Troubleshoot Webex Calling SIP Trunk Impairment - Firewall Blocking Inbound Connections from Webex Peers

Contents

Issue

A Webex Calling SIP trunk configured to connect to an AudioCodes Session Border Controller (SBC) displayed an "Impaired" status. The trunk was configured for certificate-based signaling using TCP port 5062. While outbound SIP OPTIONS from the SBC to all four Webex peers (peering1-4.eun.sipconnect.bcld.webex.com) succeeded and received proper responses, inbound SIP OPTIONS from Webex toward the SBC were failing for some peers, specifically those labeled as "EUN 2 and 4".

The specific error observed was:

```
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
```

Firewall packet captures showed inbound TCP SYN packets from Webex peers reaching the firewall, but no corresponding SYN-ACK or RST packets were observed returning from the SBC, preventing TCP session establishment and subsequent SIP OPTIONS health checks from completing successfully.

Environment

- Webex Calling certificate-based SIP trunk
- AudioCodes Session Border Controller
- TCP port 5062 for SIP over TLS signaling
- Four Webex peers: peering1-4.eun.sipconnect.bcld.webex.com
- Firewall infrastructure between Webex cloud and customer SBC
- Organization ID: 173b6146-6c50-4890-9ccc-43f73b6c85d5

Resolution

The issue was resolved by resetting the firewall connections, which restored proper bidirectional connectivity for SIP OPTIONS health checks between all Webex peers and the SBC.

Diagnostic Steps Performed

Step 1: Verified trunk configuration and DNS resolution.

Confirmed that the SBC could successfully resolve all four Webex peer FQDNs and establish outbound connections to each peer.

Step 2: Analyzed firewall packet captures.

Collected synchronized packet captures from firewall ingress and egress interfaces during SIP OPTIONS testing. The captures revealed:

- Inbound TCP SYN packets from Webex peers were reaching the firewall.
- No SYN-ACK or RST responses were being sent back from the SBC.
- TCP handshakes were failing to complete for specific peer connections.

Step 3: Reviewed SBC syslogs and traces.

SBC logs showed successful TLS handshakes when connections did establish, but no transport errors or certificate failures that would explain the connection timeouts.

Step 4: Reset firewall connections.

Firewall connections were reset to clear any stale session states or connection tracking entries that can have been preventing proper bidirectional communication.

Verification

After the firewall connection reset, the SIP trunk status changed from "Impaired" to operational, with all four Webex peers successfully completing SIP OPTIONS health checks bidirectionally.

Cause

The root cause was firewall infrastructure blocking or dropping inbound TCP connections from specific Webex peer IP addresses to the SBC on port 5062. This prevented the completion of TCP handshakes required for SIP over TLS signaling, causing trunk health checks to fail and resulting in the "Impaired" status. The issue was likely due to stale firewall connection states, asymmetric routing, or security policies that were interfering with inbound session establishment from certain Webex cloud peers.

Related Content

- Port Reference Information for Webex Calling
- Configure Trunks, Route Groups, and Dial Plans for Webex Calling
- Security Requirements for Webex Calling
- Get Started with Local Gateway
- Cisco Technical Support & Downloads