Exam : 070-350

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

Ver : 03.21.07

QUESTION 1
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed three ISA Server 2004 computers to the domain which will be used by the client computers for Internet access. You have received instruction from the CIO to plan the implementation to ensure that the client computers view all three servers as one.
You are additionally required to ensure that the load on ISA Server 2004 is distributed among the three ISA Server 2004 computers.
What should you do?

A. The Windows Server 2003 computer should be configured as a Network Load Balancing (NLB) cluster
B. The Windows Server 2003 computer should be configured as a three-node Active/Passive cluster
C. All the Windows Server 2003 computers should be configured as stand-alone servers
D. All the Windows Server 2003 computers should be configured with the same IP address

Answer: A

Explanation: In the scenario the host record should be configured with the virtual IP address to the external interface of the NLB cluster. Since NLB is used as a cluster technique which is used to allow two or more servers to share the processing load it should be used in the scenario.
Incorrect Answers:
B:
The configuration made with a three-node Active/Passive cluster should not be considered in the scenario because it will not help in any way.
C: The stand-alone server configuration should not be considered in the scenario because the server that is not a member of the domain will provide access to all resources that are available in it.
D: The configuration should not be used at all in the scenario as you will be responsible for have creating IP address conflicts on the network.

QUESTION 2
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Microsoft Windows NT 4.0 with Microsoft Proxy 2.0 Winsock Proxy client installed and the other computers run Windows XP Professional and all have the ISA Server 2000 Firewall Client installed.
The Certkiller .com network contains an ISA Server 2004 server named

Certkiller -SR01 which is used for Internet access. You have received instruction from the CIO to configure all client computers to use encryption while communicating wit h Certkiller -SR01.
What should you do (Choose three)

A. ISA Server 2004 must be configured to enable Require all users to authenticate setting
B. The Firewall client settings should be configured on ISA Serve r2004 to enable the Allow non-encrypted Firewall client connections setting
C. The ISA Server 2000 Firewall Client software should be upgraded on the Windows XP Professional computers to ISA Server 2004 Firewall Client
D. The Winsock Proxy client should be uninstalled from the client computers running Microsoft Windows NT 4.0 and install the ISA Server 2004 Firewall Client
E. An in-place upgrade should be performed on Certkiller -SR01 by using the ISA Server 2004 Migration Tool

Answer: C, D, E

Explanation: In the scenario you should perform an in-place upgrade and uninstall the Winsock Proxy client from the computers and install the ISA Server 2004 Firewall Client software on both workstation computers NT 4.0 and XP Professional as ISA Server 2000 does not have encryption.
Incorrect Answers:
A: The setting should not be configured in the scenario because the settings are used for Web proxy clients and the ISA server will prompt for user credentials.
B: This setting should not be considered in the scenario as you are required to provide encryption and the Firewall Client in question should not be configured this way.

QUESTION 3
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed 4 Microsoft ISA 2004 server computers that are to be used for connecting to the Internet. You decided to configure the ISA server computers as a Network Load Balancing cluster.
You have received instruction from the CIO to allow the client computers to connect to the NLB cluster by using DNS and to load balance the network traffic to the ISA server computers across the NLB cluster. You firstly create a host (A) resource record for the NLB cluster and need to decide what to do next.
What should you do?

A. DNS round-robin should be used to map the cluster's FQDN to the IP addresses of each network adapter of the NLB cluster nodes
B. The host record must be configured with the IP address assigned to one of the external interfaces of the NLB cluster nodes
C. The host record must be configured with the IP address assigned to one of the internal

interfaces of the NLB cluster nodes
D. The host record must be configured with the virtual IP address of the NLB cluster

Answer: D

Explanation:
In the scenario the host record should be configured with the virtual IP address to the external interface of the NLB cluster. Since NLB is used as a cluster technique which is used to allow two or more servers to share the processing load it should be used in the scenario.
Incorrect Answers:
A: DNS round-robin should not be used in the scenario because the NLB clusters FQDN should be mapped to the cluster's virtual IP address.
B, C: The host record should not be configured with the IP Address assigned to the internal or external NLB cluster interfaces because the internal IP address is used for internal communication and the second interface is not configured with a unique IP address.

QUESTION 4
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA Server 2004 computer to the domain named Certkiller -SR01 which will be used by the client computers for Internet access.
You have received instruction from the CIO to secure Certkiller -SR01 before it starts providing Internet access to client computers on the network an you need to know how to configure security for the ISA Server 2004 computer.
What should you do? (Choose two)

A. All users should be granted Deny access to this computer from the network right
B. The Allow log on locally right should be granted only to the Administrators group
C. The Allow log on locally right should be granted only to the Authenticated Users group
D. The Remote Access Connection Manager service should be disabled on Certkiller -SR01

Answer: A, B

Explanation:
In the scenario you should grant only the Administrators group the Allow log on locally right and the Deny access to this computer from the network must be assigned to all users as this will ensure that users in the administrative group has the rights to manage monitor and configure the ISA server.
Incorrect Answers:

C, D: The Allow log on locally right should not be assigned in the scenario because the authenticated users group contains all the users in the domain who are authenticated allowing every authenticated user to access or log on locally to the ISA server.

QUESTION 5
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA Server 2004 computer to the domain which will be used by the client computers for Internet access. The Firewall client installation share will be placed on the ISA Server 2004 computer and the clients will connect to the ISA Server 2004 and install the firewall client software from the share and are required to know which service to enable to allow client computers to connect to ISA Server 2004 and install Firewall Client software from the share.
What should you do?

A. Enable the Windows Installer service
B. Enable the Workstation service
C. Enable the Net Logon service
D. Enable the Server service

Answer: D

Explanation: The Server service should be enabled in the scenario because the service is used to connect to the ISA 2004 Server and install Firewall Client software from the Firewall Client Installation share on the network.
Incorrect Answers:
A:
The Windows Installer service should not be enabled in the scenario because the service adds, modifies and removes applications provided as .msi packages
B: The Workstation service should not be enabled in the scenario because the service creates and maintains client network connections to remote servers.
C: Net Logon should not be enabled in the scenario because the service maintains a secure channel between the client computer and the domain controller to authenticate users and services.

QUESTION 6
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains an ISA Server 2004 computer named Certkiller -SR01 configured with the external and internal network adapters IP addresses of 100.100.10.2 and 192.168.100.2 respectively.

During the course of the day you discover that Certkiller -SR01 is unable to receive SMTP traffic from the Internet. You are required to query a single TCP port to verify if Certkiller -SR01 is listening on TCP port 25 or not.
What should you do?

A. The portqry n 100.100.10.2p tcp e 25 command should be run on Certkiller -SR01
B. The portqry n 100.100.10.2 p tcp r 25 command should be run on Certkiller -SR01
C. The netstat a p tcp command should be run on Certkiller -SR01
D. The netstat a p tcp command should be run on Certkiller -SR01

Answer: A

Explanation: In the scenario the best option is to run the portqry n 100.100.10.2 p tcp e 25 command on Certkiller -SR01 as this command is capable of querying a single port to check if the server is listening on that particular port in the scenario.
Incorrect Answers:
B: This command should not be used in the scenario because you want to scan a single port and the command is used to scan a range of ports.
C: This command should not be used in the scenario because the command is used to display all the connections and listening ports for TCP.
D: This command should not be considered for the scenario because the command is used to display all the addresses and port numbers in a numerical form for TCP.

QUESTION 7
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch office in Miami.
The Certkiller .com main office has an ISA 2004 Server named Certkiller -SR01. You are about to deploy a second ISA Server 2004 computer in the branch office named Certkiller -SR02 which will be used to provide Internet access for branch users. You perform the following:
1. You export the ISA Server configuration settings of Certkiller -SR01 to a file named Certkiller -SR01Config.xml by using the ISA Server 2004 Migration Tool.
2. On Certkiller -SR02 you install ISA Server 2004 and import the Certkiller -SR01Config.xml file on Certkiller -SR02.
3. Certkiller -SR02 was configured with a valid IP address for the external network adapter.
4. Certkiller -SR02 was configured with a valid IP address range for the internal network of the branch office.
5. The client computers in the branch office must be configured as Web Proxy clients of Certkiller -SR02.
You have received instruction from the CIO to redirect the Web requests from the branch office to Certkiller -SR01.
What should you do?

A. A Firewall chaining rule must be configured on Certkiller -SR02 to redirect Web requests to Certkiller -SR01
B. The branch office users should be configured as Firewall clients of Certkiller -SR02
C. Automatic discovery should be enabled on Certkiller -SR02
D. A Web chaining rule should be configured on Certkiller -SR02 to redirect Web requests to Certkiller -SR01

Answer: D

Explanation: In the scenario you should consider configuring a Web chaining rule on Certkiller -SR02 to redirect requests to Certkiller -SR01. Web chaining is used to allow the client computer to route their web requests to a single location.
Incorrect Answers:
A: Firewall chaining should not be considered in the scenario because firewall chaining forwards requests from SecureNAT and firewall clients to an upstream ISA server.
B: The usage of firewall clients should not be considered in the scenario as firewall clients would require additional software to access the ISA Server 2004 computers.
C: This should not be configured in the scenario because the setting will enable the clients to automatically receive their proxy configuration at startup.

QUESTION 8
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch office in Dallas.
The Certkiller .com network contains an ISA Server 2004 computer named Certkiller -SR01 which is configured with access rules to allow Internet access to the main office users who are all configured as Firewall Clients of Certkiller -SR01. During the business week you decide to deploy a new ISA Server 2004 computer named Certkiller -SR02 to the branch office.
You later run the ISA Server 2004 Migration Tool on Certkiller -SR01 and export configuration settings to a file named Certkiller -SR01Config.xml. You finished installing ISA Server 2004 on Certkiller -SR02 and are about to import the configuration settings. You configure Certkiller -SR02 with a valid IP address for the external network adapter. You configure branch office users as Firewall Clients of Certkiller -SR02 and configure a Firewall chaining rule on Certkiller -SR02 to forward requests from clients in the branch office to Certkiller -SR01
Recently the branch office users started reporting they are unable to connect to the Internet. You must ensure that the branch office client computers can connect to the Internet.
What should you do?

A. Certkiller -SR02 must be configured to include a valid IP address range for the internal network of the branch office.

B. A Web chaining rule must be configured on Certkiller -SR02 to forward requests from branch office computers to Certkiller -SR01.
C. On Certkiller -SR02 you must configure automatic discovery.
D. The branch client computers must be configured as Web Proxy clients of Certkiller -SR02.

Answer: A

Explanation: The configuration made here should be used in the scenario because the .xml file contains the External IP address of the source and are used to specify for which ISA Server to accept requests in the scenario.
Incorrect Answers:
B: Web chaining should not be considered for this scenario as it is used to allow the client computer to route their web requests to a single location.
C: This should not be configured in the scenario because the setting will enable the clients to automatically receive their proxy configuration at startup.
D: This should not be configured in the scenario because the client that has a Web Proxy application will not be of much use in the scenario.

QUESTION 9
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA Server 2004 computer to the domain named Certkiller -SR01 which will be used by the client computers for Internet access. Later during the day you install two new ISA Servers named Certkiller -SR02 and Certkiller -SR03 and perform the actions below:
1. You export the USA Server 2004 configuration settings from Certkiller -SR01 to two separate Certkiller -SR01Config.xml files for the new servers
2. You edit each of the Certkiller -SR01Config.xml files to include a valid IP address for the external network adapter an d the internal network address range served by the new ISA Servers
You have received instruction from the CIO to perform the unattended installation on the new ISA Server 2004 computers.
What should you do?

A. A file named C:\ Certkiller \Msisaund.ini on the new ISA servers and edit the file to include the following lines:
IMPORT_ISA_CONFIG = 1
FILEPATH = Certkiller -SR01Config.xml
Then run an unattended setup on the new ISA server using the Msisaund.ini file
B. A file named C:\ Certkiller \Msisaunattended.ini must be created on both new ISA servers and edit the file to include the IMPORT_CONFIG = Certkiller -SR01Config.xml property then run the unattended setup on the new ISA servers

C. A file named C:\ Certkiller \Unattended.txt must be created on the new ISA servers and edit the file and include the (IMPORT_CONFIG_FILE = Certkiller -SR01Config.xml property and run an unattended setup on the new ISA servers using the file
D. On both the new ISA servers a file named C:\ Certkiller \Msisaund.ini should be created and edited to include the IMPORT_CONFIG_FILE = Certkiller -SR01Config.xml property and run the unattended setup on the new ISA servers using the file

Answer: D

Explanation: In the scenario you would be correct in doing so because creating a separate .xml file for the same configuration and edit the files to include both the internal network range and a valid IP address of the external network adapter.
Incorrect Answers:
A, B, C: This configuration should not be made in the scenario because you are not allowed to use the Msisaunattended.ini file to perform an unattended installation. You may not use the unattended.txt file to perform an unattended installation of Microsoft ISA Server 2004.

QUESTION 10
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch office in Miami.
The Certkiller .com network headquarters contains an ISA Server 2004 server named Certkiller -SR01 configured with rules to allow Internet access for Chicago users who are all configured as Firewall Clients of Certkiller -SR01. The Certkiller .com network recently deployed an ISA Server 2004 computer named Certkiller -SR01 to the branch office. You run the ISA Server 2004 Migration Tool to export the configuration settings of Certkiller -SR01 to a file named Certkiller -SR01Config.xml
You install ISA Server 2004 and import the Certkiller -SR01Config.xml file on Certkiller -SR02 and configure Certkiller -SR02 with a valid IP address for the external network adapter and configure the client computers as Firewall Clients of Certkiller -SR02. You are in the process of configuring a Firewall chaining rule on Certkiller -SR02 to forward all requests from the branch office to Certkiller -SR01. After this move the branch office users complain about the inability to connect to the Internet. You must ensure the branch office users can connect to the Internet.
What should you do?

A. Certkiller -SR02 should be configured to include a valid IP address range for the internal network of the branch office.
B. A Web chaining rule must be configured on Certkiller -SR02 to forward request from branch office clients to Certkiller -SR01.
C. The branch office clients should be configured as Web Proxy clients of

Certkiller -SR02.
D. On Certkiller -SR02 you must enable automatic discovery.

Answer: A

Explanation: You must configure Certkiller -SR02 to include a valid range for the internal network of the branch office and additionally you should edit the .xml file properly in the scenario.
Incorrect Answers:
B: Web chaining should not be considered for this scenario as it is used to allow the client computer to route their web requests to a single location.
C: This should not be configured in the scenario because the client that has a Web Proxy application will not be of much use in the scenario.
D: This should not be configured in the scenario because the setting will enable the clients to automatically receive their proxy configuration at startup.

QUESTION 11
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA Server 2004 computer to the domain named Certkiller -SR01 which has the Firewall Client installation placed on a share. All of the network clients are configured as Firewall clients of Certkiller -SR01. During the course of the day you distribute the CKMS_FWC.msi file to all clients using Group Policy.
A network user named Rory Allen from a partner of Certkiller .com has been hired to work on a project and will require connecting to Certkiller -SR01 from the external network. You decide to grant the necessary rights to connect to the internal network through a Virtual Private Network (VPN) connection. Rory Allen attempts to connect to the Firewall Client installation share but is unable to do so. You are required to ensure Rory Allen is able to connect to the Firewall Client share and install the software.
What should you do?

A. The default gateway on Rory Allen's computer should be configured with the IP address of the external network adapter of Certkiller -SR01.
B. Rory Allen must be granted the Access this computer from the network user right.
C. A computer set must be created on Certkiller -SR01 and include Rory Allen's client computer in the set.
D. The client computer of Rory Allen should be added to the list of trusted computers on Certkiller -SR01.

Answer: D

Explanation: By default the network clients of the internal network are capable of

accessing the share, the external network users must first be added to the list of trusted computers on the ISA Server 2004 computer Certkiller -SR01.
Incorrect Answers:
A: This should not be configured in the scenario because the gateway is used to define to which IP address of the next hop to which data is sent.
B: This should not be considered in the scenario because the computer will be allowed access to computers on the internal network.
C: There is no need for a set to be created in the scenario because the set is used to hold IP addresses of computers who have rules defined and the set is used to define to who the rules should be applied.

QUESTION 12
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA Server 2004 computer to the domain named Certkiller -SR01 which has the Firewall Client software located in a share on the server. The network client computers were all configured as SecureNAT clients on Certkiller -SR01 and the users of the Finance department require access to the Internet whilst maintaining the highest level of security.
The Finance client computers are located in an OU named FinanceOU which has no administrative rights on their client computers. You decide to install the Firewall Client software on the client computers of the Finance department and are required to ensure the Firewall Client is installed on the Finance computers using the least amount of administrative effort.
What should you do?

A. The users of the Finance department should be added to the Authenticated Users group on their computers and use Group Policy to assign the MS_FWC.msi file to the FinanceOU.
B. The users of the Finance department should be added to the local Administrators group on their computers and configure the permissions on the \\ Certkiller -SR01\MspcInt share to allow the authenticated Users group to connect to the share and install the Firewall Client.
C. The Finance department users should be asked to perform an unattended installation of the Firewall Client.
D. Group Policy must be used to assign the MS_FWC.msi file to the FinanceOU.

Answer: D

Explanation: In the scenario you should consider making use of Group Policy because Group Policy is used to allow the logged-on user the capability run and install the software as required in the scenario SecureNAT.
Incorrect Answers:
A: The users should not be added to the local administrators group as there will be too

much administrative effort involved in the scenario.
B: You should not make this configuration in the scenario because then users of all departments will be able to install the software as users who successfully logged on are added to the Authenticated Users group.
C: You should not consider this move as the users will require being members of the local administrators group on the client computer.

QUESTION 13
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently installed an ISA Server 2004 computer to the domain named Certkiller -SR01 to increase the network security and all client computers are configured as Firewall Clients of Certkiller -SR01. The network users use an IP-based client/server application to store product data and the users require accessing the Internet through this application to update information about the latest products.
What should you do?

A. An Application.ini file must be configured on the client computer used for the Internet updates.
B. A Management.ini file should be configured on the client computer used for the Internet updates.
C. A Wspcfg.ini file must be configured on the client computer used for the Internet updates.
D. A Common.ini file must be configured on the client computer used for the Internet updates.

Answer: A

Explanation: In the scenario your best option would be to configure the client computer used for the Internet updates with an Application.ini file because the file will specify configuration settings for specific applications.
Incorrect Answers:
B: This file should not be considered for use in the scenario because the file is used to specify Firewall Client Management configuration settings.
C: There is no need for the Wspcfg.ini file to be configured in the scenario because the file allows you to add specific client configuration information.
D: This file should not be considered for use in the scenario because the file specifies common settings for all applications.

QUESTION 14
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client

computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA Server 2004 computer and two routers to the domain which will be used to provide Internet access for the Finance and Research departments whose client's computers will access the Internet as SecureNAT clients after the server is deployed. The network is in the 172.20.50.0/24 subnet range
During the course of the day you examine the client computers and discover that the client computers are configured with incorrect TCP/IP configuration.
What should you do? (Choose two)

A. The client computers of the Finance department should be configured with a default gateway IP address of 172.50.20.6.
B. The client computers of the Research department should be configured with a default gateway IP address of 172.10.50.1.
C. The client computers of the Finance department should be configured with a default gateway IP address of 192.168.10.5.
D. The client computers of the Finance department should be configured with a default gateway IP address of 192.168.10.6.

Answer: A, B

Explanation: In the scenario you should keep in mind that SecureNAT are the easiest clients to configure because the only settings you have to configure in the scenario would be network settings.
Incorrect Answers:
C, D: The other default gateway addresses should not be used in the scenario because they will not allow the two departments Internet access.

QUESTION 15
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains an ISA Server 2004 computer named Certkiller -SR01. Certkiller .com has recently partnered with a company named Partner.com. You install a second ISA Server 2004 computer named Certkiller -SR02 to the Partner.com network which is connected to the headquarters through a WAN connection and all the network clients have Firewall clients installed and a few use Web Proxy clients.
You are required to ensure that the load on Certkiller -SR02 is minimal by preventing Web Proxy clients from looping back through the firewall to access the internal network resources while connecting to servers using a single label name or computer name.
What should you do?

A. The list of domain names available on the internal network must be configured on

Certkiller -SR02 to include the branch domain.
B. The list of computer addresses or domain names should be configured on Certkiller -SR02 for Direct Access.
C. The Directly access computers specified in the Domain tab option must be selected on Certkiller -SR02.
D. The Bypass proxy server in this network option should be selected on Certkiller -SR02.

Answer: D

Explanation: In the scenario it seems that the best choice of configuration is for you to make use of the Bypass proxy for Web server in this network option as this will stop the loop back of the proxy server in the scenario.
Incorrect Answers:
A: This will have no affect on the network and should not be used unless you also select the Directly access computers specified in the Domain tab option.
B: This should not be done in the scenario because this configuration affects both the Web proxy and Firewall Clients.
C: This should not be selected in the scenario because you will allow Firewall client computers to bypass the Web proxy configuration while connecting to host.

QUESTION 16
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch office in Miami.
The Certkiller .com network recently deployed three ISA Server 2004 computers to the domain named Certkiller -SR01, Certkiller -SR02 and Certkiller -SR03. Certkiller -SR01 is located at the Chicago office and Certkiller -SR02 and Certkiller -SR03 are located at the branch office that uses Linux computers.
You later configure an access rule on Certkiller -SR01 that allows authenticated users to download files from an external FTP server using the FTP protocol. You want to install Firewall Client on the Chicago office computers. Both offices network user's report they are unable to download files from the external FTP servers using the FTP protocol. The branch office users now require the ability to upload files to the external FTP servers. You must ensure both offices are able to download files and that branch office users ca upload files.
What should you do?

A. The Firewall Client settings on Certkiller SR02 and Certkiller -SR03 must be configured to enable the Allow non-encrypted Firewall client connections setting
B. Half the clients of Certkiller -SR02 must e configured as Firewall clients and the other half of Certkiller -SR03 clients must be configured as Web Proxy clients
C. The client computers if Certkiller -SR02 and Certkiller -SR03 must be configured as Web Proxy clients

D. Half the client computers of Certkiller -SR02 must be configured as Firewall clients and the other half of the Certkiller -SR03 clients must be configured as SecureNAT clients

Answer: D

Explanation: You will be correct in the scenario if you made the configurations suggested in the option because SecureNAT clients support application filters and can download files from and upload file to the FTP external server.
Incorrect Answers:
A: This option should not be used in the scenario as the users will still be unable to download or uploads files to the external FTP server.
B: There should be no Web proxy clients in the scenario as they can only download and the users are required to be able to upload as well.
C: This should not be done as the Firewall Client software is not compatible with Macintosh computers like Linux.

QUESTION 17
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network has its headquarters in Chicago and branch office in Dallas.
The Certkiller .com main office has an ISA Server 2004 computer named Certkiller -SR01. You are in the process of deploying an ISA server to the branch office named Certkiller -SR02. Certkiller -SR02 is configured to forward Web requests to Certkiller -SR01 and the branch clients are configured as Firewall clients of Certkiller -SR02. The Certkiller .com network requires that you configure the client computers in the branch to directly access the Web servers in the main office. You select Directly access computers specified in the Domain tab option on Certkiller -SR02.
What else should you do?

A. The list of domain names available on the internal network on Certkiller -SR02 must be configured to include the Certkiller .com domain.
B. The client computers in the branch office must be configured as SecureNAT clients of Certkiller -SR02.
C. The CNAME resource record should be created for the internal Web servers on the branch DNS server.
D. The Use default URL option must be enabled on Certkiller -SR02.

Answer: A

Explanation: In the scenario the proper thing to do is enabling the Directly access computers specified in the Domains tab option as Firewall Clients do not use the ISA server while connecting to domains listed on the Domains tab.

Incorrect Answers:
B: This should not be done as the scenario objective will not be reached because SecureNAT routes requests to the ISA server.
C: This should not be considered in the scenario because it can not be used to help directly connect to the Web servers.
D: The settings defined in the option can not be used to help you achieve the desired scenario objective.

QUESTION 18
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 with all the client computers configured as Firewall clients. Certkiller -SR01 hosts a Web application named CK_Webapp which is configured to use port 80 on Certkiller -SR01. The Certkiller .com network users will use the application to exchange confidential information but the users require the application to use port 443. You are required to configure the Web application to use port 443.
What should you do?

A. An Application.ini file must be configured on the client computers and include the LocalBindTcpPorts=443 entry in the Application.ini file.
B. An Application.ini file must be configured on the client computers and include the RemoteBindTcpPorts=443 entry in the Application.ini file.
C. On the Application Settings tab in the Define Firewall Client Settings dialog box on Certkiller -SR01 the value of the LocalBindTcpPorts entry must be set to 443.
D. On the Application Settings tab in the Define Firewall Client Settings dialog box on Certkiller -SR01 the value of the RemoteBindTcpPorts entry must be set to 443.

Answer: A

Explanation: In the scenario we should consider using the Application.ini file because the file specifies configuration settings for specific applications and the settings defined in the Application.ini file always takes precedence over the configured settings at the server level.
Incorrect Answers:
B: This configuration should not be used in the scenario because the application must be configured on the local machine not the remote server.
C: This setting should not be set in the scenario because by configuring these settings they will become a server-level configuration which will be applied to all Firewall clients.
D: This entry should not be configured in the scenario because the entry here is used to specify the port that will be used by the application on the remote server not the local machine.

QUESTION 19
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA Server 2004 computer to the domain named Certkiller -SR01 which has three network adapters that are connected to the Internet the perimeter network and the internal network. The Certkiller .com network also has two DNS servers named Certkiller -SR02 and Certkiller -SR03 located on the internal network.
The Certkiller .com network client computers are configured as Firewall clients of Certkiller -SR01. The perimeter network users recently started complaining about the inability to connect to the Internet whilst internal network users report no such problems and can connect to the Internet. You must decide what to do in order to enable all client computers the ability to access the Internet.
What should you do?

A. The interface address of Certkiller -SR01 that is connected to the perimeter network must be included in the Perimeter Network list of addresses.
B. The client computers in the perimeter network must be configured as Web Proxy clients of Certkiller -SR01.
C. The .root zone must be deleted and disabled on Certkiller -SR03.
D. The .root zone must be deleted and disabled on Certkiller -SR02.

Answer: A

Explanation: In the scenario you should know that a perimeter network is a network that is used to permit external users to use specific servers that are located on the perimeter network to prevent access to an internal corporate network.
Incorrect Answers:
B: This will not be off much help in the scenario and should not be used unless you include the interface address of Certkiller -SR01 that is connected to the perimeter network in the list of addresses for the perimeter network.
C, D: This should not be done in the scenario because by additionally disabling recursion on either of the DNS servers is not recommended. The recursion is used to enable a DNS server to perform recursive queries for the DNS clients and servers for which the queries were made too.

QUESTION 20
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network consists of an ISA Server 2004 computer that is configured as an Edge Firewall.
The Certkiller .com network Graphics department has Macintosh computers

configured as SecureNAT clients of the ISA 2004 server and the Finance department has Firewall clients. Both the Finance and Graphics departments require NNTP access to the external network. You decide to create a rule allowing NNTP for the All Authenticated Users. Now the Graphics department users report they are unable to access newsgroups through NNTP. The Finance department users do not report any problems connecting to newsgroups. You need to ensure that both departments are able to access newsgroups using NNTP.
What should you do?

A. An Access rule should be created to allow NNTP for the All Users user set and remove the access rule for the All Authenticated Users user set.
B. The Authenticated access rule must be modified to include the users of the graphics department.
C. A route relationship between the internal and the external network must be created.
D. All the users must be configured as SecureNAT clients.

Answer: A

Explanation: The best option in the scenario is creating the access rule and configuring the rule properly and remember that the All Authenticated Users user set includes all the users who are authenticated using any type of authentication and SecureNAT clients are not authenticated until they connect through VPN.
Incorrect Answers:
B: This will not allow you to achieve the scenario objective and should not be used instead you should create an access rule.
C: This should not be done in the scenario because when you are using an Edge Firewall a network rule that specifies a route relationship between the internal network and VPN clients are already applied.
D: This should not be considered in the scenario because this will nor allow you to achieve the scenario objective and the All Authenticated Users user ser does not include non-VPN SecureNAT clients.

QUESTION 21
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network contains an ISA Server 2004 computer named Certkiller -SR01.
The network users of the Finance and Research departments of Certkiller .com sometimes work remotely and require access to the internal network resources from outside the network. You just completed configuring Certkiller -SR01 as a remote VPN server and both PPTP and L2Tp/IPSec are selected on the VPN Clients Properties dialog box.
The Certkiller .com remote client s can either use PPTP or L2TP/IPSec to connect to Certkiller -SR01 and all network clients are configured as both Web Proxy and Firewall clients of Certkiller -SR01. You are additionally required to create an

access rule enabling remote users to access the internal resources using a VPN connection you are in the process of configuring an Access Policy and require help. What should you do?

A. The Access rule should be modified to allow the connections from VPN Clients to the internal network to select PPTP as the outbound protocol.
B. The VPN Clients properties should be checked and uncheck the Enable PPTP option.
C. The VPN Clients properties should be checked and uncheck the Enable L2TP/IPSec option.
D. The access rule should be modified to allow access to the users of the Research department.

Answer: D

Explanation: In the scenario you should consider modifying the access rule for the Research department as access rules are used to configure the traffic passing through the ISA Server and includes all the traffic from the internal network to the Internet and back to internal network.
Incorrect Answers:
A: In the scenario you should not consider this option instead the users of the Research department should be added to the User Sets page enabling them access to the internal resources.
B: You should not check this checkbox in the scenario because this option will not allow the Research users to connect to the Internet
C: You should not check this checkbox in the scenario because this option will not allow the users to access the internal resources remotely.

QUESTION 22
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server and two routers to the network to provide Internet access to the client computers who will access the Internet as Secure NAT clients after the deployment. The network users are supposed to run IP addresses in the range 172.10.50.0/24. During maintenance you discover that none of the client computers are configured with the proper IP addresses. You are required to allow the client computers in the two departments access to the Internet
What should you do? (Choose two)

A. The client computers in the Finance department must be configured with a default gateway of 192.168.10.0.
B. The client computers in the Research department must be configured with a default gateway of 192.168.20.20.
C. The client computers in the Research department must be configured with a default

gateway of 172.20.50.6.
D. The client computers in the Finance department must be configured with a default gateway of 172.10.50.1.

Answer: C, D

Explanation: In the scenario you should keep in mind that SecureNAT are the easiest clients to configure because the only settings you have to configure in the scenario would be network settings.
Incorrect Answers:
A, B: The other default gateway addresses should not be used in the scenario because they will not allow the two departments Internet access.

QUESTION 23
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network recently deployed an ISA Server 2004 computer named Certkiller -SR01 to ensure security.
The Certkiller .com network client computers are configured as Web Proxy clients. You enabled IP routing so that you can use the Ping diagnostics utility to check connectivity. You ping the external resources from the Web Proxy clients to validate connectivity. CertK ig.com network also has corporate users who work in the office and have separate user's accounts created in the Vendors group for these users. The Group Policy states that vendors have limited access to corporate resources and access to all the servers is encrypted by using IPSec. In order for the vendors group to access and download their mail from their corporate mail servers you create a access rule for POP3 and SMTP on Certkiller -SR01
For network security you configured the external vendors working from the office to have no additional protocols other than POP3 and SMTP. You configure the vendors as Firewall clients of Certkiller -SR01 and enable the Outlook option in the Firewall Client settings dialog box to enable the vendors to access and download mail. You just performed the operation and the vendors immediately start complaining that they are unable to download mail using POP3 and SMTP. You are required to choose what to do next.
What should you do?

A. Deselect the Allow non-encrypted Firewall client connections checkbox on Certkiller -SR01 in the Firewall Client Settings dialog box
B. The services setting must be configured and enabled in the Firewall Client Settings dialog box on Certkiller -SR01
C. The Vendor group on Certkiller -SR01 must be allowed to access the HTTP and HTTPS protocols
D. In the IP Preferences dialog box IP routing should be disabled

Answer: D

Explanation: In the scenario you should consider having the IP routing disabled because when you disable IP routing the ISA server will send only the data and not the original network packet to the destination.
Incorrect Answers:
A: This should not be configured in the scenario because there are no down-level Windows clients in the scenario.
B: You should not consider this configuration in the scenario because it is not used to configure Outlook and wont help.
C: The scenario clearly stipulates that the Vendors group should not have any other protocols except SMTP and POP3.

QUESTION 24
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network recently deployed an ISA Server 2004 computer to increase security.
The Certkiller .com network clients are all configured as Secure NAT clients and are able to browse Web sites but report they are unable to connect to FTP sites. You are required to ensure that the client computers are able to access the Internet for HTTP, HTTPS and FTP access by using the ISA server.
What should you do?

A. The FTP Access application filter should be enabled
B. The internal network adapter should be configured with a blank default gateway
C. The Link Translation Webb filter should be enabled
D. A static route should be created

Answer: A

Explanation: In the scenario you should consider enabling the filter because FTP uses port 20 for connection and port 12 for data transfer which is not understood by SecureNAT making use of this option will enable the SecureNAT clients to access FTP HTTP and HTTPS sites.
Incorrect Answers:
B: This should not be done in the scenario because the users will not be enabled to access the FTP HTTP and HTTPS sites.
C: This should not be considered in the scenario as it can not be used to enable FTP access to the Internet.
D: There is no need for this configuration as it will not ensure the users are able to access FTP HTTPS and HTTP sites.

QUESTION 25
You work as the network administrator at Certkiller .com. The Certkiller .com

network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network consists of an ISA Server 2004 computer named Certkiller -SR01 configured as a remote access VPN and is configured to accept PPTP remote connections.
You plan to configure Certkiller -SR01 to use only L2TP/IPSec connections from remote clients to increase network security. You decide to create a new Connection Manager profile by using Connection Manager Administration Kit (CMAK) and distribute the kit to the remote users. The Certkiller .com remote users were disconnected from Certkiller -SR01 while trying to connect to the internal network. You are required to ensure that remote users can connect to the internal network.
What should you do?

A. A computer certificate should be issued to the VPN client computers.
B. The ISA firewall must be configured to support pre-shared keys.
C. IP routing should be disabled.
D. The Block IP fragments option should be disabled.

Answer: D

Explanation: In the scenario when Block IP fragments option is enabled the L2TP/IPSec connection is not established properly because of packet fragmentation.
Incorrect Answers:
A: This should not be considered in the scenario because the certificate provided will not stop the problem of packet fragmentation in the scenario.
B, C: This option should not be tried in the scenario because the option can not be used to help allow remote users to connect to internal resources.

QUESTION 26
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network contains an ISA Server 2004 computer configured as an Edge Firewall.
The Certkiller .com network client computers are configured as Firewall clients. You implement a firewall policy used to allow access to the clients using HTTP, HTTPS an FTP protocols whilst other network access is blocked as required by company policy. You recently finished deploying the ISA server when the Firewall clients computers report they are unable to download information from FTP server but can upload information, you diagnose and discover the problem is not page specific and need to know what to do to enable the clients to download and upload FTP information.
What should you do?

A. The route relationship between the internal and external networks must be modified.

B. The Firewall policy must be modified to allow access to all protocols.
C. All the client computers should be configured as Web Proxy clients.
D. The FTP policy must be configured to disabled the Read Only option.

Answer: D

Explanation: In the scenario the best option would be to modify the policy thereby ensuring that you enable the network clients the ability to download and upload files to FTP sites.
Incorrect Answers:
A: This should not be done in the scenario because when you are using an Edge Firewall a network rule that specifies a route relationship between the internal network and VPN clients are already applied.
B: There is no requirement for additional protocols in the scenario because the given protocols in the scenario are enough for the users to download and upload FTP files.
C: This configuration should not be made in the scenario because the Web Proxy client can only download files but are unable to upload.

QUESTION 27
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows 200 Professional or Windows XP Professional. The Certkiller .com network contains an ISA Server 2004 computer named Certkiller -SR01.
Certain members of Certkiller .com will work remotely and require access to the internal network resources. You configure Certkiller -SR01 as a VPN server to provide authentication and authorization to VPN clients. You configured Certkiller -SR01 to make use of a RADIUS server named Certkiller -SR02. You configure Certkiller -SR01 to use L2TP connections using pre-shared keys. You decide to enable the use of a custom IPSec security policy on Certkiller -SR01 and configure a pre-shared in the VPN properties. You use the CMAK kit and create a Connection Manager profile and distribute the pre-shared key within the Connection Manager profile to CPN clients.
You recently during the business day tested the VPN connectivity fro the clients by using the Connection Manager profile. You find you are able to connect to the internal network from the VPN clients. You later discover during routine maintenance that there are a lot of UDP requests on the internal adapter of Certkiller -SR01 to secure this you block the UDP traffic to the ISA server's internal network adapter. After you made these changes the external remote users report they are unable to access the VPN server.
What should you do?

A. A new Connection Manager profile should be configured using the CMAK kit to use certificates in stead of pre-shared keys and instruct the VPN users to use the new Connection Manager profile

B. A new Connection Manager profile should be configured to use pre-shared keys with certificates and instruct the VPN users to use the new Connection Manager profile
C. On the internal network adapter of Certkiller -SR01 you must enable UDP ports 1512, 1513, 1445 and 1446
D. On the internal network adapter of Certkiller -SR01 you must enable UDP ports 1812. 1813, 1645 and 1646

Answer: D

Explanation: In the scenario you should enable the UDP ports 1812, 1812, 1645 and 1646 ensuring that the ISA server can communicate with the RADIUS server which means the users will be authenticated.
Incorrect Answers:
A, C: This should not be considered for use in the scenario as it will not improve scenario conditions and the wrong ports are used in the scenario.
B: The pre-shared key should not be used with certificates in the scenario because the additional digital certificates will not allow clients to access the VPN server.

QUESTION 28
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 with the external adapter configured with a single IP address.
You recently enabled the caching feature of Certkiller -SR01. The Certkiller .com network users Finance department will be working out of the office and require access to an Exchange 2003 mail server named Certkiller -SR02 who is available on the internal network.
The remote users will use MS Outlook 2003 from within the internal network and the VPN clients will also use MS Outlook 2003. The Domain Administrators group is the only group enabled for VPN-client access. The Certkiller .com network policy stipulates that mail access to external users should only be browser based. You decide to create a protocol definition for the outbound TCP port 80 to allow mail access via Outlook Web Access for the Senior Management group. You later create an access rule using the protocol definition which is applied to the Finance and Senior Management group. You verified the connections are working. The remote network users start complaining that they are unexpectedly logged off while accessing the internal mail server by using Outlook Web Access from a public computer.
What should you do?

A. OWA forms-based authentication must be configured in the Authentication dialog box of the Web listener.
B. The bridging mode must be configured an select the Secure connection to clients and mail server option.

C. The Web listener must be configured to select the
Log off OWA when the user leaves OWA option.
D. A cache rule should be created to prevent the caching of Outlook Web Access objects.

Answer: D

Explanation: In the scenario the best option is to create a cache rule to prevent the Outlook Web Access objects because when you enable the caching feature of ISA Server all of the Outlook Web Access objects will be cached if you do not configure the ISA server to use forms-based authentication.
Incorrect Answers:
A, C: The Web listener should not be configured with this option because you cannot configure OWA forms-based authentication as you cannot have a mutually exclusive authentication method using a single IP address. You should not even configure OWA forms-based authentication either.
B: This mode should not be considered on the scenario because this creates a Web Publishing Rule ensuring a secure SSL connection from the client to the OWA Web site.

QUESTION 29
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 to enhance network security and a DNS server named Certkiller -SR02. You decided to enhance network security more by selecting the Enable IP Options filtering, Block IP fragments and Enable IP routing options in the IP Preferences dialog box on Certkiller -SR01. The Certkiller .com management decided to deploy a streaming server named Certkiller -SR03 on the internal network which will host multimedia files that will be accessed by the users of the Finance department both inside and outside the Certkiller .com network.
You were later instructed to publish the streaming server on Certkiller -R01. You ensure that there is enough bandwidth for optimal streaming of multimedia files. You check the performance of the connection by allowing access to the files to a limited set of external users who are able to connect to the streamed files but they report the connection to the streaming server is erratic and terminates while playing the multimedia files. You are required to ensure the multimedia files are optimized and persistent.
What should you do?

A. A DNS server should be installed on Certkiller -SR01 and instruct the external clients to use the new DNS server for name resolution.
B. The .root zone should be deleted and then disable recursion on Certkiller -SR02.
C. IP routing should be disabled on Certkiller -SR01.
D. IP fragment blocking should be disabled on Certkiller -SR01.

Answer: D

Explanation: In the scenario we should consider disabling the block IP fragments option because when this option is enabled one IP datagram is separated into multiple small datagrams or IP fragments which all will be dropped when the ISA server filters packet fragments.
Incorrect Answers:
A: This should not be done in the scenario because the users can already access the multimedia files using the first DNS server Certkiller -SR02.
B: This zone should not be considered for deletion because the zone is important and is created by default in Windows Server 2003 and is used for recursive queries.
C: This should definitely not be considered in the scenario because IP routing allows the original packets to be forwarded to their destinations.

QUESTION 30
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network contains an ISA Server 2004 computer configured as an Edge Firewall and a DNS server on the internal network.
The ISA server will be responsible for controlling Web access to client computers in the domain. The Certkiller .com network recently acquired a new project that requires any form of data transfer including OS-related error reporting should be prevented from being transmitted to external sites because the data may contain information related to the work environment of the project. You configure the network clients as Firewall clients of the ISA server a dare required to ensure that OS-related error reporting data is not transmitted.
What should you do?

A. The communication to the Microsoft configuration group should be disabled.
B. The HTTP Connectivity verifiers configuration group should be disabled.
C. The Remote Logging (NetBIOS) configuration group should be disabled.
D. The ICMP configuration group should be disabled.

Answer: A

Explanation: In the scenario the best option would be for you to have the Communication to the Microsoft configuration group disabled as this group is used to define the method which ISA 2004 uses to interact with network resources.
Incorrect Answers:
B: This configuration setting in question should not be changed in the scenario as the group allows the Local Host network to use HTTP or HTTPS protocols to access computers on any network.
C: This should not be considered for disabling in the scenario as it will not prevent the OS-related error reporting to Microsoft.

D: The use of ICMP should not be disabled in the scenario because the policy rule allows access to the Diagnostic Services ICMP configuration group and the ISA server uses ICMP group to access all networks.

QUESTION 31
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network has headquarters in Chicago and a branch office in Miami connected to the main office through a WAN connection.
The Certkiller .com network has recently installed an ISA server to the main office named Certkiller -SR01 and an ISA server in the branch office named Certkiller -SR02. The Certkiller .com management plan to remotely perform all ISA administrative tasks for Certkiller -SR02 from the main office. You require access to non-ISA services like DNS to configure the firewall. You firstly export the current system policy to ensure you are able to perform all administrative tasks for Certkiller -SR02 from Certkiller -SR01.
What should you do?

A. The Microsoft Management Console configuration group on Certkiller -SR02 should be enabled.
B. The Windows Networking configuration group on Certkiller -SR02 should be enabled.
C. The Allowed Sites configuration group on Certkiller -SR02 should be enabled.
D. The Terminal Server configuration group on Certkiller -SR02 should be enabled.

Answer: D

Explanation: In the scenario the best choice of configuration is enabling the Terminal Server configuration group in the scenario as the group is the best option to achieve the scenario objective.
Incorrect Answers:
A: The Microsoft Management Console configuration group should not be enabled in the scenario because the group is used to remotely administer ISA Server 2004 through MMC.
B: This option should not be enabled in the scenario because the Windows Networking configuration group allows NetBIOS communication on the network by default.
C: There is no need to have this option enabled as it is enabled by default in ISA Server 2004.

QUESTION 32
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network recently

deployed an IS Server 2004 computer named Certkiller -SR01 to enhance network security.
A new Certkiller .com security policy states that access to certain Web sites must be restricted. You create URL sets for the restricted Web sites and rules to deny access to the sites in Certkiller -SR01. The Certkiller .com network recently expanded and acquired a new branch office and the number of subnets in the branch office will vary on the regional requirement and expansion plans.
You decide to implement two new ISA Server 2004 computers in the branch office to secure the network. You configured the network configuration on the new ISA servers. You need to know how to configure access rules for the new ISA server to block the restricted sites.
What should you do?

A. The System Policy rules on Certkiller -SR01 should be exported to Certkiller -SR01.xml using the Export System Policy task and import the Certkiller -SR01.xml file to the new ISA servers.
B. All the network objects in the Toolbox tab in Certkiller -SR01 should be exported to Certkiller -SR01.xml and imported on the new ISA servers.
C. The complete configuration settings on Certkiller -SR01 should be exported to Certkiller -SR01.xml and imported to the new ISA servers.
D. The URL sets network objects on Certkiller -SR01 should be exported to Certkiller -SR01.xml and imported to the new ISA servers.

Answer: D

Explanation: In the scenario the best configuration choice would be to export the file to an .xml file because the configuration in the .xml file can be used to either backup for your configuration or to copy the settings to the new ISA servers.
Incorrect Answers:
A: This should not be considered in the scenario because the Network objects are used as source and destination elements in access rules specifying the type of traffic allowed between networks.
B, C: There is no need to make this export in the scenario because the scenario states the number of subnets varies and the branch office has different settings.

QUESTION 33
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed two ISA Server 2004 computers named Certkiller -SR01 to enhance network security. You recently configured a number of scheduled content download jobs on Certkiller -SR01 and requests to have Certkiller -SR01 have increased. You plan to implement two new ISA 2004 Servers named Certkiller -SR02 and Certkiller -SR03.
The Firewall policies of Certkiller -SR02 and Certkiller -SR03 will be configured

the same as Certkiller -SR01. You later export the Firewall policy settings to a file named SR01firepolicy.xml and import the file to the new servers respectively. After the configuration network clients of Certkiller -SR02 and Certkiller -SR03 report they are experiencing slow access and download from the Internet. You are required to optimize Internet access for the new ISA servers.
What should you do?

A. The Export confidential information (encryption will be used) option should be selected during the export of the Firewall policy settings to SR01firepolicy.xml and import the file to the new ISA servers.
B. All the network objects in the Toolbox tab should be exported on Certkiller -SR01 to SR01firepolicy and import the file to the new ISA servers.
C. The Web Listeners network object should be exported from Certkiller -SR01 to SR01firepolicy.xml and import the file to the new ISA servers.
D. The System Policy rules on Certkiller -SR01 should be exported using the Export System Policy task and import the System Policy rules on the new ISA servers.

Answer: D

Explanation: In the scenario the best option to have the new ISA servers configured is to export the System Policy rules because if you simply exporter the Firewall policy the System Policy rules are not included and the rules are important.
Incorrect Answers:
A: This option should not be used in the scenario as it is meant for sending user passwords pre-shared keys for IPSec and more.
B: This should not be done in the scenario because the ISA 2004 Server does not allow selecting all network objects in a single step.
C: This option should not be used in the scenario because it will not optimize network performance.

QUESTION 34
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network recently deployed an IS Server 2004 computer named Certkiller -SR01 to enhance network security.
The Certkiller .com network recently expanded and acquired a new branch office whose network computers run Linux and some UNIX variants. You decide to install an additional ISA server named Certkiller -SR02 to the branch office to secure access to the Internet and the Certkiller .com security policy states all requests to Internet must pass through Certkiller -SR01.
What should you do?

A. Firewall chaining should be configured on Certkiller -SR02 and configure Certkiller -SR02 to forward client requests to Certkiller -SR01.

B. A demand-dial VPN connection to the main office should be created and configure Certkiller -SR02 to use the VPN connection as a default gateway and configure a firewall chaining user account.
C. On Certkiller -SR01 you must configure firewall chaining and configure Certkiller -SR01 to get client requests from Certkiller -SR02.
D.
On Certkiller -SR01 you must configure Web chaining and configure Certkiller -SR02 as the downstream proxy server.

Answer: A

Explanation: In the scenario the best configuration choice of option would be to configure firewall chaining because firewall chaining is used to route requests from client computers in the branch office to the ISA server in the main office.
Incorrect Answers:
B: This should not be configured in the scenario because it will send all requests made to connect to the server or resource in a remote location to the demand-dial VPN connection.
C: This configuration should not be made because Certkiller -SR02 should forward the requests to Certkiller -SR01 in the scenario.
D: This configuration should not be made in the scenario because this will allow the network clients to route Web requests through a single location.

QUESTION 35
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows 2000 Professional or Windows XP Professional. The Certkiller .com network recently deployed an IS Server 2004 computer named Certkiller -SR01 to enhance network security and all client computers are Firewall clients.
The Certkiller .com network recently expanded and acquired a new branch office whose network computers run Linux and some UNIX variants. You decide to install an additional ISA server named Certkiller -SR02to the branch office to secure access to the Internet and the Certkiller.com security policy states all requests for Internet must pass through Certkiller -SR01.
What should you do?

A. Firewall chaining should be configured on Certkiller -SR02 and configure Certkiller _SR02 to forward client requests to Certkiller -SR01.
B.
A demand-dial VPN connection to the main office should be created and configure Certkiller -SR02 to use the VPN connection as a default gateway and configure a firewall chaining user account.
C. On Certkiller -SR01 you must configure firewall chaining and configure Certkiller -SR01 to get client requests from Certkiller -SR02.

D. On Certkiller -SR01 you must configure Web chaining and configure Certkiller -SR02 as the downstream proxy server.

Answer: A

Explanation: In the scenario the best configuration option would be to configure firewall chaining because firewall chaining is used to route requests from client computers in the branch office to the ISA server in the main office.
Incorrect Answers:
B: This should not be configured in the scenario because it will send all requests made to connect to the server or resource in a remote location to the demand-dial VPN connection.
C: This configuration should not be made because Certkiller -SR02 should forward the requests to Certkiller -SR01 in the scenario.
D: This configuration should not be made in the scenario because this will allow the network clients to route Web requests through a single location.

QUESTION 36
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows 2000 Professional or Windows XP Professional. The Certkiller .com network recently deployed an IS Server 2004 computer named Certkiller -SR01 to enhance network security and the network contains a DNS server named Certkiller -DC01.
The majority of Certkiller .com network employees require persistent connectivity to the Internet. You configure three more ISA servers named Certkiller -SR02, Certkiller -SR03 and Certkiller -SR04 for creating an ISA server array which configuration is shown below:
1. Certkiller -SR01 - internal IP: 192.168.1.1 - external IP: 15.15.1.1
2. Certkiller -SR02 - internal IP: 192.168.1.2 - external IP: 15.15.1.2
3. Certkiller -SR03 - internal IP: 192.168.1.3 - external IP: 15.15.1.3
4. Certkiller -SR04 - internal IP: 192.168.1.4 - external IP: 15.15.1.4
You later decided to configure Network Load Balancing (NLB) and test connectivity. You discover network clients can not connect to the Internet.
What should you do?

A. The network to be load balanced should be reconfigured as Internal and specify a virtual IP address as 192.168.1.5.
B. The network must be reconfigured to select both Internal and External.
C. The virtual IP address must be reconfigured to 15.15.1.1.
D. The virtual IP address must be reconfigured to192.168.1.5.

Answer: A

Explanation: In the scenario at hand the best option of configuration is to

reconfigure the network to load balance as Internal and specify the virtual IP address of 192.168.1.5 as the external IP address is configured to the adapter for the cluster.
Incorrect Answers:
B: This should not be considered in the scenario as you are only required to provide network load balancing to internal clients.
C: You should not configure this way as the IP address is already in use you would only be causing more network problems with conflicting IP addresses.
D: This option should not be used in the scenario as you will be unable to provide Internet access to most of the users.

QUESTION 37
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 or Windows 2000 Server and all client computers run Windows XP Professional. The Certkiller .com network also contains two domain controllers named Certkiller -DC01 and Certkiller -DC02 both configures as DNS servers.
The Certkiller .com network security policy requires forwarding of DNS requests from clients to external DNS servers. You configure Certkiller -DC02 to forward requests to Certkiller -DC01. The Certkiller .com network recently deployed an ISA server 2004 computer named Certkiller -SR01 to ensure network security and control access to the Internet.
Some of Certkiller .com network clients are configured as SecureNAT clients and the rest are Web Proxy clients. You decide to configure an access rule for the clients to access the Internet and the default gateway for the SecureNat clients is configured as 10.10.10.3 but the SecureNAT clients can not browse the Internet. You must ensure they can browse the Internet.
What should you do?

A. The preferred DNS server must be configured for the SecureNAT clients as 10.10.10.2 and a secondary DNS server as 10.10.10.1.
B. A static route should be added between the internal network and the Internet on Certkiller -SR01.
C. The default gateway should be configured for the SecureNAT clients as 15.14.21.54.
D. The root zone on Certkiller -DC01 should be deleted.

Answer: D

Explanation: In the scenario the best solution to enable forwarding of DNS is by deleting the root zone and then the DNS forwarding option is disabled disabling it to act as a forwarder.
Incorrect Answers:
A: This configuration should not be made in the scenario as you are required to forward request from Certkiller -DC02 to Certkiller -DC01.
B: The static route should not be added in the scenario because the route is used only

when multiple subnets exist and will not help in the scenario.
C: There should be no default gateway changes in the scenario because in the question it is already configured properly.

QUESTION 38
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows 2000 Professional or Windows XP Professional. The Certkiller .com network recently deployed an IS Server 2004 computer named Certkiller -SR01 to enhance network security.
The ISA server Certkiller -SR01 contains three network adapters used for the internal network, the perimeter network and the private network. After you configured Certkiller -SR01 using the 3-Leg Perimeter network template you decide to create an access rule between the internal network and the Internet and between the internal network and the perimeter network.
The Certkiller .com network additionally has a Web server that needs to be accessed by internal network users and the Internet users. You decide to create an access rule allowing HTTP traffic from the internal network to the Web server in the perimeter network. You make use of the Web Publishing Wizard to allow HTTP traffic from the External network to the Web server in the perimeter network. The users immediately start reporting they are unable to access the Internet or browse the Web server from the internal network.
What should you do?

A. The route relationship between the internal network and Perimeter network must be configured as Route and between the Perimeter network and the Internet as NAT.
B. The route relationship between the Internal and Perimeter network must be configured as Route.
C. The route relationship between Perimeter network and Internet must be configured as NAT.
D. The route relationship between internal network and Internet must be configured as Route.

Answer: A

Explanation: The correct response to the scenario would be to configure the route relationship between the required networks as done in the answer, network rules have to be defined to allow communication between network objects.
Incorrect Answers:
B, C: You should not make these configurations in the scenario because when using a 3-Leg Perimeter network template a default configuration would be applied.
D:
This should not be done in the scenario as you will not provide users from the Internet access to the Web server on the Perimeter network.

QUESTION 39
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network recently deployed two ISA Server 2004 computers named Certkiller -SR01 and Certkiller -SR02 to enhance network security. The Certkiller .com network uses two subnets 172.10.50.0/24 and 10.120.2.0/24
A new Certkiller .com network security policy states that all outbound traffic from the internal network and intranet resources be accessible using NAT. You are required to ensure that the ISA Server implementation adheres to the security policy. You must decide which interface or interfaces should be configured as the internal interface.
What should you do? (Choose two)

A. Configure the interface that has an IP address of 10.120.2.104
B. Configure the interface that has an IP address of 172.10.50.1
C. Configure the interface that has an IP address of 192.168.20.54
D. Configure the interface that has an IP address of 192.168.10.53

Answer: A, B

Explanation: The best choice in the scenario would be to use the IP addresses used in the answers as they are private IP addresses and can not be routed across the Internet and therefore you should use them.
Incorrect Answers:
C, D: The IP addresses here can be routed across the Internet and should not be considered for use in the scenario as it fails to meet the scenario objectives required.

QUESTION 40
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network recently deployed two ISA Server 2004 computers named Certkiller -SR01 and Certkiller -SR02 to enhance network security. The Certkiller .com network uses two subnets 172.10.50.0/24 and 10.120.2.0/24
A new Certkiller .com network security policy states that all outbound traffic from the internal network and intranet resources be accessible using NAT. You are required to ensure that the ISA Server implementation adheres to the security policy. You must decide which interface or interfaces should be configured as the internal interface.
What should you do? (Choose two)

A. Configure the interface that has an IP address of 10.120.2.104
B. Configure the interface that has an IP address of 172.10.50.1

C. Configure the interface that has an IP address of 192.168.1.50
D. Configure the interface that has an IP address of 192.168.1.49

Answer: A, B

Explanation: The best choice in the scenario would be to use the IP addresses used in the answers as they are private IP addresses and can not be routed across the Internet and therefore you should use them.
Incorrect Answers:
C, D: The IP addresses here can be routed across the Internet and should not be considered for use in the scenario as it fails to meet the scenario objectives required.

QUESTION 41
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network are using the 192.169.1.0/24 subnet configuration
The Certkiller .com network contains two routers named TestRouter01 and BillRouter02, TestRouter01 is used to connect various segments together and BillRouter02 is used centrally for Internet access. During the course of the week you decide to replace BillRouter02 with an ISA 2004 Server named Certkiller -SR01 to enable policy based security. After you finished installed and deployed Certkiller -SR01 with the IP address 100.200.20.20. The users of the 192.168.1.0/24 subnet segment report they are unable to connect to the Internet. You later troubleshoot and discover TrstRouter01 is configured with no gateway
What should you do?

A. The default gateway of TestRouter01 must be configured with the IP address of the internal network adapter of Certkiller -SR01
B. The default gateway of TestRouter01 must be configured with the IP address of 172.124.22.1
C. The default gateway of TestRouter01 must be configured with the IP address of 100.200.20.20
D. The default gateway of TestRouter01 must be configured with the IP address of 192.168.10.1

Answer: D

Explanation: In the scenario the TestRouter01 router was not configured with a default gateway and the IP address used in the option fits into the subnet the network is running. The default gateway provides the IP address of the next hop to which data should be sent.
Incorrect Answers:
A, B: The addresses used here should not be used in the scenario because the IP address 100.200.20.20 is the IP address of Certkiller -SR01 and the other address does not fit in

the network subnet.
C: This configuration should not be used in the scenario because the users will still be unable to access the Internet via Certkiller -SR01.

QUESTION 42
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows 2000 Professional or Windows XP Professional
The Certkiller .com network recently deployed two ISA Server 2004 computers named Certkiller -SR01 with the IP address 100.200.20.20 on the external interface to enhance network security. The Certkiller .com network also contains a router named BillRouter01 with the IP address 172.20.50.10 on the external interface and 172.60.50.20 on the internal interface.
The Certkiller .com Internal network contains a Web server hosting the Certkiller .com Web site and all clients are configured to use an internal DNS server.
You are required to ensure that all client computers are able to access the internal Web server.
What should you do?

A. The default gateway of the client computers must be configured with the IP address of the ISA server's external IP address 100.200.20.20.
B. The default gateway of the client computers must be configured with the IP address of the Billrouter02 external IP address 172.20.50.10.
C. The default gateway of the client computers must be configured with a blank IP address.
D. The default gateway of the client computers must be configured with the IP address of the 172.60.50.20.

Answer: D

Explanation: In the scenario the best option to you is configuring the computers with the internal IP address of the BillRouter01 router as the Web server is also located on the internal network this is the logical option.
Incorrect Answers:
A: The external IP address of the Certkiller -SR01 should not be used in the scenario because the users will then be unable to access Certkiller -SR01 and won't access the Web server either
B: The external IP address of the Router should not be used in the scenario because the users will then be unable to access Certkiller -SR01 and won't access the Web server either.
C: The IP address for the default gateway should not be configured as blank as the users still wont be able to access the Web server.

QUESTION 43
You work as the network administrator at Certkiller .com. The Certkiller .com

network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network is configured to use the 1923.168.0.0/24 subnet.
The Certkiller .com network recently deployed two ISA Server 2004 computers named Certkiller -SR01 to enhance network security and all client computers are configured as Firewall clients. After the deployment has been made users started complaining that they are unable to access the Internet. You later try and connect from the same subnet and are unsuccessful. You are required to ensure that the client computers can access Internet resources.
What should you do?

A. The client computers are to be reconfigured as SecureNAT clients with the default IP address of 172.60.10.2.
B. A static route should be added on Certkiller -SR01 which contains the 28.24.32.2 subnet.
C. A persistent static route should be added on Certkiller -SR01 for the 172.32.0.0/24 subnet.
D. A persistent static route should be added on Certkiller -SR01 for the 192.168.0.0/24 subnet.

Answer: D

Explanation: In the scenario you should add a persistent static route on Certkiller -SR01 for the 192.168.0.0/24 subnet as this is the subnet stated in the scenario in addition the routing table should also be configured properly in the scenario.
Incorrect Answers:
A: This configuration should not be made in the scenario as there is no need to reconfigure the client computers as SecureNAT clients.
B, C: There is no need for this static route to be added in the scenario because the scenario states the Certkiller .com network use the 192.168.0.0/24 subnet.

QUESTION 44
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed two ISA Server 2004 computers named Certkiller -SR01 to enhance network security. Users of Certkiller .com have been hired as editors who write reviews about books before they are released and require collecting information for their reviews by visiting various book Web sites which includes web sites that contain static content and dynamically changing entertainment Web sites
The Certkiller .com users often view drafts of the books which go through peer reviews and are downloaded again and again by the users. To have the speed

optimized you created a caching rule. You select the If any version of the object exists in the cache. If none exist, route the request to the server option in the content retrieval page of the New Cache Rule Wizard. You later also select the Content for Offline Browsing (302, 307 responses) option in the Cache Content page.
You then go about decreasing the Time-To-Live (TTL) for HTTP objects. You are about to validate the configuration by getting an editor feedback of access time to various entertainment sites and the editor reports no noticeable difference in access times. You are required to ensure that the content from the various sites is always available to the editors.
What should you do?

A. The Content requiring user authentication for retrieval option should be selected in the Cache Content page.
B. The Also apply these TTL boundaries to sources that specify expiration option should be selected.
C. The Only if a valid version of the object exists in the cache. If none exist, route the request to the server option in the content retrieval page should be selected.
D. The Dynamic Content option should be selected in the Cache Content page.

Answer: D

Explanation: This scenario requires you to take the action of the configurations in the answer because caching is used to store Web content in the memory of an ISA 2004 server or on the hard disk.
Incorrect Answers:
A: This option should not be used in the scenario because the option is used to cache information that may require user authentication.
B: This setting should not be considered in the scenario because the option is used to override the expiration data included with the content.
C: This option should not be used in the scenario because you would only retrieve information from the cache that has not expired.

QUESTION 45
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed one ISA Server 2004 computers named Certkiller -SR01 to enhance network security. The Certkiller .com network Finance and Sales departments frequently access the Internet to research Finance and Sales related information. The users visit various web sites and access files that are common between them. You decide to configure caching of Internet objects on Certkiller -SR01 to speed up data access for the Finance and Sales users.
You are required to ensure caching is configured for HTTP and FTP objects that contain static and dynamic content whilst ensuring that the object is retrieved from the cache if it has not expired.

What should you do?

A. A caching rule should be created which enables the Only if a valid version of the object exists in the cache. If none exist, route the request to the server option and select Dynamic content and enable HTTP and FTP caching.
B. A caching rule should be created which enables the
If any version of the object exists in the cache. If none exist, route the request to the server option and select Content for offline browsing (302, 307 responses) option and on the cache rule decrease the TTL for HTTP objects.
C. A cache rule must be created that enables the Cache objects that have an unspecified last modification time and select Dynamic content.
D. A cache rule must be created that enables the Cache objects that have an unspecified last modification time and select Dynamic content and enable HTTP and FTP caching.

Answer: A

Explanation: In the scenario you should create a rule that enables the Only if a valid version of the object exists in the cache. If none exist, route the request to the server option and select Dynamic content and enable HTTP and FTP caching because caching also reduces the bandwidth usage when a user requests Web information that is already cached.
Incorrect Answers:
B: The configuration options in this answer should not be used in the scenario because the responses indicate that the content has been temporarily relocated or the client has been temporarily redirected.
C, D: This option should not be used in the scenario because the option will take the cached items and clear them from the cache based upon the parameters defined in the cache rule.

QUESTION 46
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network contains three ISA 2004 Servers named Certkiller -SR01, Certkiller -SR02 and Certkiller -SR03 with all client computers configured as Web Proxy clients.
You later decided to configure the client computers to automatically download the configuration script and configured an array that contains the three ISA servers.
The ISA server array is configured to cache Web requests from clients on the network and define the cache drive on each ISA server to store the cached information. The Certkiller .com ISA servers are also configured to store confidential files. You are required to configure the array so the cached information is distributed between the three ISA servers whilst ensuring very few cached objects are stored on Certkiller -SR01
What should you do?

A. On the Internal network array you must enable Cache Array Routing Protocol (CARP) and configure the load factor on Certkiller -SR01.
B. A content download job must be configured on the ISA servers and on Certkiller -SR01 disable caching dynamic content.
C. On the Internal network array you must configure network load balancing (NLB) and configure the load factor on Certkiller -SR01.
D. On Certkiller -SR02 and Certkiller -SR03 the Cache Array Routing Protocol (CARP) should be enabled and configure the load factor on Certkiller -SR01.

Answer: A

Explanation: The CARP protocol should be used in the scenario because the protocol is used to enable ISA servers to provide distributed cache which are distributed by the CARP protocol used by Web Proxy clients.
Incorrect Answers:
B: This option should not be used in the scenario because a content download job downloads the content to the ISA server before network clients request that content.
C: This option should not be considered for configuration because distributed caching does not occur with NLB.
D: This option should not be considered in the scenario because no one server can have CARP enabled specifically for one server.

QUESTION 47
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed one ISA Server 2004 computers named Certkiller -SR01 to enhance network security. The users of the Certkiller .com Finance department regularly access scientific Web sites to download information and the Sales department also access Web sites frequently to download product manuals. The other network departments recently started reporting Internet access when the Finance and Sales users access the Internet.
You decide to investigate and discover that outgoing Web requests by the Sales and Finance users use a lot of bandwidth. You are required to provide faster Internet access to the affected departments by decreasing the use of bandwidth by the Sales and Finance users whilst minimizing the traffic from the internal network to the Internet.
What should you do?

A. A content download job should be configured on Certkiller -SR01.
B. The client computers must be enabled to download the automatic configuration script.
C. Active Caching should be enabled.
D. On Certkiller -SR01 reverse caching should be enabled.

Answer: A

Explanation: In the scenario you should consider scheduling a content download job in the scenario because the content download job can be used to improve the performance of caching in the scenario which is what is required of you.
Incorrect Answers:
B: The client computers should not be configured this way in the scenario because the automatic configuration script is used to automatically configure Web Proxy clients.
C: This option should not be considered in the scenario because this type of caching preempts users from accessing content from the Internet by automatically downloading the content within the cache.
D: This type of caching should not be configured in the scenario because reverse caching occurs when the Internet users request Web content located on a server on the Certkiller .com network.

QUESTION 48
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and a branch office in Miami.
The Certkiller .com network main office contains an ISA 2004 Server computer named Certkiller -SR01 and the branch office has all the client computers. Certkiller -SR01 will be responsible for providing the two offices with Internet access. The Certkiller .com company website www. Certkiller .com is published on an external Web server and the branch users need access to www. Certkiller .com regularly to get updated product information.
You later decide to increase the performance and decrease the bandwidth usage by installing a new ISA server named Certkiller -SR02 in the branch office. You configure the two ISA servers as a single array. You later configure a content download job to get contents from www. Certkiller .com and schedule it to run daily after office hours. After the configurations are made the branch users started reporting that the connection to www. Certkiller .com is very slow. You are required to ensure the branch users are able to access www. Certkiller .com quickly.
What should you do?

A. Cache Array Routing Protocol (CARP) should be enabled on Certkiller -SR02 on the local host network.
B. The array in the network must be disabled and configure the ISA servers as standalone servers.
C. In the array bidirectional affinity should be enabled.
D. The System policy rule should be disabled that allows content download.

Answer: A

Explanation: The CARP protocol should be used in the scenario because the protocol is used to enable ISA servers to provide distributed cache which are

distributed by the CARP protocol used by Web Proxy clients.
Incorrect Answers:
B: This is impossible because if the servers are not members of the domain they cannot be part of an array.
C: This should not be configured in the scenario because the configuration ensures that traffic is handled both directions by the sane array server.
D: This configuration should not be made in the scenario because you scheduled a content download job to occur and this disables the action.

QUESTION 49
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed one ISA Server 2004 computers named Certkiller -SR01 to the network. The Certkiller .com network additionally includes a perimeter network consisting of an Internet Information Server (IIS) acting as a Web server hosting the Intranet site of the organization as well as other sites like library Web sites which are used by network clients to read and download online books. You decided to create a URL set for the Intranet Web site and enable caching for this URL set using a cache rule on Certkiller -SR01.
You create a second cache rule to prevent Web designers responsible for updating the Intranet site from viewing the cached HTTP and FTP objects. The new cache rule is configured to include the URL for the Intranet site and enable the Never, no content will ever be cached setting. After you applied the rules the Web designers report lag times in viewing changes made to the Internet site. You are required to ensure that the Web designers are able to see changes made immediately.
What should you do?

A. The more specific cache rule should be reordered for the Web Designers to be processed first
B. The computer set of the Web designers should be added in a cache rule and configure the rule to prevent caching the URL set for the Intranet
C. The first rule should be deleted that enables the caching of the URL set
D. Another rule should be created to disable caching for the All Users group

Answer: A

Explanation: In the scenario you should consider reordering the cache rules because in the scenario there is more than one rule so the order in which the rules are processed is very important.
Incorrect Answers:
B: This rule should not even be considered in the scenario as you would effectively affect all the network users requesting the Intranet Web site.
C: The first rule should not be deleted in the scenario because this would affect all the users in the network.

D: There is no need for another rule to be created instead the order of the rule should be changed to specify which rule is processed first.

QUESTION 50
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed two ISA Server 2004 computers named Certkiller -SR01 and Certkiller -SR02 configured as a single array to enhance network security. The Certkiller .com network Web site is published on an internal Web server named Certkiller -SR03 and the ISA serve array is responsible for providing internal and external client's access to the company Web site.
The content of the Certkiller .com Web site is updated every night and for optimized bandwidth usage and faster access to the internal Web site you create a content download job to run every morning which download the updated Web content to the array before it is requested by internal and external clients. The Certkiller .com network clients recently started reporting that access to the internal Web site is very slow. You need to ensure that internal and external clients have quick access to the Internal Web site.
What should you do?

A. Distributed caching should be enabled using Cache Array Routing Protocol (CARP)
B. The system Policy rule must be enabled to allow content download
C. Network Load Balancing (NLB) should be enabled
D. The Web site should be published on an external Web server

Answer: A

Explanation: In the scenario you should consider using the CARP protocol as it enables an ISA server to provide caching by distributing the cache used by Web Proxy clients across the array of ISA servers in the scenario.
Incorrect Answers:
B: This option should not be used in the scenario because a content download job downloads the content to the ISA server before network clients request that content.
C: This option should not be considered for configuration because distributed caching does not occur with NLB.
D: This option should not be considered in the scenario because the option will not help you achieve the scenario objective.

QUESTION 51
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.

The Certkiller .com network recently deployed an ISA Server 2004 computer named Certkiller -SR01 to enhance network security. The Certkiller .com network users frequently access sites from customers and sales related sites which consume a lot of bandwidth. You want to optimize the bandwidth to handle client requests for other network resources. To optimize the bandwidth you create rules for the non-customer related sales Web sites and apply them to the client computers in the sales department. You increase the percent of free memory to be used for caching to speed up retrieval of cached objects.
In order to prevent sales users from getting cached information for customer Web sites you create a URL set for the customer Web sites and configure a cache rule to include the URL set for the customer Web site. The Sales department users started reporting that they are unable to get updated content for customer sites and they receive totally outdated data for the other sales related sites. You are required to ensure that the objects related to the sales sites are cached but not outdated.
What should you do?

A. The value of the TTL for the caching rule must be decreased for the cache rule pointing.
B.
The cache rule for the sales site should be deleted and in the cache rule for the customer sites include the URL set for the sales site in the Exceptions section.
C. A cache rule should be created that disables caching of HTTP content on the sales sites.
D. A cache rule should be created that disables caching of FTP content on the sales sites.

Answer: A

Explanation: In the scenario you should consider decreasing the TTL value as the value will determine when the cached contents are expired and will attempt to download updated information.
Incorrect Answers:
B: In the scenario you should not consider this option because the sites in question are not part of the original set and therefore cannot be accepted.
C, D: Making these configurations should not be considered in the scenario because you are required to cache objects related to the sales sites and this will not help you achieve the scenario objective.

QUESTION 52
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed four ISA Server 2004 computers configured as an array to enhance network security and all the client computers are configured as SecureNAT clients and Web Proxy clients. The Certkiller .com network clients require access to the Internet an you enable the Cache Array

Routing Protocol (CARP) on the array for the outgoing Web requests from the internal clients. You also create and apply a cache rule to make sure that only updated objects are returned to the client computers.
The Certkiller .com network users recently started reporting that the Internet connection is very slow. You decide to use the Performance Monitor to check caching statistics. You discover the cached content is not returned to the clients.
You are required to ensure that client computers in the internal network are able to access the cached content.
What should you do?

A. Caching should be disabled and then enabled to clear the cache.
B. Automatic discovery must be enabled and configure all client computers as Web Proxy clients.
C. The array must be configured to disable CARP.
D. The order of the caching rules should be modified.

Answer: A

Explanation: This is the best option to use in the scenario because caching can be used to reduce bandwidth usage and in the scenario you should clear the cache.
Incorrect Answers:
B: The order of the caching rules should not be modified in the scenario because cache rules are configured to define what type of content is cached on the ISA server.
C: This option should not be considered as the protocol is used to provide distributed caching.
D: This option should not be considered in the scenario because the option is used to discover the correct location to automatically download the configuration.

QUESTION 53
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows 2000 Server and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA Server 2004 computer so server as a Web caching server to enhance network security as all the network clients require Internet access. You later enable and configure caching on The ISA server but the users report access to the Internet is very slow, you check the configuration and discover the following event in the event log:
"14193, Cache was initialized with less memory cache than configured."
You are required to provide faster Internet access to the network users whilst ensuring that the event does not occur again.
What should you do?

A. The percentage of free memory should be configured to be used for caching setting.
B. The maximum size of objects in the cache should be decreased.
C. The size of the cache drive should be increased.

D. A cache drive must be configured on the ISA server.

Answer: A

Explanation: In the scenario this option seems the best choice because the ISA server caused the event to be recorded by not having enough memory allocated for caching.
Incorrect Answers:
B: This option should not be considered in the scenario as you would consume even more memory.
C: There is no need to increase the size of the cache drive because this option only defines the maximum size of the cache drive.
D: There is no need to configure a cache drive in the scenario because the option is used to define the cache drive to store cached content.

QUESTION 54
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA Server 2004 computer named Certkiller -SR01 to provide Internet access and enhance network security. The Certkiller .com Finance users recently require accessing foreign language programs from an e-learning Web site on the Internet and the modules for the programs are non-streaming audio files and the Web site contains some less frequently used video files that are more than 15 MB in size and the audio files are around 1 MB in size.
In order to provide faster access to the audio files for the Finance team you create a cache rule on Certkiller -SR01 and observe that the larger video files are cached.
You are required to prevent that heavy video files are cached and ensure that the cache drive is used optimally and caches smaller files.
What should you do?

A. The cache rule should be modified and specify the size of the objects that can be cached.
B. The memory parameters should be modified and specify the size of objects that can be cached.
C. The Max cache size (MB) option should be configured.
D. The TTL value of the bigger objects should be decreased.

Answer: A

Explanation: In the scenario your best option would seem that you should modify the cache rule in order to prevent the larger video files from being cached in the scenario.
Incorrect Answers:
B: The memory parameters should not be configured in the scenario because when

configuring a cache drive the objects are cached on the hard disk configured as the cache drive.
C: This option should not be configured in the scenario because this option is used to define the size of the cache drive that is used to store the content.
D: This value should not be decreased in the scenario as this will cause them to expire quicker and be cached more regularly.

QUESTION 55
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA Server 2004 computer named Certkiller -SR01 to enhance network security and the network also has a perimeter network where an Internet Information Server(IIS) acting as a Web server named Certkiller -SR02 resides. Certkiller -SR01 hosts the Intranet site of the company and also hosts other sites like library Web sites from where the users can download and read online books.
In order to reduce the load on Certkiller -SR01 you create a URL set for all the Web sites hosted on Certkiller -SR02 and enable caching for the sites on Certkiller -SR01 using a cache rule. You are required to ensure that Web designers responsible for updating the Intranet site can see changes to the Intranet site immediately after updating the site.
What should you do?

A. A Domain name set for the Intranet site must be created and create a cache rule to include the Domain Name set for Intranet site and enable the Never, no content will ever be cached option.
B. A computer ser for the Intranet site must be created and create a cache rule to include the computer set in Intranet site an enable the Never, no content will ever be cached option.
C. A network set for Intranet site must be created and create a cache rule to include the network set for Intranet site and enable the Never, no content will ever be cached option.
D. A URL ser for the Intranet site should be created and create a cache rule to include the URL set for Intranet site and enable the Never, no content will ever be cached option.

Answer: D

Explanation: This option should be used in the scenario because caching is used to store Web content in memory of the ISA server or on the server's hard disk. Cache rules can additionally also be used to specify how Web information is stored.
Incorrect Answers:
A: This option should not be considered in the scenario because the option defines one or more domain names as a single set enabling you to apply access rules to the specified domains

B: This option should not be used in the scenario because the option defines one or more computer to form a single set enabling you to apply access rules to the specified computers.
C: There is no need for creating a network set because the set is used to represent a grouping of one or more networks.

QUESTION 56
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed three ISA Server 2004 computers to enhance network security and the client computers are all configured as Firewall clients and the internal computers are configured as Web Proxy clients. The internal network users recently started reporting that Internet access is very slow. You make use of the Network Monitor and discover that HTTP objects have been duplicated. You also discover that The HTTP objects have been cached on all three ISA servers. You are required to ensure that the users have faster Internet access. What should you do?

A. Automatic discovery should be enabled and configure all client computers as Web Proxy clients.
B. Automatic discovery should be enabled and configure all client computers as Firewall clients.
C. Network Load Balancing (NLB) should be enabled on the ISA server array.
D. On the ISA server array you should enable CARP.

Answer: D

Explanation: The CARP protocol should be used in the scenario because the protocol is used to enable ISA servers to provide distributed cache which are distributed by the CARP protocol used by Web Proxy clients.
Incorrect Answers:
A, B: This should not be configured in the scenario because the setting will enable the clients to automatically receive their proxy configuration at startup.
C: This option should not be considered for configuration because distributed caching does not occur with NLB.

QUESTION 57
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server configured as an Internet-Edge Firewall and is responsible for controlling Internet access to users on the internal network. You created and applied an access rule to allow unrestricted

access to the Internet for all users. The Certkiller .com Finance department informed you that they require attending a live Web cast between 1100 hours and 1300 hours and they require minimum Internet activity from other users during this period.
You later sent e-mail messages to the other departments stating that Internet access will not be available between 100 hours and 1300 hours. You are required to ensure that Internet access is not available to the other departments between 100 hours and 1300 hours.
What should you do?

A. Create an access rule named Bill1 to allow all protocols to All Users group.
Create another access rule named Bill2 to deny all protocols to the users of the Finance department.
Configure Bill2 schedule to be enabled between 1100 hours and 1300 hours.
Ensure that Bill2 is placed above Bill1.
B. Create an access rule named Bill1 to deny all protocols to All Users group.
Create another access rule named Bill2 to allow all protocols to the users of the Finance department.
Configure Bill2 schedule to be enabled between 1100 hours and 1300 hours.
Ensure that Bill2 is placed above Bill1.
C. Create an access rule named Bill1 to deny all protocols to All Users group.
Create another access rule named Bill2 to allow all protocols to the users of the Finance department.
Configure both rules schedules to be enabled between 1100 hours and 1300 hours.
Ensure that Bill2 is placed above Bill1.
D. Create an access rule named Bill1 to deny all protocols to All Users group.
Create another access rule named Bill2 to allow all protocols to the users of the Finance department.
Configure Bill2 and Bill 1 schedule to be enabled between 1100 hours and 1300 hours.
Ensure that Bill2 is placed above Bill1.

Answer: D

Explanation: In the scenario you should consider using the two rules you created because access rules are used to configure traffic passing through the ISA server including traffic passing from the internal network to the Internet to the internal network.
Incorrect Answers:
A: This option should not be considered in the scenario because the configuration would enable all the protocols between 1100 hours and 1300 hours enabling the other users to access the Internet.
B, C: This option should not be considered in the scenario because the configuration used here will disallow Internet access for everyone between 1100 hours and 1300 hours.

QUESTION 58
You work as the network administrator at Certkiller .com. The Certkiller .com

network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The users of Certkiller .com are located in a newly opened Certkiller .com centre.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 that will be used to provide the network users with Internet access. The Certkiller .com centre is isolated from the network. You perform the following tasks:
1. Install a second ISA 2004 server named Certkiller -SR02 at the edge of the Certkiller .com centre
2. And you configure all client computers in the Certkiller .com centre as Web Proxy clients
You are required to ensure the Certkiller .com centre environment is isolated but that the client computers are able to access the Internet through Certkiller -SR01 after authentication.
What should you do?

A. Firewall chaining should be configured on Certkiller -SR02 and configure Firewall chaining to use a user account.
B. Both Certkiller -SR01 and Certkiller -SR02 should be configured as a single array and enable NLB.
C. An automatic dial-up connection must be configured on Certkiller -SR02.
D. Web chaining should be configured on Certkiller -SR02 and configure it to use authentication.

Answer: D

Explanation: In the scenario it would be an excellent idea considering configuring Web chaining because Web chaining allows the client computer to route Web requests through a single location and enables you to route requests from client computers located in multiple branch offices.
Incorrect Answers:
A: This configuration should not be made as it will not affect the users as they are Web Proxy clients and the configuration affects SecureNAT clients and Firewall clients.
B: This option should not be considered in the scenario because this option will not ensure that the Certkiller .com centre is isolated.
C: This should not be configured in the scenario because the client computers will be allowed to automatically dial an Internet connection through Certkiller -SR01.

QUESTION 59
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as an Edge Firewall responsible for providing

Internet access with all the client computers either Firewall or Web Proxy clients.
The Certkiller .com network was approached by the government recently to start a project of a sensitive nature that requires special security. You decided to deploy Certkiller -SR01 in the Demilitarized Zone (DMZ) mode by creating a Perimeter network. The Perimeter will be configured to use a public IP address range.
All of the file resources and FTP servers related to the project have been placed on the perimeter network. You also created a new Perimeter network object for the Perimeter network. The internal network users are working on the project and require access to the FTP servers.
What should you do?

A. A NAT relationship should be created between the internal network and the Perimeter network and create an access rule to grant the internal client computers access to the FTP servers in the Perimeter network.
B. A NAT relationship should be created between the internal network and the Perimeter network and create an access rule to allow limited Web access to the internal clients.
C. A NAT relationship should be created between the internal network and the Perimeter network.
D. An access rule should be created that allows the internal clients access to the FTP server in the Perimeter network.

Answer: A

Explanation: In the scenario we should consider making a NAT relationship between the two networks because a NAT relationship is used for communication between trusted and untrusted networks and furthermore a NAT relationship is unidirectional.
Incorrect Answers:
B: This configuration should not be used in the scenario because the configuration states allow limited web access which will not allow the clients to access the FTP servers.
C: This should not be done in the scenario because by simply creating the relationship between the networks you will not achieve the scenario objective.
D: You should not simply create an access rule in the scenario because the rule on its own can not be used to achieve the scenario objective.

QUESTION 60
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 to enhance network security and all the client computers are configured as a mix of SecureNAT, Firewall and Web Proxy clients. The Certkiller .com network security states that the SecureNAT clients should have anonymous access to the FTP and Web Proxy and Firewall clients should have authenticated access to the FTP.

To adhere to this you create an access rule that allows access to the All Users group for the FTP protocol. You create another rule allowing access to only the All Authenticated Users group for the FTP protocol. After the rules were created you discover Web Proxy clients and Firewall clients access the FTP site anonymously. You are required to ensure that Web Proxy and Firewall clients are only allowed Authenticated access to FTP sites you have to achieve this using the least amount of administrative effort.
What should you do?

A. The access rules should be reordered to ensure the access rule for the All Authenticated Users group to be processed before the access rule for the All Users group.
B. The access rule that allows access to the All Users group to the FTP protocol should be deleted.
C. All the client computers should be configured as Firewall and Web Proxy clients.
D. An access rule should be created for the SecureNAT clients to enable access to the FTP site.

Answer: A

Explanation: In the scenario the best option we could use is to reorder the access rules because in the scenario the SecureNAT clients who have not been authenticated are therefore not in the Authenticated users group will not have the first rule applied.
Incorrect Answers:
B:
You should not create a new access rule because the SecureNAT clients only need to have the order of the access rules reordered.
C: This should not be considered in the scenario because the SecureNAT clients do not support authentication and they will not be able to access the FTP site.
D: This configuration should not be considered in the scenario because you are not required to configure all the client computers as Firewall and Web Proxy clients.

QUESTION 61
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows 200 Professional or Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named CERTKILLER-SR01 to enhance network security and deployed a domain controller named Certkiller -DC01 configured as the internal DNS server forwarding DNS requests to the ISP's DNS server. The company web site http://home. Certkiller .com is hosted at an ISP location and for security reasons the Certkiller .com management decided to host the Web site inside the Certkiller .com network.
You decided to configure a Web server named Certkiller -SR02 in the internal network and host the Web site on it. The network users complain after the configurations that the Web site on Certkiller -SR02 is very slow to diagnose the

situation you check the log files and discover requests for http://home. Certkiller .com are being routed through Certkiller -SR01. You are required to ensure that requests for internal servers are not routed through Certkiller -SR01.
What should you do? (Choose two)

A. The Allow limited Web access and access to ISP network services policy should be configured.
B. The Block Internet access/allow access to Internet service provider (ISP) network services policy should be configured.
C. The Directly access computers specified in the Domain tab option on Certkiller -SR01 should be enabled.
D. Certkiller .com should be added to the list of domain names available on the internal network on Certkiller -SR01.

Answer: C, D

Explanation: The best choice in the scenario would be to enable the required options because this option allows Web Proxy and Firewall clients to bypass the proxy configuration when connecting to hosts in the domain.
Incorrect Answers:
A, B: This should not be configured in the scenario because this policy does not ensure the requests for internal resources are not routed through Certkiller -SR01.

QUESTION 62
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows 200 Professional or Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 to enhance network security. The Certkiller .com network also contains a FTP server. You are about to enable users to access from the Internet by creating an access rule to allow FTP access for all the users on the default FTP ports. You will travel frequently. You therefore decide to configure Certkiller -SR01 and the FTP server for remote management so you are able to manage them when outside the office. You are required to remotely manage Certkiller -SR01 and the FTP server.
What should you do?

A. One RDP server publishing rule must be configured on Certkiller -SR01 to remotely manage Certkiller -SR01 and configure a second RDP server publishing rule on port 12 to remotely manage the FTP server.
B. One RDP server publishing rule must be configured on Certkiller -SR01 to remotely manage the FTP server and from the FTP server remotely connect to he ISA server using MMC.
C. One RDP server publishing rule must be configured on Certkiller -SR01 to remotely manage Certkiller -SR01 and from Certkiller -SR01 remotely connect to the FTP

server using the MMC.
D. Two external IP addresses should be configured on Certkiller -SR01 and create two server publishing rules to enable RDP access.

Answer: D

Explanation: In the scenario the best option is to configure two external IP addresses because when a server publishing rule is created you actually configure the ISA server to listen for client requests using a particular port number.
Incorrect
Answer:
A: This option should not be considered in the scenario because the use of MMC for the connections is not secure because communication is not protected.
B: This should not be considered in the scenario because using two rules and two listeners is not entirely secure and should not be used in the scenario.
C: This configuration should not be considered in the scenario instead two external IP addresses should be configured.

QUESTION 63
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 to enhance network security and control access to the Internet.
The Certkiller .com network hosts two Web sites named Finance and Distribution on two Web server named Certkiller -SR02 and Certkiller -SR03 both located on the internal network.
You are in the process of publishing the Finance and Distribution Web sites on Certkiller -SR01 and require providing access to both sites. You want to configure anonymous access for the Finance Web site and Basic authentication for the Distribution Web site. You must know how to configure the access for the sites.
What should you do?

A. Two Web publishing rules should be created and configure each rule to forward to a different Web server and configure the rule to use different Web listeners.
B. Two Web publishing rules should be created and configure each rule to forward to a different Web server and configure the rule to use the same Web listener.
C. One Web publishing rule should be created and configure the rule to forward to both Web servers and configure the rule to use a Web listener.
D. One Web publishing rule should be created and configure the rule to forward to two different Web servers and configure the rule to use the default Web listener.

Answer: A

Explanation: In the scenario you should remember that a Web listener defines how

the ISA server listens for HTTP and SSL requests and defines the network, IP address and port number on which the listener listens for client requests.
Incorrect Answers:
B: This option should not be considered in the scenario because the same Web listener can not be used for two Web sites.
C, D: This should not be considered in the scenario because it is impossible to publish two Web sites using different authentication methods.

QUESTION 64
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 to enhance network security and control Internet access and the network contains an Exchange 2003 server configured as an e-mail server named Certkiller -SR02. The Certkiller .com network security policy states all inbound requests from the Internet are authenticated. The Certkiller .com network users Finance department travels frequently and required access to their e-mail when out of the office.
To achieve the requirement you create and apply a Web publishing rule on Certkiller -SR01 and configure the rue to use a Web listener named BillListener configured to use forms-based authentication to enable access for Outlook Web Access (OWA). The remote users of the Finance department are able to use OWA to access their e-mail. The Certkiller .com network users recently requested access to their e-mail through wireless mobile clients. You plan to enable access to Certkiller -SR02 through Outlook Mobile Access (OMA).
What should you do?

A. A Web listener that uses SSL should be created and create another Web publishing rule to push Certkiller -SR02 on Certkiller -SR01 for OMA and configure the rule to use the Web listener.
B. A new Web listener should be created and modify the existing Web publishing rule for OWA and configure it also for OMA and configure the rule to use the new listener.
C. Another Web publishing rule should be created to publish Certkiller -SR02 on Certkiller -SR01 for OMA and configure the rule to use BillListener.
D. The existing Web publishing rule should be modified for OWA and configure it also for OMA and configure the rule to use BillListener.

Answer: A

Explanation: In the scenario you should remember that you are required to use a different Web listener for OMA and a Web listener is configured to use forms-based authentication which OMA does not support in the scenario.
Incorrect Answers:
B, C, D: This option should not be used in the scenario because in order to publish more

than one Web client mail service which require different authentication methods you require a separate Web publishing rule.

QUESTION 65
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 to enhance network security and a domain controller named Certkiller -DC01 hosts the DNS server and the network has an Exchange 2003 server named Certkiller -SR02. The Certkiller .com network senior managers have requested for permission to use their Personal Digital Assistants (PDAs) and mobile phones to access their company e-mails. You want to allow the senior manager group access to the company -emails using PDAs. You are required to ensure that the Senior Managers group can access the e-mails using their PDAs through ActiveSync even when outside the office.
What should you do?

A. An IMAP server publishing rule should be created and configure the rule to point to the Exchange 2003 server.
B. A POP3 server publishing rule should be created and select the Exchange ActiveSync option on the Select Services page.
C. An HTTP server publishing rule should be created and configure the rule to point to the Exchange 2003 server.
D. A mail server publishing rule should be created and select the Exchange ActiveSync option on the Select Services page.

Answer: D

Explanation: In the scenario you should remember that the Exchange ActiveSync service allows users to synchronize their Exchange information with their ActiveSync enabled mobile devices.
Incorrect Answers:
A, B: This rule should not be configured in the scenario because the rule cannot be used to configure users to access their e-mails using PDAs through ActiveSync.
C: This configuration should not be used in the scenario because the ISA server must be enabled to allow the users access to company e-mails using their PDAs.

QUESTION 66
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01configured as an Edge Firewall to enhance network security and

control access to the Internet and the network also contains an Exchange 2003 server named Certkiller -SR02. You recently decided to enable secure and encrypted access to the Exchange server for Microsoft Outlook 2003 clients using the following steps:
1. You configure an RPC Proxy server.
2. You create a Web listener configures for SSL.
3. You create an HTTPS Web publishing rule on Certkiller -SR01 to direct traffic to the RPC Proxy server.
The Certkiller .com network internal and remote employees use Outlook 2003 to access company e-mails. The network also contains contractors who access their mailboxes using Outlook Express. You want to enable secure and encrypted access for the contractors.
What should you do?

A. A new server publishing rule should be created and enable the POP3, IMAP4, and SMTP protocols.
B. You should upgrade to Outlook 2003 and create a new server publishing rule to enable POP3, SMTP and IMAP4 protocols.
C. The clients should be upgraded to Outlook 2003 and make use of the existing publishing rule.
D. A new server publishing rule should be created and enable the POP3, IMAP4, and SMTP protocols.

Answer: A

Explanation: In the scenario you should try and remember that the RPC over HTTP feature can be enabled by configuring an RPC Proxy server and a secure Web publishing rule to publish the server to secure RPC traffic.
Incorrect Answers:
B, D: The new rule should not be created to enable POP3, IMAP4 and SMTP as the Outlook express clients use only POP3 or IMAP4 to read messages.
C: This configuration should not be made in the scenario even though hit may involve less administration effort.

QUESTION 67
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as an Edge Firewall configured with two IP addresses one for the internal and one for the external network adapter. You want to publish two FTP server named Certkiller -SR02 and Certkiller -SR03 located on the internal network. Certkiller -SR02 will be accessed by the internal users and Certkiller -SR03 will be accessed by the users of the Finance department to share the latest product versions with a few customers.

You are required to ensure that the Users on the Internet are able to access and download information from Certkiller -SR02 and ensure that the Finance department accesses a nonstandard port on Certkiller -SR03.
What should you do?

A. A server publishing rule should be created for the RDP protocol on port 21 and configure the rule to enable port override option.
B. Two server publishing rules should be created and configure the rule for Certkiller -SR01 to allow anonymous access using the default FTP port and configure a new outbound protocol definition named FTPBill for non-standard TCP port. The rule must be configured for Certkiller -SR03 to use FTPBill.
C. A server publishing rule should be created and configured to allow access to two different ports.
D. Two server publishing rules should be created and configure the rule for Certkiller -SR01 to allow anonymous access using the default FTP port and configure a new inbound protocol definition named FTPBill for non-standard TCP port. The rule must be configured for Certkiller -SR03 to use FTPBill.

Answer: D

Explanation: In the scenario you should create two server publishing roles because server publishing rules are configured to grant access to internal resources using protocols other than HTTP and HTTPS.
Incorrect Answers:
A: This configuration should not be considered for usage in the scenario because the Terminal Services uses port 3389 to communicate between client and the server.
B: This configuration should not be made as it is impossible to configure two ports for used using a single server publishing rule.
C: In the scenario you are not require to configure any outbound settings as this option will not help you achieve the scenario objective.

QUESTION 68
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 used to control Internet access with all the users configured as Firewall and Web Proxy clients. The Certkiller .com network security policy requires that the IP addresses of remote clients be visible to the published servers on the internal network which contains an application server named Certkiller -SR02. A user from a partner company named Rory Allen requires access to Certkiller -SR02 for remote administration. You want to allow a Remote Desktop Connection to Certkiller -SR02 using a nonstandard TCP port. You make the following configurations:
1. Create a new protocol definition for the nonstandard TCP port.

2. Create a server publishing rule that uses the new protocol definition.
Rory Allen recently reported he is unable to access Certkiller -SR02 using a Remote Desktop connection.
What should you do?

A. The server publishing rule should be modified to use the default TCP port for connection.
B. The server publishing rule should be modified to allow authentication on the ISA server.
C. The server publishing rule should be modified to use the default TCP port for connection and configure it to redirect the requests on the default port to the nonstandard TCP port.
D. Certkiller -SR02 should be configured as a SecureNAT client.

Answer: D

Explanation: Remember in the scenario that the server publishing rules do not provide the option of authentication as it is implemented using Network Address Translation (NAT) and the internal servers must be configured as SecureNAT clients.
Incorrect Answers:
A, C: This configuration should not be made in this scenario because RDP uses port 3389 to communicate between the clients and the server.
B: This option should not be considered for usage in the scenario because server publishing rules do not support authentication of users.

QUESTION 69
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch office in Miami.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as an Edge Firewall. The branch office users require access to the internal resources of the main office but the branch office uses a third-party VPN server. You want to design a solution that is secure for the connection. You plan to implement a site-to-site VPN connection between the offices.
During the course of the day you configure Certkiller -SR01 as a VPN server and enabled the L2TP/IPSec on Certkiller -SR01. The branch office users later started reporting that they are unable to connect to Certkiller -SR01. You want to ensure they are able to access the internal resources.
What should you do?

A. Certkiller -SR01 should be configured to use IPSec tunnel mode.
B. The IPSecPol tool should be installed on the third-party VPN server in the branch

office.
C. Certkiller -SR01 should be configured to use PPTP.
D. The IPSecPol tool should be installed on Certkiller -SR01.

Answer: A

Explanation: In the scenario you should remember that IPSec is used in tunnel mode to provide encapsulation for IP traffic for IP traffic only and that IPSec tunnel mode can be used to connect to a third-party VPN server.
Incorrect Answers:
B, D: This tool should not be considered for installation on Certkiller -SR01 nor should it be installed on the third-party VPN server because the tool is used to configure IPSec policies either in Active Directory or the local or remote registry.
C: This protocol should not be used in the scenario because the protocol is used to connect to an ISA server or Windows Routing and Remote Access servers.

QUESTION 70
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch office in Dallas.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 used to control Internet access both inbound and outbound. The Certkiller .com branch office also contains an ISA server named Certkiller -SR02 both the office ISA servers are configured as Edge Firewall. During the course of the day you configure a site-to-site L2TP/IPSec VPN connection using certificate-based machine authentication between Certkiller -SR01 and Certkiller -SR02.
Recently the Certkiller .com network users that run Windows NT Workstation 4.0 report they are unable to access resources in the main office. You are required to ensure that all the branch office users are able to access resources in the main office using the least amount of administrative effort.
What should you do?

A. The Microsoft L2TP/IPSec VPN client should be downloaded and installed on the client computers running Windows NT Workstation 4.0.
B. All the computers should be upgraded to Windows XP Professional and create an access rule on Certkiller -SR01 to enable outbound access to PPTP.
C. Another access rule should be created on Certkiller -R02 to enable outbound access to PPTP for client computers running Windows NT Workstation 4.0.
D. Another access rule should be created to enable outbound access to L2TP/IPSec with EAP for client computers running Windows NT Workstation 4.0.

Answer: A

Explanation: You should remember in the scenario if you are to enable client computers running Windows NT Workstation 4.0 you are required to download and install the Microsoft L2TP/IPSec VPN Client for those computers.
Incorrect Answers:
B, C: This option should not be used in the scenario because the PPTP option is only used when the server does not support machine certificate authentication.
D: This option should not be used in the scenario because the result will be not all branch users will be able to access resources in the main office.

QUESTION 71
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch office in Miami.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 in the main office and a Routing and Remote Access Server (RRAS) named Certkiller -SR02 in the branch office configured to connect to each other using a site-to-site L2TP/IPSec VPN connection that uses pre-shared keys.
You are busy planning to migrate the RRAS on Certkiller -SR02 to the ISA server Certkiller -SR01 and perform the following steps:
1. Install ISA Server 2004 on Certkiller -SR02
2. Remove the preshared key from the RRAS console and enter the preshared key on the Authentication tab of the VPN properties dialog box on Certkiller -SR02
After the migration the branch office users start reporting they are unable to connect to resources in the main office. You are required to ensure that the branch office users can access resources on the main office using the site-to-site L2TP/IPSec VPN connection with preshared keys for authentication.
What should you do?

A. The pre-shared key should be entered in the RRAS console on Certkiller -SR02 and re-enter the pre-shared key in the RRAS console on Certkiller -SR02.
B. The pre-shared key should be exported from Certkiller -SR02 to Certkiller -SR01.
C. Certkiller -SR02 should be configured to use L2TP/IPSec.
D. Outgoing VPN connections should be enabled on Certkiller -SR02.

Answer: D

Explanation: You should remember in the scenario that when you are upgrading RRAS to ISA Server 2004 that the credentials for site-to-site connections are not exported and outgoing VPN connections are enabled on the ISA server until you configure them.
Incorrect Answers:
A: This configuration should not be used in the scenario as you would be unable to establish a site-to-site L2TP/IPSec VPN connection.
B:

There is no need for you to make this configuration in the scenario as it has already been done.
C: There is no need to export the pre-shared key in the scenario because when you are upgrading RRAS to ISA Server 2004 that the credentials for site-to-site connections are not exported.

QUESTION 72
You work as the network administrator at Certkiller .com branch office. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch office in Dallas
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 in the main office and a DNS server named Certkiller -SR02 in the branch office. You recently configured Certkiller -SR01 as a remote access VPN server to enable a site-to-site PPTP VPN connection with the main office ISA server Certkiller -SR03. The Certkiller .com main office also has a DHCP server named Certkiller -SR04.
The Certkiller .com main office users started reporting that they are unable to connect to the branch office using the site-to-site VPN connection, you check the Event Viewer on Certkiller -SR03 and note the error below:
"Unable to contact a DHCP server. The Automatic Private IP Address 169.254.160.130 will be assigned to dial-in clients. Clients may be unable to access resources on the network."
You are required to ensure that VPN clients from the main office are able to connect toe the branch office network using the site-to-site VPN connection.
What should you do? (Choose two)

A. Certkiller -SR04 should be configured to include an IP address pool for the branch office.
B. Certkiller -SR01 should be configured to use Certkiller -SR04 as the DHCP server.
C. A DHCP server must be installed and configured at the branch office.
D.
Certkiller -SR01 should be configured wit ha static pool of IP addresses to assign to the VPN clients

Answer: C, D

Explanation: You should remember in the scenario when you configure the ISA server to use a DHCP server to assign IP addresses or a static pool of IP addresses you are not required tocreate special routing table entries to support the VPN clients.
Incorrect Answers:
A, B: The configurations here should not be used in the network as the servers are

located on different segments. You should not configure Certkiller -SR03 to include an IP address pool for the branch office users in the scenario.

QUESTION 73
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch office in Dallas. The Dallas office users require access to the resources in the main office.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as a VPN server. The shared resources in the main office are highly confidential and a Certkiller .com network security policy states that all remote VPN clients fulfill the requirements below:
1. The remote client computers have Windows XP Professional SP2 installed.
2. The remote VPN client should have updated antivirus software.
3. All the network connections on the remote VPN clients must have Windows Firewall enabled.
In the network main office you configure VPN quarantine control on the ISA 2003 Server and also create the CK_Quarantinetest.vbs script to validate the client configuration. You are required to ensure only remote VPN clients passing the security criteria are allowed to access the resources.
What should you do?

A. An access rule must be configured for the CK_Quarantinetest.vbs script to run when a remote VPN client attempts to connect to the VPN server.
B. The registry entry for the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\rqs key to pass CK_Quarantinetest.vbs as a parameter should be configured for AllowedSet key.
C. The location of the CK_Quarantinetest.vbs script must be passed as a parameter to the Rqs.exe components.
D. A Connection Manager (CM) profile should be created that includes the CK_Quarantinetest.vbs script and distribute the CM profile to all remote VPN clients in the branch office.

Answer: D

Explanation: In the scenario you should remember that the CM profile is used to contain a script that performs validation checks on the remote-access client computer to verify the network policies.
Incorrect Answers:
A: There is no need to create an access rule for the script you should simply create a CM profile that uses the CK_Quarantinetest.vbs script.
B: This option should not be used in the scenario because the option will not enable the branch office users to access the VPN server remotely.

C: There is no need for this configuration in the scenario because you should simply create a CM profile that uses the CK_Quarantinetest.vbs script.

QUESTION 74
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as an Edge Firewall outside the Active Directory domain. The Certkiller .com network domain contains an internal enterprise Certification Authority (CA). The Certkiller .com network security policy states that all VPN connections must be configured to use L2TP/IPSec with certificate-based authentication. You plan to configure Certkiller -SR01 as a VPN server.
You later configure a Group Policy Object (GPO) to enable Certkiller -SR01 and other network computers to acquire computer certificates through automatic enrollment and perform the following tasks to ensure this for Certkiller -SR01:
1. You create a access rule to allow all protocols from Certkiller -SR01 to the internal network.
2. You disable the Enforce strict RPC compliance setting temporarily.
3. You disable the RPC application filter temporarily.
You then discover that automatic enrollment has failed for Certkiller -SR01 but was successful for the client computers. You are required to ensure Certkiller -SR01 can successfully acquire the computer certificate.
What should you do? (Choose two)

A. The Certkiller -SR01 firewall should be restarted to request the certificate.
B. The Enforce strict RPC compliance checkbox should be enabled and the RPC filter should be enabled on Certkiller -SR01.
C. Certkiller -SR01 should be joined to the domain.
D. A Web enrollment site must be used to obtain the certificate.

Answer: C, D

Explanation: In the scenario you should try to remember that in order to request a certificate for an ISA server that you do not enforce strict RPC compliance by modifying the firewall then will the auto enrollment succeed.
Incorrect Answers:
A: The only time you will be required to do this is when you are making use of Certificates MMC before disabling the RPC filter.
B: This option should not be used in the scenario because DCOM is a RPC protocol required for services such as enrollment of certificates.

QUESTION 75
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All

servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as a remote VPN server using L2TP/IPSec which will be used to provide network employees connecting as remote VPN client access to required internal resources. You later ensure the internal Certification Authority (CA) is online and has the permissions needed to issue certificates. You are busy requesting a server certificate from the C
A. You receive the error message below:
"The certificate request failed because of one of the following conditions:
The certificate request was submitted to a Certification Authority that was not started.
You do not have the permissions to request certificates from the available CAs."
You are now required to ensure that a server certificate is successfully issued to the ISA server to enable Certkiller -SR01 to function as an L2TP/IPSec-based remote access VPN server.
What should you do?

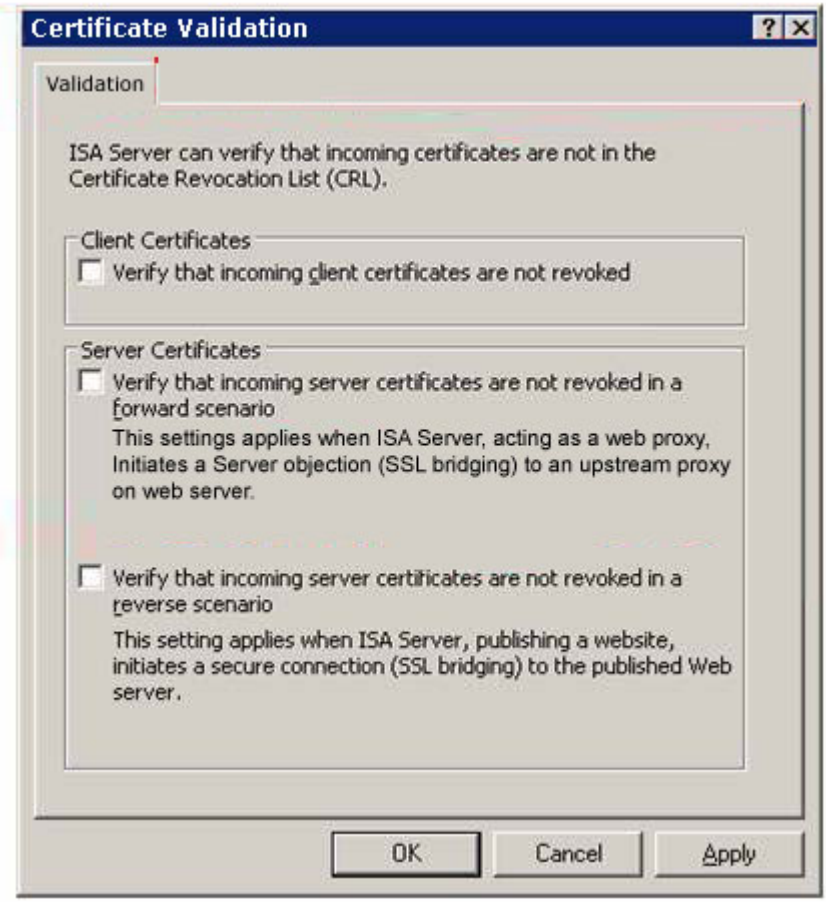
A. The Extensible authentication protocol (EAP) with smartcard or other certificate check box should be selected on Certkiller -SR01.
B. The Verify that incoming client certificates are not revoked check box should be selected on Certkiller -SR01.
C. The CA root certificate should be manually placed into the Trusted Root Certification Authorities store on Certkiller -SR01.
D. The System Policy should be edited to clear the Enforce strict RPC compliance check box on Certkiller -SR01.

Answer: D

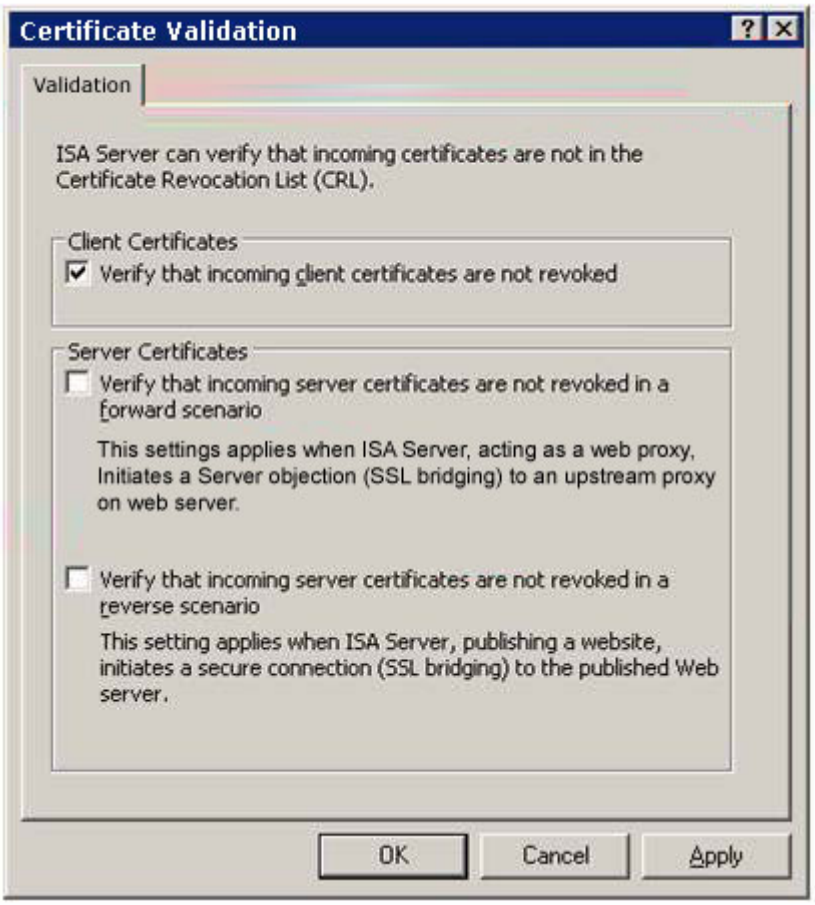
Explanation: In the scenario you should remember that DCOM traffic to the ISA server can only be allowed when the Enforce strict RPC compliance check box has been unchecked.
Incorrect Answers:
A: This option should only be used in the situation where the remote site gateway or VPN client initiates a connection to the ISA Server Certkiller -SR01.
B: This option should only be used if you want to stop users from connecting to the server if their certificates are revoked.
C: This would only be required if all the servers are not members of the domain and in the scenario all computers are members of the domain.

QUESTION 76
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named

Certkiller -SR01 and all client computers are configured as Web Proxy clients.
You are busy configuring Certkiller -SR01 as a L2TP/IPSec VPN server by using certificate-based authentication to provide secure access to the internal network resources for remote VPN clients.
During the course of the day you deploy client certificates on Certkiller -SR01 and other remote users using an external C
A. You want to configure Certkiller -SR01
to deny access to clients with revoked certificates. You decide to enable the Allow HTTP from the ISA Server to all networks for CRL download system policy rule.
You are required to prevent VPN clients with revoked certificates from establishing a VPN connection.
What should you do? (To answer, configure the following exhibit appropriately)



Answer:



Explanation:
You should select the 'Verify that the incoming client certificates are not revoked' checkbox. This option prevents remote users from connecting the ISA server if their certificates have been revoked.
Incorrect Answers:
The options in the Server Certificate section pertain to servers and not client computers.

QUESTION 77
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network domain functional level is at Windows Server 2000 mixed-mode.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as a remote access VPN server that allows L2TP/IPSec remote access client connections. During the course of the day you configured Certkiller -SR01 to allow VPN access to members of the Domain Users global group whilst ensuring you take other steps to ensure their access and the users report they successfully can access the VPN server. A new network user named Rory Allen has joined the Finance departments. You create a user account with the default settings. Rory Allen has reported that he is unable to connect to the

remote VPN server.
What should you do?

A. The user account properties should be modified for dial-in access.
B. The remote access policy must be modified to add the user Rory Allen.
C. The domain functional level should be downgraded.
D. User mapping should be enabled for the remote VPN clients.

Answer: A

Explanation: In the scenario you should remember that the domain functional level is at Windows 2000 server mixed-mode. You created a user account with the default setting which in this functional level has the dial-in permissions disabled.
Incorrect Answers:
B: This option should not be used in the scenario because Rory Allen still will be unable to access the remote access VPN.
C: This should not be considered in the scenario because upgrading the functional level of a domain is a one way process.
D: You should not consider using this option in the scenario because User mapping is used to map VPN clients connecting to the ISA server using non-Windows authentication methods such as RADIUS.

QUESTION 78
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as an Edge Firewall and is configured as a remote access VPN server that allows Point-to-Point Tunneling Protocol (PPTP) remote access connections. The remote VPN clients of Certkiller .com access resources on the internal network but some users started reporting they are unable to access some resources on the internal network. You are required to determine whether the VPN client connections are successful or not.
What should you do?

A. A report job should be created.
B. A connectivity verifier should be set up.
C. The Web Proxy log view should be used.
D. A session filter should be configured.

Answer: D

Explanation: You should remember that in the scenario you can use session monitoring to determine whether a VPN client connection is successful or not making this the best choice to use.

Incorrect Answers:
A: This option should not be used in the scenario because the report job is used to create a report automatically on a specified schedule and can not be used for the scenario.
B: This should not be considered in the scenario because the verifier allows an ISA server to check connectivity by sending HTTP GET requests to the specified computer.
C: This option is only useful if you are trying to determine which users can not access an external Web site while other users are able to.

QUESTION 79
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as an Edge Firewall. The Certkiller .com network users travel frequently and require access to internal network resources to get updated information while traveling. You decided to configure Certkiller -SR01 as a remote access VPN server configured to allow L2TP/IPSec remote access client connections to the remote users. You are required to configure dial-in permissions in Active Directory to enable the remote users to access the VPN server remotely using the least amount of administrative effort.
What should you do?

A. A new access policy must be created and configure the dial-up permissions for each user manually.
B. Dial-in access must be configured on a per-account basis in Active Directory.
C. The domains functional level should be lowered.
D. The remote access policy should be modified.

Answer: D

Explanation: In the scenario you should consider modifying the remote access policy because the domain is Windows Server 2003 you are simply able to modify the remote access policy.
Incorrect Answers:
A: This option should not be used in the scenario as there is way to much administrative effort involved with the process.
B: This should not be considered in the scenario because in Windows Server 2003 this is controlled by remote access policy.
C: This should not be considered in the scenario because upgrading the functional level of a domain is a one way process.

QUESTION 80
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client

computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as an Edge Firewall. You are in the process of configuring Certkiller -SR01 as a remote access VPN server to enable remote client access to internal network resources. You configured Certkiller -SR01 to support only EAP authentication for the remote VPN clients and a user certificate has been issued to all remote VPN client computers. You are required to ensure that access policy rules are applied to users logging in by using Windows authentication are also applied to all remote VPN clients logging in using EAP authentication.
What should you do?

A. User mapping should be enabled for the remote VPN clients.
B. The When username does not contain a domain, use this domain option should be deselected in the VPN Clients Properties dialog box.
C. Certkiller -SR01 should be configured as a stand-alone server outside the domain.
D. Certkiller -R01 should be configured to use MS-CHAPv2 authentication.

Answer: A

Explanation: In the scenario the best option is to enable user mapping as this would allow you to ensure that access policy rules are applied to users logging in using Windows authentication and EAP authentication.
Incorrect Answers:
B: This option should not be used in the scenario because this option can only be enabled if you have user mapping enabled.
C: This configuration should not be considered in the scenario because the server should be part of the domain when making these configurations.
D: This should not be configured in the scenario as you already require the users only to use EAP authentication and issued user certificates.

QUESTION 81
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 used to control Internet access and that is configured by using the 3-Leg Perimeter network template. You recently enabled Web caching on Certkiller -SR01 and configured all the client computers as Web Proxy clients. You are busy using the Microsoft SQL Server 2000 Desktop Engine (MSDE) database log storage format for the Web Proxy logs and have configured the total size of the log file to 10 GB.
The Certkiller .com network users report that access to frequently visited sites is very slow. You configure the following System Monitor performance counters to find the sources of slow performance:
1. Memory\Pages/sec.

2. PhysicalDisk\Avg. Disk Queue Length.
You are required to choose which counter would indicate the worst performance bottleneck.
What should you do?

A. A high Memory\Page/sec value and a low PhysicalDisk\Avg. Disk Queue Length value.
B. A low Memory\Page/sec value and a low PhysicalDisk\Avg. Disk Queue Length value.
C. A low Memory\Page/sec value and a high PhysicalDisk\Avg. Disk Queue Length value.
D. A high Memory\Page/sec value and a high PhysicalDisk\Avg. Disk Queue Length value.

Answer: D

Explanation: Remember in the scenario if you are experiencing slow Web performance after configuring MSDE the best method to check performance is used in the answer.
Incorrect Answers:
A, B, C: The scenario requires that you select the worst performance stat and these three options do not have the worst performance bottleneck.

QUESTION 82
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 used to control Internet access as all the network users of Certkiller .com require Internet access. The network users often visit the same Web site on the Internet. You enable forward caching on Certkiller -SR01 to accelerate outbound requests from the internal users.
The Certkiller .com internal users started reporting that the Web sites access is very slow. You suspect that insufficient memory is causing Certkiller -SR01 to perform slowly. You decide to monitor Certkiller -SR01 by adding the following counter to the System Monitor:
1. Memory\Pages/sec.
2. ISA Server Cache\Memory Usage Ratio Percent (%).
You decided to delegate the task to an assistant named Dean Austin but Dean Austin reports that he is unable to monitor the performance by using system monitor.
What should you do?

A. Dean Austin must be added to the Server Operators domain group.
B. An access rule must be created to allow Dean Austin to connect to Certkiller -SR01.

C. The ISA Server Basic Monitoring rights must be assigned to Dean Austin.
D.
Dean Austin should be added to the Windows Server 2003 Performance Monitor Users group.

Answer: D

Explanation: In the scenario you should keep in mind that only the members of the Performance Monitor Users group are capable of monitoring and using performance counters on domain controllers in the domain.
Incorrect Answers:
A, B, C: This option should not be considered in the scenario because in order to view and use performance counters the users are required to be members of the Performance Monitor Users group are capable of monitoring and using performance counters on domain controllers in the domain.

QUESTION 83
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as an Edge Firewall used to control Internet access and all the client computers are configured as Firewall clients and Web Proxy clients. The Certkiller .com network regularly accesses a partner Web site that is updated frequently. You enable Web caching on Certkiller -SR01 and configure a content download job to run regularly after office hours to ensure that the users have access to the latest information without utilizing precious bandwidth. The Certkiller .com network users started reporting the partner Web site access is very slow. You decide to add the counters below to the System Monitor to monitor performance bottlenecks:
1. Memory\Pages/sec.
2. PhysicalDisk\Avg. Disk Queue Length.
You are required to verify the cache disk parameters to identify the reason of the slow performance.
What should you do? (Choose all that apply)

A. The ISA Server Cache\Total Actively Refreshed URLs performance counter should be added to the System Monitor console.
B. The ISA Server Cache\Memory Usage Ratio Percent (%) performance counter should be added to the System Monitor console.
C. The ISA Server Cache\Total URLs Cached performance counter should be added to the System Monitor console.
D. The ISA Server Cache\URL Commit Rate (URL/sec) performance counter should be added to the System Monitor console.
E. The ISA Server Cache\Total Disk Failures performance counter should be added to the

System Monitor console.

Answer: C, D, E

Explanation: In the scenario you should configure these performance counters to determine whether or no the Certkiller .com network is operating efficiently or are suffering from performance bottlenecks.
Incorrect Answers:
A: This counter should not be considered for use in the scenario because it is used to display the cumulative number of URLs in the cache that have been actively refreshed.
B: The performance counter in question in this option should not be considered for use in the scenario because the counter is used to display the ratio between cache fetches from the memory cache and the total cache fetches.

QUESTION 84
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 used to control Internet access both outbound and inbound. You configure Certkiller -SR01 as a Web caching server. The Certkiller .com network regularly accesses a partner Web site that is updated frequently. You configure a content download job to run regularly every morning before office hours to ensure that the users have access to the latest information without utilizing precious bandwidth.
The Network users started reporting that access to the partner Web site is slow. You suspect the problem us occurring because the cache is getting trimmed because of insufficient memory. You are required to verify that reduction in the cache size due to low memory is the cause of the slow performance and should select which performance counters to use.
What should you do? (Choose two)

A. Memory\Cache Bytes.
B. Memory\Available Bytes.
C. Memory\Pages/sec.
D. ISA Server Cache\Memory Usage Ratio Percent (%).

Answer: A, B

Explanation: In the scenario you should keep in mind that you can use Windows 200 Server or Windows Server 2003 System monitor to access the performance of an ISA server computer. You can use ISA Server Performance Monitor installed with the ISA Server Management Console.
Incorrect Answers:
C: This performance counter should not be used in the scenario because the counter

measures the number of pages per second that are paged out of Random Access Memory (RAM) to hard disk or paged into RAM from hard disk.
D: This performance counter should not be used in the scenario because the counter display the ratio between cache fetches from the memory cache and the total cache fetches.

QUESTION 85
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 configured as an Edge Firewall that is used to control Internet access outbound and inbound. The Certkiller .com management has requested a report published for a Web server on the internal network that should include the IP address of the Web clients. You configure Certkiller -SR01 to generate the required report a publish the report to a shared folder. You grant the Allow Read permission for the shared folder to the management staff.
You decide to test the report. You discover that the report contains only the internal IP address of Certkiller -SR01. You are required to ensure that the report displays the IP addresses of clients who made the Web requests.
What should you do?

A. Server publishing should be used to log the original IP address of the client who made the request.
B. The allowed permissions granted for the management staff for the shared folder should be changed from Allow Read to Allow Full Control.
C. Web publishing must be used to log the original IP address of the client who made the Web request
D. Third-party ISA server add-ons should be used to generate the required report.

Answer: A

Explanation: In the scenario you should consider using the server publishing to log the original IP address of the client making the Web request and the source IP address in the host header does not change when a request is forwarded by the server publishing rule.
Incorrect Answers:
B: This option should not be considered in the scenario because the shared folder permissions are used to control user access to the folder where the reports are published.
C: This option should no be used in the scenario because the source header of the host will be changed who made the Web request resulting in you not getting the original IP address.
D: This option should not be used in the scenario because the ISA server does have built-in Report Publishing feature.

QUESTION 86
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 used to control Internet access. The Certkiller .com network security policy states that all the shared folders that exist should have the minimum NTFS permissions required for job performance and no other user other than the ISA Server administrator should be granted any administrative right on CERTKILLER-SR01 and all shared folders on the network are configured with Allow Read permission by default.
The Certkiller .com management recently requested a report on the We sites that the network employee's visit frequently. You create a report job on Certkiller -SR01 and configure the job to send an e-mail containing a link to the report to the Certkiller .com management. You alter additionally publish the report in the security context of the Certkiller -SR01\Administrator account to a shared folder to which the management have Allow Read permission. You later check the shared folder. You discover the report was not published. You are required to ensure the Management is able to access the weekly report whilst adhering to network security policy.
What should you do?

A. The Allow Read & Execute permission should be granted to the Certkiller -SR01\Administrator account for the shared folder.
B. The Allow Full Control permission should be granted to the Certkiller -SR01\Administrator account for the shared folder.
C. The Allow Modify permission should be granted to the Certkiller -SR01\Administrator account for the shared folder.
D. The Allow Write permission should be granted to the Certkiller -SR01\Administrator account for the shared folder.

Answer: D

Explanation: You should remember in the scenario that you are required to have the Allow Write permission in order to have the report published and by granting the user the required permissions the scenario objective is achieved.
Incorrect Answers:
A, B, C:
These permissions should not be granted in the scenario because all of the options here do not adhere to the network security policy of Certkiller .com and therefore they are not to be used in the scenario.

QUESTION 87
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All

servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 used to control Internet access. The Certkiller .com network security policy states that all URLs of the Web sites visited by the users on the internal network be logged. To ensure that the Web sites are logged you configure all client computers as Web Proxy clients and configure Certkiller -SR01 to log information in a text file format.
The network users of the Reporting group require access to information store in the ISA server logs to consolidate the annual report. You want to grant permissions to view the ISA server logs to the Reporting group and ensure they are unable to create firewall policies.
What should you do?

A. The ISA Server Extended Monitoring role should be assigned to the users of the Reporting group.
B. The ISA Server Basic Monitoring role should be assigned to the users in the Reporting group.
C. The ISA Server Full Administrator role should be assigned to the Reporting group.
D. The ISA Server Basic Monitoring role with special privileges should be assigned to users in the Reporting group.

Answer: A

Explanation: Remember in the scenario that the ISA Server Extended Monitoring role allows users to perform monitoring tasks, log configuration, alert definition configuration as well as export and import secret configuration information.
Incorrect Answers:
B, D: These options should not be used in the scenario because users assigned this role are unable to view log files.
C: This option should not be used as the Reporting group would be able to do what they desire.

QUESTION 88
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch office in Dallas.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 in the branch office used to control Internet access both inbound and outbound. The Certkiller .com network clients are all configured as Web Proxy clients. You configured Certkiller -SR01 to log all the data in a text file format.
The Certkiller .com management staff requested information about sites the client's visited from the log files which you check using the Log Viewer and discover the log information is displayed. You are required to ensure that you are able to view the

information using the Log Viewer.
What should you do?

A. The ISA server log files must be configured to be saved in the Microsoft SQL Server 2000 Desktop Engine (MSDE) database log storage format.
B. All the client computers should be configured as SecureNAT clients on the network.
C. All the client computers should be configured as Firewall clients on the network.
D. The ISA server log files should be configured to be saved in a text file format.

Answer: A

Explanation: In the scenario you should always remember that only log files stored in the MSDE format can be viewed later using the Log Viewer.
Incorrect Answers:
B, C: Only the Web Proxy clients would be able to resolve Web sites through the ISA server using this configuration in the scenario.
D: There is no need for you to configure this type of format as it is already used in the scenario.

QUESTION 89
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 used to control Internet access and the network also deployed a SMTP server named Certkiller -SR02 and a DNS server named Certkiller -SR03. You recently created a DNS intrusion alert that will detect host name overflow and zone transfer attacks. You additionally configured the actions below if a DNS intrusion is detected:
1. Send e-mail to admin@ Certkiller .com.
2. Run a program named ckDNSAlert.cmd.
3. Write the event to the Windows event log.
During the course of the day you discover that when a DNS intrusion is detected the event was written to the Windows event log and the e-mail was sent to the specified e-mail account but the ckDNSAlert.cmd program did not execute. You run the batch separately and it works fine. You verify that the user account and validated the account under whose security context the ckDNSAlert.cmd program executes. You also ensure the program has the log on as a batch job right. You are required to ensure the ckDNSAlert.cmd program runs.
What should you do?

A. A System Policy rule must be defined to allow the Local Host network to access the folder in which the ckDNSAlert.cmd program resides.
B. A Firewall access rule should be enabled to allow the Local Host network to access the folder in which the ckDNSAlert.cmd program resides.

C. The user account should be granted the Allow Full Control permission for the folder in which the ckDNSAlert.cmd program resides.
D. The password of the user account under whose security context the ckDNSAlert.cmd program runs should be reconfigured.

Answer: D

Explanation: In the scenario you should remember that you are required to reconfigure the password of the account in question if the program does not run and it has the Log on as batch job right assigned.
Incorrect
Answer:
A, B: These options should not be considered for use in the scenario because the ISA server is referred to as the Local Host network you only require a user account that has the Log on as a batch job right.
C: This option would not help in the scenario because the user already has enough permissions to run the program.

QUESTION 90
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 used to control Internet access both inbound and outbound. The Certkiller .com network security policy states that login for the network daily and monthly summaries should be done for at least 65 days and two years. You make the changes below to the Log summary Properties dialog box of the ISA server:
1. Change the value of the Daily summaries files from the default value of 32 to 66.
2. Change the value of the Monthly summaries field from the default value of 13 to 25.
Later during the course of the day you receive a request from the Certkiller .com management for the daily Web usage summary for the past two months and the monthly Web usage report for the past two years. You then generate the required report and configure it to send an e-mail to the Certkiller .com management with a link to the report. The Certkiller .com management receives the e-mail but complain that they receive a "Page cannot be displayed" message wile attempting to open the link. You open the report from Certkiller -SR01 and check to ensure the report opens properly. You are required to ensure that the Certkiller .com management can access the report.
What should you do?

A. A new folder should be created and specify the path to the new folder in the This folder field on the Log Summary Properties dialog box.
B. The System Policy rule must be enabled to allow the Local Host network to access the internal network by using SMTP protocol.

C. The value of the Daily and Monthly summaries should be changed to the default values.
D. The report should be published to a shred folder.

Answer: D

Explanation: In the scenario you should always remember that in order for user to view the report it is imperative that you first publish the report to a shared folder.
Incorrect Answers:
A, C: This should not be done in the scenario because the report was created successfully. You only need publish it to a shared folder.
B: This should not be done in the scenario because this action should only be used to access the internal network in the scenario.

QUESTION 91
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network recently deployed an ISA server named Certkiller -SR01 used to control Internet access both outbound and inbound. You decided to configure and define the intrusion detection alert in the form of an e-mail when five or more incidents of intrusions are detected by the ISA server. You are required to configure the alert in such a way that the e-mail is sent to you and need to select which options to use.
What should you do?

A. The Report to Windows event log option should be selected on the Actions tab of the Intrusion detected Properties dialog box and enable e-mail forwarding in the Windows Event Viewer.
B. The Run a program option should be selected on the Actions tab of the Intrusion detected Properties dialog box and choose the e-mail service to be launched.
C. The Run a program option should be selected on the Actions tab of the Intrusion detected Properties dialog box and choose a batch file to send the mail to the SMTP service.
D. The Send e-mail option should be selected on the Actions tab of the Intrusion detected Properties dialog box.

Answer: D

Explanation: In the scenario you best choice is to select the send e-mail option on the Actions tab of the Intrusion detected Properties dialog box because Intrusion detection is a feature of ISA which is used to detect when an attack against the server is made.
Incorrect Answers:

A: This option should not be used in the scenario because this option specifies that the event will be written in the Windows Event Log when the alert conditions are met.
B, C: This option should not be used in the scenario because this option specifies that a specific program be run when the alert conditions are met.