

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:** leZae0ti. [la prima lettera è una i maiuscola]
- **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.

Note for Windows users: consider applying the fix described [here](#).

General note: on [this repo](#) you can find many problems in connecting to the VPN server we are using

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?

Before activating the VPN, the public IP address is 140.105.162.88. After connecting to the VPN using nmcli connection up id "VPN 1", the public IP address changes to 130.192.9.241, indicating that all traffic is now routed through the VPN server.

The new ppp0 interface is assigned a private IP address of 192.168.42.10, which is provided by the VPN server. The peer IP is 192.168.42.1, which is the gateway address of the VPN server.

Now, all traffic is routed through the ppp0 interface, directing it towards the VPN gateway. The public IP visible on the internet changes because the traffic is routed through the VPN server, masking the original public IP.

After activating the VPN, a new default route through ppp0 is added with a metric of 50, indicating a higher priority than the previous default gateway through enp0s3.

Finally, the VPN adds a specific route to the remote network via the VPN gateway at 192.168.42.1, which is necessary for routing encrypted traffic through the VPN server.

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?

I observed two packets sent with the ISAKMP protocol that are not encrypted and one that is encrypted, corresponding to the Main Mode stages: Security Association, Key Exchange, and Identification. In the Security Association packet, the encryption algorithm is chosen; in the Key Exchange packet, the secret key is exchanged; and in the Identification packet, the user is authenticated over an encrypted payload. This ensures that credentials, such as the username and password, remain protected.

After Main Mode, ISAKMP packets in Quick Mode are exchanged to configure the rules and secure the actual VPN traffic.

When performing a ping with the VPN active, I observe packets on the physical interface enp0s3 that are not encrypted, as ICMP traffic (used for the ping) remains visible. For normal data traffic, we find UDP headers with the payload encrypted using the ESP protocol.

Additionally, the traffic captured on the ppp0 virtual interface is not encrypted and uses ICMP with both IPv4 and ICMP headers.

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?

Yes, it is possible to identify a visited website by analyzing network packets, even if the traffic is encrypted (HTTPS). Without a VPN, you can use a DNS protocol filter in Wireshark to detect the domain of the site being visited. By searching for A or AAAA records, which resolve the domain name to an IP address, you can see the requested domain in the DNS packets, provided the traffic is not encrypted. When the traffic is HTTPS (port 443), the content is encrypted, but you can still see the destination server's IP address in the IP header.

However, when using a VPN, all traffic from your machine to the internet is encrypted and encapsulated in a tunnel. In this case, the captured packets will only show the IP address of the VPN server, not the website you are visiting. You won't be able to directly identify the requested site unless you have access to the VPN server itself. Moreover, with a VPN, the page-loading process may be slightly slower due to the overhead of encryption.

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 ([hwds12/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?