أستكشاف أخطاء نظام FTD Cluster وإصلاحها مما يتسبب في حدوث Asymmetric حالات فشل في اتصال TCP

مسألة

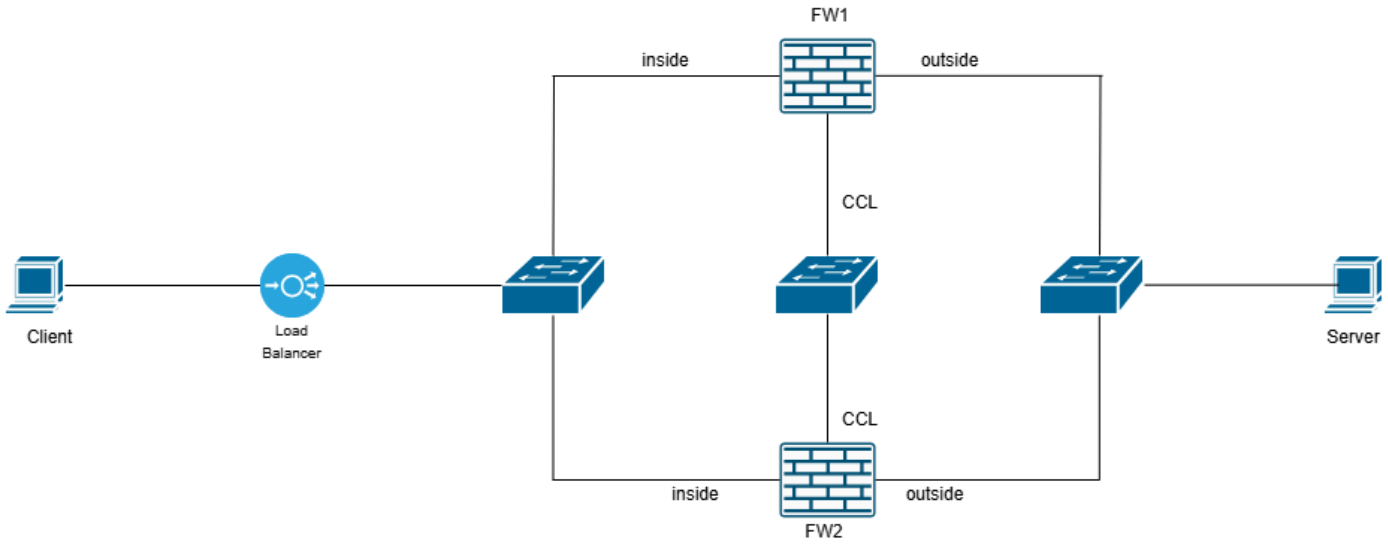
قد تظهر واحدة أو أكثر من هذه الأعراض:

- حالات انقطاع متقطعة في الاتصال للتطبيقات التي تتجاوز مجموعة FTD.
- يفشل تأكيد اتصال TCP الثلاثي أثناء محاولات الاتصال.
- يرسل العميل حزمة SYN، ولكنه لا يتلقى إستجابة SYN-ACK المتوقعة.
- يرسل العميل حزمة RST بعد النظام الأولي.

البيئة

- شوهد أول مرة في برنامج Secure Firewall Threat Defense 7.4 — يمكن أن تتأثر نسخ أخرى أيضا
- تكوين نظام المجموعة
- موازن التحميل في مسار الشبكة — هذا إختياري

المخطط



inline_image_0.png

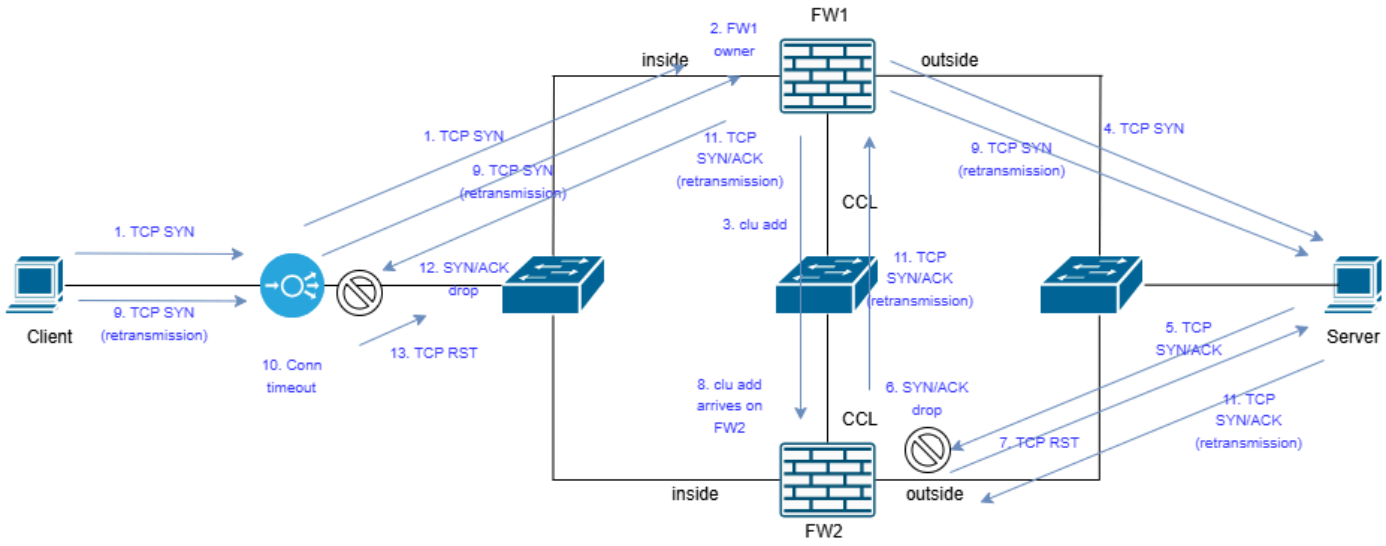
قرار

لتقرير المشكلة تحتاج إلى التقاط صور متزامنة في هذه النقاط:

- FW1 داخلي قارن (مع reinject-hide)
- FW1 الواجهة الخارجية (مع reinject-hide)
- واجهة مجموعة FW1 (CCL)
- واجهة FW2 الداخلية (مع reinject-hide)
- الواجهة الخارجية FW2 (with reinject-hide)
- واجهة نظام المجموعة ل FW2 (CCL)
- العميل (أو أقرب ما يمكن إلى العميل)
- الخادم (أو أقرب ما يمكن إلى الخادم)

للحصول على تفاصيل حول كيفية تكوين فحص الالتقاط: كيفية تمكين مجموعات نظام المجموعة.

تكشف عمليات الالتقاط التي تم التقاطها على جدران الحماية إلى جانب العميل والخادم عن هذه الطوبولوجيا:



inline_image_0.png

1. يرسل العميل TCP syn. تصل الحزمة إلى موازن التحميل (LB) ويتم إرسالها إلى FW1.

2. يستلم FW1 حزمة TCP syn ويصبح مالك التدفق.

3. يقوم FW1 بإبلاغ المدير (FW2) عن مالك التدفق من خلال إرسال رسالة نظام مجموعة خاصة (CLU add).

4. يرسل FW1 نظام TCP إلى الخادم الوجهة.

ملاحظة: تحدث الخطوتان 3 و 4 بدون ترتيب محدد.

5. يرد الخادم مع SYN/ACK. في هذه الحالة، لدينا تدفق غير متماثل منذ أن تم إرسال SYN/ACK إلى FW2 بسبب خوارزمية موازنة حمل قناة المنفذ.

6. يصل SYN/ACK إلى FW2 قبل إضافة رسالة CLU. هذا شرط عرقي وبيئي محض (مثل زمن الوصول في CCL). وبما أن FW2 لا يعرف من هو مالك التدفق، يتم إسقاط SYN/ACK.

7. يتم إرسال TCP RST إلى الخادم.

8. تصل رسالة إضافة clu إلى FW2.

9. يرسل العميل حزمة TCP syn. تتم إعادة توجيه حزمة TCP syn إلى الخادم الوجهة.

10. في LB، ينتهي اتصال TCP الخاص بالتدفق المحدد.

11. عم مداخلا دري SYN/ACK (إلاسرإ ةداعإ TCP). لصت ةمزح SYN/ACK إلى FW2. هذه ةرملا، فرعي FW2 عن كلامال قفدتلا هنأل حصل ىلع ةلاسرلا ةفاضإ CLU متيو ةداعإ هيجوت SYN/ACK إلى كلامال قفدتلا ربع CCL. متي إلاسرإ SYN/ACK إلى ليمعلا.

12 - فرعت الو ةكرشلا ةيربيللا نع اذه قفدتلاو يقلتي ماظن SYN/ACK، نمو ،مث ال لصي ماظنلا/ACK أبدا إلى ليمعلا.

13. LB دحاو وأ رثكأ نم مزح TCP RST.

عبتتلا ليلحت مادختساب ةيامحلا رادج طاقتلالا

تاهجاولاو CCL تاهجاو ىلع ةيامحلا رادج نم طاقتلالا تايلمع عيمجت مت ،تاجرخملا هذه يفو مداخلا هجاوت يتلا.

· ىلع CCL نوكي طاقتلالا ىلع ذفنم UDP 4193.

· رايخ مادختساب ةيانلا طاقن نيب TCP رورم ةكرح طاقتلالا قباطي ،تانايبلا تاهجاو ىلع لعفلاب مزحلا لصت نيأ ىرن نأ ديرن اننأ وه ببسلا .hide-جاردإلا.

· ناونع IP 192.0.2.65 = ليمعلا

· ناونع IP 192.0.2.6 = مداخلا

ةوطخلا 1: مدختسأ اذه رمألا ىلع زاهج رادج ةيامحلا يذلا يحصل ىلع SYN/ACK ةفرعملو تقو ةفاضإ ك ةلاسرلا ضرع متي (CLI) رماوألا رطس ةهجاو جارخإ يف .CLU ةفاضإ ةلاسر لوصو قفدت.

```
Firepower# ضرع طاقتلال CCL ريفشت كف

ةمزِح 3 طاقتلا مت

1: 08:14:20.630521 127.2.1.1.51475 > 127.2.2.1.4193: udp 820

ةلاسر ASP ماظنل ةعومجملا: لسرملا: 1، ملتسملا: 0

إضافة تدفق: كلاملا 1، ريدملا 0، خسنلا يطايتحالا 0،

IFC_IN (7020a7) و IFC_OUT (7020a7)
```

TCP SRC 192.0.2.65/37468, dest 192.0.2.6/80

الخطوة 2: تتبع حزمة SYN/ACK والتركيز على الطابع الزمني ونتيجة التتبع:

Firepower# show capture CAPI Packet-Number 1 تتبع

تم التقاط 13 حزمة

1: 08:14:20.628690 802.1Q vlan#200 P0 192.0.2.6.80>192.0.2.65.37468: S 2524735158:2524735158(0) ACK 2881263901 win 651660 <mss 1460،sackOK،timestamp 611712900 970937593،nop،wscale 7>

المرحلة: 1

النوع: التقاط

النوع الفرعي:

النتيجة: السماح

وقت المنقضي: 1708 نانو ثانية

التكوين:

معلومات إضافية:

MAC إلى الوصول قائمة

المرحلة: 2

النوع: قائمة الوصول

النوع الفرعي:

النتيجة: السماح

ةينانث ونان 1708 :يضقنملا تقولا

:نيوكتلا

ةينمض ةدعاق

:ةيفاضإ تامولعم

MAC ىلإ لوصولا ةمئاق

3 :ةلحرملا

input-route-lookup :عونلا

جورخلا ةهجاو لح :يعرفلا عونلا

حاسملا :ةجيتنلا

ةينانث ونان 13664 :يضقنملا تقولا

:نيوكتلا

:ةيفاضإ تامولعم

Egress IFC Inside (vrfid:0) مادختساب 192.168.200.140 ةيلاتلا ةوطخلا ىلع روثعلا مت

4 :ةلحرملا

Cluster-event :عونلا

:يعرفلا عونلا

حاسملا :ةجيتنلا

ةينانث ونان 16104 :يضقنملا تقولا

:نيوكتلا

:ةيفاضإ تامولعم

'Inside' :لاخدإلا ةهجاو

قفدت دجوي ال :قفدتلا عون

كلاملا حبصأس (0) نأ

5 :ةلحرملا

object_group_search :عونلا

:يعرفلا عونلا

حاسملا :ةجيتنلا

ةينات ونان 19520 :يضقنملا تقولا

:نيوكتلا

:ةيفاضإ تامولعم

0 :ردصملا تانئاك ةعومجم ةقباطم ددع

0 :ردصملا NSG ةقباطم تارم ددع

0 :ةهجولل NSG ةقباطم تارم ددع

1 :فينصتلا لودج نع ثحبلا ددع

1 :ثحبلا ددع يلامجإ

0 :حيتافملا چوز ددع رارکت

4 :لودجلا ةقباطم ددع فينصت

6 :ةلحرملا

لوصولا ةمئاق :عونلا

:يعرفلا عونلا

حاسلا :ةجيتنلا

ةينات ونان 366 :يضقنملا تقولا

:نيوكتلا

access-group CSM_FW_ACL_ global

id 268436480-ةدعاق يأ ip مدقتم حيرصت _CSM_FW_ACL list-لوصولا

يضارتفالا - mzafiro_blank :لوصولا جهن: rule-id 268436480 ةظحالم access-list CSM_FW_ACL_

يضارتفالا عارجإلا ةدعاق :L4 ةدعاق rule-id 268436480: ةظحالم access-list csm_fw_acl_

:ةيفاضإ تامولعم

مكحلا ىلإ لوصولا متيس ثيح ةجلاعملا نم ديزملا ريشلا ىلإ ةمزحلا هذه لاسرإ متيس

7 :ةلحرملا

conn-settings :عونلا

:يعرفلا عونلا

حاسلا :ةجيتنلا

ةينات ونان 366 :يضقنملا تقولا

:نيوكتلا

ةئفلا ةطيرخل TCP لوكوتورب

لوصولا ةمئاقب صاخلا TCP لوكوتورب قباطت

ةساي سلا_ةمدخلا ةمدخلا ةساي سلا ةطيرخ

class tcp

set connection conn-max 0 جنيني-conn-max 0 random-sequence-number disable syn-cookie-mss 1380

policy-service-policy_يموموع

:ةيفاضإ تامولعم

8 :ةلحرملا

NAT :عونلا

ةسلج لكل :يرفلا عونلا

حامسلا :ةجيتنلا

ةينا ثوان 366 :يضقنملا تقولا

:نيوكتلا

:ةيفاضإ تامولعم

9 :ةلحرملا

IP تارايخ :عونلا

:يرفلا عونلا

حامسلا :ةجيتنلا

الوقت المنقضي: 366 ثانية ونان

التكوين:

معلومات إضافية:

النتيجة:

واجهة الإدخال: INSIDE(vrfid:0)

حالة الإدخال: لأعلى

حالة خط الإدخال: لأعلى

واجهة الإخراج: Inside(vrfid:0)

حالة الإخراج: لأعلى

حالة خط الإخراج: لأعلى

الإجراء: drop

الوقت المستغرق: 54168 ثانية ونان

سبب الإسقاط: (tcp-not-syn) أول حزمة TCP ليست SYN، drop-location: إطار snp_sp:7459 flow (NA)/NA

النقاط الرئيسية

- في اقباس SYN/ACK ~2 msec كان بينما 08:14:20.630521 إلى تدفق إضافة رسالة وتلت 08:14:20.628690. هذه هي حالة السباق.

- في هذه الحالة. تم إسقاط حزمة SYN/ACK بواسطة جدار الحماية بسبب TCP-not-syn ASP. في هذه الحالة، أن جدار الحماية لم يحدد ما إذا كان هناك مالك تدفق معروف أم لا، وبالتالي، حاول جدار الحماية المرحلة 4 أن يصبح مالك تدفق.

يظهر هذا الإخراج مسارا ل SYN/ACK عندما يعرف جدار الحماية التدفق:

تتبع Firepower# show capture CAPI Packet-Number 3

تم التقاط 13 حزمة

3: 08:14:21.629560 802.1Q vlan#200 P0 192.0.2.6.80>192.0.2.65.37468: S
2540375172:2540375172(0) ACK 2881263901 win 651660 <mss 1460،sackOK،timestamp 611713901
970938595،nop،wscale 7>

المرحلة: 1

النوع: التقاط

النوع الفرعي:

النتيجة: السماح

الوقت المنقضي: 1708 نانو ثانية

التكوين:

معلومات إضافية:

MAC إلى الوصول قائمة

المرحلة: 2

النوع: قائمة الوصول

النوع الفرعي:

النتيجة: السماح

الوقت المنقضي: 1708 نانو ثانية

التكوين:

قاعدة ضمنية

معلومات إضافية:

قائمة الوصول إلى MAC

المرحلة: 3

النوع: Cluster-event

النوع الفرعي:

النتيجة: السماح

الوقت المنقضي: 3416 نانو ثانية

التكوين:

معلومات إضافية:

واجهة الإدخال: 'Inside'

نوع التدفق: كعب روتين

لدي (0) تدفق، مالك صالح (1).

المرحلة: 4

النوع: الالتقاط

النوع الفرعي:

النتيجة: السماح

الوقت المنقضي: 7808 نانو ثانية

التكوين:

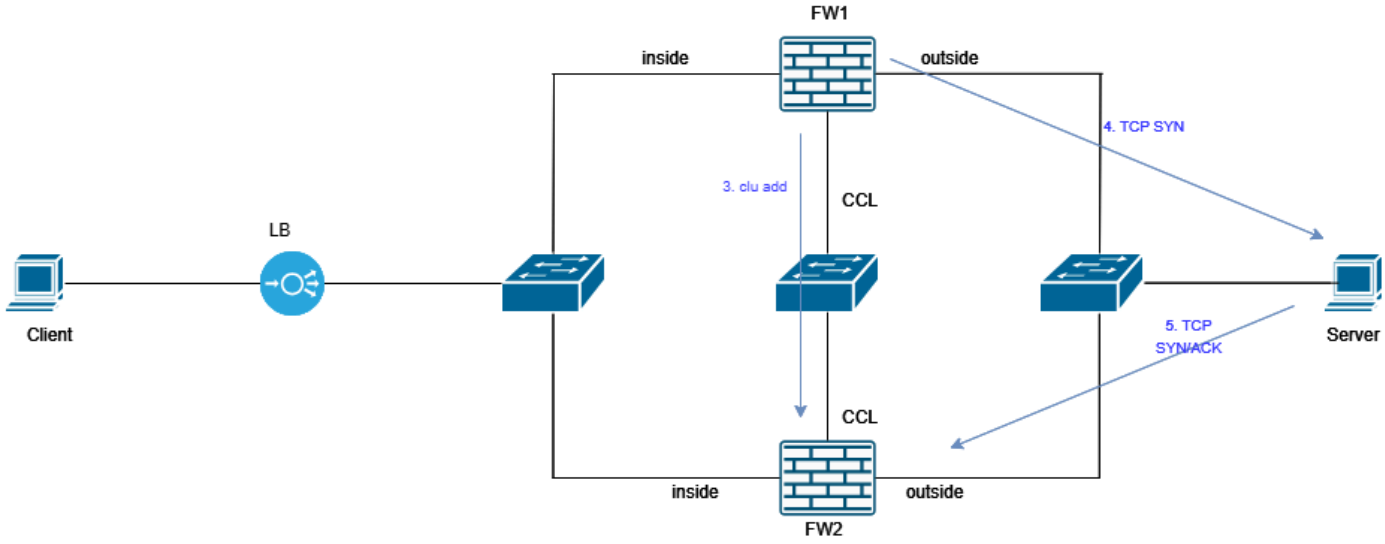
```
معلومات إضافية:

قائمة الوصول إلى MAC

النتيجة:

واجهة الإدخال: INSIDE(vrfid:0)

حالة الإدخال: ألعلى

حالة خط الإدخال: للأعلى

الإجراء: السماح

الوقت المستغرق: 14640 نانو ثانية

تم عرض حزمة واحدة

Firepower#
```

النقطة الأساسية في المرحلة 3. يعرف جدار الحماية أن وحدة نظام المجموعة 1 هي مالك الجلسة والجهاز الذي هو الوحدة 0 لمعرفة الجهاز الذي يمكنك إستخدام الأمر show cluster info .تدفق. الوحدة 1.

الأسئلة المتكررة

س. لماذا نرى مشكلات اتصال TCP المتقطعة؟

أ. بما أن هذه هي حالة عرقية، فإنها تحدث عشوائيا. ويمكن تصوير حالة السباق تبعا لذلك:

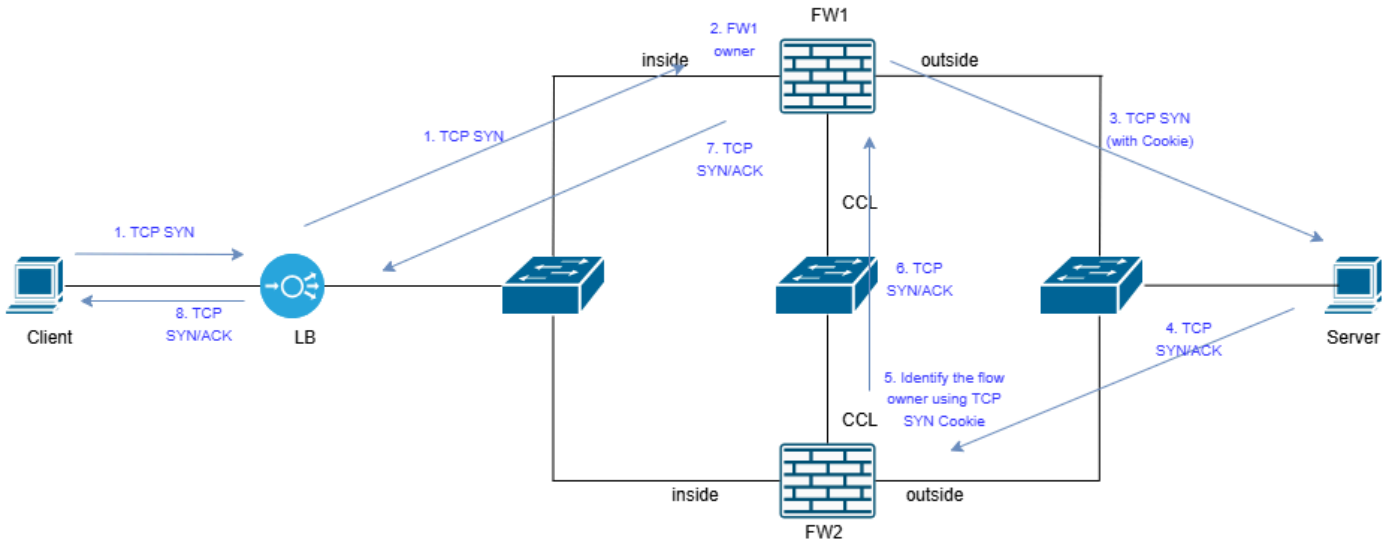


inline_image_0.png

س. ما هي الحلول الممكنة لتجنب حالة السباق؟

ج.

الحل 1: تمكين تحويل رقم تسلسل TCP عشوائيا للاستفادة من آلية ملف تعريف إرتباط TCP SYN. في هذه الحالة يتم تنظيم الاتصال وفقا لذلك:



inline_image_1.png

الحل 2: تخلص من عدم التناظر في الشبكة. أولا، تحتاج إلى تحديد سبب عدم التناظر. قد يتطلب ذلك ضبط خوارزمية موازنة حمل قناة المنفذ، وإعادة توصيل كبلات قناة المنفذ بترتيب مختلف، من بين أمور أخرى.

السبب

السبب الجذري هو حالة سباق ناجمة عن عدم تناسق نظام المجموعة داخل نشر نظام المجموعة مختلفة عن FTD. تتم معالجة حزم SYN-ACK من الخادم بواسطة عقدة نظام مجموعة FTD في .FTD التي عالجت حزمة SYN الأولية، مما يمنع إنشاء جلسة TCP المتناسبة.

المحتوى ذي الصلة

- 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).