أستكشاف أخطاء المصادقة المستندة إلى شهادة نقطة الوصول وإصلاحها من خلال FTD

مسألة

يتم الإبلاغ عن هذه الأعراض بعد ترحيل جهاز الأمان القابل للتكيف طراز 5508 من Cisco إلى برنامج Cisco Secure Firewall (CSF) Threat Defense (FTD) 1230 في الفرع الرئيسي (HQ):

1. تفشل نقاط الوصول (AP) الموجودة في المكاتب الفرعية في المصادقة على خادم RADIUS في HQ باستخدام مصادقة الشهادة.

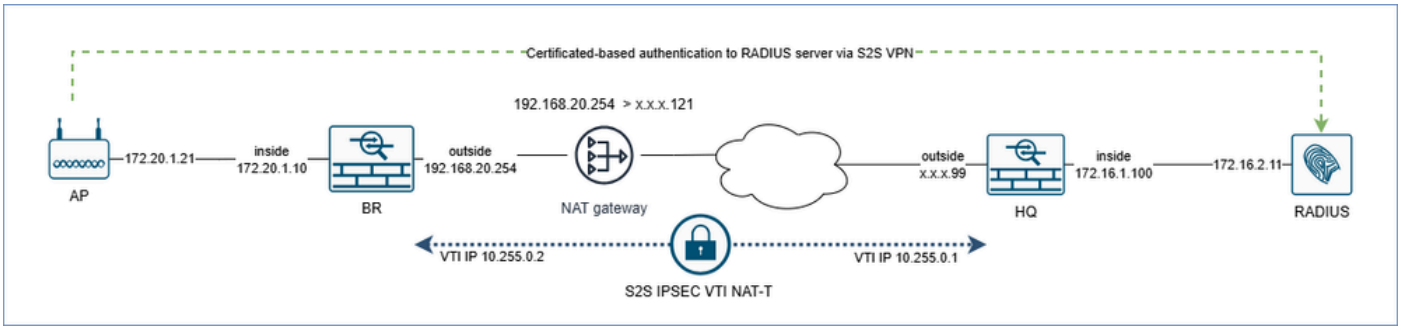
2. المصادقة باسم المستخدم وكلمة المرور ناجحة.

وتلاحظ الأعراض على نقاط الدخول في جميع الفروع.

البيئة

برنامج CSF 1230 المدار من قبل FMC في تكوين عالي التوافر يشغل الإصدار 7.7.10.1 في HQ وبرنامج Firepower 1010 المستقل المتعدد الذي يشغل الإصدار 7.4.2.4 في الفروع، يمكن أن يتأثر إصدار البرامج الأخرى أيضا. الأعراض في هذه الحالة هي عقم الجهاز.

المخطط



inline_image_0.png

النقاط الرئيسية حول الطوبولوجيا:

- BR ةيامح رادجل ةيعرفلا ةكبشلا يف لوصولا ةطقن نوكت ،ةكبشلا ةقبط يف (عرفلا) لخاد ةهجاولا.
- ماع ناونع ىلإ ةهجاولل IP ناونع جراخ BR ةيامح رادج ةمجرتب NAT ةباوبك هجوملا موقي ىلع ةدحاو ةطقن رادقمب HQ ةيامح رادج نع دعبي BR ةيامح رادج نأ ينعي اذهو .x.x.x.121 لقألا.
- نم (S2S VPN) ةيرهاظلا ةصاخلا تاكبشلا مادختساب BR و HQ ةيامح ناردج ليصوت متي نامألا ةلومح نيمضت عم (IPsec) تنرتنإلا لوكوتورب نامأ مادختساب عقوم ىلإ عقوم (ESP) ةهجاوو قفنلا ةيرهاظلا (VTI) ربع NAT.
- لخاد HQ ةيامح رادجل ةيعرفلا ةكبشلا يف RADIUS مداخ دجوي ،ةكبشلا ىوتسم ىلع ةهجاولا.

رارق

للتحليل التقني، تم تجميع مجموعات الحزم من جدران الحماية في المقر الرئيسي وبي آر.

على مستوى بيانات جدار الحماية HQ و BR، يتم التقاط/طرح البيانات على الواجهات المادية، والتقاط على واجهات VTI، يلتقط إسقاط ASP لحركة المرور الداخلية والخارجية استنادا إلى عنوان IP النظير:

جدار حماية BR:

```
cap br_inside interface inside packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16
cap br_vti interface vti-hq packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16.2.
cap br_asp match ip host x.x.x.99 any
cap br_asp match ip host 172.20.1.21 host 172.16.2.11
cap br_outside interface outside packet-length 9000 buffer 33554400 match ip host x.x.x.99 any
```

لاحظ أنه يتم إستبدال x.x.x.99 بعنوان IP حقيقي.

جدار حماية HQ:

```
cap hq_inside interface inside packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16
cap hq_vti interface vti-br packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16.2.
cap hq_asp match ip host x.x.x.121 any
cap hq_asp match ip host 172.20.1.21 host 172.16.2.11
cap hq_outside interface outside packet-length 9000 buffer 33554400 match ip host x.x.x.121 any
```

ظحال نأ هنم متي إستبدال x.x.x.121 ناونعب IP يلعف.

بالإضافة إلى ذلك، تم توصيل رادج ةيامحلا دوجوملا يف رقملا (HQ) عمجب تاعومجم تالوحملا تاهجاو عيمجو يجراخلا مسالا ىلإ ادانتسا لكيهلا تاهجاو يف هاجتإلا ةيئانث ةيلخادلا تالصولا:

```
cap hqfxos switch interface outside direction both packet-length 2048 match ip x.x.177.121
cap hqfxos switch interface in_data_uplink1 direction both packet-length 2048 match ip x.x.x.121
cap hqfxos switch interface in_data_uplink2 direction both packet-length 2048 match ip x.x.x.121
cap hqfxos switch interface in_data_uplink3 direction both packet-length 2048 match ip x.x.x.121
no cap hqfxos switch stop.
```

ينف ليلحت

HQ ةيامح رادج

1. متي هنأ ىلإ HQ ةيامح رادج يف (ASP) عيرسلا نامألا راسم طاقسإ تاليجست ريشت ءزجلا عيمجت ةداعإ لشف يف ببسلا دوجو عم ءازجألا طاقسإ:

<#root>

```
>

show capture hq_asp

Target:     OTHER
Hardware:   CSF-1230
Cisco Adaptive Security Appliance Software Version 99.23(37)127
ASLR enabled, text region aaaae5d50000-aaaae902d504
172.20.1.21.38676 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (

fragment-reassembly-failed

) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
172.20.1.21.38676 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (

fragment-reassembly-failed

) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
172.20.1.21.56952 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (

fragment-reassembly-failed

) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
```

2. ديزي عداد المهلة لواجهة VTI في إخراج الأمر show fragment في جدار حماية HQ:

<#root>

```
>

show fragment

Interface: vti-br
Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
Run-time stats: Queue: 0, Full assembly: 0
Drops: Size overflow: 0,

Timeout: 1217

,
Chain overflow: 0, Fragment queue threshold exceeded: 0,
Small fragments: 0, Invalid IP len: 0,
Reassembly overlap: 0, Fraghead alloc failed: 0,
SGT mismatch: 0, Block alloc failed: 0,
Invalid IPV6 header: 0, Passenger flow assembly failed: 0
Cluster reinsert collision: 0
```

وفقا لمرجع الأمر (https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html#wp4144096608)، فإن المهلة هي "الحد الأقصى لعدد الثواني التي تنتظر وصول الحزمة المجزأة بالكامل". القيمة الافتراضية هي 5 ثوان. وهذا يعني أنه إذا لم تصل سلسلة الأجزاء بأكملها إلى جدار الحماية في غضون 5 ثوان، سيتم إسقاط الأجزاء المستلمة، ويفشل إعادة تجميع الأجزاء.

3. استنادا إلى النقطة السابقة، لا يتلقى جدار حماية HQ سلسلة التجزئة الكاملة التي ينتج عنها فشل إعادة تجميع الأجزاء.

جدار حماية BR

1. استنادا إلى عمليات االلتقاط، ترسل نقطة الوصول طلب مصادقة مستند إلى شهادة RADIUS في جزأين منفصلين إلى جدار حماية BR. يظهر االلتقاط br_inside من نيتردشذ المدخل من 1514 بايت و475 بايت على التوالي. رأيت ال نفسه ربط في ال BR VTI قارن على أن يبدي ربط قبل تشفير:

172.20.1.21	172.16.2.11	IPv4			1514	0xf20b (61963)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20b) [Reassembled in #9]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20b (61963)	64	Access-Request id=255
172.20.1.21	172.16.2.11	IPv4			1514	0xf20c (61964)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20c) [Reassembled in #11]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20c (61964)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20d (61965)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20d) [Reassembled in #13]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20d (61965)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20e (61966)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20e) [Reassembled in #15]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20e (61966)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20f (61967)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20f) [Reassembled in #17]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20f (61967)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf210 (61968)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f210) [Reassembled in #19]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf210 (61968)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf211 (61969)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f211) [Reassembled in #21]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf211 (61969)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf212 (61970)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f212) [Reassembled in #23]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf212 (61970)	64	Access-Request id=255, Duplicate Request

inline_image_0.png

وحدة الإرسال القصوى (MTU) لواجهة BR الخارجية هي 1500 بايت. ولهذا السبب، يجب تجزئة الجزء الذي يحتوي على 1514 بايت إلى حزمتين قبل التشفير.

2. التقاط إسقاط ASP br_asp لحركة مرور RADIUS الداخلية على جدار حماية BR التي تعرض الحزم التي تم إسقاطها. في الوقت نفسه، لحركة المرور الخارجية، هناك عمليات إسقاط من حزم سعة 226 بايت مع سبب عدم توقع الحزمة:

```
<#root>

                                                                    firepower#

                                                                    show capture br_asp

                                                                      Target:     OTHER
                                                                    Hardware:   FPR-1010
                                    Cisco Adaptive Security Appliance Software Version 9.20(2)121
                                                ASLR enabled, text region 560817d6b000-56081d1ae26d
                                                                    103 packets captured
  1: 10:13:22.160239       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
  2: 10:13:23.160727       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
  3: 10:13:24.161200       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
```

192.168.20.254		.99	ESP	4500	4500	226	0x7254 (29268)	64	6275	ESP (SPI=0x1592a843)
192.168.20.254		.99	ESP	4500	4500	226	0x7e97 (32407)	64	6278 ✓	ESP (SPI=0x1592a843)
192.168.20.254		.99	ESP	4500	4500	226	0x0fc6 (4038)	64	6281 ✓	ESP (SPI=0x1592a843)
192.168.20.254		.99	ESP	4500	4500	226	0x3511 (13585)	64	6284 ✓	ESP (SPI=0x1592a843)
192.168.20.254		.99	ESP	4500	4500	226	0x5868 (22632)	64	6287 ✓	ESP (SPI=0x1592a843)

inline_image_1.png

لاحظ أن إخراج الأمر show capture br_asp يعرض 184 بايت من طول الحمولة، بينما يكون الطول الإجمالي لكل حزمة 226 بايت.

3. للتحقق من ما إذا كانت حزم ESP المسقطة ذات صلة بحركة المرور المتأثرة بين نقطة الوصول وخادم RADIUS أم لا، فقد تمت إعادة تشغيل التقاط br_inside في المختبر الداخلي باستخدام نفس تكوينات نهج الأمان من جدران حماية الموقع (HQ) و BR. يظهر التقاط br_vti من جهاز المختبر أجزاء 1514-بايت و475-بايت، أي قبل التشفير:

Source	Destination	Protocol	Sport	Dport	Length	IP ID	IP TTL	Info
172.20.1.21	172.16.2.11	IPv4			1514	0xe69d (59037)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69d) [Reassembled in #9
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69d (59037)	63	Access-Request id=218
172.20.1.21	172.16.2.11	IPv4			1514	0xe69e (59038)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69e) [Reassembled in #1
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69e (59038)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe69f (59039)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69f) [Reassembled in #1
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69f (59039)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a0 (59040)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a0) [Reassembled in #1
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a0 (59040)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a1 (59041)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a1) [Reassembled in #1
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a1 (59041)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a2 (59042)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a2) [Reassembled in #1
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a2 (59042)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a3 (59043)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a3) [Reassembled in #2
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a3 (59043)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a4 (59044)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a4) [Reassembled in #2
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a4 (59044)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a5 (59045)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a5) [Reassembled in #2
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a5 (59045)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a6 (59046)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a6) [Reassembled in #2
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a6 (59046)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a7 (59047)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a7) [Reassembled in #2
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a7 (59047)	63	Access-Request id=218, Duplicate Request

inline_image_2.png

4. تظهر عمليات التقاط br_outside نقص الحزم ذات 226 بايت والفجوة في أرقام تسلسل ESP بين الحزم ذات 562 بايت و 1506 بايت:

Source	Destination	Protocol	Sport	Dport	Length	IP ID	IP TTL	ESP Sequence	Wrong Sequence Number	Info
192.168.20.254	.99	ESP	4500	4500	1506	0x2d7e (11646)	64	6448		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x0b2c (2860)	64	6450	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x6ca9 (27817)	64	6451		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x51cf (20943)	64	6453	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x7d60 (32096)	64	6454		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x42de (17118)	64	6456	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x4553 (17747)	64	6457		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x7389 (29577)	64	6459	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x50f9 (20729)	64	6460		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x169f (5791)	64	6462	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	178	0x32d8 (13016)	64	6463		ESP (SPI=0x1592a843)

inline_image_3.png

النقاط الرئيسية:

- ASP جدار حماية BR في إسقاطه تم لأنه ،br_external التقاط في مفقود 226-byte باستخدام سبب إسقاط ASP للحزمة غير المتوقعة.
- يشرح إسقاط الحزمة الفجوة في أرقام تسلسل ESP.
- وبالإضافة إلى ذلك، يعني رقم التسلسل المفقود في النطاق أن حزمة ESP ذات 226 بايت تم إنشاؤها بواسطة جدار حماية BR ولكن لم يتم إرسالها من الواجهة الخارجية.
- نظرا لأنه لم يتم إرسال الحزمة ذات 226 بايت من جدار حماية BR خارج الواجهة، فإن جدار حماية HQ لم يتلقاها قط.
- أدى نقص الحزمة ذات 226 بايت في جدار حماية HQ إلى فشل إعادة تجميع الجزء كما هو موضح في "قسم جدار حماية HQ".

الشرح

تتطابق النتائج من قسم التحليل التقني مع أعراض معرف تصحيح الأخطاء من Cisco CSCwp10123.

نظرة عامة عالية المستوى على إجراءات جدار الحماية لإنشاء حزم ESP وإرسالها إلى واجهة الخروج:

1. يستقبل جدار الحماية حزم مجزأة من المفترض إرسالها عبر نفق VTI.
2. إذا كان طول الحزمة الداخلية أكبر من حجم MTU للواجهة ناقص مصروفات IPSec، حينئذ تتم تجزئة الحزمة.
3. استنادا إلى بحث جدول التوجيه، يتم العثور على الخطوة التالية. في حالة ال VTI، الخطوة تالي هو النظير VTI عنوان.
4. بناء على النفق غاية عنوان المخرج قارن والتالي جنجل عينت (مثل، خارج قارن).
5. يتم تضمين الحزم الأصلية داخل حزم ESP.
6. يتم إجراء بحث التجاوز للخطوة التالية من الخطوة 3 ويتم إرسال الحزم إلى واجهة الخروج.

بسبب معرف تصحيح الأخطاء من Cisco CSCwp10123، يتم تنفيذ الأجزاء التي تم تغليفها ESP (غير الأولية) التالية في الخطوة 4 بحث المسار الجديد. إذا كان جدار الحماية يحتوي على موجهات أكثر تحديدا إلى عنوان IP للنظير (أو الشبكة الفرعية)، فسيتم استخدام المسار الجديد بدلا من المسار للحزمة الأولية. في هذا المثال، عنوان IP لواجهة جدار حماية HQ هو x.x.x.99. يقوم جدار حماية HQ بالإعلان عن شبكته الفرعية الخارجية إلى جدار حماية BR عبر VTI الذي يعمل عبر بروتوكول العبارة الحدودية (BGP):

```
<#root>

>

show route bgp

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRFGateway of last resort is 192.168.20.1 to network 0.0.0.0

B        x.x.x.96 255.255.255.224 [20/0] via 10.255.0.1, 13:57:43

<--BR firewall learns /27 route via BGP over VTI

<#root>

>

show bgp summary
```

```
                                BGP router identifier 192.168.179.10, local AS number 65001
                                     BGP table version is 25, main routing table version 25
                                              23 network entries using 4600 bytes of memory
                                                 24 path entries using 1920 bytes of memory
                                2/2 BGP path/bestpath attribute entries using 416 bytes of memory
                                                1 BGP AS-PATH entries using 24 bytes of memory
                                              0 BGP route-map cache entries using 0 bytes of memory
                                             0 BGP filter-list cache entries using 0 bytes of memory
                                                                BGP using 6960 total bytes of memory
                                           BGP activity 23/0 prefixes, 24/0 paths, scan interval 60 secs
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd

10.255.0.1      4        65000 762     761           25    0    0 13:59:01  18

>

show ip

…
Tunnel1                vti-hq                10.255.0.2      255.255.255.252 CONFIG <--

10.255.0.1

is the peer VTI IP
…
```

<#root>

```
>

show ip

…
Tunnel1                vti-hq                10.255.0.2      255.255.255.252 CONFIG <--

10.255.0.1

is the peer VTI IP in the same subnet
…
```

يتم إرسال حزمة ESP ذات 1514 بايت من الواجهة الخارجية. ولكن بالنسبة لجدار الحماية سعة 226 بايت في الخطوة 3، يقوم بإجراء بحث عن المسار ويبحث عن مسار محدد نحو عنوان IP للنظير عبر VTI. بمعنى آخر، بدلا من إرسال الحزم من واجهة إنهاء VPN، يستخدم جدار الحماية واجهة VTI ويحاول حل التجاوز على واجهة VTI. ونظرا لأن واجهات VTI لا تحتوي على مفهوم التجاوز، يتم إسقاط الحزم أخيرا باستخدام سبب إسقاط الحزمة غير المتوقع.

كحل بديل، في CSF1230، أدرج المستخدم قائمة الوصول (ACL) في خريطة المسار. بعد نشر النهج، رفضت قائمة التحكم في الوصول (ACL) إستخدام الشبكة الفرعية الخارجية، مما أدى إلى إزالة نشر الشبكة الفرعية الخارجية من توجيه BGP بشكل فعال. ونظرا لهذا التغيير،

لا تتلقى جدران حماية BR بادئة الشبكة الفرعية الخارجية HQ عبر واجهة النفق.

لماذا يتم إسقاط الحزم ذات 266 بايت بعد الترحيل من ASA إلى جدار الحماية الآمن؟

قام تكوين جدار حماية ASA بحظر نشر الشبكة الفرعية للواجهة الخارجية HQ بشكل صريح في الفروع:

ASA5508

```
router bgp 65000
...
redistribute connected route-map BGP_RM
route-map BGP_RM permit 10
match ip address bgp-connected-routes
access-list bgp-connected-routes standard deny x.x.x.96 255.255.255.224 <-- deny = do not redistribute
```

CSF1230

```
router bgp 65000
...
redistribute connected route-map BGP_RM
route-map BGP_RM permit 40 <-- No match, means redistribute all connected routes
```

السبب

تم تشغيل المشكلة بسبب أختلاف التكوين في إعادة توزيع مسار BGP بين ASA 5508 و FTD 1230 الجديد. كان ASA 5508 يتضمن قائمة تحكم في الوصول ترفض إعادة توزيع الشبكة الفرعية x.x.x.96/27، بينما تم تكوين FTD 1230 لإعادة توزيع جميع المسارات المتصلة. أثار هذا تشكيل فرق cisco بق id CSCwp10123.

المحتوى ذي الصلة

- معرف تصحيح الأخطاء من Cisco CSCwp10123

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).