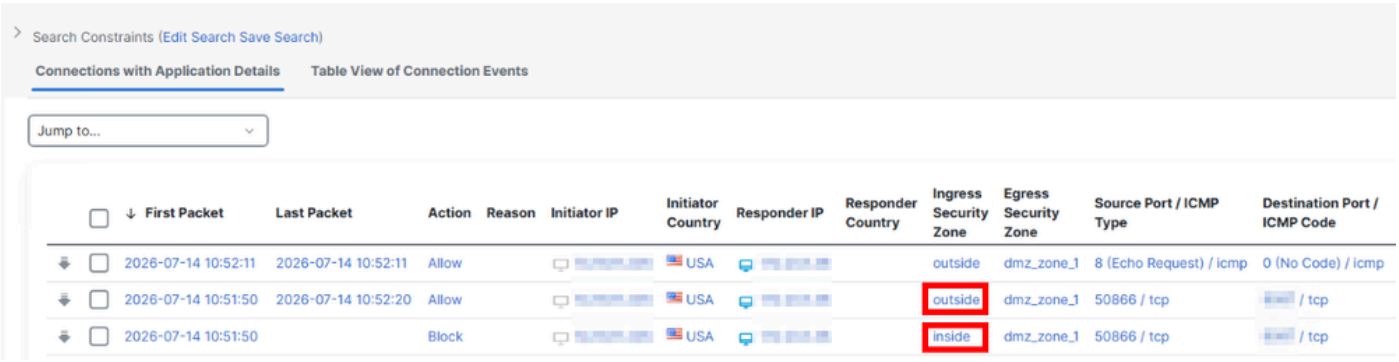
Problemen oplossen met asymmetrische FTD-routering die TCP-druppels en Dual Zone-verbindingslogboeken veroorzaakt

Inhoud

uitgifte

Inkomende verbindingen met een DMZ-gehoste toepassing achter een Cisco Secure Firewall Threat Defense (FTD) HA-paar tonen met tussenpozen twee beveiligingszones als de verkeersbron voor dezelfde verbindingspoging. FMC-verbindingsevenementen geven de verwachte toegestane verbinding van de buitenzone weer, gevolgd door geweigerd verkeer in verband met de binnenzone, wat resulteert in een mislukte TCP-verbinding.



- De FTD-route en pakkettracers bevestigen de juiste routering, NAT en regels tussen de bron en bestemming.
- Het FTD-`systeemondersteuningsspoor` toont echter alleen inkomende pakketten van de bron, maar geen terugkerend verkeer van de bestemming.

<#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,
```

- Van de gastheer, de verbinding uiteindelijk time-out.
- Opnames op de FTD 'buiten'-interface bevestigen dat 10.x.x.200 SYN en Echo Request naar de externe bestemming stuurt 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
```

- De FTD UNNAT verwijst dit naar het IP-adres van de interne bestemming 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
```

- De FTD staat het verkeer toe met de juiste Allow-regel zoals bedoeld.

<#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
```

- Hetzelfde verkeer gaat dan correct naar de uitgang op de "dmz_zone_1" interface naar de DMZ bestemming 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
```

- Opnames op de FTD dmz_zone_1-interface bevestigen dat 10.x.x.200 SYN en Echo Request naar de interne bestemming IP 10.x.x.220 stuurt.

<#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
```

- De FTD dmz_zone_1-interface toont echter nooit retourverkeer vanaf interne bestemming IP 172.x.x.36.
- Opnames bevestigen dat de bestemming 172.x.x.36 SYN, ACK en Echo Reply in plaats daarvan op FTD in de interface komen.

<#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
```

- Als de bestemming SYN, ACK retourneert op de verkeerde interface, de FTD laat het verkeer als het wordt geïdentificeerd als een eerste pakket dat niet een SYN.

Opmerking: Andere TCP-druppels kunnen optreden als gevolg van asymmetrische routering en kunnen worden gezien in de FTD-`show asp-drop`-output.

<#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
```

milieu

- Cisco Secure Firewall Threat Defense voor alle modellen en versies

- Cisco Secure Firewall Management Center voor alle modellen en versies
- Extern routeringsapparaat of proxy geconfigureerd naast de FTD die hetzelfde verkeer beïnvloedt.

resolutie

1. Los het asymmetrische routeringsgedrag op bij het apparaat dat het retourverkeer naar de verkeerde FTD-interface stuurt.

2. Configureer anders TCP-statusbypass om asymmetrische routering op te lossen.

- Hiermee kan de firewall TCP-sessies verwerken met inkomende en uitgaande pakketten die op verschillende interfaces aankomen.
- De bypass schakelt bepaalde stateful checks uit die vallen veroorzaken in asymmetrische routeringsscenario's, maar moet voorzichtig en selectief worden gebruikt vanwege beveiligingsafwegingen.
- Houd er rekening mee dat dit een poging is om asymmetrische routering te omzeilen die buiten de FTD wordt veroorzaakt, en het is het beste om die factor als een primaire stap op te lossen.

TCP-statuscontroles omzeilen voor asymmetrische routering (TCP-statusbypass): 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] TCP-statuscontroles omzeilen voor asymmetrische routering (TCP-statusbypass): https://www.youtube.com/watch?v=v6vJUpPqdYk

Oorzaak

Het probleem werd veroorzaakt door asymmetrische routering buiten de FTD-firewall. Inkomende pakketten kwamen de firewall binnen via de outside_primary-interface en werden correct doorgestuurd naar de bestemming op dmz_zone_1, maar de terugkerende pakketten van 172.x.x.36 kwamen terug op de FTD binnen interface in plaats van de verwachte

dmz_zone_1Źinterface.

Omdat het retourverkeer op een andere interface aankwam dan de oorspronkelijke stroom, behandelde de FTD stateful inspection engine de pakketten als ongeldig en liet ze vallen met de druppelreden "tcp-not-syn First TCP packet not SYN". Dit gedrag wordt verwacht voor stateful TCP inspectie wanneer asymmetrische routering optreedt over meerdere interfaces.

Gerelateerde inhoud

- TCP-statuscontroles omzeilen voor asymmetrische routering (TCP-statusbypass)
- FTD: TCP State Bypass Configuration inschakelen met FlexConfig-beleid
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.