CYSE 608: Hands-On Lab Report 7

Name: **BRYANT WATKINS**

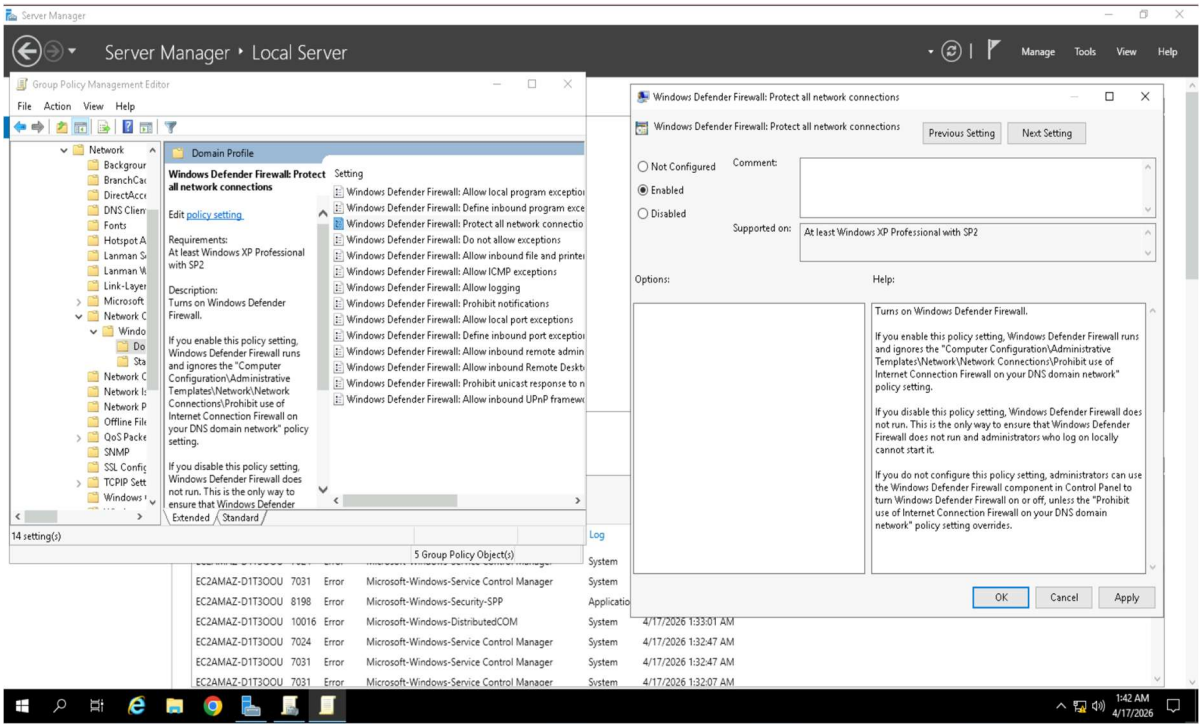
Directions: Review the tutorial video found in Module 7 and complete the following tasks. Submit your completed report in Canvas.

Enable or Disable Firewall Using Group Policy in Windows Server 2019

Total Points = 50 points

Task 1. [12.5 points]

1. The most relevant task you can complete/perform.
2. Provide a screenshot of the completed task.

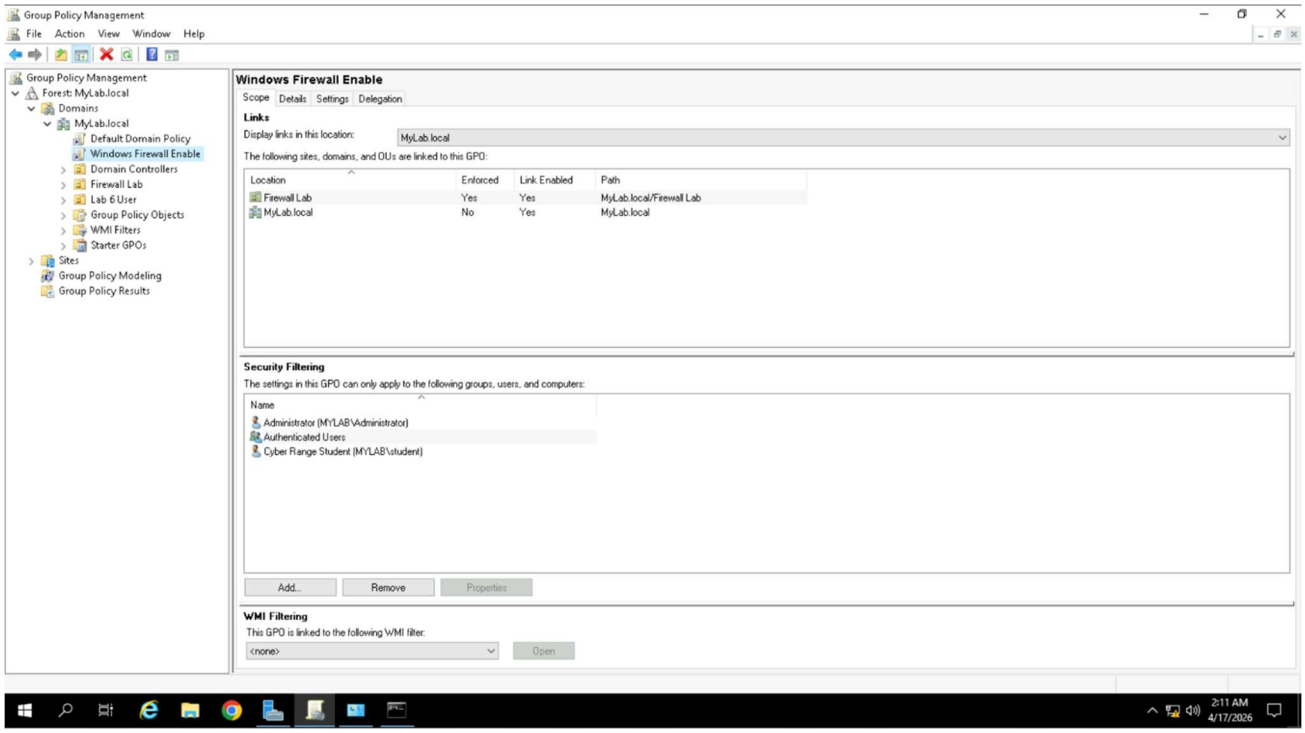


3. Briefly describe the screenshot, explaining the task or tool used.

The image displayed above illustrates the enabling of Windows Defender Firewall for all network connections. This task enables the firewall for the domain profile. This is a critical step for any cybersecurity administrator to ensure a successful defense-in-depth secure environment is in place for the network.

Task 2. [12.5 points]

1. The most relevant task you can complete/perform.
2. Provide a screenshot of the completed task.

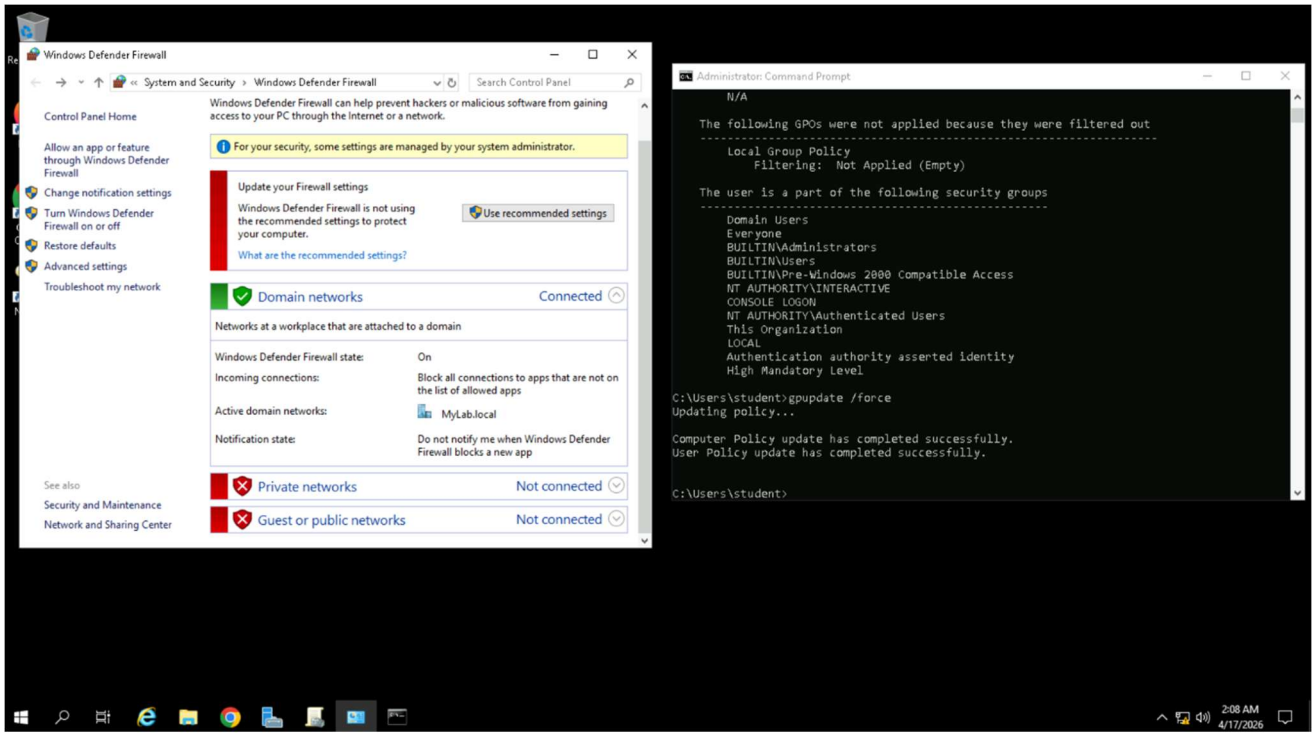


3. Briefly describe the screenshot, explaining the task or tool used.

The screenshot above displays the successful creation of a new firewall policy in the Group Policy Management window. The new firewall policy was successfully linked to the desired domain. Completing this task is beneficial and effective due to its ability to maintain centralized management and uniformity across the network.

Task 3. [12.5 points]

1. The most relevant task you can complete/perform.
2. Provide a screenshot of the completed task.

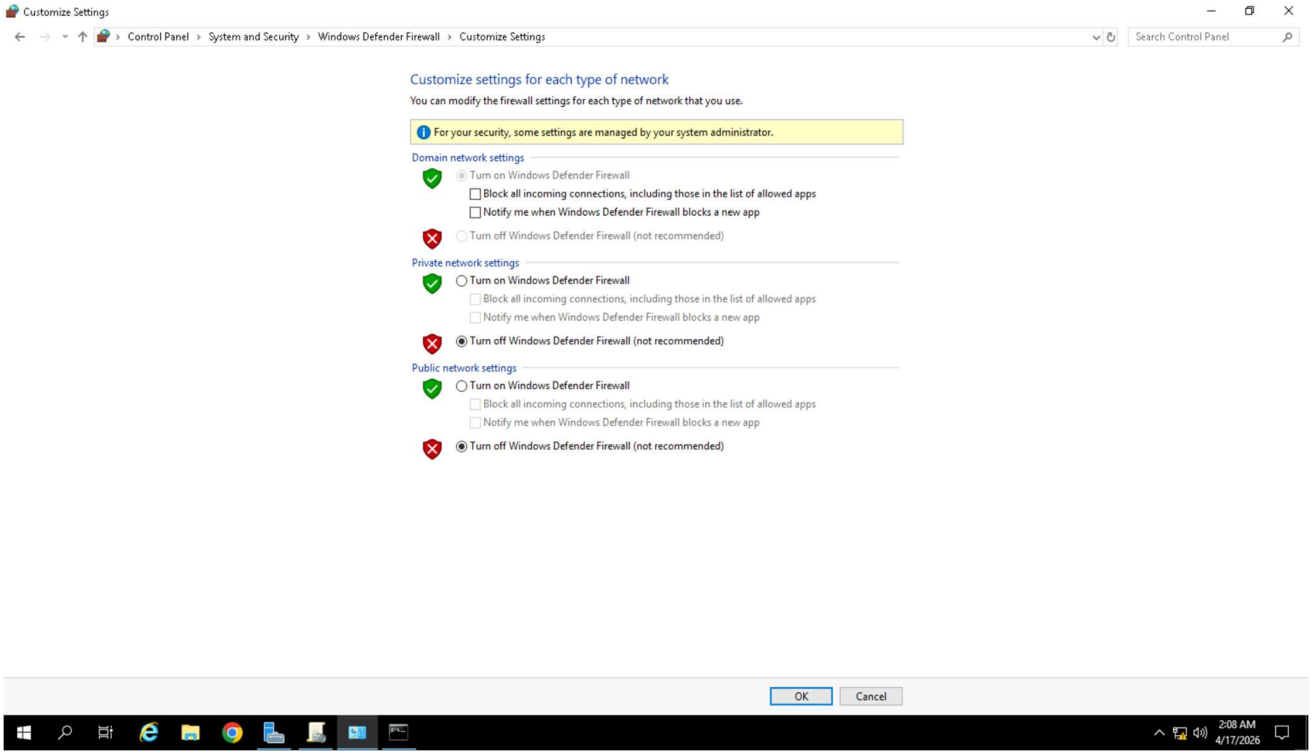


3. Briefly describe the screenshot, explaining the task or tool used.

The screen image illustrated above shows the successful implementation of a new firewall group policy. *Gpupdate /force* is the applicable CMD Prompt command to ensure that the group policy is updated to reflect the necessary changes. Upon entering the command, the Windows Defender Firewall window reflects the application of the new firewall policy in real time. The desired effect is also indicated by the disclaimer seen in yellow, stating that, "For your security, some settings are managed by your system administrator".

Task 4. [12.5 points]

1. The most relevant task you can complete/perform.
2. Provide a screenshot of the completed task.



3. Briefly describe the screenshot, explaining the task or tool used.

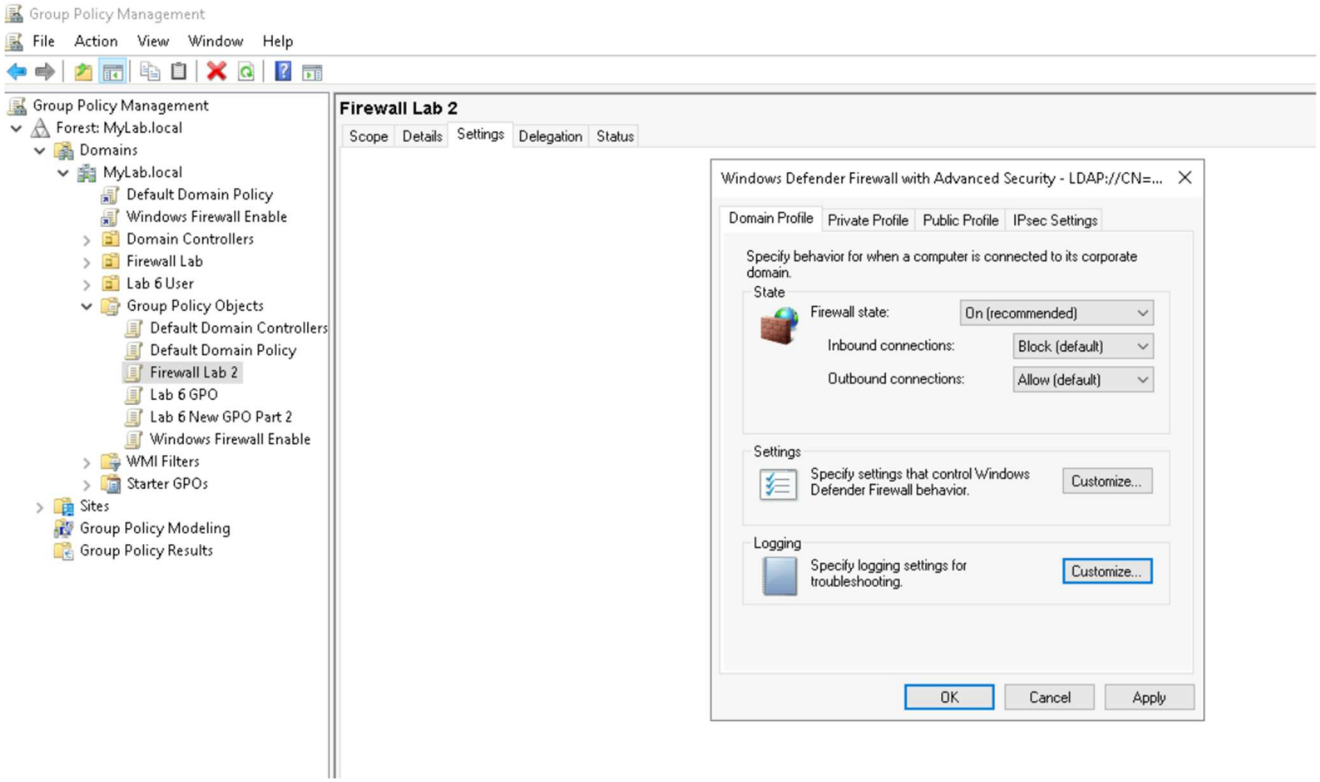
The image displayed above reinforces the previous task and confirms the results. I attempted to toggle the Windows Defender Firewall to *off* as I was previously capable of. After implementing the group policy update, however, I am no longer capable of configuring the Windows Defender Firewall to either the *off* or *on* option any longer. My inability to toggle these options is due to the firewall group policy now being active. This is another critical operation has administrators can take these steps to ensure centralized management of firewall states for an organization.

Configure Windows Firewall Using Group Policy in Active Directory

Total Point = 50 points

Task 5. [12.5 points]

1. The most relevant task you can complete/perform.
2. Provide a screenshot of the completed task.

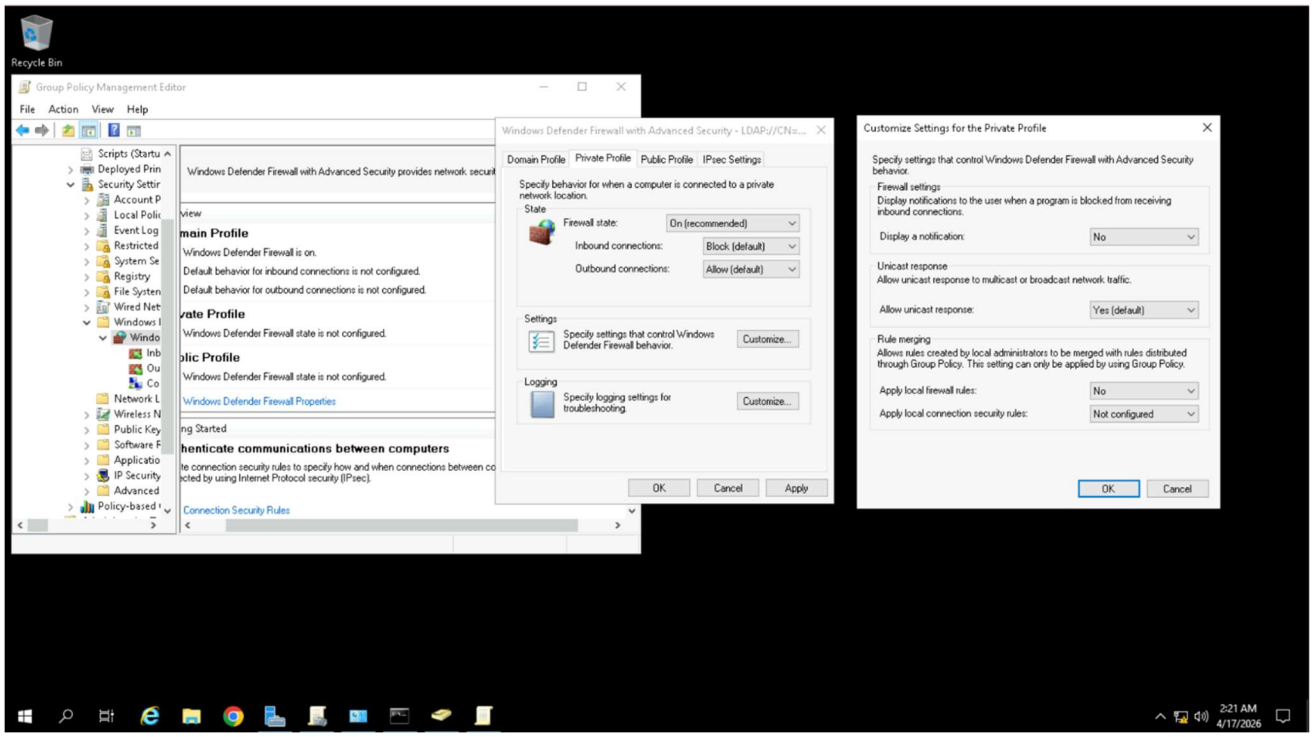


3. Briefly describe the screenshot, explaining the task or tool used.

The above screenshot illustrates the task of configuring Windows Defender Firewall properties for the Domain profile. The *Inbound connections* have been set to *Block (default)*, while the *Outbound connections* have been set to *Allow (default)*. These changes will configure the Domain profile firewall to only allow for outbound movement.

Task 6. [12.5 points]

1. The most relevant task you can complete/perform.
2. Provide a screenshot of the completed task.

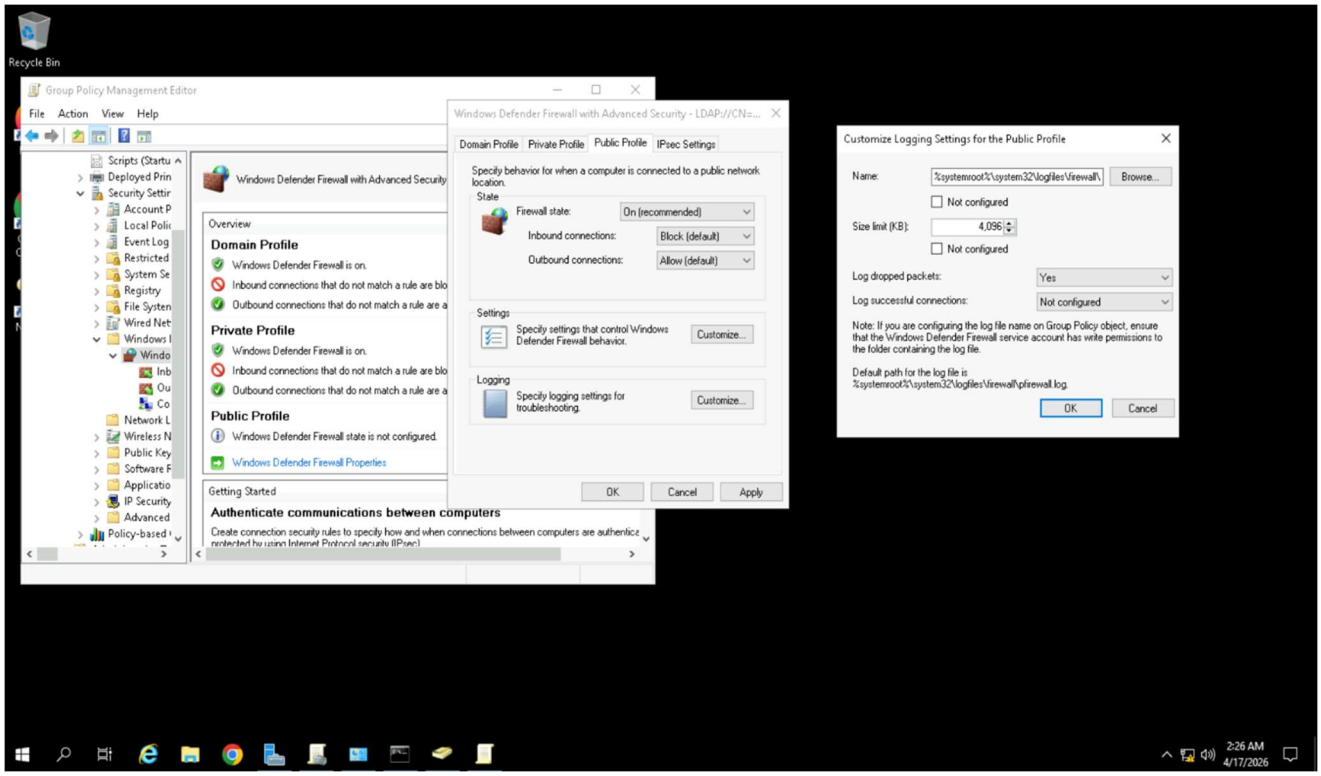


3. Briefly describe the screenshot, explaining the task or tool used.

The above screenshot illustrates the task of configuring Windows Defender Firewall properties for the Private profile. In this process, I began configuring the settings. I configured the settings to *not* display a notification, *allow* a unicast response, *not* apply local firewall rules (preventing users from toggling firewall on or off), and *not* to configure local connection security rules. These are options that require understanding and configuration to ensure the desired effects by the system administrator.

Task 7. [12.5 points]

1. The most relevant task you can complete/perform.
2. Provide a screenshot of the completed task.

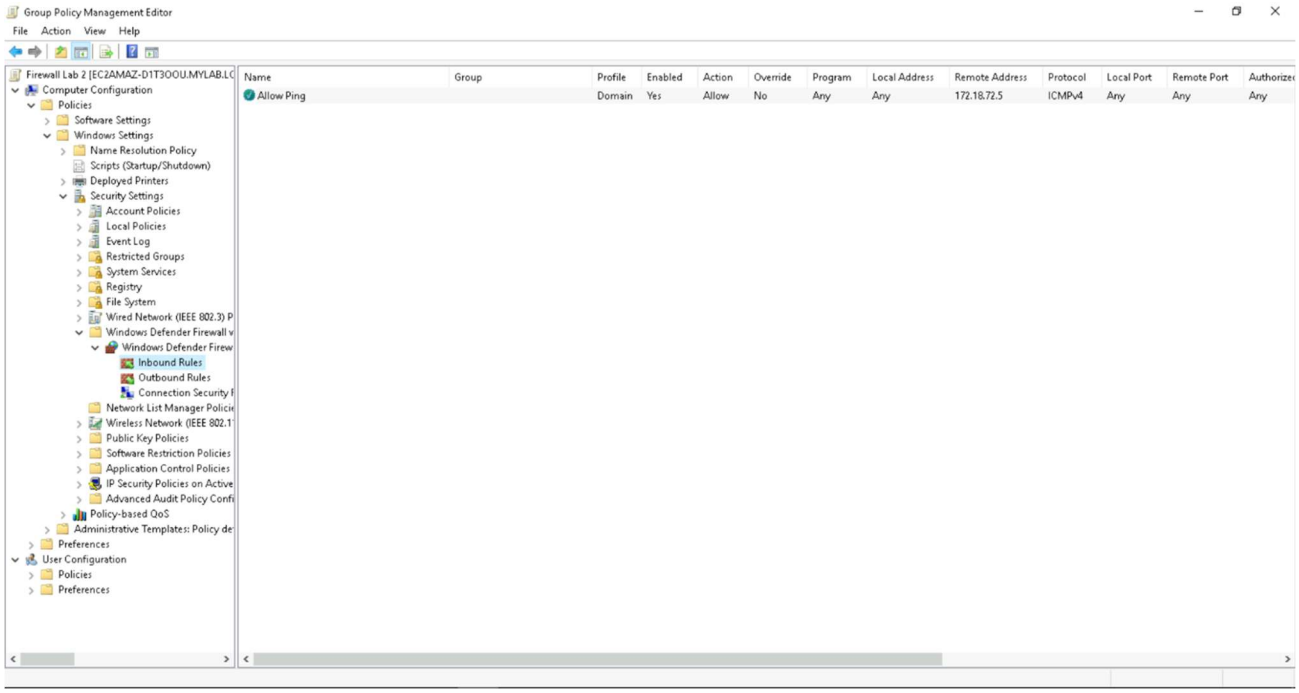


3. Briefly describe the screenshot, explaining the task or tool used.

The above screenshot illustrates the task of configuring Windows Defender Firewall properties for the Public profile. I configured the *Logging* settings to store the log data in the desired location. I then configured the *Size limit* to allow for customization as needed. Finally, I toggled *Log dropped packets* to *Yes*, as making this change will now ensure that all dropped packets will be documented for further viewing or analysis as needed. There is also an option to *Log successful connections*, but I chose to forgo that option for this lab. Making changes to the Domain, Private, and Public profiles are integral to the understanding of Windows Defender Firewall configuration and system administration.

Task 8. [12.5 points]

1. The most relevant task you can complete/perform.
2. Provide a screenshot of the completed task.



3. Briefly describe the screenshot, explaining the task or tool used.

The screenshot displayed above highlights the success of creating a new Inbound rule for Windows Defender Firewall. Creating firewall rules through group management policy is one of the most effective and important tasks for a system administrator. Creating these rules allows for the strategic configuration of a network's cybersecurity infrastructure. These rules also fall under centralized management and control, allowing for efficiency and consistency across an organization's network.