NAME

ipfstat - reports on packet filter statistics and filter list

SYNOPSIS

ipfstat [**-46aAdfghIilnoRsv**]
ipfstat -t [**-6C**] [**-D** <addrport>] [**-P** <protocol>] [**-S** <addrport>] [**-T** <refresh time>]

DESCRIPTION

ipfstat examines /dev/kmem using the symbols **_fr_flags**, **_frstats**, **_filterin**, and **_filterout**. To run and work, it needs to be able to read both /dev/kmem and the kernel itself. The kernel name defaults to **/boot/kernel/kernel**.

The default behaviour of **ipfstat** is to retrieve and display the accumulated statistics which have been accumulated over time as the kernel has put packets through the filter.

OPTIONS

-4 Display filter lists and states for IPv4, if available. This is the default when displaying states. **-4** and **-6** is the default when displaying lists.

-6 Display filter lists and states for IPv6, if available.

-a Display the accounting filter list and show bytes counted against each rule.

-A Display packet authentication statistics.

-C This option is only valid in combination with **-t**. Display "closed" states as well in the top. Normally, a TCP connection is not displayed when it reaches the CLOSE_WAIT protocol state. With this option enabled, all state entries are displayed.

-d Produce debugging output when displaying data.

-D <addrport>
This option is only valid in combination with **-t**. Limit the state top display to show only state entries whose destination IP address and port match the addrport argument. The addrport specification is of the form ipaddress[,port]. The ipaddress and port should be either numerical or the string "any" (specifying any IP address resp. any port). If the **-D** option is not specified, it defaults to "**-D** any,any".

-f Show fragment state information (statistics) and held state information (in the kernel) if any is present.

-g Show groups currently configured (both active and inactive).

-h Show per-rule the number of times each one scores a "hit".

-i Display the filter list used for the input side of the kernel IP processing.

-I Swap between retrieving "inactive"/"active" filter list details. For use in combination with **-i**.

-n Show the "rule number" for each rule as it is printed.

-o Display the filter list used for the output side of the kernel IP processing.

-P <protocol>
This option is only valid in combination with **-t**. Limit the state top display to show only state entries that match a specific protocol. The argument can be a protocol name (as defined in **/etc/protocols**) or a protocol number. If this option is not specified, state entries for any protocol are specified.

-R Don't try to resolve addresses to hostnames and ports to services while printing statistics.

-s Show packet/flow state information (statistics only).

-sl Show held state information (in the kernel) if any is present (no statistics).

-S <addrport>
This option is only valid in combination with **-t**. Limit the state top display to show only state entries whose source IP address and port match the addrport argument. The addrport specification is of the form ipaddress[,port]. The ipaddress and port should be either numerical or the string "any" (specifying any IP address resp. any port). If the **-S** option is not specified, it defaults to "**-S** any,any".

-t Show the state table in a way similar to the way **top(1)** shows the process table. States can be sorted using a number of different ways. This option requires **curses(3)** and needs to be compiled in. It may not be available on all operating systems. See below, for more information on the keys that can be used while ipfstat is in top mode.

-T <refreshtime>
This option is only valid in combination with **-t**. Specifies how often the state top display should be updated. The refresh time is the number of seconds between an update. Any positive integer can be used. The default (and minimal update time) is 1.

-v Turn verbose mode on. Displays more debugging information. When used with either **-i** or **-o**, counters associated with the rule, such as the number of times it has been matched and the number of bytes from such packets is displayed. For "keep state" rules, a count of the number of state sessions active against the rule is also displayed.

SYNOPSIS

The role of **ipfstat** is to display current kernel statistics gathered as a result of applying the filters in place (if any) to packets going in and out of the kernel. This is the default operation when no command line parameters are present.

When supplied with either **-i** or **-o**, it will retrieve and display the appropriate list of filter rules currently installed and in use by the kernel.

One of the statistics that **ipfstat** shows is **ticks**. This number indicates how long the filter has been enabled. The number is incremented every half-second.

STATE TOP

Using the **-t** option **ipfstat** will enter the state top mode. In this mode the state table is displayed similar to the way **top** displays the process table. The **-C**, **-D**, **-P**, **-S** and **-T** command line options can be used to restrict the state entries that will be shown and to specify the frequency of display updates.

In state top mode, the following keys can be used to influence the displayed information:

b show packets/bytes from backward direction.

f show packets/bytes from forward direction. (default)

l redraw the screen.

q quit the program.

s switch between different sorting criterion.

r reverse the sorting criterion.

States can be sorted by protocol number, by number of IP packets, by number of bytes and by time-to-live of the state entry. The default is to sort by the number of bytes. States are sorted in descending order, but you can use the **r** key to sort them in ascending order.

STATE TOP LIMITATIONS

It is currently not possible to interactively change the source, destination and protocol filters or the refresh frequency. This must be done from the command line.

The screen must have at least 80 columns. This is however not checked. When running state top in IPv6 mode, the screen must be much wider to display the very long IPv6 addresses.

Only the first X-5 entries that match the sort and filter criteria are displayed (where X is the number of rows on the display. The only way to see more entries is to resize the screen.

FILES

/dev/kmem
/dev/ipl
/dev/ipstate
/kernel

SEE ALSO

ipf(8)

BUGS

-4 and **-6** are only valid with **-i**, **-o**, and **-t**. An error should result when used with other arguments.