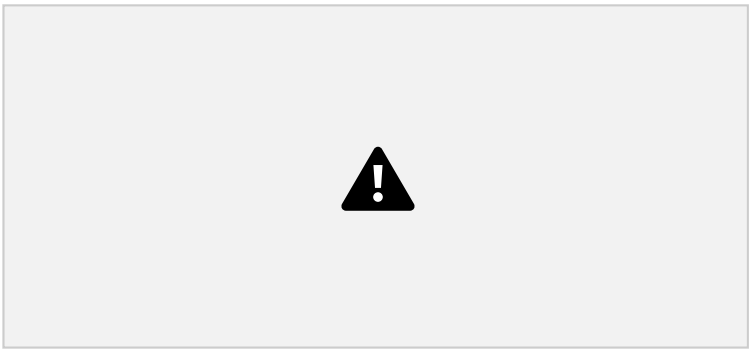
Setting Up Firewall with Advanced Setting

Technical Terms

- Malware - any software intentionally designed to cause damage to a computer, server, client, or computer network.
- Inbound Rule - filter traffic passing from the network to the local computer based on the filtering conditions specified in the rule.
- Outbound Rule - filter traffic passing from the local computer to the network based on the filtering conditions specified in the rule.

The Windows Firewall with Advanced Security is a tool which gives you detailed control over the rules that are applied by the Windows Firewall. You can view all the rules that are used by the Windows Firewall, change their properties, create new rules or disable existing ones.

A firewall is hardware or software that can help protect your PC from unauthorized users or malicious software (malware). Running a firewall on each PC on your network can help control the spread of malicious software on your network, and help protect your PCs when you're accessing the Internet.



https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/

Port Protection

Every communication using TCP/IP is associated with a port number. HTTPS, for instance, by default uses port 443. A firewall is a way of protecting a computer from intrusion through the ports.

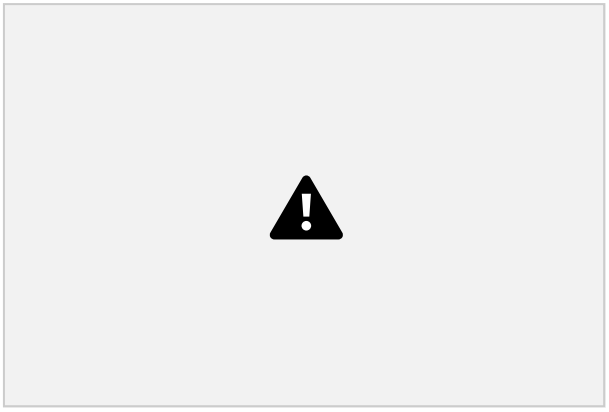
With port protection, the user can control the type of data sent to a computer by selecting which ports will be open and which will be secured. Data being transported on a network is

called traffic.

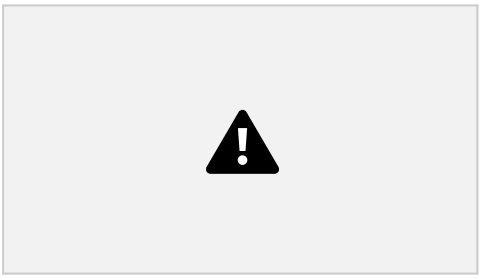
Setting Up Firewall with Advanced Security

You have several alternatives to opening the Windows Firewall with Advanced Security:

1. One is to open the standard Windows Firewall window, by going to "Control Panel - > System and Security -> Windows Firewall". Then, click or tap Advanced settings.



2. In Windows 7, another method is to search for the word firewall in the Start Menu search box and click the "Windows Firewall with Advanced Security" result.



3. In Windows 8.1, Windows Firewall with Advanced Security is not returned in search results and you need to use the first method shared above for opening it. 4. In Windows 10, you can use either of the 2 methods.

5. What Are The Inbound & Outbound Rules?

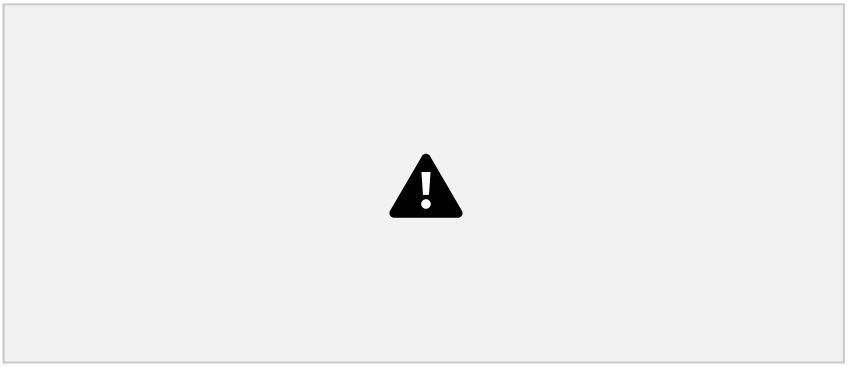
   a. In order to provide the security you need, the Windows Firewall has a standard set of inbound and outbound rules, which are enabled depending on the location of the network you are connected to.

   b. Inbound rules are applied to the traffic that is coming from the network and the Internet to your computer or device. Outbound rules apply to the traffic from your computer to the network or the Internet.

   c. These rules can be configured so that they are specific to: computers, users, programs, services, ports or

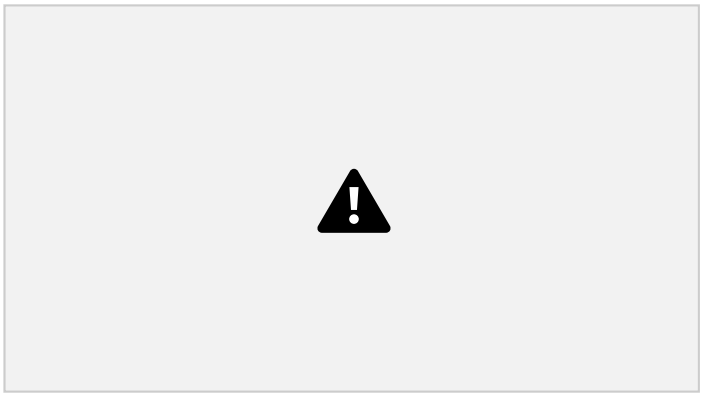
protocols. You can also specify to which type of network adapter (e.g. wireless, cable, virtual private network) or user profile it is applied to.

d. In the Windows Firewall with Advanced Security, you can access all rules and edit their properties. All you have to do is click or tap the appropriate section in the left-side panel.

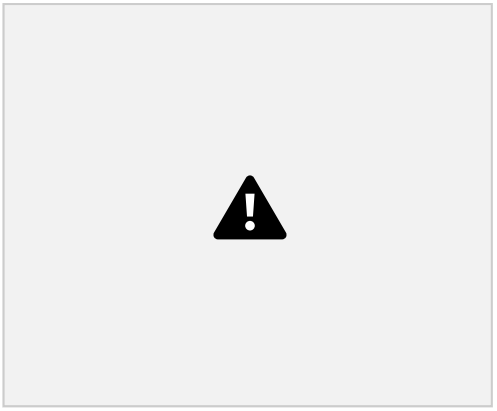


6. The rules used by the Windows Firewall can be enabled or disabled. The ones which are enabled or active are marked with a green check-box in the Name column. The ones that are disabled are marked with a gray check-box.

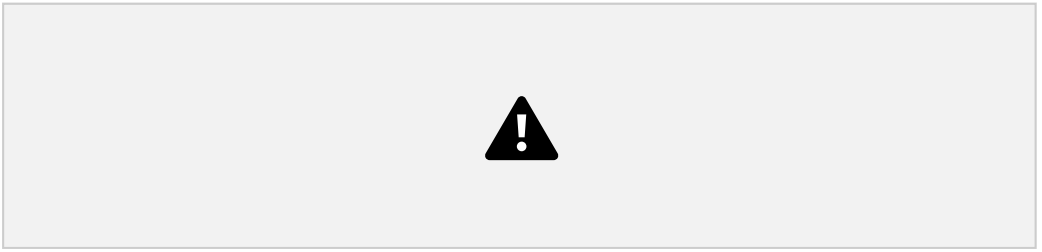
7. If you want to know more about a specific rule and learn its properties, right click on it and select Properties or select it and press Properties in the column on right, which lists the actions that are available for your selection.



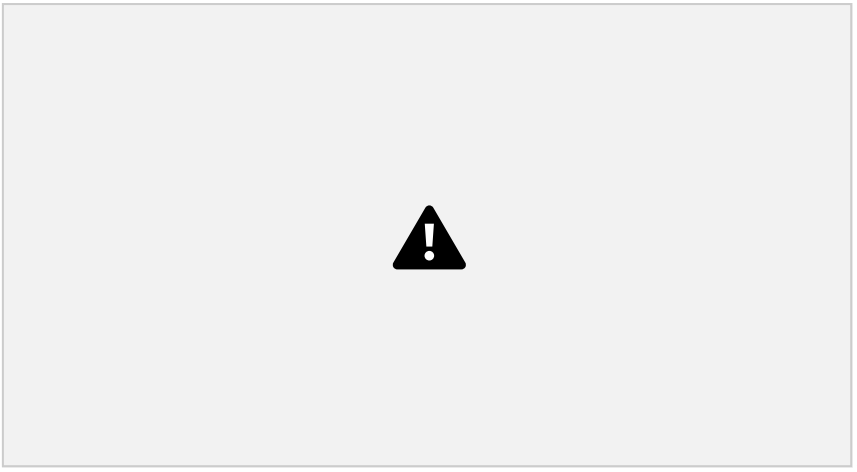
8. In the Properties window, you will find complete information about the selected rule, what it does and in when it is applied. You will also be able to edit its properties and change any of the available parameters.



9. What Are The Connection Security Rules?
   a. Connection security rules are used to secure traffic between two computers while it crosses the network. One example would be a rule which defines that connections between two specific computers must be encrypted.
   b. Unlike the inbound or outbound rules, which are applied only to one computer, connection security rules require that both computers have the same rules defined and enabled.
   c. If you want to see if there are any such rules on your computer, click or tap "Connection Security Rules" on the panel on the left. By default, there are no such rules defined on Windows computers and devices. They are generally used in business environments and such rules are set by the network administrator.



10. What Does the Windows Firewall with Advanced Security Monitor? The Windows Firewall with Advanced Security includes some monitoring features as well. In the Monitoring section you can find the following information: the firewall rules that are active (both inbound and outbound), the connection security rules that are active and whether there are any active security associations.



30

11. You should note that the Monitoring section shows only the active rules for the current network location. If there are rules which get enabled for other network locations, you will not see them in this section.

If you want the firewall to prevent all programs from communicating, including programs that you have previously allowed to communicate through the firewall, select the Block all incoming connections, including those in the list of allowed programs check box.

Self – Check 3.5

Direction: Write SECURITY if the statement is correct and VIRUS if it is not correct. Use a separate sheet of paper.

1. A firewall is hardware or software that can help protect your PC from unauthorized users or malicious software (malware).
2. Running a firewall on each PC on your network won't help control the spread of malicious software on your network.
3. In order to provide the security you need, the Windows Firewall has a standard set of inbound and outbound rules.
4. These rules can't be configured so that they are specific to: computers, users, programs, services, ports or protocols.
5. In the Windows Firewall with Advanced Security, you can access all rules and edit their properties.
6. Connection security rules are used to secure traffic between two computers while it crosses the network.
7. Monitoring section shows only the active rules for the current network location. 8. Unlike the inbound or outbound rules, which are applied only to one computer, connection security rules require that both computers have the same rules defined and

enabled.
9.Windows Firewall with Advanced Security is a tool which gives you detailed control over the rules that are applied by the Windows Firewall.
10. Inbound rules are applied to the traffic that is coming from the network and the Internet to your computer or device.