在安全防火墙威胁防御上为远程访问VPN配置基于地理定位的策略

目录

简介

本文档介绍根据安全防火墙威胁防御(FTD)上的特定地理位置允许或拒绝RAVPN连接的过程。

先决条件

要求和限制

Cisco 建议您了解以下主题：

- 安全防火墙管理中心(FMC)
- 远程访问VPN(RAVPN)
- 基本地理位置配置

基于地理定位的策略的当前要求和限制如下：

- 仅在FTD 7.7.0+版本上受支持，由FMC 7.7.0+版本管理。
- 在安全防火墙设备管理器(FDM)管理的FTD上不受支持。
- 在集群模式下不支持
- 基于地理位置的未分类IP地址不按地理来源分类。对于这些情况，FMC将实施默认服务访问

策略操作。

- 基于地理定位的服务访问策略不适用于WebLaunch页面，允许您无限制地下载安全客户端。

使用的组件

本文档中的信息基于以下软件版本：

- 安全防火墙版本7.7.0
- 安全防火墙管理中心版本7.7.0

有关此功能的完整详细信息，请参阅Cisco Secure Firewall Management Center 7.7设备配置指南中的基于地理位置管理远程用户的VPN访问部分。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

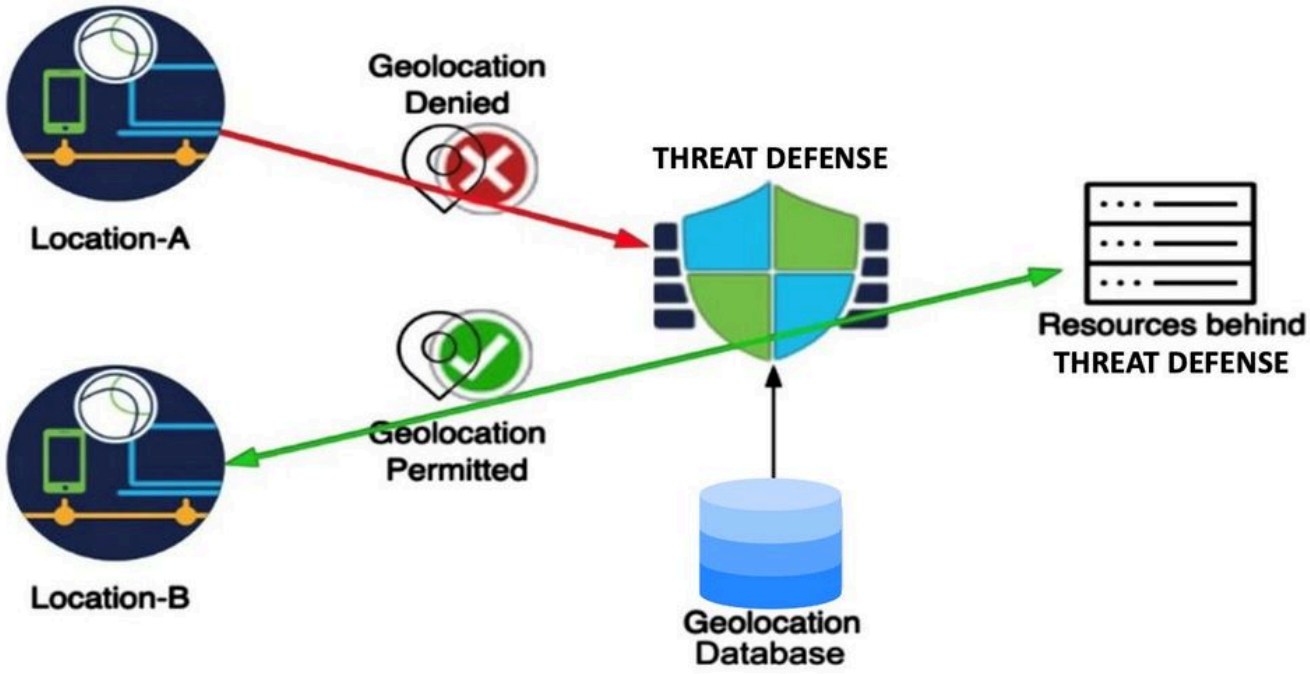
背景信息

基于地理位置的访问策略在当今的网络安全方面提供了巨大的价值，它允许基于地理位置阻止流量。传统上，组织可以为通过防火墙的一般网络流量定义流量访问策略。现在，通过引入此功能，可以对远程访问VPN会话请求应用基于地理定位的访问控制。

此功能提供以下优势：

- 基于地理定位的规则：客户可以根据特定地理位置（例如国家/地区或大陆）创建规则来允许或拒绝RAVPN请求。这样可以精确控制哪些地理位置可以启动VPN会话。
- 预身份验证阻止：这些规则为拒绝操作标识的会话在身份验证之前会被阻止，出于安全考虑，这些尝试会被正确记录。这种先发式操作有助于减少未经授权的访问尝试。
- 合规性和安全性:此功能有助于确保遵守本地组织和监管策略，同时减少VPN服务器的攻击面。

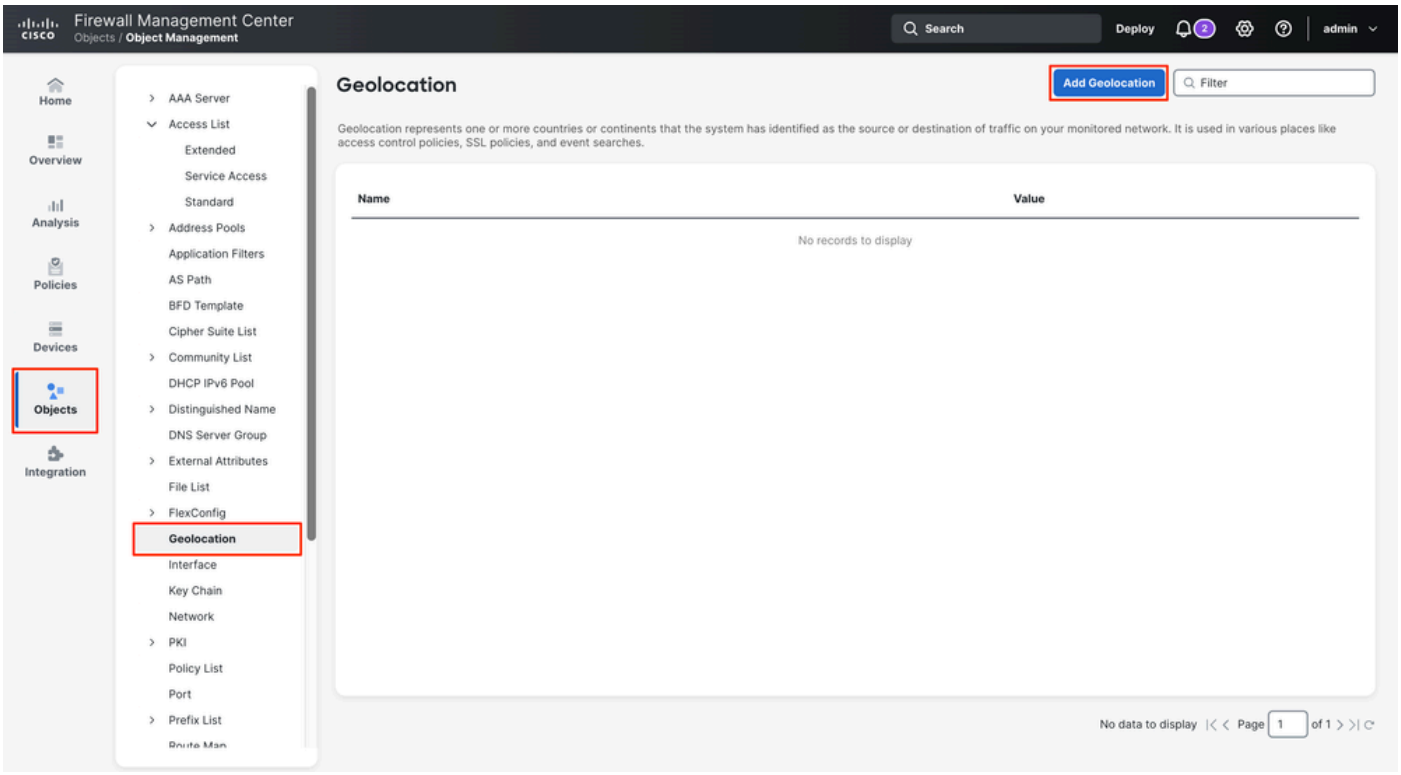
鉴于VPN服务器具有可通过互联网访问的公有IP地址，引入基于地理定位的规则使组织能够有效地限制来自特定地理定位的用户请求，从而降低暴力攻击的可能性。



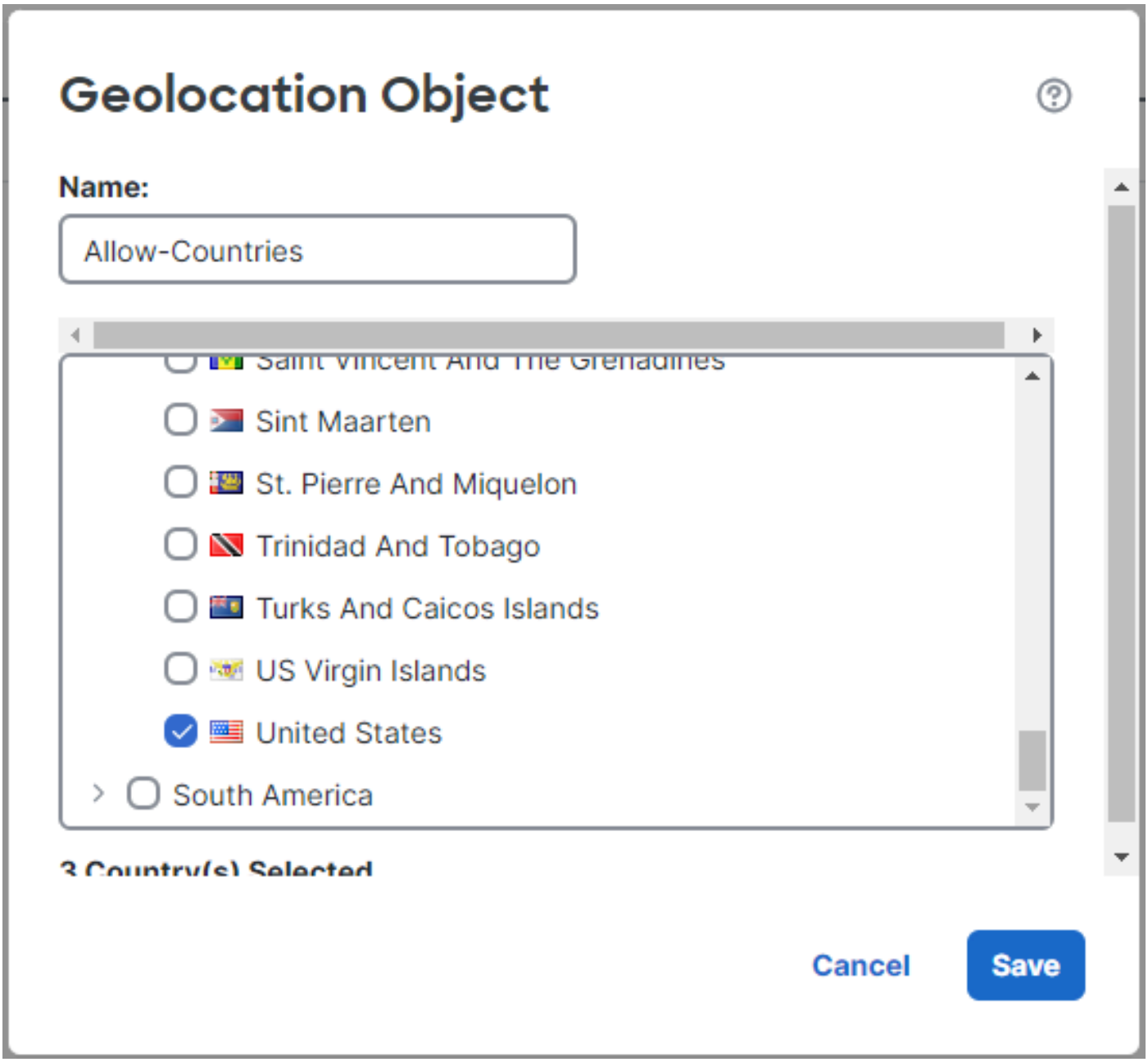
配置

步骤1.创建服务访问对象

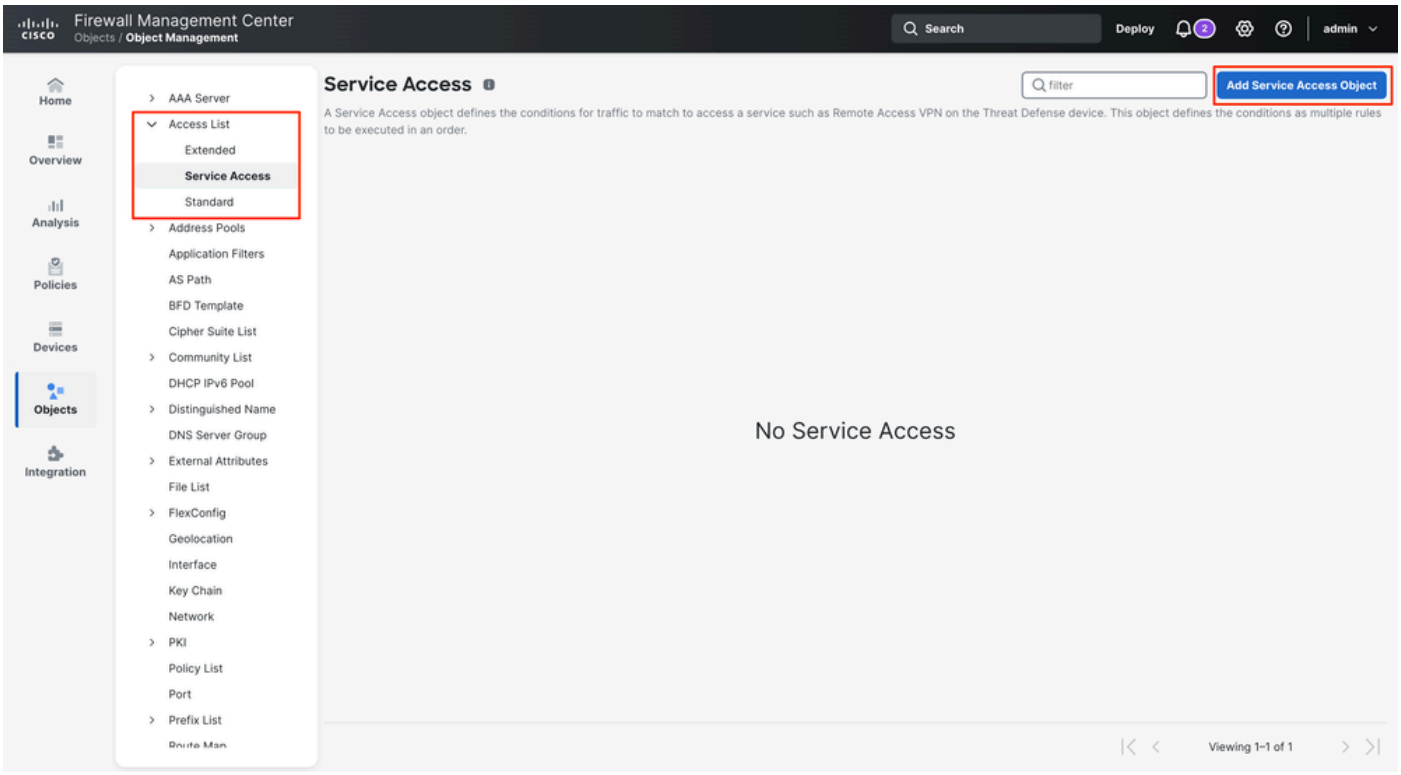
1.登录安全防火墙管理中心。
2.定位至对象 > 对象管理 > 地理定位，然后单击添加地理定位以创建地理定位对象。



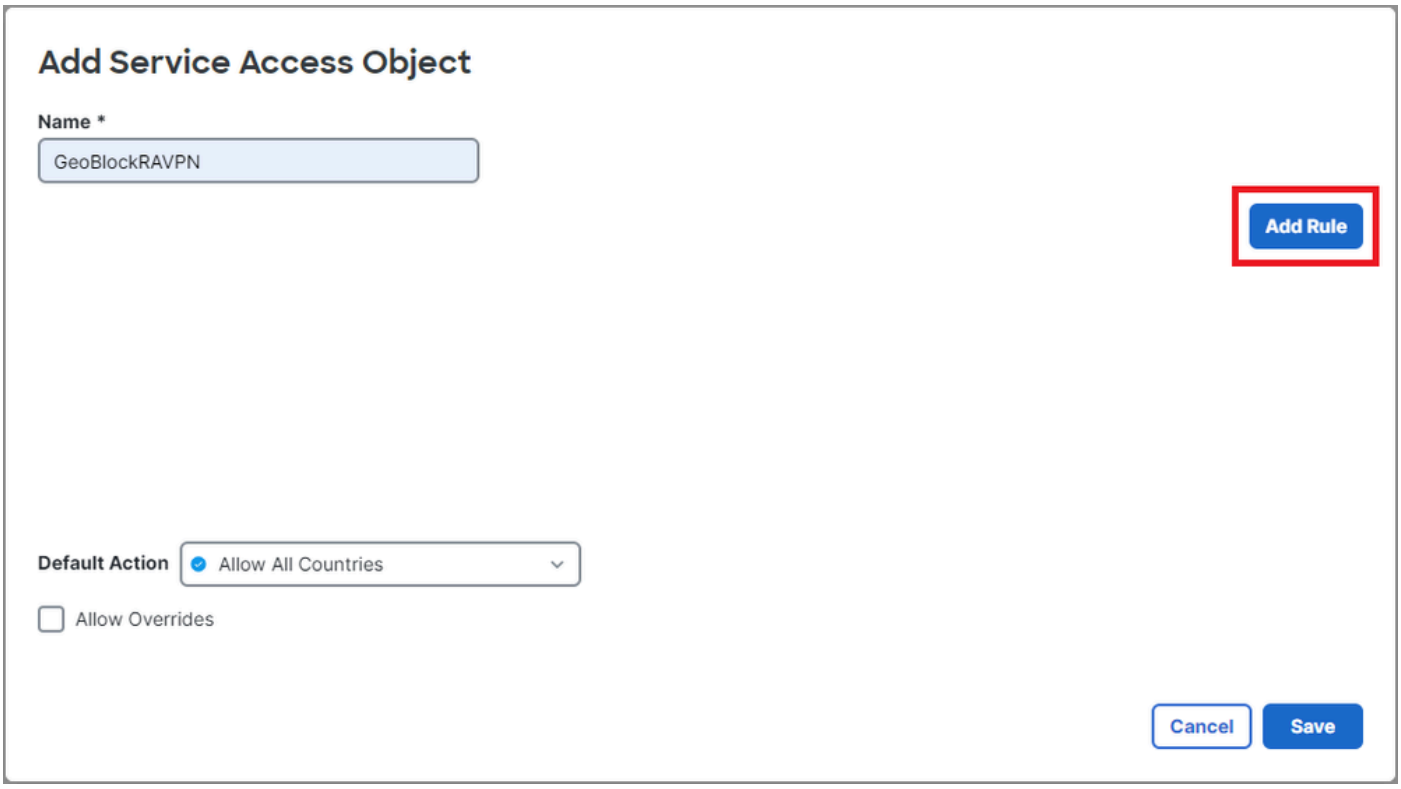
3.根据对象是被允许还是被拒绝，通过为每个组选择适当的国家/地区标志来创建对象。



4.创建地理定位对象后，转至“对象”>“对象管理”>“访问列表”>“服务访问”，然后单击添加服务访问对象。



5.定义规则名称，然后单击Add Rule。

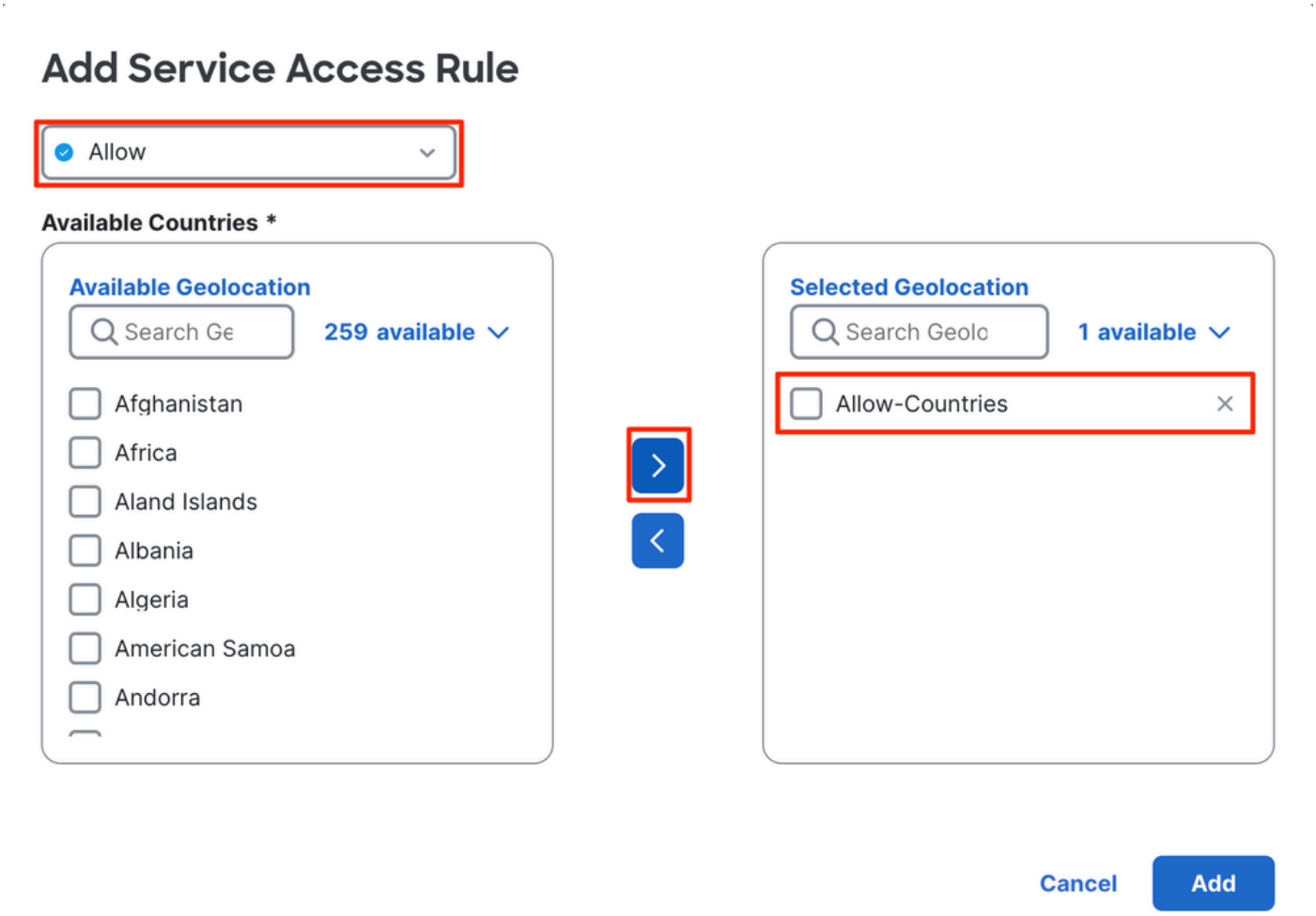


6.选择规则的操作（允许或拒绝），找到以前创建的Geolocation对象，然后通过单击右箭头将其添

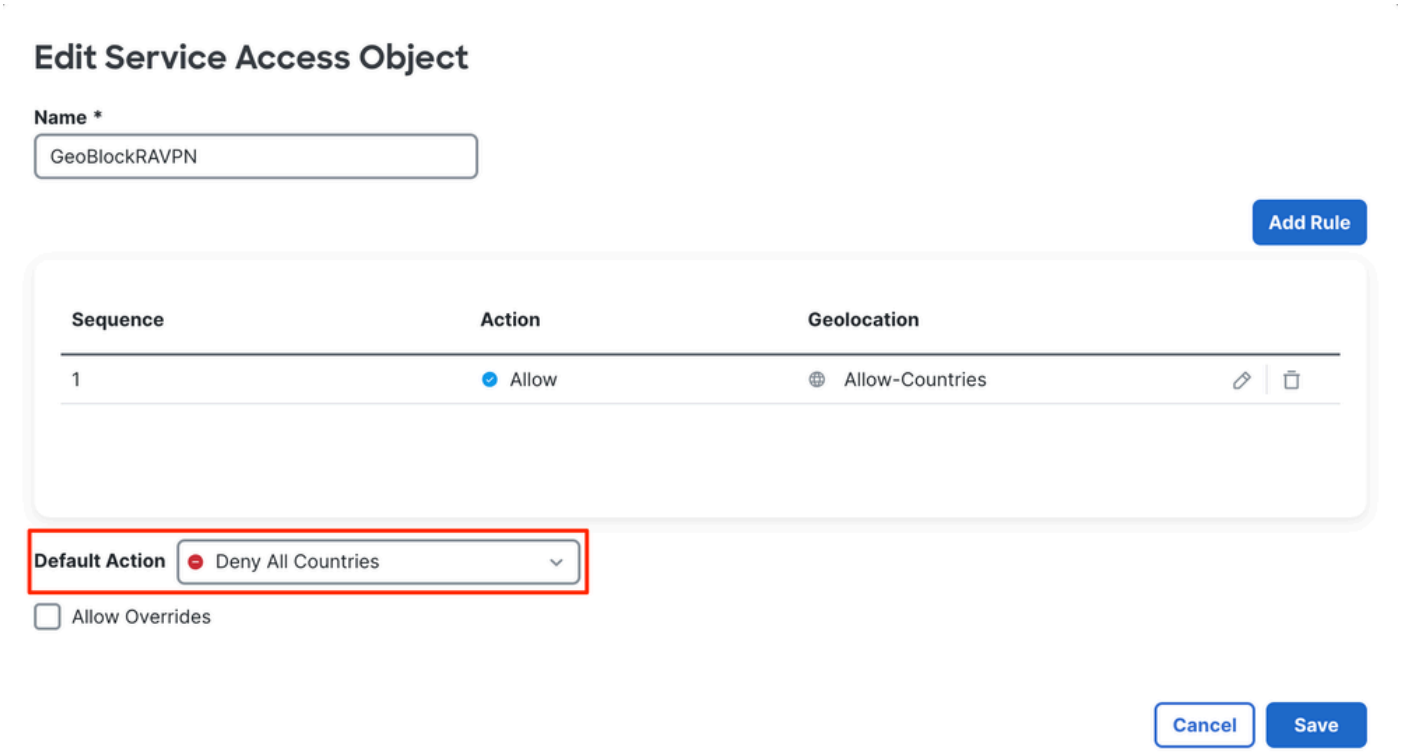
加到规则中。然后，单击Add创建规则。

注意：在服务访问对象中，地理定位对象（国家/地区、大陆或自定义地理定位）只能用于一个规则。

注意：确保以正确的顺序配置服务访问规则，因为这些规则无法重新排序。



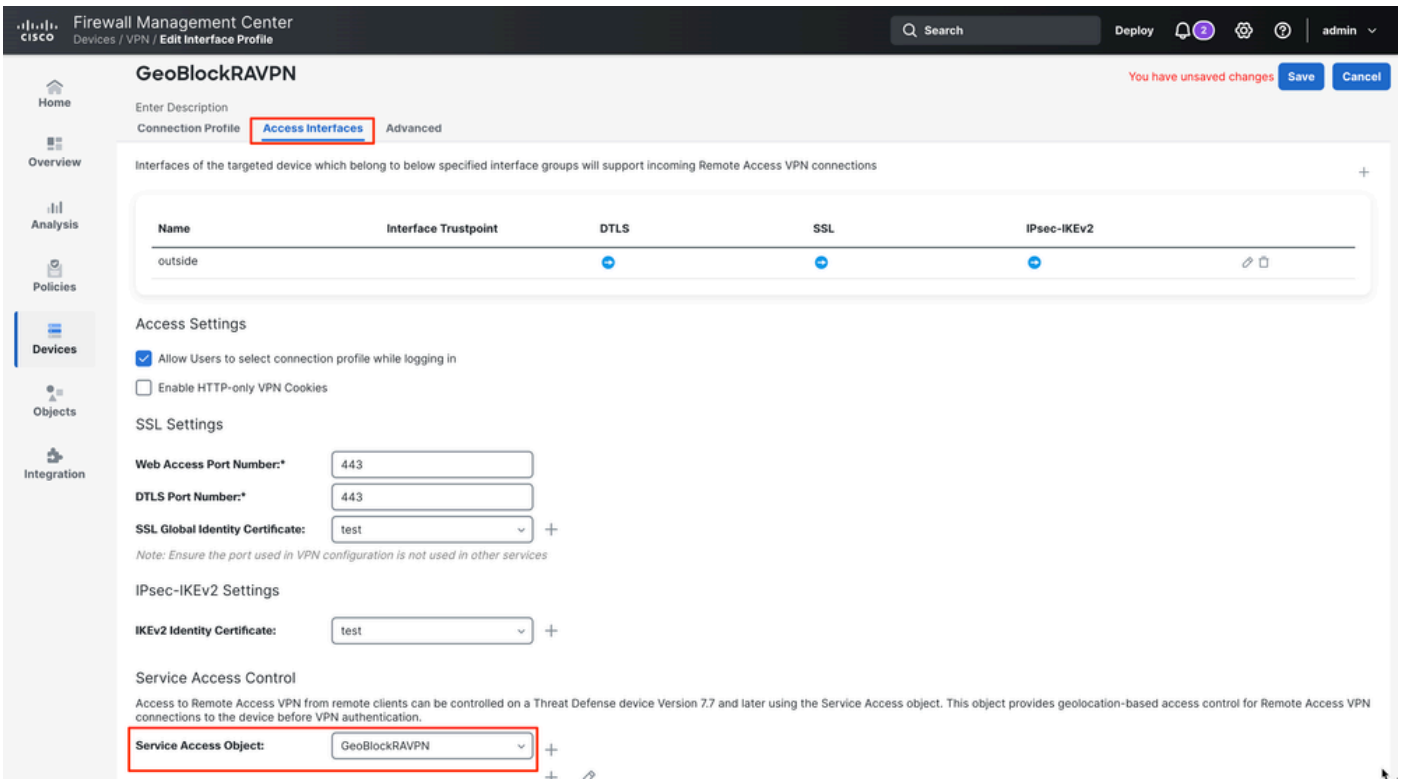
7.将默认操作更改为拒绝所有国家/地区，以拒绝来自其它国家/地区的会话请求。



步骤2.应用RAVPN中的服务对象配置。

1.导航到设备>远程访问> RAVPN配置对象>访问接口中的RAVPN配置。

2.在服务访问控制部分，选择之前创建的服务访问对象。

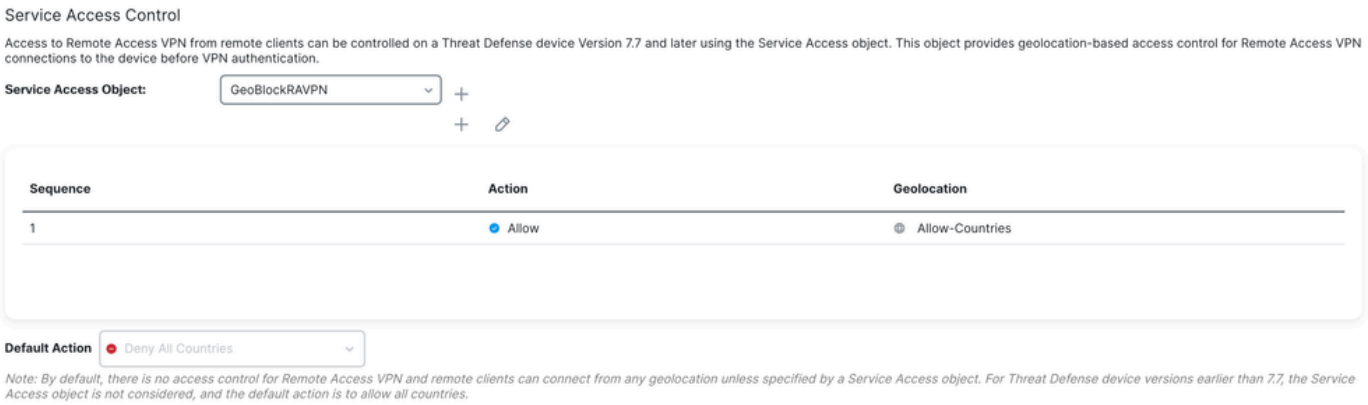


3.您选择的“服务访问”对象现在显示规则摘要和默认操作。

4.最后，保存更改并部署配置。

验证

保存配置后，规则将出现在服务访问控制部分中，允许您验证哪些组和国家/地区被阻止或允许。



运行 show running-config service-access 命令，确保服务访问规则可从FTD CLI获得。

<#root>

```
firepower#
```

show running-config service-access

```
service-access permit ra-ssl-client ra-ikev2 geolocation FMC_GEOLOCATION_8589938211_418243765
service-access deny ra-ssl-client ra-ikev2 geolocation FMC_GEOLOCATION_8589938211_487190092
service-access permit ra-ssl-client ra-ikev2 geolocation any
```

系统日志和监控

安全防火墙引入新的系统日志ID来捕获与基于地理定位的策略阻止的RAVPN连接相关的事件：

- 761031：指示基于地理定位的策略拒绝IKEv2连接的时间。此系统日志是现有VPN日志记录类的一部分。

%FTD-6-751031:根据基于地域的规则(geo=<country_name>, id=<country_code>)，拒绝faddr <client_ip> laddr <device_ip>的IKEv2远程访问会话

- 751031：指示基于地理定位的策略拒绝SSL连接的时间。此系统日志是现有WebVPN日志记录类的一部分。

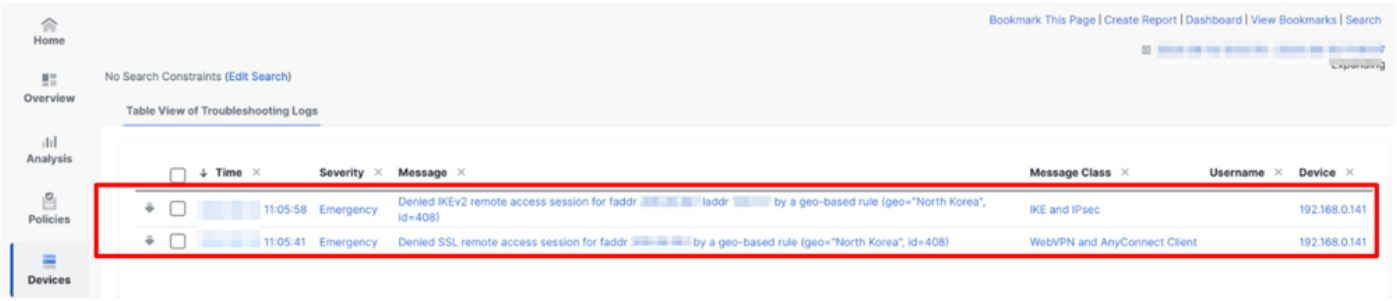
%FTD-6-716166:已拒绝基于地理位置的规则(geo=<country_name>, id=<country_code>)为faddr <client_ip>进行的SSL远程访问会话

注意：从相应的日志记录类启用时，这些新系统日志的默认严重性级别为informational。但是，您可以单独启用这些系统日志ID并自定义其严重性。

监控被阻止的连接

要验证阻止的连接，请导航到设备 > 故障排除 > 故障排除日志。此处显示与受阻连接相关的日志，包括影响连接的规则和会话类型的信息。

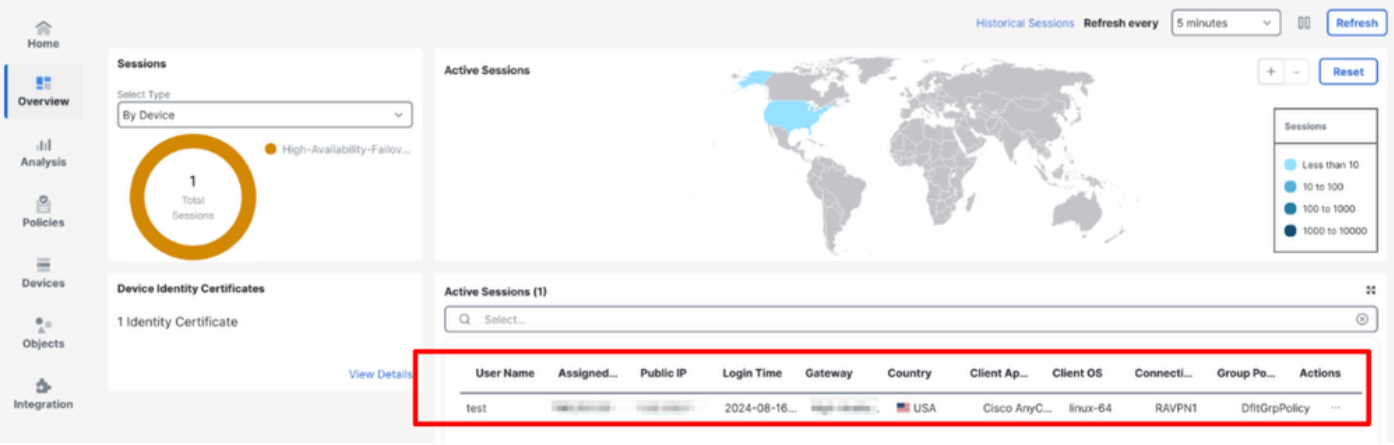
注意：必须将系统日志配置为在故障排除日志中收集此信息。



监控允许的连接

在Overview > Remote Access VPN dashboard中监控允许的会话，其中显示会话信息，包括源国家/地区。

注意：此控制面板中仅显示来自允许连接的国家和用户的连接。被拒绝的连接不会显示在此控制面板中。



故障排除

要进行故障排除，请执行以下步骤：

1. 验证规则在服务访问对象中是否正确配置。
2. 检查当允许的地理定位请求会话时，Troubleshooting Logs部分中是否显示拒绝系统日志。
3. 确保FMC中显示的配置与FTD CLI中的配置匹配。
4. 使用以下命令收集更多详细信息，这些信息对故障排除很有帮助：

- 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 context
- show geodb counters
- show geodb ipv4
- show geodb ipv6

相关信息

- 如需更多帮助，请联系TAC。需要有效的支持合同：思科全球支持联系人。
- 您还可以在此处访问Cisco VPN社区。

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）。