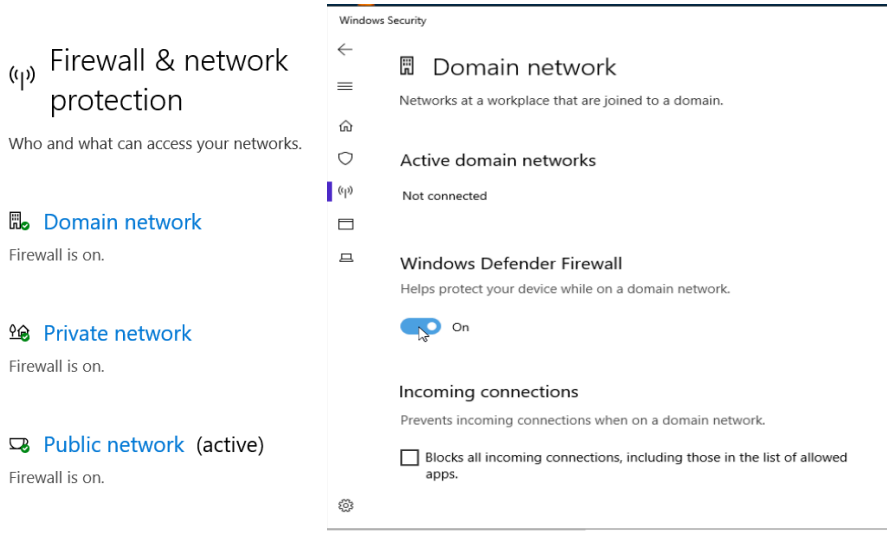
Enabling and configuring Microsoft Windows Defender Firewall to alter connectivity to networks

In this project I received instructions on how to enable Windows Firewall before configuring the firewall to allow some applications to connect to networks while blocking others.

Enabling Windows Defender Firewall for each network

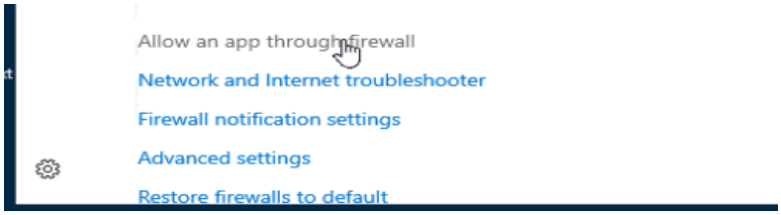
First I needed to make sure that the Windows Firewall was enabled for all three networks (Domain, Private, Public). To do this, I navigated my way to the Firewall and network protection page. I first clicked on the Windows button at the bottom left corner or the screen before selecting the 'Settings' option. After this, I selected 'Update and security' before choosing the 'Windows security' option. Following this, I selected the 'Firewall and network protection' option.



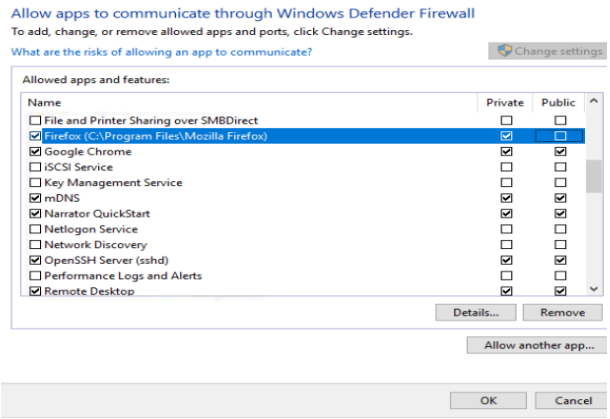
In this page I selected each of the three networks to make sure the Windows Defender Firewall was activated for each as shown in the screenshots above.

Configuring Windows Defender Firewall

I was instructed to change the firewall configuration to allow Mozilla Firefox to communicate on the public network.



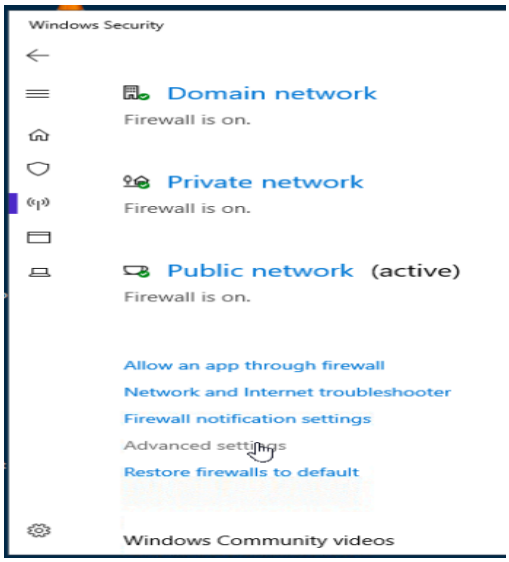
To do this I selected 'Allow an app through firewall' in the Firewall and network protection page as shown in the screenshot above.



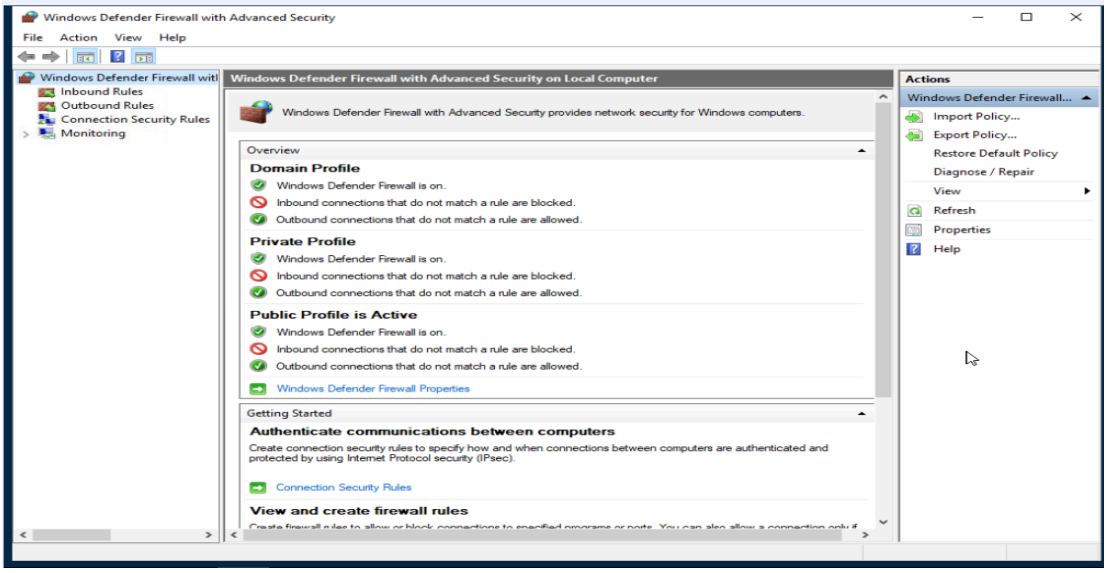
This opened up the page shown in the screenshot above. I then checked the public box in the Firefox row to enable connection to the public network. Following this, I pressed ‘Ok’ to apply the change.

Configuring Windows Defender Firewall with Advanced Security

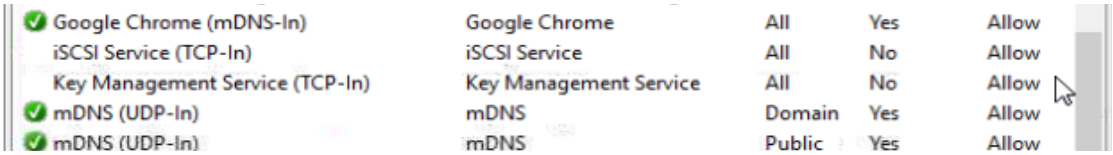
I then utilised the advanced security option as it provides more in-depth options for configuration.



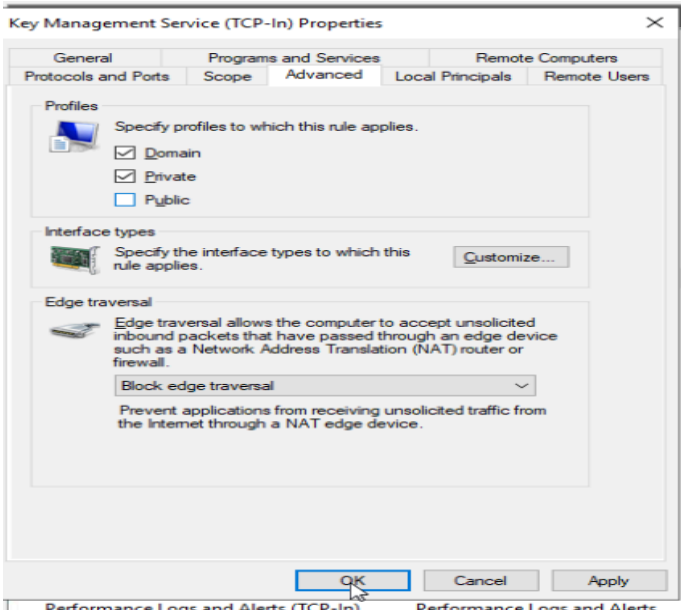
To do this, I selected ‘Advanced settings’ in the Firewall and network protection page as shown in the screenshot above.



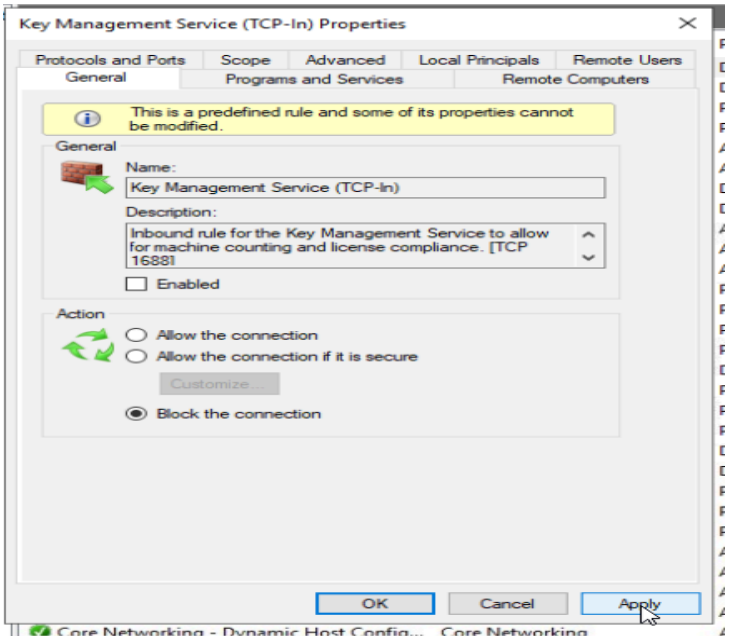
This opened up the page displayed above. I then clicked on ‘Inbound rules’.



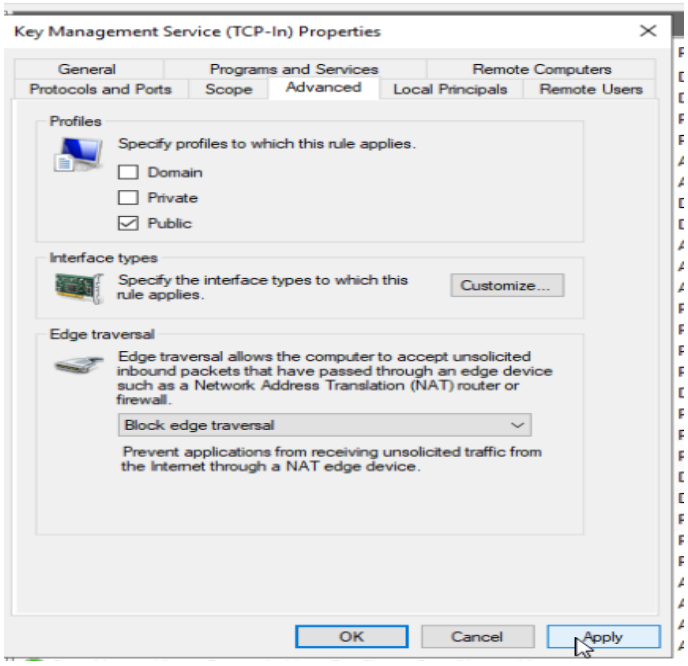
This opened up all the rules that were set up which determine communication settings for software to networks. I was instructed to scroll to find ‘Key Management Service’ and to double-click it as shown in the screenshot above.



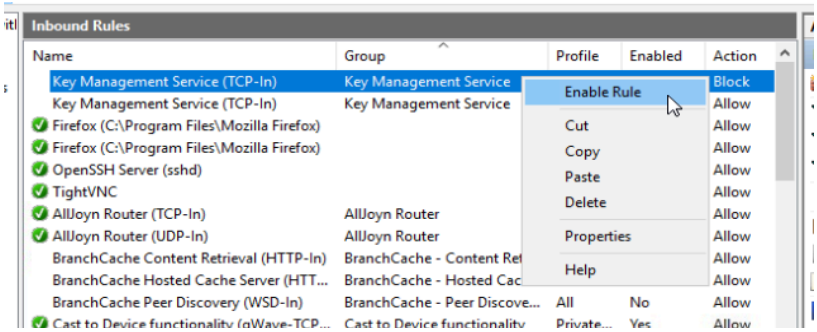
This then opened up a page detailing the Key Management Service properties. I navigated to the ‘Advanced’ section and unchecked the ‘Public’ box so that Key Management Service could communicate with the private and domain network only. I then clicked ‘Apply’ and ‘OK’.



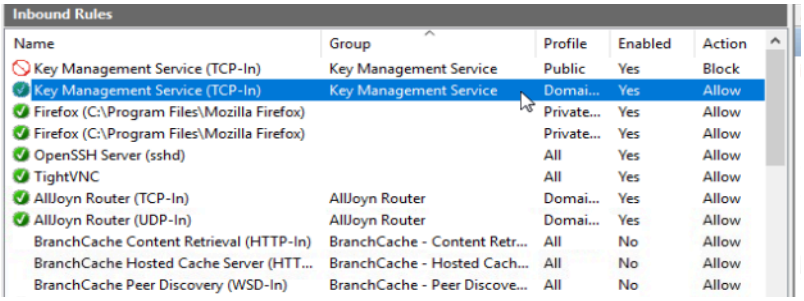
I then needed to block communication with the Public network for Key Management Service so that only communication to the private and domain networks were possible. To do this, I copied and pasted the same rule from earlier and then double-clicked the copy. Then, in the ‘General’ tab I chose ‘Block the connection’ as displayed in the screenshot above before pressing ‘Apply’.



Next, I navigated to the ‘Advanced’ section to uncheck ‘Domain’ and ‘Private’ and to check ‘Public’, so that only communication with the public network would be blocked. I then clicked ‘OK’.



After this I needed to enable both rules. To do this I right-clicked each rule before selecting ‘Enable rule’ as shown in the screenshot above.



The screenshot above shows how the two rules for ‘Key Management Service’ looked after configuring and enabling them.

Summary

After completing this project I now know how to enable and configure the Microsoft Windows Defender Firewall so that it allows certain connections and blocks others. I also know how to use the advanced settings to further expand on firewall rules to customise restrictions and permissions in depth.