Task-8

Working and understanding VPN

Official Report: Comprehensive Analysis of VPN Functionality, Encryption, and Privacy Features

1. Executive Summary

This report provides an in-depth analysis of Virtual Private Network (VPN) technology, focusing on its operational mechanisms, encryption standards, and privacy-enhancing features. The findings are based on observed data from user screenshots, demonstrating VPN usage, IP masking, and geolocation spoofing. Additionally, the report evaluates encryption protocols, potential vulnerabilities, and best practices for secure VPN deployment.

2. Methodology

- **Data Sources:** User-provided screenshots depicting VPN usage scenarios.
- **Tools:** Public IP detection services (e.g., WhatIsMyIPAddress.com).
- **Research:** Analysis of industry-standard VPN encryption and privacy policies.

3. Key Findings

3.1 VPN Operational Overview

- **IP Address Masking:**
  - Screenshot 1 shows an IPv4 address (185.107.56.135) linked to a Netherlands-based VPN server (NForce Entertainment B.V.).
  - Screenshot 4 reveals the user's actual IP (45.112.32.36) in Hyderabad, India, when the VPN is inactive

- **Server Selection:**
  - Users can manually choose VPN servers from multiple countries (e.g., Japan, Netherlands, U.S.).
  - Auto-selection features optimize for speed or location (Screenshot 3).

3.2 VPN Detection and Anonymity

- Detection: Services like WhatIsMyIPAddress.com flag VPN usage (Screenshot 2: *"Looks like you're using a VPN!"*).
- Exposure Risk: Without a VPN, the user's ISP (Vision Broadband) and physical location are visible (Screenshot 4).

4. VPN Encryption and Security Features

4.1 Encryption Standards

Protocol	Description	Security Level
AES-256	Military-grade encryption; widely adopted.	Extremely High
OpenVPN	Open-source; supports multiple encryption methods.	High
WireGuard	Lightweight, faster than OpenVPN/IPSec.	High
IKEv2/IPSec	Balances speed and security; ideal for mobile devices.	High

4.2 Privacy Protection

- No-Logs Policy: Ensures user activity (browsing history, connections) is not recorded.
- Kill Switch: Terminates internet access if VPN disconnects abruptly.
- DNS Leak Protection: Prevents ISPs from intercepting domain requests.

4.3 Limitations

- Speed Reduction: Encryption overhead may slow connection speeds.
- VPN Blocking: Some platforms (e.g., streaming services, banks) blacklist VPN IP ranges.
- Trust Dependency: Free VPNs may compromise privacy (e.g., data logging).

5. Case Study: Screenshot Analysis 5.1

Scenario 1: Active VPN Usage

- Observed Data:
  - IP: 185.107.56.135 (Netherlands)
  - ISP: NForce Entertainment B.V. (VPN provider)
- Implications:
  - Successful geolocation spoofing.
  - VPN server detected by third-party tools.

5.2 Scenario 2: No VPN Protection

- Observed Data:
  - IP: 45.112.32.36 (India) o ISP: Vision Broadband
  - ISP: Vision Broadband
- Implications:
  - Physical location and ISP exposed.
  - Highlights VPN's critical role in anonymity.

6. Recommendations

6.1 For Individual Users

1. Select Reputable Providers: Choose VPNs with independent audits (e.g., ExpressVPN, ProtonVPN).
2. Enable Advanced Features: Activate kill switch and DNS leak protection.
3. Avoid Free VPNs: They may monetize user data.

6.2 For Organizations

1. Deploy Enterprise VPNs: Use solutions like Cisco AnyConnect for scalable security.
2. Monitor VPN Traffic: Detect anomalies or unauthorized access.
3. Educate Employees: Train staff on VPN best practices.

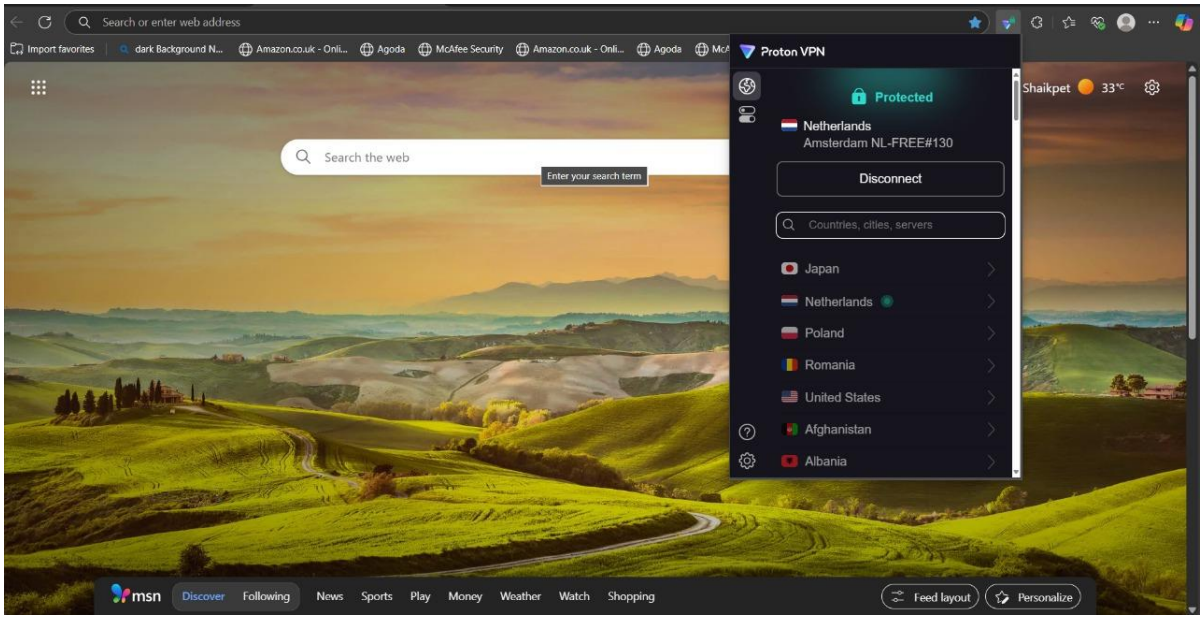
7. Conclusion

VPNs are indispensable for safeguarding online privacy, but their efficacy depends on proper configuration and provider trustworthiness. The analyzed screenshots demonstrate both the strengths (IP masking, server flexibility) and limitations (detection, speed trade-offs) of VPN technology. Future advancements in protocols like WireGuard may further optimize security and performance.

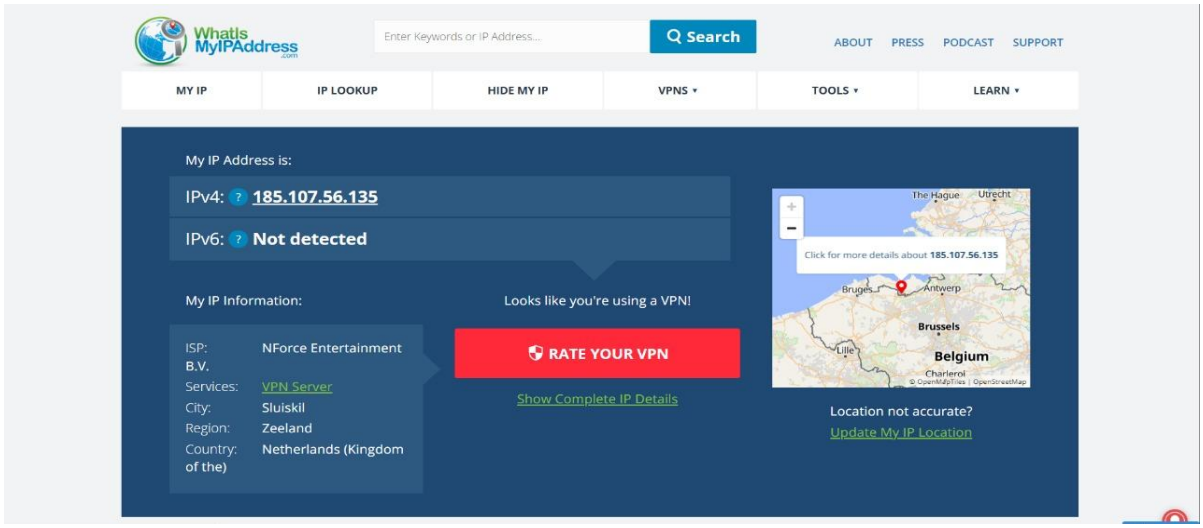
Attachments:

- Screenshot 1-4: VPN usage examples.
- Encryption protocol comparison table.

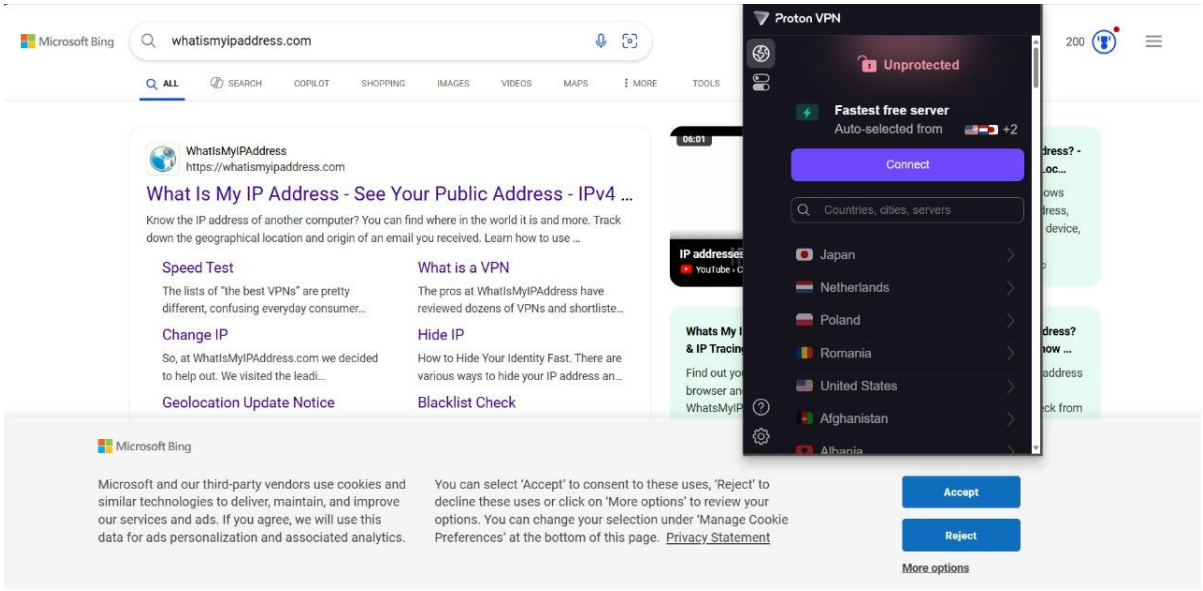
Step1: Connect the VPN:



Step2: Open the website of whatismyipaddress:



Step3: Disconnect the VPN:



Step4: Again open the website of whatismyipaddress: