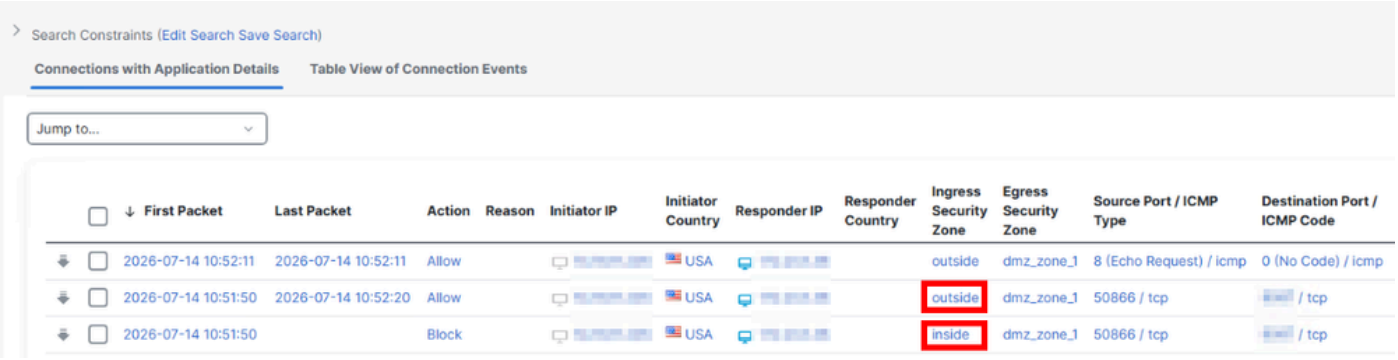
疑難排解導致TCP捨棄和雙區連線記錄的FTD非對稱路由問題

目錄

問題

對思科安全防火牆威脅防禦(FTD)HA對後方的DMZ託管應用的入站連線會間歇性地顯示兩個安全區域作為同一連線嘗試的流量來源。FMC連線事件顯示外部區域預期的允許連線，然後顯示與內部區域關聯的拒絕流量，導致TCP連線失敗。



- FTD路由和封包追蹤器會確認來源和目的地之間的路由選擇、NAT和規則是否正確。
- 但是,FTD系統支援追蹤只顯示來自源的傳入封包，但不會從目的地傳回流量。

<#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,
```

- 從主機，連線最終超時。
- FTD「outside」介面上的擷取會確認10.x.x.200將SYN和回應要求傳送到外部目的地IP 10.x.x.220。

<#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 NAT會將此內容傳送至內部目的地IP位址172.x.x.36。

<#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
```

- FTD允許流量按預期使用適當的允許規則。

<#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
```

- 接著，相同流量會正確從「dmz_zone_1」介面退出，前往DMZ目的地172.x.x.36。

<#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 介面上的擷取會確認10.x.x.200將SYN和回應要求傳送到內部目的地IP 10.x.x.220。

<#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
```

- 但是，FTD dmz_zone_1介面從不顯示來自內部目的地IP 172.x.x.36的返回流量。
- 擷取會確認目的地172.x.x.36 SYN、ACK和回應回覆是否改在FTD inside介面上傳入。

<#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
```

- 當目的地SYN、ACK在不正確的介面上傳回時，FTD捨棄被識別為不是SYN的初始封包的流量。

附註：其他TCP捨棄可能會由於非對稱路由而發生，可從FTD `show asp drop`輸出中看到。

<#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
```

環境

- 思科安全防火牆威脅防禦所有型號和版本
- Cisco Secure Firewall Management Center的所有型號和版本

- 在影響相同流量的FTD旁設定的外部路由裝置或代理。

解析

1.解決將返回流量傳送到錯誤FTD介面的裝置上的非對稱路由行為。

2.否則，請配置TCP狀態旁路以嘗試解析非對稱路由。

- 這允許防火牆處理具有到達不同介面的傳入和傳出封包的TCP作業階段。
- 旁路會禁用某些在非對稱路由場景中導致丟棄的狀態檢查，但出於安全權衡考慮，必須謹慎地選擇性地使用這種檢查。
- 請注意，這是嘗試解決在FTD之外引起的不對稱路由，最好將此因素作為主要步驟來解決。

針對非對稱路由的略過TCP狀態檢查（TCP狀態略過）：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

[影片]繞過TCP狀態檢查非對稱路由（TCP狀態繞過）：https://www.youtube.com/watch?v=v6vJUpPqdYk

原因

此問題是由於FTD防火牆外部的非對稱路由所導致。傳入封包透過outside_primary介面進入防火牆，並已正確轉送到dmz_zone_1上的目的地，但從172.x.x.36傳回的封包傳回FTD inside介面，而不是預期的dmz_zone_1介面。

由於返回流量到達的介面與原始流量不同，FTD狀態檢查引擎將封包視為無效，並以捨棄原因「tcp-not-syn First TCP packet not SYN」將其捨棄。 當多個介面上發生非對稱路由時，狀態TCP檢測會存在此行為。

相關內容

- 針對非對稱路由繞過TCP狀態檢查（TCP狀態繞過）
- FTD:如何使用FlexConfig策略啟用TCP狀態旁路配置
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。