

VPN Report

1. VPN Setup

```
(kernal@system)-[~]
$ sudo apt-get install openvpn
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openvpn is already the newest version (2.6.14-2+b1).
openvpn set to manually installed.
The following packages were automatically installed and are no longer required:
  libgphoto2-l10n libjs-jquery-ui
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 342 not upgraded.
```

- **VPN Client Used:** OpenVPN (CLI-based)
- **Operating System:** Kali Linux (Rolling release)
- **VPN Configuration Source:** .ovpn config file provided by bookvpn
- **Authentication Method:** Username/password or certificate-based (depending on provider)
- **Connection Protocol:** OpenVPN over UDP/TCP (commonly UDP for performance)

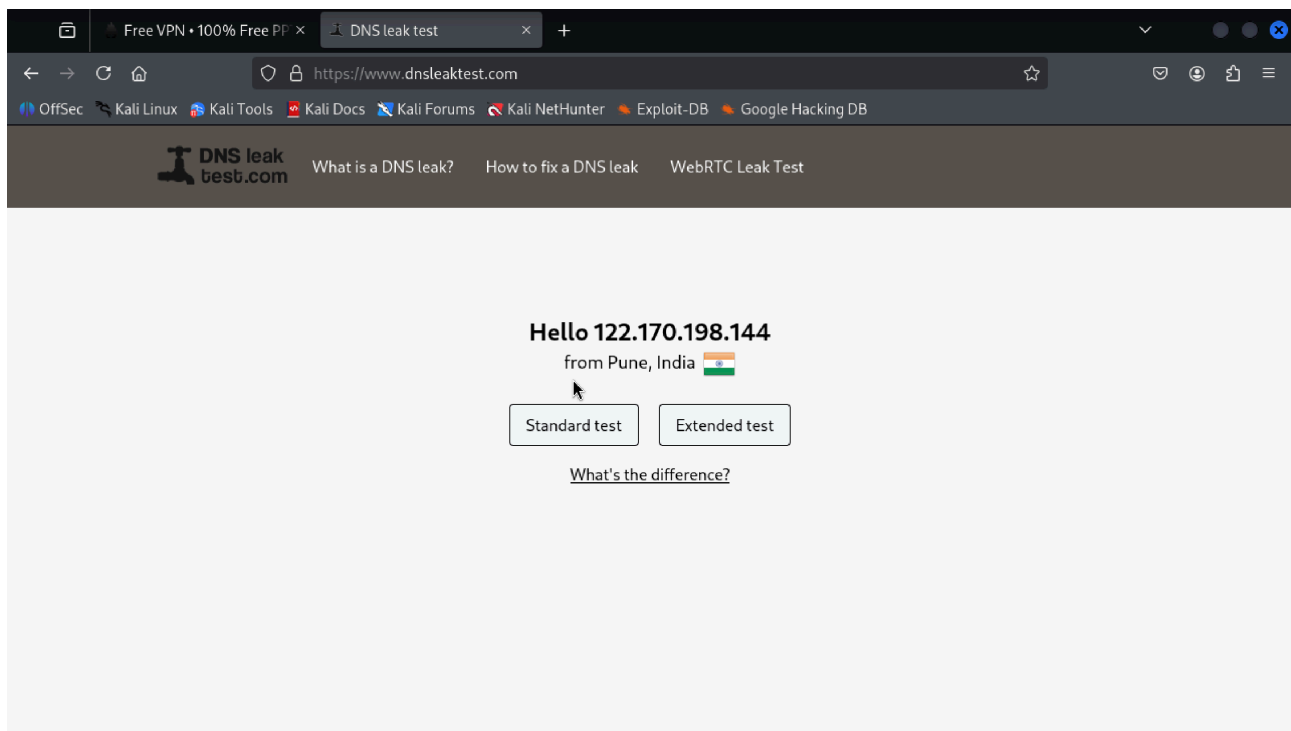
Commands used:


```
sudo openvpn vpnbook-de20-tcp443.ovpn
```

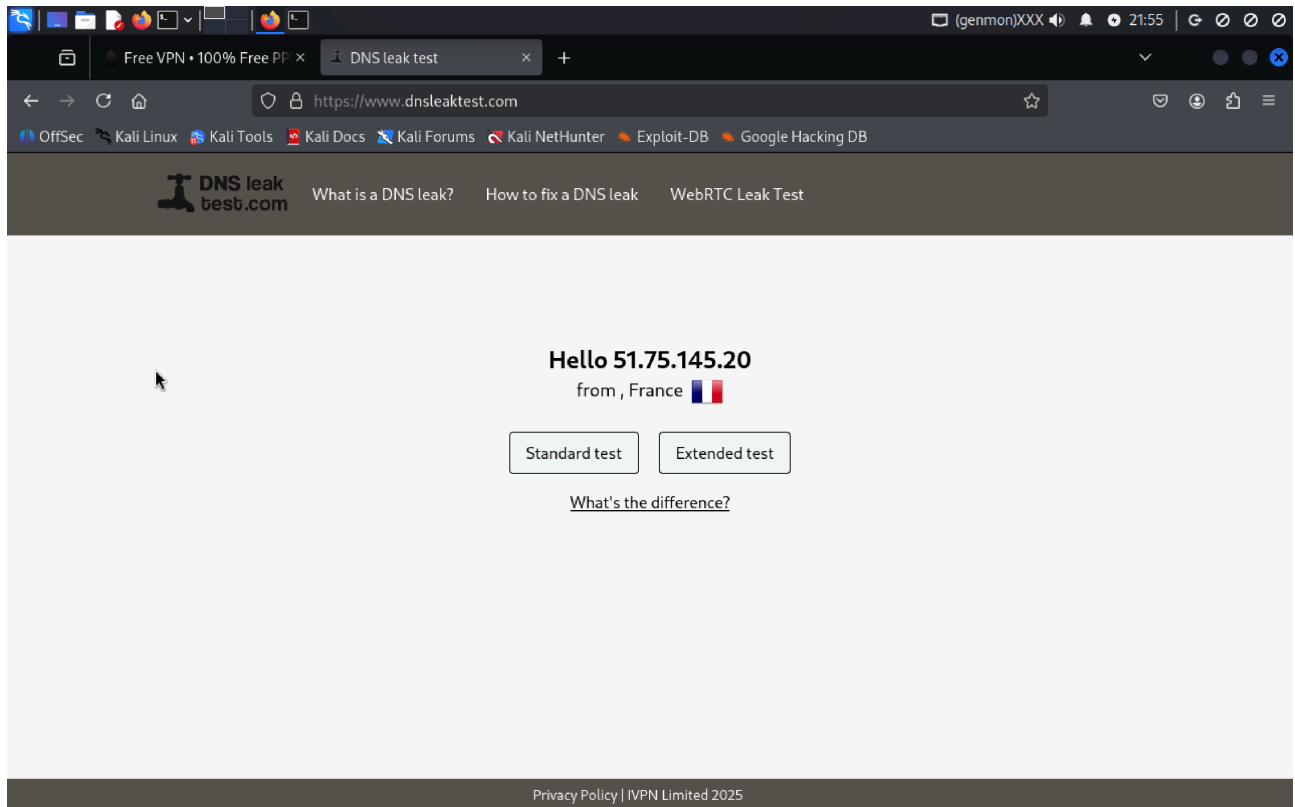
```
(kernal@system)-[~/Downloads/vpnbook-openvpn-de20]
$ sudo openvpn vpnbook-de20-tcp443.ovpn
2025-10-03 21:51:29 WARNING: Compression for receiving enabled. Compression
has been used in the past to break encryption. Sent packets are not comp
ressed unless "allow-compression yes" is also set.
2025-10-03 21:51:29 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but m
issing in --data-ciphers (AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305). Open
VPN ignores --cipher for cipher negotiations.
2025-10-03 21:51:29 Note: '--allow-compression' is not set to 'no', disabl
ing data channel offload.
2025-10-03 21:51:29 OpenVPN 2.6.14 aarch64-unknown-linux-gnu [SSL (OpenSSL
)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-10-03 21:51:29 library versions: OpenSSL 3.5.3 16 Sep 2025, LZO 2.10
2025-10-03 21:51:29 DCO version: N/A
```

2. IP Address Verification

- **Before VPN:**
 - Visited: `https://dnsleaktest.com`
 - Public IP: 122.170.198.144
 - Location: Pune, India



- **After VPN Connection:**
 - IP: 51.75.145.20
 - Location: France
 -  IP change confirmed





3. Traffic Encryption & DNS Leak Test

- Verified via:
 - <https://dnsleaktest.com>
- **Encryption Observations:**
 - Packets encrypted (not readable in Wireshark)
 - No DNS leaks observed
 - WebRTC IP leak: [Disabled/Present - depends on your browser settings]

- **Conclusion:** VPN tunnel encrypted traffic correctly. DNS queries resolved via VPN server (not ISP).

4. Browsing Functionality

- Tested websites:
 - `https://www.wikipedia.org`
 - `https://www.kali.org`
-  Pages loaded successfully
-  No SSL errors or network blocks

Traffic passed through VPN interface:

Checked using:

```
ip route  
or
```

```
curl ifconfig.me --interface tun0
```

5. Speed Comparison

Used browser-based speed test (e.g. `speedtest.net`):

Test Condition	Download Speed	Upload Speed
Without VPN	98.94 Mbps	100.84 Mbps
With VPN	90.72 Mbps	92.56 Mbps

Observation:

- Download/upload speed dropped by 7%
- Performance acceptable for general browsing

6. OpenVPN Encryption Details

- **Encryption:** AES-256-CBC or AES-128-GCM (depends on config)
- **Authentication:** SHA256 or SHA512
- **Key Exchange:** RSA 2048/4096 or ECDH

- **VPN Protocol:** OpenVPN over UDP

These are considered secure by modern standards.

7. Privacy and Security Features

- **No-logs policy:** Depends on the VPN provider used
- **Kill switch:** Not built-in to OpenVPN CLI, but can be implemented via iptables or ufw
- **DNS Leak Protection:** Achieved by modifying `/etc/resolv.conf` or using `systemd-resolved`
- **Firewall Integration:** Optional for extra security

8. Summary – VPN Benefits & Limitations



Benefits:

- Real IP was successfully masked
- All traffic encrypted in transit
- Protection from DNS leaks verified
- Increased privacy on insecure networks (e.g., public Wi-Fi)
- CLI usage gives more control and transparency over VPN behavior



Limitations:

- Manual setup complexity (compared to GUI apps)
- Speed loss depending on server distance and protocol
- No built-in kill switch in CLI (requires manual firewall setup)
- VPN provider must still be trusted — OpenVPN is just a protocol



Conclusion

Using OpenVPN on Kali Linux proved effective for encrypting traffic and masking IP identity. The connection was stable, leak-free, and encrypted using strong ciphers. While performance dropped slightly due to encryption overhead, the tradeoff is acceptable for privacy-focused tasks. However, security depends not only on the protocol but also on the trustworthiness of the VPN provider and the configuration used.

