NAME

pfil, **pfil_head_register**, **pfil_head_unregister**, **pfil_link**, **pfil_run_hooks** - packet filter interface

SYNOPSIS

#include <sys/param.h>
#include <sys/mbuf.h>
#include <net/pfil.h>

pfil_head_t
pfil_head_register(*struct pfil_head_args *args*);

void
pfil_head_unregister(*struct pfil_head_t *head*);

pfil_hook_t
pfil_add_hook(*struct pfil_hook_args* *);

void
pfil_remove_hook(*pfil_hook_t*);

int
pfil_link(*struct pfil_link_args *args*);

int
pfil_run_hooks(*phil_head_t *, pfil_packet_t, struct ifnet *, int, struct inpcb* *);

DESCRIPTION

The **pfil** framework allows for a specified function or a list of functions to be invoked for every incoming or outgoing packet for a particular network I/O stream. These hooks may be used to implement a firewall or perform packet transformations.

Packet filtering points, for historical reasons named *heads*, are registered with **pfil_head_register**(). The function is supplied with special versioned *struct pfil_head_args* structure that specifies type and features of the head as well as human readable name. If the filtering point to be ever destroyed, the subsystem that created it must unregister it with call to **pfil_head_unregister**().

Packet filtering systems may register arbitrary number of filters, for historical reasons named *hooks*. To register a new hook **pfil_add_hook**() with special versioned *struct pfil_hook_args* structure is called. The structure specifies type and features of the hook, pointer to the actual filtering function and user readable name of the filtering module and ruleset name. Later hooks can be removed with

pfil_remove_hook() functions.

To connect existing *hook* to an existing *head* function **pfil_link**() shall be used. The function is supplied with versioned *struct pfil_link_args* structure that specifies either literal names of hook and head or pointers to them. Typically **pfil_link**() is called by filtering modules to autoregister their default ruleset and default filtering points. It also serves on the kernel side of ioctl(2) when user changes **pfil** configuration with help of pfilctl(8) utility.

For every packet traveling through a *head* the latter shall invoke **pfil_run_hooks**(). The function can accept either *struct mbuf* * pointer or a *void* * pointer and length. In case if a hooked filtering module cannot understand *void* * pointer **pfil** will provide it with a fake one. All calls to **pfil_run_hooks**() are performed in network epoch(9).

HEADS (filtering points)

By default kernel creates the following heads:

inet IPv4 packets.

inet6 IPv6 packets.

ethernet Link-layer packets.

Default rulesets are automatically linked to these heads to preserve historical behaviour.

SEE ALSO

ipfilter(4), ipfw(4), pf(4), pfilctl(8)

HISTORY

The **pfil** interface first appeared in NetBSD 1.3. The **pfil** interface was imported into FreeBSD 5.2. In FreeBSD 13.0 the interface was significantly rewritten.