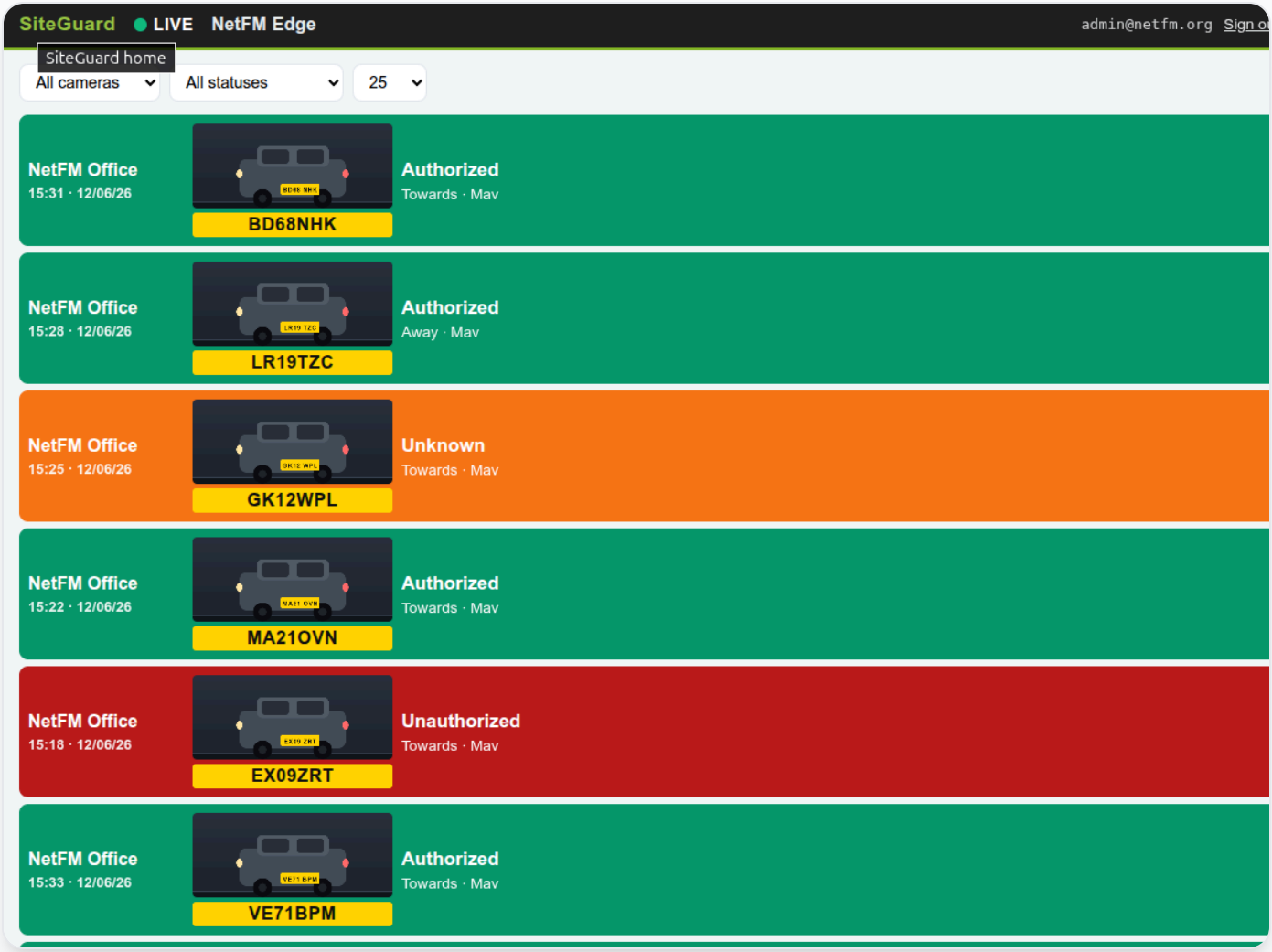
SITEGUARD

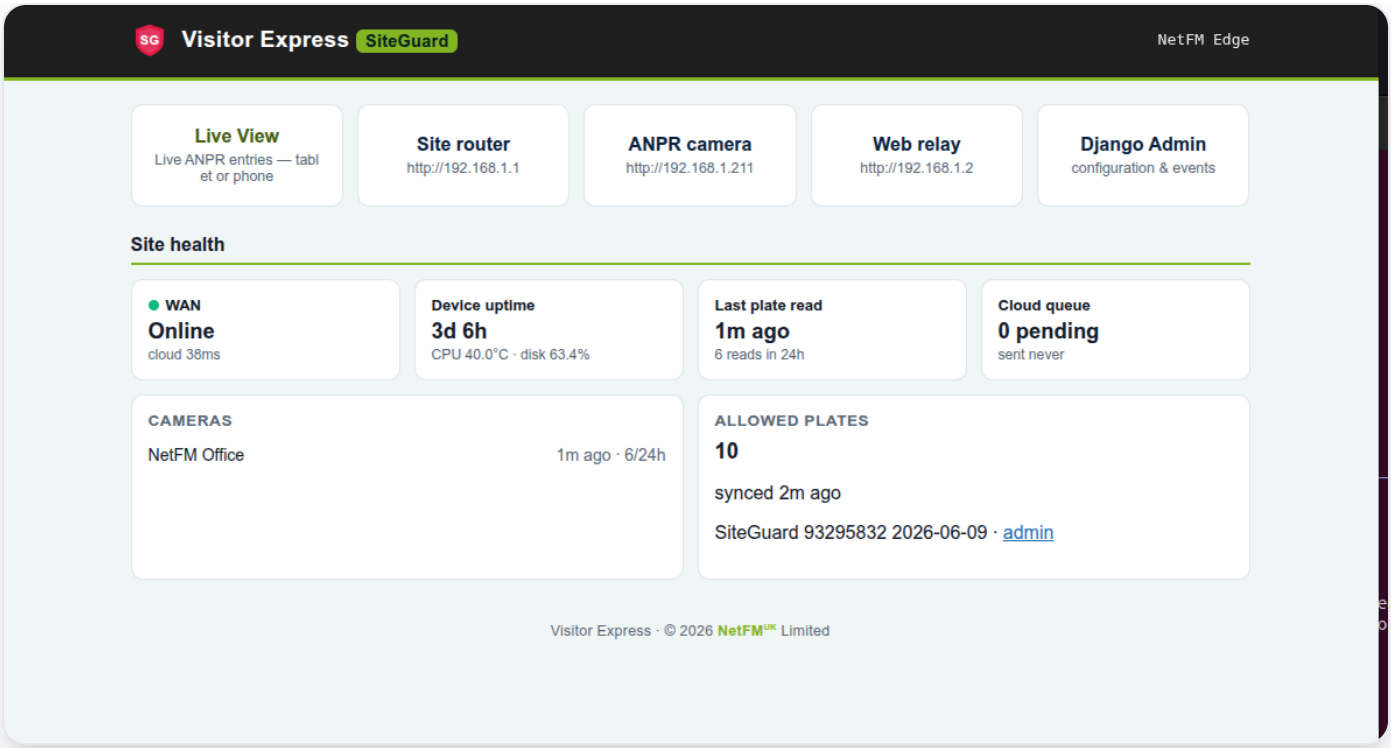
Secure site connectivity — without a static IP

SiteGuard is NetFM's answer to providing secure remote access using intelligent edge devices — with **no longer any need for static IPs or port-forwarding rules**. Our customers operate over geographically large areas across the UK, which demands many types of connectivity: fibre broadband, fixed line, 4G/5G mobile networking and Starlink. We've designed SiteGuard to work across these heterogeneous networks and provide a single access-control page within Visitor Express.

SiteGuard incorporates a **WireGuard VPN network based on Tailscale** alongside an intelligent edge device that manages all site-based services — allowing fully autonomous operation using direct local access to control digital access screens and barriers, with the ability to cache over two weeks of on-site booking and entry data.



Live View. Every gate read streams to the guard in real time — authorised (green), unauthorised (red) or unknown (amber). Runs on a wall tablet *or* the guard's own phone.



Site health at a glance. WAN connectivity, device uptime, last plate read, forward-queue backlog and allow-list sync — all on-device, no cloud round-trip.

THE OLD WAY

A rented static IP and a row of open ports

Reaching equipment at a remote site has traditionally meant a router with a **public static IP address** and a stack of **port-forwarding rules** — the camera on one port, the web relay on another, the router's own admin page on a third. Each one is a door onto the public internet, guarded by little more than a password.

- ✕ Static IPs cost money — a monthly line-rental add-on from the ISP, every site, every month.
- ✕ On 4G/5G a public IP is often expensive or simply unavailable behind carrier-grade NAT (CGNAT).
- ✕ Every forwarded port is internet-facing — continuously scanned and brute-forced.
- ✕ A single reused or weak device password exposes the whole access-control system.

```
# Typical legacy site — everything on one public IP
203.0.113.10:9001 → ANPR camera admin
203.0.113.10:9002 → web relay / barrier
203.0.113.10:443 → router admin

# 3 open ports · 1 rented static IP · public-facing
```

THE SITEGUARD WAY

One private mesh. Zero open ports. No static IP.

The SiteGuard edge device joins a **private mesh network** built on Tailscale (WireGuard®), coordinated by NetFM's **own dedicated Headscale control server**. The device dials *out* to join the mesh — it never needs an inbound port, a static IP, or any change to the customer's firewall.

ON SITE

SiteGuard edge device

Behind any connection — 4G/5G, broadband, even CGNAT. Makes outbound-only connections.

PRIVATE MESH

Encrypted WireGuard tunnel

Direct, end-to-end encrypted, peer-to-peer. Reachable only by name (`site.cn.netfm.org`) on the tailnet.

CORE PLATFORM

Visitor Express

Bookings, allow-lists and plates flow down; arrivals and audit logs flow back — all inside the mesh.

SECURITY ARCHITECTURE

How the private mesh works

Tailscale splits a network into three independent layers — and that split is exactly why SiteGuard is both cheaper and more secure than the static-IP approach.

01 · CONTROL PLANE

Headscale decides membership. It distributes keys and addresses — but never sees traffic.

02 · POLICY

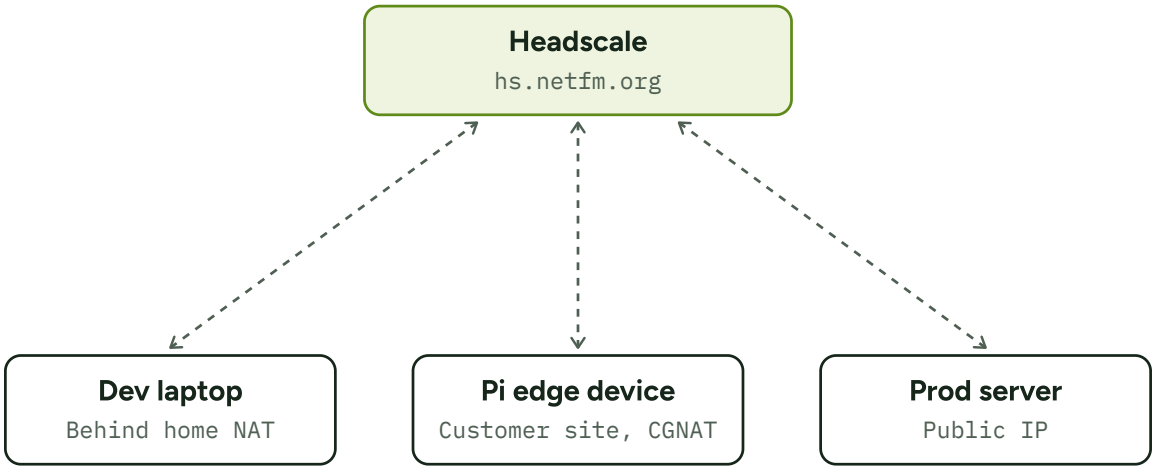
ACL tags partition the mesh — controlling which nodes may reach which. Default deny.

03 · DATA PLANE

WireGuard carries the actual traffic, encrypted end-to-end between peers.

Headscale — the coordination layer

Tailscale is a mesh VPN built on **WireGuard**: rather than funnelling traffic through a central hub, devices form direct peer-to-peer connections, traversing NAT and CGNAT to reach each other. Headscale is a self-hosted re-implementation of Tailscale's coordination server, so NetFM runs the standard Tailscale clients on every device while the **control plane lives on its own UK infrastructure**. Its job is deliberately narrow: it distributes each node's public key and overlay address so the fleet can find one another — and nothing more.

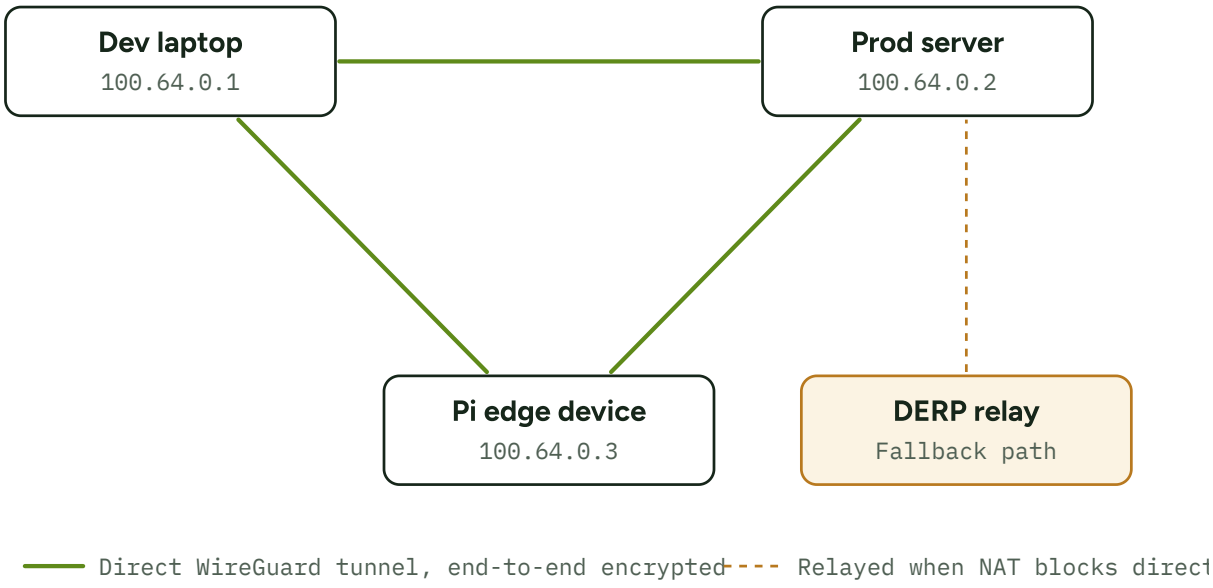


Control plane. Each node registers with Headscale over HTTPS and receives the network map. Dashed links carry keys and endpoints only — never application traffic.

Security property: Headscale only replaces the control plane. The WireGuard private keys never leave the devices, so a **fully compromised coordinator still cannot decrypt a single packet** — it controls *membership* of the network, not the traffic within it.

The mesh and NAT traversal

Once nodes know each other's keys, they connect **directly** — end-to-end encrypted, peer-to-peer — even when both ends sit behind NAT or carrier-grade NAT, by learning their public endpoints and punching through. Where a hard symmetric NAT blocks a direct path, traffic falls back to an encrypted **DERP relay** that forwards already-encrypted packets and cannot read them.



Data-plane mesh. Direct tunnels carry traffic peer-to-peer. The DERP relay forwards already-encrypted packets and cannot read them — a slower, opaque pipe used only when a direct path fails.

✓

Resilient even if the control server goes down

Because the control plane is *not* in the data path, every node caches its peer list and policies locally. If NetFM's Headscale server is ever unavailable, **all existing connections keep working** — sites stay reachable and the edge keeps making access decisions. Only new device enrolments, key rotations and policy changes pause until the control server returns.

Source: Tailscale — "What happens if the coordination server is down?" and Control and data planes.

Removes the cost. Enhances the security.

No static IP, no rental

Works on any link — 4G/5G, broadband, even CGNAT. The recurring ISP static-IP charge disappears at every site.

Zero open inbound ports

Nothing is exposed to the public internet. No internet-facing camera, router or relay admin pages to scan or brute-force.

End-to-end WireGuard encryption

Modern, audited cryptography on every byte between the site and the core — never in the clear, never on the open internet.

UK-hosted private control plane

Coordination and keys stay on NetFM infrastructure — data sovereignty by design, not a shared third-party SaaS.

Out-of-band remote support

NetFM securely reaches cameras, routers and relays for maintenance — without the customer opening a single port.

Fast, clean deployment

Enrol the device, get a name on the mesh. No firewall changes, NAT rules or static-IP paperwork at the customer site.

See SiteGuard on your site

Local-first access control with secure, static-IP-free connectivity and a UK-hosted private control plane. Book a demo and we'll show you the edge device, the guard view and the mesh.

Request a demo →
