

NAME

`ipfstat` - user level front-end to examine the ipfil kernel module

SYNOPSIS

```
ipfstat [-afhIiosv] [-d device]
```

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 `/bsd`.

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

The following command line options can be used:

- a Display the accounting filter list and show bytes counted against each rule. Must be accompanied by either `-i` or `-o`.
- d *device*
Use a *device* other than `/dev/ip1` for interfacing with the kernel.
- f Show fragment state information (statistics) and held state information (in the kernel) if any is present.
- h Show per-rule the number of times each one scores a “hit”. For use in combination with `-i` or `-o`.
- 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` or `-o`.
- o Display the filter list used for the output side of the kernel IP processing.
- s Show packet/flow state information (statistics) and held state information (in the kernel) if any is present.
- v Turn verbose mode on. Displays more debugging information.

TUNIX NOTES

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

EXAMPLES

The output of `ipfstat` without arguments might look like this:

```
# ./ipfstat
input packets:          blocked 159336 passed 2160500 nomatch 0 counted 0
output packets:        blocked 0 passed 2100369 nomatch 0 counted 0
input packets logged:  blocked 38 passed 0
output packets logged: blocked 0 passed 0
packets logged:        input 0 output 0
log failures:          input 0 output 0
fragment state(in):    kept 0 lost 0
fragment state(out):   kept 0 lost 0
packet state(in):      kept 0 lost 0
packet state(out):     kept 0 lost 0
ICMP replies: 0        TCP RSTs sent: 0
Result cache hits(in): 0          (out): 0
Packet log flags set: (0)
                    none
```

FILES

/dev/ipl

The interface (driver) of the ipfil module in the kernel.

/bsd

The UNIX kernel.

SEE ALSO

ipf(1), ipf(7), ipmon(8).

BUGS

Please report bugs to fwsupport@tunix.nl.

AUTHOR

Copyright 1993, 1994, 1995 by Darren Reed.

VERSION

Version \$Revision: 1.6 \$ \$Date: 2003/05/16 13:54:13 \$ (\$Name: IPF_01 \$)