Configurer le blocage du trafic basé sur la géolocalisation sur FTD pour le filtrage du trafic entrant et sortant

Table des matières

Problème

- Décrire la meilleure façon de bloquer le trafic en fonction de la géolocalisation sur Cisco Secure Firewall Threat Defense (FTD), à la fois pour le trafic provenant d'une région et pour le trafic destiné à une région.
- Des questions se posent quant à savoir si des règles de contrôle d'accès distinctes sont nécessaires pour le filtrage du trafic entrant et sortant, et si des objets Geolocation supplémentaires doivent être créés lorsque des entrées de géolocalisation sont déjà disponibles dans l'onglet Geolocations sous l'onglet Réseaux de la règle de contrôle d'accès.

Environnement

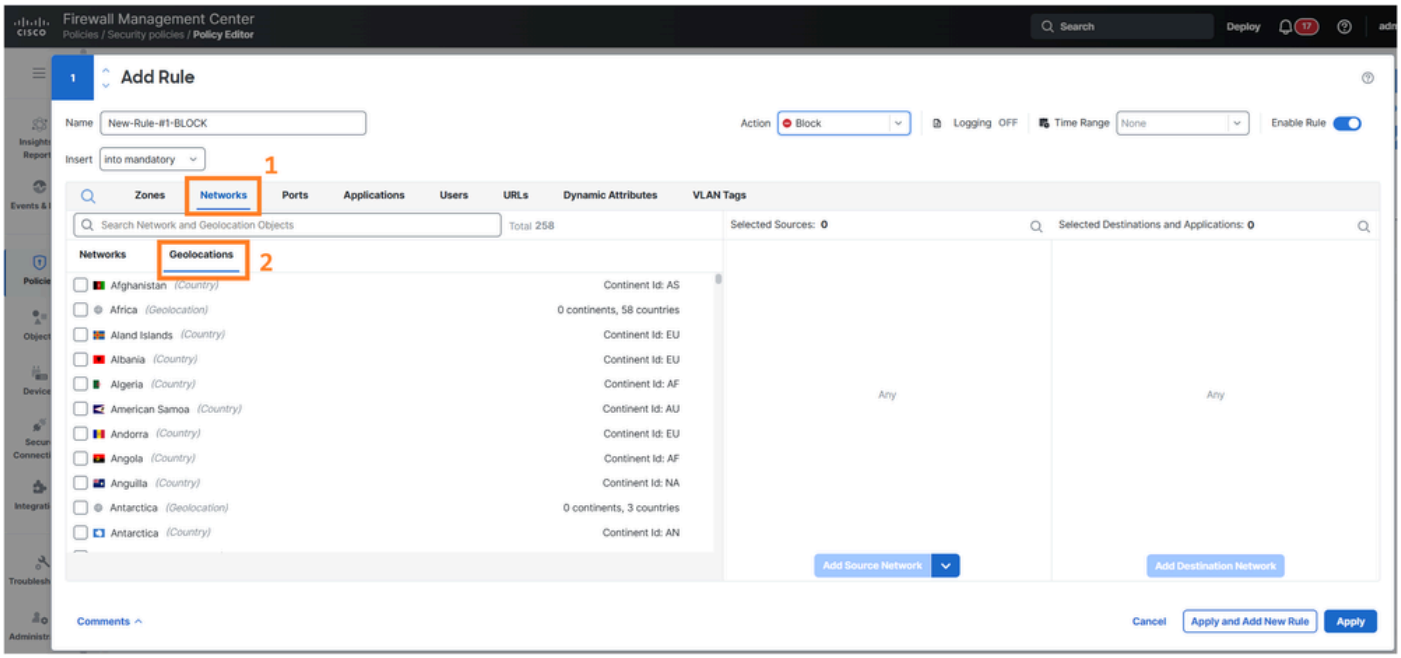
- Logiciel FTD version 7.1. Les autres versions logicielles sont également affectées.
- Logiciel Cisco Secure Firewall Management Center (FMC) version 7.1. Les autres versions logicielles sont également affectées.

Résolution

Le filtrage du trafic basé sur la géolocalisation sur Cisco FTD peut être géré efficacement à l'aide de la fonctionnalité de géolocalisation existante disponible dans l'onglet Réseaux, section Règle de contrôle d'accès de l'interface utilisateur FMC. L'approche de configuration dépend de la direction du trafic et des exigences de la politique spécifiques.

Accès à la configuration de géolocalisation

Accédez à Politiques > Politiques de sécurité > Éditeur de politiques, modifiez une règle et sélectionnez Réseaux > onglet Géolocalisations dans l'interface utilisateur de FMC. Les entrées de géolocalisation existantes disponibles dans cette section peuvent être utilisées directement pour créer des politiques de contrôle d'accès sans nécessiter d'objets de géolocalisation distincts.



Stratégie de création de règles

L'approche de création de règles varie en fonction de la direction du trafic et des objectifs de politique.

Pour bloquer le trafic entrant à partir de géolocalisations spécifiques

Créer des règles de contrôle d’accès qui identifient le trafic source provenant de régions géographiques spécifiques et appliquer des actions de blocage. Ces règles doivent être positionnées de manière appropriée dans l'ordre des règles afin d'assurer une application correcte des politiques.

Pour contrôler le trafic sortant vers des emplacements géographiques spécifiques

Configurez des règles de contrôle d'accès qui identifient le trafic de destination dirigé vers des régions géographiques spécifiques. En fonction de la stratégie de sécurité, ceux-ci peuvent être configurés pour autoriser ou bloquer le trafic vers ces destinations.

Exigences de règles distinctes

Des règles de contrôle d'accès distinctes sont nécessaires lors de la mise en oeuvre du filtrage bidirectionnel de géolocalisation pour les raisons suivantes :

- Le filtrage entrant nécessite des règles qui évaluent les attributs de géolocalisation source.
- Le filtrage sortant nécessite des règles qui évaluent les attributs de géolocalisation de destination.
- La directionnalité du trafic détermine quel champ de géolocalisation (source ou destination) est évalué par le moteur de contrôle d'accès.

La configuration spécifique des règles dépend de la topologie du réseau, des exigences de sécurité et des objectifs de contrôle de flux de trafic souhaités pour chaque région géographique.

Motif

La nécessité de clarifier la situation découle de la complexité de la mise en oeuvre du contrôle d'accès basé sur la géolocalisation, où différents types de règles et configurations sont requis en fonction de la direction du trafic. La disponibilité d'entrées de géolocalisation préexistantes dans l'onglet Réseaux des règles de contrôle d'accès de la stratégie de sécurité peut créer une confusion quant à la nécessité de créer des objets supplémentaires pour l'implémentation de la stratégie.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

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.