

20 October 2006

By: Marius Nestor, Linux Editor



## Shoreline Firewall Beginners Guide

### *Secure Your Linux Box!*

Iptables is an amazing software, it's every Linux box firewall, but sometimes it's hard for a beginner to learn how to set up Iptables and to remember all those configuration lines, so for this, there are many Iptables-based firewalls. One of them, and a very good one, is [Shoreline Firewall](#), more commonly known as "Shorewall". Shorewall is a high-level tool for configuring Netfilter. You describe your firewall/gateway requirements using entries in a set of configuration files. Shorewall reads those configuration files and with the help of the iptables utility, Shorewall configures Netfilter to match your requirements. Shorewall can be used on a dedicated firewall system, a multi-function gateway/router/server or on a standalone GNU/Linux system. **Installation:** Great, now that we know what Shorewall is and what it can do, let's install it. If you are on a Fedora machine, you can install it with yum. Open a console and type: `yum install shorewall` On a Debian machine, you can install it using apt. Open a console and type: `apt-get install shorewall` Or, of course, you can always install it from the source archive which you can download from [here](#). Once installed, Shorewall **can't** run until you configure it! That's what I'm gonna teach you in this guide.

**Configuration:NOTE:** The following configuration reefers to a Linux machine with a single public IP interface. To understand what each configuration file does, please read carefully every one of them, as they contain examples of usage. All the configuration files of Shorewall are stored in `/etc/shorewall` folder. Go there as you will need to edit some of the configuration files before Shorewall can start protecting your computer. **WARNING:** Debian users will find that the `/etc/shorewall` directory is empty. This is intentional. The released configuration file skeletons may be found on your system in the directory `/usr/share/doc/shorewall/default-config`. All you have to do is copy the files you need from that directory to `/etc/shorewall` and modify the copies. **Step 1 - Configuring Zones** Just open the file `/etc/shorewall/zones` and edit it as follows: **Step 2 - Configuring Policy** Open the file `/etc/shorewall/policy` and edit it as follows: The above policy will: 1. Allow all connection requests from the firewall to the internet; 2. Drop (ignore) all connection requests from the internet to your firewall; 3. Reject all other connection requests (Shorewall requires this catchall policy). **Step 3 - Configuring Interfaces** If your IP is dynamic, assigned by the DHCP server of your provider, edit the `/etc/shorewall/interfaces` file as follows: For a manually assigned IP address, that is a statical IP, just remove the "dhcp" option from the above example. **Step 4 - Starting Shorewall** Before you can start the firewall, you must enable startup by editing the `/etc/shorewall/shorewall.conf` file and set `STARTUP_ENABLED=No` option to "Yes", like this: `STARTUP_ENABLED=Yes` After you have enabled startup, Shorewall can be started very simple with the following command: `/etc/init.d/shorewall start` Have a look at our example to see that everything is fine and the Shorewall firewall has started successfully. **Rules examples:** You must understand that all the Shorewall rules can be configured in the `/etc/shorewall/rules` file. I will give you two short examples, to allow a BitTorrent client to access the internet: **Example 1** With this simple rule, I have allowed BitTorrent to use the 6971 port to connect to the torrent trackers. **Example 2** With this rule, I have allowed UDP connections via 6972 port for the Azureus client. **WARNING:** You must restart the firewall after every added rule, with the following command: `/etc/init.d/shorewall restart` **Credits:** All credits go to Thomas M. Eastep, the man who made Shoreline Firewall. You can download Shoreline Firewall now from [Softpedia](#).