

FirePOWER管理中心显示某些TCP连接事件的方向错误

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

本文档介绍FirePOWER管理中心(FMC)在发起方IP是TCP连接的服务器IP，响应方IP是TCP连接的客户端IP的反向显示TCP连接事件的原因和缓解步骤。

注意：发生此类事件有多种原因。本文档解释了此症状的最常见原因。

先决条件

要求

Cisco 建议您了解以下主题：

- FirePOWER技术
- 自适应安全设备(ASA)的基本知识
- 对传输控制协议(TCP)定时机制的理解

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本6.0.1及更高版本的ASA Firepower威胁防御(5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)
- 运行的ASA Firepower威胁防御(5512-X、5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、FP9300、FP4100)软件版本6.0.1及更高版本
- 具备Firepower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及更高版本
- Firepower管理中心(FMC)6.0.0版及更高版本

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。本文档中使用的所有设备都以清除（默

认) 配置启动。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连接中，**客户端**是指发送初始数据包的IP。当受管设备（传感器或FTD）看到连接的初始TCP数据包时，FirePOWER管理中心会生成连接事件。

跟踪TCP连接状态的设备定义了空闲超时，**以确保终端错误关闭的连接不会消耗长时间的可用内存**。FirePOWER上已建立的TCP连接的默认空闲超时为**三分钟**。FirePOWER IPS传感器不跟踪空闲了三分钟或更久的TCP连接。

超时后的后续数据包被视为新TCP流，转发决策根据与此数据包匹配的规则执行。当数据包来自服务器时，服务器的IP记录为此新流的发起者。为规则启用日志记录时，FirePOWER管理中心上会生成连接事件。

注意：根据配置的策略，超时后数据包的转发决策与初始TCP数据包的转发决策不同。如果配置的默认操作为“阻止”，则丢弃数据包。

以下屏幕截图显示了此症状的示例：

	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

通过增加TCP连接的超时，可以**缓解**上述问题。要更改超时，

1. 导航至Policies > Access Control > Intrusion。
2. 导航至右上角，然后选择Network Access Policy。



3. 选择**创建策略**，选择名称，然后单击**创建和编辑策略**。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，然后选择“TCP流配置”。
5. 导航至配置部分，并根据需要更改超时值。

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. 导航至策略>访问控制>访问控制。
7. 选择“编辑”选项可编辑应用于相关受管设备的策略或创建新策略。

Access Control > Access Control

Access Control

New Policy

8. 在访问策略中选择高级选项卡。
9. 找到Network Analysis and Intrusion Policies部分，然后单击Edit图标。

Rules Security Intelligence HTTP Responses **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Default Network Analysis Policy的下拉菜单中，选择在步骤2中创建的策略。
11. 单击确定并保存更改。
12. 单击Deploy选项，将策略部署到相关受管设备。

警告：超时增加预期会导致内存利用率提高，FirePOWER必须跟踪终端在较长时间内未关闭的流。内存利用率的实际增加对于每个唯一网络来说都不同，因为它取决于网络应用程序使TCP连接保持空闲的时间。

结论

每个网络的TCP连接空闲超时基准都不同。它完全取决于正在使用的应用。必须通过观察网络应用程序使TCP连接保持空闲的时间来确定最佳值。对于与Cisco ASA上的FirePOWER服务模块相关的问题，当无法推断最佳值时，可以通过在ASA超时值之前的步骤中增加超时值来调整超时。

相关信息

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