Roll no. : 53
Name: Shreya Kamath
Date: 19th October, 2023.

LAB ASSIGNMENT NO. 10

AIM: To study and configure Firewalls using IP tables.

LAB OUTCOME ATTAINED:

LO 6: Demonstrate the network security system using open source tools.

THEORY:

A **Firewall** is a network security device or software that monitors and controls incoming and outgoing network traffic. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet. Firewalls are designed to enforce security policies, filter traffic based on rules, and protect the network from unauthorised access, threats, and malicious activity.

Different types of firewalls include:

1. Packet Filtering Firewalls: These firewalls filter traffic based on attributes of individual network packets, such as source and destination IP addresses, port numbers, and protocol types.

2. Stateful Inspection Firewalls: Stateful firewalls keep track of the state of active connections and make decisions based on the context of the traffic. They can determine if a packet is part of an established connection and allow or deny it accordingly.

3. Proxy Firewalls: Proxy firewalls act as intermediaries between internal and external networks. They receive network requests on behalf of clients, inspect and filter the traffic, and forward it to the destination. This adds an additional layer of security.

4. Next-Generation Firewalls (NGFW): NGFWs combine traditional firewall capabilities with advanced security features such as intrusion detection, application-layer filtering, and deep packet inspection.

5. Application Layer Gateways (ALG): ALGs work at the application layer and understand specific application protocols. They can provide more granular control over application traffic.

6. Web Application Firewalls (WAF): WAFs are specialised firewalls designed to protect web applications from various web-based attacks, such as SQL injection and cross-site scripting (XSS).

7. Cloud Firewalls: Cloud providers offer firewall services for virtual machines and resources in cloud environments, allowing users to define network security rules.

Different options used in configuring a firewall can include:

- Allow Rules: Define which traffic is permitted to pass through the firewall.
- Deny Rules: Specify which traffic is blocked or rejected.
- Port-Based Rules: Control traffic based on specific ports (e.g., allowing traffic on port 80 for HTTP).
- IP Address-Based Rules: Filter traffic by source or destination IP addresses.

- Protocol Rules: Restrict traffic based on the protocol or service (e.g., allowing only FTP or SSH traffic).
- Stateful Rules: Track and allow or deny traffic based on the state of connections.
- Logging and Monitoring: Configure logging rules to keep records of allowed and denied traffic for auditing and analysis.
- Security Groups: In cloud environments, security groups are used to control inbound and outbound traffic to resources.

Commands for configuring a firewall using IPTABLES

1. To list existing rules:
   iptables -L

2. To allow incoming traffic on a specific port (e.g., port 80 for HTTP):
   iptables -A INPUT -p tcp --dport 80 -j ACCEPT

3. To deny incoming traffic on a specific port (e.g., port 22 for SSH):
   iptables -A INPUT -p tcp --dport 22 -j DROP

4. To save the rules:
   service iptables save

5. To restart the firewall:
   service iptables restart

These commands are just examples, and configuring a firewall with IPTABLES can be complex and requires careful consideration of security policies and network requirements. It's essential to understand the potential impact of firewall rules on your network.

Roll no. : 53
Name: Shreya Kamath
Date: 19th October, 2023.

SCREENSHOTS:

```
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 -A INPUT -p tcp --dpo
rt ssh -j ACCEPT
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# IPTABLES -l
IPTABLES: command not found
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
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#
```

Roll no. : 53
Name: Shreya Kamath
Date: 19th October, 2023.

```
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File  Edit  View  Search  Terminal  Help
IPTABLES: command not found
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
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 --dpo
rt 80 -j ACCEPT
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
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 INPUT -p icmp --dp
ort 80 -j ACCEPT
iptables v1.6.1: unknown option "--dport"
Try `iptables -h' or 'iptables --help' for more information.
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A INPUT -j DROP
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -l
iptables v1.6.1: unknown option "-l"
Try `iptables -h' or 'iptables --help' for more information.
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
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#
```

Roll no. : 53
Name: Shreya Kamath
Date: 19th October, 2023.

```
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File  Edit  View  Search  Terminal  Help
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 A
CCEPT
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
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

   14  1000 ACCEPT     all  --  lo     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
  780  104K 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 34 packets, 2428 bytes)
 pkts bytes target     prot opt in     out     source               destination

root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

Roll no. : 53
Name: Shreya Kamath
Date: 19th October, 2023.

```
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File  Edit  View  Search  Terminal  Help
ACCEPT     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

   14  1000 ACCEPT     all  --  lo     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
  780  104K 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 34 packets, 2428 bytes)
 pkts bytes target     prot opt in     out     source               destination

root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# man iptables
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -D INPUT 1
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
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#
```

Roll no. : 53
Name: Shreya Kamath
Date: 19th October, 2023.

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

Roll no. : 53
Name: Shreya Kamath
Date: 19th October, 2023.

```
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File  Edit  View  Search  Terminal  Help
CCEPT
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
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# ping 192.168.92.17
PING 192.168.92.17 (192.168.92.17) 56(84) bytes of data.
^C
--- 192.168.92.17 ping statistics ---
89 packets transmitted, 0 received, 100% packet loss, time 90114ms

root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -A INPUT -p icmp -j D
ROP
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
DROP       all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere
DROP       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# ping 192.168.92.17
PING 192.168.92.17 (192.168.92.17) 56(84) bytes of data.
^C
--- 192.168.92.17 ping statistics ---
25 packets transmitted, 0 received, 100% packet loss, time 24563ms

root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# ping www.google.com
ping: www.google.com: Name or service not known
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

Roll no. : 53
Name: Shreya Kamath
Date: 19th October, 2023.

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
DROP       all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere
DROP       icmp --  anywhere             anywhere
DROP       tcp  --  anywhere             anywhere
^[[A^[[A^C
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# iptables -F
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# ping 192.168.0.153
PING 192.168.0.153 (192.168.0.153) 56(84) bytes of data.
64 bytes from 192.168.0.153: icmp_seq=1 ttl=64 time=0.455 ms
64 bytes from 192.168.0.153: icmp_seq=2 ttl=64 time=0.529 ms
64 bytes from 192.168.0.153: icmp_seq=3 ttl=64 time=0.538 ms
64 bytes from 192.168.0.153: icmp_seq=4 ttl=64 time=0.527 ms
64 bytes from 192.168.0.153: icmp_seq=5 ttl=64 time=0.527 ms
64 bytes from 192.168.0.153: icmp_seq=6 ttl=64 time=0.528 ms
64 bytes from 192.168.0.153: icmp_seq=7 ttl=64 time=0.534 ms
64 bytes from 192.168.0.153: icmp_seq=8 ttl=64 time=0.576 ms
64 bytes from 192.168.0.153: icmp_seq=9 ttl=64 time=0.528 ms
64 bytes from 192.168.0.153: icmp_seq=10 ttl=64 time=0.532 ms
64 bytes from 192.168.0.153: icmp_seq=11 ttl=64 time=0.527 ms
64 bytes from 192.168.0.153: icmp_seq=12 ttl=64 time=0.572 ms
64 bytes from 192.168.0.153: icmp_seq=13 ttl=64 time=0.531 ms
64 bytes from 192.168.0.153: icmp_seq=14 ttl=64 time=0.529 ms
64 bytes from 192.168.0.153: icmp_seq=15 ttl=64 time=0.484 ms
64 bytes from 192.168.0.153: icmp_seq=16 ttl=64 time=0.573 ms
^C
--- 192.168.0.153 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15337ms
rtt min/avg/max/mdev = 0.455/0.530/0.576/0.038 ms
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

CONCLUSION:

In summary, firewalls are essential for network security, offering protection against external threats. Different firewall types and configuration options provide flexibility in safeguarding networks. Understanding firewall management tools like IPTABLES is crucial for effective rule creation and maintenance. Well-configured firewalls are fundamental in maintaining network security and enforcing access control policies.