Exam Code: 070-298
Designing Security for a MS Windows Server 2003 Network

Demo Version

To Access Full Version, Please go to
www.itexamworld.com

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.com and ADO.com.

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.com and ADO.com.

It is accessible from anywhere on the Internet .

The Web site also includes static content about each resort.

Directory Services

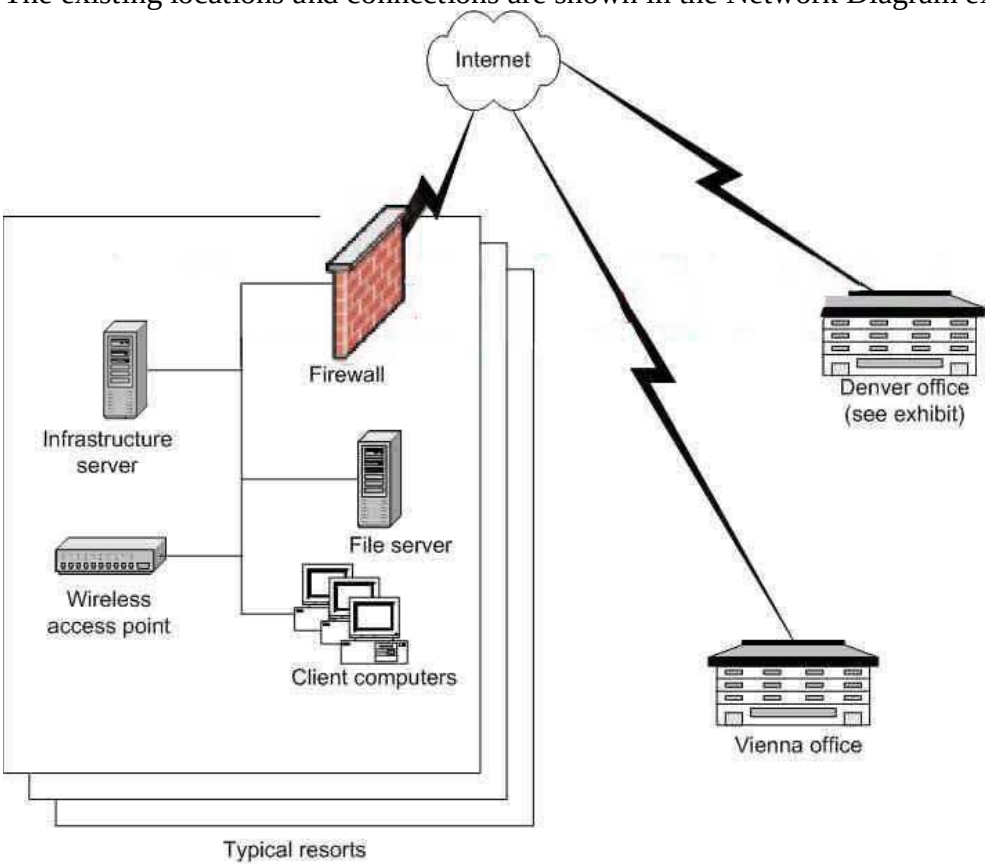
The company uses an Active Directory domain named alpineskihouse.com for North America. The Denver IT Department administers the domain. The alpineskihouse.com domain will remain the forest root domain.

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

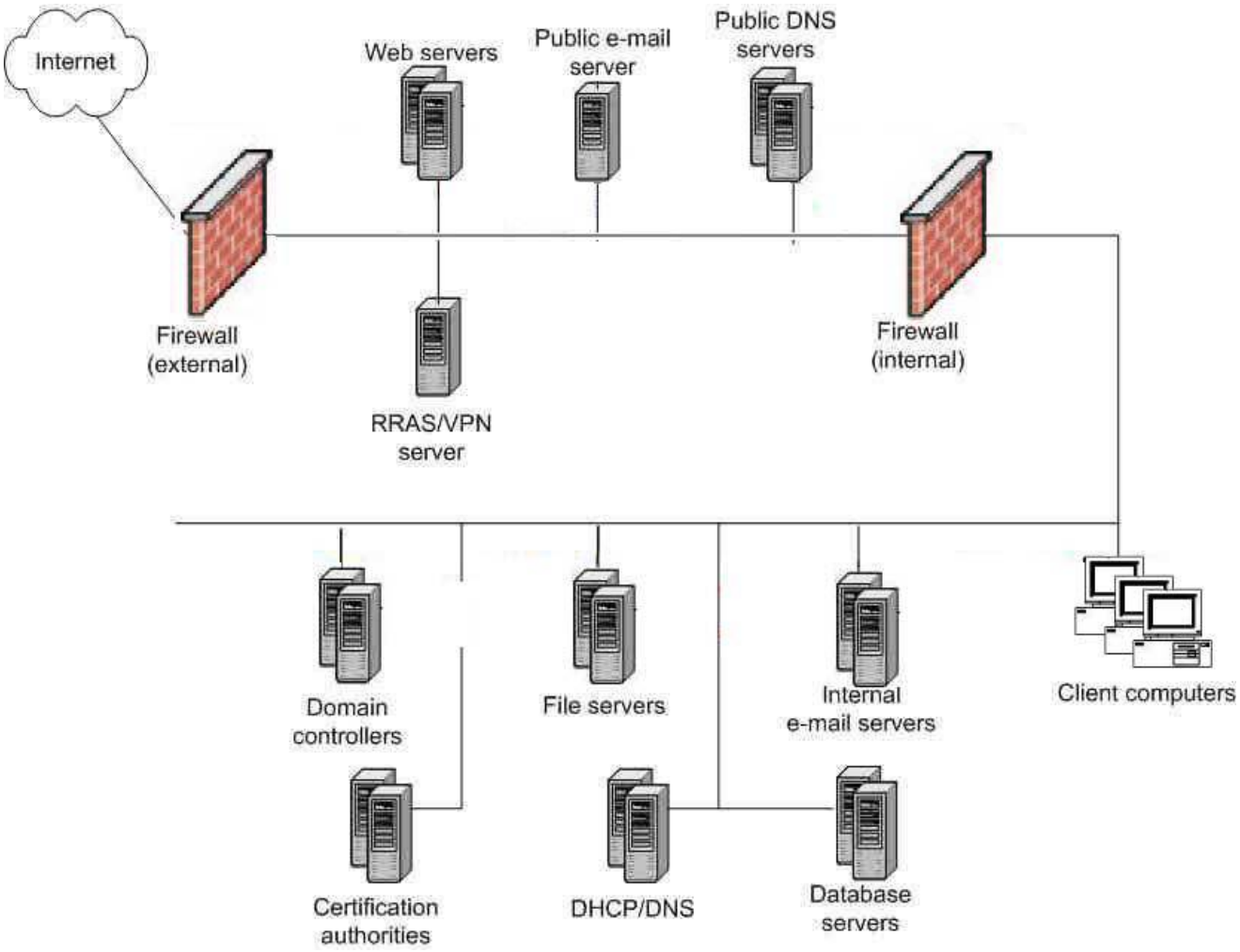
All employees have user accounts in either Active Directory or in the Windows NT 4.0 domain.

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 polices. 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

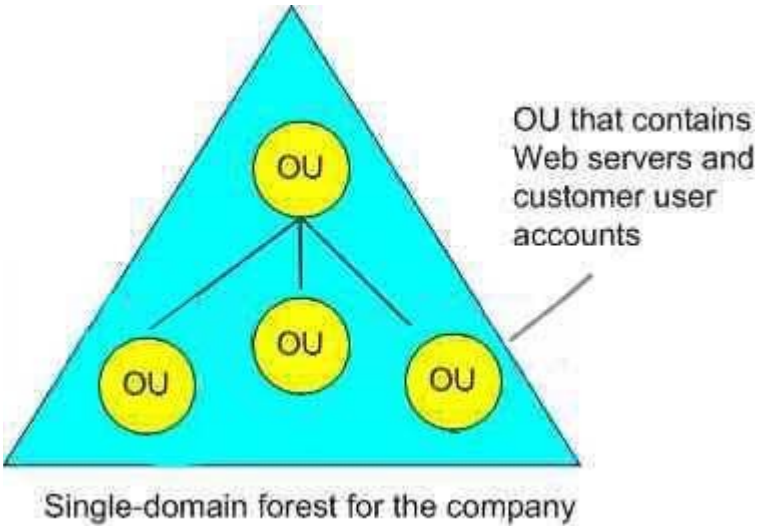
The following customer requirements for wireless access and kiosk computers must be considered:
Staff and customers must be able to access the wireless network; however, corporate servers must be accessible only to staff.
Kiosk computers can be used for browsing the Internet only. Kiosk computers will 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.

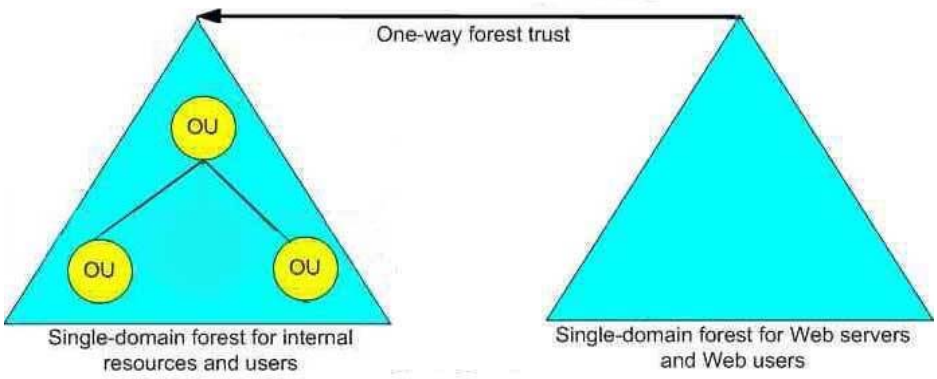
All IT staff that support users must be members of the AllSupport security group. Highly skilled IT staff must also be members of the security group named AdvancedSupport. Less experienced staff members must also be members of the BasicSupport group.
All client computers in Europe must be configured 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 user Remote Desktop Protocol (RDP) to manage the servers in the perimeter network.
IT staff must be also be able to use RDP to manage severs 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.

QUESTION 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.

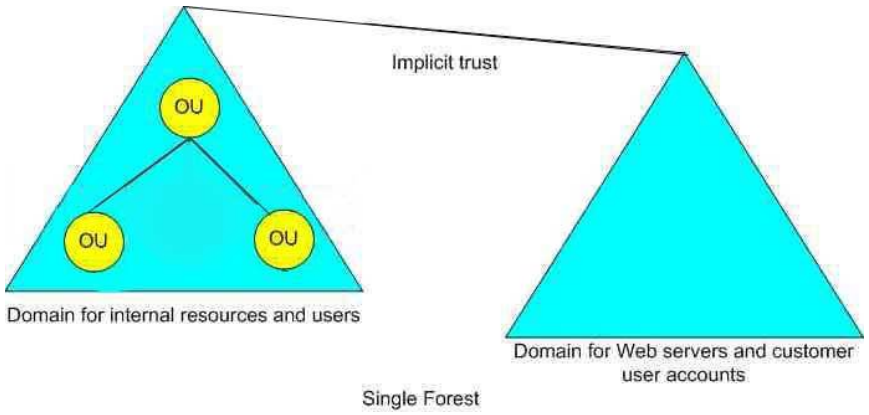


Single-domain forest for the company

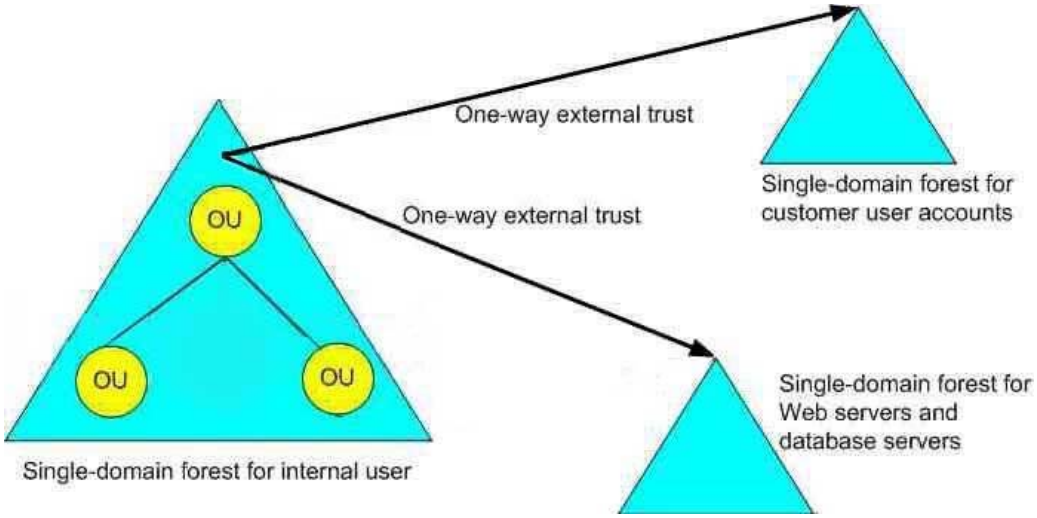
B.



C.



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(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 103

QUESTION 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?

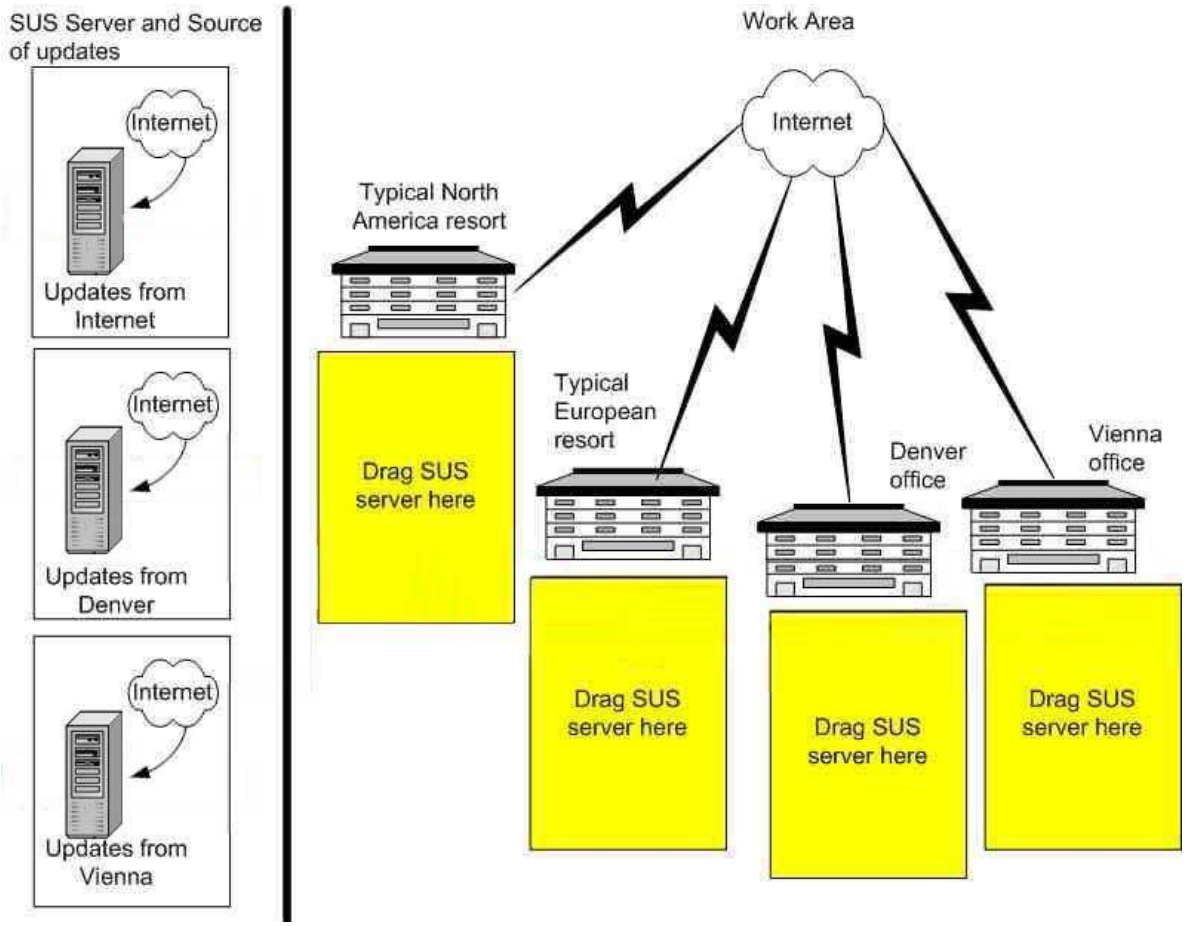
A. Configure the kiosk computers as computers that are not members of any domain.
Use Local Computer Policy to configure the computers with the collection of settings in the Kiosk Desktop Specification.
B. Install one kiosk computer as a model.
Configure this computer with the collection of settings 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

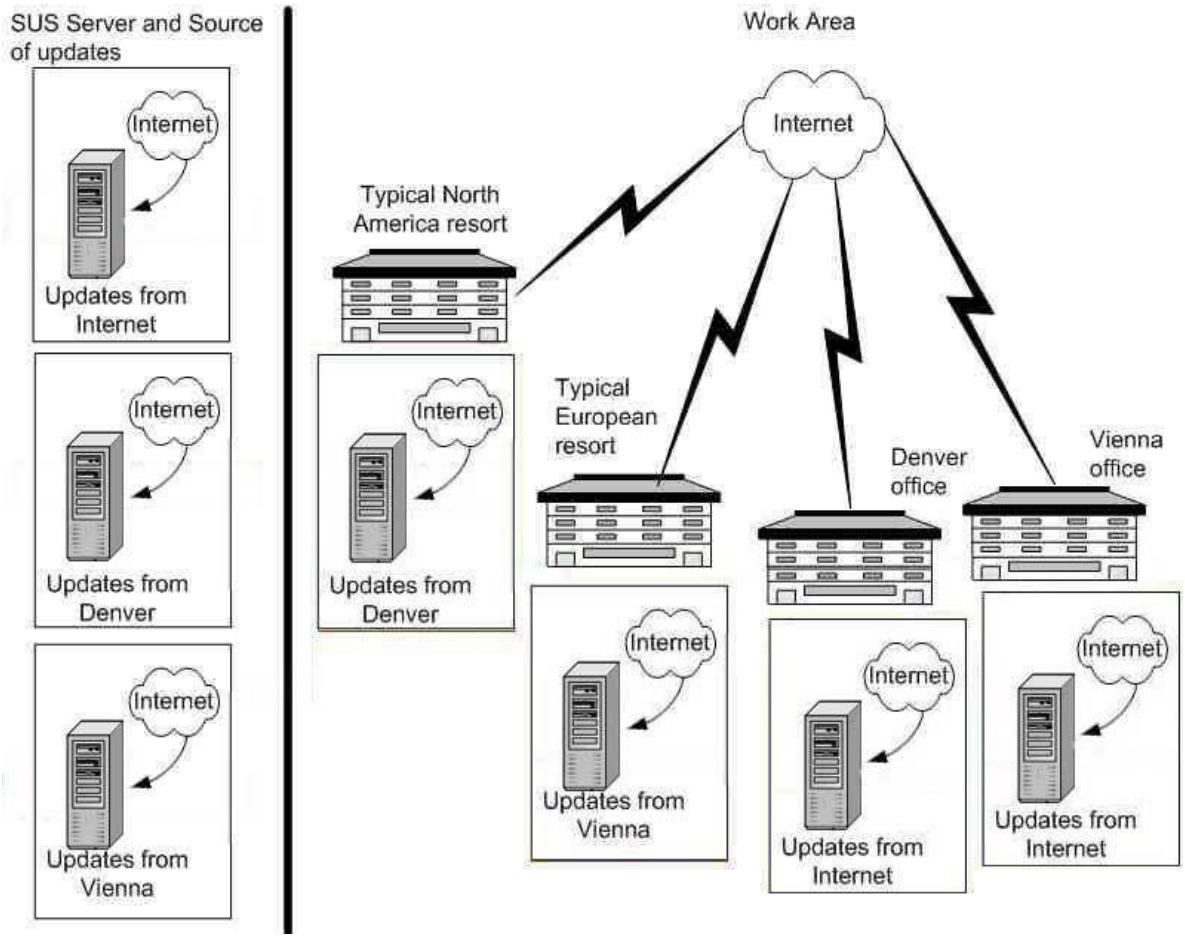
Explanation: Group Policy Object (GPO) is a set or sets of rules for managing client configuration settings that pertain to desktop lockdowns and the launching of applications. GPOs are data structures that are attached in a

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(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 21

QUESTION 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.


SUS Server and Source of updates
Internet
Updates from Internet
Internet
Updates from Denver
Internet
Updates from Vienna
Work Area
Internet
Typical North America resort
Drag SUS server here
Typical European resort
Drag SUS server here
Denver office
Drag SUS server here
Vienna office
Drag SUS server here

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:

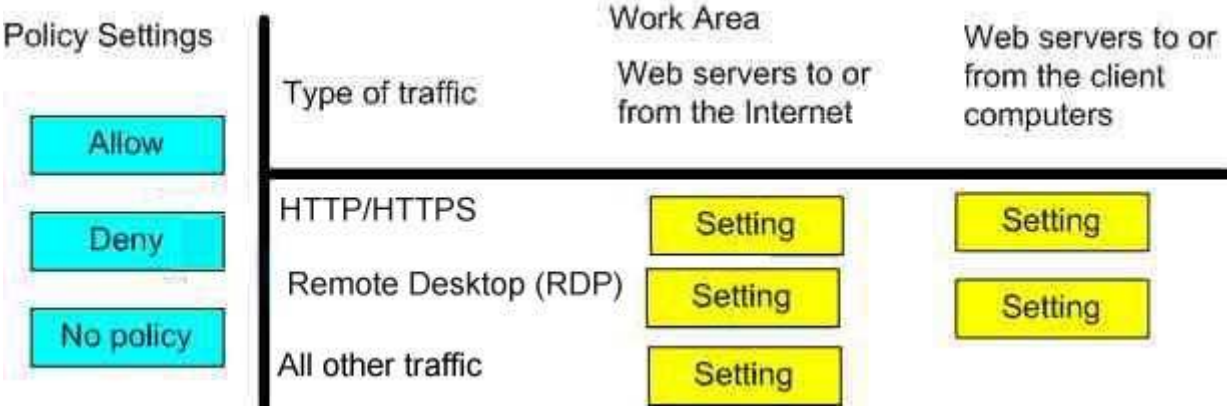
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 588

QUESTION 4

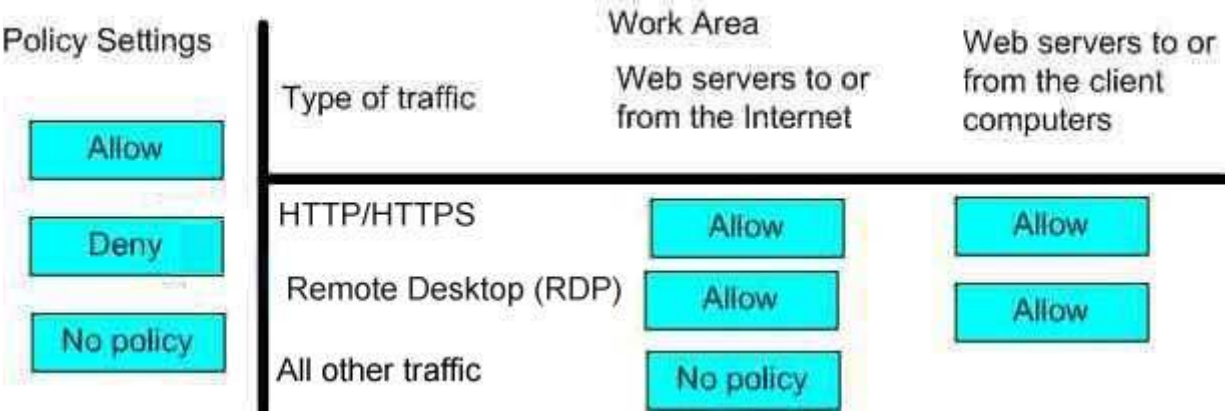
You need to design the IPSec policy for the Web servers in the Denver office. You need to decide which policy settings to use.

What should you do?

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



Answer:



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(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 576

QUESTION 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(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 21

QUESTION 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 that it was even three or five years ago.
Reference:
Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows (r) Server 2003 Environment Management and Maintenance Study Guide, p. 557
Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 9, p. 325

QUESTION 7
You 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 (r) Server 2003 Environment Management and Maintenance Study Guide, p. 143

QUESTION 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(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 21