Setup and Use a Firewall on Windows/Linux

Objective

This report documents the configuration and testing of basic firewall rules on two distinct operating systems: Windows Firewall (GUI-based) and Ubuntu Server using UFW (Command-Line). The goal was to configure and test rules to allow (SSH, port 22) and block (Telnet, port 23) specific traffic.

Summary: How Firewalls Filter Traffic

A firewall acts as a security checkpoint for network traffic, determining which packets are allowed to pass and which are blocked. Firewalls operate primarily by examining three key components of a network packet:

1. **Source/Destination IP Address:** Who is sending the traffic, and where is it trying to go.
2. **Protocol (TCP/UDP):** The type of communication being used.
3. **Port Number:** The specific channel being used for the application (e.g., 80 for HTTP, 22 for SSH, 23 for Telnet).

Firewalls operate based on a defined **Rule Set**. When a packet arrives, the firewall compares it against the rules in order (top-down). The first rule that matches the packet's criteria (IP, Protocol, Port) determines the action:

- **ALLOW (Accept):** The packet is permitted to proceed.
- **DENY (Drop):** The packet is silently discarded.
- **REJECT:** The packet is discarded, and an error message is sent back to the sender.

If no rule matches, the firewall applies its **Default Policy** (usually DENY for incoming traffic) for maximum security.

Part 1: Windows Firewall Configuration and Testing

This section documents the Graphical User Interface (GUI) steps and verification for the host machine's firewall.

1.1. GUI Steps: Creating the Outbound Block Rule

To create the test rule, the following GUI steps were performed:

1. Open **Windows Firewall with Advanced Security**.
2. Navigate to **Outbound Rules** in the left pane.
3. Click **New Rule** in the Actions pane.
4. Select **Port** for the rule type, and click Next.
5. Select **TCP** and specify port number 23 for *Specific remote ports*.

6. Select **Block the connection** as the action.
7. Apply the rule to all three profiles (Domain, Private, Public).
8. Name the rule **"Block Port 23 Test"**.

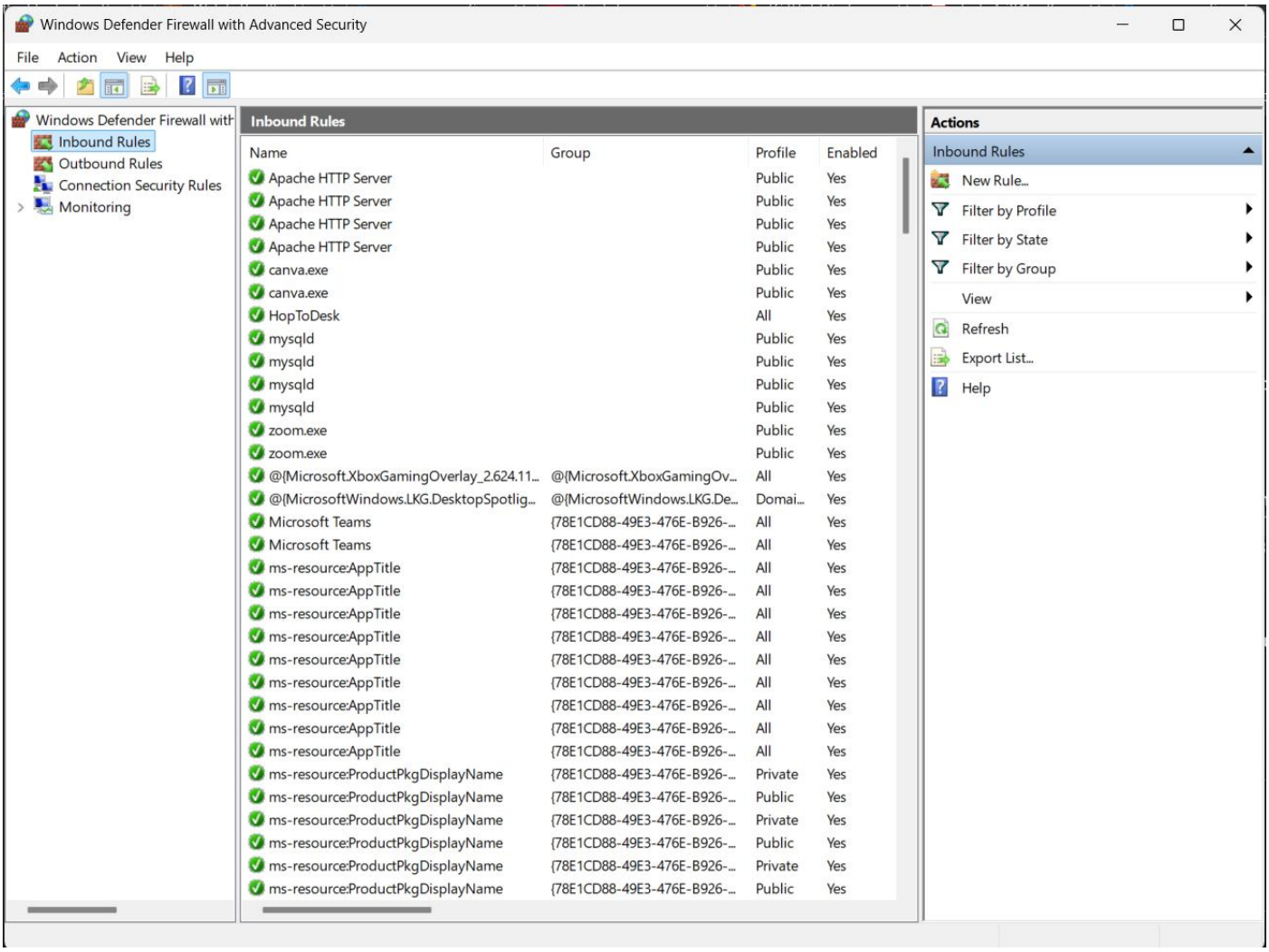
1.2. Verification of Block Rule

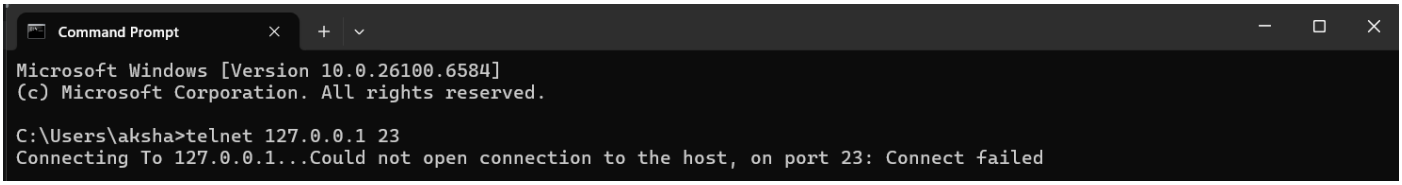
A test was conducted using the command line to verify the Port 23 block rule (Step 3) was enforced.

Command Executed:

telnet 127.0.0.1 23

Result: The connection attempt failed immediately, confirming the Windows Firewall actively blocked outbound traffic on TCP port 23.





Part 2: Ubuntu Server (UFW) Configuration and Cleanup

This section documents the command-line (CLI) steps for configuring the UFW firewall in the virtual machine.

2.1. UFW Activation and Initial Rule Set (Steps 1, 3, 5)

After logging into the server terminal (Step 1), the following commands were executed to install UFW, enable the firewall, and create the required rules (Steps 3 and 5).

Commands Executed:

sudo apt install ufw # Install UFW (necessary if missing)

sudo ufw enable # Activates the firewall

sudo ufw deny 23/tcp # Step 3: Block Telnet traffic

sudo ufw allow 22/tcp # Step 5: Allow SSH traffic

Intermediate State Verification

The following screenshot confirms the firewall is active and shows all four rules (IPv4 and IPv6) created by the deny 23 and allow 22 commands, fulfilling the requirement to list current rules.

```
Ubuntu 24.04.3 LTS pixie11 tty1

pixie11 login: hyacinth11
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-84-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
hyacinth11@pixie11:~$ sudo ufw enable
[sudo] password for hyacinth11:
Firewall is active and enabled on system startup
hyacinth11@pixie11:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23/tcp                     DENY IN     Anywhere
[ 2] 22/tcp                     ALLOW IN    Anywhere
[ 3] 23/tcp (v6)                DENY IN     Anywhere (v6)
[ 4] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

2.2. Rule Cleanup and Final State Verification

The final requirement was to remove the temporary Port 23 block rules to restore the state, ensuring only the persistent Port 22 rule remained active.

Commands Executed for Deletion:

The Port 23 block rules were deleted using their assigned numbers from the list (sudo ufw status numbered), and then the final state was verified.

Example commands used to delete the Port 23 block rules

sudo ufw delete [NUMBER] # Delete the IPv4 Port 23 rule

sudo ufw delete [NUMBER] # Delete the IPv6 Port 23 rule

Final State Verification

The final screenshot confirms that the temporary block rules for port 23 have been successfully removed, leaving only the persistent, required allow rules for port 22.

Command Executed:

sudo ufw status verbose

Result: The UFW firewall is active, and only necessary SSH traffic is permitted, restoring the original policy state with the allowed exception.