070-220

TEST KING

LEADING THE WAY IN IT
TESTING AND CERTIFICATION TOOLS!

Designing Security for a Microsoft Windows 2000 Network

Version 1

Important Note
Please Read Carefully

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of just cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

We are constantly adding and updating our products with new questions and making the previous versions better so email us once before your exam and we will send you the latest version of the product.

Each .PDF file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that particular .PDF file being distributed by you. Testking will reserve the right to take legal action against you according to the International Copyright Law. So don't distribute this PDF file.

Case Study No: 1

JUST TOGS

Background:
Just Togs is a clothing retailer that has been in business for eight years. Last year's total sales for all retail stores were $240 million. After tremendous growth during the past eight years, the clothing business has slowed in its existing retail stores.

Organization:

Headquarters:
Headquarters is located in San Jose. California, Headquarters employs 80 people. Twelve of these employees are in the IT department.

Retail Stores:
Retail stores are located in California. There are 50 employees at each retail store

Problem Statement:

President:
Our old business model relied on expansion by building new retail stores. However, expansion takes time, and the area served by a single retail store is limited. The only way to rapidly increase sales is to build a Web site. This site would allow customers from across the United States to buy our clothing.

IT Director:
We have three major areas of concern. First, we must ensure that the information on our Web server can be modified only with proper authorization and that the information is distributed only to those authorized. We also want to be informed when someone accesses data on the Web server. Second, information must be secure as it travels from the customer's computer to our server. We must prevent user IDs, passwords, and financial information from being intercepted as this information travels to our server. Third, information that customers download must not damage their software or violate licensing agreements.

Our IT department will be expanded to include a Webmaster, who will administer the Web site, Web developers who will write code for the Web pages, and Web authors who will create the Web content.

Marketing Director
We have developed an ActiveX control that customers will be able to download from the Web site. Customers can use this control to display different sizes of clothing on a 3-0 model. They can customize the model with their measurements. They can then dress the model with our clothes to show how the clothes will fit and select the correct size.

When people first view our Web site, they will be considered visitors. After visitors enter their name and address and receive an ID we will consider them customers.

From our Web site, we must include a method for the customer to view our clothes and place selected items in a shopping basket. We will need a checkout function that allows the customer to enter shipping and billing information. This should include the customer's name, address, phone number, and credit card number. This information, including the customer's ID and password will be stored in a database.

When customers revisit our site, we will be able to identify them automatically by their ID and password. They can then view the status of their orders or place additional orders. We should also let customers know that they are connected to the Just Togs Web site.

The entire transaction should be logged. The information will be stored in a transaction-tracking file. This file will contain credit card numbers and other confidential customer information. The transaction-tracking file will allow us to bill the customer and to provide information for our customer service employees if problems arise.

Customer Service Director:
All customer service employees must have access to customer information. This includes customers' personal information, such as name, address, phone number, and account number.

Existing IT Environment:

Headquarters:
Headquarters has four Windows NT Server 4 0 computers. The remote access server is named JTRAS. The primary domain controller is named JTDC1. The other two servers are used to run applications.

Retail Stores:
Each retail store has two Windows NT Server 4 0 computers. One server controls all cash register functions. The second server handles inventory and word processing functions and has a dial-up connection to headquarters. All retail stores use TCP/IP. Each office has its own user account for dial-up access. This connection is used to transmit daily sales and merchandise orders to headquarters.

Connectivity:
All computers in the headquarters LAN are connected through a 100-Mbps connection. Each retail store is connected to headquarters through a WAN through a 56-Kbps dial-up connection.

Envisioned IT Environment:

Headquarters:
The existing Windows NT Server domain controller will be upgraded to Windows 2000 native mode, and a single forest will be created. The envisioned placement of servers is shown in the exhibit. Click the exhibit button.

A DMZ will be set up between the public and private network. In addition, Just Togs plans to add six new Windows 2000 Server computers. A Web server named JTWEB will be multi-homed. A server named JTDEV will be used by programmers to develop the Web content. A server named JTDATA will contain all customer, inventory, and order information. This information will be stored in Microsoft SQL Server databases. A server named JTVPN will be used as the VPN server. JTDC2 will be a new domain controller.

The company wants to eliminate its remote access server and allow the retail stores to submit their data over the Internet through a VPN.

Retail Stores:
The hardware and software at the retail stores will remain the same.

Connectivity:
The WAN and LAN bandwidth will remain the same.

Questions Just Togs

Q. 1
Which audit policy should you use to detect possible intrusions into the Just Togs network?

A. Success and failure audit for process tracking
B. Success and failure audit for privilege use
C. Success and failure audit for policy change
D. Success and failure audit for logon events

Answer: D
Explanation: Audit Account Logon Events records information about any attempt to log on to a computer or server to gain access to the network. By auditing success and failure, we will record all attempted logons whether they are successful or not. This information can be used to determine which user accounts are being used to attempt to access the network.

Incorrect Answers:
A: Process Tracking audits applications and records information about the actions that a particular application performs. This information can be used to determine which files and registry keys an application requires access to. It cannot be used to detect possible network intrusions.
B: We can audit Privilege Use to record information about when a user exercises a user right, such as changing the system time, or any time an administrator takes ownership of a file. This can be used to trace an intruder’s actions once the intruder has access to the network but it will not aide in detecting a potential intrusion.
C: We can audit Policy Change to record events in which changes to the local policies are brought about through Group Policy. Audit for Policy Change does not record information that can be used to detect possible network intrusions.

Q. 2
Which type of CA should you use to digitally sign the ActiveX control?

A. Enterprise subordinate CA
B. Third-party CA
C. Enterprise root CA
D. Stand-alone root CA

Answer: B

Explanation:
When an application that requires certificates runs on a public network, such ActiveX controlls that run on the internet, you should use certificates from Third-Party Cas. The use of a third-party certificate increases customer trust in the application. Consumers may not trust a small or unknown organization when that same organization issues the certificate for the Web site. Third-Party CAs are managed by companies such as Entrust or Verisign.

Incorrect Answers:

A: Enterprise CAs are integrated with Active Directory and publish certificates and CRLs to Active Directory. They use certificate template information, user account information, and security group information that are stored in Active Directory to approve or deny certificate requests. For a certificate request to be approved, the user that requests the certificate must have Enroll permissions granted by the security Access Control Lists of the certificate template for the certificate type that is requested. When a certificate is issued, the enterprise CA uses information in the certificate template to generate a certificate with the appropriate attributes for that certificate type. Therefore Enterprise CAs can only issue certificates for users that have user accounts in Active Directory.

Furthermore, we can create a hierarchy of CAs. The CA at the top of a hierarchy is referred to as a root CA and the CAs below the root are referred to as subordinate CAs. The root CA is a very important point of trust in an organization as all certificates flow from the root. It issues its own certificate and the certificates for its subordinate CAs. We should therefore take the root CA offline once the subordinates have been granted certificates. The subordinates would then respond to certificate requests.

C: Enterprise CAs are integrated with Active Directory and publish certificates and CRLs to Active Directory. They use certificate template information, user account information, and security group information that are stored in Active Directory to approve or deny certificate requests. For a certificate request to be approved, the user that requests the certificate must have Enroll permissions granted by the security Access Control Lists of the certificate template for the certificate type that is requested. When a certificate is issued, the enterprise CA uses information in the certificate template to generate a certificate with the appropriate attributes for that certificate type. Therefore Enterprise CAs can only issue certificates for users that have user accounts in Active Directory.

Furthermore, we can create a hierarchy of CAs. The CA at the top of a hierarchy is referred to as a root CA and the CAs below the root are referred to as subordinate CAs. The root CA is a very important point of trust in an organization as all certificates flow from the root. It issues its own certificate and the certificates for its subordinate CAs. We should therefore take the root CA offline once the subordinates have been granted certificates. The subordinates would then respond to certificate requests.

D: Unlike Enterprise CAs, Stand-alone CAs does not require Active Directory and does not use certificate templates. Instead all information about the requested certificate must be included in the certificate request. By default, all certificate requests submitted to stand-alone CAs are held in the Pending Queue until the CA administrator approves them. We can configure stand-alone CAs to issue certificates automatically but this would represent an increase in security risk and is usually not recommended.

Furthermore, we can create a hierarchy of CAs. The CA at the top of a hierarchy is referred to as a root CA and the CAs below the root are referred to as subordinate CAs. The root CA is a very important point of trust in an organization as all certificates flow from the root. It issues its own certificate and the certificates for its subordinate CAs. We should therefore take the root CA offline once the subordinates have been granted certificates. The subordinates would then respond to certificate requests.

Q. 3
Which audit policy should you use on JTWEB?

A. Success and failure audit for process tracking
B. Success and failure audit for object access
C. Success and failure audit for logon events
D. Success and failure audit for directory service access

Answer: B
Explanation:
According to the IT Director, Just Togs wants to ensure that the information on their Web server can be modified only with proper authorization; that the information is distributed only to authorized users; and that Just Togs be informed when someone accesses data on the Web server. The information or data on the Web server are called objects. We would thus want to Audit Object Access. By auditing successful and failed object acess, enteries will recorded to a log when a user attempts to gain access to a file or folder. However, the administrator must configure which specific files and folders should be audited.

Incorrect Answers:

A: Process Tracking audits applications and records information about the actions that a particular application performs. This information can be used to determine which files and registry keys an application requires access to. It cannot be used to log attempted file and folder access, for this we should audit object access.

C: Audit Account Logon Events records information about any attempt to log on to a computer or server to gain access to the network. By auditing success and failure, we will record all attempted logons whether they are successful or not. This information can be used to determine which user accounts are being used to attempt to access the network, however, we need to audit access to a Web server and not the network in this scenario. We therefore cannot use Audit Account Logon Events.

D: Audit Directory Service Access is used to record information whenever a user gains access to an Active Directory object. To log this type of access, we must configure specific Active Directory objects for auditing. Active Directory provides the directory service in a Windows 2000 network. It stores information about network resources and makes the resources accessible to users and applications by uniquely identifying resources on a network.

Q. 4
Which methods should you use to identify and authenticate existing customers on the Web site?

A. SSL, NTLM logon, and database validation
B. SSL, anonymous logon, and CHAP
C. SSL, NTLM logon and CHAP
D. SSL, anonymous logon and database validation

Answer: A
Explanation:
By implementing Secure Socket Layer (SSL) protocol we can protect secure areas of the Web server as SSL encrypts all data transferred between the customer on the public network and the Web server. We have no control over which operating system the customers will use to access the web site. We therefore cannot use Kerberos authentication as Kerberos is only supported on Windows 2000 and UNIX clients. We should instead use can use Kerberos. We therefore require the use of NTLM to provide authentication for downlevel clients. According to the Marketing Director, when people first view the Just Togs Web site, they are considered visitors until they enter their name and address and receive an ID. Thereafter they are considered customers. Therefore we would not use anonymous logon. Furthermore, the customer's ID and password are stored in a database. We can therefore validate the customer's logon credentials against the information stored in the database.

Incorrect Answers:

B: We would use SSL to secure the website. We would however not use anonymous logon for existing customers because, according to the Marketing Director, when people first view the Just Togs Web site, they are considered visitors until they enter their name and address and receive an ID. Thereafter they are considered customers. We would also not use the Challenge Handshake Authentication Protocol (CHAP). CHAP sends the password and a challenge from the server through a hashing algorithm. The recipient identifies the user, obtains the password from the directory, and performs the same hashing algorithm against the challenge and password. If the results match, the user is authenticated. CHAP authentication requires that the user's password be stored in plaintext or in reversibly encrypted format at the domain controller for comparison purposes. When this attribute is set, the storage of the plaintext password format doesn't take place until the user changes the password after the attribute is enabled. In this scenario the logon credentials of the customers are stored in a database and not in plain text or on the domain controller.

C: We would use SSL to secure the website and NTLM for logon purposes. We would however not use the Challenge Handshake Authentication Protocol (CHAP). CHAP sends the password and a challenge from the server through a hashing algorithm. The recipient identifies the user, obtains the password from the directory, and performs the same hashing algorithm against the challenge and password. If the results match, the user is authenticated. CHAP authentication requires that the user's password be stored in plaintext or in reversibly encrypted format at the domain controller for comparison purposes. When this attribute is set, the storage of the plaintext password format doesn't take place until the user changes the password after the attribute is enabled. In this scenario the logon credentials of the customers are stored in a database and not on in plain text or the domain controller.

D: We would use SSL to secure the website and NTLM We would however not use anonymous logon for existing customers because, according to the Marketing Director, when people first view the Just Togs Web site, they are considered visitors until they enter their name and address and receive an ID. Thereafter they are considered customers. Furthermore, we would use database validation to validate the customer’s credentials as the customer’s ID and password are stored in a database. We can therefore validate the customer’s logon credentials against the information stored in the database

Q. 5
How should you authenticate visitors to the Web site?

A. Authenticate visitors to an anonymous account
B. Authenticate visitors by requiring them to enter their user ID and password
C. Authenticate visitors by using cookies
D. Authenticate visitors that place an order as new or existing customers

Answer: A
Explanation:
According to the Marketing Director, when people first view the Just Togs Web site, they are considered visitors. After they enter their name and address and receive an ID they are considered customers. In other words new visitors to the Just Togs Web site would not have user credentials which Just Togs can use to authenticate them. Therefore we should allow anonymous access to the web site.

Incorrect Answers:

B: We cannot authenticate new visitors by requiring them to enter their user ID and password as they would not have these credentials.

C: A company with a Web site could monitor a person's use and activities while on that site. Web sites store the information on the visitor’s computers in a cookies.txt file. This information indicates that the visitor had been at the site before and may also have an indication of what the visitor’s interests are as determined by what they have looked at previously. Cookies do not contain logon information unless the visitor had voluntarily registered at the site before. However, these are new visitors that may not have been to the Web site before or may be previous visitors who had not yet registered with the Web site. We therefore cannot authenticate users by using cookies. Cookies would also not be the preferred means of authenticating existing customers as cookies are related to the visitor’s computer and not to the specific visitor.

D: According to the Marketing Director, visitors must first acquire a user ID and password, in other words they must first register with Just Togs before they can place orders.

Q. 6
Which technology should you use to securely connect the retail stores to headquarters?

A. MS-CHAP
B. IPSec
C. EAP-TLS
D. PPTP
E. L2TP

Answer: D
Explanation:
Just Togs wants to eliminate its remote access server and allow the retail stores to submit their data over the Internet through a VNP. In addition Just Togs will be setting up a DMZ. In addition to deploying a firewall between the public network and the the company’s network that the public can gain access to, which is also called an extranet, many companies also place a firewall between the company’s private network and their etranet to ensure the protection of the private network if the external firewall or resources in the extranet are compromised. This configuration is referred to as a Demilitarized Zone (DMZ), perimeter network, or screened subnet. PPTP is supported by Windows 95, Windows 98, Windows NT 4.0, and Windows 2000 remote access clients. PPTP uses MPPE to provide encryption of the transmitted data. MPPE can use 40-bit, 56-bit, or 128-bit encryption keys. However, we must configure the firewall to allow the PPTP packets to pass through the firewall.

Incorrect Answers:

A: Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). MS-CHAP increases security by dropping the requirement to store the user's password in a plaintext format at the domain controller. MS-CHAP creates the challenge response by passing the challenge and the user's password through the Message Digest v4 (MD4) hashing algorithm rather than the MD5 algorithm. Because the algorithm is well known, MS-CHAP is also vulnerable to dictionary attacks if short passwords or passwords that are found in a dictionary are used. MS-CHAP uses Microsoft Point-to-Point Encryption (MPPE) Protocol to encrypt all data transmitted between the remote access client and the Network Access Server (NAS).

B: IPSec tunnel mode uses Encapsulated Security Payloads (ESPs) to encrypt all traffic passing between the VPN tunnel endpoints. The original IP packets are encrypted within the IPSec tunnel mode packet as they are transmitted across the unsecured network. The data is decrypted when it reaches the endpoint nearest the destination computer. We can use IPSec tunnel mode as a VPN solution if we need to provide secure interoffice connectivity with third-party firewalls, routers or gateways that do not support L2TP/IPSec or PPTP VPN tunneling technology. However, IPSec does not provide user authentication, it only provides machine authentication. It therefore only supports network-to-network connectivity and does not support client-to-network VPN access..

C: Extensible Authentication Protocol (EAP) provides two-factor authentication by using devices such as smart cards to provide network credentials. It uses Transport Layer Security (TLS) to secure the authentication process. However, EAP requires that both the remote access client and the NAS run Windows 2000 and that a Public Key Infrastructure (PKI) is deployed to provide certificates for both the Network Access Server and the remote access clients. In this scenario the Retail Stores will retain their Windows NT 4.0 Windows NT 4.0ver computers. We therefore cannot use EAP to connect the connect the retail stores to headquarters.

E: L2TP can provide both client-to-server and server-to-server access. However, L2TP does not include an encryption mechanism and therefore requires IPSec to negotiate a security association between the two computers using the L2TP tunnel. Furthermore, L2TP cannot pass through a firewall.

Q. 7

Which authentication protocol should you use to secure the VPN connection from the retail stores to headquarters?

A. EAP
B. PAP
C. SPAP
D. MS-CHAP

Answer: D

Explanation:

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) does not require that the user's password be store in a plaintext format on the domain controller. Instead MS-CHAP creates the challenge response by passing the challenge and the user's password through the Message Digest v4 (MD4) hashing algorithm. This algorithm is, however, well known and is vulnerable to dictionary attacks if short passwords or passwords that are found in a dictionary are used. MS-CHAP should therefore be used in conjuction with password complexity.

Incorrect Answers:

A: Extensible Authentication Protocol (EAP) provides two-factor authentication by using devices such as smartcards to provide network credentials. It uses Transport Layer Security (TLS) to secure the authentication process. However, EAP requires that both the remote access client and the NAS run Windows 2000 and that a Public Key Infrastructure (PKI) is deployed to provide certificates for both the Network Access Server and the remote access clients. In this scenario the Retail Stores will retain their

Windows NT 4.0 Windows NT 4.0ver computers. We therefore cannot use EAP to connect the connect the retail stores to headquarters.

B: Although Password Authentication Protocol (PAP) is supported by almost all dial-up network services and consequently offers the most flexibility among the authentication protocols. It is not the most secure as PAP sends the user password as plain text. Therefore PAP is not recommended for networks that require security.

C: Shiva Password Authentication Protocol (SPAP) uses a reversible encryption method supported by Shiva remote access servers and Windows 2000 remote access servers. The encryption algorithms are stronger than those used in PAP, but SPAP does not provide protection against server impersonation.

Q. 8
Which changes should the retail stores make to Support the VPN connection?

A. Configure the connection type to dial in to headquarters. Use L2TP over IPSec to communicate with the VPN server.

B. Configure the connection type to dial in to the ISP. Use L2TP over IPSec to communicate with the VPN server.

C. Configure the connection type to dial in to the ISP. Use PPTP to communicate with the VPN server.

D. Configure the connection type to dial in to headquarters. Use PPTP to communicate with the VPN server.

Answer: C
Explanation:
In this scenario the Retail Stores are currently configured to use the Remote Access Servers (RRAS) to access the network at Headquarters. The Remote Access Servers (RRAS) are to be eliminated and replaced by VPN. VPN differs from RRAS in that an existing IP connection, usually to an ISP, must exist before we can establish a VPN connection, which is a tunnel that runs over an existing network connection while RRAS uses a modem to dial into the server itself. We must therefore configure the computers at the retail stores to dial-up to an ISP. In addition, Just Togs will be implementing a DMZ, which is a firewall that is placed between the private network and the extranet. We therefore require a secure connection that can pass through a firewall. PPTP, which is supported by Windows NT 4.0, and Windows 2000 remote access clients, uses MPPE to provide encryption of the transmitted data and can pass packets through the firewall.

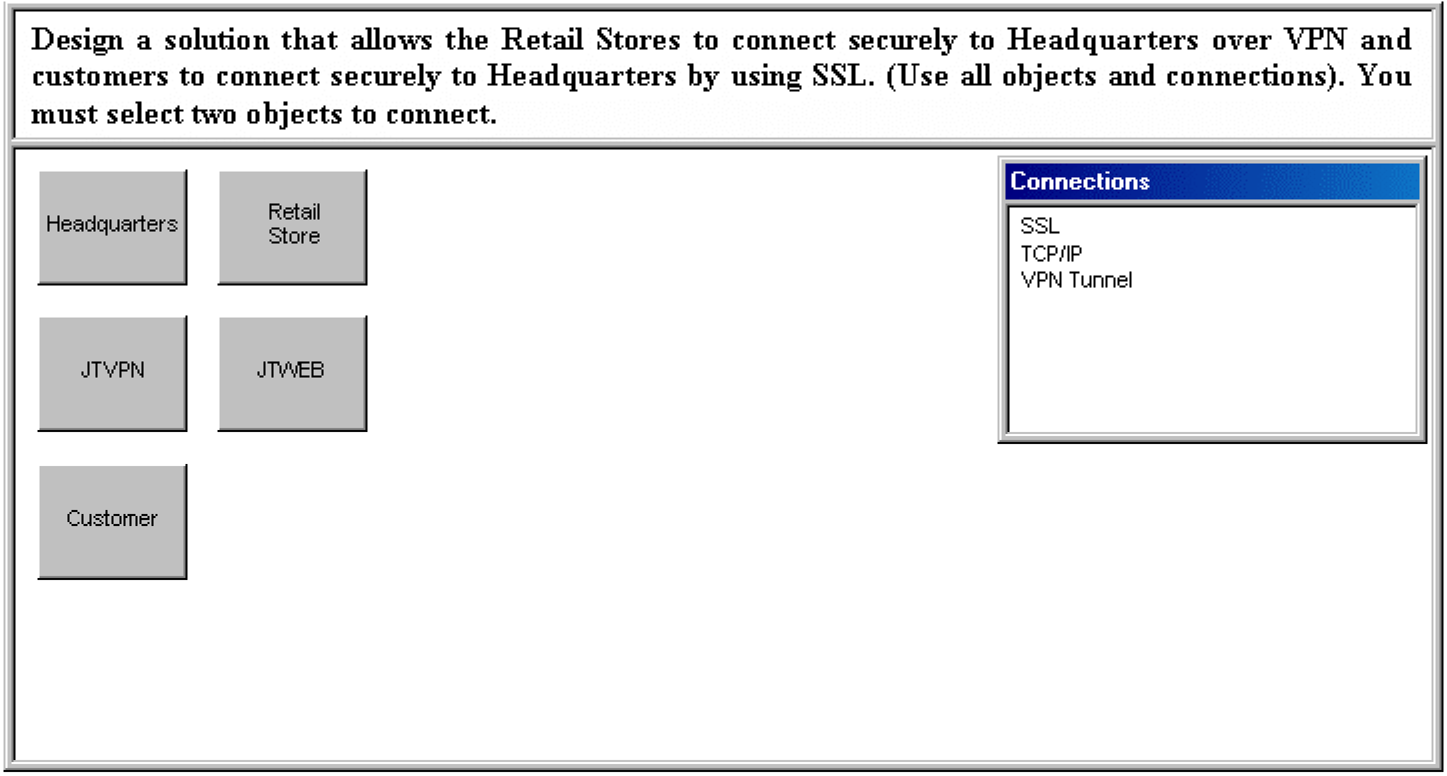
Incorrect Answers:

A: A VNP requires the presence of an existing IP connection exist before we can establish a VPN connection, which is a tunnel that runs over an existing network connection. VNP is not used to dial-up directly to the host server. Instead it tunnels through an existing IP network, such as the Internet. This method is used to reduce the cost of creating the connection as it allows us to dial up to a local ISP and connect to the server at Headquarters through the Internet, thus replacing long distance phone calls from remote Retail Stores. Furthermore, Just Togs will be setting up a DMZ, which is a firewall that is placed between the private network and the extranet. L2TP however cannot be used to transmit network traffic through a firewall. We should thus use PPTP instead.

B: A VNP requires the presence of an existing IP connection exist before we can establish a VPN connection, which is a tunnel that runs over an existing public network such as the Internet. We would therefore need to dial-up to an ISP before we can establish a VPN. However, Just Togs will be setting up a DMZ, which is a firewall that is placed between the private network and the extranet. L2TP cannot be used to transmit network traffic through a firewall. We should thus use PPTP instead.

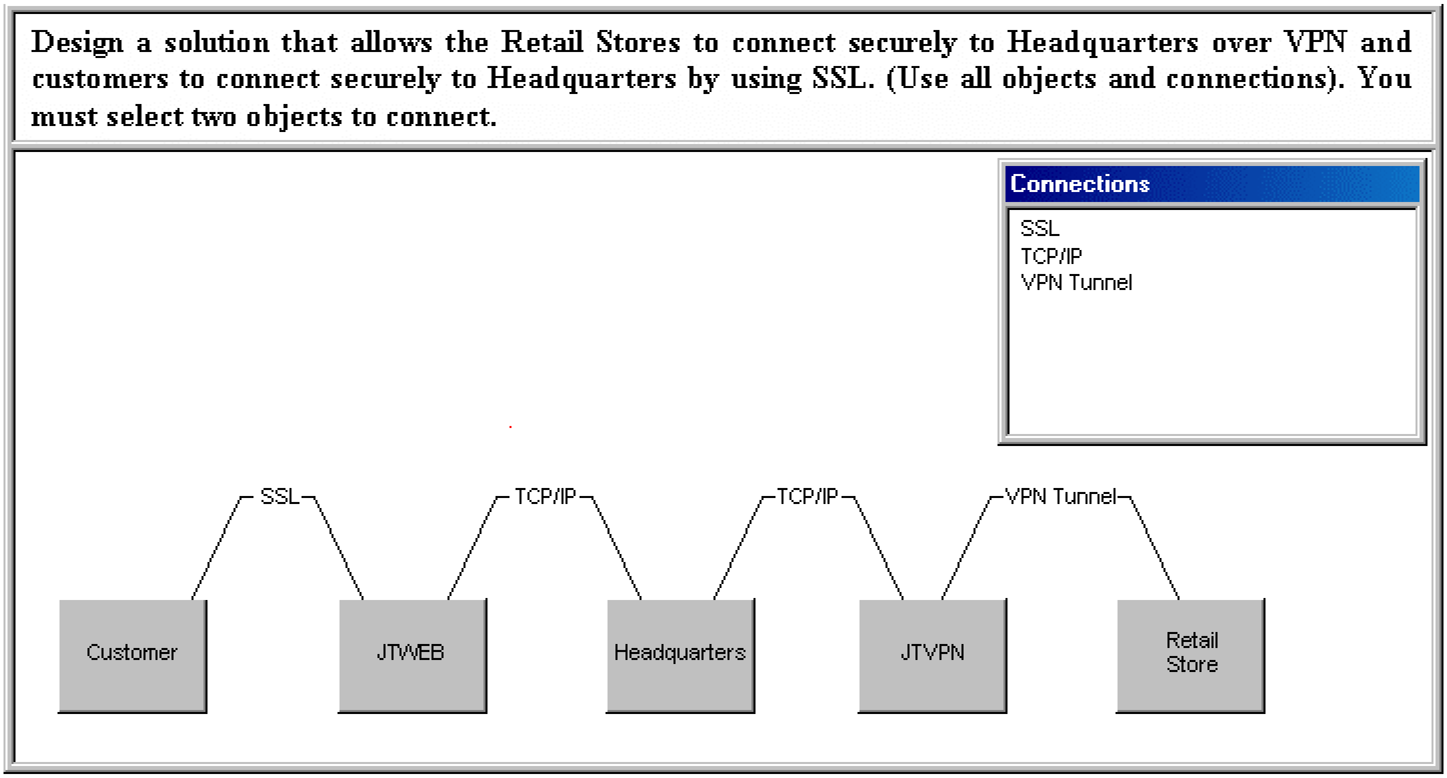
D: A VNP requires the presence of an existing IP connection exist before we can establish a VPN connection, which is a tunnel that runs over an existing network connection. VNP is not used to dial-up directly to the host server. Instead it tunnels through an existing IP network, such as the Internet. This method is used to reduce the cost of creating the connection as it allows us to dial up to a local ISP and connect to the server at Headquarters through the Internet, thus replacing long distance phone calls from remote Retail Stores. Just Togs will be implementing a DMZ, which is a firewall that is placed between the private network and the extranet. We therefore require the use of PPTP, which is supported by Windows NT 4.0 computers used in the retail stores, and can pass network packets through the firewall.

Q. 9



Design a solution that allows the Retail Stores to connect securely to Headquarters over VPN and customers to connect securely to Headquarters by using SSL. (Use all objects and connections). You must select two objects to connect.

Answer:



Design a solution that allows the Retail Stores to connect securely to Headquarters over VPN and customers to connect securely to Headquarters by using SSL. (Use all objects and connections). You must select two objects to connect.

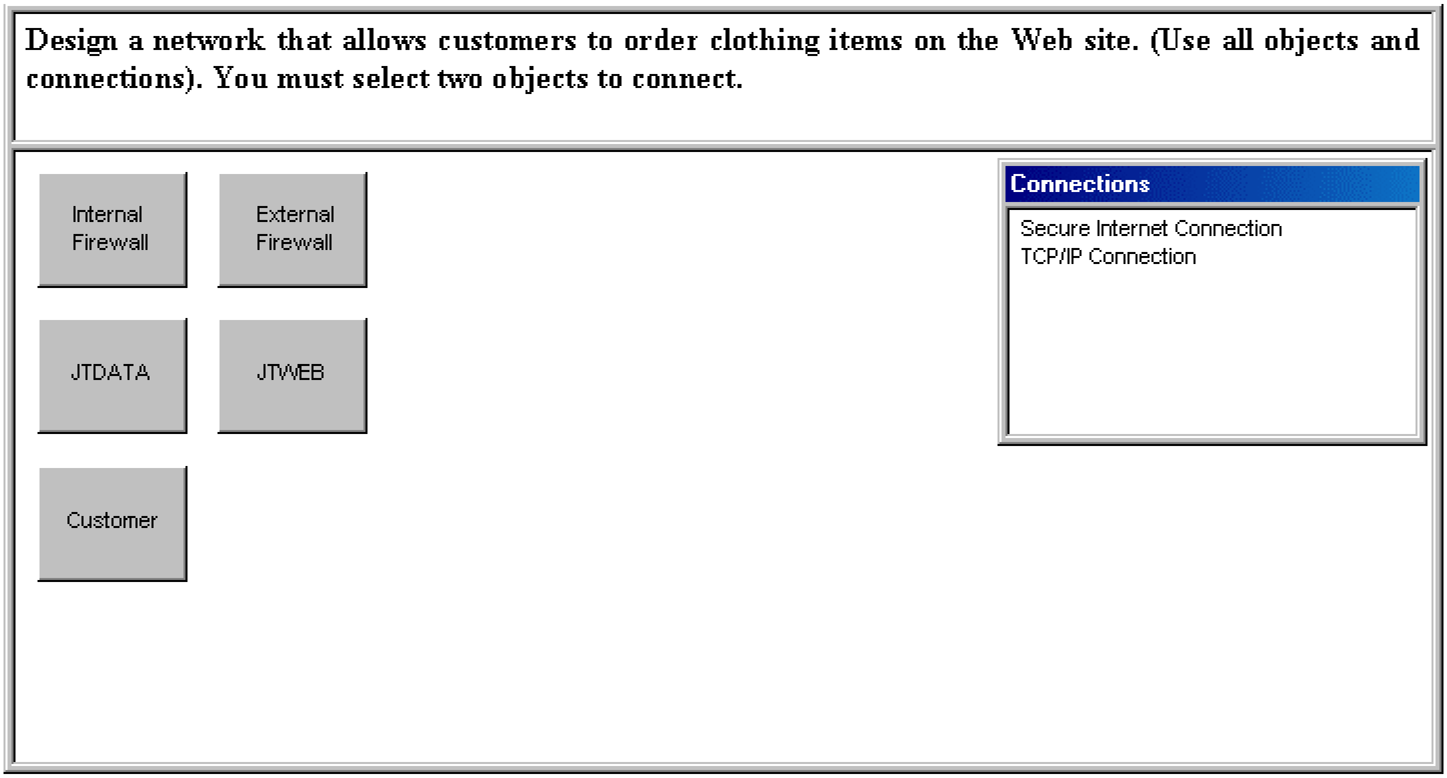
Explanation:
We need to secure network communication between customers and the Just Togs Web site which is hosted on the JTWEB server. This network communication is across the Internet therefore we should use SSL to secure this communication.

The JTWEB server is a server located in the domain at Headquarters. There would therefore be a trust relation between JTWEB and the Domain Controllers at Headquarters. Consequently, we only require the TCP/IP connection within the domain.

Just Togs will be eliminating the Remote Access Server at Headquarters and will replace it with a VPN server named JTVPN. The Retail Stores will then connect to Headquarters via a VPN Tunnel.

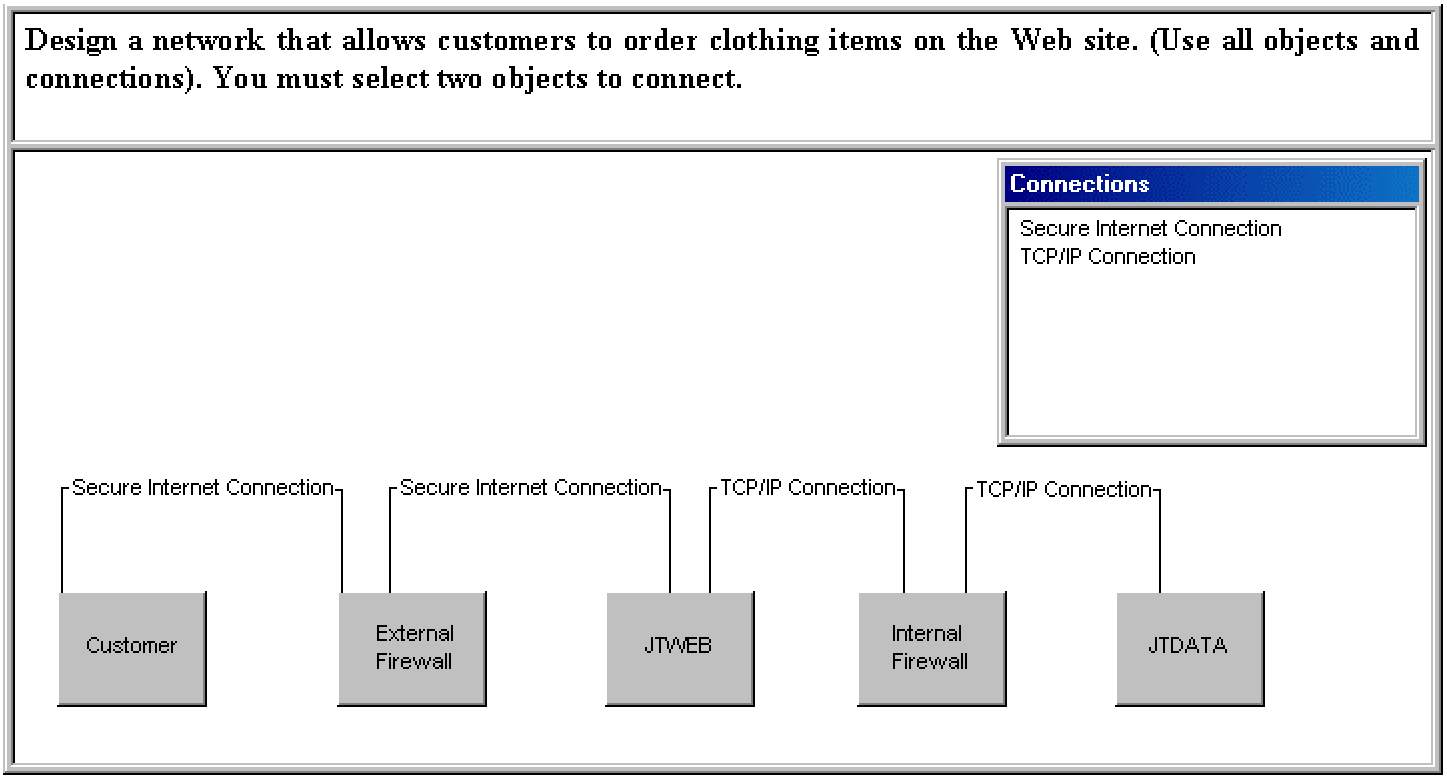
The JTVPN server is also a server located in the domain at Headquarters. There would therefore be a trust relation between JTVPN and the Domain Controllers at Headquarters. Consequently, we only require the TCP/IP connection within the domain.

Q. 10



Design a network that allows customers to order clothing items on the Web site. (Use all objects and connections). You must select two objects to connect.

Answer:



Design a network that allows customers to order clothing items on the Web site. (Use all objects and connections). You must select two objects to connect.

Explanation:
We need to secure network communication between customers and the Just Togs Web site which is hosted on the JTWEB server. This network communication is across the Internet and must pass through an external firewall. We would therefore use SSL to secure this communication between the Customers and the JTWEB server through the External Firewall.

JTWEB is part of the Just Togs extranet. In other words it is part of the Just Togs network that the public has access to. Just Togs wants to set up a DMZ. A DMZ is a firewall that is placed between the extranet, JTWEB in this scenario, and the private network. Although customers require access to the JTDATA server, which holds the Just Togs database, we would want to place JTDATA in the private network to reduce its vulnerability should the external firewall be compromized. Therefore the Internal Firewall will be placed between JTWEB and JTDATA. JTWEB and JTDATA are part of the same domain and are not connected via the Internet. We would therefore connect these servers via TCP/IP

Case Study No: 2

HIABUV TOYS

Background:

Hiabuv Toys is an electronic toys retailer that owns and operates retail stores throughout the United States. Hiabuv Toys buys popular electronic toys directly from manufacturers in bulk quantities and resells these products to the public at discounted rates.

Organization:

Headquarters:

Hiabuv Toys headquarters are located in Minneapolis, Minnesota. Headquarters includes the sales and marketing, IT, legal, accounting, Human Resources, and executive departments. It employs 4,500 people. The annual growth rate of employees at headquarters is 20 percent.

Retail Stores:

Hiabuv Toys has retail stores in 350 locations around the United States. Each retail store employs 50 to 100 people, Hiabuv Toys is scheduled to open 50 retail stores each year. The company plans to open a retail store in Casablanca, Morocco.

Service Centers:

Hiabuv Toys has service centers in 15 locations around the United States. Each service center employs 100 service center technicians and five managers..

Existing IT Environment:

WAN Connectivity:

All stores and service centers are connected to headquarters by 128-Kbps lines. This connection is backed by a 56-Kbps dial-up connection.

LAN Connectivity:

All headquarters buildings are connected by T1 lines.

Computers:
There are 4,500 Windows NT Workstation computers, and 150 Windows NT Server computers located at headquarters. The Servers are used as application servers and file servers. One server named SALES1 is used as a backup domain controller. It runs Internet Information Services (IIS), and is in the SALES domain. Only domain controllers and applications have shared resources.

Human Resources has a server named HR1. All connections to this server must be encrypted.

Each store has 30 Windows 2000 Professional computers and two Windows NT Server computers. One for a primary domain controller for the local domain, and the other is a backup domain controller.

Each service center has 30 Windows 2000 Professional computers and one Windows NT Server, which is a backup domain controller.

Network:
The company's Internet domain is named hiabuvtoys.com. On the internal network, the private IP address is 172.16.0.0. All computers use TCP/IP. At headquarters, the Windows NT Servers use static addresses and the Windows NT Workstations use DHCP.

Static addresses are used for all retail stores, and service center computers.

Envisioned IT Environment:

WAN Connectivity:
The Casablanca retail store will have a LAN with a 64-Kbps Internet connection and a 64-Kbps connection to headquarters.

LAN Connectivity:
The LAN bandwidth will remain the same.

Computers:
The company will upgrade to a Windows 2000 network with one Active Directory tree and two domains sharing the same namespace. Hiabuv Toys wants to design a directory service that allows for some autonomy, and wants to ensure that business units can be added, removed, or changed without undue overhead. The SALES1 server will not be upgraded. It will be replaced with a Windows 2000 Server after all other computers are upgraded to Windows 2000. After this server is replaced, the network will run in native mode. The legal department will have its own Windows 2000 Server named LEGAL1. The department will implement a secure private network between LEGAL1 and HR1.

Network:

The physical network will not change. The company wants to create one account domain for headquarters, and one account domain for its retail stores. The Casablanca retail store will have a help desk employee located on-site to perform end-user application support and to resolve hardware issues.

Security:

Authorized remote users should be able to access shared resources at headquarters through secure tunneling. Confidential documents should be sent internally in a secure manner. Hiabuv needs to accept transmission of confidential information from manufacturers in a fast, easy, and reliable manner. No training should be required. The company wants to implement a Public Key Infrastructure (PKI).

Network Roles and Usage:

Information Technology:

The IT department administers user and computer accounts for the company. Strong passwords are not implemented. Users at headquarters have access to e-mail and the Internet. The IT department is divided into three groups: the WAN group, the LAN group, and the Internet group. The LAN group manages user accounts, oversees the LAN, the Windows 2000 Servers and domains and the retail store servers. The WAN group oversees the WAN. The Internet group oversees Internet security and connectivity. Each group has a different manager. Communication and agreement among the groups is poor. The Internet group wants autonomy within the Active Directory.

Sales and Marketing:

The sales and marketing department uses the network to exchange e-mail and download information from manufacturer and competitor Web sites. It works with more than 1,000 manufacturers. The department needs to receive information from new manufacturers and to verify their authenticity securely. The sales and marketing department needs to access the retail stores for sales history information. They require color printing, and depend on portable computers to access information regardless of their location.

Legal:

The legal department needs to copy confidential documents to shard folders for the Human Resources department, the executive department, and the company's law firm.

Retail Stores:

The cash registers run Windows NT Workstation. Cash registers boot with a generic logon for cashier access. The cash registers do not contain any data. Store managers have Windows 2000 Professional desktop computers, with e-mail and unlimited Internet access. Each store also has five secured Windows NT

Workstation computers for employees to browse pre-approved Inter-net Web sites. Each store has three public kiosks. Customers can use kiosks to register for gifts or place orders. The kiosks automatically boot with and authenticate to a secured generic account.

Service Centers:

Each center uses unique logon names for access to the network. Each center technician has access to e-mail and the Internet.

Questions Hiabuv Toys

Q. 1
Which security requirement will affect design of the Windows 2000 forest?

A. Implementation of Kerberos authentication
B. Secure transactions at Store Registers
C. Organization of user accounts
D. Secure communication between legal and HR.

Answer: C
Explanation:
A forest is a collection of domains that share a common schema, configuration, and global catalog. All domains in a forest are connected using transitive trust relationships. In this scenario the forest will consist of a single tree that comprises two domains: one for headquarters and the other for the Retail Stores. Furthermore, Hiabuv Toys opens 50 new stores each year. Each store employs 50 – 100 people. We would thus have to design a forest that makes allowance for the expansion in terms of new user accounts for the additional staff employed at the Retail Stores that are opened each year.

Incorrect Answers:
A: Kerberos is the default protocol for authentication in a Windows 2000 network environment. It is used pervasively in Windows 2000. In other words you do not need to install or initiate it. Kerberos authentication protocol allows a single logon to access all network resources. This allows a fast, single logon to network services within a domain and to services residing in trusted domains as Kerberos verifies both the identity of the user and of the network services, thus providing mutual authentication.
B: Security at the Store Registers is adequate. The cash registers boot with a generic logon for cashier access and do not contain any data. Store managers have Windows 2000 Professional desktop computers, with e-mail and unlimited Internet access. Each store also has five secured Windows NT Workstation computers for employees to browse pre-approved Inter-net Web sites. Each store has three public kiosks. Customers can use kiosks to register for gifts or place orders. The kiosks automatically boot with and authenticate to a secured generic account.
D: In the envisioned IT environment, the legal department will have its own Windows 2000 Server named LEGAL1. The department will implement a secure private network between LEGAL1 and HR1. There would thus be a secure private connection between two servers and would not have an impact on the design of the forest.

Q. 2

Which server or servers provide the least security for user access?

A. Retail store servers
B. Service centers servers
C. SALES1
D. HR1
E. LEGAL1

Answer: C
Explantion:
SALES1 is the least secure server. It is a Windows NT 4.0 server machine that is used as a backup domain controller (BDC). A BDC is used for logon authentication. SALES1 also runs Internet Information Services (IIS) and will not be upgraded. Thus SALES1, which can be used for logon authentication, is connected to the Internet. It is thus vulnerable to attacks on the internet as are logon authentication requests that pass across the Internet.

Incorrect Answers:
A: In the existing network, the Retail Stores have two Windows NT Server computers. One is a Primary Domain Controller for the local domain, and the other is a Backup Domain Controller. Addition the store managers have Windows 2000 Professional desktop computers, with e-mail and unlimited Internet access; and each store has five secured Windows NT Workstation computers for employees to browse pre-approved Internet Web sites. The servers at the Retail Stores are thus not connected to the Internet. Furthermore, these servers will be upgraded to Windows 2000 servers.
B: Each service center has 30 Windows 2000 Professional computers and one Windows NT Server, which is a backup domain controller. Unlike SALES1, the Server Centers' BDCs are not used to access the internet. In addition these servers will be upgraded to Windows 2000 servers.
D: The Human Resources department has a server named HR1 that is located in the domain at Headquarters. All connections to this server will be encrypted.
E: In this scenario the legal department needs to copy confidential documents to shard folders for the Human Resources department, the executive department, and the company's law firm. The legal department will have its own Windows 2000 Server named LEGAL1 and will implement a secure private network between LEGAL1 and HR1.

Q. 3
How should you secure the new servers at the Casablanca store?

A. Install the serves into a new OU and implement Group Policies at the Site Level
B. Install the serves into a new OU and implement Group Policies at the OU Level
C. Install the servers into their own Active Directory tree and implement Group Policies at the Domain Level

D. Install the servers into the same Active Directory tree as stores and modify the schema

Answer: B

In Windows 2000 network, Group Policies can be applied at the Site level, the Domain level, and the Organizational Unit (OU) level. Group Policy precedence follows the Group Policy model and is applied hierarchically from the least restrictive object, i.e. the Site, to the most restrictive object, i.e. the OU. In other words Windows 2000 applies Group Policies that are linked to sites first, then Group Policies that are linked to domains, and then Group Policies that are linked to OU. Thus, the Group Policy settings of the OU of which a user or computer is a member are the final Group Policy settings that are applied and will override the Group Policy settings linked to the Site or Domain where these are in conflict wit the settings in the Group Policy linked to the OU. We would therefore secure the new servers at the Casablanca store by organizing them into a new OU. We configure the security settings for these servers in a Group Policy and link that Group Policy to the new OU.

Incorrect Answers:

A: Windows 2000 applies Group Policies that are linked to sites first, then Group Policies that are linked to domains, and then Group Policies that are linked to OU. Thus, the Group Policy settings of the OU of which a user or computer is a member are the final Group Policy settings that are applied and will override the Group Policy settings linked to the Site or Domain where these are in conflict wit the settings in the Group Policy linked to the OU. We would therefore secure the new servers at the Casablanca store by organizing them into a new OU. We configure the security settings for these servers in a Group Policy and link that Group Policy to the new OU. We would not link the Group Policy at the Site level as these may be overwritten by Group Policy settings linked to the OU level.

C: Hiabuv Toys wants to upgrade to a Windows 2000 network with one Active Directory tree and two domains sharing the same namespace. The company wants to create one account domain for headquarters, and one account domain for its retail stores. We therefore will not be able to create another tree for the servers at the Casablanca store.

D: Hiabuv Toys wants to upgrade to a Windows 2000 network with one Active Directory tree and two domains sharing the same namespace. The company wants to create one account domain for headquarters, and one account domain for its retail stores. We therefore will not be able to create another tree for the servers at the Casablanca store. Furthermore, a forest is a collection of domains that share a common schema, configuration, and global catalog. Thus by editing the schema, the Casablanca tree would no longer be part of the same Forest.

Q. 4

Which strategy should you use to accommodate the new Casablanca store?

A. Place the Help Desk employee in the Domain Admins group.
B. Place the Help Desk employee in the Enterprise Admins group.
C. Delegate authority to the Help Desk employee to manage client computers.

D. Delegate authority to the Help Desk employee to modify user accounts and groups

Answer: D
Explanation:
Hiabuv Toys wants to implement a network that consists of a single-tree forest that comprises two domains: one for the Retail Stores and one for headquarters. The Casablanca retail store will have a Help Desk employee located on-site to perform end-user application support and to resolve hardware issues. These can be accomplished if the Help Desk Employee has been delegated the authority to modify user accounts and groups.

Incorrect Answers:
A: Members of the Domain Admins group can administer the entire domain in which they are defined. In this scenario, Hiabuv Toys wants to implement a network that consists of a single-tree forest that comprises two domains: one for the Retail Stores and one for headquarters. Thus by placing the Help Desk employee in the Domain Admins group we would give them the rights to access and control all objects in the Retail Stores' domain. For security reasons this is not desirable.
B: Members of the Enterprise Admins group have forest-wide administrative scope and are able to modify Enterprise-wide configuration. Thus by placing the Help Desk employee in the Enterprise Admins group we would give them the rights to access and control all objects in the entire forest. For security reasons this is not desirable.
C: The Help Desk employee at the Casablanca store will be required to perform end-user application support and to resolve hardware issues. That employee would thus have to modify user accounts so as to give the appropriate users in the Casablanca store the right to use appropriate applications. These settings pertain to the user and not the computer. Therefore the Help Desk employee should be granted the authority to modify user accounts and groups and not rather than the authority to manage client computers.

Q. 5
Which security method should you implement to provide data security between LEGAL1 and HR1?

A. Group Policies for shared folders
B. IPSec with ESP
C. IPSec with AH
D. EFS

Answer: B
Explanation:
We need to ensure that all network communication to the HR1 server is encrypted. This applies to the LEGAL1 server as well. We thus require a mechanism that provides encryption, confidentiality, data authentication, integrity, and anti-replay to IP packets. For this we can use IPSec with ESP Windows 2000 incorporates

Internet Protocol security (IPSec) for data protection of network traffic. IPSec provides end-to-end security, meaning that the IP packets are encrypted by the sending computer, are unreadable en route, and can be decrypted only by the recipient computer. To provide confidentiality, data authentication, integrity, and anti-replay we can use Encapsulating Security Payload (ESP). This protects the IP data payload.

Incorrect Answers:

A: For encryption we can use Internet Protocol security (IPSec) which Windows 2000 incorporates for data protection of network traffic. IPSec provides end-to-end security, meaning that the IP packets are encrypted by the sending computer, are unreadable en route, and can be decrypted only by the recipient computer. However, Authentication Header (AH) only provides authentication and integrity services to transmitted data.

C: Authentication Header (AH) provides authentication, integrity, and anti-replay for the entire IP packet, i.e. for both the IP header and the data payload carried in the packet. It however does not encrypt the data and thus does not provide confidentiality. In other words the data is readable, but protected from modification. For encryption we should use IPSec with ESP.

D: Encypting File System (EFS) is a new feature that has been introduced with Windows 2000 and can be used to encrypt files and folders on NTFS volumes. When a user encrypts a file, only that user will be able to use the file. This means that encrypted files cannot be accessed by another user and cannot be shared.

Q. 6

Which security solution should you implement to allow the service centers to communicate with manufactures?

A. Dfs with Crypto API
B. IPSec
C. Secure DNS
D. Secure Email

Answer: D

Explanation:

The Service Centers have access to the Internet and to e-mail. Both of which can be used to communicate with the manufacturers. The only mechanism to secure Internet communication is IPSec. This however requires a connection between two computers over the Internet. In other words it requires a RRAS or VPN, neither of which is available. Te only other option then is to secure email communication.

Incorrect Answers:

A: Distributed File System (Dfs) is a service that layers on top of the Workstation service to connect file shares into a single namespace even though the file shares can reside on different computers. Because

Dfs allows us to organizing file servers and their shares into a logical hierarchy, it makes it easier to manage and use information resources. Dfs functionality is integrated with Active Directory; the Dfs topology is published to Active Directory. Because changes to a domain-based Dfs topology are automatically synchronized with Active Directory, we can restore a Dfs topology if the Dfs root is unavailable. Dfs must however reside in the same domain namespace. The manufacturers will not share the same domain namespace with the Service Centers. Therefore we cannot use Dfs. Furthermore, CryptoAPI allow s applications to encrypt or digitally sign data in a flexible manner while providing protection for private keys. The Service Centers will however not use applications to communicate with manufacturers.

B: Windows 2000 uses IPSec for data protection of network traffic between two computers over an insecure network. To use this suite of protocols we must establish a connection between the two computers. This can either be a RRAS connection or a VPN connection. In this scenario there are no such connections between the Service Centers and the manufacturers. Instead Service Centers only have access to the Internet and to e-mail.

C: DNS is used for name resolution. In other words it resolves domain and computer names to IP address and IP addresses to computer names. It is not used for communication purposes. Furthermore, there is no Secure DNS, only secure dynamic DNS updates.

Q. 7
How should you design Windows 2000 domain and OU structure for HIABUV TOYS?

A. Create two accounts domains, and migrate all resource domains into OUs under the Headquarters domain.
B. Create two accounts domains, and migrate all resource domains into OUs under the Retail Store Domain.
C. Create two accounts domains, and migrate existing Retail Stores resource domain into OUs under the Retail Store domain.
D. Create two accounts domains, and migrate existing Retail Stores resource domain into OUs under the Headquarters domain.

Answer: C
Explanation:
In this scenario we are required to create a network that is a single-tree forest. This forest will consist of two accounts domains. One accounts domain for Headquarters and one for the Retail Stores. We should thus organize the existing Retail Stores resource domains into OUs and place them under the Store Domain. This will allow us to link Group Policies that are applicable to all the Retail Stores.

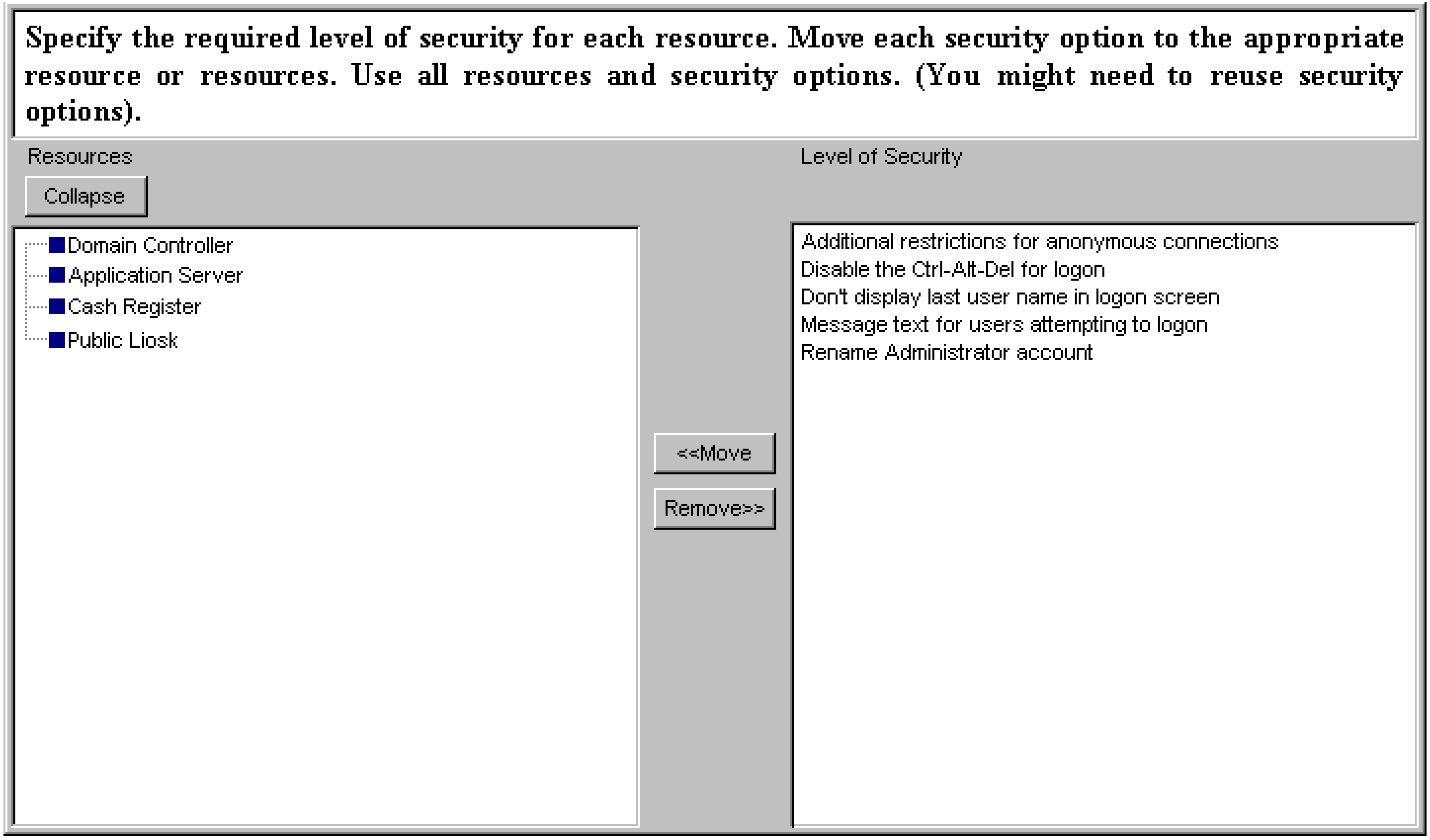
Incorrect Answers:

A: By placing all of the resource domains into OUs located under the Headquarters domain, we would not be able to link Group Policies that are applicable to the Retail Stores and not Headquarters at the domain level. It will also make the Retail Stores account domain redundant.

B: We would not want to place all resource domains into OUs under the Retail Stores domain as this will not allow us to link Group Policies to the Headquarters domain. And would make the Headquarters account domain redundant.

D: We would not want to place the existing Retail Stores resource domains into OUs under the Headquarters domain as this will not allow us to delegate control over the Retail Stores resources to members of the Retail Stores domain.

Q. 8



Specify the required level of security for each resource. Move each security option to the appropriate resource or resources. Use all resources and security options. (You might need to reuse security options).

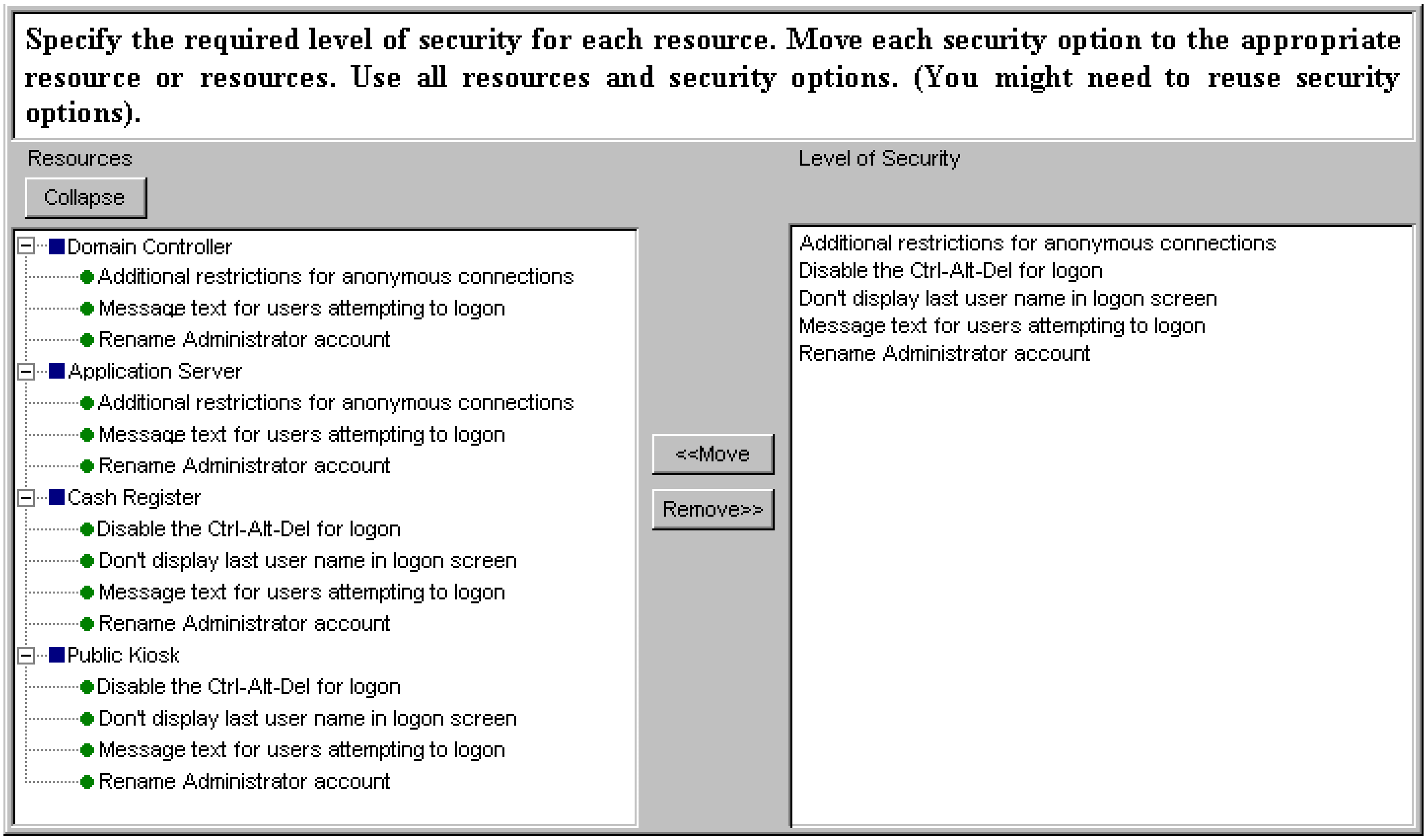
Resources

- Domain Controller
- Application Server
- Cash Register
- Public Liosk

Level of Security

- Additional restrictions for anonymous connections
- Disable the Ctrl-Alt-Del for logon
- Don't display last user name in logon screen
- Message text for users attempting to logon
- Rename Administrator account

Answer:



Specify the required level of security for each resource. Move each security option to the appropriate resource or resources. Use all resources and security options. (You might need to reuse security options).

Resources

- Domain Controller
  - Additional restrictions for anonymous connections
  - Message text for users attempting to logon
  - Rename Administrator account
- Application Server
  - Additional restrictions for anonymous connections
  - Message text for users attempting to logon
  - Rename Administrator account
- Cash Register
  - Disable the Ctrl-Alt-Del for logon
  - Don't display last user name in logon screen
  - Message text for users attempting to logon
  - Rename Administrator account
- Public Kiosk
  - Disable the Ctrl-Alt-Del for logon
  - Don't display last user name in logon screen
  - Message text for users attempting to logon
  - Rename Administrator account

Level of Security

Additional restrictions for anonymous connections
Disable the Ctrl-Alt-Del for logon
Don't display last user name in logon screen
Message text for users attempting to logon
Rename Administrator account

Explanation:
Domain Controllers are vital to the security of the network. It is responsible for all security-related interaction between the user and the domain interactions as well as the centralization of administration. We would thus want to restrict anonymous connections to the Domain Controller. To increase security we could use message texts for users attempting to logon and we should rename the Administrator account.

To secure the Application server we would want to restrict anonymous connections to the Server. We would also increase security by using message texts for users attempting to logon and we should rename the Administrator account.

To secure the Cash Registers we should disable Ctrl-Alt-Del for logon as the Cash Registers have generic logon accounts. We should also configure the Cash Registers not to show the last user name in the login screen. In addition we could use message texts for users attempting to logon and we should rename the Administrator account. We should apply the same settings to the Public Kiosks.

Case Study No: 3

HANSON BROTHERS

Background

Hanson Brothers is a medical supply company. The headquarters are located in Chicago, Illinois. There are more than 1,000 employees at the headquarters location. Hanson Brothers sells and distributes medical supplies to large hospitals in 23 states.

The company has distribution centers in Boston, Massachusetts; Dallas, Texas; Miami, Florida; Minneapolis, Minnesota; New Orleans, Louisiana; Tampa, Florida; Seattle, Washington; and St Louis, Missouri.

Business Process:

Sales Representatives:

More than 200 of the company's employees are sales representatives. Sales representatives visit their existing customers at least once per week. During the visit, the sales representative receives a weekly supply order from the purchasing manager at the hospital. The sales representative then goes to the hospital warehouse, where the supplies are located. The sales representative checks each supply at the warehouse and fills out a paper order form for the supplies that need to be replenished. The sales representative then faxes the order form to the nearest distribution center.

Distribution Centers:

After receiving a faxed order from the sales representative, a clerk at the distribution center enters the order into the mainframe computer. The order is then filled and delivered to the hospital. The entire process from the time the sales representative visits the hospital until the supplies are delivered takes approximately three days.

Employees from each distribution center deliver supplies only within their region. Each distribution center has sales representatives who also check and order supplies within the same region. Sales representatives do not work for multiple distribution centers.

Customer Service:

Sales representatives must call the customer service department at the distribution center to request the status of an order. Sales representatives also call to request the availability of an item. Sales representatives use toll-free numbers to place phone calls and send faxes to Hanson Brothers. Eight customer service employees answer order status and availability questions.

Existing IT Environment:

Computers:

Hanson Brothers has one mainframe computer, which is located at headquarters. There are 250 computer terminals at headquarters connected to the mainframe computer. There are 10 computer terminals at each distribution center.

WAN Connectivity:

A T1 line connects the computer terminals at the distribution centers to the mainframe computer.

Envisioned IT Environment:

Computers:

The mainframe computer at headquarters will be replaced with Windows 2000 Server computers, which will function as domain controllers. Headquarters will also set up a VPN server.

All sales representatives will use their own portable computers, and they will be able to load personal programs onto their computers. The portable computers will run Windows 2000 Professional. The portable computers will contain a program named Salesforce, which will be used to order supplies. The portable computers will also contain customer information. This information must be encrypted and recoverable. A Sales Representative group will be created for resource access.

The IT manager must be aware of attempted unauthorized access to the new network.

Distribution Centers:

All computer terminals at the distribution centers will be replaced with desktop computers running Windows 2000 Professional. Each distribution center will have a domain controller that runs Routing and Remote Access. Each distribution center will be its own organizational unit (OU). Each distribution center will have an IT administrator. This administrator will be able to add new users, add users to existing groups, modify existing group membership, and create computer accounts.

Each distribution center will have a folder for each hospital. Each hospital's folder will have two subfolders. One subfolder will contain the order status for the hospital, and the other subfolder will contain sales information. The sales information is confidential and will be used only by that hospital's sales representative. The sales representatives can add, delete, and change their hospital folders.

Customer Service:

Customer service should have the ability to read and modify orders for all hospitals.

Hospitals:
Hospitals should be able to view only their own order status. They will be connected to headquarters by using Routing and Remote Access. Hanson Brothers will supply each hospital with a computer. The hospital will supply the phone line. Each hospital will have a user account.

Problem Statement:

Marketing Manager:
Sales representatives are spending too much time servicing existing accounts. The sales representatives need a way to place orders quickly, which allow them to increase their number of accounts. The portable computers will allow sales representatives to visit each stockroom in the hospital instead of visiting a warehouse. The sales representatives will use Salesforce to enter the quantities of supplies in each location, and the program will report whether the supply should be ordered. If a supply is needed, an order will be created automatically. After all stockrooms have been checked, the sales representative will connect his or her computer to a phone line in the hospital, connect to the distribution center, and upload the batch of orders. The fulfillment process will not change.

When hospitals call their sales representative to request an order status, it can take up to one day for the sales representative to return the call. The sales representatives should be able to connect to the distribution center at any time to view the status of an order.

Sales representatives should also be able to connect to headquarters either by dialing directly to the remote access server or by dialing a local ISP and connecting through a VPN. Only sales representatives should be able to place an order. A verification process must be in place. Sales representatives should not be able to view other sales representatives' information.

IT Manager:
Phone costs are increasing dramatically. An average of 200 faxes are received per day. Fax transmissions can last up to five minutes each. Hanson Brothers receives an average of 300 phone calls per day requesting order status and item availability.

We will add a new distribution center in Pittsburgh, Pennsylvania. The new distribution center will have good Internet connectivity. Because of the high cost of a T1 line, this distribution center will be connected to headquarters through a VPN.

The Salesforce program is updated regularly with a disk containing software patches. A copy of the patch is sent on a floppy disk to each center. One person at each distribution center makes a copy of the disk for each of the sales representatives at that distribution center. The copy is distributed to the sales representatives at a monthly sales meeting. We have to make sure that the sales representative receives an unaltered copy of the patch. We have had some problems in the past with employees displaying inappropriate wallpaper on their computers. We need to restrict employees from changing the wallpaper on their computers.

Questions Hanson Brothers

Q. 1
What are the existing and envisioned IT administrative models for Hanson Brothers?

A. Existing centralized
Envisioned centralized
B. Existing centralized
Envisioned decentralized
C. Existing decentralized
Envisioned centralized
D. Existing decentralized
Envisioned decentralized

Answer: B
Explanation:
In the existing network consists of a mainframe/terminal model. There is one mainframe computer located at Headquarters to which the terminals connect. In other words the terminals do no processing, all processing is done at the mainframe. This model is thus centralized. In the envisioned IT environment, the mainframe computer will be replaced by Windows 2000 server computers. In addition each Distribution centre will have a Domain Controller and its own Organizational unit (OU). This model is decentralized.

Incorrect Answers:
A: In the existing network consists of a mainframe/terminal model. There is one mainframe computer located at Headquarters to which the terminals connect. In other words the terminals do no processing, all processing is done at the mainframe. Thus this model is indeed centralized. However, in the envisioned IT environment, the mainframe computer will be replaced by Windows 2000 server computers. In addition each Distribution centre will have a Domain Controller and its own Organizational unit (OU). This model is decentralized.
C: In the existing network consists of a mainframe/terminal model. There is one mainframe computer located at Headquarters to which the terminals connect. In other words the terminals do no processing, all processing is done at the mainframe. This model is thus centralized and not decentralized. Furthermore, in the envisioned IT environment, the mainframe computer will be replaced by Windows 2000 server computers. In addition each Distribution centre will have a Domain Controller and its own Organizational unit (OU). This model is decentralized.
D: In the existing network consists of a mainframe/terminal model. There is one mainframe computer located at Headquarters to which the terminals connect. In other words the terminals do no processing, all processing is done at the mainframe. This model is thus centralized. However, in the envisioned IT environment, the mainframe computer will be replaced by Windows 2000 server computers. In addition

each Distribution centre will have a Domain Controller and its own Organizational unit (OU). This model is thus decentralized.

Q. 2
How should hospitals connect to headquarters to view the status of their orders?

A. Use the VPN with Windows 2000 logon authentication
B. Use Routing and Remote Access with Windows 2000 logon authentication
C. Use the VPN with Remote Authentication Dial-In User Service (RADIUS) authentication.
D. Use Routing and Remote Access with Remote Authentication Dial-In User Service (RADIUS) authentication

Answer: B
Explanation:
In the envisioned IT environment, the hospitals should be able to view only their own order status. Hanson Brothers will supply each hospital with a computer with which the hospitals will connected to headquarters by using Routing and Remote Access (RRAS). In addition, each hospital will have a user account which will be authenticated and authorized when a user attempts to connect to a RRAS server. If RRAS is configured to use Windows authentication, Windows 2000 security verifies the username and password credentials for authentication while the dial-up properties of the user account, and locally stored remote access policies authorize the connection. Only if the connection attempt is both authenticated and authorized, the connection attempt is accepted. We would thus allow hospitals to connect to Headquarters via RRAS and would use Windows authentication.

Incorrect Answers:
A: In the envisioned IT environment, the hospitals should be able to view only their own order status. Hanson Brothers will supply each hospital with a computer with which the hospitals will connected to headquarters by using Routing and Remote Access (RRAS). Hanson Brother will not be setting up a VNP server for the hospitals.
C: In the envisioned IT environment, the hospitals should be able to view only their own order status. Hanson Brothers will supply each hospital with a computer with which the hospitals will connected to headquarters by using Routing and Remote Access (RRAS). Hanson Brother will not be setting up a VNP server for the hospitals. Furthermore, RADIUS allows single sign-on capabilities to remote users by allowing them to authenticate with the domain account and password. Single sign-on allows access to all resources on a network with a single user account and password, rather than having to provide different account/password combinations for connecting to the ISP and to the corporate network through a VPN connection. This single user account and password can be used at any remote access server or network device that's configured as a RADIUS client to the IAS server.
D: In the envisioned IT environment, the hospitals should be able to view only their own order status. Hanson Brothers will supply each hospital with a computer with which the hospitals will connected to

headquarters by using Routing and Remote Access (RRAS). In addition, each hospital will have a user account which will be authenticated and authorized when a user attempts to connect to a RRAS server. If RRAS is configured to use Remote Authentication Dial-In User Service (RADIUS) authentication, the username and password credentials of the user attempting to connect to RRAS is passed to the RADIUS server for authentication and authorization. If the connection attempt is both authenticated and authorized, the RADIUS server sends an accept message back to the remote access server and the connection attempt is accepted. If the connection attempt is either not authenticated or not authorized, the RADIUS server sends a reject message back to the RAS server and the connection process is denied. In Windows 2000, the RADIUS server is a Windows 2000-based computer running the Internet Authentication Service (IAS). However, RADIUS allows single sign-on capabilities to remote users by allowing them to authenticate with the domain account and password. Single sign-on allows access to all resources on a network with a single user account and password.

Q. 3
To which type of group should you assign sales representatives?

A. Universal
B. Local
C. Global
D. Domain local

Answer: C
Explantion:
We should use global groups to combine users and other global groups who have similar business requirements. Then, instead of assigning permissions directly to a global group, we should make the global group a member of a domain local group so that members of that global group inherit the permissions assigned to the domain local group.

Note: Global groups may only contain user accounts and global groups from the same domain as members. Membership of global groups is maintained in the domain where the domain local group exists Global groups are used for combining users who share a common access profile based on job function or business role. Typically, organizations use global groups for all groups where membership is expected to change frequently. These groups can only have as members user accounts defined in the same domain as the global group. Global groups can be nested to allow for overlapping access needs or to scale for very large group structures. The most convenient way to grant access to global groups is by making the global group a member of a resource group that is granted access permissions to a set of related resources.

Incorrect Answers:
A: We use Universal groups to collect similar groups that exist in multiple domains. The key difference between universal groups and other security groups is that memberships are stored both in the domain

where the universal group exists and in the global catalog. If the membership is stored in the global catalog, membership can be verified without contacting a Domain Controller where the universal group is defined. Instead of assigning permissions directly to a universal group, make the universal groups members of domain local groups and assign the necessary permissions to the domain local group. Universal groups are used in larger, multidomain organizations where there is a need to grant access to similar groups of accounts defined in multiple domains. It is better to use global groups as members of universal groups to reduce overall replication traffic from changes to universal group membership. Users can be added and removed from the corresponding global group within their account domains and a small number of global groups are the direct members of the universal group. Universal groups are easily granted access by making them a member of a domain local group used to grant access permissions to resources. Furthermore, the Windows 2000 domain must be in native mode to use universal groups.

B: Windows 2000 computers that are not Domain Controllers maintain Computer local groups with their own user accounts database. However, the servers at Headquarters as well as one server at each Distribution Center will function as Domain Controllers. We therefore cannot use Computer local groups.

D: Domain local groups are used for granting access rights to resources such as file systems or printers that are located on computer in the domain where common access permissions are required. The advantage of domain local groups used to protect resources is that members of the domain local groups can come from both inside the same domain and outside the domain. Typically, resource servers are in domains that have trust to one or more Master User Domains, or what are known as account domains. Furthermore, a domain local group can be used to grant access to resources on any computer only in native mode domains. In mixed mode, domain local groups must be on domain controllers only.

Q. 4
How should you grant the necessary permissions to the IT administrator at each distribution center?

A. Create a new administrator account for each distribution center's organizational unit (OU). Grant the necessary permissions to this account.
B. Create an administrator group for each distribution center's organizational unit (OU). Add an existing user designated as an administrator to this account. Grant the necessary permissions to this group.
C. Create a new administrator account for each distribution center's organizational unit (OU) in the headquarters root. Grant the necessary permissions to each new administrator's account.
D. Create an administrator group for each organizational unit (OU) at the headquarters root. Add an existing user designated as an administrator from each OU to this group. Grant the necessary permissions to this group.

Answer: B
Explanation:

In order to grant permission to the IT administrator at the distribution centers we must create an Administrator group for each Distribution Center OU and place the user that is designated as the administrator in this group. We must then assign the appropriate permission to the group. This will allow the designated user to logon to the domain as an administrator by using his or her own user account. It will also allow us to add or remove additional users to this group without having to assign or remove permissions from the existing user accounts.

Incorrect Answers:

A: We would want to assign the permissions at the group level as this would ease administration of the accounts. By assigning the permissions at the group level we will be able to add or remove additional users to this group without having to assign or remove permissions from the existing user accounts.

C: We would not want to create an additional administrator account in the headquarters root as this will give the designated user control over the entire forest. We only want to grant the user permissions at the OU level.

D: We would not want to create an additional administrator account in the headquarters root as this will give the designated user control over the entire forest. We only want to grant the user permissions at the OU level.

Q. 5
How should you encrypt orders from the sales representatives to the distribution centers?

A. Use 40-bit encryption for Routing and Remote Access. Use PPTP with packet filtering for VPN
B. Use 40-bit encryption for Routing and Remote Access. Use PPTP without packet filtering for VPN.
C. Use 128-bit encryption for Routing and Remote Access. Use PPTP with packet filtering for VPN
D. Use 128-bit encryption for Routing and Remote Access. Use PPTP without packet filtering for VPN

Answer: C
Explanation:
Sales representatives can use either Routing and Remote Access (RRAS) or VPN to access Headquarters from the Distribution Centers. As all the Distribution Centers are located in the USA, it would be possible to use 128-bit encryption. Indeed the highest level of encryption should be used wherever possible. In addition we would use PPTP for VPN as it supports encryption. We would also use packet filtering to define which protocols are allowed to pass through the firewall.

Incorrect Answers:

A: Sales representatives can use either Routing and Remote Access (RRAS) or VPN to access Headquarters from the Distribution Centers. Although we would use PPTP with packet filtering for VPN, we would want to use 128-bit encryption and not 40-bit encryption. All the Distribution Centers are located in the USA and it would thus be possible to use 128-bit encryption.

B: Sales representatives can use either Routing and Remote Access (RRAS) or VPN to access Headquarters from the Distribution Centers. As all the Distribution Centers are located in the USA, it would be possible to use 128-bit encryption. And indeed we would want to use 128-bit encryption and not 40-bit as the highest level of encryption should be used wherever possible.

D: Although we would use 128-bit encryption for RRAS, we would want to use packet filtering for VPN as well. Packet filtering allows us to configure which protocols are allowed to pass through the firewall.

Q. 6
Which four actions should you take to meet the security requirements for the Windows 2000 upgrade? (Choose four)

A. Ensure that only the sales representatives can create new orders.
B. Verify that only the Salesforce program can be loaded onto the portable computers.
C. Encrypt data transmitted to the distribution centers.
D. Verify that only unaltered versions of the Salesforce program are loaded onto the portable computers.
E. Restrict access to order status information to authorized Hanson Brothers employees and authorized hospitals.
F. Prevent distribution centers from using VPN to access information at other distribution centers.
G. Secure data on the portable computers.

Answer: C, D, E, G
Explanation:
Communication with the Distribution Centers occurs via the Internet. We should therefore encrypt communication with the Distribution Centers to improve security.

The Salesforce program is instrumental in the business process of Hanson Brothers. It is used to enter quantities of supplies and to report whether supplies should be ordered. It is thus important that the integrity of the Salesforce program be verifiable. One way of doing this is to ensure that unaltered versions of the program are loaded on the portable computers.

According to the Marketing manager, only sales representatives should be able to place an order and should only be able to view their own information. Hospitals should also only be able to view their own orders. Therefore we should restrict access to order information to authorized Hanson Brothers employees and authorized hospitals.

The information on the portable computers must be encrypted and recoverable. Therefore we must secure the data on the portable computers.

Incorrect Answers:

A: Customer Services should have the ability to read and modify orders for all hospitals. This might include the ability to place new orders.

B: The Sales Representatives will use their own portable computers and will be able to load personal programs onto their computers. We are therefore not required to ensure that only the Salesforce program is loaded on the portable computers.

F: Sales Representatives will be able to use either RRAS or VPN to connect to Headquarters. For this purpose a VNP server will be set up at Headquarters. No VPN server will be set up at the Distribution Centers. Therefore Distribution Centers will not be able to connect to each other via VPN.

Q. 7
How should you implement auditing on the Windows 2000 Server computers?

A. Enable success audit for logon events on the VPN server
B. Enable failure audit for logon events on the VPN server
C. Enable success audit for logon events on the domain controllers
D. Enable failure audit for logon events on the domain controllers

Answer: D
Explanation:
The IT manager must be aware of attempted unauthorized access to the network. Therefore we must audit logon events on the domain controller. We would only audit for logon failure as authorized access would be successful. We would audit events on the Domain Controllers are all logon authentication occurs at the Domain Controllers.

Incorrect Answers:

A: The IT manager must be aware of attempted unauthorized access to the network events pertaining to attempted access to the network would be recorded in logon failure and not logon success. The later would record authorized access to the network. We should therefore audit logon events for failure and not success. Furthermore, we would want to run auditing on the Domain Controllers and not the VPN sever. Network logon authentication and authorization is performed on the Domain Controllers while only VPN access is performed by the VPN server. Auditing the VPN server would thus only record information about access via the VPN server.

B: The IT manager must be aware of attempted unauthorized access to the network events pertaining to attempted access to the network would be recorded in logon failure. However, we would want to run auditing on the Domain Controllers and not the VPN sever. Network logon authentication and authorization is performed on the Domain Controllers while only VPN access is performed by the VPN server. Auditing the VPN server would thus only record information about access via the VPN server.

C: The IT manager must be aware of attempted unauthorized access to the network events pertaining to attempted access to the network would be recorded in logon failure and not logon success. The later would record authorized access to the network. We should therefore audit logon events for failure and not success. We would audit events on the Domain Controllers are all logon authentication occurs at the Domain Controllers.

Q. 8
Which Group Policy strategy should you use to prevent changes to the wallpaper on all computers?

A. Create a Group Policy for each distribution center, and apply the Group Policy at the headquarters domain
B. Create a Group Policy for each distribution center, and apply the Group Policy at each distribution center's organizational unit (OU)
C. Create one Group Policy for all distribution centers, and apply the Group Policy at the headquarters domain.
D. Create one Group Policy for all distribution centers, and apply the Group Policy at each distribution center's organizational unit (OU)

Answer: C
Explanation:
In a Windows 2000 network, we can use Group Policies to control users' desktop environments. This includes wallpaper settings. Group Policies can be applied at the Site level, the Domain level, and the Organizational Unit (OU) level. Group Policy precedence follows the Group Policy model and is applied hierarchically from the least restrictive object, i.e. the Site, to the most restrictive object, i.e. the OU. In other words Windows 2000 applies Group Policies that are linked to sites first, then Group Policies that are linked to domains, and then Group Policies that are linked to OU. However, in this scenario we must ensure that wallpaper is not changed on any of the computers in the entire domain. We should therefore apply the Group Policy at the root domain, i.e. at Headquarters.

Incorrect Answers:
A: As the settings should be applied to all the computers, it is possible to create a single Group Policy for all the Distribution Centers rather than creating one for each Distribution Center. By creating one Group Policy for all Distribution Centers we will reduce administrative effort.
B: As the settings should be applied to all the computers, it is possible to create a single Group Policy for all the Distribution Centers rather than creating one for each Distribution Center. By creating one Group Policy for all Distribution Centers we will reduce administrative effort. We should also apply the Group Policy at the root domain rather than at the OU level. This would mean that the Group Policy should be applied at the level of the Headquarters Domain.
D: In a Windows 2000 network, we can use Group Policies to control users' desktop environments. This includes wallpaper settings. Group Policies can be applied at the Site level, the Domain level, and the Organizational Unit (OU) level. Group Policy precedence follows the Group Policy model and is applied hierarchically from the least restrictive object, i.e. the Site, to the most restrictive object, i.e. the OU. In other words Windows 2000 applies Group Policies that are linked to sites first, then Group Policies that are linked to domains, and then Group Policies that are linked to OU. However, in this scenario we must ensure that wallpaper is not changed on any of the computers in the entire domain.

We should therefore apply the Group Policy at the root domain, i.e. at Headquarters, and not at the level of the OUs.

Q. 9
How should you restrict hospital dial-up connections to only authorized hospitals?

A. Configure Routing and Remote Access on the remote access server to use callback. Configure callback to dial a phone number specified by the hospital computer during the connection request.
B. Configure Routing and Remote Access on the remote access server to use callback. Configure callback to dial a predefined phone number at the hospital.
C. Set up a proxy server (NAT) on the private side of the remote access server. Configure the proxy server to accept the IP addresses of the hospital computers.
D. Set up a proxy server (NAT) on the public side of the remote access server. Configure the proxy server to accept the IP addresses of the hospital computers.

Answer: B
Explanation:
To increase security in dial-up connections we can configure Callback options. We can choose to implement no callback security and have the remote access client provide the phone number to call back or we can require callbacks to predetermined phone numbers. Configuring callback to call a specific number provides the highest form of security.

Note: The Callback options are:

- Assign a Static IP Address

If this property is enabled, the administrator assigns a specific IP address to the user when the connection is made.

- Apply Static Routes

If this property enabled, the administrator defines a series of static IP routes that are added to the routing table of the remote access server when a connection is made. This setting is designed for user accounts that Windows 2000 routers use for demand-dial routing.

If a Windows 2000 Routing and Remote Access service server is a member of a Windows NT 4.0 domain or a Windows 2000 mixed domain, then only the Remote Access Permission (Allow access and Deny access options) and Callback Options dial-in properties are available.

The User Manager for Domains administrative tool can be used to grant or deny dial-in access and set callback options.

Incorrect Answers:

A: When we can configure Callback options to callback to the telephone number provided by the remote access client, we do not ensure the authenticity of the remote access client.

C: Proxy Server can be used to protect the network from malicious attacks that originate on the Internet. RRAS does not make use of the Internet ro establish a connection. Therefore Proxy servers are inappropriate to this scenatrio. In additoin, Proxy servers can only be configured to filter IP addresses. It cannot be used for authenticate purposes.

D: Proxy Server can be used to protect the network from malicious attacks that originate on the Internet. RRAS does not make use of the Internet ro establish a connection. Therefore Proxy servers are inappropriate to this scenatrio. In additoin, Proxy servers can only be configured to filter IP addresses. It cannot be used for authenticate purposes.

Q. 10
How should you restrict hospitals' access to the order status information?

A. Set permissions on each hospital's order file to grant all hospitals Read permission to all order files.
B. Set permissions on each hospital's order file to grant that hospital Read permission to its own order file.
C. Enable Encrypting File System (EFS) on the order status folder, and give a single copy of the recovery' key to all hospitals.
D. Enable Encrypting File System (EFS) on the order status folder, and give a copy of the unique recovery key to each hospital.

Answer: B
Explanation:
Hospitals must only be able to view the order status information that pertains to the hospital itself. Therefore we should set permissions on each hospital's order file to grant that hospital Read permission to its own order file.

Incorrect Answers:

A: Hospitals must only be able to view the order status information that pertains to the hospital itself. Therefore we should set permissions on each hospital's order file to grant that hospital Read permission to its own order file. If we grant each hospital read permissions to all order files then the hospitals will be able to view the order status of the other hospitals as well. This is not desired in this scenario.

C: When a user encrypts files, only that user the will be able to use the file. Recovery Agents, and Administrators who are members of the Recovery Agents group by default, would be able to decrypt the file. We therefore cannot use EFS in this scenario.

D: When a user encrypts files, only that user the will be able to use the file. Recovery Agents, and Administrators who are members of the Recovery Agents group by default, would be able to decrypt the file. We therefore cannot use EFS in this scenario.

Q. 11
How should you configure secure communications between the Pittsburgh distribution center and headquarters?

A. Enable L2TP and configure an enterprise subordinate CA on the private Hanson Brothers network
B. Enable L2TP and configure an enterprise root CA on the private Hanson Brothers network
C. Enable L2TP and configure an enterprise root CA on the public network.
D. Enable L2TP and configure an enterprise subordinate CA on the public network

Answer: A
Explanation:
The new distribution center in Pittsburgh, Pennsylvania will be connected to headquarters through a VPN. To secure communication across a VPN we can use L2TP over IPSec. L2TP creates the necessary IPSec security policy to secure tunnel traffic. We do not need to assign or activate our own IPSec policy on either computer. If the computer already has an IPSec policy active, the L2TP will simply add a security rule to protect L2TP tunnel traffic to the existing policy. For an L2TP over IPSec connection to occur, we need to install computer certificates on the VPN client and VPN server computers. In other words IPSec requires that we establish the trust relationship using certificates issued to each computer.

Enterprise CAs are integrated in Active Directory. Therefore, to ensure the security of the Enterprise CA we would want to take the CA off line. To do this we would need to set up a subordinate Enterprise CA which will receive a certificate from the Enterprise root CA and will issue certificates on behalf of the Enterprise Root CA. This will prevent the Enterprise root CA from which all Certificates flow from being compromised.

Note: The Distribution Centers are part of the private Hanson Brothers network.

Incorrect Answers:
B: To ensure the security of the Enterprise CA we would want to take the CA off line. To do this we would need to set up a subordinate Enterprise CA which will receive a certificate from the Enterprise root CA and will issue certificates on behalf of the Enterprise Root CA. This will prevent the Enterprise root CA from which all Certificates flow from being compromised.
C: To ensure the security of the Enterprise CA we would want to take the CA off line. To do this we would need to set up a subordinate Enterprise CA which will receive a certificate from the Enterprise root CA and will issue certificates on behalf of the Enterprise Root CA. This will prevent the Enterprise root CA from which all Certificates flow from being compromised. Furthermore, the Distribution Centers are part of the Hanson Brothers’ private network.
D: Enterprise CAs are integrated in Active Directory. Therefore, to ensure the security of the Enterprise CA we would want to take the CA off line. To do this we would need to set up a subordinate Enterprise CA which will receive a certificate from the Enterprise root CA and will issue certificates on behalf of the Enterprise Root CA. This will prevent the Enterprise root CA from which all Certificates flow from being compromised. However, the Distribution Centers are part of the Hanson Brothers’ private network. Therefore the CA should be on the private network.

Q. 12

How should you implement IP filters at headquarters to secure the connection to the Pittsburgh distribution center?

A. Add source filters for the Pittsburgh distribution center for UDP port 500 and IP protocol 50. Add destination filters for headquarters for UDP port 500 and IP protocol 50

B. Add source filters for the Pittsburgh distribution center for UDP port 1701 and IP protocol 50. Add destination filters for headquarters for UDP port 1701 and IP protocol 50

C. Add source filters for headquarters for UDP port 500 and IP protocol 50. Add destination filters for the Pittsburgh distribution center for UDP port 500 and IP protocol 50.

D. Add source filters for headquarters for UDP port 1701 and IP protocol 50. Add destination filters for the Pittsburgh distribution center for UDP port 1701 and IP protocol 50

Answer: B

Explanation:

The new distribution center in Pittsburgh, Pennsylvania will be connected to headquarters through a VPN. We would use L2TP over IPSec to secure transmissions over VPN. L2TP uses User Datagram Protocol (UDP) port "Any" and destination port 1701. Also set routing and remote access input and output permit filters for the Internet key exchange (IKE) protocol, which uses UDP source port "Any" and destination port 500, prohibiting everything but L2TP over IPSec traffic. Furthermore, IP port 50 is used for both inbound and outbound Encapsulating Security Protocol (ESP) traffic. Therefore we should filter the VPN client in Pittsburgh, Pennsylvania by allowing UDP port 1701 and IP protocol 50. We would not need to configure UDP port 500 as the IKE will not originate from the client but from the VPN server at Headquarters.

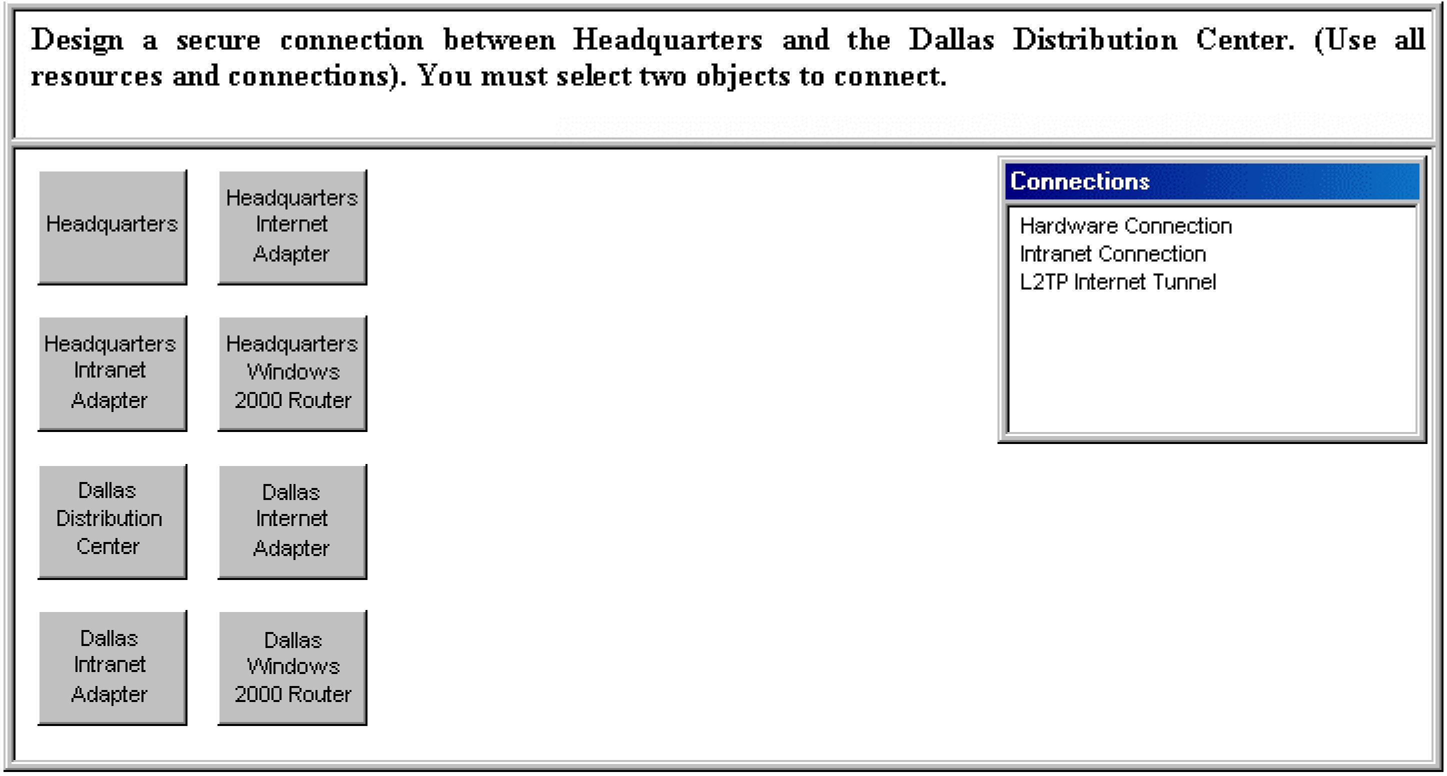
Incorrect Answers:

A: Internet key exchange (IKE) protocol, which uses UDP source port "Any" and destination port 500. However, the IKE will not originate from the client but from the VPN server at Headquarters. Therefore we would not need to configure UDP port 500.

C: Internet key exchange (IKE) protocol, which uses UDP source port "Any" and destination port 500. However, the IKE will not originate from the client but from the VPN server at Headquarters. Therefore we would not need to configure UDP port 500.

D: We must configure the ports at the client, not at the server.

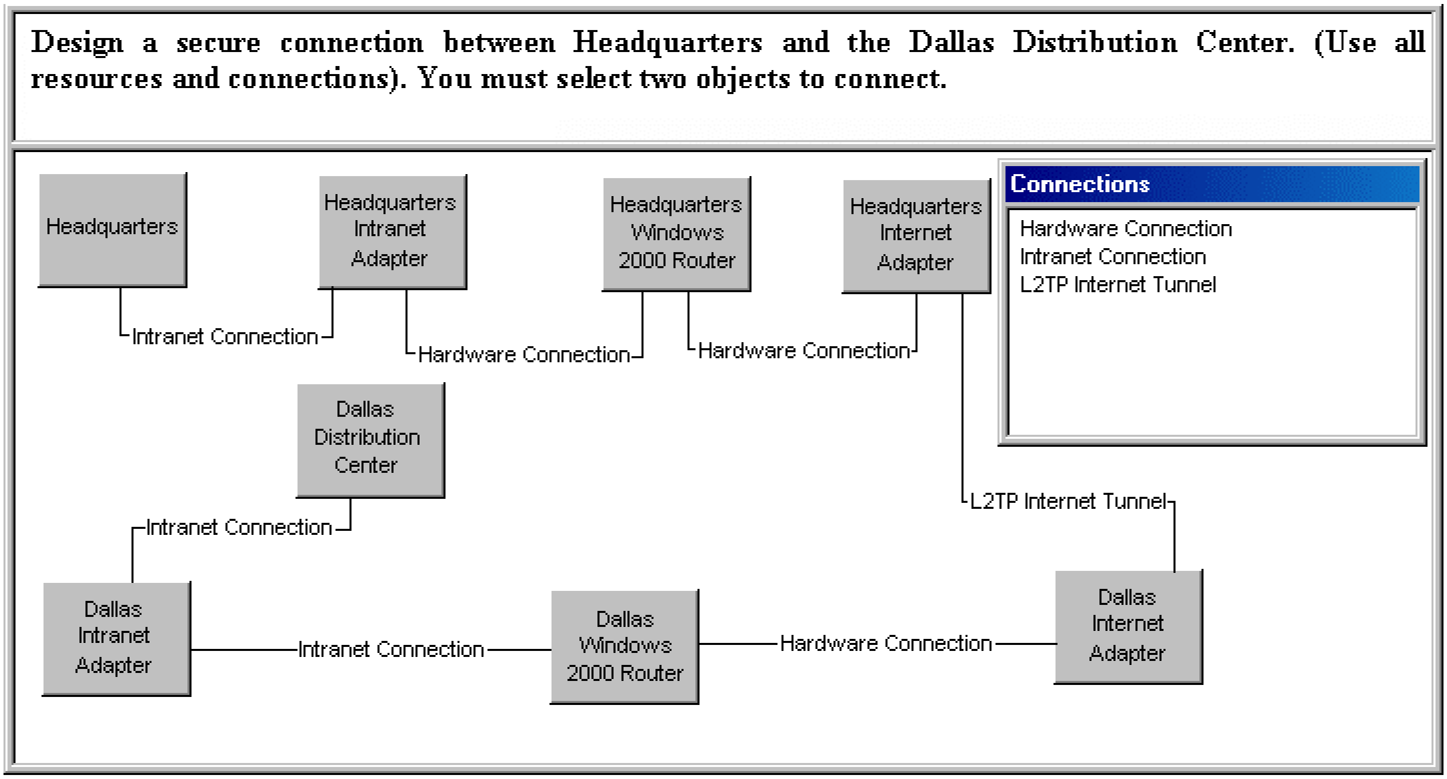
Q. 13



Design a secure connection between Headquarters and the Dallas Distribution Center. (Use all resources and connections). You must select two objects to connect.

Headquarters
Headquarters Internet Adapter
Headquarters Intranet Adapter
Headquarters Windows 2000 Router
Dallas Distribution Center
Dallas Internet Adapter
Dallas Intranet Adapter
Dallas Windows 2000 Router
Connections
Hardware Connection
Intranet Connection
L2TP Internet Tunnel

Answer:



Design a secure connection between Headquarters and the Dallas Distribution Center. (Use all resources and connections). You must select two objects to connect.

Explanation:

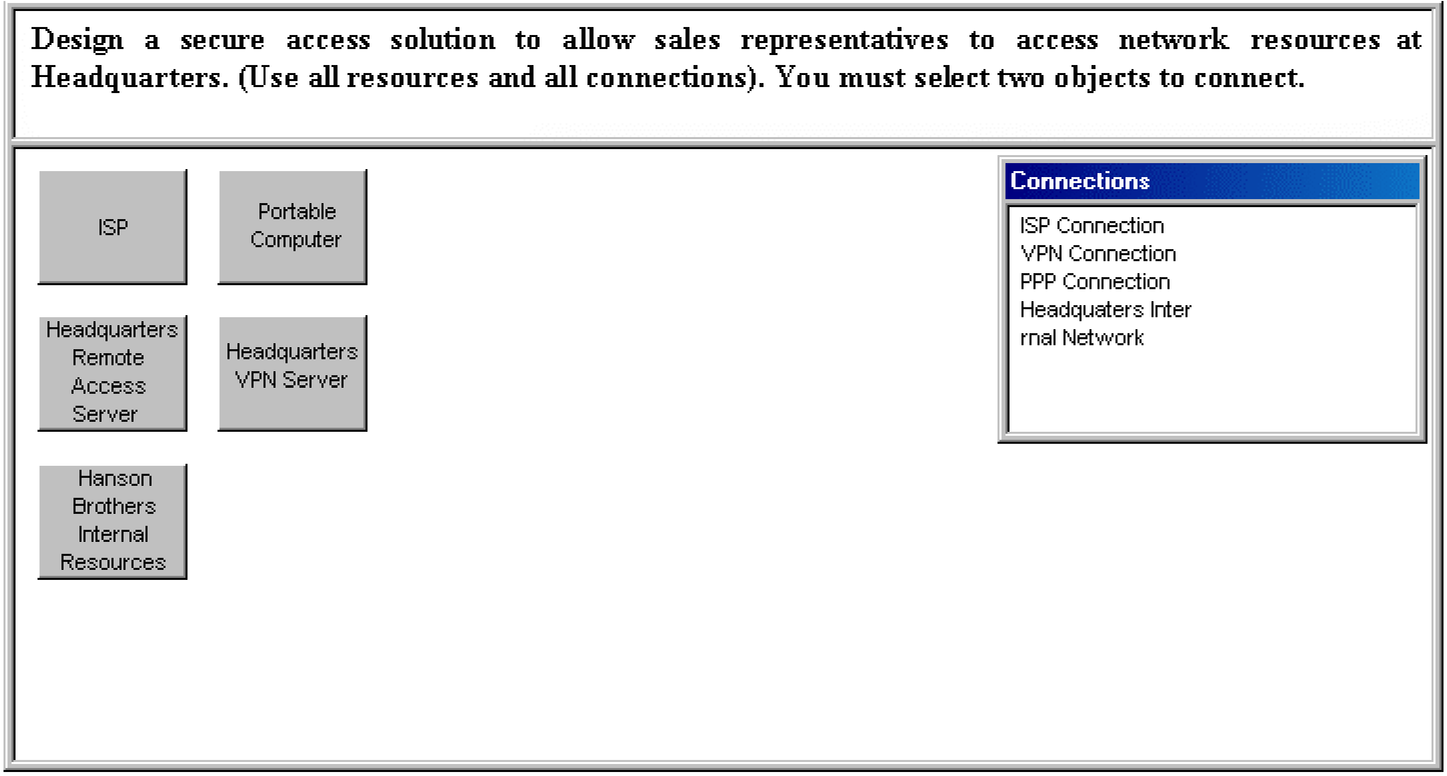
Headquarters is connected to the Headquarters Intranet Adapter, i.e. its Network Adapter Card, by means of an Intranet, or LAN Connection.

Similarly, the Dallas Distribution Center is connected to the Dallas Intranet Adapter by means of an Intranet Connection.

A Windows 2000 Router is a Windows 2000 server computer that has either two Network Adapter Cards to connect two Subnets, or a Network Adapter Card and an Internet Adapter, i.e. a Modem. These will be connected together by a physical Hardware Connection. This applies to both the Windows 2000 router at Headquarters and the Windows 2000 Router in Dallas.

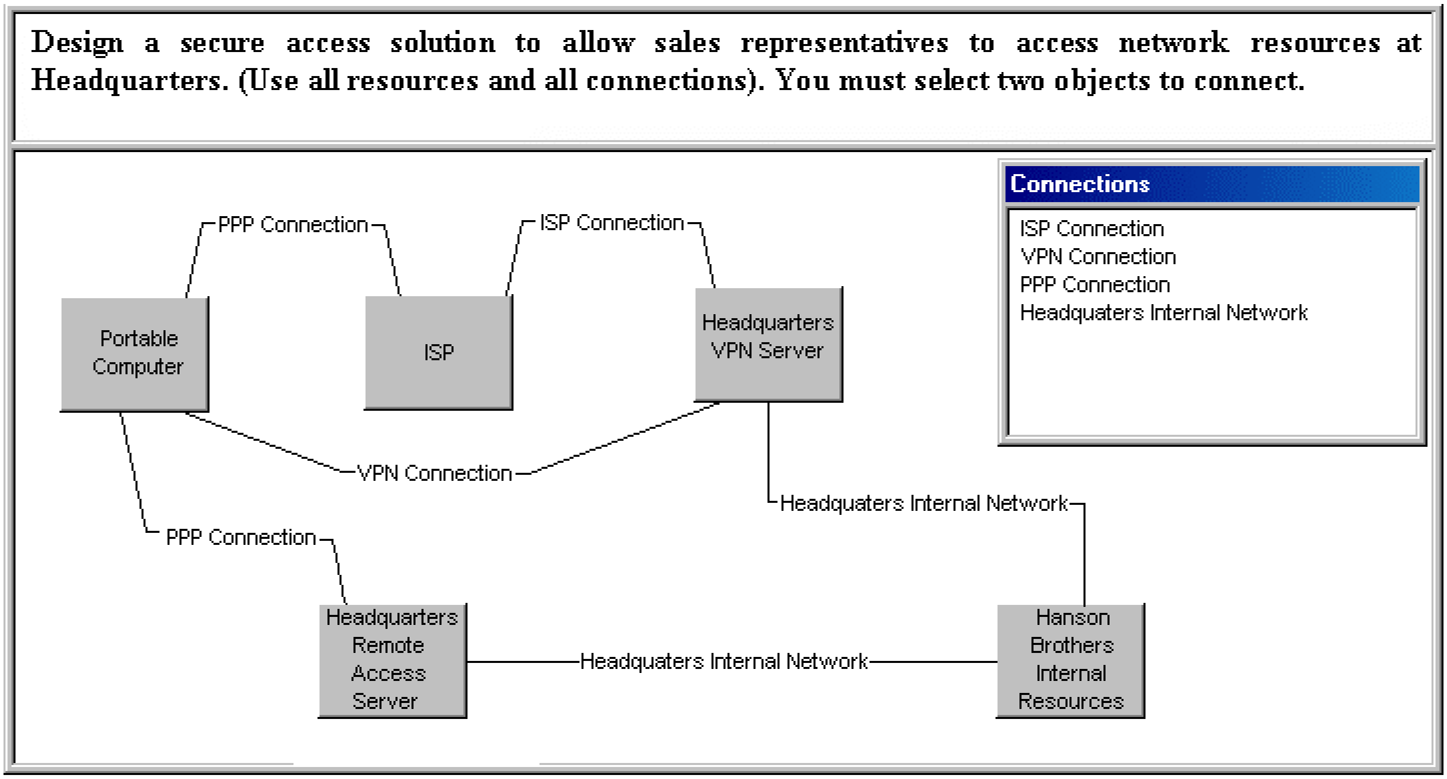
The Headquarters Internet Adapter is connected to the Dallas Internet Adapter via a VPN. A VPN is a tunnel through a public network such as the Internet.

Q. 14



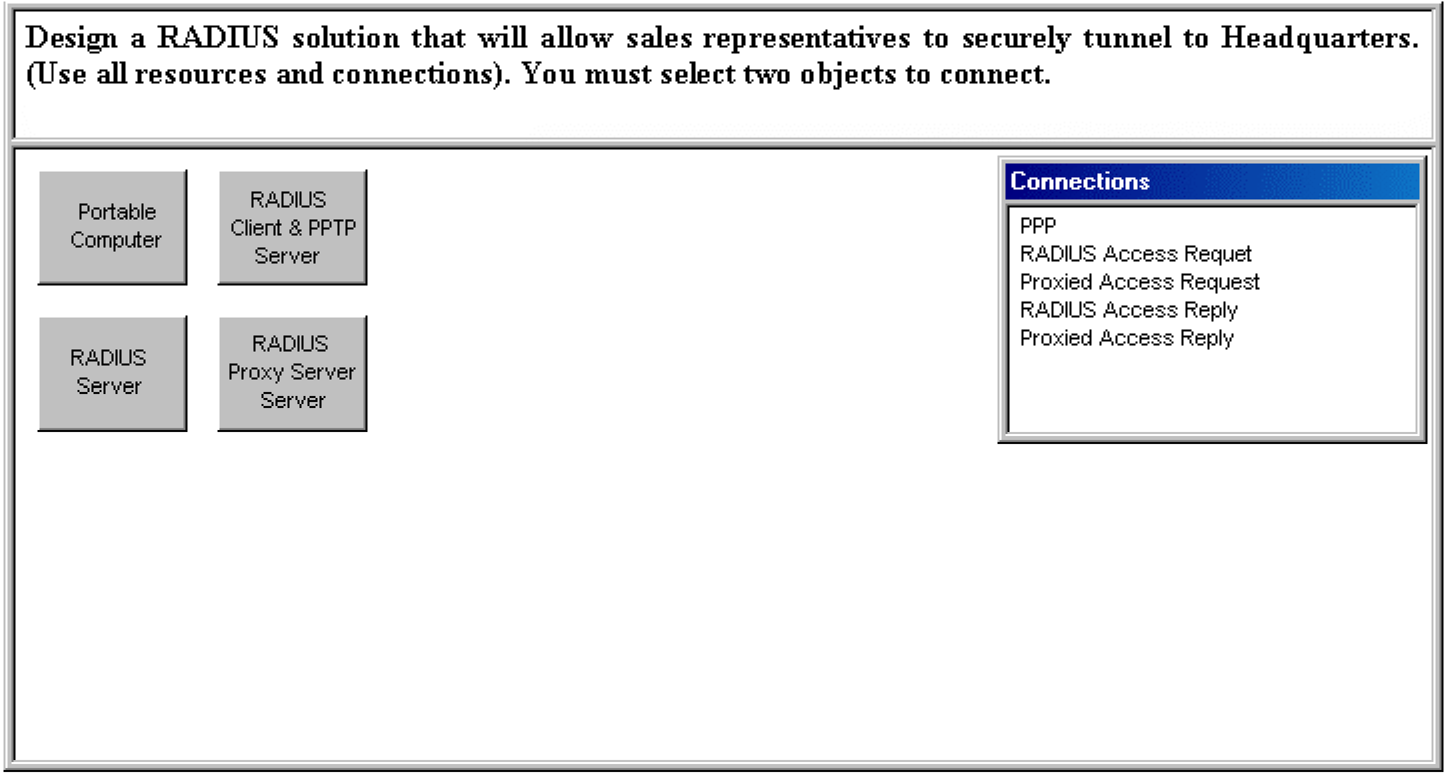
Design a secure access solution to allow sales representatives to access network resources at Headquarters. (Use all resources and all connections). You must select two objects to connect.

Answer:



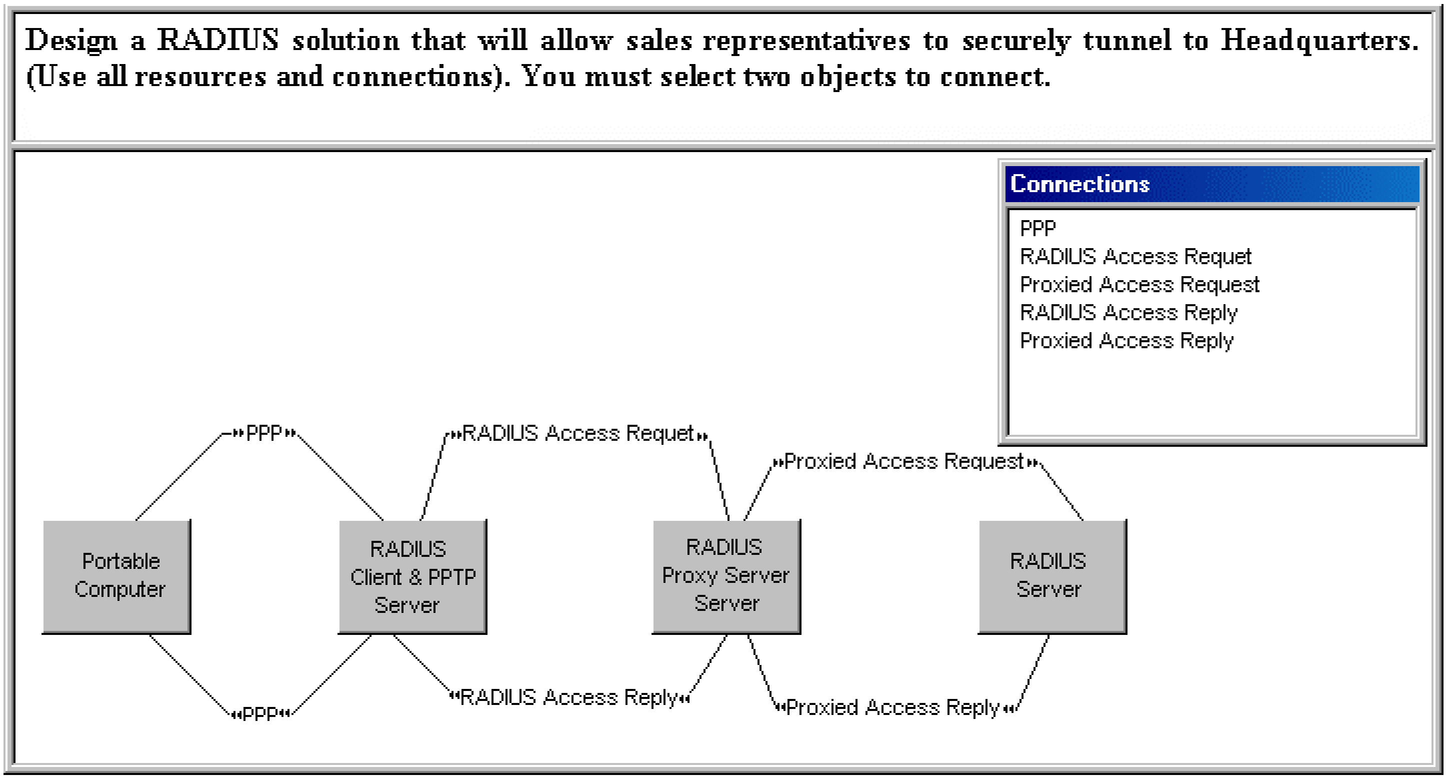
Design a secure access solution to allow sales representatives to access network resources at Headquarters. (Use all resources and all connections). You must select two objects to connect.

Q. 15



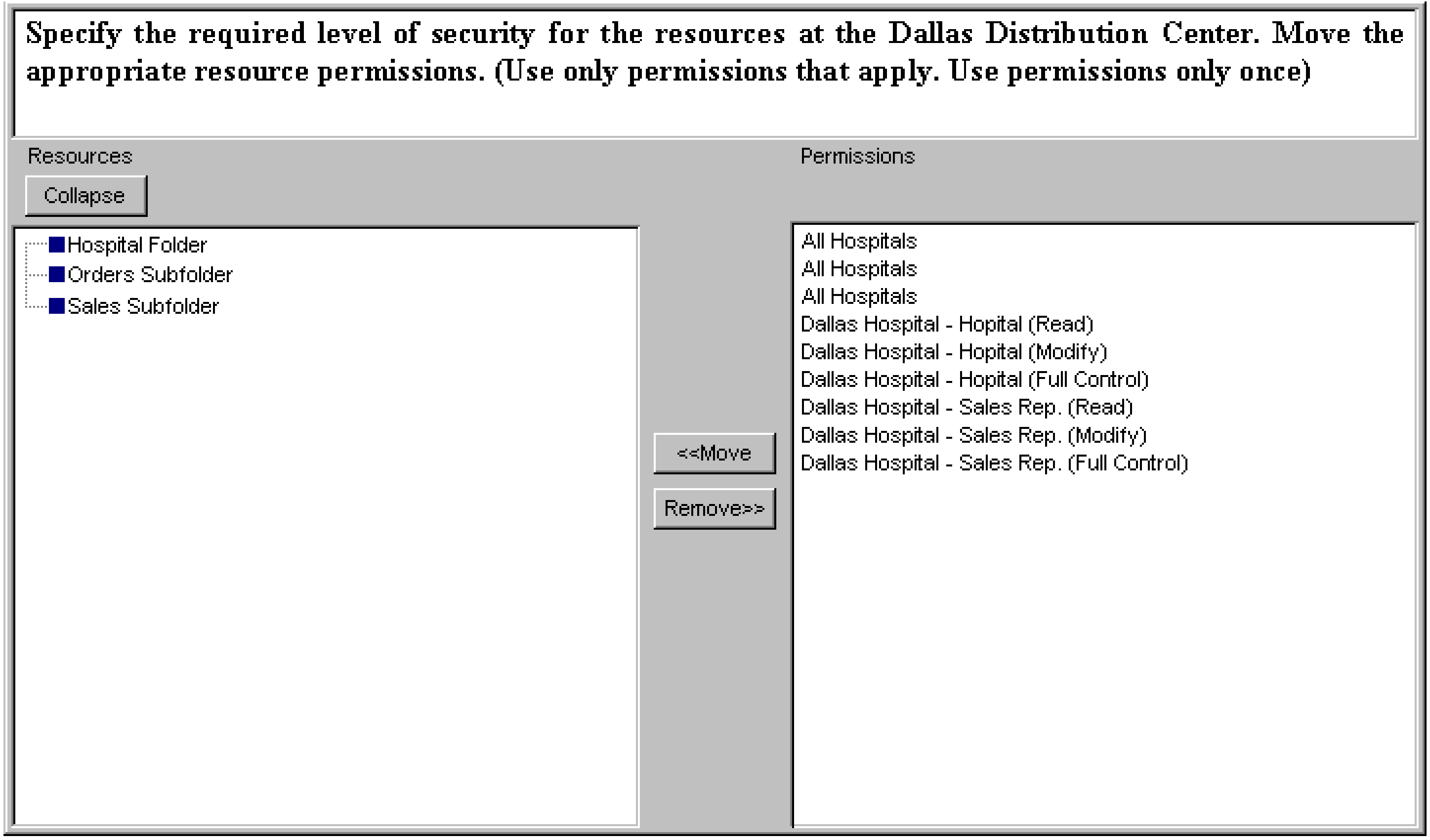
Design a RADIUS solution that will allow sales representatives to securely tunnel to Headquarters. (Use all resources and connections). You must select two objects to connect.

Answer:



Design a RADIUS solution that will allow sales representatives to securely tunnel to Headquarters. (Use all resources and connections). You must select two objects to connect.

Q. 16

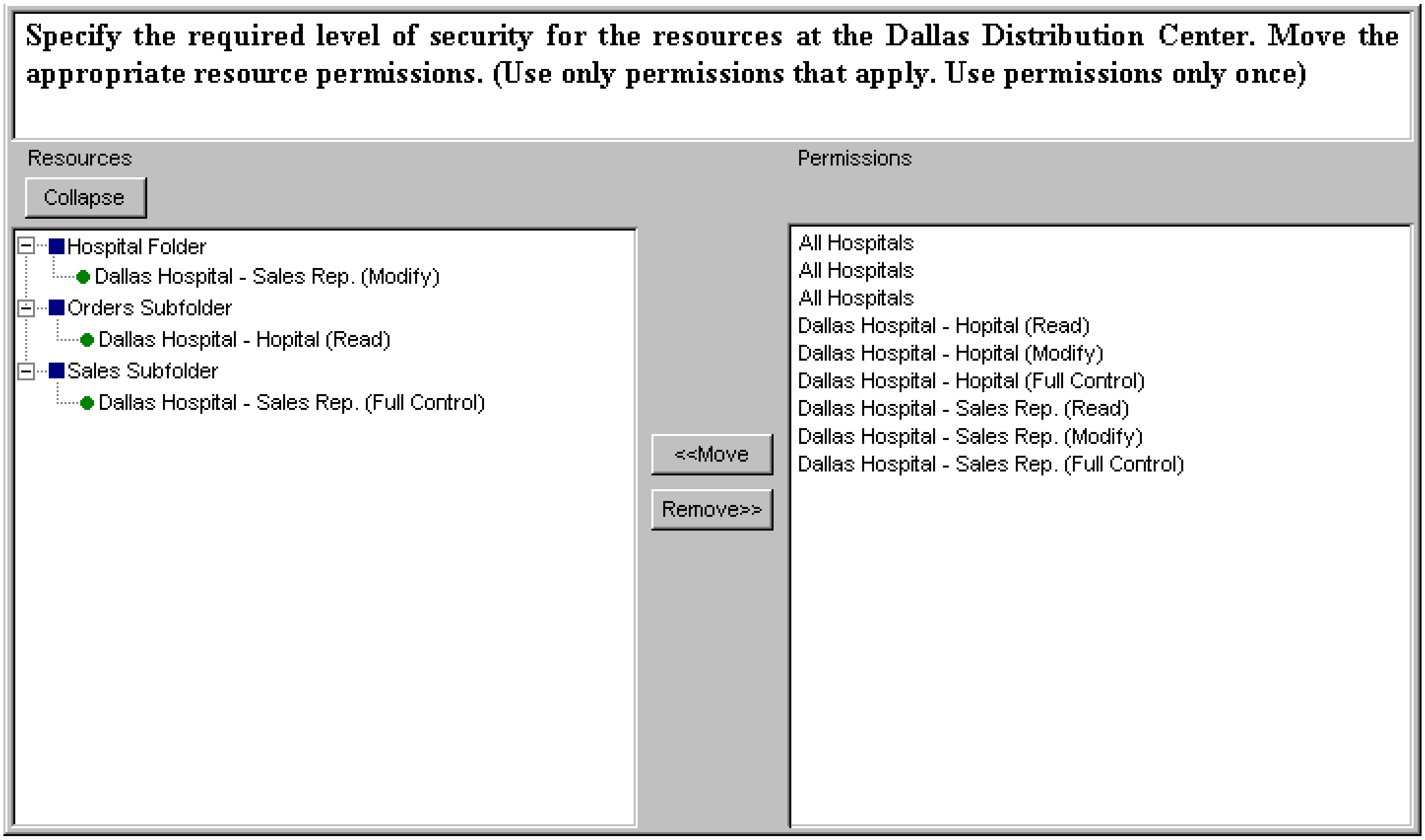


Specify the required level of security for the resources at the Dallas Distribution Center. Move the appropriate resource permissions. (Use only permissions that apply. Use permissions only once)

- Hospital Folder
- Orders Subfolder
- Sales Subfolder

All Hospitals
All Hospitals
All Hospitals
Dallas Hospital - Hopital (Read)
Dallas Hospital - Hopital (Modify)
Dallas Hospital - Hopital (Full Control)
Dallas Hospital - Sales Rep. (Read)
Dallas Hospital - Sales Rep. (Modify)
Dallas Hospital - Sales Rep. (Full Control)

Answer:



Specify the required level of security for the resources at the Dallas Distribution Center. Move the appropriate resource permissions. (Use only permissions that apply. Use permissions only once)

- Hospital Folder
  - Dallas Hospital - Sales Rep. (Modify)
- Orders Subfolder
  - Dallas Hospital - Hopital (Read)
- Sales Subfolder
  - Dallas Hospital - Sales Rep. (Full Control)

All Hospitals
All Hospitals
All Hospitals
Dallas Hospital - Hopital (Read)
Dallas Hospital - Hopital (Modify)
Dallas Hospital - Hopital (Full Control)
Dallas Hospital - Sales Rep. (Read)
Dallas Hospital - Sales Rep. (Modify)
Dallas Hospital - Sales Rep. (Full Control)

Case Study No: 4

MILLER TEXTILES

Background:

Miller Textiles:

Miller Textiles is a manufacturer of industrial fabrics. Miller Textiles has more than 12,000 employees. The headquarters are located in Boston, Massachusetts and there are manufacturing facilities in Atlanta, Georgia; Baja, Mexico and Dublin, Ireland. The Chief Information Officer (CIO) has requested a security design proposal for Miller Textiles.

Fabrikam, Inc.:

Fabrikam, Inc. is a manufacturer of specialty blankets. The company has more than 300 employees. Fabrikam, Inc. has only one manufacturing facility in Miami, Florida.

Joint Venture:

Miller Textiles has just completed an agreement with Fabrikam, Inc. to begin a joint venture. Both companies want to expand their product lines to include space blankets. These blankets will protect satellites from collisions with meteorites and other space debris. Engineers from Miller Textiles and Fabrikam, Inc. will work together to produce the fabric that will be used in the blankets. This joint venture will require the two companies to communicate with each other frequently.

Organization:

Miller Textiles and Fabrikam Inc. both have a similar organizational structure. Each company has an engineering department, a manufacturing department, and a sales department. The engineering department includes engineers who will create the designs for the space blankets. The manufacturing department includes employees who will manufacture the blankets. The sales department includes sales representatives who will sell the blankets.

Existing IT Environment:

Miller Textiles:

Computers:

All servers, desktop computers, and portable computers run Windows 2000. Each manufacturing facility and headquarters has a server named MANUFACTURING and a server named ENGINEERING. The MANUFACTURING server contains a schedule that shows the availability of every type of fabric produced by that facility. The ENGINEERING server contains all information needed to produce a new item or improve an existing item.

LAN and WAN Connectivity:

The manufacturing facilities are connected to headquarters with T1 lines. The maximum usage for the T1 connection is 40 percent. There is one remote access server at headquarters and one remote access server at each manufacturing facility. The LAN at each manufacturing facility and headquarters runs at 100 Mbps. Miller Textiles has a single domain named MILLER. Each manufacturing facility has its own organizational unit (OU). The OUs are named ATLANTA, BAJA, BOSTON, and DUBLIN.

Domain Model:

We are committing major resources to the space blanket project. The data related to the project must remain secure. Each manufacturing facility has its own IT employees who administer its OU. This distributed administration will be retained in the new security plan.

Existing IT Environment:

Fabrikam, Inc.:

Fabrikam, Inc. has just completed a full upgrade to Windows 2000 on all servers and desktop computers. There is a single domain named FABRIKAM and a domain namespace named Fabrikam.com. The company has its own unique Active Directory schema. In addition, Fabrikam, Inc has a VPN server named FABHQVPN and an e-mail server.

All files for the joint venture are stored in a shared folder named MILLERSPACE. This folder is shared by engineers from Fabrikam, Inc, and Miller Textiles. It allows engineers from Miller Textiles to view and modify all files in the MILLERSPACE folder.

Envisioned IT Environment

Miller Textiles:

Computers:

All sales representatives will have a folder named Customer on their portable computers. Because this folder will be used to store confidential customer information, the folder must be secure and encrypted. The folder will be updated when the sales representatives dial in to headquarters. The connection must be secure. The envisioned environment at headquarters is shown in the exhibit. (Click the Exhibit button).

Miller Textiles will have shared folders that will contain information about the joint venture. This folder will be named FABRIKAMSPACE. One folder will exist on the ENGINEERING server at each location. The

ENGINEERING and MANUFACTURING servers at each location will contain engineering and manufacturing data for that location only.

LAN and WAN Connectivity:
The T1 line between headquarters and all manufacturing facilities will remain the same. All remote access servers at the manufacturing facilities will be eliminated. Sales representatives will connect to the network by using a dial-up connection located at headquarters. The remote access server at headquarters will be used as a backup to the VPN. Communication across the VPN connection should be encrypted. Miller Textiles has a frame relay connection to the Internet through a VPN server.

Domain Model:
There will be one DNS namespace named millertextiles.com. The existing domain will be in one forest. The engineering department and the manufacturing department will have their own organizational unit (OU) at each manufacturing facility and headquarters IT employees located at each manufacturing facility will administer the OU for that manufacturing facility. The OU administrators will have full control of all folders on all servers within their OUs.

A trust relationship will be established between BOSTON and FABRIKAM that will allow engineers access to each other’s domains.

Problem Statement

Miller Textiles:

Chief Executive Officer (CEO):
Engineers from all of our branch offices and engineers from Fabrikam Inc. will be working together. All engineering data that is related to the joint venture must be available to all engineers.

We are committing major resources to the space blanket project. The data related to the project must remain secure.

IT Director:
Our employees are encouraged to transfer between branch offices to enhance their job skills. During transfers, it has been difficult to move employees’ accounts from one OU to another. During the joint venture, resources from both companies will be shared. For example, an employee from Miller Textiles should be able to print to a Fabrikam printer and a Fabrikam employee should be able to print to a Miller Textiles printer.

Customer information on the sales representatives’ portable computers must be secure. I want to know who is modifying or viewing the information in the FABRIKAMSPACE folder in any of our branch offices.

Sales Director:
The sales representatives are very excited about our new joint venture. The profit on these blankets will be very high, but the number of buyers is limited. We must not let our traditional business suffer. The sales representatives will continue to visit our existing customers and search for new customers within their assigned territory. While visiting our customers, our sales representatives must have access to all manufacturing schedules. Many potential customers want to know about the availability of the product.

Envisioned IT Environment

Fabrikam, Inc.:
The security design for Fabrikam, Inc. will not change.

Questions Miller Textiles

Q. 1
What are the two primary security risks for Miller Textiles? (Choose two)

A. Fabrikam, Inc., engineers modifying the manufacturing schedules for Miller Textiles
B. Unauthorized users viewing manufacturing schedules
C. Fabrikam, Inc, employees viewing confidential information from Miller Textiles
D. Unauthorized users gaining access to data for the space blankets
E. Unauthorized users gaining access to customer information on the portable computers

Answer: D, E
Explanation:
According to the CEO of Miller Textiles, the company has committed major resources to the space blanket project. The data related to the space blanket project must thus remain secure. In addition, the IT Director of Miller Textiles also wants to know who is modifying or viewing data in the folder that contains information about the space blanket project.

Furthermore, all sales representatives have a folder on their portable computers that contains confidential information that should be secure and encrypted. In addition the IT Director of Miller Textiles, customer information on the sales representatives' portable computers must be secure.

Incorrect Answers:
A: A trust relation will be established between the manufacturing OU in Boston, i.e. the BOSTON OU, and the Fabrikam domain. This is to ensure that Engineers will have access to each others domains. Therefore the possibility of Fabrikam, Inc., engineers modifying the manufacturing schedules for Miller Textiles is not a major concern.
B: A manufacturing schedules shows the availability of every type of fabric produced by the facility. According to the Sales Director, the sales representatives must have access to all manufacturing schedules as potential customers will want to know about the availability of the products. This is thus not sensitive information and is therefore not a security concern.
C: The only confidential information from Miler Textiles pertains to the joint project with Fabrikam, Inc. there is thus no concern that Fabrikam, Inc, employees viewing confidential information from Miller Textiles.

Q. 2
Which security group strategy should you use for the Miller Textiles sales representatives?

A. Assign all sales representatives to domain local groups within their own domain. Put the domain local groups into global groups.
B. Assign all sales representatives to global groups. Put the global groups into domain local groups
C. Assign all sales representatives to universal groups. Put the global groups into universal groups
D. Assign all sales representatives to computer local groups. Put the computer local groups into universal groups

Answer: B
Explanation:
In this scenario the Miller Textiles sales representatives perform a similar job function and will require similar access to files and folders in the domain. We can therefore place the sales representatives in global groups and place the global groups in domain local groups. We should use global groups to combine users and other global groups who have similar business requirements. Then, instead of assigning permissions directly to a global group, we should make the global group a member of a domain local group so that members of that global group inherit the permissions assigned to the domain local group.

Note: Global groups may only contain user accounts and global groups from the same domain as members. Membership of global groups is maintained in the domain where the domain local group exists Global groups are used for combining users who share a common access profile based on job function or business role. Typically, organizations use global groups for all groups where membership is expected to change frequently. These groups can only have as members user accounts defined in the same domain as the global group. Global groups can be nested to allow for overlapping access needs or to scale for very large group structures. The most convenient way to grant access to global groups is by making the global group a member of a resource group that is granted access permissions to a set of related resources.

Incorrect Answers:
A: Windows 2000 does not permit the nesting of Domain Local Groups in other groups. In other words we cannot place Domain Local Groups into any group, even if that group is in the same domain. We therefore cannot assign all sales representatives to domain local groups within their own domain and put the domain local groups into global groups.
C: We use Universal groups to collect similar groups that exist in multiple domains. The key difference between universal groups and other security groups is that memberships are stored both in the domain where the universal group exists and in the global catalog. If the membership is stored in the global catalog, membership can be verified without contacting a Domain Controller where the universal group is defined. Instead of assigning permissions directly to a universal group, make the universal groups members of domain local groups and assign the necessary permissions to the domain local group. Universal groups are used in larger, multidomain organizations where there is a need to grant access to similar groups of accounts defined in multiple domains. It is better to use global groups as members of universal groups to reduce overall replication traffic from changes to universal group membership. Users can be added and removed from the corresponding global group within their account domains and a small number of global groups are the direct members of the universal group. Universal groups are

easily granted access by making them a member of a domain local group used to grant access permissions to resources. Furthermore, the Windows 2000 domain must be in native mode to use universal groups. In this scenario there is only one domain therefore we would not use universal groups.

D: Windows 2000 computers that are not Domain Controllers maintain Computer local groups with their own user accounts database. However, the servers at Headquarters will function as Domain Controllers. We therefore cannot use Computer local groups.

Q. 3
How should you encrypt information over the VPN between the BOSTON organizational unit (OU) and the FABRIKAM domain?

A. Implement L2TP over IPSec at the BOSTON OU only
B. Implement L2TP over IPSec at both the BOSTON OU and the FABRIKAM domain
C. Implement PPTP at both the BOSTON OU and the FABRIKAM domain
D. Implement PPTP at the BOSTON OU only

Answer: B
Explanation:
L2TP is a method of providing VPN access to the network. It can be used to provide both client-to-server and server-to-server access. Although L2TP does not include an encryption mechanism, IPSec is used to negotiate a security association between the two computers using the L2TP tunnel. IPSec then provides the encryption. Thus, whenever the L2TP is used to establish a VPN, Windows 2000 automatically enables IPSec protection for the L2TP tunnel. We do not have to define IPSec filters in this case because Windows 2000 automatically protects the data transmitted through the L2TP tunnel by enabling IPSec ESP protection.

In this scenario communication could originate from either end of the VPN therefore L2TP must be implemented at both the BOSTON OU and the FABRIKAM domain.

Incorrect Answers:

A: We would want to implement L2TP to secure communitation across the VPN, however, communication could originate from either end of the VPN therefore L2TP must be implemented at both the BOSTON OU and the FABRIKAM domain.

C: PPTP is commonly used to support for down-level clients, such as Windows 95, Windows 98, and Windows NT 4.0 clients and to transmit secured communication across a firewall or perimeter network that performs Network Address Translation an the NAT process are not protected by the MPPE encryption. However, PPTP does not support the authentication of the computers used in the remote access connection. If MS-CHAPv2 is used, then the user account and the computer account of the remote access server are authenticated, but the computer account of the remote access client computer is not authenticated. Furhtermore, L2TP provides a higher level of encryption than PPTP.

D: PPTP is commonly used to support for down-level clients, such as Windows 95, Windows 98, and Windows NT 4.0 clients and to transmit secured communication across a firewall or perimeter network that performs Network Address Translation an the NAT process are not protected by the MPPE encryption. However, PPTP does not support the authentication of the computers used in the remote access connection. If MS-CHAPv2 is used, then the user account and the computer account of the remote access server are authenticated, but the computer account of the remote access client computer is not authenticated. Furhtermore, L2TP provides a higher level of encryption than PPTP.

Q. 4
How should you protect the Internet interface on the Miller Textiles VPN server from unauthorized users?

A. Use Routing and Remote Access filters on the Internet interface of the VPN server
B. Use Routing and Remote Access filters on the internal interface of the VPN server
C. Disable dynamic DNS updates on the internal interface of the VPN server
D. Disable dynamic DNS updates on the Internet interface of the VPN server

Answer: A
Explanation:
IP and IPX packet filters on the demand-dial interface can be used to restrict the types of traffic that are allowed in to and out of the interface. IP and IPX packet filtering only occurs when the demand-dial interface is in a connected state. Packet filtering is especially useful for an extranet, a portion of your private intranet that is accessible to business partners over demand-dial connections. In addition to demand-dial interface packet filtering, TCP/IP packet filters can be configured on the profile of the remote access policy configured for calling routers. While primarily designed to restrict the traffic of remote access connections, remote access policy profile–based TCP/IP packet filters can be used for demand-dial routing. Rather than configure the same IP packet filters on many demand-dial interfaces, if all the demand-dial connections share the same IP packet filters and remote access policy, then remote access policy profile packet filters allow you to configure the IP packet filters once for all the demand-dial connections. This configuration would be applied on the Internet interface of the VPN server.

Incorrect Answers:
B: To increase the security on the VPN we would configure the VPN server to use only Routing and Remote Access. This will however be configured on the Internet interface and not the internal interface.
C: DNS is used to translate domain names to IP addresses. It is thus a map of the internal structure of the Since DNS can reveal the internal structure of your network to a potential attacker, security within your DNS infrastructure is an important. DNS services available on the Internet could expose the internal IP addressing scheme of the internal network. We should therefore not allow DNS services to cross the Internet. This however will not secure access to the Internet interface on the VPN server.

D: DNS is used to translate domain names to IP addresses. It is thus a map of the internal structure of the Since DNS can reveal the internal structure of your network to a potential attacker, security within your DNS infrastructure is an important. DNS services available on the Internet could expose the internal IP addressing scheme of the internal network. We should therefore not allow DNS services to cross the Internet. This however will not secure access to the Internet interface on the VPN server.

Q. 5
How should you authenticate users from Fabrikam, Inc who access Miller Textiles network over the VPN?

A. Use the fully qualified domain name (FQDN) and password
B. Use certificate-based authentication
C. Use EAP
D. Use Internet Authentication Service (IAS)

Answer: A
Explanation:
Fabrikam and Miller Textiles exist in a trust relationship as the Farikam domain and the BOSTON OU have a trust relation. We would therefore use the FQDN and a password for authenticaton purposes. This will allow us to authentcate the computer that is used in creating the connection.

Incorrect Answers:
B: Certificate based authentication is the process of establishing trust relations through exchange of keys. Fabrikam and BOSTON OU already exist in a trust relation. We therefore do not require cetificates.
C: EAP provides extensions to dial-up and VPN connections. These extensions provide two-factor authentication by using devices such as smart cards to provide network credentials. EAP uses Transport Layer Security (TLS) to secure the authentication process. EAP provides mutual authentication, negotiation of encryption methods, and secured key exchange between the Network Access Server (NAS) and the remote access client. EAP requires that both the remote access client and the NAS run Windows 2000 and that a Public Key Infrastructure (PKI) is deployed to provide certificates for both the NAS and the remote access clients. In this scenario both Fabrikam and Miller Textiles use Windows 2000 computers, however, the two domain exist in a trust relationship as the Farikam domain and the BOSTON OU have a trust relation. We would therefore use the FQDN and a password for authenticaton purposes. This will allow us to authentcate the computer that is used in creating the connection.
D: Windows 2000 Server includes Internet Authentication Service (IAS) as an optional component. This service implements an industry-standard network authentication security protocol, Remote Authentication Dial-In User Service (RADIUS), which allows centralization of account authorization. RADIUS also allows you to specify how long the session can last and what IP address can be used. IAS can also record session details, providing accountability, and reporting options. IAS authenticates accounts against native Windows 2000 domains and Windows NT 4.0 domains. However, Fabrikam has

its own unique Active Directory schema and thus exists in a forest part from Miller Textiles. We therefore cannot use IAS for authentication.

Q. 6
How should you assign the authority for adding new user accounts at Miller Textiles after the upgrade?

A. Create one administrative group at the BOSTON organizational unit (OU) with the authority to create new users at each OU
B. Delegate authority to a domain administrator at each organizational unit (OU) to create new users for all OUs
C. Delegate authority to a domain administrator at the BOSTON organizational unit (OU) to create new users at each OU
D. Create a new administrative group at each organizational unit (OU) with the authority to create new users at that OU

Answer: D
Explanation:
In the existing IT network, each manufacturing facility has employees who administer its OU. In addition, in the envisioned IT environment, the engineering department and the manufacturing department will have their own organizational unit (OU) at each manufacturing facility and headquarters IT employees located at each manufacturing facility will administer the OU for that manufacturing facility. The OU administrators will have full control of all folders on all servers within their OUs. Therefore we must create an administrative group at each organizational unit (OU) with the authority to create new users at that OU.

Incorrect Answers:
A: IT employees located at each manufacturing facility will administer the OU for that manufacturing facility. This would include the addition of used accounts. Therefore we cannot centralize the authority to create new users at each OU at the BOSTON organizational unit (OU).
B: By default, domain administrators have the authority to create user accounts. It is thus not necessary to delegate that authority to the domain administrators. However, the IT employees in the OUs must be granted the authority to create user accounts in their respective OUs.
C: By default, domain administrators have the authority to create user accounts. It is thus not necessary to delegate that authority to the domain administrators. However, the IT employees in the OUs must be granted the authority to create user accounts in their respective OUs. Therefore we cannot centralize the authority to create new users at each OU at the BOSTON organizational unit (OU).

Q. 7
Which two security components should you use on the portable computers? (Choose two)

A. Internet Authentication Service (IAS)
B. PPTP
C. Remote access policy
D. L2TP over IPSec
E. Remote Authentication Dial-In User Service (RADIUS)
F. Encrypting File System (EFS)

Answer: D, F
Explanation:
According to the Sales Director, IT Director, the customer information on the sales representatives' portable computers must be secure. These computers will have a folder that stores confidential customer information and must be secured and encrypted. This folder will be updated when the sales representatives dial in to Headquarters. The sales representatives will primarily use VPN to dial in to Headquarters. This connection must therefore also be secure.

To secure the dial in connection to Headquarters, we would implement L2TP over IPSec to secure communication between the portable computers and Headquarters. L2TP is a method of providing VPN access to the network. It can be used to provide both client-to-server and server-to-server access. Although L2TP does not include an encryption mechanism, IPSec is used to negotiate a security association between the two computers using the L2TP tunnel. IPSec then provides the encryption. Thus, whenever the L2TP is used to establish a VPN, Windows 2000 automatically enables IPSec protection for the L2TP tunnel. We therefore do not have to define IPSec filters in this case because Windows 2000 automatically protects the data transmitted through the L2TP tunnel by enabling IPSec ESP protection

To secure the data in the folder we should ensure that EFS is implemented. EFS is used to encrypt files and folders on NTFS volumes. When a user encrypts a file or folder, only that user will be able to access the file or folder. The data in the confidential folder should be encrypted to ensure that only the owner of the portable computer can access the files in it. This will secure the data in the event that the portable computer is stolen.

Incorrect Answers:
A: Windows 2000 Server includes Internet Authentication Service (IAS) as an optional component. This service implements an industry-standard network authentication security protocol, Remote Authentication Dial-In User Service (RADIUS), which allows centralization of account authorization. RADIUS also allows you to specify how long the session can last and what IP address can be used. IAS can also record session details, providing accountability, and reporting options. However, in this scenario the sales representatives will connect to Headquarters via VPN. VPN requires that the sales representatives first create a connection to an ISP. We therefore cannot specify which IP addresses can be used to connect to VPN.
B: It is possible to use PPTP to secure the transmission. However, PPTP cannot authenticate computer accounts. It can only authenticate user accounts. In addition, L2TP provides higher levels of encrypted transmissions.

C: Remote Access Policy is set on the Windows 2000 server that functions as a remote access server. These policies establish whether a server accepts requests for remote access and, if so, during what hours of what days, what protocols are used, and what types of authentication are required. This, however, cannot be used to secure connections between the remote access client and the server.

E: RADIUS is similar to IAS. It allows centralized authentication, accounting, and management of remote access policy.

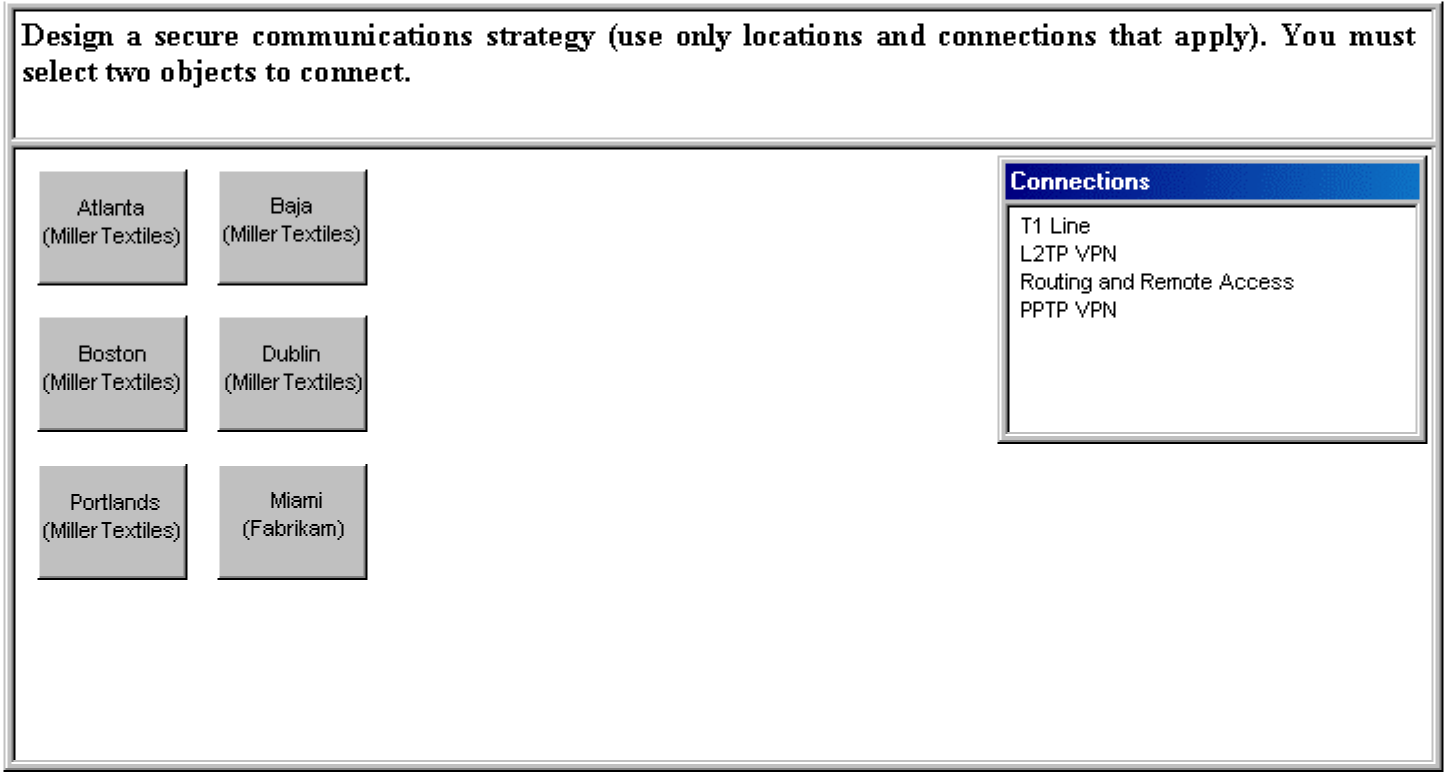
Q. 8

For the Miller Textiles sales representatives how should you implement Encrypting File System (EFS) on the portable computers to allow central recovery?

A. Create enterprise root CAs at the BOSTON, ATLANTA, BAJA, and DUBLIN organizational units (OUs). Define the recovery agent at the OU level.
B. Use a third-party CA. Use the third party as the recovery agent.
C. Use a self-signed certificate. Define the local administrator as the recovery agent.
D. Create an enterprise root CA at the BOSTON organizational unit (OU), and create enterprise subordinate CAs at the ATLANTA, BAJA, and DUBLIN OUs. Define the recovery agent at the domain level

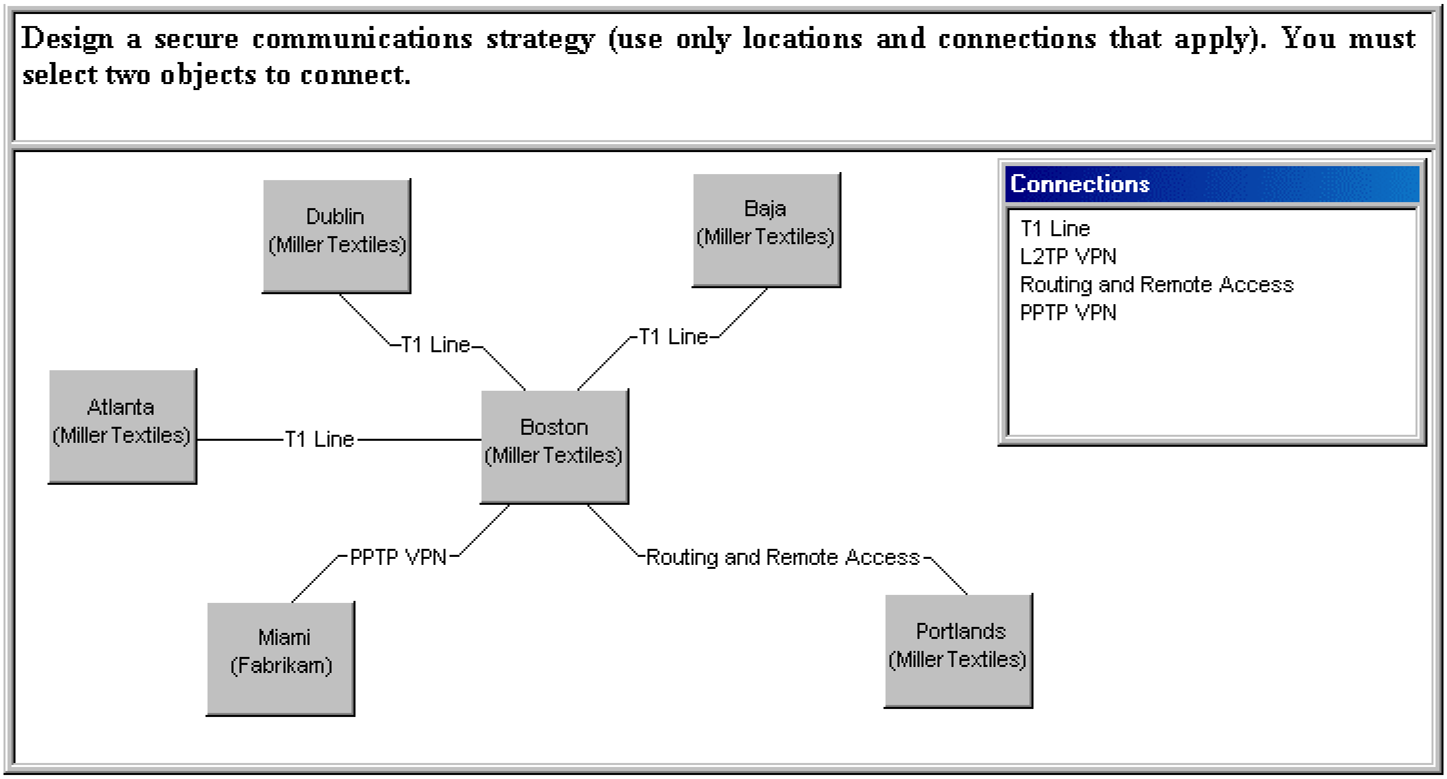
Answer: D
Explanation:

Q. 9



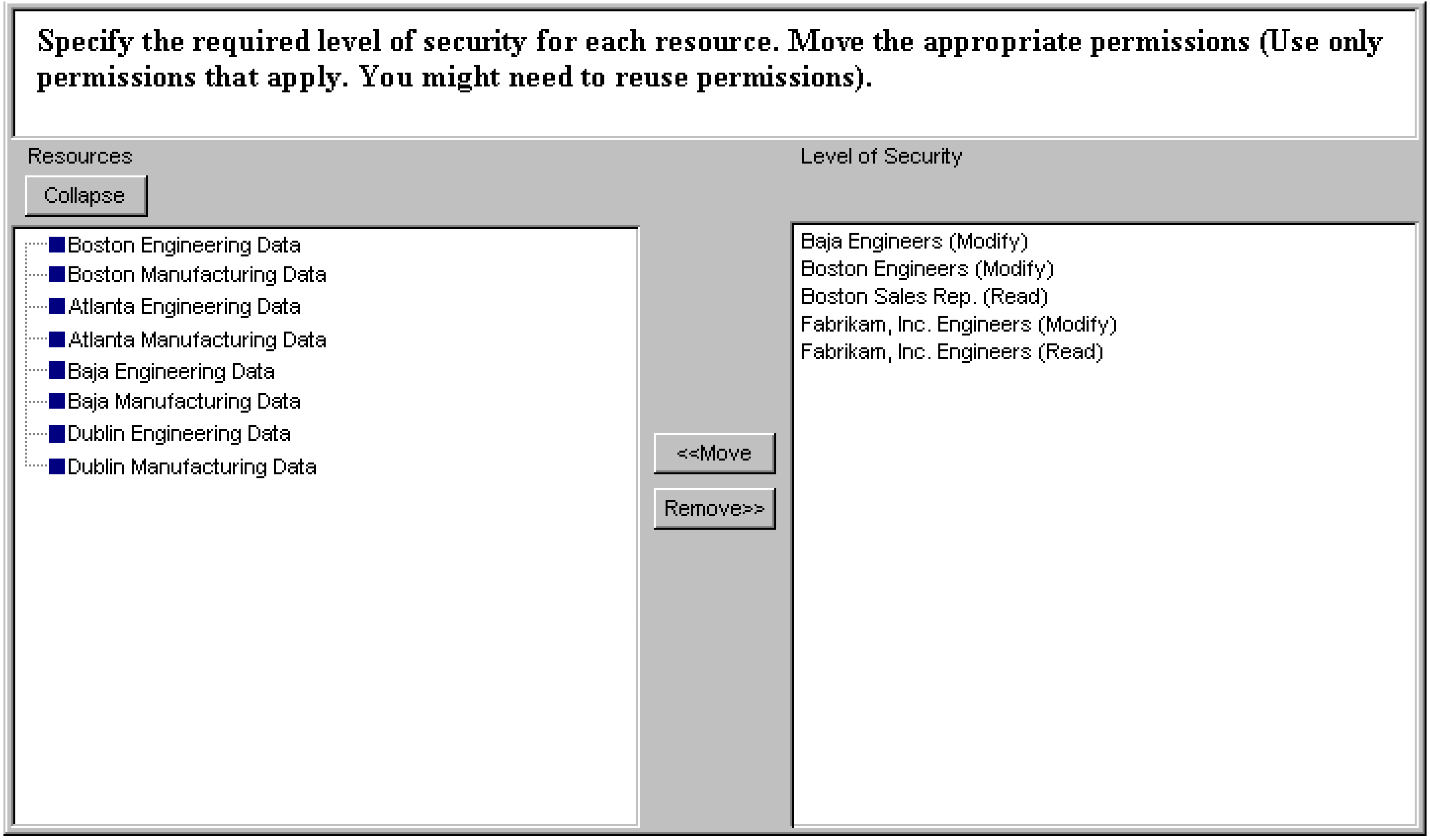
Design a secure communications strategy (use only locations and connections that apply). You must select two objects to connect.

Answer:



Design a secure communications strategy (use only locations and connections that apply). You must select two objects to connect.

Q. 10



Specify the required level of security for each resource. Move the appropriate permissions (Use only permissions that apply. You might need to reuse permissions).

Resources

Collapse

- ■Boston Engineering Data
- ■Boston Manufacturing Data
- ■Atlanta Engineering Data
- ■Atlanta Manufacturing Data
- ■Baja Engineering Data
- ■Baja Manufacturing Data
- ■Dublin Engineering Data
- ■Dublin Manufacturing Data

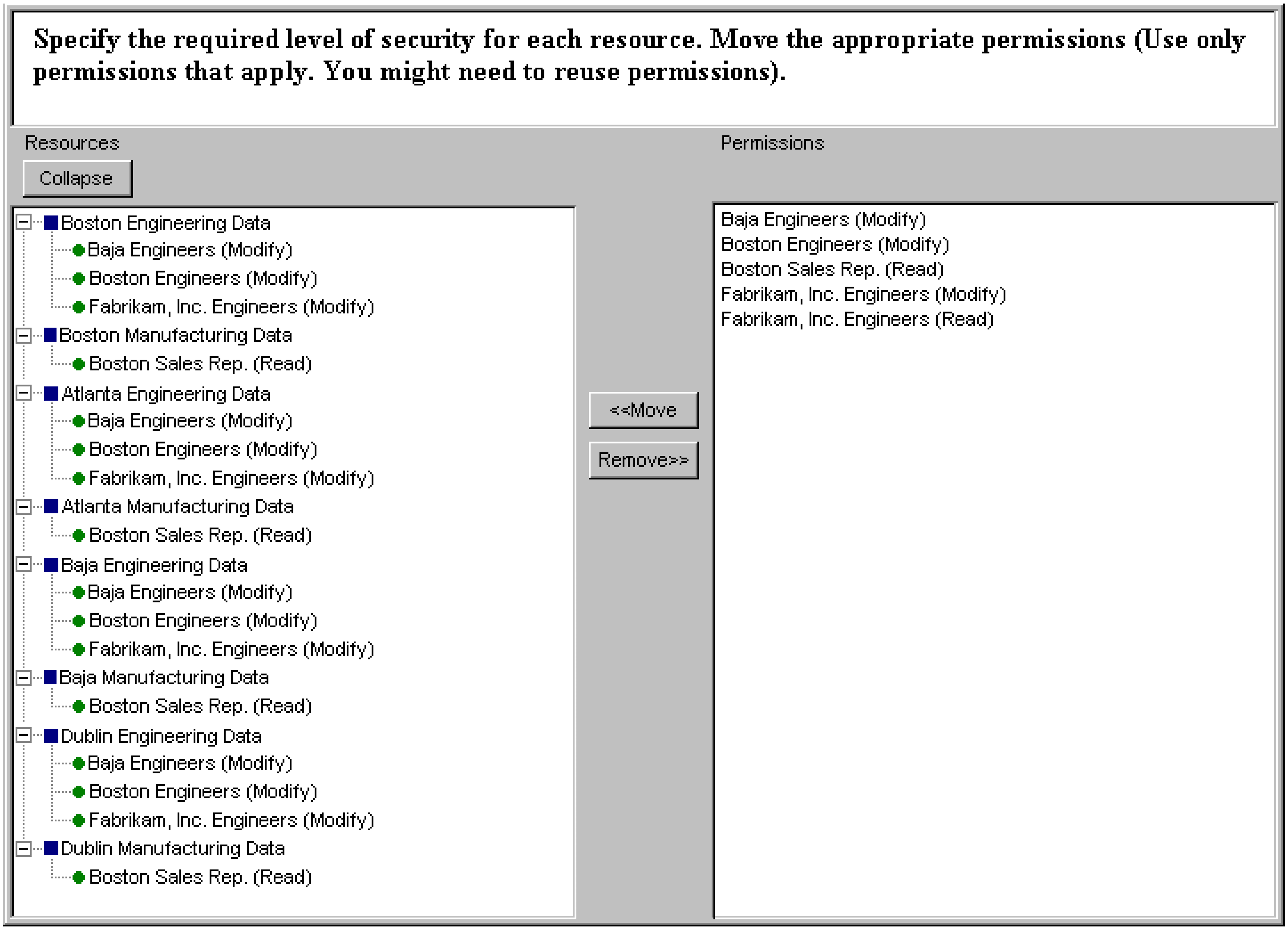
<<Move

Remove>>

Level of Security

Baja Engineers (Modify)
Boston Engineers (Modify)
Boston Sales Rep. (Read)
Fabrikam, Inc. Engineers (Modify)
Fabrikam, Inc. Engineers (Read)

Answer:



Specify the required level of security for each resource. Move the appropriate permissions (Use only permissions that apply. You might need to reuse permissions).

- ■ Boston Engineering Data
  - ● Baja Engineers (Modify)
  - ● Boston Engineers (Modify)
  - ● Fabrikam, Inc. Engineers (Modify)
- ■ Boston Manufacturing Data
  - ● Boston Sales Rep. (Read)
- ■ Atlanta Engineering Data
  - ● Baja Engineers (Modify)
  - ● Boston Engineers (Modify)
  - ● Fabrikam, Inc. Engineers (Modify)
- ■ Atlanta Manufacturing Data
  - ● Boston Sales Rep. (Read)
- ■ Baja Engineering Data
  - ● Baja Engineers (Modify)
  - ● Boston Engineers (Modify)
  - ● Fabrikam, Inc. Engineers (Modify)
- ■ Baja Manufacturing Data
  - ● Boston Sales Rep. (Read)
- ■ Dublin Engineering Data
  - ● Baja Engineers (Modify)
  - ● Boston Engineers (Modify)
  - ● Fabrikam, Inc. Engineers (Modify)
- ■ Dublin Manufacturing Data
  - ● Boston Sales Rep. (Read)

Baja Engineers (Modify)
Boston Engineers (Modify)
Boston Sales Rep. (Read)
Fabrikam, Inc. Engineers (Modify)
Fabrikam, Inc. Engineers (Read)

Case Study No: 5

CONTOSO LTD.

Background

Contoso Ltd. is a wholly owned subsidiary of A.Datum Corporation, a large financial services company primarily dealing in life insurance. Contoso Ltd. is creating a web site that will allow insurance brokers to configure an insurance policy, receive a quotation for that policy and purchase the policy. When orders are placed the actual creation and delivery of the policy will be handled by a third-party fulfillment company.

The web site is designed to serve independent insurance brokers who are not employed by Contoso or A.Datum. Although there is a public section with content describing Contoso Ltd. and its products in general terms most of the web site is restricted to use only by brokers and policyholders. Brokers must register with Contoso before they can use web site.

Some of the policies that are sold by Contoso allow policyholders to allocate the value of the policy into various investment options. A policyholder can view the current allocation and make changes online in accordance with well-defined rules. Policyholders cannot buy new policies or terminate existing policies without the aid of a broker. They can change the allocation of funds in existing policies every three months.

Problem:

Vice President of Sales (A.Datum Corp.):

Although our company has been successful with traditional approaches to the financial market we are beginning to loose some of our customers especially in the area of web based service offerings. The new web site and its complement of web-based products will help us to maintain our existing customers and attract new customers. The brokers I have spoken with do not want many extra features but they are concerned about other brokers accessing their information. In addition they do not want to hire a computer expert just to be able to use this site.

The financial industry has shown leadership in adopting new technologies and these brokers are willing to embrace this new approach. They will not insist on personal assistance if we provide them with online resources to guide them. Depending on the success of this project we might attempt more projects like this one or we might sell the entire company.

Chief Information Officer (Contoso Ltd.):

Although the web site is viewed as distinctly separate from A.Datum Corp., we still must report results to them at frequent intervals especially during the first year. We also must allow A.Datum to check the status of this site any time. In addition the Vice President of Sales, the IS Director and myself are required to keep up to date with developments at A.Datum. We have user accounts on A.Datum’s network for this purpose.

IS Director (Contoso Ltd.):
We have been given a mandate to develop and implement a web site that will act as a virtual insurance company. The development work is already in progress. We have chosen Windows 2000 as our platform and we are developing a multi-tier Windows DNA insurance application.

In addition to the insurance application the web site will also include content describing the company and its products. We need to create this site and a network environment to run it on with only six servers. Our primary focus now is to ensure that the site is secure and to effectively audit who is using the site. We have three distinct categories of users: brokers, policyholders and employees from both Contoso and A.Datum. There are further subdivisions within these categories.

Lead Developer (Contoso Ltd.):
In the past when we needed to control access to web sites we usually just stored user-ids and passwords in a MS SQL Server database. Although this was easy to implement we have always recognized shortcomings with this approach. We want to take advantage of the Public Key Infrastructure (PKI) security features in Windows 2000 to provide increased security.

Logistics Manager (Contoso Ltd.):
During an initial enrolment period we will be actively signing up new brokers to use this site. Based on our research there might be up to 5000 brokers during this period. After the enrolment period we expect a relatively small number of brokers to join or leave on a daily basis. We have only one or two people that will manage memberships, but we can hire temporary employees during the initial enrolment period. Certification registration and delivery will be handled off-line. Brokers must register for a certificate either in person or by telephone. After Contoso employees verify a broker’s identity and create a client certificate it will be delivered on floppy disk or CD through a secure courier service.

Envisioned IT Environment:

Servers:
All servers for this site will exist within a single domain. Six servers will be used for the initial rollout for this site. CONTWEB1 will be used as the web server. This server runs Internet Information Services (IIS) and mid-tier COM-components that will be designed specifically for the insurance application. CONTDATA will be used as the database server. This server will run MS SQL Server 7.0. CONTDC will be a domain controller and certificate server and it will run DNS, WINS and DHCP. CONTVPN, a multi-homed server, will be used to create a VPN to A.Datum Corp. through the Internet. CONTWEB2 will be used as an intranet web server, as a file and print server for employees of Contoso and a domain controller. CONTFIRE will be used as a firewall server. It will run third-party firewall software.

Local Client Computers:
A primary objective of the project is to minimize the employees needed to support this virtual insurance company. It is estimated that there will be fewer than 20 people associated with this project and its site. This includes employees for office administration, creating the web content, designing new insurance products and sales and marketing. Fewer than 5 employees will use portable computers and might require remote access when they travel. The other employees will use desktop computers

Internet Client Computers:
Brokers will connect to this site over the Internet. Because it is anticipated that they will generally have a limited technical background any set-up process needed for this site must be easy to follow. The target audience for this site is a relatively static group of users who are expected to use the site regularly. Most of this site will not be available to the public. Therefore the site will be designed specifically for Internet Explorer 4.0 or later. The public section of this site will designed for both Internet Explorer and Netscape browsers

Administration:
A small group of people will handle the administration of this site, such as updating content and providing maintenance for the application. In general they will perform these tasks directly on the servers or from a locally connected desktop computer.

LAN:
A new LAN is being created to host the web site. All necessary services such as DNS will be provided by Windows 2000 Server computers on the LAN. Two Class C address spaces have been acquired. One will be used for publicly visible servers and the other one will be used for internal computers that should not be accessed from the Internet. Network address translation (NAT) will not be used. All desktop computers will run Windows 2000 Professional.

WAN:
Contoso Ltd. will host this site at its office, which is a separate company owned facility dedicated to the project. It will not be directly connected to A.Datum Corp's WAN; instead a VPN connection through the Internet will be used. A.Datum has already begun the process of upgrading to Windows 2000 at its headquarters.

Internet Connectivity:
Contoso has secured a domain name CONTOSO.COM to use for the site. A single T3 line has been leased to provide Internet connectivity.

Questions Contoso Ltd.

Q. 1
What is Contoso Ltd.'s tolerance for risk? (Choose one)

A. Contoso Ltd. is willing to try some new approaches.
B. Contoso Ltd. is comfortable with a high level of risk.
C. Contoso Ltd. is willing to risk the entire company for large rewards.
D. Contoso Ltd. is willing to try only those approaches that they have successfully implemented before.
E. Contoso Ltd. is very conservative and does not take any chances.

Answer: A
Explanations:
According to the Vice President of Sales, the Financial Industry has show leadership in adopting new technologies. Contoso Ltd is prepared to embrace this new approach.

Incorrect Answers:
B: Contoso Ltd is not comfortable with a high level of risk. Instead they will review the new web-bases project and either attempt more projects like this or might sell the entire company.
C: Contso Ltd is not prepared to risk the entire company. It has not placed all its resources in the new project but will maintain its existing operation.
D: According to the Vice President of Sales, the Financial Industry has show leadership in adopting new technologies. Contoso Ltd is prepared to embrace this new approach. In other words, these are new approaches that Contoso Ltd has not implemented before.
E: According to the Vice President of Sales, the Financial Industry has show leadership in adopting new technologies. Contoso Ltd is prepared to embrace this new approach. In other words, Contoso Ltd. is not conservative and is prepared to take chances.

Q. 2
What is the primary security risk for the desktop computers at Contoso Ltd.? (Choose one)

A. Another Contoso Ltd. employee connected to a desktop computer via the LAN.
B. Denial-of-service attack launched from the internet targeting a desktop computer.
C. Remote hackers directly connected to a desktop computer via the internet.
D. Remote hackers directly connected to a desktop computer via modem.

Answer: A
Explanation:

In the envisaged IT environment, only the servers will be visible on the internet. Te internal LAN will have a different Class C address space. The desktop computers will thus not be accessible from the internet. Therefore the only security risk for the desktop computers is an unauthorized employee connecting to the desktop computers via the LAN.

Incorrect Answers:

B: In the envisaged IT environment, only the servers will be visible on the internet. Te internal LAN will have a different Class C address space. The desktop computers will thus not be accessible from the internet. Therefore the desktop computers are not susceptible to denial-of-service attacks launched trough the Internet.

C: In the envisaged IT environment, only the servers will be visible on the internet. Te internal LAN will have a different Class C address space. The desktop computers will thus not be accessible from the internet. Therefore there is little chance of a remote hacker gaining access to the desktop computers.

D: In the envisaged IT environment, only the servers will be visible on the internet. Te internal LAN will have a different Class C address space. Furthermore, Contoso Ltd. will not be making use of a Routing and Remote Service (RRAS). Remote clients can only access a network through a direct modem connection when RRAS is implemented. It is not in this scenario.

Q. 3
How should you design the active directory structure for Contoso Ltd.? (Choose one)

A. Create a single domain in its own forest. Do not establish trust relationships.
B. Create a single domain in its own forest. Establish a one-way trust relationship with A.Datum
C. Create one child domain. Place the child domain in the same forest as A.Datum's domain tree.
D. Create one domain in its own domain tree. Place the domain tree within the same forest as A.Datum's domain tree.

Answer: B
Explanation:
As all the servers will exist within a single domain, we will have to create a forest that consists of a single domain. In addition, we need to give A.Datum Corp access to the site at anytime. For this purpose Contoso Ltd has user accounts on the A.Datum network. Contoso Ltd, however, does not need to access the A.Datum network. Therefore we need implement only a one-way trust with A.Datum.

Incorrect Answers:

A: As all the servers will exist within a single domain, we will have to create a forest that consists of a single domain. However, we need to give A.Datum Corp access to the site at anytime. For this purpose Contoso Ltd has user accounts on the A.Datum network. Contoso Ltd, however, does not need to access the A.Datum network. We therefore must implement a one-way trust with A.Datum.

C: The Web site is viewed as distinctly separate from A.Datum Corp therefore we would not place the Contoso.com as a child of the A.Datum domain tree.

D: The Web site is viewed as distinctly separate from A.Datum Corp therefore we would not place the Contoso.com in the same forest as the A.Datum domain tree.

Q. 4
Which three options should you include in a security template for CONTWEB1? (Choose three)

A. Rename the administrator account.
B. Allow CD-ROM access to all users.
C. Limit CD-ROM access to users who are logged on locally.
D. Enforce strong passwords.
E. Set the NTLM authentication level to LM and NTLM.
F. Disable account lockout.

Answer: A, D, E
Exlanation:
The Administrator account is a default account. Therefore it is a known user account that hackers can use to attempt to gain access to a server through brute force or dictionary attacks. By renaming the Administrator account this option is not available.

To reduce the effectiveness of dictionary attacks we should implement complex passwords that contain letters and digits.

Furthermore, because the CONTWEB1 server is an IIS server, it will be access via the internet. We must therefore ensure that the users that access the IIS are authenticated. While Kerberos is used automatically for authentication on Windows 2000 computers we need to implement a authentication protocol that will support down-level computers as well. We should therefore use NTLM.

Incorrect Answers:

B: The use of the CD-Rom would not be crucial to the operation of the server therefore we do not need to configure any security setting for the CD-Rom.

C: The use of the CD-Rom would not be crucial to the operation of the server therefore we do not need to configure any security setting for the CD-Rom.

F: Account lockout is a mechanism that monitors the successive failed attempts to logon to the network. When a user does not provide the correct password after a certain number of consecutive tries, this mechanism assumes that a hacker is using the account name to try to gain access to the network and disables the user account. That account then cannot be used for subsequent logon attempts unless the Administrator clears the lockout.

Q. 5
Which technology or technologies should you implement to provide the highest level of security for communications between employees of A.Datum and Contoso Ltd.? (Choose one)

A. Internet authentication services (IAS) and NTLM authentication.
B. PPTP
C. SSL, digital certificates, and directory services (DS) mapping.
D. Basic authentication with SSL.
E. L2TP over IPSec

Answer: B
Explanation:
Contoso and A.Datum are two distinct entities that will be connected across the Internet via a VPN. To secure network communication across the Internet we would normally use L2TP over IPSec. However, Contoso will be implementing a firewall on a server named CONTFIRE. L2TP cannot pass network traffic through a firewall. PPTP is supported by Windows 95, Windows 98, Windows NT 4.0, and Windows 2000 remote access clients. PPTP uses MPPE to provide encryption of the transmitted data. MPPE can use 40-bit, 56-bit, or 128-bit encryption keys and can pass network traffic through a firewall. However, we must configure the firewall to allow the PPTP packets to pass through the firewall. Furthermore, A.Datum has began to upgrade their computers to Windows 2000. This means that they still have Windows NT 4.0. Kerberos, which is used pervasively as an authentication protocol in Windows 2000, is not supported on Windows NT 4.0 computers. We would therfore require NTLM which provides support of down-level computers.

Incorrect Answers:

A: Windows 2000 Server includes Internet Authentication Service (IAS) as an optional component. This service implements an industry-standard network authentication security protocol, Remote Authentication Dial-In User Service (RADIUS), which allows centralization of account authorization. RADIUS also allows us to specify how long the session can last and what IP address can be used. IAS can also record session details, providing accountability, and reporting options. IAS authenticates accounts against native Windows 2000 domains and Windows NT 4.0 domains. However, A.Datum and Contoso are two distinctly different entities for which we will establish a trust relationship. A trust relationship is a link between at least two domains in which the trusting domain honors the logon authentication of the trusted domain. User accounts and groups defined in a trusted domain can be given rights and resource permissions in a trusting domain, even though those accounts do not exist in the trusting domain's directory database. We therefore would not require any further authentication.

C: We will establish a trust relation between A.Datum and Contoso. A trust relationship is a link between at least two domains in which the trusting domain honors the logon authentication of the trusted domain. User accounts and groups defined in a trusted domain can be given rights and resource permissions in a trusting domain, even though those accounts do not exist in the trusting domain's directory database. We therefore would not require any further authentication.

D: Basic Authentication is used to support Internet connections. A.Datum will however use VPN to connect to Contoso. Furthermore, we will establish a trust relation between A.Datum and Contoso. A trust relationship is a link between at least two domains in which the trusting domain honors the logon authentication of the trusted domain. User accounts and groups defined in a trusted domain can be given rights and resource permissions in a trusting domain, even though those accounts do not exist in the trusting domain's directory database. We therefore would not require any further authentication.

E: Contoso and A.Datum are two distinct entities that will be connected across the Internet via a VPN. To secure network communication across the Internet we would normally use L2TP over IPSec. However, Contoso will be implementing a firewall on a server named CONTFIRE. L2TP cannot pass network traffic through a firewall.

Q. 6
How should you separate intranet resources from publicly visible internet servers? (Choose one)

A. Use a private IP address space. Configure both the internal DNS and the authoritative internet based DNS server to resolve both internal and external names.

B. Use corp.contoso.com as a suffix for all internal sites. Configure both the internal DNS and the authoritative internet based DNS server to resolve both internal and external names.

C. Use corp.contoso.com as a suffix for all internal sites. Configure the internal DNS to resolve internal names, but do not include these names in the authoritative internet based DNS server.

D. Use a private IP address space. Configure the authoritative internet based DNS server to resolve internal names, but do not include these names on the internal DNS server.

Answer: C
Explanation:
To ensure the security of the intranet, we would want to separate the intranet from the Internet site. To do this we would create a separate domain for the intranet. However, in envisaged IT environment, we will be creating a single domain. We would thus have to create a child domain for the intranet as the Internet site would use the root domain name space. We would also want to prevent the Internet based DNS sever from resolving internal name resolution queries. We will therefore configure the internal DNS to resolve internal names, but do not include these names in the authoritative internet based DNS server. In so doing no internal name resolution queries will pass on to the Internet DNS based DNS server. Internal name resolution will thus remain within the intranet.

Incorrect Answers:

A: Windows 2000 networks are based on domain namespace and nor IP address namespace. Furthermore, by configuring both the internal DNS and the authoritative internet based DNS server to resolve both internal and external names, we would allow internal name resolution to be performed by the Internet based DNS. This represents a security risk as the Internet based DNS is accessible from the Internet.

B: To ensure the security of the intranet, we would want to separate the intranet from the Internet site. To do this we would create a separate domain for the intranet. However, in envisaged IT environment, we will be creating a single domain. We would thus have to create a child domain for the intranet as the Internet site would use the root domain name space. However, by configuring both the internal DNS and the authoritative internet based DNS server to resolve both internal and external names, we would allow internal name resolution to be performed by the Internet based DNS. This represents a security risk as the Internet based DNS is accessible from the Internet.

D: Windows 2000 networks are based on domain namespace and nor IP address namespace. We would however want to prevent the Internet based DNS sever from resolving internal name resolution queries. We will therefore configure the internal DNS to resolve internal names, but do not include these names in the authoritative internet based DNS server. In so doing no internal name resolution queries will pass on to the Internet DNS based DNS server. Internal name resolution will thus remain within the intranet.

Q. 7
Which technology or technologies should you include in your security strategy to secure broker access to the web site? (Choose one)

A. Basic authentication with SSL.
B. SSL, digital certificates, and directory services (DS) mapping.
C. Internet authentication services (IAS) and an ODBC database.
D. L2TP over IPSec

Answer: B
Explanation:
We would use the Secure Socket Layer (SSL) protocol to protect secure areas of the Web server as SSL encrypts all data transferred between the customer on the public network and the Web server. For authentication purposes, we will use certificates. According to the Logistics Manager, brokers will have to register with Contoso Ltd. They will then be given a certificate which they would use to access the Contoso web site. The use of certificates will prevent a user name and password from being intercepted as they are transmitted across the network. Only the certificate is transmitted across the network.This certification registration and delivery will occur offline. When the Web server receives the certificate and looks either at its own mapping table or at the mapping table in Active Directory to determine the user account associated with (or mapped to) the certificate. The certificate proves the user's identity. The easiest place to perform the mappings is in Active Directory. Because each account acquires its certificate from an Enterprise CA, there's no need to redo the same mappings that exist in Active Directory at the IIS server. By using Active Directory, we also ensure that the certificate mappings will not have to be reentered for an additional IIS server if the same certificate mappings are required for separate applications.

Incorrect Answers:

A: According to the Logistics Manager, brokers will have to register with Contoso Ltd. They will then be given a certificate which they would use to access the Contoso web site. This certification registration and delivery will occur offline. We would thus not be using Basic Authentication, which is the least secure form of authentication. It is inherently insecure as passwords are encoded but not securely encrypted. As a result, a simple network sniffer can watch for the HTTP authentication headers and Base64 decode this data to obtain the real password.

C: According to the Lead Developer, Contoso had previously used database verification of user-ids and passwords but have recognized the shortcomings of this approach. Contoso now wants to take advantage of the Public Key Infrastructure security features in Windows 2000.

D: Contoso will be implementing a firewall on a server named CONTFIRE. L2TP cannot pass network traffic through a firewall.

Q. 8
How should you implement a Public Key Infrastructure (PKI) for Contoso Ltd.? (Choose one)

A. Install an online enterprise root CA. Install an online enterprise subordinate CA. Import a self signed server certificate on the subordinate CA. Issue client certificates on the subordinate CA.

B. Install an offline stand alone root CA. Install an online stand alone subordinate CA. Issue client certificates on the root CA.

C. Install an online stand alone root CA. Import a server certificate from a third party CA to the root CA certificate trust list. Use client certificates from third party CA.

D. Install an offline enterprise root CA. Install an online enterprise subordinate CA. Issue client certificates on the subordinate CA.

Answer: D
Explanation:
Enterprise CAs are integrated with Active Directory and publish certificates and CRLs to Active Directory. They use certificate template information, user account information, and security group information that are stored in Active Directory to approve or deny certificate requests. For a certificate request to be approved, the user that requests the certificate must have Enroll permissions granted by the security Access Control Lists of the certificate template for the certificate type that is requested. When a certificate is issued, the enterprise CA uses information in the certificate template to generate a certificate with the appropriate attributes for that certificate type. Therefore Enterprise CAs can only issue certificates for users that have user accounts in Active Directory.

Furthermore, we can create a hierarchy of CAs. The CA at the top of a hierarchy is referred to as a root CA and the CAs below the root are referred to as subordinate CAs. The root CA is a very important point of trust in an organization as all certificates flow from the root. It issues its own certificate and the certificates for its subordinate CAs. We should therefore take the root CA offline once the subordinates have been granted certificates. The subordinates would then respond to certificate requests.

Incorrect Answers:

A: Enterprise CAs are integrated with Active Directory and publish certificates and CRLs to Active Directory. They use certificate template information, user account information, and security group information that are stored in Active Directory to approve or deny certificate requests. For a certificate request to be approved, the user that requests the certificate must have Enroll permissions granted by the security Access Control Lists of the certificate template for the certificate type that is requested. When a certificate is issued, the enterprise CA uses information in the certificate template to generate a certificate with the appropriate attributes for that certificate type. Therefore Enterprise CAs can only issue certificates for users that have user accounts in Active Directory.

Furthermore, we can create a hierarchy of CAs. The CA at the top of a hierarchy is referred to as a root CA and the CAs below the root are referred to as subordinate CAs. Subordinate CAs cannot issue their own certificates but receive their certificates from the root CA. The root CA is a very important point of trust in an organization as all certificates flow from the root. It issues its own certificate and the certificates for its subordinate CAs. We should therefore take the root CA offline once the subordinates have been granted certificates. The subordinates would then respond to certificate requests.

B: We would use stand-alone CAs if the organization will be issuing certificates to users or computers outside the organization. A stand-alone CA has a simple default policy module and does not store any information remotely. Therefore, a stand-alone CA does not need to have Active Directory available. In this scenario the brokers will be given domain membership. Therefore we would use an Enterprise CA.

C: We would use stand-alone CAs if the organization will be issuing certificates to users or computers outside the organization. A stand-alone CA has a simple default policy module and does not store any information remotely. Therefore, a stand-alone CA does not need to have Active Directory available. In this scenario the brokers will be given domain membership. Therefore we would use an Enterprise CA.

Q. 9
What should you include in an audit policy for CONTDC? (Choose all that apply)

A. Success and failure audit for object access.
B. Success and failure audit for directory services access.
C. Success and failure audit for policy change.
D. Success and failure audit for account management.
E. Success and failure audit for account logon events.

Answer: B, E
Explanation

Audit Directory Service Access is used to record information whenever a user gains access to an Active Directory object. To log this type of access, we must configure specific Active Directory objects for auditing. Active Directory provides the directory service in a Windows 2000 network. It stores information about network resources and makes the resources accessible to users and applications by uniquely identifying resources on a network

Audit Account Logon Events records information about any attempt to log on to a computer or server to gain access to the network. By auditing success and failure, we will record all attempted logons whether they are successful or not. This information can be used to determine which user accounts are being used to attempt to access the network

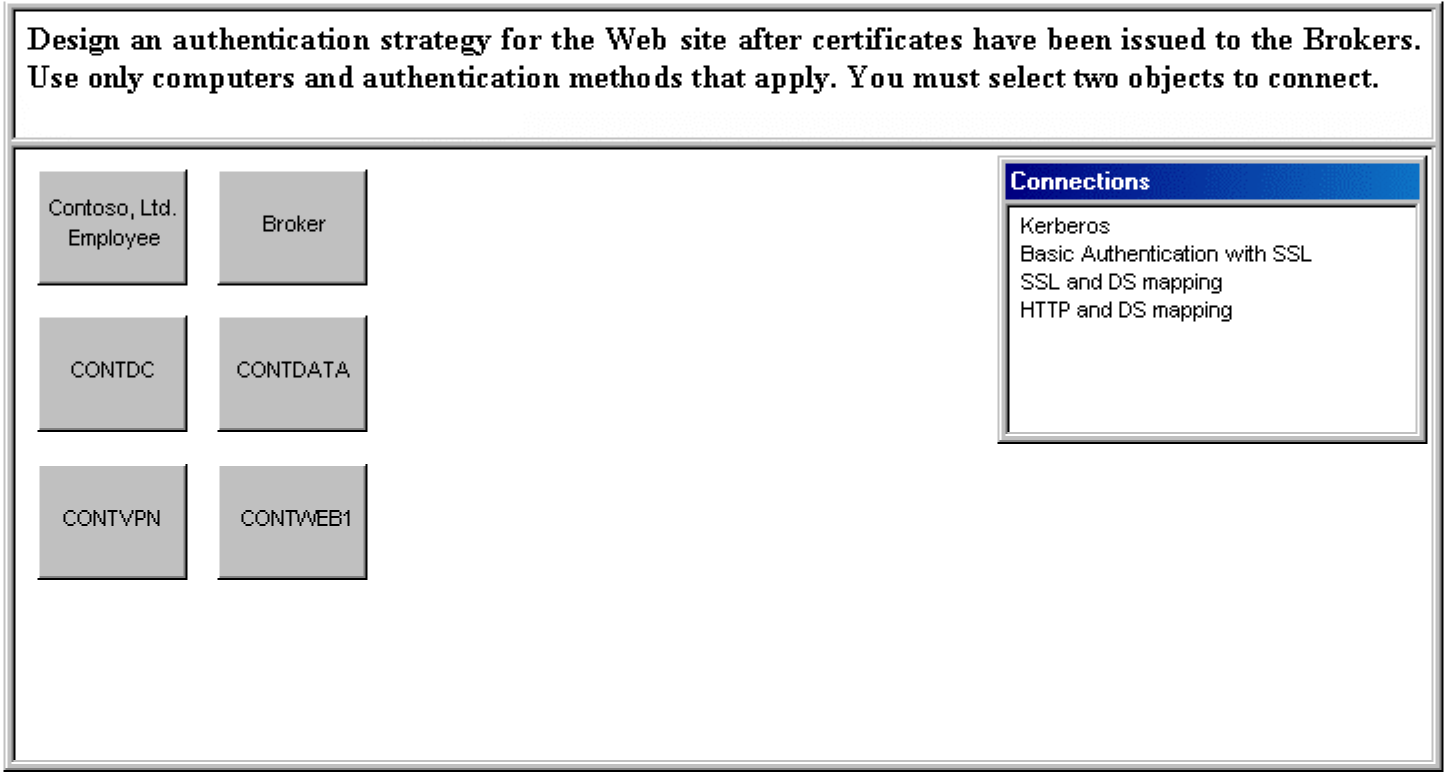
Incorrect Answers:

A: Files, folders and printers are called objects. By auditing successful and failed object access, enteries will recorded to a log when a user attempts to gain access to these objects. However, the administrator must configure which specific files and folders should be audited.

C: We can audit Policy Change to record events in which changes to the local policies are brought about through Group Policy.

D: By Auditing account management we can track the creation of user and computer accounts, the deletion of accounts and the modification of accounts.

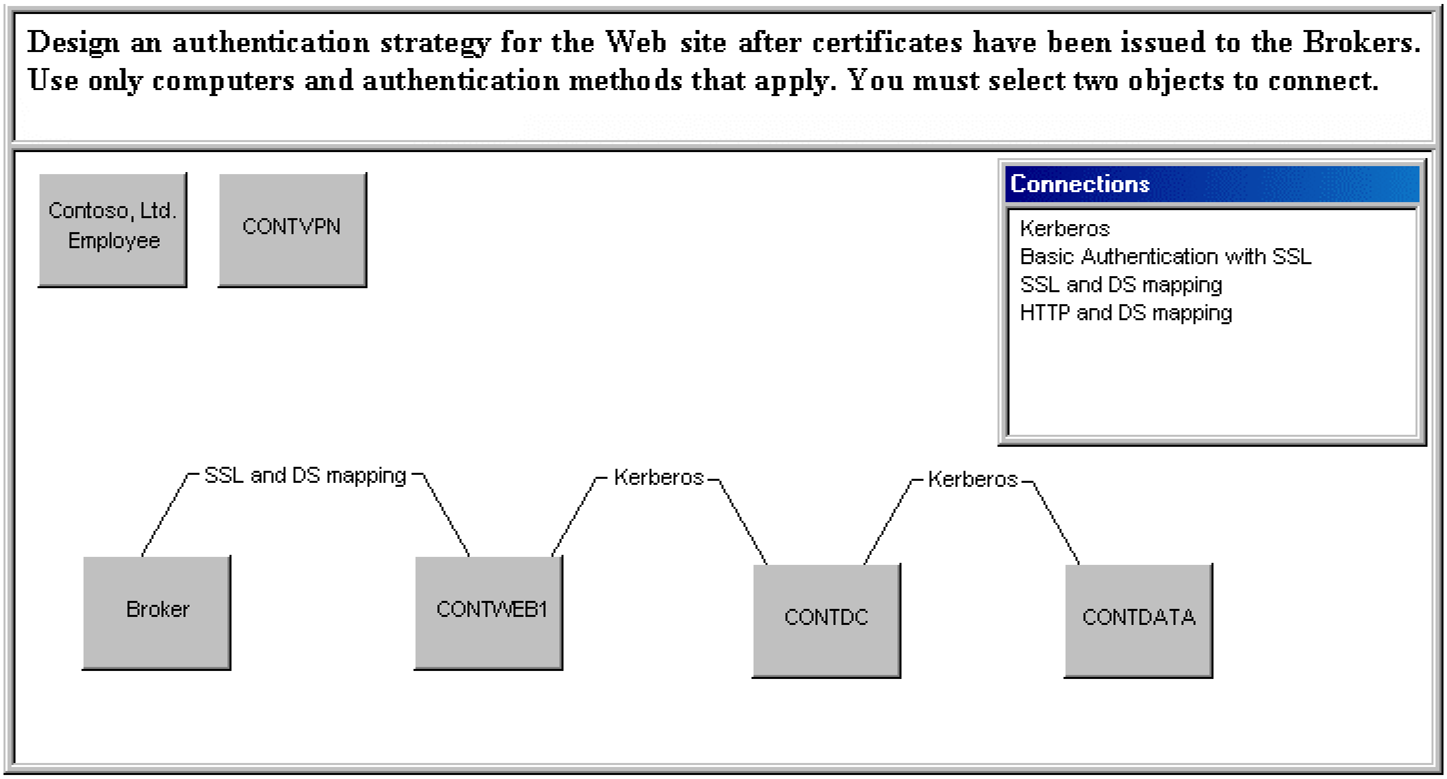
Q. 10



Design an authentication strategy for the Web site after certificates have been issued to the Brokers. Use only computers and authentication methods that apply. You must select two objects to connect.

Kerberos
Basic Authentication with SSL
SSL and DS mapping
HTTP and DS mapping

Answer:



Design an authentication strategy for the Web site after certificates have been issued to the Brokers. Use only computers and authentication methods that apply. You must select two objects to connect.

Leading the way in IT testing and certification tools, www.testking.com

Case Study No: 6

ENCHANTED LAKES CORPORATION

Background

Enchanted Lakes is a software-consulting firm. The annual growth rate of income for the company is 200%. The annual growth of office resources, which includes employees and computers, is 50%.

Headquarters:

The headquarters are located in Minneapolis, Minnesota. Headquarters, which employs approximately 300 people, includes Marketing, Sales, IT, HR, Executive, and Accounting departments. Approximately 250 of the 300 headquarters employees are consultants.

Branch Offices:

Branch offices are located in Copenhagen, Denmark, Des Moines, Iowa and Omaha, Nebraska. Each branch office employs 10-12 consultants and one office manager. Each office manager is also responsible for sales, marketing and HR for that specific office.

Existing IT Environment:

Computers:

The network at headquarters consists of 17 Windows 2000 Advanced Server computers and 250 Windows 2000 Professional client computers. The sales department has 2 Windows 2000 Server computers running MS SQL Server 7.0. Of the 250 client computers, 20 are desktop computers and 230 are portable computers.

The Marketing, IT and HR departments are equipped with desktop computers. All other departments are equipped with portable computers and the users have been granted dial-in permissions. Enchanted Lakes also maintains a dial-in server that resides inside a hardware-based firewall. The dial-in server is RAS1. Only employees have dial-up access. Headquarters also has a remote access server named VPN1. The company has an Internet Information Server (IIS) named TIME1. A program named TIME ENTRY is installed on this server. Consultants access this program to enter their hours of work for the week. Customers can access this program only to request resources. The company has also an Outlook Web Access (OWA) named OWA1. This server enables off-site employees to view email by using a web browser. Off-site employees can connect to OWA1 only via a secure connection. Most employees require remote connections to headquarters, because is anticipated remote connections are likely to increase.

WAN Connectivity:
Headquarters has a T1 connection to the Internet. The Des Moines and the Omaha branch offices connect to headquarters via frame relay. The Copenhagen branch office is not connected to headquarters.

LAN Connectivity:
The headquarters LAN runs on a 100-Mbps network.

Branch Offices:
Each branch office has approximately 10-15 Windows 2000 portable computers and one Windows 2000 desktop computer. Each branch office has a T1 connection to the Internet. The Copenhagen branch office has a MS Exchange Server computer, a domain controller and a remote access server named RAS2. Copenhagen sets up, administers and maintains its own network.

Security:

Headquarters:
Network security at Enchanted Lakes is extremely important. Password policies have been established and network resources are secured. Although the company has never had its network security compromised portable computers containing customer data have been stolen.

The company's law firm requires Enchanted Lakes to be proactive in its network security especially by preventing unauthorized network access. In the past Enchanted Lakes has incorrectly granted permissions to shared files for internal employees. Sometimes this has led to accidental unauthorized access to confidential data. Enchanted Lakes wants to encrypt data for transmissions to vendors and customers by implementing a Public Key Infrastructure (PKI).

Branch Offices:
The Copenhagen office will implement PKI to issue certificates to Copenhagen employees. Enchanted Lakes wants to use secure tunnelling for the Copenhagen office. The WAN connection to Omaha and Des Moines will remain the same.

Network Roles and Usage:

Human Resources:
The HR department uses a network file server to store confidential employee information. The HR manager has the ability to manage HR resources throughout the company.

Information Technology:
The IT department maintains the corporate network and recommends hardware and software purchases for the entire company. The department also implements physical and network security for the company.

The server operators group designs networks, resolves second level support problems and resolves the company's network problems.

The help desk administers the network, resolves first level support problems and resolves problems with employees computers.

Sales:
Employees from the Sales department save personal sales documents to their portable computers and they save shared sales documents to the SALES\DOCUMENTS folder. Sales employees want their personal and shared sales documents to be more secure. The Sales department hosts a shared folder named TIPS, which is located on the intranet. This folder contains sales leads that are submitted by employees. Employees who submit leads that result in future business are rewarded with a bonus. All employees must be able to submit leads. The Sales department needs to run reports on the Sales leads information and the Executive department needs to review the leads and the reports. The IT department publishes the web page that lists the leads.

Consultants:
Consultants use the corporate network to communicate with other consultants and employees and to store customer related documents. Every week consultants must enter their work hours into the TIME ENTRY program. The TIME ENTRY program requires the consultants to enter the date and number of hours billed, the customer to bill, expenses incurred and a description of the work that has been performed. The consultants must access the TIME ENTRY program through a secure web browser.

Branch Offices:
Occasionally employees located at branch offices connect to headquarters to access customer and billing information. Employees from Omaha and Des Moines offices can access this information through the current WAN environment. However employees from Copenhagen office cannot access the information in the current environment.

Questions Enchanted Lakes Corporation

Q. 1
What are the four most important security priorities for Enchanted Lakes? (Choose four)

A. Providing secure communications between Copenhagen and headquarters.
B. Ensure secure authentication.
C. Implementing two-factor authentication for the IT department.
D. Preventing denial-of-service attacks.
E. Implementing certificate services for Omaha.
F. Protecting employee data on portable computers.
G. Preventing unauthorized network access.

Answer: A, B, F, G
Explanation:

A: The Company does not have a connection between its Copenhagen branch and Headquarters. The company wants to use secure tunneling to the Copenhagen office.

B: The Company's law firm requires Enchanted Lakes to be proactive in its network security by preventing unauthorized network access. Therefore it would want to ensure secure user authentication ...

G: ... so as to prevent unauthorized network access.

F: In the past, portable computers containing customer data have been stole. The company would thus want to secure data on the portable computers.
Note: Although the question states 'employee data' and not 'customer data', none of the other answers are appropriate.

Incorrect Answers:

C: The IT department is equipped with desktop computers and not portable computers; therefore we cannot use smartcards and EAP for authentication. Smartcards and EAP are used on portable computers.

D: Network security at Enchanted Lakes is extremely important and the company has never had its network security compromised. Furthermore, the company is proactive in its network security. There is thus little chance of denial-of-service attacks.

E: The Company wants to implement certificate services for Copenhagen and not for Omaha. The existing T1 WAN connection to Omaha will remain the same.

Q. 2
What are the two primary security risks for Enchanted Lakes? (Choose two)

A. Incorrect authentication of network users.

B. Data stolen from portable computers.
C. Unauthorized network access by employees.
D. Unauthorized network access by intruders.
E. A denial-of-service attack on OWA1.

Answer: B, C
Explanation:

B: The Company has never had its network security compromised, however, portable computers containing customer data has been stole in the past. This continues to be a risk.

C: Although the Company has never had its network security compromised, the Company's law firm requires Enchanted Lakes to be proactive in its network security by preventing unauthorized network access. In the past Enchanted Lakes has incorrectly granted permissions to shared files for internal employees. Sometimes this as had led to unauthorized access to confidential data.

Incorrect Answers:

A: Network security is important to the Company and its has not yet suffered a compromise in its network security. Furthermore, the Company is proactive in preventing unauthorized network access.

D: Network security is important to the Company and it has not yet suffered a compromise in its network security. Furthermore, the Company is proactive in preventing unauthorized network access.

E: Off-site users can only connect to OWA1 via a secure connection. This would prevent hackers from using denial-of-services attacks on OWA1.

Q. 3
Which data from Copenhagen should you encrypt?

A. All data.
B. Slip data
C. NetBIOS data
D. L2TP data

Answer: D
Explanation:
Network security is important to Enchanted Lakes and they are proactive in preventing unauthorized network access. Indeed they have never suffered a compromise in their network security. Thus data on the network itself is secure. However, data that must be transmitted from the branches, such as the Copenhagen office, to Headquarters must be secured. The Copenhagen office will connect to Headquarters via Secure Tunneling. This refers to creating a tunnel through an existing public network like the Internet, in other words, a VPN. We would use the L2TP protocol to transmit data on a VPN connection. L2TP can provide both client-to-server and

server-to-server access. However, L2TP does not include an encryption mechanism. Therefore IPSec would be used to provide encryption.

Incorrect Answers:

A: Network security is important to Enchanted Lakes and they are proactive in preventing unauthorized network access. Indeed they have never suffered a compromise in their network security. Thus data on the network itself is secure. There fore it is not necessary to encrypt the data in the network. Furthermore, encrypting data prevents other users and applications from accessing the data. This could present problems when data has to be shared.

B: SLIP, or Serial Line Internet Protocol, is a remote access protocols supported by Windows 2000 remote access and is used by older remote access servers.

C: The Copenhagen office will not contain NetBIOS data. NetBIOS is a computer naming system used on pre-Windows 2000 computers. The computers at Copenhagen will be Windows 2000 computers.

Q. 4

How should you encrypt the sales department's files?

A. Encrypt all folders that contain sales documents.
B. Encrypt only shared folders that contain sales documents.
C. Encrypt only personal sales documents individually.
D. Encrypt only shared sales documents individually.

Answer: C

Explanation:

When a file is encrypted it can only be accessed by the person who encrypted the file. Therefore we can only encrypt personal sales documents.

Incorrect Answers:

A: When a file is encrypted it can only be accessed by the person who encrypted the file. Therefore, if we encrypt all the folders that contain sales data, they will be accessible only by the person who did the encryption.

B: When a file is encrypted it can only be accessed by the person who encrypted the file. Once a file is encrypted it thus cannot be shared.

D: When a file is encrypted it can only be accessed by the person who encrypted the file. Once a file is encrypted it thus cannot be shared.

Q. 5

How should you implement certificate services for the Omaha office?

A. Use a third-party certificate services vendor.
B. Use the certificate services from the Minneapolis office.
C. Install certificate services on the Omaha office.
D. Share certificate services with the Des Moines office.

Answer: B
Explanation:
Certificates are used on the two networks involved in the communication. As Omaha would communicate with Headquarters in Minneapolis, the certificate services should be installed in the Minneapolis office.

Incorrect Answers:
A: We can use third-party certificate services to deploy CAs and issue certificates for our organizations, however, Windows 2000 Certificate Services provide many benefits that third-party CAs do not because Windows 2000 Certificate Services are fully integrated with the Windows 2000 public key infrastructure and Active Directory
C: A domain cannot grant its own certificate. Certificates are used to establish trust relationships between two networks.
D: Omaha would communicate with Headquarters therefore the CA should be located at Headquarters, which is in Minneapolis, and not Des Moines.

Q. 6
Which two technologies should you implement to provide additional security for portable computers? (Choose two)

A. Distributed file system (Dfs)
B. Encrypted file system (EFS)
C. Digital certificates.
D. IPSec
E. Kerberos authentication

Answer: B, C
Explanation:
To verify the identity of people and organizations on the Web and to ensure content integrity, Internet Explorer uses industry-standard X.509 v3 digital certificates. Certificates are electronic credentials that bind the identity of the certificate owner to a pair (public and private) of electronic keys that can be used to encrypt and sign information digitally. These electronic credentials assure that the keys actually belong to the person or

organization specified. Messages can be encrypted with either the public or private key, and then decrypted with the other key.

Incorrect Answers:

A: Distributed file system (Dfs) makes it easier for us to find and manage data on our network. Dfs provides mapping and a uniform naming convention for collections of servers, shares, and files. Dfs adds the capability of organizing file servers and their shares into a logical hierarchy, making it considerably easier to manage and use information resources. With Dfs, we can create a single directory tree that includes multiple file servers and file shares in a group, division, or enterprise. Any Windows 2000 server can host a Dfs root or Dfs volumes. A Dfs root is a local share that serves as the starting point and host to other shares. Dfs however does not protect data.

D: IPSec is used to secure data that is transmitted from one computer to another over the internet. It is not used to secure data on the computer.

E: Kerberos is a default authentication protocol used on Windows 2000 networks. It is used pervasively, which means it is installed by default and we do not need to configure the network to use it. As this is a Windows 2000 network, Kerberos would be used by default. We would therefore not be improving security by using Kerberos as it is already in use.

Q. 7
How should you configure OWA1 and TIME1 to allow secure access for remote employees? (Choose all that apply)

A. Place TIME1 in a DMZ.
B. Place OWA1 in a DMZ.
C. Place TIME1 on the internal network.
D. Place OWA1 on the internal network.
E. Enable all connections from the external network.
F. Allow only TCP port 80 connections from the external network.
G. Allow only TCP port 443 connections from the external network.

Answer: A, B, G
Explanation:
In addition to deploying a firewall between the public network and the the company's network that can be accessed tthrough the public network by means ofa browser, which is also called an extranet, many companies also place a firewall between the company's private network and their extranet to ensure the protection of the private network if the external firewall or resources in the extranet are compromised. This configuration is referred to as a Demilitarized Zone (DMZ), perimeter network, or screened subnet. PPTP is supported by Windows 95, Windows 98, Windows NT 4.0, and Windows 2000 remote access clients. PPTP uses MPPE to provide encryption of the transmitted data. MPPE can use 40-bit, 56-bit, or 128-bit encryption keys. However, we must configure the firewall to allow the PPTP packets to pass through the firewall. As TIME1 and OWA1 are both part of the Enchanted Lakes extranet as brokers must be able to access those two servers from the

public network. Therefore TIME1 and OWA1 would be placed within the DMZ. We would then need to configure the Firewall to allow traffic to pass through TCP port 443 which is used for PPTP traffic.

Incorrect Answers:

C: Brokers need to be able use a browser to access the TIME1 server. Therefore the TIME1 server should be place in the DMZ zone.

D: Brokers need to be able use a browser to access the OWA1 server. Therefore the OWA1 server should be place in the DMZ zone.

E: To secure the connection to a server that can be accessed through a public network we would want to restrict the connections that would be allowed to reach that server through the firewall. We would therefore accept only certain connection, in this scenario PPTP traffic.

F: TCP port 80 is used for HTTP traffic. We do not want configure the Firewall to permit this traffic. We only want to permit PPTP traffic. Therefore we would configure the Firewall to permit traffic through TCP port 443 only.

Q. 8
Which type of CA should you implement at Headquarters? (Choose one)

A. An online enterprise root CA with an online enterprise subordinate CA.
B. An offline enterprise root CA with an online enterprise subordinate CA.
C. An offline enterprise root CA with an offline enterprise subordinate CA.
D. An online enterprise root CA with an offline enterprise subordinate CA.

Answer: B
Explanation:
An Enterprise Certificate Authority is a Windows 2000 certification authority that is fully integrated with Active Directory it thus uses Active Directory for user information and policy decisions and can publish certificates and the Certificate Revocation List (CRL) to Active Directory. A CRL is a list of certificates that have been revoked before their scheduled expiration date because its associated private key has been compromised or the user that requested the certificate is no longer employed by the company.

Furthermore, Certificate Authorities can be stacked in a hierarchy. Root CAs preside over domains, using a self-signed certificate, i.e., a certificate they issue to themselves. They also issue certificates to subordinated authorities but they generally do not issue user certificates. Subordinate authorities issue certificates to users and other end entities and might also issue certificates to other subordinate CAs. Root CAs are implicitly trusted while subordinate CAs and clients derive trust from the root. The use of subordinate CAs will provide scalability, ease of administration, and consistency with a growing number of third-party CA products.

Incorrect Answers:

A: We would not want to keep the root CA offline as it is the origin of all trust relations and would be vulnerable to attacks while online.

C: We cannot have both the root and the subordinate CA offline as neither would then be able to issue certificates. We would want only the root CA to be offline.

D: We would not want to keep the root CA rather than the subordinate CA offline as the former is the origin of all trust relations and would be vulnerable to attacks while online.

Q. 9
Which permissions should you grant for the TIPS folder? (Choose one)

A. IT department Full Control
Sales department Full Control
Authenticated users Modify

B. IT department Full Control
Sales department Full Control
Everyone Read

C. IT department Full Control
Sales department Read
Authenticated users Read

D. IT department Full Control
Sales department Full Control
Everyone Modify

Answer: A
Explanation:

The Sales department hosts a shared folder named TIPS, which is located on the intranet. This folder contains sales leads that are submitted by employees. Employees who submit leads that result in future business are rewarded with a bonus. All employees must be able to submit leads. The Sales department needs to run reports on the Sales leads information and the Executive department needs to review the leads and the reports. The IT department publishes the web page that lists the leads. Therefore the IT department and Sale department require Full Control permissions. To allow employees to submit leads, we would need to give authenticated users modify permissions. This will allow them to modify and delete the file in the folder. It also allows them to perform the actions permitted by the Write permission and the Read & Execute permission.

Note: We would not grant them Full Control as this allows the user to change permissions and take ownership of the file.

Incorrect Answers:

B: We would grant the IT and Sales departments Full Control permissions. We would, however not grant the Everyone group Read permissions. Authenticated and guest accounts are part of the Everyone group and would thus be able to read the data in the files. Furthermore, this would not allow employees to submit leads. To be able to submit leads the employees would require write permissions. But they would also need read permissions to verify that someone has no already submitted a similar lead.

C: We would grant the IT department Full Control permissions. We would, however, not grant the Sales department and the Authenticated users read permissions only as this would not permit the Sales department to use the data in reports and it would not permit employees to submit leads.

D: We would grant the IT and Sales departments Full Control permissions. We would, however not grant the Everyone group Read permissions. Authenticated and guest accounts are part of the Everyone group and would thus be able to modify, read and delete the data in the files.

Q. 10

Which type of CA should you implement for the Copenhagen office after it is connected to the WAN? (Choose one)

A. Enterprise subordinate CA.
B. Enterprise root CA.
C. Stand-alone subordinate CA.
D. Stand-alone root CA.

Answer: A

Explanation:

An Enterprise Certificate Authority is a Windows 2000 certification authority that is fully integrated with Active Directory it thus uses Active Directory for user information and policy decisions and can publish certificates and the Certificate Revocation List (CRL) to Active Directory. A CRL is a list of certificates that have been revoked before their scheduled expiration date because its associated private key has been compromised or the user that requested the certificate is no longer employed by the company.

Furthermore, Certificate Authorities can be stacked in a hierarchy. Root CAs preside over domains, using a self-signed certificate, i.e., a certificate they issue to themselves. They also issue certificates to subordinated authorities but they generally do not issue user certificates. Subordinate authorities issue certificates to users and other end entities and might also issue certificates to other subordinate CAs. Root CAs are implicitly trusted while subordinate CAs and clients derive trust from the root. The use of subordinate CAs will provide scalability, ease of administration, and consistency with a growing number of third-party CA products.

Incorrect Answers:

B: Certificate Authorities can be stacked in a hierarchy. Root CAs preside over domains, using a self-signed certificate, i.e., a certificate they issue to themselves. They also issue certificates to subordinated authorities but they generally do not issue user certificates. Subordinate authorities issue certificates to users and other end entities and might also issue certificates to other subordinate CAs. Root CAs are implicitly trusted while subordinate CAs and clients derive trust from the root. The use of subordinate CAs will provide scalability, ease of administration, and consistency with a growing number of third-party CA products.

C: A stand alone CA is a Windows 2000 certification authority that is not integrated with Active Directory while the root CA is the CA that is located at the topmost point in the CA hierarchy. We will be implementing Active Directory in this scenario therefore we should use an Enterprise CA as the enterprise CA is integrated with Active Directory and can thus use Active Directory for user information and can publish the CRL to Active Directory instead of requiring the certificate requestor to supply all user-identifying information.

D: A stand alone CA is a Windows 2000 certification authority that is not integrated with Active Directory while the subordinate CA is the CA that is located below the root CA in the CA hierarchy, and receives a certificate from the root CA. This will provide scalability, ease of administration, and consistency with a growing number of third-party CA products. However, we will be implementing Active Directory in this scenario therefore we should use an Enterprise CA.

Case Study No: 7

LITWARE, INC.

Background

Litware, Inc. sells digital cameras, printers and supplies to photography studios throughout North America. The Company's Headquarters are located in Cleveland, Ohio.

Photography studios use digital cameras to take pictures of their customers and then allow customers to immediately view the proofs at the studio. When customers decide which pictures they want to purchase, the pictures are either printed at the studio, if the studio has a digital printer, or sent to a film-processing laboratory on a Zip disk or CD. Customers can choose to pick up the pictures at the studio or have the pictures mailed directly to them.

Existing Environment:

President:

We have supplied photography studios with camera equipment and supplies for the past 20 years. For the past year, we have sold digital cameras. Even though we sell the latest digital equipment, many studios still view us as a traditional photographic supplier. Nearly 2, 000 studios buy our products. The number of studios is increasing.

We recently merged with a French photographic supply company that has three offices in France. We now have eight offices and employ 1, 200 people.

IT Director:

All of our company's offices are connected through a WAN. I have a staff of five IT employees to maintain the computers in each regional office. Headquarters has four network engineers, one Webmaster, three Web developers for the intranet, and 10 programmer/analysts. The programmer/analysts maintain the inventory, purchasing, billing, and payroll applications.

Customer Service Representative:

Each office has its own customer service employees. Studios call us when they are having problems with their equipment. Studios also call us to order supplies. We keep records of each call. If a studio or customer calls to report a problem with our Web site, we will either try to make changes the photo folders to resolve it or notify the Webmaster.

Envisioned Environment:

President:
We want to offer more services to the studios. I would like to develop a Web site that studios can use to post proofs of their customers' photos. The studios would give IDs and passwords to customers so that they can access their photos over the Internet. Customers could then view their proofs on our company's Web site and place orders for photos. Customers could share their IDs and passwords with relatives or friends, who could also view proofs and order photos from the Web site.

IT Director:
The Web site will be hosted at headquarters. We will use Windows 2000 and Internet Information Services (IIS) on the servers. When a customer, visits the Web site to view photos, programs developed in Microsoft Visual Basic will be loaded on their computers. These programs will format the pictures for viewing on the customer's computer. The programs will be stored in a folder named Program on the Web server.

I will hire five Web developers to develop the Web site and a Webmaster to administer the Web site. The Webmaster will have total control of the Web servers. Each studio will have its own folder on the Web server. Each studio's folder will contain a folder for the studio's purchase history and a customer folder for each of the studio's customers. The customer folder will contain confidential information that should not be available to the customer. The photos will be placed in a separate photo folder inside the customer folder. Each customer will have only one folder for photos. An office manager at each studio will be responsible for creating customer folders and placing photos in the folders. We will also train office managers to add customers to the Active Directory tree for their studio.

Problem Statement:

IT Director:
I'm not sure how to secure files from customers that don't have IDs and passwords. To take it easier for customers to order from the Web site, we should allow studios to give each customer a plastic card with the customer's ID and password printed on it.

Customer Service Representative:
When a studio calls with a problem, we have to look through paper files to find out if the studio is under warranty or uses a maintenance contract. If the studio calls to order supplies, we have to look through paper files to find the studio's credit terms.

Sales Representative:
Currently, customer information is stored in several places. Customer service representatives sometimes take an order when the studio is on the phone and then do not inform the sales representatives about the order. We have to look through the paper files to find any history of problems or purchases.

Photography Studio:
I want to ensure that no one can change the photos on the Web site. When customers place an order, I want to ensure that their credit cards will be secure and that their information will not be accessed by one of my competitors.

Requirements:

President:
We need a Web site that will allow our studios to display their customers' photos. The customers should be able to securely access their photos, and order prints. The customers should also be able to specify whether they want to pick up their pictures at the studio or have the pictures mailed to them. The Web site should be able to handle 5,000 active customer accounts. I also need to see how many orders are placed on our Web site.

IT Director:
The new Web site will have two servers. The first server, named LITWWEB, will be the Web server that will display all of the photos. All hard disks on the Web server will be formatted with NTFS. All offices will use the same Web server. The second server, named LITWDATA, will contain customer information, such as name, address, and order history. In addition, we will have a proxy server named LITWPROX and a domain controller named LITWDC.

Web developers should be limited to a development environment; they should not have any access to the Web server. Only the Webmaster should be able to move new programs to LITWWEB. Studios should be able to post pictures to the Web site over the Internet. Studios should also be able to maintain their own customer accounts. The company will have a single domain named LITWARE. Each studio and customer will have a user account in this domain. Each studio will be an organizational unit (OU).

Photography Studio:
We need an easy way to load our photos onto the Web site and set up the customer data, including IDs and passwords. We want the customer photos to be displayed on the Web for only 30 days. We will disable the customer account and remove the photos after 30 days.

Customer:
I want to be sure that my credit card information is not made available to anyone other than the studio and the film-processing laboratory.

Web Developer:
If changes to the Web software are requested, we need to be able to upgrade the Web server.

Customer Service Representative:
We need access to customer information to resolve questions.

Sales Representative:
We need access to the customer order history so that we can see what customers have bought and whether they have had any problems with our equipment and service.

Webmaster:
My main goal is a secure and stable Web site. I need to move programs from a test computer to the Web server and to upgrade the Web software as needed. I will also be responsible for identifying and fixing problems in each studio's folder on the Web site.

Conclusion:
The new Web site should enable customers to securely view and order photos. It should allow photography studios to load photos only to their folders. Customer information should be available for reports, support, and marketing. The Web site should be stable.

Questions Litware, Inc.

Q. 1
What is the primary security requirement for the studios?

A. Ensure that photos on the Web site cannot be altered
B. Ensure that customers can access only their own photos on the Web site
C. Ensure that customers' credit card numbers are secure.
D. Prevent customers' computers from being infected with a virus when they view their photos on the Web site

Answer: C
Explanation:
The primary security concern of any e-commerce company would be to ensure that the customer's credit card numbers are secure. If these are not secure, customers would not be willing to trade on the web site which would render the web site meaningless.

Incorrect Answers:
A: LitWare wants to ensure that no one can change the photos on the Web site. However, they must also ensure that the customer's credit card numbers are secure as this would be crucial to their e-commerce operation. Should credit card numbers not be secure, customers would not be willing to trade, therefore the security of credit card numbers are of greater importance.
B: Although the IT Director shows some concern about securing files from customers that do not have Ids and passwords, he does not show any concern for customers to be restricted to only their photos.
D: The web developers will use Microsoft Visual Basic to develop programs that would allow he customers to load and view the pictures on their computers. Ensuring that the programs do not contain viruses would occur in house, as the developers would test the program.

Q. 2
Network configurations are shown in the exhibit (Click the Exhibit button). Which network configuration provides the most security for LitWare, Inc?

A. Figure A
B. Figure B
C. Figure C
D. Figure D

Answer: B

Q. 3
To which type of group should you assign all Web developers?

A. Global
B. Local
C. Domain local
D. Universal

Answer: A
Explantion:
We should use global groups to combine users and other global groups who have similar business requirements. Then, instead of assigning permissions directly to a global group, we should make the global group a member of a domain local group so that members of that global group inherit the permissions assigned to the domain local group.

Note: Global groups may only contain user accounts and global groups from the same domain as members. Membership of global groups is maintained in the domain where the domain local group exists Global groups are used for combining users who share a common access profile based on job function or business role. Typically, organizations use global groups for all groups where membership is expected to change frequently. These groups can only have as members user accounts defined in the same domain as the global group. Global groups can be nested to allow for overlapping access needs or to scale for very large group structures. The most convenient way to grant access to global groups is by making the global group a member of a resource group that is granted access permissions to a set of related resources.

Incorrect Answers:
B: Windows 2000 computers that are not Domain Controllers maintain Computer local groups with their own user accounts database. However, the servers at Headquarters as well as one server at each Distribution Center will function as Domain Controllers. We therefore cannot use Computer local groups.
C: Domain local groups are used for granting access rights to resources such as file systems or printers that are located on computer in the domain where common access permissions are required. The advantage of domain local groups used to protect resources is that members of the domain local groups can come from both inside the same domain and outside the domain. Typically, resource servers are in domains that have trust to one or more Master User Domains, or what are known as account domains. Furthermore, a domain local group can be used to grant access to resources on any computer only in native mode domains. In mixed mode, domain local groups must be on domain controllers only.
D: We use Universal groups to collect similar groups that exist in multiple domains. The key difference between universal groups and other security groups is that memberships are stored both in the domain where the universal group exists and in the global catalog. If the membership is stored in the global

catalog, membership can be verified without contacting a Domain Controller where the universal group is defined. Instead of assigning permissions directly to a universal group, make the universal groups members of domain local groups and assign the necessary permissions to the domain local group. Universal groups are used in larger, multidomain organizations where there is a need to grant access to similar groups of accounts defined in multiple domains. It is better to use global groups as members of universal groups to reduce overall replication traffic from changes to universal group membership. Users can be added and removed from the corresponding global group within their account domains and a small number of global groups are the direct members of the universal group. Universal groups are easily granted access by making them a member of a domain local group used to grant access permissions to resources. Furthermore, the Windows 2000 domain must be in native mode to use universal groups.

Q. 4
How should you ensure that each customer's account is disabled after 30 days?

A. Manually disable each customer's user account after 30 days
B. Add a Group Policy to the LitWare organizational unit (OU) that specifies the expiration rules for each customer's user account
C. Add a Group Policy to each studio's organizational unit (OU) that specifies the expiration rules for each customer's user account
D. Set an expiration date on each customer's user account

Answer: D
Explanation:
We can set an expire date on a user account on the Account tab of a specified user account properties dialog box. This would allow us to automatically terminate a temporary user’s access to the network. By default user accounts are set to never expire. We can access the user account properties dialog box by clicking on the Start button; pointing to Programs; pointing on Administrative tools; and clicking on Active Directory users and computers. In the Active Directory users and computers console, expand Users; right-click on the User Account that you want to set an expire date for; and click properties.

Note: On this setting we must specify a date on which the account will terminate. We must therefore calculate what the date would be in 30 days time when we create the account.

Incorrect Answers:
A: It is possible to set an expire date on the accounts. This will allow us to terminate the account automatically once the expire date has been set.
B: We cannot use a Group Policy in this scenario as we can only set a date on which the account would expire. We cannot set the account to expire after a certain amount of days.

C: We cannot use a Group Policy in this scenario as we can only set a date on which the account would expire. We cannot set the account to expire after a certain amount of days.

Q. 5
Which task should you delegate to the office managers?

A. Modify the membership of a group.
B. Manage Group Policy links.
C. Create, delete, and manage customer accounts.
D. Create, delete, and manage groups.

Answer: C
Explanation:
According to the IT Director, an office manager at each studio will be responsible for creating customer folders and placing photos in the folders. They will also be trained to add customers to the Active Directory tree for their studio. Therefore we need to delegate the authority to Create, delete and manage customer accounts to the office managers.

Incorrect Answers:

A: The office managers will be responsible for the creation of user accounts for the customers. When we provide them with permission to modify group membership, they will be able to work with groups by adding existing users or groups and removing users and groups from other groups. They would thus be able to add existing user accounts to groups but would not be able to create them.

B: The office managers will be responsible for the creation of user accounts for the customers. When we allow them to manage Group Policy links, we give them permission to link security setting to sites, domains and OUs. This could present a security risk. Furthermore, it would not allow them to create user accounts for the customers.

D: The office managers will be responsible for the creation of user accounts for the customers. When we provide them the authority to create, delete and manage groups, they will be allowed to create and modify groups. This would include adding users and removing users from groups. However, they would only be able to work with existing user accounts and would not be able to create new ones.

Q. 6
Which type of CA should you use to digitally sign the Microsoft Visual Basic programs?

A. Third-party CA
B. Enterprise root CA
C. Stand-alone root CA
D. Enterprise subordinate CA

Answer: A
Explanation:
When an application that requires certificates runs on a public network, such ActiveX controlls that run on the internet or Visual Basic programs that are installed over the internet, you should use certificates from Third-Party CAs. The use of a third-party certificate increases customer trust in the application. Consumers may not trust a small or unknown organization when that same organization issues the certificate for the Web site. Third-Party CAs are managed by companies such as Entrust or Verisign.

Incorrect Answers:

B: Enterprise CAs are integrated with Active Directory and publish certificates and CRLs to Active Directory. They use certificate template information, user account information, and security group information that are stored in Active Directory to approve or deny certificate requests. For a certificate request to be approved, the user that requests the certificate must have Enroll permissions granted by the security Access Control Lists of the certificate template for the certificate type that is requested. When a certificate is issued, the enterprise CA uses information in the certificate template to generate a certificate with the appropriate attributes for that certificate type. Therefore Enterprise CAs can only issue certificates for users that have user accounts in Active Directory.

Furthermore, we can create a hierarchy of CAs. The CA at the top of a hierarchy is referred to as a root CA and the CAs below the root are referred to as subordinate CAs. The root CA is a very important point of trust in an organization as all certificates flow from the root. It issues its own certificate and the certificates for its subordinate CAs. We should therefore take the root CA offline once the subordinates have been granted certificates. The subordinates would then respond to certificate requests.

C: Unlike Enterprise CAs, Stand-alone CAs does not require Active Directory and does not use certificate templates. Instead all information about the requested certificate must be included in the certificate request. By default, all certificate requests submitted to stand-alone CAs are held in the Pending Queue until the CA administrator approves them. We can configure stand-alone CAs to issue certificates automatically but this would represent an increase in security risk and is usually not recommended.

Furthermore, we can create a hierarchy of CAs. The CA at the top of a hierarchy is referred to as a root CA and the CAs below the root are referred to as subordinate CAs. The root CA is a very important point of trust in an organization as all certificates flow from the root. It issues its own certificate and the certificates for its subordinate CAs. We should therefore take the root CA offline once the subordinates have been granted certificates. The subordinates would then respond to certificate requests.

D: Enterprise CAs are integrated with Active Directory and publish certificates and CRLs to Active Directory. They use certificate template information, user account information, and security group information that are stored in Active Directory to approve or deny certificate requests. For a certificate request to be approved, the user that requests the certificate must have Enroll permissions granted by the security Access Control Lists of the certificate template for the certificate type that is requested. When a certificate is issued, the enterprise CA uses information in the certificate template to generate a certificate with the appropriate attributes for that certificate type. Therefore Enterprise CAs can only issue certificates for users that have user accounts in Active Directory.

Furthermore, we can create a hierarchy of CAs. The CA at the top of a hierarchy is referred to as a root CA and the CAs below the root are referred to as subordinate CAs. The root CA is a very important point of trust in an organization as all certificates flow from the root. It issues its own certificate and the certificates for its subordinate CAs. We should therefore take the root CA offline once the subordinates have been granted certificates. The subordinates would then respond to certificate requests.

Q. 7
Which two authentication methods should you use to allow customers access to their photos on the Web site? (Choose two)

A. Basic authentication with SSL
B. Anonymous access
C. Integrated Windows authentication
D. Digest authentication with SSL
E. Digest authentication without SSL
F. Basic authentication without SSL

Answer: A, D
Explanation:

A: Basic Authentication is supported by all types of Web browsers, including the oldest ones. If users accessing our site are using older browsers that cannot be authenticated using other forms of authenticated access, we would need to enable basic authentication. With Basic Authentication, the customers will be presented with a dialog box requesting credentials and those credentials are then passed over the network connection in unencrypted form, which is intrinsically not secure. We can use SSL to establish a secure session and make passwords more secure, and hence Basic authentication more secure. SSL is short for Secure Socket Layer and was developed by Netscape for transmitting private documents securely via the Internet. SSL secures communication by using a public key to encrypt data that is transferred over the SSL connection. Many e-commerce websites use the protocol to secure the transmission of confidential user information such as credit card numbers. SSL is supported on both Navigator and Internet Explorer. By using Basic authentication and SSL, the password will still not be encoded, but the HTTP session carrying the data will be encrypted using cryptographically-secure mechanisms.

D: Digest Authentication is supported by IIS 5 and can work across firewalls and proxy servers. A hash or message digest is passed across the connection instead of the user's actual credentials. The information is transmitted in clear text but is hashed, so that it is secure. However, the domain controller for which the authentication request is made requires a plain-text copy of the user's password. Therefore precautions must be taken to secure the domain controller.

In addition we would use the SSL protocol to encrypt Web traffic between client and server. SSL is essential as we plan to use our server for running Web applications that involve financial transactions. Web browsers access a secure server using SSL by using URLs that are prefixed by https:// instead of the usual http:// prefix. SSL is based on public-key cryptography, in which digital certificates are used to establish the identity and trustworthiness of servers (and of clients), while a public/private-key pair is used for encrypting and decrypting transmissions to ensure that the information being transmitted is secure and has integrity.

Incorrect Answers:

B: Anonymous Access allows users to access the content in the Web site using their Web browsers without needing to have their credentials authenticated in any way, and is the typical authentication method used for public Web sites on the Internet. We however want to restrict access to the Web site to customers only. These customers will be granted user names and passwords. We therefore would not allow Anonymous Access.

C: Integrated Windows Authentication is a cryptographic exchange is used to securely authenticate the user without actually passing credentials across the connection. The user is not prompted for credentials; instead, his or her currently logged on credentials are used. Integrated Windows authentication can also use Kerberos authentication if the server has Active Directory installed on it and if the client browser supports it. In this scenario the customers would not be logged on to the network. We would therefore not be able to use Integrated Windows Authentication.

E: Basic Authentication is supported by all types of Web browsers, including the oldest ones. If users accessing our site are using older browsers that cannot be authenticated using other forms of authenticated access, we would need to enable basic authentication. With Basic Authentication, the customers will be presented with a dialog box requesting credentials and those credentials are then passed over the network connection in unencrypted form, which is intrinsically not secure.

F: Digest Authentication is supported by IIS 5 and can work across firewalls and proxy servers. A hash or message digest is passed across the connection instead of the user's actual credentials. The information is transmitted in clear text but is hashed, so that it is secure. However, the domain controller for which the authentication request is made requires a plain-text copy of the user's password. Therefore precautions must be taken to secure the domain controller. However, we would use the SSL protocol to encrypt Web traffic between client and server. SSL is essential as we plan to use our server for running Web applications that involve financial transactions.

Q. 8
How should you allow studios to create their own customer accounts?

A. Delegate authority to the office manager in each studio's organizational unit (OU)
B. Delegate authority to the administrator in the LitWare organizational unit (OU)

C. Add a new organizational unit (OU) under each studio, add an Administrator account in the new OU, and assign administrator rights to the new Administrator account by using Group Policy

D. Add a new organizational unit (OU) for each studio under the Litware OU, add an Administrator account in the new OU, and assign administrator rights to the new Administrator account by using Group Policy

Answer: A

Explanation:

According to the IT Director, studios should be able to post pictures to the Web site over the Internet. The office manager at each studio should also be able to maintain their own customer accounts. The company will have a single domain named LITWARE. Each studio and customer will have a user account in this domain. Each studio will be an organizational unit (OU). Therefore, we would need to delegate the authority to create customer accounts to the office manager in each studio's organizational unit (OU).

Incorrect Answers:

B: By delegating the authority to the administrator in the LitWare OU, the administrator would have to create the customer accounts but would only be able to create them in the LitWare OU.

C: The Studios have been organized into separate OU already. It is therefore not necessary to create a new OU. Furthermore, by creating an administrator account for the office managers, we would grant them too much authority.

D: The Studios have been organized into separate OU already. It is therefore not necessary to create a new OU. Furthermore, by creating an administrator account for the office managers, we would grant them too much authority.

Q. 9

Which authentication method or methods can you use to allow studios to securely post pictures to Litweb? (Choose all that apply)

A. Digest authentication without SSL

B. Anonymous access

C. Integrated Windows authentication

D. Basic authentication without SSL

E. Digest authentication with SSL

F. Basic authentication with SSL

Answer: E, F

Explanation:

E: Digest Authentication is supported by IIS 5 and can work across firewalls and proxy servers. A hash or message digest is passed across the connection instead of the user's actual credentials. The information is transmitted in clear text but is hashed, so that it is secure. However, the domain controller for which the authentication request is made requires a plain-text copy of the user's password. Therefore precautions must be taken to secure the domain controller.

In addition we would use the SSL protocol to encrypt Web traffic between client and server. SSL is based on public-key cryptography, in which digital certificates are used to establish the identity and trustworthiness of servers (and of clients), while a public/private-key pair is used for encrypting and decrypting transmissions to ensure that the information being transmitted is secure and has integrity. This would ensure the origin of the data that is posted.

F: Basic Authentication is supported by all types of Web browsers, including the oldest ones. If users accessing our site are using older browsers that cannot be authenticated using other forms of authenticated access, we would need to enable basic authentication. With Basic Authentication, the client will be presented with a dialog box requesting credentials and those credentials are then passed over the network connection in unencrypted form, which is intrinsically not secure. We can use SSL to establish a secure session and make passwords more secure, and hence Basic authentication more secure. SSL is short for Secure Socket Layer and was developed by Netscape for transmitting private documents securely via the Internet. SSL secures communication by using a public key to encrypt data that is transferred over the SSL connection. Many e-commerce websites use the protocol to secure the transmission of confidential user information such as credit card numbers. SSL is supported on both Navigator and Internet Explorer. By using Basic authentication and SSL, the password will still not be encoded, but the HTTP session carrying the data will be encrypted using cryptographically-secure mechanisms.

Incorrect Answers:

A: Digest Authentication is supported by IIS 5 and can work across firewalls and proxy servers. A hash or message digest is passed across the connection instead of the user's actual credentials. The information is transmitted in clear text but is hashed, so that it is secure. However, the domain controller for which the authentication request is made requires a plain-text copy of the user's password. Therefore precautions must be taken to secure the domain controller. However, we would use the SSL protocol to encrypt Web traffic between client and server. SSL is essential as we plan to use our server for running Web applications that involve financial transactions.

B: Anonymous Access allows users to access the content in the Web site using their Web browsers without needing to have their credentials authenticated in any way, and is the typical authentication method used for public Web sites on the Internet. We however want to ensure that only studios can post pictures. We therefore would not allow Anonymous Access.

C: Integrated Windows Authentication is a cryptographic exchange is used to securely authenticate the user without actually passing credentials across the connection. The user is not prompted for credentials; instead, his or her currently logged on credentials are used. Integrated Windows authentication can also use Kerberos authentication if the server has Active Directory installed on it and if the client browser supports it. In this scenario the customers would not be logged on to the network. We would therefore not be able to use Integrated Windows Authentication.

D: Basic Authentication is supported by all types of Web browsers, including the oldest ones. If users accessing our site are using older browsers that cannot be authenticated using other forms of authenticated access, we would need to enable basic authentication. With Basic Authentication, the customers will be presented with a dialog box requesting credentials and those credentials are then passed over the network connection in unencrypted form, which is intrinsically not secure.

Q. 10
How should you allow programming changes to the Web site?

A. Grant the Webmaster Full Control permission
B. Grant the Webmaster Read and Write permission only
C. Grant the Web developers Full Control permission.
D. Grant the Web developers Read and Write permission only

Answer: A
Explanation:
The webmaster will be responsible for ensuring the stability of the Web site. The Webmaster would thus be responsible for moving the new programs developed by the Web development team to the web site, for testing the web site, and for fixing problems on the Web site. To adequately perform these tasks the Webmaster would require Modify, Read and Write permissions to the Web site. All theses permissions are included in the Full Control permission.

Incorrect Answers:
B: The webmaster will be responsible for ensuring the stability of the Web site. The Webmaster would thus be responsible for fixing problems on the Web site. This would require modify permissions in addition to the read and write permissions. Therefore, granting the Webmaster Read and Write permission only would be insufficient.
C: According to the IT Director, Web developers should be limited to a development environment; they should not have any access to the Web server. Only the Webmaster should be able to move new programs to the Web server, LITWWEB. We would therefore not grant the Web development team any permissions to Web site.
D: According to the IT Director, Web developers should be limited to a development environment; they should not have any access to the Web server. Only the Webmaster should be able to move new programs to the Web server, LITWWEB. We would therefore not grant the Web development team any permissions to Web site.

Q. 11
Which audit policy should you use on LlTWWEB to detect unauthorized access to the credit card files?

A. Failure audit for logon events
B. Success audit for logon events
C. Success and failure audit for process tracking
D. Success and failure audit for object access

Answer: D
Explanation:
The customers' credit card information will be held in a file on the server. In a network environment, files are referred to as objects. We would therefore need to audit object access. By auditing successful and failed object acess, enteries will recorded to a log when a user attempts to gain access to a file or folder. However, the administrator must configure which specific files and folders should be audited.

Incorrect Answers:

A: Audit Account Logon Events records information about any attempt to log on to a computer or server to gain access to the network. By auditing failure, we will record all attempted logons that have been denied access. This information can be used to determine which user accounts are being used to attempt to access the network.

B: Audit Account Logon Events records information about any attempt to log on to a computer or server to gain access to the network. By auditing success, we will record all attempted logons to the server that have been successful. This, however, will not indicate access to files.

C: Process Tracking audits applications and records information about the actions that a particular application performs. This information can be used to determine which files and registry keys an application requires access to. It cannot be used to detect access to confidential files.

Q. 12
How should you secure the customer photos on LITWWEB?

A. Grant customers Read permission to their own photo folder
B. Digitally sign each customer's photo folder, and give the private key to the customer
C. Apply Encrypting File System (EFS) to each customer's photo folder, and give the private key to the customer
D. Grant customers Read permission to each photo in their own photo folder

Answer: A
Explanation:
We need to allow the customers to share access to their photos with their friends and family. We must therefore restrict access to the folder by means user accounts. The easiest way to do this is to grant the customer's account read permissions only to the folder that contains their photos.

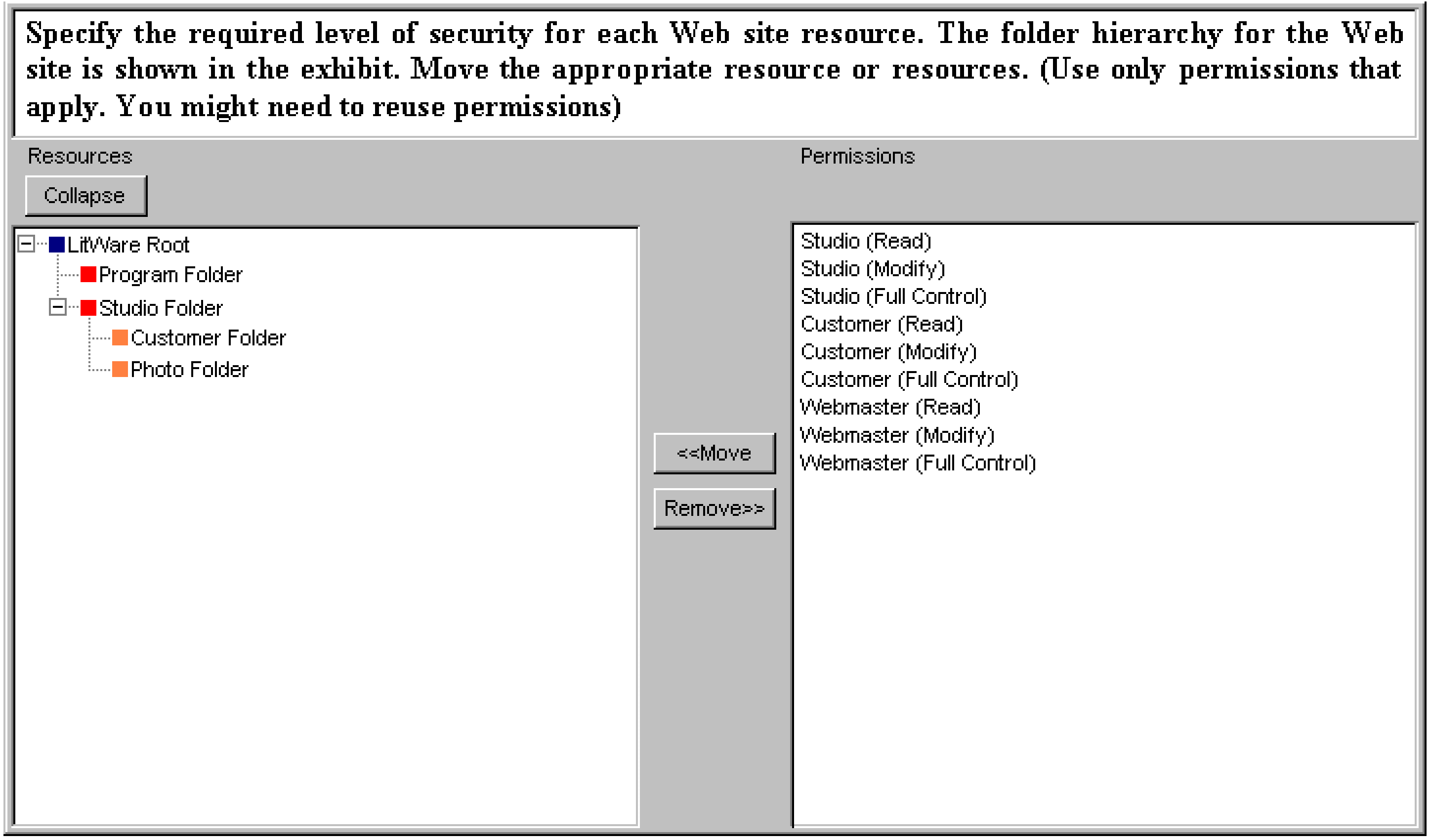
Incorrect Answers:

B: By digitally signing the customer's photo folder, and give the private key to the customer, only the customer will be able to access the folder. However, the studio is responsible for posting the photo’s in the folder and would not be able to do this if they do not have a copy of the private key

C: When a folder is encrypted, only the user with the private key will have access to that folder. However, the studio is responsible for posting the photo’s in the folder and would not be able to do this if they do not have a copy of the private key.

D: We could grant customers Read permission to each photo in their own photo folder but it would require less administrative effort to apply the permissions at the level of the folder.

Q. 13



Specify the required level of security for each Web site resource. The folder hierarchy for the Web site is shown in the exhibit. Move the appropriate resource or resources. (Use only permissions that apply. You might need to reuse permissions)

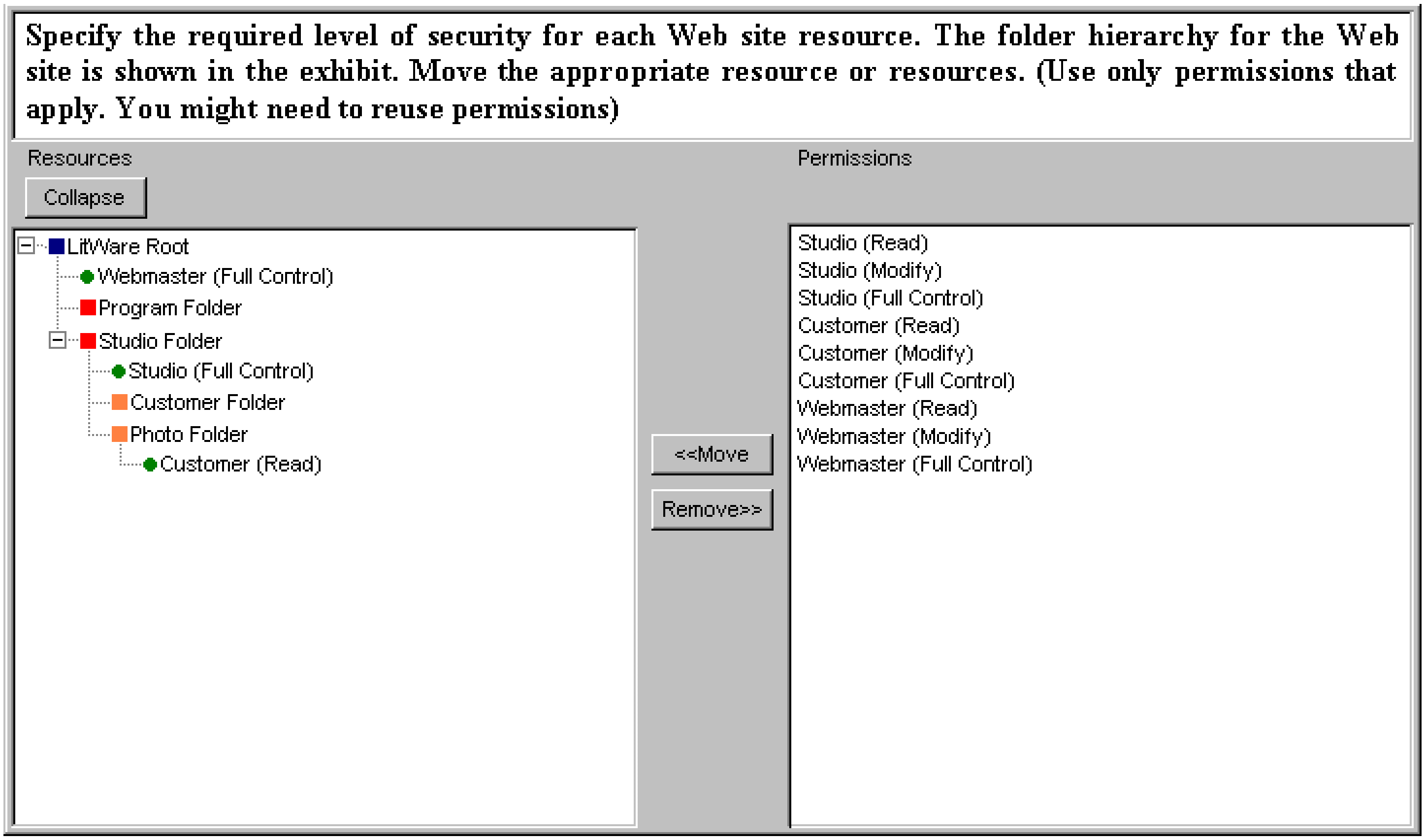
Resources

- LitWare Root
  - Program Folder
  - Studio Folder
    - Customer Folder
    - Photo Folder

Permissions

Studio (Read)
Studio (Modify)
Studio (Full Control)
Customer (Read)
Customer (Modify)
Customer (Full Control)
Webmaster (Read)
Webmaster (Modify)
Webmaster (Full Control)

Answer:



Specify the required level of security for each Web site resource. The folder hierarchy for the Web site is shown in the exhibit. Move the appropriate resource or resources. (Use only permissions that apply. You might need to reuse permissions)

Resources

- ■ LitWare Root
  - ● Webmaster (Full Control)
  - ■ Program Folder
  - ■ Studio Folder
    - ● Studio (Full Control)
    - ■ Customer Folder
    - ■ Photo Folder
      - ● Customer (Read)

Permissions

- Studio (Read)
- Studio (Modify)
- Studio (Full Control)
- Customer (Read)
- Customer (Modify)
- Customer (Full Control)
- Webmaster (Read)
- Webmaster (Modify)
- Webmaster (Full Control)

Case Study No: 8

PROSEWARE

Background

ProseWare Corp is a temporary staffing agency that provides companies with temp employees. ProseWare employs 2,500 people nationwide.

Organization:

Headquarters:

Headquarters is located in Chicago, Illinois. Headquarters includes the Accounting, Payroll, Human Resources, and IT departments. Headquarters employs 150 people.

Branch Offices:

ProseWare Corporation has branch offices in 200 locations nationwide. Each branch office employs from 5 to 20 people. Each branch office has a branch manager. One person in each branch office is a representative for the IT department. This person resets routers and helps the IT department troubleshoot technical problems that occur at the branch office.

Regions:

Several branch offices that are in the same geographic area make up a region. There are eight regions. One regional manager is assigned to each region. The regional managers submit information about branch offices, regions, and markets for posting on the Web page. Branch managers must approve the content before it is published on the company's Internet Web page.

On-Site Offices:

For ProseWare Corp largest customers, the company provides one to five employees from the sales department to work full time at the Customer offices. This helps ProseWare identify customer needs more efficiently.

Payroll Centers:

There are payroll centers in Dallas, Texas and San Francisco, California. Payroll centers process paychecks for all employees within their region.

Existing IT Environment:

Computers:
All headquarters employees, except employees within the IT department, use Windows 98 desktop computers. The IT department uses Windows NT Workstation 4.0 desktop computers.

ProseWare Corporation has 28 Windows NT Server 4.0 computers at headquarters. One of these computers is a certificate server that is not being used, two are file servers that store company data, and 25 run Windows NT Server 4.0, Terminal Server Edition.

In addition, ProseWare Corporation has one Outlook Web Access (OWA) server named OWA1, two domain controllers named DC1 and DC2, three Microsoft Exchange Server 5.5 computers, four UNIX servers that contain Oracle databases, and one remote access server named RAS1.

On-site employees use OWA1 to connect to headquarters. Anonymous users can connect to OWA1 to post resumes to an Exchange public folder named Recruiting and to fill out online applications. Each branch office has access to this public folder. The IT representative maintains control of this folder.

The company also maintains an Intranet, which includes Web pages for technical support, human resources information, and other company information. Branch offices all have desktop terminals and one computer with a modem. The branch offices connect to a Terminal server at headquarters. There are no servers in the branch offices.

All headquarters employees are granted access to e-mail and the Internet. Users in branch offices and on-site offices are granted access to e-mail and the Internet from the computers. Users of desktop terminals are not granted access to the Internet.

WAN Connectivity:
Branch offices are connected to headquarters by fractional T1 lines the committed information rate is 128 Kbps. ProseWare Corporation has a T1 line to the Internet. The company's domain name is proseware.com. ProseWare Corporation maintains a web page under this domain.

On-site offices are not connected to the WAN.

Network:
All servers have static IP addresses. All client computers use DHCP. Each branch office has its own subnet and a router.

Envisioned IT Environment:

Computers:

ProseWare Corporation wants to upgrade its network to Windows 2000 and use one Active Directory tree. All servers will be upgraded to Windows 2000 Server. All Terminal servers will use the Terminal Services feature. All desktop computers will be upgraded to Windows 2000 Professional.

ProseWare Corporation plans to add an additional remote access server, which will be named RAS2. Both remote access servers will run 2000 with Routing and Remote Access. In addition, the company will add an Internet Information Services (IIS) server.

OWA1 will not be upgraded to windows 2000.

WAN Connectivity:

The WAN bandwidth will remain the same.

Network:

ProseWare Corporation wants to build a network that can easily accommodate future growth.

Security:

ProseWare Corporation has implemented digital certificates to communicate securely with customers. The company has implemented one enterprise root CA. ProseWare Corporation wants to set up a certificate server for internal use only. The company also wants to implement secure communications to the Human Resources shared folder to prevent theft of confidential data during transmission. The company might consider two-factor authentication methods for portable computers.

Network Roles and Usage:

Human Resources:

The Human Resources department maintains a folder that contains confidential employee data. This folder is located on one of the Windows NT 4.0 file servers.

IT:

IT department maintains the network. The Terminal servers provide complete centralized administration for ProseWare Corporation. This allows all IT employees to be located at headquarters. The IT department is composed of network administrators and help desk personnel.

Sales:
The Sales department uses the network to send and receive information from potential temporary employees and to communicate with customers. Sales employees often send confidential information, such as personnel schedules, through e-mail.

Branch Offices:
Branch offices store confidential employee data, such as benefits information, in the Human Resources shared folder. The branch manager copies this information to the folder. Only the branch manager has access to this information. The IT representatives in the branch offices report network downtime and are allowed to create global groups on the network for their offices.

Payroll Centers:
Payroll centers connect to the Oracle databases at headquarters to obtain payroll data. This data is used to create paychecks.

Questions ProseWare

Q. 1
Which business requirement will have the most impact on the Windows 2000 security design?

A. Improved network performance
B. Continued use of the OWA1 server in the Windows 2000 environment
C. Projected number of branch offices
D. Resource access for on-site offices

Answer: B
Explanation:
The OWA1 server will not be upgraded. Furthermore, users will access the server over the internet which would need to be secured. In addition, anonymous users will be allowed to connect to OWA1 to post resume. They would therefore need to be able to write to the server. This would need to be taken into account when designing security.

Incorrect Answers:
A: Network performance would not impact on security.
C: The envisaged network is to make allowance for scalability. This would not impact on network security.
D: The on-site offices will have access to email and the Internet. They would use OWA1 to connect to Headquarters.

Q. 2
Which two security solutions should you implement for headquarters? (Choose two)

A. EFS
B. Digital Certificate
C. Encrypted data transmissions
D. PAP authentication
E. Two-factor authentication

Answer: B, C
Explanation:
Digital Certificates are used to authenticate clients and servers on the Internet to ensure secure browser communications. It is used to verify the identity of people and organizations on the Internet and to ensure content integrity.

We would also use the Secure Socket Layer (SSL) protocol to encrypt all data transferred from Headquarters.

Incorrect Answers:

A: Encrypting File System is a Windows 2000 feature that allows a user to protect the confidentiality of his or her documents. Once a file is encrypted, on the owner of the file will be able to access and use the file. Therefore we cannot share files that are encrypted.

D: PAP authentication sends user passwords in plain text. This is not a secure means of authentication.

E: Two-factor authentication requires users to present a physical object that encodes their identities plus a password. The most common example of two-factor authentication is the automated teller machine (ATM) card that requires a personal identification number (PIN). Biometric identification is another form of two-factor authentication. A special device scans the user's handprint, thumbprint, iris, retina, or voiceprint in place of an access card. Then the user enters the equivalent of a password. This approach is expensive but it makes identity interception and masquerading very difficult. For business enterprises, the emerging two-factor technology is the smart card. This card is not much larger than an ATM card and is physically carried by the user. It contains a chip that stores a digital certificate and the user's private key. The user enters a password or PIN after inserting the card into a card reader at the client computer. Because the private key is carried on a chip in the user's pocket, it is very hard for a network intruder to steal. Windows 2000 directly supports smart card authentication.

Q. 3
Which authentication method should ProseWare Corporation's employees at on-site offices use after the computers are upgraded to Windows 2000?

A. NTLM
B. Basic Authentication with SSL
C. MS-CHAP
D. Kerberos

Answer: B.
Explanation:
On-site workers will access Headquarters via OWA which uses an internet connection. We must therefore allow access using basic authentication. Basic authentication is supported by most browsers and uses Base-64 encoding to encode user name and password data transmissions. These can however be decoded by anyone with a decoding utility. We can use SSL to establish a secure session and make passwords more secure, and hence Basic authentication more secure. SSL is short for Secure Socket Layer and was developed by Netscape for transmitting private documents securely via the Internet. SSL secures communication by using a public key to encrypt data that is transferred over the SSL connection. Many e-commerce websites use the protocol to secure the transmission of confidential user information such as credit card numbers. SSL is supported on both

Navigator and Internet Explorer. By using Basic authentication and SSL, the password will still be encoded, but the HTTP session carrying the data will be encrypted using cryptographically-secure mechanisms.

Incorrect Answers:

A: The Kerberos authentication protocol is the primary security protocol for domains in Windows 2000. It supports single logon, allowing faster authentication and faster network response and can be used for any clients using Kerberos v5 that are members of a trusted domain. However, it cannot authenticate between domains in separate forests. On-site staff has limited access to the customer’s network and connect to HQ via Internet access. They therefore do not exist in the same domain as HQ. Consequently, they cannot use Kerberos for authentication.

C: The NTLM authentication protocol is the primary security protocol for domains in Windows NT. It supports single logon, allowing faster authentication and faster network response and can be used for any clients using NTLM and NTLMv2 that are members of a trusted domain. However, it cannot authenticate between domains in separate forests. It is retained in Windows 2000 as a backward compatible authentication protocol to support compatibility with previous versions of Microsoft operating systems and mixed mode domains. It provides authentication between NT 4.0 BDCs and Windows 2000. On-site staff have limited access to the customer’s network and connect to HQ via Internet. They therefore do not exist in the same domain as HQ. Consequently, they cannot use Kerberos for authentication.

D: The MS-CHAP v1 is an encrypted authentication mechanism in which the remote access server sends a challenge to the remote client that consists of a session ID and an arbitrary challenge string. The remote client must return the user name and a Message Digest 4 (MD4) hash of the challenge string, the session ID, and the MD4-hashed password. The remote access server keeps a duplicate of the hash and compares it to the hash in the MS-CHAP Response. If the hashes are the same, the remote access server sends back an MS-CHAP Success message. If the hashes are different, an MS-CHAP Failure message is sent. MS-CHAP is however used for Remote Access and not internet access. The On-site workers will access HQ via OWA which uses an internet connection and not Remote Access therefore we cannot use MS-CHAP.

Q. 4
How can you allow ProseWare Corporation's employees at on-site offices to communicate securely with headquarters?

A. Implement L2TP over IPSec
B. Use basic authentication with SSL
C. Implement DNS security and Group Policies
D. Use encrypted authentication with SSL

Answer: B.
Explanation:

On-site workers will access Headquarters via OWA which uses an internet connection. We must therefore allow access using basic authentication. Basic authentication is supported by most browsers and uses Base-64 encoding to encode user name and password data transmissions. These can however be decoded by anyone with a decoding utility. We can use SSL to establish a secure session and make passwords more secure, and hence Basic authentication more secure. SSL is short for Secure Socket Layer and was developed by Netscape for transmitting private documents securely via the Internet. SSL secures communication by using a public key to encrypt data that is transferred over the SSL connection. Many e-commerce websites use the protocol to secure the transmission of confidential user information such as credit card numbers. SSL is supported on both Navigator and Internet Explorer. By using Basic authentication and SSL, the password will still be encoded, but the HTTP session carrying the data will be encrypted using cryptographically-secure mechanisms.

Incorrect Answers:

A: L2TP over IPSec is used in Virtual Private Networks (VPN) to enable the secure transport of data over the Internet. This type of secure connection is used for small or remote office clients that need access to the corporate network. A VNP achieves this by creating a tunnel through the internet. L2TP creates the necessary IPSec security policy to secure tunnel traffic. For an L2TP over IPSec connection to occur, we must install computer certificates on the VPN client and VPN server computers, however, in this scenario on-site workers will use OWA, which uses an Internet connection, to access Headquarters. We therefore cannot use L2TP over IPSec.

C: DNS is used for name resolution. In other words it resolves domain and computer names to IP address and IP addresses to computer names. It is not used for communication purposes. Furthermore, there is no Secure DNS, only secure dynamic DNS updates. In addition, Group Policies are used to set the security configuration of user and computer accounts. It too is not used to secure communication.

D: Windows 2000 does not support an Encrypted Authentication option. It only supports Anonymous Access; Basic Authentication; Digest Authentication; and Integrated Windows Authentication.

Q. 5

After all computers are upgraded to Windows 2000, which security component should you reconfigure?

A. IPSec
B. Authentication Protocols
C. Certificate Services
D. Network Access Permissions

Answer: D

Explanation:

Once the network is set up our first task is to ensure that only authorized users have access to network resources, and that the correct level of authorizations are used. In other words we need to ensure that users have the correct permissions to the various network resources and that only users that are authorized to have access to certain resources are allowed to access those resources. To accomplish this we would need to assign users the appropriate permissions.

Incorrect Answers:

A: IPSec is used to secure IP communication. However, on a Windows 2000 network, Kerberos and trust relations are used to authenticate user accounts. Only if higher levels of security are required will we implement IPSec.

B: On a Windows 2000 network, Kerberos and trust relations are used to authenticate user accounts. Kerberos is used pervasively, which means it is installed and used by default and does not need to be set.

C: Certificates are used to ensure the integrity of data transmissions; however, in a Windows 2000 network integrity is based on trust relations which are established between all domains, including child domains in the forest.

Q. 6

What is the primary security risk for ProseWare Corp.?

A. Unauthorized network authentication.
B. Theft of HR data
C. Unauthorized changes to web content
D. Theft of payroll center data

Answer: B.

Explanation:

The security measures that Proseware's envisages is focused on securing communication between HR shared folder to prevent theft of data during transit and may consider two-factor authentication for mobile computers. This is also Proseware's main commodity.

Incorrect Answers:

A: The Company wants to set up digital certificates for internal use. This will prevent unauthorized network authentication.

C: Proseware has a strategy for posting data on the Web. The Regional managers submit information about branch offices, regions and markets for posting on the Web page. Branch managers must approve the content before it is posted. Therefore there is little risk that unauthorized users will be able to change web content.

D: Although this may be a concern, Proseware's security arrangements are geared toward securing its HR data.

Q. 7

How can you implement secure communications between the IT Department and the HR Department? (Choose two)

A. Use Kerberos authentication, 3DES encryption, and AH
B. Use Kerberos authentication, 3DES encryption, and ESP
C. Use certificate based authentication, 3DES encryption, and AH
D. Use certificate based authentication, 3DES encryption, and ESP
E. Use pre-shared key authentication, 3DES encryption, and AH
F. Use pre-shared key authentication, 3DES encryption, and ESP
G. Implement digital certificates to secure communication between PCs.

Answer: A, B
Explanation:
Both the IT department and the HR departments are located at headquarters. In the envisaged network, all computers will run Windows 2000 except for the OWA server. The network will also be organized into a single Active Directory tree, in other words, a forest that consists of a single tree or a single domain. We can therefore use the Kerberos authentication protocol which is the primary security protocol for domains in Windows 2000, or we can use certificate based authentication. It supports single logon, allowing faster authentication and faster network response and can be used for any clients using Kerberos v5 that are members of a trusted domain. However, it cannot authenticate between domains in separate forests. On-site staff has limited access to the customer’s network and connect to HQ via Internet access.

To increase security we can use 3DES for encryption and AH to ensure data integrity. 3DES is an encrypting algorithm that processes each data block three times, using a unique key each time. This prevents the entire data set from being compromised if one key is broken.

AH is short for Authentication Header and provides authentication, integrity, and anti-replay for both the IP header and the data payload carried in the packet, in other words, for the entire packet. It does not provide confidentiality, which means it does not encrypt the data. The data is readable, but protected from modification. However, we can use AH with ESP. With ESP the data payload is encrypted and signed for integrity. Upon receipt, after the integrity verification process is complete, the data payload in the packet is decrypted and the recipient can be certain of the transmission source that the data is unmodified, and that no one else was able to read it.

Incorrect Answers:

C: Certificate based authentication uses digital credentials that bind the identity of the certificate owner to a pair (public and private) of electronic keys that can be used to encrypt and sign information. These credentials assure that the keys actually belong to the specified person or organization. Messages can then be encrypted with either the public or private key, and then decrypted with the other key. Public key certificates can be used in situations that include Internet access, remote access to corporate resources, external business partner communications, any L2TP-based communications, or computers that do not run the Kerberos v5 authentication protocol. As all communication between the IT department and the HR department will be between Windows 2000 computers that are located in the same domain, Kerberos will be the default means of authentication.

D: Certificate based authentication uses digital credentials that bind the identity of the certificate owner to a pair (public and private) of electronic keys that can be used to encrypt and sign information. These credentials assure that the keys actually belong to the specified person or organization. Messages can then be encrypted with either the public or private key, and then decrypted with the other key. Public key certificates can be used in situations that include Internet access, remote access to corporate resources, external business partner communications, any L2TP-based communications, or computers that do not run the Kerberos v5 authentication protocol. As all communication between the IT department and the HR department will be between Windows 2000 computers that are located in the same domain, Kerberos will be the default means of authentication. Furthermore, we would not use ESP as in ESP only the data payload is encrypted and signed for integrity. Upon receipt, after the integrity verification process is complete, the data payload in the packet is decrypted and the recipient can be certain of the transmission source that the data is unmodified, and that no one else was able to read it. However, ESP does not normally sign the entire packet unless it is being tunneled. We will not be using tunneling as the IT department and the HR department are located in the same domain, therefore we need not create a Virtual Private Network through a public network.

E: A pre-shared key is a certificate based authentication model in which a shared, secret key that is previously agreed upon by two users is used. It is quick to use and does not require the client to run the Kerberos v5 protocol or have a public key certificate. Both parties must manually configure their IPSec policies to use this pre-shared key. This can be used on a limited basis when Kerberos or certificate-based authentication is not available. With this key only authentication is protected. It does not encrypt the data. In this scenario both departments will use Kerberos as they will both use Windows 2000 computers and would be located in the same domain. Microsoft also does not recommend the frequent use of pre-shared key authentication, because the authentication key is stored, unprotected, in the IPSec policy.

F: A pre-shared key is a certificate based authentication model in which a shared, secret key that is previously agreed upon by two users is used. It is quick to use and does not require the client to run the Kerberos v5 protocol or have a public key certificate. Both parties must manually configure their IPSec policies to use this pre-shared key. This can be used on a limited basis when Kerberos or certificate-based authentication is not available. With this key only authentication is protected. It does not encrypt the data. In this scenario both departments will use Kerberos as they will both use Windows 2000 computers and would be located in the same domain. Microsoft also does not recommend the frequent use of pre-shared key authentication, because the authentication key is stored, unprotected, in the IPSec policy. Furthermore, we would not use ESP as in ESP only the data payload is encrypted and signed for integrity. Upon receipt, after the integrity verification process is complete, the data payload in the packet is decrypted and the recipient can be certain of the transmission source that the data is unmodified, and that no one else was able to read it. However, ESP does not normally sign the entire packet unless it is being tunneled. We will not be using tunneling as the IT and the HR departments are located in the same domain, therefore we need not create a Virtual Private Network through a public network.

G: Digital Certificates are used to authenticate clients and servers on the Internet to ensure secure browser communications. It is used to verify the identity of people and organizations on the Internet and to ensure content integrity.

Q. 8
Which type or types of CA should you implement for internal use? (Choose all that apply)

A. Stand alone root CA
B. Enterprise subordinate CA
C. Third Party CA
D. Stand alone subordinate CA
E. Enterprise root CA

Answer: B, E.
Explanation:
An Enterprise Certificate Authority is a Windows 2000 certification authority that is fully integrated with Active Directory it thus uses Active Directory for user information and policy decisions and can publish certificates and the Certificate Revocation List (CRL) to Active Directory. A CRL is a list of certificates that have been revoked before their scheduled expiration date because its associated private key has been compromised or the user that requested the certificate is no longer employed by the company.

Furthermore, Certificate Authorities can be stacked in a hierarchy. Root CAs preside over domains, using a self-signed certificate, i.e., a certificate they issue to themselves. They also issue certificates to subordinated authorities but they generally do not issue user certificates. Subordinate authorities issue certificates to users and other end entities and might also issue certificates to other subordinate CAs. Root CAs are implicitly trusted while subordinate CAs and clients derive trust from the root. The use of subordinate CAs will provide scalability, ease of administration, and consistency with a growing number of third-party CA products.

Incorrect Answers:
A: A stand alone CA is a Windows 2000 certification authority that is not integrated with Active Directory while the root CA is the CA that is located at the topmost point in the CA hierarchy. We will be implementing Active Directory in this scenario therefore we should use an Enterprise CA as the enterprise CA is integrated with Active Directory and can thus use Active Directory for user information and can publish the CRL to Active Directory instead of requiring the certificate requestor to supply all user-identifying information.
C: We can use third-party certificate services to deploy CAs and issue certificates for our organizations, however, Windows 2000 Certificate Services provide many benefits that third-party CAs do not because Windows 2000 Certificate Services are fully integrated with the Windows 2000 public key infrastructure and Active Directory.

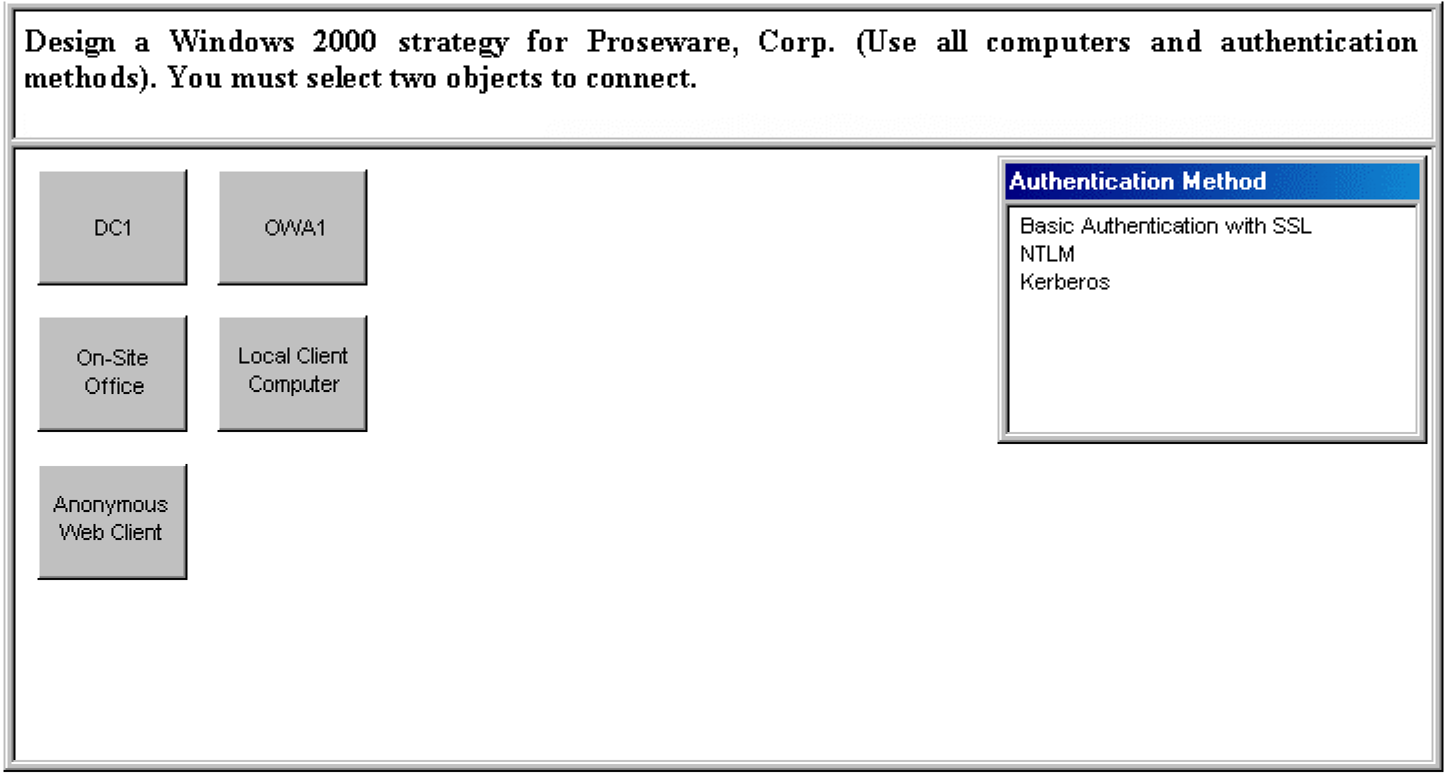
D: A stand alone CA is a Windows 2000 certification authority that is not integrated with Active Directory while the subordinate CA is the CA that is located below the root CA in the CA hierarchy, and receives a certificate from the root CA. This will provide scalability, ease of administration, and consistency with a growing number of third-party CA products. However, we will be implementing Active Directory in this scenario therefore we should use an Enterprise CA.

Q. 9
How should you implement security for the HR department?

A. Assign the Server (Request Security) IPSec policy at the HR_Users OU, and assign the Client (Respond Only) IPSec policy at the domain level
B. Assign the Secure Server (Require Security) and the Client (Respond Only) IPSec policy at the Branch_Users, HR_Users, and IT_Users OUs
C. Assign the Secure Server (Require Security) IPSec policy at the HR_Servers OU, and assign the Client (Respond Only) IPSec policy at the Domain level.
D. Assign the local policy and the Client (Respond Only) IPSec at the domain level.

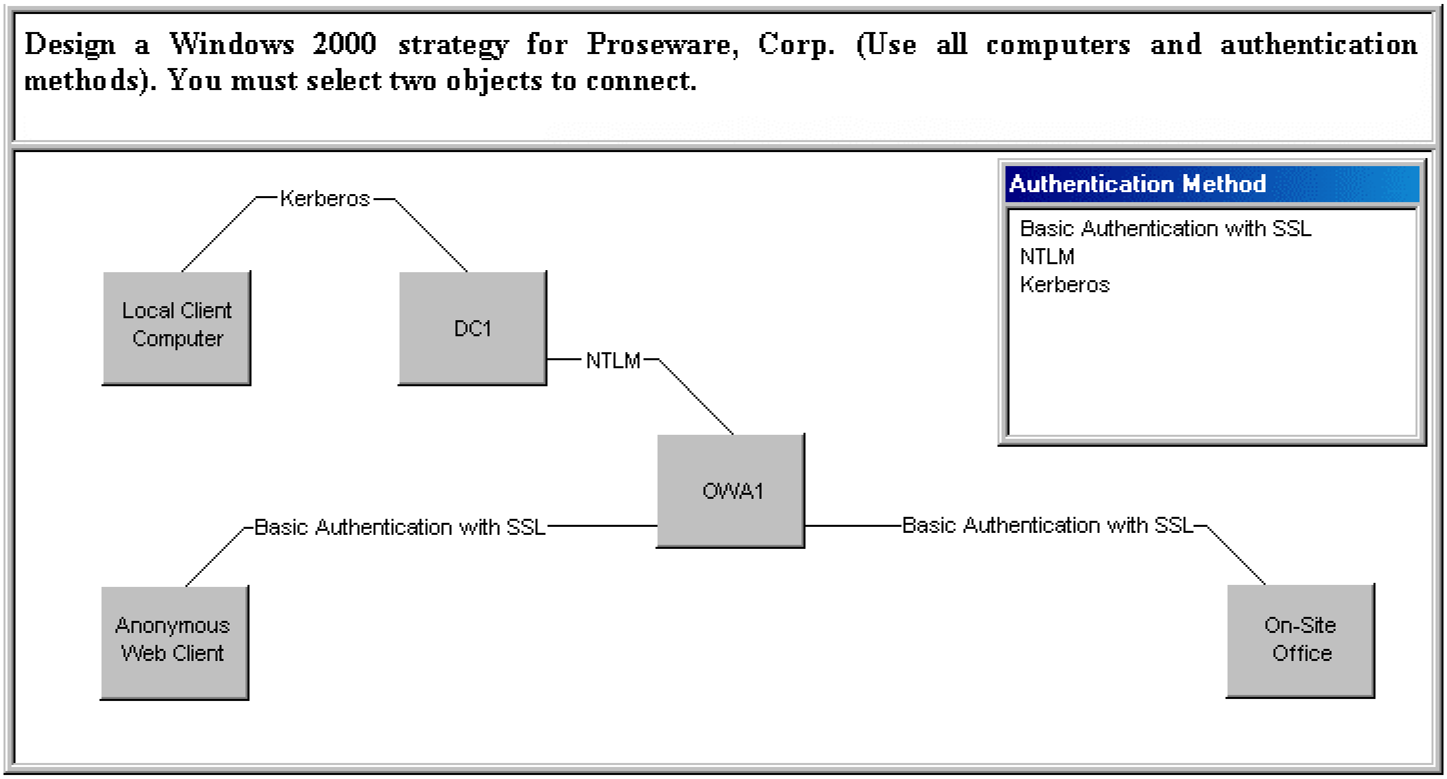
Answer: C
Explanation:

Q. 10



Design a Windows 2000 strategy for Proseware, Corp. (Use all computers and authentication methods). You must select two objects to connect.

Answer:



Design a Windows 2000 strategy for Proseware, Corp. (Use all computers and authentication methods). You must select two objects to connect.

Explanation:

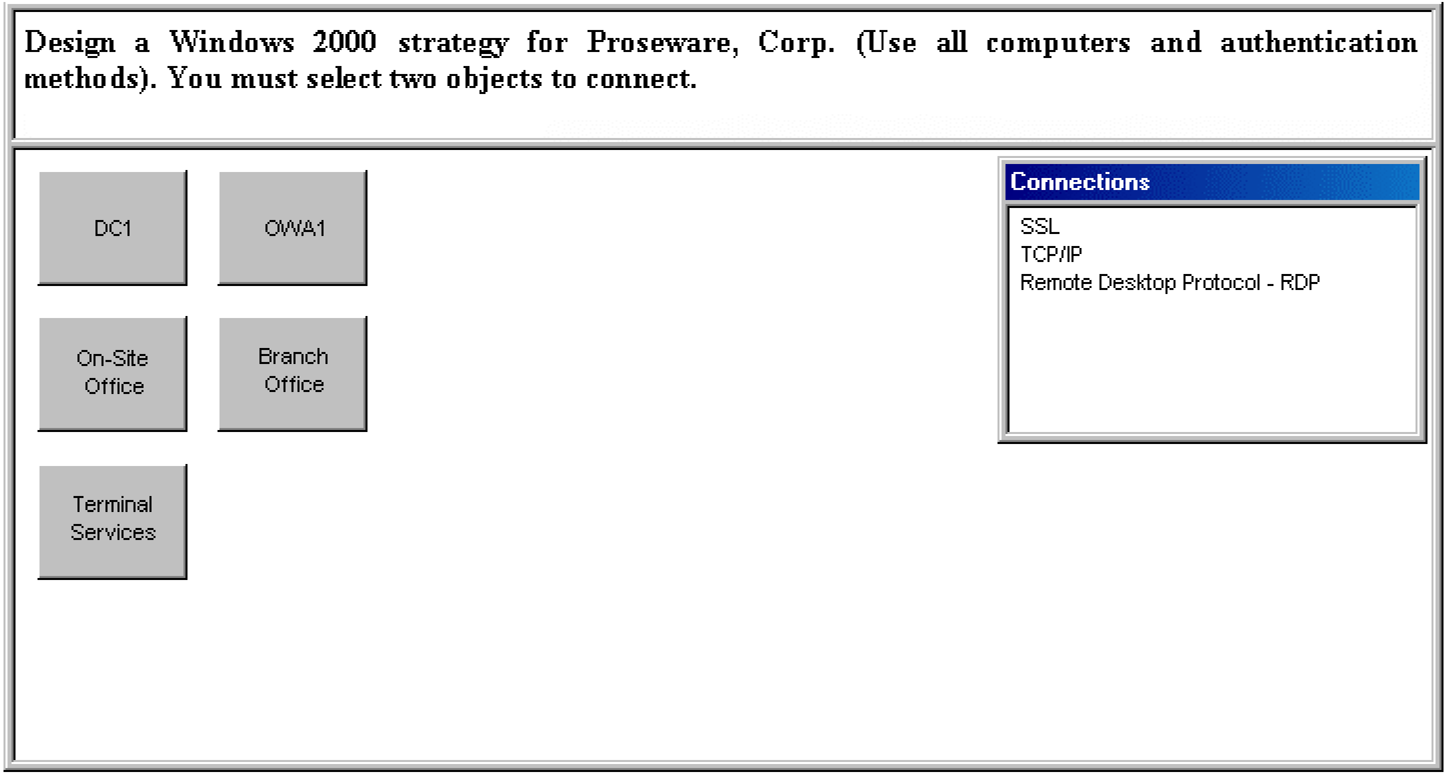
Local Client Computers and DC1 are located on the network at Headquarters. They are Windows 2000 computers. Kerberos is the default authentication protocol used on Windows 2000 computers.

OWA1, however, is a Windows NT 4.0 server that will not be upgraded. Windows NT 4.0does not support Kerberos. Windows 2000 does support NTLM which is the default authentication protocol on Windows NT 4.0 computers. We can thus use NTLM for network communication between DC1 and OWA1

Both Anonymous Web Clients and the On-Site Offices would use their Web Browsers to connect to Headquarters via OWA1. Basic Authentication is supported by all types of Web browsers, including the oldest ones. If users accessing our site are using older browsers that cannot be authenticated using other forms of authenticated access, we would need to enable basic authentication. With Basic Authentication, the customers will be presented with a dialog box requesting credentials and those credentials are then passed over the network connection in unencrypted form, which is intrinsically not secure. We can use SSL to establish a secure session and make passwords more secure, and hence Basic authentication more secure. SSL is short for Secure Socket Layer and was developed by Netscape for transmitting private documents securely via the Internet. SSL secures communication by using a public key to encrypt data that is transferred over the SSL connection. Many e-commerce websites use the protocol to secure the transmission of confidential user information such as credit card numbers. SSL is supported on both Navigator and Internet Explorer. By using Basic authentication and

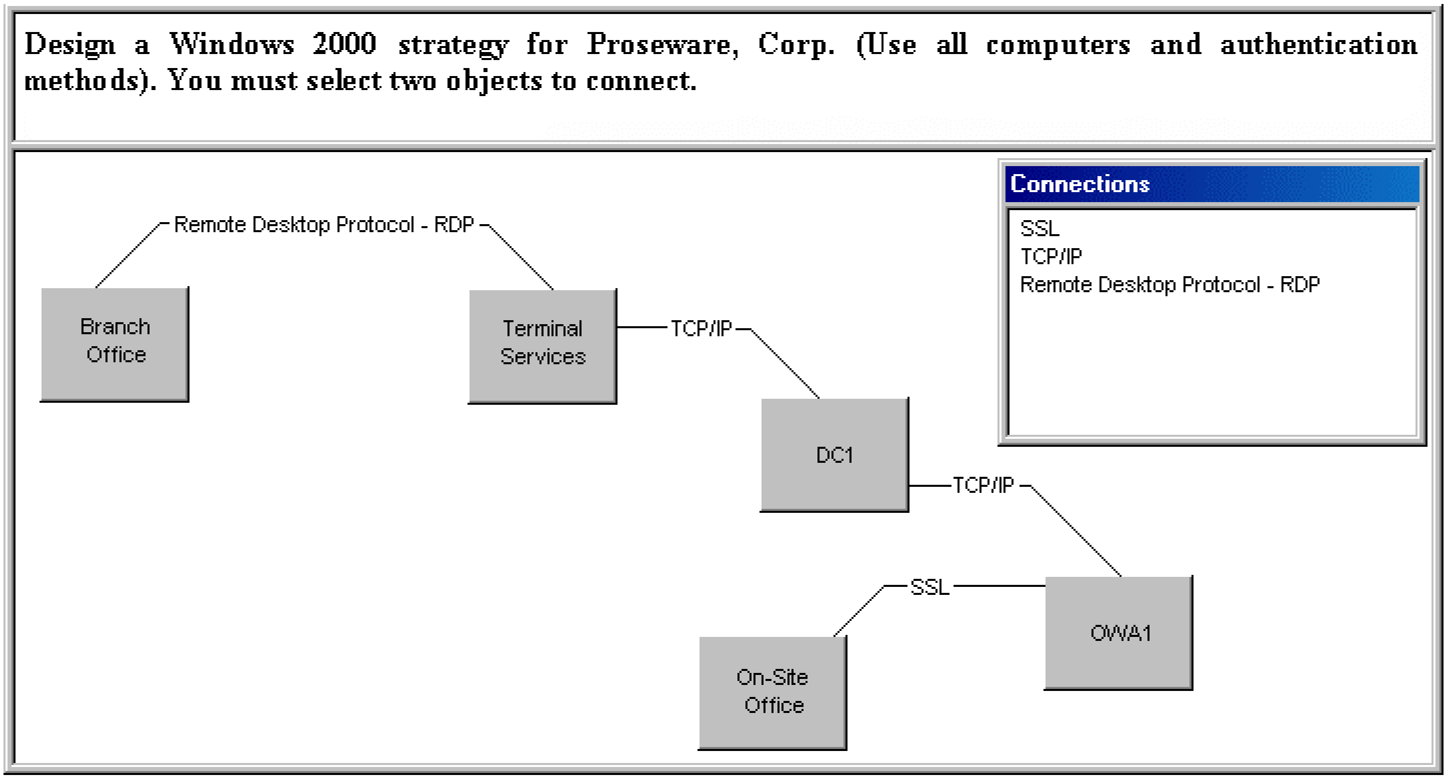
SSL, the password will still not be encoded, but the HTTP session carrying the data will be encrypted using cryptographically-secure mechanisms.

Q. 11



Design a Windows 2000 strategy for Proseware, Corp. (Use all computers and authentication methods). You must select two objects to connect.

Answer:



Design a Windows 2000 strategy for Proseware, Corp. (Use all computers and authentication methods). You must select two objects to connect.

Explanation:

Terminal services uses the RDP protocol to receive input from remote clients, in this scenario from clients at the Branch offices

Terminal Services, DC1 and OWA1 are located at network at Headquarters. They would thus be connect via TCP/IP which is the default protocol used in Windows 2000 networks.

The on-site offices would use OWA1 to access the network at Headquarters from the Internet. We would implement SSL to secure communication across the Internet.