在安全防火墙FTD上启用威胁检测的地理定位部署故障行为

目录

问题

尝试在思科安全防火墙FTD 3105上配置基于地理位置的流量过滤时，遇到了几个问题：

- 基于地理位置的访问控制策略(ACP)和预过滤器规则未阻止HTTPS远程访问VPN(RA-VPN)连接尝试阻止区域到FTD外部接口。
- 升级到版本7.7.11后，策略中包含Netherlands或Netherlands Antilles国家/地区时，配置基于RA-VPN地理的服务访问无法部署。
- FMC部署在83%时失败，并显示以下错误消息：

```
FMC >> object-group geolocation FMC_GEOLOCATION_184683596782_116848397
FMC >> location "Netherlands"
device >> [error] :
location "Netherlands"
^
ERROR: % Invalid input detected at '^' marker.
Config Error -- location "Netherlands"
```

环境

- 由FMC管理的思科安全防火墙Firepower威胁防御(FTD)3105
- 升级的软件版本：7.7.11-1061
- 需要基于国家/地区的访问限制的RA-VPN配置

分辨率

解决方案涉及多个步骤，以正确验证基于地理位置的工作访问控制。此外，还发现启用威胁检测功能时存在限制，从而导致提供有关流量匹配行为的新指南。

1:将FMC和FTD都升级到版本7.7.11-1061以启用RA-VPN基于地理的服务访问功能，因为只有版本7.7.0及更高版本支持此功能。

2:根据Cisco文档配置基于RA-VPN地域的服务访问，并将其与RA-VPN策略相关联。

3:若要解决在添加特定国家/地区(如荷兰或荷属安的列斯)时由于Cisco Bug ID CSCwq15499而导致的部署故障，请应用以下解决方法：

1. 创建未配置国家/地区的空白RA-VPN服务访问对象。
2. 将空白服务访问对象应用于RA-VPN策略并成功部署。
3. 编辑相同的服务访问对象并添加所需的国家/地区规则。
4. 重新部署配置 — 部署现在成功，地理位置过滤处于活动状态。

4:确认部署成功完成，并且RA-VPN访问和日志反映预期的国家/地区限制。监控系统以确保地理位置限制按预期运行。

5:确定FTD上是否已启用任何威胁检测功能，该功能在流量到达访问策略之前会与其匹配。当威胁检测在策略应用之前接管时，此类配置会导致跳过地理定位规则。

<#root>

```
device# show run threat-detection
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
```

threat-detection service invalid-vpn-access
threat-detection service remote-access-authentication hold-down 1440 threshold 5
threat-detection service remote-access-client-initiations hold-down 1440 threshold 5

6:关联与威胁检测匹配和分流相关的任何系统日志ID，以确认流量正在进入威胁检测而不是地理定位。

- %FTD-4-401002:舜补充说：IP_address IP_address port port
- %FTD-4-401003:Shun已删除：IP地址
- %FTD-4-401004:避开的数据包：IP_address ==> IP_address on interface_name
- %FTD-4-733102:威胁检测将主机主机添加到规避列表
- %FTD-4-733103:威胁检测从规避列表中删除主机主机
- %FTD-4-733201:威胁检测：Service[remote-access-client-initiations] Peer[peer-ip]:超过值的故障阈值：正在向接口接口添加shun。SSL:RA过多的客户端启动请求。
- %FTD-4-733201:威胁检测：Service[remote-access-client-initiations] Peer[peer-ip]:超出阈值故障阈值：正在向接口接口添加shun。IKEv2:RA_excessive_client_initiation_requests

```
<164>Feb 26 2026 23:05:45: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:07:36: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:12:25: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:00:00: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
---
device# show shun
```

原因

遇到的问题有两个明显的根本原因：

- 地理位置规则匹配限制：仅支持从软件版本7.7.0及更高版本开始的RA-VPN基于地理位置的访问控制。此外，配置的RAVPN威胁检测可以对流量执行操作，这阻止其在基于地理的规则上进行匹配。
- Cisco Bug ID CSCwq15499（仅限注册用户）：在版本7.7.11上，由于RA-VPN地理服务访问处理机制中存在已知软件漏洞，将某些国家/地区添加到RA-VPN基于地理服务的服务访问策略时，会发生部署失败。

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）。