

How to block IP address with pf on FreeBSD, NetBSD and OpenBSD

Author : admin



I've noticed some IPs which had a kind of too aggressive behaviour towards my Apache webserver and thus decided to filter them out with the Firewall.

As the server is running FreeBSD and my firewall choice is bsd's **pf** I added the following lines to my **/etc/pf.conf** to filter up the abuser IP:

```
table persist file "/etc/pf.blocked.ip.conf"
EXT_NIC="ml0" # interface connected to internet
block drop in log (all) quick on $EXT_NIC from to any
echo '123.123.123.123' >> /etc/pf.blocked.ip.conf
```

As you see I'm adding the malicious IP to **/etc/pf.blocked.ip.conf**, if I later decide to filter some other IPs I can add them up there and they will be loaded and filtered by pf on next pf restart.

Next I restarted my pf firewall definitions to make the newly added rules in pf.conf to load up.

```
freebsd# pfctl -d
freebsd# pfctl -e -f /etc/pf.conf
```

To show all IPs which will be inside the **blockips** filtering tables, later on I used:

```
pfctl -t blockips -T show
```

I can also later use pf to add later on new IPs to be blocked without bothering to restart the firewall with cmd:

```
freebsd# pfctl -t blockedips -T add 111.222.333.444
```

Deleting an IP is analogous and can be achieved with:

```
freebsd# pfctl -t blockedips -T delete 111.222.333.444
```

There are also logs stored about pf IP blocking as well as the other configured firewall rules in **/var/log/pflog** file.

Hope this is helpful to somebody.