OpenVPN no Debian (Stable) com cliente Windows 2000 ou XP

Kairo Araújo <kairo@kairoaraujo.org>
Última Atualização: Thu Dec 2 14:34:49 2004

Este documento é uma Linux / Debian Notes de configuração de uma VPN utilizando o OpenVPN, e como clientes máquinas rodando Windows XP ou 2000. O Servidor está rodando em um Debian GNU/Linux STABLE (Woody)

Notas iniciais

1. NÃO EXISTEM GARANTIAS POR MINHA PARTE DO USO DESTE DOCUMENTO. Ele foi escrito sendo uma 'Linux Note' para uso pessoal, mas é livre para utilização seguindo a FDL.
2. Se alguma dúvida, algo acrescentar, doação ou reclamação, fique à vontade para me enviar um email kairo@kairoaraujo.org .

Atualizações

- 1.0
  - Primeira versão.

Instalando o OpenVPN e o OpenSSL

Editar o `/etc/apt/sources.list` e acescentar a seguinte linha:

```
# OpenVPN
deb http://www.backports.org/debian/ woody openvpn

# apt-get install openssl openvpn
```

.P.S.: Nas duas opções de configuração do OpenVPN, escolha sim. Caso não tenha escolhido, reconfigure utilizando o comando abaixo.

```
# dpkg-reconfigure openvpn
```

Configurando o OpenSSL para Autoridade Certificadora (CA)

Crie o diretório que vai armazenar os certificados:

```
# cd /etc/ssl
# mkdir certificados
```

Edite o arquivo `/etc/ssl/openssl.cnf` e modifique as seguintes linhas:

```
dir             = /etc/ssl/certificados # Where everything is kept

certificate     = $dir/my-ca.crt        # The CA certificate

private_key     = $dir/my-ca.key        # The private key
```

Crie os diretórios e arquivos necessários

```
# touch index.txt
# echo 01 > serial
# mkdir newcerts
```

Configurando o OpenVPN

Crie um link simbólico para os certificados dentro do diretório de configuração do OpenVPN.

```
# ln -s /etc/ssl/certificados /etc/openvpn/
```

Gerando as chaves da CA

```
# openssl req -nodes -new -x509 -keyout my-ca.key -out my-ca.crt
```

Preencha todos os campos. Opte por usar LETRAS MAIÚSCULAS.

```
# openssl dhparam -out dh.pem 1024
```

P.S.: O valor (aqui 1024) deve ser o correspondente ao usado no `/etc/ssl/openssl.conf` (ele pode ser 1024 ou 2048)

Configurando o Servidor OpenVPN para receber o cliente

Abaixo vamos usar como exemplo a criação do *cliente01*.

Criando as chaves para o cliente01

```
# cd /etc/ssl/certificados

# openssl req -nodes -new -keyout cliente01.key -out cliente01.csr
```

Preencha todos os camos com **excessão** do password deixando em branco. Lembre-se de Optar por LETRAS MAIúSCULAS

Agora assine as chaves e certificados.

```
# openssl ca -out cliente01.crt -in cliente01.csr
```

Dê yes (y) para as duas perguntas.

Configurando o Servidor OpenVPN para o Cliente01

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

Criando o Arquivo de configuração do Servidor

Crie o arquivo de configuração `/etc/openvpn/cliente01.conf` usando o exemplo abaixo.

```
# Exemplo de configuração do OpenVPN
# para a Matriz, usando o modo SSL/TLS e
# chaves RSA.
#
# '#' ou ';' são comentarios.
#
# Obs: Tradução livre do arquivo
# sample-config-files/tls-office.conf
# no diretorio de sources do OpenVPN.

# Usar como interface o driver tun.
dev tun

# 10.100.100.1 é o nosso IP local (matriz).
# 10.100.100.2 é o IP remoto (filial).
ifconfig 10.100.100.1 10.100.100.2

# Diretorio onde estão todas as configurações
cd /etc/openvpn

# O OpenVPN irá executar esse script
# quando o tunel estiver carregado.
# Ideal para setar as rotas
up ./cliente01.up

# No modo SSL/TLS a matriz irá
# assumir a parte do servidor,
# e a filial será o cliente.
tls-server

# Parametros Diffie-Hellman (apenas no servidor)
dh certificados/dh.pem

# Certificado da CA
ca certificados/my-ca.crt

# Certificado publico da Matriz
cert certificados/cliente01.crt

# Certificado privado da Matriz
key certificados/matriz.key

# OpenVPN usa a porta 5000/UDP por padrão.
# Cada tunel do OpenVPN deve usar
# uma porta diferente.
# O padrão é a porta 5000
port 5000

# Mudar UID e GID para
# "nobody" depois de iniciado
# para uma segurança exta.
; user nobody
; group nobody

# Envia um ping via UDP para a parte
# remota a cada 15 segundos para manter
# a coneção em firewall statefull
# Muito recomendado, mesmo se você não usa
```

```
# um firewall baseado em statefull.
ping 15

# Nivel dos logs.
# 0 -- silencioso, exeto por erros fatais.
# 1 -- quase silencioso, mas mostra erros não fatais da rede.
# 3 -- médio, ideal para uso no dia-a-dia
# 9 -- barulhento, ideal para solução de problemas
verb 3
```

Agora é preciso mais um arquivo, que irá conter as rotas. Sendo assim, crie o `/etc/openvpn/cliente01.up` utilizando o exemplo abaixo.

```
#!/bin/bash
route add -net 10.100.100.0 netmask 255.255.255.0 gw $5
route add -net IP_LAN_REMOTA netmask MASCARA_LAN_REMOTA gw $5
```

P.S.: Substitua o IP_LAN_REMOTA pelas informações.

Startando o Servidor OpenVPN

```
# /etc/init.d/openvpn restart
Stopping openvpn: .
Starting openvpn: cliente01.
```

Verificando:

```
# ifconfig tun0
tun0  Link encap:Point-to-Point Protocol
      inet addr:10.100.100.1  P-t-P:10.100.100.2  Mask:255.255.255.255
      UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:0 (0.0 b)  TX bytes:0 (0.0
```

Configurando o Cliente OpenVPN

Agora, estaremos criando as configurações que serão utilizadas pelo *cliente01*.

Criando os diretórios e arquivos necessários

```
# cd /etc/openvpn
# mkdir cliente01-files
# cd cliente01-files
# cp ../certificados/cliente01.key .
# cp ../certificados/cliente01.crt .
# cp ../certificados/dh.pem .
# cp ../certificados/my-ca.crt
```

Arquivo de configuração `cliente01.ovpn`:

```
# Exemplo de configuração do OpenVPN
# para a Filial, usando o modo SSL/TLS e
# chaves RSA.
#
# '#' ou ';' são comentarios.
#
# Obs: Tradução livre do arquivo
# sample-config-files/tls-office.conf
# no diretorio de sources do OpenVPN.

# Usar como interface o driver tun.
dev tun

# Ip da parte remota.
```

```
remote vpn.empresa.com.br

# 10.100.100.2 é o nosso IP local.
# 10.100.100.1 é o IP remoto (matriz).
ifconfig 10.100.100.2 10.100.100.1

# em vez de rodar um script para setar as rotas,
# vamos setar no arquivo de configuração.
route 10.100.100.0 255.0.0.0 10.100.100.1
route IP_REDE_REMOTO MASCARA 10.100.100.1

# No modo SSL/TLS a matriz irá
# assumir a parte do servidor,
# e a filial será o cliente.
tls-client

# Certificado da CA
ca my-ca.crt

# Certificado publico da Filial
cert cliente01.crt

# Certificado privado da Filial
key cliente01.key

# OpenVPN usa a porta 5000/UDP por padrão.
# Cada tunel do OpenVPN deve usar
# uma porta diferente.
# O padrão é a porta 5000
port 5000

# Envia um ping via UDP para a parte
# remota a cada 15 segundos para manter
# a coneção em firewall statefull
# Muito recomendado, mesmo se você não usa
# um firewall baseado em statefull.
ping 15

# Nivel dos logs.
# 0 -- silencioso, exeto por erros fatais.
# 1 -- quase silencioso, mas mostra erros não fatais da rede.
# 3 -- médio, ideal para uso no dia-a-dia
# 9 -- barulhento, ideal para solução de problemas
verb 3
```

Criando o ZIP para o Cliente01

```
# cd ..
# apt-get install zip
# zip -r cliente01.zip cliente01-files
```

Envie para a máquina (cliente01) o arquivo cliente01.zip

Instalando o Cliente e Rodando

Baixe o cliente do OpenVPN para Windows no link abaixo

http://prdownloads.sourceforge.net/openvpn/

Instale: Next, Next... até o Finish e reinicie quando solicitar.

Dentro do diretório em que foi instalado do OpenVPN (`Arquivos de programas\OpenVPN`), existe um diretório chamado `config`, descompacte o cliente01.zip dentro deste diretório. ATENÇÃO: Os arquivos devem ficar dentro do diretório config e não dentro de um sub-diretório!

Agora:

```
Iniciar > Executar > cmd

cd Arquivos de programas\OpenVPN\config
openvpn --config cliente01.ovpn
```

Criando um novo Cliente

Basta fazer novamente a partir do Item *Configurando o Servidor OpenVPN para receber o cliente* para um novo, mudando por exemplo para cliente01 e a rede para 10.100.101.1 e 10.100.101.2.

Fonte

Este documento, como mencionado é apenas um Linux Note que fiz para uso pessoal. Uma documentação completa e excelente, onde **toda** esta documentação foi baseada está em:
http://www.altoriopreto.com.br/artigo_vpn.php

Sendo assim, eu tenho que dizer: Obrigado Luiz Antonio Cassetari Vieira Filho <luiz!@altoriopreto.com.br>, pela excelente documentação que desenvolveu.