Configure Geolocation-Based Traffic Blocking on FTD for Inbound and Outbound Traffic Filtering

Contents

Issue

- Describe what is the best way to block traffic based on geolocation on Cisco Secure Firewall Threat Defense (FTD), both for traffic originating from a region and traffic destined for a region.
- Questions arise regarding whether separate access control rules are required for inbound and outbound traffic filtering, and whether additional Geolocation objects need to be created when geolocation entries are already available in the Geolocations tab under access control rule Networks tab.

Environment

- FTD software version 7.1. Other software versions are also affected.
- Cisco Secure Firewall Management Center (FMC) software version 7.1. Other software versions are also affected.

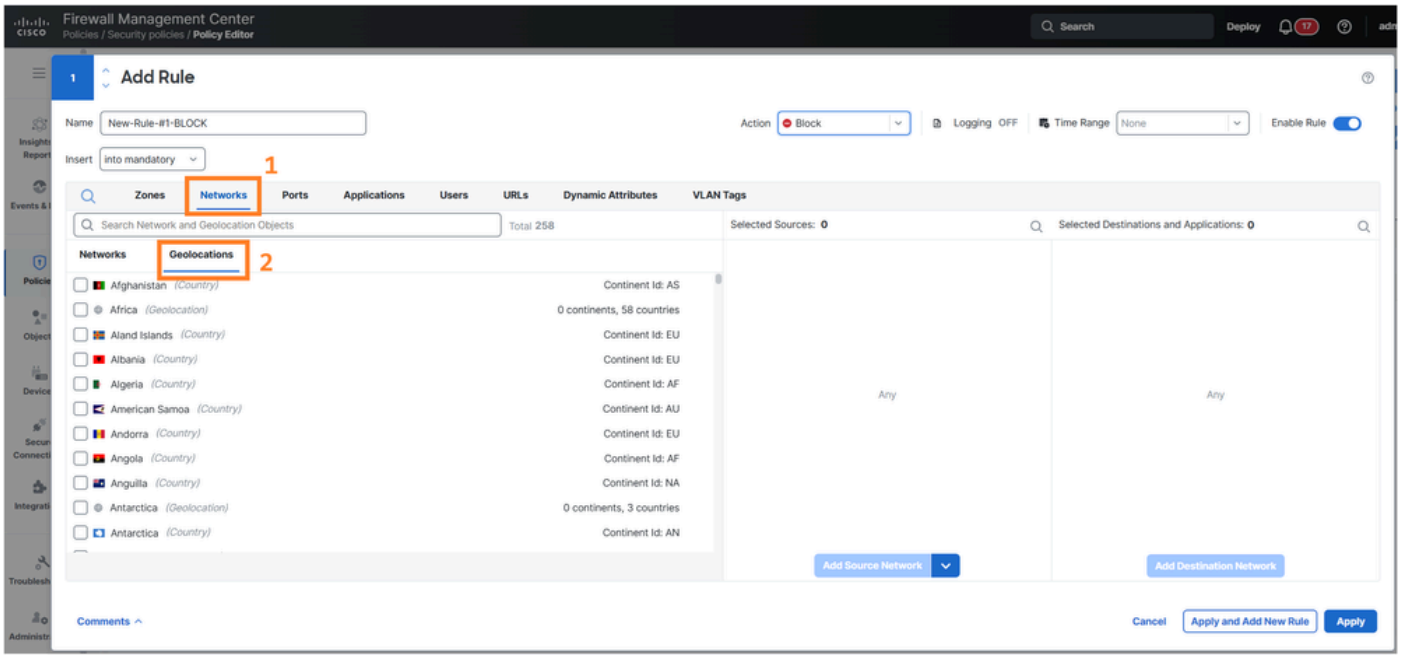
Resolution

Geolocation-based traffic filtering on Cisco FTD can be effectively managed using the existing Geolocations functionality available in the Networks tab, Access Control Policy Rule section of the FMC User Interface (UI). The configuration approach depends on the specific traffic direction and policy requirements.

Accessing Geolocation Configuration

Navigate to **Policies** > **Security policies** > **Policy Editor**, edit a rule and select **Networks** > **Geolocations** tab in the FMC UI. The existing geolocation entries available in this section can be utilized directly for

creating access control policies without requiring separate Geolocation objects.



Rule Creation Strategy

The rule creation approach varies based on traffic directionality and policy objectives.

Block Inbound Traffic from Specific Geolocations

Create access control rules that identify source traffic originating from specific geographic regions and apply block actions. These rules have to be positioned appropriately in the rule order to ensure proper policy enforcement.

Control Outbound Traffic to Specific Geolocations

Configure access control rules that identify destination traffic directed toward specific geographic regions. Depending on the security policy, these can be configured to either allow or block traffic to those destinations.

Separate Rule Requirements

Separate access control rules are necessary when implementing bidirectional geolocation filtering because:

- Inbound filtering requires rules that evaluate source geolocation attributes.
- Outbound filtering requires rules that evaluate destination geolocation attributes.
- Traffic directionality determines which geolocation field (source or destination) is evaluated by the access control engine.

The specific rule configuration depends on the network topology, security requirements, and the desired traffic flow control objectives for each geographic region.

Cause

The need for clarification arises from the complexity of geolocation-based access control implementation, where different rule types and configurations are required based on traffic direction. The availability of pre-existing geolocation entries in the Networks tab of the security policy access control rules, can create confusion about whether additional object creation is necessary for policy implementation.

Related Content

- Cisco Technical Support & Downloads