Windows Firewall is a host-based firewall that is included in Windows Server 2012. This snap-in runs on the local computer and restricts network access to and from that computer.

Unlike a perimeter firewall, which provides protection only from threats on the Internet, a host-based firewall provides protection from threats wherever they originate. For example, Windows Firewall protects a host from a threat within the local area network (LAN).

Inbound and Outbound Rules

Inbound rules control communication that another device or computer on the network initiates with the host computer. By default, all inbound communication is blocked, except the traffic that is allowed explicitly by an inbound rule.

Outbound rules control communication that is initiated by the host computer, and is destined for a device or computer on the network. By default, all outbound communication is allowed except the traffic that is explicitly blocked by an outbound rule. If you choose to block all outbound communication except the traffic that is explicitly allowed, you must carefully catalog the software that is allowed to run on that computer and the network communication required by that software.

You can create inbound and outbound rules based on User Datagram Protocol (UDP) and TCP ports, as well as other protocols. You also can create inbound and outbound rules that allow a specific executable network access, regardless of the port number that is being used.

Connection Security Rules

You use Connection Security Rules to configure IPsec for Windows Server 2012. When you configure these rules, you can authenticate communication between computers, and then use that information to create firewall rules based on specific user and computer accounts.

Additional Configuration Options

Windows Firewall with Advanced Security is a Microsoft Management Consoles (MMC) snap-in that allows you to perform advanced configuration of Windows Firewall.

Windows Firewall in Windows 8 and Windows Server 2012 provides the following features:

- Supports filtering for both incoming and outgoing traffic
- Integrates firewall filtering and IPsec protection settings
- Enables you to configure rules to control network traffic
- Provides network location-aware profiles
- Enables you to import or export policies

You can configure settings for Windows Firewall on each computer individually, or by accessing the following location from the GPMC:

Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security

- **Note:** Windows Server 2012 introduces the additional option for administering Windows Firewall by using the Windows PowerShell command-line interface.

Discussion: Why Is a Host-Based Firewall Important?

Review the discussion question and participate in a discussion to identify the benefits of using a host-based firewall, such as Windows Firewall with Advanced Security.

Question: Why is it important to use a host-based firewall, such as Windows Firewall with Advanced Security?

Firewall 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.

Connection Security Rules

A connection security rule forces authentication between two peer computers before they can establish a connection and transmit secure information. They also secure that traffic by encrypting the data that is transmitted between computers. Windows Firewall with Advanced Security uses IPsec to enforce these rules.

The configurable connection security rules are:

- Isolation. An isolation rule isolates computers by restricting connections that are based on credentials such as domain membership or health status. Isolation rules allow you to implement an isolation strategy for servers or domains.
- Authentication Exemption. You can use an authentication exemption to designate connections that do not require authentication. You can designate computers by a specific IP address, an IP address range, a subnet, or a predefined group such as a gateway.
- Server-to-Server. A server-to-server rule protects connections between specific computers. This type of rule usually protects connections between servers. When creating the rule, specify the network endpoints between which communications are protected. Then designate requirements and the authentication that you want to use.
- Tunnel. With a tunnel rule, you can protect connections between gateway computers. Typically, you use a tunnel rule when connecting across the Internet between two security gateways.
- Custom. Use a custom rule to authenticate connections between two endpoints when you cannot set up authentication rules that you need by using the other rules available in the new Connection Security Rule Wizard.

How Firewall Rules and Connection Security Rules Work Together

Firewall rules allow traffic through the firewall, but do not secure that traffic. To secure traffic with IPsec, you can create connection security rules. However, connection security rules do not allow traffic through a firewall. You must create a firewall rule to do this. Connection security rules are not applied to programs and services. Instead, they are applied between the computers that make up the two endpoints.

Deploying Firewall Rules

How you deploy Windows Firewall rules is an important consideration. Choosing the appropriate method ensures that rules are deployed accurately and with minimum effort.

You can deploy Windows Firewall rules:

- Manually. You can configure firewall rules individually on each server. However, in an environment with more than a few servers, this is labor intensive and prone to error.

  Typically, you use this method only during testing and troubleshooting.
- By using Group Policy. This is the preferred way to distribute firewall rules. By using Group Policy, you can create and test a GPO with the required firewall rules, and then deploy the firewall rules quickly and accurately to a large number of computers.
- By exporting and importing firewall rules. You have the option to import and export firewall rules when you use Windows Firewall with Advanced Security. For example when you are troubleshooting, you can export firewall rules to create a backup before you configure them manually.

  Note: When you import firewall rules, they are treated as a complete set, and replace all currently-configured firewall rules.