Firewalls
SS-E 2019

Kevin Chege

ISOC

What’s a Firewall?

- Computer network security device to protect devices, or restrict access to or from a network
- Analyzes traffic coming in or going out (or through it) and determines a course of action based on a pre-defined rule set
- Firewalls can be found anywhere:
  - On your laptop OS
  - On routers
  - On server OS
  - On network hardware appliances

Types of firewalls

- Packet Filters – analyze network packets and decide a course of action based on configuration
- Stateful Filters – track network “conversations” and maintain a table of which connections are in an active conversations
- Application layer – aka Layer 7 firewalls are able to detect if an unwanted protocol is attempting to bypass the firewall on an allowed port

Keeping State vs Stateless

- Stateful inspection refers to ability to track the state, or progress, of a network connection
- By storing information about each connection in a state table, a firewall is able to quickly determine if a packet passing through the firewall belongs to an already established connection.
- If it does, it is passed through the firewall without going through ruleset evaluation saving time and avoiding extra processing.

Typical features of a Firewall

- Rule Syntax
- NAT control
- Able to pass, redirect or drop traffic based on the rules
- Logging feature – to allow audit of activities and of traffic
- Stateful inspection - not all and may need to be enabled with extra config options
- Ability to be either inclusive or exclusive - An exclusive firewall allows all traffic through except for the traffic matching the ruleset (default is to allow). Inclusive firewall does the reverse (default is to block)

FreeBSD Firewalls

- FreeBSD ships with 3 Main firewalls:
  - IPFW – IP FireWall is (by default) a stateless firewall. FreeBSD sponsored firewall software application authored and maintained by FreeBSD volunteer staff members.
  - IPF – IP Filter can be configured as stateful or stateless. Open source application and has been ported to FreeBSD, NetBSD, OpenBSD, SunOS™, HP/UX, and Solaris™ operating systems. IPFILTER is actively being supported and maintained, with updated versions being released regularly.
  - PF – Packet Filter can be configured as stateful or stateless. Maintained by OpenBSD Project

Linux IPTables

- **iptables** is a user-space utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall which are implemented as different Netfilter modules
- Netfilter offers various functions and operations for packet filtering, network address translation, and port translation, which provide the functionality required for directing packets through a network and prohibiting packets from reaching sensitive locations within a network.

More on “iptables”

```
$ sudo apt-get install man

$ man iptables
```

What about default deny?

- The recommended practice when setting up a firewall is to take a "default deny" approach.
- That is, to deny *everything* and then selectively allow certain traffic through the firewall.
- This approach is recommended because it errs on the side of caution and also makes writing a ruleset easier. the first two filter rules should be:
- **HOWEVER**, you may opt to approach your firewall rules differently depending on the scenario

Some iptables examples

sudo iptables -A INPUT -p icmp -j ACCEPT

- **-A** - Append one or more rules to the end of the selected chain
- **INPUT** - The filter table is the default table. It contains the actual firewall filtering rules. The built-in chains include these INPUT, OUTPUT, FORWARD
- **-p icmp**– Protocol (tcp, udp,, icmp, all, among others**)**
- **-j ACCEPT** – Jump -This specifies the target of the rule; i.e., what to do if the packet matches it: either ACCEPT or DROP

sudo iptables -A INPUT -p icmp -j ACCEPT

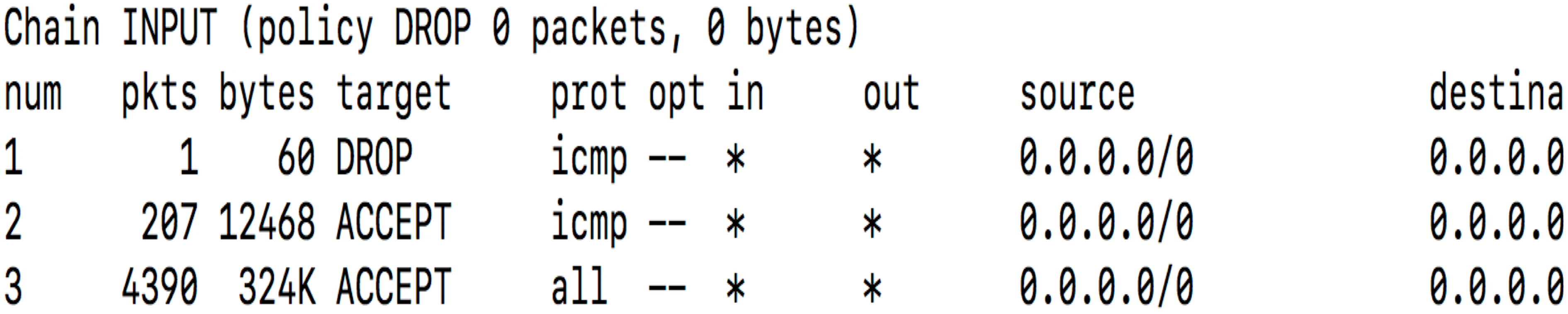
- **-A** - Append one or more rules to the end of the selected chain
- **INPUT** - The filter table is the default table. It contains the actual firewall filtering rules. The built-in chains include these INPUT, OUTPUT, FORWARD
- **-p icmp**– Protocol (tcp, udp,, icmp, all, among others**)**
- **-j ACCEPT** – Jump -This specifies the target of the rule; i.e., what to do if the packet matches it: either ***ACCEPT*** or DROP

sudo iptables -I INPUT -p icmp -j DROP

- **-I** - Inserts a rule at the beginning of the chain
- **INPUT** - The filter table is the default table. It contains the actual firewall filtering rules. The built-in chains include these INPUT, OUTPUT, FORWARD
- **-p icmp**– Protocol (tcp, udp,, icmp, all, among others**)**
- **-j DROP** – Jump -This specifies the target of the rule; i.e., what to do if the packet matches it: either ACCEPT or ***DROP***

Show the order of the rules

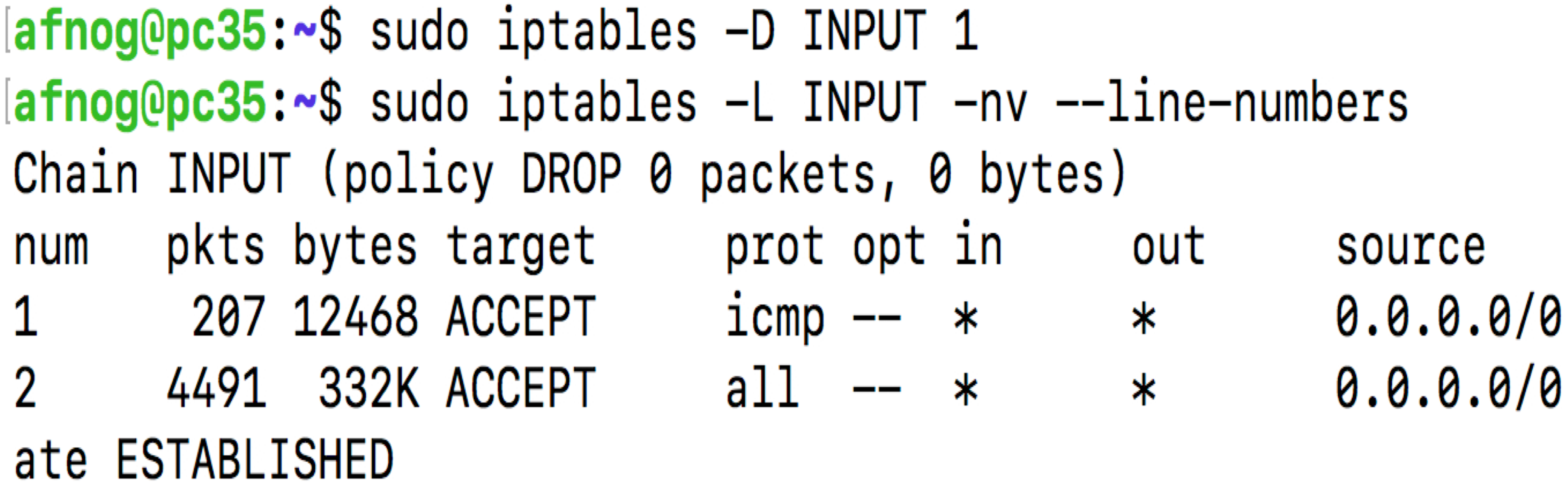
sudo iptables -L INPUT -nv --line-numbers



```
Chain INPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destina
1        1    60 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0
2      207 12468 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0
3     4390  324K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0
```

Delete a rule

sudo iptables -D INPUT 1



```
afnog@pc35:~$ sudo iptables -D INPUT 1
afnog@pc35:~$ sudo iptables -L INPUT -nv --line-numbers
Chain INPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source
1      207 12468 ACCEPT     icmp --  *      *       0.0.0.0/0
2     4491  332K ACCEPT     all  --  *      *       0.0.0.0/0
ate ESTABLISHED
```

Comparison with BSD firewall PF

```
good_ports=“{ 22, 443, 80 }”
me=“192.168.0.1”
set skip on lo0
block in all
pass out all
pass in on em0 inet proto tcp from any to $me    port $good_ports
```

##This is sufficient to allow any communication that the server initiates (pass out all), allow all incoming tcp traffic to the good ports and block all other incoming traffic. The “pass out all” is needed despite PF having an implicit pass rule. Removing it will mean traffic out will not match any rule but incoming replies to conversations initiated by the server will be matched against the “block in all” rule.

References and more reading

- http://en.wikipedia.org/wiki/PF_%28firewall%29
- http://www.openbsd.org/faq/pf/filter.html
- http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls-pf.html
- http://en.wikipedia.org/wiki/Firewall_%28computing%29
- http://www.informit.com/articles/article.aspx?p=421057&seqNum=4