安全访问RA-VPN IPv6连接失败 — 协议配置问题

目录

问题

通过IPv6到Cisco Secure Access的RA-VPN连接无法建立，Cisco Secure Client UI显示一般连接失败消息。该问题影响使用现有RA-VPN配置文件对基于IPv6的远程访问连接的测试。研究表明，SSE RA-VPN配置文件未正确设置IPv6连接的协议字段。

环境

- 安全访问 — 安全客户端远程访问
- Cisco安全客户端尝试IPv6远程访问连接

分辨率

要解决IPv6 RA-VPN连接故障，必须在RA-VPN配置文件中正确配置IP Protocol Supported设置。按照以下步骤启用IPv6支持。

步骤 1：访问客户端设置

导航到Cisco Secure Access管理界面中的Client Settings部分。

步骤 2：配置管理员设置

在Client Settings中，找到并访问Administrator Settings部分。

步骤 3：设置支持的IP协议

配置IP Protocol Supported下拉列表以包括IPv6支持。此设置控制RA-VPN配置文件为客户端连接支持哪些IP协议。

步骤 4：保存配置

保存更新的RA-VPN配置文件配置以确保应用IPv6协议设置。

步骤 5：测试连接

使用Cisco安全客户端重新测试IPv6 RA-VPN连接，以验证连接现在是否成功建立。

原因

IPv6 RA-VPN连接故障的根本原因是RA-VPN配置文件中的IP Protocol Supported设置未配置为支持IPv6连接。SSE RA-VPN配置文件需要显式配置协议字段以启用IPv6连接。如果未正确配置此设置，Cisco安全客户端将无法建立到Cisco安全访问平台的基于IPv6的VPN连接。

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）。