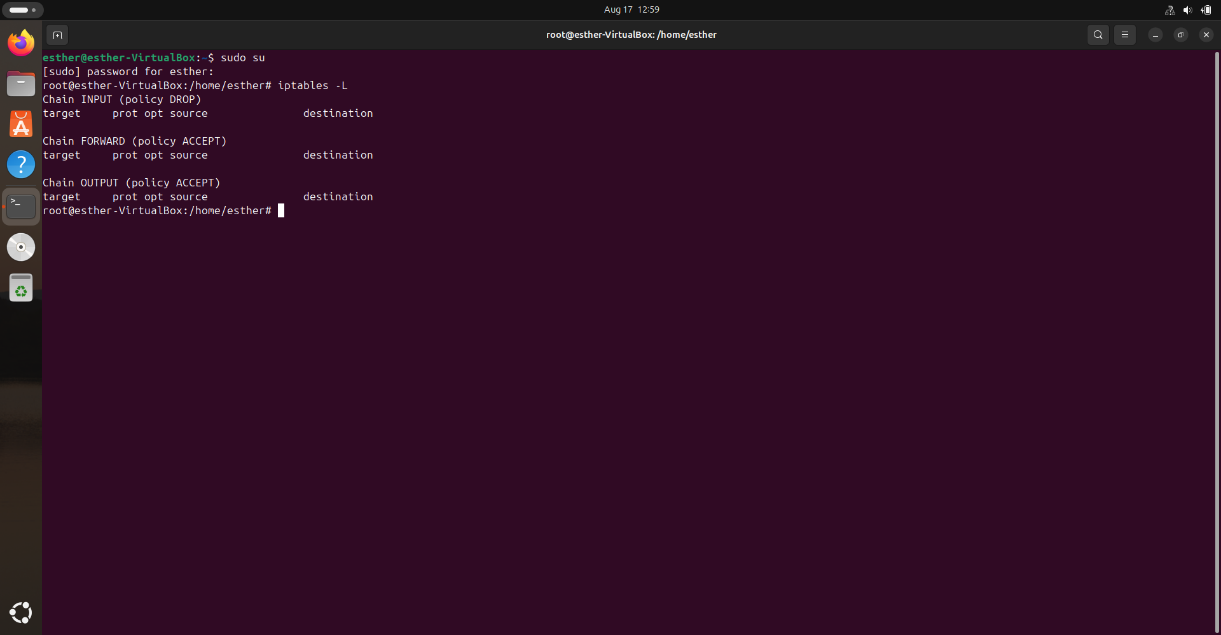
**FIREWALL RULES WITH IPTABLES**

* 1. Definition:

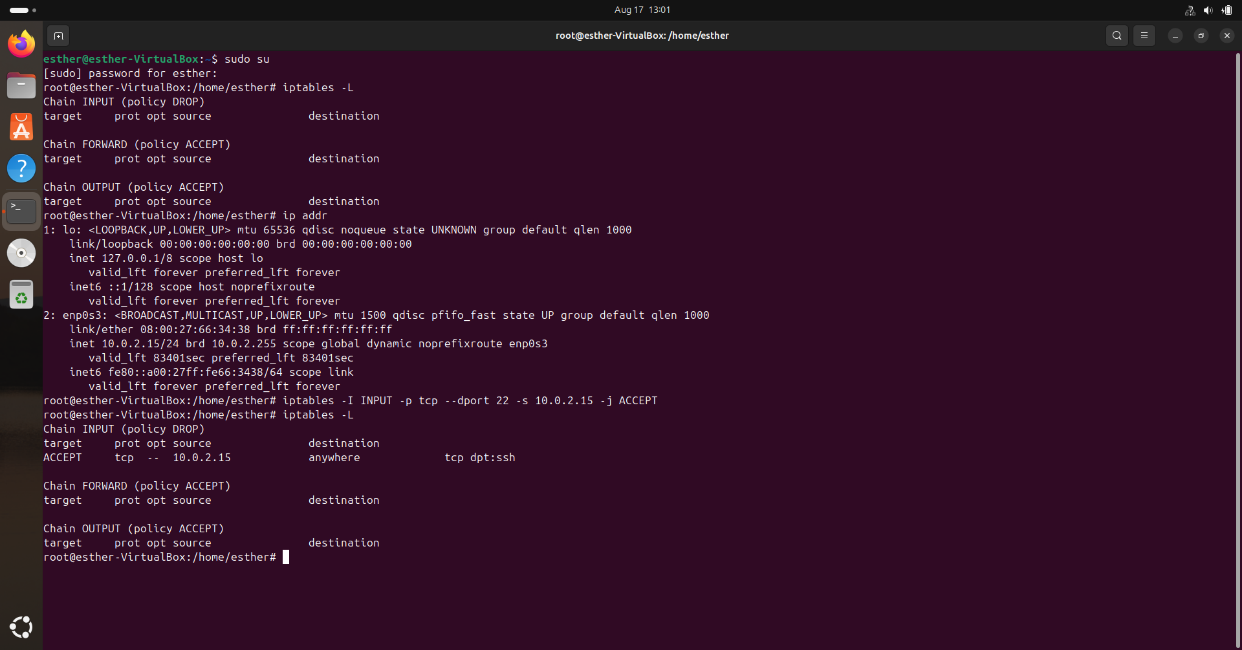
Firewall Rules with IPTables refers to the configuration and management of rules that control network traffic on a Linux system using the iptables utility. Iptables is a command-line tool that interacts with the Linux kernel's netfilter framework to define policies for incoming and outgoing packets.

* 1. Functions of IPTables:
* Block or allow traffic based on criteria such as IP address, port number, and protocol type.
* Redirect traffic to specific addresses or ports, often used in NAT (Network Address Translation).
* Track the state of connections (e.g., new, established) to allow or deny packets based on connection state.
* Monitor and log packet activity, useful for detecting and diagnosing network issues or security breaches.
* Control traffic that is forwarded between interfaces, typically in routers and gateway systems.
  1. Tools Required:-
* Iptables: Core tool for managing firewall rules.
* Text Editor: nano or vim for editing configuration files.
* Networking Tools: netstat, nmap, tcpdump for testing and analysis.

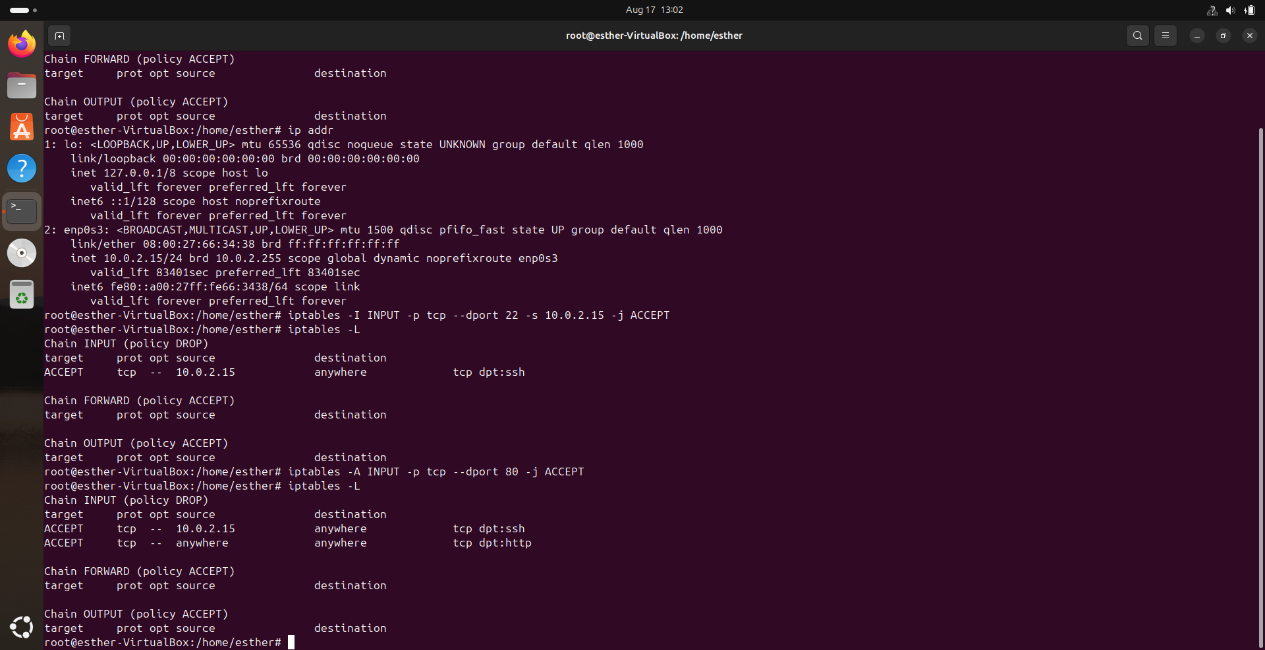
* 1. PROCEDURE:-

**STEP 1:** To configure iptables, switch to the root user to have administrative privileges for configuring firewall rules using ‘sudo su’. The default policy for the INPUT chain is set to DROP, meaning all incoming traffic is blocked unless explicitly allowed by a rule

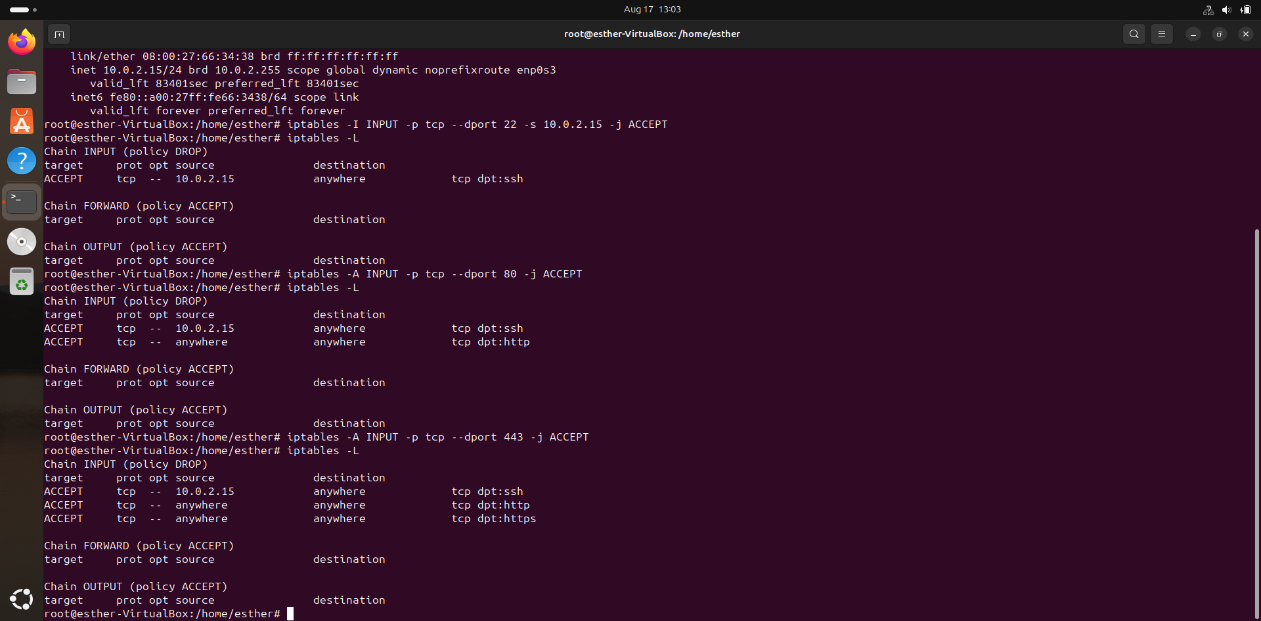
**STEP 2:** Retrieve your IP address to set up specific access rules. Allow SSH from a specified IP to secure remote management.



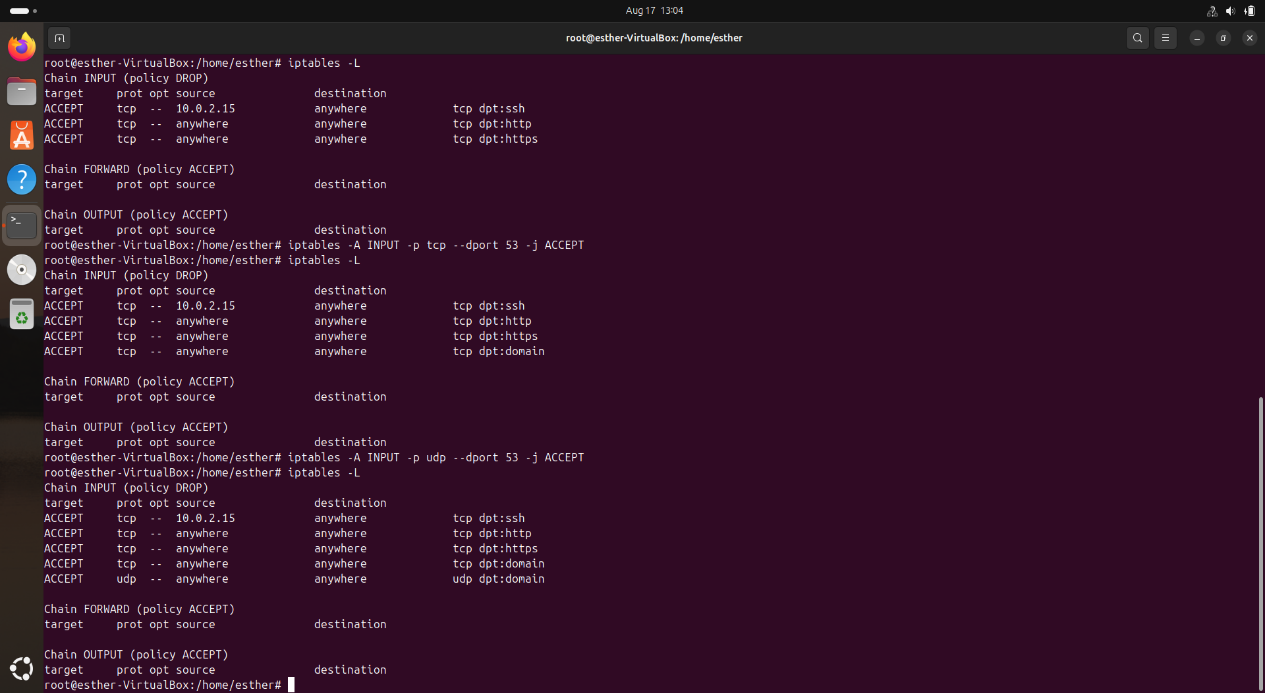
**STEP 3:** This command appends a rule to the INPUT chain to accept TCP traffic on port 80 (the default port for HTTP). This rule ensures that web servers or clients can access web services hosted on your machine.



**STEP 4:** This command appends a rule to the INPUT chain to accept TCP traffic on port 443 (the default port for HTTPS). This rule is important for secure web communication and ensures that secure web services can be accessed.



**STEP 5:** The first command allows DNS traffic over TCP on port 53. While DNS typically uses UDP, TCP is used for larger queries and responses. The second command allows DNS traffic over UDP on port 53. DNS usually operates over UDP for most queries.



These rules ensure that your machine can send and receive DNS queries to resolve domain names into IP addresses.

Configuring firewall rules with iptables is essential for managing network security and controlling traffic to and from your Linux system

Configuring iptables involves setting rules to manage incoming and outgoing network traffic. By switching to the root user, identifying IP addresses, and adding rules for SSH, HTTP, HTTPS, and DNS, you secure your system while allowing essential services. Setting the default policy to DROP ensures only specified traffic is permitted. To maintain these settings, save your rules for persistence across reboots.