Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

FreeBSD / OpenBSD: PF Firewall Filter Large Number Of Subnets and IP Address

Posted by Vivek Gite <vivek@nixcraft.com>

Q. How do I filter larger number of subnets and IPs using OpenBSD's pf firewall under FreeBSD 7.x server? How do I log all dropped packets from such ips? How do I block upto 10000 IPs or subnet without any performance penalty?

[1]

A. You can easily filter large number of IPs or subnets using pf firewall. PF provides tables to hold large number of IPv4 and IPv6 address. Lookups against a table are very fast and consume less memory and processor time. Tables are created in pf.conf file. Tables can also be populated from text files containing a list of IP addresses and networks.

How do I configure tables to drop large number of IPs?

Open pf.conf file, enter:

```
# vi /etc/pf.conf
```

Add following code:

```
table <blockedips> persist file "/etc/pf.blocked.ip.conf"
ext_if="em1" # interface connected to internet
```

Add following code to drop and log all ips / subnet listed in /etc/pf.blocked.ip.conf, file

```
block drop in log (all) quick on $ext_if from <blockedips> to any
```

Save and close the file. Now create file /etc/pf.blocked.ip.conf file using vi text editor, enter:

```
vi /etc/pf.blocked.ip.conf
```

Sample output:

```
192.168.1.0/24
202.54.1.5
# 202.54.4.5
```

The file /etc/pf.blocked.ip.conf should contain a list of IP addresses and/or CIDR network blocks, one per line. Any line beginning with # is treated as a comment and ignored by pf. To load new rules, simply type:

```
# pfctl -nf /etc/pf.conf
# pfctl -f /etc/pf.conf
```

How do I view all IP address listed in tables?

Type the following command

```
# pfctl -t blockedips -T show
```

Sample output:

```
   58.65.232.0/21
   58.83.12.0/22
   64.28.176.0/20
   64.255.128.0/19
   66.231.64.0/20
   67.213.128.0/20
   69.8.176.0/20
```

How do I add subnet called 91.196.232.0/22 on the fly?

Use pfctl command itself, to add CIDR or IP on fly, enter:

```
# pfctl -t blockedips -T add 202.54.11.11
# pfctl -t blockedips -T add 91.196.232.0/22
```

How do I delete subnet called 91.196.232.0/22 on the fly?

Type the command as follows:

```
# pfctl -t blockedips -T delete 91.196.232.0/22
```

Please note that all changes made using pfct are dynamic. You need to update your file on disk to save the changes.

How do I see statistics for each IP / CIDR?

The -v option can display statistics for each table entry (IP/CIDR), enter:

```
# pfctl -t blockedips -T show -v
```

Sample output:

```
   216.243.240.0/20
        Cleared:     Thu Jul 10 03:01:01 2008
        In/Block:    [ Packets: 0                 Bytes: 0                 ]
        In/Pass:     [ Packets: 0                 Bytes: 0                 ]
        Out/Block:   [ Packets: 0                 Bytes: 0                 ]
        Out/Pass:    [ Packets: 0                 Bytes: 0                 ]
   216.255.176.0/20
        Cleared:     Thu Jul 10 03:01:01 2008
        In/Block:    [ Packets: 0                 Bytes: 0                 ]
        In/Pass:     [ Packets: 0                 Bytes: 0                 ]
        Out/Block:   [ Packets: 0                 Bytes: 0                 ]
        Out/Pass:    [ Packets: 0                 Bytes: 0                 ]
```

How do I view log of dropped IP from default /var/log/pflog file?

Use tcpdump command to read a log file:

```
# tcpdump -n -e -ttt -r /var/log/pflog
# tcpdump -n -e -ttt -r /var/log/pflog port 80
# tcpdump -n -e -ttt -r /var/log/pflog and host 202.33.1.2
```

You can also view log in real time, enter:

```
# tcpdump -n -e -ttt -i pflog0
# tcpdump -n -e -ttt -i pflog0 port 80
# tcpdump -n -e -ttt -i pflog0 host 202.33.1.2
```

Further readings:

- man pages - pf.conf, pfctl, tcpdump, pf

URL to article: **http://www.cyberciti.biz/faq/opebsd-pf-firewall-block-subnets-ip-address/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/openbsd/**
