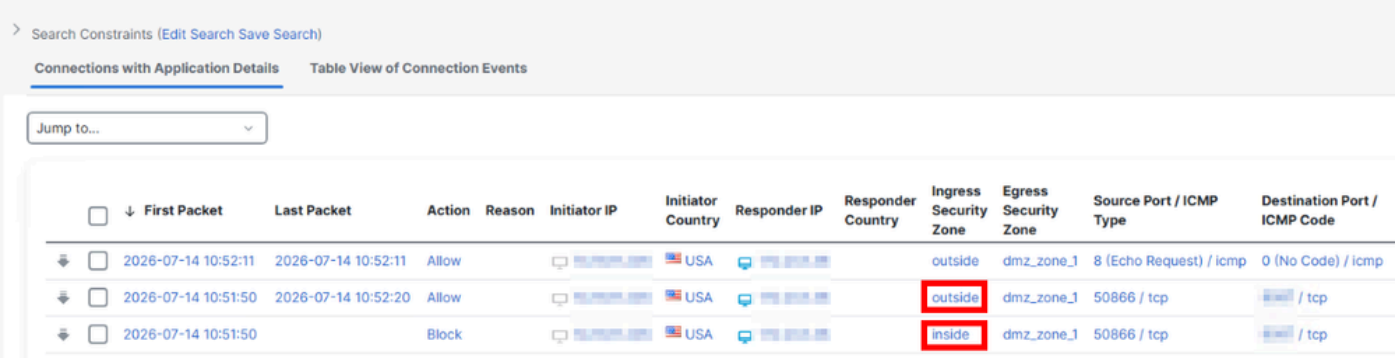
TCP 삭제 및 이중 영역 연결 로그를 유발하는 FTD 비대칭 라우팅 문제 해결

목차

문제

Cisco FTD(Secure Firewall Threat Defense) HA 쌍 뒤에 있는 DMZ 호스팅 애플리케이션에 대한 인바운드 연결에서는 간헐적으로 두 개의 보안 영역을 동일한 연결 시도의 트래픽 소스로 표시합니다. FMC 연결 이벤트는 외부 영역에서 허용되는 예상 연결과 내부 영역과 연결된 거부된 트래픽을 표시하여 실패한 TCP 연결을 표시합니다.



- FTD 경로 및 패킷 추적기는 소스와 대상 간의 적절한 라우팅, NAT 및 규칙을 확인합니다.
- 그러나 FTD 시스템은 추적을 지원하여 소스에서 들어오는 패킷만 표시하고 목적지에서 트래픽을 반환하지는 않습니다.

<#root>

```
> system support trace
.....
10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=6 GR=1-1 New firewall session
10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=6 GR=1-1 using HW or preset rule order 23, 'intended
10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=6 GR=1-1 allow action


10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=6 GR=1-1 app event changes: created
10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=9 GR=1-1 Got start of flow event from hardware with
10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=9 GR=1-1 Generating an SOF event with rule_id = 2684
10.x.x.200 39194 -> 172.x.x.36 9997 6 AS=0 ID=7 GR=1-1 Got end of flow event from hardware with fl
10.x.x.200 39194 -> 172.x.x.36 9997 6 AS=0 ID=7 GR=1-1 Rule Match Data: rule_id 0, rule_action 0 r
```

```
10.x.x.200 39194 -> 172.x.x.36 9997 6 AS=0 ID=7 GR=1-1 Generating an EOF event with rule_id = 2684

10.x.x.200 39194 -> 172.x.x.36 9997 6 AS=0 ID=7 GR=1-1 Received EOF, deleting the snort session
10.x.x.200 39194 -> 172.x.x.36 9997 6 AS=0 ID=7 GR=1-1 Deleting Firewall session flags=0x20190040,
```

- 호스트에서 연결이 결국 시간 초과됩니다.
- FTD '외부' 인터페이스의 캡처는 10.x.x.200이 외부 대상 IP 10.x.x.220에 SYN 및 에코 요청을 전송하는지 확인합니다.

<#root>

```
firepower# show capture outside_intf

 1: 13:59:03.051388       10.x.x.200.39194 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535



   2: 13:59:04.063458       10.x.x.200.39194 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535
   3: 13:59:06.073009       10.x.x.200.39194 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535
   4: 13:59:10.081477       10.x.x.200.39194 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535
   5: 13:59:18.090876       10.x.x.200.40812 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535

  6: 13:59:24.127984       10.x.x.200 > 10.x.x.220 icmp: echo request
```

- FTD UNNAT는 이를 내부 대상 IP 주소 172.x.x.36으로 보냅니다.

<#root>

```
firepower# show capture 1 packet-number 1 trace detail
.....
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 3186 ns
Config:

nat (dmz_zone_1,outside_primary) source static dmz1-172.x.x.36 outside-10.x.x.220
Additional Information:
NAT divert to egress interface dmz_zone_1(vrfid:0)
Untranslate 10.x.x.220/0 to 172.x.x.36/0
```

- FTD는 의도한 대로 적절한 허용 규칙으로 트래픽을 허용합니다.

<#root>

```
Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:

access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit object-group ping-echo ifc outside_primary any ifc dmz_zon
access-list CSM_FW_ACL_ remark rule-id 268434459: ACCESS POLICY: nf-policy - Mandatory


access-list CSM_FW_ACL_ remark rule-id 268434459: L7 RULE: intended_allow_rule


object-group service ping-echo
 service-object icmp echo
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
 Forward Flow based lookup yields rule:
 in  id=0x146e745dbd00, priority=12, domain=permit, deny=false
        hits=3532, user_data=0x0000000000000000, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
        src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=8, tag=any, ifc=outside_primary(vrfid:0)
        dst ip/id=172.x.x.36, mask=255.255.255.255, icmp-code=0, tag=any, ifc object-group id 4590
```

- 그런 다음 동일한 트래픽이 "dmz_zone_1" 인터페이스에서 DMZ 대상 172.x.x.36으로 나가는 것으로 올바르게 진행됩니다.

```
<#root>

Result:

input-interface: outside_primary(vrfid:0)


input-status: up
input-line-status: up

output-interface: dmz_zone_1(vrfid:0)


output-status: up
output-line-status: up

Action: allow


Time Taken: 106476 ns
```

- FTD dmz_zone_1 인터페이스의 캡처를 통해 10.x.x.200에서 내부 대상 IP 10.x.x.220으로 SYN 및 에코 요청을 전송하는지 확인합니다.

```
<#root>

firepower# show capture dmz_intf
```

```
 1: 13:59:03.051709       802.1Q vlan#600 P0 10.x.x.200.39194 > 172.x.x.36.9997: S 1245309079:1245

   2: 13:59:04.063610       802.1Q vlan#600 P0 10.x.x.200.39194 > 172.x.x.36.9997: S 1245309079:12
   3: 13:59:06.073146       802.1Q vlan#600 P0 10.x.x.200.39194 > 172.x.x.36.9997: S 1245309079:12
   4: 13:59:10.081630       802.1Q vlan#600 P0 10.x.x.200.39194 > 172.x.x.36.9997: S 1245309079:12
   5: 13:59:18.091166       802.1Q vlan#600 P0 10.x.x.200.40812 > 172.x.x.36.9997: S 1210202278:12

 6: 13:59:24.128197       802.1Q vlan#600 P0 10.x.x.200 > 172.x.x.36 icmp: echo request
```

- 그러나 FTD dmz_zone_1 인터페이스에는 내부 대상 IP 172.x.x.36의 반환 트래픽이 표시되지 않습니다.
- 캡처는 대상 172.x.x.36 SYN,ACK 및 에코 응답이 FTD 내부 인터페이스에 대신 들어오는지 확인합니다.

<#root>

```
firepower# show capture inside_intf

 1: 13:59:03.051861       802.1Q vlan#667 P0 172.x.x.36.9997 > 10.x.x.200.39194: S 3938871380:3938

   2: 13:59:03.051938       802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:12
   3: 13:59:03.051968       802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:12

   4: 13:59:04.063839       802.1Q vlan#667 P0 172.x.x.36.9997 > 10.x.x.200.39194: S 3938871380:39

   5: 13:59:04.063915       802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:12
   6: 13:59:04.064068       802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:12
  .....

 23: 13:59:24.128411       802.1Q vlan#667 P0 172.x.x.36 > 10.x.x.200 icmp: echo reply
```

- 대상 SYN,ACK가 잘못된 인터페이스에서 반환되면 FTD는 SYN이 아닌 초기 패킷으로 식별되면서 트래픽을 삭제합니다.

참고: 다른 TCP 삭제는 비대칭 라우팅으로 인해 발생할 수 있으며 FTD `show asp drop`

출력에서 볼 수 있습니다.

<#root>

```
Result:

input-interface: inside(vrfid:0)


input-status: up
input-line-status: up
output-interface: outside_primary(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Time Taken: 15572 ns

Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame snp_sp:7337 flow (NA)/NA


.....
firepower# show asp drop
Frame drop:
  SVC Module does not have a channel for reinjection (mp-svc-no-channel)
  SVC Module unable to fragment packet (mp-svc-no-fragment)                  25
  Flow is being freed (flow-being-freed)                                     78
  No valid adjacency (no-adjacency)                                         707
  Flow is denied by configured rule (acl-drop)                             1738


First TCP packet not SYN (tcp-not-syn)                                     760



 TCP failed 3 way handshake (tcp-3whs-failed)                               34
  TCP RST/FIN out of order (tcp-rstfin-ooo)                                1785
  TCP SEQ in SYN/SYNACK invalid (tcp-seq-syn-diff)                            5
  TCP SYNACK on established conn (tcp-synack-ooo)                             1
  TCP packet SEQ past window (tcp-seq-past-win)                              87
  TCP invalid ACK (tcp-invalid-ack)                                           1
  TCP RST/SYN in window (tcp-rst-syn-in-win)                                  1


  DNS Inspect id not matched (inspect-dns-id-not-matched)                    12
  FP L2 rule drop (l2_acl)                                                   34
  Dropped pending packets in a closed socket (np-socket-closed)             145
  NAT failed (nat-xlate-failed)                                               1
  Connection to PAT address without pre-existing xlate (nat-no-xlate-to-pat-pool)
  TCP Proxy retransmited packet drop (tcp-proxy-retransmit-drop)             90
  TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)             223
  TCP Proxy probe receive drop (tcp-proxy-probe-tcp-probe-drop)             129
  Blocked or blacklisted by the firewall preprocessor (firewall)              2
  Blocked or blacklisted by the stream preprocessor (stream)                301
  Packet is blacklisted by snort (snort-blacklist)                           81
  Packet is blocked as requested by snort (snort-block)                      26
```

환경

- Cisco Secure Firewall Threat Defense 모든 모델과 버전
- Cisco Secure Firewall Management Center 모든 모델 및 버전
- 동일한 트래픽에 영향을 주는 FTD에 인접하여 구성된 외부 라우팅 디바이스 또는 프록시.

해결

1. 반환 트래픽을 잘못된 FTD 인터페이스로 보내는 디바이스에서 비대칭 라우팅 동작을 해결합니다.

2. 그렇지 않으면 비대칭 라우팅을 확인하도록 TCP 상태 우회를 구성합니다.

- 이를 통해 방화벽은 인바운드 패킷과 아웃바운드 패킷이 서로 다른 인터페이스에 도착하는 TCP 세션을 처리할 수 있습니다.
- 우회는 비대칭 라우팅 시나리오에서 삭제를 유발하는 특정 상태 저장 검사를 비활성화하지만, 보안 트레이드 오프로 인해 주의 깊게 선택적으로 사용해야 합니다.
- 이는 FTD 외부에서 발생한 비대칭 라우팅 문제를 해결하기 위한 시도이며, 이 문제를 기본 단계로 해결하는 것이 가장 좋습니다.

비대칭 라우팅에 대한 TCP 상태 검사 우회(TCP 상태 우회):
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/advanced-access-service-policies.html#ID-2068-00000337

[Video] 비대칭 라우팅에 대한 TCP 상태 검사 우회(TCP 상태 우회):
https://www.youtube.com/watch?v=v6vJUpPqdYk

원인

이 문제는 FTD 방화벽 외부의 비대칭 라우팅으로 인해 발생했습니다. 인바운드 패킷이

outside_primary 인터페이스를 통해 방화벽에 진입하고 dmz_zone_1의 대상에 올바르게 전달되었지만, 172.x.x.36에서 반환되는 패킷이 예상 dmz_zone_1 인터페이스 대신 FTD 내부 인터페이스에 다시 도착했습니다.

반환 트래픽이 원래 흐름과 다른 인터페이스에 도착했기 때문에 FTD 상태 저장 검사 엔진은 패킷을 잘못된 것으로 처리하여 삭제 사유 "tcp-not-syn First TCP packet not SYN"으로 패킷을 삭제했습니다. 이 동작은 비대칭 라우팅이 여러 인터페이스에서 발생할 때 스테이트풀 TCP 검사에 필요합니다.

관련 콘텐츠

- Bypass TCP state checks for asymmetric routing(TCP 상태 우회)
- FTD: FlexConfig 정책을 사용하여 TCP 상태 우회 구성을 활성화하는 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.