Lucas Lorenzo Jakin

Lab 2: Virtual Private Networks

Reti di Calcolatori II – Università di Trieste – Martino Trevisan

In this lab, you will use a Virtual Private Network, and you will dig into its operation. Moreover, using Wireshark and Linux tools, you will understand how it interacts with the configuration of your PC and how the resulting network traffic look like. To complete the assignment, fill the answer in the provided space. Be clear and concise and, if needed, enlarge the boxes dedicated to the answer.

You can use any Unix-like system, but we recommend Ubuntu Desktop or any other Linux distribution. MacOS is fine, Windows is not. If you have MacOS or Windows, we recommend creating an Ubuntu Virtual Machine or set up a Dual Boot.

VPN configuration

You have to set up a VPN using L2TP and IPSec. Configuration parameters are:

- **Gateway**: sonda2.polito.it
- **Username**: studente
- **Password**: IeZae0ti
- **IPSec Pre-Shared Key**: retidicalcolatori

If you are using Ubuntu, access the Network Manager by clicking on the  icon in the top bar. Then, click on “Edit Connection” and create a new VPN. Now, enter the configuration parameters.

Once the VPN connection is configured, enable it by using the Network Manager.

IP addresses

Which is the IP address of your network adapter(s)? When using the VPN, do you see any additional network interface? Does it have an IP address?

Check your public IP address before and after enabling the VPN using e.g., *https://whatismyipaddress.com/*. Does it change? **Note**: you can also check your public IP issuing the Bash command: `curl ifconfig.me`

Look at the routing table of your machine (using e.g., the `ip route` command): how they are modified once you start the VPN?

The public IP address of my network adapter is 37.162.35.9 (private) before enabling the VPN connection. Once the VPN is enabled and working the public IP addresses changes into 130.192.9.241

I used the command “ip route” for looking on the IP addresses that are active. Before enabling the VPN, my machine was having an interface named “enp0s3” and all the traffic was going through it. After the VPN was enabled, the machine had 2 interfaces, one was the same as before “enp0s3”, and another one called “ppp0” which is the virtual address of the VPN where its virtual IP address is 192.168.42.1.

Authentication phase and data packets

Using Wireshark, describe the authentication phase. Is it encrypted? Are username and password in clear?

Consider a normal data packet: which protocol headers do you find? Is the payload encrypted?

What happens if you use Wireshark on the virtual interface? How the traffic looks like? Is it encrypted? Which headers do protocols include?

After establishing a VPN connection Wireshark detected several packets using the ISAKMP protocol, which is a protocol used for establishing and managing security associations. It works in conjunction with IKE to securely exchange the keys. Using Wireshark I detected that 6 (3 pairs) initial ISAKMP packets were sent where each pair represented a Request and a Response. The first two pairs of packets have the payloads “Security Association” and “Key Exchange” and are not encrypted, so their content is visible. They are needed for choosing the cryptographic algorithms to be used and then for exchanging keys and nonces. The last pair of packets have the purpose of confirming the authenticity of the connection and it is ENCRYPTED.

In a normal data packet I found a UDP header and the payload of the packet was encrypted with ESP protocol.

The traffic captured on the virtual interface ppp0 is not encrypted. The transmission uses the ICMP protocol and when pinging to some host I saw all the ICMP requests and responses. Headers use protocols ICMP and IPv4

Webpage visit

Visit a webpage (e.g., www.repubblica.it) and analyse the traffic your machine generates on the physical interface with Wireshark. Is there any way to guess the visited website only by looking at the network packets?

Access the website with and without the VPN. Do you contact the same server IP address when visiting the webpage? Is the page load time approximately the same?

When the VPN connection is established and we are looking at the traffic on the physical interface, all the packets that are sent are being encapsulated in a tunnel and the payloads are not visible, because of encryption. In the case of active VPN, the packets show the IP address of the VPN server, keeping the IP address of the website hidden. With a VPN, the page loading time takes a little bit more than without having a VPN, because of the overhead of the encryption.

When not using VPN, it is possible to identify the visited website. It can be done by using The DNS protocol to detect the domain of the website.

Play with the routing tables (Optional)

Modify the routing tables of your machine to route through the VPN only the traffic to whatismyipaddress.com. Check it works by comparing the webpage you get when visiting it and when visiting www.mio-ip.it. On Linux, use the `ip route` command. Alternatively, check the ***Routes*** option on the VPN configuration panel.

Set up your own VPN Server (Optional)

In the Lab directory, you find the scripts to set up your own VPN server. The scripts starts a docker container (hwdsl2/ipsec-vpn-server) which implements an IPSec VPN server. Use another PC (or a VM) to establish a VPN with the server.

- Look at the traffic to the VPN server
- Look at the logs of the VPN server (when it starts, when someone connects and disconnects)
- Start a shell in the container:
    - Look at the processes running and their configuration files
    - Where the subnet used for virtual addresses is specified?
    - Where the subnet(s) that the client must route through the VPN are specified?