Troubleshoot Webex Calling Certificate-Based SIP Trunk Registration Failure with Oracle SBC

Contents

Issue

A certificate-based SIP trunk between Webex Calling and a third-party Oracle SBC fails to register and activate. The trunk status shows as "Impaired" in Control Hub. During troubleshooting, these specific issues were identified:

- TLS connection failures related to certificate validation between the Local Gateway and Webex Calling.
- SIP OPTIONS messages sent to the Local Gateway not receiving responses.
- TCP three-way handshake not completing - SYN and SYN-ACK packets are exchanged between 170.72.242.77 and 10.8.100.2 on TCP port 5062, but the final ACK is not received.
- Repeated TCP connection attempts from Webex Calling to the Oracle SBC that fail to establish a complete session.

Environment

- Webex Calling with certificate-based SIP trunk configuration.
- Third-party Oracle Session Border Controller (SBC)
- Oracle SBC certificate chain containing GlobalSign and IdenTrust certificates.
- Network Address Translation (NAT) configuration mapping public IP 201.221.125.143 to internal IP 10.8.100.2
- Firewall and network security devices between Webex Calling and the Oracle SBC.
- TCP port 5062 used for SIP communication.

Resolution

The issue was resolved by implementing a firewall configuration change to use direct NAT mapping between the internal and public IP addresses.

Step 1: Verify Certificate Chain Compatibility

Verify that the Oracle SBC certificate issuer and certificate chain are supported by Webex Calling by comparing against the supported root certificate authority documentation.

The customer's certificate chain included:

- GlobalSign RSA OV SSL CA 2018 (intermediate certificate)
- GlobalSign Root CA - R3 (root certificate)
- IdenTrust certificates in the chain

Step 2: Analyze Network Connectivity Issues

Packet capture analysis revealed that TCP connections from 170.72.242.77 to 10.8.100.2 on TCP port 5062 were failing to complete the three-way handshake. The SBC was responding with SYN-ACK packets, but the final ACK from Webex Calling was not being received.

Step 3: Implement Direct NAT Configuration

The customer implemented a firewall change to configure direct NAT mapping between the internal IP address and the public IP address. This change resolved the TCP session establishment issues.

After the firewall configuration change:

- The trunk between Webex Calling and the SBC came online.
- TCP three-way handshake completed successfully.
- SIP OPTIONS communication was established.

Step 4: Validate Service Operation

After the resolution, the customer performed service testing and validation to confirm that traffic inspection does not impact call quality or functionality.

Cause

The root cause was a network configuration issue where the firewall's NAT implementation was preventing the completion of TCP three-way handshakes between Webex Calling and the Oracle SBC. The firewall was not properly handling the return traffic (final ACK packets) from Webex Calling to the SBC, causing TLS connection establishment failures and preventing SIP trunk registration. The direct NAT mapping configuration resolved the asymmetric routing or firewall policy issues that were blocking the TCP session completion.

Related Content

- What Root Certificate Authorities are Supported for Calls to Cisco Webex Audio and Video Platforms
- Port Reference Information for Webex Calling
- Cisco Technical Support & Downloads