

**Actualtests.com**

The Power of Knowing



**Exam : 070-298**

**Title : Designing Security for a MS Windows Server  
2003 Network**

**Ver : 04.03.08**

## Topic 1, City Central Utilities, Scenario

### **Background**

City Central Utilities is one of the largest manufacturers of genuine quality approved utilities which are used across the world.

### **Physical Locations**

City Central Utilities has its headquarters in Atlanta. City Central Utilities has a branch office in Brisbane which maintains a production facility and a retail branch office in Auckland which maintains a distribution facility.

City Central Utilities also has a retail office in London. The City Central Utilities has 525 users in the Atlanta office, 25 users in the Brisbane office and 225 users in the Auckland office.

### **Planned Changes**

City Central Utilities has hired you to design and implement a security plan which should be based on results of a security audit which was performed by a contractor of City Central Utilities. The security audit was conducted at City Central Utilities over a period of 4 months. The contractor hired by City Central Utilities has produced a report identifying several security issues. The security issues will have to be addressed in your security design.

### **Existing Environment**

#### **Directory Services**

The City Central Utilities company consists of a single Active Directory domain named citycentral.com. The functional level of the domain is set at Windows Server 2003. City Central Utilities has recently decided to create a site for each branch office and configure appropriate site links.

The domain controllers of City Central Utilities remain in the default Domain Controllers container. The management has also decided to have the administrative user accounts remain in their default Users container. The network administrators of City Central Utilities make use of their client computers for accessing the network. It is imperative to City Central Utilities that interactively logging on to the servers and domain controllers be prohibited.

#### **Network Services**

City Central Utilities has deployed multiple domain controllers to ensure that there is fault tolerance. All servers on the citycentral.com network run Windows Server 2003 and all client computers run Windows 2000 Professional or Windows XP Professional.

The City Central Utilities network has three servers located in different offices configured as file servers. The servers used by City Central Utilities are named CCU-SR01, CCU-SR02, CCU-SR03. The server named CCU-SR01 resides in the Atlanta office, CCU-SR02 resides in the Brisbane office and CCU-SR03 resides in the Auckland office. All of the file servers host a shared data folder shown below:

| Folder Name   | Location | Share Permission        | NTFS Permission         |
|---------------|----------|-------------------------|-------------------------|
| Data_Atlanta  | CCU-SR01 | Everyone – Full Control | Everyone – Full Control |
| Data_Brisbane | CCU-SR02 | Everyone – Full Control | Everyone – Full Control |
| Data_Auckland | CCU-SR03 | Everyone – Full Control | Everyone – Full Control |

City Central Utilities also has a member server residing in Brisbane named CCU-SR04. CCU-SR04 is used to host an inventory control application which is accessed only by Auckland and Brisbane network users.

The Management of City Central Utilities has also decided to deploy a Wireless network in Brisbane. City Central Utilities are planning to install multiple access points (APs) on each department to provide full wireless coverage in the facility. City Central Utilities has only issued 15 portable computers with wireless adapters. All the network portable computers run Windows XP Professional.

### Web Services

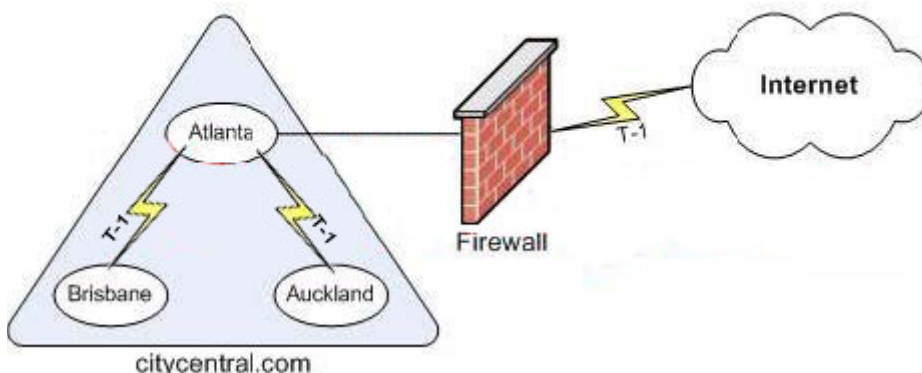
City Central Utilities has an internal Website and a Web-based inventory tracking application which is hosted on a server named CCU-SR05. City Central Utilities has Web site content that is updated and created by network users in the Human Resources (HR) department. City Central Utilities makes use of the intranet Web site to communicate the company information with the citycentral.com employees. The City Central Utilities inventory tracking application is used by the City Central Utilities Sales staff and management. CCU-SR05 runs Windows Server 2003, Web Edition and resides on the internal network. The network users of City Central Utilities make use of Internet Explorer 5.5 for Internet and Intranet Web browsing.

### Wide Area Network (WAN)

City Central Utilities makes use of the Atlanta main office to provide Internet connectivity to the Brisbane and Auckland branch offices via T-1 connection.

The City Central Utilities network environment is shown in the Infrastructure exhibit:

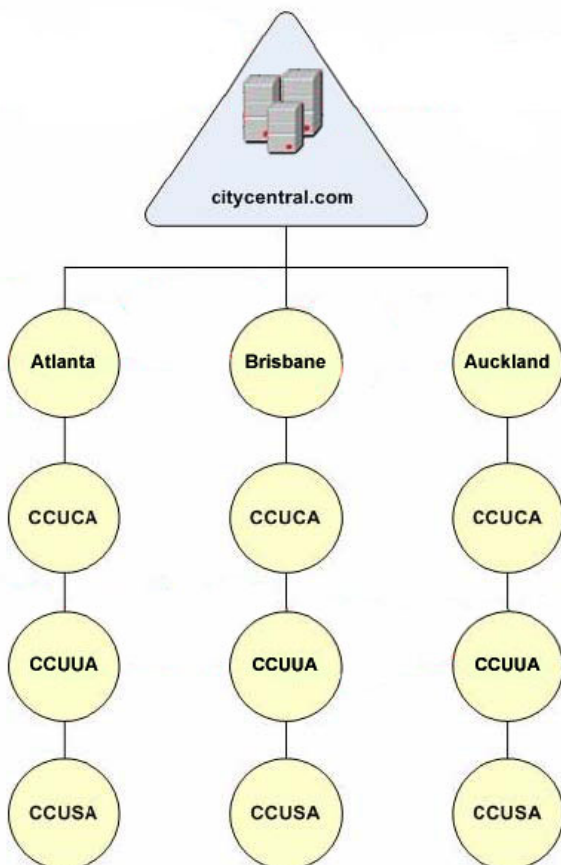
**Infrastructure**



### Organizational Unit (OU) Structure

The City Central Utilities network OU structure is shown in the OU Structure exhibit:

## OU Structure



City Central Utilities has defined a top-level OU for each City Central Utilities location which contains three child OUs each location specific. City Central Utilities makes use of the OU named CCUCA to contain all the client computer accounts in the specific location. The child OU named CCUUA is used by City Central Utilities to contain all the user accounts and the child OU named CCUSA is used to contain the server accounts in the location.

City Central Utilities has also defined a global security group for each location to simplify the assignment of permissions to non-administrative users. The City Central Utilities management wants the membership to these groups to be based upon the user's location. The City Central Utilities groups and membership parameters are below:

1. BUsers - is used to contain the Brisbane users
2. AUsers - is used to contain the Auckland users
3. ATUsers - is used to contain the Atlanta users

The City Central Utilities company also has a global security group named CCUAdmin which is used to assign permissions and user rights to the technical support team. City Central Utilities also uses a global security group named CCUWebAdmin which is used to assign permissions and user rights to members of the IT administration responsible for the management of the internal Web server.

### **The City Central Utilities Security Audit Report from the contractor**

City Central Utilities wants to have the following security issues considered:

1. Some of the City Central Utilities users have modified the initial security policy in Control Panel which allows unsafe ActiveX controls to be inadvertently downloaded and installed on their computers. The City Central Utilities also install applications on client computers without management approval. This leaves the City Central Utilities network administrators unable to provide support for a large number of applications currently deployed.
2. The City Central Utilities company has not defined a consistent baseline security configuration for either network domain controllers or member servers. The City Central Utilities wireless network is currently configured using a pre-shared key on each wireless access point and portable computer. City Central Utilities makes use of a simple key which is not changed on a regular basis.
3. City Central Utilities does not apply security patches consistently to the network computers. Because of this some network computers were recently infected by a virus which could have been avoided if the security patches were up-to-date. Most of the City Central Utilities network users do not lock their computers when leaving it unattended over extended periods of time. This action has recently caused contents of a sensitive document to be made public because it was left open on the user portable computer. An unauthorized user has viewed the documents while delivering files to the office.
4. The City Central Utilities generally do not protect network credentials. The City Central Utilities in the past shared user names and passwords with other employees. Some of the network users even taped pieces of paper noting passwords to the monitor which are acquired by unauthorized individuals. The portable computers in the Brisbane network are particularly vulnerable to unauthorized access. The City Central Utilities intranet Web site currently allows access to the company information without user authentication.

### **Interviews**

#### **Chief Information Officer (CIO)**

"Our industry is not a high-security industry but an inconsistent revenue cycle requires City Central Utilities to increase and decrease staffing levels on a regular basis. These actions have caused City Central Utilities to be more vigilant protecting network access. The City Central Utilities network functions reliably and the upgrade to Windows Server 2003 occurred over time and was not designed to meet the City Central Utilities security requirements. Because of this the design has resulted in some security related events which were the impetus for the external security audit."

"I want the network design to be modified to increase the security and resolve the issues specified in the audit. I also want any configurations to be centrally defined and applied to the network domain controllers and network server as well as client computers when possible."

"The management of City Central Utilities has decided to continue issuing portable computers to the Brisbane users but the authentication to the wireless portion of the City Central Utilities network should be strictly controlled. City Central Utilities should ensure that user credentials for portable computers and desktop computers are tightly controlled using two-factor authentication. The City Central Utilities management has

authorized the purchasing of additional equipment to secure all points of network access if required."

### **Chief Security Officer**

"I want the users to be allowed to only view approved Internet Web sites. I also want only the administrators to be allowed to add and remove sites from the list of approved Web sites. The City Central Utilities network users should not be allowed to override these restrictions by modifying the Internet security settings in Control Panel."

"We should have a consistent set of programs and applications to be defined and deployed. The City Central Utilities Domain users should not be able to update or install any software components other than those approved by members of the CCUAdmin group."

"Our domain account policies must be as secure as the account policy settings dictated by the Securedc.inf security template at least. The security settings should also be customized to meet the City Central Utilities requirements and the current settings that are more secure than the security template should be retained and settings not required disabled."

"Another concern of mine is that user access to the inventory tracking application on CCU-SR05 be secured by using certificate-based authentication. I want auditing enabled on CCU-SR05 to monitor all users accessing this application. You should then be able to verify who is logged on to the application and who the owner of the user account is."

### **IT Administrator**

"I want access to the shared folders in each location to be secure. This requires non-administrative users only to be granted access to the files located on their local file server. The users in their respective locations should be able to edit files in the local shared folder but should not be able to take ownership or change permission of user files."

"Another concern is that the security audit showed incidents where users were logged onto the network using logon credentials of other users. I want steps to be taken in order to prevent this in the future. I want to implement a process that will be used to track the incidents to identify all the unauthorized logon attempts."

### **Project Requirements**

The following project parameters are to be considered for City Central Utilities:

The City Central Utilities management wants the users who access the shared data over the network to only be able to view the files located on their specific file server.

1. City Central Utilities wants all the attempts by unauthorized users to access the data folders on the file server to be monitored. City Central Utilities Also wants the users to be required to authenticate using their Active Directory user account credentials when accessing the intranet Web site. The authentication will be required to be automatic requiring no user intervention during the authentication process

2. City Central Utilities wants the user accessing the intranet Web site to be prevented from executing scripts or applications on the site. City Central Utilities Also wants the users allowed to view a hypertext listing of all files and subdirectories in the Web site virtual directory.

## Topic 1, City Central Utilities (10 Questions)

---

### QUESTION 1

You need to start configuring the data stored on the file servers. You are required to reconfigure the NTFS permissions on the shared folders located on the file servers to restrict access to the data.

What should you do? (Choose all that apply.)

- A. You should remove the Everyone group and add the BUsers group and assign the group Full Control NTFS permission
- B. You should remove the Everyone group and add the ATUsers group and assign the group Full Control permission
- C. You should remove the Everyone group and add the ATUsers group and assign the group Modify permission
- D. You should remove the Everyone group and add the BUsers group and assign the group Modify permission
- E. You should remove the Everyone group and add the AUsers group and assign the group Modify permission

Answer: C, D, E

Explanation: You should consider taking the actions in the answers in the scenario because currently the effective permissions allow users to connect from all locations remotely and modify the contents of the shared folders.

1. The IT administrator of the City Central Utilities network wants access to the shared folders in each location to be secure. This requires non-administrative users only to be granted access to the files located on their local file server. The users in their respective locations should be able to edit files in the local shared folder but should not be able to take ownership or change permission of user files

Incorrect Answers:

A, B: You should not consider the actions used in these options in the scenario as you would be granting the users the ability to take ownership of the files giving them too much administrative privileges.

---

### QUESTION 2

You need to design the security solution for the internal Web site. You are required to ensure that only authorized network users in the domain are able to access the internal Web site. You are also required to select how to configure access to the site.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. You should enable Digest authentication
- B. You should enable Web site connection limits
- C. You should enable Integrated Windows authentication
- D. You should disable Anonymous authentication

Answer: C, D

Explanation: In the scenario you should disable the Anonymous authentication and enable the Integrated Windows authentication because the Anonymous authentication allows the users to establish connections to the Web site using an Anonymous account or guest account.

1. City Central Utilities wants all the attempts by unauthorized users to access the data folders on the file server to be monitored. City Central Utilities Also wants the users to be required to authenticate using their Active Directory user account credentials when accessing the intranet Web site. The authentication will be required to be automatic requiring no user intervention during the authentication process

Incorrect Answers:

A: This option should not be used in the scenario because it requires a realm to be configured and is more suited for authentication passing through a firewall.

B: This option should not be used in the scenario as this will not stop unauthorized access to the internal Web site.

---

### QUESTION 3

You need to modify the Default Domain Policy GPO. You should stop the ability of the network users to install any application which is not approved. Your solution is required to prevent the network users of the City Central Utilities network from being able to install unauthorized software.

What should you do?

- A. You should enable the Disable Windows Installer policy with a setting of For non-managed apps only
- B. You should add a Software Installation Policy which assigns approved applications to domain users
- C. You should Enable the Disable Windows Installer policy with a setting of Always
- D. You should Disable the Windows Installer policy

Answer: A

Explanation: In the scenario you should consider making these configuration changes as this will allow you to control the applications that the users are capable of installing thereby stopping unauthorized applications from being installed.

1. The Chief Security Officer also wants to have a consistent set of programs and applications to be defined and deployed. The City Central Utilities Domain users should not be able to update or install any software components other than those approved by members of the CCUAdmin group.

Incorrect Answers:

B: In the scenario you should not use this option because this will not prevent the users from installing unauthorized application but will simply assign or publish the applications to the users.

C, D: You should not take this action in the scenario because this allows the users to install Windows Installer-based applications at will be it unauthorized or not.

---

**QUESTION 4**

You need to design a solution for the client computers in the Brisbane office. The solution you are designing should configure the client computers to meet the requirements of the network Chief Security Officer.

What should you do?

- A. The users connecting to CCU-SR05 should be required to use smart card-authenticated terminal services connections
- B. Secure Sockets Layer (SSL) should be required for connections between the Brisbane clients and CCU-SR05
- C. The Brisbane network users should be required to connect to CCU-SR05 using Integrated Windows authentication
- D. IPSec-encrypted connections should be required between the Brisbane clients and CCU-SR05

Answer: A

Explanation: In the scenario you are required to provide two-factor authentication on the network for communicating with CCU-SR05. The configuration used in the answer successfully implements the required configuration and meets the requirements.

1. Another concern of the Chief Security Officer is that user access to the inventory tracking application on CCU-SR05 be secured by using certificate-based authentication. The Chief Security Officer also wants auditing enabled on CCU-SR05 to monitor all users accessing this application. You should then be able to verify who is logged on to the application and who the owner of the user account is

Incorrect Answers:

B: You should not consider using SSL in the scenario because SSL requires machine certificates in order to establish a secure channel.

C: In the scenario the users shared their credentials so making this configuration will not adhere to the requirements of the Chief Security Officer.

D: You should not consider using IPSec in the scenario because IPSec will identify the two computers and you are required to identify the users.

---

**QUESTION 5**

You need to design an authentication method for the portable computer used on the network. The solution you are designing should be employed to provide the desired level of security for the remote portable computer?

- A. MS-CHAP v2.
- B. Two-factor authentication.
- C. IPSec authentication.

D. 802.1x authentication.

Answer: B

Explanation

: When two-factor authentication is implemented, users will be required to swipe smart card into a smart card reader and then enter a PIN to authenticate to the computer. Before a smart card is used, the user's logon certificate, public key, and private key must be programmed on the smart card. You can program the smart card using a Smart Card Enrollment station, which is integrated with certificate services. You can use the EAP-TLS protocol for certificate and smart card authentication.

1. The management of City Central Utilities has decided to continue issuing portable computers to the Brisbane users but the authentication to the wireless portion of the City Central Utilities network should be strictly controlled. City Central Utilities should ensure that user credentials for portable computers and desktop computers are tightly controlled using two-factor authentication

Incorrect Answers:

A: MS-CHAP v2 does not support smart cards and does not provide the required two-factor authentication.

C: IPsec is used to generate keys for encrypting data during PPTP and L2TP tunneling transmissions. It is not a user authentication protocol.

D: IEEE 802.1x authentication is a certificate-based standard that supports authenticated network access to wired Ethernet networks from 802.11 networks which is wireless. This method will provide support for centralized user identification, authentication, dynamic key management and accounting. This is ideal for wireless LAN implementations.

---

### QUESTION 6

You need to design an authentication strategy that will be used to strengthen the current network security. The solution you are designing must ensure you meet the requirements of City Central Utilities.

What should you do? (Each correct answer represents a part of the solution. Choose TWO.)

- A. Configure all computers in the Finance department to use PEAP authentication.
- B. Issue smart cards and smart card readers to all users and computers.
- C. Install user certificates on all computers.
- D. Configure the domain to require smart cards during logon for all users.
- E. Configure the domain to respond to requests for IPsec encryption.
- F. Configure the domain to require NTLMv2 authentication.

Answer: B, D

Explanation: Following are the relevant information regarding an authentication strategy for the tightening of network security as described in the case study:

1. In response to this City Central Utilities wants the network design to be modified to increase the security and resolve the issues specified in the audit. City Central Utilities also wants any configurations to be centrally defined and applied to the network domain

controllers and network server as well as client computers when possible.

Smart cards provide a secure method of logging on to a Windows Server 2003 domain. It is a credit-card-sized device that is used to securely store public and private keys, passwords, and other types of personal information. To use a smart card, you need a smart card reader attached to the computer and a personal identification number (PIN) for the smart card. In Windows Server 2003, you can use smart cards to enable certificate-based authentication and SSO to the enterprise.

The smart cards "force" the employee to use the asymmetric key and a PIN to authenticate.

Making use of smart cards and smart card readers and configuring the domain to require smart cards during logon implementing two-factor authentication as is required in the case study.

Incorrect Answers:

A: Protected EAP authentication doesn't provide any authentication itself. Instead, it relies on external third-party authentication methods that you can retrofit to your existing servers. This is not what is required.

C: Making use of user certificates is not going to enforce two-factor authentication.

E: Configuring all computers to respond to requests for IPSec encryption is not going to enforce two-factor authentication.

F: Depending on the operating system in use, the clients might not be able to use the NTLM v2 authentication protocol. If they cannot and there is an account on the secured server that the down-level client needs to access, it will be unable to do so.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 2, p. 74

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 283

---

### **QUESTION 7**

You need to design an authentication solution for the wireless network. The solution you are designing should adhere to the security requirements of City Central Utilities. You are required to select which protocol is suitable for use on the portable computers with wireless technology.

What should you do?

- A. The wireless network should be configured to use Wired Equivalent Privacy (WEP).
- B. An Internet Authentication Service (IAS) server should be installed and configured
- C. IEEE 802.1x authentication should be configured with smart cards.
- D. Wireless VPNs using L2TP/IPSec should be created between the client computers to the wireless access point.

Answer: A

Explanation: You should consider making use of the WEP protocol in the scenario because using this protocol ensures that you adhere to the security policy of City

Central Utilities.

1. The City Central Utilities network CIO has recently said that their network is not a high-security industry but an inconsistent revenue cycle requires City Central Utilities to increase and decrease staffing levels on a regular basis. These actions have caused City Central Utilities to be more vigilant protecting network access.

---

**QUESTION 8**

You need to design a solution for network users using the Web content security zones. The solution you are designing should be used to prevent the network users from making changes to the settings for Web content security zones.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. A new GPO should be created and enable the Security Zones: Do not allow users to add/delete sites policy
- B. The new GPO should be linked to each CCUCA OU
- C. The new GPO should be linked to the Atlanta, Brisbane and Auckland OU
- D. The new GPO should be linked to the domain level

Answer: A, B

Explanation:

In the scenario you are required to configure the settings to allow the network users only to view approved sites. By making these configurations you completely adhere to the requirements in the scenario.

1. The Chief Security Officer wants the users to be allowed to only view approved Internet Web sites. The Chief Security Officer also wants only the administrators to be allowed to add and remove sites from the list of approved Web sites. The City Central Utilities network users should not be allowed to override these restrictions by modifying the Internet security settings in Control Panel.

Incorrect Answers:

C: The GPO should not be linked to the parent OU as the OUs contain the client computer accounts in each location.

D: You should not take this action on the domain as this will affect all the network users and that is not required in the scenario.

---

**QUESTION 9**

You need to design an auditing solution. The auditing solution you are designing should meet the requirements for the file server of the City Central Utilities network. You are required to select which of the following to audit?

- A. Audit success and failures events for logon events.
- B. Audit success and failure events for object access.
- C. Audit failures events for privilege use.
- D. Audit success and failures events for privilege use.

Answer: B

Explanation: Auditing object access audits user access to objects such as files, folders, registry keys, and so forth. As with the other audit policies, you can either monitor the success or failure of these actions.

1. City Central Utilities wants all the attempts by unauthorized users to access the data folders on the file server to be monitored. City Central Utilities Also wants the users to be required to authenticate using their Active Directory user account credentials when accessing the intranet Web site. The authentication will be required to be automatic requiring no user intervention during the authentication process

Incorrect Answers:

A:

In the scenario you should not audit logon events because each instance of a user logging onto or off from the network. The policy will audit events where the logon occurs.

C, D: Auditing privilege use tracks events when a user exercises a right.

---

### QUESTION 10

You need to design a solution for the desktop computers. The solution you are designing should ensure that the user's desktop is protected when they leave their computers unattended. Your solution should require the least amount of administrative effort.

What should you do?

A. A security template should be used that configures all computers to automatically log off users when their logon time expires. The new template should be imported into the local security policy on all domain controllers

B. An administrative template should be created and enable and password protect a screen saver. You should then import the new template into the Default Domain Policy GPO

C. All computers should be configured to automatically log off users when their logon time expires in the Default Domain Controller Policy GPO

D. You should enable a screen saver and password protect it in the Default Domain Policy GPO

Answer: D

Explanation: In the scenario you should consider enabling a screen saver and protect it with a password. By making this configuration you ensure that all the computers on the domain require a password to log on if the computer is left unattended for a period of time defined.

1. City Central Utilities does not apply security patches consistently to the network computers. Because of this some network computers were recently infected by a virus which could have been avoided if the security patches were up-to-date. Most of the City Central Utilities network users do not lock their computers when leaving it unattended over extended periods of time. This action has recently caused contents of a sensitive document to be made public because it was left open on the user portable computer. An

unauthorized user has viewed the documents while delivering files to the office

Incorrect Answers:

A, C:

These options should not be used in the scenario because the option is used to have users disconnected from the local computer when logging on outside their valid logon hours.

B: This option should not be used in the scenario because you are required to use the least administrative effort. This option involves too much administrative effort.

## Topic 2, TestLabs, Inc., Scenario

### Background

TestLabs, Inc. is a national company that specializes in the development and retail of pharmaceutical medicines. The company is closely aligned to the Medical Science department at the University of Chicago.

### Physical Locations

TestLabs, Inc. has its headquarters in Chicago and a branch office in Detroit. The two offices are connected by a 128 Kbps ISDN line.

TestLab, Inc. users and departments are distributed among the two offices as shown in the following table:

| Office  | Users | Departments                                               |
|---------|-------|-----------------------------------------------------------|
| Chicago | 395   | Human Resources, Research and Information Technology (IT) |
| Detroit | 80    | Manufacturing                                             |

### Business Processes

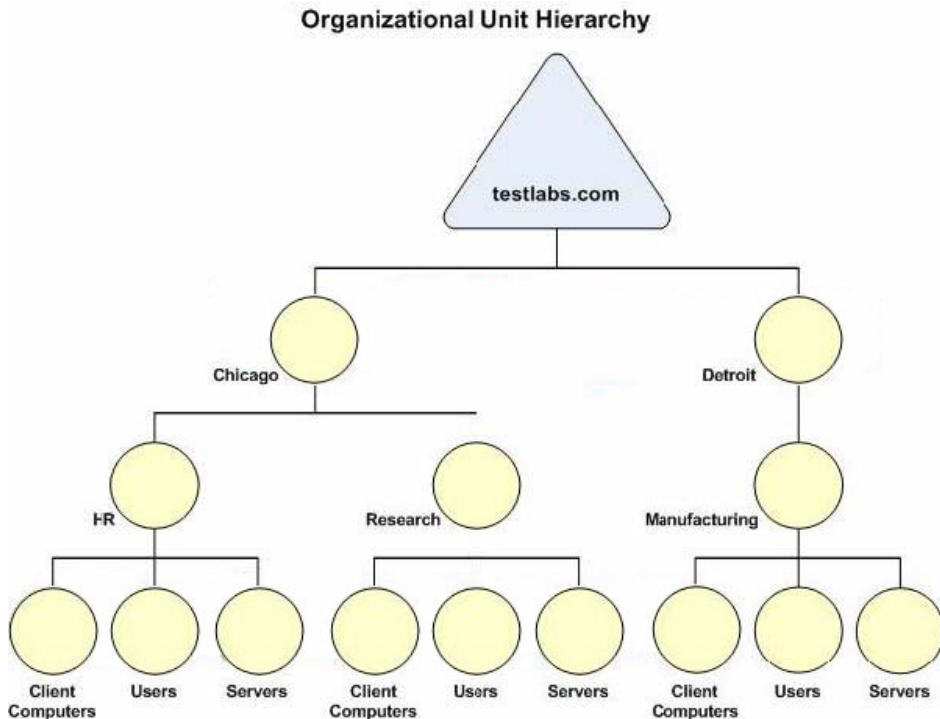
Members of the IT department use client computers to remotely administer all servers and domain controllers on the TestLabs, Inc. network.

Users update an internal tracking Web application that tracks the testing and development of new pharmaceutical drugs. The tracking Web application is available on an internal Web site that is hosted on a Web server named TL-SR07. TL-SR07 is running Internet Information Services (IIS) 6.0.

### Directory Services

The TestLabs, Inc. network consists of a single Active Directory domain named testlabs.com. All servers on the TestLabs, Inc. network run Windows Server 2003, Enterprise Edition. The IT department in Chicago is responsible for the administration of Active Directory.

Each office is organized into a separate organizational unit (OU) with the user and computer accounts located in child OUs as shown in the Organizational Unit Hierarchy exhibit.



The ChicagoAdmins, HRAdmins, ResearchAdmins, and ManufacturingAdmins global user groups are located in their respective OUs and have full control of that OU.

### Network Infrastructure

The HR department uses a legacy application that can run only on Windows NT Workstation 4.0. The client computers for all other departments run Windows XP Professional.

The testlabs.com domain has a public key infrastructure (PKI) that comprises of an internal root certification authority (CA) and an internal subordinate enterprise CA. The

internal subordinate enterprise CA issues certificates to users and computers.

The Chicago office has three domain controllers named TL-DC01, TL-DC02, and TL-DC03. The Detroit office has one domain controller named TL-DC04.

The Chicago office has a Microsoft Internet Security and Acceleration (ISA) Server 2000 computer named TL-SR05, and wireless access points (APs). TL-SR05 and the wireless APs support wireless desktop and portable client computers in the Research department. IEEE 802.1x, RADIUS, and Wired Equivalent Privacy (WEP) is implemented in the wireless network infrastructure.

### Problem Statements

#### Chief Information Officer:

"Security is my main concern. We must improve security on client computers, servers, and domain controllers. We should implement a secure password policy. Legislation requires that the servers in the Research department display a logon message that tells users that access to the server is restricted to authorized users."

#### System Administrator:

"Our current patch management solution is problematic. It requires too much time, consumes too much bandwidth and leads to too much down time. Each department needs different security patches. We need a test network to test security patches and updates before they are deployed to the rest of the network. After testing a patch, it must be deployed automatically to servers in the appropriate department. We need to limit the network bandwidth used to obtain and deploy security patches."

**Chief Security Officer:**

"My main concern is permission escalation and unauthorized access to the wireless network. We need to know when an administrator changes the user permissions on server or on a domain controller and when the local security account manager objects on any server are changed."

"We must also improve the secure of the wireless network in the Chicago office. We must ensure that only Research department users can connect to the wireless network. We need to implement the most secure method for authenticating users that access the wireless networks and we need to protect the data that is transmitted between the wireless client computers and the wireless access points. We must also ensure that our wireless client computers receive the required wireless network access security settings automatically."

**Backup Operator:**

"We run backups of all users' My Document folders but some users in the Detroit office have changed the location of their My Documents folders to network folders on one to the servers in their office. We should prevent them from doing this so that we can effectively backup user data."

**Research Department Manager:**

"Members of the ResearchAdmins group is a problem. I suspect we have unauthorized users in this group. We need to restrict membership to this group to authorized users."

"We store documents in a network share named Projects on a file server named TL-SR06. Users in my department need to encrypt data in the Projects folder from our client computers but we can't. Every time we try to we receive an error message stating that we cannot encrypt data located in the Projects folder. We need to be able to encrypt this data."

**Written Security Policy**

The following requirements are included in the written security policy for TestLabs, Inc.

1. Passwords must be at least eight characters long and must contain uppercase and lowercase letters and numbers.
2. Passwords may not contain all or part of the user's account name.
3. Passwords must have a minimum password age must be 15 days and a maximum password age of 45 days.
4. Access to data on servers in the Manufacturing department must be logged.
5. All servers on the TestLabs, Inc. network, including domain controllers, must be configured and managed from the Chicago office.
6. A standard set of security settings must be deployed to all servers in the HR, Research,

and Development departments.

7. The services on domain controllers and the administrators that have permission to stop and start services must be managed from the Chicago office.
8. All servers must be examined regularly for missing security patches and service packs.
9. All servers must be examined regularly to ensure that they are not running any unnecessary services.
10. The TL-SR07 must be examined regularly for missing IIS Security patches.
11. The Web site users and the files they download must be logged to a Microsoft SQL Server database server named TL-DB05.
12. Medical Science department users from the University of Chicago who use Windows 95 or Windows 98 client computers must have the Active Directory Client Extensions software installed to be able to authenticate to domain controllers on the TestLabs, Inc. network.

## Topic 2, TestLabs, Inc. (11 Questions)

---

### QUESTION 1

You are designing a certificate distribution method to meet the requirements of the Chief Security Officer.

What should you do? (Each correct answer presents part of the solution. Choose THREE.)

- A. Instruct the users in the Research department to submit a request for user certificates from the CA Web site enrollment page.
- B. Create a Group Policy object (GPO) and configure it to allow autoenrollment of user and computer certificates.
- C. Link the Group Policy object (GPO) to the Research OU.
- D. Instruct the users in the Research department to run the gpupdate command.
- E. Link the Group Policy object (GPO) to the testlabs.com domain.
- F. Configure certificate templates.

Answer: B, C, F

Explanation:

The Auto-enrollment features are set by CA administrators in the certificate templates and will automatically issue certificates.

Group Policy Object (GPO) is a set or sets of rules for managing client configuration settings that pertain to desktop lockdowns and the launching of applications. GPOs are data structures that are attached in a specific hierarchy to selected Active Directory Objects. It can be applied to sites, domains, or organizational units. This reduces the administrative effort required to apply the same policies on an individual basis. In this scenario we need to apply the GPO to the Research department OU as only members in the Research department must be able to access the wireless network.

Incorrect Answers:

A: Instructing users to submit requests for a user certificate from the CA web site enrollment page would require unnecessary user intervention. The chief security officer

wants wireless client computers to receive the required wireless network access security settings automatically, i.e., without user intervention.

D: The gpupdate command forces a GPO update.

E: The GPO must be applied at the Research OU level as only members in the Research department must be able to access the wireless network. Applying the GPO at the domain level will allow all users to access the wireless network.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 3, 4 & 9, pp. 181, 197, 566-569

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 21

---

## QUESTION 2

### DRAG DROP

You are planning the configuration of the servers in the Research department to meet the requirements of the Chief Information Officer. You decide to use a Group Policy object to implement the configuration.

What should you do? (To answer, drag the appropriate steps from the pane on the left and arrange them in the correct order in the pane on the right.)

#### Steps, select from these

- Configure the Group Policy object (GPO) to require a screensaver password.
- Configure the Group Policy object (GPO) not to require the CTRL+ALT+DELTE keys.
- Configure the Group Policy object (GPO) to display a logon message.
- Link the Group Policy object (GPO) to the Research OU
- Link the Group Policy object (GPO) to the Research department's Servers OU.
- Link the Group Policy object (GPO) to the domain.

#### Steps, place here

- Place first step here.
- Place second step here, if any.
- Place third step here, if any.
- Place fourth step here, if any.
- Place fifth step here, if any.
- Place sixth step here, if any.

Answer:

| Steps, select from these                                                        | Steps, place here                                                           |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Configure the Group Policy object (GPO) to require a screensaver password.      | Link the Group Policy object (GPO) to the Research department's Servers OU. |
| Configure the Group Policy object (GPO) not to require the CTRL+ALT+DELTE keys. | Configure the Group Policy object (GPO) to display a logon message.         |
|                                                                                 | Place third step here, if any.                                              |
| Link the Group Policy object (GPO) to the Research OU                           | Place fourth step here, if any.                                             |
|                                                                                 | Place fifth step here, if any.                                              |
| Link the Group Policy object (GPO) to the domain.                               | Place sixth step here, if any.                                              |

Explanation: GPOs can be applied to sites, domains, or organizational units. We need the GPO to apply to the servers in the Research department; therefore we must apply the GPO to the Server OU in the Research department. Network users perform an interactive logon when they present their network credentials to the operating system of the computer that they are attempting to log on to. Thus an interactive logon is a logon when the user logs on from the computer where the user account is stored on the computer's local database. This is also called a local logon. This will be the way to go about designing a method to configure the servers in the development department since this department is in Denver.

1. We need a logon message that tells users that access to servers in the development department is restricted to authorized users only.
2. We must improve security on client computers, servers, and domain controllers by implementing a secure password policy.

Incorrect Answers:

This is not the way to log on interactively. You will have to them the Log On Locally user right. Otherwise users will receive an error message that they cannot log on interactively.

A screensaver requiring a password is not complying with security policy since the servers would still be available from other workstations through the network.

We need the GPO to apply to the servers in the Research department; therefore we must apply the GPO to the Server OU in the Research department.

### QUESTION 3

You need to log user permissions changes on server or on a domain controller. You also need to log changes to the local security account manager objects on all servers. What should you do?

- A. Configure auditing of privilege user and object access on all servers and domain controllers and set it to failure.
- B. Configure auditing of policy change and account management on all servers and domain controllers and set it to success.

- C. Configure auditing of process tracking and logon events on all servers and domain controllers and set it to success.
- D. Configure auditing of system events and directory service access on all servers and domain controllers and set it to failure.

Answer: B

Explanation: Auditing for policy change events allows you to see attempts to alter policy settings, including changes to audit policies. And auditing the account management on all servers and domain controllers allows you to see attempts to alter security account manager objects. If you want to log changes that are made to servers and domain controllers and want to track when local security account manager objects are being modified then you need to success audit for policy change events and account management on all servers and domain controllers.

Incorrect Answers:

A: These options of auditing will not work; you need to enable success audit and not failure audit.

C: Auditing process tracking events monitors processes running on computers. Logon events

are generated when a user logs on to or off of a computer. Every time a user logs on or off, whether on a workstation or server, an event is generated. Even enabling success auditing will not provide you with the correct information to do your task.

D: These options of auditing will not work; you need to enable success audit and not failure audit. Furthermore, System events are generated when the computer environment is changed in some significant way, either by a user or by a process; and Directory Service access events record when directory services were accessed. You need to audit for policy change and account management.

Reference:

---

#### **QUESTION 4**

You need to ensure that all TestLab, Inc. servers have the latest security and that no unnecessary services are running on the servers. You must ensure that your solution can be implemented by the members of the IT department at headquarters.

What should you do?

- A. Run the Resultant Set of Policy (RSOP) wizard in planning mode from a domain controller in the Chicago office.
- B. Create a custom security template and run Security Configuration and Analysis to analyze the security settings of each server against the custom security template.
- C. Create a startup script that runs the secdit command and apply the script to all servers in the domain.
- D. Install the Microsoft Baseline Security Analyzer (MBSA) on a server in the Chicago office and use it to scan for Windows vulnerabilities on all servers in the domain.

Answer: D

Explanation: MBSA can perform local or remote scans of Windows systems. It verifies whether your computer has the latest security updates and whether there are any common security violation configurations that have been applied to your computer. If you run MBSA on a server to scan for Windows vulnerabilities on all servers in the domain then you will comply with requirements for maintaining security patches.

Incorrect Answers:

A:

RSOP is a tool that can show the effective policy applied to a user or computer or what the policy would be, for planning purposes. It does not scan for missing security patches.

B: Security Configuration and Analysis tool is a Windows 2003 utility that is used to analyze and to help configure a computer's local security settings. Security Configuration and Analysis works by comparing the computer's actual security configuration to a security database configured with the desired settings. However this would involve too much administrative effort than is necessary.

C: The command line tool, secedit.exe, is used to analyze, configure, and export system security settings. There are a variety of command-line switches used with secedit. This tool is often used in batch programs or scheduled tasks to apply security settings automatically. It is also the preferred tool for reapplying default security settings. But this does not necessarily mean that missing security patches will be checked for.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 159

---

### **QUESTION 5**

You need a strategy to log access to data on servers in the Manufacturing department.

What should you do?

A. Install the Microsoft Baseline Security Analyzer (MBSA) on a server in the Chicago office and use it to scan for Windows vulnerabilities on all servers in the Manufacturing department.

B. Create a custom security template and run Security Configuration and Analysis to analyze the security settings of each server in the Manufacturing department against the custom security template.

C. Create a Group Policy Object (GPO) and configure the GPO to audit successful logon attempts. Link the GPO to the Manufacturing department's Servers OU.

D. Create a Group Policy Object (GPO) and configure the GPO to enable auditing for object access. Link the GPO to the Manufacturing department's Servers OU.

Answer: D

Explanation:

Auditing object access audits user access to objects such as files, folders, registry keys, and so forth. As with the other audit policies, you can either monitor the

success or failure of these actions. Further more making use of a GPO will ease the administrative effort. Linking this GPO to the Manufacturing department's Servers OU should be the strategy used to monitor the data on the serves in the Manufacturing department.

Incorrect Answers:

A: MBSA verifies whether your computer has the latest security updates and whether there are any common security violation configurations that have been applied to your computer. This is not the same as monitoring the servers to meet business requirements. Auditing object access if what is required.

B: The Security Configuration and Analysis tool is used to analyze and to help configure a computer's local security settings. Security Configuration and Analysis works by comparing the computer's actual security configuration to a security database configured with the desired settings. This is not the same as tracking all access to data on the servers in the Manufacturing department.

C: You should audit object access to track access to data. Auditing logon attempts will only log attempts to logon to the server it will not log access to data over the network.

---

### **QUESTION 6**

You need to plan for the security of the wireless network and wireless traffic in the Chicago office to meet the requirements of the Chief Security Officer. What should you do?

A. Configure Media Access Control (MAC) address filtering on the wireless access points in the Chicago office.

B. Configure the wireless access points in the Chicago office to use a Sever Set ID (SSID) and a 128-bit Wired Equivalent Privacy (WEP) shared key.

C. Enroll and deploy computer certificates to all wireless client computers in the Chicago office and configure each wireless client computer to use Protected EAP (PEAP).

D. Create a wireless network policy that enables data encryption and dynamic key assignments for the Chicago network. Implement wireless network policy through a GPO that is linked to the Chicago OU.

Answer: D

Explanation:

The Chief Security Officer requires that data sent between the wireless client computers and the wireless access points be protected; that wireless client computers need to automatically obtain wireless network access security settings; and that the most secure method for authenticating wireless users that access the wireless network is implemented. These requirements can be accomplished by using a wireless network policy and applying that policy through a GPO that is linked to the Chicago OU.

Incorrect Answers:

A: Filtering MAC addresses will ensure that only authorized computers can access the wireless network. However, it does not protect wireless traffic.

B: You could configure the wireless access points in the Chicago office to use a Sever

Set ID (SSID) and a 128-bit Wired Equivalent Privacy (WEP) shared key but you would need to configure the wireless client computers with these settings. The Chief Security Officer requires that wireless client computers obtain wireless network access security settings automatically. You should use a GPO to distribute the WEP keys to all wireless client computers in the Chicago OU.

C: Protected Extensible Authentication Protocol (PEAP) can make use of various authentication methods that are based on passwords, public key certificates or other credentials. It ensures the secure transmission of authentication credentials over wired or wireless networks. However, PEAP is not an encryption protocol and does not protect data that is transmitted over a wireless connection.

---

**QUESTION 7**

You need a strategy to log access to the testlabs.com intranet Web site to meet the requirements in the written security policy.

What should you do?

- A. Enable logging on the intranet Web site on TL-SR07 and select the NCSA Common Log File Format. Store the log files on TL-DB05.
- B. Create a Group Policy Object (GPO) and configure the GPO to audit successful logon attempts and object access. Apply the GPO to TL-SR07.
- C. Configure the intranet Web site on TL-SR07 to require Windows authentication. Create a Group Policy Object (GPO) and configure the GPO to audit successful logon attempts and object access. Apply the GPO to TL-SR07.
- D. Enable logging on the intranet Web site on TL-SR07 and select the ODBC Logging option.

Answer: D

Explanation: You should enable logging on the company web site and select ODBC logging. Open Database Connectivity (ODBC) logging allows you to log data directly to a SQL database using an ODBC connection. Since the case study mentions that all users of the website and the files that they download, should be tracked and the data stored in a SQL database, you should also configure the logging options through a non-administrative SQL account.

Incorrect Answers:

- A: NCSA Common Log File Format logging will not yield the proper information to address the issue of logging all access to the website and the files that users download.
- B, C: You should audit object access to track access to files; however, auditing logon attempts will only log attempts to logon to the Web server rather than the Web site. This method also does not store the logs to a Microsoft SQL Server database server named TL-DB05.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 731

Lisa Donald with Suzan Sage London and James Chellis, MCSA/MCSE: Windows

Server 2003 Environment Management and Maintenance Study Guide, pp. 321, 374-9, 446-51

---

**QUESTION 8**

You need to plan a membership strategy for the ResearchAdmins group to meet the requirements of the Research Department Manager.  
What should you do?

- A. Place the members of the ResearchAdmins group in the Research OU.
- B. Place the ResearchAdmins group in the Research OU.
- C. Place the ResearchAdmins group in the Chicago OU.
- D. Place the members of the ResearchAdmins group in the Chicago OU.

Answer: B

Explanation:

On a Windows Server 2003 member server, you can use only local groups. A local group resides on the Windows Server 2003 member server's local database. Since the members of the ResearchAdmins group comprises of both authorized and unauthorized users, the whole group should be moved to the Research OU so as to restrict membership to only authorized users in the Research department.

Incorrect Answers:

A: Moving the members of the ResearchAdmins group to the Research OU will not work as the ResearchAdmins group will still exist outside the Research OU. You need to move the ResearchAdmins group to the Research OU.

C: Moving the members of the ResearchAdmins group to the Chicago OU will allow all members of the Chicago OU to be members of the ResearchAdmins group. You need to restrict membership to the Research department. You should therefore move the ResearchAdmins group to the Research OU.

D: Moving the members of the ResearchAdmins group to the Research OU or the Chicago OU will not work as the ResearchAdmins group will still exist outside the Research OU. You need to move the ResearchAdmins group to the Research OU.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, pp. 100-101

---

**QUESTION 9**

You need to design a patch management system to meet requirements of the System Administrator.  
What should you do?

- A. Install Software Update Services (SUS) on three servers named TL-SR08, TL-SR-09 and TL-SR10.  
Deploy TL-SR08 to a test network in the Chicago office, TL-SR09 to the production network in the Chicago office and TL-SR10 to the Detroit office.

Configure TL-SR09 and TL-SR10 to download administrator-approved updates from TL-SR08.

B. Install Software Update Services (SUS) on two servers named TL-SR08, TL-SR-09. Deploy TL-SR08 to the Chicago office and TL-SR09 to the Detroit office.

Configure TL-SR09 to download administrator-approved updates from TL-SR08.

C. Install MBSA on a server named TL-SR08 and deploy TL-SR08 to a test network in the Chicago office.

Deploy MBSA as a Windows Installer package to all computers in the Chicago OU and the Detroit OU.

Configure MBSA to scan for updates from TL-SR08.

D. Install Software Update Services (SUS) on a server named TL-SR08. Deploy TL-SR08 to a test network.

Create a Web site named ApprovedUpdates on TL-SR07 that contains administrator-approved updates.

Configure an autoupdate policy in the testlabs.com domain to download and deploy updates from the ApprovedUpdates Web site

Answer: A

Explanation: Software Update Services (SUS) is used to leverage the features of Windows Update within a corporate environment by downloading Windows Update to a corporate server, which in turn provides the updates to the internal corporate clients. This allows administrators to test and have full control over what updates are deployed within the corporate environment.

Deploying a Windows Server 2003 computer to run the SUS in the test network and then deploying SUS servers in each office for downloading of approved updates is the solution.

Incorrect Answers:

B: Making use of Autoupdate policies in each child domain as described in this option is not the solution since it does not mention that the downloads will be administrator approved updates from the test network SUS server.

C: MBSA verifies whether your computer has the latest security updates and whether there are any common security violation configurations that have been applied to your computer. This is not what is required in this question.

D: You could create a website on the Web server to distribute approved updates, but this would not reduce the bandwidth required to apply the updates to computers in the Detroit office. It would be better to configure one server in the Detroit office to download the approved updates and distribute it to the rest of the computers in the Detroit office.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 477

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 2, p. 51

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide, p. 55

---

**QUESTION 10**

You need to design a method to implement an account policy that meets the requirements in the written security policy.  
What should you do?

- A. Configure required account policy settings in a GPO and link the GPO to the Chicago OU and the Detroit OU.
- B. Configure the Local Security Policy with the required account policy settings on all computers in the domain.
- C. Configure the required account policy settings in the Default Domain Policy GPO.
- D. Configure the required account policy settings in the Default Domain Controllers Policy GPO.

Answer: C

Explanation: To implement account policies that meet these requirements you need to configure the Default Domain Policy GPO with the necessary account policy settings. Setting policies in the Default Domain Policy sets them for all computers in the domain.  
Incorrect Answers:

- A: You could configure required account policy settings in a GPO and link the GPO to the Chicago OU and the Detroit OU but configuring the required account policy settings in the Default Domain Policy GPO would require less effort and would be the better option.
- B: You could configure the Local Security Policy with the required account policy settings on all computers in the domain but configuring the required account policy settings in the Default Domain Policy GPO would require less effort and would be the better option.
- D: You should configure the Default Domain Policy GPO and not the Domain Controllers GPO. The Domain Controllers GPO applies the setting to domain controllers and not all computers in the domain.

---

**QUESTION 11**

You need to design a method of deploying security configuration settings to all servers in the domain.  
What should you do?

- A. Run the Resultant Set of Policy wizard with a Windows Management Instrumentation (WMI) filter on each department's Server OU.
- B. Log on to each server and use the System Policy Editor to configure the server's security settings.
- C. Create a customer security template. Log on to a domain controller in the Chicago office and use the secedit command to import the security template.
- D. Create a customer security template and import the security to a GPO. Link the GPO to each department's Server OU.

Answer: D

Explanation: You can define a base security template on a single computer and then export the security template to all the servers in your network. The security template is used as a comparative tool. You do not set security through the security template. Rather, the security template is where you organize all of your security attributes in a single location. Once you have configured a security template, you can import it for use. To deploy security configuration settings to servers you should first create a customer security template and then a group policy object to import the security template. After that you link the GPO to each department's Server OU.

Incorrect Answers:

A: Resultant Set of Policy (RSOP) is a new feature of Windows Server 2003 that provides the ability to see exactly how the various policies within the domain will apply to a specific user or computer. However, you do not just want to view how and which policies are applied, you need to create a method to deploy security configuration settings.

B: This option suggests an administratively intensive procedure. Furthermore it ignores the fact that a standard set of security settings should be deployed which should have been configured and managed from a central location.

C: This command is used to force updates on policies. But this implies that the security policy is already in place and only being edited.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, pp. 127-128, 173

## Topic 3, Willow Bridge, Ltd., Scenario

### Background

Willow Bridge, Ltd. manufactures security systems. They distribute these products to retail stores and the public.

A company named Bilco.com provides components for Willow Bridge, Ltd. products. Willow Bridge, Ltd. recently bought Bilco.com.

### Physical Locations

The Willow Bridge, Ltd. headquarters are located in Chicago. The company has branch offices in New York and Los Angeles. Bilco.com is located in Detroit.

The Willow Bridge, Ltd. branch offices are connected to the head quarters via a T1 leased line. And the Chicago office is connected to the Internet through a T1 leased line. The Bilco.com office connects to Chicago through a VPN connection.

The Chicago office consists of the Finance, Marketing, Sales, Human Resources and IT departments.

The Los Angeles and New York offices: consist of a Sales department.

The Bilco.com office in Detroit consists of the Research and Development department.

### Planned Changes

Willow Bridge, Ltd. plans to make the following changes.

1. The Finance Department client computers will be upgraded to Microsoft Windows XP Professional.
2. An organizational unit (OU) named Research and Development will be created in the willowbridge.com domain.
3. Three child OUs will be created in the Research and Development OU: Research, Wireless Clients, and desktop clients.
4. A server named RRAS1 will be deployed on the internal network
5. Two remote access servers named VPN1 and VPN2 will be configured for the VPN connection between the Chicago and Detroit offices.
6. A wireless access point will be deployed in the Chicago office.
7. The Detroit office will also make use of a Web server named WEB2
8. Our customers will in future be able to use the willowbridge.com Web site to keep track of their orders and its status that they had placed.

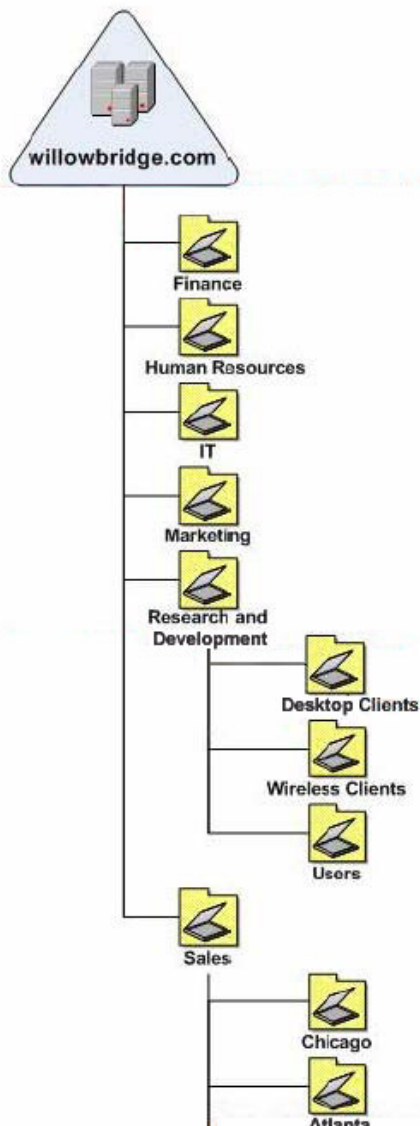
### **Active Directory**

The Willow Bridge, Ltd. network consists of single Active Directory domain named willowbridge.com. The willowbridge.com domain is located in the Chicago office, and all domain controllers run Windows Server 2003.

The Bilco.com domain, after the takeover, has been migrated to the willowbridge.com Active Directory domain and will thus constitute the Research and Development department of willowbridge.com

The OU structure for the network is illustrated in the OU Structure exhibit.

## OU Structure



Six top-level organizational units (OUs) have been created. These OUs hold the user and computer accounts of their respective departmental users. These OUs represent the different departments:

1. Finance OU
2. Marketing OU
3. Sales OU
4. Human Resources OU
5. IT OU
6. Research and Development OU

The Sales OU contains three child OUs that represent the different offices where there are Sales Department users, named: Chicago, Los Angeles, and New York; respectively. The Research and Development OU contains three child OUs that hold all the computer accounts of the Bilco.com users based on their functions. These child OUs are named Wireless clients, Desktop clients, Users, respectively.

## Network Infrastructure

All servers in the willowbridge.com network run Microsoft Windows Server 2003.

All willowbridge.com client computers run a mix of Microsoft Windows 2000

Professional, Microsoft

Windows NT Workstation 4.0, and Microsoft Windows XP Professional with the latest service pack.

Each office will have at least one domain controller to support local authentication.

There is a router-to-router VPN connection between the Chicago office and the Detroit (Bilco.com) office. Two remote access servers named VPN1 and VPN2 will be configured for the VPN connection.

A dial-up connection is configured on a server named RAS1. RAS1 will be deployed on the internal network and will be used by the Sales Department users who are unable to access an ISP when they are traveling.

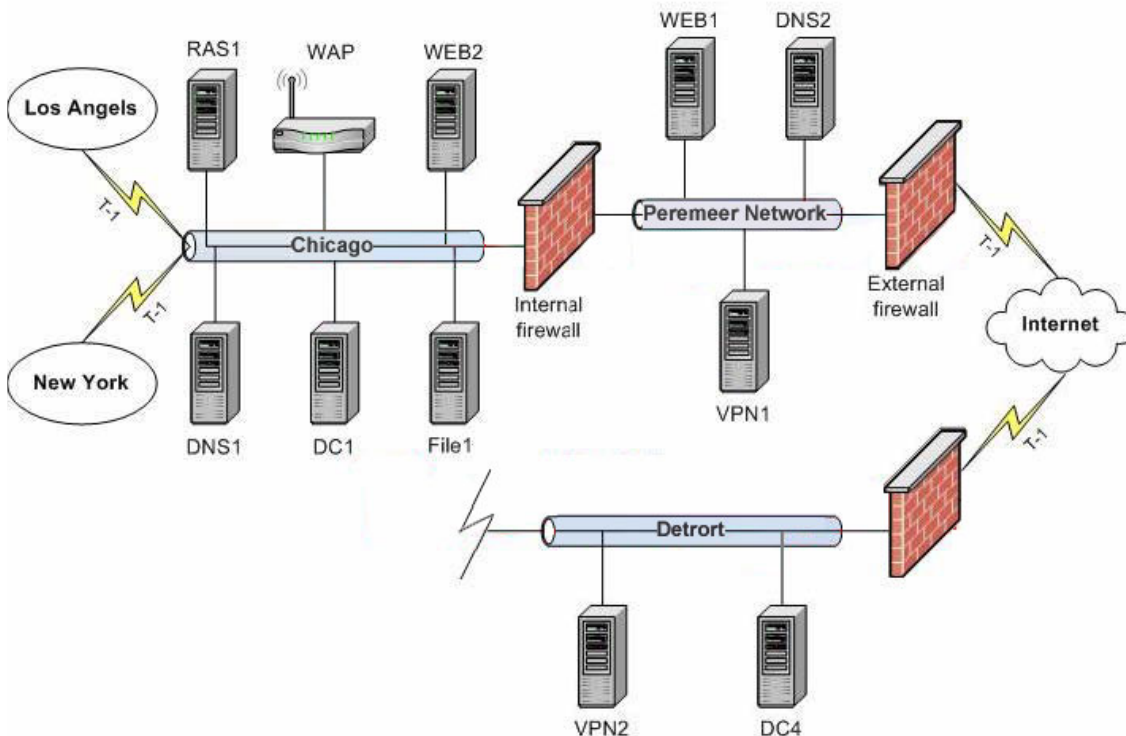
A wireless network has been set up on the Chicago office. Wireless client computers in Chicago have IEEE 802.11g wireless adapters. These wireless computers are assigned to the IT administrators.

The Chicago office also holds two DNS servers named DNS1 and DNS2 respectively. DNS1 and DNS2 are both configured with the default remote Desktop connection settings.

1. DNS1 is used to provide host name resolution services for the internal network clients and will host the standard primary zone local.willowbridge.com. DNS1 is located on the internal network in the Chicago office.

2. DNS2 is used to provide external host name resolution services and will host the external primary zone willowbridge.com. DNS2 is located on the perimeter network in the Chicago office.

**Partial Network Infrastructure**



### **Web Services**

All Web sites are hosted by using the Internet Information Server (IIS) 6.0. A web server named WEB1 is located on the perimeter network and is used to host the willowbridge.com Web site. This Web site is used for marketing, order status and contact information purposes. This Web site also has a secure section that is used by the Sales Department to provide them with access to the Willow Bridge, Ltd. inventory and order applications.

A Web server named WEB2 is located on the Willow Bridge, Ltd. internal network and is used for Web application development and testing purposes. The Detroit office will also make use of WEB2 via the VPN tunnel.

### **Problem Statements:**

#### **Chief Security Officer**

"We need to implement a public key infrastructure (PKI) to include the Detroit office, and our branch offices. We need to deploy certificates to increase security for all our new projects that are in the pipeline. All security applications and programs should be tested for compatibility before authorization for installation is granted. We must also ensure that our users do not install unauthorized software on the company client computers."

"We must ensure that all our servers that provide connections to our network are secure. All connections to these servers must be authenticated."

#### **IT Department Manager**

"The Chicago office has the wireless access point. We need to allow administrators the ability to access and modify network configurations from all areas of this office.

Currently the non-administrative users can also connect to the wireless section of the network using their personal laptop computers. This should not be allowed. Only the IT users should be able to connect to the willowbridge.com wireless network."

"We need to deploy security patches efficiently. In the past we have relied on users to download security updates directly from the official Microsoft Windows Update Web site. This led to a situation where some users plainly neglected to perform updates in a timely manner. The consequence was thus that we became vulnerable to Internet-spread viruses. All security patches must be tested and approved by the IT department in the Chicago office. We need to make sure that our patch management system must support compatibility testing of all updates before the updates are deployed to the production network. We want to enable all client computers automatically update themselves. We also want to be able to ascertain which security patches have been applied to client computers."

#### **IT administrator**

"We recently had a server failure. This could have been prevented. However, be that as it may, a non-administrative user connected to DNS1 by accident and modified some of the registry settings on DNS1, with the result that we had to make do without this server until we could restore the system state from our backup. We need to ensure that both DNS1 and DNS2 are protected against this accidental modification. I want to see only administrators able to remotely connect to DNS1 and DNS2 to modify the registry settings. I also want to have the ability to detect all attempts to log on interactively to

either of these servers."

#### **Web site administrator**

"The Sales Department makes use of the willowbridge.com Web site to provide them with access to the Willow Bridge, Ltd. inventory and order applications when traveling. Our customers will in future also make use of the willowbridge.com Web site to keep track of their orders and its status that they had placed. We must make allowances for our customers. However, we must also ensure that they register to be able to access this portion of the Web site. This registration activity must be stored in a shared folder named Customer Registration. Customer Registration can be located on a file server named FILE1. At present the Users group has been granted Allow-Full Control permission over Customer Registration."

#### **End User - Finance Department**

"We know it has become a necessity to upgrade the client computers in the Finance department. We users make use of a client/server application where the client portion was developed to run on Microsoft Windows NT Workstation 4.0. We do not have access to an upgrade for this application for ten to twelve months, to this end I want to suggest that we postpone the upgrade of the Finance Department client computers."

#### **Security**

The following security requirements must be considered:

1. Only administrators should be allowed to modify the registry on DNS1 and DNS2.
2. Security updates and patches are to be deployed in a centralized, efficient manner that minimizes traffic over WAN connections.

All solutions must ensure that WAN traffic is kept to a minimum.

3. All servers and all client computers' baseline security configuration on the willowbridge.com network must be standardized.
4. No unauthorized software must be installed on any of the computers on the Willow Bridge, Ltd. network.
5. No users other than the authenticated wireless clients should be able to connect to the wireless network in the Chicago office.  
No unauthorized wireless access points should be allowed to join the network.
6. The Chicago office administrators must make use of two-factor authentication to access the wireless network.
7. The Chicago office administrators must be able to roam between access points.
8. Certificates should be distributed to network users.  
These certificates should not require user intervention.
9. The Willow Bridge, Ltd. PKI should be tightly integrated with Active Directory.

## **Topic 3, Willow Bridge, Ltd. (11 Questions)**

---

### **QUESTION 1**

You need to design an access control strategy for the wireless access point in the Chicago office. Take care in your solution to address the IT manager's concerns. What should you do?

- A. Use EAP-TLS for authentication purposes.
- B. Use PEAP-TLS for authentication purposes.
- C. Use EAP-MS-CHAP v2 for authentication purposes.
- D. Use PEAP with MS-CHAP v2 for authentication purposes.

Answer: B

Explanation: To provide the Chicago administrators with two-factor authentication that also supports fast reconnect, you should configure wireless client to use PEAP-TLS. PEAP has the flexibility of EAP and in addition also provides additional security in that it incorporates Secure Sockets Layer (SSL) technology to protect authentication communications.

1. A wireless network has been set up on the Chicago office. Wireless client computers in Chicago have IEEE 802.11g wireless adapters. These wireless computers are assigned to the IT administrators.

2.

Currently the non-administrative users can also connect to the wireless section of the network using their personal laptop computers. This should not be allowed. Only the IT users should be able to connect to the willowbridge.com wireless network

Incorrect Answers:

A: EAP does not make provision for fast reconnect as PEAP does.

C: While EAP-MS-CHAP v2 protects user credential during authentication by sending a hash to the authenticator, it does not use a secure channel for authentication, therefore the hash that is transmitted during authentication can be captured and the associated password can be guessed by way of a possible offline dictionary attack.

D: MS-CHAP v2 does not provide the level of security that can be found in certificate based authentication mechanisms. And it also does not provide the required two-factor authentication.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 3 & 5, pp. 159, 181, 316

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, MCSE 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, pp. 595, 598

---

## QUESTION 2

Which client computers not will be affected if you configure software restriction policy at domain level by creating the appropriate rules?

- A. The Chicago office users.
- B. The IT department users.
- C. The Finance department users.
- D. The wireless network clients.

Answer: C

Explanation: you will not be able to limit application installation for the Finance department. If you configure restriction policies in Group Policy then you can only deploy these restrictions on Microsoft Windows 2000, Microsoft Windows XP Professional and Microsoft Windows Server 2003 computers. The finance department client computers run on Microsoft Windows NT Workstation 4.0.

1.  
All willowbridge.com client computers run a mix of Microsoft Windows 2000 Professional, Microsoft Windows NT Workstation 4.0, and Microsoft Windows XP Professional with the latest service pack
2. all domain controllers run Windows Server 2003
3. We users make use of a client/server application where the client portion was developed to run on Microsoft Windows NT Workstation 4.0. We do not have access to an upgrade for this application for ten to twelve months, to this end I want to suggest that we postpone the upgrade of the Finance Department client computers.

Incorrect Answers:

A: The Chicago office users can be limited if you configure software restriction policy at domain level by creating the appropriate rules. They will be upgraded to Microsoft Windows XP Professional.

B: The IT Department users if you configure software restriction policy at domain level by creating the appropriate rules. They will be upgraded to Microsoft Windows XP Professional.

D: The wireless network clients if you configure software restriction policy at domain level by creating the appropriate rules. They will be upgraded to Microsoft Windows XP Professional.

---

### **QUESTION 3**

You need to design an authentication method for communications between users who connect remotely and the Chicago office. Take care that you solution meet the requirements.

What should you do? Each correct answer presents part of the solution. Choose TWO.)

- A. Install IAS on VPN1 and VPN2. Configure both as RADIUS servers.
- B. Install IAS on DC1 and DC4. Configure both as RADIUS servers.
- C. Install IAS on RAS1, VPN1 and VPN2. Configure these servers as RADIUS servers.
- D. Configure VPN1 and VPN2 as RADIUS clients.
- E. Configure DC1 and DC4 as RADIUS clients
- F. Configure RAS1, VPN1, VPN2 and wireless access point as RADIUS clients
- G. Configure VPN1 and VPN2 as RADIUS clients

Answer: B, F

Explanation:

The RADIUS server will provide centralized connection for authentication,

authorization, and accounting functions for networks that include wireless access, VPN remote access, Internet access, extranet business partner access, and router-to-router connections. IAS proxy functions are different from these server functions, and include forwarding IAS authorization and accounting information to other IAS servers. With IAS, you should configure all network access servers, including the wireless access points, as RADIUS clients. This will provide a centralized access control solution for the network whilst allowing you to use security groups and remote policies to control remote user access.

Incorrect Answers:

A: If you install IAS on the VPN servers then you will not be able to control access on all the access points to the network. This in essence will exclude some methods of access to the network.

C: This option will exclude the wireless access point and this also needs to be included as it is an access point to the network.

D: This option will exclude some areas that are also access points on the Willow Bridge, Ltd. network.

E: This option will exclude some areas that are also access points on the Willow Bridge, Ltd. network.

G: This option will exclude some areas that are also access points on the Willow Bridge, Ltd. network.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 6, pp. 369-370  
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 335

---

#### **QUESTION 4**

You need to design an audit strategy for the Willow Bridge, Ltd. network. In your solution take care to use the least amount of administrative effort.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. Create a security template that enables Audit account logon events policy for success and failure.

B.

Create a security template that enables Audit logon events policy for success and failure.

C. Create a GPO, link the GPO to the willowbridge.com domain then import the template into the GPO.

D. Import the template into the local policy on both DNS1 and DNS2.

E. Create a GPO, link the GPO to each site/office then import the template into the GPO.

F. Create a GPO, link the GPO to each departmental OU then import the template into the GPO.

Answer: B, D

Explanation: A security template that enables Audit logon vents for success and failure will record each instance of a user logging on to, logging off from, or making a network connection to the computer. You should import this template into the local policy on DNS1 and DNS2 to ensure that any attempts to log on interactively with either a local account or a domain account will be recorded on the respective DNS server.

1. We need to ensure that both DNS1 and DNS2 are protected against this accidental modification
2. A non-administrative user connected to DNS1 by accident and modified some of the registry settings on DNS1
3. I also want to have the ability to detect all attempts to log on interactively to either of these servers

Incorrect Answers:

A: Auditing the account logon events for success and failure will record events on the computer where the logon is validated. Besides local logon events are not sent to the domain controller and only logon events that occur when a computer receives a request to validate a user account stored locally. This is not going to address the concerns of the IT administrator.

C, E, F: Linking the GPO to either the domain, site or departmental OU would apply the desired audit policy settings to object in these containers only. The objective of this solution is to use the least amount of administrative effort when designing the audit strategy for the Willow Bridge, Ltd. network.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris & Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 3, pp. 177-179

---

### **QUESTION 5**

You need to design a solution to address the concern of the Chief Security officer regarding the installation of unauthorized software on domain computers.

What should you do? (Each correct answer presents a complete solution. Choose TWO.)

- A. Disable the Disable Windows Installer policy in the Default Domain GPO.
- B. Enable the Disable Windows Installer policy and select the For non-managed apps only setting in the Default Domain GPO.
- C. Enable the Disable Windows Installer policy and select the Never setting in the Default Domain GPO.
- D. Enable the Disable Windows Installer policy and select the Always setting in the Default Domain GPO.
- E. Configure software restriction policy at domain level by creating the appropriate rules.

Answer: B, E

Explanation: Enabling the Disable Windows Installer policy and selecting the For non-managed apps only setting in the Default Domain GPO will ensure that only administrator approved applications will be installed.

You can also control the software deployment by means of configuring a software

restriction policy at domain level.

1. No unauthorized software must be installed on any of the computers on the Willow Bridge, Ltd. network.

2. We must also ensure that our users do not install unauthorized software on the company client computers."

Incorrect Answers:

A: If you disable the Disable Windows Installer policy because it will allow any application to be installed.

C: Selecting the Never setting on the Disable Windows Installer policy on the Default Domain GPO will prevent the installation of any applications, but will also prevent the administrator-approved applications from being installed.

D: Selecting the Always setting on the Disable Windows Installer policy on the Default Domain GPO will prevent the installation of any applications, but will also prevent the administrator-approved applications from being installed.

---

### **QUESTION 6**

You need to design the public key infrastructure (PKI) for the Willow Bridge, Ltd. network. Take care that your solution meets the requirements.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. Place a root enterprise CA in the Chicago office and issuing subordinate enterprise CAs in Detroit, Los Angeles, and New York.

B. Place a root enterprise CA in the Chicago office and issuing subordinate enterprise CAs in Chicago, Detroit, Los Angeles, and New York

C. Place a root standalone CA in the Chicago office and issuing subordinate enterprise CAs in Detroit, Los Angeles, and New York.

D. Configure certificate templates for autoenrollment.

E. Configure cross-certification between the willowbridge.com domain and the bilco.com domain

F. Configure certificate templates for manual enrollment.

Answer: B, D

Explanation: A root enterprise CA placed in Chicago and issuing subordinate CAs in all the locations will result in a minimization of WAN traffic, even in the event of a WAN failure. Autoenrollment of certificate templates will reduce PKI administrative requirements and will allow users and computers to be issued with certificates automatically, no user intervention. A PKI relies heavily on Active Directory information to determine the identity of the requester and for storage of certificate information. And enterprise CA is thus recommended especially since a large number of certificates will be enrolled and approved automatically. It is mentioned in the scenario:

1. The Willow Bridge, Ltd. PKI should be tightly integrated with Active Directory

2. All solutions must ensure that WAN traffic is kept to a minimum.

3. Certificates should be distributed to network users.

These certificates should not require user intervention.

Incorrect Answers:

A: You should also place an issuing subordinate enterprise CA in the Chicago office as this will reduce WAN traffic considerably, especially in the case of WAN failure. If the WAN link fails then the Chicago users' requests will not be fulfilled.

C: You should not deploy a root standalone CA because it is not integrated with Active Directory and one of the requirements states that it must be tightly integrated with Active Directory. Standalone CAs does not support V2 certificate templates, and therefore will not support autoenrollment which is another requirement since certificates should be issued without requiring user intervention.

E: Configuring cross-certification between the willowbridge.com domain and the bilco.com domain will not address the requirements stated.

F: Manual enrollment goes hand-in-hand with standalone CAs. You cannot configure autoenrollment as standalone CAs do not offer support and will require user intervention.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris & Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 3, p. 186

---

### **QUESTION 7**

You need to design a patch management strategy for Willow Bridge, Ltd. Take care that you solutions meet the requirements.

What should you do?

A. Create a test network representing a SUS server and all types of computers to be found in the production environment in all the offices.

Test all updates in the test networks and approve the appropriate updates.

Deploy a SUS server in each office.

Use Group Policy to configure network computers to download approved updates from their local SUS servers.

B. Deploy a SUS server in Chicago and a child SUS server in New York, Los Angeles and Detroit and configure each SUS server to connect to the official Microsoft Windows Updates Web site and download updates.

Test all updates in the test network and approve the appropriate updates on the parent SUS server for distribution to the child SUS servers at the other offices.

Configure the child SUS servers to receive updates from the parent SUS server.

Use Group Policy to configure network computers to download approved updates from their local SUS servers.

C. Create a test network representing a SUS server and all types of computers to be found in the production environment in the Chicago office.

Test all updates in the test network and approve the appropriate updates on the parent SUS server for distribution to the child SUS servers at the other offices.

Configure the child SUS servers to receive updates from the parent SUS server.

Use Group Policy to configure network computers to download approved updates from their local SUS servers.

D. Create a test network representing a SUS server and all types of computers to be found in the production environment in the Chicago office.

Test all updates in the test network and approve the appropriate updates on the parent SUS server for distribution to the child SUS servers at the other offices.  
Configure the child SUS servers to receive updates from the parent SUS server.  
Use Group Policy to configure network computers to receive the list of approved updates from their local SUS servers and download these updates from the official Microsoft Windows Updates Web site.

Answer: C

Explanation: In the Scenario it is stated that:

1. All solutions must ensure that WAN traffic is kept to a minimum.
2. Security updates and patches are to be deployed in a centralized, efficient manner that minimizes traffic over WAN connections.
3. We also want to be able to ascertain which security patches have been applied to client computers.
4. We want to enable all client computers automatically update themselves.
5. We need to make sure that our patch management system must support compatibility testing of all updates before the updates are deployed to the production network.
6. All security patches must be tested and approved by the IT department in the Chicago office.
7. We need to deploy security patches efficiently.

Thus you should create a test network representing a SUS server and all types of computers to be found in the production environment in the Chicago office. Then test all updates in the test network and approve the appropriate updates on the parent SUS server for distribution to the child SUS servers at the other offices. The child SUS servers must then be configured to receive updates from the parent SUS server. Use Group Policy to configure network computers to download approved updates from their local SUS servers to ascertain which security patches have been applied to client computers.

Incorrect Answers:

A: Setting up test environments in each office will result in a decentralized patch management and the scenario states a desire for centralized control over patch management. There is also the added problem of increased WAN traffic.

B: The deployment of SUS server in Chicago and a child SUS server in New York, Los Angeles and Detroit and configure each SUS server to connect to the official Microsoft Windows Updates Web site and download updates makes the rest of the option obsolete. Since the requirements states that you need to ensure that updates should be installed in a timely manner and this will not ensure that each office will keep up to date and distribute tested and approved updates.

D:

Using Group Policy to configure network computers to receive the list of approved updates from their local SUS servers and download these updates from the official Microsoft Windows Updates Web site will result in each of the local SUS servers connecting to the Internet to download updates, albeit a list a approved updates, and this will violate the one requirement that all solutions should minimize WAN traffic.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris & Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 2, p. 140

---

**QUESTION 8**

You need to identify which security patches are missing on the Willow Bridge, Ltd. client computers.

What should you do?

- A. Use the qchain.exe command.
- B. Use the qfecheck.exe command
- C. Use the Microsoft Baseline Security Analyzer (MBSA) utility.
- D. Use the Resultant Set of Policies (RSOP) utility.
- E. Use the Security Configuration and Analysis utility.

Answer: C

Explanation: MBSA is a GUI-based tool used to perform centrally executed scans and to identify common security configuration errors. It is useful to run MBSA as part of the patch management to scan for missing security updates which is a requirement in this scenario. MBSA included the mbsacli.exe command line interface tool which makes it possible to generate individual security reports for each computer that it scans.

Incorrect Answers:

A: The qchain command is used to install multiple patches in series; it is not used to check for missing security patches.

B: The qfechain command is used to track and verify patches that have been installed on Windows 2000 computers only. This is not suitable in this scenario to check for missing updates.

D: RSOP displays settings for a user or computer. In planning mode this tool will analyze planned changes to Group Policy settings. Whether in planning mode or not, it cannot be used to identify missing security patches.

E:

The Security Configuration and Analysis tool is used to check security settings against a custom security template; it is not used to identify missing security patches.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris & Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 2, p. 140

---

**QUESTION 9**

You need to design an access control strategy for the Willow Bridge, Ltd. internal DNS zone file. Take care in your solution to meet the requirements.

What should you do?

- A. Enable secure dynamic updates on the willowbridge.com zone.
- B. Enable secure dynamic updates on the local.willowbridge.com zone.
- C. Convert local.willowbridge.com to an Active Directory-integrated zone then enable secure dynamic updates for the zone.

D. Convert willowbridge.com to an Active Directory-integrated zone then enable secure dynamic updates for the zone.

Answer: C

Explanation: You need to convert local.willowbridge.com to an Active Directory-integrated zone then enable secure dynamic updates for the zone. Active Directory-integrated zone files are stored in the Active Directory database and are replicated during normal directory replication. It will also allow for secure dynamic updates by restricting DNS zone dynamic updates only to computers that are authenticated and joined to the Active Directory domain where the DNS server is located. It will thus prevent unauthenticated computers from creating source records.

1. DNS1 is used to provide host name resolution services for the internal network clients and will host the standard primary zone local.willowbridge.com. DNS1 is located on the internal network in the Chicago office.

2. We need to ensure that both DNS1 and DNS2 are protected against this accidental modification

Incorrect Answers:

A:

You first need to convert the zone to an Active Directory-integrated zone. Because at this stage the local.willowbridge.com zone is a primary DNS zone, which will not allow for support for secure Dynamic DNS (SDDNS). Besides you should not allow externally available zones to be stored in the Active Directory or configured to support dynamic updates.

B: You first need to convert the zone to an Active Directory-integrated zone. Because at this stage the local.willowbridge.com zone is a primary DNS zone, which will not allow for support for secure Dynamic DNS (SDDNS).

D: The internal DNS zone is hosted by the DNS1 server which is located on the local.willowbridge.com zone and not willowbridge.com.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris & Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 9 & 10, pp. 565, 642-645

---

### **QUESTION 10**

You need to design an access control strategy to prevent unauthorized users from modifying the registry on the DNS servers.

What should you do?

A. Change the RestrictAnonymous registry subkey from 0 to 1 or 2.

B. Ensure that DNS1 and DNS2 have to correct permissions set on the WINREG subkey for all groups.

C. Create a Domain Local group and add unauthorized users in this group on DNS1 and DNS2.

D. Remove the Domain Users group from the Remote Desktop users group on DNS1 and DNS2.

Answer: B

Explanation: The WINREG subkey controls the users and groups that can connect remotely to the computer and modify its registry settings. If the key has been deleted then all users can connect remotely and modify the registry settings. By default the Administrators group has Allow-Full Control permission for this subkey. The Backup Operators group has Allow-Read permission. This is what is required for the proper administration of the server.

1. We need to ensure that both DNS1 and DNS2 are protected against this accidental modification.
2. I want to see only administrators able to remotely connect to DNS1 and DNS2 to modify the registry settings.
3. I also want to have the ability to detect all attempts to log on interactively to either of these servers."

Incorrect Answers:

A: The RestrictAnonymous registry subkey is used to restrict anonymous users from displaying lists of users and their security permissions on the computer. This setting whether set to 1 or 2; will not affect the ability to connect remotely to a computer to modify its registry.

C: In AGDLP, the recommended way to assign permissions to a resource, user accounts are added to global groups, and then global groups are added to Domain Local groups. Permissions or user rights assignments are finally assigned to the Domain Local group. Regardless: in this scenario you want to prevent unauthorized users from modifying the registry. Thus this option is incorrect.

D: The Remote Desktop Users group is able to create Remote Desktop connections to the local computer. Usually this group is not populated and members of the local Administrators group can access the computer via Remote Desktop connection. It is mentioned in the case study:

1. DNS1 and DNS2 are both configured with the default remote Desktop connection settings.

Thus the Domain Users group is not a default member of the Remote Desktop Users group. This option is thus not correct.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris & Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 8, p. 454

---

### **QUESTION 11**

You need to test the remote access security solutions. To this end in the test environment in the Chicago office, you install an IAS server on TestRAS1. After RADIUS clients have been configured appropriately, users in the test environment who attempt to connect via TestVPN1 are not authenticated. You need to address this issue for deployment to the production network. You thus need to ensure that all Testdomain user accounts are authenticated using the IAS on TestRAS1. What should you do?

- A. Upgrade TestRAS1 to domain controller.
- B. Upgrade both TestRAS1 and TestVPN1 to domain controllers.
- C. Add TestRAS1 to the RAS and IAS Servers group in Active Directory.
- D. Add TestRAS1 and TestVPN1 to the RAS and IAS Servers group in Active Directory.

Answer: C

Explanation: Given that the RADIUS clients have been configured appropriately, you need to ensure that the RADIUS server is properly configured. For TestRAS1 to be able to perform authentication, it must have permission to read the attributes from the user object in Active Directory. By default this permission is not granted when RAS/IAS is installed on a member server. This permission is assigned when you add the server, in this case, TestRAS1 to the built-in RAS and IAS Servers security group.

Incorrect Answers:

- A: In the production environment, RAS1 is not a domain controller. This will make the test invalid.
- B: The test results would be invalid. Besides if TestRas1 were to be upgraded to domain controller status then you will add additional security concerns to the design.
- D: This will be obsolete since you only require the IAS server to access user attributes in Active Directory. There is no need to add TestVPN also to the RAS and IAS Servers group in Active Directory.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 6, pp. 369-370  
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 335

## Topic 4, Stanford Finance, Scenario

### Background

Stanford Finance is an international company that specializes in the provision of investment and financial services for its clients. Stanford Finance operates across two continents, namely Europe and North America.

### Physical Locations

The Stanford Finance head quarters are located in New York and branch offices in Chicago, USA; London, England; and Milan, Italy.

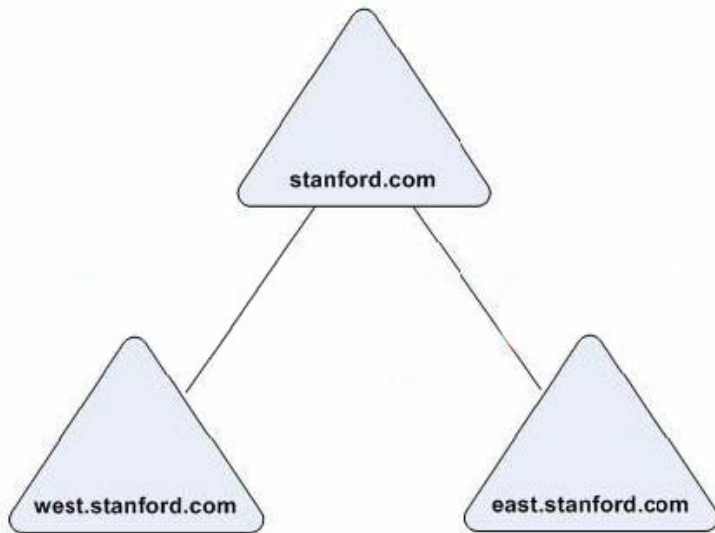
### Directory Services

Currently the Stanford Finance Active Directory infrastructure is as follows:

The network consists of a single Active Directory forest. The forest contains three domains named stanford.com, west.stanford.com, and east.stanford.com respectively.

The functional level of the forest is set at Windows Server 2003. The Active Directory Infrastructure exhibit illustrates the current Active Directory infrastructure.

### Active Directory Infrastructure



### Web Services

The Stanford Finance web presence is provided by two Web sites that are hosted by using Internet Information Services (IIS) 6.0.

1. The one site is a secure Web site that is accessed by the employees to store and update customer records. This site is also accessed by customers to make use of the on-line services that are offered to them. All users who want to gain access to the resources on this secure Web site must connect to the domain and be authenticated.
2. The other Web site is a public site that provides general information regarding the company. This site is accessible to any Internet user. They are not required to log in.

### Organizational Unit (OU) Hierarchy

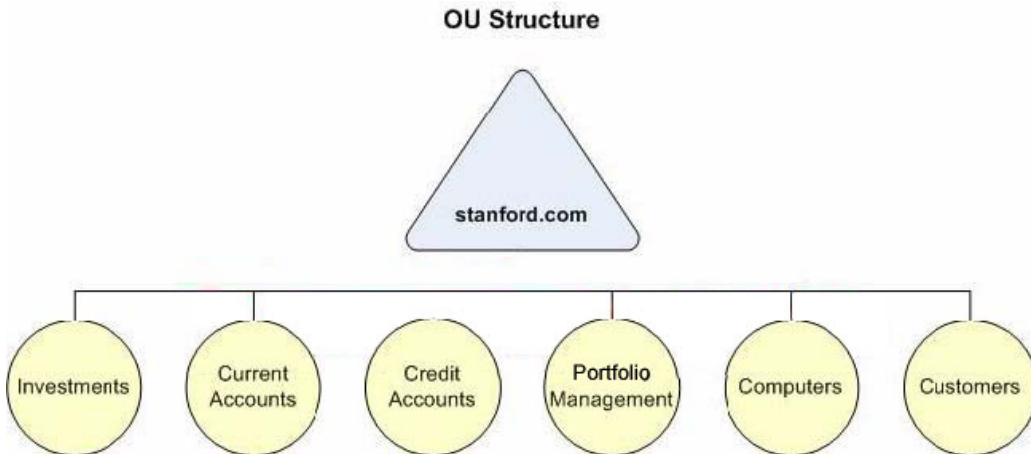
There are four top-level Organizational Units (OUs) - these are used to organize the Stanford Finance departments such as: Investments, Current Accounts, Credit Accounts,

### Portfolio Management.

There are two further top-level OUs namely Computers and Customers.

1. The Computers OU contains all the Stanford Finance desktop computer accounts.
2. The Customers OU contains all the user accounts that have been created for the Stanford Finance customers as well as the computer accounts for the users' laptop computers.

The OU structure of the Stanford Finance network is shown in the OU Structure exhibit.



### **Network Infrastructure**

#### **Connectivity:**

The local area network (LAN) at each of the offices is running at 512 Kbps. Each of the offices is connected to the head quarters via a T3 connection. The New York office is connected to the Internet and the other offices connects to the Internet through the New York office.

#### **Servers and workstations:**

All Stanford Finance servers run Microsoft Windows Server 2003.

All Stanford Finance client computers run Microsoft Windows 98, Microsoft Windows NT Workstation 4.0, Microsoft Windows 2000 Professional, and Microsoft Windows XP Professional; with the Chicago- and New York offices running Windows XP Professional. All servers and client computers are members of the domain.

#### **Each office contains:**

1. a minimum of two domain controllers
2. a file server that is used to store all confidential customer data
3. an on-site IT department that performs desktop maintenance and troubleshooting tasks

The New York office contains:

A Central IT department that performs all server-level operations remotely

Backup strategy:

At present the Stanford Finance backup strategy is as follows:

1. A full data backup on all servers on a weekly basis.
2. Differential backups on most servers twice a week.
3. Daily backups on some file servers that store frequently changed data files.

#### **Planned Changes**

Stanford Finance is entering into a joint venture with Willow Bridge, Ltd., which operates as a worldwide asset management company. The Willow Bridge, Ltd., network consists of a single Windows 2000 Active Directory domain. There are currently no plans that involve the upgrading of the Willow Bridge, Ltd., servers to Windows Server 2003. The Internet will be used as the medium of communication and collaboration between Stanford Finance and Willow Bridge, Ltd., A Shared folder named Customer Data will be located on a Stanford Finance Web server that is located on the internal network.

Customer Data will be used by both companies.

Access to all resources' integrity and security should be ensured. Thus only authorized users should have access. In the budget provision will be made for the purchase of equipment that will support the user of smart cards for authorized users. There are no additional funds for IT infrastructure upgrades except for the fact that all Stanford Finance client computers in Milan will be upgraded to Windows XP Professional in the next fiscal year. The IT department must maximize the existing hardware and software to meet the security requirements.

### **Problem Statements**

The following business problems must be considered:

1. It is difficult to maintain all client computers with the latest security patches. Security patches must be installed by using the minimum amount of WAN bandwidth.
2. The information technology (IT) department in each office must test security patches before deploying them to client computers.
3. All users who remotely connect to the network should do so using a smart card. A personal identification number (PIN) should be required to prevent unauthorized use of a lost or stolen card.
4. In the case of Stanford Finance users logging on to the network using different computers, their user credential must never be stored on the local computer and should never be exposed to other users.
5. Unauthorized users have modified the registry on some servers. Unauthorized users must not be able to modify the registry on company servers.
6. Access to resources is assigned per user, which causes administrative overhead. This administrative overhead must be reduced.
7. Stanford Finance offers online services that must be available to customers and the partner company, Willow Bridge, Ltd., on a twenty four hour basis. Access to Customer Data in the New York office must be available to the Willow Bridge, Ltd., users as well.
8. Stanford Finance is in a joint venture with Willow Bridge Ltd to provide investment and asset management services for customers. Willow Bridge, Ltd., users have access to the extranet in the New York office. These users need to be able to access Customer Data that is located on a file server in the New York internal network.
9. Users from Willow Bridge, Ltd., require access to information stored on a Microsoft SQL Server 2000 computer that is located on the New York internal network. Users on the internal network must also be able to access the information on the SQL Server by using Microsoft Access 2000.

### **Chief Information Officer (CIO) problem statement**

"Before the joint venture our focus has been to prevent external threats. With the joint venture we find ourselves in, we need to prevent internal threats as well. It was brought to our attention that recently confidential customer information was released to the public. In addition I have a further suspicion that unauthorized users are attempting to delete or modify files. From time to time we need to review who has access to company resources. We need to make use of our infrastructure's security features to meet our security needs so as to avoid unnecessary expenses."

"Most customer data should be retained on Customer Data for a minimum period of three

months, after which it will be stored on tape for a further three years. The three month period is to accommodate all customers to make use of our on-line service to track their investments.

All customer records that are retained on-line compel us to retain any audit logs that detail user access to this data for as long as the data is kept on line. This means that all Web access information should be retained for a minimum of three months. Server event logs that document other network resource access must thus also be retained."

"This also means that we should reduce storage costs. To this end we should plan the data retention strategy so that only the minimum number of backup tapes is kept."

**IT administrator problem statement:**

"We currently have a situation where all users, including our customers who have authorized access, download their security updates from the official Microsoft Windows Update Web site. This results in an inconsistent deployment of security patches. Only some customers install the required security patches, while most of the Stanford Finance users install security patches when instructed to do so by their respective office IT departments. There should be a real concern regarding a fact that a remote user will fail to keep up to date with critical security patches and in this way introduce a virus that could exploit this vulnerability into the Stanford Finance network."

"Before security patches are deployed, all domain computers must first be examined for security configuration errors and missing security patches. This type of analysis should be performed as a routine until we are confident in the new patch management system."

**Written Security Policy**

Following is a list of the requirements that must be met by the Stanford Finance written security policy:

1. All customer information must be kept confidential.
2. All access to customer information must be tracked.
3. The public Web site is to be used for marketing information and service offering literature. Stanford Finance must track unauthorized modification of the marketing information only.
4. Management must be able to access company financial information that is stored in Microsoft SQL Server 2000 databases and in shared folders.
5. All e-mail messages sent between Stanford Finance and Willow Bridge, Ltd., must be encrypted.
6. Authorized users must make use of smart cards and PINs to access company resources.
7. All users must be responsible for their own smart card and PIN.
8. All content updates to the Web server must be protected from interception.
9. An encrypted channel must be used when remote server administration is being conducted.
10. No perimeter network servers may be accessed via Remote Desktop for Administration.

**Topic 4, Stanford Finance. (10 Questions)**

---

**QUESTION 1**

You need to design a smart card issuance system that will meet the Stanford Finance security requirements. You need to take certain steps in the design to issue the smart cards.

What should you do?

A. All smart card recipients will receive their smart cards via certified mail to their primary address.

Smart card recipients should present a Stanford Finance bill or correspondence as proof of identity.

A complex PIN in a sealed security envelope must be issued to each smart card holder.

B. All smart card recipients must, in person, sign a security agreement when issued the smart cards at the Stanford Finance offices.

Smart card recipients should present two forms of identification: one should have a photo.

A temporary PIN must be issued to each smart card holder which must be changed during the card-issuance process.

C. All smart card recipients must register online before a smart card is issued via registered mail to their primary address.

A temporary PIN must be issued online to each smart card holder which must be changed when the recipient receives the card.

D. Smart card recipients should present at least a Stanford Finance bill or correspondence as form of identification.

All recipients should register for their smart cards by providing detailed information using the Web-based application form.

A complex PIN must be issued to each smart card recipient.

Answer: B

Explanation: Using smart cards and two-factor authentication will provide added security to the authentication process for the remote users. Each recipient should actually go to the Stanford offices in person, with two types of identification, one which is at least a government issued identity document that has photo identification. There they should sign a security agreement when receiving a temporary PIN. This temporary Pin must be used by the recipient at a Smart Card Enrollment station to immediately establish a new private PIN. Thus no Stanford Finance employee will have access to a recipient's PIN which makes the recipient fully responsible for the security of the new PIN.

1. Authorized users must make use of smart cards and PINs to access company resources.

2. All users must be responsible for their own smart card and PIN.

Incorrect Answers:

A: Mailing smart cards is not recommended, even if the mail is certified. This will definitely violate the security requirements. Using a Stanford Finance bill does not provide the required level of security.

C: Recipients should not be allowed to register online as a form of identification. This can be risky. Further allowing the Stanford Finance employee to establish the PIN online albeit temporary adds additional risk to the number of individuals who have access to the

PIN. And it also reduces the recipient's responsibility for smart card security.

D: Making use of complex PINs in sealed security envelopes will make it difficult for the PIN to be stolen, but this would not be user friendly. It may require some recipients to write it down which makes it vulnerable to compromise. This option is akin to registering online which should not be allowed.

---

## **QUESTION 2**

You need to design an access control strategy for resources that are located in the intranet for Willow Bridge, Ltd., and Stanford Finance users, whilst ensuring that your solution meet business and security requirements.

What should you do?

- A. Create a new child domain named intranet.west.stanford.com in the existing forest. Create user accounts for Willow Bridge, Ltd., users in the new child domain. Create shortcut trusts in which the child domain trusts every domain in the forest.
- B. Create a new forest and domain named intranet.stanford.com. Create user accounts for Willow Bridge, Ltd., users in the new domain. Create a one-way forest trust relationship in which the intranet.stanford.com trusts the willowbridge.com domain.
- C. Create a new forest and domain named intranet.stanford.com. Create user accounts for Willow Bridge, Ltd., users in the new domain. Create an external trust relationship in which the intranet domain trusts the west.stanford.com domain.
- D. Create a child domain of the west.stanford.com domain for the intranet. Create user accounts for Willow Bridge, Ltd., users in the new child domain. Create an external trust relationship in which the forest root domain trusts the intranet domain.

Answer: B

Explanation: Windows Server 2003 allows trust relationships between separate Active Directory forests. Forest trusts act much like domain trusts, except that they extend to every domain in two forests. Domains are connected to one another through logical structure relationships. The relationships are implemented through domain trees and domain forests.

A domain tree is a hierarchical organization of domains in a single, contiguous namespace. In the Active Directory, a tree is a hierarchy of domains that are connected to each other through a series of trust relationships (logical links that combine two or more domains into a single administrative unit). The advantage of using trust relationships between domains is that they allow users in one domain to access resources in another domain, assuming the users have the proper access rights.

A forest is a set of trees that does not form a contiguous namespace. For example, you might have a forest if your company merged with another company. With a forest, you could each maintain a separate corporate identity through your namespace, but share information across Active Directory.

1. Stanford Finance offers online services that must be available to customers and the

partner company, Willow Bridge, Ltd., on a twenty four hour basis.

2. Stanford Finance is in a joint venture with Willow Bridge Ltd to provide investment and asset management services for customers. Willow Bridge, Ltd., users have access to the extranet in the New York office. These users need to be able to access Customer Data that is located on a file server in the New York internal network.

3. Users from Willow Bridge, Ltd., require access to information stored on a Microsoft SQL Server 2000 computer that is located on the New York internal network. Users on the internal network must also be able to access the information on the SQL Server by using Microsoft Access 2000.

Thus you would design your access control strategy by creating intranet.stanford.com, a new forest and domain. After which you create user accounts for the users from the partner companies in the new domain and then create a one-way forest trust relationship in which the intranet forest trusts the company forest.

Incorrect Answers:

A: Child domains are not required. And shortcut trusts will not meet business and security requirements. What is required is a new forest and domain and a one-way trust in which the intranet forest trusts the company forest.

C: An external trust relationship is unnecessarily risky and will not comply with security requirements.

D: Child domains are not required. And shortcut trusts will not meet business and security requirements. What is required is a new forest and domain and a one-way trust in which the intranet forest trusts the company forest. Also, an external trust relationship is unnecessarily risky and will not comply with security requirements.

---

### **QUESTION 3**

You need to design an access control strategy that meets business and security requirements, whilst ensuring that your solution minimize forest-wide replication. What should you do?

A. A global group per department and a global group per location must be created.

Add users to their respective departmental groups as members.

Place the departmental global groups within the location global groups.

Assign the location global groups to file and printer resources in their respective domains, and then use the location global groups to assign permissions for the file and printer resources.

B. A global group per department must be created. Add users in their respective global groups.

Create domain local groups for file and printer resources.

Add the global groups to the respective domain local groups.

Then use the domain local groups to assign permissions to the file and printer resources.

C. A local group on each server must be created.

Then add the authorized users as members.

Then use the local groups to assign appropriate permissions for the file and printer resources.

D. Create A universal group per location must be created.

Then add the respective users as members.

Assign the universal groups to file and printer resources.  
Then use the universal groups to assign permissions.

Answer: B

Explanation: A global group is a type of group used to organize users who have similar network access requirements. It is simply a container of users and global groups (in native mode) from the local domain.

Domain local groups are used to assign permissions to resources. Domain local groups can contain user accounts, universal groups, and global groups from any domain in the tree or forest. A domain local group can also contain other domain local groups from its own local domain. Microsoft recommends that global groups be added to domain local groups in a single domain environment and that universal groups are added to the domain local group in a multi-domain environment. You would need to make use of a global group for each department and add the respective users as its members, create domain local groups for file and printer resources. After which you should add the global groups to the respective domain local groups and then assign permissions using the domain local groups for the different resources. This should comply with security requirements while servicing business operational requirements.

1. All customer information must be kept confidential.
  2. All access to customer information must be tracked.
  3. We must use our existing infrastructure's security features to meet our security needs.
- Also, we suspect that unauthorized users are attempting to delete files. Therefore, we need to review which users have access to company resources from time to time.

Incorrect Answers:

A: This option will result in unnecessary replication taking place.

C: A local group is a group that is stored on the local computer's accounts database. This is not the answer in this scenario.

D: Creating universal groups would be creating a special type of group used to logically organize global groups and appear in the Global Catalog (a search engine that contains limited information about every object in the Active Directory). Universal groups can contain users (not recommended) from anywhere in the domain tree or forest, other universal groups, and global groups. This will obviously result in forest wide replication which should be kept to a minimum.

---

#### **QUESTION 4**

You need to design a method to encrypt confidential data whilst ensuring that your solution address the concerns of the chief information officer.

What should you do?

- A. Customer information must be encrypted when it is stored and when it is being transmitted.
- B. Only encrypted connections to the public Web site, which is hosted on the Web server on the perimeter network, must be allowed.
- C. All marketing information on file servers and client computers must be encrypted.
- D. Allow only encrypted connections to all file servers.

Answer: A

Explanation: The Chief information officer is concerned about customer data that is leaked to the public. You thus need to encrypt this information when stored as well as when it is being transmitted.

1. It was brought to our attention that recently confidential customer information was released to the public. In addition I have a further suspicion that unauthorized users are attempting to delete or modify files. From time to time we need to review who has access to company resources. We need to make use of our infrastructure's security features to meet our security needs so as to avoid unnecessary expenses.

Incorrect Answers:

B: Encrypted connections to the public Web site hosted on the Web server on the perimeter network will not work in this scenario.

C: You need to keep the customer information confidential. Marketing information is for public consumption. "The public Web site is to be used for marketing information and service offering literature. Stanford Finance must track unauthorized modification of the marketing information only."

D: Encrypted connections to all the file servers will also render information other than the confidential data encrypted. This is not what is needed.

---

### **QUESTION 5**

You need to design a method to update the content on the Web server whilst ensuring that your solution meet business and security requirements.

What should you do? (Each correct answer presents a complete solution. Choose TWO.)

A. Use SSH to encrypt content as it is transferred to the Web server on the perimeter network.

B. Install the Microsoft FrontPage Server Extensions, and use FrontPage to update content.

C. Use Web Distributed Authoring and Versioning (WebDAV) over SSL connection to the Web server to update content.

D. Use FTP over an IPSec connection to transfer content to the Web server.

E. Use Telnet to connect to the Web server, and then perform content changes directly on the server.

Answer: C, D

Explanation:

C: WebDAV is a file sharing protocol that is commonly used in Windows Internet-related applications. It is a secure file transfer protocol over intranets and the Internet. You can download, upload, and manage files on remote computers across the Internet and intranets using WebDAV. WebDAV is similar to FTP. WebDAV always uses password security and data encryption on file transfers (FTP does not support these tasks). Thus making use of WebDAV over SSL connection should comply with the

company's security requirements.

D: The File Transfer Protocol (FTP) is a valuable component of IIS 6.0. FTP is used to "swap" or "share" files between servers and clients. This could be dangerous practice for businesses with sensitive information. Most large organization firewalls will block FTP access. We need to implement FTP communication over a secure channel like VPN. VPNs use the Point-to-Point Tunneling Protocol (PPTP) or Secure Internet Protocol (IPSec) to encrypt data and facilitate secure FTP communication. We can also use SSL encryption on WebDAV supported directories for the same purpose.

Incorrect Answers:

A: SSH is independent of the operating system and is therefore suitable for use in a mixed operating system environment. However, not all terminal concentrators provide built-in security functions, so you'll need to consult with the vendor's documentation to see what, if any, security is provided. Thus this option is a security risk.

B: Making use of Microsoft FrontPage Server Extensions and updating the content with FrontPage will not comply with security requirements.

E: You should enable the Telnet service only if you see a real need for it, especially since the other administrative tools at your disposal offer more features and far better security. The Telnet service should remain disabled unless a need arises that requires it. In this instance it would be unnecessary.

---

### **QUESTION 6**

You need to design a monitoring strategy for the folders that contain confidential customer information, in the Customer Data folder to support the new data retention strategy.

What should you do?

A. Audit success and failures for object access on the folders that contain customer information, in the Customer Data folder.

B. Audit failure of object access on only the Customer Data folder.

C.

Enable auditing on only the Customer Data folder using the Security Configuration and Analysis tool.

D. Audit directory access failures.

E. Analyze security on Customer data by running Microsoft Security Baseline Analyzer (MBSA).

Answer: A

Explanation: The data retention strategy must be configured to store user information and network data. To support this strategy you need to monitor and log all access to Customer Data and you need to maintain the log files that detail this access for future reference. Thus you should enable Audit failure of object access on only the Customer Data folder. If enabled the Audit object access setting triggers auditing of user access to objects such as files, folders, Registry keys, and so forth. As with the other audit policies, you can either monitor the success or failure of these actions.

1. All customer information must be kept confidential.
2. All access to customer information must be tracked.

Incorrect Answers:

B: Auditing failure of object access only will only constitute half of the tracking that is required as stated in the Stanford Finance written security policy.

C: The Security Configuration and Analysis tool is used to analyze and to help configure a computer's local security settings. This is not the same as tracking all access to the Customer data folders and subfolders.

D: Auditing directory access failures will not work in this scenario where more is expected.

E: MBSA is a GUI-based tool used to perform centrally executed scans and to identify common security configuration errors. However, while it is useful to run MBSA as part of the patch management, it is not required for data retention.

## QUESTION 7

### DRAG DROP

You must create a data retention plan for the Stanford Finance file servers that contain the customer data. In your solution you need to make use of the existing disaster recovery plan backup tapes.

What should you do? (To answer choose the appropriate option and place it in the corresponding work area.)

| Backup Options, select from these                                                          |  |  | Work Area, place here        |
|--------------------------------------------------------------------------------------------|--|--|------------------------------|
| <b>Backup Type:</b><br><div>Incremental</div> <div>Differential</div> <div>Full</div>      |  |  | <div>Backup Type.</div>      |
| <b>Backup Frequency</b><br><div>Daily</div> <div>Weekly</div> <div>Monthly</div>           |  |  | <div>Backup Frequency.</div> |
| <b>Retention Period:</b><br><div>13 months</div> <div>26 months</div> <div>39 months</div> |  |  | <div>Retention Period.</div> |

Answer:

| Backup Options, select from these                                                 |  |  | Work Area, place here |
|-----------------------------------------------------------------------------------|--|--|-----------------------|
| <b>Backup Type:</b><br><div>Incremental</div> <div>Differential</div> <div></div> |  |  | <div>Full</div>       |
| <b>Backup Frequency</b><br><div>Daily</div> <div>Weekly</div> <div></div>         |  |  | <div>Monthly</div>    |
| <b>Retention Period:</b><br><div>13 months</div> <div>26 months</div> <div></div> |  |  | <div>39 months</div>  |

Explanation:

You need to retain a full backup set per server each month and retain these backup sets for three years and three months. As part of the current disaster recovery plan, Stanford

Finance performs a full backup each week in conjunction with incremental or differential backup sets. In addition to this the CIO states that customer data should be retained for at least three months online and a further three years. This means that one full backup set each month will provide the monthly snapshot of customer data and will allow the data to be retained for the full period, as required. It will also meet the CIO's requirement regarding the use of the minimum amount of tapes. Weekly or daily will not meet this requirement.

You should not retain incremental or differential backup sets. While these tapes might be useful for restoring data after a loss, their usefulness expires after the next full backup set has been validated.

You should not retain the file server backup for either One year and One month or Two years and two months. The CIO states that the customer data must be retained for at least three months online and three years on tape. For adequate disaster recovery and data retention, backup tapes must be retained for the online period as well as the additional three year offline period.

### QUESTION 8

#### DRAG DROP

You need to create the new data retention plan.

What should you do? (To answer: choose the appropriate objects from the Data objects column and place them in the appropriate work area which depicts the Retention Duration. You may use the Data Object more than once where necessary.)

| Data Objects                                     | Retention Period, Place here |                     |                     |
|--------------------------------------------------|------------------------------|---------------------|---------------------|
|                                                  | One Month                    | Three Months        | 3 Years, 3 Months   |
| Retain Domain Controller system state backups.   |                              |                     |                     |
| Retain Customer files online.                    | Place here.                  | Place here.         | Place here.         |
| Retain Web server access logs online.            | Place here, if any.          | Place here, if any. | Place here, if any. |
| Retain Customer data on backup tape.             | Place here, if any.          | Place here, if any. | Place here, if any. |
| Retain Staff e-mail transactions online.         | Place here, if any.          | Place here, if any. | Place here, if any. |
| Retain Domain Controller event logs online.      | Place here, if any.          | Place here, if any. | Place here, if any. |
| Retain Member Server event logs online.          | Place here, if any.          | Place here, if any. | Place here, if any. |
| Retain Staff e-mail transactions on backup tape. | Place here, if any.          | Place here, if any. | Place here, if any. |

Answer:

| Data Objects                                     | Retention Period, Place here |                                             |                                                  |
|--------------------------------------------------|------------------------------|---------------------------------------------|--------------------------------------------------|
|                                                  | One Month                    | Three Months                                | 3 Years, 3 Months                                |
| Retain Domain Controller system state backups.   |                              |                                             |                                                  |
| Retain Customer files online.                    | Place here.                  | Retain Domain Controller event logs online. | Retain Customer data on backup tape.             |
| Retain Web server access logs online.            | Place here, if any.          | Retain Member Server event logs online.     | Retain Staff e-mail transactions on backup tape. |
| Retain Customer data on backup tape.             | Place here, if any.          | Retain Customer files online.               | Place here, if any.                              |
| Retain Staff e-mail transactions online.         | Place here, if any.          | Retain Staff e-mail transactions online.    | Place here, if any.                              |
| Retain Domain Controller event logs online.      | Place here, if any.          | Retain Web server access logs online.       | Place here, if any.                              |
| Retain Member Server event logs online.          | Place here, if any.          | Place here, if any.                         | Place here, if any.                              |
| Retain Staff e-mail transactions on backup tape. | Place here, if any.          | Place here, if any.                         | Place here, if any.                              |

**Explanation:**

Regarding the CIO's problem statement: Web server access, domain controller event logs, member server event logs and customer data should be retained online for three months. This is the minimum period specified. You are not required to maintain these data sets offline after the three month online period.

There is no requirement that stated that domain controller system state backups, except as part of the normal disaster recovery plan, should be retained for one month.

All customer files and e-mail transactions must be retained on backup tape for the full three year and three month period. It must also be backed up to tape each week, and the backup tapes should be retained for an additional three years beyond the online period. Because staff e-mails may contain confidential details, they must be retained for the same period as customer data.

**QUESTION 9**

Which authentication method should be employed to provide for the desired level of security for customers who log on using portable computers?

- A. MS-CHAP v2.
- B. Two-factor authentication.
- C. IPSec authentication.
- D. 802.1x authentication.

Answer: B

Explanation: When two-factor authentication is implemented, users will be required to swipe smart card into a smart card reader and then enter a PIN to authenticate to the

computer. Before a smart card is used, the user's logon certificate, public key, and private key must be programmed on the smart card. You can program the smart card using a Smart Card Enrollment station, which is integrated with certificate services. You can use the EAP-TLS protocol for certificate and smart card authentication.

Incorrect Answers:

A: MS-CHAP v2 does not support smart cards and does not provide the required two-factor authentication.

C: IPsec is used to generate keys for encrypting data during PPTP and L2TP tunneling transmissions. It is not a user authentication protocol.

D: IEEE 802.1x authentication is a certificate-based standard that supports authenticated network access to wired Ethernet networks from 802.11 networks which is wireless. This method will provide support for centralized user identification, authentication, dynamic key management and accounting. This is ideal for wireless LAN implementations. But this is not the case in the Stanford Finance network.

---

### **QUESTION 10**

You need to implement a new patch management system. There are some steps that should be performed prior to the implementation of the new patch system.

What should you do?

- A. Run Microsoft Baseline Security Analyzer (MBSA) to poll network computers for vulnerabilities.
- B. Run Security Configuration and Analysis tool to check security settings against a custom security template.
- C. Run gpresult command on each domain controller and analyze the results.
- D. Run Resultant Set of Policy (RSOP) wizard in planning mode on the Computers OU

Answer: A

Explanation: MBSA is a GUI-based tool used to perform centrally executed scans and to identify common security configuration errors. It is useful to run MBSA as part of the patch management to scan for missing security updates which is a requirement in this scenario.

Incorrect Answers:

B: The Security Configuration and Analysis tool is used to check security settings against a custom security template; it is not used to identify missing security patches.

C: gpresult should not be used on a domain controller because it displays Group Policy settings for a user or computer.

D: RSOP displays settings for a user or computer. In planning mode this tool will analyze planned changes to Group Policy settings. Whether in planning mode or not, it cannot be used to identify missing security patches.

## **Topic 5, Bilco Engineering, Inc., Scenario**

### **Background**

Bilco Engineering, Inc. is one of the largest manufacturers of genuine quality approved

lumber products in North America.

### **Physical Locations**

Bilco Engineering, Inc. has its headquarters in Chicago. Bilco Engineering, Inc. maintains a milling facility and a retail office in Dallas which maintains a distribution facility.

Bilco Engineering, Inc. has eight retail offices in North America. Three of the Bilco Engineering, Inc. retail offices are located in St. Louis and three stores are located in Atlanta. Bilco Engineering, Inc. has recently acquired two new retail offices in Denver. Each retail office will have between 100 and 150 users.

### **Planned Changes**

The following planned changes will be made within the next three months:

1. A new retail office will be opened in Phoenix to support the two Denver retail offices the same way the Chicago office currently supports the North American retail offices
2. All servers and client computers will be upgraded to Windows Server 2003 and Windows XP Professional. Install and configure a new file server named BE-FS01
3. After the upgrade of the member servers and client computers in the Windows NT 4.0 domain, the domain will be migrated into Active Directory
4. All the retail offices will have several kiosks installed for authenticated users such as the consumers. The need for Wireless networking capability must be made to keep up with the upscale market. The consumers will be able to make wireless Internet connections

### **Business Process**

Bilco Engineering, Inc. has an Information Technology (IT) department located in Chicago. The IT department is responsible for operating the Bilco Engineering, Inc. Web, database and e-mail servers as well as client computers. The Bilco Engineering, Inc. IT department will periodically need to travel to remote retail offices to perform upgrades, installations and troubleshooting.

There will be at least one desktop support technician assigned for each retail office. The support technicians depending on experience will have administrative rights to server located in the North American retail offices.

The two new retail offices share a common Finance department. The Bilco Engineering, Inc. HR department maintains a Web application named Bilcobenefits.bilco.com providing confidential personalized information to each employee. The application characteristics are shown below:

1. The application makes use of ASP.NET and ADO.NET.
2. A Web server in Chicago hosts the application.
3. The application can be accessed by employees from work and home.

Bilco Engineering, Inc. has a public Web site named bilco.com that is maintained by the reservations department. The Web site Characteristics are shown below:

1. The Web site uses ASP.NET and ADO.NET.
2. The Web site is accessible from anywhere on the Internet.
3. Static content about each retail office is also included in the Web site.

### Directory Services

The Bilco Engineering, Inc. uses an Active Directory domain named bilco.com. The IT Department in Chicago will be responsible for administering the domain. The bilco.com domain will always remain the forest root domain.

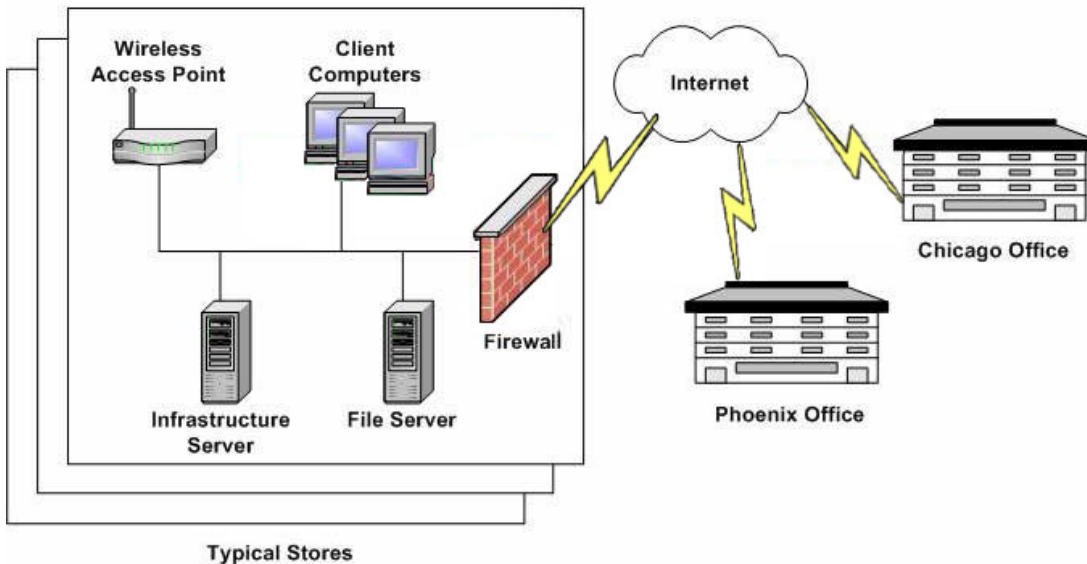
The Finance department of the two new retail offices has a Windows NT 4.0 domain named bilcoinc.com. The two retail offices each have contains a domain controller that runs Windows NT Server 4.0

The Bilco Engineering, Inc. network users have user accounts in Active Directory or in the Windows NT 4.0 domain.

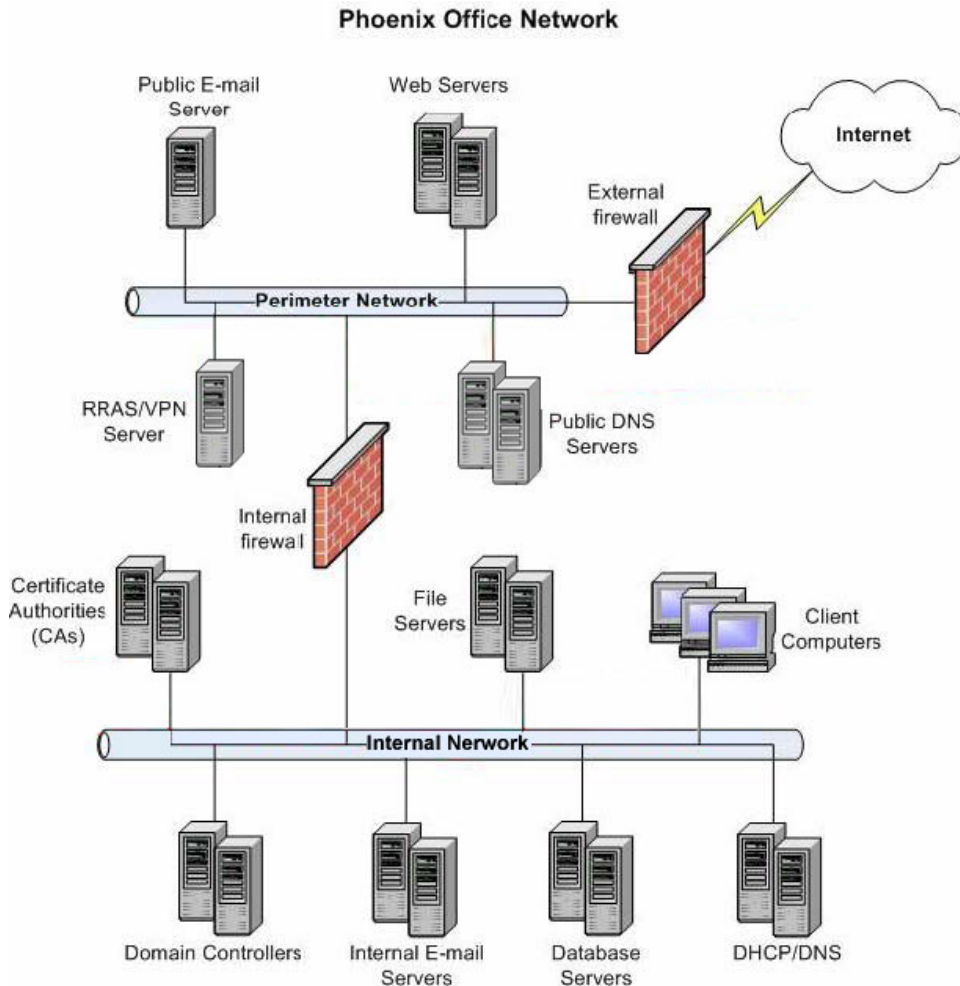
### Network Infrastructure

Bilco Engineering, Inc.'s existing locations and connections are shown in the Network Diagram exhibit.

**Network Diagram**



The Bilco Engineering, Inc. Phoenix office network configuration is shown in the Phoenix Office Network exhibit.



The Bilco Engineering, Inc. network servers all run Windows 2000 Server except the servers in the two new retail offices which run Windows NT Server 4.0. All client computers on the Bilco Engineering, Inc. network currently run Windows 2000 Professional.

All the Bilco Engineering, Inc. retail offices have one file server each and are connected by VPN's across the Internet. Bilco Engineering, Inc. has recently installed Wireless access points at each retail office for network use.

### **Chief Information Officer**

Bilco Engineering, Inc. considers their security of their corporate data as vitally important. Below are the properties configured:

1. Bilco Engineering, Inc. keeps a significant amount of customer information on file. Bilco Engineering, Inc. sees the data as an important corporate asset and should be protected.
  2. Bilco Engineering, Inc. requires all the public key infrastructure (PKI) certificates used to be trusted widely to ensure that consumers are not be required to perform additional actions to gain access to the Bilco Engineering, Inc. Web sites.
- Bilco Engineering, Inc. has insured that any violations against the policies of the network are made will be punished. Bilco Engineering, Inc. has established security policies and logging requirements for this purpose and the administrator is notified immediately in

order to respond quickly.

### **IT Manager**

The Bilco Engineering, Inc. IT manager wants to avoid using expensive dedicated WAN links so Bilco Engineering, Inc. will make use of VPNs instead. Bilco Engineering, Inc. also does not require the users to be able to download updates directly from the Internet. Bilco Engineering, Inc. requires having the routine administrative duties automated as on busy days not all important administrative tasks are completed. Bilco Engineering, Inc. IT Administration should have little manual overhead.

Bilco Engineering, Inc. must ensure that the network staff is not overwhelmed by the amount of log items showing regular actions like logging in and printing. Bilco Engineering, Inc. wants to ensure that nothing important will be missed.

Bilco Engineering, Inc. currently makes use of legacy applications at the retail offices to manage retail office functions by reading and writing a registry value which unauthorized users cannot access. Bilco Engineering, Inc. believes that the application will run properly if the users are made administrators on the client computer. Bilco Engineering, Inc. realizes that this move violates the company's written security policy.

### **Organizational Goals**

Bilco Engineering, Inc. requires having the organizational goal below taken into consideration:

1. Bilco Engineering, Inc. requires sharing information between retail offices. The retail customer's confidential information and Bilco Engineering, Inc. corporate data should be encrypted when it is stored and while it is in transit.

### **Written Security Policy**

Bilco Inc.'s written security policy includes the requirements below to be considered:

1. Bilco Engineering, Inc. requires security related actions performed by an administrator that affects company servers to be logged. Bilco Engineering, Inc. wants all the log files and a second administrator should audit the event.
2. Administrative permissions on client computers are to be allowed only to the IT staff at the retail offices to change other user's configurations. Bilco Engineering, Inc. requires the Kiosk computers to be more restrictive with certain desktop settings named the Kiosk Desktop Specification. Bilco Engineering, Inc. wants only the administrators to be able to change these settings.
3. Bilco Engineering, Inc. wants to have all their client computers must be configured with certain desktop settings named the Desktop Settings Specification which includes a password-protected screen saver. Bilco Engineering, Inc. also wants the client computers to be kept up-to-date with critical updates and security patches when Microsoft issues them. Bilco Engineering, Inc. thinks it is imperative that the IT administrator should approve the updates for computers in the two new retail offices. Bilco Engineering, Inc. wants only IT administrators to be capable of approving updates.
4. Bilco Engineering, Inc., requires their public Web servers not to be capable to accept TCP/IP connections from the Internet intended for services the public are not authorized to use. Bilco Engineering, Inc. also wants each employee to use a PKI certificate for identification in order to connect to the [Bilcobenefits.bilco.com](#).

5. Bilco Engineering, Inc. wants to have all the data in the Bilcobenefits.bilco.com Web application to be encrypted when in transit over the Internet. Bilco Engineering, Inc. also requires having customer accounts not be stored in the same Active Directory domain as the employee accounts. Bilco Engineering, Inc. wants the Administrators accounts from the domain which are domains that store the customer user accounts not to be capable of administering employee accounts.

### **Customer Requirements**

Bilco Engineering, Inc. considers the requirements below for wireless access and kiosk computers:

1. Bilco Engineering, Inc. Staff and customers are required to be able to access the wireless network whilst all the customers' personnel information should be encrypted while it is in transit on the Internet. Bilco Engineering, Inc. also requires the corporate servers only to be accessible to staff.
2. Bilco Engineering, Inc. wants to ensure the Kiosk computers can be used for browsing the Bilco Web-site only. Kiosk computers will run Windows XP Professional. Bilco Engineering, Inc. also wants regular customers to be able to establish accounts through acc.bilco.com. The information of the accounts will be stored in Active Directory.

### **Active Directory**

Bilco Engineering, Inc. has the following plans and requirements for Active Directory to be considered:

1. Bilco Engineering, Inc. requires only one top-level organizational unit (OU) to be contained for each retail office location. Bilco Engineering, Inc. requires the accounts for the staff members to be located in the OU for their primary work location. The two new retail offices client computers should be configured according to the Desktop Settings Specification even in the event that if the domain upgrade is incomplete at the required time.
2. Bilco Engineering, Inc. requires the Desktop support technicians at each retail office to be capable of resetting user passwords for staff. Bilco Engineering, Inc. also requires all IT staff be members of the AllSupport security group. The highly skilled IT staff will be members of the security group named Bilco Support whilst the rest of the staff are members of the Basic Support group.

### **Network Infrastructure**

Bilco Engineering, Inc. requires having the following network infrastructure requirements considered:

1. Remote Desktop Protocol (RDP) should be used by authorized IT staff to manage the servers in the perimeter network. Bilco Engineering, Inc., also requires the IT staff to be able to use RDP to manage servers at resorts.
2. Bilco Engineering, Inc. requires having the retail offices receive critical updates and security patches from their own continent. Bilco Engineering, Inc. wants to ensure that each retail office has one or more Windows Server 2003 computers configured as infrastructure. The Infrastructure server will be responsible for handling DNS, DHCP, and any VPN connections.
3. All the Bilco Engineering, Inc. users in should be able to create and read files stored in

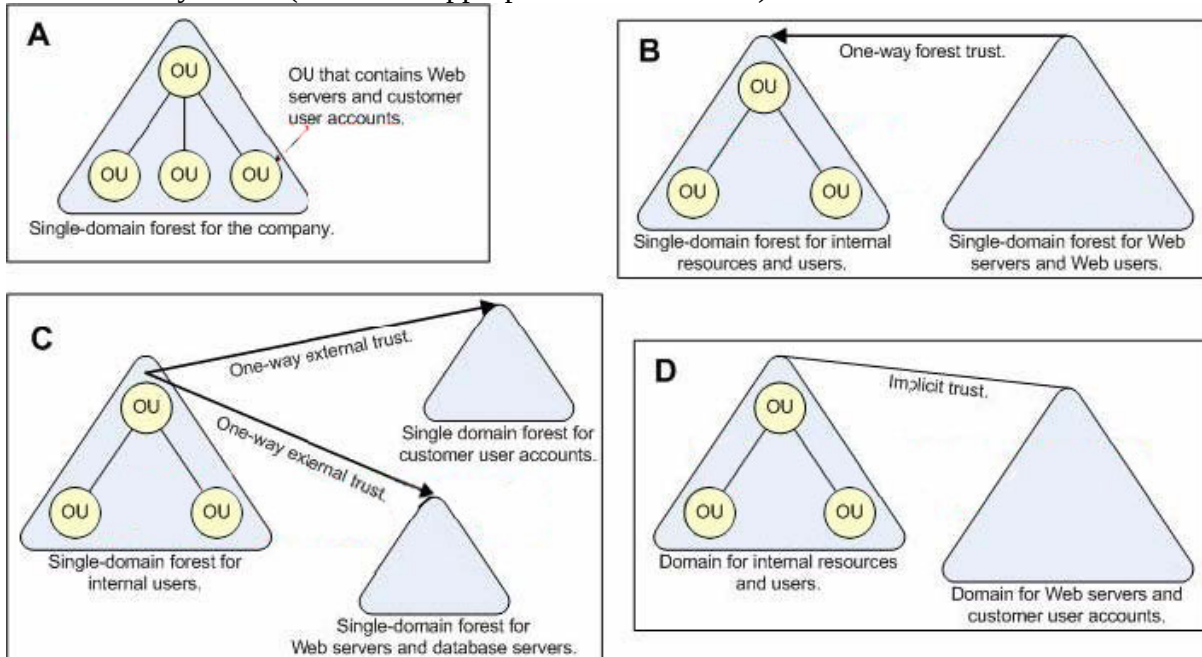
a shared folder named AllUsers and BE-FS01 after the deployment of BE-FS01. Bilco Engineering, Inc. requires only members of the Web Publishers security group to be capable of making changes to the public Web site. Bilco Engineering, Inc. considers it important that all changes be encrypted while being transmitted.

## Topic 5, Bilco Engineering, Inc. (12 Questions)

### QUESTION 1

You work as a network administrator at Bilco Engineering, Inc. You have received instruction from the Bilco Engineering, Inc. network CIO to start designing the company's Active Directory structure. You are required to provide a solution which will meet the public Web site's security requirements. You are required to choose which of the following designs are suitable.

What should you do? (Select the appropriate exhibit to use)



- A. A
- B. B
- C. C
- D. D

Answer: B

Explanation: In the scenario you should keep in mind that a forest trust is used to share resources between forests. A forest trust can be one-way or two-way. Windows Server 2003 supports trust relationships between different Active Directory forests. This option achieves:

1. Bilco Engineering, Inc. requires their public Web servers not to be capable to accept TCP/IP connections from the Internet intended for services the public are not authorized to use.

Incorrect Answers:

A: This option should not be used in the scenario because this option is a single domain forest where all the Organizational Units are residing. This option represents a security risk since the public Web servers are not to accept TCP/IP connections.

C: This option should not be used in the scenario because the option represents a trust relationship between itself and the Web servers and database servers. The option also has a trust relationship between itself and customer user accounts.

D: This option should not be used in the scenario because the option represents a single forest with an implicit trust between the domains.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 103

---

## **QUESTION 2**

You work as the network administrator at Bilco Engineering, Inc. You have recently received instruction to start designing the configuration for the kiosk computers. The configuration you design for the kiosk computers should be implemented by using the minimum amount of administrative effort. What should you do?

A. A Group Policy object (GPO) should be created and configured with the collection of settings in the Kiosk Desktop Specification: The appropriate software restriction policy should also be included. Make kiosk computers should then be made members of the Active Directory domain, the computer account objects should be placed in a dedicated OU and link the GPO to the OU.

B. A system policy file named Ntconfig.pol should be created and configured with the collection of settings in the Kiosk Desktop Specification. The kiosk computers should also be made members of the Active Directory domain. A Group Policy object (GPO) should then be used to run a startup script that copies the Ntconfig.pol file to the System32 folder on each kiosk computer.

C. One kiosk computer should be installed as a model. The computer should also be configured with the collection of settings in the Kiosk Desktop Specification. The content of the C:\Documents and Settings\Default Users folder from the model computer should then be copied to all other kiosk computers.

D. The kiosk computers should be configured as computers which are not members of any domain. The

Local Computer Policy should then be used to configure the computers with the collection of settings in the Kiosk Desktop Specification.

Answer: A

Explanation: In the scenario you should keep in mind that Group Policy Object (GPO) is used to set or sets of rules for managing client configuration settings that pertain to desktop lockdowns and the launching of applications. The GPOs are actually data structures which can be attached in a specific hierarchy to selected

Active Directory Objects. This option will achieve:

1. Bilco Engineering, Inc. Staff and customers are required to be able to access the wireless network.
2. Bilco Engineering, Inc. requires the Kiosk computers to be more restrictive with certain desktop settings named the Kiosk Desktop Specification. Bilco Engineering, Inc. wants only the administrators to be able to change these settings.

Incorrect Answers:

B: In the scenario you are not required to run a startup script as you are required to minimize the amount of administrative effort.

C: This option should not be considered in the scenario as you are required to use the minimum amount of administrative effort and the option requires allot of administrative effort.

D: In the scenario you should not consider configuring the Kiosk computers as non-members of any domain as this will not achieve the scenario objective.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 21

---

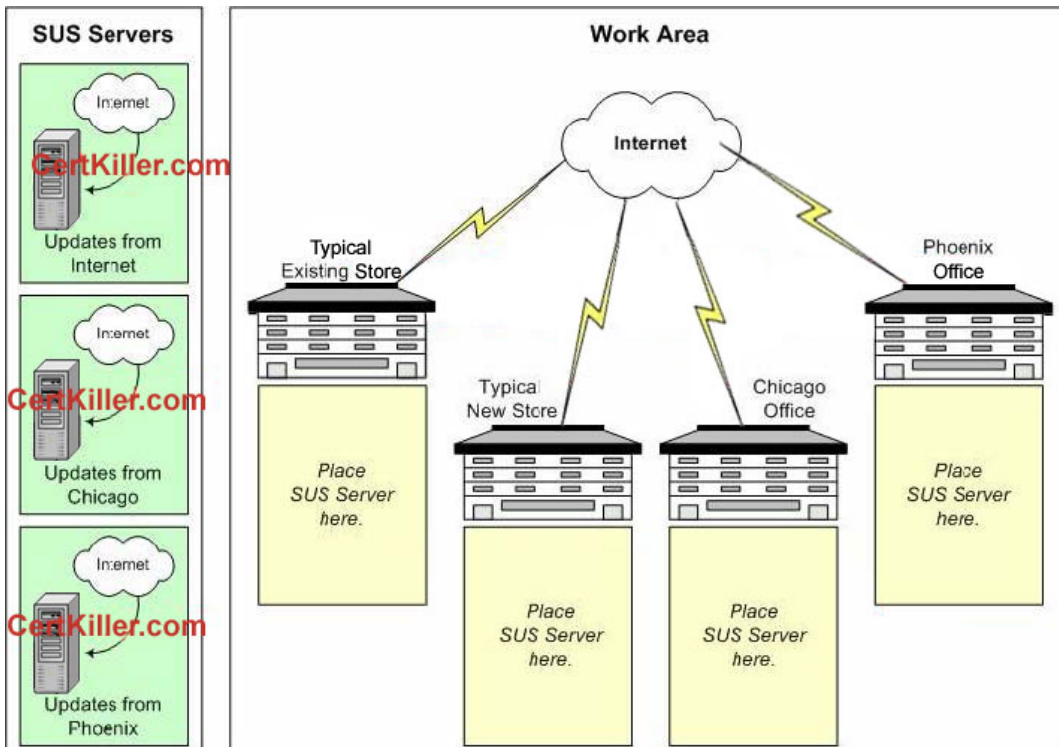
### **QUESTION 3**

#### **DRAG DROP**

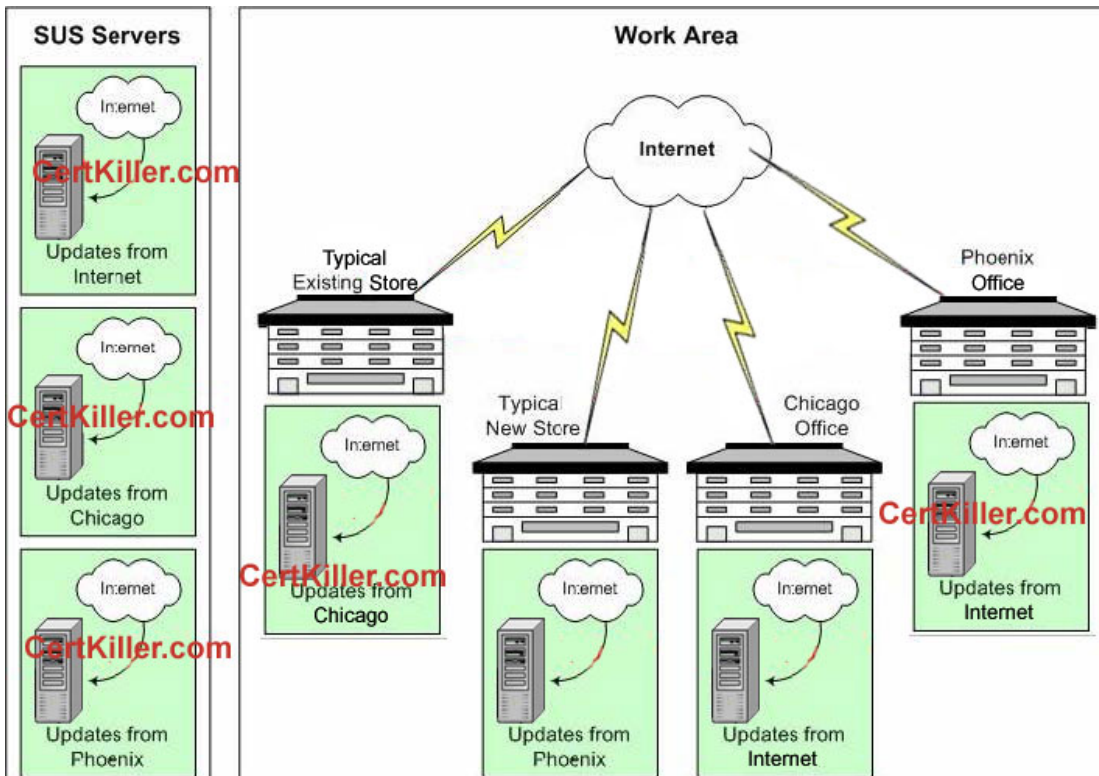
You work as a network administrator at Bilco Engineering, Inc. Below is a logical diagram of a portion of the Bilco Engineering, Inc. network shown in the work area. You have received instruction to start designing a software Update Services (SUS) infrastructure for at Bilco Engineering, Inc.

You will be required to decide where the SUS servers will be placed and also you should decide whether the servers will receive updates from Microsoft server on the Internet or SUS servers within the Bilco Engineering, Inc. network. Your solution design should use the fewest number of SUS servers possible.

What should you do? (To answer, drag the appropriate SUS server type to the appropriate location or locations in the work area.)



Answer:



Explanation:

In the scenario you are required to use the least amount of SUS server which will be achieved by configuring the Chicago and the Phoenix offices obtain updates from the Internet and they also will serve as SUS servers to the typically North American and

European resorts respectively. This will achieve:

1. A new retail office will be opened in Phoenix to support the two Denver retail offices the same way Chicago main office currently supports the North American retail offices.
2. Bilco Engineering, Inc. also wants the client computers to be kept up-to-date with critical updates and security patches when Microsoft issues them. Bilco Engineering, Inc. thinks it is imperative that the IT administrator should approve the updates for computers in the two new retail offices. Bilco Engineering, Inc. wants IT administrators to be capable of approving updates.
3. The retail office should receive critical updates and security patches from their own office.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 588

#### QUESTION 4

##### DRAG DROP

You work as the network administrator at Bilco Engineering, Inc. You have recently received instruction to start designing an IPSec policy for the Web servers in the Chicago office. You are required to decide which of the policy settings are suitable for use in the scenario.

What should you do? (To answer, drag the appropriate policy setting or settings to the correct location or locations in the work area.)

| Settings,<br>select from these | Work Area, place here |                                    |                                           |
|--------------------------------|-----------------------|------------------------------------|-------------------------------------------|
|                                | Type of traffic       | Web server to or from the Internet | Web server to or from the client computer |
| Allow                          | HTTP/HTTPS            | Setting.                           | Setting.                                  |
| Deny                           | Remote Desktop (RDP)  | Setting.                           | Setting.                                  |
| No policy                      | All other traffic     | Setting.                           | Setting.                                  |

Answer:

| Settings,<br>select from these | Work Area, place here |                                                                                   |
|--------------------------------|-----------------------|-----------------------------------------------------------------------------------|
|                                | Type of traffic       | Web server to or from the Internet      Web server to or from the client computer |
| Allow                          | HTTP/HTTPS            | Allow      Allow                                                                  |
| Deny                           | Remote Desktop (RDP)  | Allow      Allow                                                                  |
| No policy                      | All other traffic     | Deny      No policy                                                               |

In the scenario you should remember that (RDP) is a connection that needs to be configured in order for clients to connect to the Terminal Services server. The HTTP and HTTPS protocol is an Internet protocol that transfers HTML documents over the Internet. In the scenario applying the Deny Policy setting to the Web servers to or from the Internet as this will compromise security. Also you should also apply the Allow Policy setting for RDP, HTTP and HTTPS traffic on the Web servers to or from the client computers. This will achieve:

1. Bilco Engineering, Inc. has an information technology (IT) department located in Chicago. The IT department is responsible for operating the Bilco Engineering, Inc. Web, database and e-mail servers as well as client computers. The Bilco Engineering, Inc. IT department will periodically need to travel to remote retail offices to perform upgrades, installations and troubleshooting.
2. Bilco Engineering, Inc. also requires the IT staff to be able to use RDP to manage servers at resorts IT staff must also be able to use RDP to manage servers at resorts.
3. Remote Desktop Protocol (RDP) should be used by authorized IT staff to manage the servers in the perimeter network.
4. The Bilco Engineering, Inc. Company uses an Active Directory domain named bilco.com. The It Department in Chicago will be responsible for administering the domain. The bilco.com domain will always remain the forest root domain.
5. Bilco Engineering, Inc. requires their public Web servers not to be capable to accept TCP/IP connections from the Internet intended for services the public are not authorized to use.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 576

### QUESTION 5

You work as a network administrator at Bilco Engineering, Inc. You have received instruction from the Bilco Engineering, Inc. CIO to start designing a security strategy for the infrastructure servers at the resorts. You are required to select which of the actions you should perform.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Group Policy objects (GPOs) should be used to apply the custom security template or templates to the infrastructure servers.
- B. A custom security template should be established that contains unique required settings for each combination of services running on the infrastructure servers.
- C. All infrastructure servers should be placed in subnets that cannot exchange information with the Internet.
- D. The local policy settings should be edited to configure each individual server.

Answer: A, D

Explanation: In the scenario you should keep in mind that Group Policy Object (GPO) is used to set or sets of rules for managing client configuration settings that pertain to desktop lockdowns and the launching of applications. The GPOs are actually data structures which can be attached in a specific hierarchy to selected Active Directory Objects as this will:

1. One or more Windows Server 2003 computer that is configured as an infrastructure server to handle DNS, DHCP, and any VPN connections are required at each retail office.
2. Bilco Engineering, Inc. requires having the routine administrative duties automated as on busy days not all important administrative tasks are completed.
3. Bilco Engineering, Inc. IT Administration should have little manual overhead.

Incorrect Answers:

C: This option should not be used in the scenario because the option will not help the situation in the scenario.

D: In the scenario you should not use this option as you are required to apply the custom security template to the infrastructure servers.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 21

---

## **QUESTION 6**

You work as a network administrator at Bilco Engineering, Inc. The Bilco Engineering, Inc. employees require connecting to the Bilco Engineering, Inc. network using wireless technology. You have received instruction to start the design of a Security strategy for the wireless network at all resort locations. What should you do?

- A. All wireless access points should be configured to require the Wired Equivalent Privacy (WEP) protocol for all connections. A Group Policy object (GPO) should be used to distribute the WEP keys to all computers in the domain.
- B. IPSec policies should be established on all company servers to request encryption from all computers that connect from the wireless IP networks.
- C. On a domain controller Internet Authentication Service (IAS) should be installed. Configure The wireless access points should be configured to require IEEE 802.1x authentication

D. The wireless access points should be connected to a dedicated subnet. The subnet should be allowed direct access to the Internet, but not to the company network. The Bilco Engineering, Inc. users should be required to establish a VPN to access company resources.

Answer: D

Explanation: In the scenario you should remember that when a user is allowed access to the Bilco Engineering, Inc. organization you should make use of a VPN account. If they connect through the network firewall, then TCP Port 3389 should be opened if the users connect through a network firewall, which may be considered a security risk. This will help Bilco Engineering, Inc.:

1. The need for Wireless networking capability must be made to keep up with the upscale market. The consumers will be able to make wireless Internet connections.
2. All the Bilco Engineering, Inc. retail offices have one file server and are connected by VPN's across the Internet.
3. One or more Windows Server 2003 computer that is configured as an infrastructure server to handle DNS, DHCP, and any VPN connections are required at each retail office.

Incorrect Answers:

A: In the scenario you should remember that the WEP encryption protocol has flaws and that several software applications exists which are capable of easily cracking WEP encryption.

B: This option should not be used in the scenario because the option will not help you achieve your scenario objective.

C: In the scenario you do not require using the 802.1X standard as Bilco Engineering, Inc. makes use of VPN's.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide, p. 557

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 9, p. 325

---

### **QUESTION 7**

You work as a network administrator at Bilco Engineering, Inc. You have received instruction to start the design of an access control and permission strategy that will be used for user objects in Active Directory. You are required to select the appropriate actions to take in the scenario  
What should you do?

A. The permissions on the domain object and its child objects should be changed that the BasicSupport security group is denied permissions. Also you should add permission to each OU that contains user accounts allowing the AllSupport security group members to reset passwords in that OU.

B. Full control should be delegated over all OUs that contain user accounts to all AllSupport security group.

- C. The members of the AdvancedSupport security group should be made members of the Domain Admins security group.
- D. Each desktop support technician should be given permission to reset passwords for the top-level OU that contains user accounts at their own location.

Answer: D

Explanation: You should remember in the scenario that you can make use of the Active Directory Users And Computers utility. The utility is used for managing the Active Directory users, groups, and computers. In the scenario all the desktop support technician should be able to reset passwords for the top level OU containing all the user accounts at their locations. This will achieve:

1. Bilco Engineering, Inc. requires the Desktop support technicians at each retail office to be capable of resetting user passwords for staff.
2. There will be at least one desktop support technician assigned for each retail office. The support technicians depending on experience will have administrative rights to server located in the North American retail offices.
3. Bilco Engineering, Inc. requires the accounts for the staff members to be located in the OU for their primary work location.

Incorrect Answers:

A: This option should not be used in the scenario as this will not help. The objectives overview states less experienced staff members must also be members of the BasicSupport group.

B: This should not be done in the scenario as you would be over compensating. The objective overview states all IT staff that support users must be members of the AllSupport security group.

C: In the objectives overview the highly skilled IT staff must also be members of the security group named BilcoSupport.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide, p. 143

---

## **QUESTION 8**

You work as a network administrator at Bilco Engineering, Inc. You have received instruction recently to start the design of a permission structure for registry objects that enables the legacy application at the retail offices to run. You are required to make your design solution comply with the written security policy. What should you do?

- A. A GPO should be created and link the GPO to the OUs that contain computer accounts for computers that run the Legacy application. The GPO should be used to make all users who require access to the application members of Local Administrators group on each computer.
- B. A GPO should be created and link the GPO to the OUs that contain computer accounts for computers that run the Legacy application. The GPO should be used to give all users who require access to the application full control for the Ntuser.dat file.

C. A GPO should be created and link the GPO to the OUs that contain computer accounts for computers that run the legacy application. The GPO should be used to give the Domain Users security group full control on the HKEY\_USERS partition of the registry.

D. A GPO should be created and link the GPO to the OUs that contain computer accounts for computers that run the legacy application. The GPO should be used to give the Domain Users security group full control on the partitions of the registry that the legacy application uses.

Answer: D

Explanation: In the scenario you should keep in mind that Group Policy Object (GPO) is used to set or sets of rules for managing client configuration settings that pertain to desktop lockdowns and the launching of applications. The GPOs are actually data structures which can be attached in a specific hierarchy to selected Active Directory Objects. By following the actions in the answer you ensure you comply with the security requirements of Bilco Engineering, Inc.:

1. Bilco Engineering, Inc. IT Administration should have little manual overhead.
2. Bilco Engineering, Inc. requires having the routine administrative duties automated as on busy days not all important administrative tasks are completed.
3. Bilco Engineering, Inc. currently makes use of legacy applications at the retail offices to manage retail office functions by reading and writing a registry value which unauthorized users cannot access. Bilco Engineering, Inc. believes that the application will run properly if the users are made administrators on the client computer. Bilco Engineering, Inc. realizes that this move violates the company's written security policy.

Incorrect Answers:

A: This option should not be used in the scenario as you would be violating the written security policy of Bilco Engineering, Inc.

B: This option should not be used in the scenario because the NTUSER.DAT file is created for a user profile and this is not required.

C: This option should not be used because the Domain Users group should have control on the partitions of the registry that the legacy application uses.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 21

---

## QUESTION 9

You work as a network administrator at Bilco Engineering, Inc. You have received instruction recently to start the design that includes features that meet the written security policy requirements for the Bilco Engineering, Inc. network. You are required to select which of the authentication protocols should be used for wireless connection clients in the design.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Make use of a VPN account.
- B. Make use of an IAS server.
- C. Make use of WEP.
- D. Make use of IEEE 802.1x.
- E. Make use of IPSec policies.

Answer: A, E

Explanation: By making use of the IPSec policies and configuring a VPN account you would successfully be adhering to the written security policy in the scenario as required. This option will:

1. One or more Windows Server 2003 computer that is configured as an infrastructure server to handle DNS, DHCP, and any VPN connections are required at each retail office.

Incorrect Answers:

B: This option should not be used in the scenario because Bilco Engineering, Inc. already makes use of a VPN server that will be used.

C: In the scenario you should remember that the WEP encryption protocol has flaws and that several software applications exists which are capable of easily cracking WEP encryption.

D: In the scenario you do not require using the 802.1x standard as Bilco Engineering, Inc. makes use of VPN's

---

### **QUESTION 10**

You work as a network administrator at Bilco Engineering, Inc. You have recently received instruction to configure the servers hosting confidential data. The solution you are busy designing should require security related actions performed by an administrator that affects company servers to be logged. You are required to select which of the actions you would perform.

What should you do?

- A. The Security Configuration and Analysis snap-in should be run
- B. The Microsoft Baseline Security Analyzer should be used
- C. An IPSec policy should be created that requires IPSec encryption
- D. An audit policy should be created to track object access events on the required server

Answer: D

Explanation: In the scenario you should ensure that events that can affect the servers operations are logged and audited. By using this option you adhere to the company policy.

1. Bilco Engineering, Inc. requires security related actions performed by an administrator that affects company servers to be logged. Bilco Engineering, Inc. wants all the log files and a second administrator should audit the event

Incorrect Answers:

A: This option should not be used in the scenario because it is used to configure or

analyze the security settings on a single computer.

B: This option should not be used in the scenario because it is a GUI-based tool used to perform centrally executed scans of Windows-based computers to identify common security problems.

C: This option should not be used in the scenario because this will not allow you to audit access as required.

---

**QUESTION 11**

You work as a network administrator at Bilco Engineering, Inc. You have received instruction to start designing the configuration for the wireless network. The solution you are in the process of designing should meet the requirements of the wireless users.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Make use of static wired equivalent privacy (WEP)
- B. Make use of service set identifier (SSID) broadcasts
- C. Make use of ad hoc networking
- D. Make use of IEEE 802.1x authentication
- E. Make use of Internet Authentication Service (IAS)

Answer: D, E

Explanation: In the scenario you should consider making use of the IEEE802.1x authentication protocol as well as an IAS server because only then you would be adhering to the wireless network users' requirements in the scenario.

1. Bilco Engineering, Inc. are planning to use a new inventory and shipping management solution which allows wireless handheld computers in the warehouses to connect in real time to the inventory database

Incorrect Answers:

A: This option should not be used in the scenario because many application exists that are capable of cracking the pre-shared key used by this authentication.

B: In the scenario you should not consider assigning service set identifiers (SSIDs) as this will not adhere to the wireless networking requirements.

C: This option should not be used in the scenario as it is not appropriate in environments where security is an issue.

---

**QUESTION 12**

You need to design a solution that ensures that the network users are kept up-to-date with the latest security patches as Microsoft releases them. You are required to select which of the following tools can be used to identify all the missing security updates on network computers.

What should you do?

- A. Run the gpresult.exe tool
- B. Run the qfecheck.exe tool

- C. Run the qchain.exe tool
- D. Run the mbsacli.exe tool

Answer: D

Explanation: In the scenario you should remember in order for the administrator or person in charge to identify which security updates have not been applied that you should make use of the mbsacli.exe tool.

1. Bilco Engineering, Inc. additionally wants the client computers to be kept up-to-date with critical updates and security patches when Microsoft issues them. Bilco Engineering, Inc. thinks it is imperative that the IT administrator should approve the updates for computers in the two new retail offices

Incorrect Answers:

A: This option should not be used in the scenario because the utility is used to provide a listing of Group Policy settings and the Resultant Set of Policy (RSOP) for a user's computer.

B: This option should not be used in the scenario because the utility is used to track patches that have been installed on Windows 2000 computers only.

C: In the scenario you should not consider using the qchain.exe because the utility is used to install multiple patches or hot fixes in series.

## Topic 6, Certkiller .com, Scenario

### Overview

Certkiller .com is a software company that develops and distributes shrink wrapped business applications for the Microsoft Windows platform. The company recently merged with a delivery company named Mondo Transport, Ltd. Mondo Transport, Ltd. delivers the software applications to Certkiller .com's customers in North-East USA.

### Physical Locations

Certkiller .com has its headquarters near the center of Philadelphia and branch offices in Detroit, Washington, and Montreal. The Philadelphia office consists of a business office and a dispatch warehouse where Mondo Transport, Ltd. users pick up application packages for delivery.

The Information Technology (IT) department, Sales department, Administration and Development department are located in the Philadelphia office.

Each branch office has a Customer Support department and a Sales department. The Customer Support department provides on-site customer support.

The Mondo Transport, Ltd. office is located in Chicago.

### Planned Changes:

Certkiller .com plans to expand into South-East USA and will open a branch office in Atlanta. The Atlanta office will be added to the Certkiller .com domain. An organizational unit (OU) named Atlanta OU and two child OUs named Development and Support be added to the Certkiller .com domain for the new branch office.

### **Business Processes**

Certkiller .com has a public Web site that is hosted on a Web server named Certkiller -SR04. Certkiller -SR04 is located in Philadelphia.

Certkiller .com accepts phone orders and Web orders from customers. The Sales department is responsible for handling orders and invoicing.

All products that must be delivered are prepared by the Sales department who enter the delivery details into an intranet Web site.

Mondo Transport, Ltd. delivery personnel use a Web kiosk in the dispatch warehouse to pick up delivery assignments. The Web kiosks run only Microsoft Internet Explorer 5.5. Delivery personnel use a password to log on to the subsystem, and they are supposed to log off after they retrieve delivery details. Delivery personnel do not have physical access to the business office.

The Customer Support department at each branch office has mobile users that provide on-site support to Certkiller .com customers. These mobile users connect to a remote access server named Certkiller -SR05 that is located at the Philadelphia office.

All customer billing and contact information must remain confidential.

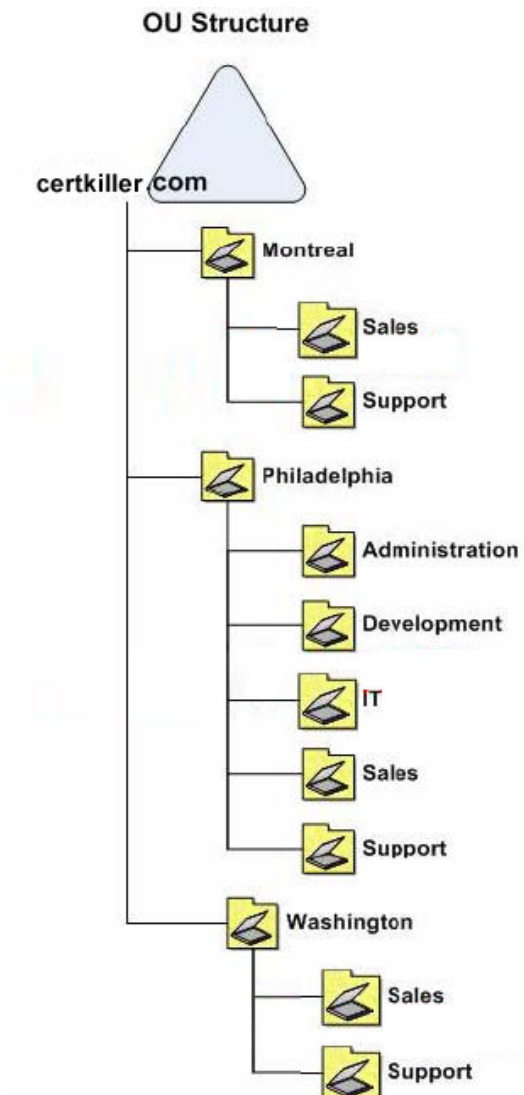
### **Directory Services**

The Certkiller .com network consists of two domains: an Active Directory domain named Certkiller .com; and a Windows NT 4.0 domain named TKDOM. A two-way external trust relationship exists between the Active Directory domain and the Windows NT 4.0 domain.

The IT department manages Active Directory centrally from the Philadelphia office.

All users have domain user accounts.

The organizational unit (OU) structure for the Active Directory domain is shown in the OU Structure exhibit.



The Mondo Transport, Ltd. network consists of a single Active Directory domain named mondo.com. All domain controllers on the Mondo Transport, Ltd. network run Windows Server 2003.

### Network Infrastructure

The network at the Philadelphia office consists of three subnets named SubnetA, SubnetB and SubnetC. A router connects the three subnets. All servers in the Philadelphia office are located on SubnetA; all client computers in the Philadelphia business office are located on SubnetB; and all kiosks in the dispatch warehouse are located on SubnetC. SubnetA contains two Windows Server 2003 domain controllers named Certkiller -DC01 and Certkiller -DC02.

The branch offices are connected to the Philadelphia office by 128 Kbps ISDN lines. The operating system installed on the client computers in each office is shown in the following table.

| Office       | Operating System                                          |
|--------------|-----------------------------------------------------------|
| Philadelphia | Windows XP Professional                                   |
| Montreal     | Windows XP Professional                                   |
| Washington   | Windows 2000 Professional                                 |
| Detroit      | Windows XP Professional and<br>Windows NT Workstation 4.0 |
| Chicago      | Windows 2000 Professional and<br>Windows XP Professional  |

All managers and mobile sales users have Windows XP Professional client computers.

### **Problem Statements**

#### **Chief Executive Officer**

"Software development is the core of our business. We need to absolutely certain that our competitors do not obtain our development data. This information is critical to the success of our business and must remain secure. We also need to increase security for our customer data and our delivery data in the dispatch warehouse. We need to able to identify users who gain unauthorized access to this data."

"We need to enable stronger authentication strategy for the network and we need to integrate Mondo Transport, Ltd. into this strategy."

"Our budget makes allowance for security equipment but we cannot hire more employees."

#### **Chief Information Officer**

"Our IT staff use their administrative user accounts for everything. They often log on to client computers in the business office and they forget to log off when they are done. Consequently, business office users can perform tasks by using administrator privileges. We need to put a stop to this."

"Our current patch management system is also problematic. Our IT staff test security patches when they come out but they have problems deploying them to the other offices. We need ensure that the servers and client computers in both domains always have the latest updates and security patches. Our IT staff must be able to control which updates and security patches are deployed to the other offices. Our firewall prevents client computers from accessing the Windows Update Web site. We want to retain this setting."

"We need to limit unnecessary traffic across the WAN links."

"Our IT staff is stretched as it is, so any solutions to these problems should not increase the workload on our IT staff."

#### **Chief Security Officer**

"Only senior executives are allowed to use Encrypting File System (EFS) on local computers but we sometimes have problems with lost user profiles. This makes restoring access to encrypted files as quickly as possible a real problem."

"I think we need a two-factor authentication method for the mobile users in the Customer Support departments. When they log on remotely from a customer site, they should to log on by means of a secure VPN connection. The solution must be easy to implement."

"We need a public key infrastructure (PKI) that is not vulnerable to compromise. We also need a PKI that will allow only specific administrators to control the enrollment of smart

card certificates."

"We also need to track configuration changes on all domain controllers."

"The Mondo Transport, Ltd. users use simple passwords and the often guess each other's passwords. This is a major problem I term of securing customer and delivery data on the dispatch warehouse Kiosks."

### **Senior IT Administrator**

"We have a problem with our workload. We simply do not have enough staff to support all the branch offices and the newly acquired mondo.com domain. Currently, we rely on the desktop support technician at each branch office to perform minimal everyday administrative tasks, such as resetting passwords. Even though Mondo Transport, Ltd. has its own IT staff, we are responsible for administration of the mondo.com domain."

Mondo Transport, Ltd. Delivery Personnel

"I know I should pick a difficult password but I can only remember so much. To simplify my life, I use the same password for every job. I have heard that other delivery men watch and steal their colleagues' passwords, but it has never happened to me."

### **Written Security Policy**

The following requirements are included in the written security policy for Certkiller .com:

1. Only managers and executives must have access to customer data in the CK\_Customers folder.
2. Only managers and executives must have access to software development data.
3. All access to development, customer, and delivery data must be monitor and tracked.
4. Only senior executives must be able to encrypt files stored on file servers or on their local computers.
5. Customer Support users must be able to encrypt the offline files cache.
6. Attempts to make system registry configuration changes on client computers in the business office must be monitored and track. We do not need to monitor or track everyday actions on client computers.
7. All computers must be maintained with current security patches for critical updates. The senior IT administrator is responsible for first testing all patches and then releasing them to all client and server computers in the company.
8. Only IT staff will have access to administrative accounts and users must not be able to log on interactively to client computers by using accounts that have administrative privileges.
9. Two-factor authentication must be required to perform administrative tasks.
10. Mobile users must use only L2TP VPN connections to connect to the internal network.

## **Topic 6, Certkiller .com (8 Questions)**

---

### **QUESTION 1**

You need to design a remote access strategy that meets business requirements. You want to test you remote access security solutions. You configure a server named Certkiller -SR06 as a VPN server. You then install Internet Authentication Service (IAS) on Certkiller -SR05 and configure the RADIUS clients. However, when

remote users attempt to connect to the corporate network through Certkiller -SR06 they are not authenticated by Active Directory. You need to ensure that remote users can be authenticated by using IAS on Certkiller -SR05. What should you do?

- A. Install Active Directory on Certkiller -SR05.
- B. Add Certkiller -SR05 to the RAS and IAS Servers group in Active Directory.
- C. Add Certkiller -SR06 to the RAS and IAS Servers group in Active Directory.
- D. Install Active Directory on Certkiller -SR06.

Answer: B

Explanation: RADIUS must have the required permissions to read user account attributes in Active Directory, You should add the server providing RADIUS to the RAS and IAS Servers group to provide it with the required permissions.

Incorrect Answers:

A, D: Installing Active Directory on the RAS server or the VPN server will promote them to domain controllers. This would introduce security risks as these servers must be accessible from the Internet.

C: Certkiller -SR06 does not perform authentication and does not need to be added to the RAS and IAS Servers group in Active Directory.

---

## **QUESTION 2**

You need to design the network to support mobile Customer Support users who need remote access to the corporate network. You need to ensure that you solution meets business requirements.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Create a Group Policy object (GPO) and configure it to allow autoenrollment of user and computer certificates.
- B. Instruct the mobile Customer Support users to submit a request for user certificates from the CA Web site enrollment page.
- C. Configure a Certificate Services hierarchy.
- D. Use a password generator application to create a preshared key, and distribute it to all mobile users.

Answer: A, C

Explanation: The Auto-enrollment features are set by CA administrators in the certificate templates and will automatically issue certificates.

Group Policy Object (GPO) is a set or sets of rules for managing client configuration settings that pertain to desktop lockdowns and the launching of applications. GPOs are data structures that are attached in a specific hierarchy to selected Active Directory Objects. It can be applied to sites, domains, or organizational units. This reduces the administrative effort required to apply the same policies on an individual basis.

1. Each office has mobile Customer Support users. These mobile users connect to a remote access server at headquarters by using a dial-up connection.
2. We need a two-factor authentication method for the mobile Customer Support users.
3. We want to require all remote users to log on by means of a secure VPN connection.

The solution must be easy to implement.

Considering the above, you should configure autoenrollment for user certificates and computer certificates and you should also configure Certificate Services hierarchy in the litwareinc.com domain.

Incorrect Answers:

B: Web enrollment would require unnecessary user intervention.

D: Making use of a password generator to issue pre-shared keys to mobile users is not going to support the mobile users.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 3, p. 181

---

### **QUESTION 3**

You need to design an Encrypted File System (EFS) strategy that meets the requirements of the Chief Security Officer.

What should you do?

- A. Configure key archival on each certification authority (CA).
- B. Configure a certificate trust list (CTL) that includes the root certification authority (CA) certificate.
- C. Create a security group named SeniorExecs.  
Assign the appropriate NTFS permissions to the SeniorExecs group for the senior executives' data.
- D. Create an organizational unit (OU) named SeniorExecs OU.  
Add the senior executives' user accounts to the SeniorExecs OU.  
Configure an IPsec policy on the SeniorExecs OU.

Answer: A

Explanation: Safely storing and archiving recovery agent credentials will ensure that you're always able to decrypt important files even after you've changed recovery agents. Files that might sit dormant for some time might need to be decrypted long after the file's owner leaves the company, so archiving is a critical step.

Thus a Windows Server 2003 Enterprise Edition computer with the certificates services can be configured to issue EFS certificates with a file archival property. Especially when you take into account the relevant pieces of information from the case study mentioned below:

1. Only senior executives are allowed to use Encrypting File System (EFS) on local computers but we sometimes have problems with lost user profiles. This makes restoring access to encrypted files as quickly as possible a real problem.
2. I think we need a two-factor authentication method for the mobile users in the

Customer Support departments. When they log on remotely from a customer site, they should log on by means of a secure VPN connection. The solution must be easy to implement.

3.  
We need a public key infrastructure (PKI) that is not vulnerable to compromise. We also need a PKI that will allow only specific administrators to control the enrollment of smart card certificates.

4. We also need to track configuration changes on all domain controllers.

5. The Mondo Transport, Ltd. users use simple passwords and they often guess each other's passwords. This is a major problem in terms of securing customer and delivery data on the dispatch warehouse Kiosks.

Incorrect Answers:

B: The CTL documents the trusted certificates of the enterprise. This signed list is issued by the CAs. However, this is not what is needed by Denver IT administrator.

C, D: These options will not address the concerns stated.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 3 & 9, pp. 157-159, 181, 565-569

---

#### **QUESTION 4**

You need to design a strategy to provide maximum protection for customer and delivery data. You need to ensure that your solution meets Certkiller .com's business requirements.

What should you do?

A. Create a separate domain to authenticate Mondo Transport, Ltd. delivery personnel.

B. Implement smart card authentication for Mondo Transport, Ltd.

Configure the Kiosks to log off when a user removes their smart card.

C. Modify the Default Domain Policy Group Policy object (GPO) to require complex user account passwords.

Require all Mondo Transport, Ltd. delivery personnel to change their passwords the next time they log on to the Kiosks.

D. Use Encrypting File System (EFS) to encrypt all customer and delivery data.

Answer: B

Explanation

: Smart cards provide a secure method of logging on to a Windows Server 2003 domain. Smart cards are physical cards that contain a certificate. This certificate identifies a user to Windows. Using smart cards is more secure than standard logons, because users must have possession of their card to logon. Smart cards are protected with a pin code in case of accidental loss or theft. In addition to logging on to a domain, smart cards are used for client authentication to applications and for securing e-mail. Since it is stated that money can be spent on security, this would be the option best suited for the company's requirement.

Incorrect Answers:

A: A separate domain for Mondo Transport, Ltd. delivery personnel authentication is not feasible in the circumstances in which the company operates. Mondo Transport, Ltd. delivery personnel get their assignments from kiosk computers that are on the domain. Putting them in a different domain will disable them accessing their assignments.

C: Making use of complex user account passwords will not be as effective as smart card authentication especially in view of Mondo Transport, Ltd. delivery personnel stealing each other's passwords.

D: Encrypting all files containing customer data does not mean preventing access to encrypted files.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 283

---

### **QUESTION 5**

You need to design a public key infrastructure (PKI) for Certkiller .com. You need to ensure that your solution meets Certkiller .com's business requirements.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Add one offline stand-alone root certificate authority (CA).
- B. Add two online enterprise subordinate certificate authorities (CAs).
- C. Add one online enterprise root certification authority (CA).
- D. Add one offline enterprise subordinate certification authority (CA).

Answer: A, B

Explanation

: The root CA is the top of the CA hierarchy and should be trusted at all times. The certificate chain will ultimately end at the root C

A. The enterprise can have a root CA as enterprise or a stand-alone C

A. The root CA is the only entity that can self sign, or issue self certificates in the enterprise. Windows Server 2003 only allows one machine to act as the root C

A. The root CA is the most important C

A. If the root CA is compromised, all the CAs in the enterprise will be compromised. Therefore, it is a good practice to disconnect the root CA from the network and use a subsidiary CA to issue certificates to users. Any CAs that is not the root CA is classified as subordinate CAs. The first level of subordinate CAs will obtain their certificates from the root C

A. These servers are commonly referred to as intermediary or policy CAs. They will pass on the certificate information to the issuing CAs down the chain. They are referred to as intermediary because they act as a "go-between" with the root CA and the issuing CAs.

You need to protect the root. Install the root CA as a Windows Server 2003 stand-alone root C

A. This type of CA does not need to be on the network. Take the root CA offline. When the root CA is not connected to the network, it cannot be attacked across the network.

1. We need a public key infrastructure (PKI) that is not vulnerable to compromise. We also need a PKI that will allow only specific administrators to control the enrollment of smart card certificates.

Incorrect Answers:

C: It is best practice to have a root CA offline. Thus these options will leave your network vulnerable.

D: The enterprise subordinate CA is the issuing CA and would need to be online.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 3, p. 159, 181

---

### **QUESTION 6**

You need to design a security patch management strategy that addresses the concerns of the Chief Information Officer. You need to ensure that your solution must meet the company's business requirements.

What should you do?

A. Run the Microsoft Baseline Security Analyzer (MBSA) on all computers.

Use a Group Policy object (GPO) to configure all computers to use Automatic Updates to obtain security patches from the Windows Update Web site.

B. Upgrade all client computers to either Windows 2000 Professional or Windows XP Professional.

Implement Software Update Services (SUS).

C. Upgrade all client computers to either Windows 2000 Professional or Windows XP Professional.

Implement Systems Management Server (SMS).

D. Install the Active Directory Client Extensions on all Windows 95, Windows 98, and Windows NT Workstation 4.0 computers.

Download all security patches to a Distributed File System (DFS) replica and instruct all users to use the DFS replica to install security patches.

Answer: B

Explanation: Take into consideration the following:

1. Our current patch management system is also problematic. Our IT staff test security patches when they come out but they have problems deploying them to the other offices. We need ensure that the servers and client computers in both domains always have the latest updates and security patches. Our IT staff must be able to control which updates and security patches are deployed to the other offices. Our firewall prevents client computers from accessing the Windows Update Web site. We want to retain this setting.
2. We need to limit unnecessary traffic across the WAN links.
3. Our IT staff is stretched as it is, so any solutions to these problems should not increase the workload on our IT staff.

This option will accommodate the utilization of group policy objects to apply the company's security patch management process.

Incorrect Answers:

A: MBSA can perform local or remote scans of Windows systems. It verifies whether your computer has the latest security updates and whether there are any common security violation configurations that have been applied to your computer. However, you need a system to deploy security patches without requiring client computers to access the Windows Update Web site.

C: SMS is a software solution uses to consolidate change and management tasks and can be used to distribute security updates and patches. However, Software Update Services (SUS) is the better system to use to automate the distribution of updates.

D: This option involves far too much administrative effort that can be avoided.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, p. 807

---

### **QUESTION 7**

You need to design an auditing strategy for the CK\_Customers folder the meets the business requirements.

What should you do?

E. Audit success and failures events for object access.

F. Audit failure events for object access.

G. Audit failures events for privilege use.

H. Audit success and failures events for privilege use.

Answer: B

Explanation: Auditing object access audits user access to objects such as files, folders, registry keys, and so forth. As with the other audit policies, you can either monitor the success or failure of these actions.

Incorrect Answers:

A: Auditing failure of object access only will only constitute half of the tracking that is required as stated in the written security policy.

C, D: Auditing privilege use tracks events when a user exercises a right.

---

### **QUESTION 8**

You need to redesign the network infrastructure to support the implementation of Software Update Services (SUS).

What should you do?

A. Place the Windows NT Workstation 4.0 client computers in a separate organizational unit (OU).

B. Upgrade the Windows NT Workstation 4.0 client computers to at least Windows 2000 Professional.

C. Migrate the Windows NT 4.0 domain to Active Directory.

D.  
Install the Active Directory Client Extensions on the Windows NT Workstation 4.0 client computers.

Answer: B

Explanation: SUS is not supported on Windows NT Workstation 4.0 and Windows 9x. These systems must be updated to at least Windows 2000 Professional. Furthermore, Microsoft no longer provides updates for Windows NT Workstation 4.0 and Windows 9x.

Incorrect Answers:

A, C: Placing the Windows NT Workstation 4.0 client computers in a separate OU or migrating the Windows NT 4.0 will not enable the Windows NT Workstation 4.0 client computers to access SUS. Furthermore, Microsoft no longer provides updates for Windows NT Workstation 4.0 and Windows 9x.

D: Installing the Active Directory Client Extensions on all legacy client computers will not enable these computers to access SUS. Furthermore, Microsoft no longer provides updates for Windows NT Workstation 4.0 and Windows 9x.

## Topic 7, A2B Aviation, Scenario

### Background

A2B Aviation is a research company that develops and improves technologies that are used in the aviation industry.

### Physical locations

A2B Aviation has their main office is located in Phoenix. A2B Aviation also has branch offices in Detroit and Miami.

### Planned Changes

A2B Aviation has recently decided to enter into a partnership with International Retailers, Inc. to collaborate on research projects. A2B Aviation requires that encrypted communications be enabled when communicating with International Retailers, Inc. A2B Aviation has recently decided to implement a new wireless network and upgrade all client computers to Windows XP Professional.

### Existing Environment

#### Business Processes

A2B Aviation has several users in the marketing department who access marketing data. A2B Aviation makes use of a Web-based application that is installed on a server running Internet Information Services (IIS) 6.0.

A2B Aviation requires their research intellectual property stored on database servers. A2B Aviation users of the research intellectual accesses research intellectual property data on the database servers by using a Web-based application residing on the company intranet. A2B Aviation requires the researchers' level of access to the data to be dependent upon the department position in the project involvement.

A2B Aviation also stores some intellectual property information in a shared folder named A2BResearch on a server named A2B-SR01. A2B Aviation knows that the information in the Research Stats folder is the only intellectual property information shared. A2B Aviation ensures that the Research Stats folder contains a subfolder for each research project and the following:

1. Engine
2. Fuel
3. International

A2B Aviation has set permission set on all research intellectual property to ensure unauthorized users do not have access to the information.

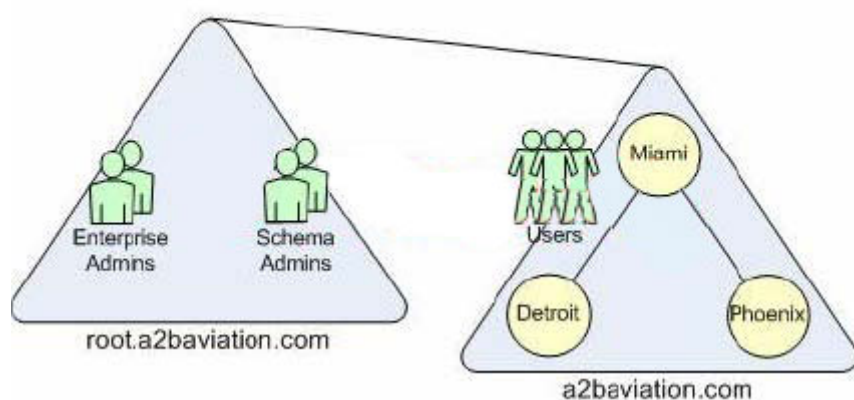
The A2B Aviation subset of the groups, group members, and associated levels of access used at A2B Aviation Research is shown below:

| Group                   | Members                                                          | Access                                                                        |
|-------------------------|------------------------------------------------------------------|-------------------------------------------------------------------------------|
| International_Retailers | International Retailers, Inc. employees, and IT department users | Allowed access to only the International folder                               |
| HR                      | Human Resources (HR) department users                            | Allowed access to employee data                                               |
| IT                      | IT Department users                                              | Allowed access to the network except HR servers and data                      |
| Marketing_Sales         | Marketing, sales and IT department users                         | Allowed access to marketing and Sales information including the Engine folder |
| Research                | Research and IT department users                                 | Allowed access to research data                                               |

### Directory Services

A2B Aviation's Windows Server 2003 Active Directory environment is shown in the Existing Active Directory Structure exhibit:

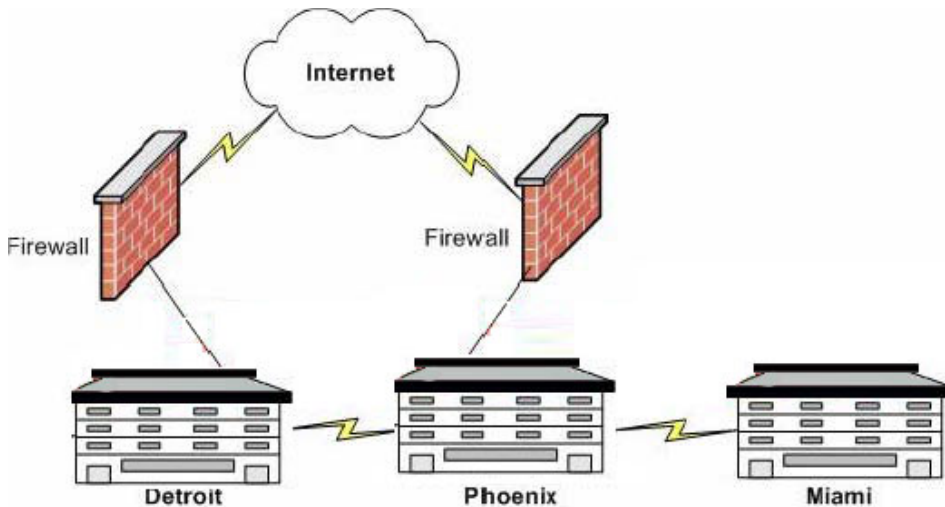
#### Existing Active Directory Structure



A2B Aviation has the root.a2baviation.com domain configured as an empty root domain.

### Network Infrastructure

A2B Aviation's Existing network is shown below:



The A2B Aviation server on the network and where they reside is shown in the table lists below:

| Server               | Location | Operating System    | Function                                                    |
|----------------------|----------|---------------------|-------------------------------------------------------------|
| A2B-SR12             | Detroit  | Windows Server 2003 | MS SQL Server 2000 used to store confidential research data |
| A2B-SR11<br>A2B-SR10 | Detroit  | Windows Server 2003 | File and print server                                       |
| A2B-SR09             | Miami    | Windows Server 2003 | File, print and global catalog server                       |
| A2B-SR08             | Phoenix  | Windows Server 2003 | Terminal server                                             |
| A2B-SR07             | Phoenix  | Windows Server 2003 | MS SQL Server 2000 used to store confidential research data |
| A2B-SR06             | Phoenix  | Windows 2000 Server | MS Exchange 2000 Server                                     |
| A2B-SR05             | Phoenix  | Windows Server 2003 | Intranet and Web-based marketing application                |
| A2B-SR04             | Phoenix  | Windows Server 2003 | Certification Authority (CA)                                |
| A2B-SR03             | Phoenix  | Windows Server 2003 | File and print server                                       |
| A2B-SR01<br>A2B-SR02 | Phoenix  | Windows Server 2003 | File and print server                                       |

A2B Aviation uses Firewalls to allow all DNS name resolution. A2B Aviation also wants to deploy a public key infrastructure (PKI) was on A2B-SR04. A2B Aviation plans to have the PKI integrated with Active Directory and use Certificate Services. A2B Aviation has recently decided to start using smart cards. A2B Aviation will host the encrypted files on A2B-SR02.

### Problem Statements

A2B Aviation wants to have the following business problems considered:

1. A2B Aviation requires users to remember up to five passwords and access data and applications. A2B Aviation also requires some researchers to have stored encrypted confidential information on their client computers

2. A2B Aviation realizes that Administrators do not have adequate time to maintain servers and client computers with the latest security patches because they are too busy addressing other issues.

## Interviews

### Chief Executive Officer

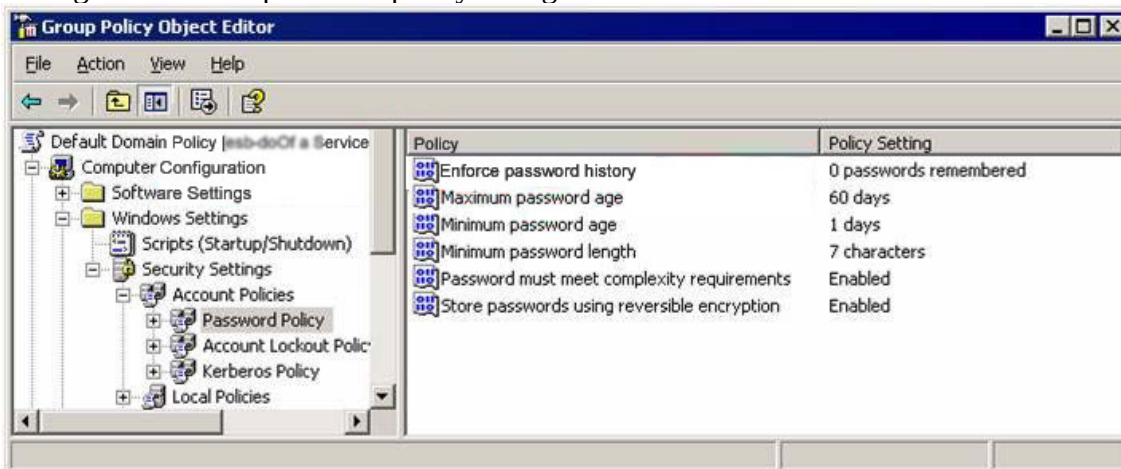
A2B Aviation requires having the effectiveness of research efforts to improve by fostering collaboration both within A2B Aviation and with International Retailers, Inc. A2B Aviation wants to have the efficiency of data sharing increased. A2B Aviation knows that they should share some information, but it is still imperative that research information is kept confidential.

A2B Aviation has their scientists and other network users in the research department often working long hours in the office and from home. A2B Aviation now requires a secure method of accessing the network and using shared resources.

International Retailers, Inc. also wants to share confidential data with A2B Aviation. The requirement for this is now that the International Retailers, Inc. users will now require secure methods, to access our company's network and shared resources.

### Chief Information Officer

The CIO of A2B Aviation has recently informed the network management that information shared between A2B Aviation and other companies use the strongest encryption and authentication possible in order to keep the information confidential. A2B Aviation realizes that internally, identify management is a problem. To address the problem A2B Aviation wants to physically issue smart cards. A2B Aviation requires having their current password policy strengthened which is shown in the exhibit below:



A2B Aviation recently realized that minimizing IT expenses is important but they require implementing a cost-effective solution that addresses accessing multiple resources, including the new wireless LAN, the intranet Web server, and the terminal server. A2B Aviation requires the solution to have a two-factor authentication.

### System Administrator

A2B Aviation's system administrator has recently said because other companies have different network environments and business processes, sharing research data with International Retailers, Inc. might be technically challenging.

A2B Aviation for this purpose requires creating a better security patch management process. Currently, client computers are not updated with security updates until the security patches are incorporated into service packs.

## **Business Requirements**

### **Security Requirements**

A2B Aviation wants the following security requirements considered:

1. A2B Aviation wants all communications to the research database servers to be encrypted. A2B Aviation also wants all traffic to the Web-based marketing and research applications to be encrypted
2. A2B Aviation wants to have the security patches tested before they are deployed. A2B Aviation also does not want the security to interfere with application functionality.
3. The HR segment needs additional protection to prevent non-HR internal users from gaining unauthorized access.
4. Company intellectual property cannot be stored on client computers; it must be stored in the database containing intellectual property or in the appropriate folder on a file server. Confidentiality of this data must be enforced.
5. A2B Aviation wants only authorized users and computers can connect to the wireless network. The A2B administrators are responsible for enrolling users. A2B Aviation also wants DNS records not to be transferred to external sources.

## **Topic 7, A2B Aviation (11 Questions)**

---

### **QUESTION 1**

You work as a network administrator at A2B Aviation. You have received instruction to start designing an authentication solution. The authentication solution you are designing should meet the business requirements for Terminal Services. What should you do?

- A. The Remote Desktop Users group should be denied access to the terminal server.
- B. A2baviation.com users should be restricted from logging on locally to the terminal server.
- C. The terminal server should be configured to use smart cards.
- D. IPSec should be configured to permit only Remote Desktop Protocol (RDP) connections to the terminal server.

Answer: D

Explanation: In the scenario by making use of the IPSec configuration you ensure that you are adhering to the business requirements for the terminal server in the scenario.

1. A2B Aviation recently realized that minimizing IT expenses is important but they require implementing a cost-effective solution that addresses accessing multiple resources, including the new wireless LAN, the intranet Web server, and the terminal server. A2B Aviation requires the solution to have a two-factor authentication.

## QUESTION 2

You work as a network administrator at A2B Aviation. You have received instruction to start designing an authentication solution for the wireless network. The solution you are designing should adhere to the security requirements of A2B Aviation.  
What should you do?

- A. The wireless network should be configured to use Wired Equivalent Privacy (WEP).
- B. An Internet Authentication Service (IAS) server should be installed and configured
- C. IEEE 802.1x authentication should be configured with smart cards.
- D. Wireless VPNs using L2TP/IPSec should be created between the client computers to the wireless access point.

Answer: A

Explanation: You should consider making use of the WEP protocol in the scenario because using this protocol ensures that you adhere to the security policy of A2B Aviation.

1. A2B Aviation wants only authorized users and computers can connect to the wireless network. The A2B administrators are responsible for enrolling users.

---

## QUESTION 3

You work as a network administrator at A2B Aviation. You have received instruction to start designing a strategy to move confidential data from research users' client computers to A2B-SR02. The solution you are busy designing should adhere to the business requirements of A2B Aviation. You are required to instruct the research users what to do.  
What should you do?

- A. The encrypted data should be moved to a new server that is not a member of the domain, and then move it to A2B-SR02.
- B. The encrypted data should be moved to a compressed folder on A2B-SR02 by using Web Distributed Authoring and Versioning (WebDAV) over SSL.
- C. The encrypted data should be moved to a folder on A2B-SR02 over an IPSec connection.
- D. The encrypted data should be moved to an Encrypting File System (EFS) folder on A2B-SR02 over an IPSec connection.

Answer: D

Explanation: In the scenario you should consider making use of an EFS folder on A2B-SR02 as this will ensure that you are completely adhering to the business requirements of A2B Aviation.

1. A2B Aviation wants all communications to the research database servers to be encrypted. A2B Aviation also wants all traffic to the Web-based marketing and research applications to be encrypted

---

**QUESTION 4**

You work as a network administrator at A2B Aviation. You have received instruction to start designing an access control strategy for the marketing application. The solution you are busy designing should minimize impact on server and network performance.

What should you do?

- A. All marketing application Web pages should be configured to require SSL.
- B. The high security setting should be required on Terminal Services connections to the marketing application.
- C. Client computers should be required to connect to the marketing application by using a VPN connection.
- D. IPSec should be used to encrypt communications between the servers in the Miami and Phoenix offices.

Answer: A

Explanation: In the scenario you should consider making use of SSL because by making use of SSL A2B Aviation will ensure that the required objectives are met in the scenario.

1. A2B Aviation wants all communications to the research database servers to be encrypted. A2B Aviation also wants all traffic to the Web-based marketing and research applications to be encrypted

---

**QUESTION 5**

You work as a network administrator at A2B Aviation. You have received instruction to start designing the PKI infrastructure. The solution you are busy designing should completely adhere to the business requirements of A2B Aviation. What should you do?

- A. A stand-alone subordinate CA should be created to issue certificates.
- B. A qualified subordinate CA should be used.
- C. Configure Certificate template access control lists (ACLs) should be configured on A2B-SR02.
- D. A2B-SR02 should be moved offline and create an enterprise subordinate CA to issue certificates.

Answer: D

Explanation: In the scenario you should consider moving A2B-SR02 offline because doing this ensures that A2B Aviation completely adheres to the business requirements that should be met.

1. A2B Aviation uses Firewalls to allow all DNS name resolution. A2B Aviation also wants to deploy a public key infrastructure (PKI) was on A2B-SR04. A2B Aviation plans to have the PKI integrated with Active Directory and use Certificate Services

---

**QUESTION 6**

You work as a network administrator at A2B Aviation. You have received instruction to start designing a method for the research intellectual property to remain confidential. The solution you are busy designing for A2B Aviation should meet security requirements.

What should you do?

- A. Communications between A2B-SR12, A2B-SR10, A2B-SR07, and A2B-SR01 should be required to use IPSec.
- B. A separate subnet for all servers should be created that contain research intellectual property.
- C. A2B-SR12 and A2B-SR07 should be placed on a separate virtual LAN from the internal network. Access to these virtual LAN segments should be granted to only the client computers that are used by authorized users.
- D. Client computers should be required to connect to research intellectual property through a SSL VPN.

Answer: A

Explanation: You should consider ensuring that communications between the servers in question make use of IPSec because by using IPSec you are adhering to the security requirements of A2B Aviation.

1. Company intellectual property cannot be stored on client computers; it must be stored in the database containing intellectual property or in the appropriate folder on a file server. Confidentiality of this data must be enforced

---

**QUESTION 7**

You work as a network administrator at A2B Aviation. You have received instruction to start providing users in the research department access to different functions of the Web-based research application based on their individual user roles in A2B Aviation.

What should you do?

- A. Permissions should be defined by using access control lists (ACLs).
- B. One-to-many client certificate mapping should be used.
- C. Windows directory service mapper should be used and enable Microsoft .NET Passport authentication.
- D. Authorization rules and scopes should be created by using Authorization Manager.

Answer: D

Explanation: In the scenario you should consider making use of the Authorization Manager because the Authorization Manager will ensure that you at all times are adhering to company policy.

1. A2B Aviation wants all communications to the research database servers to be encrypted. A2B Aviation also wants all traffic to the Web-based marketing and research applications to be encrypted

---

**QUESTION 8**

You work as a network administrator at A2B Aviation. You have received instruction to start designing a password policy. The solution for the password policy you are designing should meet the business requirements of A2B Aviation. What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. The minimum password age should be set to zero days.
- B. The maximum password age should be increased.
- C. The number of passwords that are remembered should be increased.
- D. Reversible encryption should be disabled.

Answer: C, D

Explanation: In the scenario the users are required to remember 5 different passwords. Furthermore in the exhibit you can see that reversible encryption is enabled. This is a high security risk because everyone can simply "hack" stored passwords on a workstation. You have to disable the reversible encryption.

1. A2B Aviation realizes that internally, identify management is a problem. To address the problem A2B Aviation wants to physically issue smart cards. A2B Aviation requires having their current password policy strengthened

Incorrect Answers:

A, B: These options should not be considered for use in the scenario because you are required to strengthen the password policy and this option decreases the security.

---

**QUESTION 9**

You work as a network administrator at A2B Aviation. You have received instruction to start designing a certificate management process. The solution you are busy designing will be used for the internal users. What should you do?

- A. Enrollment stations should be established and store user certificates in a smart card.
- B. Connection Manager scripts should be created to identify the client computer operating system, and configure Web proxy settings to specify the appropriate Web enrollment service.
- C. A Web enrollment service should be established for internal users to request access to resources.
- D. Enrollment Agent rights should be granted to users.

Answer: A

Explanation: In the scenario you should consider establishing enrollment stations

and store the user certificates in a smart card; this will ensure that you meet A2B Aviation business needs.

1. A2B Aviation uses Firewalls to allow all DNS name resolution. A2B Aviation also wants to deploy a public key infrastructure (PKI) was on A2B-SR04. A2B Aviation plans to have the PKI integrated with Active Directory and use Certificate Services. A2B Aviation has recently decided to start using smart cards
2. A2B Aviation realizes that internally, identify management is a problem. To address the problem A2B Aviation wants to physically issue smart cards

---

**QUESTION 10**

You work as a network administrator at A2B Aviation. You have received instruction to start designing a method to standardize and deploy a baseline security configuration for servers. The solution you are busy designing should completely meet business requirements of A2B Aviation.

What should you do?

- A. A GPO should be used to distribute and apply a custom security template.
- B. The System Policy Editor should be used to configure each server's security settings.
- C. A script that installs the Hisecdc.inf security template should be created.
- D. A GPO should be used to distribute and apply the Hisec.inf security template.

Answer: A

Explanation: In the scenario you should consider making use of a GPO to distribute and apply a custom security template because this ensures that you are adhering to the business requirements of A2B Aviation in the scenario.

1. A2B Aviation wants to have the security patches tested before they are deployed. A2B Aviation also does not want the security to interfere with application functionality

---

**QUESTION 11**

You work as a network administrator at A2B Aviation. You have received instruction to start designing an authentication method that will provide the required level of security. The authentication solution you are busy designing should meet the requirements of A2B Aviation for remote computers.

What should you do?

- A. Use Two-factor authentication
- B. Use VPNs that require using L2TP/IPSec
- C. Use IPSec authentication
- D. Use IEEE 802.1x authentication

Answer: A

Explanation: You should consider making use of the two-factor authentication because this will have the users require swiping a smartcard through a smartcard reader.

1. A2B Aviation recently realized that minimizing IT expenses is important but they require implementing a cost-effective solution that addresses accessing multiple resources, including the new wireless LAN, the intranet Web server, and the terminal server. A2B Aviation requires the solution to have a two-factor authentication.

## Topic 8, National Traders, Inc., Scenario

### **Background**

National Traders, Inc. is a specialty gardening retailer that sells a variety of exotic plants and bulbs, and organic fertilizers.

The company recently acquired another company named Mondo Transport, Ltd. that provides shipping services for National Traders, Inc.'s customers.

### **Physical Locations**

National Traders, Inc. has its headquarters in Washington and six retail stores located in Atlanta, Miami, New Orleans, St Louis, Chicago, and Houston.

Mondo Transport, Ltd. is located in Chicago. Mondo Transport, Ltd. operates the warehouse for National Traders, Inc.

### **Planned Changes**

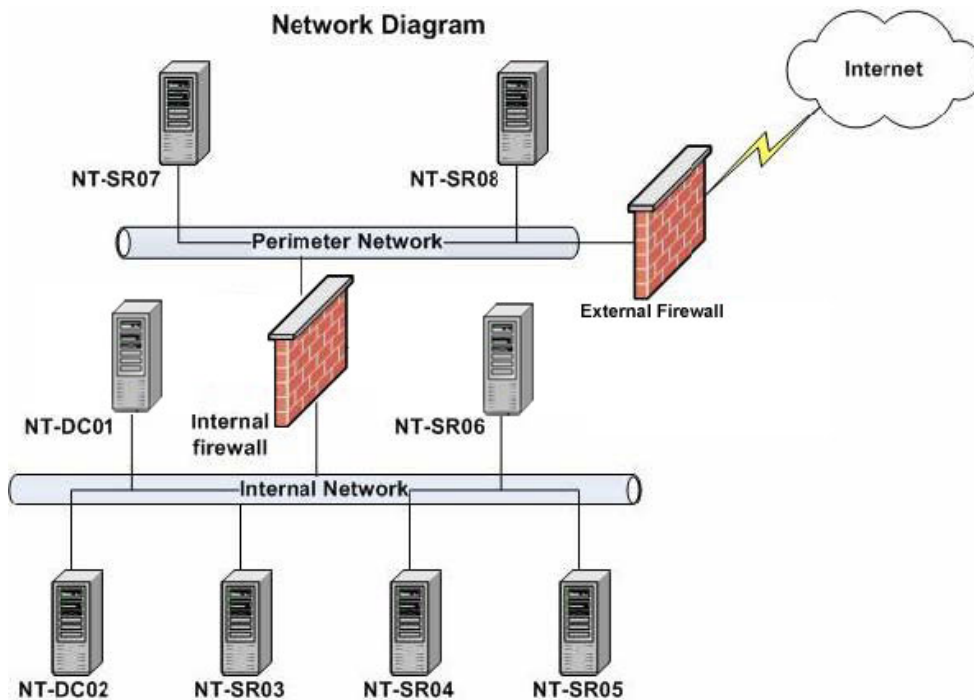
National Traders, Inc. wants to redesign its network infrastructure. The proposed network infrastructure will include a perimeter network that will contain a VPN server named NT-SR08 and a Web server named NT-SR07. All remote National Traders, Inc. users will access that corporate network through NT-SR08 while NT-SR07 will host the company's e-Commerce Web site.

A Web server named NT-SR05 will be installed on the National Traders, Inc.'s internal network for development and testing.

A Routing and Remote Access Service (RRAS) server named NT-SR06 will be install on the internal network. Internet Authentication Service (IAS) will also be installed on NT-SR06.

Where possible, all client computers in the Washington office will be upgraded to Windows XP Professional.

The proposed network infrastructure is shown in the Network Diagram exhibit.



### Business Processes

National Traders, Inc. has six departments named Administration, Human Resources (HR), Finance, and Sales.

Customers who place orders on the nationaltraders.com Website must register with National Traders, Inc. before they can place an order. The Web customer's information is stored in a database named CK\_Customers that is hosted on a SQL Server 2000 database server named NT-SR04. These users are then registered as Web customers and their logon information is set to them in an e-mail message.

Web customers connect to a virtual Internet Information Services (IIS) directory on NT-SR07 named Members. Here they can view available merchandise and place orders. After the Web customer places an order, the request is submitted to Mondo Transport,

### Ltd. for packaging and shipping.

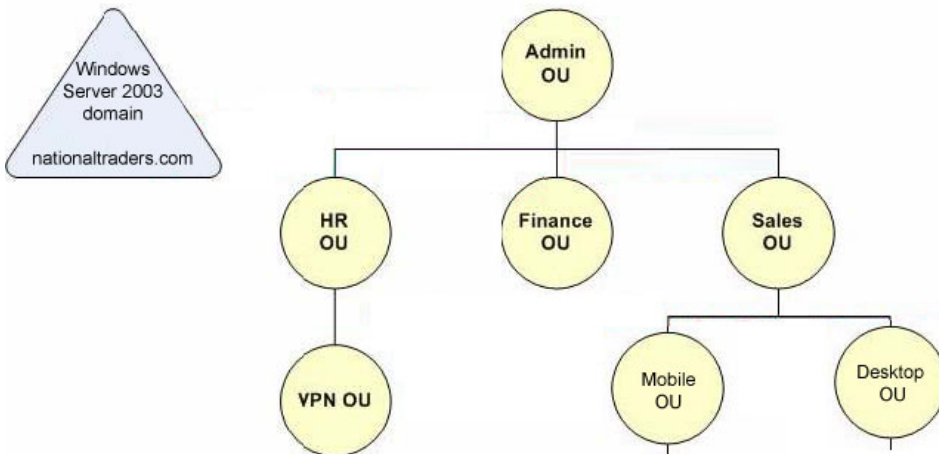
A record of all sales transactions is stored on a file server named NT-SR03 in a shared folder named NT\_SALES. The Allow - Full Control share permission on the NT\_SALES folder is assigned to the Authenticated Users group.

### Active Directory

The network consists of a single Active Directory domain named nationaltraders.com. All servers on the National Traders, Inc. network run Windows Server 2003 and all client computers currently run either Windows NT Workstation 4.0 or Windows 98. The latest service packs are installed on all network computers.

The relevant portion of the organizational unit (OU) structure is shown in the OU Structure exhibit.

## OU Structure



The Mobile OU contains the computer accounts for the portable computers while the Desktop OU contains computer accounts for desktop computers. All user and computer accounts for the Finance department are located in the Finance OU.

### Network Infrastructure

The Washington office has two Microsoft Internet Security and Acceleration (ISA) Server 2000 computers named NT-SR09 and NT-SR10, and wireless access points (APs). ISA servers and the wireless APs support wireless client computers in the Sales department.

A public e-Commerce Web site is hosted on a Web server named NT-SR07. NT-SR07 is running Internet Information Services (IIS) 6.0. Mondo Transport, Ltd. users access NT-SR07 by means of a VPN tunnel established between National Traders, Inc. and Mondo Transport, Ltd.

The Finance department uses a legacy application that can run only on Windows NT Workstation 4.0. The client computers for all other departments run Windows 98.

The HR department stores personnel information on a file server named NT-SR03. NT-SR03 is also configured as an offline stand-alone root certification authority (CA).

### Problem Statements

#### Chief Information Officer

"Lately our Internet connection has been overutilized. We must take measures to reduce this and must not to place extra strain on this connection."

"One area where we can reduce bandwidth usages is in our current patch management solution. It consumes too much bandwidth and requires too much time. We should optimize our patch management solution. We also need to be able to identify which security patches are installed on company computers."

"I'm also concerned about buffer overflow attacks against our Web server. If such an attack occurs against our Web server, I want to be able to redirect the user to a web page that informs them that legal action will be taken against them."

#### Chief Security Officer

"I'm concerned about the security of our wireless network. I think our current wireless

configuration makes our network vulnerable to attack. We need to improve security here and we need to protect the data that is transmitted between the wireless client computers and the wireless access points. I also want to use Group Policy objects (GPOs) to manage our wireless network."

"I'm also concerned about the security of the servers that users from Mondo Transport, Ltd. access. We need to improve security here as well.

"To date, no certificates have been issued to any user. We should make better use of our public key infrastructure (PKI). We should implement companywide user certificates as the first phase of our new authentication strategy."

"Users in the Finance department will no longer be able to change their passwords while they are logging on to their client computers once the proposed upgrades have been completed. We need to make allowance for this."

#### **System Administrator:**

"Some users have downloaded unauthorized software from the Internet and installed it on company computers. This caused several client computers to stop responding. In some cases the client computers had to be recovered from backup, which was totally unnecessary. We should prevent users from downloading and installing unauthorized software."

#### **Written Security Policy**

The relevant portion of National Traders, Inc.'s written security policy includes the following requirements:

1. Only users in the Sales department must be able to connect to the wireless network.
2. Strong authentication is required for the wireless network.
3. Data traffic between the HR department users and NT-SR03 must be secure and encrypted at all times.
4. Only members of the Sales department who have portable computers are allowed to encrypt data.
5. The Sales department must have its own data recover agent.
6. Two-factor authentication must be implemented for users in the Finance department.
7. Data in the NT\_SALES folder must be accessible to only the Administration department staff and must be encrypted.
8. All traffic to the Member virtual directory on NT-SR07 must be encrypted.
9. Web customers must be able to verify the identity of NT-SR07.
10. All attempts to use a local user account to log on to Windows Server 2003 and Windows XP Professional computers must be tracked.
11. Only members of the Administration department must be able to remotely modify the registry on NT-SR05.
12. All software must be approved for company use.
13. NT-SR08 must support MS-CHAP v2 authentication.

## Topic 8, National Traders, Inc. (9 Questions)

---

### **QUESTION 1**

DRAG DROP

You need to design an audit strategy for National Traders, Inc. You need to ensure that your solution meets the company's business requirements.

What should you do? (To answer, drag the appropriate steps from the pane on the left and arrange them in the correct order in the pane on the right.)

**Steps, select from these**

|                                                                       |
|-----------------------------------------------------------------------|
| Create a security template that audits account logon events           |
| Create a security template that audits object access.                 |
| Create a security template that audits logon events.                  |
| Import the security template into a Group Policy object (GPO)         |
| Link the Group Policy object (GPO) to the Domain Controllers OU.      |
| Link the Group Policy object (GPO) to the nationaltraders.com domain. |

**Steps, place here**

|                                 |
|---------------------------------|
| Place first step here.          |
| Place second step here, if any. |
| Place third step here, if any.  |
| Place fourth step here, if any. |
| Place fifth step here, if any.  |
| Place sixth step here, if any.  |

Answer:

**Steps, select from these**

|                                                                  |
|------------------------------------------------------------------|
| Create a security template that audits account logon events      |
| Create a security template that audits object access.            |
|                                                                  |
|                                                                  |
| Link the Group Policy object (GPO) to the Domain Controllers OU. |
|                                                                  |

**Steps, place here**

|                                                                       |
|-----------------------------------------------------------------------|
| Create a security template that audits logon events.                  |
| Import the security template into a Group Policy object (GPO).        |
| Link the Group Policy object (GPO) to the nationaltraders.com domain. |
| Place fourth step here, if any.                                       |
| Place fifth step here, if any.                                        |
| Place sixth step here, if any.                                        |

Explanation:

Audit Logon Events - Events are recorded on the computer where the access token is created. If a domain account is used, events are recorded both on the workstation and on the domain controller-one for the account logon event on the domain controller, and one for the logon event on the workstation. Events on the domain controller are recorded when Group Policy is read.

Audit Account Logon Events - Provides information on events that occur where the account used to log on resides.

In this scenario an audit strategy that would meet the business requirements should be enabling audit the logon events for success and failed attempts, in a new security template that should be linked to the domain. You also need to import the new template in to the new GPO to apply it.

Incorrect Answers:

Linking the GPO to the Domain Controllers OU will audit events on the domain controllers and not the other systems on the network. This is fine if you are auditing account logon events but if you are auditing logon events you should link the GPO to the domain.

Enabling the Audit account logon events policy allows you to capture authentication events rather than which accounts are attempting to logon. You should enable the Audit logon events policy instead.

Enabling the Audit object access policy allows you to track access to objects such as files, folders and systems.

Reference:

Roberta Bragg, MCSE Self-Paced Training Kit (Exam 70-298): Designing Security for a Microsoft Windows Server 2003 Network, Chapter 9, p. 38

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 9, p. 544

---

## **QUESTION 2**

You need to design an access control strategy for NT-SR05. You need to ensure that your solution meets National Traders, Inc.'s business requirements.  
What should you do?

- A. Enable logging on the e-Commerce Web site on NT-SR05.
- B. Configure the Winreg registry key on NT-SR05.
- C. Install a Secure Sockets Layer (SSL) certificate on NT-SR05.
- D. Configure the e-Commerce Web site on NT-SR05 to require Windows authentication.

Answer: B

Explanation: The Registry is given a high level of security by default. The only users who are granted full access to the entire Registry are administrators. Other users are generally given full access to the keys related to their own user accounts located in HKEY\_CURRENT\_USER. They are also generally given read-only access to other areas of the Registry related to the computer and the software. Users are granted no access to other users' account data. If a user has permission to modify a key, that user can modify that key and any key beneath it in the hierarchy. In this case only members of the Administration department must be able to remotely modify the registry on NT-SR05; therefore what is needed is to modify the Winreg registry key on NT-SR05.

Incorrect Answers:

A: Enabling logging on a website will track access to the website. However, you need to control access to the registry on the server rather than the website.

C: SSL can be used to secure communication between a web server and a browser. It

cannot be used to provide access control.

D: Enabling Windows authentication on a website will control the users who can access to the website. However, you need to control access to the registry on the server rather than the website.

Reference:

Roberta Bragg, MCSE Self-Paced Training Kit (Exam 70-298): Designing Security for a Microsoft Windows Server 2003 Network, Chapter 13, p. 11

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 9, p. 541-543

---

### **QUESTION 3**

You need to design a solution that addresses the Chief Information Officer's security concerns.

What should you do?

- A. Run the Resultant Set of Policy (RSOP) wizard in planning mode from a domain controller.
- B. Run the gpresult command on each domain controller and analyze the results.
- C. Install the Microsoft Baseline Security Analyzer (MBSA) and use it to scan for Windows vulnerabilities on all computers in the domain.
- D. Create a startup script that runs the secedit command and apply the script to all computers in the domain.
- E. Create a custom security template and run Security Configuration and Analysis to analyze the security settings of each computer against the custom security template.

Answer: C

Explanation: The Chief Security Officer has two security concerns: buffer overflow attacks against the Web server and the current patch management. Mbsacli.exe is a command that can perform local or remote scans of Windows systems. This utility scans an entire network of computers and produces reports that list missing patches. By making use of this command the chief security officer will be forewarned.

Incorrect Answers:

A: RSOP is a tool that can show the effective policy applied to a user or computer or what the policy would be, for planning purposes. It does not scan for missing security patches.

B: The gpresult.exe command displays Resultant Set of Policy (RSOP) about users and computers. RSOP shows the effective policy for a particular user and a specified machine. This will not address the chief information officer's concerns.

D: The command line tool, secedit.exe, is used to analyze, configure, and export system security settings. There are a variety of command-line switches used with secedit. This tool is often used in batch programs or scheduled tasks to apply security settings automatically. It is also the preferred tool for reapplying default security settings. But this does not necessarily mean that missing security patches will be checked for.

E: The Security Configuration and Analysis tool is used to check security settings against a custom security template; it is not used to identify missing security patches.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 2, pp. 51-52

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, pp. 147, 158

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 398, 633

---

**QUESTION 4**

**DRAG DROP**

You need to design a security strategy for NT-SR08. You need to ensure that your solution meets National Traders, Inc.'s business requirements.

What should you do? (To answer, drag the appropriate steps from the pane on the left and arrange them in the correct order in the pane on the right.)

**Steps, select from these**

**Steps, place here**

|                                                                                       |
|---------------------------------------------------------------------------------------|
| Create and configure a security template.                                             |
| Configure the remote access policy on NT-SR08.                                        |
| Configure NT-SR08 as a RADIUS client of NT-SR06.                                      |
| Import the security template into the Default Domain Policy Group Policy object (GP0) |
| Move NT-SR08 into the VPN OU.                                                         |
| Import the security template into the local policy on NT-SR08.                        |

|                                 |
|---------------------------------|
| Place first step here.          |
| Place second step here, if any. |
| Place third step here, if any.  |
| Place fourth step here, if any. |
| Place fifth step here, if any.  |
| Place sixth step here, if any.  |

Answer:

| Steps, select from these                                                              | Steps, place here                              |
|---------------------------------------------------------------------------------------|------------------------------------------------|
| Create and configure a security template.                                             | Move NT-SR08 into the VPN OU.                  |
|                                                                                       | Configure the remote access policy on NT-SR08. |
| Configure NT-SR08 as a RADIUS client of NT-SR06.                                      | <i>Place third step here, if any.</i>          |
| Import the security template into the Default Domain Policy Group Policy Object (GPO) | <i>Place fourth step here, if any.</i>         |
|                                                                                       | <i>Place fifth step here, if any.</i>          |
| Import the security template into the local policy on NT-SR08.                        | <i>Place sixth step here, if any.</i>          |

Explanation: A security strategy for NT-SR08 should be moving it into the VPN OU and then configure the remote access policy on it because all user and computer accounts for the HR department are located in the HR OU and the VPN OU is connected to the HR OU.

1. A VPN server named NT-SR08 will be placed in the perimeter network. Mobile users will use NT-SR08 to connect to the company network.
2. NT-SR08 must support MS-CHAP v2 authentication.

Incorrect Answers:

You should configure at least two IAS servers within your Active Directory environment. If you have only one server configured and the machine hosting IAS becomes unavailable, dial-up and VPN clients will be denied access to network resources until you bring the IAS server back online. By using two servers, you can configure your remote access clients with the information for both, allowing them to automatically fail over to the secondary IAS server if the primary one fails. This way, your remote users will be able to have continuous access to your internal resources without sacrificing the security provided by IAS. This option suggests making use of only one server which is not recommended.

A new security template and importing it, is not necessary. All that has to be done is to move NT-SR08 into the VPN OU and then configure remote access policy on NT-SR08.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 33, 624, 627-628  
 Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 10, pp. 662-663

## QUESTION 5

You need to design an authentication strategy for the Finance. You need to ensure that your solution meets National Traders, Inc.'s business requirements.

What should you do? (Each correct answer represents a part of the solution. Choose TWO.)

- A. Configure all computers in the Finance department to use PEAP authentication.
- B. Issue smart cards and smart card readers to all users and computers in the Finance department.
- C. Install user certificates on all computers in the Finance department.
- D. Configure the domain to require smart cards during logon for all users in the Finance department.
- E. Configure the domain to respond to requests for IPSec encryption.
- F. Configure the domain to require NTLMv2 authentication.

Answer: B, D

Explanation: Following are the relevant information regarding an authentication strategy for the Finance department as described in the case study:

1. The HR department stores personnel information on a file server named NT-SR03. NT-SR03 is also configured as an offline stand-alone root certification authority (CA).
2. I want to implement companywide user certificates as the first phase of our new authentication strategy.
3. Two-factor authentication must be implemented for users in the Finance department. Smart cards provide a secure method of logging on to a Windows Server 2003 domain. It is a credit-card-sized device that is used to securely store public and private keys, passwords, and other types of personal information. To use a smart card, you need a smart card reader attached to the computer and a personal identification number (PIN) for the smart card. In Windows Server 2003, you can use smart cards to enable certificate-based authentication and SSO to the enterprise. The smart cards "force" the employee to use the asymmetric key and a PIN to authenticate.

Making use of smart cards and smart card readers and configuring the domain to require smart cards during logon for the Finance department will thus be implementing two-factor authentication as is required in the case study.

Incorrect Answers:

A: Protected EAP authentication doesn't provide any authentication itself. Instead, it relies on external third-party authentication methods that you can retrofit to your existing servers. This is not what is required.

C: Making use of user certificates is not going to enforce two-factor authentication.

E: Configuring all Finance department computers to respond to requests for IPSec encryption is not going to enforce two-factor authentication.

F: Depending on the operating system in use, the clients might not be able to use the NTLM v2 authentication protocol. If they cannot and there is an account on the secured server that the down-level client needs to access, it will be unable to do so. Thus this option is not the answer.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 2, p. 74

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied,  
MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003  
Environment Study Guide & DVD Training System, pp. 283

---

**QUESTION 6**

You need to design a security solution for NT-SR07. You must ensure that your solution addresses the Chief Information Officer's concerns.  
What should you do?

- A. Configure NT-SR07 to use Web distributed Authoring and Versioning (WebDAV).
- B. Install URLScan on NT-SR07 and configure the ISAPI filter.
- C. Create a Group Policy Object (GPO) and configure the GPO to audit successful logon attempts and object access. Apply the GPO to NT-SR07.
- D. Configure the Web site redirection option in the Internet Information Services (IIS) console on NT-SR07.

Answer: B

Explanation: URLScan allows the administrator to set rules for filtering incoming requests for the IIS server. By setting restrictions or rules, the administrator can filter out requests that might compromise the security of the IIS server or the network behind it. Intruders often use unusual requests to "trick" the server. Some common requests used by hackers include: (1) Unusually long requests that can cause buffer overflow vulnerabilities, (2) Request an unusual action that might be incorrectly interpreted or responded to, (3) Be encoded by an unusual character set that might be incorrectly interpreted or responded to and (4) Include unusual character sequences that might cause unspecified results.

Windows Server 2003 includes IIS 6.0, which include the features of URLScan. And since the public Web site, hosted on NT-SR07 is running IIS 6.0 this option is the answer.

1. A public Web site is hosted on a server running IIS 6.0 named NT-SR07. Users at Mondo Transport, Ltd. have access to NT-SR07 by means of a VPN tunnel established between National Traders, Inc. and Mondo Transport, Ltd.
2. Recently our Internet connection has been overutilized, and measures must be taken not to place extra strain on this connection.
3. I'm concerned about buffer overflow attacks against our Web servers. If such an attack occurs against our public Web server, I want to be able to redirect the user request to an HTML document.

Incorrect Answers:

- A: WebDAV is a secure file transfer protocol that can be used over intranets and the Internet. You can download, upload, and manage files on remote computers across the Internet and intranets using WebDAV. But this alone will not address the chief information officer's concerns.
- C: auditing logon attempts will only log attempts to logon to the Web server rather than the Web site.
- D: Configuring a Web site redirection will not fully address the concern about buffer

overflow attacks in this scenario. It will only address the need to respond to the attack.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, pp. 206

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 2 & 6, pp. 114, 386

---

**QUESTION 7**

You need to design a software usage policy for the employees of National Traders, Inc. You need to ensure that your solution meets National Traders, Inc.'s business requirements.

What should you do?

- A. Configure a software restriction policy and apply it through the Default Domain Policy Group Policy object (GPO).
- B. Configure a Software Installation Policy that publishes approved applications to users and apply it through the Default Domain Policy Group Policy object (GPO).
- C. Configure ingress and egress filtering on the internal firewall.
- D. Configure the Internet Explorer settings and apply it through the Default Domain Policy Group Policy object (GPO).

Answer: A

Explanation:

1. The HR department uses a custom application that can run only on Windows NT Workstation 4.0.
  2. Recently, users downloaded and installed unauthorized software from the Internet. This caused several computers on the company network to stop responding.
  3. All software must be approved for company use.
- Setting policies in the Default Domain Policy sets them for all computers in the domain. Taking the above into account, your design would be best suited if you configured the software restriction policy in the Default Domain Group Policy object. Software restrictions must be applied due to all the unauthorized downloading and installing of software from the Internet.

Incorrect Answers:

- B: A software installation policy can be used to distribute authorized software to users but it will not prevent the installation of unauthorized software.
- C: A firewall can protect an internal network from attackers on a public network by means of filtering ports and IP addresses. However, it cannot filter software.
- D: Group Policy provides several configuration options for systems within your enterprise environment. You can install software packages, configure desktop options, and configure Internet Explorer settings, and configure security settings just to name a few. However, this option will not be practical in the light of the way business is conducted.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 147

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 398, 633

---

**QUESTION 8**

You need to design phase one of the new authentication strategy for National Traders, Inc. You need to ensure that your solution meets the company's business requirements.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Install a Windows Server 2003 enterprise subordinate CA.
- B. Install a Windows Server 2003 stand-alone subordinate CA.
- C. Create a logon script for the client computers in the HR department.
- D. Configure certificate templates for autoenrollment.
- E. Install a Windows Server 2003 stand-alone root CA.

Answer: A, D

Explanation:

The root CA is the top of the CA hierarchy and should be trusted at all times. The certificate chain will ultimately end at the root C

A. The enterprise can have a root

CA as enterprise or a stand-alone C

A. The root CA is the only entity that can self

sign, or issue self certificates in the enterprise. Windows Server 2003 only allows one machine to act as the root C

A. The root CA is the most important C

A. If the root

CA is compromised, all the CAs in the enterprise will be compromised. Therefore, it is a good practice to disconnect the root CA from the network and use a subsidiary CA to issue certificates to users. Any CAs that is not the root CA is classified as subordinate CAs. The first level of subordinate CAs will obtain their certificates from the root C

A. These servers are commonly referred to as intermediary or policy CAs. They will pass on the certificate information to the issuing CAs down the chain. They are referred to as intermediary because they act as a "go-between" with the root CA and the issuing CAs.

Auto-enrollment for users is available under Windows Server 2003. Auto-enrollment features are set by CA administrators in the certificate templates. A user who is authorized to use these Certificate templates will be auto-enrolled.

1. I want to implement companywide user certificates as the first phase of our new

authentication strategy. I also want to manage our wireless network by using Group Policy objects (GPOs).

2. No users currently possess user certificates. Administrators do not have time to assist all users.

Thus you would design phase one of the new authentication strategy by installing a Windows Server 2003 enterprise subordinate CA and then configure certificate templates for autoenrollment.

Incorrect Answers:

B, E: You need to install a Windows Server 2003 enterprise subordinate CA and not a Windows Server 2003 stand-alone subordinate CA or a stand-alone root C

A. Stand-alone

CA does not have the ability to self sign.

C: There is no need to write logon scripts for the client computers in the HR department as PKI supports Windows NT 4.0.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 3, p. 159, 181

---

### **QUESTION 9**

You need to design a patch management strategy for National Traders, Inc. You need to ensure that your solution meets the company's business requirements.

What should you do?

A. Run the Microsoft Baseline Security Analyzer (MBSA) on all computers.

Use a Group Policy object (GPO) to configure all computers to use Automatic Updates to obtain the missing security patches from the Windows Update Web site.

B. Run the Security Configuration and Analysis console to analyze the security settings on all computers.

Use a Group Policy object (GPO) to configure all computers to use Automatic Updates to obtain and test the missing security patches from the Windows Update Web site.

C. Deploy a Software Update Services (SUS) test server named NT-SR09.

Obtain security patches from the Windows Update Web site and test them.

Use a Group Policy object (GPO) to configure all computers to automatically obtain approved updates from NT-SR09.

D. Deploy a Systems Management Server (SMS) test server named NT-DC01.

Obtain security patches from the Windows Update Web site and test them.

Use SMS to distribute approved updates to all computers.

Answer: C

Explanation: The current situation regarding patch management is as follows:

1. Our current patch management solution requires too much time and too many resources, and it needs to be optimized. We also need to be able to identify which security patches are installed on company computers.

Software Update Services (SUS) is used to leverage the features of Windows Update within a corporate environment by downloading Windows Update to a corporate server,

which in turn provides the updates to the internal corporate clients. This allows administrators to test and have full control over what updates are deployed within the corporate environment.

Under these circumstances your strategy would need to include deploying a SUS server, testing all security patches and approving them and then configure all client computers to automatically update from the server.

Incorrect Answers:

A: MBSA can perform local or remote scans of Windows systems. It verifies whether your computer has the latest security updates and whether there are any common security violation configurations that have been applied to your computer. However, you need to test the patches before they are applied.

B:

Security Configuration and Analysis tool is a Windows 2003 utility that is used to analyze and to help configure a computer's local security settings. Security Configuration and Analysis works by comparing the computer's actual security configuration to a security database configured with the desired settings. However, it does not check which security updates are installed.

D: SMS is a software solution uses to consolidate change and management tasks and can be used to distribute security updates and patches. However, Software Update Services (SUS) is the better system to use to automate the distribution of updates. You should also not test updates and patches on a domain controller.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide, p. 55

## Topic 9, International Retailers, Ltd., Scenario

### Background

International Retailers, Ltd. is a well recognized global import export business. The International Retailers, Ltd. group deals with different types of technologies from hardware appliances to cars and computer technologies.

### Physical Locations

International Retailers, Ltd. has its headquarters in Miami and three retail branch offices in Dallas, Chicago and Atlanta. The International Retailers, Ltd. departments are distributed as shown below in the table:

| Office  | Departments                                                          |
|---------|----------------------------------------------------------------------|
| Miami   | Finance, Corporate Services, IT, Sales, Marketing, Order Fulfillment |
| Dallas  | Sales, Order Fulfillment                                             |
| Chicago | Sales, Order Fulfillment                                             |
| Atlanta | Purchasing                                                           |

The International Retailers, Ltd. group owns three warehouses of inventory, one each in Miami, Dallas, and Chicago.

### Planned Changes

International Retailers, Ltd. are planning to use a new inventory and shipping management solution which allows wireless handheld computers in the warehouses to connect in real time to the inventory database.

International Retailers, Ltd. use a new Windows application named InternationalSales which is used to allow the remote sales to access key information on the inventory in stock and customer account information. InternationalSales will be run on a terminal server named IR-SR01. IR-SR01 will be required to access the database servers. IR-SR01 only has the InternationalSales user application running.

International Retailers, Ltd. has decided to launch a new Web site named thoughts.int-retailers.com which will be used by the public to allow them to submit ideas and sources for new products. This will ensure a brighter future with relations to International Retailers, Ltd. customers.

International Retailers, Ltd. also launched a new Web-based application named InternationalCustomer which will be used by the public to allow them to submit ideas and sources for new products. This will make sure that future relations are better. The International Customer will also allow larger companies to check the status of shipments and to place new orders. The InternationalCustomers Web application will use ASP.NET. The International Retailers, Ltd. group has decided to use the Dallas retail branch office as an internal help desk. International Retailers, Ltd. wants the help desk staff to be able to reset passwords, disable and enable user accounts, and clear account lock-outs for users in the Dallas retail branch office. The user accounts of the International Retailers, Ltd. company for the Dallas retail branch office staff will be members of the RetailHelpDesk global security group.

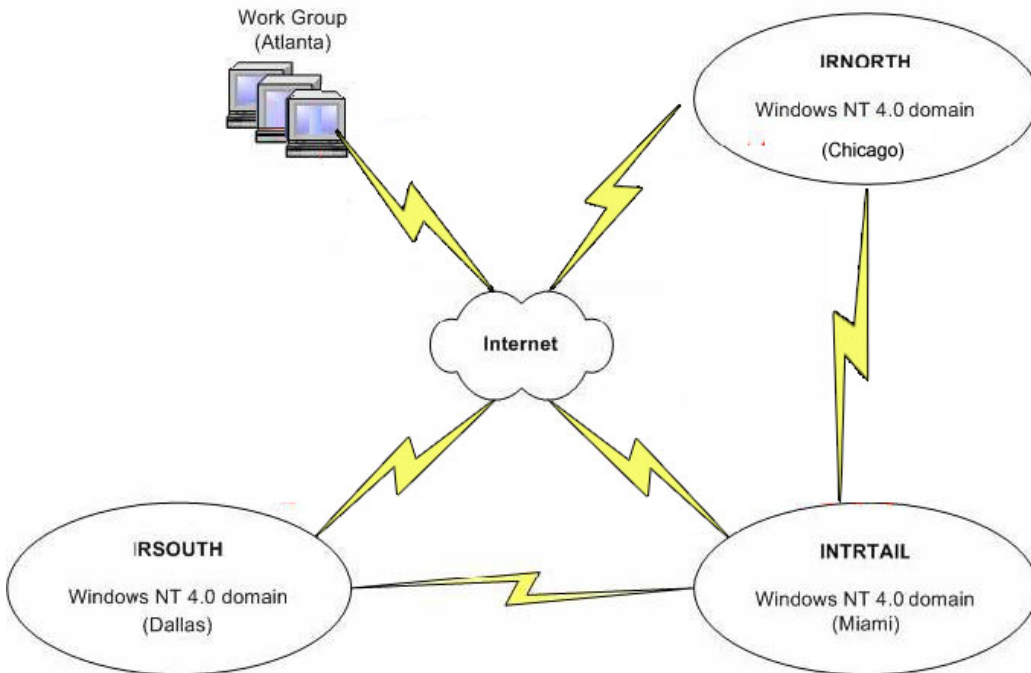
### **Business Process**

The International Retailers, Ltd. group has organized all the users of the Finance department to be members of the FinanceUsers global security group. The Finance department users make use of a server IR-SR02 which is dedicated for use by the Finance department.

The International Retailers, Ltd. group Atlanta retail branch office supports a large staff and hires additional contract agents. Most of the Atlanta retail branch office users work remotely from home or in remote locations.

### **Directory Services**

The existing physical and network topology of the International Retailers, Ltd. is shown below:

**Existing Network Topology**

International Retailers, Ltd. has configured the members of the int-retailers.com Domain Admins group so that they administer all three domains. International Retailers, Ltd. has granted some users in the dallas.int-retailers.com and chicago.int-retailers.com domains administrative privileges in their respective domains so that they can respond quickly to emergencies.

**Network Infrastructure**

International Retailers, Ltd. has all the network servers which provide information or resources to the entire company located in the Miami office. The server residing in the Miami office include eight Microsoft SQL Server database servers that run Windows Server 2003, and six Microsoft Exchange Server 5.5 mail servers that run Windows 2000 Server.

International Retailers, Ltd. has given the Dallas and Chicago retail branch offices their own local file and print servers that run Windows Server 2003, Windows 2000 Server, or Windows NT Server 4.0. The Dallas and Chicago retail offices also each has one Windows 2000 Server mail server that runs Microsoft Exchange Server 5.5. The International Retailers, Ltd. domain controllers currently run Windows NT Server 4.0. The Atlanta retail office network will be connected to the Miami network by an L2TP/IPSec VPN tunnel between two Windows Server 2003 Routing and Remote Access servers named IR-SR03 and IR-SR04. The IT department will be responsible of maintaining both IR-SR03 and IR-SR04 from the Miami network.

**Mobile Users**

International Retailers, Ltd. has the Miami-based sales department relying on an ISP with global dial-up numbers which are used when high-speed connections are not available. The International Retailers, Ltd. remote users first connect to the Internet and then they

connect to IR-SR03 by using a VPN. The Miami-based sales users make use of portable computers which are members of the int-retailers.com domain.

The International Retailers, Ltd. purchasing staff in the Atlanta retail office travel extensively to remote areas. International Retailers, Ltd. considers support from the IP department not to be easily accessible to users when they are not in the office.

### **Chief Executive Officer**

International Retailers, Ltd. considers having their data protected whilst the users in our sales department need remote access to some information to be efficient and responsive. International Retailers, Ltd. is planning to upgrade all client computers running operating systems older than Windows 2000 Professional to Windows XP Professional.

International Retailers, Ltd. also has plans to bring the Atlanta retail office into our domain structure. International Retailers, Ltd. considers it imperative that we have secure remote access to all servers and that we have remote access to the server in the Atlanta retail office to control travel costs.

International Retailers, Ltd. also wants to give local staff some administrative privileges without making them full domain administrators to decrease travel to other offices and lower costs. International Retailers, Ltd. also importantly considers how much work is needed to implement the design and whenever possible the minimum amount of administrative effort should be used to achieve our goals.

1. International Retailer wants all the employees to be able to digitally sign outgoing e-mail messages for the external contacts to verify that the message is legitimate.

International Retailers, Ltd. also wants all the employees to receive encrypted e-mail messages from other employees and external contacts.

2. International Retailers, Ltd. wants remote connections to private resources in the company to use an encrypted VPN. International Retailers, Ltd. also wants nonadministrative users not to be able to change security settings after the settings are deployed.

3. The company network will establish VPN connections only with previously approved computers.

4. International Retailers, Ltd. wants the portable computer users to encrypt confidential files stored on their portable computers. International Retailers, Ltd. also wants the desktop computer users allowed to encrypt confidential files on their desktop computers.

5. International Retailers, Ltd. wants the IT department to be able to recover encrypted files stored on any client computer.

International Retailers, Ltd. wants to support the written policies and promote a reliable environment. The Senior Network Administrator of International Retailers, Ltd. has specified the following requirements. International Retailers, Ltd. may make some exceptions in rare circumstances. The International Retailers, Ltd. requirements include:

1. International Retailers, Ltd. also has planned an automated monthly process which will discover the computers not running current operating system security patches and critical updates. The International Retailers, Ltd. group also wants security patches and critical updates to be tested. The IT department will be responsible for this then automatically and remotely deployed to all client computers.

2. International Retailers, Ltd. wants their users to be able to sign on with just one set of credentials. International Retailers, Ltd. also requires it to be possible to track which

resources are accessed by which users.

3. The International Retailers, Ltd. group wants the passwords used to establish VPNs to be changed at least every three months.

4. The International Retailers, Ltd. requires the call center computers to run only an e-mail application, a dedicated order processing application and Internet Explorer. The call centre computer users are permitted to connect to only Web servers operated by International Retailers, Ltd. when using the call centre computers. International Retailers, Ltd. also wants only the Finance department employees to access the data on IR-SR02. Any unauthorized attempts to access this data must be tracked.

5. International Retailers, Ltd. sees it as imperative that the customer data be protected as it is transmitted between the customer's Web browser and thoughts.int-retailers.com Web site.

6. International Retailers, Ltd. requires that only authorized users be permitted to access the InternationalCustomer application or to see the data it contains. International Retailers, Ltd. also wants all the InternationalCustomer information like user credentials and data be encrypted as it is transmitted over the Internet.

International Retailers, Ltd. has the following Active Directory requirements that must be considered.

1. International Retailers, Ltd. wants to have the Windows NT 4.0 domains in the Miami, Dallas and Chicago retail offices and the workgroup in the Atlanta retail office should be combined into a single Active Directory domain named ad.int-retailers.com. International Retailers, Ltd. also plans to have the domain contain a top-level organizational unit (OU) for each office. International Retailers, Ltd. then ensures that each top-level OU will contain additional OUs as required. The Miami office OU should also contain an OU for mobile users without assigned office locations.

2. International Retailers, Ltd. are considering having all domain controllers run Windows Server 2003 at the domain functional level and the forest functional level of Windows Server 2003. International Retailers also require a domain controller named IR-DC01 located in the Miami office. IR-DC01 will be configured as an enterprise CA that is chained to the offline, stand-alone root C

A. IR-DC01 will be used to issue certificates to users and computers.

3. The International Retailers, Ltd. group wants the Miami main office call center's 120 client computer accounts to be placed in one OU named InterCall Center. International Retailers, Ltd. wants the InterCall Center OU to be a child OU of the Miami top-level OU. If a network packet originates outside the company network the network configuration of the International Retailers, Ltd. group, it will be accepted or processed by the Web servers only if it is an HTTP or HTTPS packet.

4. The International Retailers, Ltd. group wants to have the IT department in the Miami office be able to manage the VPN tunnel between the Miami and Atlanta office. The International Retailers, Ltd. group also envisage that VPN credentials be changed regularly, without involving users in the Atlanta office. International Retailers, Ltd. will then also deploy a new stand-alone root certification authority (CA) that is offline from the network.

5. International Retailers, Ltd. group wants each of the network DHCP servers in the Miami office to be able to adequately support the network in Miami independently, if the

other server fails. The networks DHCP servers should not process any unauthorized packets.

## Topic 9, International Retailers, Ltd. (10 Questions)

---

### QUESTION 1

You work as a network administrator at International Retailers, Ltd. You have received instruction to start designing a strategy for e-mail. Your design will be required to meet all the International Retailers, Ltd. requirements for e-mail. What should you do?

- A. Group Policy objects (GPOs) and IPSec policies that require all client computers to use Kerberos authentication to connect to mail servers should be specified.
- B. IPSec encryption should be required on all TCP connections that are used to send or receive e-mail messages.
- C. An SSL server certificate should be acquired for each mail server from a commercial CA whose root certificate is already trusted.
- D. A certificate template that is suitable for S/MIME should be configured and published. A Group Policy object (GPO) should be deployed so that a certificate that is based on this template is automatically issued to all domain users.

Answer: D

Explanation: You should remember in the scenario all employees must be able to receive encrypted e-mail messages from other employees and external contacts. Also all employees must be able to digitally sign outgoing e-mail messages so that the external contacts can verify that the message is legitimate.

1. International Retailers, Ltd. also requires a domain controller named IR-DC01 located in the Miami office. IR-DC01 will be configured as an enterprise CA that is chained to the offline, stand-alone root C

A. IR-DC01 will be used to issue certificates to users and computers.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 3, p. 159, 181

---

### QUESTION 2

You work as a network administrator at International Retailers, Ltd. You have recently received instruction to start designing a security strategy for the DHCP servers in the Seattle office. You are required to select the appropriate actions to take in the scenario.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. : The discretionary access control lists (DACLS) in Active Directory should be modified so that only members of the Enterprise Admins security group can

authorize additional DHCP servers.

B. A digital certificate should be installed for SSL on each DHCP server.

C. An IPSec policy that allows only the packets necessary for DHCP and domain membership for each DHCP server should be used.

D. All unnecessary services should be disabled on each DHCP server.

Answer: C, D

Explanation: In the scenario you should keep in mind that DHCP is the method used in Windows Server 2003 to dynamically assign IP addresses for legitimate domain member computers. It is also possible that malicious users conceivably could attempt to lease all the IP addresses from a DHCP server resulting in the inability of legitimate computers to obtain an IP address.

1.

International Retailers, Ltd. group wants each of the network DHCP servers in the Miami office to be able to adequately support the network in Miami independently, if the other server fails. The networks DHCP servers should not process any unauthorized packets

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 2 & 5, pp. 249-250

---

### QUESTION 3

You work as a network administrator at International Retailers, Ltd. You have received instruction to start designing desktop and security settings for the client computers in the Miami call center. You are required to select which of the actions to perform. Your solution requires to be implemented by using the minimum amount of administrative effort.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. A Group Policy object (GPO) should be designed that enforces a software restriction policy on all client computers in the call center.

B. Assign the Deny - Read permission for all unauthorized executable files to the client computer domain accounts using NTFS permissions.

C. In the call center on each client computer you should configure a local policy that lists only authorized programs in the Allowed Windows Programs list.

D. A Group Policy object (GPO) should be designed that implements an IPSec policy on all client computers in the call center. Ensure that the IPSec policy rejects connections to any Web servers that the company does not operate.

Answer: A, D

Explanation: In the scenario you should keep in mind that the call center computers will run only an e-mail application, a dedicated order processing application, and Internet Explorer. The users are required to be permitted to connect only to

International.com operated web servers when using a call center computer.

Incorrect Answers:

B: In the scenario this options should not be used because this will not have the desired affect on the network.

C: This option should not be considered for use in the scenario because this action will not achieve the scenario objective.

1. The International Retailers, Ltd. requires the call center computers to run only an e-mail application, a dedicated order processing application and Internet Explorer. The call centre computer users are permitted to connect to only Web servers operated by International Retailers, Ltd. when using the call centre computers

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 2, pp. 51-52

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 147

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, pp. 398, 633

---

#### **QUESTION 4**

You work as a network administrator at International Retailers, Ltd. You have received instruction to start designing a method to allow the thoughts.int-retailers.com Web site. The Web site will e required to function in accordance with security and business requirements. What should you do?

- A. Traffic between Web browsers and the Web server should be required to use SSL.
- B. Certificate mappings between the Web server and Active Directory should be required.
- C. A PPTP VPN should be required for all connections to the Web server.
- D. Traffic between Web browsers and the Web server should be required to use an L2TP/IPSec tunnel.

Answer: A

Explanation: In the scenario you should remember to use SSL because SSL provides three major functions in encrypting Web-based traffic which are server authentication, client authentication and encrypted connections. Web page encryption is implemented using the Secure Sockets Layer (SSL) protocol.

1.

International Retailers, Ltd. has decided to launch a new Web site named thoughts.int-retailers.com which will be used by the public to allow them to submit ideas and sources for new products.

2. International Retailers, Ltd. sees it as imperative that the customer data be protected as it is transmitted between the customer's Web browser and new-thoughts.int-retailers.com

Web site.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 335

Elias N. Khnaser, Susan Snedak, Chris Peiris & Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 9 & 10, pp. 565, 642-645

---

### **QUESTION 5**

You work as a network administrator at International Retailers, Ltd. You have received instruction to start designing the configuration on one Windows Server 2003 terminal server hosting the InternationalSales application to meet security requirements. You are required to select from the following which actions to take. What should you do? (Choose all that apply.)

- A. Software restriction policies should be used in Group Policy objects (GPOs) that apply to the terminal server.
- B. The terminal server should be configured so that users log on by using domain accounts.
- C. The server should be configured to run InternationalSales in a dedicated window when a user logs on to the terminal server.
- D. The terminal server should be configured so that users log on by using domain accounts.
- E. The terminal server should be configured so that users log on by using local user accounts.
- F. Appsec.exe should be used to restrict applications on the terminal server.

Answer: A, B, C

Explanation: In the scenario you should try and remember that a new Windows application named InternationalSales will allow the remote sales force to access key information about inventory in stock and customer account information.

1. International Retailers, Ltd. wants their users to be able to sign on with just one set of credentials.
2. International Retailers, Ltd. are considering having all domain controllers run Windows Server 2003 at the domain functional level and the forest functional level of Windows Server 2003

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 21

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, p. 807

---

**QUESTION 6**

You work as a network administrator at International Retailers, Ltd. You have recently received instruction to start designing the configuration of the Windows Server 2003 Routing and Remote Access server in the Miami office. Your design should ensure that the configuration adheres to the business requirements. What should you do?

- A. The Routing and Remote Access server should be configured to use only IPSec over L2TP connections. Configure IPSec to use certificates.
- B. The Routing and Remote Access server should be configured to use only PPTP connections.
- C. A remote access policy should be configured on the Routing and Remote Access server to require MS-CHAP v2 for all connections.
- D. A Group Policy object (GPO) should be used to configure a Restricted Groups policy that applies to the Routing and Remote Access server. This Restricted Groups policy should then be used to remove all accounts from the local Users group, and then add authorized computer accounts.

Answer: A

Explanation: In the scenario you should always remember that remote connections to private resources in the company network must use an encrypted VPN. The L2TP with IPSec is used to provide for higher layer encapsulation and encryption features necessary for VPN connectivity.

1.

The Atlanta retail office network will be connected to the Miami network by an L2TP/IPSec VPN tunnel between two Windows Server 2003 Routing and Remote Access servers named IR-SR03 and IR-SR04. The IT department will be responsible of maintaining both IR-SR03 and IR-SR04 from the Miami network.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 335

---

**QUESTION 7**

You work as a network administrator at International Retailers, Ltd. You have recently received instruction to start designing the network to support the company's VPN requirements for mobile users who connect to the network in Miami. You are required to select which of the actions to perform. What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. IPSec policies should be configured on all Routing and Remote Access servers to require the use of digital certificates.
- B. A digital certificate that can be used for SSL should be acquired from a commercial CA for each computer that established a VPN connection.

- C. A password generator application should be used to create a pre-shared key, and distribute it to all mobile users.
- D. Computer autoenrollment should be used to create digital certificates that can be used to authenticate to a VPN server.

Answer: A, D

Explanation: In the scenario you should remember that auto-enrollment features are set by CA administrators in the certificate templates. The users who are authorized to use these Certificate templates will be auto-enrolled. In the scenario IPSec is an excellent part of the security solution for remote access as it is used to secure the communication channel between computers and to secure the data flowing across that channel.

1. International Retailers, Ltd. also require a domain controller named IR-DC01 located in the Miami office. IR-DC01 will be configured as an enterprise CA that is chained to the offline, stand-alone root C

A. IR-DC01 will be used to issue certificates to users and computers.

2. International Retailers, Ltd. wants remote connections to private resources in the company to use an encrypted VPN.

Incorrect Answers:

B: In the scenario you should not make use of the digital certificate as this will not help you achieve the scenario objective.

C: In the scenario making use of a password generator to issue pre-shared keys to mobile users will not support the mobile users.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 3 & 5, pp. 181, 250, 284-289

---

### **QUESTION 8**

You work as a network administrator at International Retailers, Ltd. You are in the process of designing the wireless networks for the three warehouses. You are required to have your design support the inventory and shipping management solution. Your design should meet the security requirements. What should you do?

- A. A server should be configured to use Internet Authentication Service (IAS). The wireless networking equipment should be configured to use the IEEE 802.1x protocol and the IAS server.
- B. A firewall should be created to block traffic to any IP address that did not originate from the company's DHCP servers. You should ensure that all wireless access points connect behind this new firewall.
- C. You should ensure that the IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g wireless networking protocols and all wireless networking equipment are fully supported.
- D. A random service set identifier (SSID) should be assigned to each wireless access

point. Broadcasting of SSIDs should be disabled on all wireless access points.

Answer: A

Explanation: In the scenario you should keep in mind that IAS provides a secure border control for wired/wireless network connections. The 802.1X standard is used to improve security because both the wireless client and the network authenticate to each other. A unique per-user/per-session key will be used to encrypt data over the wireless connection. The keys are dynamically generated, reducing administrative overhead and eliminating the ability to crack a key.

1. International Retailers, Ltd. are planning to use a new inventory and shipping management solution which allows wireless handheld computers in the warehouses to connect in real time to the inventory database.

Incorrect Answers:

A: In the scenario you should not consider assigning service set identifiers (SSIDs) to all access points and then disabling broadcasting.

B: In the scenario you should not create a firewall as it is inappropriate and will not achieve the scenario objective at hand.

C: In the scenario by ensuring the mentioned protocols are supported is not enough because the scenario objective will not be achieved.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide, p. 557

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 9, p. 325

---

### **QUESTION 9**

You work as a network administrator at International Retailers, Ltd. You have received instruction to start designing the settings for IR-SR02. You are required to specify which of the permissions will be used. You are also required to specify any additional settings required by International Retailers, Ltd.

What should you do?

A. All firewalls should be configured to track when any packets addresses to IR-SR02 are dropped.

B. An IPSec policy should be created that requires IPSec encryption between IR-SR02 and the firewall.

C. On IR-SR02 a digital certificate should be installed for Encrypting File System (EFS).

D. On the access to files and objects you should activate failure auditing.

Answer: D

Explanation: In the scenario you should remember that if Audit object access - if enabled, this setting triggers auditing of user access to objects such as files, folders, Registry keys, and so forth.

1. The International Retailers, Ltd. group has organized all the users of the Finance department to be members of the FinanceUsers global security group. The Finance department users make use of a server IR-SR02 which is dedicated for use by the Finance department. Any unauthorized attempts to access this data must be tracked.

Incorrect Answers:

A: In the scenario this action should not be used because the firewall is used to prevent intrusion attempts on IR-SR02.

B: In the scenario by applying IPSec encryption between IR-SR02 and the firewall will not work as you will be unable to track unauthorized access attempts.

C: In the scenario the digital certificate is not required as this will not track unauthorized access attempts.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 5 & 8, pp. 292-293, 481

---

### **QUESTION 10**

You work as a network administrator at International Retailers, Ltd. You have received instruction to start designing a Group Policy object (GPO) settings to support the use of the Encrypting File System (EFS). International Retailers, Ltd. requires that the solution you are busy designing meets business and security requirements of the company. You are required to select which of the actions you should perform

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. A data recovery agent should be designated and issue an EFS certificate to the data recovery agent.

The private key should be exported and restrict access to the exported key.

B. The data recovery agent should be made a local administrator on all client computers.

C. The default data recovery agent should be removed from the Default Domain Policy GPO. Then, include the new data recovery agent instead.

D. The Default Domain Policy GPO should be deleted. A new GPO linked to the domain should be configured that does not specify a data recovery agent.

Answer: A, C

Explanation: In the scenario you should remember that managing EFS throughout the organization requires Export private keys for recovery accounts on secure media. International Retailers, Ltd. wants only use the recovery agent account for file recovery. This keeps the credentials secure by limiting their use.

1. International Retailers, Ltd. considers data recovery to be important when employees leave the company or lose their private keys.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 9, p. 571-576

## Topic 10, Grand National Bank, Scenario

### **Background**

Grand National bank is a financial institution that provides personal and commercial banking services. In addition, Grand National Bank also provides financial and accounting services for customers. As part of the services that Grand National Bank offers its clientele, they operate a 24-hour call center.

Grand National Bank is divided into the following departments:

1. Accounts

\* Credit accounts

\* Debit accounts

\* Mortgage accounts

\* Loan accounts.

1. Investments

\* Long term Investments

\* Short term Investments

1. Accounting Services

2. Marketing

3. Human resources

4. Information Technology (IT)

### **Physical Locations**

The Grand National Bank head quarters are located in Chicago. There are 750 employees at the Chicago office.

There are two Grand National Bank regional offices: one is located in Los Angeles and the head quarters doubles as the other regional office. The Los Angeles office has 500 employees.

There are 100 branch offices located in major cities throughout the western United States. Each branch office has between 20 and 30 employees.

The Los Angeles Regional office services the branch offices that are located in California, Oregon, and Washington.

The Chicago Regional office/head quarters services the branch offices that are located in Colorado, New Mexico, Utah, and Arizona.

### **Business Processes**

The Chicago office hosts the Human Resources (HR) department.

There is a 24-hour call center in the Chicago and Los Angeles offices.

Both the Chicago office and the Los Angeles office have an IT department.

No IT personnel have been deployed in the branch offices.

The IT departments in these offices contain the data center, which provides the relevant IT services for its respective region.

The IT departments are responsible for all administrative tasks for the network, i.e. the help desk function.

### **The Existing IT environment:**

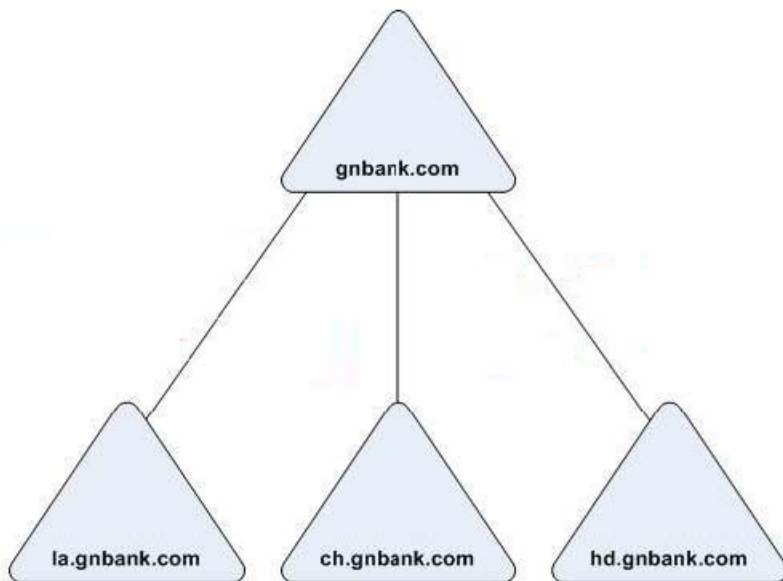
## Directory Services

The Grand National Bank network consists of a single Active Directory forest that contains four domains:

1. The forest root domain is named gnbank.com
2. The three child domains that have been created are named la.gnbank.com, ch.gnbank.com, hd.gnbank.com, respectively.

These are illustrated in the exhibit below.

**Active Directory Infrastructure**



The call center personnel user accounts are located in the hd.gnbank.com domain. The provision of support for both internal and external customers users are their responsibility.

The HR department members all belong to the CH-HRUsers group.

Each branch office has been designated as an organizational unit (OU).

Both la.gnbank.com and ch.gnbank.com contain OUs for the branch offices in their geographic area.

## Network Infrastructure

The Grand National Bank network servers all run Windows Server 2003.

The Grand National Bank network client computers run Windows XP Professional.

The Chicago and Los Angeles offices host the wireless access points.

These wireless access points support:

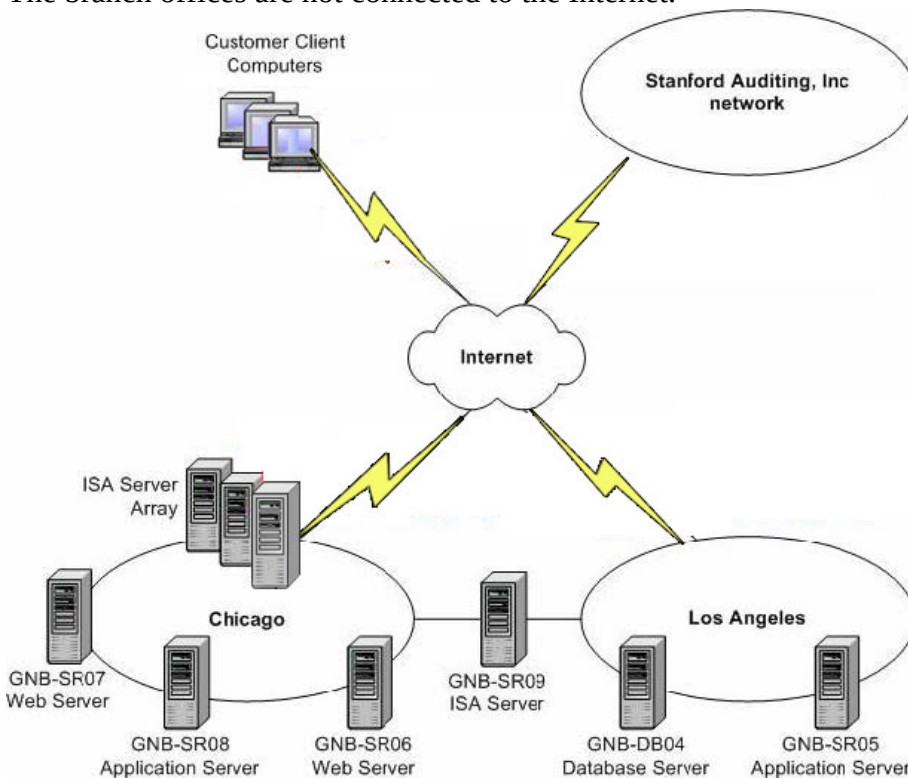
1. Support the IEEE 802.11q specification and Wired Equivalent Privacy (WEP) encryption.
2. Support the use of certificates and RADIUS for authentication.
3. Has no encryption or authentication methods configured.

There is a test network in the Chicago data center where security patches and updates are tested prior to deployment to the rest of the Grand National Bank network.

A dedicated WAN connection exists between the Chicago and Los Angeles offices. Both the Chicago and Los Angeles offices have a dedicated connection to the Internet.

A frame-relay line connects each branch office to its regional office.

The branch offices are not connected to the Internet.



A Web server named GNB-SR06 host:

1. an application that connects to a custom application hosted on a Windows Server 2003 computer in the Los Angeles data center
2. Web sites that contain publicity accessible information for both customers and the public.

The Chicago network has dual functionality in that it also functions as an extranet for partner company access.

A Web server named GNB-SR08 is installed in the Chicago data center. GNB-SR08:

1. runs IIS 6.0
2. hosts a Web site that is accessible by kiosk computers in each branch office
3. has membership of the Kiosk OU

The kiosk computers connect to the Web site using a user account named KioskUser.

### Problem statements:

#### Chief Information Officer

"Our core business revolves around handling confidential data and as such our success depends on our ability to efficiently secure our data. I am concerned with the security risks that the wireless network might pose to our network. With this in mind I want to ensure that only authorized users and computers access to the wireless network."

"I am also concerned about the possible compromise of our public key infrastructure (PKI). Such an occurrence would undermine the trust our customers place in our bank. Furthermore recovery would be very expensive in terms of time and money especially after trust has already been undermined. To ensure that our PKI is never compromised we should provide our partners and regular customers with access to the extranet. We will use smart cards to verify the identity of all users who access information from the Web-based application or Web site. These cards will contain a user certificate issued by

the Grand National Bank certification (CA). Smart card readers will be provided to these users as well."

We also need highly available and secure client/server application that will manage or largest customer's access to data. Data transmissions must be very secure and we must ensure this."

"I am also concerned that the kiosk computers in the branch offices could be used to compromise network security and to allow unauthorized access to company resources."

"We also have a problem with tellers at the branch offices running unauthorized applications on their computers."

### **IT Director**

"The Grand National Bank Written security policy states that all Windows updates and security patches should be tested in the test environment in the Chicago office before deployment to the production network. At present these updates are copied to a CD-ROM and delivered to all company locations either by mail or overnight delivery service or delivery by the administrators themselves. To sum it up: Patch Management as it is currently is time consuming, expensive and often requiring travel by IT personnel to all branch locations. Apart from the patch management system, the administrators also have to travel to branch offices to perform many maintenance tasks on the servers. We need to provide a secure method to perform these tasks without requiring the administrator to travel to the site. I want a method to deploy updates and automatically to all computers in the network."

"In the event of our administrators compelled to travel, they must be able to securely connect to and manage any server in his/her region using a laptop computer and dial-up ISP account. These administrators are allowed to connect remotely to the network and the remote access policies that govern their level of access are defined differently in each region. The managers in the regional IT departments make the decisions regarding their level of access. Regardless, I want to ensure that every administrator uses a secure connection when he/she remotely connects to the network via the Internet."

"Often it happens that after an administrator is added to perform a particular task, the administrator account often remains in the group after the task has been completed. This is meant to be temporary and we should take guard and ensure that these users are removed from the administrative security group as soon as the project is completed."

### **HR Manager**

"My greatest concern regards the unauthorized users that are able to access personnel information. Only HR users should have access to this information. Not even IT staff should be able to access this information."

### **Organizational Goals**

The following organizational requirements must be taken into consideration:

1. All IT personnel will be issued with new laptop computers that have wireless network adapters because they should be able to perform their administrative tasks even when not behind their desks.
2. Each call center user works six hours at the call center. Then for four hours after that they are on call. These users must be issued laptop computers and high-speed Internet access.

They must be enabled to use Terminal Services to run support applications from Windows Server 2003 computers in the call centers.

3. Grand National Bank partners with an external auditing company named Stanford Auditors, Inc. that provides audit services for customers. Stanford Auditors, Inc. users must have access to the extranet in the Chicago office. These users need to be able to access file resources that are located on a server on the Chicago internal network named GNB-SR01.

4. Branch office tellers must be able to run only a third-party application named BankTeller 2.0 on their computers. No other user applications must run on these computers, regardless of any actions taken by an end user. The regional offices users must be able to run their required applications.

The following Active Directory requirements must be taken into consideration:

1. The application used on the extranet application server requires changes to be made to the Active Directory schema. These changes must not affect the rest of the network.
2. Currently all branch office network administration is performed by administrators in the Chicago office or the Los Angeles office. The IT department wants to deploy a single administrator who will be responsible for all branch offices in a particular city. This administrator responsibility will include all user, group, and resource management for only the branch offices in his or her particular city.
3. Help desk personnel require the ability to perform limited administrative tasks like resetting users' passwords and creating new user accounts for branch office users in the ch.gnbank.com domain and the la.gnbank.com domain. They should not be able to perform any other administrative tasks.

The following network infrastructure requirements must be taken into consideration:

1. All connections made over the frame-relay WAN connections must be encrypted and authenticated.
2. At least one server in each domain should have Certificate Services installed. CA configuration must be based on the needs of each domain.
3. Both the ch.gnbank.com domain and the la.gnbank.com domain must have a Software Update Services (SUS) server installed.
4. The Microsoft Baseline Security Analyzer (MBSA) must be deployed to all computers in all domains.

The following security requirements must be taken into consideration:

1. Access to all personnel data that is stored on a server named GNB-SR02 will be restricted to only users in the HR department. Provision must be made to allow the IT personnel to perform backups and restore this data as scheduled.
2. All connections made by IT personnel from outside the network must use the strongest available encryption and authentication methods since they will be allowed to connect to the Grand National Bank network from home.
3. GNB-SR03 runs Terminal Services and is located on the extranet. All access to resources on the internal network must occur through GNB-SR03.
4. Customers must be granted access to their personal account information via the company Web site. All customers are issued smart cards and smart card readers. The smart cards also double as debit cards and to access personal account information. The smart cards contain a user certificate issued by a Grand National Bank certification authority (CA).

The following customer requirements must be taken into consideration:

1. Stanford Auditors, Inc. users need access to information stored on a Microsoft SQL Server 2000 database server named GNB-DB04 that is located on the Los Angeles internal network. Users on the internal network must also be able to access the information on GNB-DB04 by using Microsoft Access 2000.
2. Grand National Bank customers must be able to access their personal account information securely.
3. Kiosk computers must provide access to public bank information for Customers and prospective customers. Each branch office will contain at least one kiosk computer. All kiosk computers must run Microsoft Windows XP Professional.

## Topic 10, Grand National Bank (9 Questions)

---

### QUESTION 1

You need to design a remote access strategy for the call center users for when they are on call. In your solution you should take care to meet the security requirements. What should you do?

- A. Deploy an L2TP/IPsec VPN server in each call center.  
Configure the laptop computers as L2TP VPN clients.
- B. Configure IPsec tunnel mode connections between the Call center users' home and the Grand National Bank routers.
- C. Configure IP packet filters on the Grand National Bank routers to allow the Remote Desktop Protocol (RDP).  
Configure IPsec filters on GNB-SR03 to allow only RDP connections.
- D. Assign the Secure Server (Require Security) IPsec policy to the GNB-SR03.  
Assign the Client (Respond only) IPsec policy to the laptop computers.

Answer: A

Explanation: L2TP can encapsulate PPP frames just as PPTP can, but in contrast can then be sent over IP, ATM, or Frame Relay. It is rather more complicated than PPTP, and it is more secure. Bottom line: L2TP with IPsec to provide for higher layer encapsulation and encryption features necessary for VPN connectivity. This combination is known as L2TP/IPsec.

Requirements for an L2TP implementation of a LAN-to-LAN VPN: First, a user certificate needs to be installed on the calling router, and a computer certificate needs to be installed on the answering router.

Now consider the following:

1. Grand National Bank operates a 24-hour call center to support customers and partners.
2. The Chicago and Los Angeles offices each maintain a customer support call center.
3. IT personnel must be able to connect to the network from home. All connections made by IT personnel from outside the network must use the strongest available encryption and authentication methods.

You would thus need to deploy a L2TP/IPsec VPN server in each call centre and configure the laptop computers as L2TP VPN clients so as to comply with security requirements.

Incorrect Answers:

B: Creating IPSec tunnel mode connections between customer support users home and the company's Internet-facing routers is not going to comply with all the security requirements. A L2TP/IPSec VPN connection will be more suitable and secure.

C: This option does not comply with security requirements as stated in the case study.

D: Deploying a L2TP/IPSec VPN server in each call centre and configure the laptop computers as L2TP VPN client would be the best option and not just simply assigning IPSec policy.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 335

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 7, pp. 433-438

---

## **QUESTION 2**

You need to implement a certificate authority (CA) hierarchy to support the remote administration requirements. In your solution take care to meet the business and security requirements.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Deploy an offline enterprise root CA in each domain.
- B. Deploy an online enterprise root CA in the gnbank.com domain.
- C. Deploy an offline enterprise root CA in the gnbank.com domain.
- D. Deploy a subordinate issuing CA in each child domain.
- E. Deploy a standalone issuing CA in each child domain.

Answer: B, D

Explanation: The administrators will use Layer two Tunneling Protocol over IP Security (L2TP/IPSec) for the remote connections to ensure the security of these connections.

Using certificate based authentication will compel both the connecting computer and the VPN server to create L2TP/IPsec connections since both will require a computer certificate. To support L2TP/IPSec, you will need an enterprise certificate authority (CA) in the forest root domain and you should also deploy enterprise subordinate CA in each of the child domains. This will server as redundancy as well as fulfilling domain computers' requests for certificates.

Incorrect Answers:

A: A root CA is the highest level CA in the CA hierarchy. You should, in this scenario, have it in the root domain and online.

C: An offline enterprise root CA in the gnbank.com domain will not work in an L2TP/IPSec connection since both connecting computers need to sign both computer certificates.

E: Standalone CAs allows one to take the CA offline. This is not what is required. Besides not all Windows Server 2003 features can support standalone CAs.

**QUESTION 3**

You need to redesign the Grand National Active Directory structure to support the new client/server application. This means accommodating an access control strategy for resources that are located in the extranet for partners and for internal users. In your solution take care to meet business and security requirements. What should you do?

- A. Create a new child domain named extranet.gnbank.com in the existing forest. Create user accounts for Stanford Auditors, Inc. users in this domain. Create shortcut trusts in which the child domain trusts every domain in the forest.
- B. Create a new forest and domain named extranet.gnbank.com. Create all user accounts for Stanford Auditors, Inc. users in this domain. Create a one-way forest trust relationship in which the extranet forest trusts Stanford Auditors, Inc. forest.
- C. Create a new forest and domain named extranet.gnbank.com. Create user accounts for Stanford Auditors, Inc. users in this domain. Create an external trust relationship in which the extranet domain trusts the ch.gnbank.com domain.
- D. Create a child domain of the ch.gnbank.com domain for the extranet. Create user accounts for Stanford Auditors, Inc. users in this domain.

Answer: B

Explanation: With Windows Server 2003 one is allowed trust relationships between separate Active Directory forests. A forest is a security boundary. Forest trusts act much like domain trusts, except that they extend to every domain in two forests. Domains are connected to one another through logical structure relationships. The relationships are implemented through domain trees and domain forests.

A domain tree is a hierarchical organization of domains in a single, contiguous namespace. In the Active Directory, a tree is a hierarchy of domains that are connected to each other through a series of trust relationships (logical links that combine two or more domains into a single administrative unit). The advantage of using trust relationships between domains is that they allow users in one domain to access resources in another domain, assuming the users have the proper access rights.

A forest is a set of trees that does not form a contiguous namespace. For example, you might have a forest if your company merged with another company. With a forest, you could each maintain a separate corporate identity through your namespace, but share information across Active Directory.

1. Grand National Bank operates a 24-hour call center to support customers and partners.
2. Each call center user works six hours at the call center. Then for four hours after that they are on call. These users must be issued laptop computers and high-speed Internet access. They must be enabled to use Terminal Services to run support applications from Windows Server 2003 computers in the call centers.
3. Grand National Bank partners with an external auditing company named Stanford Auditors, Inc. This company provides audit services for customers. The audit company

must have access to the extranet in the Chicago office. These users need to be able to access file resources that are located on a server on the Chicago internal network named GNB-SR01.

4. Users from Stanford Auditors, Inc. require access to information stored on a Microsoft SQL Server 2000 database server named GNB-DB04 that is located on the Los Angeles internal network. Users on the internal network must also be able to access the information on the SQL Server by using Microsoft Access 2000.

Thus you would design your access control strategy by creating extranet.gnbank.com, a new forest and domain. After which you create user accounts for the users from the partner companies in the new domain and then create a one-way forest trust relationship in which the extranet forest trusts the company forest.

Incorrect Answers:

A: Child domains are not necessary. Furthermore shortcut trusts will not meet business and security requirements. What is necessary is a new forest and domain and a one-way trust in which the extranet forest trusts the company forest.

C: An external trust relationship is unnecessarily risky and will not comply with security requirements.

D: This will not work for the reasons stated in A and C above. And above all this would only represent half a solution.

---

#### **QUESTION 4**

You need to design an authentication strategy for the administrators of the IT department to remotely connect to the network. In your solution take care to meet security requirements.

What should you do?

A. Install Internet Authentication Services (IAS) on a server in the ch.gnbank.com domain. Configure the VPN servers as RADIUS clients.

B. Install Internet Authentication Services (IAS) on a stand-alone server in the Chicago extranet. And create local user accounts for the IT personnel on the IAS server.

C. Create a remote access policy on each of the VPN servers. And configure the policy to use the ch.gnbank.com to authenticate remote access users.

D. Create a remote access policy on each of the VPN servers. And then configure the policy to require L2TP to establish a connection

E. Create local user accounts for the IT personnel on the VPN servers.

Answer: A

Explanation: IAS in Windows Server 2003 allows for a centralized approach that implements a RADIUS server and a RADIUS proxy. The RADIUS server will provide centralized connection for authentication, authorization, and accounting functions for networks that include wireless access, VPN remote access, Internet access, extranet business partner access, and router-to-router connections. IAS proxy functions are different from these server functions, and include forwarding IAS authorization and accounting information to other IAS servers.

IAS is installed as an optional server in Windows Server 2003, and is not installed by

default. Therefore, we need to add IAS manually to our Windows Server 2003.

There are several remote access methods in an enterprise: dial-in client desktops, VPN clients, and wireless devices in our demonstration. The dial-in clients will connect to a dial-in server. The VPN clients will connect to a VPN server. The wireless devices will access the network through a wireless access server. All three servers will connect to a Windows Server 2003 RADIUS IAS proxy machine. This proxy will channel the requests to the IAS server. The IAS server will communicate with the DC and the Active Directory to perform authentication duties.

The Chicago and Los Angeles offices host the wireless access points.

These wireless access points support:

1. Support the IEEE 802.11q specification and Wired Equivalent Privacy (WEP) encryption.
2. Support the use of certificates and RADIUS for authentication.
3. Has no encryption or authentication methods configured.
4. The IT department is responsible for all administrative tasks for the network. There are no IT personnel at the branch offices.
5. All IT personnel will be issued with new laptop computers that have wireless network adapters because they should be able to perform their administrative tasks even when not behind their desks.
6. All IT personnel have new laptop computers that have wireless network adapters.
7. IT personnel must be able to connect to the network from home. All connections made by IT personnel from outside the network must use the strongest available encryption and authentication methods.

Therefore you should install IAS on a server in the ch.gnbank.com domain and configure the VPN servers as RADIUS clients to meet the security requirements for remote access of the users in the IT department.

Incorrect Answers:

B: There is not need to create local user accounts for the IT personnel on a stand-alone IAS server. This option will not meet security requirements.

C: You should configure the VPN servers as RADIUS clients to ensure that the strategy meets the security requirements and not make use of a remote access policy that requires L2TP to establish a connection.

D: This option will not work in these circumstances.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 6, pp. 369-370

---

### **QUESTION 5**

You need to design an access control solution for customer information that is transmitted over the Internet. In your solution take care to meet security requirements.

What should you do? (Each correct answer presents part of the solution. Choose THREE.)

- A. Disable anonymous access to the Web site.
- B. Configure the Web site to use only Microsoft .NET Passport authentication.

- C. Configure the Web site to require SSL connections.
- D. Configure a custom local IPSec policy on the Web servers to require IPSec communications.
- E. Configure the Web site to require client certificates.
- F. Enable and configure client certificate mapping on the Web site.
- G. Configure the IPSec policy to use certificate-based authentication and encryption.

Answer: C, E, F

Explanation:

Authenticated client access to a secure site - With SSL you can provide access to authenticated clients to a secure site by requiring both client and server certificates and by mapping those certificates. Client certificates can be mapped on a one-to-one basis or a many-to-one basis via Active Directory Users and Computers. You can create a group of designated users, map the users' certificates to the group, and give the group permission to access the secure site.

1. Customers must be able to access personal account information by means of the company Web site. All customers are issued smart cards and smart card readers. The smart cards are used by customers as debit cards and to access personal account information. The smart cards contain a user certificate issued by a Grand National Bank certification authority (CA).
2. Bank customers must be able to securely access their personal account information.
3. Customers and prospective customers must be able to access public bank information by means of kiosk computers running Windows XP Professional. Each branch office will contain at least one kiosk computer.

To comply with security requirements while designing an access control strategy for customer information, taking the above into account, you should configure the Web site to require SSL connections and require client certificates. After that you should enable and configure client certificate mapping on the site.

Incorrect Answers:

A: Disabling anonymous access to the Web site and will not comply with security requirements as it would be allowing non-registered users access.

B: Making use of only Microsoft .NET Passport authentication will not work in this scenario.

D: IPSec is best used for packet filtering and is thus not suited for securing a Web server.

G: IPSec is used for host-to-host security along specific paths and is thus not suited to be used to authenticate or encrypt Web servers.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 6, p. 404

---

## **QUESTION 6**

You need to design a security strategy that will ensure that no unauthorized users are able to access personnel data.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. In the Default Domain Policy Group Policy object (GPO) for the gnbank.com domain, add the CH-HRUsers group to the Restricted Groups list.
- B. In the Default Domain Policy Group Policy object (GPO) for the ch.gnbank.com domain, add the CH-HRUsers group to the Restricted Groups list.
- C. In the Default Domain Policy Group Policy object (GPO) for the ch.gnbank.com domain, add the CH-HRUsers group and the Backup Operators group to the Restricted Groups list.
- D. Add only the HR department user accounts to the Allowed Members list.
- E. Add only the HR department user accounts and the administrator user accounts to the Allowed Members list for each group.
- F. Add only the administrator user accounts to the Allowed Members list for the Backup Operators group.

Answer: A, D

Explanation: Setting policies in the Default Domain Policy sets them for all computers in the domain.

Thus you should design the security strategy that will ensure no unauthorized access to personnel data by adding the CH-HRUsers group to the Restricted Groups list and in addition add only the HR department user accounts to the Allowed Members list in the Default Domain Group Policy object for the ch.gnbank.com domain. Especially when you take the following into consideration:

1. All members of the HR department are members of a group named CH-HRUsers.
2. I am concerned about unauthorized users being able to access personnel information. Only HR users should have access to this information. Not even IT staff should be able to access this information.
3. All personnel data is stored on a server named GNB-SR02. Access to personnel data must be restricted to only users in the HR department. However, IT personnel must be able to backup and restore this data as scheduled.

Incorrect Answers:

A: This option suggests application to the wrong domain.

C: Only the CH-HRUsers group should be added to the Restricted Groups list and not the Backup Operators group as well.

E: Only the HR department user accounts should be added to the Allowed Members list in the ch.gnbank.com domain and not the administrator user accounts.

F: This option suggests the correct domain, but the Backup Operators group should not be considered in this scenario.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 147

**QUESTION 7**

You need to design a PKI solution. In your solution take care to meet business and security requirements.

What should you do?

- A. Implement an enterprise root CA in the gnbank.com domain.  
Implement subordinate CAs in both the ch.gnbank.com and the la.gnbank.com domains.  
Take the root CA offline.
- B. Implement an enterprise root CA in the gnbank.com domain.
- C. Implement an enterprise root CA in both the ch.gnbank.com and the la.gnbank.com domains.  
Take the enterprise CA in each domain offline.
- D. Implement an enterprise root CA in the gnbank.com domain.  
Implement a stand-alone root CA in both the ch.gnbank.com and the la.gnbank.com domains.

Answer: A

Explanation: The root CA is the top of the CA hierarchy and should be trusted at all times. The certificate chain will ultimately end at the root C

A. The enterprise can

have a root CA as enterprise or a stand-alone C

A. The root CA is the only entity

that can self sign, or issue self certificates in the enterprise. Windows Server 2003 only allows one machine to act as the root C

A. The root CA is the most important

C

A. If the root CA is compromised, all the CAs in the enterprise will be compromised. Therefore, it is a good practice to disconnect the root CA from the network and use a subsidiary CA to issue certificates to users. Any CAs that is not the root CA is classified as subordinate CAs. The first level of subordinate CAs will obtain their certificates from the root C

A. These servers are commonly referred to as intermediary or policy CAs. They will pass on the certificate information to the issuing CAs down the chain. They are referred to as intermediary because they act as a "go-between" with the root CA and the issuing CAs.

Following is the relevant information regarding the PKI solution required by Grand National Bank:

1. "I am also concerned about the possible compromise of our public key infrastructure (PKI). Such an occurrence would undermine the trust our customers place in our bank. Furthermore recover would be very expensive in terms of time and money especially after trust has already been undermined.

2. Grand National Bank customers must be access their personal account information securely

Customers must granted access to their personal account information via the company Web site. All customers are issued smart cards and smart card readers. The smart cards

also double as debit cards and to access personal account information. The smart cards contain a user certificate issued by a Grand National Bank certification authority (CA). Thus in the current situation you thus need to implement an enterprise root CA in the gnbank.com domain. Implement subordinate CAs in each child domain and then take the root CA offline.

Incorrect Answers:

B: This option is risky and only suggests half of the design needed to comply with business and security requirements.

C: You should not implement the enterprise root CA in each of the child domains. This can result in a compromise if too many domains are enabled to issue certificates.

D: Implementing a stand-alone root CA in each of the child domains is an unnecessary security risk.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 3, p. 159, 181

---

### **QUESTION 8**

You need to design an authentication solution for wireless network access for the administrators in their regions. Your solution must meet business and technical requirements.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. Deploy an offline enterprise root CA in the gnbank.com domain.

Deploy subordinate enterprise root CAs in both the ch.gnbank.com and the la.gnbank.com domain.

Install Internet Authentication Service (IAS) on a member server in both the ch.gnbank.com domain and the la.gnbank.com domain.

B. Deploy an enterprise root CA in each domain.

Install Internet Authentication Service (IAS) on a member server in the gnbank.com domain.

Install the Routing and Remote Access service (RRAS) on a member server in both the ch.gnbank.com domain and the la.gnbank.com domain.

Configure these servers as RADIUS clients.

C. Deploy user certificates to all administrators and computer accounts that have wireless network adapters.

Configure each laptop computer to use Protected EAP (PEAP) for authentication purposes.

D. Deploy computer certificates to all laptop computers that have wireless network adapters.

Configure each laptop computer to use EAP-MS-CHAP v2 for authentication.

Answer: A, C

Explanation: The root CA is the top of the CA hierarchy and should be trusted at all times. The certificate chain will ultimately end at the root C

A. The enterprise can have a root CA as enterprise or a stand-alone C

A. The root CA is the only entity that can self sign, or issue self certificates in the enterprise. Windows Server 2003 only allows one machine to act as the root C

A. The root CA is the most important C

A. If the root CA is compromised, all the CAs in the enterprise will be compromised. Therefore, it is a good practice to disconnect the root CA from the network and use a subsidiary CA to issue certificates to users. Any CAs that is not the root CA is classified as subordinate CAs. The first level of subordinate CAs will obtain their certificates from the root C

A. These servers are commonly referred to as intermediary or policy CAs. They will pass on the certificate information to the issuing CAs down the chain. They are referred to as intermediary because they act as a "go-between" with the root CA and the issuing CAs.

WEP and WPA provide secure communication, but some method must be used to authenticate users. Different 802.1X-based WLANs offer different solutions to this need. The preferred solution within the Windows Server 2003 environment is the use of the IETF standard called Extensible Authentication Protocol (EAP). EAP can make use of various authentication methods that are based on passwords, public key certificates or other credentials.

Thus when you take the information pertaining to wireless network access, mentioned below, into account, then options A and C is the solution.

1. The network consists of four Active Directory domains in a single forest.
2. All servers run Windows Server 2003. All client computers run Windows XP Professional.
3. Wireless access points are installed in the Chicago and Los Angeles offices. The wireless access points support the IEEE 802.11q specification and Wired Equivalent Privacy (WEP) encryption.
4. Currently, no encryption or authentication methods are configured on the wireless access points.
5. A dedicated WAN connection exists between the Chicago and Los Angeles offices.
6. A frame-relay line connects each branch office to its regional office. The branch offices are not connected to the Internet.
7. The Chicago and Los Angeles offices each have a dedicated connection to the Internet.
8. IT personnel must be able to perform administrative tasks even when they are not at their desks. All IT personnel have new laptop computers that have wireless network adapters.

Incorrect Answers:

B: Employing an enterprise root CA in each domain is not advisable. Furthermore IAS should be installed on one member server in the ch.gnbank.com domain and one member server in the la.gnbank.com domain.

D: This option will not comply with business requirements. While EAP-MS-CHAP v2 protects user credential during authentication by sending a hash to the authenticator, it does not use a secure channel for authentication, therefore the hash that is transmitted

during authentication can be captured and the associated password can be guessed by way of a possible offline dictionary attack.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 3 & 5, pp. 159, 181, 316

---

### **QUESTION 9**

You need to design a method implement a patch management system. In your solution take care to meet technical requirements.  
What should you do?

A. Deploy a Software Update Services (SUS) server in the test network at the Chicago office.

Deploy regional SUS servers to receive the administrator-approved updates from the test network SUS server.

Configure all Grand National Bank client computers to receive the updates from their respective regional SUS server.

B. Deploy a Windows Server 2003 computer running Software Update Services (SUS) in the test network.

Configure all Grand National Bank client computers to receive the updates from the test SUS server.

C. Install MBSA on a Windows Server 2003 computer in the network.

Deploy MBSA as a Windows Installer package to all computers in the child domains, and configure MBSA to scan for updates from the server in the test network.

D. Install Internet Information Services (IIS) on a Windows Server 2003 computer in the test network.

Create a Web site named Updates on this server.

Configure an autoupdate policy in each child domain to download and deploy updates from the Updates Web site

E. Deploy a Software Update Services (SUS) server in the regional offices.

Configure each SUS server to download updates from the Windows Update servers on the Official Microsoft Windows Update site.

Configure all Grand National Bank client computers to receive the updates from the appropriate regional SUS server.

Answer: A

Explanation: Software Update Services (SUS) is used to leverage the features of Windows Update within a corporate environment by downloading Windows Update to a corporate server, which in turn provides the updates to the internal corporate clients. This allows administrators to test and have full control over what updates are deployed within the corporate environment.

1. A Software Update Services (SUS) server must be installed in each regional office domain. The Microsoft Baseline Security Analyzer (MBSA) must be deployed to all computers in each domain.

2. The Chicago data center includes a test network for testing security patches and updates before they are deployed to the rest of the network.

Deploying a Windows Server 2003 computer to run the SUS in the test network and then deploying SUS servers in each child domain, and then configuring the client computers to get their updates from their regional SUS servers is the solution.

Incorrect Answers:

B: Making use of Autoupdate policies in each child domain as described in this option is not the solution since it does not mention that the downloads will be administrator approved updates from the test network SUS server. This is not recommended since you will then be introducing a single point of failure into the system. If the test SUS server is to fail then all clients would be unable to receive updates.

C: MBSA verifies whether your computer has the latest security updates and whether there are any common security violation configurations that have been applied to your computer. This is not what is required in this question.

D: Installing IIS is not the option to be taken in this scenario.

E: This solution does not ensure administrator tested and approved updates to all client computers.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 477

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 2, p. 51

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide, p. 55

## Topic 11, International Pisces Breeders, Scenario

### **International Pisces Breeders Overview**

International Pisces Breeders is an international company which specializes in breeding with marine aquatic animals which includes cross breeding different fish species which can be bought by customers in North America and Europe.

International Pisces Breeders Physical Locations

The International Pisces Breeders main office is located in New York. International Pisces Breeders additionally currently has three branch offices in the following locations:

1. Seattle
2. London
3. Madrid

### **International Pisces Breeders Planned Changes**

International Pisces Breeders has recently decided that they should enter into a joint venture with Bilco Aquatic, a worldwide breeding professional company. The Bilco Aquatic network consists of a single Windows 2000 Active Directory domain named bilco.com which has not planned to upgrade its servers to Windows Server 2003.

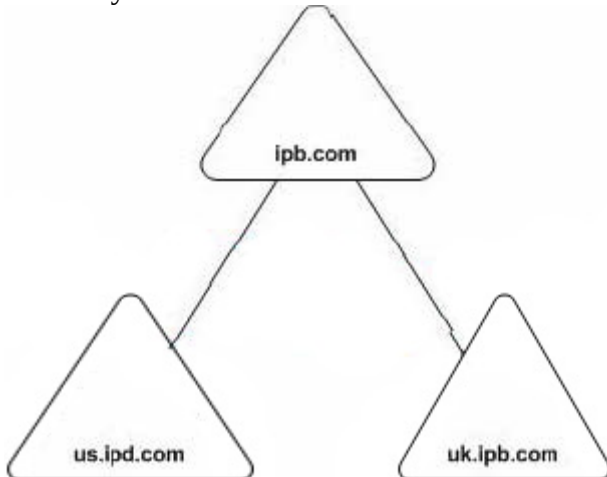
International Pisces Breeders is aware that the collaboration between the two companies will take place entirely over the Internet. International Pisces Breeders wants to ensure

that users from both companies will access a shared folder name Customer Data, which will be located on a Windows Server 2003 computer on the International Pisces Breeders internal network.

International Pisces Breeders wants to ensure that all their client computers in Madrid will be upgraded to Windows XP Professional.

### **International Pisces Breeders Directory Services**

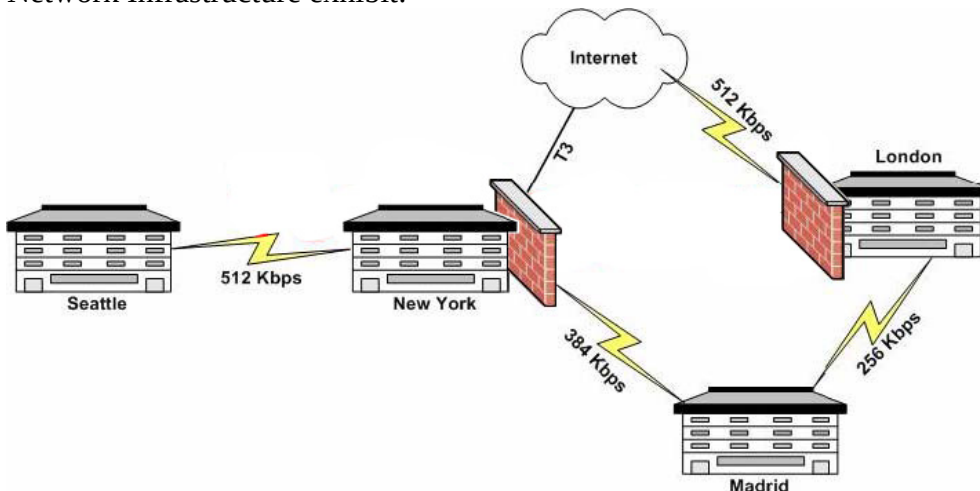
The International Pisces Breeders existing Active Directory forest is shown in the Active Directory Infrastructure exhibit.



The International Pisces Breeders network consists of a single Windows Server 2003 Active Directory forest which contains three domains named ipb.com, us.ipb.com, and uk.ipb.com

### **International Pisces Breeders Network Infrastructure**

The International Pisces Breeders existing network infrastructure is shown in the Network Infrastructure exhibit:



International Pisces Breeders makes use of a Windows Server 2003 Web server is located in the New York office perimeter network. International Pisces Breeders has configured all client computers in North America run Windows XP Professional and each office was configured to contain a domain controller. The domain controllers also serve as file and print servers.

### **International Pisces Breeders Problem Statements**

International Pisces Breeders wants to have the following business problems considered:

1. International Pisces Breeders knows that currently it is difficult to maintain all client computers with the latest security patches.
2. International Pisces Breeders also discovered that unauthorized users have modified the registry on some servers. Unauthorized users must not be able to modify the registry on company servers.
3. International Pisces Breeders additionally knows that access to resources is assigned per user, which causes administrative overhead. This administrative overhead must be reduced

International Pisces Breeders Chief Information Officer

The International Pisces Breeders chief information officer has discovered during the past year that they have focused on preventing external threats. International Pisces Breeders recently came to understanding that they should also prevent internal threats. International Pisces Breeders has also discovered that there was recently, confidential customer information was released to the public and it is suspected that unauthorized users are attempting to delete files. It is because of this that International Pisces Breeders has decided that they need to review which users have access to company resources periodically whilst avoiding increasing expenses, so we must use our existing infrastructure's security features to meet our security needs.

International Pisces Breeders Business Requirements

International Pisces Breeders wants to have the following business requirements considered:

1. International Pisces Breeders wants to ensure that security patches must be installed by using the minimum amount of WAN bandwidth.
2. International Pisces Breeders wants to have the information technology (IT) department in each office to test security patches before deploying them to client computers.
3. International Pisces Breeders also need all the client computers to be kept up-to-date with critical updates and security patches when Microsoft issues them. The company thus thinks it is imperative that the IT administrator should approve the updates.

International Pisces Breeders Written Security Policy

International Pisces Breeders wants to have the company's written security policy adhered to which includes the following requirements:

1. International Pisces Breeders wants to have all customer information must be kept confidential. All access to customer information must be tracked.
2. International Pisces Breeders additionally wants to ensure that the marketing information and service offering literature is available to the public. International Pisces Breeders wants to be able to track unauthorized modification of the marketing information only.
3. International Pisces Breeders wants to have the management to be able to access company financial information that is stored in Microsoft SQL Server 2000 databases and in shared folders.
4. International Pisces Breeders also wants to have all e-mail messages sent between International Pisces Breeders and Bilco Aquatic to be encrypted.

5. International Pisces Breeders also decided that they should have all authorized users autoenrolled in certificate services to access company resources.
6. International Pisces Breeders considers it as imperative that all the content updates to the Web server must be protected from interception.
7. International Pisces Breeders additionally wants it required that all remote server administration must be conducted over an encrypted channel.
8. International Pisces Breeders wants to ensure that Remote Desktop for Administration cannot be used to connect to servers on the perimeter network.

## Topic 11, International Pisces Breeders (8 Questions)

---

### QUESTION 1

You need to design an access control strategy that meets business and security requirements of International Pisces Breeders whilst ensuring the design solution minimizes forestwide replication.  
What should you do?

- A. You should consider creating a local group on each server and add the authorized users as members.  
You should then assign appropriate permissions for the file and printer resources to the local groups
- B. You should consider creating a universal group for each location, and add the respective users as members.  
You should then assign the universal groups to file and printer resources and finally assign permissions by using the universal groups
- C. You should consider creating a global group for each department and a global group for each location.  
You should then add users to their respective departmental groups as members and place the departmental global groups within the location global groups.  
You should finally assign the location global groups to file and printer resources in their respective domains, and then assign permissions for the file and printer resources by using the location global groups
- D. You should consider creating a universal group for each location and add the respective users as members.  
You should then assign the universal groups to file and printer resources.  
You should finally assign the permissions by using the universal groups

Answer: D

Explanation: A global group is a type of group used to organize users who have similar network access requirements. It is simply a container of users and global groups (in native mode) from the local domain.  
Domain local groups are used to assign permissions to resources. Domain local groups can contain user accounts, universal groups, and global groups from any domain in the tree or forest. A domain local group can also contain other domain local groups from its own local domain. Microsoft recommends that global groups be added to domain local

groups in a single domain environment and that universal groups are added to the domain local group in a multi-domain environment. You would need to make use of a global group for each department and add the respective users as its members, create domain local groups for file and printer resources. After which you should add the global groups to the respective domain local groups and then assign permissions using the domain local groups for the different resources. This should comply with security requirements while servicing business operational requirements.

1. All customer information must be kept confidential. All access to customer information must be tracked.
2. We must use our existing infrastructure's security features to meet our security needs. Also, we suspect that unauthorized users are attempting to delete files. Therefore, we need to review which users have access to company resources periodically.

Incorrect Answers:

A: A local group is a group that is stored on the local computer's accounts database. This is not the answer in this scenario.

B: Creating universal groups would be creating a special type of group used to logically organize global groups and appear in the Global Catalog (a search engine that contains limited information about every object in the Active Directory). Universal groups can contain users (not recommended) from anywhere in the domain tree or forest, other universal groups, and global groups. This will obviously result in forest wide replication which should be kept to a minimum.

C: This option will result in unnecessary replication taking place.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows (r) Server 2003 Environment Management and Maintenance Study Guide, p. 167

---

## **QUESTION 2**

You need to design a remote administration solution for servers on the internal network. The solution you design must meet the business and security requirements of International Pisces Breeders.

What should you do?

- A. You should consider requiring administrators to make use of Remote Desktop for Administration connections to manage the servers
- B. You should consider permitting administrators to manage the servers by using Microsoft NetMeeting
- C. You should consider permitting only administrators to connect to the servers' Telnet service
- D. You should consider permitting administrators to use an HTTP interface to manage servers remotely

Answer: A

Explanation: If you look closely the question asks about servers on the internal network. The Case study as cited below says RDP cannot be used on servers on the perimeter

network. The requirement cited is not valid since the question is asking about the internal network, not the perimeter network.

---

**QUESTION 3**

You need to design a method of deploying security configuration settings to all servers in the domain.

What should you do?

- A. Run the Resultant Set of Policy wizard with a Windows Management Instrumentation (WMI) filter on each department's Server OU.
- B. Log on to each server and use the System Policy Editor to configure the server's security settings.
- C. Create a customer security template and import the security to a GPO. Link the GPO to each department's Server OU.
- D. Create a customer security template. Log on to a domain controller in the Chicago office and use the secedit command to import the security template.

Answer: C

Explanation: You can define a base security template on a single computer and then export the security template to all the servers in your network. The security template is used as a comparative tool. You do not set security through the security template. Rather, the security template is where you organize all of your security attributes in a single location. Once you have configured a security template, you can import it for use. To deploy security configuration settings to servers you should first create a customer security template and then a group policy object to import the security template. After that you link the GPO to each department's Server OU.

Incorrect Answers:

A: Resultant Set of Policy (RSOP) is a new feature of Windows Server 2003 that provides the ability to see exactly how the various policies within the domain will apply to a specific user or computer. However, you do not just want to view how and which policies are applied, you need to create a method to deploy security configuration settings.

B: This option suggests an administratively intensive procedure. Furthermore it ignores the fact that a standard set of security settings should be deployed which should have been configured and managed from a central location.

D: This command is used to force updates on policies. But this implies that the security policy is already in place and only being edited.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, pp. 127-128, 173

---

**QUESTION 4**

You need to design a method to encrypt confidential data. The design solution must address the concerns of the chief information officer.

What should you do?

- A. You should consider requiring encrypted connections to all file servers
- B. You should consider encrypting all marketing information on file servers and client computers
- C. You should consider requiring encrypted connections to the public Web site, which is hosted on the Web server on the perimeter network
- D.  
You should consider encrypting customer information when it is stored and when it is being transmitted

Answer: D

Explanation: The Chief information officer is concerned about customer data that is leaked to the public. You thus need to encrypt this information when stored as well as when it is being transmitted.

1. Recently, confidential customer information was released to the public. Also, we suspect that unauthorized users are attempting to delete files. Therefore, we need to review which users have access to company resources periodically. We must avoid increasing expenses, so we must use our existing infrastructure's security features to meet our security needs.

Incorrect Answers:

A: Encrypted connections to all the file servers will also render information other than the confidential data encrypted. This is not what is needed.

B: You need to keep the customer information confidential. Marketing information is for public consumption. "Marketing information and service offering literature is available to the public. Humongous Insurance must track unauthorized modification of the marketing information only."

C: Encrypted connections to the public Web site hosted on the Web server on the perimeter network will not work in this scenario.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 9, pp. 571-576

---

### **QUESTION 5**

You need to design a method to update the content on the Web server. The design solution must meet business and security requirements of International Pisces Breeders.

What should you do? (Choose TWO.)

- A. You should consider using Web Distributed Authoring and Versioning (WebDAV) over and SSL connection to the Web server to update content
- B. You should consider using FTP over an IPSec connection to transfer content to the Web server
- C.  
You should consider using Telnet to connect to the Web server, and then perform content changes directly on the server

- D. You should consider installing the Microsoft FrontPage Server Extensions, and use FrontPage to update content
- E. You should consider using SSH to encrypt content as it is transferred to the Web server on the perimeter network

Answer: A, B

Explanation:

A: WebDAV is a file sharing protocol that is commonly used in Windows Internet-related applications. It is a secure file transfer protocol over intranets and the Internet. You can download, upload, and manage files on remote computers across the Internet and intranets using WebDAV. WebDAV is similar to FTP. WebDAV always uses password security and data encryption on file transfers (FTP does not support these tasks). Thus making use of WebDAV over SSL connection should comply with the company's security requirements.

B: The File Transfer Protocol (FTP) is a valuable component of IIS 6.0. FTP is used to "swap" or "share" files between servers and clients. This could be dangerous practice for businesses with sensitive information. Most large organization firewalls will block FTP access. We need to implement FTP communication over a secure channel like VPN. VPNs use the Point-to-Point Tunneling Protocol (PPTP) or Secure Internet Protocol (IPSec) to encrypt data and facilitate secure FTP communication. We can also use SSL encryption on WebDAV supported directories for the same purpose.

Incorrect Answers:

C: You should enable the Telnet service only if you see a real need for it, especially since the other administrative tools at your disposal offer more features and far better security. The Telnet service should remain disabled unless a need arises that requires it. In this instance it would be unnecessary.

D: Making use of Microsoft FrontPage Server Extensions and updating the content with FrontPage will not comply with security requirements.

E: SSH is independent of the operating system and is therefore suitable for use in a mixed operating system environment. However, not all terminal concentrators provide built-in security functions, so you'll need to consult with the vendor's documentation to see what, if any, security is provided. Thus this option is a security risk.

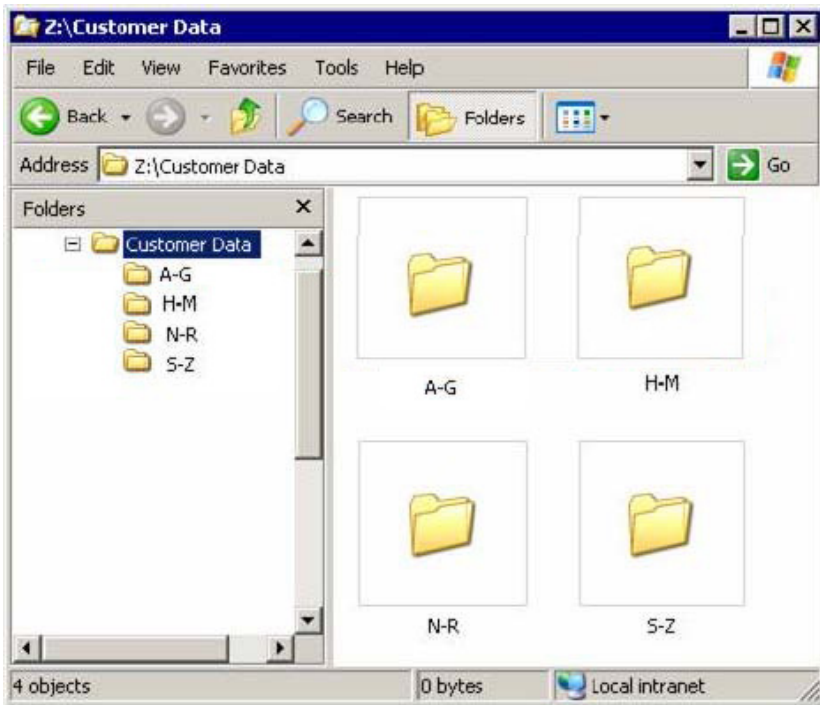
Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 4 & 6, pp. 208, 383-384, 386

---

## **QUESTION 6**

You need to design a monitoring strategy for the folders that contain customer information, which are shown in the Customer Data window below:



What should you do?

- A. You should consider auditing directory access failures
- B. You should consider using Security Configuration and Analysis to enable auditing on only the Customer Data folder
- C. You should consider auditing failure of object access on only the Customer Data folder
- D. You should consider auditing success and failures for object access on the Customer Data folder and all subfolders

Answer: D

Explanation: Audit object access If enabled, this setting triggers auditing of user access to objects such as files, folders, Registry keys, and so forth. As with the other audit policies, you can either monitor the success or failure of these actions. To be able to track all the access to customer information you will need to audit both success and failures for object access on the folder in question.

1. All customer information must be kept confidential. All access to customer information must be tracked.

Incorrect Answers:

A: Auditing directory access failures will not work in this scenario where more is expected.

B: The Security Configuration and Analysis tool is used to analyze and to help configure a computer's local security settings. Security Configuration and Analysis works by comparing the computer's actual security configuration to a security database configured with the desired settings. This is not the same as tracking all access to the Customer data folders and subfolders.

C: Auditing failure of object access only will only constitute half of the tracking that is needed as per the company's written security policy.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 2 & 8, pp. 64-66, 481-485

---

### **QUESTION 7**

You need to design a solution that ensures that the network users are kept up-to-date with the latest security patches as Microsoft releases them. You are required to select which of the following tools can be used to identify all the missing security updates on network computers.  
What should you do?

- A. Run the gpresult.exe tool
- B. Run the qfecheck.exe tool
- C. Run the qchain.exe tool
- D. Run the mbsacli.exe tool

Answer: D

Explanation: In the scenario you should remember in order for the administrator or person in charge to identify which security updates have not been applied that you should make use of the mbsacli.exe tool.

1. International Pisces Breeders knows that currently it is difficult to maintain all client computers with the latest security patches.

Incorrect Answers:

A: This option should not be used in the scenario because the utility is used to provide a listing of Group Policy settings and the Resultant Set of Policy (RSOP) for a user's computer.

B: This option should not be used in the scenario because the utility is used to track patches that have been installed on Windows 2000 computers only.

C: In the scenario you should not consider using the qchain.exe because the utility is used to install multiple patches or hot fixes in series.

---

### **QUESTION 8**

You need to evaluate making all business office users administrators on their client computers. You are required to design a method to ensure that this change can be made in a manner that meets business and security requirements.  
What should you do?

- A. You should consider configuring registry access auditing for all registry keys that are considered sensitive by the company's written security policy on all client computers
- B. You should consider implementing logon auditing for all user account logons on all domain controllers.
- C. You should consider implementing registry access auditing for all registry keys that

are considered sensitive by the company's written security policy on all domain controllers

D. You should consider implementing logon auditing for all user account logons on all client computers.

Answer: A

Explanation:

To be able to identify unauthorized user access as well as making users the administrators on their own computers, you need to configure registry access auditing for all registry keys that is regarded as sensitive in lieu with the company's written security policy. "... there was recently, confidential customer information was released to the public and it is suspected that unauthorized users are attempting to delete files. It is because of this that International Pisces Breeders has decided that they need to review which users have access to company resources periodically whilst avoiding increasing expenses, so we must use our existing infrastructure's security features to meet our security needs"

This option would be justified if you keep in mind the user's comment about other users stealing passwords and the company's written policy regarding the fact that they want to monitor and track when business office users attempt to make a system registry configuration change to their computers. We do not need to monitor or track everyday actions on client computers.

Incorrect Answers:

B: It is a case of checking the registry access auditing to be able to identify unauthorized access and comply with company's written security policy.

C: Implementing registry access auditing on the domain controllers will not ensure that administrators will be able to identify and track unauthorized access and comply with the company's written security policy.

D: Auditing on the client computers would be correct in this case. However, auditing the logon for all user accounts will not address your concern of checking unauthorized access.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris & Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 9, p. 541

## Topic 12, Consolidated Traveling Solutions, Scenario

### **Consolidated Traveling Solutions Overview**

Consolidated Traveling Solutions is a large company that specializes in booking customers their flights right around the world from a single office.

### **Consolidated Traveling Solutions Physical Locations**

The Consolidated Traveling Solutions main office is near the center of the city. The main office includes a business office and a courier dispatch lounge where couriers pick up their assignments.

### **Consolidated Traveling Solutions Business Processes**

Consolidated Traveling Solutions are well aware that the business staff handles customer billing, accepts phone calls for new courier assignments, and enters the assignments into a custom, Active Directory-integrated, client-server application.

Consolidated Traveling Solutions has also decided that the couriers use Web kiosk in the lounge to pick up their assignments. The Web kiosks run only Internet Explorer. Couriers use a password to log on to the subsystem, and they are supposed to log off after they read their assignments. Consolidated Traveling Solutions has recently decided that the couriers should be paid according their assignment, they must log in and mark each assignment as complete to be paid. Consolidated Traveling Solutions has also ensured that the couriers do not have physical access to the business office. The company always experiences a high rate of turnover among the courier staff.

1. Consolidated Traveling Solutions are totally aware that the information technology (IT) department has one senior administrator and two junior administrators who provide all IT support for company users and couriers.
2. Consolidated Traveling Solutions has also recently stated that the business staff requires access to mail servers, file servers, and client-server applications on the company LAN. Couriers need access to only the specialized Web-based application that is available to them on the Web kiosk in the dispatch lounge.
3. Consolidated Traveling Solutions knows that the network currently, access to resources is secured by using NTFS permissions and Active Directory-integrated application-specific authentication.
4. Consolidated Traveling Solutions wants to have all of their customer billing and contact information to remain confidential.

There are however also couriers that are employed on a permanent basis and they have been issued with laptop computers. All authentications to the wireless portion of the Consolidated Traveling Solutions network should be strictly controlled. The company should ensure that user credentials for portable computers and desktop computers are tightly controlled using two-factor authentication.

### **Consolidated Traveling Solutions Directory Services**

The Consolidated Traveling Solutions network consists of a single Active Directory domain. The network also makes provision for wireless network access. All users have domain user accounts. The senior IT administrator centrally manages all accounts.

### **Consolidated Traveling Solutions Directory Services**

The Consolidated Traveling Solutions network consists of a single Active Directory domain. All users have domain user accounts. The senior IT administrator centrally manages all accounts.

#### **Consolidated Traveling Solutions Network Infrastructure**

The Consolidated Traveling Solutions network consists of the following three segments:

1. Segment 1 contains all server computers.
2. Segment 2 contains all business staff client computers.
3. Segment 3 contains all dispatch lounge courier kiosks.

Consolidated Traveling Solutions makes use of a router connects the three segments. The router also connects the LAN to the Internet and provides basic firewall services. The

Internet connection has a range of 64 to 256 Kbps of bandwidth.

Consolidated Traveling Solutions knows that there are five Windows Server 2003 computers on Segment 1.

Consolidated Traveling Solutions knows that the courier dispatch lounge contains only Windows XP Professional client computers.

Consolidated Traveling Solutions business office contains client computers that run the following operating systems:

1. Windows 2000 Professional
2. Windows 98 Second Edition
3. Windows NT Workstation 4.0
4. Windows XP Professional
5. Windows 95

### **Consolidated Traveling Solutions Problem Statements**

Consolidated Traveling Solutions are well aware that access to customer data and courier assignments is not sufficiently secure. Consolidated Traveling Solutions has discovered that couriers use simplistic passwords and often guess other couriers' passwords.

Consolidated Traveling Solutions have also discovered that in the past, couriers have gained unauthorized access to confidential customer data. The company has no means of discovering who gained unauthorized access. As a result the company wants all users to make use of smart cards and PINs to access company resources. All users must also be responsible for their own PIN.

### **Consolidated Traveling Solutions Chief Executive Officer**

The Consolidated Traveling Solutions chief executive officer is well aware that though some of our data is not confidential, we need to increase security for our data that is confidential. Consolidated Traveling Solutions chief executive officer are aware that they have had major security problems in the past, including compromised confidential customer data. The Consolidated Traveling Solutions chief executive officer is additionally aware that this is a problem because we are contractually obliged to protect customer data. We also need to be able to identify users who do gain unauthorized access. To achieve our goals, we can spend money on security, but we cannot increase the number of employees.

### **Consolidated Traveling Solutions Chief Information Officer**

The Consolidated Traveling Solutions chief information officer is aware that our IT staff use their administrative accounts for everything which is acceptable on their own client computers. Consolidated Traveling Solutions are additionally aware that they often log on to business office client computers with their own administrative account, and they forget to log off after they are done. Consolidated Traveling Solutions has recently discovered that consequently, business office users can perform tasks by using administrator privileges, which creates network problems.

Consolidated Traveling Solutions chief information officer is also aware that we also struggle to maintain client computers and services with current security patches.

Consolidated Traveling Solutions is aware that though IT staff test security patches when they come out, they cannot always find the time to deploy them. Consolidated Traveling

Solutions has also discovered that we cannot use Windows Update on client computers because of our low Internet bandwidth. To conserve bandwidth, our firewall prevents client computers from accessing Windows Update. So, although servers have access to Windows Update administrators often forget to run it.

Solutions to these problems cannot require any more ongoing work from IT staff.

**Consolidated Traveling Solutions Senior IT Administrator**

The Consolidated Traveling Solutions senior IT administrator is aware that the junior administrators need to help to create new user accounts. However, they are not currently authorized to create new administrative staff accounts or to edit any existing accounts. Consolidated Traveling Solutions wants to ensure that although company policy allows junior administrators to only reset passwords, the domain permissions do not currently allow them to do so.

### **Consolidated Traveling Solutions Junior IT Administrator**

The Consolidated Traveling Solutions junior IT administrator has recently stated that our biggest security patch management problem is that our users are not administrators on their computers. Consolidated Traveling Solutions are also aware that even though we would need to track user administrative actions, I think we should make users administrators on their own computers.

### **Consolidated Traveling Solutions Courier**

The Consolidated Traveling Solutions courier is aware that they should pick a difficult password, but can only remember so much. The Consolidated Traveling Solutions courier has decided to use the same password all over to simplify their lives. The Consolidated Traveling Solutions have also been informed that couriers watch and steal other courier's passwords, but it has never happened to me.

Consolidated Traveling Solutions written security policy contains the following requirements:

1. Consolidated Traveling Solutions wants to ensure that they monitor and track when business office users attempt to make system registry configuration changes to their computers. Consolidated Traveling Solutions are aware that they do not need to monitor or track everyday actions on client computers.
2. Consolidated Traveling Solutions has additionally decided that they must monitor and track all access to sensitive company data, including most customer data and courier assignments.
3. Consolidated Traveling Solutions also wants to ensure that they maintain all computers with current security patches for critical updates. Consolidated Traveling Solutions are well aware that the senior IT administrator is responsible for first testing all patches and then releasing them to all client and server computers in the company.
4. Consolidated Traveling Solutions also wants to ensure that they must limit the use of user accounts that have domain administrators or other administrator privileges. Only IT staff will have access to domain administrative accounts.

## **Topic 12, Consolidated Traveling Solutions (9 Questions)**

---

**QUESTION 1**

You need to evaluate making all business office users administrators on their client computers. You thus need to design a method to ensure that this change can be made in a manner that meets business and security requirements.

What should you do?

- A. You should consider configuring registry access auditing for all registry keys that are considered sensitive by the company's written security policy on all client computers
- B. You should consider implementing logon auditing for all user account logons on all domain controllers.
- C. You should consider implementing registry access auditing for all registry keys that are considered sensitive by the company's written security policy on all domain controllers
- D. You should consider implementing logon auditing for all user account logons on all client computers.

Answer: A

Explanation: To be able to identify unauthorized user access as well as making users the administrators on their own computers, you need to configure registry access auditing for all registry keys that is regarded as sensitive in lieu with the company's written security policy.

1. We also need to be able to identify users who gain unauthorized access.
2. We should make users administrators on their own computers.
3. We must monitor and track when business office users attempt to make a system registry configuration change to their computers. We do not need to monitor or track everyday actions on client computers.

This option would be justified if you keep in mind the courier's comment about other couriers stealing passwords and the company's written policy regarding the fact that they want to monitor and track when business office users attempt to make a system registry configuration change to their computers. We do not need to monitor or track everyday actions on client computers.

Incorrect Answers:

B: You do not need to audit logon on the user accounts on the domain controllers. It is a case of checking the registry access auditing to be able to identify unauthorized access and comply with company's written security policy.

C: Implementing registry access auditing on the domain controllers will not ensure that administrators will be able to identify and track unauthorized access and comply with the company's written security policy.

D: Auditing on the client computers would be correct in this case. However, auditing the logon for all user accounts will not address your concern of checking unauthorized access.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris & Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 9, p. 541

**QUESTION 2**

You need to identify potential security threats. Which of the following security breaches might occur under the current IT and security practices?

- A. You should consider that all users could use their user accounts to gain the ability to install untested security patches on their client computers
- B. You should consider that the business office staff could discover couriers' passwords and use them to access couriers' information
- C. You should consider that the couriers could gain access to domain administrator privileges
- D. You should consider that it could be a virus that infects an IT administrator's client computer could gain domain administrator privileges.

Answer: D

Explanation: According to the Business process employed in the company, it would be easy for a virus that infects an IT administrator's client computer and gain domain administrator privileges to occur. Consider the following businesses practices in Consolidated Traveling Solutions:

1. Couriers use simplistic passwords and often guess other couriers passwords. In the past, couriers have gained unauthorized access to confidential customer data. The company has no means of discovering who gained unauthorized access.
2. To conserve bandwidth, our firewall prevents client computers from accessing Windows Updates.
3. Couriers use a Web kiosk in the lounge to pick-up their assignments.
4. Couriers do not have physical access to the business office.
5. Business staff handles customer billing, accepts phone call for new courier assignments, and enters the assignment into a custom, Active Directory-integrated, client server application.

Incorrect Answers:

A: Installing untested security patches on client computers by all the users will not happen since there is currently a firewall in place that will prevent client computers from accessing Windows Updates.

B:

Business office staff accessing couriers' information will only occur as far as the assignment gets entered into a custom, active Directory -integrated, client-server application under the current circumstances.

C: Couriers are already working, and do not have physical access to the business office, for the company and them gaining access to domain administrator privileges, is not considered as great a risk by the company as a virus that has the potential to gain domain administrator privileges. Also under the current circumstances NTFS permissions are in place to negate this type of risk.

Reference:

Roberta Bragg, MCSE Self-Paced Training Kit (Exam 70-298): Designing Security for a Microsoft Windows Server 2003 Network, p. 1:17

**QUESTION 3**

You need to design a method for junior IT administrators to perform more IT support tasks whilst ensuring your design solution meet business and security requirements.

What should you do?

A. You should consider creating new domain user accounts for each junior IT administrator.

You should then create new domain user accounts for each junior IT administrator.

B. You should consider making the junior IT administrators' domain user accounts member of the local Administrators group on all client computers

C. You should consider creating a custom Microsoft Management Console (MMC) that uses taskpad views to enable the appropriate tasks for the junior IT administrators

D. You should consider adding the junior IT administrators' user accounts to the Domain Admins user group

E. You should consider delegating appropriate Active Directory permissions to the junior IT administrators

Answer: E

Explanation: The junior administrators currently do not have authorization to do more administrative tasks as the domain permissions will not allow them. With NTFS permissions in place you have a situation where access to resources is secured by using NTFS permissions and Active Directory-integrated application-specific authentication. Consider the following information:

1. The information technology (IT) department has one senior administrator and two junior administrators who provide all IT support for company users and couriers.
2. The junior administrators need to help create new user accounts. However, they are not currently authorized to create new administrative staff accounts or to edit any existing accounts. Although company policy allows junior administrators to only reset passwords, the domain permission do not currently allow them to do so.

Incorrect Answers:

A: To create new domain user accounts for the junior IT administrators and instructing them to use it only for appropriate use is impractical.

B: Making junior administrators' accounts part of local Administrators group on all client computers will only work when all accounts are joined to a domain.

C: This option will not grant the junior administrators with appropriate permissions to carry out their tasks.

D: All user accounts are currently domain user accounts. Thus this option will not accomplish anything new.

Reference:

Roberta Bragg, MCSE Self-Paced Training Kit (Exam 70-298): Designing Security for a Microsoft Windows Server 2003 Network, pp. 9:10-14

Elias N. Khnaser, Susan Snedak, Chris Peiris & Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 4 & 8, pp.

201, 455

---

**QUESTION 4**

You need to design security changes that provide maximum protection for customer data and courier assignments.

What should you do?

A. You should consider modifying the Default Domain Policy Group Policy object (GPO) so that couriers must use complex user account passwords.

You should then require all couriers to change their passwords the next time they log on to the Web application

B. You should consider using Encrypting File System (EFS) to encrypt all files that contain customer data

C. You should consider creating a separate domain for courier authentication

D. You should consider implementing smart card authentication for business office users and couriers, upgrading client operating systems as needed.

You should then modify the Web kiosks to require smart card presence for continued access

Answer: D

Explanation: Smart cards provide a secure method of logging on to a Windows Server 2003 domain. Smart cards are physical cards that contain a certificate. This certificate identifies a user to Windows. Using smart cards is more secure than standard logons, because users must have possession of their card to logon. Smart cards are protected with a pin code in case of accidental loss or theft. In addition to logging on to a domain, smart cards are used for client authentication to applications and for securing e-mail. Since it is stated that money can be spent on security, this would be the option best suited for the company's requirement.

Incorrect Answers:

A: Making use of complex user account passwords will not be as effective as smart card authentication especially in view of couriers stealing each other's passwords.

B: Encrypting all files containing customer data does not mean preventing access to encrypted files.

C: A separate domain for courier authentication is not feasible in the circumstances in which the company operates. Couriers get their assignments from kiosk computers that are on the domain. Putting them in a different domain will disable them accessing their assignments.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, p. 283

---

**QUESTION 5**

You need to improve the company's security patch management process. You must ensure that your design solution meet existing business requirements and it cannot increase the number of employees or unnecessarily increase ongoing administrative

effort.

What should you do?

A. You should consider installing the Active Directory Client Extensions on all Windows 95, Windows 98, and Windows NT Workstation 4.0 computers.

You should then manually download all security patches to a Distributed File System (DFS) replica.

You should finally instruct all users to use the DFS replica to install security patches

B. You should consider installing the Active Directory Client Extensions on all Windows 95, Windows 98, and Windows NT Workstation 4.0 computers.

You should then install a Software Update Services (SUS) server and make all users local administrators on their client computers

C. You should consider upgrading all client computers to either Windows 2000 Professional or Windows XP Professional.

You should then make all users members of the Power Users group on their client computers

D. You should consider providing all users with the ability to access and use the Windows Update Web site

E. You should consider upgrading all client computers to either Windows 2000 Professional or Windows XP Professional.

You should then implement Software Update Services (SUS)

Answer: E

Explanation: Take into consideration the following:

1. To conserve bandwidth, our firewall prevents client computers from accessing Windows Updates.

2. We also struggle to maintain client computers and services with current security patches. Though IT staff test security patches when they come out, they cannot always find the time to deploy them. We cannot use windows Update on client computers because of our low Internet bandwidth.

3. So, although servers have access to windows Update administrators often forget to run it.

This option will accommodate the utilization of group policy objects to apply the company's security patch management process.

Incorrect Answers:

A: This option involves far too much administrative effort that can be avoided if one follows option B's reasoning.

B: This option will grant too many rights to the users than is advisable.

C:

By making all users are members of the Power Users group on their client computers will allow members to have the ability to manage accounts, resources, and applications that are installed on a workstation, stand-alone server, or member server. Administrative tasks that can be performed by members of this group include creating local users and groups; modifying and deleting accounts that they have created; removing users from the Power Users, Users, and Guests groups; installing most applications; and creating and

deleting file shares. However, this group does not exist on domain controllers. This is not advisable in this scenario and neither can it be done.

D: Providing all the users with access and use of the Windows Update Web site will allow all user to be able to access all update patches whether they are tested or not.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, p. 807

---

### **QUESTION 6**

You need to design a smart card issuance system that will meet the company's security requirements. You need to take certain steps in the design to issue the smart cards.

What should you do?

A. All smart card recipients must register online before a smart card is issued via registered mail to their primary address.

A temporary PIN must be issued online to each smart card holder which must be changed when the recipient receives the card.

B. All smart card recipients must, in person, sign a security agreement when issued the smart cards at the company offices.

Smart card recipients should present two forms of identification: one should have a photo.

A temporary PIN must be issued to each smart card holder which must be changed during the card-issuance process.

C. All smart card recipients will receive their smart cards via certified mail to their primary address.

Smart card recipients should present a company bill or correspondence as proof of identity.

A complex PIN in a sealed security envelope must be issued to each smart card holder.

D. Smart card recipients should present at least a company bill or correspondence as form of identification.

All recipients should register for their smart cards by providing detailed information using the Web-based application form.

A complex PIN must be issued to each smart card recipient.

Answer: B

Explanation: Using smart cards and two-factor authentication will provide added security to the authentication process for the remote users. Each recipient should actually go to the company offices in person, with two types of identification, one which is at least a government issued identity document that has photo identification. There they should sign a security agreement when receiving a temporary PIN. This temporary Pin must be used by the recipient at a Smart Card Enrollment station to immediately establish a new private PIN. Thus no employee will have access to a recipient's PIN which makes

the recipient fully responsible for the security of the new PIN.

Incorrect Answers:

A: Recipients should not be allowed to register online as a form of identification. This can be risky. Further allowing the employee to establish the PIN online albeit temporary adds additional risk to the number of individuals who have access to the PIN. And it also reduces the recipient's responsibility for smart card security.

C: Mailing smart cards is not recommended, even if the mail is certified. This will definitely violate the security requirements. Using a company bill does not provide the required level of security.

D: Making use of complex PINs in sealed security envelopes will make it difficult for the PIN to be stolen, but this would not be user friendly. It may require some recipients to write it down which makes it vulnerable to compromise. This option is akin to registering online which should not be allowed.

---

### **QUESTION 7**

You need to design an authentication method for the portable computers used on the network and still provide the desired level of security?

- A. Two-factor authentication.
- B. MS-CHAP v2.
- C. 802.1x authentication.
- D. IPSec authentication.

Answer: A

Explanation: When two-factor authentication is implemented, users will be required to swipe smart card into a smart card reader and then enter a PIN to authenticate to the computer. Before a smart card is used, the user's logon certificate, public key, and private key must be programmed on the smart card. You can program the smart card using a Smart Card Enrollment station, which is integrated with certificate services. You can use the EAP-TLS protocol for certificate and smart card authentication.

Incorrect Answers:

B: MS-CHAP v2 does not support smart cards and does not provide the required two-factor authentication.

C: IEEE 802.1x authentication is a certificate-based standard that supports authenticated network access to wired Ethernet networks from 802.11 networks which is wireless. This method will provide support for centralized user identification, authentication, dynamic key management and accounting. This is ideal for wireless LAN implementations.

D: IPSec is used to generate keys for encrypting data during PPTP and L2TP tunneling transmissions. It is not a user authentication protocol.

---

### **QUESTION 8**

You need to design a method of deploying security configuration settings to all servers in the domain.

What should you do?

- A. Log on to each server and use the System Policy Editor to configure the server's security settings.
- B. Run the Resultant Set of Policy wizard with a Windows Management Instrumentation (WMI) filter on each department's Server OU.
- C. Create a customer security template. Log on to a domain controller in the Chicago office and use the secedit command to import the security template.
- D. Create a customer security template and import the security to a GPO. Link the GPO to each department's Server OU.

Answer: D

Explanation

: You can define a base security template on a single computer and then export the security template to all the servers in your network. The security template is used as a comparative tool. You do not set security through the security template. Rather, the security template is where you organize all of your security attributes in a single location. Once you have configured a security template, you can import it for use. To deploy security configuration settings to servers you should first create a customer security template and then a group policy object to import the security template. After that you link the GPO to each department's Server OU.

Incorrect Answers:

A: This option suggests an administratively intensive procedure. Furthermore it ignores the fact that a standard set of security settings should be deployed which should have been configured and managed from a central location.

B: Resultant Set of Policy (RSOP) is a new feature of Windows Server 2003 that provides the ability to see exactly how the various policies within the domain will apply to a specific user or computer. However, you do not just want to view how and which policies are applied, you need to create a method to deploy security configuration settings.

C: This command is used to force updates on policies. But this implies that the security policy is already in place and only being edited.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, pp. 127-128, 173

---

### **QUESTION 9**

You need to design a solution that ensures that the network users are kept up-to-date with the latest security patches as Microsoft releases them. You are required to select which of the following tools can be used to identify all the missing security updates on network computers.

What should you do?

- A. Run the gpresult.exe tool
- B. Run the qfecheck.exe tool
- C. Run the qchain.exe tool
- D. Run the mbsacli.exe tool

Answer: D

Explanation: In the scenario you should remember in order for the administrator or person in charge to identify which security updates have not been applied that you should make use of the mbsacli.exe tool.

1. Consolidated Traveling Solutions chief information officer is also aware that we also struggle to main client computers and services with current security patches.

Consolidated Traveling Solutions is aware that though IT staff test security patches when they come out, they cannot always find the time to deploy them.

Incorrect Answers:

A: This option should not be used in the scenario because the utility is used to provide a listing of Group Policy settings and the Resultant Set of Policy (RSOP) for a user's computer.

B: This option should not be used in the scenario because the utility is used to track patches that have been installed on Windows 2000 computers only.

C: In the scenario you should not consider using the qchain.exe because the utility is used to install multiple patches or hot fixes in series.

## Topic 13, GNB Lumberjacks Scenario

### **GNB Lumberjacks Background**

GNB Lumberjacks is a lumber felling company which specializes in products made from different wood types and elements. In addition, GNB Lumberjacks also provides custom production services where customers send their plans and we produce the merchandise. As part of the services that GNB Lumberjacks offers its clientele, they operate a 24-hour call center.

### **GNB Lumberjacks is divided into the following departments:**

1. Accounts
  - \* Credit accounts
  - \* Debit accounts
  - \* Mortgage accounts
  - \* Loan accounts.
1. Investments
  - \* Long term Investments
  - \* Short term Investments
1. Accounting Services
2. Marketing
3. Human resources
4. Information Technology (IT)

### **GNB Lumberjacks Physical Locations**

The GNB Lumberjacks head quarters are located in Chicago. There are 750 employees at the Chicago office.

There are two GNB Lumberjacks regional offices:

1. Los Angeles and the head quarters doubles as the other regional office. The Los

Angeles office has 500 employees.

2. GNB Lumberjacks are well aware that there are 100 branch offices located in major cities throughout the western United States. GNB Lumberjacks are also aware that each branch office has between 20 and 30 employees.

3. GNB Lumberjacks are also aware that the Los Angeles Regional office services the branch offices that are located in California, Oregon, and Washington.

1. GNB Lumberjacks additionally knows that the Chicago Regional office/head quarters services the branch offices that are located in Colorado, New Mexico Utah, and Arizona.

GNB Lumberjacks Business Processes

The GNB Lumberjacks Chicago office hosts the Human Resources (HR) department.

1. GNB Lumberjacks is well aware that there is a 24-hour call center in the Chicago and Los Angeles offices.

2. GNB Lumberjacks knows that both the Chicago office and the Los Angeles office have an IT department.

3. GNB Lumberjacks knows that there have been no IT personnel have been deployed in the branch offices.

4. GNB Lumberjacks also knows that the IT departments in these offices contain the data center, which provides the relevant IT services for its respective region.

5. GNB Lumberjacks are additionally aware that the IT departments are responsible for all administrative tasks for the network, i.e. the help desk function.

### **The GNB Lumberjacks Existing IT environment:**

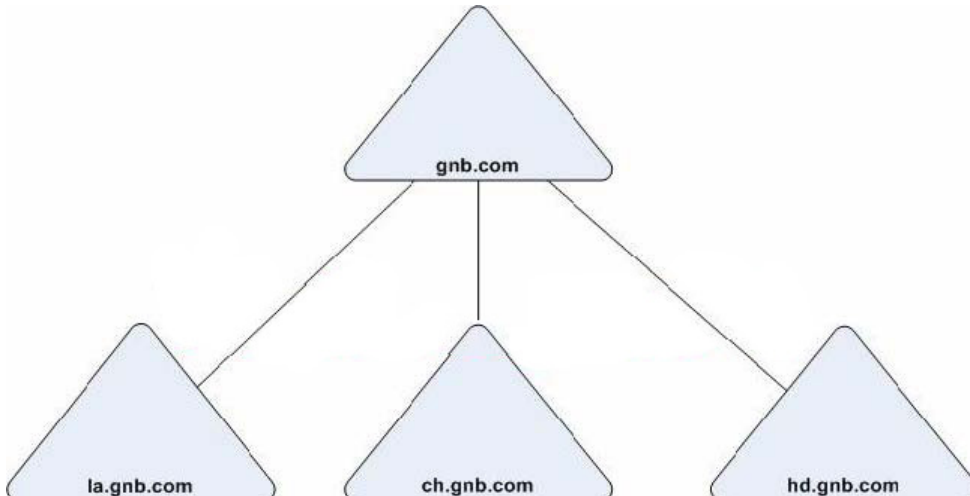
GNB Lumberjacks Directory Services

The GNB Lumberjacks network consists of a single Active Directory forest that contains four domains:

1. The forest root domain is named gnb.com

2. The three child domains that have been created are named la.gnb.com, ch.gnb.com, hd.gnb.com, respectively.

These are illustrated in the exhibit below.



GNB Lumberjacks knows that the call center personnel user accounts are located in the hd.gnb.com domain. The provision of support for both internal and external customers users are their responsibility.

GNB Lumberjacks is also aware that the HR department members all belong to the

CH-HRUsers group.

GNB Lumberjacks has also configured each branch office has been designated as an organizational unit (OU).

Both la.gnb.com and ch.gnb.com contain OUs for the branch offices in their geographic area.

### **GNB Lumberjacks Network Infrastructure**

The GNB Lumberjacks are additionally aware that network servers all run Windows Server 2003.

The GNB Lumberjacks are aware that the network client computers run Windows XP Professional.

The Chicago and Los Angeles offices host the wireless access points.

#### **These wireless access points support:**

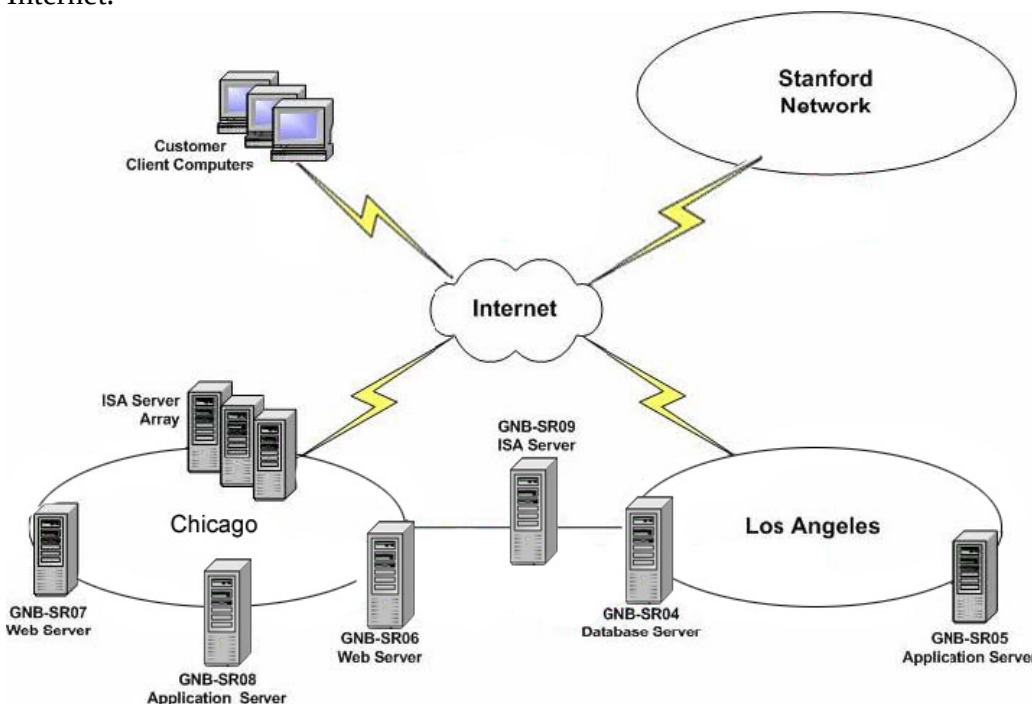
1. Support the IEEE 802.11q specification and Wired Equivalent Privacy (WEP) encryption.
2. Support the use of certificates and RADIUS for authentication.
3. Has no encryption or authentication methods configured.

GNB Lumberjacks also knows that there is a test network in the Chicago data center where security patches and updates are tested prior to deployment to the rest of the GNB Lumberjacks network.

GNB Lumberjacks additionally has a dedicated WAN connection exists between the Chicago and Los Angeles offices. Both the Chicago and Los Angeles offices have a dedicated connection to the Internet.

GNB Lumberjacks also makes use of a frame-relay line connects each branch office to its regional office.

GNB Lumberjacks has currently none of the branch offices are not connected to the Internet.



**A Web server named GNB-SR06 host:**

1. GNB Lumberjacks knows that an application that connects to a custom application hosted on a Windows Server 2003 computer in the Los Angeles data center
2. GNB Lumberjacks also knows that Web sites that contain publicity accessible information for both customers and the public.

The Chicago network has dual functionality in that it also functions as an extranet for partner company access.

A Web server named GNB-SR08 is installed in the Chicago data center. GNB-SR08:

1. runs IIS 6.0
2. hosts a Web site that is accessible by kiosk computers in each branch office
3. has membership of the Kiosk OU

The kiosk computers connect to the Web site using a user account named KioskUser.

**GNB Lumberjacks Problem statements:**

**Chief Information Officer**

The GNB Lumberjacks chief information officer knows that our core business revolves around handling confidential data and as such our success depends on our ability to efficiently secure our data. The GNB Lumberjacks is additionally concerned with the security risks that the wireless network might pose to our network. GNB Lumberjacks knows that with this in mind I want to ensure that only authorized users and computers access to the wireless network."

The GNB Lumberjacks chief information officer is additionally concerned about the possible compromise of our public key infrastructure (PKI). Such an occurrence would undermine the trust our customers place in our bank. The GNB Lumberjacks chief information officer also knows that recovery would be very expensive in terms of time and money especially after trust has already been undermined. GNB Lumberjacks additionally wants to ensure that our PKI is never compromised we should provide our partners and regular customers with access to the extranet. We will use smart cards to verify the identity of all users who access information from the Web-based application or Web site. GNB Lumberjacks are well aware that these cards will contain a user certificate issued by the GNB Lumberjacks certification (CA). Smart card readers will be provided to these users as well."

1. GNB Lumberjacks knows that they also need highly available and secure client/server application that will manage our largest customer's access to data. GNB Lumberjacks also knows that data transmissions must be very secure and we must ensure this."
2. GNB Lumberjacks chief information officer is also concerned that the kiosk computers in the branch offices could be used to compromise network security and to allow unauthorized access to company resources."
3. GNB Lumberjacks additionally knows that they also have a problem with tellers at the branch offices running unauthorized applications on their computers.

**GNB Lumberjacks IT Director**

The GNB Lumberjacks Written security policy states that all Windows updates and security patches should be tested in the test environment in the Chicago office before deployment to the production network. GNB Lumberjacks knows that at present these updates are copied to a CD-ROM and delivered to all company locations either by mail

or overnight delivery service or delivery by the administrators themselves. GNB Lumberjacks are also well aware that in order to sum it up: Patch Management as it is currently is time consuming, expensive and often requiring travel by IT personnel to all branch locations. GNB Lumberjacks additionally knows that apart from the patch management system, the administrators also have to travel to branch offices to perform many maintenance tasks on the servers. GNB Lumberjacks also knows that they need to provide a secure method to perform these tasks without requiring the administrator to travel to the site. I want a method to deploy updates and automatically to all computers in the network.

GNB Lumberjacks additionally knows that in the event of our administrators compelled to travel, they must be able to securely connect to and manage any server in his/her region using a laptop computer and dial-up ISP account. GNB Lumberjacks are also aware that these administrators are allowed to connect remotely to the network and the remote access policies that govern their level of access are defined differently in each region. GNB Lumberjacks also wants to ensure that the managers in the regional IT departments make the decisions regarding their level of access. Regardless, I want to ensure that every administrator uses a secure connection when he/she remotely connects to the network via the Internet.

GNB Lumberjacks also recently stated that often it happens that after an administrator is added to perform a particular task, the administrator account often remains in the group after the task has been completed. GNB Lumberjacks are well aware that this is meant to be temporary and we should take guard and ensure that these users are removed from the administrative security group as soon as the project is completed.

### **GNB Lumberjacks HR Manager**

The GNB Lumberjacks HR manager has recently stated that the greatest concern regards the unauthorized users that are able to access personnel information. GNB Lumberjacks wants to ensure that only HR users should have access to this information. Not even IT staff should be able to access this information."

### **GNB Lumberjacks Organizational Goals**

GNB Lumberjacks wants to have the following organizational requirements taken into consideration:

1. GNB Lumberjacks additionally knows that all IT personnel will be issued with new laptop computers that have wireless network adapters because they should be able to perform their administrative tasks even when not behind their desks.
2. GNB Lumberjacks also knows that each call center user works six hours at the call center. Then for four hours after that they are on call. These users must be issued laptop computers and high-speed Internet access. They must be enabled to use Terminal Services to run support applications from Windows Server 2003 computers in the call centers.
3. GNB Lumberjacks knows that their partners with an external auditing company named Stanford, Ltd. that provides audit services for customers. Stanford Ltd users must have access to the extranet in the Chicago office. These users need to be able to access file resources that are located on a server on the Chicago internal network named GNB-SR01.

4. GNB Lumberjacks are also aware that Branch office tellers must be able to run only a third-party application named BankTeller 2.0 on their computers. No other user applications must run on these computers, regardless of any actions taken by an end user. The regional offices users must be able to run their required applications.

**GNB Lumberjacks wants to have the following Active Directory requirements taken into consideration:**

1. GNB Lumberjacks knows that they make use of the application used on the extranet application server which requires changes to be made to the Active Directory schema. These changes must not affect the rest of the network.
2. GNB Lumberjacks are well aware that they currently all branch office network administration is performed by administrators in the Chicago office or the Los Angeles office. GNB Lumberjacks knows that their IT department wants to deploy a single administrator who will be responsible for all branch offices in a particular city. GNB Lumberjacks knows that this administrator responsibility will include all user, group, and resource management for only the branch offices in his or her particular city.
3. GNB Lumberjacks knows that their Help desk personnel require the ability to perform limited administrative tasks like resetting users' passwords and creating new user accounts for branch office users in the ch.gnb.com domain and the la.gnbank.com domain. They should not be able to perform any other administrative tasks.

**GNB Lumberjacks wants to have the following network infrastructure requirements taken into consideration:**

1. GNB Lumberjacks wants to ensure that all connections made over the frame-relay WAN connections must be encrypted and authenticated.
2. GNB Lumberjacks additionally at least one server in each domain should have Certificate Services installed. CA configuration must be based on the needs of each domain.
3. GNB Lumberjacks also recently both the ch.gnbank.com domain and the la.gnbank.com domain must have a Software Update Services (SUS) server installed.
4. GNB Lumberjacks has also decided that the Microsoft Baseline Security Analyzer (MBSA) must be deployed to all computers in all domains.

**GNB Lumberjacks wants to have the following security requirements taken into consideration:**

1. GNB Lumberjacks wants to ensure that access to all personnel data that is stored on a server named GNB-SR02 will be restricted to only users in the HR department. GNB Lumberjacks is well aware that provision must be made to allow the IT personnel to perform backups and restore this data as scheduled.
2. GNB Lumberjacks additionally wants to ensure that all connections made by IT personnel from outside the network must use the strongest available encryption and authentication methods since they will be allowed to connect to the GNB Lumberjacks network from home.
3. GNB Lumberjacks also recently stated that GNB-SR03 runs Terminal Services and is located on the extranet. All access to resources on the internal network must occur through GNB-SR03.

4. GNB Lumberjacks are additionally aware that their customers must be granted access to their personal account information via the company Web site. All customers are issued smart cards and smart card readers. GNB Lumberjacks wants to ensure that the smart cards also double as debit cards and to access personal account information. The smart cards contain a user certificate issued by a GNB Lumberjacks certification authority (CA).

**GNB Lumberjacks wants to have the following customer requirements taken into consideration:**

1. GNB Lumberjacks wants Stanford Ltd users need access to information stored on a Microsoft SQL Server 2000 database server named GNB-DB04 that is located on the Los Angeles internal network. GNB Lumberjacks are also aware that users on the internal network must also be able to access the information on GNB-DB04 by using Microsoft Access 2000.
2. GNB Lumberjacks are well aware that their customers must be able to access their personal account information securely.
3. GNB Lumberjacks wants to ensure that their Kiosk computers must provide access to public bank information for Customers and prospective customers. Each branch office will contain at least one kiosk computer. All kiosk computers must run Microsoft Windows XP Professional.

## Topic 13, GNB Lumberjacks (9 Questions)

---

### QUESTION 1

You need to design a remote access strategy for the call center users for when they are on call. In your solution you should take care to meet the security requirements. What should you do?

A. You should consider assigning the Secure Server (Require Security) IPSec policy to the GNB-SR03.

You should then assign the Client (Respond only) IPSec policy to the laptop computers

B. You should consider configuring IP packet filters on the GNB Lumberjacks routers to allow the Remote Desktop Protocol (RDP).

You should then configure IPSec filters on GNB-SR03 to allow only RDP connections

C. You should consider configuring IPSec tunnel mode connections between the Call center users' home and the GNB Lumberjacks routers

D. You should consider deploying an L2TP/IPsec VPN server in each call center.

You should then configure the laptop computers as L2TP VPN clients

Answer: D

Explanation: L2TP can encapsulate PPP frames just as PPTP can, but in contrast can then be sent over IP, ATM, or Frame Relay. It is rather more complicated than PPTP, and it is more secure. Bottom line: L2TP with IPSec to provide for higher layer encapsulation and encryption features necessary for VPN connectivity. This combination is known as L2TP/IPSec.

Requirements for an L2TP implementation of a LAN-to-LAN VPN: First, a user certificate needs to be installed on the calling router, and a computer certificate needs to be installed on the answering router.

Now consider the following:

1. GNB Lumberjacks operates a 24-hour call center to support customers and partners.
2. The Chicago and Los Angeles offices each maintain a customer support call center.
3. IT personnel must be able to connect to the network from home. All connections made by IT personnel from outside the network must use the strongest available encryption and authentication methods.

You would thus need to deploy a L2TP/IPSec VPN server in each call centre and configure the laptop computers as L2TP VPN clients so as to comply with security requirements.

Incorrect Answers:

A: Deploying a L2TP/IPSec VPN server in each call centre and configure the laptop computers as L2TP VPN client would be the best option and not just simply assigning IPSec policy.

B: This option does not comply with security requirements as stated in the case study.

C: Creating IPSec tunnel mode connections between customer support users home and the company's Internet-facing routers is not going to comply with all the security requirements. A L2TP/IPSec VPN connection will be more suitable and secure.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 335

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 7, pp. 433-438

---

## **QUESTION 2**

You need to implement a certificate authority (CA) hierarchy to support the remote administration requirements whilst you ensure in your solution to meet the business and security requirements.

What should you do? (Choose TWO.)

- A. You should consider deploying an online enterprise root CA in the gnb.com domain
- B. You should consider deploying an offline enterprise root CA in each domain
- C. You should consider deploying a subordinate issuing CA in each child domain
- D. You should consider deploying an offline enterprise root CA in the gnbank.com domain
- E. You should consider deploying a standalone issuing CA in each child domain

Answer: A, C

Explanation: The administrators will use Layer two Tunneling Protocol over IP Security (L2TP/IPSec) for the remote connections to ensure the security of these connections.

Using certificate based authentication will compel both the connecting computer and the VPN server to create L2TP/IPsec connections since both will require a computer

certificate. To support L2TP/IPSec, you will need an enterprise certificate authority (CA) in the forest root domain and you should also deploy enterprise subordinate CA in each of the child domains. This will server as redundancy as well as fulfilling domain computers' requests for certificates.

Incorrect Answers:

B: A root CA is the highest level CA in the CA hierarchy. You should, in this scenario, have it in the root domain and online.

D: An offline enterprise root CA in the gnbank.com domain will not work in an L2TP/IPSec connection since both connecting computers need to sign both computer certificates.

E: Standalone CAs allows one to take the CA offline. This is not what is required.

Besides not all Windows Server 2003 features can support standalone CAs.

---

### **QUESTION 3**

You need to redesign the Grand National Active Directory structure to support the new client/server application. This means accommodating an access control strategy for resources that are located in the extranet for partners and for internal users whilst ensuring your solution meets business and security requirements.

What should you do?

A. You should consider creating a new forest and domain named extranet.gnb.com

You should then create user accounts for Stanford Ltd users in this domain

You should finally create an external trust relationship in which the extranet domain trusts the ch.gnbank.com domain

B. You should consider creating a child domain of the ch.gnb.com domain for the extranet

You should then create user accounts for Stanford Ltd users in this domain

C. You should consider creating a new child domain named extranet.gnb.com in the existing forest.

You should then create user accounts for Stanford Ltd users in this domain

You should finally create shortcut trusts in which the child domain trusts every domain in the forest

D. You should consider creating a new forest and domain named extranet.gnb.com.

You should then create all user accounts for Stanford Ltd users in this domain

You should finally create a one-way forest trust relationship in which the extranet forest trusts Stanford Ltd forest

Answer: D

Explanation: With Windows Server 2003 one is allowed trust relationships between separate Active Directory forests. A forest is a security boundary. Forest trusts act much like domain trusts, except that they extend to every domain in two forests. Domains are connected to one another through logical structure relationships. The relationships are implemented through domain trees and domain forests.

A domain tree is a hierarchical organization of domains in a single, contiguous namespace. In the Active Directory, a tree is a hierarchy of domains that are connected to

each other through a series of trust relationships (logical links that combine two or more domains into a single administrative unit). The advantage of using trust relationships between domains is that they allow users in one domain to access resources in another domain, assuming the users have the proper access rights.

A forest is a set of trees that does not form a contiguous namespace. For example, you might have a forest if your company merged with another company. With a forest, you could each maintain a separate corporate identity through your namespace, but share information across Active Directory.

1. GNB Lumberjacks operates a 24-hour call center to support customers and partners.
2. Each call center user works six hours at the call center. Then for four hours after that they are on call. These users must be issued laptop computers and high-speed Internet access. They must be enabled to use Terminal Services to run support applications from Windows Server 2003 computers in the call centers.
3. GNB Lumberjacks partners with an external auditing company named Stanford Ltd. This company provides audit services for customers. The audit company must have access to the extranet in the Chicago office. These users need to be able to access file resources that are located on a server on the Chicago internal network named GNB-SR01.
4. Users from Stanford Ltd require access to information stored on a Microsoft SQL Server 2000 database server named GNB-DB04 that is located on the Los Angeles internal network. Users on the internal network must also be able to access the information on the SQL Server by using Microsoft Access 2000.

Thus you would design your access control strategy by creating extranet.gnbank.com, a new forest and domain. After which you create user accounts for the users from the partner companies in the new domain and then create a one-way forest trust relationship in which the extranet forest trusts the company forest.

Incorrect Answers:

- A: An external trust relationship is unnecessarily risky and will not comply with security requirements.
- B: This will not work for the reasons stated in A and C above. And above all this would only represent half a solution.
- C: Child domains are not necessary. Furthermore shortcut trusts will not meet business and security requirements. What is necessary is a new forest and domain and a one-way trust in which the extranet forest trusts the company forest.

---

#### **QUESTION 4**

You need to design an authentication strategy for the administrators of the IT department to remotely connect to the network whilst ensuring your solution meets security requirements.

What should you do?

- A. You should consider creating a remote access policy on each of the VPN servers and configuring the policy to require L2TP to establish a connection
- B. You should consider creating a remote access policy on each of the VPN servers and configuring the policy to use the ch.gnbank.com to authenticate remote access users
- C. You should consider installing Internet Authentication Services (IAS) on a stand-alone

server in the Chicago extranet and create local user accounts for the IT personnel on the IAS server

D. You should consider installing Internet Authentication Services (IAS) on a server in the ch.gnbank.com domain

You should then configure the VPN servers as RADIUS clients

Answer: D

Explanation

: IAS in Windows Server 2003 allows for a centralized approach that implements a RADIUS server and a RADIUS proxy. The RADIUS server will provide centralized connection for authentication, authorization, and accounting functions for networks that include wireless access, VPN remote access, Internet access, extranet business partner access, and router-to-router connections. IAS proxy functions are different from these server functions, and include forwarding IAS authorization and accounting information to other IAS servers.

IAS is installed as an optional server in Windows Server 2003, and is not installed by default. Therefore, we need to add IAS manually to our Windows Server 2003.

There are several remote access methods in an enterprise: dial-in client desktops, VPN clients, and wireless devices in our demonstration. The dial-in clients will connect to a dial-in server. The VPN clients will connect to a VPN server. The wireless devices will access the network through a wireless access server. All three servers will connect to a Windows Server 2003 RADIUS IAS proxy machine. This proxy will channel the requests to the IAS server. The IAS server will communicate with the DC and the Active Directory to perform authentication duties.

The Chicago and Los Angeles offices host the wireless access points.

These wireless access points support:

1. Support the IEEE 802.11q specification and Wired Equivalent Privacy (WEP) encryption.
2. Support the use of certificates and RADIUS for authentication.
3. Has no encryption or authentication methods configured.
4. The IT department is responsible for all administrative tasks for the network. There are no IT personnel at the branch offices.
5. All IT personnel will be issued with new laptop computers that have wireless network adapters because they should be able to perform their administrative tasks even when not behind their desks.
6. All IT personnel have new laptop computers that have wireless network adapters.
7. IT personnel must be able to connect to the network from home. All connections made by IT personnel from outside the network must use the strongest available encryption and authentication methods.

Therefore you should install IAS on a server in the ch.gnbank.com domain and configure the VPN servers as RADIUS clients to meet the security requirements for remote access of the users in the IT department.

Incorrect Answers:

A: This option will not work in these circumstances.

B:

You should configure the VPN servers as RADIUS clients to ensure that the strategy

meets the security requirements and not make use of a remote access policy that requires L2TP to establish a connection.

C: There is not need to create local user accounts for the IT personnel on a stand-alone IAS server. This option will not meet security requirements.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 6, pp. 369-370

---

### **QUESTION 5**

You need to design an access control solution for customer information that is transmitted over the Internet whilst ensuring your solution meets security requirements.

What should you do? (Choose THREE.)

- A. You should consider configuring the Web site to require SSL connections
- B. You should consider configuring the Web site to require client certificates
- C. You should consider enabling and configure client certificate mapping on the Web site
- D. You should consider disabling anonymous access to the Web site
- E. You should consider configuring the Web site to use only Microsoft .NET Passport authentication
- F. You should consider configuring a custom local IPSec policy on the Web servers to require IPSec communications
- G. You should consider configuring the IPSec policy to use certificate-based authentication and encryption

Answer: A, B, C

Explanation: Authenticated client access to a secure site - With SSL you can provide access to authenticated clients to a secure site by requiring both client and server certificates and by mapping those certificates. Client certificates can be mapped on a one-to-one basis or a many-to-one basis via Active Directory Users and Computers. You can create a group of designated users, map the users' certificates to the group, and give the group permission to access the secure site.

1.

Customers must be able to access personal account information by means of the company Web site. All customers are issued smart cards and smart card readers. The smart cards are used by customers as debit cards and to access personal account information. The smart cards contain a user certificate issued by a GNB Lumberjacks certification authority (CA).

2. Bank customers must be able to securely access their personal account information.

3. Customers and prospective customers must be able to access public bank information by means of kiosk computers running Windows XP Professional. Each branch office will contain at least one kiosk computer.

To comply with security requirements while designing an access control strategy for customer information, taking the above into account, you should configure the Web site to require SSL connections and require client certificates. After that you should enable

and configure client certificate mapping on the site.

Incorrect Answers:

D: Disabling anonymous access to the Web site and will not comply with security requirements as it would be allowing non-registered users access.

E: Making use of only Microsoft .NET Passport authentication will not work in this scenario.

F: IPSec is best used for packet filtering and is thus not suited for securing a Web server.

G: IPSec is used for host-to-host security along specific paths and is thus not suited to be used to authenticate or encrypt Web servers.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 6, p. 404

---

### QUESTION 6

You need to design a security strategy that will ensure that no unauthorized users are able to access personnel data.

What should you do? (Choose TWO.)

A. You should consider adding the CH-HRUsers group to the Restricted Groups list in the Default Domain Policy Group Policy object (GPO) for the gnb.com domain.

B. You should consider adding the CH-HRUsers group to the Restricted Groups list in the Default Domain Policy Group Policy object (GPO) for the ch.gnbank.com domain

C.

You should consider adding the CH-HRUsers group and the Backup Operators group to the Restricted Groups list in the Default Domain Policy Group Policy object (GPO) for the ch.gnbank.com domain.

D. You should consider adding only the HR department user accounts to the Allowed Members list.

E. You should consider adding only the HR department user accounts and the administrator user accounts to the Allowed Members list for each group.

F. You should consider adding only the administrator user accounts to the Allowed Members list for the Backup Operators group.

Answer: A, D

Explanation: Setting policies in the Default Domain Policy sets them for all computers in the domain.

Thus you should design the security strategy that will ensure no unauthorized access to personnel data by adding the CH-HRUsers group to the Restricted Groups list and in addition add only the HR department user accounts to the Allowed Members list in the Default Domain Group Policy object for the ch.gnbank.com domain. Especially when you take the following into consideration:

1. All members of the HR department are members of a group named CH-HRUsers.
2. I am concerned about unauthorized users being able to access personnel information. Only HR users should have access to this information. Not even IT staff should be able to access this information.

3. All personnel data is stored on a server named GNB-SR02. Access to personnel data must be restricted to only users in the HR department. However, IT personnel must be able to backup and restore this data as scheduled.

Incorrect Answers:

A: This option suggests application to the wrong domain.

C: Only the CH-HRUsers group should be added to the Restricted Groups list and not the Backup Operators group as well.

E: Only the HR department user accounts should be added to the Allowed Members list in the ch.gnbank.com domain and not the administrator user accounts.

F: This option suggests the correct domain, but the Backup Operators group should not be considered in this scenario.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 147

---

### **QUESTION 7**

You need to design a PKI solution whilst ensuring your solution meets business and security requirements.

What should you do?

A. You should consider implementing an enterprise root CA in the gnb.com domain

You should then implement a stand-alone root CA in both the ch.gnbank.com and the la.gnb.com domains

B. You should consider implementing an enterprise root CA in both the ch.gnbank.com and the la.gnb.com domains

You should then take the enterprise CA in each domain offline

C. You should consider implementing an enterprise root CA in the gnb.com domain

D. You should consider implementing an enterprise root CA in the gnb.com domain  
You should then implement subordinate CAs in both the ch.gnbank.com and the la.gnbank.com domains and take the root CA offline

Answer: D

Explanation: The root CA is the top of the CA hierarchy and should be trusted at all times. The certificate chain will ultimately end at the root C

A. The enterprise can

have a root CA as enterprise or a stand-alone C

A. The root CA is the only entity

that can self sign, or issue self certificates in the enterprise. Windows Server 2003 only allows one machine to act as the root C

A. The root CA is the most important

C

A. If the root CA is compromised, all the CAs in the enterprise will be compromised. Therefore, it is a good practice to disconnect the root CA from the network and use a subsidiary CA to issue certificates to users. Any CAs that is not

the root CA is classified as subordinate CAs. The first level of subordinate CAs will obtain their certificates from the root C

A. These servers are commonly referred to as intermediary or policy CAs. They will pass on the certificate information to the issuing CAs down the chain. They are referred to as intermediary because they act as a "go-between" with the root CA and the issuing CAs.

Following is the relevant information regarding the PKI solution required by GNB Lumberjacks:

1. "I am also concerned about the possible compromise of our public key infrastructure (PKI). Such an occurrence would undermine the trust our customers place in our bank. Furthermore recover would be very expensive in terms of time and money especially after trust has already been undermined.

2.  
GNB Lumberjacks customers must be access their personal account information securely Customers must granted access to their personal account information via the company Web site. All customers are issued smart cards and smart card readers. The smart cards also double as debit cards and to access personal account information. The smart cards contain a user certificate issued by a GNB Lumberjacks certification authority (CA). Thus in the current situation you thus need to implement an enterprise root CA in the gnbank.com domain. Implement subordinate CAs in each child domain and then take the root CA offline.

Incorrect Answers:

A: Implementing a stand-alone root CA in each of the child domains is an unnecessary security risk.

B: You should not implement the enterprise root CA in each of the child domains. This can result in a compromise if too many domains are enabled to issue certificates.

C: This option is risky and only suggests half of the design needed to comply with business and security requirements.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 3, p. 159, 181

---

### **QUESTION 8**

You need to design an authentication solution for wireless network access for the administrators in their regions whilst ensuring your solution meets business and technical requirements.

What should you do? (Choose TWO.)

A. Deploy an offline enterprise root CA in the gnbank.com domain.

Deploy subordinate enterprise root CAs in both the ch.gnbank.com and the la.gnbank.com domain.

Install Internet Authentication Service (IAS) on a member server in both the ch.gnbank.com domain and the la.gnbank.com domain.

B. Deploy an enterprise root CA in each domain.

Install Internet Authentication Service (IAS) on a member server in the gnbank.com domain.

Install the Routing and Remote Access service (RRAS) on a member server in both the ch.gnbank.com domain and the la.gnbank.com domain.

Configure these servers as RADIUS clients.

C. Deploy user certificates to all administrators and computer accounts that have wireless network adapters.

Configure each laptop computer to use Protected EAP (PEAP) for authentication purposes.

D. Deploy computer certificates to all laptop computers that have wireless network adapters.

Configure each laptop computer to use EAP-MS-CHAP v2 for authentication.

Answer: A, C

Explanation: The root CA is the top of the CA hierarchy and should be trusted at all times. The certificate chain will ultimately end at the root C

A. The enterprise can have a root CA as enterprise or a stand-alone C

A. The root CA is the only entity that can self sign, or issue self certificates in the enterprise. Windows Server 2003 only allows one machine to act as the root C

A. The root CA is the most important C

A. If the root CA is compromised, all the CAs in the enterprise will be compromised. Therefore, it is a good practice to disconnect the root CA from the network and use a subsidiary CA to issue certificates to users. Any CAs that is not the root CA is classified as subordinate CAs. The first level of subordinate CAs will obtain their certificates from the root C

A. These servers are commonly referred to as intermediary or policy CAs. They will pass on the certificate information to the issuing CAs down the chain. They are referred to as intermediary because they act as a "go-between" with the root CA and the issuing CAs.

WEP and WPA provide secure communication, but some method must be used to authenticate users. Different 802.1X-based WLANs offer different solutions to this need. The preferred solution within the Windows Server 2003 environment is the use of the IETF standard called Extensible Authentication Protocol (EAP). EAP can make use of various authentication methods that are based on passwords, public key certificates or other credentials.

Thus when you take the information pertaining to wireless network access, mentioned below, into account, then options A and C is the solution.

1. The network consists of four Active Directory domains in a single forest.

2. All servers run Windows Server 2003. All client computers run Windows XP Professional.

3. Wireless access points are installed in the Chicago and Los Angeles offices. The wireless access points support the IEEE 802.11q specification and Wired Equivalent Privacy (WEP) encryption.

4.

Currently, no encryption or authentication methods are configured on the wireless access points.

5. A dedicated WAN connection exists between the Chicago and Los Angeles offices.

6. A frame-relay line connects each branch office to its regional office. The branch offices are not connected to the Internet.

7. The Chicago and Los Angeles offices each have a dedicated connection to the Internet.

8. IT personnel must be able to perform administrative tasks even when they are not at their desks. All IT personnel have new laptop computers that have wireless network adapters.

Incorrect Answers:

B: Employing an enterprise root CA in each domain is not advisable. Furthermore IAS should be installed on one member server in the ch.gnbank.com domain and one member server in the la.gnbank.com domain.

D: This option will not comply with business requirements. While EAP-MS-CHAP v2 protects user credential during authentication by sending a hash to the authenticator, it does not use a secure channel for authentication, therefore the hash that is transmitted during authentication can be captured and the associated password can be guessed by way of a possible offline dictionary attack.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 3 & 5, pp. 159, 181, 316

---

### **QUESTION 9**

You need to design a method implement a patch management system whilst ensuring your solution meets technical requirements.

What should you do?

A. Deploy a Software Update Services (SUS) server in the test network at the Chicago office.

Deploy regional SUS servers to receive the administrator-approved updates from the test network SUS server.

Configure all GNB Lumberjacks client computers to receive the updates from their respective regional SUS server.

B. Deploy a Windows Server 2003 computer running Software Update Services (SUS) in the test network.

Configure all GNB Lumberjacks client computers to receive the updates from the test SUS server.

C. Install MBSA on a Windows Server 2003 computer in the network.

Deploy MBSA as a Windows Installer package to all computers in the child domains, and configure MBSA to scan for updates from the server in the test network.

D. Install Internet Information Services (IIS) on a Windows Server 2003 computer in the test network.

Create a Web site named Updates on this server.

Configure an autoupdate policy in each child domain to download and deploy updates from the Updates Web site

E. Deploy a Software Update Services (SUS) server in the regional offices.  
Configure each SUS server to download updates from the Windows Update servers on the Official Microsoft Windows Update site.  
Configure all GNB Lumberjacks client computers to receive the updates from the appropriate regional SUS server.

Answer: A

Explanation: Software Update Services (SUS) is used to leverage the features of Windows Update within a corporate environment by downloading Windows Update to a corporate server, which in turn provides the updates to the internal corporate clients. This allows administrators to test and have full control over what updates are deployed within the corporate environment.

1. A Software Update Services (SUS) server must be installed in each regional office domain. The Microsoft Baseline Security Analyzer (MBSA) must be deployed to all computers in each domain.

2. The Chicago data center includes a test network for testing security patches and updates before they are deployed to the rest of the network.

Deploying a Windows Server 2003 computer to run the SUS in the test network and then deploying SUS servers in each child domain, and then configuring the client computers to get their updates from their regional SUS servers is the solution.

Incorrect Answers:

B: Making use of Autoupdate policies in each child domain as described in this option is not the solution since it does not mention that the downloads will be administrator approved updates from the test network SUS server. This is not recommended since you will then be introducing a single point of failure into the system. If the test SUS server is to fail then all clients would be unable to receive updates.

C: MBSA verifies whether your computer has the latest security updates and whether there are any common security violation configurations that have been applied to your computer. This is not what is required in this question.

D: Installing IIS is not the option to be taken in this scenario.

E: This solution does not ensure administrator tested and approved updates to all client computers.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 477

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 2, p. 51

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide, p. 55