Roll No – 06

Name – Prasad Sunil Arote

Date – 13/10/2023

Lab Assignment 11

AIM: To study and configure Firewalls using IP tables.

LO6: Demonstrate network security system using open source tools.

THEORY:

What is a Firewall?

A firewall is a type of cybersecurity tool used to filter traffic on a network. Firewalls can separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having unique pros and cons.

Different types of Firewall

Type 1: Packet-Filtering Firewalls

Packet filtering firewalls operate at the network layer (Layer 3) of the OSI model. They examine network packets and make filtering decisions based on criteria such as source and destination IP addresses, port numbers, and protocols. These firewalls can allow or block traffic based on predefined rules.

Type 2: Stateful Inspection Firewall:

Stateful firewalls operate at the network layer (Layer 3) and transport layer (Layer 4). They keep track of the state of active connections and make decisions based on the state of the connection. This allows stateful firewalls to better understand and control complex traffic flows and prevent unauthorized access.

Proxy Firewall:

Proxy firewalls, also known as application-level gateways (ALGs), operate at the application layer (Layer 7). They act as intermediaries between internal and external systems, forwarding requests and responses on behalf of clients. This can enhance security by not exposing the internal network's IP addresses.

Application Layer Firewall: Application layer firewalls, also known as deep packet inspection firewalls, are highly advanced and operate at the application layer (Layer 7). They can understand and filter traffic based on specific application protocols. This allows them to provide granular control over application-specific traffic, making them effective at detecting and blocking application-layer threats.

Write the different options that can be used in configuring firewall?

When configuring a firewall, you can use various options and parameters to define rules and policies that control the traffic entering and exiting your network. The specific options available can vary depending on the firewall software or device you're using, but here are some common options and parameters:

Source Address (-s): You can specify the source IP address or range of IP addresses from which traffic is allowed or denied.

Destination Address (-d): This option allows you to define the destination IP address or IP address range for which the rule applies.

Protocol (-p): You can specify the network protocol, such as TCP, UDP, or ICMP, to which the rule applies.

Source Port (--sport): Define the source port or port range from which the traffic originates.

Destination Port (--dport): Specify the destination port or port range to which the traffic is headed.

Action (-j): Determine what action to take if a packet matches the rule. Common actions include ACCEPT, DROP, REJECT, and LOG. For example, -j ACCEPT allows the packet, while -j DROP discards it.

Interface In (-i): Define the incoming network interface where the traffic should be filtered.

Interface Out (-o): Specify the outgoing network interface for filtering outbound traffic.

Stateful Inspection (-m state): This option is used in stateful inspection firewalls to track the state of established connections. It is typically used with -p to define the protocol.

Logging (-j LOG): You can log information about packets matching a rule for analysis and auditing. Logging rules are often used with the -j LOG target.

Match Extensions (-m): Some firewalls support extensions or modules that allow you to match packets based on specific criteria. These extensions provide additional filtering capabilities, such as -m tcp, -m udp, or -m multiport.

Default Policy (-P): Set the default action for packets that do not match any of the configured rules. Common policies include ACCEPT and DROP.

Connection Tracking (-m conntrack): In stateful firewalls, this option allows you to match packets based on their connection state (e.g., NEW, ESTABLISHED, RELATED).

Time-Based Rules: Some firewalls support time-based rules that allow you to control traffic based on the time of day or specific schedules.

User and Group-Based Rules: In more advanced firewalls, you can configure rules based on user or group identities, providing fine-grained control over access.

Write the commands used for configuring firewall using IPTABLES?

iptables is a popular command-line tool for configuring a firewall on Linux systems. It allows you to set up rules to control incoming and outgoing network traffic. Below are some common iptables commands for configuring a firewall. Please note that to use these commands, you typically need superuser or root privileges (e.g., using sudo).

Flush Existing Rules: Before setting up your firewall rules, it's a good practice to flush existing rules to start with a clean slate. Use the following command to do this:

```
sudo iptables -F
```

Set Default Policies:

To set the default policy for incoming traffic (e.g., deny all incoming traffic by default):

```
sudo iptables -P INPUT DROP
```

To set the default policy for outgoing traffic (e.g., allow all outgoing traffic by default):

```
sudo iptables -P OUTPUT ACCEPT
```

Allow SSH (Port 22): To allow incoming SSH traffic, which is essential for remote server access:

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

Allow HTTP (Port 80) and HTTPS (Port 443): To permit web traffic:

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

Allow Established and Related Connections: To allow incoming traffic related to established connections, which is crucial for established connections to work:

```
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

Save Rules: After configuring your firewall rules, save them to ensure they persist after a reboot. This command depends on your Linux distribution. For example, on Ubuntu, you can use:

```
sudo netfilter-persistent save
```

On CentOS/RHEL:

```
sudo service iptables save
```

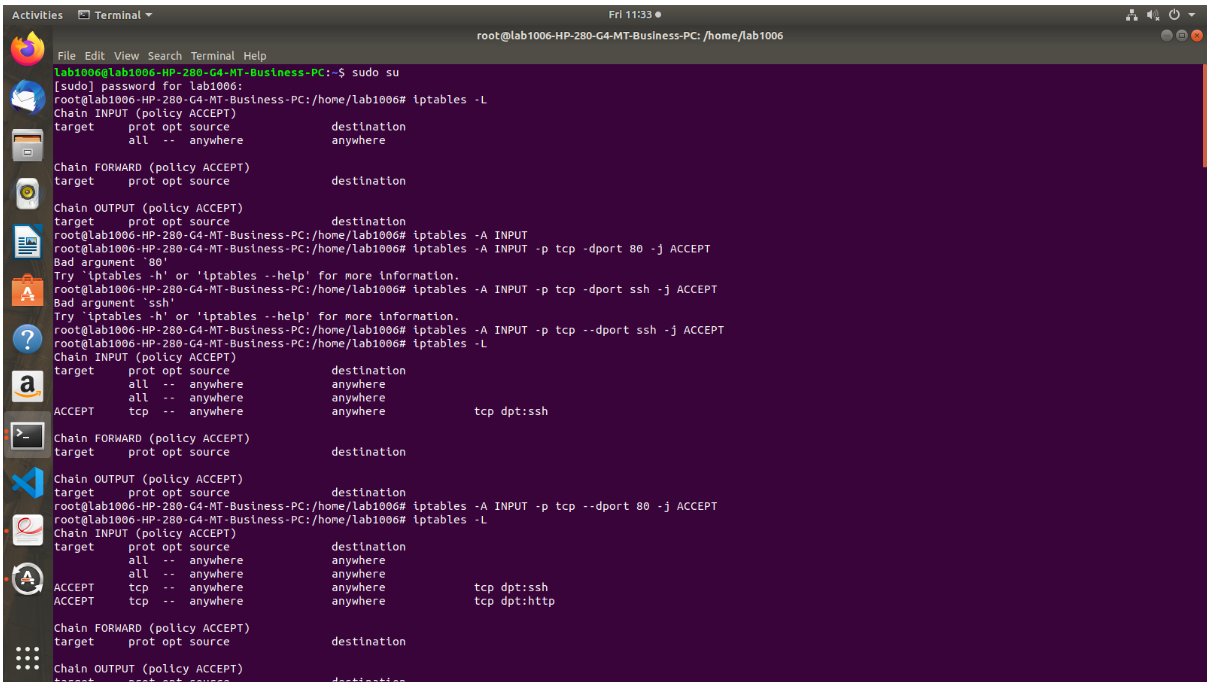
On some distributions, you might need to install iptables-persistent for rule persistence.

List Rules: To view the configured rules, use the following command:

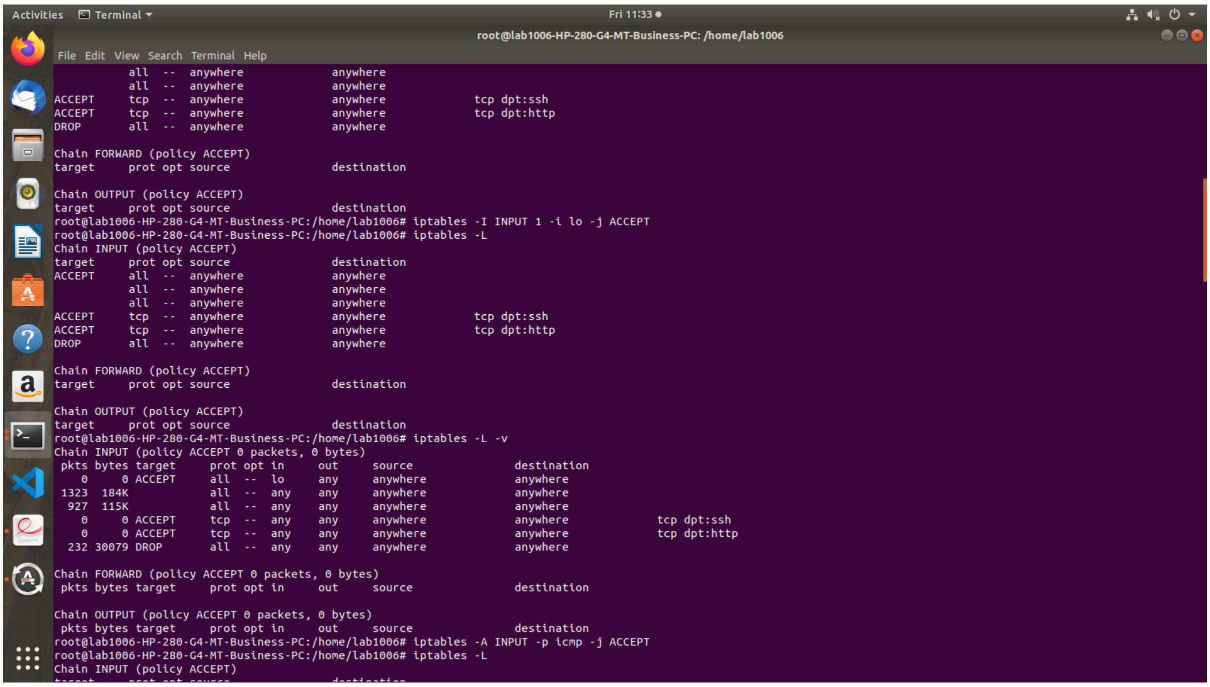
```
sudo iptables -L
```

Delete a Rule: To delete a specific rule, identify its number from the list generated by iptables -L and use the -D option. Replace N with the rule number:

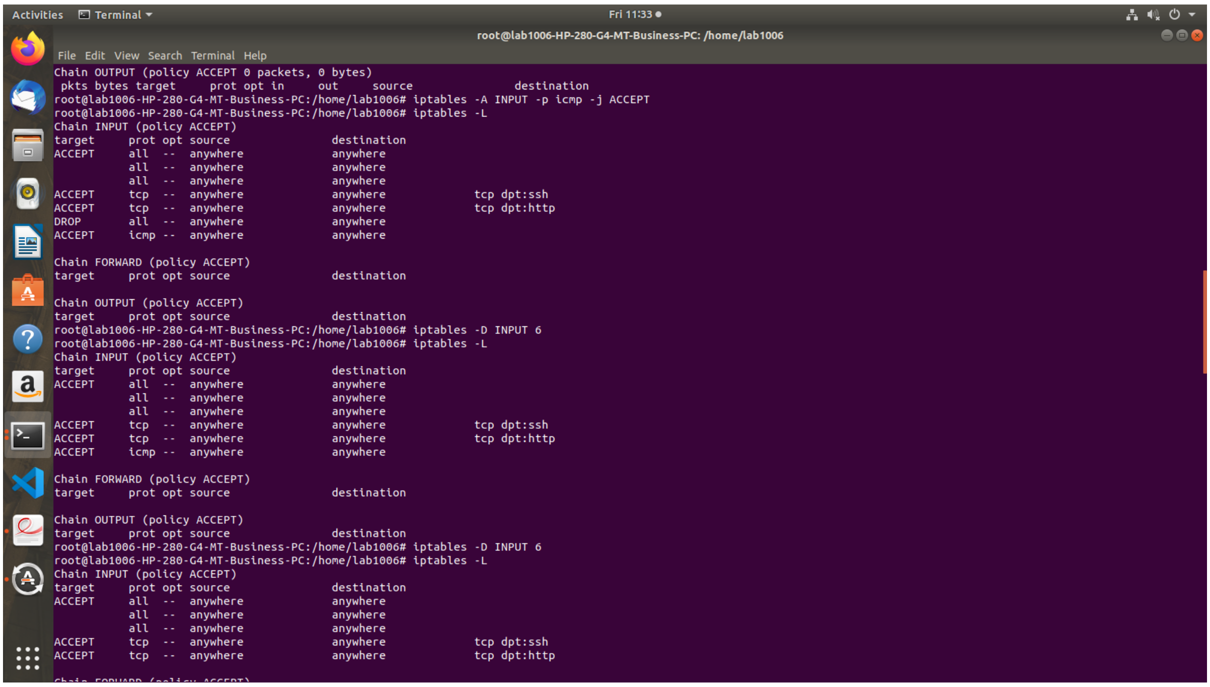
```
sudo iptables -D INPUT N
```


Activities
Terminal
Fri 11:33
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

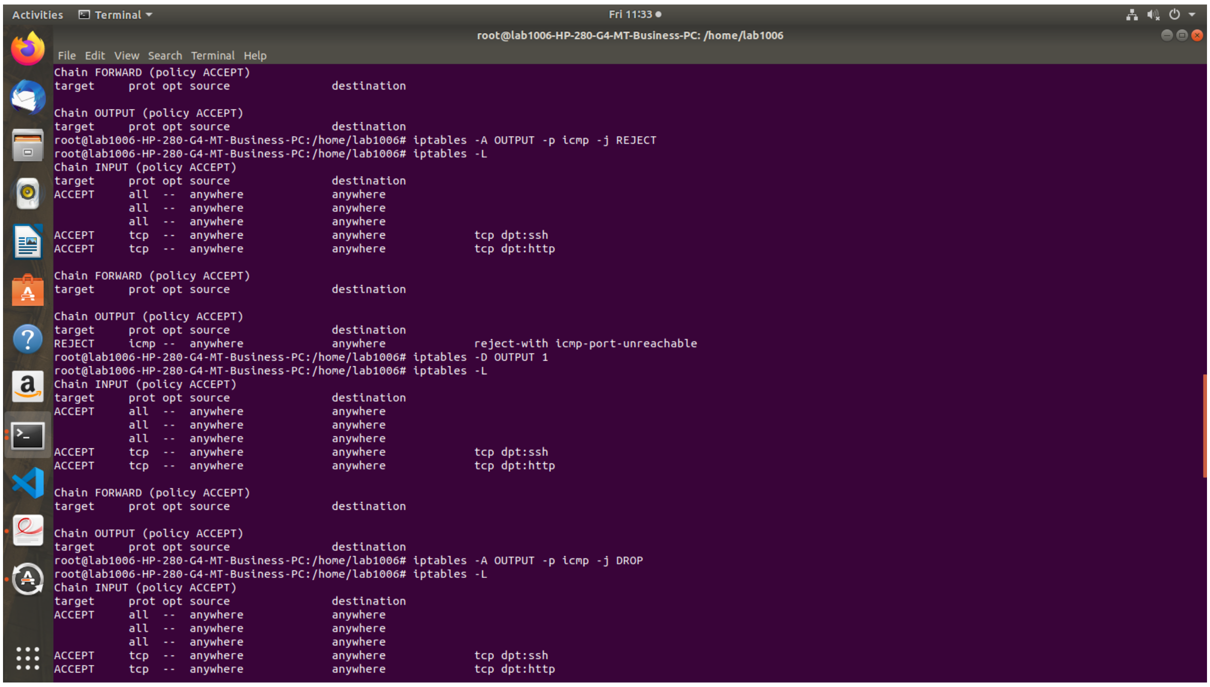
```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo su
[sudo] password for lab1006:
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
           all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A INPUT
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A INPUT -p tcp -dport 80 -j ACCEPT
Bad argument `80'
Try `iptables -h' or 'iptables --help' for more information.
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A INPUT -p tcp -dport ssh -j ACCEPT
Bad argument `ssh'
Try `iptables -h' or 'iptables --help' for more information.
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A INPUT -p tcp --dport ssh -j ACCEPT
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
           all  --  anywhere             anywhere
           all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
           all  --  anywhere             anywhere
           all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```


Activities
Terminal
Fri 11:33
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

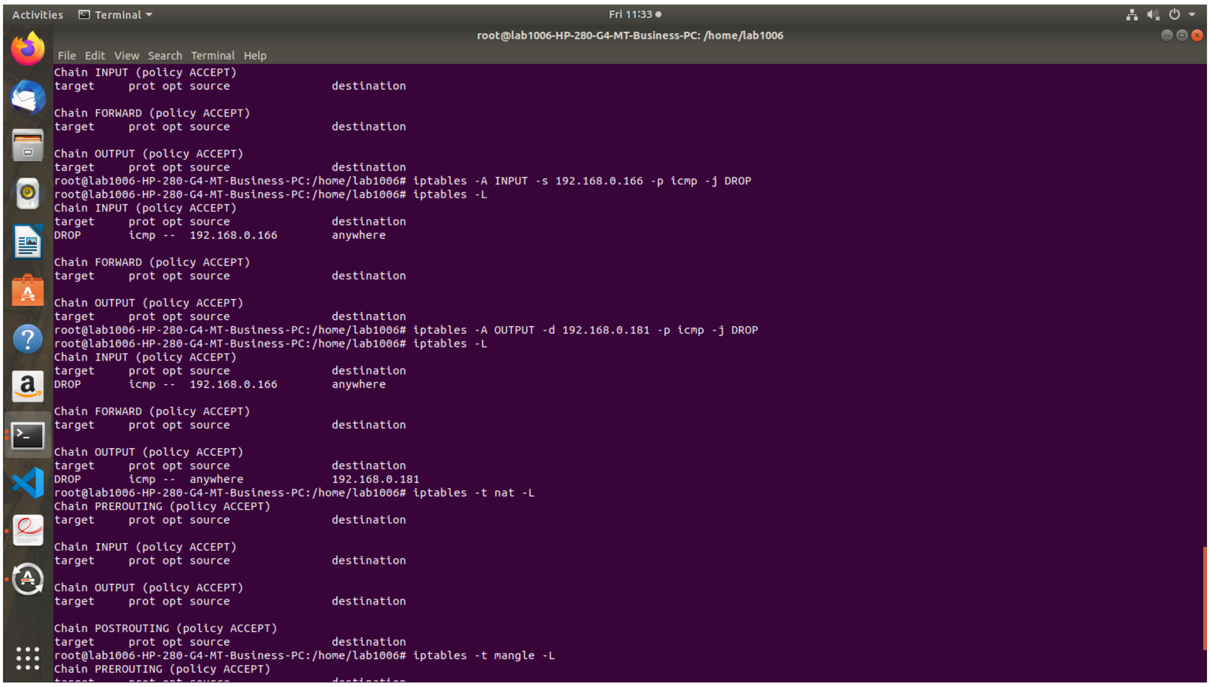
```
           all  --  anywhere             anywhere
           all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -I INPUT 1 -i lo -j ACCEPT
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
           all  --  anywhere             anywhere
           all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
 1323  184K            all  --  any    any     anywhere             anywhere
  927  115K            all  --  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:http
  232 30079 DROP       all  --  any    any     anywhere             anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A INPUT -p icmp -j ACCEPT
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
```


Activities
Terminal
Fri 11:33
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

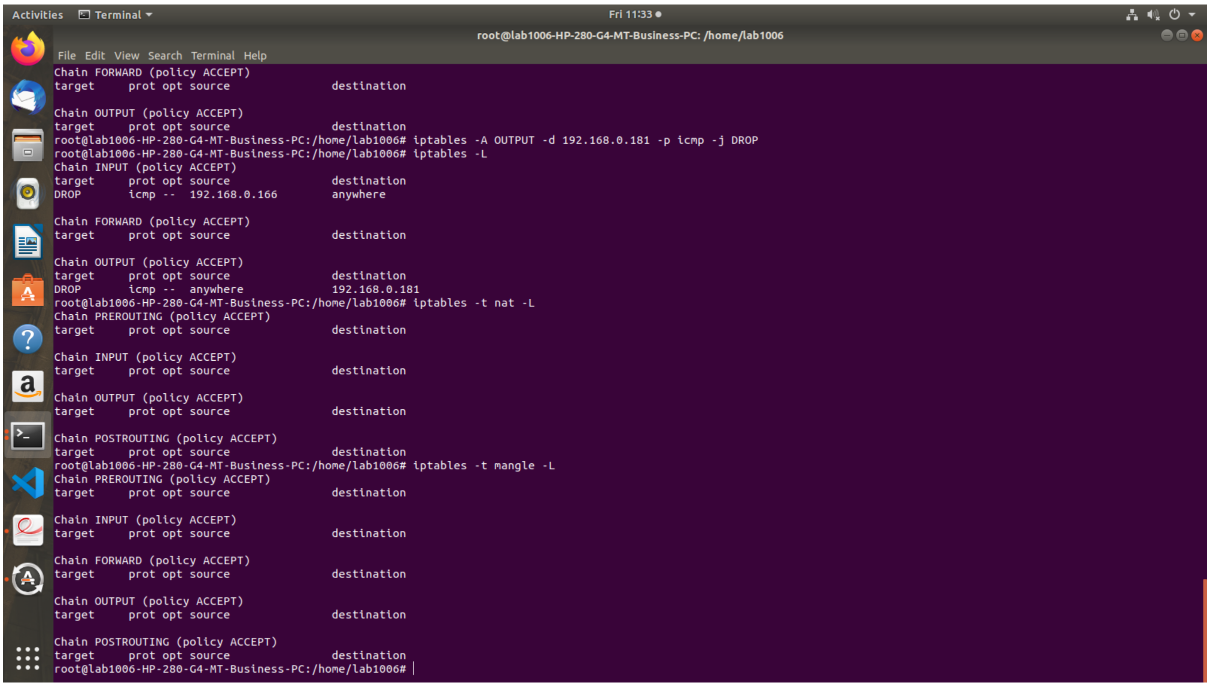
```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A INPUT -p icmp -j ACCEPT
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
           all  --  anywhere             anywhere
           all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
DROP       all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -D INPUT 6
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
           all  --  anywhere             anywhere
           all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     icmp --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -D INPUT 6
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
           all  --  anywhere             anywhere
           all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
```


Activities
Terminal
Fri 11:33
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A OUTPUT -p icmp -j REJECT
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
           all  --  anywhere             anywhere
           all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     icmp --  anywhere             anywhere             reject-with icmp-port-unreachable
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -D OUTPUT 1
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
           all  --  anywhere             anywhere
           all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A OUTPUT -p icmp -j DROP
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
           all  --  anywhere             anywhere
           all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
```


Activities
Terminal
Fri 11:33
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A INPUT -s 192.168.0.166 -p icmp -j DROP
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  192.168.0.166        anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A OUTPUT -d 192.168.0.181 -p icmp -j DROP
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  192.168.0.166        anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             192.168.0.181
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -t mangle -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
```


Activities
Terminal
Fri 11:33
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A OUTPUT -d 192.168.0.181 -p icmp -j DROP
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  192.168.0.166        anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             192.168.0.181
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -t mangle -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 
```

CONCLUSION:

Firewalls are essential components in network security, serving as a crucial defense against cyber threats. They come in various types, each tailored to specific security needs. The choice of firewall and its configuration options depend on the specific requirements of the network or system to be protected. Configuring firewalls should be done with careful consideration of security policies and best practices, as well as an understanding of the firewall software or device in use.