Shorewall Traffic Accounting

Tom Eastep

2004-04-19

Shorewall Traffic Accounting support was added in Shorewall release 1.4.7.

Shorewall accounting rules are described in the file /etc/shorewall/accounting. By default, the accounting rules are placed in a chain called "accounting" and can thus be displayed using "shorewall show accounting". All traffic passing into, out of or through the firewall traverses the accounting chain including traffic that will later be rejected by interface options such as "tcpflags" and "maclist". If your kernel doesn't support the connection tracking match extension (Kernel 2.4.21) then some traffic rejected under "norfc1918" will not traverse the accounting chain.

The columns in the accounting file are as follows:

- **ACTION** - What to do when a match is found. Possible values are:
  - COUNT- Simply count the match and continue trying to match the packet with the following accounting rules
  - DONE- Count the match and don't attempt to match any following accounting rules.
  - <*chain*> - The name of a chain to jump to. Shorewall will create the chain automatically. If the name of the chain is followed by ":COUNT" then a COUNT rule matching this rule will automatically be added to <chain>. Chain names must start with a letter, must be composed of letters and digits, and may contain underscores ("_") and periods ("."). Beginning with Shorewall version 1.4.8, chain names man also contain embedded dashes ("-") and are not required to start with a letter.
- **CHAIN** - The name of the chain where the accounting rule is to be added. If empty or "-" then the "accounting" chain is assumed.
- **SOURCE** - Packet Source. The name of an interface, an address (host or net) or an interface name followed by ":" and a host or net address.
- **DESTINATION** - Packet Destination Format the same as the SOURCE column.
- **PROTOCOL** - A protocol name (from `/etc/protocols`), a protocol number or "ipp2p". For "ipp2p", your kernel and iptables must have ipp2p match support from Netfilter Patch_o_matic_ng.
- **DEST PORT** - Destination Port number. Service name from `/etc/services` or port number. May only be specified if the protocol is TCP or UDP (6 or 17). If the PROTOCOL is "ipp2p", then this column is interpreted as an ipp2p option without the leading "--" (default "ipp2p"). For a list of value ipp2p options, as root type **iptables -m ipp2p --help**.
- **SOURCE PORT**- Source Port number. Service name from /etc/services or port number. May only be specified if the protocol is TCP or UDP (6 or 17).
- **USER/GROUP** (Added in Shorewall 2.2.0) - This column may only be non-empty if the CHAIN is OUTPUT. The column may contain:

  ```
  [!][<user name or number>][:<group name or number>]
  ```

  When this column is non-empty, the rule applies only if the program generating the output is running under the effective <user> and/or <group> specified (or is NOT running under that id if "!" is given).

  Examples:

  joe #program must be run by joe

  :kids #program must be run by a member of the 'kids' group.

  !:kids #program must not be run by a member of the 'kids' group

In all columns except ACTION and CHAIN, the values "-","any" and "all" are treated as wild-cards.

The accounting rules are evaluated in the Netfilter "filter" table. This is the same environment where the "rules" file rules are evaluated and in this environment, DNAT has already occurred in inbound packets and SNAT has not yet occurred on outbound ones.

Accounting rules are not stateful -- each rule only handles traffic in one direction. For example, if eth0 is your internet interface and you have a web server in your DMZ connected to eth1 then to count HTTP traffic in both directions requires two rules:

```
#ACTION CHAIN   SOURCE  DESTINATION     PROTOCOL        DEST            SOURCE
#                                                       PORT            PORT
DONE    -       eth0    eth1            tcp             80
DONE    -       eth1    eth0            tcp             -               80
```

Associating a counter with a chain allows for nice reporting. For example:

```
#ACTION         CHAIN   SOURCE  DESTINATION     PROTOCOL        DEST            SOURCE
#                                                               PORT            PORT
web:COUNT       -       eth0    eth1            tcp             80
web:COUNT       -       eth1    eth0            tcp             -               80
web:COUNT       -       eth0    eth1            tcp             443
web:COUNT       -       eth1    eth0            tcp             -               443
DONE            web
```

Now “shorewall show web” will give you a breakdown of your web traffic:

```
[root@gateway shorewall]# shorewall show web
Shorewall-1.4.6-20030821 Chain web at gateway.shorewall.net - Wed Aug 20 09:48:56 PDT 2003

Counters reset Wed Aug 20 09:48:00 PDT 2003

Chain web (4 references)
pkts bytes target     prot opt in     out     source               destination
  11  1335            tcp  --  eth0   eth1    0.0.0.0/0            0.0.0.0/0          tcp dpt:80
  18  1962            tcp  --  eth1   eth0    0.0.0.0/0            0.0.0.0/0          tcp spt:80
   0     0            tcp  --  eth0   eth1    0.0.0.0/0            0.0.0.0/0          tcp dpt:443
   0     0            tcp  --  eth1   eth0    0.0.0.0/0            0.0.0.0/0          tcp spt:443
  29  3297 RETURN     all  --  *      *       0.0.0.0/0            0.0.0.0/0
  [root@gateway shorewall]#
```

Here is a slightly different example:

```
#ACTION         CHAIN   SOURCE  DESTINATION     PROTOCOL        DEST            SOURCE
#                                                               PORT            PORT
web             -       eth0    eth1            tcp             80
web             -       eth1    eth0            tcp             -               80
web             -       eth0    eth1            tcp             443
web             -       eth1    eth0            tcp             -               443
COUNT           web     eth0    eth1
COUNT           web     eth1    eth0
```

Now “shorewall show web” simply gives you a breakdown by input and output:

```
[root@gateway shorewall]# shorewall show accounting web
Shorewall-1.4.6-20030821 Chains accounting web at gateway.shorewall.net - Wed Aug 20 10:27:21 PDT 2003

Counters reset Wed Aug 20 10:24:33 PDT 2003

Chain accounting (3 references)
    pkts bytes target     prot opt in     out     source               destination
    8767  727K web        tcp  --  eth0   eth1    0.0.0.0/0            0.0.0.0/0          tcp dpt:80
       0     0 web        tcp  --  eth0   eth1    0.0.0.0/0            0.0.0.0/0          tcp dpt:443
   11506   13M web        tcp  --  eth1   eth0    0.0.0.0/0            0.0.0.0/0          tcp spt:80
       0     0 web        tcp  --  eth1   eth0    0.0.0.0/0            0.0.0.0/0          tcp spt:443

Chain web (4 references)
    pkts bytes target     prot opt in     out     source               destination
    8767  727K            all  --  eth0   eth1    0.0.0.0/0            0.0.0.0/0
   11506   13M            all  --  eth1   eth0    0.0.0.0/0            0.0.0.0/0
[root@gateway shorewall]#
```

Here's how the same example would be constructed on an HTTP server with only one interface (eth0).

Caution

READ THE ABOVE CAREFULLY -- IT SAYS **SERVER**. If you want to account for web browsing, you have to reverse the rules below.

```
#ACTION         CHAIN   SOURCE  DESTINATION     PROTOCOL        DEST            SOURCE
#                                                               PORT            PORT
web             -       eth0    -               tcp             80
web             -       -       eth0            tcp             -               80
web             -       eth0    -               tcp             443
web             -       -       eth0            tcp             -               443
COUNT           web     eth0
COUNT           web     -       eth0
```

Note that with only one interface, only the SOURCE (for input rules) or the DESTINATION (for output rules) is specified in each rule.

Here's the output:

```
[root@mail shorewall]# shorewall show accounting web Shorewall-1.4.7
Chains accounting web at mail.shorewall.net - Sun Oct 12 10:27:21 PDT 2003

Counters reset Sat Oct 11 08:12:57 PDT 2003

Chain accounting (3 references)
 pkts bytes target     prot opt in     out     source               destination
 8767  727K web        tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0          tcp dpt:80
11506   13M web        tcp  --  *      eth0    0.0.0.0/0            0.0.0.0/0          tcp spt:80
    0     0 web        tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0          tcp dpt:443
    0     0 web        tcp  --  *      eth0    0.0.0.0/0            0.0.0.0/0          tcp spt:443

Chain web (4 references)
 pkts bytes target     prot opt in     out     source               destination
 8767  727K            all  --  eth0   *       0.0.0.0/0            0.0.0.0/0
11506   13M            all  --  *      eth0    0.0.0.0/0            0.0.0.0/0
[root@mail shorewall]#
```

For an example of integrating Shorewall Accounting with MRTG, see http://www.nightbrawler.com/code/shorewall-stats/.