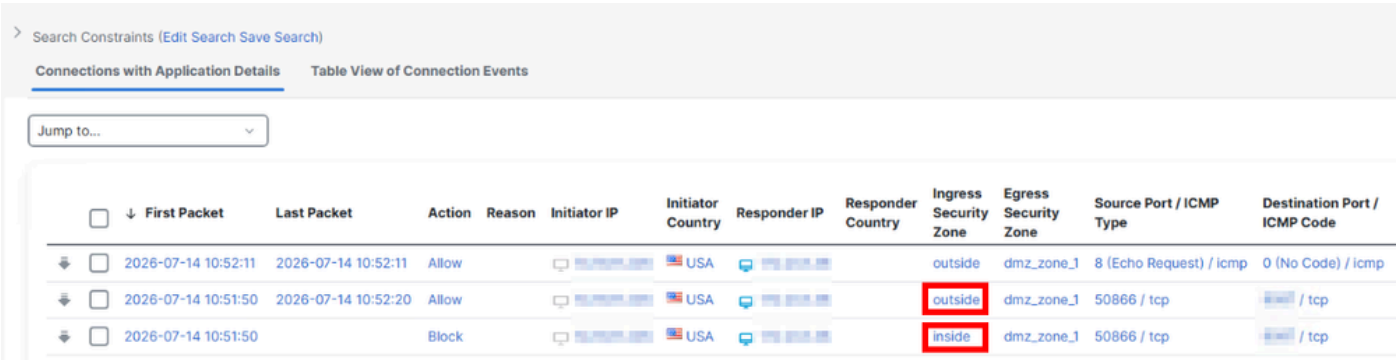
Dépannage du routage asymétrique FTD causant des abandons TCP et des journaux de connexion à deux zones

Table des matières

Problème

Les connexions entrantes vers une application hébergée dans une zone DMZ derrière une paire HA Cisco Secure Firewall Threat Defense (FTD) affichent par intermittence deux zones de sécurité comme source de trafic pour la même tentative de connexion. Les événements de connexion FMC affichent la connexion autorisée attendue de la zone externe, suivie d'un trafic refusé associé à la zone interne, ce qui entraîne l'échec de la connectivité TCP.



- La route FTD et les traceurs de paquets confirment le routage, la NAT et les règles appropriés entre la source et la destination.
- Cependant, le `système` FTD `prend en charge le suivi et` affiche uniquement les paquets entrants provenant de la source, mais pas le trafic de retour de la destination.

<#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,
```

- À partir de l'hôte, la connexion finit par expirer.
- Les captures sur l'interface « externe » FTD confirment que 10.x.x.200 envoie une requête SYN et Echo à l'adresse IP de destination externe 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
```

- La fonction FTD UNNAT envoie ce message à l'adresse IP de destination interne 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
```

- Le FTD autorise le trafic avec la règle Allow appropriée.

<#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
```

- Le même trafic sort alors correctement de l'interface « dmz_zone_1 » vers la destination 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
```

- Les captures sur l'interface FTD dmz_zone_1 confirment que 10.x.x.200 envoie SYN et une requête d'écho à l'adresse IP de destination interne 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
```

- Cependant, l'interface FTD dmz_zone_1 n'affiche jamais le trafic de retour en provenance de l'IP de destination interne 172.x.x.36.
- Les captures confirment que la destination 172.x.x.36 SYN, ACK et Echo Reply se trouvent sur l'interface interne FTD.

<#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
```

- Comme la destination SYN,ACK retourne sur l'interface incorrecte, le FTD abandonne le trafic car il est identifié comme un paquet initial qui n'est pas un SYN.

Remarque : D'autres abandons TCP peuvent se produire en raison du routage asymétrique et peuvent être vus dans la sortie FTD `show asp drop`.

<#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
```

Environnement

- Cisco Secure Firewall Threat Defense tous les modèles et versions

- Cisco Secure Firewall Management Center tous les modèles et versions
- Périphérique de routage externe ou proxy configuré à côté du FTD affectant le même trafic.

Résolution

1. Résolvez le comportement de routage asymétrique au niveau du périphérique qui envoie le trafic de retour à la mauvaise interface FTD.

2. Sinon, configurez le contournement d'état TCP pour tenter de résoudre le routage asymétrique.

- Cela permet au pare-feu de gérer les sessions TCP dont les paquets entrants et sortants arrivent sur différentes interfaces.
- Le contournement désactive certaines vérifications avec état qui provoquent des pertes dans des scénarios de routage asymétrique, mais doit être utilisé avec prudence et de manière sélective en raison des compromis de sécurité.
- N'oubliez pas qu'il s'agit d'une tentative de contourner le routage asymétrique provoqué en dehors du FTD, et qu'il est préférable de résoudre ce facteur comme étape principale.

Contourner les contrôles d'état TCP pour le routage asymétrique (contournement d'état 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

[Vidéo] Contourner les contrôles d'état TCP pour le routage asymétrique (contournement d'état TCP) : https://www.youtube.com/watch?v=v6vJUpPqdYk

Motif

Le problème est dû à un routage asymétrique externe au pare-feu FTD. Les paquets entrants sont entrés dans le pare-feu via l'interface outside_primary et ont été correctement transférés vers la destination sur dmz_zone_1, mais les paquets renvoyés par 172.x.x.36 sont revenus sur l'interface FTD interne au lieu de l'interface dmz_zone_1 attendue.

Étant donné que le trafic de retour est arrivé sur une interface différente du flux d'origine, le

moteur d'inspection avec état FTD a traité les paquets comme non valides et les a abandonnés avec la raison d'abandon « tcp-not-syn First TCP packet not SYN ». Ce comportement est attendu pour l'inspection TCP avec état lorsque le routage asymétrique se produit sur plusieurs interfaces.

Autres informations utiles

- Contourner les contrôles d'état TCP pour le routage asymétrique (contournement d'état TCP)
- DFT : Comment activer la configuration de contournement d'état TCP en utilisant la stratégie FlexConfig
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.