CHAPTER 22

Network Security Devices

The only way to keep a computer 100 percent safe from attacks is to never turn it on. When you start using it, especially when it is connected to a network, the risk of attacks rises significantly. Defense-in-depth refers to the practice of using multiple layers of security to protect systems and networks. Digital security methods play a large role in network security. This chapter covers several digital security methods used on networks, with a strong focus on firewalls.

Exam 220-801 objectives in this chapter:

- 2.6 Install, configure, and deploy a SOHO wireless/wired router using appropriate settings.
  - Port forwarding, port triggering
  - Firewall
  - DMZ
  - Basic QoS
- 2.9 Compare and contrast network devices and their functions and features.
  - Firewall
  - Internet appliance

Exam 220-802 objectives in this chapter:

- 1.4 Given a scenario, use appropriate operating system features and tools.
  - Administrative
    - Windows firewall
    - Advanced security
- 1.5 Given a scenario, use Control Panel utilities (the items are organized by “classic view/large icons” in Windows).
  - Common to all Microsoft Operating Systems
    - Security center
    - Windows firewall

- 1.6 Setup and configure Windows networking on a client/desktop.
  - Proxy settings
  - Remote desktop
  - Home vs. Work vs. Public network settings
  - Firewall settings
    - Exceptions
    - Configuration
    - Enabling/disabling Windows firewall
- 2.1 Apply and use common prevention methods.
  - Digital security
    - Firewalls

Securing a Network

If you pay attention to the news, you've probably heard about many different types of IT attacks. Criminals are regularly looking for ways to break into networks and systems. Sometimes they're doing it for monetary gain, and other times they're attacking for revenge or espionage.

When they successfully hit large corporations, you hear about it on the news. When individuals or small business owners lose a few thousand dollars from an attack, you typically won't hear anything. However, these types of losses are happening every day.

Threats and Attacks

IT security professionals know that if a computer has a public IP address on the Internet, it's only a matter of time before it's discovered and probed looking for vulnerabilities.

Sometimes criminals can access systems remotely and scour the drives looking for data. Sometimes they use automated tools to launch attacks. Two common types of attacks are *denial of service (DoS)* and *distributed denial of service (DDoS)* attacks.

- **DoS.** This is an attack against a computer from one other computer. The goal is to disrupt the normal operation so that the computer can't provide service to users. For example, a DoS attack against a web server prevents it from answering requests for webpages in a timely manner.
- **DDOS.** This is a DoS attack from multiple attackers simultaneously. Botnets are frequently used to attack targets with thousands of zombie computers.

MORE INFO **CHAPTER 26, "RECOGNIZING MALWARE AND OTHER THREATS"**

Chapter 26 covers botnets and other threats. Some botnets have controlled more than a million computers at a time. The computers within the botnet act like zombies and do whatever the bot herder tells them to do.

It's important to be aware that threats are real. There are multiple digital security methods available that can help protect a computer, but when people ignore the threats, they often perceive the digital security methods as a hindrance and ignore them. One of the primary digital security methods that you'll find on almost every computer is a firewall.

Understanding Firewalls

Firewalls block or allow network traffic, with the goal of protecting networks and computers. The concept is similar to a firewall in a car, which separates the engine compartment from the passenger compartment. If the engine catches fire, the firewall protects the passengers by preventing the fire from reaching them.

Similarly, a computer firewall protects systems from malicious traffic. The most common source of malicious traffic is from the Internet, so it's important to use a firewall for any system connected to the Internet.

Firewalls are classified as either network-based or host-based.

- **Network-based firewall.** This controls traffic allowed in or out of the network. A network-based firewall can be a dedicated appliance that acts as only a firewall, or it can be another device, such as a router, that includes firewall capabilities.
- **Host-based firewall.** This is software running on a computer or host. Windows-based systems include the Windows Firewall, which is a Control Panel applet running within Windows, and many third-party software applications are also available.

Figure 22-1 shows a simple network using both network-based and host-based firewalls. The network firewall controls traffic to and from the Internet. The desktop computers and the server have host-based firewalls controlling traffic to and from each system.

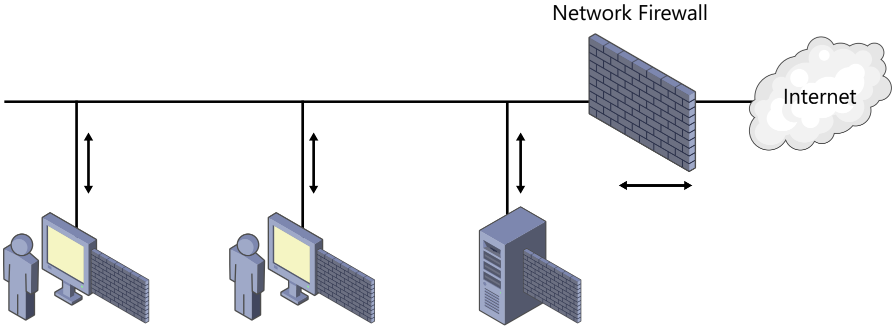


FIGURE 22-1 Network with network-based and host-based firewalls.

NOTE ROUTERS AND FIREWALLS

Most routers used in small office home office (SOHO) or home networks include firewall capabilities. These include default configurations needed by most users for Internet access and include web access pages you can use to modify the settings.

You might be wondering why there are so many firewalls being used. After all, if the network firewall is blocking malicious traffic from the Internet, why would you need firewalls on individual computers too? It's a common question.

The answer is based on a defense-in-depth philosophy of using multiple layers. It's very easy for a user to unknowingly bring in malicious software (malware) from his computer on a USB flash drive. After infecting his work computer, it could start crawling through the network to infect other computers. Host-based firewalls help protect against this type of scenario.

Exceptions

Most firewalls start with an implicit deny policy, meaning that they automatically block all traffic. Of course, you want to allow some traffic, so exceptions are allowed. For example, if you want to allow Hypertext Transfer Protocol (HTTP), you can configure a rule to identify the exception. The firewall will then block all traffic *except* for HTTP traffic.

Exceptions are identified as rules and stored in an *access control list (ACL)*. Firewalls will typically have many rules in place.

Packet-Filter Exceptions

A basic packet-filtering firewall can filter network packets based on the following components:

- **IP address.** A rule can be configured to block or allow traffic from a specific IP address such as 192.168.1.1 or from entire networks by using a network ID such as 192.168.1.0/24.
- **Ports.** Protocols are identified with ports, and traffic can be controlled by using these port numbers. For example, if you want to allow Simple Mail Transfer Protocol (SMTP) traffic, you can create an exception for port 25, the well-known port for SMTP.

MORE INFO CHAPTER 20, CHAPTER 21, AND CHAPTER 24

Chapter 20, "Understanding Protocols," covers ports, including the well-known ports specifically mentioned in the CompTIA A+ objectives. Chapter 21, "Comparing IPv4 and IPv6," covers IP addresses and network IDs. Chapter 24, "Connecting and Troubleshooting a Network," covers troubleshooting commands such as ping and tracert.

- **Protocol IDs.** Some protocols are identified with a protocol ID instead of a port. For example, the ping and tracert commands use Internet Control Message Protocol (ICMP), and ICMP traffic is identified with a protocol ID of 1. You can allow or block all ping and tracert traffic by using protocol ID 1.
- **A combination.** Packet rules can be created using any combination of these. For example, if an email server has an IP address of 192.168.1.10, you can create an SMTP rule that allows a computer to send port 25 packets only to 191.68.1.10. Port 25 packets with any other destination will be blocked.

EXAM TIP

As a PC technician, you might need to configure rules to allow or block specific types of traffic. The most common way this is done is by creating a port rule. This section has repeated that port 25 is used for SMTP traffic, but there are some other ports that you should memorize. Specifically, you should memorize the ports listed in Chapter 20, "Understanding Protocols," in Table 20-3.

Other Exceptions

Firewalls have become sophisticated over the years. Packet-filter firewalls are considered first generation firewalls, and newer files are called second generation and third generation. The advanced firewalls include the basic capabilities but add to them.

In addition to examining a single packet, these advanced firewalls can examine traffic from an entire network conversation between computers. Normal traffic follows specific patterns, but attackers use abnormal methods when attacking systems. These advanced firewalls can often detect abnormal traffic and block it.

Understanding DMZs

A *demilitarized zone (DMZ)* is a buffer zone that provides a layer of security protection. It is most commonly used to host Internet-facing servers and normally uses two firewalls.

Imagine a company that wants to host its own website. One method is to install *Internet Information Services (IIS)* on a Windows Server product such as Windows Server 2012. IIS works as a web server and is available for free on many Windows-based systems.

If the company places this server directly on the Internet, the server is highly susceptible to attacks. If the company puts it in its internal network, the Internet traffic adds risk to other computers on the internal network. Instead, the company places it in a buffer zone (the DMZ) between the Internet and the internal network, as shown in Figure 22-2.

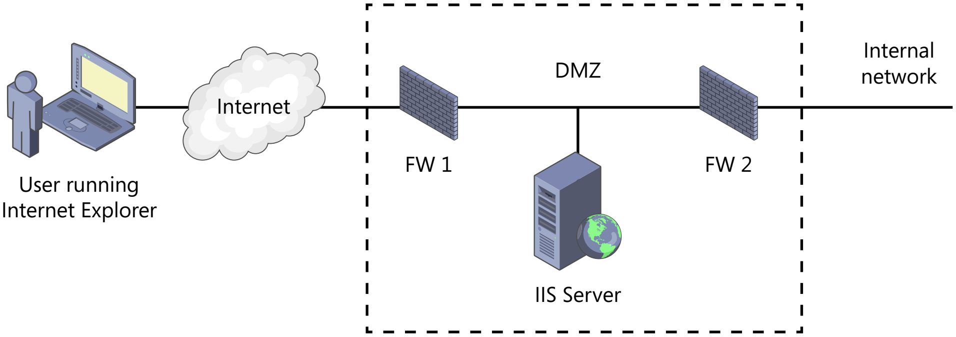


FIGURE 22-2 Hosting a web server in a DMZ.

The first firewall (FW1) provides access to the IIS server for Internet users. It also provides a layer of protection by controlling what traffic is allowed into the DMZ. The second firewall (FW2) provides an additional layer of protection for the internal network. Each firewall will have separate exception rules specifying what traffic is allowed.

NOTE **THREE-LEGGED DMZ**

It's common for a DMZ to have two firewalls, but there are other possible configurations. For example, a three-legged DMZ is a single firewall with three connections. One connection is for the Internet, another is for the web server, and the third is for the internal network. This is cheaper because only one firewall is used, but it is also more complex to configure.

✓ Quick Check

1. What is created in a firewall to allow traffic to pass?
2. How does a firewall identify SMTP traffic?

Quick Check Answers

1. A rule or an exception.
2. By the use of port 25.

Port Forwarding

Most routers and firewalls support port forwarding. This allows specific traffic from the Internet to be forwarded to an internal system. Without port forwarding, Internet clients cannot access this internal system.

For example, imagine that you have a SOHO network protected by a firewall, as shown in Figure 22-3. The firewall is connected to the Internet with a public IP address, and the internal SOHO network has private IP addresses.

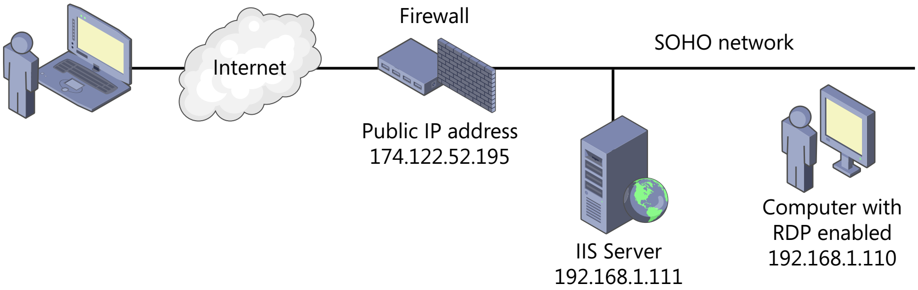


FIGURE 22-3 SOHO network with a web server and RDP-enabled computer.

If you had a laptop computer and you wanted to use it to connect to computers in your SOHO network while you were away, you could do so by enabling port forwarding on the firewall. The overall steps to do this with Remote Desktop are as follows:

1. Enable Remote Desktop Protocol (RDP) on the home computer. This includes ensuring that port 3389 is open on the computer's firewall.
2. Enable port forwarding on the firewall. You could use port 3389 so that any traffic on the Internet side of the firewall is forwarded to your home computer.
3. Start Remote Desktop Connection (mstsc) from an Internet location, and connect to the public IP address of your home firewall.

Remote Desktop Connection uses port 3389 by default. When you connect to the firewall by using port 3389, it will forward the traffic to your internal computer and you will have a remote connection.

MORE INFO **CHAPTER 20, "UNDERSTANDING PROTOCOLS"**

Chapter 20 covers the remote connectivity protocols, including RDP and the Remote Desktop Connection. They are commonly used by administrators to remotely administer servers. The Windows Firewall section later in this chapter shows how to enable Remote Desktop exceptions on Windows-based systems.

You can also use port forwarding to access other systems. For example, if you configured a web server using IIS, you could forward traffic to it as well. A web server uses HTTP, and the default for HTTP is port 80, so you could configure the firewall to forward all traffic from the Internet to the internal web server by using port 80.

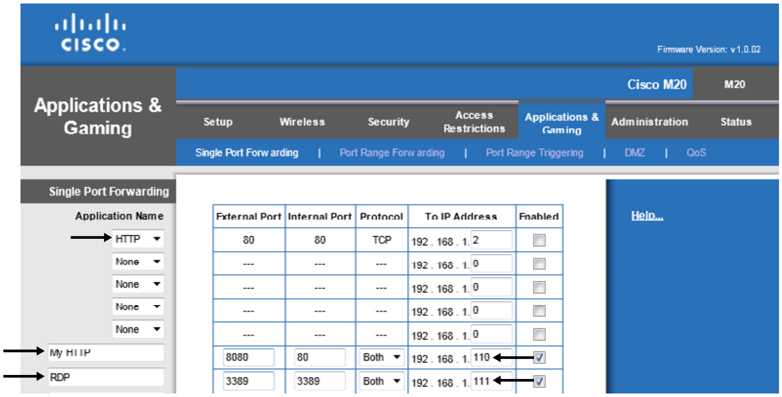
Configuring Port Forwarding

The steps you use to configure port forwarding on a router or firewall are dependent on the brand. You might need to dig out the manual to identify the steps. Many routers used in SOHOs have web-based pages that you can access from a computer, and these often include easy-to-use menus.

For example, Figure 22-4 shows the port forwarding page on a Cisco router. The router includes several pages, and I can access them by using *http://192.168.1.1* in the uniform resource locator (URL) of a web browser and then logging on. In the figure, I've selected the Applications & Gaming section, which includes port forwarding.

MORE INFO **CHAPTER 23, "EXPLORING WIRELESS NETWORKING"**

Table 23-3 in Chapter 23 lists default IP addresses, administrator names, and passwords used to access the web-based pages in many routers. These passwords should be changed from the default to prevent anyone from accessing them.



Application Name	External Port	Internal Port	Protocol	To IP Address	Enabled
HTTP	80	80	TCP	192 . 168 . 1. 2	☐
None	---	---	---	192 . 168 . 1. 0	☐
None	---	---	---	192 . 168 . 1. 0	☐
None	---	---	---	192 . 168 . 1. 0	☐
None	---	---	---	192 . 168 . 1. 0	☐
My HTTP	8080	80	Both	192 . 168 . 1. 110	☑
RDP	3389	3389	Both	192 . 168 . 1. 111	☑

FIGURE 22-4 Configuring port forwarding on a router.

The default port for RDP is 3389. The RDP setting in Figure 22-4 is using this port as the trigger to forward traffic to the internal computer by using the IP address of 192.168.1.110.

I could have used the preconfigured HTTP setting. Notice that it uses the default port of 80 for the external IP address of the firewall and port 80 for the internal computer. If I used it, I would have entered 192.168.1.111 as the address of the internal web server and selected Enabled. A user from the Internet could use this URL *(http://174.122.52.195),* and traffic would be forwarded to the web server.

However, just because port 80 is the default port of HTTP doesn't mean that you must use it on the external IP address for port forwarding. I instead chose to use port 8080 as the external port.

The My HTTP setting forwards all traffic using port 8080 to 192.168.1.111, port 80, which is the web server. If you wanted to access this from the Internet, you'd use the following URL: *http://174.122.52.195:8080*.

If the IP address is registered with Internet Domain Name System (DNS) servers, you can use the name instead of the IP address. For example, if Darrilgibson.com is registered with DNS and uses 174.122.52.195, you can enter the URL as *http://darrilgibson.com:8080*.

MORE INFO **PORTFORWARD.COM**

Figure 22-4 shows the port forwarding page for one router, but all routers are not the same. Port Forward (*http://portforward.com/*) includes multiple resources and guides that provide the steps for configuring port forwarding on hundreds of different routers.

Port Forwarding and IP Addresses

There's an important point to realize with port forwarding: the internal computers must always have the same IP addresses.

Internal desktop computers are typically assigned IP addresses with Dynamic Host Configuration Protocol (DHCP). When they are restarted, they can get a different IP address, and if the IP address is changed, port forwarding will no longer work for that computer.

EXAM TIP

The most common reason that port forwarding doesn't work is that it isn't configured correctly. It needs to be configured on the router with the correct ports, and the IP addresses of internal computers must not change.

Port Forwarding and SSH

Port forwarding is often associated with Secure Shell (SSH). SSH is an encryption protocol used to secure many different types of traffic, such as Secure File Transfer Protocol (SFTP) and Secure Copy (SCP). Both protocols use port 22.

When port forwarding is used to forward SSH traffic, it's common to use port 22 as the external port. Any external traffic using port 22 will be forwarded to an internal system configured to accept SSH traffic.

Port Triggering

Port triggering is used to open an incoming port in response to traffic on an outgoing port. The incoming port is normally closed and will close again a short while after the session is closed.

For example, imagine that you have an application that sends data out on port 5678 and receives data back on port 8765, as shown in Figure 22-5. You would configure the router to recognize outgoing port 5678 as the trigger, and when it received outgoing traffic on this port, it would open incoming port 8765.

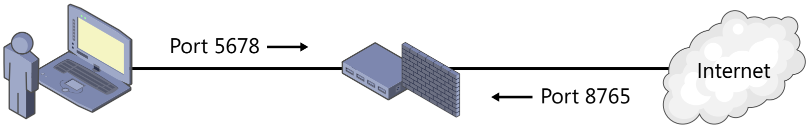


FIGURE 22-5 Using port triggering on a router.

EXAM TIP

Port triggering is used by internal clients only to open an incoming port. Port triggering is not used to open ports in response to triggers from an Internet computer.

Port triggering often uses port ranges. That is, the trigger range might be 5670 to 5680 and the input range might be 8760 to 8770. When the router receives outgoing traffic using any port between 5670 to 5680, it opens incoming ports 8760 to 8770.

One benefit is that port triggering isn't based on IP addresses. Therefore, internal clients can still use DHCP. The router returns data to the same IP address that sent the traffic that triggered the port.

A downfall is that only one internal client can use it at a time. If Joe started an application and triggered the port, it would work for him. If Holly then opened an application and triggered the port, either Joe's connection is lost or Holly's connection is refused. Some routers give preference to the first connection and won't close it. Other routers give preference to the most recent connection request.

Using Proxy Servers

Proxy servers are used in many networks to optimize and control Internet traffic. They are most commonly used with HTTP and Hypertext Transfer Protocol Secure (HTTPS), but they can be used with other protocols, such as File Transport Protocol (FTP).

Figure 22-6 shows a network with a proxy server. Computers configured to use the proxy server send URL requests to the proxy server instead of to the actual Internet web servers. The proxy server retrieves the webpage and returns it to the client.

The proxy server has one or more public IP addresses assigned to it and has direct access the Internet. The internal network has private IP addresses, and the proxy server uses network address translation (NAT) to translate the private IP addresses to public and the public IP address back to private.

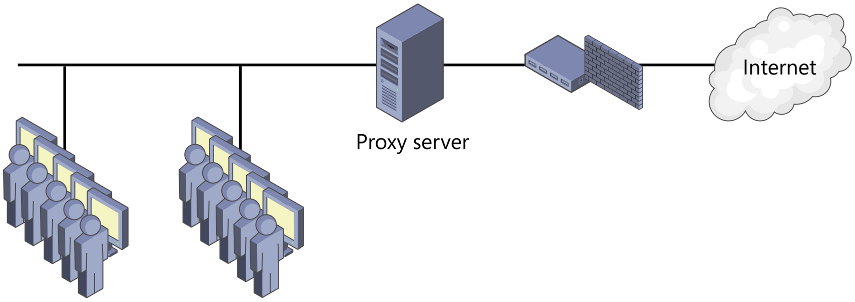


FIGURE 22-6 Network with a proxy server.

MORE INFO **CHAPTER 21**

Chapter 21 covers NAT in more detail. If a network isn't using a proxy server, it would usually run NAT on a router or firewall that is connected to the Internet. If NAT isn't used, all internal clients would need to have public IP addresses, which is expensive. In addition to saving money on public IP addresses, NAT also helps hide the internal clients.

Proxy Server Benefits

Proxy servers provide two important benefits: caching and content filtering. Caching reduces Internet bandwidth usage, and content filtering controls which sites users can access.

As an example of caching, imagine Joe uses his web browser to read some A+ blogs at *http://blogs.GetCertifiedGetAhead.com*. Joe's computer sends the URLs to the proxy server, and the proxy server retrieves the webpages. When the proxy receives the webpages, it stores a copy in an area of its memory called cache and also returns a copy to Joe's computer.

If another user tries to access any of these webpages, the proxy server returns the pages from cache rather than retrieving them from the Internet again. This reduces Internet bandwidth usage because the same pages don't need to be retrieved again.

Content filtering is used to restrict access to websites and block certain content. For example, an organization might decide that they do not want users to visit gambling websites from work computers.

Administrators configure the proxy server with a list of restricted websites, and if a user tries to access a site on the list, the user is redirected to another page. Many organizations display a page that indicates that access to the website is restricted and give information about the organization's security policy.

NOTE **PROXY SERVER SUBSCRIPTIONS**

Many companies sell lists of websites based on categories such as gambling. Organizations purchase subscriptions of these lists and use them to automate the configuration of the proxy server.

Proxy Exceptions

Proxy servers support the use of exceptions with proxy exception rules. For example, a proxy server could include the GetCertifiedGetAhead.com URL among its blocked domains. Administrators could then add proxy exception rules for a specific page within the domain or to an entire subdomain—for example, for the following URLs:

- *http://GetCertifiedGetAhead.com/aplus.aspx*
- *http://blogs.GetCertifiedGetAhead.com*.

After the exception rules are added, users will be able to access the Aplus page and the blog articles within the blogs subdomain, but all other access to the domain remains blocked.

Configuring Proxy Settings

The most common way that systems are configured to use a proxy server is from within the web browser. On Windows-based systems, you can access the Internet Explorer options through the Control Panel Internet Options applet.

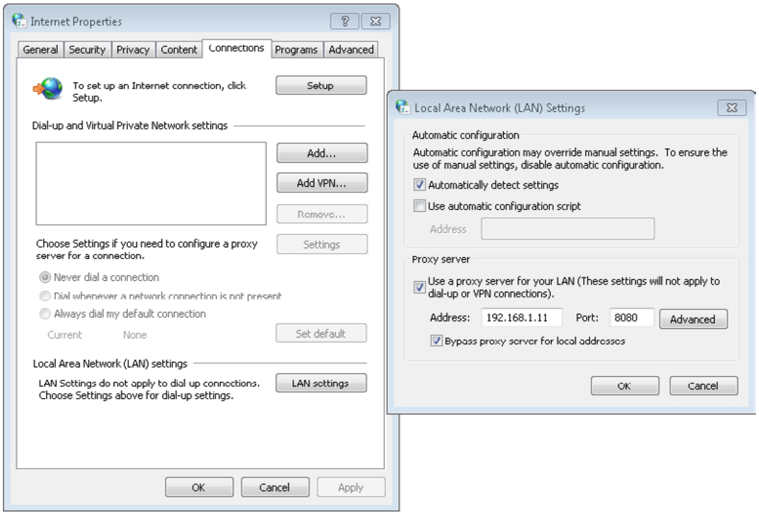
MORE INFO **CHAPTER 13, "USING WINDOWS OPERATING SYSTEMS"**

Chapter 13 covers the Internet Options applet, including how to view and configure many of the other settings.

The following steps can be used to configure the Proxy settings for Internet Explorer via the Internet Options applet:

1. Click Start, Control Panel. If necessary, change the display to Large Icons or Classic View, depending on your operating system.
2. Select Internet Options. You can also access this through Internet Explorer. Press Alt+X to open the Tools menu, and select Internet Options.
3. Click the Connections tab.
4. Click the LAN Settings button.
5. In the proxy server area, select the Use A Proxy Server For Your LAN check box.

6. Enter the internal IP address of the proxy server and the port that the proxy server uses. You display will be similar to the following graphic. By default, these settings apply to all HTTP, HTTPS, and File Transfer Protocol (FTP) traffic, but you can click Advanced and configure different proxy servers for different protocols.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial up connections. Choose Settings above for dial-up settings.

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings
□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.1.11 Port: 8080

☑ Bypass proxy server for local addresses

***NOTE* COMMON PROXY SERVER SETTINGS**

It isn't a requirement, but proxy servers often use port 8080 instead of port 80 to listen for HTTP queries. The Bypass Proxy Server for Local Addresses is selected if the company has internal web servers. It allows computers to connect to internal web servers directly, without going through the proxy server.

Enforcing Proxy Server Use

When an organization has a proxy server in use, they often take steps to ensure that all Internet access is through the proxy. For example, users might realize that the proxy server is blocking access to a site and remove the proxy settings from the web browser.

A common way this is blocked is with a firewall rule. The rule will accept HTTP traffic from the proxy server but block all other HTTP traffic. If a user removes the proxy settings, this firewall rule blocks Internet access until the proxy settings are restored.

Some malware modifies or clears these settings when it takes over or hijacks a web browser. The malware author's goal is to allow the system to access malicious websites that wouldn't normally be accessible through the proxy. However, with the firewall rule in place, this modification effectively blocks all HTTP access for the infected system.

EXAM TIP

If a user has lost Internet access and a proxy server is in use, check the proxy server's settings. If they have been modified, the system might be infected with malware and a full scan should be run with up-to-date antivirus software. Similarly, if you've just cleaned a virus off a system but it still doesn't have Internet access, check these settings.

Basic QoS

Quality of Service (QoS) refers to techniques used to control traffic on a network. For example, users might regularly use computers to watch video from the Internet. Video is sent in a steady stream and can take up a lot of bandwidth. If too many users are streaming video at the same time, it has the potential to slow the network to a crawl.

QoS techniques can be used to give video traffic a lower priority. Streaming video is allowed, but if too many people are streaming videos at the same time, only their connections become slower. Other connections are unaffected, and the overall network performance remains high.

Another way QoS is used is to give higher priority to some traffic. For example, when Voice over Internet Protocol (VoIP) is used for phone calls or teleconferences, the voice data can be choppy if there isn't enough bandwidth. You might hear every other word a speaker says. Giving VoIP a higher priority helps minimize this problem.

QoS is implemented differently on different routers and firewalls. In general, you use rules but associate the rules with QoS. You then assign either a maximum bandwidth for the traffic or a priority.

✓ Quick Check

1. **What is used to allow Internet access to an internal web server through a firewall?**
2. **What might cause proxy settings to be reconfigured without user interaction?**

Quick Check Answers

1. **Port forwarding.**
2. **Malware.**

Windows Firewall

Windows-based systems since Windows XP have included the Windows Firewall. It's a host-based firewall running as software and can be accessed via the Control Panel.

In each operating system, the overall goal of Windows Firewall is the same: to control traffic and help protect the system from malicious traffic. However, criminals are constantly discovering new methods of attack, and security experts are constantly identifying newer and better methods of protection. Because of these improvements, there are some differences in Windows Firewall between different operating systems.

Home vs. Work vs. Public Network Settings

The Windows Firewall in Windows Vista and Windows 7 uses network locations to simplify settings. These are related to the risk level associated with the different locations, as follows:

- **Public risk.** If you connect to the Internet via a wireless network in an airport or coffee shop, you are connected in a public network. You really don't know who else is on the network, and your computer could be attacked. A public network represents the highest risk.
- **Home or work environment risk.** If you connect your computer to a network in your home or where you work, the risk is significantly reduced. It is much harder for an outsider to connect to these networks and launch attacks. Home and work networks are referred to as private networks.

The Windows Firewall is configured with stronger security when it is connected to a public network. This limits some usability but provides greater protection in high risk locations. When connected to a home or work network, the security settings are relaxed, providing increased usability.

Network Discovery

Network discovery is a group of network settings in Windows Vista–based and Windows 7–based computers that makes it easier for computers to locate each other when connected in a network. It is used in private (work and home) networks but disabled in public networks.

When network discovery is turned off, it effectively hides a computer from other devices on the network. It also prevents the computer from seeing other network devices. Network discovery should be turned off when a computer is in a public place.

Network Locations

The three primary network locations are as follows:

- **Home Network.** This is used for homes or SOHOs. Network discovery is enabled, making it easy for computers to see each other and share resources. Users running Windows 7 can create and join homegroups.

EXAM TIP

Access to homegroups is available only in the Home network location. Network Discovery is disabled in the Public Network, blocking homegroups. In the Work network location, Network Discovery is enabled but access to homegroups is blocked.

- **Work Network.** This is used in work environments and can be used for a SOHO. Network discovery is enabled, making it easy for computers see each other and share resources. However, users cannot create or join a homegroup when the work network location is selected.
- **Public Network.** This is used when the computer is connected to an untrusted location. It primarily refers to public locations, such as wireless networks in coffee shops, but should also be selected if a computer is connected directly to the Internet. This setting makes it difficult for other network devices to see the computer and also makes it difficult for the computer to see other network devices. The primary goal is to help protect the computer against malicious attacks.

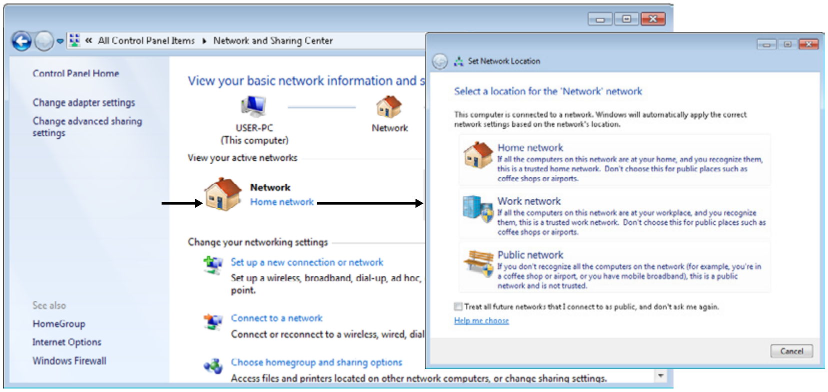
EXAM TIP

The Public network location disables network discovery and makes it difficult for a computer to be discovered and attacked. It should be selected when a computer is connected to a public network or connected directly to the Internet. For example, a single computer connected to a broadband connection at home should use the Public network.

If the computer is joined to a domain, administrators can force it to use a fourth choice called the Domain network location. It's not available to users as a choice, and when it's assigned, regular users cannot change it.

The first time that users connect to a new network, they are prompted to identify their current location. After they make a choice, network discovery and firewall settings are configured for that location.

You can view the current network from the Network and Sharing center. Additionally, you can change the network by clicking the link and selecting a different network. Figure 22-7 shows a system configured as a Home network and the network selection page that appears after clicking Home Network.



View your basic network information and s

View your active networks

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, point.

Connect to a network
Connect or reconnect to a wireless, wired, dial

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Select a location for the 'Network' network

This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.

Home network
If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports.

Work network
If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports.

Public network
If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public network and is not trusted.

☐ Treat all future networks that I connect to as public, and don't ask me again.

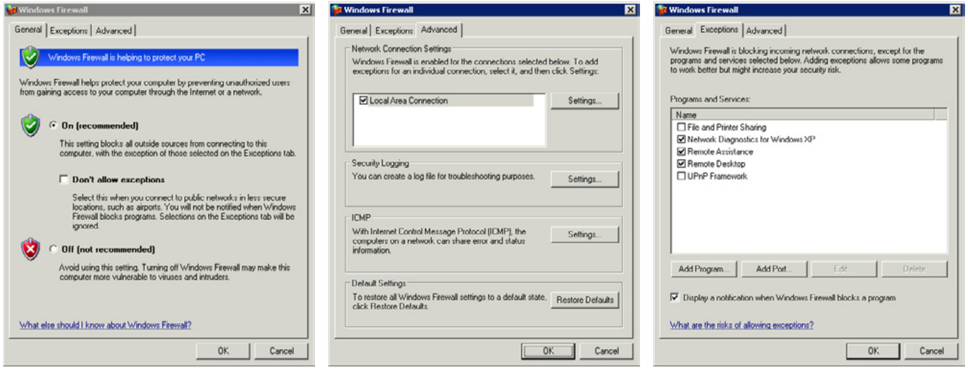
Help me choose

FIGURE 22-7 Network location choices.

Microsoft has a short video about choosing network locations, which you can view from here: *http://windows.microsoft.com/en-us/windows7/Choosing-a-network-location*.

Configuring Windows Firewall on Windows XP

You can start Windows Firewall on Windows XP from the Control Panel. Change the Control Panel view to Classic View, and double-click Windows Firewall. It has three tabs, as shown in Figure 22-8.



Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

☐ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?

Network Connection Settings
Windows Firewall is enabled for the connections selected below. To add exceptions for an individual connection, select it, and then click Settings:

☑ Local Area Connection

Security Logging
You can create a log file for troubleshooting purposes.

ICMP
With Internet Control Message Protocol (ICMP), the computers on a network can share error and status information.

Default Settings
To restore all Windows Firewall settings to a default state, click Restore Defaults.

Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name
☐ File and Printer Sharing
☑ Network Diagnostics for Windows XP
☑ Remote Assistance
☑ Remote Desktop
☐ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

FIGURE 22-8 Windows XP Windows Firewall choices.

The General tab is used to enable or disable the firewall. It's recommended to leave it on, but if a third-party firewall is installed, you can use this page to turn it off. Windows XP doesn't use network locations, but the Don't Allow Exceptions choice is similar to the Public network location.

You can create firewall exceptions from the Exceptions tab. It includes five predefined rules that you enable or disable by checking the box. For example, if you want to enable Remote Desktop on a computer, select the Remote Desktop check box.

If you need to allow network access to a specific program, you can click the Add Program button and select a program. Clicking the Add Port button allows you to add a rule based on a port number alone.

The Advanced tab includes several other settings. If the computer has more than one network interface card (NIC), you can enable or disable the firewall for each NIC. The Security Logging setting allows you to enable logging. If you suspect traffic is being blocked by the firewall, you can enable logging with the Security Logging settings and then view the log to verify that the traffic is blocked.

By default, the Windows Firewall blocks ICMP traffic, including ping commands. Ping is useful for troubleshooting, and you might want to enable it. The ICMP settings page gives you several options to enable traffic used by ping and other ICMP-based tools.

✓ **Quick Check**

1. **What network location should be used when connected to an unknown network?**
2. **What network location(s) supports homegroups?**

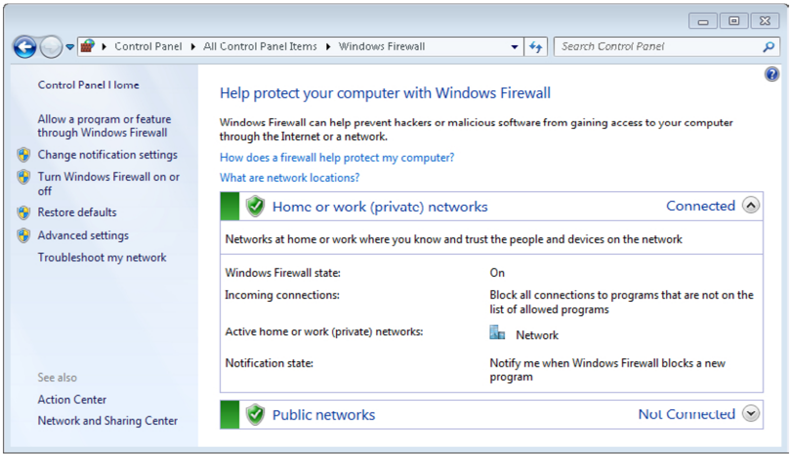
Quick Check Answers

1. **Public.**
2. **Only the Home network.**

Configuring Windows Firewall on Windows Vista and Windows 7

The Windows Firewall applet can be accessed from the Control Panel in Windows Vista and Windows 7, just as it can be accessed from Windows XP. To start it, open the Control Panel, change the view to Classic View for Windows Vista or Large Icons for Windows 7, and double-click Windows Firewall.

Figure 22-9 shows the Windows Firewall on Windows 7. It’s similar on Windows Vista, although you have more choices on Windows 7. The left pane includes several links to modify the settings, and the center pane provides information about its current configuration.



Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

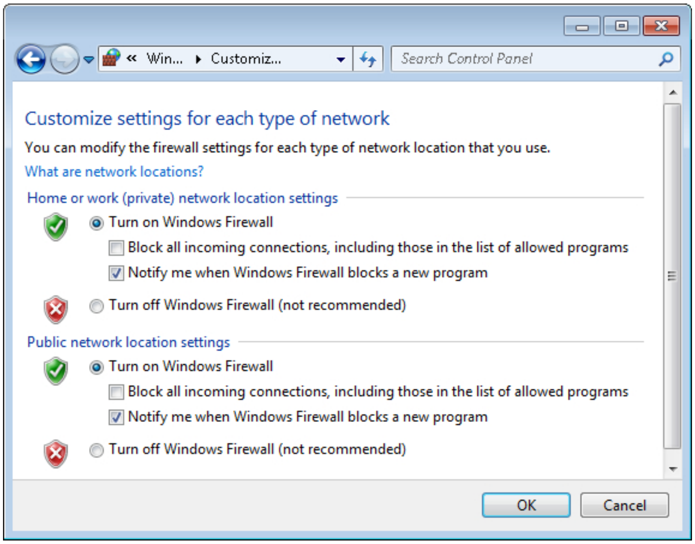
Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Network
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks — Not Connected

FIGURE 22-9 Windows 7 Windows Firewall choices.

Enable/Disable Windows Firewall

The Windows Firewall page includes a link labeled Turn Windows Firewall On Or Off. If you click it, you'll see a display similar to Figure 22-10. Notice that this gives you the option of manipulating the settings for the firewall in different network locations.



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

- ● Turn on Windows Firewall
  - ☐ Block all incoming connections, including those in the list of allowed programs
  - ☑ Notify me when Windows Firewall blocks a new program
- ○ Turn off Windows Firewall (not recommended)

Public network location settings

- ● Turn on Windows Firewall
  - ☐ Block all incoming connections, including those in the list of allowed programs
  - ☑ Notify me when Windows Firewall blocks a new program
- ○ Turn off Windows Firewall (not recommended)

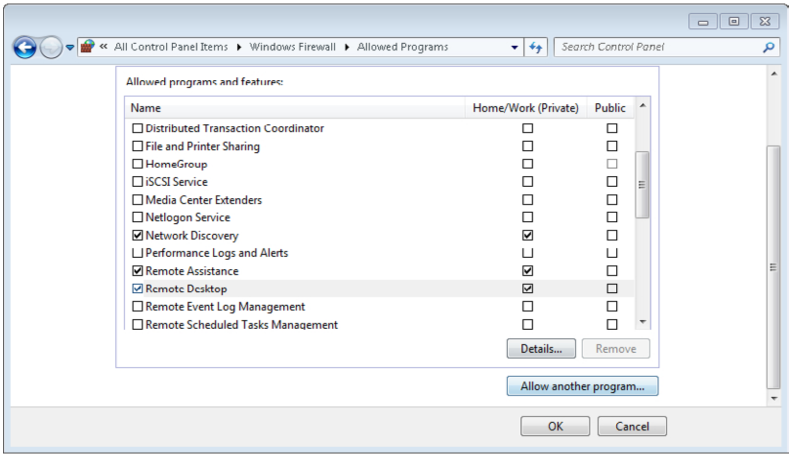
FIGURE 22-10 Enabling or disabling Windows Firewall on Windows 7.

If you suspect that the computer is infected with malware and connecting to external systems, you can select Block All Incoming Connections, Including Those In The List Of Allowed Programs. This will stop all traffic.

Enable Remote Desktop

The Windows Firewall page includes a link labeled Allow A Program Or Feature Through Windows Firewall. You can use this to enable or disable traffic by using predefined rules or by creating a new rule for specific programs or features.

For example, if you want to enable Remote Desktop, you can click the link and select Remote Desktop, as shown in Figure 22-11.


« All Control Panel Items ▸ Windows Firewall ▸ Allowed Programs
Search Control Panel

Allowed programs and features:

Name	Home/Work (Private)	Public
☐ Distributed Transaction Coordinator	☐	☐
☐ File and Printer Sharing	☐	☐
☐ HomeGroup	☐	☐
☐ iSCSI Service	☐	☐
☐ Media Center Extenders	☐	☐
☐ Netlogon Service	☐	☐
☑ Network Discovery	☑	☐
☐ Performance Logs and Alerts	☐	☐
☑ Remote Assistance	☑	☐
☑ Remote Desktop	☑	☐
☐ Remote Event Log Management	☐	☐
☐ Remote Scheduled Tasks Management	☐	☐

FIGURE 22-11 Enabling Remote Desktop on Windows 7.

Notice that it has separate selections for Home/Work and Public. As shown, Remote Desktop is enabled as long as the computer is connected to a Home or Work network location. However, if the computer is connected to a Public network location, Remote Desktop is disabled.

Windows Firewall has several predefined rules, but you can click Allow Another Program and select another program. This works similarly to how it works in Windows XP. You can't add rules based on ports from this page, but you can do so by using Windows Firewall With Advanced Security.

NOTE **REMOTE DESKTOP CONNECTIONS**

When Remote Desktop is enabled on a system, you can use Remote Desktop Connection (started with mstsc) to connect to most Windows-based systems. You cannot connect to Windows 7 Starter–based or Windows 7 Home Premium–based systems with Remote Desktop Connection. The following page has more details: *http://windows.microsoft.com/en-US/windows7/Remote-Desktop-Connection-frequently-asked-questions*.

Windows Firewall with Advanced Security

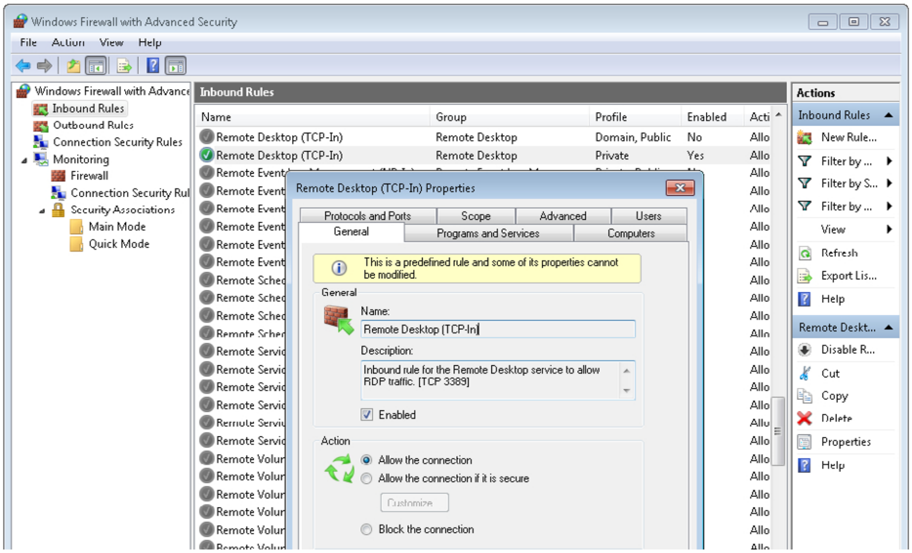
Windows Vista and Windows 7 include the Windows Firewall With Advanced Security applet. Settings in this applet apply to the Windows Firewall, but you have much more control over what you can accomplish.

You can create incoming rules for traffic coming into the computer and outgoing rules for traffic going out. The rules can be based on IP addresses, network IDs, ports, protocol IDs, or applications. You can also create rules for Home/Work network locations as Private, rules for the Public network location, and Domain rules.

To start this tool, open the Administrative Tools group in the Control Panel and double-click Windows Firewall With Advanced Security. It can also be started by entering wf.msc from the command prompt or in the Start, Search text box.

Figure 22-12 shows this tool open to the Inbound Rules section with the predefined rule for Remote Desktop open. This is the same Remote Desktop rule shown in Figure 22-11, but Windows Firewall allows you only to enable or disable it. With Advanced Security, you can view all of the properties, although many of the properties can't be changed in a predefined rule.

The Actions pane on the right in Figure 22-12 includes the New Rule link. Clicking this link with Inbound Rules selected opens the New Inbound Rule Wizard. If you select Outbound Rules and click New Rule, it opens the New Outbound Rule Wizard.



Inbound Rules

Name	Group	Profile	Enabled	Acti
Remote Desktop (TCP-In)	Remote Desktop	Domain, Public	No	Allo
Remote Desktop (TCP-In)	Remote Desktop	Private	Yes	Allo
Remote Event				Allo
Remote Event				Allo
Remote Event				Allo
Remote Event				Allo
Remote Event				Allo
Remote Event				Allo
Remote Sched				Allo
Remote Sched				Allo
Remote Sched				Allo
Remote Sched				Allo
Remote Servic				Allo
Remote Servic				Allo
Remote Servic				Allo
Remote Servic				Allo
Remote Servic				Allo
Remote Servic				Allo
Remote Volur				Allo
Remote Volur				Allo
Remote Volur				Allo
Remote Volur				Allo
Remote Volur				Allo

Remote Desktop (TCP-In) Properties

Protocols and Ports | Scope | Advanced | Users
General | Programs and Services | Computers

This is a predefined rule and some of its properties cannot be modified.

General

Name: Remote Desktop (TCP-In)

Description: Inbound rule for the Remote Desktop service to allow RDP traffic. [TCP 3389]

☑ Enabled

Action

● Allow the connection
○ Allow the connection if it is secure
Customize
○ Block the connection

FIGURE 22-12 Enabling Remote Desktop by using Windows Firewall With Advanced Security.

✓ **Quick Check**

1. How can you open the Windows Firewall?
2. What would you use to configure a port-based rule in Windows 7?

Quick Check Answers

1. Via the Control Panel.
2. Windows Firewall with Advanced Security.

Other Security Tools

In addition to Windows Firewall and Windows Firewall with Advanced Security, some other security tools are worth mentioning.

Security Center

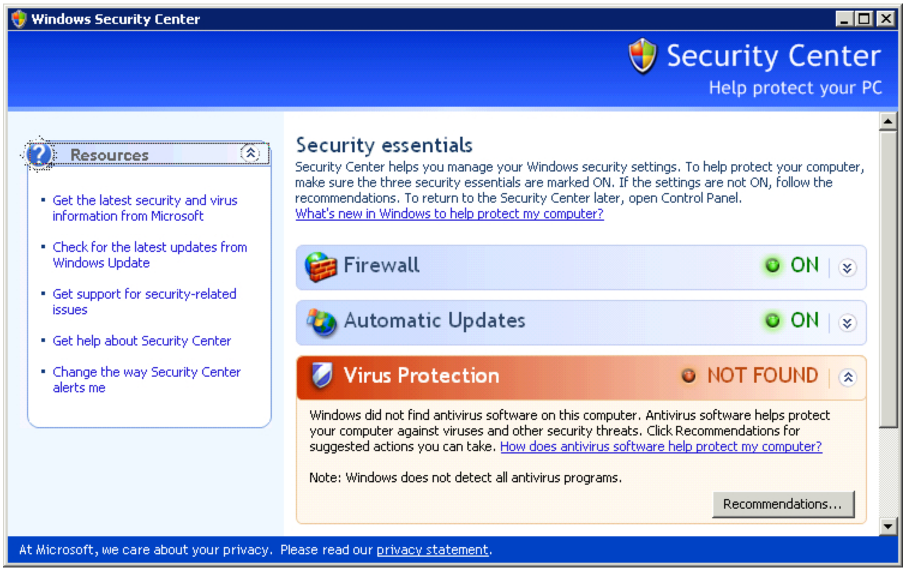
Windows XP and Windows Vista use the Security Center applet to monitor a computer's security and provide feedback to users when unsafe settings are discovered. It regularly checks the following three items:

- **Firewall.** It checks to see whether either the Windows Firewall or a third-party firewall is enabled.
- **Automatic Updates.** It checks to see whether Automatic Updates is set to Automatic. This is the recommended setting and will automatically download and install updates without requiring user interaction.
- **Virus Protection.** This check looks for an antivirus program running on the computer.

Windows Vista expands this with additional checks. It ensures that the Internet security settings used when browsing the Internet are configured at the recommended levels and ensures that User Account Control (UAC) is enabled.

By default, the Security Center provides alerts when the system fails any of these checks. You'll see a red shield with a white X next to the clock in the notification area of the taskbar. Periodically, a text balloon appears indicating that there's an issue. If you double-click it, it opens the Security Center and you can identify the problem. You can also open it from the Control Panel.

Figure 22-13 shows the Security Center in a system that doesn't have any virus protection installed. An easy fix is to download and install Microsoft Security Essentials. Chapter 26 provides information about antivirus programs, including Microsoft Security Essentials, which is available for free to home users. You can read about it and download it from here: *http://windows.microsoft.com/mse.*



- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?

Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

Note: Windows does not detect all antivirus programs.

At Microsoft, we care about your privacy. Please read our privacy statement.

FIGURE 22-13 Security Center in Windows XP.

Action Center

The Security Center is replaced by the Action Center on Windows 7–based systems. It monitors the same settings as the Security Center but also monitors additional items in both Security and Maintenance categories.

- Security categories include the firewall, Windows Update, and antivirus checks similar to the Security Center. It also checks for spyware protection, security settings in Internet Explorer, and UAC settings.
- Maintenance categories provide information about recent problems and offer solutions if one is known. They also provide feedback if a system isn't being backed up or if Windows Updates need any attention.

The Action Center adds a flag in the notification area of Windows. You can click the flag to open it, or you can open the Action Center from the Control Panel.

EXAM TIP

You can disable notifications in both the Security Center and the Action Center. For example, if you're running third-party antivirus software that isn't recognized on a Windows 7–based computer, you can click Turn Off Messages About Virus Protection and the Action Center will no longer monitor the system for antivirus software.

Netsh

The net shell (netsh) is a powerful command prompt command that you can use to view and manipulate many settings. It is a shell command, meaning that it has multiple layers, but the focus here is only on using it with the firewall.

The following code shows how you can use it to view firewall settings. After starting a command prompt, you can type in the bolded text. The unbolded text shows how the prompt changes as you type in commands.

```
C:\>netsh

netsh>firewall

netsh firewall>show state
```

You can also enter it as a single command like this:

```
C:\>netsh firewall show state
```

The output shows the status of the firewall and includes a list of ports that are currently open on the firewall. For example, if you run this on Windows XP and Remote Desktop is enabled, it will list port 3389 as being open.

If you run the command on Windows 7, you'll see a message at the end indicating that you should use advfirewall instead of firewall. It includes a link (*http://support.microsoft.com/kb/947709*) to an article that shows comparable commands using advfirewall instead of firewall.

You can use the following commands to view some settings on Windows 7, but there isn't a netsh command that reliably shows the open ports:

```
C:\>netsh
netsh>advfirewall
netsh advfirewall>show currentprofile
```

You can also enter it as a single command, like this:

```
C:\>netsh advfirewall show currentprofile
```

Appliances

Within a network, the term appliance refers to a device that has built-in capabilities for a specific purpose. Appliances within a home, such as washing machines and toasters, make life simpler. You plug them in and they work. You don't have to understand how a toaster works, but you do understand that you can put bread in and get toast out.

Similarly, network appliances have a level of complexity in how they work, but they are simple to use. You might have to do some basic configuration, but for the most part, you plug them in and they work.

Network Security Appliance

Many organizations use network security appliances to streamline security. Firewalls and proxy servers can be quite complex, with a number of settings. If they're misconfigured, they might compromise security or make it more difficult for users to accomplish their jobs.

A network security appliance is a hardware device that runs specialized security software and simplifies installation and maintenance. Customers can plug them in, and they provide a wide range of security without requiring in-depth knowledge of their inner workings. Some of the services that a network security appliance can provide include the following:

- **Firewalls.** At their core, they are designed to control what traffic is allowed in or out of a network.
- **Proxy server content filtering.** Many include the same content-filtering capabilities of a proxy server. They can filter traffic based on URLs and block access to malicious websites.
- **Malicious software (malware) filtering.** They filter all traffic and can detect and block malicious software.
- **Spam filtering.** Many include the ability to detect and block spam before it reaches the user.
- **Intrusion detection systems (IDSs).** These monitor traffic and can detect attacks. They include a notification system to provide alerts when an attack is detected.
- **Intrusion prevention systems (IPSs).** These are an extension of IDSs and can prevent attacks. They are placed in line with the traffic to block malicious traffic before it reaches the network.
- **Network access control (NAC).** Clients are inspected to ensure that they meet certain requirements before access is granted. For example, a virtual private network (VPN) client might be inspected to ensure that it has up-to-date antivirus software before it is granted full VPN access.

NOTE **UNIFIED THREAT MANAGEMENT (UTM)**

Network security appliances that provide multiple security capabilities are commonly referred to as Unified Threat Management (UTM) solutions.

Some companies, such as Check Point Software, sell UTM solutions using their own hardware and software. Other companies bundle and configure someone else's software on an appliance. For example, nAppliance has a range of network appliances that use the Microsoft Forefront Edge Security suite.

Internet Security Services

Some companies sell Internet security services that an organization can use without purchasing any hardware or configuring software. These are very useful for SOHOs and small businesses that don't have the resources to purchase and maintain their own security appliance.

For example, Online Spam Solutions sells an email-filtering subscription service that blocks spam and malware. When you subscribe, your email is routed through their servers, where it is scanned and filtered before being sent to you. They have all the hardware, software, and supporting staff to maintain the service. You only have to authorize the payment.

Internet Appliance

An Internet appliance is a specialized device used for accessing the Internet by a single person. People use it to browse the Internet or access email, but it isn't designed to do much more.

EXAM TIP

Internet appliance **is specifically listed in the CompTIA objectives, while other terms, such as network security appliance and Internet security services, aren't listed. An Internet appliance is not related to security, but because the term is so rarely used, people sometimes confuse it with a network security appliance or as an Internet security service.**

Some of the devices, such as the Sony eVilla, use full-size monitors with a small form-factor computer. Other devices, such as the Nokia N810, are small handheld devices with a touch screen or keyboard. The features of these devices have been integrated into many mobile devices, such as smartphones and tablets, so you'll rarely hear the term anymore.

✓ **Quick Check**

1. **How will a user know whether the Windows Firewall is disabled on Windows 7?**
2. **What command prompt command can you use to view firewall settings?**

Quick Check Answers

1. **Alerts from the Action Center remind the user.**
2. **Netsh.**

Chapter Summary

- Firewalls are classified as network-based or host-based firewalls. A network-based firewall controls traffic in and out of a network. A host-based firewall controls traffic in and out of a single computer.
- Firewalls use an implicit deny philosophy, blocking all traffic unless there is an explicit rule to allow it. Rules that allow traffic are called exceptions.
- A basic packet-filtering firewall can filter traffic based on IP addresses, ports, and protocol IDs. Most firewalls can filter traffic by using advanced methods.
- Port forwarding is configured on a router or firewall to allow Internet clients to access internal resources. For example, incoming traffic using port 3389 can be forwarded to a specific system that has Remote Desktop enabled.
- Port triggering is used to open an incoming port when a specific outgoing port is used. For example, if an internal system sends outgoing traffic by using port 6789, the port trigger on the firewall could be configured to open incoming port 9876.
- Proxy servers can reduce Internet bandwidth usage with caching and control Internet access with content filtering. Malware has been known to modify a web browser’s proxy server settings.
- Windows Firewall is available in Windows XP, Windows Vista, and Windows 7. Windows Firewall with Advanced Security provides access to advanced firewall settings in Windows Vista and Windows 7.
- Windows Vista and Windows 7 use network locations. Home and Work network locations are considered private networks and have fewer firewall restrictions.
- The Public network location is used for unknown or public networks and has the most stringent firewall control. Network discovery is disabled in the public network location, making it more difficult for computers to see each other.
- All of the Windows Firewall versions include several predefined rules that can be enabled or disabled. You can also create additional rules based on ports or applications. Windows Firewall With Advanced Security provides the most options.
- The Security Center in Windows XP and Windows Vista performs basic security checks. Users are alerted if these settings are configured in a way that makes their computer less safe. The Action Center in Windows 7 replaces the Security Center and includes additional checks.
- Network security appliances that provide a bundled security solution in an easy-to-use device are available.

Chapter Review

Use the following questions to test your knowledge of the information in this chapter. The answers to these questions, and the explanations of why each answer choice is correct or incorrect, are located in the "Answers" section at the end of this chapter.

1. You are hosting a website on your home network, and you want to be able to access it when you're away from home. Of the following choices, what can you use to meet your goal?

   A. Port forwarding

   B. Port triggering

   C. A proxy server

   D. A Public network location

2. You successfully removed a virus from a user's computer, and a virus scan shows that it is clean. However, the user no longer has Internet access. What is the most likely reason?

   A. The Windows Firewall is enabled.

   B. The proxy settings for the browser are incorrect.

   C. Port forwarding has been disabled.

   D. The computer has been reconfigured for the Home location.

3. A user has configured four Windows 7 Professional–based computers in a SOHO but has not been able to get homegroups to work. Of the following choices, what is the most likely reason?

   A. Homegroups are not supported on Windows 7 Professional.

   B. The Windows Firewall is enabled on the computers.

   C. The Network location is set to Home.

   D. The Network location is set to Work.

4. You just connected to a wireless network in a coffee shop and plan on doing some work. You're prompted to choose a network location. What should you select?

   A. Home

   B. Work

   C. Public

   D. Private

5. You recently installed a program on a Windows 7–based computer that requires port 4545 to be opened on the firewall. What program would you use to configure it?

   A. Windows Firewall

   B. Remote Desktop

   C. Network Discovery

   D. Windows Firewall With Advanced Security

6. You are helping a small business owner increase network security. The owner is willing to purchase a product to protect against malicious Internet traffic but wants to minimize maintenance. What would you suggest to provide the greatest security?

   A. Install a router.

   B. Install a firewall.

   C. Install a network security appliance.

   D. Install an Internet appliance.

Answers

This section contains the answers to the chapter review questions in this chapter.

1. **Correct Answer:** A
   - **A. Correct:** Port forwarding can forward requests from the Internet to an internal computer.
   - **B. Incorrect:** Port triggering supports internal clients by opening an incoming port when an internal client uses a specific outgoing port.
   - **C. Incorrect:** A proxy server provides centralized Internet access for internal clients.
   - **D. Incorrect:** The Public network location blocks most network access and wouldn't help in this situation.
2. **Correct Answer:** B
   - **A. Incorrect:** Users can access the Internet with the firewall enabled.
   - **B. Correct:** Some malware modifies proxy settings, blocking Internet access.
   - **C. Incorrect:** Port forwarding is not used to access the Internet from an internal computer.
   - **D. Incorrect:** The Home network location would not block Internet access.
3. **Correct Answer:** D
   - **A. Incorrect:** You can create homegroups on any edition of Windows 7 except Windows 7 Starter or Home Basic.
   - **B. Incorrect:** Homegroups can work with the Windows firewall enabled.
   - **C. Incorrect:** Homegroups are enabled in the Home network location, so this wouldn't block homegroups.
   - **D. Correct:** Homegroups are disabled in the Work and Public network locations.
4. **Correct Answer:** C
   - **A. Incorrect:** A home network is a private network.
   - **B. Incorrect:** A work network is a public network.
   - **C. Correct:** A coffee shop network is in a public place, and the Public network location should be selected.
   - **D. Incorrect:** Private isn't a choice, but both Home and Work networks are considered private networks.

5. **Correct Answer:** D
   A. **Incorrect:** Windows Firewall on Windows 7 doesn’t give you the option of creating rules based on ports.
   B. **Incorrect:** Remote Desktop is used to connect to remote systems, but it isn’t used to open firewall ports.
   C. **Incorrect:** Network Discovery isn’t a program but is instead a feature used to make it easier for computers to locate each other when it’s enabled.
   D. **Correct:** Windows Firewall With Advanced Security includes the ability to create rules based on ports.
6. **Correct Answer:** C
   A. **Incorrect:** A router provides only basic protection.
   B. **Incorrect:** A firewall provides protection but isn’t as effective as a network security appliance.
   C. **Correct:** A network security appliance provides a bundled solution, and many can be set up and maintained with minimal effort.
   D. **Incorrect:** An Internet appliance is a single-user device used for web browsing and email only.