

Redes de Computadores

Prof. Jean Carlos

Aluno

Rafael Augusto Campos Plinio

VPN

Introdução

Vivemos na era da informação, dados para todos os lados e a maioria das pessoas não tem noção alguma de como funciona a grande teia mundial, a internet. A internet está cada vez mais presente na vida das pessoas, podemos obter informações de qualquer tipo na internet, ou seja, se você pode obter informações diversas na internet, as outras pessoas também podem, assim como a disponibilização de dados ou informações dos mais variados tipos, os dados pessoais públicos e privados (de certa forma) também.

Uma possibilidade de evitar a proliferação de dados (públicos ou privados) podemos utilizar um formato de rede chamado Virtual Private Network (VPN) ou Rede Virtual Privada. Esta rede possibilita a criação de uma “mini-internet” para quem está a utilizá-la. Desta forma, apenas quem está nesta rede particular possui acesso aos dados que nela trafegam. Além do fato de ser mais segura para situações que necessitam de segurança, também vale destacar que o investimento necessário na criação de uma VPN é vantajoso, oferecendo um ótimo custo-benefício.

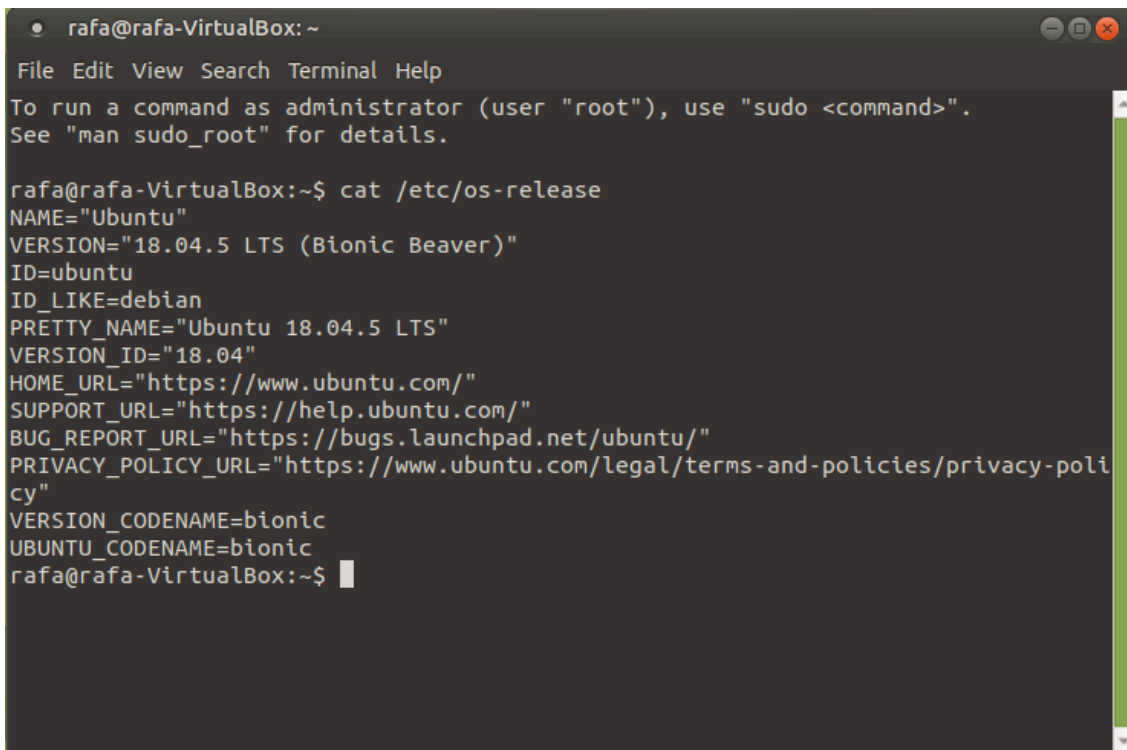
Instalação

VPN

Utilizaremos uma máquina virtual (VirtualBox) para criar 2 computadores com Linux (Ubuntu MATE, um será o host e o outro será o cliente), o OpenVPN e um LZO (é um compressor de dados, necessário para o OpenVPN).

Host – Ubuntu MATE

Distro e versão Linux: `cat /etc/os-release`



```
rafa@rafa-VirtualBox: ~  
File Edit View Search Terminal Help  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
rafa@rafa-VirtualBox:~$ cat /etc/os-release  
NAME="Ubuntu"  
VERSION="18.04.5 LTS (Bionic Beaver)"  
ID=ubuntu  
ID_LIKE=debian  
PRETTY_NAME="Ubuntu 18.04.5 LTS"  
VERSION_ID="18.04"  
HOME_URL="https://www.ubuntu.com/"  
SUPPORT_URL="https://help.ubuntu.com/"  
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"  
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"  
VERSION_CODENAME=bionic  
UBUNTU_CODENAME=bionic  
rafa@rafa-VirtualBox:~$
```

Instalando OpenVPN e biblioteca de compressão LZO: `apt install openvpn liblzo2-dev`

```
rafa@rafa-VirtualBox: ~  
File Edit View Search Terminal Help  
(Reading database ... 155436 files and directories currently installed.)  
Preparing to unpack .../libc-dev-bin_2.27-3ubuntu1.2_amd64.deb ...  
Unpacking libc-dev-bin (2.27-3ubuntu1.2) ...  
Selecting previously unselected package linux-libc-dev:amd64.  
Preparing to unpack .../linux-libc-dev_4.15.0-117.118_amd64.deb ...  
Unpacking linux-libc-dev:amd64 (4.15.0-117.118) ...  
Selecting previously unselected package libc6-dev:amd64.  
Preparing to unpack .../libc6-dev_2.27-3ubuntu1.2_amd64.deb ...  
Unpacking libc6-dev:amd64 (2.27-3ubuntu1.2) ...  
Selecting previously unselected package liblzo2-dev:amd64.  
Preparing to unpack .../liblzo2-dev_2.08-1.2_amd64.deb ...  
Unpacking liblzo2-dev:amd64 (2.08-1.2) ...  
Selecting previously unselected package manpages-dev.  
Preparing to unpack .../manpages-dev_4.15-1_all.deb ...  
Unpacking manpages-dev (4.15-1) ...  
Setting up linux-libc-dev:amd64 (4.15.0-117.118) ...  
Setting up libc-dev-bin (2.27-3ubuntu1.2) ...  
Setting up manpages-dev (4.15-1) ...  
Setting up libc6-dev:amd64 (2.27-3ubuntu1.2) ...  
Setting up liblzo2-dev:amd64 (2.08-1.2) ...  
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...  
rafa@rafa-VirtualBox:~$
```

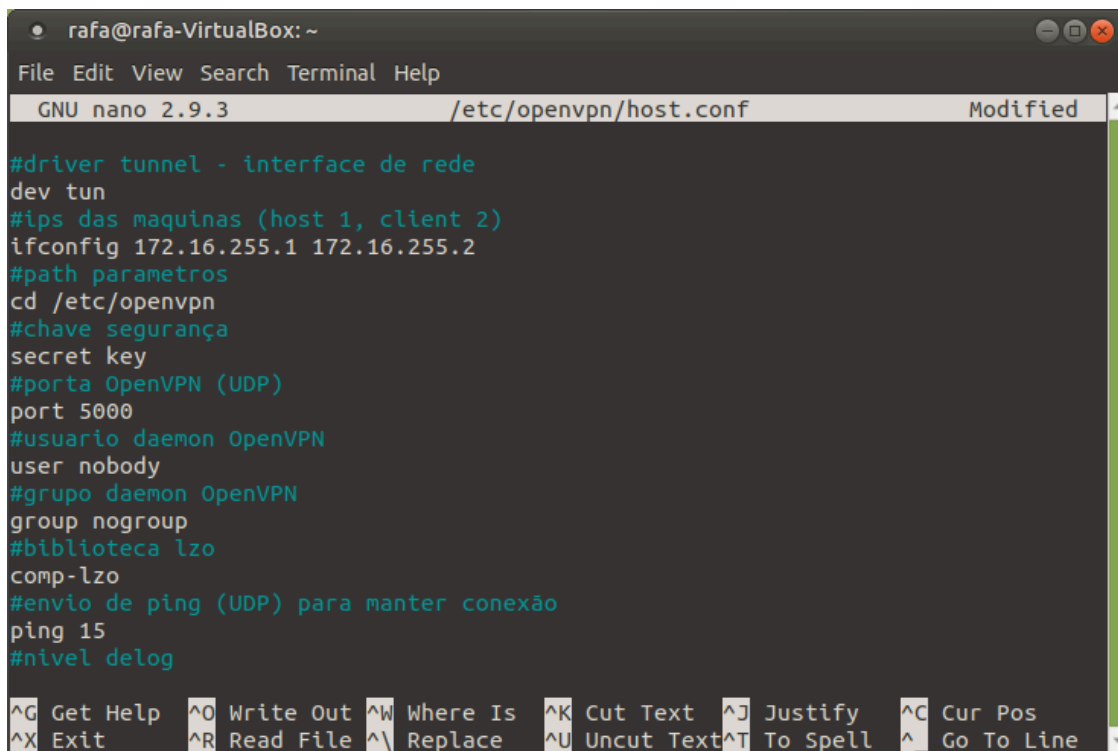
Criando a Chave de Segurança do OpenVPN: `openvpn --genkey --secret /etc/openvpn/key`

Exibindo a chave: `cat /etc/openvpn/key`

```
rafa@rafa-VirtualBox: ~  
File Edit View Search Terminal Help  
cat: /etc/openvpn/key: Permission denied  
rafa@rafa-VirtualBox:~$ sudo cat /etc/openvpn/key  
#  
# 2048 bit OpenVPN static key  
#  
-----BEGIN OpenVPN Static key V1-----  
2c11cc55dec7a240e970be65e7f025b6  
553b397ab2d60a3c6c81400a89243ea5  
716fd360467aade742f9de0864706bb6  
7c75896445c90b119ddcd2a33b2ebe85  
ca4b8909a6c508ec98fe29afa249fc99  
0e4a606251c4cade848cfd0985c6462  
25c25cd7ef7acfab41b3c6745a6978d3  
148853dfa7e18cf46eeef37c4012c41  
0773e303b43a2a11b2f223e7587be250  
16a19e6b8cadd57109461d69d58aab74  
78bcf66ff9f7fe27a9aca2731e79a6c5  
16fe617ce422fd1e48f3946a8a40c991  
9ab99cd839712dc0d1b0986493e0946a  
35350f057304a3941f3729546e655bcb  
b09178af57c8177bca674470ee129ed0  
80554e38cea308bd0d290c107e548d11  
-----END OpenVPN Static key V1-----  
rafa@rafa-VirtualBox:~$
```

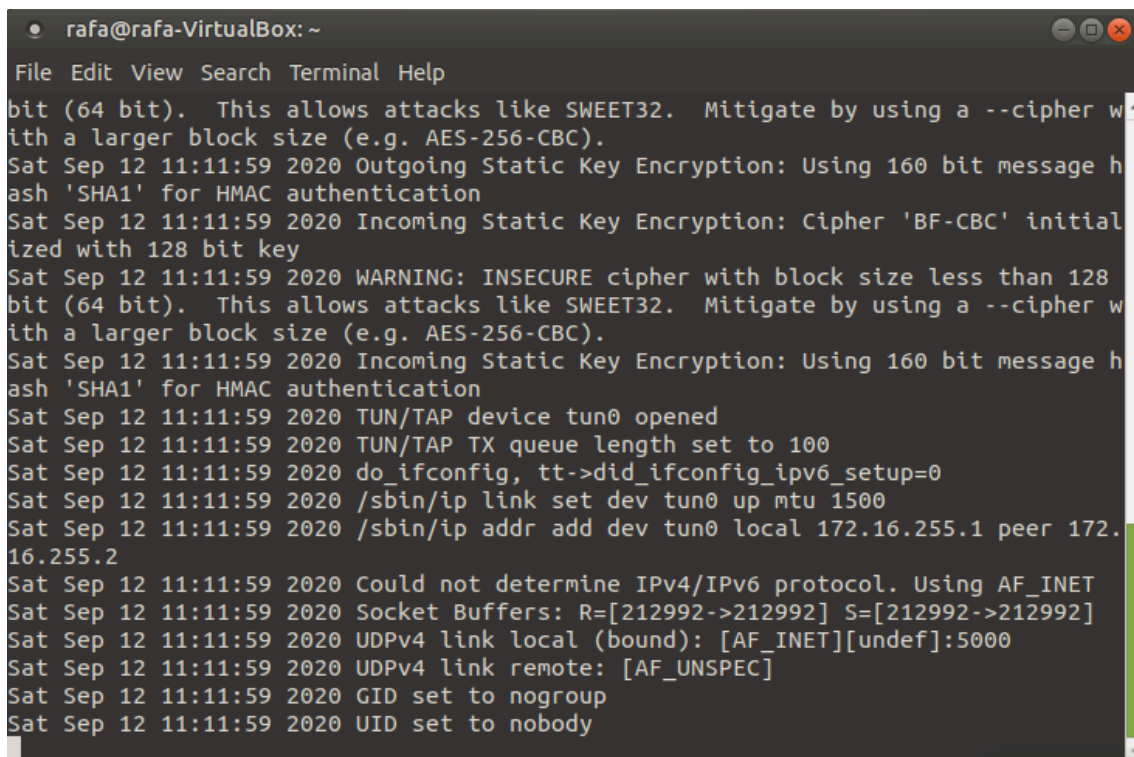
Acessando e configurando o arquivo host.conf (pessoalmente prefiro o nano):

`nano /etc/openvpn/host.conf`



```
rafa@rafa-VirtualBox: ~  
File Edit View Search Terminal Help  
GNU nano 2.9.3 /etc/openvpn/host.conf Modified  
  
#driver tunnel - interface de rede  
dev tun  
#ips das maquinas (host 1, client 2)  
ifconfig 172.16.255.1 172.16.255.2  
#path parametros  
cd /etc/openvpn  
#chave segurança  
secret key  
#porta OpenVPN (UDP)  
port 5000  
#usuario daemon OpenVPN  
user nobody  
#grupo daemon OpenVPN  
group nogroup  
#biblioteca lzo  
comp-lzo  
#envio de ping (UDP) para manter conexão  
ping 15  
#nivel debug  
  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

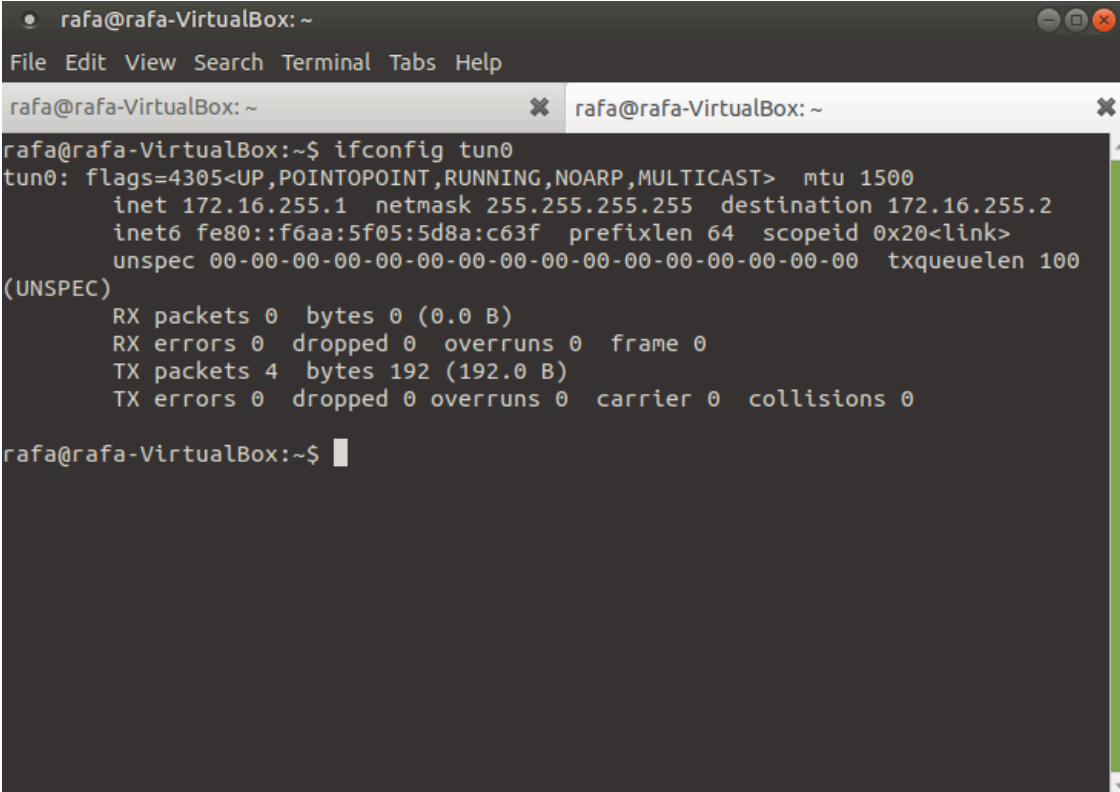
Iniciando o serviço: `openvpn --config /etc/openvpn/host.conf`



```
rafa@rafa-VirtualBox: ~  
File Edit View Search Terminal Help  
bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher w  
ith a larger block size (e.g. AES-256-CBC).  
Sat Sep 12 11:11:59 2020 Outgoing Static Key Encryption: Using 160 bit message h  
ash 'SHA1' for HMAC authentication  
Sat Sep 12 11:11:59 2020 Incoming Static Key Encryption: Cipher 'BF-CBC' initial  
ized with 128 bit key  
Sat Sep 12 11:11:59 2020 WARNING: INSECURE cipher with block size less than 128  
bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher w  
ith a larger block size (e.g. AES-256-CBC).  
Sat Sep 12 11:11:59 2020 Incoming Static Key Encryption: Using 160 bit message h  
ash 'SHA1' for HMAC authentication  
Sat Sep 12 11:11:59 2020 TUN/TAP device tun0 opened  
Sat Sep 12 11:11:59 2020 TUN/TAP TX queue length set to 100  
Sat Sep 12 11:11:59 2020 do_ifconfig, tt->did_ifconfig_ipv6_setup=0  
Sat Sep 12 11:11:59 2020 /sbin/ip link set dev tun0 up mtu 1500  
Sat Sep 12 11:11:59 2020 /sbin/ip addr add dev tun0 local 172.16.255.1 peer 172.  
16.255.2  
Sat Sep 12 11:11:59 2020 Could not determine IPv4/IPv6 protocol. Using AF_INET  
Sat Sep 12 11:11:59 2020 Socket Buffers: R=[212992->212992] S=[212992->212992]  
Sat Sep 12 11:11:59 2020 UDPv4 link local (bound): [AF_INET][undef]:5000  
Sat Sep 12 11:11:59 2020 UDPv4 link remote: [AF_UNSPEC]  
Sat Sep 12 11:11:59 2020 GID set to nogroup  
Sat Sep 12 11:11:59 2020 UID set to nobody
```

Verificando se a interface de rede está ativa (ctrl + C para fechar o servidor). É necessário manter o servidor ligado e abrir uma nova aba para o terminal.

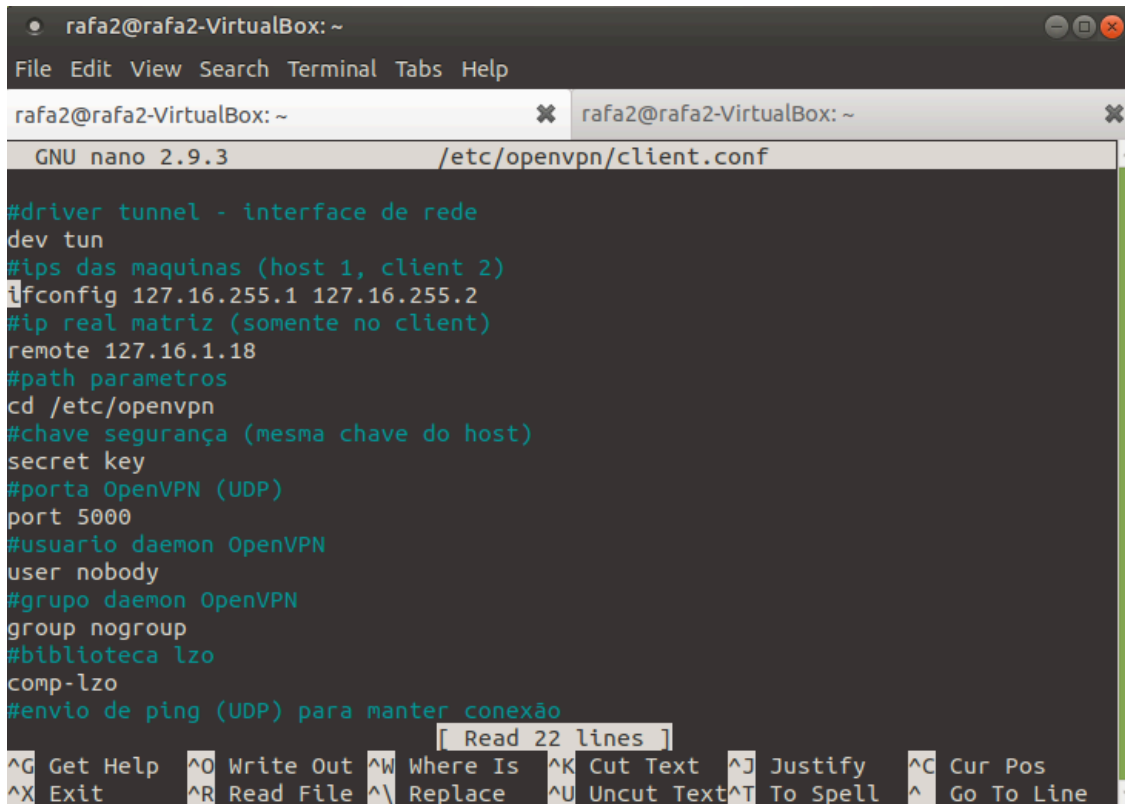
Ifconfig tun0



```
rafa@rafa-VirtualBox: ~  
File Edit View Search Terminal Tabs Help  
rafa@rafa-VirtualBox: ~ x rafa@rafa-VirtualBox: ~ x  
rafa@rafa-VirtualBox:~$ ifconfig tun0  
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500  
    inet 172.16.255.1 netmask 255.255.255.255 destination 172.16.255.2  
    inet6 fe80::f6aa:5f05:5d8a:c63f prefixlen 64 scopeid 0x20<link>  
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100  
(UNSPEC)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 192 (192.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
rafa@rafa-VirtualBox:~$
```

Client – Ubuntu MATE

Em uma segunda máquina (client), repetir os mesmos passos do host, com a diferença de que a chave de segurança do host precisa ser exatamente a mesma no cliente, a utilização de um ip remoto e atribuição de ip diferente (host/cliente) como na figura abaixo.



```
rafa2@rafa2-VirtualBox: ~
File Edit View Search Terminal Tabs Help

rafa2@rafa2-VirtualBox: ~
GNU nano 2.9.3 /etc/openvpn/client.conf

#driver tunnel - interface de rede
dev tun
#ips das maquinas (host 1, client 2)
ifconfig 127.16.255.1 127.16.255.2
#ip real matriz (somente no client)
remote 127.16.1.18
#path parametros
cd /etc/openvpn
#chave segurança (mesma chave do host)
secret key
#porta OpenVPN (UDP)
port 5000
#usuario daemon OpenVPN
user nobody
#grupo daemon OpenVPN
group nogroup
#biblioteca lzo
comp-lzo
#envio de ping (UDP) para manter conexão

[ Read 22 lines ]

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

Testando o tunelamento

Antes de iniciar o teste de ping, é necessário subir os servidores:

- `openvpn --config /etc/openvpn/host.conf`
- `openvpn --config /etc/openvpn/client.conf`

Em uma outra aba do terminal entrar com os comandos de ping.

Ping entre os computadores (host -> client): ping 127.16.255.2

```
rafa@rafa-VirtualBox: ~  
File Edit View Search Terminal Tabs Help  
rafa@rafa-VirtualBox: ~ x rafa@rafa-VirtualBox: ~ x  
rafa@rafa-VirtualBox:~$ ping 127.16.255.2  
PING 127.16.255.2 (127.16.255.2) 56(84) bytes of data.  
64 bytes from 127.16.255.2: icmp_seq=1 ttl=64 time=0.013 ms  
64 bytes from 127.16.255.2: icmp_seq=2 ttl=64 time=0.034 ms  
64 bytes from 127.16.255.2: icmp_seq=3 ttl=64 time=0.035 ms  
64 bytes from 127.16.255.2: icmp_seq=4 ttl=64 time=0.035 ms  
64 bytes from 127.16.255.2: icmp_seq=5 ttl=64 time=0.023 ms  
64 bytes from 127.16.255.2: icmp_seq=6 ttl=64 time=0.048 ms  
64 bytes from 127.16.255.2: icmp_seq=7 ttl=64 time=0.033 ms  
64 bytes from 127.16.255.2: icmp_seq=8 ttl=64 time=0.034 ms  
64 bytes from 127.16.255.2: icmp_seq=9 ttl=64 time=0.035 ms  
64 bytes from 127.16.255.2: icmp_seq=10 ttl=64 time=0.034 ms  
64 bytes from 127.16.255.2: icmp_seq=11 ttl=64 time=0.026 ms  
64 bytes from 127.16.255.2: icmp_seq=12 ttl=64 time=0.033 ms  
64 bytes from 127.16.255.2: icmp_seq=13 ttl=64 time=0.032 ms  
64 bytes from 127.16.255.2: icmp_seq=14 ttl=64 time=0.034 ms  
64 bytes from 127.16.255.2: icmp_seq=15 ttl=64 time=0.025 ms  
^C  
--- 127.16.255.2 ping statistics ---  
15 packets transmitted, 15 received, 0% packet loss, time 14343ms  
rtt min/avg/max/mdev = 0.013/0.031/0.048/0.009 ms  
rafa@rafa-VirtualBox:~$
```

Ping entre os computadores (cliente -> host): ping 127.16.255.1

```
rafa2@rafa2-VirtualBox: ~  
File Edit View Search Terminal Tabs Help  
rafa2@rafa2-VirtualBox: ~ x rafa2@rafa2-VirtualBox: ~ x  
rafa2@rafa2-VirtualBox:~$ ping 127.16.255.1  
PING 127.16.255.1 (127.16.255.1) 56(84) bytes of data.  
64 bytes from 127.16.255.1: icmp_seq=1 ttl=64 time=0.017 ms  
64 bytes from 127.16.255.1: icmp_seq=2 ttl=64 time=0.023 ms  
64 bytes from 127.16.255.1: icmp_seq=3 ttl=64 time=0.042 ms  
64 bytes from 127.16.255.1: icmp_seq=4 ttl=64 time=0.077 ms  
64 bytes from 127.16.255.1: icmp_seq=5 ttl=64 time=0.035 ms  
64 bytes from 127.16.255.1: icmp_seq=6 ttl=64 time=0.034 ms  
64 bytes from 127.16.255.1: icmp_seq=7 ttl=64 time=0.035 ms  
64 bytes from 127.16.255.1: icmp_seq=8 ttl=64 time=0.034 ms  
64 bytes from 127.16.255.1: icmp_seq=9 ttl=64 time=0.026 ms  
64 bytes from 127.16.255.1: icmp_seq=10 ttl=64 time=0.024 ms  
64 bytes from 127.16.255.1: icmp_seq=11 ttl=64 time=0.035 ms  
64 bytes from 127.16.255.1: icmp_seq=12 ttl=64 time=0.035 ms  
64 bytes from 127.16.255.1: icmp_seq=13 ttl=64 time=0.034 ms  
64 bytes from 127.16.255.1: icmp_seq=14 ttl=64 time=0.037 ms  
^C  
--- 127.16.255.1 ping statistics ---  
14 packets transmitted, 14 received, 0% packet loss, time 13311ms  
rtt min/avg/max/mdev = 0.017/0.034/0.077/0.015 ms  
rafa2@rafa2-VirtualBox:~$
```


Conclusão

Alguns anos atrás a preocupação na internet era apenas em relação aos crimes cibernéticos, mas agora, além dos crimes cibernéticos, também existem as empresas que querem seus dados para, de uma maneira ou de outra, utilizá-los em prol da própria empresa e as vezes até mesmo contra os usuários (em formas de propaganda, rastreios, etc), então a ideia de utilizar uma VPN hoje em dia é uma excelente opção de se manter mais seguro, talvez esse seja o futuro da internet, VPNs!