TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technology

Ali Izady Sadr 194444IVSB

Comparative Analysis of Virtual Private Network Solutions for Peer-to-peer Content Delivery: the Case of Iran

Bachelor Thesis

Supervisor: Kaido Kikkas

Ph.D.

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Ali Izady Sadr 194444IVSB

Võrdvõrkudes sisujagamiseks mõeldud virtuaalse privaatvõrgu lahenduste võrdlev analüüs Iraani näitel

Bachelor Thesis

Juhendaja: Kaido Kikkas
Ph.D.

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This report has not been presented for examination anywhere else.

Author: Ali Izady Sadr

15.05.2023

Abstract

In this thesis, Virtual Private Network (VPN) solutions are evaluated against Internet Service Provider (ISP) Deep Packet Inspection (DPI) surveillance technology for uncompromised Peer-to-Peer (P2P) content delivery. VPNs encrypt data to safeguard the traffic between the device being used by the user and the server running a VPN. VPNs also hide users' locations and identities via a remote server, making it challenging for servers to capture user activity and browsing data. Furthermore, the issue statement requires assessing VPN solutions' ability to block ISPs' deep inspection of online activity. Inadequate knowledge about essential factors when choosing a VPN service for P2P content delivery could expose people's safety and security to risk. It's possible that rules and limits established by the state will limit the abilities of P2P users to make informed decisions in protecting their privacy using VPN technology, provided that they lack sufficient background knowledge on the subject. The study aims to determine the effectiveness of VPN solutions in preventing DPI, identify the most important factors to consider when choosing a VPN solution for P2P content delivery, and assess P2P end-user approval with various VPN solutions. The research can be beneficial to a group of people comprising P2P users in Iran, whose access to free Internet is severely restricted by the state, to the extent to which their lack of knowledge of the subject, will endanger their lives, given that over 10 individuals are executed weekly by the authorities. Based on research, industry reports, trustworthy reviews, and user interviews, VPN systems will be compared. This research will illuminate VPN options for P2P users and guide the users to select the most effective solution. It also provides insights into VPN customers' P2P content distribution reasons and preferences, which may assist with enhancing VPN service effectiveness and usability. The majority of respondents expressed gratification with their VPN for P2P content distribution and expressed concern for their privacy in the absence of a VPN, according to this study. This thesis seeks to close the existing information gap regarding the efficacy of VPN P2P solutions against Deep Packet Inspection and to assist end-users in making informed decisions.

List of Abbreviation and Terms

API	Application Programming Interface
AES-256	Advanced Encryption Standard
APOD	Adaptive Port Obfuscation Defense
BFS	Breadth-First Search
BTP	Bramble Transport Protocol
BSP	Bramble Synchronization Protocol
CDA	Communications Decency Act
DFI	Deep Flow Inspection
DHCP	Dynamic Host Configuration Protocol
DHT	Distributed Hash Table
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
DOC	Distributed Object Computing
DPI	Deep Packet Inspection
dVPN	Decentralized VPNs
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FTP	File Transfer Protocol
GFW	Great Firewall
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
ICHRI	International Campaign for Human Rights in Iran
ICMP	Internet Control Message Protocol
ICR	Internet Connection Records
IKE	Internet Key Exchange
iOS	iPhone Operating System
IP	Internet Protocol
IIOP	Internet Inter-Orb Protocol

IPOP	IP-over-P2P
IPSec	IP Security
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
L2TP	Layer 2 Tunnel Protocol
LAN	Local Area Network
MGM	Metro Goldwyn Mayer
NAT	Network Address Translation
NATO	the North Atlantic Treaty Organization
NCA	National Crime Agency
NCSAM	National Cybersecurity Awareness Month
OS	Operating System
OSI	Open System Interconnection
OTT	Over the top
P2P	Peer to Peer
PIA	Private Internet Access
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
QR code	Quick Response code
RAM	Random Access Memory
RFC	Request for Comments
RPC	Remote Procedure Call
RSF	Reporters sans Frontières
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SMH	Smart Multi-Homed name Resolution
SPID	Statistical Protocol Identification
TCP	Transmission Control Protocol
Tor	The Onion Router
UDP	User Datagram Protocol
UKUSA	United Kingdom – United States of America Agreement

URL	Uniform Resource Locator
VAN	Virtual Anonymous Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VPS	Virtual Private Server
WebRTC	Web Real-Time Communication

1. Introduction

This chapter discusses the study's motivation, problem statement, objectives, and scope. In this section, the overall structure of the investigation is also presented.

1.1 Problem Statement

As a means of safeguarding online activity, the adoption of VPN solutions, particularly for P2P users, has grown more popular. The use of VPNs with a concentration on P2P surveillance by ISPs DPI protection is a novel alternative to the widespread use of traditional VPN solutions. [1] On the other hand, there are not many studies that look at how well VPNs work, how safe they are, and how private they are for P2P users. Finally, it should be noted that there are P2P users residing in Iran whose safety is at risk if they fail to employ appropriate anti-surveillance technologies and select the appropriate VPN solution. [2], [3], [4], [5] Therefore, in order to assist P2P end-users in selecting the optimal solution, which takes into account the various security and privacy features that are available, a comprehensive analysis of VPN solutions and utilized technologies in those solutions to circumvent ISP DPI is required.

In addition, it is vital to evaluate the efficacy of VPN solutions in blocking surveillance methods such as DPI, which may put the privacy and security of users at risk. To acquire a better understanding of how VPN systems might protect themselves against such surveillance approaches, further study is required.

The scope of the problem: The objective of this research is to conduct a comparative evaluation of Virtual Private Network (VPN) solutions for Peer-to-Peer (P2P) end-users. The study primarily concentrates on VPN solutions for content distribution through P2P networks and their impact on user privacy. The research is engaging P2P end-users located in Turkey, Estonia, and Iran, while the main focus remains on Iranian P2P end-users. The following characteristics of VPN solutions for P2P content distribution will be the primary focus of the investigation:

1. Technical specifications: The purpose of this research is to investigate the technical specifications of VPN solutions for P2P end-users. These technical requirements include encryption techniques, tunneling protocols, and server locations.

2. Security features: The study will evaluate the safety characteristics of VPN systems for P2P end-users. These characteristics include protection against IP leaks, Domain Name Service (DNS) leaks, and Web Real-Time Communication (WebRTC) leaks, among others.
3. Ease of use: The research will evaluate the ease of use of VPN solutions for P2P end-users, including aspects such as the simplicity of installation, the convenience of operation, and the availability of customer assistance.

In order to reduce the scope of the study, the following privacy technologies and policies will not be included in the investigation:

1. The study will not look into other privacy-enhancing technologies outside VPNs, such as Tor or proxies. In addition, the legal difficulties that are associated with P2P technology and the influence that it has on owners of copyright will not be discussed in the research.
2. VPN for Remote Access: This sort of VPN facilitates user connection to an enterprise network from a remote location.
3. Site-to-Site VPN: VPN that is used to connect many networks together.
4. A client-to-server VPN is a sort of VPN that facilitates remote user connections to a single server.
5. Single-Protocol vs. Multi-Protocol VPNs: The investigation of VPN options for P2P content distribution is not helped by this comparison.

Limitations: The study will be subject to a limited time frame, potentially impacting the comprehensiveness of the investigation. ISPs may monitor the data without full disclosure as a result of the lack of documentation techniques, which may restrict the accuracy of the data that is acquired. In addition, the researchers will not have access to the logging and monitoring databases maintained by the ISPs; this might potentially restrict the scope of the probe.

Conclusion: It is claimed that there is a safe solution for P2P content distribution. This method enables secure communication and the sharing of content while avoiding interception by DPI protection offered by ISPs. This strategy is particularly effective for individuals or groups that

suffer internet restrictions and constraints on their actions, such as those who were imprisoned in Iran for sharing news and information about current events online. These users are able to communicate with the outside world in a risk-free and protected manner thanks to the technology, which eliminates the possibility that their communications may be intercepted or monitored by third parties.

1.2 Research Questions

This thesis intends to present a comparative analysis of VPN choices for P2P clients, focusing on their benefits and drawbacks, effectiveness in preventing thorough surveillance by ISPs, and client impressions of privacy and security. The subsequent research questions steer this study:

- How effective are VPN solutions at preventing ISPs from conducting DPI and monitoring the online activities of P2P users?
- What are the most essential technologies to consider when selecting a VPN solution for content distribution over P2P networks?
- Which VPN service is the most optimal choice for distributing P2P content in the case of Iran?

The research will evaluate several VPN systems in terms of their user approval, as well as their P2P security features and technical specifications. The analysis will be informed by a comprehensive literature study consisting of research, industry reports, reliable reviews, and user interviews. By demonstrating the usefulness of P2P VPN technologies, this research aims to facilitate their development and widespread use.

1.3 Research Methodology

This section will outline the methodology and approach used in this study. The effectiveness of VPN technologies against ISP Deep Packet Inspection for P2P content delivery, public assessments, and user interviews regarding VPNs and anonymous content delivery technology will be compared. The fourth chapter will contain findings and suggestions.

Research Design: The most effective VPN service for shielding P2P networks from DPI carried out by ISPs was identified through a comparative research that was carried out on the most up-to-date versions of the VPNs that are now on the market. The investigation was based on a number of aspects, such as the technologies that were implemented, evaluations from the public, and user input gathered via interviews.

In order to ensure the validity of the outcomes of the comparative analysis, a very stringent methodology was employed in this study. The most advanced VPN technologies were selected after thorough review of their industry standing, as well as their capacity to shield P2P networks from ISP DPI.

Regarding each VPN service, public evaluations were also taken into consideration. Additionally, interviews were carried out with a representative sample of end-users who make frequent use of P2P networks and VPNs in order to obtain their feedback on the reliability of their ISPs and the efficacy of the VPNs that were chosen to protect against DPI.

The degree to which users have faith in their ISPs and how well various VPNs shield users from DPI was evaluated in this study. The many sources of information were merged to find the most effective VPN solution for protecting P2P networks from data collection by ISPs.

In order to gain a deeper comprehension of the primary factors that influence users of P2P apps, investigation on the strategies that ISPs employ for conducting surveillance in relation to P2P applications were done. This research will assist in determining the primary privacy and security problems that VPN solutions for P2P end-users need to solve in order to be effective.

The approach of this comparative study aimed to provide a comprehensive analysis of the various VPN solutions that are now available, in order to assist consumers in making well-informed judgments about the VPN service they finally choose.

2. Background

This chapter discusses P2P apps' privacy risks and uses. Internet Service Providers' privacy breach technologies and state applications are reviewed. This investigation aims to shed light on P2P application use, privacy breaches, and their methodologies.

2.1 P2P Applications Major Usage Spectrum

P2P networks were long known to computer scientists and networking professionals, but they weren't widely employed until the late 1990s Napster case and the 2005 MGM v. Grokster Supreme Court judgment. These developments affected legal professionals, who are now paying greater attention to P2P networks. [6] Their impact extends beyond law to sociology, political science, and economics. P2P systems are seen as widely distributed platforms for storing and retrieving information rather than simple "sharing networks,". [7] Distributed computing uses P2P networks for resource utilization, dependability, and information coverage. [8]

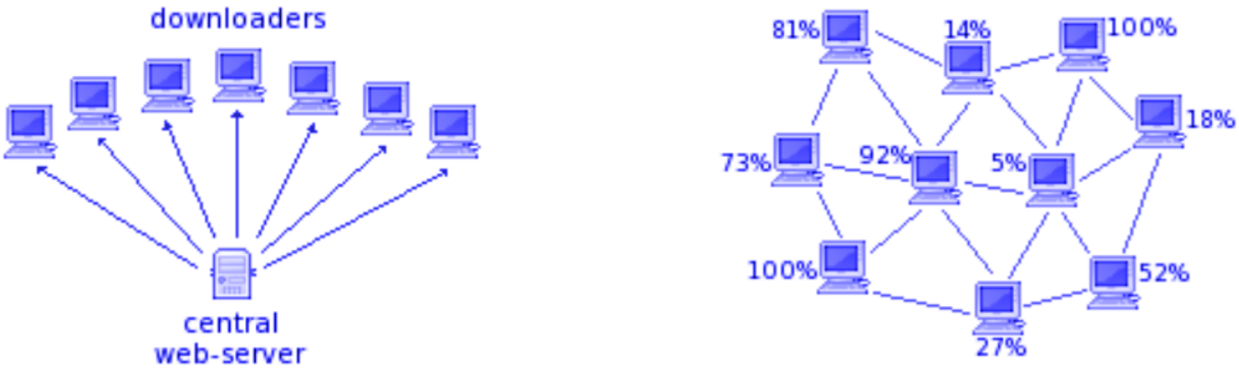
- Shared resources in P2P networks boost computer throughput.
- Without centralized coordinators, P2P networks may operate even if some peers are offline, improving dependability.
- Information Access—The P2P network can link to all Internet computers, providing complete information access. [8]

“Peer-to-peer is a class of applications that take advantage of resources—storage, cycles, content, and human presence—available at the edges of the internet,”. [8] P2P systems and applications leverage decentralized resources to share, compute, and communicate. These systems are usually in ad hoc or web-peripheral networks. [9]

- Low-cost interoperability creates beneficial externalities and increases the total.
- Utilizing existing infrastructure and sharing maintenance costs lowers ownership costs and facilitates cost sharing.
- Such requirements in P2P system design and algorithms and giving peers more control over their resources and data help protect anonymity and privacy. [9]

P2P structures distribute files, as seen in Figure 1. A peer queries its connected peers, who broadcast the request to their peers, to find a file. Unlike the web's client-server design, this lets PCs immediately transfer information without specialized servers. Peers handle irrelevant query packets, making Breadth-First Search (BFS) inefficient. Each peer functions as a server and an end user, along with joining the network by connecting to one or more peers. [8]

Figure 1 - Central Web-server-based Network vs. Decentralized P2P Network (Recreated) [10]



2.1.1 Content Delivery

There are a few different ways that P2P structures are categorized, and one of them is based on how content is shared and accessed. In a P2P structure, clients both offer and utilize resources that are accessible. In contrast to client-server architectures, P2P structures have the ability to distribute more content in response to an increase in the number of users using the system. [11] The details are depicted in Figure 2.

One of the most advanced and flexible content sharing platforms, that excludes malware, ads, and other gimmicks seen in other clients, is Tixati using BitTorrent to let peers share files and download massive amounts of data efficiently. [10]

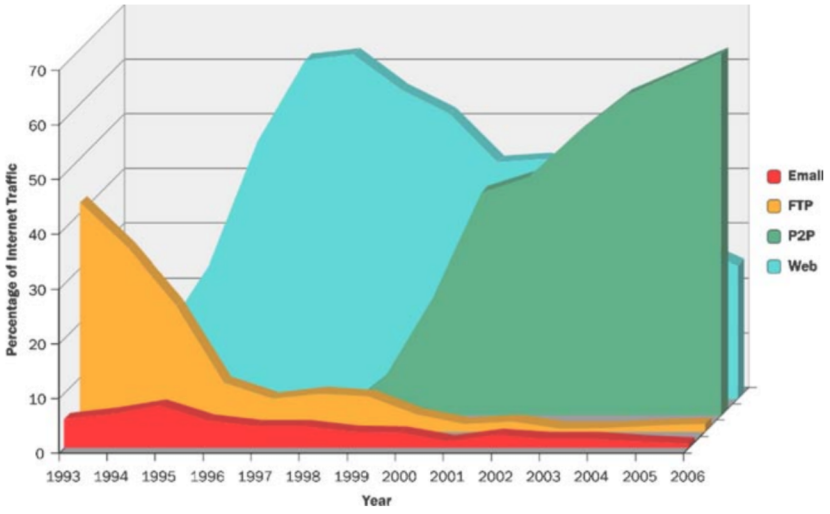


Figure 2 - Increase in P2P traffic [11]

There are now accessible messaging programs such as Briar which deliver content through the utilization of P2P structures. [12] The app is referred to as protected interaction, no matter where, by use of mesh networking. [13] It also boosts secret message insertion bandwidth using a 32-byte random salt and a 24-byte IV, higher than Telegram and Signal messaging apps. [14]

This messaging program was created particularly to serve activists involved in political activities together with journalists, and individuals seeking a secure, dependable, and user-friendly method of interaction. Briar does not possess a server, in comparison to other messaging services. Instead, personal device owners independently exchange messages. [12] It can synchronize through Wi-Fi connections or Bluetooth connections, regardless of whether the internet is present. This guarantees the continued traveling of information during a time of crisis. When connected to the web, it is able to keep pace with the Tor network, shielding users and their interactions against surveillance. [12]

Users must scan each other's QR codes to add contacts. After identities are confirmed, only two devices can communicate using proprietary protocols. Bramble Transport Protocol (BTP) secures data exchange, and Bramble Synchronization Protocol (BSP) synchronizes the communication data between clients. BSP uses offers, messages, and requests to synchronize immutable data across devices. [15]

2.1.2 File Sharing Networks

P2P programs support a wide range of communication protocols., enabling them to support different networks. P2P systems are designed to share content among peers effectively, and some of them also offer searching for information and viewing the files of distant peers. [16] The most common applications as well as protocols for sharing files among peers are outlined in Table 1.

Table 1 - Typical P2P file sharing programs and protocols [17]

Protocol	Applications	Search Support	Browse Support
Gnutella	LimeWire Shareaza BearShare Phex	Yes	Yes
BitTorrent	BitTorrent Vuze LimeWire Shareaza	No	No
eDonkey	eMule Shareaza	Yes	No

2.1.3 Multimedia

Programs for P2P file sharing of multimedia files are the leading contributors to Internet traffic. P2P networks make it feasible to distribute enormous files without a requirement for central infrastructure by combining the power of an array of different computers and other devices into one network. P2P multimedia file sharing structures may use either a tree-based or a data-driven approach when designing their network structure. [18]

2.2 Privacy Violation and Invasive Technology

Few privacy-protecting measures that focus on data sharing rather than data collection are in place to manage the massive amounts of data collected in the U.S. The Constitution grants a limited right to privacy for physical integrity, but information privacy laws are limited. Major data gathering activities in public settings are exempt from privacy torts, and contractual agreements offer minimal protection. Sensor and data aggregation technologies are surpassing privacy-enhancing technologies, and many customers are ignorant of their role in the privacy arms race. [19]

2.2.1 ISP Invasive Privacy History

Protecting privacy from the government is a challenging task, as individuals are often required to disclose private data in order to comply with regulations or fulfill tax obligations without the ability to regulate what data is divulged. This lack of control over personal data makes safeguarding privacy challenging in a government context. [1] According to estimates from Facebook, the government of the United States of America sent in the most applications in 2019. The total amount is 50,714 units. These requests were on a total of 82,461 users and accounts. [20]

Personal data is created, stored, and transmitted in personal devices, ISPs, and websites. Users' choices for anonymity or exposure can still create personal data, leading to complex processes of producing, combining, and selling data that are difficult to understand and control. [21] The use of tailored or flexible advertising gives marketers the ability to target certain audiences, certain demographics, or real-time viewing segments. This may include subscribers in a zip code who are interacting with a program at a specified time or who have watched certain programs before. To reach their target demographic, advertisers might give ISPs names, addresses, and email addresses. Some ISPs offer "cross-screen" services that let advertisers reach consumers on smartphones and TVs. These services depend on the ISP's capacity to link advertising identifiers across devices and identify households using customer data or broker data. [22]

ISPs are a significant privacy concern because they convey and monitor their users' personal information. Recent technological advancements in surveillance have made it simpler for ISPs to violate the privacy of their customers. Advertisers and copyright holders have persuaded ISPs to sell their customers' data, resulting in intrusive surveillance. This is only the beginning of a surge in ISP surveillance that will continue to intensify. [6] ISPs are in an exceptional position to monitor the flow of electronic data, since their networks are the only ones via which traffic can enter or depart the Internet. This gives them a privileged vantage point from which to do so. Using modern packet inspection and capture techniques, ISPs can examine and collect the content of unencrypted traffic. [23]

Ben Wagner compares DPI technology to an automated postal service system. DPI examines, modifies, and retransmits data packets, enabling ISPs to identify and filter online traffic. This includes communications, websites, and activities for sharing files, including the downloading of multimedia and programs. In certain nations, ISPs must use DPI according to the law. [24]

There are instances of ISPs being discovered red-handed. A blog post from August 2007 disclosed an especially intrusive technique employed by the American cable company Comcast. In 2007, Comcast utilized DPI hardware from SandVine to purposefully interrupt P2P traffic as well as slow it down. [25] When this was made public, Comcast stated the practice was limited to high-traffic periods, but this claim was quickly disproven. Widespread media coverage of Comcast's outage resulted in Federal Communications Commission (FCC) complaints and petitions, as well as a class action lawsuit. [26]

The intervention of Comcast affects all types of online content, creating obstacles or impossibilities for BitTorrent users to download pirated music or independent films. P2P traffic accounts for between (50% - 90%) of all traffic on the Internet, much to the chagrin of ISPs. Comcast violates the principle of treating all Internet traffic equally by obstructing the attempts to share files by some of its ultra-fast internet clients. [27]

After criticism, Comcast ceased application-based bandwidth throttling. This event sparked worries about ISPs blocking customer traffic or targeting providers. This helped the network neutrality effort, which culminated in the FCC's August 2008 judgment that Comcast violated consumer rights. Comcast disputed the FCC's power. Net neutrality-supporting Obama FCC policies were suggested. [28]

A company by the name of Phorm promotes a program for a novel approach to offering customized Internet marketing. [29] British ISPs British Telecom, Carphone Warehouse, and Virgin Media intend to collaborate with Phorm in order to target advertisements based on the browsing behavior of users. Phorm will reconfigure ISPs' servers to analyze and classify user-visited web pages into distinct advertising channels. [30] If a user frequently visits travel-related websites, they will observe more travel-related advertisements on Phorm-affiliated

websites. Virsb Vahidi, the chief operating officer of Phorm, declared that they could classify all Internet activities as clients browse, and they have had access to the entirety of the Internet. [31]

More views are generated by behavior-targeted advertisements, which increases revenue for ISPs like Phorm and hosting sites. British Telecom alone is estimated to earn £87 million per year. The prospective profits are substantial. The Investigatory Powers Act of 2016 enables the British government to develop a new surveillance system and database that grants authorities access to monitor online activities, including Internet Connection Records (ICR), even in the absence of criminal suspicion. [32]

2.2.2 VPN Awareness and Statistics

Since the year 2020, VPN awareness has dramatically increased, and use cases have shifted. During National Cybersecurity Awareness Month (NCSAM), a study revealed that the American populace's familiarity with VPNs is developing. Approximately (90%) of adults correctly identified VPNs as remote encrypted gateways that enhance online security and privacy by shielding internet activity from hackers, trackers, and censors. This indicates an increase in the previous year's already remarkable numbers. [33]

Despite increased familiarity with VPN solutions, the data revealed that their utilization has not increased over the past year, with usage rates between 2021 and 2022 remaining virtually identical. COVID-19's precipitous transition to a universal work-from-home economy led to a substantial increase in business VPN usage. This requirement for extensive remote network access positioned VPNs as the most reliable solution. As a result of the return of many employees to their offices (and their secure Internet connections), however, a significant number of organizations no longer require expanded VPN access. [33]

Regardless of whether VPNs were used for personal or professional purposes, or both, the study uncovered significant information regarding VPN usage. Males were observed to manifest a greater propensity for VPN usage than females. (57%) of males used VPNs for personal use, compared to, (43%) of females; (28%) of VPN users were between the ages of 45 and 60; and

(40%) used VPNs to protect their data and privacy. One-third used VPNs to reduce hazards on free wireless networks, while one-third used them for work. [34]

US and UK VPNs must share consumer data with law enforcement. Importantly, an order to remain silent may be included, so you may not discover the privacy danger until it's too late. IPVanish, a prominent US VPN, sent user data to the Federal Bureau of Investigation (FBI) in 2016 despite its no-logs policy. Riseup, a US VPN/email firm, complied with two warrants for user data under gag order. After denying government encryption keys, Lavabit closed in 2013. Ironically, Snowden was investigated. UK VPN provider HideMyAss openly shares user data with the authorities. [35] The 1946 Agreement allowed UK and US intelligence services to exchange intercepted interactions. Australia, Canada, and New Zealand joined "Five Eyes" within a decade. This cooperation was crucial in aiding allied activities during World War II, monitoring nuclear arsenals during the Cold War, and tracking terrorist cells after 9/11. [36]

2.2.3 DPI Surveillance Framework

DPI surveillance technologies are a form of communication surveillance that facilitates the monitoring of content data by tracing Internet network traffic and its associated data at all seven levels of the OSI Reference Model. [37] DPI has positive applications, but it raises significant privacy concerns. When combined with data from other sources, DPI can be used to create detailed user and online activity profiles. This information can be used to target advertisements, manipulate individuals, and restrict their online freedom of expression. [38] The details are depicted in Figure 3.

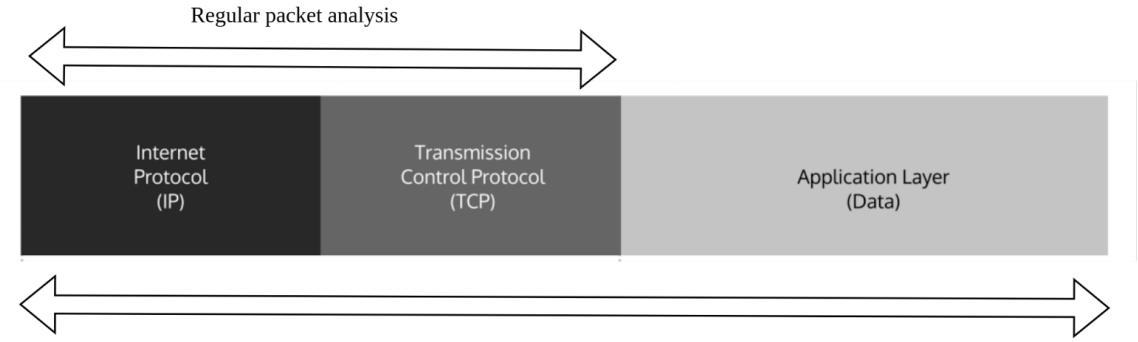


Figure 3 - Deep Packet Inspection [Recreated Graph] [38]

Deep packet inspection allows administrators to analyze both the payload and header of IP packets. Regular expressions are used by DPI systems to identify patterns of relevance in network data streams. The equipment is configured to determine how to manage a packet or a stream of packets based on the identification of a regular expression or pattern within the payload. Consequently, networks can classify and regulate traffic based on its content, applications, and subscribers. [28]

Network surveillance questions, the old ISP responsibility dispute. Section 230 of the Communications Decency Act (CDA) and Section 512 of the Digital Millennium Copyright Act (DMCA) restrict US and European ISPs' responsibility for user behavior. ISPs are protected, but must follow a notice and takedown process for infringing content. ISPs' data liability is limited under the European E-Commerce Directive's safe harbor. Under Article 15 of the Directive, Member States cannot require ISPs to monitor their networks for illicit activities. [39]

DPI engine examines packet payloads in real time. DPI manipulates and alerts bit streams. Notification alerts, records, or billing issues without disrupting traffic, whereas manipulation actively alters a live traffic stream based on rule sets. Mueller Copyright DPI is tricky. Since 2005, copyright holders have pressured ISPs to restrict Internet users from using DPI to optimize bandwidth or market services. DPI tracks digital copyrights. DPI must calculate unique perceptual properties to distinguish copyrighted information in fragments and diverse media formats or compression levels, unlike virus detection, and compare media fingerprints to registered fingerprints to identify copyright breaches. [39]

DPI-free copyright: Copyright holders employ DPI's fingerprint-matching technology for "over-the-top" (OTT) monitoring. ISPs must match IP addresses to accounts and inform, restrict, or terminate guilty users. ISPs inform, block, and disconnect users using DPI and OTT. Table 2 contrasts DPI-based and French "graduated response" copyright enforcement. DPI-free copyright enforcement is possible. [39]

Table 2 - Copyright Enforcement Modes on the Internet (Recreated Table) [39]

Activity	Status quo	Hybrid (OTT)	Inside the Network (DPI)
Detection	Rights holder	Rights holder	ISP
Mapping	Rights holder subpoenas ISP	Government agency and ISP	ISP
Notification	Rights holder	Government agency with ISP	ISP
Enforcement	Court system	Government agency Courts and/or ISP	ISP

The DPI technology is rapidly becoming an essential part of the supporting infrastructure of the World Wide Web, where it is being incorporated as part of the technical stack. In addition to being capable of doing real-time analysis and differentiation of the flow of data that is being transferred over the internet, it is also capable of merging a broad variety of characteristics into a single device. This technology can be beneficial to a wide range of companies, including governments, network operators, content suppliers, and ISPs. The fact that the parties engaged have interests in the fields of politics, economics, and technology accordingly brings all three of these spheres into play, which is a direct effect of the fact that the parties involved have interests in those fields. [40]

These tables highlight the myriad of parameters that have an influence on the monitoring, management, and classification of internet traffic, as well as the antiquated technologies that an integrated DPI system may be able to replace with more efficacy in the future. [40] The data are shown in their entirety in Table 3, which is found further down.

Table 3 - Monitoring variables and technologies an integrated DPI system may replace

Purpose	**Old**	**New**	**Drivers**
lawful interception, surveillance	TCPdump, Wireshark, dsniff etc. (store & analyze)	DPI (analyze packets and make decisions in real-time)	police, intelligence community
content regulation	blocking based on DNS, IP#, URL	hash-based blocking or surveillance	efforts against hate-speech, child-porn, political censorship
copyright enforcement	DRM Lawsuits	hash-based filtering	content industry
bandwidth management	TCP congestion management, QoS	application-based routing	ISPs: last mile over-subscription, P2P and video traffic
subscriber management	pay per minute, pay per volume	differentiated services and pricing	ISPs: heterogenous user behaviour and user needs in context of bandwidth scarcity
network security	stateful firewalls, asynchronous monitoring (TCPDump etc.)	content-based real-time monitoring	corporate network operators; anti-spam and malware efforts by ISPs
vertical integration	product tying	block or discriminate competing services	video on demand, integrated phone & internet providers, triple play.
behavioural-based advertising	cookies (website owners)	ad injection	ISPs, ad networks

The utilization of DPI for bandwidth control makes it feasible for a service provider to change the behavior of margin-operated applications and services, which has an immediate influence on the idea of end-to-end connectivity. Some people are concerned that ISPs will have unique points of view on their customers and the services they supply, which will inhibit competition and innovation. Others argue that network providers, who are obliged to make considerable and occasionally risky investments in bandwidth, have the right and the need to limit their capacity in light of the fact that demand for bandwidth continues to exceed supply. This is because network providers are required to make significant expenditures on bandwidth. The huge amount of conversation that has taken place surrounding the neutrality of networks is indicative of how critical this modification is. [41]

2.2.4 DPI Peer-to-Peer Detection

P2P traffic is identified via DPI, deep flow inspection (DFI), port-based approaches, and combinations of these methods. The port-based technique assumes P2P clients use TCP and/or UDP ports to send data and messages. Recent P2P clients employ user-defined ports, random ports, modified ports, or camouflage ports to circumvent the port identification mechanism, making this method ineffective. DPI detects P2P packets using packet signatures and content. DFI can detect P2P packets using TCP flow characteristics like packet size and bytes sent. Finally, combining the strategies will increase detection. [42]

1. The first method uses TCP or UDP. This method assumes P2P programs communicate with peers on devices through fixed ports. Its simplicity and low computing load are advantages. Traffic identification based on port may also quickly and easily eliminate well-known non-P2P programs like File Transfer Protocol (FTP) and E-Mail and specifically identify P2P applications like eMule and BitTorrent. Since most P2P programs employ new technologies like user specified ports, random ports, changeable ports, and camouflage ports to prevent port detection software. Thus, the port-based approach is obsolete. [42]

2. DPI, the second discovery method, uses packet content. This detection system will look for P2P data properties. P2P software's handshaking signals often match. They have a few application layer functionalities. BitTorrent's algorithm illustrates that "BitTorrentprotocol" always occurs in their handshakes. This DPI approach is accurate and well-executed, yet it has downsides. The payload must be verified before enabling encryption. Second, examining the payload's data creates privacy problems. Protocols evolve, hence the P2P protocol's signature may change. Finally, open-source software is hard to analyze. Closed-source software often faces additional challenges. [42]

3. DFI exploits network movement to detect P2P activities. P2P data is evaluated using a flow-based methodology, focusing on connection-level use patterns of P2P programs. It requires no data analysis, unlike DPI. Payload analysis is unnecessary for encrypted data

streams. This method's shortcoming is that it takes an additional step to generate P2P traffic connection level patterns. This approach has no standard network function. [42]

2.2.5 Peer-to-Peer Application Obfuscation

P2P cryptography has two views. Encrypting user data is the first step in securing the P2P protocol from ISPs and others. Encrypting shared data allows only the intended receiver to decode it. The second strategy prevents "free-loading" users from utilizing P2P networks. [43]

Diffie-Helman key exchanges were used to encrypt P2P data. The kind of data can be determined using this sort of encryption, but not the content. Users must encrypt packets to avoid DPI. The protocol flow may be identified. Each form of Internet application layer data traffic has a unique flow, including packet destination and source, packet size, packet orientation, and communication length. Prying eyes may utilize these properties to determine data transit between parties. Statistical Protocol Identification (SPID) uses a statistical model to recognize user protocols, including P2P, streaming, and VoIP. Users must conceal their information flow and encrypt their traffic. [43]

Diffie-Helman exchanging key was used to disguise P2P data. Encrypting packets may defeat DPI. However, prying eyes may still discern the kind of data communication between two parties utilizing unique data flow features and Statistical Protocol Identification (SPID). To improve privacy and security, users must encrypt and conceal their data flow. [43]

For encrypting and hiding a P2P client, packet data is initially encrypted utilizing a shared random password to fool DPI devices. The padding message is designed to lower the statistical chance of identifying the BitTorrent protocol flow. These additional signals increase packet variability, avoiding SPID. Thirdly, random flashes increase packet size and variation to avoid SPID. A unique peer ID informs sharing peers that communication is encrypted and disguised. If the peer cannot handle obfuscation, they must reconnect and complete sharing in plain text. The provided method won't entirely hide the protocol type, since packet frequency is not changed. It does hide the protocol type from most protocol identification methods. [43]

"Trick before Treating" encodes every bit of data to minimize "free-riders" in P2P networks. If most network users are free riders, "capacity per user" decreases. Seeders that utilize Trick before Treatment must encrypt their file pieces before sharing them. Users must submit certain sections to neighbors for a subkey to decrypt them. The first seeder gave parasites who downloaded file fragments a subkey. Decrypting file portions requires n and k subkeys. To decrypt the file, users would have to transfer their own file portions to other users, forcing them to engage in the network and eliminating most free-riders. [43]

2.2.6 Privacy Invasion and ISP DPI by the Regime in Iran

A poll of Alexa's top websites assessed Iran's censorship. The top 500 websites from each of the 18 Alexa categories using a crawler were requested. As predicted, adult websites were the most restricted, with almost 95% prohibited. Over 50% of the Top 500 websites were blocked. Art was restricted third after society and news. DNS hijacking affected just Facebook.com, YouTube.com, and plus.google.com domains. Iran-accessed websites failed frequently. Most of these websites were in U.S.-sanctioned areas like banking (bankofamerica.com) and technology (nvidia.com), and several blocked Iranian IP addresses. [44] Figure 4 shows these findings.

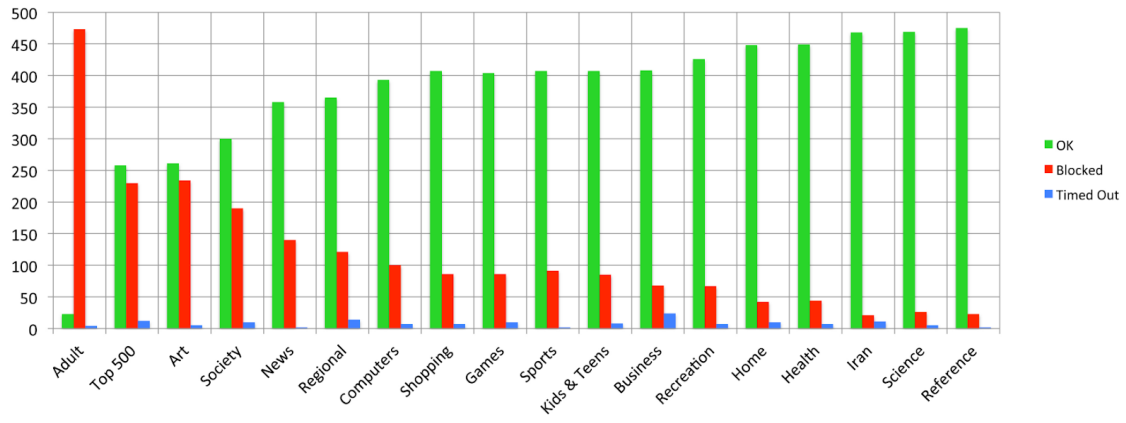


Figure 4 - Alexa's top websites assessed Iran's censorship [44]

When the regime’s police chief in Iran, Ahmadi Moghaddam, boasted in January 2010 that "the new technologies allow us to identify conspirators and lawbreakers without having to control every individual," he likely understood the impact of his words, even if he exaggerated his abilities. Each detention of a blogger, whether based on genuine surveillance practices, reports

from the public, or random means, functions as a deterrent to subversive action, particularly among those who are not full-time dissidents. [45]

One apparent application of face-recognition technology would be to enable the regime’s authorities to rapidly identify protesters photographed in Tehran. [45] The regime promptly blocked access to the proxies used by its opponents during the 2009 rallies, many of which were tweeted by unknowing Westerners, Face-recognition technology might help police in Iran to identify protesters in Tehran swiftly. [45]

The United Nations Rapporteur's August 2014 assessment found that regulations and procedures continue to unduly constrain freedom of expression and information. In the month of June 2014, Reporters sans Frontières (RSF) stated that Iran's freedom of information had not been improved since the moderate conservative president took office in June 2013. RSF additionally stated that the justice system and government intelligence agencies continued to persecute journalists. [46], [1]

The International Campaign for Human Rights in Iran (ICHRI) which is located in New York [47], [2] states: security and intelligence agency hardliners are persecuting activists, and that Rouhani's inauguration has boosted online activist arrests. [46], [48], [49], [50], The UN United Nations Human Rights Council points out that through the years 2009 and 2013, the government suspended 35 press media outlets, delivered 106 warnings, and terminated 11 and 1 news organization licenses. The Regime closed 14 news outlets from June 2013 to June 2014. [46]

Users in Iran have to experiment with hundreds of different applications and VPNs before they can discover a method to get past the limitations imposed by their ISPs, while most people in the rest of the world see access to the Internet as a given. And although some VPNs are phony or banned, there are others, like the 20Speed VPN, that are intentionally packed with malware. These VPNs are not to be trusted. When the user downloads the filter-breaking file, spyware of this kind is allowed to reach the computer of the victim. [51]

Technology specialists within and outside Iran said Iran's Internet content monitoring had gone beyond blocking websites or terminating Internet connections. The government's response to political unrest appears to be Deep Packet Inspection. This technology allows authorities to impede, monitor, and influence communication to gather personal data and propagate misinformation. [52] In the aggregate Top 500 category, more than fifty percent of the Internet's most popular websites were blocked. Surprisingly, art was the third most censored category, after society and news. [52]

Internet access has purportedly been cut off in parts of Tehran and Kurdistan, and social media platforms such as Instagram and WhatsApp have been blocked by authorities in an effort to suppress the escalating protest movement. After the death of a 22-year-old Kurdish woman, named Mahsa Amini, perished in the hands of police on16th of September 2022, demonstrations extended to numerous locations. Police stations and cars were burned by the demonstrators. [53]

Simultaneously, Footage of women flaming their headscarves have gained traction on social media platforms as anti-regime demonstrations have migrated online. In protest, women have uploaded videos of themselves trimming their heads in solidarity with Amini, who was allegedly detained for inadequately wearing her hijab. The hashtag #Mahsa_Amini has been used to gain additional traction and support for the movement. [53]

While authorities deny that Amini was critically struck in the head while in custody, her family believes that she was brutally beaten and tortured, which ultimately led to her perishing. An inquiry has been initiated to ascertain the reason(s) behind her passing away. The current internet shutdown and social media blockades imposed by the government highlight the intensified tensions and repression faced by dissidents in the country. [53] Since then, weekly executions by the authorities have been taking place. [54] [55]

Consider a surveillance system that examines each Internet packet to determine whether it is suitable for transmission or malevolent. As a consequence of the high volume of internet packages, they are queued for inspection, resulting in a decrease in overall access speed. [56]

The Islamic regime in Iran has a long tradition of using various types of social media in order to advance its political agenda. In the year 2022, Iranian protestors claimed that Instagram's censors were censoring postings that were critical of the leadership in Iran. An ex-employee of a German business working for Instagram has stated that the government in Iran security apparatus allegedly made a financial offer to him in exchange for him deleting certain accounts. [57]

The individual, who requested anonymity like the current moderator, was employed by Telus International, a third-party company entrusted with managing Instagram and Facebook user reports and complaints. "A reviewer may independently delete a post that has been flagged without facing serious repercussions," he explained. [58]

3. Anti-Surveillance Solutions

This section will offer an overview of the most up-to-date technologies that are applied in VPN solutions for the security of users from monitoring by ISPs. Multi-Hop and Obfuscation, Bypassing Traffic Shaping, Port Hopping, Dynamic IP address, DNS Leak Protection, Split Tunneling, Kill Switch, and Distributed and Decentralized Network Architecture are some of the technologies that fall under this category.

3.1 VPN Protection Technologies Evading ISP P2P DPI Surveillance

Data is rerouted when a VPN is utilized, while flowing via the VPN server before returning and is secured using two approaches, and encrypted during transmission. The user's IP address is hidden, preventing prying eyes from accessing it and the destination server from establishing its origin. Data is safeguarded and delivered to the user's device by reversing the steps. [59]

VPNs times out when the latency is increased tremendously, since a basic OpenVPN configuration works for a few minutes. After identifying VPN TCP/UDP connections using heuristics, the Great Firewall (GFW) drops all traffic. One Hacker News member noted that the only option to manually hide VPN traffic is to disguise it as HTTPS. [60] P2P traffic is converted to HTTP to facilitate caching through widely deployed web cache proxies used by enterprises and ISPs. This method achieves similar results to dedicated P2P caches without the cost. By "HTTPifying," data is segmented into files or streams into chunks, utilizing HTTP protocol to transfer them, and ensuring these chunks are cacheable. [61]

3.1.1 Multi-Hop and Obfuscation

"Hop" refers to the process of routing data via a number of intermediate servers in VPNs. Double-hop authentication uses two servers to transfer data between its origin and destination, unlike single-hop VPNs. "Double VPN" is the same as "multi-hop VPN," allowing customers to send data over more than two servers. Hops hide the surfing data's content, but not its volume. Even with many VPN hops, ISPs may monitor data transmission. VPNs may not avoid ISP data use limits. [59]

The information is encrypted on the client's device first, and afterwards, it is encrypted one more time, it is encrypted before being sent to the initial VPN server, and in a multi-hop, the server placed as the first gets the protected information. After being transmitted to the second server, the encrypted information is decrypted by removing the first layer of encryption. Data is decrypted and sent to the final server/destination. [18] The details of the described process are depicted in Figure 5.

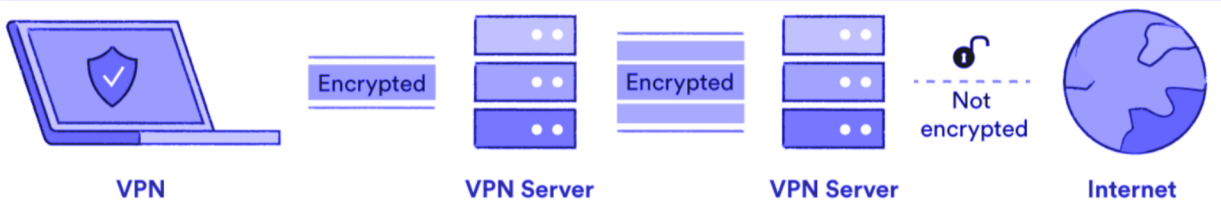


Figure 5 - Double Hop VPN [62]

It is possible for obfuscated servers to bypass VPN firewalls. It is the responsibility of the VPN provider to strip any information pertaining to the VPN from the user data and then transform it into standard data packets. This protects data from being stolen. Encryption protocols like SSL and SSH are utilized by VPN providers in order to safeguard data packets and VPN-related information. This functions in a manner analogous to that of cryptographic encryption. Data scrambling can make it more difficult to decipher information from the packet header. This creates the appearance of a typical HTTPS transaction containing random data, which firewalls are unable to identify and hence provide access to the resource. It is possible for VPN constraints imposed by private networks, service providers, and nations to be circumvented using encryption-based methods. Once the connection has been made, a VPN blocker or firewall will no longer be able to recognize VPN traffic. [63]

Obfuscated VPN servers conceal themselves in a variety of ways. VPN protocols conceal uniquely. Attempts are made by censorship regimes to identify and prohibit all forms of camouflaged VPNs. This range of options may appear complex, but it allows consumers to select a different option if their initial choice does not meet the requirements. Common methods for utilizing an obfuscated VPN include Tor Bridge, ShadowSocks, OpenVPN, Scrambled/SSH,

Obfuscated VPN Hosting on VPS (Virtual Private Servers), and paying a nominal subscription fee to a reputable service provider. [64]

3.1.2 Bypassing Traffic Shaping and Port Hopping

The practice of traffic shaping belongs to the field of Quality of service (QoS), and it is a method which is applied to interfaces of the network. High-priority traffic is accelerated during network congestion. Shaping the traffic gives higher priority to the transmission of critical data packets by reducing the amount of available bandwidth for low-priority packets. This decreases the risk of delayed vital data packets or lost when they are being transmitted out of the interface. [65]

DPI has certain disadvantages, such as the fact that P2P apps might masquerade as interactive ones, which calls for more complex DPI methods. P2P apps, on the other hand, strengthen their users' anonymity by encrypting their data, resulting in a continuous battle. It is possible that DPI is just a stopgap measure, and what is really required for resource allocation is an architectural strategy that is better suited. [66] The details are depicted in Figure 6.

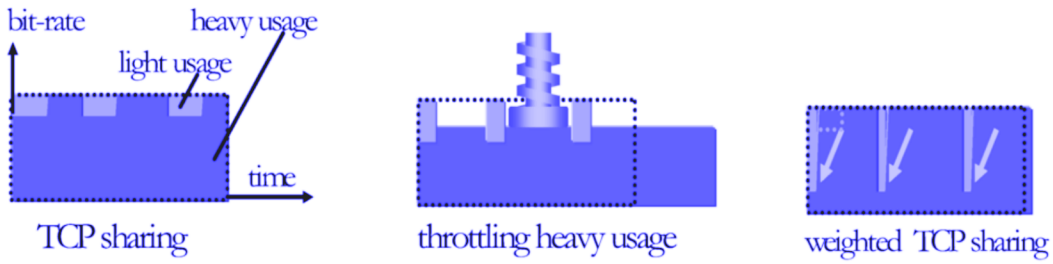


Figure 6 - Resource sharing. Left: TCP sharing (base case). Middle: Limit volume (DPI). Right: Limit congestion volume (Recreated) [37]

Using a VPN secures the connection between the user's computer and the VPN provider's servers. So, the data is fully secured while it is traveling through the ISP, and the ISP can't tell what services or data are being sent by the user in order to shape the traffic. [39] The original packet is repackaged in a way that keeps its IP address secret and uses a new IP address. The protected file is then sent straight to the VPN server for delivery, identification, and decoding at

the target. This process makes the link constant, encrypted, and untraceable. The only thing the ISP can see is an encrypted connection. [67]

Port/Address hopping dynamically changes a service's IP address and TCP port to hide its actual identity and confound attackers during reconnaissance. TCP messages have a source, a destination address and port. Higher-level Distributed Object Computing (DOC) protocols like IIOP include TCP information in object references. IP Port hopping involves replacing the source and destination ports with random ones and diverting traffic. Address hopping requires random address changes. Intruders intercept packets with temporary addresses, such as one minute. ISPs must identify and scan current ports within one refresh cycle to find them. [68]

Network communications have long associated port numbers with applications or services. HTTP traffic utilizes port 80, and DNS traffic port 53. However, owing to obfuscation measures like changeable port numbers and port hopping in certain apps, these traditional standards are less reliable for identifying programs. The port-based technique can detect (30%–70%) of Internet activity, according to recent research. [68], [69]

The Network Address Translation (NAT) gateway and hopping delegate client component work hand in hand. The client machine or process hosts the hopping delegate. It intercepts client-to-server Remote Procedure Call (RPC) calls and replaces all (realaddress:realport) header data with (fakeaddress:fakeport). The server's LAN or host's NAT gateway reverse maps (fakeaddress:fakeport) to (realaddress:realport). The (fakeaddress:fakeport) combination is randomly picked from a range of IP addresses and ports and utilized for a cycle period before being generated and used again. Stale pairs are retained to detect suspect communication. This approach relies on synchronizing random number generators across components. This process takes place when both generators are seeded the same value. Time synchronization is also needed to switch to a freshly created (fakeaddress:fakeport) pair. Two use cases yielded two designs and implementations: [67] Figure 7 shows the main components of the hopping mechanism and their roles.

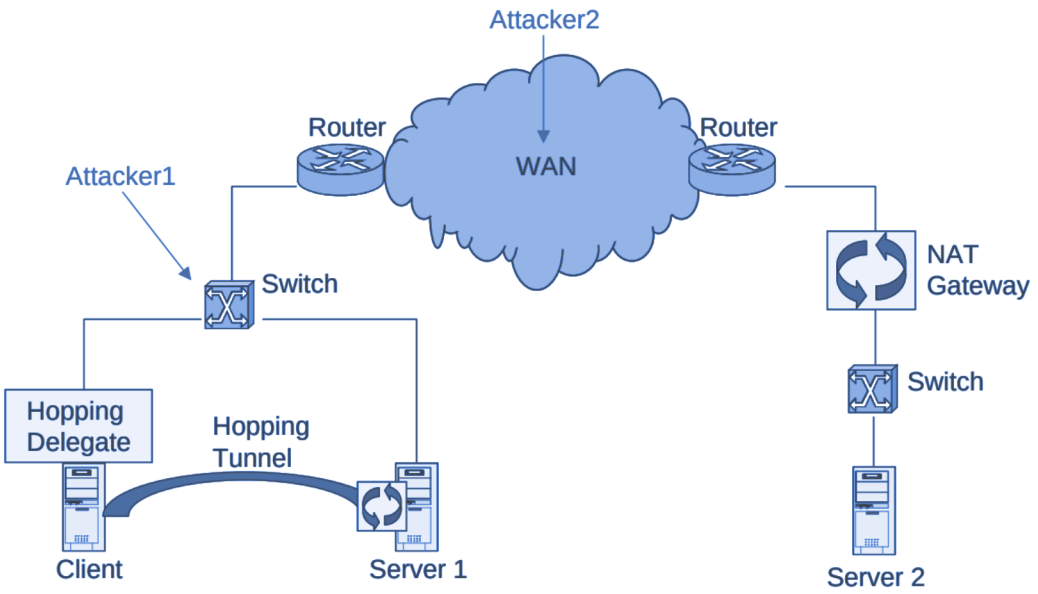


Figure 7 - Two designs for implementing port and address hopping (Recreated) [67]

Two distinct Adaptive Port Obfuscation Defense (APOD) use cases and their respective implementations are described. In the first use case, both the client and server share the same IP network, and their communication does not involve any routers. To avoid detection from Attacker1, the client's delegate redirects traffic to Server1 through a tunnel, altering the server-side and possibly client-side ports of the tunnel at random intervals. APOD's adaptive defense is limited to port jumping in this scenario. [67]

In the second use scenario, the client and server are on separate IP networks; thus, the client component changes the destination address of packets meant for Server2 to a random IP address in the same IP network and selects a random port. The NAT gateway sends the packet to Server2. Server2 replies to the client are again passed via the NAT gateway to adapt their source IP address and port to the random selection. Attacker1 and Attacker2 can only view client-to-random IP addresses and ports in this case. If needed, an identical NAT gateway on the client's LAN may further obscure the client's IP address and port, so Attacker2 only sees communication between random hosts in the two LANs. [67] Port hopping as a defense mechanism against application-based intrusion is insufficient against attacks targeting protocols

below TCP/UDP, including ICMP. IP Randomization techniques may be utilized to counteract these and other types of intrusions. [70]

3.1.3 Dynamic IP address and DNS Leak Protection

A Software-Defined Networking (SDN) controller manages IP-addresses traffic between network devices using network randomization. The network-layer device first validates source-destination pairings and then installs rules for encoding/decoding randomized IP addresses. These rules may be static, random, or pushed by a trustworthy third-party. Importantly, the IP Address-Randomizer may be installed without changing the communicating endpoint processes. [70]

Dynamic IP randomization and port hopping approaches maintain connectivity among two hosts , but reactive IP address randomization has a greater performance impact than port hopper. For low-bandwidth applications like Supervisory Control and Data Acquisition (SCADA), Reactive IP address randomization preserves resources and flow-rules by employing them only when necessary for communication, and systems that need larger bandwidth and are intolerant to delay may employ proactive IP address randomization. [70]

Tor hides the user's IPs using a Virtual Anonymous Network (VAN) while the VPN gives anonymous IP addresses to transparently anonymize IP-based network communication. Because every host needs client-side software and a VPN encryption key, this solution may not scale well. An SDN-based strategy may be more effective since it integrates this solution into the network, decreasing the pressure on larger scale networks. To reduce damage from concentrated reconnaissance attacks, the goal is to prevent an adversary from learning the IP addresses and port identifiers for network-based service implementations. [70]

DNS leaks expose VPN users' browsing activity and location to their ISPs. All VPN services depend on the OS routing table setup, which is not checked for changes, compromising security. VPN clients may disregard the IPv6 routing table, circumventing the VPN. IPv6 traffic makes this crucial. Common operating system IPv4/6 dual stack implementations cause the vulnerability. These implementations favor IPv6 over the VPN connection when available. IPv6

is preferred because IPv4 VPN tunnel overheads delay resolution. IPv6 leakage occurs because all IPv6 traffic leaves the host through the native network interface. [71], [72] The details are depicted in Figure 8.

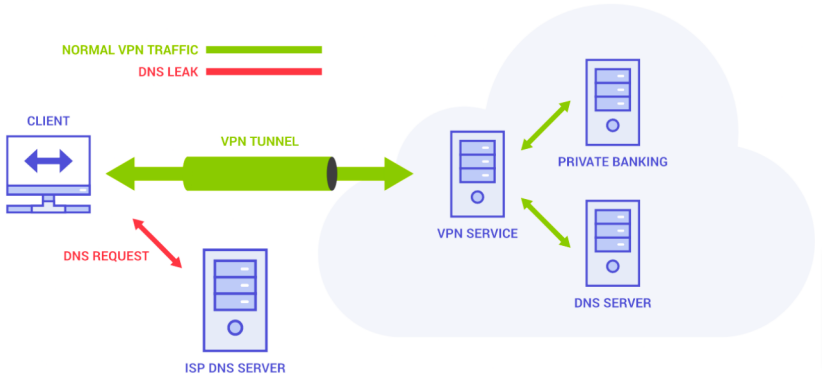


Figure 8 - DNS requests are leaked [73]

There are several circumstances that may result in a DNS compromise, including:

1. Most frequently, DNS intrusions are a consequence of improper VPN configuration, which assigns a client's ISP DNS server. This is inclined to occur when clients frequently switch between networks.
2. A VPN service without its own DNS servers is unable to detect DNS breaches effectively.
3. IPv6-unsupported VPNs route DNS queries outside the encrypted channel.
4. Some ISPs use transparent DNS proxies, which can result in DNS breaches by redirecting users' web activity to their own DNS servers, even if they use a third-party VPN and alter their DNS settings. [71]
5. Windows 8 and subsequent OS systems' Smart Multi-Homed Name Resolution (SMHNR) capability transmits DNS queries to accessible servers and accepts the first responding DNS server, which might leak DNS and leave users open to spoofing attacks. [71]
6. Windows Teredo: Windows Teredo helps convert IPv4 to IPv6, however it may override the VPN tunnel, compromising VPN security. [71]

3.1.4 Split Tunneling and Kill Switch

Users of VPNs have the ability to guide the flow of web traffic through either an encrypted VPN tunnel or a conventional network tunnel, thanks to a feature known as split tunneling. The use of VPNs enables users to achieve this capability. By implementing this feature, users are given the authority to choose which data transactions or apps should be encrypted securely and which ones should not be protected. Users have the chance to select which data transactions or applications should be encrypted securely and which ones should not be protected. Users also have the power to determine which ones should not be protected by the system, and the system will take into consideration the decisions that users make in this regard. The user is given the opportunity to pick the VPN service provider that is best equipped to satisfy the specifications that the user has selected for their connection when split tunneling is put into action. These parameters can be customized by the user. [74]

Split tunneling techniques differ. Users are able to encrypt particular web addresses employing a VPN with the assistance of uniform resource locator-based split tunneling. This is a goal that VPN browser add-ons can achieve. Users are able to select which programs connect via their VPN versus those that join over their local network when using application-based split tunneling. Inverted split tunneling operates differently. As opposed to defaulting to an open network and allowing users to determine which setting they would prefer, inverted split tunneling directs any communication via the VPN by default. Users are able to decide which apps and sites should not use the VPN by applying this feature. [74]

To enable transparent transmission over a public network whilst using a VPN, a tunneling approach encapsulates one protocol (protocol X) inside another (protocol Y). Protocol X is shown to enclose protocol Y in Figure 9, which depicts the protocol architecture of a VPN, which is implemented via tunneling. Encapsulating IP requires the use of IP tunneling protocols that include GRE, L2TP, IPSec, and IP/IP. These are all examples of IP tunneling technologies. Due to the fact that certain protocols for tunneling are not VPN-specific, it is possible that they will not satisfy all the clients’ VPN installation requirements. [75]

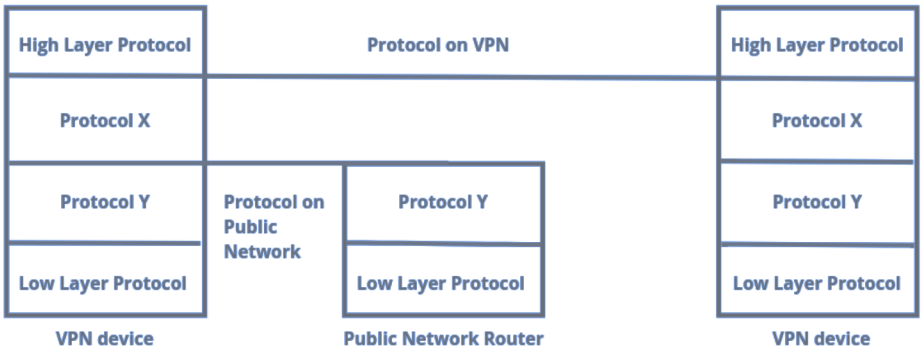


Figure 9 - The Protocol Architecture of VPN [75] [76] (Recreated)

In case of tunnel failure, VPNs' "kill switch" avoids traffic leakage. In the event of a VPN malfunction, the connectivity to the internet on all associated devices is disrupted. This guarantees that your actual IP address remains concealed. [77] This service safeguards user data against cyberattacks. Since kill-switches determine VPN protection, their default state is under examination. To safeguard users from security breaches, VPNs should be tested for tunnel failure robustness. [75] Some VPN providers allow customers to transport their encrypted VPN communications across Tor. This feature prevents VPN logging and Tor exit assaults. This feature has severe performance costs that may influence user experience. The functioning of the kill switch feature is illustrated in Figure 10. [78]

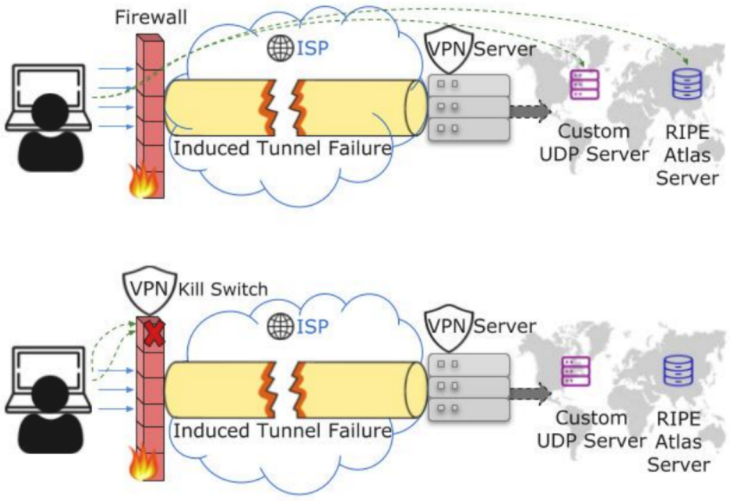


Figure 10 - VPN kill switch feature is disabled [78]

3.1.5 Distributed, Decentralized Network Architecture

Customers of VPNs desire privacy, but centralized VPNs may have a significant problem. There must be confidence that VPN providers will not intercept or record user communications. VPN providers are enterprises that may use various cloud services for global expansion. Thus, even reputable merchants may be unaware of provider issues such as surveillance, misconfiguration, and malware. These vulnerabilities may pose a risk to user privacy. [79]

A network that is distributed is a collection of independently managed independent structures. Typically, these structures are located in various geographic locations to improve reliability and provide numerous access points for enhanced performance. This architecture allows the networks to interact with one another for service redundancy, performance gains, and the automated exchange of resources. Although these structures operate independently, their administration and supervision are centralized, allowing for uniform policies and end-to-end visibility. [80]

It is necessary to assess centrally managed structures as well as distributed structures to determine how to design networks and application solutions. In a conventional client-server design, endpoints are linked to a specific piece of software or asset via a centralized infrastructure architecture. Centrally managed networks may lack backup for network-based applications and servers during a significant outage. In a distributed structure construction, networks and clusters of servers interact with one another and a centrally managed server. [80]

VPNs have been structures of networks that have been managed centrally, which are used as links between dispersed staff for older remote protocols. All remote clients connected to a solitary VPN head-end that was placed near the organizations' perimeter. This established a single spot of malfunction for the entire network to fail. The availability and stability of networks and applications are enhanced by distributed structures. [80]

Both types of structures exchange information and responsibilities at particular points. Networks that are decentralized collaborate on problems, procedures, and data storage structures that are decentralized are mutually reliant on one another and are unable to function alone, which necessitates the participation of dispersed networks. [80]

Administration of distributed structures complicates system-wide security and policy enforcement, but it may also improve resilience and defect tolerance in the face of unanticipated malfunctions or attacks. Decentralized structures, on the other hand, lack a central control interface for managing the system. Instead, each function is managed independently. [80]

Structures that are managed centrally or in a non-central way, as well as distributed ones, generally have their own distinct pros and cons. In an architecture managed in a central way, every single one of the servers is linked to a central structure so that they are able to interact with other servers. A non-centrally managed structure organizes its server clusters in accordance with the purpose of the applications or services they host, as well as the geographic location of those servers' assets. The distributed network layout uses autonomous nodes grouped in a dense mesh to ensure both the network's stability and its high level of efficiency. The visualization of designs may be aided by the use of network diagrams like the one shown in Figure 11. [80]

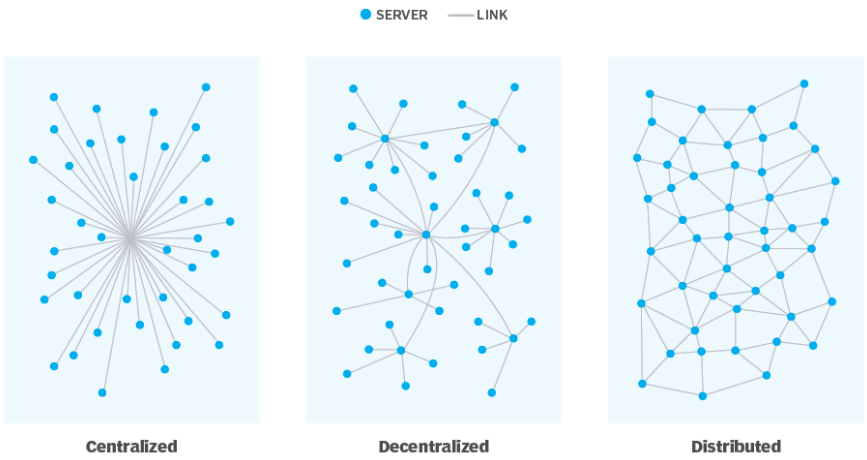


Figure 11 - Centralized, decentralized, and distributed structures. [80]

In an empirical examination of the commercial VPN ecosystem, research [81], conducted an investigation into sixty-two commercial VPN operators. The findings of the study highlighted many issues linked to the non-logging policies of the providers. Modification of client traffic as well as differences between the claimed and real locations of VPN nodes However, upon learning of the concerns, all service providers took rapid action to remedy the misconfigurations that were

revealed. This was despite the fact that the authors observed that some VPN provider misconduct was due to erroneous setups rather than malicious activities. [79]

Decentralized Virtual Private Networks, or dVPNs, feature a new kind of VPN that doesn't have a centralized authority. In a dVPN, each user acts as both a VPN client and a relay exit node, analogous to a P2P network. dVPNs provide safety for users' privacy, but using them comes with several potential dangers. There have been several findings that point to the possibility that a user's workstation may unknowingly broadcast unlawful or harmful network traffic [82]. As a result, dVPNs need to undergo exhaustive testing before being put into operation. [82]

Decentralized virtual private networks may more easily manage network space, address allocation, and discovery with the use of structured overlays and Distributed Hash Tables (DHTs). Each IPOP (IP-over-P2P) group has its own namespace in order to prevent several VPNs from coexisting inside the same overlay. This is made possible by the structured overlay, which guarantees that every VPN peer has a P2P address. [83]

Peers store IP-to-P2P address mappings in the DHT for scalable and decentralized address allocation and discovery. Hash(namespace + IP) = P2P address is the usual mapping. Peers place this (key, value) pair into the overlay when allocating addresses. The first peer gets the IP address. The DHT must enable atomic writes. [83]

Dynamic Host Configuration Protocol (DHCP), manual IP address setting, or VPN integration with OS APIs may self-configure the local system's IP address and network specifications. VPN software starts address discovery when a remote peer's outgoing packet arrives. The VPN searches the DHT using the IP address to get the owner's P2P address and passes the packet. [83]

To summarize, file sharing through P2P networks is common. However, this method might jeopardize users' privacy and security; thus, it's important to utilize a VPN tailored for safe P2P use. Consider the following requirements to fully protect VPNs from Internet Service Providers' P2P DPI. [84]

1. P2P sharing is more efficient and secure with a VPN with P2P-optimized servers. [85] [84]
2. A kill switch and threat protection are essential for preventing data breaches and mitigating potential security threats. In addition, the VPN must be equipped with strong encryption technology, such as AES-256, to protect both the security and privacy of data transmitted during P2P file sharing. [86], [84], [87]
3. Additionally, VPNs must have fast tunneling protocols, obfuscated servers, and RAM-only servers, as these characteristics can accelerate downloads and increase security. [88], [84]
4. P2P file sharing requires a no-logging policy and an independent data privacy and security audit. [89], [84]
5. P2P file-sharing is more reliable and faster when facilitated by VPNs that support port forwarding. [90], [84]

Selecting a VPN service that offers specialized P2P servers, strong security, robust encryption, fast tunneling, obfuscated RAM-only servers, no-logs, audit, and port forwarding capability is essential for ensuring a secure and efficient P2P sharing experience and protecting against ISP P2P DPI. [91], [84], [92]

The following is a list of notable VPNs that are designed to protect users from P2P data collection strategies utilized by ISPs. The incorporation of these VPNs, often known as VPNs, is dependent on their ongoing support from 10 distinct technical websites. This illustrates not just their prevalence, but also how effective they are in avoiding the dangers associated with DPI. These five VPNs were compiled from several websites that cover a wide range of technology topics. Some of these websites include, but are not limited to, the following: The details are depicted in Table 4.

Table 4 - Technical websites listing VPNs for evading P2P ISP DPI

[https://www.top10vpn.com] [93]	[https://en.cybernews.com][84]
[https://www.pcworld.com] [94]	[https://www.security.org][95]
[https://www.internetsecurity.org][96]	[https://uk.pcmag.com][97]
[https://www.vpnranks.com][98]	[https://restoreprivacy.com/][99]
[https://www.techradar.com][100]	[https://www.vpnmentor.com/][101]

3.2. Reports on Notable VPNs for ISP P2P DPI Protection

This compilation of reviews on notable VPNs was put together with the purpose of offering a complete overview of the features, capabilities, and security given by a number of VPN solutions. The reviews cover a wide range of VPNs, from those that are free to those that cost a lot of money. These reports were compiled using information that was gathered from a broad variety of trustworthy sources and sourced appropriately.

3.2.1 NordVPN

The founder of Nord Security, Tomas Okmanas also developed Lithuania's second tech unicorn, NordVPN in 2012. [102] NordVPN does not join the Five Eyes, which is the longest-running multinational arrangement after NATO, [103] or the Fourteen Eyes, which is prolonging the United Kingdom and United States of America Agreement (UKUSA) [35] alliances. The company has facilities in several countries, including Panama, whose laws are not in conflict with the company's policies, making it an ideal location for the VPN's servers. [104], [105], [106] Details are in Table 5.

Table 5 - Technical analysis of NordVPN features

Multi Hop	Yes [107]
Obfuscation	Yes [62]
Bypassing Traffic Shaping	Yes [108]
Port hopping	Yes [90]
Dynamic IP address	Yes [109]
Split Tunneling	Yes [110]
DNS leak protection	Yes [111]
P2P Decentralized	No (Meshnet) [112]
P2P servers	Yes [113]
Fast Tunneling Protocols	Yes (OpenVPN, IKEv2/IPsec, WireGuard) [114]
Encryption	AES-256 [115]
RAM-only Servers	Yes [116]
No-Logs Policy	Yes [117]
Kill switch	Yes [118]

3.2.2 ExpressVPN

A British Virgin Islands-based enterprise offering a VPN service. The software encrypts online communications and hides IPs to protect clients' confidentiality and security. Kape Technologies is the owner of the company, a four-million-user VPN, as of September 2021. [119] The provider revealed in April 2019 that the servers used RAM instead of hard disks. After powering down the server, the corporation claims all data is lost. Rebooting the server recreates the VPN architecture, making it new. [119], [120] The details are depicted in Table 6.

Table 6 - Technical analysis of ExpressVPN features

Multi Hop	No [119]
Obfuscation	Yes [121]
Bypassing Traffic Shaping	Yes [122]
Port hopping	No
Dynamic IP address	Yes [123]
Split Tunneling	Yes [124]
DNS leak protection	Yes [125]
Decentralized	No
P2P servers	No
Fast Tunneling Protocols	Yes (Lightway, OpenVPN, IKEv2, L2TP/IPsec, PPTP) [126]
Encryption	AES-256 [127]
RAM-only Servers	Yes [128] [129]
No-Logs Policy	Yes [89]
Kill switch	Yes [130]

3.2.3 CyberGhost

CyberGhost SA administers CyberGhost VPN from its corporate office in Romania, in the city of Bucharest. IPSec, L2TP/IPSec, PPTP, WireGuard, and OpenVPN are utilized with Windows, Android, macOS, and iOS proprietary software. Due to the company's controversial reputation, its purchase was critiqued. In the month of March 2018, following this merger, it ended up being Kape Technologies assets. The business's main offices are located in Tel Aviv, Israel, and it has divisions in London, Nicosia, and a number of other cities. To advertise its brand, Kape Technologies holds ZenMate and Private Internet Access. [131], [132] The details are depicted in Table 7.

Table 7 - Technical analysis of CyberGhost features

Multi Hop	No
Obfuscation	No
Bypassing Traffic Shaping	Yes [133]
Port hopping	No
Dynamic IP address	Yes [134]
Split Tunneling	Yes [135]
DNS leak protection	Yes [136]
Decentralized	No
P2P servers	No
Fast Tunneling Protocols	Yes (OpenVPN, IKEv2/IPsec, WireGuard) [137]
Encryption	AES-256 [138]
[139]RAM-only Servers	Yes [139]
No-Logs Policy	Yes [132]
Kill Switch	Yes [140]

3.2.4 Surfshark

The name "Surfshark" refers to a VPN that has its headquarters in the European nation of the Netherlands. The combination of Nord Security and Surfshark took place in 2021, however the two firms remained functioning separately. The organization is able to do hidden searches, check for data leaks, and offer VPN services. By making use of the GPS-Spoofing function, users have the ability to disguise their specific location by relocating to one of the server's locations. It utilizes WireGuard, IKEv2, OpenVPN, tunneling technologies. AES-256-GCM is used for protecting all the data that is sent between clients and servers. [141]

The details are depicted in Table 8.

Table 8 - Technical analysis of Surfshark features

Multi Hop	Yes [142]
Obfuscation	Yes [143]
Bypassing Traffic Shaping	Yes [144]
Port hopping	Yes [145]
Dynamic IP address	Yes [146]
Split Tunneling	Yes [147]
DNS leak protection	Yes [148]
Decentralized	No
P2P servers	Yes [149]
Tunneling Protocols	Yes (OpenVPN, IKEv2, WireGuard) [150]
Encryption	AES-256 [151]
RAM-only Servers	Yes [152]
No-Logs Policy	Yes [153]
Kill Switch	Yes [154]

3.2.5 Private Internet Access

The year 2010 saw the beginning of Andrew Lee's venture with London Trust Media, which would later become known as Private PIA after undergoing a name change. Lee started this firm with the goal of furthering the cause of ensuring people's privacy when using the internet, and he has succeeded in doing so. As a direct result of the efforts put forth by PIA, the client software used by PIA to power its next-generation VPN has had its underlying source code made freely accessible to the general public. After Kape Technologies completed the acquisition of PIA, the firm came to the conclusion that it was important to reassure its customers that the protection of their personally identifiable information and financial data would continue to be its primary focus. [155], [156] The details are depicted in Table 9.

Table 9 - Technical analysis of Private Internet Access features

Multi Hop	Yes [157]
Obfuscation	No
Bypassing Traffic Shaping	Yes [158]
Port hopping	Yes [159]
Dynamic IP address	Yes [160]
Split Tunneling	Yes [161]
DNS leak protection	Yes [162]
Decentralized	No
P2P servers	No
Fast Tunneling Protocols	Yes (OpenVPN, WireGuard) [163]
Encryption	AES-256 [163]
RAM-only Servers	Yes [156]
No-Logs Policy	Yes [164]
Kill Switch	Yes [165]

4. Analysis of Technologies, VPN Solutions, and Reviews in P2P Networks

This analysis will investigate the effectiveness of VPN solutions in preventing ISPs from conducting DPI and monitoring P2P user activity. It will also identify the most important technologies to take into consideration when selecting a VPN solution for content distribution through P2P networks. It will evaluate user opinions and technological reviews to determine which VPN service is best for distributing content. Finally, it recommends the most appropriate solutions for P2P users to circumvent ISPs' DPI.

4.1 Anti-Surveillance Technologies Analysis for VPNs

The comparative analysis is utilized to identify the essential anti-surveillance technologies for VPN systems that offer protection against ISP DPI for P2P activities. These technologies include:

1. Encrypting: The Advanced Encryption Standard, sometimes shortened as simply AES, is an encoding scheme that is currently being employed in numerous VPN solutions. AES, is a kind of protection technique that employs keys that are symmetric, usually encode and decode content making use of a key that has a specific length. It is well-established that the aforementioned encrypted approach, it has an ideal key bit size of 256 bits, is one of the most secure, and it is being utilized in the current day and is one of the approaches applied. These innovations provide integrity, privacy, and identification, all of these are crucial aspects of private communication and are offered by these advancements. [166]

2. Tunneling : VPN solutions are required to utilize tunneling methods that include IPSec and SSL/TLS. These technologies make it more difficult for DPI to detect and analyze traffic by assisting to encapsulate and encrypt communication. VPN solutions tend to employ protocols known as OpenVPN, IPSec, and the Secure Sockets Layer (SSL) protocols. OpenVPN is almost universally regarded as the finest protocol due to its open-source nature, adaptability, and sturdiness. The aforementioned IPSec mechanism suite, on the other hand, is a suite of protocols that offers an extensive collection of safety parameters for VPNs. Cryptography, identification, and key management are included in the aforementioned safety features. SSL, the protocol most commonly used to secure

online transactions, is also a popular option for VPNs due to its simplicity of setup and compatibility with the vast majority of web browsers. [76]

3. Obfuscation Technology: It is possible to further improve VPN systems by using obfuscation methods such as domain fronting and onion routing, which make it more difficult for DPI to identify VPN traffic. These technologies assist in masking the real destination and source of traffic, making it more difficult for DPI to recognize VPN connections and therefore restrict them. [62]

VPN solutions for P2P ISP DPI security require VPN protocols (such as OpenVPN and WireGuard), encryption algorithms (such as AES), tunneling technologies (such as IPSec and SSL/TLS), and obfuscation techniques (such as domain fronting and onion routing). The use of such technologies is necessary for VPN solutions. By collaborating, these technologies not only make it more difficult for DPI to detect and block VPN traffic, but they also ensure that conversations are kept private and cannot be overheard by unauthorized parties. [166], [76], [62]

4.2 Technical Analysis of the VPN Solutions

It is essential to maintain one's objectivity and abstain from supporting any particular VPN service provider in order to avoid seeming biased. In spite of this, it is possible to draw the conclusion that NordVPN offers solid privacy and security features by taking into consideration the information that has been offered in the studies about significant VPN solutions. These characteristics include a strict no-logs policy, superior encryption, and compatibility with numerous protocols. The following is a comparison and study of the five VPN services, with an emphasis on why NordVPN is the superior option: [167]

NordVPN: It is a VPN service that is well-known. It provides exceptional security features in addition to quick connection speeds. NordVPN offers a large and dependable network that gives clients access to content from all around the globe. The company has over 5,400 servers located in 59 different countries. Your online actions will be kept private and safe thanks to NordVPN's stringent no-logs policy. This VPN is notorious for refusing to comply with unreasonable requests from authorities. [168] Moreover, this VPN provider does not participate in

intelligence-sharing alliances, distinguishing it from other VPN providers. [169], [115], [113], [112], [111], [118], [110], [107], [170],

ExpressVPN: As a widely acclaimed VPN company offering the highest-ranking privacy protections in addition to blazing-fast connectivity. It supplies clients with a broad network that is perfect for getting access to content from practically everywhere, as it has servers in place in over ninety-four nation-states all over the entire globe. The pricing is much higher compared to that of NordVPN. Due to its location in the British Virgin Islands (BVI), it is not subject to Fourteen Eyes Alliance jurisdiction. [171], [172], [173], [119], [174], [175], [176], [177], [125], [178]

CyberGhost: A service that is simple to use as a VPN, friendly to one's budget, offers fast connectivity, and offers strong encryption. It provides users with connections to a vast network that is fantastic for accessing material from all over the world. The company's servers can be found in more than ninety different nations. On the other hand, its customer support does not react to inquiries as rapidly as NordVPN does, and it does not offer nearly as many sophisticated security characteristics as NordVPN does. [140], [179], [132], [139], [135], [136], [180], [132], [179]

Private Internet Access: It is a VPN that is available to consumers on a shoestring budget. It offers rapid connection speeds in addition to strong encryption, making it an attractive option for clients. PIA offers a stable network for accessing information from all corners of the world, and this is made possible by the fact that the servers can be found in more than seventy-eight different regions. Conversely, Private Internet Access has had some problems in the past with its logging policy, and as a result, it is considered to have a lower level of trustworthiness compared to NordVPN. [181], [164], [156], [163], [161], [160], [182], [163], [164]

Surfshark: A VPN service offering connections with high speeds in addition to powerful, secure encryption. The trustworthy network provided by Surfshark is an excellent resource in order to access information originating from anywhere. More than sixty-five nations are represented by the location of the company's servers. Conversely, the VPN in question lacks the advanced security features that are available with NordVPN. Additionally, it may not be as reliable as other

VPNs that have been in operation for a longer duration. [152], [150], [149], [183], [144], [145], [151], [143], [154]

Our research revealed that NordVPN is the ideal choice for consumers since it offers a large and trustworthy network, cutting-edge security measures, and a strong no-logs policy. These features make it the clear winner among the rest. In addition to this, it offers fast connection speeds and affordable costs.

4.3 Analysis of VPNs vs. ISP DPI Surveillance in Iran

An in-depth study on the utilization of VPNs and DPI on the part of ISPs has been carried out both inside and outside of Iran. It has been discovered that, due to the tight measures implemented by the regime in Iran, VPN obfuscation technology proved to be an efficient method for bypassing VPN bans. This discovery was made, because this technology conceals VPN protocols from inspection, it makes it impossible for ISPs to track VPN usage.

Encryption and tunneling are two other critical components that must be included in a VPN to ensure that data remains secure when the VPN connection is suddenly lost. In addition, a kill switch is required in order to prevent any data from being transmitted until a VPN connection has been successfully recovered. [52], [53], [46], [44]

ISPs in Iran have a reputation for decreasing their users' bandwidth and weakening transmissions by slowing down the speed and bandwidth, which makes it harder for individuals to interact with one another. [52] It is important to note that ISPs in Iran have a history of engaging in such activities, particularly during times of political upheaval. As a result, a dependable VPN needs to be able to function despite the limitations of such low bandwidth and speed.

The primary purposes served by ISPs making use of DPI in nations such as the UK are those of traffic shaping and protecting intellectual property rights. However, in Iran, the majority of DPI use is political, and the purpose of this usage is to conduct surveillance on users in order to determine whether their interactions with the outside world are in line with the regime's goals. As a result, it is vital to bear in mind a VPN provider that has a no-logging policy in order to

guarantee that the data will not be purchased by any third party that is affected by the mentioned government. [56]

There is a significant danger in making use of the applications offered by large technology companies, since these companies are continuously pressured to provide data to various governments. Assuming there is 1% chance of getting compromised, It is not a good idea to utilize Meta's products because of the company's reputation and the way it provides information to various government agencies [184], [185] and involving third party moderators. [186], [187], [58] Instead, political activists should think about employing decentralized P2P applications for content distribution, particularly when it comes to messaging app usage. [12] It is essential to understand that the absence of a centralized authority over the network enables these apps to deliver improved levels of security and privacy to their users. [20]

VPN users should avoid ISPs that employ transparent DNS proxies, as this practice may lead to DNS breaches by redirecting user traffic to the ISP's DNS servers. It should be noted that even if users use third-party VPNs and adjust their DNS settings, their DNS may still be compromised if the ISP in question uses transparent DNS proxies. [71]

4.4 Analysis of End-User Interviews

As part of the analysis, a comprehensive review of numerous VPN service providers was carried out. Ten specialized websites, which served as the primary sources of data for this research, were consulted in order to identify the VPN service providers that were suggested the most frequently. In the following steps, the VPNs that provide the highest level of protection against ISP P2P DPI techniques were discovered. [170], [176], [132], [188], [101], [156]

A curated list of VPNs and their applicable features that are especially beneficial in lowering the risks connected with P2P DPI tactics utilized by ISPs is the result of the in-depth study that was conducted. People who seek to improve their security and privacy online by utilizing P2P networks may find this list highly useful. In addition, the list is utilized in an interview setting with individuals who use any of these VPN services for P2P sharing activities. This provides the

interviewees with essential protection against DPI-related hazards imposed by their respective ISPs.

The interviews were conducted to gather information about the viability of using VPNs for the distribution of P2P content despite the presence of ISP protection, the primary factors that go into the selection of such VPNs, and the respondents' concerns about privacy protection while using P2P networks. The findings are analyzed in this section of the survey, which is devoted to the analysis, and repeating patterns and trends are identified.

4.4.1 Demographics

The majority of those who took part in this survey were men (63.4%). [189] This conclusion is consistent with previous research that has repeatedly shown that young guys have a heightened inclination for the use of VPNs [129]. This result is consistent with prior research, since it is consistent with these results. Furthermore, many of the participants were young, (61.0%) of the individuals were between 18 and 30 years old, while (34.1%) were between 30 and 40 years old. The fact that students made up more than half of those who participated in the survey (61.0% of the total) may be indicative of a heightened knowledge and security and confidentiality concerns regarding their usage of the internet within this specific population. These heightened levels of awareness are most likely the result of the substantial media attention that has been dedicated to cybersecurity concerns in recent years, as well as a better familiarity with internet technology among younger folks. [190]

4.4.2 Results

When it comes to using P2P content distribution systems without the support of VPNs, the results of the interviews that were done for the purpose of this research reveal that respondents have a significant worry for ensuring that their information is kept private. Despite this, the overwhelming majority of participants were pleased with the performance of their VPN-based solutions for P2P content distribution. The encryption protocol AES-256, Dynamic IP, fast tunneling protocols, a no-logs policy, DNS leak protection, and obfuscation were thought to be the most important features for VPNs to have in order to effectively support the requirements for content delivery. These results clearly imply that VPN providers need to prioritize offering

dependable and trustworthy services that focus on user privacy, in addition to delivering fast speeds at a reasonable price point, in order to properly respond to the needs of their audience. [190], [189] The details are depicted in Figure 12.

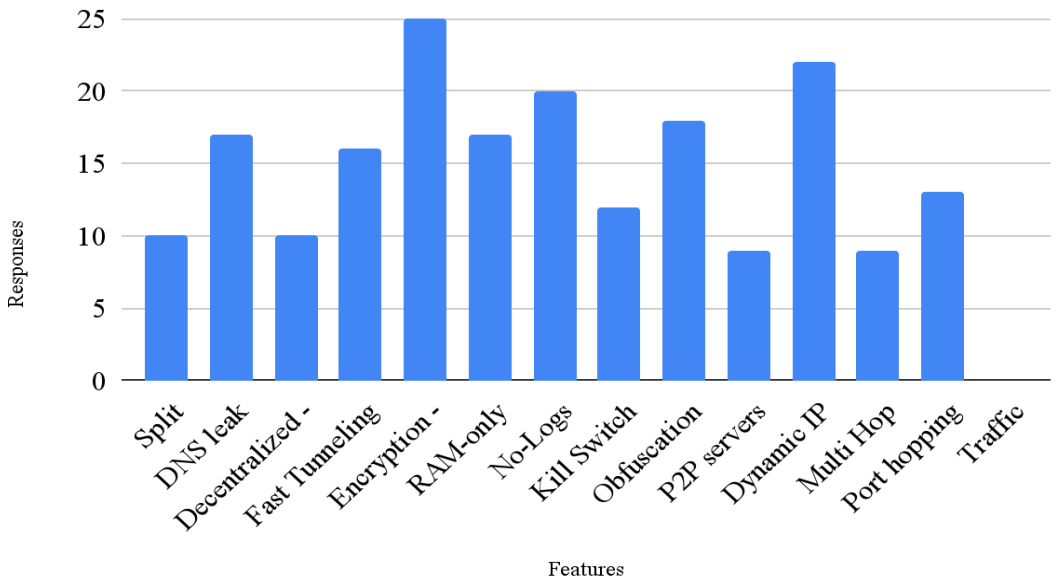


Figure 12 - VPN features priority. [190], [189]

According to the results of our poll, the most popular reasons for utilizing a VPN were to protect one's privacy (40%), get around geographical restrictions (36%), defend oneself against hackers (24%), and enable work-related activities (12%). The conclusions of this research are consistent with the findings of other studies, which demonstrated that worries about one's safety and privacy online are the primary motivators for using a VPN. [16] However, just 24.0 percent of those asked acknowledged utilizing a VPN as a protective measure against hacking. This provides evidence that there may be a need for more awareness and education on the risks associated with hacking and the advantages of using a VPN as a form of security. [191] [192]

A finding that emerged as very pertinent was the fact that when questioned, the majority of respondents (51.2%) claimed that they were concerned about their Internet service provider compromising their privacy while utilizing P2P material sharing without a VPN, which is (19.2%) higher than (32%) of American ISP users have carefully perused their ISP's privacy policy as a sign of concern that their privacy has been compromised. [193], [189] This finding

came about as a result of the fact that the majority of respondents indicated that they were concerned about their ISP breaching their privacy. This highlights the need for adopting a VPN for the purpose of protecting one's privacy and avoiding interference by ISPs. On the other hand, only (34.1%) of respondents reported using a VPN for less than a year. This suggests that there is still a need for more education and understanding about the benefits of utilizing VPNs for protecting one's privacy and identity when using an ISP. [190], [189]. The details are depicted in Figure 13.

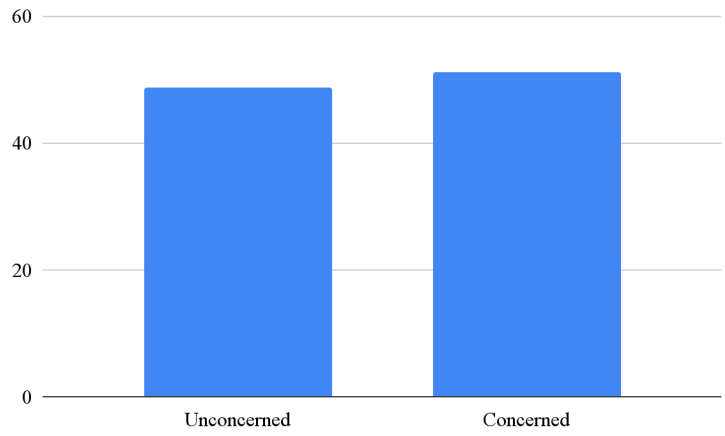


Figure 13 - Concern about ISP privacy invasion when using P2P content delivery [190], [189]

According to the findings of the poll, a large percentage (58.5%) of all respondents, thought that their Internet service provider was intruding into their private life. On the other side, (41.5%) of respondents were under the impression that their Internet service provider was not engaging in intrusive conduct. These results highlight the importance of further education and awareness-raising initiatives to be taken in order to educate customers about the intrusive activities of ISPs. [190], [189] The details are depicted in Figure 14.

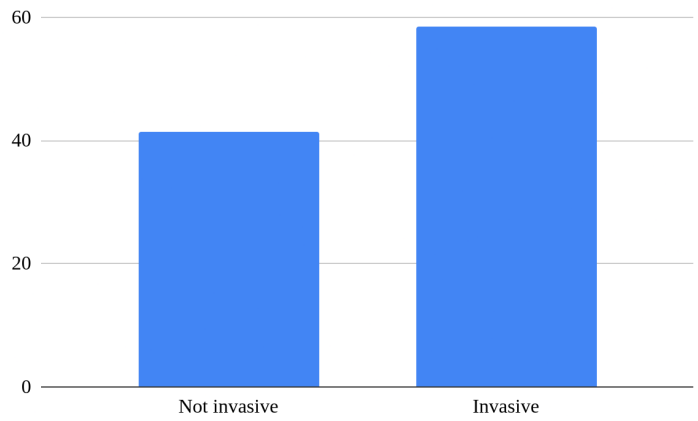


Figure 14 - User rating for ISP invasiveness [190], [189]

According to the results of the research, (56.1%) of respondents, had no previous experience with problems relevant to cybersecurity, whilst a considerably smaller percentage (19.5%) of respondents claimed to have substantial competence in this sector. This conclusion highlights the need for enhanced education and understanding about the challenges and recommended practices around cybersecurity, especially among those who may be less acquainted with these ideas. [190], [189] The details are depicted in Figure 15.

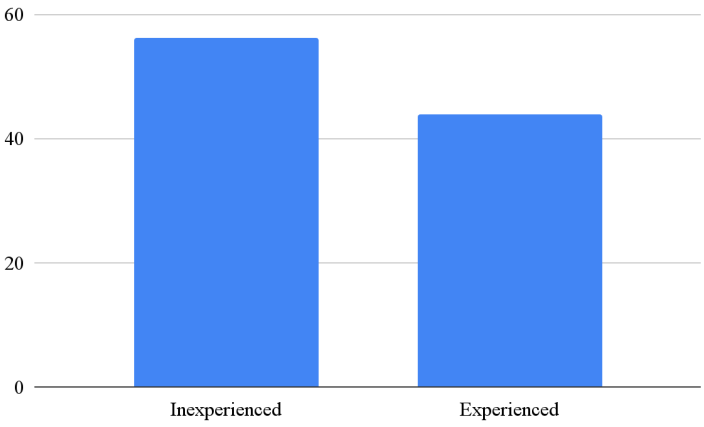


Figure 15 - User cybersecurity experience [190], [189]

ExpressVPN was the virtual private network that was used by the respondents most of the time (29.3%), followed by NordVPN (26.8%), and Private Internet Access (17.1%). The outcomes of the poll are shown below. In addition, there were additional VPNs utilized at the same rate as PIA, which brings the total to 100%. Many participants considered their VPN solution to be "very effective" (22.5%), with an additional 67.5% stating that it was "effective," and just 10% claiming that it was "not effective." In addition, a large percentage of respondents (87.8%) were of the opinion that the VPN solution they were using provided an appropriate level of protection against ISP DPI while they were utilizing P2P networks. According to these results, ExpressVPN, NordVPN, and PIA are the main competitors in the VPN market for ensuring privacy and security, particularly when it comes to defending against intrusive tactics by ISPs. PIA is also a strong contender in this market. [100], [93], [94], [96], [190], [189] The details are depicted in Figures 16, Figure 17 and Figure 18.

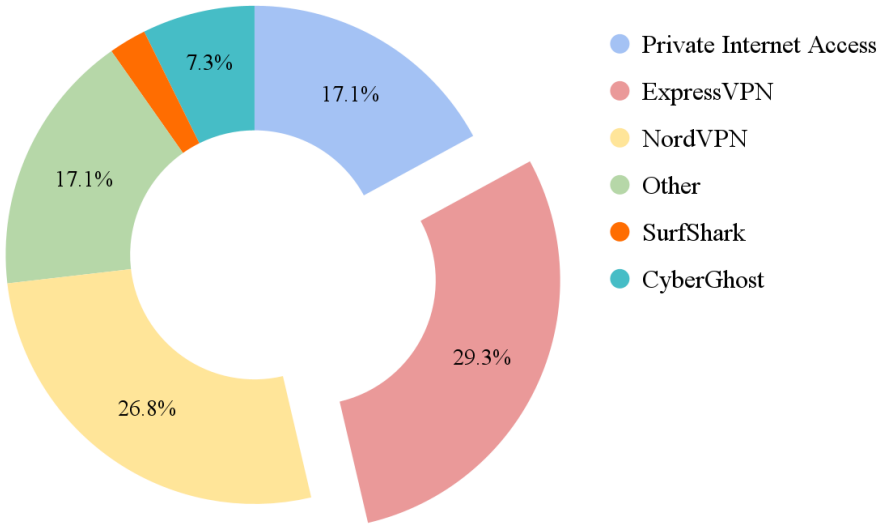


Figure 16 - VPN usage for P2P content delivery [190], [189]

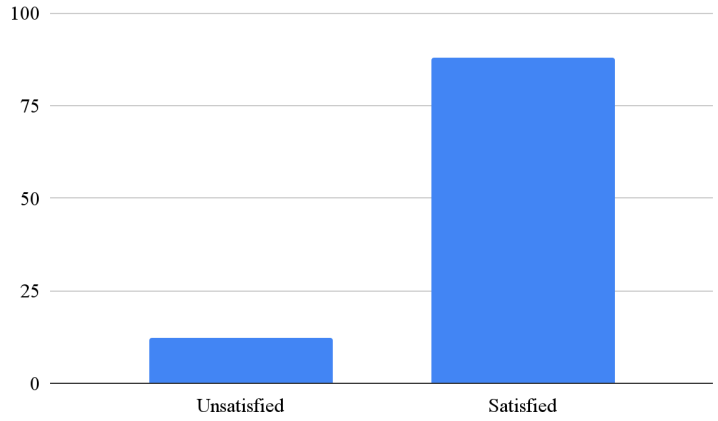


Figure 17 - User satisfaction for VPN solution for P2P content delivery [190], [189]

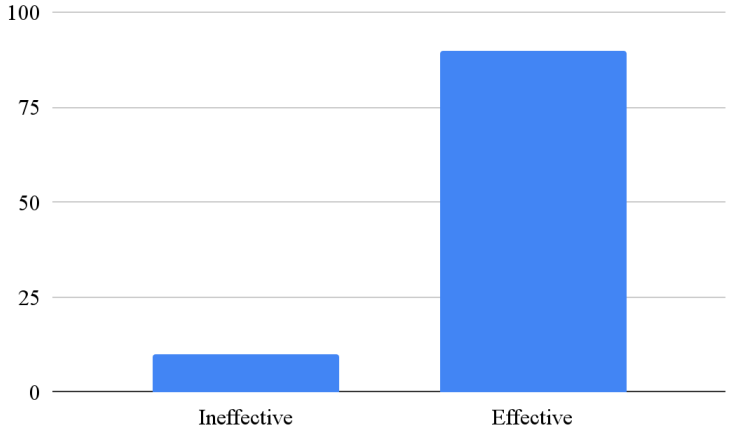


Figure 18 - User assessment of VPN solution P2P content distribution. [190], [189]

Concerns about the constitutionality of P2P content delivery, the need for education about VPNs and the numerous advantages they offer, and the importance of selecting a dependable and trustworthy VPN vendor were common themes in the comments section. These topics highlight the need for greater education and awareness regarding online security and confidentiality, as well as the benefits of adopting VPNs for safeguarding one's privacy and shielding themselves from their ISP.

According to the results of the study, Estonia had the greatest percentage of participants with 34.1%, followed by Iran (19.5%), and Turkey (12.2%). As a result of the political context in Iran, it is quite conceivable that people from Iran were particularly concerned with concealing their identities in order to prevent their names from being added to a list of political prisoners in the future. This is because of the political situation in Iran, which made the interviews be conducted in an anonymous manner. [48]

Throughout the entirety of the procedure, the interviews were carried out in a manner that ensured the participants' right to maintain their privacy. [2], [4] In perilous circumstances such as this one, the utilization of a VPN is very necessary. This is evidence that those individuals who wish to engage with the rest of the world in a free and secure manner, despite the possibility that their own governments will place restrictions on such interactions, will likely have a high demand for the best VPNs that were utilized by participants. [190], [189] The details are depicted in Figure 19.

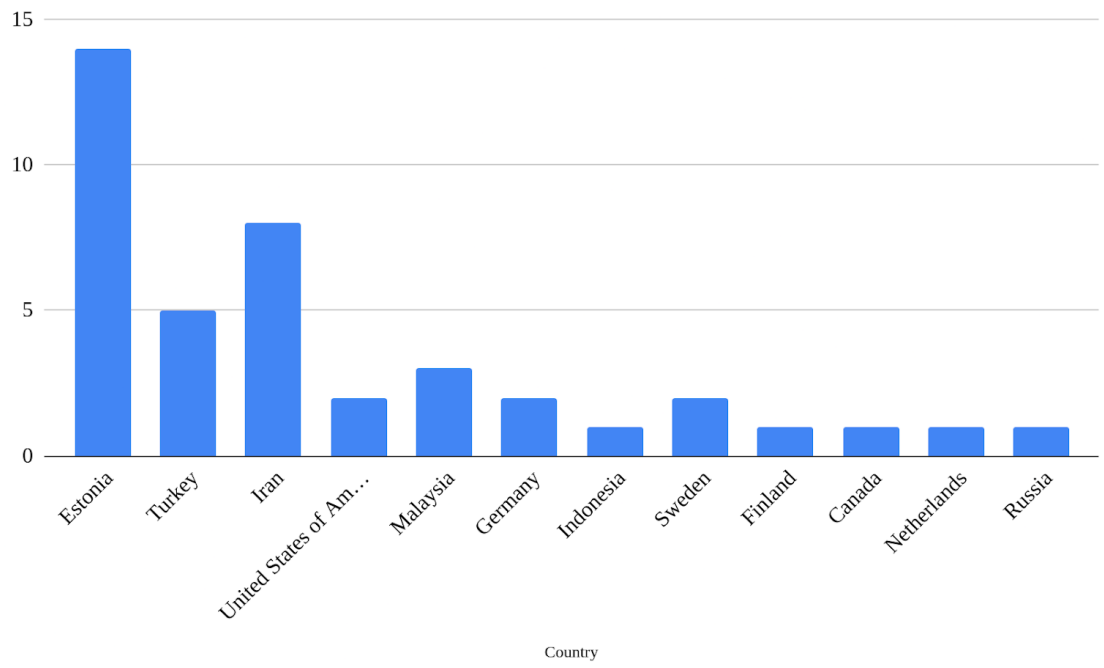


Figure 19 - Location of VPN user for P2P content delivery [190], [189]

In conclusion, the findings of the interviews reveal that the respondents felt a significant amount of anxiety about their privacy when utilizing P2P content sharing without a VPN. This fear was indicated by the findings of the interviews. The fact that the respondents brought up this topic provided evidence that it is worthy of consideration.

The results of the interviews provide some insight into this concern that a lot of individuals have. This matter was brought to light, in part, by the fact that the respondents voiced significant levels of concern over the preservation of their privacy. In addition, many of the respondents were happy with the VPN service that they made use of in order to transfer files using P2P applications. However, there is still a need for additional education and awareness regarding the risks associated with the distribution of P2P content without the use of a VPN, as well as the benefits associated with utilizing VPNs to protect one's privacy from breaches caused by ISPs.

This is because the risks associated with the distribution of P2P content without the use of a VPN are not widely known. Despite the fact that there is a requirement for further education and awareness of these hazards, this is the situation that has arisen. It is proposed that suppliers of VPN services concentrate their efforts on offering services that are reputable and trustworthy, not shared with any third party, and to place a premium on the privacy of their clients. The results of this study shed light on the reasons for P2P content sharing end users to use VPNs optimized for such intent. The preferences that VPN users have in connection to this kind of content sharing were highlighted. In consequence, these realizations may prove valuable in enhancing the construction of a VPN service that is more efficient. [190], [189]

4.5 Recommendations

According to the findings of the research, it is suggested that VPN solutions for P2P protection against ISP DPI should call for the utilization of VPN protocols like OpenVPN and WireGuard, encryption algorithms like AES, tunneling technologies like IPSec and SSL/TLS, and obfuscation techniques like domain fronting and onion routing. These technologies will, by working together, make it more difficult for DPI to detect and stop VPN traffic. This will ensure that conversations are kept secret and that unauthorized parties are unable to listen in on them.

In selecting a VPN service provider, NordVPN is highly recommended due to practicing pro-client security and privacy measures in the form of features. These features include a stringent no-logs policy, superior encryption, and compatibility with a wide variety of protocols. Its vast and stable network provides access to content sourced from all corners of the world, with over 5,400 servers dispersed throughout 59 countries.

The findings of the research were compiled into a curated list of VPNs , together with their related characteristics, that are particularly useful in reducing the dangers connected with P2P DPI strategies implemented by ISPs. It is suggested to ensure that the selected VPN is not a member of any intelligence-sharing alliances. [35] Those who desire to improve their online privacy and security by making use of P2P networks may find the list beneficial. In addition to this, it is employed in the context of an interview to provide vital protection against the risks associated with DPI that are enforced by ISPs.

According to the findings of the survey, respondents had substantial concerns about the confidentiality of their personal information when it comes to utilizing P2P content distribution methods that do not make use of VPNs . On the other hand, the vast majority of participants approved of the functionality of their VPN-based solutions for P2P content sharing. The AES-256 encryption protocol, Dynamic IP, circumventing traffic shaping, fast tunneling protocols, a no-logs policy, DNS leak prevention, and obfuscation were deemed to be the most significant qualities that VPNs should have in order to successfully satisfy the criteria for content delivery. According to the findings, VPN service providers must emphasize the provision of dependable and trustworthy services that place an emphasis on user privacy in addition to the

provision of high download speeds at an affordable price point in order to effectively cater to the requirements of their target audience.

The most common justifications for employing a VPN were to safeguard one's privacy, circumvent geographical limits, protect oneself from hackers, and facilitate activities relating to one's place of employment. However, only (24.0%) of those polled reported using a VPN as a preventative step against hacking. This indicates that there is a need for increased awareness and education on associated risks with hacking, and on the benefits associated with using a VPN as a method of protection.

Because the vast majority of respondents indicated that they were concerned about their ISP invading their privacy when using P2P content distribution without a VPN, the study also highlights the need to adopt a VPN for the purpose of protecting one's privacy and avoiding interference by ISPs. This is because the majority of respondents stated that they were concerned about their ISP invading their privacy when using P2P content distribution without a VPN. However, only (34.1%) of respondents reported using a VPN for less than a year, indicating a need for additional education and understanding about the benefits of utilizing VPNs for protecting one's privacy and identity when using an ISP.

It is strongly suggested that users who wish to access the free world through P2P networks ensure that their ISP is not using transparent DNS proxies. Furthermore, they should avoid using operating systems known for DNS leaks or vulnerabilities, [71] and finally make use of a combination of encrypted information, anonymous P2P applications, and a VPN that makes use of the most dependable obfuscation, encryption, and tunneling technologies. This is so that they may remain protected. This is of utmost significance for Iranians who use the internet to communicate with the rest of the free world because it protects them from potential danger.

5. Summary

The purpose of this thesis is to investigate the reasons behind, and preferences held by, users of VPNs for P2P content distribution. According to the outcome of the survey, a large proportion of respondents voiced concern about their privacy whilst utilizing P2P content distribution without a VPN. The study also indicated that the most prevalent reasons for using a VPN were to protect one's privacy and get around geo-blocking. The respondents came up with a list of elements that are essential for VPNs to have in order to satisfy the requirements for content delivery. These features include obfuscation, DNS leak prevention, and protection against traffic shaping bypass. According to the outcome of the research, VPN service providers should make user confidentiality top priority, while also promoting knowledge of the advantages of VPNs for ISP protection and confidentiality.

In accordance with the survey's observations, ExpressVPN, NordVPN, and Private Internet Access are the best VPN companies when it comes to protecting users' privacy and online safety. An exhaustive study of VPNs for users of P2P applications was not available. This gap was filled by this thesis by examining the technical specifications, security, and confidentiality aspects given by different systems, as well as offering a contrasting evaluation of their advantages and shortcomings. P2P users' views of privacy and security, as well as the efficacy of VPNs in avoiding deep inspection by ISPs, were also explored. End customers may benefit from the valuable information offered about VPN P2P solutions, which can assist them in making educated selections regarding which solution to choose.

The study required undertaking an in-depth analysis of the existing written content on VPNs, which consisted of product evaluations, academic publications, and technical reports. After this, an empirical research was carried out, which consisted of analyzing the most popular VPN solutions now available on the market with regard to the technical features, security, and P2P DPI privacy protection that they provide. With regard to, the research’s discoveries were used in the development of a comparative analysis of the VPN solutions for the utilization of the P2P protocol. This analysis emphasized the benefits and drawbacks of each solution and gave suggestions for end-users.

The results of the study can have important implications for future research. The research makes a significant contribution to the current body of scholarly work on VPNs for P2P users by providing a detailed examination of the aforementioned solutions from the point of view of end users. Additionally, it illustrates the technical hurdles and limits of VPNs for P2P DPI protection and gives insights into how these issues might be handled in future studies. In addition, it draws attention to the fact that VPNs are not invincible. The advice that the research provides for end-users may assist them in making educated choices when selecting a VPN solution for the use of P2P protocols, therefore enhancing their online privacy and security against their ISP's DPI. In addition, the assessment framework and methodology used in this study may provide a foundation for other investigations into the evaluation of various network security and privacy solutions. This thesis contributes to our overall knowledge of VPNs for P2P end users and the role that VPNs play in strengthening online privacy and security.

In conclusion, this work makes a substantial contribution to Iranian P2P users who are subject to censorship and restrictions on their natural right to communicate with the free world. By recommending appropriate technologies and VPN solutions, these users can ensure their online security by circumventing the Deep Packet Inspection implemented by their ISPs. This allows them to communicate with the free world without endangering their lives or the lives of their loved ones. Implementing these solutions is essential for Iranian P2P users to exercise their democratic entitlements to freedom of expression and access to information.

References

[1] V. Seničar, B. Jerman-Blažič, and T. Klobučar, “Privacy-Enhancing Technologies—approaches and development,” *Comput. Stand. Interfaces*, vol. 25, no. 2, pp. 147–158, May 2003, doi: 10.1016/S0920-5489(03)00003-5.

[2] M. Motamedi, “Fact check: Has Iran sentenced 15,000 protesters to death?” https://www.aljazeera.com/news/2022/11/16/have-15000-protesters-been-sentenced-to-death-in-iran-explainer (accessed May 05, 2023).

[3] “Joint Statement on Internet Shutdowns in Iran,” *United States Department of State*. https://www.state.gov/joint-statement-on-internet-shutdowns-in-iran/ (accessed May 05, 2023).

[4] “Iran protests: What happened while the internet was turned off?” https://www.aljazeera.com/program/the-stream/2019/11/27/iran-protests-what-happened-while-the-internet-was-turned-off (accessed May 05, 2023).

[5] C. Nast, “Iran’s total internet shutdown is a blueprint for breaking the web,” *Wired UK*. Accessed: May 05, 2023. [Online]. Available: https://www.wired.co.uk/article/iran-news-internet-shutdown

[6] P. Ohm, “The rise and fall of invasive ISP surveillance,” *U Ill Rev*, p. 1417, 2009.

[7] “viewcontent.pdf.” Accessed: Apr. 19, 2023. [Online]. Available: https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=2402&context=faculty_scholarship

[8] S. Androutsellis-Theotokis and D. Spinellis, “A survey of peer-to-peer content distribution technologies,” *ACM Comput. Surv. CSUR*, vol. 36, no. 4, pp. 335–371, 2004.

[9] J. Li, “On peer-to-peer (P2P) content delivery,” *Peer--Peer Netw. Appl.*, vol. 1, pp. 45–63, 2008.

[10] “Tixati.com - Discover Tixati!” https://www.tixati.com/discover/ (accessed Apr. 22, 2023).

[11] M. Liberatore, R. Erdely, T. Kerle, B. N. Levine, and C. Shields, “Forensic investigation of peer-to-peer file sharing networks,” *Digit. Investig.*, vol. 7, pp. S95–S103, 2010.

[12] “How it works - Briar.” https://briarproject.org/how-it-works/ (accessed May 02, 2023).

[13] M. R. Albrecht, J. Blasco, R. B. Jensen, and L. Mareková, “Mesh messaging in large-scale protests: Breaking Bridgefy,” presented at the Topics in Cryptology–CT-RSA 2021: Cryptographers’ Track at the RSA Conference 2021, Virtual Event, May 17–20, 2021, Proceedings, Springer, 2021, pp. 375–398.

[14] A. Chakraborti, D. Suciu, and R. Sion, “Wink: Deniable Secure Messaging,” *ArXiv Prepr. ArXiv220708891*, 2022.

[15] “A Quick Overview of the Protocol Stack · Wiki · briar / briar · GitLab,” *GitLab*, Sep. 30, 2019. https://code.briarproject.org/briar/briar/-/wikis/A-Quick-Overview-of-the-Protocol-Stack (accessed May 02, 2023).

[16] Y. Zhang and M. van der Schaar, “Peer-to-peer multimedia sharing based on social norms,” *Signal Process. Image Commun.*, vol. 27, no. 5, pp. 383–400, 2012.

[17] M. Liberatore, R. Erdely, T. Kerle, B. N. Levine, and C. Shields, “Forensic investigation of peer-to-peer file sharing networks,” *Digit. Investig.*, vol. 7, pp. S95–S103, Aug. 2010, doi: 10.1016/j.diin.2010.05.012.

[18] “What Is Double VPN (Multi-Hop) and How Do You Use It?,” Feb. 07, 2023. https://www.top10vpn.com/guides/what-is-double-vpn/ (accessed Mar. 05, 2023).

[19] A. M. Froomkin, “Regulating mass surveillance as privacy pollution: Learning from

environemntal impact statements," *U Ill Rev*, p. 1713, 2015.
[20] A. B. C. News, "Facebook says government requests for user data have reached all-time high," *ABC News*. https://abcnews.go.com/Business/facebook-government-requests-user-data-reached-time-high/story?id=66981424 (accessed May 02, 2023).
[21] P. M. Schwartz, "Privacy and democracy in cyberspace," *Vand Rev*, vol. 52, p. 1607, 1999.
[22] "p195402_isp_6b_staff_report.pdf." Accessed: May 05, 2023. [Online]. Available: https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf
[23] C. Parsons, *Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials*. Surveillance Studies Centre, Queen's University Kingston, Canada, 2008.
[24] B. Wagner, "Deep Packet Inspection and Internet Censorship: International Convergence on an'Integrated Technology of Control'," *Available SSRN 2621410*, 2009.
[25] "Comcast Throttles BitTorrent Traffic, Seeding Impossible * TorrentFreak." https://torrentfreak.com/comcast-throttles-bittorrent-traffic-seeding-impossible/ (accessed Feb. 19, 2023).
[26] A. K. Brauer-Rieke, "The FCC Tackles Net Neutrality: Agency Jurisdiction and the Comcast Order," *Berkeley Technol. Law J.*, vol. 24, p. 593, 2009.
[27] "Comcast throttles BitTorrent users • The Register." https://www.theregister.com/Print/2007/08/22/comcast_throttles_bittorrent_users/ (accessed Feb. 19, 2023).
[28] R. Bendrath and M. Mueller, "The end of the net as we know it? Deep packet inspection and internet governance," *New Media Soc.*, vol. 13, no. 7, pp. 1142–1160, 2011.
[29] L. Story, "A company promises the deepest data mining yet," *N. Y. Times Httpwww Nytimes Com20080320businessmedia20adcoside Html*, 2008.
[30] R. Clayton, "The phorm 'webwise'system," *Tech. Anal. Univ. Camb. Available Httpwww Cl Cam Ac Uk Rnc1080518-Phorm Pdf*, vol. 253, 2008.
[31] L. Story, "A Company Promises the Deepest Data Mining Yet," *The New York Times*, Mar. 20, 2008. Accessed: Feb. 19, 2023. [Online]. Available: https://www.nytimes.com/2008/03/20/business/media/20adcoside.html
[32] M. Jackson, "Government Moves Forward with UK ISP Internet Snooping System," *ISPreview UK*, Jun. 27, 2022. https://www.ispreview.co.uk/index.php/2022/06/government-moves-forward-with-uk-isp-internet-snooping-system.html (accessed Feb. 19, 2023).
[33] "3rd Annual VPN Market Report 2022," *Security.org*. https://www.security.org/resources/vpn-consumer-report-annual/ (accessed Apr. 24, 2023).
[34] "2023 Research Into VPN Usage (Updated Statistics)," *Security.org*. https://www.security.org/vpn/statistics/ (accessed Apr. 24, 2023).
[35] "5-Eyes, 9-Eyes, And 14-Eyes Agreement Explained," *Cybernews*, Dec. 18, 2020. https://cybernews.com/resources/5-eyes-9-eyes-14-eyes-countries/ (accessed May 11, 2023).
[36] H. F. von Stein zu Nord-und Ostheim, "The UKUSA Agreement: The History of an Enduring Relationship," 2022.
[37] C. Fuchs, "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society.," Jul. 2012. http://www.projectpact.eu/documents-1 (accessed Feb. 20, 2023).

[38] “What is deep packet inspection? Firewalling at its finest,” *NetworkTigers News*, Mar. 25, 2021. https://news.networktigers.com/opinion/what-is-deep-packet-inspection-firewalling/ (accessed Feb. 20, 2023).
[39] M. Mueller, A. Kuehn, and S. M. Santoso, “Policing the network: Using DPI for copyright enforcement,” *Surveill. Soc.*, vol. 9, no. 4, pp. 348–364, 2012.
[40] R. Bendrath, “Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection,” presented at the International Studies Annual Convention, 2009.
[41] M. L. Mueller and H. Asghari, “Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States,” *Telecommun. Policy*, vol. 36, no. 6, pp. 462–475, Jul. 2012, doi: 10.1016/j.telpol.2012.04.003.
[42] R. Wong, “BitTorrent Traffic Detection with Deep Packet Inspection and Deep Flow Inspection,” Master of Science, San Jose State University, San Jose, CA, USA, 2011. doi: 10.31979/etd.6d8k-gr9q.
[43] E. Hjelmvik and W. John, “Breaking and improving protocol obfuscation,” *Chalmers Univ. Technol. Tech Rep*, vol. 123751, 2010.
[44] S. Aryan, H. Aryan, and J. A. Halderman, “Internet Censorship in Iran: A First Look.,” presented at the FOCI, 2013.
[45] E. Morozov, *The net delusion: How not to liberate the world*. Penguin UK, 2011.
[46] U. N. H. C. for Refugees, “Refworld | Iran: Government surveillance capacity and control, including media censorship and surveillance of individual Internet activity,” *Refworld*. https://www.refworld.org/docid/550fdcc34.html (accessed Apr. 30, 2023).
[47] “9e49a4addd,” *United States Department of State*. https://www.state.gov/report/custom/9e49a4addd/ (accessed May 06, 2023).
[48] “New Data Suggest More People Died In Iran During Protests,” *Iran International*. https://www.iranintl.com/en/202301240166 (accessed May 05, 2023).
[49] D. Parent, G. Habibiazad, and A. Kelly, “At least 58 Iranian children reportedly killed since anti-regime protests began,” *The Guardian*, Nov. 20, 2022. Accessed: May 05, 2023. [Online]. Available: https://www.theguardian.com/global-development/2022/nov/20/iran-protests-children-killed-reports-mahsa-amini
[50] “Center for Human Rights in Iran,” *Center for Human Rights in Iran*, May 04, 2023. https://iranhumanrights.org (accessed May 06, 2023).
[51] “Iranian Spyware Steals People’s Info Via VPN,” *Iran International*. https://www.iranintl.com/en/202301130343 (accessed Apr. 30, 2023).
[52] C. R. in N. York and L. C. in Beijing, “Iran’s Web Spying Aided By Western Technology,” *Wall Street Journal*, Jun. 23, 2009. Accessed: May 01, 2023. [Online]. Available: https://www.wsj.com/articles/SB124562668777335653
[53] W. Strzyżyńska, “Iran blocks capital’s internet access as Amini protests grow,” *The Guardian*, Sep. 22, 2022. Accessed: May 01, 2023. [Online]. Available: https://www.theguardian.com/world/2022/sep/22/iran-blocks-capitals-internet-access-as-amini-protests-grow
[54] “Iran: Over 200 executed since January; Türk calls for end to death penalty | UN News,” May 09, 2023. https://news.un.org/en/story/2023/05/1136497 (accessed May 14, 2023).
[55] “Iran: Alarming Surge in Executions,” *Human Rights Watch*, May 12, 2023. https://www.hrw.org/news/2023/05/12/iran-alarming-surge-executions (accessed May 14,

2023).
[56] P. Foundation, “Iranian internet users to be cut off from World Wide Web,” *P2P Foundation*, Jan. 15, 2012. https://blog.p2pfoundation.net/iranian-internet-users-to-be-cut-off-from-world-wide-web/2012/01/15 (accessed May 01, 2023).
[57] “Iran Had Access To Private Info Of Facebook Users: Documents,” *Iran International*, May 02, 2023. https://www.iranintl.com/en/202302098881 (accessed May 02, 2023).
[58] “Instagram moderators say Iran offered them bribes to remove accounts,” *BBC News*, May 26, 2022. Accessed: May 05, 2023. [Online]. Available: https://www.bbc.com/news/world-middle-east-61516126
[59] P. Bischoff, “What is a multi-hop VPN and do you need one?,” *Comparitech*, Dec. 20, 2018. https://www.comparitech.com/blog/vpn-privacy/multi-hop-vpn/ (accessed Mar. 05, 2023).
[60] C. Tang, “In-depth analysis of the Great Firewall of China,” *Dep. Comput. Sci. Tufts Univ.*, 2016.
[61] G. Shen, Y. Wang, Y. Xiong, B. Y. Zhao, and Z.-L. Zhang, “HPTP: Relieving the Tension between ISPs and P2P.,” presented at the IPTPS, Citeseer, 2007.
[62] “What are Obfuscated Servers, and why do you need them? | NordVPN,” Jan. 12, 2021. https://nordvpn.com/features/obfuscated-servers/ (accessed Mar. 05, 2023).
[63] P. Bodenmann, “Obfuscated VPN - How to Bypass VPN Blocks?,” Dec. 17, 2022. https://cloudzy.com/blog/obfuscated-vpn/ (accessed Mar. 05, 2023).
[64] “What is Traffic Shaping (Packet Shaping)?,” *Networking*. https://www.techtarget.com/searchnetworking/definition/traffic-shaping (accessed Mar. 05, 2023).
[65] L. Burness, P. Eardley, and R. Hancock, “The trilogy architecture for the future internet,” in *Towards the Future Internet*, IOS Press, 2009, pp. 79–90.
[66] V. Mujović, “How to Bypass Traffic Shaping with a VPN?,” *Le VPN*, Aug. 22, 2018. https://www.le-vpn.com/bypass-traffic-shaping/ (accessed Mar. 06, 2023).
[67] M. Atighetchi, P. Pal, F. Webber, and C. Jones, “Adaptive use of network-centric mechanisms in cyber-defense,” presented at the Sixth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, 2003., IEEE, 2003, pp. 183–192.
[68] M. Kırlıdog, O. Uçkan, and I. B. Fidaner, “Deep packet inspection: Privacy and communication rights violations,” *Türkiyede İnternet Konf.*, 2011.
[69] A. Madhukar and C. Williamson, “A Longitudinal Study of P2P Traffic Classification,” in *14th IEEE International Symposium on Modeling, Analysis, and Simulation*, Monterey, CA, USA: IEEE, 2006, pp. 179–188. doi: 10.1109/MASCOTS.2006.6.
[70] A. R. Chavez, W. M. Stout, and S. Peisert, “Techniques for the dynamic randomization of network attributes,” presented at the 2015 international carnahan conference on security technology (ICCST), IEEE, 2015, pp. 1–6.
[71] “What Is a DNS Leak?,” *Fortinet*. https://www.fortinet.com/resources/cyberglossary/dns-leak (accessed Apr. 19, 2023).
[72] V. C. Perta, M. V. Barbera, G. Tyson, H. Haddadi, and A. Mei, “A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients,” *Proc. Priv. Enhancing Technol.*, vol. 2015, no. 1, pp. 77–91, Apr. 2015, doi: 10.1515/popets-2015-0006.
[73] “VPN Leak Test | Astrill VPN.” https://www.astrill.com/vpn-leak-test (accessed Apr. 24,

2023).
[74] “What Is VPN Split Tunneling? When Do You Need It?,” *Cybernews*, May 19, 2022. https://cybernews.com/what-is-vpn/split-tunneling/ (accessed Mar. 06, 2023).
[75] Zhao Aqun, Yuan Yuan, Ji Yi, and Gu Guanqun, “Research on tunneling techniques in virtual private networks,” in *WCC 2000 - ICCT 2000. 2000 International Conference on Communication Technology Proceedings (Cat. No.00EX420)*, Beijing, China: IEEE, 2000, pp. 691–697. doi: 10.1109/ICCT.2000.889294.
[76] Z. Aqun, Y. Yuan, J. Yi, and G. Guanqun, “Research on tunneling techniques in virtual private networks,” presented at the WCC 2000-ICCT 2000. 2000 International Conference on Communication Technology Proceedings (Cat. No. 00EX420), IEEE, 2000, pp. 691–697.
[77] M. Bazzell, *Extreme Privacy: What It Takes to Disappear*. Great Britain: Independently published, 2020.
[78] R. Ramesh, L. Evdokimov, D. Xue, and R. Ensafi, “VPNalyzer: systematic investigation of the VPN ecosystem,” presented at the Network and Distributed System Security, 2022, pp. 24–28.
[79] “Requirement Analysis of Decentralized Virtual Private Networks (dVPNs),” *Brave Browser*, May 23, 2019. https://brave.com/analysis-of-dvpns/ (accessed Mar. 07, 2023).
[80] “A guide to distributed network architectures | TechTarget,” *Networking*. https://www.techtarget.com/searchnetworking/tip/A-guide-to-distributed-network-architectures (accessed Mar. 07, 2023).
[81] M. T. Khan, J. DeBlasio, G. M. Voelker, A. C. Snoeren, C. Kanich, and N. Vallina-Rodriguez, “An empirical analysis of the commercial vpn ecosystem,” presented at the Proceedings of the Internet Measurement Conference 2018, 2018, pp. 443–456.
[82] “Adios, Hola! - Why you should immediately uninstall Hola,” May 10, 2019. https://web.archive.org/web/20190510183022/http://adios-hola.org/ (accessed Mar. 07, 2023).
[83] D. I. Wolinsky, K. Lee, P. O. Boykin, and R. Figueiredo, “On the design of autonomic, decentralized vpns,” presented at the 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2010), IEEE, 2010, pp. 1–10.
[84] “Best VPNs - Mar 2023 - Cybernews.com.” https://en.cybernews.com/lp/best-vpn/?utm_source=bing&utm_medium=cpc&utm_campaign=Bing_CN_VPN_P_T2_Full-Coverage_G-B_English&utm_content=83082206329963&utm_term=best%20vpn&campaignId=440230572&adgroupId=1329311069717087&adId=83082206329963&targetId=kwd-83082777080443:loc-175&device=c&munique=4b932d62816e1943c425496b6abeef58&source=bing&medium=cpc&campaign=Bing_CN_VPN_P_T2_Full-Coverage_G-B_English&content=83082206329963&term=best%20vpn (accessed Mar. 09, 2023).
[85] “What Is Peer-to-Peer (P2P) VPN? Are P2P VPNs Safe?,” *Fortinet*. https://www.fortinet.com/resources/cyberglossary/peer-to-peer-p2p-vpn (accessed May 05, 2023).
[86] “VPN kill switch: What is it and how does it work?” https://us.norton.com/blog/privacy/vpn-kill-switch-what-is-it-how-does-it-work (accessed May 05, 2023).
[87] “What is a kill switch and how does it work?,” *WhatIs.com*.

https://www.techtarget.com/whatis/definition/kill-switch (accessed May 05, 2023).
[88] Z. Aqun, Y. Yuan, J. Yi, and G. Guanqun, “Research on tunneling techniques in virtual private networks,” presented at the WCC 2000-ICCT 2000. 2000 International Conference on Communication Technology Proceedings (Cat. No. 00EX420), IEEE, 2000, pp. 691–697.
[89] “Private VPN With No Activity Logs & No Connection Logs.” https://www.expressvpn.com/what-is-vpn/policy-towards-logs (accessed Mar. 13, 2023).
[90] “Port Forwarding and VPNs: A Complete Guide | NordVPN,” Dec. 07, 2021. https://nordvpn.com/blog/port-forwarding/ (accessed Mar. 13, 2023).
[91] “Explained: 8 Important VPN Features and How They Work,” *MUO*, Aug. 07, 2022. https://www.makeuseof.com/important-vpn-features-explained/ (accessed May 05, 2023).
[92] A. Kochovski, “VPN Features Guide 2023 [What’s the Meaning & How it Works],” *Cloudwards*, Jul. 16, 2021. https://www.cloudwards.net/vpn-features-guide/ (accessed May 05, 2023).
[93] “Top 10 Best VPN for Torrenting - Compare & Find Your Ideal VPN,” Mar. 2023. https://www.top10vpn.com/best-vpn-for-torrenting/ (accessed Mar. 13, 2023).
[94] Contributor, “The best VPN for torrenting: Speed, privacy, and support matter,” *PCWorld*. https://www.pcworld.com/article/624123/best-vpn-for-torrenting.html (accessed Mar. 13, 2023).
[95] “The Best VPN for Torrenting in 2023,” *Security.org*. https://www.security.org/vpn/best/torrenting/ (accessed Mar. 13, 2023).
[96] “The Best VPNs for 2021 | InternetSecurity.org.” https://www.internetsecurity.org/compare/torrenting?mtid=63ca622a74cfa2302f65194a9b4f9f64 (accessed Mar. 13, 2023).
[97] “The Best VPN Services for 2023,” *PCMag UK*, Mar. 07, 2023. https://uk.pcmag.com/vpn/138/the-best-vpn-services (accessed Mar. 09, 2023).
[98] “The Best VPN for Torrenting in UK [Updated 2023],” *VPNRanks*. https://www.vpnranks.com/uk/best-vpn/torrenting/ (accessed Mar. 13, 2023).
[99] “Best VPN for Torrenting: Only 4 VPNs Pass (March 2023),” *RestorePrivacy*. https://restoreprivacy.com/vpn/best/torrenting/ (accessed Mar. 13, 2023).
[100] A. M. last updated, “The best VPN for torrenting and torrents 2023,” *TechRadar*, Nov. 01, 2022. https://www.techradar.com/vpn/best-vpn-for-torrenting (accessed Mar. 13, 2023).
[101] “10 Best VPNs for Torrenting Safely in 2023 — Fast and Private,” *vpnMentor*. https://www.vpnmentor.com/bestvpns/torrents/ (accessed Mar. 13, 2023).
[102] “Tom Okman,” *Slush*. https://www.slush.org/person/tom-okman/ (accessed May 11, 2023).
[103] A. O’Neil, “Australia and the ‘Five Eyes’ intelligence network: the perils of an asymmetric alliance,” *Aust. J. Int. Aff.*, vol. 71, no. 5, pp. 529–543, 2017.
[104] M. W. last updated, “NordVPN review,” *TechRadar*, Oct. 24, 2022. https://www.techradar.com/reviews/nordvpn (accessed May 15, 2023).
[105] “NordVPN for Torrenting Reviewed (Setup, Use & Speed Test),” Jun. 14, 2022. https://vpnalert.com/guides/nordvpn-torrenting/ (accessed Mar. 13, 2023).
[106] “The best online VPN service for speed and security | NordVPN.” https://nordvpn.com/ (accessed May 05, 2023).
[107] “Extra Security With Double VPN | NordVPN,” Jun. 14, 2017. https://nordvpn.com/features/double-vpn/ (accessed Mar. 13, 2023).

[108] "What is bandwidth throttling? How to stop it | NordVPN," Jul. 01, 2022. https://nordvpn.com/blog/what-is-bandwidth-throttling/ (accessed Mar. 13, 2023).
[109] "Different types of IP address | NordVPN," Jan. 15, 2022. https://nordvpn.com/blog/types-of-ip-addresses/ (accessed Mar. 13, 2023).
[110] "What is VPN split tunneling? How does it work? | NordVPN," Oct. 30, 2020. https://nordvpn.com/features/split-tunneling/ (accessed Mar. 13, 2023).
[111] "DNS leak test and protection | NordVPN," Jun. 15, 2017. https://nordvpn.com/features/dns-leak-test/ (accessed Mar. 13, 2023).
[112] "NordVPN introduces Meshnet | NordVPN," Jun. 20, 2022. https://nordvpn.com/blog/meshnet-feature-launch/ (accessed Mar. 13, 2023).
[113] S. Cook, "NordVPN for Torrenting: Can you torrent safely with this VPN?," *Comparitech*, Aug. 23, 2019. https://www.comparitech.com/blog/vpn-privacy/nordvpn-torrenting/ (accessed Mar. 13, 2023).
[114] "Which NordVPN protocol should I choose? | NordVPN support | NordVPN support." https://support.nordvpn.com/FAQ/1047408592/Which-protocol-should-I-choose.htm (accessed Mar. 13, 2023).
[115] "Next-Generation VPN Encryption: How does it work? | NordVPN," Mar. 02, 2020. https://nordvpn.com/features/next-generation-encryption/ (accessed Mar. 13, 2023).
[116] "How NordVPN will become more secure than ever | NordVPN," Oct. 26, 2019. https://nordvpn.com/blog/security-plan/ (accessed Mar. 13, 2023).
[117] "The Best No-Log VPN - Stay Anonymous & Secure | NordVPN," Jun. 14, 2017. https://nordvpn.com/features/strict-no-logs-policy/ (accessed Mar. 13, 2023).
[118] "VPN Kill Switch - prevent unprotected access | NordVPN," Oct. 19, 2021. https://nordvpn.com/features/vpn-kill-switch/ (accessed Mar. 13, 2023).
[119] E. Editor, "ExpressVPN review," *Tech Advisor*. https://www.techadvisor.com/article/717837/expressvpn-review-3.html (accessed Mar. 13, 2023).
[120] M. W. last updated, "ExpressVPN review," *TechRadar*, Oct. 24, 2022. https://www.techradar.com/reviews/expressvpn (accessed May 04, 2023).
[121] "Bypass VPN Blocks Using the Power of Obfuscation," *Bestvpn.co*. https://www.bestvpn.co/guides/vpn-obfuscation (accessed Mar. 13, 2023).
[122] "What is ISP Throttling and How to Bypass It | ExpressVPN." https://www.expressvpn.com/features/isp-throttling (accessed Mar. 13, 2023).
[123] "Does ExpressVPN offer static or dynamic IPs? | ExpressVPN," *ExpressVPN Customer Support*, Sep. 28, 2022. https://www.expressvpn.com/support/knowledge-hub/does-expressvpn-offer-static-or-dynamic-ips/ (accessed Mar. 13, 2023).
[124] "What Is VPN Split Tunneling? | ExpressVPN." https://www.expressvpn.com/features/split-tunneling (accessed Mar. 13, 2023).
[125] "What Is a DNS Leak and How To Prevent It | ExpressVPN Blog," *Home of internet privacy*, Mar. 16, 2018. https://www.expressvpn.com/blog/what-is-a-dns-leak/ (accessed Mar. 13, 2023).
[126] "What Is a VPN Tunnel and How Does It Work? | ExpressVPN." https://www.expressvpn.com/what-is-vpn/vpn-tunnel (accessed Mar. 13, 2023).
[127] "How Does VPN Security Work? Get a Secure VPN | ExpressVPN."

https://www.expressvpn.com/what-is-vpn/secure-vpn (accessed Mar. 13, 2023).
[128] "Introducing ExpressVPN TrustedServer technology," *Home of internet privacy*, Apr. 17, 2019. https://www.expressvpn.com/blog/introducing-trustedserver/ (accessed Mar. 13, 2023).
[129] "Deep Dive Into Our Innovative Server Tech | ExpressVPN Blog," *Home of internet privacy*, Jul. 05, 2022. https://www.expressvpn.com/blog/trustedserver-a-deep-dive-into-the-security-of-our-innovative-server-tech/ (accessed Mar. 13, 2023).
[130] "What Is a VPN Kill Switch? How Do They Work? | ExpressVPN." https://www.expressvpn.com/features/network-lock (accessed Mar. 13, 2023).
[131] M. W. published, "CyberGhost VPN review," *TechRadar*, Oct. 24, 2022. https://www.techradar.com/reviews/cyberghost-vpn (accessed May 15, 2023).
[132] E. Smith, "CyberGhost VPN Review 2023: More Than a Secure VPN?," *BestVPNz.com*, Dec. 28, 2022. https://www.bestvpnz.com/reviews/cyberghost-vpn/ (accessed Mar. 13, 2023).
[133] S. Max, "How to Bypass Bandwidth Limit Restrictions in 2023 [Full Speed]," *Cloudwards*, Jul. 04, 2021. https://www.cloudwards.net/how-to-bypass-bandwidth-limit-restrictions/ (accessed Mar. 13, 2023).
[134] "Static vs Dynamic IPs: Which Is Better?," *CyberGhost Privacy Hub*, Oct. 06, 2022. https://www.cyberghostvpn.com/en_US/privacyhub/static-vs-dynamic-ip/ (accessed Mar. 13, 2023).
[135] "How to use split tunneling with CyberGhost for Android," *Support Center - CyberGhost VPN*. https://support.cyberghostvpn.com/hc/en-us/articles/360022345054-How-to-use-split-tunneling-with-CyberGhost-for-Android (accessed Mar. 13, 2023).
[136] "DNS Leak Test: Find & Prevent DNS Leaks with CyberGhost." https://www.cyberghostvpn.com/en_US/dns-leak-test (accessed Mar. 13, 2023).
[137] "Most Popular VPN Protocols Explained." https://www.cyberghostvpn.com/en_US/vpn-protocols (accessed Mar. 13, 2023).
[138] "Fast, Secure & Anonymous VPN service | CyberGhost VPN." https://www.cyberghostvpn.com/en_US/ (accessed Mar. 13, 2023).
[139] "VPN Encryption: Why Does CyberGhost VPN Use 256-bit Encryption?" https://www.cyberghostvpn.com/en_US/vpn-encryption (accessed Mar. 13, 2023).
[140] "CyberGhost VPN Killswitch: Impenetrable Privacy Anywhere." https://www.cyberghostvpn.com/en_US/killswitch-vpn (accessed Mar. 13, 2023).
[141] M. W. from A. T. last updated, "Surfshark VPN review," *TechRadar*, Oct. 24, 2022. https://www.techradar.com/reviews/surfshark (accessed May 15, 2023).
[142] "MultiHop double VPN," *Surfshark*. https://surfshark.com/features/multihop (accessed Mar. 13, 2023).
[143] "Obfuscation," *Surfshark*. https://surfshark.com/features/obfuscated-servers (accessed Mar. 13, 2023).
[144] A. Jokšaitė, "Am I being throttled, and how do I stop it?," *Surfshark*, Nov. 14, 2022. https://surfshark.com/blog/am-i-being-throttled (accessed Mar. 13, 2023).
[145] M. Klimas, "What is port forwarding and does it work with a VPN," *Surfshark*, Sep. 01, 2022. https://surfshark.com/blog/vpn-port-forwarding (accessed Mar. 13, 2023).

[146] "Do you offer dedicated IPs?," *Surfshark Customer Support*, Mar. 07, 2023. https://support.surfshark.com/hc/en-us/articles/360020099119-Do-you-offer-dedicated-IPs- (accessed Mar. 13, 2023).
[147] "VPN split tunneling with Bypasser," *Surfshark*. https://surfshark.com/features/split-tunneling (accessed Mar. 13, 2023).
[148] "DNS leak test," *Surfshark*. https://surfshark.com/dns-leak-test (accessed Mar. 13, 2023).
[149] P. Whittaker, "Is Surfshark Good for Torrenting?," *BitTorrentVPN*, Apr. 23, 2019. https://www.bittorrentvpn.com/surfshark-torrenting/ (accessed Mar. 13, 2023).
[150] "VPN protocols: WireGuard, OpenVPN, IKEv2 - Surfshark." https://surfshark.com/features/surfshark-vpn-protocols (accessed Mar. 13, 2023).
[151] M. Klimas, "What is VPN encryption and how does it work?," *Surfshark*, Jul. 20, 2022. https://surfshark.com/blog/vpn-encryption (accessed Mar. 13, 2023).
[152] Surfshark, "Surfshark upgraded its infrastructure to 100% RAM-only servers," *Surfshark*, Jul. 15, 2020. https://surfshark.com/blog/surfshark-upgraded-to-ram-only-servers (accessed Mar. 13, 2023).
[153] "No-log VPN," *Surfshark*. https://surfshark.com/features/no-logs (accessed Mar. 13, 2023).
[154] "Reliable VPN Kill Switch technology," *Surfshark*. https://surfshark.com/features/kill-switch (accessed Mar. 13, 2023).
[155] M. W. last updated, "Private Internet Access (PIA) VPN review," *TechRadar*, Oct. 24, 2022. https://www.techradar.com/reviews/private-internet-access-vpn (accessed May 15, 2023).
[156] "Private Internet Access Review 2023 — Good, but Is It Safe?," *vpnMentor*. https://www.vpnmentor.com/reviews/private-internet-access/ (accessed Mar. 13, 2023).
[157] "Understanding the Multi-Hop Feature - Knowledgebase / Technical / Application Settings and Features / Application & Features - PIA Support Portal." https://helpdesk.privateinternetaccess.com/kb/articles/understanding-the-multi-hop-feature (accessed Mar. 13, 2023).
[158] C. Hauk, "How to Stop ISP Throttling," *Pixel Privacy*, Dec. 17, 2020. https://pixelprivacy.com/resources/stop-isp-throttling/ (accessed Mar. 13, 2023).
[159] "How do I enable port forwarding on my VPN? - Knowledgebase / Technical / Browsing and Internet / Torrents - PIA Support Portal." https://helpdesk.privateinternetaccess.com/kb/articles/how-do-i-enable-port-forwarding-on-my-vpn (accessed Mar. 13, 2023).
[160] P. I. A. Inc, "Get Your Dedicated IP VPN (Personal, Static IP Address) | PIA." https://www.privateinternetaccess.com/vpn-features/dedicated-ip-vpn (accessed Mar. 13, 2023).
[161] "What is VPN Split Tunneling? | Private Internet Access." https://www.privateinternetaccess.com/vpn-features/split-tunneling (accessed Mar. 13, 2023).
[162] "IP Address Leak - Knowledgebase / Technical / Troubleshooting / Connection - PIA Support Portal." https://helpdesk.privateinternetaccess.com/kb/articles/ip-address-leak (accessed Mar. 13, 2023).
[163] P. I. A. Inc, "VPN Encryption - What's Needed For Data Security? | PIA VPN." https://www.privateinternetaccess.com/vpn-features/vpn-encryption (accessed Mar. 13, 2023).

[164] P. I. A. Inc, “The #1 No-Logs VPN: Private & Secure | Private Internet Access.” https://www.privateinternetaccess.com/vpn-features/no-logs-vpn (accessed Mar. 13, 2023).
[165] “The Kill Switch and ensuring your security and privacy are not interrupted. - Knowledgebase / Technical / Application Settings and Features / Kill Switch - PIA Support Portal.” https://helpdesk.privateinternetaccess.com/kb/articles/the-kill-switch-and-ensuring-your-security-and-privacy-are-not-interrupted (accessed Mar. 13, 2023).
[166] A. M. Abdullah, “Advanced encryption standard (AES) algorithm to encrypt and decrypt data,” *Cryptogr. Netw. Secur.*, vol. 16, pp. 1–11, 2017.
[167] “NordVPN Review 2023: How Good & Safe this VPN Truly is?,” *Cybernews*, Jul. 22, 2022. https://cybernews.com/best-vpn/nordvpn-review/ (accessed May 04, 2023).
[168] “After rejecting the Indian government’s new cyber security guidelines, NordVPN to shut down its servers in India by June 26,” *Business Insider*. https://www.businessinsider.in/tech/news/nordvpn-to-shut-down-its-servers-in-india-by-june-26-2022/articleshow/92229519.cms (accessed May 11, 2023).
[169] “NordVPN Review: Feature-Rich and Speedy, but Privacy and Transparency Issues Need Attention,” *CNET*. https://www.cnet.com/tech/services-and-software/nordvpn-review/ (accessed May 04, 2023).
[170] “23 benefits of a VPN (virtual private network) | NordVPN,” Apr. 18, 2018. https://nordvpn.com/features/ (accessed May 04, 2023).
[171] “ExpressVPN review: is it worth the price?,” *Cybernews*, Jul. 29, 2022. https://cybernews.com/best-vpn/expressvpn-review/ (accessed May 04, 2023).
[172] “User Feedback - ExpressVPN In-depth Review,” *MalwareTips Forums*, Nov. 05, 2018. https://malwaretips.com/threads/expressvpn-in-depth-review.87833/ (accessed May 04, 2023).
[173] “ExpressVPN Review 2023: Safe, But Is It Worth The Price?,” *vpnMentor*. https://www.vpnmentor.com/reviews/expressvpn/ (accessed May 04, 2023).
[174] “ExpressVPN review: is it worth the price?,” *Cybernews*, Jul. 29, 2022. https://cybernews.com/best-vpn/expressvpn-review/ (accessed May 04, 2023).
[175] “ExpressVPN Delivers Top Speeds and Solid Transparency Efforts.” https://www.cnet.com/tech/services-and-software/expressvpn-review-pricey-but-speedy-and-great-for-streaming/ (accessed May 04, 2023).
[176] “ExpressVPN,” *PCMag UK*, Mar. 09, 2023. https://uk.pcmag.com/vpn/83190/expressvpn (accessed May 04, 2023).
[177] “7 Common VPN Protocols Explained and Compared | ExpressVPN.” https://www.expressvpn.com/go/what-is-vpn/protocols (accessed Mar. 05, 2023).
[178] “BVI Jurisdiction: Why It Matters | ExpressVPN,” *Home of internet privacy*, Apr. 28, 2017. https://www.expressvpn.com/blog/bvi-privacy-legislation/ (accessed May 11, 2023).
[179] “Does CyberGhost log ? Absolutely not !,” *Support Center - CyberGhost VPN*. https://support.cyberghostvpn.com/hc/en-us/articles/213898965-Does-CyberGhost-log-Absolutely-not- (accessed Mar. 13, 2023).
[180] “CyberGhost VPN is rated ‘Excellent’ with 4.3 / 5 on Trustpilot,” *Trustpilot*, Apr. 20, 2023. https://www.trustpilot.com/review/cyberghostvpn.com (accessed Apr. 20, 2023).
[181] P. I. A. Inc, “What is VPN Split Tunneling? | Private Internet Access.” https://www.privateinternetaccess.com/vpn-features/split-tunneling (accessed Mar. 13, 2023).

[182] "Private Internet Access is rated 'Excellent' with 4.5 / 5 on Trustpilot," *Trustpilot*, Apr. 19, 2023. https://www.trustpilot.com/review/privateinternetaccess.com (accessed Apr. 20, 2023).
[183] "Surfshark is rated 'Excellent' with 4.5 / 5 on Trustpilot," *Trustpilot*, Apr. 18, 2023. https://www.trustpilot.com/review/surfshark.com (accessed Apr. 20, 2023).
[184] https://www.nytimes.com/by/michael-laforgia and https://www.nytimes.com/by/gabriel-dance, "Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence," *The New York Times*, Jun. 05, 2018. Accessed: May 05, 2023. [Online]. Available: https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html
[185] Reuters, "U.S. senators question Meta over Chinese, Russian access to Facebook data -statement," *Reuters*, Feb. 06, 2023. Accessed: May 05, 2023. [Online]. Available: https://www.reuters.com/technology/us-senators-question-meta-over-chinese-russian-access -facebook-data-statement-2023-02-06/
[186] WayneMainland, "The communication at Telus has gone from bad to worse!," *r/Lionbridge*, Jan. 13, 2023. www.reddit.com/r/Lionbridge/comments/10aupct/the_communication_at_telus_has_gone_f rom_bad_to/ (accessed May 05, 2023).
[187] "TELUS International - Scam! Beware! A.I. runs everything." https://www.glassdoor.com/Reviews/Employee-Review-TELUS-International-RVW661161 49.htm (accessed May 05, 2023).
[188] "Surfshark Review," *Surfshark*. https://surfshark.com/surfshark-review (accessed May 05, 2023).
[189] "VPN Simple Questionaire (Responses)," *Google Docs*. https://docs.google.com/spreadsheets/d/1X3GcJsuprtCw6IVE46MVCEai1RB-ZoB0pFCrkd n2Xt0/edit?resourcekey&usp=embed_facebook (accessed May 03, 2023).
[190] "VPN Questionnaire," *Google Docs*. https://docs.google.com/forms/d/e/1FAIpQLScTIKa3p5i9ua8dZwOxyvwaAcQLrB4j2ClNZ ZHOY-z_M1YnXA/viewform?usp=embed_facebook (accessed May 03, 2023).
[191] C. Kaur and Dr. Y. Sharma, "The vital role of VPN in making secure connection over internet world," vol. 8, pp. 2336–2339, Mar. 2020, doi: 10.35940/ijrte.F8335.038620.
[192] "VPN security: How VPNs help secure data and control access," *Cloudflare*. https://www.cloudflare.com/learning/access-management/vpn-security/ (accessed May 05, 2023).
[193] "Survey Information: Americans Care Deeply About Their Privacy," *Center for Democracy and Technology*, Oct. 22, 2009. https://cdt.org/insights/survey-information-americans-care-deeply-about-their-privacy/ (accessed May 05, 2023).
[194] "NordVPN is rated 'Excellent' with 4.4 / 5 on Trustpilot," *Trustpilot*, Apr. 18, 2023. https://www.trustpilot.com/review/nordvpn.com (accessed Apr. 20, 2023).
[195] "ExpressVPN is rated 'Excellent' with 4.7 / 5 on Trustpilot," *Trustpilot*, Mar. 11, 2023. https://www.trustpilot.com/review/expressvpn.com (accessed Apr. 20, 2023).

Appendix 1 – Public Reviews Based on TrustPilot Ratings

Attached herewith is an appendix consisting of public reviews regarding VPNs that support P2P content delivery protection.

NordVPN

This Trustpilot-based assessment examines NordVPN's features and capabilities. NordVPN is currently one of the most trusted and well-known VPN companies. Trustpilot has frequently shown NordVPN to be superior in security, connection speed, and ease of use. This essay will cover NordVPN's features, pros, and cons. [194] The details are depicted in Figure 20.

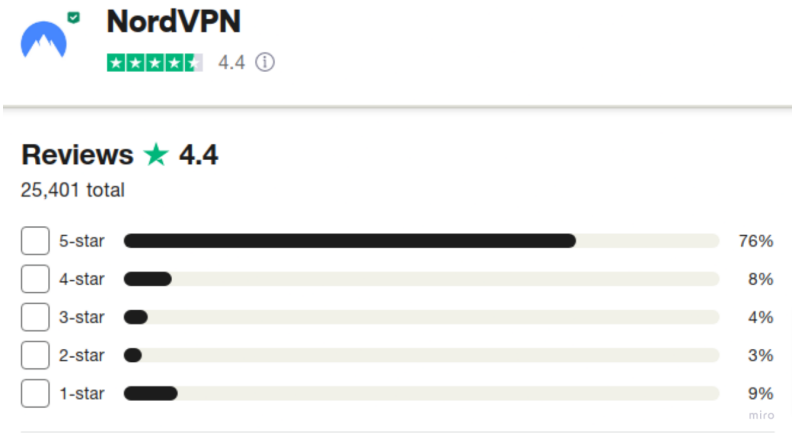


Figure 20 - NordVPN public review on Trustpilot [194]

Security: Users of NordVPN have access to an abundance of options that are both safe and protective of their privacy, allowing them to hide their online actions from anybody who may be interested in seeing them. The data you transmit over NordVPN is protected by encryption using the industry-standard AES-256 algorithm. While NordVPN supports OpenVPN in addition to IKEv2/IPSec, WireGuard only provides support for those two protocols. The VPN does not record the activities of its users or the types of data they access. In the unlikely scenario that the VPN link connectivity fails for whatever reason, the kill switch will immediately disconnect the user from the VPN service. Following these steps will ensure that that data is kept confidential. Users of NordVPN who take advantage of the company's Double VPN service enjoy an increased level of protection for all of their activities conducted online.

Connection: High connection rates constitute this VPN as a fantastic option for gaming, transferring data, and streaming. NordVPN's 5,500 servers across 59 nations enable users to get connected to a server in close proximity, thus decreasing latency and improving upload and download performance. In addition to P2P, Onion over VPN, and Reserved IP servers, which provides consumers with a customized experience.

Ease of Use: The app is famous for its practical navigation. The VPN is functional with different operating systems including Linux, macOS, iOS, Android, routers and Windows. During installation, users can smoothly transfer servers and protocols. CyberSec feature bans advertisements, tracking technologies, as well as risky websites, expanding the user experience.

Conclusion: Trustpilot reviews laud NordVPN's good security, quick connection, and friendly UI. Due to its wide variety of hosts, VPN protocols, and specialized server systems, It is an excellent option for users who wish to improve their online anonymity and security, access geographically-blocked content, or accelerate their browsing speeds.

ExpressVPN

Based on Trustpilot evaluations, This review will delve into the features and capabilities of ExpressVPN. [195] The details are depicted in Figure 21.

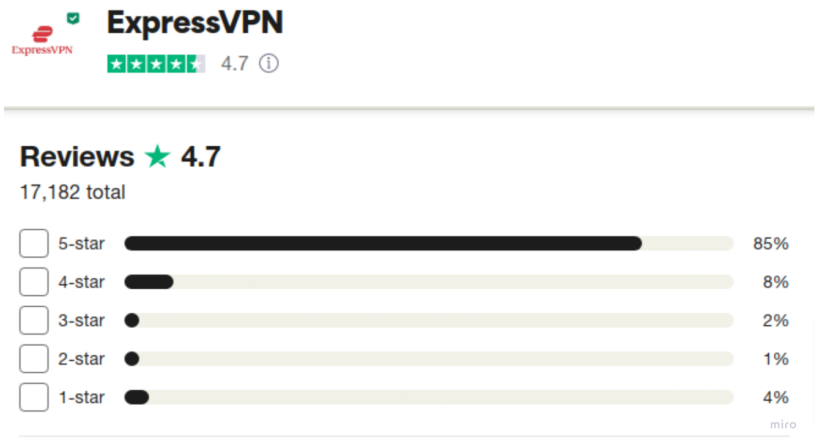


Figure 21 - ExpressVPN public review on Trustpilot [195]

Security: This VPN increases digital security and private browsing. Due to its robust protocols of security, It ranks as one of the most dependable VPNs. AES-256, the most trusted cryptography, is utilized by the VPN. IKEv2 and OpenVPN are also utilized by it, which increases reliability. Its no-logs policy signifies that the service doesn't save any user activity. This policy is validated by third-party audits. If the connection fails, the kill feature will prevent the user from accessing the web. Prevents data compromises.

Connection: Because of its instantaneous connection rate, it is ideal for video streaming, downloading purposes, and online gaming. In ninety-four nations, there are over 3,000 servers. This network enables consumers to connect to a local server, thereby accelerating data transmission and reducing delay times. ExpressVPN's (99.9%) uptime demonstrates its reliability. During their session, users will never encounter service interruptions or delays. It also offers round-the-clock consumer service for any challenges that happen while using the application.

Ease of Use: It has a simple, novice-friendly layout. It is functional with Microsoft Windows, Apple macOS, Android, Linux, and routers. After an easy setup, users can easily transition between servers and protocols. Its divided tunneling capability allows users to select which apps and websites leverage the VPN versus those that do not. This feature is solely accessible to paid users.

Conclusion: This VPN company is among the leading VPN vendors due to its steady support, sophisticated security, and quick connectivity. It receives high ratings via Trustpilot for its simplicity of use, extensive server network, and courteous customer service. This service is recommended for anyone who wishes to boost up their connection to the web, access content that is geographically restricted, or enhance their digital security and confidentiality.

CyberGhost VPN

This VPN company is among the leading VPN vendors due to its steady support, sophisticated security, and quick connectivity. It receives high ratings via Trustpilot for its simplicity of use, extensive server network, and courteous customer service. This service is recommended for anyone

who wishes to boost up their connection to the web, access content that is geographically restricted, or enhance their digital security and confidentiality. [180] The details are depicted in Figure 22.

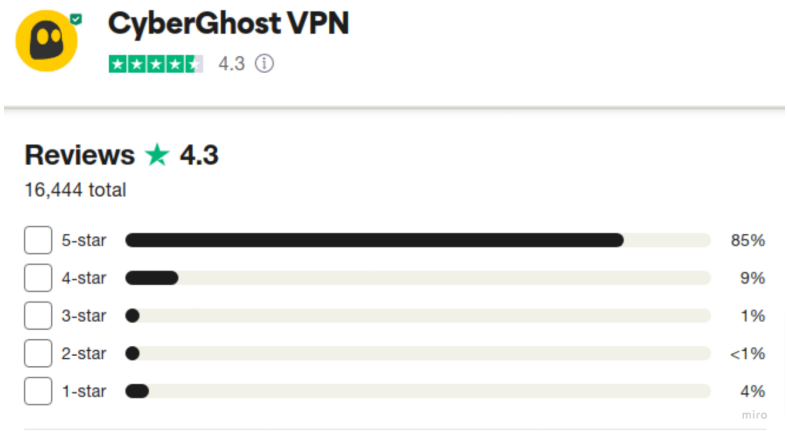


Figure 22 - CyberGhost public review on Trustpilot [180]

Security: It incorporates AES-256 as the finest encrypted methods. It enables OpenVPN, and L2TP/IPSec, presenting clients with a variety of options based on their requirements. CyberGhost's no-logs strategy safeguards user confidentiality by never logging user information.

Connection: It possesses strongly substantial VPN servers, having 7,300 sites within 91 different nations. The broad network enables users to establish connections to the servers located in various sites, thereby enhancing browsing rates and facilitating utilization of restricted resources, including video streaming platforms and webpages. By communicating to a server in close proximity, This VPN's network reduces latency. This accelerates perusing and enhances the internet experience.

Ease of Use: The VPN will be simpler to configure, employ, and troubleshoot. The consumer service is also highly regarded. Numerous consumers are pleased with the quality of service. The phenomenal client support has improved the client encounter and enhanced CyberGhost's VPN's reputation, resulting in an unparalleled assistance. The client care is among the finest in the industry. Clients acclaim the round-the-clock live chat feature of the VPN service for its efficiency and helpfulness. It additionally offers a broad information base with installation and troubleshooting guides.

Conclusion: This service has a consistent VPN due to its numerous security features, enormous infrastructure and superior customer support. It's reliable and reputable VPN connections enable users to get to geographically restricted websites and browse the web securely. The AES-256 encoding, automated death switch, and no-logging policy of the VPN defend the security of users' private data as well as surfing habits.

Surfshark VPN

Surfshark is A VPN that is gaining recognition in the marketplace due to the fact that it offers unique features at competitive prices. Recent Trustpilot reviews have given Surfshark high ratings for its user-friendliness, level of protection, and level of concealment. [183] The details are depicted in Figure 23.

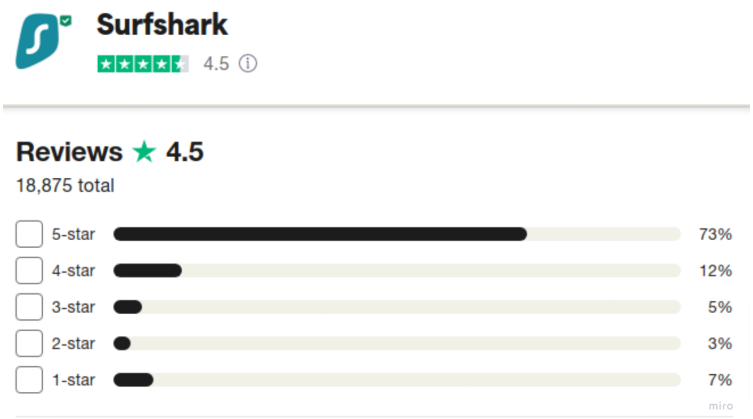


Figure 23 - Surfshark public review on Trustpilot [183]

Unique Features: It is a solid VPN that separates itself from the competition with cutting-edge capabilities. CleanWeb, which removes ads, tracking tools, and malicious software, is adored by its users. This function enhances navigation. Multi Hop enables people to get connected to countless VPN servers at once, thereby enhancing cybersecurity.

Security: Being a stable VPN that possesses numerous security advantages. AES-256 encryption, the industry standard for optimal security, is utilized by the Surfshark. Plus, Surfshark works with IKEv2, OpenVPN, which enhances confidence. The VPN's policy of not recording user activity while connected has also been praised. A kill switch of Surfshark stops the user's web access if the

communication drops, assuring security. MultiHop, and NoBorders are popular Surfshark functions because they enhance browsing and online protection. The No Borders' mode of Surfshark received rave evaluations from consumers overseas with strict net limits. This function enables users to get around VPN constraints and surf the web without filtering or surveillance. Surfshark's extensive network covering almost sixty countries ensures its customers can connect to the closest servers. This enhances browsing quickness and effectiveness.

Ease of Use: Surfshark's VPN service is known for its user-friendly design and inexpensive rates. Its user-friendly programs are available for many devices, making it widely accessible. Surfshark's 24/7 live chat support provides prompt service, according to Trustpilot reviews. Surfshark's price tiers are affordable, and one account can be used on an infinite number of devices.

Conclusion: Recent reviews on trustpilot.com indicate that it is a VPN which provides distinctive benefits and comprehensive security and privacy protections. Its affordable pricing, user-friendly interface, and exceptional service levels make it an attractive option for users seeking a reputable VPN service.

Private Internet Access

PIA has served as an esteemed VPN provider since 2010. Recent Trustpilot reviews indicate that it has earned high marks for security, confidentiality and dependability. [182] The details are depicted in Figure 24.

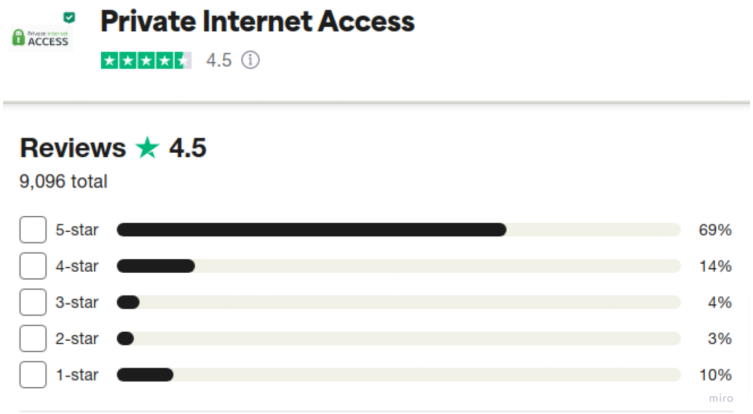


Figure 24 - Private Internet Access public review on Trustpilot [182]

Security: This VPN service prioritizes client confidentiality and security. It supports WireGuard, OpenVPN and the great AES-256 data encryption protocol. PIA's no-logs policy protects user privacy by not storing user information. Additionally, PIA offers a disabled device. This function prevents internet traffic disruptions. PIA has an outstanding rating on Trustpilot and prioritizes consumer confidentiality and security. PIA will appeal to clients seeking a secure VPN.

Connection: The most efficient and reputable VPN. For remote access via VPN, PIA offers more than thirty-five thousand servers in eighty-eight nations. It offers unhindered resources for swift video streaming and browsing. The unlimited bandwidth offered by PIA enables streaming, and a fast surfing experience. Due to Trustpilot submissions, PIA is attractive to VPN users who prioritize performance and dependability.

Ease of Use: PIA has an intuitive user interface, excellent customer service, and affordable fares. Users appreciate the company's multi-device applications and 24/7 live support. Customers can utilize a single PIA account on up to ten devices, making it cost-effective for households and small businesses.

Conclusion: In accordance with the most recent assessments on Trustpilot, it provides comprehensive safety and privacy safeguards, connection speeds that are both quick and dependable, and a simple interface. Users who have been searching for an established VPN supplier ought to think about this company's service because of its competitive price and excellent customer support.

Appendix 2 - Interviews Questions and Results

Interview Questions

Attached herewith is an appendix consisting of a questionnaire designed to gather public opinion on the usage of VPN for P2P content delivery.

1. How experienced are you with Cybersecurity or Information Technology in general?
   A. Very inexperienced B. Inexperienced C. Experienced D. Very experienced

2. How much are you concerned about your ISP for invading your privacy when using P2P content delivery?
   B. Very unconcerned B. unconcerned C. Concerned D. Very Concerned

3. How invasive do you think the ISPs are?
   A. Not very invasive B. Not invasive C. Invasive D. Very invasive

4. How long have you been using a VPN for P2P content delivery ISP protection?
   A. Below 1 year B. 1 year C. 1 - 2 year D. More than 2 years

5. What is your reason for using a VPN?

6. Which one of the following VPNs are you using for content delivery over P2P networks?
   A. NordVPN B. ExpressVPN C. CyberGhost D. SurfShark
   E. Private Access Internet F. Other (Please specify)

7. How effective do you think your VPN solution for P2P content delivery is?
   A. Not Very effective B. Not effective C. Effective D. Very Effective

8. Which features are the most important for you in the selection of your VPN solution for content delivery over P2P networks?

Table 10 - VPN for Peer to Peer content delivery

Feature	Definition	Select
Multi Hop	Data transmission through multiple servers	
Obfuscation	Circumvent VPN-blocking firewalls	
Bypassing Traffic Shaping	Continuous, encrypted, unidentifiable connection	
Port hopping	Concealing the true identity of the service	
Dynamic IP address	Encoding/decoding randomized IP addresses	
Split Tunneling	Selecting which apps or data flows to secure	
DNS leak protection	Stopping inadvertent leakage of VPN traffic	
Decentralized	VPN servers are decentralized	
P2P servers	VPN servers use peer to peer structures	
Fast Tunneling Protocols	Yes (OpenVPN, IKEv2/IPsec, WireGuard)	
Encryption	AES-256	
RAM-only Servers	No data is stored on the servers	
No-Logs Policy	No logs are saved on the servers	
Kill Switch	Prevent traffic leakage in the event of a tunnel failure	

9. How satisfied are you with your selection of VPN solution for P2P content delivery?
   A. Not very satisfied B. Not satisfied C. Satisfied
   D. Very satisfied

10. Are there any other comments or insights that you would like to share about using VPN solutions for Content Delivery over P2P networks?

11. What is your age group?
   A. Below 18 B. 18 - 30 C. 30 - 40 D. 40 above

12. What is your gender?
   A. Male B. Female

13. Where do you live?

Interview Results

Attached herewith is an appendix consisting of answers gathering public opinion on the usage of VPN for P2P content delivery. The details are depicted in Figures 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38.

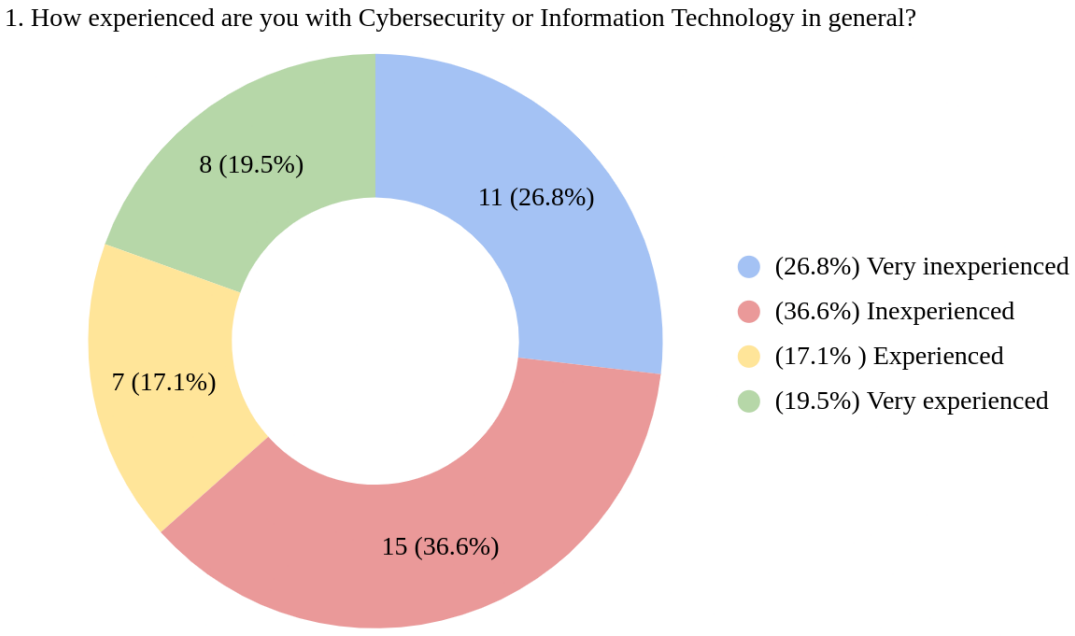


Figure 25 - VPN user Cybersecurity experience

2. How invasive do you think your ISP (Internet Service Provider) is?

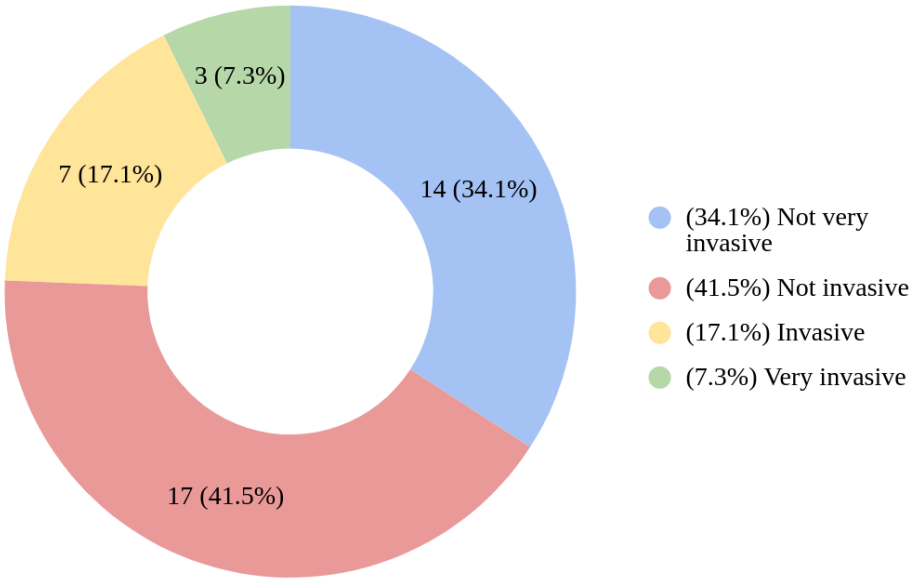


Figure 26 - User opinion on ISP invasiveness

3. How concerned are you about your ISP invading your privacy while using P2P content delivery without a VPN?

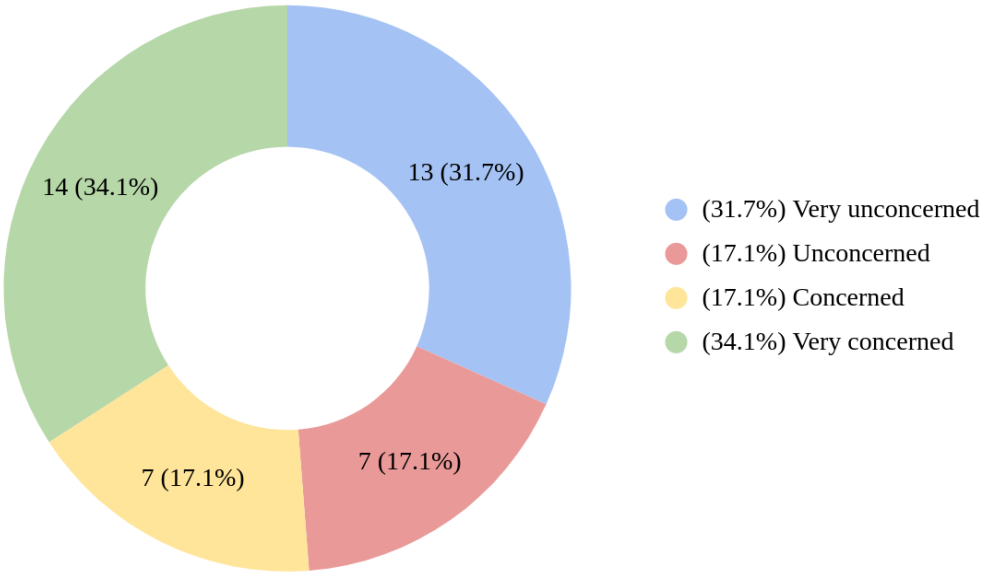


Figure 27 - User concern on ISP privacy invasion while using P2P content delivery

4. How long have you used a VPN for P2P content delivery and ISP protection?

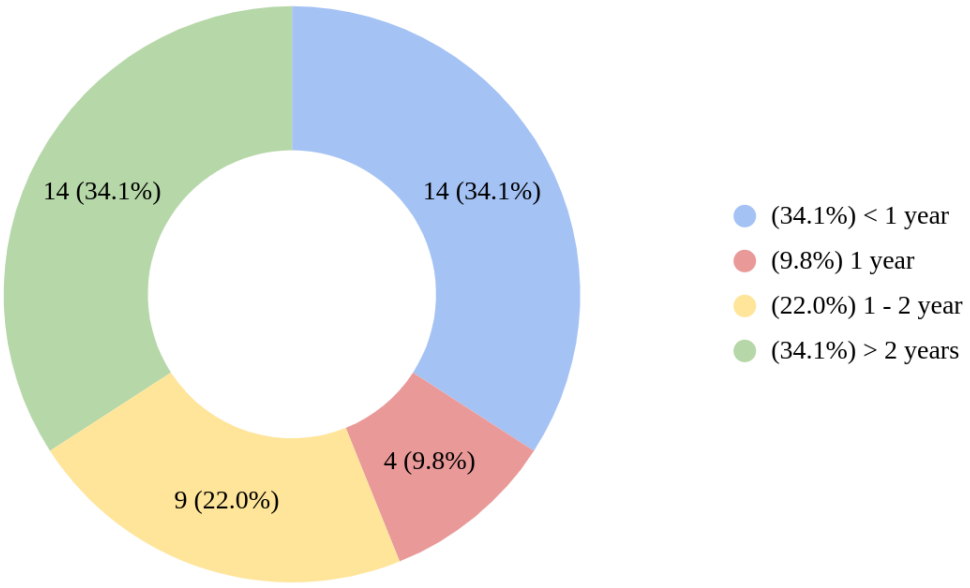


Figure 28 - User VPN usage duration

5. What is your reason for using a VPN?

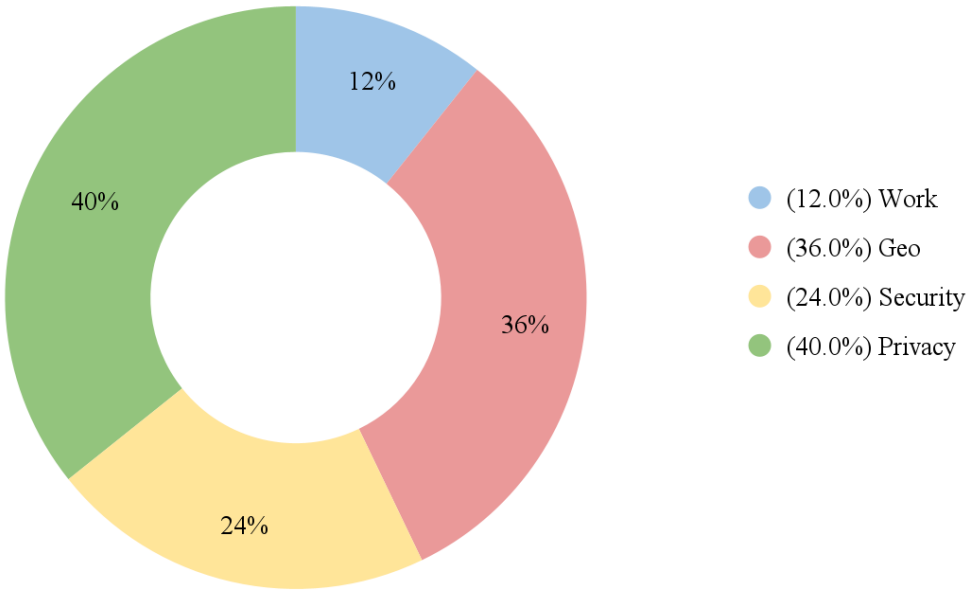


Figure 29 - User personal reason for using VPN

6. What VPN are you using for P2P content delivery?

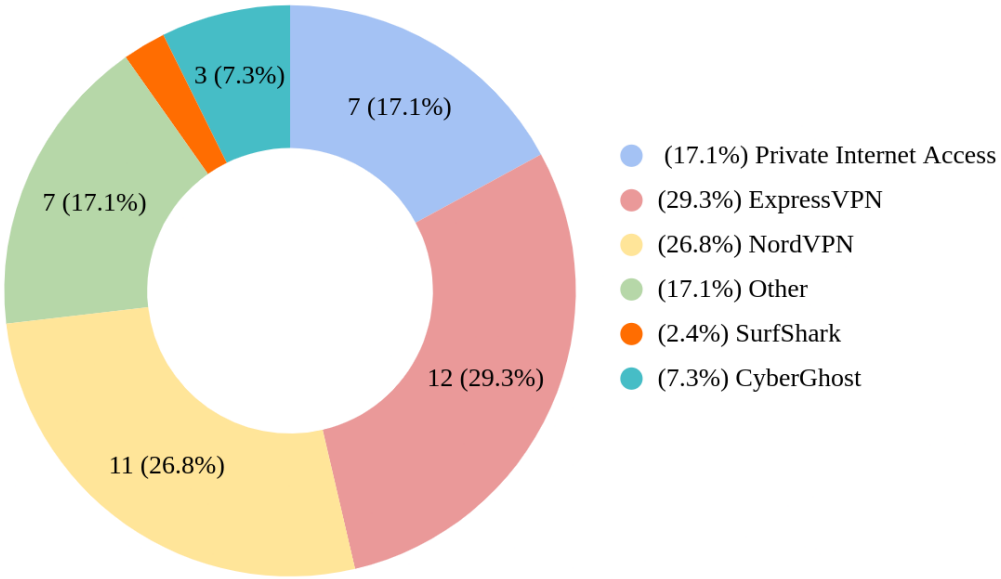


Figure 30 - VPN solution usage for P2P content delivery

7. How effective is your VPN solution for P2P content delivery?

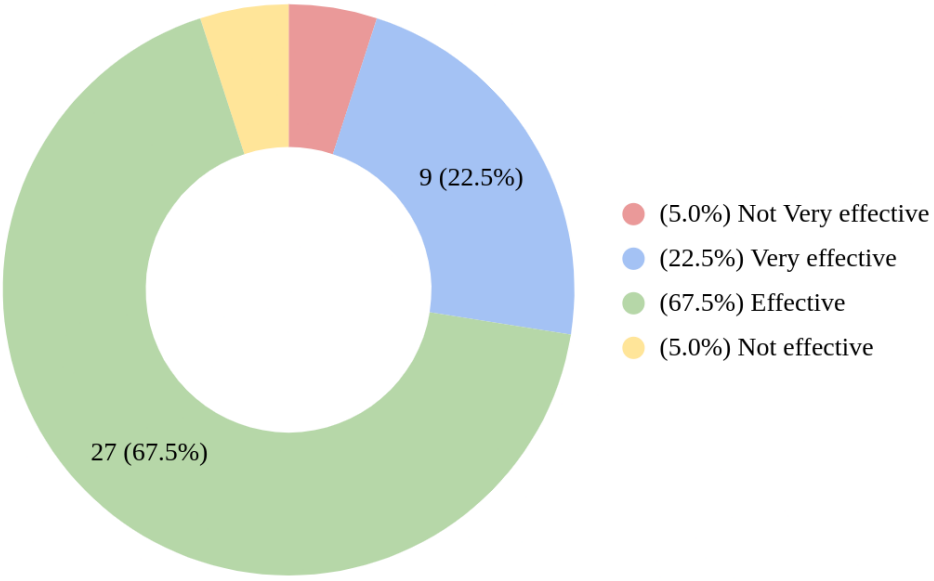


Figure 31 - User opinion on effectiveness of VPN solution

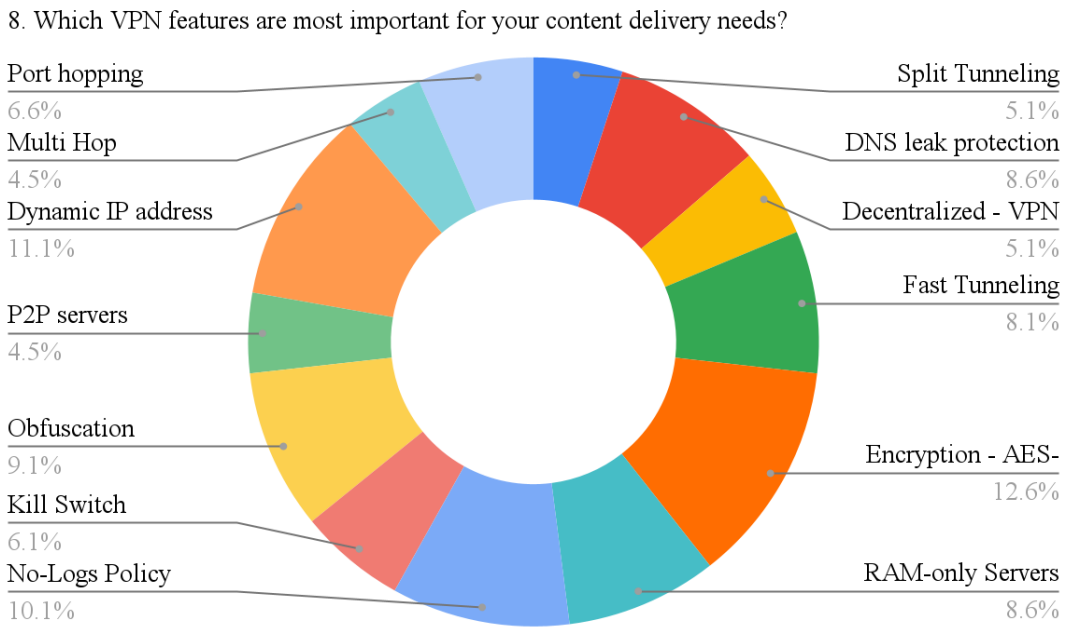


Figure 32 - User opinion on VPN necessary technology for P2P content delivery

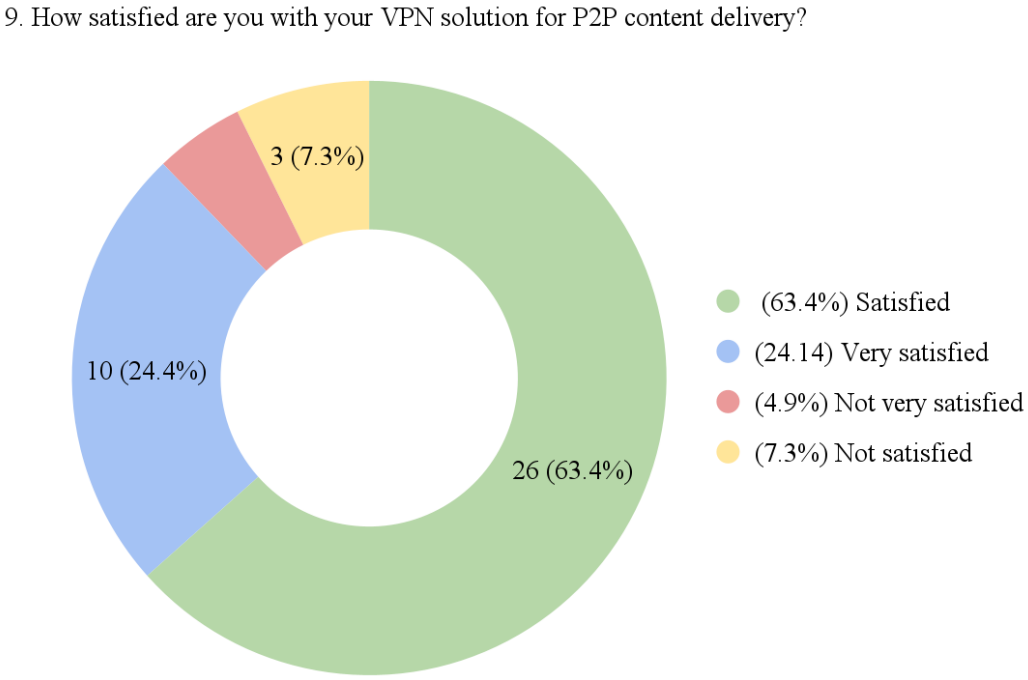


Figure 33 - User satisfaction on selected VPN solution

10. What is your age group?

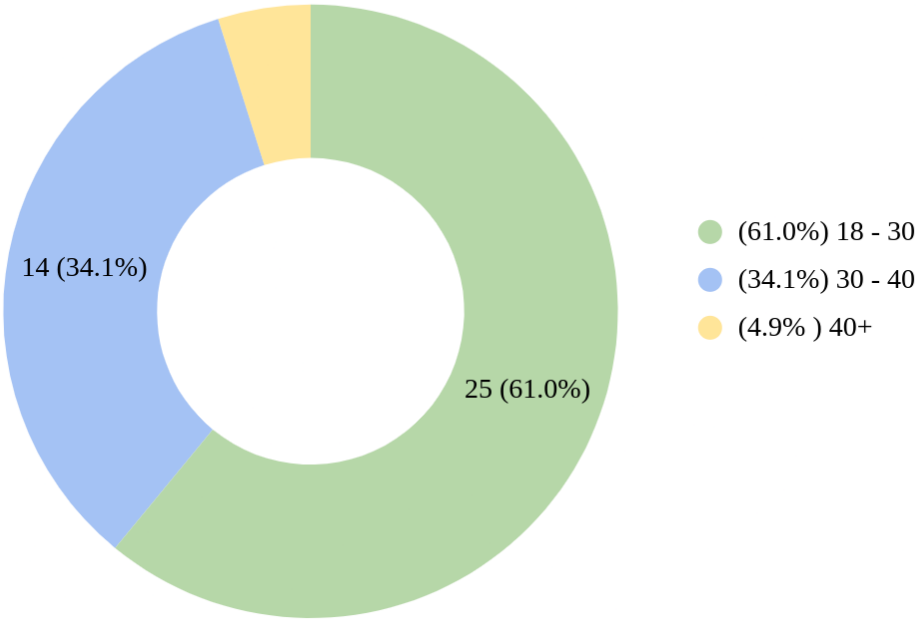


Figure 34 - User age group

11. What is your gender?

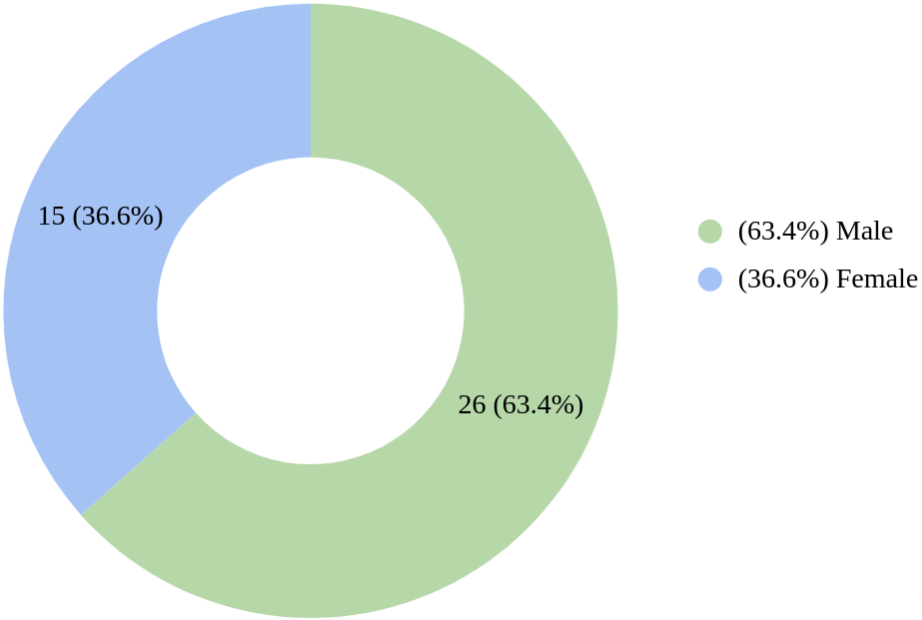


Figure 35 - User gender

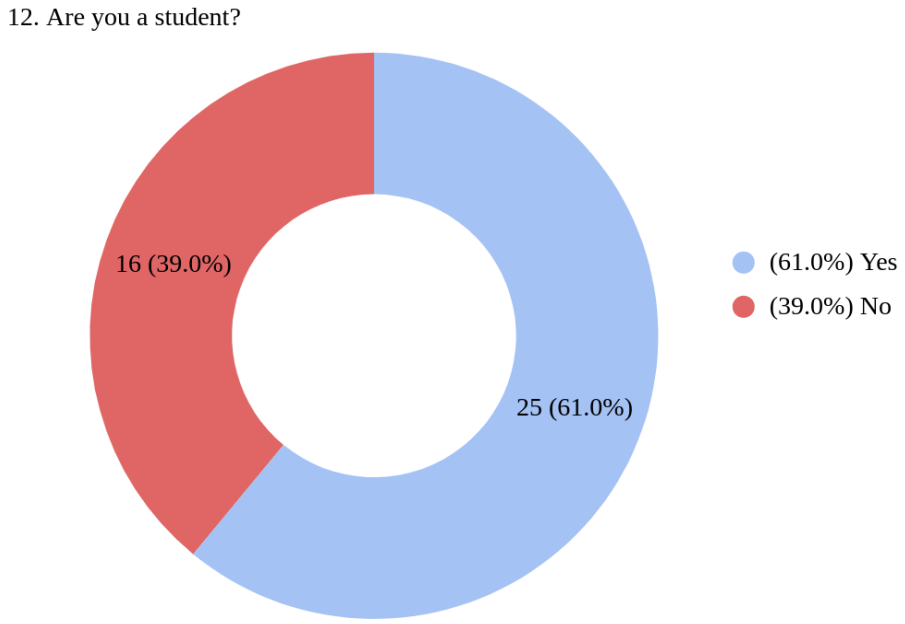


Figure 36 - User educational status

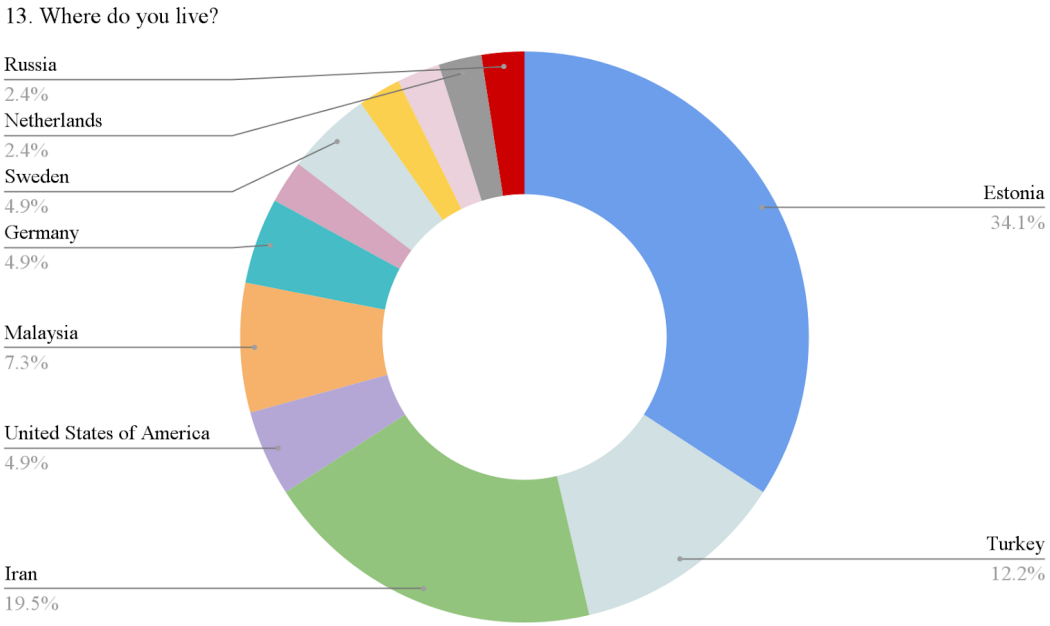


Figure 37 - User country of living

Appendix 3 - License

Attached herewith is an appendix consisting of a Non-exclusive license for reproduction and publication of a Thesis[1]

I, Ali Izady Sadr

1. Grant Tallinn University of Technology free license (non-exclusive license) for my Diploma Thesis "Comparative Analysis of Virtual Private Network Solutions for Peer-to-peer Content Delivery: the Case of Iran", supervised by Kaido Kikkas.

1.1. To be reproduced for the purposes of preservation and electronic publication of the internship report, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the nonexclusive license.

3. I confirm that granting the non-exclusive license does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

15.05.2023

[1] The non-exclusive license is not valid during the validity of access restriction indicated in the student's application for restriction on access to the internship report that has been signed by the school's dean, except in case of the university's right to reproduce the report for preservation purposes only. If an internship report is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her internship report consent to reproduce and publish the internship report in compliance with clauses 1.1 and 1.2 of the non-exclusive license, the non-exclusive license shall not be valid for the period.