



**TestKingonline.com**

**No Pass No Pay!**

**MCSE, CCNA, CCNP, OCP, CIW, JAVA, Sun Solaris, Checkpoint**

**World No 1 Cert Guides**

**Installing, Configuring and Administering ISA Server**

**2000, Enterprise Edition**

**Exame 70-227**

## **Congratulations!**

You have purchased a TestKingonline. Study Guide.

This study guide is a complete collection of questions and answers that have been developed by our professional & certified team. You must study the contents of this guide properly in order to prepare for the actual certification test. The average time that we would suggest you for studying this study guide is approximately 10 to 20 hours and you will surely pass your exam. We guarantee it!

**GOOD LUCK!**

## **DISCLAIMER**

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

## **Guarantee**

If you use this study guide correctly and still fail the exam, send a scanned copy of your official score notice at: [Sales@Testkingonline.com](mailto:Sales@Testkingonline.com)

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

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

## Table of contents

|                                                                                                                        |    |
|------------------------------------------------------------------------------------------------------------------------|----|
| Topic 1, Installing ISA Server                                                                                         | 5  |
| Section 1: Preconfigure network interface.....                                                                         | 5  |
| Subsection, Verify Internet connectivity before installing ISA Server (0 questions).....                               | 5  |
| Subsection, Verify DNS name resolution (0 questions).....                                                              | 5  |
| Section 2, Install ISA Server. Installation modes include integrated, firewall, and cache (4 questions) .....          | 5  |
| Subsection, Construct and modify the local address table (LAT) (6 questions) .....                                     | 10 |
| Subsection, Calculate the size of the cache and configure it (0 questions) .....                                       | 18 |
| Subsection, Install an ISA Server computer as a member of an array (2 questions) .....                                 | 18 |
| Section 3, Upgrade a Microsoft Proxy Server 2.0 computer to ISA Server (2 questions) .....                             | 22 |
| Subsection, Back up the Proxy Server 2.0 configuration (0 questions) .....                                             | 23 |
| Section 4: Troubleshoot problems that occur during setup (0 questions).....                                            | 23 |
| Topic 2, Configuring and Troubleshooting ISA Server Services .....                                                     | 24 |
| Section 1: Configure and troubleshoot outbound Internet access (2 questions).....                                      | 24 |
| Section 2, Configure ISA Server hosting roles.....                                                                     | 27 |
| Subsection, Configure ISA Server for Web publishing (9 questions) .....                                                | 28 |
| Subsection, Configure ISA Server for SSL (1 question) .....                                                            | 38 |
| Subsection, Configure ISA Server for server publishing (6 questions) .....                                             | 39 |
| Section 3: Configure H.323 Gatekeeper for audio and video conferencing (1 question).....                               | 47 |
| Subsection, Configure gatekeeper rules. Rules include telephone, e-mail, and Internet Protocol (IP) (2 questions)..... | 47 |
| Subsection, Configure gatekeeper destinations by using the Add Destination Wizard (2 questions) .....                  | 50 |

|                                                                                                                                                                                     |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Section 4: Set up and troubleshoot dial-up connections and Routing and Remote Access dial-on-demand connections (4 questions)..                                                     | 52  |
| Subsection, Set up and verify routing rules for static IP routes in Routing and Remote Access. (4 questions) .....                                                                  | 57  |
| Section 5, Configure and troubleshoot virtual private network (VPN) access (3 questions) .....                                                                                      | 64  |
| Subsection, Configure the ISA Server computer as a VPN endpoint without using the VPN Wizard (0 questions)..                                                                        | 67  |
| Subsection, Configure the ISA Server computer for VPN pass-through (1 question) .....                                                                                               | 67  |
| Section 6: Configure multiple ISA Server computers for scalability. Configurations include Network Load Balancing (NLB) and Cache Array Routing Protocol (CARP) (5 questions) ..... | 68  |
| Topic 3, Configuring, Managing, and Troubleshooting Policies and Rules.....                                                                                                         | 75  |
| Section 1, Configure the firewall in accordance with corporate standards.....                                                                                                       | 75  |
| Subsection, Configure the packet filter rules for different levels of security, including system hardening (5 questions) .....                                                      | 75  |
| Section 2: Create and configure access control and bandwidth policies (1 question) .....                                                                                            | 83  |
| Subsection, Create and configure site and content rules to restrict Internet access (6 questions) .....                                                                             | 84  |
| Subsection, Create and configure protocol rules to manage Internet access (7 questions).....                                                                                        | 93  |
| Subsection, Create and configure routing rules to restrict Internet access (0 questions) .....                                                                                      | 98  |
| Subsection, Create and configure bandwidth rules to control bandwidth usage (0 questions).....                                                                                      | 98  |
| Section 3, Troubleshoot access problems .....                                                                                                                                       | 99  |
| Subsection, Troubleshoot user-based access problems (1 question).....                                                                                                               | 99  |
| Subsection, Troubleshoot packet-based access problems (0 questions).....                                                                                                            | 100 |
| Section 4, Create new policy elements. Elements include schedules, bandwidth priorities, destination sets,                                                                          |     |

|                                                                                                                                                                                                                             |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| client address sets, protocol definitions, and content groups (5 questions)                                                                                                                                                 | 101 |
| Section 5: Manage ISA Server arrays in an enterprise (3 questions)                                                                                                                                                          | 106 |
| Subsection, Create an array of proxy servers (0 questions)                                                                                                                                                                  | 109 |
| Subsection, Assign an enterprise policy to an array (1 question)                                                                                                                                                            | 109 |
| Topic 4, Deploying, Configuring, and Troubleshooting the Client Computer                                                                                                                                                    | 112 |
| Section 1, Plan the deployment of client computers to use ISA Server services. Considerations include client authentication, client operating system, network topology, cost, complexity, and client function (6 questions) | 112 |
| Section 2, Configure and troubleshoot the client computer for security-enhanced network address translation (SecureNAT) (7 questions)                                                                                       | 122 |
| Section 3, Install the Firewall Client software. Considerations include the cost and complexity of deployment (4 questions)                                                                                                 | 130 |
| Subsection, Troubleshoot autodetection (1 question)                                                                                                                                                                         | 135 |
| Section 4, Configure the client computer's Web browser to use ISA Server as an HTTP proxy (12 questions)                                                                                                                    | 137 |
| Topic 5, Monitoring, Managing, and Analyzing ISA Server Use                                                                                                                                                                 | 154 |
| Section 1, Monitor security and network usage by using logging and alerting (2 questions)                                                                                                                                   | 154 |
| Subsection, Configure intrusion detection (1 question)                                                                                                                                                                      | 156 |
| Subsection, Configure an alert to send an e-mail message to an administrator (0 questions)                                                                                                                                  | 157 |
| Subsection, Automate alert configuration (0 questions)                                                                                                                                                                      | 157 |
| Subsection, Monitor alert status (0 questions)                                                                                                                                                                              | 157 |
| Section 2: Troubleshoot problems with security and network usage                                                                                                                                                            | 157 |
| Subsection, Detect connections by using Netstat (0 questions)                                                                                                                                                               | 157 |
| Subsection, Test the status of external ports by using Telnet or Network Monitor (0 questions)                                                                                                                              | 157 |

|                                                                                                                                                                        |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Section 3: Analyze the performance of the ISA Server computer. Methods include the use of Performance Monitor, reports, and log files (4 questions).....               | 158 |
| Section 4, Optimize the performance of the ISA Server computer. Considerations include capacity planning, allocation priorities, and trend analysis (2 questions)..... | 164 |
| Subsection, Control the total RAM used by ISA Server for caching (2 questions).....                                                                                    | 168 |
| Topic 6, Mixed Questions (X Questions).....                                                                                                                            | 170 |
| Topic 7, Practice Questions (26 Questions).....                                                                                                                        | 172 |

Number of questions: 150

## Topic 1, Installing ISA Server

### Section 1: Preconfigure network interface

Subsection, Verify Internet connectivity before installing ISA Server (0 questions) Subsection, Verify DNS name resolution (0 questions)

### Section 2, Install ISA Server. Installation modes include integrated, firewall, and cache (4 questions)

#### QUESTION NO: 1

You are the new network administrator for TestKing. The network includes an ISA Server computer named Testking1. Testking1 was configured by a previous administrator. Testking1 functions as a firewall between the TestKing network and the Internet. During a routine audit of Testking1's log files, you discover that several non-standard services are installed and configured to start automatically. Your manager tells you that the previous administrator installed additional services on Testking1 for monitoring and reporting purposes. Your manager wants Testking1 to function only as a firewall. You want to ensure that no additional services on Testking1 are opening ports on Testking1. You do not want to change the status of any built-in services. What should you do?

- A. Run the **nbtstat –an** command.  
Disable any of the additional services that are listed as **Registered**.
- B. Run the **netstat –an** command.  
Disable all services that are listening on authorized ports.

C. Run the ISA Server Security Wizard to set the system security level of Testking1 to **Secure**.

D. Run the ISA Server Security Wizard to set the system security level of Testking1 to **Limited Services**.

**Answer: D**

System hardening has three steps:

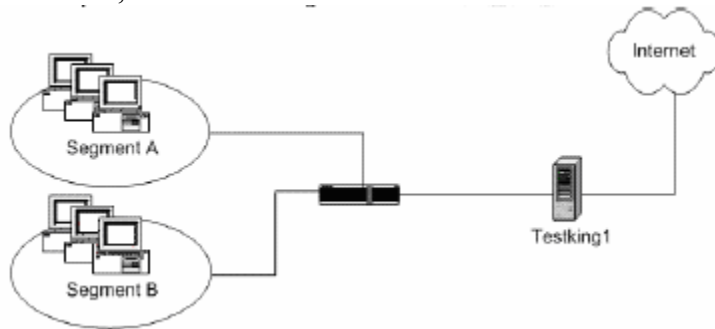
Dedicated (only Firewall, would be the best, but is not here as a point),

Secure (ISA as Firewall and Caching Maschine),

Limited Services (lowest step, ISA and other services).

nbstat has no "-an" and "netstat -an hostname" shows no ports and no

Protocols, it shows netbios nametable and macaddress



. According to the MOC, ISA Server security has three levels: Dedicated, Limited Services (Use this settings to function as a combined firewall and cache server), and Secure (use this settings when the ISA Server performs other functions, such as running web server, database, etc.) Security level For a server For a domain controller  
Dedicated hisecws.inf hisecdc.inf Limited Services Securews.inf securedc.inf Secure Basicsv.inf basicdc.inf

**QUESTION NO: 2**

**You are the network administrator for TestKing. The network includes 1,000 Microsoft Windows 98 client computers, 5,000 Windows XP Professional client computers, and 15 UNIX-based client computers.**

**All client computers use Microsoft Internet Explorer as their only Web browser.**

**You purchase a new ISA Server computer named Testking1. You configure Testking1 to function as a firewall and cache server and you install it so that it connects to TestKing's network to the Internet. The relevant portion of the network configuration is shown in the exhibit. TestKing policy states that only users who are authenticated by the domain are allowed to send any traffic to the Internet.**

**However, this policy contains an exception that allows unauthenticated users to send HTTP traffic after they provide the name and password of a special user account.**

**You configure Testking1 to require authentication for all outgoing traffic and to support Basic and Integrated authentication. Another administrator creates the special user account.**

**You need to comply with TestKing policy.**

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

- A. Configure Testking1 so that the system security level is set to **Secure**.
- B. Install the Firewall Client software on all Windows-based client computers.
- C. Configure Internet Explorer on all client computers to use Testking1 as the proxy server.
- D. Configure all client computers to use Testking1's internal IP address as their default gateway.
- E. Modify the local address table on Testking1 so that all internal IP addresses are included.

**Answer: A, C**

A and C, ISA Firewall and Caching is supported by all OS.

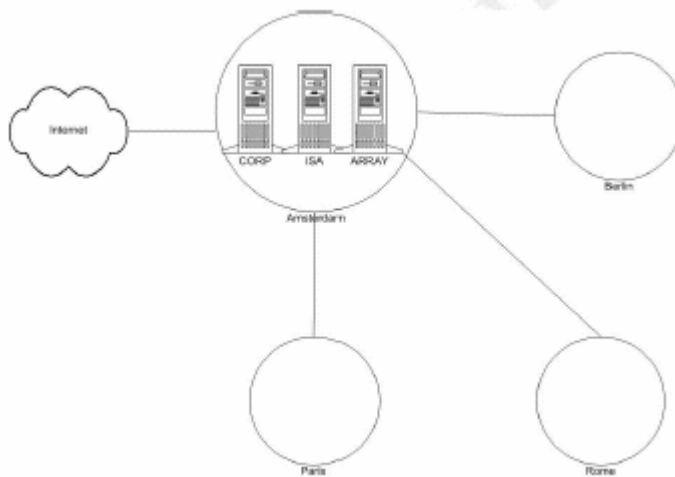
B is not going, because there are UNIX-Clients.

E is not going, because this is only working with Firewallclients

D is not good, because SecureNATClients could not work with Authorisation.

### QUESTION NO: 3

**You are the enterprise administrator for Trey Research. TestKing 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.

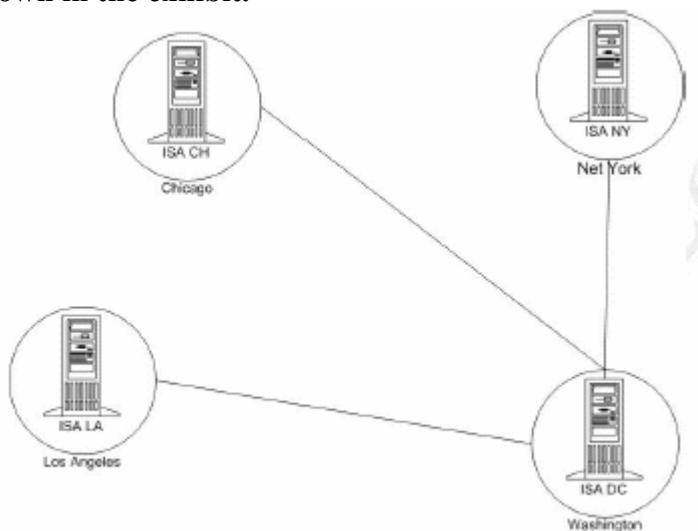
**D:** Firewall client software could be useful on client, not on ISA servers however.

**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: 4**

**You are the domain administrator of TestKing 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.

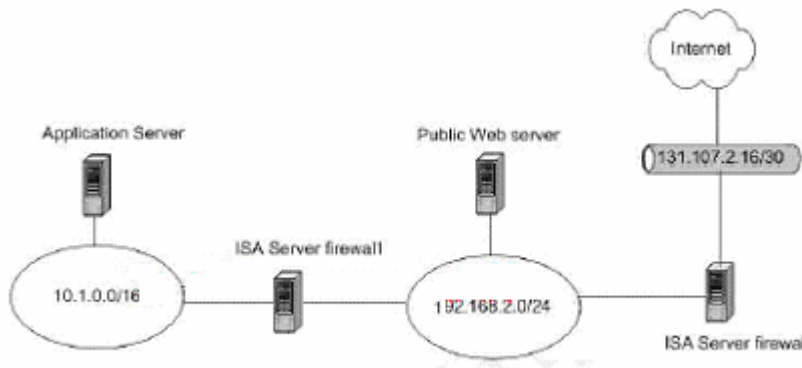
**Subsection, Construct and modify the local address table (LAT) (6 questions)**

**QUESTION NO: 1**

**You are the administrator of TestKing's network. The network consists of a single Microsoft Windows 2000 domain. All server computers run Windows 2000 Server. All client computers run either Windows 2000 Professional or Windows XP Professional. All client computers receive their TCP/IP configuration from a Windows 2000 DHCP server. All client computers use Microsoft Internet Explorer 5.5 or later as their Web browser.**

**All Internet access is controlled by an ISA Server computer. You configure the client configuration options on the ISA Server computer to allow automatic**

discovery of client settings for both Web Proxy and Firewall clients. You configure scope options on the DHCP server as shown in the exhibit.



Several mobile users need access to a custom application that is hosted on the application server. You want to ensure that only the mobile users can access the application from external locations and that all information is transmitted securely. You perform the following actions on the external ISA Server computer.

- Create packet filters to allow L2TP connections to the external ISA Server computer.
- Enable Routing and Remote Access and create a static address pool that contains addresses from the perimeter network (also known as the DMZ).
- Grant dial-in permission to the mobile users.
- Run the ISA VPN Server Wizard.

You perform the following actions on the internal ISA Server computer.

- Create a new protocol definition named AppDef1 for the application.
- Create a new protocol rule named AppPR1 to allow the AppDef1 protocol.
- Create a server publishing rule to allow access to the application.

The mobile users report that they cannot access the application server on the internal network. The users are able to establish a VPN connection. However, they still cannot access the application.

You need to ensure that the mobile users can securely access the application server on the internal network.

What should you do?

- A. On the external ISA Server computer, create a destination set that includes the IP addresses in the static address pool.
- B. On the internal ISA Server computer, create a client address set that includes the IP addresses in the static address pool.  
Add the client address set to the server publishing rule.
- C. On the external ISA Server computer, create and register a new custom application filter for the application.
- D. On the internal ISA Server computer, create packet filters to allow the protocols used by the application.

**Answer: A**

**QUESTION NO: 2**

**You are the administrator of TestKing's network. The network consists of a single Microsoft Windows 2000 domain. The network is currently connected to the Internet by means of a Network Address Translation (NAT) router, as shown in the exhibit.**



**You replace the NAT router with an ISA Server computer that is configured as a member of an array named CorpArray. You complete installation of ISA Server and you receive no error message. When you attempt to connect to the ISA Server computer by using ISA Management, you receive the following error message:**

ISA Error

The operation failed

Failed to connect!

Error 0x8007203a

Details:

The server is not operational

**When you check the Event Viewer on the ISA Server computer, you discover that none of the ISA Server services have started. The ISA Server Control service generated the following event message:**

Event Type: Warning

Event Source: Microsoft ISA Server Control

Event Category: None

Event ID: i3ii0

Date: 12/15/2001

Time: 13:21

User: N/A

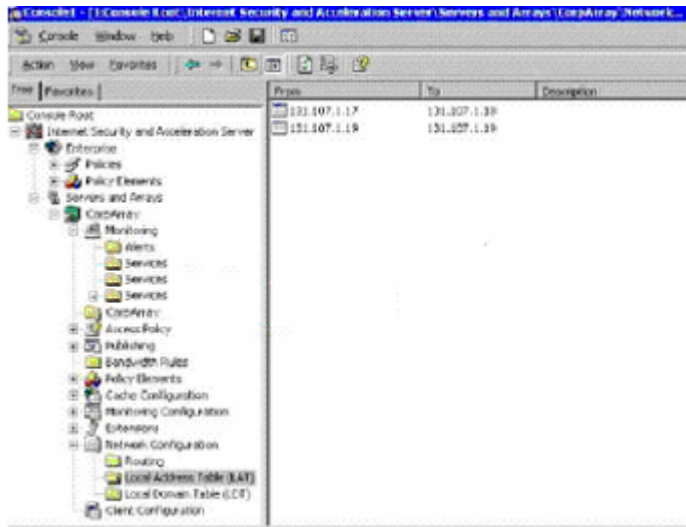
Computer: ISA-Server1

Description:

ISA Server snapin failed to retrieve the array lists

Established. It will next try to retrieve the arrays information from current domain. Check your Active Directory configuration, DNS settings and ensure that the 'Net Logon' service is started.

**You install ISA Management on your Windows 2000 Professional computer and you connect to CorpArray. You view the configuration as shown in the exhibit named "ISA Management"**



**You need to configure CorpArray to allow the services to start. What should you do?**

- A. Delete all current entries in the local address table.  
Manually add the address range of 172.30.0.0-172.30.255.255
- B. Delete all current entries in the local address table.  
Manually add the address range 131.107.1.0-131.107.1.255.
- C. Add the addresses of the domain's DNS servers to the TCP/IP properties of the ISA Server computer.
- D. Add the addresses of the domain's WINS servers to the TCP/IP properties of the ISA Server computer.

**Answer: A**

The error message says that the LAT is defect. The exhibit shows also this point.

### **QUESTION NO: 3**

**You are the administrator of TestKing's network. The network consists of a single Microsoft Windows 2000 domain named testkingonline.com. All server computers run Windows 2000 Server. All client computers run Windows 2000 Professional or Windows NT Workstation 4.0.**

**The network includes an ISA Server computer to control Internet access. The ISA Server computer was upgraded from Microsoft Proxy Server 2.0. All client computers are configured as Web Proxy and Firewall clients. Only members of the Domain Users group are allowed access to Internet resources.**

**A user in the Research department has a multihomed Windows NT Workstation 4.0 computer. This computer connects to both TestKing's network and a private network used in the Research lab. When the user attempts to connect to computers on the lab network, he receives the following error message:**

**"Host not found." He can successfully ping the IP addresses of the computers in the lab.**

**The user needs to be able to connect to resources in the lab in addition to those on the Internet.**

**What should you do?**

- A. Uninstall the Firewall Client software from the client computer and configure the client computer as a SecureNAT client.
- B. Uninstall the Firewall Client software from the client computer and reinstall the Proxy Server 2.0 WinSock Proxy client software.
- C. On the client computer, modify the msplat.txt file to include the range of IP addresses used by the computers in the lab.
- D. On the client computer, create a file named locallat.txt that contains the range of IP addresses used by the computers in the lab.

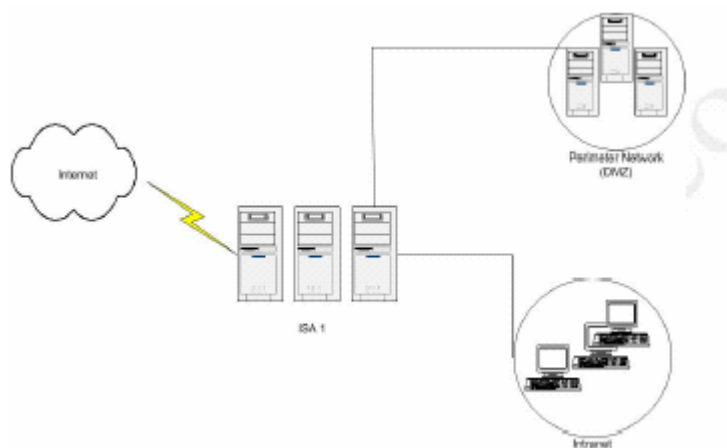
**Answer: D**

The firewall client receives a copy of the LAT every 6 hours copied via the control channel, and all of the old

LAT info is overwritten. A custom LAT are stored in locallat.txt and firewall client LAT is stored in msplat.txt both of these files are checked before a request to the Firewall service is sent.

#### **QUESTION NO 4**

**You are configuring a computer named ISA1. You will use these computers as the ISA server computer for TestKing'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)**

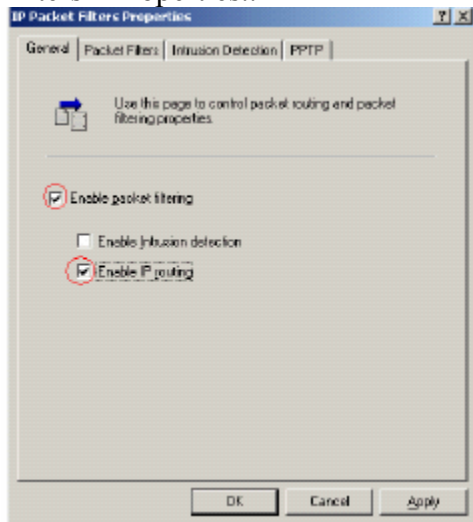
- A. On ISA1, enable routing and remote access and enable the computer as a router.

- 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 5**

**TestKing 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 TestKing 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 TestKing.

**Reference:** ISA Server help, Configuring the local address table

**Incorrect Answers**

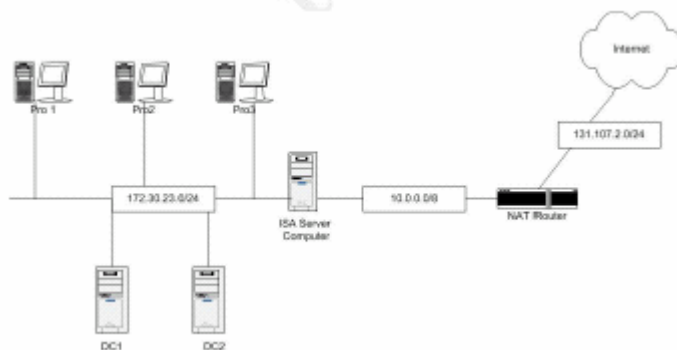
**A:** The computers are unable to access Internet through ISA2. Configuration of outbound client access on ISA2 could fix this problem.

**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: 6**

**You are the administrator of TestKing 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.

**Subsection, Calculate the size of the cache and configure it (0 questions)**

**Subsection, Install an ISA Server computer as a member of an array (2 questions)**

**QUESTION NO: 1**

**You are the network administrator for TestKing. The network includes a single Microsoft Windows 2000 domain and an ISA Server array named Array1. Array1 is used by all network users and provides the only connection between TestKing's network and the Internet.**

**You purchase a new Windows 2000 Server computer named Testking1. You run ISA Server Setup on**

**Testking1 and instruct Setup to join Testking1 to Array1. You receive the following error message: "Unable to locate Array1." You cancel Setup.**

**You verify that the network DNS server is functioning properly. You also verify that Testking1 has the correct IP configuration settings, including the IP address of the DNS server.**

**You need to install ISA Server on Testking1 and ensure that Testking1 is a member of Array1. What should you do?**

- A. On Testking1, run the msisaent.exe application from the ISA Server CD-ROM. Rerun ISA Server Setup.
- B. Join Testking1 to the domain. Log non to Testking1 as a member of the Domain Admins user group. Rerun ISA Server Setup.
- C. Add an SRV (service) resource record to the DNS server. Configure the SRV record with the IP address of Testking1.

Rerun ISA Server Setup.

D. Obtain a volume license product key for ISA Server.

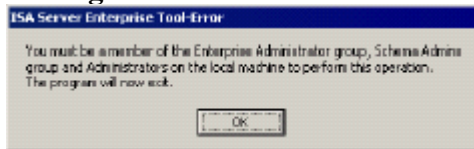
Rerun ISA Server Setup and provide the volume license product key when Setup requests a CD key.

**Answer: B**

Members of one Array have to be in the same domain and in the same site.

## QUESTION NO: 2

**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: C**

The issue here is that it is not a permission issue. The error message takes you for a detour steering you away from the real problem. The AD Schema is locked by default, and to unlock it you need to use the snap-in and enable the updates. There are very few MS products that involve this, they include Exchange 2000, SQL Server 2000 Enter & ISA Server Enter. This is a gotcha situation because you are probably doing your first schema update, you get this error, and you get confused.

The extension or the modification of the Active Directory schema requires write access to the schema. This is enabled by means of the "Schema Update Allowed" registry key. Schema updates may be enabled by means of the Schema Management Console, or directly in the registry. The schema updates can only be enabled on the domain controller that holds the schema master role.

-----  
To Enable Schema Updates by Means of the Schema Management Console:  
At a command prompt, type:

regsvr32 schmmgmt.dll

NOTE: RegSvr32 has been successfully registered when a DllRegisterServer in schmmgmt.dll succeeded dialog box is displayed. Open a new management console by clicking Start, click Run, and then type:

MMC On the Console menu, click Add/Remove Snap-in.

Click Add to open the Add Standalone Snap-in dialog box.

Click Active Directory Schema, and then click Add.

"Active Directory Schema" is displayed in the Add/Remove snap-in. Click

Close, and then click OK to return to the console.

Click Active Directory Schema so that the Classes and Attributes sections are displayed on the right-hand side.

Right-click Active Directory Schema and click Operations Master.

Click to select the Schema may be modified on this Domain Controller check box. Click OK, and then exit the console.

The schema may now be updated on the domain controller that holds the schema operations master role.

-----  
To Enable Schema Updates by Means of the Registry:

It is not recommended to enable schema updates by directly editing the "Schema Update Allowed" registry key. Schema updates should be enabled through the console method, whenever possible. If for some reason the console method cannot be used, the following registry key may be edited directly:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

To directly edit this registry key, perform the following steps:

Click Start, click Run, and then in the Open box, type:

regedit

Then press ENTER.

Locate and click the following registry key:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

On the Edit menu, click New, and then click DWORD Value.

Enter the value data when the following registry value is displayed:

Value Name: Schema Update Allowed

Data Type: REG\_DWORD

Base: Binary

Value Data: Type 1 to enable this feature, or 0 (zero) to disable it.

Quit Registry Editor.

The schema may now be updated on the domain controller that holds the schema operations master role.

-----  
Reference:

Microsoft Technet Article : Q285172

Microsoft Technet Article : Q279978

**Incorrect Answers:**

**A:** install the ISA Server schema to the Windows 2000 Active Directory. You must be an administrator on the

local computer. Also, you must be a member of the Enterprise Admins and Schema Admins groups.

**B:** install the ISA Server schema to the Windows 2000 Active Directory. You must be an administrator on the

local computer. Also, you must be a member of the Enterprise Admins and Schema Admins groups.

**D:** The ISA Server is installed on a member server. Not on a domain Controller. You can only transfer FSMO

Roles to a domain controller

### **Section 3, Upgrade a Microsoft Proxy Server 2.0 computer to ISA Server (2 questions)**

#### **QUESTION NO: 1**

**You are the administrator of TestKing 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 2**

**You are the administrator of TestKing's Microsoft Windows 2000 network. For outbound Internet access, TestKing 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.

**Subsection, Back up the Proxy Server 2.0 configuration (0 questions)**

**Section 4: Troubleshoot problems that occur during setup (0 questions)**

**Topic 2, Configuring and Troubleshooting ISA Server Services**

## Section 1: Configure and troubleshoot outbound Internet access (2 questions)

### QUESTION NO 1

**You are the network administrator of a branch office for TestKing. 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: D**

#### **Explanation:**

The Branch Offices and the Main Office are connected by DEDICATED (Read : leased Lines, No Internet) lines. So we do NOT need Firewall capabilities.

Further we need take advantage of the cache on the ISA server array in the main office. So we need CACHE mode.

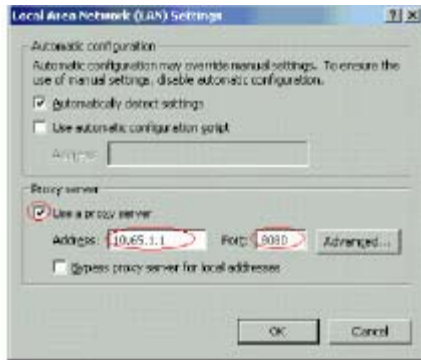
Now the Caching Feature is provided by the WEB PROXY SERVICE and can only be used if :

---> We install the ISA server in Cache Mode or Integrated mode.

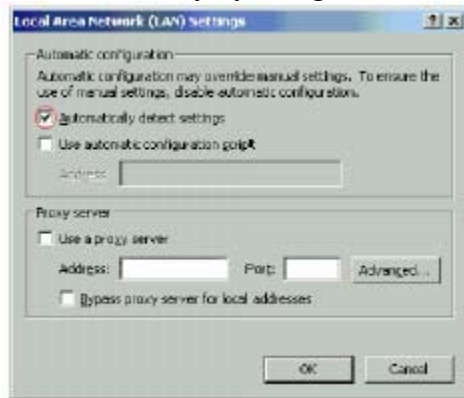
---> We use clients that are configured as Firewall client (Integrated mode) or as Web Proxy Clients (Cache Mode) by DEFAULT !!. SecureNAT is NOT Supported.

So we have to install our clients as WEB PROXY CLIENTS. Now to install a client as Web Proxy client we

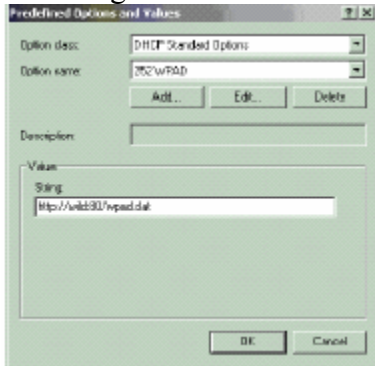
must configure our web browser. We can do this manually:



or automatically by using WPAD.



To configure a DHCP server for automatic discovery of ISA Server:



- > Open DHCP, in the console tree, right-click the DHCP server that assigns IP addresses to client computers, and then click Set Predefined Options.
- > In the Predefined Options and Values dialog box, click Add.
- > In the Option Type dialog box, specify the following information, and then click OK.
- > In the Name box, type WPAD. In the Data type box, click String. In the Code box, type 252
- > In the Value area, in the String box, type <http://name/wpad.dat> (where name is the name of the ISA Server computer that will supply the configuration information), and then click OK.
- > In the Local Area Network (LAN) Settings dialog box, select the Automatically detect settings check box, and then click OK twice.

**Reference:**

**Incorrect Answers:**

**A,C:** The Branch Offices and the Main Office are connected by DEDICATED (Read : leased Lines, No Internet) lines. So we do NOT need Firewall capabilities. Further we need take advantage of the cache on the ISA server array in the main office. So we need CACHE mode.

**B:** Configuring the clients with an default gateway applies the SecureNAT. SecureNAT is not supported in Cache Mode

**QUESTION NO 2**

**You are the network administrator for TestKing, 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 to create 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.

## **Section 2, Configure ISA Server hosting roles**

### **Subsection, Configure ISA Server for Web publishing (9 questions)**

#### **QUESTION NO: 1**

**You are the administrator for TestKing's network. The network consists of a single Microsoft Windows 2000 domain named testkingonline.com. The domain contains all the user accounts. TestKing uses an ISA Server computer to control Internet access. The ISA Server computer is a member of the domain and its not a member of an array.**

**Users on the network use different CERN-compliant Web browsers to connect to Web sites on the Internet. The Web browsers are configured to use the ISA Server computer as a proxy server. TestKing policy states that the ISA Server computer log files must include information about which users access which Web sites.**

**You configure a protocol rule that allows outgoing Web requests. The rule applies to the Domain Users group. The outgoing Web requests properties of the ISA Server computer are configured to ask unauthenticated users for identification.**

**You receive reports that some users are not able to access the Internet, while other users have no difficulty accessing the Internet. You do not want to install new Web browsers on the client computers.**

**What should you do?**

- A. Change the protocol rule that allows outgoing Web requests to apply to any requests.
- B. Disable the option to ask unauthenticated users for identification for outgoing Web requests.
- C. Enable the option to configure listeners per individual IP address for outgoing Web requests.
- D. Change the listener configuration to enable Basic authentication for outgoing Web requests.

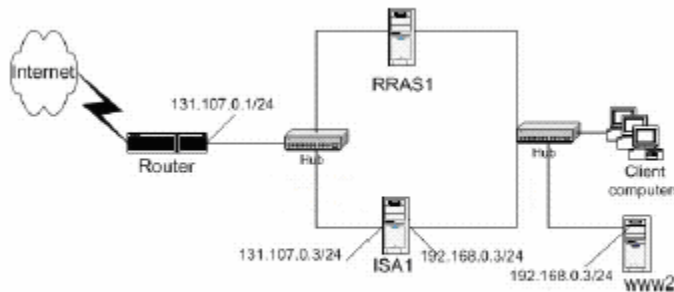
**Answer: D**

**Incorrect answers:**

- A: Rule is working for other users in the domain.
- B: We need logging users access ( Testking Policy )
- C: Not working

## QUESTION NO: 2

**You are hired to administer a Microsoft Windows 2000 network for TestKing Ltd.. This network already configured before you began your job. The relevant portion of the current configuration is shown in the exhibit:**



**The current configuration includes as ISA server computer named ISA1 and a Windows 2000 Server computer named RRAS1. Both ISA1 and RRAS1 provide VPN access to internal resources. ISA1 also provides firewall and caching services, and it is the web server for TestKing'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 3**

**You install an ISA server computer named ISA1 on TestKing named. You plan to use ISA1 to provide access to your two public web sites, [www.treyresearch.com](http://www.treyresearch.com) and [www.parnellaerospace.com](http://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](http://www.parnellaerospace.com) from the Internet, [www.treyresearch.com](http://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](http://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](http://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](http://www.parnellaerospace.com) and another for the fully-qualified domain name of [www.treyresearch.com](http://www.treyresearch.com). Create one web publishing rule named [www.parnellaerospace.com](http://www.parnellaerospace.com) and another named [www.treyreaserach.com](http://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](http://www.parnellaerospace.com) and [www.treyresearch.com](http://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**

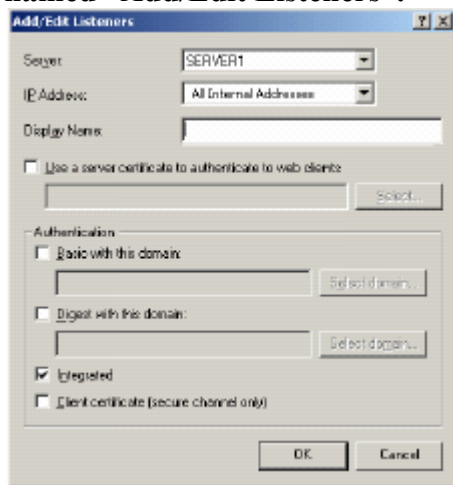
**A:** This will not work.

**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: 4**

**You are the network administrator for TestKing. You install ISA server on a computer named ISAserver1. 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: D**

**Explanation:**

We want enforce user authentication for external web requests, but we don't want users to be prompted to enter credentials. This can be achieved by using client certificates and by selecting the Select Ask unauthenticated users for identification on the outgoing Web request tab.

**Reference:**

MOC2159a Deploying and managing Microsoft Internet Security and Acceleration Server 2000 - Module 3 -  
Page 33

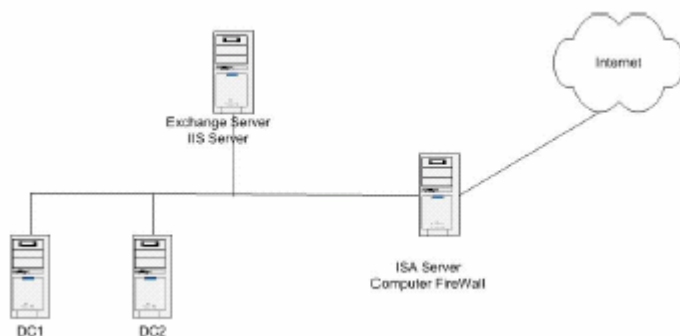
**Incorrect Answers:**

**A, B:** There is NO such thing as : Select Ask authenticated users for identification on the outgoing Web requests tab.

**C:** Basic authentication. Prompts users for a user name and password before allowing Web access. Basic authentication sends and receives user information as plain text and does not use encryption. Basic authentication is the least secure authentication method that ISA Server supports. Because basic authentication is part of the HTTP specification, most browsers support it.

**QUESTION NO: 5**

**You are the administrator of TestKing 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: 6**

**You are the administrator for TestKing's ISA Server computers. The network contains Microsoft Windows 2000 Professional client computers and Windows 2000 Server computers. The ISA Server computers are used to control Internet access. Users on the internal network access video streams and high quality audio streams from the Internet.**

**TestKing policy states that the ISA Server computers must be configured to be as secure as possible, as long as Internet access is not affected.**

**You secure the ISA Server computers by changing several of the configuration options for IP packet filters. However, users now report that they can no longer access video streams and high quality audio streams from the Internet.**

**What should you do?**

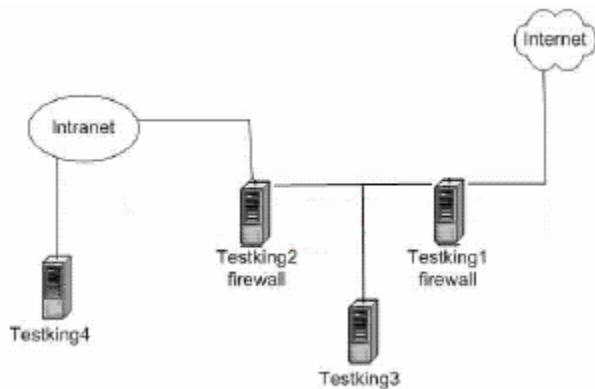
- A. Select the **Enable IP routing** option.
- B. Clear the Enable filtering of IP fragments option.
- C. Clear the Enable filtering IP options option.
- D. Enable the **ICMP source quence** IP packet filter.
- E. Enable the **ICMP ping response (in)** IP packet filter.

**Answer: B**

Multimedia is receiving in blocks = fragmented.

**QUESTION NO: 7**

You are the network administrator for Testkingonline.com. The network includes two ISA Server computers named Testking1 and Testking2. The network also include two Microsoft Exchange 2000 Server computers named Testking3 and Testking4. The relevant portion of the network configuration is shown in the exhibit.



The network is configured as follows:

- Testking1 is configured to permit SMTP traffic between Testking3 and the Internet.
- Testking2 is configured to permit SMTP traffic between Testking3 and Testking4.
- All TestKing users connect to Testking4 to send and receive e-mail.
- Testking4 is configured to forward outgoing e-mail to Testking3.
- Testking3 is configured to forward incoming e-mail to Testking4.

You configure Testking1 so that intrusion detection is enabled. You also configure an alert to send you an e-mail message whenever an intrusion is detected. You configure the alert to use the IP address of Testking4 as the SMTP server.

Several days later, you perform a routine audit of Testking1's log files and discover several intrusion events. However, you did not receive an e-mail message from the intrusion detection system. You verify that you are able to receive e-mail from both internal and external users.

You want to ensure that Testking1 sends you an e-mail message whenever an intrusion is detected. You also want to ensure that your Exchange Server computers remain as secure as possible.

What should you do?

**\*\*MISSING\*\***

**Answer: Pending.** Send your suggestion to [feedback@testkingonline.com](mailto:feedback@testkingonline.com)

**QUESTION NO: 8**

You are the network administrator for TestKing. 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 TestKing.
- 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 9**

You are the administrator of TestKing 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.

**Subsection, Configure ISA Server for SSL (1 question)**

### QUESTION NO 1

You are the administrator of TestKing 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.

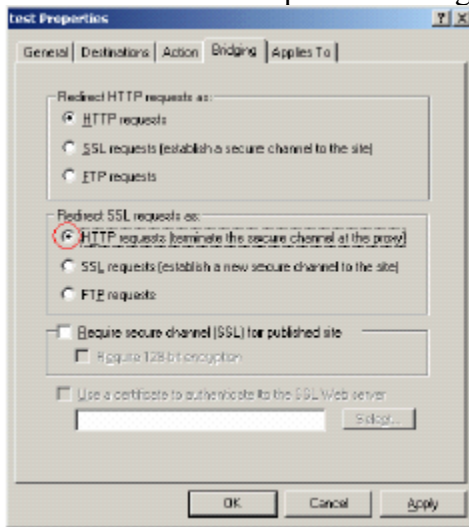
When you test the secure channel from the Internet, you receive a 500 Internal server error message indicating that the network logon has failed.

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.

### **Subsection, Configure ISA Server for server publishing (6 questions)**

#### **QUESTION NO: 1**

**You are the administrator of Testkingonline.com's network. Testkingonline.com uses ISA Server to control internet access. The network contains a Microsoft Windows 2000 Server computer named Testking1. Testking1 is a management server that runs Terminal Services. The Terminal Services software is configured to listen on TCP port 3500 instead of on the default Terminal Services TCP port. You want to publish Testking1 so that users from TestKing can connect to Testking1 from the Internet. What should you do?**

- A. Create a protocol rule that applies to Testking1 and allow network traffic on both the default port and port 3500.
- B. Create a Web publishing rule and redirect to port 3500 on Testking1.
- C. Create a server publishing rule to publish port 3500 and redirect to Testking1.
- D. Create a server publishing rule to publish the default Terminal Services port and redirect to Testking1.

**Answer: C**

We have to create a server publishing rule to publish port 3500 and redirect to Testking 1.

**Reference:** How to Server Publish a Terminal Server with ISA While also Running Terminal Services on the ISA Server, Microsoft Knowledge Base Article - 294720

#### **QUESTION NO: 2**

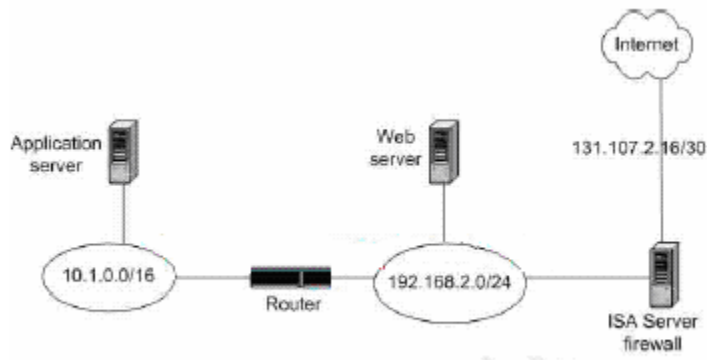
**You are the administrator of Testkingonline.com's network. Testkingonline.com uses ISA Server to control Internet access. You plane to run an application on the ISA Server computer. The application sends data to a remote server on the Internet on destination TCP port 4047. You want to ensure that the ISA Server computer allows the network traffic from the application to the remote server on TCP port 4047. What should you do?**

- A. Create an IP packet filter that allows outbound network traffic to TCP port 4047.
- B. Create a protocol rule that allows outbound network traffic to TCP port 4047. Apply the rule to the internal IP address of only the ISA Server computer.
- C. Create a new protocol definition for TCP port 4047. Create a site and content rule that allows network traffic to the remote server. Apply the rule to the internal IP address of only the ISA Server computer.
- D. Create a server publishing rule that maps the internal IP address of the ISA Server computer to the IP address of the remote server for TCP port 4047.

**Answer: D**

**QUESTION NO: 3**

**You are the administrator of TestKing's network. The network consists of a single Microsoft Windows 2000 domain named testkingonline.com. All server computers run Windows 2000 Server. All client computers run Windows 2000 Professional or Windows NT Workstation 4.0. The network is configured as shown in the exhibit.**



**Several mobile users in the Sales department need access to an application that tracks customer information. The application is hosted on a server that is located on TestKing's internal network. All mobile Sales users use portable computers that run Windows NT Workstation 4.0. You want to ensure that only the mobile Sales users can access the application from external locations. You also want to ensure that all external users can access TestKing's Web site. You take the following actions:**

- Create a protocol definition named AppProt for the protocol used by the application.
- Create a server publishing rule named AppRule to allow access to the application server by using the AppProt protocol.
- Create a Web publishing rule to allow access to TestKing's Web site.

**The mobile Sales users are able to access the application without difficulty. External users are able to access TestKing's Web site without difficulty. Later, you discover that unauthorized users are also able to access the application server. You also discover that sensitive TestKing information is being transmitted over the Internet in a nonsecure manner.**

**You need to prevent unauthorized users from accessing the application server. You also need to ensure that all TestKing information is transmitted securely.**

**What should you do?**

A. Disable IP routing in ISA Server.

Create and register a new custom application filter for the application.

Create a client address set named Mobile1 for the mobile Sales users. Modify the AppRule server publishing rule to allow requests from only Mobile1.

B. Disable IP routing in ISA Server.

Create and register a new custom application filter for the application.

Create a destination set named AppServer1 that includes the IP address for only the application server. Create a new server publishing rule that submits requests to only AppServer1.

C. Delete the AppRule server publishing rule.

Create packet filters to allow inbound access on TCP port 1723 and IP Protocol ID 47. Enable Routing and Remote Access on the ISA Server computer and create PPTP VPN ports.

Grant only the mobile Sales users dial-in permission.

D. Delete the AppRule server publishing rule.

Create packet filters to allow Receive Send access to UDP ports 1701 and 500 and IP Protocol ID 50. Enable Routing and Remote Access on the Web server computer and create L2TP VPN ports. Grant only the mobile Sales users dial-in permission

**Answer: A**

#### **QUESTION NO 4**

**You are the network administrator for TestKing. 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: 5**

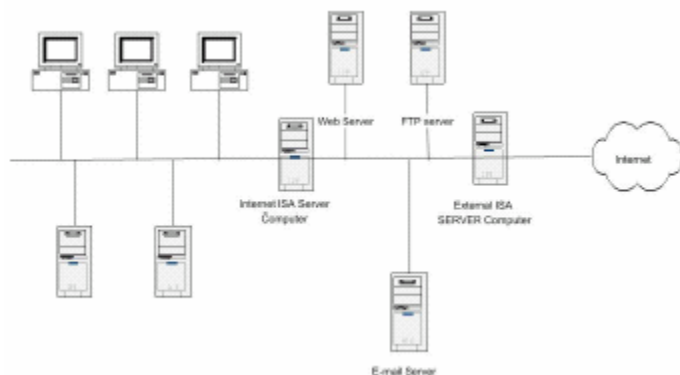
**You are employed by an aerospace manufacturer that develops sensitive projects for the national government. You are designing the Internet security solution for TestKing. Absolutely no traffic originating from the Internet can be allowed into the internal network. However, TestKing has several partners 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 the 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: 6**

**TestKing 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.

### **Section 3: Configure H.323 Gatekeeper for audio and video conferencing (1 question)**

**QUESTION NO: 1**

**You are the administrator for TestKing's network. The network contains Microsoft Windows 2000 Professional client computers and Windows 2000 Server computers. TestKing uses ISA Server to control Internet access.**

**The ISA Server computer contains a site and content rule that allows access to all sites, and a protocol rule that allows access and applies to HTTP and HTTPS protocols. Two internal Web sites are published by using Web publishing rules.**

**Users on the internal network want to use Microsoft NetMeeting to connect to NetMeeting client computers on the Internet. You ensure that the H.323 application filter is enabled and configured to allow outgoing audio and video calls.**

**When users attempt to connect to NetMeeting client computer on the Internet, the ISA Server computer does not allow the connection to be created.**

**What should you do?**

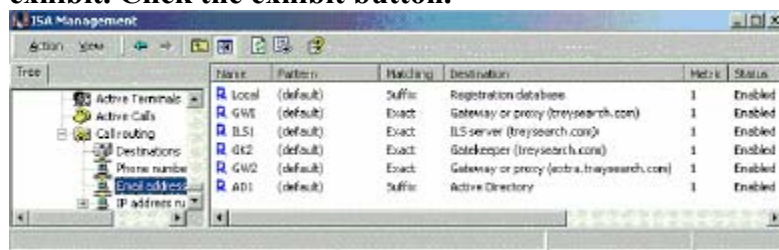
- A. Install H.323 Gatekeeper and configure the NetMeeting client computers to use the ISA Server computer as their gatekeeper.
- B. Create a protocol rule that allows access and applies to the H.323 protocol.
- C. Create an IP packet filter that allows inbound network traffic on the H.323 TCP Port.
- D. Create a server publishing rule that allows inbound network traffic to the ISA Server computer on the H.323 TCP port.

**Answer: A**

**Subsection, Configure gatekeeper rules. Rules include telephone, e-mail, and Internet Protocol (IP) (2 questions)**

**QUESTION NO: 1**

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.



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 Suffix. We should therefore:

**B:** Use the Exact Matching for the Active Directory Rule.

**C:** Change all other rules so that they use Suffix 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: 2**

**You are the administrator of TestKing's network. The network contains Microsoft Windows 2000 Professional client computers and Windows 2000 Server computers. TestKing uses ISA Server to control Internet access.**

**Users on the internal network use Microsoft NetMeeting to place audio and video calls to a partner company. The partner company also uses ISA Server to control Internet access. Both companies use**

**H.323 Gatekeeper to route the NetMeeting calls.**

**The partner company reports that users behind the ISA Server computer of the partner company cannot place NetMeeting calls to the users on your network by using e-mail addresses. If a user at the partner company specifies your ISA Server computer as a gateway, the user is able to place a NetMeeting call to your users by using phone number addressing.**

**You verify that users have registered their e-mail addresses with the H.323 Gatekeeper registration database. You also verify that the default e-mail address rule is configured correctly.**

**You want users at the partner company to be able to use e-mail addresses to place NetMeeting calls to the users on your network.**

**What should you do?**

- A. Create an H.323 Gatekeeper destination that includes the name of your domain.
- B. Create a Q931 DNS service location resource record for your domain name.
- C. Configure the H.323 application filter to allow T120 connections.
- D. Increase the metric value for the current phone number rule to be higher than the current e-mail address rule.

**Answer: B**

How to configure DNS Q931 records to support e-mail address calling by using the Internet Security and Acceleration (ISA) Server H.323 Gatekeeper service. The ISA Server H.323 Gatekeeper service was designed to optimize the benefits of LAN-to-LAN calls. When each LAN has an H.323 gatekeeper and H.323 clients (such as Microsoft NetMeeting) registered with their respective gatekeepers, users can call H.323 clients on other networks by using either an e-mail address or a telephone number. Using an e-mail address to call a destination is the easiest option for most users and administrators. Users do not need to remember phone numbers and administrators do not need to set up routing rules on the ISA Server computer to support calling by an e-mail address. 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.

**Reference: KB 315671**

### **Subsection, Configure gatekeeper destinations by using the Add Destination Wizard (2 questions)**

#### **QUESTION NO: 1**

**You are the administrator of TestKing's network. The network contains Microsoft Windows 2000 Professional client computers and Windows 2000 Server computers. TestKing uses ISA Server to control Internet access. The ISA Server computer allows all outgoing traffic from the client computer to the Internet. Users on the internal network wants to use Microsoft NetMeeting to place audio and video calls to NetMeeting client computers on the Internet. You install H.323 Gatekeeper on the ISA Server computer. You create a destination for the gatekeeper and ensure that all the default call routing rules are configured correctly.**

**You configure NetMeeting on the client computers to use the internal IP address of the ISA Server computer as their gatekeeper. You configure the H.323 application filter to use the external IP address of the ISA Server computer as its gatekeeper. However, users of the NetMeeting client computers on the internal network are unable to successfully place audio and video calls to the Internet.**

**What should you do?**

- A. Configure NetMeeting on the client computers to use the external IP address of the ISA Server computer as their gatekeeper.
- B. Configure NetMeeting on the client computers to use a gateway. Configure the internal IP address of the ISA Server computer as the gateway.
- C. Configure the H.323 application filter to use the internal IP address of the ISA Server computer as its gatekeeper.
- D. Configure the H.323 application filter to allow T120 and application sharing.

**Answer: C**

#### **QUESTION NO: 2**

**Users in TestKing frequently use NetMeeting to conduct meetings with users at other companies. The users in TestKing 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 TestKing. Administrators in the other companies want to set up an H.323 e-mail address rule to contact employees in TestKing.**

**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.

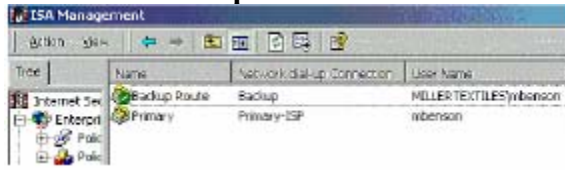
## **Section 4: Set up and troubleshoot dial-up connections and Routing and Remote**

### **Access dial-on-demand connections (4 questions)**

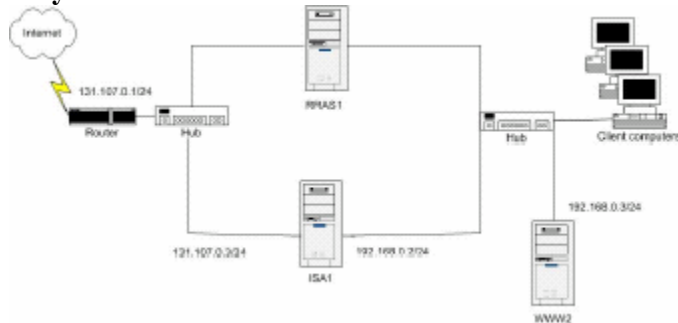
#### **QUESTION NO 1**

You are the administrator of TestKing 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



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 Internet.
- 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: 2

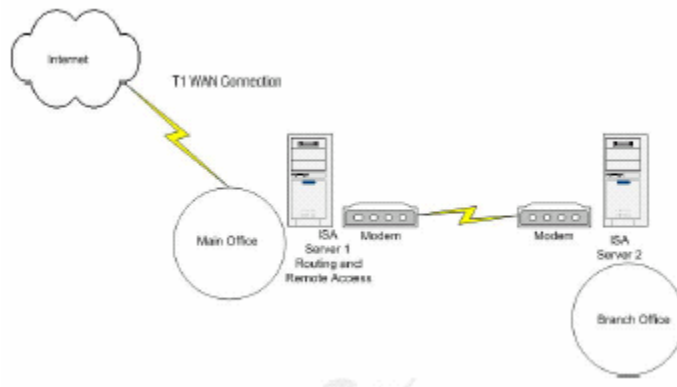
You are an administrator of TestKing's network. The network consists of a single Microsoft Windows 2000 domain named testkingonline.com. All server computers run Windows 2000 Server. The network includes an ISA Server array to control Internet access. All client computers run Windows XP Professional. The client computers use Microsoft Internet Explorer 6.0 as their Web browser. The client computers are configured as Web Proxy and SecureNAT clients. TestKing policy places no restrictions on Web sites that users can access. However, you want to prevent content from certain Web sites from being cached on the ISA Server array. What should you do?

- A. Create a new schedule that defines all hours of all days as an active time. Create a new site and content rule that denies access to the specified Web sites based on this new schedule.
- B. Create new content groups that specify the type of context that you do not want cached. Create a new site and context rule that denies access to the specified content types.
- C. Create a new client address set that specifies all client computers in your network. Configure the HTTP redirector filter to direct all requests directly to the requested Web server.
- D. Create a destination set that includes the fully qualified domain names (FQDNs) of the Web sites. Create a routing rule that specified that content from the destination set will never be cached.

**Answer: D**

### QUESTION NO 3

You are the administrator of TestKing 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 ISAserver2 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 by a default routing rule that uses 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 wants 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 4**

**You are the enterprise administrator for TestKing'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 | <input type="checkbox"/>    | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Dial-up entry       | <input type="checkbox"/>    | <input type="checkbox"/> | <input type="checkbox"/> |                                     |
| Routing Rule        | <input type="checkbox"/>    | <input type="checkbox"/> | <input type="checkbox"/> |                                     |

### Answer:

|                     | At each ISA server computer         | At the array level                  | At the enterprise level             | Check box                           |
|---------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Dial-up connections | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| Dial-up entry       | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                     |
| Routing Rule        | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     |

**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.

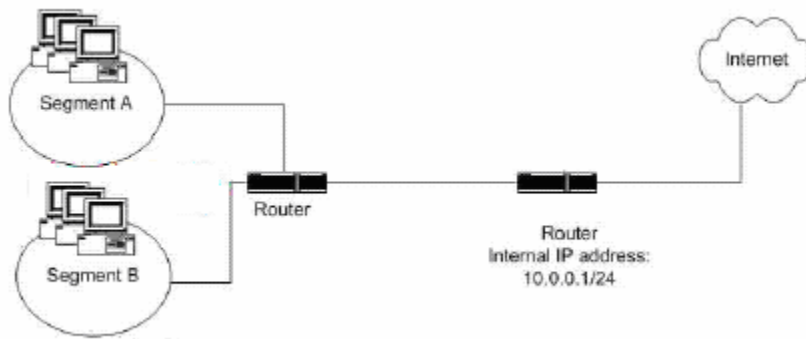
Routing rules should be defined both at the Array level and at the Enterprise level.

**Subsection, Set up and verify routing rules for static IP routes in Routing and Remote Access.**

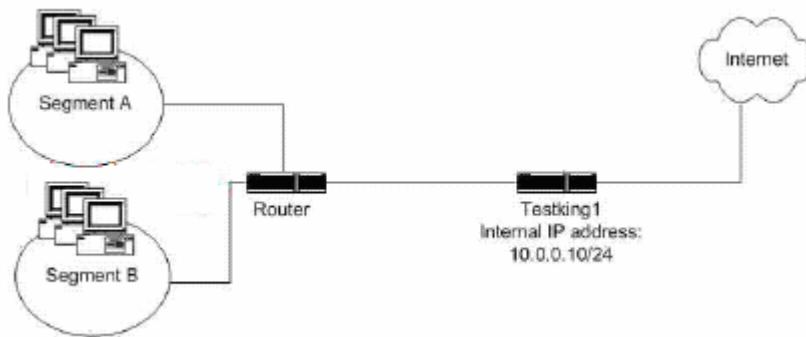
(4 questions)

### QUESTION NO: 1

You are the network administrator for TestKing. The network includes 1,000 Microsoft Windows XP Professional client computers. The network consists of multiple segments. All segments are connected by a central router. All client computers use Web browsers and instant messaging software to access the Internet. The network has a single connection to the Internet. The relevant portion of the network configuration is shown in the exhibit.



**You replace the Internet router with an ISA Server computer named Testking1. Testking1 is configured to permit authorized traffic between client computers and the Internet. The relevant portion of the new network configuration is shown in the exhibit.**



**All users immediately report that they cannot access Internet-based resources. You need to ensure that all users can continue to access Internet resources. What should you do?**

- A. Configure all client computers to be ISA Server Web Proxy clients.
- B. Configure all client computers to use 10.10.0.10 as their default gateway.
- C. Configure the internal network adapter on Testking1 to use the IP address of 10.0.0.1. Restart Testking1.
- D. Configure the local domain table on Testking1 to include the IP addresses of all TestKing's network segments. Restart Testking1.

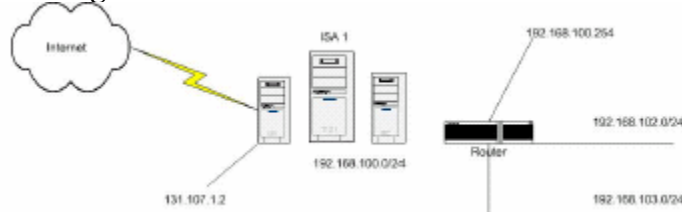
**Answer: C**

For faster routing (and not changing the actual routing tables) you should write the ip-address of old router into the isa server.

## **QUESTION NO: 2**

**You are the network administrator for TestKing. 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”.

The screenshot shows the Windows command prompt displaying the routing table. The title bar indicates the command is 'C:\WINNT\System32\cmd.exe'. The output is as follows:

```

Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0          192.168.100.254  192.168.100.1    1
127.0.0.0              255.0.0.0        127.0.0.1       127.0.0.1        1
131.107.1.0            255.255.255.0    131.107.1.2     131.107.1.2      1
131.107.1.2            255.255.255.0    131.107.1.2     131.107.1.2      1
192.168.100.0          255.255.255.0    192.168.100.1   192.168.100.1    1
192.168.100.1          255.255.255.0    127.0.0.1       127.0.0.1        1
192.168.100.255        255.255.255.0    192.168.100.1   192.168.100.1    1
224.0.0.0              224.0.0.0        192.168.100.1   192.168.100.1    1
255.255.255.255        255.255.255.0    192.168.100.1   192.168.100.1    1
Default Gateway: 192.168.100.254

Persistent Routes:
None

```

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: 3**

**You are the administrator of TestKing 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.

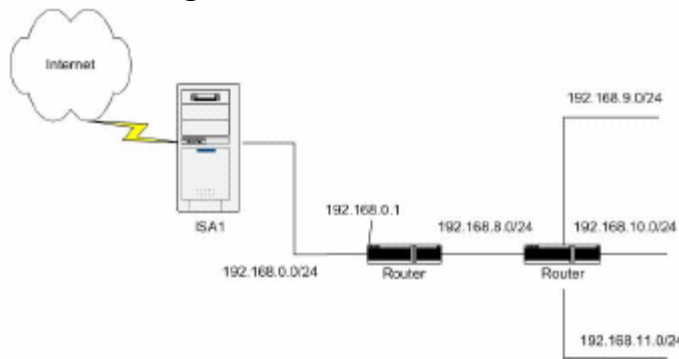
**E:** The branch office arrays should locally cache responses from the main office ISA server array.

**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 4

**You are setting up an ISA server computer named ISA1. This server will provide Internet access for users on TestKing 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.

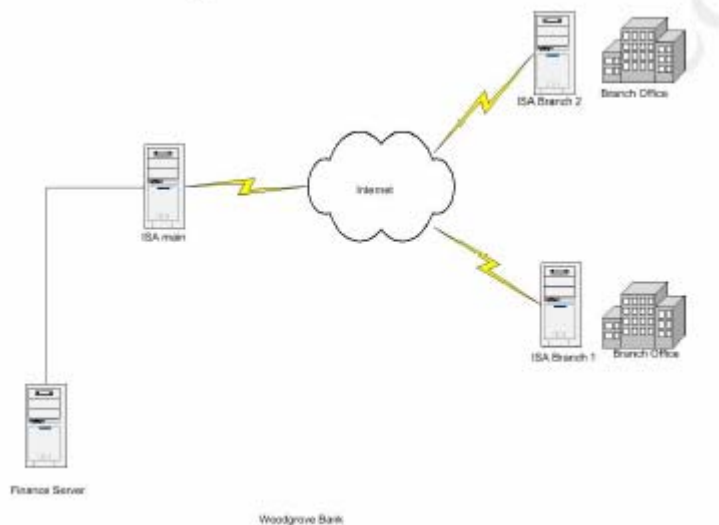
**C, D:** The -f parameter of the route command is used to clear most of the entries in the routing table. It would not be helpful in this scenario.

**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

## Section 5, Configure and troubleshoot virtual private network (VPN) access (3 questions)

### QUESTION NO: 1

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: 2**

**You are the administrator of TestKing 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 3**

**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.

**Subsection, Configure the ISA Server computer as a VPN endpoint without using the VPN Wizard (0 questions)**

**Subsection, Configure the ISA Server computer for VPN pass-through (1 question)**

### QUESTION NO 1

You are the network administrator for TestKing. 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. The results are shown in the exhibit:

| Frame | Time      | Src MAC Addr | Dst MAC Addr | Protocol |
|-------|-----------|--------------|--------------|----------|
| 21    | 9.022974  | LOCAL        | DCOM LA090E  | LCP      |
| 22    | 9.022974  | LOCAL        | DCOM LA090E  | LCP      |
| 23    | 9.022974  | LOCAL        | DCOM LA090E  | LCP      |
| 24    | 9.022974  | DCOM LA090E  | LOCAL        | PPTP     |
| 25    | 9.022974  | DCOM LA090E  | DCOM LA090E  | PPTP     |
| 26    | 9.030735  | DCOM LA090E  | LOCAL        | PPPCHAP  |
| 27    | 9.030735  | LOCAL        | DCOM LA090E  | PPPCHAP  |
| 28    | 9.103089  | DCOM LA090E  | LOCAL        | GRE      |
| 29    | 9.189219  | DCOM LA090E  | LOCAL        | TCP      |
| 30    | 9.483593  | DCOM LA090E  | LOCAL        | PPPCHAP  |
| 31    | 11.005828 | DCOM LA090E  | LOCAL        | PPPCHAP  |

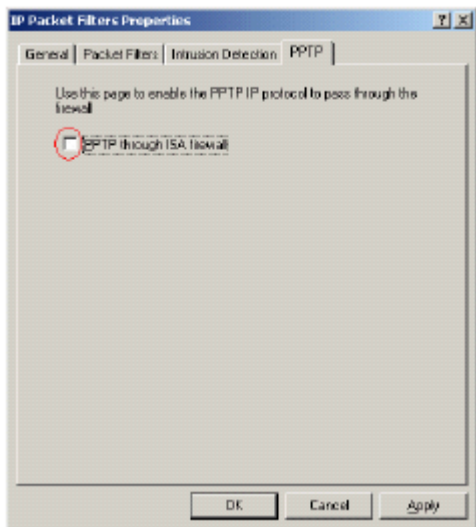
You need to reconfigure the ISA server computer so that only company-approved HTTP traffic is allowed to pass through it. What should you do?

- 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.

## **Section 6: Configure multiple ISA Server computers for scalability. Configurations include Network Load Balancing (NLB) and Cache Array Routing Protocol (CARP) (5 questions)**

### **QUESTION NO: 1**

**You are the administrator of TestKing's ISA Server computers. The ISA Server computers form a single array and are used to control Internet access. The internal network contains Microsoft Windows 2000 Professional client computers and Windows XP Professional client computers. The client computers use Microsoft Internet Explorer 6.0 to connect to the Internet.**

**You install the Firewall Client software on all the client computers. All network traffic from the client computers to the Internet is handled by the Firewall Client software. The ISA Server rules allow anonymous access to the Internet.**

**You want to improve the performance of the connections from the client computers to the Internet.**

**What should you do?**

- A. Configure the Firewall Client software to enable automatic discovery.
- B. Configure the Web browsers to use the ISA Server array as a proxy server.
- C. Configure the ISA Server array to disable the HTTP redirector filter.
- D. Configure the ISA Server array to resolve requests within the array before routing for incoming Web requests.

### **Answer: D**

The point activate CARP-Feature (Cache Array Routing Protocol) and the client questions will be answered inside the Array just before it is send to the Internet.

### **QUESTION NO: 2**

**You are the administrator of TestKing's network. The network contains Microsoft Windows 2000 Professional computers and Windows 2000 Server computers.**

**TestKing uses three Windows 2000 Advanced Server computers that run ISA Server to control Internet access. The three ISA Server computers, which are named Testking1, Testking2, and Testking3, form a single array. The Cache Array Routing Protocol (CARP) is enabled for outgoing Web requests on the array. All client computers on the network use Microsoft Internet Explorer 6.0.**

**Testking1 has a faster hard disk than Testking2 and Testking3. To optimize the use of the cache among the three servers, you want to ensure that Testking1 caches the result of 50 percent of the outgoing Web requests to the array, and Testking2 and Testking3 each cache the result of 25 percent of the outgoin Web request to the array.**

**What should you do?**

1. Configure the ISA Server properties on Testking1 to have a load factor of 200. Retain the configuration of the load factor on Testking2 and Testking3 as the default value.
2. Configure Internet Explorer on 50 percent of the client computers to use Testking1. Divide the other client computers equally between Testking2 and Testking3.
3. Implement Network Load Balancing (NLB) on the three ISA Server computers. Configure the load weight on Testking1 to be twice as high as on Testking2 and Testking3.
4. Configure the ISA Server properties on both Testking2 and Testking3 to use the IP address of Testking1 for intra-array communication.

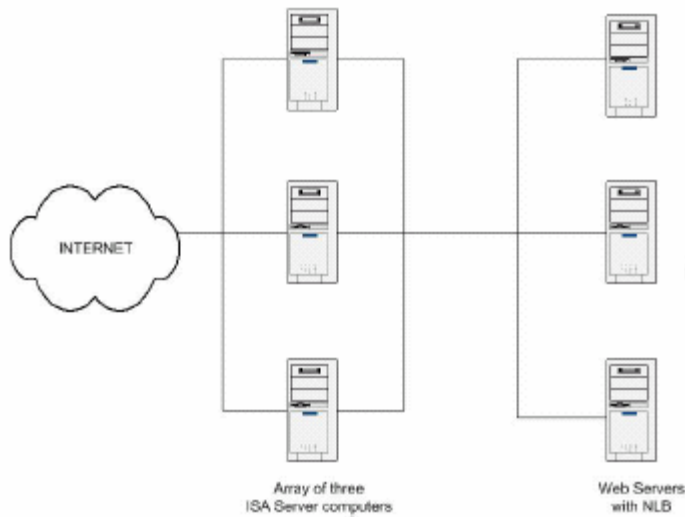
**Answer: A****Configuring Cache Array Routing Protocol**

By default, Cache Array Routing Protocol (CARP) is enabled for all the servers in the array, for outgoing Web requests. That is, the CARP algorithm will store objects in any one of the member servers' cache. By default, CARP is disabled for all incoming Web requests.

When a member server of an array determines that the requested object is not in its cache, it sends the request to another member server, using the destination server's intra-array IP address. Typically, this is the same Internet Protocol (IP) address that downstream clients and Microsoft Internet Security and Acceleration (ISA) Server computers use to communicate with this ISA Server computer. Because this value must be replicated to all ISA Server computers in the array, it is recommended that you do not change this value. For instructions on configuring a server's intra-array IP address, see Configure intra-array communication. You can configure the member servers so that different servers have different loads. For example, if one server in the array has a disk four times as large as all the other member servers, you can configure that server to receive a proportionate amount of the cache load, by configuring its load factor. The load factor determines how to divide the load among members of an array. Changing this value increases or decreases the load on an ISA Server computer. Default Load factor value = 100! Possible values: 0-200

**QUESTION NO: 3**

**You administer an array of ISA server computers. This array makes TestKing'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 outgoing 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 a 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: 4**

**You are the network administrator for Fabrikam, Inc. TestKing 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 on each 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: 5**

**You are the network administrator for TestKing. You install ISA Server on three computers named ISAServer1, 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.

## Topic 3, Configuring, Managing, and Troubleshooting Policies and Rules

### Section 1, Configure the firewall in accordance with corporate standards

**Subsection, Configure the packet filter rules for different levels of security, including system hardening (5 questions)**

#### QUESTION NO: 1

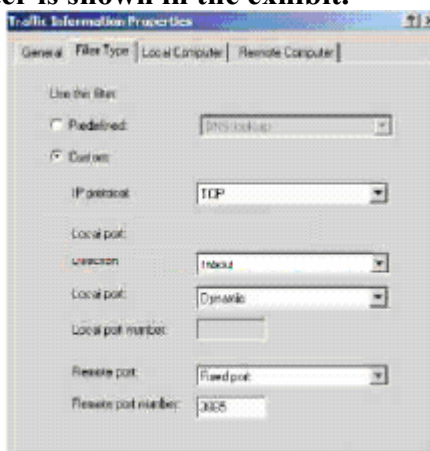
You are the network administrator for TestKing. The network contains Microsoft Windows 2000 Professional computers and Windows 2000 Server computers.

TestKing uses ISA Server to control Internet access. The ISA Server computer does not use an enterprise policy. The default site and content rule is enabled.

TestKing policy states that users are not allowed to access a specific highway traffic information application on the Internet. The application listens on TCP port 3865.

Currently, users cannot access this application on the Internet.

You want to allow access to this application for users on TestKing's network. You create a new IP packet filter. The relevant portion of the configuration of the packet filter is shown in the exhibit.



**Users on the network report that they still cannot connect to the highway traffic information application on the Internet.**

**What should you do?**

- A. Configure the properties of the IP packet filters in ISA Server to enable IP routing.
- B. Change the direction of the IP packet filter to outbound traffic instead of inbound traffic.
- C. Change the local port configuration of the IP packet filter to all ports.
- D. Delete the IP packet filter.  
Create a protocol rule that allows the use of the outbound TCP port 3865.
- E. Delete the IP packet filter.  
Create a server publishing rule that allows the use of TCP port 3865.
- F. Disable the default site and content rule.

**Answer: B**

From inside to outside not vice versa.

#### **QUESTION NO: 2**

**You administer a stand-alone ISA server computer. TestKing 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 a 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 AllowPacket 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: 3**

**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 represents 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.

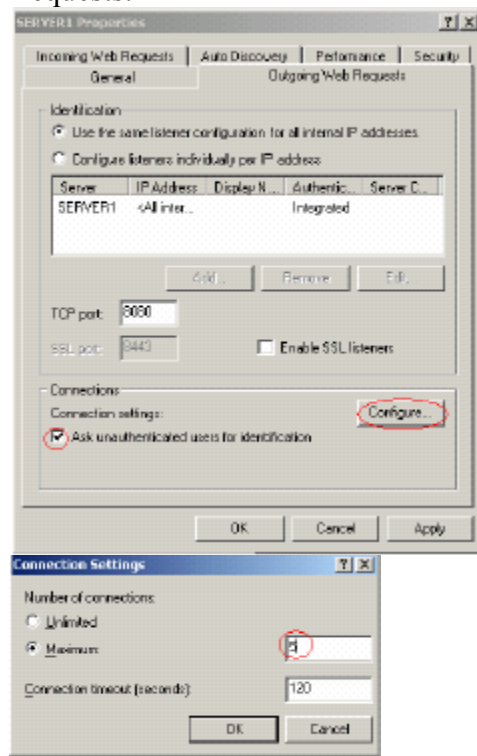
**Answer: B, C, E, G**

**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->Rightclick on the Server->Properties->Outgoing Web Requests.



**G:** We select the **Ask unauthenticated users for identification** in **Connection 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: 4**

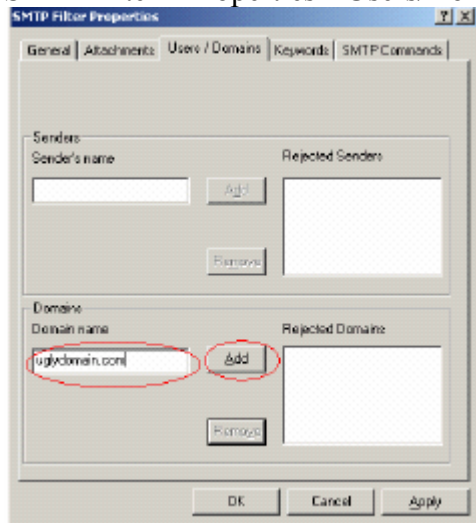
**You are the administrator of TestKing network. You install ISA server on the network to provide firewall services. Subsequently, network users report that they are receiving large amounts of unsolicited e-mail. On investigation, you discover that all the unsolicited e-mail is coming from the same Internet 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 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->Rightclick SMTP filter->Properties->Users/Domains.



**Reference:**

Technet, ISA Server Product Documentation, SMTP filter

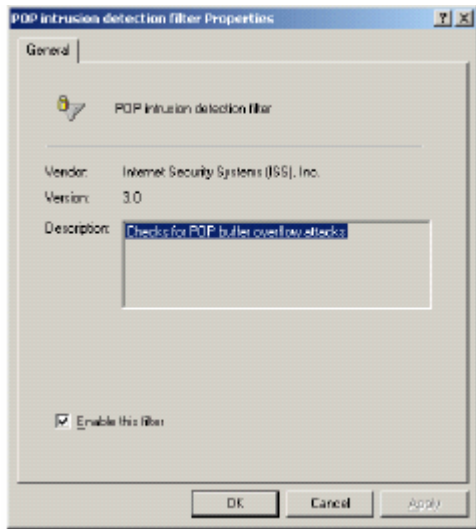
Technet, ISA Server Product Documentation, Integrated Intrusion Detection

**Incorrect Answers**

**A:** Only e-mail traffic from this specific domain should be blocked, not access in general.

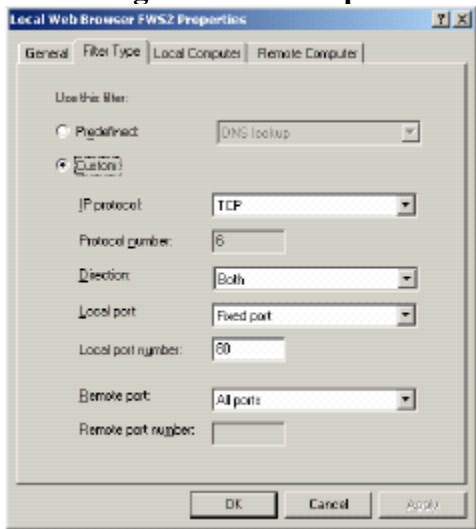
**B:** We want to block e-mail from a specific domain, not unauthorized users in general.

**C:** The POP intrusion detection filter intercepts and analyzes POP traffic destined for the internal network. The filter checks for POP buffer overflow attacks. However, you cannot configure this filter to block access from specific domains (see picture below).



### 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 try to use your Web browser on FWS2 to connect to the Internet, ISA server does 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
- 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

## **Section 2: Create and configure access control and bandwidth policies (1 question)**

### **QUESTION NO 1**

**Executives in TestKing 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

traffic

All

destinations

Always

Accounts:ISASe

rver1\Manager

3 Executives Executives

All IP

traffic

All

destinations

Always  
Accounts:ISAServer1\Executes  
4  
Administrators Administrator  
s  
All IP  
traffic  
All  
destinations  
Always  
Accounts: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.

## **Subsection, Create and configure site and content rules to restrict Internet access (6 questions)**

### **QUESTION NO: 1**

**You are the administrator of TestKing's network. The network consists of a forest that contains four Microsoft Windows 2000 domains. The ISA Server computers form a single array. You configure the ISA Server array to allow access to Web sites on the Internet. You want users to be able to connect to the Internet by designating the ISA Server array as a proxy server in the configuration properties of their Web browsers.**

**You want to forward network traffic for a specific games Web site on the Internet to an internal Web site that uses IP address 10.65.1.7.**

**What should you do?**

- A. Create a destination set that contains the games Web site.  
Create a site and content rule that denies access to the Web site in that destination set.  
Configure the rule to redirect the request to <http://10.65.1.7>.
- B. Create a destination set that contains the games Web site.  
Create a Web publishing rule that applies to that destination set.  
Configure the rule to redirect the requests to <http://10.65.1.7>.
- C. Create a server publishing rule that uses the IP address of the games Web site as the external IP address and uses 10.65.1.7 as the internal IP address.
- D. Create an IP packet filter that uses the IP address of the games Web site as the remote computer and uses 10.65.1.7 as the IP address of the local computer.  
Add the games Web site to the local domain table.

### **Answer: A**

Site and content rules can either allow or deny access to specific sites. If access is denied, then for Hypertext

Transfer Protocol (HTTP) objects, the request can be redirected to an alternate Uniform Resource Locator

(URL)—typically a page on an internal server—explaining why access is denied.

When you specify the destination to which to redirect the request, you can specify a whole different location by typing <http://> and then the URL of the location to which to redirect the request.

When access is denied, ISA Server sends the URL specified here to the Web browser client. The client Web browser then tries to access the object from the destination to which ISA Server redirected.

For example, suppose a site and content rule denies access to

<http://example.microsoft.com/>, redirecting

requests for this site to <http://widgets.microsoft.com/accessdenied.htm>. When a client requests an object on

<http://example.microsoft.com/>, ISA Server denies the request, and returns

<http://widgets.microsoft.com/accessdenied.htm> to the client. The client then requests

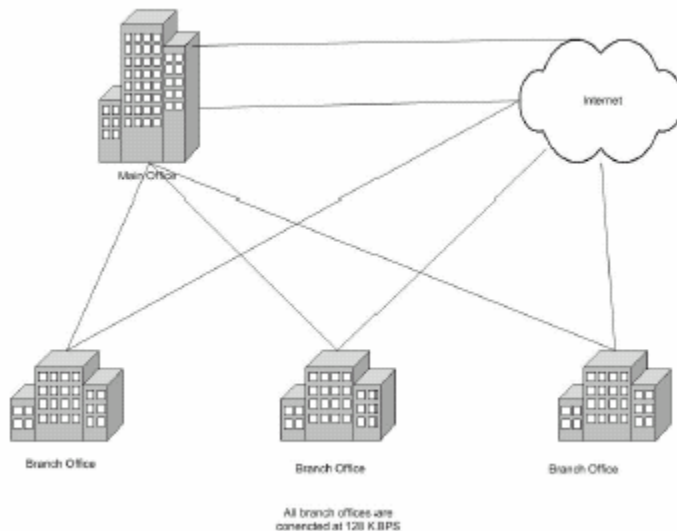
<http://widgets.microsoft.com/accessdenied.htm>.

Important

- If you choose to redirect the request, then the URL that you specify must be accessible to the selected clients or users. In other words, either the URL must be on an internal computer or some rule must explicitly allow access to the URL.

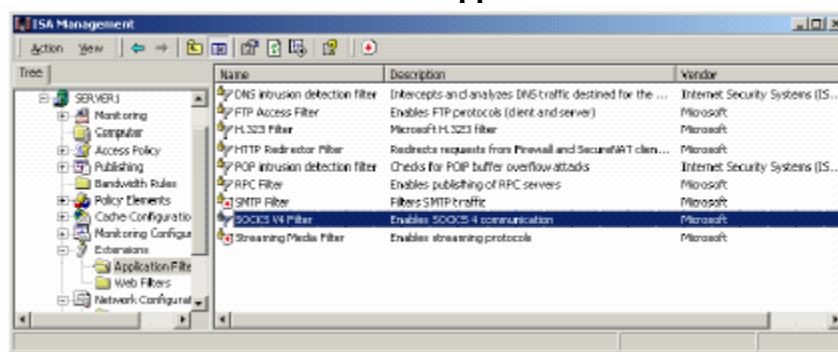
## QUESTION NO: 2

**You are the administrator of TestKing 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

MMS

protocol

Enterprise

Enterprise

Deny

Allow

PNM--Real Networks protocol (Client), PNM—Real

Networks protocol (Server)

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 mediarelated access problems.

### **QUESTION NO: 3**

**You are the administrator of TestKing 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 simply remove the User-No Access Rule. The Sales and Managers would then gain appropriate access.

Another possible solution, not listed here though, would be 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 1<sup>st</sup> 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: 4**

**You are the administrator of TestKing 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  | Client Sets: Accounting Users | Work hours | Accounting       |
| After Hours      | Enterprise | Allow  | Client Sets: Company Users    | Always     | All destinations |
| Finance Users    | Enterprise | Allow  | Client Sets: Finance Users    | Work hours | Finance          |
| Management       | Enterprise | Allow  | Client Sets: Management Users | Always     | All destinations |
| Marketing Users  | Enterprise | Allow  | Client Sets: Marketing Users  | Work hours | Marketing        |
| MIS Department   | Enterprise | Allow  | Client Sets: Admins           | Always     | All destinations |
| Sales Users      | Enterprise | Allow  | Client Sets: 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: 5

**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 TestKing network belong to a single Microsoft Windows 2000 domain.**

**Fabrikam, 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 gamesrelated 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: 6

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](http://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](http://www.litware.com/apps/patches), but they should not be allowed to access any other area of [www.litware.com](http://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](http://www.litware.com/apps/patches) you examine the site and content rules that apply to [www.litware.com](http://www.litware.com) these rules are configured as shown here:



| Name            | Scope      | Action | Applies to                  | Schedule | Destination               |
|-----------------|------------|--------|-----------------------------|----------|---------------------------|
| Litware Patches | Enterprise | Allow  | Client Set: Software Admins | Always   | Litware Patches           |
| Litware Site    | Enterprise | Deny   | Any request                 | Always   | Litware Entire Site       |
| Allow All       | Enterprise | Allow  | Any request                 | Always   | All external destinations |

The destination set named “Litware entire site” applies to [www.litwareinc.com](http://www.litwareinc.com) the destination set named “Litware patches” applies to [www.litware.com/apps/patches](http://www.litware.com/apps/patches) You want to ensure that the company's policy regarding access to [www.litware.com](http://www.litware.com) and [www.litware.com/apps/patches](http://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.

### **Subsection, Create and configure protocol rules to manage Internet access (7 questions)**

#### **QUESTION NO: 1**

**You are the network administrator for TestKing. You install and configure ISA Server with default settings on a network computer. Users in your Sales group configures 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 email. What should you do?**

- A. Create an SMTP protocol rule and a POP3 protocol rule to allow external access. Configure each rule to include the Sales group.
- B. Create an SMTP server protocol rule and a POP3 server 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**

Here it is sending and receiving emails through protocol role.

#### **QUESTION NO: 2**

**You are the network administrator for TestKing. The network contains Microsoft Windows 2000 Professional computers and Windows 2000 Server computers. All computers on the network are in the same Windows 2000 forest. TestKing uses ISA Server to control Internet access. In TestKing's main office, network connections in the conference room are on a different internal IP subnet from all other network connections. You want computers in the conference room to be able to connect to other computers on TestKing's network. However, you do not want computers in the conference room to connect to the Internet. All other computers on TestKing's network are allowed to connect to the Internet.**

**What should you do?**

- A. Create a destination set for the conference room IP.  
Create a site and content rule that applies to this destination set.  
Configure the rule to deny access.
- B. Create a client address set for the conference room IP subnet.  
Create a protocol rule that applies to this client address set.  
Configure the rule to deny requests.
- C. Create a new packet filter rule that blocks packet transmission.  
Configure the rule to apply to all IP addresses from the conference room IP subnet.
- D. Create a new local address table entry for all IP addresses from the conference room IP subnet. Restart the Firewall service.

**Answer: B**

Install client address sentences for policy element and use it inside of protocol rule. At outbound access the client address sentences are internal computers.

#### **QUESTION NO 3**

**You are the network administrator for TestKing. 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: 4**

**You are the network administrator for TestKing. 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: 5**

You are the administrator of TestKing 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. TestKing 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: 6**

You are the network administrator for TestKing. 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 email 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: 7**

**You are the network administrator for TestKing. 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 Enterp rise

FTP,FTP

download

only

Allow Accounts:

MILLERTEXTILES\Domain

Users

Always

Global

Catalog

Enterp

rise

Any RPC  
Server  
Allow Any Request Always  
HTTP\_Users Enterp  
rise  
HTTP Allow Accounts:  
MILLERTEXTILES\Sales  
Always  
HTTPS Enterp  
rise  
HTTPS Allow Accounts:  
MILLERTEXTILES\Marketin  
g  
Always  
LDAP Enterp LDAP GC Allow Any Request Always  
rise (Global  
Catalog)  
Mail Enterp  
rise  
POP3, SMTP Deny Accounts:  
MILLERTEXTILES\Graphics  
Weekends  
NNTP Enterp  
rise  
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.

**Subsection, Create and configure routing rules to restrict Internet access (0 questions)**

**Subsection, Create and configure bandwidth rules to control bandwidth usage (0 questions)**

**Section 3, Troubleshoot access problems**

**Subsection, Troubleshoot user-based access problems (1 question)**

**QUESTION NO: 1**

You are the administrator of TestKing's network. The network contains Microsoft Windows 2000 Professional client computers and Windows 2000 Server computers. You want to install ISA Server on a Windows 2000 Server computer named Testking1. Testking1 contains one network adapter that is connected to the internal network and another network adapter that is connected to the Internet. You configure each network adapter so that it has a static IP address. The configuration of the network adapters is shown in this table.

| Testking1 IP Address     | Subnet Mask | Default Gateway |
|--------------------------|-------------|-----------------|
| Internal network adapter | 10.65.7.2   | 255.255.255.0   |
| 10.65.7.1                |             |                 |
| External network adapter | 23.1.8.6    | 255.255.255.240 |
| 23.1.81                  |             |                 |

The configuration of the relevant portion of the network is shown in the exhibit. You want to configure the TCP/IP settings of the appropriate network adapter on Testking1 so that client computers can connect to the Internet after you install ISA Server. What should you do?

- A. On the internal network adapter, remove the default gateway setting.
- B. On the internal network adapter, change the subnet mask to 255.255.0.0.
- C. On the external network adapter, remove the default gateway setting.
- D. On the external network adapter, change the default gateway to 23.1.8.6

**Answer: C**

An ISA server without a standard Gateway.

**Subsection, Troubleshoot packet-based access problems (0 questions)**

## **Section 4, Create new policy elements. Elements include schedules, bandwidth priorities, destination sets, client address sets, protocol definitions, and content groups (5 questions)**

### **QUESTION NO: 1**

**You are the administrator for TestKing's network. The network consists of a single Microsoft Windows 2000 domain. All server computers run Windows 2000 Server. The network includes Windows XP Professional and Macintosh client computers.**

**The Windows XP Professional computers are configured as Web Proxy and Firewall clients. The Macintosh computers are configured as Web Proxy and SecureNAT clients.**

**The network uses an ISA Server array that is installed in integrated mode to control Internet access and to provide Web caching services. You create a site and content rule that allows unrestricted access to all sites. You also create a protocol rule that allows unrestricted access to all application protocols.**

**The users of the Macintosh computers report that they cannot access certain Internet resources by using**

**a third-party sockets-based application. The users of the Windows XP Professional computers do not report problems when they use the same application.**

**You need to ensure that the users of the Macintosh computers can access resources by using the application.**

**What should you do?**

- A. Create a client address set that includes the IP addresses of the Macintosh computers. Create a new site and content rule that specifically allows access for the computers listed in the client address set.
- B. Create a destination set that includes the fully qualified domain names (FQDNs) of the affected sites. Create a new site and content rule that specifically allows access to the sites listed in the destination set.
- C. Create a new protocol definition for the protocol used by the third-party application. Restart the Firewall service.
- D. Create a new content group that specifies the type of content being accessed by the third-party application. Restart the Web Proxy service.

**Answer: C**

### **QUESTION NO 2**

**You are the administrator of TestKing network, which includes an ISA serve 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 3**

**You are the administrator of TestKing 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: 4**

**You are the administrator of TestKing'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 mspoint.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: 5**

**You administer TestKing 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.

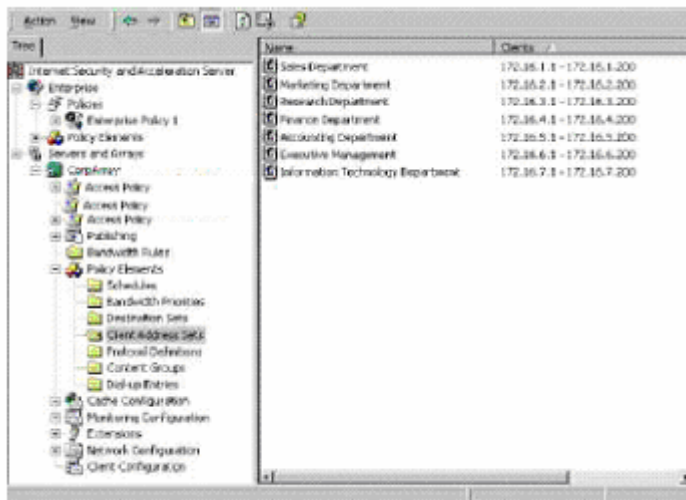
**B:** A bandwidth priority of 10 would increase the priority of HTTP traffic. HTTP traffic would not be decreased-

**C:** The content download must not be scheduled during working hours. We want to decrease HTTP traffic during working hours.

## **Section 5: Manage ISA Server arrays in an enterprise (3 questions)**

### QUESTION NO: 1

You are the administrator of TestKing's network. The network consists of a single Microsoft Windows2000 domain. All server computers run Windows 2000 Server. All client computers run Windows 2000 Professional. The network uses an ISA Server array to control Internet access. The ISA Server array consists of three Windows 2000 Server computers. The array is configured by means of an enterprise policy. You need to create rules to limit the Internet sites that employees can access. Each department has different requirements and restrictions for its employees. You create client address sets based on department, as shown in the exhibit.



However, when you attempt to create new site and content rules or new protocol rules in the default enterprise policy, none of the client addresses sets you created are available to select.

What should you do?

- A. Add the address ranges for the client addresses sets to the local address table.
- B. Configure the ISA Server array to use only an array policy.
- C. Re-create the client addresses sets in the enterprise-level policy elements.
- D. Create a new custom enterprise policy that allows an array policy.

**Answer: C**

This is a company group policy, the specified Policy Elements must be placed under the Enterprise knot, not on Array area.

### QUESTION NO: 2

You are the enterprise administrator of TestKing's network. The network consists of a single Microsoft Windows 2000 forest that contains four domains. TestKing has regional offices located in Berlin, New York, and Tokyo. Each regional office supports several smaller branch offices throughout its region. Each regional office uses an ISA Server array to control Internet access. All branch offices contain at least one ISA Server computer that is configured as an array member in an array

that is specified to each branch office. The domain administrators in each regional office need to be able to define policies and rules to control Internet access for all users in their region. The protocols that users are allowed to use vary by region. The regional domain administrators also need to be able to change their policies as requirements change, without intervention or assistance from company IT department. Administrators must not be able to change policies that apply to other regions. What should you do to accomplish these goals?

- A. Create a single enterprise policy and assign it to all arrays.  
Configure each array to allow array-level access policy.  
Add the Domain Admins group from each domain to the Enterprise Admins group.
- B. Create a single enterprise policy and assign it to all arrays.  
Configure each array to allow array-level access policy.  
Grant the Domain Admins groups from each domain the **Allow – Full Control** permission to the enterprise policy.
- C. Create a separate enterprise policy for each region and assign it to all arrays in that region.  
Add the Domain Admins group from each domain to the Enterprise Admins group.
- D. Create a separate enterprise policy for each region and assign it to all arrays in that region.  
Grant the Domain Admins groups from each domain the **Allow – Full Control** permission to the regionspecific enterprise policy.

**Answer: D**

To configure enterprise permissions

1. In the console tree of **ISA Management**, right-click **Enterprise** and then click **Properties**.

Where?

- o Internet Security and Acceleration Server
- o Enterprise

2. On the **Security** tab, do one of the following:

- o To allow additional users or groups permissions to modify the configuration:

Click **Add**, click the users or groups to add and click **OK**.

In **Name**, click a user or group and, in **Permissions**, select the appropriate check boxes.

- o To deny a user or group permission to modify the configuration, in **Name**, click a user or group and then click **Remove**.

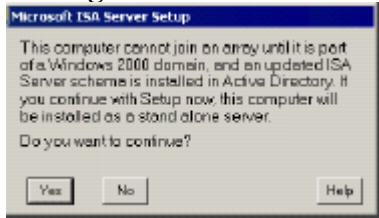
Notes

- To open ISA Management, click **Start**, point to **Programs**, point to **Microsoft ISA Server**, and then click **ISA Management**.

**QUESTION NO 3**

You are the administrator of TestKing 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 server1 as 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, 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.

**Subsection, Create an array of proxy servers (0 questions)**  
**Subsection, Assign an enterprise policy to an array (1 question)**

**QUESTION NO: 1**

**You are the administrator of TestKing'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**



**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.

## **Topic 4, Deploying, Configuring, and Troubleshooting the Client Computer**

### **Section 1, Plan the deployment of client computers to use ISA Server services. Considerations include client authentication, client operating system, network topology, cost, complexity, and client function (6 questions)**

#### **QUESTION NO: 1**

**You are the administrator for Testkingonline.com's ISA Server computers. TestKing uses the ISA Server computers to control Internet access. Users on TestKing's network use Microsoft Windows 2000 Professional computers to connect to WEB sites on the Internet. TestKing does not use ISA Server's Scheduled to Context Download service.**

**TestKing policy requires a user name to be logged for all Web connections to the Internet. You notice that in the log file for the Web Proxy service, most of the logged connections are listed with a user name, but that some of the logged connections are listed as anonymous. Users report that they can connect to Web sites on the Internet successfully.**

**You want to ensure that a user name is logged for each Web connection to the Internet. What should you do?**

- A.** Change the ISA Server computer's Web Proxy service log file format to use the ISA Server file format.
- B.** Configure the outgoing Web requests properties of the ISA Server computers to enable the use of Basic authentication for the IP listeners.
- C.** Configure the outgoing Web requests properties of the ISA Server computers to ask unauthenticated users for identification.
- D.** Configure the HTTP redirector filter to reject HTTP requests from Firewall and SecureNAT clients.

**Answer: C**

**Incorrect answers:**

**A:** Nothing changed!

**B:** Next step, if you have third party browsers!

D: Not working, we have to enable user identification!

## QUESTION NO: 2

You work as a network administrator at TestKing. You are preparing a Microsoft Windows 2000 Server computer for the installation of ISA Server. You install two network adapters on this computer. One network adapter is connected to the Internet and the other is connected to your internal network. When you issue a command to check the open ports on both network adapters, you receive the output shown in the exhibit.

| Proto | 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   | 0.0.0.0:1029       | 0.0.0.0:0        | LISTENING   |
| TCP   | 0.0.0.0:1046       | 0.0.0.0:0        | LISTENING   |
| TCP   | 0.0.0.0:1723       | 0.0.0.0:0        | LISTENING   |
| TCP   | 0.0.0.0:3087       | 0.0.0.0:0        | LISTENING   |
| TCP   | 0.0.0.0:3010       | 0.0.0.0:0        | LISTENING   |
| TCP   | 0.0.0.0:3026       | 0.0.0.0:0        | LISTENING   |
| TCP   | 0.0.0.0:3722       | 0.0.0.0:0        | LISTENING   |
| TCP   | 0.0.0.0:2138       | 0.0.0.0:0        | LISTENING   |
| TCP   | 131.107.2.2:139    | 0.0.0.0:0        | LISTENING   |
| TCP   | 131.107.2.2:3027   | 192.168.0.1:139  | TIME_WAIT   |
| TCP   | 192.168.0.254:139  | 0.0.0.0:0        | LISTENING   |
| TCP   | 192.168.0.254:1029 | 192.168.0.2:445  | ESTABLISHED |
| TCP   | 192.168.0.254:1032 | 192.168.0.2:135  | TIME_WAIT   |
| TCP   | 192.168.0.254:1033 | 192.168.0.2:1029 | TIME_WAIT   |

Before you install ISA Server, you want to configure this computer so that unauthorized external client computers cannot discover that it is capable of sharing resources. You must also maintain the highest possible level of security. What should you do?

- A. On the network adapter configured with the IP address 192.168.0.254, disable NetBIOS over TCP/IP.
- B. On the network adapter configured with the IP address 131.107.2.2, disable NetBIOS over TCP/IP.
- C. On the network adapter configured with the IP address 192.168.0.254, disable **File and Printer Sharing for Microsoft Networks**.
- D. On the network adapter configured with the IP address 131.107.2.2, disable **File and Printer Sharing for Microsoft Networks**.

**Answer : D**

### **Explanation :**

You should always disable file and print sharing for Microsoft networks on the external interface and even for the internal interface of the ISA computer. Due to the inherently insecure nature of the file-sharing protocol (SMB) used on Microsoft systems, you should never expose the file system to SMB access. The ISA server should be a device dedicated to firewall and/or Web-caching functions and should not be used as a file or network application server. You should also disable the NetBIOS interface on the external interface. No machine on the Internet needs access to the ISA server via NetBIOS over

TCP/IP; such access could provide an avenue for attackers to compromise your ISA server. When configuring the Windows 2000 machine that runs ISA server as a bastion host, the first thing you should do is disable the Client for Microsoft Networks. However,

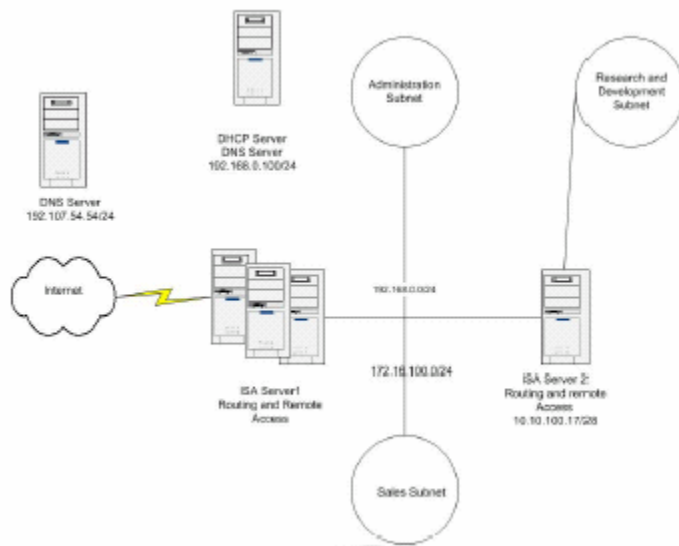
if you are running IIS on the ISA server machine, you should not do this because IIS will not start if you disable the Client for Microsoft Networks. Otherwise, be sure to disable this service on each network adapter. Another networking feature that is not required on the ISA server is the NetBIOS interface. You can disable the NetBIOS interface from the Advanced TCP/IP dialog box. However, this only disables attaching to Windows shares through the NetBIOS interface. Windows 2000 features a new way to access SMB shares through a method called direct hosting. This method uses DNS for name resolution, and shares are connected to via TCP Port 445. In order to prevent an intruder from attaching to a share via direct hosting, you need to disable the nbt.sys (the NetBIOS over TCP/IP driver). Ip address 131.107.2.2 is the external NIC and that NIC must be highly secured.

**Reference :**

Syngress - Microsoft Windows 2000 Isa Server 2000 Study Guide

**QUESTION NO 3**

**You are the administrator of TestKing 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 ..... : 00-01-02-45-3E-5A
DHCP Enabled ..... : Yes
Autoconfiguration Enabled ..... : Yes
IP Address ..... : 10.10.100.19
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: 4**

**You are the administrator of TestKing 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: 5**

**You are the administrator of TestKing 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.

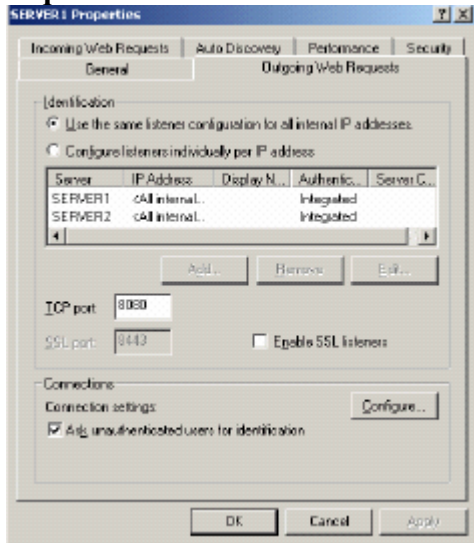
**B:** The scenario does not allow creation of trusts.

**C:** Windows integrated authentication would not work since the sites are placed in different domains and no trusts are used.

#### **QUESTION NO: 6**

**You are the administrator of an array of two ISA server computers. TestKing 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.

## Section 2, Configure and troubleshoot the client computer for security-enhanced network address translation (SecureNAT) (7 questions)

QUESTION NO: 1

**You are the administrator of TestKing's network. The network consists of a single Microsoft Windows 2000 domain. All server computers run Windows 2000 Server. All client computers run Windows XP Professional. The network contains an ISA Server computer to control Internet access. All client computers are configured as Web Proxy and Firewall clients. Several users in the Warehousing department need to be able to connect securely to a vendor's network to view the availability of and to order new products. The vendor configured a PPTP VPN server to allow this secure access. You enable the PPTP through ISA firewall option in the IP packet filter properties. Next, you configure the PPTP VPN connections on the client computers to connect to the VPN server on the vendor's network. When a user attempts to establish a VPN connection with the server, the connection fails. You need to allow the users to successfully establish VPN connections to the vendor's network through the ISA Server computer. What should you do?**

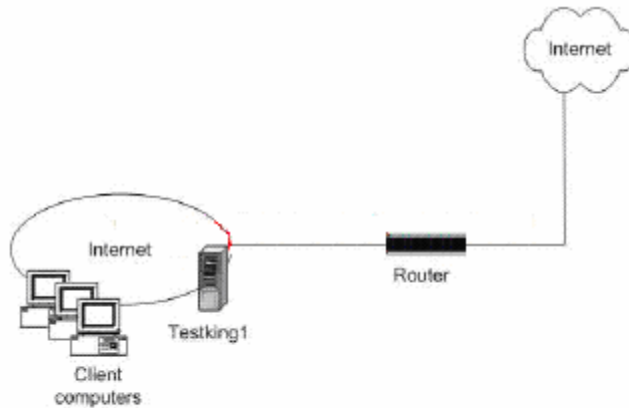
- A. Configure the client computers as SecureNAT clients.
- B. Create a new packet filter to allow outbound access on TCP port 1723.
- C. Create a new protocol rule to allow the users to use the PPTP protocols.
- D. Enable IP routing on the ISA Server computer.

**Answer: A**

VPN clients must be SecureNAT clients, and in this case, PPTP protocol is already defined, because in the question it says "you enable the PPTP through ISA firewall option in the packet filter properties".

#### **QUESTION NO: 2**

**You are the network administrator for TestKing. The network includes 2,000 Microsoft Windows XP Professional client computers and 5,000 Windows 98 client computers. The network has a single 512-Kbps connection to the Internet. All users use Microsoft Internet Explorer as their only Web browser. All users use non-Microsoft software for Internet instant messaging. You install and configure a new ISA Server computer named Testking1. Testking1 contains a single network adapter. The relevant portion of the new network configuration is shown in the exhibit.**



**You need to configure all client computers to use Testking1's cache for all Web browsing. You need to ensure that other Internet connectivity is not affected. What should you do?**

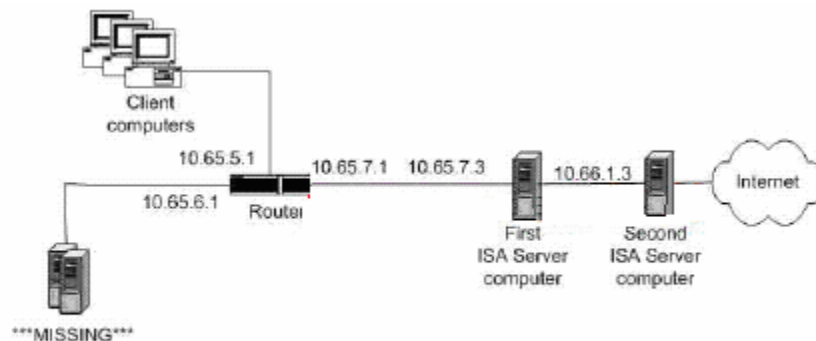
- A. Configure all client computers as ISA Server SecureNAT clients.
- B. Configure all client computers as ISA Server Web Proxy clients.
- C. Configure all client computers to use the Firewall Client software.
- D. Configure all client computers so that Internet Explorer uses <http://testking1> as their home page.

**Answer: A**

If you use SecureNAT clients in this scenario, you will not have to deploy any special software or configure the client computers. Instead, client requests are transparently passed to the ISA Server Firewall service and then on to the Web Proxy service for caching.

**QUESTION NO: 3**

**You are the administrator of TestKing's network. TestKing uses a DSL connection to the Internet. A diagram of the relevant portion of the network is shown in the exhibit.**



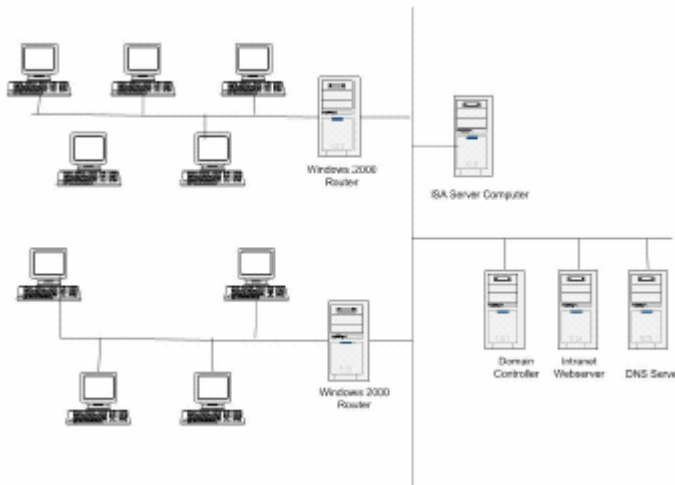
**You want to configure the client computers as SecureNAT clients.  
How should you configure the default gateway of the client computers?**

- A. Use the IP address of the router on the client computers subnet, 10.65.5.1.
- B. Use the IP address of the router on the first ISA Server computer subnet, 10.65.7.1.
- C. Use the internal IP address of the first ISA Server computer, 10.65.7.3.
- D. Use the internal IP address of the second ISA Server computer, 10.66.1.3.

**Answer: A**

#### **QUESTION NO 4**

**You are planning to configure the ISA client computers in TestKing 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: B, C, F**

**Explanation:**

**B:** To configure SecureNAT clients on a network with routers, set the default gateway settings to the router

closest to the SecureNAT client. Ensure that the router is configured to forward IP packets to the Internet so

that all packets are routed through the ISA Server computer. Optimally, routers should use a default gateway

that routes along the shortest path to the ISA Server computer. In addition, do not configure routers to

discard packets destined for addresses outside of the internal network. The ISA Server computer will

determine how to route these packets.

**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:**

MOC2159a Deploying and managing Microsoft Internet Security and Acceleration Server 2000 - Module 2 - Page 19

[http://www.isaserver.org/tutorials/Designing\\_An\\_ISA\\_Server\\_Solution\\_on\\_a\\_Complex\\_Network.html](http://www.isaserver.org/tutorials/Designing_An_ISA_Server_Solution_on_a_Complex_Network.html)

**Incorrect Answers:**

**A:** To configure SecureNAT clients on a network with routers, set the default gateway settings to the router

closest to the SecureNAT client.

**D:** We still need to provide access to internal resources.

**E:** Protocol rules are preferred to packet filters.

**QUESTION NO: 5**

**You are the administrator for TestKing 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.

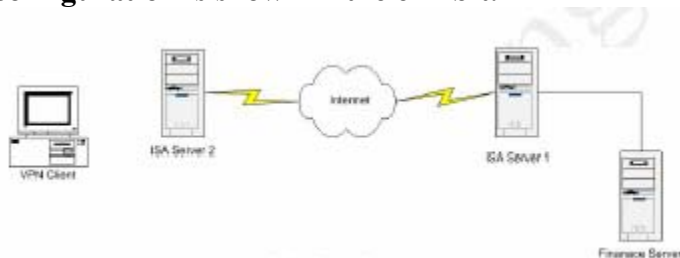
**Reference:** Increasing Security on Windows 2000 VPN Server (Q255784)

**Incorrect Answers**

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

#### QUESTION NO 6

You are the administrator of TestKing 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 VPNclient1 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.

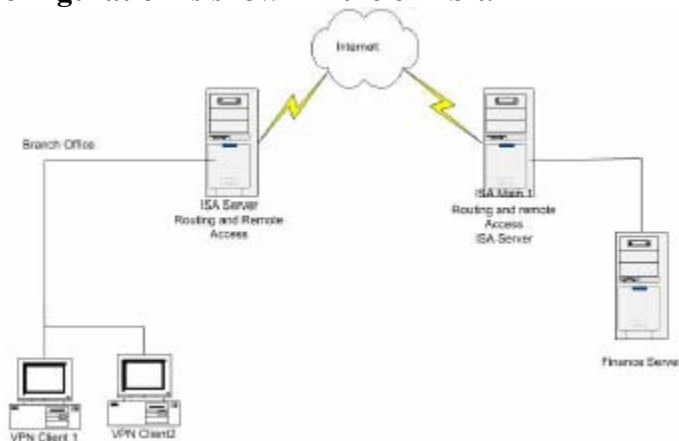
**Incorrect Answers**

**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: 7

**You are the administrator of TestKing 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.

**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.

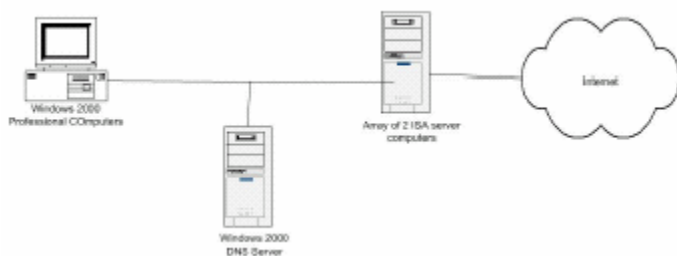
**D:** This proposed solution does not make sense. There is no such thing as executing IP addresses in the LAT.

Furthermore, an external IP address cannot be used on the internal network.

### Section 3, Install the Firewall Client software. Considerations include the cost and complexity of deployment (4 questions)

#### QUESTION NO 1

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

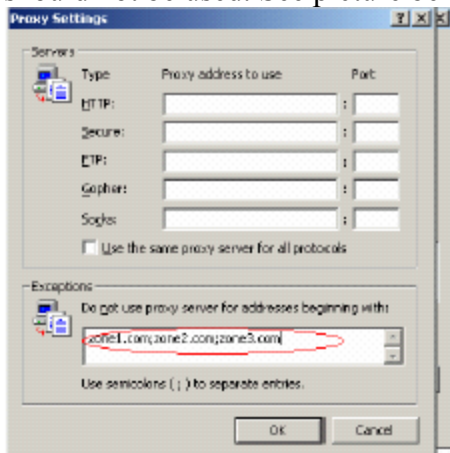
**You need to ensure that all DNS name requests for the internal network are sent to the internal DNS servers. This condition includes DNS names by Internet explorer and by the firewall client software. Which two actions should you take? Each correct answer presents part of the solution. (Choose two)**

- 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**

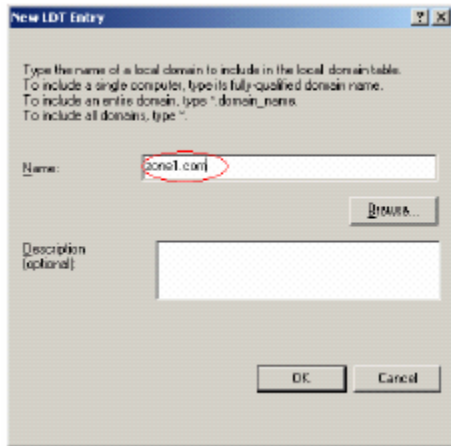
**Explanation:** We must configure Internet Explorer and the firewall clients separately.

**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: 2**

**You are the network administrator for TestKing. The network includes a Microsoft Windows 2000 domain. You purchase a new Windows 2000 Server computer named Testking1 and join it to the domain.**

**You run ISA Server Setup on Testking1. You want to make Testking1 the first member of a new ISA Server array. However, Setup informs you that ISA Server can only be installed as a stand-alone server.**

**You cancel Setup. You need to ensure that ISA Server can be installed on TestKing1, and that TestKing1 can be made the first member of a new ISA Server array.**

**What should you do on Testking1?**

- A. Run msisaent.exe from the ISA Server CD-ROM.
- B. Run rmisa.exe from the ISA Server CD-ROM.  
Run Setup.
- C. Log on as a member of the domain Enterprise Admins group.  
Run Setup.

D. Run rmisa.exe from the ISA Server CD-ROM.  
Force Active Directory to replicate.

**Answer: A**

Before you can set up Microsoft Internet Security and Acceleration (ISA) Server as an array member, the ISA Server schema must be installed to Active Directory. ISA Server includes an Enterprise Initialization utility that you can use to install the ISA Server schema in Active Directory. For details on how this impacts the Active Directory, see Active Directory. After the ISA Server schema is imported, all subsequent ISA Server installations to computers in the domain can use the ISA Server schema. You do not have to install the schema again. For more information, see The enterprise and arrays and Initialize the enterprise. 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

**QUESTION NO 3**

**You are the administrator of TestKing network, which consists of one Microsoft Windows 2000 domain and one site and a ISA server computer named DeviISA is dedicated to TestKing'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: 4**

**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. TestKing 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 we 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

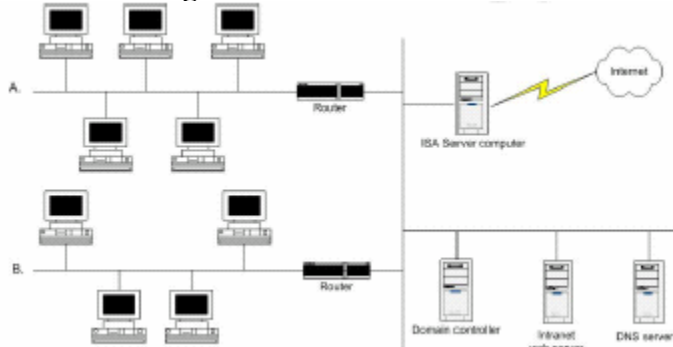
**Incorrect Answers**

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

## Subsection, Troubleshoot autodetection (1 question)

### QUESTION NO 1

You are deploying ISA server in TestKing 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 Firewall 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.

## Section 4, Configure the client computer's Web browser to use ISA Server as an HTTP proxy (12 questions)

**QUESTION NO: 1**

**You are the administrator of TestKing's network. The network consists of a single Microsoft Windows 2000 domain. All server computers on the network run Windows 2000 server. All client computers run Windows XP Professional or MAC OS X. All client computers use Microsoft Internet Explorer 5.0 or later. You install an ISA Server computer to control Internet access. All users are allowed to access any Internet-based Web site by using HTTP or HTTPS. You configure ISA Server and the client computers' Web browsers to use an automatic configuration script. Later, users report that when they attempt to access an intranet Web server named Testking1, response times are unacceptably slow. You investigate and discover that requests issued to <http://testking1> are being directed to the ISA Server computer. You want to ensure that the client computers always directly access Testking1. What should you do?**

- A. In the Web browser client configuration settings, select the **Bypass proxy for local servers** check box.
- B. Add the fully qualified domain name (FQDN) of Testking1 to the local domain table.
- C. In ISA Management, add Testking1's IP address to the local address table.
- D. Create a new routing rule to redirect requests to internal destinations to Testking1.

**Answer: A**

Automatic configuration will be done, but this is not complete finished.

**QUESTION NO: 2**

**You are the administrator of TestKing's network. The network consists of a single Active Directory forest that contains five Microsoft Windows 2000 domains. All client computers on the network run Windows 2000 Professional and use Microsoft Internet Explorer 5.5 to connect to the Internet. All client computers are in the domains. Windows NT Server 4.0 computers that run Microsoft Proxy Server 2.0 control Internet access. You want to migrate the Windows NT Server 4.0 computers that run Proxy Server to Windows 2000 Server computers that run ISA Server. You stop the Proxy Server service. You upgrade the Windows NT Server 4.0 computers to Windows 2000, and then you install ISA Server on the Windows 2000 Server computers. After the migration, users report that they cannot connect to the Internet. You want to change the configuration of the Windows 2000 Professional computers so that users can connect to the Internet. What should you do?**

- A. Configure the default gateways to the internal IP address of an ISA Server computer.
- B. Install the Firewall Client software on the Windows 2000 Professional computers.
- C. Configure Internet Explorer to use proxy port 8080.

D. Configure Internet Explorer so that it does not bypass the proxy server for local addresses.

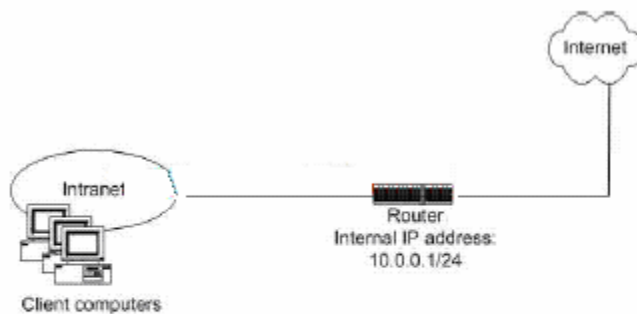
**Answer: C**

### **Web Proxy Client Requests**

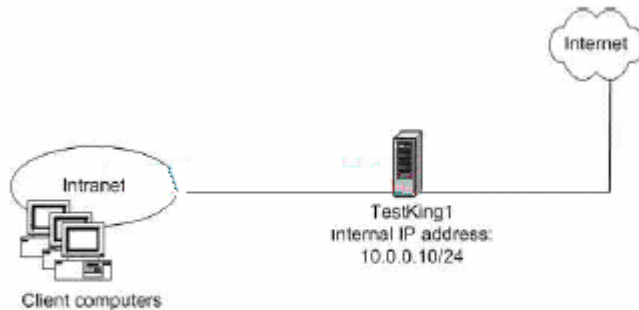
Proxy Server 2.0 listened for client HTTP requests on port 80, but when ISA Server is installed, it listens on port 8080 for the Web Proxy service. Therefore, all downstream chain members (or browsers) connecting to the ISA Server computer must connect to port 8080. You can also configure ISA Server to listen on port 80.

### **QUESTION NO: 3**

**You are the network administrator for one of TestKing's branch offices. The branch office includes 10 Microsoft Windows XP Professional client computers, 5 Windows 98 client computers, 10 Macintosh client computers, and 5 UNIX-based client computers. All client computers use Microsoft Internet Explorer as their only Web browser. All client computers also use internet-based instant messaging software. All client computers are on a single subnet. The relevant portion of the network is shown in the exhibit.**



**You replace the existing network firewall with a new ISA Server computer named Testking1. Testking1 will function as both a firewall and a cache for Web browser traffic for all network client computers. The relevant portion of the network configuration is shown in the exhibit.**



**You need to ensure that all client computers will work with Testking1. What should you do?**

- A. Configure all client computers to use 10.0.0.10 as their default gateway.
- B. Configure the local address table on Testking1 to include 10.0.0.0/24.
- C. Configure Internet Explorer on all client computers to use Testking1 as the proxy server.
- D. Configure the Windows 98 and Windows XP Professional computers to use the Firewall Client software.

**Answer: C**

All computers, Win XP,98, Mac and Unix, us'ing IE! All we need is Web Proxy Clients. So we have to configure the IE on all clients computer to use Testking1 as the proxy server!

**Incorrect Answers**

- A: Secure NAT Clients not working. All we need is Web Proxy Clients.
- B: 10.0.0.0/24, Don't use this IP address! Back to the basics!
- D: We have also Unix and MAC's in our network!

#### **QUESTION NO: 4**

**You are the network administrator for Testkingonline.com. Your purchase a new Microsoft Windows 2000 Server computer named Testking1. Testking1 contains three hard disks. Each hard disk is configured as a single logical drive.**

**You install ISA Server on Testking1. You instruct ISA Server Startup to install ISA Server's program files to drive C and use drive D for cache files.**

**After Setup finishes, you review the application log and discover the following events:**

Event Type: Error  
Event Source: Microsoft Web Proxy  
Event Category: None  
Event ID: 14176  
Date: 9/28/2002  
Time: 8:30:50 AM  
User N/A

Computer TESTKING1

Description:

Disk cache D:\urlcache\Dir1 failed to initialize. Identify the reason for cache failure by examining previous recorded events, or the error code. The error code in the Data area of the event properties indicates the cause of the failure (internal code: 504.1312.3.0.1200.50).

Data:

0000: 00000005

Event Type: Error

Event Source: Microsoft Web Proxy

Event Category: None

Event ID: 14172

Date: 9/28/2002

Time: 8:30:50 AM

User: N/A

Computer: TESTKING1

Description:

Cache failed to initialize properly. All cache drives Failed to initialize properly. Caching will be disabled. The error code in the Data area of the event properties indicates the cause of the failure. (internal code 503.329.3.0.1200.50). Identify the specific reason for failure from previous relevant event logs. Fix the problem and restart the Web Proxy service to enable caching.

Date:

0000: 000013ae

**You verify that the ISA Server services are started. You also verify that you are able to access Internet Web pages by using Testking1. However, you discover that Testking1 is not caching any of the Web pages that you access.**

**You need to resolve the problem described in the events.**

**What should you do?**

A. Configure ISA Server on Testking1 so that the system security level is set to **Disabled**.

B. Use Windows Explorer to move the Urlcache folder from drive D to another logical drive on Testking1.

C. Modify the NTFS permissions on D:\Urlcache so that the local system account has **Allow – Full**

**Control** permission.

Ensure that the new permissions propagate to all files and subfolders.

D. Configure the ISA Server services to log on by using a domain user account.

Modify the NTFS permissions on the root folder of drive D so that the Domain Users group has **Allow –**

**Read** and **Allow – Write** permissions.

E. Configure the share permissions on the D\$ shared folder so that the ISA Server service account has

**Allow – Full Control** permissions.

**Answer: C**

**Explanation:** If the everyone group does not have full control to d:\Urlcache, then the errors 14176 and 14172 are logged. When the local system account receives full control on d:\Urlcache ( all files and subfolders ), then no errors logged.

**Reference:** Q319877, Events 14176 and 14172 Are Logged If the Urlcache Folder Does Not Have Correct Permissions

### **SYMPTOMS**

The following error messages may appear in the event log:

Event Type: Error

Event Source: Microsoft Web Proxy

Event Category: None

Event ID: 14176

Date: 3/28/2002

Time: 8:30:50 PM

User: N/A

Computer: B

Description:

Disk cache D:\urlcache\Dir1 failed to initialize. Identify the reason for cache failure by examining previous recorded events, or the error code. The error code in the Data area of the event properties indicates the cause of the failure (internal code: 504.1312.3.0.1200.50).

Data:

0000: 00000005

Event Type: Error

Event Source: Microsoft Web Proxy

Event Category: None

Event ID: 14172

Date: 3/28/2002

Time: 8:30:50 PM

User: N/A

Computer: B

Description:

Cache failed to initialize properly. All cache drives failed to initialize properly. Caching will be disabled. The

error code in the Data area of the event properties indicates the cause of the failure.

(internal code

503.329.3.0.1200.50). Identify the specific reason for failure from previous relevant event logs. Fix the problem

and restart the Web Proxy service to enable caching.

Data:

0000: 000013ae

When these error messages are recorded, the Internet Security and Acceleration (ISA) Server console shows that space is used for the cache, but the cache does not work.

### **CAUSE**

This behavior may occur if the partition on which the cache is located does not have the appropriate user rights

for the Everyone user. The Everyone user must have full access rights to build the Urlcache folder during Setup,

or if you change the partition and the cache must be moved.

### **RESOLUTION**

To resolve this behavior:

1. Start Windows Explorer, and the search for the Urlcache folder.
2. If the Dir1.cdat file is missing, change the rights for the Everyone user on the Urlcache folder to Full

Control.

3. Restart all of the ISA Server services.

4. A file that is named Dir1.cdat is created. If the cache is located on only this partition, the file is the size

of the cache that is defined in the ISA Server console. If other drives are defined in the cache

configuration, there is an Urlcache folder on each drive that is defined. A Dir1.cdat file is created in each Urlcache folder.

### **QUESTION NO: 5**

**You are the administrator of an ISA Server computer named fw.testkingonline.com, which is connected to the Internet. Your internal network consists of one Microsoft Windows 2000 forest with three domains named testkingonline.com, acme.com, and medix.com. The proxy settings for Microsoft Internet Explorer are configured to use an automatic configuration script. Users report that they can successfully access Internet sites. However, you notice that your client computers are using the ISA Server computer to access Internal Web sites that they can access directly.**

**You examine the configuration script that is returned to Internet Explorer on the client computer. The**

**first part of the script is shown here:**

```
BackupRoute="PROXY";  
UseDirectForLocal=false;  
function MakeIPs() {  
}  
DirectIPs=new MakeIPs();
```

```
cDirectIPs=0;
```

```
function MakeNames() {
```

```

}
DirectNames=new MakeNames();
cDirectNames=0;
cNodes=1;
function MakeProxies() {
this[0]=new Node("fw.testkingonline.com:8080",17645,1.00);
}
Proxies = new MakeProxies();
function Node(name, hash, load) {
this.name = name;
this.hash = hash;
this.load = load;
this.score = 0;
return this;
}

```

**Client computers need to access Internal Web sites directly, without using the ISA Server computer. What should you do?**

- A. In the ISA Server console, configure the local address table to include the addresses of all three domains.
- B. In Internet Explorer on the client computers, include the three domain names in the list of exceptions that should not use the proxy server.
- C. In the ISA Server console, configure the Web browser properties to list the three domain names that client computers can access directly.
- D. Change the Internet Explorer proxy settings to bypass the proxy server for local addresses.

**Answer: B**

**Explanation:**

In Internet Explorer on the client computers, include the three domain names in the list of exceptions that should not use the proxy server. You can configure this via Poedit or Group Policies on your domain.

**Incorrect Answers :**

**A.** The requirement stated : Client computers need to access Internal Web sites directly, without using the ISA Server computer. With this solution the clients requests are directed to the ISA Server. Furthermore the Local Address Table is used for IP-adresses, Not domain names.

**C.** The requirement stated : Client computers need to access Internal Web sites directly, without using the ISA Server computer. With this solution the clients requests are directed to the ISA Server.

**D.** This action is NOT sufficient. We still have to include the three domain names in the list of exceptions that should not use the proxy server.

**Reference :**

Syngress - Microsoft Windows 2000 Isa Server 2000 Study Guide

**QUESTION NO: 6**

**You are the administrator of TestKing's network. The network consists of a single domain named testkingonline.com that contains all the Microsoft Windows 2000 Professional client computers and all the Windows 2000 Server computers on the network.**

**One of the Windows 2000 Server computers is named Testking2 and it is a DNS server. All computers on the network are configured to use Testking2 as their DNS server. The DNS server on Testking2 is configured to use the DNS server of your ISP as a forwarder.**

**You want to install ISA Server on a Windows 2000 Server computer named Testking1. Testking1 contains one network adapter that is connected to the internal network and another network adapter that is connected to the Internet. You configure each network adapter so that it has a static IP address.**

**Testking1 is configured to use Testking2 as its DNS server.**

**You plan to install the Firewall Client software on all Windows 2000 Professional client computers.**

**The configuration of the relevant portion of the network is shown in the exhibit.**

**Before you install ISA Server, you want to configure the TCP/IP settings of Testking1 so that client computers can connect to the Internet.**

**What should you do?**

- A. Configure the TCP/IP settings of the internal network adapter to use the connection's DNS suffix in DNS registration.
- B. Configure the TCP/IP settings of the internal network adapter so that parent suffixes of the primary DNS suffix are not appended.
- C. Configure the TCP/IP settings of the external network adapter to have an interface metric of 2.
- D. Configure the TCP/IP settings of the external network adapter so that the connection's addresses are not registered in DNS.
- E. Configure the TCP/IP settings of the external network adapter to use the DNS suffix of the Windows 2000 domain.

**Answer: B**

#### **QUESTION NO: 7**

**You work as a network administrator at TestKing. You recently upgraded your Microsoft Proxy Server 2.0 computer to ISA Server. Before the upgrade, users on your internal network were able to access any Web site on the Internet.**

**Now, users report that they can no longer browse on the Internet.**

**You must enable users to browse Web sites on the Internet.**

**What should you do?**

- A. Configure a site and content rule to allow the users to access external Web sites.

- B. Configure a protocol rule to allow outbound HTTP traffic.
- C. Configure the client Web browsers to send CERN-compliant requests to TCP port 1080.
- D. Configure ISA Server to listen for outbound Web requests on TCP port 80.

**Answer: D**

**Explanation :**

When you upgrade to ISA Server, most rules, network settings, monitoring configurations, and cache configurations in Proxy Server 2.0 are migrated to ISA Server. The differences and exceptions between Proxy Server 2.0 and ISA Server are listed as follows:

- \* **Publishing.** Proxy Server 2.0 requires that you configure publishing servers as Winsock Proxy clients. ISA Server allows you to publish internal servers without requiring any special configuration or software installation on the publishing server. Instead, ISA Server recognizes the publishing servers as SecureNAT clients.
- \* **Cache.** Proxy Server 2.0 cache content is not migrated because of the vastly different cache storage engine in ISA Server. ISA Server Setup deletes Proxy Server 2.0 cache content and initializes the new storage engine based on existing cache and drive settings.
- \* **SOCKS.** ISA Server policy does not support the migration of Proxy Server 2.0 SOCKS rules. ISA Server includes the SOCKS applications filter, which allows client SOCKS applications to communicate with the network by using the applicable array or enterprise policy to determine if the client request is allowed.

After you install ISA Server, you may have to upgrade your client computers:

- \* **Winsock Proxy clients.** Because both the Winsock Proxy Client that is included with Proxy Server 2.0 and the Firewall Client that is included with ISA Server are compatible with both server products, you can upgrade client computers at any time after installing ISA Server and maintain a mixed environment during migration.
- \* **Web Proxy clients.** Proxy Server 2.0 uses port 80 for client Hypertext Transfer Protocol (HTTP) requests. By default, ISA Server uses port 8080. Therefore, you must configure all downstream chain members and browsers that connect to the ISA Server computer to connect to port 8080. Alternatively, you can configure ISA Server to use port 80 for client HTTP requests.

**Reference :**

MOC2159a Deploying and managing Microsoft Internet Security and Acceleration Server 2000 - Module 2 - Page 13

**QUESTION NO 8**

**You administer TestKing 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.

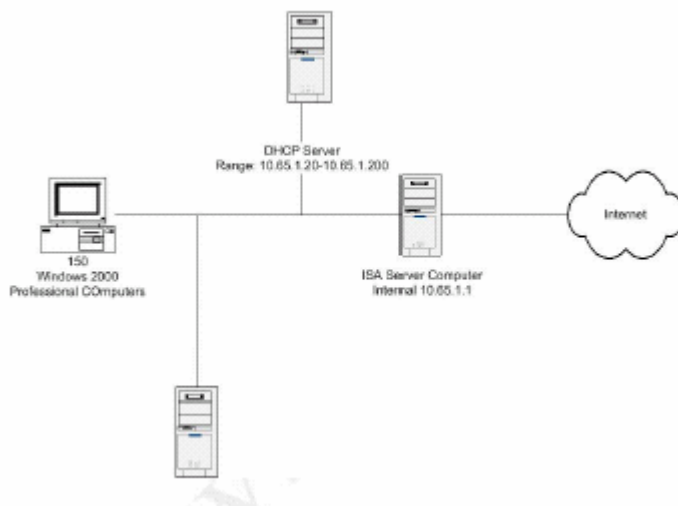
**C:** Firewall computers can not be used as Firewall clients.

**E:** Digest authentication can only be used by Windows 2000 and Windows XP clients.

**F:** Only Windows computers can use integrated authentication.

### QUESTION NO 9

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)

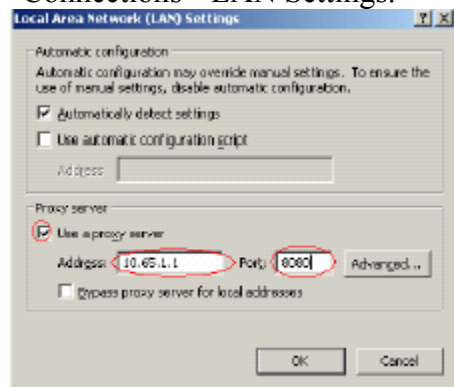
- A. Configure DHCP to assign 10.65.1.1 as the DNS address for the client computers.
- B. Configure DHCP to assign 10.65.1.7 as the DNS address for the client computers.
- C. Configure the web browsers on the client computers to use a proxy server. Specify 10.65.1.1 as the proxy address and use the ISA 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.

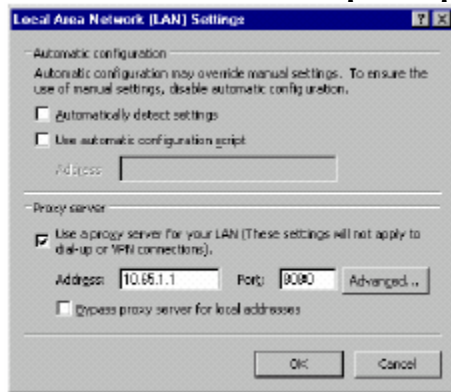
**D:** The DNS server cannot be used as proxy server.

**E:** If we want to configure the internal 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 10

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.

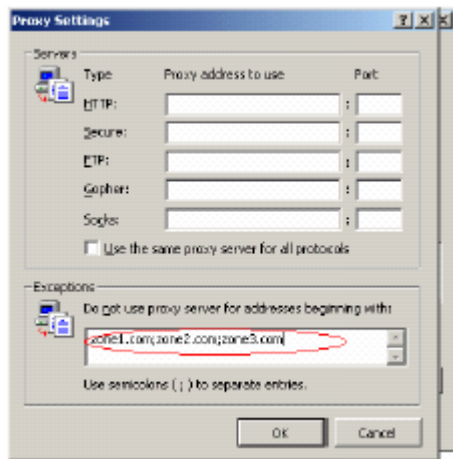


You verify that users can successfully connect to Internet sites through the ISA server computer. However, you notice that network traffic for local web servers is frequently routed to this server. You need to ensure that network traffic for the local web servers in your three domains is not routed to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

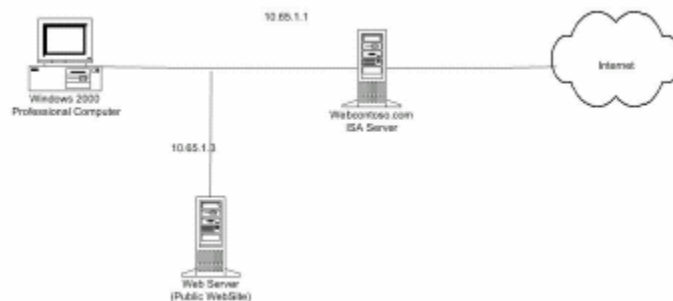
**C:** The local domain table (LDT) lists all the domain names in the internal network that are served by the ISA Server computer. However, Internet Explorer does not use the LDT. LDT is used by the firewall client, but the firewall client is not mentioned in this scenario.

**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: 11

**You administer an ISA server computer that makes TestKing'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.**

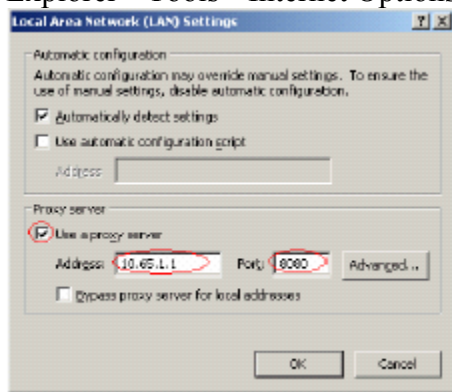


**You want to use Microsoft Internet explorer on the ISA Server computer to access Internet sites. You also want to benefit from the web proxy cache on this server. What should you do?**

- 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 12**

**You are the administrator of TestKing network, which consists of a single Microsoft Windows 2000domain 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 userlevel 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.

## **Topic 5, Monitoring, Managing, and Analyzing ISA Server Use**

### **Section 1, Monitor security and network usage by using logging and alerting (2 questions)**

### QUESTION NO: 1

You are the administrator of TestKing's ISA Server computer. The ISA Server computer is used to control Internet access. The internal network contains Microsoft Windows 98 client computers, Windows 2000 Professional client computers, and Windows XP Professional computers. Consultants from outside TestKing frequently work at TestKing's offices. They bring their own client computers and connect to the internal network. You want to find out how many different types of Web browsers are used on the internal network to access the Internet. What should you do?

- A. Inspect the information in the ISA Server packet filter log files.
- B. In ISA Management, enable automatic discovery, and then view the information in the application event log.
- C. Create a report and view the information in the Web Usage report.
- D. Use Performance Monitor to view the Web Service counters that indicate the maximum client access license (CAL) usage.

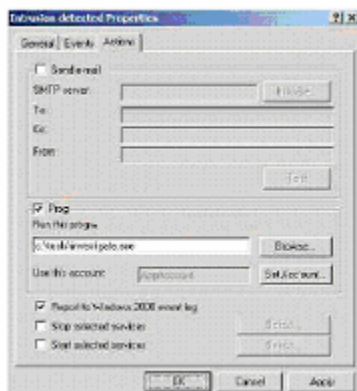
**Answer: C**

All browser types are found here.

### QUESTION NO: 2

You are the administrator of TestKing's ISA Server computers. The ISA Server computers are used to control Internet access.

You want ISA Server to run a third-party application named investigate.exe whenever an intrusion attempt is detected. The investigate.exe application is installed in the C:\Tools folder. You create a new user account named AppAccount and configure the Intrusion detected alert. You do not want to grant AppAccount more rights and permissions than are necessary to start the application. The configuration of the alert is shown in the exhibit.



ISA Server detects an intrusion attempt, but the investigate.exe application is not started. ISA Server reports the following message in the event log: "One or more of the actions associated with alert intrusion detected has failed."

**You verify that AppAccount has sufficient permissions to read the C:\Tools folder. You want to ensure that ISA Server runs investigate.exe whenever an intrusion attempt is detected. What should you do?**

- A. Grant AppAccount the **Log on as a batch job** user right.
- B. Grant AppAccount the **Manage auditing and security log** user right.
- C. In the ISA Management list of alerts, assign the **Allow – Read Alerts Information** permission to AppAccount.
- D. In the Windows Explorer event log folder, assign the **Allow – Read & Execute** permission to AppAccount.

**Answer: A**

### **Configuring alerts**

The alert service of Microsoft Internet Security and Acceleration (ISA) Server notifies you when specified events occur. You can configure alerts to trigger a series of actions when an event occurs. The ISA Server alert service acts as a dispatcher and as an event filter. It is responsible for catching events, checking whether certain conditions are met, and taking corresponding actions. You can use ISA Management to view the full list of events supplied with ISA Server and to configure which actions should be triggered when an event occurs.

### **Alert condition**

You can select which event and additional condition triggers an alert action. You can also limit the event to a particular server in the array.

You can also configure the following thresholds, which determine when the alert action should be performed:

- How many times per second the event should occur before issuing an alert (also called the *event frequency threshold*).
- How many events should occur before the alert is issued.
- How long to wait before issuing the alert again.

### **Alert action**

You can set one or more of the following actions to be performed when an alert condition is met:

- Send an e-mail message.
- Take a specific action.
- Log the event in the Windows event log.
- Stop or start any ISA Server service: Firewall service, Web Proxy service, or Scheduled Content Download service.

You can configure which credentials should be used when an application is executed. Be sure that the specified

user has **Logon as batch job** privileges. Use the Local Security Policy to configure user privileges.

When the alert action is to execute a command, the path specified for the command action must exist on all

servers in the array. It is recommended that you use environment variables (such as %SystemDrive%) within

the path name.

#### **Subsection, Configure intrusion detection (1 question)**

##### **QUESTION NO: 1**

**You are the administrator of TestKing's ISA Server computer. TestKing uses ISA Server to control Internet access.**

**A new TestKing policy states that computers on a partner company's network are allowed to connect to computers on TestKing's network.**

**On the ISA Server computer, you create a new rule named Partner Access that allows incoming network connections from all IP addresses on the partner company's network. You want to prevent users on the Internet from misusing the Partner Access rule by using a forged sender IP address and routing the return traffic back to their computer.**

**What should you do?**

- A. Enable the Enable filtering of IP fragments option.
- B. Enable the Enable filtering IP options option.
- C. Configure intrusion detection and enable the detection of all listed attacks.
- D. Configure the IP packet filters to block outgoing ICMP ping response packets.

**Answer: C**

Could be a spoofing problem, could be found with Intrusion detection system.

**Subsection, Configure an alert to send an e-mail message to an administrator (0 questions)**

**Subsection, Automate alert configuration (0 questions)**

**Subsection, Monitor alert status (0 questions)**

**Section 2: Troubleshoot problems with security and network usage**

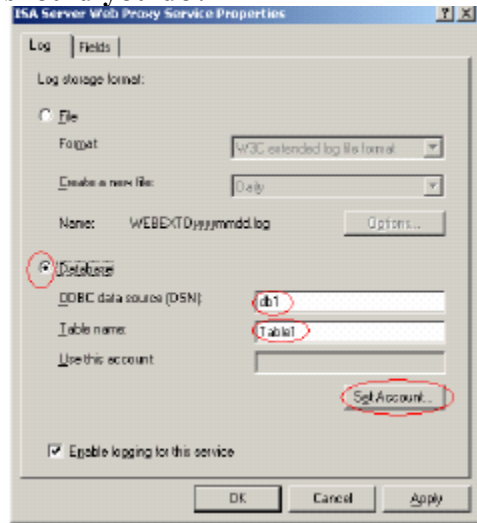
**Subsection, Detect connections by using Netstat (0 questions)**

**Subsection, Test the status of external ports by using Telnet or Network Monitor (0 questions)**

**Section 3: Analyze the performance of the ISA Server computer. Methods include the use of Performance Monitor, reports, and log files (4 questions) QUESTION NO 1**

**You are the network administrator for TestKing. 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 ODBCcompliant 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 2

You are the administrator for TestKing. 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

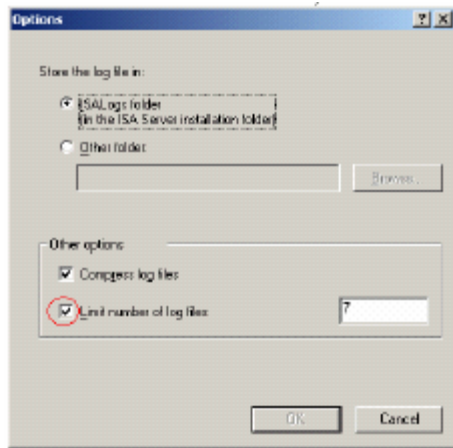
Management->Servers and Arrays->Monitoring Configuration->ISA Server Web Proxy Service (or Packet filters or ISA Server Firewall service)->Fields.

**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: 3**

**You are the administrator of Testkingonline.com's ISA Server computer. The ISA Server computer is used to control Internet access. The internal network contains 750 Microsoft Windows 2000 Professional client computers.**

**The ISA Server computer cached responses from the Internet. You have historical information on caching behavior of the ISA Server.**

**You implement active caching on the ISA Server computer. You want to find out what effect active caching has on the ISA Server computer.**

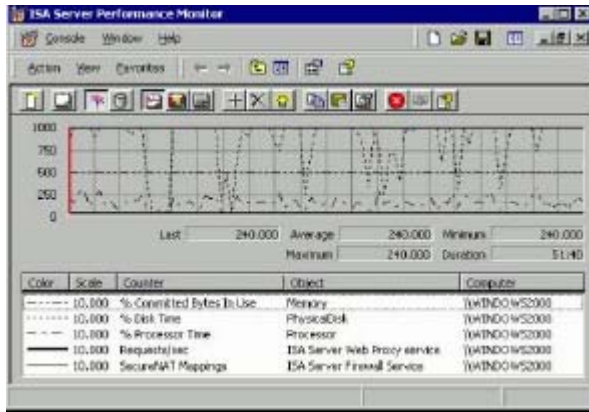
**What should you do?**

- A. View the contents of the Urlcache folder on the hard disk.
- B. Inspect information about anonymous connections in the Web Proxy service log files.
- C. Use the CacheDir utility to view the contents of the ISA Server computer cache.
- D. Use Performance Monitor to analyze the caching behavior of the ISA Server computer.

**Answer: D**

### **QUESTION NO 4**

You are the network administrator for TestKing. 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.

## Section 4, Optimize the performance of the ISA Server computer. Considerations include capacity planning, allocation priorities, and trend analysis (2 questions)

### QUESTION NO 1

You are the administrator of TestKing 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 %               |
| <b>Total</b>                                                                 | <b>509</b> | <b>100 %</b>        |

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.

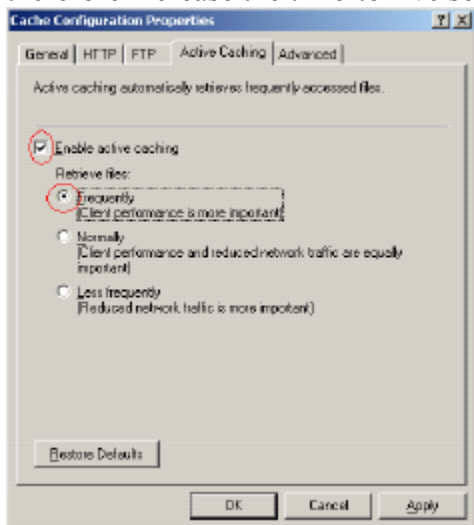
We should enable active caching and configure it to retrieve files frequently (default setting is normally). See

picture. These settings can be configured in ISA management Console->Servers and Arrays->Server->Rightclick

Cache configuration->Properties->Active Caching.

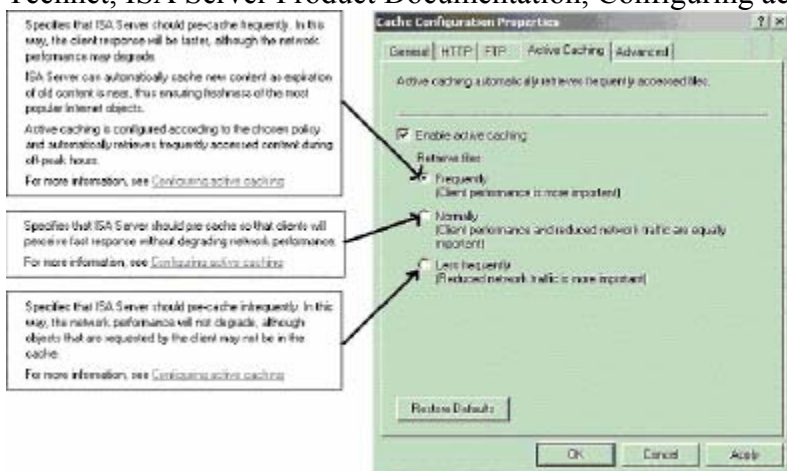
Furthermore, we should ensure that cached HTTP objects do not expire before they are refreshed. We should

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 2

**You are the administrator of TestKing 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 | 332         | 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 %               |
| <b>Total</b>                                                                 | <b>1391</b> | <b>100 %</b>        |

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

- A. Configure the active cache settings to do more pre-fetching. Increase the time-to-live (TTL) settings for cached HTTP objects.
- B. Increase the disk cache size on the ISA server computer. Decrease the time-to-live (TTL) 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 prefetching with active caching.

**D:** Caching dynamic content (object with question marks in the URL) would not improve network performance

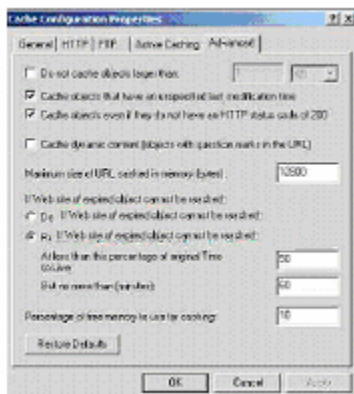
much since the dynamic content is not reused much.

**Subsection, Control the total RAM used by ISA Server for caching (2 questions)**

### QUESTION NO: 1

**You are the administrator of TestKing's ISA Server computer. The internal network contains Microsoft Windows 2000 Professional client computers.**

**The ISA Server computer is the single member of an array. The array does not use an enterprise policy. You enable active caching on the ISA Server computer. The configuration of the cache is shown in the exhibit.**



0

**Users report that response times from the ISA Server are slow. You want to improve the performance of the ISA Server computer.**

## What should you do?

- A. Remove the ISA Server computer from the array.
- B. Use the ISA Management to increase the value of the array membership load factor.
- C. Modify the ISA Server cache configuration so that it uses a larger maximum size of URL cached in memory.
- D. Modify the ISA Server cache configuration so that it uses a higher percentage of memory for caching.

**Answer: D**

RAM caching simply means that ISA Server can store the most popular objects both in its disk cache and in RAM. When a client requests an object stored in RAM, it can be

immediately returned to the client without having to be read from the disk, which makes service to clients faster. By default objects that are smaller than 12800 bytes are stored in RAM and on the ISA Server's disk cache. Objects larger than this are only stored on the disk. By default ISA Server is configured to use 50% of its free memory to store cached objects.

#### **QUESTION NO: 2**

**You are the administrator of TestKing's network. The network consists of a single Microsoft Windows 2000 domain. All client computers run Windows 2000 Professional. The network contains an ISA Server array that is running in integrated mode. The array consists of three ISA Server computers. All client computers are configured to use SecureNAT to access the Internet.**

**You set the cache size to 3 GB on each array member and schedule content downloads for the most frequently accessed Web sites**

**Users report that access to external Web sites is very slow. You verify that the physical connection to the Internet is not congested.**

**You need to increase the speed of access to external Web sites.**

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

- A. Enable IP routing in the ISA Server array policy.
- B. Enable IP packet filtering in the ISA Server array policy.
- C. Increase the size of the cache file on each ISA Server computer.
- D. Move the cache location to a separate physical hard disk on each array member.
- E. Increase the amount of available RAM used by the Web Proxy service for caching.

**Answer: D, E**

For more performance, changing to different physical harddisk and reserve more space for caching. you should also use E for more caching.

## **Topic 6, Mixed Questions (X Questions)**

#### **QUESTION NO: 1**

**You are the administrator for TestKing's network. The network consists of a single Microsoft Windows 2000 domain. All server computers run Windows 2000 Server.**

**All client computer run either Windows 2000 Professional or Windows XP**

**Professional. All client computers receive their TCP/IP configuration**

**from a Windows 2000 DHCP server. All client computers use Microsoft Internet Explorer 5.5 or later as their Web browser. All Internet access is controlled by an**

**ISA Server computer. You configure the client configuration options on the ISA Server computer to allow automatic discovery of client settings for both Web Proxy and Firewall clients. You configure scope options on the DHCP server as shown in the exhibit.**

| Option Name            | Vendor   | Value                                  | Class |
|------------------------|----------|----------------------------------------|-------|
| 003 Router             | Standard | 172.30.23.1                            | None  |
| 006 DNS Servers        | Standard | 172.30.23.2                            | None  |
| 015 DNS Domain Name    | Standard | rhovain.net                            | None  |
| 044 WINS/NBNS Servers  | Standard | rhovain.net                            | None  |
| 046 WINS/NBT Node Type | Standard |                                        | None  |
| 252 WPAD               | Standard | http://(ISAserver.domain.net)/WPAD.DAT | None  |

Later, you discover that the proxy settings in the Web browser on the client computers are not being configured by the automatic discovery feature. However, the computer's Web browsers function properly when they are configured manually. You need to ensure that the client computers use the DHCP-supplied URL for automatic discovery or configuration settings for their Web browser. What should you do?

- A. In DHCP, reconfigure option 252 to use only lowercase characters in the automatic discovery URL.
- B. In DHCP, reconfigure option 252 to use TCP port 8080 in the automatic discovery URL.
- C. In ISA Management, configure the Web browser proxy settings to use port 80 for the proxy server.
- D. In ISA Management, configure the Web browser proxy settings to use the IP address of the ISA Server computer instead of the DNS name.

**Answer: B**

## Topic 7, Practice Questions (26 Questions)

Study these questions as well.

### QUESTION NO: 1.

You manage a five-member ISA Server array. You use the Windows 2000 backup utility to back up each server daily. You suffer a complete system failure of one of the array members. You obtain a fresh computer, and perform a restore operation from yesterday's backup tape.

What must be done to restore this computer to the ISA Server array?

- A. Nothing additional must be done. Array membership is unaffected.
- B. Rebuild the cache contents.
- C. Restore the array configuration from a .bif file.
- D. Reinstall ISA Server.

**Answer: C**

**QUESTION NO: 2.**

**You are the Network Administrator for Testkingonline.com. You are managing a Windows 2000 based network. You want to set up your ISA Server as the dedicated caching server. You need to support 1900 users. Your server has the following specifications:**

**P333 CPU**

**256MB RAM**

**8GB Hard drive**

**2 NICs**

**Before proceeding with installation,**

**What should you do first (Choose all that apply)?.**

- A. Upgrade the drive
- B. Upgrade the CPU
- C. Upgrade the NICs
- D. Upgrade the RAM

**Answer: A, B**

**QUESTION NO: 3**

**A handful of users inside your network can connect to a remote VPN site directly using PPTP. You do not want to create a VPN with the remote site using ISA Server since the users already know how to use their local Routing and Remote Access Services to connect to the remote endpoint. You know that you want to allow PPTP to pass through the firewall. Once you are in the ISA Management MMC Snapin, where do you find the checkbox labeled 'PPTP through ISA firewall' that will allow you to do this?**

- A. From the Action menu of <ISA Server Name>\Access Policy\IP Packet Filters, select Properties and go to the PPTP tab.
- B. From the Action menu of <ISA Server Name>\IP Packet Filters, select Properties and go to the PPTP tab.
- C. From the Action menu of <ISA Server Name>\Network Configuration, select Allow VPN client connections.
- D. From the Action menu of <ISA Server Name>\Network Configuration, select Set Up Local ISA VPN Server.

**Answer: A**

**QUESTION NO: 4.**

**You are the ISA Server Administrator for Testkingonline.com. You are using ISA Server named TestKing5 to protect your network. Your internal clients are accessing the Internet via this ISA Server computer. You also want to configure the existing Internet Explorer 5 on the client computers.**

**Which of the following is the quickest way to do so?**

- A. Connect to `http://TestKing5/array.dll?Get.Routing.Script`
- B. Connect to `http://TestKing5/Get.Routing.Script`
- C. Deploy the software via an installer package of type MSI
- D. Deploy the software via an installer package of type MST
- E. Deploy the software via an installer package of type ZAP
- F. Run the firewall client installation program

**Answer: A**

**QUESTION NO: 5.**

**You are the network administrator of Testkingonline.com. You have a standalone ISA Server to protect your network. Inside your network there is a secure web server that requires HTTPS protocol.**

**You have configured your site and content rule as well as the default packet filters and the protocol rules accordingly.**

**What should you do so that external clients can connect to your secure web server (Choose all that apply)?**

- A. Configure SSL Bridging
- B. Configure ISA Server to listen to port 443
- C. Create new web publishing rule to redirect SSL connections as HTTP
- D. Configure ISA server to ask unauthenticated users to provide credentials
- E. Specify a server certificate
- F. Specify a client certificate.

**Answer: A, B, E**

**QUESTION NO: 6**

**You are the ISA Server Administrator for Testkingonline.com. For security purpose, you need to allow VPN access to your network for your business partner's network running Windows 2000. Which of the following tools can be used to configure the settings (Choose all that apply)?**

- A. Local ISA VPN Wizard
- B. Remote ISA VPN Wizard
- C. Clients to ISA Server VPN Wizard
- D. Enable PPTP filtering
- E. Enable L2TP protocol rule

**Answer: A, B**

**QUESTION NO: 7.**

**You are the ISA Server Administrator for Testkingonline.com. You use ISA Server array and CARP to protect your network and increase outgoing performance. Which of the following is a critical setting that must be correct so that when an object is not found in the cache the request will be forwarded to another CARP member?**

- A. Intra-array IP address
- B. Load factor
- C. Routing rules
- D. Cache address table
- E. LAT

**Answer: A**

**QUESTION NO: 8.**

**Your network contains a site and content rule allowing all users access to everything, all the time. You create a site and content rule that denies access to research.megacorp.com/area51. A user affected by this rule attempts to access HTTP content from research.megacorp.com/public and is successful. The same user attempts to access HTTP-S content from research.megacorp.com/public and is unsuccessful.**

**What must you do to enable this user to access HTTP-S content from research.megacorp.com/public?**

- A. Delete the deny rule for area51.
- B. Enable SSL bridging to redirect SSL requests as HTTP requests.
- C. Install the Firewall client on the user's computer.
- D. Create an allow rule for research.megacorp.com/public

**Answer: A**

**QUESTION NO: 9.**

**You have installed ISA Server in integrated mode. You configure the Local Address Table (LAT) to include private IP address ranges and address ranges based on the Windows 2000 routing table. You create appropriate site and content rules and protocol rules to allow Internet communications through ISA Server. During testing, you discover that some client requests for a local address are being routed to the Internet. What is the most likely cause of this problem?**

- A. The problem clients have a missing or incorrectly configured locallat.txt file.
- B. The problem clients are SecureNAT clients that do not maintain a local copy of the LAT.
- C. The Windows 2000 routing table was incorrectly set.

D. The problem clients are Firewall clients that are having their local LAT files overwritten by the ISA Server LAT file.

**Answer: C**

**QUESTION NO: 10.**

**Testkingonline.com has just entered into a business partnership with another company. In connection with this partnership, a special Web application was written that will only be accessed by users in Testkingonline.com and in the partnering company. The internal network is 10.255.2.0/24. The Web application runs on an internal Web server with an IP address of 10.255.2.30. All requests from the external company will come across the Internet from an address in the 204.137.64.0/24 network. Users on your partner's network will connect to the application by browsing to <http://partner.testkingonline.com>. You already have a Web**

**Publishing rule that forwards all external IP addresses to Testkingonline.com's marketing Web site, <http://www.testkingonline.com>, which is hosted on a computer with an IP address of 10. 255. 2. 2.**

**You decide to create an additional Web Publishing rule to meet the needs of the partnership by redirecting Web requests to 10.255.2.30.**

**Which of the following will ensure that Web requests from the partnering company will be forwarded to the dedicated internal Web server running the special Web application? (Choose 3)**

- A. Add client address set with a range from 204.137.64.1 to 204.137.64.255 and include it in the new Web Publishing rule.
- B. Create a destination set with a name of partner.yourcompany.com and include it in the new Web Publishing rule.
- C. Make sure the new rule is higher in the order list in the Web Publishing Rules folder by giving it a lower order number in the ISA Management utility.
- D. Create a destination set with an IP Address of 10.255.2.30 and include it in the new Web Publishing rule.
- E. Add client address set with a range from 10.255.2.30 to 10.255.2.30.
- F. Make sure the new rule is lower in the order list in the Web Publishing Rules folder by giving it a higher order number in the ISA Management utility.

**Answer: A, B, C**

**QUESTION NO: 11.**

**You are the ISA Server Administrator for Testkingonline.com. You use ISA Server Array to connect to the Internet on behalf of your internal web clients. You found that whenever clients request for non-HTTP content, authentication is requested. However, this does not apply to HTTP content.**

**You want to ensure that authentication takes place no matter what. What should you do?**

- A. Configure the array option to Ask unauthenticated users for identification.
- B. Use Basic authentication for the Windows 2000 clients
- C. Configure pass-through authentication
- D. Configure trusted authentication
- E. Configure PPTP connection

**Answer: A**

**QUESTION NO: 12.**

**You are creating a site and content rule to allow Testkingonline.com technical support personnel to access a group of Web sites. For security reasons, you only want this access available from each technician's assigned workstation. These workstations are desktop workstations located on subnet 192.186.100.0. All technical support technicians belong to a security group called 'Tech Support.' You have an existing Destination Set policy element called 'Research Sites' that you will use for this rule. You invoke the New Site and Content Rule Wizard. You make the following selections:**

- Rule Action - Allow**
- Rule Configuration - Custom**
- Destination Sets - Apply this rule to specified destination set (select 'Research Sites')**
- Client Type - Specific computers (client address sets)**

**At this point, you realize that you have not defined a client address set for your technical support personnel. What should you do to create the new rule with the minimum amount of administrative effort?**

- A. Exit the wizard. From the ISA Management tool, navigate to Policy Elements – Client Address Sets. If you are not in Taskpad view, select 'Taskpad' from the 'View' menu. In the Taskpad, select the 'Open User Manager' icon to create a new client set. Run the New Site and Content Rule Wizard again.
- B. Select 'Back' to return to the 'Client Type' screen. Select 'Specific users and groups,' then select 'Next.'  
From the 'Users and Groups' screen, select 'Add.' Select the 'Tech Support' security group. Finish the wizard.
- C. Select 'Next' to move to the 'Client Sets' screen. Select 'Add.' Select 'New' from the 'Add Client Sets' dialog box. Create your client set on the 'Client Set' dialog box that appears. Navigate back to the 'Client Sets' screen, and select your new client set. Finish the wizard.
- D. Exit the wizard. From the ISA Management tool, navigate to Policy Elements – Client Address Sets.  
Right-click 'Client Address Sets' and select New - Set. Create the client set. Run the New Site and Content Rule Wizard again.

**Answer: C**

**QUESTION NO: 13.**

**You are the Network Administrator for Testkingonline.com. You are managing a Windows 2000 based network. You want to install ISA Server for your network. You need to select how the enterprise policy is applied at the array level. You decide to use "Enterprise Policy only".**

**Which of the following correctly describe the results (Choose all that apply)?**

- A. Policy dictated by the enterprise administrator.
- B. Only the selected enterprise policy applies.
- C. No new rules can be added at the array level.
- D. The array policy can impose additional limitations
- E. The array policy can be more permissive than the enterprise policy.

**Answer: A, B, C**

**QUESTION NO: 14**

**You are the Network Administrator for Testkingonline.com. You are managing a Windows 2000 based network.**

**You configure an ISA Server. This ISA Server sits between your LAN and the Internet. You want to control bandwidth usage using the ISA Server. Which of the following correctly describe the nature of ISA Server's bandwidth control mechanism (Choose all that apply)?**

- A. It determines what connection gets priority over another.
- B. It limits how much bandwidth can be used.
- C. It influences the Windows 2000 QoS packet scheduling service how to prioritize network connections.
- D. It influences the Windows 2000 network browsing service how to prioritize network connections.

**Answer: A, C**

**QUESTION NO: 15.**

**You are the administrator of Testkingonline.com 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)  |               |

**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**

#### **QUESTION NO: 16.**

**You are the administrator of ISA server computer. This computer is connected to the Internet by means of a 128-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 128-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 90.
- B. Create a new bandwidth rule for HTML documents and configure it with an inbound bandwidth priority

of 20.

C. Schedule content downloads from frequently visited web sites to occur during non-working hours.

D. Schedule content downloads from frequently visited web sites to occur during working hours.

**Answer: C**

**QUESTION NO: 17.**

**You are the network administrator for Testkingonline.com. 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 email 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 and everyone to only receive e-mails.**

**What should you do?**

A. Create a SMTP protocol rule to allow external access. Configure rule to include the sales group. Create a POP3 protocol rule to allow external access. Configure this rule to include the everyone group.

B. Create a SMTP server protocol rule and POP3 protocol rule to allow external access. Configure each rule to include the everyone 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**

**QUESTION NO: 18.**

**You want to deploy the Firewall client to every client computer in your organization.**

**What is the proper method to achieve this?**

A. Copy the mspclnt.ini file to each computer. Run 'setup.exe.'

B. E-mail the mspclnt.ini file to each user. Instruct them to run 'setup.exe.'

C. Use the Windows 2000 Software Installation snap-in to deploy the Firewall client's .msi file to each computer.

D. Use the Windows 2000 Software Installation snap-in to deploy the Firewall client's .msi file to each user.

**Answer: C**

**QUESTION NO: 19.**

**You are the network administrator of Testkingonline.com. You suspect that POP is the source of problematic traffics that goes into your network. In response, you deploy the POP intrusion detection filter with ISA Server. Which of the following can be achieved (Choose all that apply)?**

- A. POP traffic destined for the internal network are intercepted and analyzed
- B. POP traffic destined for the external network are intercepted and analyzed
- C. POP buffer overflow attacks can be detected.
- D. Mail box access are disabled.
- E. Clients must use SMTP as an alternative to POP.

**Answer: A, C**

**QUESTION NO: 20.**

**You are the ISA Server Administrator for Testkingonline.com. You use ISA Server to provide caching and Internet access for your internal clients. In Testkingonline.com there is a group of roaming Web Proxy client users. You want to ensure that they will always connect to the appropriate ISA Server computer when they log on. These clients are currently running Internet Explorer 4. What should you do (Choose all that apply)?**

- A. Apply the Internet Explorer 4 SP1 to the client computers.
- B. Apply the Internet Explorer 4 SP2 to the client computers.
- C. Install Internet Explorer 5 to the client computers.
- D. Enable automatic discovery.
- E. Stop and restart the ISA Server services

**Answer: C, D**

**QUESTION NO: 21.**

**You are the ISA Server Administrator for Testkingonline.com. You use ISA Server to publish your internal servers. A network maintenance job has disrupted the network connections between the ISA Server and the rest of the internal network. When the connection is up again, your external clients complain that they cannot send mail via the computer running Exchange Server 5.5 that is set up as a Firewall client behind the ISA Server computer. How do you fix the problem?**

- A. Install Exchange Server onto the ISA Server computer.
- B. Configure Exchange Server as a firewall client.
- C. Configure Exchange Server as a SecureNAT client.
- D. Configure Exchange Server as a Winsock client..
- E. Stop the alert service that uses port 25.
- F. Restart the Exchange Server Services.

**Answer: F**

**QUESTION NO: 22.**

**You are the ISA Server Administrator for Testkingonline.com. You use ISA Server to provide web access for clients. You have a mix of Win2000 clients and UNIX clients in your network. The Unix Server is responsible for authenticating all the clients that belongs to the network. You want to use the most secure user authentication wherever possible. How do you configure the Windows 2000 clients and the UNIX clients (Choose all that apply)?**

- A. Use Digest authentication for the Windows 2000 clients.
- B. Use Windows Integrated authentication for the Windows 2000 clients.
- C. Use Basic authentication for the Windows 2000 clients.
- D. Use Digest authentication for the Unix clients.
- E. Use Windows Integrated authentication for the Unix clients.
- F. Use Basic authentication for the Unix clients.

**Answer: C, F**

**QUESTION NO: 23.**

**You are responsible for supporting the network of a research facility. ISA server is acting as both a firewall and a caching server. It supports 720 client systems and 27 servers, and has 640MB of RAM, as well as a SQL Server database for custom log processing. You've been using System Monitor to keep tabs on resource usage, and you notice that the Memory Usage Ratio percentage is consistently up around 85% during working hours. The Memory Cache Allocated Space counter indicated that there is an average of 275MB RAM allocated for caching. The server is currently using the installation defaults for its cache size, and you would like to allocate more memory for caching. What should you set the cache percentage to be if you would like to increase the amount of allocated cache memory to 410MB?**

- A. 75%
- B. 35%
- C. 90%
- D. 50%

**Answer: A**

**QUESTION NO: 24.**

**You are the network administrator for Testkingonline.com. You will be off-site at a conference, but you still need to monitor your ISA Server array for network attacks and alert conditions. You have a Windows Millennium Edition (ME)-equipped laptop with a built-in Ethernet adapter and a 56 Kbps modem. How can you accomplish your goal with minimum administrative overhead?**

- A. Install the ISA Management tool on your laptop. Periodically check the alert status of your ISA Server array under Arrays - <array name> - Monitoring - Alerts.
- B. Configure selected alert conditions to send you e-mail.
- C. Configure selected alert conditions to post an HTML response to your Web server.
- D. Install the ISA Management tool on your laptop. Periodically check the alert status of your ISA Server array under Arrays - <array name> - Monitoring Configuration - Alerts.

**Answer: B**

**QUESTION NO: 25.**

**You are the ISA Server Administrator for Testkingonline.com. You are using ISA Server to protect your network. Your ISA Server system is running on NTFS partitions. Your disk drive is nearly running of space. You do not want to give up logging for freeing disk space.**

**What should you do to free up disk space without the need to purchase additional drive or deleting existing data?**

- A. Use W3C format for logging into a text over a remote network share
- B. Use ISA format for logging into a text file
- C. Configure to log via ODBC to a remote drive
- D. Compress the log files via ISA Management
- E. Compress the log files via NTFS compression

**Answer: D**

**QUESTION NO: 26.**

**You are the ISA Server Administrator for Testkingonline.com. You use ISA Server to protect your network. Recently you receive an event error 14111 saying that "ISA Server Cache could not start because it was configured incorrectly."**

**Which of the following actions can you take to fix the problem?**

- A Stop the Web Proxy service. Restore the default cache settings and restart the service.
- B Stop the Web Proxy service and restart the service.
- C Stop the Web Proxy service. Restore the default cache settings. Turn off the computer, and restart the service.
- D Modify the registry in Windows 2000, stop and restart the computer.

**Answer: A**