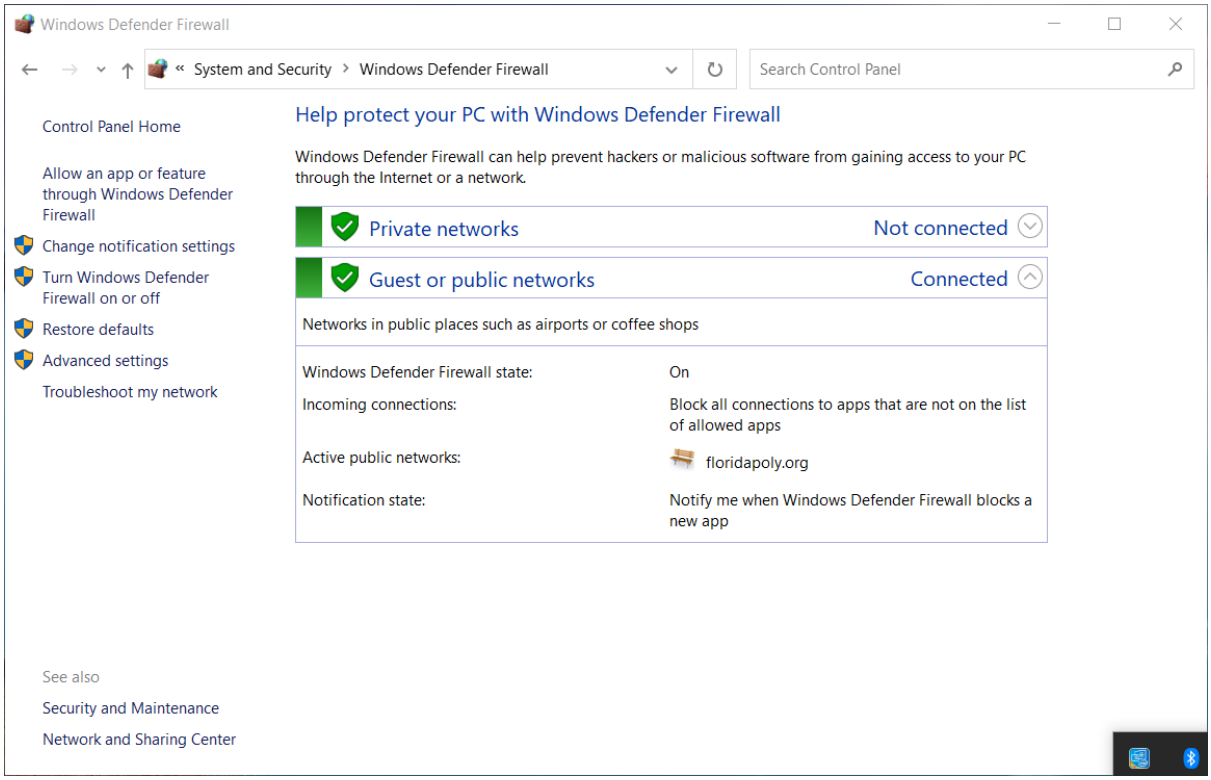
CIS4204.01 **Brandon Thompson**
Dr. Ashokkumar Patel Due: 1/24/21

Lab Homework 1: Configuring Windows Firewall

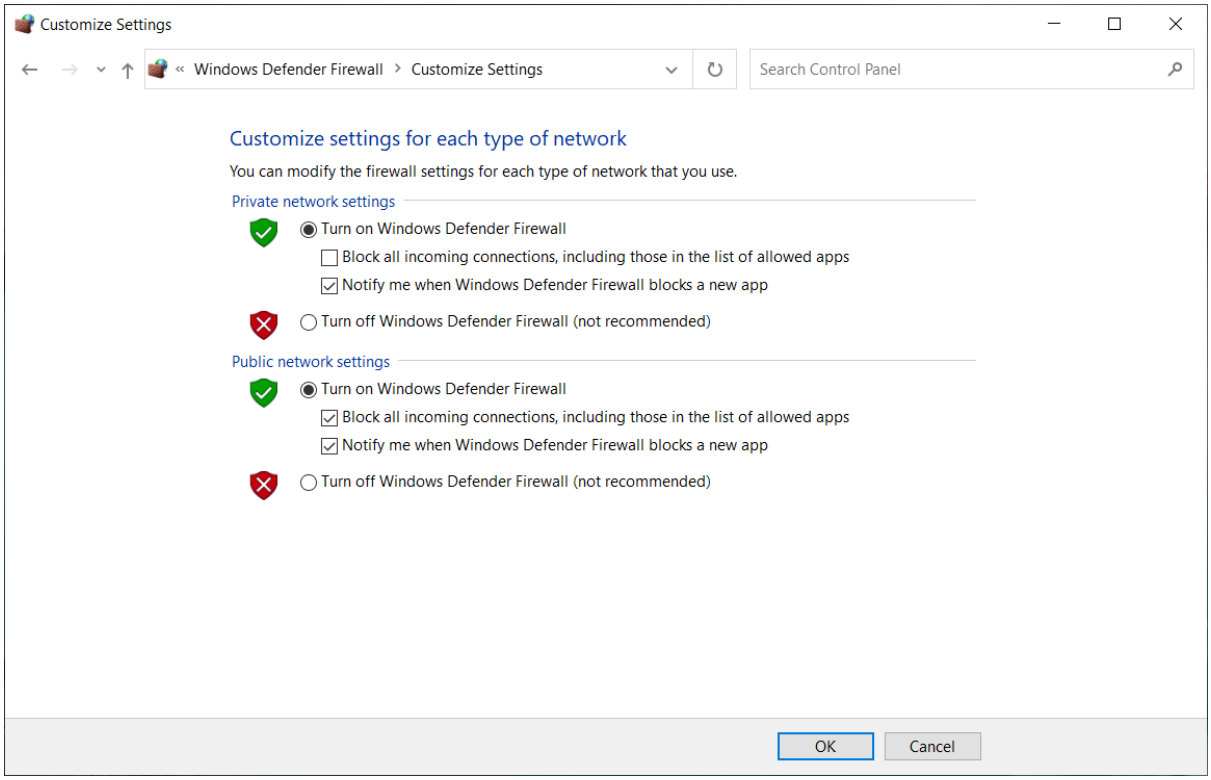
Part A

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.

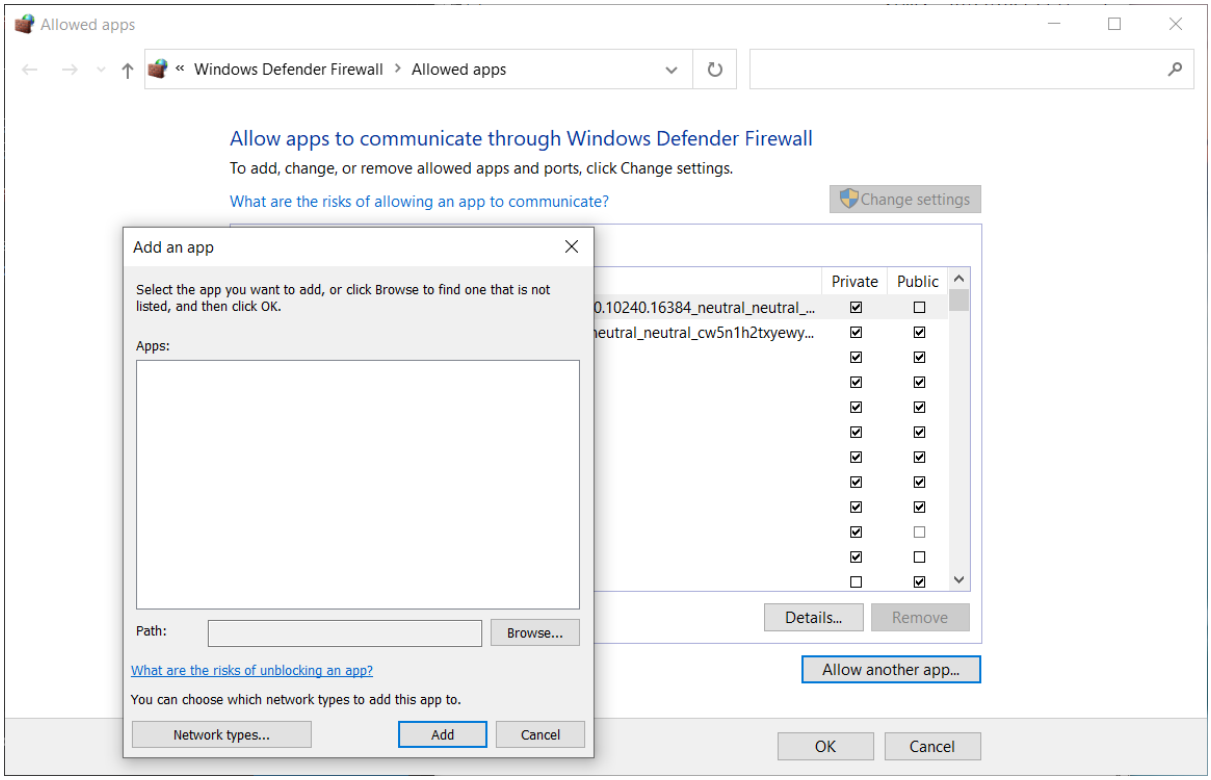
3. All incoming connections are disabled (including allowed programs) to avoid malicious incoming connections on public networks.



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.

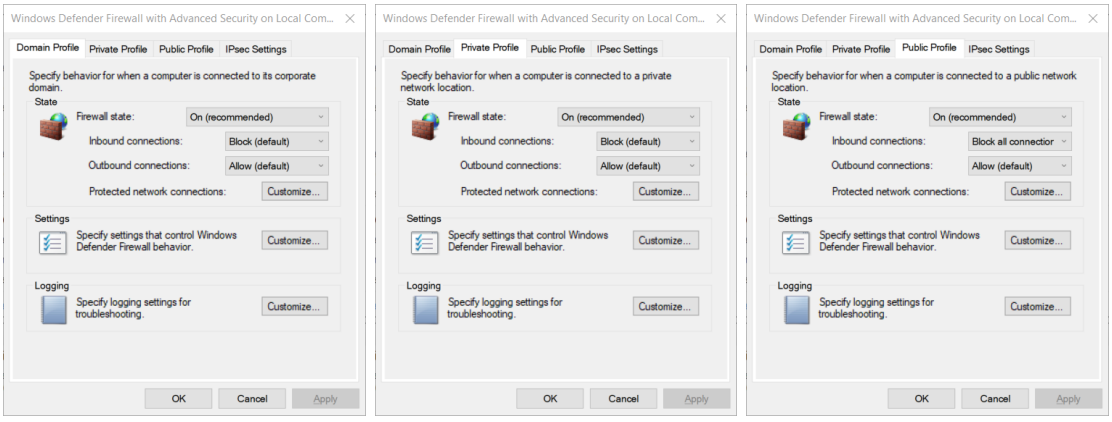
6. We do not allow any apps to bypass the public firewall because this is a security risk.



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.

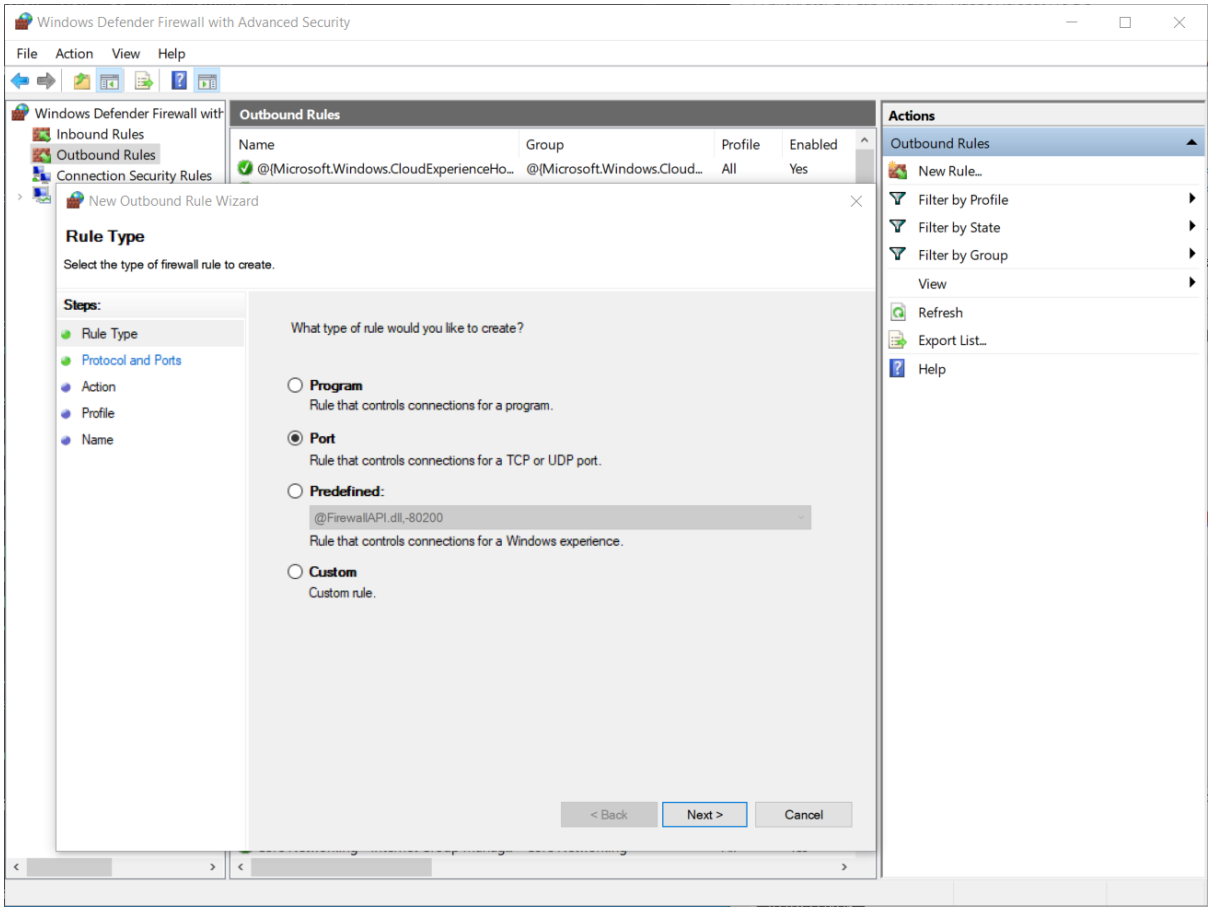
11. Now we return to the Windows firewall advanced security page.

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.

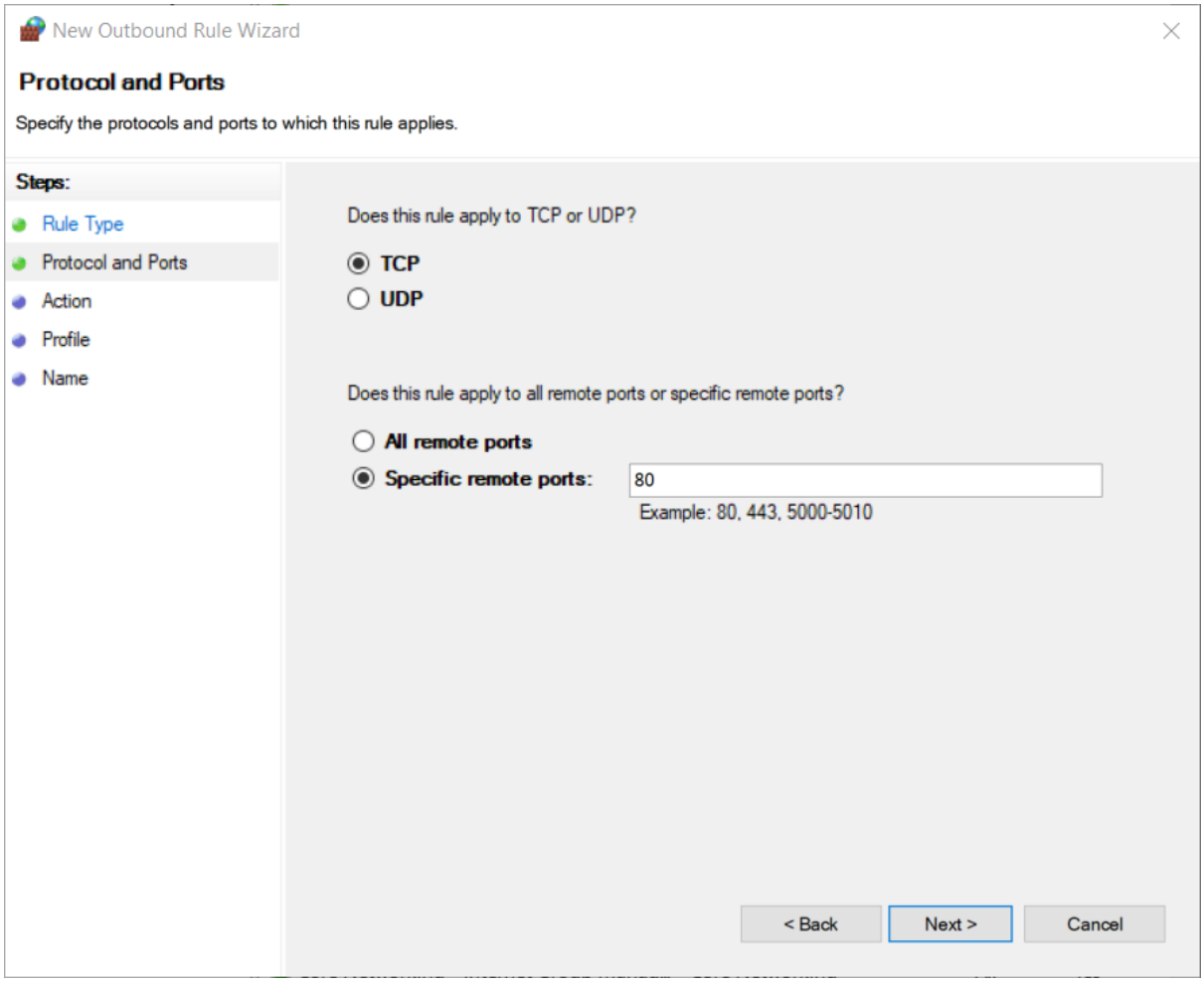
13. To create a new outbound rule, click the **New rule** option.

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.

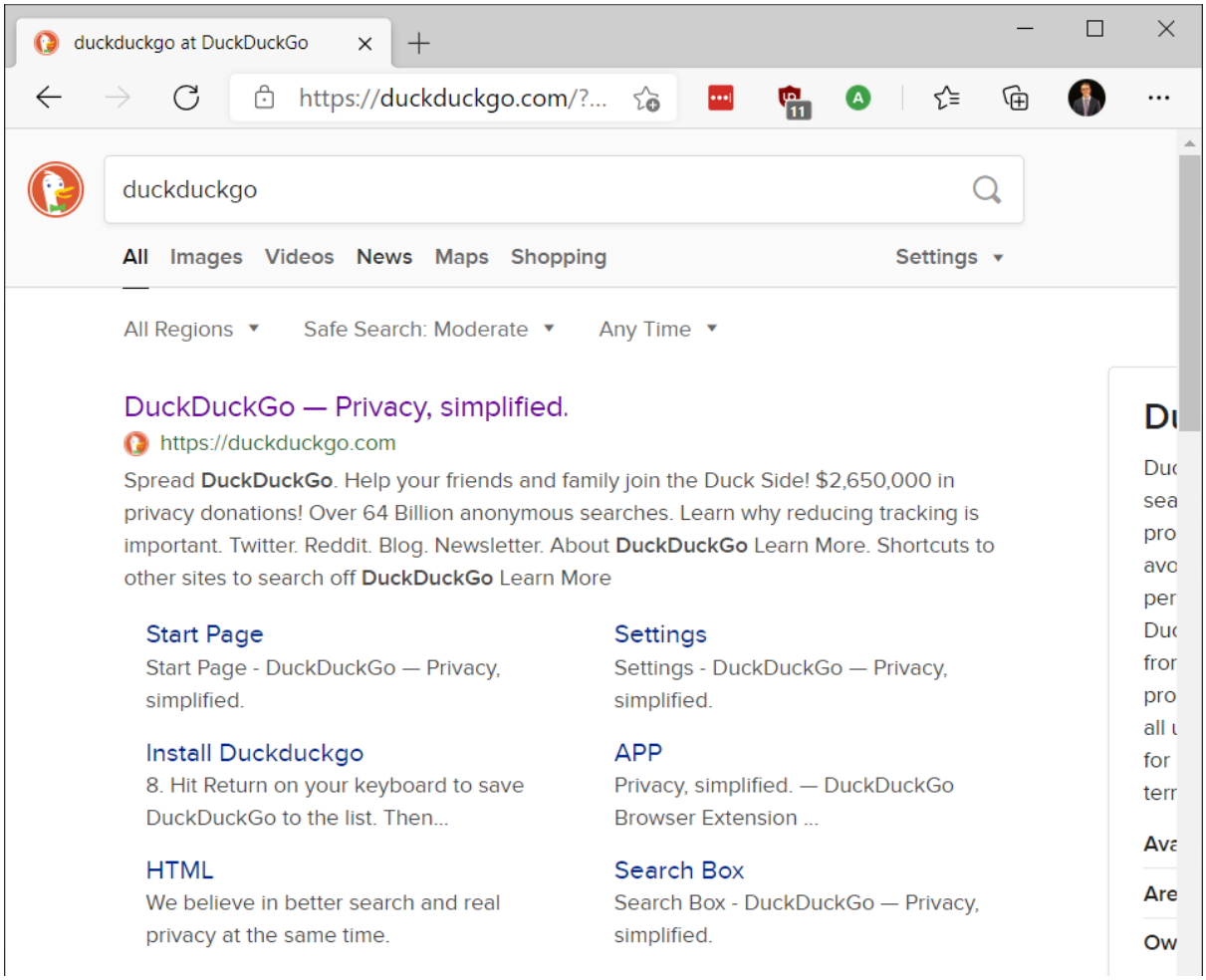


17. With the port specified, **Block the connection** is selected to disable the port.

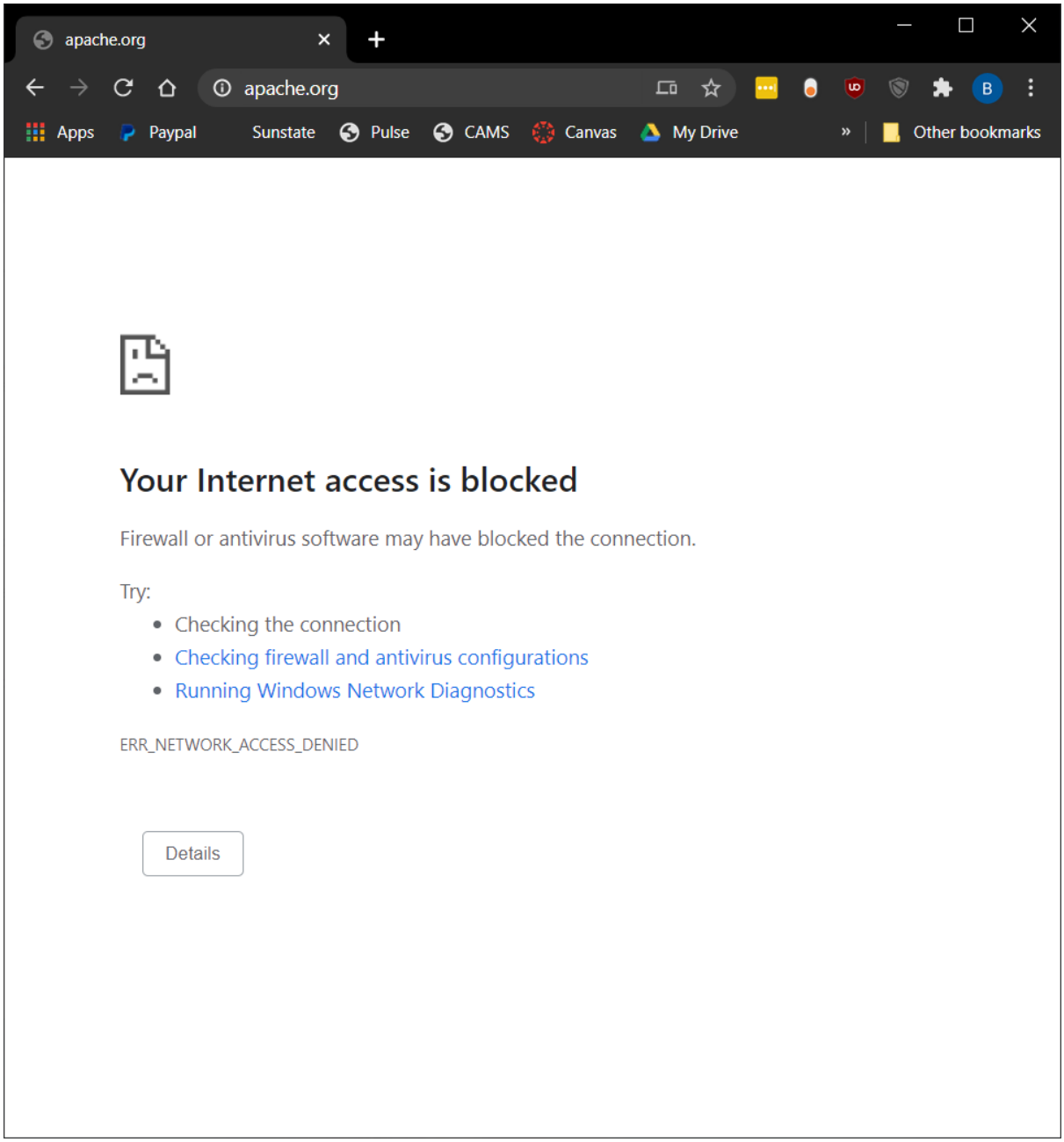
18. We apply the rule to all three firewall domains: Public, Private and Domain.

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.



During this lab we learned about configuring the Windows Firewall. The firewall monitors three types of networks, Domain, Public and Private. In Part A we disabled all incoming connections on the **Public** network to improve security, and validated this in the **Advanced Settings** menu. The Windows firewall is both application and rule based. You can disallow a specific application or create a rule that disables communication ports, stopping programs from communicating beyond the computer. In Part B we disable port 80, corresponding to unsecured web communication using HTTP. We then validated that the rule was working by visiting websites using HTTP and HTTPS. With the rule enabled we were unable to connect to any website using HTTP.