Understand ICMP Packet Messages "unreachable - admin prohibited filter"

Contents

Issue

Understand the packet information attached to the Internet Control Message Protocol (ICMP) packets "unreachable - admin prohibited filter".

Cisco Secure Firewall Threat Defense (FTD) capture example:

<#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
```

Environment

It can be seen in any of these products:

- FTD
- Adaptive Security Appliance (ASA)

Resolution

Understanding ICMP Type 3, Code 13 Messages

ICMP "unreachable - admin prohibited filter" messages correspond to ICMP Type 3, Code 13 (Destination Unreachable - Communication Administratively Prohibited). These messages indicate that traffic has been explicitly denied by a security policy or access control list (ACL) rather than being unreachable due to network connectivity issues.

Analyzing Packet Capture Information

Step 1. Identify the source of ICMP deny messages

Review the packet capture to identify which devices are generating the ICMP Type 3, Code 13 responses. In this case, the deny messages originated from specific IP addresses (192.0.2.2).

Step 2. Examine the original packet headers

The ICMP deny messages contain information about the original packets that were blocked. This includes the original source and destination IP addresses, protocol information, and port numbers that triggered the administrative prohibition.

Step 3. Correlate deny messages with traffic patterns

Match the ICMP responses to the specific traffic flows being denied. For example, UDP traffic to port 7351 was being rejected by the device with IP address 192.0.2.2 in the CAPO capture.

Packet Capture Analysis Limitations

When working with text-exported packet captures, detailed packet-by-packet analysis can be limited compared to binary pcap files. For comprehensive analysis, binary packet capture files (pcap format) provide more complete information including:

- Full packet headers and payload information
- Precise timing information
- Complete protocol decode capabilities
- Enhanced filtering and analysis options

Cause

The root cause is typically one of these:

- ACLs configured to deny specific traffic flows
- Firewall rules blocking certain protocols, ports, or IP addresses

In this example, the message was caused by a downstream ACL.

Related Content

- 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