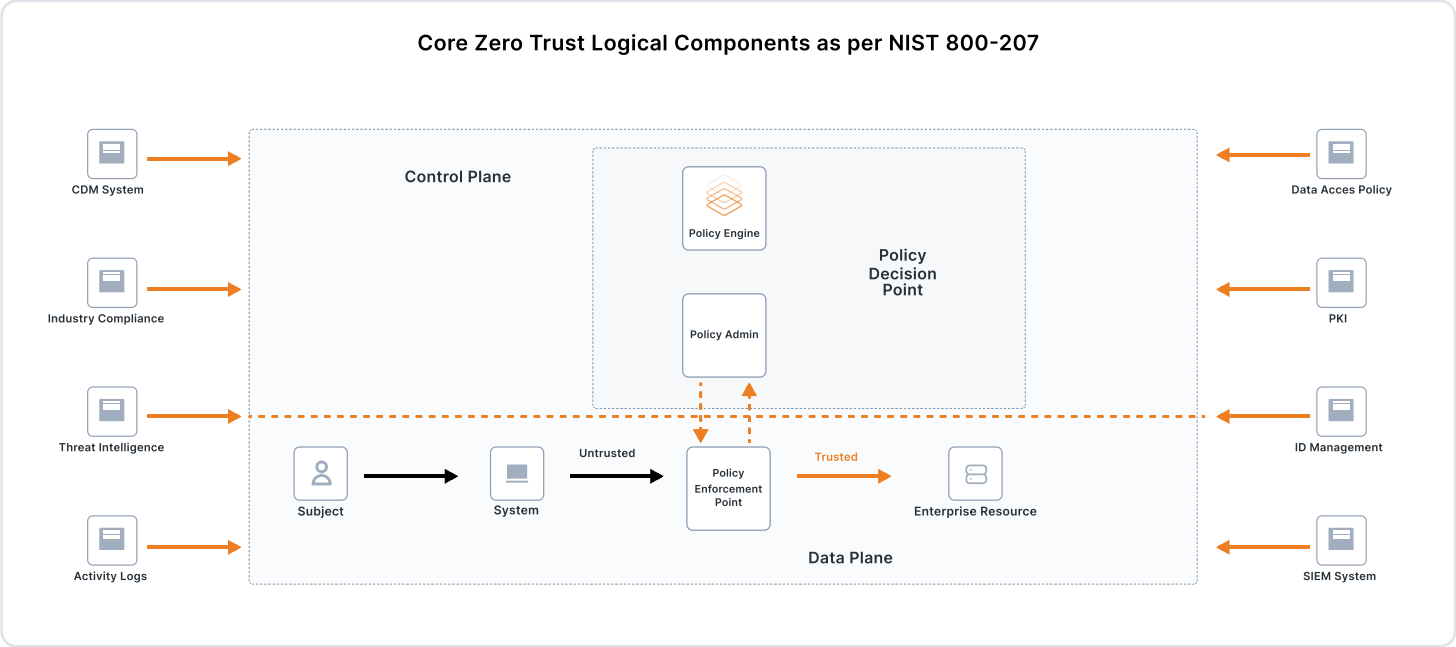
OpenVPN Cloud Zero Trust Network Access (ZTNA)

How Does ZTNA Work?

A zero trust solution with granular access control allows network admins to set access control policies that don't negatively impact user experience. A ZTNA service lets you build a zero trust model that prevents lateral movement from unmanaged devices and enforces least privilege access while giving users access to specific applications.

According to the National Institute of Standards and Technology (NIST), the principles (or tenets) planners should keep in mind when developing a zero trust architecture are:

- Network identity
- Endpoint health
- Data flows

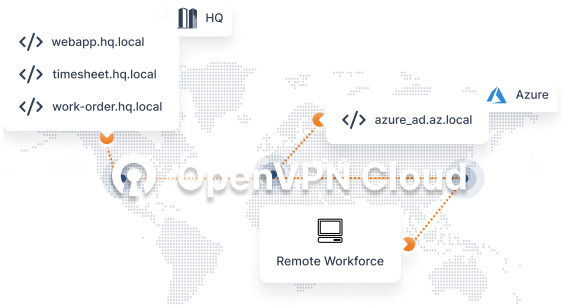


How Does OpenVPN Cloud deliver the essential elements of ZTNA?

OpenVPN Cloud delivers the essential features of ZTNA, making it easier than ever for you to create an identity-and context-based, logical access boundary around a single application or a set of applications. And ZTNA's adaptability and scalability make it ideal for addressing business changes.

Zero Trust Access to Private Applications

Unconstrained network access is easy, so it invites lateral movement breaches. Conceal and protect your network by easily configuring applications using domain names and providing identity-based application access instead. Patent-pending technologies create a secure overlay network that spans all your data centers and routes to applications even if the sites have overlapping IP addresses.

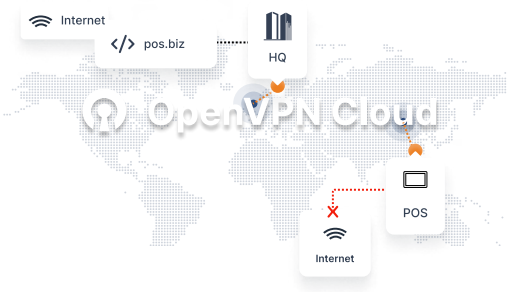


Zero Trust Access to SaaS Applications

OpenVPN Cloud lets you secure access to SaaS applications by tunneling only SaaS traffic to your corporate network. You can then enforce SaaS access by limiting logins — whether it's employees, vendors, or partners — to those made via the corporate network.

Zero Trust Access to Trusted Internet Destinations Only

With OpenVPN Cloud your business gets advanced zero trust internet access to use with specialized connected devices — POS hardware, connected printers, Internet of Things (IoT) devices — that can be locked down by blocking all internet access except to internet destinations needed for their operation.



OpenVPN Cloud ZTNA / Datasheet

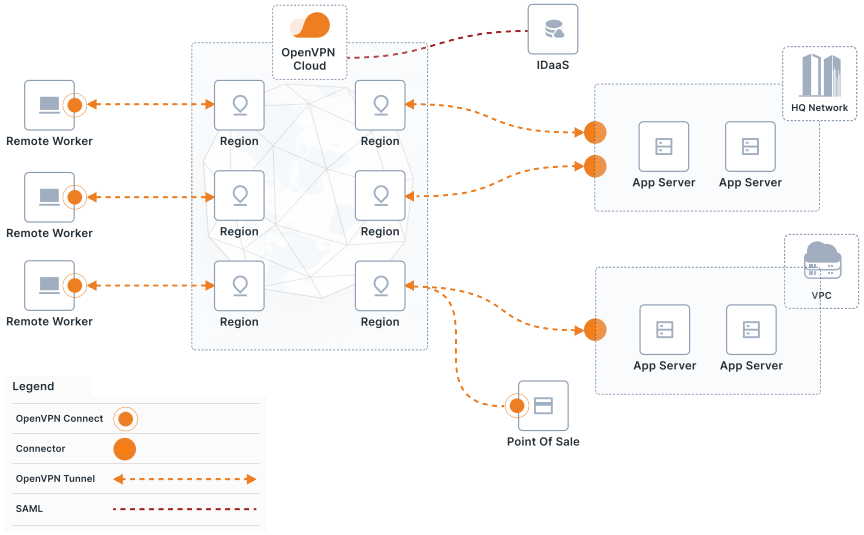
Enforcing Zero Trust Access

OpenVPN Cloud gives businesses of all sizes the ability to create a secure virtualized network. This network expands secure access to protect workers using home and public WiFi networks, as well as SaaS applications outside your network perimeter.

In addition to comprehensive connection, this secure virtual overlay network also isolates your applications from the public internet, making them invisible to the internet, application servers, and networks making outgoing connections to OpenVPN Cloud. This transfers DOS attack risk to OpenVPN Cloud.

To prevent lateral movement, our patent-pending domain name routing hides the IP subnet routes for your private networks from connected devices. Access to individual apps can be protected by per-app firewalls that restrict access to pre-configured application protocols.

Our unique combination of application-domain name routing, per-app firewalls, and identity-based access policies creates zero trust access to applications – not the network hosting the applications.



Why is OpenVPN Cloud the Best Choice for a Cloud-Delivered ZTNA Service?

OpenVPN Cloud has the controls modern businesses need to enable identity-aware, role-based least privilege zero-trust network access to applications.

Technologies

- Complete separation of control and data plane with everything in software
- Control plane built using cloud-native technologies
- Data plane on bare-metal servers using kernel-optimized data forwarding
- Vertical integration of security and data forwarding stacks
- Multi-tenant service
- Full-mesh connected core network

Outcomes

- Centralized network and security policy administration
- Unlimited service scale
- Distributed enforcement close to edge
- Instant creation of secure virtualized overlay networks
- Low latency, high performance connections with built-in security
- High availability and redundancy

Get all the details about OpenVPN Cloud ZTNA

Download Whitepaper

Why is OpenVPN Cloud the Best Choice for a Cloud-Delivered ZTNA Service?

Cloaking

- Services kept private to reduce attack surface
- No private network routes are leaked
- No incoming tunnel connections to networks
- PoPs terminate connections and protect against DoS

Segmentation

- Only authorized services available as routes
- Patent-pending domain routing segments by app
- Hosts can be used to access private apps and not the network
- Multi-WPC allows a WPC to be used to segment based on use case, department, privileged access
- Per-App firewalls only allow authorized protocols

Identity

- Built-in 2FA
- SSO using SAML or LDAP
- Digital certs for IoT and unattended clients
- Access Control for Networks, Hosts, and User Groups between each other and to applications and IP service segments

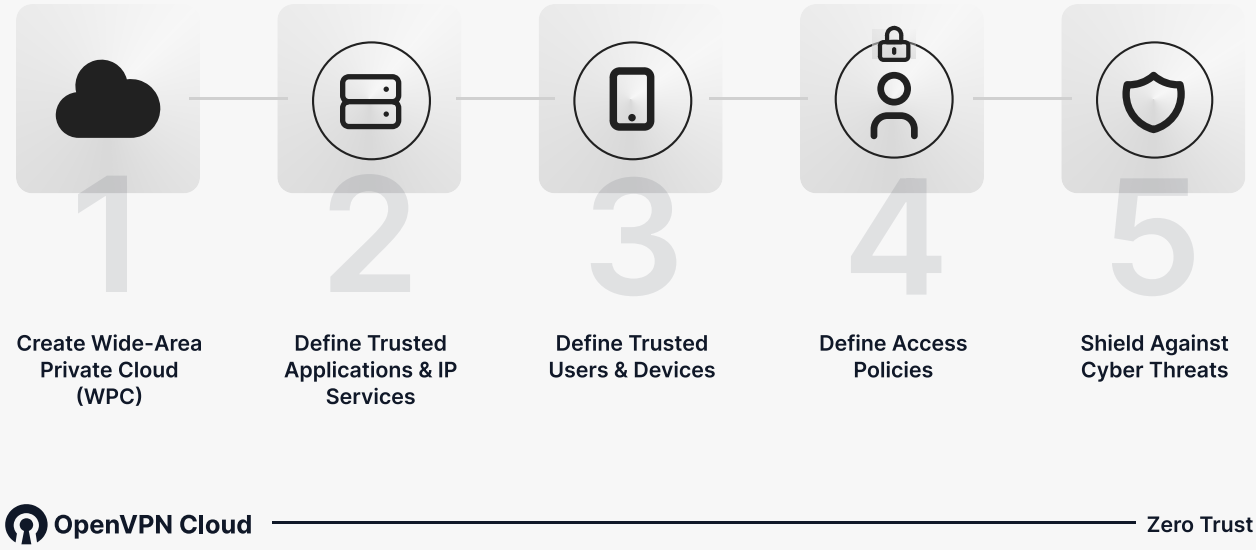
Why is OpenVPN Cloud the Best Choice for a Cloud-Delivered ZTNA Service?

Our Differentiators

- Segregation of trusted and untrusted traffic flows.
- Multiple options to secure untrusted internet traffic.
- Bi-directional Accessibility: Supports network-initiated flows and can also apply policies around it.
- Restricted Internet Access: Locks down the device and allows it to only reach a set of authorized private and trusted public destinations.
- ZTNA for IoT: IoT devices can authenticate using digital certificates and get access to applications based on identity-aware policies.
- ZTNA for Server to Server communications or API communications: Servers and other API originators or endpoints can be given a unique identity and therefore identity-based access policies.
- ZTNA between Sites: Provides all devices on a network access to authorized applications hosted on a different network.
- Built-in security: Content filtering and IDS/IPS.
- Automatic network segmentation: Automatically segments the routes based on requesting entity's identity and access controls.
- Access to applications hosted on networks with overlapping IP address subnets.
- Protection of access to SaaS apps: Secures SaaS application access by tunneling traffic to those trusted application via a customer-owned internet gateway while allowing other internet traffic to use local direct internet access.
- Peer-to-Peer Communications: Enforces policies around whether a group of devices can communicate with each other or another group of devices directly Self-service Scaling: On-demand scale the number of connections needed for ZTNA up or down with immediate effect.

ZTNA Using OpenVPN Cloud

How to create ZTNA with OpenVPN Cloud



Have any questions? Feel free to contact us at: sales@openvpn.net

Published January 2023