瞭解ICMP資料包消息"；無法訪問 — 管理禁止的過濾器"

目錄

問題

瞭解附加到網際網路控制訊息通訊協定(ICMP)封包的封包資訊「無法連線 — 管理禁止過濾器」。

思科安全防火牆威脅防禦(FTD)擷取範例：

<#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
```

環境

以下任何產品均可看到這種情況：

- FTD
- Adaptive Security Appliance (ASA)

解析

瞭解ICMP型別3，代碼13訊息

ICMP「無法到達 — 管理禁止過濾器」消息對應於ICMP型別3代碼13（目的地無法到達 — 通訊管理性禁止）。 這些訊息表示流量已遭安全原則或存取控制清單(ACL)明確拒絕，而不是因為網路連線問題而無法連線。

分析資料包捕獲資訊

步驟1.識別ICMP拒絕消息的來源

檢視資料包捕獲，確定哪些裝置正在生成ICMP第3類、第13類響應。在本例中，deny消息源自特定IP地址(192.0.2.2)。

步驟2.檢查原始封包標頭

ICMP deny消息包含有關被阻止的原始資料包的資訊。這包括觸發管理禁止的原始源和目標IP地址、協定資訊和埠號。

步驟3.將拒絕消息與流量模式關聯

將ICMP響應與被拒絕的特定流量進行匹配。例如，CAPO捕獲中IP地址為192.0.2.2的裝置拒絕了到埠7351的UDP流量。

資料包捕獲分析限制

使用文本匯出的資料包捕獲時，與二進位制pcap檔案相比，詳細的資料包分析可能會受到限制。為了進行全面的分析，二進位制資料包捕獲檔案（pcap格式）提供了更完整的資訊，包括：

- 完整的資料包報頭和負載資訊
- 精確的計時資訊
- 完整的協定解碼功能
- 增強的過濾和分析選項

原因

根本原因通常為以下其中一項：

- 配置為拒絕特定流量的ACL
- 防火牆規則阻止某些協定、埠或IP地址

在本範例中，訊息是由下游ACL引起的。

相關內容

- 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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。