PF101

An Introduction to Firewallowing with OpenBSD

CapBUG - May 2009
Jason Dixon
What is a Firewall?
What is a Firewall?

- Routes packets between networks
What is a Firewall?

- Routes packets between networks
- Bridges packets between networks
What is a Firewall?

- Routes packets between networks
- Bridges packets between networks
- Filters traffic
What is a Firewall?

• Routes packets between networks
• Bridges packets between networks
• Filters traffic
• Historically operates at OSI layers 2, 3 and 4
What is a Firewall?

- Routes packets between networks
- Bridges packets between networks
- Filters traffic
- Historically operates at OSI layers 2, 3 and 4
- “Application firewalls” filter at layer 7
OpenBSD PF
OpenBSD PF

- Replaced Darren Reed’s IPFilter
OpenBSD PF

- Replaced Darren Reed’s IPFilter
- Stateful IP filtering
SYN

SYN-ACK
OpenBSD PF

- Replaced Darren Reed’s IPFilter
- Stateful IP filtering
OpenBSD PF

- Replaced Darren Reed’s IPFilter
- Stateful IP filtering
- Easy to administer
OpenBSD PF

- Replaced Darren Reed’s IPFilter
- Stateful IP filtering
- Easy to administer
- Linguistic approach to filter rules
OpenBSD PF

• Replaced Darren Reed’s IPFilter
• Stateful IP filtering
• Easy to administer
• Linguistic approach to filter rules
• Advanced features
PF Features
PF Features

• Macros
PF Features

- Macros
- Tables
PF Features

- Macros
- Tables
- Options
PF Features

- Macros
- Tables
- Options
- Scrub
PF Features

- Macros
- Tables
- Options
- Scrub
- Queueing
PF Features

- Macros
- Tables
- Options
- Scrub
- Queueing
- Translation
PF Features

- Macros
- Tables
- Options
- Scrub
- Queueing
- Translation
- Filtering
Macros

• User-defined variables
• Strings, lists, etc.
• Examples:

  ext_if = "em0"

  int_if = "em1"

  dmz_tcp_svcs = "{ http https smtp }"
Tables

- Store IP address blocks
- More efficient than lists
- Can be modified “on the fly”

Examples:

```bash
table <www> { 10.20.0/28 }

table <rfc1918> { 10/8, 172.16/12, 192.168/16 }

table <ssh_drones> persist
```
Options

• Override global defaults (on a global scale)

• Examples:

  set block-policy drop

  set limit states 500000

  set skip on lo0

  set timeout frag 60
Scrub

- Fragment normalization ("defrag")
- First match wins
- Negation

Examples:

```
scrub in all tcp fragment reassemble min-ttl 15
scrub out all reassemble tcp
no scrub on lo0
```
Queueing

- “Bandwidth throttling” or prioritization
- Schedulers
  - Priority (priq)
  - Class Based (cbq)
  - Hierarchical Fair Service Curve (hfsc)
- Scheduler Options (red, ecn, borrow, etc)
Translation

- Network Address Translation (nat)
- Redirection (rdr)
- Bidirectional Mapping (binat)
- First match wins
- Negation
Translation

- **Examples:**

  nat on $ext_if from ($int_if:network) to any -> ($ext_if)

  rdr on $ext_if from any to ($ext_if) port http -> <www_int>

  binat on $ext_if from <smtp_int> to any -> <smtp_ext>
Filtering

- Selectively block (bad) or pass (good)
- Filter at layer 2 (tagged by bridge)
- Filter at layer 3 (IPv4 or IPv6)
- Filter at layer 4 (TCP, UDP, ICMP or ICMPv6)
- Filter at layer 7 with `relayd(8)`
- Last match wins (except with `quick` keyword)
Filtering

• Predictable structure
• Most attributes are optional
• Examples:

```plaintext
block

pass in on $int_if

pass in on $ext_if inet proto tcp to <ssh_int> \
  port ssh flags S/SAFR synproxy state \
  (max-src-conn 5, max-src-conn-rate 10/60, \
  overload <ssh_abuse> flush global)
```
Administration

• Edit your ruleset in /etc/pf.conf
• Manage PF with /sbin/pfctl
• Enable PF in /etc/rc.conf.local
• Review logged packets on pflog0
Administration

• Test your syntax with `pfctl -nf /etc/pf.conf`
• Load your ruleset with `pfctl -f /etc/pf.conf`
• Show your filter rules with `pfctl -s rules`
• Show your nat rules with `pfctl -s nat`
• Show your queues with `pfctl -s queue`
• Show your states with `pfctl -s states`
• Add `-v` to display statistics
Random Thoughts

• Block by default
• Translation occurs before Filters
• Use macros where they simplify, not obfuscate
• I hate quick and you should too
• Is everything enabled?

```
sysctl net.inet.ip.forwarding
pfctl -si
pfctl -e
```
VLANs

- IEEE 802.1Q encapsulation
- Multiple logical networks
- OpenBSD pseudo-device `vlan(4)`

Examples:

    ifconfig vlan300 vlan 300 vlandev em0 up

    ifconfig vlan300 30.30.30.1 netmask 255.255.255.0

    ifconfig carp0 vhid 1 carpdev vlan300
Questions?
Lab

• External network on VLAN ID 100
• Internal network on VLAN ID 200
• DHCP on external network (10.10.10.??/24)
• Static on internal network (20.20.???.1/24)
• NAT outbound traffic from internal network
• RDR inbound SSH traffic (port 22?? -> 20.20.???.2)
• Block all other traffic
• “Bonus points” - Prioritize outbound SSH over HTTP
Thanks!