**What is iptables?**

iptables is a **firewall tool** in **Linux**.  
It controls **network traffic** — what’s allowed in or out of your computer or server.

Think of it like a **security guard** for network packets:

* “You can come in” ✅
* “You can’t go out” ❌

**🔍 How it works (in short)**

Linux has a system called **Netfilter** inside the kernel (the core of Linux).  
iptables is the **user command** to control Netfilter rules.

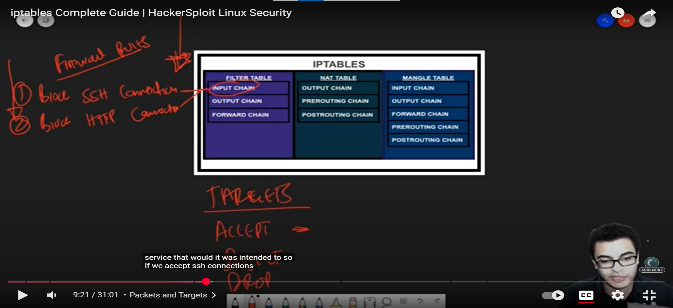
Traffic flows through **tables** → which contain **chains** → which contain **rules**.

**📊 Structure**

| **Table** | **Purpose** | **Common Chains** |
| --- | --- | --- |
| filter | Main table for allowing/blocking | INPUT, OUTPUT, FORWARD |
| nat | Used for address translation (e.g. port forwarding) | PREROUTING, POSTROUTING |
| mangle | Modify packets (advanced) | INPUT, OUTPUT, etc. |
| raw | For connection tracking control | PREROUTING, OUTPUT |

**🔧 Common Chains**

| **Chain** | **Description** |
| --- | --- |
| INPUT | Traffic **coming into** your system |
| OUTPUT | Traffic **going out** from your system |
| FORWARD | Traffic **passing through** your system (e.g., router) |

**🪄 Common Commands**

**1. View current rules**

sudo iptables -L -v -n

**2. Allow traffic**

Example: allow SSH (port 22)

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

**3. Block traffic**

Example: block all incoming HTTP (port 80)

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

**4. Allow specific IP**

sudo iptables -A INPUT -s 192.168.1.10 -j ACCEPT

**5. Block specific IP**

sudo iptables -A INPUT -s 203.0.113.5 -j DROP

**6. Save your rules**

Different systems use different commands:

sudo iptables-save > /etc/iptables/rules.v4

(or service iptables save on older systems)

**7. Clear all rules**

⚠️ Be careful — this removes all firewall rules.

sudo iptables -F

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT ACCEPT