

Exam : Microsoft 70-350

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

Version : Demo

1. You are a network administrator for Litware, Inc. The network contains an ISA Server 2004 computer named ISA1. ISA1 is configured to allow outbound Internet access. A listener named DefaultHTTP is also configured to listen for requests on port 80 on the external interface.

The Internal network contains two Web sites named HR and Sales, which are used by employees. The HR Web site is stored on a Web server named Web1.litwareinc.com. The Sales Web site is stored on a Web server named Sales1.litwareinc.com. Employees access the Litware, Inc., Web site by using the URL <http://www.litwareinc.com>.

You must allow employees to access both the HR Web site and the Sales Web site from the Internet. You must ensure that employees can access the HR Web site by using the URL <http://www.litwareinc.com/hr>. You must also ensure that employees can access the Sales Web site by using the URL <http://www.litwareinc.com/sales>.

What should you do?

A. Configure one of the Web servers to listen for HTTP requests on port 8080.

Create two server publishing rules. Create one of the rules to respond to requests on port 8080, and configure this rule to forward requests to one internal Web server. Create the other rule to use the DefaultHTTP listener, and configure this rule to forward to the other internal Web server.

B. Create one Web publishing rule by using the path /Sales/* and redirect to Web1.litwareinc.com. Create one Web publishing rule by using the path /HR/* and redirect to Sales1.litwareinc.com. Configure each rule to use the DefaultHTTP listener.

C. Create two server publishing rules. Configure each rule to forward to a different internal Web server. Configure each internal Web server to listen for HTTP requests on an unused port.

D. Create one Web publishing rule by using the path /HR/* and redirect to Web1.litwareinc.com. Create one Web publishing rule by using the path /Sales/* and redirect to Sales1.litwareinc.com. Configure each rule to use the DefaultHTTP listener.

Answer: D

2. Your network contains a single ISA Server 2004 computer named ISA1. ISA1 is not yet configured to allow inbound VPN access.

You deploy a new application named App1. The server component of App1 is installed on an internal server named Server1. The client component of App1 is installed on employee and partner computers. Employees

and partners will establish VPN connections when they use App1 from outside the corporate network.

You identify the following requirements regarding VPN connections to the corporate network.

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

You need to plan the VPN configuration for the company.

What should you do?

A. Configure ISA1 to accept incoming VPN connections from partners and employees.

Enable Quarantine Control on ISA1.

Configure Quarantine Control to disconnect users after a short period of time.

use access rules to allow access to only the permitted resources.

B. Configure ISA1 to accept incoming VPN connections from partners and employees.

Enable Quarantine Control on ISA1.

Exempt partners from Quarantine Control.

use access rules to allow access to only the permitted resources.

C. Configure ISA1 to accept incoming VPN connections from partners and employees.

Enable Quarantine Control on ISA1.

Enable RADIUS authentication and user namespace mapping.

Configure a Windows Server 2003 Routing and Remote Access server as a RADIUS server.

Create a single remote access policy.

D. Add a second ISA Server 2004 computer named ISA2.

Configure ISA1 to accept VPN connections from employees. Do not enable Quarantine Control on ISA1.

Configure ISA2 to accept VPN connections from partners. Enable Quarantine Control on ISA2.

On each server, use access rules to allow access to only the permitted resources.

Answer: B

3. In your organization client computers on the internal network are divided among several subnets by

using routers.

You install an ISA Server 2004 computer named ISA1. ISA1 policies have been configured to allow users to access Web sites on the Internet. You configure TCP/IP on ISA1 as shown in the exhibit. (Click the Exhibit button.)

```
C:\Documents and Settings\Administrator.CONTOSO>ipconfig

Windows IP Configuration

Ethernet adapter External:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.212
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

Ethernet adapter Internal:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 172.16.0.102
    Subnet Mask . . . . .             : 255.255.0.0
    Default Gateway . . . . .         : 172.16.0.254

C:\Documents and Settings\Administrator.CONTOSO>
```

Users report that they cannot access Web sites on the Internet.

You need to ensure that users can access Web sites on the Internet.

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

- A. Configure the internal default gateway to match the external default gateway.
- B. Configure a static route to each subnet.
- C. Add the IP address of the internal default gateway to the Remote Management Computers computer set.
- D. Configure the internal network adapter with a blank default gateway.
- E. Create a network set for each subnet.

Answer: DB

4. Your company has a main office, two branch offices, and one research office. An ISA Server array is configured for the main, and the two branch offices. All arrays are members of the same ISA Server 2004 enterprise.

A Configuration Storage server is located in the main office. Replica Configuration Storage servers are located in each branch office. Administrators at the main office administer the enterprise settings and the main office array. The administrators at each branch office administer the arrays at their respective branch

offices.

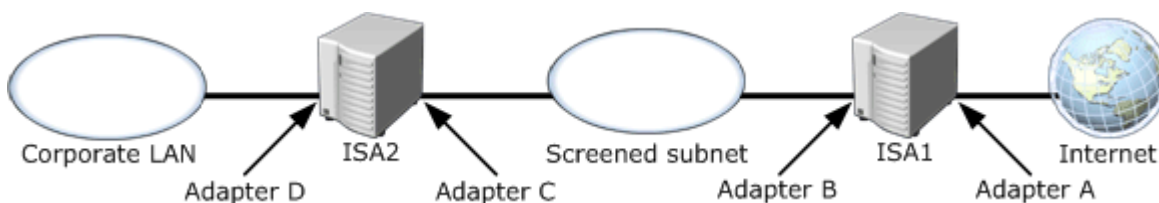
You need to install a new ISA Server array in the research office. You need to ensure that only research office administrators can manage access rules for the array.

What should you do?

- A. Configure a replica Configuration Storage server. Assign the research office administrators the ISA Server Array Administrator role.
- B. Configure a new array in the existing enterprise. Assign the research office administrators the ISA Server Array Administrator role.
- C. Configure a new array in the existing enterprise. Assign the research office administrators the ISA Server Enterprise Administrator role.
- D. Configure a new Configuration Storage server in the research office. Configure it as a new enterprise. Assign the research office administrators the ISA Server Enterprise Administrator role.

Answer: D

5. You are a network administrator for your company. You are installing ISA Server 2004 on two computers named ISA1 and ISA2. The network is configured as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that the implementation plan meets the following requirements:

- All devices that pass outbound traffic must perform network address translation (NAT).
- All Internet-accessible internal resources must be published.
- All traffic between two network interfaces on an ISA Server computer must be subject to inspection.

Which interface or interfaces should be configured as an internal interface? (Choose all that apply.)

- A. Adapter A
- B. Adapter B
- C. Adapter C
- D. Adapter D

Answer: (B AND D) AND ONLY (B, D)

6. You are the administrator of an ISA Server 2000 computer named ISA1. You use the ISA Server 2004 Migration Tool to perform an in-place upgrade on ISA1. You install the Firewall Client installation component on ISA1.

Client computers in the sales department run Windows NT Workstation 4.0 with Internet Explorer 5.0 and the Microsoft Proxy 2.0 Winsock Proxy client installed. All other client computers run Windows XP Professional. The ISA Server 2000 Firewall Client was installed on the Windows XP Professional computers by using Group Policy.

You discover that all client computer requests to ISA1 are being sent unencrypted.

You need to configure all client computers to communicate to ISA1 by using encryption.

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

A. Uninstall the Winsock Proxy client from the client computers in the sales department.

Run Setup.exe to install the ISA Server 2004 Firewall Client.

B. Uninstall the Winsock Proxy client from the client computers in the sales department.

Enable the Allow non-encrypted Firewall client connections setting on the Internal network.

C. Uninstall the Winsock Proxy client from the client computers in the sales department.

Enable the Require all users to authenticate setting. Configure SSL certificate authentication for all Firewall clients on the Internal network.

D. Upgrade the Firewall Client for ISA Server 2000 software on the Windows XP Professional client computers.

Configure the Windows XP Professional computers as Web Proxy clients.

E. Upgrade the Windows XP Professional client computers by assigning the ISA Server 2004 Firewall Client.

Configure the software installation package to remove older versions of the software.

Answer: AE

7. Your network consists of a single Active Directory domain. The network contains an ISA Server 2004 computer named ISA1. Client computers on the network consist of Windows XP Professional computers, UNIX workstations, and Macintosh portable computers. All client computers are domain members.

You configure ISA1 by using the Edge Firewall network template. You manually configure ISA1 with access rules to allow HTTP and HTTPS access to the Internet. You configure ISA1 to require all users to

authenticate.

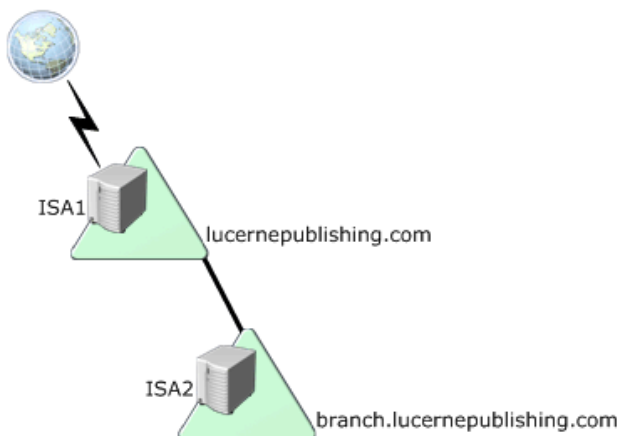
You need to provide Internet access for all client computers on the network while preventing unauthorized non-company users from accessing the Internet through ISA1. You also want to reduce the amount of administrative effort needed when you configure the client computers.

What should you do?

- A. Configure all client computers as Web Proxy clients. Configure Basic authentication on the Internal network.
- B. Configure all client computers as Web Proxy clients. Configure Basic authentication on the Local Host network.
- C. Configure all client computers as SecureNAT clients. Configure Basic authentication on the Internal network.
- D. Configure the Windows-based computers as Firewall clients. Configure the non-Windows-based computers as Web Proxy clients. Configure Basic authentication on the Local Host network.

Answer: A

8. You are the network administrator for Lucerne Publishing. The company has a main office and one branch office. The network contains two ISA Server 2004 computers named ISA1 and ISA2. The relevant portion of the network is configured as shown in the exhibit. (Click the Exhibit button.)



ISA1 is located at the main office. ISA2 is located at the branch office and connects to the main office by using a dedicated WAN connection. You configure ISA2 to forward Web requests to ISA1. All client computers are configured to use an internal DNS server in each office. All client computers are configured as SecureNAT clients.

While monitoring ISA2, you discover that Web requests from client computers in the branch office for

servers located in the branch office are being resolved by ISA2.

You need to configure the client computers in the branch office to directly access servers in the branch office.

What should you do?

- A. Configure the client computers as Web Proxy clients of ISA2. Configure the list of domain names available on the Internal network on ISA1 to include the *.lucernepublishing.com domain.
- B. Configure the client computers as Web Proxy clients of ISA2. Configure the Web browser to include the *.branch.lucernepublishing.com domain.
- C. Configure the client computers as Firewall clients. Configure the list of domain names available on the Internal network on ISA2 to include the *.branch.lucerncepublishing.com domain.
- D. Configure the client computers as Firewall clients. Configure the list of domain names available on the Internal network on ISA1 to include the *.branch.lucerncepublishing.com domain.

Answer: B

9. Your network consists of a single Active Directory domain named contoso.com. The network contains an ISA Server 2000 computer named ISA1.

All client computers have the ISA Server 2000 Firewall Client software installed. Client computers are configured to use an internal DNS server. Two Windows Server 2003 computers named App1 and App2 run a Web-based application that is used to process company data.

You configure ISA1 with protocol rules to allow HTTP, HTTPS, RDP, POP3, and SMTP access.

The list of domain names available on the Internal network on ISA1 contains the following entries:

- *.south.contoso.com
- *.north.contoso.com
- *.east.contoso.com
- *.west.contoso.com

You perform an in-place upgrade of ISA1 by using the ISA Server 2004 Migration Tool. When you use Network Monitor on ISA1, you discover that client requests for App1 and App2 are being passed through ISA1.

You need to provide a solution that will allow clients to directly access company data on App1 and App2.

What should you do?

-
- A. Create and configure HTTP, HTTPS, RDP, POP3, and SMTP access rules on ISA1.
 - B. Configure an Application.ini file on the client computers.
 - C. Redeploy the ISA Server 2004 Firewall Client software by distributing it to the client computers by using Group Policy.
 - D. Add app1.contoso.com and app2.contoso.com to the list of domain names available on the Internal network on ISA1.

Answer: D

10. Your network contains a single ISA Server 2004 computer named ISA1. All Internet access for the local network occurs through ISA1.

The network contains a Web server named Server1. Server1 is configured as a SecureNAT client. A Web application runs on Server1 that communicates with an external Web site named www.contoso.com.

You configure ISA1 with two access rules for outbound HTTP access. The rules are named HTTP Access 1 and HTTP Access 2.

HTTP Access 1 is configured to use the All Authenticated Users user set as a condition. HTTP Access 2 is configured to use the All Users user set as a condition, and it restricts outbound HTTP traffic to the IP address of Server1.

You verify that users can access external Web sites. However, you discover that the Web application cannot access www.contoso.com.

You need to allow the Web application to use anonymous credentials when it communicates with www.contoso.com. You also need to require authentication on ISA1 for all users when they access all external Web sites.

What should you do?

- A. On Server1, configure Web Proxy clients to bypass the proxy server for the IP address of the server that hosts www.contoso.com.
- B. On ISA1, add the fully qualified domain name (FQDN) www.contoso.com to the list of domain names available on the Internal network.
- C. On ISA1, disable the Web Proxy filter for the HTTP protocol.
- D. Modify the order of the access rules so that HTTP Access 2 is processed before HTTP Access 1.

Answer: D