**UNIT 7 TASK 4 – IMPLEMENT STATEGIES TO PROTECT AN IT SYSTEM FROM SECUIRTY THREATS**

**Mohammed Mahin Ibnay Mamun (346584)**

**TESTING PLAN FOR THE ORGANISATION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test no | Threat to test | action | Expected outcome | Actual outcome |
| 1 | Virus / malware | Runs against the virus scan. | No viruses detected on any system on the network. |  |
| 2 | Os vulnerability | Inspects to make sure systems are up to date. | Every system on the network is running on the latest update |  |
| 3 | Software vulnerability | Examines all software inclusive of security software is reconditioned | Each and every software is up to date online. |  |
| 4 | Ransomware/ rootkit | Processes antivirus and alternative checks. | None to be noticed on the network. |  |
| 5 | File access | Views all files which can be obtained effortlessly by anybody in the network which are not privileged. | No files owned by users on the network that possess full ingress permissions carry sensitive data |  |
| 6 | External threats (wiretap / DoS) | scrutinize the security system and ports. EG – port 80 | Ports are shut and open. |  |
| 7 | Firewall threat | Looks over firewall. | Ports are closed and unbarred. |  |

**Justification of method**

**Why did you choose specific methods?**

They help not only to rid the system of existing malware or other threats, but also help to clean out the system of future malware and other threats, Furthermore, detecting and eliminating preexisting threats should be part of the approach as well. In addition to updating the OS, a virus scan can help detect pre-existing threats and remove them.

**How will they defend the system from threats?**

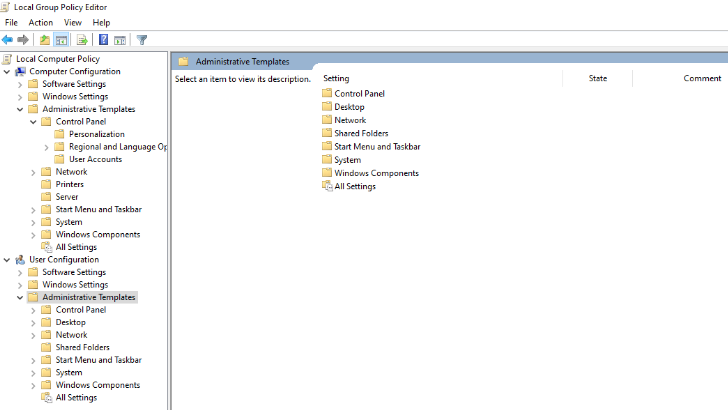
By strengthening the security of the organization's network, threats will have a harder time getting into and affecting the system. By weakening the threat of an attack, the organization will be able to protect its network.

**Are there any other ways the system could be defended from those threats?**

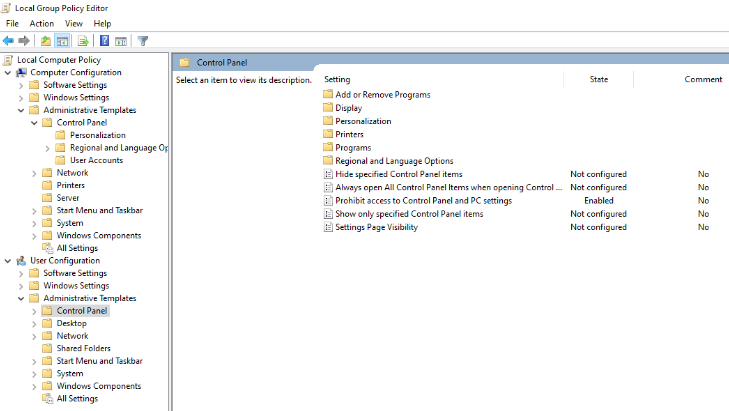
It is possible to implement policies to further protect the network against viruses and other threats. It is also possible to prevent hidden malware from entering the system by banning external devices from the network. Furthermore, certain files containing sensitive information can be protected with policies that limit the number of users that can access them.

**Example of protecting a system**

**The group policy editor:**



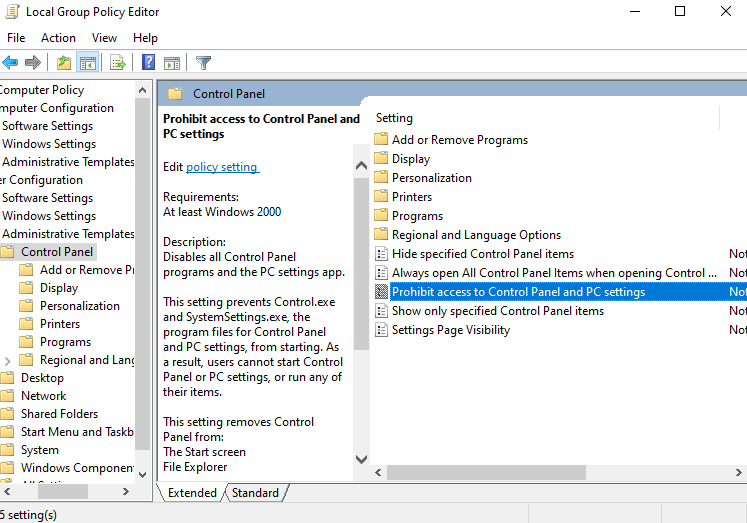
With Windows 10, there is a group policy editor that administrators can use. Device administrators can use this tool for managing group policies in Windows 10 as an administrator.



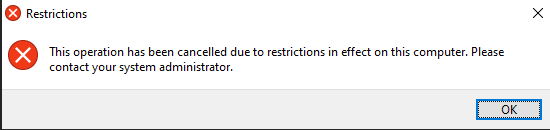
For example, restricting access to the control panel can be changed. In the left-hand panel of the editor, you will find a list of all the settings and options.

As shown in the picture below, an administrator changes the restrictions for the control panel by selecting the "control panel" folder, in which it is possible to disable what is visible and to disable the control panel.

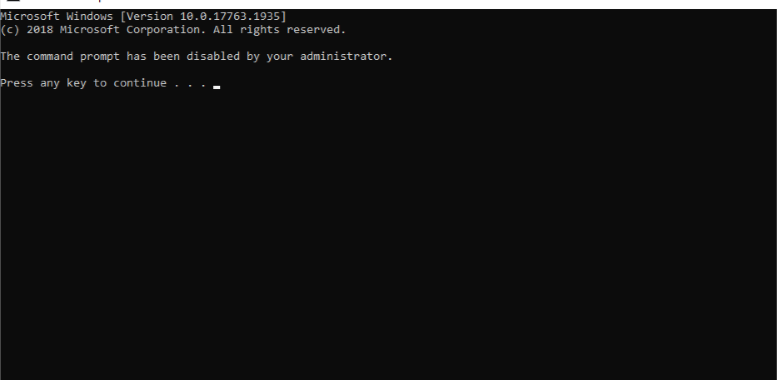
When an administrator clicks on the control panel and opens another panel, he or she has the choice of how to modify each setting. Anyone attempting to access the control panel above will not be able to as the image above prevents access to the control panel. Using these changes, here is a screen shot of a user trying to access the control panel.

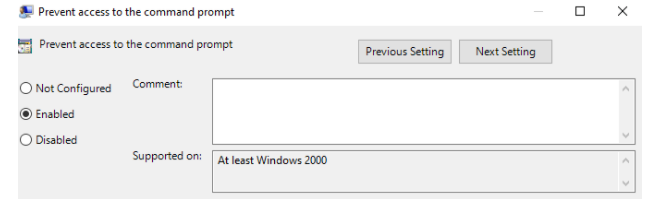


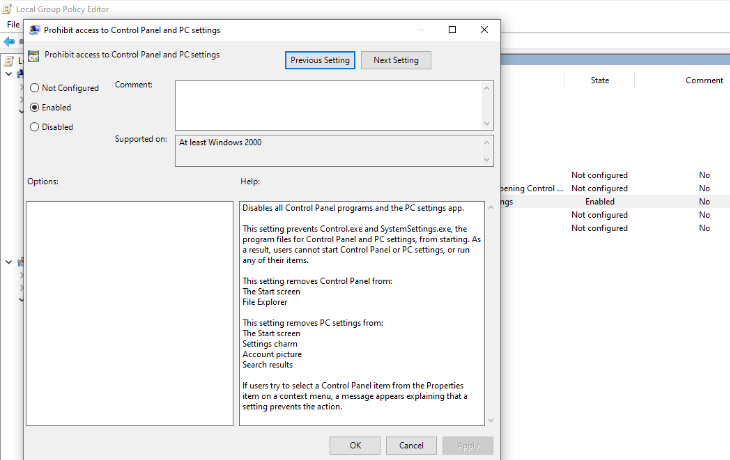
After that, a message like this one will appear. To accept the message, simply click on the okay button.



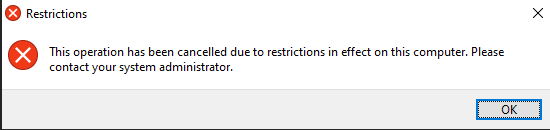
Hold down Windows + R while you click to run the command prompt. The command prompt is another example. Administrators can change the option by clicking on the same window from earlier.



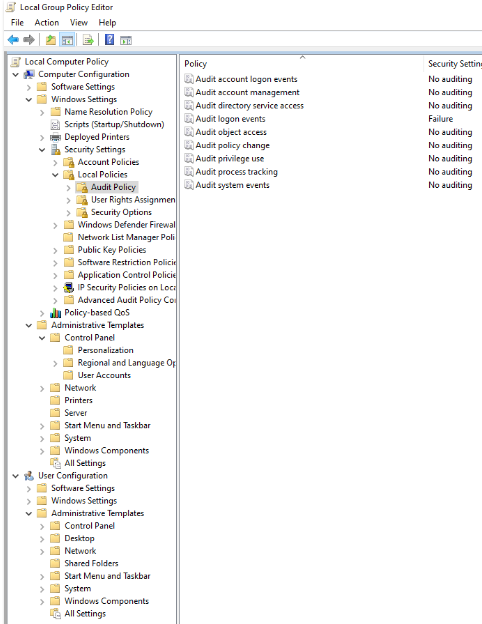
  
the user at this stage has access to add or disable any command prompts. They can also add comments in the provided space.



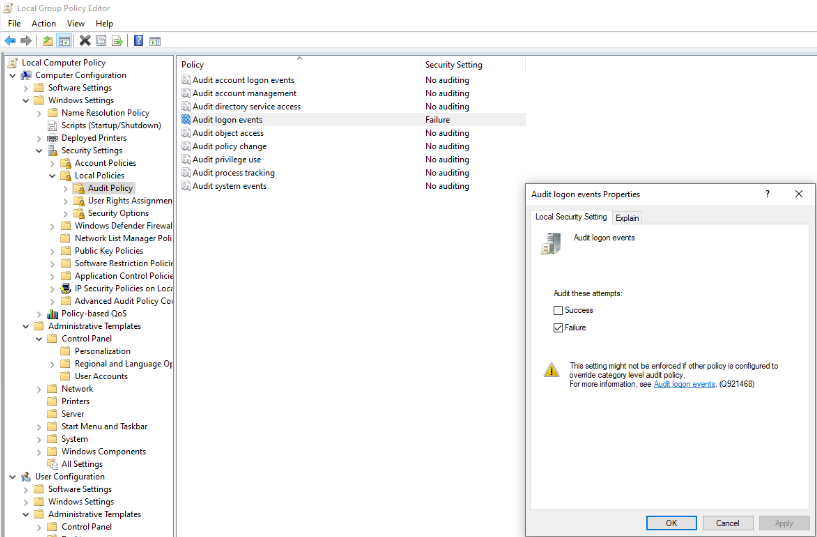
In order to make changes to each setting of the control panel, the administrator needs to open another panel by clicking on the control panel. This panel enables the administrator to select what access is allowed. Attempts to access the control panel in the image above will be denied because it is enabled to prevent access. Which gives this error message again

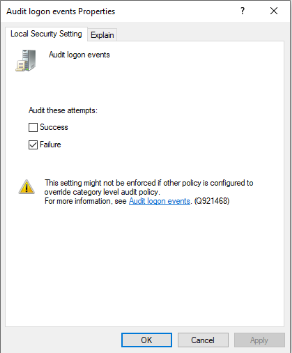


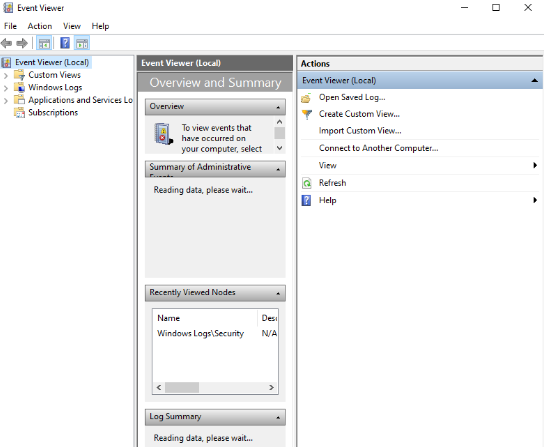
**Audit policy:**

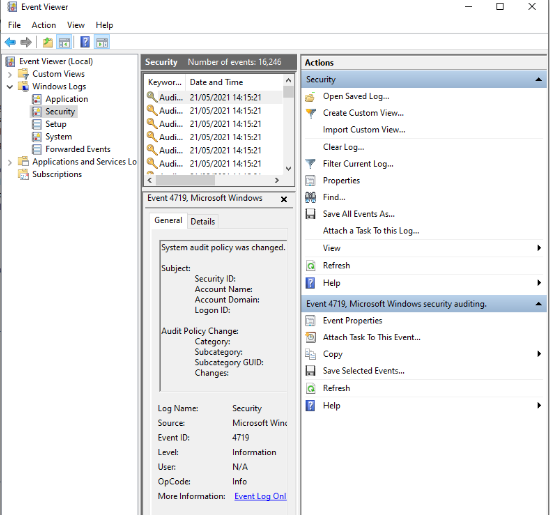


The audit policy editor permits for administrator to detect and even set up events which takes place on each user’s account/computer. Events can also be tracked through the editor.

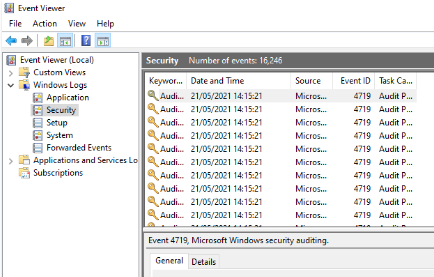


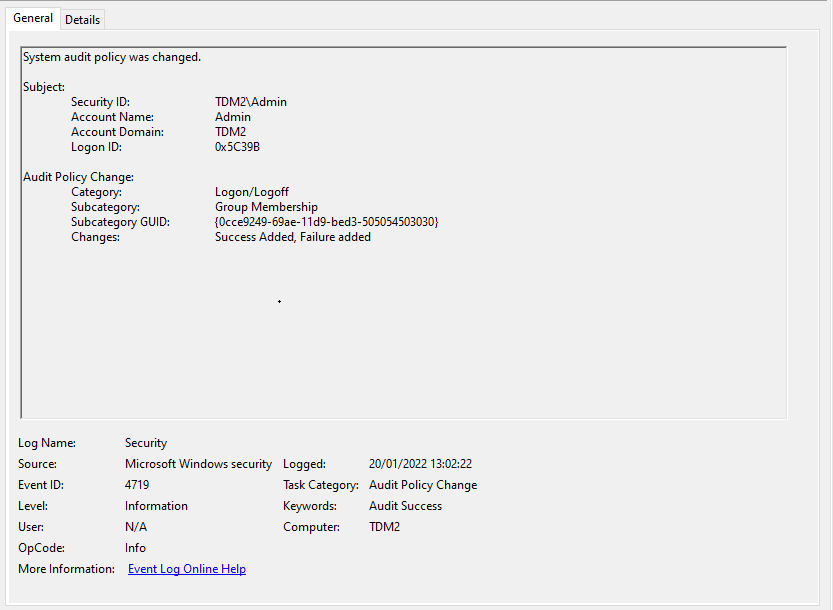






This is the event viewer which displays a list of all events that have occurred on a computer.

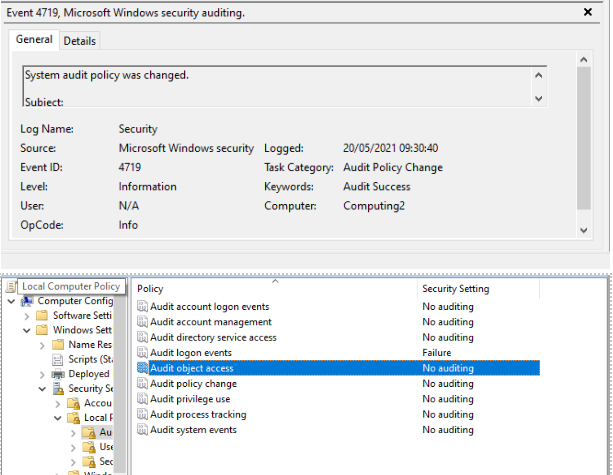




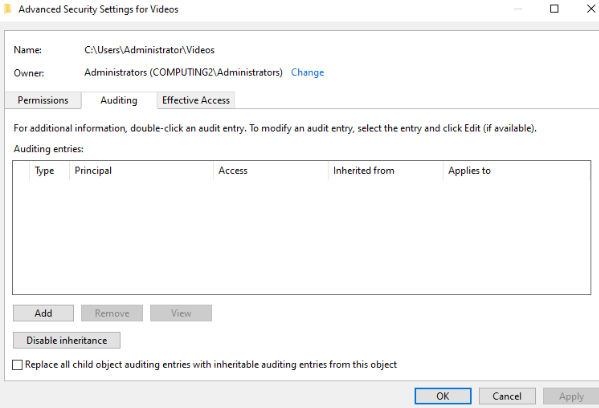
A list of all events occurring on the computer can be seen in this event viewer. If you click on an event, it shows more information about that event. For example, it shows when the event took place, which user was involved, and what happened.

**Object Audit Access**

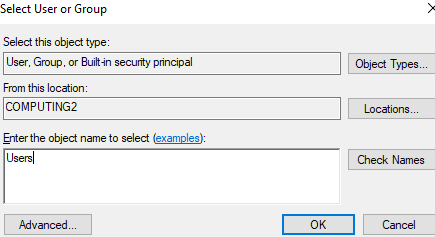
Administrative users can add audits to specific objects, such as files or folders. As a result, every time that file or folder is modified, read, opened, or deleted, an event is created in the event viewer. Using this feature can help ensure that people who should not have access to a particular file or folder do not have access to that file or folder

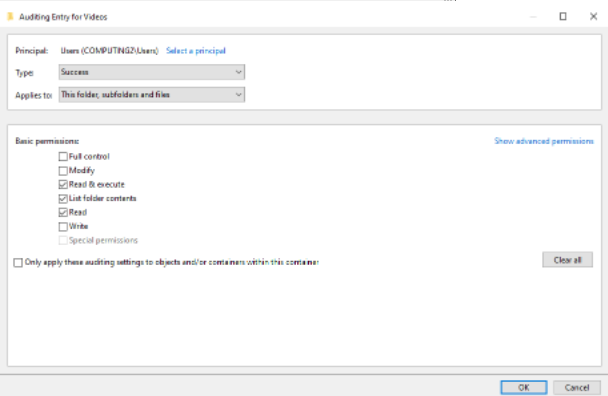


Administrators have access to set audits, to do this they must right click on a file/ folder -> security -> advanced -> auditing. When they are here the administrator can click the button to bring up another window of all the audits.

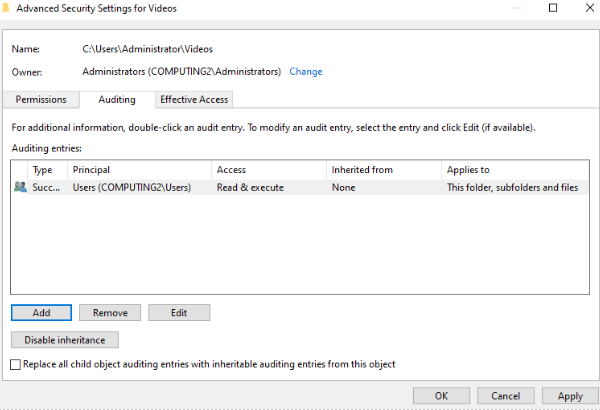


This example shows how to add a new audit to a folder.



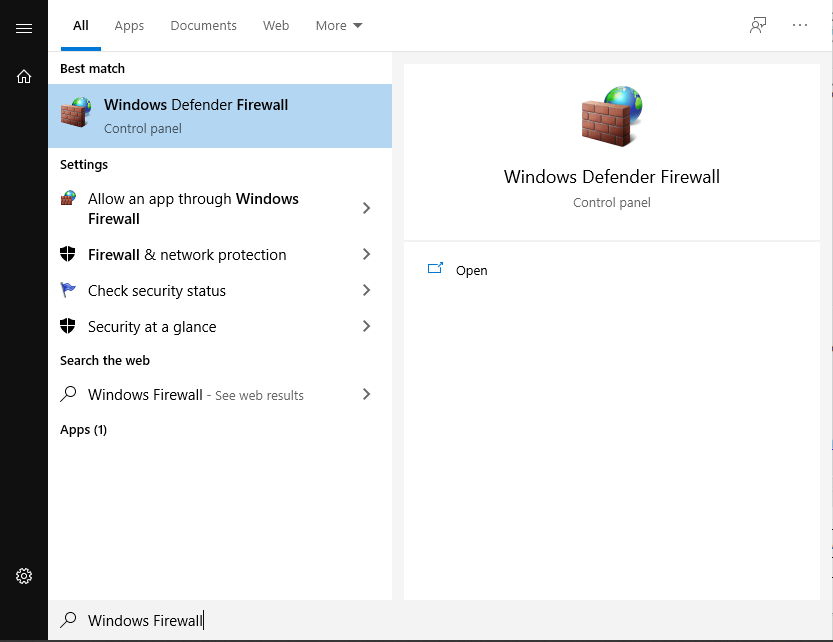


The following screen shows the results of a successful audit. Including writing, reading, and editing events will apply to all users.

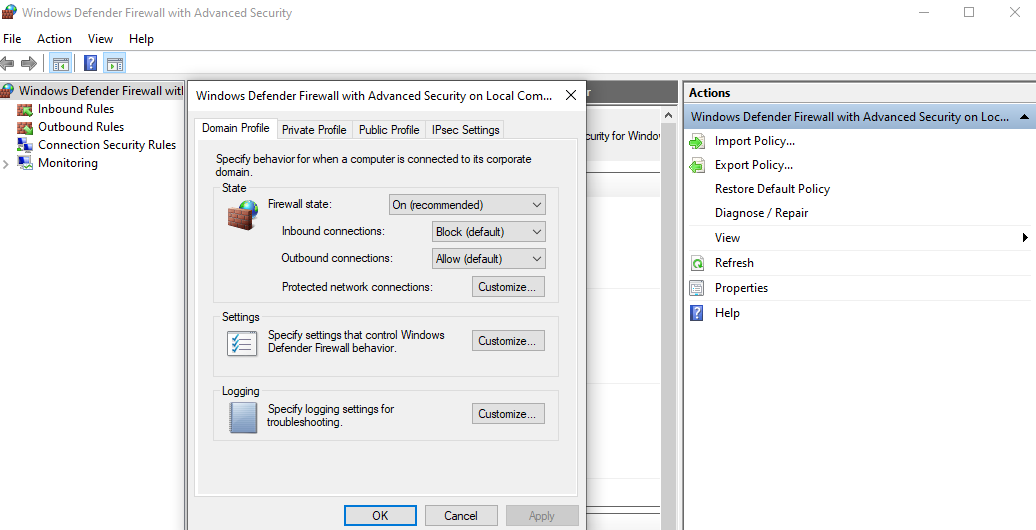


**Enabling and managing firewalls / Building and managing firewalls**

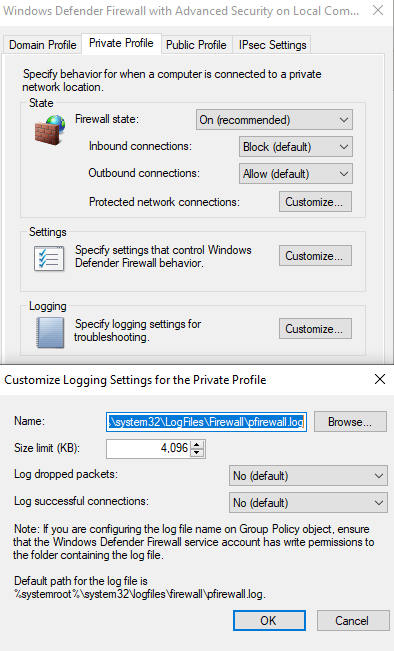
All windows 10 devices now come with this software, windows defender firewall. This tool can be used to enable and disable firewall set up by administration. This tool can be accessed by simply typing in firewall on the start menu (window key).



If you right click on the firewall option, you gain further access to the system and you can also adjust areas.



By making your packet size smaller, it will block off anu packets which are much higher than the required amount. There are also other settings which you can change here.



The firewall monitoring tab is used to view the firewall-on-firewall defender. The monitor will represent whether, since settings are currently active and things such as the firewall public, private and domain profiles.

