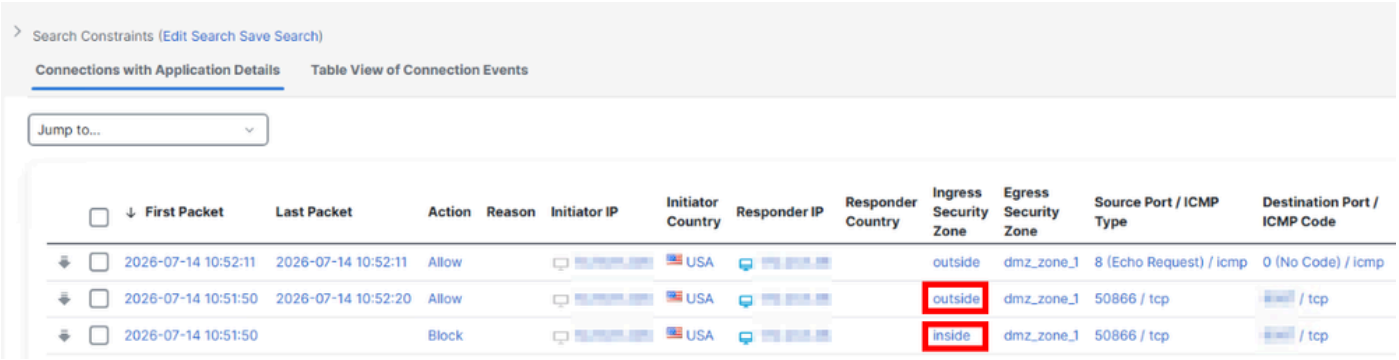
Fehlerbehebung: FTD Asymmetric Routing, das TCP-Verluste und Dual-Zone-Verbindungsprotokolle verursacht

Inhalt

Problem

Eingehende Verbindungen zu einer DMZ-gehosteten Anwendung hinter einem Cisco Secure Firewall Threat Defense (FTD) HA-Paar zeigen zeitweise zwei Sicherheitszonen als Datenverkehrsquelle für denselben Verbindungsversuch an. FMC-Verbindungsereignisse zeigen die erwartete zulässige Verbindung von der externen Zone an, gefolgt von verweigertem Datenverkehr, der der internen Zone zugeordnet ist, was zu einer fehlerhaften TCP-Verbindung führt.



- Die FTD-Route und die Paket-Tracer bestätigen das korrekte Routing, NAT und die Regeln zwischen Quelle und Ziel.
- Das FTD-`System unterstützt` jedoch nur `Trace`, um eingehende Pakete von der Quelle anzuzeigen, aber keinen zurückkehrenden Datenverkehr vom Ziel.

<#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,
```

- Die Verbindung mit dem Host wird irgendwann unterbrochen.
- Die Erfassungen an der FTD-Schnittstelle "outside" bestätigen, dass 10.x.x.200 eine SYN- und Echo-Anforderung an die externe Ziel-IP-Adresse 10.x.x.220 sendet.

<#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
```

- Der FTD UNNAT sendet diese an die interne Ziel-IP-Adresse 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
```

- Die FTD lässt den Datenverkehr wie vorgesehen mit der entsprechenden Allow-Regel zu.

<#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
```

- Derselbe Datenverkehr wird dann korrekt an der Schnittstelle "dmz_zone_1" an das DMZ-Ziel 172.x.x.36 weitergeleitet.

<#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
```

- Die Erfassungen auf der FTD-dmz_zone_1-Schnittstelle bestätigen, dass 10.x.x.200 eine SYN- und Echoanfrage an die interne Ziel-IP 10.x.x.220 sendet.

<#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
```

- Die FTD-dmz_zone_1-Schnittstelle zeigt jedoch nie Datenrückverkehr von der internen Ziel-IP 172.x.x.36 an.
- Captures bestätigen, dass das Ziel 172.x.x.36 SYN, ACK und Echo Reply kommen auf FTD innerhalb Schnittstelle statt.

<#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
```

- Da das Ziel SYN,ACK an der falschen Schnittstelle zurückgegeben wird, verwirft die FTD den Datenverkehr, da es sich um ein Anfangspaket handelt, das keine SYN ist.

Anmerkung: Andere TCP-Übertragungen können aufgrund von asymmetrischem Routing auftreten und sind in der FTD-`Ausgabe mit asp`-Übertragungen zu sehen.

<#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
```

Umwelt

- Cisco Secure Firewall Threat Defense - alle Modelle und Versionen
- Cisco Secure Firewall Management Center Alle Modelle und Versionen
- Ein externes Routing-Gerät oder ein Proxy, das bzw. der neben dem FTD konfiguriert ist und denselben Datenverkehr beeinträchtigt.

Auflösung

1. Beheben Sie das asymmetrische Routing-Verhalten am Gerät, das den zurückfließenden Datenverkehr an die falsche FTD-Schnittstelle sendet.

2. Konfigurieren Sie andernfalls die TCP-Zustandsumgehung, um zu versuchen, das asymmetrische Routing aufzulösen.

- Dadurch kann die Firewall TCP-Sitzungen verarbeiten, bei denen eingehende und ausgehende Pakete an verschiedenen Schnittstellen eingehen.
- Der Bypass deaktiviert bestimmte Stateful-Prüfungen, die in asymmetrischen Routing-Szenarien zu Verlusten führen, muss jedoch aufgrund von Sicherheitsabwägungen vorsichtig und selektiv verwendet werden.
- Beachten Sie, dass es sich hierbei um einen Versuch handelt, asymmetrisches Routing zu umgehen, das außerhalb des FTD verursacht wird, und dass es am besten ist, diesen Faktor als primären Schritt zu beheben.

TCP-Statusprüfungen für asymmetrisches Routing umgehen (TCP-Statusumgehung): 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-Zustandsprüfungen für asymmetrisches Routing umgehen (TCP-Zustandsumgehung): https://www.youtube.com/watch?v=v6vJUpPqdYk

Ursache

Das Problem wurde durch asymmetrisches Routing außerhalb der FTD-Firewall verursacht. Eingehende Pakete gelangten über die outside_primary-Schnittstelle in die Firewall und wurden

korrekt an das Ziel auf dmz_zone_1 weitergeleitet, aber die zurückkehrenden Pakete von 172.x.x.36 kamen auf der FTD-internen Schnittstelle zurück, anstatt auf der erwarteten dmz_zone_1-Schnittstelle.

Da der zurückkehrende Datenverkehr an einer anderen Schnittstelle ankam als der ursprüngliche Datenstrom, behandelte die Stateful Inspection-Engine der FTD die Pakete als ungültig und verwarf sie mit dem Verwerfungsgrund "tcp-not-syn First TCP packet not SYN". Dieses Verhalten wird für die Stateful-TCP-Prüfung erwartet, wenn über mehrere Schnittstellen hinweg asymmetrisches Routing stattfindet.

Verwandte Inhalte

- TCP-Statusprüfungen für asymmetrisches Routing umgehen (TCP-Statusumgehung)
- FTD: So aktivieren Sie die Konfiguration der TCP-Zustandsumgehung mithilfe der FlexConfig-Richtlinie
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.