

Exam 70-350 study material

Made available by Examsexpert.com



Free 70-350 Exam Preparation Questions

Exam 70-350: Implementing Microsoft Internet Security and Acceleration (ISA) Server
2004

Question: 1

Your network contains a server that runs ISA Server 2004. Your company uses an extranet Web site. You create a Web Publishing rule to provide user access to the extranet. The Web Publishing rule uses SSL bridging. You define a cache drive on the ISA Server. You need to prevent encrypted information from being cached on the ISA Server. What should you do?

- A. Ensure that Encrypted File System (EFS) is disabled on the ISA Server.
- B. For the Web Publishing rule, enable the Block high bit characters option of the HTTP policy.
- C. For the advanced cache settings, disable the Cache objects even if they do not have an HTTP status code of 200 option.
- D. Create a URL set that includes the URL of the extranet. Create a cache rule for the new URL set. In the cache rule, disable the Cache SSL Responses option.

Answer: D

Question: 2

Your network contains a server that runs ISA Server. The ISA Server is configured as a firewall and as a VPN gateway. Your company, Contoso, Ltd., acquires Adventure Works. Adventure Works uses a third-party firewall and VPN solution. You need to recommend a solution that provides TCP/IP connectivity between the two networks. Users from both networks must be able to access resources on both networks. What should you recommend?

- A. SSL-to-SSL bridging
- B. Publishing rule for PPTP
- C. Site-to-site VPN that uses IPsec tunnel mode
- D. Site-to-site VPN that uses L2TP/IPsec and Kerberos

Answer: C

Question: 3

Your network contains a VPN server that runs ISA Server 2004. You plan to implement two-factor authentication for VPN access. You need to identify the authentication protocol that will support your planned Implementation. Which authentication method should you choose?

- A. Unencrypted password (PAP)
- B. Encrypted authentication (MS-CHAP)
- C. Microsoft encrypted authentication version 2 (MS-CHAPv2)
- D. Extensible authentication protocol (EAP) with smart card or other certificate

Answer: D

Question: 4

Your company has a main office and a branch office. Each office has an IT staff. Each office contains an ISA Server Enterprise Edition array that provides firewall and proxy services. You create two security groups named MainIT and BranchIT. You add the user accounts for the IT staff from the main office to the MainIT group. You add the user accounts for the IT staff from the branch office to the BranchIT group. You need to configure the security of your ISA Server environment to meet the following requirements:

Give the IT staff in the main office full administrative access to both ISA Server arrays. Allow IT staff in the branch office to view firewall rules for the branch office ISA Server array. Prevent IT staff in the branch office from changing the configuration of the branch office ISA Server array. Prevent IT staff in the branch office from accessing the configuration of the main office ISA Server array. What should you do?

- A. Assign the BranchIT group to the ISA Server Enterprise Auditor role. Assign the MainIT group to the ISA Server Enterprise Administrators role.

- B. Assign the BranchIT group to the ISA Server Array Auditor role on the branch office array.
Assign the MainIT group to the ISA Server Enterprise Administrators role.
- C. Assign the BranchIT group to the ISA Server Array Monitoring Auditor role on the branch office array.
Assign the MainIT group to the ISA Server Enterprise Administrators role.
- D. Assign the BranchIT group to the ISA Server Array Auditor role on the branch office array.
Assign the MainIT group to the ISA Server Enterprise Auditor role.

Answer: B

Question: 5

You have an ISA Server array that contains two servers. The array provides Winsock Proxy access to the Internet. All client computers have Firewall Client for ISA Server installed. One of the servers fails and some users report that they are unable to access an Internet-based application that uses a custom port. You need to ensure that all users can access the Internet-based application in the event that a single server fails. What should you do?

- A. Publish the Internet-based application as a Web Server Farm.
- B. Enable the Cache Array Routing Protocol (CARP) on the internal network.
- C. Enable Network Load Balancing on the internal network. Update the Firewall Client settings on all users computers.
- D. Enable Network Load Balancing on the external network. Update the Firewall Client settings on all users computers.

Answer: C

Question: 6

Your company has a main office and a branch office. The network consists of a single ISA enterprise. The ISA enterprise contains two ISA Server 2004 Enterprise Edition arrays named Array 1 and Array2. You need to enable a support technician to monitor log information for Array 1. You want to achieve this goal while providing the minimum permissions possible. What ISA role should you assign to the support technician?

- A. ISA Server Enterprise Auditor
- B. ISA Server Enterprise Monitoring Auditor
- C. ISA Server Array Monitoring Auditor for Array1
- D. ISA Server Array Auditor for Array1

Answer: D

Question: 7

Your network contains a single server that runs ISA Server 2004. You need to create a report that lists the client operating systems that are most frequently used to connect to the ISA Server. Which type of content should you include in the report?

- A. Security
- B. Summary
- C. Traffic and Utilization
- D. Web Usage

Answer: D

Question: 8

You are the network administrator for your company. The network contains two ISA Server 2004 computers named ISA1 and ISA2. The company has a main office and one branch office. ISA1 is located in the main office and connects to the Internet. ISA2 is located in the branch office and connects to the main office over a dedicated WAN link. All client computers run Windows XP Professional. All client computers can update virus definitions from the virus update Web site. ISA2 can connect to the virus

update Web site and the Windows Update Web site. You discover that ISA cannot connect to the virus update Web site or the Windows Update Web site. The firewall policy on ISA is configured as shown in the exhibit. (Click the Exhibit button.) You need to ensure that ISA can connect to the virus update Web site and the Windows Update Web

U...	Name	Action	Protocols
16	Allow remote SQL logging from ISA Server to selected servers	Allow	Microsoft S...
17	Allow HTTP/HTTPS requests from ISA Server to specified sites	Allow	HTTP,HTTPS
18	Allow HTTP/HTTPS requests from ISA Server to selected servers for connectivity verifiers	Allow	HTTP,HTTPS
19	Allow access from trusted computers to the Firewall Client installation share on ISA Server	Allow	Microsoft ...
20	Allow remote performance monitoring of ISA Server from trusted servers	Allow	NetBios Da...
21	Allow NetBIOS from ISA Server to trusted servers	Allow	NetBios Da...
22	Allow RPC from ISA Server to trusted servers	Allow	RPC (all int...

- On ISA, ensure that the Schedule Download Jobs configuration group is enabled and create a computer set that has the IP addresses of both the virus update Web site and the Windows Update Web site.
- On ISA, ensure that the Allowed sites configuration group is enabled and add the URL of the virus update Web site to the System Policy Allowed Sites domain name set.
- Create a new URL set named VirusUpdates that includes the URLs for the virus update Web site and the Windows Update Web site. On ISA2, create a new HTTP access rule that includes the VirusUpdates URL set.
- Create a new domain name set named VirusUpdates that includes the URLs for the virus update Web site and the Windows Update Web site. On ISA1, create a new HTTP access rule from the Internal network to the VirusUpdates domain name set.

Answer: B

Question: 9

You have a server that runs ISA Server 2004. The ISA Server provides forward Web Proxy services for all users. The ISA Server uses an SQL database server for the Firewall logs and the Web Proxy logs. The SQL database fails. Users report that they are unable to access the Internet. You need to configure the ISA Server to ensure that Internet access is available in the event that the SQL database fails. What should you do?

- Disable the Stop selected services option of the Log Failure alert definition.
- Disable the Audit: Shut down system immediately if unable to log security audits option in the local security policy.
- Increase the size of the Security event log and enable the Overwrite events as needed option.
- Modify the Restart service after value in the Recovery tab of the Microsoft Firewall service.

Answer: A

Question: 10

Your network consists of an Active Directory domain. All computers in the network are members of the Active Directory domain. The network contains a server that runs ISA Server. The server is configured as a firewall and as a Web proxy. The existing Internet access rule defines useraccess to HTTP, HTTPS, FTP, and RDP. You change the user set of the Internet access rule from All Users to All Authenticated Users. Users report the following:

They can access the Internet by using a Web browser. They cannot connect to remote computers by using the Remote Desktop client. You need to ensure that users can establish RDP connections to

servers on the Internet. What should you do?

- A. Configure the Auto Configuration URL in Group Policy.
- B. On all client computers, install the Firewall Client for ISA Server software.
- C. On all client computers, configure the ISA Server as the default gateway.
- D. Replace the existing rule with two new Internet access rules. The first rule contains HTTP, HTTPS, and FTP for All Authenticated Users. The second rule contains RDP for All Users.

Answer: B

Question: 11

Your company has one office that connects to the Internet by using a high-speed link. There are 6,000 users on the network. All users require access to the Internet. You plan to deploy an array that contains two new ISA Server Enterprise Edition servers. You will configure the array as a Web cache and as a Winsock proxy. You need to recommend a hardware configuration for the new array. Your recommendations must allow the array to be configured to meet the following requirements: Provide fault tolerance for all types of ISA Server clients. Provide fault tolerance if the Microsoft Firewall service fails on either server. Maximize performance for Internet access. Which hardware configuration should you use in each server?

- A. One network adapter for the internal network one disk drive for the cache database one disk drive for the logs
- B. One network adapter for the internal network one network adapter for the external network one disk drive for the cache database and the logs
- C. One network adapter for the internal network one network adapter for the external network one disk drive for the cache database one disk drive for the logs
- D. Two network adapters for the internal network two network adapters for the external network on each network adapter, enable network teaming one disk drive for the cache database one disk drive for the logs

Answer: C

Question: 12

Your network contains an ISA Server 2004 array. The array provides Internet access and Web caching. A Web hosting company hosts your corporate Web site at www.tailspintoys.com. The webmaster reports that when he updates content on the Web site the changes do not appear to take effect. The Web page authoring tool indicates that the pages were updated successfully. You need to configure ISA Server to ensure that you can view recent changes to the content on the Web site. What should you do?

- A. Create a URL set named External Web Site and add <http://www.tailspintoys.com>. Create and enable a new cache rule that has HTTP caching set to Disabled. Include the new URL set as the destination.
- B. Create a URL set named External Web Site and add <http://www.tailspintoys.com>. Create and enable a new cache rule that has HTTP caching set to Enabled. Include the new URL set as the destination. On the HTTP tab, set the Set TTL of objects (% of the content age) option to 100%.
- C. Create a URL set named External Web Site and add <http://www.tailspintoys.com>. Create and disable a new cache rule that has HTTP caching set to Enabled. Include the new URL set as the destination.
- D. Create a domain name set named External Web Site and add www.tailspintoys.com. Create and disable a new cache rule that has HTTP caching set to Disabled. Include the new domain name set as the destination. In the Store in Cache area, select the Never, no content will ever be cached option.

Answer: A

Question: 13

Your network contains a server that runs ISA Server 2004. The ISA Server provides forward Web caching for internal users. A Web hosting company hosts your company's Web site at www.cpandl.com. The Web browser on internal client computers uses www.cpandl.com as the default home page. You need to ensure that internal users can access www.cpandl.com. You want to achieve this goal while minimizing the usage of Internet bandwidth. What should you do?

- A. Increase the size of the cache drive.
- B. Create a new URL set that includes www.cpandl.com. Create a cache rule for the new URL set. In the cache rule, decrease the TTL of objects value.
- C. Create a content download job to download content from www.cpandl.com. Configure the content download job to run daily.
- D. Create a new URL set that includes www.cpandl.com. Create a cache rule for the new URL set. In the cache rule, disable the Cache SSL Responses option.

Answer: C

Question: 14

Your company has a main office and one branch office. The network contains two ISA Server 2004 computers named ISA1 and ISA2. ISA1 is located at the main office. ISA2 is located at the branch office. An IPsec tunnel mode site-to-site VPN connects the main office and branch office networks. ISA1 has three addresses bound to its external network adapter, and ISA2 uses a non-primary IP address to establish the IPsec tunnel mode connection to ISA1. Users at the branch office report that they can connect to file shares at the main office, but they cannot connect to the Microsoft Outlook Web Access Web site. You need to ensure that users at the branch office can access the Outlook Web Access Web site. What should you do?

- A. Use a network address translation (NAT) relationship between the branch office network and the main office network.
- B. Add IP addresses to the external network adapter of ISA2.
- C. Create a new protocol definition for TCP port 80 outbound and use the definition in the access rule named Allow Direct HTTP. Create a Deny access rule using the same new protocol and place it immediately before the Allow Direct HTTP rule.
- D. Create a new protocol definition for TCP port 80 outbound and use the definition in the access rule named Allow Direct HTTP. Create a Deny access rule using the same new protocol and place it immediately following the Allow Direct HTTP rule.

Answer: D

Question: 15

Your company has employees who require remote access to the network. Your network has an ISA Server Enterprise Edition array that contains two servers. The array provides firewall services and Web proxy services. You need to configure the array to provide VPN gateway services for remote client connections. What are two possible ways to configure the array using the ISA Server management console? (Each correct answer provides a complete solution. Choose two.)

- A. Enable VPN Client Access. Enable the PPTP protocol. Assign IP addresses by using DHCP.
- B. Enable VPN Client Access. Enable the PPTP protocol. Assign IP addresses by using a static address pool.
- C. Enable VPN Client Access. Enable the L2TP/IPsec protocol. Assign IP addresses by using DHCP.
- D. Enable VPN Client Access. Enable the L2TP/IPsec protocol. Assign IP addresses by using a static address pool.

Answer: B, D

Question: 16

Your network contains a server that runs ISA Server 2004. Your company uses Microsoft Exchange Server 2007 for e-mail. Users access their e-mail by using Microsoft Office Outlook 2007. You need to allow users to access their e-mail remotely. Your solution must minimize the number of ports that are opened. What should you do?

- A. From the Exchange Publishing Rule Wizard, select the ActiveSync service.
- B. From the Mail Server Publishing Rule Wizard, select the Outlook (RPC) service.
- C. From the Exchange Publishing Rule Wizard, select the Outlook Web Access service.
- D. From the Exchange Publishing Rule Wizard, select the Outlook Anywhere (RPC/HTTP(s)) service.

Answer: D

Question: 17

You install Windows Server 2003 Service Pack 1 on a server named ISA1. You deploy ISA Server 2004 as a firewall on ISA1. A new company security policy states that servers that connect directly to the Internet must only run required services. You need to ensure that your deployment of ISA1 meets the new company security policy. What should you do on ISA1?

- A. Start the Windows Firewall service.
- B. Install Windows Server 2003 Service Pack 2.
- C. Disable the IP Routing feature of ISA Server 2004.
- D. Run the Security Configuration Wizard (SCW), and then select the Microsoft Internet Security and Acceleration Server 2004 server role.

Answer: D

For complete [Exam 70-350 Training kits and Self-Paced Study Material](http://www.Examexpert.com/70-350.html)

Visit:

<http://www.Examexpert.com/70-350.html>



For Latest 70-350 Exam Questions and study guides- visit- <http://www.Examexpert.com/70-350.html>