

B5: VPN

Motivation

The government is spying on your internet use. Hackers are spying on you. Use VPN to protect yourself. Service providers are blocking overseas customers. Use VPN to bypass this.

You may have heard statements like the ones above from tech news, your favourite streamer or podcaster and VPN advertisements. VPNs can be used as proxies to hide the origin of web traffic by routing traffic through a VPN server in another location. They can also be used to hide your traffic from prying eyes by encrypting the traffic between your computer and the VPN server and burying the traffic into the massive flood of traffic going to and from the VPN server on the other end of the tunnel.

In this assignment, however, you will create a VPN bridge, that allows you to access a LAN network from the outside, as if the computer was a part of that network. You will provide an IP address from said network for the computer. This method can be used for accessing e.g. a corporate network over the internet.

Description of the exercise

This assignment introduces you to the Virtual Private Network (VPN) concept. You will use OpenVPN and all three VMs to establish a VPN in practice by creating and examining a host-to-net VPN scenario. A roadwarrior host (lab3, RW) establishes a secure tunnel to a gateway (lab1, GW). Traffic can flow from the roadwarrior through the gateway to a Storage server (lab2, SS) and back. Hosts on the right-side local link can not eavesdrop or modify the traffic flowing inside the tunnel. Here's what the resulting network will look like.



The goal of this assignment is to test communication between the Storage Server and the Road Warrior by successfully pinging and tracerouting each other in both directions. OpenVPN will be used in bridging mode to connect the RW to the local network of SS and GW.

Additional reading

- [OpenVPN HOWTO](#)

- [How to Create Keys](#)

1. Initial Setup

Install *openvpn* package for GW and RW if it has not been preinstalled. Install also *bridge-utils* for GW.

On lab1 (GW):

- Assign a static IP from the subnet 192.168.0.0/24 to the interface enp0s8
- Assign a static IP from the subnet 192.168.2.0/24 to the interface enp0s9

On lab2 (SS):

- Assign a static IP from the subnet 192.168.0.0/24 to the interface enp0s8

On lab3 (RW):

- Assign a static IP from the subnet 192.168.2.0/24 to the interface enp0s8

In this exercise, the enp0s3 interfaces are only used for SSH remote access. Do not use them for any other traffic. Verify that you can ping the gateway from the other hosts, and that you can not ping the RW from the SS or vice versa. Write down the network configuration.

- 1.1 Present your network configuration. What IPs did you assign to the interfaces (4 interfaces in all) of each of the three hosts? 1p

2. Setting up a PKI (Public Key Infrastructure)

The first step in establishing an OpenVPN connection is to build the public key infrastructure (PKI).

You'll need to generate the master Certificate Authority (CA) certificate/key, the server certificate/key and a key for at least one client. In addition you also have to generate the Diffie-Hellman parameters for the server. Note: the Ubuntu openvpn package no longer ships with easy-rsa.

After you have generated all the necessary certificates and keys, copy the necessary files (securely) to the road warrior (RW) host.

- 2.1 What is the purpose of each of the generated files? Which ones are needed by the client? 2p

- 2.2 Is there a simpler way of authentication available in OpenVPN? What are its benefits/drawbacks? 1p

3. Configuring the VPN server

On GW copy `/usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz` to for example `/etc/openvpn` and extract it. You have to edit the `server.conf` to use bridged mode with the correct virtual interface. You also have to check that the keys and certificates point to the correct files. Set the server to listen for connection in GW's `enp0s9` IP address.

Start the server on GW with `openvpn server.conf`.

- 3.1 List and give a short explanation of the commands you used in your server configuration. 2p
- 3.2 What IP address space did you allocate to the OpenVPN clients? 1p
- 3.3 Where can you find the log messages of the server by default? How can you change this? 1p

4. Bridging setup

Next you have to setup network bridging on the GW. We'll combine the `enp0s8` interface of the gateway with a virtual TAP interface and bridge them together under an umbrella bridge interface.

OpenVPN provides a script for this in `/usr/share/doc/openvpn/examples/sample-scripts`. Copy the `bridge-start` and the `bridge-stop` scripts to a different folder for editing. Edit the parameters of the script files to match with GW's `enp0s8`. Start the bridge and check with `ifconfig` that the bridging was successful.

- 4.1 Show with `ifconfig` that you have created the new interfaces (virtual and bridge). What's the IP of the bridge interface? 1p
- 4.2 What is the difference between routing and bridging in VPN? What are the benefits/disadvantages of the two? When would you use routing and when bridging? 3p

5. Configuring the VPN client and testing connection

On RW copy `/usr/share/doc/openvpn/examples/sample-config-files/client.conf` to for example `/etc/openvpn`. Edit the `client.conf` to match with the settings of the server. Remember to check that the certificates and keys point to the right folders.

Connect RW to the server on GW with openvpn `client.conf`. Pinging the SS from RW should now work.

If you have problems with the ping not going through, go to VirtualBox network adapter settings and allow promiscuous mode for internal networks that need it.

- | | | |
|-----|---|----|
| 5.1 | List and give a short explanation of the commands you used in your VPN client configuration. | 1p |
| 5.2 | Demonstrate that you can reach the SS from the RW. Setup a server on the client with netcat and connect to this with telnet/nc. Send messages to both directions. | 2p |
| 5.3 | Capture incoming/outgoing traffic on GW's <code>enp0s9</code> or RW's <code>enp0s8</code> . Why can't you read the messages sent in 5.2 (in plain text) even if you comment out the cipher command in the config-files? | 2p |
| 5.4 | Enable ciphering. Is there a way to capture and read the messages sent in 5.2 on GW despite the encryption? Where is the message encrypted and where is it not? | 1p |
| 5.5 | Traceroute RW from SS and vice versa. Explain the result. | 1p |

6. Setting up routed VPN

In this task, you have to set up routed VPN as opposed to the bridged VPN above. Stop openvpn service on both server and client.

1. Reconfigure the `server.conf` and the `client.conf` to have routed vpn.
2. Restart openvpn service on both server and client.
3. Now you should be able to ping virtual IP address of vpn server from client.

6.1	List and give a short explanation of the commands you used in your server configuration	2p
-----	---	----

6.2	Show with ifconfig that you have created the new virtual IP interfaces . What's the IP address?	1p
-----	---	----

7. Finishing your work

When finishing your work, please remember to backup files related to the assignment and after your demo possibly reset the configuration changes that you did to the lab environment (Lab1, Lab2, Lab3) to start the next assignment with a clean slate.