PRODUCT OVERVIEW

Hydra: a steadier way to use many VPN exits

A session-aware Linux gateway that distributes new client traffic across a healthy VPN pool while keeping established flows on the path that created them.

PUBLISHED BY ANTIDESIGN SOFTWARE | PRODUCT OVERVIEW

One gateway. Many healthy paths.

Traditional single-tunnel VPN gateways force the whole network through one egress. Hydra operates a bounded pool and makes a policy-aware decision for each new assignment.

2-20	1:1	30/30/60	IPv4
active tunnel contract	replacement capacity	default graceful lifecycle	VPN routing with IPv6 blocked

Hydra is designed for teams and advanced networks that want endpoint diversity without treating every connection as disposable. It combines health-aware selection, layered affinity, on-demand geography, and deterministic recovery behind one LAN gateway.

What changes for users

- Devices use one gateway and one local management address.
- Every on-LAN IPv4 device receives balanced VPN-only routing automatically after the pool is ready.
- Users can optionally choose stronger stickiness, faster rotation, a country, a city, or an exact server for only their own device.
- New traffic stops instead of escaping directly when health, minimum capacity, or required geography cannot be satisfied.

Built around the hard part: continuity

Hydra does not promise that a public-IP change is invisible. It deliberately preserves what can be preserved and makes the unavoidable boundaries explicit.

Capability	Business value
Flow-level conntrack affinity	Established transports stay on the VPN path that created them.
Destination and client affinity	Related application work can retain a consistent egress within policy limits.
Replacement-before-drain	Planned rotation adds healthy capacity before retiring an endpoint from new selection.
Health and minimum floor	The gateway withdraws new assignments when safe capacity is unavailable.
On-demand geography	A catalog location can be prepared in existing replacement capacity without creating an unbounded second pool.
Source-scoped controls	Users manage their own device; the administrator retains global policy authority.

Three user modes

01

Balanced

Session-safe diversity for everyday use.

02

Client sticky

Strongest endpoint consistency for sensitive apps.

03

Maximum rotation

Aggressive new-assignment change when capacity permits.

A real fail-closed boundary

An unavailable location, a pool below its minimum, an unready service, off-LAN traffic, and forwarded IPv6 do not receive a direct-WAN escape route.

Operational confidence is part of the product

Hydra isolates tunnels, constrains privilege, journals ownership, and verifies cleanup so the gateway can recover without guessing what it changed.

Design choice	Why it matters
One network namespace per tunnel	Overlapping provider routes and tunnel addresses remain isolated.
Narrow privileged worker	The web/control plane stays unprivileged; network mutation crosses a peer-authenticated Unix socket.
Atomic nftables policy	The kill-switch policy is syntax-checked, applied as one transaction, and verified by signature.
Write-ahead ownership journal	Crash recovery removes only Hydra-owned routes, marks, namespaces, UFW rules, and forwarding changes.
Resolver-independent bootstrap	Provider endpoint discovery does not depend on DNS state pushed by a tunnel.
Atomic configuration updates	The administrator gets full-candidate validation, previous-file recovery, controlled restart, and readiness tracking.

Recovery without guesswork

Hydra treats recovery as part of normal operation: owned network state is recorded before mutation, reconstructed deterministically after interruption, and held behind the fail-closed boundary until the pool and DNS service are ready.

Deployment fit

Hydra is an on-premises Linux gateway for networks prepared to make deliberate routing and DNS choices.

Good fit	Plan for
A LAN that needs diversified IPv4 VPN egress	Ubuntu Server 26.04 and IPVanish OpenVPN profiles
Applications that benefit from session-aware rotation	An existing DHCP service or manual gateway/DNS configuration
Teams that want per-device geography without per-device VPN apps	IPv4 VPN service; forwarded IPv6 is blocked
Operators who value fail-closed behavior and deterministic recovery	Reserved addresses when durable per-device overrides matter

Bounded scale by design

Hydra supports a configured pool of 2 through 20 active tunnels plus an equal replacement cohort. Capacity remains bounded while planned rotation, individual failure recovery, privileged-worker reconstruction, and reboot recovery preserve the routing contract.

> **Start with a fit assessment**
>
> AntiDesign Software can evaluate interface topology, DHCP and DNS integration, expected client behavior, provider profiles, pool size, lifecycle timing, and operational ownership before gateway activation.

Hydra is a routed gateway, not a VPN provider and not a DHCP server. Provider service terms, endpoint availability, and network conditions remain external dependencies.

ANTIDESIGN SOFTWARE

Software for complex operations. Built with explicit boundaries, observable behavior, and recovery in mind.