Configurer les stratégies de géolocalisation pour le VPN distant sur le FTD sécurisé

Table des matières

Introduction

Conditions préalables

- Exigences et limitations
- Composants utilisés

Informations générales

Configurer

- Étape 1 : création d'un objet d'accès aux services
- Étape 2 : application de la configuration de l'objet de service dans RAVPN

Vérifier

Syslogs et surveillance

- Surveiller les connexions bloquées
- Surveiller les connexions autorisées

Dépannage

Informations connexes

Introduction

Ce document décrit le processus d'autorisation/de refus des connexions VPN d'accès à distance en fonction de géolocalisations spécifiques sur Secure Firewall Threat Defense.

Conditions préalables

Exigences et limitations

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Centre de gestion du pare-feu sécurisé (FMC)
- VPN d'accès à distance (RAVPN)
- Configuration de base de géolocalisation

Les exigences et les limites actuelles des politiques basées sur la géolocalisation sont les

suivantes :

- Pris en charge uniquement sur FTD version 7.7.0+, géré par FMC version 7.7.0+.
- Non pris en charge sur le FTD géré par Secure Firewall Device Manager (FDM).
- Non pris en charge en mode cluster.
- Les adresses IP non classées basées sur la géolocalisation ne sont pas classées par origine géographique. Pour ceux-ci, le FMC applique l'action de stratégie d'accès au service par défaut.
- Les stratégies d'accès au service basées sur la géolocalisation ne s'appliquent pas aux pages WebLaunch, ce qui vous permet de télécharger le client sécurisé sans restrictions.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles suivantes :

- Secure Firewall version 7.7.0
- Secure Firewall Management Center version 7.7.0

Pour plus d'informations sur cette fonctionnalité, consultez la section Manage VPN Access of Remote Users Based on Geolocation dans le Guide de configuration des périphériques Cisco Secure Firewall Management Center 7.7.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

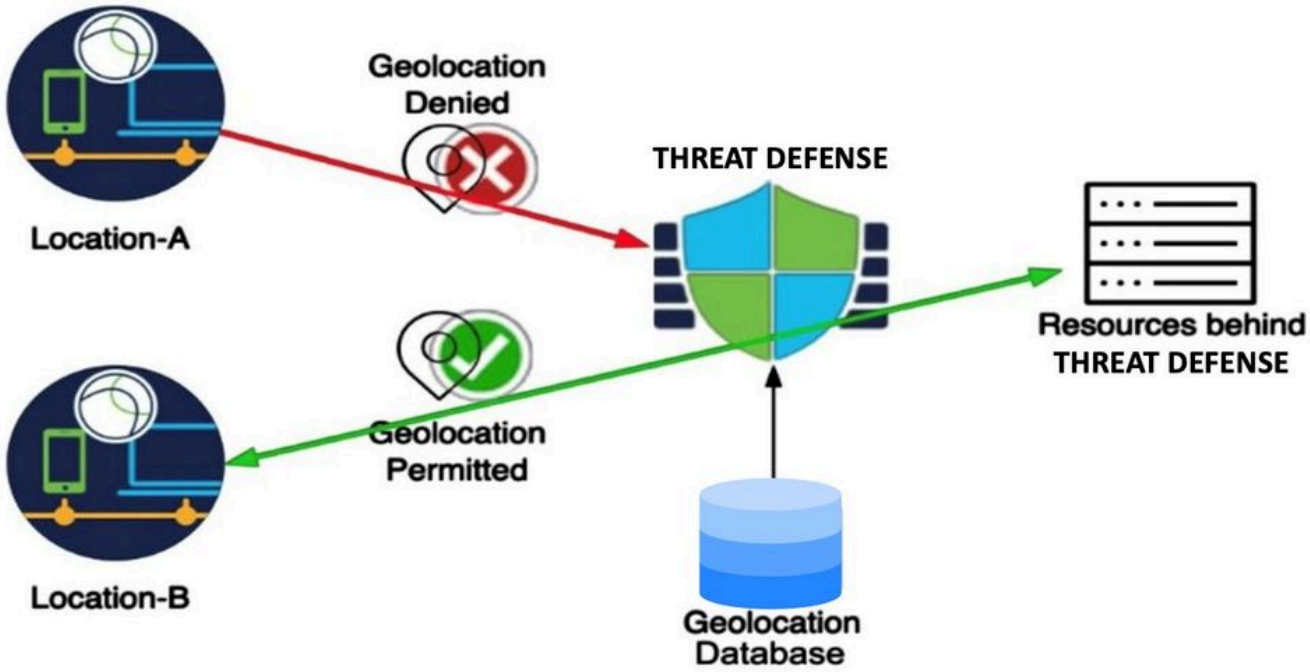
Informations générales

Les politiques d'accès basées sur la géolocalisation offrent aujourd'hui une valeur significative en matière de sécurité du réseau, permettant le blocage du trafic en fonction de son origine géographique. Traditionnellement, les entreprises peuvent définir des politiques d'accès au trafic pour le trafic réseau général qui passe par le pare-feu. Maintenant, avec l'introduction de cette fonctionnalité, il est possible d'appliquer un contrôle d'accès basé sur la géolocalisation pour les demandes de session VPN d'accès à distance.

Cette fonction offre les avantages suivants :

- Règles de géolocalisation : Créez des règles pour autoriser ou refuser les requêtes RAVPN en fonction de géolocalisations spécifiques, telles que des pays ou des continents. Cela permet un contrôle précis sur les emplacements géographiques qui peuvent lancer des sessions VPN.
- Blocage de pré-authentification : Les sessions identifiées par ces règles pour une action de refus sont bloquées avant l'authentification et ces tentatives sont correctement consignées à des fins de sécurité. Cette action préventive permet de limiter les tentatives d'accès non autorisées.
- Conformité et sécurité : Cette fonctionnalité permet de garantir le respect des politiques locales d'organisation et de gouvernance, tout en réduisant la surface d'attaque du serveur VPN.

Étant donné que les serveurs VPN ont des adresses IP publiques accessibles via Internet, l'introduction de règles basées sur la géolocalisation permet aux entreprises de restreindre efficacement les requêtes des utilisateurs à partir de géolocalisations spécifiques, réduisant ainsi la vulnérabilité aux attaques en force.

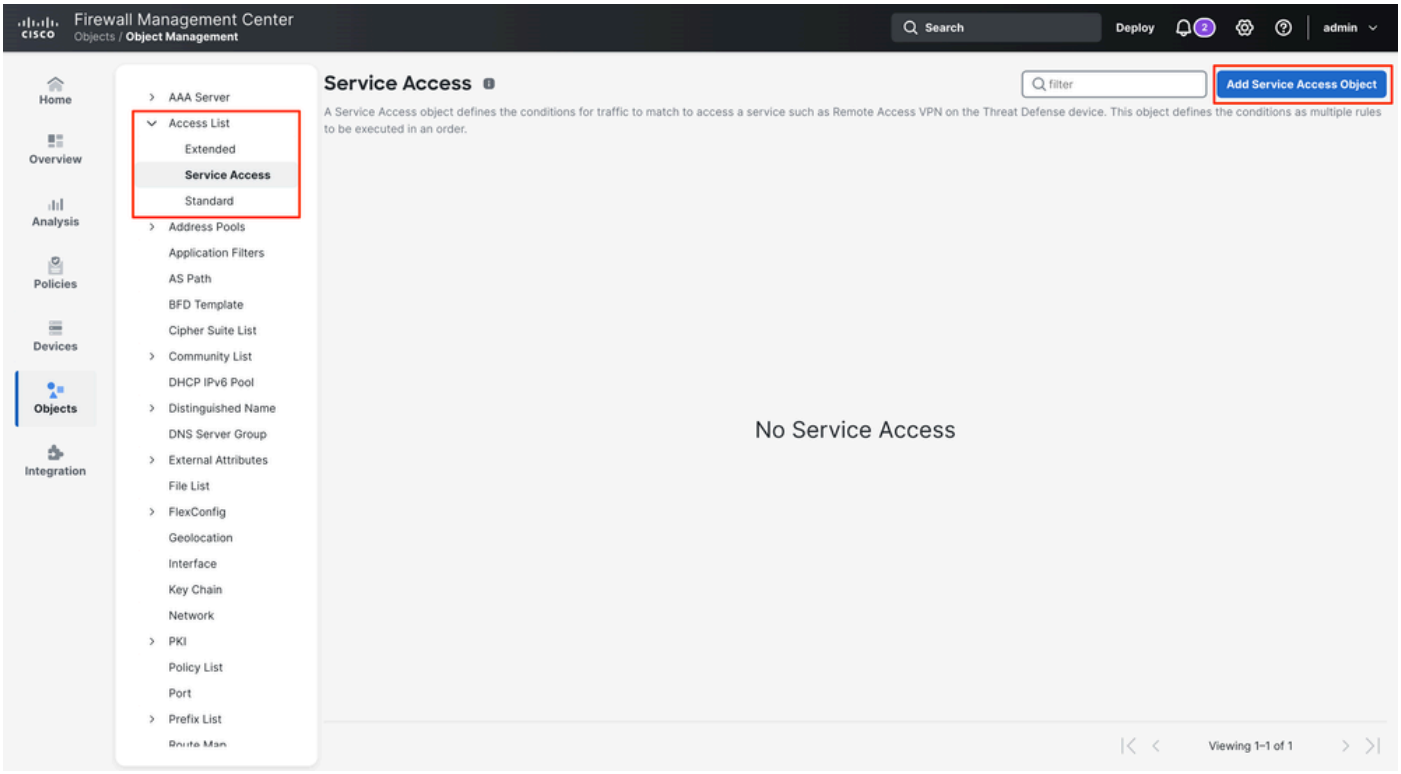


Configurer

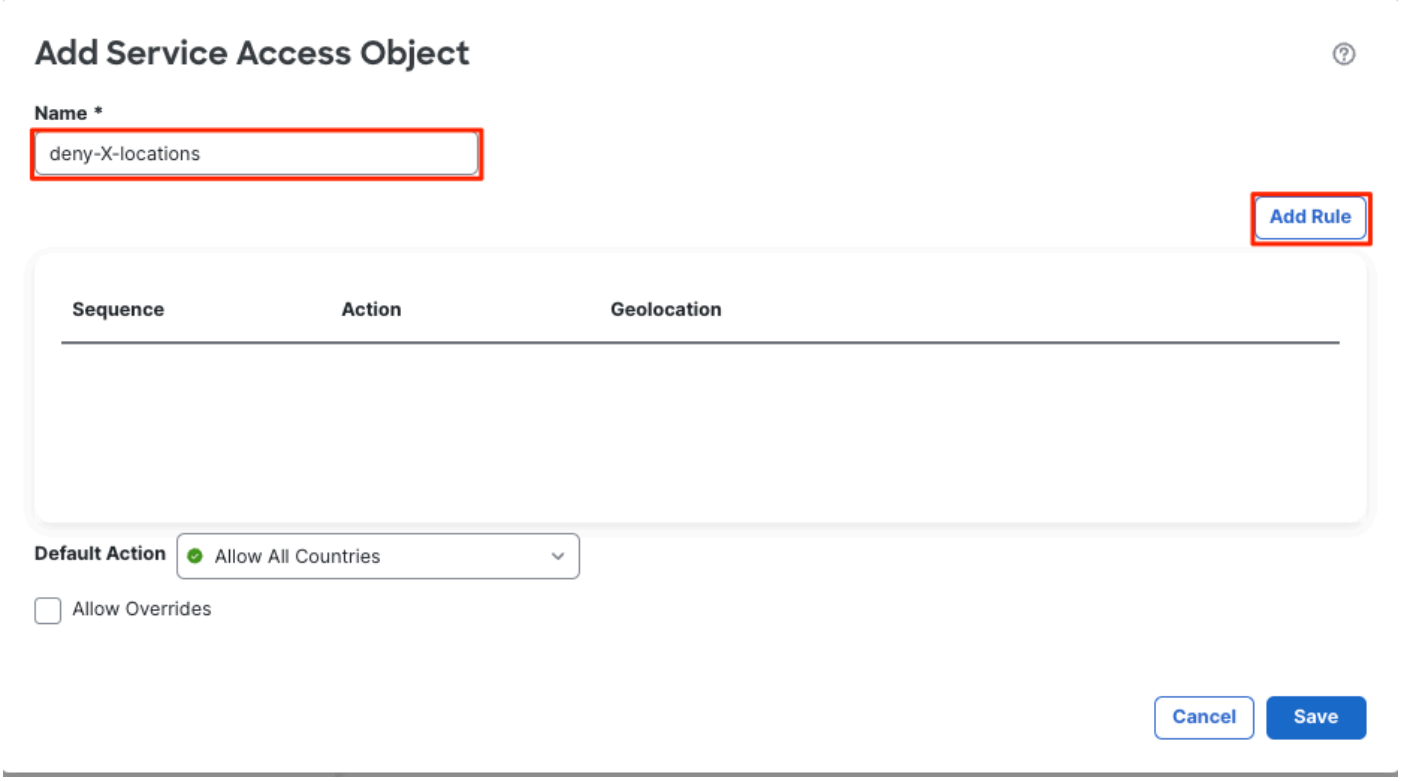
Étape 1 : création d’un objet d’accès aux services

1. Connectez-vous à Secure Firewall Management Center.

2. Accédez à Objets > Gestion des objets > Liste d'accès > Accès aux services et cliquez sur Ajouter un objet d'accès aux services.



3. Définissez le nom de la règle, puis cliquez sur Ajouter une règle.

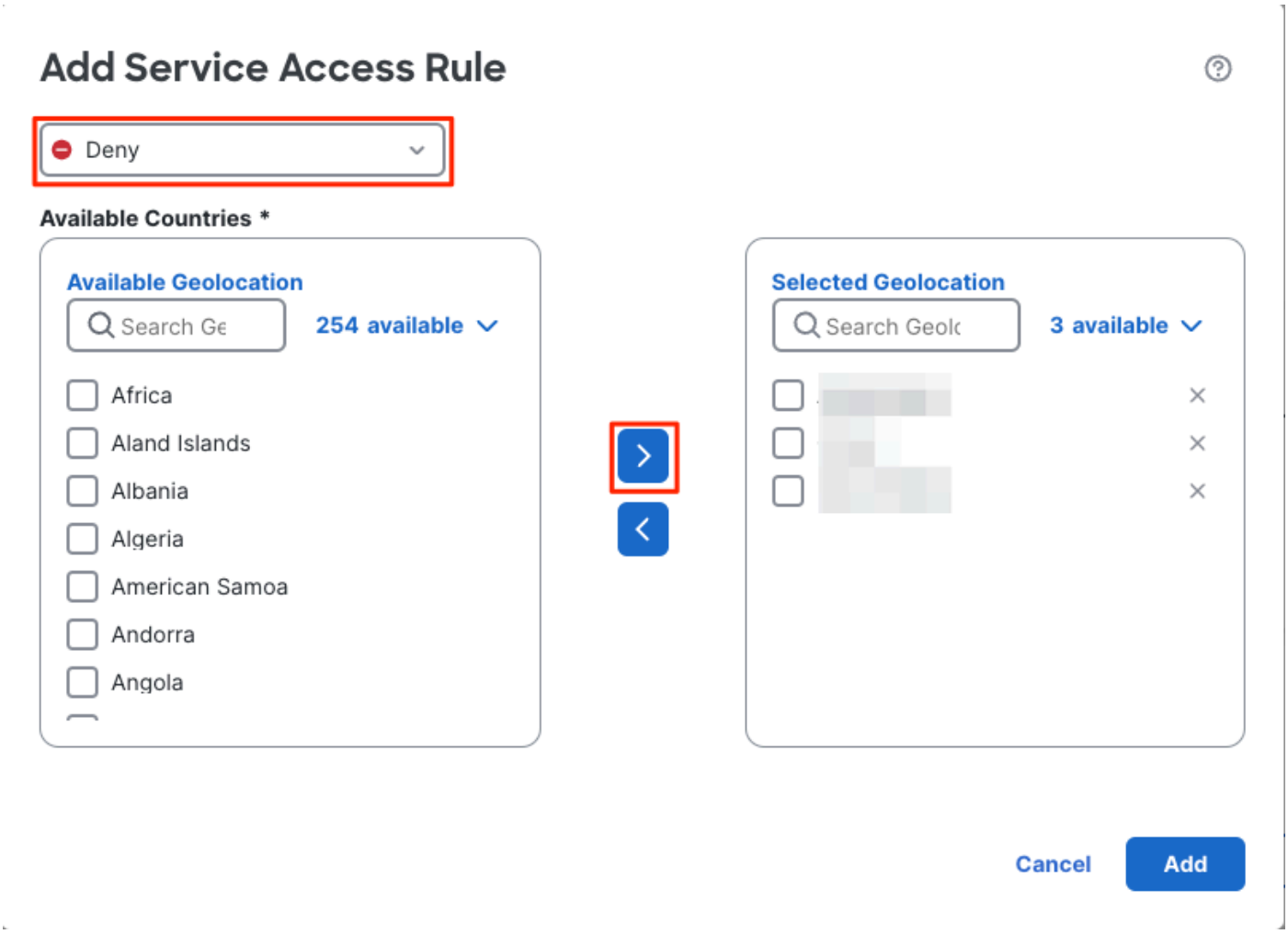


4. Configurez la règle d'accès au service :

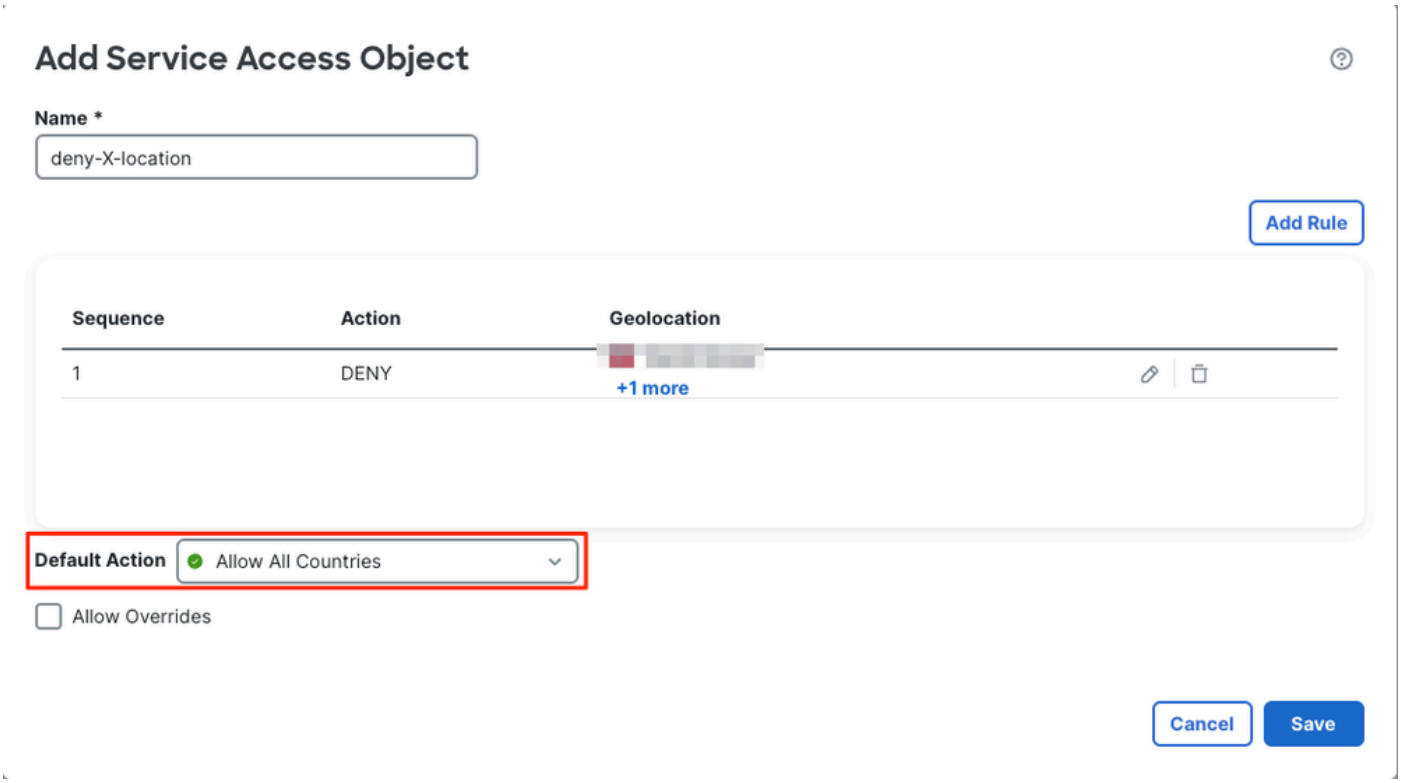
- Sélectionnez l'action de la règle : Allow ou Deny.
- Dans Pays disponibles, sélectionnez des pays, des continents ou des objets de géolocalisation définis par l'utilisateur et déplacez-les vers la liste Géolocalisation sélectionnée.
- Cliquez sur Add pour créer la règle.

Remarque : Dans un objet d'accès au service, un objet de géolocalisation (pays, continent ou géolocalisation personnalisée) ne peut être utilisé que dans une seule règle.

Remarque : assurez-vous de configurer les règles d'accès au service dans le bon ordre, car ces règles ne peuvent pas être réorganisées.



5. Choisissez l'action par défaut : Autoriser tous les pays ou Refuser tous les pays. Cette action s'applique aux connexions qui ne correspondent à aucune des règles d'accès au service configurées.

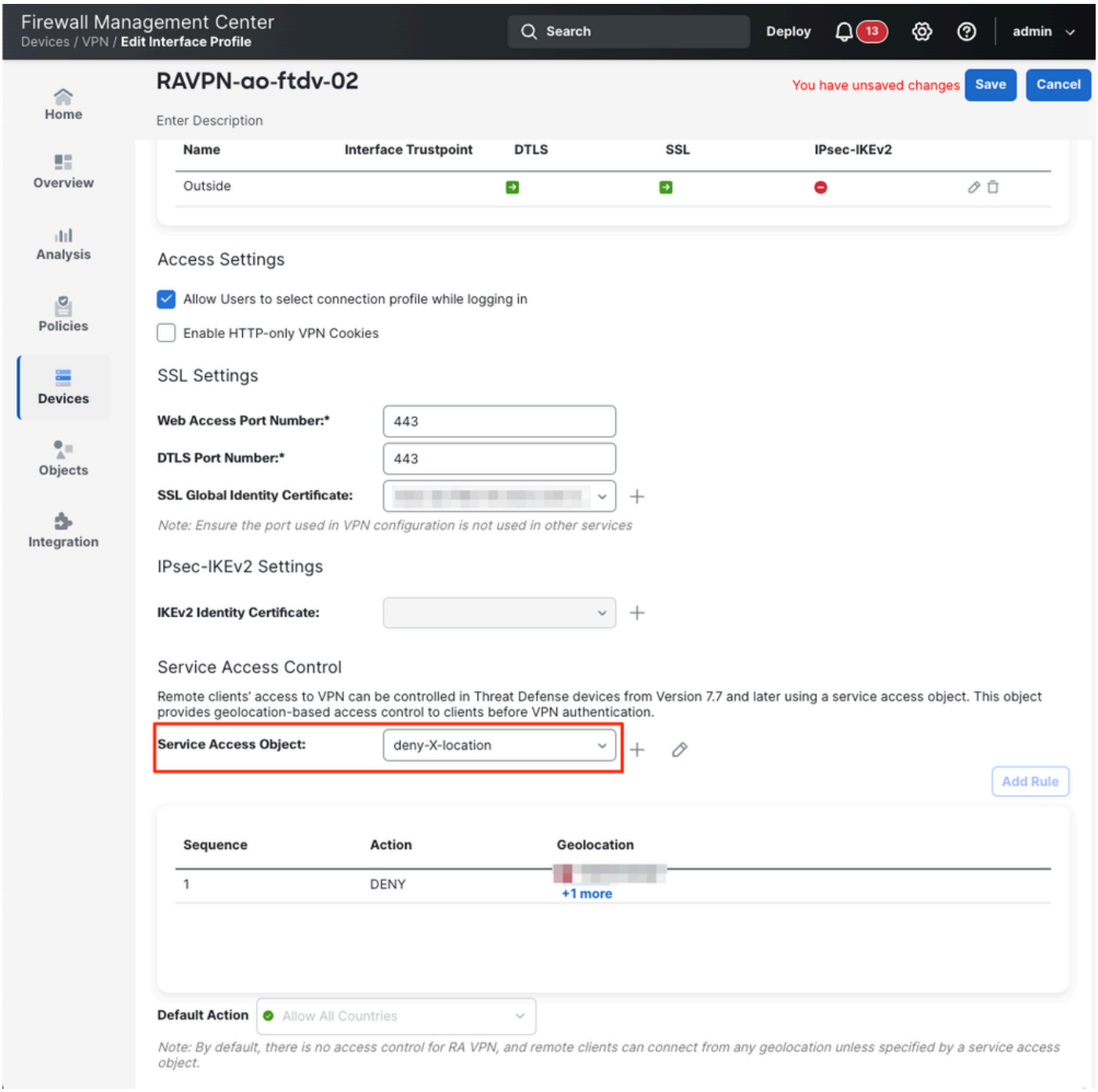


6. Cliquez sur Enregistrer.

Étape 2 : application de la configuration de l'objet de service dans RAVPN

1. Accédez à la configuration RAVPN dans Périphériques > Accès à distance > Objet de configuration RAVPN > Interface d'accès

2. Dans la section Contrôle d'accès aux services, sélectionnez l'objet d'accès aux services que vous avez créé précédemment.

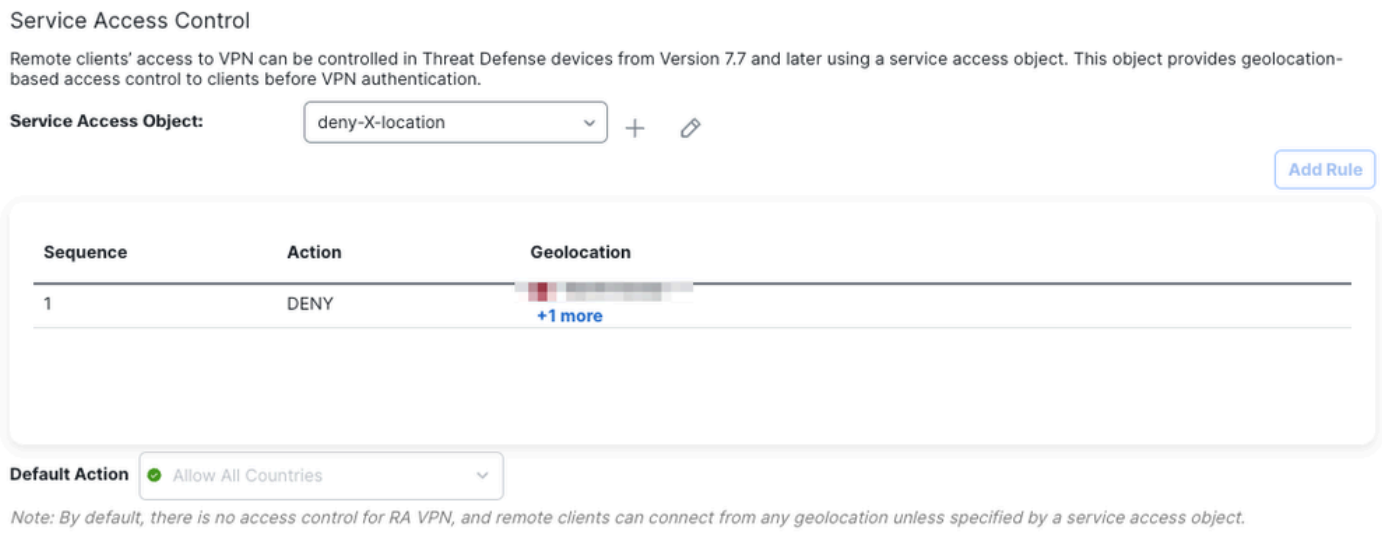


3. L'objet Accès au service que vous avez sélectionné affiche maintenant la synthèse des règles et l'action par défaut. Assurez-vous que ce message est correct.

4. Enfin, enregistrez les modifications et déployez la configuration.

Vérifier

1. Une fois la configuration enregistrée, les règles apparaissent dans la section Service Access Control, vous permettant de valider quels groupes et pays sont bloqués ou autorisés.



2. Exécutez la commande show running-config service-access pour vous assurer que les règles d'accès au service sont disponibles à partir de l'interface de ligne de commande 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"
```

Syslogs et surveillance

Secure Firewall introduit de nouveaux ID Syslog pour capturer les événements liés aux connexions RAVPN bloquées par des politiques basées sur la géolocalisation :

- 761031 : indique lorsqu'une connexion IKEv2 est refusée par une stratégie basée sur la géolocalisation. Ce syslog fait partie de la classe de journalisation VPN existante.

%FTD-6-751031 : Session d'accès à distance IKEv2 refusée pour faddr <ip_client> laddr <ip_périphérique> par une règle basée sur la zone géographique (geo=<nom_pays>, id=<code_pays>)

- 751031 : indique lorsqu'une connexion SSL est refusée par une stratégie basée sur la géolocalisation. Ce syslog fait partie de la classe de journalisation WebVPN existante.

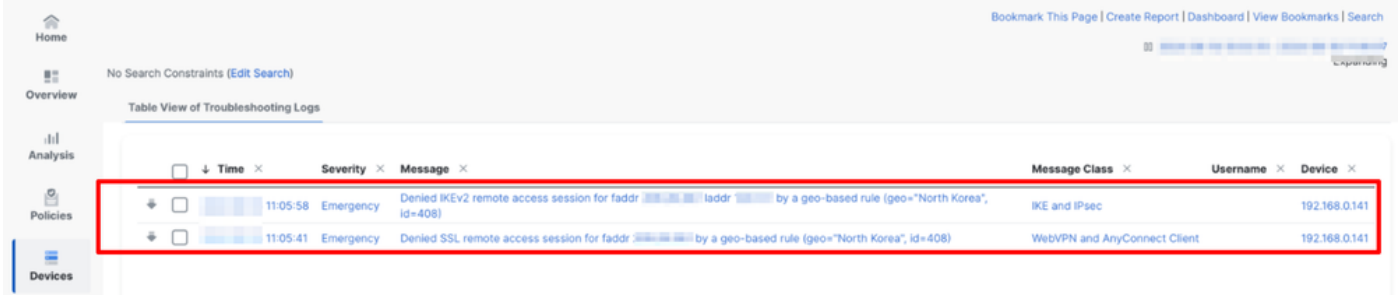
%FTD-6-716166 : Session d'accès à distance SSL refusée pour faddr <client_ip> par une règle basée sur la zone géographique (geo=<nom_pays>, id=<code_pays>)

Remarque : Le niveau de gravité par défaut pour ces nouveaux syslogs est informatif lorsqu'il est activé à partir des classes de journalisation respectives. Cependant, vous pouvez activer ces ID Syslog individuellement et personnaliser leur gravité.

Surveiller les connexions bloquées

Pour valider les connexions bloquées, accédez à Devices > Troubleshoot > Troubleshooting Logs. Les journaux associés aux connexions bloquées sont affichés, y compris des informations sur les règles affectant la connexion et le type de session.

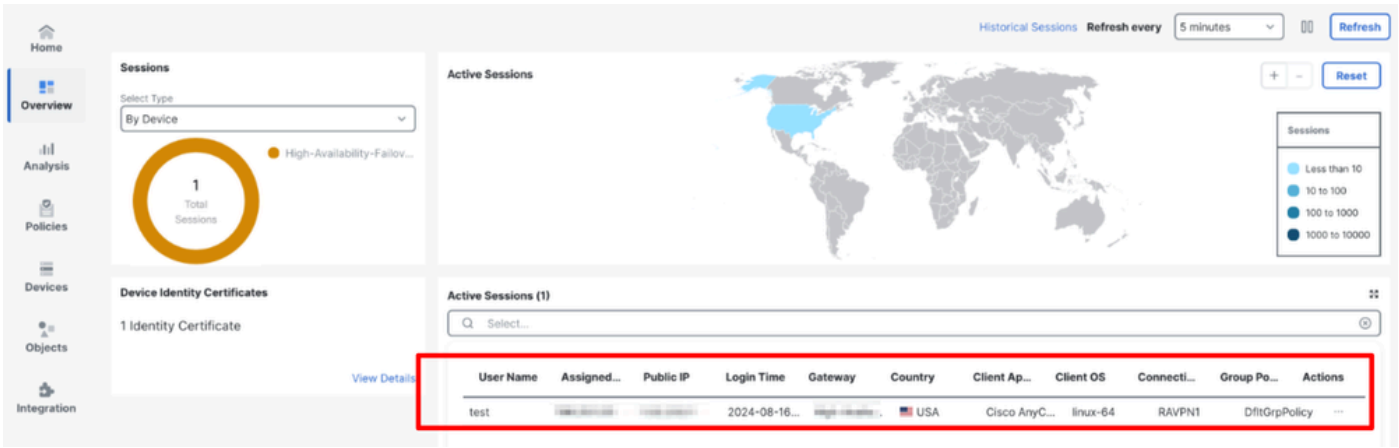
Remarque : Syslog doit être configuré pour collecter ces informations dans les journaux de dépannage.



Surveiller les connexions autorisées

Les sessions autorisées sont surveillées dans Overview > Remote Access VPN dashboard, où les informations de session sont affichées, y compris le pays d'origine.

Remarque : Seules les connexions des pays et utilisateurs autorisés à se connecter sont affichées sur ce tableau de bord. Les connexions rejetées ne sont pas affichées sur ce tableau de bord.



Dépannage

Pour les besoins du dépannage, révisez ces étapes :

1. Vérifiez que les règles sont correctement configurées dans l'objet Service Access.

2. Vérifiez si un syslog deny apparaît dans la section Journaux de dépannage lorsqu'une géolocalisation autorisée demande une session.
3. Assurez-vous que la configuration affichée dans le FMC correspond à celle de l'interface de ligne de commande du FTD.
4. Utilisez les commandes suivantes pour obtenir plus de détails utiles à des fins de dépannage :

- debug geolocation <1-255>
- show service-access
- show service-access detail
- show service-access interface
- show service-access location
- show service-access service
- show geodb ipv4 location <Country> detail
- show geodb counters
- show geodb ipv4 [lookup <adresse IP>]
- show geodb ipv6

Informations connexes

- Pour obtenir de l'aide supplémentaire, contactez le TAC. Un contrat d'assistance valide est requis :Contacts d'assistance internationale Cisco
- Vous pouvez également visiter la communauté VPN Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.