NAME

mac_bsdextended - file system firewall policy

SYNOPSIS

To compile the file system firewall policy into your kernel, place the following lines in your kernel configuration file:

```
options MAC
options MAC_BSDEXTENDED
```

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

```
options MAC
```

and in loader.conf(5):

```
mac_bsdextended_load="YES"
```

DESCRIPTION

The **mac_bsdextended** security policy module provides an interface for the system administrator to impose mandatory rules regarding users and some system objects. Rules are uploaded to the module (typically using ugidfw(8), or some other tool utilizing libugidfw(3)) where they are stored internally and used to determine whether to allow or deny specific accesses (see ugidfw(8)).

IMPLEMENTATION NOTES

While the traditional mac(9) entry points are implemented, policy labels are not used; instead, access control decisions are made by iterating through the internal list of rules until a rule which denies the particular access is found, or the end of the list is reached. The **mac_bsdextended** policy works similar to ipfw(8) or by using a *first match semantic*. This means that not all rules are applied, only the first matched rule; thus if Rule A allows access and Rule B blocks access, Rule B will never be applied.

Sysctls

The following sysctls may be used to tweak the behavior of **mac_bsdextended**:

security.mac.bsdextended.enabled
: Set to zero or one to toggle the policy off or on.

security.mac.bsdextended.rule_count
: List the number of defined rules, the maximum rule count is current set at 256.

security.mac.bsdextended.rule_slots
List the number of rule slots currently being used.

security.mac.bsdextended.firstmatch_enabled
Toggle between the old all rules match functionality and the new first rule matches functionality. This is enabled by default.

security.mac.bsdextended.logging
Log all access violations via the AUTHPRIV syslog(3) facility.

security.mac.bsdextended.rules
Currently does nothing interesting.

SEE ALSO

libugidfw(3), syslog(3), mac(4), mac_biba(4), mac_ddb(4), mac_ifoff(4), mac_lomac(4), mac_mls(4), mac_none(4), mac_partition(4), mac_portacl(4), mac_seeotheruids(4), mac_test(4), ipfw(8), ugidfw(8), mac(9)

HISTORY

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

The "match first case" and logging capabilities were later added by Tom Rhodes *<trhodes@FreeBSD.org>*.

AUTHORS

This software was contributed to the FreeBSD Project by NAI 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.