레이어 7 검사가 멀티레이어 트래픽에 미치는 영향: Snort3 구현 검토

목차

문제

ACP(Access Control Policy)에서 DNS 싱크홀 규칙을 활성화한 후 캡슐화된 VXLAN 트래픽이 Snort 3 엔진 버전을 실행하는 FTD(Firepower Threat Defense) 디바이스에서 예기치 않게 삭제되기 시작했습니다.

· DNS 싱크홀 정책을 활성화한 후 VXLAN 캡슐화된 트래픽이 삭제됩니다.

· 외부 VXLAN 헤더 대신 내부 IP 주소(예: 100.70.x.x)를 표시하는 연결 이벤트

· 랩 테스트 중 Snort 3 구현에서 예기치 않은 동작이 발견되었습니다.

환경

•플랫폼: FTD HA(High Availability) 쌍

· 영향 받는 버전: 7.6.2.1(Snort 3)

· 고정 버전: 7.6.4+(Snort 3)

해결

7.6.2.1의 솔루션:

############

1단계:

사전 필터 정책(권장)

VXLAN 트래픽에 대한 Snort 검사를 우회하도록 프리필터 규칙을 생성합니다.

· 사전 필터 정책

•작업: Fastpath(터널 규칙)

· 출처: <외부_VXLAN_소스_IP>

•대상: <외부_VXLAN_대상_IP>

•프로토콜: UDP

•포트: 4789

2단계:

기존 연결 지우기

· clear conn address <outer_ip_1> address <outer_ip_2>

사전 필터 정책을 사용하지 않는 경우 규칙 순서 조정

ACP에서 L7 규칙(DNS 싱크홀, App-ID)을 내부 IP 허용 규칙 앞에 둡니다.

장기적인 솔루션:

############

1. FTD 7.6.4 이상으로 업그레이드

· CSCwo54753(PSIRT 결함) 해결

· 일관된 멀티 레이어 검사 동작을 제공합니다.

2. DNS 싱크홀에 대한 내부 및 외부 규칙을 모두 구성합니다.

· 캡슐화된 트래픽에서 DNS 싱크홀 또는 기타 보안 인텔리전스 기능을 사용하는 경우

3. 비SI Layer 7 기능(URL 필터링, App Control)의 경우:

· ACP에는 내부 헤더 규칙만 필요합니다.

· 외부 헤더 규칙은 필요하지 않습니다.

멀티레이어 VXLAN 검사 기능에 대한 자세한 정보

##

FTD에는 SI(Security Intelligence) 및 레이어 7 기능을 위한 멀티 레이어 검사 기능이 포함되어 있습니다. 이 기능은 구성된 레이어 7 정책을 기반으로 Snort가 외부 캡슐화 헤더 또는 내부 페이로드 헤더를 검사할지 여부를 결정합니다.

레이어 7 기능은 다음과 같습니다.

· DNS 싱크홀

· 애플리케이션 컨트롤(App-ID)

•URL 필터링

· 지오로케이션

· 침입 방지

주요 동작:

#########

ACP에서 레이어 7 기능이 활성화된 경우 Snort는 캡슐화된 패킷의 가장 안쪽의 헤더(예: VXLAN,

GRE, IP-in-IP)를 검사하는 것으로 이동합니다.

기술 분석:
############
Snort 3(7.6.2.1) - 결함 동작

레이어 7 규칙 제외:

· Snort는 Lina(ASA datapath 엔진)의 연결 메타데이터를 사용합니다.

· 트래픽은 외부 헤더 규칙에 따라서만 허용되거나 거부됩니다.

· 내부 헤더 검사는 수행되지 않습니다.

레이어 7 규칙 사용:

· Snort는 ACP 검사를 수행하고 멀티레이어 검사를 시행합니다.

· 규칙 명령 사항(Snort 3의 결함)

· Inner IP 규칙이 L7 규칙 → Vxlan 트래픽 드롭 —> 결함 동작 앞에 나타나는 경우

LAB 출력:
LAB FTD — 7.6.2.1 — snort3 — Inner IP ACP 규칙 및 L7 규칙 — 삭제

랩 패킷 추적기 세부 정보:

17:46:48.773778 10.142.133.15:36066 > 10.126.133.15:4789 udp 80

내부(vrfid:0)

개체_그룹_검색

NGIPS 모드

| ngips 모드

액세스 목록

NGIPS 이그레스 인터페이스 조회

| 이그레스 인터페이스 확인

플로우 생성

외부 검사

SNORT

유형:

SNORT

결과:

삭제

설정:

경과 시간:

814472 ns

추가 정보

결과: 삭제

입력 인터페이스:

내부(vrfid:0)

입력 상태:

위로

입력 라인 상태:

위로

출력 인터페이스:

외부(vrfid:0)

출력 상태:

위로

출력 라인 상태:

위로

작업:

삭제

소요 시간:

928908 ns

삭제 사유:

(방화벽) 방화벽 프리프로세서에 의해 차단됨 <— DROP REASON

삭제 세부 정보:

저장 위치: frame inspect_dp_snort_snp_drop_frame_wcaller:58 flow (NA)/NA

외부(vrfid:0)

· L7 규칙이 Inner IP 규칙 앞에 나타나며 Vxlan 트래픽→ 허용되는 경우

DNS 싱크홀 특정 동작(Snort 3):

· DNS 싱크홀은 규칙 순서에 따라 트래픽이 허용되는 경우에도 멀티레이어 검사를 트리거합니다.

Snort 3(7.6.4+) - 고정 동작

사후 수정(CSCwo54753):

· 멀티레이어 검사는 L7 기능이 있을 때 일관성 있게 활성화됩니다.

· 규칙 순서는 동작에 영향을 미치지 않습니다.

· 트래픽 검사는 규칙 위치와 상관없이 가장 안쪽 헤더를 기반으로 합니다.

· DNS 싱크홀 시나리오의 경우 ACP에서 내부 및 외부 헤더를 모두 허용해야 합니다.

테스트 사례 비교 표

테스트 시나리오	FTD 7.6.2.1(Snort 3)	FTD 7.6.4+(Snort 3)	예상 동작
L7 규칙 뒤에 Inner IP 규칙	허용됨	허용됨	허용된 트래픽
내부 IP 규칙이 L7 규칙을 따름	삭제(결함)	허용됨	허용된 트래픽
내부 IP 규칙만(L7 없음)	차단됨	차단됨	차단됨(내부 허가 없음)
외부 IP 규칙만(L7 없음)	허용됨	차단됨	Snort 3은 가장 안쪽 헤더를 검사합니다.
외부 IP + DNS 싱크홀만	차단됨	차단됨	L7 규칙은 내부 검사를 시행합니다.
내부 IP + DNS 싱크홀만	차단됨	차단됨	L7 규칙은 내부 검사를 시행합니다.

원인

이러한 동작은 Snort 3의 보안 인텔리전스 기능을 위한 멀티 레이어 검사 기능 때문에 발생합니다. DNS 싱크홀(Security Intelligence의 일부)이 활성화되면 Snort 3은 전송 계층에 관계없이 캡슐화된 패킷 내에서 가장 안쪽 IP 주소를 탐지하고 평가하는 심층 패킷 검사를 수행합니다.

이 문제는 Cisco 버그 ID CSCwt12564에 문서화되어 있습니다. "규칙에서 L7 조건(url 필터링, app-id, 지오로케이션 등)을 사용하거나 ACP의 보안 인텔리전스 기능을 사용하는 경우 매칭할 규칙에 대한 내부 헤더가 포함된 ACP 규칙이 필요합니다. SI의 DNS 정책에 속하는 dns 싱크홀을 사용하는 경우, 규칙을 매칭하려면 ACP에서 내부 및 외부 헤더가 모두 필요합니다."

이 동작은 레이어 7 또는 보안 인텔리전스 기능이 구성되지 않은 경우 전송 VXLAN 트래픽에 대해 외부 헤더만 평가되는 일반 작업과 다릅니다.

관련 콘텐츠

- Snort 3 컨피그레이션 가이드
- Cisco 기술 지원 및 다운로드
- Cisco 버그 ID CSCwt12564
- Cisco 버그 ID CSCwt07320
- Cisco 버그 ID CSCwu75396
- Cisco 버그 ID CSCwt58320

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.