

NAME

`ipf` - user level front-end to manipulate the `ipfil` kernel module

SYNOPSIS

```
ipf [-AEDIsnovdr] [-l { block|pass|nomatch }] [-F { i|o|a }]
    -f filename [-f filename] ...
```

DESCRIPTION

`Ipf` opens the *filenames* listed (treating “-” as standard input) and parses the file for a set of rules which are to be added or removed from the packet filter rule set.

Each rule processed by `ipf` is added to the kernel's internal lists if there are no parsing problems. Rules are added to the end of the internal lists, matching the order in which they appear when given to `ipf`.

The following command line options are recognized:

- A set the list to make changes to the active list (default).
- E Enable the filter (if disabled). Not effective for loadable kernel versions.
- D Disable the filter (if enabled). Not effective for loadable kernel versions.
- F { i|o|a }
This option specifies which filter list to flush. The parameter should either be “i” (input), “o” (output) or “a” (remove all filter rules). Either a single letter or an entire word starting with the appropriate letter maybe used. This option maybe before, or after, any other with the order on the command line being that used to execute options.
- d Turn debug mode on. Causes a hexdump of filter rules to be generated as it processes each one.
- f *filename*
This option specifies which *filename(s)* `ipf` should use to get input from for modifying the pack filter rule lists.
- I Set the list to make changes to the inactive list.
- l { block|pass|nomatch }
Use of the `-l` flag toggles default logging of packets. Valid arguments to this option are `pass`, `block` and `nomatch`. When an option is set, any packet which exits filtering and matches the set category is logged. This is most useful for causing all packets which don't

match any of the loaded rules to be logged.

- n This flag (no-change) prevents `ipf` from actually making any `ioctl` calls or doing anything which would alter the currently running kernel.
- o Force rules by default to be added/deleted to/from the output list, rather than the (default) input list.
- s Swap the active filter list in use to be the “other” one.
- r Remove matching filter rules rather than add them to the internal lists.
- v Turn verbose mode on. Displays information relating to rule processing.

TUNIX NOTES

Using a specific syntax in the filter set (which was not described), it is possible to add, delete or change individual lines in a filter set. We do not recommend to do so, because it is rather error prone.

Instead of that we advise to change the filter set in a file - using an editor - and after that swapping the contents of the active filter with the filter set in the file. Swapping is done by first downloading a new filter set in the “inactive” filter in the kernel and after that exchanging the active and inactive kernel filter with the following sequence of commands:

```
ipf -I -F a          # flush inactive list in kernel
ipf -I -f ipf.rules # load new filter set from file ipf.rules
ipf -s              # swap active and inactive
```

Local extensions or modifications to the generated `ipfil` ruleset can be made with the file `/usr/local/config/config.ipfextra`. Automatic generation of the ruleset can be disabled by creating a custom ruleset in the file `/usr/local/config/config.ipf`. Making your own ruleset or modifying the generated ruleset requires a profound knowledge of packet filtering techniques and the `ipfil` ruleset syntax.

FILES

`/etc/ipf.rules`

The (generated) ipfilter ruleset lives here.

`/usr/local/config/config.ipfextra`

Local additions and/or modifications to the generated ruleset.

`/usr/local/config/config.ipf`

Custom made ruleset.

SEE ALSO

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

BUGS

Please report bugs to fwsupport@tunix.nl.

AUTHOR

Copyright 1993, 1994, 1995 by Darren Reed.

VERSION

Version \$Revision: 1.7 \$ \$Date: 2003/05/16 13:54:13 \$ (\$Name: IPF_01 \$)