Network Security and Resilience

NSR/AS Lab 3 – VPNs

Xuan Tuan Minh Nguyen
103819212

Abstract

The main purpose of this report is to provide a closer perspective on Virtual Private Network (VPN), Internet Protocol Security Virtual Private Network (IPSec VPN) and goes through the steps to setup an IPSec VPN on two Ubuntu virtual machines using OpenVPN as the main software. The objective is to focus on introducing the characteristics and the capabilities of Virtual Private Network, the benefits and advantages of Virtual Private Network, IPSec Virtual Private Network and how it could be used for implementing security policy in an organizational way. Moreover, this report will throughly discusses the steps to setup an easy Virtual Private Network tunnel using OpenVPN, the behaviour of OpenVPN and answer the questions regarding features and mechanisms of the Virtual Private Network based on the discussed processes above.

Introduction to VPNs

1. VPN Characteristics and Capabilities

In the context of establishing a secure and reliable connection in the internet environment, Virtual Private Networks, or VPNs pop up as the top-notch solution for user (or enterprise) to protect the data from being stolen on the internet. According to Tomaschek and Long (2023), in simple term, a VPN is a software that establishes a secure connection between your computer and the internet by running your internet traffic through an encrypted tunnel to a server in a remote location. This tunnel ensures that user privacy is protected in the internet environment, while can help user to bypass firewalls and unblock the geographic restricted content.

Nowadays, Virtual Private Networks have several different varieties, from the system wide VPN softwares that hides user's IP Address to browser extensions, site to site, etc., however, all of them are created to serve some identical purposes and create considerate benefits that could be listed as:

i) Bypass Geo-locked Content – By using a Virtual Private Network software to change the user's current address appear to be in that geographic position, user can easily access to the contents that are geographically restricted while staying in a different position. (CDW Expert, 2022)

ii) Safety Through Anonymity – As mentioned above, user when using a Virtual Private Network will have the ability to hide their identities, such as IP Address, data when transmitted through the network. Thus decreasing the chances for hackers to steal essential informations from the users as they will only able to receive the identity datasets from the Virtual Private Network server rather than the datasets coming from the user. (CDW Expert, 2022)

iii) Cost-Effective Security – Technologies are evolving every day, and so do the "security solutions". In the market, there are dozens of new "security solutions" that is developed every single day. However, one notable problem with these solutions are the expensive price to own a license. While a Virtual Private Network might not support scanning virusses or blocking intruders, a VPN might be able to prevent the features as it helps user to be "invisible" online. Thus using a VPN would be a more cost-effective security.

iv) Reliablity – Virtual Private Networks will ensure the integrity and the reliability of the process of transmitting and receiving data when combining with any extensions that help detecting any alteration of transmitted / received data.

2. How VPNs could be used to implement security policy in organizations ?

With the given benefits above, Virtual Private Networks are not only useful for single user, but for companies or big enterprises, VPN plays a huge role on creating a safe, encryted environment for enterprises to transmit essential informations. For companies and big enterprises, a set of security policies is more than essential when it comes to setting up a secure and reliable network environment, as organizations are massively depends on the internet for daily trading operations, thus the internet environment must guarantee the Confidentiality, Integrity and Availabilty triad rule (CIA triad). Such that a network environment must protects data from unauthorized (outside) access, reliable under the cybersecurity attacks and always available (Kidd, 2023). Since a VPN has owned the base concept of a private network, which isolates the traffic inside the network from the outside network environment, thus using a good VPN will ensure that no attackers shall be able to capture the transmitted content inside the VPN. In addition, with more and more improvements and techniques that have been added to Virtual Private

Network, such as IPSec VPN, user authentication, encryption, etc., VPN now is also able to overcome security vulnerabilities regarding public network. In general, having a Virtual Private Network installed is a big advantage for organizations to control the business operation flawlessly without the concerning the security threats, and also acts as a big candidate to be included in every security policies.

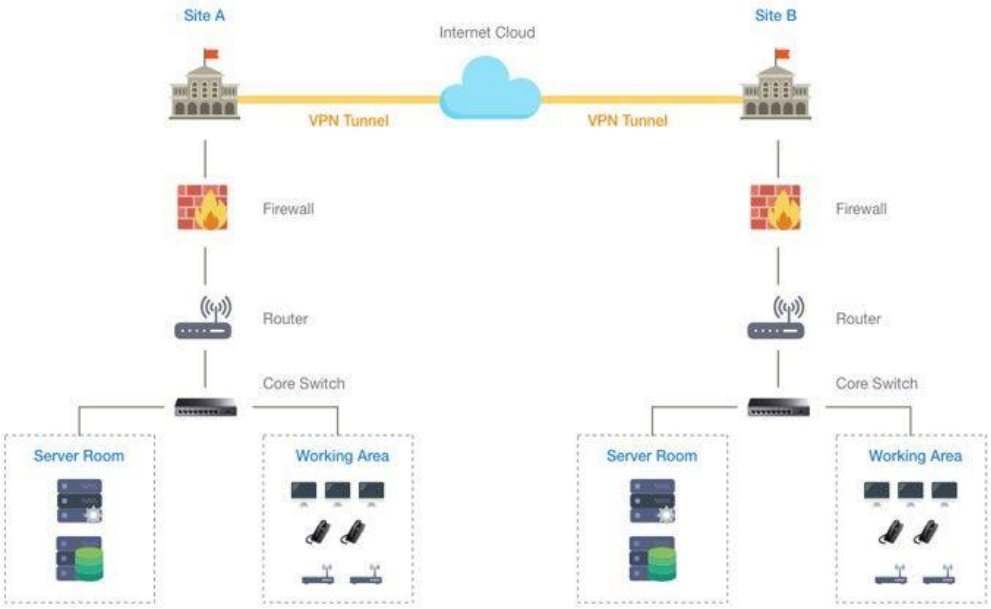

Figure 1: Illustration the mechanism of VPN

OpenVPN Behavior

1. Discussion

We have discussed through how a normal Virtual Private Network works and the advantages that VPN brought, now we will focus on discussing an "improvement version" of Virtual Private Network, which is IPsec VPN. Internet Protocol Security Virtual Private Network, or IPsec VPN in short, is created to protect the IP traffic on the network layer that follows the rule of CIA triad, which must ensure that sender and receiver must be able to read the transmitted data, the data in the packets must not be changed and the sender / receiver could authenticate each other's (Molenaar, 2018). In the figures given below, two Linux Virtual Machines have been established the VPN tunnel using OpenVPN and have been configured with IPsec feature. Here are the steps that took to configure:

i) Generate the static key that will use for authentication between machines using OpenVPN key generator. Figure 2 shows the process of creating static key using the following command "openvpn –genkey –secret mykey". The static key will be in 2048 bit encoded-style key and has the BEGIN and END to mark the begin and end section of the static key.

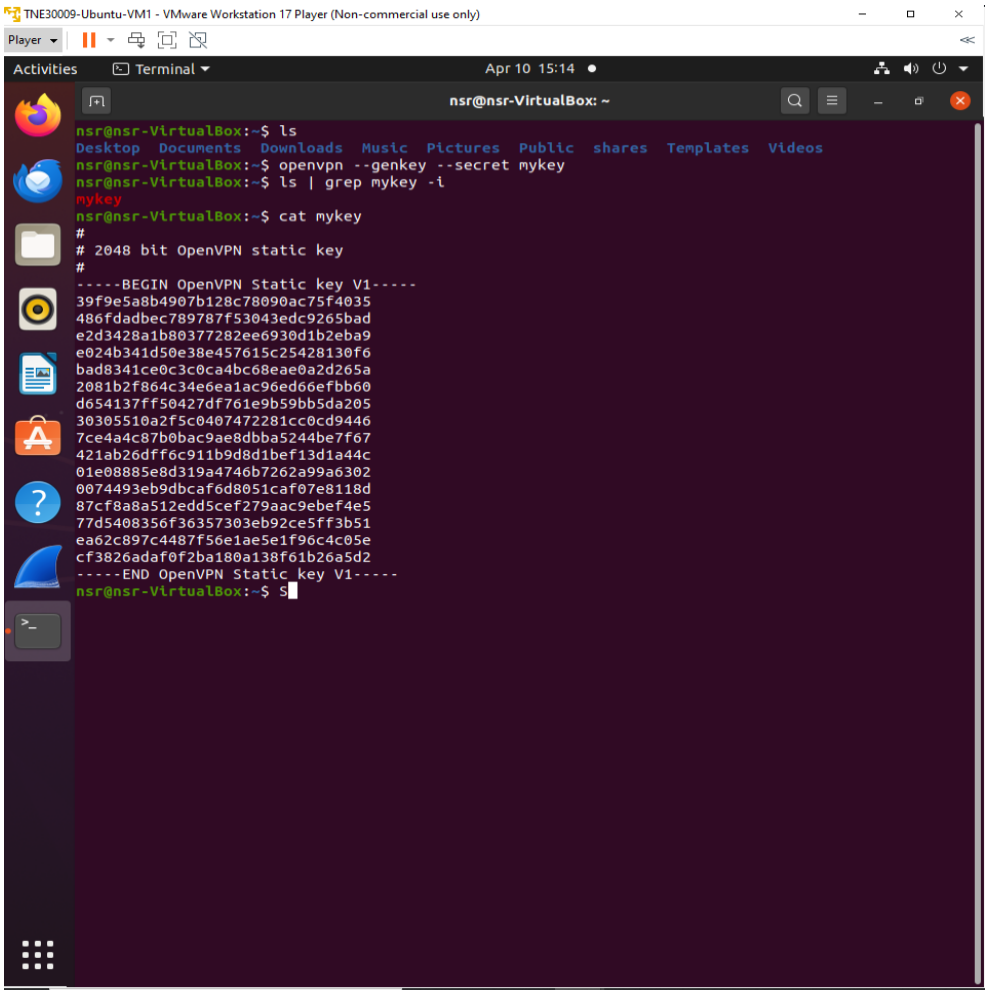

Figure 2: Process of generating OpenVPN static key

ii) The command "scp mykey nsr@192.168.199.129:mykey" (Figure 3) has been used for transferring the static key from the first Linux VM (which has the IP Address of 192.168.199.128) to the second Linux VM (which has the IP Address of 192.168.199.129)

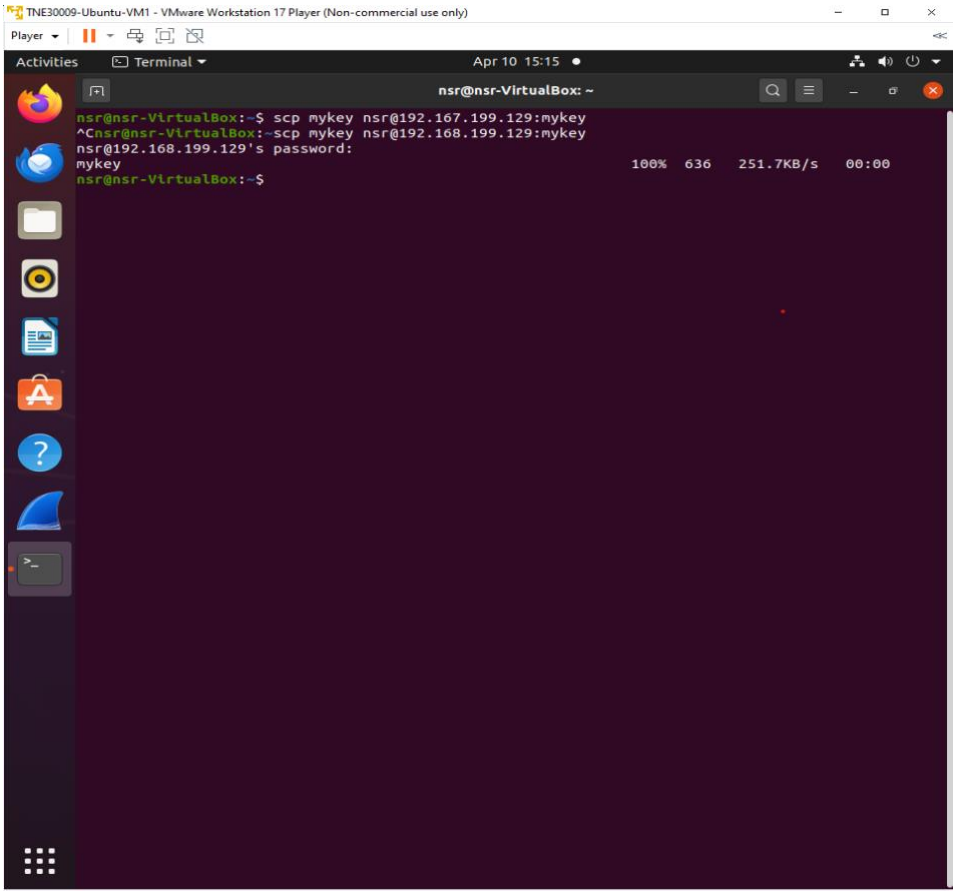

Figure 3: Process of transferring secret key

iii) Figure 4 shows the process of initializing the tunnel that connects two Virtual Machines together using the command "sudo openvpn --remote <IP Address> --dev tun1 --ifconfig 10.4.0.1 10.4.0.2 --verb 5 --secret mykey" where "–remote <IP Address>" specifies the endpoint IP Address that will be used for establishing the tunnel, the "–dev tun1" option tells OpenVPN to use the tunnel device "tun1" while the "—ifconfig 10.4.0.1 10.4.0.2" option is to setup the tunnel with the local IP Address (10.4.0.1) and remote IP Address (10.4.0.2). The last two options, "—verb 5" and "—secret mykey" tells OpenVPN to set the verbosity level to 5 and use the previously generated key (Figure 3) as the secret key for authentication.

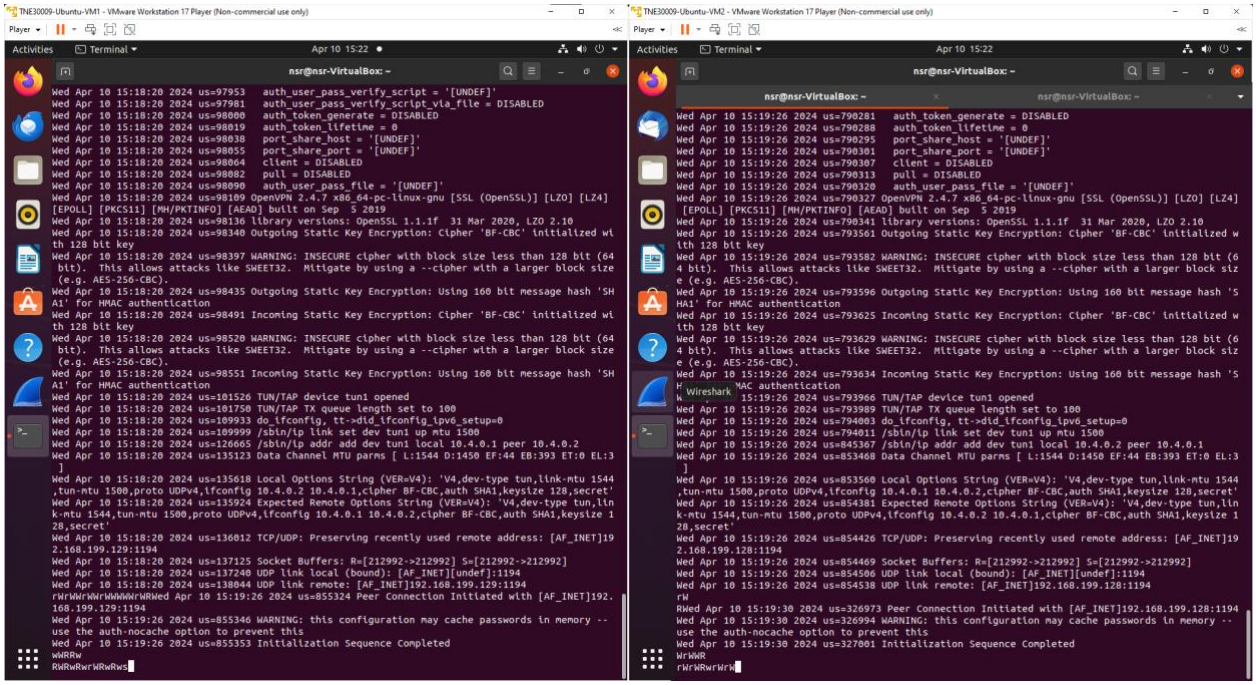

Figure 4: Establishing VPN tunnel between VMs

iv) Figure 5 and 6 shows the tunnel device “tun1” has been uplink after the tunnel is created and is able to communicate with the other end device, which in this case 10.4.0.1.

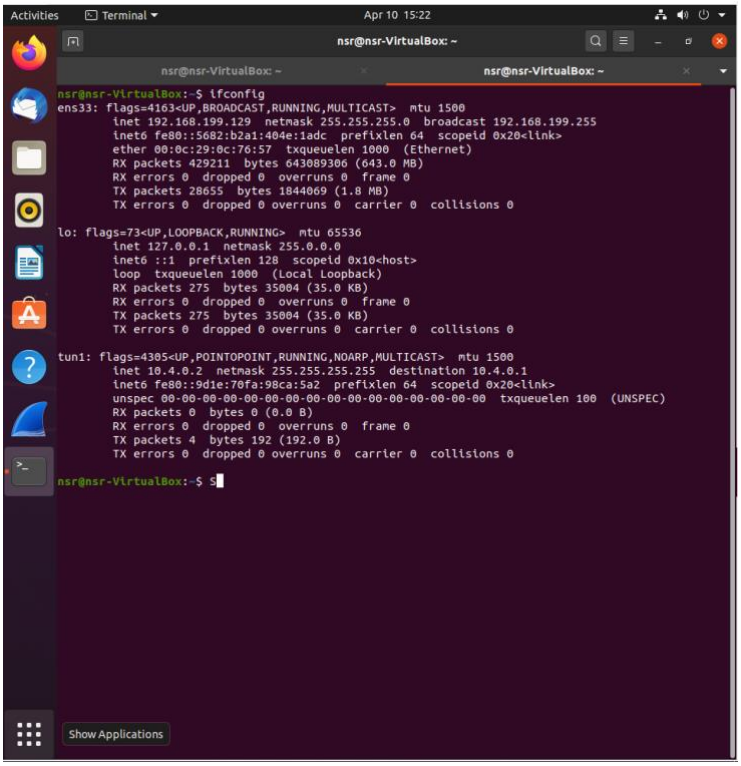

Figure 5: Tunnel device uplink

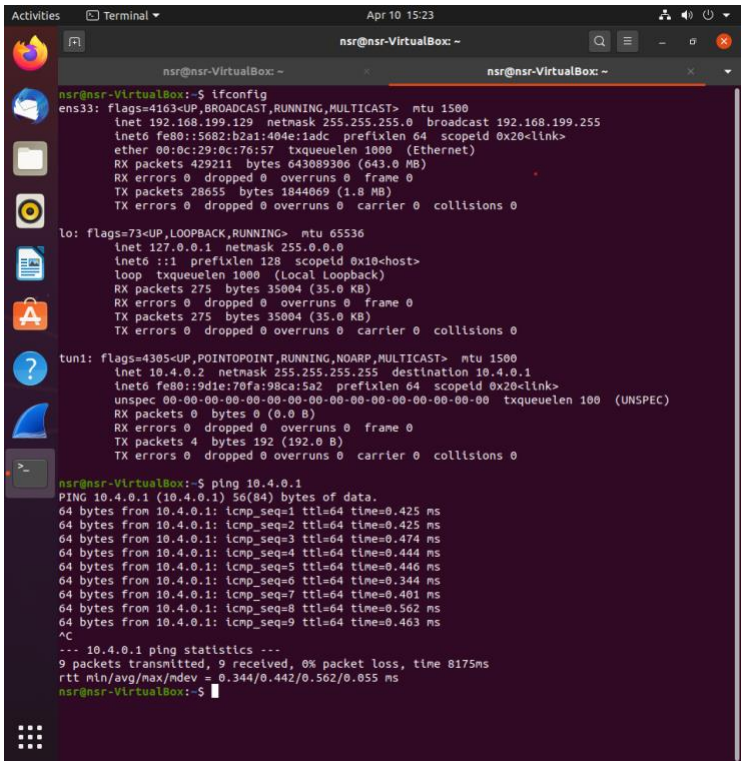

Figure 6: Ping result of the tunnel

2. Traffic encryptions

Capturing inside the tunnel

Figure 7 shows the result when capturing inside the tunnel device (tun1) while telnetting from Virtual Machine 2 (10.0.4.2) to Virtual Machine 1 (10.4.0.1). We can clearly see that the traffic inside the tunnel is not encrypted at all, Wireshark has captured TELNET and TCP protocol while pinging to Virtual Machine 2 (10.4.0.2). The observed traffics, which are TELNET and TCP protocols, are the traffics that are being sent into the tunnel and the traffics coming out from the tunnel.

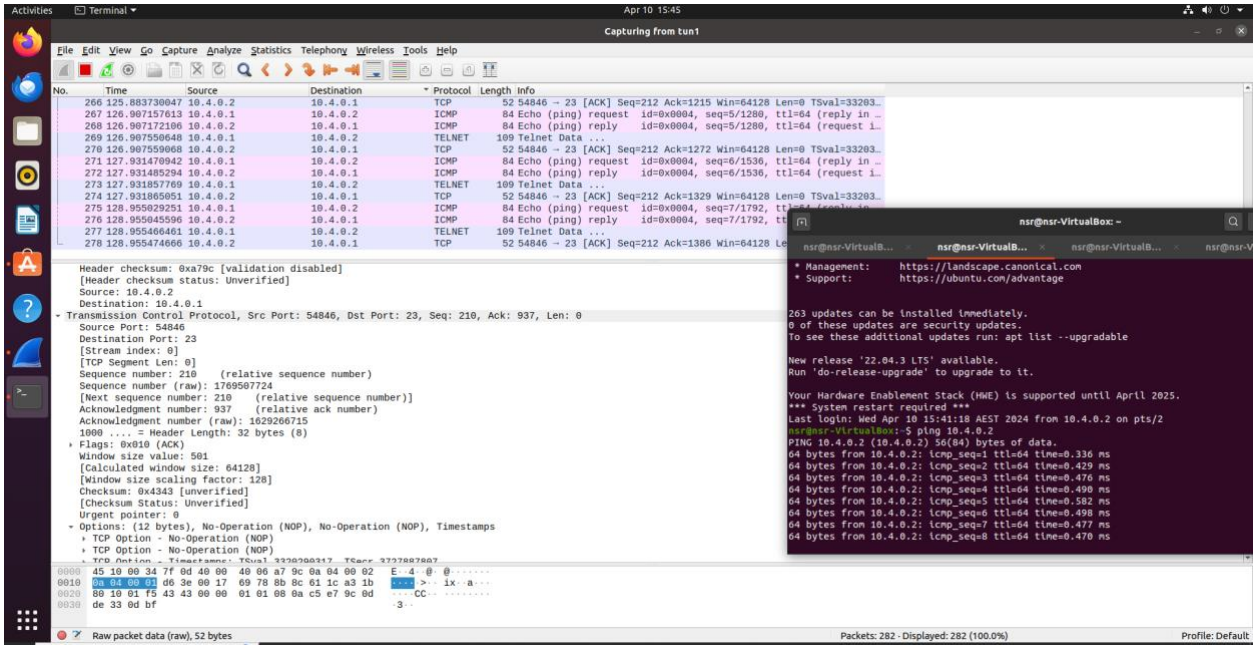

Figure 7: Packet inspecting inside the tunnel

Capturing outside the tunnel

However, in Figure 8, which shows the captured packages when inspecting outside of the tunnel device (ens33 interface in this case), we could see that instead of capturing decrypted packets, such as TELNET and TCP when inspecting inside the tunnel. In this case, the captured packets are OpenVPN, the reason for this is OpenVPN starts encrypting and decrypting the traffic over the physical network before it is delivered locally, thus the captured packages that are outside of the tunnel are mostly encrypted.

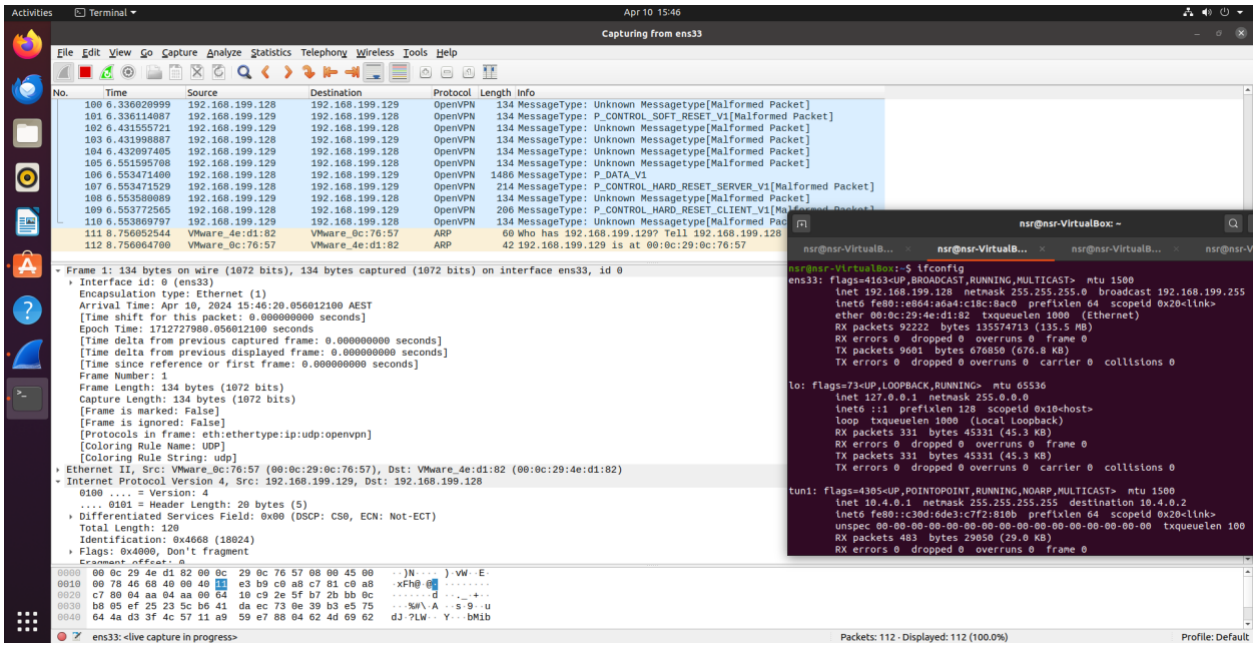

Figure 8: Packet inspecting outside the tunnel

On which interface is traffic encrypted and which interface traffic is not encrypted? Why?

Based on the answer given above, the interface that does not encrypt traffic is the tunnel interface (tun1) and the interface that encrypts traffic is the ethernet interface (ens33). To explain this, tunnel interface (tun1) is the "inner side" of the tunnel, which shows the traffic after the VPN has decrypted for applications and services usage on the local machine. On the other hand, ethernet interface, which ens33 in this case, shows the traffic that is being transmitted over the physical network, or the "outer side" of the tunnel, thus only able to capture the encapsulated and encrypted data packets.

3. *"What is a VPN tunnel?"*

According to Jančis (2021), a Virtual Private Network tunnel is an encrypted connection between the user device and a VPN server, or a private route to the internet via intermediary servers. It is an uncrackable connection without a cryptographic key (Figure 2), thus prevent attackers or even the Internet Service Provider (ISP) gain any access to the transmitted / received data inside the tunnel and also helps user to hide identity while accessing to the internet.

Conclusion

In general, this report provides an overview on what is a Virtual Private Network, its advantages for single user and enterprises. This report also shows the process of creating a VPN Tunnel and how the encrypting / decrypting mechanism works in the VPN Tunnel. We can see how the Virtual Private Network could be able to establish a safe and anonymous connection, how it transmits / receives the data in a very anonymous and unbreakable way in the internet environment. Above all, the main lesson here is user or enterprise who wants to enjoy the benefits of a secure, reliable and who demands to have higher privacy should use the VPN as the main "protection" when going online.

References

[1] A. Tomaschek and M. Long, "VPN FAQ: What You Need to Know About Virtual Private Networks," *CNET*, May 04, 2023. https://www.cnet.com/tech/services-and-software/vpn-faq-what-you-need-to-know-about-virtual-private-networks/

[2] CDW, "Advantages and Disadvantages of a VPN | CDW," *www.cdw.com*, Nov. 07, 2022. https://www.cdw.com/content/cdw/en/articles/security/advantages-and-disadvantages-of-vpn.html

[3] C. Kidd, "Is The CIA Triad Relevant? Confidentiality, Integrity & Availability Today," *Splunk-Blogs*, Jan. 11, 2023. https://www.splunk.com/en_us/blog/learn/cia-triad-confidentiality-integrity-availability.html

[4] R. Molenaar, "IPsec (Internet Protocol Security) | NetworkLessons.com," *NetworkLessons.com*, Jul. 18, 2018. https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security

[5] M. Jančis, "What is a VPN Tunnel and How Does it Work?," *CyberNews*, Sep. 02, 2021. https://cybernews.com/what-is-vpn/what-is-a-vpn-tunnel/