NAME

netfuzzlog — Netfuzz Log Interface

SYNOPSIS

device netfuzzlog

DESCRIPTION

The **netfuzzlog** interface is a pseudo-device which makes visible all packets modified by netfuzz(4). The packets are logged before and after it is modified. Logged packets can easily be monitored in real time by invoking tcpdump(8) on the **netfuzzlog** interface.

Each packet retrieved on this interface has a header associated with it of length NETFUZZLOG_HDRLEN. This header documents the interface name, rule number, log type, and probability.

This structure, defined in <netfuzz/if_netfuzzlog.h> looks like

```
struct netfuzzloghdr {
    u_int8_t    length;
    u_int32_t   netfuzz_seq;
    u_int8_t    logtype;
    u_int32_t   rule_id;
    char        ifname[IFNAMSIZ];
    u_int32_t   probability;
    u_int8_t    pad[2];
}__attribute__((__aligned__(4)));
```

The value of logtype determines the memory layout after the initial header.

NETFUZZLOG_TYPE_FUZZED
: A following header documents a fuzzed packet before its modification and what function that was used to modify the packet.

  This structure, defined in ⟨netfuzz/if_netfuzzlog.h⟩ looks like

```
struct netfuzzlog_fuzzhdr {
    u_int32_t   offset_start;
    u_int32_t   offset_end;
    u_int32_t   rule_id;
    u_int32_t   count;
    u_int8_t    origpacket[NETFUZZ_MTU_MAX];
    u_int32_t   origlen;
} __attribute__((__aligned__(4)));
```

NETFUZZLOG_TYPE_DROPPED
: The appended packet was dropped

NETFUZZLOG_TYPE_DUPED
: The appended packet was duplicated

NETFUZZLOG_TYPE_TCPKILL
: The appended RST packet was sent to terminate a TCP session

EXAMPLES

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

```
# ifconfig netfuzzlog0 create
# ifconfig netfuzzlog0 up
```

```
# tcpdump -vv -e -n -tttt -i netfuzzlog0
```

SEE ALSO

inet(4), inet6(4), netintro(4), netfuzz(4), ifconfig(8), tcpdump(8)

HISTORY

This is the second generation of the network fuzzing suite of programs that was first implemented as a kernel patch on OpenBSD

AUTHORS