Microsoft 70-284

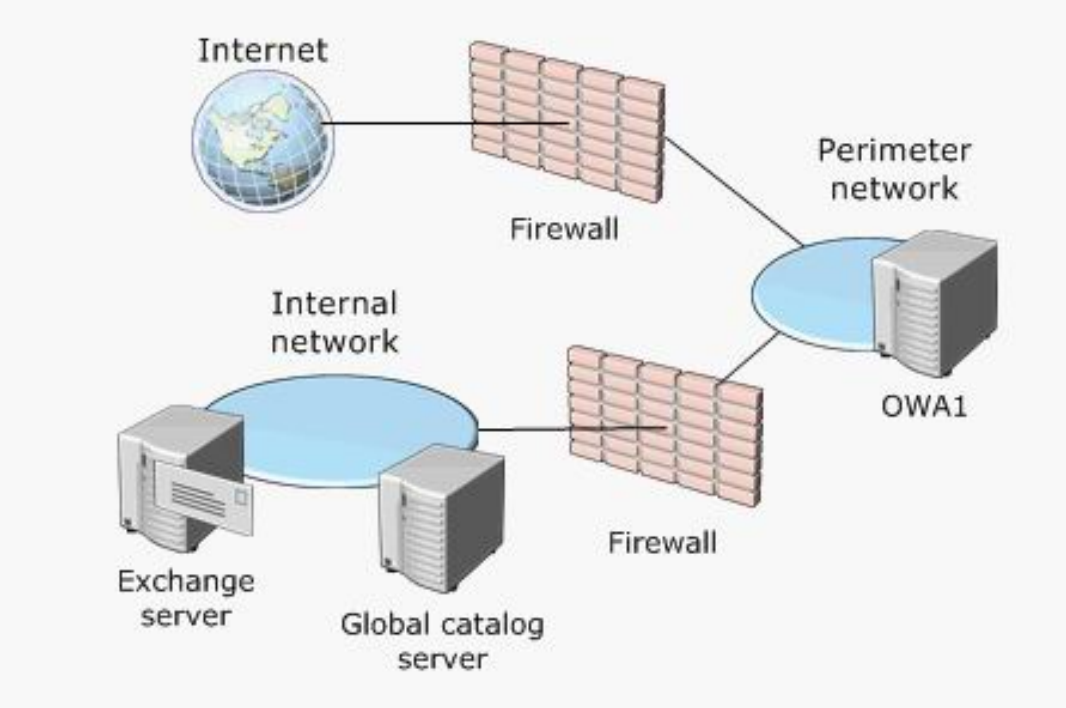
Microsoft 70-284 Installing, Configuring, and Administering Microsoft Exchange 2003 Server Implementing &Managing MS Exchange Server 2003

Practice Test

Version 2.5

QUESTION NO: 1

You are the Exchange administrator for your company. All Exchange servers run Exchange Server 2003. The relevant portion of the network configuration is shown in the exhibit. (Click the Exhibit button.) OWA1 is a front-end server. Its only function is to enable Internet users to access their Exchange mailboxes by using Microsoft Outlook Web Access over SSL. Internet users report that they cannot access their mailboxes. They receive an error message stating that the page or server cannot be located. You discover that internal users can access OWA1 and can use Outlook Web Access. You need to ensure that Internet users can access their e-mail. To achieve this goal, you plan to reconfigure the Internet firewall so that Internet users can access only one port on OWA1. Which protocol should be accessed by Internet users?



A. HTTP
B. HTTP SSL
C. IMAP4 SSL
D. IMAP4

Answer: B

Explanation:
HTTP SSL use port 443. The external firewall does not currently allow on port 443 traffic to pass. Reconfigure Internet firewall on port 443 will permit to Internet users to access by OWA to OWA1.

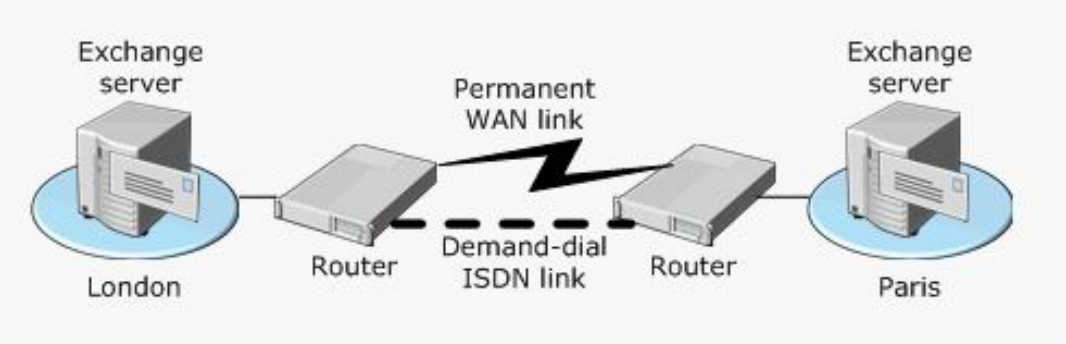
Ports to open for OWA access in a perimeter Firewall architecture

Origin	Destination	Service	Protocol and port
Internal/External	Perimeter network	HTTP HTTPS IMAP4 IMAP4TLS	TCP 80 TCP 443 TCP 143 TCP 993
Perimeter Network	Network Internal/Private	DNS HTTP RPC EndPoint Mapper KERBEROS LDAP NETLOGON DSAccess (GC) TCP High Ports	TCP, UDP 53 TCP 80 TCP 135 TCP UDP 88 TCP 389 TCP 445 TCP 3268 TCP 1024+

Reference:
MS white paper Exchange Server 2003 RPC over HTTP Deployment Scenarios
MS white paper Exchange Server2003 Client Access Guide
MS white paper Exchange 2003 Front-End Back-End Topology

QUESTION NO: 2

You are the Exchange administrator for your company. The relevant portion of the network is configured as shown in the following diagram. The network serves two offices, one in London and one in Paris. Each office contains a single Exchange Server 2003 computer in its own routing group. The routing groups are connected by a routing group connector. The only network traffic between the two offices is e-mail messages. There is a permanent WAN link that connects the two offices. The WAN link is connected to a hardware router in each office. The two hardware routers each also have an ISDN dial-up interface. Demand-dial routing is defined between the two offices. You view network utilization statistics in the Paris office, and you discover that traffic from the Paris Exchange server frequently causes the ISDN link to connect. There is little utilization of the permanent WAN link between the two offices. The WAN link has been very reliable and has suffered no downtime. You need to ensure that the ISDN link is used only when the permanent WAN link fails. What should you do in the Paris office?



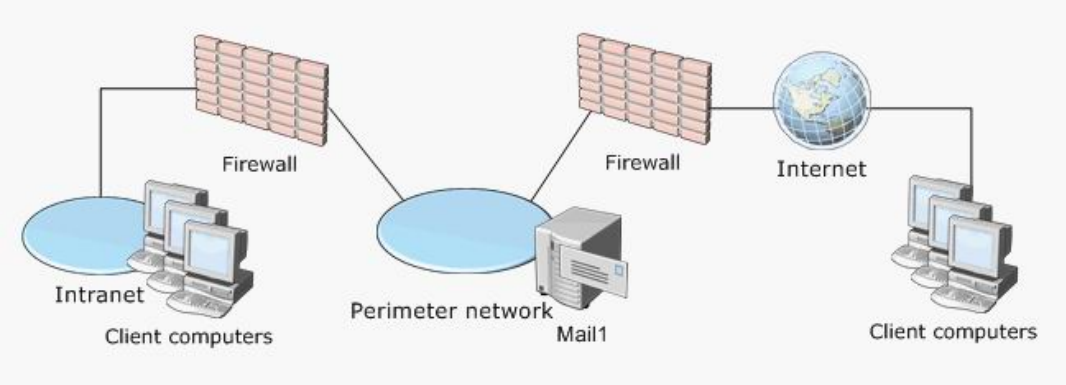
A. On the Exchange server, replace the routing group connector with an SMTP connector that uses the London Exchange server as a smart host.
B. On the Exchange server, replace the routing group connector with an SMTP connector that uses the ETRN command.
C. On the Exchange server, create a TCP/IP static route to the London Exchange server.
D. Request the network administrator to remove the IP route that uses the ISDN link from the routers.
E. Request the network administrator to reconfigure the routers, so that the IP route that uses the ISDN link is assigned a higher cost than the permanent WAN link.
F. Request the network administrator to reconfigure the routers, so that the IP route that uses the ISDN link is assigned a lower cost than the permanent WAN link.

Answer: E

Explanation:
When you assign a higher cost to a route, that route will only be used if the primary line fails.

QUESTION NO: 3

You are the Exchange administrator for your company. The Exchange organization contains a single Exchange Server 2003 computer named Mail1. Mail1 is connected to a perimeter network. The relevant portion of the network is configured as shown in the exhibit. (Click the Exhibit button.) Mail1 hosts Microsoft Outlook Web Access and all user mailboxes. To access Mail1, intranet users use Outlook, and Internet users use Outlook Web Access. Mail1 is the target of a series of HTTP-based denial of service (DoS) attacks from the Internet. Each attack makes Mail1 unavailable to all users for a long time. You need to implement a solution that will protect Mail1 from DoS attacks. You need to ensure that Internet users can use Outlook Web Access to access their e-mail. Even during an attack, Mail1 must be available to intranet users. Your solution must not compromise the security of the internal network. What should you do?



A. Move Mail1 to the intranet. Configure both firewalls to allow HTTP traffic from the Internet to pass to Mail1.
B. Install a new server that runs Exchange Server 2003. Move half of the mailboxes from Mail1 to the new Exchange server.

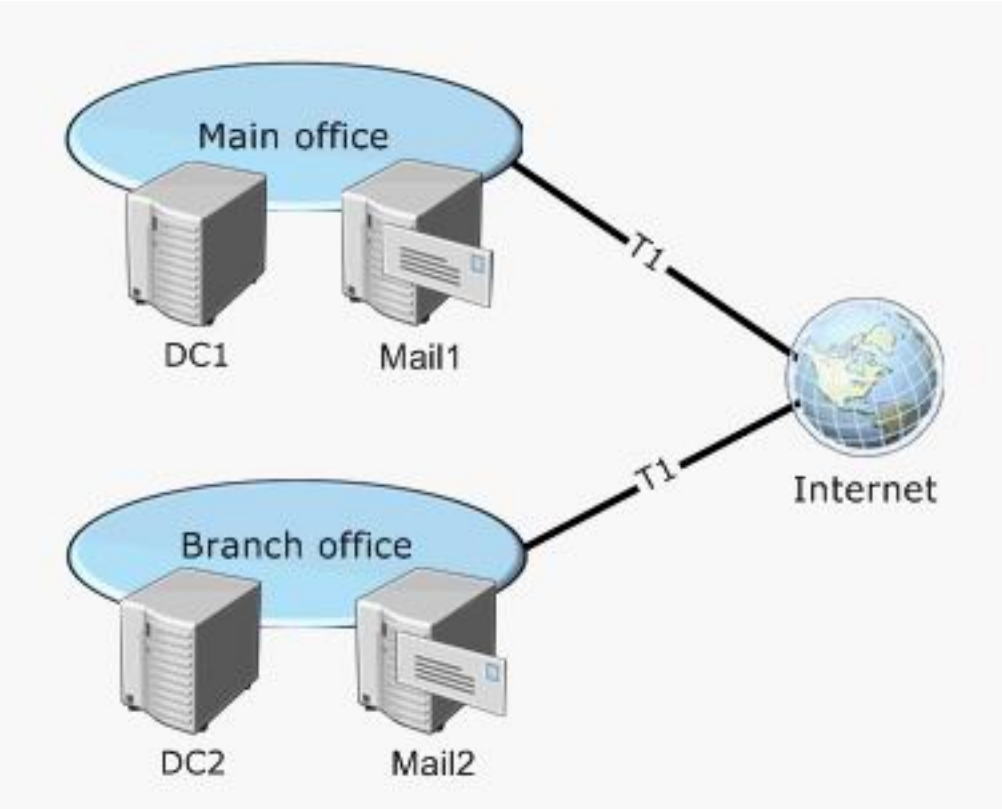
C. Move Mail1 to the intranet. Install a new server that runs Exchange Server 2003 on the perimeter network. Name the server Mail2 and configure it as a front-end server that hosts Outlook Web Access.
D. Configure the internal firewall to block all HTTP traffic from the Internet. Configure the external firewall to block all HTTP traffic from the intranet.

Answer: C

Explanation:
When you assign a higher cost to a route, that route will only be used if the primary line fails.

QUESTION NO: 4

You are the network administrator for your company. The company operates a main office and one branch office. Both offices are connected to the Internet and use a VPN for interoffice communications. The relevant portion of the network is configured as shown in the exhibit. (Click the Exhibit button.) The network consists of a single Active Directory domain. Each office has one domain controller. Each office also has one Exchange Server 2003 computer, which hosts all mailboxes for users in that office. Users in the branch office report that sending e-mail messages from Mail2 sometimes requires several minutes. However, the problem does not occur consistently. You discover that a large quantity of LDAP queries are passed from the branch office to DC1. You verify that DC2 is configured as a global catalog server. You need to reduce the LDAP traffic sent across the VPN. What should you do?



A. Add the fully qualified domain name (FQDN) and IP address of DC2 to the Hosts file on Mail2.
B. Promote Mail2 to domain controller.
C. Configure Mail2 to force the selection of DC2 as a global catalog server.
D. Modify Active Directory to place both office networks in the same site.

Answer: C

Explanation:
Exchange use Dsaccess service to find a set of available directory service servers. For each available directory service server, DSAccess opens LDAP connections dedicated solely on behalf of each process that is using DSAccess . DSAccess updates these LDAP connections with directory service state information (Up, Slow, or Down) that it detects, and channels requests based on this state information. The set of LDAP connections to those available domain controllers and global catalogs and their associated states forms the profile of the process. For reliability and scalability, DSAccess supports a load-balancing mechanism to distribute user context directory service requests in a round-robin fashion among these LDAP connections.

Only one Recipient Update Service is active within each Active Directory domain; the others remain idle. The Recipient Update Service is fully integrated with the Exchange System Attendant (Mad.exe). According to the schedule you've set or by means of the Update Now option, the service contacts a local domain controller and proceeds to update address lists based on the rules set.

By default DSAccess is configured to perform the "automatically discover servers"

Mail2 is not included in the same site as DC1 and DSAccess is already configured with DC1 as the configuration server for the tesking.com domain. It is thus querying to DC1 server across the wan link and generating a large quantity of LDAP queries

To fix this issue you can change dcsaccess order and point to DC2 by changing the automatically discover server to manually although is not a MS recommended practice

Incorrect Answer
* Can FIX the problem but is not a good option
* If tesking2 can resolve DC1 you can suppose that resolve DC2, but the problem is not resolve the name is resolve who the global catalog and configuration domain controller for Exchange
* If you put both DC's in the same site, Exchange mad.exe will be still querying to DC1 as Configuration Domain Controller

References
Understanding and Troubleshooting Directory Access MS Book Online
Microsoft Exchange 2000 Server Service Pack 2 Deployment Guide
Event ID 2080 from MSExchangeDSAccess KB article 316300

QUESTION NO: 5

You are the Exchange administrator for your company. The network consists of a single Active Directory domain. A server named Exch1 runs Exchange Server 2003 and hosts all user mailboxes. Exch1 also sends and receives SMTP e-mail messages to and from the Internet. Exch1 is protected by a firewall that connects the intranet to the Internet. Users report that they receive a large number of unsolicited e-mail messages every day. You discover that all users receive the same unsolicited e-mail messages, which are sent to a universal distribution group in the domain. You need to ensure that distribution groups cannot be used to send e-mail messages from the Internet to company users. Your solution must not affect the ability of company users to send and receive legitimate e-mail messages. What should you do?

A. Convert the universal distribution groups to universal security groups.
B. Configure Exch1 to reject incoming SMTP traffic from external IP addresses.
C. Configure the distribution groups so that messages are only accepted from authenticated users.
D. Configure Exch1 to send and receive SMTP traffic to and from the firewall. Configure the firewall to reverse publish the SMTP port on Exch1.

Answer: C

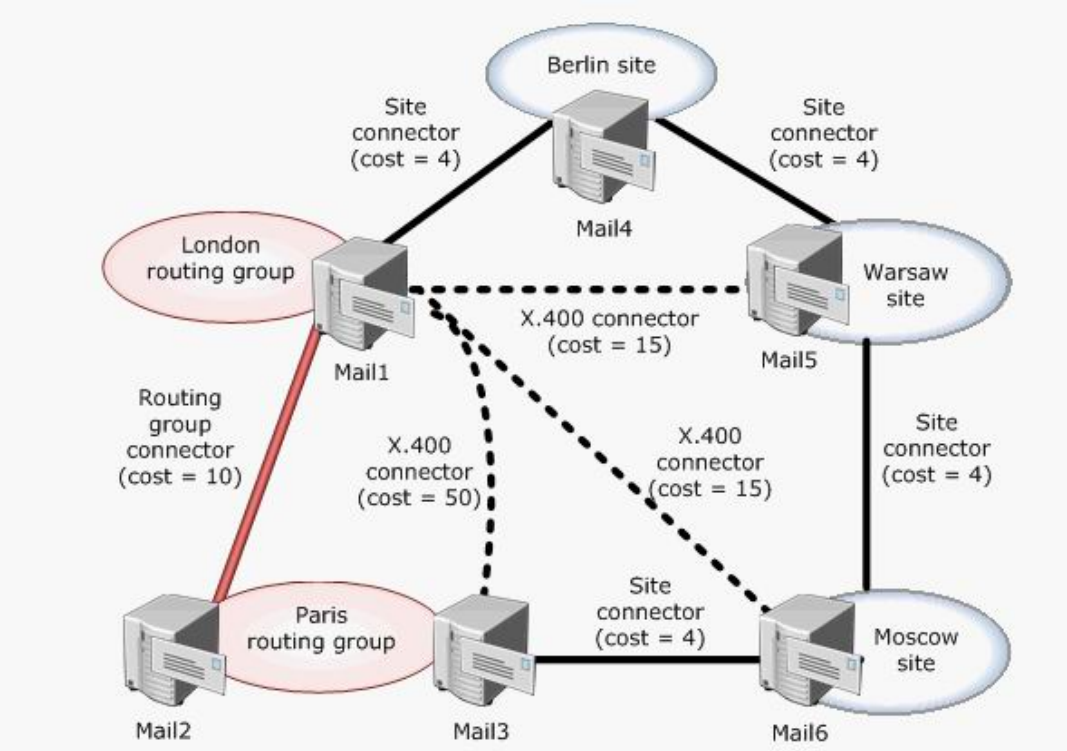
Explanation:
The universal group is used for mail distribution in your organization. To stop receiving spam, you can configure the distribution group to accept mail for authenticate users only.

Incorrect answers
* Converting universal group to security group on its own will not protect your against unsolicited mail.
* If you configure Exch1 to reject incoming SMTP traffic from external IP addresses, you will not receive mail from anybody.
* Although not recommended, you can position the Exchange Server2003 front-end server acting as the RPC proxy server inside the perimeter network. In this scenario, you configure your Exchange servers as in Scenario1. However, you will need to make sure to open the ports required by RPC over HTTP on your internal firewall, in addition to those already required for an Exchange front-end server. The ports for RPC over HTTP are TCP6001, 6002, and 6004.

Reference:
MS white paper Exchange Server 2003 RPC over HTTP Deployment Scenarios
MS white paper Exchange Server2003 Client Access Guide
MS white paper Exchange 2003 Front-End Back-End Topology
MS white paper Exchange Server 2003 Message Security Guide
MS white paper Microsoft Exchange Intelligent Message Filter Deployment Guide

QUESTION NO: 6

You are the Exchange administrator for your company. The Exchange organization is shown in the exhibit. (Click the Exhibit button.) In the Paris routing group, Mail2 runs Exchange Server 2003, and Mail3 runs Exchange Server 5.5. Mail2 is configured as the bridgehead server for all routing group connectors in the Paris routing group. Mail3 is configured as the bridgehead server for the X.400 connector in the Paris routing group. Mailboxes for all Paris users are on Mail3. Mail2 is shut down for repairs. Users who have mailboxes on Mail1 report that there is an unusual delay in the delivery of messages to Paris recipients. You discover that messages between London users and Paris users are being forwarded to the servers in the following sequence: Mail1, Mail4, Mail5, Mail6, and Mail3. You need to ensure that messages are delivered as quickly as possible between the London and Paris routing groups. You do not want to alter the normal flow of messages between any of the other sites or routing groups. What should you do?



A. Decrease the cost of the X.400 connector between the London and Paris routing groups to 20.
B. Decrease the cost on the routing group connector between London and Paris to 5.
C. Modify the routing group connector between the London and Paris routing groups to add Mail3 to the list of bridgehead servers in the Paris routing group.
D. Increase the cost of all site connectors to 25.

Answer: C

Explanation:
There must be a routing group connector between routing groups if you want to be able to send mail between them. In this case we have two links. They told us that Mail2 is shut down for

repairs. Mail2 is also the bridgehead server for all routing group connectors in the Paris routing group.

If Mail2 is down, the new server in routing group is Mail 3. The only way to go form London to Paris will be based on cost. I f we add Mail 3 to the list of London routing group connector and because this server is Exchange 2003, and because by default the cost will be 10 the mail will be flow through the company site connector between Mail1 and Mail4

Incorrect answers:
* Increasing the cost of all connectors to 25 will disrupts the normal flow of mail for all other sites
* Decreasing cost of routing group connector between London and Paris to 5 would not help as the other server in Paris is not a bridgehead server and does not automatically accept connections. (In 5.5, bridgehead connections did not exist, but there would be an explicit site connector, and that connector does not exist here.) Even if it did, the given value of 10 would have still work, and mail would not take the circular route that is currently the problem.
* Decreasing the cost of the London to Paris routing group cost to 20 would still be higher than the link costs of the current route combined, and would be higher than the x.400 connection between London-Moscow-Paris.

QUESTION NO: 7

You are the Exchange administrator for your company. The Exchange organization contains three Microsoft Windows Server 2003 member servers that run Exchange Server 2003. The company's network has a firewall. One of the functions of the firewall is queuing and delivery of outbound SMTP mail. The written company policy states that Exchange servers must not send SMTP mail directly to the Internet. The three Exchange servers must be able to send mail directly to each other. You need to ensure that messages for external recipients are delivered to the Internet through the firewall. What should you do?

A. Configure each SMTP virtual server to use the firewall as a smart host.
B. Configure an SMTP connector that will use the firewall as a smart host.
C. Configure each SMTP virtual server to use the firewall as its external DNS server.
D. Configure each SMTP virtual server to forward e-mail with unresolved recipients to the firewall.

Answer: A

Explanation:
The three Exchange servers must be Able to send mail directly to each other. We can achieve this by using routing groups. The company policy states that Exchange servers must not send SMTP mail directly to the Internet. Therefore, w e will need to configure on each a SMTP connector that will send all the traffic to an smart host in this case the firewall because they require that One of the functions of the firewall is queuing and delivery of outbound SMTP mail.

Incorrect answers:
* Since the firewall has no DNS lookups, this will not work. In addition, any external lookups from the Exchange Server will fail.
* The mail would cease to be routed at this point, as the firewall would not know what to do with the SMTP traffic once it arrived
* To be a possible answer the statement must be Configure an SMTP connector for each SMTP virtual server to use the firewall as a smart host

References
MS article 821911, How to Configure Exchange Server 2003 to Use a Smart Host IP Address
Using ISA Server 2000 with Exchange Server 2003 MS White paper

QUESTION NO: 8

You are the Exchange administrator for your company. The Exchange organization contains 10 servers that run Exchange Server 2003. All users send and receive e-mail messages by using Microsoft Outlook. Your company has many different departments and a total of 10,000 users. For each department, management asks you to create one address list that contains all users in that department. Management also asks you to create a confidential address list. The membership of the confidential address list will consist of several users from every department. For each department, you create an address list that uses the department attribute. Now you need to create the confidential address list. You must ensure that members of the Managers group are the only users who can identify the members of the list by using Outlook. You must not affect any existing e-mail functionality. What should you do?

A. Modify the permissions on the user accounts of individuals in the confidential address list so that only the Managers group has permission to send e-mail messages to these accounts. Create a confidential address list that includes the required user accounts.
B. Modify the permissions on the user accounts of individuals in the confidential address list so that only the Managers group has permission to view these accounts. Create a confidential address list that includes the required user accounts.
C. Configure the department attribute as Confidential for the user accounts of individuals in the confidential address list. Create an address list that uses the department attribute. Modify the permissions on the address list so that only the Managers group has permission to view its membership.
D. Configure a custom attribute as Confidential for the user accounts of individuals in the confidential address list. Create an address list that uses the custom attribute. Modify the permissions on the address list so that only the Managers group has permission to view its membership.