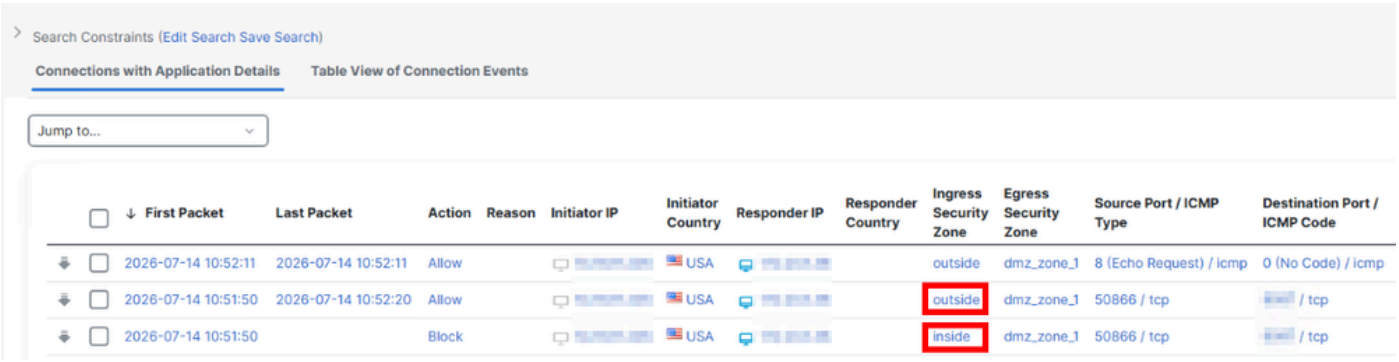
Solucionar problemas de roteamento assimétrico de FTD que causam quedas de TCP e logs de conexão de zona dupla

Contents

Problema

As conexões de entrada para um aplicativo hospedado na DMZ por trás de um par HA Cisco Secure Firewall Threat Defense (FTD) mostram intermitentemente duas zonas de segurança como a fonte de tráfego para a mesma tentativa de conexão. Os eventos de conexão do FMC exibem a conexão permitida esperada da zona externa, seguida pelo tráfego negado associado à zona interna, resultando em falha na conectividade do TCP.



- A rota de FTD e os rastreadores de pacotes confirmam o roteamento, o NAT e as regras apropriados entre a origem e o destino.
- No entanto, o `rastreamento de suporte do sistema de` FTD mostra apenas os pacotes de entrada da origem, mas não o tráfego de retorno do 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,
```

- A partir do host, a conexão acaba expirando.
- As capturas na interface 'externa' do FTD confirmam que o 10.x.x.200 envia SYN e Echo Request ao IP de destino externo 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
```

- O FTD UNNAT faz isso para o endereço IP destino 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
```

- O FTD permite o tráfego com a regra de permissão apropriada, conforme pretendido.

<#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
```

- O mesmo tráfego então prossegue corretamente para sair na interface "dmz_zone_1" em direção ao 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
```

- As capturas na interface FTD dmz_zone_1 confirmam que 10.x.x.200 envia SYN e Echo Request ao IP de destino interno 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
```

- No entanto, a interface FTD dmz_zone_1 nunca mostra o tráfego de retorno do IP de destino interno 172.x.x.36.
- As capturas confirmam que o destino 172.x.x.36 SYN, ACK e Echo Reply entra na interface interna do 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
```

- Como o destino SYN,ACK retorna na interface incorreta, o FTD descarta o tráfego, pois é identificado como um pacote inicial que não é um SYN.

Note: Outros descartes de TCP podem ocorrer devido ao roteamento assimétrico e podem ser vistos na saída 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
```

Ambiente

- Cisco Secure Firewall Threat Defense para todos os modelos e versões

- Cisco Secure Firewall Management Center todos os modelos e versões
- Dispositivo de roteamento externo ou proxy configurado adjacente ao FTD que afeta o mesmo tráfego.

Resolução

1. Resolva o comportamento de roteamento assimétrico no dispositivo que está enviando o tráfego de retorno para a interface incorreta de FTD.

2. Caso contrário, configure o desvio de estado TCP para tentar resolver o roteamento assimétrico.

- Isso permite que o firewall manipule sessões TCP que tenham pacotes de entrada e de saída que cheguem em diferentes interfaces.
- O desvio desabilita determinadas verificações stateful que causam quedas em cenários de roteamento assimétrico, mas que devem ser usadas com cautela e seletivamente devido a compensações de segurança.
- Lembre-se de que essa é uma tentativa de contornar o roteamento assimétrico causado fora do FTD, e é melhor resolver esse fator como uma etapa principal.

Ignorar verificações de estado TCP para roteamento assimétrico (desvio 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]Ignorar as verificações de estado TCP para roteamento assimétrico (desvio de estado TCP): https://www.youtube.com/watch?v=v6vJUpPqdYk

Causa

O problema foi causado pelo roteamento assimétrico externo ao firewall FTD. Os pacotes de entrada entraram no firewall através da interface outside_primary e foram encaminhados corretamente para o destino em dmz_zone_1, mas os pacotes de retorno de 172.x.x.36 chegaram de volta à interface FTD inside em vez da interface esperada dmz_zone_1.

Como o tráfego de retorno chegou em uma interface diferente do fluxo original, o mecanismo de inspeção stateful do FTD tratou os pacotes como inválidos e os descartou com a razão de queda "tcp-not-syn Primeiro pacote TCP não SYN". Esse comportamento é esperado para inspeção de TCP stateful quando o roteamento assimétrico ocorre em várias interfaces.

Conteúdo relacionado

- Ignorar verificações de estado TCP para roteamento assimétrico (desvio de estado TCP)
- DTF: Como habilitar a Configuração de desvio de estado TCP usando a Política FlexConfig
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.