NAME

pflog - packet filter logging interface

SYNOPSIS

device pflog

DESCRIPTION

The **pflog** interface is a device which makes visible all packets logged by the packet filter, pf(4). Logged packets can easily be monitored in real time by invoking tcpdump(1) on the **pflog** interface, or stored to disk using pflogd(8).

The pflog0 interface is created when the **pflog** module is loaded; further instances can be created using ifconfig(8). The **pflog** module is loaded automatically if both pf(4) and pflogd(8) are enabled.

Each packet retrieved on this interface has a header associated with it of length PFLOG_HDRLEN. This header documents the address family, interface name, rule number, reason, action, and direction of the packet that was logged. This structure, defined in <*net/if_pflog.h*> looks like

```
struct pfloghdr {
        u_int8_t   length;
        sa_family_t        af;
        u_int8_t   action;
        u_int8_t   reason;
        char               ifname[IFNAMSIZ];
        char               ruleset[PF_RULESET_NAME_SIZE];
        u_int32_t rulenr;
        u_int32_t subrulenr;
        uid_t              uid;
        pid_t              pid;
        uid_t              rule_uid;
        pid_t              rule_pid;
        u_int8_t   dir;
        u_int8_t   pad[3];
        u_int32_t ridentifier;
};
```

EXAMPLES

Create a **pflog** interface and monitor all packets logged on it:

```
# ifconfig pflog create
```

```
pflog1
# ifconfig pflog1 up
# tcpdump -n -e -ttt -i pflog1
```

SEE ALSO

tcpdump(1), inet(4), inet6(4), netintro(4), pf(4), ifconfig(8), pflogd(8)

HISTORY

The **pflog** device first appeared in OpenBSD 3.0.

BUGS

FreeBSD does not set a process id in the *pid* field in pfloghdr.