NAME

    ipfwpcap - copy diverted packets to a file in tcpdump format

SYNOPSIS

    ipfwpcap [**-dr**] [**-b** *maxbytes*] [**-p** *maxpkts*] [**-P** *pidfile*] *portnum dumpfile*

DESCRIPTION

    The **ipfwpcap** utility is used to copy diverted packets to a file in tcpdump(1) format. The interesting
    packets are diverted by ipfw(8) to a port on which **ipfwpcap** listens. The packets are then dropped
    unless **-r** is used.

    The options are as follows:

    -d   Turns on extra debugging messages.

    -r   Writes packets back to the divert(4) socket.

    -rr   Indicates that it is okay to quit if *maxbytes* or *maxpkts* are reached. Diverted packets will
          silently disappear if nothing is listening on the divert(4) socket.

    -b *maxbytes*
          Stop dumping after *maxbytes* bytes.

    -p *maxpkts*
          Stop dumping after *maxpkt* packets.

    -P *pidfile*
          File to store PID number in. Default is */var/run/ipwfpcap.portnr.pid*.

    The *portnum* argument specifies which divert(4) socket port to listen on. The *dumpfile* argument is the
    path to the file to write captured packets to. Specify '**-**' to write to stdout.

EXIT STATUS

    The **ipfwpcap** utility exits 0 on success, and >0 if an error occurs.

EXAMPLES

        ipfwpcap -r 8091 divt.log &

    Starts **ipfwpcap** as a background job listening to port 8091 and reflecting the packets back to the socket.

    ipfw add 2864 divert 8091 ip from 192.0.2.101

Example ipfw(8) rule to divert all packets from 192.0.2.101 to port 8091. See ipfw(8) for details.

SEE ALSO
   tcpdump(1), pcap(3), divert(4), ipfw(8)

HISTORY
   The **ipfwpcap** utility first appeared in FreeBSD 7.0.

AUTHORS
   ipfwpcap was written by P. Kern *<pkern@cns.utoronto.ca>*. This manual page was written by Niclas
   Zeising *<zeising@FreeBSD.org>*.