Objective: Configure and test basic firewall rules to allow/block specific network traffic using:

:**Windows Firewall**

:**UFW (Uncomplicated Firewall)** on Linux

Linux (UFW): Configuration

INPUT:

```
# Install and enable UFW
sudo apt update
sudo apt install ufw
sudo ufw enable

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

# Allow SSH, HTTP
sudo ufw allow ssh
sudo ufw allow 80/tcp

# Deny specific IP
sudo ufw deny from 192.168.1.100

# Check status
sudo ufw status numbered
```

OUTPUT:

```
sudo ufw status verbose > ufw_rules.txt
```

```
history | grep ufw > ufw_commands_log.txt
```

2. For Windows Firewall (PowerShell)

Add & View Firewall Rules via PowerShell

powershell

Copy code

Allow inbound HTTP

```
New-NetFirewallRule -DisplayName "Allow HTTP" -Direction Inbound -Protocol TCP -LocalPort 80 -Action Allow
```

Block traffic from specific IP

```
New-NetFirewallRule -DisplayName "Block IP" -Direction Inbound -RemoteAddress 192.168.1.100 -Action Block
```

Export all rules (text)

```
Get-NetFirewallRule | Format-Table -AutoSize > firewall_rules.txt
```

Windows Firewall Configuration

:Allowed: HTTP inbound on port 80

: Blocked: Inbound traffic from 192.168.1.100

PowerShell Commands Used

powershell

Copy code

```
New-NetFirewallRule -DisplayName "Allow HTTP" -Direction Inbound -Protocol TCP -LocalPort 80 -Action Allow
New-NetFirewallRule -DisplayName "Block IP" -Direction Inbound -RemoteAddress 192.168.1.100 -Action Block
```

Basic Firewall Configuration (Windows & Linux)

Objective

To configure and test basic firewall rules to:

- **Allow specific ports (e.g., SSH, HTTP)**
- **Block certain IP addresses**

Linux (UFW) Configuration

Default policy: Deny incoming, Allow outgoing

Allowed: SSH (port 22), HTTP (port 80)

Blocked: IP 192.168.1.100

Commands Used

```bash
sudo ufw default deny incoming
sudo ufw allow 22/tcp
sudo ufw allow 80/tcp
sudo ufw deny from 192.168.1.100
```