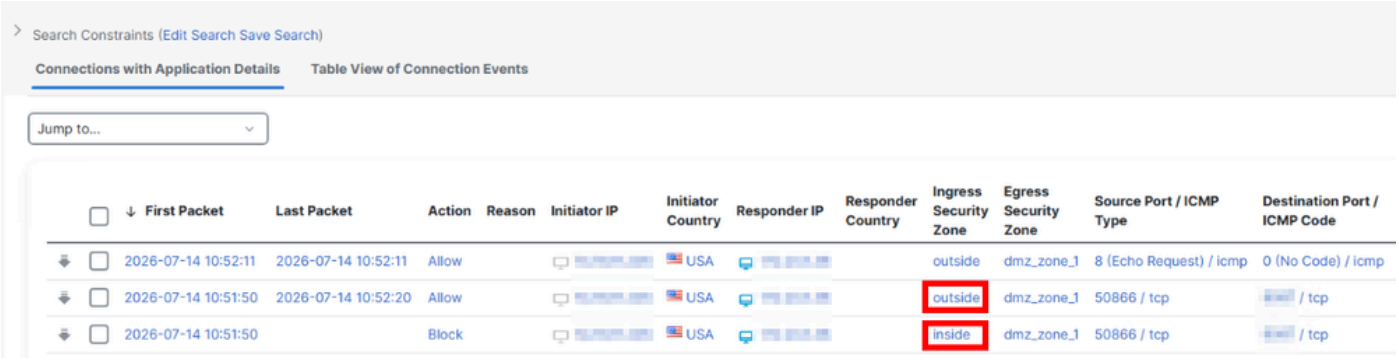
Risoluzione dei problemi relativi al routing asimmetrico FTD che provoca interruzioni TCP e log delle connessioni a doppia zona

Sommario

Problema

Le connessioni in entrata a un'applicazione ospitata nella zona DMZ dietro una coppia HA Cisco Secure Firewall Threat Defense (FTD) mostrano a intermittenza due aree di sicurezza come origine del traffico per lo stesso tentativo di connessione. Gli eventi di connessione FMC visualizzano la connessione consentita prevista dalla zona esterna, seguita dal traffico negato associato alla zona interna, con conseguente errore di connettività TCP.



- Il router FTD e i traccianti dei pacchetti confermano il routing corretto, il NAT e le regole tra l'origine e la destinazione.
- Tuttavia, il `sistema` FTD `supporta la traccia` solo per mostrare i pacchetti in arrivo dall'origine, ma non per restituire il traffico dalla destinazione.

<#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,
```

- Dall'host, la connessione alla fine si interrompe.
- Le acquisizioni sull'interfaccia 'esterna' FTD confermano che 10.x.x.200 invia SYN e Richiesta echo alla destinazione esterna 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
```

- L'FTD UNNAT comunica questo all'indirizzo IP di destinazione interno 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
```

- L'FTD consente il traffico con la regola Consenti appropriata come previsto.

<#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
```

- Lo stesso traffico quindi procede correttamente all'uscita sull'interfaccia "dmz_zone_1" verso la destinazione DMZ 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
```

- Le acquisizioni sull'interfaccia dmz_zone_1 dell'FTD confermano che 10.x.x.200 invia una richiesta SYN ed Echo all'indirizzo IP 10.x.x.220 della destinazione interna.

<#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
```

- Tuttavia, l'interfaccia FTD dmz_zone_1 non mostra mai il traffico di ritorno dalla destinazione interna IP 172.x.x.36.
- Le acquisizioni confermano che la destinazione 172.x.x.36 SYN, ACK e Echo Reply vengono invece acquisite tramite FTD all'interno dell'interfaccia.

<#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
```

- Come SYN di destinazione, ACK torna sull'interfaccia errata, l'FTD rifiuta il traffico in quanto viene identificato come un pacchetto iniziale che non è un SYN.

Nota: Altre perdite TCP possono verificarsi a causa del routing asimmetrico e possono essere visualizzate nell'output `show asp drop` FTD.

<#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
```

Ambiente

- Cisco Secure Firewall Threat Defense per tutti i modelli e le versioni

- Cisco Secure Firewall Management Center per tutti i modelli e le versioni
- Dispositivo di routing esterno o proxy configurato accanto all'FTD con impatto sullo stesso traffico.

Risoluzione

1. Risolvere il comportamento di routing asimmetrico sul dispositivo che invia il traffico di ritorno all'interfaccia FTD errata.

2. In caso contrario, configurare il bypass dello stato TCP in modo che tenti di risolvere il routing asimmetrico.

- In questo modo, il firewall può gestire le sessioni TCP con pacchetti in entrata e in uscita in arrivo su interfacce diverse.
- Il bypass disabilita alcuni controlli con informazioni sullo stato che causano interruzioni in scenari di routing asimmetrici, ma deve essere utilizzato con cautela e in modo selettivo a causa di compromessi sulla sicurezza.
- Tenere presente che questo è un tentativo di aggirare il routing asimmetrico causato al di fuori dell'FTD, ed è meglio risolvere quel fattore come fase principale.

Ignora controlli di stato TCP per routing asimmetrico (bypass stato TCP): 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] Ignora controlli di stato TCP per routing asimmetrico (bypass stato TCP): https://www.youtube.com/watch?v=v6vJUpPqdYk

Causa

Il problema è stato causato da un routing asimmetrico esterno al firewall FTD. I pacchetti in entrata sono entrati nel firewall attraverso l'interfaccia outside_primary e sono stati inoltrati correttamente alla destinazione su dmz_zone_1, ma i pacchetti restituiti da 172.x.x.36 sono tornati all'interno dell'interfaccia FTD invece che all'interfaccia dmz_zone_1.

Poiché il traffico di ritorno è arrivato su un'interfaccia diversa da quella del flusso originale, il motore di ispezione con stato FTD ha trattato i pacchetti come non validi e li ha scartati con il motivo di rilascio "tcp-not-syn First TCP packet not SYN". Questo comportamento è previsto per l'ispezione TCP con stato quando si verifica il routing asimmetrico su più interfacce.

Contenuto correlato

- Ignora controlli di stato TCP per routing asimmetrico (bypass stato TCP)
- FTD Come abilitare la configurazione di bypass dello stato TCP utilizzando il criterio FlexConfig
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).