



Business VPN

vs



Personal VPN

As already mentioned, one of NordLayer’s key offerings is a VPN specifically designed for business use. The table below highlights the key differences between the two types of VPN as well as the benefits for companies using NordLayer over a personal VPN.

## NordLayer

Business VPN

## NordVPN

Personal VPN

### Business use

Protects your company’s network and enables workers to safely access the company’s resources while working remotely. Secures all internet traffic with powerful encryption. Provides next-generation VPN solutions.

### Personal use

Creates an encrypted tunnel for online traffic so nobody can get their hands on your internet data. Provides peace of mind when using public Wi-fi and keeps your browsing history private.

### Multiple users

Covers the needs of an entire organization. All employees can get access to a VPN and securely reach their company’s resources, from any location. Every user can secure up to 6 devices. Licenses, dedicated servers, and company gateways can be added as the organization grows.

### A single user

Designed for an individual user. Can secure up to 6 devices at the same time, on all major operating systems.

### Centralized billing

Centralized billing means you won’t have to arrange a payment every time a new user joins – it will be done automatically.

### Individual subscription

Each customer pays for their own user license.

## Users are managed centrally

The owner of the organization creates an account and invites their colleagues to join. Via the Control Panel, he/she adds more members, assigns them rights, and creates teams.

Core and Premium plan holders are able to set up private gateways and dedicated servers. They can see which gateways and devices the members are using and audit all Control Panel actions made by them and other admins.

Settings such as biometric authentication, SSO and 2FA can also be enforced and implemented centrally — so that layers of protection are mandatory for staff.

## Personal use

You have complete control over your account.

## Dedicated server option

You can purchase dedicated servers with static private IP addresses, allow-list the IPs, and create gateways for convenient access control. A dedicated server ensures a more stable performance because it's not shared with any other organization.

## Dedicated IP option

You may use a shared IP or purchase a dedicated IP solely for your use. A dedicated IP is less likely to be excluded from certain websites, enables you to avoid CAPTCHAs, and makes online payments easy.

## Two-factor authentication and Single Sign-On

A team member can use their existing credentials to log in to the app with Azure AD, Google, and Okta.

Two-factor authentication is also available and can be enforced for the whole organization.

## Two-factor authentication

You can protect your account with an extra layer of security by setting up 2FA.

As you can see, you need a personal VPN to protect your data online, have more privacy, and access global content. But using a personal VPN won't cover the complex needs of an organization and won't provide you with benefits such as scalable user license management, Single Sign-On, and centralized settings or billing.