排除CSF CLI上的流量问题

目录

简介

本文档介绍如何使用Cisco Secure Firewall CLI验证路由、数据包流和Snort行为，从而解决流量问题。

先决条件

本文档没有任何特定的要求。

要求

Cisco 建议您了解以下主题：

- Firepower管理中心(FMC)策略和对象配置
- 思科安全防火墙(CSF)路由和接口逻辑
- 数据包检测和防火墙故障排除概念

使用的组件

本文档不限于CSF的特定软件和硬件版本。文档中使用的设备运行代码7.6.5。

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最初均采用原始（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。

相关产品

本文档还可与以下硬件和软件版本一起使用：

- Secure Firewall Management Center (FMC)
- 思科安全防火墙(CSF)
- Firepower威胁防御CLI工具

重要信息

当设备的CPU、内存或I/O使用率提高时，执行故障排除命令会加剧性能降级。建议首先调查并解决资源耗尽情况，然后进行流量问题诊断。诊断命令会消耗额外的系统资源，这会进一步降低可用性并延长恢复时间。

背景信息

CSF上的流量故障排除通常首先确认数据包必须通过防火墙的逻辑路径。一旦了解路由和接口映射，下一步是将预期路径与实际数据包流进行比较。这可以通过路由查找、packet-tracer模拟、数据包捕获和Snort引擎跟踪来执行。

每种工具都提供不同层次的可视性：

- show route确认数据包的路由路径和接口标识。
- packet-tracer模拟流量并确定ACL、NAT和接口决策。
- 数据包捕获会检查通过防火墙的实时流量。
- 系统支持跟踪公开了对策略相关块或检查事件的Snort决策。

提示：在捕获流量之前先进行路由和Packet Tracer验证，这样您就可以在分析实时流量之前确认预期的路径和访问控制决策是否正确。

问题

流量未按预期运行，管理员需要确定数据包是否采用正确的路径、防火墙是否允许或拒绝连接，以及Snort或策略检测是否阻止流量。

步骤 1：查找路由

确定路由路径并确定与源IP地址和目的IP地址关联的逻辑接口名称。大多数故障排除命令都需要逻辑接口名称，因此这必须是故障排除工作流程的第一步。

对源IP地址和目标IP地址运行命令：

```
show route <IP>
```

依赖默认路由的互联网流量需要标识逻辑出口接口。可通过执行以下步骤来确定逻辑接口名称：

```
show route 0.0.0.0
```

示例输出：

```
FTD1# show route 192.168.0.11

Routing entry for 192.168.0.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

    directly connected, via Inside
    Route metric is 0, traffic share count is 1
```

```
FTD1# show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

    128.107.0.1, via Outside
    Route metric is 0, traffic share count is 1
```

在本示例中，逻辑入口接口为Inside，出口接口为Outside。

警告：网络地址转换(NAT)可以重定向通过不同接口的流量，而不是路由表指示NAT策略何时与流量匹配。排除连接故障时，请验证NAT配置是否与预期流量路径一致。

提示：逻辑接口名称用于CLI故障排除命令。请注意逻辑名称以供将来参考。

步骤 2：运行Packet Tracer

使用packet-tracer模拟防火墙如何评估特定流量。此工具可帮助确认使用哪些接口、是否应用了NAT策略，以及ACL是允许还是拒绝流量。

使用以下命令语法：

```
packet-tracer input <source interface> <protocol> <source IP> <source port> <destination IP> <destinati
```

命令示例：

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443
```

查看输出，确认数据包遵循预期路径并在模拟过程中被允许。当您在参与实时数据包分析之前需要确定问题是否与路由、NAT或策略匹配有关时，此功能非常有用。

packet Tracer中的transmit关键字导致模拟数据包被注入入口接口，使其能穿越所有防火墙处理阶段，而不是作为模拟保留。

命令示例：

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443 transmit
```

步骤 3：运行捕获

使用数据包捕获检测通过防火墙的实时流量。数据包捕获与Packet Tracer不同，因为它们捕获实际流量，因此必须与捕获处于活动状态时通过防火墙的实际流量匹配。数据包捕获是双向的，记录连接的两端。

对于大多数流量故障排除场景，请配置以下捕获：

- 入口捕获 — 捕获到达源端接口的流量
- 出口捕获 — 捕获离开目标端接口的流量
- ASP Drop Capture — 捕获防火墙丢弃的数据包并匹配配置的标准

通用捕获语法：

```
capture <name> interface <interface name> trace match ip host <source IP> host <destination IP>
```

入口捕获示例：

```
FTD1# capture in interface trace Inside match ip host 192.168.0.11 host 72.163.4.161
```

出口捕获示例：

```
FTD1# capture out interface trace Outside match ip host 128.107.0.22 host 72.163.4.161
```

ASP丢弃捕获示例：

```
FTD1# cap asp type asp-drop match ip host 192.168.0.11 host 72.163.4.161
```

数据包捕获是双向的，这意味着可以根据定义的匹配条件捕获转发和返回流量。跟踪功能可直观显示防火墙对实际流量做出的决策。

⚠ 警告：如果正在执行NAT，则出口捕获必须使用转换后的源IP而不是原始源IP来正确捕获NAT后的流量。

步骤 4：运行系统支持跟踪

使用系统支持跟踪查看特定流量的实时Snort检测流程。当流量匹配ACL允许规则但仍被策略检测阻止时，此功能尤其有用。标准数据包捕获显示数据包被阻止，但系统支持跟踪可以让您了解为什么以这种方式处理数据包。系统支持跟踪是双向的，这意味着它接收来自两端的流量。这意味着IP添加到工具中的顺序并不重要。

运行此命令并响应提示：

```
> system support trace


Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 72.163.4.161
Please specify a server port: 443
```

当环境使用应用或URL规则、基于身份的规则、文件策略或入侵策略时，此工具特别有用。这些功能在ACL匹配后进行评估，因此访问控制策略可以允许数据包，但仍会被Snort检测阻止。

注意：如果确切的源端口未知，客户端端口可以留空。

验证

同时使用路由查找、Packet Tracer模拟、数据包捕获和系统支持跟踪的输出确认流量行为。目标是确定数据包是否采用正确的路径、防火墙是否允许或拒绝该数据包，以及Snort是否基于更深入的检查阻止该数据包。

完整的故障排除流程通常会确认：

- 路由查找显示逻辑入口和出口接口。
- Packet Tracer确认预期的转发路径和策略评估。
- 数据包捕获可确认流量是否按预期到达和离开。
- 系统支持跟踪可确认Snort或策略检查是否导致阻止。

故障排除

当流量问题持续存在时，请查看以下区域：

- 检查路由查找是否与预期的源接口和目标接口匹配。
- 验证Packet Tracer输出是否显示流量在ACL或NAT阶段被拒绝。
- 检查入口和出口数据包捕获，确认流量到达防火墙并留在正确的接口上。
- 使用ASP丢弃捕获确认防火墙是否在内部丢弃流量。
- 在ACL允许决策之后，使用系统支持跟踪确定Snort是否阻止了流量。

相关信息

- 分析Firepower防火墙捕获以排除网络故障
- 使用Firepower威胁防御捕获和Packet Tracer

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）。