安全访问VPN — 无法访问Jabber

目录

问题

使用专用访问策略时，安全客户端用户无法通过安全访问VPN隧道访问内部和专用应用（例如Jabber和Epic）。用户尝试通过VPN连接访问这些关键业务应用时遇到了连接故障。在故障排除期间，观察到来自安全访问VPN隧道的ping和TCP SYN流量的Epic资源的单向流量，但在Palo Alto防火墙上发现返回流量验证问题。此外，记录了Jabber可达性问题，其中CUCM FQDN通过内部DNS解析，而流量引导配置为基于IP的路由，从而导致流量不匹配。

环境

- 使用VPN隧道配置的思科安全访问
- 用于VPN连接的安全客户端
- 私有访问策略实施
- 适用于Jabber服务的思科统一通信管理器(CUCM)
- Epic应用程序资源
- Palo Alto防火墙用于网络安全
- CUCM FQDN的内部DNS解析

分辨率

解决方案涉及多个配置更改和故障排除步骤，以通过安全访问VPN隧道恢复与内部应用的连接：

子网配置和隧道修改

步骤 1：向VPN隧道添加其他子网

受影响的资源的VPN隧道配置中添加了其他子网。实施此更改后，之前无法访问的资源开始成功加

载。

CUCM IP地址引导配置

步骤 2：配置CUCM IP引导

为了解决在流量引导基于IP时通过内部DNS解析CUCM FQDN的Jabber连接问题，将CUCM IP地址引导至安全客户端。此配置更改使DNS解析与流量控制机制保持一致。

步骤 3：创建访问策略规则

创建访问策略规则以允许与CUCM IP地址的可达性。此规则恢复到CUCM基础设施的正确连接，从而通过VPN隧道启用Jabber功能。

静态路由配置

步骤 4：配置CUCM子网的静态路由

确保CUCM IP地址和整个CUCM子网包括在网络隧道的静态路由表中。此配置可确保正确路由安全客户端用户池和CUCM基础设施之间的流量。

返回流量验证

步骤 5：验证数据包流和返回流量

验证数据包流配置，确认返回流量可以到达安全客户端用户池。这包括检查Palo Alto防火墙配置，以确保对所有内部资源进行适当的返回路径验证，特别是对于观察到单向流量的Epic连接。

原因

连接问题是由安全访问VPN实施中的多个配置间隙引起的：

- VPN隧道中缺少子网配置，导致无法正确路由到内部应用资源
- CUCM服务的DNS解析（基于FQDN）和流量引导配置（基于IP）之间的不匹配导致Jabber连接故障

- 访问策略规则不完整，不允许流量到达CUCM IP地址
- 网络隧道配置中缺少CUCM子网的静态路由条目
- 影响双向通信的Palo Alto防火墙上的返回流量路径验证问题

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）。