

## 1. Configurando uma VPN IPSec Openswan no SUSE Linux 9.3

### 1.1. Termos de Uso

#### Nota de Copyright

```
Copyright (c) 2007 Linux2Business.  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the GNU Free Documentation License, Version 1.2  
or any later version published by the Free Software Foundation;  
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover  
Texts. A copy of the license is included in the section entitled "GNU  
Free Documentation License".
```

O conteúdo textual deste documento está disponível sob a licença GNU FDL. Para maiores informações acesse <http://www.gnu.org/copyleft/fdl.html>. Os logotipos, marcas registradas e símbolos usados neste livro são de propriedade de seus respectivos proprietários.

### 1.2. Introdução

Neste artigo veremos como instalar e configurar uma VPN utilizando o IPSec e Openswan. A distribuição utilizada foi o SUSE Linux 9.3.

### 1.3. Conceito de VPN

VPN, *Virtual Private Network*, surgiu a partir da necessidade de utilizar redes de comunicação não confiáveis para trafegar informações de forma segura, por exemplo, interligar matriz e filial, parceiros de negócios ou qualquer outra situação que exija uma conexão segura por meios inseguros.

A VPN utiliza um padrão de criptografia mundial, estipulado por órgãos mundiais IETF, *Internet Engineering Task Force*. O grande objetivo da VPN é trafegar dados entre redes WAN de forma a criar um túnel, no qual possa manter as informações encriptadas. Também tem como objetivo melhorar o processo de segurança na rede, ao criar uma relação de confiança, deixando assim, cada gateway dependente de sua própria chave pública que é trafegada durante o processo de conexão.

A VPN baseia-se na tecnologia de tunelamento, onde essa técnica consiste em encapsular um protocolo dentro do outro. É importante registrar que, para estabelecer um túnel, é necessário que as duas extremidades utilizem o mesmo protocolo de tunelamento.

O tunelamento pode ocorrer na camada 2 ou 3, respectivamente enlace e rede. Os protocolos para tunelamento nível 2 são: PPTP (*Point-to-Point Tunneling Protocol*), L2TP (*Layer 2 Tunneling Protocol*) e L2F (*Layer 2 Forwarding*).

Para o tunelamento nível 3, temos o IPSec (*IP Security Tunnel Mode*), que permite que pacotes IP sejam criptografados e encapsulados com cabeçalho adicional desse mesmo protocolo para serem transportados numa rede IP pública ou privada.

O IPSec utiliza 3 protocolos: AH (*Authentication Header*), ESP (*Encapsulating Security Payload*) e IKE (*Internet Key Exchange*). É importante deixar registrado que todos os protocolos utilizam UDP e a porta 500. O protocolo AH tem o número 51 e o protocolo ESP tem o número 50.

**Obs.:** O IPSec não garante a segurança de usuários e nem das máquinas que estão na rede, a única coisa que ele faz é criptografar e garantir a segurança das informações que estão passando pelo túnel.

#### 1.4. Instalação

Para instalação dos pacotes, utilizaremos o YaST, através do comando apresentado abaixo:

```
# yast sw_single
```

O pacote que deve ser instalado é openswan, que apresenta como dependência o pacote ipsec-tools.

**Obs.:** Para instalação dos pacotes será preciso os CDs ou DVD de instalação do SUSE Linux 9.3. Se foram configuradas outras fontes de instalação que utilizem a internet, é necessário que o acesso a internet esteja disponível.

#### 1.5. Configuração

Os arquivos de configuração utilizados pelo IPSec são `ipsec.conf` e `ipsec.secrets`, localizados no diretório `/etc`. O arquivo `ipsec.conf` armazena as configurações gerais do IPSec e também as configurações das VPNs.

Antes de começar a configuração é sempre interessante manter uma cópia de segurança deste arquivo.

```
# cd /etc
# cp -p ipsec.conf ipsec.conf.default
# cp -p ipsec.secrets ipsec.secrets.default
```

A VPN criada interliga 2 servidores entre a matriz e a filial, conforme esquema abaixo:

```
Subnet1      <=>   Gateway1      (Internet)      Gateway2      <=>   Subnet2
192.168.172.0/24   200.153.247.71           200.153.247.70   192.168.173.0/24
```

A partir do arquivo original, vamos inserir alguns parâmetros e alterar outros, conforme apresentado abaixo:

```
# /etc/ipsec.conf - Openswan IPsec configuration file
# RCSID $Id: ipsec.conf.in,v 1.13 2004/03/24 04:14:39 ken Exp $

# This file: /usr/share/doc/packages/openswan/ipsec.conf-sample
#
```

```
# Manual:      ipsec.conf.5

version 2.0      # conforms to second version of ipsec.conf specification

# basic configuration
config setup
    # Debug-logging controls: "none" for none, "all" for lots.
    #klipsdebug=all
    #plutodebug="control parsing"
    #plutodebug=all
    # Certificate Revocation List handling
    #crlcheckinterval=600
    #strictcrlpolicy=yes
    # Change rp_filter setting, default = 0 (switch off)
    #rp_filter=%unchanged
    # Switch on NAT-Traversal (if patch is installed)
    #nat_traversal=yes

# default settings for connections
conn %default
    # Default: %forever (try forever)
    keyingtries=3
    # Sig keys (default: %dnsondemand)
    lefttrsasigkey=%cert
    righttrsasigkey=%cert
    # Lifetimes, defaults are 1h/8hrs
    #ikelifetime=20m
    #keylife=1h
    #rekeymargin=8m
    authby=rsasig

# Linux2Business VPN
conn matriz-filial
    # Left security gateway, subnet behind it, next hop toward
right.
    left=200.153.247.71
    leftsubnet=192.168.172.0/24
    # RSA 2048 bits
    lefttrsasigkey=0sAQOwK8vxtiHMURv...
    # Right security gateway, subnet behind it, next hop toward
left.
    right=200.153.247.70
    rightsubnet=192.168.173.0/24
    # RSA 2048 bits
    righttrsasigkey=0sAQOU3S8FUzrBtE...
    # To authorize this connection, but not actually start it, at
startup,
    # uncomment this.
    auto=start

#Disable Opportunistic Encryption
include /etc/ipsec.d/examples/no_oe.conf
```

**Obs.:** Não estarei entrando em detalhes sobre cada parâmetro da configuração, onde caso necessário existe uma boa documentação disponível no diretório `/usr/share/doc/packages/openswan`.

Este arquivo deve ser idêntico em ambos os lados da VPN, somente com o parâmetro `auto` diferente, onde no lado da matriz deixamos com o valor `add` e no lado da filial com o valor `start`.

Os parâmetros `leftrrsasigkey` e `rightrsasigkey` são conseguidos com o seguinte comando, sendo executado em cada lado da VPN:

```
# ipsec showhostkey --left
# RSA 2048 bits
leftrrsasigkey=0sAQOwK8vxtiHMURv...
```

ou

```
# ipsec showhostkey --right
# RSA 2048 bits
rightrsasigkey=0sAQOU3S8FUzrBtE...
```

Esta chave está disponível também no arquivo `ipsec.secrets`, onde é possível gerar uma nova chave RSA com o seguinte comando:

```
# ipsec newhostkey --output /etc/ipsec.secrets
```

Uma vez configurado, vamos iniciar os serviços em ambos os lados, através do comando:

```
# rcipsec start
```

É possível observar o que está acontecendo através do arquivo de log `/var/log/messages` ou através do comando:

```
# ipsec auto --status
```

Caso algum problema aconteça, é recomendado alterar os parâmetros `start`, em ambos os lados, para `add` e iniciar a comunicação da VPN manualmente. Sempre que o arquivo `ipsec.conf` for alterado é preciso reiniciar o serviço `ipsec`.

```
# rcipsec restart
# ipsec auto --up matriz-filial
```

Outros parâmetros do comando `ipsec` podem ser visualizados através do parâmetro `--help`:

```
# ipsec auto --help
```

## 1.6. Firewall para VPN

Veremos aqui apenas alguns pontos de como configurar um firewall para trabalhar com a VPN.

```
# Negociações do IKE
iptables -A INPUT -p udp --sport 500 --dport 500 -j ACCEPT
iptables -A OUTPUT -p udp --sport 500 --dport 500 -j ACCEPT
# ESP - Encriptação e Autenticação
iptables -A INPUT -p 50 -j ACCEPT
iptables -A OUTPUT -p 50 -j ACCEPT
# AH - Cabeçalho de Autenticação
iptables -A INPUT -p 51 -j ACCEPT
iptables -A OUTPUT -p 51 -j ACCEPT
```

## 1.7. Referências

- ✓ Openswan Home Page  
<http://www.openswan.org>
- ✓ Configurando uma VPN IPSec FreeSwan no Linux  
<http://www.secforum.com.br/article.php?sid=1033>
- ✓ Using a Linux L2TP/IPsec VPN server  
<http://www.jacco2.dds.nl/networking/freeswan-l2tp.html>
- ✓ Livro: Projeto de Segurança em Software Livre  
<http://www.temporeal.com.br/produtos.php?id=168378>
- ✓ Livro: Openswan: Building and Integrating Virtual Private Networks  
<http://www.temporeal.com.br/produtos.php?id=170211>