**Linux Firewall Configuration**

**Commands Summary**

sudo apt install ufw -y # Install UFW

sudo ufw enable # Enable UFW

sudo ufw status verbose # View rules

sudo ufw deny 23/tcp # Block Telnet (port 23)

telnet localhost 23 # Test the block (optional)

sudo ufw allow 22/tcp # Allow SSH (port 22)

sudo ufw delete deny 23/tcp # Remove Telnet block rule

**Summary: How Firewall Filters Traffic**

A **firewall** is a network security system that monitors and controls network traffic based on predefined rules. It serves as a protective barrier between a trusted internal network and potentially harmful external networks, such as the internet. By filtering traffic, a firewall helps prevent unauthorized access, data breaches, and various forms of cyberattacks.

Firewalls work by inspecting **network packets**—small units of data transmitted over a network—and deciding whether to **allow**, **deny**, or **drop** the packets based on specified rules. These rules can be based on multiple criteria, including:

* **Port numbers** (e.g., allowing HTTP traffic on port 80, blocking Telnet on port 23)
* **IP addresses or IP ranges** (e.g., blocking traffic from a specific malicious IP)
* **Protocols** (e.g., TCP, UDP, ICMP)
* **Direction of traffic** (inbound or outbound)

There are two main types of firewall rule policies:

* **Allow by default**, blocking only specified ports or IPs.
* **Deny by default**, allowing only explicitly defined traffic (more secure).

In Linux environments, tools like **UFW (Uncomplicated Firewall)** provide a simplified interface to configure firewall rules, making it user-friendly for administrators and beginners. For example, using UFW, one can easily block access to insecure services like Telnet (port 23) and ensure access to essential services like SSH (port 22).

By filtering traffic in this way, firewalls:

* Reduce the system’s attack surface
* Enforce access control policies
* Prevent exploitation of known vulnerabilities
* Contribute to overall network and system security

In summary, firewalls are a critical component of any secure computing environment, enabling administrators to tightly control how data enters and leaves the system.