

安全防火墙FTD版本要求的基于RAVPN地理定位的策略配置

目录

[问题](#)

[环境](#)

[分辨率](#)

[原因](#)

[相关内容](#)

- [问题](#)
 - [环境](#)
 - [分辨率](#)
 - [原因](#)
 - [相关内容](#)
-

问题

为AnyConnect安全套接字层虚拟专用网络(SSL VPN)连接配置了基于地理定位的过滤规则的访问控制策略未按预期运行。该策略包括一条规则，专门设计为仅允许来自沙特阿拉伯的AnyConnect SSL VPN连接。这些规则用于根据来源国识别和过滤流量的基于地理位置的访问控制策略功能当前的Cisco Secure Firewall Threat Defense(FTD)v 7.0.9无法正常工作。

环境

- Cisco Secure Firewall Management Center (FMC)
- 思科安全防火墙威胁防御(FTD)版本7.0.9
- 使用地理位置服务进行Firepower应用控制
- AnyConnect SSL VPN配置，包含基于地理定位的访问控制规则
- 配置了国家/地区特定过滤的访问控制策略

分辨率

RAVPN功能的基于地理位置的访问控制策略需要FTD 7.7版或更高版本才能正常工作。由于当前环境运行的是FTD版本7.0.9，因此必须升级才能解决此问题。

- FMC升级优先级：必须首先升级FMC，并且必须运行等于或高于目标FTD版本的版本。确保在升级FTD之前相应升级FMC。
- 配置备份：在启动升级过程之前，对FMC和FTD配置进行完全备份。
- 维护窗口：规划维护窗口，因为升级过程需要重新启动设备并且可能导致临时流量中断。
- 版本说明回顾：查看每个临时版本和目标版本的版本说明，了解任何已知问题或注意事项。

原因

从FTD 7.7版及更高版本开始，仅支持远程访问虚拟专用网络(RAVPN)的基于地理定位的访问控制策略功能。当前的FTD 7.0.9版不支持此功能，这会阻止基于地理定位的过滤规则在访问控制策略中正常运行。

相关内容

- [配置基于地理定位的安全防火墙威胁防御策略](#)
- [思科安全防火墙威胁防御软件下载 — 7.7.11版](#)
- [Cisco Secure Firewall Management Center升级规划指南](#)
- [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）。