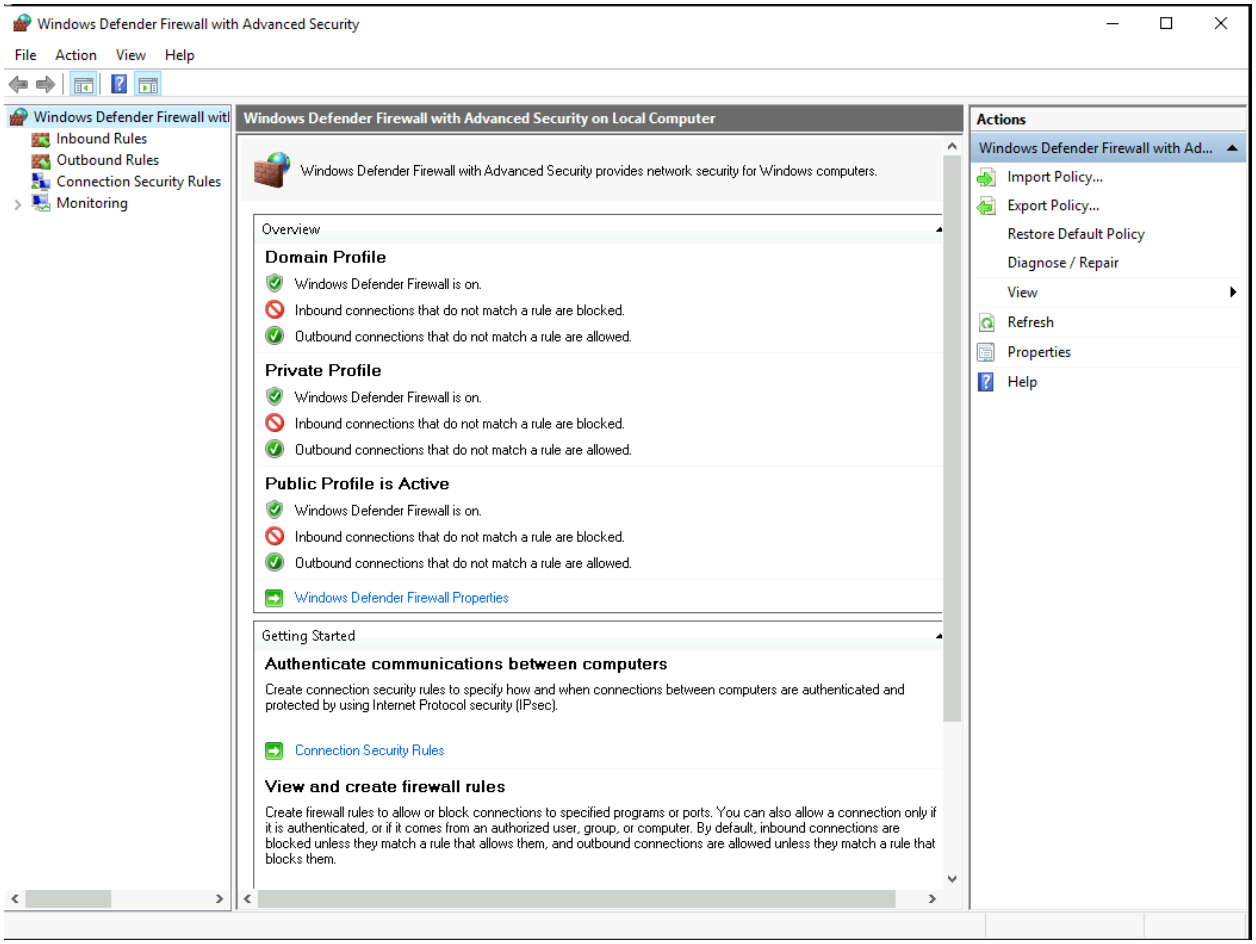
CYSE 680 – Windows Firewall and Group Policy Lab

Task 1: Open Windows Firewall with Advanced Security

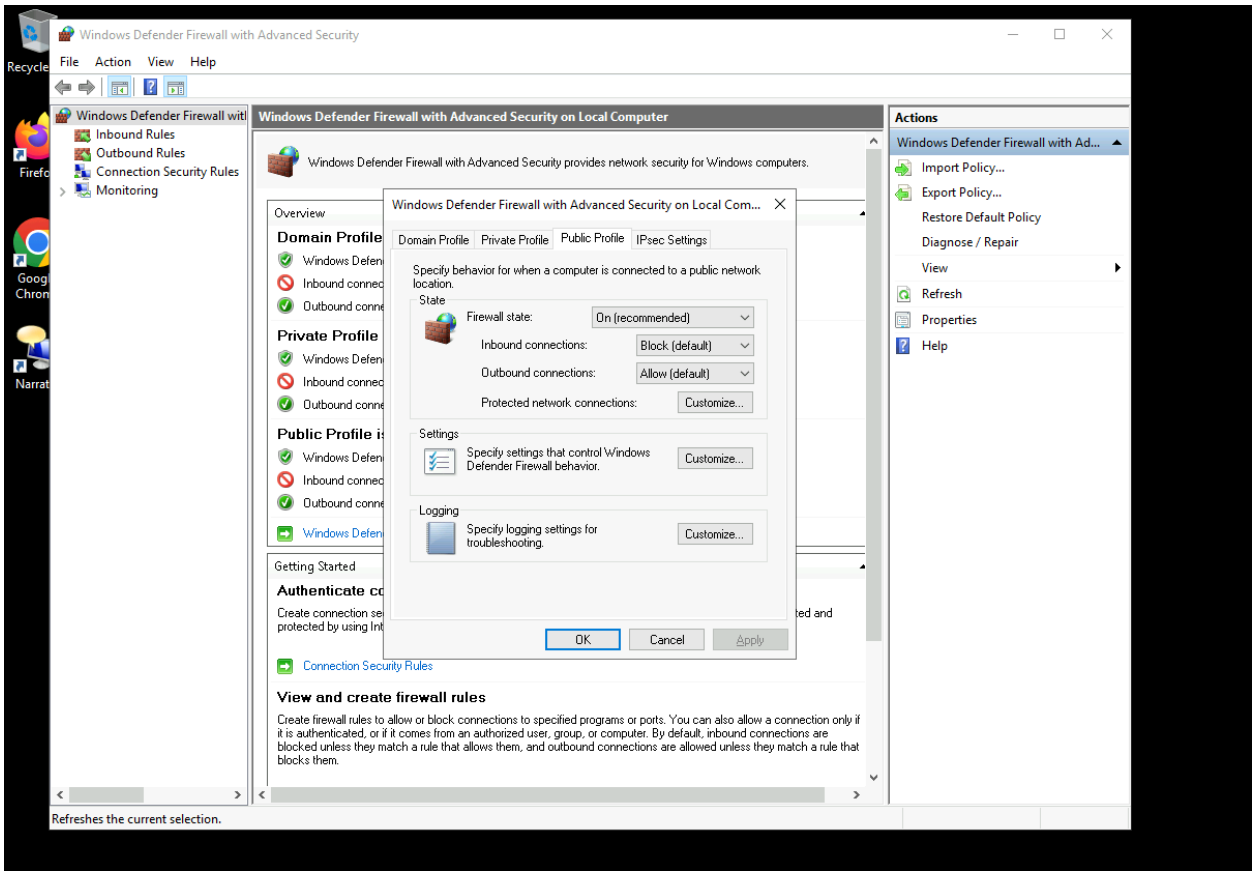
1. Start your Virginia Cyber Range Virtual Lab.
2. Press **Windows Key + R**.
3. The **Run** window will open.
4. Type:
   `wf.msc`
5. Click **OK** or press **Enter**.
6. **Windows Defender Firewall with Advanced Security** will open.
7. Take a screenshot showing the firewall console.



Windows Defender Firewall with Advanced Security is an application that allows for the creation of firewall policies and modification of inbound and outbound rules. The significance of this application is to ensure that unwanted network traffic is not allowed on a network or device.

Task 2: Examine Firewall Profiles

1. In the left panel, click **Windows Defender Firewall with Advanced Security on Local Computer**.
2. In the middle panel, click **Windows Defender Firewall Properties**.
3. Examine the following profiles:
    - Domain Profile
    - Private Profile
    - Public Profile
4. Record whether the firewall is **On or Off** for each profile.
5. Take a screenshot of the Firewall Properties window.



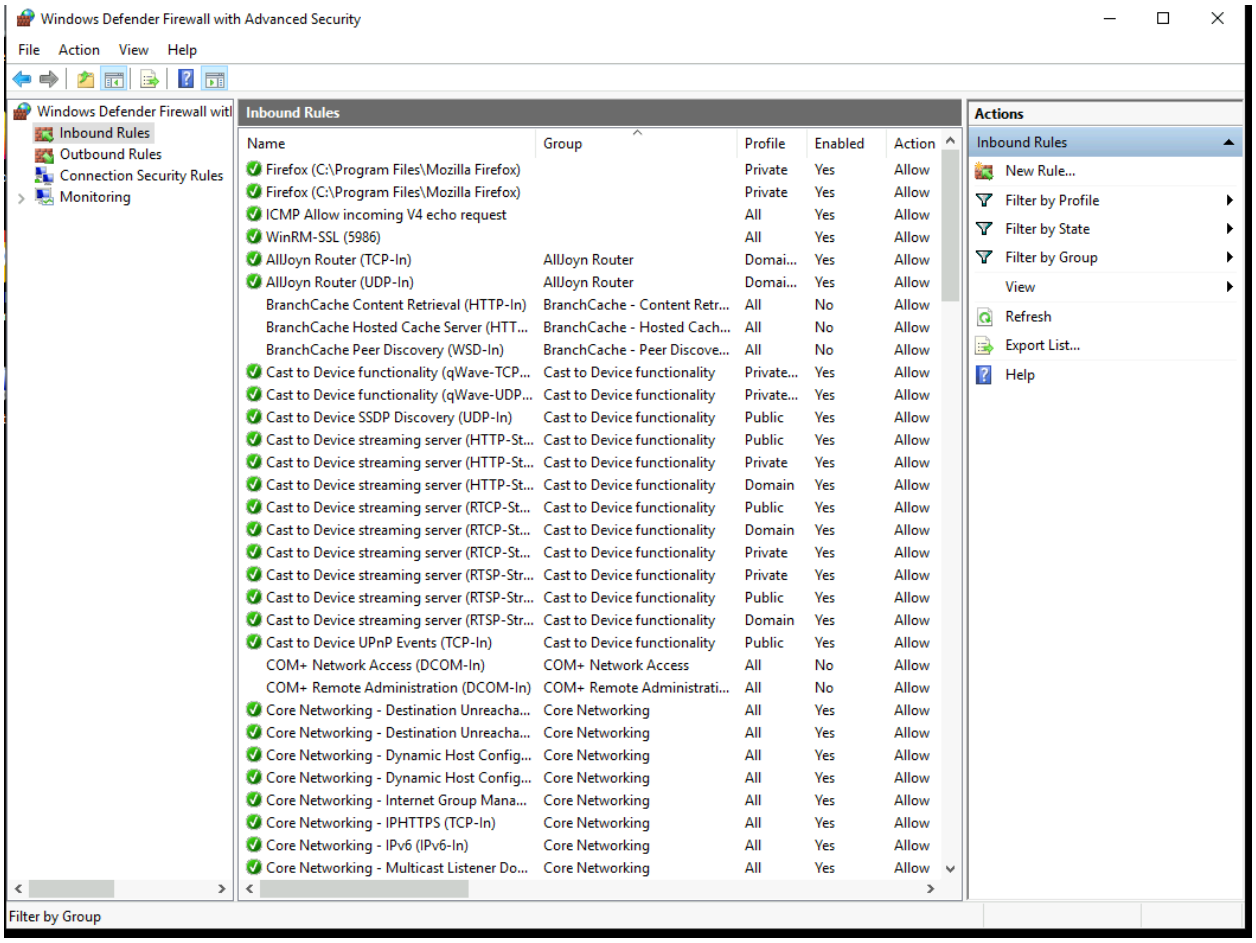
The firewall is enabled for all three profiles. The profiles apply when a device is connected to a corporate managed network, a private network, or a public network. For example, a public network would require stricter firewall rules than a personal home network.

Task 3: Examine Inbound Rules

1. Close the Firewall Properties window.
2. In the left panel, click **Inbound Rules**.
3. Examine several existing rules.
4. Identify:

- Rule name
- Enabled/Disabled status
- Protocol
- Local port
- Action (Allow/Block)

5. Take a screenshot showing the Inbound Rules list.

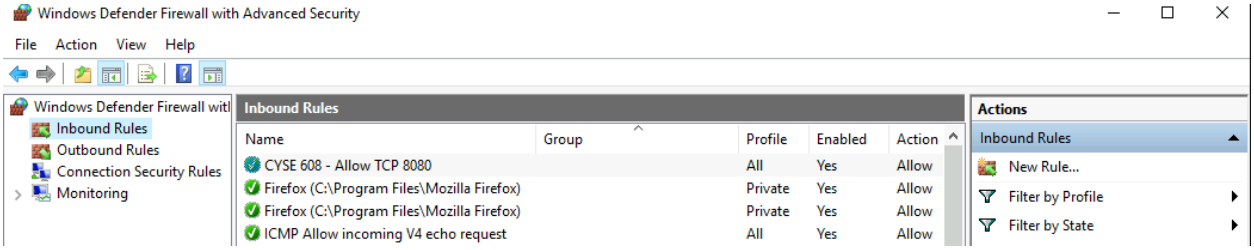


Inbound firewall rules control inbound traffic. Specifically what connections and ports should be allowed or blocked.

Task 4: Create an Inbound Firewall Rule

1. Right-click **Inbound Rules**.
2. Select **New Rule**.
3. Select **Port**.
4. Click **Next**.
5. Select **TCP**.
6. Select **Specific local ports**.

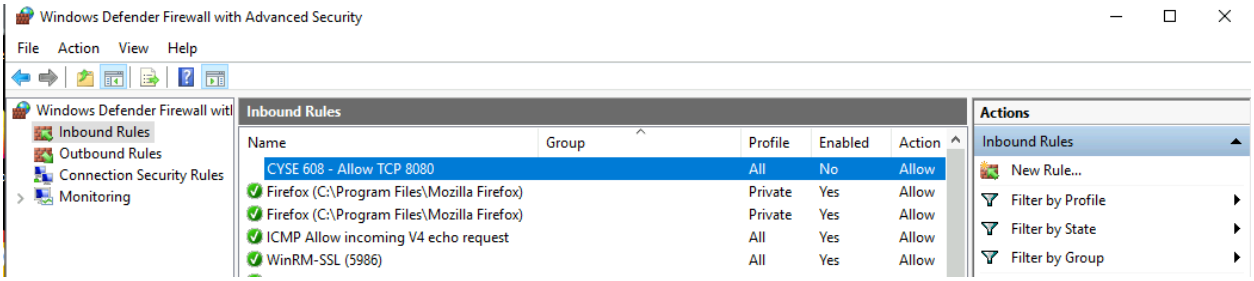
7. Enter:
   `8080`
8. Click **Next**.
9. Select **Allow the connection**.
10. Click **Next**.
11. Select:
    - Domain
    - Private
    - Public
12. Click **Next**.
13. Name the rule:
    `CYSE 680 - Allow TCP 8080`
14. Click **Finish**.
15. Find your new rule in the Inbound Rules list.
16. Take a screenshot showing the rule.

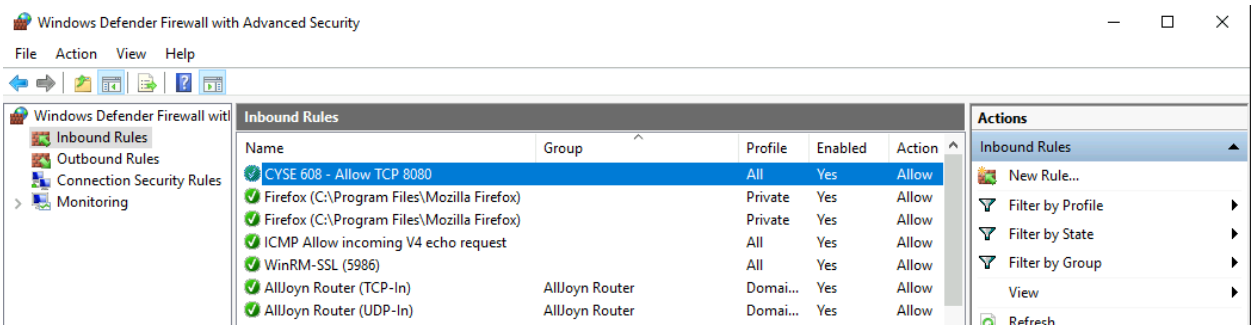


This rule allows incoming TCP traffic on port 8080. Controlling inbound connections is important, as closing unnecessary ports limits the attack surface for attackers.

Task 5: Disable and Re-enable the Firewall Rule

1. Find **CYSE 680 - Allow TCP 8080**.
2. Right-click the rule.
3. Select **Disable Rule**.
4. Take a screenshot showing that the rule is disabled.
5. Right-click the same rule again.
6. Select **Enable Rule**.
7. Take another screenshot showing that the rule is enabled.

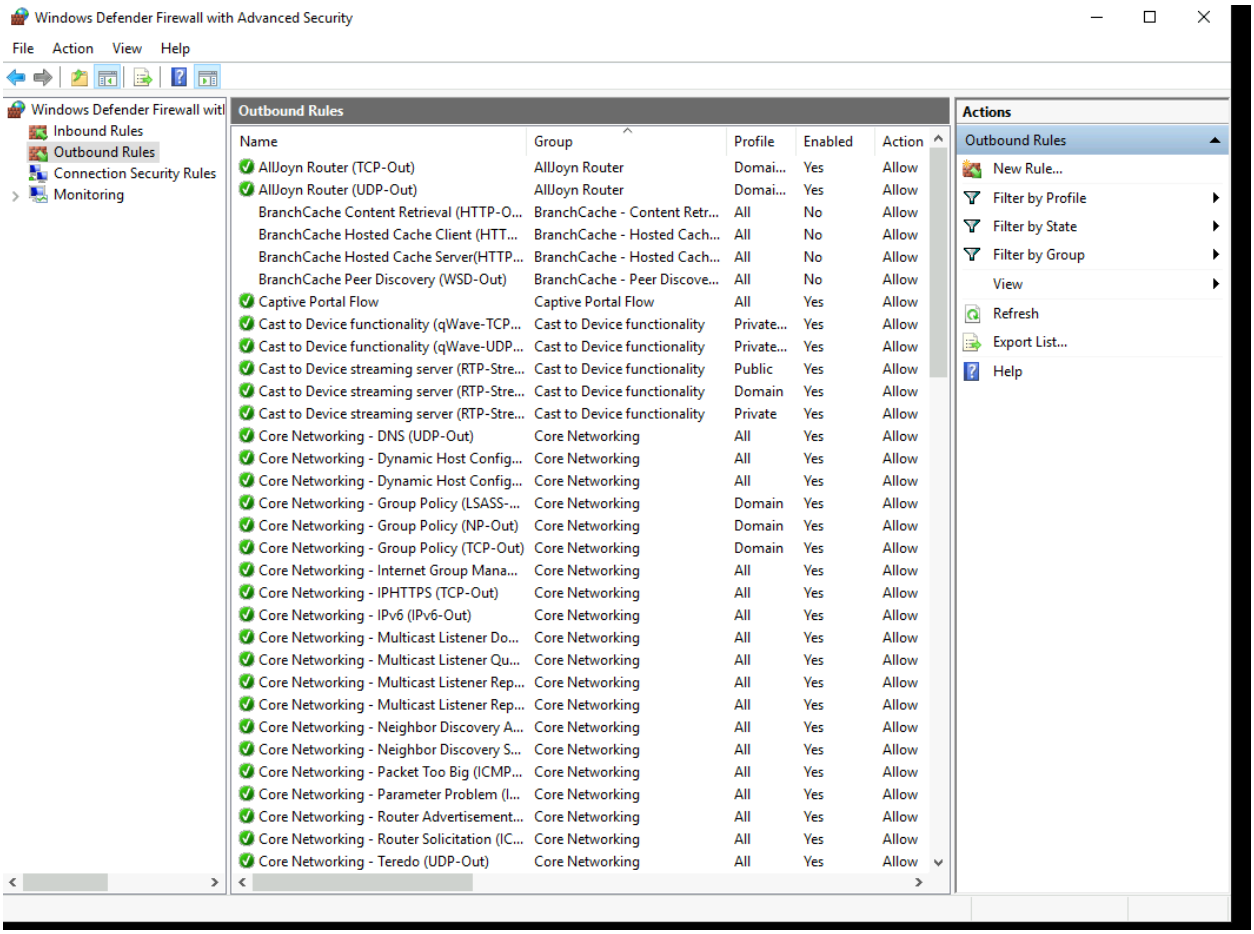




An enabled firewall rule means that the parameters set by the firewall rule are active. When disabled, the firewall rules are not applied.

Task 6: Examine Outbound Rules

1. Click **Outbound Rules** on the left.
2. Examine several existing rules.
3. Identify:
    - Rule name
    - Enabled/Disabled status
    - Protocol
    - Port
    - Action
4. Take a screenshot.

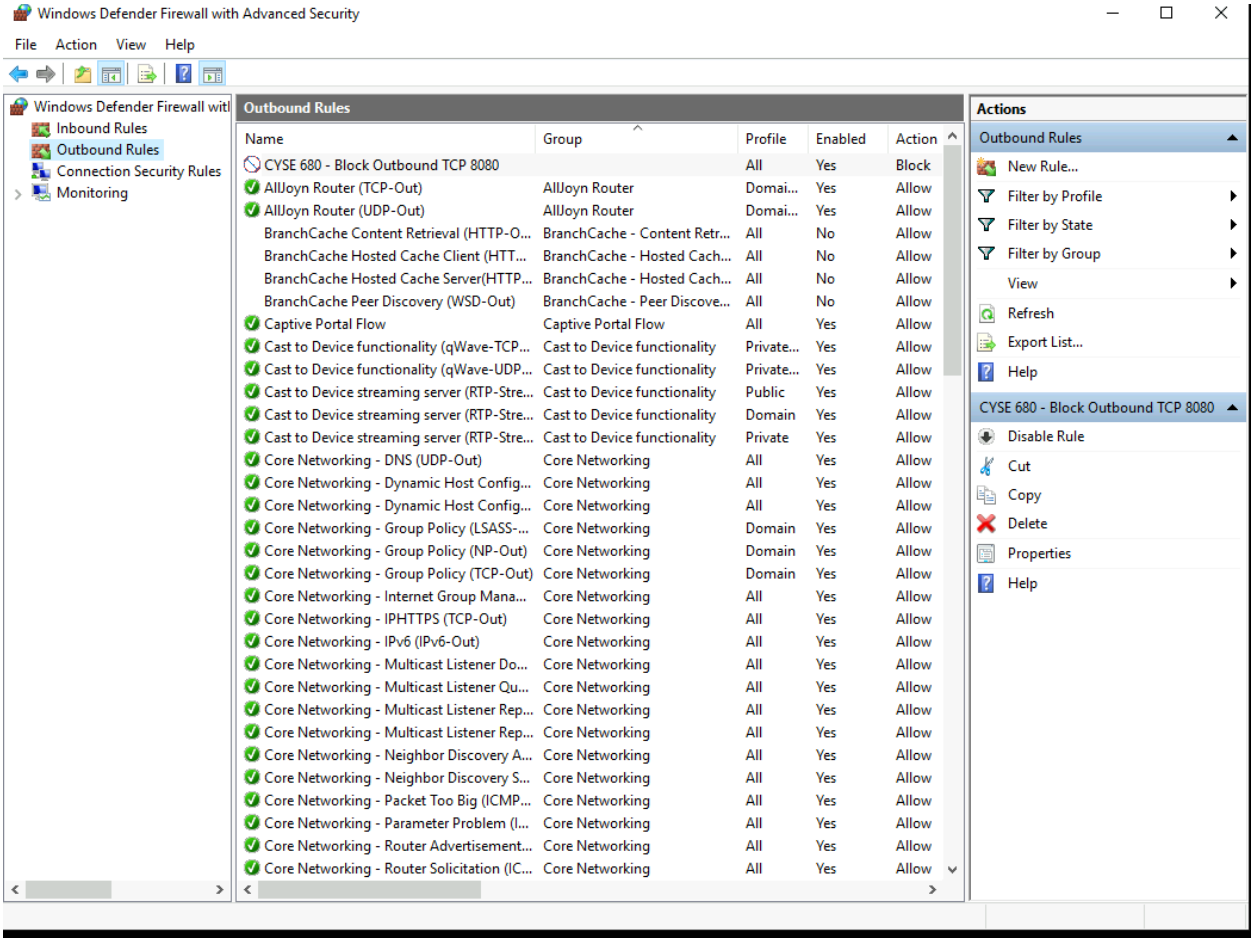


Outbound rules deal with outbound network traffic. While inbound manages inbound connections, outbound manages outbound connections.

Task 7: Create an Outbound Block Rule

1. Right-click **Outbound Rules**.
2. Select **New Rule**.
3. Select **Port**.
4. Click **Next**.
5. Select **TCP**.
6. Select **Specific local ports**.
7. Enter:
   `8080`
8. Click **Next**.
9. Select **Block the connection**.
10. Click **Next**.
11. Select:
    - Domain
    - Private
    - Public

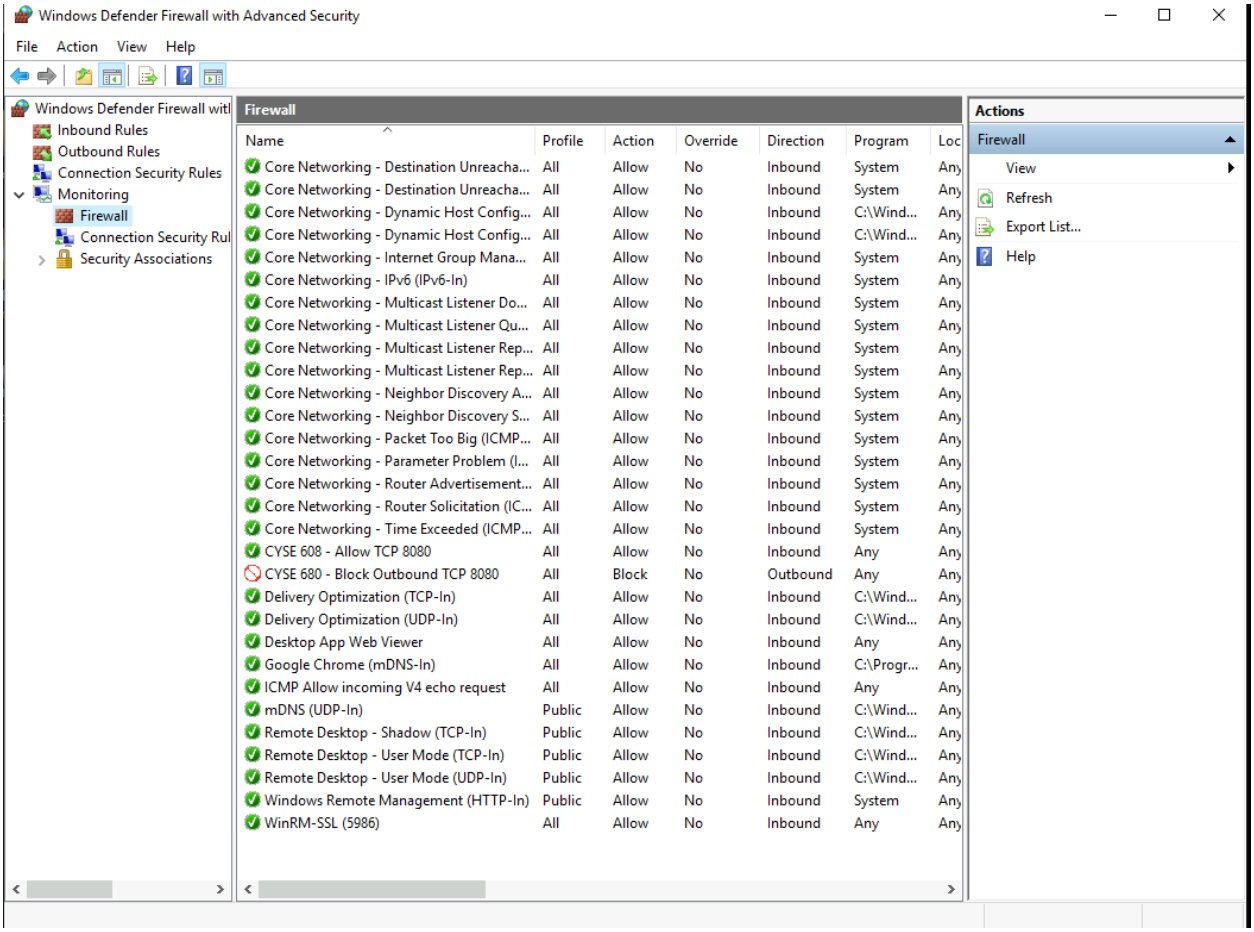
12. Click **Next**.
13. Name the rule:
    `CYSE 680 - Block Outbound TCP 8080`
14. Click **Finish**.
15. Take a screenshot showing the new rule.



An outbound rule manages outbound traffic. An organization may want this rule to prevent internal systems from connecting with outside devices.

Task 8: Examine Firewall Monitoring

1. In the left panel, expand:
   Monitoring
2. Select **Firewall** if available.
3. Examine the displayed firewall information.
4. Take a screenshot.



Monitoring is important for a cybersecurity professional as it allows an overview of all inbound and outbound rules. The details of the inbound and outbound rules are also visible.

Group Policy Section

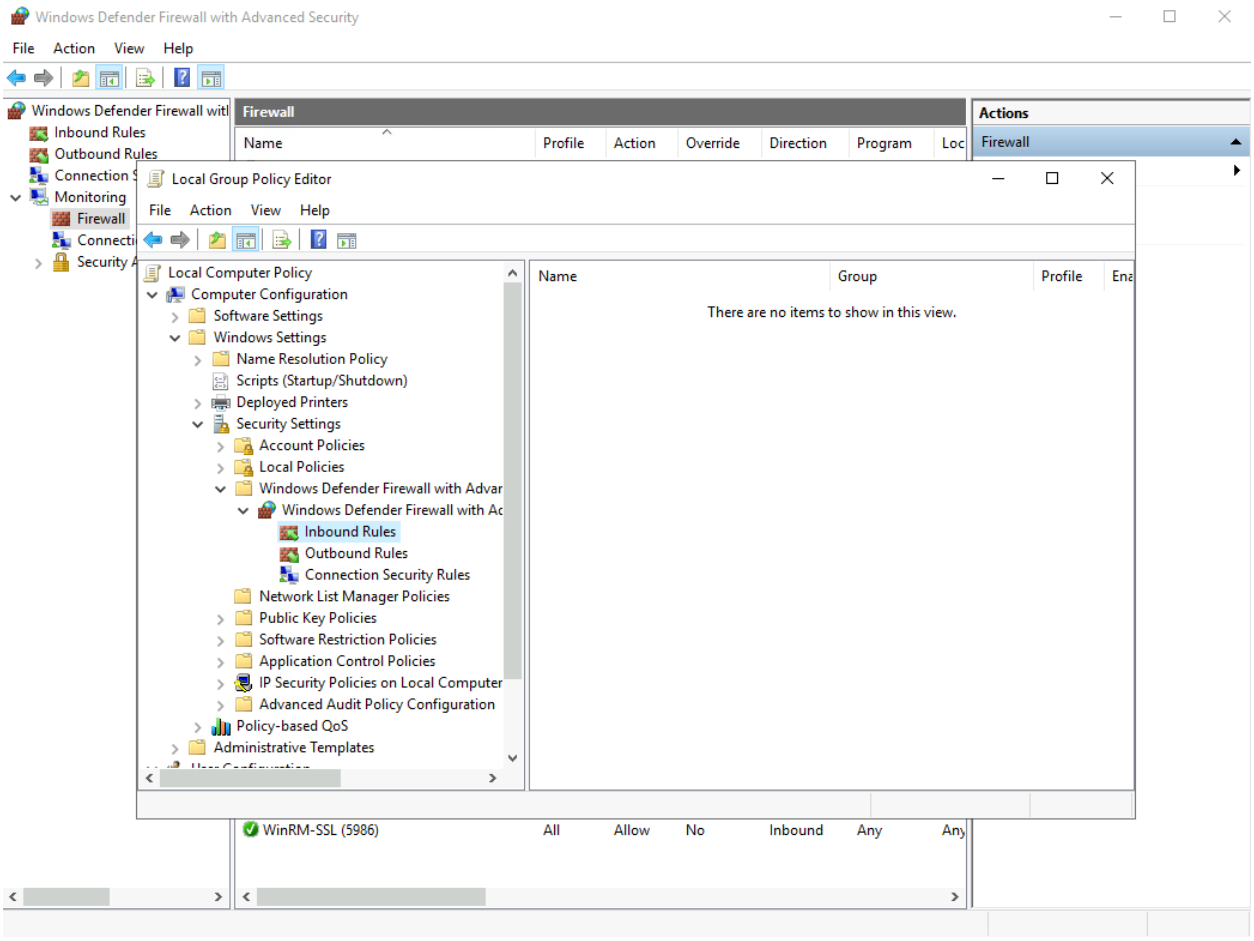
Task 9: Open Local Group Policy Editor

1. Press **Windows Key + R**.
2. The **Run** window will appear.
3. Type:
   `gpedit.msc`
4. Press **Enter**.
5. The **Local Group Policy Editor** will open.
6. On the left side, expand:

   Computer Configuration
   → Policies
   → Windows Settings

→ **Security Settings**
→ **Windows Defender Firewall with Advanced Security**

7. Expand **Windows Defender Firewall with Advanced Security**.
8. Click **Inbound Rules**.
9. Take a screenshot showing this navigation path.



Group Policy manages groups of users across a network or device. This can be useful for managing a large number of users without making changes to individual accounts.

Task 10: Create a Firewall Rule Through Group Policy

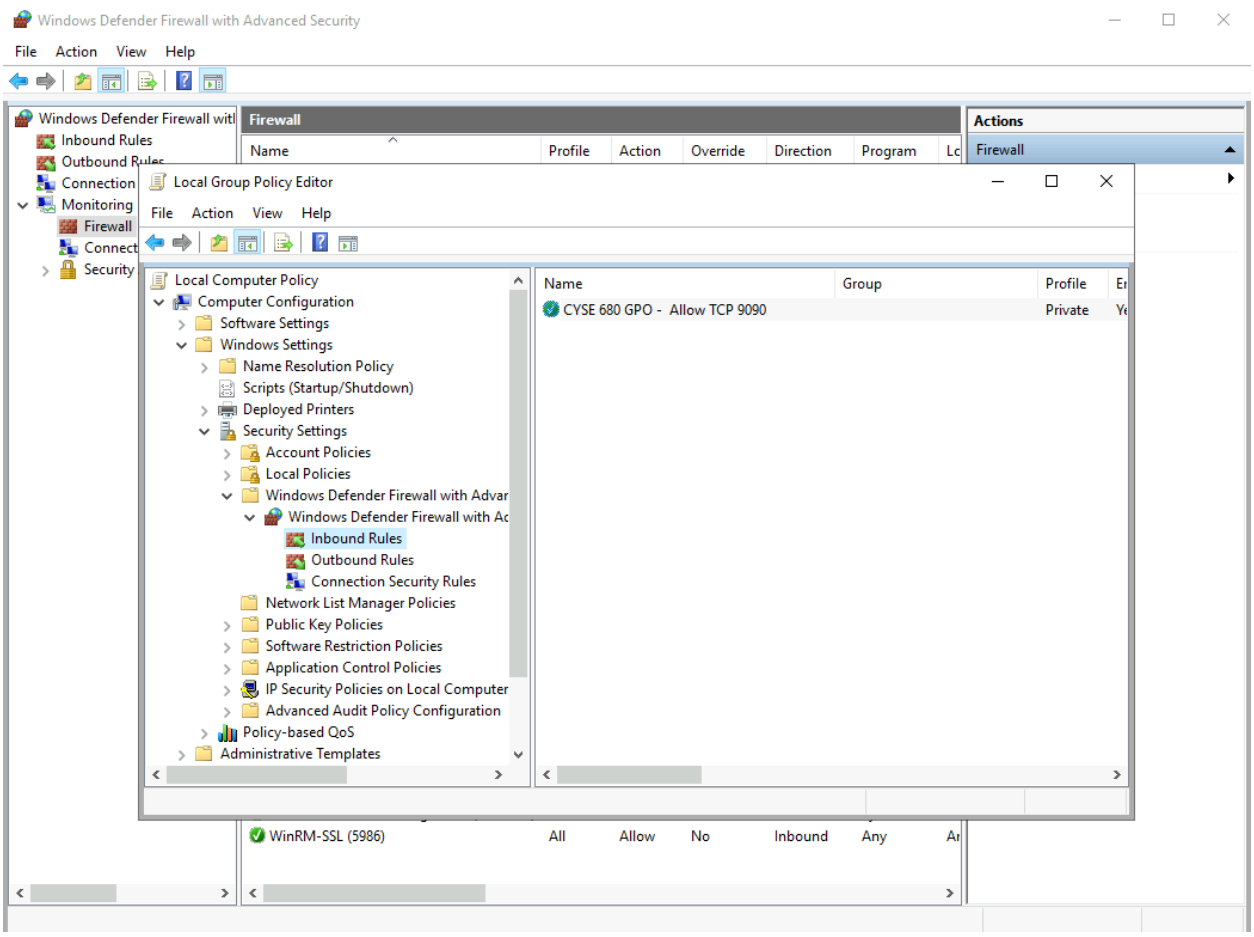
1. Make sure you are in:

   Computer Configuration → Policies → Windows Settings → Security Settings → Windows Defender Firewall with Advanced Security → Inbound Rules

2. Right-click **Inbound Rules**.
3. Select **New Rule**.
4. Select **Port**.
5. Click **Next**.
6. Select **TCP**.
7. Select **Specific local ports**.
8. Enter:
   `9090`
9. Click **Next**.
10. Select **Allow the connection**.
11. Click **Next**.
12. Select **Private**.
13. Click **Next**.
14. Enter the rule name:
    `CYSE 680 GPO - Allow TCP 9090`
15. In the description field, enter:

```
Firewall rule created through Group Policy for the CYSE 680 laboratory.
```

16. Click **Finish**.
17. Take a screenshot showing the new rule.



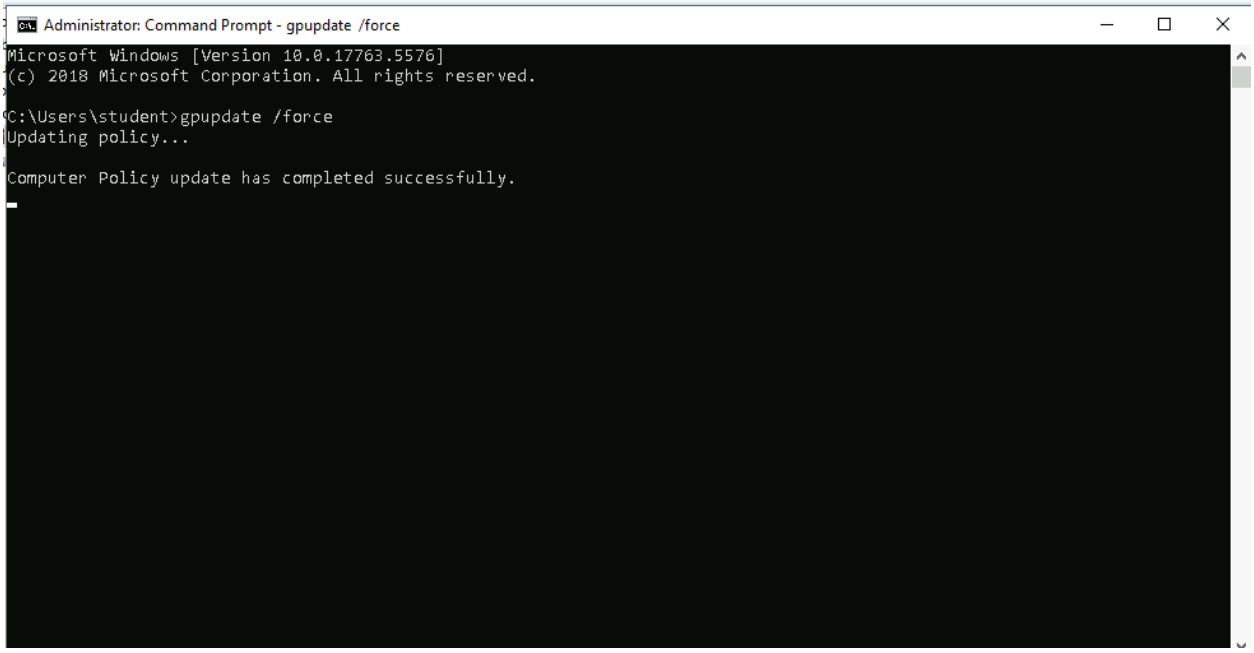
This can assist administrators in pushing firewall rules to specific users or groups. This can drastically reduce the time necessary to complete tasks.

Task 11: Apply the Group Policy

1. Press **Windows Key + R**.
2. Type:
   `cmd`
3. Press **Enter**.
4. In Command Prompt, type:

   ```
   gpupdate /force
   ```

5. Press **Enter**.
6. Wait until the update finishes.
7. Take a screenshot showing the completed `gpupdate /force` command.



Group Policy update is a command that updates the firewall policies. Force forces the command to run.

Task 12: Verify Firewall Rules Using PowerShell

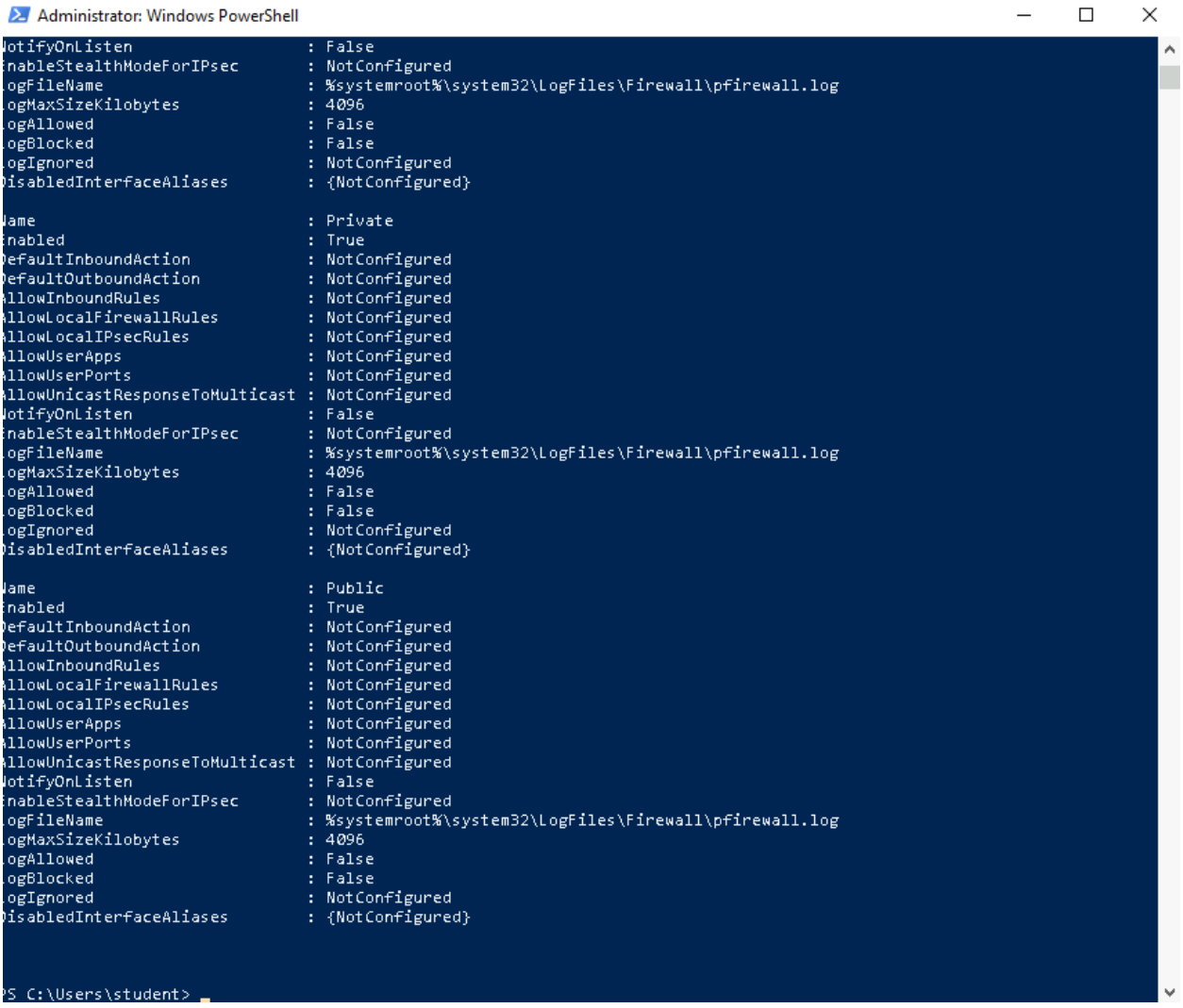
1. Right-click the **Start** button.
2. Open **Windows PowerShell** or **Terminal**.
3. Run:

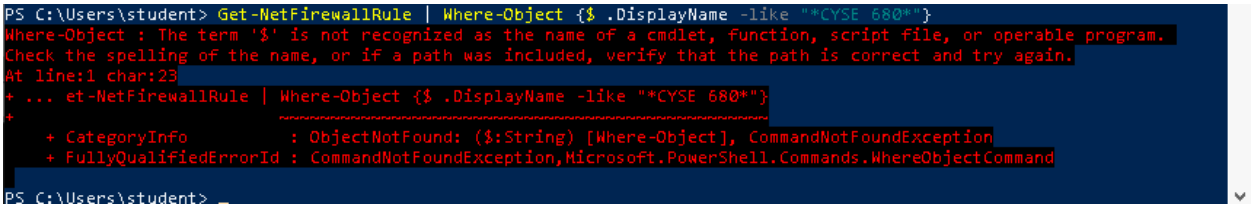
```
Get-NetFirewallProfile
```

4. Take a screenshot of the results.
5. Then run:

```
Get-NetFirewallRule | Where-Object {$_.DisplayName -like "*CYSE 680*"}
```

6. Take a screenshot showing your CYSE 680 firewall rules.





PowerShell is a powerful tool for managing firewall configurations. It allows commands to be run from a centralized location to view and edit firewall rules while also allowing the management of other systems.

Task 13: Temporarily Disable and Re-enable the Private Firewall Profile

Perform this task only inside your laboratory VM.

1. Open **PowerShell as Administrator**.
2. Check the current firewall status:

```
Get-NetFirewallProfile
```

3. Temporarily disable the Private profile:

```
Set-NetFirewallProfile -Profile Private -Enabled False
```

4. Verify the change:

```
Get-NetFirewallProfile -Profile Private
```

5. Take a screenshot.
6. **Immediately re-enable the firewall:**

```
Set-NetFirewallProfile -Profile Private -Enabled True
```

7. Verify again:

```
Get-NetFirewallProfile -Profile Private
```

8. Take another screenshot.

```
PS C:\Users\student> Set-NetFirewallProfile -Profile Private -Enabled False
PS C:\Users\student> Get-NetFirewallProfile -Profile Private


Name                            : Private
Enabled                         : False
DefaultInboundAction            : NotConfigured
DefaultOutboundAction           : NotConfigured
AllowInboundRules               : NotConfigured
AllowLocalFirewallRules         : NotConfigured
AllowLocalIPsecRules            : NotConfigured
AllowUserApps                   : NotConfigured
AllowUserPorts                  : NotConfigured
AllowUnicastResponseToMulticast : NotConfigured
NotifyOnListen                  : False
EnableStealthModeForIPsec       : NotConfigured
LogFileName                     : %systemroot%\system32\LogFiles\Firewall\pfirewall.log
LogMaxSizeKilobytes             : 4096
LogAllowed                      : False
LogBlocked                      : False
LogIgnored                      : NotConfigured
DisabledInterfaceAliases        : {NotConfigured}
```

```
PS C:\Users\student> Set-NetFirewallProfile -Profile Private -Enabled True
PS C:\Users\student> Get-NetFirewallProfile -Profile Private


Name                            : Private
Enabled                         : True
DefaultInboundAction            : NotConfigured
DefaultOutboundAction           : NotConfigured
AllowInboundRules               : NotConfigured
AllowLocalFirewallRules         : NotConfigured
AllowLocalIPsecRules            : NotConfigured
AllowUserApps                   : NotConfigured
AllowUserPorts                  : NotConfigured
AllowUnicastResponseToMulticast : NotConfigured
NotifyOnListen                  : False
EnableStealthModeForIPsec       : NotConfigured
LogFileName                     : %systemroot%\system32\LogFiles\Firewall\pfirewall.log
LogMaxSizeKilobytes             : 4096
LogAllowed                      : False
LogBlocked                      : False
LogIgnored                      : NotConfigured
DisabledInterfaceAliases        : {NotConfigured}


PS C:\Users\student>
```

Disabling firewall rules provides a larger attack surface fore potential attackers. We immediately re-enable the firewall to ensure that the virtual environment remains secure.

Task 14: Clean Up the Laboratory Environment

1. Open `wf.msc`.
2. Go to **Inbound Rules**.
3. Find:
   `CYSE 680 - Allow TCP 8080`
4. Right-click it and select **Delete**.
5. Go to **Outbound Rules**.
6. Find:
   `CYSE 680 - Block Outbound TCP 8080`

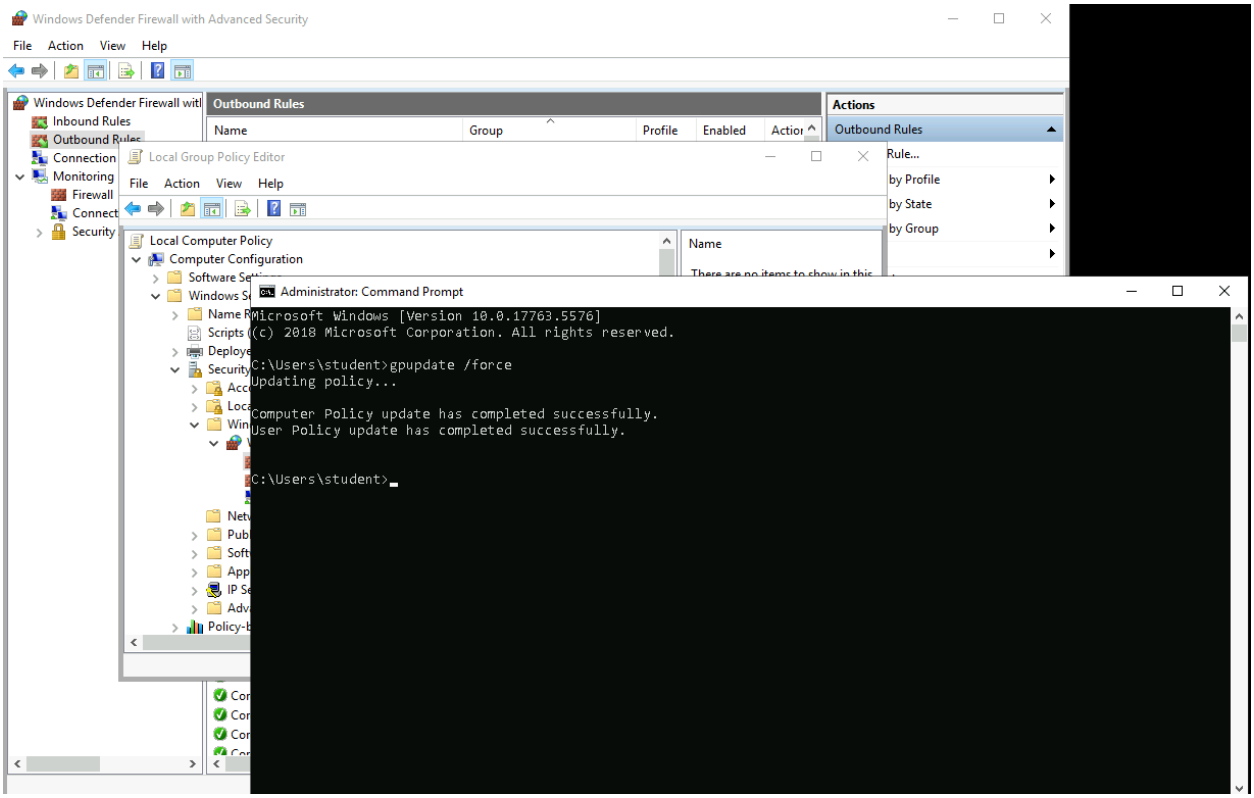
7. Right-click it and select **Delete**.
8. Open `gpedit.msc`.
9. Navigate to:

   Computer Configuration → Policies → Windows Settings → Security Settings → Windows Defender Firewall with Advanced Security → Inbound Rules

10. Remove the temporary **CYSE 680 GPO - Allow TCP 9090** rule if required by your instructor.
11. Run:

```
gpupdate /force
```

12. Make sure your **Private Firewall Profile is enabled** before finishing the lab.



Temporary firewall rules should be removed after testing as leaving port open could be a security risk. Generally, default firewall rules are sufficient for security; however, sometimes they may need to be modified.