22127060-22127085-22127159

SECURITY FIREWALLD

Dynamic firewall management

CONTENTS

NETFILTER

- Introduction

IPTABLES

- Introduction
- Table
- Chain
- Packet flow

FIREWALLD

- Introduction
- Key characteristic
- Zone
- Service and Port
- Masquerade
- Installation
- Common codes

DEMO VIDEO

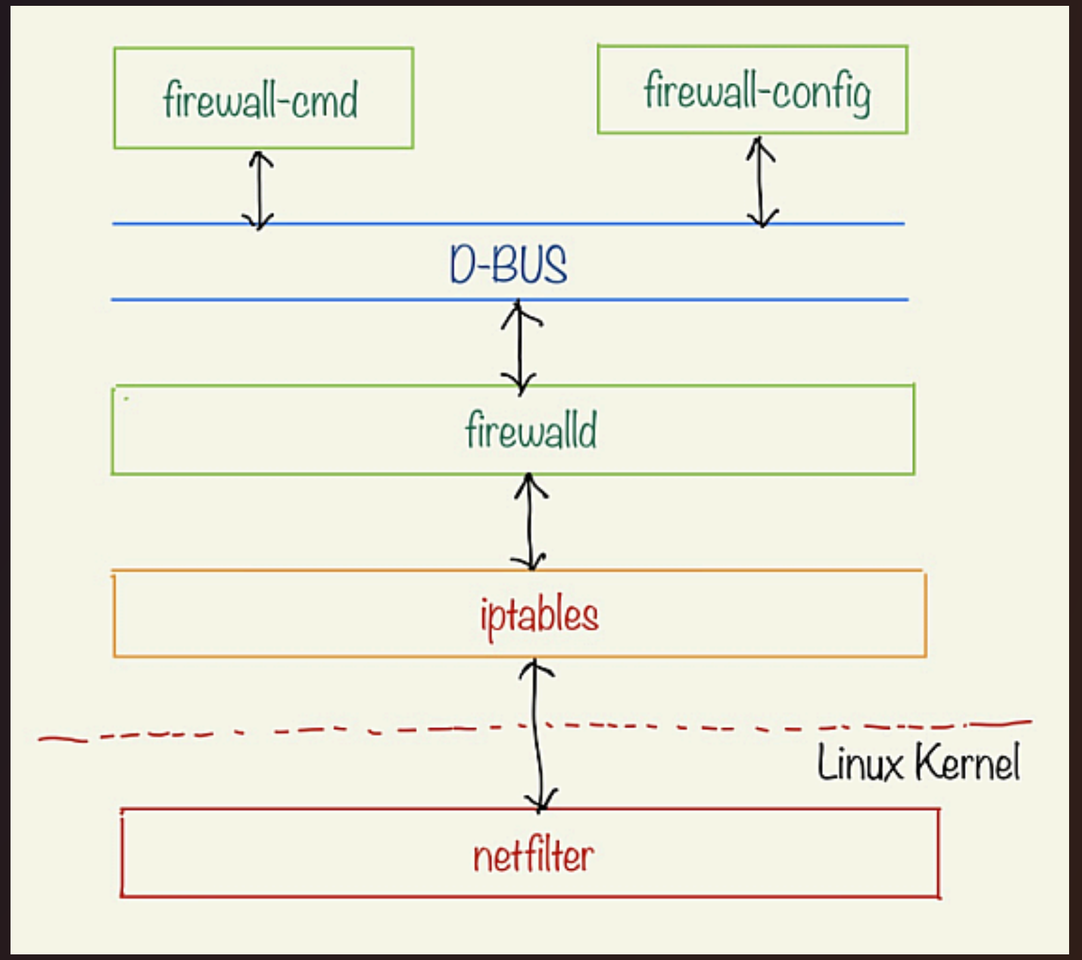
NETFILTER

- Built-in packet filtering framework in the Linux kernel

- Handles:
  - Packet filtering (firewall rules)
  - Network Address Translation (NAT)
  - Connection tracking

- Operates at kernel level for high performance

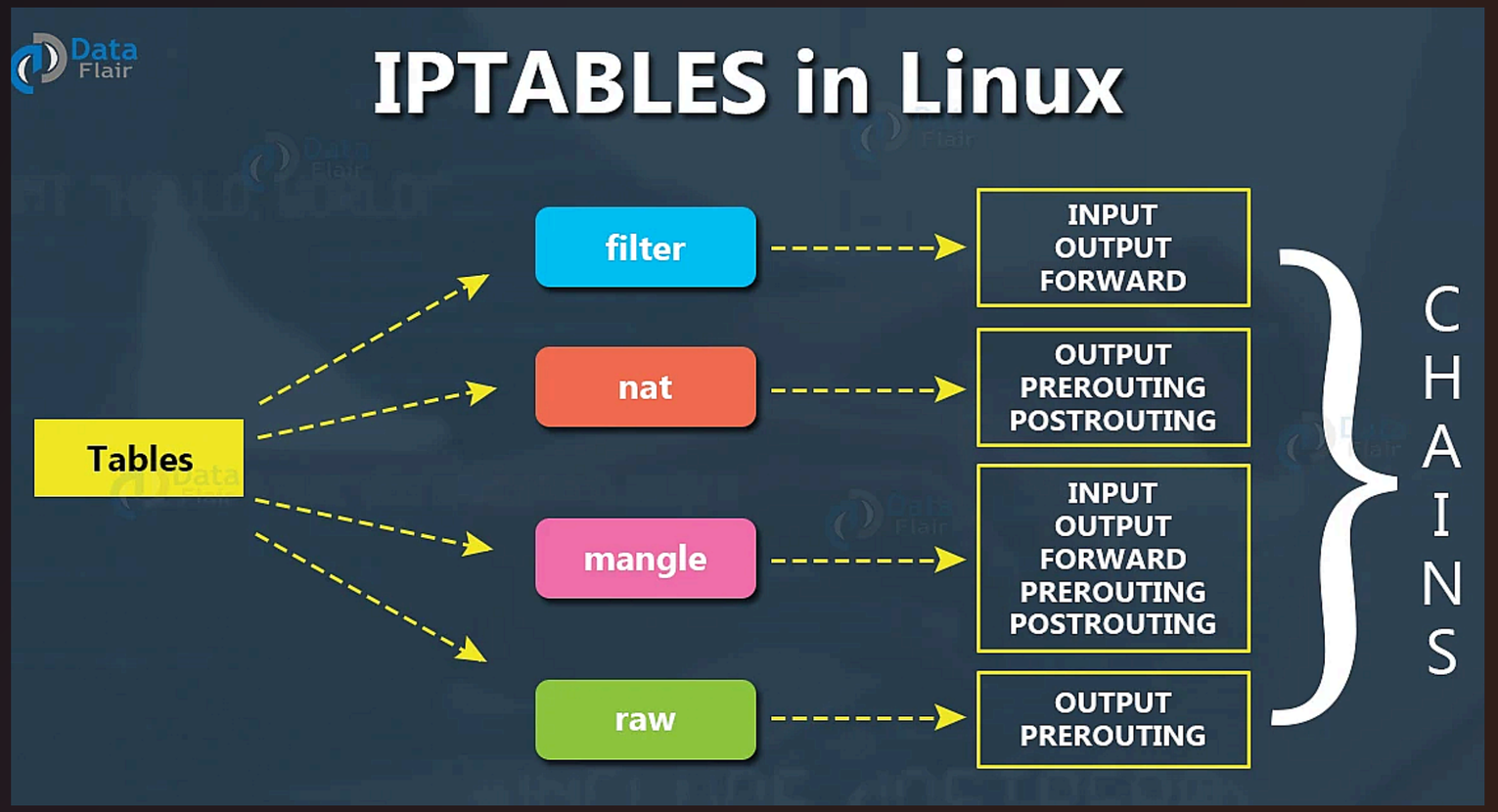
- Controlled by user-space tools:
  - iptables
  - nftables
  - firewalld (via iptables/nftables backend)



IPTABLES

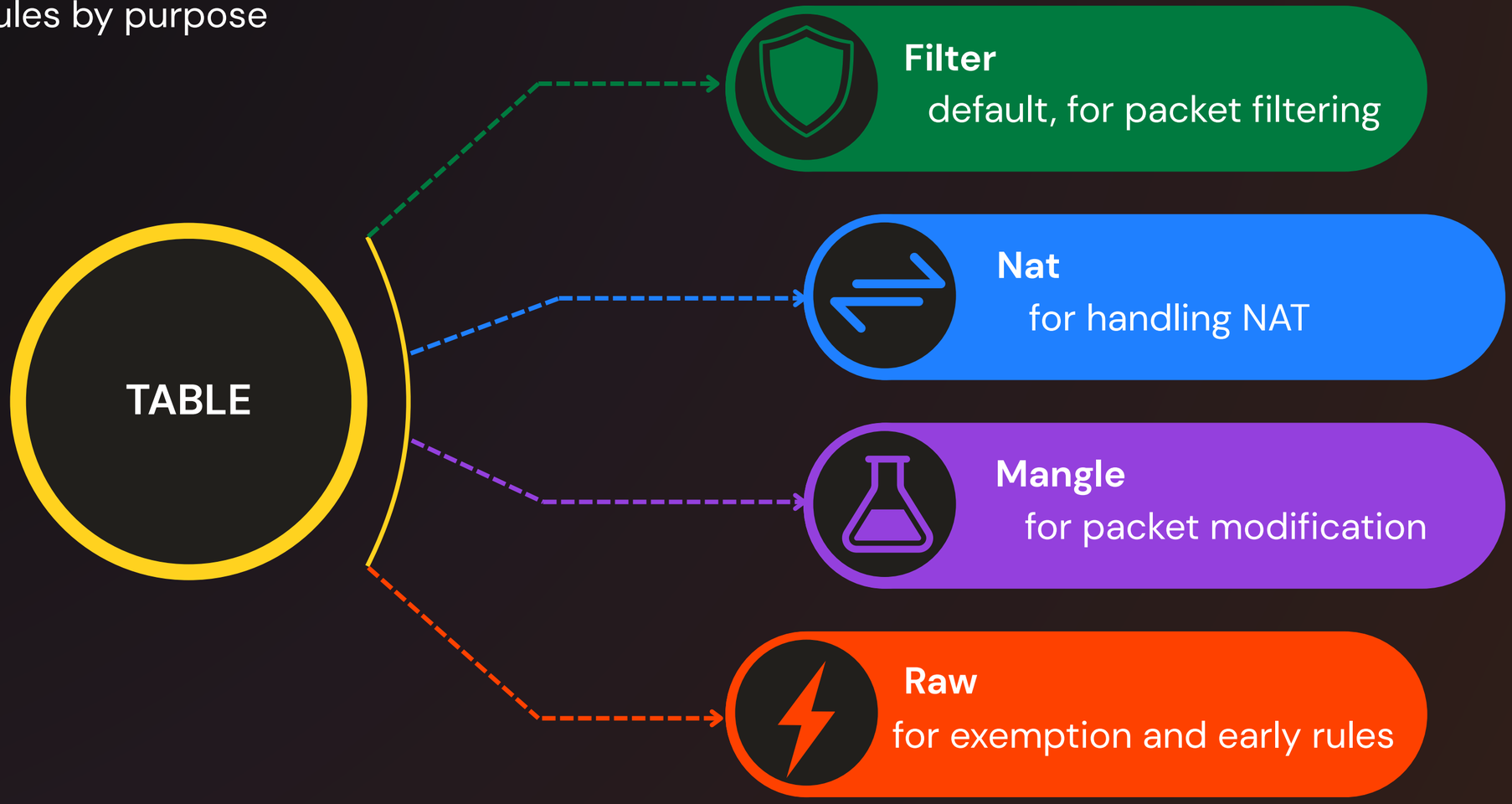
INTRODUCTION

- Userspace utility to configure Linux firewall rules.
- Controls how Netfilter filters or modifies packets.
- Common on traditional Linux systems before firewalld.
- Uses tables and chains to define rule sets.



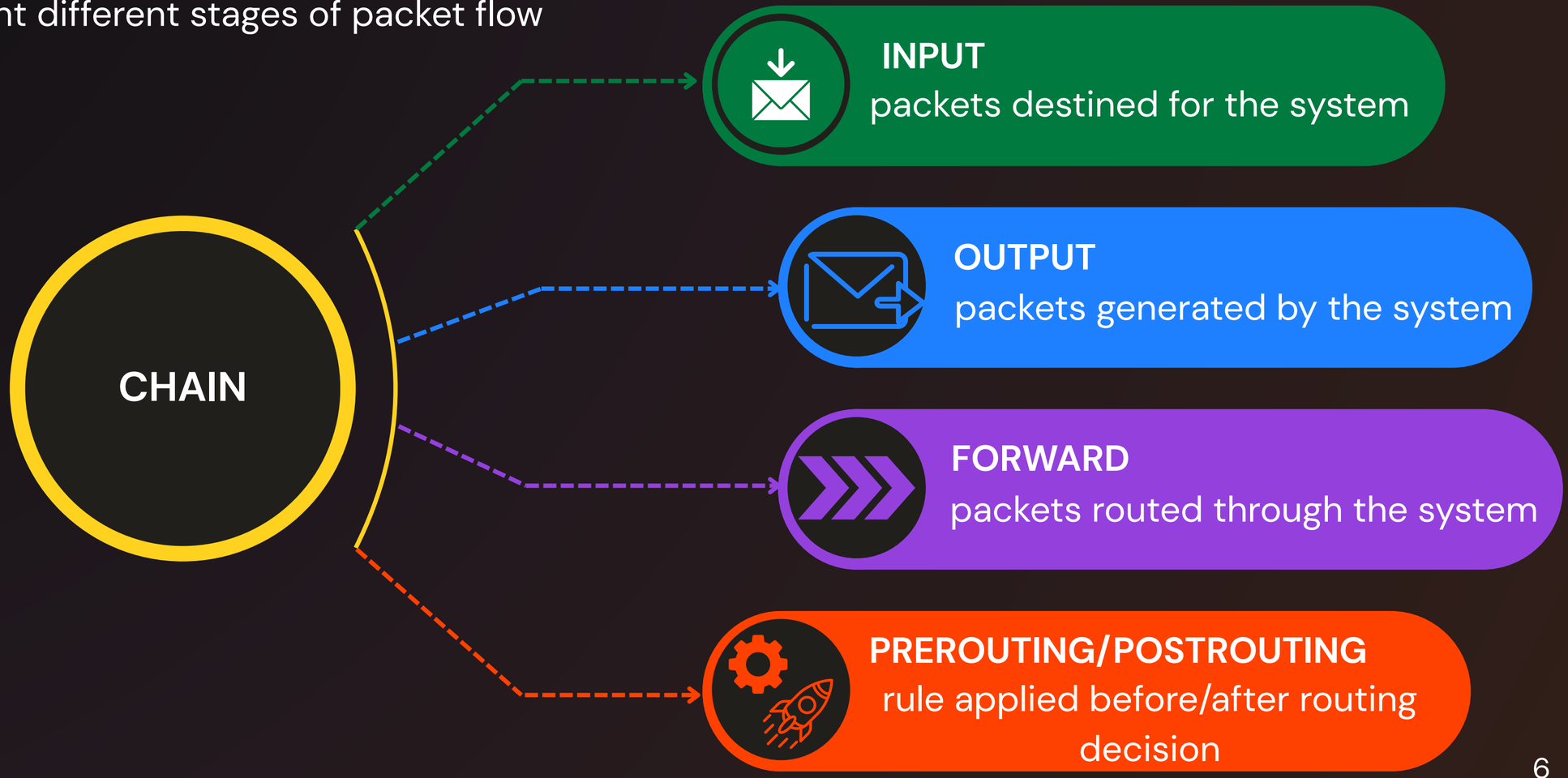
IPTABLES

TABLES Group rules by purpose



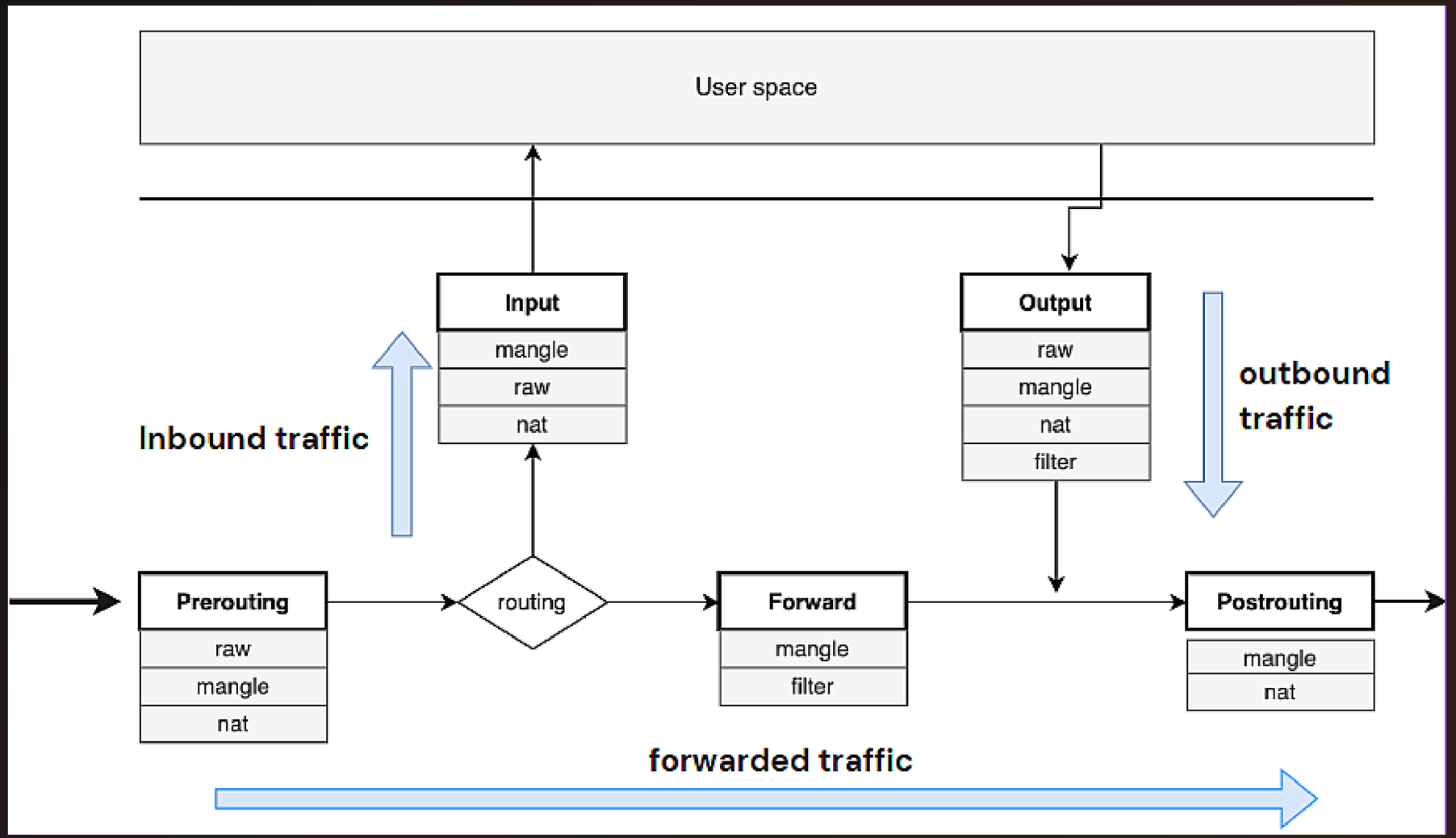
IPTABLES

CHAINS Represent different stages of packet flow



IPTABLES

PACKET FLOW



FIREWALLD OVER IPTABLES ?

Feature	iptables	firewalld
Rule management	Static (reload needed)	Dynamic (runtime changes)
Abstraction	Low-level	Zone & service aware
Ease of use	Complex CLI only	CLI + GUI (firewall-config)
Risk of misconfig	High (manual syntax)	Lower (structured rules)
Default in modern distros	Old version only	Yes (RHEL 7+, Fedora, CenOS 7+)

FIREWALLD

INTRODUCTION

- A dynamic firewall manager for Linux systems
- Replaces traditional static iptables rules
- Default firewall system on RHEL, Fedora, CentOS, AlmaLinux...

→ Help manage firewall rules more easily and safely

FIREWALLD

KEY CHARASTERISTIC

Backend abstraction

Works as a front-end to iptables or nftables

User-friendly tools

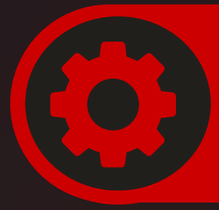
Offers CLI (firewall-cmd) and GUI (firewall-config) for ease of use

Dynamic

Can apply changes at runtime

Zone-based

Uses zones to define different trust levels for network or interface



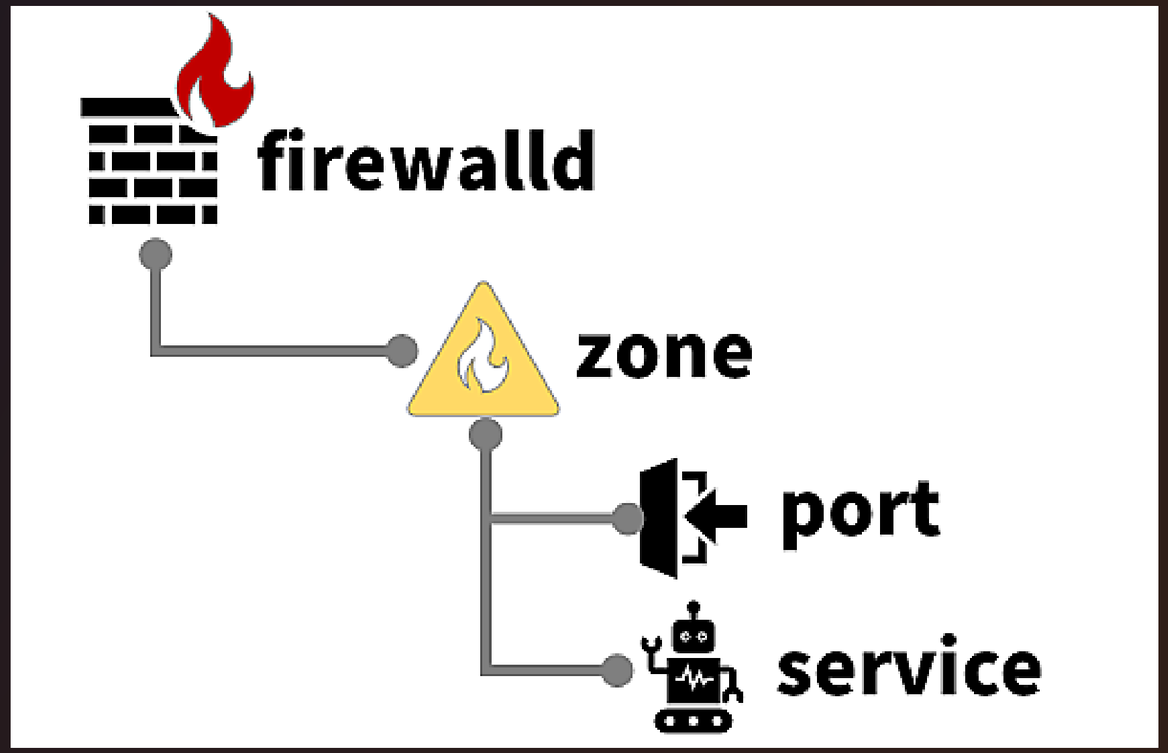
Service-aware

Manages services (ssh, http, ...) instead of raw port numbers

FIREWALLD

COMPONENT: ZONE – INTRODUCTION

- Defines trust level for a connection , interface or source address binding
- Each zone has its own ruleset (allowed services, ports, etc.)
- A zone can handle many connections, but each connection maps to one zone
- A system can have multiple zones active at the same time
- **DEFAULT ZONE**: The zone applied to all network connections not explicitly assigned to another zone



FIREWALLD

COMPONENT: ZONE – PREDEFINED ZONE

drop

Drop all incoming, no reply

block

Reject incoming, send ICMP reject

public

Minimal trust, allow selected services

external

For routers/NAT; masquerading enabled

dmz

Publicly accessible with limited access

work

Office network, allow selected services

home

Trusted home network, more open

internal

Fully trusted internal devices

trusted

Trust everything, allow all traffic

FIREWALLD

COMPONENT: SERVICE AND PORT – INTRODUCTION

SERVICE

- Predefined group of ports and protocols for common applications
- Examples: ssh, http, https, samba, dns
- Easier to use than raw port numbers
- Services are defined in XML files in /usr/lib/firewalld/services/

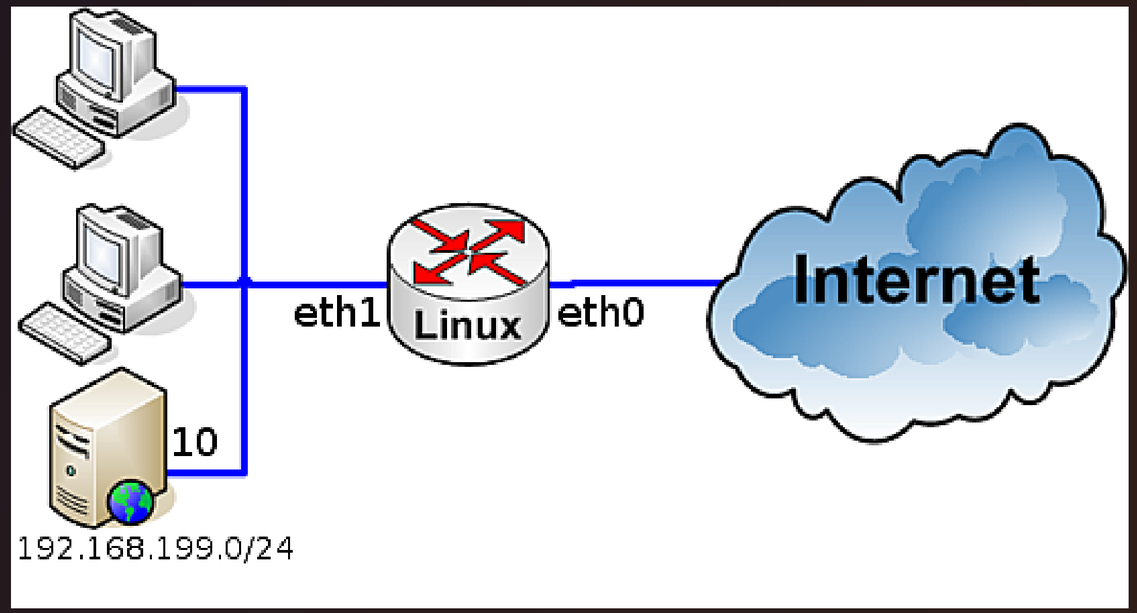
PORT

- Allows opening custom port numbers if the service is not predefined
- Use when working with non-standard apps or development tools

FIREWALLD

COMPONENT: MASQUERADE

- Enables NAT (Network Address Translation)
- Allows multiple devices in a private network to access the internet via one public IP
- Requires:
  - Two interfaces.
  - IP forwarding enabled in system (/etc/sysctl.conf or sysctl)
  - Masquerade rule set on the external zone



WHEN TO USE IPTABLES VS FIREWALLD

IPTABLES

- Scripting complex chains/tables manually
- Fine-grained, low-level control
- Advanced packet mangling or custom modules

FIREWALLD

- Dynamic rule changes (no restart)
- Desktop or server with GUI/CLI preference
- Simple to moderate firewall needs

FIREWALLD

INSTALLATION

```
sudo dnf install firewalld -y
  # Install the firewalld package

sudo systemctl start firewalld
  # Initiate the firewalld service

sudo systemctl enable firewalld
  # Enable firewalld to start automatically on boot

firewall-cmd --state
  # Check if firewalld is running
```

FIREWALLD

COMMON COMMANDS WITH ZONES

```
firewall-cmd --get-default-zone
  # Show the system's current default zone


firewall-cmd --get-active-zones
  # Initiate the firewalld service

firewall-cmd --zone=home --list-all
  # Display zones currently in use (mapped to interfaces)
```

FIREWALLD

COMMON COMMANDS WITH ZONES (continue)

```
sudo firewall-cmd --zone=home --change-interface=eth0
  # Temporarily assign interface eth0 to the 'home' zone

sudo firewall-cmd --set-default-zone=home
  # Set 'home' as the default zone for unmanaged
  interfaces

sudo firewall-cmd --zone=home --change-interface=eth0
--permanent
 # Permanently assign eth0 to the 'home' zone (requires
 reload)
```

RUNTIME

- Apply change immediately
- Can’t survive reboot
- Use case: temporary or quick test

PERMANENT

- Need reload
- Add **`--permanent`**
- Use case: long-term config

FIREWALLD

COMMON COMMANDS WITH SERVICE AND PORT

```
firewall-cmd --get-services
  # Show all predefined services supported by firewalld

sudo firewall-cmd --zone=public --add-service=http
  # Temporarily allow HTTP service in the 'public' zone
                ----------------------

sudo firewall-cmd --zone=public --permanent --add-
service=http
  # Permanently allow HTTP service in the 'public' zone

sudo firewall-cmd --reload
  # Reload needed
```

FIREWALLD

COMMON COMMANDS WITH SERVICE AND PORT (continue)

```
sudo firewall-cmd --zone=public --add-port=5000/tcp
  # Temporarily open TCP port 5000 in the 'public' zone
sudo firewall-cmd --zone=public --permanent --add-port=5000/tcp
  # Permanently open TCP port 5000 (reload needed)
                ----------------------
sudo firewall-cmd --zone=public --add-port=4990-4999/udp
   # Temporarily open UDP ports from 4990 to 4999
sudo firewall-cmd --zone=public --permanent --add-port=4990-
4999/udp
  # Permanently open UDP port from 4990 to 4999 (reload needed)
```

FIREWALLD

COMMON COMMANDS WITH MASQUERADE

```
firewall-cmd --zone=public --add-masquerade
  # Temporarily enable masquerading in the public zone

firewall-cmd --zone=public --permanent --add-masquerade
  # Permanently enable masquerading (reload needed)
```

FIREWALLD

COMMON COMMANDS WITH PORT FORWARDING

```
firewall-cmd --zone=public --add-forward-
port=port=22:proto=tcp:toport=3753
  # Forward incoming TCP traffic on port 22 to port 3753
  on the same machine
firewall-cmd --zone=external --add-forward-
port=port=22:proto=tcp:toaddr=192.0.2.55
  # Forward incoming TCP traffic on port 22 to internal
  host 192.0.2.55
firewall-cmd --zone=external --add-forward-
port=port=22:proto=tcp:toport=2055:toaddr=192.0.2.55
  # Forward port 22 to port 2055 on internal host 192.0.2.55
```

DEMO PRESENTATION

hackmd.io/@denver67