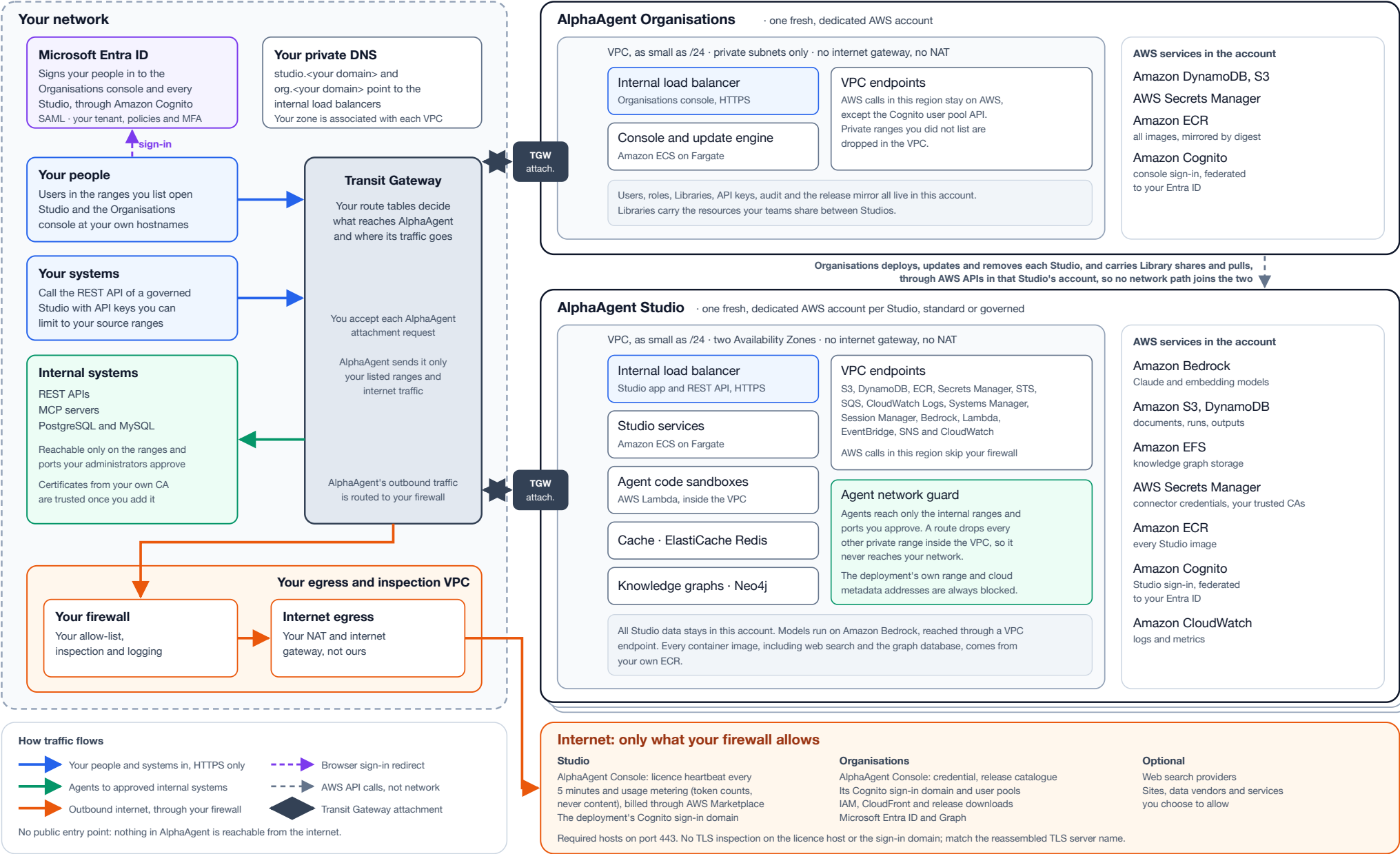


AlphaAgent private deployment on your AWS network

Studio and Organisations, reached only over your Transit Gateway, with outbound traffic through your firewall



How it works, and what each side provides

The same design for every deployment: one fresh, dedicated AWS account for Organisations and one for each Studio

How traffic flows

- Your people and systems reach AlphaAgent over your Transit Gateway.** Studio and the Organisations console sit behind internal load balancers at your own hostnames, admitting HTTPS only from the user access ranges you list. Nothing is reachable from the internet.
- Sign-in uses your Microsoft Entra ID.** The Organisations console and each Studio federate to your tenant through Amazon Cognito (SAML). Organisations creates each Studio's enterprise application through Microsoft Graph. Only sign-in redirects take this path, never your data.
- Agents reach your internal systems only where you allow.** Connectors and agent code reach the internal service ranges and ports your administrators approve, and trust your own certificate authorities once you add them. A route in each VPC drops every other private range.
- All outbound internet traffic goes through your firewall.** Each AlphaAgent VPC's default route points to your Transit Gateway, and your route tables send it to your egress or inspection VPC. No AlphaAgent VPC has a NAT gateway, internet gateway or public subnet.
- AWS services stay on AWS.** VPC endpoints carry the calls to Bedrock, S3, DynamoDB, ECR, Session Manager and the other services shown on the diagram, and every container image comes from your own ECR.
- Organisations manages Studios through AWS APIs.** It deploys, updates and removes each Studio with a cross-account IAM role, and moves Library shares and pulls the same way, so no network path joins the two.
- Licensing goes to the AlphaAgent Console.** Studio sends a signed licence heartbeat every 5 minutes and usage metering (token counts, never content), billed through AWS Marketplace. Organisations uses the same host for its credential and releases.

Design principles

- Identical units.** Organisations and every Studio each run in a fresh, dedicated AWS account with their own VPC, built the same way. Upgrades, support and removal behave the same for one deployment or a hundred.
- Compact address ranges.** A VPC can be as small as a /24. Organisations checks every range against your other deployments and its own, so nothing overlaps on your network.
- Clean ownership.** AlphaAgent owns everything inside its accounts. You own your network, Transit Gateway route tables, firewall and DNS, and AlphaAgent never changes them.
- Fixed, checked settings.** Network access, outbound path, VPC range and Transit Gateway are fixed for each deployment's life. Every install, upgrade and reconfiguration first checks your firewall path from inside the VPC.

Firewall allow-list

Destination (port 443)	Used by	Why	Rule
telemetry.api.alphaagent.prometheusrl.com	Studio, Organisations	Licence, heartbeat, metering; credential, release catalogue	Required No TLS inspection
<prefix>.auth.<region>.amazoncognito.com	Studio, Organisations	Sign-in: the load balancer completes each one	Required No TLS inspection
cognito-idp.<region>.amazonaws.com	Organisations	User pools of the Organisation and each Studio	Required
iam.amazonaws.com, cloudfront.amazonaws.com	Organisations	Global AWS services: name checks, Verify, Clear account	Required
prl-alphaagent-artifacts-prod.s3.amazonaws.com, prl-alphaagent-artifacts-prod.s3.eu-west-2.amazonaws.com	Organisations	Release downloads; allow both names	Required
login.microsoftonline.com, graph.microsoft.com	Organisations	Microsoft Entra ID, once you connect it	Once connected
www.google.com, cse.google.com, html.duckduckgo.com, search.brave.com	Studio	Web search; each one you allow adds results	Optional

Match the TLS server name after reassembling the ClientHello, which can span more than one TCP segment. <region> is the deployment's or the Organisation's region; Organisations also needs the AWS endpoints of any other region you deploy Studio into.

Who provides what

You provide	AlphaAgent creates and runs
Fresh AWS accounts: one for Organisations, one per Studio	The VPC, private subnets, internal load balancer and VPC endpoints in each account
Your Transit Gateway, shared to those accounts; someone to accept each attachment; routes back to each VPC range, and 0.0.0.0/0 to your egress VPC	The attachment request; routes to the ranges you list and a default route to your Transit Gateway; a route that drops every other private range
Firewall rules for the allow-list above, and your firewall's public egress IP addresses	A check at every install, upgrade and reconfiguration that each required host is reachable and not intercepted
A VPC range per deployment (a /24 is enough), user access ranges, internal service ranges and ports	Overlap and capacity checks across your Organisation, shown in the Address plan
Private DNS records and certificates for your hostnames, with the zone associated with each VPC	Sign-in through your Entra ID, and the Studio services, data stores and agent sandboxes
Your CA certificates, if your internal services use your own CA	Upgrades by Update Manager, with rollback to a restore point