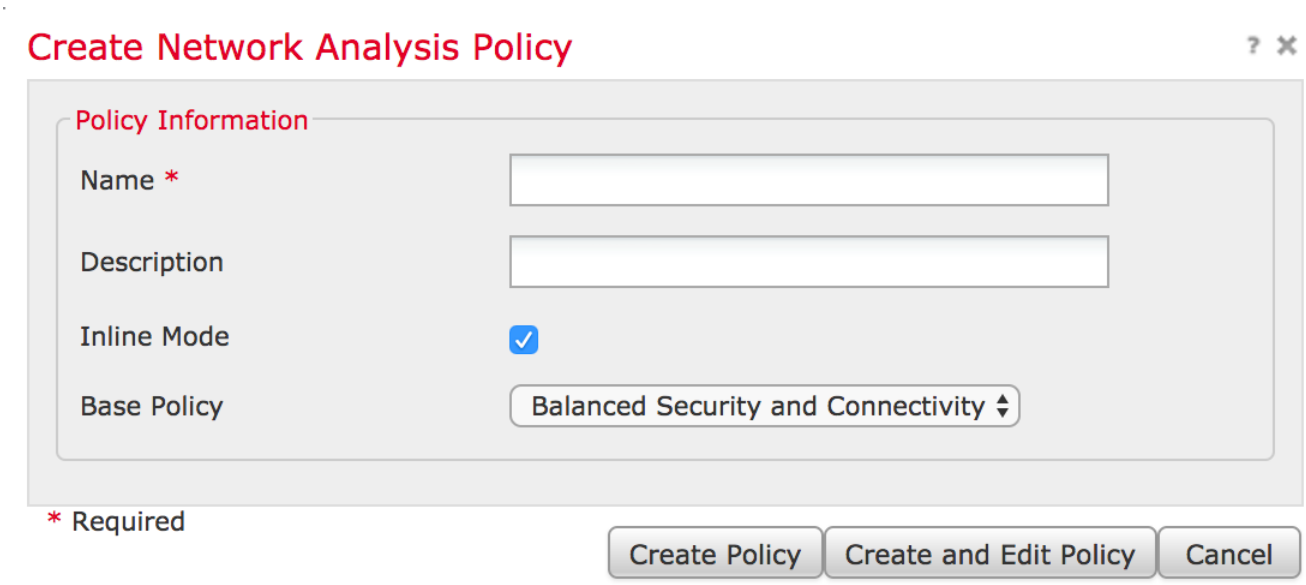
	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
	2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
	2017-05-12 17:39:13		Allow		192.168.38.30		10.32.38.30				44705 / tcp	443 (https) / tcp

解决方案

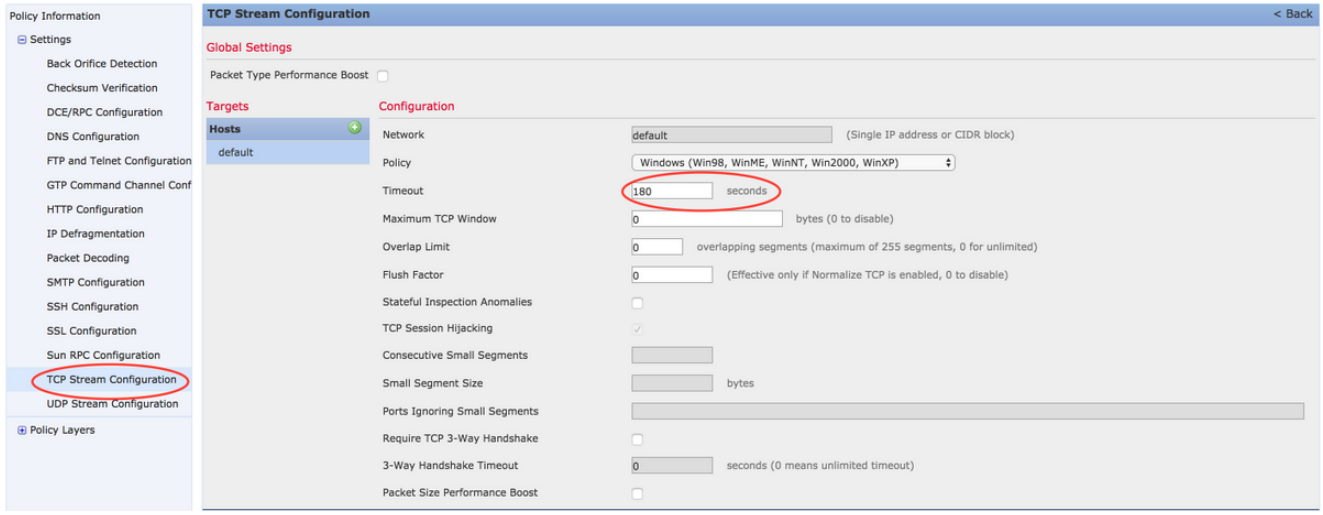
上述的问题通过增加TCP连接**超时**减轻。按顺序请更改超时，

1. 连接对**策略>访问控制>闯入**。
2. 连接对右上角并且选择**网络访问策略**。

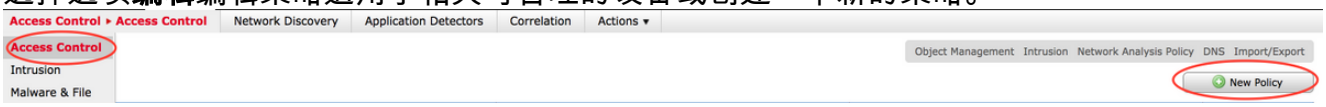
3. 选择**创建策略**，选择名字并且点击**Create并且编辑策略**。请勿修改**基本策略**。



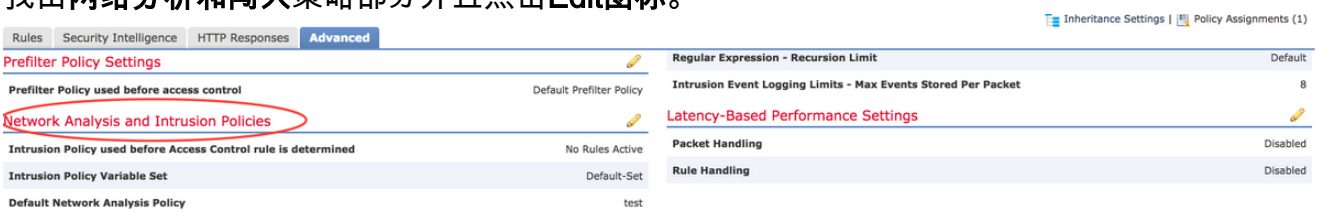
4. 扩展**设置**选项并且选择**TCP流配置**。
5. 连接对配置部分并且更改如期望的一样**超时的**值。



6. 连接到**策略>访问控制>访问控制**。
7. 选择选项**编辑**编辑策略适用于相关可管理的设备或创建一个新的策略。



8. 选择在访问策略的**高级选项卡**。
9. 找出**网络分析和闯入**策略部分并且点击**Edit图标**。



10. 从**默认网络分析策略**下拉菜单，请选择在创建的策略第2.步。
11. 点击OK键并且**保存**更改。
12. 点击**Deploy**选项配置修正到相关manged设备。

警告：增加超时预计引起高端内存利用率， Firepower必须跟踪没有由最长时间的终端结束的流。在存储器利用率的实际增量为每个唯一网络是不同的，因为取决于网络应用程序多久保持TCP连接空闲。

结论

TCP连接空闲超时的每网络的基准是不同的。它完全地取决于是在使用中的应用程序。必须通过观察设立一个最佳值网络应用程序多久保持TCP连接空闲。对于适合于到在Cisco ASA的Firepower服务模块的问题，当一个最佳值不可能推导时，超时可以通过增加它调整ASA的超时值的步骤。

Related Information

- ASA Cisco Firepower威胁防御快速入门指南
- Technical Support & Documentation - Cisco Systems
- ASA Firepower快速入门指南