

NAME

mac_ifoff - interface silencing policy

SYNOPSIS

To compile the interface silencing policy into your kernel, place the following lines in your kernel configuration file:

```
options MAC
options MAC_IFOFF
```

Alternately, to load the interface silencing policy module at boot time, place the following line in your kernel configuration file:

```
options MAC
```

and in loader.conf(5):

```
mac_ifoff_load="YES"
```

DESCRIPTION

The **mac_ifoff** interface silencing module allows administrators to enable and disable incoming and outgoing data flow on system network interfaces via the sysctl(8) interface.

To disable network traffic over the loopback (lo(4)) interface, set the sysctl(8) OID *security.mac.ifoff.lo_enabled* to 0 (default 1).

To enable network traffic over other interfaces, set the sysctl(8) OID *security.mac.ifoff.other_enabled* to 1 (default 0).

To allow BPF traffic to be received, even while other traffic is disabled, set the sysctl(8) OID *security.mac.ifoff.bpfrecv_enabled* to 1 (default 0).

Label Format

No labels are defined.

SEE ALSO

mac(4), mac_bsdextended(4), mac_lomac(4), mac_mls(4), mac_none(4), mac_partition(4), mac_portacl(4), mac_seeotheruids(4), mac_test(4), mac(9)

HISTORY

The **mac_ifoff** policy module first appeared in FreeBSD 5.0 and was developed by the TrustedBSD Project.

AUTHORS

This software was contributed to the FreeBSD Project by Network Associates Labs, the Security Research Division of Network Associates Inc. under DARPA/SPAWAR contract N66001-01-C-8035 ("CBOSS"), as part of the DARPA CHATS research program.

BUGS

While the MAC Framework design is intended to support the containment of the root user, not all attack channels are currently protected by entry point checks. As such, MAC Framework policies should not be relied on, in isolation, to protect against a malicious privileged user.