

Table Of Contents

Table Of Contents 1

Install pftop 2

 Start pftop 2

 Further readings: 3

[Home](#) > [Faq](#) > [FreeBSD](#)

BSD PF Firewall: Displays Active Packetfilter States And Rules

Posted by [Vivek Gite](#) <vivek@nixcraft.com>

Q. How do I view active connections with [PF firewall](#) ^[2] under FreeBSD / OpenBSD UNIX operating system?

A. You need to use pftop command which displays the active packetfilter states and rules, and periodically updates this information. It provides a "top" like view of the PF state table.



Install pftop

pftop can be installed from the FreeBSD / OpenBSD ports collection, or downloaded from the pftop website. Under FreeBSD type the following command to update ports and install the latest version:

```
# portsnap fetch update
# cd /usr/ports/sysutils/pftop
# make install clean
```

Start pftop

pftop displays source and destination IP addresses, TCP and UDP port numbers, packets and bytes transmitted, the age of a connection, and the time left until a connection will be removed from the state table:

```
# pftop
```

Sample output:

```
pftop: Up State 1-21/55, View: default, Order: none, Cache: 10000 07:40:34
PR  D SRC          DEST          STATE  AGE  EXP  PKTS  BYTES
udp  I 213          1:35450      200.43.78.162:53 2:2   40   20    4    550
udp  I 83           1:20106      200.43.78.162:53 1:2   37    0    2    256
udp  I 200          53          200.43.78.162:53 1:2   37    0    2    200
udp  I 210          0:5525      200.43.78.162:53 1:2   35    0    2    200
udp  I 163          170:17086   200.43.78.162:53 1:2   34    0    2    256
udp  I 163          130:9573    200.43.78.162:53 1:2   34    0    2    256
udp  I 83           1:3119      200.43.78.162:53 1:2   33    0    2    258
udp  I 190          0:54687     200.43.78.162:53 1:2   32    0    2    256
udp  I 90           1:50040     200.43.78.162:53 1:2   32    0    2    200
udp  I 90           1:26602     200.43.78.162:53 1:2   32    0    2    100
udp  I 90           1:55241     200.43.78.162:53 1:2   32    0    2    200
udp  I 193          15:53       200.43.78.162:53 1:2   32    0    2    200
udp  I 195          1:27050     200.43.78.162:53 1:2   32    0    2    200
udp  I 130          5:37504     200.43.78.162:53 1:2   31    0    2    220
udp  I 130          5:62897     200.43.78.162:53 1:2   31    0    2    200
udp  I 205          1:10591     200.43.78.162:53 1:2   26    4    2    270
udp  I 212          0:48790     200.43.78.162:53 1:2   25    5    2    256
udp  I 205          1:10310     200.43.78.162:53 1:2   23    7    2    200
udp  I 205          1:44865     200.43.78.162:53 1:2   23    7    2    204
udp  I 205          1:54073     200.43.78.162:53 1:2   23    7    2    270
udp  I 205          1:34599     200.43.78.162:53 1:2   23    7    2    204
```

Fig.01: pftop in action (click to enlarge)

To exit press **q**. Following commands are currently recognized:

c	Enable/disable state caching (enabled by default).
f	Set the state filter expression.
h,?	Display a summary of the commands (help screen).
n	Set number of lines to display.
o	Select next sorting Order.
p	Pause/resume display updates.
q	Quit pftop.
r	Reverse current sorting order.
s	Set display update interval in Seconds.
v	Select next View.

0-7	Select one of the views directly.
Cursor	Scroll display (up/down), and switch views (left/right). Most of the emacs/mg motion keys work as well.
SPACE	Update display immediately.
CTRL-L	Refresh display.
CTRL-G	Clear command entry line.

Further readings:

- man page pftop, pf and pfctl

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our [daily email](#) newsletter or [weekly newsletter](#) to make sure you don't miss a single tip/tricks. Alternatively, subscribe via [RSS/XML](#) feed.

Article printed from Frequently Asked Questions About Linux / UNIX: <http://www.cyberciti.biz/faq/>

URL to article: <http://www.cyberciti.biz/faq/bsd-pf-viewing-active-connections-with-pftop/>

URLs in this post:

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

[2] PF firewall: <http://bash.cyberciti.biz/firewall/pf-firewall-script/>

[3] Image: <http://www.cyberciti.biz/faq/category/freebsd/>

[4] Image: <http://www.cyberciti.biz/faq/wp-content/uploads/2008/09/pftop.png>