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 nu mber, and credit card number. This information, including the customer's ID a nd 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:

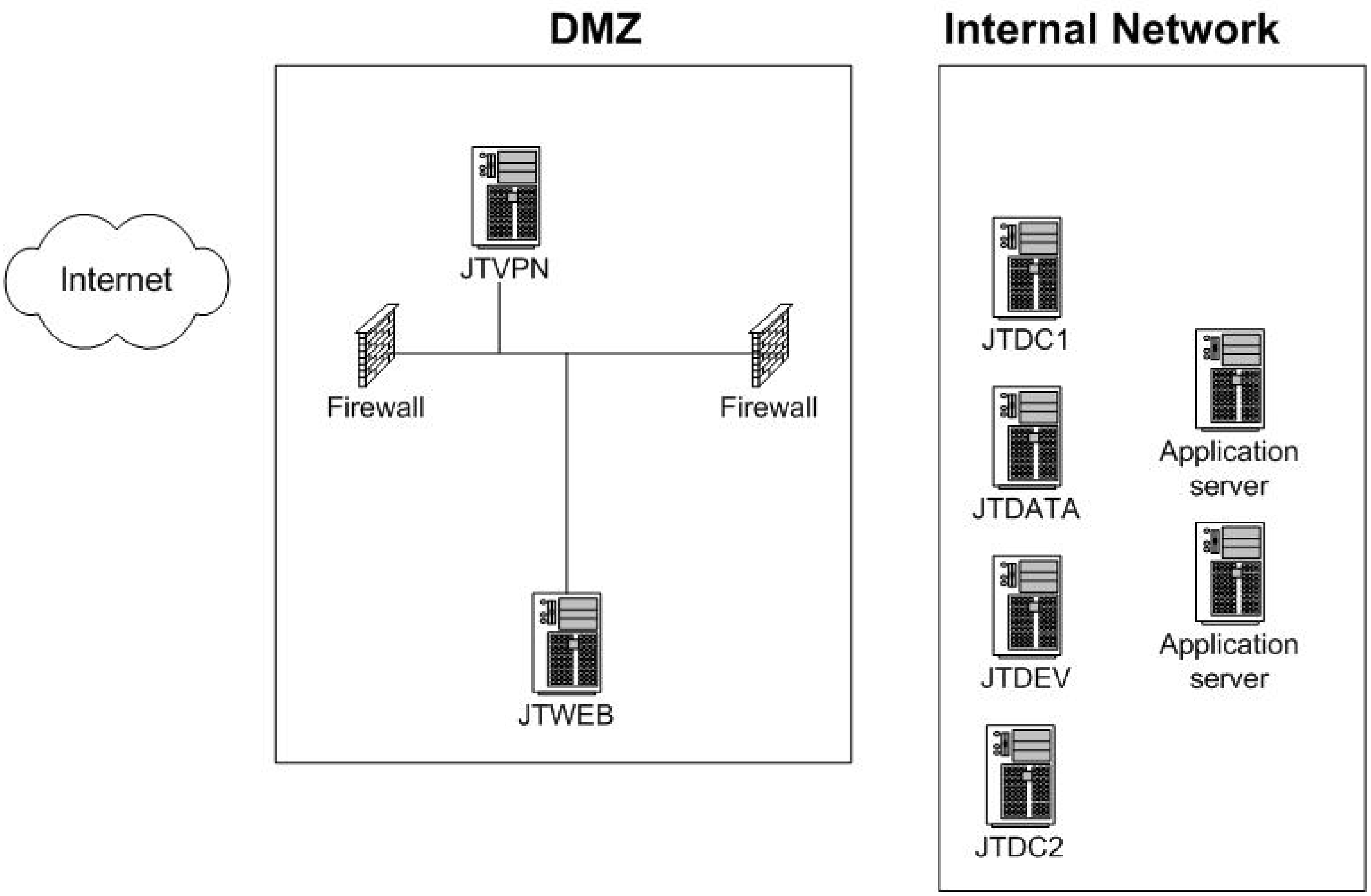
Headquarters:
Headquarters has four Windows NT Server 4 0 computers. The remote access server is named JTRAS. The primary domain controller is named JTDC1. The other two servers are used to run applications.

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 200 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. 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: D
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 cannot use NTLM either since it can only be used within a domain. We must can use anonymous login. 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:
A: NTLM logon can only be used within a domain, not on a web accessed by external customers from the Internet.
B: 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'spassword 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.

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 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.

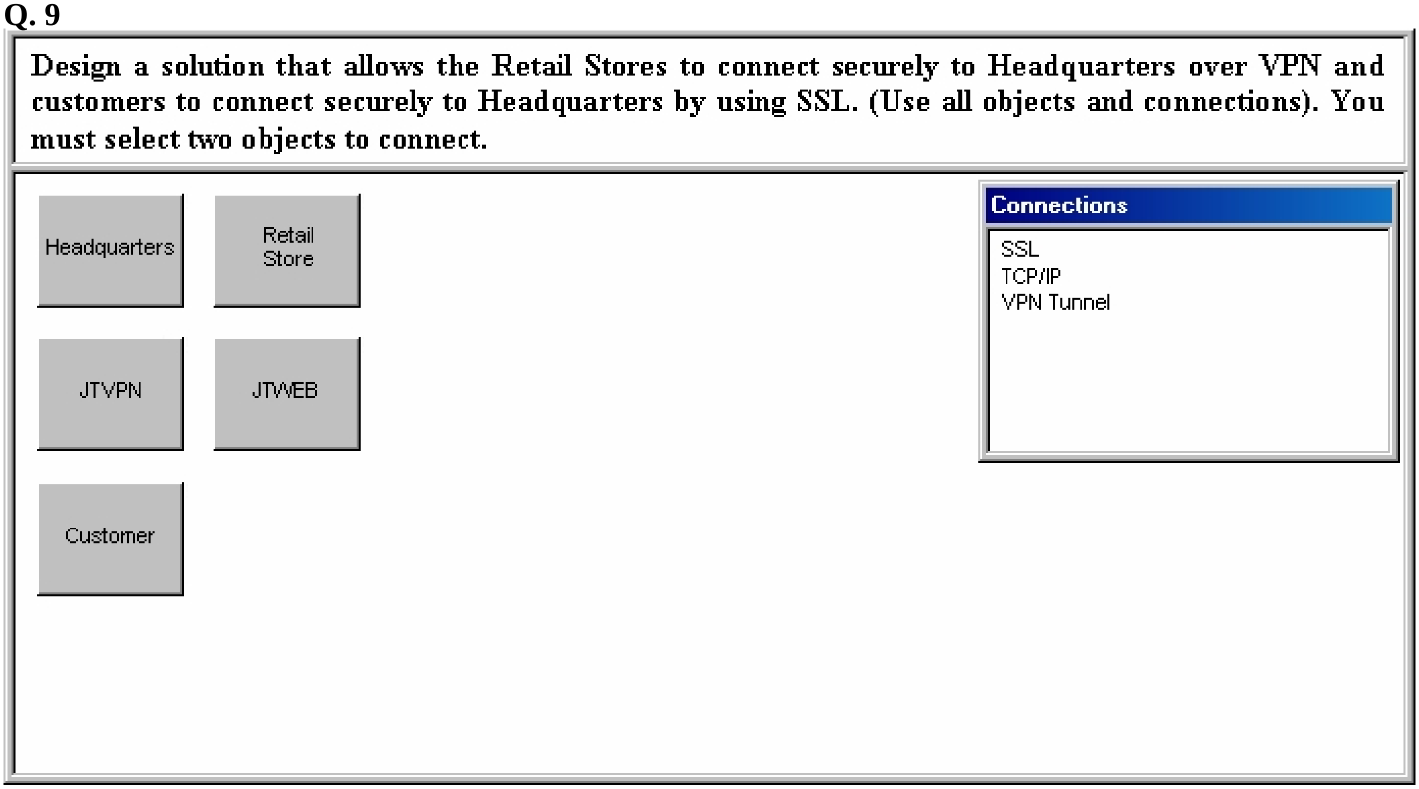
Incorrect Answers:

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.

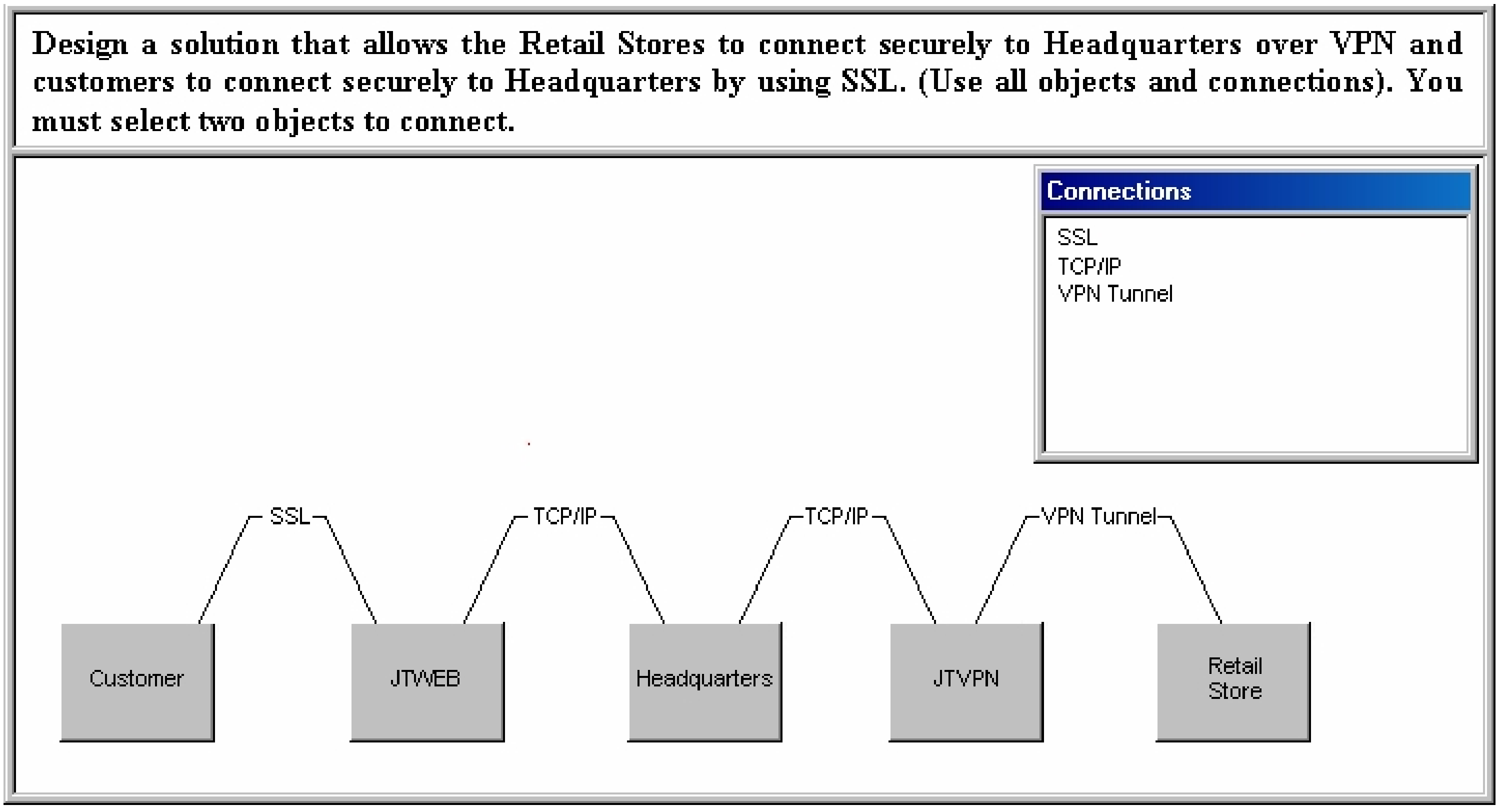
D: A VNP requires the presence of an existing IP connection exist before we can establish a VPN connection, which is a tunnel that runs over an existing network connection. VNP is not used to dial-up directly to the host server. Instead it tunnels through an existing IP network, such as the Internet. 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.

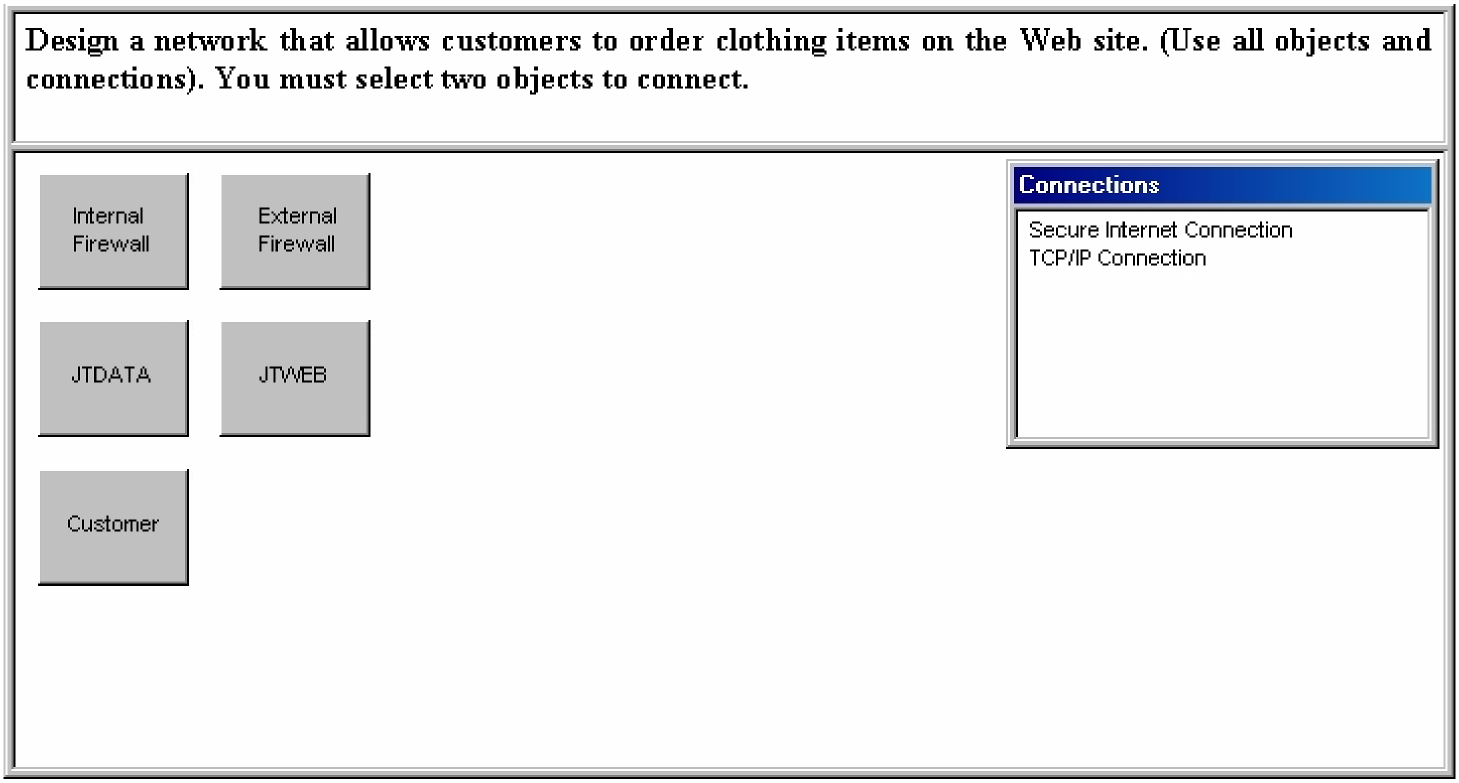
Explanation:
We need to secure network communication between customers and the Just Togs Web site which is hosted on the JTWEB server. This network communication is across the Internet therefore we should use SSL to secure this communication.

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.

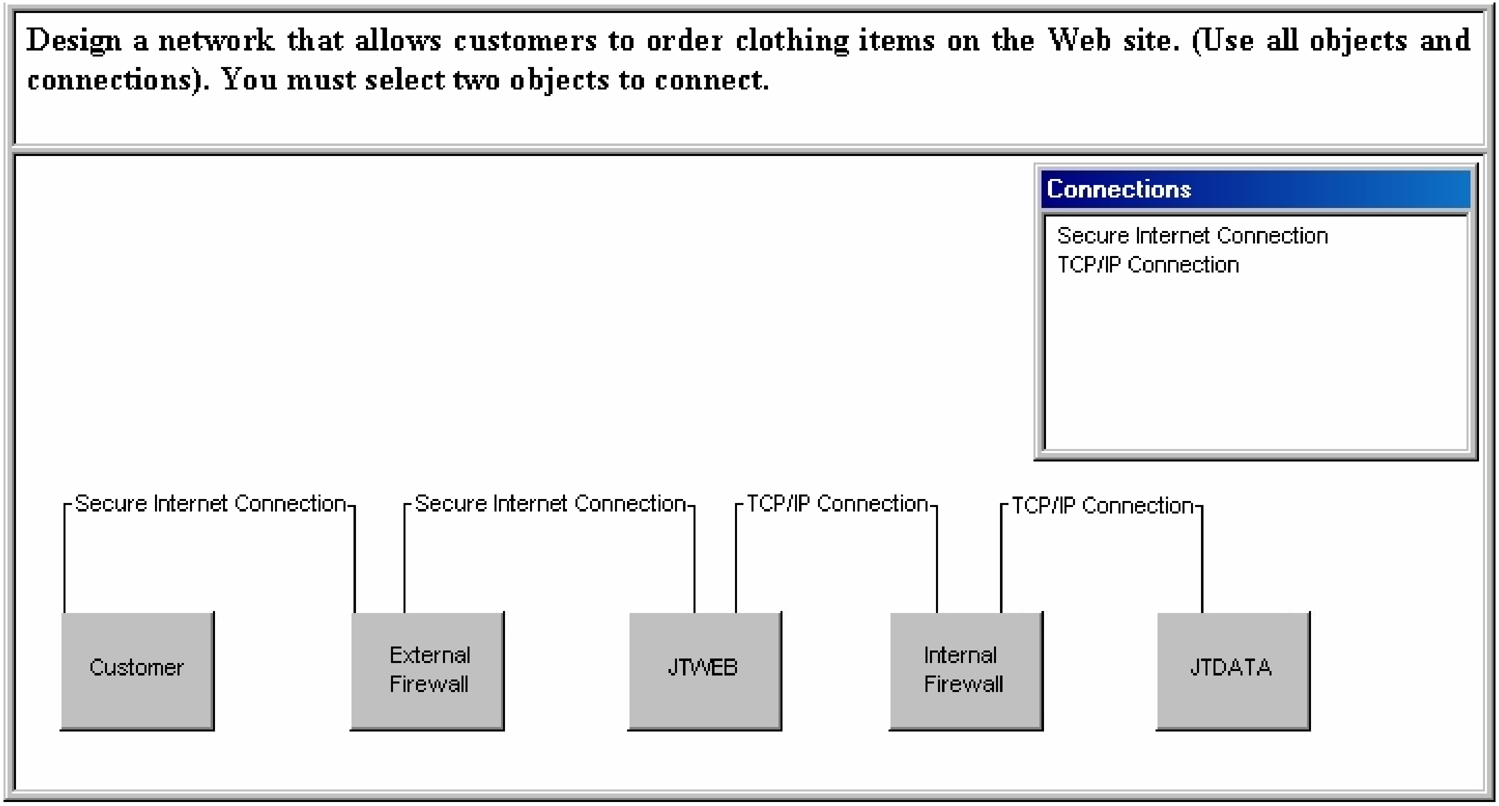
The JTVPN server is also a server located in the domain at Headquarters. There would therefore be a trust relation between JTVPN and the Domain Controllers at Headquarters. Consequently, we only require the TCP/IP connection within the domain.

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