Shorewall Logging

Tom Eastep

2004-12-27

Table of Contents

How to Log Traffic Through a Shorewall Firewall

The disposition of packets entering a Shorewall firewall is determined by one of a number of Shorewall facilities. Only some of these facilities permit logging.

1. The packet is part of an established connecection. The packet is accepted and cannot be logged.
2. The packet represents a connection request that is related to an established connection (such as a data connection associated with an FTP control connection). These packets also cannot be logged.
3. The packet is rejected because of an option in /etc/shorewall/shorewall.conf or /etc/shorewall/interfaces. These packets can be logged by setting the appropriate logging-related option in /etc/shorewall/shorewall.conf.
4. The packet matches a rule in /etc/shorewall/rules. By including a syslog level (see below) in the ACTION column of a rule (e.g., "ACCEPT**:info** net fw tcp 22"), the connection attempt will be logged at that level.

5. The packet doesn't match a rule so it is handled by a policy defined in /etc/shorewall/policy. These may be logged by specifying a syslog level in the LOG LEVEL column of the policy's entry (e.g., “loc net ACCEPT **info**”).

Where the Traffic is Logged and How to Change the Destination

By default, Shorewall directs NetFilter to log using syslog (8). Syslog classifies log messages by a *facility* and a *priority* (using the notation *facility.priority*).

The facilities defined by syslog are *auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp* and *local0* through *local7.*

Throughout the Shorewall documentation, I will use the term *level* rather than *priority* since *level* is the term used by NetFilter. The syslog documentation uses the term *priority*.

Syslog Levels

Syslog levels are a method of describing to syslog (8) the importance of a message. A number of Shorewall parameters have a syslog level as their value.

Valid levels are:

7 - **debug** (Debug-level messages)
6 - **info** (Informational)
5 - **notice** (Normal but significant Condition)
4 - **warning** (Warning Condition)
3 - **err** (Error Condition)
2 - **crit** (Critical Conditions)
1 - **alert** (must be handled immediately)
0 - **emerg** (System is unusable)

For most Shorewall logging, a level of 6 (info) is appropriate. Shorewall log messages are generated by NetFilter and are logged using the *kern* facility and the level that you specify. If you are unsure of the level to choose, 6 (info) is a safe bet. You may specify levels by name or by number.

Syslogd writes log messages to files (typically in /var/log/*) based on their facility and level. The mapping of these facility/level pairs to log files is done in /etc/syslog.conf (5). If you make changes to this file, you must restart syslogd before the changes can take effect.

Syslog may also write to your system console. See Shorewall FAQ 16 for ways to avoid having

Shorewall messages written to the console.

Configuring a Separate Log for Shorewall Messages (ulogd)

There are a couple of limitations to syslogd-based logging:

1. If you give, for example, kern.info it's own log destination then that destination will also receive all kernel messages of levels 5 (notice) through 0 (emerg).
2. All kernel.info messages will go to that destination and not just those from NetFilter.

Beginning with Shorewall version 1.3.12, if your kernel has ULOG target support (and most vendor-supplied kernels do), you may also specify a log level of ULOG (must be all caps). When ULOG is used, Shorewall will direct netfilter to log the related messages via the ULOG target which will send them to a process called “ulogd”. The ulogd program is included in most distributions and is also available from http://www.gnumonks.org/projects/ulogd. Ulogd can be configured to log all Shorewall messages to their own log file.

Note

The ULOG logging mechanism is completely separate from syslog. Once you switch to ULOG, the settings in /etc/syslog.conf have absolutely no effect on your Shorewall logging (except for Shorewall status messages which still go to syslog).

Once you have installed ulogd, edit /etc/ulogd.conf (`/usr/local/etc/ulogd.conf` if you built ulogd yourself) and set:

1. syslogfile <*the file that you wish to log to*>
2. syslogsync 1

Also on the firewall system:

touch <*the file that you wish to log to*>

Your distribution's ulogd package may include a logrotate file in /etc/logrotate.d. If you change the log file location, be sure to change that logrotate file accordingly.

You will need to change all instances of log levels (usually “info”) in your Shorewall configuration files to “ULOG” - this includes entries in the policy, rules and shorewall.conf files. Here's what I have:

```
[root@gateway shorewall]# grep LOG * | grep -v ^\#
params:LOG=ULOG
policy:loc fw  REJECT $LOG
policy:net all DROP   $LOG    10/sec:40
policy:all all REJECT $LOG
rules:REJECT:$LOG loc net tcp 6667
shorewall.conf:TCP_FLAGS_LOG_LEVEL=$LOG
shorewall.conf:RFC1918_LOG_LEVEL=$LOG
[root@gateway shorewall]#
```

Finally edit /etc/shorewall/shorewall.conf and set LOGFILE=<*file that you wish to log to*>. This tells the /sbin/shorewall program where to look for the log when processing its “show log”, “logwatch” and “monitor” commands.

Syslog-ng

Here is a post describing configuring syslog-ng to work with Shorewall.

Understanding the Contents of Shorewall Log Messages

For general information on the contents of Netfilter log messages, see http://logi.cc/linux/netfilter-log-format.php3.

For Shorewall-specific information, see FAQ #17.