ACS Quickconnect Data-flow Diagram

Non-Public Application Testing · https://docs.functionize.com/hc/en-us/articles/42178425704087-ACS-Quickconnect-Data-flow-Diagram

A complete data-flow diagram of how the QuickConnect desktop agent (and the ACS agent) connects a customer host to the Functionize platform, annotated with every protocol, port, and TLS version. It's built to hand to a customer's networking/security team for sign-off.

What the diagram shows

The diagram traces **ten numbered flows**, [0]–[9], all agent-initiated and outbound, across **four trust zones**: the customer environment, Tailscale infrastructure (third-party SaaS), the Functionize GCP platform, and the Functionize-managed relay VMs.

The data path, in preference order

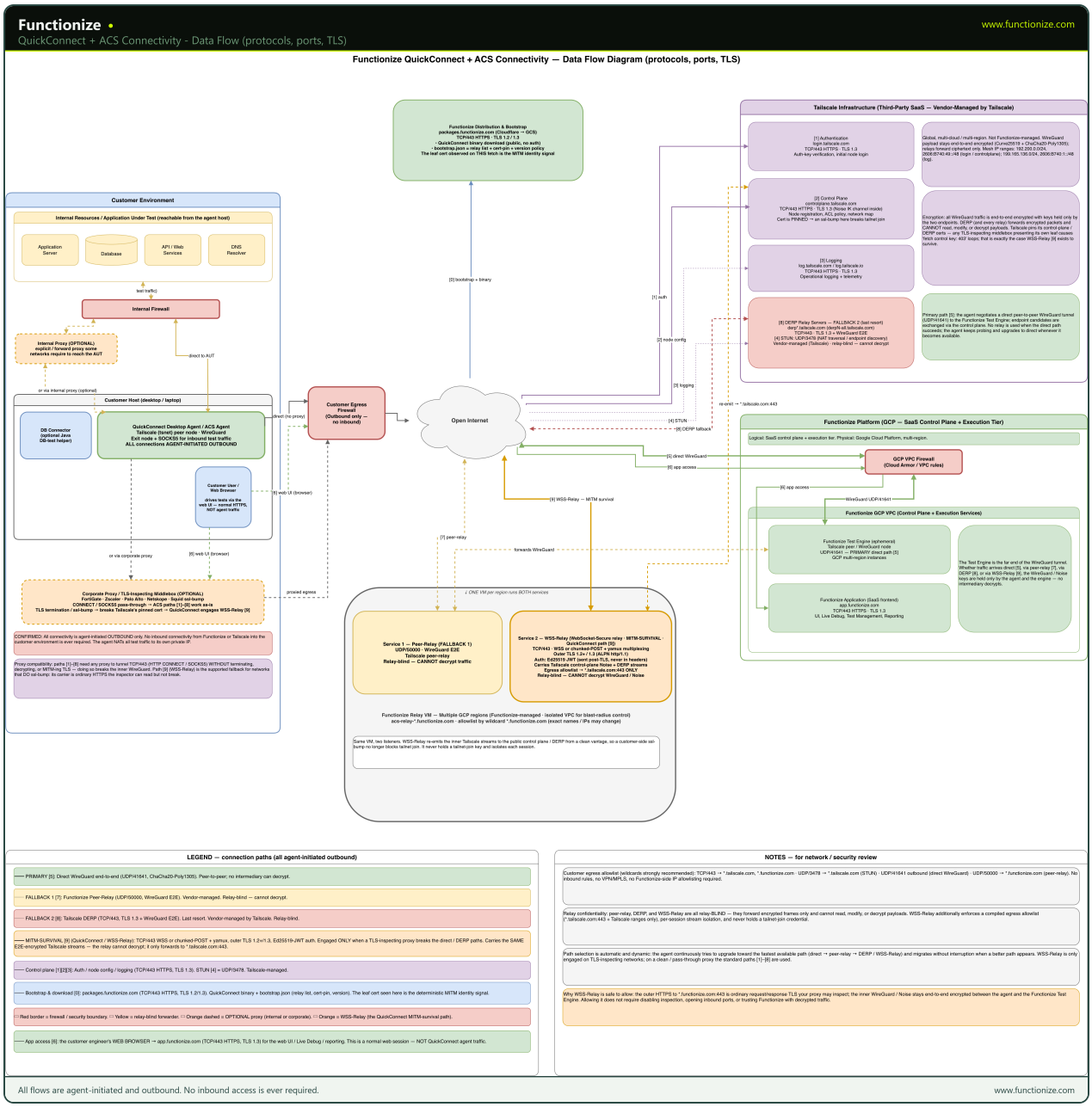
The tunnel's data path follows a fixed preference order — direct WireGuard [5] → peer-relay [7] → DERP [8] → WSS-Relay [9] — with the WSS-Relay engaged only on TLS-inspecting networks.

What your network team needs to allow

It also marks the firewalls, the optional internal and corporate proxies, and the egress allow-list: TCP/443 to `*.tailscale.com` and `*.functionize.com`, plus UDP/3478, 41641 and 50000.

Two things to read off it directly

Two review notes are worth reading off the diagram directly: **no inbound access is ever required**, and **every relay is blind to the end-to-end-encrypted payload**.



Click the diagram to open it full size (5364 px wide) — it is far too detailed to read at article width.

Functionize Quickconnect Data-flow Diagram

Related

- Functionize Quickconnect (ACS Quickconnect) — what it is and why IT can approve it
- Before You Point Studio at Your Own Application — the wider access checklist