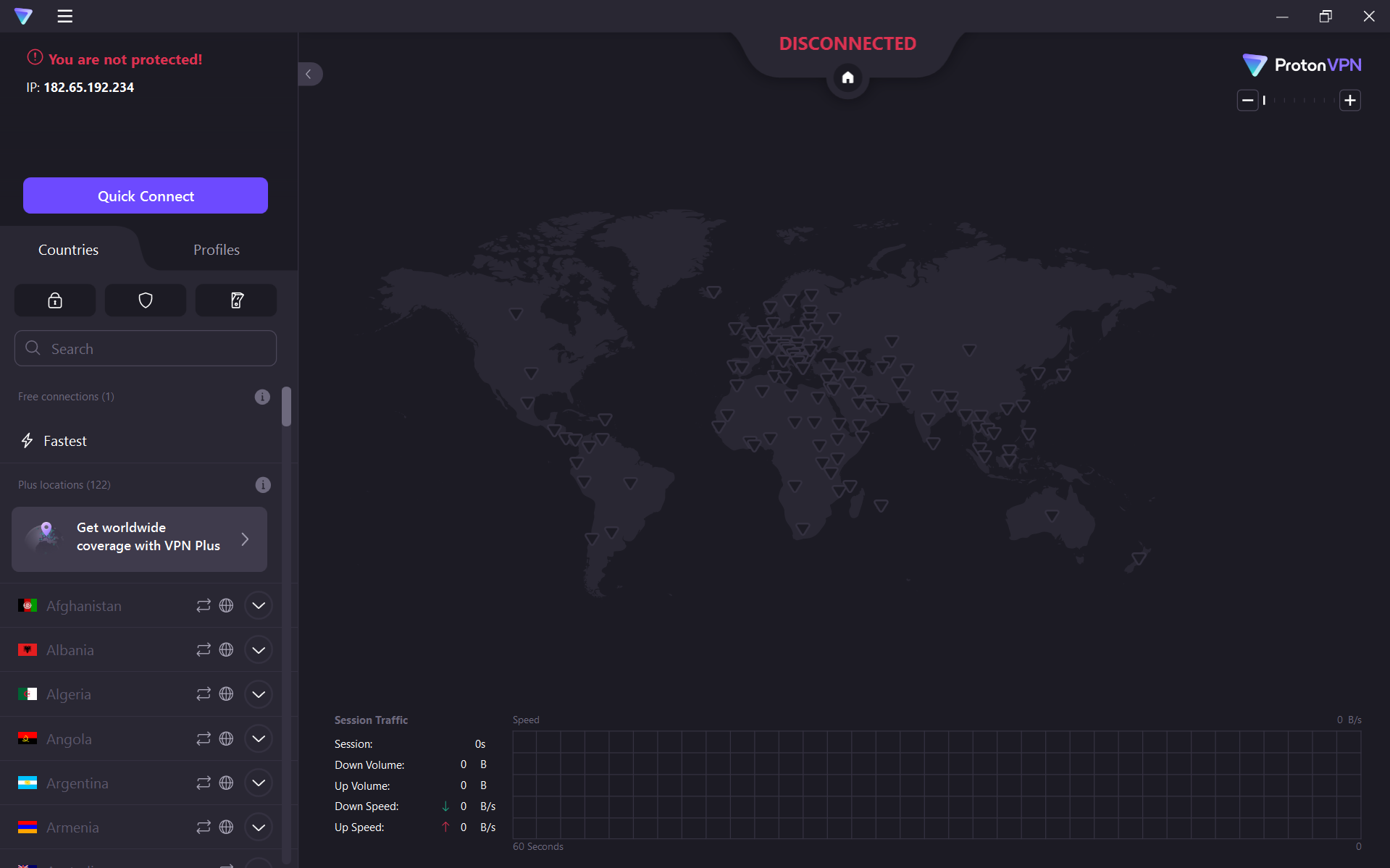
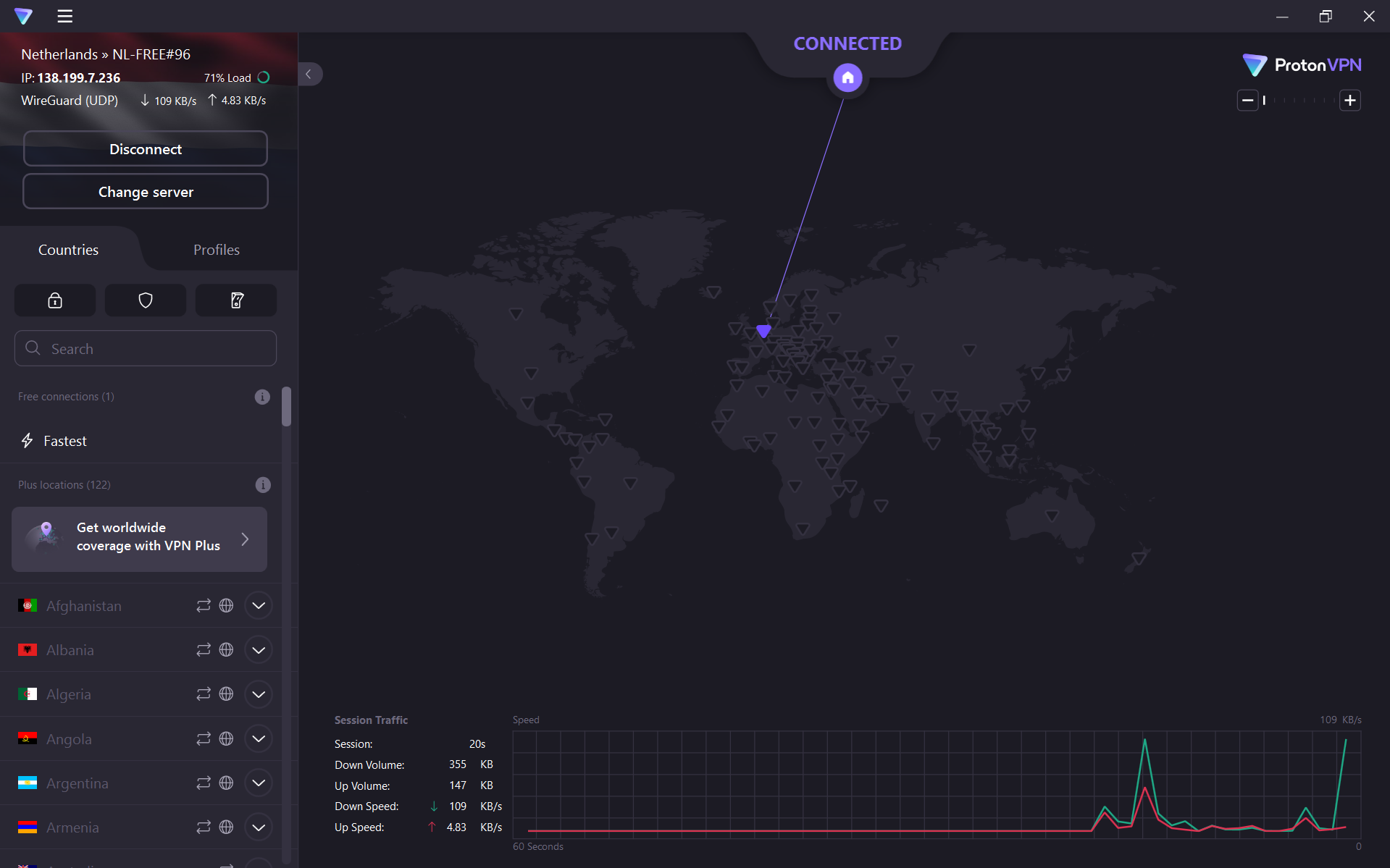
**TASK 8: Understand the role of VPNs in protecting privacy and secure communication.**

1. Choose a reputable free VPN service and sign up.
2. Download and install VPN client.

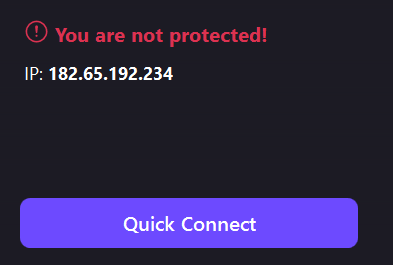


1. Connect to a vpn server.

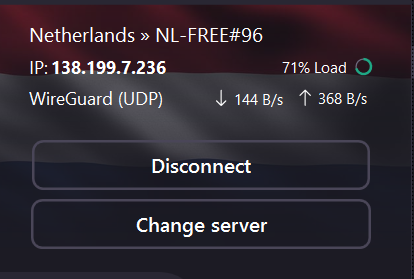


1. Verify your IP address has changed.

Previous IP:



New IP after connecting VPN:



1. Browse a website to confirm the traffic is encrypted.
2. Disconnect VPN and compare browsing speed and IP.

I tried browsing with and without VPN, the speed varies.

When VPN was connected, the speed seems a bit lower than the usual speed. After disconnecting VPN, the speed was normal.

1. Research VPN encryption and privacy features.

* Data encryption
* Perfect forward secrecy
* Kill switch
* Split tunneling
* No-logs policy
* IP & DNS leak protection
* Obfuscation
* Multi-hop vpn

1. Summary:

A Virtual Private Network (VPN) enhances both encryption and privacy by creating a secure, encrypted tunnel for your internet traffic. It uses strong encryption protocols like OpenVPN, WireGuard, or IKEv2/IPSec, with advanced ciphers such as AES-256 or ChaCha20 to protect data from eavesdropping. Features like Perfect Forward Secrecy ensure that even if one session key is compromised, past and future sessions remain secure. Privacy is further reinforced through strict no-logs policies, which prevent VPN providers from storing user data, and through IP/DNS leak protection that hides your real identity. Additional features like kill switches stop data leaks when the VPN disconnects, while split tunnelling allows selected apps to bypass the VPN. Obfuscation modes help users bypass VPN blocks in restrictive countries, and advanced options like multi-hop connections and Tor over VPN provide even deeper anonymity. Together, these features make VPNs essential tools for maintaining online privacy and protecting sensitive information from surveillance and cyber threats.