IP-TABLES

Credits By

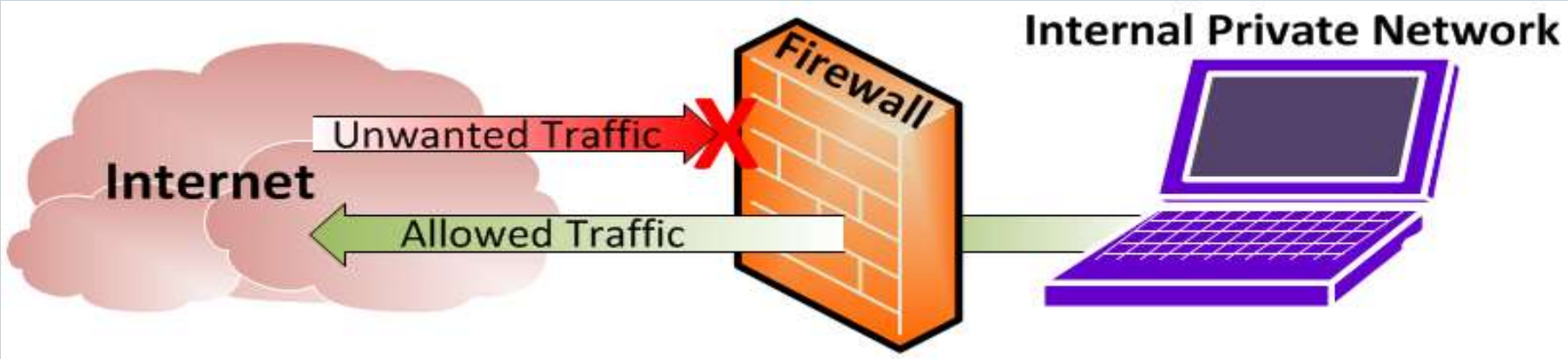
SYED FAWAD UL HASSAN GILLANI

Outline

- Firewall
- What is the iptables
- Why need the iptables
- What you can do with iptables
- Basic Structure of iptable
- Graphical View of iptables, Chains and Rules
- Types of iptables use in Filtering
- Rules in Chains
- Targets
- Few Examples
- Implementation

Firewall

- You can implement a **firewall** in either hardware or software form, or a combination of both. Firewalls prevent unauthorized Internet or intranet traffic .



What is the iptables

- The basic firewall software used in Linux is called iptables.
- iptables is a user-space utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall (implemented as different Netfilter modules) and the chains and rules it stores.
- The Linux kernel’s network packet processing subsystem is called Netfilter

Why need the iptables

- With the help iptables secure the system (PC) from unauthorized access.
- The Linux kernel firewall has the built-in ability to filter packets and allow outgoing and incoming network traffic into system (PC).
- Power full software firewall.

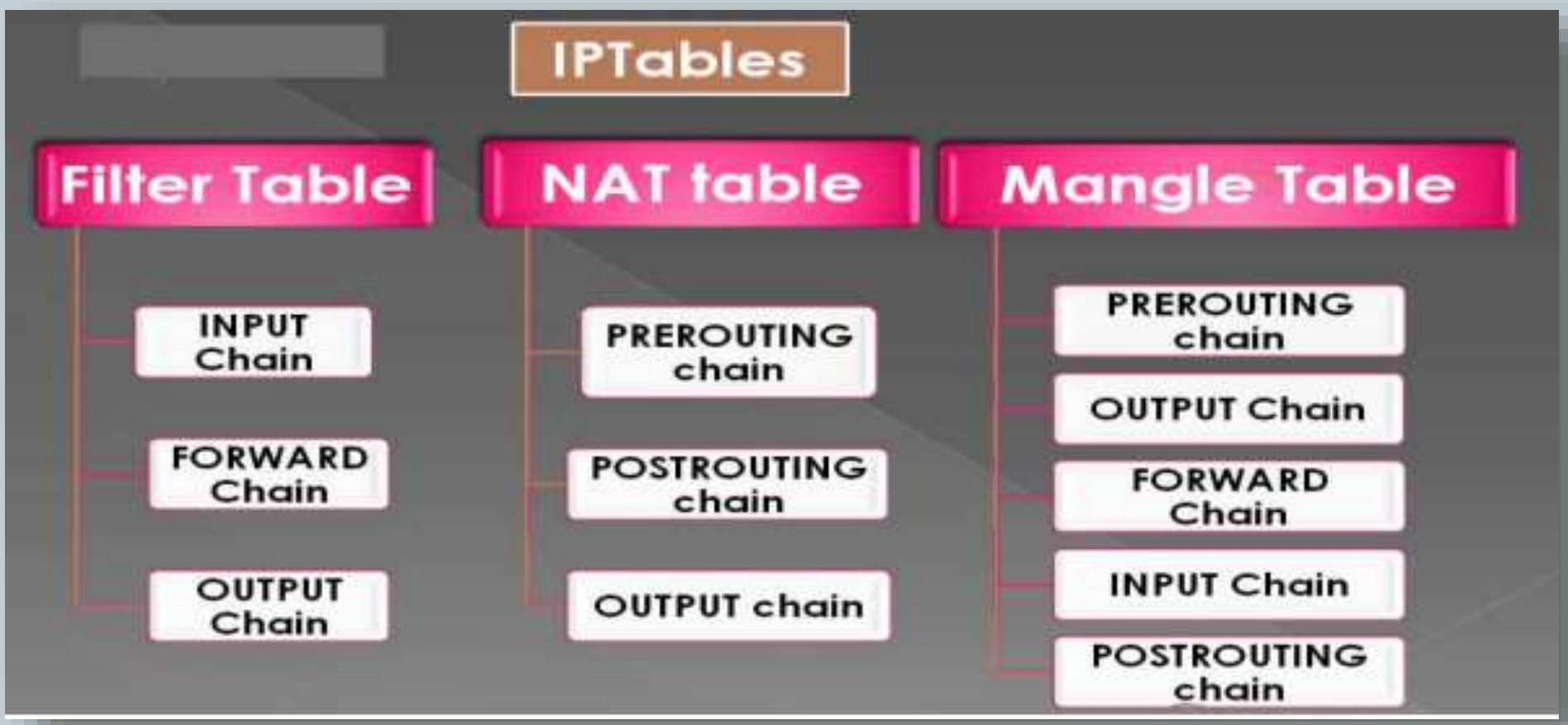
What you can do with IP-tables

- Control network traffic with iptables.
- You can use iptables to block all traffic and only allow traffic from certain IP addresses.
- iptables is an application that allows users to **configure** specific rules. It acts as a packet filter that examines and directs traffic based on **port**, **protocol** and other **criteria.**

Basic Structure of iptable

- The default structure of iptables is like:
- "**T**ables which has **C**hains and the **C**hains which contains **R**ules"
- **Tables —> Chains —> Rules.**
  Tables are bunch of chains, and chains are bunch of firewall rules.
- The rules are defined to control the packets for Input/output

Graphical View of IP tables



1-Packet Filtering(Filter)

Packet filtering is the most basic type of network packet processing. Packet filtering involves examining packets at various points as they move through the kernel's networking code and making decisions about how the packets should be handled (accepted into the next stage or drop).

2-Network address translation (NAT)

NAT is a type of packet mangling that involves overwriting the source and/or destination addresses and/or port numbers. Connection tracking information is used to mangle related packets in specific ways.

3-Packet mangling(Mangle)

Packet mangling involves making changes to packet header fields (such as network addresses and port numbers) or payloads.

Rules in Chains

- There are **five types of rules** implemented in all types of iptable chains:

1. **Input:** The input chain is used for any packet coming into the system. Used by mangle and filter tables.
2. **Output:** The output chain is for any packet leaving the system. Used by Mangle, NAT and Filter tables.

Rules in Chains

3. **Forward:** The forward chain is for packets that are forwarded (routed) through the system. Used by Mangle and Filter tables.
4. **Prerouting:** Prerouting allows altering of packets before they reach the input chain.Used by Mangle and NAT tables.
5. **Postrouting:** Postrouting allows altering packets after they exit the output chain. Used by Mangle and NAT tables.

Targets

Every iptables rules have some "**target**" which is executed. If a packet matches the rule, the target specifies what should be done with it. For example, a packet can be accepted, dropped, logged, or sent to another chain to be compared against more rules.

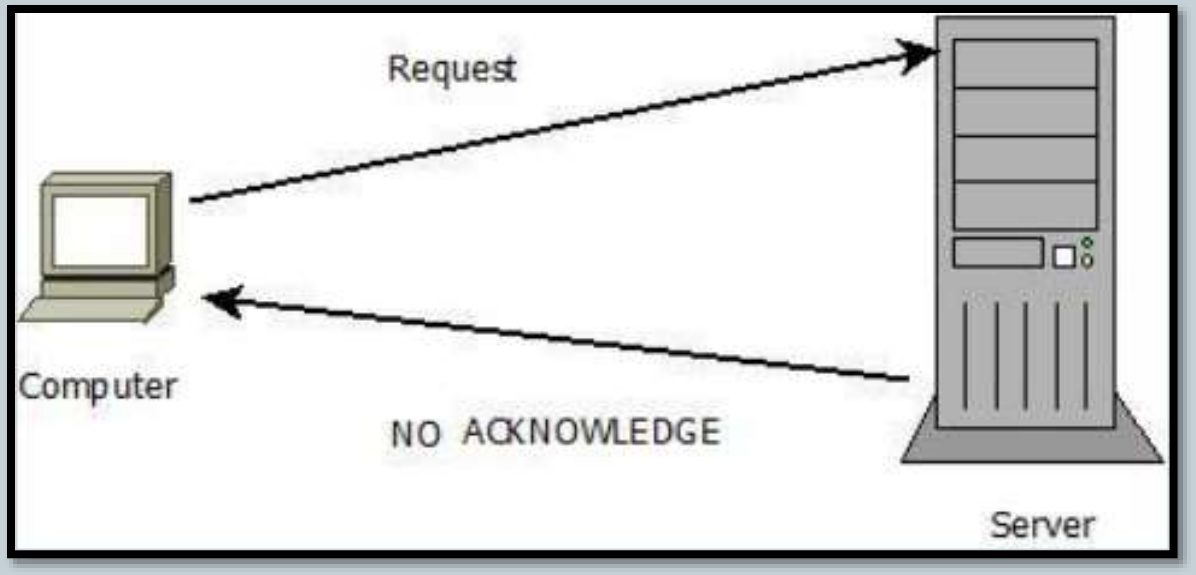
- **ACCEPT:** Packet is accepted and goes to the application for processing.

Targets

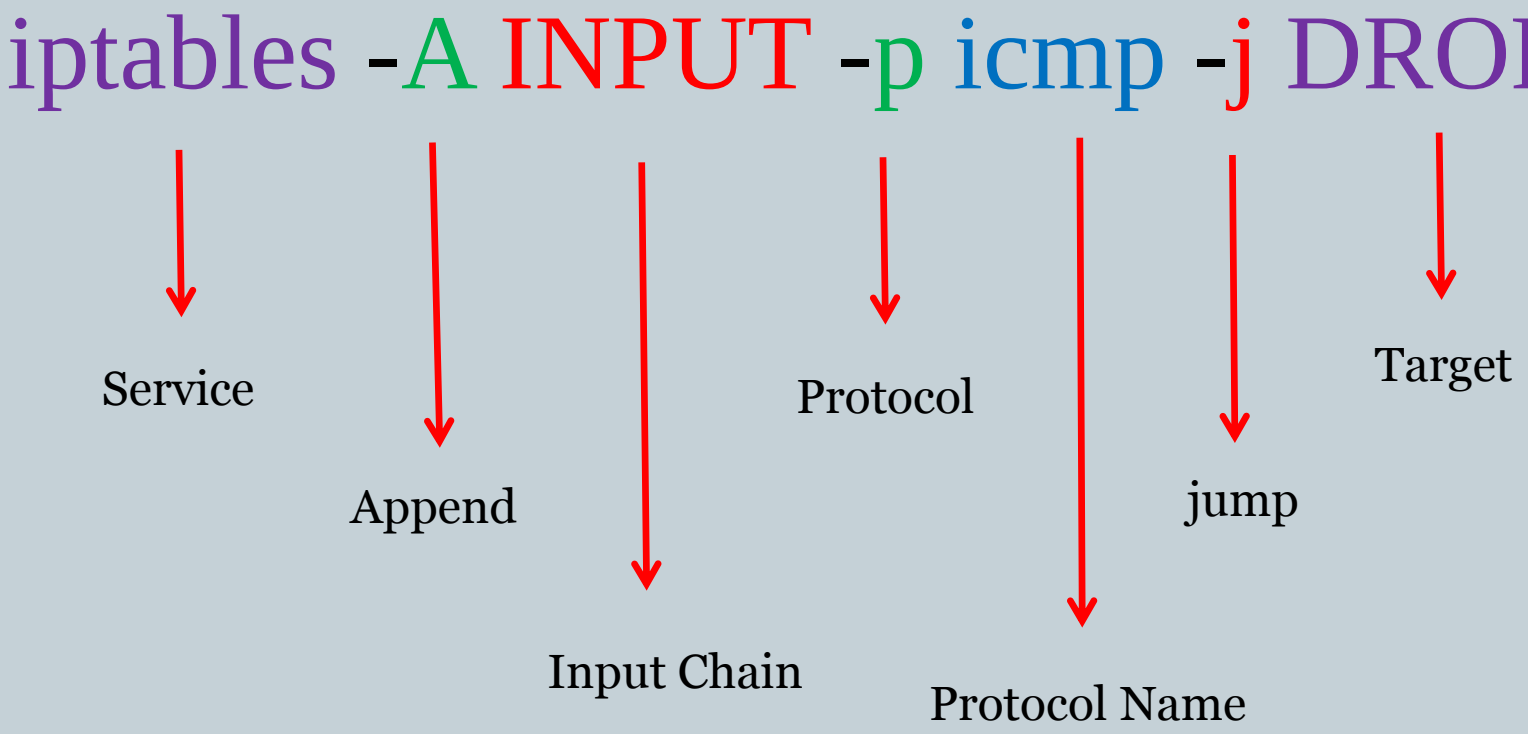
- **DROP:** Packet is dropped. No information regarding the drop is sent to the sender.
- **REJECT:** Packet is dropped and information (error) message is sent to the sender.
- **LOG:** Packet details are sent to for logging.
- **DNAT:** Rewrites the destination IP of the packet
- **SNAT:** Rewrites the source IP of the packet

Examples-1 (DROP)

- iptables -A INPUT -p icmp -j DROP

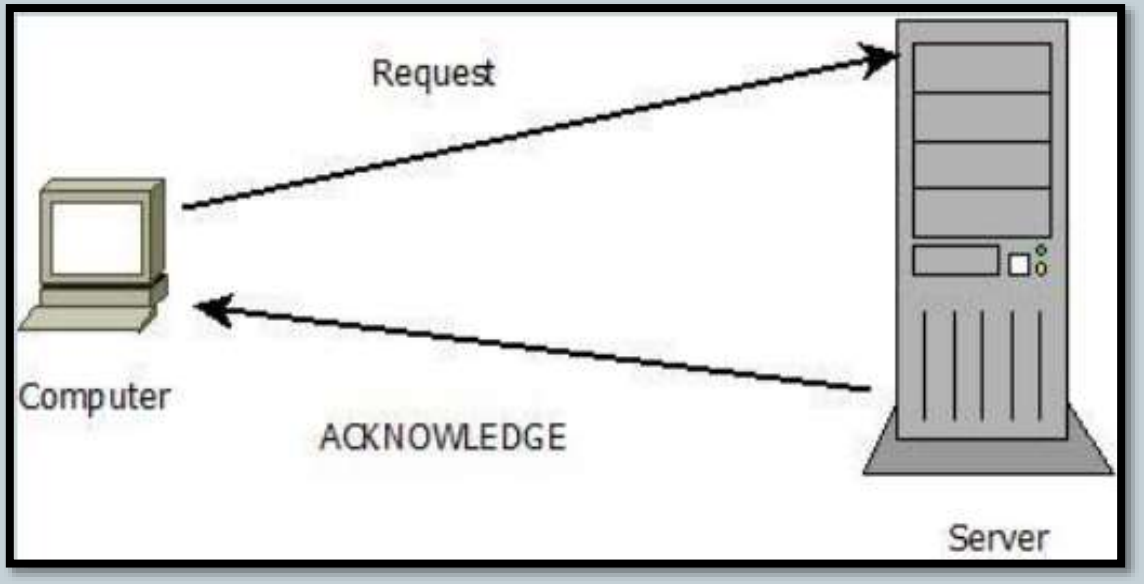


Examples-1 (DROP)

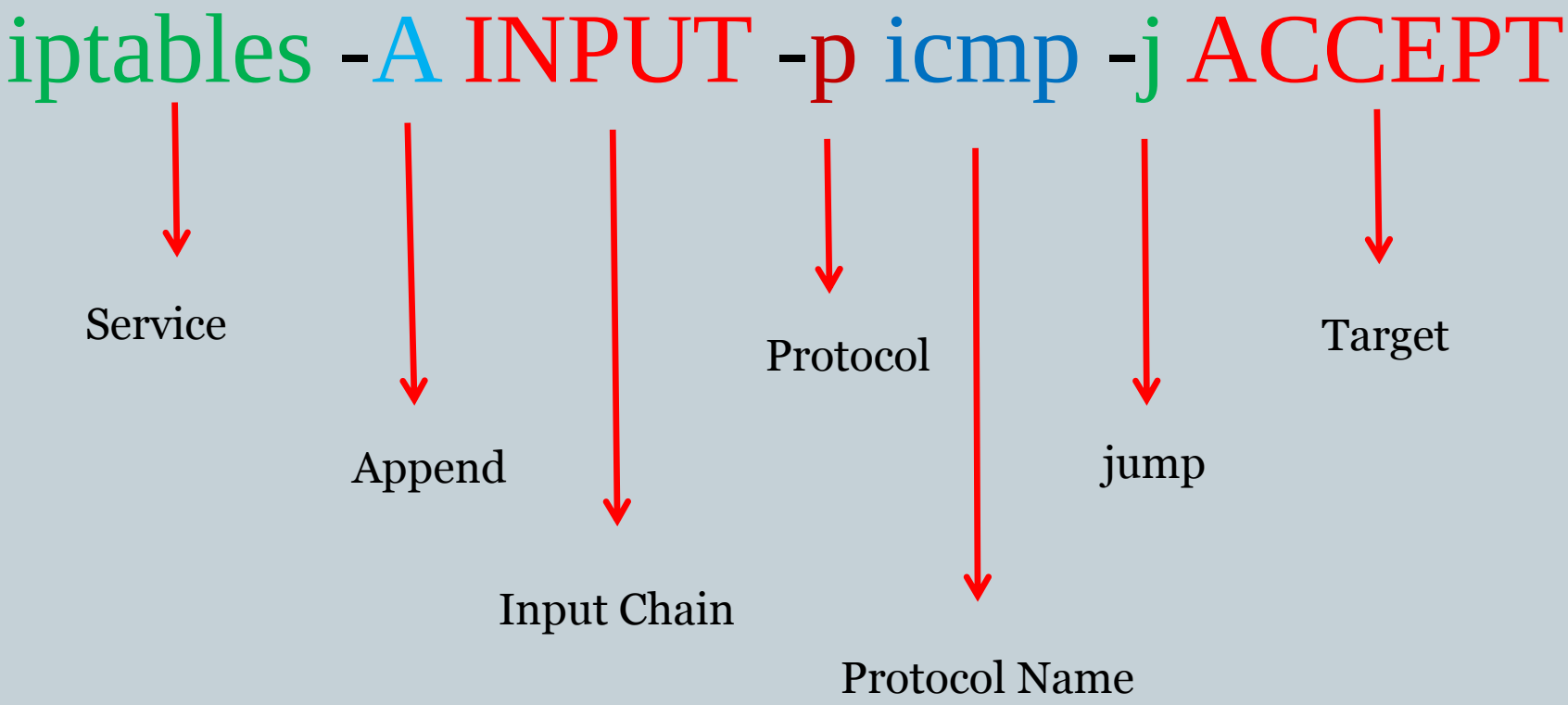


Examples-2 (ACCEPT)

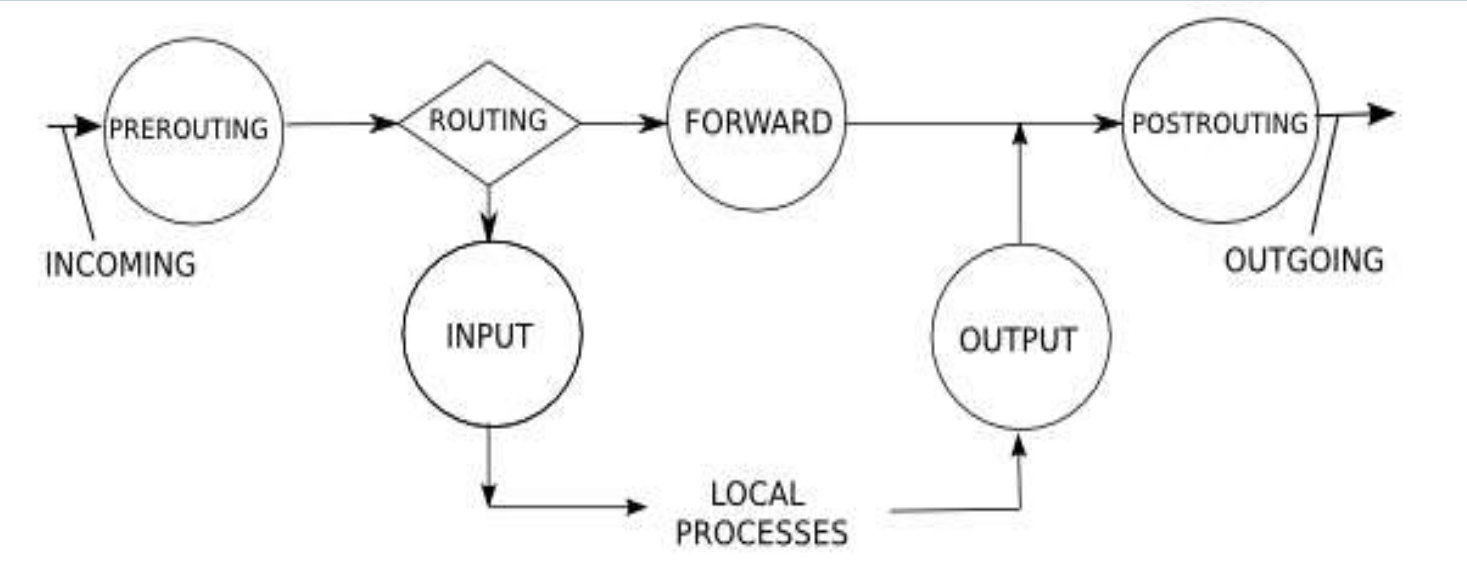
- **iptables -A INPUT -p icmp –j ACCEPT**



Examples-2 (ACCEPT)



Flowchart


PREROUTING
ROUTING
FORWARD
POSTROUTING
INCOMING
OUTGOING
INPUT
OUTPUT
LOCAL
PROCESSES

THANK YOU