

FirePOWER管理中心显示在错误方向的一些TCP连接事件

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景](#)

[解决方案](#)

[结论](#)

[相关信息](#)

简介

本文描述原因和缓解步骤FirePOWER管理的显示TCP连接事件在发起者IP是TCP连接的服务器IP的反向的Center(FMC)，并且响应方IP是TCP连接的客户端IP。

注意：有出现的多个原因的这样事件。本文解释此症状的多数常见原因。

[先决条件](#)

[要求](#)

Cisco 建议您了解以下主题：

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

使用的组件

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

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开始与一清楚(默认

)配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景

在TCP连接，**客户端**是指发送初始数据包的IP。FirePOWER管理中心生成连接事件，当受管理设备(传感器或FTD)时看到连接的最初的TCP数据包。

跟踪TCP连接的状态的设备有定义的空闲超时确保，没有由终端不正确关闭的连接不浪费可利用的内存在长时间时间。已建立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，在超时对待后一个新的TCP流和转发决策根据匹配此数据包的规则被采取。当数据包是从服务器时，服务器IP被记录，当此的发起者新的流。当记录为规则时启用，连接事件在FirePOWER管理中心生成。

注意：根据已配置的策略，来的数据包的转发决策，在超时是与最初的TCP数据包的后决策不同。如果已配置的默认操作是“块”，数据包丢弃。

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。按顺序更改超时，

1. 导航对**策略>访问控制>入侵**。
2. 导航对右上角并且选择**网络访问策略**。



3. 选择**创建策略**，选择名称并且点击**Create**并且**编辑策略**。请勿修改基本策略。

Create Network Analysis Policy



Policy Information

Name *

Description

Inline Mode

Base Policy Balanced Security and Connectivity ▾

* Required

Create Policy Create and Edit Policy Cancel

4. 展开设置选项并且选择TCP数据流配置。
5. 导航对配置部分并且更改值如期望的一样超时。

TCP Stream Configuration

Global Settings

Packet Type Performance Boost

Targets

Hosts default

Configuration

Network default (Single IP address or CIDR block)

Policy Windows (Win98, WinME, WinNT, Win2000, WinXP)

Timeout 180 seconds

Maximum TCP Window 0 bytes (0 to disable)

Overlap Limit 0 overlapping segments (maximum of 255 segments, 0 for unlimited)

Flush Factor 0 (Effective only if Normalize TCP is enabled, 0 to disable)

Stateful Inspection Anomalies

TCP Session Hijacking

Consecutive Small Segments

Small Segment Size bytes

Ports Ignoring Small Segments

Require TCP 3-Way Handshake

3-Way Handshake Timeout 0 seconds (0 means unlimited timeout)

Packet Size Performance Boost

6. 导航到策略>访问控制>访问控制。
7. 选择选项编辑编辑策略应用对相关受管理设备或创建一项新的策略。

Access Control > Access Control

Access Control

New Policy

8. 选择在访问策略的高级选项卡。
9. 找出网络分析和入侵策略部分并且点击Edit图标。

Advanced

Network Analysis and Intrusion Policies

Regular Expression - Recursion Limit

Intrusion Event Logging Limits - Max Events Stored Per Packet

Latency-Based Performance Settings

Packet Handling

Rule Handling

10. 从默认网络分析策略下拉菜单，请选择在步骤创建的策略2。
11. 点击OK键并且保存更改。
12. 点击Deploy选项部署修正到相关manged设备。

警告：增加超时预计引起更高的存储器利用率，FirePOWER必须跟踪没有由最长时间的终端关闭的流。在存储器利用率的实际增加为每唯一的网络是不同的，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不同的。它完全取决于是在使用中的应用程序。必须通过观察设立最佳值网络应用程序多久保持TCP连接空闲。对于适合于到在思科ASA的FirePOWER服务模块的问题，当最佳值不可能推导时，超时可以通过增加它调整在ASA的超时值的步骤。

相关信息

- [思科Firepower威胁ASA的防御快速入门指南](#)
- [技术支持和文档 - Cisco Systems](#)
- [ASA Firepower快速入门指南](#)