**What is a firewall**

* **Security Barrier**: A firewall acts as a barrier between a trusted internal network and untrusted external networks, like the internet.
* **Traffic Control**: It monitors and controls incoming and outgoing network traffic based

on predefined security rules.

* **Protection Levels**: Firewalls provide different levels of protection, from basic packet filtering to more

advanced stateful inspection and application layer filtering.

* **Prevents Unauthorized Access**: It prevents unauthorized users and malicious software from

accessing private networks or devices.

* **Network Security Essential**: Firewalls are essential for network security, helping to defend against various cyber threats such as hacking attempts, malware, and data breaches.
* A firewall is a specialized network security device that acts as a barrier between a trusted internal network and untrusted external networks, such as the internet.
* It inspects all incoming and outgoing traffic and applies predefined security rules to determine whether to allow or block specific data packets.
* This proactive approach helps organizations enforce security policies, mitigate risks from potential cyber threats, and maintain the confidentiality and availability of their network resources

Firewall Terminology

* Understanding firewall terminology is crucial for effective network security management.
* Key terms include packet filtering, where data packets are inspected and either permitted or denied based on predefined rules.
* Stateful inspection enhances security by monitoring the state of active connections and validating incoming packets against established sessions.
* Access Control Lists (ACLs) are rules defining which traffic is allowed or blocked based on criteria such as IP addresses, ports, and protocols.
* The Demilitarized Zone (DMZ) is a network segment that isolates publicly accessible servers from the internal network, offering an additional layer of protection."

Understanding IP Addresses

* IP addresses are fundamental identifiers assigned to devices connected to a network, enabling communication between them.
* IPv4 addresses, such as 192.168.1.1, and IPv6 addresses, like 2001:0db8:85a3:0000:0000:8a2e:0370:7334, uniquely identify each device.
* They play a crucial role in routing data across networks, ensuring messages reach their intended destinations efficiently.
* Understanding IP addressing helps network administrators manage and troubleshoot connectivity issues, ensuring smooth and secure communication within their networks.

LAN vs WAN

* Local Area Networks (LANs) and Wide Area Networks (WANs) are two primary types of network architectures.
* LANs typically cover a small geographic area, such as an office building or a home, connecting devices like computers and printers. In contrast, WANs span larger distances, often connecting multiple LANs across cities or countries via telecommunications links or satellite connections. LANs offer high-speed connectivity within confined spaces, while WANs provide broader coverage, facilitating global communication and access to remote resources

Internet Traffic

* Internet traffic refers to the exchange of data between devices connected to the internet. This includes various activities such as web browsing, email communication, file transfers, and multimedia streaming. Each interaction involves data packets traveling between source and destination devices across multiple networks. Managing internet traffic efficiently is essential for optimizing network performance, ensuring timely data delivery, and safeguarding against security threats like unauthorized access and data breaches.

IP Header

* "The IP header is a crucial component of the IP packet structure, containing essential information for routing and delivering data packets across networks. It includes source and destination IP addresses, identifying the sending and receiving devices, and the protocol field specifying the type of data being transmitted, such as TCP or UDP. Understanding the IP header allows network administrators to troubleshoot connectivity issues, analyze network traffic patterns, and implement security measures to protect against unauthorized access and data manipulation."

TCP (Transmission Control Protocol)

* "TCP (Transmission Control Protocol) is a core communication protocol used in internet protocol (IP) networks. It ensures reliable and ordered delivery of data packets by establishing and maintaining connections between devices. TCP incorporates mechanisms like error-checking, flow control, and congestion avoidance to guarantee data integrity and efficient transmission. Applications such as web browsing, email, and file transfer rely on TCP for seamless data exchange, making it indispensable for modern network communications."

TCP Header

* "The TCP header is part of the TCP segment structure, responsible for managing communication between devices. It includes essential fields such as source and destination ports, identifying the sending and receiving applications, sequence numbers for data ordering, and acknowledgment numbers confirming receipt of data. By examining the TCP header, network administrators can monitor and optimize network performance, detect potential security threats, and troubleshoot connectivity issues effectively."

What is iptables?

* iptables is a command-line tool for managing the firewall built into the Linux kernel. It allows administrators to create chained rules that regulate both inbound and outbound network traffic.
* These rules form a strong security system by specifying which network packets are allowed and which are denied. By doing so, iptables helps safeguard Linux systems against data breaches, unauthorized access, and various network security threats.
* Network administrators utilize iptables to implement security policies and defend Linux systems from different types of network-based attacks.

**How Does iptables Work?**

iptables operates by applying rules to decide how to handle a network packet. The utility is organized into several components:

* 1. Tables: These are collections of related rules, each containing multiple chains.
  2. Chains: Chains are sequences of rules within a table. When a packet arrives, iptables selects the appropriate table and processes the packet through the chain of rules until it finds a match.
  3. Rules: These are specific conditions that packets are compared against to determine a match. Once matched, the packet is directed to a target.
  4. Targets: Targets dictate the action taken on a packet—whether to accept, drop, or reject it.

1. **Tables**

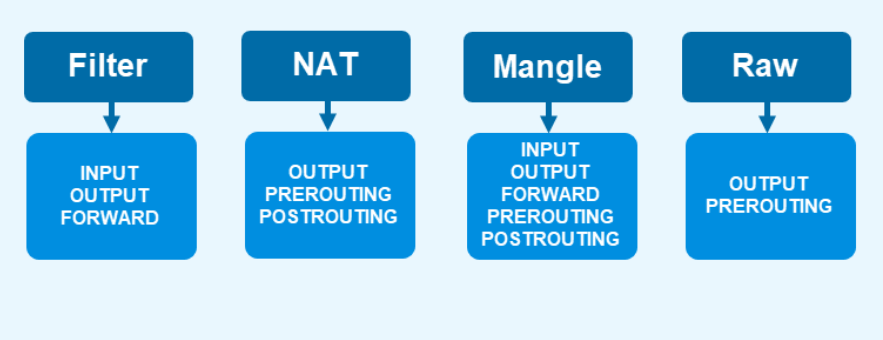
iptables in Linux uses four default tables to handle various rule chains:

* + **Filter**: This is the main table for packet filtering. It determines which packets are allowed to pass through or are blocked from entering or leaving the network.
  + **Network Address Translation (NAT)**: Holds rules for NAT, which directs packets to other networks and is used for modifying packets.
  + **Mangle**: Adjusts properties in the IP headers of packets for specialized handling.
  + **Raw**: Skips connection tracking for certain packets to enhance performance.

2. **Chains**

Chains are lists of rules within tables, guiding how packets should be handled at various stages of processing. Each chain has a unique role:

* + **INPUT**: Deals with incoming packets that are destined for a local application or service. Found in the filter and mangle tables.
  + **OUTPUT**: Controls outgoing packets generated by local applications or services. This chain is present in all tables.
  + **FORWARD**: Manages packets that pass through the system, traveling from one network interface to another. Found in the filter, mangle, and security tables.
  + **PREROUTING**: Modifies packets before they are routed, i.e., before any routing decisions are made. Located in the NAT, mangle, and raw tables.
  + **POSTROUTING**: Changes packets after they have been routed, i.e., after routing decisions are made. Found in the NAT and mangle tables.



**3. Rules**

Rules specify conditions for identifying packets. Each rule belongs to a chain and includes criteria like source or destination IP addresses, port numbers, or protocols. When a packet meets a rule's conditions, it is directed to a target that decides its fate.

**4. Targets**

Targets define what happens to a packet once it matches a rule. Common targets include:

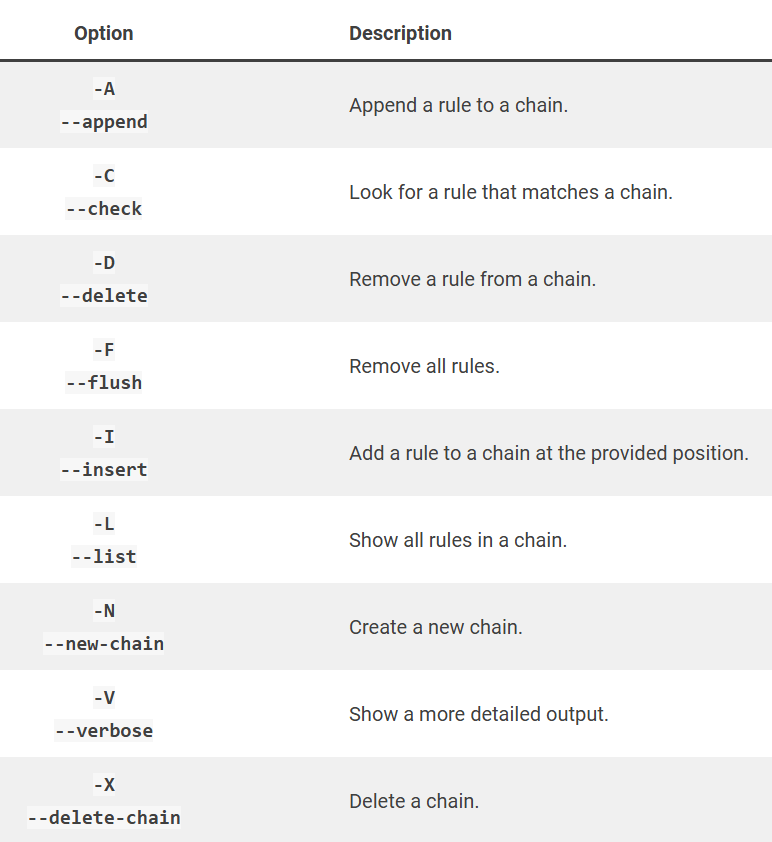
* + **ACCEPT**: Lets the packet proceed through the firewall.
  + **DROP**: Silently discards the packet without notifying the sender.
  + **REJECT**: Discards the packet and sends an error message back to the sender.
  + **LOG**: Logs details about the packet to a log file.
  + **SNAT**: Source Network Address Translation, which changes the packet's source address.
  + **DNAT**: Destination Network Address Translation, which modifies the packet's destination address.
  + **MASQUERADE**: Alters the packet's source address, useful for connections with dynamically assigned IPs.

**How to Install iptables on Linux**

* sudo apt install iptables

iptables Syntax and Options

* An iptables command looks as follows:
* iptables [options] [chain] [criteria] -j [target]



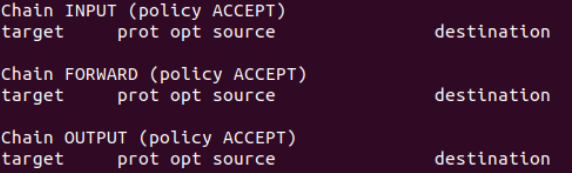
**How to Configure iptables on Linux**

* The iptables command applies actions to the filters table by default. To use a different table, add the -t option followed by the table name (for example, use -t nat for the NAT table).
* View Current Rules

To view the current rules, use the command with the -L option:

sudo iptable –L



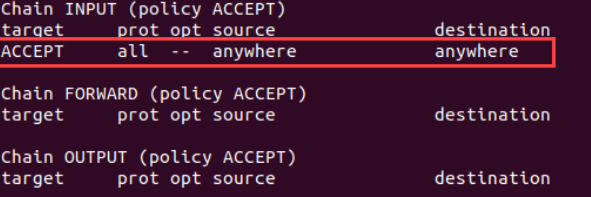


**Enable Loopback Traffic**

* Allowing traffic from your system (localhost) is secure and allows applications to communicate with the localhost interface. Enter the following to append the INPUT chain:

sudo iptables -A INPUT -i lo -j ACCEPT





**Allow Traffic for Specific Services**

1. Allow HTTP web traffic:

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

2. Allow only incoming SSH (Secure Shell) traffic:

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

3. Allow HTTPS traffic:

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

**Control Traffic by IP Addres**

1.Accept all traffic from an IP address:

sudo iptables -A INPUT -s [IP-address] -j ACCEPT

2. Drop traffic from an IP address:

sudo iptables -A INPUT -s [IP-address] -j DROP

3. Reject traffic from an IP address range:

sudo iptables -A INPUT -m iprange --src-range [IP-address-range] -j REJECT

**Block All Incoming Traffic Except SSH**

To block all incoming traffic, except for SSH connections, do the following:

1. Set the default policy for the INPUT chain to DROP:

sudo iptables -P INPUT DROP

2. Allow SSH connections:

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

3. Allow related and established connections:

sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT