**VPN em Linux com OpenVPN**

Autor: Guilherme Rezende de Almeida <guilerezende at hotmail.com>
Data: 04/06/2005

**Introdução**

Quando iniciei meu primeiro projeto de *VPN* (uns 3 anos atrás), me deparei com algumas ferramentas disponíveis para atender tal serviço. Como as coisas sempre aparecem e tem que ser executadas de última hora, resolvi sem muito planejamento e estudo utilizar a ferramenta Freeswan, usando o protocolo Ipsec, até porque encontrei mais artigos sobre essa ferramenta na Internet. Vantagens e desvantagens sobre o uso do protocolo Ipsec podem ser conferidas em www.altoriopreto.com.br.

No entanto, depois de algumas semanas de "quebra cabeça", consegui configurar minha VPN com essa ferramenta e até então fiquei satisfeito com o resultado que obtive, pois já tinha perdido algumas noites de sono e me senti recompensado por todo o esforço feito.

Passado um tempo, resolvi mudar de software de VPN, passando a utilizar o *OpenVPN* em meus serviços. Depois de muita leitura sobre essa ferramenta, resolvi tomar essa decisão em virtude do mal funcionamento do Freeswan, pois os pacotes UDP dessa ferramenta enfrentavam dificuldades ao passar por firewall baseado em Statefull, problemas com conexão de IP inválido, dificuldade em sua configuração e, além disso, o projeto está descontinuado.

Esse artigo tem como objetivo mostrar de forma rápida e simples a configuração de uma VPN baseada em *Linux* utilizando o OpenVPN como ferramenta, sendo que este é um software estável, simples de configurar, além de ser um projeto que está sempre em desenvolvimento.

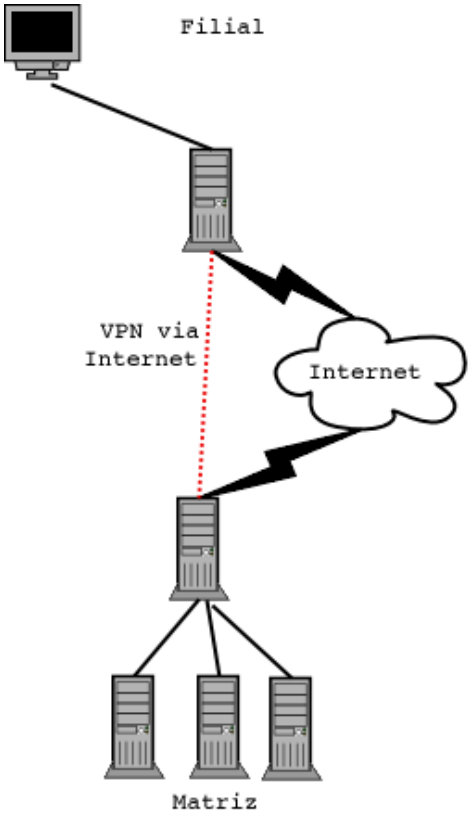
Vamos considerar o caso de interligar as redes internas de uma empresa (matriz e filial), sendo que ambas se localizam em lugares diferentes e bem distantes, que cada empresa possui uma conexão ADSL rodando Linux como servidor e suas respectivas redes internas conforme o exemplo hipotético abaixo:

Matriz

- ADSL com IP 200.217.222.222
- LAN com a classe 192.168.1.0/24

Filial

- ADSL com ip 200.141.64.33
- LAN com a classe 192.168.2.0/24




Em nossa VPN, teremos como principal objetivo fazer com que qualquer máquina da rede interna da Matriz se conecte diretamente com qualquer máquina da rede interna da Filial (ou vice versa), deixando a impressão de que ambas as redes estão no mesmo meio físico.

**Instalação**

Antes de começar, devemos checar primeiramente se o driver TUN/TAP se encontra no kernel. Caso o mesmo não se encontre, precisaremos ativar esse driver dentro da opção "Network Device Support", conforme exemplo abaixo:

```
[*] Network device support
        ARCnet devices  --->
        < > Dummy net driver support
        < > Bonding driver support
        < > EQL (serial line load balancing) support
        <*> Universal TUN/TAP device driver support
        < > Ethertap network tap (OBSOLETE)
        < > General Instruments Surfboard 1000
        Ethernet (10 or 100Mbit)  --->
        Ethernet (1000 Mbit)  --->
        [ ] FDDI driver support
        [ ] HIPPI driver support (EXPERIMENTAL)
        <*> PPP (point-to-point protocol) support
        < > SLIP (serial line) support
        Wireless LAN (non-hamradio)  --->
        Token Ring devices  --->
        [ ] Fibre Channel driver support
        < > Red Creek Hardware VPN (EXPERIMENTAL)
        < > Traffic Shaper (EXPERIMENTAL)
        Wan interfaces  --->
```

Não irei abortar nesse artigo exemplos de compilação de kernel, bem como a configuração de conexão ADSL no *Linux*, uma vez que existem bons artigos abordando esses assunto no site.

NOTA: Nas distros RedHat 9.0, Slackware 9.1, 10.0 e 10.1 não foi preciso mexer no kernel. Já na Slackware 9.0 tive que recompilar o kernel com suporte ao driver TUN/TAP. Também só usei em produção as distros citadas acima.

Baixe os pacotes lzo-1.08.tar.gz (biblioteca de compressão de dados) e o pacote openvpn-1.5.0.tar.gz.

**1º Passo**

```
$ tar -xzvf lzo-1.08.tar.gz
$ cd lzo-1.08
```

```
$ ./configure
$ make
$ su
# make install
```

**2º Passo**

```
$ tar -xzvf openvpn-1.5.0.tar.gz
$ cd openvpn-1.5.0
$ ./configure
$ make
$ su
# make install
```

Pronto. O *OpenVPN* já está instalado em nosso sistema com suporte à biblioteca de compressão de dados. Agora só resta a configuração de nossa VPN.

## Configuração da Matriz

Configurando nossa VPN na Matriz:

O OpenVPN pode operar com 3 tipos de criptografia. Nenhuma criptografia (apenas o túnel), criptografia com chaves estáticas e no modo TLS, em que as chaves são trocadas periodicamente. No nosso exemplo, usaremos criptografia com chaves estáticas.

1 - Execute os seguintes comandos:

**# mkdir /etc/openvpn**

Criamos o diretório onde estarão todos os arquivos de configuração.

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

Foi gerada uma chave de criptografia com o nome de chave (pode ser qualquer nome de arquivo) dentro do diretório /etc/openvpn.

**# cat /etc/openvpn/chave**

Só para visualizarmos o conteúdo da chave que geramos.

**# touch /etc/openvpn/matriz.conf**

Crie esse arquivo com o seguinte conteúdo:

```
# Usar como interface o driver TUN
dev tun
# 10.0.0.1 ip que será assumido na matriz
# 10.0.0.2 ip remoto, ou seja, esse será o ip da filial
ifconfig 10.0.0.1 10.0.0.2
# Entra no diretório onde se encontram os arquivos de configuração
cd /etc/openvpn
# Indica que esse túnel possui uma chave de criptografia
secret chave
# OpenVPN usa a porta 5000/UDP por padrão.
# Cada túnel do OpenVPN deve usar
# uma porta diferente.
# O padrão é a porta 5000
port 5000
# Usuário que rodará o daemon do OpenVPN
user nobody
# Grupo que rodará o daemon do OpenVPN
group nobody
Usa a biblioteca lzo
comp-lzo
# Envia um ping via UDP para a parte
# remota a cada 15 segundos para manter
# a conexão de pé em firewall statefull
# Muito recomendado, mesmo se você não usa
# um firewall baseado em statefull.
ping 15
# Nível de log
verb 3
```

Em seguida, vamos iniciar a conexão no servidor, faltando apenas configurar a filial. Execute o seguinte comando no servidor da Matriz:

**# openvpn --config /etc/openvpn/matriz.conf -daemon**
**# ifconfig tun0**

```
tun0      Link encap:Point-to-Point Protocol
          inet addr:10.0.0.1  P-t-P:10.0.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1255  Metric:1
          RX packets:1383257 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1144968 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:10
          RX bytes:82865921 (79.0 Mb)  TX bytes:383951667 (366.1 Mb)
```

Se aparecer algo assim ou parecido, o túnel na Matriz já está pronto e a espera da conexão da filial.

### Configuração da Filial

Configurando nossa VPN na Filial:

A parte da instalação na filial é exatamente igual a da Matriz, é só seguir os passos descritos no tópico instalação.

Já na parte de configuração, não muda muita coisa também, pois o maior trabalho é simplesmente copiar a chave que geramos na Matriz por um canal seguro até a filial. Execute os seguintes comandos. Criaremos o mesmo diretório de configuração na filial:

**# mkdir /etc/openvpn**

Copie a chave gerada na matriz para a filial com seguinte comando:

**# scp /etc/openvpn/chave ip_filial:/etc/openvpn**

Em seguida crie o arquivo de configuração chamado filial.conf:

**# touch /etc/openvpn/filial.conf**

Crie esse arquivo com o seguinte conteúdo:

```
# Usar como interface o driver TUN
dev tun
# 10.0.0.1 ip que será assumido na matriz
# 10.0.0.2 ip remoto, ou seja, esse será o ip da filial
ifconfig 10.0.0.2 10.0.0.1
# Indica onde está o ip da Matriz (essa é a única linha que acrescentamos
# no arquivo de configuração da filial), o resto é tudo igual.
remote 200.217.222.222
# Entra no diretório onde se encontram os arquivos de configuração
cd /etc/openvpn
# Indica que esse túnel possui uma chave de criptografia
secret chave
# OpenVPN usa a porta 5000/UDP por padrão.
# Cada túnel do OpenVPN deve usar
# uma porta diferente.
# O padrão é a porta 5000
port 5000
# Usuário que rodará o daemon do OpenVPN
user nobody
# Grupo que rodará o daemon do OpenVPN
group nobody
# Usa a biblioteca lzo
comp-lzo
# Envia um ping via UDP para a parte
# remota a cada 15 segundos para manter
# a conexão de pé em firewall statefull
# Muito recomendado, mesmo se você não usa
# um firewall baseado em statefull.
ping 15
# Nível de log
verb 3
```

Inicie a conexão na filial com o seguinte comando:

**# openvpn --config /etc/openvpn/filial.conf -daemon**

**# ifconfig tun0**

```
tun0      Link encap:Point-to-Point Protocol
          inet addr:10.0.0.2  P-t-P:10.0.0.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1255       Metric:1
          RX packets:1383257 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1144968 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:10
          RX bytes:82865921 (79.0 Mb)  TX bytes:383951667 (366.1 Mb)
```

Ok! Se aparecer algo assim, sua VPN, está de pé!!! Teste pingando de uma ponta a outra:

**# ping 10.0.0.1**
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=63 time=11.9 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=63 time=6.09 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=63 time=5.93 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=63 time=8.15 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=63 time=6.19 ms

Se aparecer algo assim, sua VPN já esta funcionando. Agora só falta adicionarmos as rotas para as redes internas se enxergarem.

**Adicionando rotas**

NOTA: Antes de adicionarmos as rotas, é necessário ativar o roteamento no kernel em ambas as pontas (Matriz e Filial). Execute os seguintes comandos na matriz e filial:

**# echo 1 > /proc/sys/net/ipv4/ip_forward**

Para adicionar a rota com destino a rede da Filial, execute de dentro do servidor da Matriz o seguinte comando:

**# route add -net 192.168.2.0/24 gw 10.0.0.2**

Para adicionar a rota com destino a rede da Matriz, execute de dentro do servidor da Filial o seguinte comando:

**# route add -net 192.168.1.0/24 gw 10.0.0.1**

Bom, agora é só testar. Tente pingar de dentro de uma máquina da LAN da Matriz com destino a LAN da Filial. Vale lembrar também que temos que colocar toda a seqüência de comandos acima no rc.local de sua distro, para que a mesma carregue as configurações ao iniciar o sistema operacional.

Para terminar, podemos também configurar um servidor WINS com o Samba ou Windows NT/2000 para que ambos os micros das duas redes internas sejam visualizados no Ambiente de Rede do Windows. Mas isso é assunto para um novo artigo.

Bom, no mais, espero que tenha colaborado para toda a comunidade Open Source.

Qualquer dúvida é só mandar um e-mail para guilherme@linesol.com.br que responderei a medida do possível.

Abraço à todos!!!!!!!!!!!!!!!!!!!

---