IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **070-350**

Title : Implementing Microsoft Internet Security and Acceleration (ISA) Server 2004

Version : DEMO

1. You are the network administrator for Contoso, Ltd. 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 Web2 resides in a perimeter network. Web2 contains two company Web sites named http://internal.contoso.com and http://external.contoso.com. Members of the graphics team make frequent changes to the Web site named http://internal.contoso.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 the updates to http://internal.contoso.com. What should you do?

A. Add the contoso.com domain name to the list of domains on the Internal 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 a URL set for http://internal.contoso.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 Web2. Create a cache rule to include the computer set. Disable HTTP caching on the cache rule.
Answer: C

2. You are the network administrator for Contoso, Ltd. The network contains two ISA Server 2004 computers named ISA1 and ISA2. The network also contains a Routing and Remote Access server named RRAS1. The 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.contoso.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.contoso.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.contoso.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.contoso.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 chaining rule. On the rule, redirect SSL requests as SSL requests.Add a URL set for http://sales.contoso.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 exists 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

3. You are the network administrator for your company. 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

4. You are the network administrator for your company. The 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:Export the ISA Server 2004 configuration on ISA1 to a file named ISASETUPCONFIG.XML.Edit the ISASETUPCONFIG.XML file to include a valid external IP address. 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.xmlRun 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.XMLRun 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 IMPORT_ISACONFIG=1 FILEPATH=ISASETUPCONFIG.XMLRun an unattended setup by using this Msisaunattend.txt file on each new ISA Server 2004 computer.
Answer: C

5. You are the network administrator for your company. 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

6. 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 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 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

7. You are a network administrator for your company. 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 other 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

8. You are the network administrator for your company. 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:Create an access rule to allow all traffic between the Internal network and the Internet.Create an access rule to allow all traffic between the Internal network and the perimeter network.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.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 relationships 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 relationships between the Internal network, perimeter network, and External network to NAT.
Answer: A

9. You are the network administrator for your company. 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 users 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 types 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

10. You are a network administrator for your company. The 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:Ensure that users in the branch office can access the Internet.Ensure that users in the branch office are restricted by the main office access rules when accessing the Internet.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

11. You are a network administrator for Litware, Inc. 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.litwareinc.com. The URL resolves to a single virtual IP address. You implement a new Web site named Site1. To access Site1, users must authenticate by using credentials that are stored on a third-party RADIUS server. You publish Site1 on the array. You need to ensure that users can access Site1 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.litwareinc.com on one listener. Configure the other array member to listen for requests to Site1 on a new listener. Configure each listener to use the appropriate authentication method.

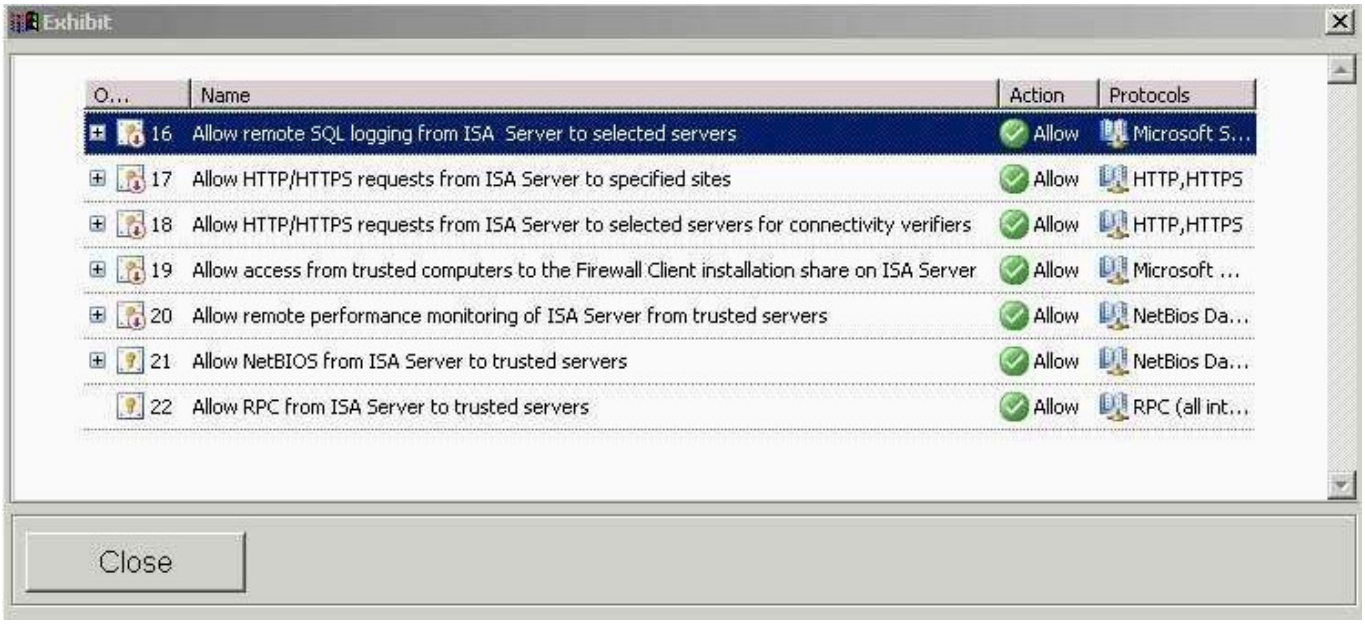
C. Use the Network Load Balancing console to configure each array member to use an affinity setting of None. Configure the listener to use RADIUS authentication.

D. Add a second unique network address to the external interface of each array member. Configure www.litwareinc.com

to resolve to the new addresses by using DNS round robin. Configure the listener to use RADIUS authentication.
Answer: A

12. 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. 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 Web site. The firewall policy on ISA1 is configured as shown in

the exhibit. (Click the Exhibit button.) You need to ensure that ISA1 can connect to the virus update Web site and the Windows Update Web site. What should you do?

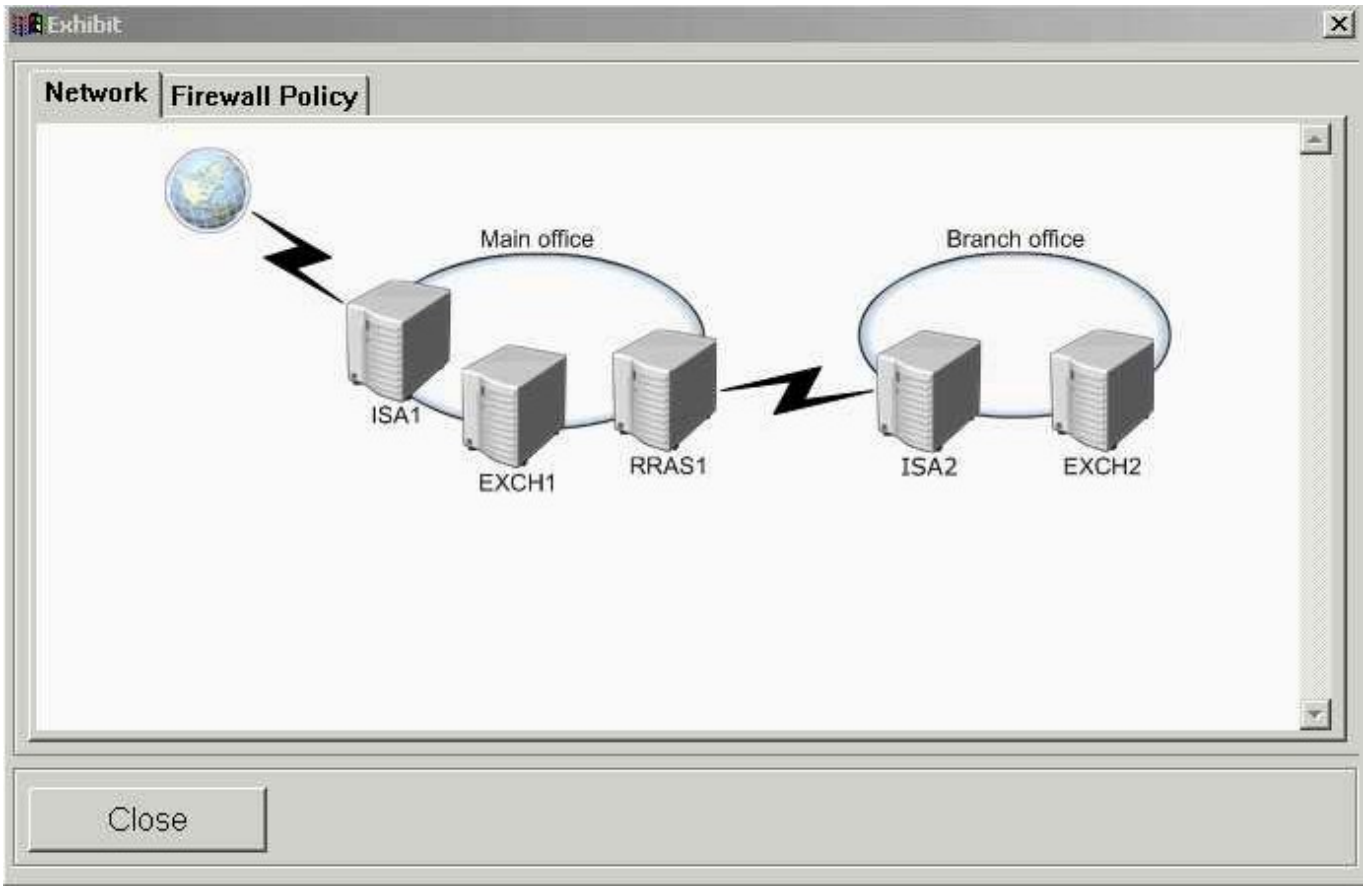


A. Enable the HTTP connectivity verifiers configuration group. On ISA1, create a network set that has the IP addresses of both the virus update Web site and the Windows Update Web site.

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 13. You are the network administrator for Contoso, Ltd. The relevant portion of the network is configured as shown in the Network exhibit. (Click the Exhibit button.) The 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. (Click the Exhibit button.) You configure the dial-on-demand failure alert on ISA2 to send an e-mail alert to the securityadmin@contoso.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

14. 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 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:*.south.contoso.com*.north.contoso.com*.east.contoso.com*.west.contoso.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?

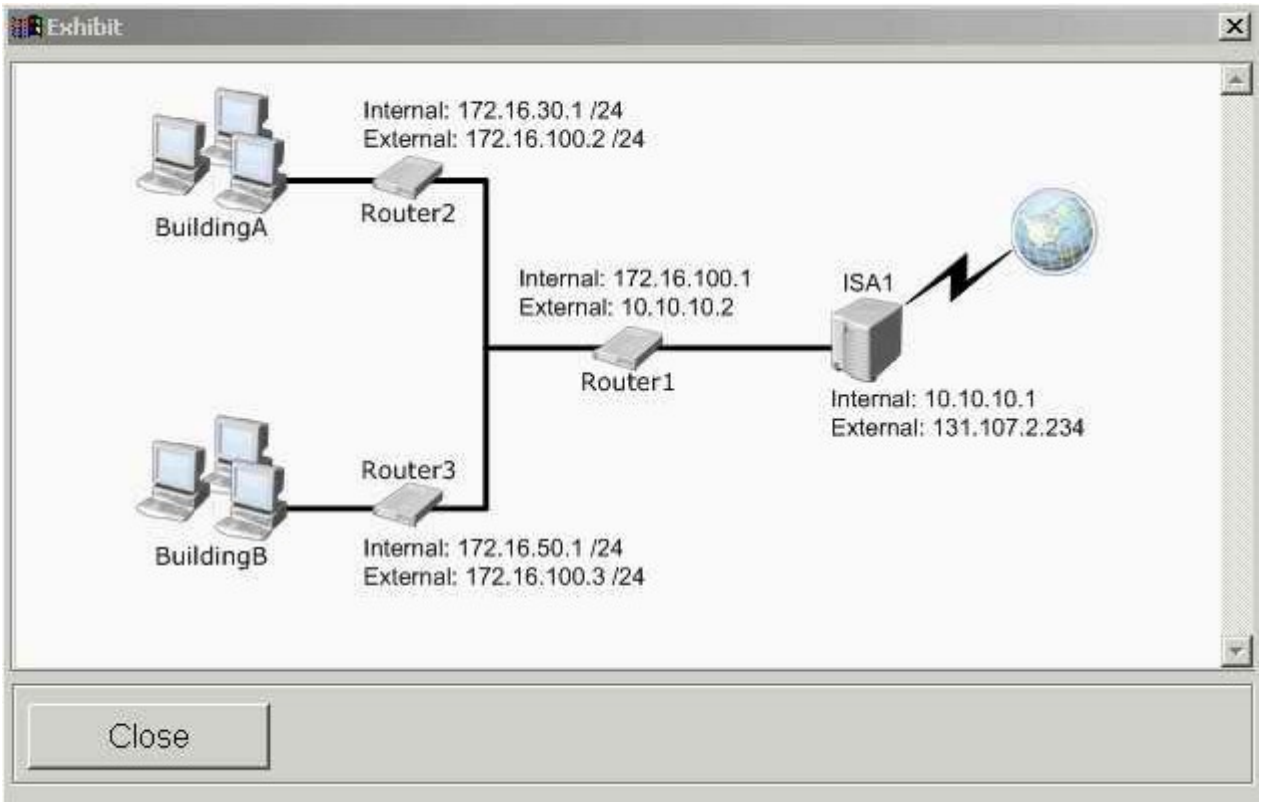
A. Create and configure HTTP, HTTPS, RDP, POP3, and SMTP access rules on ISA1.

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.contoso.com and app2.contoso.com to the list of domain names available on the Internal network on ISA1.
Answer: D

15. 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. (Click the Exhibit button.) 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 BuildingA with a default gateway IP address of 172.16.100.1.

B. Configure client computers in BuildingB with a default gateway IP address of 172.16.50.1.

C. Configure client computers in BuildingA with a default gateway IP address of 10.10.10.1.

D. Configure client computers in BuildingB with a default gateway IP address of 172.16.100.1.

E. Configure client computers in BuildingA 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: BE

16. You are the network administrator for your company. 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

17. You are the network administrator for your company. The network consists of a single Active Directory domain. All client computers run either Windows 2000 Professional or Windows XP Professional. All client computers are members of the domain. Users on the network use an IP-based client/server application on a server named Server1 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 Server1. 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 Server1. You need to configure client computers on the network to allow the application on Server1 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

18. You are the network administrator for your company. The network contains a single ISA Server 2004 computer, which is named ISA1. ISA1 provides access to the Internet for computers on the Internal network, which consists of a single subnet. The companys 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. 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?

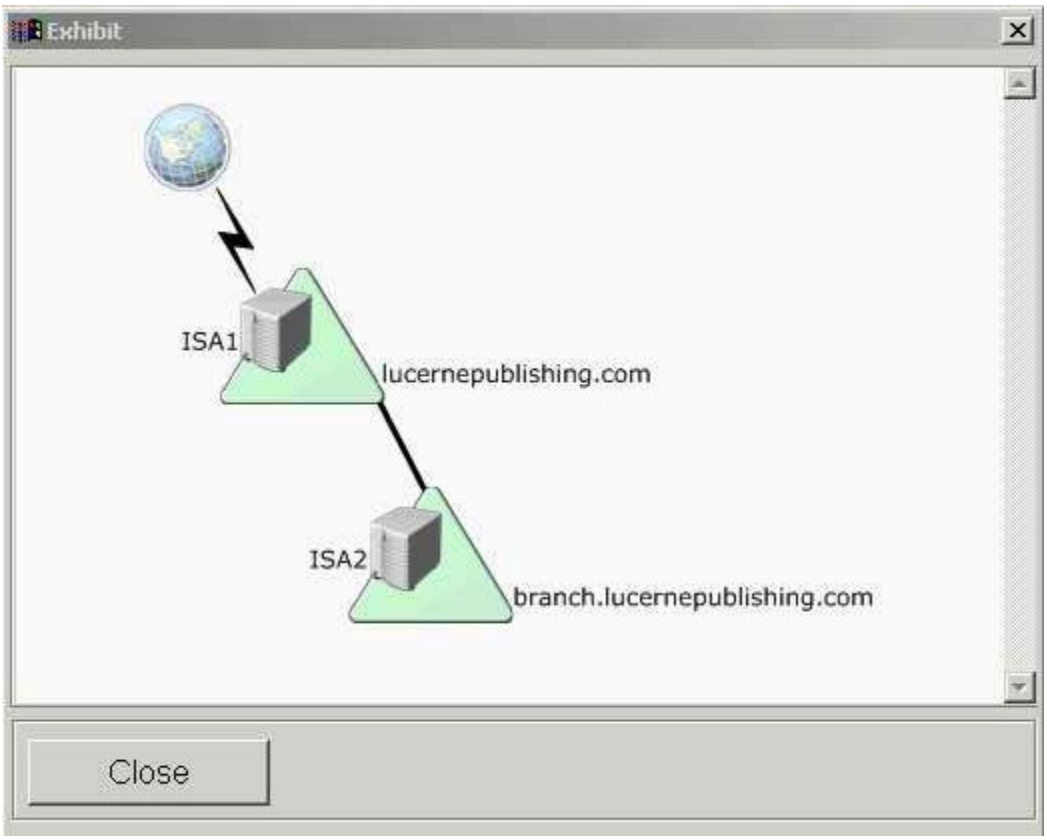
A. Configure the marketing computers with the IP address of a DNS server that can resolve external names to IP addresses.

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

19. You are the network administrator for Lucerne Publishing. The company has a main office and one branch office. 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. (Click the Exhibit button.) 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 *.lucernepublishing.com domain.

B. Configure the client computers as Web Proxy clients of ISA2. Configure the Web browser to include the *.branch.lucernepublishing.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.lucerncepublishing.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.lucerncepublishing.com domain.
Answer: BC

20. You are the network administrator for your company. 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 Server1. Server1 is configured as a SecureNAT client. A Web application runs on Server1 that communicates with an external Web site named www.contoso.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 Server1. You verify that users can access external Web sites. However, you discover that the Web application cannot access www.contoso.com. You need to allow the Web application to use anonymous credentials when it communicates with www.contoso.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 Server1, configure Web Proxy clients to bypass the proxy server for the IP address of the server that hosts www.contoso.com.

B. On ISA1, add the fully qualified domain name (FQDN) www.contoso.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