远程访问用户无法通过RAVPN访问内部服务

目录

问题

使用Secure Access的远程访问用户无法访问内部服务，包括总部的域控制器，而Internet访问仍然正常工作。用户可以成功浏览Internet，但无法访问内部资源，例如RAVPN上的域控制器（远程访问VPN）。

环境

- 思科安全访问 — 安全客户端远程访问（VPN、状态、专用资源）
- 报告为up且正常的RAVPN（远程访问VPN）隧道
- 正在使用SD-WAN基础设施
- 总部的内部DNS服务器
- 总部位置的域控制器服务
- 通过基础设施连接多个分支机构网络

分辨率

为了解决远程访问连接问题，执行了以下故障排除和解决步骤：

步骤 1：数据包捕获分析

从客户端和边缘设备（双向）收集同步数据包捕获，以分析流量流模式。

流程：

RA VPN客户端----------Cisco安全访问--------Ipsec隧道----------边缘设备---------专用资源

- 确认来自客户端的DNS查询是否成功到达边缘设备并要发送到DNS服务器。
- 检查是否观察到从本地DNS服务器向客户端返回的DNS应答
- 本地DNS服务器正在发送响应，但这些响应从未返回到隧道接口。

步骤 2：根本原因识别

根据数据包捕获分析，该问题被确定为返回路径路由问题。流量分析显示，当DNS查询通过思科安全访问基础设施成功到达本地DNS服务器时，包含DNS响应的返回流量由于基础设施上的路由或配置问题未到达远程访问客户端。

步骤 3：配置审核和补救

检查并纠正内部网络配置和内部网络配置，特别关注：

- DNS配置和返回流量路由
- VPN返回流量的内部路由策略
- 内部网络路由配置
- 边缘设备端缺少配置元素

步骤 4：服务恢复验证

经过配置审查和更正后，安全访问功能已基本恢复。大多数远程访问用户重新获得了内部服务（包括总部的域控制器）的访问权限。

原因

根本原因确定为内部网络基础设施内的返回路径路由问题。来自远程访问客户端的DNS查询通过思科安全访问基础设施成功到达本地DNS服务器时，包含DNS响应的返回流量未正确路由回客户端。这是由于内部网络基础设施端缺少配置或配置不正确导致DNS应答和TCP响应无法通过VPN连接访问远程访问客户端。

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）。