تكوين السياسات المستندة إلى الموقع الجغرافي للوصول عن بعد إلى VPN على الدفاع ضد تهديد جدار الحماية الآمن

المحتويات

المقدمة

يصف هذا المستند عملية السماح باتصالات RAPN أو رفضها استنادا إلى مواقع جغرافية معينة على "الدفاع ضد تهديد جدار الحماية الآمن (FTD)".

المتطلبات الأساسية

المتطلبات والحدود

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة جدار الحماية الآمن (FMC)
- شبكة VPN للوصول عن بعد (RAVPN)
- تكوين الموقع الجغرافي الأساسي

المتطلبات والقيود الحالية للسياسات المستندة إلى الموقع الجغرافي هي:

- مدعوم فقط على الإصدار 7.7.0+ من برنامج الإرسال فائق السرعة (FTD)، الذي تتم إدارته بواسطة الإصدار 7.7.0+ من FMC.
- غير مدعوم على FTD المدار بواسطة مدير أجهزة جدار الحماية الآمن (FDM).

- غير مدعوم في وضع نظام المجموعة
- لا يتم تصنيف عناوين IP غير المصنفة المستندة إلى الموقع الجغرافي حسب الأصل الجغرافي. ولهذه الأسباب، تفرض وحدة التحكم في الوصول إلى الخدمات إجراء سياسة الوصول إلى الخدمة الافتراضي.
- لا تنطبق سياسات الوصول إلى الخدمة المستندة إلى الموقع الجغرافي على صفحات WebLaunch، مما يتيح لك تنزيل "العميل الآمن" دون قيود.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- Secure Firewall، الإصدار 7.7.0
- Secure Firewall Management Center، الإصدار 7.7.0

يمكن العثور على تفاصيل كاملة حول هذه الميزة في دليل تكوين جهاز إدارة وصول VPN للمستخدمين البعيدين استنادا إلى الموقع الجغرافي داخل Cisco Secure Firewall Management Center 7.7.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

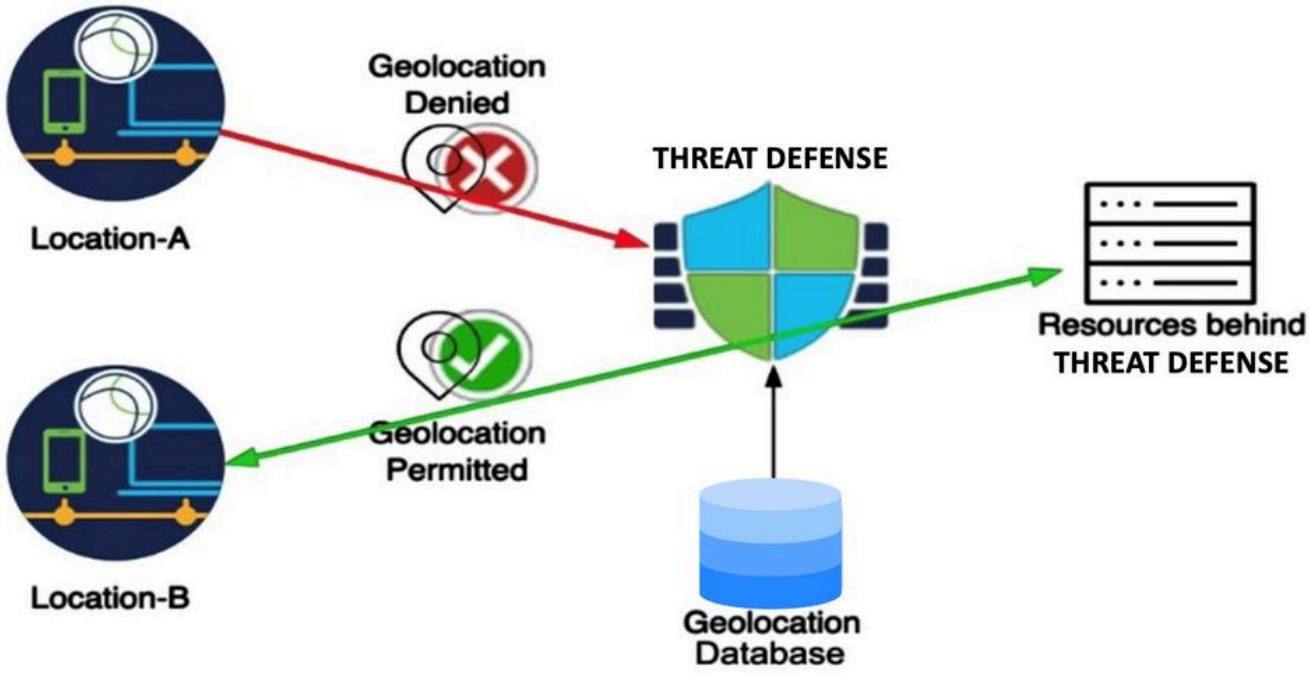
معلومات أساسية

توفر سياسات الوصول القائمة على الموقع الجغرافي قيمة كبيرة في أمان الشبكة اليوم، مما يسمح بحظر حركة المرور استنادا إلى أصلها الجغرافي. وبشكل تقليدي، يمكن للمؤسسات تحديد سياسات الوصول إلى حركة مرور البيانات لحركة مرور الشبكة العامة التي تمر عبر جدار الحماية. الآن، مع تقديم هذه الميزة، من الممكن تطبيق التحكم في الوصول المستند إلى الموقع الجغرافي لطلبات جلسات عمل الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد.

توفر هذه الميزة الميزات التالية:

- القواعد المستندة إلى الموقع الجغرافي: يمكن للعملاء إنشاء قواعد للسماح بطلبات RAVPN أو رفضها استنادا إلى مناطق جغرافية معينة، مثل البلدان أو القارات. وهذا يسمح بالتحكم الدقيق في المواقع الجغرافية التي يمكنها بدء جلسات VPN.
- حظر قبل المصادقة: يتم حظر جلسات العمل المحددة بواسطة هذه القواعد إجراء الرفض قبل المصادقة، ويتم تسجيل هذه المحاولات بشكل صحيح لأغراض الأمان. يساعد هذا الإجراء الاستباقي في الحد من محاولات الوصول غير المصرح بها.
- التوافق والأمان: تساعد هذه الميزة في ضمان الالتزام بالسياسات التنظيمية والإدارية المحلية، مع تقليل سطح الهجوم لخادم الشبكة الخاصة الظاهرية (VPN) في الوقت نفسه.

ونظرا لأن خوادم الشبكات الخاصة الظاهرية (VPN) تحتوي على عناوين IP عامة يمكن الوصول إليها عبر الإنترنت، فإن إدخال القواعد المستندة إلى الموقع الجغرافي يمكن المؤسسات من تقييد طلبات المستخدم من مواقع جغرافية معينة بشكل فعال، وبالتالي الحد من التعرض لهجمات القوة الغاشمة.

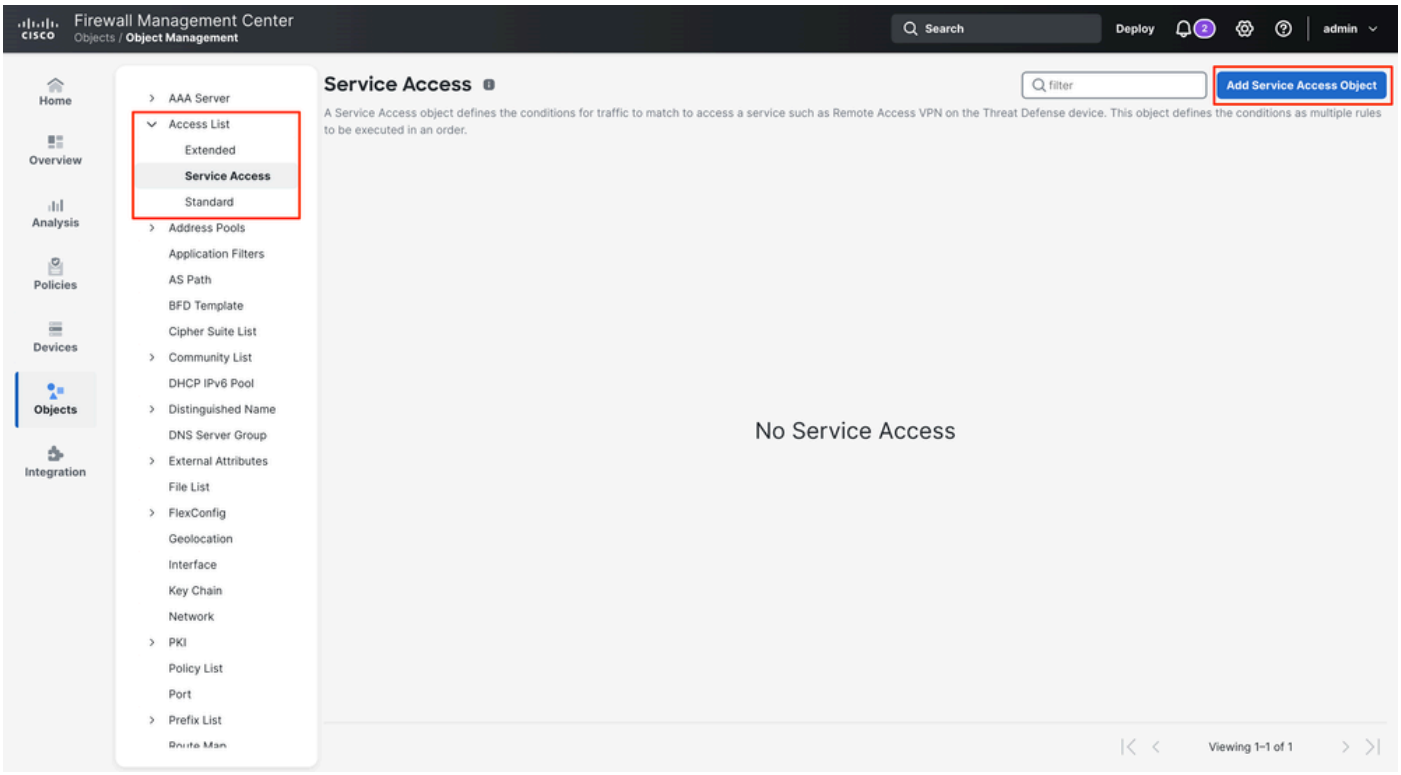


التكوين

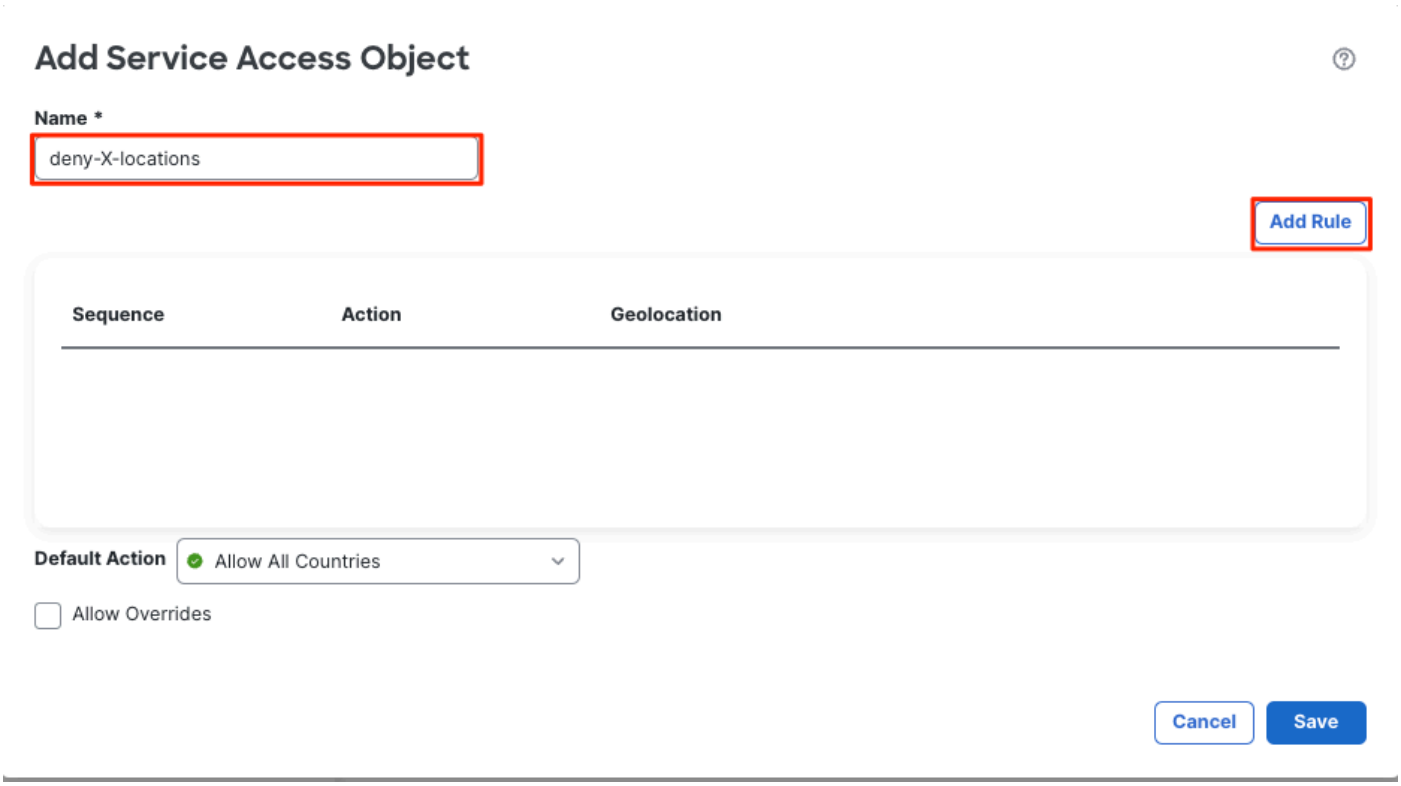
الخطوة 1. إنشاء كائن وصول إلى الخدمة

1. سجل الدخول إلى مركز إدارة جدار الحماية الآمن.

2. انتقل إلى الكائنات > إدارة الكائنات > قائمة الوصول >الوصول إلى الخدمة وانقر فوق إضافة كائن الوصول إلى الخدمة.



3. حدد اسم القاعدة، ثم انقر فوق إضافة قاعدة.

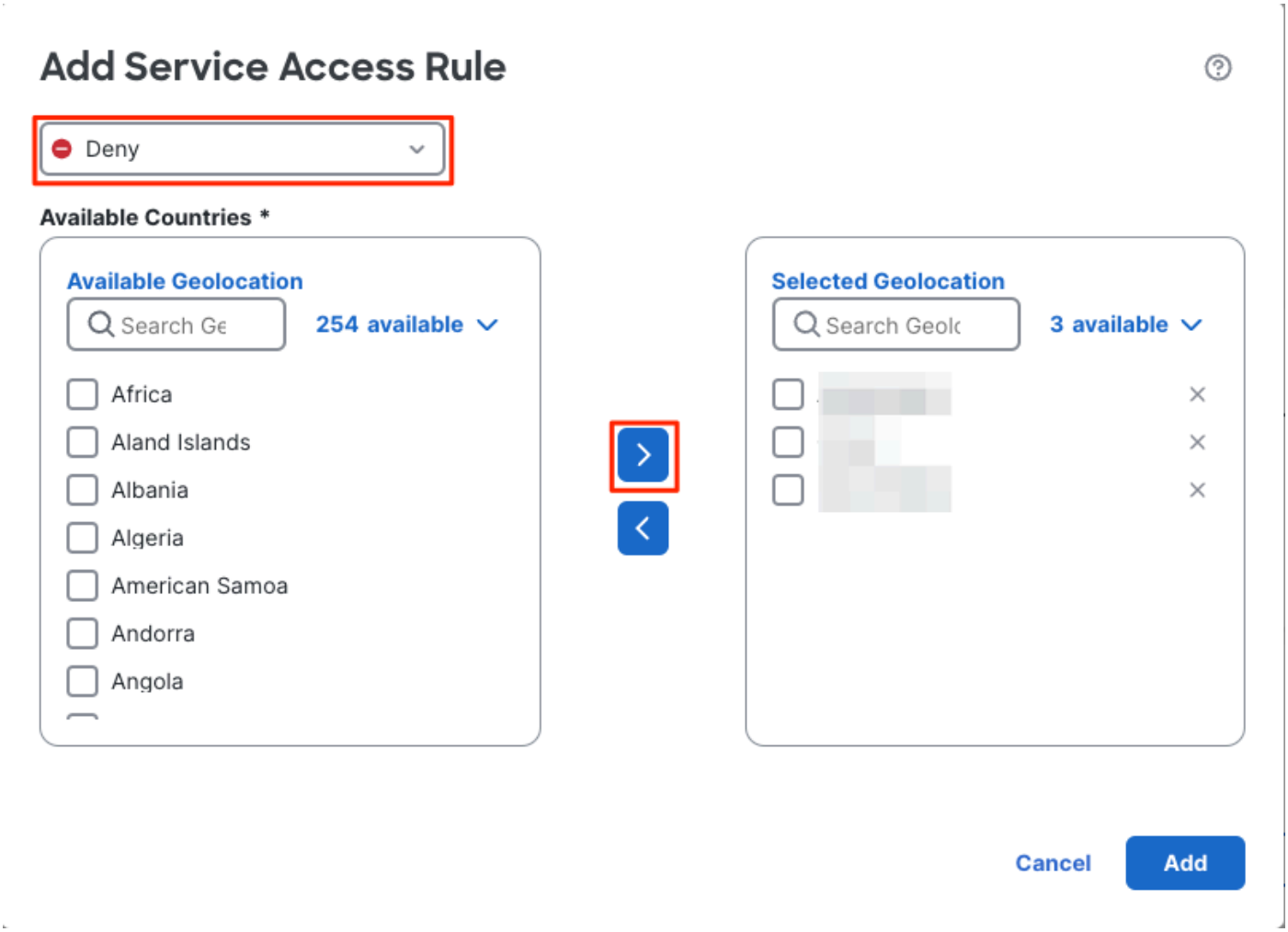


4. قم بتكوين قاعدة الوصول إلى الخدمة:

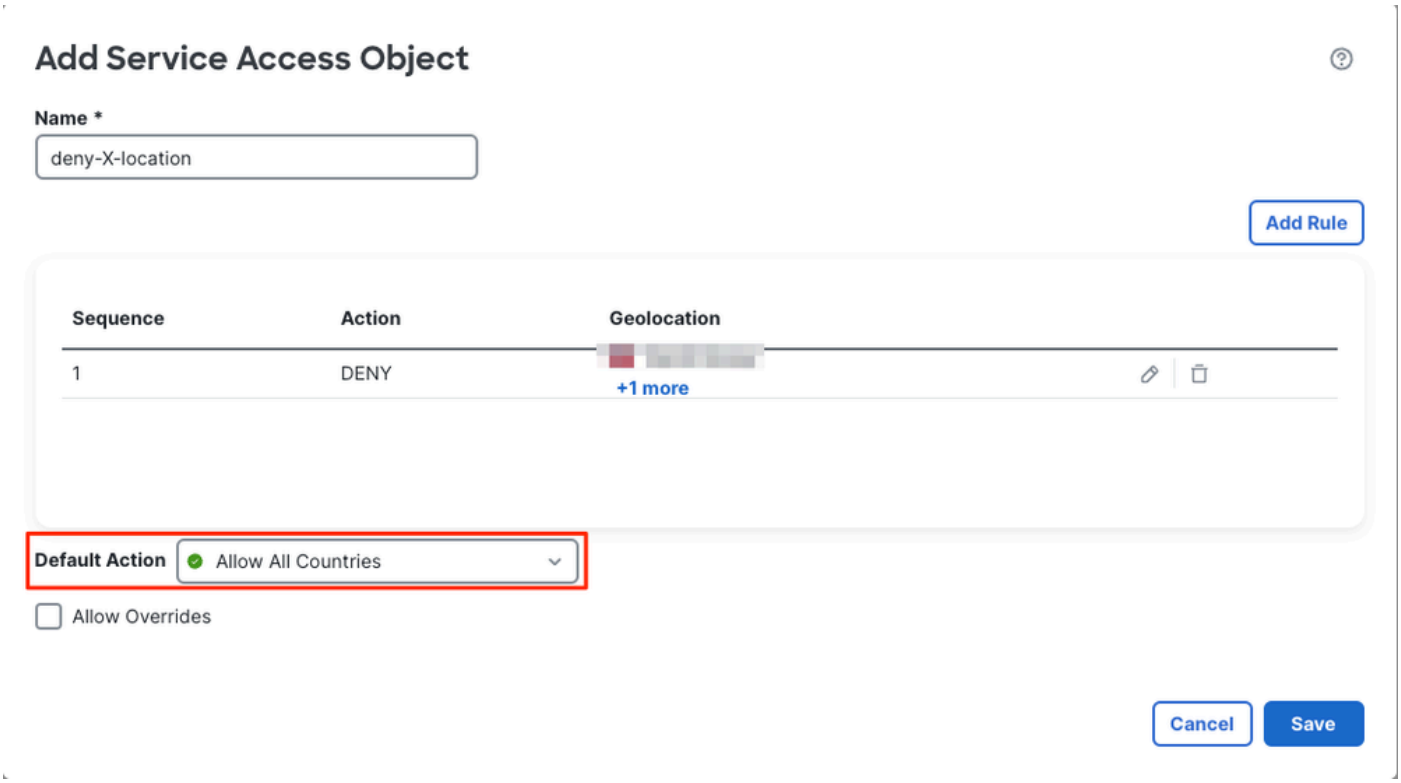
- حدد إجراء القاعدة: السماح أو الرفض.
- من البلدان المتاحة، حدد بلدان أو قارات أو كائنات تحديد الموقع الجغرافي من قبل المستخدم ونقلها إلى قائمة تحديد الموقع الجغرافي.
- انقر فوق إضافة لإنشاء القاعدة.

ملاحظة: في كائن الوصول إلى الخدمة، يمكن إستخدام كائن الموقع الجغرافي (البلد أو القارة أو الموقع الجغرافي المخصص) في قاعدة واحدة فقط.

ملاحظة: تأكد من تكوين قواعد الوصول إلى الخدمة بالترتيب الصحيح، حيث لا يمكن إعادة ترتيب هذه القواعد.



5. أختر الإجراء الافتراضي: اي تسمح لكل الدول اي ترفض كل الدول. ينطبق هذا الإجراء على الاتصالات التي لا تطابق أي من قواعد الوصول إلى الخدمة التي تم تكوينها.

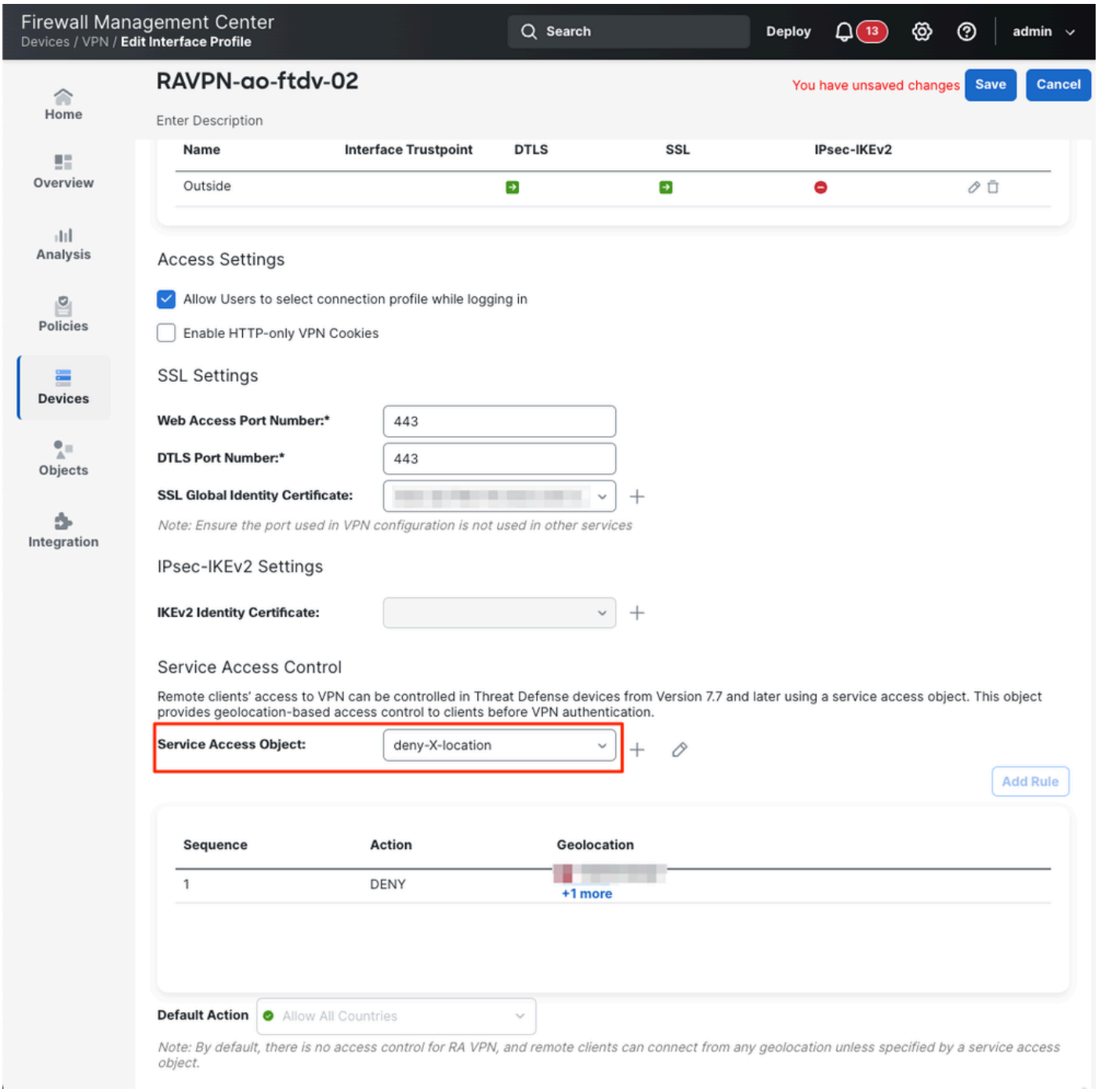


6. انقر فوق حفظ.

الخطوة 2. تطبيق تكوين كائن الخدمة في RAVPN.

1. انتقل إلى تكوين RAPN في الأجهزة > الوصول عن بعد > كائن تكوين RAPN > واجهة الوصول.

2. في قسم التحكم في الوصول إلى الخدمة، حدد كائن الوصول إلى الخدمة الذي أنشأته سابقا.

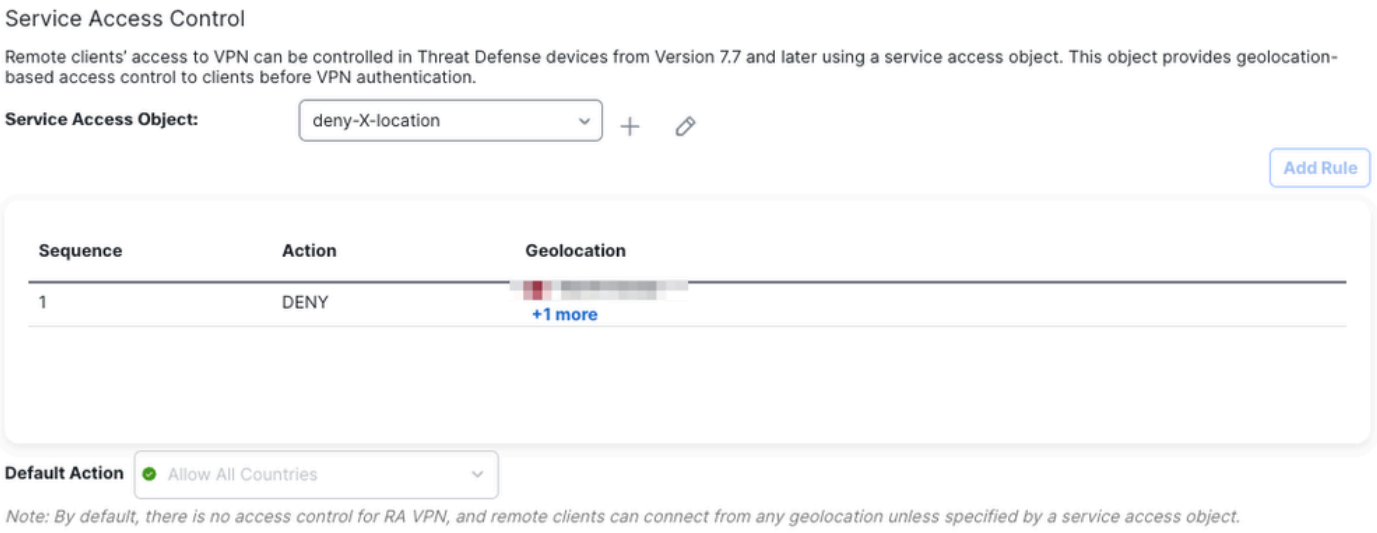


3. يعرض كائن الوصول إلى الخدمة الذي قمت بتحديده الآن ملخص القواعد والإجراء الافتراضي. تأكد من صحة ذلك.

4. أخيرا، احفظ التغييرات وقم بنشر التكوين.

التحقق من الصحة

بمجرد حفظ التكوين، تظهر القواعد في قسم التحكم في الوصول إلى الخدمة، مما يتيح لك التحقق من المجموعات والدول التي تم حظرها أو السماح بها.



قم بتشغيل الأمر show running-config service-access لضمان توفر قواعد الوصول إلى الخدمة من واجهة سطر الأوامر (CLI) الخاصة ب FTD.

```
<#root>

firepower#

show running-config service-access


service-access deny ra-ssl-client geolocation FMC_GEOLOCATION_146028889448_536980902
service-access permit ra-ssl-client geolocation any

firepower# show running-config object-group idFMC_GEOLOCATION_146028889448_536980902
object-group geolocation FMC_GEOLOCATION_146028889448_536980902
location "Country X"
location "Country Y"
```

Syslog والمراقبة

يقدم جدار الحماية الآمن معرفات syslog جديدة لالتقاط الأحداث المتعلقة باتصالات RAPN التي يتم حظرها بواسطة السياسات المستندة إلى الموقع الجغرافي:

- يشير 761031: إلى حالة رفض اتصال IKEv2 من قبل نهج يستند إلى الموقع الجغرافي. يعد هذا syslog جزءا من فئة تسجيل VPN الحالية.

٪ftd-6-751031: تم رفض جلسة عمل الوصول عن بعد ل IKEv2 ل <client_ip> عنوان <device_ip> بواسطة قاعدة جغرافية (geo=<country_name>، id=<country_code>)

- يشير 751031: إلى وقت رفض اتصال SSL من قبل نهج يستند إلى الموقع الجغرافي. يعد هذا syslog جزءا من فئة تسجيل WebVPN الحالية.

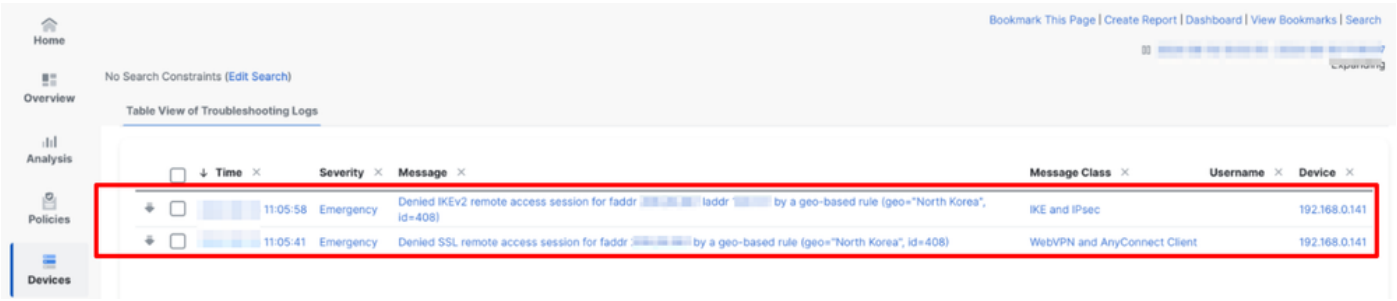
٪ftd-6-716166: تم رفض جلسة عمل الوصول عن بعد إلى SSL لـ <client_ip> بواسطة قاعدة جغرافية (geo=<country_name>، id=<country_code>)

ملاحظة: يكون مستوى الخطورة الافتراضي لهذه syslogs الجديدة معلوميا عند تمكينها من فئات التسجيل المقابلة. ومع ذلك، يمكنك تمكين معرفات syslog هذه بشكل فردي وتخصيص خطورتها.

قام جهاز العرض بحظر الاتصالات

للتحقق من صحة الاتصالات المحظورة، انتقل إلى الأجهزة > أستكشاف الأخطاء وإصلاحها > أستكشاف الأخطاء وإصلاحها السجلات. هنا، تعرض السجلات المتعلقة بالاتصالات المحظورة، بما في ذلك معلومات عن القواعد التي تؤثر على الاتصال ونوع الجلسة.

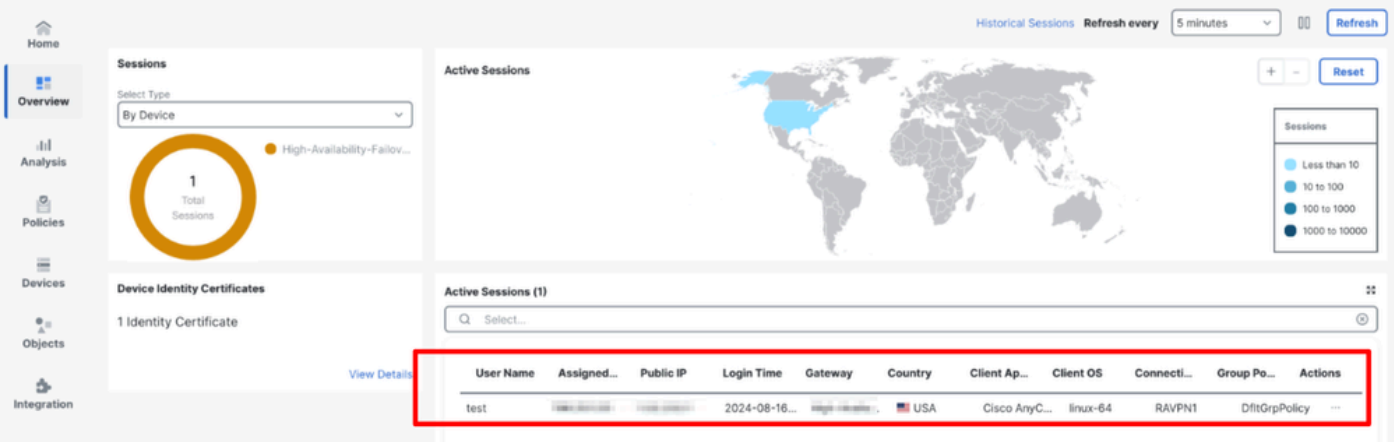
ملاحظة: يجب تكوين syslog لجمع هذه المعلومات في سجلات أستكشاف الأخطاء وإصلاحها.



مراقبة الاتصالات المسموح بها

تتم مراقبة الجلسات المسموح بها في نظرة عامة > لوحة معلومات VPN للوصول عن بعد، حيث يتم عرض معلومات الجلسة، بما في ذلك دولة المنشأ.

ملاحظة: يتم عرض الاتصالات فقط من الدول المسموح بها والمستخدمين المسموح لهم بالاتصال في لوحة المعلومات هذه. لا يتم عرض الاتصالات التي تم رفضها في لوحة المعلومات هذه.



استكشاف الأخطاء وإصلاحها

لأغراض أستكشاف الأخطاء وإصلاحها، اتبع الخطوات التالية:

1. تحقق من تكوين القواعد بشكل صحيح في كائن الوصول إلى الخدمة.
2. تحقق مما إذا كان يظهر رفض syslog في قسم سجلات أستكشاف الأخطاء وإصلاحها عند طلب الموقع الجغرافي المسموح به لجلسة عمل.
3. تأكد من أن التكوين الموضح في وحدة التحكم في الإدارة الأساسية (FTD) يطابق ما هو في واجهة سطر الأوامر (CLI) في FTD.
4. أستخدم الأوامر التالية لجمع المزيد من التفاصيل المفيدة لأغراض أستكشاف الأخطاء وإصلاحها:

- debug geolocation <1-255>
- show service-access
- show service-access detail
- show service-access interface
- إظهار موقع الوصول إلى الخدمة
- show service-access service
- عرض تفاصيل موقع <Country> Geodb IPv4
- show geodb counters
- show geodb ipV4 [lookup <ip address>]
- show geodb ipV6

معلومات ذات صلة

- للحصول على مساعدة إضافية، يرجى الاتصال ب TAC. يلزم عقد دعم صالح: جهات اتصال الدعم العالمية من Cisco.
- يمكنك أيضا زيارة مجتمع Cisco VPN هنا.

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).