Konfigurieren der standortbasierten Datenverkehrsblockierung in FTD für die Filterung von ein- und ausgehendem Datenverkehr

Inhalt

Problem

- Beschreiben Sie, wie Datenverkehr, der aus einer Region stammt, und Datenverkehr, der für eine Region bestimmt ist, am besten blockiert werden kann, wenn der Datenverkehr auf der Basis von Geolokalisierung über Cisco Secure Firewall Threat Defense (FTD) erfolgt.
- Es stellen sich Fragen, ob separate Zugriffskontrollregeln für die Filterung von ein- und ausgehendem Datenverkehr erforderlich sind und ob zusätzliche Geolocation-Objekte erstellt werden müssen, wenn Geolocation-Einträge bereits auf der Registerkarte Geolocations unter der Registerkarte Access Control Rule Networks (Netzwerke der Zugriffskontrollregel) verfügbar sind.

Umwelt

- FTD Software Version 7.1. Andere Softwareversionen sind ebenfalls betroffen.
- Cisco Secure Firewall Management Center (FMC) Softwareversion 7.1. Andere Softwareversionen sind ebenfalls betroffen.

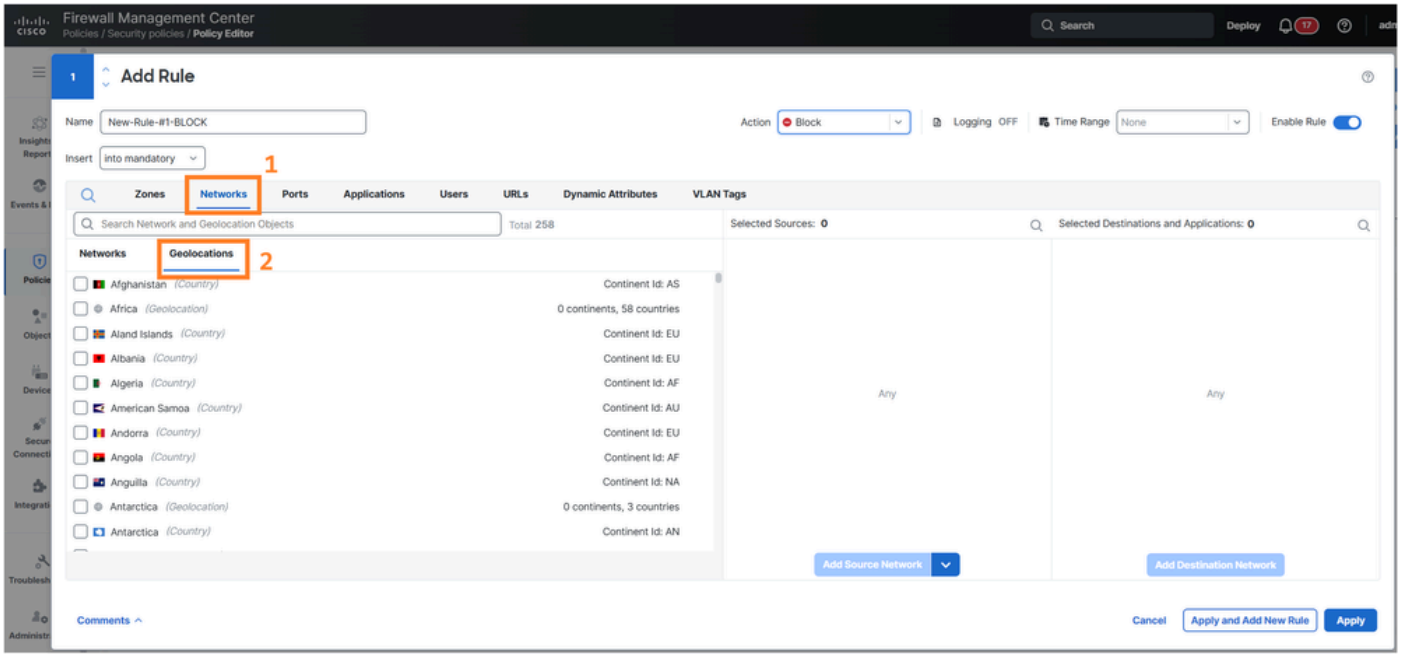
Auflösung

Die standortbasierte Datenverkehrsfilterung auf Cisco FTD kann mithilfe der vorhandenen Geolocations-Funktionen, die auf der Registerkarte "Networks" (Netzwerke) im Abschnitt "Access

Control Policy Rule" (Zugriffskontrollrichtlinie) der FMC User Interface (UI) verfügbar sind, effektiv verwaltet werden. Der Konfigurationsansatz hängt von der jeweiligen Datenverkehrsrichtung und den Richtlinienanforderungen ab.

Zugreifen auf die Standortkonfiguration

Navigieren Sie zu Richtlinien > Sicherheitsrichtlinien > Richtlinien-Editor, bearbeiten Sie eine Regel, und wählen Sie Netzwerke > Geolocations (Geolocationen) auf der FMC-Benutzeroberfläche aus. Die vorhandenen, in diesem Abschnitt verfügbaren Geolocation-Einträge können direkt zum Erstellen von Zugriffskontrollrichtlinien verwendet werden, ohne dass separate Geolocation-Objekte erforderlich sind.



Strategie zum Erstellen von Regeln

Der Ansatz zur Regelerstellung hängt von der Richtung des Datenverkehrs und den Richtlinienzielen ab.

Blockierung von eingehendem Datenverkehr von bestimmten Standorten

Erstellen Sie Zugriffskontrollregeln, die Quelldatenverkehr aus bestimmten geografischen Regionen identifizieren und Blockierungsaktionen anwenden. Diese Regeln müssen in der Regel angemessen positioniert werden, um eine ordnungsgemäße Durchsetzung der Richtlinien zu gewährleisten.

Steuerung des ausgehenden Datenverkehrs zu bestimmten geografischen Standorten

Konfigurieren Sie Zugriffskontrollregeln, die Zieldatenverkehr identifizieren, der an bestimmte geografische Regionen gerichtet ist. Je nach Sicherheitsrichtlinie können diese so konfiguriert werden, dass sie Datenverkehr zu diesen Zielen zulassen oder blockieren.

Anforderungen für separate Regeln

Bei der Implementierung der bidirektionalen Standortfilterung sind aus folgenden Gründen separate Zugriffskontrollregeln erforderlich:

- Für die eingehende Filterung sind Regeln erforderlich, die die Attribute der Quellortungsangabe bewerten.
- Für die ausgehende Filterung sind Regeln erforderlich, die die Attribute der Ziel-Geolokalisierung auswerten.
- Die Verkehrsausrichtung bestimmt, welches Geolokalisierungsfeld (Quelle oder Ziel) von der Zugriffskontroll-Engine ausgewertet wird.

Die spezifische Regelkonfiguration hängt von der Netzwerktopologie, den Sicherheitsanforderungen und den angestrebten Zielen für die Datenverkehrsflusskontrolle in den einzelnen geografischen Regionen ab.

Ursache

Die Notwendigkeit der Klärung ergibt sich aus der Komplexität der geolokationsbasierten

Implementierung der Zugriffskontrolle, bei der je nach Datenverkehrsrichtung unterschiedliche Regeltypen und Konfigurationen erforderlich sind. Die Verfügbarkeit bereits vorhandener Geolocation-Einträge auf der Registerkarte "Networks" (Netzwerke) der Zugriffskontrollregeln für Sicherheitsrichtlinien kann zu Verwirrung darüber führen, ob für die Richtlinienimplementierung zusätzliche Objekte erstellt werden müssen.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.