Personal Specialization Project (PSP)

Document

Cybersecurity Specialization

|  |  |
| --- | --- |
|  | **Written By:**  - Farros Ramzy, Farros |
|  | (3767353) |

**Abstract**

This document is written by Farros Ramzy to fill in the personal specialization project in cybersecurity semester 4 in Fontys ICT Eindhoven. And this document will contain information of the project which is holding the topic of the influence of virtual private network (VPN) on the internet. The information will mostly explain the reasons of choosing this topic for the project, things that have been researched for the topic, time that was spent by the writer to do the research, and the results of the research and information gatherings about the VPN. Diagrams, conclusions, and recommendations for the readers regarding to this project topic is also included.

**Table of Document Version**

|  |  |  |
| --- | --- | --- |
| Document Version | Date | Description |
| 0.1 | 06/06/2023 | Adding the goal of the topic and Research Question. |
| 0.1.1 | 06/06/2023 | Adding the sub-questions and defining the DOT Framework approaches. |
| 0.5 | 07/06/2023 | Finishing the introduction. |
| 0.5.1 | 09/06/2023 | Adding a brief description of the VPN. |
| 0.5.2 | 09/06/2023 | Adding some examples of the VPN. |
| 0.5.3 | 10/06/2023 | Adding the advantages of using VPN. |
| 0.5.4 | 10/06/2023 | Adding the disadvantages of using VPN. |
| 0.5.5 | 10/06/2023 | Adding a diagram image in the finding section. |
| 0.5.6 | 11/06/2023 | Adding Experiment Result. |
| 0.5.7 | 12/06/2023 | Adding Conclusion & Recommendation. |
| 1.0 | 12/06/2023 | Captioning all image and tables |
| 1.2 | 14/06/2023 | Adding research method to the research question and changing the DOT Framework paragraph. |

**Timetable**

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Activity | Date | Time range |
| 1. | Searching for a sufficient topic. | 01/06/2023 | 15.00 – 20.00 () |
| 2. | Searching for a sufficient topic. | 02/06/2023 | 09.00 – 14.00 () |
| 3. | Exploring the topic, finding the pros and cons of the topic from the internet. | 05/06/2023 | 09.00 – 14.00 () |
| 4. | Starting the document structure by adding the abstract, headings, goals, and research questions. | 06/06/2023 | 09.00 – 14.00 () |
| 5. | Searching examples and applying them to the project, also creating diagrams for the topic. | 09/06/2023 | 09.00 – 12.00 ()  13.00 – 16.00 () |
| 6. | Finding out references to add further information about the topic. | 10/06/2023 | 09.00 – 12.00 ()  13.00 – 16.00 () |
| 7. | Finding out references to add further information about the topic. | 11/06/2023 | 09.00 – 12.00 ()  13.00 – 16.00 () |
| 8. | Deciding the conclusion and finalize all image and table editing. | 12/06/2023 | 09.00 – 13.00 () |
| 9. | Finalizing document. | 14/06/2023 | 09.00 – 15.00 () |

**Table of Abbreviations**

|  |  |  |
| --- | --- | --- |
| No. | Abbreviation | Description |
| 1. | VPN | Virtual Private Network |
| 2. | IP | Internet Protocol |
| 3. | MAC | Media Address Control |
| 4. | PSP | Personal Specialization Project |
| 5. | IoT | Internet of Things |
| 6. | DOT | Development Oriented Triangulation |
| 7. | SSL | Secure Sockets Layer |
| 8. | TLS | Transport Layer Security |
| 9. | PPTP | Point-to-Point Tunneling Protocol |
| 10. | SSTP | Secure Socket Tunneling Protocol |
| 11. | L2TP | Layer 2 Tunneling Protocol |
| 12. | IKE | Internet Key Exchange |
| 13. | TCP | Transmission Control Protocol |
| 14. | UDP | User Datagram Protocol |
| 15. | PPP | Point-to-Point Protocol |
| 16. | OS | Operating System |
| 17. | TOR | The Onion Router |

**List of Figures**

[Figure 2. 2. 1 VPN diagram 10](#_Toc137674109)

[Figure 2. 3. 1 Cisco AnyConnect 11](#_Toc137674124)

[Figure 2. 3. 3 ExpressVPN 11](#_Toc137674125)

[Figure 2. 3. 4 NordVPN 12](#_Toc137674126)

[Figure 2. 3. 2 SuperVPN 13](#_Toc137674127)

[Figure 2. 5. 1 The NMAP command example. 15](#_Toc137674144)

[Figure 2. 5. 2 The NMAP result. 15](#_Toc137674145)

[Figure 2. 5. 3 AnyConnect Activation. 15](#_Toc137674146)

[Figure 2. 5. 4 NMAP result after using the VPN. 16](#_Toc137674147)

**List of Tables**

[Table 1. 1 List of applied DOT Framework. 7](#_Toc137641108)

[Table 2. 1 List of VPN protocols. 8](#_Toc137641116)

[Table 2. 2 List of pros and cons of the VPN. 13](#_Toc137641117)

Table of Contents

[1. Introduction 6](#_Toc137677382)

[1.1. Goal of The Project 6](#_Toc137677383)

[1.2. Research Questions 6](#_Toc137677384)

[1.2.1. Main Question 6](#_Toc137677385)

[1.2.2. Sub Questions 6](#_Toc137677386)

[1.3. DOT Framework 7](#_Toc137677387)

[2. Findings 8](#_Toc137677388)

[2.1. About VPN 8](#_Toc137677389)

[2.2. The Way How VPN Works 9](#_Toc137677390)

[2.3. Examples of VPN 10](#_Toc137677391)

[2.3.1. AnyConnect 11](#_Toc137677392)

[2.3.2. ExpressVPN 11](#_Toc137677393)

[2.3.3. NordVPN 12](#_Toc137677394)

[2.3.4. SuperVPN 13](#_Toc137677395)

[2.4. Advantage & Disadvantage 13](#_Toc137677396)

[2.5. Experiment Result 14](#_Toc137677397)

[3. Conclusions 16](#_Toc137677398)

[4. Recommendation 17](#_Toc137677399)

[5. Reference 18](#_Toc137677400)

# Introduction

Personal Specialization Project (PSP) is a project that assigned to the cybersecurity student regarding to find out the importance of cybersecurity in a daily life of internet, social media, and device accessing. Other than that, this project purpose is to find out a solution to solve a common cyber threat which highly happens to a lot of users of the internet and IoT devices.

The topic of this PSP can be variative, depending on the choice of the student for the portfolio and profile document.

And following to that reason, the writer of this document had chosen to do research about an internet security system named virtual private network (VPN).

Virtual private network is a tool to establish a protected network connection for a user while using any public network such as Wi-Fi network so the user identity cannot be sought by others. The way of how the VPN is protecting the identity of the user is by encrypting the internet traffic and disguise the online identity of the user, such as the IP and the MAC address. And this encryption process usually just takes place in real time.

## Goal of The Project

By the chosen topic, this project is aimed to tell the readers about VPN from both two different point of views. And this is starting from giving a general idea of a VPN, the way of how it works in a network system, the safety levels of VPN based on examples, until the advantages and the disadvantages of the VPN.

Other than that, the goal of this project is to find out the effect of the VPN to the worldwide network security.

## Research Questions

Regarding to the goal and the scope of this project, the following research question and sub-questions must be answered by the end of the project.

### Main Question

Why is VPN very important for the internet users nowadays?

To answer this question, some literature studies about the important of VPN has been done. The research is mostly about reading articles which are mentioned in the Reference. Some question-and-answer sessions from social media is also one other solution to get the answer for this question. The result of this question is mentioned in Findings and Advantage & Disadvantage section of this document.

### Sub Questions

From the answer to the Main Question above, the topic of the research can be elaborated into some sub-questions which are written down here.

|  |  |
| --- | --- |
| 1. | What exactly is a VPN?  This question is answered by doing the literature study about the VPN from the reference. The result of this research is a brief knowledge about the VPN which is written in About VPN of the Findings section. |
| 2. | How to use a VPN?  This question is answered by analyzing the behavior of an available VPN product, then doing the experiment with it. The result of the experiment is listed in Experiment Result section of this document. |
| 3. | What makes VPN applications very popular?  This question is answered by looking at the information from any available articles of the VPN and its example products. General information about the VPN that results the reason of its popularity is written in this About VPN of this document. |
| 4. | What makes a VPN is good for the internet users?  A literature study through out the article in Reference section and the question-and-answer session from a certain social media have answered this question. The answers are written inside the About VPN and Advantage & Disadvantage sections below the Findings of this document. |
| 5. | What might be the disadvantage of using a VPN?  A literature study and problem analysis have been done to answer this question. A security test result from the experiment to the VPN product is also become a proof of the answer from this question. |

And the mentioned methods to answer each question are classified by the DOT Framework section below.

## DOT Framework

Based on the progress of this project, there are three types of frameworks from the DOT which have been done. And with the methods that have been mentioned in the Research Questions section above to answer each of the question, each method and framework can be classified inside this Table 1. 1 below.

Table 1. List of applied DOT Framework.

|  |  |  |
| --- | --- | --- |
| Framework | Methods | Description |
| Field | Problem Analysis | This method is done by creating questions regarding to the topic of the issue. The questions are determined by understanding the topic of the project. In this case, the research questions that have been written in the previous section are the results of this approach. |
| Library | Literature Study | This method is done by reading and looking out to any source of information that related to the topic, to gather any data that might become the best answers for each research questions of the topic. |
| Available Product Analysis | This method is done by looking on information from some product examples that are related to the topic of this project. |
|  |  |  |
|  |  |  |
| Lab | Security Test | This method is done by using one of the product examples and to find out any advantage and disadvantage that results from the product example to the testing device. |

# Findings

By doing this project based on the DOT framework system, along with the timeline table mentioned in the front page of the document, there are five findings of this VPN topic which are now listed in this section of this report document.

And these findings are mostly about:

|  |  |
| --- | --- |
| 1. | An explanation about VPN. |
| 2. | The way how the VPN works. |
| 3. | Some examples of VPN. |
| 4. | The advantages and the disadvantages of the VPN. |
| 5. | An Experiment, using VPN |

## About VPN

As explained in the Introduction of this document, VPN is a tool to disguise an internet user identity to protect the user of a network from any risk of data leaks.

Based on the protocol, there are different types of VPN which are commonly used over the internet. Some of these protocols are listed in this Table 2. 1 below.

Table 2. List of VPN protocols.

|  |  |  |
| --- | --- | --- |
| No. | VPN Protocol | Description |
| 1. | OpenVPN | OpenVPN is an open-source protocol which uses techniques to create secure point-to-point and site-to site connections in routed or bridged configurations and remote access facilities. This protocol is implementing both client and server applications.  The encryptions that this VPN protocol use are the SSL/TLS encryption which can support various authentication methods.  And because of this, this VPN protocols known by its strength and flexibility. |
| 2. | PPTP | PPTP is the oldest VPN protocol ever known. It is still using a TCP control channel and a generic routing encapsulation tunnel to encapsulate the PPP packets instead of using the UDP.  This VPN protocol known to have a good speed quality and compatible with most OS, but it is less secure than the other protocols. |
|  |  |  |
|  |  |  |
| 3. | SSTP | SSTP protocol is a form of VPN protocol which provides a mechanism to transport PPP traffic through the SSL/TLS channel. This SSL/TLS channel provides transport-level security with key negotiation, encrypting, and traffic integrity checking.  This protocol can bypass firewalls because this protocol is operating under port number 443, which also used by the HTTPS. |
| 4. | L2TP | L2TP is a form of VPN protocol which provides the cost-effective access for its remote users. It is doing it by letting a collection of network system to manage the assigned IP address for the remote user.  In computer networking, L2TP is used to tunneling a private network as a part of the ISP services. The encryption that this protocol used are only for its own control messages. |
| 5. | IKE | IKE or what currently known as the IKEv2 protocol is a VPN protocol which provides the best security and speed stability. It establishes a secured communication between devices and defines negotiation and authentication processes for IP security associations. |

These five protocols in Table 2. 1 above are the most common protocols which are still being used by most VPN nowadays, even there are less VPN which still using the PPTP protocol, except for encapsulating the PPP packets of a data. Mostly, the PPTP protocol is combined with the SSTP or OpenVPN protocol.

So, how secure is a VPN?

Unlike using private browsing system from a web-browser, using a VPN as a network protection can be the safe way to browse the internet. The VPN security is sure can protect the IP and encrypt data history of a user to prevent any reconnaissance threat from the internet data provider, government, and malicious cyberthreat in the network. However, it is unlikely to fully protect the network user from every bad scenario from the cyberthreat itself.

The main thing is just to disguise.

Unlike firewall, VPN is not blocking any attack that is launched through the network to a connected device. However, VPN allows user to protect themselves and their organization by creating a private web browsing session. This is especially important while using the public Wi-Fi or public network to prevent other people from eavesdropping on the user’s online activity and the data, also the information they share within the network. A VPN creates a secure tunnel between a user’s computer and the VPN server, which hides their online activity and location.

## The Way How VPN Works

VPN hides the IP address by letting the connected network to redirect a connection through a specially configured remote server, run by a VPN host. This process means that if a user surf online with a VPN, the VPN server becomes the source of the user’s data. This process made the internet service provider and other third parties on the same network cannot see which connection that the user is visiting at that moment, or what data that the user send and receive in that network.

This process also can be seen in the diagram which has drawn in this Figure 2. 2. 1 below.

A diagram of a network connection

Description automatically generated with medium confidence

Figure 2. 2. VPN diagram

From that Figure 2. 2. 1 above, it is known that the VPN is acting as the intermediate server on the network communication between the user and the internet. In this position, the sniffer and hacker cannot see anything that goes from the user to the VPN because the VPN is encrypting the user device network identity. Even if both malicious actors are trying to peek on the connection from the VPN to the internet, they will not have a chance to find the user’s network identity either because the network IP is unknown.

Other than this, the VPN security may connect a user’s device to the VPN server, then passing their internet traffic through the VPN provider’s internet connection. This behavior hides browsing information and makes it more difficult for bad actors to gather or monitor the user’s online activity. The traffic passing may also disguise the user’s whereabouts, like because the demographic location data comes from a server in another country, the actual location of the user cannot be determined.

In addition, most VPN services do not store logs of the user’s activities, unlike some regular internet providers on a third-party range of the user’s network. This is the reason why VPN is popular and considered as an important security tool for the internet nowadays.

## Examples of VPN

To get to know more about VPN, these below are some examples of the VPN, based on a rough search from the internet references.

### AnyConnect

|  |  |
| --- | --- |
| Figure 2. 3. Cisco AnyConnect | AnyConnect is a VPN product from the Cisco Company. This product has a system that supports the virtual private clients.  Based on the article in the Reference, the software of this VPN product provides a secure way to connect to computer networks via SSL VPN protocol which allows access to a remote network.  The advantage of this VPN product is it has the additional security protection when tunneling to private commercial networks through the internet hotspot. And in addition, it also includes an additional secure connection to a certain important computer network, network management access, web security, and more with many benefits and capabilities from its AnyConnection tool. |

AnyConnect software, along with a very simple and easy implementation of VPN remote access, can meet the organization’s security needs to protect users against attackers and cyber threats. This VPN tool is an integrated agent which designed to protect organization. It provides several security services and enables the activities of the employees of an organization remotely while using their own personal smart device without any difficulties and interruptions.

However, the AnyConnect tool is not a free budget VPN for the user. To get a good service from this VPN, the user must buy and subscribe to get its license by its policy.

### ExpressVPN

|  |  |
| --- | --- |
| A red and white logo  Description automatically generated with medium confidence  Figure 2. 3. ExpressVPN | ExpressVPN is a VPN service offered by the British Virgin Islands registered company Express Technologies Ltd. The software of this product is marketed as a privacy and security tool that encrypts users’ web traffic and masks their IP address.  The apps that were released by the ExpressVPN company are compatible with Windows, macOS, iOS, Android, Linux, and routers.  The software product of this VPN tool also featured a smart DNS feature called the MediaStreamer, to add the VPN capabilities to devices that do not support them which make this tool almost compatible with a lot of type of devices that are using a network protocol. |

The parent company of this VPN tool is also developing a leak testing tool, which enable the ExpressVPN users to determine if their VPN provider is leaking a network traffic, DNS, or true IP addresses while it is connected to the VPN, like when the device is switching from the wireless to a wired internet connection, or the other way around.

But similar like AnyConnect, ExpressVPN is not a free budget VPN for the user. The user should create a subscription data if they want to use this app with various security budget that are already provided. Nevertheless, the user can still get a free charge from the budget subscription at the start of the appliance for at least, seven days.

### NordVPN

|  |  |
| --- | --- |
| A logo of a mountain  Description automatically generated with low confidence  Figure 2. 3. NordVPN | The NordVPN is a VPN tool service provided by the Nordsec Ltd. with some software applications for the Microsoft Windows, macOS, Linux, Android, iOS, and Android TV OS. And beside these, this VPN service also have a manual setup which available for the wireless routers, NAS devices, and other platforms.  This VPN tool routes all users’ internet traffic through a remote server run by the service, thereby hiding their IP address and encrypting all incoming and outgoing data. For encryption, NordVPN has been using the OpenVPN and IKEv2 protocols in its product.  It also uses L2TP and PPTP connection one time, but they were later removed due to a large, outdated version issues. |

Besides the feature of the general-use VPN servers, the NordVPN offers servers for specific purposes, including the P2P sharing, double encryption, and connection to the TOR anonymity network. And it has a free feature to enable users to create a local mesh network.

The mesh feature allows the NordVPN users to create their own local network between their included devices without any disruption of the public network connectivity and third-party interruption. The number of devices that may linked into this network are roughly up to sixty.

But again, this VPN is not a free budget VPN. To get a full security service, the users must apply a paid subscription. And the subscription choices that were provided by the NordVPN start from the monthly, to yearly subscription.

### SuperVPN

|  |  |
| --- | --- |
| A blue shield with white text  Description automatically generated  Figure 2. 3. SuperVPN | SuperVPN is an Android VPN service which provides the user a free in charge security service. But despite its free in charge service, this software is lacking a lot of essential features as a VPN.  Based on the expert review, even this VPN offers a good speed internet, support torrenting, and offers a free plan, the VPN tool is missing all the industry-standard VPN security features. This VPN does not use the 265-bit AES encryption to encrypt the users’ network identity. And after that, the tool does not have a kill switch, and it keeps logs of the user data.  The software itself have no offers for customer support which make this VPN untrustworthy. |

The system policy of this VPN tool is also inconsistent. When the user tried to change its connection traffic, the user’s IP address did not change. Instead, it only masks the device name into unknown. And the data of the users during the network activities still leaking somewhere else.

This made the app looks more malicious to the user rather than secured.

## Advantage & Disadvantage

Based on what was written in the Introduction, the basic advantage of a VPN is it may work as a disguising tool to protect the user’s network identity. And the most disadvantage of the VPN is when it is not meant to fully protect the user’s network connection.

However, there are more pros and cons about VPN that have found from the article references.

And this pros & cons information can be seen inside this Table 2. 2 below:

Table 2. List of pros and cons of the VPN.

|  |  |  |
| --- | --- | --- |
| No. | Advantage | Disadvantage |
| 1. | VPN may give a primary benefit such as increased security. The encryption provided by the VPN mostly made to block the user’s data from being peeked or accessed by the ISP, third-party of the network, and hackers. This is very important, especially when the user is connected to an unsecured public network. | The benefit of the VPN mostly not come for free for the users. Although there are many free VPN product on the internet, most of them are not reliable, and possible to be an ungenuine product. |
|  |  |  |
|  |  |  |
| 2. | The privacy that the VPN provide to the user by encrypting the network traffic is also a good benefit to use the VPN. By changing the network traffic, the network user will appear to be unknown on the websites, so advertisers, or other entities in the websites cannot track the user activity, nor the user location either. | While the VPN changing the user’s network traffic, the user’s network speed is also reduced. This speed reduction is mostly caused by the extended encrypt and decrypt process inside the network communication while the VPN is activated. |
| 3. | VPN may allow the network user to bypass the geo-restriction from the network government in their actual geography area. This is caused by the method of the VPN to encrypt the user’s network traffic, which make it visible as the user is surfing on the foreign server. | Although the VPN allowed user to bypass their network’s geo-restriction, the user still might face a potential legal and policy issues. It is very important to understand the laws and regulations regarding to the usage of the VPN in the local jurisdiction. |
| 4. | VPN also has a remote access which is enabled to private networks, which might be useful for doing a business remotely while the users supposed to need to access company resources directly. And this connection service is still secured for both ways because the network traffic and identities are encrypted. | A lot of VPN service have a compatibility issue to the device it was installed in. Sometimes, the users must fully understand their internet protocol and device version before installing the VPN that they are subscribing to. And the users also must know the tools and service that the VPN is providing because every tool in every VPN product might be vary. |
| 5. | VPN can help to protect the user’s sensitive data, for example, the transaction history, personal information, and data transfer through the network from being intercepted by reconnaissance activities from a potential hackers or snoopers. | The VPN users usually must put their trust to the VPN providers and the network traffic providers that they were switching into. This regulation sometimes needed because every network traffic has their own geo-restrictions.  And the VPN providers need the trust certificate regulation that must be accepted by the user because of this restriction issue.  However, this regulation might be dangerous for the user if the VPN product is not legit. |

## Experiment Result

While researching the security of the VPN, a testing experiment is truly needed. In this section, the document will explain what findings that have been found while doing an experiment with a VPN app, such as the Cisco AnyConnect from the Examples of VPN section which is already written in this document above.

To do this experiment, two devices are needed. One of them is a device with Kali Linux, and the other one is a device with an installed VPN application.

In this case, the writer uses the PC with Kali OS, and an Android phone which is already installed with AnyConnect application.

To test the security, it is better to connect both devices into the same Wi-Fi connection.

And the first thing to do after that is running an NMAP command such as:

*$ nmap -sP <IP address/divider>*

Since the writer pretend if the device is a random target device, the last digit of the IP address should be written as zero (0) like this Figure 2. 5. 1 below.

And since the IP address uses 24 digits of binary value to address the host, then the divider value should be written as 24.

A picture containing text, screenshot, font

Description automatically generated

Figure 2. 5. The NMAP command example.

After the command has proceed, the next step is looking at the NMAP result.

Like in this Figure 2. 5. 2 below, the NMAP is showing the Android device with IP address and MAC address. In summary, the network data of the device is already exposed to the Kali Linux.

A picture containing text, screenshot, font

Description automatically generated

Figure 2. 5. The NMAP result.

Nevertheless, this Android device is installed with the VPN app already.

To hide the network data of the device, the user must activate the VPN app.

And in this case, the user is using the AnyConnect VPN to hide the device identity.

|  |  |
| --- | --- |
| A screenshot of a phone  Description automatically generated with medium confidence  Figure 2. 5. AnyConnect Activation. | To do this, the user must choose the connection server to the AnyConnect app. It can be done by select the connection in the main screen of the App and click the plus button to add a new server.  The user then can write the server’s name and click add after the “add new server” input box popped up on the screen. However, most server should have credentials authentication.  When the user is trying to connect to this kind of server in this VPN app, the user must fill in their username and password.  Once the login succeeds, the VPN will run the program to connect the system into the selected server. |

After that, when the Kali run the same NMAP command again in the same IP address, the result will be changed into this Figure 2. 5. 4 below for the same device.

A picture containing text, screenshot, font

Description automatically generated

Figure 2. 5. NMAP result after using the VPN.

Comparing Figure 2. 5. 2 and Figure 2. 5. 4 above, the device name changed to unknown after it is connected to the VPN. And other than that, the MAC address has changed either.

Even the IP address is similar, the device is now communicating to the network using the other IP address which is not visible to this NMAP scanning.

Even if the spoofer looking further into this IP address in Figure 2. 5. 4 above, the spoofer will not see the internet activity of the device user.

# Conclusions

Based on the findings, it is known that the VPN service is very important to keep the user privacy data safe while doing network activities. The VPN is become popular nowadays because the risk of suffering an internet sniffing and the network spoofing while doing a regular internet surfing, also social media activities using the public network such as the Wi-Fi network is very high.

Other than that, the changing terms of private browsers where the third-party of the internet network host and server provider can see the users’ internet activity make it very difficult for the internet users to trust the safety of their network identity. And the other problem is whenever the user uses the private browsers, they will still get a spam and malicious ads brought by their standard internet cookies because of this changing terms.

And other than that, a lot of countries put too much geo-restrictions on their main network even to the unnecessary public sites which made some people must face some difficulties to access some network sites.

However, not every VPN is safe for the user. And most VPNs are costly in their subscriptions. Even if there is a free subscription VPN, that VPN is highly possible to be fake, or lacked too many security features as it should be.

Besides that, most VPN with a high demand of encryption process will highly slow down the network connection of the user’s device.

And unfortunately, some VPNs use a policy where they ask their users to fully trust their privacies to the VPN. This policy can be dangerous for the users themselves, knowing that the VPN is still not a firewall.

# Recommendation

For a safe network experience, VPN is worth to be used by everyone. However, it is also recommended to use a firewall after the VPN because as it is known from the start, VPN only blocks visibility to any reconnaissance actor, not defend the system from an exploitation attack.

Looking back at the product example, it is recommended to use or subscribe to at least the cheapest subscription VPN, which is legit, rather than blindly install a free VPN such as the SuperVPN with an ambiguous credential. At least, there are still many legit VPN tools which still have a free basic service in its app, under their subscription choices.

# Reference

* VPN Security: How Secure is it & do you need one?

[https://www.fortinet.com/resources/cyberglossary/are-vpns-safe#:~:text=A%20VPN%20creates%20a%20secure,from%20tracking%20their%20browsing%20activity](https://www.fortinet.com/resources/cyberglossary/are-vpns-safe%23:~:text=A%20VPN%20creates%20a%20secure,from%20tracking%20their%20browsing%20activity).

* Benefits of a VPN

<https://www.fortinet.com/resources/cyberglossary/benefits-of-vpn#:~:text=If%20you%20use%20a%20VPN,and%20receive%20secure%20and%20anonymous>.

* What is VPN?

<https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>

* Best Free VPN Trials in 2023

<https://www.vpn-mentors.com/best-free-vpn-trials/?keyword=best%20vpn&geo=9065223&device=&cq_src=google_ads&cq_cmp=12816219245&cq_term=best%20vpn&cq_plac=&cq_net=g&cq_plt=gp&gad=1&gclid=CjwKCAjwp6CkBhB_EiwAlQVyxYv9mQDUYNZvB152jJK2DObINgyVCPza8A9e7NK6ytJUCmSMresc7RoCnH0QAvD_BwE>

* Why are VPNs so popular today?

<https://www.quora.com/Why-are-VPNs-so-popular-today>

* What is AnyConnect?

<https://operavps.com/what-is-anyconnect/>

* SuperVPN review

<https://www.safetydetectives.com/best-vpns/supervpn/#features>

* ExpressVPN

<https://en.wikipedia.org/wiki/ExpressVPN>

* NordVPN

<https://en.wikipedia.org/wiki/NordVPN>