在FTD上配置基于地理定位的流量阻止以进行入站和出站流量过滤

目录

问题

- 描述在思科安全防火墙威胁防御(FTD)上根据地理定位阻止流量的最佳方法，对于来自区域的流量和发往区域的流量。
- 出现的问题涉及入站和出站流量过滤是否需要单独的访问控制规则，以及当访问控制规则“网络”(Networks)选项卡下的“地理位置”(Geolocations)选项卡中已有可用的地理定位条目时，是否需要创建其他地理定位对象。

环境

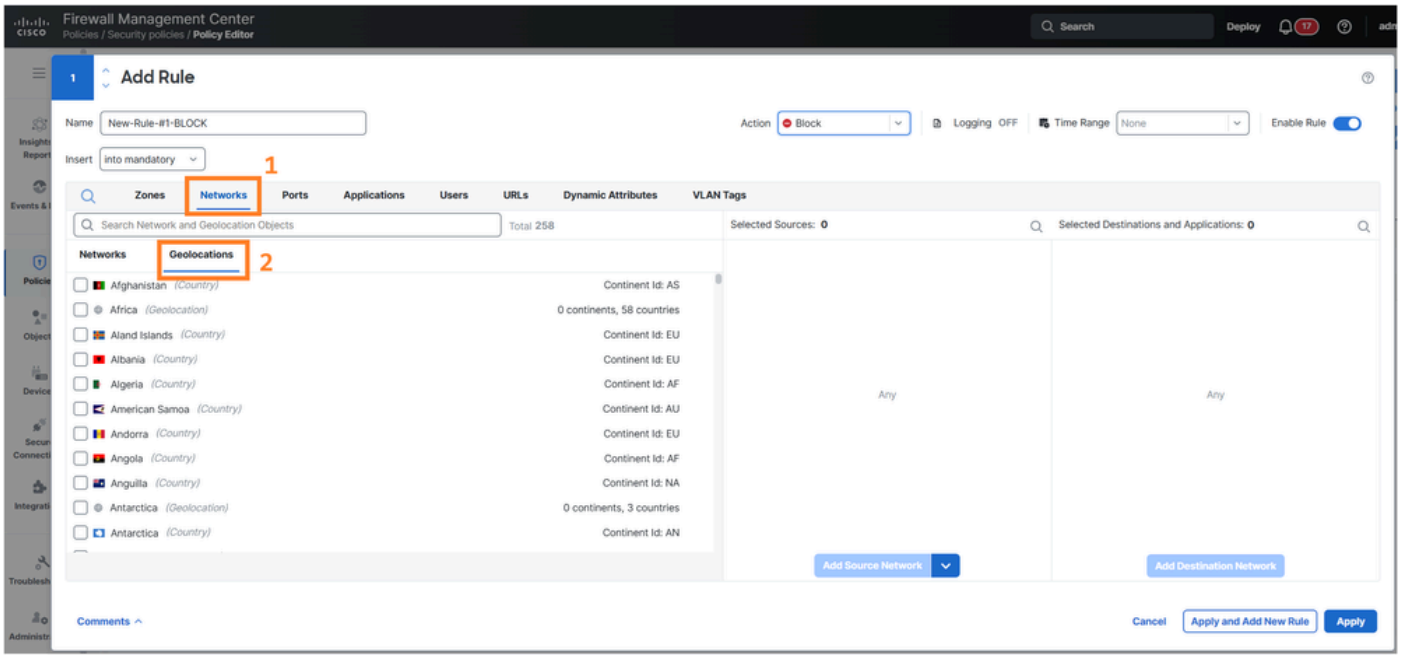
- FTD软件版本7.1。其他软件版本也受到影响。
- Cisco Secure Firewall Management Center(FMC)软件版本7.1。其他软件版本也会受到影响。

分辨率

使用FMC用户界面(UI)的“网络”(Networks)选项卡“访问控制策略规则”(Access Control Policy Rule)部分中提供的现有地理定位功能，可以有效地管理思科FTD上基于地理定位的流量过滤。 配置方法取决于特定的流量方向和策略要求。

访问地理位置配置

导航到Policies > Security policies > Policy Editor，编辑规则并在FMC UI中选择Networks > Geolocations选项卡。本节中可用的现有地理定位条目可直接用于创建访问控制策略，无需单独的地理定位对象。



规则创建策略

规则创建方法因流量方向性和策略目标而异。

阻止来自特定地理位置的入站流量

创建访问控制规则，识别源自特定地理区域的源流量并应用阻止操作。这些规则必须在规则中适当定位，以确保正确的策略实施。

控制到特定地理位置的出站流量

配置访问控制规则，以识别定向到特定地理区域的目标流量。根据安全策略，可以将这些策略配置为允许或阻止流向这些目标的流量。

单独的规则要求

实施双向地理位置过滤时，需要独立的访问控制规则，因为：

- 入站过滤需要用于评估源地理位置属性的规则。
- 出站过滤需要评估目标地理位置属性的规则。
- 流量方向性决定访问控制引擎评估哪个地理位置字段（源或目标）。

具体规则配置取决于网络拓扑、安全要求以及每个地理区域的预期流量控制目标。

原因

基于地理定位的访问控制实施非常复杂，需要基于流量方向的不同规则类型和配置，因此需要对其进行澄清。安全策略访问控制规则的“网络”(Networks)选项卡中预先存在的地理定位条目的可用性可能会造成策略实施是否需要额外创建对象的混乱。

相关内容

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。