



TestKingprep.com

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

70-350

Congratulations!

You have purchased a TestKingprep. Study Guide.

This study guide is a complete collection of questions and answers that have been developed by our professional & certified team.

You must study the contents of this guide properly in order to prepare for the actual certification test. The average time that we would suggest you for studying this study guide is approximately 10 to 20 hours and you will surely pass your exam. We guarantee it!
GOOD LUCK!

DISCLAIMER

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

Guarantee

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

Sales@TestKingprep.com

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

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

Question: 1

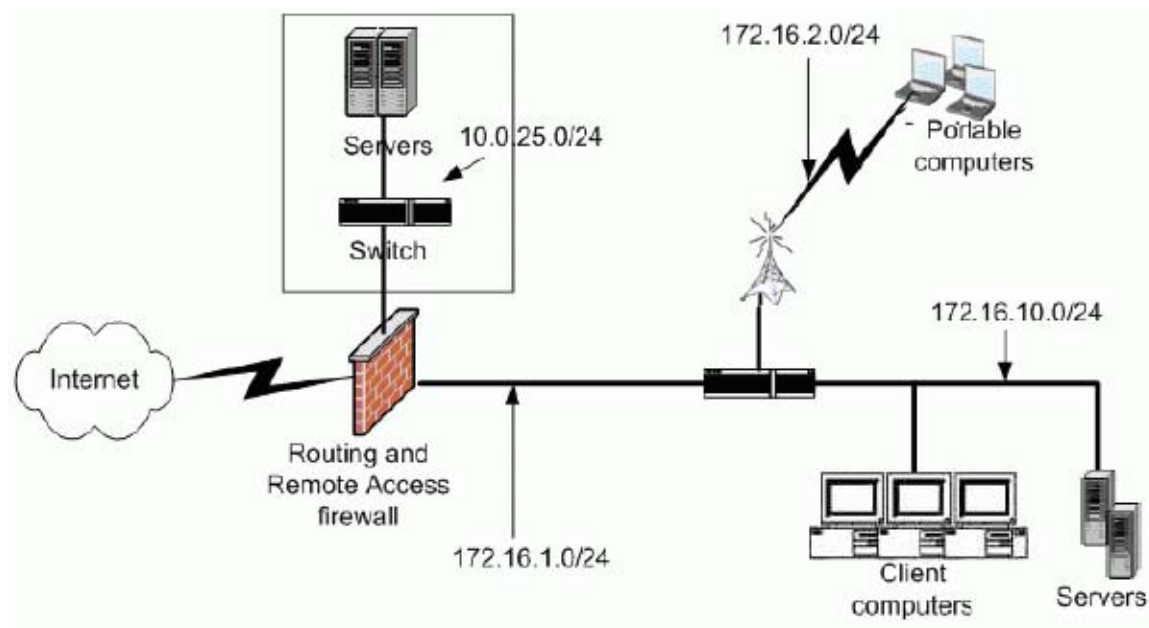
You are a network administrator for Company.com. You plan to implement ISA Server 2004 as a SecureNAT firewall for client computers on the network. The implementation will consist of a Windows Server 2003 Network Load Balancing cluster. External client computers that connect to resources published by ISA Server must be loadbalanced across the Network Load Balancing cluster when they connect by using DNS. You need to plan the external DNS implementation before you deploy ISA Server 2004. What should you do?

- A. Create three service locator (SRV) resource records. Configure each record to use the _HTTP service and to reference the IP address of one of the internal interfaces of the Network Load Balancing cluster nodes.
- B. Create three host (A) resource records. Configure each record with the IP address of one of the external interfaces of the Network Load Balancing cluster nodes.
- C. Create one host (A) resource record. Configure the record with the virtual IP address that is assigned to the external interface of the Network Load Balancing cluster.
- D. Create one host (A) resource record. Configure the record with the virtual IP address that is assigned to the internal interface of the Network Load Balancing cluster.

Answer: C

Question: 2

You are a network administrator for Company.com. The network is configured as shown in the exhibit.



You are upgrading the Routing and Remote Access server to ISA Server 2004. You need to configure the Internal network. You need to create access rules that are specific for each subnet. Which three IP address ranges should you use? (Each correct answer presents part of the solution. (Choose three)

- A. 10.0.25.1 - 10.0.25.255
- B. 172.16.1.0 - 172.16.1.255
- C. 172.16.2.0 - 172.16.2.255
- D. 172.16.10.0 - 172.16.10.255
- E. 192.168.1.0 - 192.168.255.255

Answer: B, C, D

Explanation:

A is not right because of that IP range is not Internal, it is a DMZ. B is an internal Range C is an internal Range D is an internal Range E is not found in the image at all

Question: 3

You are a network administrator for Company.com. Client computers on the internal network are divided among several subnets by using routers. You install an ISA Server 2004 computer named ISA1. ISA1 will be used to allow users to access Web sites on the Internet. You configure TCP/IP on ISA1 as shown in the exhibit.



```
Command Prompt
C:\Documents and Settings\Administrator\CONTOSO>ipconfig

Windows IP Configuration

Ethernet adapter External:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.212
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Internal:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 172.16.0.102
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 172.16.0.254

C:\Documents and Settings\Administrator\CONTOSO>
```

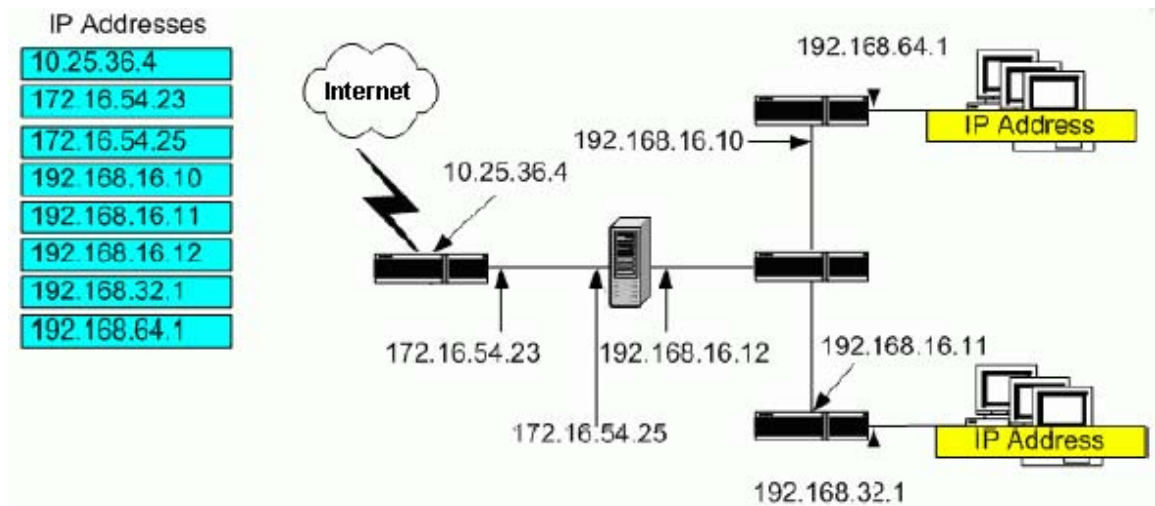
After ISA1 is installed, users report that they cannot access Web sites on the Internet. You need to ensure that users can access Web sites on the Internet. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Configure the internal default gateway to match the external default gateway.
- B. Configure a static route to each subnet.
- C. Add the IP address of the internal default gateway to the Remote Management Computers computer set.
- D. Configure the internal network adapter with a blank default gateway.
- E. Create a network set for each subnet.

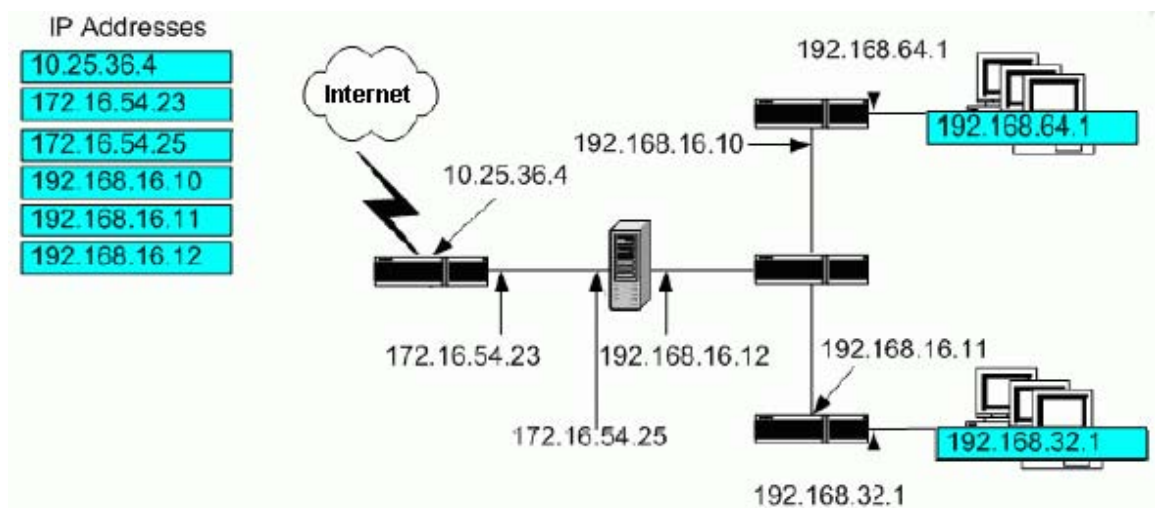
Answer: B, D

Question: 4 DRAG DROP

You are a network administrator for Company.com. You plan to deploy one ISA Server 2004 computer, three routers, and one switch to provide Internet access to client computers on the network. This planned network is shown in the answer area. You must ensure that client computers can access the Internet as SecureNAT clients after ISA Server is deployed. You examine several client computers and discover that the default gateway is not configured. You need to configure the correct default gateway for client computers. What should you do? To answer, drag the appropriate default gateway IP address or addresses to the correct groups of client computers in the answer area.



Answer:



Question: 5

You are a network administrator for Company.com. Company has a main office and three branch offices. You are planning to deploy ISA Server 2004 in the branch offices to provide users which access to the Internet. The ISA Server computers will be configured as stand-alone servers. The FirewallClient installation share will be placed on an existing file server in each branch office. You install Windows Server 2003 on the computers that will run ISA Server 2004. You need to configure additional security for the ISA Server computers. What are three possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose three)

- A. Grant the Allow log on locally right to only the Administrators group.
- B. Disable the external network adapter.
- C. Enable the Secure Server (Require Security) IPSec policy.
- D. Disable the Server service.
- E. Remove all users from the Access this computer from the network right.

Answer: A, D, E

Question: 6

You are a network administrator for Company.com. The network contains a single ISA Server 2004 computer named ISA1. ISA1 is not yet configured to allow inbound VPN access. You deploy a new application named App1. The server component of App1 is installed on an internal server named Company1. The client component of App1 is installed on employee and partner computers. Employees and partners will establish VPN connections when they use App1 from outside the corporate network. You identify the following requirements regarding VPN connections to the corporate network.

- 1 Employees must be allowed access to only Company1, three file servers, and an internal Web server named Web1.
- 2 Employees must have installed all current software updates and antivirus software before connecting to any internal resources.
- 3 Partners must be allowed access to only Company1.

4 You must not install any software other than the App1 client on any partner computers. You need to plan the VPN configuration for Company. What should you do?

- A. Configure ISA1 to accept incoming VPN connections from partners and employees. Enable Quarantine Control on ISA1. Configure Quarantine Control to disconnect users after a short period of time. Use access rules to allow access to only the permitted resources.
- B. Configure ISA1 to accept incoming VPN connections from partners and employees. Enable Quarantine Control on ISA1. Exempt partners from Quarantine Control. Use access rules to allow access to only the permitted resources.
- C. Configure ISA1 to accept incoming VPN connections from partners and employees. Enable Quarantine Control on ISA1. Enable RADIUS authentication and user namespace mapping. Configure a Windows Server 2003 Routing and Remote Access server as a RADIUS server. Create a single remote access policy.
- D. Add a second ISA Server 2004 computer named ISA2. Configure ISA1 to accept VPN connections from employees. Do not enable Quarantine Control for ISA1. Configure ISA2 to accept VPN connections from partners. Enable Quarantine Control on ISA2. On each server, use access rules to allow access to only the permitted resources.

Answer: B Question: 7

You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory domain named contoso.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 is configured as a VPN server and allows only VPN connections that use PPTP. ISA1 is configured to use a RADIUS server named Server1 to provide authentication and authorization for VPN client connections. You want to configure ISA1 to also allow VPN connections that use L2TP. For testing purposes, you want VPN clients to be able to use preshared keys for authentication. You perform the following actions on ISA1: In the Routing and Remote Access console, you enable the Allow custom IPsec policy for L2TP connection option and enter a value for a preshared key. In the ISA Server Management console, you enable L2TP over IPsec settings in the VPN Clients Properties dialog box. You test L2TP functionality by configuring a VPN connection object on a computer named Workstation1, which runs Windows XP Professional with Service Pack 2. The VPN connection object is configured to use the same preshared key that you configured on ISA1. However, when you try to connect to ISA1 by using L2TP, you receive the following error message: Error 792: The L2TP connection failed because security negotiation timed out. You need to configure ISA1 to support L2TP connections that use preshared keys. What should you do?

- A. In the ISA Server Management console, enable the use of a custom IPsec policy and configure a preshared key in the Virtual Private Networks (VPN) Properties dialog box.
- B. In the ISA Server Management console, enable EAP in the Virtual Private Networks (VPN) Properties dialog box.
- C. In the RADIUS remote access policy profile for the VPN connection, add MD5-Challenge as an authentication method.
- D. In the RADIUS remote access policy profile for the VPN connection, add Protected Extensible Authentication Protocol (PEAP) as an authentication method.

Answer: A

Question: 8

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 functions as a remote access VPN server for the network. Remote access VPN clients can use either PPTP or L2TP over IPsec to connect to ISA1. Users report that after connecting to the corporate network, they cannot access file shares on the network file server without first being presented with an authentication prompt. You need to ensure that users are not asked for credentials when they access file shares. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Instruct the users to log on by using their domain credentials via dial-up networking.
- B. Configure ISA1 as a RADIUS client.
- C. Create an access rule to enable the LDAP and LDAP5 protocols from the Local Host network to the Internal network.
- D. Join ISA1 to the domain.

Answer: A, D

Question: 9

You are the network administrator for Company.com. Company has a main office and one branch office. The network contains two ISA Server 2004 computers named ISA1 and ISA2. ISA1 is located at the main office. ISA2 is located at the branch office. An IPsec tunnel mode site-to-site VPN connects the main office and branch office networks. ISA1 has three addresses bound to its external network adapter, and ISA2 uses a non-primary IP address to establish the IPsec tunnel mode connection to ISA1.

Users at the branch office report that they can connect to file shares at the main office, but they cannot connect to the Microsoft Outlook Web Access Web site. You need to ensure that users at the branch office can access the Outlook Web Access Web site. What should you do?

- A. Use a network address translation (NAT) relationship between the branch office network and the main office network.
- B. Add IP addresses to the external network adapter of ISA2.
- C. Change the Phase II IPsec configuration on both ISA1 and ISA2 to use Message Digest 5 (MD5) as its integrity algorithm.
- D. Create a new protocol definition for TCP port 80 outbound and use the definition in the access rule.

Answer: D

Question: 10

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1, which is configured as a remote access VPN server. You configure ISA1 to accept both PPTP and L2TP over IPsec VPN connections from remote access clients. Several users report that they cannot connect to the network. You review the log files on ISA1 and discover that the users with failed connection attempts are all using L2TP over IPsec. You need to ensure that the users can connect to the network. What should you do?

- A. Disable IP fragment blocking.
- B. Disable IP routing.
- C. Disable IP options filtering.
- D. Disable verification of incoming client certificates.

Answer: A

Question: 11

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. You enable VPN Quarantine Control on ISA1. You create a Connection Manager (CM) profile and install it on VPN client computers. The CM profile contains a script named quarantine.vbs that performs several tests on VPN client computers to ensure conformance with Company policy. If a computer passes the tests, the script executes the following command:

RQC %1 %2 %3 %4 SV1.

The variables in the command represent the parameters inherited from the CM profile. The parameters are shown in the following table.

Variable	Parameter
%1	%DialRasEntry%
%2	%TunnelRasEntry%
%3	%Domain%
%4	%UserName%

Users report that after they establish a VPN connection with ISA1, they receive a message stating that their computer has been placed in quarantine mode. The VPN connection is terminated, and they are prompted to reconnect. You verify that the client computer configurations conform to Company policies and pass the tests on the quarantine.vbs script.

The System log displays a large number of instances of the following warning message: "A remoteaccess client at IP address w.x.y.z connected by Company\username has been rejected because it presented the following unrecognized quarantine string: SV1" You need to ensure that VPN client computers can be moved out of the Quarantined VPN Clients network when the quarantine.vbs script executes successfully. What should you do?

- A. Create a new CM profile by using the Connection Manager Administration Kit (CMAK). Append the text string "SV1" to the list of parameters for the custom action.
- B. Edit the quarantine.vbs script so that it used the following command: RQC %DialRasEntry% %TunnelRasEntry% 7250 %Domain% %UserName%
- C. On ISA1, configure the AllowedSets values for the RQS service by including the text string "SV1".
- D. Use the Connection Manager Administration Kit (CMAK) to change the post-connect action to Rqc.exe.

Answer: C

Question: 12

You are the network administrator for Company.com. Company has a main office and one branch office. The main office has one ISA Server 2004 computer named ISA1, which runs Windows Server 2003. The branch office has one ISA Server 2004 computer named ISA2, which runs Windows 2000 Server. You create a site-to-site VPN connection between ISA1 and ISA2. You configure IPSec tunnel mode for the site-to-site connection. When you test the site-to-site VPN connection, the connection attempt fails. You need to enable the IPSec tunnel mode site-to-site VPN connection between the main office and the branch office. What should you do?

- A. Install the IPsecPol tool on ISA1.
- B. Install the IPsecPol tool on ISA2.
- C. Configure a custom IPSec policy on ISA1.

D. Configure a custom IPSec policy on ISA2.

Answer: B

Question: 13

You are the network administrator for Company.com. Company has a main office and is adding a branch office. You are connecting the main office and branch office networks. You install ISA Server 2004 on a computer at each office, and you create a site-to-site VPN connection between the ISA Server computers. You create remote site networks on the ISA Server computers at both offices. You choose the L2TP over IPSec VPN protocol. You want to use a preshared key for the IPSec authentication. You open the Routing and Remote Access console and enter the preshared key in the Properties dialog box for the Routing and Remote Access server. The site-to-site L2TP over IPsec connection is successful. You then restart the ISA Server computers and discover that the site-to-site connection fails. You need to ensure that the L2TP over IPSec site-to-site VPN connections continue to function properly after the ISA Server computers are restarted. What should you do?

- A. Re-enter the preshared keys on the ISA Server computers at both offices. Change the preshared keys so that they include mixed-case letters, numbers, and symbols.
- B. Remove all certificates for the ISA Server computers at both offices.
- C. On the ISA Server computers at both offices, remove the preshared key from the Routing and Remote Access console, and enter the key on the Authentication tab of the Virtual Private Networks (VPN) Properties dialog box.
- D. Install user certificates on the ISA Server computers in both offices and enable EAP user authentication for the demand-dial accounts.

Answer: C

Question: 14

You are the network administrator for Company.com. Company has a main office and is adding a branch office. The main office and the new branch each have an ISA Server 2004 computer. You want to connect the main office and the branch office networks by using a site-to-site VPN. You create a site-to-site VPN connection that connects the office networks by using the L2TP over IPSec VPN protocol. Computer certificates are installed on the ISA Server computer at each office. When you create the remote site network on each ISA Server computer, you configure it to use certificates and a preshared key. At each office, the preshared key is configured as the office name on the ISA Server computer at that office. From the ISA Server computer at the main office, you repeatedly run the ping command to a host on the branch office network. The site-to-site VPN fails. You open the Routing and Remote Access console and manually dial the demand-dial interface. You receive the following error message: "The last connection attempt failed because: The L2TP connection attempt failed because the security layer encountered a processing error during initial negotiations with the remote computer." You need to enable the site-to-site VPN connection by using the most secure IPSec authentication method possible. What should you do?

- A. Restart the ISA Server computer at both offices.
- B. Re-enter the preshared keys on the ISA Server computer at both offices. Change the preshared keys so that they include mixed-case letters, numbers, and symbols.
- C. Remove the preshared key from the remote site network configuration on the ISA Server computer at both offices.
- D. Delete the remote site network on the ISA Server computer at both offices, and re-create the remote site networks with the original parameters.

Answer: C

Question: 15

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 functions as a VPN remote access server. Remote access VPN clients use either PPTP or L2TP over IPSec to connect to ISA1. All remote access VPN client computers are configured as both Web Proxy and Firewall clients of ISA1.

You create an access rule to allow domain users on the VPN Clients network access to all protocols and Web sites on the Internet. A user named Bob logs on to his portable computer by using a local user account and establishes a VPN connection to ISA1 by using his domain credentials. You discover that Bob cannot connect to the Internal network when the VPN connection to ISA1 is active. You need to ensure that Bob can access the Internet network while maintaining a VPN connection to ISA1. What should you do?

- A. Disable the Firewall client before establishing the VPN connection.
- B. Disable the Web Proxy configuration before establishing the VPN connection.
- C. Create an access rule to allow connections from the VPN Clients network to the Internal network.
- D. Remote the authentication requirement on the access rule that allows VPN Clients access to the Internet.

Answer: C

Question: 16

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 provides Internet access for all users on Company's network. All computers on the network are configured as SecureNAT clients. You create an access rule on ISA1 that allows all users access to all protocols on the External network. You view the Firewall log and the Web Proxy filter log on ISA1 and notice that the URLs of Websites visited by Company users are not displayed. You need to ensure that the URLs of Web sites visited by Company users are displayed in the ISA1 log files. What should you do?

- A. Configure all network computers as Web Proxy clients.
- B. Configure all network computers as Firewall clients.
- C. Configure ISA1 to require authentication for Web requests.
- D. Configure ISA1 to require authentication for all protocols.

Answer: A

Question: 17

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 is configured to provide forward Web caching for users on the Internet network. During periods of peak usage, users report that it takes longer than usual for Web pages to appear. You suspect that insufficient memory is the source of the slow performance of ISA1. You need to verify whether insufficient memory is the source of the slow performance. Which two System Monitor performance counters should you add? (Each correct answer presents part of the solution. Choose two)

- A. Memory\Pages/sec
- B. Process(W3Prefch)\Pool Nonpaged Bytes
- C. ISA Server Cache\Memory Usage Ratio Percent (%)
- D. Physical Disk\Avg. Disk Queue Length
- E. ISA Server Cache\Disk Write Rate (writes/sec)
- F. Memory\Pool Nonpaged Bytes

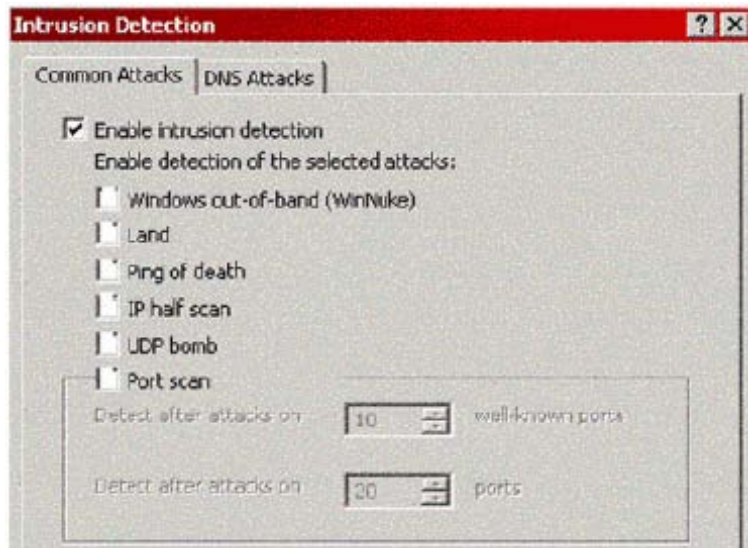
Answer: A, C

Question: 18 HOTSPOT

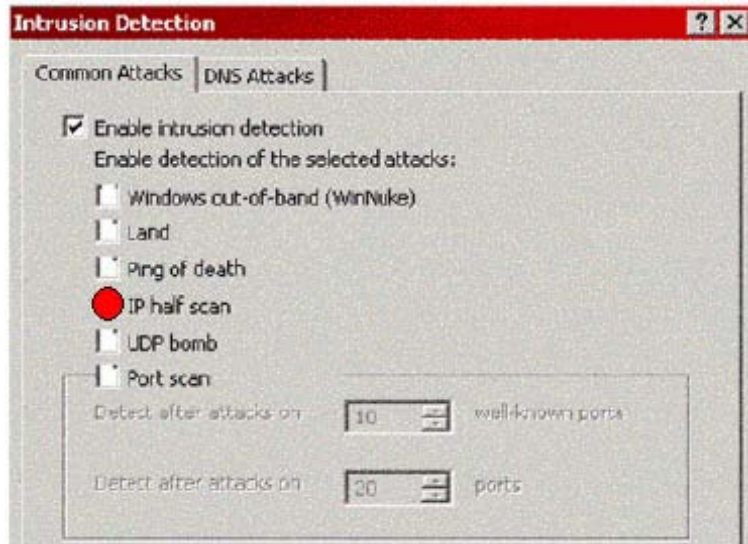
You are the network administrator for Company.com. The network contains an ISA Server 2004 computer names ISA1. You use Network Monitor to capture and analyze inbound traffic from the Internet to ISA1. You notice a high volume of TCP traffic that is sent in quick succession to random TCP ports on ISA1. The flag settings of the traffic are shown in the following example.

TCP: Flags = 0x00 : TCP: ..0..... = No urgent data TCP: ...0.... = Acknowledgment field not significant TCP:0... = No Push function TCP:0.. = No Reset TCP:0. = No Synchronize TCP:0 = No Fin

This traffic slows the performance of ISA1. You want to be able to create a custom alert that is triggered whenever ISA1 experience traffic that uses invalid flag settings to discover open ports. You do not want the alert to be triggered by traffic that uses valid flag settings in an attempt to discover open ports. You want to accomplish this goal by selecting only the minimum number of options in the Intrusion Detection dialog box. What should you do? To answer, configure the appropriate option or options in the dialog box in the answer area.



Answer: Question: 19



You are the administrator of an ISA Server 2004 computer named ISA1. ISA1 is configured to publish two Web sites named www.fabrikam.com and www.Company.com. Both Web sites are located on a Windows Server 2003 computer named Company1. The IP address of Company1 is 10.0.0.2.

The Web publishing rules are configured as shown in the following display.

Order	Name	Action	Protocols	From / Listener	To	Condition
1	Web Publish 1	Allow	HTTP	WebListener1	10.0.0.2	All Users
2	Web Publish 2	Allow	HTTP	WebListener1	10.0.0.2	All Users

Both the www.fabrikam.com/info and www.Company.com/info virtual point to a common share file. The default log view does not allow you to easily distinguish between requests for www.fabrikam.com/info and requests for www.Company.com/info. A sample of the log with the relevant entries is shown in the following table.

Destination IP	Rule	URL
10.0.0.2	Web Publish 1	10.0.0.2/info
10.0.0.2	Web Publish 2	10.0.0.2/info

You need to ensure that the log viewer displays the fully qualified domain names (FQDNs) for the Web site requests. In addition, you need to filter the log viewer to display only the requests for both the www.Company.com/info and the www.fabrikam.com/info virtual subdirectories. What should you do?

- On ISA1, configure two Hosts file entries that resolve both FQDNs to 10.0.0.2. Configure each Web publishing rule to use the FQDN of its respective Web site on the To tab. In the log viewer, add to the default log filter expression a condition where the URL contains the text string "info".
- On ISA1 configure two Hosts file entries that resolve both FQDNs to the external IP address of ISA1. Configure each Web publishing rule so that requests appear to come from the original client computer. In the log viewer, add a column to display the destination host name. In the log viewer, add to the default log filter expression a condition where the URL contains the text string "info".
- In the log viewer, add two conditions to the default log filter expression. Configure the first condition so that the Rule equals Web Publish 1. Configure the second condition so that the Rule equals Web publish 2. In the log viewer, add a column to display the destination host name.
- In the log viewer, add two conditions to the default log filter expression. Configure the first condition so that Server contains Fabrikam. Configure the second condition so that Server contains Company. In the log viewer, add a column to display the destination host name.

Answer: A

Question: 20

You are the network administrator for Contoso, Ltd. The network contains an ISA Server 2004 computer named ISA1 and a Windows Server 2003 computer named Server1. Both ISA1 and Server1 are members of an Active Directory domain named contoso.com. You configure ISA1 to generate daily reports and automatically publish them to a shared folder named DailyReports on Server1. You create an account named Contoso\IsaReports. You configure ISA1 to create reports in the security context of the Contoso\IsaReports account. The current permissions on the DailyReports folder are shown in the following table. Group or user name Allow permissions Server1\Administrators Full Control System Full Control Contoso\Managers Read List Folder Contents Read & Execute Contoso\IsaReports Full Control You need to configure the minimum NTFS permissions on the DailyReports folder. What should you do?

- Change the allowed permissions for the system object from Full Control to Modify.
- Change the allowed permissions for the Contoso\IsaReports object from Full Control to Read.

- C. Change the allowed permissions for the Contoso\IsaReports object from Full Control to Write.
- D. Change the allowed permissions for the system object from Full Control to Read and Write.

Answer: C

Question: 21

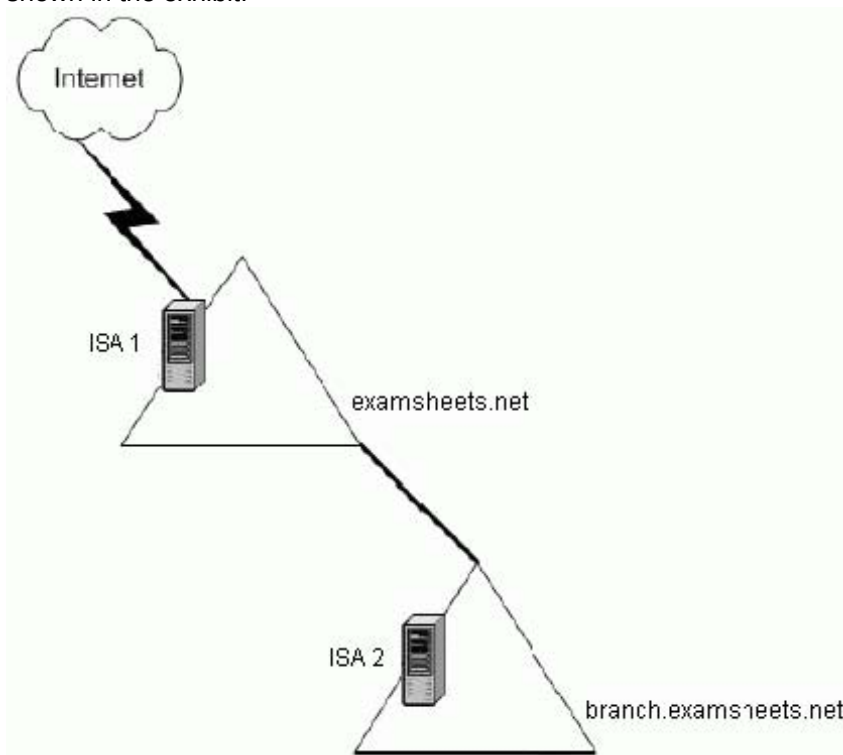
You are the network administrator for Company.com. The network consist of a single ActiveDirectory domain. All client computers run either Windows 2000 Professional or Windows XPProfessional. All client computers are members of the domain. Users in the network use an IP-based client/server application on a server named Company1 to record company data. To increase network security, you install ISA Server 2004 on a computer named ISA1. ISA1 connects to the Internet. You configure automatic discovery on the network. You configure client computers as SecureNAT clients. You verify that client computers can use the application on Company1. You then distribute the Firewall Client software to all client computers by using Group Policy. Users now report that they cannot use the application on Company1. You need to configure client computers on the network to allow the application on Company1 to function properly. Your solution must not affect other applications. What should you do?

- A. Configure a Wspcfg.ini file.
- B. Configure an Application.ini file.
- C. Configure the Management.ini file.
- D. Configure the Common.ini file.

Answer: B

Question: 22

You are the network administrator for Company.com. Company has a main office and one branchoffice. The network contains two ISA Server 2004 computers named ISA1 and ISA2. The relevant portion of the network is configured as shown in the exhibit.



ISA1 is located at the main office. ISA2 is located at the branch office and connects to the main office by using a dedicated WAN connection. You configure ISA2 to forward Web requests to ISA1. All client computers are configured to use an internal DNS server in each office. All client computers are configured as SecureNAT clients. While monitoring ISA2, you discover that Web requests from client computers in the branch office for servers located in the branch office are being resolved by ISA2. You need to configure the client computers in the branch office to directly access servers in the branch office. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

- A. Configure the client computers as Web Proxy clients of ISA2. Configure the list of domain names available on the Internal network on ISA1 to include the *.Company.com domain.
- B. Configure the client computers as Web Proxy clients of ISA2. Configure the Web browser to include the *.branch.Company.com domain.
- C. Configure the client computers as Firewall clients. Configure the list of domain names available on the Internal network on ISA2 to include the *.branch.Company.com domain.
- D. Configure the client computers as Firewall clients. Configure the list of domain names available on the Internal network on ISA1 to include the *.branch.Company.com domain.

Answer: B, C

Question: 23

You are the network administrator for Company.com. The network contains a single ISA Server 2004 computer, which is named IS1. ISA1 provides access to the Internet for computers on the Internal network, which consists of a single subnet. Company's written security policy states that the ISA Server logs must record the user name for all outbound Internet access. All client computers are configured with the Firewall client and the Web Proxy client and are not configured with a default gateway.

Users in the marketing department require access to an external POP3 and SMTP mail server so that they can use an alternate e-mail address when they sign up for subscriptions on competitors Web sites. You create and apply an ISA Server access rule as shown in the following display.

Order	Name	Action	Protocols	From / Listener	To	Condition
1	POP3 and SMTP for Marketing	Allow	POP3 SMTP	Internal	External	Marketing

The marketing department users configure Microsoft Outlook to connect to the external mail server. They report that they receive error messages when they attempt to read or send e-mail from the external mail server. You examine the ISA1 logs and discover that ISA1 denies POP3 and SMTP connections from the client computers. You need to ensure that the marketing department users can connect to the external mail server. What should you do?

- A. Configure the marketing computers with the IP address of a DNS server that can resolve external names to IP addresses.
- B. Configure the marketing computers with a default gateway address that corresponds to the IP address of ISA1 on the Internal network.
- C. On ISA1, enable Outlook in the Firewall client settings.
- D. On ISA1, create a computer set that contains the marketing computers.

Answer: C

Question: 24

You are the network administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The network contains an ISA Server 2000 computer named ISA1. All client computers have the ISA Server 2000 Firewall Client software installed. Client computers are configured to use an internal DNS server. Two Windows Server 2003 computers named App1 and App2 run a Web-based application that is used to process Company

data. You configure ISA1 with protocol rules to allow HTTP, HTTPS, RDP, POP3, and SMTP access. The list of domain names available on the Internal network on ISA1 contains the following entries:

- 1 *.south.Company.com
- 2 *.north.Company.com
- 3 *.east.Company.com
- 4 *.west.Company.com

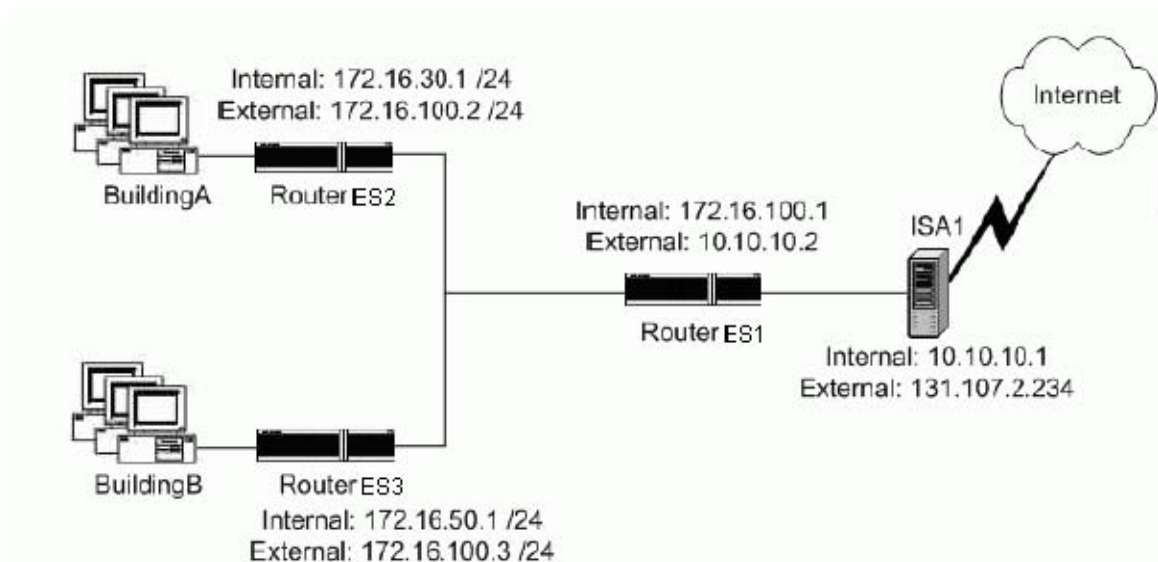
You perform an in-place upgrade of ISA1 by using the ISA Server 2004 Migration Tool. When you use Network Monitor on ISA1, you discover that client requests for App1 and App2 are being passed through ISA1. You need to provide a solution that will allow clients to directly access Company data on App1 and App2. What should you do?

- A. Create and configure HTTP, HTTPS, RDP, POP3, and SMTP access rules on ISA1.
- B. Configure an Application.ini file on the client computers.
- C. Redeploy the ISA Server 2004 Firewall Client software by distributing it to the client computers by using Group Policy.
- D. Add app1.Company.com and app2.Company.com to the list of domain names available on the Internal network on ISA1.

Answer: D

Question: 25

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. The relevant portion of the network is shown in the exhibit.



You configure ISA1 by using the Edge Firewall network template. You create access rules to allow Internet access for users on the network. Users on the network report that they cannot access the Internet. You need to configure the client computers on the network to allow Internet access. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Configure client computers in Building A with a default gateway IP address of 172.16.100.1.
- B. Configure client computers in Building B with a default gateway IP address of 172.16.50.1.
- C. Configure client computers in Building A with a default gateway IP address of 10.10.10.1.
- D. Configure client computers in Building B with a default gateway IP address of 172.16.100.1.
- E. Configure client computers in Building A with a default gateway IP address of 172.16.30.1.

F. Configure client computers in BuildingB with a default gateway IP address of 10.10.10.1

Answer: B, E

Question: 26

You are the network administrator for Company.com. The network contains a single ISA Server 2004 computer named ISA1. All Internet access for the local network occurs through ISA1. The network contains a Web server named Company1. Company1 is configured as a SecureNAT client. A Web application runs on Company1 that communicates with an external Web site named www.Company.com. You configure ISA1 with two access rules for outbound HTTP access. The rules are named HTTP Access 1 and HTTP Access 2. HTTP Access 1 is configured to use the All Authenticated Users user set as a condition. HTTP Access 2 is configured to use the All Users user set as a condition, and it restricts outbound HTTP traffic to the IP address of Company1. You verify that users can access external Web sites. However, you discover that the Web application cannot access www.Company.com. You need to allow the Web application to use anonymous credentials when it communicates with www.Company.com. You also need to require authentication on ISA1 for all users when they access all external Web sites. What should you do?

- A. On Company1, configure Web Proxy clients to bypass the proxy server for the IP address of the server that hosts www.Company.com
- B. On ISA1, add the fully qualified domain name (FQDN) www.Company.com to the list of domain names available on the Internal network.
- C. On ISA1, disable the Web Proxy filter for the HTTP protocol.
- D. Modify the order of the access rules so that HTTP Access 2 is processed before HTTP Access 1.

Answer: D

Question: 27

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 is connected to the Internet. All client computers run Windows XP Professional. All client computers are configured as SecureNAT clients and require access to the Internet. Client computers in the marketing department are located in an organizational unit (OU) named Marketing_Computers. An external partner company hosts a custom marketing application named Webapp. Webapp uses SSL and TCP port 3333. You create a security group named Marketing for the marketing department. You add the users in the marketing department to the Marketing group. You create an access rule to allow TCP port 3333 for only the users in the marketing department. Members of the Marketing group report that they cannot connect to Webapp. You need to ensure that only users in the marketing department can connect to Webapp. What should you do?

- A. Enable the Firewall Client installation configuration group on ISA1. Add the marketing client computers to the list of trusted computers.
- B. Use Group Policy to assign the MS_FWC.msi file to the client computers in the Marketing group.
- C. Enable Web Proxy client support on the Local Host network. Enable SSL listening on port 8443.
- D. Configure the Internal network on ISA1 to require authentication for all users. Enable SSL certificate authentication on the Internal network.

Answer: B

Question: 28

You are a network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. Remote users establish VPN connections to ISA1 to access resources on the Internal network. Remote users are required to use a smart card when they establish VPN connections. Another administrator reports that remote users can

still establish VPN connections to ISA1 after their smart card certificate has been revoked and a new certification revocation list (CRL) has been published. You need to ensure that users whose smart card certificates are revoked cannot establish VPN connections to ISA1. What should you do?

- A. Select the Use RADIUS for authentication check box.
- B. Select the Extensible authentication protocol (EAP) with smart card or another certificate check box.
- C. Select the Verify that incoming client certificates are not revoked check box.
- D. Select the Verify that incoming server certificates are not revoked in a reverse scenario check box.

Answer: C

Question: 29

You are the network administrator for Company.com. You install ISA Server 2004 on a computer that has three network adapters. One of the network adapters is connected to the Internet, one is connected to the Internal network, and one is connected to a perimeter network. The perimeter network adapter and the internal network adapter are connected to private address networks. You configure ISA Server by applying the 3-Leg Perimeter network template. You run the 3-Leg Perimeter Network Template wizard. You then make the following changes to the firewall policy:

- 1 Create an access rule to allow all traffic between the Internal network and the Internet.
- 2 Create an access rule to allow all traffic between the Internal network and the perimeter network.
- 3 Create an access rule to allow SMTP traffic from an SMTP server on the perimeter network to a Microsoft Exchange Server computer on the Internal network.
- 4 Create a server publishing rule to allow SMTP traffic from the External network to the SMTP server on the perimeter network.

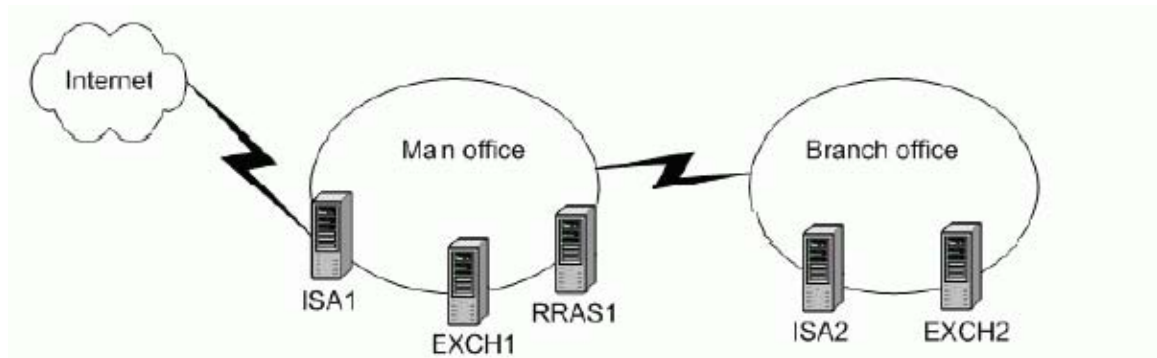
Users report that they cannot receive e-mail messages from users outside of the Internal network. You need to allow users to receive e-mail messages from other users on the Internet. You do not want to create a server publishing rule. What should you do?

- A. Change the network rule that controls the route relationship between the perimeter network and the Internal network to Route.
- B. Change all network rules that control the route relationship between the Internal network, perimeter network, and External network to Route.
- C. Change the network rule that controls the route relationship between the perimeter network and the External network to Nat.
- D. Change all network rules that control the route relationship between the Internal network, perimeter network, and External network to Nat.

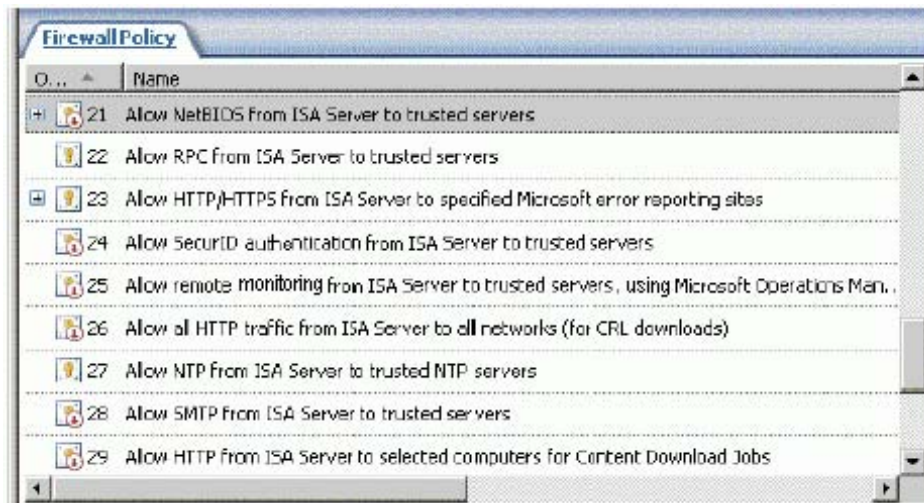
Answer: A

Question: 30

You are the network administrator for Company.com. The relevant portion of the network is configured as shown in the Network exhibit.



Company has a main office and one branch office. An ISA Server 2004 computer named ISA2 connects to a Routing and Remote Access server named RRAS1. You create a mailbox for the securityadmin user account on a Microsoft Exchange Server computer named EXCH2. You view the firewall policy on ISA2 as shown in the Firewall Policy exhibit.



You configure the dial-on-demand failure alert on ISA2 to send an e-mail alert to the securityadmin@Company.com SMTP alias. EXCH2 is listed as the mail server on the dial-on-demand failure alert. You confirm that the alert is issued, but the e-mail for the alert is not received. You need to configure ISA2 to ensure that the e-mail alert is received. What should you do?

- A. Enable the RPC from ISA Server to trusted servers system policy rule.
- B. Enable the Allow SMTP from ISA Server to trusted servers system policy rule.
- C. On ISA2, configure an access rule to allow POP3 from the Local Host network to EXCH2.
- D. On ISA2, configure a server publishing rule to EXCH2 for Exchange RPC.

Answer: B

Question: 31

You are the administrator of an ISA Server 2004 computer named ISA1. ISA1 has two network adapters. Access rules allow users on the Internal network to have HTTP access to the Internet. You add a third network adapter to ISA1 and connect the third network adapter to a perimeter network. You place a Web server named WebServerES2 on this perimeter network segment. WebServerES2 must be accessible to computers on the Internal network. You create a computer object for WebServerES2 and then create an access rule that allows Internal network clients HTTP access to WebServerES2. Users are not required to authenticate with ISA1 to access

WebServerES2. Users report that they cannot access information on WebServerES2. When they attempt to access the Web site, they receive the following error message: "Error Code 10060: Connectiontimeout. Background: There was a time out before the page could be retrieved. This might indicate that the network is congested or that the website is experiencing technical difficulties." You need to ensure that users on the Internal network can access information on WebServerES2. First, you verify that WebServerES2 is operation. What should you do next?

- A. Create a network rule that sets a route relationship between the Internal network and the perimeter network.
- B. Create a server publishing rule that publishes WebServerES2 to the Internal network.
- C. Create a Web publishing rule that publishes WebServerES2 to the Internal network.
- D. Create an access rule that allows WebServerES2 access to the Internal network.

Answer: A

Question: 32

You are the network administrator for Company.com. Company has a main office and three branch offices. The network contains an ISA Server 2004 computer named ISA1, which is located at the main office. You plan to deploy new ISA Server 2004 computers for the branch offices. You name one of the new computers ISA2. You perform the following tasks:

- 1 Export the ISA Server 2004 configuration on ISA1 to a file named ISASETUPCONFIG.XML.
- 2 Edit the ISASETUPCONFIG.XML file to include a valid external IP address.
- 3 Create a file named C:\Msisaund.ini on ISA2.

You install ISA Server 2004 on ISA2 by using an unattended installation. When the installation is finished, you discover that the ISA Server 2004 configuration settings from ISA1 are not copied to ISA2. You need to deploy the ISA Server 2004 computers in the branch offices with the configuration settings from ISA1. You want to accomplish this goal by using the minimum amount of administrative effort. What should you do?

- A. Export the system policy rules on ISA1 to another file named ISA1SystemPolicy.xml. Add the following lines to the C:\Msisaund.ini file on ISA2: `IMPORTISACONFIG=1` `IMPORT_CONFIG=ISASETUPCONFIG.XML` `IMPORT_CONFIG=ISA1SystemPolicy.xml` Run an unattended setup by using this Msisaund.ini file on each new ISA Server 2004 computer.
- B. Back up the array configuration on ISA1. Save the file as C:\Msisaunattended.xml. Run the following command from the ISA Server 2004 installation media: `setup.exe /unattended:ISASETUPCONFIG.XML C:\Msisaund.ini`
- C. Create an individual ISASETUPCONFIG.XML file for each branch office ISA Server 2004 computer. Edit each ISASETUPCONFIG.XML file to include the internal network addresses for the respective branch office. Edit the Msisaund.ini file from ISA2 by adding the following line. `IMPORT_CONFIG_FILE=ISASETUPCONFIG.XML` Run an unattended setup by using the Msisaund.ini file from ISA2 on each new ISA Server 2004 computer.
- D. Create a file named Msisaunattend.txt. Include the following lines: `UNATTENDED=1` `EXPORT_ISACONFIG=0` `FILEPATH=ISASETUPCONFIG.XML` Run an unattended setup by using this Msisaunattend.txt file on each new ISA Server 2004 computer.

Answer: C

Question: 33

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. You deploy an internal certification authority (CA). You deploy client certificates to users. You configure client certificate mapping for internal network users. All client computers are configured as Web Proxy clients. You configure the Internal network to allow only certificate-based authentication for Web Proxy clients. You revoke a user's certificate. After one week, you discover that ISA1 is still authenticating Web requests for that user. You need to configure ISA1 to deny Internet access to the user. What should you do on ISA1?

- A. Add the All Networks (and Local Host) network set as a destination for the Allow access to directory services for authentication purposes system policy rule.
- B. Create a new content type set. Select the application/pkix-crl and application/x-x509-ca-cert MIME types as the content type to allow.
- C. Enable the Verify that incoming server certificates are not revoked in reverse scenario certificate validation setting on ISA1, and enable the related system policy rule.
- D. Enable the Verify that incoming client certificates are not revoked certificate validation setting on ISA1, and enable the related system policy rule.

Answer: D

Question: 34

You are a network administrator for Company.com. The network contains an ISA Server 2004 array that is configured to use Network Load Balancing. The array contains two members. The array is used to publish internal Web servers. Users access internal Web servers by using the URL <http://www.Company.com>. The URL resolves to a single virtual IP address. You implement a new Web site named Company1. To access Company1, users must authenticate by using credentials that are stored on a third-party RADIUS server. You publish Company1 on the array. You need to ensure that users can access Company1 by using the third-party RADIUS server. You must ensure that requests are load balanced by all array members. What should you do?

- A. On each array member, add a second IP address. Create a new listener that uses the new address. Configure the listener to use RADIUS authentication.
- B. Configure one array member to listen for requests to www.Company.com on one listener. Configure the other array member to listen for requests to Company1 on a new listener. Configure each listener to use the appropriate authentication method.
- C. Use the Network Load Balancing console to configure each array member to use an affinity setting for None. Configure the listener to use RADIUS authentication.
- D. Add a second unique network address to the external interface of each array member. Configure www.Company.com to resolve to the new addresses by using DNS round robin. Configure the listener to use RADIUS authentication.

Answer: A

Question: 35

You are the network administrator for Company.com. The network contains an ISA Server 2000 computer named ISA1. ISA1 connects to the Internet. ISA1 is configured with access rules to allow Internet access for all users. All client computers are configured as Web Proxy clients of ISA1. You are deploying a new ISA Server 2004 computer named ISA2 for use by the research department. You run the ISA Server 2004 Migration Tool on ISA1. You save the resulting configuration to a file named Backupconfig.xml. You install ISA Server 2004 on ISA2, and you import Backupconfig.xml on ISA2. On ISA2, you configure the Internal network with a valid IP address range for the research department client computers. You configure a Web chaining rule on ISA2 to redirect Web requests to ISA1. You configure client computers in the research department as Web Proxy clients of ISA2. Users of the research department client computers report that they cannot connect to the Internet. You need to ensure that users of client computers in the research department can connect to the Internet. What should you do?

- A. Change the external IP address on ISA2 to a valid IP address for the external network.
- B. On ISA2, save its configuration as ISAbackup.xml. Restart the Microsoft Firewall service on ISA2. Then import the configuration.
- C. Configure the research department client computers as Firewall clients of ISA2. Enable automatic discovery on ISA2.
- D. Perform an ISA Server 2004 in-place upgrade on ISA1. On ISA2, configure access rules to allow Internet access for the research department users.

Answer: A

Question: 36

You are a network administrator for Company.com. Company has a main office and one branch office. The main office has a high-speed Internet connection. The branch office has a dial-up Internet connection. An administrator in the main office configures one ISA Server 2004 computer to provide Internet access to users in the main office. The administrator configures access rules and enables VPN access to the ISA Server computer. The access rules allow only authorized users access to the Internet. You install an ISA Server 2004 computer in the branch office. You need to configure the branch office ISA Server computer to meet the following requirements:

- 1 Ensure that users in the branch office can access the Internet.
- 2 Ensure that users in the branch office are restricted by the main office access rules when accessing the Internet.
- 3 Ensure that all information sent over the Internet is encrypted between the offices.

What should you do?

- A. Create a dial-up connection to the main office. Configure ISA Server to use the dial-up connection as the default gateway. Configure a dial-up user account.
- B. Create a dial-up connection to an ISP. Configure ISA Server to use the dial-up connection as the default gateway. Configure Web Proxy chaining.
- C. Create a demand-dial VPN connection to the main office. Configure ISA Server to use the VPN connection as the default gateway. Configure firewall chaining. Configure a firewall chaining user account.
- D. Create a demand-dial VPN connection to an ISP. Configure firewall chaining. Configure a firewall chaining user account.

Answer: C

Question: 37

You are the network administrator for Company.com. The network contains two ISA Server 2004 computers named ISA1 and ISA2. Company has a main office and one branch office. ISA1 is located in the main office and connects to the Internet. ISA2 is located in the branch office and connects to the main office over a dedicated WAN link. All client computers run Windows XP Professional. All client computers can update virus definitions from the virus update Web site. ISA2 can connect to the virus update Web site and the Windows Update Web site. You discover that ISA1 cannot connect to the virus update Web site or the Windows Update Website. The firewall policy on ISA1 is configured as shown in the exhibit.

Q...	Name	Action	Protocols
L6	Allow remote SQL logging from ISA Server to selected servers	Allow	Microsoft S...
L7	Allow HTTP/HTTPS requests from ISA Server to specified sites	Allow	HTTP, HTTPS
L8	Allow HTTP/HTTPS requests from ISA Server to selected servers for connectivity verifiers	Allow	HTTP, HTTPS
L9	Allow access from trusted computers to the Firewall Client installation share on ISA Server	Allow	Microsoft ...
L20	Allow remote performance monitoring of ISA Server from trusted servers	Allow	NetBios Da...
L21	Allow NetBIOS from ISA Server to trusted servers	Allow	NetBios Da...
L22	Allow RPC from ISA Server to trusted servers	Allow	RPC (all int...

You need to ensure that ISA1 can connect to the virus update Web site and the Windows Update Web site. What should you do?

- A. Enable the HTTP connectivity verifiers configuration group. On ISA1, create a network set that has the IP addresses of both the virus update Web site and the Windows Update Web site.

- B. Enable the Allowed sites configuration group. On ISA1, add the URL of the virus update Web site to the System Policy Allowed Sites domain name set.
- C. Create a new URL set named VirusUpdates that includes the URLs for the virus update Web site and the Windows Update Web site. On ISA2, create a new HTTP access rule that includes the VirusUpdates URL set.
- D. Create a new domain name set named VirusUpdates that includes the URLs for the virus update Web site and the Windows Update Web site. On ISA1, create a new HTTP access rule from the Internal network to the VirusUpdates domain name set.

Answer: B

Question: 38

You are the network administrator for Company.com. The network contains an ISA Server 2004 array. The array contains six members. You enable Cache Array Routing Protocol (CARP) so that outbound Web requests are resolved within the array. Soon after you enable CARP on the array, Web users on the corporate network report that Internet access is slower than normal. You use Network Monitor to check network traffic patterns on each of the ISA Server 2004 array members. You discover that there is very high network utilization on the intra-array network. You need to reduce the amount of intra-array traffic. What should you do?

- A. Enable Network Load Balancing on the intra-array network.
- B. Configure the client computers as SecureNAT clients.
- C. Use automatic discovery to configure the client computers as Web Proxy clients.
- D. Enable CARP on the intra-array network.

Answer: C

Question: 39

You are the network administrator for Company.com. The network contains two ISA Server 2004 computers named ISA1 and ISA2. The network also contains a Routing and Remote Access server named RRAS1. Company has a main office and one branch office. ISA2 uses a dial-up connection to connect to RRAS1. On ISA2, you create a Web chaining rule that redirects requests to ISA1. Users in the branch office frequently access a published Web site named <http://sales.Company.com>. This sales Web site resides on a Web server in the perimeter network. Users in the branch office report that occasionally during business hours they cannot connect to <http://sales.Company.com>. You configure and enable a content download job to ensure that Web site content is loaded into the Web cache on ISA2. You need to ensure that content from <http://sales.Company.com> will always be available to users in the branch office, even if the connection is unavailable. What should you do on ISA2?

- A. Create a new Web chaining rule. On the rule, enable a backup route to ISA1. Add a URL set for <http://sales.Company.com> to the Web chaining rule. On the default cache rule, increase the Time to Live (TTL) for HTTP objects.
- B. Create a new Web caching rule. On the rule, redirect SSL requests as SSL requests. Add a URL set for <http://sales.Company.com> to the Web chaining rule. On the default cache rule, decrease the Time to Live (TTL) for HTTP objects.
- C. Create a cache rule. Enable If any version of the object exists in cache. If none exists, route the request. Enable Content for offline browsing. On the cache rule, decrease the Time to Live (TTL) for HTTP objects.
- D. Create a cache rule. Enable Only if a valid version of the object exist in cache. If no valid version exists, route the request. Enable Content for offline browsing. On the cache rule, increase the Time to Live (TTL) for HTTP objects.

Answer: C

Question: 40

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. You enable a cache drive on ISA1. ISA1 is a multi-homed server. A Web server named Company2 resides in a perimeter

network. Company2 contains twocompany Web sites named <http://internal.Company.com> and <http://external.Company.com>. Members of the graphics team make frequent changes to the Web site named <http://internal.Company.com>. When the team members update the Web site, they cannot see changes from other members of the team. You need to configure ISA1 to allow members of the graphics team to immediately view updates to <http://internal.Company.com>. What should you do?

- A. Add the Company.com domain name to the list of domains on the Internet network. Disable the Bypass proxy for Web servers in this network option.
- B. Add the client computers used by the members of the graphics team to a computer set. Create a cache rule to include the computer set. Enable the Never. No content will ever be cached setting.
- C. Create URL set for <http://internal.Company.com>. Create a cache rule to include the URL set. Enable the Never. No content will ever be cached setting.
- D. Create a new computer set for Company2. Create a cache rule to include the computer set. Disable HTTP caching on the cache rule

Answer: C

Question: 41

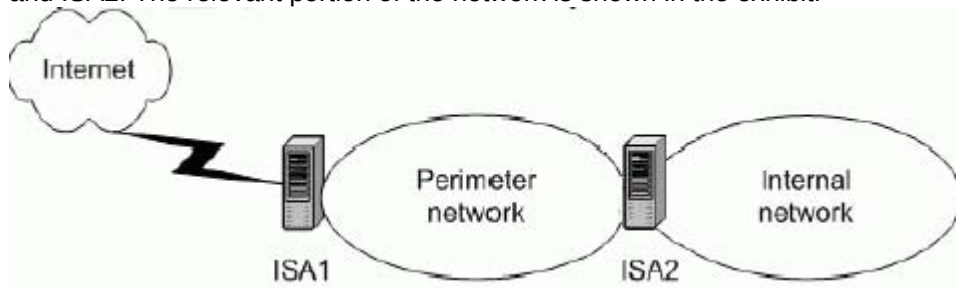
You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. Company uses Microsoft Exchange Server 2003 as its e-mail server. Company's written security policy states that all user names and passwords must be encrypted when they are sent over the Internet. Company is adopting Web-enabled cellular phones and wants to allow users to use these phones to access their e-mail over the Internet. The phones have a Wireless Access Protocol (WAP) browser and an e-mail client that is capable of only POP3 and IMAP4. You need to configure ISA1 to give users access from their cellular phones to e-mail. You need to ensure that you adhere to Company's security policy. What should you do?

- A. Create an HTTPS server publishing rule. Configure the rule to point to the Microsoft Outlook Web Access site.
- B. Create an HTTP server publishing rule. Configure the rule to point to the Microsoft Outlook Mobile Access site.
- C. Create a POP3 server publishing rule. Configure the rule to point to an Exchange Server 2003 computer.
- D. Create an IMAP server publishing rule. Configure the rule to point to an Exchange Server 2003 computer.

Answer: B

Question: 42

You are the network administrator for Company.com. The network contains two ISA Server 2004 computers named ISA1 and ISA2. The relevant portion of the network is shown in the exhibit.



Company's written security policy states that employees must connect to the VPN server installed on ISA2 by using the most secure method possible. You need to configure ISA1 to allow employees to connect to the VPN server on ISA2. What should you do?

- A. On ISA1, create a PPTP server publishing rule. On ISA2, configure VPN connections to use EAP authentication.

- B. On ISA1, create an L2TP server publishing rule. On ISA2, configure VPN connections to use EAP authentication.
- C. On ISA1, create a PPTP server publishing rule. On ISA2, configure VPN connections to use PAP authentication.
- D. On ISA1, create an L2TP server publishing rule. On ISA2, configure VPN connections to use PAP authentication.

Answer: B

Question: 43

You are the network administrator for Company.com. ISA Server 2004 is installed as Company's firewall. All of Company's portable computers run Microsoft Outlook 2003. Company's written security policy states that all e-mail communications to the Microsoft Exchange Server 2003 computer over the Internet must be encrypted. You need to ensure that all employees use Outlook 2003, whether they use e-mail in the office or use e-mail remotely over the Internet. What should you do?

- A. Configure Microsoft Outlook Web Access on internal server. Configure an HTTP Web publishing rule to direct traffic to the Exchange Server computer.
- B. Configure Microsoft Outlook Web Access on an internal server. Configure an HTTP Web publishing rule to direct traffic to the Exchange Server computer.
- C. Configure an RPC Proxy server. Create a server publishing rule to direct all Exchange RPC traffic to the RPC Proxy server.
- D. Configure an RPC Proxy server. Create an HTTPS Web publishing rule to direct traffic to the RPC Proxy server.

Answer: D

Question: 44

You are the administrator of an ISA Server 2004 computer named ISA1. ISA1 is connected to the Internet. All client computers are configured as SecureNAT clients. Company's new written security policy states that only Web-based traffic will be allowed on the network. In the past, all instant messaging applications were allowed. You need to configure ISA1 to block all instant messaging traffic and all other non-Web traffic. What should you do?

- A. Delete all current access rules. Create a new access rule that has only HTTP and HTTPS as the allowed protocols. Configure HTTP filtering and add signatures for instant messaging applications.
- B. Create a new access rule that denies all instant messaging protocols. Create a new access rule that has only HTTP and HTTPS as the allowed protocols.
- C. Create a new access rule that has only HTTP and HTTPS as the allowed protocols. Configure HTTP filtering and add signatures for instant messaging applications. Unbind the HTTP filter from the HTTP protocol definition.
- D. Create a computer set definition for instant messaging servers on the Internet. Create a new access rule that denies all instant messaging protocols to the computer set you defined. Create a new access rule that has only HTTP and HTTPS as the allowed protocols.

Answer: A

Question: 45

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1, which was recently installed. Company's written security policy states that all HTTP traffic must go through ISA1. The human resources (HR) department creates a new HR Web site, which employees use to access and manage their benefits. The HR Web site has its own Windows Server 2003 Webserver and its own server publishing rule on ISA1. Security requirements dictate that employees must not be able to access the HR Web site from an untrusted client computer. You need to configure the server publishing rule to meet the security requirements. Which network object should you enable?

- A. External
- B. Local Host
- C. Quarantined VPN Clients
- D. All Protected Networks

Answer: D

Question: 46

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer. Users on the Internet network require access to a partner VPN server. The partner VPN server does not support machine certificate authentication for VPN connections. You enable a route relationship between the Internal network and the External network. You need to ensure that Company users can access the partner VPN server. What should you do?

- A. Create an access rule to enable outbound access to the PPTP Client protocol.
- B. Create an access rule to enable outbound access to the IPSec with Encapsulation Security Payload (ESP) Server protocol.
- C. Create an access rule to enable outbound access to the IKE Client protocol.
- D. Create an access rule to enable outbound access to the L2TP Client protocol.

Answer: A

Question: 47

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer. A network rule defines a network address translation (NAT) relationship between the Internal network and the External network. The Internal network contains a Windows Server 2003 computer named Company1. You need perform remote administration of Company1 by using Remote Desktop. You also need to allow users to establish a Remote Desktop connection to Company1 by using the non-standard TCP port 12345. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Configure a new protocol definition for TCP port 12345 inbound named RDP-x.
- B. Configure a new protocol definition for TCP port 12345 outbound named RDP-x.
- C. Create an access rule that uses RDP-x.
- D. Create a server publishing rule that uses RDP-x.

Answer: A, D

Question: 48

You are the network administrator for Company.com. The network contains a single ISA Server 2004 computer. Company is creating a new Web site for access by a business partner. The Web site will be hosted on an internal Web server. The Web site will be accessed by customers. Requests from client computers should first be validated by using SSL authentication. However, if client certificate requests fail, customers should still be prompted to log in by using a user name and password. You need to configure a publishing rule to allow access to the new Web site and to fulfil the authentication requirements. What should you do?

- A. Create an HTTP server publishing rule. Configure the rule to accept connections from client computers at the partner location.
- B. Create an HTTPS server publishing rule. Configure the rule to accept connections from client computers at the partner location.
- C. Create a Web publishing rule. Configure a new Web listener for the HTTP protocol. Configure the Web listener to allow both Integrated Windows authentication and Digest authentication.
- D. Create a Web publishing rule. Configure a new Web listener for the HTTPS protocol. Configure the Web listener to

allow both SSL certificate authentication and Basic authentication.

Answer: D

Question: 49

You are the network administrator for Company.com. The network contains two ISA Server 2004 Enterprise Edition computers named ISA1 and ISA2. ISA1 and ISA2 are configured as members of an ISA Server 2004 array. You configure the array to cache outgoing Web requests. You configure the array so that the cached Web content is distributed between ISA1 and ISA2. You want to minimize the traffic on the intra-array network. What should you do?

- A. Enable Cache Array Routing Protocol (CARP) on the Local Host network.
- B. Enable the client computers to download the automatic configuration script.
- C. Configure a content download job on the array.
- D. Configure Network Load Balancing on the Internal network.

Answer: B Question: 50

You are the network administrator for Company.com. The network contains a single ISA Server 2004 computer named ISA1. Company's written security policy states that ISA1 must authenticate users before users on the Internet are allowed to access corporate Web servers. You install a new Web server on the Internal network. Partners and customers will access the Web pages hosted by this Web server only from the Internet. You need to configure ISA1 to publish the Web site hosted by this Web server, and you need to adhere to Company's security policy. What should you do?

- A. Create a Web publishing rule. Configure the rule to require user authentication.
- B. Create a Web publishing rule. Configure the rule to perform link translation.
- C. Create an HTTP server publishing rule. Configure the rule to specify that requests appear to come from ISA1.
- D. Create an HTTP access rule. Configure the rule to allow connections from the External network to the Internal network

Answer: A

Question: 51

You are the network administrator for your company. The network contains two ISA Server 2004 computers named ISA1 and ISA2. The company has a main office and one branch office. The main office connects to the branch office over a dedicated 56-Kbps frame relay WAN link. A client computer named Client2 in the branch office connects to the main office through ISA2.

Name	Internal IP address	Default gateway
Client1	10.10.10.123/24	10.10.10.1
Client2	172.16.100.114/24	172.16.100.1
ISA1	192.168.100.1/24	
ISA2	172.16.1.1/24	

Two computers in each office are configured as shown in the following table. Name Internal IP address Default gateway
Client1 10.10.10.123/24 10.10.10.1
Client2 172.16.100.114/24 172.16.100.1
ISA1 192.168.100.1/24
ISA2 172.16.1.1/24
Users of Client1 and Client2 report that they cannot connect to the Internet. Client2 can connect to the main office network. You want to maintain a high level of security on the external network adapter on ISA1 and on ISA2. You need to verify connectivity to ISA1 from either Client1 or Client2. What should you do?

- A. Configure Client1 with the default gateway IP address of the internal network adapter of ISA1. Issue the ping command to 192.168.100.1 from Client1.
- B. Configure Client2 with the default gateway IP address of the internal network adapter of ISA2. Issue the tracert

command to 172.16.1.1 from Client2.

- C. Edit the Diagnostic Services ICMP configuration group on ISA1 by adding the main office network as a destination network. Issue the pathping command to 192.168.100.1 from Client1.
- D. Edit the Remote Management ICMP (PING) configuration group on ISA1 by adding Client1 to the Remote Management Computers computer set. Issue the ping command to 192.168.100.1 from Client1.

Answer: C

Question: 52

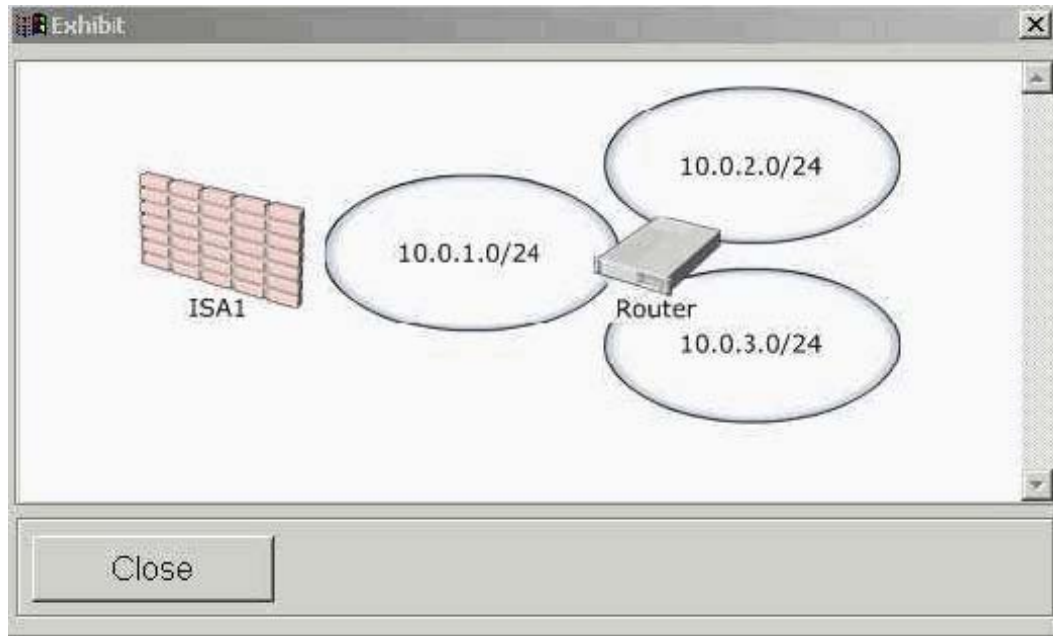
You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 connects to the Internet. ISA1 is configured with access rules for Internet access. A Windows Server 2003 computer named CERT1 is configured as an internal certification authority (CA). ISA1 can download the certificate revocation list (CRL) from CERT1. You are deploying 10 new ISA Server 2004 computers on the network. On ISA1 you export the firewall policy settings into a file named ISA1export.xml. You configure the network configuration settings on each new ISA Server computer. You import the firewall policy settings from the ISA1export.xml file on each new ISA Server computer. You test the imported configuration on each of the new ISA Server computers. You discover that each new ISA Server computer cannot download the CRL from CERT1. You need to ensure that the new ISA Server computers can download the CRL. What should you do?

- A. Edit the ISA1export.xml file by adding the following lines: StorageType=Allow HTTP from ISA Server to all networks (for CRL downloads) String=0 Enabled=1 Import the ISA1export.xml file on each new ISA Server computer.
- B. Export the system policy rules on ISA1 by using the Export System Policy task. Import the system policy rules on each new ISA Server computer.
- C. Export the array configuration settings on ISA1 to an .xml file. Import the .xml file on the new ISA Server computers.
- D. Create a destination set for the new ISA Server 2004 computers. Add this destination set to the destination list on the Allow all HTTP traffic from ISA Server to all networks (for CRL downloads) system policy rule.

Answer: B

Question: 53

You are the network administrator for your company. The network contains an ISA Server 2004 computer named ISA1. The relevant portion of the network is configured as shown in the exhibit.



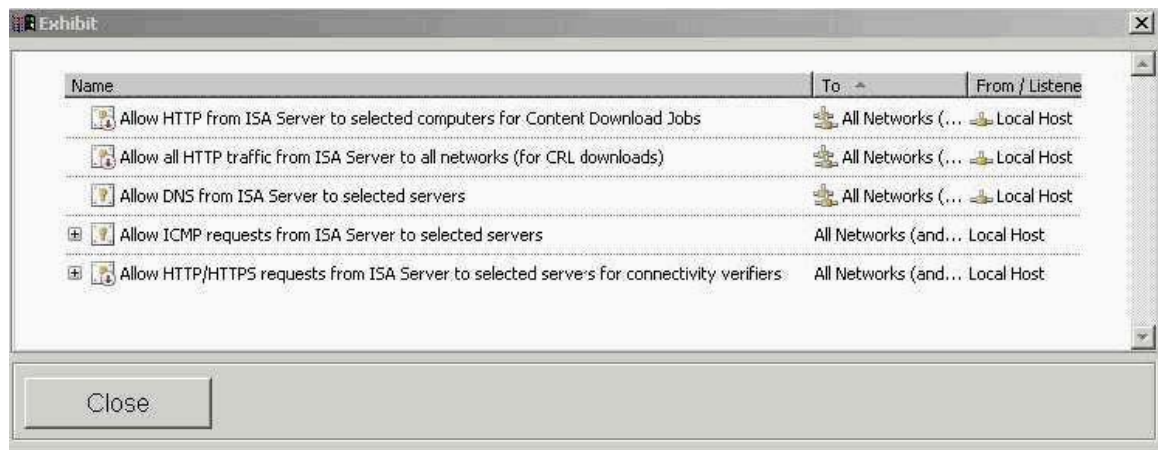
When you installed ISA Server 2004 on ISA1, you defined the Internal network address range as 10.0.1.0 through 10.0.1.255. You create an access rule to allow all traffic from the Internal network to the External network. Users are not required to be authenticated to use this rule. Users on network IDs 10.0.2.0/24 and 10.0.3.0/24 report that they cannot connect to the Internet. You examine the routing tables on the router and on ISA1 and confirm that they are correctly configured. You need to ensure that users on network IDs 10.0.2.0/24 and 10.0.3.0/24 can connect to the Internet. What should you do?

- A. Create a subnet network object for network ID 10.0.2.0/24 and for network ID 10.0.3.0/24.
- B. Add the address ranges 10.0.2.0 through 10.0.2.255 and 10.0.3.0 through 10.0.3.255 to the definition of the Internal network.
- C. Create two new networks, one for network ID 10.0.2.0/24 and one for 10.0.3.0/24. Create access rules to allow these networks access to the Internet.
- D. Create two new networks, one for network ID 10.0.2.0/24 and one for 10.0.3.0/24. Create a new network set containing these networks. Create an access rule to allow this network set access to the Internet.

Answer: B

Question: 54

You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory domain named contoso.com. The network contains an ISA Server array. The array contains two ISA Server 2004 computers named ISA1 and ISA2. ISA1 and ISA2 connect to the Internet. All client computers on the network are configured as Web Proxy clients. The firewall policy on the ISA Server array is configured as shown in the exhibit.



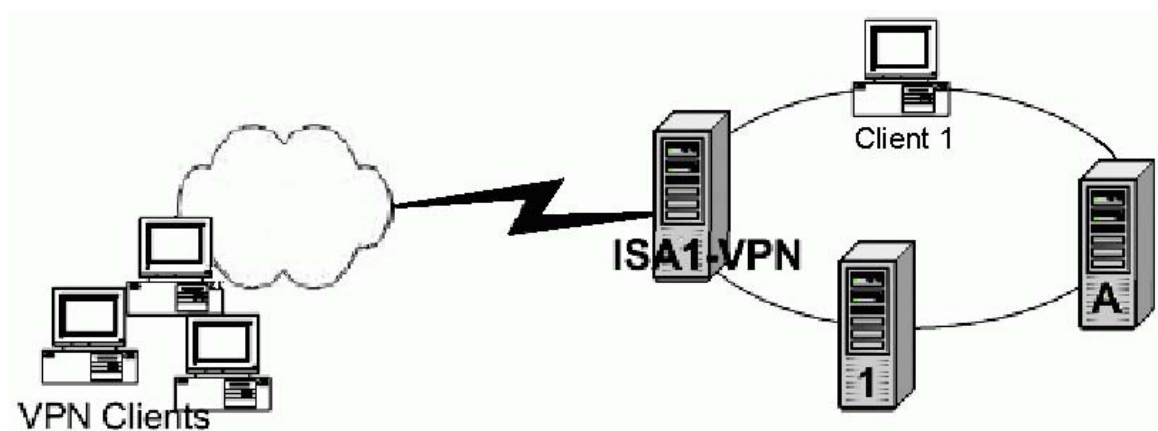
Users report that when they access www.contoso.com Web pages, the network is very slow. You discover that the content download jobs to www.contoso.com have failed. You need to configure the array to allow users on the network to access www.contoso.com Web pages more quickly. What should you do?

- A. Enable the Allow HTTP/HTTPS requests from ISA Server to selected servers for connectivity verifiers system policy rule.
- B. Enable the Allow HTTP from ISA Server to selected computers for Content Download Jobs system policy rule.
- C. Enable a new HTTP access rule that includes the Internal network. Configure the rule to use port 8080.
- D. Enable Cache Array Routing Protocol (CARP) on the Local Host network.

Answer: B

Question: 55

You are the network administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains a Windows Server 2003 domain controller named CompanyA and a Windows Server 2003 RADIUS server named Company1. Both CompanyA and Company1 are members of the Company.com domain. The relevant portion of the network is configured as shown in the Network exhibit.



You configure an ISA Server 2004 computer named ISA1-VPN to meet the following requirements:

- 1 Allow external VPN connections.
- 2 Allow Internet VPN server access for internal VPN clients.
- 3 Allow only RADIUS authentication for VPN connections.

The system policy on ISA1-VPN is configured as shown in the System Policy exhibit.

Or...	Name	Action	From / ...	To
	Allow access to directory services for authentication purposes	 Allow	Local Host	
	Allow remote logging to trusted servers using NetBIOS	 Allow	Local Host	Internal
	Allow RADIUS authentication from ISA Server to trusted RADIUS servers	 Allow	Local Host	
	Allow Kerberos authentication from ISA Server to trusted servers	 Allow	Local Host	

A client computer named Client1 can connect to VPN servers on the Internet. However, externalVPN client computers cannot be authenticated when they try to connect to ISA1-VPN. You need to ensure that external VPN client computers can create VPN connections to ISA1-VPN. What should you do?

- A. Create a new server publishing rule by using Company1.Company.com. Configure the new publishing rule to use L2TP Server as the protocol. Configure the publishing rule to use the External network as the listener.
- B. Create a new server publishing rule by using Company1.Company.com. Configure the new publishing rule to use PPTP Server as the protocol. Configure the publishing rule to use the Internal network as the listener.
- C. Edit the Allow access to directory services for authentication purposes system policy rule by replacing the computer element CompanyA.Company.com with Company1.Company.com.
- D. Edit the Allow RADIUS authentication from ISA Server to trusted RADIUS servers system policy rule by replacing the computer element CompanyA.Company.com with Company1.Company.com.

Answer: D

Question: 56

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 is connected to the Internet. VPN access is configured to ISA1. RADIUS is configured as the only type of authentication for VPN connections. All remote users can connect to ISA1 by using a VPN connection. All internal users can connect to the Internet. You are replacing ISA1 with a new ISA Server computer named ISA2. You export the network-level node configuration settings on ISA1 to a file named ISAconfig.xml. You import the ISAconfig.xml file on ISA2. You replace ISA1 with ISA2 on the network. Remote VPN users report that they cannot authenticate to gain access to the network. Internal network users report that they cannot connect to the Internet. You need to configure ISA2 to allow incoming and outgoing access for company users. What should you do?

- A. Export the system policy configuration settings on ISA1 to an .xml file. Import the .xml file on ISA2.
- B. Export the array configuration settings on ISA1. Include confidential information in the exported configuration file. Import the file on ISA2.
- C. Export the array configuration settings on ISA1. Include user permission settings in the exported configuration file. Import the file on ISA2.
- D. Export the VPN Clients configuration on ISA1. Include confidential information in the exported configuration file. Import the file on ISA2.

Answer: B

Question: 57

You are a network administrator for Company.com. The company has a main office and two branch offices. Users in the main office use client computers that run Windows XP Professional. Users in the branch offices use Macintosh-based client computers. You deploy one ISA Server 2004 computer in the main office and one ISA Server 2004 computer in

each branch office. You configure an access rule on the main office ISA Server computer. The rule allows authenticated users to download e-mail by using the POP3 protocol. You install the Firewall Client on the Windows XP Professional computers. Users in the branch offices report that they cannot download e-mail by using the POP3 protocol. You need to ensure that users in the branch offices can download e-mail by using the POP3 protocol. You also need to ensure that authentication is required for all outbound traffic from the main office. What should you do?

- A. On each branch office ISA Server computer, configure Firewall client settings. Allow non-encrypted Firewall clients to connect to the ISA Server computer.
- B. On each branch office ISA Server computer, configure firewall chaining. Configure firewall chaining to use a user account.
- C. On the main office ISA Server computer, configure a server publishing rule. Publish the POP3 server the users are attempting to connect to.
- D. On the main office ISA Server computer, configure IP preferences. Disable IP routing.

Answer: B

Question: 58

You are the administrator of an ISA Server 2004 computer named ISA1. ISA1 has two network adapters. Access rules allow users on the Internal network to have HTTP access to the Internet. You add a third network adapter to ISA1 and connect the third network adapter to a perimeter network. You place a Web server named WebServer2 on this perimeter network segment. WebServer2 must be accessible to computers on the Internal network. You create a computer object for WebServer2 and then create an access rule that allows Internal network clients HTTP access to WebServer2. Users are not required to authenticate with ISA1 to access WebServer2. Users report that they cannot access information on WebServer2. When they attempt to access the Web site, they receive the following error message: "Error Code 10060: Connection timeout. Background: There was a time out before the page should be retrieved. This might indicate that the network is congested or that the website is experiencing technical difficulties." You need to ensure that users on the Internal network can access information on WebServer2. First, you verify that WebServer2 is operational. What should you do next?

- A. Create a network rule that sets a route relationship between the Internal network and the perimeter network.
- B. Create a server publishing rule that publishes WebServer2 to the Internal network.
- C. Create a Web publishing rule that publishes WebServer2 to the Internal network.
- D. Create an access rule that allows WebServer2 access to the Internal network.

Answer: A

Question: 59

Exhibit

Protocol	Local address	Foreign address	State
TCP	192.168.100.141:80	0.0.0.0	LISTENING
TCP	192.168.100.141:139	0.0.0.0	LISTENING
UDP	192.168.100.141:137	*,*	
UDP	192.168.100.141:138	*,*	

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. The IP address bound to the external network adapter of ISA1 is 192.168.100.141.

You run the netstat - na command on ISA1. The relevant portion of the output is shown in the following table. You need to ensure that ISA1 accepts connection requests for only HTTP traffic. You need to be able to quickly verify whether ISA1 is listening on TCP port 139. What should you do?

- A. From a remote computer, run the pathping command to query ISA1.
- B. From a remote computer, use a port scanner to query ISA1.
- C. On ISA1, use the Portqry.exe tool to query ISA1.
- D. On ISA1, use the Netdiag.exe tool to query ISA1.

Answer: B Question: 60

You are the administrator of an ISA Server 2004 computer named ISA1. ISA1 is configured to generate daily and monthly reports. ISA1 publishes the reports to a folder named IsaReports. You generate custom reports to indicate user activity during the weekends of the last three months. The reports for the last five weekends display correct data. However, reports for previous weekends cannot be displayed. Only monthly activity summary reports are available for previous months. You need to provide custom reports that show the actual activity for all the weekends during the last three months. What should you do?

- A. Configure the Microsoft Data Engine (MSDE) database log files to be saved for 130 days. Restore the MSDE database log files from backup for the last three months.
- B. Configure daily reports to be saved for 130 days. Restore the log summary files from backup for the last three months.
- C. Delete the log summary files. Configure daily reports to be saved for 130 days. Disable and then re-enable log summary reports.
- D. In the IsaReports folder, create a new folder for each of the weekends. Copy the respective daily report files for each day of a weekend into their corresponding folders.

Answer: B

Question: 61

You enable the default Network configuration changed alert. You add a custom alert named Network Connectivity. The properties of the Network Connectivity alert are configured as shown in the Alert Events exhibit and the Alert Actions exhibit.

General Events Actions

Event:

Network configuration changed

Description:

A network configuration change that affects ISA Server was detected.

Additional condition:

Network disconnected

Specify how many times the event should occur before the alert is triggered:

☐ Number of occurrences:

☐ Number of events per second:

Each subsequent time the thresholds are met, trigger the alert:

☒ Immediately

☐ Only if the alert was manually reset

☐ If time since last execution is more than

minutes

General | Events | Actions

☐ Send e-mail Test

SMTP server: Browse...

From:

To:

Cc:

☒ Run a program

Browse...

Use this account: Set Account...

☒ Report to Windows event log

☐ Stop selected services Select...

☐ Start selected services Select...

You test the Network Connectivity alert by disabling the ISA1 network adapter that is connected to the perimeter network. You see the corresponding alert in both the Alerts view and the application log of Event Viewer. However, the message is not received on any of the administrative computers. You need to ensure that the administrative computers receive the text message when the Network Connectivity alert is triggered. You also need to be able to test the alert by disabling any of the network adapters on ISA1. What should you do?

- A. Disable the default Network configuration changed alert.
- B. Enable and start the messenger service and the alert service on ISA1 and on your administrative computer.
- C. On ISA1, configure the DisabledDHCPMediaSense entry with a value of 1.
- D. Configure the Network Connectivity alert actions to run NetworkAlert.cmd by using an account that has the Log on as a batch job right.

Answer: D

Question: 62

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 is configured to provide forward Web caching for users on the Internal network. Microsoft SQL Server 2000

Desktop Engine (MSDE 2000) database logging is enabled on ISA1. ISA1 is configured with 512 MB of RAM and a single 60-GB hard disk. During periods of peak usage, users report that it takes longer than usual for Web pages to appear. You need to identify the source of the slow performance. Which two System Monitor performance counters should you add? (Each correct answer presents part of the solution. Choose two.)

- A. Memory\Pages/sec
- B. Memory\Pool Nonpaged Bytes
- C. MSSQL\$MSFW:Databases(*)\Transactions/sec
- D. MSSQL\$MSFW:MemoryManager\Target Server Memory (KB)
- E. Physical Disk\Avg. Disk Queue Length
- F. Physical Disk\SplitIO/sec

Answer: A, E

Question: 63

You are the network administrator for Company.com. The company has a main office, two branch offices and one research office. An ISA Server array is configured for each of these three offices. All arrays are members of the same ISA Server 2004 enterprise. A Configuration Storage server is located in the main office. Replica Configuration Storage servers are located in each branch office. Administrators at the main office administer the enterprise settings and the main office array. The administrators at each branch office administer the arrays at their respective branch offices. You need to install a new ISA Server array in the research office. You need to ensure that only research office administrators can manage access rules that affect client computers in the research office. What should you do?

- A. Configure a replica Configuration Storage server. Assign the research office administrators the ISA Server Array Administrator role.
- B. Configure a new array in the existing enterprise. Assign the research office administrators the ISA Server Array Administrator role.
- C. Configure a new array in the existing enterprise. Assign the research office administrators the ISA Server Enterprise Administrator role.
- D. Configure a new Configuration Storage server in the research office. Configure it as a new enterprise. Assign the research office administrators the ISA Server Enterprise Administrator role.

Answer: D

Question: 64

You are a network administrator for Company, Inc. The network contains an ISA Server 2004 computer named ISA1. ISA1 is configured to allow outbound Internet access only. A listener named DefaultHTTP is configured to listen for requests on port 80 on the external interface. The internal network contains two Web sites named HR and Sales, which are used by employees. The HR Web site is stored on a Web server named Web1.Company.com. The Sales Web site is stored on a Web server named http://www.Company.com. You must allow employees to access both the HR Web site and the Sales Web site from the Internet. You must ensure that employees can access the HR Web site by using the URL http://www.Company.com/hr.

You must also ensure that employees can access the Sales Web site by using the URL http://www.Company.com/sales. What should you do?

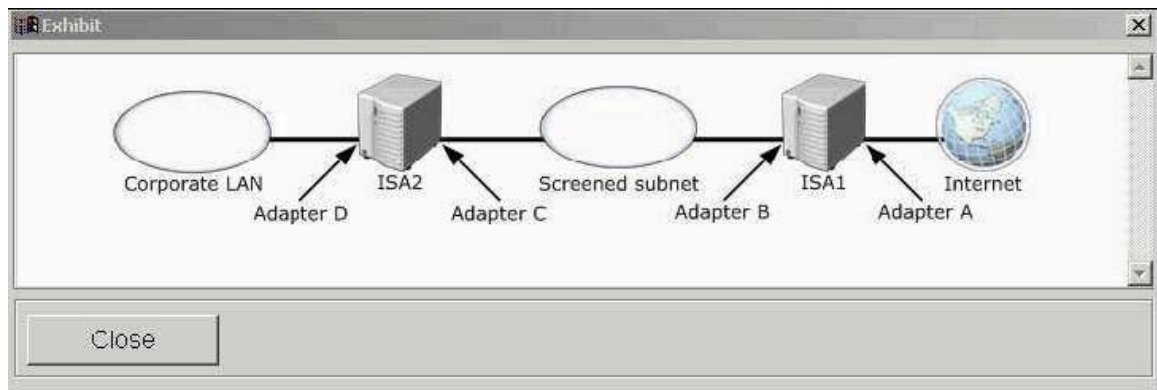
- A. Configure one of the Web servers to listen for HTTP requests on port 8080. Create two server publishing rules. Create one of the rules to respond to requests on port 8080, and configure this rule to forward requests to one internal Web server. Create the other rule to use the DefaultHTTP listener, and configure this rule to forward to the other internal Web server.
- B. Configure one of the Web servers to listen for HTTP request on port 8080. Create a new listener that uses HTTP on port 8080. Create two Web publishing rules. Configure each rule to forward to a different internal Web server.

- Configure each rule to use a different listener.
- C. Create two server publishing rules. Configure each rule to forward to a different internal Web server. Configure each internal Web server to listen for HTTP requests on an unused port.
- D. Create two Web publishing rules. Configure each rule to forward to a different internal Web server. Configure each rule to use the DefaultHTTP listener.

Answer: D

Question: 65

You are a network administrator for your company. You are installing ISA Server 2004 on two computers named ISA1 and ISA2. The network is configured as shown in the exhibit.



You need to ensure that the implementation plan meets the following requirements: All devices that pass outbound traffic must perform network address translation (NAT). All Internet-accessible internal resources must be published. All traffic between two network interfaces on an ISA Server computer must be subject to inspection. Which interface or interfaces should be configured as an internal interface? (Choose all that apply.)

- A. Adapter A
- B. Adapter B
- C. Adapter C
- D. Adapter D

Answer: B

Question: 66

You are the network administrator for Company.com. The network consists of a single Active Directory domain. The network contains an ISA Server 2004 computer named ISA1. ISA1 is a member of the Active Directory domain. You configure ISA1 as a remote access VPN server that allows both PPTP and L2TP over IPSec remote access client connections. You want to control VPN access by using a remote access policy. You configure ISA1 to allow VPN access to members of the Domain Users global group. However, VPN connections fail. You examine the properties of several domain user accounts and you discover that the Control access through Remote Access Policy option is not available. You need to enable remote access permission by using a remote access policy. What should you do?

- A. Configure a RADIUS-based remote access policy.
- B. Configure the ISA Server remote access policy.
- C. Elevate the domain functional level.
- D. Enable user mapping for VPN client connections.

Answer: C

Question: 67

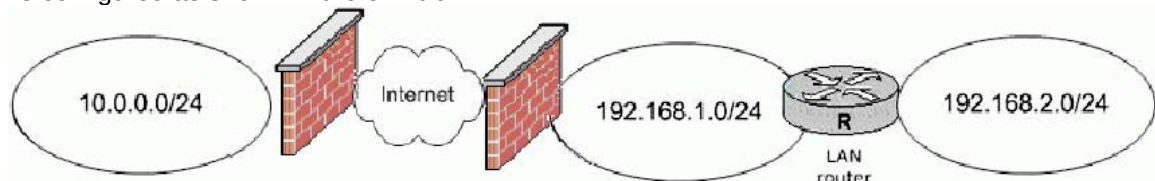
You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 is configured with two network adapters. The external network adapter is connected to the Internet. The internal network adapter is connected to the Internal network. The Internal network address range is 10.0.0.0 through 10.0.0.255. You define the VPN assignment as a static pool that extends from 10.0.1.0 through 10.0.1.255. You enable VPN client access. You test the VPN configuration and successfully establish a VPN connection to ISA1 from an external Windows XP Professional client computer named XP1. You discover that you cannot browse external Web sites from XP1 while it has a VPN session with ISA1. You confirm that internal client computers can browse external Web sites. You need to ensure that VPN clients can browse external Web sites while connected to ISA1. You also need to ensure that all requests for external Web sites from VPN clients are processed through ISA1. What should you do?

- A. On the VPN clients, in the VPN connection object in the Network Connections folder, clear the check box to use the default gateway on the remote network.
- B. On the VPN clients, in the Internet Explorer, configure the dial-up and virtual network settings for the VPN connection object to use the proxy server settings for ISA1.
- C. On ISA1, reconfigure the VPN address assignments to use DHCP. Ensure that the address assignments are within the range defined for the Internal network.
- D. On ISA1, create an access rule that allows outbound HTTP and HTTPS access from the VPN client network for the All Authenticated Users user set.

Answer: D

Question: 68

You are the network administrator for your company. The company has a main office and one branch office. You want to connect the main office to the branch office by using a site-to-site VPN connection. The main office has an ISA Server 2004 computer named ISA1. The branch office has an ISA Server 2004 computer named ISA2. The relevant portion of the network is configured as shown in the exhibit.



The main office network includes two network IDs: 192.168.1.0/24 and 192.168.2.0/24. The 192.168.1.0/24 network is directly connected to ISA1 and is configured as the default Internal network. The 192.168.2.0/24 network is connected to the 192.168.1.0/24 network by a router on the main office Internal network. You create two subnet network objects in the ISA Server Management console: one network for the 192.168.1.0/24 network and one for the 192.168.2.0/24 network. The internal network adapter on ISA2 is on network ID 10.0.0.0/24. You create an access rule on ISA1 and on ISA2 to allow all traffic to and from the main office and branch office networks. You create an access rule on ISA1 to allow all traffic between the default Internal network and the branch office network. Users on network ID 192.168.2.0/24 report that they cannot connect to computers at the branch office. You need to ensure that all users at the main office can connect to resources located on the branch office network. What should you do?

- A. Add the addresses in network ID 192.168.2.0/24 to the default Internal network at the main office.
- B. Add the addresses in network ID 10.0.0.0/24 to the default Internal network at the main office.
- C. Remove the router connecting the two networks at the main office, and place both network IDs on a single Ethernet broadcast segment.
- D. On ISA2, create a subnet network object representing the 192.168.2.0/24 network. Add this network object to the list of destination computers that the branch office computers can connect to.

Answer: A

Question: 69

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1, which allows outgoing connections to the Internet. A network rule defines a network address translation (NAT) relationship between the Internal network and the Internet. Users on ISA Server protected networks require access to PPTP and L2TP over IPsec VPN servers on the Internet. You configure all network computers, except ISA1, as both Web Proxy and Firewall clients. You create access rules on ISA1 to allow outbound connections to the Internet by using PPTP Client, IPsec NAT Traversal (NAT-T) Client, and IKE Client protocols. You discover that users cannot connect to Internet PPTP and L2TP over IPsec VPN servers. You need to ensure that users can connect to PPTP and L2TP over IPsec VPN servers on the Internet. What should you do?

- A. Disable the Web Proxy client configuration on the network computers.
- B. Disable the Firewall client configuration on the network computers.
- C. Configure the network computers as SecureNAT clients.
- D. Configure the network computers to use IPsec tunnel mode.

Answer: C

Question: 70

You are the network administrator for Company.com. The network consists of a single Active Directory domain named Company.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 is a member of the domain. The fabrikam.com domain contains an enterprise certification authority (CA) that is installed on a Windows Server 2003 computer named Company3. You want to configure ISA1 as a VPN server. You want VPN clients to connect by using L2TP over IPsec. You want the VPN clients to use certificate-based authentication. You configure a Group Policy object (GPO) so that ISA1 and other member computers acquire computer certificates through automatic enrollment. ISA1 does not receive a computer certificate through automatic enrollment. However, automatic enrollment of the computer certificate is successful for other member computers. You examine the system log and the application log on ISA1. You discover several events related to the failure of the automatic enrollment of the certificate. The events indicate an inability of ISA1 to use RPC and Distributed Component Object Model (DCOM) to acquire the certificate through automatic enrollment. You need to install a computer certificate on ISA1 from the enterprise CA. You also need to ensure that the computer certificate can be used for only client authentication and server authentication. What should you do?

- A. On ISA1, add the Certificates snap-in for the local computer to an MMC console. In the Personal certificate store of the Certificates snap-in, use the Certificate Request wizard to manually request a computer certificate.
- B. On ISA1, using Internet Explorer, connect to the certificate server Web enrollment pages on Company3. Use the Advanced Certificate Web enrollment pages to request a certificate based on the Administrator certificate template and to store the certificate in the local computer certificate store.
- C. From a Web server on the Internal network, request a Web certificate from Company3 that uses ISA1.fabrikam.com as the common name and that contains an exportable private key. Import the certificate to the Personal certificate store for the local computer on ISA1.
- D. On ISA1, temporarily disable the RPC application filter and create an access rule to allow all protocols from ISA1 to the Internal network. Temporarily, disable the setting to enforce strict RPC compliance. Manually refresh the GPO.

Answer: D

Question: 71

You are the network administrator for Company.com. The company has a main office and is adding a branch office. You need to connect the two offices to each other so that employees in the branch office can access file, Web and database servers at the main office. You create a site-to-site VPN by creating remote site networks on ISA Server 2004 computers in both offices. You configure L2TP over IPsec as the VPN protocol for the site-to-site connection. You configure the ISA

Server computers in both offices to use computer certificates and to use a preshared key. The L2TP over IPSec connection is successfully established, but when you view the connection parameters in the IPSec console, you discover that the preshared key is used to establish the IPSec connection. You need to allow the computer certificates to be used instead of the preshared key for the IPSec negotiations. What should you do?

- A. Remove the preshared key from only the main office ISA Server computer's remote site network configuration.
- B. Remove the preshared key from only the branch office ISA Server computer's remote site network configuration.
- C. Remove the preshared key from the ISA Server computer's remote site network configuration at both offices.
- D. Remove the computer certificates on the ISA Server computers at both offices and replace them with user certificates.

Answer: C

Question: 72

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. ISA1 is configured as a remote access VPN server and as a DHCP server. VPN client computers need to be assigned the following DHCP options:

- 1 DNS
- 2 WINS
- 3 Domain name

On the DHCP server, you create a DHCP scope that includes the three DHCP options. VPN users report that they cannot connect to file shares after logging on to the network. You discover that no WINS or DNS server address is assigned to the VPN clients, and no primary domain name is listed. You need to ensure that the DHCP options are assigned to the VPN client computers. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Remove the DHCP server from ISA1 and place it on a computer that is behind ISA1.
- B. Configure the Routing and Remote Access internal network adapter as a DHCP client.
- C. In the ISA Server Management console, configure VPN address assignment to use the Internal network for the DHCP, DNS and WINS services.
- D. Install a DHCP Relay Agent on ISA1

Answer: A, D

Question: 73

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1, which functions as a remote access VPN server for the network. ISA1 is a member of a workgroup. ISA1 is configured to accept only EAP authentication for VPN clients. All VPN clients have been assigned user certificates from the corporate enterprise certification authority (CA). Users report that they cannot connect to the network. They state that they receive the following error message: "Error 691: Access was denied because the username and/or password was invalid for the domain." You need to ensure that VPN users can connect to the network. What should you do?

- A. Join ISA1 to the corporate network domain.
- B. Place the CA certificate into the VPN clients' Trusted Root Certification Authorities computer certificate store.
- C. Enable remote access permissions for the VPN user accounts in Active Directory.
- D. Configure ISA1 to use RADIUS authentication.

Answer: A

Question: 74

You are the network administrator for Company.com. The company has a main office and is adding a branch office. ISA Server 2004 Standard Edition is deployed at the main office and at the branch office.

You are connecting the main office with the new branch office by using a site-to-site VPN. You configure the remote site networks and access rules to allow communications between the main and branch office networks. Users at the main office report that they cannot connect to servers at the branch office. Users at the branch office report that they cannot connect to servers at the main office. You view the Event Viewer services log on the ISA Server computer in each office. You see the following error message: "Unable to contact a DHCP server. The Automatic Private IP Address 169.254.99.87 will be assigned to dial-in clients. Clients may be unable to access resources on the network." You need to enable users at the main and the branch office to connect to resources on the other side of the site-to-site VPN connection. What should you do?

- A. Install and configure a DHCP server at the main office.
- B. Install and configure a DHCP server at the branch office.
- C. Install and configure a DHCP server at each office.
- D. Configure both ISA Server computers to use their ISP's DHCP server.

Answer: C

Question: 75

You are the network administrator for Company.com. The network contains a single ISA Server 2004 computer. Employees use an application named App1, which is hosted on a server named Server1. Server1 has Terminal Services installed. On a Windows Server 2003 computer, you enable Remote Desktop connections. You create a Web publishing rule to publish the Remote Desktop connections virtual directory. Users can connect to the Remote Desktop Web Connection site by using Internet Explorer. However, they cannot establish a Terminal Services connection. You need to ensure that users can access App1. What should you do?

- A. Configure an RDP server publishing rule.
- B. Configure an RPC Services server publishing rule.
- C. Configure a new RDP protocol definition.
- D. Configure a new RPC protocol definition.

Answer: A

Question: 76

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer. The company's written security policy states that all incoming connections from the Internet into the corporate network must be encrypted, and only SSL Web connections are allowed. The company upgrades to the latest version of Microsoft Exchange Server. You configure a server publishing rule to allow inbound secure Exchange RPC connections to the Exchange Server computer. You need to allow users to connect to Outlook Web Access and you need to adhere to the company's security policy. What should you do?

- A. Create an NNTPS server publishing rule.
- B. Create an HTTP Web publishing rule.
- C. Delete the current Exchange RPC server publishing rule. Create an HTTPS Web publishing rule.
- D. Delete the current Exchange RPC server publishing rule. Create an IMAPS server publishing rule.

Answer: C

Question: 77

You are the network administrator for Company.com. You plan to install an ISA Server 2004 array on the network. Users access a Secure Shell protocol (SSH)-based application on a partner Web site. Access to this application is mission-critical to Company.com. You need to configure ISA Server 2004 to ensure that Internet access is still available if the ISA Server computer fails. What should you do?

- A. Configure Network Load Balancing on the array.
- B. Configure Cache Array Routing Protocol (CARP) on the array.
- C. Create a new enterprise policy on the array and apply the policy to the array.
- D. Create two publishing rules for the partner Web site.

Answer: A

Question: 78

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1 and a Web server named Web1. The company has two Web sites named SiteA and SiteB. Both Web sites are hosted on Web1. SiteA requires users to be authenticated. SiteB needs to have only anonymous access configured. You need to configure COMPANY1 to publish both Web sites and to meet the security requirements of each Web site. What should you do?

- A. On COMPANY1, configure a Web publishing rule for each Web site. Configure the rule for SiteA to allow anonymous connections.
- B. On COMPANY1, configure a Web publishing rule for each Web site. Configure the rule for SiteA to use Basic authentication.
- C. Configure one Web publishing rule for the two Web sites. Configure the rule to use EAP authentication.
- D. Configure one Web publishing rule for the two Web sites. Configure the rule to use forms-based authentication.

Answer: B

Question: 79

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. The company's written security policy states that users must be allowed access to the Internet only between the hours of 08:00 and 17:00. You need to configure ISA1 to allow all Internet traffic between 08:00 and 17:00 and to not allow outbound Internet traffic at other times. What should you do?

- A. Create an access rule to allow all protocols. Configure the rule's schedule to be enabled between 08:00 and 17:00.
- B. Create an access rule to deny all protocols. Configure the rule's schedule to be enabled between 08:00 and 17:00.
- C. Create an access rule to allow all protocols at all times. Create another access rule that denies all protocols between 17:00 and 8:00. Ensure that this rule is placed immediately below the allow rules.
- D. Create an access rule to deny all protocols at all times. Create another access rule that allows all protocols between 08:00 and 17:00. Ensure that this rule is placed immediately below the deny rule.

Answer: A

Question: 80

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1.

The company uses Microsoft Exchange Server 2003 as its e-mail server. Remote users need to access the Exchange server by using either Microsoft Outlook Web Access or Microsoft Outlook 2003. You need to use HTTPS to provide access for both Outlook Web Access and Outlook 2003. You want to use forms-based authentication for Outlook WebAccess. ISA1 is configured with three Web listeners named WebListen1, WebListen2 and Weblisten3. You configure WebListen1 to use SSL certificate authentication. You configure WebListen2 to use forms-based authentication. You configure WebListen3 to use Windows Integrated authentication. You need to ensure that remote users can access the Exchange server. What should you do?

- A. Create two Web publishing rules for the Exchange server. Configure one of the rules to use WebListen1. Configure the other rule to use WebListen3.
- B. Create one Web publishing rule for the Exchange server. Configure the rule to use WebListen2.
- C. Create two Web publishing rules for the Exchange server. Configure one of the rules to use WebListen1. Configure the other rule to use WebListen2.
- D. Create one Web publishing rule for the Exchange server. Configure the rule to use WebListen1.

Answer: C

Question: 81

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer. Users on the Internal network require access to a partner VPN server. The partner VPN server uses machine certificate authentication for VPN connections. You enable a network address translation (NAT) relationship between the Internal network and the External network. You need to ensure that company users can access the partner VPN server. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Create an access rule to enable outbound access to the PPTP Client protocol.
- B. Create an access rule to enable outbound access to the IPsec with Encapsulating Security Payload (ESP) Server protocol.
- C. Create an access rule to enable outbound access to the IKE Client protocol.
- D. Create an access rule to enable outbound access to the IPsec NAT-T Client protocol.

Answer: C, D

Question: 82

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named ISA1. The company deploys a new secure Web site. The Web site hosts an application named App1. App1 requires client certificate authentication, and must record the client IP source address for every request. You need to configure ISA1 to publish the new Web site. First, you create an SSL Web publishing rule. Now, you need to configure the rule to meet the requirements. What should you do?

- A. Configure the rule's link translation to replace absolute links in all Web pages.
- B. Configure the rule to forward the original host header to the published Web server.
- C. Configure the rule to forward the requests so that they appear to come from ISA1.
- D. Configure the rule to forward the requests so that they appear to come from the original client.

Answer: D

Question: 83

You are the network administrator for Company.com. The network contains a single ISA Server 2004 computer named ISA1. The company's new written security policy states that internal computer names must not be published or accessible via the Internet. You need to publish a new Web site that has many internal computer names within the Web site. You must publish this Web site while adhering to the company's security policy. What should you do?

- A. Configure an HTTP server publishing rule. Configure the rule so that requests sent to the published server forward the URLs so that they appear to come from the original client computer.
- B. Configure an HTTP server publishing rule. Configure the rule so that requests sent to the published server forward the URLs so that they appear to come from ISA1.
- C. Create a Web publishing rule. On the rule, enable and configure HTTP bridging.
- D. Create a Web publishing rule. On the rule, enable and configure the link translator.

Answer: D

Question: 84

You are the administrator of an ISA Server 2000 computer named ISA1. You use the ISA Server 2004 Migration Tool to perform an in-place upgrade on ISA1. You install the Firewall Client installation component on ISA1. Client computers in the sales department run Windows NT Workstation 4.0 with Internet Explorer 5.0 and the Microsoft Proxy 2.0 Winsock Proxy client installed. All other client computers run Windows XP Professional. The ISA Server 2000 Firewall Client was installed on the Windows XP Professional computers by using Group Policy. You discover that all client computer requests to ISA1 are being sent unencrypted. You need to configure all client computers to communicate to ISA1 by using encryption. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Uninstall the Winsock Proxy client from the client computers in the sales department. Run Setup.exe to install the ISA Server 2004 Firewall Client.
- B. Uninstall the Winsock Proxy client from the client computers in the sales department. Enable the Allow non-encrypted Firewall client connections setting on the Internal network.
- C. Uninstall the Winsock Proxy client from the client computers in the sales department. Enable the Require all users to authenticate setting. Configure SSL certificate authentication for all Firewall clients on the Internal network.
- D. Upgrade the Firewall Client for ISA Server 2000 software on the Windows XP Professional client computers.

Answer: A, E

Question: 85

You are the network administrator for Company. The network consists of a single Active Directory domain Company.com. The network contains an ISA Server 2004 computer named ISA1. Client computers on the network consist of Windows 98 computers, Windows XP Professional computers, UNIX workstations and Macintosh portable computers. You configure ISA1 by using the Edge Firewall network template. You manually configure ISA1 with access rules to allow HTTP and HTTPS access to the Internet. You configure ISA1 to require all users to authenticate. You need to provide Internet access for all client computers on the network while preventing unauthorized non-company users from accessing the Internet through ISA1. You also want to reduce the amount of administrative effort needed when you configure the client computers. What should you do?

- A. Configure all client computers as Web Proxy clients. Configure Basic authentication on the Internal network.
- B. Configure all client computers as Web Proxy clients. Configure Basic authentication on the Local Host network.
- C. Configure all client computers as SecureNAT clients. Configure Basic authentication on the Internal network.
- D. Configure the Windows-based computers as Firewall clients. Configure the non-Windows-based computers as Web Proxy clients. Configure Basic authentication on the Local Host network.

Answer: A

Question: 86

You are the network administrator for Company.com. The network contains an ISA Server 2004 computer named COMPANY1, which controls access between three segments on the network. The network is configured as shown in the

exhibit. A network address translation (NAT) relationship exists from the Internal network to the perimeter network. A Windows Server 2003 computer named DNS1 functions as a DNS server. Web Proxy clients can access Web sites on the Internet. However, when SecureNAT clients try to access hosts on the Internet, they receive the following error message: "Cannot find server or DNS error." You need to ensure that SecureNAT clients can perform DNS name resolution correctly for hosts on the Internet. You also need to ensure that DNS name resolution is optimized for Active Directory. First, from a SecureNAT client, you run the nslookup command and set the default server to 172.16.0.11.

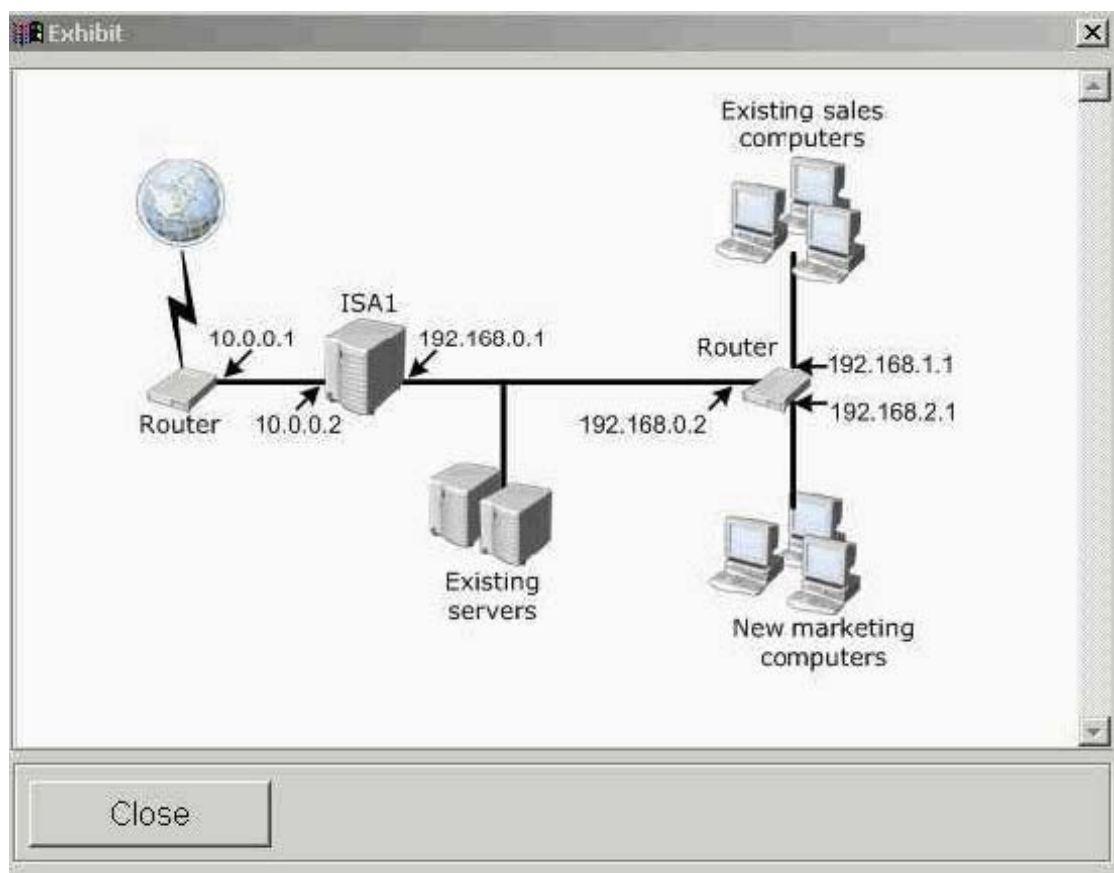
From the Nslookup console, you are able to query name server (NS) resource records on the Internet. What should you do next?

- A. On COMPANY1, replace the DNS server publishing rule with an equivalent access rule.
- B. On COMPANY1, change the NAT relationship between the perimeter network and the Internal network to a route relationship.
- C. On COMPANY1, delete the .(root) zone and then disable recursion.
- D. On DNS1, remove forwarding configuration and add a .(root) zone.

Answer: C

Question: 87

You are a network administrator for your company. The network contains an ISA Server 2004 computer named ISA1. ISA1 is configured to allow users in the sales department access to resources on the Internet. Users in the marketing department also want access to resources on the Internet. You add a new network and computers for the marketing department. You install the Firewall Client and configure the Web Proxy client on all computers in the new network. The company's network is configured as shown in the exhibit.



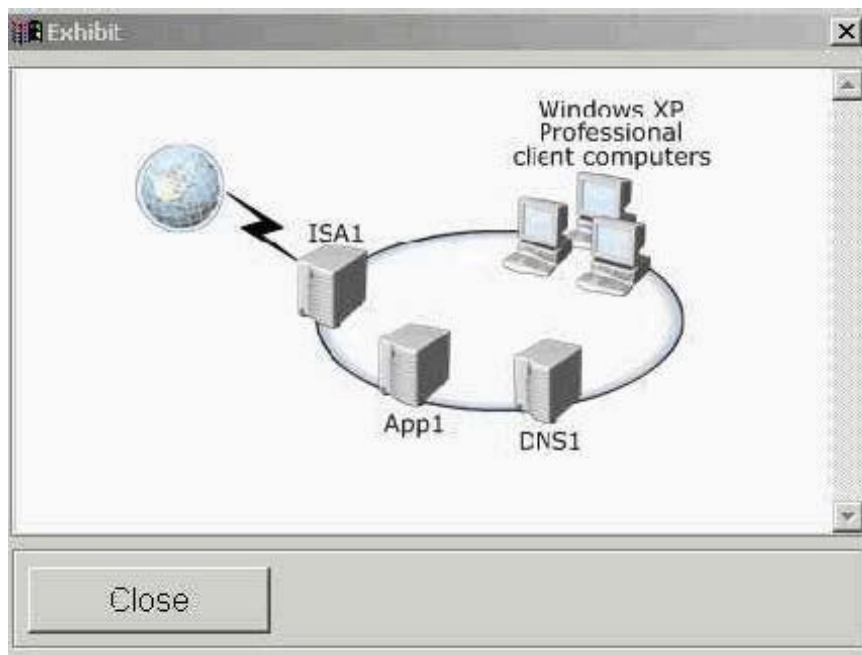
Users in the marketing department report that they cannot access resources on the Internet. You verify that users in the sales department and the internal servers can still access resources on the Internet. You need to ensure that users in the marketing department can access resources on the Internet. What should you do?

- A. Configure the marketing computers to use 192.168.0.1 as the default gateway.
- B. On ISA1, add a static route for the 192.168.2.1 network.
- C. On ISA1, add a network object for the marketing department.
- D. Configure the DNS settings of the marketing computers to use a DNS server that can resolve Internet names.

Answer: B

Question: 88

You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory domain named contoso.com. The relevant portion of the network is configured as shown in the exhibit.



An ISA Server 2004 computer named ISA1 is configured with the 3-Leg Perimeter network template. All client computers are configured as Firewall clients and Web Proxy clients. Client computers are configured to use a DNS server named DNS1. DNS1 is configured to forward requests to an ISP's DNS server. An application server named App1 runs a Web-based application. Users on the network report that access to App1 is very slow. You monitor ISA1 and discover that client computer requests for App1 are being passed through ISA1. You need to configure ISA1 to allow faster access to App1. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Create an access rule for DNS client protocol.
- B. Enable IP routing between the perimeter network and the Internal network.
- C. In the properties of the Internal network on ISA1, enable the Directly access computers specified in the Domains tab option.
- D. Add contoso.com to the list of domain names available on the Internal network on ISA1.
- E. Add app1.contoso.com to the system policy DNS configuration group.

Answer: C, D

Question: 89

You are the network administrator for your company. The company has a main office and one branch office. The network contains an ISA Server 2004 computer named ISA1, which functions as a firewall for the branch office. The number of employees at the branch office has doubled in the last week. Users at the branch office report that they frequently receive outdated versions of Web pages when they access Web servers operated by some of your companys business partners. You need to ensure that users always receive the most up-to-date content for Web pages they access from the partner Web sites. You must also optimize bandwidth use at the branch office. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Increase the value for the Maximum size of URL cached in memory (bytes) setting.
- B. Create cache rules that disable the caching of content from the partner Web sites.
- C. Increase the size of the Web Proxy disk cache.
- D. Increase the percentage of free memory to use for caching.

Answer: B, C

Question: 90

You are the network administrator for Company.com. The network contains two COMPANY Server 2004 computers named COMPANY1 and COMPANY2. COMPANY1 is configured as the Enterprise Configuration Storage server. COMPANY1 and COMPANY2 are members of a single enterprise array. A Web server named Web1 resides in the perimeter network. You publish an external Web site on Web1. You publish an internal Web site on the array. COMPANY1 and COMPANY2 are each configured with a RAID-5 volume. You enable a cache drive on COMPANY1. You enable Cache Array Routing Protocol (CARP) on the Internal network on COMPANY1 and COMPANY2. Users report that access to Web1 is very slow. You discover that physical disk usage is extremely high on COMPANY1 and Web1. You need to configure COMPANY Server 2004 to allow faster access to Web1. What should you do?

- A. On COMPANY1, increase the HTTP caching Time to Live (TTL) setting to 50.
- B. On COMPANY1, increase the size of the cache drive.
- C. On COMPANY2, enable a content download job for the Web sites on Web1.
- D. On COMPANY2, configure a cache drive.

Answer: D

Question: 91

You are the network administrator for your company. The network contains an ISA Server 2004 Enterprise Edition computer named ISA1. You enable and configure Cache Array Routing Protocol (CARP) on ISA1. You configure a 1-GB cache drive on ISA1. You monitor ISA1 and discover that a large number of cached Web requests are coming from the sales department. You install ISA Server 2004 Enterprise Edition on two additional computers named ISA2 and ISA3. All of the ISA Server computers are joined to a single array. Array members are configured as shown in the following table.

Host name	Internal IP address	External IP address	Load factor
ISA1	10.10.10.10/24	131.107.200.10/24	50
ISA2	10.10.10.11/24	131.107.200.11/24	50
ISA3	10.10.10.12/24	131.107.200.12/24	50

You discover that many of the Internet Web requests are still being retrieved from the Internet. You need to reduce the number of Web requests that are being retrieved from the Internet. What should you do?

Host name	Internal IP address	External IP address	Load factor
ISA1	10.10.10.10/24	131.107.200.10/24	50
ISA2	10.10.10.11/24	131.107.200.11/24	50
ISA3	10.10.10.12/24	131.107.200.12/24	50

You discover that many of the Internet Web requests are still being retrieved from the Internet. You need to reduce the number of Web requests that are being retrieved from the Internet. What should you do?

- A. On ISA1, change the load factor to 100.
- B. On ISA1, increase the size of the cache drive to 2 GB.
- C. On ISA2 and ISA3, configure a cache drive.
- D. On ISA2 and ISA3, change the load factor to 100.

Answer: C

Question: 92

You are the network administrator for your company. The network contains an ISA Server 2004 computer named ISA1. The company's written security policy states that users must be allowed access to the Internet only between the hours of 08:00 and 17:00. You need to configure ISA1 to allow all Internet traffic between 08:00 and 17:00 and to not allow outbound Internet traffic at other times. What should you do?

- A. Create an access rule to allow all protocols. Configure the rules schedule to be enabled between 08:00 and 17:00.
- B. Create an access rule to deny all protocols. Configure the rules schedule to be enabled between 08:00 and 17:00.
- C. Create an access rule to allow all protocols at all times. Create another access rule that denies all protocols between 17:00 and 08:00. Ensure that this rule is placed immediately below the allow rule.
- D. Create an access rule to deny all protocols at all times. Create another access rule that allows all protocols between 08:00 and 17:00. Ensure that this rule is placed immediately below the deny rule.

Answer: A