STI
MEI/MIEBIOM

2022/2023

Practical class #4

- Packet filtering firewalls using IPTables

IPTables/netfilter

netfilter

firewalling, NAT, and packet mangling for linux

Netfilter:

- A framework inside the Linux kernel
- Hooks in the Linux kernel allows modules to register callback functions with the network stack

IPTables:

- Table structure for the definition of rulesets
- Rules consist of a number of classifiers (matches) and one action (target)

IPTables

Tables available:

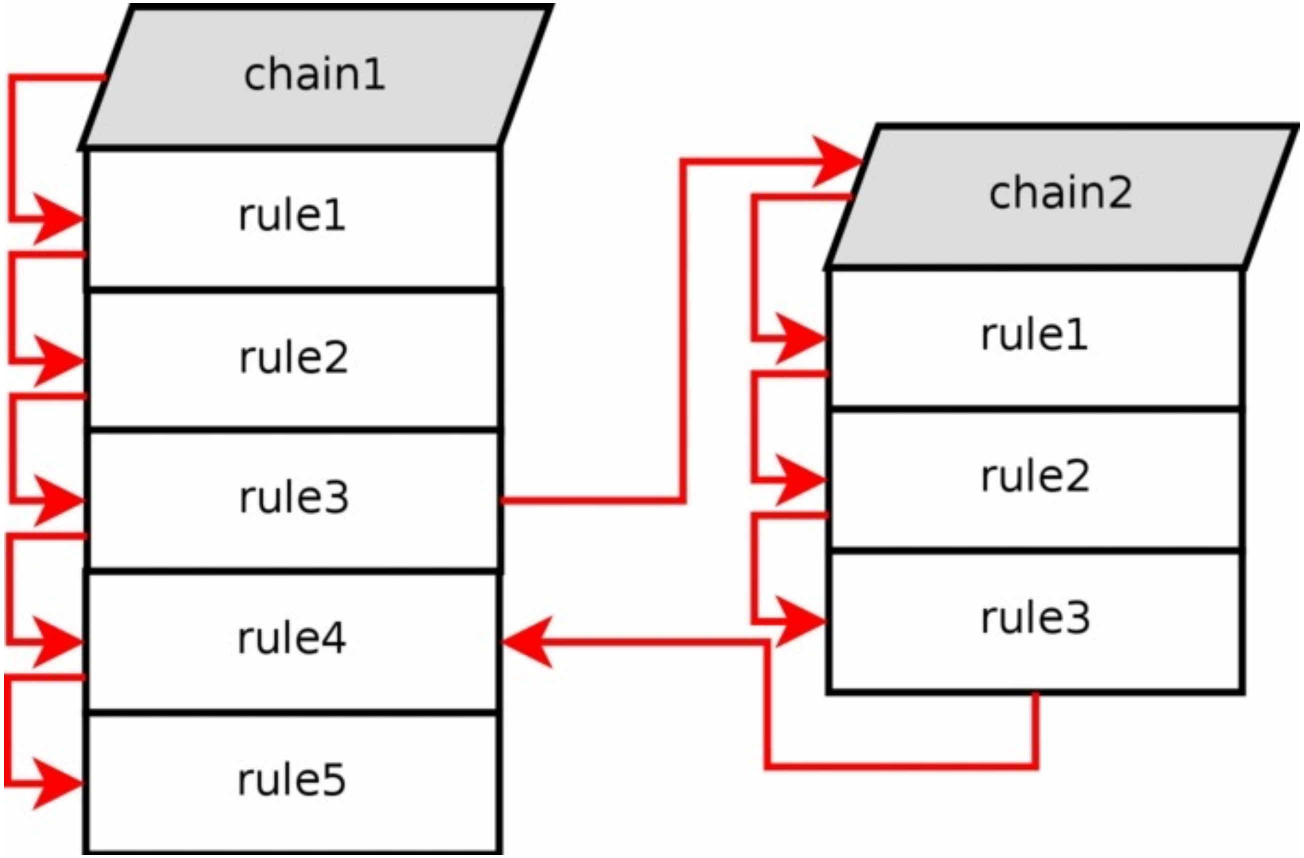
- Table **filter** supports packet filtering
- Table **nat** supports network address (and port) translation
- Table **mangle** supports packet mangling

Chains available in each table:

filter	nat	mangle
INPUT	PREROUTING	PREROUTING
FORWARD	POSTROUTING	OUTPUT
OUTPUT	OUTPUT	FORWARD
		INPUT
		POSTROUTING

IPTables

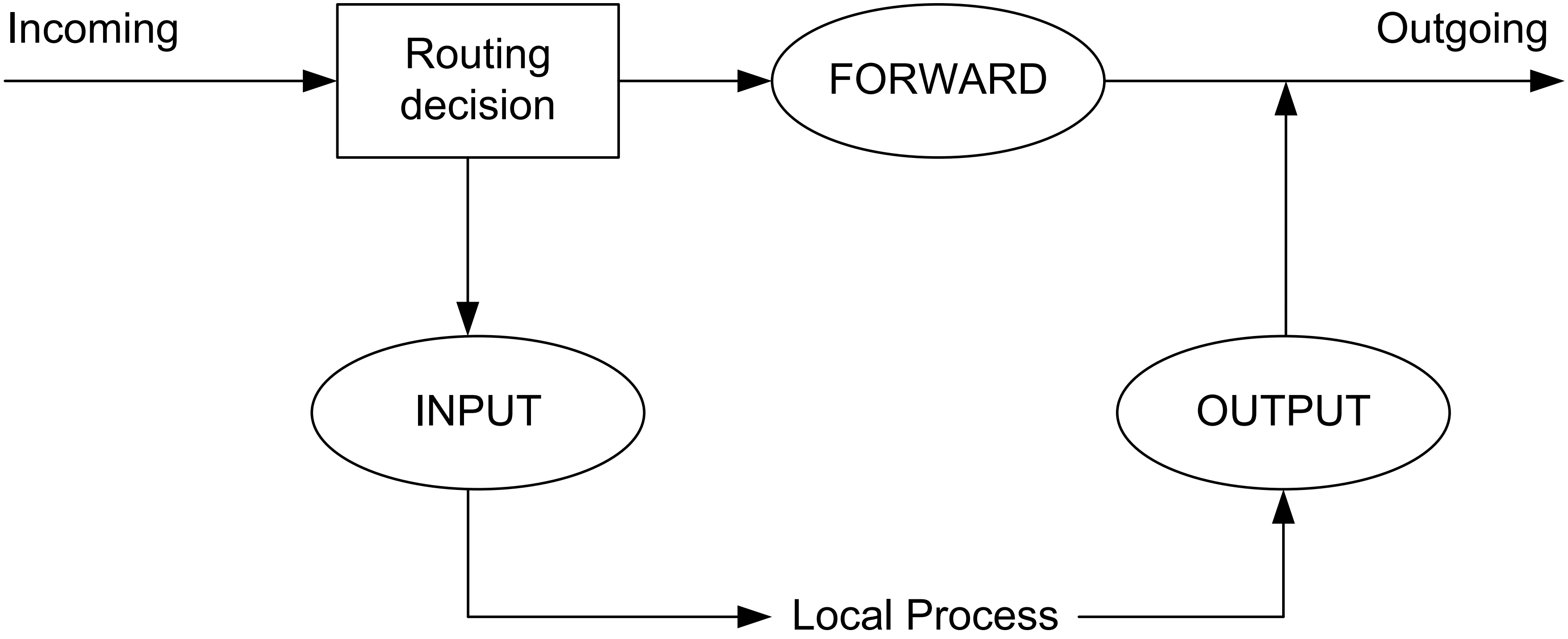
Tables rules traversal:



http://www.iptables.info/en/structure-of-iptables.html

IPTables

filter table:



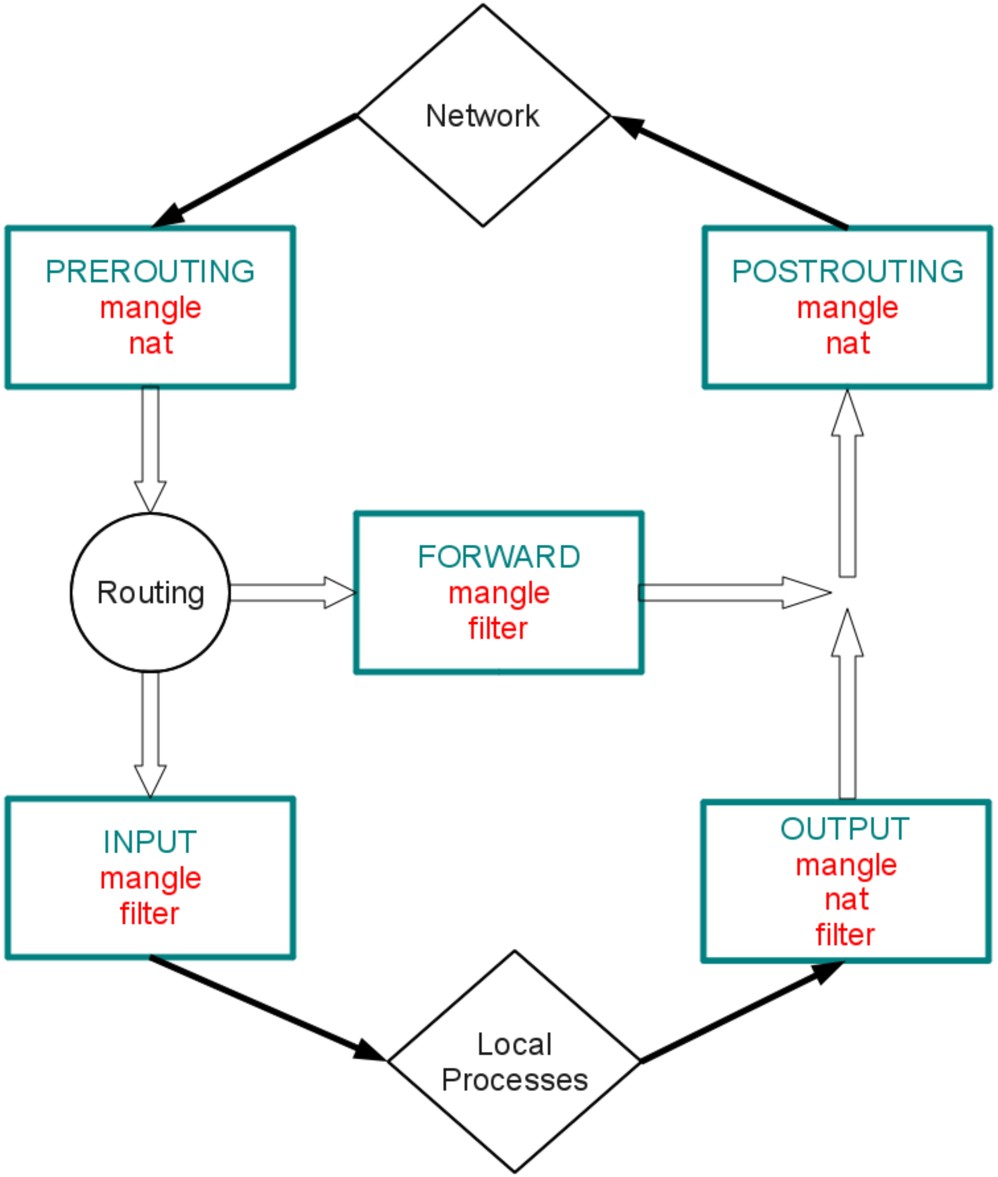
IPTables

IPTables rules using the **filter** table, examples:

```
iptables -A INPUT -s 10.1.0.1 -p icmp --icmp-type echo-request
          -j ACCEPT

iptables -A OUTPUT -o eth0 -p udp -j DROP

iptables -A FORWARD -s ftp.dei.uc.pt -o eth1 -p tcp -m state
          --state RELATED -j ACCEPT

iptables -A INPUT -s 193.137.203.0/25 -p tcp ! –syn -j ACCEPT
```

IPTables

filter, **nat** and **mangle** tables:



https://cs.senecac.on.ca/~michal.heidenreich/ops335/journal.shtml

IPTables/netfilter

IPTables rules using the **nat** table, examples:

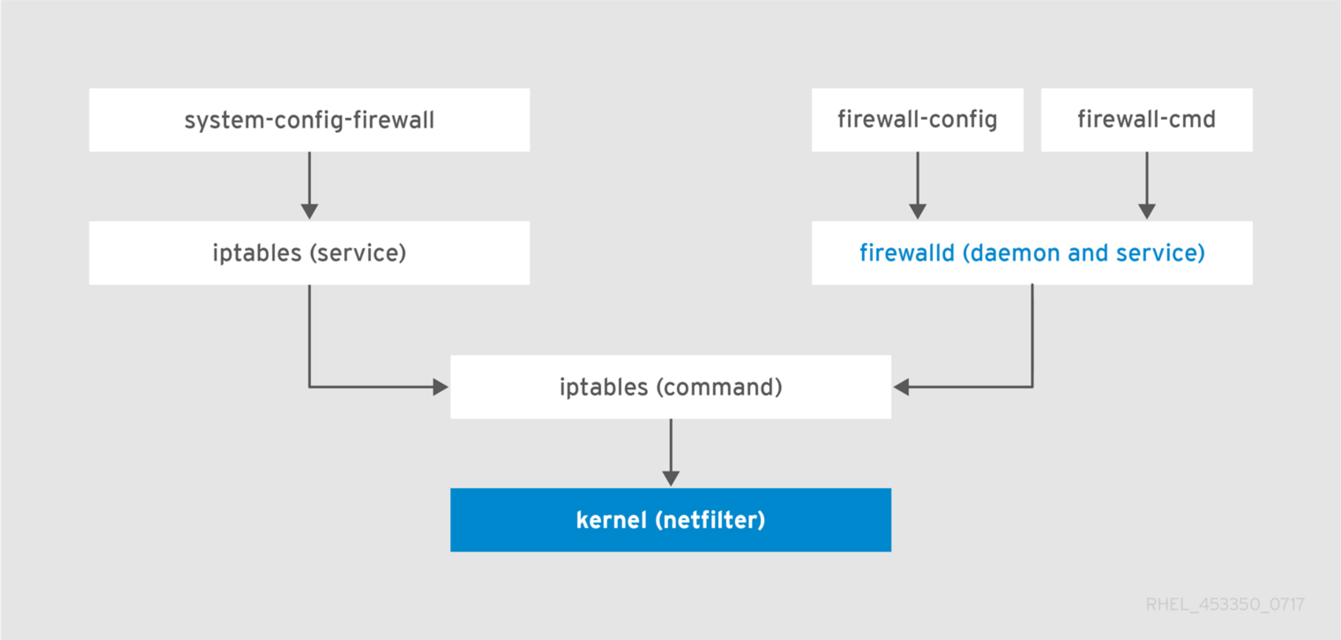
SNAT (Source NAT):

```
iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT
          --to-source 193.137.212.1
```

DNAT (Destination NAT):

```
iptables -t nat -A PREROUTING -p tcp –d  193.137.212.10
          --dport 22 -j DNAT --to-destination 10.254.0.1
```

IPTables versus Firewalld



system-config-firewall

iptables (service)

firewall-config

firewall-cmd

firewalld (daemon and service)

iptables (command)

kernel (netfilter)

RHEL_453350_0717

Disabling **Firewalld** and enabling **IPTables** on CentOS 7

```
yum install iptables-services
systemctl stop firewalld
systemctl disable firewalld
systemctl mask firewalld
systemctl enable iptables
```