Elevate Labs
Cybersecurity Internship Report

Task 4: Setup and Use a Firewall on Windows

Submitted by: Namita Rana

Role: Cybersecurity Intern

Company: Elevate Labs

Date of Submission: 08 August 2025

Privacy and Ethical Considerations

All steps in this task were executed on a single local machine in a controlled environment. The exercise involved configuring and testing Windows Defender Firewall rules using only safe, pre-defined ports for demonstration purposes. No real or active network services were exposed to the internet during the process.

The screenshots and configuration outputs included in this report have been thoroughly reviewed to remove or exclude any personal identifiers, usernames, IP addresses, MAC addresses, or other sensitive network details. Only non-sensitive, generic application names, standard software installation paths, and commonly known port numbers have been retained for clarity of explanation.

This activity was undertaken solely for academic learning and skill development in **network security**. All testing adhered to ethical cybersecurity principles and applicable guidelines. At no stage were unauthorized scans, intrusions, or connections made to external devices or networks. Upon completion of the demonstration, all temporary firewall rules created for testing were deleted or disabled, restoring the system to its original secure state.

Acknowledgement

I would like to express my heartfelt gratitude to my faculty, mentors, and coordinators for their invaluable guidance, motivation, and continuous support throughout the completion of this practical task on firewall configuration and traffic control. Their encouragement and constructive feedback have greatly enhanced my understanding of network security concepts and their application in real-world scenarios.

I am also thankful for the opportunity to work with **Windows Defender Firewall**, which enabled me to practically implement and test inbound and outbound traffic rules in a safe, controlled, and ethical environment. This hands-on experience has strengthened my ability to analyse network traffic, apply filtering rules, and ensure system security through proper configuration.

I extend my appreciation to all those who provided indirect support—be it through resource materials, discussions, or moral encouragement—which helped me successfully complete this task. Finally, I acknowledge that this task was carried out solely for academic purposes, adhering to all ethical cybersecurity practices, with no harm or disruption caused to any external systems or networks.

— Namita Rana

Table of Contents

Chapter 1: Introduction

1.1 Objective of the Task

The objective of this task is to develop practical skills in configuring and managing firewall rules on a Windows-based operating system using the built-in **Windows Defender Firewall with Advanced Security** tool. The exercise involves:

- Reviewing the currently configured firewall rules to understand the system's security posture.
- Creating a new inbound rule to block traffic on a selected TCP port (used here as an example for demonstration purposes).
- Testing the applied rule by simulating a connection attempt under safe, controlled conditions.
- Removing or disabling the test rule to return the firewall to its original state.

The primary goal is to strengthen the ability to implement access control through firewall configuration while ensuring a safe and authorized testing environment.

1.2 Importance of Firewall Configuration in Cybersecurity

Firewalls serve as a critical component of network defense, filtering network traffic according to predefined security rules. An improperly configured firewall can result in:

- **Unauthorized Access:** Exploitation of open or unused ports to gain system access.
- **Malware and Exploits:** Entry of malicious software through unmonitored or unprotected network paths.
- **Data Loss or Exfiltration:** Unauthorized transmission of sensitive information outside the system.

Effective firewall configuration enables:

- **Port and Service Control:** Restricting access to only necessary services.
- **Traffic Filtering:** Stopping malicious or unwanted traffic before it reaches applications.
- **Security Policy Enforcement:** Ensuring consistent implementation of access rules.

Through this task, learners develop the ability to apply, test, and verify firewall rules that improve the security posture of a system without impacting legitimate network operations.

1.3 Tools and Environment Used

- **Operating Environment:** Windows operating system (version withheld for privacy), with administrative access for configuration tasks.
- **Firewall Management Tool:** Windows Defender Firewall with Advanced Security (GUI interface).
- **Testing Method:**
  - Example: Using a basic network utility to verify if the test port is blocked.
- **Lab Environment:**
  - Conducted on a test machine in a controlled, non-production setting.
  - No scanning or blocking was performed on any live or sensitive systems.
  - All configuration changes were fully reversible.

1.4 Scope and Limitations of the Task

Scope:

- Navigating the Windows Defender Firewall interface.
- Creating a sample inbound firewall rule to block TCP traffic on a demonstration port.
- Testing the firewall rule's effect using a safe simulation.
- Restoring the firewall configuration to its initial state.

Limitations:

- Outbound firewall rules and advanced rule conditions (such as IP-based restrictions or program-specific rules) were not included.
- No testing was performed on enterprise networks or with third-party firewall tools.
- The exercise was limited to a single device setup in a controlled lab; multi-device and external network scenarios were excluded.

Chapter 2: Overview of Firewall Technology

2.1 Definition and Purpose of a Firewall

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access, malware infiltration, or data leakage.

On Windows systems, the built-in **Windows Defender Firewall** plays a critical role in ensuring that only legitimate and safe traffic is allowed. By managing which applications and services can communicate through the network, the firewall helps reduce the attack surface and protect sensitive information.

The primary purposes of a firewall include:

- **Blocking Unauthorized Access:** Prevents external threats from exploiting vulnerabilities.
- **Allowing Safe Communications:** Permits trusted traffic for legitimate applications.
- **Monitoring Network Activity:** Tracks and logs connection attempts for analysis.
- **Policy Enforcement:** Ensures compliance with organizational or user-defined security policies.

2.2 Types of Firewalls

Firewalls can be categorized based on their deployment method, functionality, and scope. In practice, most systems combine multiple types for layered protection.

1. Hardware Firewalls

- **Definition:** Physical devices placed between the network and the internet to filter traffic at the perimeter.
- **Usage:** Often used in enterprise environments, data centers, or for protecting home networks through integrated router-based firewalls.
- **Advantages:**
  - Dedicated processing power for filtering.
  - Independent from the host operating system.
  - Protects multiple devices at once.
- **Limitations:**
  - Additional cost.
  - Requires physical installation and configuration.

2. Software Firewalls

- **Definition:** Applications or operating system features installed on individual devices to control network traffic.
- **Example in Windows: Windows Defender Firewall**.
- **Advantages:**
    - Highly customizable for each device.
    - Easy to update and manage.
    - Can apply rules specific to applications or users.
- **Limitations:**
    - Consumes host system resources.
    - Protects only the device on which it is installed.

3. Cloud-Based Firewalls (Firewall-as-a-Service, FWaaS)

- **Definition:** Firewalls hosted in the cloud and managed by third-party providers.
- **Usage:** Common in organizations using cloud services or distributed workforces.
- **Advantages:**
    - No on-premises hardware required.
    - Scalable and accessible from anywhere.
- **Limitations:**
    - Relies on internet connectivity.
    - May introduce latency.

4. Packet-Filtering Firewalls

- **Function:** Filters network traffic based on IP addresses, ports, and protocols.
- **Strength:** Simple, fast, and effective for basic filtering.
- **Weakness:** Limited inspection capability—cannot examine packet contents.

5. Stateful Inspection Firewalls

- **Function:** Tracks the state of active connections and makes decisions based on both packet content and connection state.
- **Strength:** More secure than simple packet filtering.
- **Weakness:** Requires more processing power.

6. Next-Generation Firewalls (NGFW)

- **Function:** Combines traditional firewall functions with advanced features like intrusion prevention, deep packet inspection, and application awareness.
- **Usage:** Common in modern enterprise security setups.

2.3 How a Firewall Filters Traffic

A firewall uses predefined or custom rules to allow or block network packets. These rules can be based on:

- **IP Addresses:** Restrict access to or from specific sources.
- **Ports:** Limit communication to certain services (e.g., port 80 for HTTP).
- **Protocols:** Allow or deny specific protocols like TCP, UDP, or ICMP.
- **Applications:** Permit only trusted programs to send or receive data.
- **Direction:** Control inbound (incoming) and outbound (outgoing) traffic separately.

The filtering process generally follows these steps:

1. **Packet Reception:** Firewall intercepts the packet before it reaches the target system or network.
2. **Rule Matching:** Packet details are compared against the rule set.
3. **Decision:** If the packet matches an “allow” rule, it is forwarded; if it matches a “deny” rule, it is blocked.
4. **Logging:** Actions are recorded for monitoring and troubleshooting.

2.4 Common Use Cases for Firewall Rules in Network Security

Firewalls are applied in a variety of scenarios to maintain security:

1. **Blocking Malicious IP Ranges**
    - Prevents known threat actors from connecting to the system.
2. **Restricting Unused Ports**
    - Minimizes the attack surface by disabling unnecessary services.
3. **Allowing Only Trusted Applications**
    - Ensures only verified software can communicate externally.
4. **Enforcing Network Segmentation**
    - Separates sensitive network zones from public-facing areas.
5. **Outbound Traffic Control**

- Stops malware from sending data to command-and-control servers.

6. **Custom Rules for Compliance**
   - Meets industry standards (e.g., PCI-DSS, HIPAA) by enforcing strict communication policies.

Chapter 3: Setting Up a Firewall on Windows

3.1 Introduction

Windows operating systems come with a built-in firewall feature—**Windows Defender Firewall**—designed to help prevent unauthorized access to or from your private network. Setting up a firewall correctly is a crucial step in securing a system, ensuring that only trusted traffic is allowed and potentially harmful data packets are blocked.

The configuration process involves enabling the firewall, defining rules, and customizing its behaviour for specific network profiles (Domain, Private, and Public). Proper setup ensures optimal protection while minimizing disruptions to legitimate network activities.

3.2 Accessing Windows Defender Firewall

To configure a firewall in Windows, follow these steps:

1. **Open Control Panel**:
   - Press Windows + R, type control, and press **Enter**.
2. **Navigate to Windows Defender Firewall**:
   - Select **System and Security → Windows Defender Firewall**.
3. **Verify Status**:
   - On the left pane, you can check whether the firewall is active for **Domain**, **Private**, and **Public** network profiles.

3.3 Enabling and Disabling the Firewall

While it is strongly recommended to keep the firewall **enabled** at all times, there may be instances (such as troubleshooting) where temporary disabling is needed.

- **Enable**:
  - Go to **Turn Windows Defender Firewall on or off** in the left menu and select **Turn on** for all network profiles.
- **Disable** *(not recommended)*:
  - Select **Turn off** only when necessary and re-enable promptly.

3.4 Configuring Basic Firewall Settings

Windows Defender Firewall provides different profiles with specific configurations:

- **Domain Profile** – Applied when the computer is connected to a domain network.
- **Private Profile** – Used for trusted home or office networks.
- **Public Profile** – Used for public or untrusted networks, offering the highest level of restriction.

Steps to configure:

1. Go to **Advanced settings** from the left pane.
2. Open **Windows Defender Firewall with Advanced Security**.
3. Adjust inbound and outbound rules for each profile.

3.5 Best Practices for Windows Firewall Setup

- Always keep the firewall **enabled** on all network profiles.
- Regularly review and update rules to remove unnecessary permissions.
- Use **specific** rules instead of broad “Allow All” rules.
- Combine firewall protection with antivirus and other security measures.

Chapter 4: Firewall Configuration and Rule Management

Configuring and managing firewall rules is a fundamental aspect of system and network security. In this task, the focus is on creating, testing, and removing a specific inbound rule using **Windows Defender Firewall with Advanced Security**. The process ensures that users understand not only how to implement security controls but also how to revert changes without impacting system stability.

4.1 Viewing and Listing Current Firewall Rules

Before implementing any changes, it is essential to review the existing firewall configuration. This step helps in:

- **Understanding the current security posture** of the system.
- Avoiding conflicts with pre-existing rules.
- Identifying if any similar rules already exist for the port in question.

Procedure:

1. Open the **Windows Defender Firewall with Advanced Security** tool.
    - Press Windows + R, type wf.msc, and press **Enter**.
2. Navigate to **Inbound Rules** in the left-hand panel.
3. Review the list of active and inactive rules, noting their **Name**, **Action** (Allow/Block), **Protocol**, and **Local Port**.

This baseline helps ensure that new configurations will not unintentionally override critical security settings.

4.2 Creating an Inbound Rule to Block Specific Port Traffic (Example: Port 23 – Telnet)

Blocking unused or vulnerable ports is a preventive security measure. In this example, **TCP Port 23**, commonly associated with Telnet, is blocked due to its lack of encryption and susceptibility to attacks.

Procedure:

1. In the **Inbound Rules** section, click **New Rule** from the right-hand **Actions** panel.
2. Select **Port** as the rule type and click **Next**.
3. Choose **TCP** and specify **Specific local ports**: 23.
4. Select **Block the connection** and click **Next**.

5. Apply the rule to **Domain**, **Private**, and **Public** profiles.
6. Assign a descriptive name such as *"Block TCP Port 23 – Telnet"* and click **Finish**.

This rule will immediately prevent inbound connections on Port 23, regardless of their source.

4.3 Testing the Rule by Attempting Connection to the Blocked Port

Testing ensures that the firewall rule is functioning as intended and has not affected unrelated services.

Procedure:

1. Enable the **Telnet Client** (if not already installed) via:
   - **Control Panel → Programs and Features → Turn Windows features on or off** → Check *Telnet Client*.
2. Open **Command Prompt** and attempt to connect:

```
telnet localhost 23
```

3. Observe the result: A **connection failure** indicates that the firewall rule is active and blocking traffic as expected.

This test should be performed both locally and, if possible, from another machine on the same network (in a lab environment) to confirm rule enforcement.

4.4 Restoring Original State by Removing the Rule

After verification, the system should be returned to its default configuration to prevent unintended service disruptions.

Procedure:

1. In **Windows Defender Firewall with Advanced Security**, locate the created rule (*Block TCP Port 23 – Telnet*).
2. Right-click the rule and select **Delete** or **Disable**.
3. Confirm that the rule no longer appears in the active inbound rules list.

This ensures that temporary testing configurations do not remain active and interfere with normal system operations.

Chapter 5: Results and Observations

This chapter outlines the outcomes obtained from implementing the firewall configuration described in Chapter 4. It details the behaviour of the system after applying the inbound blocking rule, the verification process, and key insights gained from the exercise.

5.1 Outcome of Port Blocking and Testing

After configuring the **Windows Defender Firewall** to block TCP Port 23, testing confirmed that the rule functioned as intended.

Observed Outcomes:

- Any attempt to establish a **Telnet connection** on Port 23 (both local and remote, where applicable in the lab environment) was **unsuccessful**.
- The error message during Telnet attempts indicated that the connection could not be opened, signifying that the firewall successfully intercepted and blocked inbound traffic on the specified port.
- All other network functions and services unrelated to Port 23 remained unaffected, indicating proper scope and specificity of the rule.

5.2 Effectiveness of the Applied Firewall Rule

The applied firewall rule proved **highly effective** in preventing connections over the specified port. Key indicators of its effectiveness included:

- **Isolation of target traffic** – Only traffic directed to Port 23 was blocked, while other communication channels remained operational.
- **Immediate enforcement** – The block took effect as soon as the rule was applied, without requiring a system reboot.
- **Profile-wide coverage** – Since the rule was applied to **Domain**, **Private**, and **Public** profiles, the protection was active in all network contexts.

This level of control demonstrates the importance of precise firewall rule creation for targeted security measures.

5.3 Lessons Learned from the Implementation

Through the configuration and testing process, several important lessons were learned:

1. **Granularity in Rule Creation** – Specific port targeting prevents unnecessary service interruptions and maintains system usability.

2. **Importance of Testing** – Verification steps are essential to ensure that the intended traffic is blocked and no unintended consequences occur.
3. **Temporary vs. Permanent Rules** – Temporary rules should be clearly labeled and removed after testing to maintain clean configurations.
4. **Understanding Firewall Profiles** – Applying rules across all profiles ensures consistent behaviour, regardless of network type or location.
5. **Documentation for Repeatability** – Recording the configuration steps, testing methods, and results enables reproducibility and aids future troubleshooting.

5.4 Summary of Observations

The experiment successfully showcased the process of implementing, verifying, and removing a targeted firewall rule in Windows. The results reinforced that **proper firewall configuration is a critical element of system hardening**, allowing administrators to block insecure services without disrupting legitimate network activity.

Chapter 6: Recommendations

Based on the practical exercise and the observations recorded in Chapter 5, this section provides recommendations for effective firewall management. The goal is to ensure security without compromising system usability or legitimate network functions.

6.1 Best Practices for Firewall Rule Management

1. **Apply the Principle of Least Privilege**
   - Only allow the minimum necessary ports and services required for operations.
   - Block all unused or insecure services (e.g., Telnet) to reduce the attack surface.
2. **Use Descriptive Rule Names**
   - Clearly label each firewall rule with its purpose, target port, and date of creation (e.g., *"Block_Telnet_Port_23_Test_Aug2025"*).
   - This improves maintainability and avoids confusion during audits.
3. **Regularly Audit Firewall Rules**
   - Review the firewall configuration periodically to remove outdated or redundant rules.
   - Validate that all active rules still align with current security policies.
4. **Test Before Deployment in Production**
   - Implement new firewall rules in a controlled test environment before applying them to live systems.
   - This prevents unplanned service disruptions.
5. **Backup Firewall Configurations**
   - Keep an export or backup of the firewall rule set before making major changes.
   - This ensures that configurations can be restored in case of errors.

6.2 Suggested Rules for Common Security Scenarios

- **Block Insecure Services**:
  Disable legacy and insecure protocols such as Telnet (Port 23) and FTP (Port 21) unless absolutely required.

- **Allow Only Required Application Ports**:
  Permit inbound and outbound traffic solely on ports needed for business applications (e.g., Port 443 for HTTPS).
- **Restrict Administrative Access**:
  Limit remote desktop (RDP) or SSH access to specific trusted IP addresses.
- **Segment Network Access**:
  Create rules to isolate sensitive servers from general network traffic, ensuring internal segmentation.

6.3 Periodic Review and Update of Firewall Configurations

- **Quarterly Reviews**:
  Schedule firewall configuration checks at least once every quarter to ensure alignment with evolving security threats.
- **Update with Changing Needs**:
  Modify or remove rules as services, infrastructure, and policies change.
- **Monitor for Anomalies**:
  Use built-in firewall logging features to track blocked and allowed traffic, identifying suspicious patterns that may indicate attacks.

6.4 Summary of Recommendations:

Consistent firewall management requires both technical accuracy and ongoing administrative oversight. By combining **well-defined rules, regular audits, and proactive monitoring**, administrators can ensure that firewalls remain an effective first line of defense against cyber threats.

Chapter 7: Summary and Conclusion

7.1 Recap of the Implementation Process

The task focused on configuring and testing firewall rules using **Windows Defender Firewall with Advanced Security** to block and allow specific types of network traffic. The process involved:

1. **Viewing Existing Firewall Rules** – Reviewing the current configuration to understand the system's security posture.
2. **Creating a Custom Inbound Rule** – Blocking inbound traffic on **Port 23 (Telnet)** to prevent unauthorized access via an insecure protocol.
3. **Testing the Rule** – Simulating a Telnet connection attempt to verify that the rule was functioning as intended.
4. **Restoring the Original Configuration** – Removing the test rule to ensure the system returned to its initial, stable state.

This step-by-step method allowed for a clear understanding of how firewall rules are applied, tested, and managed in a Windows environment.

7.2 Importance of Proper Firewall Management in Security

A firewall serves as a **critical barrier** between a secure system and potentially harmful external traffic. Proper configuration ensures:

- **Protection Against Unauthorized Access** – Blocking unneeded or insecure services reduces attack vectors.
- **Policy Enforcement** – Ensuring that all network communication complies with organizational security guidelines.
- **Traffic Monitoring** – Detecting unusual traffic patterns that could indicate malicious activity.

Without structured firewall management, even well-designed networks can be exposed to vulnerabilities that attackers can exploit.

7.3 Final Thoughts and Key Takeaways

From this practical task, several important lessons emerged:

- **Hands-on configuration** is essential for building real-world cybersecurity skills.
- Even basic firewall rules, when applied correctly, can significantly enhance system security.

- Documentation of steps and rules ensures repeatability and assists in troubleshooting.
- Regular **review and updates** to firewall settings are necessary to adapt to evolving threats.

In conclusion, mastering the setup and use of firewalls in Windows is a fundamental skill for any cybersecurity practitioner. By applying the principles of least privilege, careful testing, and ongoing monitoring, network defenses can remain robust against both known and emerging threats.
