ITCertifyhome.com

The Only Way to get Certified Quickly.

Exam :070-227

Title:Install and Admin Internet Security (ISA) Server 2000

Version Number:March,2003

You are now prepared to pass your exam. This ITCertifyhome will provide you with all the knowledge about the real certification exams. We hope you will take full advantage of this tool.

The Use of this ITcertifyhome is strictly for the purchaser. Illegal dissemination is harmful to everyone. So be fair to yourself and us.

For Support, please go to ITcertifyhome.com and click on "Support" link.

For future updates to this ITcertifyhome, please check our website at http://www.ITcertifyhome.com/Login.asp

If the version number has changed for this file, you can download the updated file.

Get ITcertifyhome Product...Get your Certified...
And Get your career moving!

Study Faster. Study Smarter.
Save Time.Save Money.

QUESTION NO: 1
You are the network administrator for your company. You install ISA Server on three computers named ISA-Server1, ISA-server2, and ISA-server3. During installation, you join each server to the same array. You configure each server as shown in this table:

Host Name	Internal IP address	External IP Address	Load factor
ISA_server1	10.10.100.100/24	131.107.200.1/24	100
ISA_server2	10.10.100.101/24	131.107.200.2/24	100
ISA_server3	10.10.100.102/24	131.107.200.3/24	100

Users now report that Internet access is very slow. Using network monitor, you discover that HTTP objects duplicated and cached on all three ISA server computers. You want to reduce traffic over your WAN connection.
What should you do?

A. Resolve requests within the array before routing incoming web requests.
B. Resolve requests within the array before routing outgoing web requests.
C. Increase the load factor on all three computers to 1,000
D. Increase the cache size on the three computers.

Answer: B
Explanation: Apparently the Cache Array Routing Protocol (CARP) is not used in this scenario since HTTP objects are duplicated and cached on all three ISA server computers. CARP would ensure that all ISA servers in the array use the same cache. We can enable CARP by selecting to resolve requests within the array before routing the request. We should enable CARP for outgoing web requests since only Internet access seems to be used in this scenario.

Note: ISA Server uses the Cache Array Routing Protocol (CARP) to provide seamless scaling and efficiency when using multiple ISA Server computers that are arrayed as a single logical cache.

Reference:
Technet, Configuring outgoing Web request properties
Technet, Configuring incoming Web request properties
ISA Server 2000 Administration Study Guide (Sybex), page 289-290, Cache Array Routing Protocol (CARP)
ISA Server 2000 Administration Study Guide (Sybex), page 280, Network Load Balancing

Incorrect Answers
A: The scenario does not mention any incoming web traffic, only Internet access for the local users.
C: The load factor is a relative number that compared the array members with each other. The higher load factor the greater the load. Changing the load factor from the default 100 to 1,000 would not change anything. Each array member would still take 33% of the load.
D: We should ensure that the ISA servers use a single cache. The size of the cache is not the problem in this scenario.

QUESTION NO 2
You are the network administrator for your company. You install ISA Server on a network computer in integrated mode. You configure the firewall service to use the ISA Server file format for logging. You configure the web proxy service to use the W3C extended log file format for logging.
Users now report that access to the Internet is very slow. You use performance monitor to monitor your new server. The results are shown in the exhibit.

You need to configure the ISA server computer to improve logging performance. Which two actions should you take? Each correct answer presents part of the solution. (Choose two.)

A. Monitor for frequently accessed web sites. Create and schedule a content download job for those sites.
B. Configure the logging properties of the firewall service and the web proxy service to limit the number of fields.
C. Modify the firewall service and the web proxy service to log information to an ODBC-compliant database.
D. Increase the size of the URL disk cache on the server.
E. Move the location of the log files for the firewall service and web proxy service to another hard disk drive on the server.

Answer: B, E
Explanation: We must improve logging performance
B: With the W3C log format only the selected fields are included in the log file. This would reduce the size of the log file and increase logging performance.
E: By moving the log file to a separate physical disk, ISA disk access performance would improve.

Note: ISA server supports the following log file formats
• W3C extended file format.
• ISA Server text file format.
• Any Open Database Connectivity (ODBC)–compliant database.

Reference: ISA Server 2000 Administration Study Guide (Sybex), Log File Format, Page 381

Incorrect Answers
A: Downloading the contents of frequently visited sites might improve web access performance, but it would not improve logging performance.
C: Storing log information in an ODBC-compliant database would increase overhead.
D: Increasing the size of the URL disk cache would to make an impact on the logging performance.

QUESTION NO 3
You are the enterprise administrator for your company's network, which consists of one Microsoft Windows 2000 domain and four sites. You plan to deploy the network configuration shown in the exhibit.

The Seattle, Las Vegas, and Atlanta arrays should use the same enterprise policy. Only the Chicago site has a connection to the Internet. You want the other three sites to use dial-up connections to the Chicago site.
The ISA Server computers at the Seattle, Las Vegas, and Atlanta sites should provide Internet access to client computers on the network. At what level should you configure dial-up connections, dial-up entry policy elements, and routing rules at these three sites.
To answer, click the select and place button and drag the check box from the right side to the appropriate empty boxes on the left side. You may reuse the check box as often as necessary. You might not need to fill all the empty boxes.

Quick drop

	At each ISA server computer	At the array level	At the enterprise level	Check box
Dial-up connections				√
Dial-up entry				
Routing Rule				

Answer:

	At each ISA server computer	At the array level	At the enterprise level	Check box
Dial-up connections	√			√
Dial-up entry		√		
Routing Rule		√	√	

Explanation: Only the Chicago site has a connection to the Internet so Dial-up connection must be configured at ISA server level.
Dial-up entries should be defined at the array level.
Routing rules should be defined both at the Array level and at the Enterprise level.

QUESTION NO: 4
You are the network administrator for your company. You install ISA server on a Microsoft Windows 2000 Server computer and configure it with the settings shown in the exhibit.
ISA Management

Name	Scope	Protocol	Action	Applies to	Schedule
FTP_Users	Enterprise	FTP,FTP download only	Allow	Accounts: MILLERTEXTILES\Domain Users	Always
Global Catalog	Enterprise	Any RPC Server	Allow	Any Request	Always
HTTP_Users	Enterprise	HTTP	Allow	Accounts: MILLERTEXTILES\Sales	Always
HTTPS	Enterprise	HTTPS	Allow	Accounts: MILLERTEXTILES\Marketing	Always
LDAP	Enterprise	LDAP GC (Global Catalog)	Allow	Any Request	Always

Mail	Enterprise	POP3, SMTP	Deny	Accounts: MILLERTEXTILES\Graphics	Weekends
NNTP	Enterprise	NNTP,NNTP and NNTPS	Allow	Accounts: MILLERTEXTILES\Sales	Work Hours

Client computers on your network use DHCP.

The Sales group on your network can now access external web sites, but the Marketing group cannot. You need to enable only the Marketing and Sales groups to access external web sites.
What should you do?

A. Add the marketing group to the existing HTTP_Users protocol rule.
B. Add the domain users group to the existing HTTP protocol rule.
C. Create a new site and content rule and add the Marketing group.
D. Create anew destination set and enter the range of IP addresses of the Marketing group computers.
E. Create a new protocol rule to allow the HTTP protocol. Include the IP addresses of the marketing group computers.

Answer: A
Explanation: The Marketing users must be able to access external web sites. This is achieved by enabling the HTTP protocol for this group. The Sales groups already have access to external web sites through the HTTP_Users protocol rule. We enable web access to the Marketing group by adding them to this group as well.

Incorrect Answers
B: Not all domain users should have access to external web sites.
C: A site and content rule would not, by itself, give web access to the Marketing group. A HTTP protocol rule is required.
D: A HTTP protocol rule is required.
E: It is not possible to use the IP addresses of the Marketing group computers since DHCP is used for IP configuration. If static IP addresses was in use this proposed solution would work.

QUESTION NO 5
You are the administrator of an ISA Server computer name FWS2, which has two network adapters. One network adapter connected to the Internet, and the other is connected to your internal network. You want to run a web browser on FWS2 to diagnose connectivity speed to the Internet. You do not want to use the ISA Server cache. You create an IP packet filter named local web browser FWS2. This packet filter applies only to FWS2. It is enabled and can be used by all remote computers. The configuration of the packet filter is shown in the exhibit.

When you Trey Research to use your Web browser on FWS2 to connect to the Internet, ISA server do not allow the connection. How should you correct this problem?

A. Configure ISA Server to enable IP routing.
B. Change the properties of the local web browser packet filter to use the predefined filter named HTTP server.
C. Change the properties of the local web browser packet filter to use a dynamic local port and remote port 80.
D. Create a new protocol rule that applies to FWS2 and allows the use of the HTTP protocol to access the Internet.
E. Configure your web browser to use a proxy server. Specify the internal IP address of FWS2 and the TCP port for outgoing web requests.

Answer: C
Explanation: We don't want to use caching on ISA Server so we cannot use the local port 80. Instead we have to create a dynamic local port and a static remote port 80.

Incorrect Answers
A: We want to disable caching. Routing does not affect caching.

B, D, E: We must disable caching

QUESTION NO: 6
You administer your company network, which includes an ISA server computer. This computer is connected to the Internet by means of a 56-Kbps dial-on-demand connection. You configure routing and remote access to connect the network to your local ISP.
Using network monitor, you discover that daily network traffic over the 56-Kbps connection is nearing capacity. You need to configure ISA server to decrease the volume of HTTP traffic over this connection during working hours. You also need to allocate as much bandwidth as possible to users during working hours.
What should you do?

A. Create a new bandwidth rule for HTML documents and configure it with an inbound bandwidth priority of 100.
B. Create a new bandwidth rule for HTML documents and configure it with an inbound bandwidth priority of 10.
C. Schedule content downloads from frequently visited web sites to occur during working hours.
D. Schedule content downloads from frequently visited web sites to occur during non-working hours.

Answer: D
Explanation: The ISA Server scheduled content download feature downloads the Hypertext Transfer Protocol (HTTP) content directly to the ISA Server cache, upon request or as scheduled. It updates the ISA Server cache with HTTP content that you anticipate will be requested by clients in your organization. This content will be available for access directly from the ISA Server cache, rather than from the Internet. By scheduling this download to non-working hours, HTTP traffic would decrease during working hours.

Reference:
ISA Server 2000 Product Guide, Scheduled Content Download, Page 22
ISA Server 2000 Administration Study Guide (Sybex), Creating Bandwidth Rules, Page 271

Incorrect Answers
A: 100 is the default bandwidth priority. Nothing would be changed.
B: A bandwidth priority of 10 would increase the priority of HTTP traffic. HTTP traffic would not be decreased-
C: The content download must not be scheduled during working hours. We want to decrease HTTP traffic during working hours.

QUESTION NO: 7
You are the administrator of your company's ISA server computer. Users need to connect to an internal Microsoft Windows 2000 Server computer named TS1, which runs Terminal services. TS1 is configured

as a SecureNAT client. However, when you run the server publishing wizard, you cannot select the Terminal services protocol.
You need to configure your ISA server computer to provide external access to TS1. What should you do?

A. Install the firewall client software on TS1. Ensure that the mspcint.ini file is downloaded to the directory where the firewall client software is installed.
B. Create a protocol definition for the remote desktop protocol. Specify the direction as inbound with no secondary connections.
C. Install the firewall client software on TS1. Create a wspcfg.ini file for the remote desktop protocol settings. Place the file in the directory where the firewall client software is installed.
D. Create a protocol definition for the remote desktop protocol. Specify the direction as outbound and configure a secondary connection for TCP ports above 1042.

Answer: B
Explanation: Terminal Services use the Remote Desktop Protocol (RDP). The Terminal session will be initiated from client computer TS1. We must therefore allow inbound RDP traffic. There already exists a predefined Protocol Definition for RDP. However, we create a new protocol definition for RDP and specify the direction as inbound only.

Reference: Technet, ISA Server Product Definition, Configuring protocol definitions

Incorrect Answers
A, C: We must allow RDP traffic.
D: The Terminal services session will be initiated at the client. We must allow inbound, not outbound, RDP traffic.

QUESTION NO: 8
You are the network administrator for Fabrikam,Inc. Your company specializes in manufacturing and selling fly fishing reels. Quarterly sales are declining. To increase sales, management wants you and your staff to create and maintain an Internet storefront.
You install and configure ISA server and Internet information services 5.0 on six computers. You also install network load balancing on each one. You configure all six with an NLB cluster whose IP address is 131.107.200.10/24. Each computer is now configured as shown in this table:

Host Name	Internal IP Address	External IP Address	Load Factor
ISA-server1	10.10.100.100/24	131.107.200.1/24	100
ISA-server2	10.10.100.101/24	131.107.200.2/24	25
ISA-server3	10.10.100.102/24	131.107.200.3/24	100
ISA-server4	10.10.100.103/24	131.107.200.4/24	25
ISA-server5	10.10.100.104/24	131.107.200.5/24	200
ISA-server6	10.10.100.105/24	131.107.200.6/24	100

Using network monitor, you discover that your communication link to the Internet is operating at full capacity. However, only two of the computers are processing orders.
You need to reconfigure your ISA server computers to handle inbound and outbound traffic more efficiently. Which three actions should you take? Each correct answer presents parts of the solution. (Choose three)

A. Add a host record for the web site name with the IP address 131.107.200.10.
B. Change the client computer configuration to use secure network address translation.
C. Configure each computer with the internal IP address for intra-array communication.
D. Install DNS one ach computer and implement round-robin DNS.
E. Change the load factors on ISA-server2 and ISA-server4 to 1
F. Choose the use Automatic Configuration Script option on client Web browsers and include the address of the script.

Answer: A, C, F
Explanation:
A: The clients must be able to resolve a host name to the NLB cluster. We must add a host record mapping the web site name to the IP address of the cluster.
C: The computers in the cluster must be set up for intra-cluster communication.
F: The Automatic Configuration Script option is used for a distributed Web cache which has been set up using Cache Array Routing Protocol (CARP). It distributes the URL cache evenly across a group of ISA servers..

Reference:
ISA Server 2000 Administration Study Guide (Sybex), Enabling and Configuring NLB, Pages 281-287
Technet, ISA Server 2000 Product Documentation, Using Network Load Balancing

Incorrect Answers
B: There is no need to use SecureNAT clients.
D: There is no need to install DNS on each client. Furthermore, NLB is used so there is no need to use Round Robin DNS for load balancing.
E: With a load factor of 1 server2 and server4 would hardly be used at all. This would not improve performance.

QUESTION NO 9
You are the administrator of your company network. You install ISA server with default settings on a network computer. You install the firewall software on client computers and configure then to use an automatic configuration script.
You configure the logging and reporting properties on the ISA server computer and create a report job. It generates the report shown in the exhibit.

Microsoft Internet Security & Acceleration Server 2000

Traffic and Utilization Report
Saturday, October 28, 2000 to Thursday

Cache Hit Ratio Chart

Status	Requests	% of Total Requests
Object returned from the Internet, updating an existing file in the cache	423	83. 1 %
Object returned from the cache after verifying that it has not been modified	49	9. 6 %
Object returned from the cache without verification	32	6. 3 %
Object returned from the Internet	10	2. 0 %
Object returned from another array member	0	0. 0 %
Source information unavailable, error or undefined	0	0. 0 %
Total	**509**	**100 %**

You need to configure ISA Server to improve performance for network users. What should you do?

A. Enable active caching and configure it to reduce network traffic. Configure scheduled content download jobs to include frequently visited web sites. Decrease the time-to-live settings for cached HTTP objects.
B. Enable active caching and configure it to retrieve files more frequently. Configure scheduled content download jobs to include frequently visited web sites. Increase the time-to-live settings for cached HTTP objects.
C. Enable HTTP caching. Configure scheduled content download jobs to include frequently visited web sites. Increase the time-to-live settings for cached HTTP objects.
D. Enable HTTP caching. Configure the ISA server computer to route outgoing web requests to an upstream proxy server. Decrease the time-to-live setting for cached HTTP objects.

Answer: B
Explanation: Active caching automatically retrieves frequently accessed files. With active caching enabled, ISA Server analyzes objects that are in the cache to determine which are most frequently accessed. When popular objects in the cache get ready to expire, ISA Server automatically refreshes the content in the cache. We should enable active caching and configure it to retrieve files frequently (default setting is normally). See picture. These settings can be configured in ISA management Console->Servers and Arrays->Server->Right-click Cache configuration->Properties->Active Caching.

Furthermore, we should ensure that cached HTTP objects do not expire before they are refreshed. We should therefore increase the time-to-live setting for cached HTTP objects.

Reference:
Technet, ISA Server Product Documentation, Configuring active caching

Incorrect Answers

A: Active Caching with the Less Frequently option reduce network traffic, but the cache will contain less fresh objects, especially if we decrease the time-to-live setting for cached HTTP objects as well. This is not the optimal configuration to improve performance for network users.

C: By looking at the exhibit we see that HTTP caching is already enabled (it is enabled by default). Scheduled content download from frequently visited web sites and increased TTL of HTTP objects could improve performance. However, active caching would most likely improve performance further.

D: By looking at the exhibit we see that HTTP caching is already enabled (it is enabled by default). Furthermore there is no mention of a upstream proxy server in the scenario.

QUESTION NO 10

You are the administrator of your company network. The relevant portion of its configuration is shown in the exhibit.

ISA-server2 is configured to allow inbound VPN connections. You create a VPN connection on VPN-client1 to connect to ISA-server1. Now you need to allow the users of VPN-client1 to access resources on the finance server.
What should you do?

A. On ISA-server1, enable IP routing and enable the PPTP IP protocol to pass through the firewall. Configure VPN-client1 as a SecureNAT client.
B. On ISA-server2, enable IP routing and enable the PPTP IP protocol to pass through the firewall. Configure VPN-client1 as a SecureNAT client.
C. Run the remote ISA VPN wizard on ISA-server1. Install the firewall client software on VPN-client1.
D. Run the remote ISA VPN wizard on ISA-server2. Install the firewall client software on VPN-client1.

Answer: A
Explanation: We must configure the remote ISA Server, the ISA Server closest to the Finance Server. We should enable IP routing and allow the PPTP protocol to pass through the firewall. Furthermore, we should set up the client computer as a SecureNAT client.

Note: ISA Server includes three wizards that you can use to create ISA VPN connections:
* Local ISA VPN Wizard. Use this wizard to set up the ISA Server computer that receives connections. The local ISA VPN Server can also be set up to initiate connections.
* Remote ISA VPN Wizard. Use this wizard to set up the ISA Server computer that initiates and receives connections.
* Set Up Clients to ISA Server VPN Wizard. Use this wizard to allow roaming users to connect to the VPN.

Reference:
Technet, ISA Server Product Documentation, Using an ISA Server virtual private network
ISA Server 2000 Administration Study Guide (Sybex), Configuring ISA Server for VPN Tunnels, page 218.

Incorrect Answers
B: We must configure ISA Server 1, not ISA Server 2.

C, D: There already exists a VPN connection between the two ISA Servers. There is no need to run the Remote ISA VPN Wizard.

QUESTION NO: 11
You are the network administrator for your company. You install and configure ISA server with default setting on a network computer. Users in your sales group configure their e-mail software to download e-mail from the Internet. However, when they try to send or receive e-mail, they cannot access e-mail servers on the Internet.
You need to configure your ISA server computer to allow only the sales group to send and receive e-mail. What should you do?

A. Create a SMTP protocol rule and POP3 protocol rule to allow external access. Configure each rule to include the sales group.
B. Create a SMTP server protocol rule and POP3 protocol rule to allow external access. Configure each rule to include the sales group.
C. Create and enable a DNS lookup packet filter to allow external access configure the packet filter to use port 53.
D. Create a new protocol rule for Internet access. Configure the rule to allow access for the sales group.

Answer: A
Explanation: We must enable the sending and receiving of e-mails. The SMTP protocol is used to send e-mails and the POP3 protocol is used to retrieve e-mails. We create rules for these protocols that allow external access. We then configure each rule to include the appropriate group of users.

Note: Protocol is used to define which protocols are specifically allowed or denied. The rules can be applied to all users or only to a specific group of users.

Reference: ISA Server 2000 Administration Study Guide (Sybex), Protocol Rules, Pages 258-259

Incorrect Answers
B: There is no such thing as a SMTP server protocol, there just is a SMTP protocol.
C: DNS does not apply in this e-mail scenario. There is no name resolution problem at hand.
D: We only need to allow e-mail traffic, not Internet access in general.

QUESTION NO: 12
You administer an array of ISA server computers. This array makes your company's public web site available to Internet users. The relevant portion of your network configuration is shown in the exhibit.

The ISA server array has one web publishing rule for incoming web requests. Each array member is configured to use cache of 5 GB. The web servers use Network Load Balancing (NLB).
When you monitor network traffic between the ISA server array and the web servers, you notice that the same web objects are cached by more than one of the array members.
You need to configure your network so that the array behaves as one logical cache of 15 GB. What should you do?

A. Configure NLB on the external network adapter of the three array members.
B. Configure a single IP address for intra-array communication on each array member.
C. Configure a cache load factor of 100 for each array member.
D. Configure a routing rule on each array member to forward inbound requests to the other array members.
E. Configure the array to resolve inbound web requests within the array before routing.

Answer: E
Explanation: ISA Server uses the Cache Array Routing Protocol (CARP) to provide seamless scaling and efficiency when using multiple ISA Server computers that are arrayed as a single logical cache. We enable the Cache Array Routing Protocol (CARP) by selecting to resolve requests within the array before routing the

request. We can enable CARP separately either for incoming or outing Web requests. In this scenario we should enable it for incoming web requests.

Reference:
Technet, Configuring incoming Web request properties
Technet, Cache Array Routing Protocol
ISA Server 2000 Administration Study Guide (Sybex), Cache Array Routing Protocol (CARP), Pages 289-290

Incorrect Answers
A: NLB is configured on the internal interfaces in the array.
B: A single address cannot be used for intra-array communication. Each ISA server must have an unique internal IP address.
C: A cache load factor of 100 is a default setting. Furthermore, cache load factor configuration would not enforce one single logical cache.
D: Routing is not used in the internal ISA array.

QUESTION NO 13
You are the administrator for your company. You install ISA server on a network computer and configure a report job. You use an NTFS simple volume for logging and reporting. When you examine event viewer a month later, it reports that your disk is full.
You want ISA logging and reporting to continue to create log files, but you also want to limit the amount of disk space used by these files. Which two actions should you take? Each correct answer presents part of the solution. (Choose two)

A. Configure the logging properties of the Web proxy service, the firewall service, and the packet filters to limit the number of log files.
B. Configure the logging properties of the Web proxy service, the firewall service, and the packet filters to use the ISA Server file format.
C. Configure the logging properties of the web proxy service, the firewall service, and the packet filters to create a new log monthly.
D. Configure logging properties of the web proxy service and the packet filters to use the W3C file format.
E. Configure the logging properties of the web proxy service, the firewall service and the packet filters to use a logging format with the minimum number of fields.

Answer: A, E
Explanation: The ISA log files are filling up the hard drive.
A: We should first limit the number of log files. See picture below. This setting is reached from ISA Management->Servers and Arrays->Monitoring Configuration->ISA Server Web Proxy Service (or Packet filters or ISA Server Firewall service)->Fields.

E: To decrease the size of the log files we should only select a minimum amount of fields in the log file. If we use W3C log file format (default) the log files will only include the selected fields. See picture below. This setting is reached from ISA Management->Servers and Arrays->Monitoring Configuration->ISA Server Web Proxy Service (or Packet filters or ISA Server Firewall service)->Fields.

Reference: ISA Server 2000 Administration Study Guide (Sybex), Log File Formats, Page 381

Incorrect Answers

B: The W3C log file format (default format) is preferred to the ISA log file format. The logs produced with the W3C format only include the selected fields contrary to the ISA format.

C: In one month the disk filled up, so a single log file for a whole month is not a good idea.

D: The W3C log file format should be used. However, it is selected by default so it should be no need to configure this setting. Furthermore, if this configuration should be applied it should be applied to all logs including the ISA Server Firewall service.

QUESTION NO 14

You are the network administrator for your company. You install and configure ISA server on a network computer and configure it to allow web access. You configure all client computers as firewall clients. Users report that traffic over the company's WAN link is very slow. Using network monitor, you investigate network traffic on the ISA server computer.

You need to reconfigure the ISA server computer so that only company-approved HTTP traffic is allowed to pass through it. What should you do?

A. Disable LCP extensions on the dial-up connection.
B. Disable MS-CHAP authentication on the dial-up connection.
C. Disable L2TP and IKE packet filters.
D. Disable the PPTP through ISA firewall setting.

Answer: D
Explanation:
. See picture below. This setting is reached from ISA Management console->Access Policy->Right-click IP Packet Filters->PPTP.

Reference:
How to Enable PPTP Clients to Connect Through an ISA Firewall (Q283628)

Incorrect Answers
A: There is no dial-up connection in this scenario.
B: There is no dial-up connection in this scenario.
C: There are no predefined L2TP or IKE packet filters.

QUESTION NO 15
You are the administrator of your company network, which includes a single Microsoft Windows 2000 domain. Currently, the network does not run ISA Server. You plan to install ISA sever on a computer named server1, which is a member server in the domain.
The ISA Schema initialization tool successfully updates the schema. However, when you run the ISA server setup on Server1, you receive this error message:

You want to install server1 as the first member of an ISA server array. What should you do?

A. Stop the installation of ISA server. On the Windows 2000 domain controller, rerun the initialization tool to modify the Active Directory schema. Log on to server1 as a local user with administrative privileges and the same credentials as the schema administrator. Rerun the ISA server setup.
B. Continue the installation of ISA server. After the installation is complete, log on to server1 as the enterprise and schema administrator for the domain. Run msisaent.exe to modify the Active Directory schema.
C. Stop the installation of ISA Server. Log on to server1 with a domain account that is a member of the enterprise admins group. Rerun the ISA Server setup.
D. Stop the installation of ISA Server. Log on to server1as a member of the enterprise admins group and the schema admins group. Run dcpromo.exe to promote server1 to a Windows 2000 domain controller. Rerun the ISA Server setup.

Answer: C
Explanation: There are three possible causes of this message:

- The ISA server is not part of a Windows 2000 domain.
  This does not apply in this scenario. The computer is a member server of the domain.
- The ISA Server schema is not installed in Active Directory.
  This does not apply in this scenario. The ISA Server schema has already successfully been installed.
- You do not have permission to access the schema.
  This is the cause of the problem.

Reference:
Windows 2000 Server Cannot Join Existing ISA Array (Q295654)

Incorrect Answers

A: The ISA server schema is already successfully installed. Furthermore a domain account, not a local account, must be used when installing an ISA array server.
B: The ISA server schema is already successfully installed. Furthermore, we the schema must be added before the ISA Server installation, not after.
D: There is no requirement to use Domain Controllers as members of ISA arrays. On the contrary, the extra overhead of the Domain Controller services are counter-productive.

QUESTION NO 16
You are the administrator of your company network, which is configured as shown in the exhibit.

You install and configure ISA Server with default settings on ISA-Server1 and ISA-Server2. You also install and configure a modem on each server. Users at the main office can now access the Internet, but users at the branch office cannot.
You need to enable users in the branch office to access the Internet. You also need to configure ISA-server2 to automatically connect to ISA-server1.
What should you do?

A. Create a network dial-up connection named MainOffice on ISA-server2. Create a new dial-up entry on ISA-server2. Select MainOffice as the active network dial-up connection. Configure the default routing rule to use the dial-up entry for the primary route.
B. Create a network dial-up connection named MainOffice on ISA-server1. Create a new dial-up entry on ISA-server1. Select MainOffice as the active network dial-up connection. Configure the default routing rule to use the dial-up entry for the primary route.

C. Configure routing and remote access on ISA-Server2. Create and configure a dial-on-demand interface named MainOffice. Add a routing rule on ISA-server1.
D. Configure routing and remote access on ISA-Server1. Create and configure a dial-on-demand interface named MainOffice. Add a routing rule on ISA-server1.

Answer: A
Explanation: ISA Server2 must be able to access Server1. We must configure ISA dial-up connection on Server2. First a dial-up connection is created. Then a dial-up entry must be created on the ISA server. Finally we make sure that external requests are routed to ISA Server 1. This can be accomplished be a default routing rule that use the dial-up entry as the primary route.

Reference:
ISA Server 2000 Administration Study Guide (Sybex), Set up and troubleshoot dial-up connections and Routing and Remote Access dial-on demand connections, Page 166, Page 203

Incorrect Answers
B: The ISA dial-up connection must be created on Server2, not on Server1. Server2 want to access Server1.
C: The routing rule should be added on Server2, not on Server1.
D: Server2 must access Server1, not the other way around.

QUESTION NO: 17
You are the administrator of your company network. You install ISA server on the network to provide firewall services. Subsequently, network users report that they are receiving large amounts of unsolicited e-mail. On investigation, you discover that all the unsolicited e-mail is coming from the same Internet domain
You want to block all e-mail coming from this domain. What should you do?

A. Create a destination set and a site and content rule to prohibit access to this domain.
B. Create a protocol rule that allows only authorized users to use the SMTP (server) protocol.
C. Enable the POP intrusion detection filter to block e-mail access from this domain.
D. Enable the SMTP filter and add this domain name to the list of rejected domains.

Answer: D
Explanation: The Simple Mail Transfer Protocol (SMTP) filter is an application filter that intercepts all SMTP traffic that arrives on port 25 of the ISA Server computer. The filter accepts the traffic, inspects it, and passes it on only if it the rules allow it. The SMTP filter can filter incoming mail based on source user or domain. The SMTP filter also maintains a list of rejected domains. Messages from users in those domains are also rejected. See the picture below. This setting is reached by ISA Management Console->Extensions->Applications->Right-click SMTP filter->Properties->Users/Domains.

Reference:
Technet, ISA Server Product Documentation, SMTP filter
Technet, ISA Server Product Documentation, Integrated Intrusion Detection

Incorrect Answers
A: Only e-mail traffic from this specific domain should be blocked, not access in general.
B: We want to block e-mail from a specific domain, not unauthorized users in general.
C: The POP intrusion detection filter intercepts and analyzes POP traffic destined for the internal network. The filer checks for POP buffer overflow attacks. However, you cannot configure this filter to block access from specific domains (see picture below).

QUESTION NO 18
You are the network administrator for your company. You install ISA Server with default settings on the network computer.
You need to configure the ISA server computer to log web proxy service information into an ODBC-compliant database. You want to complete this task with the least possible administrative effort. What should you do?

A. Modify and execute the Msp.sql script file to define a new table for the web proxy service. Define the data source name and the table name within the firewall service properties. Specify an account that has the ability to update the table. Configure the database application to automatically start at startup.
B. Modify and execute the W3p.sql script file to define a new table for the web proxy service. Define the data source name and the table name within the Web proxy service properties. Specify an account that has the ability to update the table. Configure the database application to automatically start at startup.
C. Create a new table named WEBEXT.log. Enter the name of the table in the logging properties of the web proxy service. Enter the data source name of the table.

D. Create a database table called WebProxyLog within the database application. Specify administrator credentials to use for access to the database. Enter the data source name.

Answer: B
Explanation: First we should should modify and execute the W3p.sql script file to define a new table for the web proxy service in the ODBC database. Then we should use Web Proxy Service Properties to configure the logging of web proxy information into the ODBC database. We specify the ODBC data source (DNS), the table name, and the account information (see below). This setting is reached from the ISA Management Console->Monitoring Configuration->Logs->Right-click ISA Server Web Proxy Service->Properties.

Incorrect Answers
A: We want to monitor web proxy server information, not firewall service information.
C: We must set account information for the ODBC database.
D: We must use the Web Proxy Service properties to define the name of the table.

QUESTION NO 19
You are the administrator of your company network. You install ISA Server with default settings on a network computer. This computer is configured with the W3C extended logging file format.

The next day you create a report job. You run the job immediately, but no Web-based report documents are generated. The default log directory contains log files.
You configure your ISA server computer to generate a daily report of application and web usage. However, when you view the report, it contains no data.
What should you do?

A. Create a report job to be scheduled immediately. View the reports following morning.
B. Create a report job to be scheduled immediately. View the reports immediately.
C. Enable logging for the firewall service and the web proxy service. Create a report job to be scheduled immediately. Import the FWSEXTDyyyymmdd.log into an HTML editor.
D. Enable logging for the firewall service and the web proxy service. Change the logging format to the ISA Server file format. Import the WEBEXTDyyyymmdd.log into an HTML editor.

Answer: A
Explanation: We must create a report job and schedule it to run immediately. The report job will not finish immediately however, so we have to let it run.

Note: The ISA Server reporting mechanism enables you to schedule reports, based on the data collected from the log files. You can schedule reports to be generated on a recurring, periodic basis: daily, weekly, monthly, or yearly.

Reference:
ISA Server help, Scheduling reports
ISA Server 2000 Administration Study Guide (Sybex), Reporting, page 384

Incorrect Answers
B: This is a daily report and it will not be finished immediately.
C: Log files already exists.
D: Log files already exists.

QUESTION NO 20
You are the administrator of your company network, which is connected to an ISP by a 56-Kbps dial-on-demand connection. You install ISA Server with default settings on a network computer. You enable and configure routing and remote access on this computer.
You then monitor Internet usage from the ISA server computer and create a report job wit default settings. The results are shown in the exhibit.

Microsoft Internet Security & Acceleration Server 2000

Traffic and Utilization Report
Saturday, October 28, 2000 to Thursday

Cache Hit Ratio Chart

Status	Requests	% of Total Requests
Object returned from the Internet, updating an existing file in the cache	945	67.9 %
Object returned from the cache after verifying that it has not been modified	532	38.2 %
Object returned from the cache without verification	61	4.4 %
Object returned from the Internet	96	6.9 %
Object returned from another array member	0	0.0 %
Source information unavailable, error or undefined	23	1.7 %
Total	**1391**	**100 %**

You need to optimize network traffic. What should you do?

A. Configure the active cache settings to de more pre-fetching. Increase the time-to-live settings for cached HTTP objects.
B. Increase the disk cache size on the ISA server computer. Decrease the time-to-live settings for cached HTTP objects.
C. Add another hard disk drive. Configure the cache settings on the ISA server computer to use the additional hard disk drive.
D. Configure the advanced cache configuration to cache dynamic content. Create a new bandwidth rule and include HTTP.

Answer: A
Explanation: With active caching, objects that are frequently accessed are automatically updated before they expire, during periods of low network traffic. More pre-fetching of the active cache optimizes network traffic. Furthermore, by increasing the time to live setting we ensure that the HTTP objects will stay in the cache for a longer time, further optimizing network traffic.

Reference: ISA Server 2000 Product Guide, Active Caching, Page 22

Incorrect Answers
B: Decreasing the time to live setting of the HTTP objects will remove objects from the cache earlier. This ensures that the cache contains fresh objects, but it would not optimize network traffic.
C: Increasing the size of the disk cache could improve network performance, but not as much as more pre-fetching with active caching.
D: Caching dynamic content (object with question marks in the URL) would not improve network performance much since the dynamic content is not reused much.

QUESTION NO: 21
You are the administrator of an ISA server computer that is connected to the Internet. Your internal network consists of one Microsoft Windows 2000 domain. All client computers run either Windows 2000 Professional, Windows NT workstation 4.0, or Windows 98. All users are members of the domain.
You are planning the deployment of ISA server. You want to accomplish these goals:

- **Allow all users to access Internet sites, except for members of the security group named Summer Workers.**
- **Allow a maximum of five computers to connect concurrently to Internet sites through the ISA server computer.**

You need to configure ISA server to accomplish these goals. Which four actions should you take? Each correct answer resents part of the solution. (Choose four)

A. Configure the security settings on ISA server to deny permissions to summer workers.
B. Create a new site and content rule that applies to Summer Workers and denies access to all destinations.
C. Create a new protocol rule that allows the use of the HTTP protocol.
D. Create a new IP packet filter that allows the use of the HTTP protocol.
E. For outgoing web requests, allow a maximum of five connections.
F. For outgoing web requests, configure listeners individually per IP address. Use five different internal IP addresses.
G. For outgoing web requests, ensure that unauthenticated users are asked for identification.

Answer: B, C, E, G
Explanation:
B: We must allow users, except members of the Summer Workers, access to Internet sites. This is achieved by the site and content rule.
C: We allow the use of the HTTP protocol with a protocol rule. Protocol rules are dynamic and are preferred to the static IP packet filter rules.
E: We use the **Connection Settings** for the **Outgoing Web Requests** to define the maximum number of outgoing connections (see below). This configuration is reached from ISA Management console->Right-click on the Server->Properties->Outgoing Web Requests.

G: We select the **Ask unathenticated users for identification** in **Coonnection Settings** for **Outgoing Web Requests** (see above) to ensure that no unauthorized users will gain Internet access.

Reference:
ISA Server help, IP Packet filters
Technet, About ISA Server rules

Incorrect Answers
A: ISA server security settings applies to access to the ISA Server itself, not to Internet access.

D: It is usually recommended that you create access policy rules, not IP packet filters, to allow internal clients access to the Internet This is because IP packet filters open the ports statically, but the access policy and publishing rules open the ports dynamically (as a request arrives).
F: Listeners could be used when we got several internal web sites that we want to make public through the ISA Server. Listeners do not apply in this scenario.

QUESTION NO: 22
You are the administrator of your company network, which consist of a single Microsoft Windows 2000 domain. All client computers run Windows 2000 Professional and use DHCP for their network configuration. ISA Server is installed in firewall mode. All client computers are configured as SecureNAT clients.
To prevent access to unauthorized web sites and content, you delete the default site and content rule. You also create protocol rules that allow only company-approved protocols to be used.
Your company uses a custom front-end application to access a project coordination application, which is hosted on the internal networks of several partners. The application uses HTTP to access the web sites of your partners, and it uses TCP port 15002 to make its initial connection to the application. It then uses TCP ports 25002 through 26001 for secondary connections, as needed.
You create a custom definition to allow the application to make its initial connection and all secondary connections. You create a custom application filter to support all connections. You register the filter with the firewall service and enable it.
Users now report that they cannot access the project coordination application. Which two actions should you take to correct this problem? Each correct answer presents parts of the solution. (Choose two)

A. Create a new packet filters to allow application traffic in both directions.
B. Disable all packet filtering on the external interface of ISA Server.
C. Create a site and content rule that allows users to access the web sites of your partners.
D. Create a protocol rule that uses your custom protocol definition. This rule allows users to access the protocols used by the custom application.
E. Create a protocol rule that allows all IP traffic. This rule allows users to access the protocols used by the custom application.

Answer: C, D
Explanation:
C: Since the default site and content rule was deleted we must create a new site and content rule.
D: To allow the customer application protocol we create a protocol rule that uses the custom protocol definition.

Reference:

Incorrect Answers

A: Packet filters are static: they keep ports open for traffic all the time. Instead we must use a protocol rule which is able to open and close ports dynamically.
B: .We should not allow all IP traffic.
E: We should only allow traffic through the propriety protocol. We should not allow all IP traffic.

QUESTION NO: 23
Your network consists of 3,500 Microsoft Windows 2000 Professional computers in one Windows 2000 domain. You administer an array of four ISA server computers that are connected to the internet. Company policy states that users on the internal network should be denied access to the entire www.litwareinc.com website. This policy has one exception; Members of the Software admins group should be allowed to access www.litware.com/apps/patches, but they should not be allowed to access any other area of www.litware.com
After the company policy is implemented on the ISA server array, members of the software admins group report that they cannot access www.litware.com/apps/patches you examine the site and content rules that apply to www.litware.com these rules are configured as shown here:

Name	Scope	Action	Applies to	Schedule	Destination	Content
Allow all destinations	Enterprise	Allow	Any request	Always	All	All
Litware site	Enterprise	Deny	Any request	Always	Litware entire site	All
Litware patches	Enterprise	Allow	Accounts: Software Admins	Always	Litware Patches	All

The destination set named "Litware entire site" applies to www.litwareinc.com the destination set named "Litware patches" applies to www.litware.com/apps/patches
You want to ensure that the company's policy regarding access to www.litware.com and www.litware.com/apps/patches is applied correctly. Which two actions should you take? Each correct answer presents part of the solution. (Choose two)

A. Modify the Allow All rule to apply to all destinations except the destination set named "Litware entire site"
B. Create a new group that includes all users except members of the Software Admins group. Modify the Litware Site rule to apply to this group.
C. Reverse the order of the Litware site rule and the Litware patches rule.
D. Delete the Litware site rule from the list of site and content rules.
E. Create a new routing rule that applies to the destination set named "Litware patches". Configure the rule to send requests to the Internet.

Answer: A, D

Explanation: The Deny rule prevents all users from accessing any source on the Litware site since a Deny rule always overrides Allow rules.
D: We should therefore remove the Deny rule.
A: We must also modify the Allow all rule to include an exception of the destination set of the Litware site. See picture below.

Note: When ISA Server processes an outgoing request, it checks routing rules, site and content rules, and protocol rules to determine if access is allowed. A request is allowed only if both a protocol rule and a site and content rule allow the request and if there is no rule that explicitly denies the request.

Reference: Platform SDK: Internet Security and Acceleration Server 2000, Controlling Outgoing Requests

Incorrect Answers
B: Creating groups that include all users except members of the Software Admins groups is an incorrect way to try to solve the problem. Members of the Software Admins groups can very well be members of others group. It is therefore impossible to create such a group.
C: The Deny rule will override the Allow rules even though it is moved to the end.
E: A routing rule would not affect the site and content rules.

QUESTION NO 24
You are the administrator of your company network. You recently upgraded your Microsoft proxy server 2.0 computer to ISA server. Before the upgrade, the proxy server computer was your web server. It also published web content on the Internet. After the upgrade, you discover that the web server component on the ISA server computer no longer functions.
You issue a command to view the active connections on the ISA server computer. The output of the command is shown in the exhibit.

```
Select C:\WINNT\System32\cmd.exe-cmd

Active Connections

Protocol    Local Address          Foreign Address    State

TCP         0.0.0.0:135            0.0.0.0:0          LISTENING
TCP         0.0.0.0:445            0.0.0.0:0          LISTENING
TCP         0.0.0.0:1050           0.0.0.0:0          LISTENING
TCP         0.0.0.0:1051           0.0.0.0:0          LISTENING
TCP         0.0.0.0:1062           0.0.0.0:0          LISTENING
TCP         0.0.0.0:1062           0.0.0.0:0          LISTENING
TCP         0.0.0.0:1144           0.0.0.0:0          LISTENING
TCP         0.0.0.0:1723           0.0.0.0:0          LISTENING
TCP         0.0.0.0:3372           0.0.0.0:0          LISTENING
TCP         131.107.2.1:139        0.0.0.0:0          LISTENING
TCP         131.107.2.1:1154       0.0.0.0:0          LISTENING
TCP         131.107.2.1:139        192.168.0.1:139    ESTABLISHED
TCP         192.168.0.254:139      0.0.0.0:0          LISTENING
```

You want to restore web server functionality to the ISA server computer. You will use the Microsoft Management Console (MMC) to accomplish this goal.
Which two actions should you take? Each correct answer presents part of the solution. (Choose two)

A. In the MMC for Internet information services, change the port used by the web server to TCP port 8080. Start the WWW publishing Service.
B. In the MMC for Internet information services, change the port used by the web server to TCP port 81. Start the WWW publishing Service.
C. In the MMC for Internet information services, create a site and content rule that allows IP traffic to all internal destinations.
D. In the MMC for ISA server, create a web publishing rule that redirects external HTTP requests to the internal network adapter of the ISA server.
E. In the MMC for ISA Server, create a packet filter that allows external traffic on the TCP port used for HTTP requests.

Answer: B, D
Explanation:
D: If IIS is installed on the ISA Server computer, you can publish IIS by configuring Web publishing rules.
B: Furthermore, IIS must be configured not to use the ports that ISA Server uses for outgoing Web requests (by default, port 8080) and for incoming Web requests (by default, port 80). We can for example use TCP Port 81.

Reference:
Technet, ISA Server Production Information, ISA Server and IIS Server
ISA Server help, Web publishing rules

Incorrect Answers
A: TCP port 8080 cannot be used since ISA Server uses it for outgoing Web requests.
C: We must use Web publishing rules, not Site and content rules.
E: We must use Web publishing rules, not packet filters.

QUESTION NO: 25
You are the administrator of an array of two ISA server computers. Your company network consists of one Microsoft Windows 2000 domain. All client computers run Windows 2000 Professional, and all users access Internet resources through the ISA server array. Company policy states that you cannot install the firewall client software or configure the web proxy service on any client computers.
The ISA server array has access policy rules that allow everyone to use the HTTP protocol to access all sites on the Internet. The array is configured for outgoing web requests as shown in the exhibit.

Users on the network now report that they cannot access Internet sites. However, they can use the Microsoft MSN messenger service to connect to the Internet. They can also use POP3 and SMTP servers on the Internet to send and receive e-mail.
You need to ensure that all users can access Internet sites. What should you do?

A. Change the authentication method to basic authentication.
B. Change the TCP listener to use port 80.
C. Disable the option to ask unauthenticated users for identification.
D. Disable the option to resolve requests within the array.

Answer: C
Explanation: The exhibit shows that the **Ask unauthenticated users for identification** option is selected. This option requires the clients to use either firewall client software or configure the web proxy service but we are not allowed to use those. We should therefore disable this setting. Furthermore, there is requirement need for authentication in this scenario.

Incorrect Answers
A: Windows 2000 clients would not require basic authentication.

B: TCP listeners does not apply in this scenario.
D: The resolve requests within the array option is only used to improve performance. Changing it would not solve the problem at hand.

QUESTION NO: 26
You are the administrator of your company network, which consists of a main office and two branch offices. The network includes three Microsoft 2000 domains, each in a separate forest. Company policy states that no trust relationships can exist between the domains.
The main office has a T1 connection to the Internet. The branch offices connect to the main office with dedicated 256-Kbps lines. The branch offices have no direct connection to the Internet.
You deploy ISA server arrays in integrated mode at each location. You want all Internet requests from the branch offices to be routed through the ISA server array in the main office. You also want to restrict access by users and groups.
Users in the branch office now report that they cannot connect to Internet resources. Users in the main office, however, are not experiencing any problems. You discover that users in the branch offices are being denied access when they try to connect to Internet resources.
How should you correct this problem?

A. Enable pass-through authentication to allow users from the branch office to access the ISA server array in the main office.
B. Create two-way trust relationships between the branch offices and the main office.
C. On the ISA server array in the main office, enable integrated Windows authentication for all incoming web requests.
D. Configure the ISA server arrays in the branch offices with a user name and password to provide authentication to the ISA server array in the main office.

Answer: D
Explanation: We explicitly configure the ISA server arrays at the branch offices with a user name and password which is valid at the main office.

Reference:
ISA Server help, Pass-through authentication

Incorrect Answers
A: Pass-through authentication would not work since the sites are placed in different domains and no trusts are used.
B: The scenario does not allow creation of trusts.
C: Windows integrated authentication would not work since the sites are placed in different domains and no trusts are used.

QUESTION NO: 27
Your company network includes a communication server named Commnet and an array of two ISA server computers. You are the administrator of the array, which is connected to the Internet. The Commnet protocol uses TCP port 2150.
Some of your users access the Internet through a local ISP named LA-ISP, which dynamically assigns IP addresses to client computers that dial in to the provider.
You want to configure the ISA server array so that only LA-ISP users can access Commnet from the Internet. Which three actions should you take? Each correct answer presents part of the solution. (Choose three)

A. Create a new protocol definition named Commnet Protocol for TCP port 2150. Configure Commnet protocol to use an inbound direction.
B. Create a new protocol definition named Commnet Protocol for TCP port 2150. Configure Commnet protocol to use an outbound direction and a secondary inbound connection.
C. Configure the ISA server to listen for incoming web requests on TCP port 2150.
D. Create a new destination set named ISP set, which includes all IP addresses used by LA-ISP.
E. Create a new client address set named ISP set, which includes all IP addresses used by LA-ISP.
F. Create a web-publishing rule for Commnet that applies to ISP Set and Commnet Protocol.
G. Create a server-publishing rule for Commnet that applies to ISP set and Commnet Protocol.
H. Create a protocol rule that allows port 2150 network traffic for all users.

Answer: A, E, G
Explanation:
A: We need to configure a new protocol definition and set it up for inbound communication.
E: We create a client address set which includes the possible IP addresses issued by LA-ISP.
G: We use the client address set and the Protocol definition we created in server publishing rule. This enables access to the communication application only to the users which access Internet through LA-ISP.

Note: Client address sets include one or more computers. Site and content rules, Protocol rules, Bandwidth rules, Server publishing rules, and Web publishing rules can specify client address sets.

Reference: ISA Server Help, Configuring client address sets

Incorrect Answers
B: Only inbound communication has to be configured, not outbound.
C: We must open traffic for TCP port 2150, not listen for traffic on this port.
D: A destination set should not be used. We want to specify clients to which the role apply, not to define destinations
F: Web publishing rules are used to make Web servers public, but we use a communication server.
H: Only specific users, not all users, should be allowed access.

QUESTION NO: 28

You are the network administrator for your company. You are using ISA Server to secure Internet access for your users. They must be able to access any external web site, but they must not be able to use other Internet applications. You create appropriate client address sets and destination sets to allow all Internet client computers to access any external web site. You also create a site and content rule to allow all these computers to access all destinations during work hours only.
Users now report that they receive a 502 Proxy Error message when they try to access external web sites, and they are denied access.
You need to enable users to access external web site. What should you do?

A. Create a new destination set to include the addresses of all allowed web sites.
B. Create a new protocol definition to include HTTP and HTTPS access.
C. Create anew site and content rule to allow all requests for Web-based content.
D. Create a new protocol rule to allow HTTP and HTTPS traffic.

Answer: D
Explanation: Initially, ISA Server does not allow any communication to or from the Internet. At the minimum we need a Site and Content rule and a Protocol row. A Site and Content Rule is already configured in this scenario. We need therefore only to create a protocol rule. This protocol rule should allow web browsing, that is it should allow the HTTP and the HTTPS protocols.

Reference: ISA Server help, Troubleshooting access policy

Incorrect Answers
A: A destination set is not required. We have already configured a Site and Content rule.
B: The HTTP and HTTPS protocols already have protocol definitions.
C: An appropriate Site and Content rule has already been defined.

QUESTION NO 29
You are the administrator of your company's Microsoft Windows 2000 network. For outbound Internet access, your company uses a Microsoft proxy server 2.0 array that consists of three servers running Windows NT server 4.0
You need to upgrade your proxy server array to an ISA server enterprise array in your Windows 2000 domain. You must perform the upgrade with the least possible administrative effort. You must also ensure that you can restore the current proxy server configuration, if necessary.
What should you do?

A. On each server in the array, use the proxy server console to back up the proxy server configuration to a text file. Uninstall proxy server. Upgrade the three servers to Windows 2000 and install ISA sever on each one.
B. On each server in the array, use the proxy server console to back up the proxy server configuration to a text file. Remove each server array. Upgrade the three servers to Windows 2000 and install ISA sever on each one.

C. On each server in the array, back up the Mailbox Store Policy directory. Remove each server from the proxy server array. Install the proxy server upgrade wizard and ISA server on each server.
D. On each server in the array, back up the Mailbox Store Policy directory. Remove each server from the proxy server array. Upgrade the three servers to Windows 2000 and install ISA server on each one.

Answer: B
Explanation: First we should back up the proxy server to be able to return to restore its configuration. This is done from the Proxy Server console. To enable the Installation of ISA Server 2000 we must then upgrade the servers to Windows 2000 Service Pack 1.

Reference:
ISA Server help, Migration process
ISA Server 2000 Administration Study Guide (Sybex), Performing the Upgrade, Page 79.

Incorrect Answers
A: We should remove the Proxy Servers from the array. It is not necessary to uninstall Proxy Server.
C, D: It is not necessary to back up the Mailbox Store Policy Directory of the Proxy Servers.

QUESTION NO 30
You are the network administrator of a branch office for your company. The branch office and the main office are connected by dedicated fractional T1 line. The main office includes an array of ISA server computers. You use group policies and DHCP to administer the configuration of all client computers, which run Microsoft Windows 2000 Professional.
You need to install ISA server at the branch office to improve the performance of FTP and HTTP requests from your client computers. Your configuration must take advantage of the cache on the ISA server array in the main office.
What should you do?

A. Install ISA server in integrated mode. Use DHCP to configure the client computers at the branch office with the internal IP address of your ISA server computer as the default gateway.
B. Install ISA server in cache mode. Use DHCP to configure the client computers at the branch office with the internal IP address of your ISA server computer as the default gateway.
C. Install ISA server in integrated mode. Use DHCP to provide the location of the WPAD.DATABASE file to the client computers at the branch office.
D. Install ISA server in cache mode. Use DHCP to provide the location of the WPAD.DATABASE file to the client computers at the branch office.

Answer: B

Explanation: Only the caching feature of ISA server is required. We should therefore install the ISA Server in cache mode. We then use DHCP to configure the clients default gateway setting to the internal address of the ISA Server.

Reference:
ISA Server help, Configuring automatic discovery

Incorrect Answers
A: Integrated mode is not called for in this scenario.
C, D: WPAD (Web Proxy Autodiscovery Protocol) is used to automate the configuration of Firewall and Web Proxy clients through the ISA Server. WPAD does not apply to this scenario however.

QUESTION NO 31
You are preparing an existing Microsoft Windows 2000 Server computer to use as an ISA server computer. This computer will protect your internal network. It currently provides a dial-on-demand VPN connection to a remote office. It also provides network address translation. This computer will continue to provide all its current functionality after it is configured as an ISA server computer.
You want to pre-configure and install ISA server with the least possible administrative effort. Which two actions should you take? Each correct answer presents part of the solution. (Choose two)

A. In the routing and remote access console, delete the external interface used for the network address translation protocol.
B. In the routing and remote access console, delete the network address translation protocol object.
C. In the routing and remote access console, enable packet filtering.
D. In the ISA server console, manually create packet filters for the VPN.
E. In the ISA server console, enable IP routing.

Answer: B, D
Explanation:
B: ISA server provides network address translation (NAT) so NAT should be removed from RRAS (routing and remote access).
D: The ISA server could protect the internal network with packet filters for the VPN.

Incorrect Answers
A: The external interface is still required.
C: ISA Server will provide the filtering. We should not use RRAS filtering on a ISA Server computer.
E: IP routing must already be enabled since VPN were previously configured.

QUESTION NO: 32

You are the network administrator for your company. You purchase a new computer, which you plan to use as the ISA server computer on your network. You want this computer to provide SMTP content filtering for your existing e-mail server. In addition, you want this computer to replace your current Web server. You install Microsoft Windows 2000 Server with default settings on the new computer.
Now you need to prepare this computer to fulfill your requirements. Which two actions should you take? Each correct answer presents part of the solution. (Choose two)

A. Uninstall the SMTP component of the new computer.
B. Uninstall the NNTP component of the new computer.
C. Configure the TCP port used by the web server component of the new computer to use a port that is not currently used.
D. Configure a new SMTP remote domain to handle mail delivery for the DNS domain of your company.
E. Assign the IP address of the new computer's default web site to the internal IP address of the new computer.
F. Assign the IP address of the SMTP server to the internal IP address of the new computer.

Answer: C, E
Explanation:
C: We want to use the ISA Server computer for web publishing. We will have to install Internet Information Server (IIS). IIS must be configured not to use the ports that ISA Server uses for outgoing Web requests (by default, port 8080) and for incoming Web requests (by default, port 80). We can for example use TCP Port 81.
E: Furthermore, we assign the default web site the internal address of the server.

Reference:
Technet, ISA Server Production Information, ISA Server and IIS Server

Incorrect Answers
A: There is no need to any SMTP component on the server. ISA will provide SMTP filtering.
B: NNTP is a protocol for newsgroups. There is no need to reconfigure NNTP in this scenario since newsgroups are not mentioned.
D: SMTP filtering can be configured within ISA Server. There is no need to create a SMTP remote domain.
F: There is no need to configure the ISA server for the SMTP server. We only need to configure an appropriate SMTP filter.

QUESTION NO: 33
You are the administrator of your company network. You install and configure ISA server on a computer named ISA-server1. An employee named Michael, who works offsite, frequently need to transfer highly confidential files to the company network. His computer runs Microsoft Windows 2000 Professional.
You need to provide Michael with VPN access to your network. What should you do?

A. Enable a PPTP tunnel to pass through ISA-server1. Configure static packet filters for PPTP call and PPTP receive.
B. Enable IP routing. Configure static packet filters for L2TP.
C. On ISA-server1, run the Remote ISA VPN Wizard. Create a VPN connection on Michael's computer.
D. On ISA-server1, run the ISA VPN server wizard. Create a VPN connection on Michael's computer.

Answer: D
Explanation: We use Set Up Clients to ISA Server VPN wizard to set up a VPN server on the ISA Server computer which supports roaming clients. This VPN Server will provide the required VPN access.

Note: ISA Server includes three wizards that you can use to create ISA VPN connections:

- Local ISA VPN Wizard. Use this wizard to set up the ISA Server computer that receives connections. The local ISA VPN Server can also be set up to initiate connections.
- Remote ISA VPN Wizard. The Remote ISA VPN Wizard sets up a remote ISA VPN server which initiates connections to a local ISA VPN server.
- Set Up Clients to ISA Server VPN Wizard. Use this wizard to allow roaming users to connect to the VPN. This is the wizard used in this scenario.

Reference: ISA Server help, Using an ISA Server virtual private network

Incorrect Answers
A: This is not the way to configure VPN access.
B: IP Routing is no used to configure VPN access.
C: The Remote ISA VPN Wizard sets up a remote ISA VPN server which initiates connections to a local ISA VPN server. In this scenario we want to set up a VPN connection between the ISA server and a client computer, not between two ISA servers.

QUESTION NO: 34
You are in the process of reconfiguring H.323 Gatekeeper, which is installed on a Microsoft Windows 2000 Server computer named GK1. Currently, all users objects in Active Directory are configured so that Active Directory can be queried to place NetMeeting calls. GK1 is configured with the e-mail address rules shown in the exhibit. Click the exhibit button.

Name	Pattern	Matching	Destination	Metric
Local	(default)	Suffix	Registration Database	1
GW1	Treyresearch.com	Exact	Gateway/proxy	1

ILS1	Treyresearch.com	Exact	ILS Server	1
Gk2	Treyresearch.com	Exact	Gatekeeper	1
GW2	Treyresearch.com	Exact	Gateway/proxy	1
AD1	Treyresearch.com	Suffix	Active Directory	1

You need to reconfigure the e-mail address rules so that Active Directory is checked first. Which two actions should you take? Each correct answer presents part of the solution. (Choose two)

A. Reorder the rules so that the Active Directory rule appears at the top.
B. Change the type of the Active Directory rule from "suffix" to "exact".
C. Except for Active Directory, change the type of all rules from "exact" to "suffix".
D. Delete the rule for the local registration database.
E. Change the type of the rule for the local registration database from "suffix" to "exact".
F. Change the metric of the rule for the local registration database to 2.

Answer: B, C
Explanation: If two rules contain the same pattern, a rule with matching type Exact has precedence over a rule with matching type Prefix. We should therefore:
B: Use the Exact Matching for the Active Directory Rule.
C: Change all other rules so that they use Suffex Matching,

Note: Once H.323 Gatekeeper has established which routing rules match, the routing rules are sorted for additional processing according to the following requirements:

1. Rules with patterns containing more digits have precedence over rules with patterns containing fewer digits.
2. If two rules contain the same pattern, a rule with matching type Exact has precedence over a rule with matching type Prefix.
3. If two rules contain the same pattern and the same matching type, a rule with a lower metric number has precedence over a rule with a higher metric number.

Reference:
Technet, ISA Server, Call routing rules
ISA Server help, H.323 Gatekeeper

Incorrect Answers
A: Putting the Active Directory rule first would not make it apply before the rules that have an Exact Matching. The order of the rules in the list is not of importance.
D: The other rules with Exact Match would still be applied before the Active Directory rule.
E: The other rules with Exact Match would still be applied before the Active Directory rule.
F: The other rules with Exact Match would still be applied before the Active Directory rule. The other rules with Exact Match would still be applied before the Active Directory rule.

QUESTION NO: 35
You are the administrator of a new ISA server computer that contains two network adapters. One network adapter is connected to the Internet, and the other is connected to your internal network. All users on the internal network use Microsoft Windows 2000 Professional or Windows NT workstation 4.0. All client computers are SecureNAT clients of the ISA server computer.
Your company wants to deploy a network application named Netapp, which uses TCP port 2731. Only users in the security group named Netapp. Users are allowed to use the Netapp protocol through the firewall.
You create a new protocol rule that allows the use of the Netapp protocol for members of Netapp Users. You verify that the protocol does not embed any IP addressed in the Netapp data.
Members of Netapp users now report that they cannot use Netapp through the firewall. How should you correct this problem?

A. Configure the ISA server computer to ask unauthenticated users for identification for outgoing web requests.
B. Create a site and content rule that allows access to the destinations used by Netapp.
C. Ensure that the network configuration of the ISA server computer allows requests from the SecureNAT client to connect to the Internet.
D. Install the firewall client software on all client computers.

Answer: D
Explanation: SecureNAT clients cannot be part in any user or group activity. We cannot use SecureNAT clients to allow only members of the NetApp. Users group access. We must use FireWall clients instead. FireWall clients support user and group-based policies.

Reference:
ISA Server 2000 Administration Study Guide (Sybex), Secure Network Translation Client, Page 318
ISA Server 2000 Administration Study Guide (Sybex), Firewall Client, Page 319

Incorrect Answers
A, B, C: SecureNAT clients cannot be used in this scenario. We should use FireWall clients instead.

QUESTION NO: 36
You are the administrator of your company network, which consists of a single Microsoft Windows 2000 domain. All client computers run Windows 2000 Professional. To secure your network from the Internet, you install ISA Server in firewall mode and enable packet filtering. The relevant portion of the resulting configuration is shown in the exhibit.

After the installation, you receive an error message indicating that an external interface could not be found for packet filtering. On investigation, you discover that both network adapters in the ISA server computer are functioning properly and can communicate on their subnets. However, packet filtering is still non-functional.

A. Remove the 172.30.23.0-172.30.23.255 address range from the local address table.
B. Remove the 10.0.0.0-10.255.255.255 address range from the local address table.
C. Enable IP routing on the external interface of the ISA server computer.
D. Disable IP routing on the external interface of the ISA server computer.

Answer: B
Explanation: The 10.0.0.0 is a private addressing range and is therefore included in the LAT (Local Address Table) by default. However, in this scenario 10.0.0.0 does not belong to the internal network. 10.0.0.0 should not in the LAT. This is causing the problems. We should remove this address range from the LAT.

Note: The local address table is a table of all internal Internet protocol (IP) address ranges used by the internal network behind the ISA Server computer. ISA Server uses the LAT to control how machines on the internal network communicate with external networks. The default LAT includes addresses known as private IP addresses.

Reference: ISA Server help, Configuring the local address table

Incorrect Answers
A: The 172.30.23.0-172.30.23.255 address range belongs to the internal network and should be included in the LAT.
C, D: There is no need to change the IP routing configuration.

QUESTION NO: 37
You are the administrator of your company network. Your employer is a design and manufacturing company that holds several original patents. Currently, the company has no Internet connection. Management wants to implement Internet connectivity to allow Internet e-mail and to host a web site. Because of the sensitive nature of company data, management wants to prevent security breaches and loss of data.
The company uses a Microsoft Exchange server 5.5 computers for all internal e-mail. Design specifications state that this computer will host a secure web site for mobile employees, a public web site for customer access, and all Internet e-mail.
You deploy ISA server as shown in the exhibit.

Management wants to ensure that no traffic originating from the Internet can enter the internal network. Which two actions should you take? Each correct answer presents part of the solution. (Choose two)

A. Create packet filters on the ISA server computer for the POP3 and SMTP protocols.
B. Create packet filters on the ISA server computer for the Exchange server RPC protocols.
C. Create packet filters on the ISA server computer for the HTTP and HTTPS protocols.
D. Create a web publishing rule on the ISA server computer to redirect all HTTP and HTTPS requests to the web server.
E. Create a secure mail server publishing rule on the ISA server computer to redirect all mail protocols to the exchange server.

Answer: D, E
Explanation:
D: ISA Server uses Web publishing rules to relieve the concerns associated with publishing Web content to the Internet without compromising internal network security. This meets the requirement to host a site.

E: We also need to make the Exchange server accessible through a publishing rule.

Reference:
ISA Server help, Web publishing rules
ISA Server 2000 Administration Study Guide (Sybex), E-mail Server publishing, Page 139

Incorrect Answers
A, B, C: There is no need for IP Packet filters since Server Publishing sets up dynamic filtering. IP packets filters are less secure because the ports are kept opened.

QUESTION NO: 38
You are the administrator of an ISA server computer at Fabrikam,Inc. This computer, which is named ISA-Server1, is connected to the Internet. All users and computers on your company network belong to a single Microsoft Windows 2000 domain.
Fabricam,Inc., maintains a company policy regarding access to certain games-related Internet sites. When users attempt to access such sites, ISA-server1 should redirect their requests to a special company web site at http://games.fabrikam.net. A routing rule named Games site is used to implement this policy on ISA-server1.
Three months after the games site rule is created, the company installs a new T1 connection to the Internet. All users except members of the Temps security group should now have free access to games-related Internet sites.
You want to ensure that members of Temp are the only users who are redirected to the special web site. You need to configure ISA-server1 to accomplish this goal.
Which two actions should you take? Each correct answer is part of the solution. (Choose two)

A. Include the IP addresses of the members of Temps in the destination set used in the games site rule.
B. Remove the games site rule from the list of routing rules.
C. Create a new site and content rule that applies only to Temps. This rule redirects users to http://games.fabrikam.net
D. Create a new web publishing rule that applies to the domain users security group. This rule allows access to games-related sites on the Internet.
E. Create a new web publishing rule that applies only to Temps. This rule redirects users to http://games.fabrikam.net

Answer: B, C
Explanation:
B: The old rule should be removed. This will allow all users access to the games site.
C: Then we restrict access to this site by creating a new rule that explicitly denies access to the games site for members of the Temps group.

Reference:

Incorrect Answers

A: The destination set should include IP addresses of selected destinations, not IP addresses of selected users.

D: The Deny rule would override any Allow rule. Furthermore, we need a site and content rule, not a web publishing rule.

E: We need a site and content rule, not a web publishing rule.

QUESTION NO: 39

You are the network administrator of Woodgrove bank. Your network consists of several Microsoft Windows 2000 domains in a single forest. The relevant portion of its configuration is shown in the exhibit named "Network Configuration".

Company policy allows only L2TP VPN connections. You run the appropriate ISA server wizards to enable a two-way demand-dial VPN connection between the main office and all branch offices. When you attempt to manually connect the demand-dial interface within Routing and Remote Access, you receive this error message:

How should you correct this problem?

A. On all ISA server computers, install a computer certificate issued by a certificate authority trusted by all these servers.
B. Promote all ISA server computers to domain controllers in the same domain.
C. Include all IP ranges from the remote networks in the local address table of each ISA server computer.
D. Configure an IPSec policy to force encryption of all traffic on VPN connection.

Answer: A
Explanation: L2TP requires computer certificates for all computers involved in the communication process. The error shows that the initial communication negotiations fails. This is an indication that the ISA server do not have appropriate computer certificates.

Incorrect Answers
B: It is not necessary to promote the ISA Servers to Domain Controllers. It would reduce the performance of the ISA services.
C: The Local Address Table (LAT) should only include local IP addresses, not remote.
D: There is a communication failure. The problem would not be solved by increasing the IPSec security.

QUESTION NO: 40
You are the administrator of a Microsoft Windows 2000 network that consists of a single Windows 2000 domain. You want to install ISA server on a member server in this domain. You log on to the domain by using an account that has sufficient permissions to set up software on the member server. However, when you run the Enterprise Initialization utility to update the schema, you receive this error message:

You need to resolve this problem and resume the installation of ISA server. What should you do?

A. Use the run as command to launch the Enterprise Initialization utility in the security context of an account that belongs to the Schema Admins group.
B. Use the run as command to launch the Enterprise Initialization utility in the security context of an account that belongs to the Domain Admins group for the domain.
C. Add the Active Directory snap-in to manage the schema. In the Active Directory schema console, configure the interface to allow schema updates
D. Add the Active Directory snap-in to manage the schema. In the Active Directory schema console, transfer the schema master to the ISA server computer.

Answer: B
Explanation: The Enterprise Initialization is not being run in the appropriate security context. In order to install the ISA Server schema to Active Directory, you must be an administrator on the local computer. In addition, you must be a member of the Enterprise Admins and Schema Admins groups.
Domain Admins are automatically members of the local administrators account. They also belong to the Schema Admins group. Furthermore, the Enterprise Initialization can be run within the security context of the Domain Admins group (instead of the Enterprise Admins group) as long as no changes are made to the default schema.

Reference:
ISA Server help, Initializing the enterprise
ISA Server 2000 Administration Study Guide (Sybex), Installing ISA as a member of an array, Page 76

Incorrect Answers
A: Members of the Schema Admins group are not member of the Enterprise Admins (or Domain Admins) groups.
C, D: The Enterprise Initialization is not being run in the appropriate security context.

QUESTION NO 41
Executives in your company require dedicated network bandwidth for video conferencing. On your ISA Server computer, you set bandwidth priorities for each user group, as in this table:

Users	**75**
Managers	**100**
Executives	**200**
Administrators	**200.**

You create the bandwidth rules shown in the exhibit.

ISA Management

Order	Name	Bandwidth Priority	Protocol	Destination	Schedule	Applies to
1	Users	Users	All IP traffic	All destinations	Always	Accounts:Every one
2	Managers	Managers	All IP	All	Always	Accounts:ISASe

			traffic	destinations		rver1\Manager
3	Executives	Executives	All IP traffic	All destinations	Always	Accounts:ISAServer1\Execute
4	Administrators	Administrators	All IP traffic	All destinations	Always	Accoounts:ISAServer1\Administrator
Last	Default rule	Windows 2000 QoS	All IP traffic	All destinations	Always	Any request

Later, executives report that a videoconference was interrupted by repeated pauses and dropped frames. On investigation, you discover that the amount of bandwidth allocated to the Users groups is the same as the amount allocated to the Executives group.
You need to ensure that the proposed bandwidth priorities are preserved, even during times of high network usage. What should you do?

A. Remove the Users bandwidth rule.
B. Remove the Executives bandwidth rule.
C. Reorder the bandwidth rules so that the users rule is listed last.
D. Reorder the bandwidth rules so that the Executives rule is listed last.
E. Reorder the bandwidth rules so that the Users rule is listed below the Executives rules.

Answer: C
Explanation: Bandwidth rules are applied in order. The first matching rule is used. Since all Executives belongs to the Users groups the Users rule will be applied to them. We must therefore make sure that the Executives rule is applied before the Users rules. This is accomplished by moving the users rule last in the list.

Note: Bandwidth rules are ordered, with the default bandwidth rule processed last. If the request matches the conditions specified by the rule, the bandwidth priority is applied to the request. Otherwise, the next rule is processed. This continues until the last default rule is processed and applied to the request.

Reference: ISA Server help, Configuring bandwidth rules

Incorrect Answers
A: Users still must have a bandwidth rule that applies to them.
B: We must make sure that the Executive rule is applied, so we cannot remove it.
D: We must make sure that the Executive rule is applied. We could make it to the first place, but moving it to the last would only make things worse since the rules are applied in order and only the first matching rule is applied.

QUESTION NO 42
You are the administrator of your company network, which includes an ISA server computer named ISA1. It also includes an FTP server named FTP1, located on a dedicated computer. You configure FTP1 to use TCP port 2021 for the initial connection from an FTP client

Now you want to enable Internet users to connect to FTP1 through ISA1. What should you do?

A. On ISA1, create a packet filter for the dynamic local port (1025-5000). Configure the direction for the packet filter as "both" and the remote port as TCP port 2021.
B. Create a new protocol definition for TCP port 2021. In the protocol definition, configure a secondary connection for TCP port 20 outbound. Use the new protocol definition to create a server publishing rule.
C. Create a new protocol definition for TCP port 2021. Create a new protocol rule that includes both the new protocol definition and the FTP Download Only protocol definition. Configure the rule so it is always available to everyone.
D. On ISA1, delete the server publishing rule for FTP1. Install the Firewall client software on FTP1. Configure a wspcfg.ini file to bind TCP port 20 as a local port and TCP port 2021 as a server port.

Answer: B
Explanation: We must publish the resource, the FTP server, so that it will be available for Internet users. First we create a protocol definition for the propriety protocol. We use this protocol definition in a server publishing rule that publishes the FTP server.

Note: ISA Server uses server publishing to process incoming requests to internal servers, such as SMTP servers, FTP servers, SQL servers, and others. This is achieved through server publishing rules.

Reference: ISA Server help, Server publishing rules

Incorrect Answers
A: Packet filters are static, the specified ports are kept open all the time, and is therefore not so secure. Server publishing rules use dynamic allocation of ports and are more secure.
C: We should use a server publishing rule, not a protocol rule, to make the FTP server available for Internet users.
D: The FTP server is a source, not a client. No client software should be installed on FTP1.

QUESTION NO 43
You are setting up an ISA server computer named ISA1. This server will provide Internet access for users on your company network. The relevant portion of your network configuration is shown in the exhibit.

You have already installed Microsoft Windows 2000 Server and configured ISA1 for Internet access. You are now configuring the internal network adapter. You will be using an IP address of 192.168.0.2/24. You need to finish configuring ISA1 so that it can transmit packets to all computers on your network. What should you do?

A. In the TCP/IP properties for the internal network adapter, specify a default gateway with the address 192.168.0.1
B. In the TCP/IP properties for the external network adapter, specify a default gateway with the address 192.168.0.1
C. From a command prompt, issue this command:
Route-f add 0.0.0.0 mask 255.255.255.0 192.168.0.1
D. From a command prompt, issue this command:
Route-f add 0.0.0.0 mask 255.255.252.0 192.168.0.1
E. From a command prompt, issue this command:
Route-p add 192.168.9.0 mask 255.255.255.0 192.168.0.1
F. From a command prompt, issue this command:
Route-p add 192.168.8.0 mask 255.255.252.0 192.168.0.1

Answer: F
Explanation: We want to transmit, or route, packets from the external interface to the internal network. The internal network is divided into several subnets so we must add a persistent route to the internal network 192.168.8.0/24 at the ISA server. The route command with the –p (persistent) parameter can be used for this purpose.

Note: The Route command displays and modifies the entries in the local IP routing table. Used without parameters, route displays help.
Syntax:

route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric Metric]]]

Reference: Windows 2000 Server help, Route

Incorrect Answers
A, B: We must add a route, not a default gateway, since the internal network has several subnets.
C, D: The –f parameter of the route command is used to clear most of the entries in the routing table. It would not be helpful in this scenario.
E: We only should route to the first internal network 192.168.8.0/24 network. The routing tables on the internal routers will achieve further routing, for example to the 192.168.9.0/24 network

QUESTION NO 44
Your company network consists of a single Microsoft Windows 2000 site. It includes an ISA server enterprise array consisting of a single computer named ISA1. You install ISA server on a new computer, which you name ISA2. You decide to add ISA2 to the array on a different subnet in the same Windows 2000 site.
ISA2 successfully joins the enterprise array, and the setup log file indicates that the setup was successful. Your SecureNAT and firewall client computers are still capable of accessing Internet resources through the default enterprise policies of ISA1. However, these computers cannot access Internet resources through ISA2.
You must enable ISA2 to provide access to Internet resources. What should you do?

A. Create a custom enterprise policy setting for ISA2. Enable outbound client access through the new policy.
B. Disable array-level access rules that restrict your enterprise policies.
C. Delete the ISA installation directory. Run the installation again.
D. Edit the local address table to ensure that it contains only address ranges from your company network.

Answer: D
Explanation: The Local Address Table (LAT) all IP addresses that are private to the network. If external addresses are added to the LAT it could result in erratic behavior as described in this scenario. We should make sure that LAT only contain private address ranges that is used by your company.

Reference: ISA Server help, Configuring the local address table

Incorrect Answers
A: The computers are unable to access Internet through ISA2. Configuration of outbound client access on ISA2 could fix this problem.
B: The scenario does not mention any specific array level access rules for ISA2.
C: There should be no need to reinstall ISA.

QUESTION NO: 45
You are the network administrator for your company. You install ISA server on a computer named ISA-server1. You enable outbound Web Access on this computer. Outgoing Web requests on ISA_server1 are configured as shown in the exhibit named "Add/Edit Listeners".

You enable logging for the Firewall service and the Web Proxy service. Both services use the ISA Server file format for logging. You examine the contents of the log file created by ISA server, as shown in the exhibit named "Log File".

WEBEXTD200011022- Note Pad
#Software: Microsoft® Internal security and acceleration Server
#Version: 1.0
#Date: 2000-10-22

#Fields:c-ip	cs-username	c-agent	sc-authenticated
10.10.100.200	anonymous	Mozilla/4.0 (compatible; MSIE	
10.10.100.200	anonymous	Mozilla/4.0 (compatible; MSIE	
10.10.100.200	anonymous	Mozilla/4.0 (compatible; MSIE	

For each user on your network, you must be able to log the user authentication information for external web requests. You do not want users to be prompted to enter credentials. You must also maintain the security of user credentials.

What should you do?

A. Select Ask authenticated users for identification on the outgoing Web requests tab. Configure an individual listener for outgoing web requests. Use integrated authentication.
B. Select Ask authenticated users for identification on the incoming Web requests tab. Configure an individual listener for outgoing web requests. Use integrated authentication.
C. Select Ask unauthenticated users for identification on the outgoing Web request tab. Use basic authentication and specify the root domain on outgoing Web requests.
D. Select Ask unauthenticated users for identification on the outgoing Web request tab. Configure outgoing Web requests to use a client certificate.

Answer: A
Explanation: We want enforce user authentication for external web requests, but we don't users to be prompted to enter credentials. This can be achieved by using client certificates.

Incorrect Answers
B, C: Integrated authentication would prompt users for credentials.
D: Basic authentication would prompt users for credentials.

QUESTION NO: 46
You are the administrator of your company network, which consists of a main office and three branch offices. Each branch office has a dedicated T1 connection to the main office. The main office has a T1 connection to the Internet. In addition, each branch office has a dedicated 128-Kbps DSL line for Internet connectivity.
Company policy allows users limited access to web-based resources. The company wants to ensure that the local caching server at each office will serve all web requests before routing any requests to the Internet. The company also wants to ensure that all requests are forwarded to the Internet go through the main office.
You install ISA server arrays at each branch office and create the routing rules shown here.

ISA Management

Order	Name	Action	Cache
1	Branch Office	Route	Connect if object not in cache, never cache the response.
Last	Default Rule	Route to alternate destination	Connect if valid object not in cache, cache the response only.

Later you discover that many identical requests from the branch offices are being served repeatedly from the cache at the main office. You also discover that requests are being sent directly to the Internet from the branch offices.

Which two actions should you take to correct this problem? Each correct answer presents part of the solution. (Choose two)

A. Route all repeat requests from the branch offices to an internal web site.
B. Route all repeat requests from the main office to an internal web site.
C. Remove the backup connection from the routing rules for branch offices.
D. Remove the backup connection from the routing rules for main office.
E. Configure the branch office arrays to cache responses from the upstream array.
F. Configure the main office array to cache all content.

Answer: C, E
Explanation:
C: The branch offices should only access Internet through the main office. We should therefore remove the backup connection from the routing rules at the Branch offices.
E: The branch office arrays should locally cache responses from the main office ISA server array.

Incorrect Answers
A, B: The internal web site cannot be used to meet the requirements in this scenario.
D: The main office has no backup connection to the Internet.
F: The main office array is already configured for caching. We must enable caching at the branch office arrays.

QUESTION NO: 47
You administer a stand-alone ISA server computer. Your company network includes 4,000 computers that use this server to access Internet resources.
The server uses the default site and content rule and the default IP packet filters. Packet filters is enabled. The server has two protocol rules that are detailed here.

Name	Scope	Action	Protocol	Applies To	Schedule
Web	Array	Allow	HTTP	Any request	Always
Web(Secure)	Array	Allow	HTTPS	Any request	Always

Users report that they cannot access Internet sites that require secure transmission of data. You verify that they can access Internet sites that do not require secure transmission.
You must ensure that users can access Internet sites that require secure transmission of data. What should you do?

A. Create new protocol rule that allows the use of HTTPS.
B. Create a new IP packet filter that allows the use of network traffic on port 443.
C. Create a new web publishing rule that redirects SSL requests as HTTP requests.
D. Configure the ISA server computer to ask unauthenticated users for identification for outgoing web requests.

E. Install and configure a stand-alone Microsoft Windows 2000-based Certificate Authority on the Internal network.

Answer: B
Explanation: Packet filtering is enabled. The only packet passing the ISA server is packets defined in Allow Packet filters. Internet sites that require secure traffic are not reachable. Port 443 is used for secure HTTP (HTTPS) traffic. Apparently there is no packet filter which allows traffic on Port 443. We need to create such a packet filter.

Note: The packet filtering feature of the Windows 2000 router is based on exceptions. You can set packet filters per interface and configure them to:
- Pass through all traffic except packets prohibited by filters.
- Discard all traffic except packets allowed by filters.

Reference:
ISA Server help, Packet filtering

Incorrect Answers
A: .There already exist a protocol rule that allows the use of HTTPS. Creating another such rule would not improve the situation.
C: Web publishing rules are used to make internal web servers accessible to external users.
D: Authentication is not required to access secured Internet sites.
E: A certification authoritative is not required to access secured Internet sites.

QUESTION NO: 48
You are the administrator of your company network, which consists of a single Microsoft Windows 2000 domain. The network is connected to the Internet by dedicated T1 line. You install ISA Server to control user access to the Internet and to secure the network from the Internet.
You want to accomplish the following goals:
- **All users in the domain must be able to send and receive e-mail on the mail server of your ISP**
- **External users must be able to perform a directory query of your Active Directory**
- **Administrative users must have unrestricted access to the Internet.**
- **Non-administrative users must be able to access only approved external web sites, and only during work hours.**
- **Non-administrative users must be able to access only approval FTP sites, and only during work hours.**

You take the following actions:
- **Create site and content rules, as summarized in this table:**

Rule Name	Action	Applies to	Schedule	Destination Set
Admins	Allow	Domain Admins	Always	All Destinations

Users-FTP	Allow	Domain Users	Always	Approved FTP Sites
Users-Web	Allow	Domain Users	Work Hours	Approve Web Sites

- **Create protocol rules, as summarized in this table:**

Rule Name	Allowed Protocols	Applies To
Administrators	All IP traffic	Domain Admins
Users	Selected Protocols: FTP (Client) HTTP (Client) LDAP DNS Query (Client)	Domain Users

Which result or results do these actions produce? (Choose all that apply)

A. All users in the domain must be able to send and receive e-mail on the mail server of your ISP.
B. External users must be able to perform a directory query of your Active Directory.
C. Administrative users must have unrestricted access to the Internet.
D. Non-administrative users must be able to access only approved external web sites, and only during work hours.
E. Non-administrative users must be able to access only approval FTP sites, and only during work hours.

Answer: C, D
Explanation:
C: The Admins Site content rule and the Administrators protocol rule gives the Administrator unrestricted access to external sources.
D: Users, except Administrators, are restricted approved external web sites during work hours only by the Users-Web site and content rule. The Users protocol rule allows the users to use the HTTP protocol.

Incorrect Answers
A: SMTP or POP are not allowed protocols for all users which means that they cannot send or receive mail.
B: External users are not authenticated users.
E: There is no time restriction on FTP usage.

QUESTION NO: 49
You are the administrator of your company network. You implement ISA server to control access to internet sites, as follows:

User	Access
Management, Management Information Service Department	Unrestricted access at all times

Sales Department, Marketing Department, Finance Department, Accounting Department, Legal Department	Access limited to certain sites during work hours; unrestricted access after work hours

You network consists of a Microsoft Windows 2000 domain. Each department has its own organizational unit. Except for MIS personnel, all user accounts are members of the Company Users group. All members of company Users also have membership in groups located in the appropriate departmental OU.
You create the site and content rules shown in the exhibit.

Name	Scope	Action	Applies to	Schedule	Destination
Accounting users	Enterprise	Allow	Accounts: DOMAIN\accounting users	Work hours	Accounting
After hours	Enterprise	Allow	Accounts: DOMAIN\company users	Always	All destination
Finance users	Enterprise	Allow	Accounts: DOMAIN\finance users	Work hours	Finance
Management	Enterprise	Allow	Accounts: DOMAIN\management users	Always	All destination
Marketing users	Enterprise	Allow	Accounts: DOMAIN\marketing users	Work hours	Marketing
MIS department	Enterprise	Allow	Accounts: DOMAIN\admins	Always	All destination
Sales Users	Enterprise	Allow	Accounts:DOMAIN\sales users	Work hours	Sales

When you review the ISA server log files, you discover that users who are not members of Management or MIS have unrestricted access to Internet sites during business hours.
How should you correct this problem?

A. Delete the After Hours site and content rules.
B. Edit the schedule of the After Hours site and content rule.
C. Restrict the allowed content of all site and content rules.
D. Restrict the allowed content only of the site and content rules that apply to non-Management and non-MIS users.

Answer: B

Explanation: The After Hours site and content rule is configured with the schedule Always. It allows all company users unrestricted Internet access. We must change the schedule of this rule to apply only after working hours

Incorrect Answers

A: By deleting the After Hours rule not all groups that require unrestricted after working hours site access will get this access.

C, D: The scheduling, not the allowed content, is the problem.

QUESTION NO: 50

You are the network administrator for your company. You are preparing to install ISA server on a Microsoft Windows 2000 computer named ISA1. This computer will become a web proxy server for your network. The relevant portion of your network is configured as shown in the exhibit "Network Configuration".

To ensure that ISA1 is configured properly for the installation of ISA server, you view the routing table of ISA1, which is shown in the exhibit named "Routing Table".

Now you need to configure the routing table so that it can transmit packets to all computers on your network, and to computers on the Internet. Which two actions should you take? Each correct answer presents the part of the solution. (Choose two)

A. From a command prompt, issue this command:
Route delete 0.0.0.0 mask 0.0.0.0 131.107.1.1

B. From a command prompt, issue this command:
Route delete 192.168.100.0 mask 255.255.255.0 192.168.100.1

C. In the TCP/IP properties for the internal network adapter, remove the entry for the default gateway.

D. In the TCP/IP properties for the external network adapter, remove the entry for the default gateway.

E. From a command prompt, issue this command:
Route –p add 192.168.100.0 mask 255.255.0.0 192.168.100.254

F. From a command prompt, issue this command:
Route –p add 192.168.102.0 mask 255.255.254.0 192.168.100.254

Answer: C, E
Explanation:
C: We remove the default gateway of the internal interface with the intention to use a static route instead.
E: We create a static route to the 192.168.100.0 network with local ISA server interface as the default gateway.

Reference: Windows 2000 help, The Windows 2000 IP routing table

Incorrect Answers
A: We should not delete the default route of 0.0.0.0.
B: Deleting this route might make sense.
D: The default gateway on the external interface must be kept. Typically it used to access the ISP.
F: There is no need to add a route to the 192.168.102.0 network.

QUESTION NO 51
You are the network administrator for your company. You install ISA Server on a Microsoft Windows 2000 Server computer and configure it as shown in the exhibit.

The Sales group on your network can now access external web sites, but the Marketing group cannot. You need to enable only these two groups to access external web sites?
What should you do?

A. Create a new HTTP protocol rule and add the Marketing group.
B. Create a new HTTP protocol rule and add the Domain User group.
C. Create a new site and content rule and add the Marketing group.
D. Create a new protocol rule to allow the HTTP protocols and include the IP addresses of the marketing group computers.
E. Create a new destination set and enter the range of IP addresses of the Marketing group computers.

Answer: A
Explanation: By adding a new HTTP protocol rule and add the Marketing group to this rule we will provide the Marketing group access to external web sites as required.

Incorrect Answers
B: Only the Marketing and the Sales, not all users, should have access to the external web sites.
C: This would restrict access to certain sites and contents. However, we must first enable access to any external web sites by a protocol rule.
D: To use IP addresses of the marketing group computers in the protocol rule the computers must have static IP address configuration. This would in most cases require a lot administrative effort.
E: Destination set should include the IP addresses of web sites that should be accessible, not of client computers.

QUESTION NO 52
You are the administrator of your company network, which consists of a single Microsoft Windows 2000 domain with Windows 2000 Professional computers and UNIX workstations. You are planning to deploy ISA Server on the network to provide Internet access for users.
You need to ensure that all users have restricted Internet access. Whenever possible, you also want to take advantage of authentication for Internet requests. What should you do?

A. Configure all Windows 2000 Professional computers and UNIX workstations as Web Proxy clients.
B. Configure all Windows 2000 Professional computers and UNIX workstations as SecureNAT clients.
C. Configure all Windows 2000 Professional computers as Firewall clients. Configure all UNIX workstations as SecureNAT and Web Proxy clients.
D. Configure all Windows 2000 Professional computers as SecureNAT clients. Configure all UNIX workstations as Web Proxy clients.

Answer: C
Explanation: Only Firewall clients support Windows authentication through the ISA server. Firewall clients cannot be used on UNIX client computers however. The UNIX computers should be configured as Web Proxy and SecureNat clients.

Note: The Web Proxy service (w3proxy) is a Windows 2000 service that supports requests from any Web browser. This allows Web access to nearly every desktop operating system, including Windows NT, Microsoft Windows 95, Windows 98, Windows 2000, Macintosh, and UNIX.
The Firewall Client software can send Windows user information, which is required for authentication purposes, to the ISA Server.
SecureNAT clients can benefit from many of the features of Microsoft Internet Security and Acceleration (ISA) Server. This includes most access control features, with the exception of high-level protocol support and user-level authentication.

Reference:
ISA Server help, Web Proxy service
ISA Server help, Firewall clients
ISA Server help, SecureNAT clients

Incorrect Answers
A: The Windows 2000 Professional computers could use the Firewall client to enable Windows authentication through the ISA server.
B: The UNIX computers should use the Web Proxy clients. Furthermore, the Windows 2000 Professional computers could use the Firewall client to enable Windows authentication through the ISA server.
D: The Windows 2000 Professional computers could use the Firewall client to enable Windows authentication through the ISA server.

QUESTION NO 53
You are configuring a computer named ISA1. You will use these computers as the ISA server computer for your company's intranet. You set up ISA1 so that it is connected to three different physical networks. The resulting configuration is shown in the exhibit.

You also plan to add a web server and an FTP server to the perimeter network (also known as DMZ). Users on the Internet should be able to access the servers in the DMZ by using FTP and HTTP. Client computers on the company intranet should be able to connect to file shares on the servers in the DMZ. You need to configure ISA1 to support this functionality. Which two actions should you take? Each correct answer presents part of the solution. (Choose two)

A. On ISA1, enable routing and remote access and enable the computer as a router.
B. In the properties page for the IP packet filters of ISA1, enable IP routing and packet filtering.
C. In the local address table of ISA1, include the address for the network adapter that is connected to the DMZ.
D. In the local address table of ISA1, exclude the address for the network adapter that is connected to the company intranet.
E. In the local address table of ISA1, exclude the address range for the DMZ.

Answer: B, E
Explanation:

B: IP routing must be enabled on ISA1. We should use the IP routing of ISA Server, not the IP routing or RRAS (routing and remote access). See picture below. This setting is reached from the ISA Management console->Access Policy->Right-click IP Packet Filters->Properties.

E: The DMZ must be protected. The IP addresses of the DMZ should be excluded from the Local Address Table (LAT).

Reference: ISA Server help, Configuring the local address table

Incorrect Answers
A: We should use the IP routing of ISA Server, not the IP routing or RRAS (routing and remote access).
C: Only Intranet IP addresses should be included in the LAT
D: The IP addresses of the Intranet should be included, not excluded, in the LAT.

QUESTION NO: 54
You are the administrator of your company network. You implement ISA server to control access to the Internet. Users in various departments require access to Internet sites, as follows:

User	Access
Administrators, Managers	Unrestricted access

Sales Department, Marketing Department	Access limited to certain customer sites
All other users	No access

Your network consists of a single Microsoft Windows 2000 domain. Each department has its own organizational unit. Except for administrators and managers, all user accounts are members of a group named company Users, which is located in the users container. All members of company Users also have membership in groups located in the appropriate departmental OU.
You create the site and content rules shown in the exhibit.

Site and Content rules
Adm & Manager rule
Users-No Access
Sales &Mktg

Users in the sales and marketing departments now report that they cannot access any Internet sales. Administrators and managers report no problems. How should you correct this problem?

A. Reorder the site and content rules so that the Users-No Access rule is listed first.
B. Reorder the site and content rules so that the Sales &Mktg rule is listed first.
C. Remove the User-No access site and content rule.
D. Remove the Sales &Mktg site and content rule.

Answer: C
Explanation: We could simple remove the User-No Access Rule. The Sales and Managers would then gain appropriate access.
Another possible solution, not listed here though, would to move the User-No Access Rule to the last position.

Reference: ISA Server help, Site and content rules

Incorrect Answers
A: The rules are applied in order and only the first matching rule is used. If we move the Users-No access rule to the 1st position, all users would be denied access.
B: If an Administrator is a member of the Sales department, the Administrator would only be able to access certain customer sites since the Sales &Mktg rule would be applied.
D: The Sales and Managers report no problem so there is no need to remove the Sales &Mktg rule.

QUESTION NO: 55
You are the administrator of your company network. The relevant portion of its configuration is shown in the exhibit named "Network Configuration".

The main office hosts a streaming media server on which company presentations, announcements, and news are stored. All company presentations are created in the Microsoft Windows media format and are accessed by using the Windows media protocol.

You install ISA Server arrays at each office. You configure the branch office arrays as downstream arrays from the main office array. Application filters are configured as shown in the exhibit named "Application Filters".

Protocol rules are configured as shown in the exhibit named "Protocol Rules".

ISA Management

Name	Scope	Action	Protocol
All media protocols	Enterprise	Deny	PNM--Real Networks protocol (Client), PNM—Real Networks protocol (Server)
MMS protocol	Enterprise	Allow	NMS--Windows media, NMS--Windows media server

Users now report that they cannot access any streaming media content, not even the allowed company content. How should you correct this problem?

A. Create a protocol definition for the Windows media protocol.
B. Create a protocol rule to allow all streaming media-related protocols.
C. Delete all streaming media-related protocol rules.
D. Enable the streaming media application filter.
E. Create a site and content rule to allow access only to company media servers.

Answer: D
Explanation: The Application Filters exhibit shows that the media application filter is not enabled. We should enable this filter.

Reference: ISA Server help, Application filters

Incorrect Answers

A: There is no need to create a protocol definition for this streaming media type since it already exists.
B: We already have a protocol rule that allows Windows media.
C: Deleting the media related protocol rules will not help. The protocol rule that denies only denies Real Networks Protocols.
E: A site and content rule is not required in this scenario as no general access problem is reported, only media-related access problems.

QUESTION NO: 56
You are the administrator of your company network. The relevant portion of its configuration is shown in the exhibit.

You install ISA server on ISA-Main1 and on ISA-Branch, selecting all default settings. You can now create VPN connection within the branch office. You run the Local ISA VPN wizard and the remote ISA VPN Wizard on both computers.
You need to configure ISA-Branch so that only VPN-client1 can access the finance server. What should you do?

A. Remove the IP addresses for the main office from the local address table. Enable the PPTP client and server packet filters on ISA-Main1 and ISA-Branch.
B. Remove the IP address of the finance server from the local address table. Add a new PPTP client packet filter that uses port 1723.

C. Edit the PPTP client and server packet filters. Include only the IP address of VPN-client1 on both packet filters.
D. Edit the local address table on ISA-Main1 and execute external IP addresses. Change the IP address of the internal network adapter to a valid external IP address.

Answer: C
Explanation: We use packet filters to only allow VPN traffic involving the specific client computer.

Reference:

Incorrect Answers
A: This would enable any VPN connection between the two ISA servers.
B: Removing the IP address of the Finance server from the LAT (Local Address Table) does not make much sense.
D: This proposed solution does not make sense. There is no such thing as executing IP addresses in the LAT. Furthermore, an external IP address cannot be used on the internal network.

QUESTION NO 57
You are the administrator of your company network, which includes an ISA server computer named ISA1 and an internal web server named Web1. You use ISA1 to publish Web1 on the Internet. Because Web1 hosts confidential information, you install an X.509 certificate on ISA1 to encrypt HTTP session traffic. You also enable the SSL listener.
When you test the secure channel from the Internet, you receive a 500 Internal server error message indicating that the network logon has failed.
You need to connect to Web1 by using an encrypted, secure channel between the Internet and ISA1. What should you do?

A. On ISA1, enable client certificate authentication for the secure channel.
B. On ISA1, enable client certificate authentication for incoming Web requests
C. In the properties of the web publishing rule for Web1, enable HTTP requests to be redirected as SSL requests.
D. In the properties of the web publishing rule for Web1, enable SSL requests to be redirected as HTTP requests.

Answer: D
Explanation: We do not need a secure channel between the Web server and the ISA server, only between the ISA Server and the Internet. We therefore select the **Redirect SSL requests as: HTTP Requests** option (see picture below). This configuration is reached from the ISA Management Console->Publishing->Web Publishing Rule->Right-click on the rule->Properties->Bridging.

Reference:
How to Set Up Internet Security and Acceleration Server to Host Web Sites by Using the Secure Sockets Layer Protocol (Q292569)
ISA Server help, SSL bridging

Incorrect Answers
A, B: Client certificates are used on client computers not on the ISA server.
C: We don't need a secure channel to the Web site, only between the ISA server and Internet.

QUESTION NO 58
You install an ISA server computer named ISA1 on your company named. You plan to use ISA1 to provide access to your two public web sites, www.treyresearch.com and www.parnellaerospace.com. Both sites are hosted on a computer named Web1 on your network. Each site is assigned a separate IP address on Web1. An internal DNS server resolves site names internally.
You configure ISA1 to publish Web1. However, when you try to connect to www.parnellaerospace.com from the Internet, www.treyresearch.com is displayed instead.
You must be able to connect to both Web sites from the Internet. What should you do?

A. On your external DNS server, create an A record for www.parnellaerospace.com that points to the external IP address of ISA1. Create a Web publishing rule that redirects requests to the IP address of www.parnellaerospace.com
B. On Web1, install the Firewall Client software. Remove the configuration for the default gateway on Web1. Create a web publishing rule on ISA1 that specifies All Internal Destinations as the destination.
C. Create one destinations set for the fully-qualified domain name of www.parnellaerospace.com and another for the fully-qualified domain name of www.treyresearch.com. Create one web publishing rule named www.parnellaerospace.com and another named www.treyreaserach.com. Each rule redirects requests to the appropriate IP address of web1.
D. Create one destinations set for the fully-qualified domain name of www.parnellaerospace.com and www.treyresearch.com. Create a web publishing rule named Publish1 with all default options. This rule redirects requests to Web1.

Answer: C
Explanation: Two internal web sites requires two web publishing rules to make them both accessible on the Internet.

Note: Web publishing rules determine how ISA Server should intercept incoming requests for Hypertext Transfer Protocol (HTTP) objects on an internal Web server and how ISA Server should respond on behalf of the Web server. Requests are forwarded downstream to an internal Web server, located behind the ISA Server computer.

Reference: ISA Server help, Web publishing rules

Incorrect Answers
A: This will not work.
B: Client software on the web server would not affect external access to the web server.
D: Two separate web publishing rules are required.

QUESTION NO: 59
You administer an ISA server computer that makes your company's public web site available to Internet users. Users on your internal network also use this server to access the Internet. The relevant portion of your network configuration is shown in the exhibit.

You want to use Microsoft Internet explorer on the ISA Server computer to access Internet sites. You also want to benefit from the web proxy cache on this server. What should you do?

A. Configure Internet explorer to use web.contoso.com as the address of the proxy server.
B. Configure Internet explorer to use 10.65.1.1 as the address of the proxy server.
C. On the ISA server computer, create an IP packet filter that allows the use of remote TCP port 80.
D. On the ISA server computer, create a routing rule that retrieves requests directly from the destination and caches the response.

Answer: B
Explanation: We configure the web browser to use a proxy server. We specify the IP address of the internal interface of the ISA server. We should also specify the port number, which usually is 8080. See picture below. You reach this setting from Internet Explorer->Tools->Internet Options->Connections->LAN Settings.

Reference: ISA Server help, To configure Microsoft Internet Explorer 5 to use the Web Proxy service

Incorrect Answers
A: It is not possible specify the proxy server with a host name (see picture above). We must use an IP address.
C, D: There is no need to change the ISA configuration. We just have to configure the web browser.

QUESTION NO: 60
You are the administrator for your company network, which contains a single Microsoft Windows 2000 domain. You add all the client computers in your finance department to an Organizational Unit named Finance.
You install and configure an ISA Server computer on the network for Internet access. You configure this computer to allow PPTP packets. You also configure all client computers on the network as SecureNAT clients. Users can now access external web sites.
A VPN server named VPN-server1 is located at the main office of one of your business partners. Users in the finance department need to access VPN-server1, but they cannot establish a VPN tunnel to it.
You need to configure only the client computers in the finance department to connect to VPN-server1.
What should you do?

A. Deploy and assign MS_FWC.msi to the Finance OU.
B. Deploy and publish the setup file for the firewall client software to the finance OU.
C. Configure each client computer in the finance department so that the address of the internal network adapter of your ISA Server computer is its default gateway.
D. Configure routing and remote access on VPN-server1. Enable TCP ports 1723 and 47 on this computer.

Answer: D
Explanation: The remote server must also be setup for VPN. First we configure routing and remote access and then we enable the PPTP specific ports, namely the TCP ports 1723 (PPTP) and 47 (GRE).

We could also set up the ISA server for VPN, but that is a different solution.

Reference: Increasing Security on Windows 2000 VPN Server (Q255784)

Incorrect Answers
A, B, C: We have to set up the remote server for VPN.

QUESTION NO: 61
You are employed by an aerospace manufacturer that develops sensitive projects for the national government. You are designing the Internet security solution for your company.
Absolutely no traffic originating from the Internet can be allowed into the internal network. However, your company has several partners and mobile users who need to access your e-mail server, your web server, and your FTP server.

You want to accomplish the following goals:
- **No traffic originating from the Internet of the perimeter network must be able to enter the internal network**
- **No traffic originating from the internet must be able to directly enter the perimeter network**
- **Partners and mobile users must be able to access the company e-mail server and web server, regardless of their operating system platform.**
- **The internal network must be protected even if a security breach occurs at the perimeter network**
- **An administrator must be notified and the affected service must be shut down if an intrusion is attempted**

Your design calls for the following actions:
- **Deploy ISA Server computers in firewall mode in a back-to-back perimeter network configuration, and deploy the e-mail server, the web server, and he FTP server on the perimeter network, as shown in the exhibit.**

- **Create publishing rules on the external ISA Server firewall to publish the web server, the FTP server, and the e-mail server**
- **Enable IP routing on the external ISA server firewall**
- **Disable packet filtering on the internal ISA Server computer.**

Which result or results do these actions produce? (Choose all that apply.)

A. No traffic originating from the Internet of the perimeter network must be able to enter the internal network
B. No traffic originating from the internet must be able to directly enter the perimeter network
C. Partners and mobile users must be able to access the company e-mail server and web server, regardless of their operating system platform.
D. The internal network must be protected even if a security breach occurs at the perimeter network
E. An administrator must be notified and the affected service must be shut down if an intrusion is attempted.

Answer: B, C
Explanation:
B: We only provide access to the perimeter network through publishing rules.
C: The publishing rules provides access to the web server, the FTP server, and the mail server. These servers use no Windows propriety protocol. They use HTTP/HTTPS, FTP, and SMTP/POP respectively.

Reference:
ISA Server help, Server publishing rules
ISA Server help, Web publishing rules

Incorrect Answers

A: Packet filtering is disabled on the internal ISA server
D: The internal ISA server is not configured for protection.
E: No alerts have been configured.

QUESTION NO: 62
You are the domain administrator of your company network, which consists of one Microsoft Windows 2000 domain and four sites. Each site has a separate T1 connection to the Internet. The relevant portion of your network configuration is shown in the exhibit.

Each site includes one ISA server computer that is connected to the Internet. All four ISA server computers are Windows 2000 member servers. The ISA enterprise initialization tool has not yet run. You need to ensure that policy rules for Internet access are the same for all four sites. Which three actions should you take? Each correct answer presents part of the solution. (Choose three)

A. Run the ISA enterprise initialization tool.
B. Promote the ISA Server computers to domain controllers in the domain.
C. Promote each stand-alone ISA Server computer to a separate array.
D. Install the ISA Server computers in one new array.

E. Configure the array properties to publish automatic discovery information.
F. Apply an Internet access enterprise policy to all ISA Server computers.
G. On one of the ISA Server computers, apply an array access policy that contains the Internet access rules.

Answer: A, C, F
Explanation:
A: We must extend the Active Directory schema.
C: We create a separate array for each site.
F: An Enterprise policy can be applied to all Enterprise ISA servers throughout the domain.

Reference:
ISA Server help, Initializing the enterprise
ISA Server help, To promote a stand-alone server

Incorrect Answers
B: It is not necessary to use Domain Controllers. At the contrary it is not wise, since performance would decrease on the ISA servers.
D: Using the same ISA array in different sites would be counterproductive. Intersite network traffic would decrease the performance.
E: Automatic discovery information is used to automate the configuration of the clients. There is no such requirement in this scenario though.
G: An array access rule would only be applied to this specific ISA array, not to all Enterprise ISA servers throughout the domain.

QUESTION NO: 63
You are the administrator of your company network, which includes a main office and a branch office. The branch office connects to the Internet through a Microsoft Proxy server 2.0 computer named Prx2. Prx2 is chained to another Proxy server 2.0 computer named Prx1, which is located in the main office. You upgrade Prx1 to ISA server. Now, users in both offices report that they cannot browse the Internet. You need to enable users in both offices to browse the Internet. Your solution must involve the least possible administrative effort. What should you do?

A. Configure your internal DNS server with a host record that points to a WSPAD.DAT file.
B. Configure your DHCP server to inform client computers of the location of a WPAD.DAT file.
C. Configure Prx1 to listen for outbound web requests on TCP Port 80.
D. Configure Prx1 to provide an automatic configuration script to Web browsers on your network

Answer: C

Explanation: Proxy Server 2.0 listens for client Hypertext Transfer Protocol (HTTP) requests on port 80, and ISA Server listens on port 8080 by default. The ISA Server, Prx1, should therefore be configured to listen on port 80.

Reference: ISA Server help, Migrating Microsoft Proxy Server 2.0 configuration

Incorrect Answers

A, B: Winsock Proxy Autodetect (WSPAD) is used to automate the configuration of clients through the ISA Server. There is no need to reconfigure the clients however, we just have to reconfigure the ISA server to listen to the Proxy Server 2.0.

D: There is no need to reconfigure the clients. We just have to reconfigure the ISA server to listen to the Proxy Server 2.0.

QUESTION NO 64

You are the administrator of an ISA server array. The relevant portion of your internal network is configured as shown is the exhibit.

The network consists of one Microsoft Windows 2000 forest with three domains. The DNS zone for the three domains are hosted on the DNS servers.

On all client computers, the Firewall Client software is installed and Microsoft Internet Explorer is configured to use the members of the ISA Server array as proxy servers. You configure all client computers to use the DNS addresses of the internal DNS servers.

When you use network Monitor to verify your configuration, you discover that the DNS names for the internal network are being resolved by the ISA Server array.

You need to ensure that all DNS name requests for the internal network are sent to the internal DNS servers. This condition includes DNS names by Internet explorer and by the firewall client software.

Which two actions should you take? Each correct answer presents part of the solution. (Choose two)

A. Configure Internet Explorer on the client computers with a list of addresses that should not use a proxy server include the three domain names.
B. Edit the msplat.txt file on the client computers to include the three domain names.
C. Configure outgoing web requests to resolve web requests within the array before routing
D. Create a new routing rule that applies to all computers in the three domains. Forwarded web requests to the internal DNS servers
E. Configure the local domain table to include the three domain names.

Answer: A, E
Explanation: We must configure Internet Explorer and the firewall clients separately.
A: First we configure the web browsers. We specify the zones for which the Proxy Server should not be used. See picture below. These settings are reached from Internet Explorer->Tools->Internet Option->Connections->LAN settings->Advanced (Use proxy server must be selected).

E: To configure the firewall clients we add three entries to the local domain table (LDT). See picture below. The New LDT entry dialog box is reached from the ISA Management console->Network Configuration->Right-click Local Domain Table (LDT)->New->LDT Entry.

Note: ISA Server to define a local domain table (LDT), which lists all the domain names in the internal network that are served by the ISA Server computer. When a client requests an object from a computer and requires name resolution, the client checks the LDT. If the domain name does not appear in the LDT, then the client requests that ISA Server resolve the domain name on its behalf.

Reference:
ISA Server help, Configuring the local domain table
ISA Server help, Firewall Client components

Incorrect Answers
B: The Msplat.txt file is a firewall client file. It contains the local address table (LAT) which defines the Internet protocol (IP) addresses of your internal network. However, in this scenario we should use the local domain table (LDT), not the local address table (LAT).
C: This is only a performance issue. It has no impact on name resolution.
D: Web requests cannot be handled by the DNS server.

QUESTION NO 65
You are the administrator of your company network, which consists of one Microsoft Windows 2000 domain and one site and a ISA server computer named DeviISA is dedicated to your company's software developers, who use only Windows 2000 Professional computers.

A group named DeveloperWorkstations contains all the computer accounts for the software developers. Another group named DeveloperUsers contains all the user accounts for the software developers. Both groups are contained in the developers OU. You have full administrative control of the developers OU. The DeveloperUsers group has been added to the administrator local group on each client computer. You must deploy the firewall client software to all computers within the developers OU. Your solution must involve the least possible administrative effort.
What should you do?

A. Create a startup script for all accounts in DeveloperWorkstations. In this script, include the following statement:
\\devisa\mspcint\setup.exe
B. Create a logon script for all accounts in DeveloperUsers. In this script, include the following statement:
\\devisa\mspcint\setup.exe
C. Create a new group policy for DeveloperWorkstations. The Group Policy will assign the MS_FWC.MSI package to each computer in DeveloperWorkstations.
D. Create a new group policy object for DeveloperUsers. The group policy will publish the MS_FWC.MSI package to each user in DeveloperUsers.

Answer: C
Explanation: By assigning the software to the appropriate computers, the software will automatically be installed the next time the computers are restarted.

Reference: Windows 2000 Server help, Understanding Software Installation

Incorrect Answers
A: The software would be installed every time the computers would be started.
B: The software would be installed every logon.
D: Published software must be installed manually. It would require considerable effort.

QUESTION NO 66
You administer one ISA server computer that is connected to the Internet. Your internal network consists of a Microsoft Windows 2000 forest with three domains. All client computers run Windows 2000 Professional, and all are configured with the Microsoft Internet explorer proxy settings shown in the exhibit.

You verify that users can successfully connect to Internet sites through the ISA server computer. However, you notice that network traffic for local web servers is frequently routed to this server. You need to ensure that network traffic for the local web servers in your three domains is not routed to the ISA server computer. What should you do?

A. Create a web publishing rule that applies to all destinations in the three domains.
B. Edit the msplat.txt file to include the IP addresses used by all computers in the three domains.
C. Configure the local domain table with a list of the three domain names.
D. Configure the Internet explorer content Advisor with a list of approved sites. Include the three domains.
E. Configure Internet explorer with a list of exceptions that should not use the proxy server. Include the three domain names.

Answer: E
Explanation: We specify the zones for which the Proxy Server should not be used. See picture below. These settings are reached from Internet Explorer->Tools->Internet Option->Connections->LAN settings->Advanced (Use proxy server must be selected).

Reference:
ISA Server help, Firewall Client components
ISA Server help, Configuring the local domain table
Internet Explorer help, Using Content Advisor to control access

Incorrect Answers

A: Web publishing rules are used to make a web server accessible to external users. A web publishing rule is of no use here.

B: The Msplat.txt file is a firewall client file. It contains the local address table (LAT) which defines the Internet protocol (IP) addresses of your internal network. The LAT does not apply to this scenario.

C: The local domain table (LDT) lists all the domain names in the internal network that are served by the ISA Server computer. However, Internet Explorer does not use the LDT. LDT is used by the firewall client, but the firewall client is not mentioned in this scenario.

D: After you turn on Content Advisor, only rated content that meets or exceeds your criteria can be displayed. This does not fit the requirements of this scenario though.

QUESTION NO: 67
You are the enterprise administrator for Trey Research. Your company network includes one Microsoft Windows 2000 domain and four sites. Each site has 500 client computers. The relevant portion of your network configuration is shown in the exhibit.

The Amsterdam site contains an array of three ISA Server computers. This array provides Internet access to client computers in all four sites.
Trey Research wants to reduce the bandwidth used on internal connections for Internet access.
Amsterdam will remain the only site with a direct connection to the Internet.
Which two actions should you take? Each correct answer presents part of the solution. (Choose two)

A. Install additional ISA Server computer in Berlin, Rome, and Paris. Join these servers to Corp ISA Array.
B. Install additional ISA Server computer in Berlin, Rome, and Paris. Create a separate array in each of these sites.
C. Create a routing rule in Berlin, Rome, and Paris to route client requests to Corp ISA array.
D. Install the firewall client software on the ISA server computers in Berlin, Rome, and Paris. Specify Corp ISA array as the destination.
E. Create a web publishing rule in Berlin, Rome, and Paris. Redirect all client requests to Corp ISA Array.
F. Configure the ISA server computers in Berlin, Rome, and Paris to use one of the IP addresses of Corp ISA Array for intra-array communication.

Answer: B, C
Explanation:
B: We create a separate ISA server array at each site to reduce unnecessary network traffic between sites.
C: Requests at the new ISA servers should be routed to the ISA array in Amsterdam.

Incorrect Answers
A: ISA servers in different sites should not be members of the same array. Performance would decrease due the increase in intersite communication.
D: Firewall client software could be useful on client, not on ISA servers however.
E: Web publishing rules are used to make a web server accessible to external users. A web publishing rule is of no use here.
F: ISA servers in different sites should not be members of the same array. Performance would decrease due the increase in intersite communication.

QUESTION NO: 68
You are hired to administer a Microsoft Windows 2000 network. This network already configured before you began your job. The relevant portion of the current configuration is shown in the exhibit. Click the exhibit button.

The current configuration includes as ISA server computer named ISA1 and a Windows 2000 Server computer named RRAS1. bBoth ISA1 and RRAS1 provide VPN access to internal resources. ISA1 also provides firewall and caching services, and it is the web server for your company's Internet site.
You now need to configure WWW2, which is your internal web server. WWW2 should be available to all employees, even if they are working from home. It requires a high level of security.
Your solution must provide public access to ISA1 and employee-only access to WWW2. It must also ensure the highest possible level of security.
What should you do?

A. Change the TCP port used by the web server component on ISA1. Create a web publishing rule to use the new port. Decommission RRAS1. Configure ISA1 to act as a VPN server and to allow remote users to connect by using PPTP.
B. Ensure that the web server component on ISA1 uses the default TCP port. Create a web publishing rule to use the default TCP port. Configure RRAS1 to act as a VPN server and to allow remote users to connect by using PPTP.
C. Change the TCP port used by the web server component on ISA1. Create a web publishing rule to use the new port. Install a digital certificate on WWW2 to encrypt HTTP session traffic. Configure ISA1 to redirect HTTPS requests to WWW2.
D. Ensure that the web server component on ISA1 uses the default TCP port.
Create a web publishing rule to use the default TCP port. Configure WWW2 to use integrated windows authentication. Configure ISA1 to redirect HTTP requests to WWW2.

Answer: A
Explanation: The web server must be configured not to use the port that ISA Server uses for outgoing Web requests (by default, port 8080) or the port used for incoming Web requests (by default, port 80).
We make the internal web site accessible to internet users by creating a web publishing rule for the new port.
We don't need the RRAS server so we decommissioned it. Finally we configure VPN on the ISA server.

Reference:
Technet, ISA Server Production Information, ISA Server and IIS Server
ISA Server help, Web publishing rules

Incorrect Answers
B, D: The default port cannot be used since ISA server use this port already.
C: A solution with certificates requires a certificate for the computer which provides remote access as well.

QUESTION NO 69
You are deploying ISA server in your company network. The relevant portion of your network configuration is shown in the exhibit.

You install ISA Server in firewall mode. You do not enable packet filtering. You then conduct a pilot deployment of ISA Server clients, and you configure several test computers on your network as SecureNAT clients. You create a single protocol rule to give all clients unrestricted access to all protocols. Your pilot users report that none of the test computers can access the Internet through the ISA Server computer. On investigation, you discover that no client requests are being received or processed by this server.
How should you correct this problem?

A. Configure the routers with a default route to the internal IP address of the ISA Server computers.
B. Configure the routers with a default route to the IP address of the router of your ISP.
C. Enable packet filtering and create packet filters on the ISA Server computer to allow all packets to cross the firewall.
D. Enable packet filtering and delete all built-in packet filters.

Answer: A
Explanation: The Firwall client must be able to access the Internal interface of the ISA server. In a routed interval network like this scenario, a default route to the ISA server must be added to the routers. This will enable the firewall clients to access the ISA server.

Incorrect Answers
B: The clients must be able to access the ISA server. The ISA server would then provide Internet access.
C, D: Packet filtering is not required for Internet access (only Site and Content + Protocol rules). Packet filtering can be used to increase the security, but it does not apply in this scenario.

QUESTION NO 70

You are the administrator of your company network, which is configured as shown in the exhibit named "Network Configuration".

You install ISA Server on ISA-Server2 and configure it to allow HTTP traffic. Now the client computers on the Research and Development subnet cannot access the Internet. These computers are configured as shown in the exhibit named "Client Configuration".

```
Client Configuration
C:\WINNT\System32\cmd.exe

Windows 2000 IP configuration

Host Name ........................ : graphical
Primary DNS Suffix ............... : fabrikam.com
Node Type ........................ : Hybrid
IP Routing Enabled ................: No
WINS Proxy Enabled ............... : No
DNS SUFFIX Search List ........... : fabrikam.com

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix .... : fabrikam.com
Description ...................... : Ethernet adapter

Physical Address ................. : 00-01-02-45-38-5A
DHCP Enabled ..................... : Yes
Autoconfiguration Enabled ........ : Yes
IP Address ....................... : 10.10.100.18
Subnet Mask ...................... : 255.255.255.240
Default Gateway .................. : 10.10.100.10
DHCP Server ...................... : 192.168.0.100
DNS Server ....................... : 192.168.0.100
Primary WINS Server ............... : 10.10.100.10
Lease Obtained ................... : Thursday, September 07, ..
Lease Expires .................... : Friday, September 15, ..
```

You must enable all users on this subnet to access the Internet. What should you do?

A. Change the DHCP router option to 10.10.100.17
B. Change the DHCP router option to 192.168.0.1
C. Change the DHCP DNS option to 131.107.54.54
D. Change the IP address of ISA-Server2 from 10.10.100.17 to 10.10.100.32
E. Change the IP address of ISA-Server2 from 10.10.100.17 to 172.16.0.1

Answer: A
Explanation: The clients have been configured with the incorrect default gateway address of 10.10.100.18 (check the exhibit). We resolve this problem by changing the DHCP router option to 10.10.100.17, the IP address of the local interface on the ISA server.

Incorrect Answers
B: The IP address of the local interface of the ISA server is 10.10.100.17, not 192.168.0.1.

C: The DNS option does not need to change. The local DNS server should be used. The local DNS server should forward external name resolution requests to an external DNS servers. If clients would be configured to use an external DNS server they would not be able to access local resources by name.
D: There is no need to change the IP address of the the local interface on the ISA server.
E: There is no need to change the IP address of the the local interface on the ISA server. Furthermore, the IP address of the local interface must be in the 10.10.100.0 range.

QUESTION NO: 71
You are the administrator of your company's network, which includes an array of three ISA server computers configured as shown in this table.

Host Name	**Internal IP Address**	**External IP Address**
ISA-server1	10.10.100.100/24	131.107.200.1/24
ISA-server2	10.10.100.101/24	131.107.200.2/24
ISA-server3	10.10.100.102/24	131.107.200.3/24

The properties of the ISA-server1 are configured as shown in the exhibit. The exhibit show following.

ISA-SERVER1 Properties

Array membership
Intra-array communication
Use this IP address for the intra-array communication.
131. 107. 200. 1

Local Factor
Specify the load factor for this server. This number indicates the relative cache availability of this server compared to the rest of array members.
100

Two network adapters are installed and configured on each array member. All three array members are configured with a Network Load Balancing (NLB) cluster whose IP address is 131. 107. 200. 10/24

Users report that Internet access is very slow. You need to configure the array members to use caching.

What should you do?

A. Change the intra-array IP address to the IP address of the NLB cluster.
B. Change the intra-array IP address to the IP address of the internal network adapter.

C. Change the intra-array IP address to the IP address of the external network adapter.
D. Change the local factor on all array members to equal numeric values.
E. Change the load factor on all array members to different numeric values.

Answer: B
Explanation: The intra-array IP address is configured to use the external address 131.107.200.1. However, the intra-array IP address must be an internal address. This IP address must be included in the local address table.

Reference: ISA Server help, Configure intra-array communication

Incorrect Answers
A: The intra-array IP address cannot be the IP address of the NLB cluster. The intra-array IP address must be an internal address
C: An external IP address is already used, but external IP addresses cannot be used for the intra-array IP address.
D, E: Changing the load factor would not fix the problem.

QUESTION NO 72
You are planning to configure the ISA client computers in your company network. The relevant portion of your network is configured as shown in the exhibit.

Client computers on Subnet A consist of Microsoft Windows 98 and Windows 2000 Professional computers and UNIX workstations. All Windows-based client computers are members of a Windows 2000 domain. All computers in the network have statically assigned IP addresses. The internal DNS server is configured as a root name server. It hosts only the zone for the company domain.
You need to configure the ISA client computers and the network components to enable all ISA client computers to access the internal and external web servers. To minimize administrative complexity and accommodate all client computer platforms, you plan to configure all client computers as SecureNAT clients.
Which three actions should you take? Each correct answer presents part of the solution. (Choose three)

A. Set the default gateway parameter on all client computers to the address of the ISA Server computer.
B. Set the default gateway parameter on all client computers to the address of the local subnet routers.
C. Remove the root zone from the internal DNS server.
D. Configure the client computers to query only DNS servers on the Internet.
E. Create packet filters on the ISA Server computer to allow Web protocols and incoming DNS requests.
F. Create a protocol rule on the ISA server computer to allow web protocols and DNS requests.

Answer: A, C, F
Explanation:

A: The clients must be able to access the ISA server computer. The ISA Server IP address should be used as default gateway on the client computers.
C: The root zone on the internal DNS server prevents any forwarding. We need forwarding to access Internet resources by host name. We must remove the root zone to enable DNS forwarding.
F: We must enable web protocols and DNS traffic to enabling access external web sites by name.

Reference:
ISA Server 2000 Administration Study Guide (Sybex), Multiple Subnet Installations, page 328.

Incorrect Answers
B: We don't use the routers as default gateway. However, the routers must be configured with a forwarding address to the ISA server.
D: We still need to provide access to internal resources.
E: Protocol rules are preferred to packet filters.

QUESTION NO 73
You are the administrator of your company network. you install ISA server with default settings on a server with two modems. You configure this server to allow Internet access for your client computers. You also configure dial-up entries on this server, as shown here.
Available Dial-Up Entries

Name	Network dial-up connection	User Name
Backup Route	Backup	MILLERTEXTILES\mbenson
Primary	Primary-ISP	Mbenson

You install routing and remote access on the ISA server computer. Users on the network now report that they cannot connect to external web sites.

You need to reconfigure your server to accomplish this goal; Whenever it receives a client request, this computer must automatically connect to the ISP by using the primary dial-up connection.
Which two actions should you take? Each correct answer is part of the solution. (Choose two)

A. Install and configure network address translation on your ISA server computer.
B. Edit the default routing rule to use the ISP dial-up connection.
C. Create a network dial-up connection that includes the user account credentials for the ISP.
D. Add a new routing rule. Specify an upstream proxy server address on the internat.
E. Set the primary dial-up connection as the active dial-up connection

Answer: B, E
Explanation:
B: We configure the default routing rule to use the ISP dial-up connection. This ensures that the dial-up interface is used for external access.
E: The active dial-up entry is used whenever ISA Server dials out to the Internet to service a client request. We set the primary dial-up connection as the active dial-up entry.

Note: Dial-up entries specify how the ISA Server computer will connect to the Internet. You use dial-up entries when you configure the Routing rules and Firewall chaining. Only one dial-up entry can be active at a time.

Reference:
Technet, ISA Server concepts, Configuring dial-up entries

Incorrect Answers
A: NAT does not have to be configured on ISA servers.
C: Appropriate dial-up entries have already been configured.
D: There is no upstream ISA server in this scenario.

QUESTION NO: 74
Users in your company frequently use NetMeeting to conduct meetings with users at other companies. The users in your company report that they can place NetMeeting calls to their counterparts at other companies, but the reverse is not true. Users at the other companies cannot use their H.323 gateway to locate NetMeeting users in your company. Administrators in the other companies want to set up an H.323 e-mail address rule to contact employees in your company.
You need to configure your network to meet these needs. What should you do?

A. Configure your external DNS server to allow dynamic updates. Configure the external network adapter of your H.323 gateway to use the external DNS server for name resolution.
B. Configure your internal DNS server to allow dynamic updates. Configure the internal network adapter of your H.323 gateway to use the internal DNS server for name resolution.
C. On your DNS server, manually add a DNS service location record for the Q931 service on TCP port 1720.
D. In the properties of the H.323 application filter, select Use DNS Gatekeeper lookup and LRQs for alias resolution.

Answer: C
Explanation: The administrator only needs to create a Q931 resource record entry for the appropriate domain. The DNS entry should be placed on a publicly-available DNS server. An SRV record for the Q931 service is created on the DNS server to support calling by an e-mail address. The TCP port number should be 1720.

Reference:
HOW TO: Configure DNS Q931 Records to Support Email Address Calling with H.323 Gatekeeper in ISA Server (Q315671)
ISA Server 2000 Administration Study Guide (Sybex), Gatekeeper-to-Gatekeeper (LAN-to-LAN) H.323 and DNS.

Incorrect Answers
A, B, D: Only a Q931 service record must be added to the appropriate DNS zone. No further configuration is required.

QUESTION NO 75
You administer a single ISA server computer. Your internal network address consists of 10 domains in one Microsoft Windows 2000 forest. The relevant portion of your network configuration is shown in the exhibit.

The network uses a root DNS server with the IP address 10.65.1.7 to host the DNS zones for the Windows 2000 domains. The ISA server computer uses the DNS server of your ISP for name resolution.
You want to configure the web browser on the client computers so that internal and external DNS names are resolved correctly. Company policy specifies that you cannot install the firewall client software.
Which two actions should you take? Each correct answer presents part of the solution. (Choose two)

A. Configure DHCP to assign 10.65.1.1 as the DNS address for the client computers.
B. Configure DHCP to assign 10.65.1.7 as the DNS address for the client computers.
C. Configure the web browsers on the client computers to use a proxy server. Specify 10.65.1.1 as the proxy address and use the ISA server HTTP listener port.
D. Configure the web browser on the client computers to use a proxy server. Specify 10.65.1.7 as the proxy address and use port 53 on the DNS server.
E. Configure the network adapter of your DNS server to use 10.65.1.1 as the DNS address.
F. Configure the client computers as secure network address translation (SecureNAT) clients. Specify 10.65.1.7 as the default gateway.

Answer: B, C
Explanation:
B: The clients must be able to access internal resources so we have to use the internal DNS server.

C: We cannot use firewall client software so we have to configure Internet Explorer to use the ISA Server as proxy server. We should also specify the HTTP listener port of the ISA Server, usually port 8080. See picture below. This configuration is reached from Internet Explorer->Tools->Internet Options->Connections->LAN Settings.

Incorrect Answers

A: The ISA server cannot be used for name resolution.
D: The DNS server cannot be used as proxy server.
E: If we want to configure the interal DNS server to forward DNS resolution we should specify an external DNS server, not the ISA server.
F: The DNS server should not be used as the default gateway.

QUESTION NO 76

You are the network administrator for your company, which includes a main office and two branch offices. Your network includes an ISA server computer named PortISA, an intranet server named PortWeb, and a DNS server named PortDNS. PortISA is configured to publish automatic configuration information. You use only the DNS service on PortDNS for host name resolution. There are no DNS records for PortISA.
You need to reconfigure PortISA so that all users can browse web sites on the Internet and upload files to FTP servers on the Internet. You also need to enable administrators in each of the branch offices to install the Firewall client software from http://PortWeb/CLNTINST/.
Which three actions should you take? Each correct answer presents part of the solution. (Choose three)

A. On PortWeb, create a virtual directory named CLNINST. Set the home directory to \\PortISA\mspcint\webinst\.

B. On PortISA, create a file share named CLNTINST on c:\program files\Microsoft ISA Server\clients\webinst.
C. On PortDNS, create an A record for PortISA. Create a CNAME record named wpad that points to the A record.
D. On PortDNS, create an A record for PortWeb. Create a CNAME record named wpad hat points to the A record.
E. On PortISA, create a protocol rule that allows Everyone to use the FTP server protocol, the HTTP server protocol, and the HTTPS server protocol.
F. On PortISA, create a protocol rule that allows Everyone to use the FTP client protocol, the HTTP client protocol, and the HTTPS client protocol.

Answer: A, C, F
Explanation: We need to automate the configuration of the firewall clients. We will use Web Proxy Autodiscovery Protocol (WPAD).
A: We set up a web site with a home directory on the ISA Server.
C: There are no DNS records for PortISA. We need create an A (Host) record for PortISA so that the clients can access the \\PortISA\mspcint\webinst\. site. Furthermore we need tocreate a CNAME (Alias) WPAD record for PortISA as well
F: The FTP client protocol allows users to upload files to FTP Servers. The HTTP client protocol allows browsing of internet sites. The HTTPS client protocol allows browsing of secure internet sites.

Reference:
ISA Server help, To configure DNS for automatic discovery of ISA Server
ISA Server Technical Briefing

Incorrect Answers
B: We should set up the Web site home directory on the ISA server.
D: We must create a WPAD entry to the ISA server, not the Web server.
E: The users must be allowed to use external FTP Servers, not to host the FTP service. The FTP client protocol, not the FTP server protocol, is required.

QUESTION NO 77
You are the network administrator for your company. You upgrade your Microsoft proxy server 2.0 computer to ISA server. Before the upgrade, you successfully published your Microsoft exchange server 5.5 computer, which resides on your internal network. After the upgrade, you configure an SMTP publishing rule. Now external users cannot send e-mail to recipients on your exchange server. External users must be able to send e-mail to your exchange server. What should you do?

A. On the ISA server computer, install the SMTP component and configure a server publishing rule to redirect SMTP traffic to the IP address of the exchange server.
B. On the exchange server, delete or rename the wscfg.ini file and configure the exchange server as a SecureNAT client.

C. Modify the service start-up order on the exchange server to ensure that the firewall client software starts up after the Internet mail connector service.
D. Configure a mail-publishing rule on the ISA server computer to redirect traffic to the IP address of the host listed in the MX record of the DNS server.

Answer: B
Explanation: With MS Proxy Server 2.0 the MS Exchange server had to be configured as Winsock proxy client. ISA Server on the other hand use the SecureNAT client for the MS Exchange server. Furthermore the MS Proxy Server 2.0 wscfg.ini is not used by ISA server, and this file could be deleted or renamed.

Reference: ISA Server 2000 Administration Study Guide (Sybex), Performing the upgrade, Server Publishing, Page 82

Incorrect Answers
A: We don't need a server publishing rule when upgrading from an integrated MS Proxy server 2.0 and MS Exchange solution.
C: The start order was important on MS Proxy Server 2.0, but not on ISA Server. Furthermore the ISA server solution requires the MS Exchange server to use the SecureNAT client, not the Firewall client.
D: This is not the way to integrate ISA server and MS Exchange. Furthermore we don't need a server publishing rule when upgrading from an integrated MS Proxy server 2.0 and MS Exchange solution.

QUESTION NO 78
You administer your company network, which consists of a single Microsoft Windows 2000 domain. You are planning the deployment of an ISA Server array that will provide internal users with HTTP access. You install ISA Server and create appropriate site and content rules and protocol rules to ensure compliance with company policies regarding Internet access.
The client computers on your network consist of Windows 98 computers, Windows NT workstation computers, Windows 2000 Professional computers, and UNIX workstations. You want to provide Internet access for all client computers while preventing non-company users from accessing the Internet through the ISA Server computer. You also want to reduce the amount of administrative effort required to configure and maintain the client computers.
Which two actions should you take to achieve these goals? Each correct answer presents part of the solution. (Choose two)

A. Configure all client computers as web proxy clients.
B. Configure all client computers as SecureNAT clients.
C. Configure all client computers as Firewall clients.
D. Configure basic authentication for outgoing web requests.
E. Configure digest authentication for outgoing web requests.
F. Configure integrated authentication for outgoing web requests.

Answer: A, D
Explanation:
A: All client computers, including the UNIX clients, can be configured as web proxy clients as long as they have a web browser.
D: All client computers, including the UNIX clients, are able to use basic authentication.

Reference: ISA Server help, Web Proxy service

Incorrect Answers
B: SecureNAT cannot be used for authentication.
C: Firewall computers can not be used as Firewall clients.
E: Digest authentication can only be used by Windows 2000 and Windows XP clients.
F: Only Windows computers can use integrated authentication.