排除ICMP数据包消息"；不可达故障 — admin prohibited filter"

目录

问题

本文档介绍附加到Internet控制消息协议(ICMP)数据包“不可达 — 管理员禁止过滤器”的数据包信息。

安全防火墙威胁防御(FTD)捕获示例：

```
<#root>
device#

show capture CAPO



106 packets captured

   1: 08:12:45.864243       198.51.100.205.7351 > 192.0.2.2.47668:  udp 111
   2: 08:12:46.400812       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   3: 08:12:46.406320       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

unreachable - admin prohibited filter



   4: 08:12:47.936856       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   5: 08:12:47.943936       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

 unreachable - admin prohibited filter



   6: 08:12:49.216739       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   7: 08:12:49.222278       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

 unreachable - admin prohibited filter



   8: 08:12:50.096079       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   9: 08:12:50.106363       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2
```

unreachable - admin prohibited filter

环境

在以下任何产品中都可见：

- FTD
- 自适应安全设备 (ASA)

分辨率

了解ICMP类型3，代码13消息

ICMP“unreachable - admin prohibited filter”消息对应于ICMP类型3的代码13(Destination Unreachable - Communication Administratively Prohibited)。 这些消息表明流量已被安全策略或访问控制列表(ACL)明确拒绝，而不是由于网络连接问题而无法访问。

分析数据包捕获信息

步骤1.确定ICMP拒绝消息的来源

查看数据包捕获，确定哪些设备正在生成ICMP类型3、代码13响应。在本例中，拒绝消息源自特定IP地址(192.0.2.2)。

步骤2.检查原始数据包报头

ICMP拒绝消息包含有关被阻止的原始数据包的信息。这包括触发管理禁用的原始源IP地址和目的IP地址、协议信息和端口号。

步骤3.将拒绝消息与流量模式关联

将ICMP响应与被拒绝的特定流量进行匹配。例如，IP地址为192.0.2.2的设备在CAPO捕获中拒绝了到端口7351的UDP流量。

数据包捕获分析限制

使用文本导出的数据包捕获时，与二进制pcap文件相比，详细的数据包分析可能会受到限制。为了进行全面的分析，二进制数据包捕获文件（pcap格式）提供了更完整的信息，包括：

- 完整的数据包报头和负载信息
- 精确的计时信息
- 完整的协议解码功能
- 增强的过滤和分析选项

原因

根本原因通常为以下其中一项：

- 配置为拒绝特定流量的ACL

- 防火墙规则阻止某些协议、端口或IP地址

在本示例中，该消息是由下游ACL导致的。

相关内容

- https://datatracker.ietf.org/doc/html/rfc792
- https://datatracker.ietf.org/doc/html/rfc1812
- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html

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）。