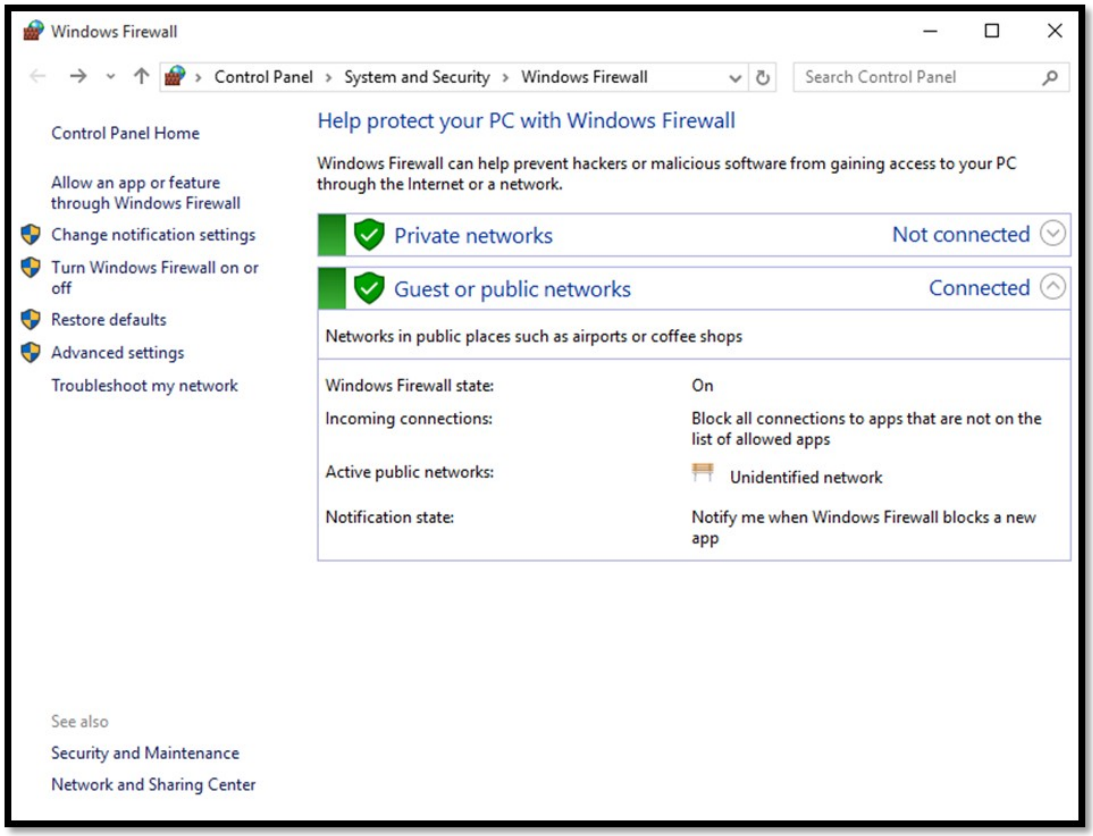
3.5 Windows Firewalls

Windows first started shipping a primitive firewall, called Internet Connection Firewall (ICF), with Windows 2000. It was very simple. Each version of Windows since then has expanded upon this idea. Windows 10 ships with a fully functioning firewall. This firewall can block inbound and outbound packets. To access the Windows 10 firewall, click the Start button and type Firewall.



Beginning with Windows Server 2008 and all versions after that, Windows Firewalls are stateful packet inspection firewalls. With the Windows 10 Firewall, you can set different rules for outbound and inbound traffic. For example, your standard workstation will probably allow outbound HTTP traffic on port 80, but you might not want to allow inbound traffic (unless you are running a web server on that workstation).

You can also set up rules for a port, a program, a custom rule, or one of the many predefined rules that Microsoft has for you to select from. You can also choose not only to allow or block the connection, but to

allow it only if it is secured by IPSec. That provides you with three options for any connection.

Rules allow or block a given application or port. You can also have different rules for inbound and outbound traffic. The rules allow you to decide whether a particular type of communication is blocked or allowed. You can have different settings for inbound and outbound traffic. You can set rules for individual ports (all 65,535 available network ports) and for applications. The rules in the Windows firewall can give you a lot of flexibility.

More importantly, you can apply rules differently depending on where the traffic comes from. You can set up rules for three areas or profiles:

- **Domain:** For those computers authenticated on your domain.
- **Public:** For computers from outside your network. You would treat outside traffic more carefully than traffic coming from another machine in your domain.
- **Private:** Private refers to traffic from your own computer, thus the term private.

Administrators should always follow these rules with all packet filtering firewalls:

- If you do not explicitly need a port, then block it. For example, if you are not running a web server on that machine, then block all inbound port 80 traffic. With home machines, you can usually block all ports. With individual workstations on a network, you may need to keep some ports open in order to allow various network utilities to access the machine.
- Unless you have a compelling reason not to, always block ICMP traffic because many utilities such as ping, tracert, and many port scanners use ICMP packets. If you block ICMP traffic, you will prevent many port scanners from scanning your system for vulnerabilities.
- Occasionally, a good suggestion is to write out acronyms such as ICMP just to make sure this is reinforced.

The Windows Firewall also has a logging feature, but it is disabled by default. Turn this feature on (when you configure the firewall you will see a place to turn on logging). Check this log periodically. You can find more details on the Windows 10 Firewall at https://docs.microsoft.com/en-us/windows/access-protection/windows-firewall/windows-firewall-with-advanced-security.