CS 482: Selected Topics in Information Security
Spring 2005 – Section 1

Shorewall Tutorial

What is Shorewall?

Shorewall is a high-level tool for configuring Netfilter on Linux machines. You configure the firewall using configuration files that allow you to set the interfaces that are on the machine, the policies that apply to the interfaces, and the exceptions to the policy in the form of rules to use when a request is sent to the interfaces. Shorewall configures Netfilter using the instructions in the configuration files with the help of the iptables utility. Shorewall can be used on a dedicated firewall system, a multi-function gateway/router/server, or on a standalone GNU/Linux system. Shorewall does not use Netfilter's ipchains compatibility mode and can thus take advantage of Netfilter's connection state tracking capabilities. (shorewall.net)

Shorewall is not a daemon. Once Shorewall has configured Netfilter, it's job is complete and there is no “Shorewall process” left running in your system. The /sbin/shorewall program can be used at any time to monitor the Netfilter firewall. (shorewall.net)

Words to Know

- Netfilter allows the root user to define a set of rules on how the system should deal with network packets. Netfilter is a set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack. (netfilter.org)
- Iptables is a tool used to configure netfilter tables. Iptables is a generic table structure for the definition of rulesets. Each rule within an IP table consists out of a number of classifiers (iptables matches) and one connected action (iptables target). (netfilter.org)

  You can use netfilter and iptables to…[1]

  - build internet firewalls based on stateless and stateful packet filtering

[1] http://www.netfilter.org/

Stateles packet filtering (or static packet filtering) tracks packets based on the inforamation in its header (contains information about where the packets came from and is going).

Stateful packet filtering (or dynamic packet filtering) works at the network layer of the OSI model; the filtering process tracks and validates each connection going through the firewall's interfaces.

- use NAT and masquerading for sharing internet access if you don't have enough public IP addresses

Network Setup

The Topology Diagram was used to setup the Shorewall firewall on Linux-FW. A copy can be found on Blackboard (blackboard.jmu.edu).

Pre-installation Check

Iproute is a set of tools that is used to control networking behavior. To verify that iproute is installed on the Linux machine by issuing the command **which ip**.
You should get as a result **/sbin/ip**. If not, install iproute on the computer *(There are no steps in this documentation on how to install the iproute package on the Linux Firewall machine)*. Iproute's rpm can be downloaded from http://rpmfind.com at http://rpmfind.net/linux/rpm2html/search.php?query=iproute.

How to Install Shorewall

There are two ways to install shorewall, you can either untar a tarred file and place the uncompressed directory structure into the system's directory structured as listed below or you can install the package using an rpm that automatically installs the necessary files and folders for you.

Using a Tarred File

- Copy the file **shorewall-lrp-2.1.11.tgz** into a folder
- At the Terminal Command Line **cd** to the folder that contains the compressed file
- Issue the command **tar -xzf shorewall-lrp-2.1.11.tgz** at the terminal window
- Copy the uncompressed directory structure to the same directory structure on the system

Unzipped File To Copy – Source	**To System File – Final Destination**
…/shorewall/etc/init.d/ Copy the file **shorewall** in the folder	/etc/init.d/
…/shorewall/etc/shorewall/ Copy the folder **shorewall** with 28 items	/etc/shorewall/
…/shorewall/sbin/ Copy the file **shorewall**	/sbin/
…/shorewall/usr/share/shorewall	/usr/share/shorewall

Copy the **shorewall** folder with 37 items	
…/shorewall/var/lib/lrpkg Copy the folder **lrpkg** with 5 items	/var/lib/lrpkg
…/shorewall/var/lib/shorewall Copy the folder **shorewall** with 0 items	/var/lib/shorewall

Using an rpm

To run the rpm and have the installation files installed in their respective directories, issue the command **rpm –ivh shorewall-2.2.1-1.noarch.rpm.** The value of "1:shorewall" will go to 100%, which signifies that the installation is complete.

The rpm installed the following files and directory when it is complete:

/etc/init.d/shorewall
/etc/shorewall/
/usr/share/shorewall/

```
[root@Linux-FW shorewall]# rpm -ivh shorewall-2.2.1-1.noarch.rpm
Preparing...                ########################################### [100%]
   1:shorewall              ########################################### [100%]
[root@Linux-FW shorewall]#
```

Shorewall with Example

The following sections contain information about making changes to five configuration files in Shorewall and they include the zones, interfaces, policy, rules, and shorewall.conf files. The configuration files for Shorewall are contained in the directory **/etc/shorewall/**. In the example setup we will only deal with the **zones, interfaces, policy, rules, and shorewall.conf** files.

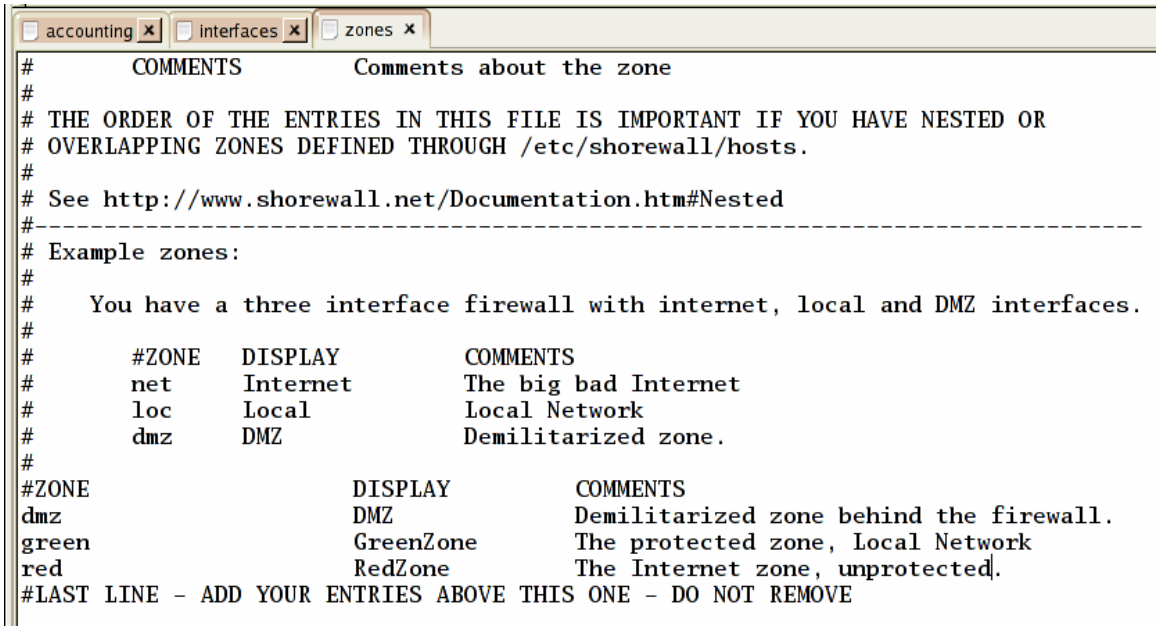
Shorewall views the network where it is running as being composed of *zones*. The information that follows is based on the configuration used on the Linux-FW virual machine in a lab setting. On Host-01 of the team's business network the Linux-FW is composed of three interfaces, which have been grouped into the following zones.

Name	Description
red	The Internet – NIC3 (or eth2) connected to the 10.0.10.0/24
green	Your Local Network – NIC2 (or eth1) connected to the local subnet 192.168.[n].160/27
dmz	Demilitarized Zone – NIC1 (or eth0) connected to 192.168.[n].32/27

The files mentioned below are snippets of code, The configuration files in /etc/shorewall should be view in their entirety for better understanding. Configure Shorewall using the following steps 1 to 5 in order.

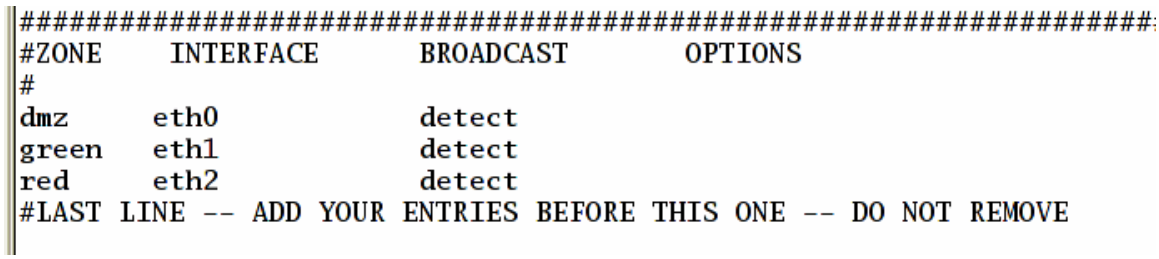
Step 1: Modify the Zones File

Shorewall zones are defined in the **/etc/shorewall/zones** file. The Shorewall firewall system is itself in a zone call **fw**; the **fw** zone is not defined in the zones file. The zone definition in the file matches the previously defined logical network separation.



Step 2: Modify the Interfaces File

Information about the interfaces and the zones that should be associated with each interface are defined in **/etc/shorewall/interfaces.** The following snippet contains the three interfaces defined in the file along with the NIC cards that they are associated with.



From the **/etc/shorewall/interfaces** file:

- the red zone interfaces with eth2 (also called NIC3),
- green zone is associated with eth1 (also called NIC2) and
- and the dmz zone interfaces with eth0 (also called NIC1).

Shorewall will detect broadcast addresses for the subnetwork when **detect** is written in the Broadcast column. The network interfaces must be up for Shorewall to detect the broadcast address when you start Shorewall. You can

also hard code the subnet mask as shown in the following example:

```
###############################################################################
#ZONE    INTERFACE       BROADCAST       OPTIONS
#
dmz     eth0            192.168.100.63
green   eth1            192.168.100.191
red     eth2            10.0.10.255
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Hard coding the broadcast address is not recommended for the simple reason that when you change the network interfaces you will have to change the broadcast address in the **interfaces** files.

Step 3: Modify the Policy File

The **/etc/shorewall/policy** file is used to configure how connections between each zone is to be handled. When new packets are received, Shorewall first checks the rules file (**/etc/shorewall/rules**). If there is no rule for that match the connection request in the rules file the policy file is then check from top to bottom until a match is found. Shorewall rules override whatever is placed in the policy document. As soon as a match is found in either the rules or policy files the associated policy is applied to the packet and no other checks is performed in either files. For example, in the policy file all traffic coming from green to fw are rejected with the Reject keyword. However, in the rules file we have specified that ICMP requests coming from green zone to the fw should be accepted.

For example, the policy for each combination of connection is REJECT because for testing purposes it was necessary to see “port/host unreachable” ICMP messages. With the DROP policy no error message is sent to the requesting machine, the request simply times out. We configured one policy for each possible zone request combinations. This is a very strict and restrictive policy, but also the most secure for our purposes.

```
###############################################################################
#SOURCE         DEST            POLICY          LOG             LIMIT:BURST
#                                               LEVEL
#dmz            fw              REJECT          info
#dmz            green           REJECT          info
#dmz            red             REJECT          info

green           fw              REJECT          info
#green          red             REJECT          info
#green          dmz             REJECT          info

#red            fw              REJECT          info
#red            green           REJECT          info
#red            dmz             REJECT          info

#fw             green           REJECT          info
#fw             red             REJECT          info
#fw             dmz             REJECT          info

all             all             DROP            warning
#LAST LINE -- DO NOT REMOVE
```

The **/etc/shorewall/policy** file states the following:

1. Reject any traffic connection going from the dmz zone to the red zone, firewall and the green zone. Log informational syslog level messages.

```
###############################################################################
#SOURCE         DEST            POLICY          LOG             LIMIT:BURST
#                                               LEVEL
dmz             fw              REJECT          info
dmz             green           REJECT          info
dmz             red             REJECT          info
```

2. Reject any traffic going from the green zone to the firewall, red zone, and the dmz. Log informational syslog level messages.

```
###############################################################################
#SOURCE         DEST            POLICY          LOG             LIMIT:BURST
#                                               LEVEL
green           fw              REJECT          info
green           red             REJECT          info
green           dmz             REJECT          info
```

3. Reject connection requests coming from the red zone to the firewall, green zone, and dmz. Also log informational syslog level messages.

```
###############################################################################
#SOURCE         DEST            POLICY          LOG             LIMIT:BURST
#                                               LEVEL
red             fw              REJECT          info
red             green           REJECT          info
red             dmz             REJECT          info
```

4. Reject connections request from the firewall to the red, green, and dmz zones. Log syslog level information messages.

```
###############################################################################
#SOURCE         DEST            POLICY          LOG             LIMIT:BURST
#                                               LEVEL
fw              green           REJECT          info
fw              red             REJECT          info
fw              dmz             REJECT          info
```

5. And as a default policy, DROP all connections requests between all the zones. Log syslog level warning messages.

```
###############################################################################
#SOURCE         DEST            POLICY          LOG             LIMIT:BURST
#                                               LEVEL
all             all             DROP            warning
```

Step 4: Modify the Rules File

Exceptions to the policy file are placed in the **/etc/shorewall/rules** file. Specifying a port number for each connection further restricts access to the protected network and would make it difficult for outside intruders to come in. *Not all available options are highlighted in this document, refer to the file for further information.*

A template of the format of the rules:

ACTION: how the traffic is handled, do you want to reject, accept, or drop traffic?

SOURCE: what host does the rule apply to? You can use as options the zone name, the zone name with a colon and the IP address of the host in the zone, the zone and the subnet, the zone and a comma separated list, the zone and the MAC address of the computer or the zone and a range of IP address.

DEST: who is receiving this traffic that the rule should apply to? Possible options: zone name

PROTO: what protocol should be use.

DEST PORT(S): what port on the remote machine should the traffic go to?

ACTION	SOURCE	DEST	PROTO	DEST PORT(S)
ACCEPT, DROP, REJECT, DNAT, DNAT-, REDIRECT, CONTINUE, LOG, QUEUE	dmz, fw, loc, net, loc:ipaddr loc:ipaddr/mask fw:~mac net:ipaddrrange dmz:ipaddr,ipaddr	dmz, fw, loc, net	tcp, udp, icmp, all	Port Range: low:high number

```
#############################################################################################################
#ACTION  SOURCE          DEST            PROTO   DEST    SOURCE     ORIGINAL     RATE            USER/
#                                                PORT    PORT(S)    DEST         LIMIT           GROUP

#Test 1
REJECT:info red         green           tcp
REJECT:info red         dmz             tcp

#Test 2
REJECT  green           dmz             tcp
ACCEPT  green           red             tcp

#Test 3
REJECT  dmz             fw

#Test 4
ACCEPT  green           dmz
REJECT  green           red
```

Test 1 states that all tcp packets from the red zone to the green or dmz zone should be rejected and the traffic should be log as informational.

Test 2 states that all tcp packets from the green zone to the dmz should be rejected while traffic from the green zone to the red zone should be accepted.

Test 3 states that all packets from the dmz and the fw should be dropped.

Test 4 states that all packets from the green zone to the dmz should be rejected while packets from the green zone to the red zone should be accepted.

Step 5: Shorewall Configuration File

Before starting shorewall, the **/etc/shorewall/shorewall.conf** file needs to be modified. The file should be used to setup different parameters. Not every

information from the conf file is included, only settings that pertained to our network are hightled.

```
#                       S T A R T U P   E N A B L E D
##############################################################################
# Once you have configured Shorewall, you may change the setting of
# this variable to 'Yes'

#CHANGED
STARTUP_ENABLED=Yes
```

Change STARTUP_ENABLED=Yes in order to be able to run the program. This option prevents Shorewall from being run accidentally.

```
# CHANGED
LOGRATE=10/hour
LOGBURST=4

#
# LOG ALL NEW
#
# This option should only be used when you are trying to analyze a problem.
# It causes all packets in the Netfilter NEW state to be logged as the
# first rule in each builtin chain. To use this option, set LOGALLNEW to
# the log level that you want these packets logged at (e.g.,
# LOGALLNEW=debug).
#

# CHANGED
LOGALLNEW=info
```

The LOGRATE is the number of seconds/minutes before a packet is logged after the first packet has been logged. If the value was 10/minute then Shorewall will log the packet and (60/10) 6 seconds later it will log the next connection request packet and so on. LOGBURST is the number of packets that will be logged and in this case it will be the first 4 packets of each connection request.

All the other options come with a default value that can be changed as necessary.

Start Using Shorewall

- Issue the **shorewall version** command at the terminal window.

  You should get **2.1.11**

- If you receive a you have mail message open and read it with **gedit /var/spool/mail/root**. The file contains error messages that was encountered, what was successful and what was not.

- Before starting shorewall, first create a log file in **/var/log** by going to **Main | Accessories | Text Edtor**. Save the blank file as **shorewall.log** into **/var/log**/.

- Issue the command **shorewall check** which will check the files for dependencies and validates all the configuration files. If you first issue the command before

configuring Shorewall you will get an error message:

```
Validating rules file…
   Error: No policy defined from zone fw to zone net
```

Configure your firewall first using steps 1 to 5 and then use the **check** command. Run **shorewall check** at the terminal. If Shorewall was able to process the entire configuration in the policy, rules, interfaces, and zones file you will received a "Configuration Validated" message.

You can now start Shorewall with **shorewall start**. Whenever changes are made to any of the configuration files you need restart Shorewall with **shorewall restart**. Shorewall can be stopped with **shorewall stop**.

To have Shorewall started automatically when the system boots up, issue the command **chkconfig shorewall on**. To disable automatic boot-up of shorewall enter the command **chkconfig shorewall off**.

Things to Keep in Mind

- Pinging the IP address of eth2 does not mean that you are communicating with the machines in the net zone. Any traffic that you generate from the local network will be associated with your local interface and will be treated as green to fw traffic. (shorewall.net)
- It is a mistake to believe that your firewall is able to forward packets just because you can ping the IP address of all of the firewall's interfaces from the local network. The only conclusion you can draw from such pinging success is that the link between the local system and the firewall works and that you probably have the local system's default gateway set correctly (shorewall.net)
- Check that you can access other resources (this includes http, telnet, and ftp) on the machines through their open ports not just pinging.

Works Cited

Eastep, M Thomas. "Shoreline Firewall". 2005. 3 Jan. 2005 <http://www.shorewall.net/>.

Welte, Harald. "Netfilter/iptables project homepage – The netfilter/iptables project." 2004. 3 Jan. 2005 <http://www.netfilter.org/>.