#### **Step by step Process of how to connect with Vpn**

#### **1. Choose a Reputable Free VPN Service**

* **ProtonVPN** (Free version):  
  + Based in Switzerland (strong privacy laws).
  + No data logging.
  + Offers decent speed and strong encryption even on the free plan.

#### **2. Download and Install the VPN Client**

* Go to<https://protonvpn.com>
* Sign up for a free account.
* Download the client for your OS (Windows/macOS/Linux/mobile).
* Install and log in.

#### **3. Connect to a VPN Server**

* Open the VPN app.
* Choose a free server location (e.g., Netherlands, USA, Japan).
* Click “Connect.”

#### **4. Verify IP Address Change**

* Visit<https://whatismyipaddress.com>
* Confirm your IP now reflects the VPN server's location (not your actual one).

#### **5. Browse a Website to Confirm Encrypted Traffic**

* Visit any secure site (like<https://www.bbc.com> or<https://duckduckgo.com>).
* The VPN encrypts your data before it leaves your device, protecting it from ISP tracking or local network snooping.

#### **6. Disconnect VPN and Compare**

* Disconnect from ProtonVPN.
* Refresh<https://whatismyipaddress.com> — your IP should return to normal.
* Notice any differences in browsing speed and latency.

**7**. **VPN Encryption and Privacy Features (ProtonVPN)**

Encryption Protocols and Standards

* OpenVPN: Uses AES-256 encryption, widely regarded as the gold standard for VPN security. It leverages the OpenSSL library, supporting a variety of encryption algorithms, and is highly customizable and secure.
* WireGuard: Employs the ChaCha20 cipher for encryption and Poly1305 for authentication. It is lightweight, fast, and secure, with a smaller codebase that reduces the attack surface, making it easier to audit. However, it is newer and still undergoing development and review.
* IKEv2/IPSec: Supports AES encryption and is known for its stability and ability to maintain connections when switching networks. However, there are concerns about potential vulnerabilities, especially due to its association with IPSec, which has been scrutinized for possible backdoors.
* SSTP: Uses AES-256 encryption and is primarily supported on Windows. Its proprietary nature and Microsoft’s involvement raise some privacy concerns.
* PPTP: Relies on MPPE encryption, which is outdated and insecure. PPTP is not recommended for privacy-sensitive use due to known vulnerabilities.

Privacy Features

* Data Encryption: All reputable VPNs encrypt user traffic, making it unreadable to ISPs, hackers, or anyone intercepting the data.
* Authentication: VPNs use various authentication methods (passwords, certificates, pre-shared keys, public key cryptography) to ensure only authorized users can connect. OpenVPN is especially flexible, while WireGuard uses public key cryptography for added security.
* Anonymity: By masking the user’s IP address and routing traffic through remote servers, VPNs help anonymize browsing activity.
* Resistance to Attacks: Modern protocols like OpenVPN and WireGuard are resistant to brute-force and timing attacks, especially when using robust ciphers like AES-256 and ChaCha20

# **8.summary on VPN benefits and limitations**

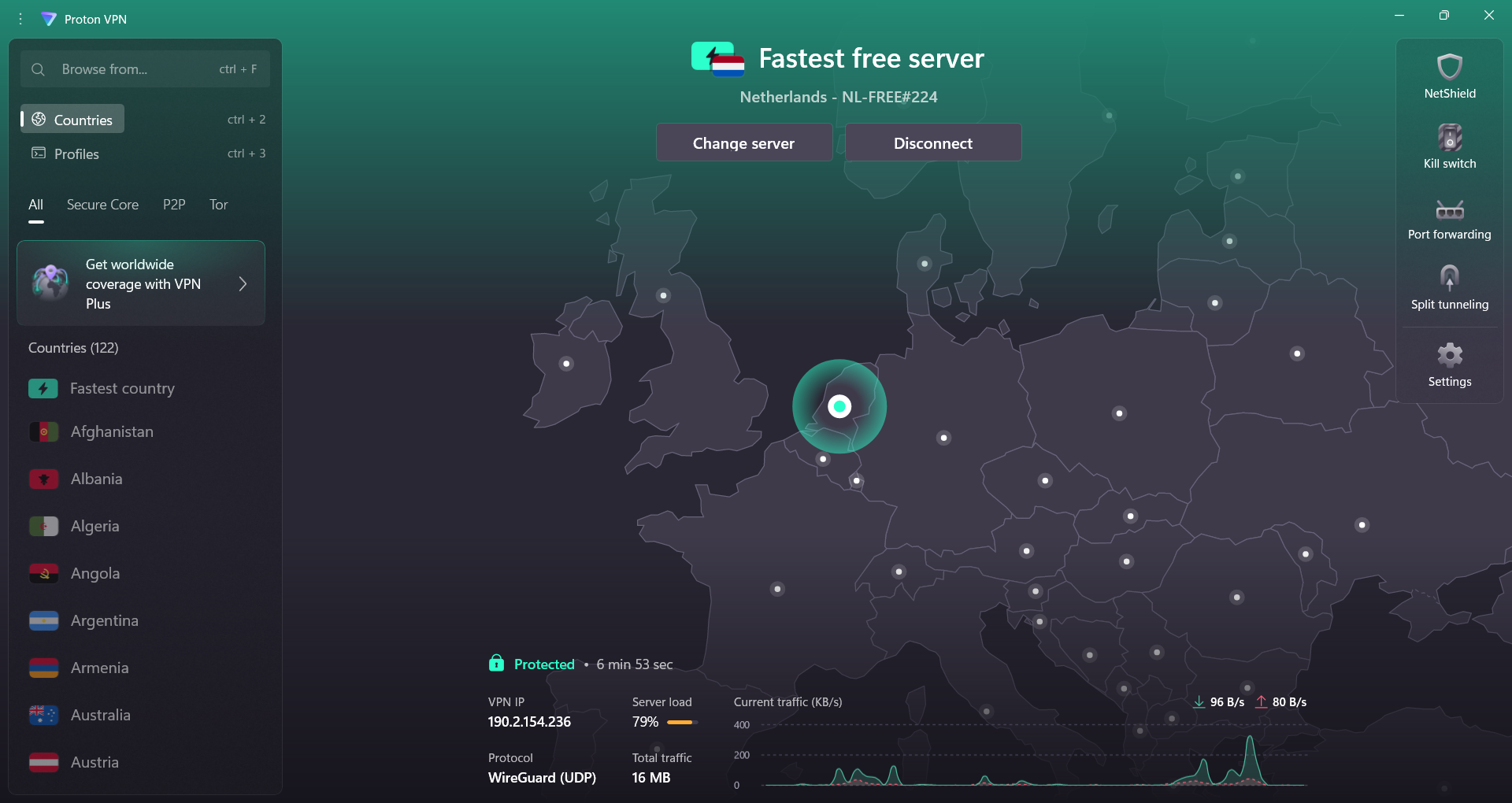
Key Benefits:

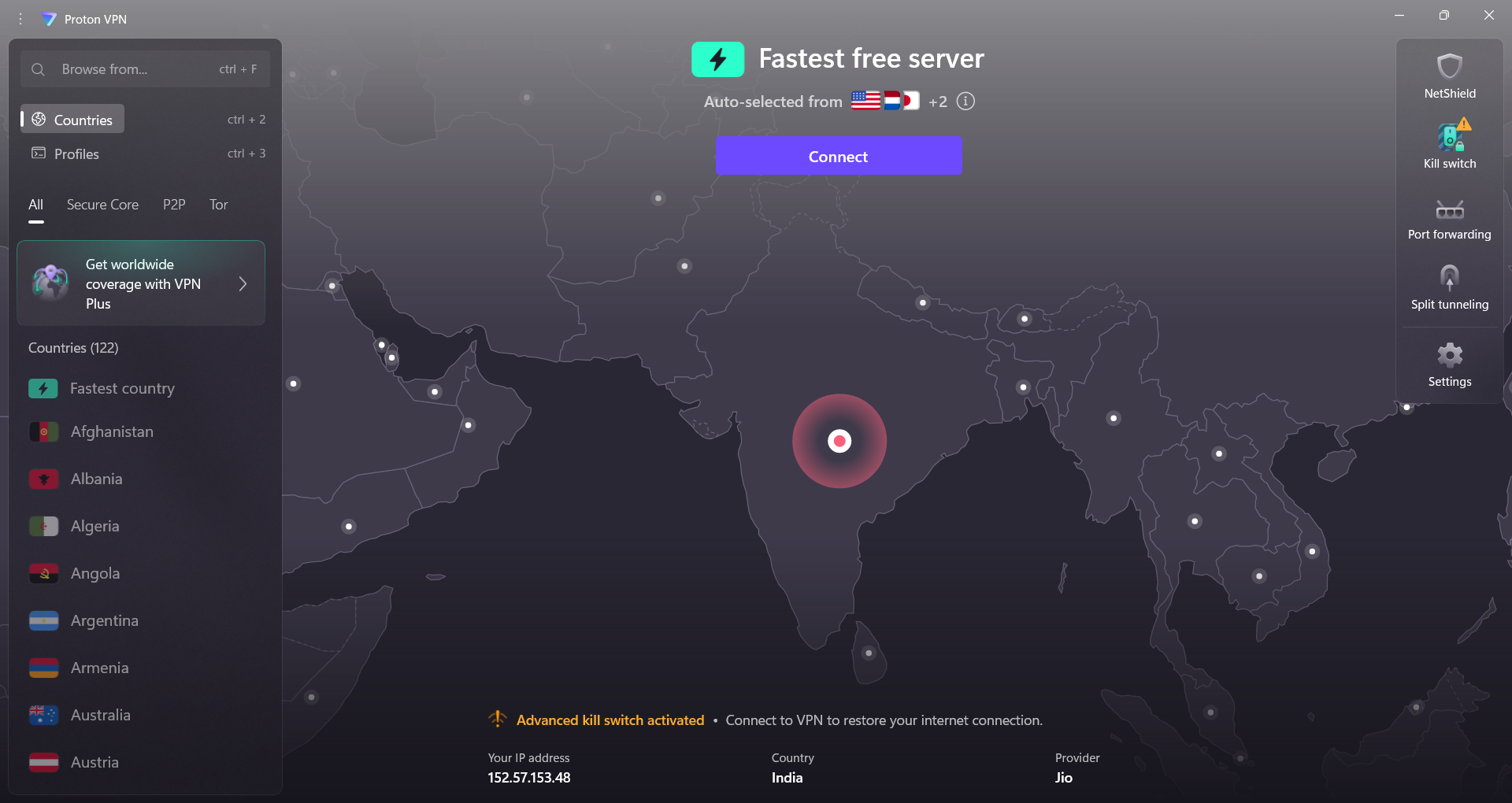
* Enhanced Security: VPNs encrypt your internet traffic, protecting your data from hackers, especially on public Wi-Fi networks.
* Improved Privacy: By masking your IP address, VPNs make it harder for websites, advertisers, and ISPs to track your online activities.
* Bypass Geo-Restrictions: VPNs allow access to region-locked or censored content by routing your connection through servers in other countries.
* Protection Against Bandwidth Throttling: VPNs can prevent ISPs from slowing down your connection based on your activities, such as streaming or gaming.
* Secure Remote Work: VPNs provide a secure way for employees to access company resources from remote locations.

Main Limitations:

* Reduced Internet Speed: Encryption and rerouting traffic through VPN servers can slow down your connection, though premium VPNs minimize this effect.
* Device Compatibility Issues: Not all devices and apps support VPNs natively, which can limit protection on certain platforms.
* Quality and Trust Issues with Free VPNs: Free VPNs may be insecure, collect user data, show ads, or offer poor performance.
* Legal and Policy Restrictions: VPN use is banned or restricted in some countries, and using a VPN to break service terms can still result in penalties

**Results:**

****

****