Firewalls

What is a Firewall?

Network security device or software that monitors and controls incoming/outgoing network traffic

What is a Firewall?

Network security device or software that monitors and controls incoming/outgoing network traffic

Uses security policies to verify and filter traffic

Very simple

Very complex

State

Stateless Firewalls

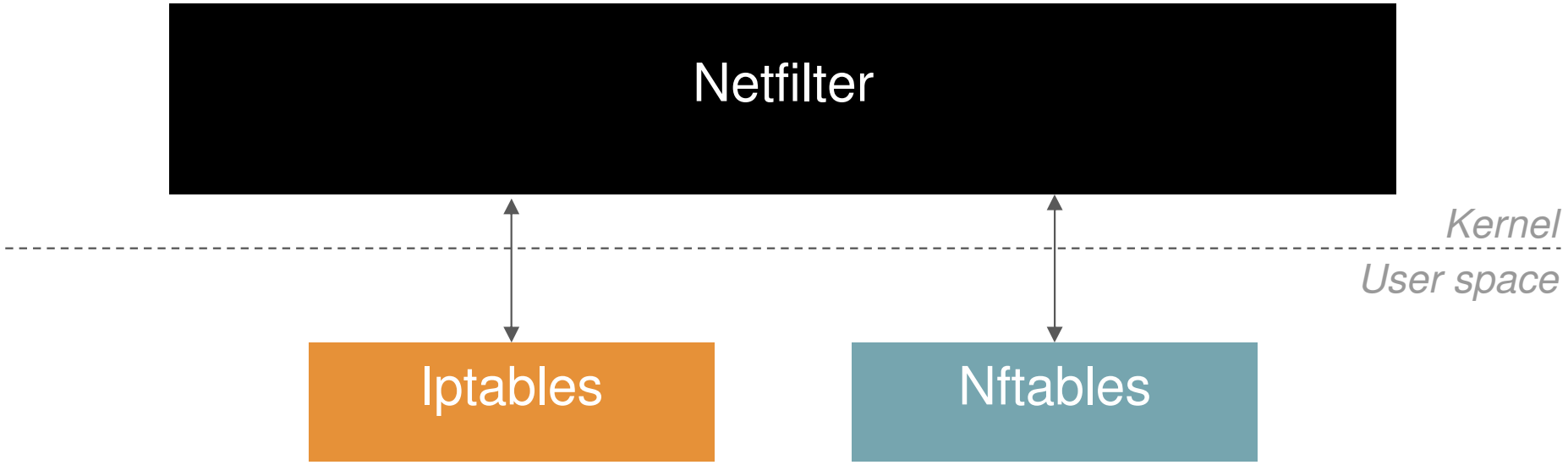
Each network connection is handled separately

Stateful Firewalls

(Stateful Packet Inspection - SPI)

Analyses each packet considering past interactions

Firewalls in Linux



Packet control points (tables)

raw	filter packets before the Kernel tracks their state
mangle	change packet headers
nat	change source or destination addresses
filter	decide if packet is allowed (default)

Packet control points (tables)

raw	filter packets before the Kernel tracks their state
mangle	change packet headers
nat	change source or destination addresses
filter	decide if packet is allowed (default)

… specified through the flag -t/--table

Filter Actions

ACCEPT

Allows packet to continue

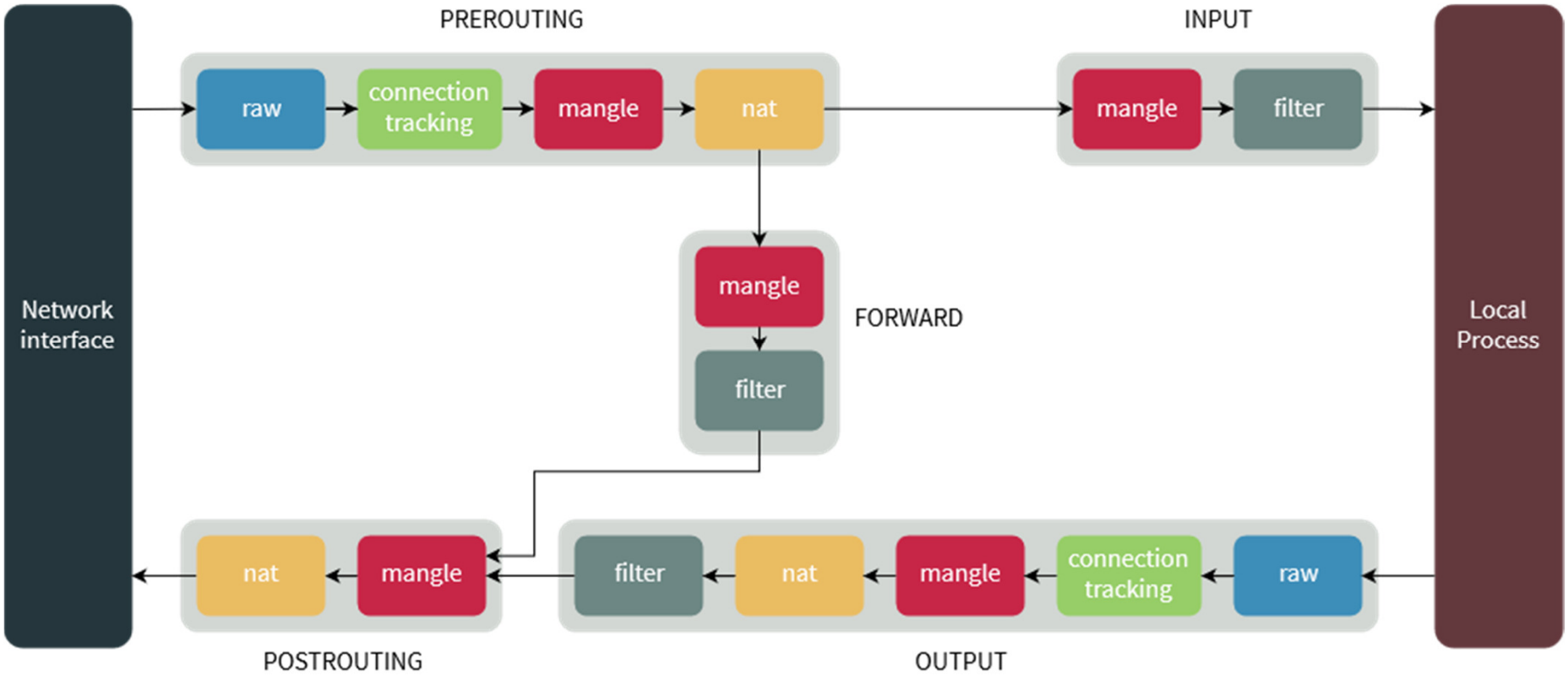
REJECT

Do not accept with denial response

DROP

Silently do not accept

Packet filter moments (chains)



https://commons.wikimedia.org/wiki/File:Iptables_diagram.png