Assignment-7

Acknowledgment

Name: Sarvesh Anand Mankar
MIS: 142203013
Subject: Cryptography Network and Security Labs
Class: Div-2, T2

Detailed Report on Configuring Windows Defender Firewall

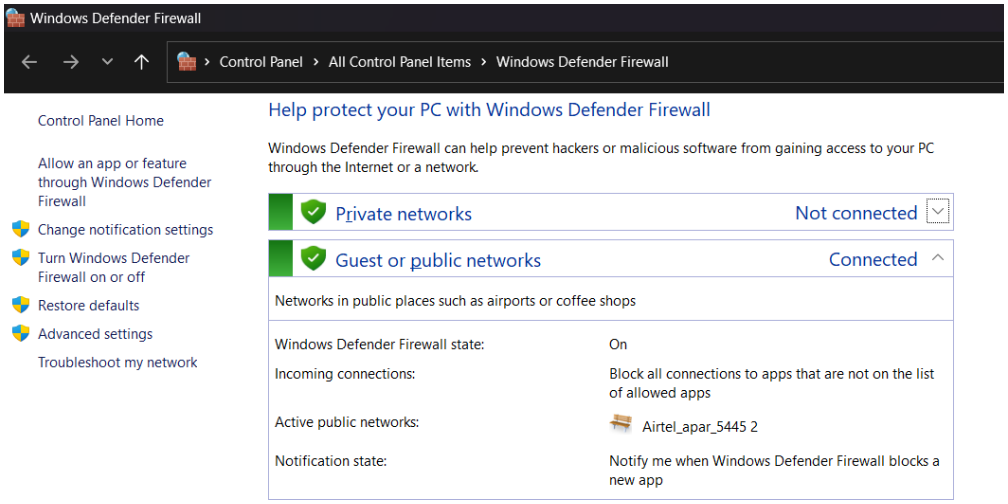
1. Introduction

- **Firewall Chosen**: Windows Defender Firewall is the default built-in firewall provided by Microsoft on all modern Windows operating systems.
- **Objective**: To implement a security policy to control network traffic, ensuring that only necessary and authorized communications are allowed, while blocking potentially harmful or unnecessary traffic.

2. Installation Process

Since Windows Defender Firewall comes pre-installed, no additional software installation is required. However, you need to ensure the firewall is active and ready for configuration:

1. **Check Firewall Status**:
    - Go to *Control Panel → System and Security → Windows Defender Firewall*.
    - Verify that the firewall is **turned on** for both private and public networks.
    - If it is disabled, click *Turn Windows Defender Firewall On or Off*, and select the appropriate options for private and public networks.


Windows Defender Firewall
Control Panel › All Control Panel Items › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

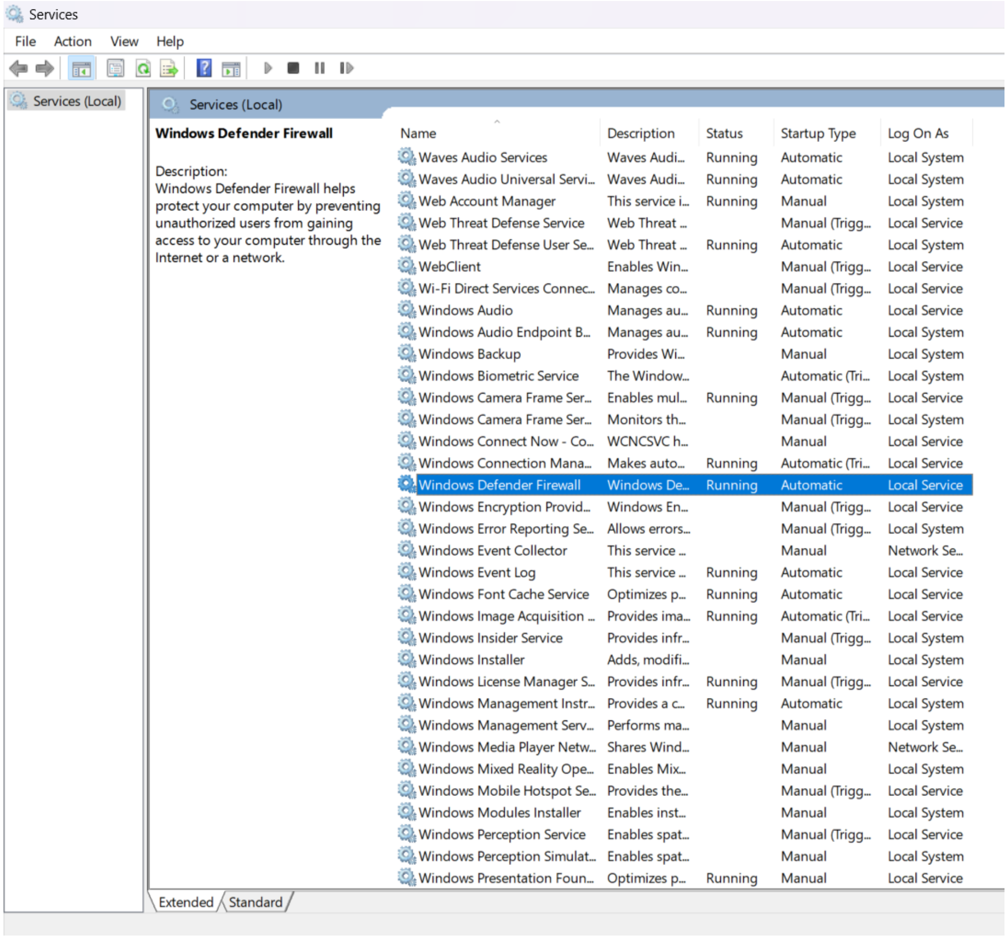
Windows Defender Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active public networks: Airtel_apar_5445 2

Notification state: Notify me when Windows Defender Firewall blocks a new app

2. **Ensure Windows Security Service is Running**:
    - Open the *Services* application (`services.msc`) from the Start menu.
    - Locate **Windows Defender Firewall Service** and ensure its status is "Running." If not, right-click and select *Start*.



Windows Defender Firewall

Description:
Windows Defender Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

Name	Description	Status	Startup Type	Log On As
Waves Audio Services	Waves Audi...	Running	Automatic	Local System
Waves Audio Universal Servi...	Waves Audi...	Running	Automatic	Local System
Web Account Manager	This service i...	Running	Manual	Local System
Web Threat Defense Service	Web Threat ...		Manual (Trigg...	Local Service
Web Threat Defense User Se...	Web Threat ...	Running	Automatic	Local System
WebClient	Enables Win...		Manual (Trigg...	Local Service
Wi-Fi Direct Services Connec...	Manages co...		Manual (Trigg...	Local Service
Windows Audio	Manages au...	Running	Automatic	Local Service
Windows Audio Endpoint B...	Manages au...	Running	Automatic	Local System
Windows Backup	Provides Wi...		Manual	Local System
Windows Biometric Service	The Window...		Automatic (Tri...	Local System
Windows Camera Frame Ser...	Enables mul...	Running	Manual (Trigg...	Local Service
Windows Camera Frame Ser...	Monitors th...		Manual (Trigg...	Local System
Windows Connect Now - Co...	WCNCSVC h...		Manual	Local Service
Windows Connection Mana...	Makes auto...	Running	Automatic (Tri...	Local Service
Windows Defender Firewall	Windows De...	Running	Automatic	Local Service
Windows Encryption Provid...	Windows En...		Manual (Trigg...	Local Service
Windows Error Reporting Se...	Allows errors...		Manual (Trigg...	Local System
Windows Event Collector	This service ...		Manual	Network Se...
Windows Event Log	This service ...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes p...	Running	Automatic	Local Service
Windows Image Acquisition ...	Provides ima...	Running	Automatic (Tri...	Local Service
Windows Insider Service	Provides infr...		Manual (Trigg...	Local System
Windows Installer	Adds, modifi...		Manual	Local System
Windows License Manager S...	Provides infr...	Running	Manual (Trigg...	Local Service
Windows Management Instr...	Provides a c...	Running	Automatic	Local System
Windows Management Serv...	Performs ma...		Manual	Local System
Windows Media Player Netw...	Shares Wind...		Manual	Network Se...
Windows Mixed Reality Ope...	Enables Mix...		Manual	Local System
Windows Mobile Hotspot Se...	Provides the...		Manual (Trigg...	Local Service
Windows Modules Installer	Enables inst...		Manual	Local System
Windows Perception Service	Enables spat...		Manual (Trigg...	Local Service
Windows Perception Simulat...	Enables spat...		Manual	Local System
Windows Presentation Foun...	Optimizes p...	Running	Manual	Local Service

3. Security Policy

We'll define a security policy to guide our configuration:

- **Inbound Connections**: Block all traffic by default, except for HTTP (port 80) and HTTPS (port 443).
- **Outbound Connections**: Allow all traffic to ensure normal internet and application functionality.

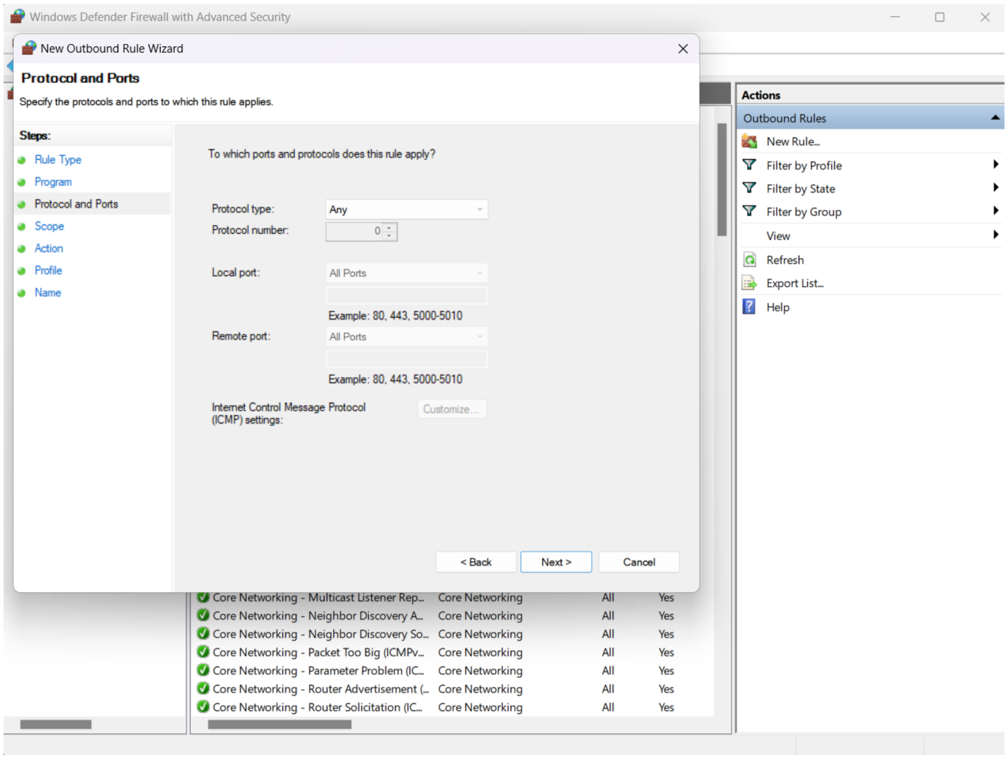
This policy ensures that unauthorized incoming traffic is blocked, protecting the system from threats while maintaining usability.

4. Configuration Steps

Accessing Windows Defender Firewall Advanced Settings

1. Open the Start Menu and type **Windows Defender Firewall with Advanced Security**.

2. Click on the result to open the advanced settings interface, which provides control over inbound and outbound traffic rules.



Windows Defender Firewall with Advanced Security

New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

To which ports and protocols does this rule apply?

Protocol type: Any
Protocol number: 0
Local port: All Ports
Example: 80, 443, 5000-5010
Remote port: All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:

Core Networking - Multicast Listener Rep...	Core Networking	All	Yes
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes
Core Networking - Neighbor Discovery So...	Core Networking	All	Yes
Core Networking - Packet Too Big (ICMPv...	Core Networking	All	Yes
Core Networking - Parameter Problem (IC...	Core Networking	All	Yes
Core Networking - Router Advertisement (...	Core Networking	All	Yes
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes

Configuring Inbound Rules

1. In the left pane, click on **Inbound Rules**, then select **New Rule** from the right-hand menu.
2. In the New Rule Wizard:
   - **Rule Type**: Select *Port* and click *Next*.
   - **Protocol and Ports**: Choose *TCP* and specify ports 80 and 443 in the "Specific local ports" field.
   - **Action**: Select *Allow the connection*.
   - **Profile**: Apply the rule to *Domain*, *Private*, and *Public* networks.
   - **Name**: Give the rule a descriptive name, e.g., *Allow HTTP and HTTPS*.
3. Create another inbound rule to block all other incoming traffic:
   - **Rule Type**: Select *Custom*.
   - **Program**: Select *All Programs*.
   - **Protocol and Ports**: Leave as default.
   - **Scope**: Leave as default unless restricting specific IPs.
   - **Action**: Select *Block the connection*.
   - **Profile**: Apply to all profiles (Domain, Private, Public).
   - **Name**: Name this rule, e.g., *Block All Other Inbound Traffic*.

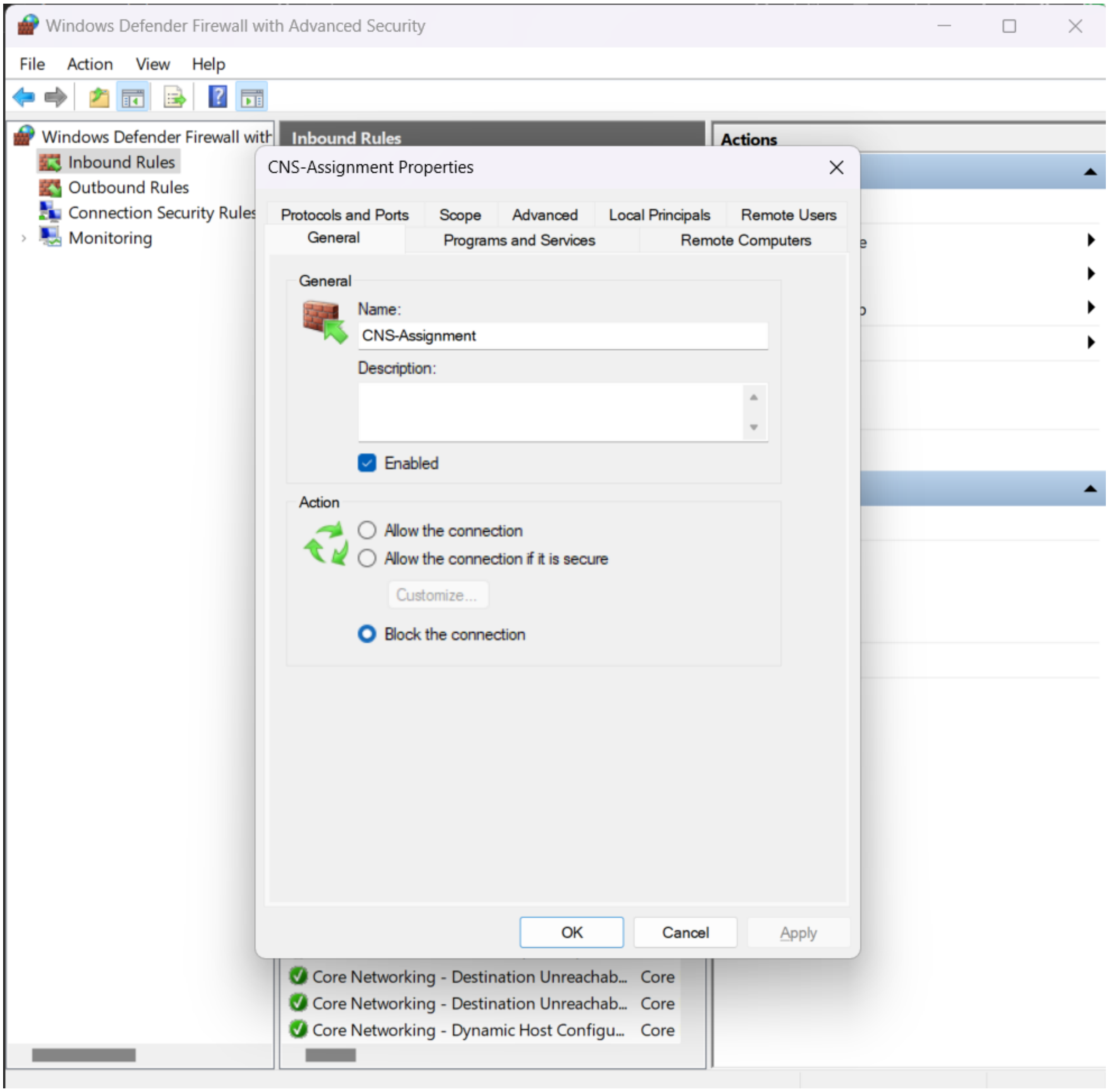
Configuring Outbound Rules

1. In the left pane, click on **Outbound Rules**, then select **New Rule** from the right-hand menu.
2. In the New Rule Wizard:
   - **Rule Type**: Select *Allow the connection*.
   - **Program**: Select *All Programs*.
   - **Profile**: Apply to all profiles (Domain, Private, Public).
   - **Name**: Name this rule, e.g., *Allow All Outbound Traffic*.

By default, Windows Defender Firewall allows outbound connections unless explicitly blocked, so additional outbound rules may not be necessary unless the security policy specifies restrictions.

Testing Rules

1. **Verify Allowed Traffic**:
   - Open a web browser and access a website (e.g., `https://www.google.com`).
   - Ensure the connection is successful, confirming HTTP/HTTPS traffic is allowed.
2. **Verify Blocked Traffic**:
   - Use a port scanner or a tool like `telnet` to test connections on blocked ports (e.g., SSH on port 22).
   - You should receive a "Connection Refused" message or no response, confirming the firewall is blocking unauthorized inbound traffic.



General

Name: CNS-Assignment

Description:

☑ Enabled

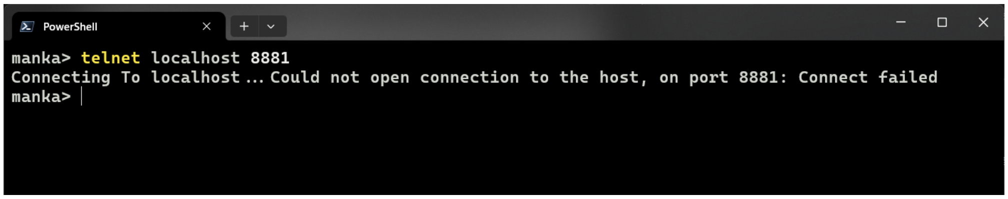
Action

○ Allow the connection

○ Allow the connection if it is secure

● Block the connection

✓ Core Networking - Destination Unreachab... Core
✓ Core Networking - Destination Unreachab... Core
✓ Core Networking - Dynamic Host Configu... Core



```
manka> telnet localhost 8881
Connecting To localhost...Could not open connection to the host, on port 8881: Connect failed
manka> 
```

5. Challenges and Observations

- **Challenges**:
  - Understanding the advanced options in the firewall interface, especially for custom rules.
  - Configuring rules for specific scenarios (e.g., testing remote access) required additional research.
- **Observations**:

- Windows Defender Firewall provides a robust set of tools to manage traffic.
- GUI simplifies rule management compared to command-line interfaces.

6. Conclusion

The configuration of Windows Defender Firewall according to the defined security policy was successful. By blocking unauthorized inbound traffic and allowing necessary communications, the system achieved a higher level of security while maintaining usability. Windows Defender Firewall proved to be an effective and user-friendly tool for this purpose.