思科安全访问VPN的Jabber DNS SRV记录解析问题

目录

问题

实施思科安全访问VPN时，由于DNS SRV记录解析冲突，Jabber客户端遇到连接问题。当Jabber到达两个DNS SRV记录时会发生此问题：一个用于CUCM(_cisco-UDS)，一个用于ExpressWay(_collab-edge)。 如果CUCM SRV记录解析，无论它是否工作，Jabber都假定它是本地的，并尝试连接到CUCM而不是ExpressWay。此行为在Jabber日志记录中很明显，在Jabber.log中看到bEdgeServerFlag = 0。此外，ExpressWay SRV记录会失败，因为它正被发送到安全客户端用于解析的专用DNS服务器，并且专用DNS服务器不会递归查找此公共SRV记录。

环境

- 思科安全访问（以前称为Cisco AnyConnect安全移动客户端）
- Cisco Jabber客户端
- 思科统一通信管理器 (CUCM)
- 用于移动和远程访问的Cisco ExpressWay
- 具有专用和公共DNS服务器的DNS基础设施
- 具有分割隧道功能的VPN隧道配置

分辨率

通过通过VPN隧道路由Jabber流量而不是尝试手动配置客户端进行ExpressWay连接，解决了此问题。此方法可确保Jabber流量使用适当的DNS解析路径，并避免SRV记录冲突导致客户端错误地假设本地连接。

故障排除步骤

步骤 1：使用wireshark数据包捕获分析DNS SRV记录查询。

```
Use Wireshark filter: dns.qry.type == 33
```

步骤 2：查看Jabber日志，了解边缘服务器标志状态

```
Check Jabber.log for: bEdgeServerFlag = 0
```

步骤 3：验证两个SRV记录的DNS解析行为

检查分辨率：

- _cisco-UDS SRV记录(CUCM)
- _collab-edge SRV记录(ExpressWay)

解决方案实施

配置Cisco安全访问VPN客户端，使其在隧道中包括Jabber流量，而不是允许其通过本地/专用DNS服务器解析DNS查询。这可确保：

- Jabber流量使用正确的DNS解析路径
- 避免SRV记录冲突
- ExpressWay连接已正确建立
- 保持完整的Jabber功能

此解决方案优先于手动配置用于ExpressWay的Jabber客户端，这会导致某些功能丢失。

原因

根本原因是Jabber客户端中的DNS SRV记录解析逻辑。当Jabber启动时，它会查询两个特定的DNS SRV记录：_cisco-UDS（适用于CUCM）和_collab-edge（适用于ExpressWay）。 客户端决策过程会优先处理CUCM SRV记录 — 如果此记录成功解析，Jabber会假定它在本地环境中运行并设置bEdgeServerFlag = 0，而不管实际的CUCM连接是否工作或者ExpressWay SRV记录是否也解析。

在使用分割隧道的VPN场景中，ExpressWay SRV记录(_collab-edge)被发送到安全客户端使用的专用DNS服务器。由于这通常是公共DNS记录，并且专用DNS服务器不对外部记录执行递归查找，因此ExpressWay SRV解析失败。此复合问题导致Jabber无法通过任一路径建立正确的连接。

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）。