1. Instalação da OpenVpn
   Para a intalação da OpenVpn no nosso servidor de grupo:
   a. sudo apt-get update && sudo apt-get install openvpn
   b. sudo apt install easy-rsa
   c. openvpn –version

```
kevin@sp33: $ openvpn --version
OpenVPN 2.5.9 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Sep 29 2023
library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
Originally developed by James Yonan
Copyright (C) 2002-2022 OpenVPN Inc <sales@openvpn.net>
```

   Criamos de seguido o diretorio easy-rsa e realizamos os links simbólicas, para que futuras atualizações possam ser replicadas nas nossas configurações.
   - mkdir ~/easy-rsa
   - ln -s /usr/share/easy-rsa/* ~/easy-rsa/

2. Configuração da OpenVpn para começar no arranque da máquina
   a. sudo systemctl enable openvpn-server@server.service
3. Configuração OpenVpn (passos seguidos)
   a. Inicializamos Pki no diretorio easy-rsa (para ser possível criar um CA mais a frente)
      i. ./easyrsa init-pki
   b. Criamos a autoridade de certitificados CA (no diretorio easy-rsa)
      i. ./easyrsa build-ca nopass (criando um ficheiro com novo certificado CA ca.crt)
      ii. ls ~/easy-rsa/pki (para verificar se foi criado corretamente ca.crt)

```
kevin@sp33:~$ ls ~/easy-rsa/pki
ca.crt           index.txt          index.txt.old       private  revoked              serial.old
certs_by_serial  index.txt.attr     issued              renewed  safessl-easyrsa.cnf
dh.pem           index.txt.attr.old openssl-easyrsa.cnf reqs     serial
```

      iii. ls ~/easy-rsa/pki/private (para verificar a chave privada da CA que criamos)

```
kevin@sp33:~$ ls ~/easy-rsa/pki/private
Alice.key  Alice.pem  ca.key  vpn_server.key  vpn_server.pem
```

   c. Criamos a chave do servidor OpenVpn
      i. cd ~/easy-rsa/ && ./easyrsa build-server-full vpn_server nopas
      ii. ls ~/easy-rsa/pki/private/ (para verificar a chave do cervidor , vpn_server.key)

```
kevin@sp33:~$ ls ~/easy-rsa/pki/private/
Alice.key  Alice.pem  ca.key  vpn_server.key  vpn_server.pem
```

      iii. ls ~/easy-rsa/pki/issued (para verificar o certificado criado para o servidor vpn)

```
kevin@sp33:~$ ls ~/easy-rsa/pki/issued
Alice.crt  vpn_server.crt
```

   d. Assinamos o certificado do servidor OpenVpn
      i. cd ~/easy-rsa/ && ./easyrsa sign-req server vpn_server

e. Geramos o parâmetro Diffie hellman
    i. cd ~/easy-rsa/ && ./easyrsa gen-dh
f. Criamos o TLS Crypt v2 para OpnVpn (permiti o fornecimento de uma chave tls-crypt especifica para cada cliente)
    i. cd ~/easy-rsa/pki/ && sudo openvpn --genkey tls-crypt-v2-server private/vpn_server.pem
g. Configuração do servidor
    i. cd /etc/openvpn/server && sudo nano server.conf (colocando a configuração pres

```
#--------------------
#VPN port
port 1194

#VPN over UDP
proto udp

# "dev tun" will create a routed IP tunnel
dev tun

ca ca.crt
cert vpn_server.crt
key vpn_server.key
tls-crypt-v2 vpn_server.pem
dh dh.pem

#network for the VPN
server 10.8.0.0 255.255.255.0

push "redirect-gateway autolocal"

# Maintain a record of client <-> virtual IP address

# associations in this file.
ifconfig-pool-persist /var/log/openvpn/ipp.txt

# Ping every 10 seconds and assume client is down if
# it receives no response in 120 seconds.
keepalive 10 120

#cryptographic cipher
cipher AES-256-GCM

#avoid accessing certain resources on restart
persist-key
persist-tun

#log of current connections
status /var/log/openvpn/openvpn-status.log

#log verbose level (0-9)
verb 4

# Notify the client when the server restarts
explicit-exit-notify 1
#----------------------------------------
```

ente na *figura 1)*

Figura 1 - Configuração do ficheiro server.conf

h. Copiamos certificados e chaves do Servidor VPN para "/etc/openvpn/server" Executamos a seguinte sequência
    i. cd ~/easy-rsa/pki/
    ii. sudo cp ca.crt /etc/openvpn/server
    iii. cd ~/easy-rsa/pki/private/
    iv. sudo cp vpn_server.key /etc/openvpn/server/
    v. sudo cp vpn_server.pem /etc/openvpn/server/
    vi. cd ~/easy-rsa/pki/issued/
    vii. sudo cp vpn_server.crt /etc/openvpn/server/
i. Demos permissões de encaminhamento
    i. sudo nano /etc/sysctl.conf (adicionado a linha net.ipv4.ip_forward = 1)
    ii. sudo sysctl -p (recarregar o arquivo)
j. Abrir a porta 1194 para dar acesso ao Servido OpenVpn
    i. sudo ufw allow 1194/udp
    ii. sudo ufw disable && sudo ufw enable (para reiniciar a firewall)
k. Inicialização do Servidor OpenVpn
    i. sudo systemctl start openvpn-server@server.service
    ii. sudo systemctl status openvpn-server@server.service (verificar o estado do servidor , no caso esta Running)

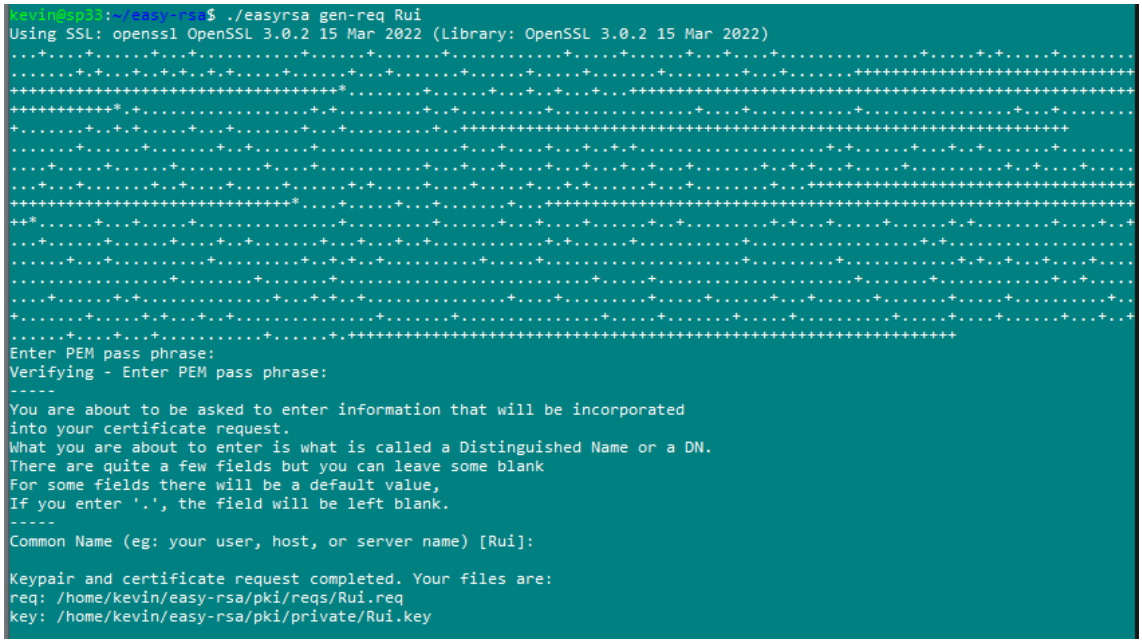
```
kevin@sp33:/etc/openvpn/server$ sudo systemctl status openvpn-server@server.service
● openvpn-server@server.service - OpenVPN service for server
     Loaded: loaded (/lib/systemd/system/openvpn-server@.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2024-04-12 14:37:15 UTC; 3h 27min ago
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 688 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 2220)
     Memory: 3.2M
        CPU: 272ms
     CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service
             └─688 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-version 2 --suppress-times>

Apr 12 14:37:15 sp33 openvpn[688]: Socket Buffers: R=[212992->212992] S=[212992->212992]
Apr 12 14:37:15 sp33 openvpn[688]: UDPv4 link local (bound): [AF_INET][undef]:1194
Apr 12 14:37:15 sp33 openvpn[688]: UDPv4 link remote: [AF_UNSPEC]
Apr 12 14:37:15 sp33 openvpn[688]: MULTI: multi_init called, r=256 v=256
Apr 12 14:37:15 sp33 openvpn[688]: IFCONFIG POOL IPv4: base=10.8.0.4 size=62
Apr 12 14:37:15 sp33 openvpn[688]: ifconfig_pool_read(), in='Alice,10.8.0.4,'
Apr 12 14:37:15 sp33 openvpn[688]: succeeded -> ifconfig_pool_set(hand=0)
Apr 12 14:37:15 sp33 openvpn[688]: IFCONFIG POOL LIST
Apr 12 14:37:15 sp33 openvpn[688]: Alice,10.8.0.4,
Apr 12 14:37:15 sp33 openvpn[688]: Initialization Sequence Completed
```

    iii. sudo systemctl enable openvpn-server@server.service (para garantir que a OpenVpn inicializa no momento em que a maquina faz boot)

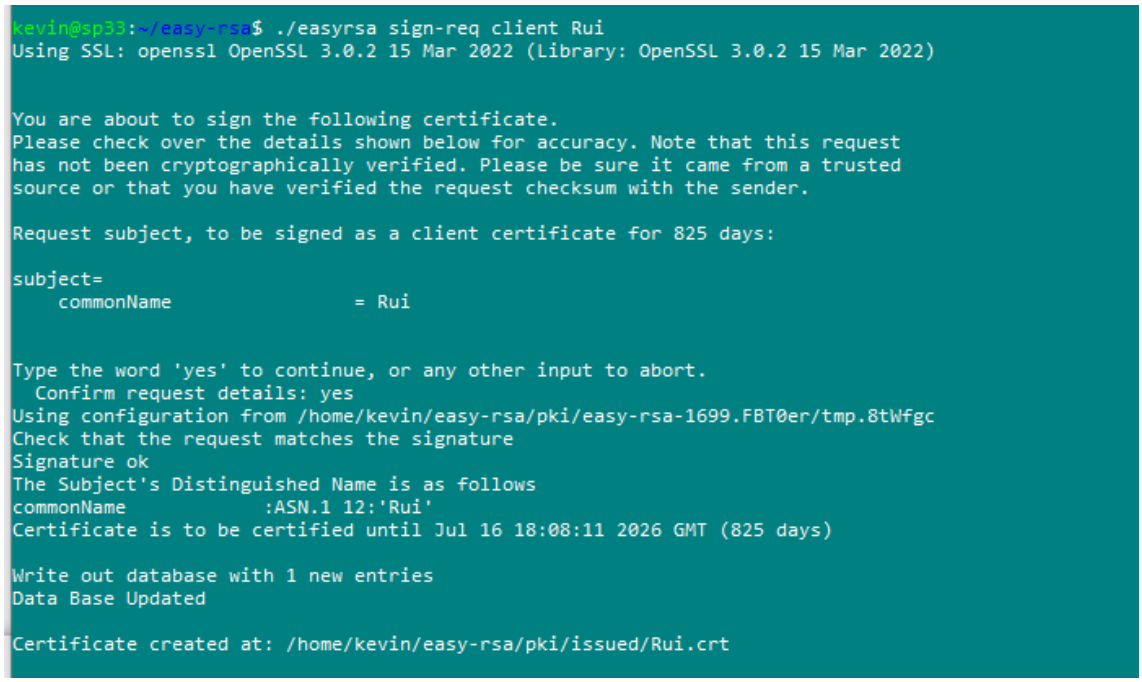
4. Configuração do cliente com username e password
    a. Criação de utilizador com username e password
        i. cd ~/easy-rsa/

ii. ./easyrsa gen-req Rui



b. Assinatura do certificado do Cliente

i. ./easyrsa sign-req client Rui



c. Criar a chave TLS Crypt v2 para o cliente

i. cd ~/easy-rsa/pki/

ii. openvpn --tls-crypt-v2 private/vpn_server.pem --genkey tls-crypt-v2-client private/Rui.pem

iii. ls ~/easy-rsa/pki/private/ (verificar que a chave foi criada)

```
kevin@sp33:~/easy-rsa/pki$ ls ~/easy-rsa/pki/private/
Alice.key  Alice.pem  ca.key  Rui.key  Rui.pem  vpn_server.key  vpn_server.pem
```

d. Preparação dos arquivos dos clientes
   i. mkdir ~/vpn_clients (diretorio que vai conter subdiretórios que correspondem clientes)
   ii. cd ~/vpn_clients && mkdir rui
   iii. Copiar ca.crt e outros arquivos do cliente criado para o respetivo diretório
   iv. cd ~/easy-rsa/pki/
   v. cp ca.crt ~/vpn_clients/rui
   vi. cd ~/easy-rsa/pki/issued/
   vii. cp Rui.crt ~/vpn_clients/rui
   viii. cd ~/easy-rsa/pki/private/
   ix. cp Rui.key ~/vpn_clients/rui
   x. cp Rui.pem ~/vpn_clients/rui
   xi. ls ~/vpn_clients/rui (para verificar as respetivas chaves e certificados foram devidamente copiados)

```
kevin@sp33:~/easy-rsa/pki/private$ ls ~/vpn_clients/rui
ca.crt  Rui.crt  Rui.key  Rui.pem
```

e. Criação do ficheiro OVPN
   Para realizar a criação deste ficheiro realizamos um script (demonstrado na figura 2)

```
#!/bin/bash

# 1 argument = Client_identifier
cat <(echo -e 'client') \
<(echo -e 'proto udp') \
<(echo -e 'dev tun') \
<(echo -e 'remote 127.0.0.1 1194') \
<(echo -e 'resolv-retry infinite') \
<(echo -e 'nobind') \
<(echo -e 'persist-key') \
<(echo -e 'persist-tun') \
<(echo -e 'remote-cert-tls server') \
<(echo -e 'cipher AES-256-GCM') \
<(echo -e '#user nobody') \
<(echo -e '#group nobody') \
<(echo -e 'verb 3') \
    <(echo -e '<ca>') \
    ca.crt \
    <(echo -e '</ca>\n<cert>') \
    ${1}.crt \
    <(echo -e '</cert>\n<key>') \
    ${1}.key \
    <(echo -e '</key>\n<tls-crypt-v2>') \
    ${1}.pem \
    <(echo -e '</tls-crypt-v2>') \
    > ${1}.ovpn
```

Figura 2 - script para criar ficheiro .ovpn

i. Mudamos o remote para o ip publico associado ao nosso servidor, no caso é 193.136.39.100 (descobri este ip com o comando "dig +short myip.opendns.com @resolver1.opendns.com")

f. No lado do cliente , instalei o openVPNGUI, numa maquina com windows, e juntamente com o ficheiro .ovpn, que criei no servidor, tentei realizar uma conexão. Contundo não tive sucesso, apresentando o seguinte erro :

TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity).

Tentei corrigir este erro, tendo em conta a documentação oficial e fórum da comunidade, contudo não tive sucesso.

```
rui@DESKTOP-NQ1I6QH:/mnt/c/Users/Jessica/Desktop/Segurança e privacidade/Projetos/Seguran-a-trabalho-2$ openvpn Rui.ovpn
2024-04-12 19:18:02 OpenVPN 2.5.9 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Sep 29 2023
2024-04-12 19:18:02 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
Enter Private Key Password:
2024-04-12 19:18:09 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2024-04-12 19:18:09 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
2024-04-12 19:18:09 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-04-12 19:18:09 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
2024-04-12 19:18:09 Incoming Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-04-12 19:18:09 TCP/UDP: Preserving recently used remote address: [AF_INET]193.136.39.100:1194
2024-04-12 19:18:09 Socket Buffers: R=[163840->163840] S=[163840->163840]
2024-04-12 19:18:09 UDP link local: (not bound)
2024-04-12 19:18:09 UDP link remote: [AF_INET]193.136.39.100:1194
2024-04-12 19:19:09 TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
2024-04-12 19:19:09 TLS Error: TLS handshake failed
2024-04-12 19:19:09 SIGUSR1[soft,tls-error] received, process restarting
2024-04-12 19:19:09 Restart pause, 5 second(s)
2024-04-12 19:19:14 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
2024-04-12 19:19:14 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-04-12 19:19:14 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
2024-04-12 19:19:14 Incoming Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-04-12 19:19:14 TCP/UDP: Preserving recently used remote address: [AF_INET]193.136.39.100:1194
2024-04-12 19:19:14 Socket Buffers: R=[163840->163840] S=[163840->163840]
2024-04-12 19:19:14 UDP link local: (not bound)
2024-04-12 19:19:14 UDP link remote: [AF_INET]193.136.39.100:1194
```