Secure Virtualized Networking for Engineering

Securing the Digital Tools Driving Engineering to New Levels of Creativity

Engineering firms are no longer tied to physical blueprints and drafting tables. From smart building devices and building information modeling (BIM) tools to cloud-based project management software, digital tools are driving engineering innovation.

However, cybercriminals and state-sponsored threat actors are more motivated than ever to extract data and intellectual property from these firms. The list of threats is long — phishing emails, lost devices, unauthorized access, insider theft — and every IoT device, employee, and subcontractor is a potential breach point.

Network Security Challenges for Engineering

This means engineering firms have to rethink how they protect their distributed data and networks. For many, the answer lies in taking a more modern, secure, and flexible approach to distributed workforce security.

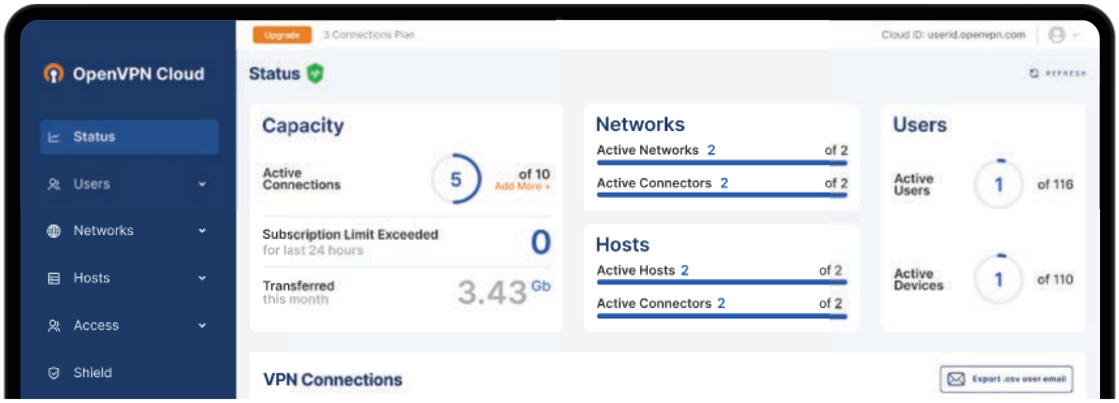
- Securing communications from IoT devices, like smart sensors and other equipment.
- Ensuring secure communication between business partners and suppliers.
- Protecting remote access to proprietary corporate data, a growing array of SaaS applications, and 3rd-party field equipment teams.
- $ Managing traditional networking hardware that can be labor-intensive, complex, and costly.
- Providing secure point-to-point connections while maintaining scalability and flexibility.

Secure Virtualized Networking for Engineering

Trusted Leader in Secure Virtualized Networking

OpenVPN® Cloud enables secure, reliable network connectivity across a telecommunication company's digital footprint, keeping your data communications safe from bad actors.

Our cloud-based platform enables organizations to maintain secure communication between their distributed workforce, IoT/IIoT devices, and the online services they rely on daily. Built on the market-proven OpenVPN protocol, the solution combines advanced network security, encrypted remote access, and content filtering into a virtualized secure network that provides the best of VPN and ZTNA security.



OpenVPN Cloud

A Single, Cost-Effective Solution

With OpenVPN Cloud, you can quickly and cost-effectively provide secure remote access to on-premise, cloud, and SaaS applications for your distributed workforce using a secure, virtualized, and reliable modern network. You control and define access rules and connection points for both on-premise and cloud applications from anywhere in the world.

Because the OpenVPN Cloud solution is entirely flexible and dynamic, you can easily add, remove, and manage users, devices, and applications as an integral part of your digital transformation initiatives. You are no longer required to manage a complex array of rigid and expensive network and security devices that only provide part of the solution. OpenVPN Cloud provides a single, cost-effective secure network connectivity solution that is ideal for securing your distributed networks and communications.

OpenVPN Cloud

Key Features and Benefits

Worldwide meshed private network

Securely connect all private networks and distributed applications

Application domain-based routing

Zero Trust Access to applications to prevent lateral movement

Identity Management

Single sign-on with identity-based access control

Content filtering and IDS/IPS

Reduce costs with integrated advanced security features

Secure, high performance tunneling

Tunnel traffic to 3rd-party security gateways and prevent unauthorized access

Easy on-demand provisioning

Reduce demands on overworked IT and networking staff

Join 20,000 + commercial customers deploying network security with OpenVPN Cloud

- ✓ Connect up to three devices free
- ✓ Scale as your business grows
- ✓ Support, upgrades and Connect Client included

Learn more

Activate Your Account Now