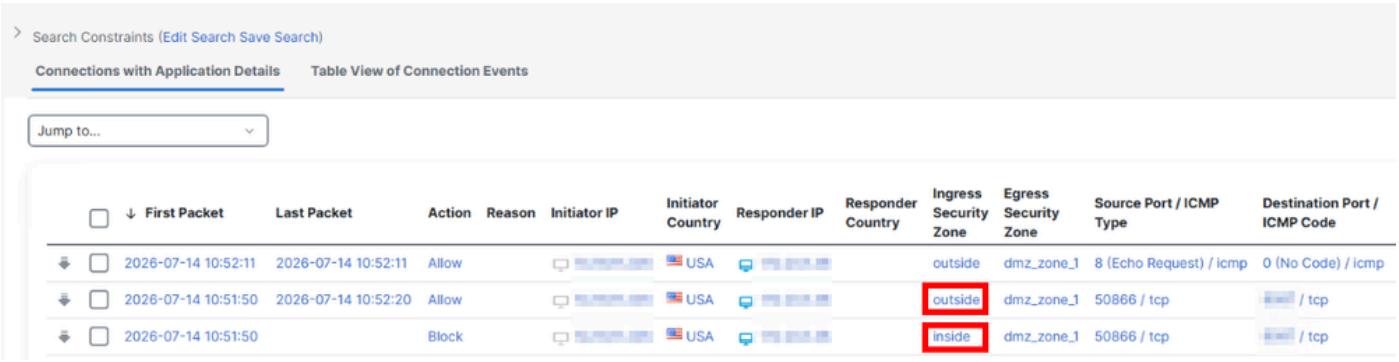
Resolución de problemas de ruteo asimétrico FTD que causa caídas de TCP y registros de conexión de zona dual

Contenido

Problema

Las conexiones entrantes a una aplicación alojada en DMZ detrás de un par HA de Cisco Secure Firewall Threat Defence (FTD) muestran de forma intermitente dos zonas de seguridad como origen del tráfico para el mismo intento de conexión. Los eventos de conexión de FMC muestran la conexión permitida esperada desde la zona exterior, seguida de tráfico denegado asociado con la zona interior, lo que produce un error en la conectividad TCP.



- La ruta FTD y los trazadores de paquetes confirman el ruteo, la NAT y las reglas correctas entre el origen y el destino.
- Sin embargo, el `seguimiento de soporte del sistema` FTD sólo muestra los paquetes entrantes del origen, pero no el tráfico de retorno del destino.

<#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,
```

- Desde el host, la conexión termina con el tiempo de espera.
- Las capturas en la interfaz 'externa' de FTD confirman que 10.x.x.200 envía SYN y la solicitud de eco a la IP de destino externa 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
```

- El FTD UNNAT lo envía a la dirección IP de destino interna 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
```

- El FTD permite el tráfico con la regla de permiso adecuada según lo 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
```

- A continuación, el mismo tráfico sale correctamente de la interfaz "dmz_zone_1" hacia el destino 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
```

- Las capturas en la interfaz FTD dmz_zone_1 confirman que 10.x.x.200 envía SYN y la solicitud de eco a la IP de destino interna 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
```

- Sin embargo, la interfaz FTD dmz_zone_1 nunca muestra el tráfico de retorno de la IP de destino interna 172.x.x.36.
- Las capturas confirman que el destino 172.x.x.36 SYN,ACK y la respuesta de eco entran en la interfaz interna FTD en su lugar.

<#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
```

- Como el SYN de destino, ACK regresa en la interfaz incorrecta, el FTD descarta el tráfico ya que se identifica como un paquete inicial que no es un SYN.

Nota: Otras caídas de TCP pueden ocurrir debido al ruteo asimétrico y pueden verse en la salida `show asp drop de` 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
```

Entorno

- Cisco Secure Firewall Threat Defence en todos los modelos y versiones

- Cisco Secure Firewall Management Center en todos los modelos y versiones
- Dispositivo de routing externo o proxy configurado junto al FTD que afecta al mismo tráfico.

Resolución

1. Resuelva el comportamiento de ruteo asimétrico en el dispositivo que está enviando el tráfico de retorno a la interfaz FTD incorrecta.

2. De lo contrario, configure el desvío del estado TCP para intentar resolver el ruteo asimétrico.

- Esto permite que el firewall maneje sesiones TCP que tienen paquetes entrantes y salientes que llegan en diferentes interfaces.
- La omisión deshabilita ciertas comprobaciones stateful que causan caídas en escenarios de ruteo asimétrico, pero se debe usar con precaución y selectivamente debido a las concesiones de seguridad.
- Tenga en cuenta que se trata de un intento de evitar el routing asimétrico causado fuera del FTD, y es mejor resolver ese factor como un paso principal.

Omitir comprobaciones de estado TCP para enrutamiento asimétrico (omisión de estado 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

[Vídeo] Omitir las comprobaciones de estado de TCP para el enrutamiento asimétrico (omisión de estado de TCP): https://www.youtube.com/watch?v=v6vJUpPqdYk

Causa

El problema fue causado por el ruteo asimétrico externo al firewall FTD. Los paquetes entrantes ingresaron al firewall a través de la interfaz outside_primary y fueron reenviados correctamente al destino en dmz_zone_1, pero los paquetes de retorno de 172.x.x.36 regresaron a la interfaz FTD inside en lugar de la interfaz dmz_zone_1 esperada.

Debido a que el tráfico de retorno llegó a una interfaz diferente al flujo original, el motor de

inspección stateful de FTD trató los paquetes como no válidos y los descartó con la razón de descarte "tcp-not-syn First TCP packet not SYN". Se espera este comportamiento para la inspección de TCP con estado cuando se produce el ruteo asimétrico a través de múltiples interfaces.

Contenido relacionado

- Omitir comprobaciones de estado de TCP para enrutamiento asimétrico (omisión de estado de TCP)
- FTD: Cómo habilitar la configuración de omisión del estado TCP mediante la política FlexConfig
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).