采用TLS/DTLS和IPsec(IKEv2)双配置的思科安全访问RAVPN协议行为

目录

问题

当主协议设置为IPsec(IKEv2)的思科安全接入RAVPN中同时启用TLS/DTLS和IPsec(IKEv2)协议时，尝试从阻止IPsec流量（UDP端口500/4500）的网络建立VPN连接时会出现连接故障。安全客户端默认为客户端UI下拉菜单中的IPsec选项，并且在IPsec连接发生故障时不会自动故障切换到TLS/DTLS，从而导致连接错误和无法从受限网络环境中建立RAVPN连接。

环境

- 采用双协议配置的思科安全访问RAVPN
- TLS/DTLS和IPsec(IKEv2)协议均启用
- 配置为IPsec(IKEv2)的主协议设置
- 包含单独IPsec和TLS选项的“使用协议选择的安全客户端”下拉列表
- 网络环境阻止UDP端口500和4500上的IPsec流量

分辨率

所观察到的行为是预期行为，而且是由设计造成的。当两个协议都启用且主协议遇到连接问题时，思科安全访问RAVPN不会执行从IPsec(IKEv2)到TLS/DTLS的自动协议故障切换。

需要手动选择协议

从阻止IPsec流量的网络进行连接时，用户必须在安全客户端中手动选择适当的协议：

步骤 1：打开安全客户端应用程序

步骤 2：在客户端界面中定位协议选择下拉菜单

步骤 3：手动将选择从IPsec选项更改为TLS选项

步骤 4：使用TLS/DTLS协议启动VPN连接

协议行为说明

Cisco Secure Access RAVPN中的Primary protocol设置确定安全客户端中显示的默认协议，但不启用自动故障切换功能。同时启用TLS/DTLS和IPsec(IKEv2)时：

- 安全客户端在下拉菜单中显示单独的协议选项
- 客户端默认为Primary protocol设置（本例中为IPsec）
- 根据网络连接条件，协议之间不会进行自动交换
- 用户必须根据其网络环境手动选择适当的协议

原因

Cisco Secure Access RAVPN设计时没有自动协议故障切换功能。当同时启用TLS/DTLS和IPsec(IKEv2)协议时，系统需要通过安全客户端接口手动选择协议。Primary protocol设置仅确定客户端下拉菜单中的默认选择，并且在主协议遇到连接问题时不会实现自动交换逻辑。

相关内容

- 思科安全访问文档
- 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）。