"향상된 애플리케이션 및 URL 탐지" 시 FTD 패킷 삭제(tcp-not-syn) 문제 해결 비대칭 트래픽 흐름의 인라인 인터페이스에서 활성화됨

목차

문제

인라인 인터페이스 세트로 구성된 FTD(Firewall Threat Defense) 어플라이언스는 ASP(Accelerated Security Path) 삭제 사유 tcp-not-syn을 사용하여 TCP 반환 트래픽을 삭제합니다. 이는 TLS TSID(Server Identity Discovery) 기능, 특히 "향상된 애플리케이션 및 URL 탐지" 옵션이 활성화된 직후에 발생합니다. 이전 FMC(Firewall Management Center) 버전에서는 이 옵션을 "Early application detection and URL categorization"이라고 합니다. 원래 SYN을 전달한 동일한 FTD 디바이스에서 반환 경로의 TCP SYN-ACK 패킷을 삭제하므로 TCP 세션이 설정되지 않습니다.

이 문제는 광범위한 TCP 연결 실패로 나타나며 TLS 트래픽에만 국한되지 않습니다. 이 기능을 활성화하면 다음과 같은 증상이 나타납니다.

- 반환 경로의 TCP SYN-ACK 패킷은 ASP 삭제 사유 tcp-not-syn과 함께 삭제됩니다.
- 새 TCP 세션은 FTD 연결 테이블에 나타나지 않습니다.
- 기능이 활성화된 후 약 10분 후에 캡처된 이 출력에서 보여주는 것처럼 높은 ASP 삭제 카운터가 빠르게 누적됩니다.

<#root>

device#

show asp drop

```
Frame drop:
 Flow is denied by configured rule (acl-drop)                                  1

 First TCP packet not SYN (tcp-not-syn)                                    34802

 TCP RST/FIN out of order (tcp-rstfin-ooo)                                     4
```

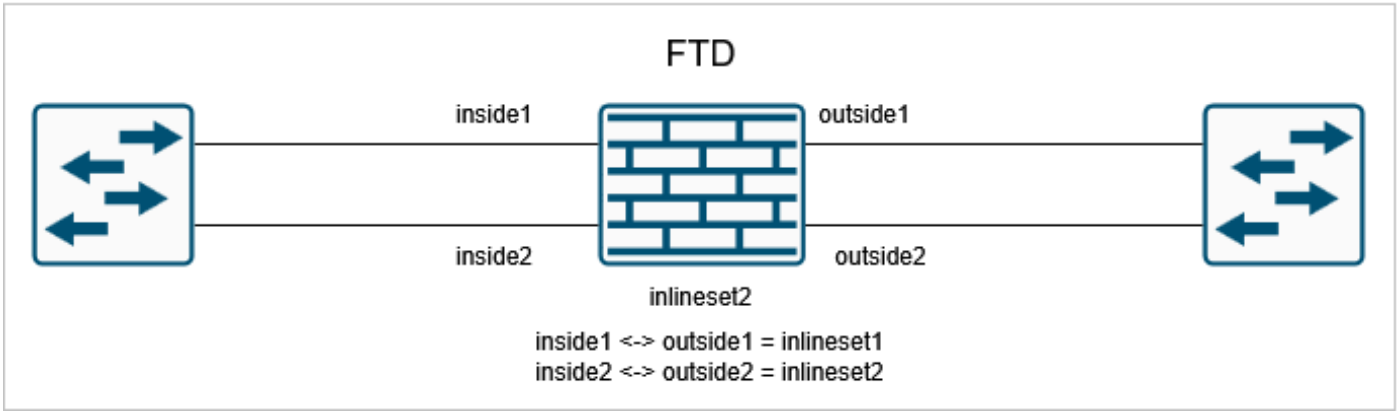
```
 Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                              995
 Dropped pending packets in a closed socket (np-socket-closed)                3
 TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)                1
 TCP Proxy probe receive drop (tcp-proxy-probe-tcp-probe-drop)                1
 Blocked or blacklisted by the reputation preprocessor (reputation)           1

Last clearing: 16:50:21 CEST Oct 24 2026 by enable_1
```

환경

- 플랫폼: Cisco Firepower 4115. 다른 플랫폼도 영향을 받을 수 있습니다.
- FTD 소프트웨어 버전: 7.6.4. 다른 소프트웨어 버전도 영향을 받을 수 있습니다.
- FMC 소프트웨어 버전: 10.1.0. 다른 소프트웨어 버전도 영향을 받을 수 있습니다.
- 인라인 인터페이스 집합이 있는 FTD.
- FTD에는 2개 이상의 인라인 인터페이스 쌍이 있습니다. inlineset1 및 inlineset2(또는 각각 하나의 인라인 집합이 있는 두 개의 서로 다른 FTD가 있음)
- 환경에 존재하는 비대칭 트래픽 흐름: TCP SYN은 outside1 인터페이스를 통해 이그레스(egress)되는 반면 해당 TCP SYN-ACK는 동일한 FTD 디바이스의 outside2 인터페이스를 통해 반환됩니다.
- TSID 기능이 FTD에서 활성화되어 있습니다.

토폴로지



해결

인라인 FTD 인터페이스를 통해 tcp-not-syn 삭제를 중지하고 TCP 연결을 복원하려면 TSID 내에서 "Enhanced application and URL Detection(애플리케이션 및 URL 탐지 향상)" 옵션을 비활성화하는 것이 좋습니다. 이렇게 하면 TCP 상태 우회가 인라인 인터페이스 세트에서 활성 상태를 유지할 수 있습니다. 이는 환경에서 비대칭 트래픽 흐름을 수용하는 데 필요합니다.

FMC에서 "Enhanced application and URL Detection(향상된 애플리케이션 및 URL 탐지)" 비활성화

다음으로 이동합니다. Policies(정책) > Access Control(액세스 제어) > [Your Access Control Policy(액세스 제어 정책)] > Advanced(고급) > TLS Server Identity Discovery(TLS 서버 ID 검색). "Enhanced application and URL Detection(애플리케이션 및 URL 탐지 향상)" 확인란의 선택을 취소하거나 비활성화한 다음 영향을 받는 FTD 디바이스에 정책을 구축합니다.

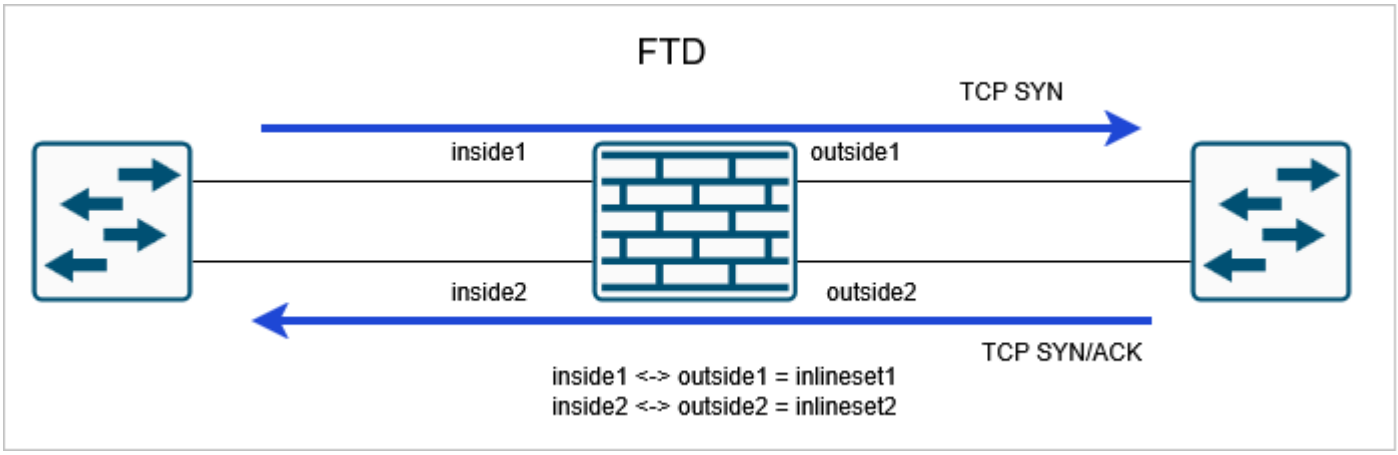
이 기능을 비활성화하면 새 세션이 연결 테이블에 나타나 TCP 연결이 3방향 핸드셰이크를 성공적으로 완료하고 있음을 확인합니다.

참고: TSID가 비활성화된 경우 FTD는 더 이상 TLS 1.3 세션에서 서버 인증서를 볼 수 없습니다. 애플리케이션 및 URL 규칙은 암호화된 트래픽에서 트래픽에 덜 정확하게 매칭합니다.

원인

tcp-not-syn 삭제의 근본 원인은 FTD의 인라인 인터페이스 집합에서 TLS 서버 ID 검색 기능과 TCP 상태 바이패스 간의 비호환성입니다.

기본적으로 FTD의 인라인 인터페이스를 통과하는 트래픽의 경우 TCP State Bypass가 활성화됩니다. TCP 상태 우회는 FTD가 엄격한 TCP 상태 추적을 적용하지 않고 비대칭 트래픽(TCP 연결의 전달 및 반환 경로가 서로 다른 인터페이스 또는 심지어 서로 다른 디바이스를 통과할 수 있음)을 전달하도록 설계되었습니다. 이는 라우팅 비대칭성이 있는 환경에서 필요한 동작입니다.

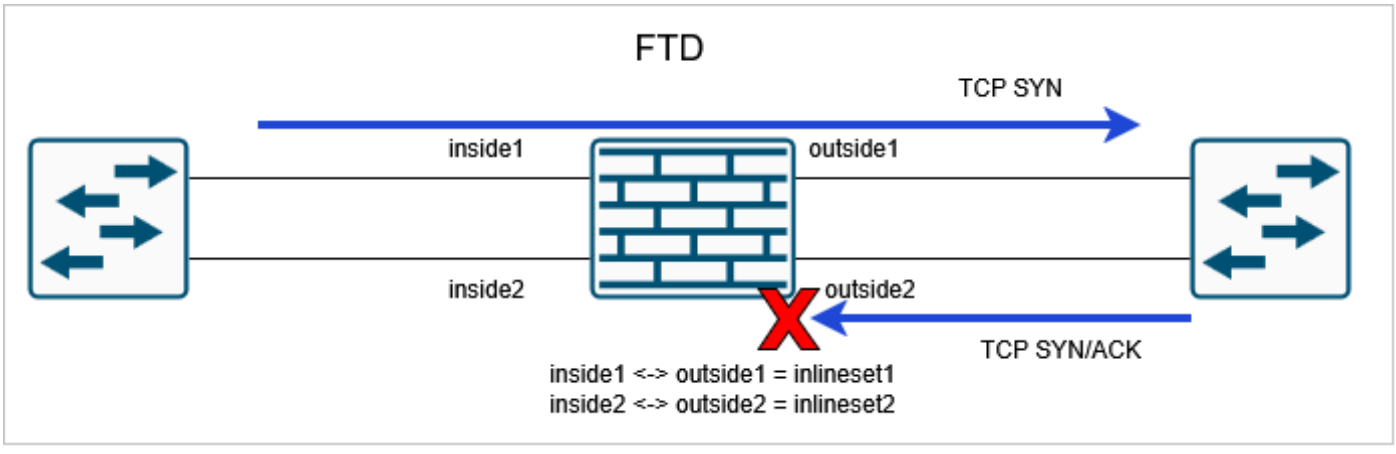


TSID가 비활성화된 경우 FTD 인라인 집합을 통한 비대칭 TCP 흐름

그러나 이러한 기능 중 하나가 활성화된 경우 FTD 시스템은 TCP 상태 우회를 재정의하고 인라인 인터페이스 트래픽에 대해 전체 TCP 상태 확인을 수행하기 시작합니다.

- TLS Server Identity Discovery(TLS 서버 ID 검색) 아래의 "Enhanced application and URL Detection(애플리케이션 및 URL 탐지 향상)" 옵션
- 모든 활성 TLS/SSL 암호 해독 정책.

TCP 상태 검사가 시행되면 FTD는 전체 TCP 핸드셰이크 시퀀스를 추적합니다. 비대칭 라우팅이 있는 환경(예: TCP SYN 패킷이 outside1 인터페이스를 통해 종료되지만 해당 TCP SYN-ACK가 동일한 디바이스의 외부 인터페이스를 통해 반환되는 환경)에서 FTD는 알려진 추적 TCP 세션에 속한 것으로 SYN-ACK를 인식하지 않습니다. SYN-ACK가 예상과 다른 인터페이스에 도착하고 해당 인터페이스에 해당 SYN이 표시되지 않으므로, FTD는 이를 알 수 없는 연결에 대한 비 SYN 패킷으로 분류하고 ASP drop reason tcp-not-syn과 함께 삭제합니다.



TSID가 활성화된 경우 FTD 인라인 집합을 통한 비대칭 TCP 흐름

관련 콘텐츠

- Cisco 버그 ID CSCwp84746 — 설명서: 인라인 집합 인터페이스에서 TLS 서버 ID 검색과 TCP 상태 우회의 비호환성
- Cisco 버그 ID CSCwx42897 — 문서: TLS 서버 ID 검색은 인라인 집합 인터페이스에서 TCP 상태 우회를 재정의하여 TCP 트래픽이 삭제됨(tcp-not-syn)
- Cisco Bug ID CSCwx42901 — 인라인 집합 인터페이스에서 TCP 상태 우회를 비활성화하는 "Early Application Detection and URL categorization"(TSID)을 활성화할 때 경고를 추가합니다
- Cisco 설명서 - TCP 상태 우회에 대한 지침(TLS 서버 ID 검색 제한 포함)
- 사례 연구 - 인라인 집합을 통한 비대칭 트래픽
- Cisco Technote — FTD 및 FMC 트러블슈팅 번들을 생성하는 방법
- 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.