Using PF for Firewall

Introduction

Packet Filtering (pf) is one of the many firewalls available with FreeBSD. I believe it originally came from OpenBSD and has been ported to many operating systems since.

To enable pf in FreeBSD, you need to create the file `/etc/pf.conf`, then add the correct stanzas in `/etc/rc.conf`.

Setting up

pf.conf

First, a basic pf.conf file. This one is designed to block all IP's outside of my country (US) since this particular machine has a very limited audience

pf.conf

```
# https://cmcenroe.me/2016/06/04/freebsd-pf-fail2ban.html
# https://www.freebsd.org/doc/handbook/firewalls-pf.html
# http://ipdeny.com/ipblocks/
# https://www.openbsd.org/faq/pf/tables.html
# https://undeadly.org/cgi?action=article&sid=20140527054301

set skip on lo0

# allow all outbound traffic
pass out quick all
# create table us_zones from file containing all us IP's
# use wget -4 --no-proxy --no-cookies --no-cache
http://ipdeny.com/ipblocks/data/countries/us.zone -O /etc/pf-
files/us.zone
table <us_zones> persist file "/etc/pf-files/us.zone"


# create table tcp_services for the only services we need
tcp_services = "{ 22, 80 }"

# the local networks, just in case
table <local_network> { 10.10.10.0/24, 172.45.42.0/24, x.x.x.x/26 }

# create a table for fail2ban to use
table <fail2ban> persist
```

```
# allow anything from our local network
pass in quick from <local_network>

# block everything by default
block in all

# block anything loaded in fail2ban table immediately
block in quick from <fail2ban>

# allow icmp from anyplace EXCEPT fail2ban
pass in quick inet proto icmp all
pass in quick inet6 proto icmp6 all

# allow our tcp services from US Zones
pass in proto tcp from <us_zones> to any port $tcp_services
```

Check your configuration file with:

```
pfctl -vnf /etc/pf.conf
```

This will process, but not start, the configuration. It does some macro expansion, which can also give you a better idea of what is actually going on.

enable pf service

To enable the service, simply add the correct lines in `/etc/rc.conf`. The following commands turns on pf and pflogger (/var/log/pflog).

```
echo '# firewall used is PF' >> /etc/rc.conf
echo 'pf_enable="YES"' >> /etc/rc.conf
echo 'pflog_enable="YES"' >> /etc/rc.conf
```

Now, you can start the firewall with:

```
service pf start
```

Useful Commands

```
# flush and reload rule set
pfctl -f ALL -f /etc/pf.conf

# show all rules. May also be nat and/or states
pfctl -s rules

# validate config file (dry run kind of thing)
pfctl -vnf /etc/pf.conf
```

```
# display all entries in the fail2ban table
pfctl -t fail2ban -T show

# add an IP to table fail2ban
pfctl -t fail2ban -T add 203.0.113.0/24

# remove IP from table fail2ban
pfctl -t fail2ban -T delete 203.0.113.0/24
```

Bibliography

- https://cmcenroe.me/2016/06/04/freebsd-pf-fail2ban.html
- https://www.freebsd.org/doc/handbook/firewalls-pf.html
- http://ipdeny.com/ipblocks/
- https://www.openbsd.org/faq/pf/tables.html
- https://undeadly.org/cgi?action=article&sid=20140527054301

From:
https://kb.unixservertech.com/ - **Unix Server Tech Knowledge Base**

Permanent link:
https://kb.unixservertech.com/unix/freebsd/packetfilter

Last update: **2018/07/04 23:39**