13.10.3 Firewall Facts

A *firewall* is a device or software running on a device that inspects network traffic and allows or blocks traffic based on a set of rules. There are two types of firewalls that you should be familiar with:

- A network-based firewall inspects traffic as it flows between networks. For example, you can install a network-based firewall on the edge of your private network that connects to the internet to protect against attacks from internet hosts. A network firewall is created using two (or more) interfaces on a network device: one interface connects to the private network, and the other interface connects to the external network.
- A host-based firewall inspects traffic received by a specific host.

A best practice is to implement both types of firewalls.

Firewalls use filtering rules, sometimes called access control lists (ACLs), to identify allowed and blocked traffic. A rule identifies characteristics of the traffic, such as:

- The interface the rule applies to
- The direction of traffic (inbound or outbound)
- Packet information such as the source or destination IP address or port number
- The action to take when the traffic matches the filter criteria

Windows includes a host-based firewall that you can configure to protect your system from attacks. Be aware of the following:

- By default, the firewall allows all outgoing web traffic and responses but blocks all other traffic.
- You can configure exceptions to allow specific types of traffic through the firewall. In Windows Firewall, you can configure two exception types:

Exception	Description
Program	Configuring an exception for a program automatically opens the ports required by the application only while the application is running. Be aware of the following: - You can select from a list of known applications or browse to and select an unlisted application. - You do not need to know the port number used; the firewall automatically identifies the ports used by the application when it starts. - After the application is stopped, the required ports are closed.
Port	Configuring an exception for a specific port and protocol (either TCP or UDP) keeps that port open all the time. Be aware of the following: - You must know both the port number and the protocol. - Some services require multiple open ports, so you must identify all necessary ports and open them. - Ports stay open until you remove the exception.

- When you turn on the firewall, you can block all incoming connections or allow exceptions. If all incoming connections are blocked, any defined exceptions are ignored.

When you configure a network-based firewall, you identify the traffic type that is allowed both into and out of your private network. Keep the following in mind:

- Most SOHO routers and access points include a firewall to protect your private network.
- By default, most SOHO routers allow all traffic initiated on the private network to pass through the firewall. Responses to those outbound requests are typically also allowed. For example, a user browsing a website will receive the web pages back from the internet server.
- All traffic initiating from the external network is blocked by default.
- You can configure individual exceptions to allow or deny specific types of traffic. A best practice is to block all ports, then open only the necessary ports.
- Some firewalls support *port triggering*, which allows the firewall to dynamically open incoming ports based on outgoing traffic from a specific private IP address and port.
  - On the firewall you identify a private IP address and port, then associate one or more public ports.
  - When the router sees traffic sent from the private network from that host and port number, the corresponding incoming ports are opened.
  - The incoming ports remain open as long as the outgoing ports show activity. When the outgoing traffic stops for a period of time, the incoming ports are automatically closed.

    - Use port triggering to open incoming ports required for specific applications (such as online games).
- Some applications identify incoming ports dynamically once a session is established with the destination device. The ports that the application might use are typically within a certain range.
    - For some applications, you can configure the application to use a specific port instead of a dynamic port. You can then open only that port in the firewall.
    - If you are unable to configure the application, you will need to open the entire range of possible ports in the firewall.
    - Use port triggering to dynamically open the ports when the application runs instead of permanently opening all required ports.
- Configure port forwarding to allow incoming traffic directed to a specific port to be allowed through the firewall and sent to a specific device on the private network.
    - Inbound requests are directed to the public IP address on the router to the port number used by the service (such as port 80 for a Web server). The port number is often called the public port.
    - Port forwarding associates the inbound port number with the IP address and port of a host on the private network. This port number is often called the private port.
    - Incoming traffic sent to the public port is redirected to the private port.

When defining firewall rules, you should be aware of the following port numbers for common network protocols:

Service	Port(s)
File Transfer Protocol (FTP)	20 TCP 21 TCP
Secure Shell (SSH)	22 TCP and UDP
Telnet	23 TCP
Simple Mail Transfer Protocol (SMTP)	25 TCP
Domain Name System (DNS)	53 UDP
HyperText Transfer Protocol (HTTP)	80 TCP
Post Office Protocol (POP3)	110 TCP
Network Basic Input/Output System (NetBIOS)	137 TCP 138 TCP 139 TCP
Internet Message Access Protocol (IMAP4)	143 TCP and UDP
HTTP with Secure Sockets Layer (SSL)	443 TCP and UDP
Service Location Protocol (SLP)	427 TCP and UDP
Server Message Block (SMB)/Common Internet File System (CIFS)	445 TCP
Apple File Protocol (AFP)	548 TCP
Remote Desktop Protocol (RDP)	3389 TCP