TechRepublic
Real World. Real Time. Real IT.
April 4, 2007

SolutionBase: Setting up a VPN server with OpenSWAN

by **Jack Wallen**

Linux can be the platform for almost any network service you might want to offer your organization's users. You can use it for file and printer sharing, or as a Web server, among other things.

One of the most popular network services needed in business is remote access for mobile users. Linux can answer that need as well; you just have to set up a VPN server using OpenSWAN. Here's how it works.

What's OpenSWAN?

OpenSWAN is an Open Source implementation of IPSec for the Linux OS; it's a code fork of the FreeS/WAN project, started by a few developers frustrated with the politics surrounding that project. OpenSWAN is, without question, the easiest of all the Linux VPN solutions to get operational; but that's not saying much, because the other solutions can be a nightmare. Fortunately, this article outlines a very simple method of getting a Linux-based VPN server up and running.

Installing OpenSWAN

Although I usually recommend installing by any method you prefer, I believe installing from the RPM is the best way, because the RPMs available contain the necessary patches to the system being installed upon. **NOTE:** On Fedora Core 5 and later, you do *not* have to patch the kernel for l2tp to work. Download the following:

- OpenSWAN
- OpenSWAN Docs
- l2tpd
- l2tpd Legacy PTY patch
- l2tpd SysV PTY patch
- l2tpd startup file

Create a new directory (we'll call this *vpnsource*) and move all of the downloaded files into that directory. Before you move on to installing the files, check to make sure you don't already have OpenSWAN installed. Run the command:

```
rpm -qa|grep openswan
```

If the above command returns anything, the package is not installed. Also run the command:

```
rpm -qa|grep ppp
```

to ensure you have PPP installed. Nearly all distributions come complete with PPP installed, so this shouldn't be a problem.

If your RPM query on OpenSWAN returns that you already have an installation on your system, remove it. You can do that with the command:

```
rpm -e openswan
```

Now we'll install the packages. From within the directory housing the files, run the commands:

```
rpm -ivhopenswan-XXX.rpm (where XXX is the release number)

rpm -ivhopenswan-doc-XXX.rpm (where XXX is the release number)
```

The installation of OpenSWAN comes with a sample IPSec configuration file. We're going to overwrite that with our own information, so back up that file with the following command:

```
cp /etc/ipsec.conf /etc/ipsec.conf_OLD
```

Now, open the */etc/ipsec.conf* file in your favorite text editor, delete all the information in it, and paste the following code into that file:

```
version 2.0

config setup

     interfaces=%defaultroute

     klipsdebug=none

     plutodebug=none

     overridemtu=1410

     nat_traversal=yes
```

```
      virtual_private=%v4:10.0.0.0/8,%v4:172.16.0.0/12,%v4:192.168.0.0/1
6

conn %default

      keyingtries=3

      compress=yes

      disablearrivalcheck=no

      authby=secret

      type=tunnel

      keyexchange=ike

ikelifetime=240m

      keylife=60m

conn roadwarrior-net

      leftsubnet=192.168.0.0/16

      also=roadwarrior

connroadwarrior-all

      leftsubnet=0.0.0.0/0

      also=roadwarrior

conn roadwarrior-l2tp

      leftprotoport=17/0

      rightprotoport=17/1701

      also=roadwarrior

conn roadwarrior-l2tp-updatedwin

      leftprotoport=17/1701

      rightprotoport=17/1701

      also=roadwarrior

connroadwarrior
```

```
      pfs=no

      left=XXX.XXX.XXX.XXX

      leftnexthop=YYY.YYY.YYY.YYY

      right=%any

      rightsubnet=vhost:%no,%priv

      auto=add

#Disable Opportunistic Encryption

include /etc/ipsec.d/examples/no_oe.conf
```

Author's Note:

This configuration file was cobbled together from various open sources. (No mice or penguins were harmed in its making.) Replace XXX.XXX.XXX.XXX with the external IP address. Also, replace YYY.YYY.YYY.YYY with your default gateway address.

Now, open */etc/ipsec.secrets* and add the following line:

```
150.150.150.150 %any: PSK "this_is_your_psk_key_phrase"
```

Change 150.150.150.150 to the external IP address.

If you want access to the network from anywhere on the Internet, keep *%any* intact. For security reasons, consider specifying the address of the machine connecting.

Make sure the PSK key phrase is long. This is the string users will have to enter to gain access; longer is better.

Installing l2tp

As I mentioned before, if you're running Fedora Core 5 or later, you will not have to patch the kernel for l2tp to work. All you need to do, as root, is run the command:

```
yum install l2tpd
```

If you are installing l2tp from source, you will need to download the l2tp source to */usr/local/src*. After that, run these commands:

```
cd /usr/local/src

tar zxf l2tpd-0.69.tar.gz
```

```
mv l2tpd-0.69.sysv.patch l2tpd-0.69/

mv l2tpd /etc/rc.d/init.d/

cd l2tpd-0.69

patch < l2tpd-0.69.sysv.patch

make

cp l2tpd /usr/sbin

chmod 755 /usr/sbin/l2tpd
```

l2tp should be properly installed.

Before you move on, it's best to take care of the start-up environment for l2tp by issuing the following commands:

```
chmod 755 /etc/rc.d/init.d/l2tpd

chkconfig --add l2tpd

chkconfig l2tpd on
```

Now it’s time to configure l2tp. The configuration files for l2tp will be located in */etc/l2tp*. If the installation didn't create this directory automatically (it should), create it.

Open */etc/l2tp/l2tp.conf* and add the following:

```
[global]

port = 1701

[lns default]

ip range = 192.168.1.101-192.168.1.254

local ip = 192.168.1.100

require chap = yes

refuse pap = yes

require authentication = yes

name = LinuxVPN

ppp debug = yes
```

```
pppoptfile = /etc/ppp/options.l2tpd

length bit = yes
```

The *ip range* configuration is the range of IP addresses that clients will be given when a connection is established. The *local ip* line is the server address. These lines can be configured to accommodate your network configuration.

PPP configuration

The VPN setup is almost done, but first configure PPP, because l2tp uses this to tunnel into the server. The l2tpd configuration we just edited specifies */etc/ppp/options.l2tpd* as *pppoptfile* (PPP options file). Create this file, and paste the following:

```
ipcp-accept-local

ipcp-accept-remote

ms-dns 192.168.1.2

ms-wins 192.168.1.3

noccp

auth

crtscts

idle 1800

mtu 1410

mru 1410

nodefaultroute

debug

lock

proxyarp

connect-delay 5000

silent
```

NOTE: Change *ms-dns* to your DNS server and *ms-wins* to your WINS server (if used.)

Now for the authentication files: CHAP will be used for PPP authentication. Open up */etc/ppp/chap-secrets* in your favorite text editor for configuration. The format of this file will be:

```
Client     server     secret     IP addresses
```

Here is an example:

```
# Secrets for authentication using CHAP

# client     server     secret         IP addresses

username     *          "password"     192.168.1.0/24

*            username   "password"     192.168.1.0/24
```

For each username, you will need two lines of configuration, because this is two-sided authentication. One line is from client-to-server; the other, server-to-client. Both IP addresses and password should be the same on both lines. The IP addresses configuration will be the range of IP addresses handed out to clients, so make sure this is configured correctly.

Start it up

The order of starting will be l2tp followed by OpenSWAN. First, run the command:

```
/etc/rc.d/init.d/l2tpd start
```

You should not receive any errors.

Next, fire up OpenSWAN with the command:

```
/etc/rc.d/init.d/ipsec start
```

If there are any errors they will be reported in */var/log/messages* and */var/log/secure*.

Now that you have OpenSWAN and l2tp up and running you will have to configure your firewall to route packets from your external to internal interfaces. In order to do this, Packet Forwarding must be switched on. To switch it on, open */etc/sysctl.conf* and change:

```
net.ipv4.ip_forward = 0
```

to

```
net.ipv4.ip_forward = 1
```

Make sure the UDP 500 and 4500 and TCP 4500 ports are all open. Without these ports open, your VPN will not allow traffic in.

If you use *iptables* as your firewall, add the following rules to the */etc/sysconfig/iptables* file:

```
-A RH-Firewall-1-INPUT -ippp+ -j ACCEPT

-A RH-Firewall-1-INPUT -i eth1 -j ACCEPT

-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 500 -
j ACCEPT

-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 4500
-j ACCEPT

-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 4500
-j ACCEPT
```

Client configuration

I assume most reading this article understand the particulars of setting up Windows clients to connect to a VPN. The only caveat to setting these connections up is remembering the PSK string used in the IPSec settings of the Windows VPN configuration (in Pre-shared Key Configuration.) Make sure you select L2TP IPSec VPN from the Type Of VPN setting. Finally, go to TCP/IP Settings | Advanced Settings | General and uncheck Use Default Gateway On Remote Network.

Instant, cheap, and reliable VPN service is now at your fingertips.

Final thoughts

VPNs are a tricky prospect. You can either go with the simple-but-costly solution with Microsoft or the complex-but-economical solution with OpenSWAN. Either way, you'll have challenges. So, before you plop down your IT department’s hard-earned budget on a proprietary solution, give OpenSWAN a try. You'll spend a little extra time with it in the beginning, but the payoff is worth not having to baby-sit your VPN server.