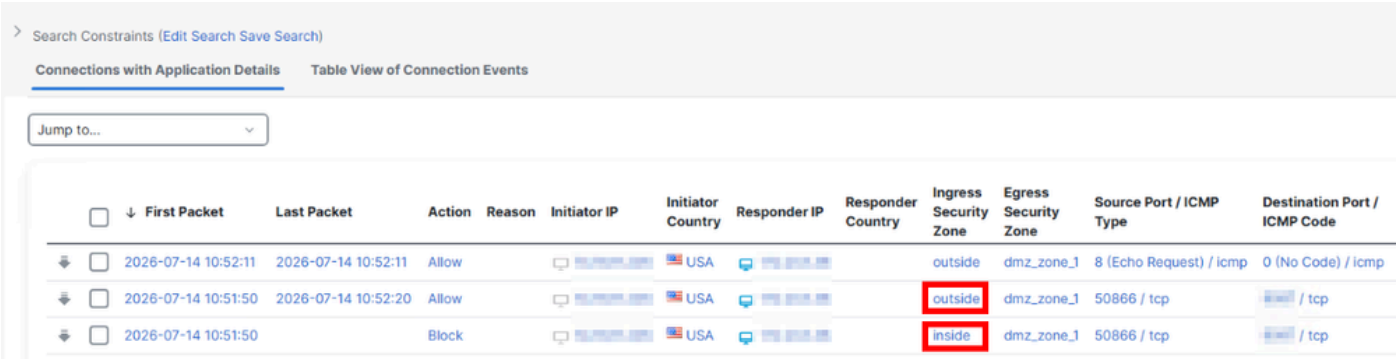
أستكشاف أخطاء التوجيه غير المتماثل لـ FTD وإصلاحها مما يتسبب في عمليات إسقاط TCP وسجلات الاتصال ثنائية المناطق

المحتويات

مسألة

تظهر الاتصالات الواردة بتطبيق مستضاف من DMZ خلف زوج HA الخاص بالدفاع الآمن عن تهديد جدار الحماية (FTD) من Cisco بشكل متقطع منطقتين أمنيا كمصدر حركة مرور لمحاولة الاتصال نفسها. تعرض أحداث اتصال FMC الاتصال المتوقع المسموح به من المنطقة الخارجية، متبوعة بحركة المرور المرفوضة المقترنة بالمنطقة الداخلية، مما يؤدي إلى فشل اتصال TCP.



- يؤكد مسار FTD و Packet-tracers التوجيه الصحيح، و NAT، والقواعد بين المصدر والوجهة.
- ومع ذلك، فإن تتبع دعم اظن م FTD يعرض الحزم الواردة من المصدر فقط، ولكنه لا يرجع حركة مرور البيانات من الوجهة.

```
<#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_allow
```

```
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 flags
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 = 268434433
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 flags 0
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 rev_id
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 = 268434459

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, logFl
```

- من المضيف، يصل الاتصال في نهاية المطاف إلى وقت التوقف.
- بعد تأكيد عمليات الالتقاط الموجودة على واجهة FTD "الخارجية" أن 10.x.x.200 يرسل طلب SYN و Echo إلى الوجهة الخارجية 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 <mss
3: 13:59:06.073009       10.x.x.200.39194 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535 <mss
4: 13:59:10.081477       10.x.x.200.39194 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535 <mss
5: 13:59:18.090876       10.x.x.200.40812 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535 <mss

6: 13:59:24.127984       10.x.x.200 > 10.x.x.220 icmp: echo request
```

- قم بإلغاء هذا الأمر إلى عنوان IP للوجهة الداخلية 172.x.x.36. يقوم FTD بـ

<#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
```

- يسمح FTD لحركة المرور باستخدام قاعدة السماح المناسبة كما هو مطلوب.

```
<#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_zone_1 ob
     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,
```

- ثم تنتقل حركة المرور نفسها بشكل صحيح إلى المخرج على واجهة "dmz_zone_1" تجاه وجهة 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
```

- و SYN بلط لسري 10.x.x.200 نأ FTD dmz_zone_1 ةهجاو على طاقتلالا تايلمع دكؤت 10.x.x.220. IP ةيلخادلا ةهجولا ىلإ Echo

<#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 1245309079:124530907

2: 13:59:04.063610 802.1Q vlan#600 P0 10.x.x.200.39194 > 172.x.x.36.9997: S 1245309079:1245309
3: 13:59:06.073146 802.1Q vlan#600 P0 10.x.x.200.39194 > 172.x.x.36.9997: S 1245309079:1245309
4: 13:59:10.081630 802.1Q vlan#600 P0 10.x.x.200.39194 > 172.x.x.36.9997: S 1245309079:1245309
5: 13:59:18.091166 802.1Q vlan#600 P0 10.x.x.200.40812 > 172.x.x.36.9997: S 1210202278:121020

6: 13:59:24.128197 802.1Q vlan#600 P0 10.x.x.200 > 172.x.x.36 icmp: echo request

- IP ةيلخادلا ةهجولا نم عاجرإلا رورم ةكرح ضرعت ال FTD dmz_zone_1 ةهجاو نإف ،كلذ عمو 172.x.x.36.
- ةهجاو على يتأت Echo Reply و ACK و syn 172.x.x.36 ةهجولا نأ طاقتلالا تايلمع دكؤت .كلذ نم الدب ةيلخادلا 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 3938871380:393887138

2: 13:59:03.051938 802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:1245309
3: 13:59:03.051968 802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:1245309

4: 13:59:04.063839 802.1Q vlan#667 P0 172.x.x.36.9997 > 10.x.x.200.39194: S 3938871380:393887

5: 13:59:04.063915 802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:1245309
6: 13:59:04.064068 802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:1245309
.....

23: 13:59:24.128411 802.1Q vlan#667 P0 172.x.x.36 > 10.x.x.200 icmp: echo reply

- بما أن الراية syn، ACK يرجع على المسار غير صحيح، لـ FTD يسقط الحزمة بما أن syn ليس هو تعيين كربط أولي أن.

ملاحظة: يمكن أن تحدث عمليات إسقاط TCP الأخرى بسبب التوجيه غير المتماثل ويمكن رؤيتها في إخراج إسقاط ASP لـ 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
```

البيئة

- الدفاع الآمن عن جميع النماذج والإصدارات عن تهديد جدار الحماية من Cisco
- مركز إدارة جدار الحماية الآمن من Cisco بجميع الطرز والإصدارات
- جهاز توجيه خارجي أو وكيل تم تكوينه بجوار FTD يؤثر على حركة المرور نفسها.

قرار

1. حل سلوك التوجيه غير المتماثل في الجهاز الذي يرسل حركة مرور الإرجاع إلى واجهة FTD الخطأ.

2. وإلا، فعليك تكوين تجاوز حالة TCP لمحاولة حل التوجيه غير المتماثل.

- وهذا يسمح لجدار الحماية بمعالجة جلسات عمل TCP التي تحتوي على حزم واردة وصادرة تصل على واجهات مختلفة.
- يؤدي السماح إلى تعطيل بعض عمليات التحقق من الحالة التي تتسبب في حالات انخفاض في سيناريوهات التوجيه غير المتماثلة، ولكن يجب إستخدامها بحذر وانتقائية بسبب مقايضات الأمان.
- حل الأفضل من FTD، ومن الجانب خارج التوجيه غير المتماثل للعمل على هذه محاولة للعمل اعلم أن ذلك العامل كخطوة أساسية.

تجاوز فحوصات حالة TCP للتوجيه غير المتماثل (تجاوز حالة 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

[video] تجاوز فحص حالة TCP للتوجيه غير المتماثل (تجاوز حالة TCP):
https://www.youtube.com/watch?v=v6vJUpPqdYk

السبب

حدثت المشكلة بسبب التوجيه غير المتماثل الخارجي لجدار حماية FTD. دخلت الحزم الواردة إلى جدار الحماية من خلال الواجهة الخارجية_الأساسية وتمت إعادة توجيهها بشكل صحيح إلى واجهة FTD داخل الوجهة على dmz_zone_1، ولكن الحزم العائدة من 172.x.x.36 وصلت مرة أخرى إلى واجهة مختلفة عن التدفق الأصلي، فإن محرك فحص حركة المرور العائدة على واجهة dmz_zone_1 المتوقعة.

نظرا لوصول حالة الحالة ل FTD تعامل الحزم كغير صحيحة وأسقطها باستخدام سبب الإسقاط "tcp-not-syn" أوأول حزمة TCP ليست SYN". من المتوقع أن يحدث هذا السلوك لفحص TCP الذي يحدد الحالة عندما يحدث التوجيه غير المتماثل عبر الواجهات المتعددة.

المحتوى ذي الصلة

- [تجاوز فحوصات حالة TCP للتوجيه القياسي (تجاوز حالة TCP)]
- [برنامج FTD: كيفية تمكين تكوين تجاوز حالة TCP باستخدام سياسة FlexConfig]
- [الدعم الفني والتنزيلات من Cisco]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).