



TestKingonline.com

No Pass No Pay!

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

**Designing Security for a Microsoft Windows Server
2003 Network**

70-298

Congratulations!

You have purchased a TestKingonline. Study Guide.

This study guide is a complete collection of questions and answers that have been developed by our professional & certified team. You must study the contents of this guide properly in order to prepare for the actual certification test. The average time that we would suggest you for studying this study guide is approximately 10 to 20 hours and you will surely pass your exam. We guarantee it!

GOOD LUCK!

DISCLAIMER

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

Guarantee

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

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

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

Case Study #1, Alpine Ski 4	
Case Study #1, Alpine Ski House (8 questions)	11
Case Study #2, Humongous Insurance	24
Case Study #2, Humongous Insurance (5 Questions)	28
Case Study #3, Lucerne Publishing	34
Case Study #3, Lucerne Publishing (13 Questions)	38
Case Study #4, Southbridge Video	54
Case Study #4, Southbridge Video (9 Questions)	59
Case Study #5, Woodgrove Bank	69
Case Study #5, Woodgrove Bank (8 Questions)	75
Case Study #6, TestKing.co 86	
Case Study #6, Testkingonline.com (11 Questions)	91
Case Study #7, Litware Inc. 102	
Case Study #7, Litware, Inc. Bank (4 Questions)	107
Case Study #8, Northwind Traders	111
Case Study #8, Northwind Traders (9 Questions)	117
Case Study #9, Consolidated Messenger	127
Case Study #9, Consolidated Messenger (5 Questions)	130
Case Study #10, Fabrikam .. 135	
Case Study #10, Fabrikam (9 questions)	136
Case Study #11, Fourth C 140	
Case Study #11, Fourth Coffee (4 questions)	141
Case Study #12, Trey Research	143
Case Study #12, Trey Research (questions)	151

Total number of questions: 95

Case Study #1, Alpine Ski House

Overview

Alpine Ski House operates ski resorts that provide accommodations, dining, and entertainment to customers.

The company recently acquired four resorts from Contoso, Ltd.

Physical Locations

The company's main office is located in Denver.

The company has 10 resorts in North America, three of which are in Canada. The four newly acquired resorts

are located in Europe. Each resort has between 90 and 160 users.

Planned Changes

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

The company will open a branch office in Vienna. The Vienna office will support the four European

resorts in the same way that the Denver office currently supports the North American resorts.

All servers in North America will be updated to Windows Server 2003.

All client computers will be upgraded to Windows XP Professional.

After the member servers and client computers in the Windows NT 4.0 domain are upgraded, the NT domain will be migrated into Active Directory.

A new file server named Server1 will be installed and configured. It will run Windows Server 2003.

Each resort will have several kiosks installed for unauthenticated users, such as resort customers.

To remain competitive in the upscale market, the company will make wireless internet connections available to customers visiting the resort.

Business Process

The information technology (IT) department is located in the Denver office. The IT department operates the company's Web, database, and e-mail servers. The IT department also manages client computers in the Denver office. IT staff members travel to resorts to perform major upgrades, new installations, and advanced

troubleshooting of servers that are located in resorts in North America.

Each resort has at least one desktop support technician to support client computers.

Depending on their

experience, some technicians might have administrative rights to the servers in their resort.

The European resorts have a common finance department.

The human resources (HR) department maintains a Web application named hrbenefits.alpineskihouse.com that provides confidential personalized information to each employee. The application has the following

characteristics:

- It uses ASP.NET and ADO.NET.

- It is hosted on a Web server in the Denver office.

- Employees can access the application from work or from home.

The reservations department maintains a public Web site named funski.alpineskihouse.com. The Web site has

the following characteristics:

- It uses ASP.NET and ADO.NET.

- It is accessible from anywhere on the Internet.

- The Web site also includes static content about each resort.

Directory Services

The company uses an Active Directory domain named alpineskihouse.com for North America. The Denver IT

Department administers the domain. The alpineskihouse.com domain will remain the forest root domain.

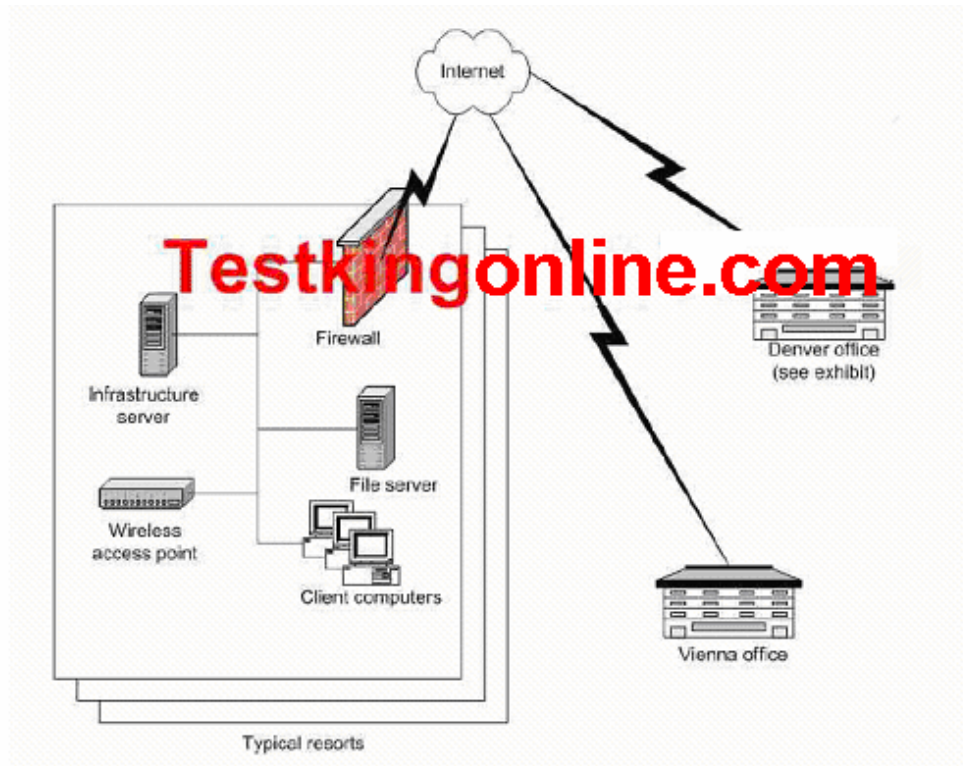
The European finance department has a Windows NT 4.0 domain named CONTOSODOM. Each European

resort contains a domain controller that runs Windows NT Server 4.0

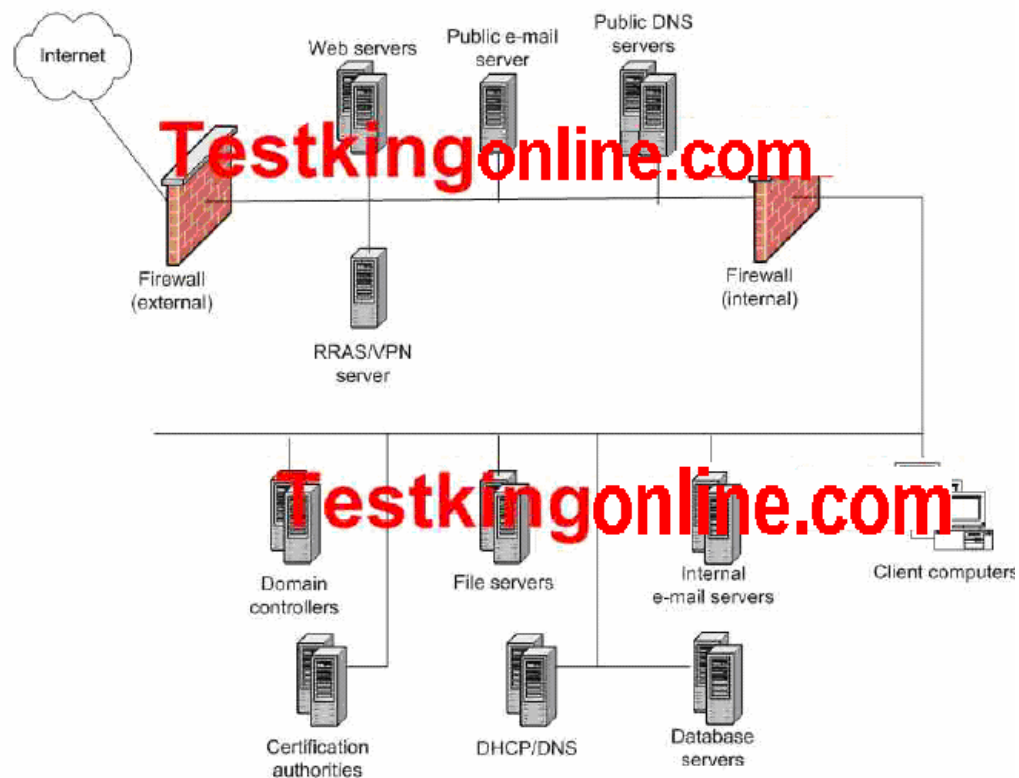
All employees have user accounts in either Active Directory or in the Windows NT 4.0 domain.

Network Infrastructure

The existing locations and connections are shown in the **Network Diagram** exhibit.



The network configuration of the Denver office is shown in the **Denver Office Configuration** exhibit.



All company servers in North America run Windows 2000 Server. All company servers in Europe run Windows NT Server 4.0. All company client computers currently run Windows 2000 Professional. There is one file server in each resort and in each office.

The company's offices and resorts are connected by VPNs across the Internet.

Wireless access points have been installed at each resort for staff use.

Chief Information Officer

Securing our corporate data is vitally important. Here are the priorities, as I see them:

We keep a significant amount of personal customer information on file. This data is an important corporate asset that we must protect.

All public key infrastructure (PKI) certificates that we use must be trusted widely.

Customers must not

be required to perform additional actions to gain access to our Web sites.

We established security policies and logging requirements. If someone attempts to violate these policies, I need to be notified immediately so that I can respond.

IT Manager

To avoid expensive dedicated WAN links, we use VPNs instead. However, we do not want users to download updates directly from the Internet.

Also, I want to automate routine administrative tasks. When we get busy, sometimes even important tasks are

not completed. So, IT administration must require as little manual overhead as possible. I am worried that my staff is overwhelmed by the amount of log items that just show regular actions like logging in and printing. I am concerned that something important is going to be missed. Currently, the legacy application used to manage resort functions at the resorts reads and writes a registry value that nonadministrative users cannot change. The application will run correctly if users are made administrators on the client computer, but this violates the company's written security policy.

Organizational Goals

The following organizational goal must be considered:

The company must be able to share information between offices and resorts, but customer's personal information and other confidential corporate data must be encrypted when it is stored and while it is in transit.

Written Security Policy

The company's written security policy includes the following requirements:

When an administrator performs a security-related action that affects company servers, the event must be logged. Logs must be saved. When possible, a second administrator must audit the event.

Only IT staff and desktop support technicians at the resorts are allowed to have administrative permissions on client computers and to change other user's configurations.

All client computers must be configured with certain desktop settings. This collection of settings is named the Desktop Settings Specification, and it include a password-protected screen saver.

Kiosk computers must be configured with more restrictive desktop settings. This collection of settings is named the Kiosk Desktop Specification. The ability to change these settings must be restricted to administrators.

All client computers must be kept up-to-date with critical updates and security patches when they are issued by Microsoft; however, the IT department must approve each update before it is applied. Only

European IT administrators are allowed to approve updates for computers in Europe.
Only North

American IT administrators are allowed to approve updates for computers in North America.

Public Web servers must not accept TCP/IP connections from the Internet that are intended for services that the public is not authorized to access.

Customer user accounts must not be stored in the same Active Directory domain as employee accounts.

Administrators accounts from the domain are domains that store the customer user accounts must not be

able to administer the employee accounts under any circumstances.

All data in the hrbenefits.alpineskihouse.com Web application must be encrypted while it is in transit

over the Internet.

Each employee must use a PKI certificate for identification in order to connect to hrbenefits.alpineskihouse.com.

Customer Requirements

The following customer requirements for wireless access and kiosk computers must be considered:

Staff and customers must be able to access the wireless network; however, corporate servers must be accessible only to staff.

Kiosk computers can be used for browsing the Internet only. Kiosk computers will run Windows XP Professional.

Frequent customers must be able to establish accounts through funski.alpineskihouse.com. The account information must be stored in Active Directory.

All customer personal information must be encrypted while it is in transit on the Internet.

Active Directory

The following Active Directory requirements must be considered:

The domain must contain one top-level organizational unit (OU) for each company location. Accounts for staff members must be located in the OU for their primary work location.

All IT staff that support users must be members of the AllSupport security group.

Highly skilled IT staff

must also be members of the security group named AdvancedSupport. Less experienced staff members

must also be members of the BasicSupport group.

All client computers in Europe must be configured according to the Desktop Settings Specification, even

if the domain upgrade is incomplete at the time.

Desktop support technicians at each resort must be able to reset user passwords for staff at that resort.

Network Infrastructure

The following network infrastructure requirement must be considered:

Authorized IT staff must use Remote Desktop Protocol (RDP) to manage the servers in the perimeter network.

IT staff must also be able to use RDP to manage servers at resorts.

Resorts must receive critical updates and security patches from their own continent.

Each resort must have one or more Windows Server 2003 computer that is configured as an infrastructure server to handle DNS, DHCP, and any VPN connections.

After Server1 is deployed, all users in the company must be able to create and read files stored in a shared folder named AllUsers and Server1.

Only members of the Web Publishers security group may make changes to the public Web site. All changes must be encrypted while being transmitted.

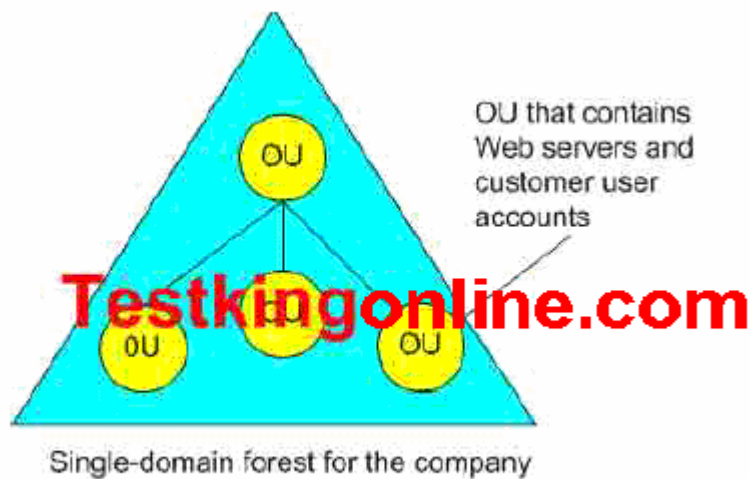
Case Study #1, Alpine Ski House (8 questions)

QUESTION NO: 1

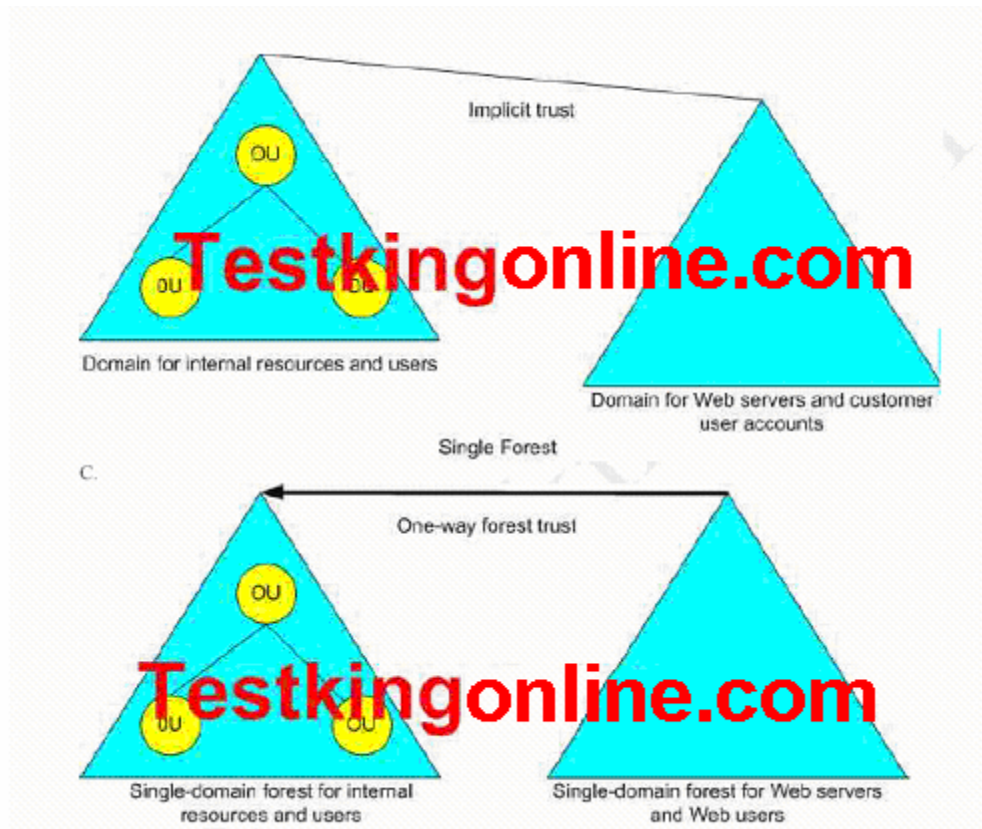
You are designing the company's Active Directory structure. Your solution must meet the public Web site's security requirements.

Which of the following design should you use?

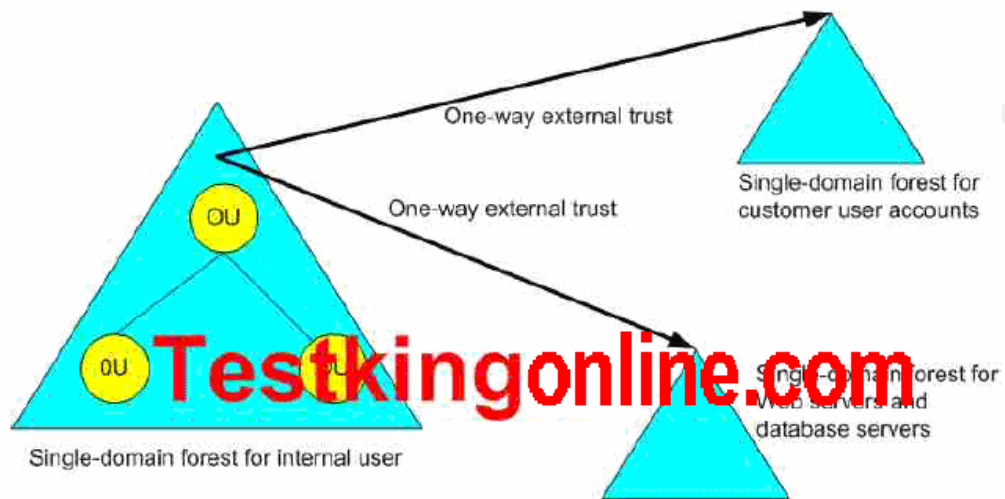
A.



B.



D.



Answer: C

Explanation: A forest trust is used to share resources between forests. It can be one-way or two-way.

Previously, system administrators had no easy way of granting permission on resources in different forests.

Windows Server 2003 resolves some of these difficulties by allowing trust relationships between separate

Active Directory forests. Forest trusts act much like domain trusts, except that they extend to every domain in

two forests. 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.

Option C represents a

one-way forest trust between the single domain forests for (1) internal resources and

users and (2) Web servers

and Web users. This is so that it complies with the Web site's security requirements.

Public Web servers must not accept TCP/IP connections from the Internet that are intended for services

that the public is not authorized to access.

Incorrect answers:

A: Option A is a single domain forest where all the Organizational Units are residing.

This would represent a

security risk since the Public Web server are not to accept TCP/IP connections from the Internet when those

connections are intended for services that does not warrant public access.

B: This option represents a single forest with an implicit trust between the domains in the forest. This is not

what is required in these circumstances.

D: This option has a trust relationship between itself and the Web servers and database servers as well as a trust

relationship between itself and the customer user accounts. This will not comply with the requirements as stated

by the case study.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows® Server 2003 Network

Infrastructure Implementation, Management, and Maintenance Study Guide, p. 103

QUESTION NO: 2

You need to design the configuration for the kiosk computers. Your solution must be able to be implemented by using the minimum amount of administrative effort. What should you do?

A. Configure the kiosk computers as computers that are not members of any domain.

Use Local Computer Policy to configure the computers with the collection of settings in the Kiosk

Desktop Specification.

B. Install one kiosk computer as a model.

Configure this computer with the collection of settings in the Kiosk Desktop Specification.

Copy the content of the C:\Documents and Settings\Default Users folder from this model computer to all other kiosk computers.

C. Create a system policy file named Ntconfig.pol and configure it with the collection of settings in the Kiosk Desktop Specification.

Make the kiosk computers members of the Active Directory domain.

Use a Group Policy object (GPO) to run a startup script that copies the Ntconfig.pol file to the System32

folder on each kiosk computer.

D. Create a Group Policy object (GPO) and configure it with the collection of settings in the Kiosk Desktop

Specification:

Also include an appropriate software restriction policy.

Make the kiosk computers members of the Active Directory domain, and place the computer account

objects in a dedicated OU.

Link the GPO to this OU.

Answer: D

Explanation: 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. You can apply GPOs to sites, domains, or organizational units.

Within the Active Directory, you can categorize the objects in the domain by using organizational units (OUs).

Organizational units are typically defined based on geography or function and the scope of administrative authority, such as (1) Limiting administrative authority within the domain, (2) Organizing users by function.

Thus an OU can represent a department, division, location, or project group. Used to ease administration of

Active Directory objects and as a unit to which group policy can be deployed.

Each resort will have several kiosks installed for unauthenticated users, such as resort customers.

Kiosk computers must be configured with more restrictive desktop settings. This collection of settings is named the Kiosk Desktop Specification. The ability to change these settings must be restricted to

administrators.

In this scenario you would need to create a GPO and include on the configuration the collection of settings in

the Kiosk desktop specification as well as the appropriate software restriction policy.

After that you need to add

kiosk computers to the Active Directory domain and place the computer account into a dedicated OU. This

GPO must then be linked to the OU.

Incorrect answers:

A: Configuring the Kiosk computers as non-members of any domain will not work in this scenario.

B: Installing and configuring one Kiosk computer as a model and then having it copied to all the rest will result

in too much administrative effort since all you need to do is to create a dedicated OU and link the appropriately configured GPO to it.

C: Running a startup script on each Kiosk computer is not necessary in this scenario. You need to limit

administrative effort to the minimum.

Reference:

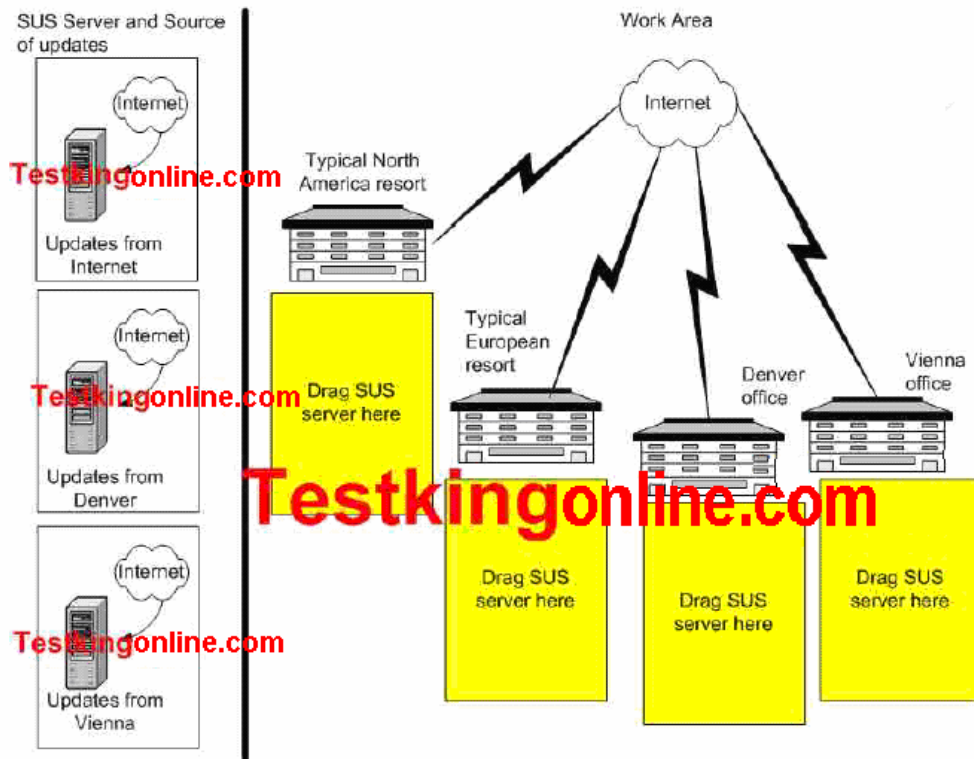
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows® Server 2003 Network

Infrastructure Implementation, Management, and Maintenance Study Guide, p. 21

QUESTION NO: 3

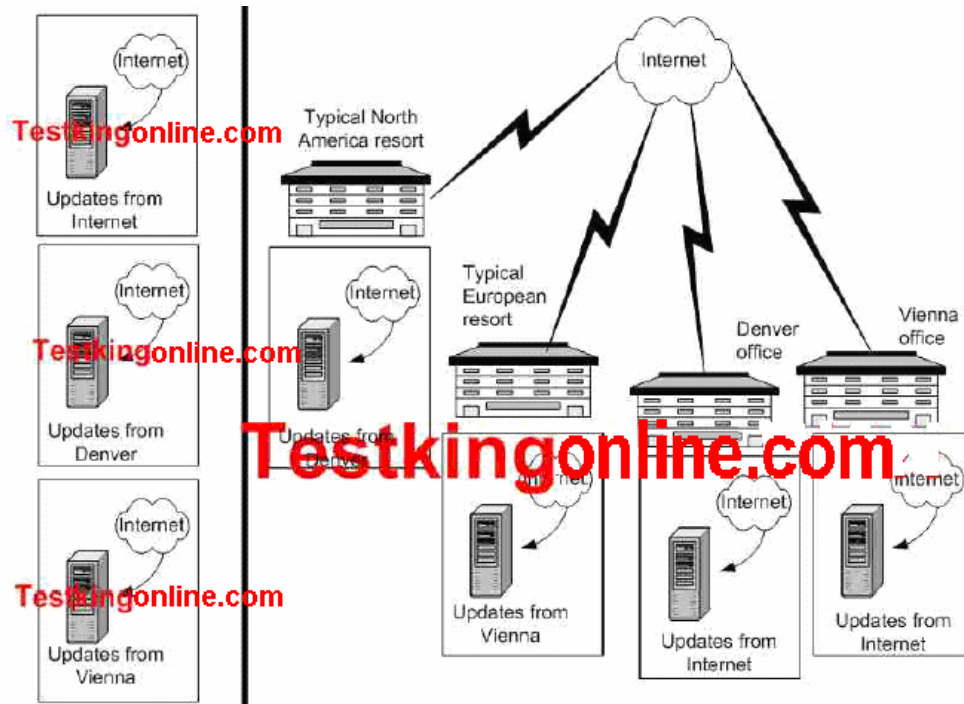
A logical diagram of a portion of the Alpine Ski House network is shown in the work area. You are designing a software Update Services (SUS) infrastructure for the company. You need to decide where to place SUS servers. Then, you need to decide if each of the new SUS servers will receive new updates from the Microsoft servers on the Internet or from another SUS server within the company. Your solution must 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: If you are supposed to make use of the fewest amount of SUS servers then you should have the Denver and the Vienna offices obtain their updates from the Internet and the two of them will respectively serve as SUS servers to the typically North American and European resorts respectively. This should work since the Denver and Vienna offices serves as support for the resorts that are on situated on the same continents respectively.

The company will open a branch office in Vienna. The Vienna office will support the four European resorts in the same way that the Denver office currently supports the North American resorts.

All client computers must be kept up-to-date with critical updates and security patches when they are issued by Microsoft; however, the IT department must approve each update before it is applied. Only European IT administrators are allowed to approve updates for computers in Europe. Only North American IT administrators are allowed to approve updates for computers in North America.

Resorts must receive critical updates and security patches from their own continent.

Reference:

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

QUESTION NO: 4

You need to design the IPSec policy for the Web servers in the Denver office. You need to decide which policy settings to use.

What should you do?

To answer, drag the appropriate policy setting or settings to the correct location or locations in the work area.



Explanation: (RDP) is a connection that needs to be configured in order for clients to connect to the Terminal Services server. Whereas HTTP and HTTPS is an Internet protocol that transfers HTML documents over the Internet and responds to context changes that happen when a user clicks a hyperlink. You will have to apply the Deny Policy setting to the Web servers to or from the Internet as this will compromise security. And you need to apply the Allow Policy setting for RDP, HTTP and HTTPS traffic on the Web servers to or from the client computers.

The information technology (IT) department is located in the Denver office. The IT department operates the company's Web, database, and e-mail servers. The IT department also manages client computers in the Denver office. IT staff members travel to resorts to perform major upgrades, new installations, and advanced troubleshooting of servers that are located in resorts in North America.

IT staff must be also be able to use RDP to manage servers at resorts.

Authorized IT staff must user Remote Desktop Protocol (RDP) to manage the servers in the perimeter network.

The company uses an Active Directory domain named alpineskihouse.com for North America. The Denver IT Department administers the domain. The alpineskihouse.com domain will remain the forest root domain.

Public Web servers must not accept TCP/IP connections from the Internet that are intended for services that the public is not authorized to access.

Reference:

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

QUESTION NO: 5

You are designing a security strategy for the infrastructure servers at the resorts. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Place all infrastructure servers in subnets that cannot exchange information with the Internet.
- B. Establish a custom security template that contains unique required settings for each combination of services that run on the infrastructure servers.
- C. Use Group Policy objects (GPOs) to apply the custom security template or templates to the infrastructure servers.
- D. Edit the local policy settings to configure each individual server.

Answer: C, D

Explanation: 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. You can apply GPOs to sites, domains, or organizational units.

One makes use of security templates as a way to apply consistent security settings to an entire network, or to a subset of computers or servers. In this scenario you should apply custom security templates to the infrastructure servers through GPOs and then edit the local policy settings to configure each individual server.

Each resort must have one or more Windows Server 2003 computer that is configured as an infrastructure server to handle DNS, DHCP, and any VPN connections.

I want to automate routine administrative tasks.
IT administration must require as little manual overhead as possible.

Incorrect answers:

A: Organizing all infrastructure servers into subnets will be obsolete.

B: Following the explanation regarding GPOs, this option would also not be correct. You need to apply the custom security template or templates 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 NO: 6

You need to design a Security strategy for the wireless network at all resort locations.

What should you do?

A. Connect the wireless access points to a dedicated subnet. Allow the subnet direct access to the Internet, but not to the company network.

Require company users to establish a VPN to access company resources.

B. Install Internet Authentication Service (IAS) on a domain controller.

Configure the wireless access points to require IEEE 802.1x authentication.

C. Establish IPSec policies on all company servers to request encryption from all computers that connect from the wireless IP networks

D. Configure all wireless access points to require the Wired Equivalent Privacy (WEP) protocol for all connections. Use a Group Policy object (GPO) to distribute the WEP keys to all computers in the domain.

Answer: A

Explanation: If you allow a user outside of your organization to access your computer, you should have them connect via a VPN account. If they connect through the network firewall, then TCP Port 3389 must be opened, which may be considered a security risk. In this specific scenario you should connect the wireless access points to a dedicated subnet. This subnet should be restricted to the Internet and be prohibited access to the company network and company users should establish a VPN to access company resources.

To remain competitive in the upscale market, the company will make wireless internet connections available to customers visiting the resort. The company's offices and resorts are connected by VPNs across the Internet.

Each resort must have one or more Windows Server 2003 computer that is configured as an infrastructure server to handle DNS, DHCP, and any VPN connections.

Incorrect answers:

B: The 802.1X standard improves security because both the wireless client and the network authenticate to each other. A unique per-user/per-session key is used to encrypt data over the wireless connection and keys are dynamically generated, reducing administrative overhead and eliminating the ability to crack a key because the key is generally not used long enough for a hacker to capture enough data to then determine the key and crack

it. But this is not necessary as the company makes use of VPNs.

C: Establishing IPSec Policy that requests encryption from the wireless IP networks is not the answer.

D: Recent studies have shown that there are flaws within the WEP encryption method, and there are now several software products available that can easily crack WEP encryption, so this method is less secure than it was even three or five years ago.

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 NO: 7

You need to design an access control and permission strategy for user objects in Active Directory. What should you do?

A. Make the members of the AdvancedSupport security group members of the Domain Admins security group.

B. Give each desktop support technician permission to reset passwords for the top-level OU that contains user accounts at their own location.

C. Delegate full control over all OUs that contain user accounts to all AllSupport security group.

D. Change the permissions on the domain object and its child objects so that the BasicSupport security group is denied permissions. Then, add a permission to each OU that contains user accounts that allows AllSupport security group members to reset passwords in that OU.

Answer: B

Explanation: One can make use of the Active Directory Users And Computers utility. Right-click the user whose password you want to change and select Reset Password. The Active Directory Users And Computers utility is the main tool for managing the Active Directory users, groups, and computers. Every desktop support technician should be able to reset passwords for the top level OU that contains all the user accounts at their locations respectively, to effect this they would need the proper permission.

Desktop support technicians at each resort must be able to reset user passwords for staff at that resort.

Each resort has at least one desktop support technician to support client computers. Depending on their experience, some technicians might have administrative rights to the servers in their resort.

Accounts for staff members must be located in the OU for their primary work location.

Incorrect answers:

A: “Highly skilled IT staff must also be members of the security group named AdvancedSupport.” A security group is a logical group of users who need to access specific resources. Security groups are listed in Discretionary Access Control Lists to assign permissions to resources. However, making these members part of Domain Admins security group is not necessary.

C: “All IT staff that support users must be members of the AllSupport security group.” Delegating Full control over all organizational units containing user accounts would be over compensating. All the desktop support technicians need is to be able to reset passwords.

D: “Less experienced staff members must also be members of the BasicSupport group.” Option D is unnecessary. It will not work in this case.

Reference:

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

QUESTION NO: 8

You need to design a permission structure for registry objects that enables the legacy application at the resorts to run. Your solution must comply with the written security policy. What should you do?

A. Create a GPO. Link the GPO to the OUs that contain computer accounts for computers that run the

legacy application, Use the GPO to give the Domain Users security group full control on the partitions of the registry that the legacy application uses.

B. Create a GPO. Link the GPO to the OUs that contain computer accounts for computers that run the legacy application. Use the GPO to give the Domain Users security group full control on the HKEY_USERS partition of the registry.

C. Create a GPO. Link the GPO to the OUs that contain computer accounts for computers that run the Legacy application. Use the GPO to make all users who require access to the application members of Local Administrators group on each computer.

D. Create a GPO. Link the GPO to the OUs that contain computer accounts for computers that run the Legacy application. Use the GPO to give all users who require access to the application full control for the Ntuser.dat file.

Answer: A

Explanation: 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 cuts down on administrative effort that has to be put in when applying the same policies on an individual basis. You should use the GPO to grant the Domain Users security group full control on the partitions of the registry that the legacy application uses. Thus should ensure that you also comply with the security requirements of the company.

IT administration must require as little manual overhead as possible.

I want to automate routine administrative tasks.

Currently, the legacy application used to manage resort functions at the resorts reads and writes a registry value that nonadministrative users cannot change. The application will run correctly if users are made administrators on the client computer, but this violates the company's written security policy.

Incorrect answers:

B: The Domain Users group should not be granted full control on the HKEY_USERS partition of the registry;

they should get control on the partitions of the registry that the legacy application uses.

C: This option will violate the security policy of the company.

D: NTUSER.DAT is the file that is created for a user profile. This is not what is required in this question.

Reference:

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

Case Study #2, Humongous Insurance

Overview

Humongous Insurance provides property and casualty insurance to customers in North America and Europe.

Physical Locations

The company's main office is located in New York. The company has three branch offices in the following locations:

- Seattle
- London
- Madrid

Planned Changes

Humongous Insurance is entering into a join venture with Contoso, Ltd., a worldwide asset management

company. The Contoso, Ltd., network consists of a single Windows 2000 Active Directory domain. Contoso,

Ltd., does not plan to upgrade its servers to Windows Server 2003.

The collaboration between the two companies will take place entirely over the Internet. Users from both

companies will access a shared folder name Customer Data, which will be located on a Windows Server 2003

computer on the Humongous Insurance internal network.

All Humongous Insurance client computers in Madrid will be upgraded to Windows XP Professional.

Directory Services

The existing Active Directory forest for Humongous Insurance is shown in the **Active Directory**

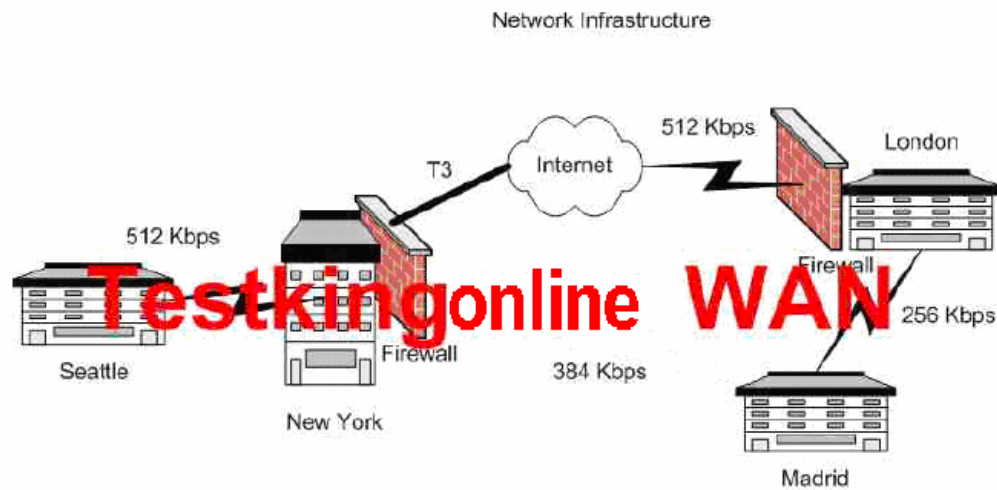
Infrastructure exhibit.



The Humongous Insurance network consists of a single Windows Server 2003 Active Directory forest. The forest contains three domains named humongousinsurance.com, na.humongousinsurance.com, and euro.humongousinsurance.com

Network Infrastructure

The company's existing network infrastructure is shown in the **Network Infrastructure** exhibit



A Windows Server 2003 Web server is located in the New York office perimeter network. All client computers in North America run Windows XP Professional. Each office contains a domain controller. The domain controllers also serve as file and print servers.

Problem Statements

The following business problems must be considered:

- It is difficult to maintain all client computers with the latest security patches.

- Unauthorized users have modified the registry on some servers. Unauthorized users must not be able to modify the registry on company servers.

- Access to resources is assigned per user, which causes administrative overhead. This administrative overhead must be reduced

Chief Information Officer

During the past year, we focused on preventing external threats. Now, we realize we also need to prevent internal threats. 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.

Business Requirements

The following business requirements must be considered:

- Security patches must be installed by using the minimum amount of WAN bandwidth.

- The information technology (IT) department in each office must test security patches before deploying them to client computers.

Written Security Policy

The company's written security policy includes the following requirements:

- All customer information must be kept confidential. All access to customer information must be tracked.

- Marketing information and service offering literature is available to the public.

Humongous Insurance

- must track unauthorized modification of the marketing information only.

- Management must be able to access company financial information that is stored in Microsoft SQL

Server 2000 databases and in shared folders.

- All e-mail messages sent between Humongous Insurance and Contoso, Ltd., must be encrypted.

- Authorized users will be autoenrolled in certificate services to access company resources.

- All content updates to the Web server must be protected from interception.

- All remote server administration must be conducted over an encrypted channel.

- Remote Desktop for Administration cannot be used to connect to servers on the perimeter network.

Case Study #2, Humongous Insurance (5 Questions)

QUESTION NO: 1

You need to design an access control strategy that meets business and security requirements.

Your solution must minimize forestwide replication.

What should you do?

A. Create a global group for each department and a global group for each location.

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

assign permissions for the file and printer resources by using the location global groups.
B. Create a global group for each department, and add the respective users as members.
Create domain local groups for file and printer resources.
Add the global groups to the respective domain local groups.
Then, assign permissions to the file and printer resources by using the domain local groups.
C. Create a local group on each server and add the authorized users as members.
Assign appropriate permissions for the file and printer resources to the local groups.
D. Create a universal group for each location, and add the respective users as members.
Assign the universal groups to file and printer resources.
Then, assign permissions by using the universal groups.

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.

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

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: 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.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows ® Server 2003 Environment Management and Maintenance Study Guide, p. 167

QUESTION NO: 2

You need to design a remote administration solution for servers on the internal network. Your solution must meet business and security requirements. What should you do?

- A. Permit administrators to use an HTTP interface to manage servers remotely.
- B. Permit only administrators to connect to the servers' Telnet service.
- C. Permit administrators to manage the servers by using Microsoft NetMeeting.
- D. Require administrators to use Remote Desktop for Administration connections to manage the servers.

Answer: B

Explanation: Telnet is a very powerful remote administration tool that allows an administrator to use command-line utilities from a text-based command-line window. Because it is infrequently used as an administrative tool and typically passes credentials using clear text, Telnet is disabled by default on all Windows Server 2003 machines. 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. Thus you need to permit the administrators only to connect to the servers' Telnet service. This scenario necessitates the administrators' need to make use of the Telnet service.

All remote server administration must be conducted over an encrypted channel.

Remote Desktop for Administration cannot be used to connect to servers on the perimeter network.

Incorrect answers:

A: Making use of HTTP interface to manage servers remotely will not comply with company security policy.

C: Having the administrators managing the servers with Microsoft NetMeeting does not meet with business requirements.

D: Compelling administrators to use RDA connections to manage the servers is not the answer since it is mentioned pertinently that “Remote Desktop for Administration cannot be used to connect to servers on the perimeter 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 4, p. 208

QUESTION NO: 3

You need to design a method to encrypt confidential data. Your solution must address the concerns of the chief information officer. What should you do?

- A. Encrypt customer information when it is stored and when it is being transmitted.
- B. Require encrypted connections to the public Web site, which is hosted on the Web server on the perimeter network.
- C. Encrypt all marketing information on file servers and client computers.
- D. Require 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.

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:

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.

“Marketing information and service offering literature is available to the public.

Humongous Insurance 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.

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 NO: 4

You need to design a method to update the content on the Web server. Your solution must meet business and security requirements. What are two possible ways to achieve this goal? (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 and 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.

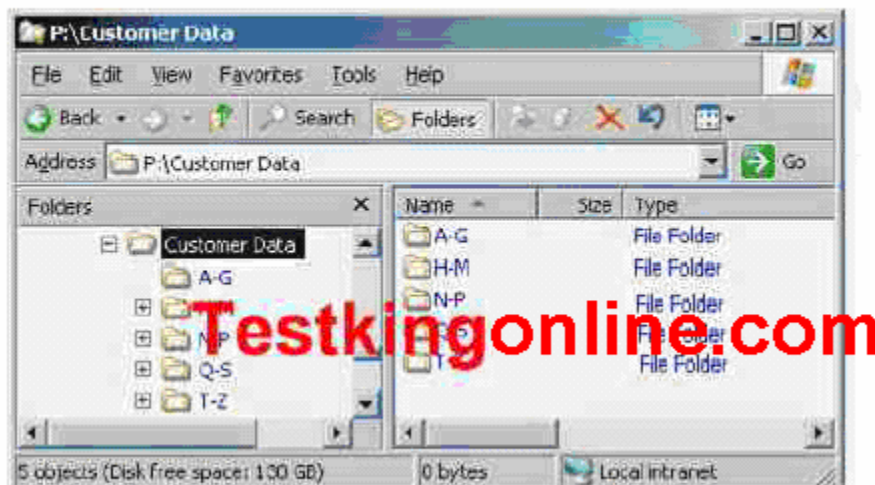
E: You should enable the Telnet service only if you see a real need for it, especially since the other administrative tools at your disposal offer more features and far better security. The Telnet service should remain disabled unless a need arises that requires it. In this instance it would be unnecessary.

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 NO: 5

You need to design a monitoring strategy for the folders that contain customer information, which are shown in the Customer Data window



c

What should you do?

- A. Audit success and failures for object access on the Customer Data folder and all subfolders.
- B. Audit failure of object access on only the Customer Data folder.
- C. Use Security Configuration and Analysis to enable auditing on only the Customer Data folder.
- D. Audit directory access failures.

Answer: A

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.

All customer information must be kept confidential. 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 needed as per the company's written security policy.

C: 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.

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

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

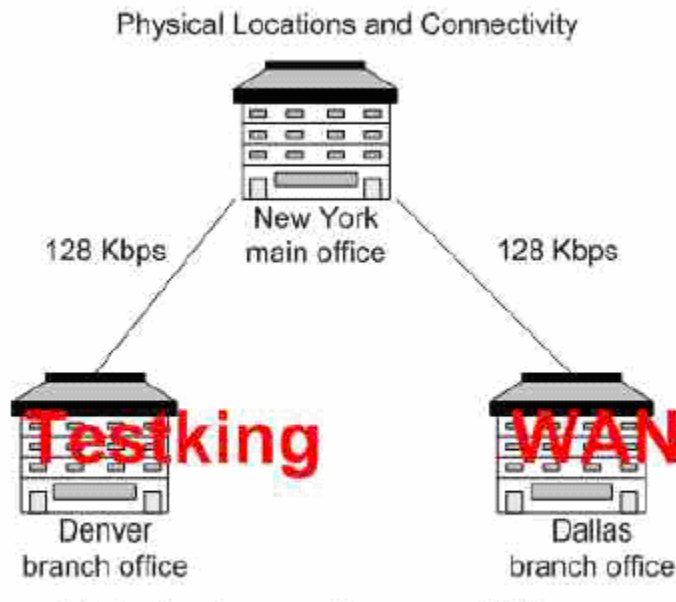
Case Study #3, Lucerne Publishing

Overview

Lucerne Publishing is an industry leader in publishing technology textbooks, e-books, and magazines.

Physical Locations

The company has three offices, as shown in the **Physical Locations and Connectivity** exhibit.



The company's main office is in New York, and it has branch offices in Denver and Dallas. The company's employees and departments are distributed as shown in the following table

Office location	Number of employees	Departments
-----------------	---------------------	-------------

New York	400	Editorial and information technology (IT)
----------	-----	---

Denver	95	Development
--------	----	-------------

Dallas	80	Production
--------	----	------------

Business Processes

The IT staff in the New York office uses client computers to remotely administer all Lucerne Publishing servers and domain controllers.

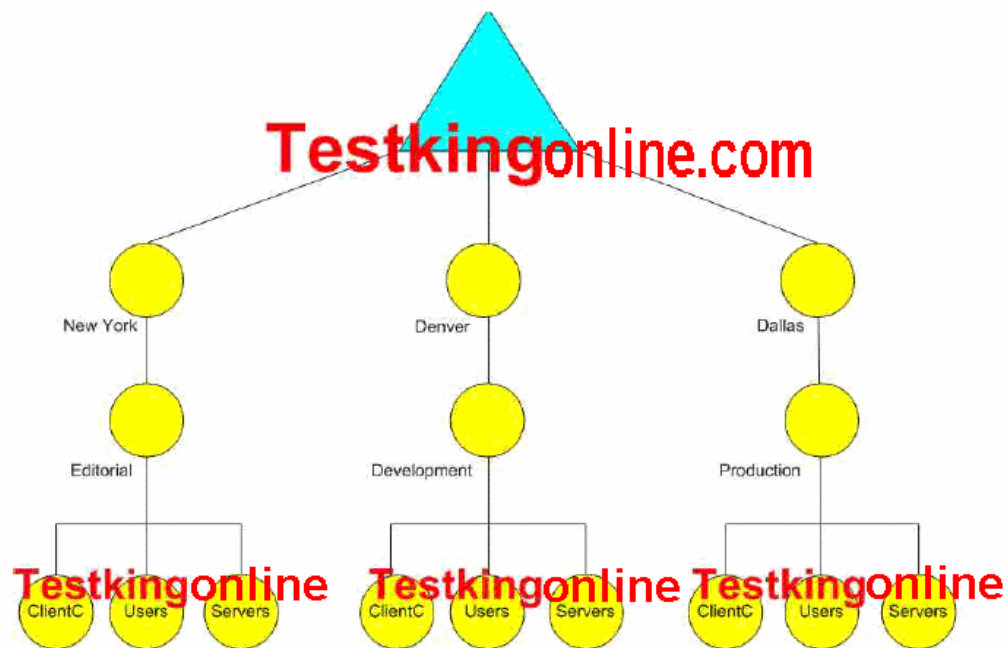
Employees use their company client computers to access archived published books and archived accounting information through an internal Web site that runs IIS 6.0.

Directory Services

The company's network consists of a single Active Directory domain named lucernepublishing.com. All servers run Windows Server 2003, Enterprise Edition. Administration of Active Directory is centralized in New York.

Denver and Dallas user and computer accounts are located in their respective child OUs, as shown in the

Organizational Unit Hierarchy exhibit.



The NYAdmins, ProductionAdmins, EditorialAdmins, and DevelopmentAdmins global user groups have full control of their respective organizational units (OUs). These global groups are located in their respective OUs.

Network Infrastructure

All client computers run Windows XP Professional.

The domain contains a public key infrastructure (PKI). The company uses an internal subordinate enterprise certification authority (CA) to issue certificates to users and computers.

Each branch office has a wireless network that supports desktop and portable client computers. The wireless network infrastructure in each branch office contains an Internet Authentication Service (IAS) server and wireless access points that support IEEE 802.1x, RADIUS, and Wired Equivalent Privacy (WEP).

Problem Statements

The following business problems must be considered:

Members of the EditorialAdmins group and unauthorized users as members to this group. Members of this group must be restricted to only authorized users.

Editors connect to a shared folder named Edits on a member server named Server5. When they attempt to encrypt data located in Edits, they receive an error message stating that they cannot encrypt data.

Editors need to encrypt data remotely on Server5.

Some users in the Dallas office changed the location of their My Documents folders to shared folders on

servers that do not back up their My Documents data. As a result, data was lost. The Dallas My

Documents folders need to be moved to a server that backs up user data. Users in the Dallas office must

be prevented from changing the location of their My Documents folder in the future.

Chief Information Officer

Security is Lucerne Publishing's primary concern. We must improve security on client computers, servers, and

domain controllers by implementing a secure password policy. For legal reasons, we need a logon message that

tells users that access to servers in the development department is restricted to only authorized users.

System Administrator

Each department needs different security patches. We need to test security patches prior to deploying them.

After they are tested, the patches need to be deployed automatically to servers in each department. As we

deploy the patches, we need to limit the network bandwidth used to obtain security patches.

Chief Security Officer

We need to automatically track when administrators modify user rights on a server or on a domain controller

and when they modify local security account manager objects on servers.

We must implement the most secure method for authenticating Denver and Dallas users that access the wireless networks.

We need to protect data as it is sent between the wireless client computers and the wireless access points. Client

computers need to automatically obtain wireless network access security settings.

Written Security Policy

The Lucerne Publishing written security policy includes the following requirements.

Passwords must contain at least seven characters and must not contain all or part of the user's account

name. Passwords must contain uppercase and lowercase letters and numbers. The minimum password

age must be 10 days, and the maximum password age must be 45 days.

Access to data on servers in the production department must be logged.

A standard set of security settings must be deployed to all servers in the development, editorial, and

production departments. These settings must be configured and managed from a central location.

Servers in the domain must be routinely examined for missing security patches and service packs and to

ascertain if any unnecessary services are running.

Services on domain controllers must be controlled from a central location. Which services start

automatically and which administrators have permission to stop and start services must be centrally

managed.

The IIS server must be routinely examined for missing IIS Security patches.

Users of the Web site and the files they download must be tracked. This data must be stored in a

Microsoft SQL Server database.

Vendors and consultants 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

company's network.

Case Study #3, Lucerne Publishing (13 Questions)

QUESTION NO: 1

You need to design a certificate distribution method that meets the requirements of the chief security officer. Your solution must require the minimum amount of user effort. What should you do? To answer, move the appropriate actions from the list of actions to the answer area, and arrange them in the appropriate order.

Actions

Instruct the users in Dallas and in Denver to submit a request for a user certificate from the CA Web site enrollment page.

Create a Group Policy object (GPO) and link it to the Dallas OU and to the Denver OU.

Configure the Group Policy object (GPO) to allow autoenrollment of user and computer certificates.

Instruct the Dallas and Denver users to run the **gpupdate** command.

Instruct the Dallas and Denver users to run the **cipher** command.

Configure certificate templates and the CA to allow autoenrollment of user and computer certificate.

Answer Area

Answer:

Actions

Instruct the users in Dallas and in Denver to submit a request for a user certificate from the CA Web site enrollment page.

Instruct the Dallas and Denver users to run the **gpupdate** command.

Instruct the Dallas and Denver users to run the **cipher** command.

Answer Area

Configure certificate templates and the CA to allow autoenrollment of user and computer certificate.

Create a Group Policy object (GPO) and link it to the Dallas OU and to the Denver OU.

Configure the Group Policy object (GPO) to allow autoenrollment of user and computer certificates.

Explanation: *Auto-enrollment* will automatically issue certificates without a CA administrator. This feature

was available in Windows 2000 Server. We could auto-enroll computer certificates in Windows 2000; however, we could not auto-enroll user certificates. The user details could be verified to a higher level of detail. Windows

Server 2003 has a better model of integrating with Active Directory. Therefore, auto-enrollment for users is

available under Windows Server 2003.

Auto-enrollment features are set by CA administrators in the *certificate templates*.

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

cuts down on administrative effort that has to be put in when applying the same policies on an individual basis.

Incorrect answers:

The *gpupdate* command forces a policy update and the *cipher* command will display the encryption state of the current folder and all files within the folder. It can be used to encrypt and decrypt files on NTFS volumes.

Instructing users to *submit requests* for a user certificate from the CA web site enrollment page is not efficient

enough. Neither is instructing each user to run a specific command.

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 NO: 2

You need to design a method to configure the servers in the development department to meet the requirements of the chief information officer.

What should you do?

A. Use error reporting on all servers in the development department to report errors for a custom application.

B. Configure all servers in the development department so that they do not require the CTRL+ALT+DELTE keys to pressed in order to log on interactively to the server.

C. Create a Group Policy object (GPO) and link it to the development department's Servers OU. Configure

the GPO with an interactive logon policy to display a message for users who attempt to log on.

D. Configure the screen saver on all servers in the development department to require a password.

Answer: C

Explanation: GPOs can be applied to sites, domains, or organizational units. It cuts down on administrative effort. 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.

We need a logon message that tells users that access to servers in the development department is restricted to authorized users only.

We must improve security on client computers, servers, and domain controllers by implementing a secure password policy.

Incorrect answers:

A: This option suggests a procedure that is administratively intensive.

B: 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.

D: A screensaver requiring a password is not complying with security policy since the servers would still be available from other workstations through the 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 10, p. 641

QUESTION NO: 3

You need to design a method to log changes that are made to servers and domain controllers. You also need to track when administrators modify local security account manager objects on servers.

What should you do?

A. Enable failure audit for privilege user and object access on all servers and domain controllers.

B. Enable success audit for policy change and account management on all servers and domain controllers.

C. Enable success audit for process tracking and logon events on all servers and domain controllers.

D. Enable failure audit for system events and directory service access on all servers and domain controllers.

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:

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. 537-540

QUESTION NO: 4

You need to design a strategy to ensure that all servers are in compliance with the business requirements for maintaining security patches.

What should you do?

A. Log on to a domain controller and run the Resultant Set of Policy wizard in planning mode on the domain.

- B. Log on to each server and run Security Configuration and Analysis to analyze the security settings by using a custom security template.
- C. Create a logon script to run the **secedit** command to analyze all servers in the domain.
- D. Run the Microsoft Baseline Security Analyzer (MBSA) on a server 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 company regulations regarding business requirements for maintaining security patches.

Servers in the domain must be routinely examined for missing security patches and service packs and to ascertain if any unnecessary services are running.

The IIS server must be routinely examined for missing IIS Security patches.

The IT staff in the New York office uses client computers to remotely administer all Lucerne Publishing servers and domain controllers.

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. This is not what is needed.

B: Security Configuration and Analysis tool 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. 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
Roberta Bragg, MCSE Self-Paced Training Kit (Exam 70-298): Designing Security for a Microsoft Windows Server 2003 Network, Chapter 5, p. 4

QUESTION NO: 5

You need to design a method to monitor the security configuration of the IIS server to meet the requirements in the written security policy.

What should you do?

- A. Log on to a domain controller and run the Resultant Set of Policy wizard in planning mode on the IIS server computer account.
- B. Run the Microsoft Baseline Security Analyzer (MBSA) on the IIS server and scan for vulnerabilities in Windows and IIS checks.
- C. Run Security Configuration and Analysis to analyze the IIS server's security settings by using a custom security template.
- D. On the IIS server, run the **gpresult** command from a command prompt and analyze the output.

Answer: B

Explanation: MBSA can perform local or remote scans of Windows systems. Microsoft Baseline Security Analyzer (MBSA) is a utility you can download from the Microsoft website to ensure that you have the most current security updates. 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. The IIS server must be routinely examined for missing IIS Security patches.

Incorrect answers:

A, C & D: There are essentially three ways to tell what the resulting security settings are: First, you can use the *Security Configuration and Analysis snap-in* to analyze the local computer. You can also use the *secedit* command to analyze the local computer or any other computer or computer group (multiple computers can be analyzed via the *secedit* command). You can also use a snap-in called *Resultant Set of Policy (RSOP)*. This

allows you to see the results of the policies applied to a particular computer. However, telling which settings are applied is not the same concept as monitoring the security configuration of the IIS server to meet the requirements in the written security policy.

Reference:

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

QUESTION NO: 6

You need to design a monitoring strategy to meet business requirements for data on servers in the production department. What should you do?

- A. Use the Microsoft Baseline Security Analyzer (MBSA) to scan for Windows vulnerabilities on all servers in the production department.
- B. Run Security and Configuration Analysis to analyze the security settings of all servers in the production department.
- C. Enable auditing for data on each server in the production department. Run System Monitor on all servers in the production department to create a counter log that tracks activity for the Objects performance object.
- D. Create a Group Policy Object (GPO) that enables auditing for object access and link it to the product department's Servers OU. Enable auditing for data on each server in the production department.

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. Further more making use of a GPO will ease the administrative effort. Linking this GPO to the product department's Servers OU should be the strategy used to monitor the data on the serves in the production department.

Access to data on servers in the production department must be logged.

We must implement the most secure method for authenticating Denver and Dallas users that access the wireless networks.

Some users in the Dallas office changed the location of their My Documents folders to shared folders on

servers that do not back up their My Documents data. As a result, data was lost. The Dallas My Documents folders need to be moved to a server that backs up user data. Users in the Dallas office must be prevented from changing the location of their My Documents folder in the future.

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 in the production department 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 production department. However multiple computers can be analyzed via the *secedit* command. This option is not a complete solution if it suggests only making use of the Security Configuration and Analysis snap-in.

C: You should be logging all access to data on the servers in the production department. Thus running a counter log that tracks the activity for the Object Performance object is not going to yield the proper information.

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 NO: 7

You need to design a method to deploy security patches that meets the requirements of the system administrator. What should you do?

To answer, move the appropriate actions from the list of actions to the answers area and arrange them in the appropriate order (Use only actions that apply. You might need to reuse actions.)

Actions

Place here

***...server. Configure the server to synchronise security patches with the Windows update servers.

Configure all departmental servers to download security patches from the Windows Update Catalog servers.

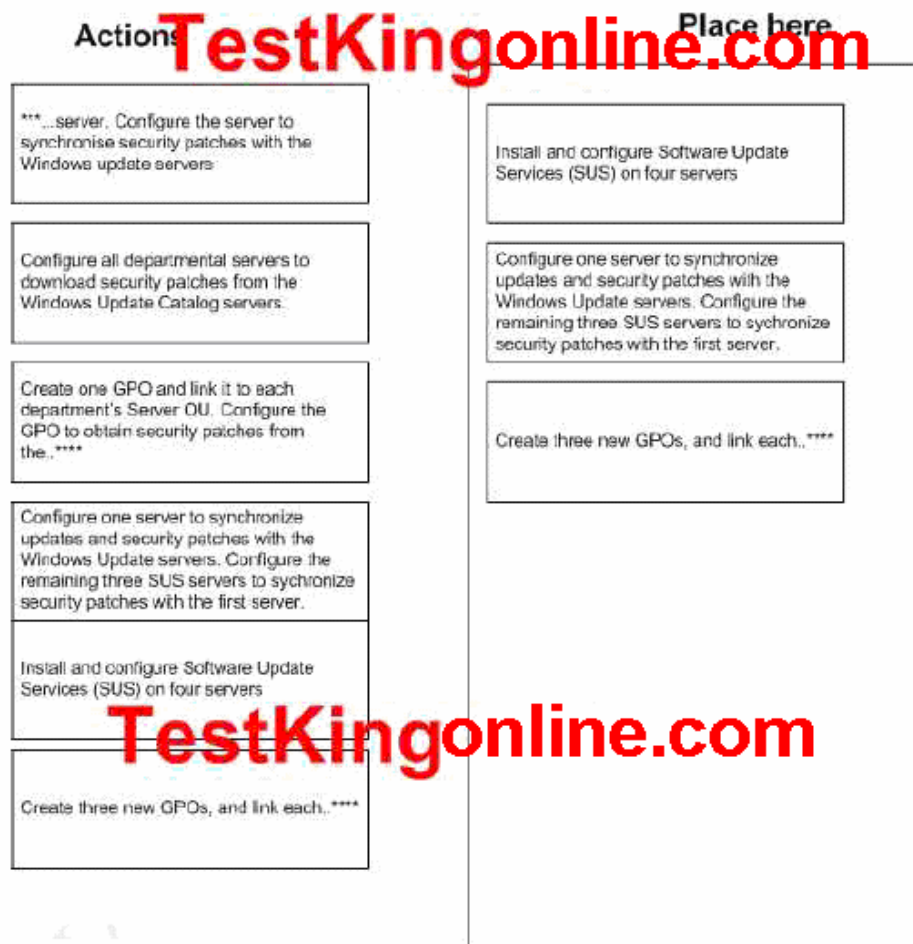
Create one GPO and link it to each department's Server OU. Configure the GPO to obtain security patches from the...****

Configure one server to synchronize updates and security patches with the Windows Update servers. Configure the remaining three SUS servers to synchronize security patches with the first server.

Install and configure Software Update Services (SUS) on four servers

Create three new GPOs, and link each...****

Answer:



Explanation: The system administrator's requirements are:

Each department needs different security patches.

We need to test security patches prior to deploying them.

After they are tested, the patches need to be deployed automatically to servers in each department.

As we deploy the patches, we need to limit the network bandwidth used to obtain security patches.

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 cuts down on administrative effort that has to be put in when applying the same policies on an individual basis.

SUS allows you to maintain what is effectively an internal Windows Update Web site, where your SUS server contacts the actual Windows Update Web site and downloads updates that an administrator can review and

approve for deployment. SUS has many advantages over Windows Update, the most obvious of which is that with SUS; you can control and approve the patches that are installed. Your first step would be to install SUS on the four servers. Secondly, you need to configure one server to synchronize updates and security patches with the Windows Update servers and the other three to synchronize with the first server. Thirdly you should make use of GPOs.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows® Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 21
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 4, pp. 210-213

QUESTION NO: 8

You need to design a method to protect traffic on the wireless network. Your solution must meet the requirements of the chief security officer. What should you do?

- A. Configure the wireless access points in Denver and Dallas to filter unauthorized Media Access Control (MAC) addresses
- B. Configure the wireless network connection properties for all computers in Denver and in Dallas to use the same network name that the wireless access points use.
- C. Create a GPO and link it to the Denver OU and to the Dallas OU. Create a wireless network policy and configure it to use Windows to configure wireless network settings for the Denver and the Dallas networks.
- D. Create a GPO and link it to the Denver OU and to the Dallas OU. Create a wireless network policy and enable data encryption and dynamic key assignments for the Denver and Dallas networks

Answer: D

Explanation: Following is the relevant information regarding the wireless network and the chief security officer's requirements:

Each branch office has a wireless network that supports desktop and portable client computers. The wireless network infrastructure in each branch office contains an Internet Authentication Service (IAS)

server and wireless access points that support IEEE 802.1x, RADIUS, and Wired Equivalent Privacy (WEP).

We need to protect data as it is sent between the wireless client computers and the wireless access points. Client computers need to automatically obtain wireless network access security settings.

We must implement the most secure method for authenticating Denver and Dallas users that access the wireless networks.

EFS is an encryption strategy for files and folders includes an assessment of vital data, an assessment of the environment, policies for using EFS, and procedures for recovering encrypted files. Files that contain sensitive data should be protected with EFS. However, EFS is not used to encrypt data traveling across the network, it does not authenticate users, it cannot be used to secure dial-in or VPN connections, and it cannot encrypt data on computers running other non-Windows operating systems. To be able to protect traffic on the wireless network you should create a GPO, linked to the Dallas and Denver OUs, that encrypts data as well as assign dynamic keys.

Incorrect answers:

A: Filtering unauthorized MAC addresses will not work because Remote policies don't allow you to deliver a unique IP address. Furthermore excluded addresses are just marked as excluded; the DHCP server doesn't maintain any information about them.

B: Configuring all computers in Denver and Dallas to use the same network name that the wireless accesspoints use will not be the proper procedure to follow.

C: You need create a network policy and enable data encryption and dynamic key assignments, not just configuring network settings for Denver and Dallas.

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 1 & 9, pp. 35, 571-576

QUESTION NO: 9

You need to design a strategy to log access to the company Web site. What should you do?

A. Enable logging on the company Web site and select the NCSA Common Log File Format. Store the log

files on a SQL Server computer.

B. Use System Monitor to create a counter log that captures network traffic to the Web server by using the

Web Service object. Store the log files on a SQL Server computer.

C. Run the Network Monitor on the Web server. Create a capture filter for the SNA protocol and save the

results to a capture file. Store the capture file on a SQL Server computer.

D. Enable logging on the company Web site and select ODBC Logging. Configure the ODBC logging

options by using a nonadministrative SQL account.

Answer: D

Explanation: You should enable logging on the company web site and select ODBC logging. Open Database

Connectivity (ODBC) - You can log data directly to a SQL database using an Open DataBase Connectivity

(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.

Users of the Web site and the files they download must be tracked. This data must be stored in a

Microsoft SQL Server database.

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: The System Monitor utility is used to collect and measure the real-time performance data for a local or

remote computer on the network. However, this is not what is required in this question.

C: SNA is a specialty IBM protocol used in networks. But this is not what is in use in this case.

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 NO: 10

You need to design a method to deploy security configuration settings to servers. 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 local policy to configure and manage the security settings.
- C. Create a customer security template. Log on to a domain controller and run the **secedit** command to import the security template.
- D. Create a customer security template. Create a GPO and import the security template. 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.

A standard set of security settings must be deployed to all servers in the development, editorial, and production departments. These settings must be configured and managed from a central location.

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

QUESTION NO: 11

You need to design a group membership strategy for the EditorialAdmins group. What should you do?

- A. Move the EditorialAdmins group to the Servers OU in the editorial department.
- B. Move the members of the EditorialAdmins group to the Editorial OU.
- C. Move the members of the EditorialAdmins group to the New York OU.
- D. Move the EditorialAdmins group to the New York OU.

Answer: D

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 EditorialAdmins group comprises of both authorized and unauthorized users, the whole group should be moved to the New York OU so as to restrict membership to this group to authorized users only.

Members of the EditorialAdmins group and unauthorized users as members to this group. Members of this group must be restricted only to authorized users.

The NYAdmins, ProductionAdmins, EditorialAdmins, and DevelopmentAdmins global user groups have full control of their respective organizational units (OUs).

Incorrect answers:

A: Moving the EditorialAdmins group to the Servers OU in the editorial department is not going to restrict unauthorized members.

B & C: Moving the members of the EditorialAdmins group to the Editorial OU or the New York OU will not work as you need to move the whole EditorialAdmins group to the New York 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 NO: 12

You need to design a method to enable remote encryption on Server5. What should you do?

- A. Configure the editor's user account properties to enable **Store password using reversible encryption**.
- B. Configure the editor's user account properties to enable **Use DES encryption for this account**.
- C. Configure the Local Security Policy on Server to enable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** security policy.
- D. Configure the Server5 computer account properties to enable **Trust computer for delegation**.

Answer: D

Explanation: Delegation is when a higher security authority assigns administrative permissions to a lesser authority. The Enable Computer And User Accounts To Be Trusted For Delegation allows a user or group to set the Trusted For Delegation setting for a user or computer object. Enabling the Trust computer for delegation in the account properties of Server5 will enable remote encryption capabilities.

Editors connect to a shared folder named Edits on a member server named Server5. When they attempt to encrypt data located in Edits, they receive an error message stating that they cannot encrypt data. Editors need to encrypt data remotely on Server5.

Incorrect answers:

A: Making use of the editor's user account to enable Store password using reversible encryption will not enable remote encryption.

B: Enabling DES encryption for this account from the editor's user account is not enabling remote encryption.

C: Configuring the Local Security Policy to enable the System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing security policy is not enabling remote encryption.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows® Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 118

QUESTION NO: 13

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

- A. Create a GPO and link it to the New York OU, to the Denver OU, and to the Dallas OU. Configure the GPO with the required account policy settings.
- B. On all computers in the domain, configure the Local Security Policy⁷ with the required account policy settings.
- C. Configure the Default Domain Policy GPO with the required account policy settings.
- D. Configure the Default Domain Controllers Policy GPO with the required account policy settings.

Answer: C

Explanation: Following is the requirements of account policies as per the company's written security policy requirements:

Passwords must contain at least seven characters and must not contain all or part of the user's account name. Passwords must contain uppercase and lowercase letters and numbers. The minimum password age must be 10 days, and the maximum password age must be 45 days. 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: Policies should be set in the Default Domain Policy GPO then it will set all the computers in the domain.

This option is obsolete.

B: Configuring Local Security Policy⁷ as this option suggests is not the way to implement account policies that meets the company's written security policy.

D: You should configure the Default Domain Policy GPO and not the Domain Controllers GPO.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows® Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 147

Case Study #4, Southbridge Video

Overview

Southbridge Video is a home video retailer. The company sells a variety of movies, documentaries, and foreign films.

Southbridge Video recently acquired Contoso, Ltd., which provides shipping services.

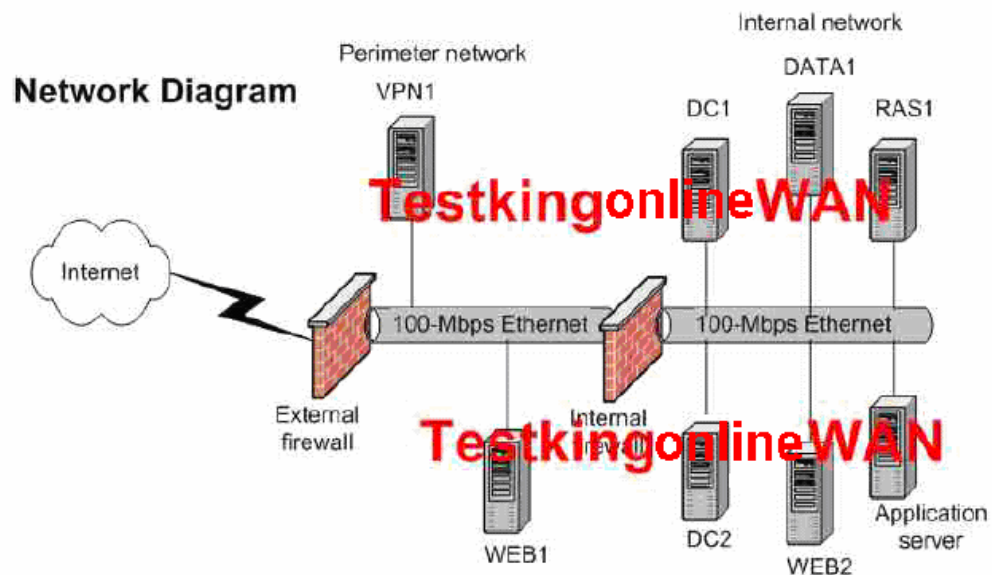
Physical Locations

Southbridge Video's main office is in Atlanta. The company also has six retail stores throughout the United States.

Contoso, Ltd., is located in Dallas.

Planned Changes

The company's proposed network infrastructure is shown in the **Network Diagram** exhibit.



A VPN server named VPN2 will be placed in the perimeter network. Mobile users will use VPN2 to connect to the company network.

All client computers in the Atlanta office, except those used by the HR department, will be upgraded to Windows XP Professional.

A Web server named WEB2 will be installed on the company's internal network for development and testing.

Business Processes

Southbridge Video consists of the following departments:

Human Resources (HR)

Accounting

Administration

Marketing

Customer service

Information technology

Internet users must register with Southbridge Video to purchase videos from the company's Web site. This

information is stored in a database. These users are then classified as Web customers and their logon

information is set to them in an e-mail message.

Web customers connect to a virtual directory named Members. After they are authenticated, Web customers can

view available merchandise and place orders by using a Web application that is running on a Web server named

Web1. After the Web customer places an order, the request is submitted to Contoso, Ltd., for packaging and shipping.

A record of all customer activity is stored on a shared folder named TRANS, which is located on a server

named DATA1. The share permissions for the TRANS folder are set to assign the **Allow – Full Control**

permission to the Authenticated Users group.

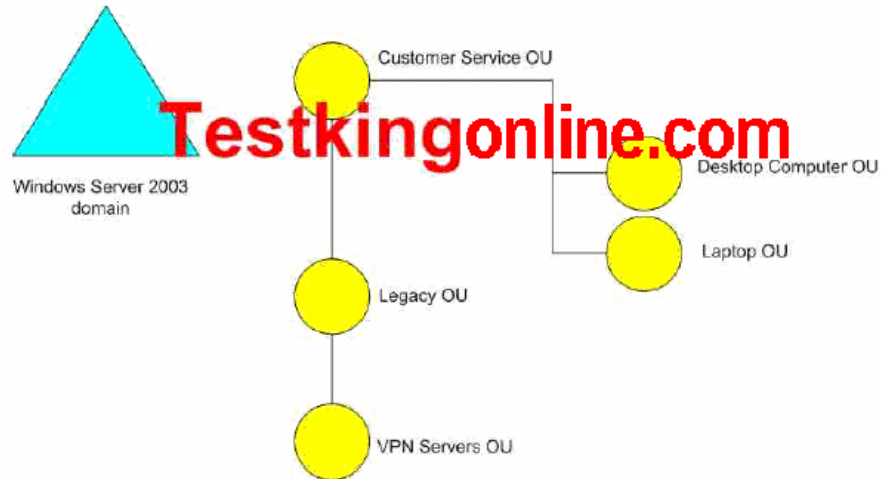
Active Directory

The network consists of a single Active Directory domain. All servers run Windows Server 2003. All client

computers run either Windows NT Workstation 4.0 or Windows 98. All computers run the latest service packs.

The relevant portion of the organizational unit (OU) structure is shown in the **OU Diagram** exhibit.

OU Diagram



The Laptop OU contains the computer accounts for the portable computers. The Desktop Computers OU contains computer accounts for desktop computers. All user and computer accounts for the HR department are located in the Legacy OU.

Network Infrastructure

The Atlanta office contains a wireless LAN.

The network contains two Microsoft Internet Security and Acceleration (ISA) Server 2000 computers named ISA1 and ISA2.

A public Web site is hosted on a server running IIS 6.0 named WEB1. Users at Contoso, Ltd., have access to Web1 by means of a VPN tunnel established between Southbridge Video and Contoso, Ltd.

The HR department uses a custom application that can run only on Windows NT Workstation 4.0.

The customer service department stores personnel information on a file server named SRV1. SRV1 is also configured as an offline stand-alone root certification authority (CA).

Problem Statements

The following business problems must be considered:

After the planned upgrades occur, the HR department users will no longer be able to change their passwords while they are logging on to their client computers.

No users currently possess user certificates. Administrators do not have time to assist all users.

Chief Information Officer

Our Internet connection has been overutilized in the past few months, and therefore measures must be taken not to place extra strain on this connection.

I have read about various buffer overflow attacks against Web servers. If such an attack occurs against my public Web server, I want to be able to redirect the user request to an HTML document that stipulates the legal consequences.

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.

Chief Security Officer

There are many reasons that we need to redesign the company's security management policies and practices. I

am concerned that our current wireless configuration makes our network vulnerable to attack. I am also

concerned about the security of the servers that users from Contoso, Ltd., can access.

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).

Recently, users downloaded and installed unauthorized software from the Internet. This caused several

computers on the company network to stop responding.

A small number of mobile users will connect to the company network. We need to ensure the security of these

connections.

Written Security Policy

The relevant portion of Southbridge Video's written security policy includes the following requirements:

Only users in the customer service department must be able to connect to the wireless network.

String authentication is required for the wireless network.

Communication between the customer service department and SRV1 must be secure and encrypted at all times.

Only members of the customer service department who have portable computers are allowed to encrypt data.

The customer service department must have its own data recover agent.

Two-factor authentication must be implemented for users in the accounting department.

Information stored in the TRANS folder must be encrypted and accessible to only the IT department staff.

All traffic to the Member virtual directory on WEB1 must be encrypted.

Web customers must be able to verify the identity of WEB1.
All attempts to log on to Windows Server 2003 and Windows XP Professional computers that involve the use of local user accounts must be tracked.
Only IT administrator must be able to remotely modify the registry on WEB2.
All software must be approved for company use.
VPN2 must support MS-CHAP v2 authentication.

Case Study #4, Southbridge Video (9 Questions)

QUESTION NO: 1

You need to design an audit strategy for Southbridge Video. Your solution must meet business requirements.

What should you do?

A. Create a new security template that enables the **Audit account logon events** policy for successful and failed attempts.

Create a new GPO, and link it to the domain.

Import the new security template into the new GPO.

B. Create a new security template that enables the **Audit account logon events** policy for successful and failed attempts.

Create a new GPO, and link it to the Domain Controllers OU.

Import the new security template into the new GPO.

C. Create a new security template that enables the **Audit logon events** policy for successful and failed attempts.

Create a new GPO, and link it to the Domain Controllers OU.

Import the new security template into the new GPO.

D. Create a new security template that enables the **Audit logon events** policy for successful and failed attempts. Create a new GPO, and link it to the domain. Import the new security template into the new GPO.

Answer: D

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.

Internet users must register with Southbridge Video to purchase videos from the company's Web site.

This information is stored in a database. These users are then classified as Web customers and their

logon information is set to them in an e-mail message.

A record of all customer activity is stored on a shared folder named TRANS, which is located on a server named DATA1.

Incorrect answers:

A: Linking the new GPO to the domain is correct, but it should be enabling Audit logon events instead.

B: You should be enabling the Audit logon events for success and failed attempts and not the Audit account

logon events. Furthermore you should link the new GPO to the domain and not the Domain Controllers OU.

C: Enabling the Audit logon events for success and failure is correct. However, you should link the new GPO to the domain and not the Domain Controllers OU.

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 NO: 2

You are designing an access control strategy for WEB2. Your solution must meet business requirements. What should you do?

A. Install the Terminal Services Advanced Client Web client on WEB2.

B. Modify the **Winreg** registry key on WEB2.

C. Install the RPC over HTTP service on WEB2.

D. Modify the **RestrictAnonymous** registry key on WEB2.

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 what is needed is to modify the **Winreg** registry key on Web2.

A Web server named WEB2 will be installed on the company's internal network for development and testing.

Only IT administrator must be able to remotely modify the registry on WEB2.

Incorrect answers:

A: This is not an access control measure.

C: Allowing RPC assignment over HTTP service is an unacceptable solution because the risk of also allowing unwanted traffic to enter is high.

D: Modifying the RestrictAnonymous registry key is not the answer.

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 NO: 3

You need to design a method to address the chief information officer's security concerns.

What should you do?

A. Configure Windows Management Instrumentation (WMI) filtering options in the Default Domain Policy GPO.

B. Use the **gpresult** command.

C. Use Mbsacl.exe.

D. Configure software restriction policy options in the Default Domain Policy GPO.

Answer: C

Explanation: Mbsaccli.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.

Our Internet connection has been overutilized in the past few months, and therefore measures must be taken not to place extra strain on this connection.

I have read about various buffer overflow attacks against Web servers. If such an attack occurs against my public Web server, I want to be able to redirect the user request to an HTML document that stipulates the legal consequences.

Incorrect answers:

A: Windows Management Instrumentation (WMI) provides an object-based method for accessing management information in a network. It provides a programming interface for developers to design management tools.

However, this is not what is required in this instance.

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: Setting policies in the Default Domain Policy sets them for all computers in the domain. This is not what is required in this question.

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 NO: 4

You need to design a security strategy for VPN2. Your solution must meet business requirements.

What should you do?

- A. Create and configure a new security template.
Import the template into the Default Domain Policy Group Policy object (GPO).
- B. Install Internet Authentication Service (IAS) on RAS1.
Configure VPN2 to be the RADIUS client of RAS1.
Configure the remote access policy on VPN2.
- C. Create and configure a new security template.
Import the template into the local policy on VPN2.
- D. Move VPN2 into the VPN Servers OU.
Configure the remote access policy on VPN2.

Answer: D

Explanation: A security strategy for VPN2 should be moving it into the VPN Servers OU and then configuring the remote access policy on it because all user and computer accounts for the HR department are located in the

Legacy OU. And the VPN Servers OU is connected to the Legacy OU.

A VPN server named VPN2 will be placed in the perimeter network. Mobile users will use VPN2 to connect to the company network.

VPN2 must support MS-CHAP v2 authentication.

Incorrect answers:

A: There is no need to configure a new security template and importing it.

B: 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.

C: A new security template and importing it, is not necessary. All that has to be done is to move VPN2 into the VPN Servers OU and then configure remote access policy on VPN2.

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 NO: 5

You are designing an authentication strategy for the accounting department. Your solution must meet business requirements.

What should you do?

A. Install wireless network cards on all accounting department computers.

Select PEAP authentication.

B. Install user certificates on all accounting department computers.

Configure these computers to respond to requests for IPSec encryption.

C. Issue smart cards and smart card readers to all accounting department users and computers.

Require NTLMv2 authentication.

D. Issue smart cards and smart card readers to all accounting department users and computers.

Configure the domain to require smart cards for the accounting department users during logon.

Answer: D

Explanation: Following are the relevant information regarding an authentication strategy for the accounting department as described in the case study:

The customer service department stores personnel information on a file server named SRV1. SRV1 is also configured as an offline stand-alone root certification authority (CA).

I want to implement companywide user certificates as the first phase of our new authentication strategy.

Two-factor authentication must be implemented for users in the accounting 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 accounting 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 thirdparty authentication methods that you can retrofit to your existing servers. This is not what is required.

B: Making use of user certificates and configuring all accounting department computers to respond to requests for IPsec encryption is not going to enforce two-factor authentication.

C: 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 NO: 6

You need to design a security solution for WEB1. Your solution must address the chief information officer's concerns.

What should you do?

- A. Enable Web distributed Authoring and Versioning (WebDAV) components on WEB1.
- B. Install and configure the URLScan ISAPI filter on WEB1.
- C. Install a computer certificate on WEB1, and enable the Server (Request Security) IPsec policy on WEB1.
- D. Configure the Web site redirection option on the properties of WEB1 in the Internet Service Manager console.

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 WEB1 is running IIS 6.0 this option is the answer.

A public Web site is hosted on a server running IIS 6.0 named WEB1. Users at Contoso, Ltd., have access to Web1 by means of a VPN tunnel established between Southbridge Video and Contoso, Ltd.

Our Internet connection has been overutilized in the past few months, and therefore measures must be taken not to place extra strain on this connection.

I have read about various buffer overflow attacks against Web servers. If such an attack occurs against my public Web server, I want to be able to redirect the user request to an HTML document that stipulates the legal consequences.

Incorrect answers:

A: WebDAV 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. But this alone will not address the chief information officer’s concerns.

C: Server (Request Security) is a combination of Client (Respond Only) and Secure Server (Require Security).

This policy will always attempt to use IPSec by requesting it when it connects to a remote machine and by allowing IPSec when an incoming connection requests it. But this is unnecessary since WEB1 runs on IIS 6.0 all you need is to install and configure URLScan ISAPI filter on WEB1.

D: Configuring a Web site redirection option on the properties of WEB1 in the Internet Service Manager console is not applicable in this scenario.

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 NO: 7

You need to design a software usage policy for the employees of Southbridge Video. The policy must meet business requirements. What should you do?

- A. Configure the software restriction policy in the Default Domain Policy Group Policy object (GPO).
- B. Create a new connection object by using the Connection Manager Administration Kit (CMAC), and install the new connection object on all client computers.
- C. Create and configure a local security policy on both of the ISA server computers.
- D. Configure the Internet Explorer settings in the Default Domain Policy Group Policy object (GPO).

Answer: A

Explanation:

The HR department uses a custom application that can run only on Windows NT Workstation 4.0.

Recently, users downloaded and installed unauthorized software from the Internet. This caused several computers on the company network to stop responding.

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: Installing a new connection object on all client computers is not going to restrict the downloading and installation of unauthorized software.

C: Creating a local security policy on both the ISA servers will not help in this scenario.

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 NO: 8

You need to design phase one of the new authentication strategy. Your solution must meet business requirements.

What should you do?

A. Install a Windows Server 2003 enterprise root CA.

Configure certificate templates for autoenrollment.

B. Install a Windows Server 2003 enterprise subordinate CA.

Configure certificate templates for autoenrollment.

C. Install a Windows Server 2003 stand-alone subordinate CA.

Write a logon script for the client computers in the HR department that contains the

Certreq.exe

command.

D. Install a Windows Server 2003 stand-alone root CA.

Write a logon script for the client computers in the HR department that contains the

Certreq.exe

command.

Answer: 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 CA. The enterprise can have a root CA as enterprise or a stand-alone CA.

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 CA. The root CA is the most important CA. 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 CA. 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.

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).

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:

A: Installing a Windows Server 2003 enterprise root CA is unnecessarily risky as described in the explanation above and will not do in this case.

C & D: First you need to install a Windows Server 2003 enterprise subordinate CA and not a Windows Server 2003 stand-alone subordinate CA. Stand-alone CA does not have the ability to self sign. Furthermore there is no need to write logon scripts for the client computers in the HR department.

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 NO: 9

You need to design a patch management strategy for Southbridge Video. Your solution must meet business requirements.

What should you do?

- A. Configure all client computers to use Automatic Updates to obtain security patches from the Windows Update Web site.
Test and install all patches.
- B. Configure a batch file to download security patches daily.

Distribute the security patches by using a .zap file and the Default Domain Policy Group Policy object (GPO).

C. Deploy a Software Update Services (SUS) server.

Test all security patches and then approve them.

Configure all client computers to automatically obtain updates from the server.

D. Configure a batch file to download security patches daily.

Manually install the security patches on all computers.

Answer: C

Explanation: The current situation regarding patch management is as follows:

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: To be able to carry out this option you first need to deploy a SUS server to enable Automatic Updates.

Furthermore obtaining updates from the Windows Update site will skip the process of testing and approving

updates first.

B: Configuring a batch file on a daily basis is time consuming as well as resource consuming. This is not

optimizing the process.

D: To manually install the security patches on all computers would be defeating insofar as time and resources

are concerned.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows ® Server 2003 Environment

Management and Maintenance Study Guide, p. 55

Case Study #5, Woodgrove Bank

Overview

Woodgrove bank provides personal and commercial banking services. Woodgrove Bank also provides financial and tax planning for customers.

Woodgrove Bank operates a 24-hour call center to support customers and partners.

Physical Locations

The company's main office is located in Los Angeles. The Los Angeles office has 1,000 employees.

The company has a regional office located in Denver. The Denver office has 800 employees.

There are 100 branch offices located in major cities throughout the western United States. Each branch office has between 10 and 20 employees.

Business Processes

Executive management for Woodgrove Bank is located in the Los Angeles office.

Regional management is located in the Los Angeles and Denver offices.

The Los Angeles office manages operations for all branch offices in California, Oregon, and Washington. The

Denver office manages operations for all branch offices in Colorado, New Mexico, Utah, and Arizona.

The Los Angeles and Denver offices each maintain a customer support call center.

The human resources (HR) department is located in Los Angeles.

The information technology (IT) department is located in both the Los Angeles and the Denver office. Each

office contains a data center, which provides IT services for its respective region. The IT department is

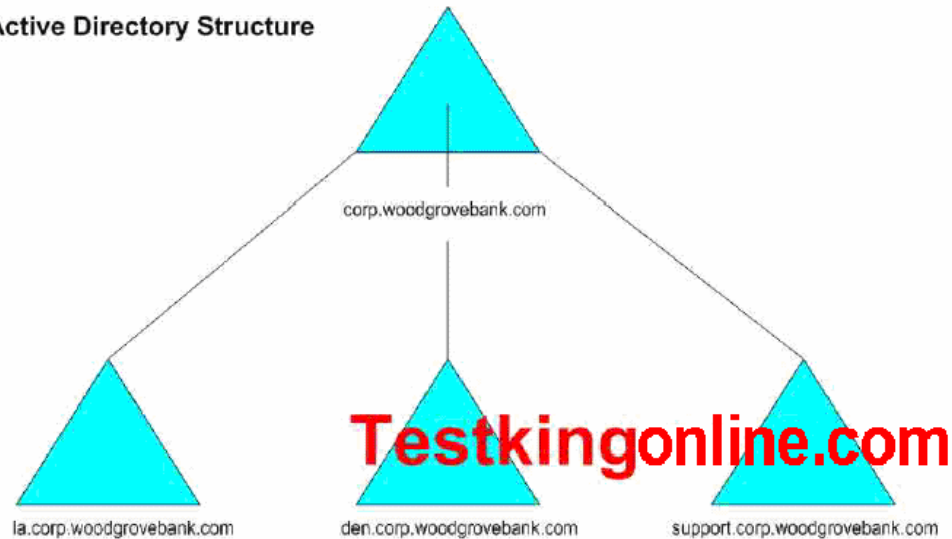
responsible for all administrative tasks for the network. There are no IT personnel at the branch offices.

Directory Services

The network consists of four Active Directory domains in a single forest as shown in the

Active Directory Structure exhibit.

Active Directory Structure



All help desk personnel have user accounts in the support.corp.woodgrovebank.com domain. These users are responsible for providing support to both internal and external customers. All members of the HR department are members of a group named LA\HRUsers. There is an organizational unit (OU) for each branch offices in their geographic area.

Network Infrastructure

All servers run Windows Server 2003. All client computers run Windows XP Professional.

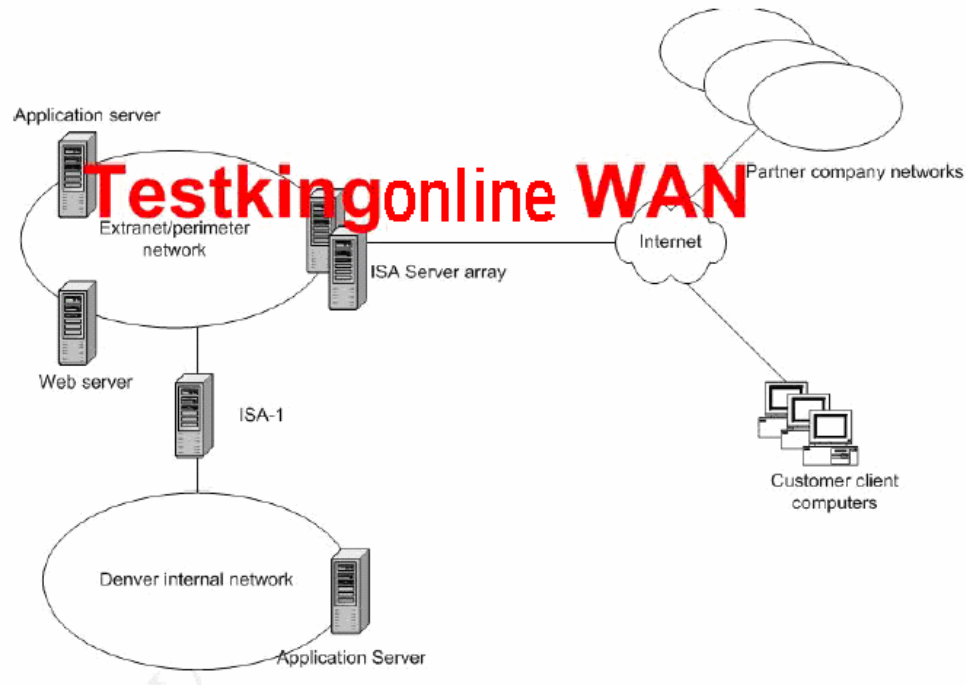
Wireless access points are installed in the Los Angeles and Denver offices. The wireless access points support the IEEE 802.11g specification and Wired Equivalent Privacy (WEP) encryption. The wireless access points support using certificates and RADIUS for authentication. Currently, no encryption or authentication methods are configured on the wireless access points.

The Los Angeles data center includes a test network for testing security patches and updates before they are deployed to the rest of the network.

The Los Angeles and Denver offices are connected by a dedicated WAN connection. Each branch office connects to its regional office by means of a frame-relay line.

The Los Angeles and Denver offices each have a dedicated connection to the Internet. The branch offices are not connected to the Internet.

Publicly accessible Web and application servers are located in a perimeter network as shown in the **Denver Extranet/Perimeter Network** exhibit.



The Web servers host an application that connects to a custom application hosted on a Windows Server 2003 computer in the Denver data center. The Web servers also host Web sites that contain publicly accessible information for both customers and the public. The perimeter network also functions as an extranet for partner company access.

A Windows Server 2003 computer named WebKiosk is installed in the Los Angeles data center. WebKiosk runs IIS 6.0 and hosts a Web site that is accessible by kiosk computers in each branch office. WebKiosk is a member of an OU named Kiosk. The kiosk computers use a user account named KioskUser to connect to the Web site.

Chief Information Officer

I am concerned with the security risks that the wireless network might pose to our network. I want to ensure that only authorized users and computers can connect 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, and recovery would be very expensive in terms of time and money.

IT Director

Patch management in our previous environment was expensive and time-consuming, often requiring travel by IT personnel to all branch locations. I want a method to deploy updates and automatically to all computers in the network.

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.

HR Directory

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.

Organizational Goals

The following organizational requirements must be considered:

Each customer support user works six hours at the call center and then is on call for four hours. These

users have portable computers and high-speed Internet access. These users need to be able to use

Terminal Services to run support applications from Windows Server 2003 computers in the call centers.

Woodgrove Bank partners with an external auditing company to provide audit services for customers.

The user from the audit company have access to the extranet in the Denver office. These users need to

be able to access file resources that are located on a server on the Denver internal network named

Server1.

IT personnel must be able to perform administrative tasks even when they are not at their desks. All IT

personnel have new portable computers that have wireless network adapters.

Tellers at the branch locations 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. However, users in the regional offices must be able to run their required

applications.

Security

The following security requirements must be considered:

All personnel data is stored on a server named HRSrv1. 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.

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.

Users from the audit company must be able to connect only to a Windows Server 2003 computer named TS-Server1. TS-Server1 runs Terminal Services and is located on the extranet. All access to resources on the internal network must occur through TS-Server1.

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 Woodgrove Bank certification authority (CA).

Customer Requirements

The following customer requirements must be considered:

Users from Partner companies require access to information stored on a Microsoft SQL Server 2000 computer that is located on the Denver internal network. Users on the internal network must also be able to access the information on the SQL Server by using Microsoft Access 2000.

Bank customers must be able to securely access their personal account information.

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.

Active Directory

The following Active Directory requirements must be considered:

The application used on the extranet application server requires changes to be made to the Active Directory schema. These modifications must not be applied to the rest of the network.

Currently all branch office network administration is performed by administrators in the Los Angeles office or the Denver office. The IT department wants to assign administration for all branch offices in a particular city to a single administrator. This administrator will be responsible for all user, group, and

resource management for only the branch offices in his or her city.

Help desk personnel require the ability to perform limited administrative tasks in the la.corp.woodgrovebank.com domain and the den.corp.woodgrovebank.com domain.

These tasks include

resetting users' passwords and creating new user accounts for branch office users. Help desk personnel

must not be able to perform any other administrative tasks.

Network Infrastructure

The following network infrastructure requirements must be considered:

All connections made over the frame-relay WAN connections must be encrypted and authenticated.

Certificate Services must be installed on at least one server in each domain. The configuration of CAs

must be based on the needs of each domain.

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.

Case Study #5, Woodgrove Bank (8 Questions)

QUESTION NO: 1

You need to design a remote access strategy for the customer support users when they work from home.

Your solution must meet security requirements.

What should you do?

A. Deploy an L2TP/IPsec VPN server in each call center.

Configure the portable computers as L2TP VPN clients.

B. Create IPsec tunnel mode connections between the customer support users home and the company's

Internet-facing routers.

C. Create IP packet filters on the company's Internet-facing routers to allow the Remote Desktop Protocol

(RDP).

Create IPsec filters on the terminal servers to allow only connections that use RDP.

D. Create IP packet filters on the company's Internet-facing routers to allow the IPsec protocols.

Assign the Secure Server (Require Security) IPsec policy to the terminal servers.

Assign the Client (Respond only) IPsec policy to the portable 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. Here's how the L2TP/IPSec combination works:

1. The client and server establish an IPSec security association using the ISAKMP and Oakley protocols. At this

point, the two machines have an encrypted channel between them.

2. The client builds a new L2TP tunnel to the server. Because this happens after the channel has been encrypted, there's no security risk.

3. The server sends an authentication challenge to the client.

4. The client encrypts its answer to the challenge and returns it to the server.

5. The server checks the challenge response to see whether or not it's valid; if so, the server can determine

which account is connecting. Subject to whatever access policies you've put in place, at this point the server

can accept the inbound connection.

Steps 3 through 5 mirror the steps for PPTP tunneling. This is because the authorization process is a function of

the remote access server, not the VPN stack. All the VPN does is provide a secure communications channel,

and something else has to decide who gets to use it.

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:

Woodgrove Bank operates a 24-hour call center to support customers and partners.

The Los Angeles and Denver offices each maintain a customer support call center.

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 portable

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 Internetfacing

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 portable 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 NO: 2

You need to design an access control strategy for resources that are located in the extranet for partners and for internal users. Your solution must meet business and security requirements.

What should you do?

A. Create a new child domain named extranet.corp.woodgrovebank.com in the existing forest.

Create user accounts for users from partner companies 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 extranet.woodgrovebank.com.

Create user accounts for users from partner companies in the new domain.

Create a one-way forest trust relationship in which the extranet forest trusts the company forest.

C. Create a new forest and domain named extranet.woodgrovebank.com.

Create user accounts for users from partner companies in the new domain.

Create an external trust relationship in which the extranet domain trusts the den.corp.woodgrovebank.com domain.

D. Create a child domain of the den.corp.woodgrovebank.com domain for the extranet.

Create user accounts for users from partner companies in the new child domain.

Create an external trust relationship in which the forest root domain trusts the extranet 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.

Woodgrove Bank operates a 24-hour call center to support customers and partners.

Woodgrove Bank partners with an external auditing company to provide audit services for customers.

The user from the audit company have access to the extranet in the Denver office. These users need to

be able to access file resources that are located on a server on the Denver internal network named Server1.

Users from Partner companies require access to information stored on a Microsoft SQL Server 2000

computer that is located on the Denver 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.woodgrovebank.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.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows ® Server 2003 Environment

Management and Maintenance Study Guide, p. 20

QUESTION NO: 3

You need to design a remote access authentication strategy that will allow users in the IT department to remotely connect to the network. Your solution must meet security requirements. What should you do?

- A. Install Internet Authentication Services (IAS) on a server in the den.corp.woodgrovebank.com domain.
Configure the VPN servers as RADIUS clients.
- B. Install Internet Authentication Services (IAS) on a stand-alone server in the Denver extranet.
Create local user accounts for the IT personnel on the IAS server.
Configure the VPN servers as RADIUS clients.
- C. Create a remote access policy on each of the VPN servers.
Configure the policy to use the den.corp.woodgrovebank.com to authenticate remote access users.
Configure the policy to require L2TP to establish a connection.
- D. Create a remote access policy on each of the VPN servers.
Create local user accounts for the IT personnel on the VPN servers.
Configure the policy to use the VPN servers' local accounts database to authenticate users.
Configure the policy to require L2TP to establish a connection.

Answer: A

Explanation: IAS in Windows Server 2003 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 wireless access points support the IEEE 802.11q specification and Wired Equivalent Privacy (WEP) encryption. The wireless access points support using certificates and RADIUS for authentication.

Currently, no encryption or authentication methods are configured on the wireless access points.

The IT department is responsible for all administrative tasks for the network. There are no IT personnel at the branch offices.

IT personnel must be able to perform administrative tasks even when they are not at their desks. All IT personnel have new portable computers that have wireless network adapters.

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 den.corp.woodgrovebank.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 NO: 4

You need to design an access control solution for customer information. Your solution must meet security requirements.

What should you do?

A. Configure the Web site to require SSL connections.

Configure the Web site to require client certificates.
Enable and configure client certificate mapping on the Web site.
B. Configure the Web site to require SSL connections.
Disable anonymous access to the Web site.
Assign the **Allow – Read** permission to the customer user accounts for the folder that contains the Web site files.
C. Configure the Web site to use only Microsoft .NET Passport authentication.
Specify the den.corp.woodgrovebank.com domain as the default domain for .NET Passport authentication.
Configure a custom local IPSec policy on the Web servers to require IPSec communications.
D. Configure the Web site to use only Windows Integrated authentication.
Configure a custom local IPSec policy on the Web servers to require IPSec communications.
Configure the IPSec policy to use certificate-based authentication and encryption.

Answer: A

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.

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 Woodgrove Bank certification authority (CA).

Bank customers must be able to securely access their personal account information.

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:

B: Disabling anonymous access to the Web site and assigning the Allow – Read permission to the customer user accounts for the folder that contains the Web site files, will not comply with security requirements.

C: Making use of only Microsoft .NET Passport authentication will not work in this scenario.

D: Neither will making use of only Windows Integrated authentication on the Web site.

:

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 NO: 5

You need to design a security strategy that will ensure that unauthorized users cannot access personnel data. Your solution must comply with security requirements and the company's new administrative model.

What should you do?

A. In the Default Domain Policy Group Policy object (GPO) for the corp.woodgrovebank.com domain, add the LA\HRUsers group to the Restricted Groups list.

Add only the HR department user accounts to the Allowed Members list.

B. In the Default Domain Policy Group Policy object (GPO) for the la.corp.woodgrovebank.com domain, add the LA\HRUsers group to the Restricted Groups list.

Add only the HR department user accounts to the Allowed Members list.

C. In the Default Domain Policy Group Policy object (GPO) for the corp.woodgrovebank.com domain, add the LA\HRUsers group and the CORP\Backup Operators group to the Restricted Groups list.

Add only the HR department user accounts and the administrator user accounts to the Allowed Members list for each group.

D. In the Default Domain Policy Group Policy object (GPO) for the la.corp.woodgrovebank.com domain, add the LA\HRUsers group and the CORP\Backup Operators group to the Restricted Groups list.

Add only the HR department user accounts to the Allowed Members list for the LA\HRUsers group.

Add only the administrator user accounts to the Allowed Members list for the CORP\Backup Operators

group.

Answer: B

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 LA\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 la.corp.woodgrovebank.com domain. Especially when you take the following into consideration:

All members of the HR department are members of a group named LA\HRUsers.

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.

All personnel data is stored on a server named HRSrv1. 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 would work, but it would be applied to the wrong domain.

C: Only the LA\HRUsers group should be added to the Restricted Groups list and not the CORP\Backup Operators group as well. Further, only the HR department user accounts should be added to the Allowed Members list in the la.corp.woodgrovebank.com domain and not the administrator user accounts.

D: This option suggests the correct domain, but the CORP\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 NO: 6

You need to design a PKI solution that meets business and security requirements. What should you do?

A. Implement an enterprise root CA in the corp.woodgrovebank.com domain.

Implement subordinate CAs in each child domain.

Take the root CA offline.

B. Implement an enterprise root CA in the corp.woodgrovebank.com domain.

C. Implement an enterprise root CA in each of the child domains.

Take the enterprise CA in each domain offline.

D. Implement an enterprise root CA in the corp.woodgrovebank.com domain.

Implement a stand-alone root CA in each of the child domains.

Answer: A

Explanation: Following is the relevant information regarding the PKI solution required by Woodgrove Bank:

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, and recovery would be very expensive in terms of time and money.

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

Woodgrove Bank certification authority (CA).

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 CA. The enterprise can have a root CA as enterprise or a stand-alone CA. 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 CA. The root CA is the most important CA. 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 CA. 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.

In the current situation you thus need to implement an enterprise root CA in the corp.woodgrovebank.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 NO: 7

You need to design an authentication solution for wireless network access. Your solution must meet business and technical requirements. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Deploy an offline enterprise root CA in the corp.woodgrovebank.com domain.

Deploy subordinate enterprise root CAs in each child domain.

Install Internet Authentication Service (IAS) on one member server in the la.corp.woodgrovebank.com

domain and one member server in the den.corp.woodgrovebank.com domain.

B. Deploy an enterprise root CA in each domain.

Install Internet Authentication Service (IAS) on a member server in the corp.woodgrovebank.com

domain.

Install the Routing and Remote Access service on a member server in each child domain, and configure

these servers as RADIUS clients.

C. Enroll and deploy user certificates to all administrators in each domain.

Enroll and deploy computer certificates to all portable computers that have wireless network adapters.

Configure each portable computer to use Protected EAP (PEAP) for authentication.

D. Enroll and deploy computer certificates to all portable computers that have wireless network adapters.

Configure each portable computer to use EAP-MS-CHAP v2 for authentication.

Configure each portable computer to connect to the Internet Authentication Service (IAS) server.

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 CA. The enterprise can have a root CA as enterprise or a stand-alone CA. 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 CA. The root CA is the most important CA. 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 CA. 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.

The network consists of four Active Directory domains in a single forest. All servers run Windows Server 2003. All client computers run Windows XP Professional.

Wireless access points are installed in the Los Angeles and Denver offices. The wireless access points support the IEEE 802.11g specification and Wired Equivalent Privacy (WEP) encryption. The wireless access points support using certificates and RADIUS for authentication.

Currently, no encryption or authentication methods are configured on the wireless access points.

The Los Angeles and Denver offices are connected by a dedicated WAN connection. Each branch office connects to its regional office by means of a frame-relay line.

The Los Angeles and Denver offices each have a dedicated connection to the Internet. The branch

offices are not connected to the Internet.

IT personnel must be able to perform administrative tasks even when they are not at their desks. All IT

personnel have new portable 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 la.corp.woodgrovebank.com domain and one member server in the den.corp.woodgrovebank.com domain.

D: This option will not comply with business 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, Chapters 3 & 5, pp. 159, 181, 316

QUESTION NO: 8

You need to design a method to automate the deployment of critical updates and security patches that are supplied by Microsoft as these updates and security patches are released. Your solution must meet technical requirements.

What should you do?

A. Deploy a Windows Server 2003 computer running SUS in the test network.

Deploy SUS servers in each child domain to download administrator-approved updates from the test network SUS server.

B. Deploy a Windows Server 2003 computer running SUS in the test network.

Use autoupdate policies in each child domain to download and deploy updates from the test network SUS server.

C. Install MBSA on a Windows Server 2003 computer in the network 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 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

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.

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.

The Los Angeles 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 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: Installing IIS is not the option to be taken in this scenario.

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

Case Study #6, Testkingonline.com

Overview

Testkingonline.com is a global import business.

Physical Locations

The company's main office in Seattle. The company has three branch offices. The company's departments are located as shown in the following table.

Office location Departments

Seattle Finance, corporate services, information technology

(IT), sales, marketing, order fulfillment

Vancouver Sales, order fulfillment

New York Sales, order fulfillment

Seoul Purchasing

The company also has three warehouses of inventory, one each in Seattle, Vancouver, and New York.

Planned Changes

A new inventory and shipping management solution will allow wireless handheld computers in each warehouse

to connect in real time to the inventory database.

A new Windows application named SalesForceMax will allow the remote sales force to access key information

about inventory in stock and customer account information. SalesForceMax will run on a terminal server named

TS-1. TS-1 will need to access the database servers. SalesForceMax is the only user application running on TS-

1.

A new Web site named new-ideas.Testkingonline.com will allow the public to submit ideas and sources for new

products.

A new Web-based application named CustomerMax will allow the public to submit ideas and sources for new

products.

A new Web-based application named CustomerMax will allow large customers to check the status of shipments

and to place new orders. CustomersMax will use ASP.NET.

An internal help desk will be established in the Vancouver office. The Vancouver help desk staff will be able to

reset passwords, disable and enable user accounts, and clear account lock-outs for users in the Vancouver

office. All user accounts for the Vancouver help desk staff will be members of the CanadaHelpDesk global

security group.

Business Process

All users in the finance department are members of the FinanceUsers global security group. The finance

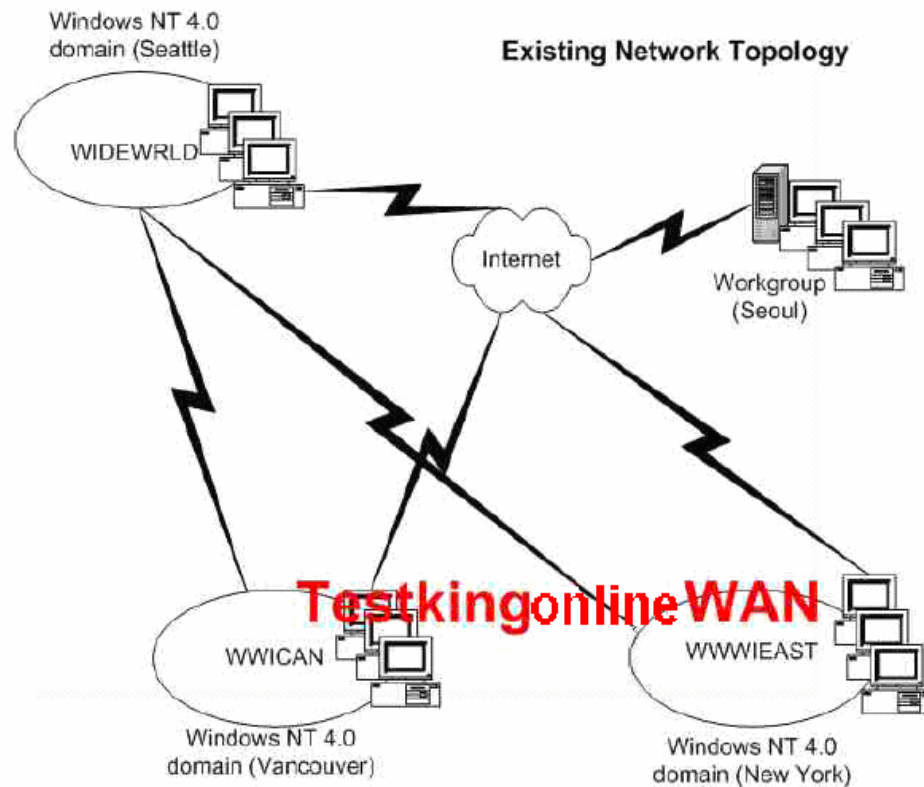
department uses a server named FinServ that is dedicated for use by the finance department.

The Seoul office supports a large staff in addition to contracted agents. Most users associated with the Seoul

office work away from the office, either from home or in remote locations.

Directory Services

The company's existing physical and network topology is shown in the **Existing Network Topology** exhibit.



The members of the WIDEWRLD Domain Admins group administer all three domains. Some users in the WWICAN and WWIEAST domains have administrative privileges in their respective domains so that they can respond quickly to emergencies.

Network Infrastructure

All servers that provide information or resources to the entire company are located in the Seattle office. These 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.

The Vancouver and New York offices contain local file and print servers that run Windows Server 2003,

Windows 2000 Server, or Windows NT Server 4.0. The Vancouver and New York offices also each have one

Windows 2000 Server mail server that runs Microsoft Exchange Server 5.5.

Domain controllers currently run Windows NT Server 4.0.

The Seoul office network is connected to the Seattle network by an L2TP/IPSec VPN tunnel between two

Windows Server 2003 Routing and Remote Access servers named SeattleRRAS and SeoulRRAS. The IP

department maintains both SeattleRRAS and SeoulRRAS from the Seattle network.

Mobile Users

The Seattle-based sales department relies on an ISP that has global dial-up numbers when high-speed

connections are not available. After connecting to the Internet, they connect to SeattleRRAS by using a VPN.

The portable computers used by the Seattle-based sales users are members of the WIDEWRLD domain.

Purchasing staff in the Seoul office travel extensively to remote areas.

Support from the IP department is not easily accessible to users when they are not in the office.

Chief Executive Officer

While users in our sales department need remote access to some information to be efficient and responsive, we must protect our data.

We will upgrade all client computers that run operating systems older than Windows 2000 Professional to Windows XP Professional.

We also need to bring the Seoul office into our domain structure. While it is important that we have secure remote access to all servers, it is particularly important that we have remote access to the server in the Seoul office so that we can control travel costs.

I want to give local staff some administrative privileges without making them full domain administrators so that my staff can decrease its travel to other offices and lower our costs.

When we look at proposed solutions, it is important to consider how much work is needed to implement them.

Whenever possible, we want to use the minimum amount of administrative effort to achieve our goals.

After a security configuration is deployed, nonadministrative users must not be able to change security settings.

All employees must be able to receive encrypted e-mail messages from other employees and external contacts.

All employees must be able to digitally sign outgoing e-mail messages so that external contacts can verify that the message is legitimate.

Remote connections to private resources in the company network must use an encrypted VPN.

The company network will establish VPN connections only with previously approved computers.

Portable computer users must encrypt confidential files stored on their portable computers.

Desktop computer users are allowed to encrypt confidential files on their desktop computers.

The IT department must be able to recover encrypted files that are stored on any client computer.

To support the written policies and to promote a reliable environment, the Senior Network Administrator has specified the following requirements. Exceptions may be allowed in rare circumstances. These requirements include:

A automated monthly process will be use to discover any computers that are not running current operating system security patches and critical updates.

Security patches and critical updates will be tested by the IT department and then automatically and remotely deployed to all client computers.

Users must be able to sign on with just one set of credentials.

It must be possible to track which resources are accessed by which users.

Passwords used to establish VPNs will be changed at least every three months.

Call center computers will run only an e-mail application, a dedicated order processing application, and

Internet Explorer. When using a call center computer, users are permitted to connect to only Web

servers operated by Testkingonline.com.

Customer data must be protected as it is transmitted between the customer's Web browser and newideas.

Testkingonline.com Web site.

Only authorized users are permitted to access the CustomerMax application or to see the data it contains.

All CustomerMax information, including user credentials and data must be encrypted as it is transmitted over the Internet.

Only employees in the finance department can access the data on FinServ. Any unauthorized attempts to access this data must be tracked.

The following Active Directory requirements must be considered.

The Windows NT 4.0 domains in the Seattle, Vancouver, and New York offices and the workgroup in

the Seoul office must be combined into a single Active Directory domain named ad.Testkingonline.com.

All domain controllers must run Windows Server 2003. The domain functional level and the forest functional level must both be Windows Server 2003.

The domain must contain a top-level organizational unit (OU) for each office. Each top-level OU will

contain additional OUs as required. The Seattle office OU will also contain an OU for mobile users who

do not have assigned office locations.

The main office call center's 120 client computer accounts must be in one OU named Call Center. The Call Center OU will be a child OU of the Seattle top-level OU.

A new stand-alone root certification authority (CA) that is offline from the network must be deployed.

A domain controller named CA1 will be located in the Seattle office. CA1 will be an enterprise CA that is chained to the offline, stand-alone root CA. CA1 will issue certificates to users and computers.

The IT department in the Seattle office must be able to manage the VPN tunnel between the Seattle office and the Seoul office. The VPN credentials must be changed regularly, without involving users in the Seoul office.

Each DHCP server in the Seattle office must be able to adequately support the network in Seattle independently, if the other server fails.

DHCP servers must not process any unauthorized packets.

If a network packet originates outside the company network, it will be accepted or processed by the Web servers only if it is an HTTP or HTTPS packet.

Case Study #6, Testkingonline.com (11 Questions)

QUESTION NO: 1

You need to design a strategy to meet the company's requirements for e-mail. What should you do?

- A. Configure and publish a certificate template that is suitable for S/MIME. Deploy a Group Policy object (GPO) so that a certificate that is based on this template is automatically issued to all domain users.
- B. Specify Group Policy objects (GPOs) and IPsec policies that require all client computers to use Kerberos authentication to connect to mail servers.
- C. For each mail server, acquire an SSL server certificate from a commercial CA whose root certificate is already trusted.
- D. Require IPsec encryption on all TCP connections that are used to send or receive e-mail messages.

Answer: A

Explanation: All employees must be able to receive **encrypted e-mail messages** from other employees and external contacts.

All employees must be able to **digitally sign outgoing e-mail messages** so that the external contacts can verify that the message is legitimate.

A new stand-alone root certification authority (CA) that is offline from the network **must be deployed.**

A domain controller named CA1 will be located in the Seattle office. CA1 will be an enterprise CA that is chained to the offline, stand-alone root CA. **CA1 will 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 NO: 2

You need to design a security strategy for the DHCP servers in the Seattle office. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Disable all unnecessary services on each DHCP server.
- B. Modify the discretionary access control lists (DACLS) in Active Directory so that only members of the Enterprise Admins security group can authorize additional DHCP servers.
- C. Use an IPSec policy that allows only the packets necessary for DHCP and domain membership for each DHCP server.
- D. Install a digital certificate for SSL on each DHCP server.

Answer: A, C

Explanation: DHCP is the method used in Windows Server 2003 to dynamically assign IP addresses for

legitimate domain member computers. Malicious users conceivably could attempt to lease all the IP addresses from a DHCP server, which would result in the inability of legitimate computers to obtain an IP address.

Without an IP address, those computers would be unable to join to the domain. In smaller companies, this is not usually a major threat, but in larger companies, this threat must be addressed.

Thus disabling the unnecessary services on the DHCP servers in conjunction with using IPSec policy that

allows on necessary packets for DHCP and domain membership should suffice.

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 NO: 3

You need to design desktop and security settings for the client computers in the Seattle call center. Your solution must be implemented by using the minimum amount of administrative effort. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. On each client computer in the call center, configure a local policy that lists only authorized programs in the Allowed Windows Programs list.
- B. Using NTFS permissions, assign the **Deny – Read** permission for all unauthorized executable files to the client computer domain accounts.
- C. Design a Group Policy object (GPO) that enforces a software restriction policy on all client computers in the call center.
- D. Design a Group Policy object (GPO) 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: C, D

Explanation: Call center computers **will run only** an e-mail application, a dedicated order processing application, and Internet Explorer. When using a call center computer, users are permitted to connect to **only web servers operated by Testkingonline.com.**

Incorrect answers:

A: Listing only the authorized programs in the Allowed Windows Programs List is not the option to take in this scenario.

B: Making use of NTFS permissions to assign the Deny – Read permission to all unauthorized executable files will not have the desired effect.

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 NO: 4

You need to design a method to allow the new-ideas-Testkingonline.com Web site to function in accordance with security and business requirements. What should you do?

- A. Require a PPTP VPN for all connections to the Web server.
- B. Require that traffic between Web browsers and the Web server uses an L2TP/IPSec tunnel.
- C. Require that traffic between Web browsers and the Web server uses SSL.
- D. Require certificate mappings between the Web server and Active Directory.

Answer: C

Explanation: SSL provides three major functions in encrypting Web-based traffic:

1. Server authentication allows a user to confirm that an Internet server is really the machine that it is claiming to be. This is another example of mutual authentication, similar to that provided by the Kerberos protocol. For example, server authentication assures the users that they're looking at a legitimate site and not a duplicate created by a hacker to capture their credit card and other personal information.
2. Client authentication to allow a server to confirm a client's identity. This would be important for a bank that needed to transmit sensitive financial information to a server belonging to a subsidiary office, for example.
3. Encrypted connections allow all data that is sent between a client and server to be encrypted and decrypted, allowing for a great deal of confidentiality. This function also allows both parties to confirm that the data was not altered during transmission.

Web page encryption is implemented using the Secure Sockets Layer (SSL) protocol. This protocol uses TCP port 443. The company's strategy has to cover both the external and the Internal Web sites.

- A new Web site named new-ideas.Testkingonline.com will allow the public to submit ideas and sources for new products.

- Customer data must be protected as it is transmitted between the customer's Web browser and new.ideas.Testkingonline.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 NO: 5

You need to design the configuration on one Windows Server 2003 terminal server that hosts the SalesforceMax application to meet security requirements.

Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

- A. Configure the terminal server so that users log on by using local user accounts.
- B. Configure the terminal server so that users log on by using domain accounts.
- C. Configure the server to run SalesforceMax in a dedicated window when a user logs on to the terminal server.
- D. Configure the server to allow each user to have a Windows desktop when the user logs on to the terminal server.
- E. Use software restriction policies in Group Policy objects (GPOs) that apply to the terminal server.
- F. Use Appsec.exe to restrict applications on the terminal server.

Answer: B, C, E

Explanation:

A new Windows application named SalesforceMax will allow the remote sales force to access key information about inventory in stock and customer account information. SalesforceMax will run on a terminal server named

TS-1. TS-1 will need to access the database servers. SalesforceMax is the only user application running on TS-1.

Users must be able to sign on with just one set of credentials.

All domain controllers must run Windows Server 2003. The domain functional level and the forest functional level must be 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 NO: 6

You need to design the configuration of the Windows Server 2003 Routing and Remote Access server in the Seattle office to meet business requirements.

What should you do?

- A. Configure a remote access policy on the Routing and Remote Access server to require MS-CHAP v2 for all connections.
- B. Use a Group Policy object (GPO) to configure a Restricted Groups policy that applies to the Routing and Remote Access server. Use this Restricted Groups policy to remove all accounts from the local Users group, and then add authorized computer accounts.
- C. Configure the Routing and Remote Access server to use only PPTP connections.
- D. Configure the Routing and Remote Access server to use only IPsec over L2TP connections. Configure IPsec to use certificates.

Answer: D

Explanation: Remote connections to private resources in the company network must use an encrypted VPN.

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.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows® Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 335

QUESTION NO: 7

You need to design Group Policy object (GPO) settings to support the use of the Encrypting File System (EFS). Your solution must meet business and security

requirements. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Designate a data recovery agent and issue an EFS certificate to the data recovery agent.
Export the private key and restrict access to the exported key.
- B. Make the data recovery agent a local administrator on all client computers.
- C. Remove the default data recovery agent from the Default Domain Policy GPO. Then, include the new data recovery agent instead.
- D. Delete the Default Domain Policy GPO. Configure a new GPO linked to the domain that does not specify a data recovery agent.

Answer: A, C

Explanation: The steps you should take to manage EFS throughout the organization are:

Export private keys for recovery accounts on secure media, stored in a safe place. Then, remove the

private keys from the computers - This prevents a user from using the recovery account to decrypt

others' files. This is particularly important for stand-alone computers where the recovery account is

typically the Administrator account. For a laptop, this makes sense because if the machine lost or stolen,

the data cannot be recovered without the recovery account keys. If the private keys have been removed

from the system, they will not be available as a potential security liability.

Only use the recovery agent account for file recovery. This keeps the credentials secure by limiting their use.

Work with users of stand-alone systems to make sure their systems remain safe. The requirements for

stand-alone systems are slightly different than for computers joined to the domain. Stand-alone systems

should create password reset disk and configure Syskey for startup key protection for the EFS users'

private keys.

Change the default recovery agent account as soon as possible. By default, the Administrator of the first

DC installed for the domain is the default recovery agent account. Set a password for each recovery

agent account. Set auditing for the use of the recovery agent account to monitor use of this account.

Export each private key associated with recovery certificates into a .PFX file, protect it with a strong

password, move it to secure removable media, and store it securely.

Do not destroy recovery certificates and private keys when recovery agent policy changes (or expires).

Keep them archived until you are absolutely certain all files protected with them have been updated with new recovery agent credentials.

Create a recovery agent archive program to ensure files can be recovered via obsolete recovery keys.

Export keys and store them in an access-controlled vault. Create a master and backup archive and store the backup archive securely offsite.

Designate two or more recovery agent accounts per OU. Designate one computer for each designated recovery agent account and grant appropriate permissions to the administrators to use the recovery agent accounts.

Never move or rename the RSA folder. The RSA folder is the only place EFS looks for private keys.

All employees must be able to receive encrypted e-mail messages from other employees and external contacts.

Data recovery is important when employees leave the company or lose their private keys. If you ever lose

your file encryption certificate and your private key through disk failure or some other reason, the

designated recovery agent can recover the data. This is why it's critical to export, save, and archive recovery

agent credentials. This also provides the ability for a company to recover an employee's data after he or she has left the company.

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

QUESTION NO: 8

You need to design the network to support the company's VPN requirements for mobile users who

connect to the network in Seattle.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Use a password generator application to create a preshared key, and distribute it to all mobile users.

B. Use computer autoenrollment to create digital certificates that can be used to authenticate to a VPN

server.

C. Acquire a digital certificate that can be used for SSL from a commercial CA for each computer that

established a VPN connection.

D. Configure IPSec policies on all Routing and Remote Access servers to require the use of digital certificates.

Answer: B, D

Explanation: 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.

RRAS must employ strong user authentication to ensure that only authenticated users gain access to network

resources. In addition, the data that flows back and forth from a remote user to the corporate network must be

secured, because in most cases, that data is traveling over a public network. This makes the data far more

susceptible to capture, monitoring, modification, and attack. IPSec is an excellent part of the security solution

for remote access. IPSec is used to secure the communication channel between computers and to secure the data

flowing across that channel. IPSec can secure any path between a pair of computers, whether it's client to client,

server to server, client to server, or between a security gateway and any host.

A domain controller named CA1 will be located in the Seattle office. CA1 will be an enterprise CA that

is chained to the offline, stand-alone root CA. **CA1 will issue certificates to users and computers.**

Remote connections to private resources in the company network must use an encrypted VPN.

Incorrect answers:

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

C: This option is not the solution.

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 NO: 9

You are designing the wireless networks for the three warehouses. Your design must support the inventory and shipping management solution, and it must meet security requirements.

What should you do?

- A. Ensure that all wireless networking equipment fully supports the IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g wireless networking protocols.
- B. Assign a random service set identifier (SSID) to each wireless access point. Disable broadcasting of SSIDs on all wireless access points.
- C. Create a firewall to block traffic to any IP address that did not originate from the company's DHCP servers. Ensure that all wireless access points connect behind this new firewall.
- D. Configure a server to use Internet Authentication Service (IAS). Configure the wireless networking equipment to use the IEEE 802.1x protocol and the IAS server.

Answer: D

Explanation: IAS provides a secure border control for wired/wireless network connections. The 802.1X standard improves security because both the wireless client and the network authenticate to each other. A unique per-user/per-session key is used to encrypt data over the wireless connection and keys are dynamically generated, reducing administrative overhead and eliminating the ability to crack a key because the key is generally not used long enough for a hacker to capture enough data to then determine the key and crack it.

A new inventory and shipping management solution will allow wireless handheld computers in each warehouse to connect in real time to the inventory database. Configuring a server to make use of IAS and configuring the wireless networking equipment to use IEEE 802.1x is the solution.

Incorrect answers:

A: Ensuring that the wireless network supports the mentioned wireless networking protocols alone is not enough.

B: Assigning service set identifiers to each wireless access point and then disabling the broadcasting thereof on all wireless access points is not the solution.

C: This is not appropriate in these circumstances.

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

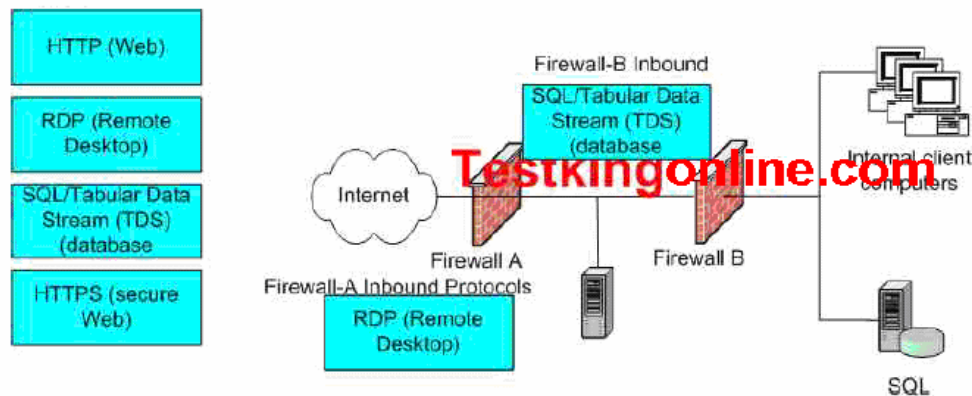
QUESTION NO: 10

You are designing firewall rules to support the company's new SalesforceMax application. You need to specify the types of incoming connections that will be allowed by Firewall-A and Firewall-B (Note that existing rules are already in place, you need to specify only the new rules required to support the SalesforceMax application.) What should you do?

A portion of the new main office network is shown in the work area. To answer, drag the appropriate connection type or types to the correct location or locations in the work area.



Answer:



Explanation:

A new Windows application named SalesforceMax will allow the remote sales force to access key information about inventory in stock and customer account information. **SalesforceMax will run on a terminal server** named TS-1. TS-1 will need to access the database servers. SalesforceMax is the only user application running on TS-1.

Remote Desktop protocol (RDP) **A protocol used by terminal services.**

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 5, pp. 292-293,

QUESTION NO: 11

You are designing the settings for FinServ. You specify the permissions that will be used. You need to specify any additional settings required by the company. What should you do?

- A. Install a digital certificate for Encrypting File System (EFS) on FinServ.
- B. Activate failure auditing on the access to files and objects.
- C. Configure all firewalls to track when any packets addresses to FinServ are dropped.
- D. Create an IPSec policy that requires IPSec encryption between FinServ and the firewall.

Answer: B

Explanation: Audit object access - if enabled, this setting triggers auditing of user access to objects such as files, folders, Registry keys, and so forth.

All users in the finance department are members of the FinanceUsers global security group. The finance department uses a server named FinServ that is dedicated for use by the finance department.

Only employees in the finance department can access the data on FinServ. Any unauthorized attempts to access this data must tracked.

You should activate failure auditing for access to files and objects.

Incorrect answers:

A: Installing a digital certificate for EFS on FinServ is not going to track unauthorized access attempts.

C: Configuring all firewall to track any dropped packets destined for FinServ will not work as firewalls designed to prevent intrusion.

D: The difference between ICF and IPSec in terms of securing the perimeter. Use ICF when you want to implement a firewall for a network interface that can be accessed via the Internet. Use IPSec when you want to secure traffic on the network or when you need to allow access only to a group of trusted computers. Applying IPSec encryption between FinServ and the firewall is not the solution. It is not going to track unauthorized access attempts. You need to audit that.

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

Case Study #7, Litware Inc.

Overview

Litware, Inc., is a manufacturer and wholesale distributor of hiking and climbing outdoor gear. The company recently merged with Contoso, Ltd.

Contoso, Ltd., provides fabrics to Litware, Inc.

Physical Locations

The Litware, Inc., main office is in Denver. The company has branch offices in Dallas, Boston, and San Francisco.

The information technology (IT) department is located in the Denver office. The company's manufacturing plant is located in Dallas. The company's east coast sales and distribution center is located in Boston, and the west coast sales and distribution center is located in San Francisco.

The Contoso, Ltd., main office is in Auckland.

The company will open a new branch office in Singapore. This new office will be added to the contoso.com

domain. Client computers in the Singapore office will run Windows XP Professional. An OU named Singapore

Sales and Distribution will be added from the contoso.com domain for the new branch office.

Computers and users in the Windows NT 4.0 domain will be migrated to an OU in the litwareinc.com domain.

The firewall will be configured to allow PPTP and L2TP VPN traffic.

Remote Desktop connections will be used for administration of servers and desktop client computers.

Routing and Remote Access servers in the branch offices will be taken offline.

Administration of the remote

access server in the Denver office will be managed by only administrators who specialize in remote access.

Business Processes

The IT staff in the Denver office manages the computers in the branch offices remotely.

Each branch office has

a desktop support technician.

All Litware, Inc., company data, including marketing, manufacturing, sales, financial, customer, legal, and

development data must not be available to the public. This data is considered to be confidential.

The company's public Web site is hosted in the Denver office. The public Web site contains press releases and product information.

Each office has mobile sales users. These mobile users connect to a remote access server at the nearest branch office by using a dial-up connection.

Directory Services

The Litware, Inc., network consists of two domains. One domain is a Windows 2000 Active Directory domain.

The second domain is a Windows NT 4.0 domain. A two-way external trust relationship exists between the Active Directory domain and the Windows NT 4.0 domain.

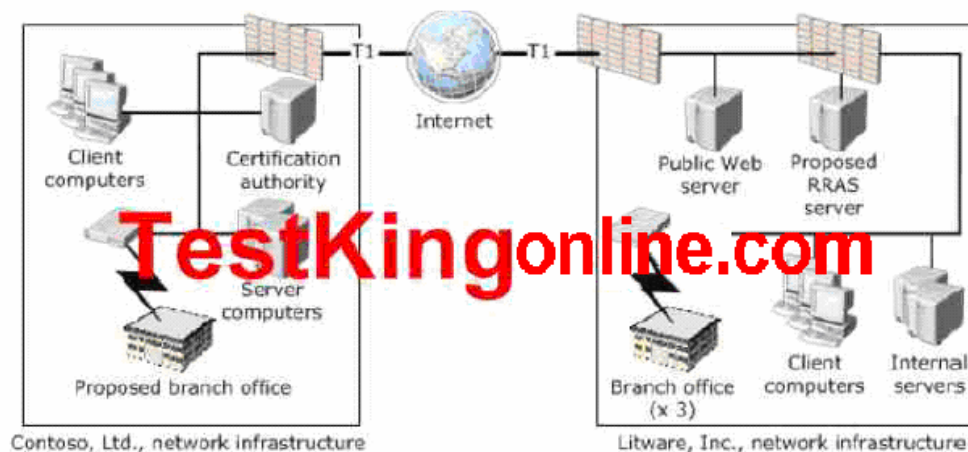
The organizational unit (OU) structure for the Active Directory domain is shown in the **OU Structure** exhibit.



The Contoso, Ltd., network consists of a single Active Directory domain named contoso.com. All domain controllers run Windows Server 2003.

Network Infrastructure

The network infrastructure after the merger is shown in the **Network Infrastructure** exhibit.



The operating system installed on the client computers in each office is shown in the following table.

Office Client operating system

Denver Windows XP Professional

Boston Windows XP Professional

San Francisco Windows 2000 Professional

Dallas Windows XP Professional and

Windows NT Workstation 4.0

Auckland Windows 2000 Professional and

Windows XP Professional

All managers and mobile sales users have client computers that run Windows XP Professional. All client computers run the latest service packs.

Problem Statements

The following business problems must be considered:

- IT administration is too complex and expensive.

- Remote access connections to the network are expensive.

- Remote access policies are not centralized.

- Employees are required to remember multiple passwords.

It takes the Denver IT staff several days to fix account problems or problems with access to network resources.

Chief Executive Officer

Because we acquired Contoso, Ltd., we now hold the patent rights to a new fabric. We need to absolutely certain that our competitors do not obtain our development data or our research data. This information is secret, and it is critical to the success of our business.

Chief Information Officer

As the company grows, we need to find more cost effective methods to manage the network and to keep it more secure.

We need to enable a stronger authentication strategy for the network. We need to integrate Contoso, Ltd., into this strategy.

Denver IT Administrator

Currently, we allow only managers to use Encrypting File System (EFS) on local computers. Sometimes we have problems with lost user profiles. We need to be able to restore access to encrypted files as quickly as possible.

I think we need a two-factor authentication method for the mobile sales users.

We need to limit unnecessary traffic across the WAN links.

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

Network Manager (Litware, Inc.)

We simply do not have the IT staff to support all the branch offices and the newly acquired contoso.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 Contoso, Ltd., has its own IT staff, we

are responsible for administration of the contoso.com domain.

We want to require all remote users to log on by means of a secure VPN connection. The solution must be easy to implement and also must reduce complexity for end users.

Also, we need to maintain both domains' servers and client computers with the latest updates and security

patches. Denver IT staff must be able to control which updates and security patches are deployed to the other offices.

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.

Business Drivers

The following business drivers must be considered:

The network environment must be more secure and it must be standardized. The network management must be minimized.

Universal principal names (UPN) single sign-on must be provided to all users.

The relevant portion of the company's written security policy includes the following requirements:

Only managers and executives must be able to access the Customer Information folder.

Only managers and executives must be able to access research and product development information.

Only managers must be able to encrypt files stored on file servers or on their local computers.

Sales users must be able to encrypt the offline files cache.

Users must not be able to log on interactively to client computers by using accounts that have administrative privileges.

Two-factor authentication is required to perform administrative tasks.

All Terminal Services connections must require encryption.

Remote access users must use only L2TP VPN connections to connect to the internal network.

Case Study #7, Litware, Inc. Bank (4 Questions)

QUESTION NO: 1

You need to design a remote access solution for the mobile sales users in the litwareinc.com domain.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Configure autoenrollment for user certificates and computer certificates.
- B. Configure Web enrollment for user certificates and computer certificates.
- C. Configure a Certificate Services hierarchy in the litwareinc.com domain.
- D. Configure qualified subordination between the litwareinc.com and the contoso.com domains.
- E. Configure PEAP authentication on the remote access servers.

Answer: A, C

Explanation: 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.

Each office has mobile sales users. These mobile users connect to a remote access server at the nearest branch office by using a dial-up connection.

Remote access connections to the network are expensive.

Remote access policies are not centralized.

We need a **two-factor authentication** method for the mobile sales users.

We want to require all remote users to log on by means of a secure VPN connection.

The solution must

be easy to implement and also must reduce complexity for end users.

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.

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 NO: 2

You need to design an EFS strategy to address the Denver IT administrator's concerns. 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 Managers.
Assign the appropriate NTFS permissions to the Managers group for the managers' data in Denver.
Add the Managers security group to the Restricted Groups in the Default Domain Policy object (GPO=.
- D. Configure IPsec certificate autoenrollment on the Default Domain Policy Group Policy object (GPO):
Configure an IPsec policy on the Managers OU.
Configure the IPsec policy to use certificate authentication.

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:

Currently, we allow only managers to use Encrypting File System (EFS) on local computers. Sometimes we have problems with lost user profiles. We need to be able to restore access to encrypted files as quickly as possible.

I think we need a two-factor authentication method for the mobile sales users.

We need to limit unnecessary traffic across the WAN links.

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

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 NO: 3

You need to design an administrative control strategy for Denver administrators. What should you do?

- A. Create a security group named HelpDesk.
Add the HelpDesk group to the Enterprise Admins group in both domains.
- B. Create a security group named HelpDesk.
Add the HelpDesk group to the Domain Admins groups in both domains.
- C. Add the Domain Admins group in the litwareinc.com domain to the Domain Admins group in the contoso.com domain.
Delegate full control of the litwareinc.com domain to the Domain Admins group in the contoso.com domain.
- D. Create a security group named HelpDesk for each office.
Delegate administrative tasks to their respective OU or domain.
Delegate full control of the contoso.com domain to the Domain Admins group from the litwareinc.com domain.

Answer: D

Explanation: When designing a delegation strategy, you should be aware that there are two types of administrators, Service Administrators and Data Administrators. Service Administrators are responsible for the overall integrity and availability of Active Directory; they maintain network services and functions for the entire user base. Data administrators are responsible for specific objects stored within Active Directory such as user and group accounts and the like. You should create your Active Directory design so that these two tasks can be separated and managed by two different people or job functions. When designing a delegation strategy, it's also imperative that you analyze your business needs for autonomy versus isolation. For example, your Human Resources department might require full and unshared control over their portion of the Active Directory

and all of their network resources, with strict policies on security. In this case, the only way to give them this level of control is by creating a separate forest for them. Another department might be more willing to accept shared administration of their resources, in which case they would fall under the category of autonomy. At this point, you can create a separate domain or OU to subdivide their resources for them. Delegation of administration can be set the forest level, domain level, and OU level. The higher the level, the more isolated the administrative model. Conversely, the lower the level of delegation, the more it tends toward autonomous administration.

The Litware, Inc., main office is in Denver.

The information technology (IT) department is located in the Denver office.

Currently, we rely on the desktop support technicians at each branch office to perform minimal everyday administrative tasks, such as resetting passwords.

Even though contoso, Ltd., has its own IT staff, we are responsible for administration of the contoso.com domain.

As the situation is, the best administrative strategy would be to create a security group for each office and then delegate administrative tasks to their respective OU or domain. Then you should delegate full control of the contoso.com domain to the Domain Admins group of the litwareinc.com domain.

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 8, pp. 497-498

QUESTION NO: 4

You need to design a PKI for Litware, Inc.

What should you do?

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

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 CA. The enterprise can have a root CA as enterprise or a stand-alone CA. 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 CA. The root CA is the most important CA. 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 CA. 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 CA. 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.

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:

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

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

Case Study #8, Northwind Traders

Overview

Northwind Traders manufactures security systems. They distribute these products to retail stores, government agencies, and the public.

A vendor named Contoso, Ltd., provides components for Northwind Trader products.

Physical Locations

Northwind Trader’s main office is located in New York. The company has branch offices in Boston and Seattle.

Contoso, Ltd., is located in London.

Northwind Traders also outsources some contract work to a group of offsite consultants.

Planned Changes

Northwind Traders plans to make the following changes.

Internet Authentication Service (IAS) will be installed on a Windows Server 2003 domain controller in the Seattle office.

An organizational unit (OU) named Seattle will be created in the northwindtraders.com domain.

Three child OUs will be created in the Seattle OU: Research, Wireless Clients, and SeattleIT.

The company will expand product sales to the Internet.

Business Processes

All administrative information technology (IT) decisions are made in the New York office. There are smaller IT

staffs in each branch office that perform specific administrative tasks.

Customers place orders by means of a faxes, e-mail messages, and phone calls.

Customers' orders are placed

with sales users in New York or Boston.

The consultants and internal Web Developers update content on both the company's external and intranet Web

servers. The consultants' network does not have a public key infrastructure (PKI).

Active Directory

The Northwind Traders network consists of two Active Directory domains named northwindtraders.com and

boston.northwindtraders.com and boston.northwindtraders.com. The

northwindtraders.com domain is located in

the New York office, and the boston.northwindtraders.com domain is located in the Boston office. The

boston.northwindtraders.com domain is a child domain of northwindtraders.com. All domain controllers run

Windows Server 2003.

The OU structure for the network is shown in the **Northwind Traders OU Structure** exhibit.

Northwind Traders OU Structure



The two domains contain the groups shown in the following table.

Domain	Group scope	Group name
Northwindtraders.com	Local	Sales, Sales Managers, Research, Executives, Web Developers
Boston.northwindtraders.com	Local	Boston Sales, BostonIT Production
Boston.northwindtraders.com	Global	Boston Customer Relations

The following shared company folders are located on member servers in New York:

- Research

- Sales

- Documentation

- Customer Information

The Customer Information shared folder contains the following folders:

- Order History

- Payment

- Contact Info

Certificate and PKI Information

The Northwind Traders network contains an enterprise root certification authority (CA) that is configured to

issue certificates to users and computers on the Northwind Traders internal network. User and computer

certificate autoenrollment is configured in the northwindtraders.com domain. Computer certificates

autoenrollment is configured in the boston.northwindtraders.com domain. User

certificates are issued only to

company employees.

The Contoso, Ltd., network consists of a single Active Directory domain named

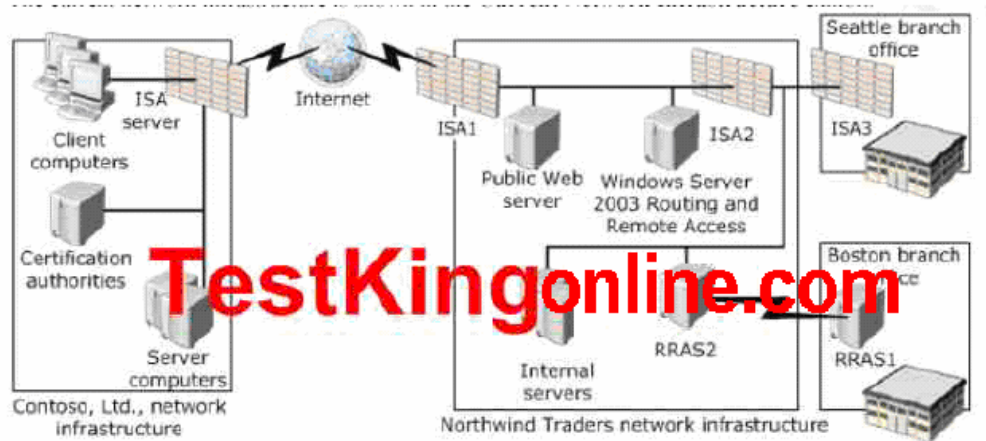
Contoso.com. Contoso, Ltd.,

has an Active Directory-integrated PKI. The network contains an enterprise root CA and an enterprise

subordinate CA that are configured to issue certificates to users on the Contoso, Ltd., internal network.

Network Infrastructure

The current network infrastructure is shown in the **Current Network Infrastructure** exhibit.



IP Address Information:

New York: 10.10.0.0/16

Boston: 10.20.0.0/16

Seattle: 10.30.0.0/16

A dial-up connection is configured on a server named RRAS1. The dial-up connection is configured with VPN

ports and Network Address Translation (NAT).

All client computers run Windows XP Professional with the latest service pack. Wireless client computers in Seattle have IEEE 802.11g wireless adapters. Client computers in the Corporate Portables OU have smart card readers.

All client computers in the Seattle office use only Microsoft Outlook Web Access (OWA) in the perimeter network for e-mail.

Problem Statements

The following business problems must be considered:

Client computers have been used by unauthorized personnel.

Web content that is used to update company Web sites is not transmitted securely.

The current dial-up method for remote client connections is not cost effective, and it transmits data unprotected.

The CA that issues certificates in the New York office is at the limit of its capability.

Chief Information Officer

We need a higher level of network security. Though we are willing to allocate funds to support security

improvements, I want to use the least expensive solution that will accomplish our goals. We allow our business partners and some government agencies access to some of our internal data. Therefore, it is important for use to protect our internal resources.

We also need to ensure that users of our external Web site do not have to make any configuration changes to their computers.

Chief Security Officer

We need to extend our internal PKI to include Contoso, Ltd., and our branch offices. We need a remote access solution that supports data encryption and that allows remote client computers access to research documentation on our products. Remote access client credentials should not rely on a single piece of information for authentication.

We accept remote access connections to the internal network only from computers that are configured to our specifications.

IT Department Manager

We need to deploy security patches efficiently. Currently, we update client computers and servers in the New York office by using Software Update Services (SUS). I want to enable all client computers in both domains to automatically update themselves. I also want to be able to ascertain which security patches from a SUS server have been applied to client computers.

All security patches must be tested and approved by the IT department in the New York office.

Currently, the consultants use FTP to send us content that we use to update the content on our Web sites. We need a method to encrypt data that consultants send.

We need to provide a single method of authentication for all Web site users. The current authentication method does not support a single logon. We do not want to create additional domains or to change the domain structure of our existing environment.

We need to expand our PKI to include CAs in each physical location. Each CA must issue certificates to only users and computers within the location. CAs in Boston must issue certificates to users and computers based on domain name.

Because there are many Routing and Remote Access servers, we need to centralize authentication for both remote access and wireless connections. We will eliminate all dial-up access to the network, because it is too costly.

End User (Finance Department)

We need to be able to encrypt e-mail messages that we send to Contoso, Ltd., and to our contacts and vendors.

The computers in our department have been used by unauthorized users.

The bandwidth that is used for administrative tasks must be minimized.

The IT staff in the New York office must be able to perform all administrative tasks in the

boston.northwindtraders.com domain.

The connection between the Boston and New York offices must be automated and persistent, and it must

encrypt data and credentials.

File servers must not run unnecessary services.

Mobile company users must use a certificate-based authentication method.

Government agencies and vendors must be able to access internal company Web sites and some internal

data.

Customers must be able to access the external Web site. Customers need a method to protect the

information that they use to place orders and view order status. This connection must be encrypted.

Security

The following security requirements must be considered:

To view data in the Research folder, government agencies and vendors must have 128-bit encrypted

connections to the internal Web server.

The Customer Information folder must be accessible to all members of the Sales group. Access to the

Customer Information\Order History and the Customer Information>Contact Info folders must be limited

to members of only the Sales, Sales Managers, and Boston Sales groups.

Access to the Customers Information\Payment folder must be limited to members of only the Sales

Managers group. The contents of the Customer Information\Payment folder must be encrypted.

All users in the finance department must encrypt documents both locally and in their network home

folders. They must be able to encrypt documents when they are working offline or on portable

computers.

The Microsoft Internet Security and Acceleration Server (ISA) computer firewall in Seattle must

minimize security risks to the branch office's internal network.

The relevant portion of the company's written security policy includes the following requirements:

All remote access clients must comply with company security policies.

All remote access connections must use L2TP and 3DES encryption.

All existing and future wireless connections must encrypt data and use password authentication.

Wireless clients must be authenticated before they are allowed access to the network.

Finance users are required to log on to the network by using two-factor authentication.

When customers access the external Web site, their user credentials and data must be encrypted.

Case Study #8, Northwind Traders (9 Questions)

QUESTION NO: 1

You need to design an access control strategy for the Payment folder for the Sales Managers group.

What should you do?

- A. Use IPsec in transport mode.
- B. Use Encrypting File System (EFS) over Web Distributed Authoring and Versioning (WebDAV).
- C. Use PEAP-EAP-TLS.
- D. Use Encrypting File System (EFS) remote encryption.

Answer: D

Explanation: For the Customer\Payment folder to remain accessible to only the Sales Managers group, you

need to make use of EFS remote encryption when you take into account the following:

Company shared folders are located on member servers in New York; they include the Research, Sales,

Documentation as well as Customer Information folders.

The Customer Information shared folder contains the following folders: Order History, Payment and

Contact Info Access to the Customer Information\Payment folder must be limited to members of only the Sales Managers group. The contents of the Customer Information\Payment folder must be encrypted.

Incorrect answers:

A: Voluntary tunneling is very similar to IPsec in Transport mode, however this is but half the solution since

there are many Routing and Remote Access servers, they need to centralize authentication for both remote access and wireless connections.

B: Because SUS locks down the IIS service, turns off Internet printing, WebDAV, and indexing, and disables

the session state, it is recommended that you dedicate an IIS server to the use of SUS and not use it for other

Web services. This makes the use of EFS over WebDAV the wrong choice.

C: PEAP-EAP-TLS will not work in these circumstances since written policy states that all remote access connections must use L2TP and 3DES encryption.

Reference:

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 NO: 2

You need to configure ISA3 in Seattle to enable communication with the network in New York.

What should you do?

- A. Open the ports for DNS, HTTP, HTTPS, Kerberos, RADIUS, LDAP, RPC endpoint mapper and client, and Server Message Block (SMB) over IP.
- B. Enable the Routing and Remote Access Basic Firewall. Open the ports for DNS, Kerberos, LDAP, Exchange RPCs, RADIUS, L2TP, and Internet Key Exchange (IKE).
- C. Create a PPTP tunnel from ISA3 to the New York network.
- D. Create an L2TP/IPSec tunnel from ISA3 to the New York network.

Answer: D

Explanation: Company written policy states amongst other things that remote access connections must make use of L2TP and 3DES encryption. L2TP is widely regarded as more secure than PPTP, even by Microsoft, and should be the protocol of choice if strong security is a primary concern of your network design.

Since there is infrastructure in place that involves certificates you can create a L2TP/IPSec tunnel.

Incorrect answers:

A: Opening ports for DNS, HTTP, HTTPS, Kerberos, RADIUS, LDAP, RPC endpoint mapper and client, and Server Message Block (SMB) over IP would be risky.

B: The case study states that they need to extend their internal PKI to include Contoso, Ltd., and their branch offices. But enabling the firewall and opening the ports for DNS, Kerberos, LDAP, Exchange RPCs, RADIUS, L2TP and Internet Key Exchange (IKE) would be opening up to wide. Having the ports open to this extent will probably allow too many connections to be successful and will be a security risk.

C: PPTP is not as secure as L2TP/IPSec.

Reference:

Roberta Bragg, MCSE Self-Paced Training Kit (Exam 70-298): Designing Security for a Microsoft Windows Server 2003 Network, Chapter 7, p. 425, 662-663

QUESTION NO: 3

You need to design a security strategy for communications between the Boston and New York offices. What should you do?

A. Configure RRAS2 as a VPN server.

Use Web enrollment to acquire computer certificates for both RRAS1 and RRAS2.

Create demand-dial L2TP/IPSec connections on both RRAS1 and RRAS2.

Configure dial-out credentials on both RRAS1 and RRAS2.

Enable the Basic Firewall settings on RRAS1 and RRAS2.

B. Configure RRAS2 as a VPN server.

Create demand-dial L2TP/IPSec connections on both RRAS1 and RRAS2.

Configure dial-out credentials on both RRAS1 and RRAS2.

Configure static routes on both RRAS1 and RRAS2.

Set the connection type to persistent on the demand-dial interface on both RRAS1 and RRAS2.

C. Create a new OU named RRAS Servers in the boston.northwindtraders.com domain.

Move RRAS1 into the RRAS Servers OU.

On the Default Domain Policy Group Policy object (GPO), edit the Secure Server (Require Security)

IPSec policy.

Configure the IPSec policy to use a certificate for authentication.

Specify RRAS2 as the tunnel endpoint.

Assign the IPSec policy.

D. Create a new OU named RRAS Server in the northwindtraders.com domain.

Move the RRAS2 into the RRAS Servers OU.

On the RRAS Servers OU create new Group Policy object (GPO) named IPSECPOL.

In IPSECPOL create an IPSec policy and specify RRAS as the tunnel.

Answer: B

Explanation: 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.

When an RRAS router initiates a demand dial connection to another RRAS router, it creates a virtual interface.

After the creation takes place, the sending router asks the receiving router to assign its new interface a public or

private IP address. The process is then reversed, and the receiving router creates its own virtual interface.

Subsequently, the receiving router then asks the sending router for an IP address for the new interface. Once both interfaces have been assigned IP addresses from the other router, the logical interface connection is complete and communication can begin.

All administrative information technology (IT) decisions are made in the New York office. There are smaller IT staffs in each branch office that perform specific administrative tasks.

Customers place orders by means of a faxes, e-mail messages, and phone calls. Customers' orders are placed with sales users in New York or Boston.

The CA that issues certificates in the New York office is at the limit of its capability.

The current dial-up method for remote client connections is not cost effective, and it transmits data unprotected.

The connection between the Boston and New York offices must be automated and persistent, and it must encrypt data and credentials.

Thus option B is the best design under the circumstances.

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. 420-423

QUESTION NO: 4

You need to design a strategy to increase security for the client computers in the finance department.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Enable automatic certificate enrollment.
- B. Enforce smart card logons.
- C. Enable Encrypting File System (EFS) for offline files.
- D. Enable a screen saver password.

Answer: B, C

Explanation: Two factor-authentications in this case would involve enforcing smart card logons as well as enabling Encrypting File System for offline files. In the case study it is mentioned that Finance users are required to log on to the network by using two-factor authentication.

Incorrect answers:

A: Automatic certificate enrollment does not constitute a two-factor authentication as is required for Finance Users.

D: A screensaver password does not make the files secure as the users would still be logged on and remote access to these files would not be hindered.

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 NO: 5

You need to design a security strategy for the Web folders and files created by the consultants and the internal Web developers.

What are two possible ways to achieve this goal? (Choose two. Each correct answer is a complete solution.)

A. Require the internal Web developers to use Telnet with Kerberos authentication.
Require the consultants to use L2TP with IPsec.

B. Require the internal Web developers to use Encrypting File System (EFS) over Web Distributed

Authoring and Versioning (WebDAV).

Require the consultants to use Microsoft .NET Passport authentication with Security Level 0.

C. Require the internal Web developers to use Web Distributed Authoring and Versioning (WebDAV) over
SSL.

Require the consultants to use WebDAV over SSL.

D. Require the internal Web developers to use L2TP with IPsec.

Require the consultants to use Encrypting File System (EFS) over Web Distributed Authoring and
Versioning (WebDAV).

E. Require the internal Web developers to use Web Distributed Authoring and Versioning (WebDAV) over
SSL.

Require the consultants to use L2TP with IPsec.

Answer: C, E

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.

E: 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.

Incorrect answers:

A: The consultants should be required to use L2TP with IPSec. The internal Web developers making use of Telnet with Kerberos authentication is however, not what is required or optimal in this case.

B: This option, though costly would work for the external website, but the passport service is just an authentication service. And this is not enough security even if used in conjunction with other methods. Also you have to keep in mind that although they are willing to spend money on security, it is a limited budget.

D: The usage of the different strategies should be vice versa.

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, Chapters 4, 6 & 10, pp. 208, 383-384, 386, 646-647

QUESTION NO: 6

You need to design a PKI for the Northwind Traders internal network. What should you do?

- A. Add an enterprise root CA to the northwindtraders.com domain. Configure cross-certification between the northwindtraders.com domain and the boston.northwindtraders.com domain.
- B. Add an enterprise subordinate issuing CA to the northwindtraders.com domain.

Configure qualified subordination for the enterprise subordinate issuing CA in Boston.
C. Add enterprise subordinate issuing CAs to the New York, Boston, and Seattle LANs. Configure qualified subordinations for each enterprise subordinate issuing CA.
D. Add a stand-alone commercial issuing CA to only the northwindtraders.com domain. Configure cross-certification between the commercial CA and the boston.northwindtraders.com domain.

Answer: C

Explanation: A PKI is usually made up of several Certificate Authorities, resources that generate and validate digital certificates. Certificate Services can be installed and run on a Windows Server 2003 computer to enable the server to function as one of several different types of CAs in the environment. Each PKI must have at least one root CA that controls the trust for the entire organization, but there can be any number of subordinate CAs distributed through the network. Certificate Services servers acting as CAs must run either in enterprise mode or stand-alone mode. Enterprise-mode CAs requires Active Directory and can automatically generate certificates based on security templates. Stand-alone CAs do not require Active Directory, must generate certificates manually, and do not use templates.

The Northwind Traders network contains an enterprise root certification authority (CA) that is configured to issue certificates to users and computers on the Northwind Traders internal. User and computer certificate autoenrollment is configured in the northwindtraders.com domain.

We need to **expand our PKI to include CAs in each physical location**. Each CA must issue certificates to only users and computers within the location. **CAs in Boston must issue certificates to users and computers based on domain name.**

Incorrect answers:

A: Adding an enterprise root CA to the domain and configuring cross-certification between the domain and

Boston.northwindtraders.com will not address the IT department Manager's concerns.

B: Enterprise subordinate issuing CAs has to be added to the different LANs respectively and not to the northwindtraders.com domain.

D: A standalone commercial issuing CA being deployed in only the northwindtraders.com domain, must generate certificates manually and does not make use of templates. This is not desired.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris & Rob Amini, MCSE Designing Security for a Windows Server

QUESTION NO: 7

You need to design a patch management strategy for Northwind Traders. What should you do?

- A. Configure the Default Domain Policy Group Policy object (GPO) for the northwindtraders.com domain to configure client computers to download updates from the SUS server in New York. Configure the Default Domain Policy GPO for the boston.northwindtraders.com domain to configure client computers to download updates from the SUS server in New York.
- B. Use Group Policy to configure client computers to download updates from a Windows Update server on the Internet. Configure the Default Domain Policy Group Policy object (GPO) with a startup script that runs Mbsaclic.exe. Configure it to scan the computers in both of the branch offices.
- C. Install and configure a SUS server in the Boston branch office. Configure the server to download updates from a Windows Update server on the Internet. Configure Microsoft Baseline Security Analyzer (MBSA) to scan for updates and computers in the New York office.
- D. Install and configure a SUS server in each branch office. Configure the SUS servers to download updates from the New York SUS server. Configure Microsoft Baseline Security Analyzer (MBSA) to scan for updates on computers in the New York office.

Answer: D

Explanation: As per the case study: "We need to deploy security patches efficiently. Currently, we update client computers and servers in the New York office by using Software Update Services (SUS). I want to enable all client computers in both domains to automatically update themselves. We also want to be able to ascertain which security patches from a SUS server has been applied to client computers." Installing SUS in each branch office and configuring it to download updates from the New York SUS server and configuring MBSA to scan for updates on computers in the New York office, would ensure that all client computers automatically update themselves while also offering the opportunity of scanning which security patches has been applied to client

computers.

Incorrect options:

A: You should make use of MBSA to scan the client computer updates and not the Default Domain Policy GPO.

B: Client computers downloading updates from a server on the Internet will defeat the purpose of the administrators who wants to be able to check which security patches from a SUS server has been applied to client computers.

C: You will need to configure a SUS server in each branch office and not only in the Boston branch. As option C is at the moment, it will only provide you with the Boston information. Thus whether you configure MBSA to scan for updates in the New York office, you will not be facilitating the other branches whose client computers should also be updated.

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 NO: 8

You need to design an access control strategy for the external and intranet Web sites.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Enable SSL on the external Web site by using a Microsoft cryptographic service provider (CSP).
- B. Enable Microsoft .NET Passport authentication on the external Web site. Use Passport Level 0 with SSL on the external Web site.
- C. Enable SSL on the external Web site by using a commercial digital certificate.
- D. Enable SSL on the intranet Web site by using an internal server certificate.
- E. Enable SSL on the external Web site by using an internal server certificate.

Answer: C, D

Explanation:

We also need to ensure that users of our external Web site do not have to make any configuration changes to their computers.

All client computers in the Seattle office use only Microsoft Outlook Web Access (OWA) in the perimeter network for e-mail.

The current dial-up method for remote client connections is not cost effective, and it transmits data unprotected.

SSL provides three major functions in encrypting Web-based traffic:

1. Server authentication allows a user to confirm that an Internet server is really the machine that it is claiming

to be. This is another example of mutual authentication, similar to that provided by the Kerberos protocol.

For example, server authentication assures the users that they're looking at a legitimate site and not a

duplicate created by a hacker to capture their credit card and other personal information.

2. Client authentication to allow a server to confirm a client's identity. This would be important for a bank that

needed to transmit sensitive financial information to a server belonging to a subsidiary office, for example.

3. Encrypted connections allow all data that is sent between a client and server to be encrypted and decrypted,

allowing for a great deal of confidentiality. This function also allows both parties to confirm that the data

was not altered during transmission.

Web page encryption is implemented using the Secure Sockets Layer (SSL) protocol.

This protocol uses

TCP port 443. The company's strategy has to cover both the external and the Internal Web sites.

Incorrect answers:

A: A CSP is a cryptographic service provider that is an independent software module providing actual

cryptographic functions. The master key is generated automatically and is periodically renewed. Any file

created in the RSA folder is automatically encrypted. Both EFS and CSPs look only in the RSA folder for

private keys. The RSA cryptographic algorithms are supported by the Microsoft Base Cryptographic Service

Provider and the Microsoft Enhanced Cryptographic Service Provider.

B: This option, though costly would work for the external website, but the passport service is just an

authentication service. And this is not enough security even if used in conjunction with other methods. Also you

have to keep in mind that although they are willing to spend money on security, it is a limited budget.

E: Enabling SSL on the external Web site by using an internal server certificate is not the answer as this poses a

security risk. Once users have gained access to a physical workstation, it's almost a given that they will require

access to resources stored on other machines on the local or wide area 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, Chapters 9 & 10, pp. 565, 642-645

QUESTION NO: 9

You need to design an access control strategy for the Contact Info and the Order History folders.

What should you do?

A. Create a domain local group named Customer Relations in the northwindtraders.com domain.

Add the Sales group and the Sales Managers groups to the Customer Relations group.

Add the Customer Relationships group to the Customer Information folder.

Assign the appropriate permissions.

Add the accounts for the sales department users in Boston to the Boston Customer Relationship group.

Add the Boston Customer Relationships group to the Customer Relations group.

Disable inheritance on the Payment folder.

B. Create a domain local group named Customer Relations in the boston.northwindtraders.com domain.

Add the Customer Relations group to the Customer Information folder.

Assign the appropriate permissions.

Add the Boston Customer Relations group to the Customer Relations group.

Disable permission inheritance on the Payment folder.

C. Create a domain local group named Customer Relations in the boston.northwindtraders.com domain.

Add the Customer Relations group to the Order History folder.

Assign the appropriate permissions.

Add the Boston Customer Relations group to the Customer Relations group.

Disable permission inheritance on the Payment folder.

D. Create a domain local group named Customer Relations in the boston.northwindtraders.com domain.

Add the Customer Relations group to the Customer Information folder.

Assign the appropriate permissions.

Add the Boston Customer Relations group to the Customer **MISSING**

Answer: A

Explanation: The Case study information is as follows: The Customer Information folder must be accessible to all members of the Sales group. Access to the Customer Information\Order History and the Customer Information>Contact folders must *be limited to members of only the Sales, Sales Managers, and Boston Sales group.*

The following shared company folders are located *on member servers* in New York: Research, Sales, Documentation and *Customer Information*. And The *Customer Information shared folder* contains the following folders: *Order History*, Payment and *Contact Info*.

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.

Incorrect answers:

B, C & D: The order of operations is wrong in this option because you first add user accounts to global groups, and then global groups are added to domain local groups.

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

Case Study #9, Consolidated Messenger

Overview

Consolidated Messenger is a large courier service company in New York. The company dispatches messengers throughout the city to pick up packages for immediate delivery elsewhere in the city.

Physical Locations

The 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.

Business Processes

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.

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. Because couriers are paid by the assignment, they must log in and mark each assignment as

complete to be paid. Couriers do not have physical access to the business office. The company always

experiences a high rate of turnover among the courier staff.

The information technology (IT) department has one senior administrator and two junior administrators who

provide all IT support for company users and couriers.

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.

Currently, access to resources is secured by using NTFS permissions and Active Directory-integrated application-specific authentication.

All customer billing and contact information must remain confidential.

Directory Services

The company's network consists of a single Active Directory domain. All users have domain user accounts. The senior IT administrator centrally manages all accounts.

Network Infrastructure

The network consists of the following three segments:

- Segment 1 contains all server computers.

- Segment 2 contains all business staff client computers.

- Segment 3 contains all dispatch lounge courier kiosks.

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.

There are five Windows Server 2003 computers on Segment 1.

The courier dispatch lounge contains only Windows XP Professional client computers.

The business office contains client computers that run the following operating systems:

- Windows 2000 Professional

- Windows 98 Second Edition

- Windows NT Workstation 4.0

- Windows XP Professional

- Windows 95

Problem Statements

Access to customer data and courier assignments is not sufficiently secure. 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.

Chief Executive Officer

Though some of our data is not confidential, we need to increase security for our data that is confidential. We

have had major security problems in the past, including compromised confidential customer data. 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.

Chief Information Officer

Our IT staff use their administrative accounts for everything which is acceptable on their own client computers.

However, they often log on to business office client computers with their own administrative account, and they

forget to log off after they are done. Consequently, business office users can perform tasks by using

administrator privileges, which creates network problems.

We also struggle to main 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. 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.

Senior IT Administrator

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. Although company policy allows

junior administrators to only reset passwords, the domain permissions do not currently allow them to do so.

Junior IT Administrator

Our biggest security patch management problem is that our users are not administrators on their computers.

Though we would need to track user administrative actions, I think we should make users administrators on

their own computers.

Courier

Event though I know I should pick a difficult password, I can only remember so much.

To simplify my life, I

use the same password at every job. I have heard that couriers watch and steal other courier's passwords, but it

has never happened to me.

Consolidated Messenger's written security policy contains the following requirements:

We must monitor and track when business office users attempt to make system registry configuration

changes to their computers. We do not need to monitor or track everyday actions on client computers.

We must monitor and track all access to sensitive company data, including most customer data and

courier assignments.

We must maintain all computers 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.

We 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.

Case Study #9, Consolidated Messenger (5 Questions)

QUESTION NO: 1

The company wants to evaluate making all business office users administrators on their client computers.

You 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. On all domain controllers, implement registry access auditing for all registry keys that are considered sensitive by the company's written security policy.
- B. On all client computers, implement logon auditing for all user account logons.
- C. On all client computers, configure registry access auditing for all registry keys that are considered sensitive by the company's written security policy.
- D. On all domain controllers, implement logon auditing for all user account logons.

Answer: C

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.

We also need to be able to **identify users who gain unauthorized access.**

We should make users administrators on their own computers.

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:

A: 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.

B: 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.

D: 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.

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 NO: 2

You need to identify potential security threats. Which of the following security breaches might occur under the current IT and security practices? (Choose all that apply)

- A. A virus that infects an IT administrator's client computer could gain domain administrator privileges.
- B. Couriers could gain access to domain administrator privileges.
- C. Business office staff could discover couriers' passwords and use them to access couriers' information.
- D. All users could use their user accounts to gain the ability to install untested security patches on their client computers.

Answer: A

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 Messenger:

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.

To conserve bandwidth, our firewall prevents client computers from accessing Windows Updates.

Couriers use a Web kiosk in the lounge to pick-up their assignments.

Couriers **do not have physical access** to the business office.

Business staff handles customer billing, **accepts phone class for new courier assignments, and enters the assignment into a custom**, Active Directory-integrated, client server application.

Incorrect answers:

B: 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.

C: 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.

D: 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.

Reference:

Roberta Bragg, MCSE Self-Paced Training Kit (Exam 70-298): Designing Security for a Microsoft Windows Server 2003 Network, p. 1:17

QUESTION NO: 3

You need to design a method for junior IT administrators to perform more IT support tasks. Your solution must meet business and security requirements. What should you do?

- A. Delegate appropriate Active Directory permissions to the junior IT administrators.
- B. Add the junior IT administrators' user accounts to the Domain Admins user group.
- C. Create a custom Microsoft Management Console (MMC) that uses taskpad views to enable the appropriate tasks for the junior IT administrators.
- D. Make the junior IT administrators' domain user accounts member of the local Administrators group on

all client computers.

E. Create new domain user accounts for each junior IT administrator.

Make the new accounts members of the Domain Admins group and instruct junior IT administrators to

use the new accounts only for appropriate administrative tasks.

Answer: A

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:

The information technology (IT) department has one senior administrator and **two junior administrators** who provide all IT support for company users and couriers.

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:

B: All user accounts are currently domain user accounts. Thus this option will not accomplish anything new.

C: This option will not grant the junior administrators with appropriate permissions to carry out their tasks.

D: Making junior administrators' accounts part of local Administrators group on all client computers will only

work when all accounts are joined to a domain.

E: To create new domain user accounts for the junior IT administrators and instructing them to use it only for appropriate use is impractical.

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 NO: 4

You need to design security changes that provide maximum protection for customer data and courier assignments.

What should you do?

- A. Create a separate domain for courier authentication.
- B. Implement smart card authentication for business office users and couriers, upgrading client operating systems as needed.
Modify the Web kiosks to require smart card presence for continued access.
- C. Modify the Default Domain Policy Group Policy object (GPO) so that couriers must use complex user account passwords.
Require all couriers to change their passwords the next time they log on to the Web application.
- D. Use Encrypting File System (EFS) to encrypt all files that contain customer 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 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.
- C:** 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.
- 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 NO: 5

You need to improve the company's security patch management process. Your solution must meet existing business requirements and it cannot increase the number of employees or unnecessarily increase ongoing administrative effort. What should you do?

- A. Provide all users with the ability to access and use 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.
Make all users members of the Power Users group on their client computers.
- D. Install the Active Directory Client Extensions on all Windows 95, Windows 98, and Windows NT Workstation 4.0 computers.
Manually download all security patches to a Distributed File System (DFS) replica.
Instruct all users to use the DFS replica to install security patches.
- E. Install the Active Directory Client Extensions on all Windows 95, Windows 98, and Windows NT Workstation 4.0 computers.
Install a Software Update Services (SUS) server and make all users local administrators on their client computers.

Answer: B

Explanation: Take into consideration the following:

To conserve bandwidth, our **firewall prevents client computers from accessing** Windows Updates.

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**.

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: 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.

C: By making all users 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: This option involves far too much administrative effort that can be avoided if one follows option B's reasoning.

E: This option will grant too many rights to the users than is advisable.

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

Case Study #10, Fabrikam

Text missing

Case Study #10, Fabrikam (9 questions)

QUESTION NO: 1

You need to design a security solution for the internally developed Web applications that meets business requirements. What should you do?

A. Install and configure a stand-alone root certification authoritative (CA) that is trusted by all company client computers. Issue encryption certificates to all developers.

B. Install and configure root certification authority (CA) that is trusted by all company client computers.

Issue code-signing certificates to all developers.

C. Purchase a root certification from a trusted commercial certification authority (CA). Install the root

certificated on all developers' computers.

D. Purchase a code-signing certificate from a trusted commercial certification authority (CA). Install the

certificate on all company client computers.

Answer: B

QUESTION NO: 2

You are designing a remote administration solution that meets business requirements. You need to specify client or server software that will be required. What should you do?

- A. Ensure that all client computers have a graphical Telnet client installed.
- B. Ensure that all client computers have the Remote Desktop Connection client software installed
- C. Ensure that all server computers have RCONSOLE installed and that it is configured to start automatically.
- D. Ensure that all server computers have Remote Administration (HTML) installed.

Answer: B

QUESTION NO: 3

You need to design a patch management strategy that meets business requirements. What should you do?

- A. Install Systems Management Server (SMS) on a computer on the internal network. Use the Default Domain Policy GPO to distribute the SMS client software to all computers in the domain.
- B. Install Microsoft Operations Manager (MOM) on a computer on the internal network. Use the Default Domain Policy GPO to distribute the MOM client software to all computers in the domain.
- C. Install Software Update Services (SUS) on a Web server, and configure it to synchronize and approve updates nightly. Configure client computers to receive automatic updates from the Web server. Ensure that users restart their client computers daily.
- D. Install Software Update Services (SUS) on a domain controller, and configure it to synchronize and approve updates nightly. Configure client computers to receive automatic updates from the domain controller. Ensure that users restart their client computers daily.

Answer: B

QUESTION NO: 4

You need to design a remote access strategy for portable computers. Your solution must meet business requirements. What should you do?

- A. Issue a computer certificate to P_RAS1. Reconfigure the remote access policy on P_RAS1 to accept only EAP-MD5 authentication. Then, specify that P_RAS1's computer certificate is to be used for authentication.
- B. Issue a user certificate to the Administrator account on P_RAS1. Reconfigure the remote access policy to accept only EAP-MD5 authentication. Then, specify that the Administrator account's user certificate is to be used for authentication.
- C. Issue a computer certificate to P_RAS1. Reconfigure the remote access policy to accept only EAP-TLS authentication. Then, specify the P_RAS1's computer certificate is to be used for authentication.
- D. Issue a user certificate to the Administrator account on P_RAS1. Reconfigure the remote access policy to accept only EAP-TLS authentication. Then, specify that the Administrator account's user certificate is to be used for authentication.

Answer: C

QUESTION NO: 5

You are designing a security strategy for the public Web server. Your solution must address the chief security officer's concerns. What should you do?

- A. Install a Web server certificate on WEB1.
- B. Enable Internet Connection Firewall (ICF) on WEB1.
- C. Configure IIS on WEB1 to operate in IIS 5.0 isolation mode.
- D. Install and configure the URLScan ISAPI filter on WEB1.

Answer: D

QUESTION NO: 6

You need to design a method of communication between the IT and HR departments. Your solution must meet business requirements. What should you do?

- A. Design a custom IPSec policy to implement Encapsulating Security Payload (ESP) for all IP traffic.
Design the IPSec policy to use certificate-based authentication between the two departments' computers.
- B. Design a custom IPSec policy to implement Authentication Header (AH) for all IP traffic. Design the IPSec policy to use preshared key authentication between the two departments' computers.

C. Design a customer IPSec policy to implement Encapsulating Payload (ESP) for all IP traffic. Design the IPSec policy to use preshared key authentication between the two departments' computers.

D. Design a customer IPSec policy to implement Authentication Header (AH) for all IP traffic. Design the IPSec policy to use certificate-based authentication between the two departments' computers.

Answer: A

QUESTION NO: 7

You need to design an authentication strategy for users of portable computers. Your solution must meet business requirements. What should you do?

A. Issue smart cards and smart card readers to all portable computer users. Configure the domain to require smart cards for login and to log off users who remove their smart cards.

B. Configure the portable computers to connect to only wireless networks that use Wired Equivalent Privacy (WEP). Install digital certificates on all portable computers.

C. Install computer certificates on all portable computers. Configure all portable computers to respond to requests for IPSec encryption.

D. Install biometric authentication devices on all portable computers. Configure the Default Domain Policy GPO to require complex passwords for all users.

Answer: A

QUESTION NO: 8

You need to design an access control strategy for the financial data used by the accounting department.

Your solution must meet business requirements. What should you do?

A. Modify the properties of the computer object named P_FS2 to enable the **Trust computer for delegation** attribute. Instruct accounting department users to use Encrypting File System (EFS) to encrypt files.

B. Modify the properties of all accounting department user accounts to enable the **Account is trusted for delegation** attribute. Instruct accounting department users to use Encrypting File System (EFS) to encrypt files.

- C. Modify the properties of accounting department computers to enable the **Trust computer for delegation** attribute. Configure accounting department client computers to use IPSec to communicate with P_FS2.
- D. Modify the properties of all administrator accounts in the forest to enable to **Account is trusted for delegation** attribute. Configure accounting department client computers to use IPSec to communicate with P_FS2.

Answer: A

QUESTION NO: 9

You need to design a method to ensure that only scripts that are approved by the IT department can run on company computers. Your solution must meet business requirements. What should you do?

- A. Create a new software restriction policy in the Default Domain Policy GPO that removes the Microsoft Visual Basic Scripting Edition and the Windows Script Component file types from the File Types list.
- B. Create a new software restriction policy in the Default Domain Policy GPO that disables the use of Wscript.exe and Cscript.exe.
- C. Configure Windows Script Host to not execute Windows Script Component file types.
- D. Configure Windows Script Host to execute only scripts that are signed by a certificate issued by an approved certification authority (CA).

Answer: D

Case Study #11, Fourth Coffee

Text missing

Case Study #11, Fourth Coffee (4 questions)

QUESTION NO: 1

You need to design a method to modify the current e-mail ordering system. Which will be used until Fourth Coffee deploys the Web-based ordering application. Your solution must address business concerns and improve security. What should you do?

- A. Configure the mail server to disallow SMTP relaying.
- B. Instruct customers to obtain digital certificates from a trusted commercial authority (CA), and digitally sign all order e-mail messages. Reject unsigned order e-mail messages.
- C. Provide customers with a public encryption key, and instruct them to encrypt all order e-mail messages. Reject unencrypted e-mail messages.
- D. Implement an e-mail filtering solution, and add customer e-mail addresses to the list of allowed addresses. Reject e-mail messages from other addresses.

Answer: B

QUESTION NO: 2

You need to design a domain model that meets the company business and security requirements for controlling access to the new Web-based ordering application. What should you do?

- A. Create a child OU within the existing domain.
- B. Create a child domain of the existing domain.
- C. Create a new domain in a new forest. Configure the new domain to trust the existing domain.
- D. Create a new tree in the existing forest. Configure the new domain to trust the existing domain.

Answer: C

QUESTION NO: 3

You need to design a security patch management strategy. Your solution must meet business and security requirements, and it must accommodate the company's resource restrictions. What should you do?

- A. Test and manually deploy updates.
- B. Deploy a Software Update Services (SUS) server. Test all updates and then approve them. Configure all client computers to automatically obtain updates from the server.
- C. Test all updates and then use a third-party utility to repackage updates in a Windows Installer file. Deploy the -.msi files by using Group Policy.
- D. Configure all client computers to use Automatic Updates to obtain security updates from the Windows Update Web site. Test all updates posted to the Windows Update Web site.

Answer: B

QUESTION NO: 4

The company is evaluating using a new Active Directory domain to contain all customer user accounts.

You need to design a monitoring or logging strategy that meets business and security requirements for the new Web-based ordering application. Your solution must minimize overhead on existing domain controllers and servers. What should you do?

- A. Enable logon auditing in both the new and the existing domains.
- B. Enable logon auditing only in the existing domain.
- C. Enable logon auditing only in the new domain.
- D. Enable logon auditing on only the Web server.

Answer: C

Case Study #12, Trey Research

Background

Overview

Trey Research is a medical research company that develops and improves technologies that are used in the health care industry.

Physical locations

The company's main office is located in Atlanta. The company has branch offices in San Francisco and New York.

Planned Changes

Trey Research is entering into a partnership with Contoso, Ltd., to collaborate on research projects. Trey

Research needs to enable encrypted communications with Contoso.

The company also plans to implement a new wireless network and upgrade all client computers to Windows XP Professional.

Existing Environment

Business Processes

Users in the marketing department access marketing data by using a Web-based application that is installed on a server running IIS 6.0.

Research intellectual property is stored on database servers. Researchers access research intellectual property

data on the database servers by using a Web-based application that resides on the company intranet. The

researchers' level of access to the data is dependent upon their position in the department and their project involvement.

Some intellectual property information is also stored in a shared folder name Research Stats on a server named

ATLFP1.1 The information in the Research Stats folder is the only intellectual property information that is

shared with partners. The Research stats folders contains a folder for each research project and the following

folders:

- M&S
- Reports
- Partner

Permission set on all research intellectual property ensures that unauthorized users do not have access to the information.

The following table lists a subset of the groups, group members, and associated levels of access used at Trey

Research for the Research Stats folder.

Group Members Access

Contoso Contoso, Ltd, employees,
information technology (IT)
department users

Allowed access to the Partner
folder only

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

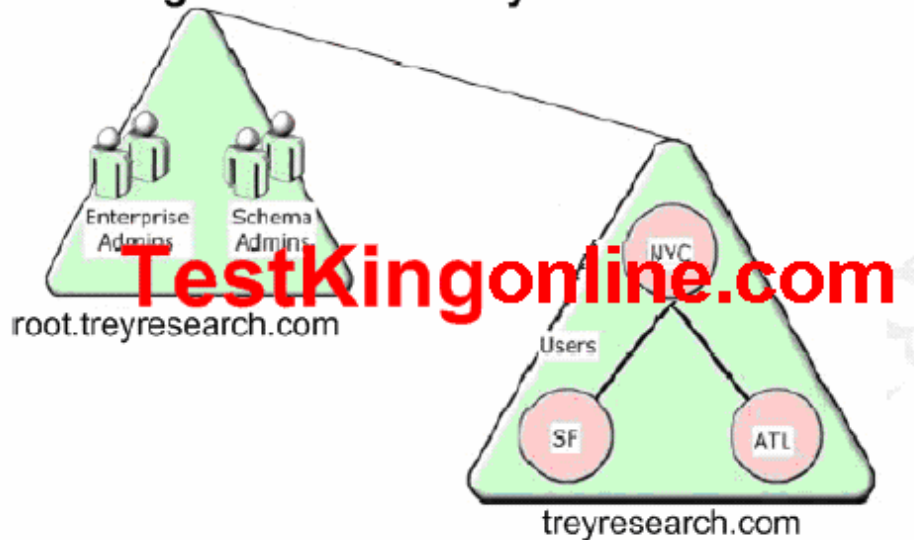
Allowed access to marketing and
Sales related information including
the M&S folder

Research Research and IT department users Allowed access to research data

Directory Services

The company Windows Server 2003 Active Directory environment is shown in the
Existing Active Directory
exhibit.

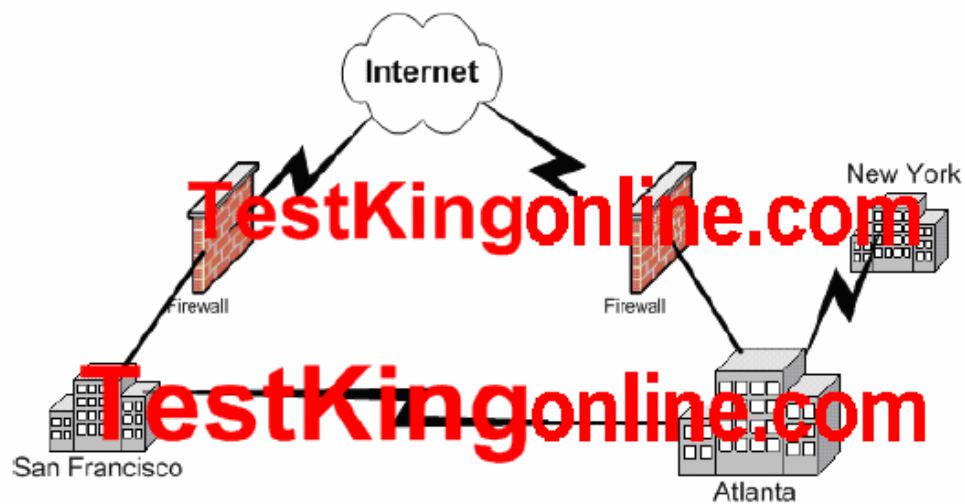
Existing Active Directory Environment



The root.treyresearch.com domain is an empty root domain.

Network Infrastructure

The network for Trey Research is shown in the Existing network exhibit.



The following table lists the servers on the network and their respective location, function, and operating system.

Firewalls allow all DNS name resolution.

A public key infrastructure (PKI) was deployed on ATLCA1. The PKI is integrated with Active Directory and uses Certificate Services. Trey Research plans to use smart cards. Encrypted files and folders reside on ATLFP2.

Problem Statements

The following business problems must be considered:

- Users need to remember up to five passwords and to access data and applications.
- 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.
- Some researchers have stored encrypted confidential data on their client computers.

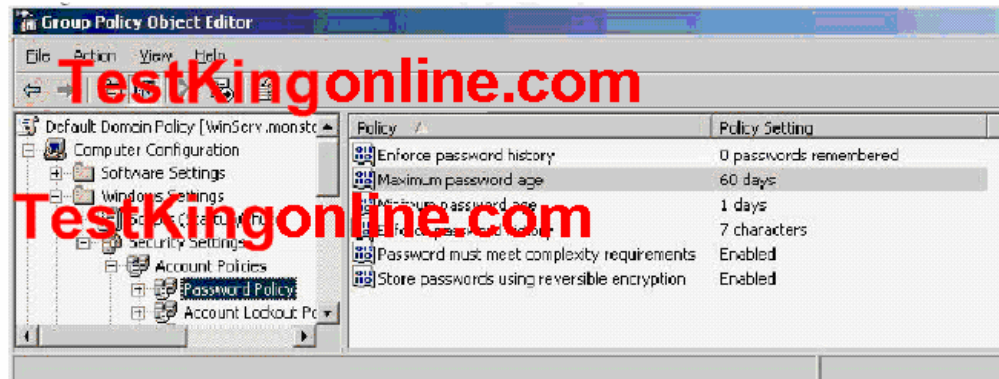
Interviews

Chief Executive Officer

To improve the effectiveness of our research efforts, we need to foster collaboration both within Trey Research and with Contoso, Ltd., by increasing the efficiency of our data sharing. Though we will share some information, it is still critical to keep research information confidential. Scientist and other users in the research department often work long hours in the office and from home, so they need a secure method of accessing the network and using shared resources. Contoso, Ltd., also shares confidential data with us, so some Contoso, Ltd., users will need secure methods, to access our company's network and shared resources.

Chief Information Officer

Information shared between Trey Research and other companies must use the strongest encryption and authentication possible in order to keep the information confidential. Internally, identify management is a problem. I want to address this problem by physically issuing smart cards. Also, we need to strengthen our current password policy, which is shown in the Current Password Policy Configuration exhibit.



Minimizing IT expenses is important but we need to implement a cost-effective solution that addresses accessing multiple resources, including the new wireless LAN, the intranet Web server, and the terminal server, Our solution must require two-factor authentication.

System Administrator

Because other companies have different network environments and business processes, sharing research data with partner company might be technically challenging. We need to create 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

The following security requirements must be considered:

- All communications to the research database servers must be encrypted.
- Security patches must be tested before they are deployed
- Security must not interfere with application functionality.
- The HR segments needs additional protection to prevent non-HR internal users from gaining unauthorized access.
- All traffic to the Web-based marketing and research applications must be encrypted.
- 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.
- Only authorized users and computers can connect to the wireless network.
- DNS records must not be transferred to external sources.
- Administrators must be responsible for enrolling users.

Case Study #12, Trey Research (10 questions)

QUESTION NO: 1

You need to design an authentication solution for Terminal Services that meets the business requirements.

What should you do?

- A. Configure the terminal server to use smart cards.
- B. Configure IPsec to permit only Remote Desktop Protocol (RDP) connections to the terminal server.
- C. Deny the Remote Desktop Users group access to the terminal server.
- D. Restrict treyresearch.com users from logging on locally to the terminal server.

Answer: B

QUESTION NO: 2

You need to design an authentication solution for the wireless network. Your solution must meet the security requirements.

What should you do?

- A. Create wireless VPNs using L2TP/IPsec between the client computers to the wireless access point.
- B. Configure IEEE 802.1x authentication with smart cards
- C. Configure the wireless network to use Wired Equivalent Privacy (WEP).
- D. Install and configure an Internet Authentication Service (IAS) server.

Answer: C

QUESTION NO: 3

You need to design a strategy to move confidential data from research users' client computers to ATLFP2. Your solution must meet the business requirements. What should you instruct the research users to do?

- A. Move the encrypted data to a folder on ATLFP2 over an IPsec connection.
- B. Move the encrypted data to an Encrypting File System (EFS) folder on ATLFP2 over an IPsec connection.
- C. Move the encrypted data to a new server that is not a member of the domain, and then move it to ATLFP2.

D. Move the encrypted data to a compressed folder on ATLFP2 by using Web Distributed Authoring and Versioning (WebDAV) over SSL.

Answer: B

QUESTION NO: 4

You need to design an access control strategy for the marketing application. Your solution must minimize impact on server and network performance. What should you do?

- A. Require client computers to connect to the marketing application by using a VPN connection.
- B. Use IPsec to encrypt communications between the servers in the New York and Atlanta offices.
- C. Require the high security setting on Terminal Services connections to the marketing application.
- D. Configure all marketing application Web pages to require SSL.

Answer: D

QUESTION NO: 5

You need to design a PKI that meets business requirements. What should you do?

- A. Move ATLCA1 offline and create an enterprise subordinate CA to issue certificates.
- B. Create a stand-alone subordinate CA to issue certificates.
- C. Use a qualified subordinate CA.
- D. Configure certificate template access control lists (ACLs) on ATLCA1.

Answer: A

QUESTION NO: 6

You need to design a method to ensure that research intellectual property remains confidential. Your solution must meet security requirements. What should you do?

- A. Require client computers to connect to research intellectual property through a SSL VPN.
- B. Place SFSQL1 and ATLSQL1 on a separate virtual LAN from the internal network. Grant access to these virtual LAN segments to only the client computers that are used by authorized users.
- C. Require that communications between SFSQL1, SFFP1, ATLSQL1, and ATLFP1 use IPsec.
- D. Create a separate subnet for all servers that contain research intellectual property.

Answer: C

QUESTION NO: 7

You need to provide users in the research department access to different functions of the Web-based research application based on individual user roles. What should you do?

- A. Use Windows directory service mapper and enable Microsoft .NET Passport authentication.
- B. Create authorization rules and scopes by using Authorization Manager.
- C. Use one-to-many client certificate mapping.
- D. Define permissions by using access control lists (ACLs).

Answer: B

QUESTION NO: 8

You need to design a password policy that meets business requirements. What should you do? Select all that apply.

- A. Increase the number of passwords that are remembered.
- B. Disable reversible encryption.
- C. Set the minimum password age to zero days.
- D. Increase the maximum password age.

Answer: A, C

QUESTION NO: 9

You need to design a certificate management process for internal users. What should you do?

- A. Establish a Web enrollment service for internal users to request access to resources.
- B. Grant Enrollment Agent rights to users.
- C. Establish enrollment stations and store user certificates in a smart card.
- D. Create Connection Manager scripts to identify the client computer operating system, and configure Web proxy settings to specify the appropriate Web enrollment service.

Answer: C

QUESTION NO: 10

You need to design a method to standardize and deploy a baseline security configuration for servers. Your solution must meet business requirements. What should you do?

- A. Create a script that installs the Hisecdc.inf security template.
- B. Use a GPO to distribute and apply the Hisec.inf security template.
- C. Use the System Policy Editor to configure each server's security settings.

D. Use a GPO to distribute and apply a custom security template.

Answer: D