NAME

mac_ipacl - IP Address access control policy

SYNOPSIS

Add the following lines in your kernel configuration file to compile the IP address access control policy into your kernel:

```
options MAC
options MAC_IPACL
```

To load the mac_ipacl policy module at boot time, add the following line in your kernel configuration file:

```
options MAC
```

and in loader.conf(5) add:

```
mac_ipacl_load="YES"
```

DESCRIPTION

The **mac_ipacl** policy allows the root of the host to use the sysctl(8) interface to limit the VNET(9) jail's ability to set IPv4 and IPv6 addresses. So, the host can define rules for jails and their interfaces about IP addresses with sysctl(8) MIBs.

Its default behavior is to deny all IP addresses for the jail if **mac_ipacl** policy is enforced and allow/deny IP (or subnets) according to the *security.mac.ipacl.rules* string specified with sysctl(8)

Runtime Configuration

The following sysctl(8) MIBs are used to control enforcement and behavior of this MAC Policy.

security.mac.ipacl.ipv4
: Enforce **mac_ipacl** for IPv4 addresses. (Default: 1).

security.mac.ipacl.ipv6
: Enforce **mac_ipacl** for IPv6 addresses. (Default: 1).

security.mac.ipacl.rules
: The IP address access control list is specified in the following format:

```
jid,allow,interface,addr_family,IP_addr/prefix[@jid,...]
```

jid Describe the jail id of the jail for which the rule is written.

allow 1 for allow and 0 for deny. Decides action performed for the rule.

interface Name of the interface the rule is enforced for. If the interface is left empty then it is a wildcard to enforce the rule for all interfaces.

addr_family
Address family of the IP_addr. The input to be given as AF_INET or AF_INET6 string only.

IP_addr IP address (or subnet) to be allowed/denied. Action depends on the prefix length.

prefix Prefix length of the subnet to be enforced by the policy. -1 implies the policy is enforced for the individual IP address. For a non-negative value, a range of IP addresses (present in subnet) which is calculated as subnet = IP_addr & mask.

EXAMPLES

Behavior of the **mac_ipacl** policy module for different inputs of sysctl variable:

1. Assign ipv4=1, ipv6=0 and rules="1,1,,AF_INET,169.254.123.123/-1"

   It allow only 169.254.123.123 IPv4 address for all interfaces (wildcard) of jail 1. It allows all IPv6 addresses since the policy is not enforced for IPv6.

2. Assign ipv4=1, ipv6=1 and rules="1,1,epair0b,AF_INET6,fe80::/32@1,0,epair0b,AF_INET6,fe80::abcd/-1"

   It denies all IPv4 addresses as the policy is enforced but no rules are specified about it. It allows all IPv6 addresses in subnet fe80::/32 except fe80::abcd for interface epair0b only.

3. Assign ipv4=1, ipv6=1, rules="2,1,,AF_INET6,fc00::/7@2,0,,AF_INET6,fc00::1111:2200/120@2,1,,AF_INET6,fc00::1111:2299/-1@1,1,,A

   It allows IPv4 in subnet 198.51.100.0/24 for jail 2 and all interfaces. It allows IPv6 addresses in subnet fc00::/7 but denies subnet fc00::1111:2200/120, and allows individual IP fc00::1111:2299 from the denied subnet for all interfaces in jail 2.

Please refer to mac/ipacl tests-framework for wide variety of examples on using the ipacl module.

LIMITATIONS/PRECAUTIONS

In the case where multiple rules are applicable to an IP address or a set of IP addresses, the rule that is defined later in the list determines the outcome, disregarding any previous rule for that IP address.

FUTURE WORKS

Rules are given with sysctl interface which gets very complex to give them all in command line. It has to be simplified with a better way to input those rules.

SEE ALSO

mac(4), mac(9)

AUTHORS

The **mac_ipacl** policy module was developed as a Google Summer of Code Project in 2019 by Shivank Garg <*shivank@FreeBSD.org*> under the guidance of Bjoern A. Zeeb <*bz@FreeBSD.org*>.