ICMP 패킷 메시지 이해(") 도달 불가 - 관리자 금지 필터(")

목차

문제

ICMP(Internet Control Message Protocol) 패킷에 첨부된 패킷 정보 "연결 불가 - 관리자 금지 필터 "를 이해합니다.

Cisco FTD(Secure Firewall Threat Defense) 캡처 예:

```
<#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

환경

다음 제품에서 확인할 수 있습니다.

- FTD
- ASA(Adaptive Security Appliance)

해결

ICMP 유형 3, 코드 13 메시지 이해

ICMP "unreachable - admin prohibited filter" 메시지는 ICMP 유형 3, 코드 13(Destination Unreachable - Communication Administrative Prohibited)에 해당합니다. 이러한 메시지는 트래픽이 네트워크 연결 문제로 인해 도달할 수 없는 것이 아니라 보안 정책 또는 ACL(Access Control List)에 의해 명시적으로 거부되었음을 나타냅니다.

패킷 캡처 정보 분석

1단계. ICMP 거부 메시지의 소스 식별

패킷 캡처를 검토하여 어떤 디바이스에서 ICMP Type 3, Code 13 응답을 생성하는지 확인합니다. 이 경우 거부 메시지는 특정 IP 주소(192.0.2.2)에서 시작됩니다.

2단계. 원래 패킷 헤더를 검사합니다.

ICMP 거부 메시지는 차단된 원래 패킷에 대한 정보를 포함합니다. 여기에는 관리 금지를 트리거한 원래 소스 및 목적지 IP 주소, 프로토콜 정보, 포트 번호가 포함됩니다.

3단계. 거부 메시지와 트래픽 패턴의 상관성 분석

거부되는 특정 트래픽 흐름에 ICMP 응답을 일치시킵니다. 예를 들어, CAPO 캡처에서 IP 주소가 192.0.2.2인 디바이스에서 포트 7351에 대한 UDP 트래픽을 거부했습니다.

패킷 캡처 분석 제한 사항

텍스트 내보내기 패킷 캡처 작업을 할 때 패킷별 상세 분석을 이진 pcap 파일에 비해 제한할 수 있습니다. 종합적인 분석을 위해 이진 패킷 캡처 파일(pcap 형식)은 다음을 포함한 더욱 완벽한 정보를 제공합니다.

- 전체 패킷 헤더 및 페이로드 정보
- 정확한 타이밍 정보
- 완전한 프로토콜 디코딩 기능
- 향상된 필터링 및 분석 옵션

원인

근본 원인은 일반적으로 다음 중 하나입니다.

- 특정 트래픽 흐름을 거부하도록 구성된 ACL
- 특정 프로토콜, 포트 또는 IP 주소를 차단하는 방화벽 규칙

이 예에서는 다운스트림 ACL로 인해 메시지가 발생했습니다.

관련 콘텐츠

- 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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.