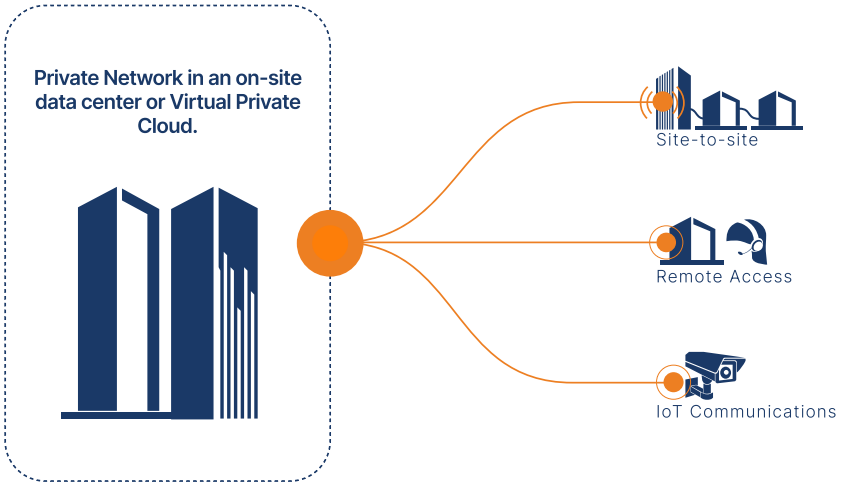
OpenVPN Access Server

What is OpenVPN Access Server?

OpenVPN Access Server, our self-hosted solution, simplifies rapid deployment of a secure remote access and site-to-site solution with a web-based administration interface and built-in OpenVPN Connect app distribution with bundled connection profiles.

We built OpenVPN Access Server using the OpenVPN open source core and additional open source software like OpenSSL. This provides full transparency of the critical security and protocol functionality. The community edition creates secure VPN connections using a custom security protocol that utilizes SSL/TLS. With over 60 million downloads to date, the community edition is a community-supported OSS (open-source software) project.

OpenVPN Access Server maintains compatibility with the open source project, making the deployed VPN immediately usable with OpenVPN protocol-compatible software on various routers and operating systems, as well as Linux. The official OpenVPN Inc.-developed client, OpenVPN Connect, is available for Windows, macOS, Linux, and mobile OS (Android and iOS) environments.



What are the Benefits of OpenVPN Access Server

Open Source

Built on a transparent, open-source code through the OpenVPN open-source project.

Admin-friendly

Easy to install, set up, and manage through an intuitive admin web portal.

Flexibility

Flexible deployment options and widespread availability on cloud marketplaces.

Remote and Site-to-Site Access

Support for both site-to-site and remote access virtual networking.

Fast Installation

Clients are bundled with connection profiles for quick installation and connectivity.

Authentication

Secure authentication methods such as PAM, RADIUS, LDAP, SAML, or a custom method. Multiple methods can be used in conjunction with each other.

Access Control

The ability to set up fine-grained access controls at user and group levels.

Economical

Budget-friendly licensing model based on the number of concurrently connected devices, plus 24/7 support included.

Scalability

Clustering and the added efficiency of sharing VPN connections across multiple Access Servers ensure high-availability and large-scale remote access.

Ready to get started?

Be up and running in less than an hour.

Start Now | Request Demo

What Makes OpenVPN Access Server Different?

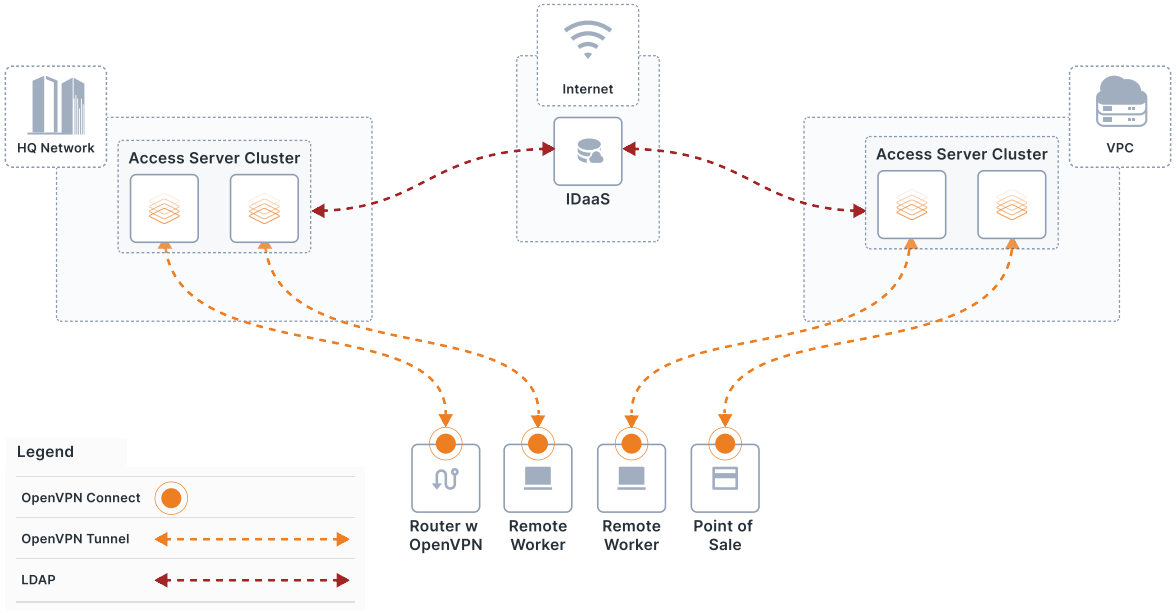
Unlike other solutions, with OpenVPN Access Server you can:

- Start right away with two free concurrent connections.
- Easily configure users, routing, authentication, and more from a web interface, whether or not you have extensive Linux knowledge.
- Purchase economical licensing with pricing based on simultaneous VPN connections.
- Launch your server with software built on the open-source core technology OpenVPN and OpenSSL — trusted and tested by millions worldwide.
- Share your subscribed connections across multiple Access Servers.
- Allow multiple authentication methods simultaneously with LDAP, SAML, RADIUS, PAM, or local.
- Use or develop your own plugins to extend the authentication system.
- Provide active-active nodes with a cluster of Access Servers.
- Purchase cloud-friendly subscriptions that don't lock to hardware and can be scaled up or down instantly.
- Choose between monthly and annual plans.
- Trust our pure-play software VPN solution.

How Does OpenVPN Access Server Work?

Secure Remote Access

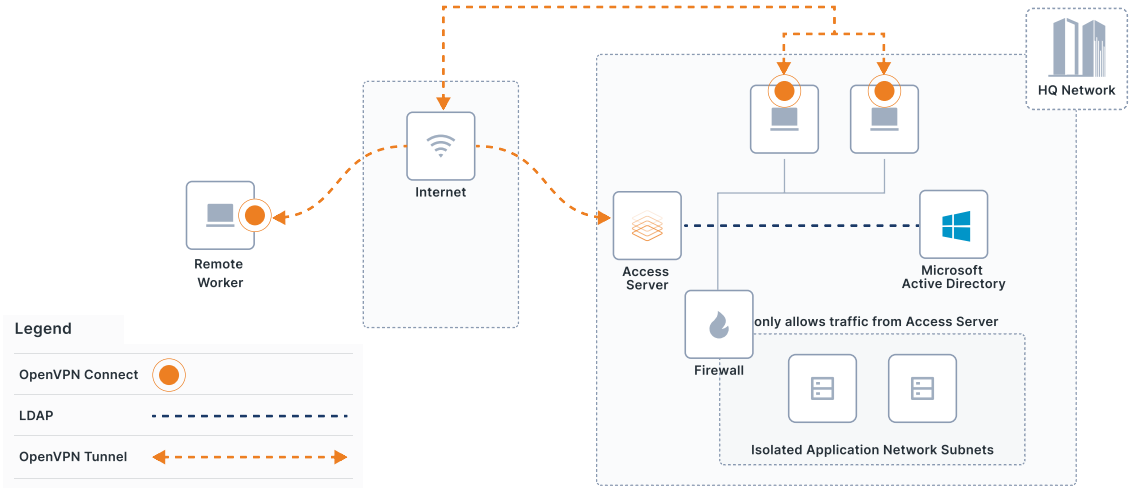
Whether you have servers in your office, an off-site data center, or a cloud-based system containing all of your data, OpenVPN Access Server can provide secure access. Depending on how you configure the access control rules in the Access Server portal, users can transparently access either all of the resources there or only specific systems or services.



How Does OpenVPN Access Server Work?

Enforcing Zero Trust Access

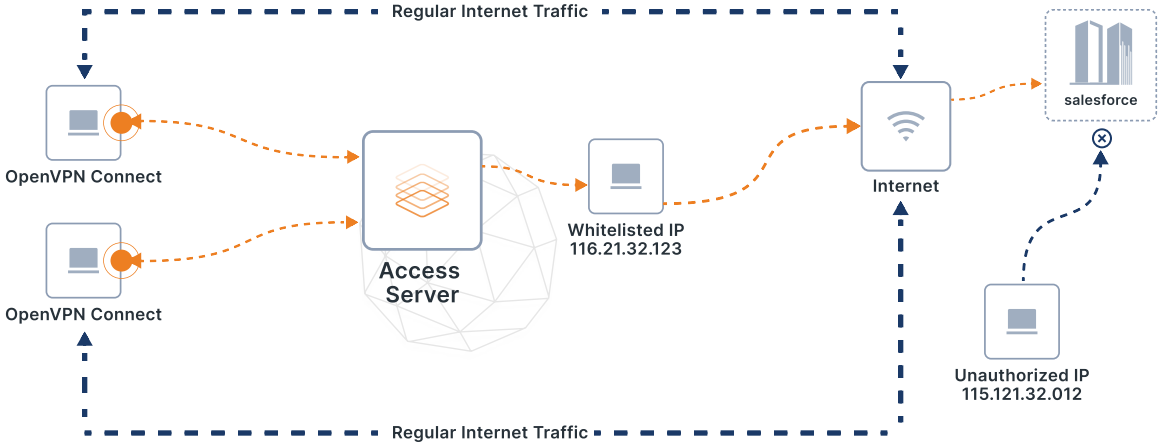
Enforcing Zero Trust Access is a critical layer of a reliable security program. OpenVPN Access Server allows businesses of all sizes the ability to create a secure virtualized network. This network expands secure access that protects workers using home and public WiFi networks, as well as SaaS applications, outside your network perimeter. We also provide all the tools and capabilities necessary for building a strong zero trust network to block or significantly mitigate attacks.



How Does OpenVPN Access Server Work?

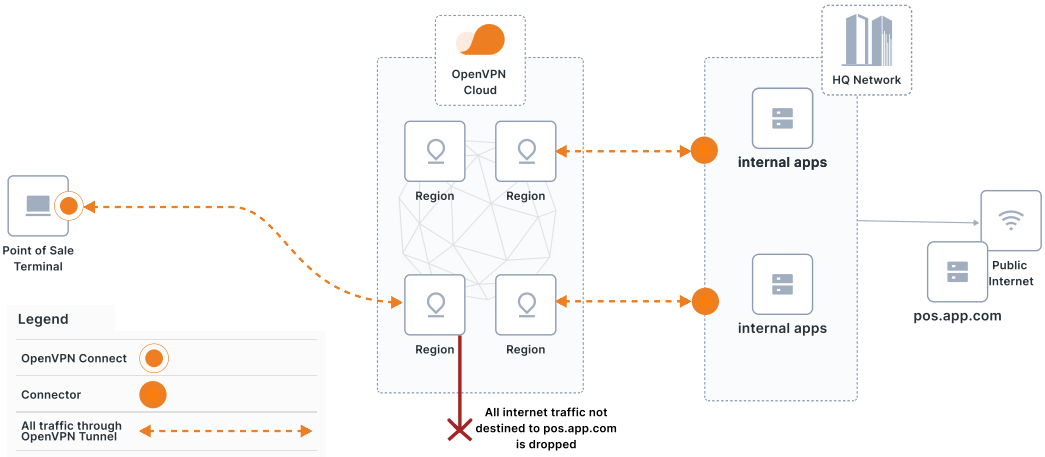
IP Address White Listing

Have your end-users connect to your applications securely from the Access Server IP address firewalls whitelist.



Protected Screen Sharing and Remote Desktop

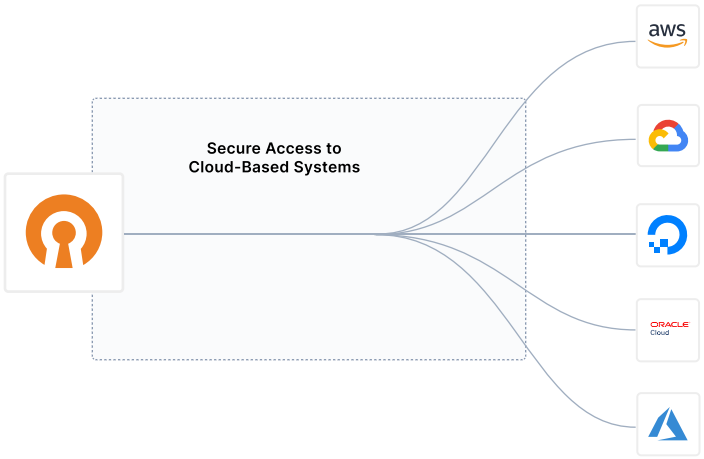
Add a layer of protection to remote desktop protocol (RDP) and other desktop screen-sharing services by enforcing VPN use with strong authentication and implementing network access authorization to restrict the use of RDP to a specific computer.



How Does OpenVPN Access Server Work?

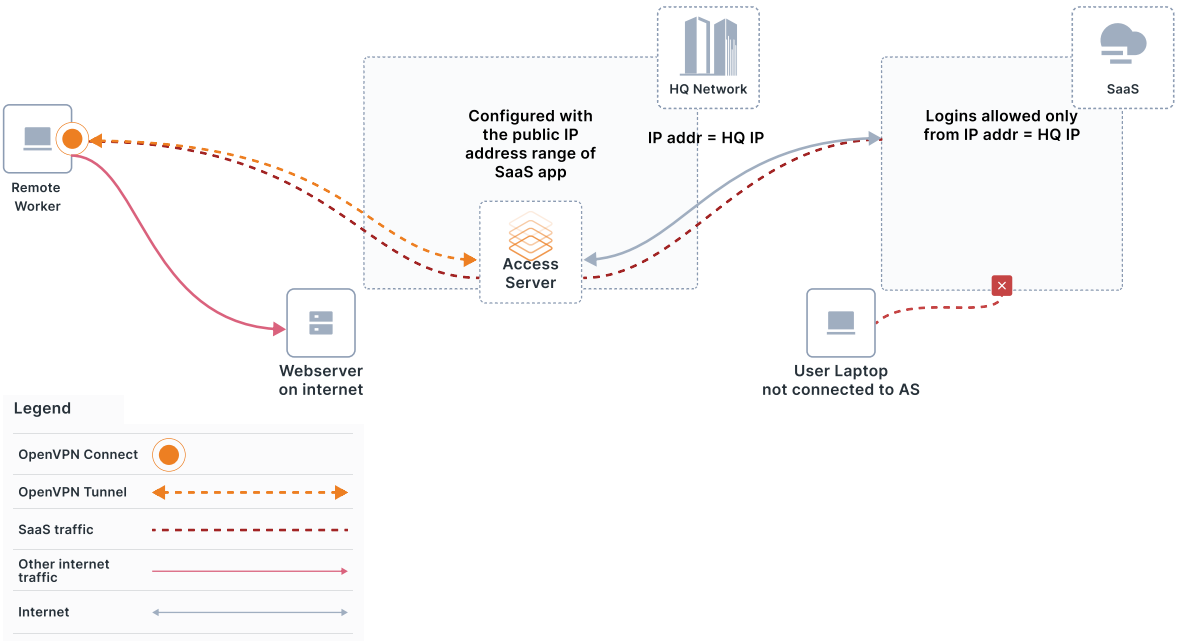
Secure Access to Cloud-Based Systems

You can extend the benefits of an IaaS cloud provider to your VPN server by using one of our pre-configured solutions.



Secure Access to SaaS Applications

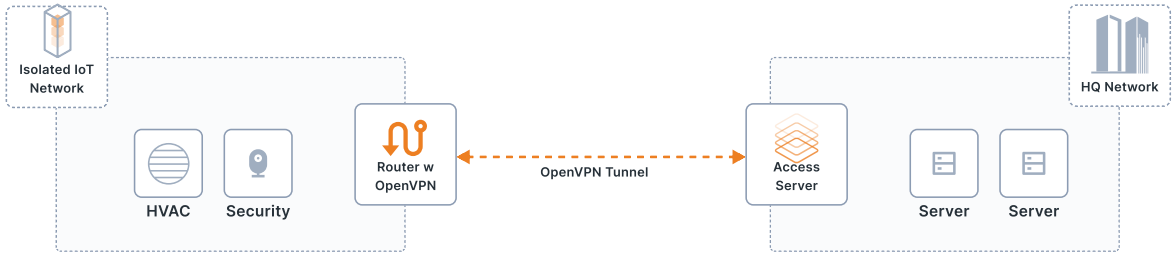
Ensure the security of your SaaS applications with private network access through Access Server. You'll get more control over who can connect — whether it's employees, vendors, or partners.



How Does OpenVPN Access Server Work?

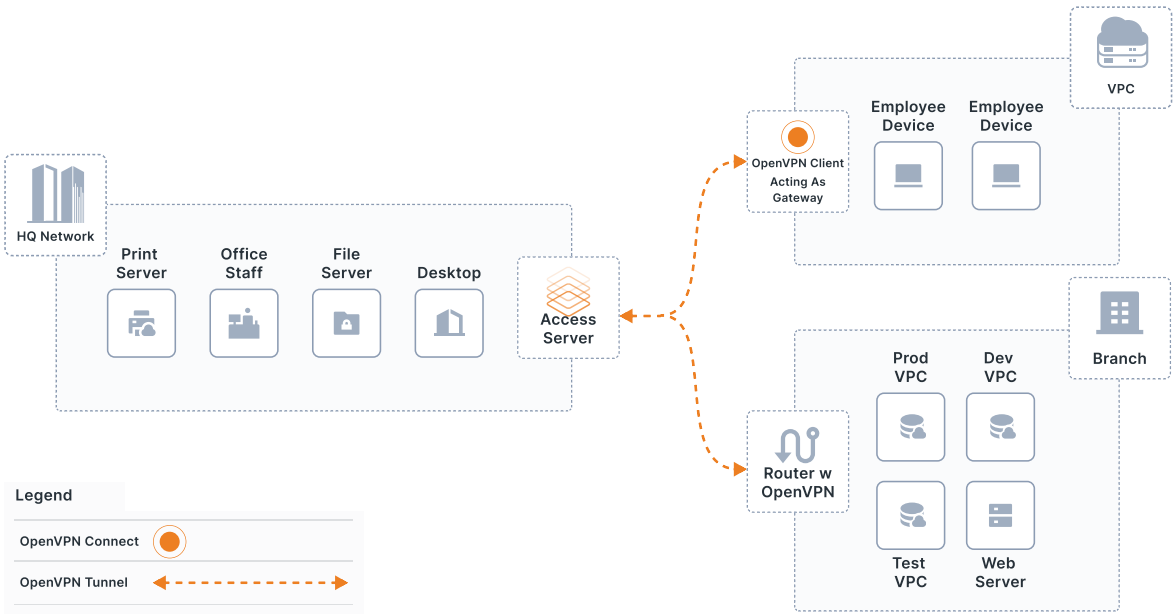
Secure IoT Communications

Create a secure virtual network to protect all traffic shared by your IoT devices. Access Server gives businesses of all sizes the enterprise-grade encryption, security, and reliability to support their growing IoT environment affordably.



Site-to-Site Connectivity

Use OpenVPN Access Server to interconnect your private networks spread among multiple sites and public clouds. Securely add your network to the VPN with OpenVPN protocol-compatible routers.



OpenVPN Access Server / Datasheet

Why is OpenVPN Access Server the Best Choice for Self-Hosted Secure Network Connectivity?

Built on Open-Source Software

We built OpenVPN Access Server on the OpenVPN open-source community edition software project. The community edition creates secure VPN connections using a custom security protocol that utilizes SSL/TLS. With over 60 million downloads, the community edition is a community-supported OSS (open-source software) project.

OpenVPN Access Server maintains compatibility with the open-source project. This makes the deployed VPN immediately compatible with OpenVPN client software across multiple platforms and devices. Access Server can accommodate Windows, macOS, Linux, and mobile OS (Android and iOS) environments.

Simple Installation

OpenVPN Access Server is simple to install, whether you host it on an on-premise server or launch it from a cloud marketplace. You can easily launch the server, configure it with the web-hosted Admin Web UI, and connect clients. Access Server comes with a built-in set of installer files for OpenVPN Connect client software1.

The client programs come pre-configured for use immediately after installation when downloaded from Access Server. You simply provide your users with the URL for your VPN server (whether it's the IP address or a custom hostname) and the appropriate credentials. Once signed in, they can choose the client software they need: Windows, macOS, Linux, Android, or iOS.

For detailed steps to start using OpenVPN Access Server, take a look at our Admin Web UI Manual.

Why is OpenVPN Access Server the Best Choice for Self-Hosted Secure Network Connectivity?

Streamlined Management

OpenVPN Access Server makes VPN management and configuration simple for anybody — with or without Linux knowledge — by providing a powerful and easy-to-use web-based admin site. While the open-source solution requires a high degree of knowledge regarding all the configuration options possible with the software, OpenVPN Access Server offers a streamlined web-based interface. The options are laid out in a graphical user interface that lowers the learning curve significantly.

Access Server integrates OpenVPN server capabilities, enterprise access management, and OpenVPN client software packages that accommodate Windows, Mac, Linux, Android, and iOS environments.

VPN Software Repository and Packages

Linux is the operating system of choice for the OpenVPN Access Server self-hosted business VPN software. It is available as software packages for Ubuntu LTS, Debian, Red Hat Enterprise Linux, and CentOS.

- Ubuntu 24 [x86_64]
- Ubuntu 24 [arm64]
- Ubuntu 22 [x86_64]
- Ubuntu 22 [arm64]
- Ubuntu 20 [x86_64]
- Ubuntu 20 [arm64]
- Debian 12, 64 bits
- Debian 11, 64 bits
- Red Hat 9, 64 bits
- Red Hat 8, 64 bits

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

Virtual Appliances

OpenVPN Access Server Virtual Appliance is a full-featured secure network tunneling VPN virtual appliance solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified user interface, and the OpenVPN Connect app that accommodates Windows, macOS, and mobile environments.

OpenVPN Access Server supports various configurations, including secure and granular remote access to internal and private cloud network resources, and applications with fine-grained access control.

Virtual Appliance VHD

- Appliance includes all Hyper-V required modules.
- Just download and import using the Hyper-V Manager.

Microsoft Hyper-V Deployment Guide

VHD Quick Start Guide

Virtual Appliance VMware ESXI

- Compatible with VMWare ESXi 5.0 or newer.
- Released as OVA file with virtual hardware revision 8.

VMWare ESXi Deployment Guide

VMWare ESXi Quick Start Guide

OPENVPN

OpenVPN Access Server / Datasheet

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

VPN Server Cloud Solutions

If your business is reaping the benefits of increased deployment agility from your Infrastructure-as-a-Service (IaaS) Cloud provider, extend those benefits to your VPN Server with our pre-configured solutions for AWS, Azure, Google Cloud, Digital Ocean, and Oracle Cloud.

Secure Access to AWS Services

Safely connect your devices over the public internet to your private, secure VPC network on Amazon AWS.

Securely connect your on-premises office network to the Amazon AWS VPC network.

Define access rules that let specific devices access only portions of your VPC network or all of it at once.

Redirect all or specific Internet traffic from your devices through the Access Server, or only access your VPC network.

Create safe connections with multiple VPCs secured with OpenVPN protocol encryption.

Create connections between Amazon AWS VPC networks and Microsoft Azure Virtual Networks.

Launch Access Server on AWS →

Secure Access to Azure Services

Safely connect your devices over the public internet to your private, secure Virtual Network on Microsoft Azure.

Securely connect your on-premises office network to the Microsoft Azure network.

Define access rules that let specific devices access only portions of your network or all of it at once.

Redirect all or specific Internet traffic from your devices through the Access Server, or only access your Virtual Network.

If you want, you can even allow connections between VPN clients or block access to local networks.

Launch Access Server on Mircosoft Azure →

Secure Access to GCP Services

Provide internet-connected devices, users, and administrators remote access to your private data center in the public cloud.

Stitch together multiple on-premises and cloud network subnets into one private network.

Add access controls to your cloud resources within your GCP Virtual Private Cloud (VPC).

Launch Access Server on Google Cloud →

Access Server for Digital Ocean

Extend your DigitalOcean Private Networking to remote users and other sites using OpenVPN Access Server.

Create hub-spoke, mesh, or other network topology to interconnect all your sites with our Digital Ocean Marketplace VPN.

Provide secure, remote access to applications deployed on Digital Ocean droplets.

Launch Access Server on Digital Ocean →

Extend Your Oracle VCP

Use SSL/TLS site-to-site VPN as a backup route for your IPSec and FastConnect connectivity.

Manage security and granular remote access to your internal network and/or private cloud network resources and applications.

Provide cross-compatibility to support any user device with Android, iOS, Linux, macOS, and Windows for secure access to Cloud resources.

Launch Access Server on Oracle →

OPENVPN

OpenVPN Access Server / Datasheet

OpenVPN Access Server Technical Specs

Connection Support

- Provides layer three virtual private networking using OpenVPN protocol.
- OpenVPN protocol uses SSL/TLS with client and server certificates to perform key exchange and mutual authentication.
- OpenVPN is firewall and web proxy friendly as encrypted traffic is tunneled via UDP or TCP.

Routing Support

- Direct Connection (server set in SNAT mode) – VPN clients initiate all communication in this mode.
- Routed Connection (server in static route as a gateway to VPN clients) – VPN clients and devices on the internal network initiate connections.
- Site-to-Site routing using a suitable Linux-based system configured as a gateway at one site with a routed connection to the VPN server at the other site.

Security Protections

- You can configure software firewalls with access control rules to specify which user or group has access to what IP addresses or subnets and whether VPN clients can route to each other.
- Control access to services by IP address, protocol, and ports.
- Compliant with FIPS restrictions.

Database Support

- Supports MySQL (defaults to SQLite database).

Client Configuration

- IP address, DNS servers, WINS server, specific routes, client-side scripts.

Virtualization Support

- Prepared VM images are available for Microsoft Hyper-V and VMWare ESXi.

Authentication Methods

- Supports multiple simultaneous authentication methods using local user database, Pluggable Authentication Modules (PAM), LDAP, secure LDAP, Active Directory, SAML, and RADIUS.
- X.509 certificate PKI solution is built-in. Integration with external PKI is available.
- Hardware address checking (UUID or MAC) as an additional security method is supported.
- Time-based One-Time Passwords (TOTP) multi-factor authentication is supported natively in Access Server. Custom extensions for MFA are also possible, such as the one for Duo Security's authentication solutions. Hardware tokens are supported in OpenVPN Connect.

OpenVPN Access Server / Datasheet

Ready to Get Started with OpenVPN Access Server?

Get Started

We make getting started with OpenVPN Access Server as easy as possible by offering two free connections.

After you create an account, you can launch OpenVPN Access Server by following the quick start guides, or download the software for the platform of your choice from the Access Server portal.

Our Technical Support team is available 24/7 to guide you through every step of set-up and configuration and answer any questions you may have.

- Create an OpenVPN account, and select an identity for your Cloud (for example, cyberone).
- Go to the Shield section, and turn ON blocking of dangerous and unwanted categories.
- Download and launch the OpenVPN Connect app.
- Add a profile in the Connect app by using your OpenVPN Cloud URL (for example, cyberone.openvpn.com), authenticate, and select a Region to connect.

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