سلوك فشل نشر الموقع الجغرافي مع تمكين اكتشاف التهديدات على FTD لجدار الحماية الآمن

المحتويات

مسألة

عند محاولة تكوين تصفية حركة المرور المستندة إلى الموقع الجغرافي على جدار حماية آمن FTD 3105 من Cisco، تمت مواجهة العديد من المشاكل:

- لم تقم سياسة التحكم في الوصول المستندة إلى العناصر الجغرافية (ACP) وقواعد HTTPS (RA-VPN) للوصول عن بعد إلى اتصال VPN بحظر محاولات اتصال VPN بعامل التصفية المسبق لحظر المناطق إلى الواجهة الخارجية لـ FTD.
- بعد الترقية إلى الإصدار 7.7.11، فشلت عملية تكوين الوصول إلى الخدمة القائمة على الموقع الجغرافي RA-VPN في النشر عندما أدرجت بلدان هولندا أو جزر الأنتيل الهولندية في هذه السياسة.
- فشل نشر FMC بنسبة 83٪ مع رسالة الخطأ هذه:

```
FMC >> object-group geolocation FMC_GEOLOCATION_184683596782_116848397
                                        FMC >> location "Netherlands"
                                                  device >> [error] :
                                               location "Netherlands"
                                                                    ^
                                ERROR: % Invalid input detected at '^' marker.
                                        Config Error -- location "Netherlands"
```

البيئة

- FMC المدارة بواسطة Cisco Secure Firewall FirePOWER Threat Defense (FTD) 3105
- إصدار البرنامج الذي تمت ترقيته: 7.7.11-1061

- تكوين RA-VPN الذي يتطلب قيود وصول قائمة على البلد

رارق

وتضمن القرار خطوات متعددة للتحقق بشكل صحيح من مراقبة الوصول القائمة على فاكتشاف الموقع الجغرافي العام. وبالإضافة إلى ذلك، تم تمكين اكتشاف حد مع تعديلات جديدة فيما يتعلق بسلوك مطابقة حركة المرور، مما أدى إلى توفير إرشادات التهديدات.

1: قم بترقية كل من FTD و FMC إلى الإصدار 7.7.11-1061 لتمكين وظيفة الوصول إلى الخدمة المستندة إلى البيئة (RA-VPN) الجغرافية، نظرا لأن هذه الميزة مدعومة فقط من الإصدار 7.7.0 والإصدارات الأحدث.

2: تكوين الوصول إلى الخدمة المستندة إلى البيئة (RA-VPN) وفقا لوثائق Cisco وربطه بسياسة RA-VPN.

3: لحل فشل النشر بسبب معرف تصحيح الأخطاء من Cisco CSCwq15499 عند إضافة دول محددة مثل هولندا أو جزر الأنتيل الهولندية، قم بتطبيق هذا الحل البديل:

1. قم بإنشاء كائن وصول فارغ لخدمة RA-VPN بدون تكوين أي دولة.
2. تطبيق كائن الوصول إلى الخدمة الفارغ على نهج RA-VPN ونشره بنجاح.
3. قم بتحرير نفس كائن الوصول إلى الخدمة وأضف قواعد البلد المطلوبة.
4. قم بنشر التكوين مرة أخرى - نجح النشر الآن وأصبحت تصفية الموقع الجغرافي نشطة.

4: تحقق من اكتمال النشر بنجاح ومن أن الوصول إلى شبكة RA-VPN والسجلات تعكس القيود القطرية المقصودة. مراقبة النظام للتأكد من أن قيود الموقع الجغرافي تعمل كما هو متوقع.

5: حدد ما إذا تم تمكين أي ميزة "الكشف عن التهديدات" بالفعل على FTD والتي قد تطابق حركة مرور البيانات قبل أن تتمكن من الوصول إلى نهج الوصول. تتسبب هذه التكوينات في تخطي قواعد الموقع الجغرافي حيث يتم التحكم في الكشف عن التهديدات قبل تطبيق النهج.

<#root>

```
device# show run threat-detection
    threat-detection basic-threat
threat-detection statistics access-list
```

```
no threat-detection statistics tcp-intercept
```

```
threat-detection service invalid-vpn-access
threat-detection service remote-access-authentication hold-down 1440 threshold 5
threat-detection service remote-access-client-initiations hold-down 1440 threshold 5
```

6: قم بربط أي معرفات syslog المتعلقة بمطابقات اكتشاف التهديدات وتجنب تأكيد حركة المرور التي تضرب اكتشاف التهديدات بدلا من الموقع الجغرافي.

- ٪FTD-4-401002: تمت إضافة شونين: IP_ADDRESS IP_ADDRESS
- ٪FTD-4-401003: تم حذف شونين: IP_ADDRESS
- ٪ftd-4-401004: حزمة منبوذة: IP_ADDRESS ==> IP_ADDRESS على interface_name
- ٪FTD-4-733102: الكشف عن التهديدات يضيف مضيف إلى قائمة تجنب
- ٪ftd-4-733103: الكشف عن التهديدات يزيل المضيف من قائمة الانقطاع
- ٪ftd-4-733201: الكشف عن التهديد: الخدمة [عمليات بدء الوصول عن بعد-client] النظير[peer-ip]: تجاوز عتبة الفشل للقيمة: إضافة تجنب إلى الواجهة. SSL: الإزالة RA عميل بدء طلبات.
- ٪ftd-4-733201: الكشف عن التهديد: الخدمة [عمليات بدء الوصول عن بعد-client] النظير[peer-ip]: تجاوز حد العتبة للقيمة: إضافة تجنب إلى الواجهة. طلبات IKEv2:RA_EXCESSIVE_CLIENT_INITIATION_REQUESTS

```
<164>Feb 26 2026 23:05:45: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:07:36: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:12:25: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:00:00: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
---
device# show shun
```

السبب

وترجع المشاكل التي تفدوص إلى سببين جذريين مميزين:

- قواعد مطابقة الموقع الجغرافي: لا يتم دعم التحكم في الوصول المستند إلى تحديد الموقع الجغرافي RA-VPN إلا بدءا من الإصدار 7.7.0 من البرنامج. أعلاه بالإضافة إلى

ذلك، يمكن أن يعمل الكشف عن تهديدات RAVPN التي تم تكوينها على حركة المرور، مما يمنعها من المطابقة مع القواعد القائمة على الأرض.

- معرف تصحيح الأخطاء من Cisco CSCwq15499: وفي النسخة 7-7-11، تحدث حالات فشل في النشر عند إضافة بلدان معينة إلى سياسات الوصول إلى الخدمات القائمة على أساس جغرافي في RA-VPN بسبب خطأ برمجي معروف في آلية معالجة الوصول إلى الخدمات الجغرافية الخاصة بشبكة RA-VPN.

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).