排除Webex呼叫SIP中继故障 — 防火墙阻止来自Webex对等体的入站连接

目录

问题

配置为连接到音频代码会话边界控制器(SBC)的Webex呼叫SIP中继显示“已损坏”状态。中继使用TCP端口5062为基于证书的信令进行了配置。虽然从SBC到所有四个Webex对等体(peering1-4.eun.sipconnect.bcld.webex.com)的出站SIP选项成功并收到了正确的响应，但是对于某些对等体，尤其是标记为“EUN 2和4”的对等体，从Webex到SBC的入站SIP选项失败。

观察到的具体错误为：

```
Failed to connect out to
atstesbc.bmd.com
./213.33.78.212:5062io.netty.channel.ConnectTimeoutException: connection timed out after 2000 ms:
atstesbc.bmd.com
./213.33.78.212:5062
```

防火墙数据包捕获显示来自Webex对等体的入站TCP SYN数据包到达防火墙，但是没有观察到从SBC返回的相应SYN-ACK或RST数据包，从而阻止成功完成TCP会话建立和后续SIP选项运行状况检查。

环境

- 基于Webex呼叫证书的SIP中继
- AudioCodes会话边界控制器
- TCP端口5062，用于通过TLS信令的SIP
- 四个Webex对等点：peering1-4.eun.sipconnect.bcld.webex.com
- Webex云和客户SBC之间的防火墙基础设施
- 组织ID:173b6146-6c50-4890-9ccc-43f73b6c85d5

分辨率

通过重置防火墙连接解决了此问题，该连接恢复了所有Webex对等体和SBC之间的SIP OPTIONS运行状况检查的正确双向连接。

执行的诊断步骤

步骤 1：已验证中继配置和DNS解析。

已确认SBC可以成功解析所有四个Webex对等体FQDN并建立到每个对等体的出站连接。

步骤 2：已分析防火墙数据包捕获。

在SIP OPTIONS测试期间，从防火墙入口和出口接口收集同步数据包捕获。捕获显示：

- 来自Webex对等体的入站TCP SYN数据包到达防火墙。
- 未从SBC发送回SYN-ACK或RST响应。
- TCP握手无法针对特定对等体连接完成。

步骤 3：已检查SBC系统日志和跟踪。

SBC日志在连接建立时显示成功的TLS握手，但没有可解释连接超时的传输错误或证书故障。

步骤 4：重置防火墙连接。

防火墙连接已重置，以清除可能阻止正确双向通信的任何过时的会话状态或连接跟踪条目。

确认

防火墙连接重置后，SIP中继状态从“已损坏”更改为可操作，所有四个Webex对等体都成功双向完成SIP选项运行状况检查。

原因

根本原因是防火墙基础设施阻止或丢弃从特定Webex对等IP地址到端口5062上的SBC的入站TCP连接。这阻止了通过TLS信令的SIP所需的TCP握手完成，从而导致中继运行状况检查失败并导致“已损坏”状态。此问题可能是由过时的防火墙连接状态、非对称路由或安全策略干扰某些Webex云对等体的入站会话建立引起的。

相关内容

- Webex呼叫的端口参考信息
- 配置Webex呼叫的中继、路由组和拨号方案
- Webex呼叫的安全要求
- 本地网关入门
- 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）。