

**KELVIN SEVERINO**

**ABNER CARLUCCI**

***TRABALHO 1***

***OPENVPN SERVIDOR E CLIENTE***

**TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**

**4º ADS**

**DISCIPLINA:** Redes de Computadores

*Prof. Me. Jean*

**São José dos Campos – SP**

**2018**

O Conteúdo abaixo é referente ao trabalho 1 – VPN da matéria de Redes de Computadores.

Para a realizar deste trabalho, foi necessário a utilização de 2 máquinas virtuais (VM):

1 – VPN Server

2 – VPN Cliente

**Configuração Inicial no Servidor OpenVPN**

**#apt-get install openvpn**

**#apt-get install easy-rsa**

**#apt-get install gzip**

Copiar diretório **easy-rsa** para **/etc/openvpn/**

**# cp -r /usr/share/easy-rsa/ /etc/openvpn/**

Dentro do diretório do easy-rsa, abrir o arquivo vars e inserir as seguintes informações

**# nano vars**

Obs. Note que você deverá inserir as seguintes informações de acordo com a sua necessidade

**#########################################################**

**# export KEY\_COUNTRY=”BR” #**

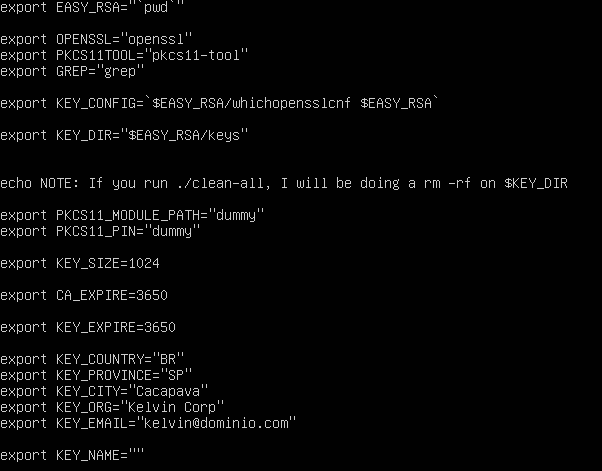
**# export KEY\_PROVINCE=”SP” #**

**# export KEY\_CITY=”Cacapava” #**

**# export KEY\_ORG=”Kelvin Corp” #**

**# export KEY\_EMAIL=”kelvin@dominio.com.br” #**

**#########################################################**



Criar o diretório keys no easy-rsa e inserir os sequintes arquivos

**# mkdir /etc/openvpn/easy-rsa/keys**

**# echo 01 > /etc/openvpn/easy-rsa/keys/serial**

**# touch /etc/openvpn/easy-rsa/keys/index.txt**

Retornar para o diretório easy-rsa

**# cd /etc/openvpn/easy-rsa/**

Rodar o comando source sobre o arquivo vars

**# source vars**

**OBS. Caso seja apresentado o erro** **“No /etc/openvpn/easy-rsa/openssl.cnf file could be found Further invocations will fail”.** É necessário ir em **/etc/openvpn/easy-rsa** para renomar o openssl, pois o mesmo não esta sendo encontrado.

**# cd /etc/openvpn/easyrsa/**

**# mv openssl-1.0.0.cnf /etc/openvpn/easyrsa/openssl.cnf**

Agora vamos criar a autoridade certificadora build-ca

**# ./build-ca**

Agora vamos criar o dh com build-dh

**# ./build-dh**

Após a criação do CA, criaremos a chave privada do Servidor com seguinte comando e depois do cliente

**# ./build-key-server servidor**

**# ./build-key cliente**

Note que a variável servidor na frente de ./build-key-server ja preencherá o Common Name (CN), isso acontecerá também na geração de chave do cliente

Agora devemos transferir as chaves a serem utilizadas na máquina cliente, sendo as chaves abaixo.

* **ca.crt**
* **cliente.crt**
* **cliente.key**
* **dh1024.pem**

**# scp ca.crt kelvin@192.168.10.114:/etc/openvpn/easy-rsa/keys**

**# scp cliente.crt kelvin@192.168.10.114:/etc/openvpn/easy-rsa/keys**

**#** **scp cliente.key kelvin@192.168.10.114:/etc/openvpn/easy-rsa/keys**

**# scp dh1024.pem kelvin@192.168.10.114:/etc/openvpn/easy-rsa/keys**

**Configuração do Servidor OpenVPN**

Devemos ir no diretório /etc/openvpn e criar o arquivo servidor.conf

cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/

tar -vzxf server.conf

cp server.conf /etc/openvpn/servidor.conf

# nano /etc/openvpn/servidor.conf

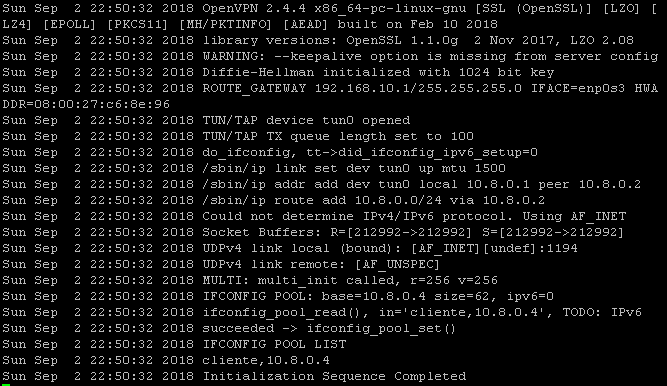


Após terminar de configurar o arquivo **servidor.conf**, vamos ativar o mesmo com o comando **openvpn --config servidor.conf**.

**Obs. Para que o comando funcione, devemos estar no diretório /etc/openvpn**

# openvpn --config servidor.conf

Se o serviço for iniciado com sucesso, você verá a imagem abaixo.



**Configuração da Máquina Cliente que acessa a VPN**

Devemos ir no diretório /etc/openvpn e criar o arquivo cliente.conf

# cd /etc/openvpn/

# > cliente.conf

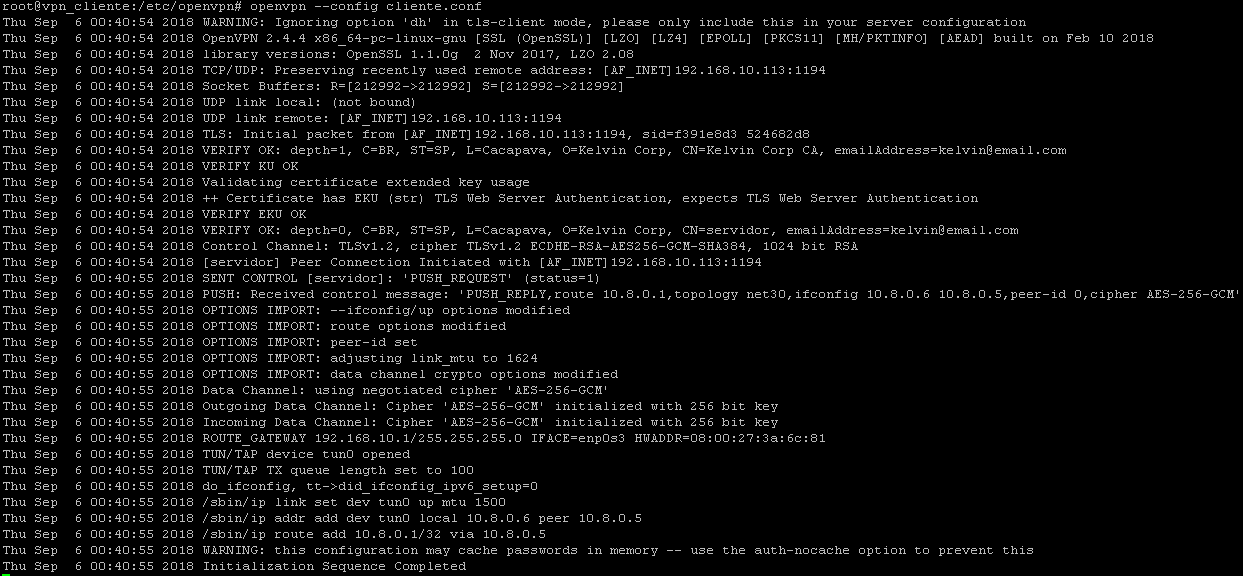


Após terminar de configurar o arquivo **cliente.conf**, vamos ativar o mesmo com o comando **openvpn --config cliente.conf**.

**Obs. Para que o comando funcione, devemos estar no diretório /etc/openvpn**

# openvpn --config cliente.conf

Se o serviço do cliente for iniciado com sucesso, você verá a imagem abaixo.

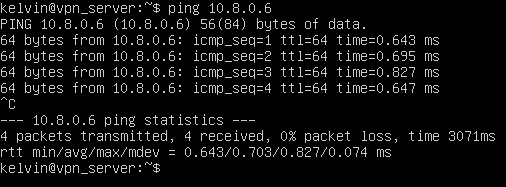


**Testes para Confirmação do Funcionamento da VPN**

Para confirmar se a foi criado um túnel da vpn entre o cliente e servidor.

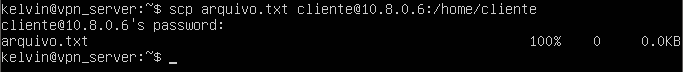
Vamos pingar utilizando o IP da VPN atribuído no cliente e servidor

**$ ping 10.8.0.6**



**Vamos enviar um arquivo via SSH para a máquina cliente utilizando o servidor.**

**# scp arquivo.txt cliente@10.8.0.6:/home/cliente**



Existem outros testes que podem ser feitos, como realizar o Ping de uma máquina fora do túnel da VPN, e esta máquina não pode conseguir pingar ou enviar qualquer dado para as máquinas que estejam no túnel da VPN por meio do IP da VPN.