

# Practical Exercises #6

## Resolution examples

---

---

## Goals

Install OpenVPN in Linux (VPN client and server)

Configure OpenVPN authentication

---

## OpenVPN installation in Linux

1. Install OpenVPN in Linux (available at <https://openvpn.net>)

```
yum install epel-release  
yum install openvpn
```

2. Configure OpenVPN as a Linux service and to start at system boot

After installation, the openvpn service can already be controlled via systemctl:

```
systemctl <start/restart/stop> openvpn
```

Please note: during configuration it is preferable to start directly using the command line:

```
openvpn --config <config_file>
```

## Materials

- Gestão de Sistemas e Redes em Linux, Jorge Granjal, FCA 2010/2013, “Capítulo 21. Acessos seguros com VPN”
- [OpenVPN HOWTO](#)
- [Wireshark](#)

## OpenVPN authentication (passwords)

For the following exercises, refer to example config files available in:  
`/usr/share/doc/openvpn/samples/sample-config-files`

```
cp server.conf /etc/openvpn/server.conf
```

```
cp cliente.conf /etc/openvpn/client.conf
```

```
openvpn --config <config_file>
```

3. Configure the OpenVPN server to accept connections from clients identified by a username and password (client certificate not required)
4. Configure a client to authenticate to the OpenVPN server with username and password. Try to connect to the server (establish a VPN tunnel)
5. Test the encryption on the VPN tunnel using Wireshark (listen on interfaces *tun0* and *Ethernet*)

When using Wireshark, communications on the “tun0” (or “tun1”) interface are not encrypted), while on the ethernet interface the same packets appear encrypted by the VPN tunnel.

## OpenVPN authentication (X.509 certificates)

6. Configure the OpenVPN server to accept connections from clients identified by a X.509 certificate
7. Configure a client to authenticate with a X.509 certificate
8. Test again the encryption on the VPN tunnel using Wireshark (listen on interfaces *tun0* and *Ethernet*)