Task 10: Firewall Configuration & Testing

NAME : KARTHIK P DATE : 30-01-2026

Firewall Configuration & Testing – Task 10 Report

1. Objective

The objective of this task is to configure a host-based firewall**, define allow/deny rules for specific ports and IP addresses, test connectivity, observe logs, and document the impact of each rule to build practical firewall management skills.** ~~2~~ ~~1~~

2. Environment Details

- **Internship Task: Cyber Security Internship – Task 10 Firewall Configuration & Testing** ~~[1]~~
- **Firewall Type: Host-based firewall**
- **Tool Used (example – edit as per your setup):**
  - **Option A UFW Uncomplicated Firewall) on Ubuntu/Debian Linux** ~~3~~ ~~4~~
  - **Option B Windows Defender Firewall on Windows** ~~5~~

You should clearly mention which one you actually used on your system.

3. Firewall Concepts Used

- Firewall: **A security mechanism (hardware or software) that monitors and controls network traffic based on predefined security rules, sitting between trusted and untrusted networks to enforce access policies.** ~~6~~ ~~2~~
- Stateful filtering: **Tracks the state of connections (e.g. NEW, ESTABLISHED ; return traffic for an allowed connection is automatically permitted.** ~~7~~ ~~8~~
- Stateless filtering: **Evaluates each packet individually without remembering previous packets; both directions must be explicitly allowed by rules.** ~~7~~
- Inbound rules: **Control traffic coming into the system from the network (e.g. allowing HTTP to a web server).** ~~9~~ ~~5~~
- Outbound rules: **Control traffic going out from the system to the network (e.g. blocking an app from reaching the internet).** ~~10~~ ~~9~~

4. Configuration Steps

4.1 Default Policy Configuration UFW example)

Commands used (edit if needed):[11] [4] [3]

```
sudo apt update
sudo apt install ufw

# Set default policies
sudo ufw default deny incoming
sudo ufw default allow outgoing
```

Impact:

- **All unsolicited inbound connections are blocked by default, reducing the attack surface.**
- **Outbound connections remain allowed, so normal user activities (browsing, updates) continue to work.**[2]

4.2 Allowing Essential Services

Example rules configured:[3] [11]

```
# Allow SSH (remote management)
sudo ufw allow 22/tcp

# Allow web traffic
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
```

Impact:

- **SSH 22/tcp is reachable for administrative access.**
- **HTTP 80/tcp and HTTPS 443/tcp) are accessible so the host can serve web content.**

4.3 Denying Insecure / Unwanted Ports

Example rules:[11] [2]

```
# Deny Telnet (insecure remote access)
sudo ufw deny 23/tcp
```

Impact:

- **Any attempt to connect to port 23 is blocked, preventing use of insecure Telnet service.**

4.4 Blocking a Malicious IP

Example rule (replace IP with the one you used):[2]

```
sudo ufw deny from 203.0.113.10
```

Impact:

- **All traffic from the specified IP address is dropped, simulating blocking a known malicious source.**

4.5 Enabling Firewall and Viewing Rules

```
sudo ufw enable
sudo ufw status numbered
```

Impact:

- **Activates the firewall with the configured rule set.**
- `status numbered` **shows active rules with IDs, which is useful for later deletion or modification.**[12]

Add screenshot of `ufw status numbered` **in your repo and reference it here.)**

5. Logging and Monitoring

5.1 Enabling Logging

```
sudo ufw logging on
```

UFW writes log entries to `/var/log/ufw.log` **on Ubuntu.**[13] [14]

5.2 Observing Logs

```
sudo tail -f /var/log/ufw.log
```

Observations (example):

- **Successful connections to allowed ports 22, 80, 443) appear as allowed packets.**
- **Blocked attempts to port 23 or from the malicious IP generate log entries showing dropped packets.**[2]

You can include a short anonymized snippet or screenshot of the log to demonstrate this.)

6. Connectivity Testing

6.1 Outbound Connectivity

- ping google.com **– Confirmed outbound ICMP and DNS traffic is allowed (from “allow outgoing” default policy).** ~~4~~ ~~3~~
- **Web browsing from the host worked as expected.**

6.2 Inbound Service Testing

From another machine (or using nmap**):** [3]

- **Checked open ports:**
  - nmap -p 22,80,443 <server-ip>
  - **Result: ports 22, 80, 443 show as** open **(matching allow rules).**
- **Attempted connection to blocked Telnet port 23**
  - nmap-p 23 <server-ip> **shows** closed **or** filtered **indicating the firewall is blocking the p ort.** [3] [2]

6.3 Malicious IP Simulation

- **From the blocked IP (or a simulated host configured with that IP , connection attempts to the server failed.**
- **Corresponding log entries showed dropped packets for that source address in** /var/log/ufw.log. ~~2~~

Describe the exact commands/tests you ran and support with screenshots.)

7. Windows Firewall Variant (if you used Windows)

If you did the task on Windows instead of UFW, document steps like: [15] [5] [9]

- **Opened** Windows Defender Firewall with Advanced Security**.**
- **Created** Inbound Rule**:**
  - **Type: Port → TCP → Local port 80 → Allow the connection → Applied to Domain/Private/Public** → Named Allow_HTTP_80.
- **Created** Inbound Rule **to block Telnet:**
  - **Port 23 → Block the connection → All profiles →** Block_Telnet_23.
- **Created** Outbound Rule **to restrict web traffic for testing:**
  - **Port 80/443 TCP → Block the connection.**

Then add:

- **Test results (browser blocked, ping behavior).**

- Screenshots of the rule list and connection tests.

8. Rule Summary Table

You can include a table like this in your report:

Rule ID	Direction	Source	Destination	Protocol	Port (s)	Action	Purpose
1	Inbound	Any	This host	TCP	22	Allow	Allow SSH remote administration. ~~11~~
2	Inbound	Any	This host	TCP	80	Allow	Allow HTTP web traffic. ~~11~~
3	Inbound	Any	This host	TCP	443	Allow	Allow HTTPS secure web traffic. 11
4	Inbound	Any	This host	TCP	23	Deny	Block insecure Telnet service. ~~2~~
5	Inbound	203.0.113.10	This host	Any	Any	Deny	Block simulated malicious IP. ~~2~~
6	Outbound	This host	Any	Any	Any	Allow	Default allow outgoing connections. ~~2~~

Adjust IDs, IPs, and ports to match your real configuration.

9. Impact Analysis

- Reduced attack surface: By setting deny incoming by default and only allowing required ports 22, 80, 443 , unnecessary services are not exposed to the internet. ~~4 3 2~~
- Protection from insecure protocols: Denying Telnet 23/tcp prevents use of an unencrypted remote access protocol that could leak credentials. ~~2~~
- Source-based blocking: Blocking a malicious IP shows how firewalls can quickly cut off traffic from known bad sources or ongoing attacks such as brute-force attempts. ~~2~~
- Network visibility: Logs from UFW or Windows Firewall provide insight into allowed and denied traffic, useful for incident investigation and tuning rules. ~~16 12~~
- Limitations: The firewall cannot stop attacks that use allowed ports (e.g. web application vulnerabilities over HTTP/HTTPS) or attacks originating from inside the host, so it must be combined with patching, secure coding, and endpoint protection. ~~17 10 3~~

10. Interview Question Snapshot

- What is a firewall?

  Afirewallisa security control that filters network traffic between different zones based on rules, allowing only authorized communication and blocking unwanted connections. ~~6~~ ~~2~~

- Stateful vs stateless firewall?

  Statefulfirewallsmaintainconnection state and automatically allow return traffic for established sessions, whereas stateless firewalls evaluate each packet on its own without remembering previous packets. ~~8~~ ~~7~~

- Why are firewalls needed?

  Theyenforce least-privilegenetwork access, separate internal networks from untrusted networks, and reduce exposure to attacks by controlling which ports, protocols, and IPs can communicate. ~~4~~ ~~3~~ ~~2~~

- What is an inbound/outbound rule?

  Inbound rules control trafficarrivingat the host from the network, while outbound rules control traffic leaving the host towards external systems. ~~5~~ ~~9~~

- Can a firewall stop all attacks?

  No.Firewalls primarilycontrol network flows; attacks via allowed ports, malicious insiders, or vulnerabilities in applications can still succeed, so multiple security layers are required. ~~17~~ 10 3