Quick Review of OpenBSD Packet Filter

New York City BSD Conference

October 11, 2008

History

- Developed by Daniel Hartmeier for OpenBSD 3.0 in 2001 to replace IPF (due to license change)
- Maintained by Daniel and rest of the OpenBSD crew
- Ported to Net, Free, and Dragonfly

Features

- Stateful packet filtering
- NAT/BiNAT/Port forwarding
- Packet normalization
- Traffic shaping / bandwidth management
- Load balancing
- Policy-based firewalling
- Tool integration
- And much more …

Activation

- /etc/rc.conf.local

  pf=YES
- /etc/sysctl.conf

  net.inet.ip.forwarding=1

  net.inet6.ip6.forwarding=1 (optional)
- /etc/pf.conf exists
- Reboot / or read pfctl(8) /

Configuration - /etc/pf.conf

- See full BNF in pf.conf(5)
- General format (in that order):
  - Macros (usually here)
  - Tables (usually here)
  - Options
  - Scrub
  - Queue definitions
  - Translation rules
  - Filtering rules

Syntactic Sugar and More

- Macro: int_if="fxp0"
- List: {192.168/16 10/8} - commas optional
- Efficiency: table <table-name>
- Interface qualifiers:
  (if), if:network, if:broadcast, if:peer, if:0
- Grammar is flexible (e.g. skip any to any)

Rules of Thumb

- Implicit pass all rule
- Rules evaluate sequentially
- Last match wins, unless you quick
- NAT and RDR - first match wins
- NAT and RDR happen before filtering
- flags S/SA keep state is the default
- Default state-policy is floating
- Default block-policy is drop
- TEST or lock yourself out of the box

Sample Setup

- Firewall box has three interfaces
- One internet connection
- Several web servers in DMZ
- Office network
- 15 lines in /etc/pf.conf …

```
ext_if="fxp0"
dmz_if="re0"
lan_if="re1"
table <web_servers> persist file "/etc/www.conf"
set skip on lo0
scrub in
rdr on $ext_if proto tcp from any to $ext_if port http -> \
    <web_servers> round-robin sticky-address
nat on $ext_if from !$ext_if:network to any -> $ext_if
block all
antispoof quick for { $ext_if $dmz_if $lan_if }
pass in quick on $lan_if from $lan_if:network modulate state
pass in log on $ext_if proto tcp to $ext_if port ssh
pass in log on $ext_if proto tcp to <web_servers> \
    port http synproxy state
pass in on $dmz_if proto { udp tcp } from <web_servers> \
    to any port { domain ntp }
```

Control - pfctl

```
# pfctl -e  enable
# pfctl -d  disable
# pfctl -f <file>  load the file (/etc/pf.conf)
# pfctl -nf <file> parse but don't load
# pfctl -Nf <file> load NAT rules only
# pfctl -Rf <file> load filter rules only
# pfctl -sn  show current NAT rules
# pfctl -sr  show current filter rules
# pfctl -ss  show current state table
# pfctl -si  show filter stats and counters
# pfctl -sa  show EVERYTHING
```

See pfctl(8) man page.

No Time to Cover

- Performance
- Passive OS Fingerprinting
- Queues and Prioritization
- Packet Tagging and Policy-Based Filtering
- Anchors and Integration
  - ftp-proxy
  - authpf
  - dhcpd
  - CARP
  - pflow
  - etc.

Resources

- PF FAQ: http://www.openbsd.org/pf
- Read The Fine Manual:

  pf(4)

  pf.conf(5)

  pf.os(5)

  sysctl(8), sysctl.conf(5)

  authpf(8)

  ftp-proxy(8)

  rc(8), rc.conf(8)

Thanks to Columbia U

Help Make It Better

Thanks to OpenBSD development team

Donate @

http://www.openbsd.org/donations.html