Chapter Three

Configuring Windows Security Features

This chapter covers the following objectives:

- Configure and troubleshoot User Account Control.
- Configure Windows Defender.
- Configure Dynamic Security for Internet Explorer 7.
- Configure Security Settings in Windows Firewall.
1. Which of the following are the types of user accounts in Windows Vista?
   - A. Administrator
   - B. Guest
   - C. Power User
   - D. Standard User
   - E. Limited

2. Which of the following user accounts should you create for normal Windows Vista users?
   - A. Standard
   - B. Administrator
   - C. Limited
   - D. Guest

3. Which of the following user accounts are created by default on a Windows Vista computer during installation?
   - A. Administrator
   - B. Initial User
   - C. Guest
   - D. Backup Operator

4. What is the level of privilege given to the Initial User account after installation of Windows Vista?
   - A. Guest
   - B. Standard User
   - C. Limited User
   - D. Administrator

5. You have enabled the built-in Administrator account on a Windows Vista computer so that you can install devices and configure system settings. It will take you a couple of days before the configuration settings are complete. What should you do to ensure the security of the account?
   - A. Enable the account only when you need it.
   - B. Turn off UAC for the account.
   - C. Rename the account.
   - D. Delete the account when you are done.
6. You have created a Standard User account for two more persons in the office with whom you share the Windows Vista computer. One of these persons has left the office. What should you do with his user account?
   - A. Delete the account.
   - B. Disable the account.
   - C. Rename the account.
   - D. Change the account password.

7. Which of the following utilities can be used to create local user accounts on a Windows Vista computer?
   - A. Local Users and Groups
   - B. Active Directory Users and Computers
   - C. User Accounts
   - D. User Manager

8. You want to create some domain user accounts on a Windows Vista computer that is a part of Windows Server 2003 Active Directory domain. When you open the Administrative Tools folder in the Control Panel, you do not find any link for the Active Directory Users and Computers. What do you need to install to create domain user accounts on this computer?
   - A. Local Users and Groups snap-in
   - B. User Accounts utility
   - C. Windows Server Administration Tools
   - D. User Manager

9. Which of the following dialog boxes displays when a user attempts to install an application on a Windows Vista computer?
   - A. Application Authentication Code
   - B. Application Access Control
   - C. User Account Control
   - D. Access Control List
10. For which of the following actions will Windows Vista display the User Account Control dialog box?
   - A. When a user tries to install an application
   - B. When an administrator tries to perform a system task
   - C. When a user tries to run a Microsoft Office application
   - D. When a user tries to run an application that is not digitally signed
   - E. When an administrator tries to run an application that is not digitally signed

11. An administrator is logged on as a standard user on a Windows Vista computer. As soon as he tries to open the Device Manager utility, the UAC dialog box is displayed. What should the administrator do?
   - A. Log off and log on with the administrator username and password.
   - B. Just click the Continue button.
   - C. Provide the administrator username and password.
   - D. Restart the computer and log on as administrator.

12. Jim has learned about User Account Control in Windows Vista, which helps prevent damage to the system by warning a user or an administrator when some application is installed or when an administrative action is performed. Jim is an administrator on his Windows Vista Home Premium edition computer and tries to start the Computer Management console but the UAC warning does not appear. What could be the reason?
   - A. UAC is turned off on the computer.
   - B. The computer hardware does not support the UAC feature.
   - C. UAC is not supported on Home Premium edition.
   - D. Jim must log on as administrator to get the UAC warning.

13. In which of the following situations will the UAC warning not appear on a Windows Vista computer?
   - A. When a user performs a nonadmin task
   - B. When an administrator performs a nonadmin task
   - C. When a user or administrator wants to change system time
   - D. When a user or administrator tries to run Computer Management console
   - E. When UAC is turned off
14. Karen is logged on as an administrator to her Windows Vista computer on which the UAC is turned on. She is attempting to install an application that is not digitally signed. Which of the following UAC warning messages will appear in the UAC dialog box?

- A. Type an Administrator Password and Click OK
- B. Windows Needs Your Permission to Continue
- C. An Unidentified Program Wants Access to Your Computer
- D. A Program Needs Your Permission to Continue

15. Mark has not changed the UAC settings on his Windows Vista computer. He has two accounts on this computer: an Administrator account and a Standard User account. He is trying to modify Windows Firewall settings on his computer, but the system won’t allow him to do so. He is not allowed even when he supplies his administrative credentials. What should he do?

- A. Turn off UAC and turn it on again.
- B. Log off and log on as administrator.
- C. Restart the computer and log on as administrator.
- D. Reinstall corrupt files related to UAC.

16. You are the system administrator for Acme.com. Acme.com has received a new accounting application that you want to test on a Windows Vista computer. The application is digitally signed, and you are logged on as an administrator. When you start the installation program, a UAC warning appears. Which button should you click?

- A. Allow
- B. Permit
- C. Cancel
- D. Continue

17. What happens to the Windows Vista desktop when the UAC warning appears?

- A. Windows takes a screen shot of the desktop and switches to Secure Desktop.
- B. The computer goes into Sleep mode while the UAC dialog box is displayed.
- C. Windows closes all running applications while the UAC dialog box is displayed.
- D. Windows takes a snapshot of the running applications, and you must click the End Process button to continue working.
18. You are the system administrator for Acme.com. Acme.com has a small Active Directory–based network that includes both Windows XP and Windows Vista desktops. Most of the users work in a secure environment where data security is of prime concern. The network consists of wired and wireless desktops. On which of the following computers should you disable UAC?

- B. On all computers that are on wireless network.
- C. On all computers that are on wired network.
- D. UAC should not be turned off on any computer.

19. You have been hired by Acme.com to work as a help desk technician by Acme.com. The company is in the process of upgrading its desktops from Windows XP to Windows Vista. One of the executives of the company has asked you to enable the Admin Approval Mode on all Windows Vista desktops. What happens when the Admin Approval Mode is enabled?

- A. No unauthorized application can be installed.
- B. Unauthorized applications can be installed only by standard users.
- C. Administrators need to confirm installation of unauthorized applications.
- D. It allows users to run applications with administrator's written approval.

20. A user is trying to run an application on a Windows Vista computer. This application was running well on a Windows XP computer. The UAC is not letting the user run the application without administrative credentials. What should the user do?

- A. Digitally sign the application.
- B. Ask the administrator for approval.
- C. Disable User Account Control.
- D. Log on as administrator.
21. A user is trying to install an application on a Windows Vista computer. This application installed without a problem well on a Windows XP computer. The UAC is not letting the user install the application without administrative credentials. The user calls in the administrator, who supplies his credentials, and the application starts installing. How does the system handle two user accounts at a time?

- A. Both the user and the administrator remain logged on, and the user can keep working with any of the accounts.
- B. The user is logged off as soon as the administrator supplied his credentials.
- C. The Administrator account is logged off as soon as the application installation completes.
- D. The user must now log off and log on using his own credentials.

22. You need to turn off User Account Control on the Windows Vista desktop of one of the IT managers of your company. You have opened the Windows Security Center in the Control Panel. Which link would you use?

- A. Windows Defender
- B. Windows Firewall
- C. Internet Options
- D. Other Security Settings

23. You are the system administrator of a medium-sized organization, Acme.com. All desktops have been upgraded to Windows Vista, but one of the applications is still required to run in Windows XP mode that needs elevated privileges. How should you configure these computers so that UAC does not bother the users?

- A. Turn off UAC on all Windows Vista computers.
- B. Run the Program Compatibility Wizard to configure the applications to run in Legacy mode.
- C. Configure the system settings so that applications run using the built-in Administrator account.
- D. Ask the users to run the application using the administrative privileges.
24. Amy is working on creating a technical manual for a network device that has been certified with the Windows Vista logo. She needs to include some snapshots of the screen in the manual showing the UAC dialog box when the device driver is installed. She takes the screenshot when the UAC is displayed, but nothing is copied and pasted in her graphics application. Amy is currently logged on as a standard user. What should she do?

○ A. Turn off the UAC when taking a screenshot.
○ B. Log off and log on as administrator.
○ C. Disable the Secure Desktop.
○ D. Supply her administrator password when the UAC is displayed.

25. Which of the following methods would you use to configure UAC settings on a Windows Vista computer working in a workgroup environment?

○ A. Local Security Policies
○ B. Windows Firewall
○ C. Windows Defender
○ D. User Accounts

26. You are configuring local security policies on a Windows Vista computer. The objective is to stop the UAC prompt for all standard users to supply administrative credentials when they want to change system settings or install any device. Which of the following UAC policies would you enable?

○ A. Admin Approval Mode for the Built-in Administrator Account
○ B. Behavior of the Elevation Prompt for Administrators in Approval Mode Prompt for Consent
○ C. Behavior of the Elevation Prompt for Standard Users to Automatically Deny Elevation Requests
○ D. Detect Application Installation and Prompt for Elevation
27. A Windows Vista computer working in a workgroup environment has all its default settings, including the UAC security policies. You want to configure UAC policies on this computer so that the UAC dialog box only prompts for consent but does not ask for credentials when an administrator performs a system task. Which of the following policies would you enable?

- A. Admin Approval Mode for the Built-in Administrator Account
- B. Behavior of the Elevation Prompt for Administrators in Approval Mode Prompt for Consent
- C. Behavior of the Elevation Prompt for Administrators in Approval Mode Prompt for Credentials
- D. Behavior of the Elevation Prompt for Administrators in Approval Mode Elevate Without Prompting

28. A Windows Vista computer working in a workgroup environment has all its default settings, including the UAC security policies. You want to configure UAC policies on this computer so that the UAC is disabled for all users. Which of the following policies would you configure?

- A. Admin Approval Mode for the Built-in Administrator Account Enabled
- B. Admin Approval Mode for the Built-in Administrator Account Disabled
- C. Run All Administrators in Admin Approval Mode Enabled
- D. Run All Administrators in Admin Approval Mode Disabled

29. A Windows Vista computer working in a workgroup environment has all its default settings, including the UAC security policies. Which of the following UAC policies are enabled by default?

- A. Admin Approval Mode for the Built-in Administrator Account
- B. Switch to Secure Desktop When Prompting for Elevation
- C. Run All Administrators in Admin Approval Mode
- D. Only Elevate Executables Which are Signed and Validated
30. You need to configure a Windows Vista desktop so that it remains secure from spyware and other malware applications. Which of the following utilities would you configure?
   - A. Windows Firewall
   - B. Windows Defender
   - C. User Account Control
   - D. BitLocker Drive Encryption

31. What does Windows Defender use to detect malicious applications?
   - A. Spyware definitions
   - B. Heuristic algorithms
   - C. Risk identification
   - D. Microsoft SpyNet

32. Which of the following actions can potentially harm your Windows Vista computer?
   - A. Software installation
   - B. Downloads from the Internet
   - C. Use of instant messaging
   - D. CDs and DVDs borrowed from friends

33. Your Windows Vista computer is always connected to the Internet. Windows Defender is configured with default settings on this computer. You receive a real-time Windows Defender alert that an application is attempting to install on your computer. Which of the following actions can you take using Windows Defender action options?
   - A. Allow
   - B. Ignore
   - C. Deny
   - D. Quarantine
   - E. Remove
   - F. Always Allow
34. You have downloaded a photo-editing application from the Internet and want to install it on your Windows Vista computer, but Windows Defender displays a severe alert message. You know that the application is safe to install and will not damage the computer or change any security settings. How should you configure Windows Defender actions so that it does not prevent installation or running the application after installation but always displays an alert when the application is running?
   - Always Allow
   - Remove
   - Quarantine
   - Ignore

35. One of the Windows Vista computers in your office has been configured to perform Windows Defender scanning during the weekends. One Monday morning, you find that an application has been removed by Windows Defender. From where can you restore the application?
   - From the original setup media
   - SpyNet Community
   - Quarantined Items
   - Software Explorer

36. You are configuring Windows Defender on one of the Windows Vista computers that will be allocated to a company executive. Which of the following categories can you select in the Software Explorer window?
   - Programs that are currently running
   - Programs that are run from the network
   - Programs that are bundled with the operating system
   - Programs that automatically start with system startup
   - List of Windows Sockets service providers
37. Your Windows Vista computer remains connected to the Internet. Recently, you have noticed that it is always running an application that you did not install. Windows Defender is not able to detect the application so far. You suspect that it might be a spyware application. How can you use Windows Defender to confirm this?

❍ A. Check the Quarantined Items link in Windows Defender.
❍ B. Check the Auto-Start Programs list in Software Explorer.
❍ C. Check the Network Connected Programs in Software Explorer.
❍ D. Check with the SpyNet community.

38. Your Windows Vista computer is configured with default settings for the Windows Defender to detect and display alerts about harmful programs. What will Windows Defender do with an application for which the alert level is Medium?

❍ A. Remove the application immediately
❍ B. Provide options to review, block, or remove
❍ C. Ignore the application and allow it to run
❍ D. Block the application until you manually run it

39. Your Windows Vista computer is configured with default settings for the Windows Defender to detect and display alerts about harmful programs. What level of alert will display if an application is rated as a virus or a Trojan horse?

❍ A. Severe
❍ B. High
❍ C. Medium
❍ D. Low

40. You are configuring Windows Defender to take appropriate actions depending on the alert level of applications with malicious code. For which of the following alert levels can you not configure an action?

❍ A. Low alert
❍ B. Medium alert
❍ C. High alert
❍ D. Severe alert
41. You suspect that some malicious application got downloaded and installed on your computer when you accidentally clicked a link on a website. You know that Windows Defender will detect the application when it scans the computer at midnight. You want to immediately detect the application and remove it using Windows Defender. Which of the following scanning options would you use?
   ○ A. Quick Scan
   ○ B. Custom Scan
   ○ C. Full System Scan
   ○ D. Scan Selected Drives and Folders

42. You share your Windows Vista computer with two other users in the office. You suspect that one of the other users keeps on downloading and installing unwanted programs on the computer. You want to use Windows Defender to search and remove any undesired programs that have been configured to start automatically with system startup. When you open Software Explorer, you cannot see any applications except the one that you normally use. What should you do to view all programs installed on the computer?
   ○ A. Click the Refresh button.
   ○ B. Click the check box for Show for All Users.
   ○ C. Change the category from Startup Programs to Network Connected Programs.
   ○ D. Click the Using Software Explorer link.

43. While working on your Windows Vista computer, you open Internet Explorer to check latest news from a newspaper website. Suddenly, another web page opens that seems to be the website of a bank. You are asked to fill out a form on the web page so that the bank may include your information for a big contest prize. You suspect the intentions of the website and that Internet Explorer is not configured to handle these types of websites appropriately. Which of the security features is not configured in Internet Explorer?
   ○ A. Parental Controls
   ○ B. Phishing Filter
   ○ C. Windows Defender
   ○ D. Windows Firewall
44. You have opened Internet Explorer for the first time after installing Windows Vista on your computer. You do not want Internet Explorer to report suspicious websites to Microsoft. Which of the following settings would you configure?

- A. Turn off Pop-up Blocker.
- B. Disable Add-ons for Windows Messenger.
- C. Turn off Windows Defender.
- D. Turn off Automatic Website Checking for Phishing Filter.

45. Which of the following statements are true about default settings in Internet Explorer 7 when Windows Vista is installed on a computer?

- A. Parental Controls are preconfigured.
- B. Phishing Filter is enabled.
- C. Pop-up Blocker is enabled.
- D. Automatic Website Checking is turned on.

46. Which of the following is the easiest and quickest way in Internet Explorer 7 to check whether a website is a security risk?

- A. Click the Phishing Filter icon on the Information bar and select Check This Website.
- B. Click Tools, Phishing Filter, and select Turn On Automatic Website Checking.
- C. Click Tools, Phishing Filter, and select Check This Website.
- D. Click the Phishing Filter icon on the Information bar and select Report This Website.

47. Which of the following is true about the Protected Mode in Internet Explorer 7?

- A. It automatically checks websites and reports them to Microsoft.
- B. It is enabled by default when Internet Explorer is installed.
- C. It protects the operating system from websites that automatically install programs.
- D. It prevents websites from writing data outside the Temporary Internet Files folder.
- E. It protects all user data from accidental damage.
48. You are configuring Internet Explorer on one of the Windows Vista computers. You do not want cookies stored on this computer to be accessed by any websites. Which of the following privacy options would you configure to accomplish this?
   - A. Low
   - B. Medium
   - C. High
   - D. Block All Cookies

49. You are filling out a form for an online retail store when you suddenly realize that the website is a fraud. You feel sad about having submitted your personal information to the website. How should you configure Internet Explorer so that such websites are automatically checked in the future?
   - A. Turn on Pop-up Blocker.
   - B. Configure Parental Controls.
   - C. Turn on Phishing Filter.
   - D. Turn on Protected Mode.

50. You are configuring privacy options in Internet Explorer 7. You are concerned about personal information being stored as cookies. You do not want websites that have no compact privacy policy to store cookies on your computer. You also do not want to be contacted by any websites that read information from the cookies. Which of the following privacy options should you select?
   - A. Low
   - B. Medium
   - C. Medium High
   - D. High

51. Which of the following filter level settings are available in Internet Explorer 7 to block pop-ups?
   - A. High
   - B. Medium Low
   - C. Medium
   - D. Low
   - E. Block All Pop-ups
52. You have configured maximum security in Internet Explorer 7 for the Windows Vista computer that will be used by the marketing manager of your organization. He wants to know the easiest way to check whether a website is using encryption. What would you tell him?
   - A. Click Tools, Phishing Filter, and select Check This Website.
   - B. Look for the Lock icon in the Information bar.
   - C. Look for the Phishing Filter when opening a website.
   - D. Look for Microsoft Genuine icon when opening a website.

53. You are configuring security for Internet Explorer 7 on the Windows Vista computer of your manager. His major concern is that the Protected Mode should always be on when he is on the Internet. Which of the following security zones do not have Protected Mode enabled by default?
   - A. Internet zone
   - B. Local Intranet zone
   - C. Trusted Sites zone
   - D. Restricted Sites zone

54. You are the help desk technician for Acme.com. Acme.com upgraded all its Windows XP computers to Windows Vista last month. A user calls you to inform that every time he visits a website a warning appears in the Information bar about the website. He reports that he can visit several websites without reporting a fraudulent website. How is the Phishing Filter configured on this user’s computer?
   - A. Report This Website.
   - B. Turn On Automatic Website Checking.
   - C. Turn Off Automatic Website Checking.
   - D. The Phishing Filter add-on is not installed.

55. How can you prevent a user from downloading any files or programs from a website but still enable him to visit the website anytime he wants?
   - A. Add the website to the Restricted Sites zone.
   - B. Enable the Phishing Filter for the website.
   - C. Add the website to the Trusted Sites zone.
   - D. Configure Advanced Privacy Settings for the Internet zone to Block.
56. You have recently upgraded a Windows XP computer at home to Windows Vista Home Premium edition. When surfing the Internet from this computer, you visited a website that installed a spyware program on the computer. You want to configure Internet Explorer security so that no website can install any application on your computer without your knowledge. What settings should you configure in the Internet Options window?
   ○ A. Block All Cookies in the Privacy tab
   ○ B. Enable Protected Mode in the Security tab
   ○ C. Enable Content Advisor in the Content tab
   ○ D. Enable Pop-up Blocker

57. You frequently visit the website of one of your wholesale suppliers. The website uses pop-ups, but pop-ups are currently blocked on your Windows Vista computer. The supplier is a trusted party, and you need to allow the pop-up so that you can view information about some items. How should you configure Internet Explorer 7 to handle pop-ups?
   ○ A. Add the website to the Allowed Sites list.
   ○ B. Disable the Pop-up Blocker.
   ○ C. Temporarily allow pop-ups when they appear.
   ○ D. Set the pop-up filter level to Low.

58. You were visiting the website of an online game provider when you accidentally installed an ActiveX control to play a game. After this, your computer started crashing repeatedly. How can you resolve this problem?
   ○ A. Enable the Phishing Filter on your computer.
   ○ B. Enable Protected Mode.
   ○ C. Disable the ActiveX control for the game.
   ○ D. Add the website to the Restricted Sites list.

59. You want to block all inbound connections from specific computers on the Internet to your computer so that you can work in a secure manner. Which of the following options available in Windows Vista would you configure?
   ○ A. Windows Defender
   ○ B. Phishing Filter
   ○ C. Pop-up Blocker
   ○ D. Windows Firewall
60. Which tab of the Windows Firewall properties dialog box contains the buttons for turning it on or off?
   ○ A. General
   ○ B. Exceptions
   ○ C. Actions
   ○ D. Advanced

61. You want to configure rules for inbound and outbound traffic that passes through the Windows Firewall on a Windows Vista computer. How can you configure these rules?
   ○ A. From the Advanced tab of Windows Firewall
   ○ B. From the Exceptions tab of Windows Firewall
   ○ C. From the Windows Firewall with Advanced Security link in Administrative Tools
   ○ D. From the Firewall Rules link in the Network and Sharing Center

62. A Windows Vista computer with two network interfaces and pre-configured Windows Firewall settings has been allocated to you for your office work. After a few hours, you find that some Windows Firewall settings are not suitable for the type of job you are working on. One of the network interfaces is repeatedly blocking some network traffic. What is the easiest way to restore the original Windows Firewall settings that are configured on installation?
   ○ A. Click the Block All Incoming Connections button in the General tab.
   ○ B. Clear all check boxes in the Exceptions tab.
   ○ C. Click the check box for Notify Me When Windows Firewall Blocks a New Program in the Exceptions tab.
   ○ D. Select the network interface in the Advanced tab and click the Restore Defaults button.
63. You want to allow certain network users on your internal network to work on an application. The application is currently blocked by Windows Firewall on your computer. You open Windows Firewall properties but do not find the program in the Exceptions tab. You add the program to the Exceptions list by using the Add Program button. The next thing you notice is that all network users can access that program on your computer. How can you configure Windows Firewall to allow only specified computers to access the application on your computer?

- A. Use the Add User button in the Exceptions list to allow only specific users.
- B. Use the Custom option in the Change Scope window to add IP addresses of computers that should be allowed.
- C. Use the Add Port button in the Exceptions tab to add port numbers of network computers that should be allowed.
- D. Use the Any Computer option in the Change Scope window to add IP addresses of specific computers manually.

64. Which of the following are true statements about Windows Firewall default settings when Windows Vista is installed on a computer that is connected to the Internet?

- A. Windows Firewall is enabled by default.
- B. No exceptions are configured.
- C. It is configured on the Local Area Connection.
- D. All incoming connected are blocked.

65. You are using your Windows Vista laptop in a public library where free Internet access is available. You do not want anyone else in the library to connect to your computer. You open the Windows Firewall properties window and notice that Windows Firewall is enabled by default on your computer. What else should you do so that no one can get access to your laptop?

- A. Click the Block All Outbound Connections check box.
- B. Click the Block All Inbound Connections check box.
- C. Click all check boxes in the Exceptions tab.
- D. Clear all check boxes in the Exceptions tab.
66. While configuring Windows Firewall on your computer, you clicked the option for Block All Incoming Connections. After this, you opened the Exceptions tab and enabled Remote Desktop, Remote Administration, and Remote Assistance. Which of the following actions can be performed on this computer with these settings?
   - A. Connecting to another computer using Remote Desktop
   - B. Connecting to this computer using Remote Assistance
   - C. Administering this computer remotely
   - D. None of above

67. You have designed a new website that you want to be viewed only by the users inside your organization's network. How can you configure Windows Firewall to block all Internet connections for your website but allow all internal computers?
   - A. By adding IP addresses of all internal computers in the Change Scope dialog box
   - B. By using the Block All Incoming Connections button and then adding IP addresses of local computers in the Exceptions list
   - C. By using the Block All Incoming Connections button and then adding IP addresses of local computers in the Exceptions list
   - D. By using the My Network Only option in the Change Scope dialog box

68. Which of the following networking protocols can be allowed or blocked using Windows Firewall?
   - A. TCP
   - B. UDP
   - C. AppleTalk
   - D. IPX/SPX

69. You have created a website for testing purposes on one of the Windows Vista computers in a test lab. Because the website is a secure website, you want to define incoming and outgoing traffic rules for the website. Which of the following features in Windows Vista will allow you to complete this task?
   - A. Phishing Filter
   - B. Windows Firewall
   - C. Windows Firewall with Advanced Security
   - D. Windows Defender
70. Which of the following network profiles is not used to configure Advanced Security in Windows Firewall?

- A. Internet
- B. Public
- C. Private
- D. Domain

71. Which of the following network profiles in Windows Firewall blocks all inbound network connections by default?

- A. Domain
- B. Public
- C. Private
- D. IPSec

72. You install Windows Vista on a new Pentium 4 computer that has two hard drives and configure Windows Firewall to Block All Incoming Connections. Later, you remove one of the hard drives and convert the remaining disk to dynamic. You then join the computer to a Windows Server 2003 domain. When you check the Windows Firewall settings, you notice that the check box for Block All Incoming Connections is cleared. What could be the reason?

- A. The hard drive with Windows Firewall settings has been removed.
- B. Windows Firewall is not supported on dynamic disks.
- C. The network profile of the computer has changed.
- D. Windows domains do not support blocking all incoming connections.

73. You have configured Windows Firewall on one of the Windows Vista computers in your network that is being used as a file server. After initial configuration, some users complain about access problems connecting to the file server. You want to analyze events related to Windows Firewall, but the log file does not contain enough information. How can you configure settings for security logging so that you can increase the size of the log file to troubleshoot the problem?

- A. From the General tab of Windows Firewall properties.
- B. From the Advanced Security for Windows Firewall snap-in.
- C. From the Advanced tab of Windows Firewall properties.
- D. The log file size cannot be changed for Windows Firewall security events.
74. You are working on a project that is critical to the production department of your organization. The computer is also used as an FTP server. You do not want anyone in the organization to upload any files to this computer until the project is completed. You want to configure Advanced Security for Windows Firewall for this purpose. Which of the following Windows Firewall rules would you configure?

- A. Inbound rule
- B. Outbound rule
- C. IPSec rule
- D. Connection Security rule

75. You want to configure Advanced Security for Windows Firewall on a group of three Windows Vista computers. The rules are to be based on the IPsec protocol and mainly will be used for authentication purposes. Which of the following rules would you configure?

- A. Inbound Rules
- B. Outbound Rules
- C. Connection Security Rules
- D. Custom Rules

76. You have configured Windows Firewall on a computer with two network interfaces. This computer is connected to two different network segments. Which of the following is true about Windows Firewall in this scenario?

- A. It will not work on any of the interfaces.
- B. It will work on only one of the interfaces.
- C. It will work on only one network interface at a time.
- D. It will work on all network interfaces.
## Quick-Check Answer Key

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>A and C</td>
<td>10.</td>
<td>A, B, D, and E</td>
<td>27.</td>
</tr>
<tr>
<td>8.</td>
<td>C</td>
<td>17.</td>
<td>A</td>
<td>34.</td>
</tr>
<tr>
<td>10.</td>
<td>A, B, D, and E</td>
<td>36.</td>
<td>A, B, D, and E</td>
<td>53.</td>
</tr>
<tr>
<td>12.</td>
<td>A</td>
<td>38.</td>
<td>B</td>
<td>55.</td>
</tr>
<tr>
<td>14.</td>
<td>C</td>
<td>40.</td>
<td>D</td>
<td>57.</td>
</tr>
<tr>
<td>15.</td>
<td>B</td>
<td>41.</td>
<td>A</td>
<td>58.</td>
</tr>
<tr>
<td>16.</td>
<td>D</td>
<td>42.</td>
<td>C</td>
<td>59.</td>
</tr>
<tr>
<td>17.</td>
<td>A</td>
<td>43.</td>
<td>B</td>
<td>60.</td>
</tr>
<tr>
<td>18.</td>
<td>D</td>
<td>44.</td>
<td>D</td>
<td>61.</td>
</tr>
<tr>
<td>21.</td>
<td>C</td>
<td>47.</td>
<td>B, C, and D</td>
<td>64.</td>
</tr>
<tr>
<td>27.</td>
<td>B</td>
<td>53.</td>
<td>C</td>
<td>70.</td>
</tr>
<tr>
<td>31.</td>
<td>A and B</td>
<td>57.</td>
<td>A</td>
<td>74.</td>
</tr>
<tr>
<td>32.</td>
<td>A, B, C, and D</td>
<td>58.</td>
<td>C</td>
<td>75.</td>
</tr>
<tr>
<td>33.</td>
<td>B, D, E, and F</td>
<td>59.</td>
<td>D</td>
<td>76.</td>
</tr>
<tr>
<td>34.</td>
<td>D</td>
<td>60.</td>
<td>A</td>
<td>77.</td>
</tr>
<tr>
<td>35.</td>
<td>C</td>
<td>61.</td>
<td>C</td>
<td>78.</td>
</tr>
<tr>
<td>37.</td>
<td>D</td>
<td>63.</td>
<td>B</td>
<td>80.</td>
</tr>
<tr>
<td>38.</td>
<td>B</td>
<td>64.</td>
<td>A and C</td>
<td>81.</td>
</tr>
<tr>
<td>41.</td>
<td>A</td>
<td>67.</td>
<td>D</td>
<td>84.</td>
</tr>
<tr>
<td>42.</td>
<td>C</td>
<td>68.</td>
<td>A and B</td>
<td>85.</td>
</tr>
<tr>
<td>43.</td>
<td>B</td>
<td>69.</td>
<td>C</td>
<td>86.</td>
</tr>
<tr>
<td>44.</td>
<td>D</td>
<td>70.</td>
<td>A</td>
<td>87.</td>
</tr>
<tr>
<td>45.</td>
<td>C</td>
<td>71.</td>
<td>B</td>
<td>88.</td>
</tr>
<tr>
<td>46.</td>
<td>A and C</td>
<td>72.</td>
<td>C</td>
<td>89.</td>
</tr>
<tr>
<td>47.</td>
<td>B, C, and D</td>
<td>73.</td>
<td>B</td>
<td>90.</td>
</tr>
<tr>
<td>48.</td>
<td>D</td>
<td>74.</td>
<td>A</td>
<td>91.</td>
</tr>
<tr>
<td>49.</td>
<td>C</td>
<td>75.</td>
<td>C</td>
<td>92.</td>
</tr>
<tr>
<td>50.</td>
<td>D</td>
<td>76.</td>
<td>D</td>
<td>93.</td>
</tr>
</tbody>
</table>
Answers and Explanations

1. **Answers A and C.** The two types of user accounts in Windows Vista are Administrator and Standard User. The Guest account is a type of standard user. Power User and Limited account types do not exist in the Windows Vista operating system.

2. **Answer: A.** You should create Standard User accounts for normal users of Windows Vista. The Administrator account is for performing administrative tasks. The Limited account does not exist in Windows Vista, and the Guest account is used for those users who need casual access to a Windows Vista computer.

3. **Answers: A, B, and C.** By default, the Administrator, Initial User, and Guest accounts are created on a Windows Vista computer during installation. Of these, the Administrator and Guest accounts remain in a disabled state. The Backup Operator account is not created during installation.

4. **Answer: D.** The Initial User account in Windows Vista is assigned to the name of the registered user. This user account gets the administrative privileges. The Guest account and the Administrator account remain in a disabled state after installation of the operating system. The Limited User account does not exist in Windows Vista.

5. **Answer: C.** The built-in Administrator account is disabled by default. If you need to use this account to perform some administrative tasks, be careful to rename it so that it cannot be easily spoofed. You must make it a habit to never use the name Administrator for any account that has administrative privileges on a computer. If you enable the account only when you need it, you will first need to log on using another Administrator account. You must also not turn off UAC for the Admin account. Accounts should also not be deleted. Instead, if an account is not in use, it should be disabled.

6. **Answer: B.** A user account should be disabled when a person is not using it any longer. A disabled account retains all its properties and can be assigned to some other user after renaming it at a later stage. It is not advisable to delete a user account. Renaming the account will keep the account enabled and can be a security risk. Changing the account password will not help because the account will still carry the same name and remain active.

7. **Answers: A and C.** Local User accounts for a Windows Vista computer can be created using the Local Users and Groups snap-in or the User Accounts utility in the Control Panel. The Local Users and Groups snap-in is available in the Computer Management console. The Active Directory Users and Computers console is used to create domain user accounts, and the User Manager utility is used in Windows NT computers.

8. **Answer: C.** To create domain user accounts on a Windows Vista computer, you need to install the Windows Server Administration Pack (Adminpak.msi) on the computer. You need not install the User Accounts utility or the Local Users and Groups snap-in; these are already available on a Windows Vista computer. The User Manager utility was available on Windows NT computers for creating user accounts.

9. **Answer: C.** The User Account Control (UAC) dialog box displays when a user attempts to install an application on a Windows Vista computer. Dialog boxes titled Application Authentication Code, Application Access Control, and Access Control List do not
display. Application Authentication Code and Application Access Control are invalid, and an access control list (ACL) applies to permissions for objects in Windows operating systems.

10. **Answers: A, B, D, and E.** Windows Vista displays the User Account Control (UAC) dialog box when a standard user tries to perform an administrative task or when he tries to install an application, whether or not it is digitally signed. The UAC dialog box also displays when an administrator tries to perform a system task or run an application that is not digitally signed. UAC is not displayed when someone runs an application such as Microsoft Office.

11. **Answer: C.** When an administrator is logged on with a Standard User account and tries to perform an administrative action such as opening the Device Manager utility, the UAC dialog box asks the user for administrative credentials. Because the administrator is logged on as a standard user, he should provide administrator username and password to continue the action. He does not have to log off and log on again with administrative credentials to restart the computer. The Continue button appears in the UAC dialog box when the administrator is logged on using his administrator credentials but UAC wants him to confirm his action.

12. **Answer: A.** The UAC warning does not appear on a Windows Vista computer only when it is turned off. UAC is a security feature and is enabled by default on all Windows Vista editions. The most possible cause of the problem is that UAC is turned off on the computer. UAC is supported on all editions of Windows Vista and does not have any specific hardware requirements. Jim does not need to log on as an administrator to view the UAC warning. However, he must log on as an administrator to turn on the UAC feature.

13. **Answers: A, B, and E.** The UAC feature is included in Windows Vista to prevent unauthorized changes to the computer. It does not appear when it is turned off or when a user or administrator tries to perform a nonadministrative task such as running Microsoft Office applications, adding a printer to the computer, or changing power management settings. It does, however, appear when a user or administrator wants to change systemwide settings such as changing system time or running the Computer Management console, provided it is not turned off. It also appears when a user or administrator tries to modify security settings.

14. **Answer: C.** The User Account Control behaves differently and prompts different warning messages depending on who is currently logged on to the computer and what application is being run. When an administrator tries to run (or install) an application that does not have a digital signature, the dialog box warns the administrator that “An Unauthorized Program Wants Access to Your Computer.” The administrator has two options: the Cancel button, to cancel the installation; the Allow button, to allow the installation. The message in option A, “Type an Administrator Password and Click OK,” appears when a user tries to run a system task or when the administrator himself is logged on as a standard user and wants to run a system task so that privileges could be elevated to perform the task. The user needs to select the Administrator account and enter the password to continue. The message in option B, “Windows Needs Your Permission to Continue,” appears when an administrator wants to perform a system task. The message in option D, “A Program Needs Your Permission to Continue,” appears when an administrator wants to run an application that has digital signatures.
15. **Answer: B.** UAC will not let an administrator perform some specific administrative tasks even when he wants to supply his administrative credentials. Security settings in Windows Vista provide the best example of such an administrative action. A user must log off and log on as an administrator to change Windows security settings. Turning off the UAC and turning it on again will not help. Mark need not restart the computer to resolve the problem. UAC files are not corrupted because the UAC feature is working fine.

16. **Answer: D.** You should click the Continue button to proceed with the installation process. The UAC dialog box is displayed just to confirm that you trust the application. Presence of a digital signature only is not sufficient. The source of the application or the publisher of the application must also be a trusted party. For this reason, the UAC warning allows you to confirm one more time that you trust the application and want to install it. The Allow button appears when you want to install an application that does not have a digital signature. The Permit button does not exist in the UAC dialog box. The Cancel button would abort the application.

17. **Answer: A.** When the UAC is kicked into action, Windows takes a snapshot of the desktop, including all running applications, and displays the UAC dialog box. During this time, the desktop is switched to a dimmed mode known as the Secure Desktop mode. You must click an appropriate button in the UAC dialog box to continue working. This is because the UAC dialog box gets priority over other running applications. The computer does not go into Sleep mode, and no application is closed. The End Process button is not a part of the UAC dialog box.

18. **Answer: D.** You should not turn off UAC on any computer because data security is important for the business. And because the UAC feature is not available in Windows XP, there is no question of turning it on or off. It does not matter whether the computer is on the wired network or wireless network, when the system/network security is of prime concern, UAC must not be turned off in any case.

19. **Answer: C.** The Admin Approval Mode in Windows Vista UAC requires an administrator to approve an application so that unauthorized applications cannot be installed automatically. Unauthorized application is usually an application that is not digitally signed or not trusted. Administrators must also click the Continue button in the UAC dialog box to install the application. It is incorrect to say that unauthorized applications cannot be installed at all or that only standard users can install unauthorized applications. Users also do not need to get written approval from the administrator to install an unauthorized application (doing so would not enable it to bypass the UAC security).

20. **Answer: B.** When a standard user tries to run an application that does not have a digital signature or that is not from a trusted party, the UAC kicks in and asks the user to supply administrative credentials. The user must ask the administrator to supply his credentials to run the application. This is called Admin Approval Mode in Windows Vista. The user cannot sign the application himself or disable the UAC to bypass the system security. The user also does not need to log on as an administrator to run the application.

21. **Answer: C.** The purpose of the admin approval or providing administrative credentials is to initiate the installation of application. This does not mean, however, that either the user is logged off or the administrator remains logged on after the installation is
The administrator is logged off, and the user can continue to work using his user account. He does not need to log off and log on again.

22. **Answer:** D. The User Account Control can be turned on or off from the Other Security Settings link available in the Windows Security Center. Click Start, Control Panel, Security to open the Windows Security Center. Click the little downward arrow to expand the Other Security Settings options. Click the Turn Off Now button to turn off the UAC. Windows Defender, Windows Firewall, and Internet Options links are not used for configuring UAC settings.

23. **Answer:** B. You can configure Windows Vista to run legacy programs that require administrative privileges to run with elevated privileges when a standard user is logged on. This is the easiest way to bypass UAC warnings when the program is executed by a Standard User account. It is not advisable to turn off UAC on any Windows Vista computer, which is an essential security feature of the operating system. In addition, you cannot run legacy applications using the built-in Administrator account.

24. **Answer:** C. Amy should disable the Secure Desktop when taking the screenshot. When the UAC is displayed, the default settings switch the desktop to Secure Desktop, which does not allow the user to perform any other action except clicking one of the buttons in the UAC dialog box. Disabling Secure Desktop will solve Amy’s problem, and she will be able to take the screenshot of the UAC dialog box. If Amy turns off the UAC, she will not get the UAC dialog box and will not be able to take the screenshot. Amy does not need to log on as an administrator to take a screenshot, and even providing administrator password will not allow her to take the screenshot.

25. **Answer:** A. For a Windows Vista computer that is a part of a workgroup, you can change the default settings of the UAC by configuring the local security policies. You can access local security policies by running the GPEDIT.MSC file, which opens the local Group Policy Object Editor window. Expand the Local Policies node in the Security Settings and click Security Options. Navigate to User Account Control Policies to view or modify any settings.

26. **Answer:** C. The Behavior of the Elevation Prompt for Standard Users to Automatically Deny Elevation Requests policy determines whether the UAC dialog box prompts users for administrative credentials when they want to perform a system task or install an application. When enabled, this policy does not display the dialog box for providing admin credentials to standard users but displays an “Access Denied” message when elevation of privileges is required. Other policies do not affect the required setting. The Admin Approval Mode for Built-in Administrator Account policy determines whether the UAC Admin Approval mode is applied to the built-in Administrator account. This policy is disabled by default.

27. **Answer:** B. The Behavior of the Elevation Prompt for Administrators in Approval Mode policy determines whether the UAC dialog box prompts the administrator for consent, asks for credentials, or whether the mode is elevated without consent when a system task is to be performed. The Prompt for Consent policy is enabled by default on all Windows Vista computers. Alternatively, you can enable the Prompt for Credentials policy, which requires the administrator to supply credentials; or, you can enable the Elevate Without Prompting policy, which will not require any administrative action. The Admin Approval Mode for Built-in Administrator Account policy determines whether
the UAC Admin Approval mode is applied to the built-in Administrator account. This policy is disabled by default.

28. **Answer: D.** Setting the Run All Administrators in Admin Approval Mode policy to Disabled turns off all UAC policies for all users on the entire Windows Vista computer. You must reboot the system to ensure that this policy takes effect. When disabled, the security of the system may be compromised. Enabling this policy decides how other UAC policies are applied to the computer depending on their respective settings. The Admin Approval Mode for Built-in Administrator Account policy determines whether the UAC Admin Approval mode is applied to the built-in Administrator account. This policy is disabled by default.

29. **Answers: B and C.** Out of the given UAC policies, the only two policies enabled by default are the Switch to Secure Desktop When Prompting for Elevation policy and the Run All Administrators in Admin Approval Mode policy. The Admin Approval Mode for the Built-in Administrator Account and Only Elevate Executables Which are Signed and Validated policies are disabled by default.

30. **Answer: B.** Windows Defender is a built-in feature of Windows Vista that provides protection against viruses, spyware, and other malware applications. Windows Defender works in the background regardless of whether any user is logged on to the system. Windows Firewall protects the computer from external networks. The User Account Control (UAC) protects the computer from unauthorized changes. BitLocker Drive Encryption is used to encrypt system files so that they are protected from any undesired and potentially damaging changes.

31. **Answers: A and B.** Windows Defender uses spyware definitions and heuristic algorithms to detect spyware and other malicious code. New Windows Defender definitions can be downloaded from the Microsoft website manually or automatically through Windows Update. Risk identification is a computer security term but is not used in Windows Defender. Microsoft SpyNet is a community that you can join to get the latest updates on security-related threats.

32. **Answers: A, B, C, and D.** Windows Vista computers can be easily harmed by installing software applications that are not signed and validated. Downloaded programs from the Internet may also damage a computer. In addition, instant messaging (IM) applications and CDs/DVDs borrowed from others can contain malicious code that may damage your operating system.

33. **Answers: B, D, E, and F.** Windows Defender allows you to choose an appropriate action when it detects a malicious code that is attempting to install on your Windows Vista computer. The actions include Ignore, Quarantine, Remove, and Always Allow. The option Allow and the option Deny do not exist.

34. **Answer: D.** If you know that it is safe to install the application, you can configure the Windows Defender action to Ignore. With this setting, Windows Defender will not prevent installation and will not prevent the application from running. However, Windows Defender will display an alert if it detects the running application during its next regular scan. With the Always Allow action, the application will be added to the Windows Defender list of allowed applications, the application will be allowed to run, and Defender will not display an alert message. With the Remove action, the application
will be permanently removed from the computer. With the Quarantine action, Windows Defender will move the application to another location on the computer and will prevent it from running.

35. Answer: C. Windows Defender usually moves malicious applications to Quarantined Items, a different location on the computer. If any application has been removed by Windows Defender, it remains in the Quarantined Items list until it is manually restored. You can also restore the application from the original setup media, but Windows Defender will again remove it. The SpyNet community will not be helpful in restoring the removed application. Software Explorer contains a list of installed software and its classification.

36. Answers: A, B, D, and E. The Software Explorer component of Windows Defender provides a basic list of programs running on the computer. The categories of programs include startup programs, currently running programs, auto-start programs, network connected programs, and Windows Sockets (WinSocks) service providers. Software Explorer does not list any programs that are bundled and shipped with the operating system.

37. Answer: D. The best way to use Windows Defender to know about a suspicious application is to use the SpyNet community. Windows Defender includes a link for Microsoft SpyNet, where you can submit the application and get free advice on unclassified applications. The Quarantined Items list includes the applications that have been detected and removed by Windows Defender. The Auto-Start Programs and Network Connected Programs lists provide lists of applications that automatically start with the system startup and run from the network, respectively.

38. Answer: B. Under its default settings, when Windows Defender detects an application with a Medium level alert, it displays the alert and provides the user an option to review the application, block it, or remove it completely from the computer. It does not automatically remove the application or ignore the alert and allow it to run. It also does not automatically block the application from running.

39. Answer: A. Under its default settings, Windows Defender will display a High alert when it detects a virus, worm, or Trojan horse on a Windows Vista computer. It will also immediately remove the application from the computer.

40. Answer: D. Windows Defender does not allow you to specify an action for applications rated with a Severe alert level when configuring actions. Instead, it will automatically remove the application. With other alert levels, you can specify an appropriate action after reviewing the details of the application.

41. Answer: A. The best course of action to immediately detect and remove the malicious application is to perform a Quick Scan using the Scan options in Windows Defender. A Quick Scan scans most parts of the Windows Vista computer, including the Windows registry, program executables, and system memory. Other options will also work but will take a little longer depending on how you want to perform the scan.

42. Answer: C. By default, the Software Explorer in Windows Defender shows only those programs that are configured to run for the currently logged-on user. As an administrator, you can click the Show for All Users check box to view all programs for all users that are configured to run automatically on system startup. These programs are
listed under the Startup Programs category. You must supply administrative credentials to perform this action. You do not need to change the category from Startup Programs to Network Connected Programs. The Refresh button will also not display programs running for all users. The Using Software Explorer link opens up help (information about using this feature).

43. **Answer: B.** The Phishing Filter is either turned off in Internet Explorer or it is not configured properly to handle websites that appear to be legitimate and try to collect personal information. It can also collect information about a suspicious website and send information to Microsoft. Parental controls in Internet Explorer are designed to control Internet usage by children. Windows Defender protects the computer from malicious programs such as spyware and adware. The purpose of Windows Firewall is to control incoming and outgoing network traffic based on firewall rules.

44. **Answer: D.** The Phishing Filter in Internet Explorer 7 reports information about suspicious websites to Microsoft when Automatic Website Checking is enabled in the Phishing Filter settings. You can turn off Automatic Website Checking so that the websites are not reported to Microsoft. To turn off automatic settings, click Tools, Phishing Filter, and select Phishing Filter Settings. This opens the Advanced tab of the Internet Options window. Scroll down to Phishing Filter node and click the radio button for Turn Off Automatic Website Checking. Alternatively, you can click the Phishing Filter icon in the notification area of the Taskbar and click Phishing Filter Settings. Turning off Pop-up Blocker or disabling add-ons for Windows Messenger will not stop Phishing Filter from checking or reporting websites to Microsoft. Windows Defender helps protect the computer from malicious programs.

45. **Answer: C.** Internet Explorer 7 is installed by default with Windows Vista. In its default configuration, only the Pop-up Blocker is enabled. Parental controls have to be configured as per your own requirements. Similarly, the Phishing Filter is not enabled by default. You need to turn it on and turn on Automatic Website Checking.

46. **Answers: A and C.** Internet Explorer 7 provides a quick-and-easy way to check a website using the Phishing Filter. Links to access the Phishing Filter are available from the Tools menu or by clicking the Phishing Filter icon on the Information bar. From this menu, you can select Check This Website to quickly check whether a website is legitimate. Turning on Automatic Website Checking will serve the same purpose but will also send information about suspicious websites to Microsoft. If you select the Report This Website option, the information about a website will be sent to Microsoft even if the website is legitimate and does not pose a security risk.

47. **Answers: B, C, and D.** Protected Mode in Internet Explorer 7 is enabled by default on Windows Vista computers and helps protect the computer from websites that want to install programs or write data to the computer without the knowledge and consent of the user. It also prevents websites from writing data outside the Temporary Internet Files folder. It does not automatically check suspicious websites or report them to Microsoft. Protected mode does not protect user data from accidental damage but does prevent system files from being damaged by websites.

48. **Answer: D.** The Block All Cookies setting in the Privacy tab of Internet Options prevents websites from getting access to cookies stored on a Windows Vista computer.
This setting also prevents websites from saving any cookies on the computer and prevents websites from reading any cookies that are already stored. The Low setting prevents third-party cookies that do not have a compact privacy policy to be stored on the computer. The Medium setting also does not allow third-party cookies that do not have a privacy policy to be stored on the computer. In addition, the Medium setting does not allow first-party or third-party cookies to be stored in a way that allows these websites to contact you without your consent.

49. **Answer: C.** You need to turn on the Phishing Filter in Internet Explorer so that fraudulent websites are automatically checked. The Phishing Filter checks a website and warns you against sending your personal information to the website. Pop-up Blocker prevents undesired advertisements from popping up on the screen when you are using Internet Explorer. Parental Controls help control the usage of the Internet by children. The Protected mode is enabled by default in Internet Explorer 7 and prevents websites from writing data to protected areas of the operating system.

50. **Answer: D.** The High setting in the Privacy tab of Internet Explorer does not allow any first-party cookies or third-party cookies to be stored on a Windows Vista computer. Under this setting, websites cannot contact you by reading information stored in cookies without your consent. The Low, Medium High, and Medium settings prevent only third-party cookies.

51. **Answers: A, C and D.** Internet Explorer allows you to select a filter level for blocking pop-ups. The three levels available are High, Medium, and Low. The Medium Low and Block All Pop-ups levels are not valid settings in Pop-up Blocker.

52. **Answer: B.** Internet Explorer displays a Lock icon in the Information bar when a secure website is opened. The Lock icon indicates that the website is using some type of encryption for transmitting data on the Internet media. The Check This Website option in the Phishing Filter checks for genuineness of a website but does not tell whether the website is using encryption. Similarly, the actions of the Phishing Filter icon indicate that the Phishing Filter is working to detect a fraudulent website. The Microsoft Genuine icon indicates that you are using legitimate Microsoft software and are not a victim of software piracy.

53. **Answer: C.** The Security tab of Internet Explorer settings provides four types of zones, and security settings can be configured for each zone separately. The Trusted Sites zone does not have Protected mode enabled by default, because these are the websites that you know will not damage your computer. You can still turn on Protected Mode for the Trusted Sites zone. The Internet, Local Intranet, and Restricted Sites zones have Protected mode on.

54. **Answers: C.** Turn Off Automatic Website Checking in Phishing Filter does not automatically check or report fraudulent websites; it just displays a warning in the Information bar. When the Phishing Filter is set as Turn On Automatic Website Checking, a red icon appears in the Information bar indicating that the website is a phishing website and may pose a security risk. The Report This Website option appears when you click the Phishing Filter icon so that you can report the website to Microsoft (which can then check whether the website is a phishing site). The Phishing Filter is a part of Internet Explorer 7 and is not installed as an add-on.
55. **Answer: A.** Adding a website to the Restricted Sites zone will allow the user to visit the website but prevent him from downloading any files or programs from the website. Enabling Phishing Filter will not prevent him from downloading files from the website. Adding the website to the Trusted Sites zone will allow the user to download anything from the website. Advanced Privacy Settings for the Internet zone will configure the way cookies are handled but will not prevent downloads from the website.

56. **Answers: B.** Protected mode in Internet Explorer 7 is enabled by default on Windows Vista computers and helps protect the computer from websites that want to install programs or write data to the protected areas of a system without the knowledge and consent of the user. It also prevents websites from writing data outside the Temporary Internet Files folder. The purpose of the Privacy tab is to handle cookies that store personal information about the user on the local computer. Content Advisor settings help select the type of website content that may be displayed in Internet Explorer. Pop-up Blocker prevents the display of pop-up advertisements while a user is surfing the Internet.

57. **Answer: A.** Adding a website to the Allowed Sites list will allow pop-ups from the supplier's website. This setting takes effect immediately and does not depend on the pop-up filter level. Disabling Pop-up Blocker will allow pop-ups from all websites. Temporarily allowing a pop-up from the supplier will allow pop-ups to appear only when allowed; you will have to allow pop-ups each time they are blocked by Pop-up Blocker. Setting the Pop-up Blocker filter level to Low will allow most pop-ups to appear.

58. **Answer: C.** The ActiveX control you installed for the game is likely causing the computer to crash. To prevent your computer from crashing in the future, you should disable this ActiveX control. Enabling the Phishing Filter will not help. Protected mode is enabled by default in Internet Explorer on Windows Vista computers. Adding the gaming website to the Restricted Sites list will prevent the site from writing data to your computer but will not disable the ActiveX control that has already been installed.

59. **Answer: D.** Windows Firewall needs to be configured to block all incoming connections to a Windows Vista computer. Windows Firewall, when configured properly, can block incoming connection requests from specific computers on the Internet. Windows Defender is a real-time scanner that protects the computer from malicious applications. Phishing Filter and Pop-up Blocker are features of Internet Explorer 7 that help protect the web surfing experience by protecting the computer from malicious websites.

60. **Answer: A.** You can turn the Windows Firewall on or off from the General tab of its properties dialog box. Windows Firewall is turned on by default on all Windows Vista computers. The Exceptions tab is used to allow certain network traffic to pass through the firewall. There is no such tab as Actions in Windows Firewall properties. The Advanced tab is used to configure Advanced Security for selected network interfaces.

61. **Answer: C.** Windows Firewall with Advanced Security is an MMC snap-in available in the Administrative Tools folder in the Control Panel. To access this snap-in, open the Control Panel and switch to Classic view. The Windows Firewall with Advanced Security link is located inside the Administrative Tools folder. The Advanced tab of the Windows Firewall Properties allows you to enable or disable Windows Firewall for a
particular network interface only. The Exceptions tab of the Windows Firewall properties is used to allow certain traffic through the firewall. There is no such link as Firewall Rules in the Network and Sharing Center.

62. **Answer: D.** When some Windows Firewall settings do not work well for you, you can restore all settings to their default values by using the Restore Defaults button in the Advanced tab of the Windows Firewall properties dialog box. In case there are two network interfaces in a computer, you can select the network interface, and then click the Restore Defaults button to restore default firewall settings for the selected network interface. When you click the Block All Incoming Connections check box, you block all network traffic from entering your Windows Vista computer. Clearing all check boxes in the Exceptions tab will also not allow most of the network traffic through the firewall. The Notify Me When Windows Firewall Blocks a New Program check box in the Exceptions tab is used to display a notification whenever Windows Firewall blocks a program from passing through the firewall.

63. **Answer: B.** When you want to allow only some specific computers on the network to access an application on your computer, you can add the application to the Exceptions list by using the Add Program button. After you have done this, click the Change Scope button to open the Change Scope dialog box. In this dialog box, you can choose which computers will be allowed by specifying their IP addresses after clicking the Custom button. If you want to allow all network computers to access the application on your computer, click the Any Computer button, which opens the application for all computers on the local network and the Internet. To allow only computers on the local network subnet, click the My Network Only button. There is no Add User button in the Exceptions tab of Windows Firewall properties.

64. **Answers: A and C.** In Windows Vista, the Windows Firewall is enabled (on) by default and is configured for the local area connection. It is incorrect to say that there are no exceptions. Some exceptions such as File and Printer Sharing, Windows Fax and Scan, Remote Access, and so on are also there to allow common network operations. Windows Firewall does not block all incoming connections by default.

65. **Answer: B.** When you click the Block All Inbound Connections check box in the General tab of the Windows Firewall properties dialog box, all incoming connections are blocked. This is a preferred setting when you are using your computer in a public place such as a library or a restaurant. Note that there is no option to block all outbound connections in the General tab of the Windows Firewall properties. When you click (select) all boxes in the Exceptions tab, you are actually allowing all inbound connections. On the other hand, clearing all check boxes in the Exceptions tab will allow you to block several types of incoming traffic, but will not totally block all incoming connections.

66. **Answers: D.** Even when you have configured exceptions in Windows Firewall for features such as Remote Desktop, Remote Administration, and Remote Assistance, these actions cannot be performed. This is because the Block All Incoming Connections setting ignores all exceptions. You must disable the Block All Incoming Connections option to use the exceptions.

67. **Answers: D.** You can allow the computers on the local network to access the website by selecting the My Network Only option in the Change Scope dialog box. This will not
allow any computer on an external network such as the Internet to access the website on your computer. You can also add IP addresses of all computers in the Change Scope dialog box, but this will be a complicated task. When you select the Block All Incoming Connections options, no connection to your computer is allowed. Moreover, you cannot block computers by IP address in the Exceptions list. The Exceptions tab is used to allow certain applications to pass through the firewall that are otherwise blocked. Note that computers are blocked or allowed using IP addresses, whereas applications are blocked by port numbers.

68. **Answers: A and B.** Windows Firewall works on TCP and UDP protocols to allow or block applications. There is no way to configure Windows Firewall to allow or block AppleTalk or IPX/SPX or their associated protocols.

69. **Answer: C.** You can define inbound and outbound network traffic rules using the Windows Firewall with Advanced Security MMC snap-in. This snap-in is available in the Administrative Tools folder in the Control Panel. The Phishing Filter monitors only those websites that pose a security risk to a Windows Vista computer. The Windows Firewall, which is turned on by default, provides only a basic security to the computer. Windows Defender monitors malicious applications that may damage the operating system.

70. **Answer: A.** Advanced Security in Windows Firewall is based on the network profile of the Windows Vista computer. The network profile can be Public, Private, or Domain. An Internet network profile does not exist for configuring Advanced Security for the Windows Firewall.

71. **Answer: B.** When the network profile of a computer is Public, the Windows Firewall blocks all inbound connections by default. Note that only one profile can be active at a time, and Windows Firewall dynamically changes the rules when the network profile of the computer is changed. IPSec refers to IP Security and is not a network profile for the purpose of Windows Firewall security.

72. **Answer: C.** The reason for changed settings in Windows Firewall is that the network profile of the computer has changed after joining the Windows Server 2003 domain. The computer now has a Domain profile. By default, only those incoming connections that do not meet the predefined rules are blocked. Removing a hard drive or converting a drive to dynamic does not affect Windows Firewall configuration. It is also incorrect to say that Windows domains do not support blocking all incoming connections.

73. **Answer: B.** The Advanced Security for Windows Firewall contains settings for logging events related to Windows Firewall. These settings are available in the Advanced tab of Windows Firewall properties in Windows XP. The General tab and the Advanced tab of Windows Firewall properties do not have the logging settings. Instead, it is in the Advanced tab that you will find the Where Can I Find ICMP and Logging Settings? link.

74. **Answer: A.** You need to configure inbound rules so that incoming FTP traffic can be blocked. Outbound Rules are applied to outgoing traffic from the computer in question. IPSec rules are configured for encrypted communications in the network. Connection Security Rules are configured for authentication purposes.

These rules do not specifically allow or block connections. Inbound Rules apply to incoming traffic, and Outbound Rules apply to outgoing traffic. A Custom Rules option does not exist in the Advanced Security for Windows Firewall snap-in. However, you can customize any predefined rules.

76. **Answer: D.** When configured on a computer with two or more network interfaces, Windows Firewall will work on all network interfaces by default. You can exclude one of the network interfaces by clearing its check box in the Advanced tab of the Windows Firewall properties. It is incorrect to say that Windows Firewall will not work on any of the interfaces. It is also incorrect to say that Windows Firewall will work only on one of the network interfaces at a time.