



OpenVPN

Sumário

Capítulo 1	
OpenVPN	3
1.1. Mãos a obra.....	4
Capítulo 2	
Gerenciando	5
2.1. Objetivos.....	5
2.1. Troubleshooting.....	5

Índice de tabelas

Índice de Figuras

Capítulo 1

OpenVPN

- Historia da VPN;
- Descrição de opções extras;
- Melhorando a segurança.

1.1. Mãos a obra

O surgimento da VPN se deve a necessidade de se utilizar redes de comunicação não confiáveis, como a Internet para trafegar informações de forma segura. A Virtual Private Network no passado já esteve associada a serviços remotos de conectividade, como a rede de telefonia pública comutada (RTPC) ou os PVCs (Permanent Virtual Circuits/Channel) do Frame Relay.



Mas como uma VPN funciona?

A VPN utiliza protocolos de tunelamento e procedimentos de encriptação, garantindo a integridade e autenticidade dos dados. Com a VPN é possível interligar duas ou mais redes, em diferente tipos de sistemas operacionais.

Algumas soluções em VPN no Linux

VPNs do tipo IPSec

É uma das VPN mais antigas que ainda é muito útil e segura quando devidamente configurada. Existem duas grandes implementações do IPSec no Linux, que estão separadas em dois projetos. O primeiro é o projeto que foi originalmente chamado FreeS/WAN, mas agora separado em Openswan e strongSwan.

Saiba mais sobre FreeS/WAN acessando:



<http://www.freeswan.org/>

Saiba mais sobre Openswan acessando:



<http://www.openswan.org/>

Saiba mais sobre strongSwan acessando:



<http://www.strongswan.org/>

VPNs do tipo PPTP

Utiliza o protocolo PPTP, apoiada pela Microsoft inicialmente na época do Windows 95. PoPToP é o principal servidor PPTP para Linux, sendo interessante utilizar L2TP sobre IPSec que é mais seguro.

Saiba mais sobre PopTop acessando:



<http://poptop.sourceforge.net/>

VPNs do tipo SSL

Utiliza SSL apenas necessitando de uma única porta TCP ou UDP para o tráfego no túnel, assim podendo facilmente atravessar a maioria dos firewalls. Seguro e flexível o OpenVPN possui versões Linux e Windows, permitindo criar túneis interligando máquinas rodando os dois sistemas operacionais.

Saiba mais sobre OpenVPN acessando:



<http://openvpn.net/>

Descrição de opções extras - OpenVPN

Vamos ver na prática algumas opções extras usando OpenVPN no Linux, além de instalar e configurar em dois servidores.

Primeiro instale o pacote openvpn



```
# aptitude install openvpn
```

Acesse o diretório /etc/openvpn e crie a chave de encriptação de 2048 bits, que será usada para criar a conexão.



```
# openvpn --genkey --secret /etc/openvpn/chave
```

Crie o arquivo de configuração do servidor.



```
# vim /etc/openvpn/server.conf
```

```
dev tun
ifconfig 172.16.3.1 172.16.3.2
secret /etc/openvpn/chave
port 5000
comp-lzo
verb 4
keepalive 10 120
persist-key
persist-tun
float
```

Veja abaixo a descrição de cada opção utilizada

dev tun → Habilita suporte ao drive TUN/TAP;

ifconfig → Cria o IP do servidor matriz (172.16.3.1) com suporte ao IP do servidor filial (172.16.3.2);

secret → Comando para chamar nossa chave criptografada e o local dela;

port → Define a porta que a OpenVPN vai rodar;

comp-lzo → Ativa suporte a compressão;

verb → Nível para depuração de erros;

keepalive → Envia um ping a cada 10 segundos sem atividade e a VPN é reiniciada depois de 120 segundos sem respostas.

persist-key → Assegura que o daemon mantenha as chaves carregadas, quando a VPN é restabelecida depois de uma queda de conexão;

persist-tun → Assegura que o daemon mantenha a interface tun aberta, quando a VPN é restabelecida depois de uma queda de conexão;

float → Permite que o túnel continue aberto mesmo que o endereço IP da outra máquina mude.

Na maquina servidor (filial), copie a chave do servidor matriz de forma segura (ssh sftp), instale o pacote do openvpn e crie o arquivo de configuração com o nome de client.conf



```
# vim /etc/openvpn/client.conf
```

```
dev tun
ifconfig 172.16.3.2 172.16.3.1
remote 192.168.200.10
secret /etc/openvpn/chave
port 5000
comp-lzo
verb 4
keepalive 10 120
persist-key
persist-tun
float
```

A única diferença na maquina cliente é a opção “remote”, que se refere ao IP da maquina matriz. Em nosso exemplo esta sendo usado um IP publico, sendo trocado por IP privado quando usado na Internet.

Levantar a VPN de forma manual e automática

Para verificar alguma informação de erro, levante sua VPN de forma manual no servidor através do comando `openvpn`.



```
# openvpn --config /etc/openvpn/server.conf
```

E na maquina cliente



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

Para levantar sua VPN de forma automática no servidor e cliente use o comando `invoke-rc.d`



```
# invoke-rc.d openvpn start
```

E na maquina cliente



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

Melhorando a segurança

A OpenVPN oferece vários mecanismos para adicionar camadas adicionais de segurança, como por exemplo rodar em `chroot`, uso de conexões TLSs, certificados, uso de chaves com maiores bits. Todas essas camadas previnem ataques como “Man in the Middle”, “DoS”, “Flooding”, “Port scanning” e “Buffer overflow”. Vamos á prática:

Rodar OpenVPN sem privilegio de root

Adicione a configuração no servidor e cliente, as opções “user” e “group” para que o OpenVPN seja executado como usuário nobody e grupo nogroup.

```
dev tun
ifconfig 172.16.3.1 172.16.3.2
secret /etc/openvpn/chave
port 5000
comp-lzo
verb 4
keepalive 10 120
persist-key
persist-tun
float
user nobody
group nogroup
```

Tls-auth HMAC

Você pode adicionar uma assinatura que será verificada antes do processamento de todos os pacotes UPD. Em nossa configuração do servidor vamos habilitar as seguintes opções:

tls-auth → Habilita o controle de conexões tls;

tls-server → Ajuda a bloquear ataques DoS e flooding na porta do OpenVPN;

ca → Certificado de autoridade (CA) que usa as bibliotecas do OpenSSL;

cert → Certificado do servidor;

key → Chave RSA de 2048 do servidor;

dh → Parâmetros Diffie-Hellman utilizado para a troca das chaves criptografadas durante a execução;

cipher → Define um tipo de criptografia maior.

Para gerar os certificados e chaves o OpenVPN traz junto a sua instalação, uma série de scripts chamados “easy-rsa”. Eles podem ser encontrados em /usr/share/doc/openvpn/examples/easy-rsa/2.0/



```
# ls /usr/share/doc/openvpn/examples/easy-rsa/2.0/
```

```
build-ca          build-key-server  Makefile          sign-req
build-dh          build-req         openssl-0.9.6.cnf.gz  vars
build-inter       build-req-pass   openssl.cnf       whichopensslcnf
build-key         clean-all       pkitoool
build-key-pass    inherit-inter   README.gz
build-key-pkcs12  list-crl        revoke-full
```

Veja que na lista de scripts cada um, tem uma função específica para criação de certificados e chaves. Vamos copiar o diretório com os scripts para nossa instalação do OpenVPN



```
# cp -a /usr/share/doc/openvpn/examples/easy-rsa/2.0 /etc/openvpn/
```

Acesse o diretório com os scripts copiados



```
# cd /etc/openvpn/2.0
```

Para você personalizar suas configurações e informações edite o arquivo vars, como exemplo vamos aumentar o tamanho da chave alterando o valor da variável KEY_SIZE.



```
# vim vars
```

```
# Increase this to 2048 if you
# are paranoid. This will slow
# down TLS negotiation performance
# as well as the one-time DH parms
# generation process.
export KEY_SIZE=2048
```

Crie o subdiretório onde serão armazenadas as chaves e certificados



```
# mkdir keys
```

Gerando certificado CA e chave RSA

Utilizando os scripts vamos gerar os certificados e chaves, que serão utilizados em nossa configuração do OpenVPN.

Instale o pacote openssl



```
# aptitude install openssl
```

Use a sequencia de comandos abaixo para gerar o certificado de autoridade



```
# . vars  
# ./clean-all  
# ./build-ca
```

Será gerado uma chave RSA de 2048 bits no subdiretório keys

```
Generating a 2048 bit RSA private key  
.....+++  
.....+++  
writing new private key to 'ca.key'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----
```

Preencha as informações do certificado

```
Country Name (2 letter code) [US]:BR
State or Province Name (full name) [CA]:SP
Locality Name (eg, city) [SanFrancisco]:Sao Paulo
Organization Name (eg, company) [Fort-Funston]:Empresa
Organizational Unit Name (eg, section) []:TI
Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:server
Email Address [me@myhost.mydomain]:aluno@empresa.com.br
```

Liste o conteúdo do subdiretório keys e verifique o arquivo de certificado (ca.crt) e o arquivo da chave (ca.key)

Gerando certificado e chave para o servidor

Use o script abaixo digitando ao lado o hostname de sua maquina



```
# ./build-key-server server
```

Sera gerado uma chave RSA de 2048 bits no subdiretório keys

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

Preencha as informações do certificado e em opções “extra” tecle Enter duas vezes para deixar em branco.

```
Country Name (2 letter code) [US]:BR
State or Province Name (full name) [CA]:SP
Locality Name (eg, city) [SanFrancisco]:Sao Paulo
Organization Name (eg, company) [Fort-Funston]:Empresa
Organizational Unit Name (eg, section) []:TI
Common Name (eg, your name or your server's hostname) [server]:server
Email Address [me@myhost.mydomain]:aluno@empresa.com.br

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Sera perguntando se você deseja assinar o certificado, tecle “y” para confirmar e tecle “y” para autenticar.

```
Using configuration from /etc/openvpn/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'BR'
stateOrProvinceName     :PRINTABLE:'SP'
localityName            :PRINTABLE:'Sao Paulo'
organizationName        :PRINTABLE:'Empresa'
organizationalUnitName  :PRINTABLE:'TI'
commonName               :PRINTABLE:'server'
emailAddress            :IA5STRING:'aluno@empresa.com.br'
Certificate is to be certified until Jan  2 07:34:08 2021 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Liste o conteúdo do subdiretório keys e verifique o arquivo de certificado do servidor (server.csr), o arquivo da chave do servidor (server.key) e o certificado auto assinado (server.crt).

Gerando parâmetros Diffie-Hellman

Os parâmetros Diffie-Hellman são utilizados para a troca das chaves criptografadas durante a execução do OpenVPN.

Use o script abaixo para gerar os parâmetros



```
# ./build-dh
```

```
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
```

```
.....
.....+.....+.....
.....
```

Liste o conteúdo do subdiretório `keys` e verifique o arquivo com os parâmetros Diffie-Hellman (`dh2048.pem`).

Configurando o servidor OpenVPN

Com os certificados e chaves gerados, abra o arquivo do servidor e adicione as opções abaixo:



```
# vim /etc/openvpn/server.conf
```

```
dev tun
ifconfig 172.16.3.1 172.16.3.2
port 5000
comp-lzo
verb 4
keepalive 10 120
persist-key
persist-tun
float
user nobody
group nogroup
tls-server
tls-auth chave 0
ca 2.0/keys/ca.crt
cert 2.0/keys/server.crt
key 2.0/keys/server.key
dh 2.0/keys/dh2048.pem
cipher DES-EDE3-CBC
```

Configurando o cliente

Ainda na maquina servidor (matriz) crie a chave e o certificado para a maquina cliente, com o hostname da maquina cliente.



```
# cd /etc/openvpn/2.0
# ./build-key client
```

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'client.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

Preencha as informações do certificado e em opções “extra” tecle Enter duas vezes para deixar em branco.

```
Country Name (2 letter code) [US]:BR
State or Province Name (full name) [CA]:SP
Locality Name (eg, city) [SanFrancisco]:Sao Paulo
Organization Name (eg, company) [Fort-Funston]:Empresa
Organizational Unit Name (eg, section) []:TI
Common Name (eg, your name or your server's hostname) [client]:client
Email Address [me@myhost.mydomain]:aluno@empresa.com.br

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Sera perguntando se você deseja assinar o certificado, tecle “y” para confirmar e tecle “y” para autenticar.

```
Using configuration from /etc/openvpn/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'BR'
stateOrProvinceName     :PRINTABLE:'SP'
localityName            :PRINTABLE:'Sao Paulo'
organizationName        :PRINTABLE:'Empresa'
organizationalUnitName  :PRINTABLE:'TI'
commonName              :PRINTABLE:'client'
emailAddress            :IA5STRING:'aluno@empresa.com.br'
Certificate is to be certified until Jan  2 10:12:20 2021 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
```

Faça a copia dos arquivos abaixo via ssh para a maquina cliente.



```
# cd /etc/openvpn/2.0/keys
# scp client.key client.crt ca.crt root@192.168.200.20:/etc/openvpn
```

```
client.key          100% 1675      1.6KB/s   00:00
client.crt          100% 5181      5.1KB/s   00:00
ca.crt              100% 1610      1.6KB/s   00:00
```

Na maquina cliente (filial) com os certificados e chaves gerados, abra o arquivo do cliente e adicione as opções abaixo:



```
# vim /etc/openvpn/client.conf
```

```
dev tun
ifconfig 172.16.3.2 172.16.3.1
remote 192.168.200.10
port 5000
comp-lzo
verb 4
keepalive 10 120
persist-key
persist-tun
float
user nobody
group nogroup
ns-cert-type server
tls-client
tls-auth chave 1
ca ca.crt
cert client.crt
key client.key
cipher DES-EDE3-CBC
```

Descrição das novas opções utilizadas:

ns-cert-type → Indica que certificado foi assinado pelo servidor;

tls-client → Habilita conexão TLS, ajudando a bloquear ataques DoS e flooding na porta do OpenVPN.

Para finalizar use o comando `invoke-rc.d` na maquina matriz e filial e teste a conectividade entre ambas. Em caso de erro veja os logs no arquivo `/var/log/daemon.log`



```
# invoke-rc.d openvpn start
```


Capítulo 2

Gerenciando

2.1. Objetivos

- Troubleshooting: VPN entre Linux e Windows.

2.1. Troubleshooting



Como posso criar um VPN entre maquinas Linux e Windows?

Através do OpenVPN que da suporte tanto ao Linux quanto ao Windows. Considerando que sua VPN esta configurada na maquina Linux com certificados e chaves, acesse a maquina Windows (filial) e baixe o arquivo de instalação do OpenVPN.

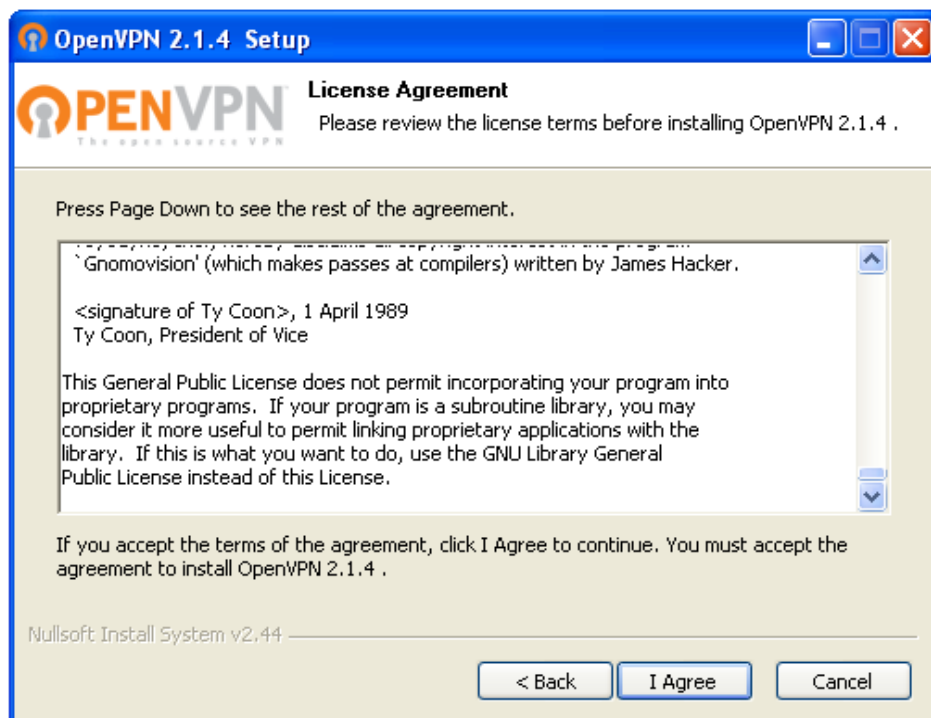


<http://swupdate.openvpn.net/community/releases/openvpn-2.1.4-install.exe>

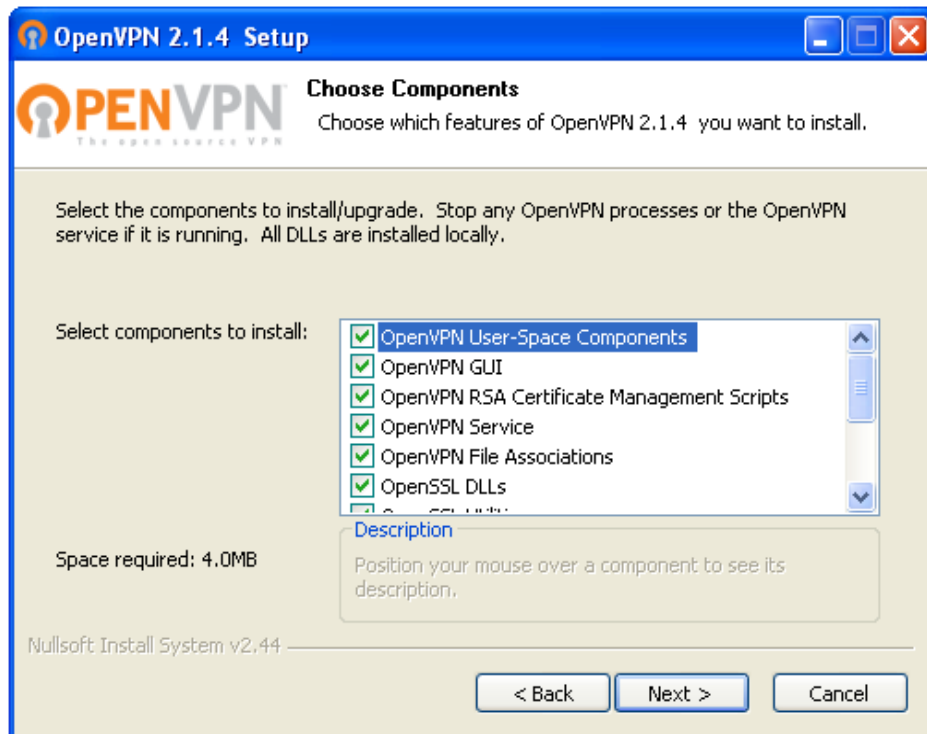
A instalação segue o padrão no estilo “setup” usando “Next”



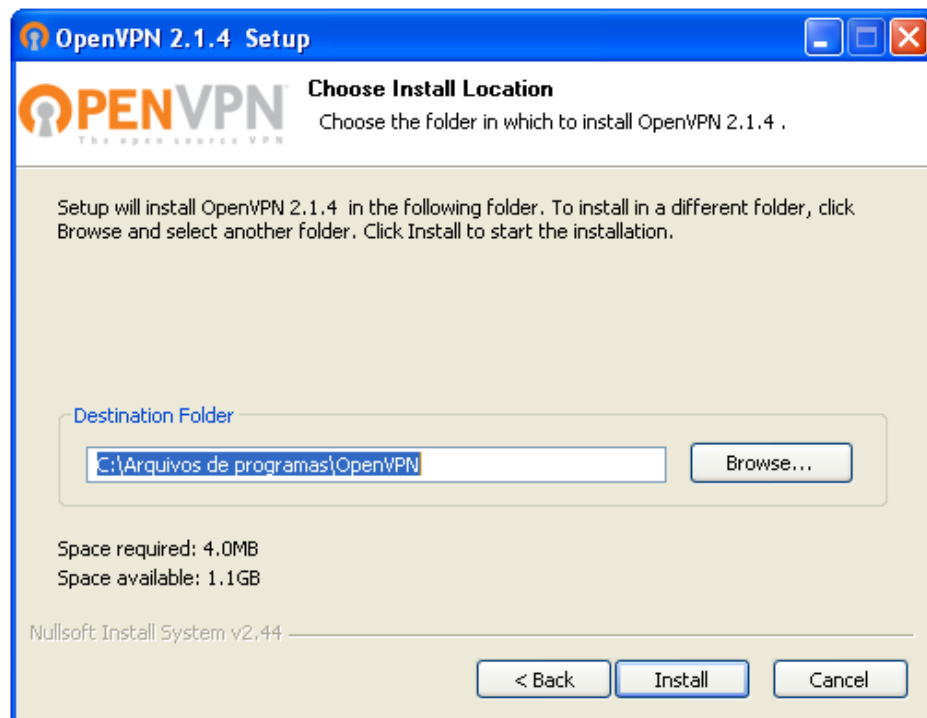
Aceite a licença de uso e clique em “I Agree” para continuar



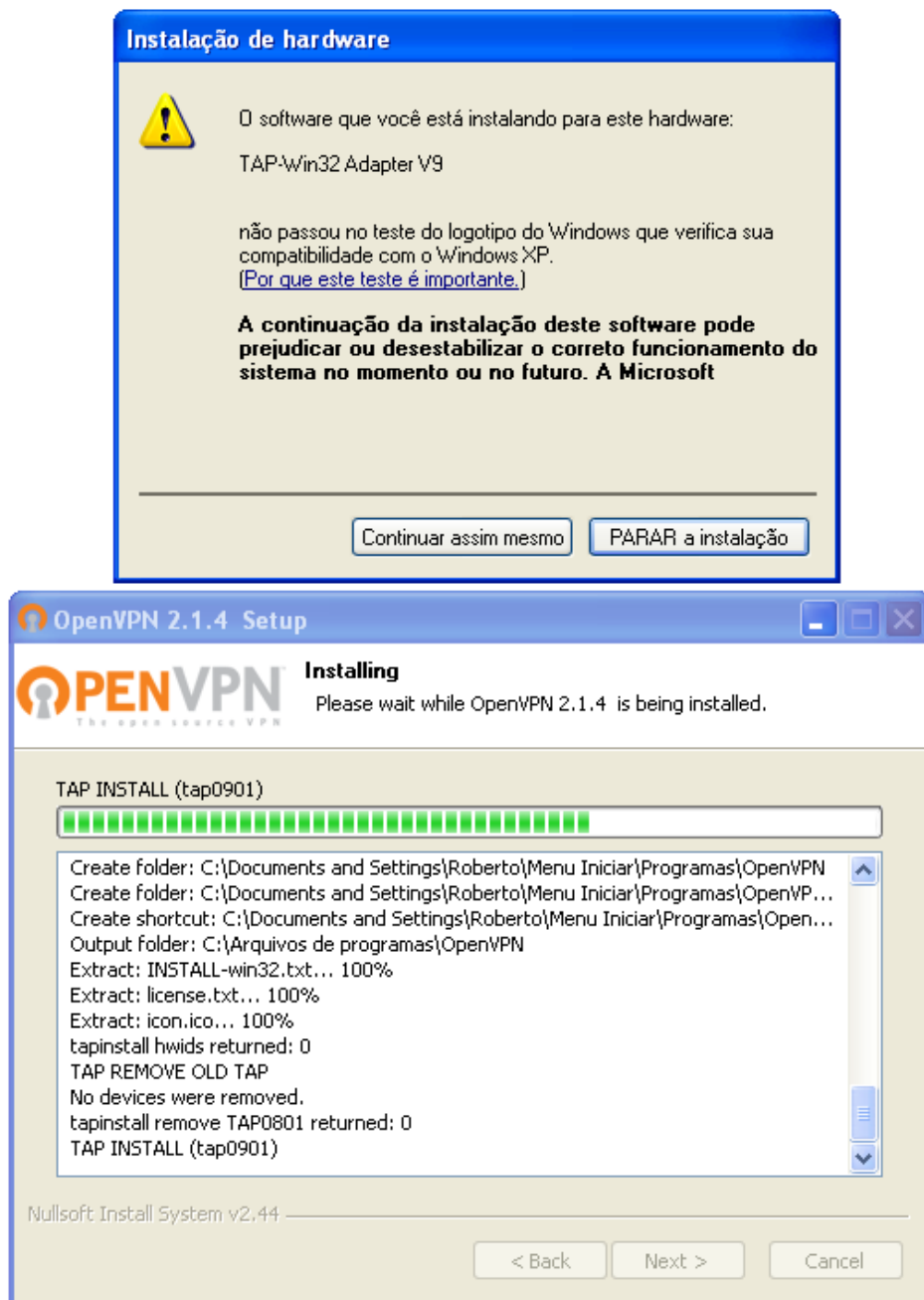
Selecione todas as opções para ter suporte a conexão TLS



Deixe como padrão o diretório da instalação, onde serão armazenados arquivos de configuração, certificados e chaves. Clique em “Install” para continuar.



Nesta etapa da instalação clique em “Continuar assim mesmo” para instalar o dispositivo Tun Tap usado na comunicação do OpenVPN.



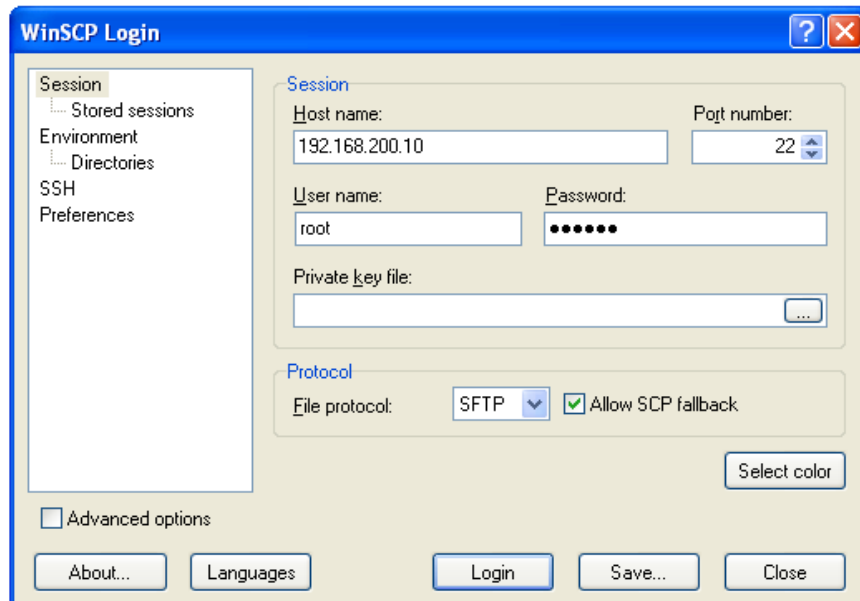
Com a instalação terminada clique em “Finish”

Agora é preciso copiar os certificados e chaves de forma segura, da máquina matriz (Linux) para a máquina filial (Windows). Para isso podemos usar o Winscp que pode ser obtido em:

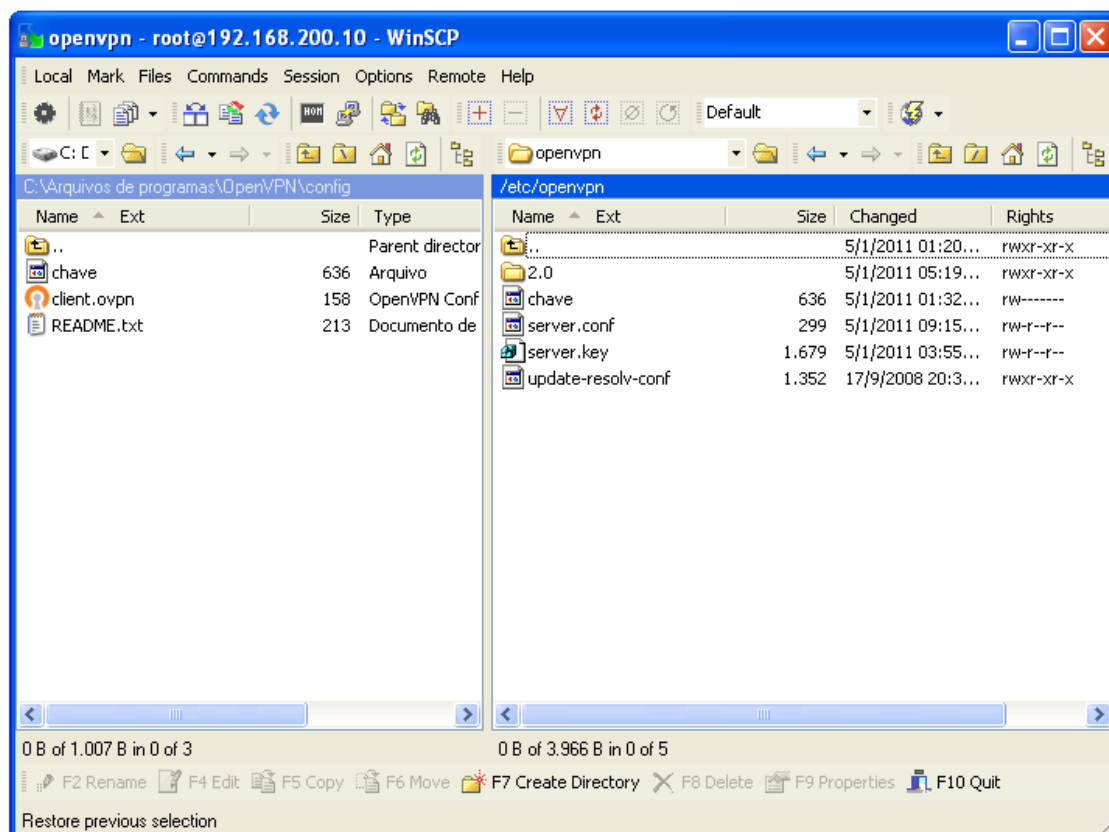


<http://winscp.net/download/winscp429setup.exe>

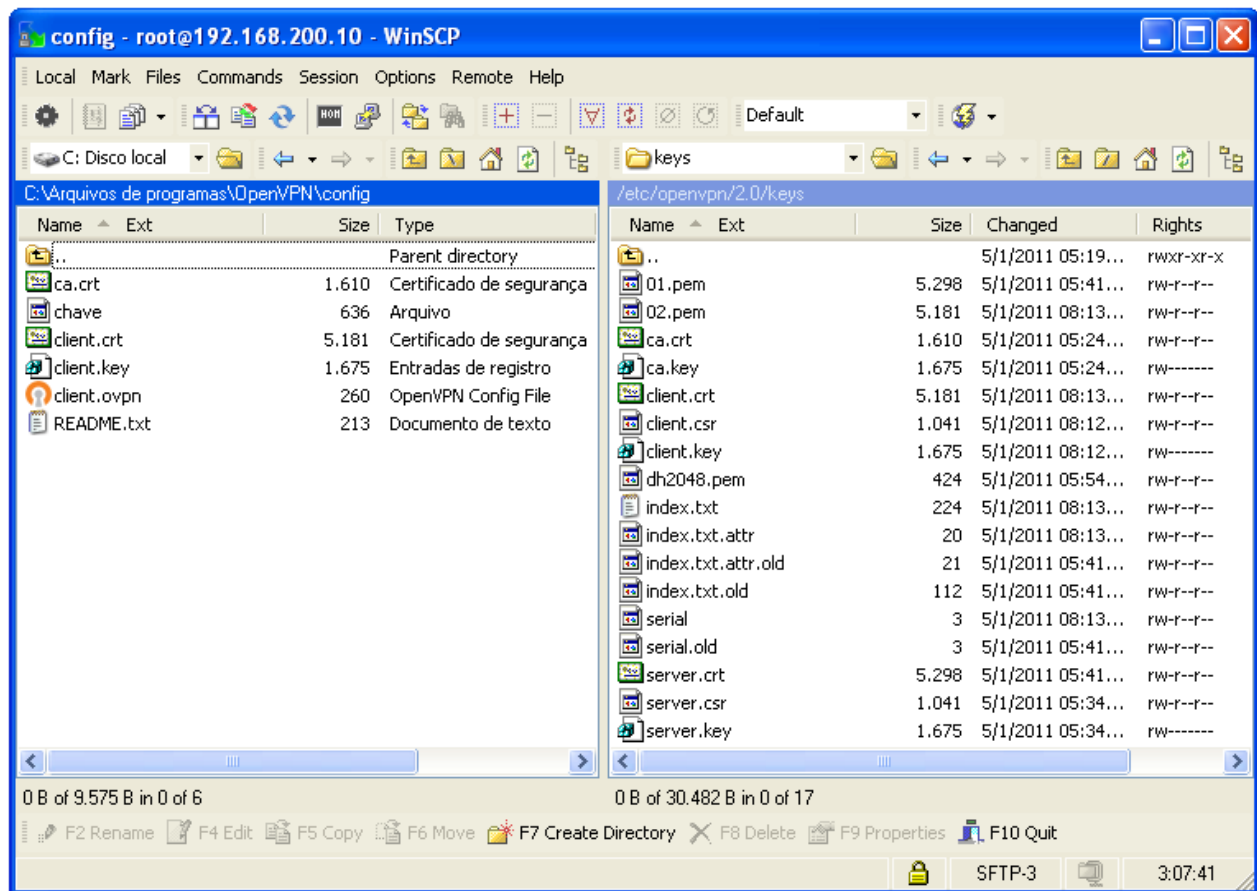
Instale o WinSCP com a opção “Commander interface” e acesse o servidor digitando o IP, nome de usuário e senha.



Clique e arraste da matriz (Linux) para a maquina filial (Windows) o arquivo chave.

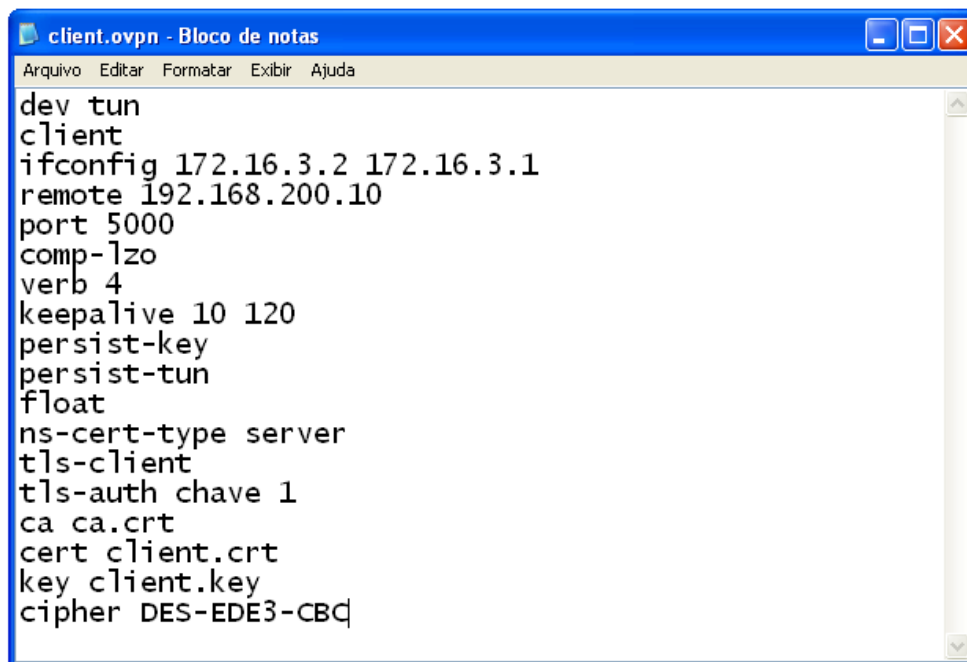


Não esqueça de clicar e arrastar da matriz (Linux) para a maquina filial (Windows) os arquivos de certificados e chave.



Criando arquivo de configuração na maquina Windows

Abra o bloco de notas e crie o arquivo client.ovpn em C:\Arquivos de programas\OpenVPN\config, com o seguinte conteúdo:



```

dev tun
client
ifconfig 172.16.3.2 172.16.3.1
remote 192.168.200.10
port 5000
comp-lzo
verb 4
keepalive 10 120
persist-key
persist-tun
float
ns-cert-type server
tls-client
tls-auth chave 1
ca ca.crt
cert client.crt
key client.key
cipher DES-EDE3-CBC

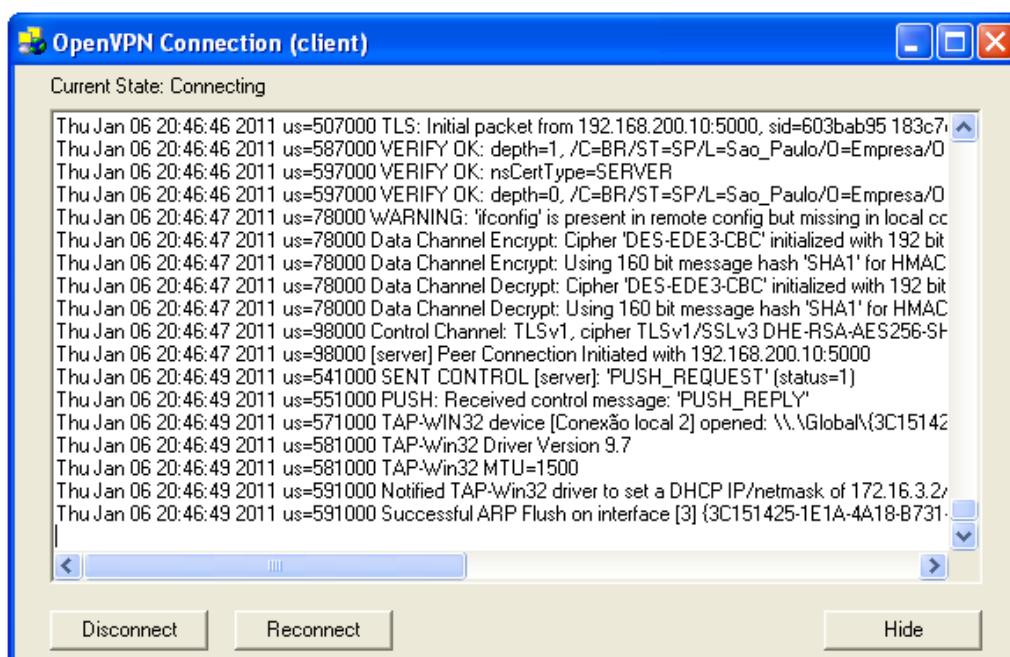
```

No servidor Linux inicie o OpenVPN com o comando `invoke-rc.d`



```
# invoke-rc.d openvpn start
```

No Windows clique em Iniciar → Todos os programas → OpenVPN → OpenVPN GUI. Depois de executar este software, você deverá ver um ícone do OpenVPN na bandeja do sistema. Clique no botão direito do mouse e escolha "Connect"



No servidor é possível acompanhar a conexão entre as máquinas, através dos logs no arquivo `/var/log/daemon.log`



```
# tail -f /var/log/daemon.log
```

```
5:5000, sid=c07cbb5c 41761682
Jan 6 20:40:19 server ovpn-server[2467]: VERIFY OK: depth=1, /C=BR/ST=SP/L=Sao_
Paulo/O=Empresa/OU=TI/CN=server/emailAddress=aluno@empresa.com.br
Jan 6 20:40:19 server ovpn-server[2467]: VERIFY OK: depth=0, /C=BR/ST=SP/L=Sao_
Paulo/O=Empresa/OU=TI/CN=client/emailAddress=aluno@empresa.com.br
Jan 6 20:40:19 server ovpn-server[2467]: WARNING: 'ifconfig' is present in loca
l config but missing in remote config, local='ifconfig 172.16.3.1 172.16.3.2'
Jan 6 20:40:19 server ovpn-server[2467]: Data Channel Encrypt: Cipher 'DES-EDE3
-CBC' initialized with 192 bit key
Jan 6 20:40:19 server ovpn-server[2467]: Data Channel Encrypt: Using 160 bit me
ssage hash 'SHA1' for HMAC authentication
Jan 6 20:40:19 server ovpn-server[2467]: Data Channel Decrypt: Cipher 'DES-EDE3
-CBC' initialized with 192 bit key
Jan 6 20:40:19 server ovpn-server[2467]: Data Channel Decrypt: Using 160 bit me
ssage hash 'SHA1' for HMAC authentication
Jan 6 20:40:19 server ovpn-server[2467]: Control Channel: TLSv1, cipher TLSv1/S
SLv3 DHE-RSA-AES256-SHA, 2048 bit RSA
Jan 6 20:40:19 server ovpn-server[2467]: [client] Peer Connection Initiated wit
h 192.168.200.15:5000
Jan 6 20:40:20 server ovpn-server[2467]: Initialization Sequence Completed
Jan 6 20:40:21 server ovpn-server[2467]: PUSH: Received control message: 'PUSH_
REQUEST'
Jan 6 20:40:21 server ovpn-server[2467]: SENT CONTROL [client]: 'PUSH_REPLY' (s
tatus=1)
```

Teste a conectividade entre as máquinas através do comando ping:

Na máquina servidor (Linux)

```
PING 172.16.3.2 (172.16.3.2) 56(84) bytes of data.
64 bytes from 172.16.3.2: icmp_seq=1 ttl=128 time=1.62 ms
64 bytes from 172.16.3.2: icmp_seq=2 ttl=128 time=1.89 ms
64 bytes from 172.16.3.2: icmp_seq=3 ttl=128 time=1.21 ms
64 bytes from 172.16.3.2: icmp_seq=4 ttl=128 time=3.55 ms
```

Na máquina cliente (Windows)

```
Disparando contra 172.16.3.1 com 32 bytes de dados:
Resposta de 172.16.3.1: bytes=32 tempo=3ms TTL=64
Resposta de 172.16.3.1: bytes=32 tempo=2ms TTL=64
Resposta de 172.16.3.1: bytes=32 tempo=1ms TTL=64
Resposta de 172.16.3.1: bytes=32 tempo=1ms TTL=64
```