Introduction to Firewalls

Networks Three

Otago Polytechnic
Dunedin, New Zealand

The Internet is a pretty scary place

- An unprotected system exposed to the Internet will be subect to attacks within minutes.
- Hosts on our networks typically emit network traffic that should not be visible outside our networks.
- Compromised machines may send unwanted traffic that should be contained.

Conclusion: We need firewalls to control the flow of network traffic.

Host or network based

- Most operating systems include firewalling capabilities to protect individual hosts.
- Network firewalls may be deployed at network perimeters to protect entire networks.
- A comprehensive security strategy should include both.

Application firewalls

Application firewalls work at the application layers, inspecting the payload data for unwanted traffic.
Examples:

- Email spam and virus filters
- Web filters

Packet filters

Packet filters inspect individual packets for network and transport layer information. They pass or block traffic according to rules based on

- Source and destination IP addresses
- Source and destination ports
- Transport layer protocols (TCP, UDP, ICMP, ICMP6)
- Traffic direction (inbound or outbound)
- Connection state

PF: OpenBSD packet filter

- PF (Packet Filter) is the firewall package included in OpenBSD.
- It is installed and enabled by default (It's just configured to pass all traffic.
- It is configured using the file `/etc/pf.conf` and from the commmand line using `pfctl`

Some handy `pfctl` commands

`# pfctl -f /etc/pf.conf`	Load the pf.conf file
`# pfctl -nf /etc/pf.conf`	Parse the file, but don’t load it
`# pfctl -sr`	Show the current ruleset
`# pfctl -ss`	Show the current state table
`# pfctl -si`	Show filter stats and counters
`# pfctl -sa`	Show EVERYTHING it can show

PF rules

PF inspects packets according to its set of *rules*. When a packet matches a rule's selection criteria, the rule's action may be carried out.

```
block in all
pass in from all to 10.4.0.3 22
pass out from 192.160.1.0/24 to any port www
```

Rule syntax

```
action [direction] [log] [quick] [on interface] [af]
  [proto protocol] [from src_addr [port src_port]]
  [to dst_addr [port dst_port]] [flags tcp_flags]
  [state]
```

Rule order

- Rules are processed in order.
- A packet may match many rules.
- The last rule matched wins.
- We can short-circuit this with the `quick` option

More information

`http://www.openbsd.org/faq/pf/index.html`