NETWORK DOCUMENTATION

Standard remote access

Google Cloud + Cloudflare Tunnel + RustDesk + Tailscale. Firewall and connectivity requirements for customer IT.

SCOPE

Controller: Google Cloud, Cloudflare Tunnel and Tailscale. Panel PC: RustDesk. Connections start from the installed equipment; allow the corresponding return traffic. No public inbound port forwarding.

IN THIS DOCUMENT

01 Services and devices 02

02 Google Cloud 03

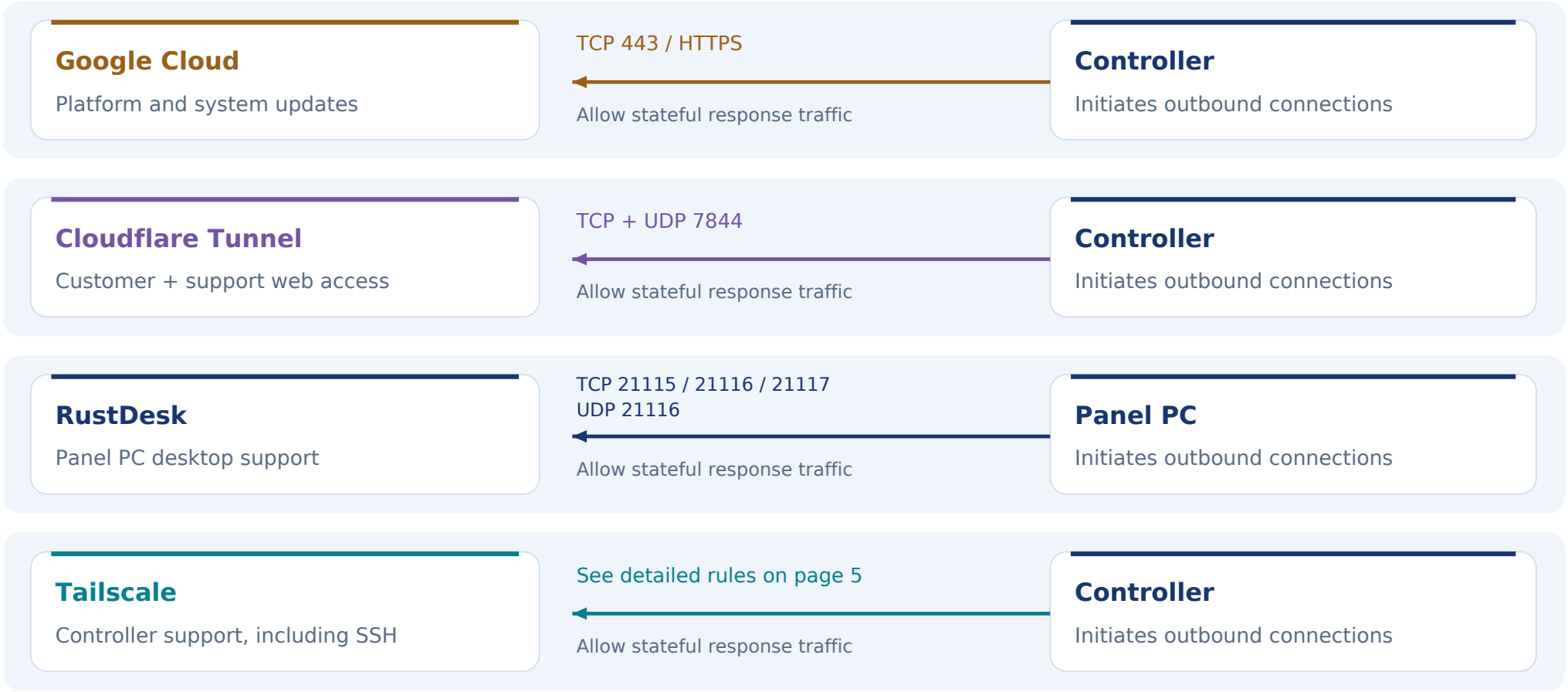
03 Cloudflare Tunnel 04

04 RustDesk and Tailscale 05

01 / STANDARD DEPLOYMENT

Four services, four roles

Customer web access, remote support and cloud operations use separate services.



Cloudflare exposes Rosepetal web software only. Shell and desktop support use Tailscale and RustDesk.

02 / CONTROLLER EGRESS

Google Cloud

Required to interact with Rosepetal Platform and manage system updates, including Docker image downloads.

Firewall setting	Required value
Direction	Outbound (egress), initiated by the Controller
Transport / destination	TCP / destination port **443**
Source port	Dynamic / ephemeral, assigned by the operating system
Application	HTTPS/TLS, with HTTP/2 and gRPC support where required
Action	Allow the connections and their return traffic through stateful inspection

AUTHORIZED DESTINATIONS BY FQDN

FQDN	Service / purpose
*.rosepetal.ai	Rosepetal services - image uploads and model training
*.pkg.dev	Artifact Registry - Docker image downloads
*.googleapis.com	Firestore, Cloud Storage and Google/Firebase authentication
*.cloudfunctions.net	Firebase Functions
*.run.app	Functions running on Cloud Run

03 / CONTROLLER EGRESS

Zero Trust Cloudflare Tunnel

Web software access for customers and remote support. No SSH or RustDesk/AnyDesk through this tunnel.

Destination	IPv4 range	Destination ports
region1.v2.argotunnel.com	198.41.192.0/24	TCP 7844 + UDP 7844
region2.v2.argotunnel.com	198.41.200.0/24	TCP 7844 + UDP 7844

TRANSPORT AND PREREQUISITES

Outbound from the Controller. UDP 7844 uses QUIC (preferred); TCP 7844 uses HTTP/2 (fallback). Request both; either protocol alone can establish the tunnel.

No fallback to 443. No proxy support. Browser HTTPS is a separate connection.

No TLS inspection. The Controller clock must be accurate, using an IT-approved NTP source. IPv4 is sufficient.

DNS AND SNI

DNS must resolve the SRV record:
`_v2-origintunneld._tcp.argotunnel.com`
and the A records of both region hostnames.

For SNI filtering, allow **cftunnel.com** and ***.cftunnel.com** on port 7844. These names have no DNS records and cannot be firewall address objects.

Current connector: with `--no-autoupdate`, the Controller does not need api.cloudflare.com or update.argotunnel.com to establish the tunnel. Users still need the project web URL. Google Cloud rules apply separately.

Full checks and implementation reference

04 / SUPPORT EGRESS

RustDesk and Tailscale

Apply each service rule to the correct device, including the corresponding return traffic.

RUSTDESK / PANEL PC

Setting	Required value
Destination	89.60.167.50 (rustdesk.rosepetal.ai)
Direction	Outbound, allowing response traffic
TCP destination ports	21115, 21116, 21117
UDP destination port	21116

No inbound port forwarding

These are destination ports on the Rosepetal RustDesk server. The standard deployment runs RustDesk on the Panel PC.

TAILSCALE / CONTROLLER

Protocol	Outbound rule / purpose
TCP	Destination 443: control services and DERP relays
UDP	Source 41641 to peer IPs/ports: direct WireGuard connections
UDP	Destination 3478: STUN
TCP	Destination 80: optional coordination transport and captive-portal checks

Allow DNS and ***.tailscale.com**, including login.tailscale.com, controlplane.tailscale.com and log.tailscale.com. Allow the current DERP destinations published by Tailscale. Control domains alone do not cover all relays.

Prefer domain-based rules. Direct Tailscale connections use UDP; DERP can relay over TCP 443 if UDP is blocked, with lower performance. For fixed-IP rules, use the current Tailscale service and relay lists.

Tailscale firewall reference