ProjectX

NETWORKING · DATASHEET

Private networks, load balancers and DNS, one rule model.

Private networks with subnets and routes, firewalls written once and translated to whatever each provider calls them, load balancers that health-check their backends, and DNS with health-checked failover and GeoDNS — all addressed through endpoints that name no upstream.

Why teams choose it

01
Write the rule once
One firewall rule model — direction, protocol, port range, CIDR — means the same thing everywhere and is translated to whatever each provider calls it.

02
Refused, not silently ignored
Incoherent configuration is rejected at validation — a certificate on a plain TCP listener is an error you fix now, not a surprise you find in production.

03
Peering without dangling resources
Networks peer across providers as a link on each side, so there is no orphan third resource to forget when you tear down.

04
DNS that fails over
Health-checked failover and location-based routing are routing policies on the record itself, on the DNS provider you choose.

In numbers

1
firewall rule model, whichever provider runs the network

L4 + L7
load balancing, with health checks and TLS termination

IPv4 + IPv6
on balancers and addresses, or both at once

What it does

Private networks and peering

A network carries its subnets, routes and firewall rules inline, CIDR-checked before any provider call, and peers across networks and providers as a link on each side rather than a dangling third resource.

Subnets, routes and rules live on the network resource itself, validated before anything is created. Peering is a link on each side of the connection, so tearing a network down leaves nothing orphaned behind it.

One firewall rule model

Write one rule — direction, protocol, port range, CIDR — that means the same everywhere and denies what it does not name, backing both the network edge and the reusable security group.

The rule you write means the same thing on every provider and is translated to whatever each one calls its firewall. What the rule does not name is denied, and the same model backs both the network edge and reusable security groups.

Load balancers

L4 and L7 on one resource with a layer field, each listener carrying its backends and a health check, SSL terminated only where it can be — a certificate on a plain TCP listener is refused rather than silently ignored.

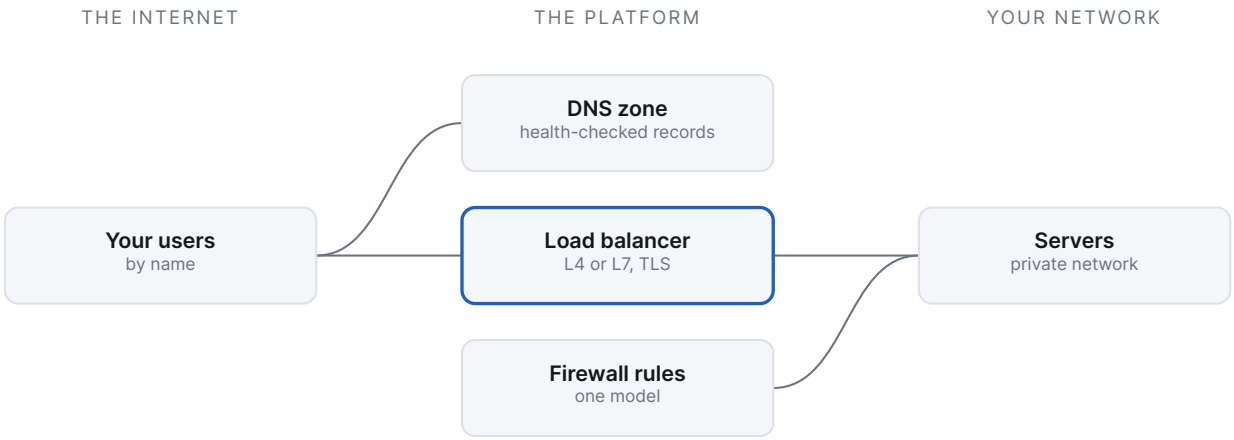
Every listener carries its backends and a health check, so traffic goes to instances that answer. Configuration that cannot work — the certificate on the plain TCP listener — is refused at validation, where it is cheap to fix.

DNS with failover and GeoDNS

Zones carrying their records inline, each with a routing policy the validator keeps coherent, on the DNS provider you choose rather than a hidden placement.

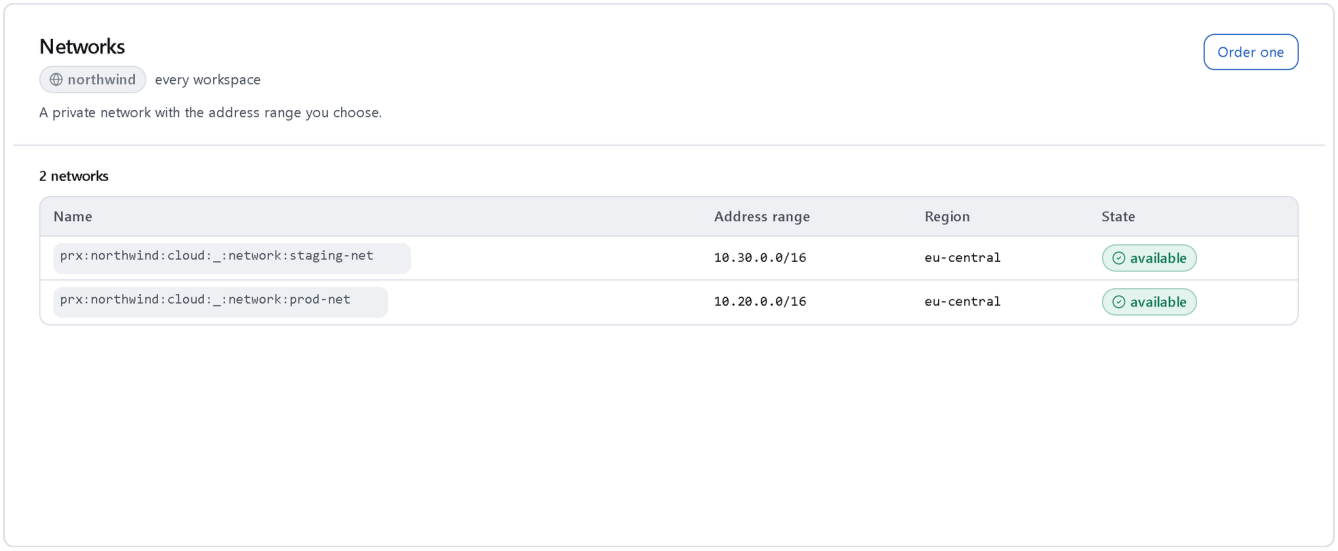
Health-checked failover and location-based routing are policies on the record itself, kept coherent by the validator. The zone runs on the DNS provider you choose — there is no hidden placement to discover later.

How it fits together

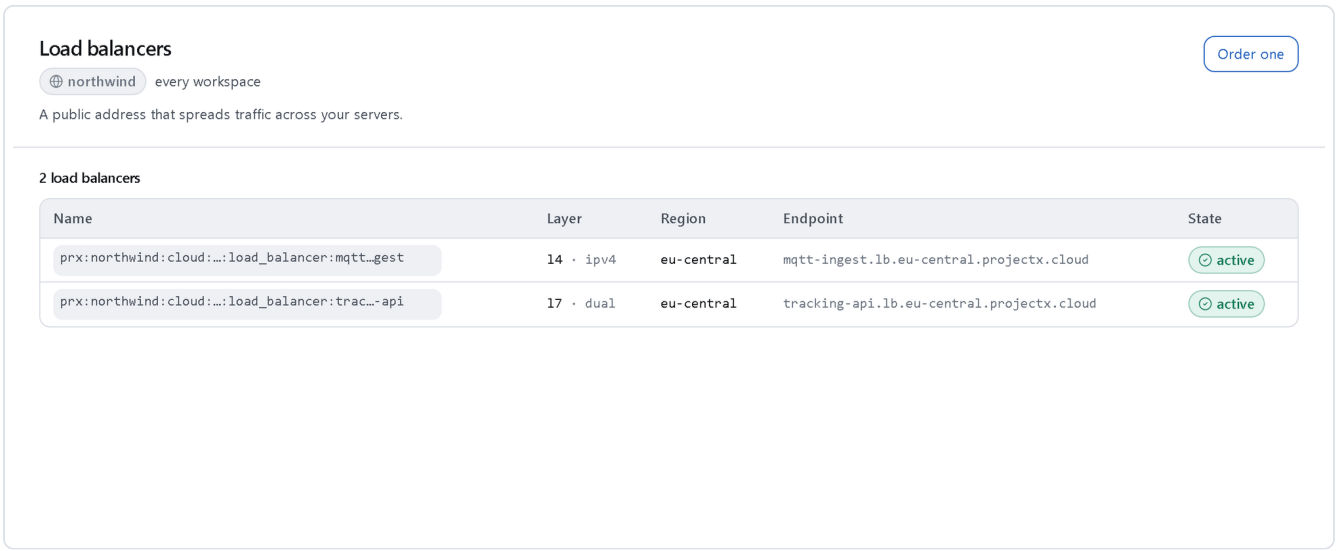


A name in your DNS zone resolves to a load balancer, which spreads traffic across healthy servers on a private network. Firewall rules written once apply to that network whichever capacity it runs on.

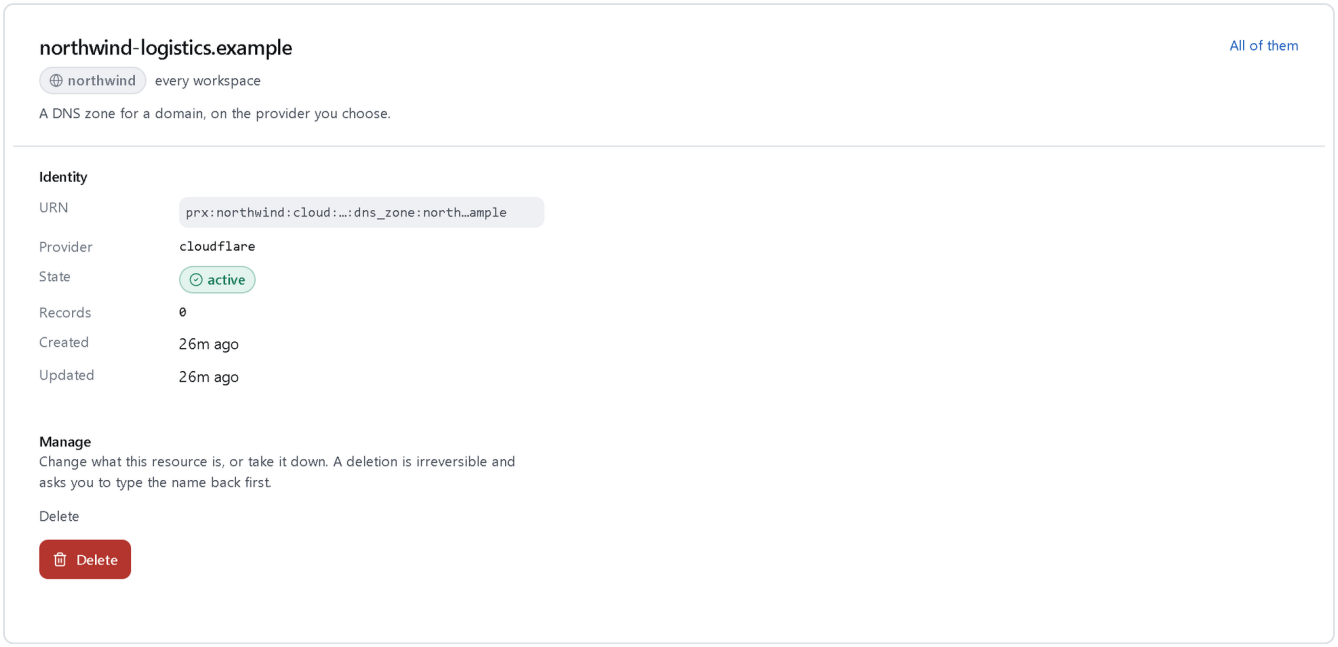
In the console



Private networks with their address ranges, in one rule model. Screens shown with demo data.



Layer 4 and layer 7 balancers, with the addresses they answer on. Screens shown with demo data.



A DNS zone, on the DNS provider you choose. Screens shown with demo data.

Key ideas

Private network

An address range you choose, with subnets and routes, that your servers talk across without touching the internet.

One rule model

Firewall rules and security groups are written in one vocabulary and translated for whichever capacity runs the network, so a rule means the same thing everywhere.

Health-checked DNS

A record can fail over to a standby when a health check fails, or answer by the visitor's location, so the name keeps working when a site does not.

In depth

Connecting places

Networks peer across providers, and site-to-site or client VPN over WireGuard or IPsec brings your office or data centre in, with private interconnect to our modular data centres.

At the edge

Certificates are issued and renewed automatically, a CDN caches in front of your origin, and a managed ingress routes HTTP without you running a proxy.

Refused, not ignored

Configuration that cannot work — a certificate on a plain TCP listener — is rejected when you submit it, so mistakes surface now rather than in production.

How it works

01 **Draw your networks** · Console
Private networks with subnets, routes and firewall rules, checked before anything is created.

02 **Write the rules once** · API
One rule model — direction, protocol, port range, CIDR — translated to whatever each provider calls it.

03 **Balance the load** · Console
Layer-4 and layer-7 load balancers with health-checked backends, on one resource.

04 **Run your DNS** · Console
Zones with health-checked failover and location-based routing, on the DNS provider you choose.

Who it is for

Multi-tier applications

Web, application and data tiers need isolation without provider lock-in.

Private networks with subnets, routes and firewalls checked before anything is created.

Public services

Traffic spread across backends that might fail.

Layer-4 and layer-7 load balancers that health-check every backend they send traffic to.

Global products

Users routed to a healthy, nearby endpoint.

DNS records with health-checked failover and GeoDNS policies the validator keeps coherent.

Works with

Console · API · TypeScript SDK · prx CLI

Questions buyers ask

Can I keep servers off the public internet?
Yes — private networks carry their own subnets, routes and firewall rules, and a rule denies everything it does not name.

Do firewall rules work the same on every provider?
You write one rule model — direction, protocol, port range, CIDR — and the platform translates it to whatever the underlying provider calls it.

What load balancing is included?
Layer-4 and layer-7 on one resource. Every listener carries its backends and a health check, and configuration that cannot work is refused at validation.

How is it billed?
Networks and DNS follow the published per-resource rates on the pricing page, on the same monthly invoice as your servers.

Pricing

Current published rates, in your currency: https://adaydev.com/pricing/cloud