TCP 연결 실패를 유발하는 FTD 클러스터 비대칭 문제 해결

문제

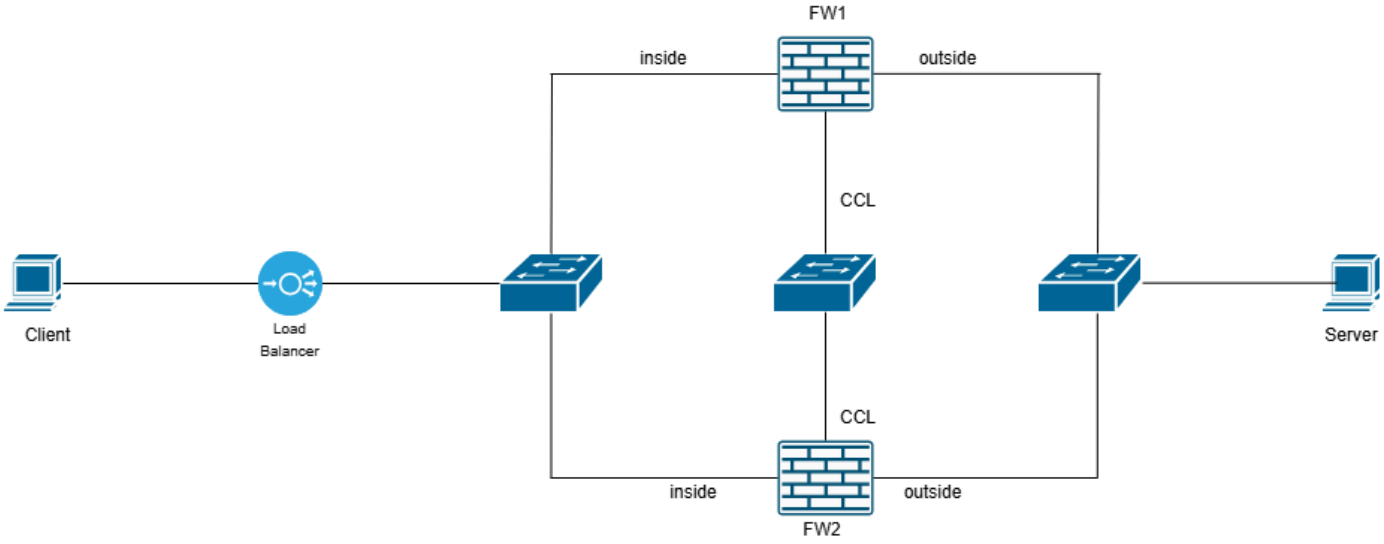
다음 중 하나 이상의 증상이 나타날 수 있습니다.

- FTD 클러스터를 지나는 애플리케이션에 대한 간헐적인 연결 실패
- TCP 3-way 핸드셰이크는 연결 시도 중에 실패합니다.
- 클라이언트가 SYN 패킷을 전송하지만 필요한 SYN-ACK 응답을 수신하지 않습니다.
- 클라이언트가 초기 SYN 이후에 RST 패킷을 전송합니다.

환경

- Secure Firewall Threat Defense 7.4에서 처음 확인 - 다른 버전도 영향을 받을 수 있음
- 클러스터 컨피그레이션
- 네트워크 경로의 로드 밸런서 — 선택 사항입니다.

토폴로지



inline_image_0.png

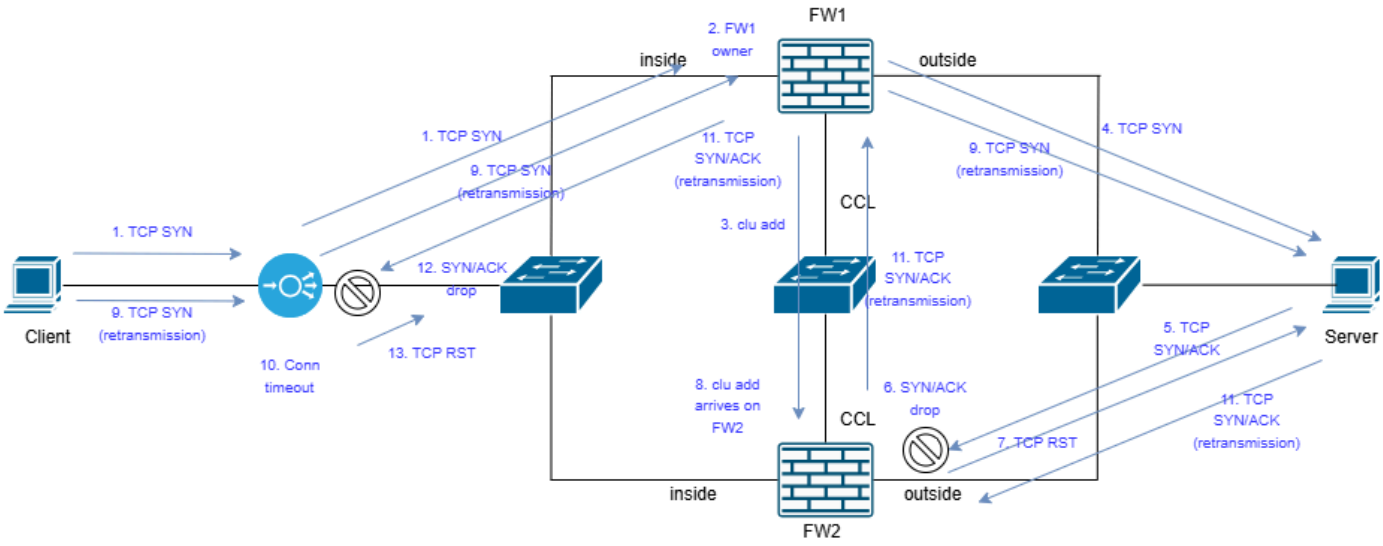
해결

문제의 근본 원인을 파악하려면 다음 시점에서 동시에 캡처해야 합니다.

- FW1 내부 인터페이스(reinject-hide 포함)
- FW1 외부 인터페이스(reinject-hide 포함)
- FW1 CCL(Cluster Interface)
- FW2 내부 인터페이스(reinject-hide 포함)
- FW2 외부 인터페이스(reinject-hide 포함)
- FW2 CCL(Cluster Interface)
- 클라이언트(또는 가능한 한 클라이언트와 가까운 위치)
- 서버(또는 가능한 한 서버에 가까운 위치)

캡처를 구성하는 방법에 대한 자세한 내용은 다음을 참조하십시오. 클러스터 캡처를 활성화하는 방법.

클라이언트 및 서버와 함께 두 방화벽에서 캡처한 결과 다음과 같은 토폴로지가 나타납니다.



inline_image_0.png

1. 클라이언트가 TCP SYN을 전송합니다. 패킷이 로드 밸런서(LB)에 도착하여 FW1로 전송됩니다.

2. FW1이 TCP SYN 패킷을 수신하고 흐름 소유자가 됩니다.

3. FW1은 디렉터(FW2)에게 특수(clu add) 클러스터 메시지를 보내 흐름 소유자에 대해 알립니다.

4. FW1은 TCP SYN을 대상 서버로 전달합니다.

참고: 3단계와 4단계는 특정 순서로 수행되지 않습니다.

5. 서버가 SYN/ACK로 응답합니다. 이 경우 포트 채널 로드 밸런싱 알고리즘으로 인해 SYN/ACK가 FW2로 전송되기 때문에 비대칭 플로우가 발생합니다.

6. SYN/ACK가 clu 추가 메시지 전에 FW2에 도착합니다. 이는 경쟁 조건이며 순전히 환경적입니다 (예: CCL의 대기 시간). FW2는 흐름 소유자가 누구인지 모르기 때문에 SYN/ACK가 삭제됩니다.

7. TCP RST가 서버로 전송됩니다.

8. 클라우드 추가 메시지가 FW2에 도착합니다.

9. 클라이언트가 TCP SYN 패킷을 다시 전송합니다. TCP SYN 패킷은 대상 서버로 전달됩니다.

10. LB에서 특정 플로우에 대한 TCP 연결이 시간 초과됩니다.

11. 서버가 SYN/ACK(TCP 재전송)로 응답합니다. SYN/ACK 패킷이 FW2에 도착합니다. 이번에는

FW2가 CLU 추가 메시지를 받았으므로 흐름 소유자를 알고 있으며 SYN/ACK가 CCL을 통해 흐름 소유자에게 전달됩니다. SYN/ACK가 클라이언트로 전송됩니다.

12. LB가 이 흐름을 모르고 SYN/ACK를 삭제합니다. 따라서 SYN/ACK가 클라이언트에 도착하지 않습니다.

13. 하나 이상의 TCP RST 패킷입니다.

추적 분석을 통한 방화벽 캡처

이러한 출력에서 캡처는 CCL 및 서버 연결 인터페이스의 방화벽에서 수집되었습니다.

· CCL에서 캡처는 UDP 4193 포트에 있습니다.

· 데이터 인터페이스에서 캡처는 reinject-hide 옵션을 사용하여 엔드포인트 간 TCP 트래픽과 일치합니다. 패킷이 실제로 도착하는 위치를 확인하고자 하기 때문입니다.

· IP 주소 192.0.2.65 = 클라이언트

· IP 주소 192.0.2.6 = 서버

1단계: SYN/ACK를 가져오는 방화벽 디바이스에서 이 명령을 사용하여 CLU 추가 메시지가 도착했는지 확인합니다. CLI 출력에는 메시지가 추가 흐름으로 표시됩니다.

```
firepower# show capture CCL decode

캡처된 패킷 3개

   1: 08:14:20.630521 127.2.1.1.51475 > 127.2.2.1.4193: udp 820

        클러스터 ASP  메시지: 보낸 사람: 1, 받는 사람: 0

        플로우 추가: 소유자 1, 디렉터 0, 백업 0,

                ifc_in INSIDE(7020a7), ifc_out INSIDE(7020a7)

                TCP src 192.0.2.65/37468, dest 192.0.2.6/80
```

2단계: SYN/ACK 패킷을 추적하고 타임스탬프와 추적 결과에 중점을 둡니다.

```
firepower# show capture CAPI packet-number 1 trace
```

캡처된 패킷 13개

```
   1: 08:14:20.628690 802.1Q vlan#200 P0 192.0.2.6.80 > 192.0.2.65.37468: S
2524735158:2524735158(0) ack 2881263901 win 65160 <mss 1460,sackOK,timestamp 611712900
970937593,nop,wscale 7>
```

단계: 1

유형: CAPTURE

하위 유형:

결과: 허용

경과 시간: 1,708ns

설정:

추가 정보:

MAC 액세스 목록

단계: 2

유형: 액세스 목록

하위 유형:

결과: 허용

경과 시간: 1,708ns

설정:

암시적 규칙

추가 정보:

MAC 액세스 목록

단계: 3

유형: INPUT-ROUTE-LOOKUP

하위 유형: 이그레스 인터페이스 확인

결과: 허용

경과 시간: 13664 ns

설정:

추가 정보:

이그레스 ifc INSIDE(vrfid:0)를 사용하여 next-hop 192.168.200.140을 찾았습니다.

단계: 4

유형: CLUSTER-EVENT

하위 유형:

결과: 허용

경과 시간: 16104 ns

설정:

추가 정보:

입력 인터페이스: 'INSIDE'

흐름 유형: 흐름 없음

I(0)이(가) 소유자가 됨

단계: 5

유형: OBJECT_GROUP_SEARCH

하위 유형:

결과: 허용

경과 시간: 19520 ns

설정:

추가 정보:

원본 개체 그룹 일치 수: 0

소스 NSG 일치 수: 0

대상 NSG 일치 수: 0

분류 테이블 조회 수: 1

총 조회 수: 1

중복 키 쌍 수: 0

분류 테이블 일치 수: 4

단계: 6

유형: 액세스 목록

하위 유형:

결과: 허용

경과 시간: 366ns

설정:

액세스 그룹 CSM_FW_ACL_ 전역

access-list CSM_FW_ACL_ advanced permit ip any rule-id 268436480

access-list CSM_FW_ACL_ remark rule-id 268436480: 액세스 정책: mzafeiro_empty - 기본값

access-list CSM_FW_ACL_ remark rule-id 268436480: L4 규칙: 기본 작업 규칙

추가 정보:

이 패킷은 판정에 도달할 추가 처리를 위해 snort로 전송됩니다

단계: 7

유형: CONN-SETTINGS

하위 유형:

결과: 허용

경과 시간: 366ns

설정:

클래스 맵 tcp

match access-list tcp

정책 맵 global_policy

 클래스 tcp

  connection conn-max 0 embryonic-conn-max 0 random-sequence-number disable syn-cookie-mss 1380
설정

서비스 정책 전역 정책 전역

추가 정보:

단계: 8

유형: NAT

하위 유형: 세션당

결과: 허용

경과 시간: 366ns

설정:

추가 정보:

단계: 9

유형: IP-OPTIONS

하위 유형:

결과: 허용

경과 시간: 366ns

설정:

추가 정보:

결과:

입력 인터페이스: INSIDE(vrfid:0)

입력 상태: up

입력 라인 상태: up

출력 인터페이스: INSIDE(vrfid:0)

출력 상태: up

출력 라인 상태: up

작업: 삭제

소요 시간: 54168 ns

Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame snp_sp:7459 flow (NA)/NA

핵심 사항

· SYN/ACK가 08:14:20.628690에 2msec 일찍 도래하는 동안 Add flow 메시지가 08:14:20.630521에 도착했습니다. 이는 경쟁 상태입니다.

· 방화벽에서 tcp-not-syn ASP 이유를 사용하여 SYN/ACK 패킷을 삭제합니다. 4단계에서 방화벽이 알려진 흐름 소유자가 있는지 확인하려고 했으나 해당 항목을 찾지 못하여 흐름 소유자가 되려고 했습니다.

이 출력은 방화벽이 흐름에 대해 알고 있을 때 SYN/ACK의 추적을 표시합니다.

```
firepower# show capture CAPI packet-number 3 trace

캡처된 패킷 13개

   3: 08:14:21.629560 802.1Q vlan#200 P0 192.0.2.6.80 > 192.0.2.65.37468: S
2540375172:2540375172(0) ack 2881263901 win 65160 <mss 1460,sackOK,timestamp 611713901
970938595,nop,wscale 7>

단계: 1

유형: CAPTURE

하위 유형:

결과: 허용

경과 시간: 1,708ns

설정:

추가 정보:

MAC  액세스 목록

단계: 2

유형: 액세스 목록

하위 유형:

결과: 허용

경과 시간: 1,708ns

설정:
```

암시적 규칙

추가 정보:

MAC 액세스 목록

단계: 3

유형: CLUSTER-EVENT

하위 유형:

결과: 허용

경과 시간: 3416ns

설정:

추가 정보:

입력 인터페이스: 'INSIDE'

흐름 유형: STUB

I(0)에 흐름이 있습니다. 올바른 소유자 (1)입니다.

단계: 4

유형: CAPTURE

하위 유형:

결과: 허용

경과 시간: 7808ns

설정:

추가 정보:

MAC 액세스 목록

결과:

입력 인터페이스: INSIDE(vrfid:0)

입력 상태: up

입력 라인 상태: up

작업: 허용

소요 시간: 14640 ns

1개 패킷 표시

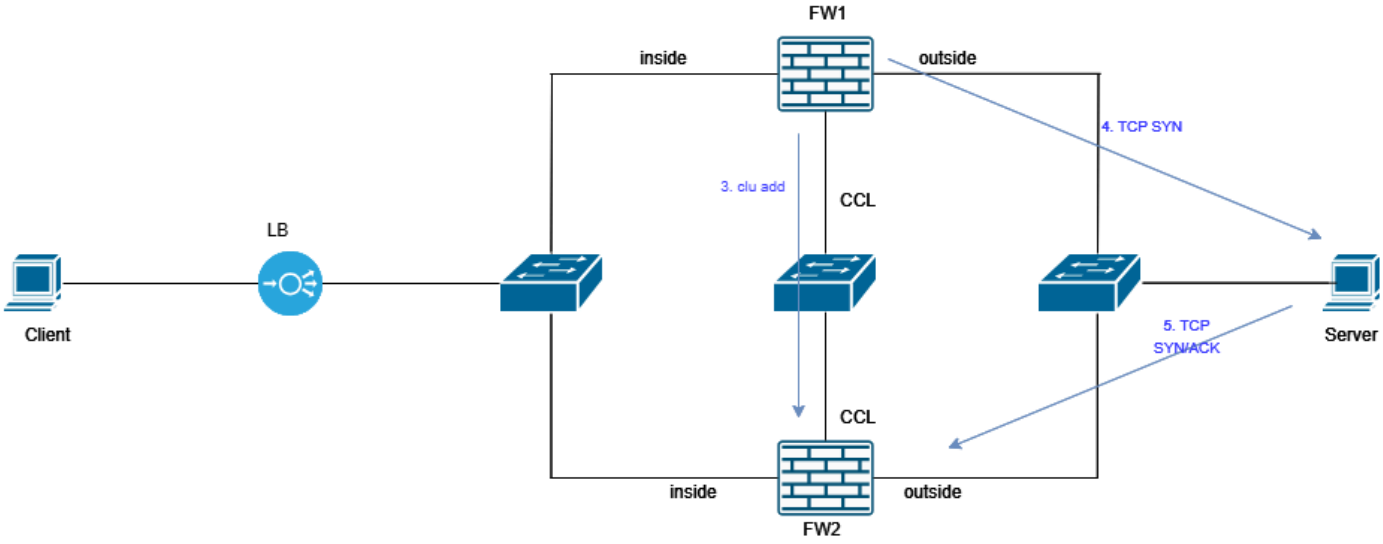
firepower 번호

핵심은 3단계입니다. 방화벽은 클러스터 유닛 1이 흐름 소유자임을 알고 있습니다. show cluster info 명령을 사용하여 어떤 디바이스가 유닛 0이고 어떤 디바이스가 1인지 확인할 수 있습니다.

자주 묻는 질문(FAQ)

Q. 간헐적인 TCP 연결 문제가 발생하는 이유는 무엇입니까?

A. 레이스 조건이므로 무작위로 발생합니다. 레이스 조건을 그에 따라 시각화할 수 있습니다.

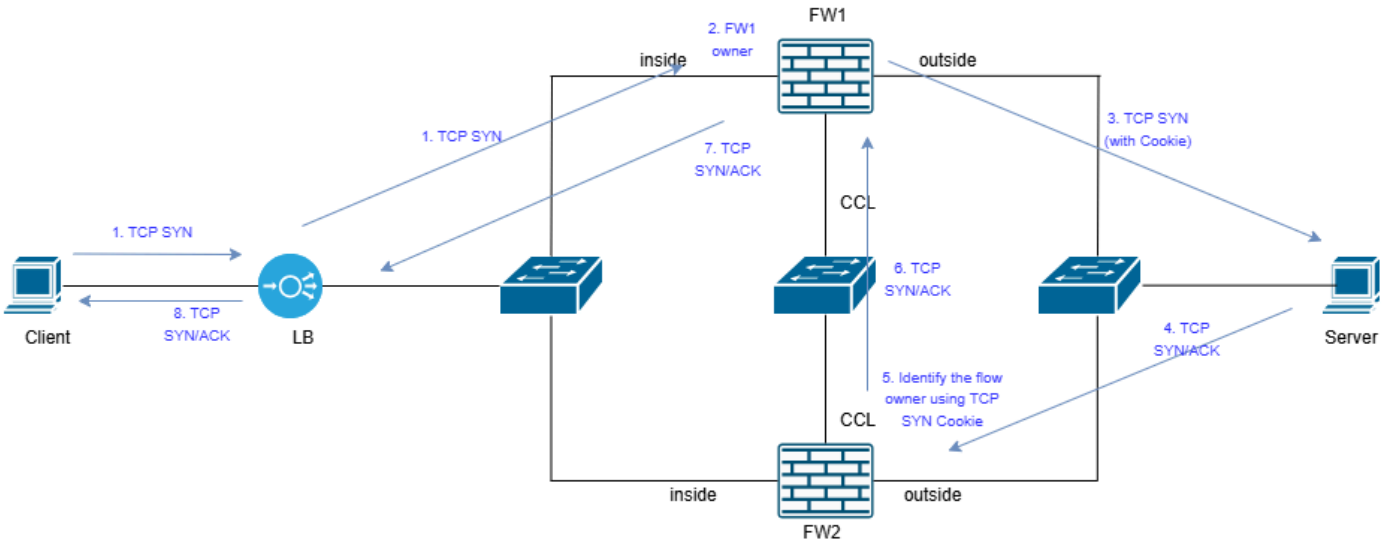


inline_image_0.png

Q. 경쟁에서 이길 수 있는 방법은 무엇일까요?

A.

해결 방법 1: TCP SYN 쿠키 메커니즘을 활용하기 위해 TCP 시퀀스 번호 임의 설정을 활성화합니다. 이 경우 통신이 적절히 구성됩니다.



인라인 이미지_1.png

해결 방법 2: 네트워크의 비대칭을 제거합니다. 먼저 비대칭의 원인을 식별해야 합니다. 이를 위해 포트 채널 부하 균형 알고리즘을 튜닝하고 다른 순서로 포트 채널 케이블을 다시 연결해야 할 수 있습니다.

원인

근본 원인은 FTD 클러스터 배포 내의 클러스터 비대칭으로 인해 발생하는 경쟁 상태입니다. 서버의 SYN-ACK 패킷이 초기 SYN 패킷을 처리한 노드와 다른 FTD 클러스터 노드에서 처리되고 있으므로 적절한 TCP 세션 설정이 불가능합니다.

관련 콘텐츠

- 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.