11. When you request a Web page, which port does the Web server use to send you the page?
    a. 80
    b. 443
    c. one higher than 1023
    d. one lower than 1023

12. Stateless packet filters are more secure than stateful packet filters because they do not contain a state table that can be exploited by an attacker. True or False?

13. A socket is a combination of a(n) _____ and a(n) _____.
    a. NetBIOS name, port number
    b. port number, MAC address
    c. MAC address, IP address
    d. IP address, port number

14. The Windows RPC service works like the UNIX _____ service.
    a. mountd
    b. Portmapper
    c. QOTD
    d. INFS

15. Which port is used for name/address resolution?
    a. 20
    b. 53
    c. 80
    d. 110

Hands-On Projects

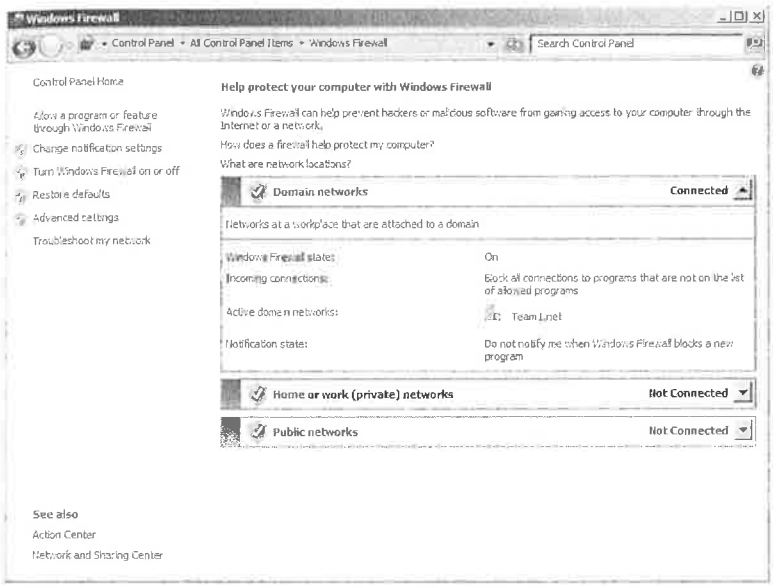
Hands-On Project 9-1: Exploring the Advanced Settings of Windows Firewall

Time Required: 15 minutes

Objective: Examine the advanced settings of Windows Firewall.

Description: The Windows Firewall in Windows 7 and Windows Server 2008 R2 has three profiles. From most restrictive to least restrictive, they are Public, Private, and Domain. Only one profile can be active at a time. The Windows Firewall has two interfaces: The interface in the Control Panel is appropriate for inexperienced users, and the advanced settings are appropriate for experienced users and technical staff.

1. If you completed the Chapter 1 hands-on projects, you installed ZoneAlarm on your Windows 7 system. Log on to the Windows 7 system, click **Start**, click **Control Panel**, click **Programs and Features**, and uninstall ZoneAlarm.
2. Click **Start**, click **Control Panel**, click the **View by** list box in the upper-right corner, and click **Small icons**. Click **Windows Firewall**.
3. Log on to the Windows Server 2008 system, and repeat Step 2 to open **Windows Firewall**.
4. On both computers, the Domain networks profile should be listed as connected. The section should be expanded and show that the Windows Firewall is on and that the Active domain network is your domain. Your results should be similar to those in Figure 9-10.



Used with permission of Microsoft Corporation

Figure 9-10 Windows Firewall on a domain computer

5. On both computers, click **Advanced settings**. As usual, when attempting administrative tasks in Windows 7, you need to provide domain administrator credentials when prompted.
6. The Overview section of the Windows Firewall with Advanced Security window should show that the Domain profile is active. The Private and Public profiles show that Windows Firewall is on, but these profiles are not active. In the middle frame, scroll down and click **Windows Firewall Properties**. Here, the first three tabs allow you to customize settings for each of the three profiles. On the Domain Profile tab, click the **Customize** button in the Settings section. In the Firewall settings section, select **Yes** from the Display a notification list box, and click **OK**. In the Logging section, click **Customize**. Note the location of the firewall log. Click **Start**, click **Computer**, and find the folder on the C: drive that holds the log files. The folder should be empty.

7. Return to the Customize Logging Settings for the Domain Profile window, set both the Log dropped packets and Log successful connections list boxes to **Yes**, and click **OK**. Click **OK** again in the next window.
8. In the left frame of the Windows Firewall with Advanced Security window, click **Inbound Rules**. Compare the differences between the rules listed in Windows Server 2008 and Windows 7. Double-click an inbound rule in the middle pane that is labeled with a green checkmark; notice that the Enabled box is checked. Click **Cancel**, and then double-click an inbound rule labeled with a gray icon; note that the Enabled box is not checked. Click **Cancel**.
9. Leave your systems running for the next project.

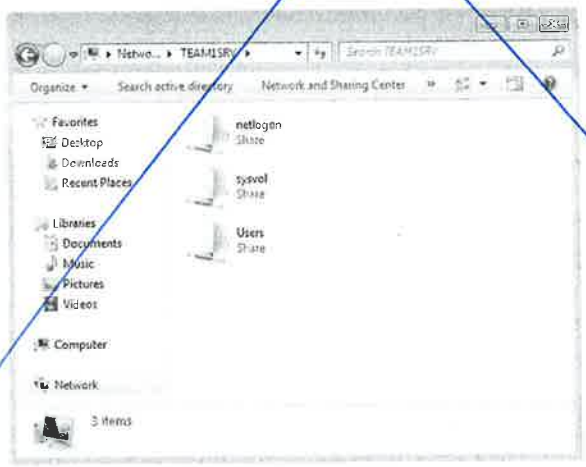
Hands-On Project 9-2: Enforcing IPsec Policies

Time Required: 40 minutes

Objective: Increase security for your domain by enforcing encryption and authentication.

Description: While IPsec is commonly used in VPN connections, as you learned in Chapter 5, it can also be used to authenticate and encrypt transmissions between computers on a LAN. A common example pertains to the critical security issue of data being transferred from a publicly accessible Web server on the DMZ to a database server on the trusted internal network that is not publicly accessible. This data often contains highly sensitive information such as customers' billing information; transmitting such information without encryption would be negligent for e-commerce companies. In this project, you require IPsec communications between computers in your domain.

1. Log on to the Windows 7 system as the Team*x* domain user administrator, where *x* represents the number assigned by your instructor.
2. Click **Start**, click **Control Panel**, click **Network and Internet**, and click **Network and Sharing Center**. Click the **Team*x*.net** icon to display the network computers. You should see both TEAM*x*CLIENT and TEAM*x*SRV. Double-click **TEAM*x*SRV**; you should see the default shares (see Figure 9-11).



Used with permission of Microsoft Corporation

Figure 9-11 TEAM*x*SRV's default shares

Rule	Source IP	Destination IP	Protocol	Action	Track	Comments
1	Any	210.100.101.1	Any	Deny	Alert	Blocks access to firewall
2	210.100.101.0 to 210.100.101.255	Any	S-HTTP	Deny	None	Blocks network access to Web server using S-HTTP
3	210.100.101.0 to 210.100.101.255	Any	HTTP, S-HTTP	Allow	None	Allows network access to all Web sites
4	Any	210.100.101.2	HTTP	Allow	Log	Allows all computers to access the Web server using HTTP
5	210.100.101.0 to 210.100.101.255	210.100.101.3	UDP	Allow	Log	Enables network to make queries to DNS server
6	210.100.101.3	Any except 210.100.101.0 to 210.100.101.255	TCP	Allow	Log	Enables DNS server to make lookups on the Internet but not in the network
7	210.100.101.0 to 210.100.101.255	210.100.101.5	TCP	Allow	None	Allows network access to POP3 server
8	Any	210.100.101.4	TCP	Allow	None	Allows any computer to access the SMTP server
9	Any	Any	Any	Deny	Log	Cleanup rule

Table 9-14 Firewall rule base

You have noted some questions that you need to address as you consider modifying the firewall rule base:

- Which rules cover the same sort of communication?
- Which rules are too far down the list and should be moved up?
- Which rules give the firewall more work than necessary? (*Hint:* Look in the Track column.)

On a separate piece of paper, create a rule base table. Using as few rows as possible, write a new rule base that addresses the questions in the preceding steps.

Case Project 9-2: Recommending a Software Firewall

Now that you have completed the new rule base for the law firm, as described in Case Project 9-1, your next task is to recommend a software firewall to install on the firm's workstations. Your supervisor wants you to consider both commercial and free products. Research both kinds of software firewalls, choose one product from each category, and then prepare a report that presents your choices and explains the advantages and disadvantages of each product.

15. Click **Define deployment options**. In the welcome window, click **Next**. In the Microsoft Update Setup window, click **Use the Microsoft Update service to check for updates (recommended)**, and click **Next**.
16. In the Forefront TMG Protection Features Settings window, verify that **Activate complementary license and enable NIS** is selected in the Network Inspection System (NIS) License box. Verify that the Web Protection License is set to **Activate evaluation license** and that **enable Web Protection** is selected. Verify that **Enable Malware Inspection** is checked, and click **Next**.
17. In the NIS Signature Update Settings window, click **Next**. In the Customer Feedback window, click **No, I don't want to participate**, and click **Next**. In the Microsoft Telemetry Reporting Service window, click the **None** option button. No information is sent to Microsoft. Click **Next**, and then click **Finish**. In the Getting Started Wizard window, uncheck **Run the Web Access wizard**, and click **Close**.
18. Leave your systems running for future projects.

Hands-On Project 10-2: Installing Apache Web Server

Time Required: 10 minutes

Objective: Install Apache.

Description: The open-source Apache program is the most popular Web server in the world. In fact, the most popular current Web server installation is the Apache program running on a Linux operating system. In this project, you install Apache in the Linux system you created in an earlier project.

To install Apache, the Linux system must be connected to the Internet.

1. Start and log on to the Linux system you installed in Hands-On Project 8-1.
2. Click the **Dash home** icon on the left side of the desktop.
3. In the search box, type **terminal**, and press **Enter**.
4. At the command prompt, type **sudo apt-get install apache2**, and press **Enter**.
5. Enter the administrator's password at the prompt.
6. If you are asked whether you want to continue, type **Y**, and press **Enter**.
7. When the installation is complete, click the **Firefox Web Browser** icon on the left side of the desktop, type **http://127.0.0.1** in the URL address box, and press **Enter**. If the installation was successful, you should see a Web page that reads "It works! This is the default web page for this server. The web server software is running but no content has been added, yet."

8. Click the **System Settings** icon on the left side of the desktop. Click the **Network** icon. Click **Configure**, and click the **IPv4 Settings** tab. Set the Method list box to **Manual**. Click **Add**, and then configure the IP address as **192.168.1.100**, the netmask as **255.255.255.0**, and the default gateway as **192.168.1.110**. Click **Save**. In the upper-right part of the Wired window, toggle the slider bar to off and then back to on. This action reinitializes the network interface card and displays the new IP address. Close all windows.
9. Leave your system on for the next activity.

Hands-On Project 10-3: Configuring a Web Access Policy

Time Required: 20 minutes

Objective: Configure the basic proxy server functions of TMG.

Description: After installation, TMG blocks all traffic by default. To allow internal clients to access the Internet, a Web access policy modification is required. (In these projects, the Linux Web server functions as the Internet.) In this project, you perform the initial configurations so that the internal Web client, Windows 7, can access the Linux Web server.

1. Verify that the four computers are configured as shown in Table 10-3. Figure 10-20 demonstrates the topology of the lab network.

Computer	IP address	Subnet mask	Default gateway	DNS
Windows 7	10.0.0.110	255.0.0.0	10.0.0.111	10.0.0.125
Windows Server 2008	10.0.0.125	255.0.0.0	10.0.0.111	10.0.0.125
TMG				
Inside	10.0.0.111	255.0.0.0	None	10.0.0.125
Outside	192.168.1.110	255.255.255.0	None	10.0.0.125
Linux	192.168.1.100	255.255.255.0	192.168.1.110	None

Table 10-3 Network configuration

2. Test Web access by opening a Web browser in both the Windows Server 2008 domain controller and the Windows 7 system and then attempting to access http://192.168.1.100. Both attempts should be unsuccessful because the systems are on a different IP segment and the TMG proxy server/firewall is not configured to pass traffic. Repeat this test from the TMG system. This attempt should be successful because TMG has an interface on the same IP segment as the Linux Web server.
3. Verify connectivity by pinging Windows 7 from Windows Server 2008 and by pinging TMG's inside address from both systems. These pings should be successful.
4. In TMG, click **Start**, click **All Programs**, click **Microsoft Forefront TMG**, and click **Forefront TMG Management**.

password, and click **OK**. In the Locations window, expand **Entire Directory**, select **Team*x*.net**, and click **OK**. In the Enter the object names to select text box, type **cjack**, and click **Check Names**. Captain Jack's name should appear underlined. Click **OK**, click **Next**, and click **Finish**. In the Add Users window, select **Web Abusers**, click **Add**, click **Close**, and click **Next**. Click **Finish**. Click **Apply**. In the Change description text box, type **Web Abusers created and enabled**. Click **Apply**, and click **OK**.

9. From the Windows 7 system, log on to the domain as Captain Jack. Open a Web browser and attempt to access the Linux Web server, as you did in Step 15 of Hands-On Project 10-3. Your attempt should fail. If your systems were connected to the Internet, access to Facebook and FTP sites would also be denied.
10. Log off the Windows 7 system, and log on as another domain user. Attempt to access the Linux Web server again. This attempt should succeed.
11. Log off all computers.

Case Projects

Case Project 10-1: Firewall Selection Parameters

You work for a network consulting firm and you have been asked to create a guide for firewall selection. Create an outline for a section that lists and defines the most important parameters of firewall functions, such as throughput.

Case Project 10-2: Proxy Server Parameters

You are still working on your guide for firewall selection from the previous case project. Create an outline for a section that lists and defines the most important functional parameters of proxy servers.