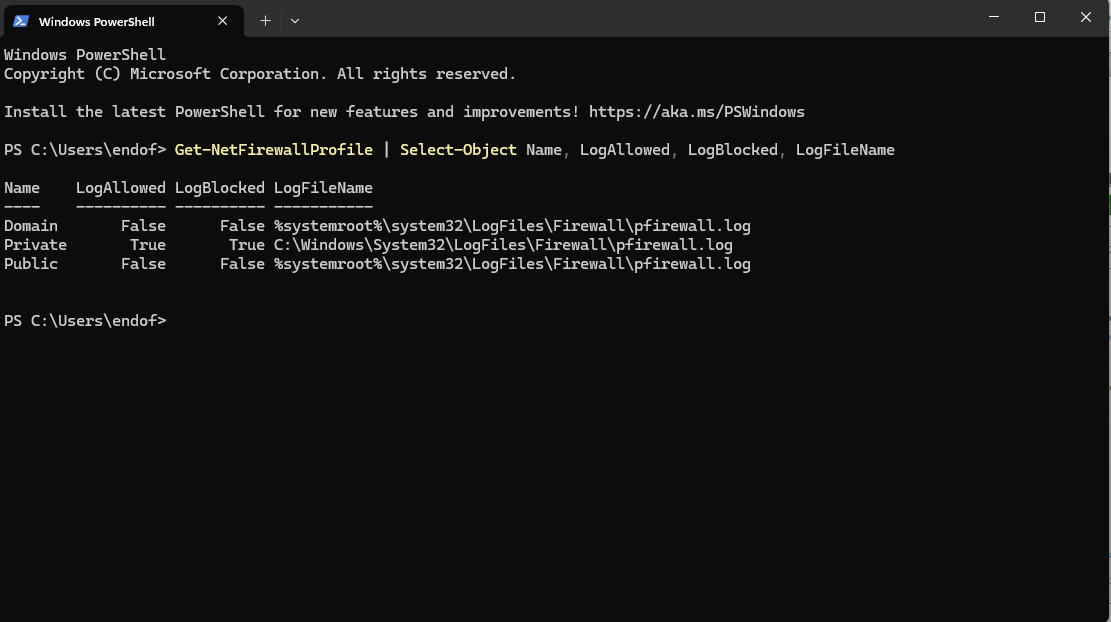
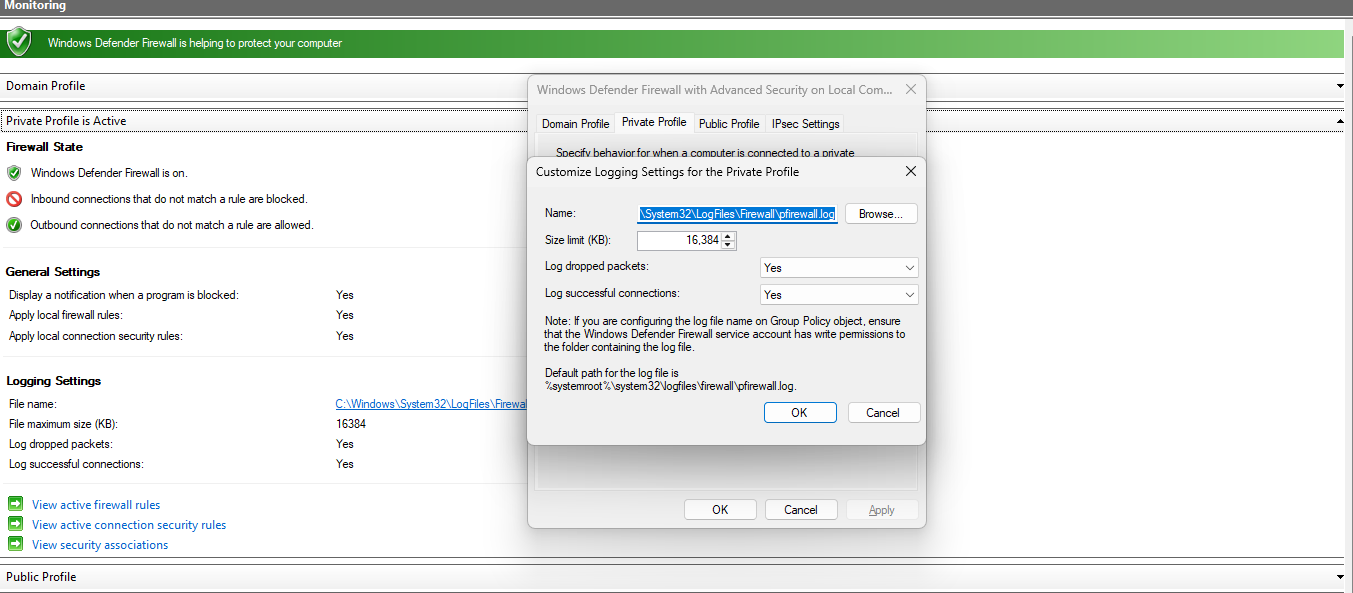
**Firewall Modifications**

At an earlier point in the document, a vulnerability scanner was run through Nexus essentials. Of the total identified scans, about 183 scans are port scans of the 183 only 17 port scanner were worth paying attention to. Of the seventeen only five did not necessitate any changes to them. These two ports, 500 and 4500, are in the usage of VPN services. There is a strong chance that a VPN be utilized in the future. One of the ports suggested was the same as Nexus essentials used, 8834, so I decided to not block that port either. The other two ports not blocked were 5040 and 8090. The other ports were within the range of 49,000 or higher. Those ports are utilized by programs like discord and Microsoft team to communicate out and in. Hence, they were not blocked in the firewall. Once the firewall was finished being created, there had to be a creation of the logging for the firewall. Initially, the logging enabling was done through windows registry changing two files to reflect the number 1 instead of being the default 0. There was double verification through PowerShell and it shows that the logging was enabled, but upon verification. It was not doing any firewall logs and the firewall GUI did not reflect until it was changed in the GUI. The firewall is created on the host machine as any firewall rules on the host machine is going to be applied to the virtual machine.





**Virtualization and Harden Browser**

The point of utilizing virtualization is to create an additional buffer of security. The virtual machine is created utilizing Ubuntu which is a Linux based operating system. For system requirements for the virtual machine, it is at present utilizing approximately 16GB of RAM as the host machine have more to spare and 4 cores with a total space of 25GBs of storage space. Since Firefox was already installed the virtual machine upon successful install, modifications were applied to the work profile. The default page always open up to about:profiles page within Firefox. This allows for a quick transition to a soft browser to a harden browser based on current requirements. The differences between the harden browser and the soft browser is that the soft browser does not have any modifications besides what page it starts in. The harden browser has various extensions and settings enabled to reduce and prevent tracking. The various extensions are NoScript, uBlockOrigin, Privacy Badger, and CanvasBlocker. The settings are custom protection based but focuses on removing third party tracking cookies and prevent any local storage of passwords within the browser to encourage the usage of a password manager such as Keypass which has compatibility with both Linux and Windows.

