

보안 방화벽 FTD - 이전 VDB로 인해 전화 오디오 차단 목록 확대(&N)

목차

문제

사용자는 통화가 연결되지만 오디오가 없는 경우 전화 확대/축소(Zoom Phone) 통화에 오디오 문제가 발생합니다. FTD는 Zoom IP 범위에서 UDP 미디어 패킷을 삭제하고 있으며, 패킷 캡처 및 ASP 삭제 카운터에서 Snort에 의해 차단된 것으로 표시합니다.

구체적인 증상은 다음과 같습니다.

- 방화벽에서 Cisco VDB(Vulnerability Database) 버전 427 이상을 실행하고 있습니다.
- 방화벽에는 Firepower 데이터베이스에서 제공하는 기본 Zoom/RTP 애플리케이션 ID를 기반으로 Zoom 트래픽을 허용해야 하는 액세스 규칙이 포함되어 있습니다. appid.[cisco.com](https://www.cisco.com)에 따르면 규칙은 Zoom AppID를 통해 이러한 모든 포트를 허용해야 합니다.
 - 사용자 확대/축소(6243): 80,443/tcp
 - 확대/축소 다운로드(4628): 80,443/tcp
 - 확대/축소 업로드(4627): 80,443/tcp
 - 확대/축소 회의(4629): 80/tcp
 - RTP 오디오(2475): 5004/udp
 - SIP(426): 5060/udp
- 그러나 packet-tracer 출력은 트래픽이 차단 목록 이유 "방화벽 프리프로세서에 의해 차단되거나 차단 목록에 추가됨"에 의해 삭제됨을 보여줍니다.

<#root>

Phase: 17
Type: SNORT
Subtype: firewall

Result: DROP

Elapsed time: 345716 ns
Config:
Network 0, Inspection 0, Detection 4, Rule ID 268434438
Additional Information:
Starting rule matching, zone 3 -> 3, geo 840 -> 840, vlan 0, src sgt: 0, src sgt type: unknown, ds
Matched rule ids 268434438 - Block

Result:
input-interface: Outside(vrfid:0)
input-status: up
input-line-status: up
output-interface: Outside(vrfid:0)
output-status: up
output-line-status: up

Action: drop

Time Taken: 640578 ns

Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame

- 패킷 캡처는 다음과 같은 이유로 삭제를 표시합니다. "snort-blacklist".

<#root>

40: 22:52:36.383692 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA
141: 22:52:36.383723 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA
142: 22:52:36.385188 206.247.118.57.60030 > 10.X.X.1.9178: udp 44

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

- 시스템 지원 추적 출력에서 트래픽은 보류 중인 애플리케이션 식별로 인해 규칙 매칭 중에 지연됩니다. 그러나 트래픽이 잘못 식별되어 차단 목록에 표시됩니다. IP 주소는 Zoom 기사 [Zoom 네트워크 방화벽](#) 또는 [프록시 서버](#) 설정에 따라 액세스가 필요한 [Zoom](#) 공용 IP입니다.

<#root>

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

pending rule order 12, 'allow-outbound', AppID

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

Deferring trust until a rule is matched

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

match rule order 28, 'Default Block', action Block

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 MidRecovery data sent for rule id: 26843

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Matched a rule, stop deferring trust

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Generating an SOF event with rule_id = 2

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

deny action

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Deleting Firewall session flags=0x20, 1c

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Packet 17168248: UDP, 04/14-14:44:53.110

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Firewall: starting rule matching, zone 1

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Firewall: block rule, 'Default Block', force_block

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

AppID: service: (-1), client: (0), payload: (0), misc: (0)

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Stream: pending block, drop

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Policies: Network 0, Inspection 0, Detect

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Verdict: blacklist

- 시스템 지원 추적은 Zoom IP가 응답을 시도할 때 "RTP 클라이언트 후보가 오류-무효(-11)"를 반환했으며 "서드파티에서 알 수 없는(0)" 메시지를 반환했습니다."

<#root>

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1 New AppId session

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

3rd party returned unknown (0)

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

RTP client candidate returned error-invalid (-11)

10.X.X.1 9824 -> 206.247.118.55 54808 17 AS=0 ID=2 GR=1-1 app event changes: created

- FTD show asp drop 명령은 차단 목록 삭제를 빠르게 증가시킵니다.

<#root>

Frame drop:

-----ABBREVIATED-----

Blocked or blacklisted by the firewall preprocessor (firewall)	11224
Blocked or blacklisted by the stream preprocessor (stream)	2354
Fragment reassembly failed (fragment-reassembly-failed)	3
Packet is blacklisted by snort (snort-blacklist)	27173
Packet is blocked as requested by snort (snort-block)	42

환경

- Cisco Firepower FTD 버전 7.7.11(FMC에서 관리)
- VDB(취약성 데이터베이스) 버전 427 이상
- Snort 버전 3.3.5.1100-66
- 주로 Zoom IP 서브넷 170.114.0.0/16 및 206.247.0.0/16에 영향을 미치는 트래픽이지만 다른 Zoom IP를 포함할 수 있습니다.

해결

Cisco 버그 ID CSCwu22106 해결 방법 - 사전 필터 규칙 구현

1: Zoom 트래픽에 대한 프리필터 규칙을 생성합니다.

Policies(정책) > Access Control(액세스 제어) > Prefilter(사전 필터)로 이동하고 이 컨피그레이션으로 새 규칙을 생성합니다.

- 규칙 이름: 확대/축소 사전 필터
- 작업: 빠른 경로

- 소스 영역: 입력 인터페이스
- 대상 영역: 출력 인터페이스
- Source address: 모두
- 소스 포트: 모두
- 대상 주소: IP 범위 확대/축소(170.114.0.0/16, 206.247.0.0/16) 및 [네트워크 방화벽 확대/축소 또는 프록시 서버 설정에](#) 명시된 기타 [항목](#).
- 대상 포트: UDP 10000-64000

2: 대체 액세스 제어 규칙 컨피그레이션

사전 필터링을 선호하지 않는 경우, Zoom 애플리케이션 식별자를 제거하고 명시적 IP 및 포트 일치 를 사용하여 기존 액세스 제어 정책 규칙을 수정합니다.

- 규칙 이름: 확대/축소 허용
- 작업: 허용
- 소스 영역: 입력 인터페이스
- 대상 영역: 출력 인터페이스
- Source address: 모두
- 소스 포트: 모두
- 대상 주소: IP 범위 확대/축소(170.114.0.0/16, 206.247.0.0/16) 및 [네트워크 방화벽 확대/축소 또는 프록시 서버 설정에](#) 명시된 기타 [항목](#).
- 대상 포트: UDP / "Zoom-Phone-Ports"(범위 10000 64000)
- 로깅: (선택 사항, 허용된 트래픽 모니터링)

3: FTD 디바이스에 컨피그레이션 변경 사항을 구축하고 양방향 오디오 기능이 복원되었는지 확인 합니다.

- ASP 삭제 카운터를 모니터링하여 차단 목록이 중지되었는지 확인합니다.

```
device# show asp drop
```

- 패킷 캡처를 검사하여 성공적인 양방향 트래픽을 확인합니다.

```
device# show capture
```

4: 결함 Cisco 버그 ID CSCwu22106이 Cisco VDB(Vulnerability Database) 버전 428 릴리스에서 해결되었습니다. 이 결함의 영향을 방지하려면 Firepower 디바이스에서 최신 VDB 버전을 실행해야 합니다. 마찬가지로 VDB 버전 395에서 관련 결함 Cisco 버그 ID CSCwn80786이 해결되었습니다.

원인

VDB(Vulnerability Database) 버전 427에서 Cisco Secure Firewall 애플리케이션 ID 시그니처가 실패하면 Zoom Phone 미디어 트래픽이 잘못 분류되어 Snort 검사 엔진에 의해 차단됩니다. 이 동작은 Cisco 버그 ID CSCwu22106 및 관련 결함 Cisco 버그 ID CSCwn80786에 따라 추적됩니다. 이는 애플리케이션 ID가 사용될 때 Zoom IP 주소 및 미디어 흐름을 잘못 처리한 것을 나타냅니다.

관련 콘텐츠

- [네트워크 방화벽 또는 프록시 서버 설정 확대/축소](#)
- [빠른 경로 사전 필터링을 위한 모범 사례](#)
- [Cisco 버그 ID CSCwu22106 - VDB 427에서 잘못 처리된 IP 주소 확대/축소](#)
- [Cisco 버그 ID CSCwn80786 - Zoom 애플리케이션 탐지기가 Zoom Phone에 대한 네트워크를 탐지하지 못함](#)
- [Cisco 기술 지원 및 다운로드](#)

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.