Zscaler Environment Checklist

for Presenter Webinar & WebRTC Connectivity

Purpose: If your presenting team uses Zscaler (or a similar cloud security proxy) for corporate network traffic, default inspection and routing policies can cause mid-session connection degradation, audio/video drops, or screen sharing failures. Use this checklist with your IT/network team **before** your scheduled presentation to prevent bandwidth throttling and packet loss.

1. Allowlist Required Domains

Ask your IT team to add the webinar platform's domains to the Zscaler allowlist (bypass SSL inspection and any content-filtering policies for these domains):

- [ ] Confirm the full list of required domains/subdomains with your platform provider
- [ ] Add all domains to Zscaler's **SSL Inspection bypass list**
- [ ] Add all domains to any **URL/Content Filtering allowlist**

2. Allow WebSocket Traffic

Real-time control signals, chat, and presentation states rely on persistent WebSocket connections.

- [ ] Confirm Zscaler is not terminating, throttling, or re-inspecting WebSocket (`wss://`) handshakes on the allowlisted domains
- [ ] If using SSL inspection bypass (Step 1), verify it applies to WebSocket upgrade requests specifically, not just standard HTTPS

3. Allow WebRTC Media Traffic (UDP/TCP)

High-definition outbound audio/video and screen sharing depend heavily on uninhibited UDP traffic, which traditional web proxies often degrade.

- [ ] Confirm Zscaler's firewall policy allows **outbound UDP** on the port ranges used by the platform's TURN/STUN servers
  - Confirm **STUN/TURN media traffic isn't being throttled or classified** as "P2P" or "unclassified" traffic
- [ ] If UDP cannot be allowed, confirm **TCP fallback (TURN over TCP/443)** is permitted as a backup path (though UDP is highly recommended to prevent latency)

4. Check for SSL/TLS Inspection Conflicts

- [ ] Confirm the corporate root CA used by Zscaler is properly trusted on presenter devices (prevents abrupt disconnects or handshake errors)
- [ ] Test from a representative presenter machine/browser to confirm no certificate warnings or socket resets occur during a live session

5. Review IP-Based Security & Routing Policies

Zscaler dynamic routing through shifting cloud nodes can change the apparent source IP mid-session, occasionally triggering platform security filters or unexpected packet routing delays.

- [ ] Flag to IT that presenter IPs may appear as Zscaler data center IPs, not the user's local network location
- [ ] If your platform has proxy/VPN detection or aggressive rate limiting, confirm Zscaler's known IP ranges are on any applicable exception list

6. Run a Pre-Event Presenter Test

- [ ] Have at least one presenter on the Zscaler-protected network join a **test session** at least 24 hours before the live event
- [ ] Confirm: outbound audio/video remains stable over time, screen sharing works without quality degradation, and no repeated reconnection attempts appear in the browser console

If Degradation Persists

If connection degradation or quality drops still occur after completing the steps above, gather the following before contacting support:

- Browser console logs (specifically tracking WebRTC packet loss or WebSocket disconnects)
- Confirmation of whether the presenter's device is actively routing through Zscaler at the time of the drop
- Approximate time and duration of the observed connection degradation

Providing these details helps the support team pinpoint whether the latency stems from inline proxy inspection, deep packet scanning, or external routing variables.