OPENVPN®
Access Server

DATASHEET

A FULL-FEATURED SOLUTION TAILORED TO MEET YOUR VIRTUAL PRIVATE NETWORK (VPN) NEEDS

OpenVPN is the author of the open source Virtual Private Network (OpenVPN) software, which has emerged to establish itself as the de-facto standard in the open source networking space. OpenVPN is also the provider of multi-platform OpenVPN applications across all OS platforms, addressing the market demands for Remote Secure Access, Access Control, and Cybersecurity — protecting businesses of all sizes, all around the globe.

OPENVPN ACCESS SERVER

OpenVPN Access Server is a complete VPN solution designed specifically for businesses. Access Server secures data communications, provides remote access for employees, secures IoT, and provides secure access to on-premise, data center, or public cloud resources.

Some of the key features of OpenVPN Access Server are:

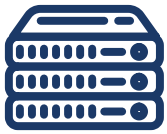
- Rock-solid, hardened, and scalable VPN server that is easy to set up and manage
- Cloud Application Marketplace availability for AWS, GCP, Azure, and DigitalOcean
- Support for both site-to-site and remote access virtual networking
- Economical licensing model that is based on the number of VPN connections
- Easy distribution of VPN clients and connection profiles directly from the OpenVPN Access Server
- Ability to set up fine-grained access controls at user and group levels

Access Server is free to install and use for a maximum of 2 simultaneous VPN connections, so you can test it without having to pay first. If you need more connections, the cost is a $15.00 license fee per connected device per year — all updates and 24/7 support included.

OPENVPN ACCESS SERVER HAS EVERYTHING YOU WOULD NEED

BYOD Regardless of Operating Systems

OpenVPN Clients free your users to choose their favorite device with support for Android, iOS, Linux, macOS, and Windows.

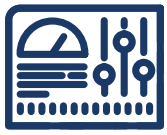


Scalable, Fault-tolerant, and Flexible Deployment Options

- Multiple Access Servers can be configured to act as a single cluster. Thus, deployments can scale horizontally, depending on the volume of incoming connections.
- Clustering provides for active/active redundancy for fault-tolerant deployments
- Server software installation images are available for:
  - Most of the popular Linux distributions
  - VMware and Microsoft virtualized infrastructure
  - AWS, GCP, Azure, and DigitalOcean

VPN Administration Web Portal

- Administrator portal provides for intuitive configuration of settings
- User connection access logs can be viewed and searched
- For those administrators that prefer Command Line Interface (CLI) access, a rich command set is available



Fine-grained Access Control

- Global, Group, and User hierarchy allows for methodical access configuration
- Rules can be defined at the IP address, protocol, and port granularity

One-click Client Distribution

- Just sharing the web address of Access Server's Client Portal with your users solves the Client distribution challenge inherent in wide-scale deployments
- After authentication, users download their Client installation files or connection profiles directly from the Access Server's Client Portal

Multiple Secure Authentication Modes

- Integrated with two-factor authentication using Google Authenticator
- Plug-ins can be used to integrate multi-factor authentication with Duo Security, smart cards and any TOTP based token generators
- Users can be authenticated using PAM, RADIUS, LDAP, Active Directory, or a local user database

No-hassle Certificate Management

- OpenVPN Access Server comes built-in with its own internal X.509 PKI, but can also support an external PKI
- VPN clients get their certificates bundled with their configuration profiles

Transparent Open Source Code

- Leverages OpenVPN, and OpenSSL open source projects
- Code is scrutinized and quick fixes are ensured due to large community support

Feature Category	Supported Features
Connection Support	Provides Layer 3 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.
Cryptographic Services	OpenSSL provides the core for secure communications and cryptography. The crypto suite can be customized to suit your needs, the defaults are AES-256-CBC cipher for encryption, HMAC-SHA256 for authentication, Diffie-Hellman Group 1 4, and 2048-bit RSA key length.
Linux OS Support	Red Hat Enterprise Linux, CentOS, Ubuntu, and Debian.
Database Support	Supports MySQL (defaults to SQLite database)
Cloud Image Availability	• Amazon Web Services (available from AWS Marketplace). Both BYOL and Tiered • Microsoft Azure (available from Azure Marketplace) • Google Cloud (available from Google Cloud Platform Marketplace) • DigitalOcean (available from DigitalOcean Marketplace)
Virtualization Support	Prepared VM images are available for Microsoft Hyper-V and VMWare ESXI
Client OS Support	OpenVPN Connect clients are available for Android, iOS, macOS, and Windows. OpenVPN open source client is included in all major Linux distributions.
Client Configuration	IP address, DNS servers, WINS server, specific routes, client-side scripts[1]
Split-Tunneling	Full-tunnel and split-tunnel redirection are possible (all VPN client Internet traffic goes through the VPN tunnel, or only specified traffic).
Authentication Methods	• Supports local user database, Pluggable Authentication Modules(PAM), LDAP, secure LDAP, Active Directory, and RADIUS • X.509 certificate PKI solution is built-in. Integration with external PKI is available • 'MAC address lock' as an additional security method is supported • Multi-factor authentication is supported in various forms. For example, Google Authenticator is built-in, and two-factor authentication using smart cards, Duo Security, or other TOTP based token generator can be added as a plug-in • User name/password authentication
Security Protections	• Software firewall can be configured with access control rules to specify which user or group has access to what IP addresses or subnets, and if VPN clients can route to each other or not • Access to services can be controlled by IP address, protocol, and ports

Feature Category	Supported Features
Management Tools	Command Line Interface (CLI), XML-RPC API, and Administration web portal
Availability, Failover	• Multiple Access Servers can be configured to form a Cluster allowing a VPN client to connect to any of the available Access Servers using the same credentials • Clustering provides for active/active redundancy for fault-tolerant deployments • UCARP-based primary-secondary failover for LAN deployments
Routing Support	• Direct Connection (Server set in SNAT mode) - All communication needs to be initiated from the VPN clients in this mode • Routed Connection (Server in static route as gateway to VPN clients) - VPN clients as well as devices on the internal network can initiate connections • Site-to-Site routing using a suitable Linux-based system configured as Gateway at one site while using a routed connection to Server at the other site
Ease of Client Deployment	Users can download preconfigured client software, or connection profiles for their device directly from your deployed Access Server's User Web Portal.
Scalability	• A typical server can handle up to 1 ,500 concurrent connections carrying real-world traffic[2]. • Multiple Access Servers can be configured, via the web administration portal, to act as a single cluster. Thus, allowing for deployments to scale horizontally, as needed, to handle large volume of incoming connections.
Reporting	Detailed client access logs are searchable, downloadable, and viewable.
Branding	Customizable Server Portal branding
Licensing Options	• Two (2) simultaneous connections are supported in trial mode free of charge • An annual licensing fee is charged based on the quantity of VPN connections. Upfront multi-year purchases are offered a discount • AWS tiered pricing is supported

1 . The ability of the Client to execute code is dependent on the device's OS and required code execution privileges. Mobile Operating Systems are not supported.

2. This is an estimate. User capacity will also depend on the bandwidth consumed per user and the system's total available bandwidth. A typical server is considered to be one with at least an 8-core CPU and 8 GB of RAM.

OPENVPN®

7901 Stoneridge Drive, Suite 540
Pleasanton, CA 94588 USA
Sales: sales@openvpn.net
Support: help@openvpn.net

OPENVPN.NET