Troubleshooting TCN Application Access Issues through SWG.

Contents

Issue

Users are unable to access the Clear Touch Call Center (TCN) application when connected through Remote Access VPN.

The specific symptoms observed include:

- Working users appear to egress with a Cisco IP address
- Non-working users egress with a public IP address, resulting in application access errors

Environment

- Cisco Umbrella Secure Web Gateway (SWG)
- Remote Access VPN (RAVPN) connectivity
- Clear Touch Call Center Application.

Resolution

Policy.test.sse.cisco.com would show Egress IP.

The resolution was to disable QUIC protocol.

Google Chrome & Microsoft Edge

- Open the browser.

- Type `chrome://flags` (Chrome) or `edge://flags` (Edge) in the address bar and press Enter.
- Search for `QUIC` or "Experimental QUIC protocol" in the search box.
- Change the setting to **Disabled**.
- Click the **Relaunch** or **Restart** button at the bottom of the page.

Mozilla Firefox

- Type `about:config` in the Firefox address bar and press Enter.
- Search for `network.http.http3.enable`.
- Double-click the entry to set it to **false**.

Opera

- Type `opera://flags` in the address bar.
- Search for `QUIC`.
- Set "Experimental QUIC protocol" to **Disabled**.
- Relaunch the browser.

Cause

The root cause was identified as intermittent bypass of the SWG/Umbrella security infrastructure, resulting in inconsistent egress IP behavior. This bypass behavior was compounded by browser-specific QUIC protocol handling, where different browsers and configurations processed the protocol differently through the security stack. The combination of these factors caused some users to egress with public IPs instead of the expected Cisco IPs, leading to application access failures for the TCN system.

Related Content

- Umbrella Organization Dashboard
- Cisco Technical Support & Downloads