Windows 11 Firewall Configuration Lab

Objective:

Learn to configure and manage Windows Firewall by creating a shared folder, viewing allowed apps, adjusting permissions, and exploring advanced security features.

Prerequisites

1. Two Computers on the Same Network: This lab assumes you have labPC-1 (the main computer) and another computer to access shared resources on labPC-1.

2. Administrator Privileges: Ensure you have admin access to make changes to Windows Firewall and network settings.

Part 1: Create and Share a Folder on labPC-1

Objective: Create a shared folder on labPC-1 and set permissions to allow network access from other devices.

1. Create a New Folder:

- On labPC-1, open File Explorer and navigate to a location, such as Documents.
- Right-click and select New > Folder to create a new folder. Name it SharedFolder.

2. Enable Folder Sharing:

- Right-click on SharedFolder, select Properties, and go to the Sharing tab.
- Click Share…, add users (e.g., Everyone if sharing with all users on the network), and set permissions (Read/Write).
- Click Share and note the network path (e.g., `\\labPC-1\SharedFolder`).

3. Confirm Sharing Settings:

- In the Advanced Sharing settings, select Permissions to adjust access levels if needed.
- Click OK to apply changes and close all dialog boxes.

Practice Questions:

- What are the security implications of sharing a folder with Everyone?
- How would you limit access to specific users or groups?

Part 2: Use File Explorer to View labPC-1’s Shared Folder from Another Device

Objective: Use a second computer to access SharedFolder on labPC-1 to verify network sharing and firewall permissions.

1. Access the Shared Folder:

- On the second computer, open File Explorer.
- In the address bar, enter the network path of the shared folder (e.g., `\\labPC-1\SharedFolder`) and press Enter.

2. Confirm Access:

- Verify you can view the contents of SharedFolder.
- Try adding a file to the folder if you have Write permissions; otherwise, confirm you can read and open files if you only have Read access.

Practice Questions:

- What would you check if the shared folder is not accessible from the second computer?
- How does firewall configuration impact file and printer sharing?

Part 3: Open Windows Firewall on labPC-1

Objective: Access Windows Firewall settings on labPC-1 to manage incoming and outgoing connections.

1. Open Windows Firewall:

- On labPC-1, go to Settings > Privacy & Security > Windows Security.

- Select Firewall & network protection and click Advanced settings to open the Windows Defender Firewall with Advanced Security console.

2. Verify Active Firewall Profiles:

- In the Firewall console, confirm that Domain, Private, and Public profiles are configured based on the network location.

Practice Questions:

- Why is it important to configure firewall settings based on network profile (e.g., Private vs. Public)?

- How can firewall profiles impact network security in different environments?

Part 4: Investigate the Windows Firewall Allowed Programs Feature

Objective: Use the Allowed Programs feature to view and manage which applications are allowed through the firewall.

1. Open Allowed Apps:

- In Firewall & network protection settings, click on Allow an app through the firewall.

- This will open the Allowed apps window, listing all applications with firewall permissions.

2. Review Allowed Programs:

- Scroll through the list to see which applications are allowed on Private and Public networks.

- Take note of any programs that might be risky if allowed through the firewall, such as remote access software.

Practice Questions:

- Why might you restrict certain applications from accessing the network?

- How does allowing an app through the firewall impact network security?

Part 5: Configure the Windows Firewall Allowed Apps Feature

Objective: Add or modify allowed apps in Windows Firewall to control which applications can communicate through the firewall.

1. Modify App Permissions:

- In the Allowed apps window, click Change settings (you may need administrator rights).

- Check or uncheck boxes to allow or block applications on Private or Public networks.

2. Add a New App:

- To add an app, click Allow another app…, browse to the application's location, select it, and click Add.

- Ensure the new app's permissions match your security requirements (e.g., allowed on Private but blocked on Public).

3. Save Changes:

- After making modifications, click OK to save changes and close the window.

Practice Questions:

- What criteria should be considered when allowing apps through the firewall?

- How might permissions differ for apps on Private versus Public networks?

Part 6: Explore Advanced Security Features in Windows Firewall

Objective: Use Advanced Security settings to create custom rules, monitor traffic, and strengthen security.

1. Access Advanced Security Console:

- Open Windows Defender Firewall with Advanced Security from Firewall & network protection.

2. Create Inbound and Outbound Rules:

- Select Inbound Rules or Outbound Rules from the left pane and click New Rule to create custom rules.

- Choose rule types, such as Port, Program, or Custom, to restrict traffic by specific parameters (e.g., block a specific port or program).

3. Configure Custom Firewall Rules:

- For example, to block a specific port (e.g., port 80), select Port rule type, specify the port, and choose Block the connection.

- Name the rule and click Finish to apply it.

4. Monitor Firewall Activity:

- Use Monitoring to view active firewall rules, connection security rules, and other network activity logs.

Practice Questions:

- How can custom rules help in securing specific applications or network services?

- When might you need to block or open specific ports in Windows Firewall?

Final Questions

1. What are the differences between allowing apps through Allowed apps and creating custom rules in the advanced security console?

2. How does configuring firewall settings enhance data protection in shared network environments?

3. Describe a scenario where modifying firewall rules would be necessary for troubleshooting network issues.