NSR/AS Lab 3 - VPNs

Marco Giacoppo
Dept. of Computer Science
Swinburne University of Technology
Melbourne, Australia
104071453@student.swin.edu.au

***Abstract*—This article describes how to use OpenVPN on Ubuntu computers to implement VPN (Virtual Private Network) technology. The goal of this lab is to use OpenVPN's flexibility and power to create a safe, encrypted VPN tunnel between two Ubuntu computers. This lab focuses on configuring a basic encrypted VPN tunnel between two machines. Using OpenVPN software, a shared secret key is created, transferred to the target computer via SCP (Secure Copy Protocol), and OpenVPN is configured to create the tunnel. This hands-on exercise introduces users to VPN technology and walks them through the basic steps needed to set up a basic encrypted VPN connection on Ubuntu using OpenVPN.**

I. Introduction to VPNs

Virtual Private Networks (VPNs) have become very important in today's networked environment, it describes the opportunity to establish a secure communication over public networks such as the internet. VPNs encrypt your internet traffic and disguise your online identity [1]. VPNs leverage encryption and tunnelling protocols to create private and encrypted connections between remote devices, effectively expanding a private network across a public infrastructure.

VPN Characteristics and Capabilities:

VPNs offer a range of essential characteristics and capabilities that underpin their effectiveness in securing communications over public networks. First and foremost, encryption is a fundamental component that guarantees that information sent over the VPN is protected from unwanted access by means of cryptographic protocols. By confirming the identities of users and devices trying to access the network, authentication mechanisms increase security by preventing unauthorised entry. Furthermore, VPNs use tunnelling protocols to encapsulate data packets inside of secure tunnels, protecting them from being manipulated or intercepted while they are being transferred over a public network. This encapsulation preserves the integrity of transmitted data while also improving privacy. Furthermore, access control mechanisms enable organisations to impose detailed rules on the accessibility of network resources, determining who has access to what information based on predetermined standards like user roles or permissions. Together, these characteristics equip VPNs with the resilience and flexibility needed to meet the diverse security needs of modern enterprises [2].

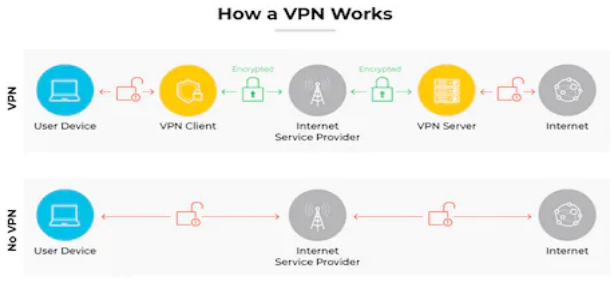

Fig. 1. How a VPN Works. Adapted from [2].

How VPNs can be used to implement organizational security policy.

Virtual Private Networks (VPNs) serve as powerful tools for organizations to enforce and enhance their security policies across distributed networks. By leveraging VPN technology, organizations can achieve several key objectives in alignment with their security policies. Firstly, VPNs facilitate secure remote access, allowing authorized users to connect to the corporate network from remote locations while ensuring that sensitive data remains protected during transmission. This capability enhances workforce mobility and productivity without compromising on security standards. Additionally, VPNs enable organizations to establish secure communication channels between geographically dispersed offices or branches. By encrypting data traffic over these connections, VPNs ensure confidentiality and integrity, mitigating the risks associated with data interception or tampering. Furthermore, VPNs support the implementation of access control measures, enabling organizations to enforce strict authentication and authorization policies for network resources. Whether through user-based access controls or role-based access management, VPNs provide the framework for defining and enforcing access privileges according to organizational security policies. Overall, the deployment of VPNs within organizational infrastructures serves as a cornerstone for achieving secure and compliant network operations while facilitating the seamless flow of information across disparate locations [3].

II. OpenVPN behaviour

A. Discussing the VPN tunnels set up in this lab

We must first confirm that both hosts are operating as intended. To view the network interfaces, we must launch a terminal on each host and type '*ifconfig*'. We had to attempt to ping each other as the hosts after completing this. After the connection was made, we had to create a shared password on one of the hosts, Ubuntu 1. The command '*openvpn -genkey --secret mykey*' was used to accomplish this. The 'mykey' file will contain a 256-byte key that is created by this command.

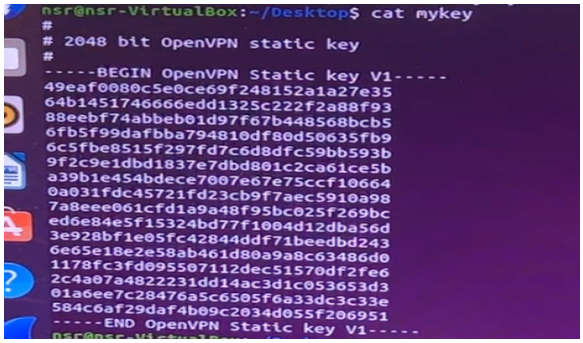

Fig. 2. 256-byte key in a file called mykey.

Following this, we had to transfer the key we generated on Ubuntu1 to Ubuntu2, the other computer. To do this, we employ Secure Copy Protocol, or SCP. I created an encrypted tunnel between the two computers as soon as I was able to successfully share the secret key between them.

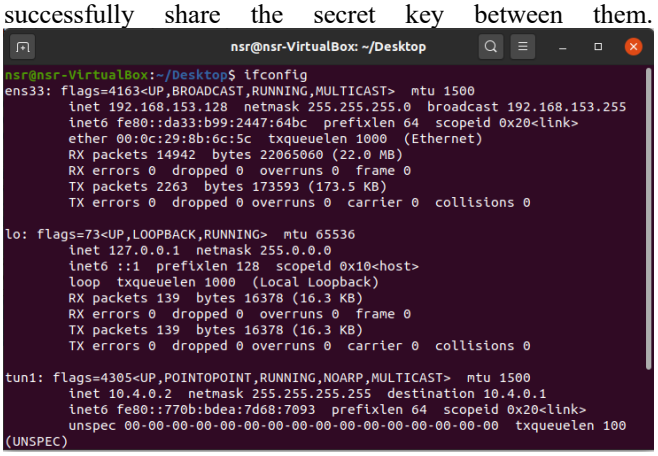

Fig. 3. Encrypted tunnel on Ubuntu2.

As we can see, the encrypted tunnel is now accessible through a new interface named "tun1." I was successful in using OpenVPN to create a tunnel from Ubuntu1 to Ubuntu2 by following the instructions on the lab. It resembles building a private road with all traffic passing through it between the two computers. It is encoded with a unique key that is kept in the "mykey" file.

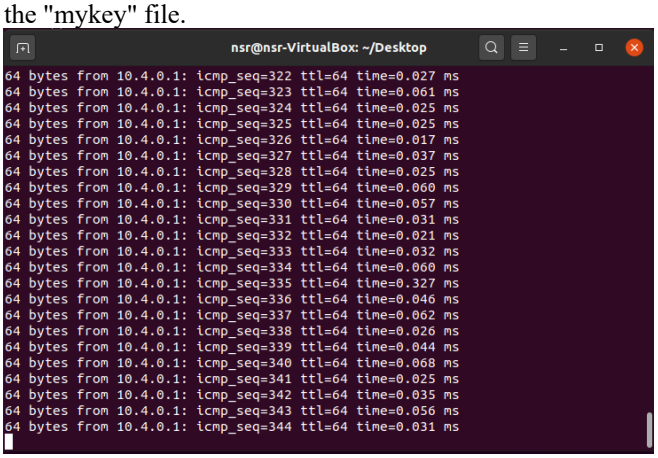

Fig. 4: Ubuntu2 pinging Ubuntu1.

Questions on section 6:

In response to the first query in this section, when accessing packets on tun1, the traffic is encrypted. The protocol, length, source, and destination were altered. OpenVPN uses the key given in the "—secret" parameter to enforce this encryption. Because of this, any attempt to intercept data via the tunnel would be unsuccessful without the decryption key.

The traffic travelling through the tunnel doesn't appear to be encrypted when Wireshark is used to monitor the traffic from the Ethernet interface on Ubuntu 2. Rather, I observed ICMP ping packets in plaintext moving between Ubuntu2 and the tunnel's destination address. This occurs as a result of Wireshark intercepting network traffic before the VPN tunnel encrypts it. Consequently, the original, unencrypted data packets that were captured from the Ethernet interface.

Wireshark shows encrypted traffic when monitoring the tun1 interface. This is a result of the tun1 interface being connected to the VPN tunnel, where OpenVPN encrypts all data travelling through it with the designated encryption key. As a result, before being sent over the network, any commands carried out or data transferred through the tun1 interface will be encrypted.

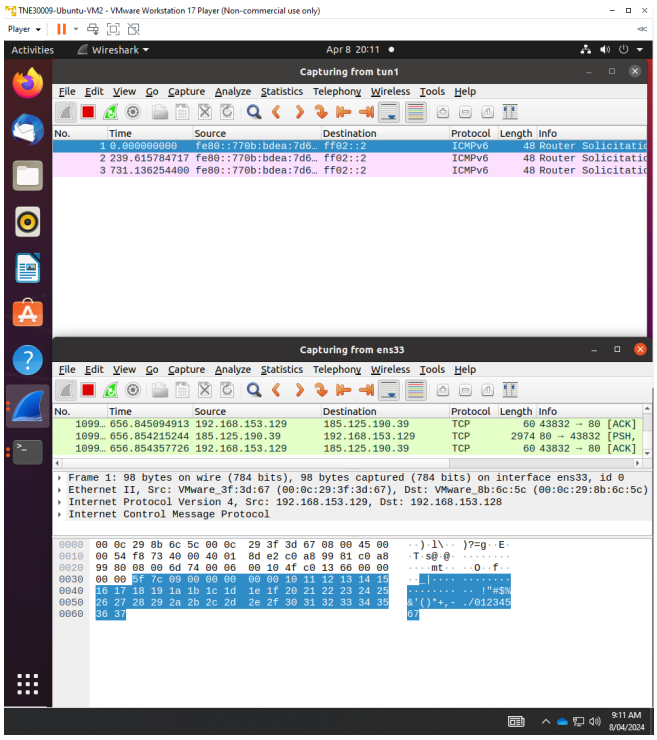

Fig. 5. Using Wireshark to capture traffic from tun1.

However, the traffic is not encrypted when it comes to monitoring the Ethernet interface. This is due to the fact that traffic is captured by the Ethernet interface prior to it entering the VPN tunnel, preserving the original, unencrypted data. Consequently, Wireshark will be able to view all commands that are executed and data that is transmitted through the Ethernet interface in plaintext.

In conclusion, traffic going through the Ethernet interface is not encrypted because it is intercepted before it enters the VPN tunnel, whereas traffic going through the tun1 interface is encrypted because it travels through the VPN tunnel.

What is a VPN tunnel? An encrypted connection between a VPN server and your devices—such as PCs, tablets, or smartphones—is known as a VPN tunnel. It encrypts the data you create while browsing the web and conceals your IP address while sending data over the internet. Because the connection cannot be broken without a cryptographic key, in this case (mykey), snoopers cannot access your online information or follow your activities.[4]

III. Conclusion

In conclusion, this report has shown the practical implementation of Virtual Private Networks (VPN) using OpenVPN on Ubuntu computers. VPNs serve as crucial components of modern network security strategies, offering organizations a versatile toolset to enforce security policies, safeguard sensitive data, and facilitate secure communication over public networks. By leveraging encryption, authentication mechanisms, and tunnelling protocols, VPNs ensure the confidentiality,

integrity, and privacy of transmitted data. By embracing VPN technology, people can effectively protect their assets, secure their data, access, and or stream regional content [5].

REFERENCES

[1] Kaspersky, "What Is a VPN and How Does It work?," Kaspersky, Nov. 03, 2020. Available: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

[2] PaloAlto, "What Is a VPN? - Palo Alto Networks," www.paloaltonetworks.com. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn.

[3] Cisco, "VPN and Endpoint Security Clients," Cisco, Nov. 2019. Available: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/index.html

[4] NordVPN, "What is a VPN tunnel and how does it work? | NordVPN," nordvpn.com, Mar. 26, 2021. Available: https://nordvpn.com/blog/vpn-tunnel/

[5] "What is a VPN? Why Should I Use a VPN? | Microsoft Azure," azure.microsoft.com. Available: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn#:~:text=A%20VPN%20protects%20its%20users.