



TestKingprep.com

**MCSE, CCNA, CCNP, OCP, CIW, JAVA, Sun Solaris, Checkpoint
World No 1 Cert Exams**

70-299

Congratulations!

You have purchased a TestKingprep.com Study Guide.

This study guide is a complete collection of questions and answers that have been developed by our professional & certified team.

You must study the contents of this guide properly in order to prepare for the actual certification test. The average time that we would suggest you for studying this study guide is approximately 10 to 20 hours and you will surely pass your exam. We guarantee it!

GOOD LUCK!

DISCLAIMER

This study guide and/or material is not sponsored by, endorsed by or affiliated with Microsoft, Cisco, Oracle, Citrix, CIW, Checkpoint, Novell, Sun/Solaris, CWNA, LPI, ISC, etc. All trademarks are properties of their respective owners.

Guarantee

If you use this study guide correctly and still fail the exam, send a scanned copy of your official score notice at:

Sales@TestKingprep.com

We will gladly refund the cost of this study guide or give you an exchange of study guide of your choice of the Free.

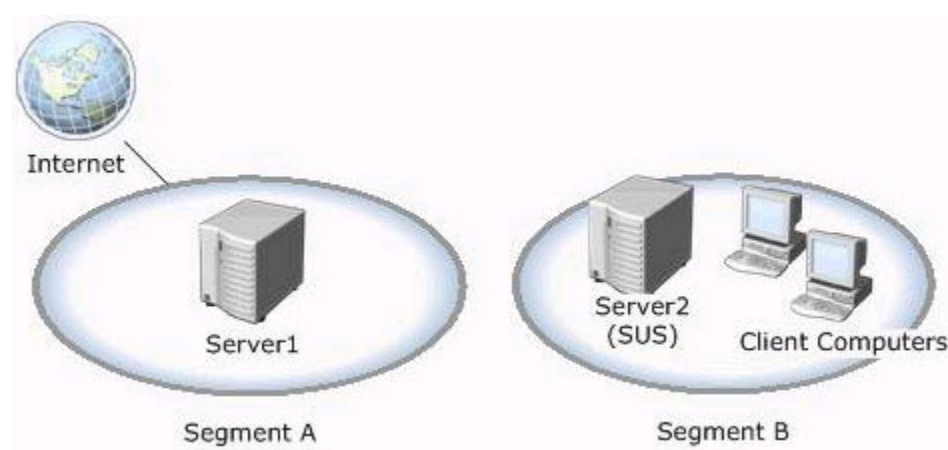
This material is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

A	Implementing, Managing, and Troubleshooting Security Policies
B	Implementing, Managing, and Troubleshooting Patch Management Infrastructure
C	Implementing, Managing, and Troubleshooting Security for Network Communications
D	Planning, Configuring, and Troubleshooting Authentication, Authorization, and PKI

Relevant objective of each question is mentioned along with question number.

Question: 1.(C)

You are the security administrator for Company. The network consists of two segments named Segment A and Segment B. The client computers on the network run Windows XP Professional. The servers run Windows Server 2003. Segment A contains a single server named Server1. Segment B contains all other computers, including a server named Server2. Company's written security policy states that Segment B must not be connected to the Internet. Segment A is allowed to connect to the Internet. There is no network connection between Segment A and Segment B. You can copy files from Segment A to Segment B only by using a CD-ROM to transport the files between the two segments. The network topology is displayed in the exhibit.



You are planning a patch management infrastructure. On Segment B, you install Software Update Services (SUS) on Server2. You configure Automatic Updates on all computers in Segment B to use `http://Server2` and to install security patches. You need to ensure that all computers in Segment B automatically install security patches. What should you do?

- A. Install SUS on Server1. Periodically copy the files in the Content folder and in the SUS root folder from Server1 to Server2.
- B. Install SUS on Server1. Periodically copy the files in the Content folder from Server1 to Server2. Copy the Approveditems.txt file from Server1 to the Windows folder on Server2.

- C. On Server1, periodically connect to the Microsoft Windows Update Catalog Web site and download new security patches. Copy the files to the Content folder on Server2.
- D. On Server1, configure Automatic Updates to use the URL of the Microsoft Windows Update Web site. Periodically copy the downloaded files and the Mssecure.xml file to the Content folder on Server2.

Answer: A

Explanation:

B – You must copy all items in the Content and SUS root folder. C – This is possible, but you would have to install the patches manually. D – Turning on AU would update Server1 does not provide files for Server2. The MBSA uses an XML-based catalog file, MSSecure.xml, to determine the security updates that are available. The catalog file is compressed and is stored in the MSSecure.cab file. If SUS is used to approve updates, it retrieves the Approveditems.txt file from the root of the IIS/SUS default website (<http://server2>) not the Windows folder. If you do not install SUS on Server1 there will be no Content folder (distribution point) on Server1.

Automatic Updates should not be turned on, on the SUS servers. SUS is a server component that, when installed on a server running Windows 2000, allows small and medium enterprises to bring critical updates from Windows Update inside their firewalls to distribute to Windows 2000 and Windows XP computers. The same Automatic Updates component that can direct Windows 2000 and Windows XP computers to Windows Update can be directed to a SUS server inside your firewall to install critical updates. Automatic Updates retrieves all critical updates and Microsoft Security Response Center security updates that are classified as moderate or important. Automatic Updates scans only for critical updates, but if its server that runs SUS contains updates other than critical ones, Automatic Updates receives and applies those as well. SUS receives critical and moderate security updates. Creating Distribution Points When you install a server that runs SUS, a distribution point is created on that server. When you synchronize the server with a parent server or with an external Web site, all the content on the Web site is downloaded to the distribution point. If new updates are downloaded, this distribution point is updated during every synchronization. During Setup, the distribution point is created in a virtual root (Vroot) named /Content. If you choose to maintain content on the public Web site instead of downloading the patches to the local server running SUS, this distribution point is empty except for the AUCatalog.cab file. AUCatalog.cab defines the updates that have been approved for deployment to clients. You can also create a distribution point on a server that is not running SUS. Such a server must be running IIS 5.0 or later. You can download and test packages on servers running SUS, and then download approved and tested packages to distribution points for client access. If your SUS design includes distribution points, perform the following tasks to create a distribution point:

- 1 Confirm that IIS is present.
- 2 Create a folder named \Content.
- 3 Copy all of the following items from the source server running SUS to the newly created \Content folder:

<root of the SUS Web site>\Aucatalog1.cab
<root of the SUS Web site>\Aurtf1.cab
<root of the SUS Web site>\approveditems.txt
All the files and folders under the \Content\cabs

4. Create an IIS Vroot called <http://<Servername>/Content> that points to the \content folder.

Question: 2.(B)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. Company's written security policy states that security patches must be manually installed on servers by administrators. You need to configure the network to comply with the written security policy. You need to maintain security patches by using the minimum amount of administrative effort. What should you do?

- A. Create a new organizational unit (OU) to contain all server computers. Create a new Group Policy object (GPO) and link it to the

- OU. Configure the GPO to disable Automatic Updates. Allow only administrators to start Automatic Updates.
- B. Create a new organizational unit (OU) to contain all server computers. Create a new Group Policy object (GPO) and link it to the OU. Configure the GPO to automatically download updates and notify when they are ready to be installed.
- C. Create a new organizational unit (OU) named Admins to contain all administrators. Create a second OU named Servers to contain all server computers. Create a new Group Policy object (GPO) and link it to the Admins OU. Configure the GPO to disable Automatic Updates.
- D. Modify the Default Domain Policy Group Policy object (GPO) to disable Windows Update and to disable Automatic Updates. Create a new organizational unit (OU) named Admins. Place all administrator accounts in the Admins OU. Block GPO inheritance on the Admins OU.

Answer: B

Explanation:

A – Cannot be done using Network Neighborhood. C – Scanning the finance subnet would report on all computers on the subnet, including non-finance computers. D – This option again would scan all systems in the domain, not just the finance once. The scan should be done from an administrative machine, not a users' machine. Objective: Implementing, Managing, and Troubleshooting Security for Network Communications Sub-Objective: 3.4.1 Monitor IPsec policies by using IP Security Monitor.

1. Planning a Host Name Resolution Strategy MCSA/MCSE Self-Paced Training Kit (Exams 70292 and 70-296): Upgrading Your Certification to Microsoft Windows Server 2003, Microsoft Press Chapter 7, The correct syntax is mbsacli /hf -i hosts.txt syntax. The -i flag is used to scan one or more Internet Protocol (IP) addresses. The mbsacli /hf -fh hosts.txt. The -fh flag causes the tool to scan the NetBIOS computer names specified in the named text file. You must specify one computer name on each line in the .txt file, up to a maximum of 256 names. The mbsacli /hf -r hosts.txt syntax. The -r flag is used to specify a range of IP addresses to be scanned. <http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q320454&ID=KB;ENUS;Q320454&&FR=1> Switches available with /hf flag

mbsacli /hf [-h hostmane] [-fh filename] [-i ipaddress] [-fip filename] [-r ipaddressrange] [-d domainname] [-n] [-sus SUS server|SUS filename] [-b] [-fq filename] [-s 1] [-s 2] [-nosum] [-sum] [-z] [-v] [-history level] [-nvc] [-o option] [-f filename] [-unicode] [-t] [-u username] [-p password] [-x] [-?] To Select Which Computer to Scan -h hostname - Scans the named NetBIOS computer name. The default location is the local host. To scan multiple hosts, separate the host names with a comma (.). -fh filename - Scans the NetBIOS computer names that are specified in the text file that you named. Specify one computer name on each line in the .txt file, to a maximum of 256 names. -i xxx.xxx.xxx.xxx - Scans the named IP address. To scan multiple IP addresses, separate each IP address with a comma. -fip filename - Scans the IP addresses that you specified in the text file that you named. Specify one IP address on each line in the .txt file, with a maximum of 256 IP addresses. -r xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx - Scans a specified range of IP addresses. Note You can use the previous switches in combination. For example, you can use a command-line with the following format:mbsacli /hf -h hostname1,hostname2 -i xxx.xxx.xxx.xxx -fip ipaddresses.txt -r yyy.yyy.yyy.yyy-zzz.zzz.zzz.zzz -d domainname - Scans a specified domain. -n - Scans all the computers on the local network. All computers from all domains in Network Neighborhood (or My Network Places) are scanned

Question: 3.(B)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The Company.com Active Directory domain contains 150 Windows Server 2003 computers and 7,500 Windows XP Professional client computers. The network is made up of 64 class C IP subnets that range from 172.16.0.0 through 172.16.63.0. The finance department uses 135 computers on the 172.16.9.0 /24 IP subnet. This subnet also contains computers that belong to other departments in the company. All finance department computers are members of the Company.com Active Directory domain. You need to produce a report that identifies which Microsoft security patches are not installed on the computers in the finance department. The report must contain information about only the finance department computers. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. Run Mbsacli.exe on a finance department computer with the option to scan computers in the Network Neighborhood.
- B. Run Mbsacli.exe on a finance department computer with the option to scan computers by using a list of individual IP addresses on the finance department computers.
- C. Run Mbsacli.exe on a finance department computer with the option to scan computers on the finance department IP subnet.
- D. Run Mbsacli.exe on a finance department computer with the option to scan computers in the Company.com Active Directory domain.

Answer: B

Explanation:

Since there are non-accounting computers on the subnet, the scan needs to be performed by individual IP. Objective: Implementing, Managing, and Troubleshooting Security for Network Communications Sub-Objective: 3.4.1 Monitor IPsec policies by using IP Security Monitor.

1. Planning a Host Name Resolution Strategy

MCSA/MCSE Self-Paced Training Kit (Exams 70-292 and 70-296): Upgrading Your Certification to Microsoft Windows Server 2003, Microsoft Press Chapter 7, The correct syntax is `mbsacli /hf -fh hosts.txt`. The `-fh` flag causes the tool to scan the NetBIOS computer names specified in the named text file. You must specify one computer name on each line in the .txt file, up to a maximum of 256 names. You should not use the `mbsacli /hf -i hosts.txt` syntax. The `-i` flag is used to scan one or more Internet Protocol (IP) addresses. You should not use the `mbsacli /hf -r hosts.txt` syntax. The `-r` flag is used to specify a range of IP addresses to be scanned. Switches available with `/hf` flag `mbsacli /hf [-h hostname] [-fh filename] [-i ipaddress] [fip filename] [-r ipaddressrange] [-d domainname] [-n] [-sus SUS server|SUS filename] [-b] [-fq filename] [-s 1] [-s 2] [-nosum] [-sum] [-z] [-v] [-history level] [-nvc] [-o option] [-f filename] [unicode] [-t] [-u username] [-p password] [-x] [-?]` To Select Which Computer to Scan `-h hostname` - Scans the named NetBIOS computer name. The default location is the local host. To scan multiple hosts, separate the host names with a comma (.). `-fh filename` - Scans the NetBIOS computer names that are specified in the text file that you named. Specify one computer name on each line in the .txt file, to a maximum of 256 names. `-i xxx.xxx.xxx.xxx` - Scans the named IP address. To scan multiple IP addresses, separate each IP address with a comma. `-fip filename` - Scans the IP addresses that you specified in the text file that you named. Specify one IP address on each line in the .txt file, with a maximum of 256 IP addresses. `-r xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx` - Scans a specified range of IP addresses. Note You can use the previous switches in combination. For example, you can use a command-line with the following format: `mbsacli /hf -h hostname1,hostname2 -i xxx.xxx.xxx.xxx -fip ipaddresses.txt -r yyy.yyy.yyy.yyy-zzz.zzz.zzz.zzz -d domainname` -Scans a specified domain. `-n` - Scans all the computers on the local network. All computers from all domains in Network Neighborhood (or My Network Places) are scanned

Reference:

Microsoft Baseline Security Analyzer (MBSA) version 1.2 is available, Microsoft Knowledge Base Article – 320454

Question: 4.(B)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional. Company has a main office and 150 branch offices located throughout the United States and Canada. The company does not use disk-imaging software. In the past, newly installed client computers were exploited by malicious Internet worms before you applied all security patches. You need to build and deploy client computers that will always have the least service packs, updates, and security patches. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. Install the operating system on the computers by using the original installation media. Use Windows Update immediately after the installation to apply updates and security patches.
- B. Install the operating system on the computers by using the original installation media. Configure Automatic Updates to immediately install updates and security patches.
- C. Create slipstream installation media that has the latest service pack. Install the operating system from the slipstream installation media. Implement a Software Update Services (SUS) server to install approved updates and security patches on client computers.
- D. Create slipstream installation media that has the latest service pack and includes Microsoft Baseline Security Analyzer (MBSA). Install the operating system from the slipstream installation media. Run MBSA immediately after installing the operating system.

Answer: C

Explanation:

A – This would allow for exploitation as the system is new and therefore unpatched and would have to download all patches. B – This is the same as the aforementioned. D – This does nothing to install patches. This is still a new install and a check just to see what patches are needed. Objective: Implementing, Managing, and Troubleshooting Patch Management Infrastructure Sub-Objective: 2.3.1 Deploy service packs and hotfixes on new servers and client computers. Considerations include slipstreaming, custom scripts, and isolated installation or test networks. Objective: Implementing, Managing, and Troubleshooting Patch Management Infrastructure Sub-Objective: 2.3.2 Deploy service packs and hotfixes to existing client and server computers.

Question: 5.(B)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computers are members of the domain. Company has a main office and six branch offices. Each branch office is connected to the main office by a dedicated leased line. All offices are connected to the Internet. Each office contains multiple servers and hundreds of client computers. You are planning a security patch management infrastructure. You install a Software Update Services (SUS) server in the main office and in each branch office. You configure the main office SUS server to store updates locally. You need to ensure that all client computers automatically install the latest security patches. You want to minimize the network traffic on the leased lines between the offices and on the connections to the Internet. Which two actions should you perform?

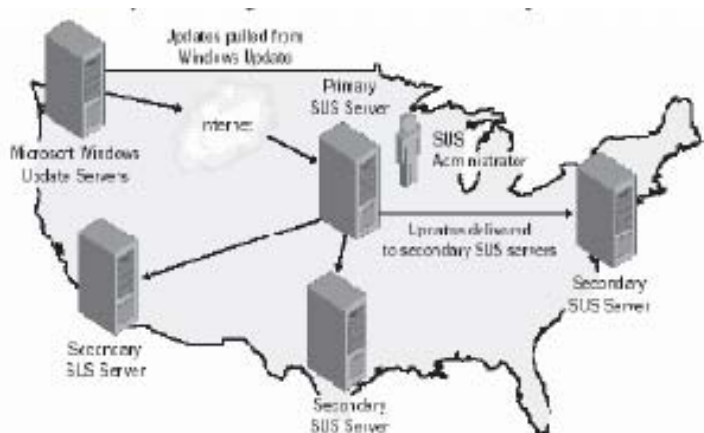
(Each correct answer presents part of the solution. Choose two)

- A. Configure the branch office SUS servers to maintain updates on the Microsoft Windows Update servers.
- B. Configure Automatic Updates on the branch office SUS servers to use the main office SUS server.
- C. Configure the branch office SUS servers to obtain updates from the main office SUS server.
- D. Configure Automatic Updates on the client computers to use the SUS server in the local office.
- E. Configure Automatic Updates on the client computers to use the main office SUS server.

Answer: C, D

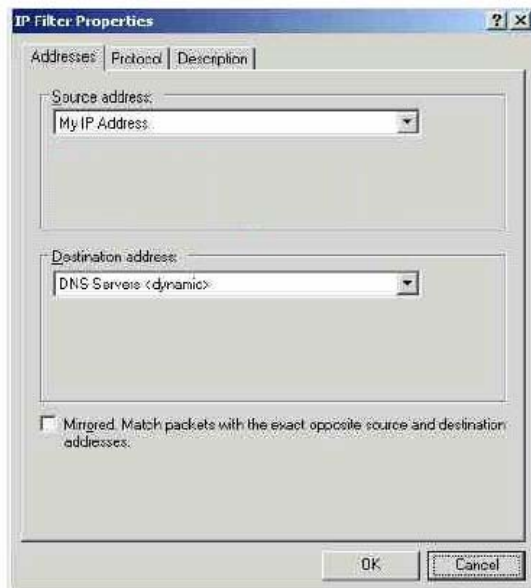
Explanation:

MCSA/MCSE Training Kit 70-299 5-20 Chapter: 5 Planning an Update Management Infrastructure Approval of updates using Software Update Services SUS is designed to be used in large organizations. Almost every aspect of the behavior can be customized. For example, the SUS server can download updates from Microsoft automatically, manually, or on a schedule specified by an administrator. SUS servers can be tiered as shown in Figure 5.4, with multiple SUS servers synchronizing updates between each other. This optimizes the use of your Internet connection by only requiring each update to be downloaded once for the entire organization. It also optimizes traffic on your wide area networks by allowing clients to download updates from a local SUS server.



Question: 6.(C)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows Server 2003 computers and Windows XP Professional client computers. The Active Directory domain consists of 10 Active Directory sites. Each Active Directory site contains a Windows Server 2003 computer that functions as a domain controller and a DNS server. A Windows Server 2003 computer named Company1 is a member of the Active Directory domain. Company1 is used to store confidential data in a Microsoft SQL Server 2000 database. You set up IP filters by using IPsec to control the types of inbound and outbound IP traffic that are allowed to and from Company1. After you configure the IP filters, you cannot resolve DNS names from Company1. The Addresses tab on the IP Filter Properties dialog box is shown in the exhibit.



This is the only rule in the IPsec policy that is relevant to DNS traffic. You need to enable Company1 to resolve DNS names. What should you do?

- A. Create an additional rule that allows DNS responses from the DNS servers to Company1.
- B. Change the Source address list to Any IP Address.
- C. Change the Destination Address list to A specific IP Subnet and type the IP subnet address That matches the IP subnet on Company1.
- D. Change the Destination address list to A specific IP Address and type an IP address of a DNS Server in the same IP subnet as Company1.

Answer: A

Question: 7.(C)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. You plan to deploy remote access to the network for users that work from home. Company's written security policy states the following remote access requirements:

- Users are allowed to use remote access during the day only.
- Enterprise Admins are never allowed to use remote access.
- Domain Admins are always allowed to use remote access.
- A user who is a member of both the Enterprise Admins group and the Domains Admins group is not allowed to use remote access.

You configure and enable Routing and Remote Access on a member server named Company1. You delete the predefined remote access policies. The remote access permission for all useraccounts in the domains is set to use remote access policies. You need to ensure that the remote access policies on Company1 comply with the written securitypolicy. What should you do? To answer, drag the remote access policy that should appear first inthe remote access policy list to the First Policy box. Continue dragging the appropriate remoteaccess policies to the corresponding umbered boxes until you list all required in the correct order.You might not need to use all numbered boxes.

Remote Access Polices

Domain Users/during day - Allow access

Domain Users/during night- Deny access

Domain Admins/all times - Allow access

Enterprise Admins/all times- Deny access

Enterprise Admins/during day - Deny access

Remote Access Policy List

First Policy

Drag policy here

Second Policy

Drag policy here

Third Policy

Drag policy here

Answer:

Remote Access Polices

Domain Users/during day - Allow access

Domain Users/during night- Deny access

Domain Admins/all times - Allow access

Enterprise Admins/all times- Deny access

Enterprise Admins/during day - Deny access

Remote Access Policy List

First Policy

Enterprise Admins/all times- Deny access

Second Policy

Domain Admins/all times - Allow access

Third Policy

Domain Users/during day - Allow access

Explanation:

The remote access policies are tried in order. The more specific remote access policies are placed in order ahead of the more general remote access policies. If the first policy in the ordered list of remote access policies does not match the connection attempt, the next policy is tried. The most specific policy is Enterprise Admins/all times Deny access, so it should be placed first. The next most specific policy is Domain Admins/all times Allow access. This policy should be placed second. The most general remote access policy is Domain Users/during day – Allow Access. This policy should be placed last. The reason for this is that everyone by default is part of the Domain Users group. If this was first or second, Enterprise Admins would be allowed to connect and Domain Admins would only be able to connect during the day. To process a connection attempt, the parameters of the connection attempt are compared to the user name, password, and dial-in properties of the user account and the configured remote access policies. Some general characteristics of remote access connection attempt processing are: If a connection attempt does not use a valid user name and password, then the connection attempt is denied. If there are no configured policies, then all connection attempts are denied. If the connection attempt does not match any of the remote access policies, then the connection attempt is denied. If the remote access permission of the user account for the remote access user is set to Deny Access, the connection attempt is always denied for that remote access user.

The only time that a connection attempt is allowed is when it matches the conditions of a remote access policy, and remote access permission is enabled either through the dial-in properties of the user account or through the remote access permission of the remote access policy (assuming the user's remote access permission is set to control access through remote access policies), and the parameters of the connection attempt match or conform to the parameters and conditions of the dial-in properties of the user account and the remote access policy profile properties. The figure depicts the specific processing of remote access connection attempts using the dial-in properties of the user account and remote access policies. Figure 7.15 assumes that the user name and password sent during the authentication process match a valid user account.

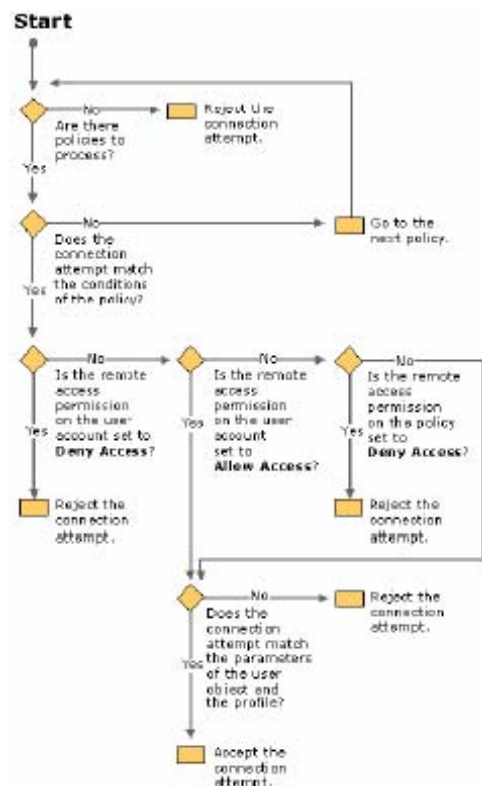
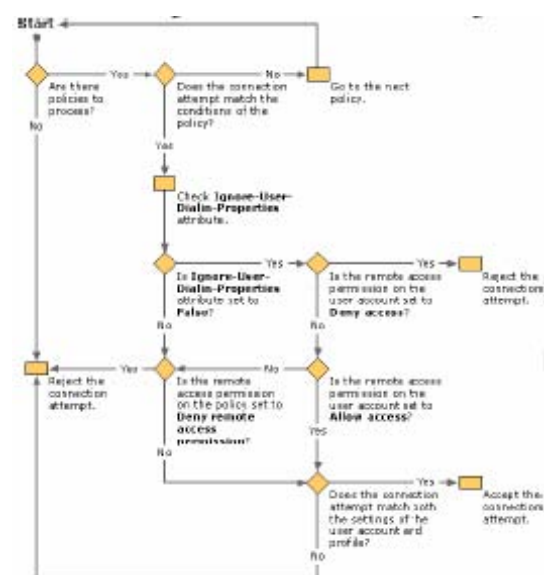


Figure Connection Attempt Processing Accepting a connection attempt When a user attempts a connection, the connection attempt is accepted or rejected, based on the following logic: The first policy in the ordered list of remote access policies is checked. If there are no policies, reject the connection attempt. If all conditions of the policy do not match the connection attempt, go to the next policy. If there are no more policies, reject the connection attempt. If all conditions of the policy match the connection attempt, check the value

of the Ignore-User-Dialin- Properties attribute. If the Ignore-User-Dialin-Properties attribute is set to False, check the remote access permission setting for the user attempting the connection. If Deny access is selected, reject the connection attempt. If Allow access is selected, apply the user account and profile properties. If the connection attempt does not match the settings of the user account and profile properties, reject the connection attempt. If the connection attempt matches the settings of the user account and profile properties, accept the connection attempt.

If the remote access permission is not set to Allow access or Deny access, the remote access permission must be set to Control access through Remote Access Policy. Check the remote access permission setting of the policy. If Deny remote access permission is selected, reject the connection attempt. If Grant remote access permission is selected, apply the user account and profile properties. If the connection attempt does not match the settings of the user account and profile properties, reject the connection attempt. If the connection attempt matches the settings of the user account properties and profile, accept the connection attempt. If the Ignore-User-Dialin-Properties attribute is set to True, check the remote access permission setting of the policy. If Deny remote access permission is selected, reject the connection attempt. If Grant remote access permission is selected, apply the profile properties. If the connection attempt does not match the settings of the profile properties, reject the connection attempt. If the connection attempt matches the settings of the profile properties, accept the connection attempt. The following illustration shows the logic of remote access policies.



Notes The profile and user account settings for the first matching policy are applied to the connection. If a connection does not match the profile or user account settings of the remote access policy, the additional remote access policies are not tried. A connection attempt might not match any of the remote access policies. If this is the case, the connection attempt is rejected regardless of the remote access permission setting on the user account. The remote access policies are tried in order. The more specific remote access policies are typically placed in order ahead of the more general remote access policies. The Ignore-User-Dialin-Properties attribute is a new feature for Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition that allows you to ignore all of the dial-in properties of a user account. For more information, see New features. You can configure IAS in Windows Server 2003, Standard Edition, with a maximum of 50 RADIUS clients and a maximum of 2 remote RADIUS server groups. You can define a RADIUS client using a fully qualified domain name or an IP address, but you cannot define groups of RADIUS clients by specifying an IP address range. If the fully qualified domain name of a RADIUS client resolves to multiple IP addresses, the IAS server uses the first IP address returned in the DNS query. With IAS in Windows Server 2003, Enterprise Edition, and Windows Server 2003, Datacenter Edition, you can configure an unlimited number of RADIUS clients and remote RADIUS server groups. In addition, you can configure RADIUS clients by specifying an IP address range. For examples of how different connection attempts are processed, see Remote access policies examples.

Question: 8.(C)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All

client computers run Windows XP Professional. All servers run Windows Server 2003. All computers on the network are members of the domain. Traffic on the network is encrypted by IPSec. The domain contains a custom IPSec policy named Lan Security that applies to all computers in the domain. The Lan Security policy does not allow unsecured communication with non-IPSec-aware computers. Company's written security policy states that the configuration of the domain and the configuration of the Lan Security policy must not be changed. The domain contains a multihomed server named Company1. Company1 is connected to the company network, and Company1 is also connected to a test network. Currently, the Lan Security IPSec policy applies to the network traffic on both network adapters on Company1. You need to configure Company1 so that it communicates on the test network without IPSec security. Company1 must still use the Lan Security policy when it communicates on the company network. How should you configure Company1?

- A. Configure a packet filter for the network adapter on the test network to block the Internet Key Exchange (IKE) port.
- B. Configure the network adapter on the test network to disable IEEE 802.1x authentication.
- C. Configure the network adapter on the test network to enable TCP/IP filtering, and then permit all traffic.
- D. Use the netsh command to assign a persistent IPSec policy that permits all traffic on the Network adapter on the test network.
- E. Assign an IPSec policy in the local computer policy that permits all traffic on the network adapter on the test network.

Answer: D

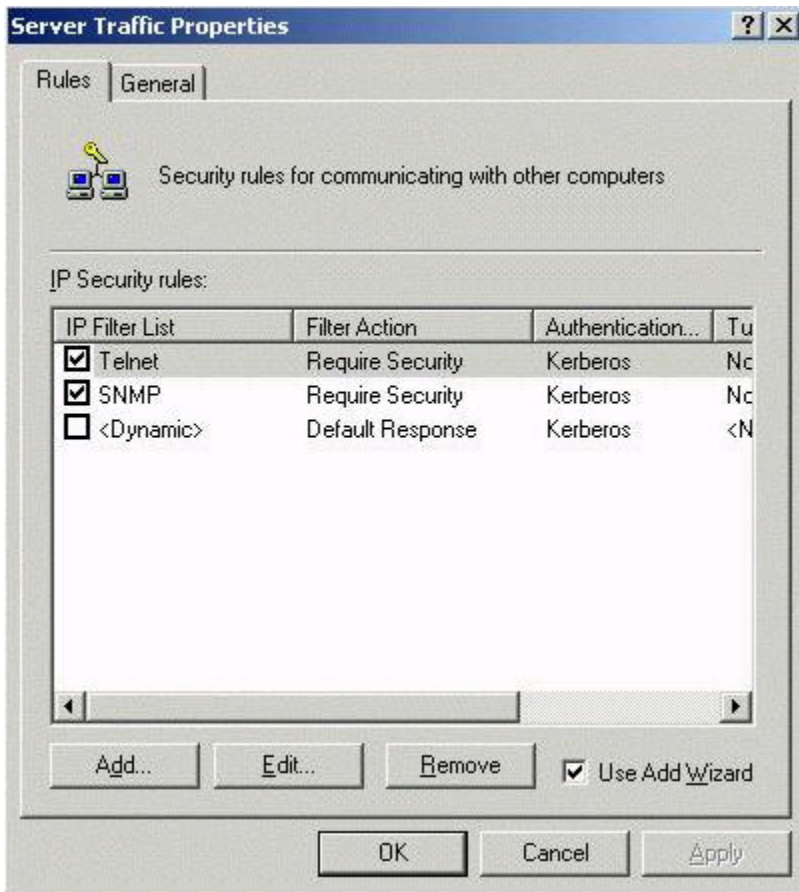
Explanation:

Assigning IPSec Policies Locally Each computer running Windows Server 2003 has one local GPO, which is also known as the local computer policy. When this local GPO is used, Group Policy settings can be stored on individual computers regardless of whether they are members of an Active Directory domain. The local GPO can be overridden by GPOs assigned to sites, domains, or OUs in an Active Directory environment that have higher precedence. On a network without an Active Directory domain (that is, a domain that does not have a domain controller running Windows 2000 or Windows Server 2003), the local GPO settings determine IPSec behavior because they are not overridden by other GPOs. Local policy assignment is a way to enable IPSec for computers that are not members of a domain. You can also create and assign persistent IPSec policy, which secures a computer even if a local IPSec policy or an Active Directory–based IPSec policy cannot be applied.

This policy adds to or overrides the local or Active Directory policy, and remains in effect regardless of whether other policies are applied or not. Persistent IPSec policies enhance security by providing a secure transition from computer startup to IPSec policy enforcement. Persistent policy also provides backup security in the event of an IPSec policy corruption, or if errors occur during the application of local or domain-based IPSec policy. To configure persistent policies, you must use the netsh ipsec static set store location=persistent command. When designing persistent IPSec policy, it is important to consider the potential impact of persistent policy on remote management. If local or domain-based IPSec policy is not applied and the persistent IPSec policy is the only policy that is applied, attempts to remotely diagnose an issue might be blocked by the persistent IPSec policy. To allow for remote management in case troubleshooting is required, it is recommended that you create appropriate permit filters when configuring persistent IPSec policy.

Question: 9.(C)

You are the security administrator of your network. The network consists of an Active Directory domain. All computers on the network are in the domain. The domain controllers and file servers on the network run Windows Server 2003. The client computers run Windows XP Professional. The file servers use a custom IPSec policy named Server Traffic. The Server Traffic policy contains rules to encrypt Telnet and SNMP traffic, as shown in the exhibit.



All client computers use the Client (Respond Only) IPsec policy. The default exemptions to IPsec filtering are disabled on the client computer. You want to configure the network so that Telnet, SNMP, and Kerberos traffic is encrypted by IPsec. You do not want to encrypt other network protocols. What should you do? (Each correct answer presents part of the solution. Choose two)

- A. On the client computers, enable the default exemptions to IPsec filtering.
- B. On the file servers, enable the default exemptions to IPsec filtering.
- C. On the file servers, configure the IPsec policy in the local computer policy to encrypt Kerberos traffic.
- D. Add a new rule to the Server Traffic policy to encrypt Kerberos traffic.
- E. Configure the Server Traffic policy to enable the Default Response rule.
- F. Configure the rules in the Server Traffic policy to use an authentication method other than Kerberos.

Answer: D, F

Question: 10.(C)

You are a security administrator for Company. Company consists of two divisions. One division is named Company Winery and is located in San Francisco. The other division is named Company Vineyard and is located in Paris. Each division is connected to the Internet by a 1.544 Mbps WAN connection. Company Winery consists of a single Active Directory forest named Companywinery.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Company Winery has a Microsoft SQL Server 2000 database that contains customer information. The SQL Server 2000 database is hosted on a Windows Server 2003 computer named Company1. Company Vineyard consists of a single Active Directory forest named Companyvineyard.com. All servers run Windows 2000 Server. All client computers run Windows 2000 Professional or Windows NT Workstation. All computers run the latest service packs.

To enable data replication, you configure a new Windows Server 2003 computer named Company2 in the Companyvineyard.com forest. You install SQL Server 2000 on Company2. Your database administrator configures the database on Company1 to replicate to Company2 every night. Management reports that a competitor acquired confidential customer data. You determine that the competitor intercepted customer data as it replicated from Company1 to Company2. You decide to use IPSec to protect customer data as it replicates.

You need to configure an IPSec policy to protect customer data as it replicates. What should you do?

- A. Configure the IPSec policy to use Authentication Header (AH) in transport mode with Kerberos authentication.
- B. Configure the IPSec policy to use Encapsulating Security Payload (ESP) with certificate-based authentication in tunnel mode.
- C. Configure the IPSec policy to use Authentication Header (AH) with certificate-based authentication in transport mode.
- D. Configure the IPSec policy to use Encapsulating Security Payload (ESP) with Kerberos authentication in tunnel mode.

Answer: B

Explanation:

IPSec can operate in two different modes: transport mode and tunnel mode. Typically, you should use transport mode to protect host-to-host communications. In transport mode, IPSec tunnels traffic starting at the transport layer, also known as layer 4. Therefore, IPSec in transport mode can encrypt the User Datagram Protocol/Transmission Control Protocol (UDP/TCP) protocol header and the original data, but the IP header itself cannot be protected. IPSec transports an application's data by adding an IPSec header and trailer to outgoing packets. Depending on the IPSec protocol used, the original contents of the outgoing packets will be encrypted. IPSec's position in the packet when functioning in transport mode is shown in Figure 8.1. The diagram shows IPSec using the ESP protocol. ESP is the most common of the two IPSec protocols because it provides both authentication and encryption. When you protect traffic sent directly between two hosts, you will almost always use IPSec transport mode.

When you protect traffic between a host and a network, or between two networks, you must use IPSec tunnel mode. Although transport mode stores the UDP/TCP header and the application data between an IPSec header and trailer, tunnel mode stores the entire original packet. The IP header, including the source and destination addresses, must be stored within the IPSec packet because the traffic is destined for a computer other than the computer to which the IPSec connection was established. If hosts on two networks are communicating across the Internet and all clients are IPSec enabled, transport mode can be used to encrypt traffic between individual hosts, or tunnel mode can be used to encrypt all traffic sent between the two networks. Naturally, tunnel mode is more convenient because it doesn't require every host to have IPSec enabled—but which is more secure? Tunnel mode is more secure than transport mode, in theory. Use transport mode when you communicate with one computer, and use tunnel mode when you communicate with an entire network, so when the decision calls for encapsulating or tunneling the IP header, use tunnel mode.

Question: 11.(D)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. You use Group Policy objects (GPOs) to manage client computers. Company has a wireless LAN (WLAN) that 50 employees who have portable computers use. Management reports that an additional 500 employees will receive portable computers in the next six months. These employees will have access to the WLAN. To address security concerns, management requires that portable computer users use smart cards to log on. You need to plan a WAN implementation to meet management requirements. You want to achieve this goal without affecting the application of Group Policy. Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

- A. Deploy WLAN hardware that supports IEEE 802.1x.
- B. Deploy WLAN hardware that supports 128-bit Wired Equivalent Privacy (WEP) keys.
- C. Implement an Internet Authentication Service (IAS) infrastructure.
- D. Implement a public key infrastructure (PKI).
- E. Implement a Routing and Remote Access infrastructure.
- F. Implement IPSec on all portable computers.

Answer: A, C, D

Question: 12.(D)

You are a security administrator for Company. The network contains a Windows Server 2003 computer that runs IIS. You use this server to host an Internet Web site for customer product purchasing. You plan to use SSL on this computer. You do not want customer to receive a certificate-related security alert when they use SSL to connect to your Web site. You need to select an appropriate certification authority (CA) to server as the issuer for your Web server SSL certificate.

What should you do?

- A. Use an online enterprise root CA.
- B. Use an online stand-alone root CA.
- C. Use a commercial CA.
- D. Use an offline stand-alone root CA.

Answer: C

Explanation:

Overview of Secure Sockets Layer (SSL) 11-5 -Used primarily for Internet communications Obtaining SSL Certificates To use SSL, the server must have a suitable public key certificate. Additionally, some SSL scenarios allow or require the client to use a public key certificate. SSL is one of the most common uses for public key certificates, and, as a result, you can obtain SSL certificates from a wide variety of places. Any organization with a computer running Windows Server 2003 can deploy Certificate Services to issue SSL certificates without any additional cost. These certificates are suitable for intranet scenarios, in which both the servers and the clients are controlled by a single organization. These certificates should not be used for communications that cross organizations, however. As with any public key infrastructure (PKI), SSL certificates can only be trusted if the root certification authority (CA) is trusted.

You can use Group Policy objects (GPOs) to add your CA to the list of trusted root CAs on clients on an intranet, but it is much more difficult to configure clients on the public Internet. For this reason, if you do not control the client computers, you should obtain an SSL certificate from a public CA that is trusted by the client applications that will be establishing a connection to your server. If the server is a Web server, your clients will be Web browsers. Microsoft Internet Explorer is configured by default to trust a large number of public CAs. Comparing SSL with IPsec IPsec is commonly used to provide the same services as SSL: authentication, privacy, and message integrity. However, the approach IPsec takes is different from that of SSL. IPsec is implemented by the operating system and is completely transparent to the applications that use IPsec. As a result, IPsec can be used to protect almost any type of network communication. IPsec also provides a flexible authentication scheme.

The Microsoft Windows implementation of IPsec allows clients and servers to authenticate each other by using either public key certificates or a shared secret. SSL, on the other hand, must be implemented by individual applications. Therefore, you cannot use SSL to encrypt all communications between two hosts. Additionally, SSL is less flexible than IPsec because it only supports authentication by means of public key certificates. SSL does provide several distinct advantages, however. Most significantly, SSL is supported by a wide variety of servers and clients, and the maturity of the standard has practically eliminated interoperability problems. Additionally, SSL allows one-way authentication, while IPsec requires both sides of a connection to authenticate. One-way authentication allows SSL to be used to authenticate the server without placing the burden of registering for a public key certificate on the client. This enables SSL to be used to encrypt communications with public Web sites while protecting the privacy of the end user by not revealing the details of a user certificate to the Web server. The other selections are for highly secure/internally controlled environments, primarily use for intranet and extranets.

Question: 13.(D)

You are a security administrator for Company. The network consists of two Active Directory forest named Company.com and public.Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. The network consists of an IEEE 802.11b wireless LAN (WLAN). Employees and external users use the WLAN. User accounts for employees are located in the Company.com forest. User accounts for external users are located in the public.Company.com forest. External users'

computers do not have computer accounts in the public.Company.com forest. To increase security, you upgrade the network hardware to support IEEE 802.1x. You configure a public key infrastructure (PKI). You issue Client Authentication certificates to employees, to client computers used by employees, and to external users. You need to configure the WLAN to authenticate employees and external users. What should you do?

- A. Configure each wireless access point to forward RADIUS requests to a server running Internet Authentication Service (IAS). Configure the IAS server to use a connection request policy to forward the requests to the appropriate forest.
- B. Configure each wireless access point to forward requests to an Internet Authentication Service (IAS) server in the Company.com forest. Configure the IAS server in the Company.com forest to use the Tunnel-Server-Endpt attribute.
- C. Use the Connection Manager Administration Kit (CMAC). Configure one connection profile for external users. Configure a second connection profile for employees.
- D. Establish a forest trust relationship between the Company.com forest and the public.Company.com forest.

Answer: A

Explanation:

Connection request policies Connection request policies are sets of conditions and profile settings that give network administrators flexibility in configuring how incoming authentication and accounting request messages are handled by the IAS server. With connection request policies, you can create a series of policies so that some RADIUS request messages sent from RADIUS clients are processed locally (IAS is being used as a RADIUS server) and other types of messages are forwarded to another RADIUS server (IAS is being used as a RADIUS proxy). This capability allows IAS to be deployed in many new RADIUS scenarios. With connection request policies, you can use IAS as a RADIUS server or as a RADIUS proxy, based on the time of day and day of the week, by the realm name in the request, by the type of connection being requested, by the IP address of the RADIUS client, and so on.

It is important to remember that with connection request policies, a RADIUS request message is processed only if the settings of the incoming RADIUS request message match at least one of the connection request policies. For example, if the settings of an incoming RADIUS Access-Request message do not match at least one of the connection request policies, an Access-Reject message is sent. For more information about how incoming RADIUS request messages from RADIUS clients are processed, see [Processing a connection request](#). **Authentication** You can set the following authentication options that are used for RADIUS Access-Request messages: **Authenticate requests on this server**.

Use a Windows NT 4.0 domain or the Active Directory directory service, or the local Security Account Manager (SAM) on Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition; for both authentication and the matching remote access policy and user account dial-in properties for authorization. In this case, the IAS server is being used as a RADIUS server. Forward requests to another RADIUS server in a remote RADIUS server group. Forward the Access-Request message to another RADIUS server in a specified remote RADIUS server group. If the IAS server receives a valid Access-Accept message that corresponds to the Access-Request message, the connection attempt is considered authenticated and authorized. In this case, the IAS server is being used as a RADIUS proxy. Accept the connection attempt without performing authentication or authorization. Do not check authentication of the user credentials and authorization of the connection attempt. An Access-Accept message is immediately sent to the RADIUS client.

This setting is used for some types of compulsory tunneling where the access client is tunneled before the user's credentials are authenticated. For more information, see [IAS and tunnels](#). **The protocol by which an entity on a network proves its identity to a remote entity.** Typically, identity is proved with the use of a secret key, such as a password, or with a stronger key, such as the key on a smart card. Some authentication protocols also implement mechanisms to share keys between client and server to provide message integrity or privacy. is MS-CHAP v2 or EAP-TLS, both of which provide mutual authentication. In mutual authentication, the access client proves that it is a valid access client to the authenticating server (the IAS server), and the authenticating server proves that it is a valid authenticating server to the access client.

When this authentication option is used, the Access-Accept message is returned. However, the authenticating server does not provide validation to the access client and mutual authentication fails. **802.1x authentication** For enhanced security, you can enable

IEEE 802.1x authentication. IEEE 802.1x authentication provides authenticated access to 802.11 wireless networks and to wired Ethernet networks. IEEE 802.1x minimizes wireless network security risks, such as unauthorized access to network resources and eavesdropping, by providing user and computer identification, centralized authentication, and dynamic key management. IEEE 802.1x supports Internet Authentication Service (IAS), which implements the Remote Authentication Dial-In User Service (RADIUS) protocol. Under this implementation, a wireless access point that is configured as a RADIUS client sends a connection request and accounting messages to a central RADIUS server.

The central RADIUS server processes the request and grants or rejects the connection request. If the request is granted, the client is authenticated, and unique keys (from which the WEP key is derived) can be generated for that session, depending on the authentication method chosen. The support that IEEE 802.1x provides for Extensible Authentication Protocol (EAP) security types allows you to use authentication methods such as smart cards, certificates, and the Message Digest 5 (MD5) algorithm. With IEEE 802.1x authentication, you can specify whether the computer attempts authentication to the network if the computer requires access to network resources whether a user is logged on or not. For example, data center operators who manage remotely administered servers can specify that the servers should attempt authentication to access the network resources. You can also specify whether the computer attempts authentication to the network if user or computer information is not available. For example, Internet service providers (ISPs) can use this authentication option to allow users access to free Internet services, or to Internet services that can be purchased.

A corporation can grant visitors with limited guest access, so that they can access the Internet, but not confidential network resources. Understanding 802.1x authentication IEEE 802.1x is a draft standard for port-based network access control, which provides authenticated network access to 802.11 wireless networks and to wired Ethernet networks. Port-based network access control uses the physical characteristics of a switched local area network (LAN) infrastructure to authenticate devices that are attached to a LAN port and to prevent access to that port in cases where the authentication process fails. During a port-based network access control interaction, a LAN port adopts one of two roles: authenticator or supplicant. In the role of authenticator, a LAN port enforces authentication before it allows user access to the services that can be accessed through that port. In the role of supplicant, a LAN port requests access to the services that can be accessed through the authenticator's port.

An authentication server, which can either be a separate entity or co-located with the authenticator, checks the supplicant's credentials on behalf of the authenticator. The authentication server then responds to the authenticator, indicating whether the supplicant is authorized to access the authenticator's services. The authenticator's port-based network access control defines two logical access points to the LAN, through one physical LAN port. The first logical access point, the uncontrolled port, allows data exchange between the authenticator and other computers on the LAN, regardless of the computer's authorization state. The second logical access point, the controlled port, allows data exchange between an authenticated LAN user and the authenticator. IEEE 802.1x uses standard security protocols, such as RADIUS, to provide centralized user identification, authentication, dynamic key management, and accounting. For an example of wireless access using the Internet Authentication Service (IAS) as a RADIUS server, see Wireless access example If you want to configure IAS for wireless access, see Checklist: Configuring IAS for wireless access If you want to configure IAS as a RADIUS server in a wireless environment, see Checklist: Wireless access To set up 802.1x authentication Open Network Connections Right-click the connection for which you want to enable or disable IEEE 802.1x authentication, and then click Properties. On the Authentication tab, do one of the following: To enable IEEE 802.1x authentication for this connection, select the Network access control using IEEE 802.1X check box.

This check box is selected by default. To disable IEEE 802.1x authentication for this connection, clear the Network access control using IEEE 802.1X check box. In EAP type, click the Extensible Authentication Protocol type to be used with this connection. If you select Smart Card or other Certificate in EAP type, you can configure additional properties if you click Properties and, in Smart Card or other Certificate Properties, do the following: To use the certificate that resides on your smart card for authentication, click Use my smart card. To use the certificate that resides in the certificate store on your computer for authentication, click Use a certificate on this computer.

To verify that the server certificate presented to your computer is still valid, select the Validate server certificate check box, specify whether to connect only if the server resides within a particular domain, and then specify the trusted root certification authority. To use a different user name when the user name in the smart card or certificate is not the same as the user name in the domain to which you are logging on, select the Use a different user name for the connection check box. To specify whether the computer should attempt authentication to the network if a user is not logged on and/or if the computer or user information is not available, do the following: To specify that the computer attempt authentication to the network if a user is not logged on, select the Authenticate as

computer when computer information is available check box. To specify that the computer attempt authentication to the network if user information or computer information is not available, select the Authenticate as guest when user or computer information is unavailable check box. This check box is selected by default.

Question: 14.(A)

You are the security administrator for Company. The network consists of a single Active Directory domain named Company.com. Servers on the network run Windows Server 2003. All computers are in the domain. You enable Remote Desktop for Administration on a member server named Company1. You want to allow members of a domain global group named Server Managers to create a Remote Desktop connection to Company1. The members of the Server Managers group are not in the Administrators group on Company1.

What should you do?

- A. Grant the Server Managers group Read permission on the Terminal Services service.
- B. Grant the Server Managers group Connect permission on the RDP-Tcp connection.
- C. Assign the Allow log on locally right to the Server Managers group.
- D. Add the Server Managers group to the Remote Desktop Users group.

Answer: D

Explanation:

To add users to the Remote Desktop Users group Open Computer Management. In the console tree, click the Local Users and Groups node. In the details pane, double-click the Groups folder.

Double-click Remote Desktop Users, and then click Add.... On the Select Users dialog box, click Locations... to specify the search location. Click Object Types... to specify the types of objects you want to search for. Type the name you want to add in the Enter the object names to select (examples): box. Click Check Names. When the name is located, click OK.

Note:

By default, the Remote Desktop Users group is not populated. You must decide which users and groups should have permission to log on remotely, and then manually add them to the group. To open Computer Management, click Start, and then click Control Panel. Click Performance and Maintenance, click Administrative Tools, and then double-click Computer Management. Related Topics

Question: 15.(A)

You are a security administrator for Company. The network consists of seven Active Directory domains. These domains are in the same Active Directory forest. All seven Active Directory domains operate at a Windows Server 2003 domain functional level. Each domain contains an internal Web site that is used to publish information to the Company managers. Access to the information on these Web sites must not be restricted to managers. An existing global group in each domain contains the management user accounts that exist in that domain. You need to restrict access to the internal Web sites to Company managers. You want to achieve this goal by using the minimum amount of administrative effort.

What should you do?

- A. Create a universal group in one of the Active Directory domains. Add the existing management global groups as members of the universal group. Assign only this universal group permissions to access the Web sites.
- B. Create a global group in one of the Active Directory domains. Add the existing management global groups as members of the global group. Assign only this global group permissions to access the Web sites.
- C. Create a domain local group in one of the Active Directory domains. Add the existing management global groups as members of the domain local group. Assign only this domain local group permissions to access the Web sites.
- D. Assign only the existing management global permissions to access the Web sites.

Answer: A

Explanation:

The members that each type of security group scope can have depends on the domain functional level. When the domain functional level is set to Windows 2000 native mode or higher, each type of group can contain the following members:

- Universal:** accounts from any domain, global groups from any domain, and universal groups from any domain
- Global:** accounts from the same domain, and global groups from the same domain
- Domain local:** accounts from any domain, global groups from any domain, universal groups from any domain, and domain local groups from the same domain

Objective: Planning, Configuring and Troubleshooting Authentication, Authorization and PKI

Sub-Objective: 4.2.2 Plan security group scope.

Domain Migration Cookbook Chapter 2: Domain Upgrade

Global Groups Windows 2000 global groups are effectively the same as Windows NT global groups. In terms of membership, they have domain-wide scope, but can be granted permissions in any domain, even in other forests and earlier version domains as long as a trust relationship exists.

Universal Groups Universal groups can contain members from any Windows 2000 domain in the forest, but cannot contain members from outside the forest. You can grant universal groups permissions in any domain, even in other forests, as long as a trust relationship exists.

Although universal groups can have members from mixed mode domains in the same forest, the universal group will not be added to the access token of these members because universal groups are not available in mixed mode. You can add users to a universal group, but it is recommended that you restrict universal group membership to global groups. Universal groups are available only in native mode domains.

Use of Universal Groups Universal groups have a number of important characteristics. You can use universal groups to build groups that perform a common function within an enterprise. One example might be virtual teams. The membership of such teams in a large company would probably be nationwide or even worldwide, and almost certainly forest-wide, with the team resources being similarly distributed. Universal groups could be used as a container in these circumstances to hold global groups from each subsidiary or department, with a single access control entry (ACE) for the universal group to protect the team resources. In using universal groups, an important factor to consider is that while global and domain local groups are listed in the global catalog (GC), their members are not, whereas universal groups and their members are listed, a fact that has implications for GC replication traffic. Exercise care in the use of universal groups.

As a guide, if your entire network has high-speed connectivity, you can simply use universal groups for all of your groups and benefit from not having to bother with managing global groups and domain local groups. If, however, your network spans wide area networks (WANs), you can improve performance in several ways by using global groups and domain local groups. If you use global groups and domain local groups, you can also designate any\ widely used groups that are seldom changed as universal groups.

Universal Groups and Access Tokens The previous discussion of universal group membership touched on the fact that universal groups can contain members from mixed mode domains, but that such members will not have the universal group's SID in their access token. This is a consequence of the way access tokens are created in Windows 2000. When a user logs on to a Windows 2000 native mode domain and has been authenticated, the Local Security Authority (LSA) on the domain controller where the user was authenticated retrieves the user's global group memberships.

The LSA then passes this information down to the workstation, where it is used to build the user's access token. At the same time, the LSA queries the GC for the user's universal group memberships, which it also passes to the workstation. If a user is a member of a universal group, the SID of that group is included in the access token on the workstation, and is added to the authorization data in the TGT issued by the KDC. Universal groups are not added to access tokens at any other time for example, when impersonation tokens are created at member servers. As a consequence, if the universal group SID is not available when the user logs on for example, where the user is logging on to a mixed mode domain it will not be added subsequently.

Nesting Groups It is recommended that you do not create groups with more than 5,000 members. This guideline is based on the fact that updates to the Active Directory store have to be capable of being made in a single transaction. Because group memberships are stored in a single multivalued attribute, a change to the membership would result in the whole attribute in other words, the whole membership list having to be updated in a single transaction.

Microsoft has tested and supports group memberships of up to 5,000 members. You can get around this limitation by nesting groups to increase the effective number of members. A further consequence is that you also reduce the replication traffic caused by replication of group membership changes. Your nesting options depend on whether the domain is in native mode or mixed mode. The following list describes what can be contained in a group that exists in a native mode domain. These rules are determined by the

scope of the group.

Universal groups can contain user accounts, computer accounts, other universal groups, and global groups from any domain.

Global groups can contain user accounts from the same domain and other global groups from the same domain.

Domain local groups can contain user accounts, universal groups, and global groups from any domain. They also can contain other domain local groups from within the same domain.

Local groups can contain global groups and user accounts from trusted domains.

Global groups can contain only user accounts.

This list describes what security groups in a mixed mode domain can contain:

References:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;326265>

Description of the Group Scopes That You Can Use to Help Secure Active Directory Objects

<http://support.microsoft.com/default.aspx?scid=kb;en-us;318862>

Universal Group Scope Is Incorrectly Documented in Windows 2000 Help

Question: 16.(D)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All domain controllers run Windows Server 2003. All client computers run Windows XP Professional. Users store files on a server named Company1. These files are confidential and must be encrypted at all times while on Company1. You configure a new certification authority (CA) and issue certificate that support Encrypting File System (EFS) to all users. Users report that they cannot encrypt files that are stored on Company1. They report that they can encrypt files that are stored locally on their client computers. You need to ensure that users can encrypt files that are stored on Company1.

What should you do?

- A. Enroll Company1 for a Computer certificate that supports file encryption.
- B. Configure a new EFS recovery agent. Deploy the EFS recovery agent by using Active Directory.
- C. Configure the Company1 computer account to be trusted for delegation.
- D. Enroll each client computer for a Computer certificate that supports file encryption.

Answer: C

Explanation:

Unable to Encrypt Files If you find that you are unable to encrypt files or folders, one of the following might be the cause: The file is not an NTFS volume. You do not have Write access to the file. If you are having trouble encrypting a remote file, check to see that your user profile is available for EFS to use on that computer (this typically means having a roaming user profile), make sure the remote computer is trusted for delegation, and make sure your account is configured to enable delegation. Sensitive accounts are not enabled for delegation by default, so users like Enterprise Administrator might not be able to encrypt or decrypt files remotely.

Note:

Sometimes users think that a file is not encrypted because they can open it and read the file. You can verify whether a file is encrypted by checking the file's attributes. For more information about formatting volumes as NTFS, see Windows XP Professional Help and Support Center. For more information about the encryption process, requirements, and procedures, see "Encrypting and Decrypting By Using EFS" earlier in this chapter.

For more information about remote EFS operations, see "Remote EFS Operations in a File Share Environment" earlier in this

chapter. Unable to Decrypt Remote Files The following are the major causes of and solutions for remote decryption failure (usually indicated by an "Access is denied" message): The computer on which the encrypted file is stored is not trusted for delegation. Every computer that stores encrypted files for remote access must be trusted for delegation. To check a computer's delegation status, open the computer's properties sheet in the Active Directory Users and Computers snap-in. The user account that EFS needs to impersonate cannot be delegated.

To check a user's delegation status, open the user's Properties sheet in the Active Directory Users and Computers snap-in. The user's profile is not available. Using roaming user profiles is the solution for this problem. One of the user's profiles is available, but it does not contain the correct private key. Using roaming user profiles is the solution for this problem. For more information about the decryption process, requirements, and procedures, see "Encrypting and Decrypting By Using EFS" earlier in this chapter. For more information about remote EFS operations, see "Remote EFS Operations in a File Share Environment" earlier in this chapter.

Question: 17.(A)

You are a security administrator for Company. The network consists of a single Active Directory forest that contains three domains in a single domain tree. All servers run Windows Server 2003. All computers are members of the domains. The functional level of the forest is Windows 2000. The functional level of each domain is Windows Server 2003. All users in the forest are in the root domain. The two child domains contain client computers accounts and server accounts. Only the root domain contains global catalog servers. Company uses an application that stores data in a custom application directory partition. The application runs on domain controllers in all three domains. You add the users that manage the data in the custom application directory partition to a global group named App Managers. You add the App Managers group to a domain local group named App Data. You assign the App Data group the Allow – Modify permission for all objects in the custom application directory partition. Some users in the App Managers group report that they receive an Access Denied message when they attempt to access the application data. Other users in the App Managers group can successfully access the application data in the application directory partition. You need to ensure that all users in the App Managers group can access the application data successfully. What should you do?

- A. Raise the functional level of the forest to Windows Server 2003.
- B. Change the scope of the App Data group to universal.
- C. Install a global catalog server in the two child domains.
- D. Create a two-way shortcut trust relationship between the two child domains.
- E. Assign the App Managers group the Allow – Allowed to Authenticate permission on all domain controllers that run the application.

Answer: B

Question: 18.(D)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers. You install Certificate Services to issue certificates to employees for secure e-mail encryption and Web site authentication. You revoke the certificates used by an employee when that employee leaves the company. Several thousand certificates are currently revoked, and multiple revocations occur daily.

Company e-mail and Web applications already use strong revocation checking of certificates. You need to reduce the time it takes for client computers to find out about certificate revocations and to process certificate revocation information. You also need to limit the negative impact that this change will have on network performance. What should you do?

- A. In the Certification Authority console, open the Revoked Certificates properties. Set the Delta Certificate Revocation List (CRL) publication interval to one hour.
- B. In the Certification Authority console, open the Revoked Certificates properties. Set the full Certificate Revocation List (CRL) publication interval to one hour.
- C. In the Certification Authority console, highlight Revoked Certificates, and then select the option to publish a full CRL after you revoke a certificate.
- D. In the Certification Authority console, highlight Revoked Certificates, and then select the Refresh option.

Answer: A

Explanation:

Certificate revocation A certificate has a specified lifetime, but CAs can reduce this lifetime by the process known as certificate revocation. The CA publishes a certificate revocation list (CRL) that lists serial numbers of certificates that it regards as no longer valid. The specified lifetime of CRLs is typically much shorter than that of a certificate. The CA might also include in the CRL the reason the certificate has been revoked. A revocation might occur because a private key has been compromised, because a certificate has been superseded, or because an employee has left the company. The CRL also includes the date the certificate was revoked. During signature verification, applications can check the CRL to determine whether a given certificate and key pair are still trustworthy.

Applications can also determine whether the reason or date of the revocation affects the use of the certificate in question. If the certificate is being used to verify a signature, and the date on the signature precedes the date of the revocation of the certificate by the CA, the signature can still be considered valid. **Off the Record:** Most applications do not analyze the reason code. If a certificate is revoked, it's revoked. The reason code just isn't that important. To reduce the number of requests sent to the CA, the CRL is generally cached by the client, which can use it until it expires. If a CA publishes a new CRL, applications that have a valid CRL do not usually use the new CRL until the one they have expires. **Installing, Configuring, and Managing Certification Services - Off the Record:**

The CRL contains the reason code you select for revoking the certificate. Before you select the reason code, think about whether you really want everyone who can access the CRL to know why you revoked it. If you did have a key compromise or a CA compromise, are you ready for that to be public information? If not, just select Unspecified. Clients discover that a certificate has been revoked by retrieving the certificate revocation list (CRL). There are two kinds of CRLs: full CRLs, which contain a complete list of all of a CA's revoked certificates, and delta CRLs. Delta CRLs are shorter lists of certificates that have been revoked since the last full CRL was published. After a client retrieves a full CRL, the client can download the shorter delta CRL to discover newly revoked certificates. **See Also:** For detailed information about CRLs, read the white paper "Troubleshooting Certificate

<http://www.microsoft.com/technet/prodtechnol/winxppro/support/tshtcrl.mspix>

Troubleshooting Certificate Status and Revocation Optimizing Delta CRLs While in itself, Delta CRLs optimize the revocation checking process, you can further optimize the Delta CRL process by reducing the number of Base CRL fetches. This means that any client who has that oldest Base CRL will not be forced to download a new Base CRL until it expires. This minimizes the number of times a Base CRL is retrieved by the client, but increases the size of the Delta CRL. The Windows .NET Certificate Authority is primarily configured to ensure that the smallest Delta CRL sizes are used. If it is desired to optimize Base CRL usage, longer lifetimes should be applied to the BaseCRL publication period.

<http://www.microsoft.com/technet/security/topics/crypto/tshtcrl.mspix?#i>

Troubleshooting Certificate Status and Revocation Delta CRLs One of the biggest decisions faced by a CA administrator is determining the publication schedule for CRLs. If a CA publishes a complete CRL frequently, then clients are aware of a newly revoked certificate very quickly. However, this causes higher amounts of network traffic due to the more frequent downloading of the updated CRL to all clients. If a CRL publishes CRLs less often, this reduces the amount of network traffic, but increases the latency before a client is aware of a newly revoked certificate.

If a CA revokes a large number of certificates, the size of the base CRL can grow to be larger than 1 MB in size if large numbers of certificates are revoked. If the CRL is published at frequent intervals, this can result in problems for clients connecting over slow connections. Alternatively, if the base CRL is published at longer intervals, this can result in the CRL information being out of date and reducing the validity of the CRL information. Delta CRLs, defined in RFC 2459, address these problems, by publishing changes to a Base CRL (bCRL), in a smaller file known as a Delta CRL (sCRL). When Delta CRLs are implemented, a client can download a Base CRL at longer intervals, and then download smaller Delta CRLs at shorter intervals to validate any presented certificates. The Delta CRLs can be published at very short intervals, such as once an hour, to increase the confidence in the certificates being validated. All of the time information stored in CRLs is stored as UTC.

Note:

This does not eliminate the requirement to download the larger Base CRLs. The Base CRL must be downloaded initially and when the previous Base CRL expires. The Delta CRL can force the client to retrieve a more recent Base CRL even though the current Base CRL is still time valid. This is achieved by having the Delta CRL point to a higher number Base CRL. When Delta CRLs are implemented, only changes from a Base CRL are published in a Delta CRL, resulting in a reduction in the size of the CRLs downloaded to the clients. This reduction in size allows for more frequent publishing of the CRL with both a minimal impact on the network infrastructure, and an improvement on the up-to-datedness of CRL information.

Publishing CRLs If you need to download a file from a server, you might access the file in several different ways. If you're logged onto the computer locally, you would use Windows Explorer to navigate to the folder containing the file. If you were on a different computer on the same network, you might map a drive to the server and download the file from a shared folder. If the server was behind a firewall and running IIS, you could open a Web browser to retrieve the file. Having multiple ways to retrieve a file from a server is important, especially when the server will be accessed by a variety of different clients. Certificate Services enables clients to retrieve CRLs by using a wide variety of different protocols: shared folders, Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Lightweight Directory Access Protocol (LDAP). By default, CRLs are published in three different locations. For clients accessing the CRL from a shared folder, they are located in the \\Server\CertEnroll\ share, which is created automatically when Certificate Services is installed. Clients who need to retrieve the CRL by using LDAP can access it from CN=CAName,CN=CAComputer-Name,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=Forest-RootNameDN. Web clients can retrieve the CRLs from http://Server/certenroll/. Though the default locations are sufficient for most organizations, you can add locations if you need to. In particular, you must add a location if you are using an offline root CA, since the CA will not be accessible by clients under normal circumstances. Additionally, if certificates are used outside your private network but your CA is behind a firewall, you should publish your CRL to a publicly accessible location.

Question: 19.(D)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Company hosts Web applications for customers. Each customer is a company that has multiple employees who require access to the Web application. Each customer has one Web application. Each Web application is configured as a virtual directory. You configure a user account for each customer. You assign this account permission to read the virtual directory that contains the customer's Web application. You need to ensure that employees can access only their company's Web application. You must accomplish this task without requiring customers to disclose passwords. What should you do?

- A. Configure anonymous access for each virtual directory. Configure each virtual directory to use the customer's assigned user account. Leave the password assigned to the user account blank.
- B. Configure Microsoft .NET Passport authentication for each virtual directory. Instruct each employee of each customer that requires access to the Web site to enroll for a new .NET Passport.
- C. Configure a certification authority (CA). Issue certificates to each employee of each customer that requires access to the Web site. Configure many-to-one certificate mapping.
- D. Acquire a Server Authentication digital certificate from a public certification authority (CA). Configure the Web server to use this certificate and to require SSL. Distribute a copy of the Server Authentication certificate to each employee of each customer that requires access to the Web site.

Answer: C**Explanation:**

Anonymous would allow access to any of the websites. Microsoft .NET Passport would have the user use passwords. 11 Deploying, Configuring, and Managing SSL Certificates IIS cannot process client certificates unless you have previously installed a server certificate and enabled HTTPS. There are two ways to improve the security of client certificates. First, you can use client certificate mapping to restrict access to users with specific certificates. (You can also use client certificate mapping to control authorization by mapping the certificates to existing user accounts.) Second, you can configure a certificate trust list (CTL) to reduce the number of root CAs that can issue certificates to your users. One-to-one client certificate mapping Client certificate mapping has two modes: one-to-one and many-to-one. One-to-one certificate mapping relates a single exported certificate to an Active Directory user account.

When Web users present the certificate, they will be authenticated as if they had presented a valid user name and password. Many-to-one client certificate mapping Many-to-one certificate mapping uses wildcard matching rules that verify whether a client certificate contains specific information, such as the issuer or subject. This mapping does not identify individual client certificates; it accepts all client certificates fulfilling the specific criteria. If a client gets another certificate containing all the same user information, the existing mapping will still work. Certificates do not need to be exported for use in many-to-one mappings. To add many-to-one certificate mappings, follow this procedure:

- 1 View the properties for the Web site, and then click the Directory Security tab.
- 2 Click the Edit button in the Secure Communications box.
- 3 Select the Enable Client Certificate Mapping check box, and then click the Edit button.
- 4 Click the Many-1 tab, and then click the Add button.
- 5 On the General page, type a name for the rule in the Description box. Click Next.
- 6 On the Rules page, click New to add a rule. Editing rule properties for many-to-one client certificate mappings
 7. In the Edit Rule Element dialog box, click the Certificate Field list to choose either Issuer or Subject. Select Issuer to filter based on the CA that issued the certificate. Choose Subject to filter based on who the certificate was issued to. After completing the rule element, click OK. Security Alert When creating certificate mapping rules, keep in mind how easy it is to create your own root CA. Attackers could easily create their own root CA using your domain names. To prevent this type of impersonation, use certificate mapping along with a certificate trust list.
 - 7 To add an additional rule, return to step 6.
 - 8 Click Next.
 - 9 On the Mapping page, click Refuse Access to reject logons that match the criteria, or click Accept This Certificate For Logon Authentication to map matching certificates to a user account. If you choose to accept the certificate, complete the Account and Password boxes. Click Finish. If prompted, confirm the password and then click OK. Before you can authenticate users with client certificates, you must issue client certificates. If the users are members of an Active Directory domain and you are using an enterprise CA, auto-enrollment is the most efficient way to enroll users. Web servers are often used to communicate with users outside of your organization, however. For these users, you should use Web enrollment. The exercise at the end of this lesson demonstrates the process of enrolling a user certificate by using Web enrollment and then authenticating that user to IIS.

Question: 20.(D)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows Server 2003 computers and Windows XP Professional client computers. You install Certificate Services on two Windows Server 2003 computers named Company1 and Company2. Company1 is the root certification authority (CA) and Company2 is the subordinate CA. You configure the root CA certificate with a validity period of eight years. You configure the subordinate CA certificate with a validity period of two years. You create a custom User certificate type that has a validity period of three years. You allow employees to enroll for this user certificate by using Company2. You discover that all issued certificates do not remain valid for three years as expected. You need to ensure that the custom User certificates are issued with validity period of three years. What should you do?

- A. Generate a new CA certificate for Company1 with a validity period of three years.
- B. Generate a new CA certificate for Company2 with a validity period of four years.
- C. Create a new custom User certificate type with a validity period of four years.
- D. Create a new custom Administration certificate type with a validity period of three years.

Answer: B

Explanation:

Validity and renewal periods Certificate-based cryptography uses public-key cryptography to protect and sign data. Over time, evildoers can obtain data protected with the public key and attempt to derive the private key from it. Given enough time and resources, this private key could be compromised, effectively rendering all protected data unprotected. Also, over time, the names guaranteed by a certificate may need to be changed. Because a certificate is a binding between a name and a public key, when either of these change, the certificate should be renewed. Validity periods Certificates are enabled for a specific length of time, which is the validity period. This time is expressed in a length of time beginning from when a certificate is issued. When that length of time is

reached, the certificate is no longer valid and cannot be trusted. Because an expired certificate can cause problems, certificates can be renewed to extend their validity period. Renewal periods A renewal period is the amount of time prior to the end of the validity period when the subject will renew the certificate using autoenrollment. Renewing the certificate during this interval ensures that last-minute requests for certificate renewal can be serviced before certificate expiration to allow uninterrupted use of the certificate.

Question: 21.(A)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows Server 2003 computers and Windows XP Professional client computers. A Windows Server 2003 computer named Company1 is a member of a workgroup. Company1 hosts a knowledge management application that is accessed from the network. Contract employees require access to the knowledge management application. However, you do not want contract employees to have the right to create other user accounts on Company1. You need to assign the contract employees appropriate permissions to use the application on Company1.

What should you do?

- A. Create the user accounts in the Active Directory domain. Place the user accounts in the default Authenticated Users group in the Active Directory domain, and then assign this group appropriate permissions on Company1.
- B. Create the user accounts in the Active Directory domain. Place the user accounts in the default Domain Users group in the Active Directory domain, and then assign this group appropriate permissions on Company1.
- C. Create the user accounts in the local accounts database on Company1. Place the user accounts in the default Users group on Company1, and then assign this group appropriate permissions on Company1.
- D. Create the user accounts in the local accounts database on Company1. Place the user accounts in the default Power Users group on Company1, and then assign this group appropriate permissions on Company1.

Answer: C

Explanation:

Since this server is not in a domain, access can only be granted by using the local SAM database. Access can be granted by using the default Users group even though Power Users would also work. However, Power User is probably more permissions than is needed to run the application. Of course this would depend on how the application was written. However, this multiple users will be accessing this server the question does not mention that the users will need the 'Access this computer from the network' right.

The Principle of Least Privilege In the real world, the built-in groups are often misused. It's a common practice to add users to the Power Users group so that an application that won't run with regular User privileges will work as expected. While this is better than adding the user to the Administrators group, there is a risk associated with this practice—the risk that the user will be granted unnecessary rights that will later be misused. Even if the user would never intentionally misuse the elevated privileges of the Power Users group, a virus or Trojan horse might take advantage of the additional privileges without the user being aware.

Question: 22.(A)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. Servers run either Windows Server 2003 or Windows 2000 Server. All client computers run Windows XP Professional. Company's written security policy states that user accounts must be locked if an unauthorized user attempts to guess the users' passwords.

The current account policy locks out a user after two invalid password attempts in five minutes. The user remains locked out until the account is reset by the administrator. Users frequently call the help desk to have their account unlocked. Calls related to account lockout constitute 25 percent of help desk calls. You need to reduce the number of help desk calls related to account lockout. What should you do?

- A. Modify the Default Domain Controllers Policy Group Policy object (GPO). Increase the maximum lifetime for service tickets.
- B. Modify the Default Domain Policy Group Policy object (GPO). Configure an account lockout threshold of 10.
- C. Modify the Default Domain Controllers Policy Group Policy object (GPO). Disable the enforcement of user logon restrictions.

D. Modify the Default Domain Policy Group Policy object (GPO). Increase the maximum password age.

Answer: B

Explanation:

Deploying and Troubleshooting Security Templates Account Lockout Policy. Determines the circumstances and length of time that an account will be locked out of the system. Security Alert Enabling account lockout doesn't necessarily increase security. In fact, it actually creates a new vulnerability. An attacker who knows valid user names can guess incorrect passwords for users and lock legitimate users out, creating a denial-of-service attack.

Question: 23.(A)

You are a security administrator for Company. The network consists of a single Active Directory forest that contains three domains in a single domain tree. All servers run Windows Server 2003. All computers are members of the domains. The functional level of the forest is Windows 2000. The functional level of each domain is Windows Server 2003. Company has a main office and five branch offices. Each branch office is configured as a separate Active Directory site. One domain controller for each of the three domains in each site. Only the main office contains global catalog servers. Users report that logging on in the branch office takes much longer than logging on in the main office. You need to ensure that the logon process in the branch offices completes more quickly. You do not want to install additional global catalog servers in the branch office, and you do not want to increase the bandwidth between the branch offices and the main office. What should you do?

- A. Raise the functional level of the forest to Windows Server 2003.
- B. Create a two-way shortcut trust between the two child domains.
- C. Enable universal group membership caching.
- D. Convert all universal groups in the three domains to domain local groups or global groups.
- E. Increase the maximum lifetime for Kerberos user tickets.

Answer: C

Explanation: Argument for C: D – is only partially right because: Universal to global. This is only allowed if the group you want to change does not have another universal group as a member. The question gives no indication that it does or doesn't have this level of nesting. If we work under the assumption the UG are in use then converting them would break access to the resources to which they were created for. Furthermore if the UGs were used in other DLGs for permissions/access, this too would stop working.

Universal group membership caching

Due to available network bandwidth and server hardware limitations, it may not be practical to have a global catalog in smaller branch office locations. For these sites, you can deploy domain controllers running Windows Server 2003, which can store universal group membership information locally. Information is stored locally once this option is enabled and a user attempts to log on for the first time. The domain controller obtains the universal group membership for that user from a global catalog. Once the universal group membership information is obtained, it is cached on the domain controller for that site indefinitely and is periodically refreshed. The next time that user attempts to log on, the authenticating domain controller running Windows Server 2003 will obtain the universal group membership information from its local cache without the need to contact a global catalog. By default, the universal group membership information contained in the cache of each domain controller will be refreshed every 8 hours. To refresh the cache, domain controllers running Windows Server 2003 will send a universal group membership confirmation request to a designated global catalog. Up to 500 universal group memberships can be updated at once. Universal group membership caching can be enabled using Active Directory Sites and Services. Universal group membership caching is site specific and requires that all domain controllers running Windows Server 2003 be located in that site to participate. For more information about how to enable this option, see To cache universal group memberships. The following list summarizes potential benefits for caching universal group memberships in branch office locations:

- Faster logon times since authenticating domain controllers no longer need to access a global catalog to obtain universal

group membership information.

No need to upgrade hardware of existing domain controllers to handle the extra system requirements necessary for hosting a global catalog.

Minimized network bandwidth usage since a domain controller will not have to handle replication for all of the objects located in the forest.

Question: 24.(B)

You are the security administrator for Company. The network consists of a single Active Directory domain named Company.com. Four Windows Server 2003 computers run IIS and serve as Web servers on the Internet. Company's written security policy states that computers that are accessible from the Internet must be hardened against attacks. The procedure for hardening computers includes disabling unnecessary services. You evaluate which services are necessary by using the following information about the Web servers:

Customers and business partners access Web content on the Web servers after they authenticate by using a user name and password. To access certain parts of the site, some of these connections use the SSL protocol.

All software is installed locally on the Web servers by using removable media, except for service packs and security patches.

The Web servers automatically download service packs and security patches from an internal computer that runs Software Update Services (SUS).

The Web servers are not functioning as any other roles.

You need to create a security template for the Web servers that disables unnecessary services and allows necessary services to operate. What should you do? To answer, drag the appropriate service startup types to the correct locations in the work area.

Service Startup Types

Automatic

Disabled

Work Area

Service	Startup Policy
Application Management	Place here
Automatic Updates	Place here
Certificate Services	Place here
DNS Server	Place here
IIS Admin Service	Place here
Internet Authentication Service	Place here
World Wide Web Publishing Service	Place here

Answer:

Service Startup Types

Automatic

Disabled

Work Area

Service

Startup Policy

Application Management

Disabled

Automatic Updates

Automatic

Certificate Services

Disabled

DNS Server

Disabled

IIS Admin Service

Automatic

Internet Authentication Service

Disabled

World Wide Web Publishing Service

Automatic

Explanation:

IIS Services IIS provides the basic services that publish information, transfer files, support user communication, and update the data stores upon which these services depend. This section introduces the services that IIS 6.0 provides. The following table lists the IIS services, as well as their primary components and service hosts.

Service	Primary Component	Hosted by
World Wide Web Publishing Service (WWW service)	lsw3adm.dll	Svchost.exe
File Transfer Protocol Service (FTP service)	Ftpsvc2.dll	Inetinfo.exe
Simple Mail Transfer Protocol Service (SMTP service)	Smtpsvc.dll	Inetinfo.exe
Network News Transfer Protocol Service (NNTP service)	Nntpsvc.dll	Inetinfo.exe
IIS Admin service	Isadmin.dll	Inetinfo.exe

World Wide Web Publishing Service World Wide Web Publishing Service (WWW service) provides Web publishing to IIS end users, connecting client HTTP requests to Web sites that are running in IIS. WWW service manages the IIS core components that process HTTP requests and that configure and manage Web applications. WWW service runs as lsw3adm.dll and is hosted by Svchost.exe.

File Transfer Protocol Service Through the File Transfer Protocol service (FTP service), IIS provides full support for managing and serving files. The service uses the Transmission Control Protocol (TCP), which ensures that file transfers are complete and that the data transferred is accurate. This version of FTP supports isolating users at the site level to help administrators secure and commercialize their Internet sites. FTP service runs as Ftpsvc2.dll and is hosted by Inetinfo.exe.

Simple Mail Transfer Protocol Service IIS can send or receive e-mail by using the Simple Mail Transfer Protocol service (SMTP service). For example, you can program the server to send mail automatically in response to events, in order to confirm successful forms submissions by users. Also, you can use the SMTP service to receive messages that collect feedback from Web site customers. SMTP service does not provide full e-mail services. To deliver full e-mail services, use Microsoft® Exchange Server. SMTP service runs as Smtpsvc.dll and is hosted by Inetinfo.exe.

Network News Transfer Protocol Service You can use the Network News Transfer Protocol service (NNTP service) to host NNTP local discussion groups on a single computer. Because this feature complies fully with the NNTP protocol, users can use any news reader client to participate in the newsgroup discussions. Through the Rfeed script, found in the inetrv folder, the IIS NNTP service now supports newsfeeds. NNTP service does not support replication. To employ news feeds or to replicate a newsgroup across multiple computers, use Exchange Server. NNTP service runs as Nntpsvc.dll and is hosted by Inetinfo.exe.

IIS Admin Service IIS Admin service manages the IIS metabase and updates the Microsoft Windows® operating system registry for the WWW service, FTP service, SMTP service, and NNTP service. The metabase is a data store that holds IIS configuration data. IIS Admin service exposes the metabase to other applications, including the core components of IIS, applications that are built on IIS, and third-party applications that are independent of IIS, such as management or monitoring tools. IIS Admin service runs as Iisadmin.dll and is hosted by Inetinfo.exe

Reference:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;321141>

HOW TO: Disable or Remove Unnecessary IIS Services

Note:

Application Management The application management service process advertises applications on the user's desktop or on the Start menu. The Application Management system service provides software installation services such as Assign, Publish, and Remove. This service processes requests to enumerate, install, and remove applications deployed via a corporate network. When you click Add in Add/Remove Programs control panel on a computer joined to a domain, the program calls this service to retrieve the list of your deployed applications. The service is also called when you use Add/Remove Programs to install or remove an application, and in cases when a component, such as the shell or COM, makes an install request for an application to handle a file extension, Component Object Model (COM) class, or ProgID that is not present on the computer. The service is started by the first call made to it; it does not terminate once started. Note: For more information about COM, COM class, or ProgID, see the Software Development Kit (SDK) information in the MSDN® developer program Library on the Web Resources page at:

<http://www.microsoft.com/windows/reskits/webresources>. If the Application Management service is stopped or disabled, users will be unable to install, remove, or enumerate applications deployed in the Microsoft Active Directory service through Microsoft IntelliMirror® management technologies. If this service is disabled, it will not retrieve deployed application information nor will this information appear in the Add New Programs section of the Add/Remove Programs control panel. The Add programs from your network dialog box will display the following message: No programs are available on the network. Stopping this service is not possible once started. If you do not require this service, you must disable it to prevent it from starting. **Automatic Updates** The Automatic Updates system service enables the download and installation of critical Windows updates. This service automatically provides your computer with the latest updates, drivers and enhancements. You no longer have to manually search for critical updates and information; the operating system delivers them directly to your computer. The operating system recognizes when you are online and uses your Internet connection to search for applicable updates from the Windows Update service. Depending on your configuration settings, the service will either notify you before download, before installation, or the service will automatically install updates for you. You can turn off the Automatic Update feature through the Systems setting in the Control Panel, or by right-clicking the My Computer icon, and then clicking Properties. You can also use the Microsoft Management Console (MMC) Group Policy Object Editor snap-in administrative template to configure an intranet server that is configured with the Software Update Services to host updates from the Microsoft Update Web sites. This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network. For more information about Software Update Services, see the Software Update Services Web site at:

<http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp>. If the Automatic Updates service is stopped or disabled, no critical updates will be downloaded to the computer automatically. Searching for, downloading and installing applicable critical fixes will have to be done by going to the Windows Update Web site at: <http://v4.windowsupdate.microsoft.com/en/default.asp>. **Internet Authentication Service** The Internet Authentication Service performs centralized authentication, authorization, auditing, and accounting of users connecting to a network - either LAN or remote - using VPN equipment, Remote Access Equipment (RAS), or 802.1x Wireless and Ethernet/Switch Access Points.

IAS implements the Internet Engineering Task Force (IETF) standard RADIUS protocol, which enables heterogeneous network access equipment. If IAS is disabled or stopped, authentication requests will failover to a backup IAS server, if it is available. If no backup IAS servers are available, users will not be able to connect to the network. If this service is disabled, any services that

explicitly depend on this service will not start. World Wide Web Publishing Service World Wide Web Publishing Service provides Web connectivity and administration of Web sites through the IIS snap-in. World Wide Web Publishing provides HTTP services for applications on the Windows platform. The service contains a process manager and a configuration manager. The process manager controls the processes in which custom applications and simple Web sites reside. The configuration manager reads the stored system configuration and ensures that Windows is configured to route HTTP requests to the appropriate application pools or operating system processes. This service can monitor the processes that house custom applications and provide recycling services for these applications. Recycling is a configuration property of an application pool and can be done on the basis of memory limits, request limits, processing time, or time of day. The service will queue HTTP requests if custom applications stop responding, and will also attempt to restart custom applications. The service depends on the IIS administration service and kernel TCP/IP support. If World Wide Web Publishing Service is stopped, the Windows Server 2003 operating system will not be able to serve any form of Web request. If this service is disabled, any services that explicitly depend on this service will not start.

Question: 25.(A)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All domain controllers and servers run Windows Server 2003. All computers are members of the domain. The domain contains 12 database servers. The database servers are in an organizational unit (OU) named DBServers. The domain controllers and the database servers are in the same Active Directory site. You receive a security report that requires you to apply a security template named Lockdown.inf to all database servers as quickly as possible. You import Lockdown.inf into a Group Policy object (GPO) that is linked to the DBServers OU. You need to ensure that the settings in the Lockdown.info security template are applied to all database servers as quickly as possible.

What should you do?

- A. On each database server, run the repadmin /replicate command.
- B. On each database server, run the gpupdate command.
- C. On each database server, run the secedit /refreshpolicy command.
- D. On each database server, open Local Computer Policy, select Security Settings, and then use the Reload command.
- E. On each database server, open Resultant Set of Policy, and then use the Refresh Query command.

Answer: B

Explanation:

Repadmin.exe is a command-line tool from the Windows 2000 Resource Kit that is included in the Support Tools folder on the Windows 2000 CD-ROM. Repadmin is a command-line tool that reports failures on a replication link between two replication partners. The following repadmin example displays the replication partners and any replication link failures for Server1 on the microsoft.com domain: repadmin /showreps server1.microsoft.com

For a complete list of repadmin options, use the ? option: repadmin /? Using secedit /refreshpolicy option is no longer available with Windows 2003. Gpupdate refreshes local and Active Directory-based Group Policy settings, including security settings. This command supersedes the now obsolete /refreshpolicy option for the secedit command. Syntax: gpupdate [/target:{computer|user}] [/force] [/wait:value] [/logoff] [/boot] Reloading the local policy updates the effective policy in the user interface. Depending on domain or OU password policies that are in effect, the effective policy may or may not have changed on your computer.

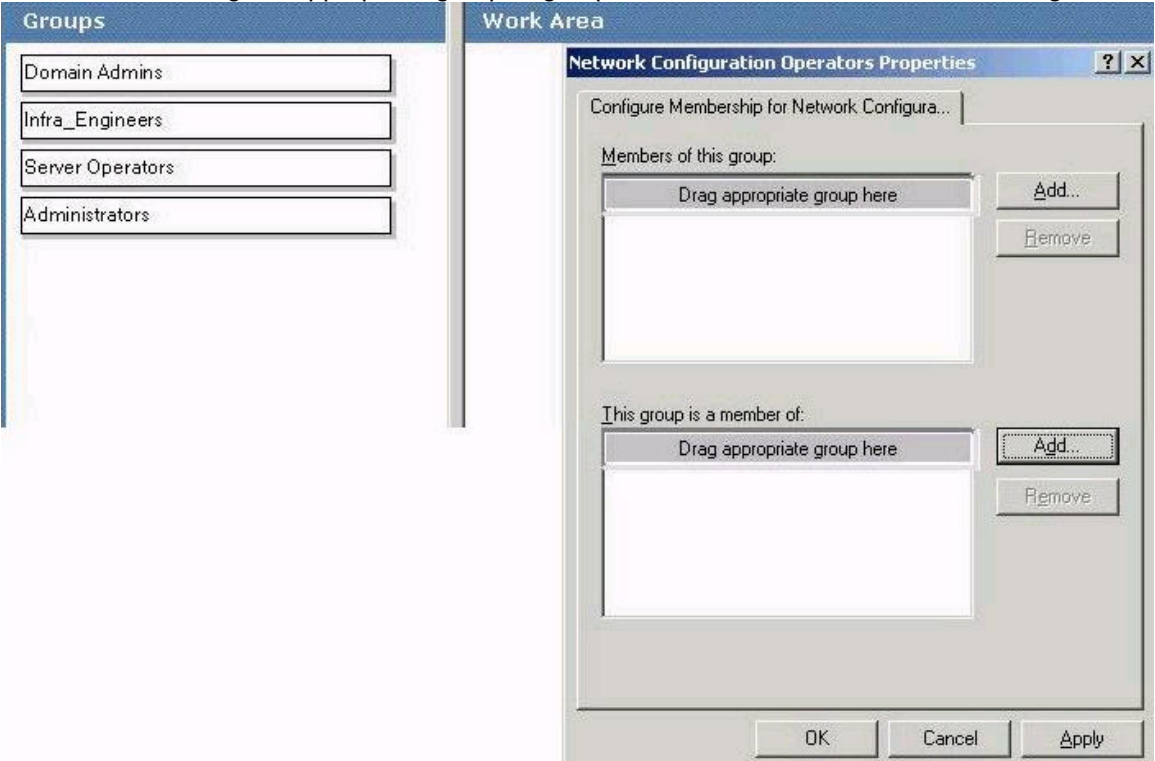
Resultant Set of Policy The Resultant Set of Policy (RSOP) snap-in (Rsop.msc) enables you to poll and evaluate the cumulative effect that local, site, domain, and organizational unit Group Policy objects (GPOs) have on computers and users.

Resultant Set of Policy enables you to check for GPOs that might affect your troubleshooting. For example, a GPO setting can cause startup programs to run after you log on to the computer. Use this snap-in to evaluate the effects of existing GPOs on your computer. This information is helpful for diagnosing deployment or security problems. Rsop.msc reports individual Group Policy settings specific to one or more users and computers, including advertised and assigned applications.

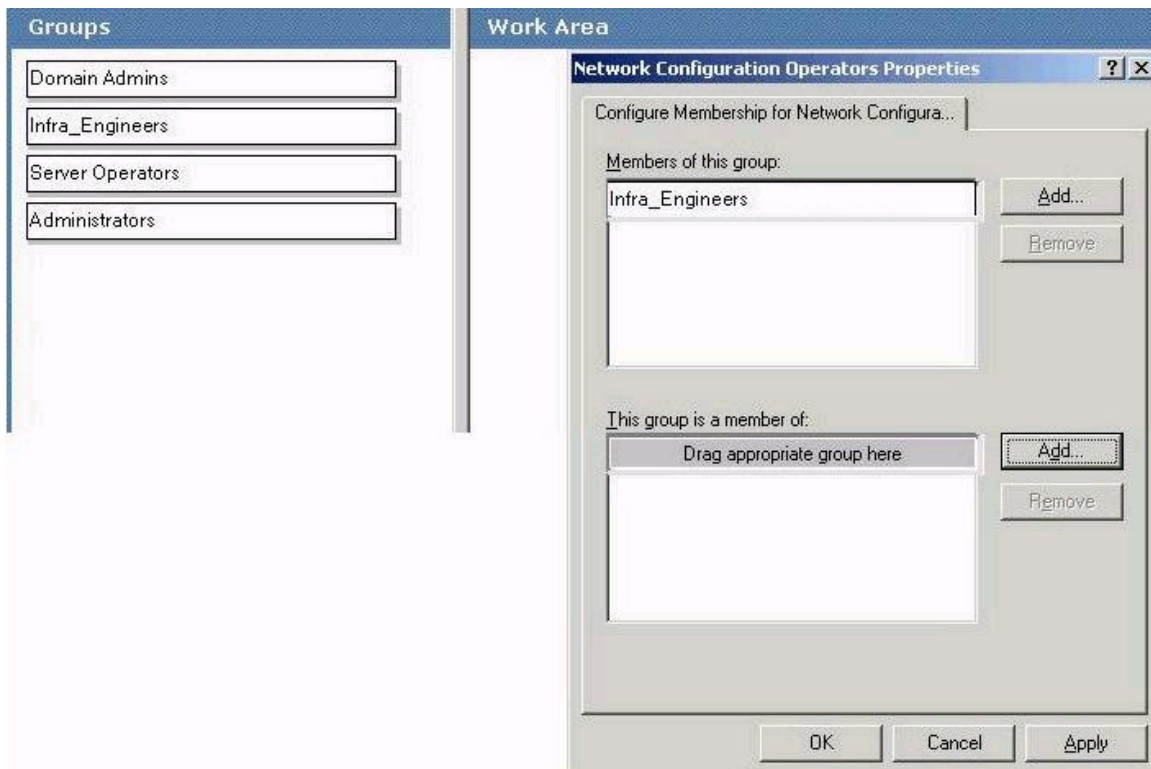
Question: 26.(A)

You are a security administrator for Company. The network consists of as single Active Directorydomain named Company.com. All servers run Windows Server 2003. All client computers runWindows XP Professional. You manage client computers by using Group Policy. Some of theadministrators in Company are responsible for managing network connectivity and TCP/IP. These administrators are known as infrastructure engineers and are members of a global group named Infra_Engineers. The infrastructure engineers must be able to configure and troubleshoot TCP/IP settings on severs and client computers. You need to reconfigure a Restricted Groups policy that ensures that only infrastructure engineers are members of the Network. Configuration Operators local group on all client computers. You want to achieve this goal without granting unnecessarypermissions to the infrastructure engineers.

What should you do? To answer, drag the appropriate group or groups to the correct list or lists in the dialog box in the work area.



Answer:



Explanation:

Description of Group Policy Restricted Groups SUMMARY: This article provides a description of Group Policy Restricted groups. Restricted groups allow an administrator to define the following two properties for security-sensitive (restricted) groups: Members Member Of The "Members" list defines who should and should not belong to the restricted group. The "Member Of" list specifies which other groups the restricted group should belong to. Using the "Members" Restricted Group Portion of Policy When a Restricted Group policy is enforced, any current member of a restricted group that is not on the "Members" list is removed with the exception of administrator in the Administrators group. Any user on the "Members" list which is not currently a member of the restricted group is added. Using the "Member Of" Restricted Group Portion of Policy Only inclusion is enforced in this portion of a Restricted Group policy. The Restricted Group is not removed from other groups. It makes sure that the restricted group is a member of groups that are listed in the Member Of dialog box. Planning and Configuring an Authorization Strategy Creating Restricted Groups Policy you can use security policies to control local group memberships on domain member computers. Windows Server 2003 includes a security policy setting called Restricted Groups that allows you to control group membership. By using the Restricted Groups policy, you can specify the membership of a group anywhere in your Active Directory domain. For example, you can create a Restricted Groups policy to limit the access on an OU that contains computers containing sensitive data. The Restricted Groups policy would remove domain users from the local users group and thereby limit the number of users who can log on to the computer. Group members that are not specified in the policy are removed when the Group Policy setting is applied or refreshed to the computer or OU. The Restricted Groups policy settings include two properties:

Members and Member Of. The Members property defines who belongs and who does not belong to the restricted group. The Member Of property specifies the other groups to which the restricted group can belong. When a Restricted Groups policy is enforced, any current member of a restricted group that is not on the Members list is removed. Members who can be removed include Administrators. Any user on the Members list who is not currently a member of the restricted group is added. In addition, each restricted group is a member of only those groups that are specified in the Member Of column. The shows Restricted Groups being used to add the Infra_Engineers group from the domainname.com domain to the Network Configuration Operators local group on all client computers. For example, use Restricted Groups to control group membership on domain members. Note: The security setting is located in a security policy object in the Restricted Groups node.

Planning and Configuring an Authorization Strategy You can apply a Restricted Groups policy in the following ways: Define the policy

in a security template, which will be applied during configuration on your local computer. Define the setting directly on a Group Policy object (GPO). Defining the setting in this way will ensure that the operating system continually enforces the restricted groups. To create a Restricted Groups policy:

- 1 Open a security policy tool, such as the Domain Security Policy console.
- 2 In the console tree, right-click Restricted Groups, and then click Add Group.
- 3 In the Group field, type the name of the group to which you want to restrict membership, and then click OK.
- 4 On the properties dialog box, click Add beside the This Group Is A Member Of field.
- 5 Under Group Membership, type the name of the group you want to add to this group, and then click OK.
- 6 Click OK again.

Note:

HOW TO: Use Restricted Groups in Windows 2000 <http://support.microsoft.com/default.aspx?scid=kb;en-us;228496> SUMMARY In Microsoft Windows 2000, the Security Settings extension to the Group Policy Editor includes a node called Restricted Groups. An administrator may use the Restricted Groups node to control the following items:

- User account membership in "restricted" groups.

Restricted group membership in other groups (reverse membership). Restricted Group Processing Administrators may configure restricted groups for a specific group policy object by adding the desired group directly to the restricted groups node of the group policy object namespace. Once groups are added, membership may be configured for each group by right-clicking the appropriate group, and then clicking Security. In the Security dialog box there are 2 list boxes, "Members of group name" and "group name is a member of", where group name is the appropriate group name. Membership is enforced as:

1. Members of group name Membership Is Strictly Enforced:

- For the restricted group, any user or group that is included in that restricted group's member list is added to the group.
- Any user or group that is currently a member of the group, but is not listed in the restricted group's member list is removed.

2. group name Is a Member of Only inclusion is enforced in this case. The restricted group is not removed from other groups based on the items in this list. This section is not present in Windows 2000 Professional.

Question: 27.(A)

Administrators in Company use scripts to perform administrative tasks when they troubleshoot problems on client computers. They connect to the Telnet service on client computers when they run these scripts. For security reasons, all Telnet traffic is encrypted by using an IPsec policy. In addition, the Telnet service is configured for manual startup on all client computers. Administrators manually start and stop the Telnet service when they perform administrative tasks. Administrators report that they sometimes cannot start the Telnet service on client computers. You examine several client computers and discover that the Telnet service is disabled. You need to ensure that administrators can troubleshoot problems on client computers at all times.

What should you do?

- A. Use a Restricted Groups policy in a new Group Policy object (GPO) to add the Domain Admins Group to the Power Users group on each client computer.
- B. Use a Restricted Groups policy in a new Group Policy object (GPO) to ensure that the Power Users group on each client computer contains no members.
- C. Use a System Services policy in a new Group Policy object (GPO) to ensure that only Domain Admins can manage the Telnet service.
- D. Use an Administrative Template setting to prevent local users from starting the Services snap-in.

Answer: C

Explanation:

The first item is not needed as they are Administrators and they have full control.

This would work as long as the user was not part of the local Administrators group and the question does not say what the user permissions are, by default local Administrators can manage this service.

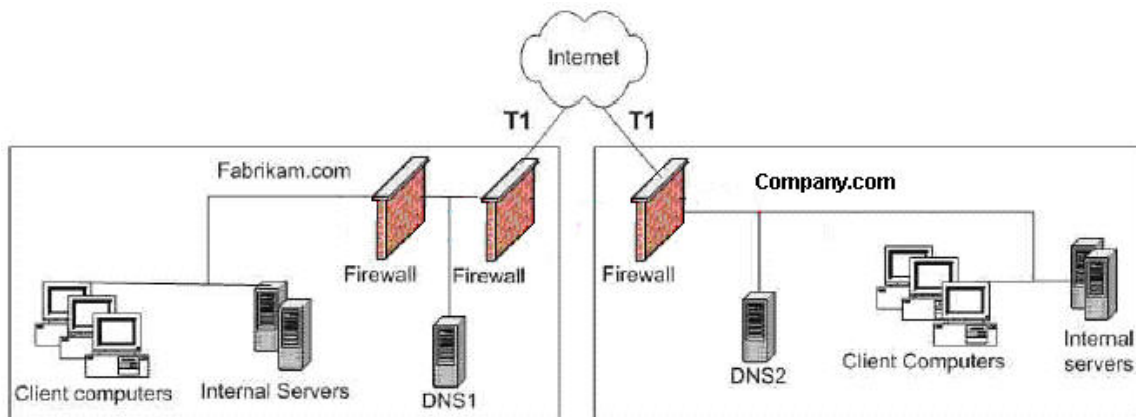
Note:

System Services This security setting allows you to define the startup mode (manual, automatic, or disabled) and access permissions for all services (Start, Stop, or Pause). You can also edit other security properties of the service, such as which user or group accounts have permission to read, write, delete, or execute inheritance settings or auditing and ownership permission by clicking Edit Security. Location GPO_name\Computer Configuration\Windows Settings\Security Settings\System Services\ Default Values Server Type or GPO Default Value Default Domain Policy Not defined for any service Default Domain Controller Policy Not defined for any service Stand-Alone Server Default Settings Not defined for any service DC Effective Default Settings Not defined for any service Member Server Effective Default Settings Not defined for any service

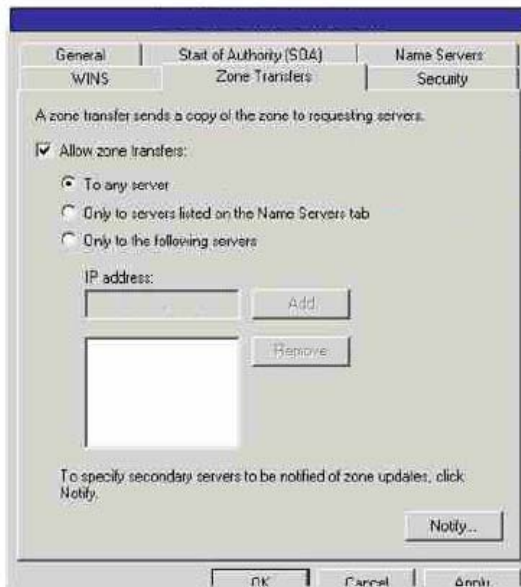
Discussion System services are processes that normally run in the background. An administrator uses the Services snap-in to manage system services directly. To manage system services through security policy, administrators can use the System Services security setting. This security setting does not appear in the local Group Policy object. If you choose to set system service startup to Automatic, perform adequate testing to verify that the services can start without user intervention. For performance optimization, set unnecessary or unused services to Manual. To find descriptions of each individual service (including what happens when you stop it from running), see the System Services chapter of "Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP," which can be downloaded from the Microsoft Web site. HOW TO: Define Security Templates By Using the Security Templates Snap-In in Windows Server 2003 <http://support.microsoft.com/?kbid=816297>

Question: 28.(C)

You are a security administrator for Company. Company has offices in two cities. The network consists of a single Active Directory forest that contains two trees. The trees are named Company.com and fabrikam.com and are located in separate cities. All servers run Windows Server 2003. All client computers run Windows XP Professional. The network is configured as shown in the Network Diagram exhibit.



Each office maintains a DNS server. The DNS server contains a primary zone for the local tree and a secondary zone for the tree in the other office. DNS zones are configured as shown in the Properties exhibit.



You examine the logs for your firewall and discover a large number of attempted connections to internal servers. You find out that external users have access to the DNS information used by your internal networks. You need to prevent external users from accessing internal DNS information. What should you do?

- A. Replace the primary zones with stub zones.
- B. Implement an IPsec policy that uses Encapsulating Payload (ESP) when replicating secondary zones.
- C. Implement an IPsec policy that uses Encapsulating Security Payload (ESP) when resolving DNS names stored in primary zones.
- D. Configure the zones to replicate to known DNS servers only.

Answer: D

Explanation:

Stub zones are used for name resolution; this will not prevent others from getting DNS information.

ESP is used to encrypt data in transmission and has nothing to do with zone transfers; this will not prevent others from getting DNS information.

<http://www.microsoft.com/resources/documentation/msa/edc/all/solution/ens/pak/build/edcbld06.msp>

Configuring Zone Transfer Security on All Zones All zone transfers should be sent only to known DNS servers. This practice prevents a malicious user from dumping the entire zone file using a tool such as nslookup. Use the information in the following table to configure the zones to perform zone transfers only with known name servers.

- 1 On each <domain_controller> (where computer_name is a domain controller from the following table), launch an instance of the MMC DNS snap-in.
- 2 Right-click each <zone_name> (where zone_name is a zone from Table 18) and select Properties.
- 3 On the Name Servers page, ensure that all <name_servers> in the table below are associated with the zone. Add any missing name servers by clicking Add, typing the name of the server, clicking Resolve, and then OK.Repeat as necessary.
- 4 On the Zone Transfers page, select Only to servers listed on the Name Servers tab, click OK.

Question: 29.(A)

You are a security administrator for Company. The network consists of two Active Directory domains. All servers run Windows Server 2003. Client computers run either Windows XP Professional or Windows 2000 Professional. All domain controllers in both Active Directory domains are Windows Server 2003 computers. All computers are Active Directory domain members. During a security assessment, you discover that you can extract LAN Manager and NTLM password hashes from domain controller computers. You are able to guess many user account passwords within a short time by using a password cracking program. This poses an unacceptable security risk for Company. You need to increase the time required to guess user account passwords. You increase the minimum user account password length to nine characters, enable the Password must meet complexity requirements setting, and require all domain users to change their password at the next logon.

What else should you do?

- A. Apply a security template to all domain controller computers that enables the Domain member: Require strong (Windows 2000 or later) session key setting.
- B. Apply a security template to all domain controller computers that establishes the Network security: LAN Manager authentication level setting at Send NTLMv2 response only.
- C. Apply a security template to all domain controller computers that enables the Network security: Do not store LAN Manager hash value on next password change setting.
- D. Apply a security template to all domain controller computers that enables the System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing setting.

Answer: C

Question: 30.(A)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional. Company's written security policy states the following requirements:

- All access to files must be audited.
- File servers must be able to record all security events.

You create a new Group Policy object (GPO) and filter it to apply to only file servers. You configure an audit policy to audit files and folders on file servers. You configure a system access control list (SACL) to audit the appropriate files. You need to ensure that the GPO enforces the written security policy. Which two additional actions should you perform to configure the GPO? (Each correct answer presents part of the solution. Choose two)

- A. Set a manual retention method for the security log.
- B. Set the security log to retain entries for 7 days.
- C. Set the maximum security log size to the maximum allowed size.
- D. Configure the GPO to shut down the computer if it is unable to log security audits.
- E. Ensure that users who are responsible for reviewing audit log data are granted the right to manage the security log.

Answer: A, D

Explanation:

HOW TO: Use the Event Log Management Script Tool (Eventlog.pl) to Manage Event Logs in Windows 2000 This article describes how to use the Event Log Management Script tool (Eventlog.pl) to manage Event Viewer logs of Windows 2000-based computers.

An event is any significant occurrence in the computer or in a program that requires either users to be notified or an entry added to a log. The Event Log Service records events to the Application, Security, and System logs in Event Viewer. Additionally, events are written to the Directory Service and File Replication Service logs on domain controllers and the DNS Server log on DNS servers. You can use Event Viewer to obtain information about your hardware, software, and system components, and to monitor security events on a local or remote computer. You can use event logs to identify and diagnose the source of current computer problems or to help you predict potential computer problems.

Eventlog.pl is available in the Windows 2000 Resource Kit Supplement 1. You can use this script tool to perform the following event log management tasks: Change the properties of event logs. Back up (save) event logs. Export event lists to text files. Clear (delete) all events from event logs. Query the properties of event logs. **IMPORTANT:** Do not use Eventlog.pl if you use Group Policy to specify event log settings. Eventlog.pl can violate Event log policies so that the following Group Policy settings for domains, organizational units, and sites may become ineffective: Maximum LogName log size Retain LogName logRetention method for LogName log Threats and Countermeasures Guide Event Log The Event log records events on the system. The Security log records audit events. The Event log container of Group Policy is used to define attributes related to the application, security, and system event logs, such as maximum log size, access rights for each log, and retention settings and methods. The Microsoft® Excel workbook called Windows Default Security and Services Configuration included with this guide that documents the default Event log settings. The Event log settings can be configured in the following location within the Group Policy Object Editor: Shut down system immediately if unable to log security audits Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Description Determines whether the system should shut down if it is unable to log security events. If this policy is enabled, it causes the system to halt if a security audit cannot be logged for any reason. Typically, an event will fail to be logged when the security audit log is full and the retention method specified for the security log is either Do Not Overwrite Events or Overwrite Events by Days. If the security log is full and an existing entry cannot be overwritten and this security option is enabled, the following blue screen error will occur: STOP: C0000244 {Audit Failed}

An attempt to generate a security audit failed. To recover, an administrator must log on, archive the log (if desired), clear the log, and reset this option as desired. By default, this policy is disabled.

Question: 31.(B)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. You manage the network by using a combination of Group Policy objects (GPOs) and scripts. File names for scripts have the .vbs file name extension. Scripts are stored in a shared folder named Scripts on a server named Company1. Users report that they accidentally run scripts that are received through e-mail and the Internet. They further reports that these scripts cause problems with their client computers and often delete or change files. You discover that these scripts have .wsh, .wsf, .vbs, or .vbe file name extensions. You decide to use software restriction policies to prevent the use of unauthorized scripts. You need to configure a software restriction policy for your network. You want to achieve this goal without affecting management of your network. Which three rules should you include in your software restriction policy? (Each correct answer presents part of the solution. Choose three)

- A. A path rule that disallows *.vb? files.
- B. A path rule that disallows *.ws? files.
- C. A trusted sites rule that allows the local intranet zone.
- D. A trusted sites rule that disallows the Internet zone.
- E. A path rule that allows \\Company1\scripts*.vb? files.

Answer: A, B, E

Explanation:

Software Restriction Policy By using the software restriction policy, you allow unknown code, which might contain viruses or code that conflicts with currently installed programs, to run only in a constrained environment (often called a sandbox) where it is disallowed from accessing any security-sensitive user privileges. For example, an e-mail attachment that contains a worm would be prohibited from automatically accessing your address book and therefore could not propagate itself. If the e-mail attachment contained a virus, the software restriction policy would restrict its ability to damage your system because it would be allowed to run only in a constrained environment.

The software restriction policy depends on assigning trust levels to the code that can run on a system. Currently, two trust levels exist: Unrestricted and Disallowed. Code that has an Unrestricted trust level is given unrestricted access to the user's privileges, so this trust level should be applied only to fully trusted code. Code with a Disallowed trust level is disallowed from accessing any security-sensitive user privileges and can run only in a sandbox so that Unrestricted code cannot load the Disallowed code into its address space. Configuring the software restriction policy for a system is done through the Local Security Policy administrative tool,

while the restriction policy configuration of individual COM+ applications is done either programmatically or through the Component Services administrative tool. If the restriction policy trust level is not specified for a COM+ application, the systemwide settings are used to determine the application's trust level.

HOW TO: Use Software Restriction Policies in Windows Server 2003 SUMMARY This article describes how to use software restriction policies in Windows Server 2003. When you use software restriction policies, you can identify and specify the software that is allowed to run so that you can protect your computer environment from untrusted code. When you use software restriction policies, you can define a default security level of Unrestricted or Disallowed for a Group Policy object (GPO) so that software is either allowed or not allowed to run by default. To create exceptions to this default security level, you can create rules for specific software. You can create the following types of rules:

Hash rules Certificate rules Path rules Internet zone rules

How to Create a Path Rule Click Start, click Run, type mmc, and then click OK. Open Software Restriction Policies. In either the console tree or the details pane, right-click Additional Rules, and then click New Path Rule. In the Path box, type a path or click Browse to find a file or folder. In the Security level box, click either Disallowed or Unrestricted. In the Description box, type a description for this rule, and then click OK.**IMPORTANT:** On certain folders, such as the Windows folder, setting the security level to Disallowed can adversely affect the operation of your operating system. Make sure that you do not disallow a crucial component of the operating system or one of its dependent programs.

Notes:

You may have to create a new software restriction policy setting for this GPO if you have not already done so. If you create a path rule for a program with a security level of Disallowed, a user can still run the software by copying it to another location.

The wildcard characters that are supported by the path rule are the asterisk (*) and the questionmark (?). You can use environment variables, such as %programfiles% or %systemroot%, in your path rule. To create a path rule for software when you do not know where it is stored on a computer but you have its registry key, you can create a registry path rule.

To prevent users from running e-mail attachments, you can create a path rule for your mail program's attachment folder that prevents users from running e-mail attachments. The only file types that are affected by path rules are those that are listed in Designated file types. There is one list of designated file types that is shared by all rules. For software restriction policies to take effect, users must update policy settings by logging off from and then logging on to their computers.

When more than one rule is applied to policy settings, there is a precedence of rules for handling conflicts. Configuring the Software Restriction Policy When you explicitly set the software restriction trust levels of a COM+ application, you are overriding the default systemwide settings for the software restriction policy. This is often necessary for COM+ server applications because the systemwide restriction policy is set the same for all server applications (because they all run in the same file, dllhost.exe).

Note When you set the trust level of a COM+ library application, you are affecting the systemwide software restriction policy for that application. For an overview of how to use the software restriction policy in COM+, see Software Restriction Policy. To set the software restriction policy Right-click the COM+ application for which you are setting the restriction policy, and then click Properties. In the application properties dialog box, click the Security tab. Under Software Restriction Policy, select the Apply software restriction policy check box to enable setting the trust level; clearing the check box causes COM+ to use the systemwide software restriction policy for the application.

In the Restriction Level box, select the appropriate level. The levels are as follows, ordered from least to most trusted: Disallowed The application is disallowed from using the full privileges of the user. Components with any restriction policy trust level can be loaded into it. Unrestricted The application has unrestricted access to the user's privileges. Only components with an Unrestricted trust level can be loaded into it. Click OK. The trust level you select takes effect the next time the application is started.

Question: 32.(A)

You are a security administrator for Company. Company has offices in New York, San Francisco, and Toronto. The network consists of a single Active Directory domain named Company.com. Each office is configured as an Active Directory site. All servers run Windows Server 2003. All client computers run Windows XP Professional. Users in the Toronto office work in the research department. User objects for users who work in the research department are stored in an organizational unit (OU) named Toronto.

Users in other offices frequently travel to the Toronto office for meeting and training. Company's written security policy requires that the following settings be enforced on computers at the Toronto office:

- A warning message that reminds users to protect Company information must be displayed before users log on.
- Domain controller authentication is required when users unlock client computers.
- The highest possible level of authentication must be used on the network at all times.

You create a new Group Policy object (GPO) named TorontoSecurity to meet the requirements of the written security policy. Users who travel to the Toronto office report that they are not presented with the warning message and that their screen savers do not require a password to deactivate. You need to ensure that the written security policy is enforced for other users only when they travel to the Toronto office. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. Link the TorontoSecurity GPO to the Toronto OU.
- B. Link the TorontoSecurity GPO to the domain.
- C. Configure a logon script to apply a custom security template when users travel to the Toronto office.
- D. Link the TorontoSecurity GPO to the Toronto site.

Answer: D

Explanation:

GPOs linked to sites might be appropriate to use for setting policy for proxy settings and network-related settings. Any GPO that is linked to a site container is applied to all computers in that site, regardless of which domain in the forest the computer belongs to. This has the following implications: Ensure that the computers do not access a site Group Policy object across a WAN link, which would lead to significant performance issues. By default, to manage site GPOs, you need to be either an Enterprise Admin, or the domain admin of the forest root domain. Active Directory service data-replication between domain controllers in different sites occurs less frequently than replication between domain controllers in the same site, and occurs during scheduled periods only. Between sites, FRS replication occurs spontaneously, and is not determined by the site link replication schedule; this is not an issue within sites. The directory service replication schedule and frequency are properties of the site links that connect sites. The default inter-site replication frequency is three hours. To change it, go to the appropriate site link, go to the IP link, and change the replication frequency or schedule as needed. Changing either the replication frequency or schedule can significantly affect policy. For example, assume that you have replication set to three hours or longer, and you create a GPO and link it to an OU in a domain that spans several sites. You will likely need to wait several hours before all users in that OU receive the GPO. If most of the users in an OU are in a remote location, and you have a domain controller in that site, you can work around inter-site replication latency by performing all Group Policy operations on a domain controller in that site. Linking GPOs To apply the settings of a GPO to the users and computers of a domain, site, or OU, you need to add a link to that GPO. You can add one or more GPO links to each domain, site, or OU by using GPMC. Keep in mind that creating and linking GPOs is a sensitive privilege that should be delegated only to administrators who are trusted and understand Group Policy. Linking GPOs to the Site If you have a number of policy settings to apply to computers in a particular physical location only

— certain network or proxy configuration settings, for example — these settings might be appropriate for inclusion in a site-based policy. Because domains and sites are independent, it is possible that computers in the site might need to cross domains to link the GPO to the site. In this case, make sure there is good connectivity. If, however, the settings do not clearly correspond to computers in a single site, it is better to assign the GPO to the domain or OU structure rather than to the site. Linking GPOs to the Domain Link GPOs to the domain if you want them to apply to all users and computers in the domain. For example, security administrators often implement domain-based GPOs to enforce corporate standards. They might want to create these GPOs with the GPMC Enforce option enabled to guarantee that no other administrator can override these settings. 3-20 Chapter 3 Deploying and Troubleshooting Security Templates If multiple Group Policy objects are linked to a single domain, site, or OU, verify that the order the policies are applied is correct. If there are conflicting settings in different policies, the higher policy in the list has higher precedence and will overwrite conflicting settings from other policies. Standard Group Policy inheritance In general, Group Policy is passed down from parent to child containers within a domain. Group Policy is not inherited from parent to child domains. For example, Lesson 2: Deploying Security Templates 3-21 Group Policy is not inherited from cohowinery.com to accounting.cohowinery.com. However, if you assign a specific Group Policy setting to a high-level parent container, that Group Policy setting applies to all containers beneath the parent container, including the user and computer objects in each container. If a policy setting is defined for a parent organizational unit and the same policy setting is not defined for a child organizational unit, the child inherits the parent's enabled or

disabled policy setting. If you explicitly specify a Group Policy setting for a child container, the child container's Group Policy setting overrides the parent container's setting. When multiple GPOs apply, and they do not have a parent/child relationship, the policies are processed in this order: local, site, domain, organizational unit. If a policy setting that is applied to a parent organizational unit and a policy setting that is applied to a child organizational unit are compatible, the child organizational unit inherits the parent policy setting, and the child's setting is also applied. If a policy setting that is configured for a parent organizational unit is incompatible with the same policy setting that is configured for a child organizational unit (because the setting is enabled in one case and disabled in the other), the child does not inherit the policy setting from the parent. The policy setting in the child is applied. You can block policy inheritance at the domain or OU level by opening the properties dialog box for the domain or organizational unit and selecting the Block Policy Inheritance check box. You can enforce policy inheritance by setting the No Override option on a GPO link. When you select the No Override check box, you force all child policy containers to inherit the parent's policy, even if that policy conflicts with the child's policy and even if Block Inheritance has been set for the child. You can set No Override on a GPO link by opening the properties dialog box for the site, domain, or organizational unit and making sure that the No Override check box is selected. Exam Tip Policies that are set to No Override cannot be blocked—know this for the exam! Group Policy inheritance with security groups You cannot link Group Policy objects directly to a security group. You can, however, use security group membership to allow or disallow members of the group from applying a Group Policy object. In this way, you can control which users receive a Group Policy object by placing them into specific groups. By default, all Authenticated Users are authorized to apply a Group Policy object. Therefore, to allow only specific groups to apply a GPO, you must first remove the default permissions for Authenticated Users, and then grant permissions for the specific groups to apply the GPO. <http://support.microsoft.com/default.aspx?scid=kb;en-us;322143#7> HOW TO: Administer GPOs in Windows 2000 How to Link a GPO to a Site, a Domain, or an Organizational Unit To link a GPO to a domain or an organizational unit, click Start, point to Programs, point to Administrative Tools, and then click Active Directory Users and Computers. Alternatively, to link a GPO to a site, click Start, point to Programs, point to Administrative Tools, and then click Active Directory Sites and Services. Right-click the site, the domain, or the organizational unit to which the GPO should be linked. Click Properties, and then click the Group Policy tab. To add the GPO to the Group Policy object Links list, click Add. Click the All tab, click the GPO that you want to add, click OK, and then click OK.

NOTE:

You link a GPO to specify that its settings apply to users and computers in the site, the domain, or the organizational unit, and to users and computers in Active Directory containers that inherit data from the site, the domain, or the organizational unit.

Question: 33.(A)

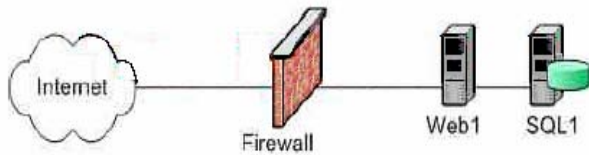
You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All servers are members of the domain. Company plans to deploy a new application named App1. The application runs on servers. To test the compatibility between App1 and other applications that run on the servers, you need to change several file and registry permissions in the Windows folder on the servers. A security template named TestPerms contains the file and registry permissions that need to be set for the application testing. You create a new Group Policy object (GPO) named TestApp. You import the TestPerms security template into the TestApp GPO. You link the TestApp GPO to an organizational unit (OU) that contains only the servers that are used for the test. You need to ensure that the file and registry permissions are set up to the permission in the TestPerms security template only during application testing. What should you do when the application testing ends?

- A. Disable the computer configuration settings in the TestApp GPO.
- B. Disable the TestApp GPO link to the OU.
- C. Unlink the TestApp GPO from the OU.
- D. Delete the TestApp GPO, and then run the gpupdate.exe /sync command.
- E. Delete the TestApp GPO, and then apply a security template that contains the original permissions.

Answer: E

Question: 34.(A)

You are a security administrator for Company. The network is configured as shown in the following



Company uses a Web application named App1 that is hosted on a Windows Server 2003 computer named Web1. App1 is accessed by users on the Internet. App1 allows users to enter data in an HTML form. The form then saves the data in a Microsoft SQL Server 2000 database hosted on a Windows Server 2003 computer named SQL1. WEB1 requires that all HTTP connections use SSL. Company uses a firewall that automatically allows replies to established connections. You need to configure the firewall to allow users to access App1. You must ensure that network security remains as strong as possible. You want to achieve this goal by using the minimum number of rules. How should you configure the firewall? To answer, drag the appropriate firewall rule element or elements to the correct location or locations in the work area.

Ports

HTTP

HTTPS

SQL

RPC

All

Protocols

TCP

UDP

Computers

All

Web1

SQL1

Direction

Outbound

Inbound

Work Area

	Source Port	Destination Port	Protocol	Source computer	Destination computer	Direction
Rule 1	Place here	Place here	Place here	Place here	Place here	Place here
Rule 2	Place here	Place here	Place here	Place here	Place here	Place here
Rule 3	Place here	Place here	Place here	Place here	Place here	Place here
Rule 4	Place here	Place here	Place here	Place here	Place here	Place here

Answer: Explanation:

Ports

HTTP

HTTPS

SQL

RPC

All

Protocols

UDP

Computers

All

Web1

SQL1

Direction

Outbound

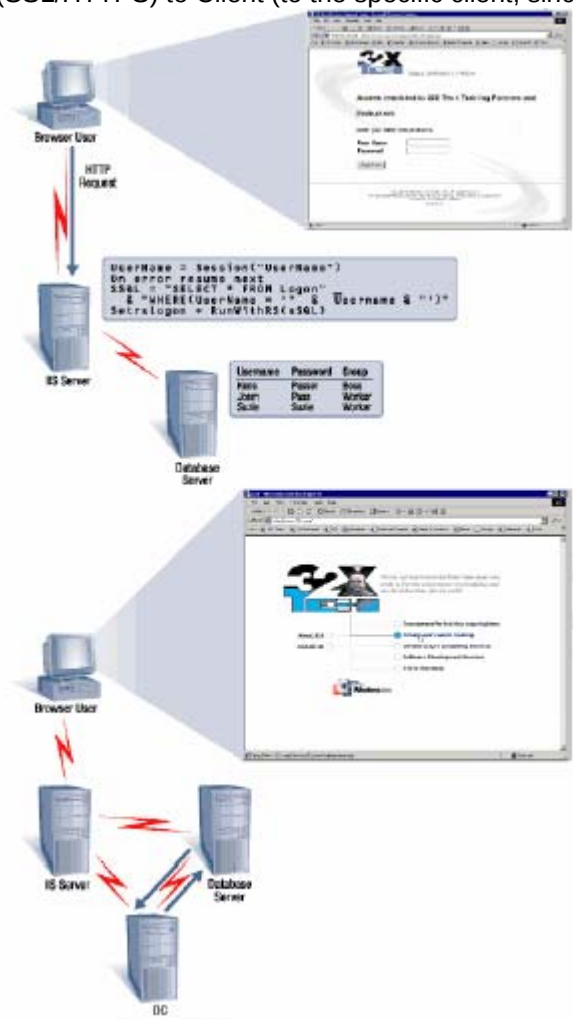
Inbound

Work Area

	Source Port	Destination Port	Protocol	Source computer	Destination computer	Direction
Rule 1	All	HTTPS	TCP	All	Web1	Inbound
Rule 2	RPC	RPC	TCP	Web1	SQL1	Inbound
Rule 3	RPC	RPC	TCP	SQL1	Web1	Outbound
Rule 4	HTTPS	All	TCP	Web1	All	Outbound

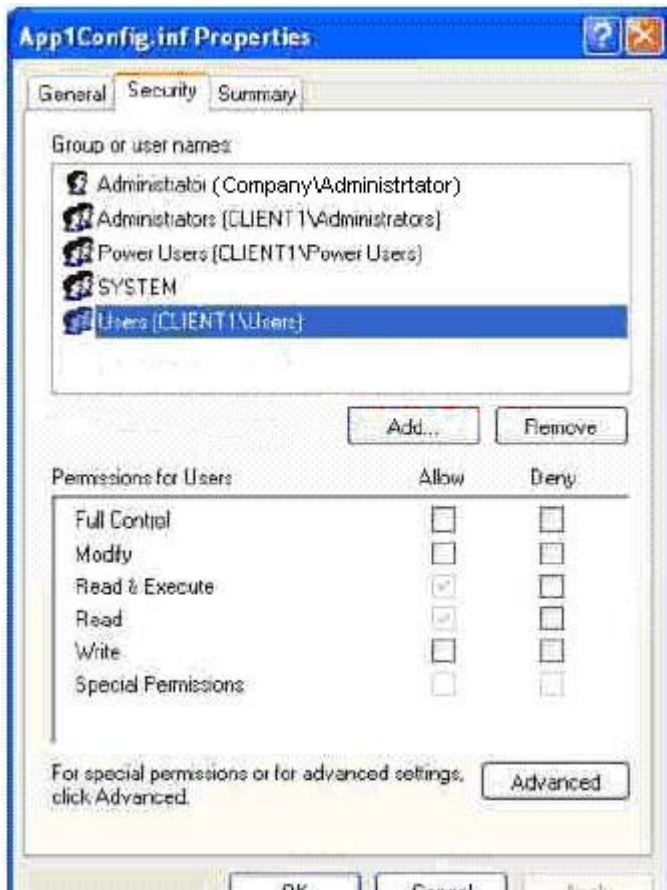
Client port to TCP 443 TCP 135 to TCP 1433

TCP 1443 to TCP 135 TCP 443 to client port Client (from any client) to Web1 (over SSL/HTTPS) Web1 (RPC since we assume SQL does not have certificate and not configured for SSL) to SQL SQL (RPC, because SQL is not using http to connect) to Web1 Web1(SSL/HTTPS) to Client (to the specific client, since the original connection was via SSL/HTTPS)



Question: 35.(A)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. One thousand users in the company use an application named App1. App1 is installed on each users' client computer. App1 uses a configuration file named App1.Config.inf. This file is stored in the `Systemroot\Program Files\App1` folder on each client computer. Users report that when they attempt to make configuration changes to App1, they sometimes receives an Access Denied messages. You examine the properties of the App1Config.inf file on one client computer. The file is configured as shown in the exhibit.



You need to ensure that users can make configuration changes to App1. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. On each client computer, assign the COMPANY\Domain Users group the Allow – Write permission for the App1Config.inf file.
- B. Modify the Default Domain Policy Group Policy object (GPO). Create a new File System security policy entry that assign the COMPANY\Domain Users group the Allow – Write permission for the App1Config.inf file.
- C. Modify the Default Domain Controllers Policy Group Policy object (GPO). Create a new File System security policy entry that assigns the COMPANY\Domain Users group the Allow – Write permission for the App1Config.inf file.
- D. Create a new logon script that runs the Xcacls.exe command. Use this command to assign the COMPANY\Domain Users group the Allow – Write permission for the App1Config.inf file. Include the logon script in the Default Domain Policy Group Policy object (GPO).

Answer: B

Explanation:

App1 is installed on the user's computer, applying a GPO at the DCs will not help. Creating a new logon script or assigning a new group to adjust perms on a single file is administrative prohibitive.

Question: 36(C)

You are a security administrator for Company.com. You plan to allow certain users to receive an EFS Recovery Agent Certificate. Currently, users do not have the option to enroll for an EFS Recovery Agent certificate. You need to restrict enrollment to members of the Company Recovery Agents domain global group. You add the EFS Recovery Agent certificate type to the list of approved certificate templates on the enterprise subordinate CA. You have not modified any other default Certificate Services or certificate

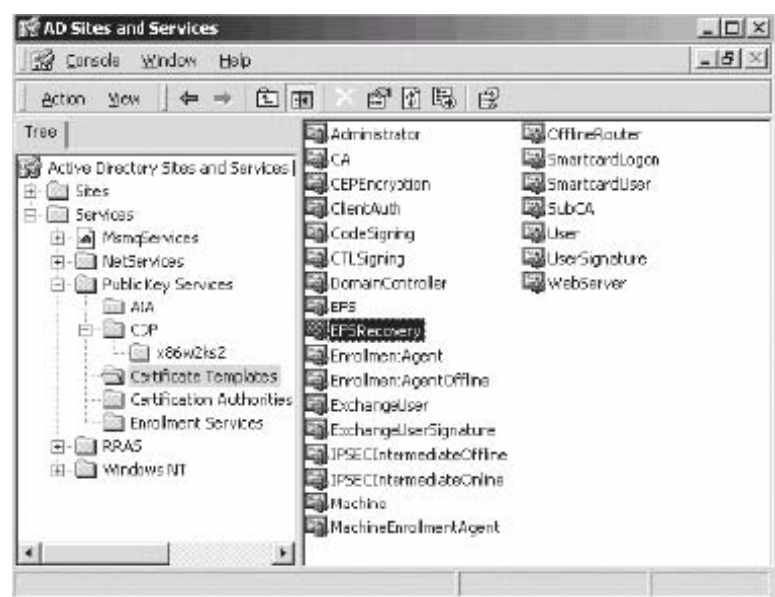
template settings. You need to allow only members of the Company Recovery Agents group to obtain EFS Recovery Agent Certificates. What should you do?

- A. Assign the Domain Users group the Allow – Enroll permission for the EFS Recovery certificate template.
- B. Assign the Domain Users group the Allow – Read permission for the EFS Recovery certificate template.
- C. Assign the Company Recovery Agents group the Allow – Enroll permission for the EFS Recovery certificate template.
- D. Assign the Company Recovery Agents group the Allow – Read permission for the EFS Recovery certificate template.

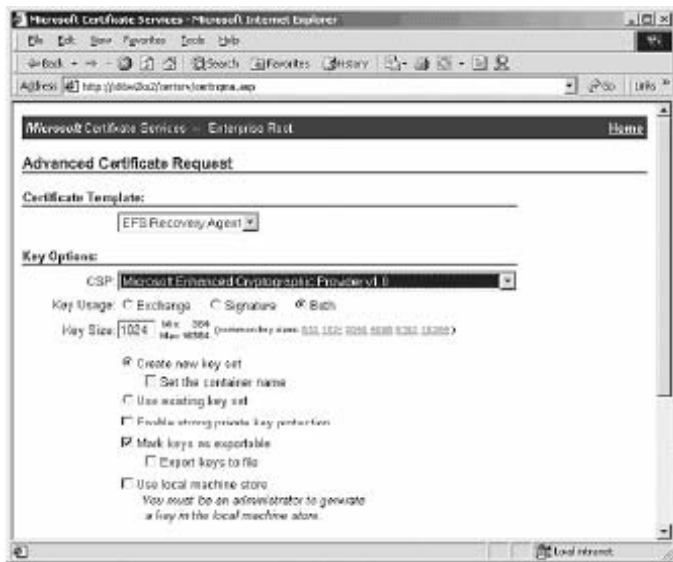
Answer: C

Explanation:

To create a recovery agent account, create a user account, then explicitly grant the account Enroll permission on Certificate Services' EFSRecovery certificate template. (The default ACL on the EFSRecovery template lets only members of the Domain Admins and Enterprise Admins groups request a recovery agent certificate.) To grant Enroll permission to a user, follow these steps: Open the Microsoft Management Console (MMC) Active Directory Sites and Services snap-in, then navigate to the Certificate Templates folder, which Figure A shows.



(If you don't see the Services node in this snap-in, select View on the MMC taskbar, then select Show Service Node.) Right-click EFSRecovery in the right pane, then select Properties. In the Properties dialog box, click the Security tab, then click Add to add the user to the template. Your CA administrator must grant each user Enroll permission. Let's say you're the assigned recovery agent. To obtain an EFS Recovery Agent certificate, point your browser to the CertSrv virtual directory on the issuing CA (e.g., <http://issuingca/certsrv>). On the resulting page, select the Request a certificate option, then click Next. On the next page, select the Advanced request option, then click Next. The next page asks how you want to make the certificate request. Select the Use a form option, then click Next. On the Advanced Certificate Request page, which Figure B shows,



select EFS Recovery Agent from the Certificate Template drop-down list. From the CSP drop-down list, select either the Microsoft Base Cryptographic Provider option or the Microsoft Enhanced Cryptographic Provider option, unless you have special requirements (e.g., if you store all your certificates on smart cards or USB tokens or have a hardware cryptographic accelerator). For the key size, enter at least 1024 bits. EFS File Recovery, Step by Step

1 Create New Users Group 1A. Right click on the Users node. 1B. Select New. 1C. Select Group. 1D. Enter the Name of the Group. 1E. Click OK.

2 Add Users to Group 2A. In the right-hand pane, double click on the new Group object. 2B. Select the Members tab. 2C. Click the Add button. 2D. Select User Accounts. 2E. Click OK twice.

3. Give This Group Enroll Permission on the EFS File Recovery Template 3A. Open Active Directory Site and Services. 3B. Click on the View menu, and select Show Services. 3C. Navigate to the Services\Public Key Services\Certificate Templates node. 3D. In the right-hand pane, right click the EFS Recovery certificates template, and select the Security tab. 3E. Click the Add button to add the File Recovery Group. Give them the Enroll permission on the template. 3F. Click OK.

3G. Remove other groups that should not act as recovery agents. 3H. Click the Advanced button. 3I. Select the Auditing tab and note that the group Everyone is being audited for success and failure on most activities, including enroll. 3J. Close the property pages and Active Directory Sites and Services.

3 Group Members Must Request Recovery Certificates 4A. Log on to the domain. 4B. Start\Run\mmc. 4C. From the Console menu, select Add-Remove Snap-in. 4D. Select the Certificates console and click Add, then Close, then OK. 4E. Right-click on the Personal Certificate Store and select All Tasks\Request new certificate. 4F. In the Certificate Request Wizard, click Next. 4G. When presented with a choice of certificates, select EFS Recovery Agent. 4H. Click Next. 4I. Add a friendly name, one that will help you identify the certificate. 4J. Click Next, then Finish. When "the certificate has been successfully issued" appears, click the View Certificate to make sure it's OK, then click OK. Then click the Install this Certificate button. This installs the certificate in your personal certificate store.

4 To Enable the Recovery Policy, Add Certificates to the GPO 5A. Open Active Directory Users and Computers. 5B. Right click on the domain object and select Properties. 5C. Select the Group Policy tab. 5D. Select Default Domain Policy. 5E. Click Edit. 5F. Right click the Windows Settings\Public Key Policy\Encrypted Data Recovery Agents node. 5G. Click New\Recovery Key Agent. 5H. In the Recovery Agent Wizard, click Next. 5I. Click the Browse Directory button. 5J. Search for and select the user File Recovery Certificate. 5K. Click Next, then Click finish. 5L. Refresh the policy by using the following command line: `secedit/refreshpolicy machine_policy`

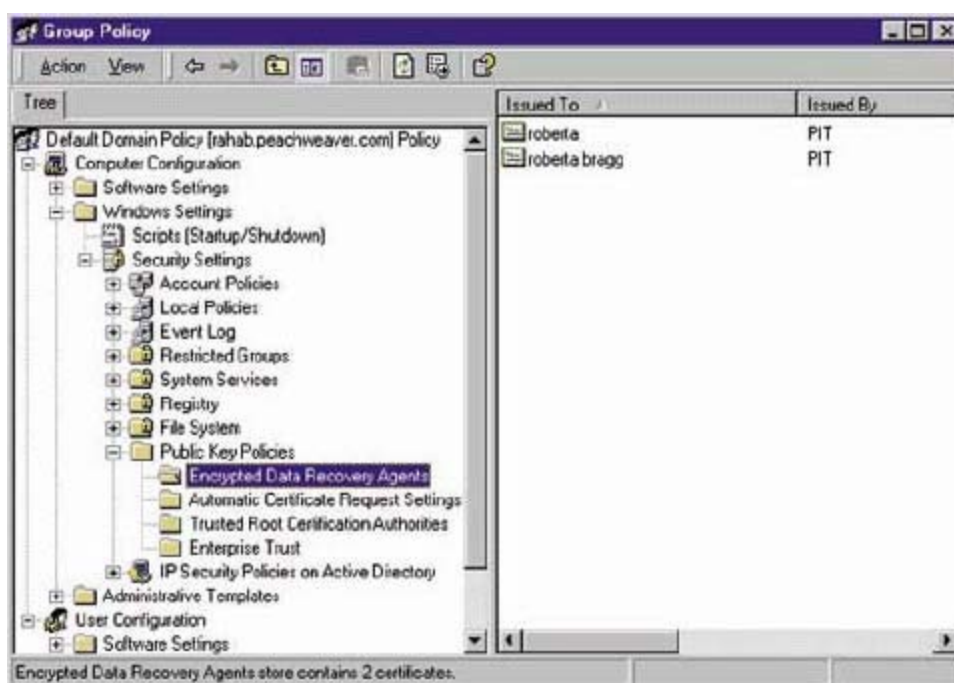
5 Test Recovery 6A. Wait until the new policy has been updated. 6B. Log on using an ordinary (no special administrative rights) user account. 6C. Request an encryption certificate. 6D. Encrypt some files. 6E. Log off and log on as another ordinary user. 6F. Attempt to open the files (you should be denied access). 6G. Log on as an approved recovery agent, and request a recovery agent certificate. 6H. Attempt to open the files (you should be allowed to open them).

6 Back Up Recovery Agent Certificates, and Remove Private Keys From the Computer 7A. The user must right click on the certificate in his personal certificate store, and then select All Tasks\Export. 7B. At the Certificate Export Wizard, select Next. 7C. Make sure Personal Information Exchange-PKCS #12 is chosen. 7D. Select Delete the private key if the export is successful. 7E.

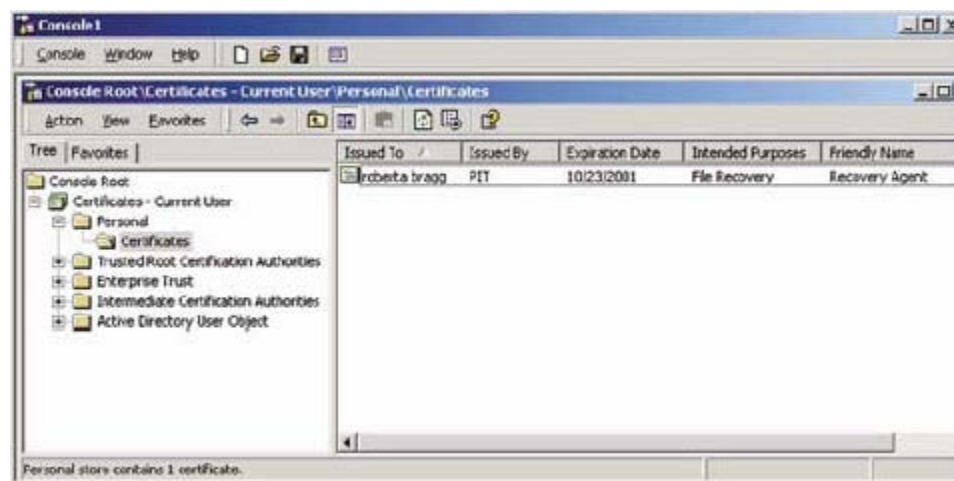
Click Next. 7F. Browse to the A:\ drive, insert a floppy diskette, enter a name, and click Next. 7G. When requested, enter a password and click Next, then click Finish. 7H. Remove the floppy disk and store in a safe, locked location.

7 Test the Recovery Policy 8A. Attempt to decrypt the files (this should fail). 8B. Back up the encrypted files and move them to the recovery station. 8C. Log on to the recovery station, and import your certificate and keys.

8D. Create a certificates console as above. 8E. Right click on the Personal Certificates store, and select All Tasks\Import. 8F. Browse to the A:\ drive, insert the backup certificate floppy disk. 8G. Select the certificate file and click OK. 8H. Decrypt the files. 8I. Move the files to the new storage location and have the appropriate user encrypt the files. 8J. Export the private key and certificate from the recovery station. Screen 1: An EFS Data Recovery Policy for the domain peachweaver.com with two certificates issued by the PIT certificate authority.



Screen 2: The Personal Certificate store holds the user's EFS Recovery Agent Certificate



Question: 37(A)
Exhibit, Hotspot

Authentication Methods

☐ Enable anonymous access

Use the following Windows user account for anonymous access:

User name:

Password:

Authenticated access

For the following authentication methods, user name and password are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☐ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

Default domain:

Realm:

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. Company.com uses the Internet to sell products. Customers place and view the status by using a Web application named CompanyApp3. CompanyApp3 is hosted on a Windows Server 2003 computer that runs IIS. Users access CompanyApp3 by using various Web browsers. You configure SSL for connections to CompanyApp3. Company.com's written security policy state the following requirements:

All users must enter a user name and password when they access CompanyApp3.

All users must use the same authentication method.

All users must use credentials in the Company.com's domain.

You need to configure IIS to support the required authentication. What should you do? (Click on the right spot on the exhibit)

Answer: Question: 38(A)



You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The network includes a public key infrastructure (PKI) that support smart card logon. All client computers have smart card readers. Managers are issued smart cards. Managers are required to use smart cards when logging on to the client computers. You need to ensure that managers are required to use a smart card when logging on to any client computer and that all other users are required to use a smart card when logging on to a client computer assigned to a manager. Which two actions should you perform? (Each correct answer is a part of the solution. Select two)

- A. On the properties of each user account used by a manager, select the Smart card required for Interactive logon check box.
- B. On the computer account for each manager's client computer, edit the DACL so that only managers are assigned the Allow – Allowed to authenticate permission.
- C. Place all client computers used by managers in an OU. Link a new GPO to the OU. Configure the GPO to enforce the Interactive logon:Require smart card setting.
- D. Place all client computers used by managers in an OU. Link a new GPO to the OU. Configure the GPO to set the startup type of the Smart Card service to Automatic..

Answer: A, C

Explanation

Designing and Deploying Directory and Security Services Selecting Group Policy Settings to Manage Smart Card Use Several Group Policy settings are specific to smart card management. You can use these Group Policy settings to manage smart cards in your organization. Other security policy settings, such as lockout policy or restricted logon times, can also impact smart card users if they use their cards for account logon. Smart card required for interactive logon When you set this policy on a user account, the user cannot log on to the account by using a password. They can only log on by using a smart card. The advantage of using this policy

setting is that it enforces strict security. However, if users are unable to log on by using conventional passwords, you must provide an alternate solution in the event that smart cards become unusable. This policy setting applies to interactive and network logons only. It does not apply to remote access logons, which are managed by policy settings that are configured on the remote access server. The Smart card required for interactive logon policy is not recommended for users who need to:

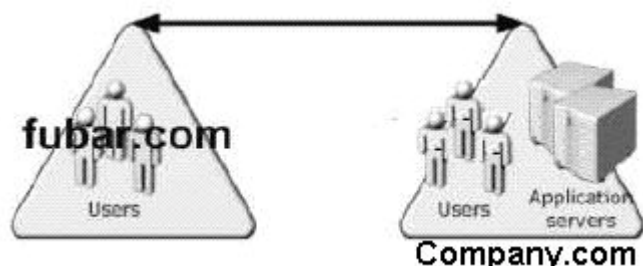
- Join a computer to a domain.

- Perform administrative tasks such as installing Active Directory on a member server.

- Configure a network connection for remote access. If you choose not to use this security policy setting, users can revert to their standard network passwords if their smart cards are damaged or unavailable. However, this weakens security. In addition, users who use their passwords infrequently might forget them, and either write them down, or call the help desk for a password reset, increasing help desk costs to the organization. On smart card removal Users who walk away from computers that are running an active logon session create a security risk. To enforce the security of your system, it is best if users either log off or lock their computers when they leave. The On smart card removal policy allows you to force users to log off or lock their computers when they remove their smart cards. If you select the forced logoff option, users need to make sure they have saved changes to documents and other files before they remove their smart cards. Otherwise, they lose any changes they have made. Whether or not you set the On smart card removal policy depends on how your users interact with their computers. For example, this policy is a good choice if using computers in an open floor or kiosk environment. This policy might not be necessary when users have dedicated computers or exclusive use of multiple computers. You can use a password-protected screensaver or other means to lock the computers of these users. The On smart card removal policy is a local computer policy that is administered on a per computer basis. Set the On smart card removal policy on a per user account basis, along with other domain security policy settings. Do not allow smart card device redirection Use the Do not allow smart card device redirection policy if you do not want to use smart cards in conjunction with Terminal Services sessions. Restrict this use of smart cards if you are concerned about the network resources required for Terminal Services sessions in your environment. Account lockout threshold Use the Account lockout threshold policy to disable accounts after a set number of failed logon attempts. An account that is locked out cannot be used until an administrator resets it, or until the account lockout duration expires. You can specify a value of between 1 and 999 failed logon attempts, or you can specify that the account is never locked out by setting the value to 0. To thwart unauthorized attempts to use a smart card and PIN, establish account lockout thresholds to a low value, such as four or five attempts.

Question: 39(A)

Network topology exhibit You are a security administrator for Company.com. The network consists of two Active Directory (AD) domains named Company.com and fubar.com. These domains are in the same Active Directory forest. The Company.com Active Directory domain operates at a Windows 2000 mixed mode domain functional level. The fubar.com Active Directory domain operates at a Windows 2000 native domain functional level. An application named CompanyApp runs on four Windows Server 2003 computers. These computers are domain member server in the Company.com AD domain. Authorized users in both the Company.com and the fubar.com domains require access to CompanyApp. The network topology can be view in the exhibit. You are required to plan an authorization model to control user access to CompanyApp. You will place Company.com user account in a group named Company AppUsers. You will place the fubar.com user accounts in group named Fubar AppUsers. You will use a group named AppResources to assign permission that allow access to CompanyApp. You need to choose the appropriate type of groups to implement your plan. Which three types of groups should you choose? (Each answer presents a part of the solution. Select three.)



- A. Use a global group named Company AppUsers in the Company.com domain.
- B. Use a domain local group named Company AppUsers in the Company.com domain.
- C. Use a global group named Fubar AppUsers in the fubar.com domain.
- D. Use a domain local group named Fubar AppUsers in the fubar.com domain.
- E. Use a global group named AppResources that contains the Company AppUsers and the Fubar Appusers in the

Company.com domain.

F. Use a global group named AppResources that contains the Company AppUsers and the Fubar Appusers in the fubar.com domain

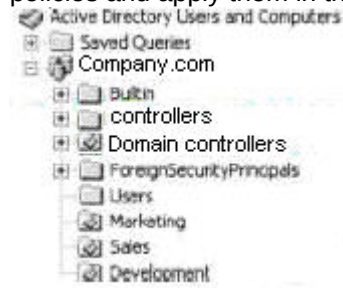
G. Use a domain local group named AppResources that contains the Company AppUsers and the Fubar Appusers in the Company.com domain.

H. Use a domain local group named AppResources that contains the Company AppUsers and the Fubar Appusers in the fubar.com domain

Answer: A, C, G

Question: 40(A)

Exhibit, OU You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The Company.com domain contains Windows Server 2003 computers and Windows XP Professional client computers. You create OUs in the Company.com domain to contain the user, computer, and group object for each department for Company.com. The OU structure is shown in the exhibit. You want to allow selected users to encrypt data by using the Encrypting File System (EFS). However, the requirements for using EFS vary based on the OU in which user's computer resides. Computers in the Sales OU must have EFS disabled. All other computers in the domain must have EFS enabled. Designated administrators must be able to help user access encrypted files on occasion. Sandra and Exams are also security administrators for Company. Sandra must be able to decrypt all files on computers in the Development OU and the Marketing OU. Exams must be able to decrypt all files on domain controllers. There are currently no EFS policies defined for computers in the domain. You need to create appropriate EFS policies and apply them in the correct manner.



Drag and Drop

Domain Containers	EFS Configuration
Domain Controller OU	<i>Place here</i>
Marketing OU	<i>Place here</i>
Sales OU	<i>Place here</i>
Development OU	<i>Place here</i>

EFS Configuration, Select from these

Disable the Allow users to encrypt files using EFS option

Enable the Do Not Require Data Recovery option

Add Sandra as the encrypted data recovery agent

Add Exar as the encrypted data recovery agent

No EFS policy is required.

Answer:

EFS Configuration	
Domain Containers	
Domain Controller OU	Add Exam as the encrypted data recovery agent
Marketing OU	Add Sandra as the encrypted data recovery agent
Sales OU	Disable the Allow users to encrypt files using EFS option
Development OU	Add Sandra as the encrypted data recovery agent

Question: 41(D)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. Company hosts a secure Web site for customers. The secure Web site is hosted on a computer Company5. Customers who want access to the Web site are issued certificates from an enterprise certification authority (CA). The enterprise CA is configured to store User certificates in Active Directory. Company.com's written security policy includes the following requirements for Company5:

Only users with valid certificates that were issued by Company.com, are permitted to access the secure Web site.

User access to the secure Web site must be maintained by using minimum amount of administrative effort.

Security administrators must be able to audit access on per user basis. You need to configure Company5 to provide the customers with access to the secure Web site. What should you do?

Configure Company5 to require SSL for all communications.

Configure Company5 to use one-to-one certificate mapping.

Configure Company5 to use many-to-one certificate mapping.

Configure Company5 to use Windows directory service mapper.

Answer: D

Question: 42(A)

You are a security administrator for Company.com. The network consists of two Active Directory forests. Each forest contains four domains. The root domains are named Company.com and foo.com. All servers on the network run Windows Server 2003. You want to allow the users in both forests to access resources in the other forest. You create a two-way forest trust relationship between the Company.com forest and the foo.com forest. However, users report that they cannot access resources on servers in the other forest. You verify that network connectivity and DNS name resolution between the two forests are functioning correctly. The users are attempting to connect to resources for which the Authenticated Users group is assigned the Allow – Read permission. You discover that all users are members of the Other Organization group when they attempt to connect to resources in the other forest. You need to ensure that users in one forest can access resources on servers in the other forests. What should you do?

A. Add the Domain Computers security group from each root domain to the Windows Authentication Access Group security group in the other root domain.

B. Configure the scope of the authentication of the forest trust relationship to disable selective authentication.

C. Configure the trusted domain object (TDO) in each forest to disable name suffix routing.

D. In each root domain, configure a domain controller to be global catalog server.

Answer: C

Question: 43(A)

You are a security administrator for Company.com. The network consists of two Active Directory domains. These domains each belong to separate Active Directory forests. The domain Company.com is used primarily to support company employees. The domain named bar.biz is used to support company customers. The functional level of all domains is Windows Server 2003 interim mode. A one-way external trust relationship exists in which the Company.com domain trusts the bar.biz domain. A Windows Server 2003 computer named Company3 is a member of the bar.biz domain. Company3 provides customers access to a Microsoft SQL Server 2000 database. The user accounts used by customers reside in the local account database on Company3. All of the customer user accounts belong to a local computer group named Customers. SQL Server is configured to use Windows Integrated authentication. Company.com has additional SQL Server 2000 database that reside on three Windows Server 2003 computers. These computers are members of the Company.com domain. Company's written security policy states that customer user accounts must reside on computers in the bar.biz domain. You need to plan a strategy for providing customers with access to the additional databases. You want to achieve this goal by using the minimal amount of administrative effort. What should you do?

- A. Create a new user account in the bar.biz Active Directory domain for each customer. Create a universal group in the bar.biz domain. Add the new customer domain user accounts as members of the new universal group. Assign this group permissions to access the databases.
- B. Create a new user account in the bar.biz Active Directory domain for each customer. Create a global group in the bar.biz domain. Add the new customer domain user accounts as members of the new global group. Assign this group permissions to access the databases.
- C. Create a new user account in the Company.com Active Directory domain for each customer. Create a global group in the Company.com domain. Add the new customer domain user accounts as members of the new global group. Assign this group permissions to access the databases.
- D. Create a new user account in the Company.com Active Directory domain for each customer. Create a global group in the Company.com domain. Add the new customer domain user accounts as members of the new global group. Assign this group permissions to access the databases.

Answer: B

Question: 44(B)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The Company.com domain contains Windows Server 2003 computers and Windows XP Professional client computers. All computers are members of the domain.

Company.com uses a custom application to track help desk calls. You receive a security bulletin that describes vulnerability in the customer application. To fix this vulnerability, you need to change a value in the user subtree of the registry for each user. Each user has only read permissions on the registry key that must be changed. You need to ensure that the registry value is changed for each user the next time the user logs onto the network. What should you do?

- A. Create a script that changes the registry value. Assign the script as login script in the domain user account of all users.
- B. Create a script that changes the registry value. Assign the script as user logon script in a Group Policy Object (GPO) that applies to all users.
- C. Create a script that change the registry value. Assign the computer startup script in a GPO that applies to all client computers.
- D. Add the registry value to the Administrative Template section of a GPO that applies to all users.
- E. Export the registry value to a registry file named appfix.reg. In the Startup group for each user, create a shortcut to the regedit.exe /s appfix.reg command.

Answer: D

Question: 45(B)

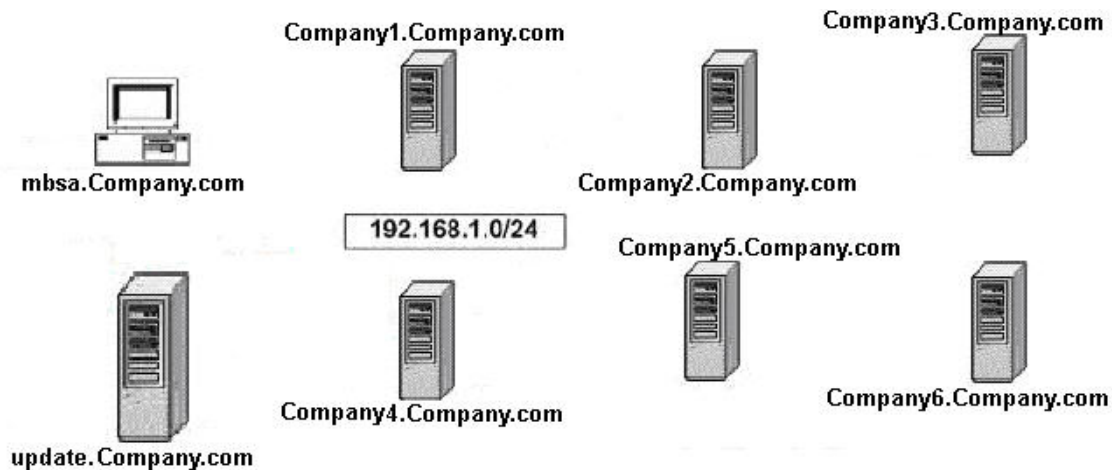
You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computers are members of the domain. The network contains 10 Active Directory sites. Each site represents one of the company's offices. The offices are located around the world. Each office has a connection to the Internet. Company maintains dedicated leased lines between the offices. You are planning a security patch management infrastructure for Microsoft security patches. You install Software Update Services (SUS) on a server named Company2. You need to ensure that Automatic Updates on the client computers and servers installs only security patches that are company approved. You want to limit the use of the leased line between the offices by allowing each computer to download security patches from the Internet. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Configure Automatic Updates on all computers to use the Microsoft Windows Update servers.
- B. Configure Automatic Updates on all computers to use SUS on Company2.
- C. Copy the Approveditems.txt file from Company2 to the Windows folder on each computer.
- D. Configure Company2 to maintain updates on the Microsoft Windows Update Servers.
- E. Use Group Policy to configure the SUS server location as the URL of the Microsoft Windows Update Web site on all computers.
- F. On all computers, configure the value of the **Run** key in the registry as the URL of the Microsoft Windows Update Web site.

Answer: B, D

Question: 46(B)

Network exhibit Exhibit, MBSA setting



Pick multiple computers to scan

Domain name:

IP address range: to

Security report name:

Options:

- ☐ Check for Windows vulnerabilities
- ☐ Check for weak passwords
- ☐ Check for IIS vulnerabilities
- ☐ Check for SQL vulnerabilities
- ☒ Check for security updates
- ☒ Use US Server

 Start scan

You are a security administrator for Company.com. The network consists of two Active Directory domains named Company.com and foo.com. Servers in both domains run Windows Server 2003. Client computers in both domains run Windows XP Professional. You want to scan a portion of your network by using Microsoft Baseline Security Analyzer (MBSA). All the computers that you want to scan are on a single IP subnet. The relevant portion of the network is shown in the Network exhibit. You install MBSA on a Windows XP Professional client computer named mbsa.Company.com. You complete a scan by using the MBSA settings shown in the MBSA Settings exhibit. The MBSA report does not contain any data about Company3.Company.com and Company4.Company.com. You need MBSA to run once and generate a report that includes results from all computers on the subnet. What should you do?

- A. Change the MBSA Domain Name setting to foo.com and start the scan.
- B. Change the MBSA Use SUS Server setting to use the URL of the Microsoft Windows Update Web site and start the scan.
- C. Change the MBSA Security report name setting to Company.com/foo.com – %computerName%(%date%) and start the scan.
- D. Change the MBSA IP address range setting to 192.168.1.1. to 192.168.1.254 and start the scan.

Answer: D

Question: 47(B)

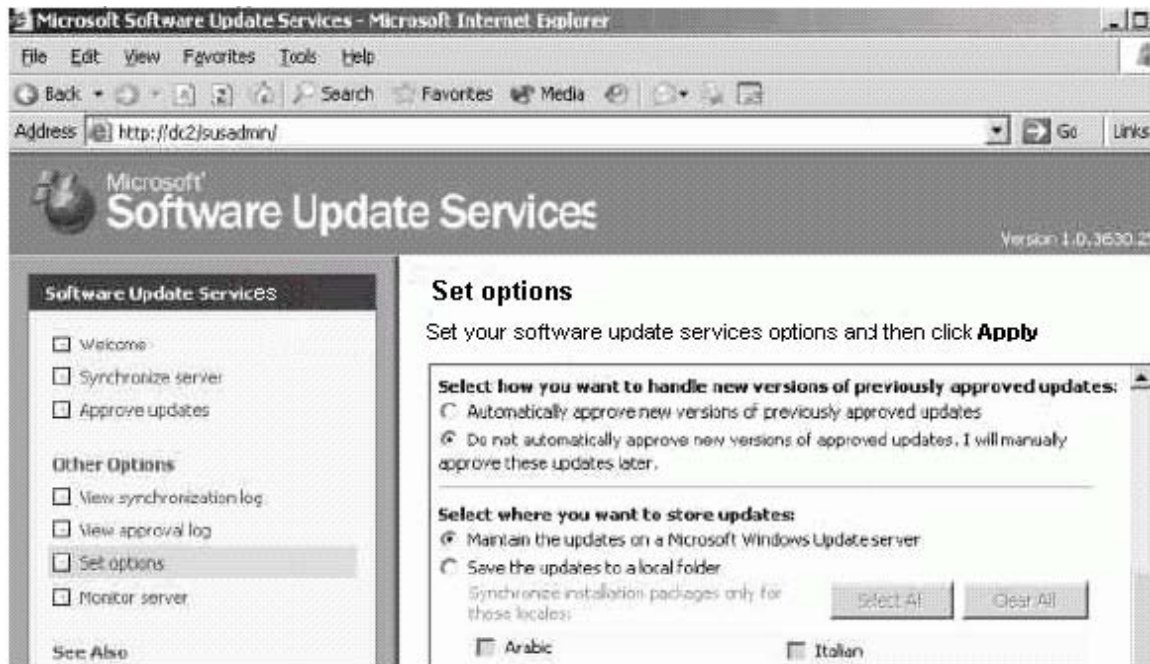
You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Some users in your company work from home offices. These users have client computers that are configured to use VPN connections to log on to the corporate domain. These computers are also members of the corporate domain. You configure these computers to use split tunneling when connecting to the corporate network. You use Software Update Services (SUS) as part of your patch management strategy. You install SUS on one server on the Company.com corporate network. You plan to review and approve security patches that meet Company.com's requirements on the SUS server. You configure a new GPO and filter the GPO to apply to computers used in home offices. You need to ensure that home office computers have the latest approved security patches. You want to achieve this goal while minimizing the amount of traffic on the corporate network and by using the least administrative effort. What should you do?

- A. Configure the GPO to automatically install security patches from the Windows Update Web site.
- B. Configure the GPO to disable Automatic updates. E-mail approved security patches to home office users.
- C. Configure the GPO to download security patches from the SUS server. Configure the SUS server to redirect clients to the Windows Update Web site.
- D. Configure the GPO to download security patches from the SUS server. Configure the SUS server to download and store security patches locally.

Answer: C

Question: 48(B)

Exhibit, SUS configuration Exhibit, GPO



You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. You deploy Software Update Services (SUS) as a part of your patch management strategy. You configure a SUS server named Company9 as displayed in the SUS exhibit.

You edit the Default Domain Policy Group Policy object (GPO) to configure client computers to download updates from the SUS server as shown in the GPO exhibit. Users report that at times the performance of the Internet connection is unacceptably slow. You examine the network and discover that the slowdown occurs shortly after a new security patch is approved. You need to ensure

that the performance of the Internet connection does not decrease when you approve a new security patch. What should you do?

- A. Configure the existing GPO to install security patches during off-peak hours.
- B. Install a second SUS server. Configure a new GPO to use the second server. Filter the new GPO to apply to half the client computers.
- C. Configure the SUS server to download and save the updates to a local folder.
- D. Configure the SUS server to automatically approve new versions of approved updates.

Answer: C

Question: 49(A)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run either Windows XP Professional or Windows 2000 Professional. You decide to use Software Update Services (SUS) as part of your patch management strategy. You need to test all software updates on test computers before you distribute the updates to your entire production network. You want to achieve this goal by using the minimum amount of administrative effort while ensuring that all computers receive updates on a regular basis. What should you do?

- A. Deploy one SUS server. On test computers, configure Automatic Updates to install updates without user involvement. On production computers, configure Automatic Updates to ask for user approval before installing updates. Send out global e-mail that users when it is safe to apply new updates to production computers.
- B. Deploy one SUS server. On test and production computers, configure Automatic Updates to install updates without user involvement. Use Group Policy to enable or disable Automatic Updates on production computers according to results from the test computers.
- C. Deploy two SUS servers. Configure one server to the test computers and one server for the production computers. Configure the test computers to use the test SUS server for updates. Configure the production computers to use the production SUS server for updates.
- D. Deploy two SUS servers. Configure one server to the test computers and one server for the production computers. Configure the test computers to use the test SUS server for updates. Configure the production computers to use the production SUS server for updates. Use Group Policy to enable to disable Automatic Updates on the production computers according to results from the test computers.

Answer: C

Explanation:

Rolling Out SUS to Your Production Environment Most people agree that before you install a new update on computers, you should first test it in your production environment. Typically, you should install a new fix with a limited rollout on some noncrucial computers and observe those computers for a week or so. At the same time, you should read the Windows & .NET Magazine UPDATE newsletters (http://email.winnetmag.com/winnetmag/winnetmag_prefctr.asp) to learn about problems early adopters have encountered. You can then roll out the update to your larger production environment. You can use two simple methods to implement the rollout process with SUS. The low-tech method involves simply downloading and installing the update manually on your test systems. When you're ready to roll out the update to your production environment, approve the update on your SUS server, as Part 1 describes. This method is appropriate for small networks, but SUS also supports a more controlled and automated method for coordinating testing and deployment of crucial updates. To use this more sophisticated method, you need to set up two SUS servers—let's call them SUSTest and SUSProd. Configure your production computers to pull their updates from SUSProd by editing an appropriate Group Policy Object (GPO) that you apply to all your production computers; maneuvering to Computer Configuration, Administrative Templates, Windows Components, Windows Update; and entering SUSProd as the Set intranet update service for detecting updates option. Next, create another GPO, link it to your test computers, and enter SUSTest as the Set intranet update service for detecting updates option. To test an update, simply approve it on SUSTest and all your test computers will install it. After you're satisfied that the update is safe for wider deployment, log on to SUSProd and approve the update. To reduce the likelihood of errors (e.g., accidentally approving the update in SUSProd before you approve it in SUSTest), you can create separate user accounts such as SUSTestAdmin and SUSProdAdmin and place each user in the local Administrators group on the corresponding SUS server.

Let's hope that Microsoft will enhance SUS so that you can manage both your test and production environments from one SUS server and that you can someday use SUS to require that an update be approved in the test environment before you can approve it in production. But, for now, the dual SUS server method isn't a bad solution. If you need to approve different updates for different types of computers (e.g., servers, workstations, domain controllers—DCs) in your production environment, you need to set up different SUS servers for each of type of system and configure those systems to pull updates from their corresponding SUS servers.

Question: 50(A)

You are a security administrator for Company.com. The network consists of a single Active Directory forest named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Several client computers at Company.com are kiosk computers and are in public locations. Company.com's written security policy states the following requirements for the use of kiosk computers:

- Users must use Remote Desktop Connection to connect to application servers and client computers
- User can run only applications that are stored in the Windows and the Program Files folders.

Local administration can run any application. You place all kiosk client computers in an OU named Kiosk. You create a new GPO named KioskPolicy, and you link the KioskPolicy GPO to the Kiosk OU. You create a software restrictions policy in the KioskPolicy GPO. You need to configure the software policy in the KioskPolicy GPO. Which two actions should you perform? (Each correct answer presents part of the solution. Select two)

- Change the default security level to disallowed.

- Change the default enforcement policy to allow local administrators to run any application.

- Create a certificate rule to allow all software signed by Microsoft.

- Create a path rule to allow Remote Desktop Connection.

Answer: A, B

Question: 51(A)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The Company.com domain contains Windows Server 2003 computers and Windows XP Professional client computers. All computers are members of the domain.

The employee user accounts in the Company.com company are members of the Administrators local group on client computers. You occasionally experience problems managing client computers because an employee removes the Domain Admins global group from the Administrators local group on the computer. You need to prevent employees from removing the Domain Admins global group from the Administrators local group on client computers. What should you do?

- A. Apply a security template to the client computers that establishes the Domain Admins global group as a member of the Administrators local group by using the Restricted Groups policy.
- B. Apply a security template to the domain controller computers that establishes the Domain Admins global group as a member of the Administrators domain local group by using the Restricted Groups policy.
- C. Modify the Domain Admins global group by assigning the Allow – Full Control permission to the Domain Admins global group.
- D. Modify the Domain Admins global group by assigning the Deny – Full Control permission to the Domain Admins global group.

Answer: A

Explanation:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;279301> Description of Group Policy Restricted Groups View products that this article applies to. This article was previously published under Q279301 SUMMARY: This article provides a description of Group

Policy Restricted groups. Restricted groups allow an administrator to define the following two properties for security-sensitive (restricted) groups: Members Member Of The "Members" list defines who should and should not belong to the restricted group. The "Member Of" list specifies which other groups the restricted group should belong to. Using the "Members" Restricted Group Portion of Policy When a Restricted Group policy is enforced, any current member of a restricted group that is not on the "Members" list is removed with the exception of administrator in the Administrators group. Any user on the "Members" list which is not currently a member of the restricted group is added. Using the "Member Of" Restricted Group Portion of Policy Only inclusion is enforced in this portion of a Restricted Group policy. The Restricted Group is not removed from other groups. It makes sure that the restricted group is a member of groups that are listed in the Member Of dialog box.

Question: 52(A)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The Company.com domain contains Windows Server 2003 computers and Windows XP Professional client computers. Some of the servers in the company are file servers. The file servers contain shared files that users in the sales and marketing department use. The file servers are in an OU named FileServers. The Company.com's written security policy states that the date and time that user successfully establishes a session to a file server must be recorded. The written security policy also states that the date and time of successful and unsuccessful attempts to modify files on the file server must be recorded. You create a new GPO and link to the FileServers OU. The Audit Policy section of the GPO is shown exhibit. You need to configure the audit policy to meet the requirements of the written security policy. You must achieve this goal by using the minimum number of audit settings. What should you do?

Drag and Drop

Policy Settings	Work Area																				
Success, Failure	<table border="1"> <thead> <tr> <th>Policy</th> <th>Policy Setting</th> </tr> </thead> <tbody> <tr> <td> Audit account logon events</td> <td>Not Defined</td> </tr> <tr> <td> Audit account management</td> <td>Not Defined</td> </tr> <tr> <td> Audit directory service access</td> <td>Not Defined</td> </tr> <tr> <td> Audit logon events</td> <td>Not Defined</td> </tr> <tr> <td> Audit object access</td> <td>Not Defined</td> </tr> <tr> <td> Audit policy change</td> <td>Not Defined</td> </tr> <tr> <td> Audit privilege use</td> <td>Not Defined</td> </tr> <tr> <td> Audit process tracking</td> <td>Not Defined</td> </tr> <tr> <td> Audit system events</td> <td>Not Defined</td> </tr> </tbody> </table>	Policy	Policy Setting	Audit account logon events	Not Defined	Audit account management	Not Defined	Audit directory service access	Not Defined	Audit logon events	Not Defined	Audit object access	Not Defined	Audit policy change	Not Defined	Audit privilege use	Not Defined	Audit process tracking	Not Defined	Audit system events	Not Defined
Policy	Policy Setting																				
Audit account logon events	Not Defined																				
Audit account management	Not Defined																				
Audit directory service access	Not Defined																				
Audit logon events	Not Defined																				
Audit object access	Not Defined																				
Audit policy change	Not Defined																				
Audit privilege use	Not Defined																				
Audit process tracking	Not Defined																				
Audit system events	Not Defined																				
Success																					
Failure																					

Answer:

Policy Settings	Work Area																				
Success, Failure Success Failure	<table border="1"> <thead> <tr> <th>Policy</th> <th>Policy Setting</th> </tr> </thead> <tbody> <tr> <td> Audit account logon events</td> <td>Not Defined</td> </tr> <tr> <td> Audit account management</td> <td>Not Defined</td> </tr> <tr> <td> Audit directory service access</td> <td>Not Defined</td> </tr> <tr> <td> Audit logon events</td> <td>Success</td> </tr> <tr> <td> Audit object access</td> <td>Success, Failure</td> </tr> <tr> <td> Audit policy change</td> <td>Not Defined</td> </tr> <tr> <td> Audit privilege use</td> <td>Not Defined</td> </tr> <tr> <td> Audit process tracking</td> <td>Not Defined</td> </tr> <tr> <td> Audit system events</td> <td>Not Defined</td> </tr> </tbody> </table>	Policy	Policy Setting	Audit account logon events	Not Defined	Audit account management	Not Defined	Audit directory service access	Not Defined	Audit logon events	Success	Audit object access	Success, Failure	Audit policy change	Not Defined	Audit privilege use	Not Defined	Audit process tracking	Not Defined	Audit system events	Not Defined
Policy	Policy Setting																				
Audit account logon events	Not Defined																				
Audit account management	Not Defined																				
Audit directory service access	Not Defined																				
Audit logon events	Success																				
Audit object access	Success, Failure																				
Audit policy change	Not Defined																				
Audit privilege use	Not Defined																				
Audit process tracking	Not Defined																				
Audit system events	Not Defined																				

Question: 53(A)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. One hundred Company.com users are currently using an application named CompanyApp. CompanyApp is stored in a folder on the hard disk of each user's client computer. To secure CompanyApp, you create a new GPO named CompanyApp Policy. The CompanyApp Policy GPO contains a file system security policy that applies a customer DACL to CompanyApp. You configure the DACL to assign all users only the Allow – Read permission. You filter the CompanyApp Policy GPO to apply only to computers that have CompanyApp installed. After you apply the CompanyApp GPO, users immediately report that they receive an error message when they attempt to use CompanyApp. You delete the entry for CompanyApp in the file system security policy. Users continue to report that they receive the same error message when they attempt to use CompanyApp. You need to configure the network so that users can use CompanyApp. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. Delete the CompanyApp Policy GPO. Restart all client computers.
- B. Create a new file system security policy in the CompanyApp Policy GPO that assigns default permissions to CompanyApp.
- C. Import the Setup security.inf security template into the CompanyApp Policy GPO.
- D. Disable the CompanyApp Policy GPO.

Answer: B

Question: 54(A)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All servers are in an OU named Servers, or in OUs contained within the Servers OU. Based in information in recent security bulletins, you want to apply settings from a security template named Messenger.info to all servers on which the Messenger service is started. You do not want to apply these settings to servers on which the Messenger service is not started. You also do not want to move servers to outer OUs. You need to apply the Messenger.inf security template to the appropriate servers. What should you do?

- A. Import the Messenger.info security template into a GPO, and link the GPO to the Servers OU. Configure Administrative Templates filtering in the GPO.
- B. Import the Messenger.info security template into a GPO, and link the GPO to the Servers OU. Configure a Windows

Management Instrumentation (WMI) filter for the GPO.

- C. Configure a logon script in a GPO, and link the GPO to the Servers OU. Configure the script to run the gpupdate command if the Messenger service is running.
- D. Edit the Messenger.info security template to set the Messenger service startup mode to Automatic, and then run the secedit /refreshpolicy command..

Answer: B

Question: 55(A)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. One server named Company3 is not a member of the domain. The other servers are members of the domain. Company.com's written security policy states that all servers must have certain security settings, including specific event log settings and registry permissions settings. The required security settings are specified in a security template named Company.inf. You need to apply the settings from Company.info security template to Company3. You do not want to add Company3 to the domain. What should you do?

- A. On Company3, from the Administrative Tools menu, open Local Security Policy, and then use the Import Policy command to import Company.inf.
- B. On Company3, open Local Security Policy, and then select Security Settings. Use the Import Policy command to import Company.inf.
- C. On Company3, open Security Configuration and Analysis. Use the Import Template command to import Company.inf, and then use the Configure Computer Now command.
- D. On Company3, copy Company.inf to the *Systemroot*\Security\Templates folder.
- E. On Company3, copy Company.inf to the *Systemroot*\System32\GroupPolicy\Machine folder.

Answer: C

Question: 56(A)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Terminal Services is running on four Windows Server 2003 computers. Members of a group named Remote Application need to access applications by using Terminal Services. You assigned the Remote Application group the appropriate NTFS permissions for the application folder and the appropriate RDP-Tcp connection permissions on the terminal servers. Currently no users have the right to connect to the terminal servers. You need to assign users in the Remote Application group the minimum rights necessary to access the applications. What should you do to configure the terminal servers?

- A. Apply a security template that assigns the Access this computer from the network right to the Remote Application group.
- B. Apply a security template that assigns the Allow log on locally right to the Remote Application group.
- C. Apply a security template that assigns the Log on as a service right to the Remote Application group.
- D. Apply a security template that assigns the Allow log on through Terminal Services right to the Remote Application group.

Answer: D

Explanation:

Allow log on through terminal services; Windows Server 2003 ... Allow log on through Terminal Services
Description This security setting determines which users or groups have permission to log on as a Terminal Services client. Default: On workstation and servers: Administrators, Remote Desktop Users. On domain controllers: Administrators. Configuring this security setting You can configure this security setting by opening the appropriate policy and expanding the console tree as such: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\ For specific instructions about how to configure security policy settings, see To edit a security setting on a Group Policy object. This setting does not have any effect on

Windows 2000 computers that have not been updated to Service Pack 2. For more information, see: Deny logon through Terminal Services User rights assignment To assign user rights for your local computer Security Configuration Manager Tools

Accessing Terminal Services Using New User Rights Options

SUMMARY This article describes new options that you can use to assign user rights in Windows that affect the Terminal Services feature. **MORE INFORMATION** Windows Server 2003 includes the following new User Rights options: • Allow logon through Terminal Services

Deny logon through Terminal Services You can use these options to change the set of permissions a user must have to establish a Terminal Services session. To establish a Terminal Services session, a user must have the following permissions:

Allow logon through Terminal Services To grant a user these permissions, start the Group Policy snap-in, open the Local Security Policy or the appropriate Group Policy, and then navigate to the following location: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Allow logon to Terminal Server To grant a user these permissions, start either the Active Directory Users and Computers snap-in or the Local Users And Groups snap-in, open the user's properties, click the Terminal Services Profile tab, and then click to select the Allow logon to Terminal Server check box.

Guest Access: Logon to the RDP-TCP connection To grant guests Logon rights to the RDP-TCP connection, start the Terminal Services Configuration snap-in, edit the RDP-TCP so that the guest has at least Logon rights. The pivotal difference between Windows 2000 and Windows Server 2003 is the "Allow logon through Terminal Services" user right. When you grant this user right, you no longer have to grant the user the Log on locally right (this was a requirement in Windows 2000). In Windows Server 2003, it is possible for a user to establish a Terminal Services session to a particular server, but not be able to log on to the console of that same server.

Question: 57(A)

You are a security administrator for Company.com. All domain controllers run Windows Server2003. All client computers run Windows XP Professional. Company has offices in Berlin, Bonn,Stuttgart, and Frankfurt. The network consists of a single Active Directory forest that contains four domains. The domains are named berlin.Company.com, bonn.Company.com, stuttgart.Company.com andfrankfurt.Company.com. Each city is configured as an Active Directory site. Each site contains file servers and client computers from every domain. To comply with local laws, the Company.com's written security policy states that security eventson file servers must be maintained as shown in the following table:

City	Presentation
Berlin	14 days
Bonn	28 days
Stuttgart	10 days
Frankfurt	31 days

You need to configure the network to comply with the written security policy. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. In each domain, create an OU for each of the other domains. Create a new GPO and link it to each OU. Configure each GPO to meet the requirements of the written security policy.
- B. Create a GPO for each city and link each GPO to the corresponding site. Configure each GPO to meet the requirements of the written security policy.
- C. Modify the Default Domain Policy GPO in each domain. Configure the GPO to meet the requirements of the written security policy.
- D. Modify the Default Domain Controllers Policy GPO in each domain. Configure the GPO to meet the requirements of the written security policy.

Answer: B

Explanation:

Special Considerations for Site-linked GPOs GPOs linked to sites might be appropriate to use for setting policy for proxy settings and network-related settings. Any GPO that is linked to a site container is applied to all computers in that site, regardless of which domain in the forest the computer belongs to. This has the following implications: Ensure that the computers do not access a site Group Policy object across a WAN link, which would lead to significant performance issues. By default, to manage site GPOs, you need to be either an Enterprise Admin, or the domain admin of the forest root domain. Active Directory service data-replication between domain controllers in different sites occurs less frequently than replication between domain controllers in the same site, and occurs during scheduled periods only. Between sites, FRS replication occurs spontaneously, and is not determined by the site link replication schedule; this is not an issue within sites. The directory service replication schedule and frequency are properties of the site links that connect sites. The default inter-site replication frequency is three hours. To change it, go to the appropriate site link, go to the IP link, and change the replication frequency or schedule as needed. Changing either the replication frequency or schedule can significantly affect policy. For example, assume that you have replication set to three hours or longer, and you create a GPO and link it to an OU in a domain that spans several sites. You will likely need to wait several hours before all users in that OU receive the GPO. If most of the users in an OU are in a remote location, and you have a domain controller in that site, you can work around inter-site replication latency by performing all Group Policy operations on a domain controller in that site.

Question: 58(C)

You are a security administrator for Company.com. Company.com uses an accounting and payroll application. Twenty payroll clerks use the application to input data from their client computers to a database running on a Microsoft SQLServer 2000 computer named Company6. You need to prevent unauthorized interception of the data as it travels over the company network. What are two possible ways to achieve this goal? (Each correct answer is a complete solution. Select two.)

- A. Configure SQL Server 2000 on Company6 to use SSL.
- B. Configure an IPSec policy to require Authentication Headers (Ahs) between the payroll client computers and Company6.
- C. Configure an IPSec policy Encapsulating Security Payload (ESP) between the payroll client computers on Company6.
- D. Configure Company6 to require Server Message Block (SMB) signing.

Answer: A, C

Question: 59(D)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Eight Windows 2003 computers are members of the domain. These computers are used to store confidential files. They reside in a data center that only IT administration personnel have physical access to. You need to restrict members of a group named Contractors from connecting to the filer server computers. All other employees require to these computers. What should you do?

- A. Apply a security template to the filer server computers that assigns the Access this computer from the network right to the Domain Users group.
- B. Apply a security template to the filer server computers that assigns the Deny access to this computer from the network right to the Contractors group.
- C. Apply a security template to the filer server computers that assigns the Allow log on locally right to the Domain Users group.
- D. Apply a security template to the filer server computers that assigns the Deny log on locally right to the Contractors group.

Answer: B

Explanation: Deny access to this computer from the network Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment Description Determines which users are prevented from accessing a computer over the network.

Question: 60(C)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run either Windows XP Professional or Windows NT Workstation 4.0. Company.com's written security policy states that all users must acknowledge a legal message before they use any client computers. You need to configure the network to ensure that all client computers comply with the written security policy. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Create a new GPO and link it to an OU. Configure the GPO to display the legal message. Place all Windows XP Professional computers in the OU.
- B. Create a new GPO and link it to an OU. Configure the GPO to display the legal message. Place all Windows NT Workstation 4.0 computers in the OU.
- C. Modify the Default Controllers Policy GPO by configuring it to display the legal message.
- D. Create a Config.pol file that displays the legal message. Place the file in the SYSVOL shared folder.
- E. Create a Config.pol file that displays the legal message. Place the file in the NETLOGON shared folder.

Answer: A, E

Question: 61(C)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. Company.com provides remote access to the company network for domain users that work from home. Users create VPN connections to a remote access server named Company4. Company4 is a member server in the domain. The authentication provider on the remote access server is Windows Authentication. To minimize the risk of a dictionary attack on user password, you implemented a domain account lockout policy in Active Directory. You also configured remote access account lockout on Company4. The account lockout threshold in the domain and the maximum number of failed attempts on Company4 are both set to four invalid logon attempts. The account lockout counters in the domain are reset after one hour. The account lockout counters on Company4 are reset after two hours.

You receive reports that several users in the domain were prevented from logging on to the Company.com network because invalid remote access login attempts locked the domain user accounts. You need to ensure that invalid remote access logon attempts do not cause the domain user account to lock out. You do not want to disable the domain account lockout policy. What should you do?

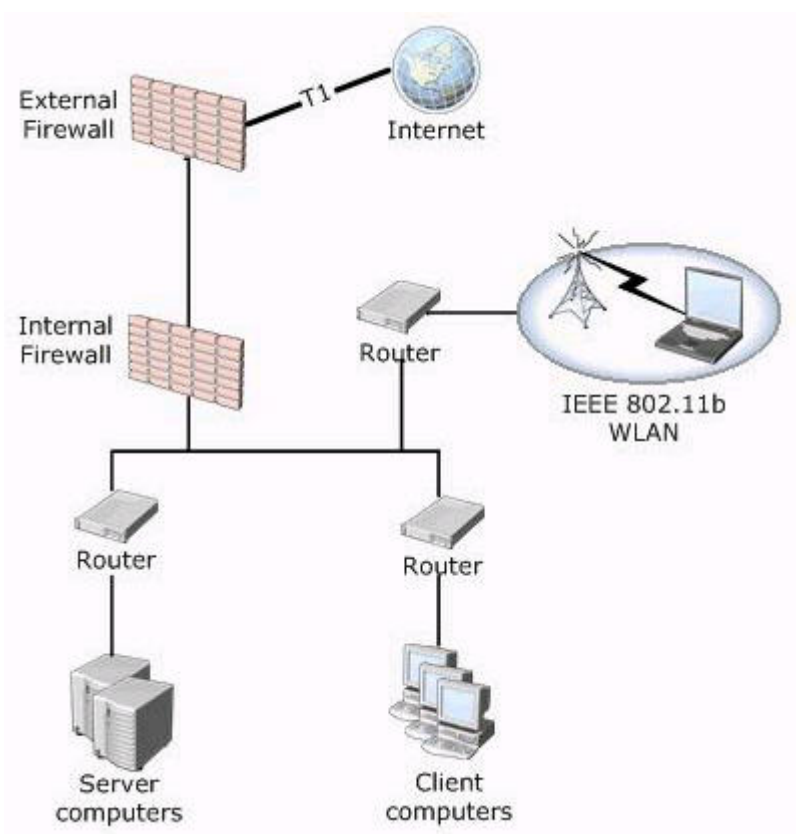
- A. Configure the remote access service on Company4 to not accept the MS-CHAP authentication method.
- B. Configure the maximum number of failed attempts on Company4 to three invalid logon attempts.
- C. Configure an account lockout policy in a GPO that is linked to the OU than contains Company4. Use an account lockout threshold of three.
- D. Add Company4 computer account to the Windows Authorization Access Group security group.

Answer: B

Explanation: Since domain lockout needs to be minimized, the best option is to allow the lockout to occur on the remote access server.

Question: 62(C)

Network topology exhibit Exhibit, WLAN





You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. The network topology is shown in the exhibit. Users in the sales department use portable computers that are not connected to the Company.com network. Each week sales users travel to Company.com main Office in Toronto and connect to the IEEE.802.11b wireless LAN (WLAN). The WLAN is configured as shown in the WLAN Exhibit. The WLAN hardware does not support IEEE.802.1x. Once a week, sales users connect to the WLAN to retrieve confidential sales documents from the file servers on the network. You discover that unauthorized users intercepted data in sales documents while the documents were transmitted over the WLAN. You need to protect sales documents from being intercepted by unauthorized users. What should you do?

- A. Configure a new VPN server on the corporate network. Configure a Connection Manager Administration Kit (CMAK) profile that connects sales users to the VPN server.
- B. Disable NetBIOS on all portable computers and file servers.
- C. Configure a packet filter on the Company3 router, which is the router that separates the WLAN and the corporate network. Configure the packet filter to allow only traffic from the WLAN to enter the Internal network.
- D. Configure the file server that contains sales documents to be trusted for delegation. Instruct sales users to use Encrypting File System (EFS) when storing files on the file server.

Answer: A

Question: 63(D)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The Company.com domain contains Windows Server 2003 computers and Windows XP Professional client computers. All computers are members of the domain, except the server Company5. The network contains an enterprise certification authority (CA). All computers on the network trust the CA. Company.com's written security policy states that all network traffic from the computers in the

domain to Company5 must be encrypted. Company5 must not be added to the domain. You configure a GPO that assigns the predefined IPsec policy named Client (Respond Only). You link the GPO to the domain. You configure Company5 to use the predefined IPsec policy named Secure Server (Require Security). When need to implement the written security policy. What should you do?

- A. Disable the default exemptions to IPsec filtering on all computers in the domain.
- B. Disable the default response rule in the Client (Respond Only) IPsec policy in the domain.
- C. Configure Company5 so that it uses the predefined IPsec policy named Server (Request Security).
- D. Configure the security options of the local computer policy on Company4 to always digitally sign communications.
- E. Configure the assigned IPsec policies on Company5 and in the domain to use certificate-based authentication.

Answer: E

Explanation: IPsec and Group Policy: The Next Step www.winnetmag.com/WindowsSecurity/Article/ArticleID/26112/26112.html
When you use IPsec certificate-based authentication, you limit authentication to certificates from a specific CA. Therefore, you need to use a dedicated Enterprise CA for each IPsec policy you plan to configure. ... You can use an existing Enterprise CA, so long as you don't need to issue IPsec certificates from that CA for other reasons. If you don't have an existing CA that you can use for this purpose, install Certificate Services on any Win2K server that's a member of your AD domain.

Question: 64(C)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The Company.com domain contains Windows Server 2003 computers and Windows XP Professional client computers. All computers are members of the domain. A Windows Server 2003 computer named Company3 runs Certificate Services. Company3 is an enterprise subordinate certification authority (CA). A Windows Server 2003 computer named Company2 runs IIS. Company2 hosts an internal human resources web site for employees. You want to ensure that the personal data of the employees is not exposed while in transit over the network. You decide to use SSL on Company2. You need to ensure that employees do not receive a certificate-related security alert when they use SSL to connect to this Web site. You want to achieve this goal without spending money to purchase this certificate unless it is necessary to do so. What should you do?

- A. Use IIS to submit a certificate request to a commercial CA.
- B. Use IIS to submit a certificate request to Company3.
- C. Use the Certificates console to submit a Client certificate request to a commercial CA.
- D. Use the Certificates console to submit a Client certificate request to Company3.

Answer: B

Explanation: Using Client Certificate Authentication with IIS 6.0 Web Sites Request a User Certificate from the Web Enrollment Site
The client computer must present a user certificate to the Web server before the Web server will accept the user's credentials. Users can log on to the Web enrollment site and request a user certificate. The user does not need to be an administrator in the domain or on the Certificate Server computer. The user only needs to have legitimate user credentials that the enterprise CA recognizes. Perform the following steps on the client computer to obtain the user certificate"

- 1 On the Web client computer, open Internet Explorer and enter <http://10.0.0.2/certsrv> in the address bar, where 10.0.0.2 is the IP address of the Certificate Server. Press ENTER.
- 2 In the log on dialog box, enter the credentials of a non-administrator user. This will demonstrate that a non-admin can obtain a user certificate. Click OK.
- 3 On the Welcome page of the Web enrollment site, click the Request a certificate link.
- 4 On the Request a Certificate page, click the User Certificate link.
- 5 On the User Certificate – Identifying Information page, click Submit.
- 6 Click Yes on the Potential Scripting Violation dialog box informing you that the Web site is requesting a certificate on your behalf.
- 7 On the Certificate Issued page, click the Install this certificate link.

- 8 Click Yes on the Potential Scripting Violation page informing you that the Web site is adding a certificate to the machine.
- 9 Close Internet Explorer after you see the Certificate Installed page. Generating a Certificate Request File Using the Certificate Wizard in IIS 5.0 The Certificate Wizard that comes with Internet Information Services (IIS) 5.0 makes managing server certificates easier than ever before. This article describes how to create a certificate request file using the wizard. The first step you will...

Question: 65(A)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All 80 servers run Windows Server 2003. All 2,000 client computers run Windows XP Professional. All computers are members of the domain. A windows Server 2003 computer named Company7 functions as an internal Web server. Employees in the marketing department regularly upload files to Company7 using the FTP service. You decide to protect this data while it is in transit via FTP to Company7. You implement IPsec and assign the default IPsec Secure Server policy on Company7. You implement IPsec and assign the default IPsec client policy on the marketing client computer. You verify that the FTP data is encrypted by monitoring the traffic between the marketing department client computer and Company7. Users report that the HTTP service on Company7 is no longer accessible from client computers that are not in the marketing department. DNS queries made from Company4 also fail to resolve. You need to restore access to the normal HTTP server and DNS client functionality on Company4 while preserving the encryption of FTP data between Company7 and the marketing department client computers. What should you do?

- A. Unassign the IPsec Secure Server policy and assign the default Server policy of Company4.
- B. Unassign the Client Policy and assign a custom IPsec policy on marketing department client computers that uses authentication headers on Company7.
- C. Unassign the IPsec Secure Server policy and assign a custom IPsec policy that requires IPsec only for FTP data on Company7.
- D. Unassign the IPsec Secure Server policy and assign a custom IPsec policy that does not require IPsec for DNS data on Company7.

Answer: C

Explanation:

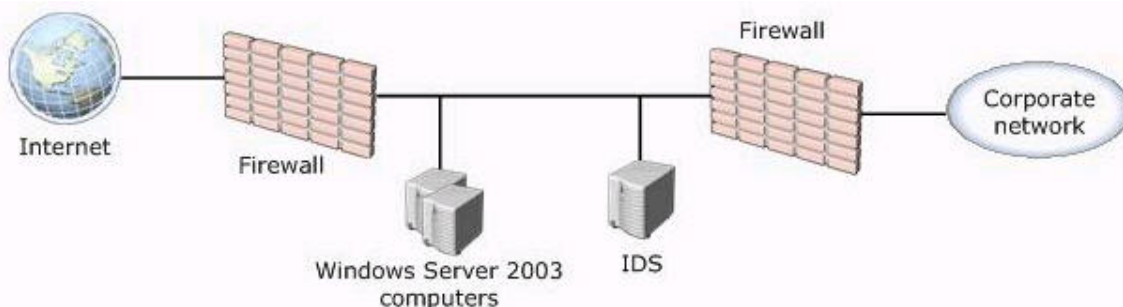
The new policy applied has caused the error. Only FTP traffic need to be secured.

Note:

FTP is commonly misunderstood as a secure means for transferring data, because the FTP server can be configured to require a valid user name and password combination prior to granting access. Be aware that neither the credentials specified at logon nor the data itself is encrypted or encoded in any way. All credentials are sent across the network in plaintext.

Question: 66(C)

Exhibit, network topology



You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. The network consists of a perimeter network that is configured as shown in the network topology exhibit. Company.com's written security policy states the following :

All computers must pass a security inspection before they are placed in the perimeter network.

Only computers that pass inspection are permitted to communicate with firewalls or other computers that pass inspection.

All communication in the perimeter network is inspected by a network-based intrusion-detection system (IDS).

Communication between computers in the perimeter network must use the strongest possible authentication methods. You decide to deploy IPSec in the perimeter network to enforce the written security policy. You enable IPSec on the firewall computers. You need to plan IPSec configuration for the Windows Server 2003 computers so that it meets the written security policy. Which three actions should you perform to configure IPSec? (Each correct answer presents a part of the solution. Select three.)

Configure tunnel mode

Configure transport mode

Enable Authentication Header (AH).

Enable Encapsulating Payload (ESP).

Use Kerberos authentication.

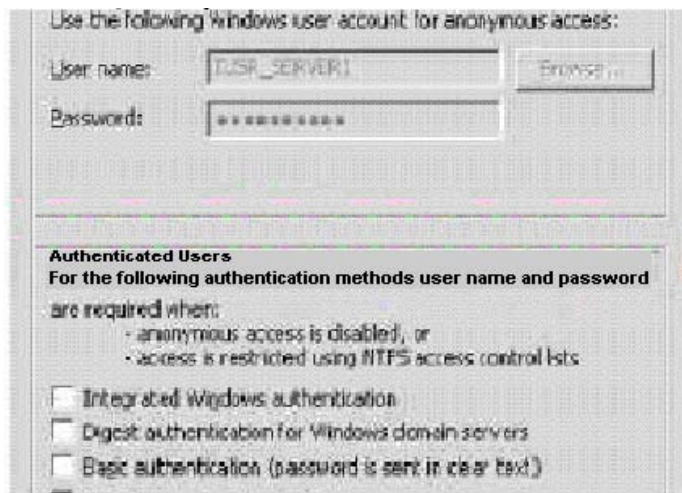
Use certificate-based authentication.

Use shared secret authentication.

Answer: B, C, E

Question: 67(A)

Exhibit, multiple hotspot



You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Company.com uses a Web application named CompanyApp. CompanyApp is hosted on a web server named Company3. Only managers who have accounts on the internal network use CompanyApp. Managers are members of a global group named CompanyManagers. Only CompanyManagers has access to CompanyApp. You need to ensure that only managers can access CompanyApp and that managers are required to enter their user name and password as seldom as possible. You need to configure IIS to support the required authentication. To answer, configure the appropriate option or options in the exhibit.

Answer: Integrated Windows authentication

Explanation:

Integrated Windows authentication, and only Integrated Windows authentication, meets the requirements of this scenario. Since only managers are allowed to access and are members of the domain, they are already authenticated to the domain. Integrated auth will simply accept the user credential used from the client workstation.

Question: 68(A)

You are a security administrator for Company.com. The network consists of two Active Directory forests that contain two domains. The domains are named Company.com and foo.com. All Active Directory domains are running at a Windows Server 2000 mixed mode functionality level. Employees in the help desk department need to modify certain attributes of employee user accounts that reside in the Company.com domain. The help desk department user accounts reside in the foo.com domain. You need to create a single group named Help Desk that contains all help desk department user accounts and that can be granted access to modify employee user accounts in the Company.com domain. What should you do?

- A. Use a universal security group in the Company.com domain named Help Desk.
- B. Use a universal security group in the foo.com domain named Help Desk.
- C. Use a global security group in the foo.com domain named Help Desk.
- D. Use a global security group in the Company.com domain named Help Desk.

Answer: C

Question: 69

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Company.com occasionally experiences downtime because of malicious Internet worms that arrive as Microsoft Visual Basic scripting Edition (VBS) files. You examine several client computers and discover that VBS files are downloaded by using Microsoft Outlook, instant messaging, or peer-to-peer file sharing programs. You need to prevent users from running VBS files regardless of how they arrive on client computers. What should you do?

- A. Use a software restriction policy to disable all unauthorized scripts.
- B. Use an Administrative Template to ensure that Outlook and Internet Explorer are in the Restricted Sites security zone.
- C. Use a centralized login script to rename the Wscript.exe file on each computer to contain a nonexecutable extension.
- D. Use a file system security policy to assign the Deny – Execute permission for the Wscript.exe file.

Answer: A

Question: 70(D)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The Company.com domain contains Windows Server 2003 computers and Windows 2000 Professional client computers. Three Windows Server 2003 computers are named Company1, Company2, and Company3. You want to implement a public key infrastructure (PKI) to support the security requirements in Company.com. All certification authorities (CAs) must belong to the same CA hierarchy. You plan to install Certificate Services on Company1 first. Company1 will not be connected to the network and will be stored in a locked cabinet in the Company.com data center. You plan to use Company2 to issue certificates for IPSec and Encrypting File System (EFS). You will configure Company2 to automatically issue these certificates. You plan to use Company3 to issue certificates that enable business partners to authenticate to your IIS Web site. Company3 will not be a member of the Active Directory domain. You need to configure Certificate Services on each server to fulfill the server's designated role. What should you do?

Drag and Drop

Company1	Place here
Company2	Place here
Company3	Place here

Certificate Services Configurations,
select from these

Stand-alone root CA	Stand-alone subordinate CA
Enterprise root CA	Enterprise subordinate CA

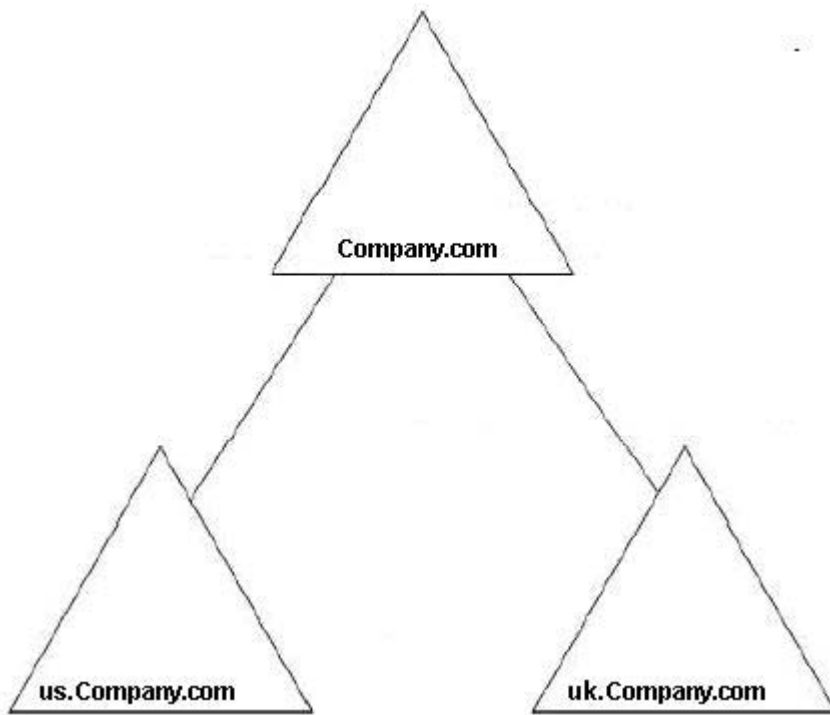
Answer:

Company1	Stand-alone root CA
Company2	Enterprise subordinate CA
Company3	Stand-alone subordinate CA

Certificate Services Configurations,
select from these

Stand-alone root CA	Stand-alone subordinate CA
Enterprise root CA	Enterprise subordinate CA

Question: 71
Exhibit



You are a security administrator for Company.com. The network consists of two Active Directory forests named Company.com and foo.com. The functional level of the Company.com forest is Windows Server 2003. The Company.com forest is displayed in the exhibit. The foo.com forest consists of a single Active Directory domain. Domain controllers in the Company.com forest run either Window Server 2003 or Windows 2000 Server. Technical support personnel in the uk.Company.com domain are responsible for creating useraccounts in the foo.com domain. Company.com's written security policy states that each user is permitted to have only one user account. You need to configure the network to allow technical support personnel to create user accounts in the foo.com domain. What should you do?

- A. Create a one-way external trust relationship in which the foo.com domain trusts the Company.com domain.
- B. Create a one-way external trust relationship in which the Company.com domain trusts the foo.com domain.
- C. Create a one-way external trust relationship in which the uk.Company.com domain trusts the foo.com domain.
- D. Create a one-way external trust relationship in which the foo.com domain trusts the uk.Company.com domain.

Answer: D

Question: 72(A)

You are a security administrator for Company.com. The network consists of two Active Directory domains named Company.com and de.Company.com. These domains are in the same Active Directory forest. Both domains operate at a Windows 2000 mixed mode functional level. A Windows Server 2003 computer named Company7 issues certificates for users and computer in the Company company. Company7 is a member in the Company.com Active Directory domain.

You plan to use Company7 to deploy certificates to authorized computer in the de.Company.comActive Directory domain. You need to create an access control solution that restricts certificate enrollment to authorizedcomputers. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. Add the accounts of authorized computers to a global group in the de.Company.com domain.
- B. Add the accounts of authorized computers to a universal group in the de.Company.com domain.
- C. Add the accounts of authorized computers to a global group in the Company.com domain.
- D. Add the accounts of authorized computers to a universal group in the Company.com domain.

Answer: A

Question: 73(D)

Exhibit



You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Company.com hosts Web applications for customers. Each customer is a company that has multiple employees who require access to the Web applications. Each customer has one Web application. Each Web application is configured as a virtual directory. The virtual directory is configured as shown in the exhibit. Many-to-one certificate mapping is configured to authenticate users that attempt to access the virtual directory. Customers request certificates from private and public certification authorities (CAs).

You discover that unauthorized users accessed Web application by using certificates that were issued by CAs that are not authorized to issue certificates to customers. You need to ensure that only authorized employees can access their company's Web application. What should you do?

- A. Configure each Web application to use a certificate trust list (CTL). Include only CAs that you trust to issue certificates to customers in the CTL.
- B. Create a new enterprise subordinate CA that uses qualified subordination. Issue Client Authentication certificates for each employee of each customer that requires access to the Web application.
- C. Create a new enterprise subordinate CA. Cross certify the new enterprise subordinate CA with each CA that you trust to issue certificates to customers.
- D. Configure the Web server to enable the Windows directory services mapper.

Answer: D

Question: 74(D)
Exhibit

Kim Properties

Environment | Sessions | Remote control
Terminal Services Profile | COM+ | Additional Account Info
General | Address | Account | Profile | Telephones | Organization
Published Certificates | Member Of | Dial-in | Object | Security

Group or user names:

- Everyone
- Pre-Windows 2000 Compatible Access (CONTOSO\Pre-Windows...)
- RAS and IAS Servers (CONTOSO\RAS and IAS Servers)
- SELF**
- SYSTEM
- Terminal Server License Servers (CONTOSO\Terminal Server Lic...)

Add... Remove

Permissions for SELF

	Allow	Deny
Create All Child Objects	☐	☐
Delete All Child Objects	☐	☐
Allowed to Authenticate	☐	☐
Change Password	☒	☐
Receive As	☒	☐
Reset Password	☐	☐
Send As	☒	☐

For special permissions or for advanced settings, click Advanced.

Advanced

OK Cancel Apply

You are a security administrator for Contoso.com. The network consists of a single Active Directory domain named Contoso.com. The Contoso.com domain contains Windows Server 2003 computers and Windows XP Professional client computers. All computers are members of the domain. Contoso.com has a main office and three branch offices. Each office is configured as an Active Directory site. Each site contains domain controllers. A domain user named Kim reports that she forgot her password. She works in one of the branch offices. A desktop support technician in the main office reset Kim's password, enables the User must change password at next logon option in Kim's user and account, and then tells Kim the new password. Kim attempts to log on by using her new password and reports she cannot change the password at logon. You investigate the problem. Kim's user account is not locked out, and it is not disabled. Permissions for the user account are shown in the exhibit. You need to ensure that Kim can log on and change her password. What should you do?

- A. Assign the SELF group the Allow – Reset Password permission for Kim's user account.
- B. Assign the SELF group the Allow – Allowed to authenticate permission for Kim's user account.
- C. Assign the Everyone group the Allow – Allowed to authenticate permission for Kim's user account.
- D. Enable the Let Everyone permissions apply to anonymous users security setting in the domain.
- E. Reset Kim's password on a domain controller in her branch office.

Answer: E

Question: 75(D)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Company.com hosts an extranet Web site that allows employees from a partner company to access confidential information over the Internet. You want to require the partner company employees to use certificate-based authentication to access the extranet Web site. You have a public key infrastructure (PKI), which consists of a stand-alone root certification authority (CA) and an enterprise subordinate CA. The partner company does not have a PKI. You decide to issue certificates from your CA hierarchy to the partner company employees. The partner company certificates will require a different certificate policy than the policy currently used for issuing certificates to internal employees. Certificate revocation checking will be used during certificate-based authentication. You need to implement the necessary PKI changes to comply with these requirements. You want to achieve this goal by using the minimum amount of administrative effort. Which three actions should you perform? (Each correct answer present part of the solution. Choose three.)

- A. Use a new subordinate CA in your CA hierarchy to issue certificates to partner company employees and to the extranet Web server.
- B. Use the existing subordinate CA in your CA hierarchy to issue certificates to partner company employees and to the extranet Web server.
- C. Add the certificate of the root CA to the Trusted Root Certification Authorities store on the partner company's computers.
- D. Add the certificate of the subordinate CA to the Trusted Root Certification Authorities store on the partner company's computers.
- E. Create new HTTP Authority Information Access (AIA) paths and certificate revocation list (CRL) distribution points that specify locations on the extranet Web site.
- F. Create new LDAP Authority Information Access (AIA) paths and certificate revocation list (CRL) distribution points that specify locations on the extranet Web site.

Answer: A, C, E

Question: 76(D)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The domain contains Windows Server 2003 computers. You manage a Windows Server 2003 computer named Company6 that is a domain member server. You use IIS on Company6 to host an Internet Web site. This web site published information to employees of a partner company. The partner company network consists of a single Active Directory domain. Approximately 500 partner company employees connect over the Internet to access company confidential data on Company6. All partner company employees need access to the same data. The partner company IT department maintains a certificate authority (CA). They use this CA to issue Authentication Session certificates to all employees in their company. Copies of these certificates are stored with employee user accounts in the partner company's Active Directory domain. You need to authenticate users to Company6 based on possession of their company-issued certificate. You want to achieve this goal by using the minimum amount of administrative effort. You enable SSL and the certificate-based authentication option on Company6. You add the partner root CA certificate to the Trusted Root Certification Authorities store on Company6. Which three additional actions you perform? (Each correct answer presents part of the solution. Choose three.)

- A. Create a security group named PartnerEmployees and a user account named PartnerUser in your Active Directory domain. Add this account to the PartnerEmployees group.
- B. Create a security group named PartnerEmployees and a user account for every partner company employee in your Active Directory domain. Add these accounts to the PartnerEmployees group.
- C. Assign the PartnerEmployees group access to the appropriate data on Company6.
- D. Add a many-to-one certificate mapping in IIS on Company6. Create a mapping rule to accept certificates issued by the partner company's internal CA.
- E. Add one-to-one certificate mappings for every partner employee in IIS on Company6.

Answer: A, C, D

Note:

Many-to-one certificate mapping uses wildcard matching rules that verify whether a client certificate contains specific information, such as the issuer or subject.

Question: 77(C)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. The network contains an enterprise certificate authority (CA). The CA is trusted by all computers. One segment of the Company network is behind a device that performs Network Address Translation (NAT) and is used as a test network. The rest of the network is the production network. The computers on the test network are not members of the domain. The computers on the production network are members of the domain. The NAT device supports both TCP and UDP address translation. Users on the test network are allowed to connect to servers on the production network.

You need to ensure that FTP traffic and e-mail traffic from computers on the test network to FTP servers and mail servers on the production network is encrypted. For monitoring reasons, all other network traffic to those servers must not be encrypted. What should you do?

- A. Implement an IPsec policy that uses Encapsulating Security Payload (ESP) rules in Transport mode.
- B. Implement an IPsec policy that uses Encapsulating Security Payload (ESP) rules in Tunnel mode.
- C. Implement an IPsec policy that uses only IPsec Authentication Header (AH).
- D. Implement an IPsec policy that uses Kerberos authentication.

Answer: A

Explanation:

Transport mode is the default mode for IPsec, and it is used for end-to-end communications (for example, for communications between a client and a server). When transport mode is used, IPsec encrypts only the IP payload. Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and antireplay protection) for the IP payload. ESP in transport mode does not sign the entire packet. Only the IP payload (not the IP header) is protected. ESP can be used alone or in combination with AH.

Question: 78(C)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. You plan to deploy remote access to the network for users that work from home, including users who are member of a group named CompanyStaff. All members of the CompanyStaff group are in the Domain Users group. The Company.com's written security policy states the following remote access requirements:

Users, except member of the CompanyStaff group, are allowed to use remote access at anytime for an unlimited duration.

Members of the CompanyStaff group are allowed to use remote access during the day only for a maximum of 30 minutes. You configure and enable Routing and Remote Access on a member server named Company3. You delete the predefined remote access policy. The remote access permission for all user accounts in the domain is set to use remote access policies.

Drag and Drop

Remote Access Policy list

First Policy	Drag policy here
Second Policy	Drag policy here
Third Policy	Drag policy here

Remote Access Policies, Select from these

Domain Users - Deny - 30 minutes	Domain Users - Grant - 30 minutes
Domain Users/During day - Grant - unlimited	Staff/During day - Grant - 30 minutes
Staff/During day - Grant - 30 minutes	

Answer:

Remote Access Policy list

First Policy	Staff/During day - Grant - 30 minutes
Second Policy	Staff - Deny - unlimited
Third Policy	Domain Users/During day - Grant - unlimited

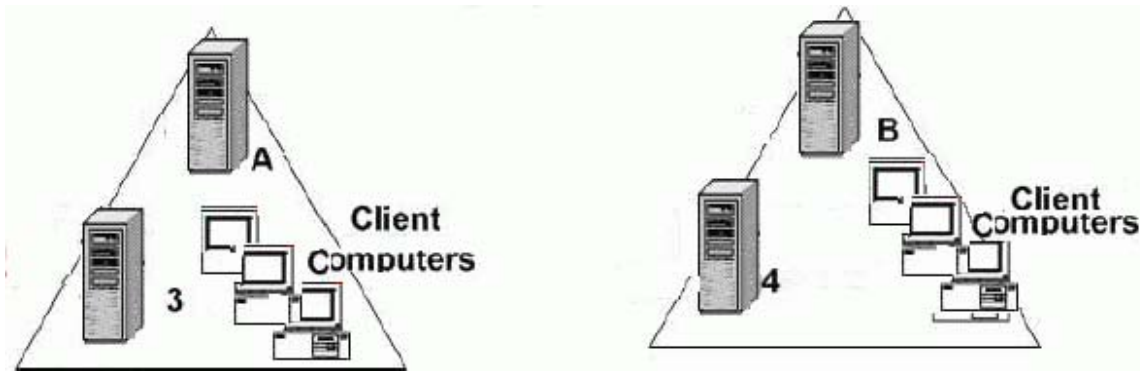
Remote Access Policies, Select from these

Domain Users - Deny - 30 minutes	Domain Users - Grant - 30 minutes
----------------------------------	-----------------------------------

Explanation:

The remote access policies are tried in order. The more specific remote access policies are placed in order ahead of the more general remote access policies. If the first policy in the ordered list of remote access policies does not match the connection attempt, the next policy is tried.

Question: 79(C)
Exhibit



You are a security administrator for Company.com. The network consists of two Active Directory domains named Company.com and foo.com. Each domain resides in a separate Active Directory forest and no trust relationships are established. The Active Directory domains each contain a Certificate Authority (CA) running Windows Server 2003 Certificate Services. These computers are named CompanyA and CompanyB. Each CA belongs to separate and isolated CA hierarchies. Computers trust only the CA in their Active Directory domain. All computers are issued a standard Computer certificate from the CA in their Active Directory domain. Two Windows Server 2003 computers named Company3 and Company4 function as file servers as shown in the exhibit. Users from both domain access confidential data on both Company3 and Company4. You decide to implement IPSec to encrypt the file data during transmission. You configure an IPSec policy that uses certificate-based IPSec authentication on both servers to encrypt file data transmissions. You configure an IPSec policy that uses certificate-based IPSec authentication on the client computers in both Active Directory domains to encrypt file data transmissions to Company3 and Company4. During testing, you notice that client computers use IPSec only when communication with the file server in the same Active Directory domain. You need to enable all client computers to use IPSec when communicating with both Company3 and Company4. What should you do?

- A. Enable the Trust Computer for delegation option on Company3 and on Company4. Add the Active Directory default (Kerberos V5 protocol) authentication method to the IPSec policies used by all computers in both Active Directory domains.
- B. Add the root CA certificates from each public key infrastructure (PKI) to the Trusted Roots Certification Authorities store on all computers in both Active Directory domains. Add the Use a certificate from this CA authentication method for the root CA certificate to the IPSec policies used by all computer in both Active Directory domains.
- C. Issue each computer in the Company.com domain an IPSec certificate from a CA in the foo.com domain. Issue each computer in the foo.com domain an IPSec certificate from a CA in the Company.com domain.
- D. Issue each computer in the Company.com domain an IPSec certificate from a CA in the Company.com domain. Issue each computer in the foo.com domain an IPSec certificate from a CA in the foo.com domain.

Answer: B

Reference:: Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure

Question: 80(C)

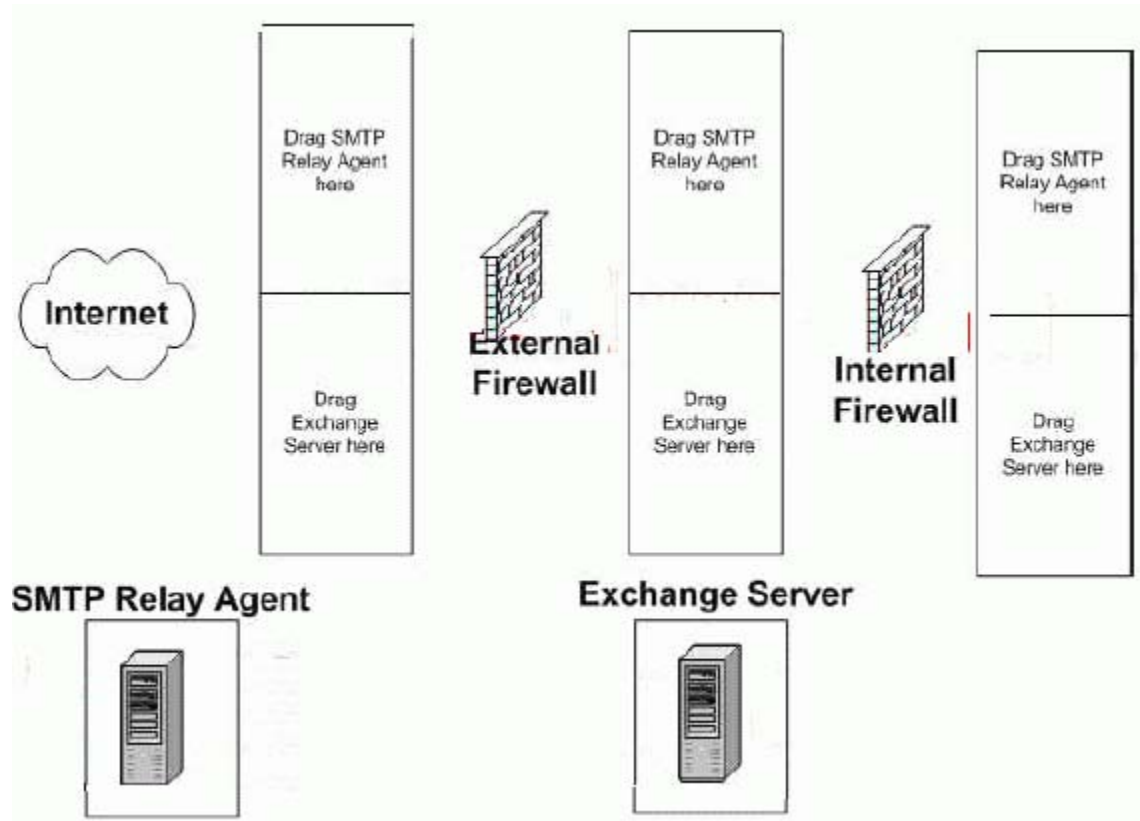
You are a security administrator for Company.com. The network consists of a single Active Directory forest named Company.com. All servers run either Windows Server 2003 or Windows 2000 Server. All domain controllers Windows Server 2003. All client computers run Windows XP Professional. Company.com uses a Microsoft Exchange Server 2003 computer. Users on the internal network connect to Exchange Server 2003 by using Microsoft Outlook. Company.com currently does not allow users to exchange e-mail with customers via the Internet. To improve communication with customers, management decides to allow e-mail communication via the

Internet. Your company updates its written security policy with the following requirements regarding the placement of Exchange Server 2003 computers:

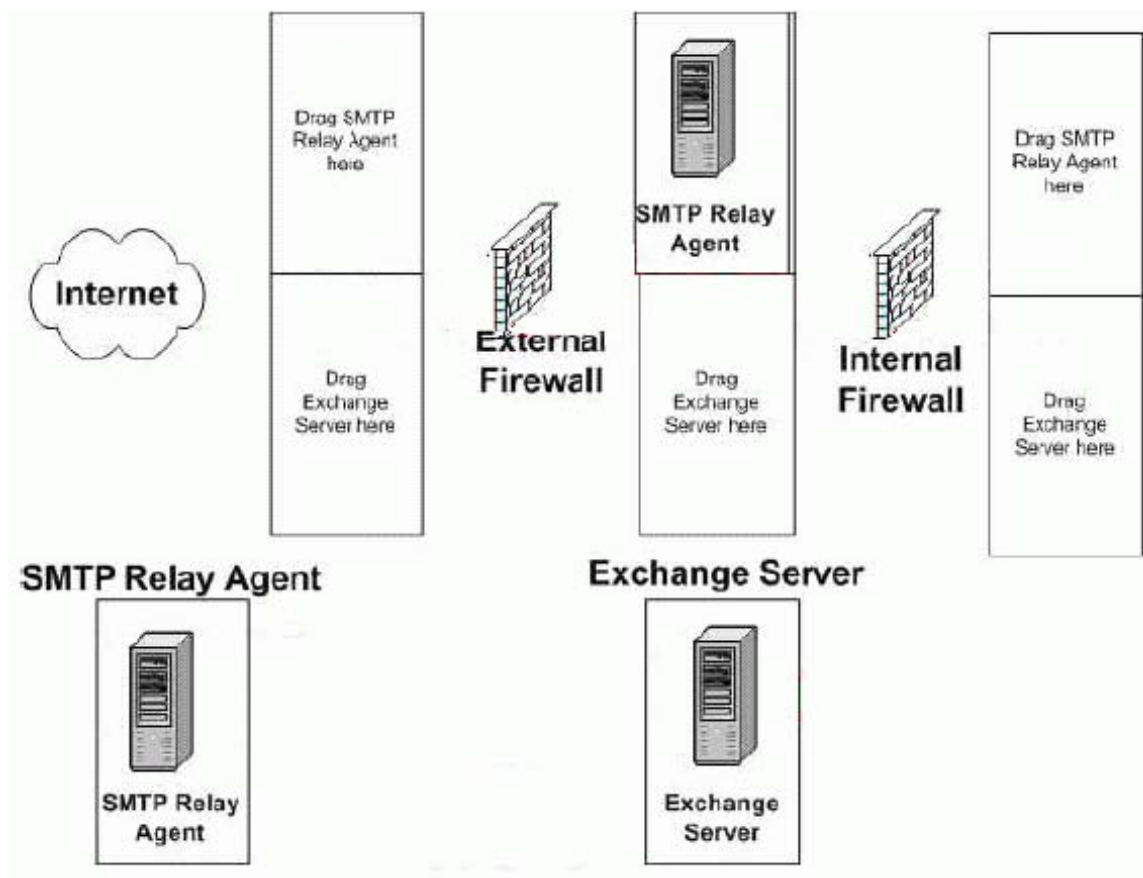
Customers on the Internet must not be able to connect directly to any computer on the internal network.

The number of ports and protocols that are allowed to pass through firewall devices must be minimized. You need to place computers to meet the company's written security policy.

Drag and Drop



Answer:



Question: 81(D)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The domain contains Windows Server 2003 domain controllers, Windows Server 2003 member servers, and Windows XP Professional client computers. Currently, all employees use the local administrator account to log on to the member servers and client computers. Company.com's written security policy states that only authorized network administration are allowed to log on by using the local administration account. The written security policy also states that passwords must be at least 12 characters long and that this requirement must be enforced at all times. You create a GPO named Corporate Policy and link it to the domain. You configure the GPO to disable local administrator accounts and to require a password that consists of at least 12 characters. The next day, you discover that the computer account for the client computer named Companyclient3 was deleted. Users report they cannot log on to Companyclient3. You create a new computer account to rejoin Companyclient3 to the domain. You discover you cannot log on to Companyclient3 as either the local administrator or the domain administrator. You need to rejoin Companyclient3 to the domain. What should you do?

- A. Disable the Corporate Policy GPO
- B. Restart Companyclient3 in Safe mode.
- C. Reset the password for the local administrator account on Companyclient3 to be at least 12 characters long.
- D. Rename the local administrator account on Companyclient3.
- E. On Companyclient3, on the Administrator Properties tab of the local administrator account, clear the Password never expires check box.

Answer: B

Explanation:

Only the computer account has been deleted, only local policies apply and only local accounts or cached domain credentials can be used to logon. Since the question does not state that cached credentials are in use they cannot be used. The CorporateGPO has disabled the local administrator account so the best solution to get this computer up and running is to use the Recovery Console using an ERD or perform a parallel install to delete the original SAM databases and restart the computer. Once restarted that SAM will be rebuilt to the default status and the local administrator account password would be blank. You could then change the machine from domain to workgroup and workgroup back to the domain and rejoin the computer to the domain. If there were not ERD and the use of the Recovery Console is not possible, then a parallel install would have to be performed, then you could delete the original SAM database, restart the system and it will rebuild. This would set the local administrator's account to be active again and the password would be blank. There are also third party tools that would assist with this. Restarting the computer in safe mode (B) would still require a local user account / local administrator's account to logon. You must still be able to authenticate to the local SAM. Until you can logon to the computer, modifications are not possible. The only modification possible is to disable the new GPO so that the original machine policies would apply.

Question: 82(B)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003 computers. All computers are members of the domain. Company.com's written security policy states that all servers must have the security settings that are specified in a security template named Verify.inf. The Verify.inf security template is copied to the *Systemroot\Security\Templates* folder on each server. You need to verify that the servers on the network meet the requirements in the written security policy. What should you do?

- A. On each server, run the gpresult command and save the result.
- B. On each server, run the secedit.exe /analyze command for the Verify.inf security template and save the results.
- C. On each server, run Microsoft Baseline Security Analyzer (MBSA) and save the results.
- D. On a domain controller, import the Verify.inf security template into Security Configuration and Analysis and then start the Resultant Set of Policy Provider service.
- E. On a domain controller, import the Verify.info security template into the Default Domain Policy GPO, and then run the gpupdate command.

Answer: B**Explanation:**

Security Configuration and Analysis performs security analysis by comparing the current state of system security against an analysis database.

Question: 83(C)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The Company.com domain contains Windows Server 2003 computers and Windows XP Professional client computers. All computers are members of the domain. Twenty Windows Server 2003 computers serve as domain controllers. Company.com uses only Active Directory integrated DNS.

Company.com's written security policy states that computers that contain employee user account names and passwords must be hardened against attacks. The procedure for hardening computers include disabling unnecessary services. You are evaluating which services are necessary by using the following information about the domain controllers:

Domain controllers do not function as web servers, application servers, file servers, or print servers.

Service packs and security patches are manually installed on domain controllers from local media. Service packs and security patches are installed only by IT administrators.

All servers in the company are remotely managed by using a third-party program.

Printing is not allowed from the domain controllers.

Domain controllers do not run any IP routing protocols.

Drag and Drop

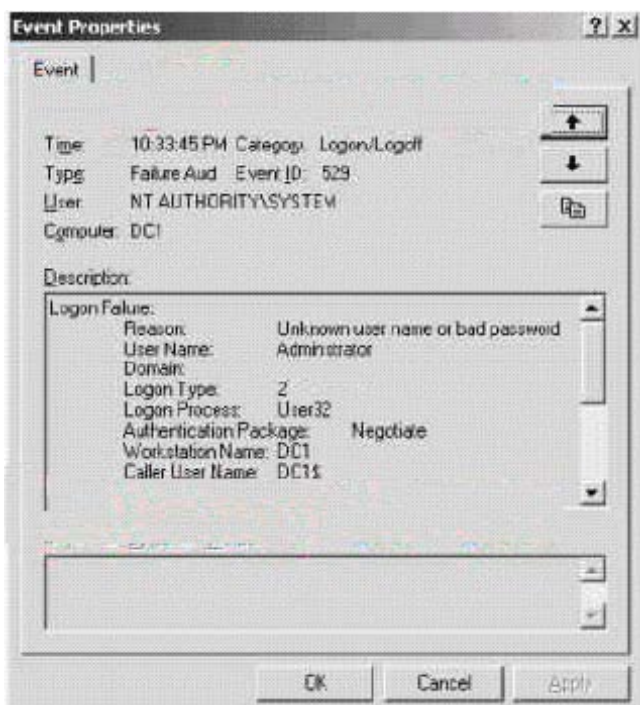
Service	Startup policy, place here	Service Startup Types Select from these
AutomaticService :		Automatic
DNS Server		Disabled
IIS Admin Service		
Net Logon		
Print Spooler		
Routing		
Terminal Services		
Windows Time		

Answer: Note:

Service	Startup policy, place here	Service Startup Types Select from these
AutomaticService :	Disabled	Automatic
DNS Server	Automatic	Disabled
IIS Admin Service	Disabled	
Net Logon	Automatic	
Print Spooler	Disabled	
Routing	Disabled	
Terminal Services	Disabled	
Windows Time	Automatic	

Unused services on a run-time image can be potential security vulnerability. You should enable only the services that are absolutely required to operate your device.

Question: 84(A)
Exhibit



You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The Company.com domain contains 50 Windows Server2003 computers that are configured as Web server. These Web servers host public Web sites for customers of Company.com. Customers access these sites anonymously. During a weekly review of the Company.com's security event logs, you notice a large number of occurrences of the event shown in the exhibit. You need to prevent unauthorized logon attempts from the Internet. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. Create a new security template that uses an IPSec policy to filter all traffic except HTTP. Use a GPO to apply the new security template to all Web server computers.
- B. Create a new security template that renames the administrator account. Use a GPO to apply the new security template to all Web server computers.
- C. Create a new security template that configures the LAN Manager Authentication Level to accept only NTLMv2 authentication. Use a GPO to apply the new security template to all Web server computers.
- D. Create a new security template that configures the LAN Manager Authentication Level to accept only NTLMv2 authentication. Use the secedit command to apply the new security template to all Web server computers.

Answer: A

Note:

Logon Events That Appear in the Security Event Log The following security events can be diagnosed using logon event entries: Local logon attempt failures Any of the following Event IDs indicates failed logon attempts: 529, 530, 531, 532, 533, 534, and 537. You will see events 529 and 534 if an attacker tries and fails to guess a username and password combination for a local account. However, these events can also occur when a user forgets their password, or starts browsing the network through My Network Places. In a large scale environment it can be difficult to interpret these events effectively. As a rule, you should investigate these patterns if they occur repeatedly or coincide with other unusual factors. For example, a number of 529 events followed by a 528 event in the middle of the night could indicate a successful password attack (or a very tired administrator).

Event ID	Description
528	A user successfully logged on to a computer.
<u>529</u>	<u>The logon attempt was made with an unknown user name or a known user name with a bad password.</u>
530	An attempt was made to log on with the user account outside of the allowed time.
531	A logon attempt was made using a disabled account.
532	A logon attempt was made using an expired account.
533	The user is not allowed to log on at this computer.
534	The user attempted to log on with a logon type that is not allowed, such as network, interactive, batch, service, or remote interactive.
535	The password for the specified account has expired.
536	The Net Logon service is not active.
537	The logon attempt failed for other reasons.
538	A user logged off.
539	The account was locked out at the time the logon attempt was made. This event can indicate that a password attack was launched unsuccessfully resulting in the account being locked out.
540	Successful Network Logon. This event indicates that a remote user has successfully connected from the network to a local resource on the server, generating a token for the network user.
682	A user has reconnected to a disconnected Terminal Services session. This event indicates that a previous Terminal Services session was connected to.
683	A user disconnected a Terminal Services session without logging off. This event is generated when a user is connected to a Terminal Services session over the network. It appears on the terminal server.

Question: 85(C)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. Server runs either Windows Server 2003 or Windows 2000 Server. All client computers run Windows 2000 Professional. The latest operating system service packs is installed on each computer. Thirty Windows Server 2003 computers are members of the domain and functions as file servers. Client computers access files on these file servers over the network by using the Server Message Block (SMB) protocol. You are concerned about the possible occurrence of man-in-the-middle attacks during SMB communications. You need to ensure that SMB communications between the Windows Server 2003 file servers and the client computers are cryptographically signed. The file servers must not communicate with client computers if the client computers cannot sign SMB communications. Client computers must be able to use unsigned SMB communications with all other computers in the domain. What should you do to configure the file servers?

- A. Apply a security template that enables the Microsoft network server:Digitally sign communications (always) setting.
- B. Apply a security template that enables the Microsoft network server:Digitally sign communications (if client agrees) setting.
- C. Apply a security template that enables the Domain member:Digitally sign secure channel data (when possible) setting.
- D. Apply a security template that enables the Domain member:Digitally encrypt or sign secure channel data (always) setting.

Answer: A

Question: 86(A)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Users are in the marketing, sales, or production department. A high-performance color print device named CompanyPrinter3 is attached to a server named Company9. CompanyPrinter3 is shared by users in the marketing department. Only users in the marketing department are permitted to print documents on CompanyPrinter3. Sandra is a user in the marketing department. Sandra is responsible for ensuring that print jobs on CompanyPrinter3 print properly. She is also responsible for replacing paper and for general print device maintenance. Sandra is not permitted to modify the printer itself. You need to configure permissions for CompanyPrinter3. You create a global group named Marketing. You add all marketing users to the Marketing global group. What else should you do?

- A. Assign the global group the Allow – Manage Documents permissions for CompanyPrinter3. Assign Sandra the Allow – Manage Printers permission for CompanyPrinter3.
- B. Assign the global group the Allow – Print permission for CompanyPrinter3. Create a local group on Company9. Add Sandra to the local group. Assign the local group the Allow – Manage Printers permissions for CompanyPrinter3.
- C. Add the global group to a local group on Company9. Assign the local group the Allow – Manage documents permission for CompanyPrinter3. Assign Sandra the Allow – Manage Printers permission for CompanyPrinter3.
- D. Add the global group to a local group on Company9. Assign the local group the Allow – Print permission for CompanyPrinter3. Create another local group on Company9. Add Sandra to the second local group. Assign the second local group the Allow – Manage documents permission for CompanyPrinter3.

Answer: D

Question: 87(B)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Several client computers are configured as kiosk computers that visitors and employees use. The kiosk computers are managed by using GPOs. The GPOs enforce a secure configuration. Multiple users log on to these computers every day. You review the results of a security audit. You discover that when some users log on the secure configuration is removed. You need to ensure that the secure configuration is enforced at all times. What should you do?

- A. Apply the Securews.inf security template to the kiosk computers.
- B. Configure the default user profile on kiosk computers as a mandatory user profile.
- C. Edit the GPO that manages kiosk computers. Disable the Secondary Logon service.
- D. Edit the GPO that manages kiosk computers. Enable loopback processing.

Answer: D

Question: 88(C)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The network contains several Windows Server 2003 computers that are configured as FTP servers. Company.com's written security policy states that security administrators must maintain a record of what time users log on to the FTP servers. You create a new security template to enforce the written security policy. You need to configure the template to comply with the written security policy. What should you do?

Drag and drop.

Policy	Policy setting, place here	Policy setting Select from these
Audit account login events	Not Defined	Succes, Failure
Audit account management	Not Defined	Succes
Audit directory service access	Not Defined	Failure
Audit logon events	Not Defined	
Audit object access	Not Defined	
Audit policy change	Not Defined	
Audit privilege use	Not Defined	

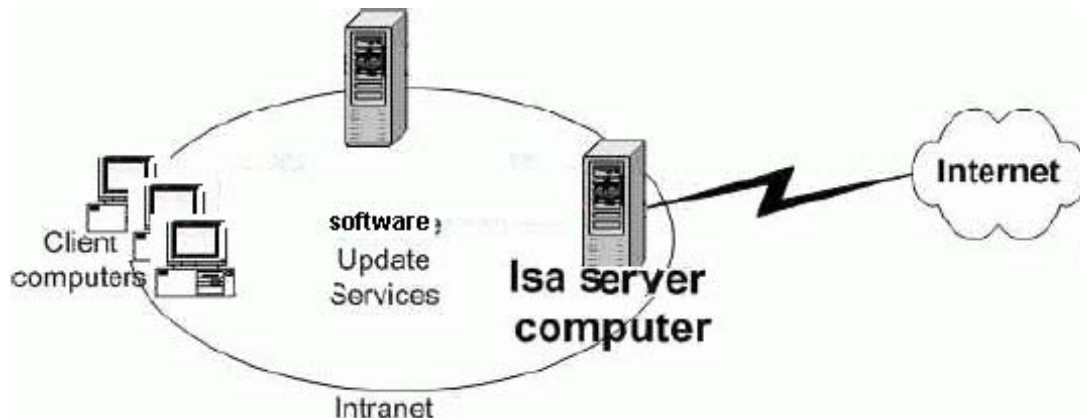
Answer: Explanation:

Policy	Policy setting, place here	Policy setting Select from these
Audit account login events	Not Defined	Succes, Failure
Audit account management	Not Defined	Succes
Audit directory service access	Not Defined	Failure
Audit logon events	Succes	
Audit object access	Not Defined	
Audit policy change	Not Defined	
Audit privilege use	Not Defined	

Account logon events are generated on domain controllers for domain account activity and on local computers for local account activity. If both account logon and logon audit policy categories are enabled, logons that use a domain account generate a logon or logoff event on the workstation or server, and they generate an account logon event on the domain controller. Additionally, interactive logons to a member server or workstation that use a domain account generate a logon event on the domain controller as the logon scripts and policies are retrieved when a user logs on.

Question: 89(C)

Network topology exhibit



You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com.

The Company.com domain contains Windows Server 2003 computers and Windows XP Professional client computers. The relevant portion of the network is shown in the exhibit. Company.com's written security policy states that all requests to the Internet must be authenticated. You install Software Update Services (SUS) on a computer named Company6. When you attempt to synchronize Company6 with Microsoft Update servers, you are unsuccessful. You review the error logs to synchronize Company6 and notice the following error message: "80072efd ERROR_INTERNET_CANNOT_CONNECT Cannot connect to the Internet server." You need to ensure that Company6 can connect to Microsoft Windows Update servers. What should you do?

- A. Configure the Microsoft Internet Security and Acceleration (ISA) Server computer to allow port 8080 traffic.
- B. Install the Microsoft Firewall Client on Company6.
- C. Configure the Microsoft Internet Security and Acceleration (ISA) Server computer to publish SUS to Company6.
- D. Configure SUS on Company6 to authenticate to the Microsoft Internet Security and Acceleration (ISA) Server computer.

Answer: D

Explanation:

To configure SUS to use a Proxy server: Goto the home page of your SUS Server by typing the URL in your browser (<http://<yourservername>/SUSAdmin>) or from the Start menu select click 'Programs | Administrative Tools | Microsoft Software Update Services'. Click on 'Set Options' in the navigation pane on the left hand side to load the Set options page Check the relevant option under the 'Select a proxy server configuration' section 'Do not use a proxy server to access the Internet' - Select this option if you're not using a Proxy server 'Use a proxy server to access the Internet' - Select this option if you are using a Proxy server and then choose the relevant option from the two below. 'Automatically detect proxy server settings' - Choose this option if your network supports automatic proxy server configuration (if you choose this option, SUS is clever enough to detect if there isn't a Proxy server) 'Use the following proxy server to access the Internet' - Choose this option if your network doesn't support automatic proxy server configuration and then complete the details such as the Address of the Proxy server and the Port it's using. If you need to provide a user ID and password to access the Proxy then check the check box beside the 'Use the following user credentials to access the proxy server' box and complete the ID and password. Some Proxies require you to provide credentials but use basic authentication. If your Proxy is one of these then make sure you also check the check box beside 'Allow basic authentication when using proxy server' Note: A quick word of warning. If you're using SUS on a Small Business Server that has an Internet Security and Acceleration (ISA) Server that requires authentication you'll need to use the following format for the username: DomainName\Username Click the 'Apply' button to apply the changes Note: There appears to be a typo in the SUS Deployment Guide. On Page 12 it talks about configuring your Proxy server which is fine until it goes onto Page 13 and makes this statement: "If you would like to bypass the proxy server for local addresses, select the checkbox beside 'Bypass proxy server for local addresses.'" This box doesn't exist on the 'Set options' screen. Microsoft have been notified of this.

Question: 90(D)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional. You regularly install security patches on Windows Server 2003 computers. You need to create a plan to restore computers to their original state if a security patch causes unwanted results. Which action should you perform first?

- A. Create a Recovery Console on the computer before you install the security patch.
- B. Create a mirrored volume on the computer before you install the security patch.
- C. Create a RAID 5 disk on the computer before you install the security patch.
- D. Create a script that runs the patch file with uninstall option.

Answer: D

Explanation: Standard Installer Command Line Options [Windows Installer] The executable program that interprets packages and installs products is Msiexec.exe. Note Msiexec also sets an error level on return that corresponds to system error codes.

Question: 91(B)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. You are planning a security patch management infrastructure. You install Software Update Services (SUS) on server named Company2. You configure client computer to use Company2. All client computers run custom applications developed by Company.com. You need to deploy custom security patches for applications that Company.com developed. What should you do?

- A. Configure a GPO to install the custom security patches when the client computers start up.
- B. Digitally sign the custom security patches, and then copy the files to the Content folder on Company2.
- C. Update the MSsecure.xml file with information about the custom security patches, and then run Microsoft Baseline Security Analyzer (MBSA) with the updated MSsecure.xml file.
- D. Copy the custom security patches to the Content folder on Company2. Run Mbsacli.exe, and configure Mbsacli.exe to use Company2.
- E. Copy the Content folder from Company2 to a new Web server. Add the custom security patches to the folder. Configure Automatic Updates on the client computers to use the new Web server.

Answer: A

Question: 92(B)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computers are configured to use Automatic Updates to install updates without user intervention. Updates are scheduled to occur during off-peak hours. During a security audit, you notice some client computers are not receiving updates on a regular basis. You verify that Automatic Updates is running on all client computers, and you verify that users cannot modify the Automatic Updates settings. You need to ensure that computers on your network receive all updates. What should you do?

- A. Enable the No auto-restart for scheduled Automatic Updates Installations settings.
- B. Disable the Specify intranet Microsoft update service location setting.
- C. Enable the Remove access to use all Windows Update features setting.
- D. Enable the Reschedule Automatic Updates scheduled installations setting.

Answer: D

Question: 93(A)

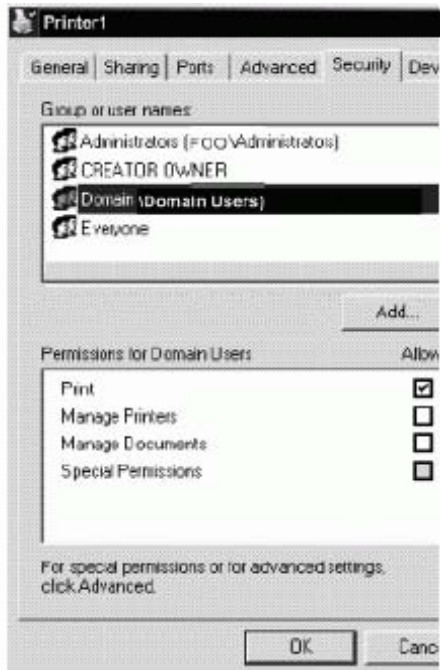
You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The domain contains Windows Server 2003 server computers. Twelve of these servers are configured as Web servers. You need to produce a report that identifies which Microsoft security patches are not installed on the Web servers. What should you do?

- A. Run Gpresult.exe on the Web servers.
- B. Run Mbsacli.exe on the Web servers.
- C. Run Secedit.exe on the Web servers.
- D. Run Qfecheck.exe on the Web servers.
- E. Run Qchain.exe on the Web servers.

Answer: B

Question: 94(A)

Exhibit



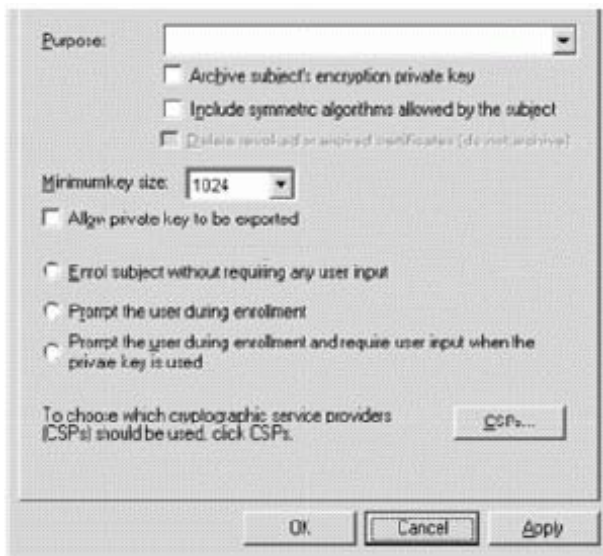
You are a security administrator for Company.com. Company.com has a subsidiary Foo.com. All servers run Windows Server 2003. All client computers run Windows XP Professional.

The network consists of two Active Directory forests named Company.com and foo.com. A two-way forest trust relationship is configured between Company.com and foo.com. The trustrelationship in which foo.com is configured to trust Company.com is configured to use selective authentication. Users in the Company.com forest report that they cannot print to a printer named CompanyPrinter1 on a server named Company3 in the foo.com forest. Users also report that they are prompted for a user name and password when they attempt to connect to CompanyPrinter1. You examine the access control list (ACL) on Printer1. The ACL is shown in the exhibit. You need to ensure that users in the Company.com can use CompanyPrinter1. What should you do?

- A. Assign the Authenticated Users group in the Company.com domain the Allow – print permission for CompanyPrinter1.
- B. Configure user principal name (UPN) routing in the Company.com domain to exclude the suffix foo.com.
- C. Edit the trust relationship in which the Company.com domain trusts the foo.com domain. Configure the trust relationship to use selective authentication.
- D. Assign the Domain Users group in the Company.com domain the Allow – Allowed to authenticate permission for Company3.

Answer: D

Question: 95(C)
Exhibit, Work area



You are a security administrator for Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Certificate Services is installed on one Windows Server 2003 computer in the role of an enterprise certification authority (CA). Company.com's written security policy includes the following file encryption requirements:

Private keys must be 2,048 bits.

Private keys and certificates must be recoverable on the CA.

Users must be able to back up their certificate and private key on their computers.

Users must be prompted by their computer every time the private key is used. You create a custom certificate template to issue Encrypting File System (EFS) certificates. The relevant properties of this certificate template are shown in the work area.

You need to configure the certificate template to enforce the written security policy. What should you do?

Answer:

Explanation:

Purpose: EFS Check x Archive subject's encryption private key Minimum key size: 2048 Check x Allow private key to be exported Radio o Prompt the user during enrollment and require user input when the private key is used.

Question: 96(C)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional. Company.com has one main office and three branch offices. Domain controllers are located in the main office and in each office of the three branch offices. Each office is configured as a separate Active Directory site. Domain controllers in the main office are stored in a physically secure location. Company.com's written security policy states that administrators must use a smart card when logging on to a domain controllers that is not stored in a physically secure location. You install smart card readers on all domain controllers and on the client computers of all administrators. You issue smart cards to all administrators. You need to ensure that smart cards are required when logging on locally only to domain controllers that are not physically secure location. What should you do?

- Create a new GPO and link it to each branch office site. Filter the GPO to apply to only domain controllers. Enable the Interactive login: Require smart card setting.
- Edit the properties of each administrator account that will be used to perform administration at the branch offices. Select the

Smart card is required for interactive logon check box.

- C. Enable Remote Desktop on each branch office domain controller. Instruct administrators to use Remote Desktop Connection to connect to branch office domain controllers. Select the Smart Card check box on the properties of the Remote Desktop Connection.
- D. Move all domain controller objects to a new OU named Branch Offices. Create a new GPO and link it to the Branch Offices OU. Enable the Interactive logon: Require smart card setting.

Answer: A

Question: 97(C)

Exhibit You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional. You create OUs in the Active Directory to contain the user, computer, and group objects for each department at Company.com. The OU structure is shown in the exhibit. You want to allow selected users to encrypt data by using Encrypting File System (EFS). However, the requirements for using EFS vary based on the OU in which the user's computer resides. Use of EFS should be disabled on all computers in the Domain Computers OU. You must enable EFS for the following OUs:



Human Resources

Finance

Engineering

Research *** MISSING *** Drag and Drop. Drag the EFS configurations to the appropriate locations.

Domain Containers

EFS Configuration

Domain Controllers OU

Place here

Human Resources OU

Place here

Finance OU

Place here

Engineering OU

Place here

Research OU

Place here

EFS Configuration, Select from these

Add Sandra as the encrypted data recovery agent

Add Exams as the encrypted data recovery agent

Disable the Allow users to encrypt files using EFS option.

Enable the Do Not Require Data Recovery Agent option.

No EFS policy is required.

Answer:

Domain Containers

EFS Configuration

Domain Controllers OU

Disable the Allow users to encrypt files using EFS option.

Human Resources OU

Add Exams as the encrypted data recovery agent

Finance OU

Add Exams as the encrypted data recovery agent

Engineering OU

Add Sandra as the encrypted data recovery agent

Research OU

No EFS policy is required.

EFS Configuration, Select from these

Add Sandra as the encrypted data recovery agent

Add Exams as the encrypted data recovery agent

Disable the Allow users to encrypt files using EFS option.

Enable the Do Not Require Data Recovery Agent option.

No EFS policy is required.

Question: 98(A)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The functional level of the domain is Windows Server 2003 interim mode. Employees in the human resources department of Company.com need to modify certain attributes of employee user accounts. You plan to use a global group named HR Users to contain all user accounts for the human resources department. You plan to create a new group that includes the HR Users global group as a member. You need to choose the appropriate type of group to implement your plan. What type of group should you choose?

A. A domain local security group

- B. A domain local distribution group
- C. A universal security group
- D. A universal distribution group

Answer: A

Question: 99(B)

You are a security administrator for Company.com. Company.com has one main office in Toronto and five branch offices in Boston, New York, Mexico City, Cape Town, and London respectively. Network administrators work in the main office and each branch office. Network administrators in the main office frequently create scripts that automate common administrative tasks. You review each script to ensure it does not introduce security vulnerabilities. Scripts that do not introduce security vulnerabilities are considered approved. Occasionally, branch office administrators modify these scripts and distribute the modified scripts to other branch office administrators. Branch office administrators often report that they accidentally run a modified version of a script. You need to ensure that branch office administrators can verify which scripts are approved scripts. What should you do?

- A. Maintain a list of the dates the approved scripts were last modified. Instruct branch office administrators to verify the file modification date.
- B. Digitally sign all approved scripts. Instruct branch office administrators to verify the signature before using a script.
- C. Distribute all approved scripts to branch office administrators in an e-mail message.
- D. Place all approved scripts on a file server in the main office. Assign all branch office administrators only the Allow – Read permission for the folder that contains the approved scripts. Instruct administrators to copy scripts from this file server.

Answer: B

Question: 100(A)

You are a security administrator for Company.com. The network consists of three Active Directory domains. All Active Directory domains are running at a Windows Server 2003 mode functionality level. Employees in the editorial department of Company.com need access to resources on file servers that are in each of the Active Directory domains. Each Active Directory domain in the company contains at least one editorial department employee user accounts and that has access to the resources on file server computers. What should you do?

- A. Create a global distribution group in the forest root domain and name it Company Editors.
- B. Create a global security group in the forest root domain and name it Company Editors.
- C. Create a universal distribution group in the forest root domain and name it Company Editors.
- D. Create a universal security group in the forest root domain and name it Company Editors.

Answer: D

Question: 101(B)

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional. You installed Terminal Server on a member server named Company7. Users in the domain connect remotely to Company7 to run applications. Terminal Services on Company7 is configured to run in Full Security mode. You do not want to change the configuration to Relaxed Security mode. You want to limit the effective permissions for the Program Files folder on Company7 when users connect remotely. By default, a few groups have Modify permissions for the Program Files folder. You want to ensure that these users have Modify permissions only when they are logged on locally to Company7. When they are remotely connected to Company7, they are not allowed to change to the Program Files folder. You need to assign the appropriate permissions. What should you do?

- A. Assign the Remote Interactive Logon group the Deny – Write permission for the Program Files folder.
- B. Assign the Remote Desktop Logon group the Deny – Write permission for the Program Files folder.
- C. Assign the Terminal Server Users Logon group the Deny – Write permission for the Program Files folder.

Success, Failure	 Audit account logon events	Success
Success	 Audit account management	Not Defined
Failure	 Audit directory service access	Not Defined
	 Audit logon events	Not Defined
	 Audit object access	Not Defined
	 Audit policy change	Not Defined
	 Audit privilege use	Not Defined

Question: 103(A)

You are a security administrator for Company. The network consists of a single Active Directory domain. The network contains Windows XP Professional client computers and Windows Server 2003 computers. The Windows Server 2003 computers were recently upgraded from Windows 2000 Server. Company.com's written security policy states that all changes and attempted changes to security principals in Active Directory must be recorded. You modify the Default Domain Controllers Policy GPO. The Audit Policy section of the GPO is shown in the work area. You need to configure the auditing policy to meet the requirements of the written security policy. You must achieve this goal by using minimum number of audit events. What should you do? Drag and Drop

Success, Failure

Success

Failure

Audit account logon events

Audit account management

Audit directory service access

Audit logon events

Audit object access

Audit policy change

Audit privilege use

Not Defined

Not Defined

Not Defined

Not Defined

Not Defined

Not Defined

Not Defined

Answer:

Success, Failure

Success

Failure

Audit account logon events

Audit account management

Audit directory service access

Audit logon events

Audit object access

Audit policy change

Audit privilege use

Not Defined

Success, Failure

Not Defined

Not Defined

Not Defined

Success

Not Defined

Question: 104(A)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers. The domain contains three domain controllers. All domain controllers are in the DomainControllers OU. A new password policy is defined in a security template

named Company.inf. You need to implement the new password policy for domain accounts. What should you do?

- A. Import the Company.inf security template into the Default Domain Policy GPO.
- B. Import the Company.inf security template into the Default Domain Controllers Policy GPO.
- C. On each domain controller, import the Company.inf security template into the local computer policy.
- D. On each domain controller, import the Company.inf security template into Security Configuration and Analysis, and then use the Configure Computer Now command.
- E. On each domain controller, run the secedit /import Company.inf command, and then run secedit /configure command.

Answer: A

Question: 105(A)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All domain controllers run Windows Server 2003. All domain controllers are in the same Active Directory site. You want to implement a new auditing policy on the domain controllers. You also want to delegate the management of the auditing and security log on the domain controllers to members of a group named Auditors. You create a new security template named Company.inf. The Company.inf security template contains the new auditing policy settings and the user right settings to delegate the management of the auditing and security log. On a domain controller named Company5, you import the Company.inf security template into Security Configuration and Analysis, and then use the Configure Computer Now command. Finally, you use the Analyze Computer now command to verify that the new settings are applied to Company5. The next day, a member of the Auditors group reports that the new auditing policy settings and user right settings are not in effect on two of the domain controllers. You need to ensure that the new auditing policy and user right settings are configured on all domain controllers. What should you do?

- A. On each domain controller, use the Configure Computer Now command to apply the Company.inf security template.
- B. On Company5, after you use the Analyze the Computer Now command, run the repadmin.exe /replicate /force command.
- C. On Company5, after you use the Analyze the Computer Now command, run the gpupdate.exe /force command.
- D. On each domain controller, import the Company.inf security template into the local computer policy.
- E. On Company5, import the Company.inf security template into the Default Domain Controllers GPO.

Answer: E

Question: 106(A)

Exhibit, Marketing GPO Exhibit, Finance GPO

Policy	Policy Setting
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) sessi...	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	This computer is reserved for users in t...
Interactive logon: Message title for users attempting to log on	Legal Notice
Interactive logon: Number of previous logons to cache (in case...	Not Defined
Interactive logon: Prompt user to change password before ex...	Not Defined
Interactive logon: Require Domain Controller authentication to...	Not Defined
Interactive logon: Require smart card	Not Defined

Policy	Policy Setting
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) sessi...	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case...	Not Defined
Interactive logon: Prompt user to change password before ex...	14 days
Interactive logon: Require Domain Controller authentication to...	Enabled
Interactive logon: Require smart card	Not Defined

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers. You create two top-level OUs. One OU is named Finance. The other OU is named Marketing. You place user and computer accounts for users in the marketing and finance departments in the corresponding OU. You create a GPO for each OU and link each GPO to the corresponding OU. The GPO linked to the Marketing OU is shown in the Marketing GPO exhibit, and the GPO linked to the Finance OU is shown in the Finance GPO exhibit. A client computer named Company143 is used by users in the marketing department. You reassign Company143 to users in the finance department. You move the computer object from the Marketing OU to the Finance OU. When you attempt to log on to Company143, you receive a message stating that the computer is intended for use by the marketing department only. You need to ensure that users in the finance department do not receive the message. You want to achieve this goal without affecting users in the Marketing OU. What should you do?

- A. Edit the Finance GPO. Configure a blank logon message.
- B. In the Marketing OU, block the inheritance of Group Policy.
- C. Move the Marketing OU into the Finance OU.
- D. Force the update of Group Policy on all client computers.

Answer: A

Question: 107(A)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers. Company.com written security policy requires that the successful backup and restoration of all files on a critical file server must be audited. You create a new GPO and filter it to apply to the file server. You configure the GPO by enabling the Audit: Audit the use of Backup and Restore privilege security option. You perform a system backup of the file server. You examine the event logs and discover that no audit information is recorded. You need to configure the auditing policy to meet the requirements of the written security policy. You want to achieve this goal by using the minimum of auditing settings. What should you do? Drag and Drop

Policy Settings

Success, Failure	 Audit account logon events	Not Defined
Success	 Audit account management	Not Defined
Failure	 Audit directory service access	Not Defined
	 Audit logon events	Not Defined
	 Audit object access	Not Defined
	 Audit policy change	Not Defined
	 Audit privilege use	Not Defined

Answer:

Policy Settings

Success, Failure	 Audit account logon events	Not Defined
	 Audit account management	Not Defined
Failure	 Audit directory service access	Not Defined
	 Audit logon events	Not Defined
	 Audit object access	Not Defined
	 Audit policy change	Not Defined
	 Audit privilege use	Success

Question: 108(A)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional, Windows 2000 Professional, and Windows Server 2003 computers. You discover that users in one domain can obtain a list of account names for users in the other domain. This capability allows unauthorized users to guess password and to access confidential data. You need to ensure that account names can be obtained only by users of the domain in which the accounts reside. Which two actions should you perform on the domain controllers? (Each correct answer presents part of the solution. Select two.)

- A. Apply a security template that disables the Network access: Allow anonymous SID/Name translation setting.
- B. Apply a security template that disables the Network access: Do not allow anonymous enumeration of SAM accounts setting.
- C. Apply a security template that disables the Network security: Do not store LAN Manager hash value on next password change setting.
- D. Apply a security template that sets the Domain controller:LDAP server signing requirements setting to Require signing.

Answer: A, B

Question: 109(D)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers. The network also consists of a public key infrastructure (PKI) that supports smart card authentication. Company.com's written security policy states the following network administration requirements:

All domain controllers must be stored in a restricted location. Only Server Administration Staff are permitted to access this location.

All Directory Services Administration staff must use a smart card when performing administrative tasks interactively on domain controllers.

All administration of domain controllers that is performed remotely must be protected by encryption.

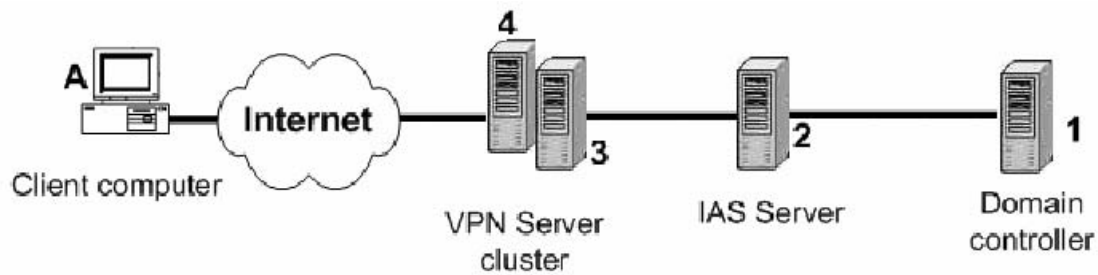
To comply with the written security policy, you move all domain controllers to a secure server room and provide only Server Administration staff with access to the server room. You create an additional account for each member of the Directory Services Administration staff. You configure the new accounts to require a smart card during authentication. You need to ensure that Directory Services Administration staff are able to administer domain controllers. You must achieve this goal without violating the written security policy. What should you do?

- A. Configure a smart card reader on the client computer of each Directory Services Administration staff member. Instruct Directory Services Administration staff to connect to domain controllers using a Remote Desktop connection.
- B. Configure a smart card reader on each domain controller. Instruct Directory Services Administration staff to use the runas command to open a Telnet session when administering domain controllers.
- C. Create a custom Microsoft Management Console (MMC). Include all snap-ins required by Directory Services Administration staff. Instruct Directory Services Administration staff to use the runas command to open the custom MMC.
- D. Install IIS on one domain controller. Include the remote administration components. Configure IIS to require HTTPS connections. Instruct administrators to connect to the remote administration Web site on the IIS server.

Answer: A

Question: 110(C)

Exhibit, Network Topology



You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network is configured as shown in the exhibit. Some of the users in the sales department are mobile users. The mobile users connect to the corporate network by establishing VPN connections. All VPN servers are configured to forward authentication requests to an Internet Authentication Service (IAS) server on the corporate network. You need to configure the network to provide stronger security for user authentication requests. What should you do?

- A. Deploy an IPsec policy that uses Encapsulating Security Payload (ESP) for all LDAP traffic between the IAS server and the domain controller.
- B. Deploy an IPsec policy that uses Encapsulating Security Payload (ESP) for all RADIUS traffic between the IAS server and the

VPN server cluster.

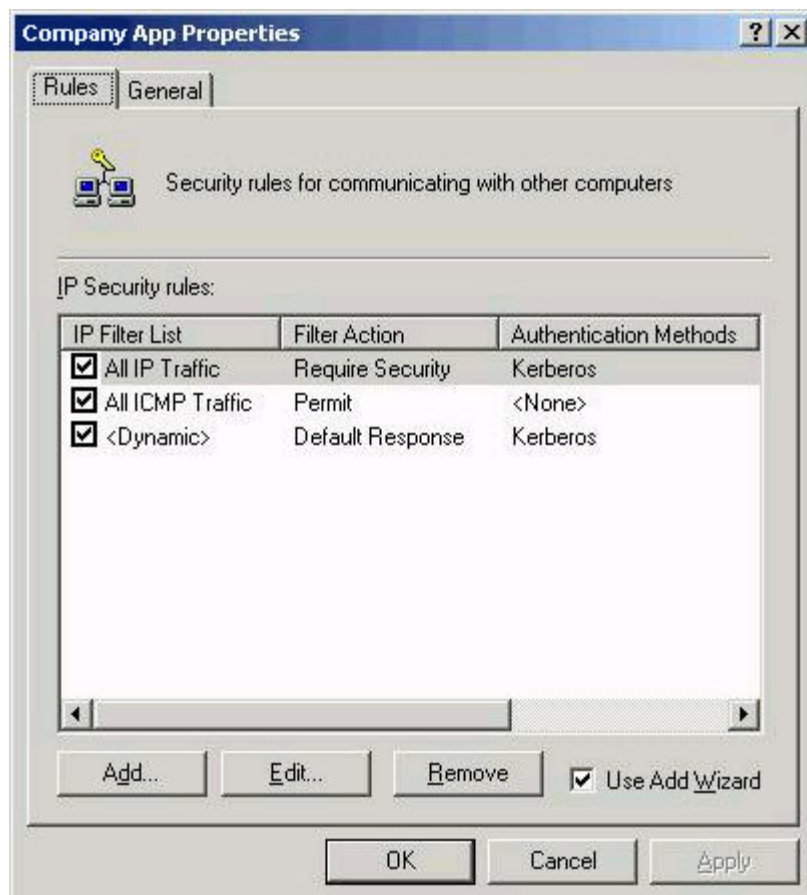
C. Deploy an IPSec policy that uses Authentication Header (AH) for all traffic between the IAS server and the VPN server cluster.

D. Deploy an IPSec policy that uses Authentication Header (AH) for all traffic between the IAS server and the domain controllers.

Answer: B

Question: 111

Exhibit You are a security administrator for Company.com. You decide to implement IPSec to encrypt the payroll application data during transmission. You configure a custom IPSec policy named CompanyApp on Company7 using the rules shown in the exhibit. You configure an IPSec default Client policy on the client computers in both Active Directory domains. During testing, you notice that client computers in the Company.com Active Directory domain use IPSec when communicating with Company7. However, client computers in the foo.com Active Directory domain cannot communicate with Company7. You need to enable all client computers to use IPSec when communicating with Company7. What should you do?



A. Modify the custom CompanyApp policy by adding the certificate authentication type to the existing rules on Company7.

B. Use the customer CompanyApp policy and issue an IPSec certificate from the internal CA to Company7.

C. Unassign the customer CompanyApp policy and assign the default Server policy on Company7.

D. Unassign the customer CompanyApp policy and assign the default Secure Server policy on Company7.

Answer: A

Question: 112(C)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only. The network contains three member servers named Company1, Company2, and Company3. The three member servers connected to the Internet. You plan to implement remote access to the Company network for users that work from home. You configure and enable Routing and Remote Access on Company1 and Company2. Sandra, who is an administrator on all member servers, configures and enables Routing and Remote Access on Company2. However, users cannot establish a VPN connection to Company3. You discover that Company3 can only authenticate Internet VPN connections from local users accounts. You need to ensure that users from the domain can successfully establish a VPN connection to Company3. What should you do?

- A. Enable the Company3 computer account in Active Directory as trusted for delegation.
- B. Assign the Authenticated Users group the Allow – Allowed to Authenticate permission for the Company3 computer account in Active Directory.
- C. Assign the Company3 computer account the Allow – Read permission on the RAS and IAS Servers Access Check container in Active Directory.
- D. Add the Company3 computer account to the RAS and IAS Servers security group.
- E. Add the Company3 computer account to the Windows Authorization Access group security group.

Answer: D

Question: 113(A)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only. All computers are members of the domain. You need to test IPSec interoperability on your network. To do this, you create a new GPO named CompanyIPSec. In the CompanyIPSec GPO, you create an IPSec policy named CompanyTest. The CompanyTest policy contains a rule that specifies the use of Encapsulating Security Payload (ESP) with null encryption. The CompanyTest policy is applied to all servers in the domain. After all the tests are concluded, you need to ensure that the CompanyTest policy is no longer used by the servers on the network. What should you do?

- A. In the domain, delete the CompanyIPSec GPO.
- B. In the CompanyIPSec GPO, unassign the CompanyTest policy.
- C. On the servers, restart the IPSec services service.
- D. On the servers, in the IP Security Policies, use the Restore Default Policies command.
- E. On the servers, run the Netsh ipsec delete policy name = "CompanyTest" command

Answer: B

Question: 114 (D)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only. You manage a Windows Server 2003 computer named Company12 that is a domain member server. You use IIS on Company12 to host an Internet Web site. Approximately 4,000 Company employees connect over the Internet to access company confidential data on Company12. You control access to data on Company12 by using NTFS file permissions assigned to groups. Different groups are assigned access to different files. Employees must have access only to files that they are assigned access to based on their membership in a group. You enable SSL on Company12 to protect confidential data while it is in transit. You issue each employee an Authenticated Session certificate and store a copy of that certificate with their user account in the Active Directory domain. You need ensure that Company12 authenticates users based on possession of their certificate. What should you do?

- A. Request a Web server certificate from a commercial certification authority (CA).
- B. Configure access restrictions based on employee IP address.
- C. Enable Digest authentication for Windows domain servers.

D. Configure client certificate mapping.

Answer: D

Question: 115(B)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The servers on the network runs Windows Server 2003, and all servers are members of the domain. You plan to deploy a new service pack for Windows Server 2003 on existing servers. You install Software Update Services (SUS) on a server named Company3. You need to deploy the new service pack to the servers in a group named TestServers before you deploy the service to all servers. What should you do?

- A. Slipstream the service pack files into the Windows folder on the servers in the TestServers group.
- B. Copy the service pack executable file to Company3. Configure read permission on the file for only the TestServers group.
- C. Copy the service pack executable file to a new SUS server. Configure Automatic Updates on the servers in the Test Servers group to use the new SUS server.
- D. Create a new GPO to deploy the service pack. Filter the GPO so that it applies to only the TestServers group.

Answer: D

Question: 116 (C)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only. There are 15 Windows Server 2003 computers that serve as domain controllers. For security reasons, you do not allow the domain controllers to access Web sites over the Internet. You need to scan all of the domain controllers to identify which security patches are not installed. You want to achieve this goal by using the minimum amount of administrative effort and by successfully completing the scan of all domain controllers. What should you do?

- A. Run Microsoft Baseline Security Analyzer (MBSA) on one of the domain controllers and target the domain controllers.
- B. Run Microsoft Baseline Security Analyzer (MBSA) on a client computer that has Internet access and target all the domain controllers.
- C. Run Microsoft Baseline Security Analyzer (MBSA) on each domain controller with a copy of the MBScan.wsf file that you downloaded from the Microsoft Web site.
- D. Run Microsoft Baseline Security Analyzer (MBSA) on each domain controller with a copy of the Mssecure.cab file that you downloaded from the Microsoft Web site.

Answer: B

Question: 117 (B)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only. You install Software Update Services (SUS) on a server named Company3. Company's written security policy states that all updates must be tested and approved before they are installed on network computers. You need to ensure that SUS uses the minimum amount of disk space on Company3. What should you do?

- A. Configure Company3 to redirect client computers to the Microsoft Windows Update servers.
- B. Compress the folder in which the downloaded updates are stored.
- C. Configure Company3 to store only the locales that are needed.
- D. Download the updates, and then delete updates that are not approved for client computers.

Answer: A

Question: 118

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All domain controllers run Windows Server 2003. All domain controllers are in the same Active Directory site. You want to implement a new auditing policy on the domain controllers. You also want to delegate the management of the auditing and security log on the domain controllers to members of a group named Auditors. You create a new security template named Company.inf. The Company.inf security template contains the new auditing policy settings and the user right settings to delegate the management of the auditing and security log. On a domain controller named Company5, you import the Company.inf security template into Security Configuration and Analysis, and then use the Configure Computer Now command. Finally, you use the Analyze Computer now command to verify that the new settings are applied to Company5. The next day, a member of the Auditors group reports that the new auditing policy settings and user right settings are not in effect on two of the domain controllers. You need to ensure that the new auditing policy and user right settings are configured on all domain controllers. What should you do?

- A. On each domain controller, use the Configure Computer Now command to apply the Company.inf security template.
- B. On Company5, after you use the Analyze the Computer Now command, run `therepadadmin.exe /replicate /force` command.
- C. On Company5, after you use the Analyze the Computer Now command, run `thegpupdate.exe /force` command.
- D. On each domain controller, import the Company.inf security template into the local computer policy.
- E. On Company5, import the Company.inf security template into the Default Domain Controllers GPO.

Answer: E

Question: 119

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only. One hundred of your users are mobile users in the sales department. These users work from home offices and use portable computers that are not members of the corporate domain. They do not connect to the corporate network on a regular basis. Mobile users communicate with users on the corporate network by using SMTP and POP3 email. All mobile users have user accounts in the corporate domain. You decide to deploy Software Update Services (SUS) as part of your patch management strategy. You install SUS on a server named Company5. You configure Company5 to be accessible to users on the Internet. You review and approve the necessary security patches. You need to configure mobile users computers to install only approved security patches. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. Create a new GPO that applies to only mobile users. Configure the GPO to download updates from Company5. Instruct users to run a script that includes the **gpupdate** command.
- B. Create a new GPO that applies to only mobile users. Configure the GPO to download updates from Company5. Instruct users to run a script that includes the **gpresult** command.
- C. Write a script that modifies the local registry of each portable computer to use Windows Update. Instruct mobile users to run the registry modification script.
- D. Write a script that modifies the local registry of each portable computer to use Company5. Instruct mobile users to run the registry modification script.

Answer: D

Question: 120

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. One hundred Company.com users are currently using an application named CompanyApp. CompanyApp is stored in a folder on the hard disk of each user's client computer. To secure CompanyApp, you create a new GPO named CompanyAppPolicy. The CompanyAppPolicy GPO contains a file system security policy that applies a customer DACL to CompanyApp. You configure the DACL to assign all users only the Allow -Read permission. You filter the CompanyAppPolicy GPO to apply only to computers that have CompanyApp installed. After you apply the CompanyApp GPO, users immediately report that they receive an error message when they attempt to use CompanyApp. You delete the entry for CompanyApp in the file system security policy. Users continue to report that they receive the same error message when they attempt to use CompanyApp. You need to configure the network so that users can use CompanyApp. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. Delete the CompanyAppPolicy GPO. Restart all client computers.
- B. Create a new file system security policy in the CompanyAppPolicy GPO that assigns default permissions to CompanyApp.
- C. Import the Setup security.inf security template into the CompanyAppPolicy GPO.
- D. Disable the CompanyAppPolicy GPO.

Answer: B

Question: 121

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. You are planning a security patch management infrastructure. You install Software Update Services (SUS) on server named Company2. You configure client computer to use Company2. All client computers run custom applications developed by Company.com. You need to deploy custom security patches for applications that Company.com developed.

What should you do?

- A. Configure a GPO to install the customer security patches when the client computers start up.
- B. Digitally sign the custom security patches, and then copy the files to the Content folder on Company2.
- C. Update the Mssecure.xml File with information about the custom security patches, and then run Microsoft Baseline Security Analyzer (MBSA) with the updated MSsecure.xml file.
- D. Copy the custom security patches to the Content folder on Company2. Run Mbsaclic.exe, and configure Mbsaclic.exe to use Company2.
- E. Copy the Content folder from Company2 to a new Web server. Add the custom security patches to the folder. Configure Automatic Updates on the client computers to use the new Web server.

Answer: A

Question: 122

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All 80 servers run Windows Server 2003. All 2,000 client computers run Windows XP Professional. All computers are members of the domain. A windows Server 2003 computer named Company7 functions as an internal Web server. Employees in the marketing department regularly upload files to Company7 using the FTP service. You decide to protect this data while it is in transit via FTP to Company7. You implement IPsec and assign the default IPsec Secure Server policy on Company7. You implement IPsec and assign the default IPsec client policy on the marketing client computer. You verify that the FTP data is encrypted by monitoring the traffic between the marketing department client computer and Company7. Users report that the HTTP service on Company7 is no longer accessible from client computers that are not in the marketing department. DNS queries made from Company4 also fail to resolve. You need to restore access to the normal HTTP server and DNS client functionality on Company4 while preserving the encryption of FTP data between Company7 and the marketing department client computers. What should you do?

- A. Unassign the IPsec Secure Server policy and assign the default Server policy of Company4.
- B. Unassign the Client Policy and assign a custom IPsec policy on marketing department client computers that uses authentication headers on Company7.
- C. Unassign the IPsec Secure Server policy and assign a custom IPsec policy that requires IPsec only for FTP data on Company7.
- D. Unassign the IPsec Secure Server policy and assign a custom IPsec policy that does not require IPsec for DNS data on Company7.

Answer: C

Explanation:

The new policy applied has caused the error. Only FTP traffic need to be secured.

Note:

FTP is commonly misunderstood as a secure means for transferring data, because the FTP server can be configured to require a valid user name and password combination prior to granting access. Be aware that neither the credentials specified at logon nor the data itself is encrypted or encoded in any way. All credentials are sent across the network in plaintext.

Question: 123

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only. All computers have access to the Internet. You are planning the security patch management infrastructure. The written security policy of Company states that all computers must install only Company approved security patches. You install Software Update Services (SUS) on a server named Company3. You configure Automatic Updates on all computers to use Company3. You place computer accounts of several computers in a new group named CompanyPatchTest. You want to test each newly approved security patch on the computers in the CompanyPatchTest group before you allow all computers to install the security patch. You need to ensure that each time a new security patch is approved, only computers in the CompanyPatchTest group download and install the security patch. What should you do?

- A. On Company3, assign NTFS permissions to the **CompanyPatchTest** group for the new security patch files.
- B. On Company3, assign NTFS permissions to the **CompanyPatchTest** group for the Approveditems.txt text files.
- C. Configure Automatic Updates on the computers in the CompanyPatchTest group to use the Microsoft Windows Update servers. Copy an Approveditems.txt file to the Windows folder on these computers.
- D. Configure Automatic Updates on the computers in the CompanyPatchTest group to use a second SUS server named Company4. Use a separate approval list on Company4.

Answer: D

Question: 124

You are a security administrator for Company.com. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional. You regularly install security patches on Windows Server 2003 computers. You need to create a plan to restore computers to their original state if a security patch causes unwanted results. Which action should you perform first?

- A. Create a Recovery Console on the computer before you install the security patch.
- B. Create a mirrored volume on the computer before you install the security patch.
- C. Create a RAID 5 disk on the computer before you install the security patch.
- D. Create a script that runs the patch file with uninstall option.

Answer: D

Explanation: Standard Installer Command Line Options [Windows Installer] The executable program that interprets packages and installs products is Msiexec.exe. Note Msiexec also sets an error level on return that corresponds to system error codes.