Firewalls and Intrusion Detection/Prevention

page 730

Firewall

- Stand alone server

- Software on your host

Types

- packet filter
- stateful filters
- application gateway

iptables

- Linux Kernel framework
  - netfilter
  - 5 spots to hook into packet processing.

https://doc.opensuse.org/documentation/leap/security/html/book.security/cha.security.firewall.html

https://www.digitalocean.com/community/tutorials/a-deep-dive-into-iptables-and-netfilter-architecture

iptables

- Tables
- Chains
  - rules

https://doc.opensuse.org/documentation/leap/security/html/book.security/cha.security.firewall.html

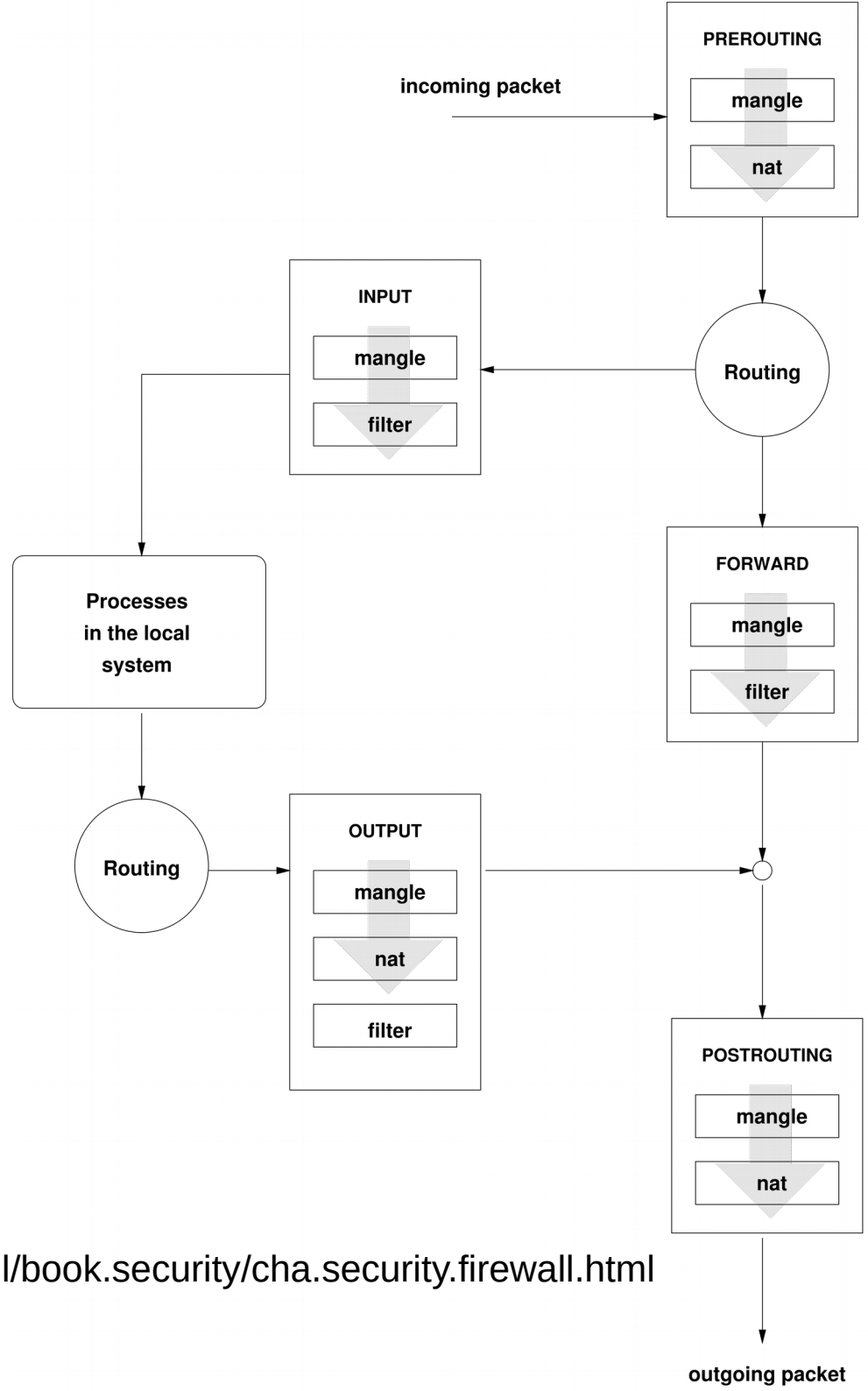
https://www.digitalocean.com/community/tutorials/a-deep-dive-into-iptables-and-netfilter-architecture

Table/Hooks/Chains

Tables↓/Chains→	PREROUTING	INPUT	FORWARD	OUTPUT	POSTROUTING
(routing decision)				✓	
raw	✓			✓	
(connection tracking enabled)	✓			✓	
mangle	✓	✓	✓	✓	✓
nat (DNAT)	✓			✓	
(routing decision)	✓			✓	
filter		✓	✓	✓	
security		✓	✓	✓	
nat (SNAT)		✓			✓

https://www.digitalocean.com/community/tutorials/a-deep-dive-into-iptables-and-netfilter-architecture

Path of an incoming packet for the local system



https://doc.opensuse.org/documentation/leap/security/html/book.security/cha.security.firewall.html
Figure 16.1

Example Rule

```
iptables -A OUTPUT -p tcp --dport 22 -d 64.59.233.197 -j DROP
```

Stateful

- Track the packet relation to the connection
  - NEW
  - ESTABLISHED
  - RELATED
  - INVALID
  - UNTRACKED

Stateful

- Log the first packet connecting out to zeus via ssh

```
iptables -A OUTPUT -p tcp -d 64.59.233.197 --dport 22
-j LOG --log-prefix "NEW zeus:22" --log-level 7
-m state --state NEW
```

```
journalctl -r
```

Mangle

- Change TTL in IP header

```
iptables -t mangle -A OUTPUT -j TTL --ttl-set 32
-p tcp -d 64.59.233.197 --dport 22
```

From the iptables man page:

Don't ever set or increment the value on packets that leave your local network!

Other Linux Kernel Mechanisms

- nftables
  - replacement for netfilter & iptables
  - FirewallD does have a nftables interface
  - slow to take over from iptables
- bpfilter

https://linux-audit.com/bpfilter-next-generation-linux-firewall/
https://lwn.net/Articles/747551/

https://cilium.io/blog/2018/04/17/why-is-the-kernel-community-replacing-iptables/

https://firewalld.org/2018/07/nftables-backend

FirewallD

- Zone
- Services

https://firewalld.org/

https://fedoraproject.org/wiki/Firewalld

Panic

Panic Options

`--panic-on`

Enable panic mode. All incoming and outgoing packets are dropped, active connections will expire. Enable this only if there are serious problems with your network environment. For example if the machine is getting hacked in.

This is a runtime only change.

`--panic-off`

Disable panic mode. After disabling panic mode established connections might work again, if panic mode was enabled for a short period of time.

This is a runtime only change.

`--query-panic`

Returns 0 if panic mode is enabled, 1 otherwise.

Intrusion Prevention

- Fail2Ban

- Brute force attack

Intrusion Detection

- Signature based

- Anomaly based