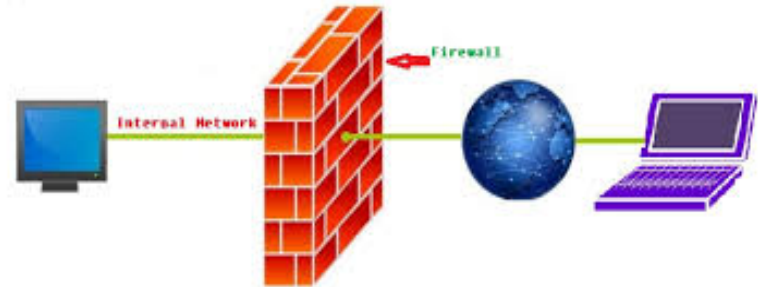


Firewalls

Firewall

- A firewall is a security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules
- A firewall can be hardware, software, or both
- It can prevent unauthorized access to your d or computing devices



Protecting Your Data & Devices

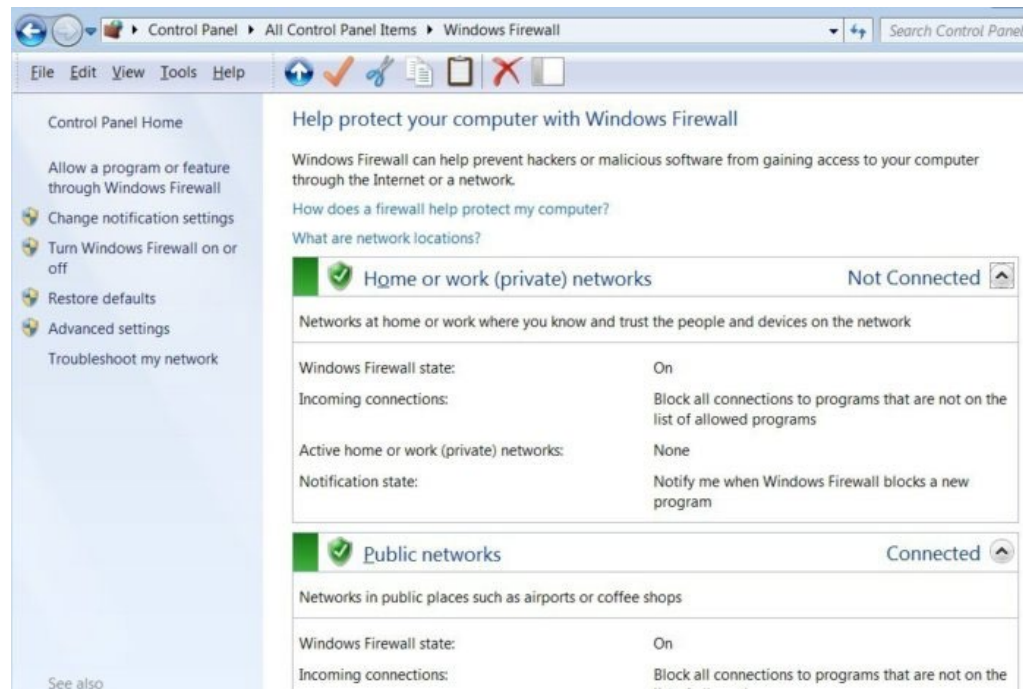
The default rules for a firewall is that all traffic is allowed out from the network \ host and no traffic in unless configured otherwise





Basic Windows Firewall

- Incorporated into Windows
- Stateful
- Fundamental rules:
 - Firewall on/off
 - Allow apps through
 - No scope



Advanced Windows Firewall

Control traffic by:

Application

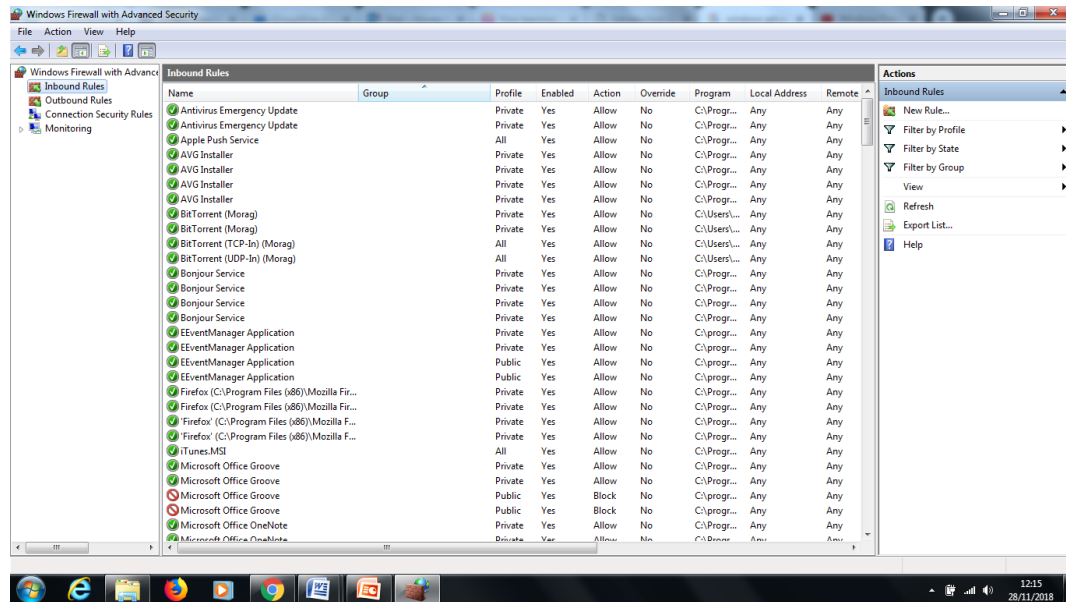
Protocol Type (UDP, TCP)

Port Number

IP address

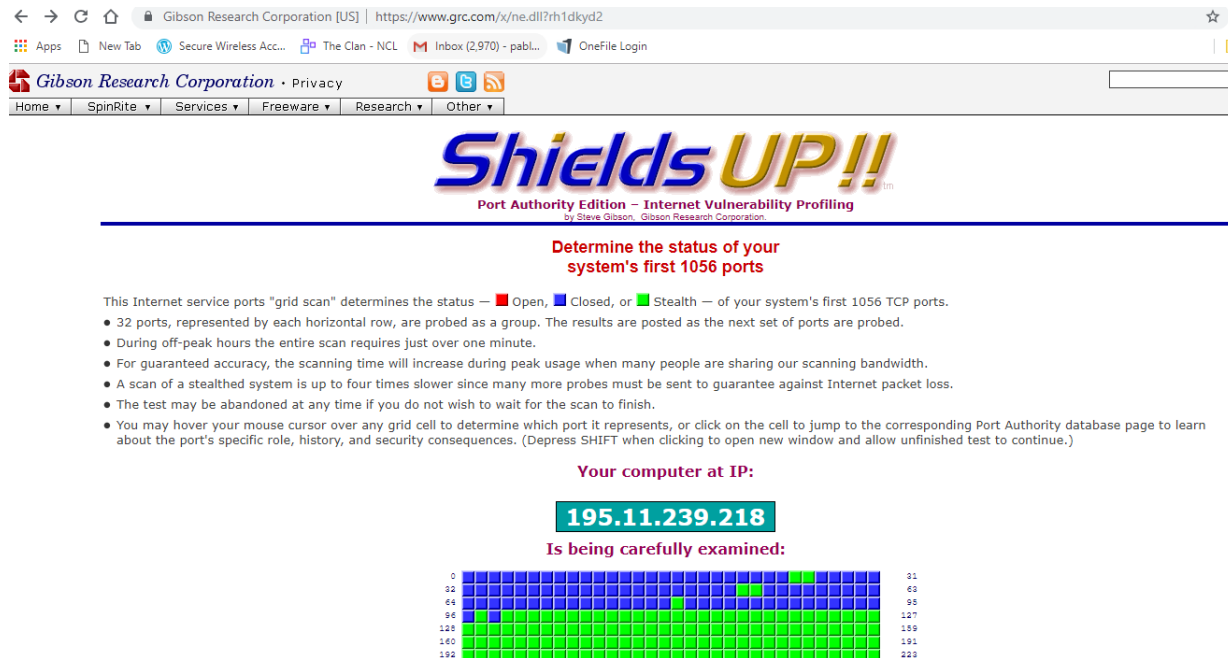
Or a mix of them!

Practical exercise on Moodle!!



ShieldsUP Security

The Shields up website (<https://www.grc.com/x/ne.dll?rh1dkyd2>) All Service Ports function will test which ports are open on your computer firewall!! (as shown below).



The screenshot shows the ShieldsUP website interface. At the top, there's a navigation bar with links like Home, SpinRite, Services, Freeware, Research, and Other. Below the navigation bar is the ShieldsUP logo, which reads "ShieldsUP!!" in a stylized font, followed by "Port Authority Edition - Internet Vulnerability Profiling" and "by Steve Gibson, Gibson Research Corporation".

The main heading is "Determine the status of your system's first 1056 ports". Below this, a paragraph explains that the "grid scan" determines the status of the first 1056 TCP ports. A list of bullet points follows:

- 32 ports, represented by each horizontal row, are probed as a group. The results are posted as the next set of ports are probed.
- During off-peak hours the entire scan requires just over one minute.
- For guaranteed accuracy, the scanning time will increase during peak usage when many people are sharing our scanning bandwidth.
- A scan of a stealthed system is up to four times slower since many more probes must be sent to guarantee against Internet packet loss.
- The test may be abandoned at any time if you do not wish to wait for the scan to finish.
- You may hover your mouse cursor over any grid cell to determine which port it represents, or click on the cell to jump to the corresponding Port Authority database page to learn about the port's specific role, history, and security consequences. (Depress SHIFT when clicking to open new window and allow unfinished test to continue.)

Below the list, it says "Your computer at IP:" followed by a green box containing the IP address "195.11.239.218". Underneath that, it says "Is being carefully examined:". At the bottom, there is a grid of 1056 cells (32 rows by 33 columns). The cells are colored blue, green, or red. Most cells are blue, indicating they are closed. A few cells are green, indicating they are open. The grid is labeled with numbers 0 to 31 on the left and 0 to 31 on the right, representing the 32 rows of 33 ports each.

Alternative personal firewalls

- Research three free personal firewalls.
- Why use them instead of Windows Firewall?