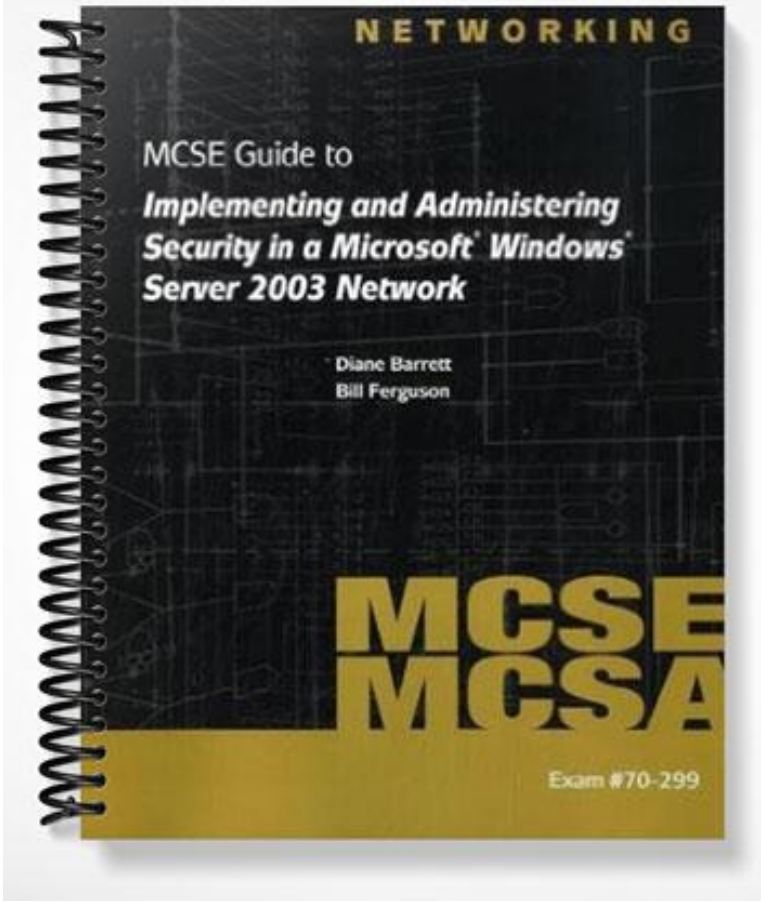
SOLUTIONS MANUAL



Chapter 2 Solutions

Review Questions

1. Which of the following is the lowest lockdown level of security for baseline templates?
   Answer: b.

2. Which of the following is the recommended template for Windows Server 2003 print servers?
   Answer: a.

3. Which of the following should you adhere to when you plan the security of a bastion host? (Choose all that apply.)
   Answer: a, b, d.

4. What is a publicly accessible computer located on the perimeter network that also may be referred to as the DMZ, (demilitarized zone) or screened subnet?
   Answer: c.

5. Properly planning an organization's security structure will result in a much more secure Active Directory design for the organization. To achieve these results, careful planning of which of the following elements is needed? (Choose all that apply.)
   Answer: a, b, d.

6. Which of the following store directory data for Active Directory and manage communication between users and domains?
   Answer: b.

7. What happens if you do not properly configure and test the GPO before linking it to the Domain Controllers OU?
   Answer: b.

8. Which of the following services do domain controllers provide? (Choose three.)
   Answer: a, c, d.

9. Which of the following are network infrastructure services? (Choose all that apply.)
   Answer: a, b, c.

10. Which of the following is a good reason why DHCP servers need to be secure? (Choose all that apply.)
    Answer: c, d.

11. Additional security measures that should be performed on an IIS server would include which of the following? (Choose three.)
    Answer: a, b, d.

12. The Enterprise Client environment is designed to provide solid security for the organization. Which of the following operating systems does it support? (Choose all that apply.)
    Answer: a, b, d.

13. Security environment is the highest lockdown level. In this environment the settings are very restrictive. Which of the following are downsides of using this type of template? (Choose all that apply.)
    Answer: a, c, d.

14. Zone security is a method that enables you to divide online Web content into groups or zones. Specific Web sites can then be assigned to each zone, depending on the degree to which the content of each site is trusted. Which of the following are security zones? (Choose all that apply.)

Answer: a, c, d.

15. On which of the following types of client computers are you likely to find a loopback policy?
Answer: a.

16. Which of the following are some of the most common uses for a bastion hosts? (Choose all that apply.)
Answer: a, c, d.

17. To which of the following types of server roles can you not apply Group Policy?
Answer: b.

18. Which of the following are administrative templates? (Choose all that apply.)
Answer: a, c, d.

19. Administrative Templates are what kind of files?
Answer: a.

20. To create exceptions to software restriction policies, you can create rules for specific software. Which of the following are types of rules that you can create? (Choose all that apply.)
Answer: a, b, c, d.

21. On which of the following types of client computers would you most likely use The Connection Manager Administration Kit (CMAK)?
Answer: c.

22. Which of the following client computers require the highest level of security?
Answer: c.

23. Which of the following security changes should be made to the baseline server template for servers that will run DHCP? (Choose all that apply.)
Answer: a, b, c.

24. Which of the following are valid exceptions for software restriction policies? (Choose all that apply.)
Answer: a, c, d.

25. Which of the following would you use to control what types of software is available to users?
Answer: d.

Activities

Activity 2-1
The purpose of the activity is to have the students install the GPMC.

Activity 2-2
The purpose of the activity is to have the students look at the default settings installed for Domain controllers by using the Group Policy Management Console.

Activity 2-3
The purpose of the activity is to have the students refresh their skills by creating the member servers OU and delegating responsibility.

Activity 2-4
The purpose of the activity is to have the students work with security templates by importing the Enterprise Client Member Server baseline template.

Activity 2-5
The purpose of the activity is to reinforce the prior activity and have the students work with security templates by importing the Enterprise Client Infrastructure Server template.

Activity 2-6
The purpose of the activity is to have the students investigate the IIS Lockdown and URLScan tool.

Activity 2-7
The purpose of the activity is to have the students investigate the additional security templates that can be used for configuring servers and clients.

Activity 2-8
The purpose of the activity is to have the students become aware of the checklists available in the Microsoft Security Guidance Kit for client machine configuration.

Activity 2-9
The purpose of the activity is to have the students practice working with security settings by importing a template, then evaluating the settings.

Activity 2-10
The purpose of the activity is to have the students enable certificates hash rules for software restriction policies.

Case Projects

Case Project 2-1
In order to choose a Microsoft model outlining the baseline templates that you would use for the servers, you would first examine the default templates. Since your network consists of all Windows 2003 servers and Windows XP clients, you can use the Enterprise Client templates. The templates you choose would be similar to these: For the five infrastructure servers - Infrastructure server , two domain controllers - Domain controller, a print server - Print server, two Web servers - IIS server or Bastion host, and two e-mail servers Bastion host.

Case Project 2-2
The Enterprise Client environment is designed to provide solid security for the organization. An Enterprise Client environment is defined as only having Windows Server 2003, Windows 2000 Professional, and Windows XP Professional computers in the environment. This allows use of more restrictive security templates for added security. Using these security templates also allows the organization to introduce additional roles on top of the baseline member server template. Settings would be configured based on the recommendations in the Windows Server 2003 Security Guide.

Case Project 2-3
By design, mobile or laptop computers and many new types of portable devices such as portable hard drives and thumb drives have a higher risk of being stolen than a nonportable device. Physical security should be an important consideration when building a template for these types of machines. If theft does occur, not only is there concern about the initial data loss but you must also consider the possibility of having an unauthorized person penetrate the network via remote dial-up or wireless networking. However, you can use Encrypted File System (EFS) to protect files. Using EFS is similar to using permissions on files and folders. An intruder who gains unauthorized physical access to your encrypted files or folders will be prevented from reading them. If the intruder tries to open or copy your encrypted file or folder he or she will receive an access denied message.

Configuring each user’s computer for remote network access or relying on users to configure their own computers for remote network access produce serious support issues. In order to reduce support issues, Connection Manager can be used to customize a self-installing service profile for mobile clients. Clients can be automatically configured to connect to your network directly or to create a VPN connection from a remote location. It allows for more gradual control over settings such as idle timeout time, maximum session time, and encryption strength.

In some types of businesses, direct wire-based connections to the network are not always practical; for example, in a warehouse setting, or where users are counting physical inventory. In these types of situations, you will use a wireless local area network (WLAN). Using a wireless local area network, allows portable computers to access network connections from any point where the organization has wireless access points. However, wireless networks have significant security risks. Wireless networking signals use radio waves to send and receive information. Anyone within a certain distance of a wireless access point can access, detect, and receive data sent to and from the wireless access point. To counter this security risk, wireless access points must be secured.

Case Project 2-4

Network security zones offer a flexible way to enforce your organization's Internet security policies, based on the origin of the Web content. Security zones enable you to group sites together, place them in a zone and then assign a security level to each zone.

Security settings can be used with administrative templates in Group Policy to restrict the settings users can change. These settings enable administrators to configure the behavior and appearance of the desktop, including the operating system, components, and applications. This helps maintain consistency across the organization.

Software restriction policies provide administrators with a means to identify software and manage its capacity to run on local computers. These policies can also be used to protect computers running Windows XP Professional in an environment against malicious viruses and Trojan horse programs. Software restriction policy integrates with Active Directory or can be used on standalone computers.

Case Project 2-5

Bastion hosts are found in a DMZ. Sometimes bastion hosts are unprotected by a firewall or filtering router, leaving them highly exposed to attacks. They must be secured as much as possible to maximize their availability and yet minimize the chance of their being compromised. Since they are so vulnerable, the design and configuration of bastion hosts must be carefully thought out to reduce the chances of an attack being successful. The most secure bastion host servers limit access to only highly trusted accounts, and enable the fewest services possible necessary to fully perform their functions. It is easier to secure services when the bastion host is dedicated to performing just one role. The more roles each host has to play, the greater the likelihood that a security hole will be overlooked. When securing bastion hosts all unnecessary services, protocols, programs, and network interfaces are disabled or removed, and then each particular one host is configured to fulfill a specific role. By using this method, the potential for successful attacks can be limited.

Applying the High Security – Bastion Host.inf security template enhances server security by reducing the attack surface of a bastion host, but makes remote management of the bastion host impossible. If you choose to increase manageability or functionality of a bastion host, the template must be modified. Make sure that the security template is configured to enable the bastion host functionality your environment requires. It is also strongly recommended that you perform a full backup of a bastion host server before applying the High Security – Bastion Host.inf security template because reverting back to the original configuration after applying the High Security – Bastion Host.inf security template is very difficult

Here are the points to evaluate as you plan the security of a bastion host:

- The *Allow log on locally* user right enables a user to start an interactive session on the computer. Limit the accounts that can be used to log on to a bastion host server console. This will help prevent unauthorized access to a server's file system and system services. Granting this right only to the Administrators group limits administrative access to bastion host servers and provides a better level of security.
- All services not required by the operating system and those not essential to the proper operation of the bastion host's role should be disabled. This may generate numerous Event Log warnings, most of which can be ignored. Again, you are faced with a tradeoff. Enabling these services will reduce Event Log messages but increase the attack surface of the bastion host. The following is a list of the services that are not essential to the proper operation of a bastion host.
    - Automatic Updates—Wuauserv
    - Background Intelligent Transfer Service—BITS
    - Computer Browser—Browser
    - DHCP Client—Dhcp
    - Network Location Awareness (NLA) —NLA
    - NTLM Security Support Provider—NtLmSsp
    - Performance Logs and Alerts—SysmonLog

    - Remote Administration Service—SrvcSurg
    - Remote Registry Service—RemoteRegistry
    - Server—lanmanserver
    - TCP/IP NetBIOS Helper Service—LMHosts
    - Terminal Services—TermService
    - Windows Installer—MSIServer
    - Windows Management Instrumentation Driver Extensions—WMI
    - WMI Performance Adapter—WmiApSrv.
- Disabling SMB and NetBIOS over TCP/IP greatly reduces the server's attack surface. Servers operating under this configuration cannot access folders shared on the network and are more difficult to manage, but disabling these protocols protects the server from being easily compromised.
- All services not required by the operating system and those not essential to the proper operation of the bastion host's role should be disabled.
- Never configure a service to run under the security context of a domain account unless absolutely necessary.
- Internet Protocol Security (IPSec) filters can provide an effective means for enhancing the level of security required for servers. Block ports by using IPSec filters.

The Error Reporting service helps Microsoft track and address errors. Error reports can potentially contain sensitive or confidential data. Since the data is transmitted in cleartext Hypertext Transfer Protocol (HTTP), it could be intercepted on the Internet and viewed by third parties. The Error Reporting setting should be set to Disabled.

Chapter 2

Planning and Configuring Security Policies

At a Glance

Instructor's Manual Table of Contents

- Overview
- Objectives
- Teaching Tips
- Quick Quizzes
- Class Discussion Topics
- Additional Projects
- Additional Resources
- Technical Notes for Activities

Lecture Notes

Overview

The best security plans and designs in the world cannot protect an organization if the plan is made, but then forgotten about. Because every organization has its own distinctive mix of clients, servers, and user requirements, planning a complete, secure environment has become a key challenge, especially with the mix of wireless, personal digital assistants (PDAs) and cell phones a network administrator must secure. Without a consistent approach to security, some areas of the network might be secured more tightly, while others may be overlooked or only marginally secured. By carefully analyzing the requirements of your organization and using a concise, consistent planning process, you can establish a high-level security framework for your environment. This chapter will provide a guide for enhancing the security setting configurations of your servers and clients to help you plan a more secure environment.

Chapter Objectives

- Define the role of servers
- Understand how security mechanisms can be used to create baseline servers
- Develop a network security structure based on server role
- Define security policies for different computer roles such as bastion hosts, IIS, and IAS
- Develop a network security structure based on client role
- Recognize and plan restriction policies based on client computer roles
- Configure client security settings
- Configure software restriction policies

Teaching Tips

Defining Computer Roles

1. Provide students with an overview of the concept of organization's security structure. Stress the point that proper planning of an organization's security structure will result in a much more secure Active Directory design for the organization.

2. Outline and explain briefly all the three elements, which are required to be carefully planned such as domains, forests, and organizational units. Be sure to point out that Active Directory design requires full understanding of the organization's requirements for services as well as data access.

3. Explain students that once the security boundaries are in place, the next step is to consider the environment.

4. Point out that these environments can be configured using security templates, which are text-based files. Be sure to mention that these files can be changed using the Security Templates snap-in to the Microsoft Management Console (MMC) or by using a text editor such as Notepad.

Teaching Tip	The way that you plan your domains, forests, and organizational units plays a critical role in defining your network's security boundaries.

Teaching Tip	Specifications for the three distinct environments can be found in Microsoft's Windows 2003 Security Guide, which can be downloaded at: www.microsoft.com/downloads/details.aspx?familyid=c3260bd0-2ebb-4496-ad07-7e9d55d0ef1f&displaylang=en.

Teaching Tip	Security Template is a standalone snap-in tool that users can use to define computer-independent security configurations.

Creating Baseline Servers Based on Roles

1. Outline three categories in which the environment needs of an organization falls, such as Legacy Client, Enterprise Client, and High Security category.

2. Point out that the idea behind these three environments is to provide a framework for evolving from a Legacy environment toward a High Security environment within a domain infrastructure. Be sure to mention that Windows Server 2003 ships with default setting values set to a secure state.

Legacy Client

1. Provide students with an overview of the Legacy Client. Point out that the Legacy Client settings are designed to work with member servers and domain controllers running Windows Server 2003, and clients running Microsoft Windows 98, Windows NT 4.0, and later versions of Windows operating systems.

2. Point out various templates for Legacy Client such as domain, domain controller, file server etc.

Enterprise Client

1. Provide students with an overview of the Enterprise Client. Point out that the Enterprise Client environment is defined as only having Windows Server 2003, Windows 2000 Professional, and Windows XP Professional computers in the environment. Mention that this environment allows use of more restrictive security templates for added security.

2. Point out various templates for Enterprise Client such as domain, domain controller, certificate services etc. as listed in the bullet points on page 30 in the text.

High Security

1. Provide students with an overview of High Security. Point out that the High Security settings are designed to work in an Active Directory domain with member servers and domain controllers running Windows Server 2003, and clients running Windows 2000,Windows XP, and later.

2. Be sure to mention that the servers may experience some impact on performance because the High Security settings are so restrictive.

3. Point out various templates for High Security such as domain, domain controller, bastion server etc. as listed in the bullet points on pages 30-31 in the text.

Teaching Tip	Microsoft's recommendations for which templates to use with the various roles are included in Windows 2003 Security Guide, which can be downloaded at: www.microsoft.com/downloads/details.aspx?familyid=c3260bd0-2ebb-4496-ad07-7e9d55d0ef1f&displaylang=en.

Quick Quiz 1

1. Which of the following is the Microsoft's recommended template for Windows Server 2003 domain controllers?
   a. Legacy Client - Domain.Controller.inf
   b. Enterprise Client – Domain.Controller.inf
   c. High Security - Domain.Controller.inf
   d. Enterprise Client – Member Server Baseline.inf
   Answer: b

2. Security templates are what kind of files?
   a. Text files
   b. Zip files
   c. .pdf files
   d. .tar files
   Answer: a

3. Which of the following operating systems are supported by High Security environment? (Choose all that apply.)
   a. Windows Server 2003
   b. Windows 2000
   c. Windows 98 SE
   d. Windows XP
   Answer: a, b, d

Server Roles

1. Provide students with an overview of the server roles. Point out that by identifying the role that each server plays, it is easier to determine which services and protocols are required.

2. Outline some of the common server roles that are found on a network as listed in the bullet points on page 32 in the text.

Establishing a Baseline Domain Controller

1. Provide students with a detailed overview of domain controllers. Mention some of its functions such as user logon processes, authentication, and directory searches etc.

2. Make sure that the students understand the importance of domain controllers and that these should only be accessible to qualified administrative staff.

3. Point out that the Domain Controller template requires a baseline group policy, making it similar in concept to a member server baseline policy. Be sure to mention that however, the policy is linked to the Domain Controllers OU; therefore, it takes precedence over the Default Domain Controllers policy.

4. Demonstrate students the installation of GPMC using Activity 2-1 on page 33 in the text.

5. Demonstrate students how to explore the default settings installed for domain controllers by using GPMC using Activity 2-2 on pages 33-34 in the text.

Teaching Tip	If GPO is not properly configured and tested, linking it to Domain Controllers OU could adversely affect the operation of the domain.

Establishing a Baseline Member Server

1. Provide students with an overview of member server baseline policy. Point out that the settings at the Member servers OU level define the common settings for all member servers in the domain.

2. Demonstrate students how to create the Member servers OU and delegate responsibility, using Activity 2-3 on pages 35-36 in the text.

3. Demonstrate students how to work with security templates by importing the Enterprise Client Member Server baseline template, using Activity 2-4 on pages 36-37 in the text.

Establishing a Baseline Infrastructure Server

1. Outline some of the network infrastructure services such as DNS, RADIUS, LDAP, Dynamic Host Control Protocol (DHCP), and PKI etc. Point out that Infrastructure services are often spread across various platforms and internal departments, making them difficult to secure against risks.

2. Explain various issues that arise on the network by running Microsoft DHCP service and what measures should be put into place for securing DHCP. Also, point out several changes that should be made to the baseline server template for servers that will run DHCP.

3. Outline various considerations for the security of internal DNS servers. Be sure to point out that in order to stop outside intruders from accessing the internal network of a company, the use of separate DNS servers for internal and Internet name is recommended.

Establishing a Baseline File Server

1. Explain why the file servers are a challenge to secure. Discuss this in terms of protocols such as NetBIOS, SMB, and CIFS that are required by applications for which services are provided by the file servers.

2. Outline various considerations for the security of file servers. Discuss DFS and FRS and how disabling them minimizes the attack surface of the file servers. Point out the importance of Internet Protocol Security (IPSec) filters in enhancing the level of security required for servers.

Establishing a Baseline Print Server

1. Explain to students that print servers also provide essential services that require the protocols such as NetBIOS, SMB, and CIFS. Mention that the network administrator is faced with the same issues in securing a print server as in securing a file server.

2. Outline various considerations for the security of print servers. Explain the feature of SMB packet digital signing that is enabled for servers in a High Security environment. Discuss also the Print Spooler service. Point out the importance of Internet Protocol Security (IPSec) filters in enhancing the level of security required for servers.

3. Demonstrate students how to work with security templates by importing the Enterprise Client Infrastructure Server template, using Activity 2-5 on page 42 in the text.

Establishing a Baseline Bastion Host

1. Explain what is bastion host and point out some of its most common uses such as Web servers, DNS servers, FTP servers, SMTP servers, and NNTP servers etc. Be sure to mention that it is also known as the DMZ (demilitarized zone), or screened subnet.

2. Explain why Group Policy cannot be applied to bastion host servers. Be sure to mention that Microsoft has recommended the High Security-Bastion Host.inf file to configure these servers.

3. Point out all-important considerations required for the security of a bastion host. Mention that like in other servers, the potential for successful attacks can be limited by disabling or removing all unnecessary services, protocols, programs, and network interfaces. Point out some of the services that are not essential to the proper operation of a bastion host as listed in the bullet points on page 45 in the text.

Teaching Tip	Microsoft's Security Guide has recommended the High Security-Bastion Host.inf file to configure these servers. Further details on bastion host can be found at: www.microsoft.com/technet/security/guidance/secmod127.mspx

Teaching Tip	It is also strongly recommended to perform a full backup of a bastion host server before applying the High Security-Bastion Host.inf security template.

Teaching Tip	Before you disable any service, be sure that you test the environment so that disabling the service will not adversely affect the operation of the applications you may be running.

Establishing a Baseline Internet Information Services Server

1. Provide students with an overview of the Internet Information Services (IIS) server. Be sure to mention that IIS is not installed by default on Windows Server 2003 and when it is installed, it is installed in a highly secure mode.

2. Explain all the three services that must be enabled in order to add Web server functionality.

3. Outline all the measures that must be performed manually for the security of IIS servers. Be sure to mention that in order to provide multiple layers of protection against attackers, URLScan has been integrated into the IIS LockdownWizard.

4. Demonstrate IIS Lockdown and URLScan tools, using Activity 2-6 on page 47 in the text. Note that IIS and URLScan 1.0 or URLScan 2.0 must be installed for this activity to be carried out. In addition, it may be required to change the Internet security settings to medium from Tools, Internet Options, Security in order to complete this activity.

Establishing a Baseline Internet Authentication Service Server

1. Provide students with an overview of the IAS server. Point out that it has the capability to authenticate users from Windows NT 4.0, Windows 2000, or Windows Server 2003 domains and it supports the Routing and Remote Access Service (RRAS).

2. Outline various recommended settings for making a security template for an IAS server. Remind students that when a member server baseline policy is established, all unneeded services and executable files are disabled or removed.

3. Remind students that in the standard edition of Windows Server 2003, IAS can have a maximum of 50 RADIUS clients and 2 remote RADIUS server groups. In Enterprise and Datacenter Editions, an unlimited number of RADIUS clients and remote groups can be configured by specifying an IP address range.

Client Roles

1. Provide students with an overview of the client roles. Discuss various reasons why client computers are bit harder to control.

2. Point out various security related issues in planning for the security of each client role. Mention that different security needs can be met by varying the strength of credentials enforced.

3. Demonstrate the investigation of additional security templates that can be used for configuring servers and clients, using Activity 2-7 on page 50 in the text.

Desktop

1. Discuss various considerations in configuring baseline security templates for desktops. Be sure to mention that desktop computer configuration ranges can vary depending on use.

Portables

1. Provide students with an overview of considerations in configuring baseline security templates for portables. Point out that security template consideration for portables will need to include accessing the network remotely, encryption, and virtual private networks (VPNs). In case of wireless LAN, security of wireless access point will be an issue.

2. Discuss the physical security issue associated with potables and how Encrypted File System (EFS) can be used to protect access to files in case of theft.

3. Explain briefly about the Connection Manager Administration Kit (CMAK) and how it can be used to reduce the support issues.

4. Ask students to investigate the checklists available in the Microsoft Security Guidance Kit for client machine configuration, using Activity 2-8 on page 52 in the text.

Kiosks

1. Provide students with an overview of considerations in configuring baseline security templates for kiosks and e-mail computers. Point out that these computers are tightly configured.

2. Point out that these computers have no direct connections to internal networks and additional considerations might include ensuring there is no device access. Introduce students to the concept of loopback policy and how it can be useful in case of kiosks.

Planning Security Based on Client Roles

1. Introduce students to the three areas of configuration while planning security for the machines, such as network security zones, security settings, and software restriction policies.

Planning Network Zones for Computer Roles

1. Explain the method of zone security. Explain briefly four zones that can be configured for security based on types of Web sites, such as Internet zone, Local intranet zone, Trusted zone and Restricted zone.

2. Discuss the security level assignment to each zone. Be sure to explain the custom level of security that can also be assigned to each zone.

Teaching Tip	The configuration of the local intranet zone requires having a good understanding of existing network configuration, proxy servers, and firewalls.

Planning and Configuring Security Settings

1. Provide students with an overview of Group Policy administrative templates, pointing out that .adm files are administrative templates. Discuss the information that is carried out by these files.

2. Discuss the storing locations of administrative templates files. Point out different local administrative templates and their uses.

3. Ask students to practice working with security settings by importing a template, then evaluating the settings, using Activity 2-9 on page 56 in the text.

Planning and Configuring Software Restriction Policies

1. Provide students with an overview of the Software Restriction Policies and discuss their features. Be sure to mention that software restriction policies are not meant to replace antivirus software.

2. Discuss various rules that can be created for exceptions to software restriction policies for specific software. Demonstrate how to enable certificates hash rules for software restriction policies, using Activity 2-10 on page 59 in the text.

Teaching Tip	For software restriction policies to take effect, users must update the policy settings by logging off from and then logging on to their computers.

Quick Quiz 2

1. Which of the following security zones consists of sites with a firewall or those specified to bypass the proxy server?
   a. Internet zone
   b. Extranet zone
   c. Local Intranet zone
   d. Trusted zone
   Answer: c

2. Which of the following services must be enabled in order to add Web server functionality to IIS servers?
   a. TCP/NetBIOS Helper Service
   b. HTTP SSL Service
   c. NLA Service
   d. DHCP Client service
   Answer: b

3. On which of the following types of client computers would you most likely use the highest level of security
   a. Developers computers
   b. Mobile or laptops
   c. Desktops
   d. Kiosks and e-mail computers
   Answer: d

Class Discussion Topics

1. Have students discuss the roles played by bastion host. What type of security template needs to be applied to such servers? What measure would they take in order to minimize the security risks? Before disabling any service, what precaution should they take?

2. Have students discuss various network infrastructure services. In their opinions, what major issues can arise of running DHCP service and how they can resolve them? In addition, what other changes should be made to the baseline server template for servers that will run DHCP?

3. Have students discuss the impact of flexible work environment on security template considerations. What are the major security issues associated with portable computers? What should they do in order to reduce the support issues?

Additional Projects

1. Have students research on major steps in restructuring the Active Directory design in case of merger of two organizations.

2. Have students research online on how to set up sites in the Local intranet zone.

3. Have students research online on how to create and test Connection Manager profiles for connections that use VPN with Layer Two Tunneling Protocol and Internet Protocol Security (L2TP/IPSec).

Additional Resources

1. WindowSecurity.com
   www.windowsecurity.com/articles/Group-Policy-Management-Console.html

2. T2seminars.com
   http://www.ts2seminars.com/resources/security_resources/index.htm

3. JSI Inc.com
   www.jsiinc.com

Technical Notes for Activities

1. The computer needs to have a domain set up for Activity 2-2. This can be done by running the wizard. Click Start, Run, type dcpromo, and press Enter.

2. While going through the Activity 2-2, pay special attention to the pop-up box on the console. Linking a Group Policy Object (GPO) or modifying the default GPO linked to the Domain Controllers OU will affect the entire domain. If you do not properly configure and test the GPO, linking it to Domain Controllers OU could adversely affect the operation of the domain.

3. Before you try to disable any service in case of bastion host, be sure that you test the environment so that disabling the service will not adversely affect the operation of the applications you may be running.

4. IIS and URLScan 1.0 or URLScan 2.0 must be installed for Activity 2-7 to be carried out.

5. For software restriction policies to take effect, users must update the policy settings by logging off from and then logging on to their computers.