Task 8: Identify and Remove Suspicious Browser Extensions

Objective: Understand the role of VPNs in protecting privacy and secure communication.

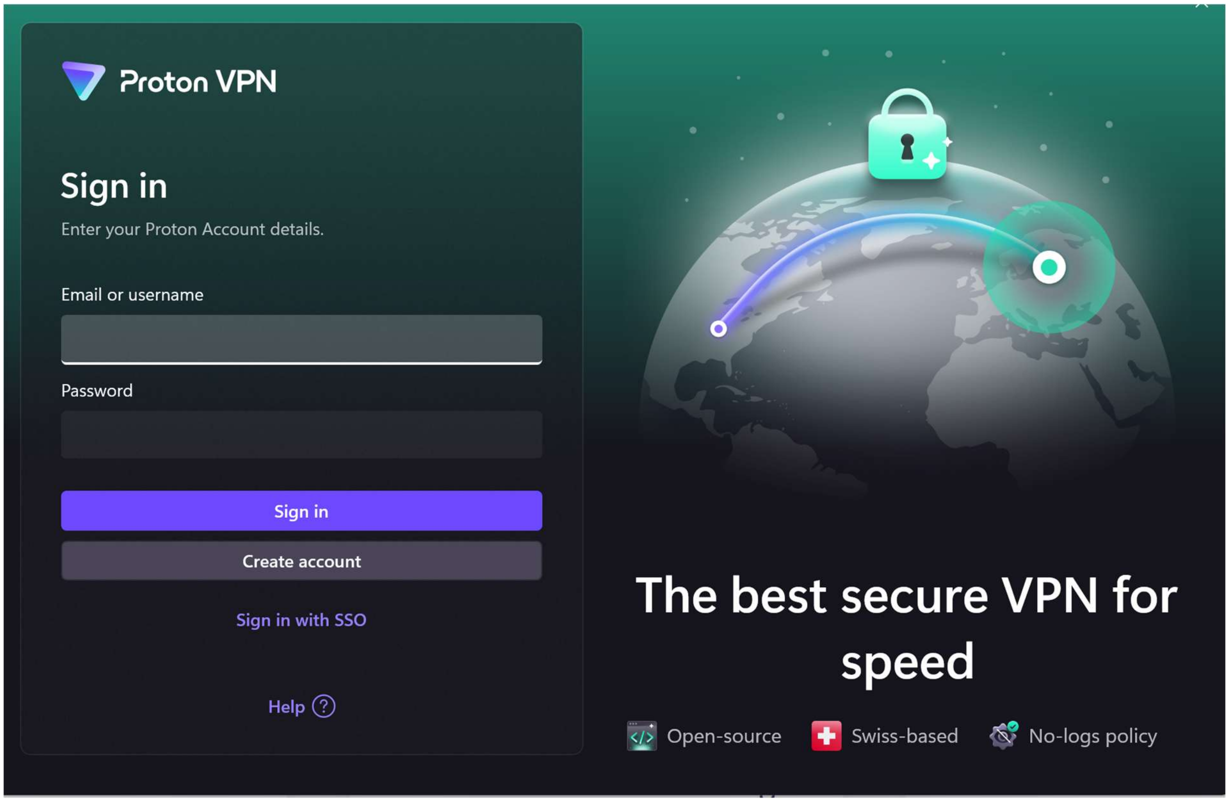
VPN: Virtual Private Network

A **VPN (Virtual Private Network)** is a technology that **creates a secure, encrypted connection** between your device (like a phone or laptop) and the internet.

Report describing VPN setup steps and connection status screenshot.

PROTON VPN

SIGN IN TO PROTON VPN



Proton VPN

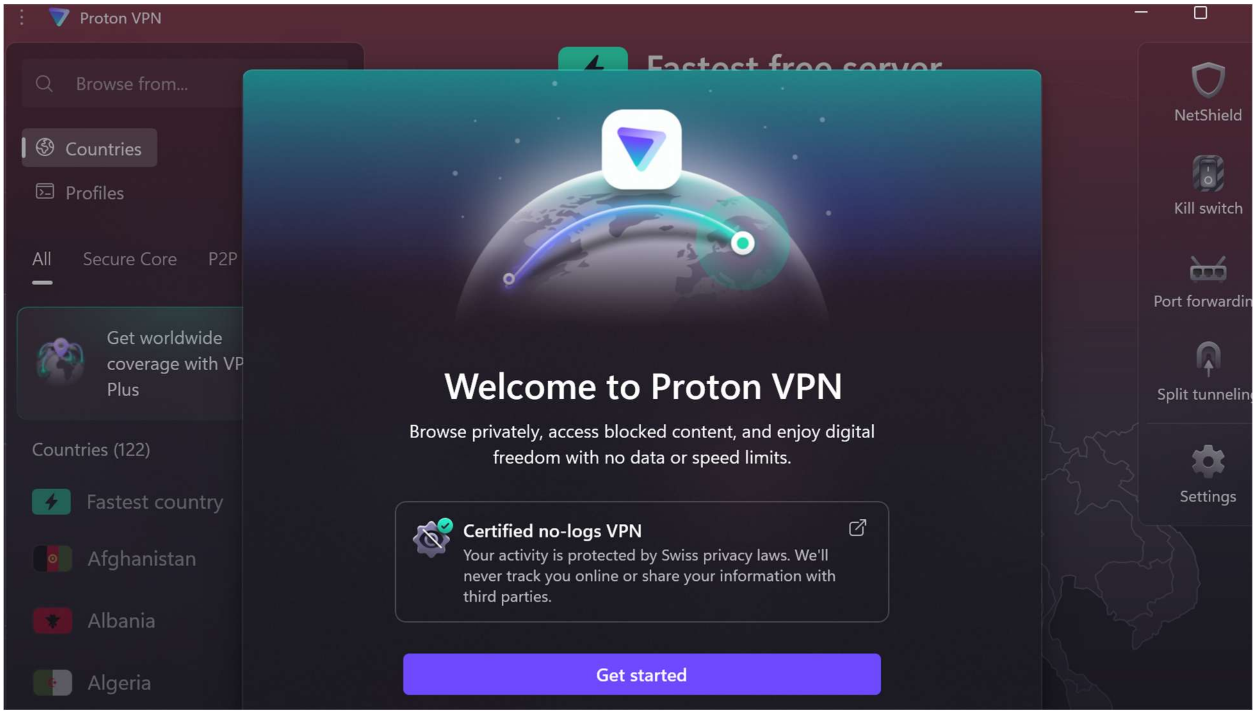
Sign in

Enter your Proton Account details.

Email or username

Password

GET STARTED



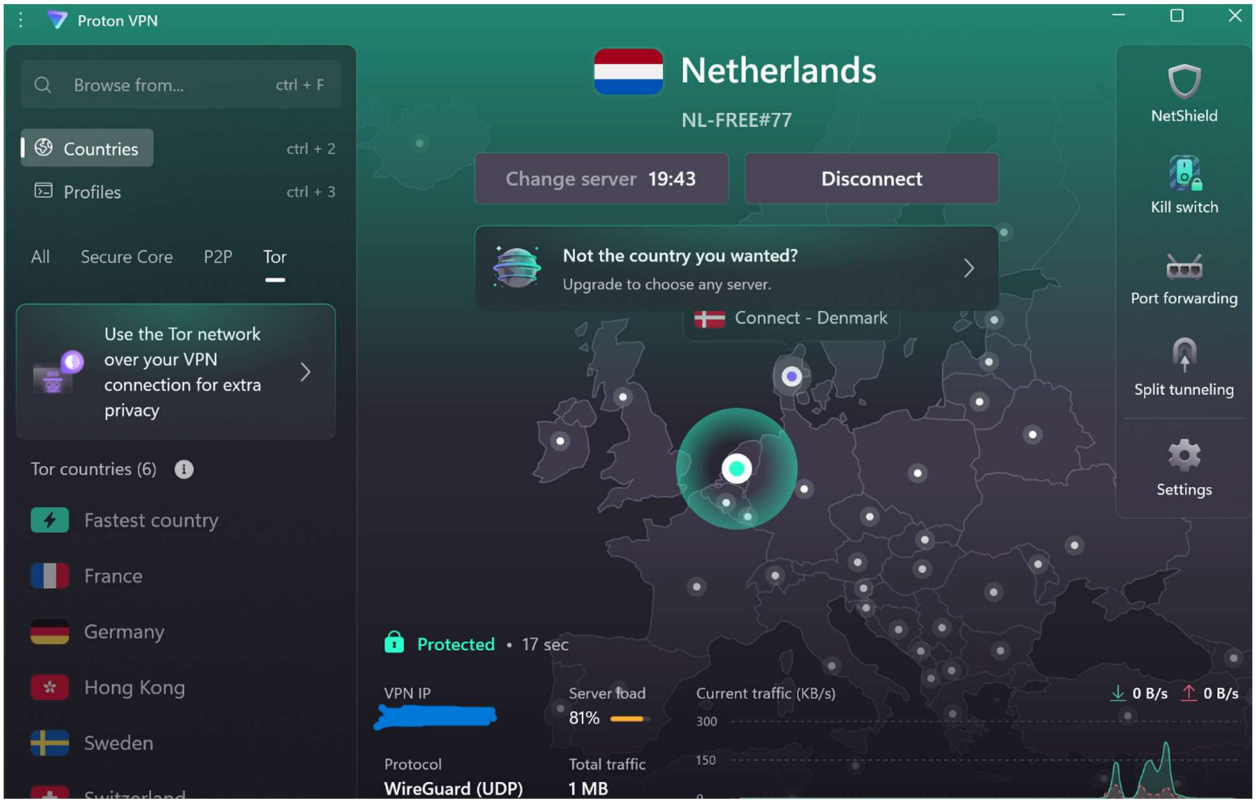
Welcome to Proton VPN

Browse privately, access blocked content, and enjoy digital freedom with no data or speed limits.

Certified no-logs VPN

Your activity is protected by Swiss privacy laws. We'll never track you online or share your information with third parties.

Connect



Use the Tor network over your VPN connection for extra privacy

Tor countries (6)

Not the country you wanted?
Upgrade to choose any server.

Protected • 17 sec

VPN IP [redacted]

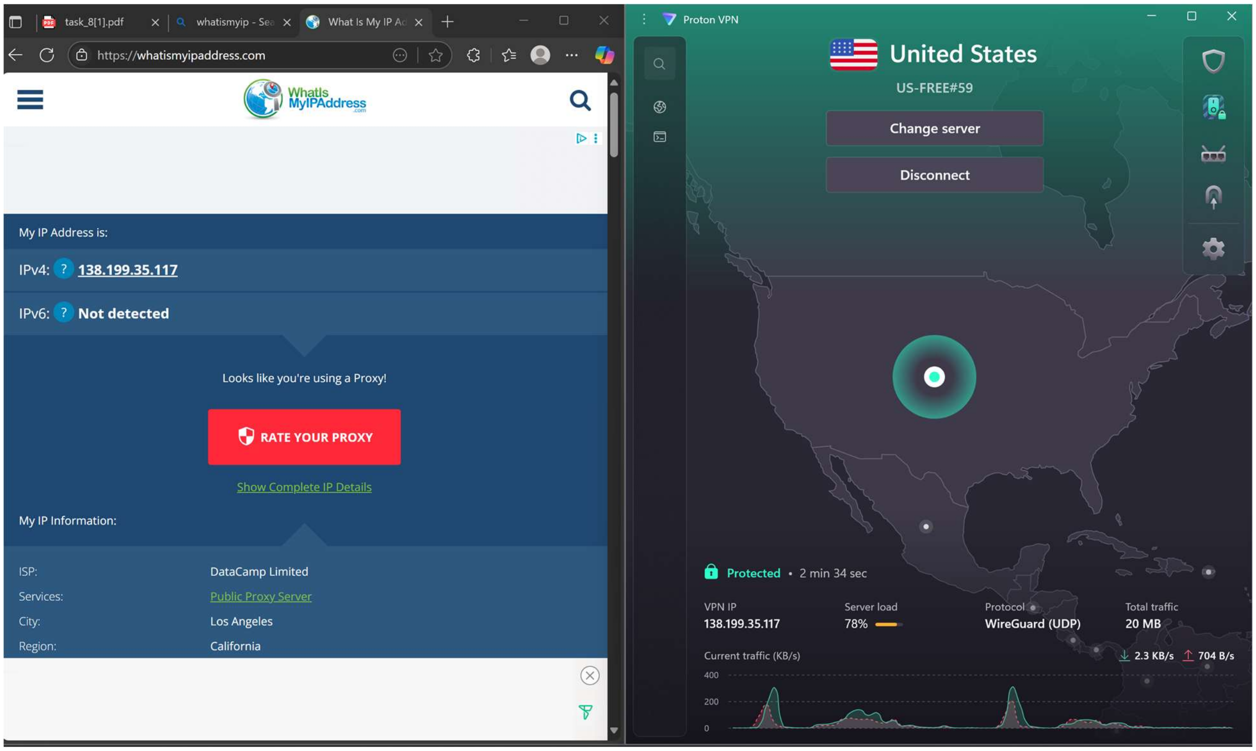
Server load 81%

Current traffic (KB/s) ↓ 0 B/s ↑ 0 B/s

Protocol WireGuard (UDP)

Total traffic 1 MB

When I changed my server, it shows my vpn IP, not my system IP on whatismyipaddress.com



My IP Address is:

IPv4: ? 138.199.35.117

IPv6: ? Not detected

Looks like you're using a Proxy!

RATE YOUR PROXY

Show Complete IP Details

My IP Information:

ISP:	DataCamp Limited
Services:	Public Proxy Server
City:	Los Angeles
Region:	California

United States

US-FREE#59

Protected • 2 min 34 sec

VPN IP	Server load	Protocol	Total traffic
138.199.35.117	78%	WireGuard (UDP)	20 MB

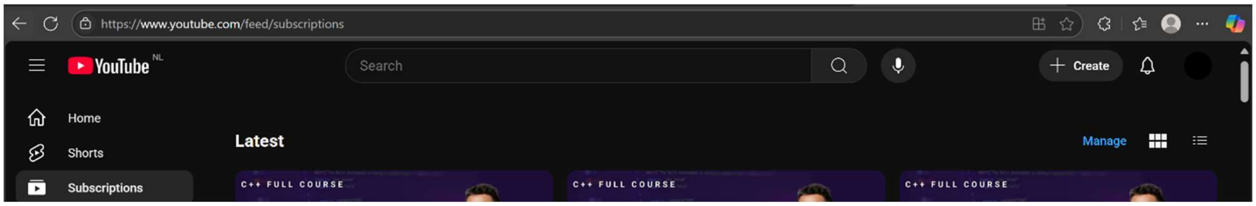
Current traffic (KB/s) ↓ 2.3 KB/s ↑ 704 B/s

A website is browsed, and confirms that traffic is encrypted

This shows that your internet traffic is now encrypted and flowing through the VPN.

Look at the **address bar**:

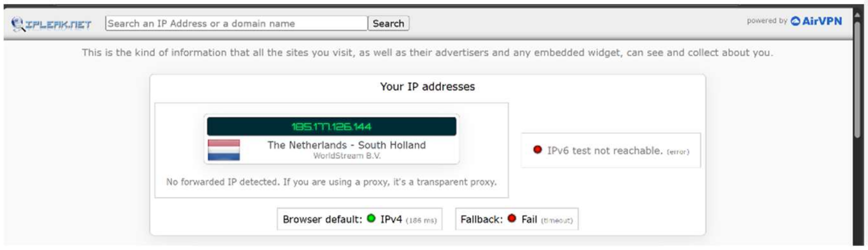
- You should see a **padlock icon** to the left of the web address.
- This confirms the site uses **HTTPS**, meaning **data between you and the site is encrypted**.



Confirm VPN Encryption in Action on https://ipleak.net

If the IP shown is **different from your real IP** and **matches the VPN server location**, you're secure.

Hence, my system is now secure.



This is the kind of information that all the sites you visit, as well as their advertisers and any embedded widget, can see and collect about you.

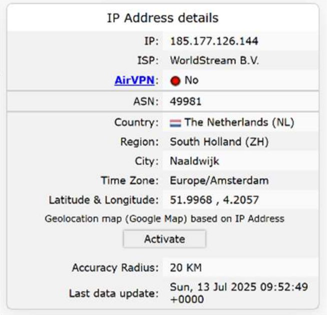
Your IP addresses

185.177.126.144
The Netherlands - South Holland
WorldStream B.V.

No forwarded IP detected. If you are using a proxy, it's a transparent proxy.

● IPv6 test not reachable. (error)

Browser default: ● IPv4 (186 ms) Fallback: ● Fail (timeout)


IP Address details

IP:	185.177.126.144
ISP:	WorldStream B.V.
AirVPN:	● No
ASN:	49981
Country:	The Netherlands (NL)
Region:	South Holland (ZH)
City:	Naaldwijk
Time Zone:	Europe/Amsterdam
Latitude & Longitude:	51.9968 , 4.2057

Geolocation map (Google Map) based on IP Address

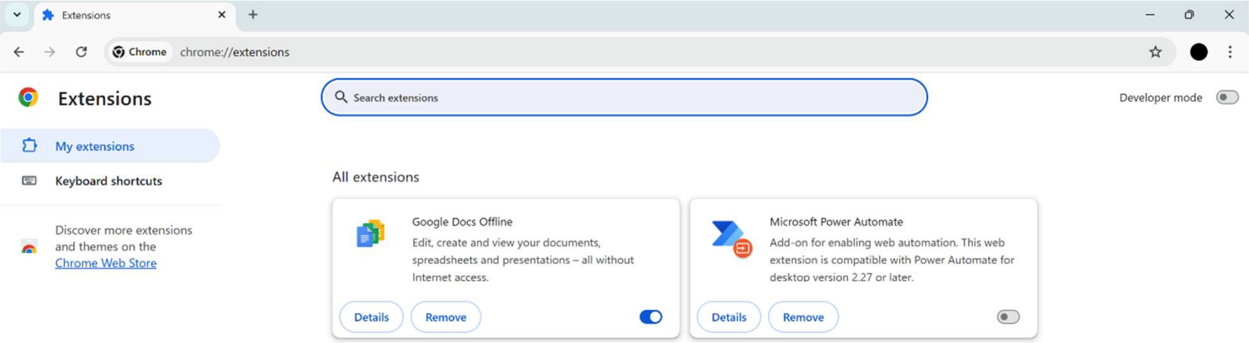
Accuracy Radius:	20 KM
Last data update:	Sun, 13 Jul 2025 09:52:49 +0000

Removing Suspicious Browser Extensions

Look for:

- Unknown or untrusted extensions
- Anything you don't remember installing

Click **Remove** next to each one.



Discover more extensions and themes on the Chrome Web Store

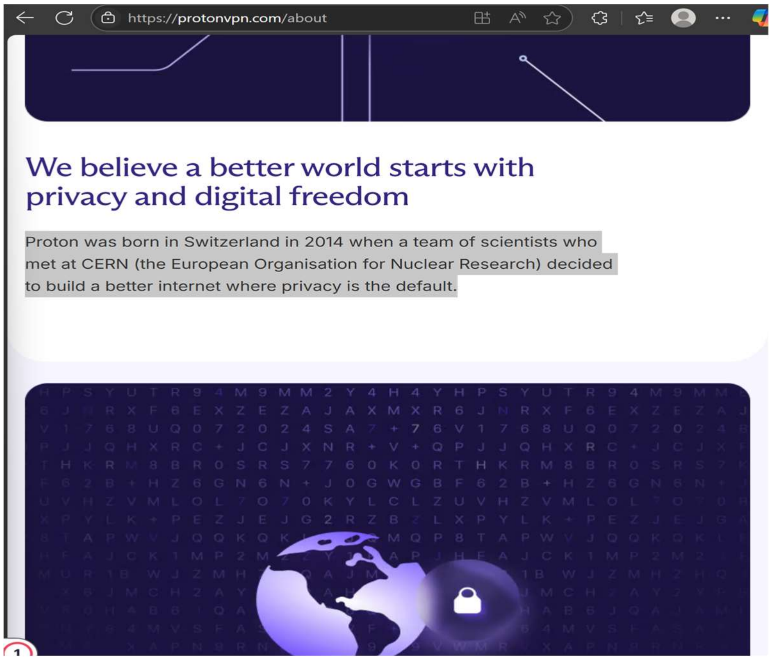
All extensions

Google Docs Offline
Edit, create and view your documents, spreadsheets and presentations – all without Internet access.

Microsoft Power Automate
Add-on for enabling web automation. This web extension is compatible with Power Automate for desktop version 2.27 or later.

Research

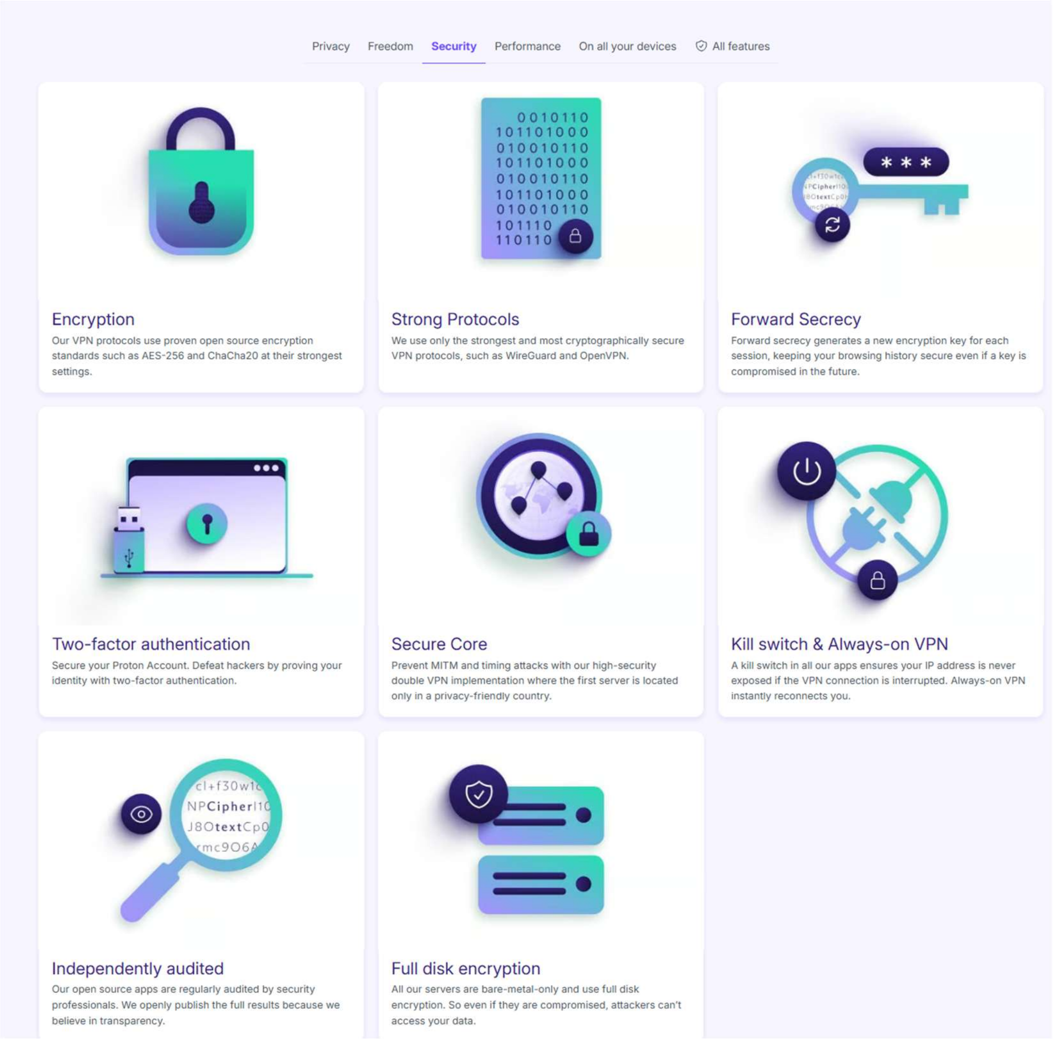
Proton was born in Switzerland in 2014 when a team of scientists who met at CERN (the European Organization for Nuclear Research) decided to build a better internet where privacy is the default.



We believe a better world starts with privacy and digital freedom

Proton was born in Switzerland in 2014 when a team of scientists who met at CERN (the European Organisation for Nuclear Research) decided to build a better internet where privacy is the default.

Encryption used: Proton VPN uses AES-256 and ChaCha20 encryption



Encryption

Our VPN protocols use proven open source encryption standards such as AES-256 and ChaCha20 at their strongest settings.

Strong Protocols

We use only the strongest and most cryptographically secure VPN protocols, such as WireGuard and OpenVPN.

Forward Secrecy

Forward secrecy generates a new encryption key for each session, keeping your browsing history secure even if a key is compromised in the future.

Two-factor authentication

Secure your Proton Account. Defeat hackers by proving your identity with two-factor authentication.

Secure Core

Prevent MITM and timing attacks with our high-security double VPN implementation where the first server is located only in a privacy-friendly country.

Kill switch & Always-on VPN

A kill switch in all our apps ensures your IP address is never exposed if the VPN connection is interrupted. Always-on VPN instantly reconnects you.

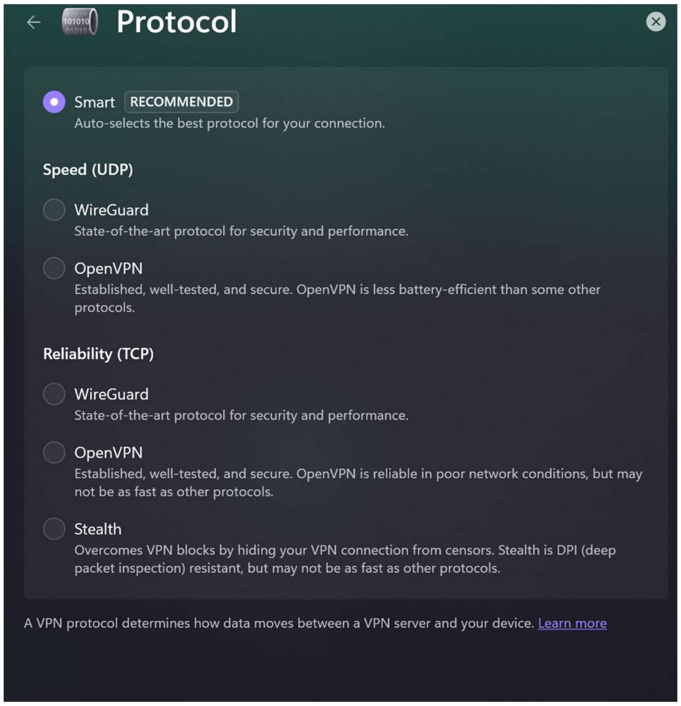
Independently audited

Our open source apps are regularly audited by security professionals. We openly publish the full results because we believe in transparency.

Full disk encryption

All our servers are bare-metal-only and use full disk encryption. So even if they are compromised, attackers can't access your data.

Protocols used: OpenVPN and WireGuard.



Protocol

● Smart RECOMMENDED
Auto-selects the best protocol for your connection.

Speed (UDP)

○ WireGuard
State-of-the-art protocol for security and performance.

○ OpenVPN
Established, well-tested, and secure. OpenVPN is less battery-efficient than some other protocols.

Reliability (TCP)

○ WireGuard
State-of-the-art protocol for security and performance.

○ OpenVPN
Established, well-tested, and secure. OpenVPN is reliable in poor network conditions, but may not be as fast as other protocols.

○ Stealth
Overcomes VPN blocks by hiding your VPN connection from censors. Stealth is DPI (deep packet inspection) resistant, but may not be as fast as other protocols.

A VPN protocol determines how data moves between a VPN server and your device. Learn more

Switch to proton VPN privacy.

It has features like:

mask your IP

swiss privacy

No-logs policy

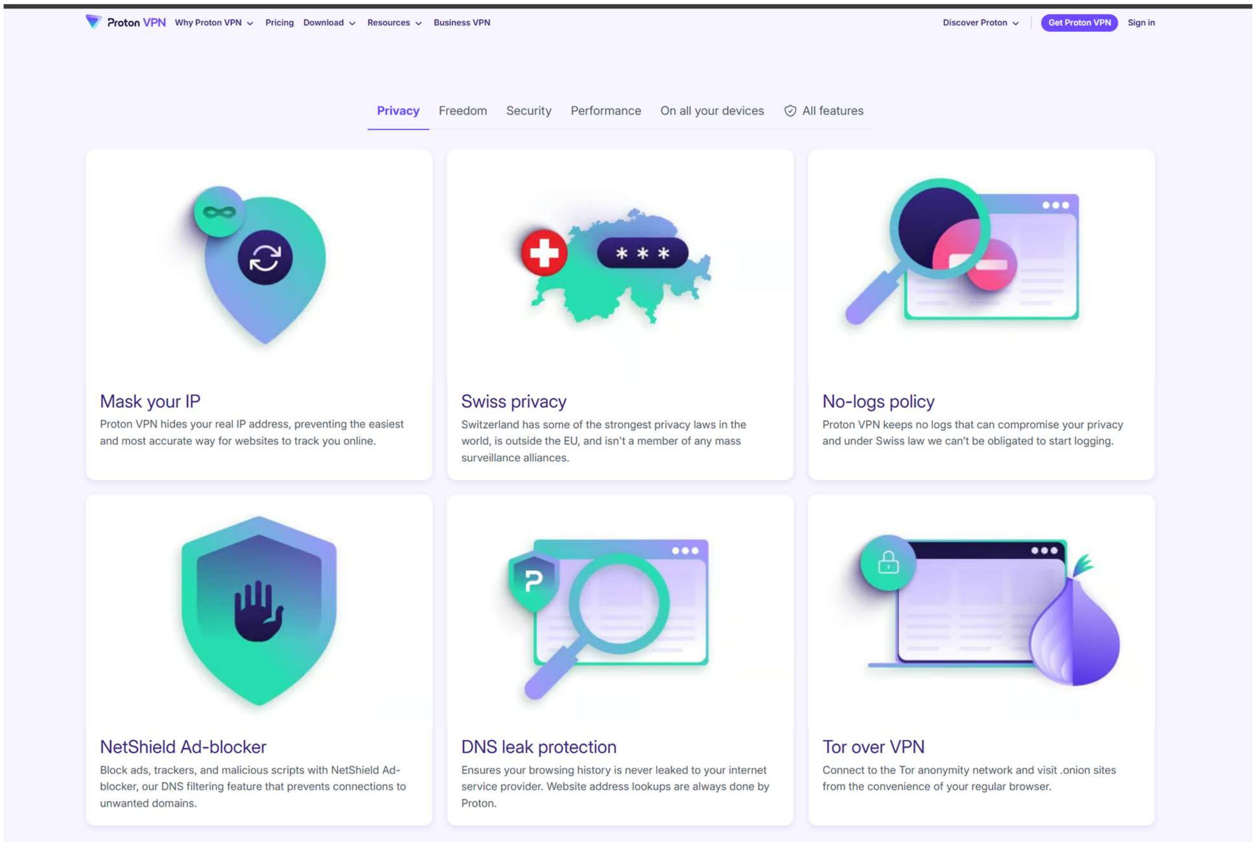
NetShield Ad-blocker

DNS leak protection

Tor over VPN

kill switch

split tunneling



Mask your IP

Proton VPN hides your real IP address, preventing the easiest and most accurate way for websites to track you online.

Swiss privacy

Switzerland has some of the strongest privacy laws in the world, is outside the EU, and isn't a member of any mass surveillance alliances.

No-logs policy

Proton VPN keeps no logs that can compromise your privacy and under Swiss law we can't be obligated to start logging.

NetShield Ad-blocker

Block ads, trackers, and malicious scripts with NetShield Ad-blocker, our DNS filtering feature that prevents connections to unwanted domains.

DNS leak protection

Ensures your browsing history is never leaked to your internet service provider. Website address lookups are always done by Proton.

Tor over VPN

Connect to the Tor anonymity network and visit .onion sites from the convenience of your regular browser.

VPN BENEFITS AND LIMITATIONS:

Benefits of VPN

1. Encrypts Internet Traffic

- VPNs encrypt your data (usually with AES-256) so third parties — like ISPs, hackers, or government agencies — can't see what you're doing online.
- Especially helpful when using public Wi-Fi (airports, cafes, hotels).

2. Hides Your IP Address and Location

- VPN replaces your IP with the IP of the VPN server.
- Helps in masking your geographical location and identity.

3. Bypasses Geo-Restrictions and Censorship

- Allows access to content blocked in your country (e.g., Netflix US from India, or WhatsApp in the UAE).
- Helps users in restrictive regions access free internet.

4. Protects Against Tracking

- Prevents websites, apps, and advertisers from tracking your real IP.

- Makes ad tracking and fingerprinting harder.

5. Safe File Sharing and Remote Work

- Enables secure connection to your company's internal systems.
- Ideal for businesses and remote workers handling sensitive information.

6. Prevents Bandwidth Throttling

- Some ISPs slow down speeds for streaming or gaming — VPNs hide your activity, reducing throttling.

7. Avoids DNS and IP Leaks

- Good VPNs use private DNS servers and leak protection to ensure your traffic doesn't escape the VPN tunnel.

8. Can Help Save Money

- Prices for flights, hotels, or digital products can vary by region — using VPN servers from cheaper regions may offer better deals.

9. Multi-Device Protection

- Most VPN services support multiple devices: PCs, phones, tablets, routers, etc.

Limitations of VPN

1. Slower Internet Speeds

- Due to encryption and rerouting of traffic, your browsing or download speed can drop, especially on free VPNs or distant servers.

2. No Absolute Anonymity

- VPNs don't make you anonymous — they only mask your IP.
- Your VPN provider can see your activity if they keep logs (use no-log services like ProtonVPN or Mullvad).

3. Doesn't Protect Against Malware or Phishing

- VPNs don't block viruses, trojans, or malicious websites.
- You still need an antivirus and a secure browser.

4. Some Services Block VPNs

- Streaming services, banks, and some websites detect and block VPN traffic.
- You may get CAPTCHA errors or be denied access.

5. Legal or Policy Issues

- In some countries (e.g., China, Iran, UAE), VPN use is restricted or illegal.
- Always check local laws before using one.

6. Free VPNs Can Be Risky

- Many free VPNs sell your data, inject ads, or provide weak encryption.
- Choose reputable free VPNs like ProtonVPN Free, Windscribe, or TunnelBear.

7. Device Compatibility and App Limits

- Some older routers, smart TVs, or IoT devices don’t support VPNs without manual configuration.

8. No Protection If VPN Drops

- If the VPN disconnects suddenly, traffic could leak unless a kill switch is enabled.