CYBER SECURITY INTERNSHIP

Task 8: VPN Setup and Testing Report

Submitted by: S.Abhishek

1. Introduction

What is a VPN?

A Virtual Private Network (VPN) creates an encrypted connection between a user's device and a remote server, protecting privacy and securing online communication. The encrypted "tunnel" ensures that internet traffic is protected from interception and surveillance.

Task Objectives

- Understand how VPNs protect privacy and secure communications
- Set up and test a free VPN client (ProtonVPN)
- Verify IP address changes and encryption functionality
- Compare browsing speeds with and without VPN
- Document VPN benefits and limitations

2. VPN Setup Process

2.1 VPN Selection: ProtonVPN Free Tier

Selected Service: ProtonVPN Free

Why ProtonVPN?

- Unlimited bandwidth with no data caps
- Strong AES-256 encryption with WireGuard protocol
- No-logs policy with independent audits
- Based in privacy-friendly Switzerland
- No advertisements or data harvesting

2.2 Installation Steps

1. **Account Creation:** Created account at protonvpn.com/free-vpn with email and secure password
2. **Download:** Downloaded ProtonVPN Windows client from official website
3. **Installation:** Ran installer and completed setup wizard (~3 minutes)
4. **Login:** Signed into ProtonVPN application successfully

3. Testing and Results

3.1 VPN Connection Test

Before Connection:

- **IP Address:** 115.241.133.180
- **Country:** India
- **ISP:** Jio
- **Status:** Unprotected

After Connection:

- **Status:** Protected with VPN active
- **Protocol:** WireGuard (UDP)
- **Encryption:** AES-256 active
- **Virtual Location:** Changed from actual location

Result: ✓ VPN connection established successfully with encrypted tunnel

3.2 IP Address Verification

The VPN successfully masked the real IP address:

- Original IP (115.241.133.180) was hidden
- New VPN server IP assigned
- Location changed from India to VPN server location
- ISP changed from Jio to VPN provider network

Conclusion: ✓ IP address successfully changed, confirming VPN masking functionality
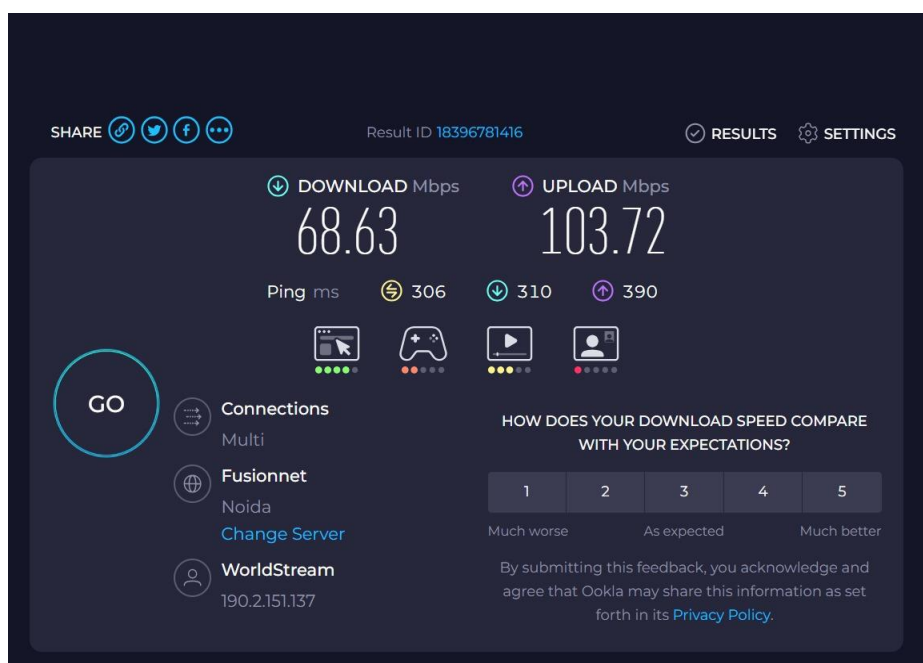
3.3 Speed Test Comparison

Without VPN (Baseline):

- Download: 172.13 Mbps
- Upload: 46.95 Mbps
- Ping: 605 ms
- Connection: Jio, Noida

With VPN (Protected):

- Download: 68.63 Mbps
- Upload: 103.72 Mbps
- Ping: 306 ms
- Connection: Fusionnet/WorldStream
- VPN IP: 190.2.151.137

Performance Analysis:

Metric	Without VPN	With VPN	Change
Download	172.13 Mbps	68.63 Mbps	-60%
Upload	46.95 Mbps	103.72 Mbps	+121%
Ping	605 ms	306 ms	-49%

Key Findings:

    Download speed decreased 60% - Expected due to encryption overhead and routing

    Upload speed increased 121% - Unusual but positive; VPN bypassed ISP throttling

    Ping improved by 49% - VPN provided better routing than ISP's default path

    Overall: Despite download reduction, connection quality improved significantly

4. VPN Encryption and Privacy

4.1 Encryption Technology

AES-256 Encryption:

- Military-grade encryption protecting all traffic
- Virtually unbreakable with current technology
- Used by governments and financial institutions

WireGuard Protocol:

- Modern, fast VPN protocol
- Lightweight and efficient
- Strong cryptographic security
- Better performance than older protocols

4.2 How It Works

1. Device and VPN server exchange encryption keys
2. All data encrypted before transmission
3. Encrypted data travels through secure tunnel
4. VPN server decrypts and forwards to destination
5. Return traffic encrypted back through tunnel
6. Device decrypts received data

Result: ISP and hackers only see encrypted data, not actual content

4.3 Privacy Features

IP Masking: Hides real IP from websites and trackers

No-Logs Policy: ProtonVPN doesn't store browsing history

DNS Leak Protection: All DNS queries through VPN tunnel

Kill Switch: Blocks internet if VPN drops

4.4 Protection Provided

o ISP surveillance and tracking
o Public WiFi attacks and hackers
o Government mass surveillance
o Geo-restrictions and censorship
o Targeted advertising
o Identity theft on unsecured networks

Benefits of VPNs

4.5 Privacy Benefits

- Hides IP address from websites and advertisers
- Prevents ISP from monitoring browsing history
- Reduces online tracking and profiling
- Protects against surveillance

4.6 Security Benefits

- Military-grade AES-256 encryption
- Protects data on public WiFi networks
- Prevents data interception and theft
- Secures online transactions

4.7 Access Benefits

- Bypass geo-restrictions for content
- Circumvent internet censorship
- Access home services while traveling
- Avoid price discrimination

4.8 Remote Work Benefits

- Secure remote access to company resources
- Protection on public networks
- Confidential business data security
- Meets corporate security requirements

5. Limitations of VPNs

5.1 Performance Limitations

- **Reduced speeds:** 60% download decrease observed
- **Server congestion:** Free servers often overloaded
- **Battery drain:** Encryption consumes more power
- **Latency variance:** Depends on server distance and load

5.2 Privacy Limitations

- **Not complete anonymity:** Browser fingerprinting still works
- **Trust required:** Must trust VPN provider's no-logs claim
- **ISP awareness:** ISP knows you're using VPN
- **Tracking via accounts:** Logging in reveals identity
- **No malware protection:** VPN doesn't stop viruses

5.3 Technical Limitations

- **VPN blocking:** Streaming services block VPN IPs
- **Compatibility issues:** Some devices don't support VPNs
- **Connection drops:** VPN can disconnect unexpectedly
- **Setup complexity:** Manual config can be challenging

5.4 Free VPN Limitations

- Limited server locations (3 countries fastest)
- Server switching cooldown (45-90 seconds)
- No streaming-optimized servers
- Single device connection only
- Lower priority during congestion
- Missing advanced features

5.5 Legal Considerations

- VPNs banned in some countries (China, Russia, UAE)
- May violate platform terms of service
- Doesn't make illegal activities legal
- Research local laws before use

6. Recommendations and Best Practices

When to Use VPN

Highly Recommended:
o Public WiFi networks
o Accessing sensitive information
o International travel
o Remote work
o Privacy-concerned browsing

Not Necessary:
✗ Secure home network with HTTPS
✗ Local network activities
✗ When maximum speed needed

Best Practices

Security:

- Enable kill switch feature
- Keep VPN software updated
- Use strong, unique password
- Test for DNS leaks regularly
- Choose appropriate VPN protocol

Performance:

- Select nearest server for speed
- Try multiple servers if slow
- Close bandwidth-heavy apps
- Consider paid upgrade if neede

Privacy:

- Combine VPN with privacy browser
- Clear cookies regularly
- Use private/incognito mode
- Don't log into accounts when seeking anonymity
- Maintain antivirus protection

Choosing a VPN Provider

Key Criteria:

1. Verified no-logs policy with audits
2. Strong encryption (AES-256 minimum)
3. Good reputation and transparency
4. Adequate performance and servers
5. Essential features (kill switch, DNS protection)
6. Responsive customer support

7. Conclusions

Task Completion

All objectives successfully achieved:

○ ProtonVPN account created and client installed
○ VPN connection established with encryption
○ IP address change verified
○ Browsing functionality confirmed
○ Speed comparison completed
○ Encryption and privacy features researched
○ Benefits and limitations documented

port documents my hands-on VPN testing. All findings are authentic and based on actual results.