



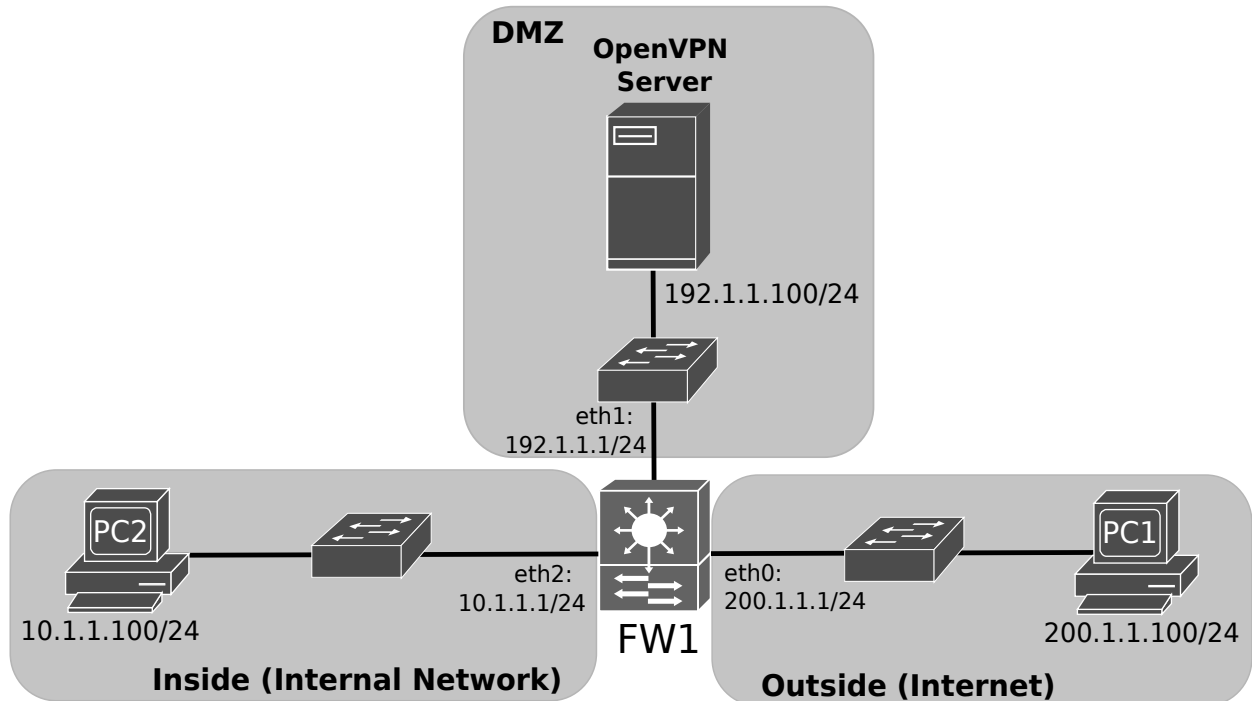
universidade de aveiro  
theoria poiesis praxis

# **SEGURANÇA EM REDES DE COMUNICAÇÕES**

**NETWORK REMOTE ACCESS**

**OPENVPN + FIREWALL**

## OpenVPN Remote Access Server



The firewall (FW1) should be implemented with a VyOS virtual machine, PC1 and Server should be a Linux virtual machine (Debian) and PC2 may be a VPCS.

With the OpenVPN server virtual machine connected to the Internet, install the openVPN server:

```
$ sudo apt install openvpn
```

Download the server configuration (server.conf) file from elearning.

With the client (PC1) connected to the Internet, install the network package with the openVPN client interface:

```
$ sudo apt install network-manager-openvpn-gnome
```

1. Assemble the above network and configure IPv4 addresses and gateways. To configure the firewall addresses (for now without zones or flow control rules):

```
# set system host-name FW1
# set interfaces ethernet eth0 address 200.1.1.1/24
# set interfaces ethernet eth1 address 192.1.1.1/24
# set interfaces ethernet eth2 address 10.1.1.1/24
# set protocols static route 10.8.0.0/24 next-hop 192.1.1.100
# commit
# save
```

2. Connect the OpenVPN server to the GNS3 network, configure address and gateway, and test connectivity.

Using easyRSA create the server and client keys/certificates:

```
$ sudo su
$ cd /etc/openvpn
$ cp -r /usr/share/easy-rsa .
$ cd easy-rsa
$ ./easyrsa init-pki
$ ./easyrsa build-ca
$ ./easyrsa build-server-full server
$ ./easyrsa build-client-full client1
$ ./easyrsa gen-dh
$ cd ../server
$ cp ../easy-rsa/pki/ca.crt .
$ cp ../easy-rsa/pki/dh.pem .
$ cp ../easy-rsa/pki/issued/server.crt .
$ cp ../easy-rsa/pki/private/server.key .

$ cp ../easy-rsa/pki/issued/client1.crt /home/labcom/
$ cp ../easy-rsa/pki/private/client1.key /home/labcom/
$ cp ../easy-rsa/pki/ca.crt /home/labcom/
$ chown labcom:labcom /home/labcom/*
```

Active the openVPN IPv4 routing by uncommentating the line "net.ipv4.ip\_forward = 1" in the file /etc/sysctl.conf. Run the following command to implement changes:

```
$ sudo sysctl -p
```

Create/use the OpenVPN server configuration file (server.conf in directory /etc/openvpn) with the following contents:

```
port 1194
proto udp
dev tun
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/server.crt
key /etc/openvpn/server/server.key
dh /etc/openvpn/server/dh.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1 bypass-dhcp"
keepalive 10 120
comp-lzo
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Activate the openVPN server with the command:

```
$ openvpn /etc/openvpn/server.conf
```

>> Analyze the server output to verify the correct stratup.

3. Download (using SSH) the openVPN CA and client certificates and client private key:

```
$ scp labcom@192.1.1.100:~/ca.crt ~/Downloads
```

```
$ scp labcom@192.1.1.100:~/client1.crt ~/Downloads
```

```
$ scp labcom@192.1.1.100:~/client1.key ~/Downloads
```

Using the network manager, create a new VPN connection to the openVPN server with the downloaded credentials files. Start packet captures in all three zones. Activate the VPN.

>> Test connectivity between the external client and the internal PC. Analyze the captured packets.

>> Analyze the virtual network interfaces that have been created.

4. At the firewall, create the necessary zones and flow control rules:

- To allow only access to the openVPN (UDP port 1194) server at the DMZ;

- Allow connect remote users (in network 10.8.0.0/24) to access the internal network.

>> Test connectivity between the external client and the internal PC and DMZ server.