通过Palo Alto和安全访问NTG从RAVPNaaS排除PR可达性故障

目录

问题

用户使用Cisco安全客户端成功建立了云VPN连接，但在连接后无法访问内部私有资源。在后端检查期间，VPN隧道似乎在安全访问端连接，但连接的用户仍无法访问内部网络服务。尽管VPN身份验证和隧道建立成功，但此连接问题仍会影响用户对内部资产的访问。

环境

- 思科安全客户端
- 安全访问上的网络隧道组
- Palo Alto作为边缘防火墙
- 内部专用网络资源配置
- 安全访问远程VPN

分辨率

连接问题通过Palo Alto防火墙一侧的协作故障排除会话和隧道重置过程得到解决。

执行的故障排除步骤

步骤 1：初始连接验证

验证当前连接状态并确认安全访问端隧道在后端检查中显示为已连接。

步骤 2：隧道重置标识

使用云本地前端(CNHE)上的数据包，确保流量是否正在离开并到达Palo Alto 。

步骤 3：Palo Alto隧道重置

在Palo Alto端没有观察到流量。

步骤 4：VPN重新连接

建议执行隧道重置。重置隧道后，用户使用安全客户端重新连接到VPN，以通过重置基础设施建立新的隧道连接。

步骤 5：连接验证

重新连接后，我们确认内部资源访问已恢复，用户可以通过VPN连接成功访问内部网络服务。

原因

根本原因与Palo Alto防火墙端上的隧道状态不一致有关，即尽管VPN身份验证成功，但会阻止内部流量的正确路由。隧道重置过程清除这些状态不一致并恢复用于内部资源访问的正确连接路径。

相关内容

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）。