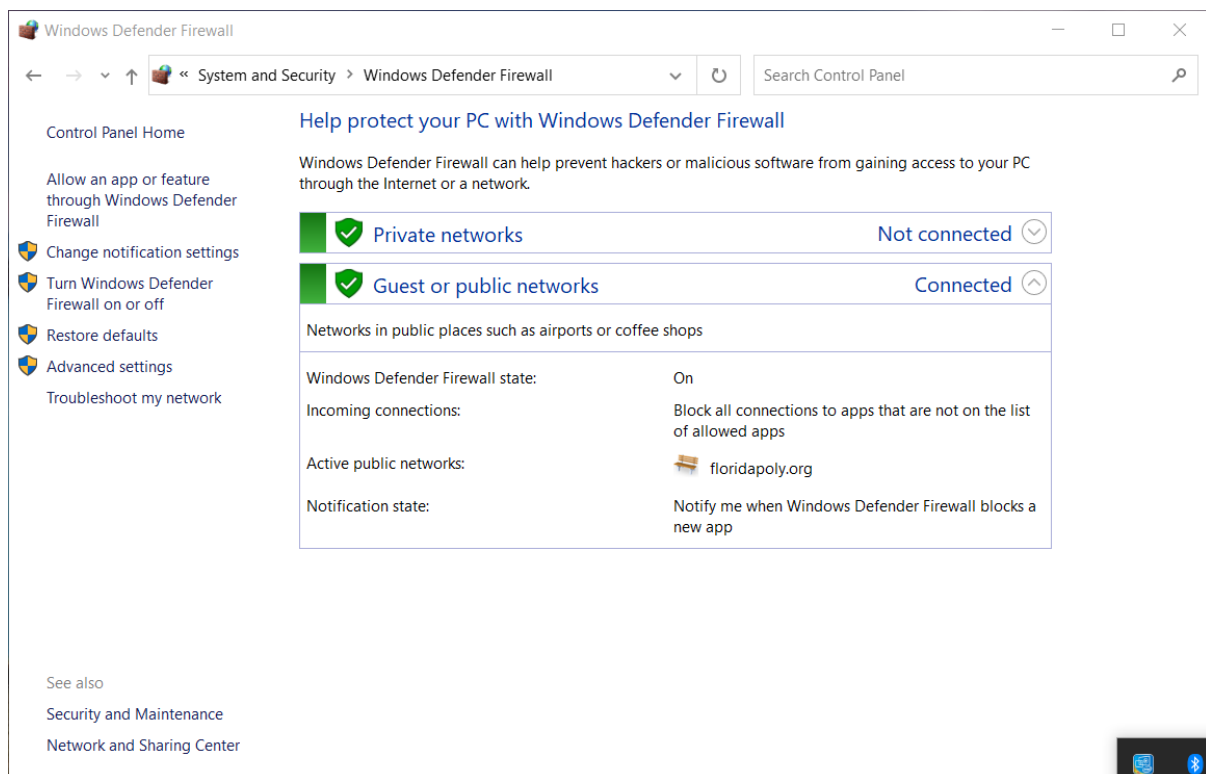


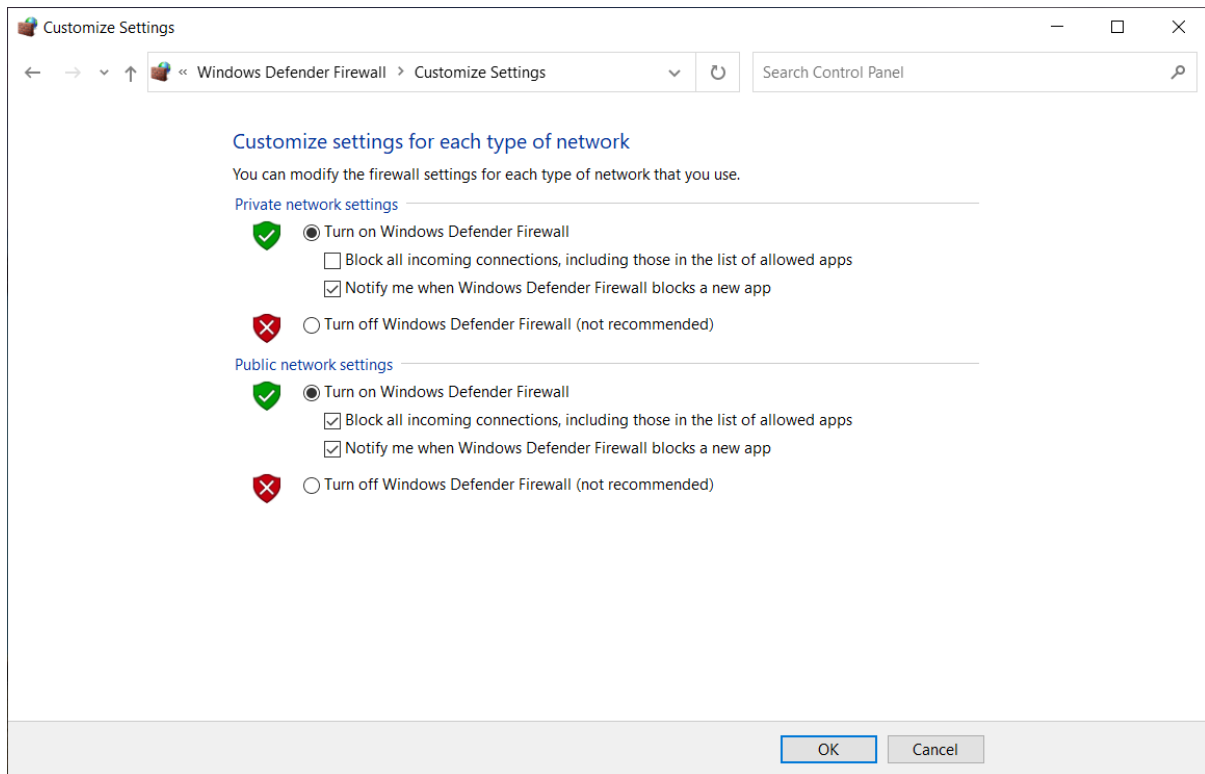
Lab Homework 1: Configuring Windows Firewall

Part A

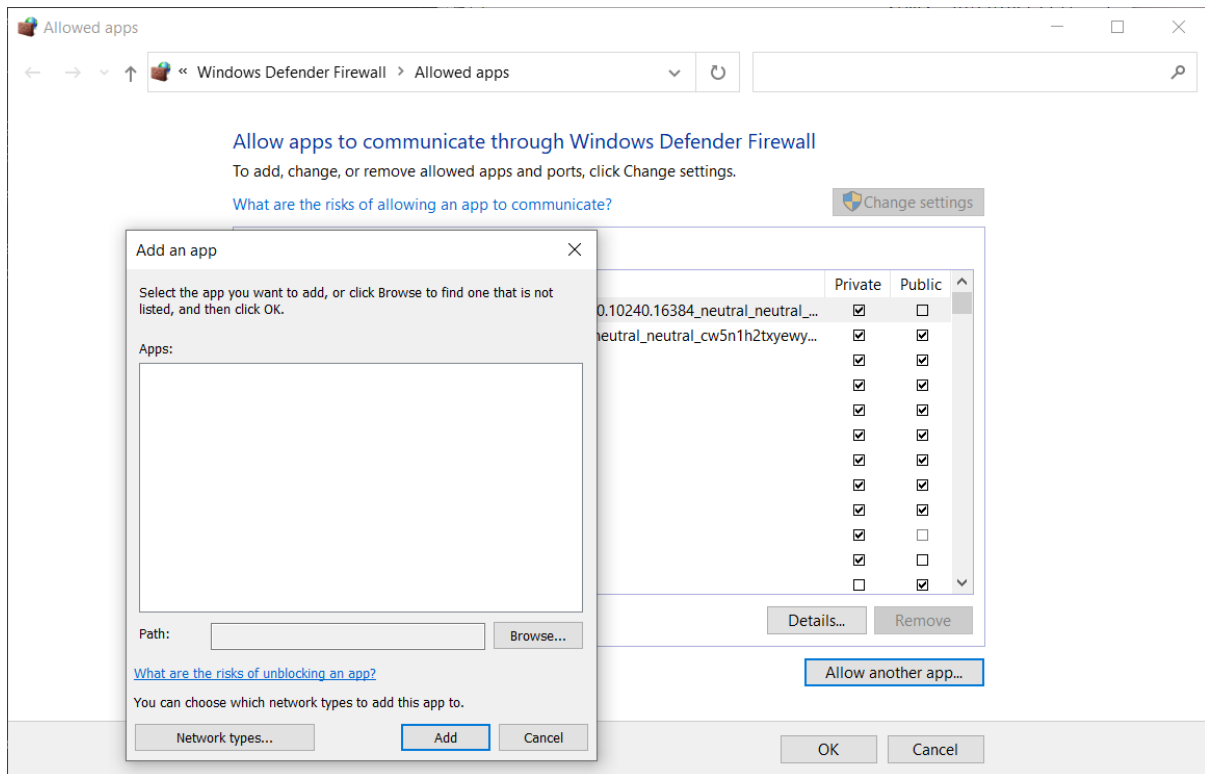
1. Navigate to the Windows Firewall menu through the System and Security settings in the Windows Control Panel.



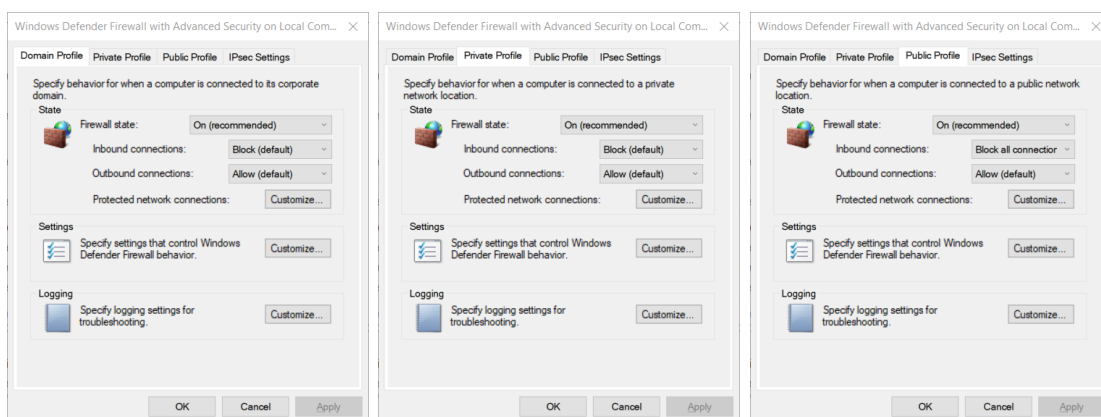
2. The Windows Firewall is active for both the **public** and **private** networks.
3. All incoming connections are disabled (including allowed programs) to avoid malicious incoming connections on public networks.



4. In order for applications to bypass the firewall, they have to be allowed in the firewalls **Allowed Apps**
5. Each program can be allowed through the public, private or both networks.
6. We do not allow any apps to bypass the public firewall because this is a security risk.



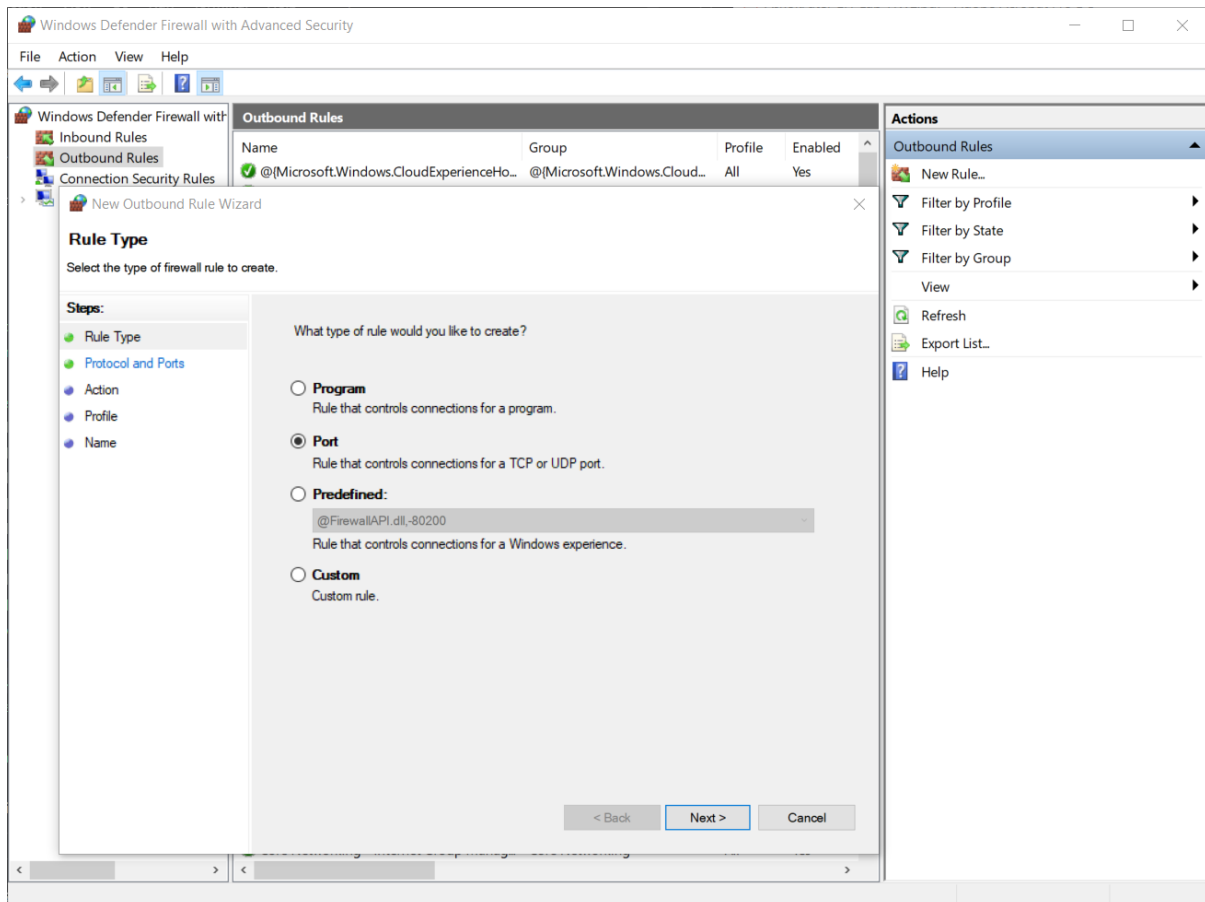
7. Navigate to the **Advanced Settings** to further examine the properties of the Windows firewall.
8. Navigate to the **Windows Firewall Properties**
9. Viewing the settings for each of the Domain, Public and Private profiles, the Public profile has the property: **Block all connections** under the **Inbound Connections** setting because this setting was altered in step 3.



10. Having the **Display a notification** enabled when a program is blocked by the firewall is important so that the user has the knowledge that a program was trying to gain access, allowing them to take the necessary actions.
11. Now we return to the Windows firewall advanced security page.

Part B

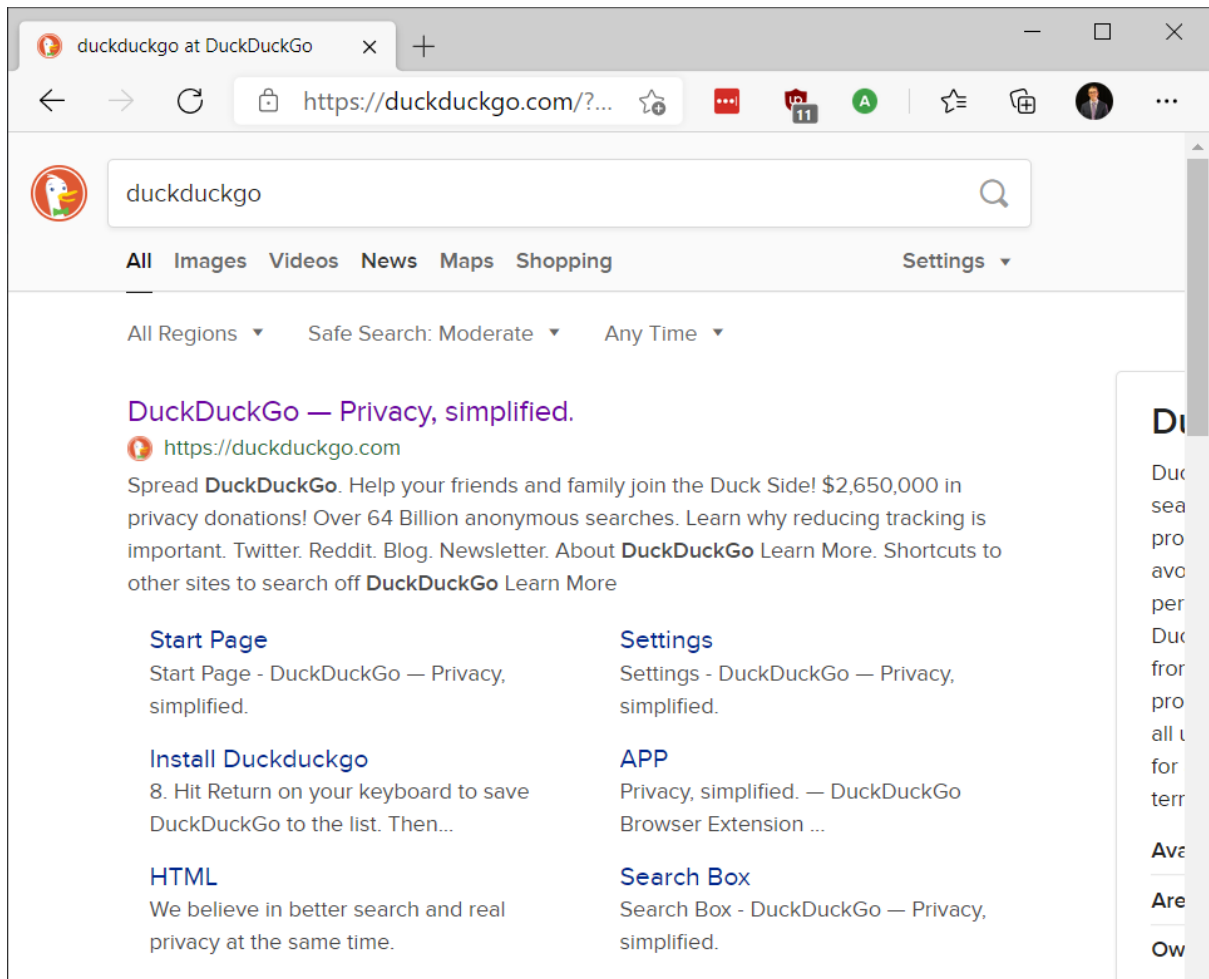
12. Windows Firewall can disallow connections from specific applications, or **outbound rules** can be set to block programs from reaching the internet. Navigate to the **Outbound Rules** section.
13. To create a new outbound rule, click the **New rule** option.
14. We create a **Port** rule.



15. The rule applies to **TCP** connections.
16. Port 80 is the specific port that will be blocked by this rule.

The screenshot shows the 'New Outbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The window title is 'New Outbound Rule Wizard' with a close button (X) in the top right corner. Below the title bar, the section is titled 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps:' sidebar lists five steps: 'Rule Type' (green dot), 'Protocol and Ports' (green dot and highlighted), 'Action' (blue dot), 'Profile' (blue dot), and 'Name' (blue dot). The main area contains two questions. The first is 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' (selected) and 'UDP'. The second is 'Does this rule apply to all remote ports or specific remote ports?' with radio buttons for 'All remote ports' and 'Specific remote ports:' (selected). Below the 'Specific remote ports:' radio button is a text input field containing '80'. Below the input field is an example text: 'Example: 80, 443, 5000-5010'. At the bottom right, there are three buttons: '< Back' (disabled), 'Next >' (active/highlighted), and 'Cancel' (disabled).

17. With the port specified, **Block the connection** is selected to disable the port.
18. We apply the rule to all three firewall domains: Public, Private and Domain.
19. We name the rule **Block Port 80** to finalize the creation.
20. Attempting to connect to a website using an **HTTPS** connection is still allowed because the connection does not use port 80.



21. While connecting using **HTTP** the access is blocked because port 80 is not enabled, thus not allowing traffic to the website.

