[How To] Protect your notebook from the ransomware WannaCry (WanaCrypt0r 2.0)

This document applies to all MSI notebooks and Vortex products.

There are many cyberattaks that have been spreading all around the world lately, including the malicious software known as ransomware.
Ransomware is a type of malware that not only might encrypt the users' personal data and important files, but also might encrypt the entire hard drive as well.
Recently, the ransomware called "WannaCry (WanaCrypt0r 2.0)" has been released through the internet and it has been heavily affecting many of the users
This article will explain how to prevent the cyberattacks of the WannaCry (WanaCrypt0r 2.0) ransomware.

Q: How to prevent my computer from getting infected by the ransomware WannaCry (WanaCrypt0r 2.0)?

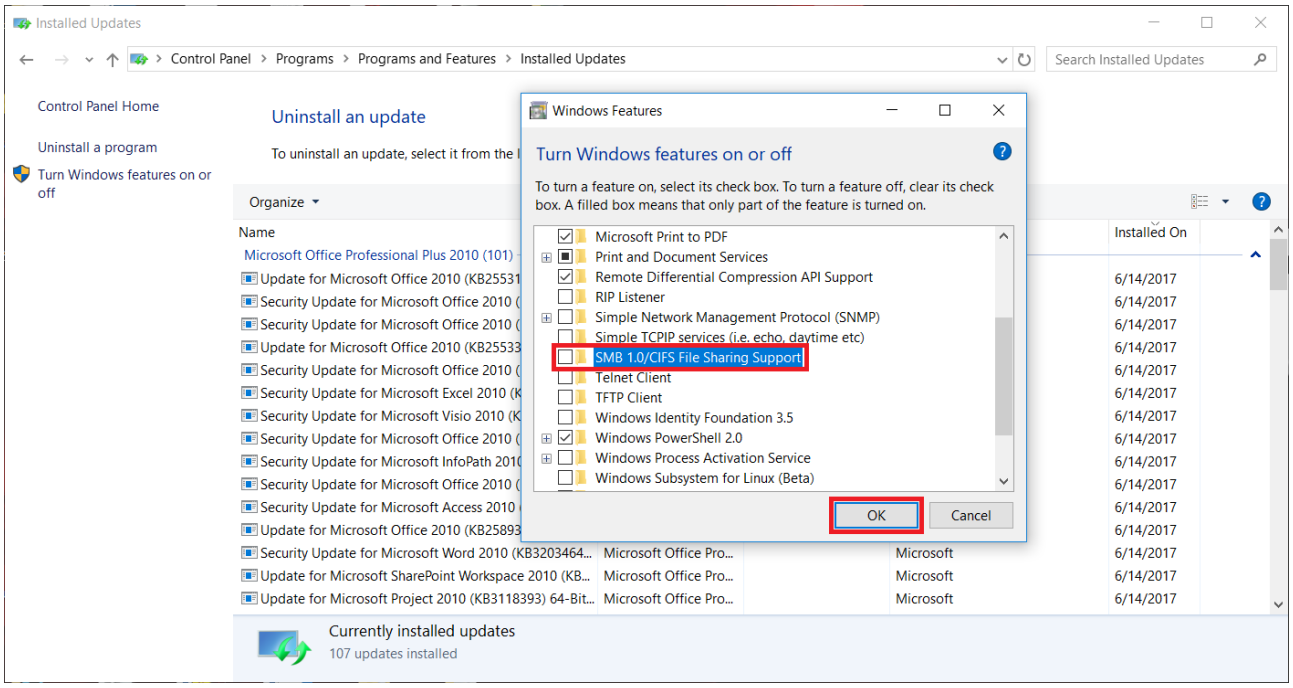
Because WannaCry (WanaCrypt0r 2.0) ransomware checks if the connection of the Port 445 is allowed and also checks if there are any leaks in the SMB v.1.0 (Service Message Block 1.0), therefore, we'd like to suggest to disconnect your notebook from the internet (by removing the LAN cable from your notebook and turning off the Wi-Fi connection), then proceed to disable SMB v.1.0 and block the connection of the Port 445 first, in order to prevent WannyCry ransomware to attack the system through those weak points.

ⓘ Since disabling the SMB. V.1.0 and blocking the connection of Port 445 may not allow the users to use the network's shared devices correctly, therefore, you may re-enable SMB v.1.0 and unblock the connection of Port 445, after the important security updates released by Microsoft are installed in the computer.

I. Disable SMB v.1.0 and Block the connection of Port 445

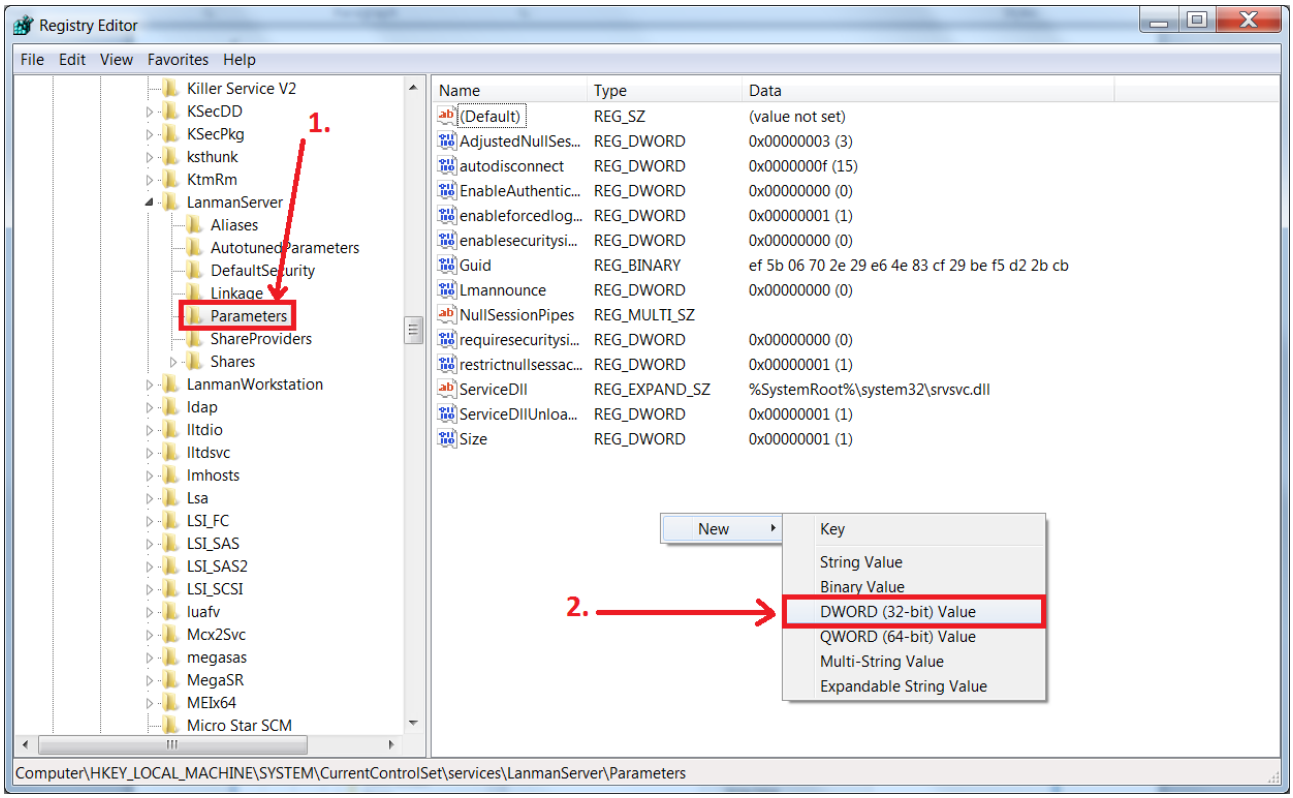
- Disable SMB v.1.0:

For Windows 8 users or above versions, please use these instructions:
Go to Control Panel ---> Programs ---> Programs and Features ---> View Installed Updates ---> Turn Windows features on or off ---> Uncheck SMB 1.0/CIFS File Sharing Support and click OK.



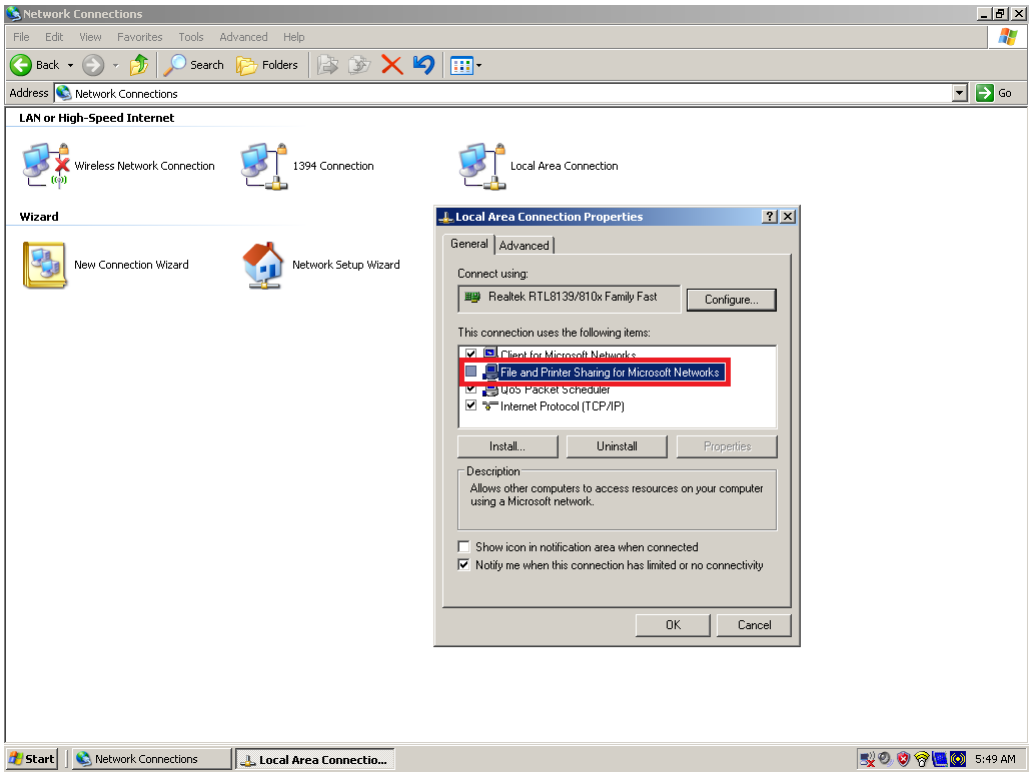
For Windows 7 users, please use this method:

Click on the Start button and type “regedit”, go to the folder of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters, on the right side of the windows, right click on any blank space, select New and add a DWORD (32-bit) value, then change the name to SMB1 and set the value data to 0. Then restart the computer in order for these settings to take effect.



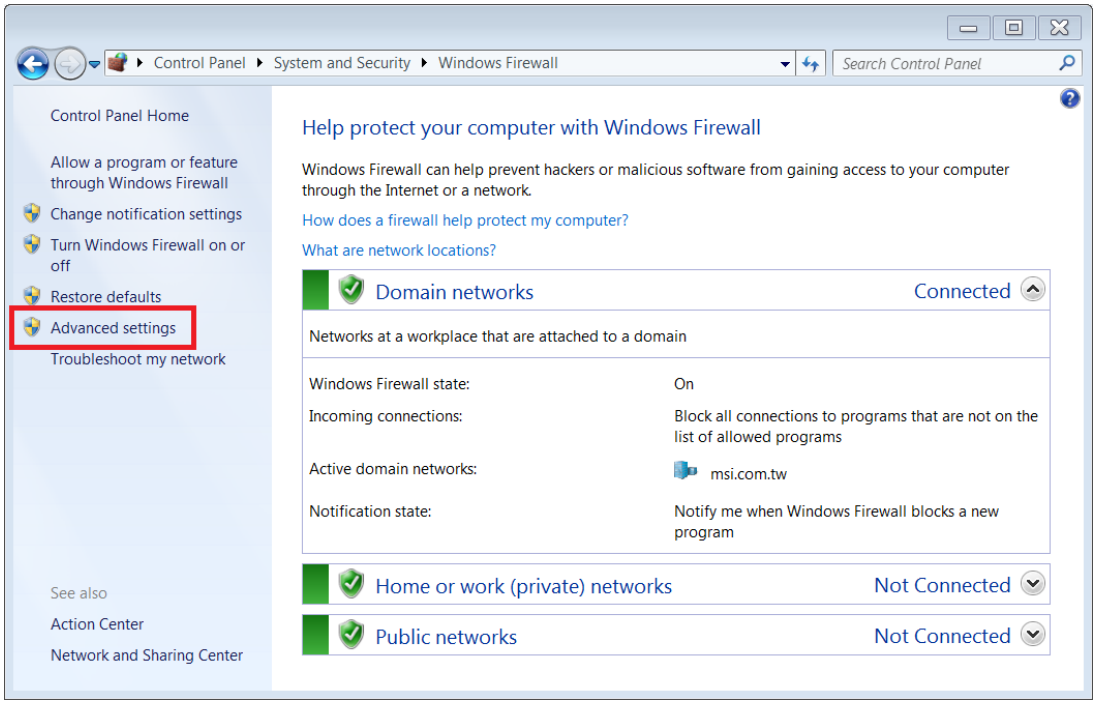
For Windows XP users, please use these instructions:

1. Go to Start ---> Control Panel ---> Network Connections
2. Right click on your Network Connection and select Properties.
3. Uncheck “File and Printer Sharing for Microsoft Networks”, click OK to apply the changes and restart your computer.

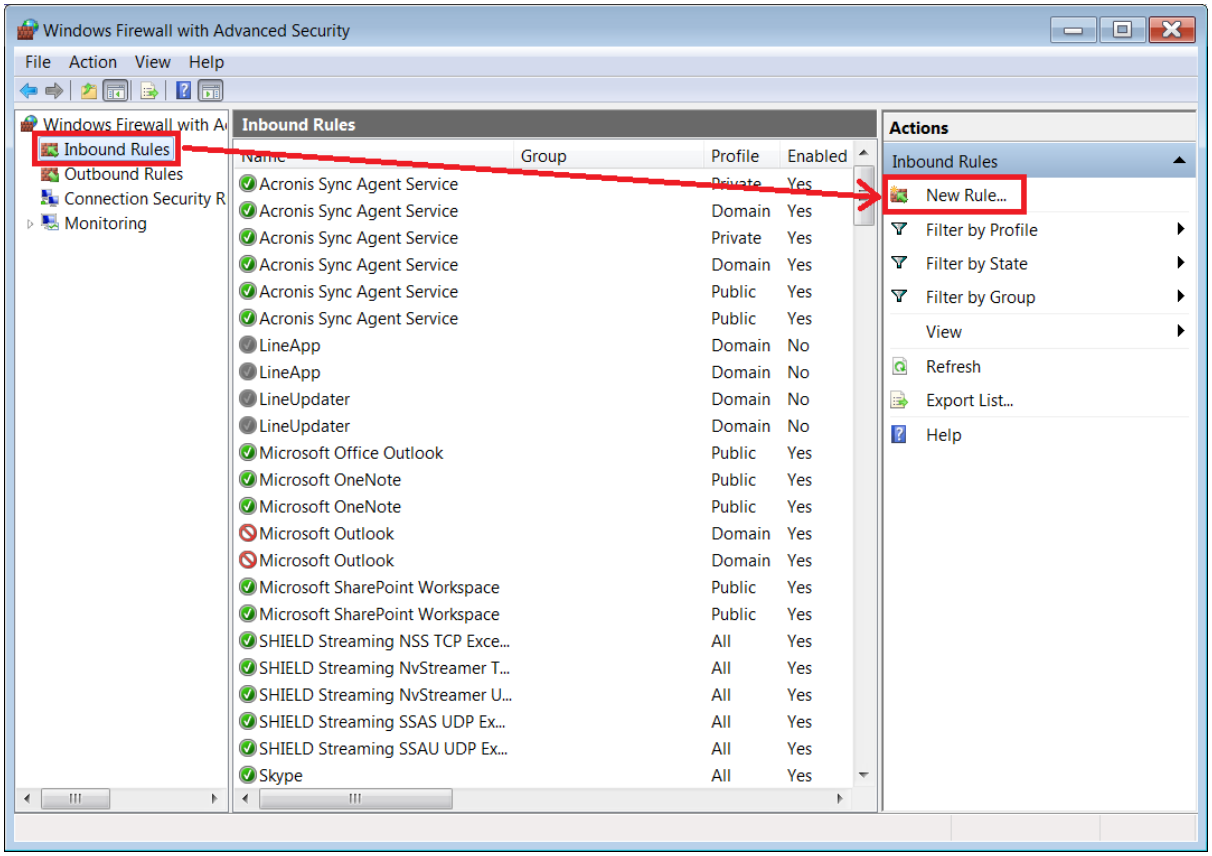


➢ Block the connection of Port 445:

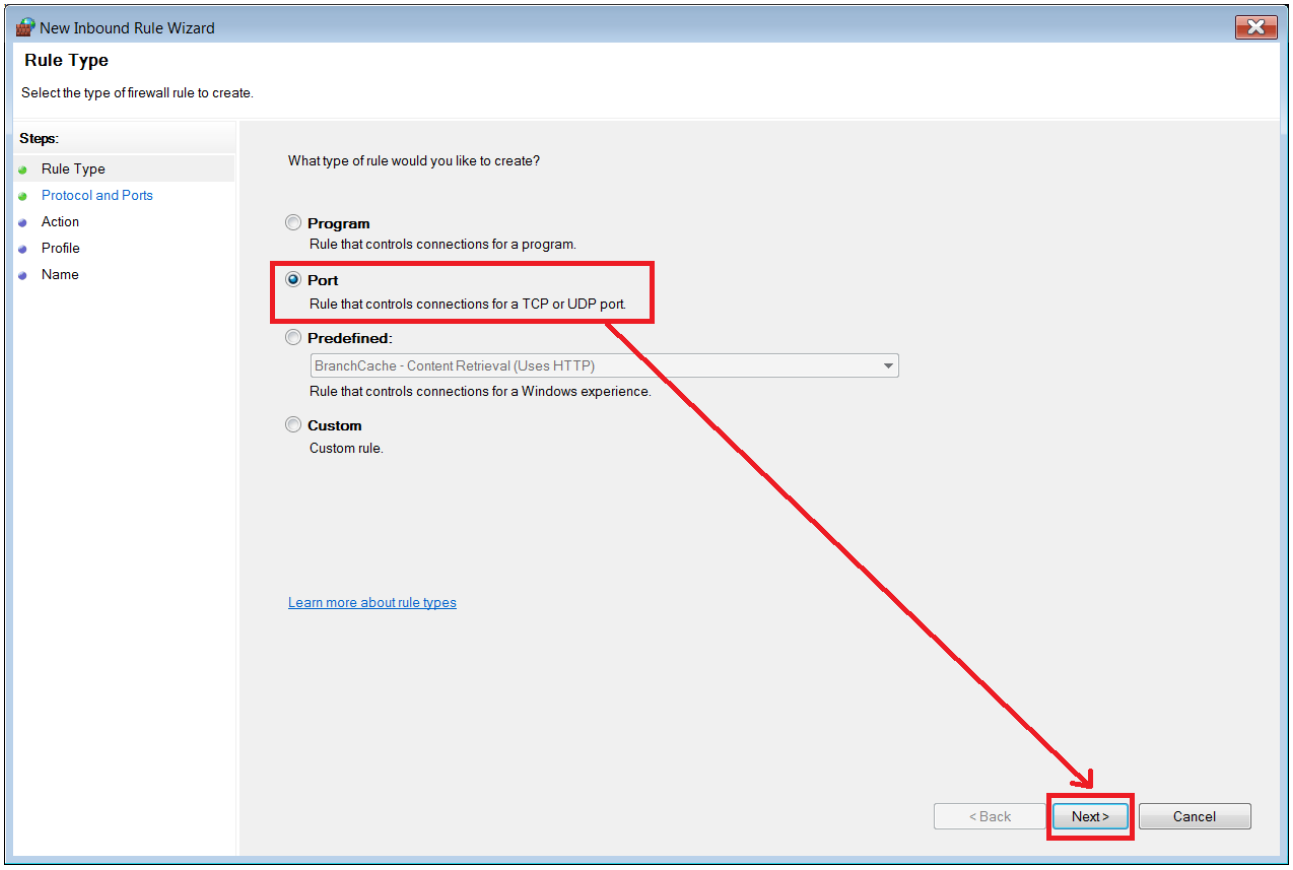
1. Go to Control Panel ---> System and Security ---> Windows Firewall ---> Advanced Settings



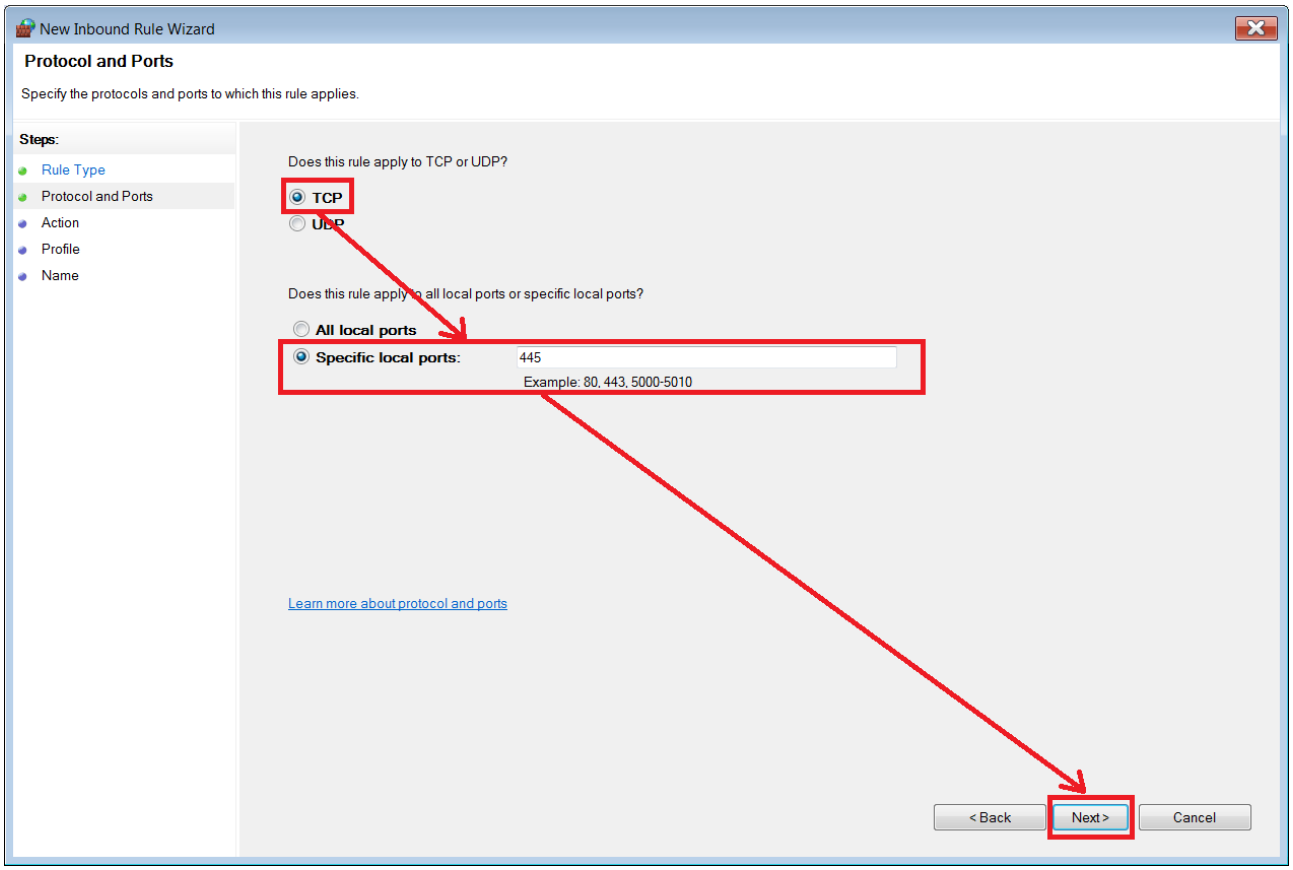
2. Click on Inbound Rules, and then select New Rule…



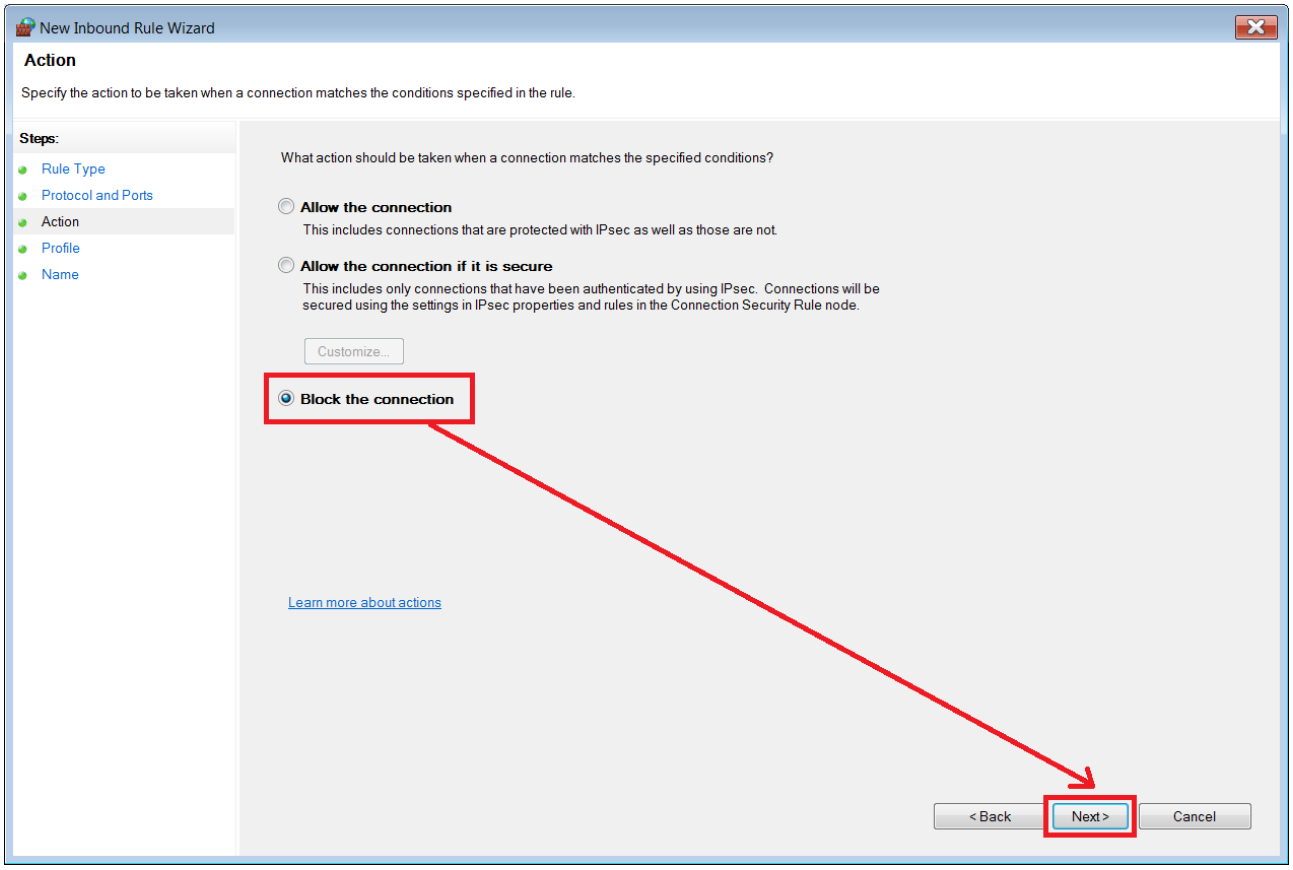
3. Choose Port, and click on Next



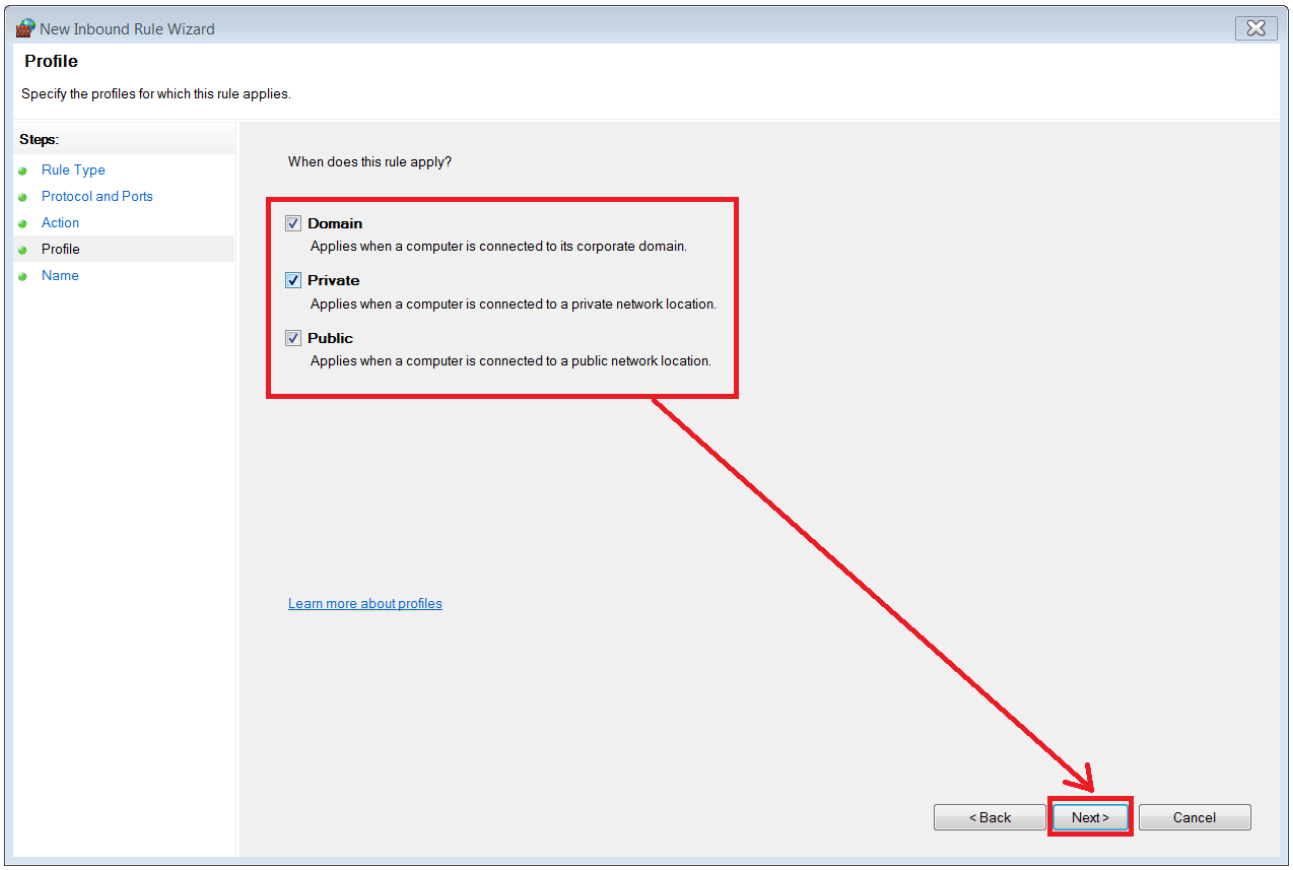
4. Click on TCP, and in Specific local ports, type 445, and then click Next



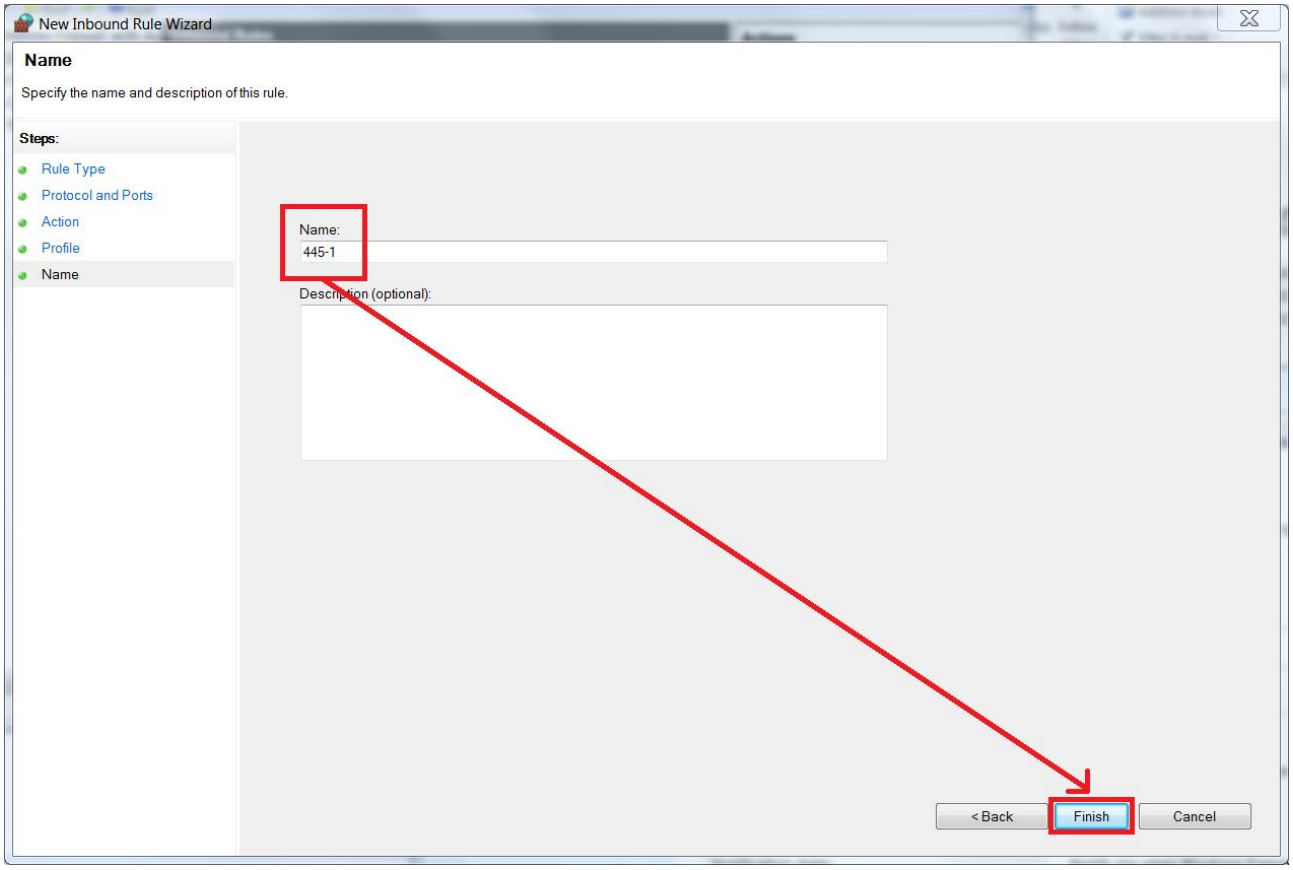
5. Choose Block the connection and click Next



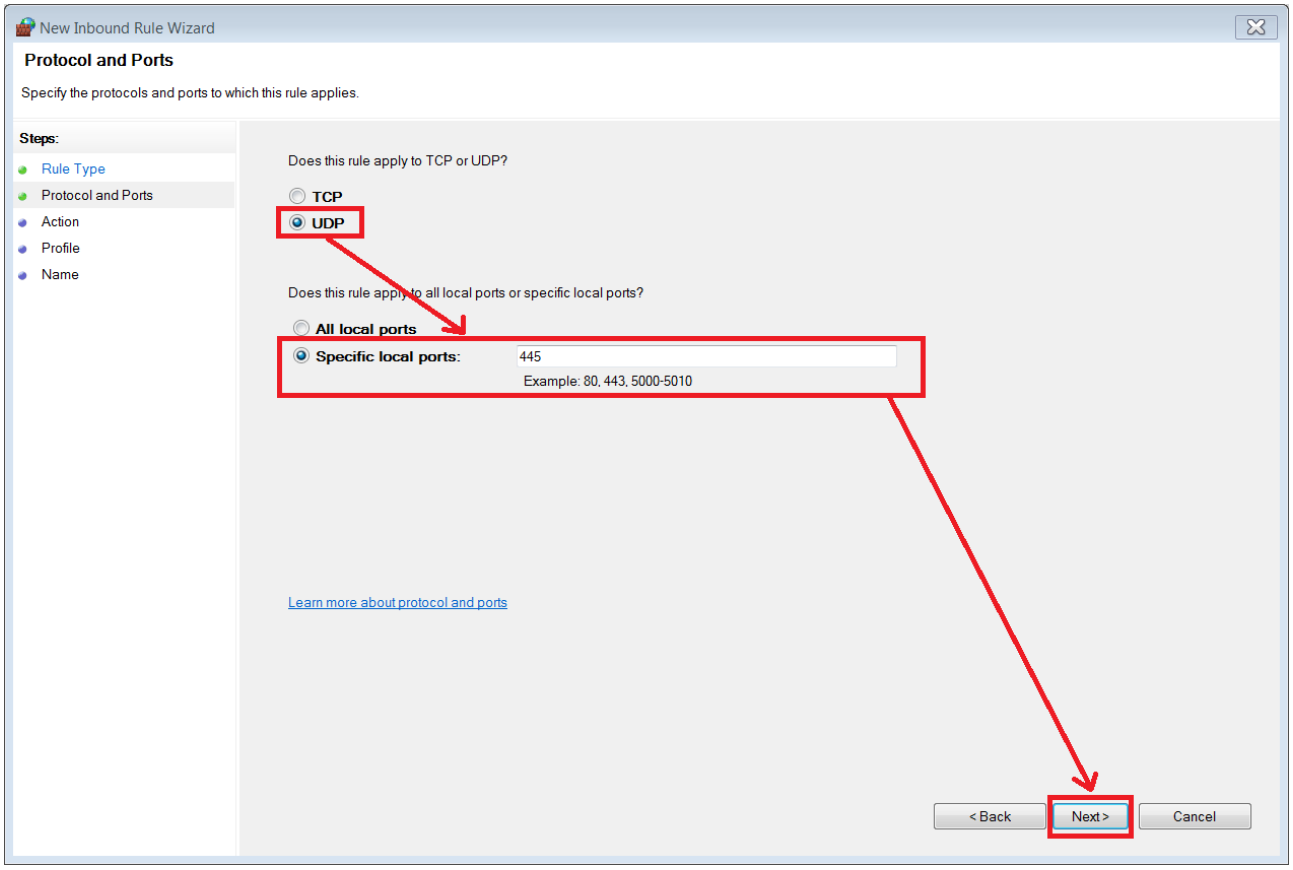
6. Select all the options, and click Next



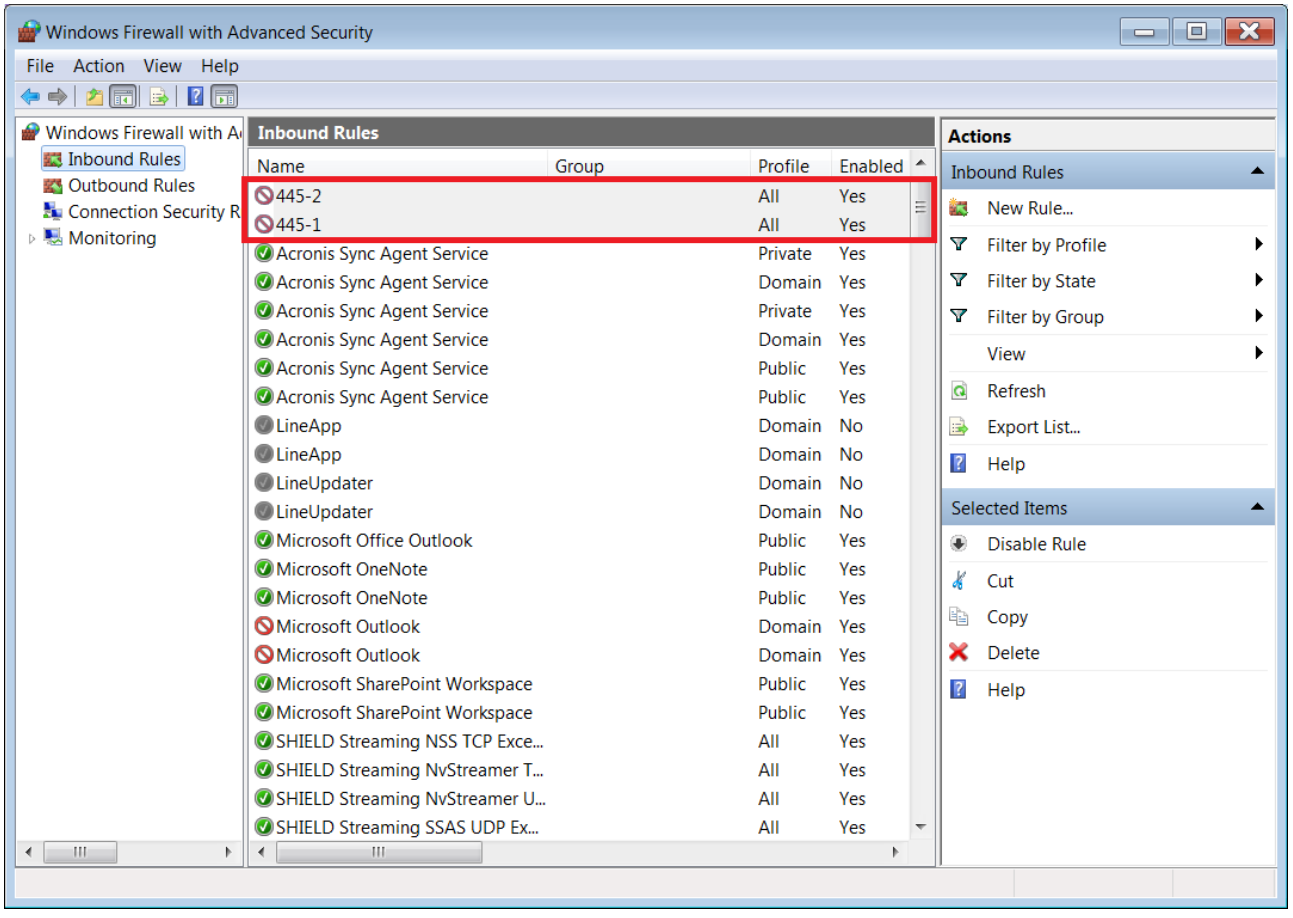
7. Assign a name to it and click on Finish



8. Now, create another rule with the same settings from above, but this time, select UDP instead.



9. That is the final step and the rules will appear like this:



II. Install the important security updates released by Microsoft

Microsoft has released important security updates that fixes the leak that allows the WannaCry (WanaCrypt0r 2.0) ransomware to attack the system. Please install this security update, according to the version of your operating system:

Operating System	Bit Version	Patch
Windows 10 Version 1511 ＊	32-bit	KB3210721 (32-bit)
Windows 10 Version 1511 ＊	64-bit	KB3210721 (64-bit)
Windows 8.1	32-bit	KB4012216 (32-bit)
Windows 8.1	64-bit	KB4012216 (64-bit)
Windows 8	32-bit	KB4012598 (32-bit)
Windows 8	64-bit	KB4012598 (64-bit)
Windows 7	32-bit	KB4012215 (32-bit)
Windows 7	64-bit	KB4012215 (64-bit)
Windows XP SP2 (English)	64-bit	KB4012598 (64-bit) - English
Windows XP SP2 (Japanese)	64-bit	KB4012598 (64-bit) - Japanese
Windows XP SP3 ＊＊	32-bit	KB4012598 (32-bit) - English KB4012598 (32-bit) - French KB4012598 (32-bit) - Russian KB4012598 (32-bit) - Finnish KB4012598 (32-bit) - Portuguese (Portugal) KB4012598 (32-bit) - (Chinese Traditional) KB4012598 (32-bit) - Hungarian KB4012598 (32-bit) - Turkish KB4012598 (32-bit) - Greek

		KB4012598 (32-bit) - Swedish KB4012598 (32-bit) - Spanish KB4012598 (32-bit) - Italian KB4012598 (32-bit) - Hebrew KB4012598 (32-bit) - Arabic KB4012598 (32-bit) - German KB4012598 (32-bit) - Japanese KB4012598 (32-bit) - Portuguese (Brazil) KB4012598 (32-bit) - Korean KB4012598 (32-bit) - Danish KB4012598 (32-bit) - Norwegian KB4012598 (32-bit) - Chinese (Simplified) KB4012598 (32-bit) - Polish KB4012598 (32-bit) - Czech KB4012598 (32-bit) - Dutch

＊For Windows 10 users, it is recommended to install Windows 10 version 1511 or later, in order to stay protected. To install the latest Windows 10 Build, please refer to the three methods that are explained in this FAQ.

＊＊Please install the security update according to the language of your operating system.

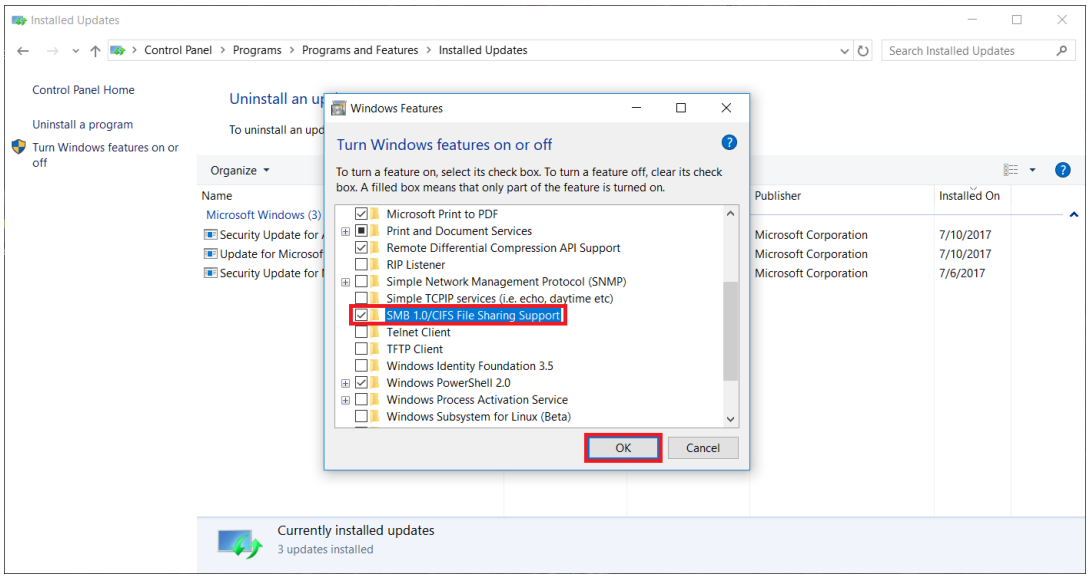
III. Re-enable SMB v.1.0 and unblock the connection of Port 445

➢ Re-enable SMB v.1.0:

After installing the important security updates released by Microsoft, please re-enable SMB v.1.0 with these instructions:

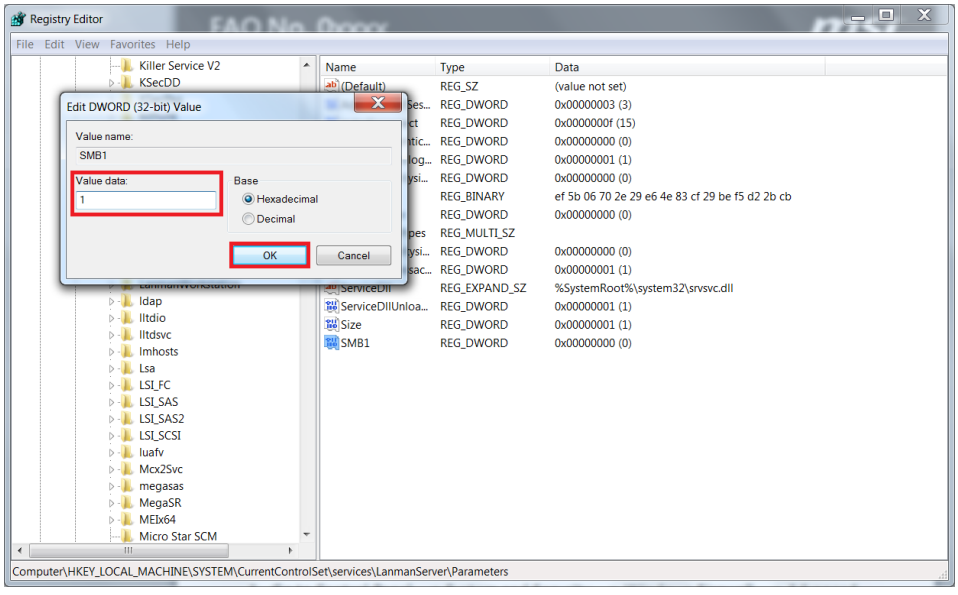
For Windows 8 users or above versions, please use these instructions:

Go to Control Panel ---> Programs ---> Programs and Features ---> View Installed Updates ---> Turn Windows features on or off ---> Check SMB 1.0/CIFS File Sharing Support and click OK.



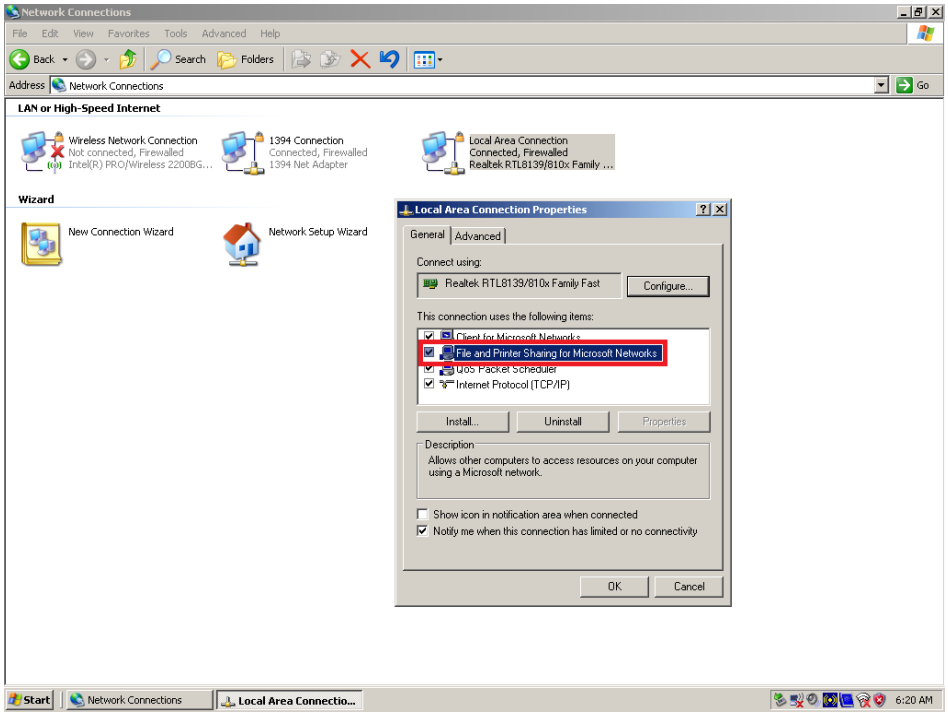
For Windows 7 users, please use this method:

Click on the Start button and type “regedit”, go to the folder of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters, on the right side of the windows, right click on SMB1 and select “Modify…”, then set the value data to 1 and click OK. Then restart the computer in order for these settings to take effect.



For Windows XP users, please use these instructions:

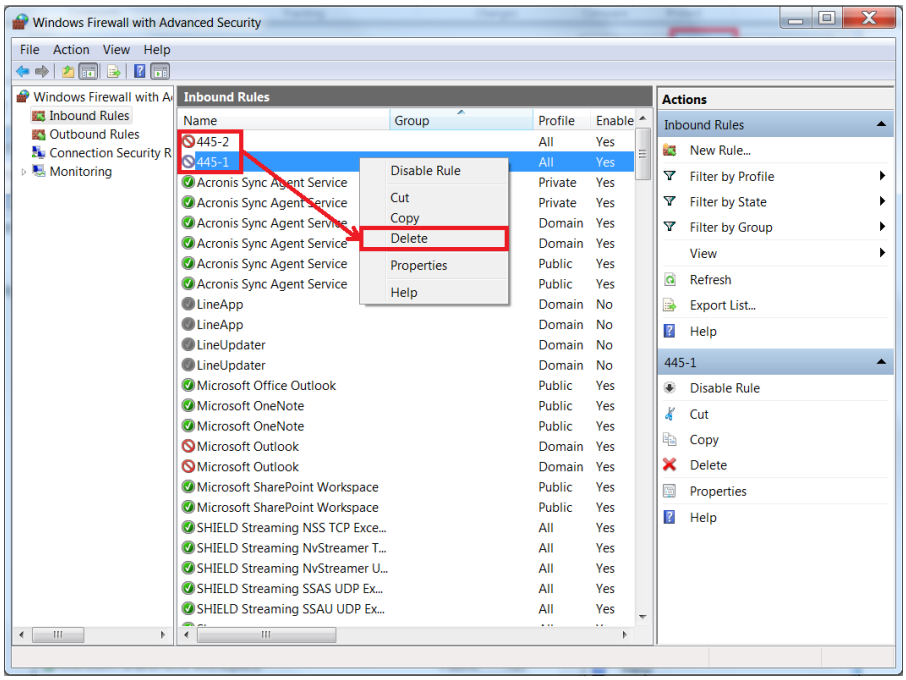
1. Go to Start ---> Control Panel ---> Network Connections
2. Right click on your Network Connection and select Properties.
3. Check “File and Printer Sharing for Microsoft Networks”, click OK to apply the changes and restart your computer.



➢ Unblock the connection of Port 445

To unblock the connection of Port 445, please follow these instructions:

Go to Control Panel ---> System and Security ---> Windows Firewall ---> Advanced Settings ---> Click on Inbound Rules ---> Right click on both rules that you've previously created (TCP and UDP) and select "Delete".



IV. Additional recommendations to increase the protection of the notebook

Besides installing the patches of Windows Update to prevent the attacks of the WannnaCry (WanaCrypt0r 2.0) ransomware, when using the computer normally, we'd also like to recommend the following steps in order to increase the protection of the computer and prevent unknown malwares to attack the system:

1. Please install an antivirus software, check and install all the latest updates of the antivirus software, in order to prevent these cyber-attack

2. For home computers, it is not advised to leave the computer connected to the Internet at all times (in order to decrease incoming attacks from malicious sources).

3. Make backups of important files periodically (for example, to DVDs, USB Flash Drives, external hard disks, etc.), and also, disconnect the computer from the Internet and turn off the computer when not in use.

4. Check and install the latest updates and patches of your operating system. Please make sure that your operating system has automatic updates enabled, or has reminders for important updates turned on.

In order to check if automatic updates has been enabled in your operating system, please visit Microsoft's official website and click on "How do I keep my PC up to date?", you will be able to see how to turn on automatic updates according to the version of our your operating system (Windows 10, Windows 8.1 or Windows 7).

5. Do not click on websites or download files from unknown sources. If your browser suddenly tells you to download some files or tells you unexpectedly that an update is needed, please reject these downloads and updates immediately, if you are not sure whether if the coming sources are safe or not.