

Contents

- 1 Shorewall provides a front-end to iptables.
- 2 Shorewall is a large application which handles the following Jobs:
- 3 Versions of Shorewall
- 4 Setup & Installation of Shorewall - Version 3.X
 - ◆ 4.1 Location of Default Shorewall Files
 - ◆ 4.2 Copy over and Edit Default Config files to /etc/shorewall/
 - ◆ 4.3 Copy over the required Macros to /etc/shorewall/
 - ◆ 4.4 Create a custom macro.Munin (if required)
 - ◆ 4.5 Final Config of /etc/shorewall/rules to Include macros
 - ◆ 4.6 Finally - Config Shorewall to start
- 5 Conclusion on Shorewall

Shorewall provides a front-end to iptables.

It allows configuration of iptables without knowing actual ports, but rather services running, such as Web, SSH, SVN etc. etc.

Shorewall is a large application which handles the following Jobs:

- Handle a single public IP address
- Standalone Linux System
- Two-interface Linux System acting as a firewall/router for a small local network.
- Three-interface Linux System acting as a firewall/router for a small local network and a DMZ.
- Handle Multiple Public IP addresses!!

Currently, we only want Shorewall to cater for a **Standalone Linux System**.

The Shorewall website <http://www.shorewall.net> provides excellent and definitive guides and how-to's on each of the points/jobs listed above!

Versions of Shorewall

There are currently two versions of Shorewall: 2.X and 3.X and there are different guides for each.

Debian Sarge as on 22nd Oct, 2006 uses version 2.X

Debian Etch(testing) as on 22nd Oct, 2006 uses version 3.X

The setup guides for each of the above versions are available on the main <http://www.shorewall.net> website - and should be taken from there directly. Click on the **Documentation** link in the left menu.

Setup & Installation of Shorewall - Version 3.X

```
apt-get install shorewall
```

The above installs the latest version of shorewall depending on whether you are running Debian Sarge or Debian Etch (testing). Due to the compulsory configuration required, debian disables the startup of Shorewall in `/etc/default/shorewall` (startup=0) on purpose. Only when Shorewall is configured - should the above file be enabled (startup=1).

The direct link to the shorewall how-to for **Standalone Linux System** is available at:
<http://www.shorewall.net/standalone.htm>

Location of Default Shorewall Files

`/usr/share/doc/shorewall/default-config` = Default Config Files for Shorewall.
`/usr/share/shorewall` = Default macros & rules for Shorewall.

Copy over and Edit Default Config files to `/etc/shorewall/`

Following the how-to guide on the main shorewall website (<http://www.shorewall.net/standalone.htm>)

```
#1. - Copy over the modules file (as described in how-to)
cp /usr/share/doc/shorewall/default-config/modules /etc/shorewall/
#2. - Copy over the zones file and enter the 2 zones - the internet (ipv4 and the firewall)
cp /usr/share/doc/shorewall/default-config/zones /etc/shorewall/
uncomment the following two lines:
    fw      firewall
    net     ipv4
comment in if required (make sure there is only 1 line {fw      firewall}):
    #fw     firewall
#3. - Copy over the default policy. (This default policy is the same as setting the main iptables po
cp /usr/share/doc/shorewall/default-config/policy /etc/shorewall/
uncomment (or include):
    $FW          net          ACCEPT
    net          all          DROP          info
    all          all          REJECT         info
#4. - Copy over and include the default interface
cp /usr/share/doc/shorewall/default-config/interfaces /etc/shorewall/
uncomment (include):
    net     eth0    136.201.192.144
#5. - Copy over the rules file which will be edited later.
cp /usr/share/doc/shorewall/default-config/rules /etc/shorewall/
```

Copy over the required Macros to `/etc/shorewall/`

```
cp /usr/share/shorewall/macro.service /etc/shorewall/
```

What are macros?

Macros are where Service based Firewall rules are made. These macros are then used inside the `/etc/shorewall/rules` file eliminating the need for several entries and port numbers. The macro.Web (for the web service) is:

Shorewall_Firewall

```
# Shorewall version 3.0 - Web Macro
#
# /usr/share/shorewall/macro.Web
#
#       This macro handles WWW traffic (secure and insecure).
#
#####
#ACTION SOURCE  DEST      PROTO  DEST   SOURCE  ORIGINAL      RATE  USER/
#              PORT      PORT(S) DEST   DEST           LIMIT  GROUP
PARAM  -        -        tcp    80
PARAM  -        -        tcp    443
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Once this macro.Web is copied to /etc/shorewall/ it is used by calling the following line inside /etc/shorewall/rules

```
Web/ACCEPT net          $FW
```

Create a custom macro.Munin (if required)

Because munin-node (statistics) uses port 4949, Shorewall does not have a pre-existing macro. A simple one can be created in /etc/shorewall/macro.Munin having the following config:

```
# Shorewall version 3.0 - Munin Macro
#
#       This macro handles Munin traffic.
#
#####
#ACTION SOURCE  DEST      PROTO  DEST   SOURCE  ORIGINAL      RATE  USER/
#              PORT      PORT(S) DEST   DEST           LIMIT  GROUP
PARAM  -        -        tcp    4949
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Final Config of /etc/shorewall/rules to Include macros

As per following the instructions on www.shorewall.net the macros are added in after: SECTION NEW

```
#####
#ACTION SOURCE          DEST      PROTO  DEST   SOURCE  ORIGINAL      RATE  USER/
#              PORT      PORT(S) DEST   DEST           LIMIT  GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
Web/ACCEPT net          $FW
SSH/ACCEPT net          $FW
AllowICMPs/ACCEPT net  $FW
Ping/ACCEPT net         $FW
SNMP/ACCEPT net         $FW
Munin/ACCEPT net        $FW
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Finally - Config Shorewall to start

```
vi /etc/default/shorewall
#change startup=0 to startup=1
```

Copy over the required Macros to /etc/shorewall/

Conclusion on Shorewall

Shorewall similar to other applications (e.g. apache), tries to keep various config files seperated out for easy management (instead of in one huge config). Shorewall keeps seperate configs for services (in macro files). Should a service change requirements - only the macro requires editing.

More Info:

http://www.besy.co.uk/projects/debian/sarge_mail_server_howto.htm