NAME

mac_partition **-** process partition policy

SYNOPSIS

To compile the process partition policy into your kernel, place the following lines in your kernel configuration file:

```
options MAC
options MAC_PARTITION
```

Alternately, to load the process partition module at boot time, place the following line in your kernel configuration file:

```
options MAC
```

and in loader.conf(5):

```
mac_partition_load="YES"
```

DESCRIPTION

The **mac_partition** policy module implements a process partition policy, which allows administrators to place running processes into "partitions", based on their numeric process partition (specified in the process’s MAC label). Processes with a specified partition can only see processes that are in the same partition. If no partition is specified for a process, it can see all other processes in the system (subject to other MAC policy restrictions not defined in this man page). No provisions for placing processes into multiple partitions are available.

Label Format

Partition labels take on the following format:

partition/*value*

Where *value* can be any integer value or "none". For example:

```
partition/1
partition/20
partition/none
```

SEE ALSO

mac(4), mac_biba(4), mac_bsdextended(4), mac_ddb(4), mac_ifoff(4), mac_lomac(4), mac_mls(4), mac_none(4), mac_portacl(4), mac_seeotheruids(4), mac_test(4), maclabel(7), mac(9)

HISTORY

The **mac_partition** 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.