



TestKingonline.com

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

70-351

Congratulations!

You have purchased a TestKingonline. 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@Testkingonline.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 the administrator of an ISA Server 2006 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: A

Question: 2

You are the administrator of an ISA Server 2006 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

Question: 3

Your network contains an ISA Server 2006 computer named ISA1. The IP address bound to the external network adapter of ISA1 is 192.168.100.141. You run the netstat Cna command on ISA1. The relevant portion of the output is shown in the following table.

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 need to be able to quickly verify whether ISA1 is allowing traffic to 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: 4

Your network contains an ISA Server 2006 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\Split IO/sec

Answer: A, E

Question: 5

Your network contains an ISA Server 2006 computer named ISA1. ISA1 provides Internet access for all users on the 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 Web sites 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: D

Question: 6

You are the administrator of an ISA Server 2006 computer named ISA1. ISA1 is configured to publish two Web sites named www.fabrikam.com and www.contoso.com. Both Web sites are located on a Windows Server 2003 computer named Server1. The IP address of Server1 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.contoso.com/info virtual directories point to a common file share. The default log view does not allow you to easily distinguish between requests for www.fabrikam.com/info and requests for www.contoso.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.contoso.com/info and the www.fabrikam.com/info virtual subdirectories. What should you do?

- A. 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.
- B. 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.
- C. 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.
- D. 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 Contoso. In the log viewer, add a column to display the destination host name.

Answer: B

Question: 7

You install ISA Server 2006 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

Question: 8

Your network contains an ISA Server 2006 computer named ISA1. ISA1 is configured to provide forward Web caching for users on the Internal 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: 9

Your network contains an ISA Server 2006 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.

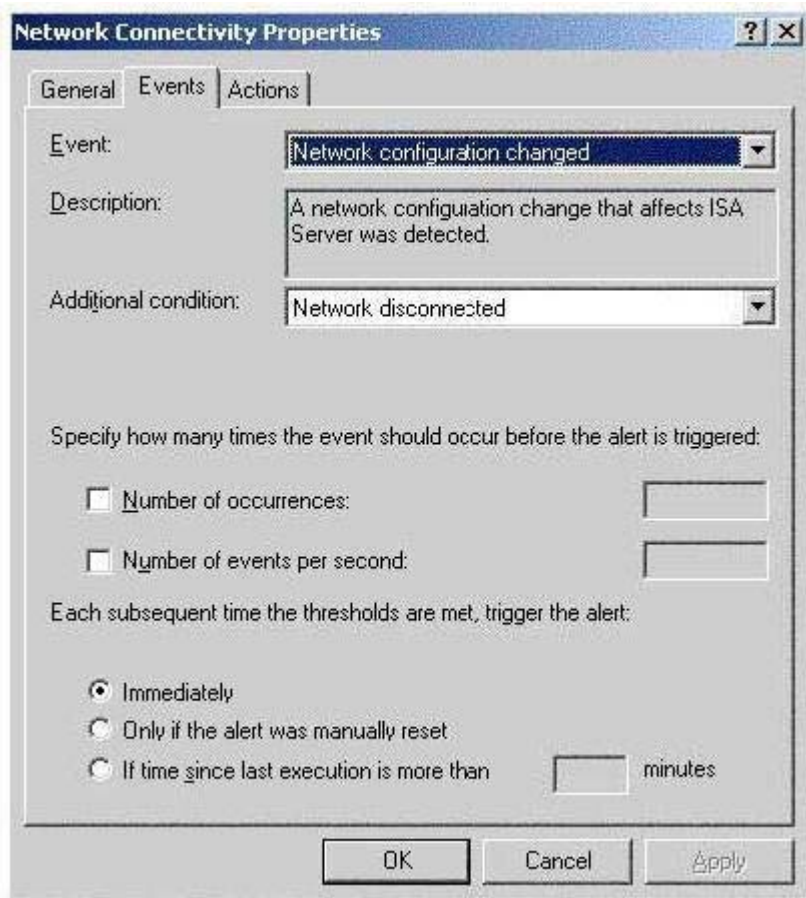
Remote VPN users report that they cannot authenticate to gain access to the network. Internal network users report that they cannot connect to the Internet. You need to configure ISA2 to allow incoming and outgoing access for company users. What should you do?

- 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: 10

Your network contains an ISA Server 2006 computer named ISA1, which runs Windows Server 2003. ISA1 has three network adapters. Each adapter is connected to one of the following: Internal network, perimeter network, and Internet. All administrative hosts exist in the Internal network. You create a file named C:\Alerts\NetworkAlert.cmd. The NetworkAlert.cmd uses net.exe to send the following message to all administrative computers: Problem with network connectivity on ISA1. 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.



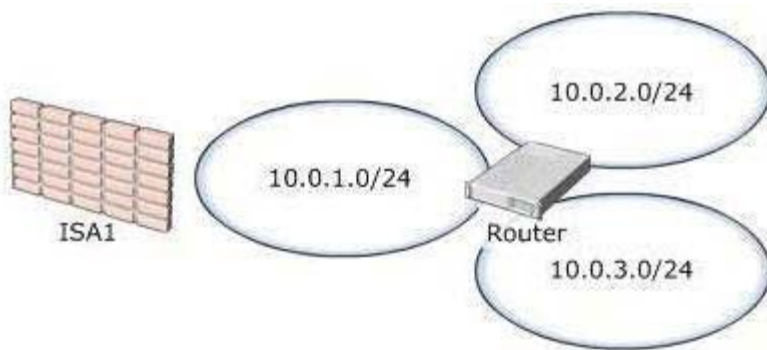
You test the Network Connectivity alert by disabling the ISA1 network adapter that is connected to the perimeter network. You see the corresponding alert in both the Alerts view and the application log of Event Viewer. However, the message is not received on any of the administrative computers. You need 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 the perimeter network adapter 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: A

Question: 11

Your network contains an ISA Server 2006 computer named ISA1. The relevant portion of the network is configured as shown in the exhibit.



When you installed ISA Server 2006 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: 12

The network contains an ISA Server 2006 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 2006 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 2006 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: 13

Your network consists of a single Active Directory domain. The network contains an ISA Server 2006 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: 14

Your network contains an ISA Server 2006 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 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: 15

Your network contains an ISA Server 2006 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:

DNS
WINS
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: 16

Your 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 2006 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: 17

Your company has a main office and is adding a branch office. The main office and the new branch each have an ISA Server 2006 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: 18

Your network contains an ISA Server 2006 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: 19

Your network contains an ISA Server 2006 computer named ISA1 operating in a Workgroup. 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 LDAPS protocols from the Local Host network to the Internal network.
- D. Join ISA1 to the domain.

Answer: A, D

Question: 20

Your network contains an ISA Server 2006 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: 21

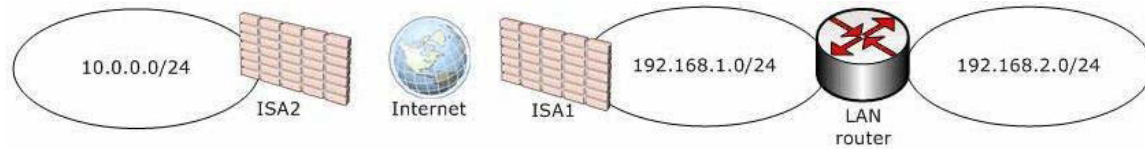
Your network contains an ISA Server 2006 computer named ISA1, which allows outgoing connections to the Internet. A network rule defines a network address translation (NAT) relationship between the Internal network and the Internet. Users on ISA Server protected networks require access to PPTP and L2TP 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: 22

Your 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 2006 computer named ISA1. The branch office has an ISA Server 2006 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: 23

Your network contains a single ISA Server 2006 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: 24

Your network contains an ISA Server 2006 computer named ISA1. The company uses Microsoft Exchange Server 2003 as its e-mail server. The company's written security policy states that all user names and passwords must be encrypted when they are sent over the Internet. The 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 the 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 HTTPS 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 IMAP4 server publishing rule. Configure the rule to point to an Exchange Server 2003 computer.

Answer: B Question: 25

ISA Server 2006 is installed as your companys firewall. All of the companys portable computers run Microsoft Outlook 2003. The companys 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 an internal server. Configure an HTTPS 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: 26

Your network contains an ISA Server 2006 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 Server1. You need to perform remote administration of Server1 from the External network by using Remote Desktop. You also need to allow users to establish a Remote Desktop connection to Server1 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 for Server1 that uses RDP-x.
- D. Create a server publishing rule for Server1 that uses RDP-x.

Answer: A, D

Question: 27

Your network contains an ISA Server 2006 computer named ISA1. The company deploys a new secure Web site. The Web site hosts an application named App1. App1 must record the client IP source address in the App1 logs 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 rules 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: 28

Your network contains a single ISA Server 2006 computer named ISA1. The companys 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 the companys 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: 29

Your network contains a single ISA Server 2006 computer named ISA1. The companys 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 companys 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 Link Translation.

Answer: D

Question: 30

Your network contains an ISA Server 2006 computer named ISA1. The companys 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

Question: 31

Your network contains two ISA Server 2006 Enterprise Edition computers named ISA1 and ISA2. ISA1 and ISA2 are configured as members of an ISA Server 2006 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: 32

Your network contains a single ISA Server 2006 computer, which is named ISA1. ISA1 provides access to the Internet for computers on the Internal network, which consists of a single subnet. The 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

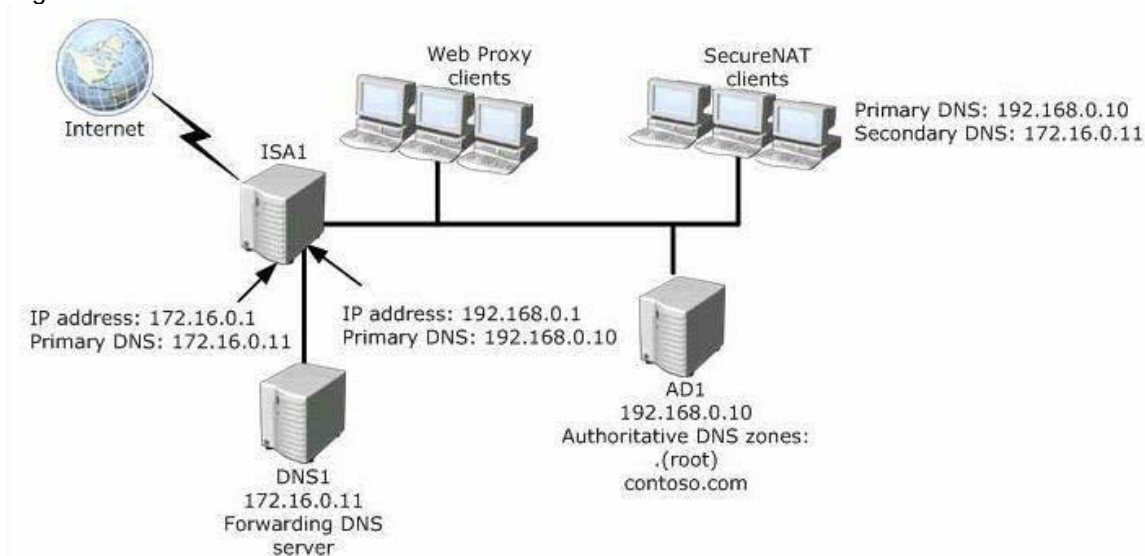
The marketing department users configure Microsoft Outlook to connect to the external mail server. They report that they receive error messages when they attempt to read or send e-mail from the external mail server. You examine the ISA1 logs and discover that ISA1 denies POP3 and SMTP connections from 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: 33

Your network contains an ISA Server 2006 computer named ISA1, 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 ISA1, replace the DNS server publishing rule with an equivalent access rule.
- B. On ISA1, change the NAT relationship between the perimeter network and the Internal network to a route relationship.
- C. On AD1, delete the .(root) zone and then disable recursion.
- D. On DNS1, remove the forwarding configuration and add a .(root) zone.

Answer: C

Question: 34

Your 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 2006 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 2006 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

Question: 35

Your network consists of a single Active Directory domain. The network contains an ISA Server 2006 computer named ISA1. Client computers on the network consist of Windows XP Professional computers, UNIX workstations, and Macintosh portable computers. All client computers are domain members. 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: 36

Your network contains a single ISA Server 2006 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

Question: 37

Your network contains an ISA Server 2006 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 2006 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: 38

Your network contains a single ISA Server 2006 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 Server1. 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.

Employees must be allowed access to only Server1, three file servers, and an internal Web server named Web1. Employees must have installed all current software updates and antivirus software before connecting to any internal resources. Partners must be allowed access to only Server1. You must not install any software other than the App1 client on any partner computers.

You need to plan the VPN configuration for the company. What should you do?

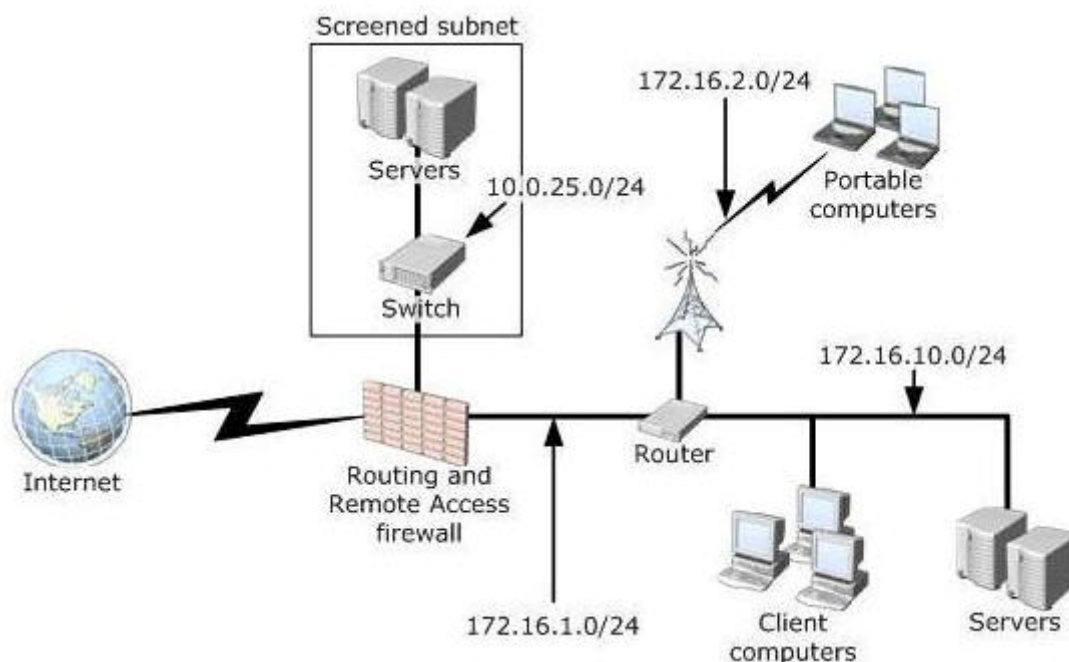
- A. Configure ISA1 to accept incoming VPN connections from partners and employees. Enable Quarantine Control on ISA1. Configure Quarantine Control to disconnect users after a short period of time. Use access rules to allow access to only the permitted resources.
- B. Configure ISA1 to accept incoming 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 2006 computer named ISA2. Configure ISA1 to accept VPN connections from employees. Do not enable Quarantine Control on 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: 39

Your network is configured as shown in the exhibit.



You are upgrading the Routing and Remote Access servers to ISA Server 2006. You need to configure the Internal network. Which three IP address ranges should you include? (Each correct answer presents part of the solution. Choose three.)

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

Answer: B, C, D

Question: 40

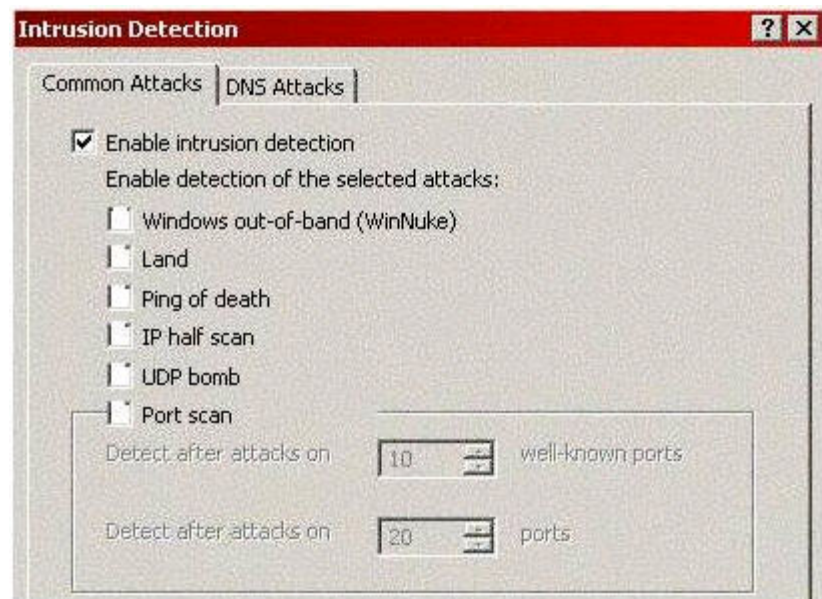
You network contains an ISA Server 2006 computer named ISA1. You use Network Monitor to capture and analyze inbound traffic from the Internet to ISA1. You notice a high volume of TCP traffic that is sent in quick succession to random TCP ports on ISA1. The flag settings of the traffic are shown in the following example.

TCP: Flags = 0x00:..... TCP: ..0.....=No urgent data TCP:

...0.....=Acknowledgement field not significant TCP:0....=No Push function TCP:
.....0...=No Reset 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 experiences 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:

