Pelion

Security

How Pelion keeps IoT devices protected, connected, and running reliably

Pelion.com

Pelion

SECURITY

Protecting Every Connection & Every Device

At the core of our offering lies a highly resilient connectivity architecture delivering 99.995% uptime across 600+ networks in more than 150 countries – backed by global SIM capability and a single management portal.

Our advanced network access, running on our own private APN, uses network segmentation and secure protocols to ensure your IoT traffic remains isolated and protected from exposure to the public internet.

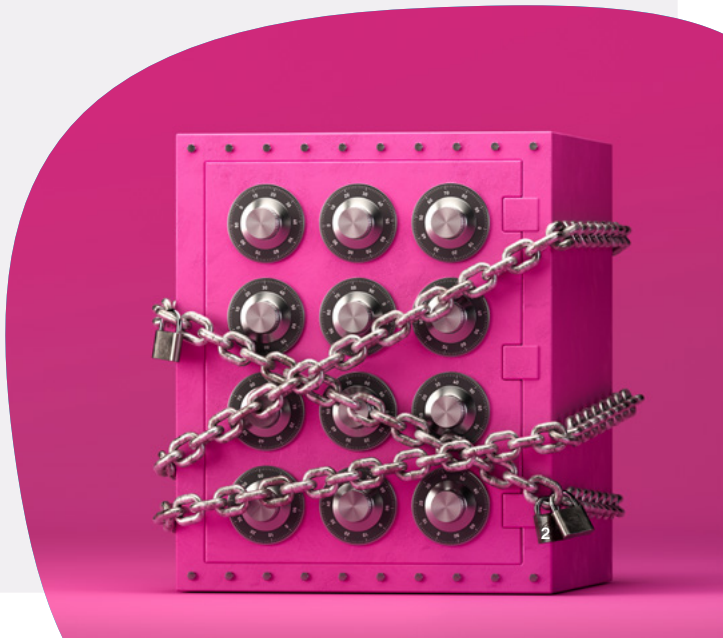
Compliance & Certifications

With Pelion, compliance is built-in.

We hold ISO 27001 certification across our global operations.

Additionally, our connectivity-management terms include robust data-processing addendums to align with GDPR requirements, enabling auditability and transparency around data transfer, breach notification and sub-processor supervision.

By partnering with Pelion, you'll benefit from a vendor who takes both security and regulatory compliance seriously – helping your deployment meet internal and external audit requirements, regulatory regimes or sector-specific standards.



Pelion

Secure Connectivity Options

We offer a full range of connectivity-security options so your device fleet can communicate safely and privately:

Private APN

What is a Private APN?

A private APN is a private mobile data network for IoT devices that keeps their traffic off the public internet and routes it securely through Pelion's network to customer systems.

About Pelion's Private APN

Our private APN enables dedicated routing of IoT device traffic through Pelion's secure network rather than the public internet.

This approach isolates IoT data flows from general mobile broadband traffic and ensures consistent enforcement of customer-specific policy across all connections.

Private APN also supports the use of static private IP addressing, allowing controlled, and predictable device access paths without exposing endpoints to the wider internet.

Security Features

- Completely isolated IoT traffic path, separated from public or consumer networks
- Enforced authentication procedure for allowed SIMs only
- No public internet breakout unless explicitly required
- End-to-end IP integrity maintained through Pelion's active-active routing

Service Features

- Static and Dynamic private IP address support
- Multi-operator, dual-site routing for maximum uptime
- Deterministic policy enforcement across the entire network path
- Geo-redundant data flow with automatic failover between sites
- Suitable for high-scale, always-on IoT deployments requiring predictable routing

Resilience

- Dual-site, load-balanced RADIUS authentication for continuous operation
- Redundant operator integrations (leased line, IPSec, L2TP) for high availability
- Traffic routed through HA firewall pairs

Private APN as Standard

Using Pelion means access to our private APN as standard. You benefit from secure, reliable connectivity out-of-the-box, with predictable performance, built-in redundancy, and full separation from public networks.

It's one of the key features that ensures your IoT devices can always communicate safely and securely, without any extra setup or configuration.

Policy-Based IPsec

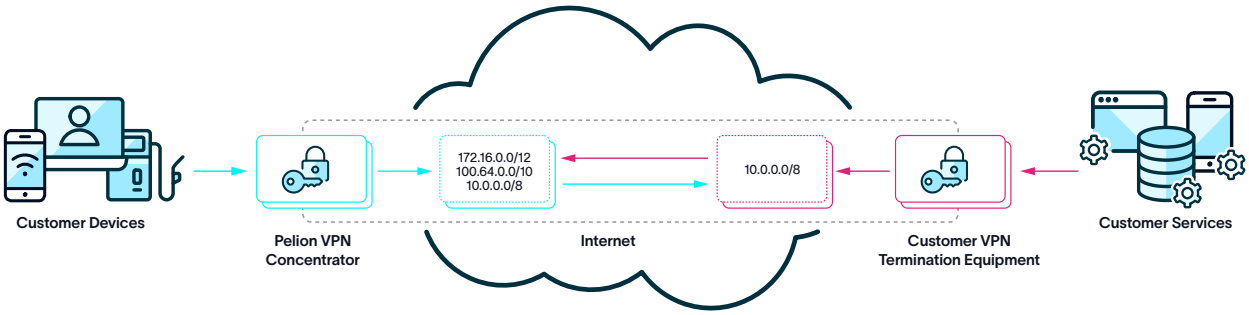
What is Policy-Based IPsec?

Policy-Based IPsec is an always-on encrypted tunnel that securely connects IoT traffic between Pelion and customer systems using fixed traffic rules.

About Pelion's Policy-Based IPsec

Policy-based IPsec delivers fixed device encryption designed for persistent, high-reliability site-to-site connectivity. It is ideal for deployments where traffic patterns are well understood, ensuring uninterrupted data delivery to your critical services.

All tunnels terminate on Pelion's high-availability, CARP-backed VPN concentrators deployed in all datacentre locations, ensuring uninterrupted connectivity even during maintenance or site outages. BGP-managed routing enables instant failover to secondary paths.



Security Features

- Strong IPsec encryption with defined subnet-to-subnet selectors
- Available with dual-datacentre termination with automatic tunnel failover
- High-availability VPN concentrators using CARP redundancy
- Strict traffic policy enforcement for deterministic routing
- Encrypted traffic isolated from public internet paths
- Compliance-aligned cryptographic standards

Service Features

- Ideal for persistent, always-on backhaul
- Predictable routing and fixed endpoint behaviour
- Seamless failover using BGP or IP SLA
- Supports high-scale device networks with static addressing

When to choose Policy-Based IPsec

Choose Policy-Based IPsec when you want strong security with simple, predictable behaviour.

It's best suited for:

- Customers early in their IoT journey
- Fixed traffic flows with little expected change
- Long-term deployments with stable network design

VTI IPsec (Route-Based IPsec)

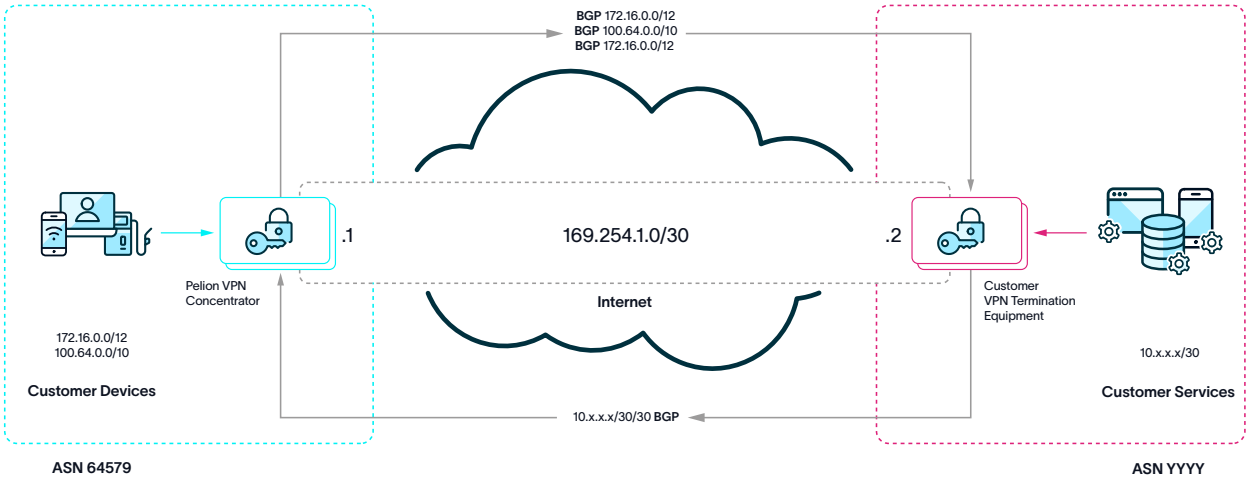
What is VTI IPsec?

VTI IPsec is a modern VPN approach that treats encrypted tunnels like fixed network links, allowing automatic routing and seamless failover.

About Pelion's VTI IPsec

VTI IPsec provides a more dynamic, route-based VPN architecture suitable for complex enterprise networks, hybrid cloud, or environments requiring flexible traffic segmentation.

Each VTI interface participates directly in Pelion's redundant routing configuration, enabling multipath routing, active-active tunnels and advanced failover behaviours.



Security Features

- Encrypted tunnel interfaces supporting dynamic routing
- Dual-site IPsec termination with high-availability firewalls
- Redundant VPNCs leveraging CARP and BGP integration
- Full isolation of IoT traffic within a private routing domain
- Supports granular route management and segmentation

Service Features

- Suitable for multi-region, cloud and complex enterprise networks
- Dynamic routing (e.g. BGP) enables flexible topology changes
- Active-active or active-standby tunnel options
- Great for multi-tenant environments and large-scale IoT estates
- Rapid failover between datacentres

When to choose VTI IPsec

Choose VTI IPsec when you want automation, resilience, and minimal operational overhead.

It's best suited for:

- Modern cloud or hybrid IoT architectures
- Customers who want fully automated failover
- Growing IoT deployments where network topology may evolve
- Environments requiring high availability without manual intervention
- "Set it and forget it" operational models

IPsec Topology

Policy based IPsec is available in a one- and two-tunnel configuration; and VTI IPsec is available in a one-, two- or four-tunnel configuration providing resilience and automated failover in the event of an issue with any of the available connectivity paths.

All tunnels are continuously monitored, and if a failure occurs between Pelion and the customer side, connectivity is automatically restored by re-routing traffic through an alternative path.

These actions can be automated and recover automatically, even outside normal business hours, ensuring uninterrupted service. If a problem occurs at a customer endpoint, we notify you promptly, providing full visibility and guidance.

This proactive monitoring and automatic recovery mean you get peace of mind: your tunnels are watched and maintained 24/7, and any issues are flagged so you can address them efficiently.

OpenVPN

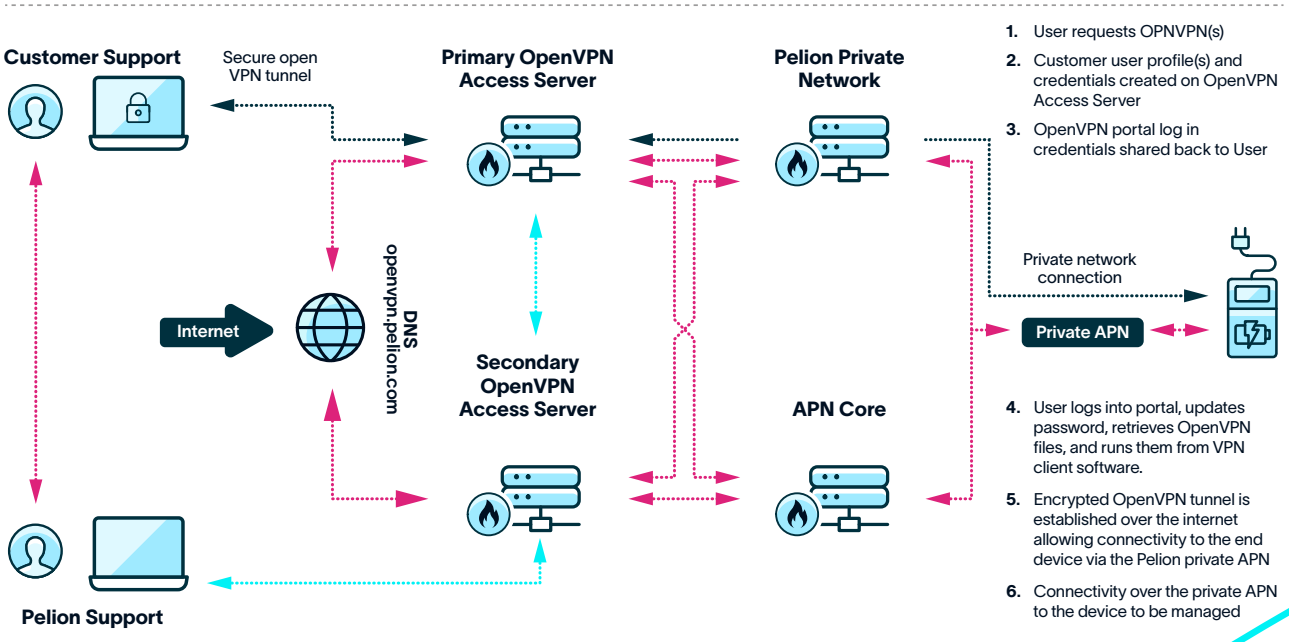
What is OpenVPN?

OpenVPN provides secure, user-based access to IoT devices, designed primarily for people rather than automated systems.

About Pelion's OpenVPN

Pelion's enterprise OpenVPN deployment provides flexible, secure access designed for engineering teams, remote troubleshooting and operational diagnostics.

The service is deployed across Pelion's active-active datacentres, utilising redundant firewall and routing paths for uninterrupted connectivity.



Security Features

- OpenVPN Enterprise deployment
- OpenVPN cryptographic layer
- High availability, redundant architecture
- Pelion software defined firewall

Service Features

- Certificate-based VPN
- User-to-Site (One-to-Many) communications
- Suited for ad-hoc access to subscribers

When to choose OpenVPN

Choose OpenVPN when individual users need secure access to devices.

It's best suited for:

- Engineering and operations teams
- Remote diagnostics and troubleshooting
- Development and testing environments
- User-specific access control
- Temporary or ad-hoc connectivity needs

PELION PROPRIETARY

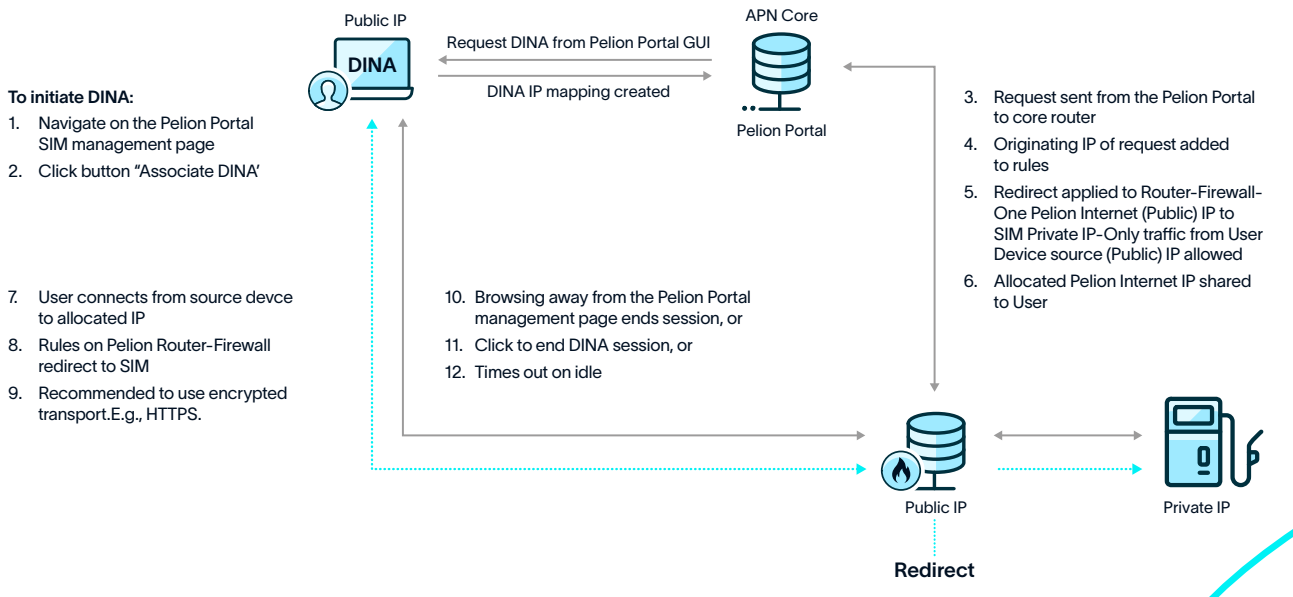
DINA (Direct Inbound Network Access)

What is DINA?

DINA allows secure, authenticated access to IoT devices without assigning permanent public IP addresses or deploying VPN tunnels.

About Pelion's DINA

A secure connectivity method that allows authenticated access without exposing fixed public IPs, combining some of the ease of access of a public IP with greater resilience and control.



Security Features

- DINA functionality is accessible to authenticated users of the Pelion Portal
- One-to-One dynamic mapping of connected device to user end point
- Recommended: Password protected access for local device administration
- Recommended: Secure transport using HTTPS, SSH, or similar

Service Features

- Simple and secure
- Suited for Ad-Hoc access to subscribers
- GUI Access
- No configuration required

When to choose DINA

Choose DINA when you need quick, controlled access without VPN complexity.

It's best suited for:

- Temporary device access
- Customers managing security at the application layer
- Lightweight alternatives to VPNs
- Proof-of-concept or smaller deployments
- External access without exposing private networks

Data Centre Connect

What is Data Centre Connect?

Data Centre Connect provides direct, private connectivity between customer infrastructure and Pelion's data centres, completely bypassing the public internet.

About Pelion's Data Centre Connects

Leveraging either cross-connects within a data centre where both parties infrastructure are hosted, or by implementing a connection from a Pelion data centre to customer deployed infrastructure, data centre connects provide the highest-performance connectivity option, delivering a dedicated, private, low-latency path between customer infrastructure and Pelion's dual active datacentres.

Traffic remains entirely off the public internet and benefits from Pelion's multi-supplier network, redundant switching layers and High Availability (HA) routing.

Security Features

- Fully private Layer-2 or Layer-3 connectivity
- No internet exposure at any point
- Available as dual supplier, dual physical path connectivity
- Redundant switching fabric and HA firewalls
- Optional MAC filtering and traffic segmentation

Service Features

- Ultra-low latency and high throughput
- Ideal for data-intensive workflows or cloud offload
- Direct interconnects into major carrier and cloud facilities
- Active-active routing across Pelion's datacentres
- Can be combined with VPN services for hybrid architectures

In combination these features provide segmentation of traffic flows, isolation of device-groups, encrypted tunnels to enterprise back-ends and controlled remote access for diagnostics or updates.

When to choose Data Centre Connect

Choose data centre connects when performance and privacy outweigh flexibility.

They're best suited for:

- High-volume or real-time data use cases
- Long-term, stable architectures
- Enterprises already present in data centres
- Strict compliance or security environments
- Hybrid designs combining VPN services

IP Management & Firewall Architecture

Pelion's connectivity platform delivers secure and controlled IP management alongside robust firewall and routing mechanisms. IP allow-listing provides an additional layer of control, enabling subscribers to communicate only with services on defined IP addresses.

This protects your devices from unauthorized access over the internet and can be applied to any VPN setup or configurations using dynamic IP addressing.

Customers can request updates or amendments at any time, ensuring ongoing control of traffic flows. We can also manage traffic redirects to customer endpoints on their behalf. It is important to note that Pelion's allow-listing accommodates IP addresses only; web or DNS addresses cannot be added.

For IP management, Pelion allocates handset IP addresses from defined private ranges (172.16.0.0/12, 100.64.0.0/10, 10.0.0.0/8 depending on the operator).

When customers request Policy-Based IPsec and encounter conflicts, Pelion can assign a fixed handset IP block, which will eliminate conflicts and providing a predictable addressing scheme. To do this, we work with the customer to ensure the allocated range does not conflict with existing private networks.

While Pelion cannot guarantee that the range will match customer preferences or that a larger subnet will be available, we use addresses across the private IP address space to avoid conflicts with customer IP allocation wherever possible.

Together, these controls ensure subscribers remain isolated within the private APN and traffic flows are strictly managed.

Firewalls and policy-based configuration ensure consistent enforcement, regardless of connectivity type.

IP allow-listing combined with dedicated handset IP ranges provide predictable, secure addressing while protecting traffic from unauthorized access and helping manage data costs.

Key Features & Benefits

Firewall

- Added layer of security
- Known subscriber traffic destination(s)
- Eliminates "excess" traffic
- Controlled traffic redirects across deployments

IP Management

- Accommodates standard IPsec conflicts
- Known IP range for subscribers

Why choose Pelion's security services?

01 Enterprise-grade protection across device, SIM, and networklayers

02 Flexible VPN, IPsec, and private APN options for secure connectivity

03 Built-in monitoring and anomaly detection

04 Certified and compliant with global standards

05 Scalable for any IoT deployment size

Whether you're deploying hundreds of devices or scaling to tens of thousands, our model is designed to deliver security by default – giving you peace of mind and control across every stage of your IoT deployment.

Pelion

Glossary:

Term	Description
APN	Access Point Name. A setting on a device that tells it which mobile data network to connect to and how to reach private or secure services.
API	Application Programming Interface. A way for software systems to talk to each other automatically, allowing customers to manage devices, data usage, and settings without logging into a website.
BGP	Border Gateway Protocol. A system that helps large networks decide the best path for data to travel across its network or the internet.
CARP	Common Address Redundancy Protocol. A method that ensures network services stay available by switching traffic to a backup system if the main one fails.
DINA	Direct Inbound Network Access. A secure way to temporarily access a device without giving it a public internet address.
GDPR	General Data Protection Regulation. A European law that protects personal data and controls how companies collect, store, and use it.
GRE	Generic Routing Encapsulation. Wraps IoT traffic for transport across different networks, often paired with IPsec to enable secure, flexible routing and advanced features like multicast. This is used for dynamic VPN routing and commonly referred to as a tunnel in a tunnel.
GUI Access	Graphical User Interface Access. The ability to use a visual website or dashboard instead of technical commands.
HA Routing	High Availability routing. A network design that ensures traffic continues flowing even if one system fails.
HTTPS	Secure version of HTTP (Hypertext Transfer Protocol) used for websites. It encrypts data so information can't be read while traveling across the internet.
IP Address	A numerical label given to a device so it can send and receive data on a network. It can change over time and may be private or public. Every device/server/switch/website/router in the world has an IP address.
IPSec	Internet Protocol Security. A method for securely encrypting data traveling between networks.
L2TP	Layer 2 Tunneling Protocol. A way to create secure connections between networks, often used in VPN setups.
MAC	Media Access Control address. A unique hardware identifier assigned to network equipment. This is physical to the equipment and will never change, unlike an IP address which is logical and can be changed.
RADIUS	A system that controls which devices are allowed on the network, assigns them access, and tracks their usage.
SIM	A small piece of hardware in a device that identifies it on a mobile network and enables connectivity.
SLA	Service Level Agreement. A contract that defines service performance expectations such as uptime and support response times.
SSH	Secure Shell. A secure way to remotely access and manage systems using encrypted connections.

Pelion

Glossary:

Term	Description
VPN	Virtual Private Network. A secure connection that encrypts data between devices and private networks.
VPNCs	Internet Protocol Security. A method for securely encrypting data traveling between networks.
VTI	Virtual Tunnel Interface. A logical network interface used to manage secure tunnels more easily.

Pelion

Global IoT Connectivity Made Effortless

Contact us today or visit our website

hello@pelion.com | Pelion.com