Proton VPN

Proton VPN Technical Reviewers Guide

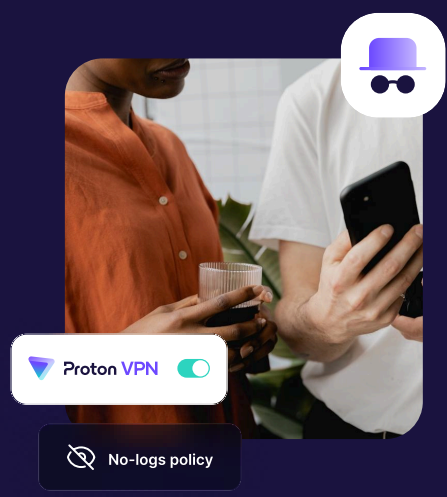
This guide aims to help reviewers fully understand Proton VPN and its features while also providing the level of granular technical detail necessary to assess our product accurately.

This guide looks at:

Proton VPN at a glance

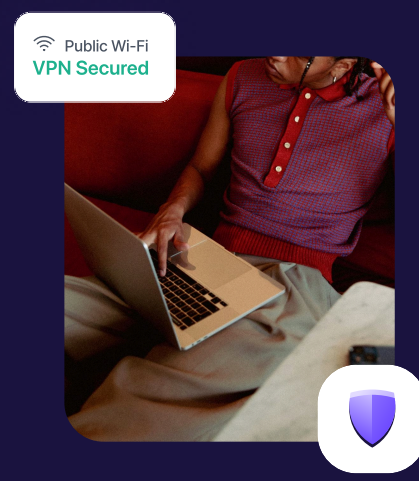
Proton VPN is committed to protecting our users' privacy, which is why we have a **strict no logs policy.** We do not keep any logs of users' online activity and do not store any metadata.

- 2025 independent security audit
- 2025 no-logs audit



Streaming and geo-blocked content

Proton VPN unblocks a wide selection of popular online media services, allowing users to access their favorite streaming content from anywhere in the world.



Built-in strong anti-censorship technologies

Proton VPN is used by journalists, activists, and organizations worldwide

Proton is also one of the few independent voices left in the VPN space. Many well-known VPN services are owned by a small number of umbrella companies (who often also own technology focused websites that review VPN services). Proton is owned by Proton AG, whose primary shareholder is the non-profit Proton Foundation, whose legally binding job it is to ensure that Proton does not deviate from our mission to build a better internet that serves the interests of all of society.

Proton VPN is available on all devices, including PCs, Macs, smartphones, and even routers. Proton VPN has native apps for **Windows, macOS, Linux, Chromebook, Android, Android TV, iOS/iPadOS,** and **tvOS** (Apple TV). We also offer browser extensions for all **Chrome/Chromium** based and **Firefox-based** browsers (and are now directly integrated into the Vivaldi browser).

What is Proton VPN?

First launched in 2017, Proton VPN was the second product from Proton (the first being our celebrated zero-knowledge, end-to-end-encrypted email service, Proton Mail). Proton now offers a suite of open-source products that make it the world's first privacy-by-default ecosystem:

- Proton VPN
- Proton Mail
- Proton Drive (with Docs in Drive)
- Proton Pass (password and identity manager)
- Proton Wallet
- Proton Calendar
- Proton Lumo (the only AI assistant that respects your privacy)
- Proton Authenticator
- Proton Meet

What makes Proton unique?

Proton's purpose is to build a better internet where people come first and privacy is the default.

Creation

Proton was born in Switzerland in 2014 when scientists who met at CERN (where the World Wide Web was born) decided to build a better internet where privacy is the default. Proton was launched after a successful public crowdfunding campaign in which over 10,000 individuals donated over $500,000 to bring our shared vision to life.

Mission

For our 10th anniversary (June 17, 2024), Proton transitioned to a non-profit model by establishing the Proton Foundation to clarify and secure Proton's mission: To remake the internet in a way that is private by default and serves the interest of all of society.

Everything we do is underpinned by four core values:

- **Community first**
  We are here to serve the world first and foremost. Proton is built by the community, for the community, trusted by over 100 million people and businesses worldwide.
- **Open source**
  We are committed to transparency and open-source software. Proton is a key contributor to the open source community, and we regularly commission third-party audits of our products.
- **Business model**
  Our freemium business model puts users first and aligns our financial incentives with users' needs.
- **Easy-to-use end-to-end encryption (E2EE)**
  We build alternatives to traditional services that are easy, safe, and private, making E2EE accessible to everyone.

Business model

To this day, Proton's only source of revenue is user subscriptions. Proton has now grown to become the world's leading privacy company, offering an E2EE ecosystem used by millions of people globally.

Based in Switzerland

Proton is headquartered in Geneva — our main office is there, and most of our core staff live in or near Geneva. Switzerland is not part of any 5-Eyes-related spying alliance and is not subject to EU laws.

As a Swiss company, we are subject solely to Swiss law and court orders from Swiss judges. Switzerland has no legal requirement for VPN providers to log user IP addresses or online activity (so we don't), and there are no legal mechanisms in place that could oblige us to start logging.

Learn more about why being based in Switzerland is good >

Why open source matters

With proprietary closed-source code, there's no way to know how secure an app is or if it's been designed to do something malicious. If an app is open source, anyone can examine its code to ensure it does what it's supposed to do — and only what it's supposed to do.

Of course, most people aren't qualified to examine code, but the very fact our code is available should give you some confidence in it. In a further demonstration of our commitment to transparency (and unlike many other VPNs), Proton commissions regular third-party audits of our apps and publishes the full results (after implementing any recommendations, of course).

Proton VPN also commissions regular third-party audits of our no-logs infrastructure.

Proton VPN plans

Price transparency is very important to us. It's therefore vital that reviewers and affiliates clearly state the full price that subscriptions purchased through discounted affiliate links will renew at.

Free

We offer a free plan so that anyone who needs a VPN can access one. This plan includes everything you need to protect your privacy online and access the internet without censorship.

- Unlimited data
- Connect to servers in ten counties (US, Netherlands, Japan, Poland, Romania, Norway, Switzerland, Singapore, Mexico, or Canada). The country is randomly selected, but you can change it after a short cooldown period.
- No logs
- No ads
- As secure as our paid VPN service

Paid

All paid Proton VPN plans provide full access to all our premium features. Our main paid plan is Proton VPN Plus (Starting at $4.49 /month for 24 months), which includes the following premium features:

- Ability to connect to any of 15,000+ servers in 130+ countries
- Secure streaming from a wide range of services worldwide
- Torrenting is permitted on our special P2P servers
- NetShield Ad-blocker (a DNS filtering feature that can help protect against ads, trackers, and malware)

Learn more about these features >

We don't artificially limit speeds for free users, but our free servers are much busier than our paid ones, which usually results in lower speeds (although these are often faster than many services offer to their paid customers).

Free users cannot access our premium features. These features provide advanced functionality and customization, but are not central to the core VPN experience.

On Android and iOS/iPadOS (and coming to other platforms), we offer a Guest mode that allows you to use our free service without the need to sign up for a Proton Account.

You're also part of the Proton ecosystem

Signing up for a Proton VPN Free or Plus plan gives you a Proton Account. You can use same username and password you use to sign in to Proton VPN to sign in to the free versions of all products in the Proton ecosystem.

Arguably, the best value plan we offer is **Proton Unlimited**. Starting at $7.99 /month for 24 months, this gives you 500 GB of storage and **full premium access to all products in the Proton ecosystem.**

Proton VPN features explained

Features labeled Plus are premium features available to users on a paid Proton VPN plan.

Privacy and security

VPN protocols

Our primary protocol is WireGuard®, although we'll continue to support manual OpenVPN configuration for legacy reasons. We intentionally do not support a long list of insecure VPN protocols, such as PPTP, L2TP/IPsec, etc. We consider this a feature of our service, as it means users cannot inadvertently put their connection at risk!

WireGuard (UDP and TCP)

As secure as OpenVPN, but much more efficient and performant. WireGuard is the future of VPN protocols.

Stealth

Developed by Proton VPN, Stealth is a WireGuard TCP-based protocol that can be effective at bypassing many censorship blocks.

OpenVPN (UDP and TCP)

Although offering proven battle-tested security, this venerable VPN protocol is heavyweight and slow compared to WireGuard.

Smart protocol

Not a VPN protocol at all. Smart protocol is a feature that automatically selects the best VPN protocol for your needs. (It defaults to WireGuard UDP, but if that is blocked, it will try different protocol and port options to establish a connection).

Strong encryption

We implement the strongest encryption settings for the VPN protocols we support.

OpenVPN

Data channel (data is encrypted before sending it through the VPN tunnel): Up to AES-256, in GCM mode to verify the data.

Control channel (used to secure the TLS key exchange): Up to AES-256-GCM for the symmetric cipher, with RSA-4096 and HMAC SHA-384 hash authentication to verify the TLS certificates. Our encryption suite also includes a Diffie-Hellman key agreement (DHE) to provide forward secrecy.

WireGuard

Uses proven state-of-the-art cryptographic primitives to secure your VPN connection.

- ChaCha20 — A symmetric key cipher. Much like AES on OpenVPN, ChaCha20 secures your actual data.
- Poly1305 — A message authentication code (MAC) used to authenticate WireGuard connections.
- Curve25519 — An elliptic curve used by the Elliptic-curve Diffie–Hellman (ECDH) protocol to secure the TLS key exchange. This ensures your connection to our VPN servers is secure.
- SipHash — An XOR-based pseudorandom hash function used to securely map hash table keys.
- BLAKE2 — A cryptographic hashing function used to verify data.

WireGuard implements forward secrecy.

NetShield Ad-blocker (Plus)

This is our DNS filtering feature. It blocks DNS queries to a list of known ad, malware, phishing and tracker domains. Because it blocks ads and other unwanted stuff from loading on your device, it can also reduce the data you use and speed up your connection.

If you want more advanced DNS filtering (such as custom blocklists and "net nanny" features), we've started rolling out Custom DNS across our apps.

NetShield Ad-blocker is available on all Proton VPN apps except Apple TV and our browser extensions, and can be easily implemented on third-party VPN apps and routers.

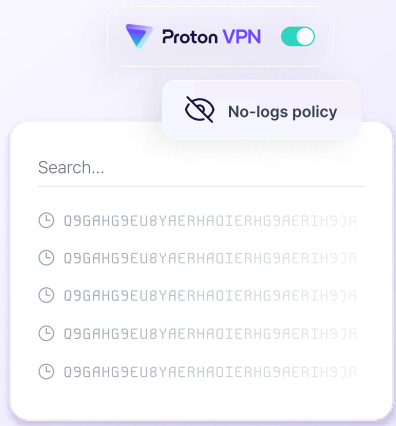
Our Windows, macOS, Android, iOS, and iPadOS apps feature a NetShield privacy panel that shows how many ads and trackers it has blocked and how much data it has saved since you last connected to Proton VPN.

DNS leak protection and IPv6 support or leak protection

By default*, all DNS queries are sent through the encrypted VPN tunnel to be performed by Proton. We implement numerous technical measures (such as firewalls and platform-specific mechanisms) to ensure they are never routed outside the VPN tunnel.

We also prevent IPv6 leaks (data being insecurely routed over IPv6 connections outside the VPN tunnel):

- We route IPv6 connections through the VPN tunnel on Windows, Linux and Android and are working to bring full IPv6 support to all our apps. This will future-proof our apps, but it will also support those few people with IPv6-only connections.
- On all other platforms, we simply block IPv6 connections. This has no impact on the user experience (unless they are IPv6-only, which remains very rare at the present time).

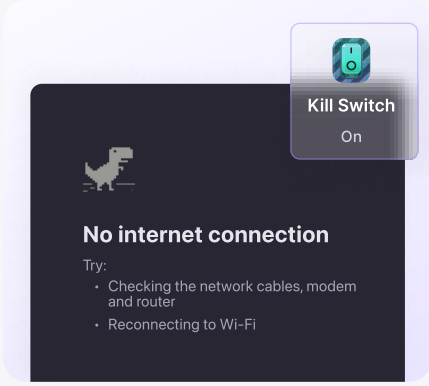


*We're starting to roll out support for Custom DNS across our apps. If this option is turned on, DNS queries are still sent through our VPN tunnel before being forwarded to your preferred third-party DNS resolver (never to your ISP or other unintended recipient). This is great for most users' privacy, but it does mean you can't connect to a DNS server on your local network.

Kill switch

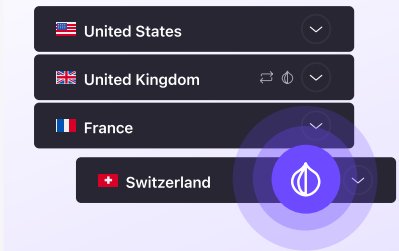
Our desktop and mobile apps all feature an optional kill switch. Our apps for Windows and Linux also feature an optional advanced kill switch:

- Kill switch — Blocks all internet traffic if the VPN connection is unexpectedly disconnected.
- Advanced kill switch — Blocks all internet traffic unless it's routed through the VPN interface. It works even if you manually disconnect the VPN.



Tor over VPN (Plus)

You can connect to the Tor anonymity network via a Proton VPN server. This hides your real IP address from the Tor entry server, removing any possibility of tracing your real P address back through the Tor network. Tbh, this feature works as intended, but almost no one uses it. We're therefore quite happy for reviewers to ignore it.



Full-disk encryption

We use only bare metal VPN servers with full-disk encryption. This means no third parties can access any data stored on the servers (which is almost non-existent, anyway).

Physical security

We have gone to extreme lengths to protect Proton VPN's Secure Core servers and ensure their security.

Critical infrastructure in Switzerland is located at a high-security data center outside of Zurich that requires biometric access, and our infrastructure in Iceland resides in a secure former military base. Our servers in Sweden are located in an underground data center.

By shipping our own equipment to these locations, we ensure that our servers are as secure as possible.

Image should not be used by partners in public.

Two-factor authentication

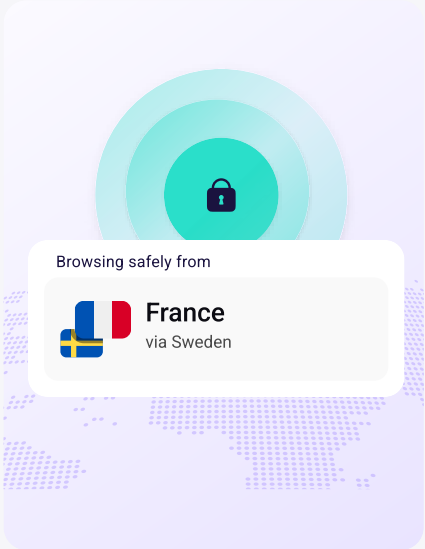
You can secure your Proton Account with 2FA. We support 2FA via TOTP smartphone authenticator apps such as Proton Authenticator, Google Authenticator, Authy, Aegis, and 2FAS, or U2F and FIDO security keys ("Yubikeys").

Secure Core (Plus)

This is our double-VPN solution, allowing you to connect to the internet via two VPN servers:

- The exit server (connected directly to the internet) is one of our regular secure VPN servers located in roughly 70 countries worldwide.
- The entry server (connected directly to your device) is a special, hardened server (see physical security above) located only in a jurisdiction with strong privacy laws (Switzerland, Iceland, or Sweden).

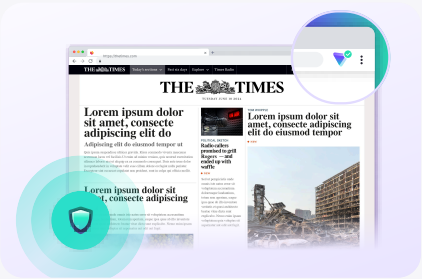
Secure Core protects against timing attacks and MITM attacks (in the unlikely event that one VPN server becomes compromised in some way). However, routing your connection through two VPN servers that are very far apart can slow down your VPN connection considerably. For that reason, we advise people to only use Secure Core if their threat model demands the highest possible levels of security.



Freedom

Alternative routing

When access to our servers is blocked, we can route connections through third-party networks that are unlikely to be blocked (such as AWS). Your data remains encrypted at all times.



Stealth protocol

As discussed above, this WireGuard TCP-based protocol was designed by Proton VPN to bypass censorship blocks.

Streaming (Plus)

Proton VPN is an excellent service for streaming, which is something we feel is something that is not always sufficiently appreciated. Using a combination advanced routing technologies, all paid Proton VPN users can now stream content reliably and hassle-free from almost 100 popular services worldwide — no matter where they are. The full list of supported services (at the time of writing this guide) is:

- 6Play (France)
- ABC.com (United States)
- ABC iview (Australia)
- Abema (Japan)
- Acorn TV (United States, Canada, Australia, New Zealand)
- aha (India)
- Amazon Prime Video (Australia, Canada, France, Germany, India, Italy, Switzerland, UK, Japan, United States)
- Apple TV+ (100+ countries worldwide)
- ARD (Germany)
- Arte (France, Germany)
- atresplayer (Spain)
- Audible US (United States)
- BBC iPlayer (United Kingdom)
- Blick TV (Switzerland)
- BritBox (United States, Canada)
- Canal+ (France, Switzerland)
- CBC (Canada)
- Channel 4 (United Kingdom)
- Channel 7 (Australia)
- Channel 9 (Australia)
- Crunchyroll (United States)
- CTV and CTV News (Canada)
- DAZN (Canada, Germany, Italy, Switzerland, United Kingdom, France, Norway, Spain)
- Deezer (over 180 countries)
- ESPN+ (United States)Eurosport Player (United Kingdom, Ireland, France)
- F1 TV (United States)
- France.tv (France)
- fuboTV (United States, Canada)
- ley (North Macedonia)
- Go3 (Lithuania)
- Hallmark+ (United States)
- hoichoi (India)
- Hulu (United States)
- ITVX (United Kingdom)
- Ivi (Russia)
- ioHotstar (India)
- Joyn (Germany)
- Kinopoisk (Russia)Kayo Sports (Australia)
- Max and HBO Max (many countries worldwide)
- Mediaset Infinity (Italy)
- MGM+ (United States)
- mitele (Spain)
- MLB.TV (United States)

- Moviestar Plus+ (Spain)
- MTV Katsomo and MTV Uutiset (Finland)
- MX Player (India)
- Netflix (25 counties worldwide)
- Network 10 (10 play) (Australia)
- NOW TV (United Kingdom, Italy)
- NRK (Norway)
- ORF-TV (Austria)
- Paramount+ (16 counties)
- Peacock (United States)
- Philo (United States)
- Pluto TV (United States)
- Pro7 (Germany)
- RAI (Italy)
- RTÉ Player (Ireland)
- RTBF Auvio (Belgium)
- RTL+ (TVNOW) (Germany, Austria, Switzerland, Liechtenstein, Luxembourg)
- RTVE Plus (Spain)
- Ruutu (Finland)
- Sat.1 (Germany)
- ServusTV (Austria)
- ShemarooMe (India)
- Sling TV (United States)
- SonyLiv (India)
- Spotify (almost everywhere)
- SRF (Switzerland)
- Sun NXT (India)
- SVT Play (Sweden)
- SyFy (United States)
- TF1 (France)
- TG4 (Ireland)
- ThreeNow (New Zealand)
- TV3 (Lithuania)
- TV4 Play (Sweden)
- TVNZ+ (New Zealand)
- TVer (Japan)
- Tubi (United States)
- Yle Areena (Finland)
- YouTube TV (United States)
- YuppTV (India)
- Vix (United States)
- Wavve (South Korea)

- Zattoo (Switzerland, Germany)
- ZEE5 (India)
- Ziggo Go (Netherlands)

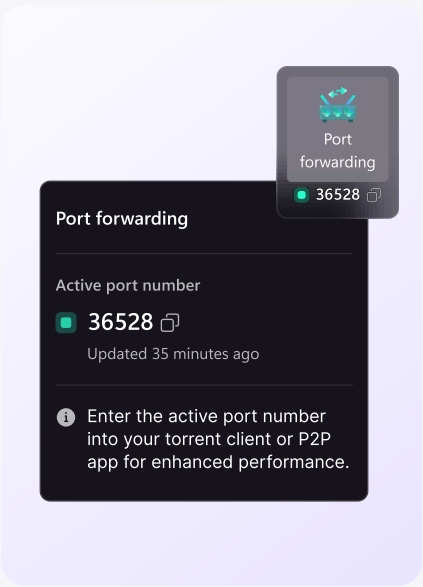
With our apps for Android TV, Fire OS ("firestick"), and tvOS (Apple TV), its easy to watch your favorite TV shows, movies, and sports events on your big screen TV. Our Android TV (and Fire OS) app now supports split tunneling, NetShield Ad-blocker, custom DNS, and LAN connections.

P2P servers + port forwarding (Plus)

We offer specially optimized P2P servers. We also support P2P users with port forwarding. ACurrently available on all desktop platforms (Windows, macOS (early access), and Linux) and coming soon to macOS, this feature routes connections through the NAT firewall Proton VPN uses to protect our customers so that P2P clients can accept incoming connections. This improves your upload (seeding) speed.

The BitTorrent protocol encourages file sharing by tying your download speed to your upload speed, so port forwarding can dramatically improve your P2P download speeds. Port forwarding also improves performance for online gamers.

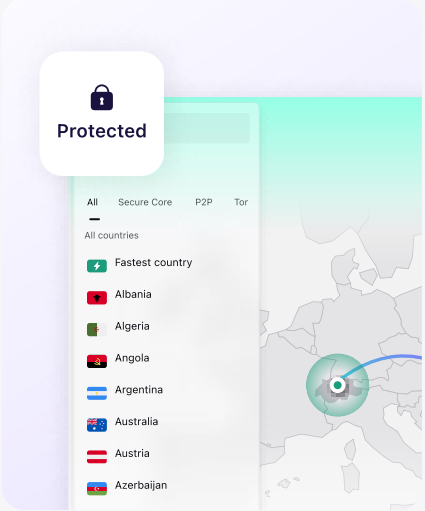
Note that Proton VPN implements port forwarding in a secure way that is not subject to the kind of abuse that has led other VPN services to discontinue the feature.



NAT type 2 (Plus)

Network address translation (NAT) maps the IP address of your device to an external IP address that can be accessed from the internet. NAT is typically performed on a router, but when using a VPN, it is performed on the VPN server so that traffic can pass through the firewall we use to protect our customers.

By default, NAT randomly maps the connection between the VPN server's IP address and the IP address of your device. This is known as NAT type 3 or strict NAT. It's good for privacy because it makes it more difficult to correlate traffic between the two devices, but the lack of a direct connection between you and other gamers can cause a variety of performance problems.



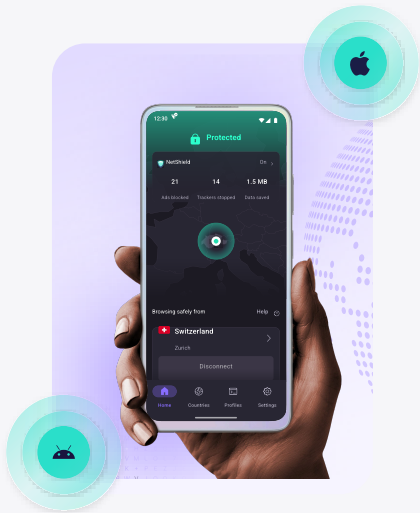
NAT type 2 (also known as moderate NAT) should be familiar to anyone with a game console. It turns off randomization of the mapping between the VPN server and your device. This slightly reduces your privacy but allows direct connections to be established with other users, thus eliminating the problems NAT type 3 can cause for online gamers. NAT type 2 is available on all our desktop and mobile apps.

Support for all major platforms

You can access Proton VPN from anywhere on any device. We have native apps for Windows, macOS, Linux, Linux CLI, Chromebook, Android, Android TV, iOS/iPadOS, and tvOS (Apple TV).

We also provide OpenVPN and WireGuard config files so you can manually configure Proton VPN on routers and third-party VPN apps. Manual configuration is also supported via a large number of support articles.

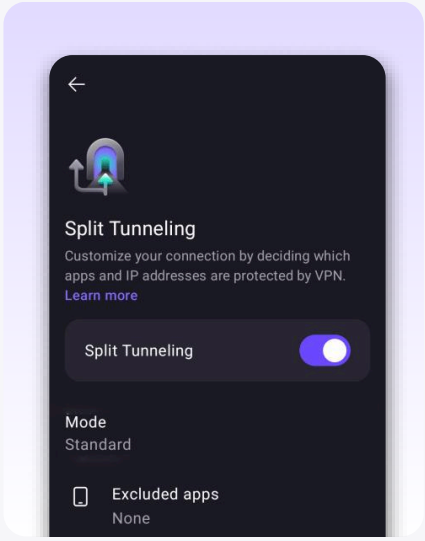
It's worth noting that we were one of the very first VPN services to launch a full GUI Linux app and are still one of the few services that support one. Our Linux app even supports features not yet available on all our apps, such as full IPv6 support, an advanced kill switch, and port forwarding. We also now offer a command-line (CLI) Linux tool.



Split tunneling (Plus)

Split tunneling allows you to choose which apps and IP addresses connect to the internet using the VPN tunnel and which bypass the encrypted tunnel. Common use cases include:

- You want to use a nearby VPN server for general privacy reasons, but exempt that one website that detects the VPN and won't let you log in.
- You want to secure your browsing history by connecting to a VPN server in another country, but you want want to appear as though you're in your country for certain services (such as local streaming services, your bank, or your government's online resources).
- To only use a VPN for specific uses (such as torrenting or when you connect to Netflix and wish to access a larger library than is available in your country).



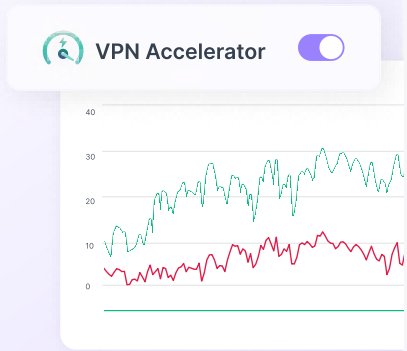
Split tunneling is currently available on Windows, macOS, Linux, Android, Android TV, and our browser extensions, and support for the feature is on our roadmap for IOS, and iPadOS.

VPN Accelerator

Unique to Proton VPN, this feature improves VPN connection stability and can increase VPN speeds by up to 400% over large distances. It addresses the problem of speed loss over large distances — the longer the distance, the more effective it is. Note that the 400% figure refers to how much faster your connection is when using VPN Accelerator than it would be if you were connected to the same VPN sever but not using VPN Accelerator.

For example: You live in New Zealand and have a 100 Mbs internet connection. When connecting to a VPN server in New Zealand, you might get speeds of 90+ Mbs, but when you connect to a VPN server in Europe, your connection speed drops to 10 Mbs due to the distance your data must travel. With VPN Accelerator, you might be able to connect to the same server in Europe at 40 Mbs.

Learn more about how VPN Accelerator works >



Custom DNS (Plus)

By default, Proton VPN handles your DNS queries and can filter them for malware, ads, and trackers with our NetShield Ad-blocker tool. With Custom DNS, you can use a third-party DNS resolver instead. This allows you to use dedicated DNS services that offer advanced DNS filtering features not available with NetShield, such as child safety ("net nanny") protection and customized blocklists.

Custom DNS is now available on all our apps (excluding Apple TV and our browser extensions).

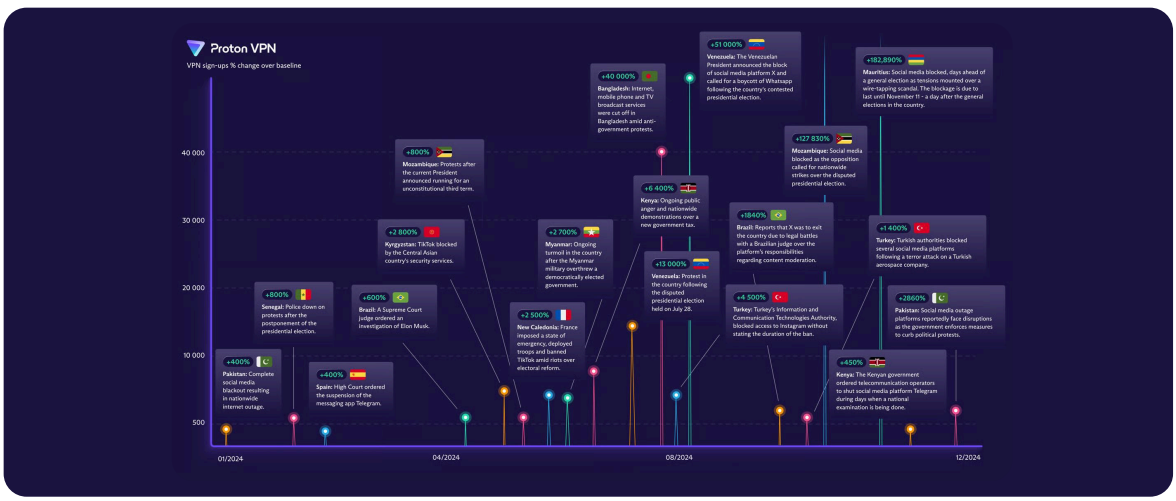
We're always working to find ways to make our apps even better with under-the-hood improvements, new features, and other enhancements to make them easy and enjoyable to use.For the latest updates and new features across all supported platforms, please see the Proton VPN release notes.

Proton VPN's unique initiatives

Proton VPN's Observatory

VPNs are essential tools to combat internet censorship. At Proton VPN, we regularly see signups spike following major geopolitical events around the world, be they protests, contested elections, or government crackdowns.

To see how people worldwide fight internet censorship, we've begun documenting all significant spikes in Proton VPN usage in response to internet shutdowns, censorship, and protests.



2024 election campaign

2024 was the biggest year for democracy in history, and around 50% of the global population went to the polls. Unfortunately, many of the countries that held elections that year have a history of undermining democratic practices and endangering fundamental human rights.

In addition to our usual work to protect free speech around the world, in 2024, Proton VPN provided free servers in 21 countries that held elections and have a history of censorship or election tampering, allowing the local population to bypass any potential government censorship and misinformation.