Windows Firewall with Advanced security profiles

Windows Firewall with Advanced Security uses firewall profiles to provide a consistent configuration for networks of a specific type, and allows you to define a network as either a domain network, a public network, or a private network.

You can define a configuration set for each type of network when you use Windows Firewall with Advanced Security. Each configuration set is a *firewall profile*. Firewall rules are activated only for specific firewall profiles.

The following table lists the Windows Firewall with Advanced security profiles

Profile	**Description**
Public	Use when you are connected to an untrusted public network. Other than domain networks, all networks are categorized as Public. By default, Windows Vista, Windows 7, and Windows 8 use the Public profile, which is the most restrictive.
Private	Use when you are connected behind a firewall. A network is categorized as private only if an administrator or a program identifies the network as private. Networks marked as Home or Work in Windows Vista, Windows 7, and Windows 8 are added to the Private profile.
Domain	Use when your computer is part of a Windows operating system domain. Windows operating systems automatically identify networks on which it can authenticate access to the domain controller. The Domain profile is assigned to these networks, and this setting cannot be changed. No other networks can be placed in this category.

Windows Server 2012 allows multiple firewall profiles to be active on a server simultaneously. This means that a multi-homed server that is connected to both the internal network and the perimeter network can apply the domain firewall profile to the internal network, and the public or private firewall profile to the perimeter network.