Firewalls

This lab involves managing firewall rules using **iptables**, focusing on configuring and testing rule sets to control network traffic. Students will learn to define and apply rules for packet filtering.

Lab setup

This lab requires to setup two virtual machines, The network configuration will be as follows

	Machine A	Machine B
VM Network adapter Network connection	NAT	NAT
VM Network subnet	192.168.0.0/24	192.168.0.0/24
Assigned IP by DHCP	no	no
IP Address	192.168.0.3	192.168.0.4
Subnet mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.0.254	192.168.0.254

Using Firewall

This is the task the linux firewall-iptables operation is required.

Preparation

First, run the following command to flush the iptables policy table and list the policy to ensure the policy table is empty

```
$ sudo iptables -F
$ sudo iptables -L
```

Lab Task

Taks 1: Prevent A from doing telnet to Machine B

Implementation

The following command is used to implement the firewall for the task objective

```
sudo iptables -A OUTPUT -p tcp --dport 23 -d 192.168.0.4 -j DROP
```

The command configures the Linux firewall to block outgoing TCP traffic destined for port 23 (Telnet) on the IP address 192.168.0.4.

- `-A OUTPUT`: Appends a new rule to the OUTPUT chain, which handles packets originating from the local system.
- `-p tcp`: Specifies that the rule applies to TCP protocol packets.
- `--dport 23`: Targets packets destined for port 23, the default port for Telnet services.
- `-d 192.168.0.4`: Applies the rule to packets addressed to the IP 192.168.0.4.
- `-j DROP`: Instructs the firewall to drop matching packets silently, without notifying the sender.

Verification

The verification is start the telnet from machine A to Machine B, the following command is used

```
telnet 192.168.0.4
```

The command result a connection timeout since the tcp packet from machine A to machine B is dropped by the iptables firewall at machine A

Taks 2: Prevent A from visiting an external web site.

Implementation

The following command is used to implement the firewall for the task objective, we use www.estin.dz as target website for testing

```
sudo iptables -A OUTPUT -d www.estin.dz -j REJECT
```