Ticket 4: ABC-2854

Status: Open
Priority: High
Summary: TLS certificate validation failures causing HTTPS/WSS connection drops in enterprise environments
Reporter: Robert Chen (SecureTech Enterprises)
Assignee: Maria Gonzalez (Security Engineering)
Created Date: June 6, 2025
Updated Date: June 8, 2025

Description

Customer-Reported Symptoms: SecureTech Enterprises reports intermittent connection failures affecting 40% of Voice Receptionist sessions. Users experience sudden call disconnections after 2-5 minutes of successful operation. The issue is exclusive to their corporate network environment and doesn't reproduce on personal devices or guest networks. SSL/TLS handshake errors appear sporadically in browser console logs.

Error Messages/Logs:

```
[2025-06-06 11:28:45] ERROR TLSHandler: Certificate validation fail
[2025-06-06 11:28:46] WARN WebSocketClient: Connection dropped duri
[2025-06-06 11:28:47] ERROR CertificateChain: Intermediate certific
[2025-06-06 11:28:48] INFO RetryManager: Attempting reconnection (3
[2025-06-06 11:28:52] ERROR NetworkManager: SSL_ERROR_BAD_CERT_DOMA
```

Environmental Details: - Browser: Chrome 125.0.6422.78 (managed corporate deployment) - Corporate Security: Symantec SSL Visibility appliance with DPI - Certificate Authority: Internal PKI with custom root CA - Network Architecture: DMZ deployment with SSL bridging - Firewall: Palo Alto PA-5220 with SSL decryption enabled - Certificate Pinning: Enabled for *.anycompany.com domains - OCSP Stapling: Required by corporate security policy -

Geographic Location: Boston, MA (headquarters), Austin, TX (branch office)

Impact on Business Operations: - Executive team unable to use Voice Receptionist for board meeting preparation - Client demonstration failures during sales presentations - IT security team questioning solution's enterprise readiness - Considering alternative vendors due to security compliance concerns - Service desk tickets increased 150% related to "connection problems"

Additional Technical Context: The SSL inspection appliance appears to be interfering with the certificate chain validation process. Network traces show successful initial TLS handshake but subsequent certificate revalidation failures during WebSocket keep-alive cycles. The corporate PKI infrastructure requires specific intermediate certificate handling not currently supported by the standard certificate chain.