V

VPN: What It Protects, What It Does Not, and Safe Setup

A VPN encrypts traffic between a device or network and a VPN gateway. It protects one part of the path but does not provide anonymity or stop every attack.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How a VPN works
02 Three common VPN types
03 What a VPN can protect
04 What a VPN does not protect
05 How to choose and configure a VPN
06 Troubleshooting and leak checks
07 VPN versus zero trust
08 Source

Quick answer: A virtual private network (VPN) creates an encrypted tunnel between your device or network and a VPN gateway. It can protect traffic on an untrusted local network and provide remote access to private resources. It does not make you anonymous,

remove malware, stop phishing, or protect traffic after it leaves the VPN provider or company gateway.

01 How a VPN works

Without a VPN, an internet service provider or local network can usually see destination and timing metadata, although HTTPS encrypts the content of most modern web sessions. With a VPN, the local network sees an encrypted connection to the VPN gateway. The gateway decrypts and forwards traffic toward its final destination, so the gateway operator becomes an important point of trust.

HTTPS is still necessary. It protects the application connection between the browser and website, while a VPN protects the tunnel segment. A VPN provider may see connection metadata and, for non-HTTPS services, content after it leaves the tunnel.

02 Three common VPN types

- **Remote-access VPN:** connects an employee or administrator device to a company network. It may expose selected internal services or route all device traffic through the organization.
- **Site-to-site VPN:** links entire office, cloud, or data-center networks through gateways.
- **Consumer privacy VPN:** sends internet traffic through a commercial provider, changing the public source IP seen by websites and reducing visibility for the local network or ISP.

A corporate VPN is not automatically a consumer privacy service, and a consumer VPN normally does not grant safe access to internal company systems.

03 What a VPN can protect

- Traffic between the VPN client and gateway against passive observation on local Wi-Fi.
- Private services that should not be exposed directly to the public internet.

- A device’s public IP from the destination site, which instead sees the gateway address.

04 What a VPN does not protect

A VPN does not prevent you from entering a password on a phishing page, opening a malicious attachment, accepting tracking cookies, or signing into an account that identifies you. It cannot fix an infected endpoint. Browser fingerprinting and account logins can link activity across IP changes. A provider that promises complete anonymity, immunity from hacking, or guaranteed access to every region is overstating what the technology does.

05 How to choose and configure a VPN

1. Define the goal: private corporate access, safer use of an untrusted network, or changing the apparent public location.
2. Use a maintained protocol and app from the organization or a provider with clear ownership, support, update history, privacy terms, and independent security assessment.
3. Enable automatic updates, a kill switch when traffic must never bypass the tunnel, and DNS handling that follows the intended route.
4. For corporate access, require phishing-resistant MFA, device compliance, least-privilege network access, and logging. Patch VPN gateways promptly because internet-facing appliances are frequent targets.
5. Understand split tunneling. It improves performance by sending only selected traffic through the VPN, but creates two simultaneous network paths and can weaken organizational monitoring.

06 Troubleshooting and leak checks

If the VPN connects but a service fails, check system time, DNS resolution, routes, proxy settings, MTU, and whether the application uses IPv6. Compare the expected public IP and DNS resolver before and after connecting. A consumer “leak test” shows routing behavior at that moment; it does not prove the provider keeps no logs or that the endpoint is secure.

07 VPN versus zero trust

Traditional remote-access VPNs can place a device broadly inside a private network. Modern access designs increasingly authenticate the user, device, and individual application for each session and reduce lateral movement. Organizations do not have to remove every VPN immediately, but should avoid treating possession of a VPN connection as unlimited trust.

08 Source

For current enterprise access considerations, see the CISA guidance on modern network access security.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com