NAME

pflogd - packet filter logging daemon

SYNOPSIS

pflogd [**-Dx**] [**-d** *delay*] [**-f** *filename*] [**-i** *interface*] [**-s** *snaplen*] [*expression*]

DESCRIPTION

pflogd is a background daemon which reads packets logged by pf(4) to a pflog(4) interface, normally *pflog0*, and writes the packets to a logfile (normally */var/log/pflog*) in tcpdump(1) binary format. These logs can be reviewed later using the **-r** option of tcpdump(1), hopefully offline in case there are bugs in the packet parsing code of tcpdump(1).

pflogd closes and then re-opens the log file when it receives SIGHUP, permitting newsyslog(8) to rotate logfiles automatically. SIGALRM causes **pflogd** to flush the current logfile buffers to the disk, thus making the most recent logs available. The buffers are also flushed every *delay* seconds.

If the log file contains data after a restart or a SIGHUP, new logs are appended to the existing file. If the existing log file was created with a different snaplen, **pflogd** temporarily uses the old snaplen to keep the log file consistent.

pflogd tries to preserve the integrity of the log file against I/O errors. Furthermore, integrity of an existing log file is verified before appending. If there is an invalid log file or an I/O error, the log file is moved out of the way and a new one is created. If a new file cannot be created, logging is suspended until a SIGHUP or a SIGALRM is received.

pflogd will also log the pcap statistics for the pflog(4) interface to syslog when a SIGUSR1 is received.

The options are as follows:

-D Debugging mode. **pflogd** does not disassociate from the controlling terminal.

-d *delay*
Time in seconds to delay between automatic flushes of the file. This may be specified with a value between 5 and 3600 seconds. If not specified, the default is 60 seconds.

-f *filename*
Log output filename. Default is */var/log/pflog*.

-i *interface*
Specifies the pflog(4) interface to use. By default, **pflogd** will use *pflog0*.

-p *pidfile*

Writes a file containing the process ID of the program to */var/run*. The file name has the form <*pidfile*>.pid. The default is *pflogd*.

-s *snaplen*

Analyze at most the first *snaplen* bytes of data from each packet rather than the default of 116. The default of 116 is adequate for IP, ICMP, TCP, and UDP headers but may truncate protocol information for other protocols. Other file parsers may desire a higher snaplen.

-x Check the integrity of an existing log file, and return.

expression

Selects which packets will be dumped, using the regular language of tcpdump(1).

FILES

/var/run/pflogd.pid	Process ID of the currently running **pflogd**.
/var/log/pflog	Default log file.

EXAMPLES

Log specific tcp packets to a different log file with a large snaplen (useful with a log-all rule to dump complete sessions):

```
# pflogd -s 1600 -f suspicious.log port 80 and host evilhost
```

Log from another pflog(4) interface, excluding specific packets:

```
# pflogd -i pflog3 -f network3.log "not (tcp and port 23)"
```

Display binary logs:

```
# tcpdump -n -e -ttt -r /var/log/pflog
```

Display the logs in real time (this does not interfere with the operation of **pflogd**):

```
# tcpdump -n -e -ttt -i pflog0
```

Tcpdump has been extended to be able to filter on the pfloghdr structure defined in <*net/if_pflog.h*>. Tcpdump can restrict the output to packets logged on a specified interface, a rule number, a reason, a direction, an IP family or an action.

ip	Address family equals IPv4.
ip6	Address family equals IPv6.
ifname kue0	Interface name equals "kue0".
on kue0	Interface name equals "kue0".
ruleset authpf	Ruleset name equals "authpf".
rulenum 10	Rule number equals 10.
reason match	Reason equals match. Also accepts "bad-offset", "fragment", "bad-timestamp", "short", "normalize", "memory", "congestion", "ip-option", "proto-cksum", "state-mismatch", "state-insert", "state-limit", "src-limit", and "synproxy".
action pass	Action equals pass. Also accepts "block".
inbound	The direction was inbound.
outbound	The direction was outbound.

Display the logs in real time of inbound packets that were blocked on the wi0 interface:

```
# tcpdump -n -e -ttt -i pflog0 inbound and action block and on wi0
```

SEE ALSO

pcap(3), pf(4), pflog(4), pf.conf(5), newsyslog(8), tcpdump(1)

HISTORY

The **pflogd** command appeared in OpenBSD 3.0.

AUTHORS

pflogd was written by Can Erkin Acar <canacar@openbsd.org>.