Lab 10 - Firewall

Firewalls –  
A firewall monitors and controls incoming and outgoing network traffic  
based on predetermined security rules.  
  
Firewalls can be hardware, software, or a combination of both.  
Hardware firewalls are typically deployed at the perimeter of a  
network, while software firewalls can be deployed on individual hosts  
or devices.  
  
Firewalls work by inspecting network traffic and comparing it to a set  
of security rules. If a packet of data matches a rule, the firewall  
will allow it to pass through. If a packet does not match any rules,  
the firewall will drop it.  
  
Perform following actions using your windows machine  
  
a)     Check firewall settings in your windows machine.  
  
b)    Describe what your windows Firewall is blocking and why.  
  
c)     What happens if you turn your firewall off?  
  
d)    Block ping command using firewall in your windows machine, also  
pair up with other students to verify the same.  
  
e)     Whether a firewall is able to block some specific pages in a  
web application? If yes then demonstrate the same using windows  
firewall.

Answers :-

Sure, here are the steps to perform the requested actions using your Windows machine:

**a) Check firewall settings in your windows machine**

1. Open the Windows Security app. Search for it in the search bar or navigate to Start > Settings > Update & Security > Windows Security.
2. Click on "Firewall & network protection".
3. Under "Domain, private, and public network settings", make sure the firewall is turned on for all network types.
4. You can also click on "Advanced settings" to view and modify more detailed firewall settings.

**b) Describe what your Windows Firewall is blocking and why**

Windows Firewall is designed to block unauthorized access to your computer by filtering incoming and outgoing network traffic. It blocks traffic based on a set of predefined rules, which can be customized to your specific needs.

Some of the things that Windows Firewall might block include:

* **Malicious software:** Windows Firewall can block known malicious software from accessing your computer.
* **Unauthorized access attempts:** Windows Firewall can block attempts by unauthorized users to access your computer.
* **Unwanted traffic:** Windows Firewall can block unwanted traffic, such as advertising and tracking cookies.

**c) What happens if you turn your firewall off?**

If you turn your firewall off, your computer will be more vulnerable to attacks. Malicious software will be able to access your computer more easily, and unauthorized users will be able to gain access to your data.

**d) Block ping command using firewall in your windows machine, also pair up with other students to verify the same**

To block the ping command using Windows Firewall, follow these steps:

1. Open the Windows Security app.
2. Click on "Firewall & network protection".
3. Click on "Advanced settings".
4. In the left-hand pane, select "Inbound Rules".
5. In the right-hand pane, click on "New rule".
6. Select "Port" and click "Next".
7. Select "UDP" and enter "147" in the Specific local ports field. Click "Next".
8. Select "Block the connection" and click "Next".
9. Select all network types and click "Next".
10. Name the rule "Block ping" and click "Finish".

To verify that the ping command is blocked, open a command prompt on another computer and type the following command:

ping <your computer's IP address>

You should not receive any replies.

**e) Whether a firewall is able to block some specific pages in a web application? If yes then demonstrate the same using windows firewall**

Firewalls are typically used to control the flow of network traffic based on various criteria such as IP addresses, ports, and protocols. While firewalls can help protect against unauthorized access to your network, they are not typically designed to block specific web pages directly.

To block specific web pages, you would usually use a different type of solution, such as content filtering or web filtering software. These solutions are designed to analyze and filter web traffic based on the content of the web pages being accessed. Some organizations and network administrators use web proxies or dedicated filtering appliances to implement content filtering.