Bachelor’s Thesis

Information and Communications Technology

2024

Oskari Turki

A Comparison of VPN Providers Focusing on their Security and Speed

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Iinformation and Communications Technology

2024 | 33 pages

Oskari Turki

A Comparison of VPN Providers Focusing on their Security and Speed

Click here to enter text.

In this thesis, various VPN service providers were compared, focusing particularly on their security, speed, and associated risks. The aim was to evaluate how the VPN services perform against two criteria: the strength of their security features and the efficiency of their data transfer speeds. Additionally, this study delved into the potential security risks and privacy issues related to free VPN services, such as data logging practices and the possible sale of user data to third parties.

The study revealed that the performance of VPN services can vary significantly. Speed tests showed substantial differences in download speeds, which can affect the user experience, especially in bandwidth-intensive activities such as streaming and gaming. A surprising finding was how well some free VPNs performed, even surpassing some paid options. This challenges the common perception that paying always provides better service.

In terms of security, several VPN services proved to be strong as they did not reveal any leaks. However, the presence of DNS and encryption leaks in some services indicates that even paid VPNs are not immune to flaws that could expose user data.

Future research could focus on testing other aspects of VPN services such as device compatibility, user experience. This would help form a more comprehensive understanding of how well different VPN services meet the diverse needs and preferences of users.

Keywords:

VPN, Digital security, Data transmission speed, Device compatibility, Encryption protocols, User experience, Network privacy.

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tieto -ja viestintätekniikan insinööritutkinto

2024 | 33 sivua

Oskari Turki

VPN-palveluntarjoajien turvallisuuden ja nopeuden vertailu

Tässä opinnäytetyössä vertailtiin eri VPN-palveluntarjoajia, tarkastellen erityisesti niiden turvallisuutta, nopeutta ja niihin liittyviä riskejä. Tavoitteena oli arvioida, miten nämä teknologiat suoriutuvat kahdessa kriteeriassa: niiden turvallisuusominaisuuksien vahvuudessa ja datan siirtonopeuksien tehokkuudessa. Lisäksi tutkimus syventyi ilmaisiin VPN-palveluihin liittyviin mahdollisiin turvallisuusriskeihin ja yksityisyysongelmiin, kuten datan kirjaamiskäytäntöihin ja mahdolliseen käyttäjätietojen myyntiin kolmansille osapuolille.

Tutkimuksessa selvisi, että VPN-palveluiden suorituskyky voi vaihdella huomattavasti. Nopeustesteissä havaittiin suuria eroja latausnopeuksissa, mikä voi vaikuttaa käyttäjäkokemukseen erityisesti kaistanleveyttä vaativissa toiminnoissa, kuten suoratoistossa ja pelaamisessa. Yllättävänä löydöksenä oli, kuinka hyvin jotkin ilmaiset VPN:t suoriutuivat, jopa ylittäen osan maksullisista vaihtoehdoista. Tämä haastaa yleisen käsityksen, että maksamalla saa aina paremman palvelun.

Turvallisuuden osalta useat VPN-palvelut osoittautuivat vahvoiksi, sillä ne eivät osoittaneet. Kuitenkin DNS ja salausprotokollien vuotojen esiintyminen joissakin palveluissa osoittaa, että jopa maksulliset VPN:t eivät ole immuuneja virheille, jotka voivat paljastaa käyttäjän tietoja.

Jatkotutkimuksessa voitaisiin keskittyä VPN-palveluiden muiden osa-alueiden, kuten laiteyhteensopivuuden, käyttäjäkokemuksen testaamiseen. Tämä auttaisi muodostamaan kattavamman kuvan siitä, miten hyvin eri VPN-palvelut vastaavat käyttäjien moninaisia tarpeita ja mieltymyksiä.

Asiasanat:

VPN, digitaalinen turvallisuus, datan siirtonopeus, laitteiden yhteensopivuus, salausprotokollat, käyttäjäkokemus, verkon yksityisyys.

Contents

Pictures

Tables

List of abbreviations

DNS	Domain Name System. Translates domain names into IP addresses.
VPN	Virtual Private Network. Creates a secure, encrypted connection over public networks.
WebRTC	Web Real-Time Communication. Enables real-time communication in web browsers and mobile apps.
Geolocation	The process of determining the geographical location of a device or user based on their IP address or other means.
Server	A computer or system that provides resources, services, or functionality to other computers, known as clients, over a network.
IP Address	A numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
Proxy	A server that acts as an intermediary between a client and other servers. It can be used for various purposes, including anonymity, caching, and access control.
Kill swich	A feature in VPN services that automatically disconnects your device from the internet if the VPN connection fails, preventing data leaks

1 Introduction

In this thesis, I will be testing the speed and security of various VPN providers. The reason I chose only speed and security as the focus of this thesis is that these are the two most important factors people consider when picking a VPN. VPNs are crucial for protecting our online privacy, keeping our data secure, and allowing us to access the internet freely. But if a VPN isn't fast or secure, it just doesn't cut it.

Additionally, I am comparing my results to TechRadar's results because I want to see if you can trust their reviews and the results you get from a simple Google search. This will help determine whether widely recognized reviews are reliable or if they might be misleading consumers.

I will first provide an introduction to what a Virtual Private Network (VPN) is, including its functions and benefits. I will then delve into the specific VPN providers, focusing on their connection methods, tunneling protocols, and security features. The theoretical section will also cover the tools used in the analysis.

Following the theoretical background, I will conduct practical testing of various VPN providers, focusing on two key aspects: speed and security.

1.1 Objectives and the Scope of the Thesis

- Evaluate the comparative effectiveness of various VPN providers in terms of securityand speed.

- Illuminate the strengths and weaknesses inherent in these providers to aid users in making informed decisions.

- Scrutinize the accuracy and trustworthiness of widely recognized VPN reviews to assess their influence on consumer decisions and verify their information accuracy.

1.2 Limitations of the Research

This study is bounded by several constraints that shape its scope and depth:

Selection Bias: The VPN technologies chosen for in-depth analysis may not encompass the full spectrum of available options, potentially skewing the comparative insights.

Rapid Technological Evolution: The fast-paced nature of digital technology development means that findings may quickly become outdated as new advancements emerge.

Platform Specificity: This research focuses exclusively on VPN performance on PC platforms. This decision excludes potential variations in VPN performance on mobile devices such as Android and iOS, which could provide different insights due to their distinct operating environments and hardware configurations.

2 Background on Virtual Private Networks (VPNs)

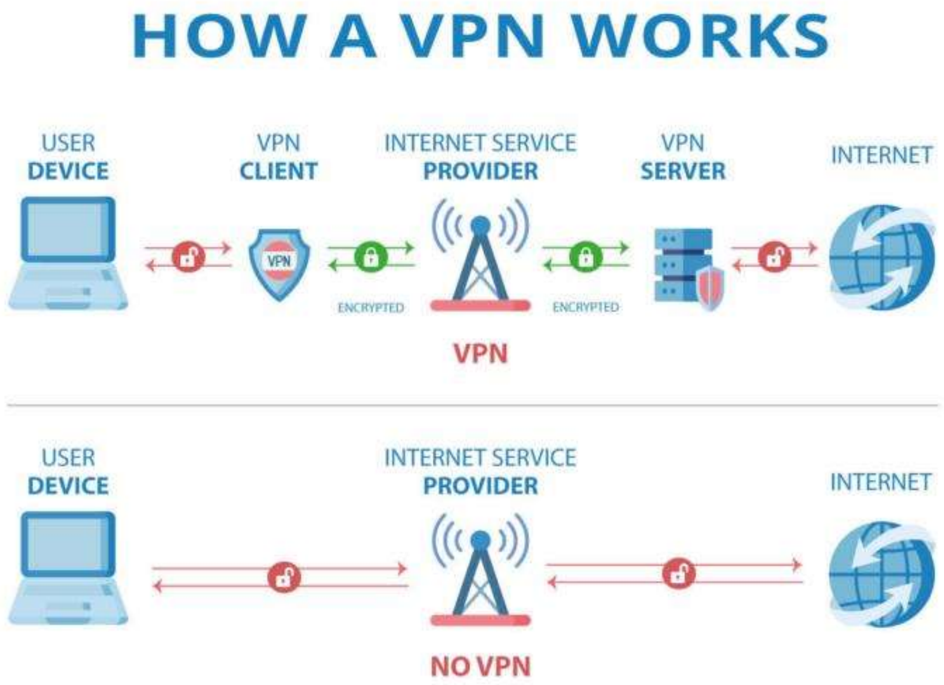
2.1 Introduction

Virtual Private Networks (VPNs) are pivotal in modern networking, providing secure connections over less secure networks such as the internet. By creating a protected network connection, VPNs ensure the confidentiality, integrity, and availability of data during transit across public networks.

2.2 What is a VPN and How Does a VPN Work?

A VPN extends a private network across a public network, enabling users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network (Costa et al., 2000). This means applications running across a VPN can benefit from the functionality, security, and management of the private network.

VPNs employ various encryption protocols to ensure that data transmitted between two points through the public network remains private (Picture 1). VPN technology uses tunneling protocols to encrypt data at the sending end and decrypt it at the receiving end. Additionally, authentication protocols allow VPN clients and servers to securely verify the identity of users on both ends (Khan, 2010).



Picture 1. How a VPN works. (Management.org 2024).

2.3 Why and Where is it Used?

Organizations use VPNs for several reasons including enabling remote workers to connect to the company network securely, safeguarding sensitive data, and providing a layer of security for their internal network communications. VPNs are widely used in environments where information confidentiality is critical, such as in governmental, financial, and healthcare sectors (Nyakomitta & Abeka, 2020).

In addition to organizational use, VPNs are also extensively utilized by private individuals for various purposes. In a study Understanding How and Why University Students Use Virtual Private Networks, university students primarily use VPNs to encrypt their internet connection, ensuring data transmitted over the internet remains secure and private. This is particularly important for students using public Wi-Fi networks, where the risk of cyber threats is higher.

Additionally, VPNs enable users to a broader range of digital content. By connecting to servers in different countries, students can enjoy unrestricted access to streaming services, websites, and applications otherwise unavailable in their region.

This is particularly useful for streaming international media, accessing libraries of digital content that vary by location, and even for getting around censorship in restrictive jurisdictions. This ability to "geo-spoof" one's location also allows individuals to shop for deals or products available in specific markets.

Thus, the versatility of VPNs makes them a valuable tool not only for businesses seeking to protect their networks and data but also for individuals looking to preserve their privacy and freedom on the internet (Dutkowska-Zuk et al., 2020).

2.4 Drawbacks and Risks of Using a VPN

While VPNs are instrumental in enhancing security, they are not devoid of drawbacks. The complexity of VPN services can lead to configuration errors, potentially exposing vulnerabilities. Furthermore, the reliance on a third-party service provider for the provision of the VPN service introduces a risk element regarding the handling and accessibility of sensitive data. Security concerns also arise from the potential for VPN services to be used as a conduit for malicious activities (Ali et al., 2003).

VPNs continue to be a vital part of network security strategies in numerous sectors, providing secure, encrypted pathways for data transmission over public networks. However, their implementation and maintenance require rigorous security measures and continuous monitoring to mitigate inherent risks.

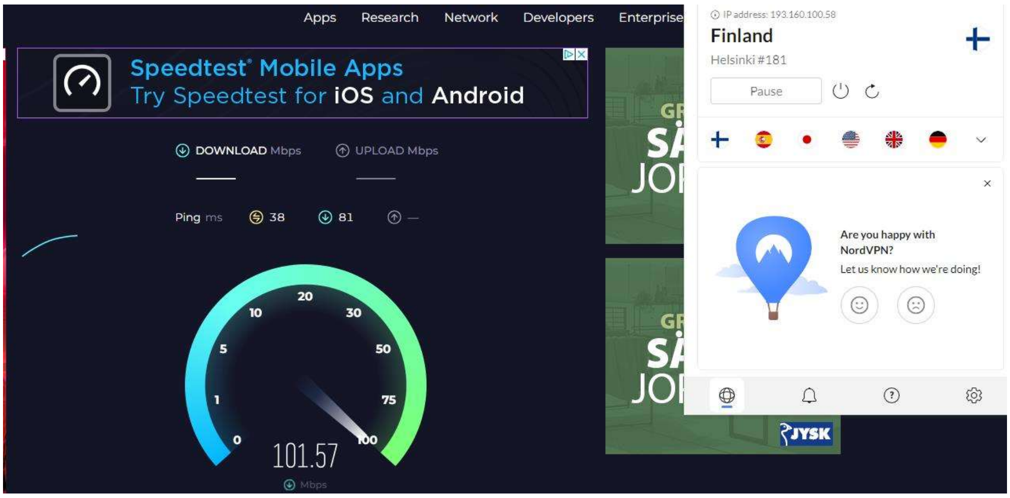
3 Methods

This thesis employs a series of tests to evaluate selected VPN providers through technical testing and case analysis. A notable focus of this methodology is the analysis of review accuracy and consumer trust, specifically examining TechRadar's "Best VPNs of 2024" list. This list is pivotal because it appears as the first result on Google for "best VPNs," reflecting its significant influence on consumer choices (Henderson, T. 2024. Best VPN).

3.1 Speed Testing

To evaluate the speed of various VPN technologies, we will use Speedtest.net, a trusted platform for internet speed measurements. The testing of free versus paid VPN provider testing will include three speed tests conducted at VPN server locations in the United States, Japan, and Spain, which represent North America, Asia, and Europe, respectively. These locations are chosen due to their availability with our testing VPN providers and their geographical diversity. To align our testing methodology with TechRadar's comparison, we will use the US and UK as the test locations, as these were the locations used in TechRadar's evaluations. (Speedtest.net. 2024).

Each location will be tested three times in a row to ensure the accuracy and consistency of our results. After these tests, we will calculate the average connection speed for each location. Once we have the average speeds for all locations, we will then calculate the overall average speed for the VPN itself. Every VPN provider will be tested this same way and the tests will be conducted at the same times each day to keep things fair and account for any changes in network traffic.



Picture 2. VPN Speed Test in Progress using speedtest.net.

3.2 Security Testing

To evaluate the VPNs, we will use IPleak.net, a tool for detecting IP leaks. IPleak.net is a free online tool designed to help users check for potential IP address leaks and other privacy issues while using a VPN or proxy. The site offers a variety of tests, including IP address detection, DNS leak tests, WebRTC leak tests, and geolocation checks. Additionally, we will use WireGuard to test encryption protocols and verify the robustness of the VPNs' encryption. We will also check if each VPN has a kill switch feature to ensure that the user's internet connection is automatically cut off if the VPN connection drops, providing an extra layer of security(IPleak.net 2024).

What are these tests that are being done?

- IP Address Detection
  This test checks whether your true IP address is being exposed while using a VPN, ensuring that only the VPN's IP address is visible.

- DNS Leak Test

This test verifies if your DNS requests are being routed through the VPN. A DNS leak occurs when your DNS requests bypass the VPN, potentially exposing your browsing activity to your ISP.

- WebRTC Leak Test
  This test examines if your WebRTC (a technology for real-time communication) is leaking your true IP address. WebRTC can sometimes bypass VPNs and expose your actual IP address.

- Geolocation Check
  This test compares the location reported by your IP address to your actual location, ensuring the VPN is successfully masking your real location and showing the VPN server's location instead.

- Encryption Test (WireGuard)
  This test checks if the VPN uses strong encryption methods to protect your data, ensuring it stays secure.

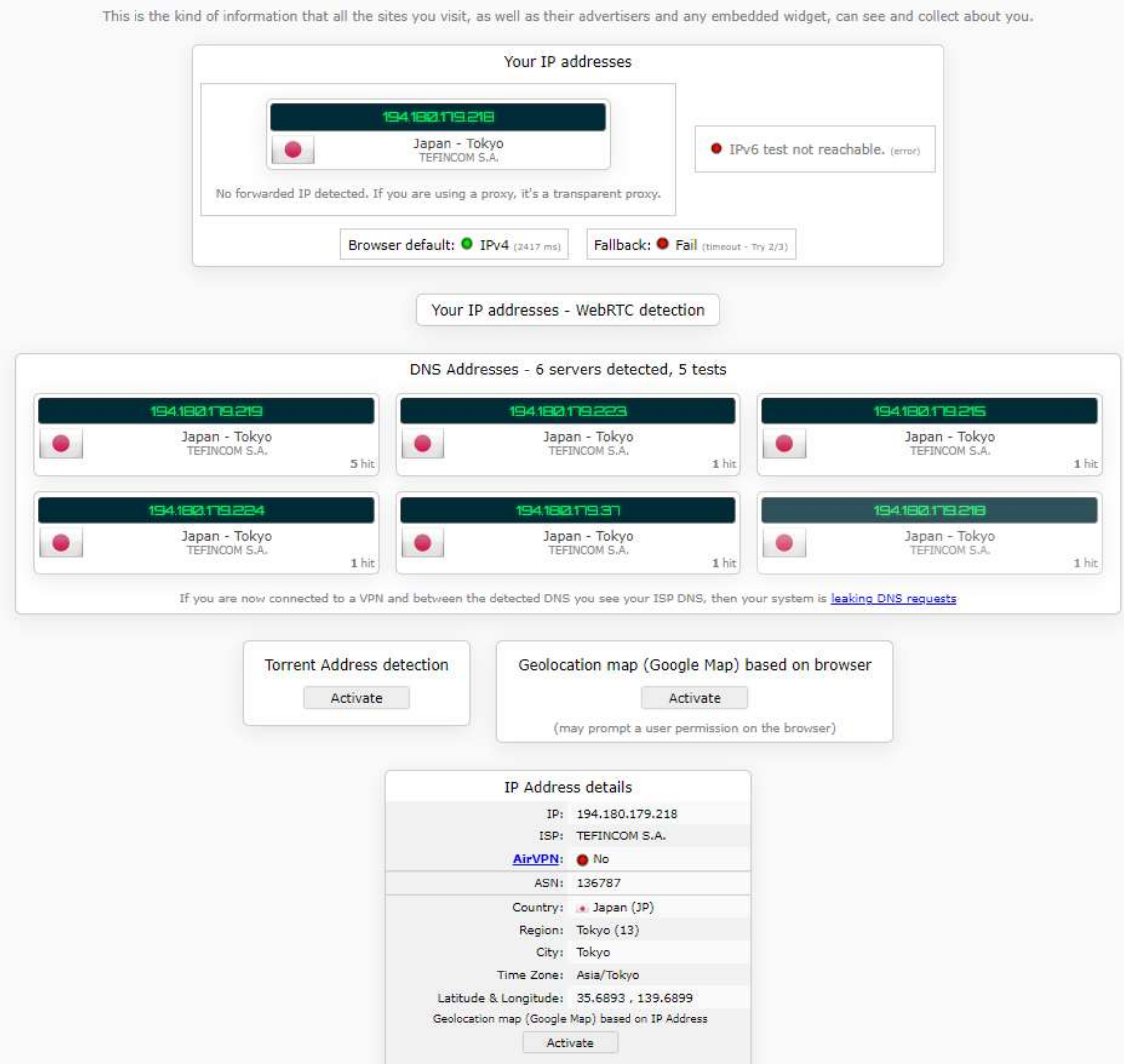
- Kill Switch Test
  This test checks if the VPN has a kill switch feature, which cuts off your internet if the VPN connection drops, keeping your data safe.

The IPleak.net testing process consists of three main steps:

1. Use IPleak.net without connecting to the VPN to record the standard IP and DNS settings. This serves as our baseline.

2. Connect to the VPN and use IPleak.net again to perform the same tests.

3. Compare the results from before and after activating the VPN to assess its effectiveness in masking the user’s IP address.



This is the kind of information that all the sites you visit, as well as their advertisers and any embedded widget, can see and collect about you.

Your IP addresses

194.180.179.218
Japan - Tokyo
TEFINCOM S.A.

No forwarded IP detected. If you are using a proxy, it's a transparent proxy.

● IPv6 test not reachable. (error)

Browser default: ● IPv4 (2417 ms) Fallback: ● Fail (timeout - Try 2/3)

Your IP addresses - WebRTC detection

DNS Addresses - 6 servers detected, 5 tests

194.180.179.219 Japan - Tokyo TEFINCOM S.A. 5 hit	194.180.179.223 Japan - Tokyo TEFINCOM S.A. 1 hit	194.180.179.215 Japan - Tokyo TEFINCOM S.A. 1 hit
194.180.179.224 Japan - Tokyo TEFINCOM S.A. 1 hit	194.180.179.37 Japan - Tokyo TEFINCOM S.A. 1 hit	194.180.179.218 Japan - Tokyo TEFINCOM S.A. 1 hit

If you are now connected to a VPN and between the detected DNS you see your ISP DNS, then your system is leaking DNS requests

Torrent Address detection
Activate

Geolocation map (Google Map) based on browser
Activate
(may prompt a user permission on the browser)

IP Address details

IP:	194.180.179.218
ISP:	TEFINCOM S.A.
AirVPN:	● No
ASN:	136787
Country:	Japan (JP)
Region:	Tokyo (13)
City:	Tokyo
Time Zone:	Asia/Tokyo
Latitude & Longitude:	35.6893 , 139.6899

Geolocation map (Google Map) based on IP Address
Activate

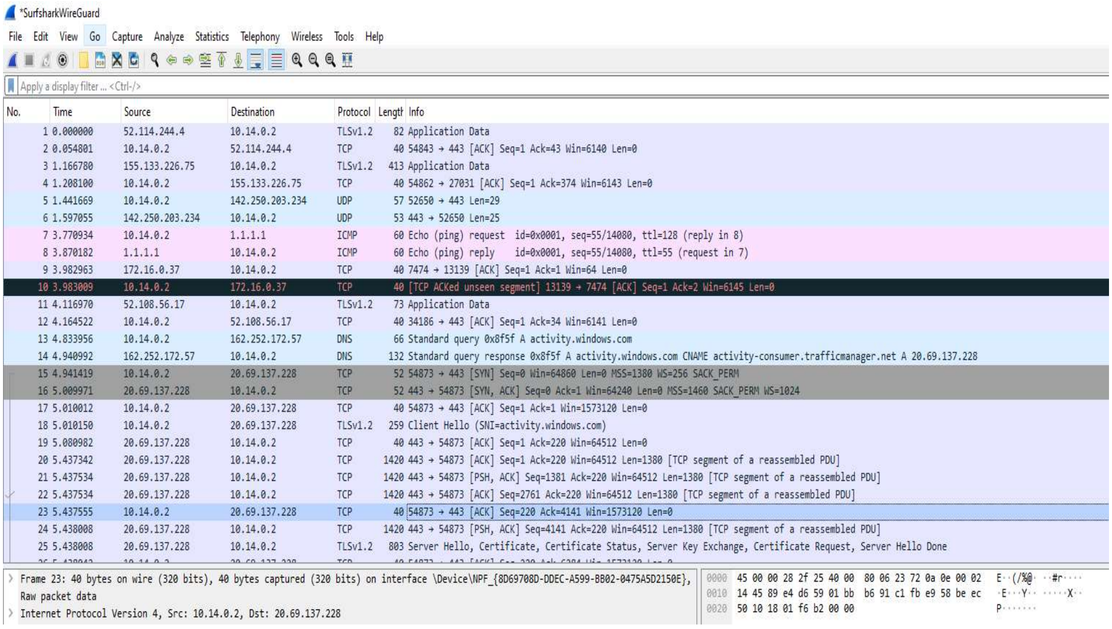
Picture 3. Testing security using ipleaks website.

The WireGuard testing process consists of three main steps:

1. Connect to the VPN using the WireGuard protocol.

2. Open and run Wireshark to capture and inspect your internet traffic.

3. Review the captured traffic to ensure all data is encrypted and secure.



```
No.   Time       Source           Destination      Protocol  Lengtl Info
    1 0.000000   52.114.244.4     10.14.0.2        TLSv1.2     82 Application Data
    2 0.054801   10.14.0.2        52.114.244.4     TCP         40 54843 → 443 [ACK] Seq=1 Ack=43 Win=6140 Len=0
    3 1.166780   155.133.226.75   10.14.0.2        TLSv1.2    413 Application Data
    4 1.208100   10.14.0.2        155.133.226.75   TCP         40 54862 → 27031 [ACK] Seq=1 Ack=374 Win=6143 Len=0
    5 1.441669   10.14.0.2        142.250.203.234  UDP         57 52650 → 443 Len=29
    6 1.597055   142.250.203.234  10.14.0.2        UDP         53 443 → 52650 Len=25
    7 3.770934   10.14.0.2        1.1.1.1          ICMP        60 Echo (ping) request  id=0x0001, seq=55/14080, ttl=128 (reply in 8)
    8 3.870182   1.1.1.1          10.14.0.2        ICMP        60 Echo (ping) reply    id=0x0001, seq=55/14080, ttl=55 (request in 7)
    9 3.982963   172.16.0.37      10.14.0.2        TCP         40 7474 → 13139 [ACK] Seq=1 Ack=1 Win=64 Len=0
   10 3.983009   10.14.0.2        172.16.0.37      TCP         40 [TCP ACKed unseen segment] 13139 → 7474 [ACK] Seq=1 Ack=2 Win=6145 Len=0
   11 4.116970   52.108.56.17     10.14.0.2        TLSv1.2     73 Application Data
   12 4.164522   10.14.0.2        52.108.56.17     TCP         40 34186 → 443 [ACK] Seq=1 Ack=34 Win=6141 Len=0
   13 4.833956   10.14.0.2        162.252.172.57   DNS         66 Standard query 0x8f5f A activity.windows.com
   14 4.940992   162.252.172.57   10.14.0.2        DNS        132 Standard query response 0x8f5f A activity.windows.com CNAME activity-consumer.trafficmanager.net A 20.69.137.228
   15 4.941419   10.14.0.2        20.69.137.228    TCP         52 54873 → 443 [SYN] Seq=0 Win=64860 Len=0 MSS=1380 WS=256 SACK_PERM
   16 5.009971   20.69.137.228    10.14.0.2        TCP         52 443 → 54873 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=1024
   17 5.010012   10.14.0.2        20.69.137.228    TCP         40 54873 → 443 [ACK] Seq=1 Ack=1 Win=1573120 Len=0
   18 5.010150   10.14.0.2        20.69.137.228    TLSv1.2    259 Client Hello (SNI=activity.windows.com)
   19 5.080982   20.69.137.228    10.14.0.2        TCP         40 443 → 54873 [ACK] Seq=1 Ack=220 Win=64512 Len=0
   20 5.437342   20.69.137.228    10.14.0.2        TCP       1420 443 → 54873 [ACK] Seq=1 Ack=220 Win=64512 Len=1380 [TCP segment of a reassembled PDU]
   21 5.437534   20.69.137.228    10.14.0.2        TCP       1420 443 → 54873 [PSH, ACK] Seq=1381 Ack=220 Win=64512 Len=1380 [TCP segment of a reassembled PDU]
   22 5.437534   20.69.137.228    10.14.0.2        TCP       1420 443 → 54873 [ACK] Seq=2761 Ack=220 Win=64512 Len=1380 [TCP segment of a reassembled PDU]
   23 5.437555   10.14.0.2        20.69.137.228    TCP         40 54873 → 443 [ACK] Seq=220 Ack=4141 Win=1573120 Len=0
   24 5.438008   20.69.137.228    10.14.0.2        TCP       1420 443 → 54873 [PSH, ACK] Seq=4141 Ack=220 Win=64512 Len=1380 [TCP segment of a reassembled PDU]
   25 5.438008   20.69.137.228    10.14.0.2        TLSv1.2    803 Server Hello, Certificate, Certificate Status, Server Key Exchange, Certificate Request, Server Hello Done
```

```
> Frame 23: 40 bytes on wire (320 bits), 40 bytes captured (320 bits) on interface \Device\NPF_{8D69708D-DDEC-A599-BB02-0475A5D2150E},
  Raw packet data
> Internet Protocol Version 4, Src: 10.14.0.2, Dst: 20.69.137.228
```

```
0000  45 00 00 28 2f 25 40 00  80 06 23 72 0a 0e 00 02   E··(/%@· ··#r····
0010  14 45 89 e4 d6 59 01 bb  b6 91 c1 fb e9 58 be ec   ·E···Y·· ·····X··
0020  50 10 18 01 f6 b2 00 00                            P·······
```

Picture 4. Encrypted Traffic Analysis Using WireGuard.

4 Speed Testing Results

This chapter presents the results from the technical evaluations of various VPN technologies as outlined in the previous chapter. The findings are split into two main parts. paid versus free VPN services and assess how our rankings stack up against Techradar's.Results of testing.

Table 1. Average Speed Comparison for Paid VPN Providers.

Paid VPN Provider	Average Download Speed (Mbps)	Average Upload Speed (Mbps)
Air VPN	65	18
Astrill VPN	87	34
Avast SecureLine	61	12
CyberGhost	56	15
ExpressVPN	94	36
Hide.me VPN	139	33
Hotspot Shield VPN	112	28
IPVanish	152	34
Mozilla VPN	72	24
Mullvad	84	24
Nord VPN	103	35
Norton Secure VPN	80	19
Private Internet Access	99	43
Privado VPN	72	26
Proton VPN	100	12
Pure VPN	87	36
Strong VPN	63	27
Surfshark	97	22
TunnelBear	19	44
Turbo VPN	95	31
VyprVPN	73	13
Windscribe	69	29

Table 2. Average Speed Comparison for Free VPN Providers.

VPN Provider	Average Download Speed (Mbps)	Average Upload Speed (Mbps)
Astrill VPN	72	23
Avast SecureLine	42	11
Betternet VPN	64	39
ExpressVPN	92	27
Hide.me VPN	142	34
Hotspot Shield VPN	95	37
Mullvad	88	38
Norton Secure VPN	35	8
Private Internet Access	85	33
Privado VPN	75	10
Proton VPN	124	42
Surfshark	91	45
Touch VPN	71	30
TunnelBear	19	44
Turbo VPN	128	36
Urban VPN	53	35
VeePN	41	28
Windscribe	88	2
ZenMate	65	37

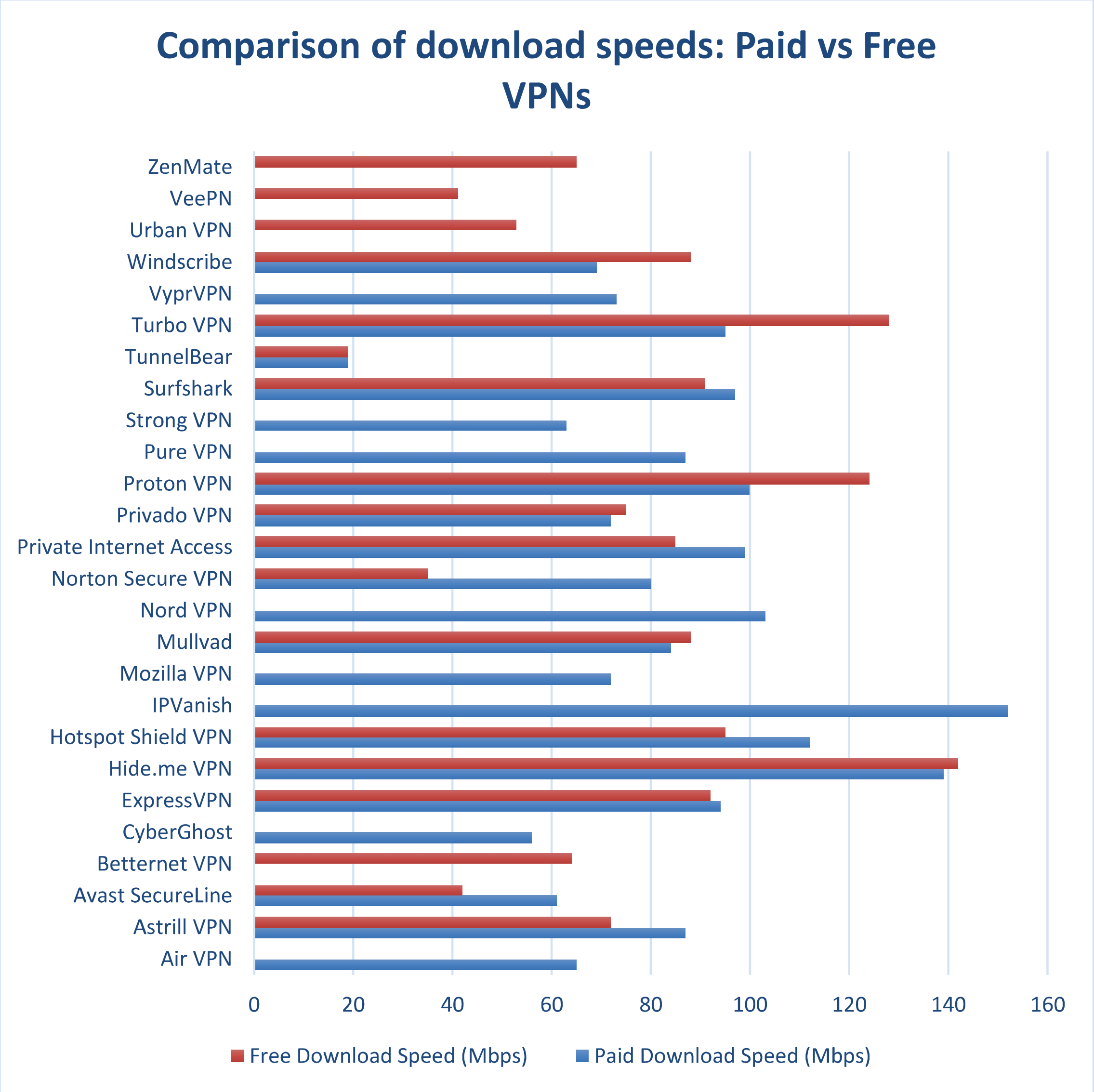
4.1 Analysis of Results

The data reveals that several paid VPN providers, such as IPVanish, Nord VPN, and Hide.me, offer very high download speeds. Other notable paid services, including ExpressVPN and Surfshark, also provide commendable speeds, reinforcing the view that paid VPNs typically deliver reliable and fast service.

On the other hand, the performance of free VPN services is notably competitive. Free offerings from Hide.me and Turbo VPN exhibit download speeds that are not only on par with but sometimes exceed those of their paid counterparts. This is significant as it challenges the conventional wisdom that paid VPNs are always superior in performance.

Overall, the analysis indicates that while paid VPNs generally offer high-speed and reliable connections, free VPNs have shown substantial progress in reaching similar performance levels. Users might consider both options based on their specific needs and budget, as the gap in performance between paid and free services appears to be narrow.

Figure 21. Comparative Average Download Speeds of Free vs. Paid VPN Providers.



4.2 Comparative analysis with TechRadar results

There is a noticeable variance between the speeds we measured and the rankings provided by TechRadar. For example, while TechRadar ranks Windscribe highly, our tests found other VPNs like Private Internet Access and ExpressVPN to perform better in terms of speed.

These discrepancies could be due to different methodologies used for testing, the times at which tests were conducted, or possible preferential biases in TechRadar's reviews.

Table 3. VPN Provider Ranking Comparison: User vs. TechRadar.

VPN Provider	My Rank	TechRadar
Private Internet Access	1	18
NordVPN	2	5
ExpressVPN	3	15
Surfshark	4	1
Hotspot Shield	5	13
IPVanish	6	8
Mozilla Vpn	7	19
PureVPN	8	7
Hide.me	9	12
Proton VPN	10	2
Astrill VPN	11	17
Norton VPN	12	6
VyprVPN	13	10
CyberGhost	14	9
AirVPN	15	11
Privado VPN	16	4
TunnelBear	17	14
Windscribe	18	3
StrongVPN	19	16

4.3 Implications of the results

This analysis indicates that consumers should not solely rely on VPN rankings from review sites when selecting a service. Instead, they should consider looking at independent test results to make a more informed decision.

Users should also be aware that some free VPNs can offer comparable, if not superior, performance to paid VPNs, although this might come with other trade-offs like security and privacy risks.

5 Security testing results

5.1 Analysis of results

The test results were quite revealing. VPNs like ExpressVPN and Surfshark showed stellar performance, with no leaks and spot-on geolocation accuracy and encrypted data suggesting they provide reliable protection. Interestingly, our findings highlighted notable differences between the security performance of free and paid VPN services. This observation reinforces the common belief that you often get better security with paid services.

However, not all VPNs were flawless. Turbo VPN and VyprVPN, for instance, had issues with potential DNS leaks. These leaks point to vulnerabilities that need attention, showing that even some paid VPNs can have gaps in fully securing user data. Additionally, Turbo VPN exhibited WebRTC leaks, further highlighting its security weaknesses. Touch VPN, a free service, showed significant issues with an IP leak and inaccurate geolocation, underscoring the variability in security performance among different VPN providers.

Regarding the presence of a kill switch Most VPNs tested, both free and paid, included a kill switch, which ensures that user data is not exposed if the VPN connection drops unexpectedly.

This evaluation drives home the point: the security strength of a VPN isn't solely determined by whether it is free or paid. It's crucial to consider how they perform in real-world tests. Users should evaluate each VPN based on actual data and performance, not just on whether there's a price tag attached. The tests demonstrated that while some free VPNs can be secure, many still have significant vulnerabilities that need to be addressed.

Table 4. Summary of VPN Security Testing Results.

VPN Provider	**IP Leak Test**	**DNS Leak Test**	**WebRTC Leak Test**	**Geolocation Accuracy**	**Encryption Protocol**	**Encryption Test Result**	**Kill Swich**
Hide.Me VPN	No leak	No leak	No leak	Accurate	AES 256-bit	All traffic encrypted	Yes
Hotspot VPN	No leak	No leak	No leak	Accurate	Catapult Hydra	All traffic encrypted	Yes
IPVanish	No leak	No leak	No leak	Accurate	AES 256-bit	All traffic encrypted	Yes
Mozilla VPN	No leak	No leak	No leak	Accurate	ChaCha20	All traffic encrypted	Yes
Mullvad	No leak	No leak	No leak	Accurate	AES 256-bit	All traffic encrypted	Yes
Nord VPN	No leak	No leak	No leak	Accurate	AES-256-GCM	All traffic encrypted	Yes
Norton VPN	No leak	No leak	No leak	Accurate	AES 256-bit	All traffic encrypted	Yes
Private Internet Access	No leak	No leak	No leak	Accurate	128-bit AES	All traffic encrypted	Yes
Privado VPN	No leak	No leak	No leak	Accurate	AES 256-bit	All traffic encrypted	Yes
Proton VPN	No leak	No leak	No leak	Accurate	AES-256 or ChaCha20	All traffic encrypted	Yes
Pure VPN	No leak	No leak	No leak	Accurate	AES 256-bit	All traffic encrypted	Yes
Strong VPN	No leak	No leak	No leak	Accurate	128-bit or 256-bit AES	All traffic encrypted	Yes

(Continue)

Table 4. (Continue)

VPN Provider	IP Leak Test	DNS Leak Test	WebRTC Leak Test	Geolocation Accuracy	Encryption Protocol	Encryption Test Result	Kill Swich
Surfshark	No leak	No leak	No leak	Accurate	AES-256 GCM	All traffic encrypted	Yes
Touch VPN (free)	Leak	No leak	No leak	Inaccurate	SSL	Not encrypted	No
TunnelBear	No leak	No leak	No leak	Accurate	AES 256-bit	All traffic encrypted	Yes
Turbo VPN (free)	No leak	Leak	Leak	Accurate	AES 256-bit	Not encrypted	Yes
Urban VPN (free)	No leak	No leak	No leak	Accurate	AES 256-bit	Not encrypted	No
VeePN	No leak	No leak	No leak	Accurate	AES-256 bit	All traffic encrypted	Yes
Vypr VPN	No leak	Potential leak	No leak	Accurate	AES 256-bit	All traffic encrypted	Yes
Windscribe	No leak	No leak	No leak	Accurate	AES 256-bit	All traffic encrypted	No
ZenMate (free)	Leak	Leak	Leak	Accurate	TLS	Not encrypted	Yes
ExpressVPN	No leak	No leak	No leak	Accurate	AES-256 bit	All traffic encrypted	Yes
CyberGhost	No leak	No leak	No leak	No leak	AES-256 bit	All traffic encrypted	Yes
Astrill VPN	No leak	No leak	No leak	No leak	AES-256 bit	All traffic encrypted	Yes
AirVPN	No leak	No leak	No leak	No leak	AES-256 bit	All traffic encrypted	Yes
BetterNet (free)	No leak	Leak	No leak	Inaccurate	AES-256 bit	All traffic encrypted	Yes

5.2 Considerations on data usage by VPN providers

Even when VPNs show no leaks in security tests, it’s crucial to consider how they manage user data. For instance, NordVPN's privacy policy specifies various conditions under which personal data is processed and shared. Despite assurances of not selling user data, their policy states:

"We do not share your personal data with third parties except as described in this Privacy Policy. Service providers...may process personal data...We use third-party service providers to help us with various operations, such as payment processing, email automation, websites and app diagnostics, analytics, and other" (NordVPN Privacy Policy, Section 3).

This excerpt highlights that while NordVPN commits to not selling user data outright, it acknowledges sharing data with third-party service providers for a range of operational purposes.

A study titled "A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN Clients" by Haddadi and Perta (2015) further emphasizes the need for caution. The research highlights that many commercial VPN services, despite their privacy claims, suffer from IPv6 traffic leakage and DNS hijacking vulnerabilities. This means that even with a VPN, users' data may still be exposed through these leaks, undermining the very privacy protections VPNs are supposed to provide. The study's findings illustrate that technical capabilities alone are insufficient if the implementation of the VPN services is flawed or incomplete. Therefore, it is crucial for users to not only review privacy policies but also understand the technical robustness of the VPN services they choose to ensure comprehensive data protection (Haddadi & Perta, 2015).

These examples raises questions about the extent to which user data might be utilized beyond the primary service, even in scenarios where the VPN technically secures the data from leaks.

Such details underscore the importance of thoroughly scrutinizing the privacy policies of VPN services, not just their technical capabilities, to ensure comprehensive privacy protection. Users need to be aware of the broader implications of how their data is handled to make informed choices about their privacy.

6 Conclusion

6.1 Overview of Key Findings

In this thesis, we delved deep into how various VPN services stack up in terms of both speed and security. From our speed tests, it was clear that performance can vary greatly among VPNs. Services such as IPVanish and Hide.me outperformed the other services with impressive download speeds, which makes them solid choices for bandwidth-heavy activities such as streaming and gaming. On the other end of the spectrum, TunnelBear and CyberGhost lagged, which could potentially dampen user experience where speed is crucial.

An unexpected finding was how well some free VPNs performed. Hide.me and Turbo VPN, for example, outpacing some paid options. This finding shakes up the common assumption that paid services provide better service at lest regarding VPN speed.

On the security front, industry giants such as Nord VPN, Surfshark and ExpressVPN were standout performers, showing no leaks and perfect geolocation matches effectively meeting all the criteria for a robust VPN service. However, the presence of DNS leaks in Turbo VPN and Vypr VPN shows that even paid VPNs are not immune to flaws that could expose user data.

Regarding free VPNs the testing revealed that free VPNs pose significant security risks overall. Turbo VPN had WebRTC leaks, highlighting its security issues, while Touch VPN, a free service, had major problems with IP leaks and inaccurate geolocation. This demonstrates that free VPNs often have varied and unreliable security levels, making them a risky choice.

6.2 Comparison with TechRadar's Findings

When comparing the results against TechRadar’s rankings, some interesting discrepancies came to light. For instance, although TechRadar held Windscribe in high regard, our tests found that Private Internet Access and ExpressVPN had the edge in speed. These differences might be due to the timing of our tests, the methodologies applied, or even TechRadar's potential biases. This highlights why it is critical for users to look at multiple sources and independent tests before deciding on a VPN.

6.3 Practical Recommendations

Based on our findings, the recommendation is to not select a VPN solely based on its cost (free or paid). Instead, evaluate its actual performance in tests similar to ours. While some free VPNs offer excellent service, it is important to be cautious of potential compromises, particularly concerning security and privacy.

Looking ahead, VPN users should remain vigilant and informed. It is crucial to stay updated on independent research, which more accurately reflects the current capabilities of VPNs in real-world conditions. Furthermore, a thorough examination of the fine print in privacy policies, such as that of NordVPN, can provide deeper insights into the actual commitments and terms beyond the surface-level assurances.

7 Closing Thoughts

As this thesis wraps up, the findings presented highlight that while VPNs can offer robust protection, their effectiveness can vary significantly, necessitating careful consideration and selection by users.

Furthermore, as technology continues to evolve, the functionality and security of VPNs must not remain static. Continuous research and updates on our understanding of these tools will be essential to ensure that VPNs can keep up with new technological challenges and meet increasingly stringent security and performance standards. This thesis lays the groundwork for future research, encouraging a proactive approach to VPN evaluation and emphasizing the importance of transparency and user education in promoting digital safety.

Moving forward, the commitment to regularly updating our knowledge of VPN technologies will be indispensable in safeguarding digital privacy. By staying informed and critical, users can better navigate the complex VPN landscape and make choices that align with their privacy and security needs.

References

Ali, A.A., Abd El-Mageed, T., & Al Gamal, S. (2003). *Virtual Private Networks: An Overview from the Security Perspective*. Ensuring Security in IT. Retrieved from (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.95.6357)

Costa, L., Fdida, S., & Duarte, O. (2000). *An Introduction to Virtual Private Networks: Towards D-VPNs*. Retrieved from (https://www.researchgate.net/publication/228964331_An_Introduction_to_Virtual_Private_Networks_Towards_D-VPNs)

Dutkowska-Zuk, A., Hounsel, A., Xiong, A., Chetty, M., Feamster, N., Roberts, M., & Stewart, B. (2020). Practicing safe browsing: Understanding how and why university students use virtual private networks. *CoRR*, abs/2002.11834. https://www.semanticscholar.org/paper/Practicing-Safe-Browsing%3A-Understanding-How-and-Why-Dutkowska-Zuk-Hounsel/3841c2e35dbf558176301ffecbc17d21646d85ce

Henderson, T. (2024, January 2). The best VPN service in 2024. *TechRadar*. https://www.techradar.com/vpn/best-vpn

IPleak.net 2024 retrieved from https://ipleak.net/

Khan, M.Y. (2010). *An Overview of Virtual Private Network (VPN)*. Edited by: Prof. R.E. Sheriff School of Engineering, Design, and Technology, University of Bradford. Retrieved from (https://bradscholars.brad.ac.uk/handle/10454/4355)

Khan, Y.F. (2018). *Cisco Secured Virtual Private Networks: A Review*. Asian Journal of Computer Science and Technology. Retrieved from (https://www.academia.edu/80581079/Cisco_Secured_Virtual_Private_Networks_A_Review)

NordVPN. (2024). Privacy Policy. Retrieved May 11, 2024, from https://my.nordaccount.com/legal/privacy-policy/

Nyakomitta, P.S., & Abeka, S.O. (2020). *Security Investigation on Remote Access Methods of Virtual Private Network*. Global Journal of Computer Science and Technology. Retrieved from (https://www.academia.edu/82129469/Security_Investigation_on_Remote_Access_Methods_of_Virtual_Private_Network)

Perta, V. C., Barbera, M. V., Tyson, G., Haddadi, H., & Mei, A. (2015). A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN Clients. *Proceedings on Privacy Enhancing Technologies*, 2015(1), 77-91. https://doi.org/10.1515/popets-2015-0006

Speedtest by Ookla retrieved 12.6.2024. www.speedtest.net