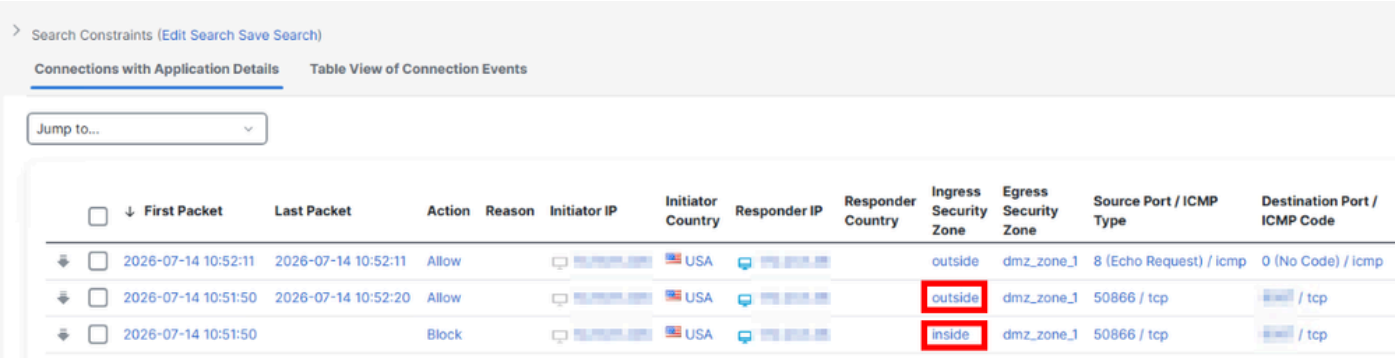
排除FTD非对称路由导致TCP丢弃和双区域连接日志故障

目录

问题

到思科安全防火墙威胁防御(FTD)高可用性对后面的DMZ托管应用的入站连接间歇性地将两个安全区域显示为同一连接尝试的流量源。FMC连接事件显示外部区域的预期允许连接，然后显示与内部区域关联的拒绝流量，导致TCP连接失败。



- FTD路由和数据包跟踪器可确认源设备与目的设备之间的路由、NAT和规则是否正确。
- 但FTD系统支持trace只显示来自源的传入数据包，但不返回来自目标的流量。

<#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,
```

- 从主机，连接最终超时。
- FTD“外部”接口上的捕获确认10.x.x.200向外部目标IP 10.x.x.220发送SYN和Echo请求。

<#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
```

- FTD NAT将此地址转换为内部目标IP地址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
```

- FTD允许流量按预期使用适当的Allow规则。

<#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
```

- 然后，相同流量会正确从“dmz_zone_1”接口退出，指向DMZ目标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
```

- FTD dmz_zone_1接口上的捕获确认10.x.x.200向内部目标IP 10.x.x.220发送SYN和回应请求。

```
<#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
```

- 但是，FTD dmz_zone_1接口从不显示来自内部目标IP 172.x.x.36的返回流量。
- 捕获确认目标172.x.x.36 SYN、ACK和Echo Reply在FTD内部接口进入。

<#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
```

- 当目标SYN，ACK在不正确的接口上返回时，FTD会丢弃被标识为不是SYN的初始数据包的流量。

注意：其他TCP丢弃可能由于非对称路由而发生，并且可以在FTD `show asp drop`输出中看到。

<#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
```

环境

- 思科安全防火墙威胁防御所有型号和版本
- 思科安全防火墙管理中心所有型号和版本

- 在影响相同流量的FTD旁配置的外部路由设备或代理。

分辨率

1.解决向错误的FTD接口发送返回流量的设备上的非对称路由行为。

2.否则，请配置TCP状态旁路以尝试解析非对称路由。

- 这使防火墙可以处理入站和出站数据包到达不同接口的TCP会话。
- 旁路会禁用某些在非对称路由场景下导致丢弃的状态检查，但出于安全权衡考虑，必须谨慎选择地使用该检查。
- 请注意，这是尝试解决在FTD之外引起的不对称路由，最好将此因素作为主要步骤来解决。

针对非对称路由绕行TCP状态检查（TCP状态绕行）：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

[视频]绕过TCP状态检查以检查非对称路由（TCP状态绕行）：https://www.youtube.com/watch?v=v6vJUpPqdYk

原因

此问题是由FTD防火墙外部的不对称路由引起的。入站数据包通过outside_primary接口进入防火墙，并已正确转发到dmz_zone_1上的目标，但从172.x.x.36返回的数据包返回FTD inside接口，而不是预期的dmz_zone_1接口。

由于返回流量到达的接口与原始流量不同，因此FTD状态检测引擎将数据包视为无效，并以丢弃原因“tcp-not-syn First TCP packet not SYN”将其丢弃。 当多个接口上发生非对称路由时，状态TCP检测会存在此行为。

相关内容

- 绕过异步路由的TCP状态检查（TCP状态绕行）
- FTD:如何使用FlexConfig策略启用TCP状态旁路配置
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。