KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **070-351**

Title : MS Internet Security & Acceleration Serv 2006, Configuring

Version : Demo

1. You are a network administrator for Litware, Inc. The network contains an ISA Server 2006 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 2006 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.

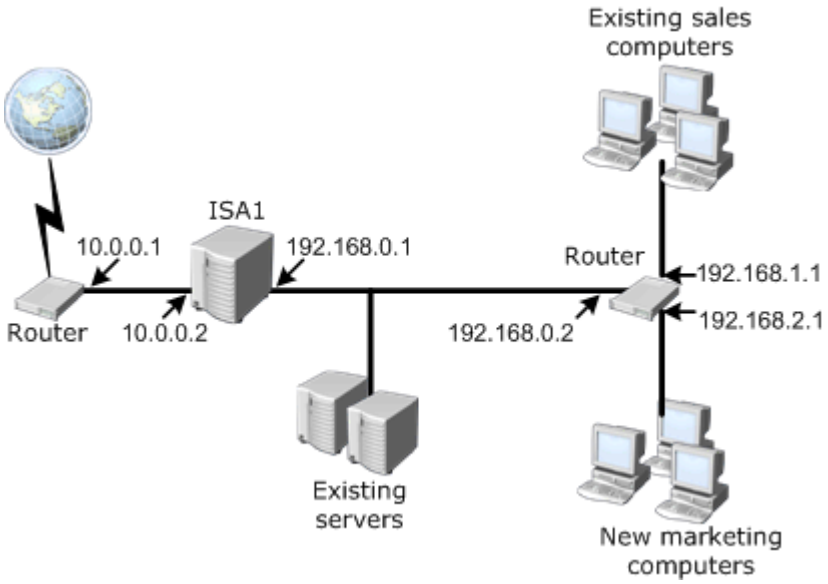
D. Modify the order of the access rules so that HTTP Access 2 is processed before HTTP Access 1.

Answer: D

3. You are a network administrator for your company. The network contains an ISA Server 2006 computer named ISA1. ISA1 is configured to allow users in the sales department access to resources on the Internet.

Users in the marketing department also want access to resources on the Internet. You add a new network and computers for the marketing department. You install the Firewall Client and configure the Web Proxy client on all computers in the new network.

The company's network is configured as shown in the exhibit. (Click the Exhibit button.)



Users in the marketing department report that they cannot access resources on the Internet. You verify that users in the sales department and the internal servers can still access resources on the Internet.

You need to ensure that users in the marketing department can access resources on the Internet.

What should you do?

A. Configure the marketing computers to use 192.168.0.1 as the default gateway.

B. On ISA1, add a static route for the 192.168.2.1 network.

C. On ISA1, add the address range for the Marketing subnet to the internal network list.

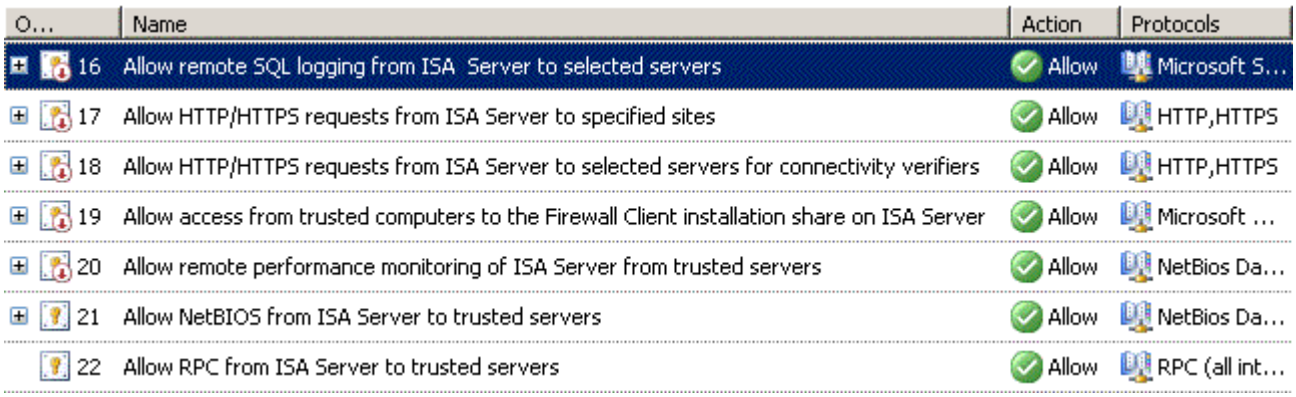
D. Configure the DNS settings of the marketing computers to use a DNS server that can resolve Internet names.

Answer: B

4. You are the network administrator for your company. The network contains two ISA Server 2006 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 ISA1 cannot connect to the virus update Web site or the Windows Update Web site. The firewall policy on ISA1 is configured as shown in the exhibit. (Click the Exhibit button.)



O...	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...

You need to ensure that ISA1 can connect to the virus update Web site and the Windows Update Web site.

What should you do?

A. On ISA1, 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.

B. On ISA1, 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.

C. 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.

D. 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

5. You install ISA Server 2006 on a computer that has three network adapters. One of the network adapters is connected to the Internet, one is connected to the Internal network, and one is connected to a perimeter network.

The perimeter network adapter and the internal network adapter are connected to private address networks.

You configure ISA Server by applying the 3-Leg Perimeter network template. You run the 3-Leg Perimeter Network Template wizard. You then make the following changes to the firewall policy:

x Create an access rule to allow all traffic between the Internal network and the Internet.

x Create an access rule to allow all traffic between the Internal network and the perimeter network.

x Create an access rule to allow SMTP traffic from an SMTP server on the perimeter network to a Microsoft Exchange Server computer on the Internal network.

x Create a server publishing rule to allow SMTP traffic from the External network to the SMTP server on the perimeter network.

Users report that they cannot receive e-mail messages from users outside of the Internal network.

You need to allow users to receive e-mail messages from other users on the Internet. You do not want to create a server publishing rule.

What should you do?

A. Change the network rule that controls the route relationship between the perimeter network and the Internal network to Route.

B. Change all network rules that control the route relationships between the Internal network, perimeter network, and External network to Route.

C. Change the network rule that controls the route relationship between the perimeter network and the External network to NAT.

D. Change all network rules that control the route relationships between the Internal network, perimeter network, and External network to NAT.

Answer: A

6. Your network contains an ISA Server 2006 array. The array contains six members.

You enable Cache Array Routing Protocol (CARP) so that outbound Web requests are resolved within the array.

Soon after you enable CARP on the array, Web users on the corporate network report that Internet access is slower than normal.

You use Network Monitor to check network traffic patterns on each of the ISA Server 2006 array members. You discover that there is very high network utilization on the intra-array network.

You need to reduce the amount of intra-array traffic.

What should you do?

A. Enable Network Load Balancing on the intra-array network.

B. Configure the client computers as SecureNAT clients.

C. Use automatic discovery to configure the client computers as Web Proxy clients.

D. Enable CARP on the intra-array network.

Answer: C

7. You are the network administrator for your company. The network contains two ISA Server 2006 computers named ISA1 and ISA2. ISA1 is configured as the Enterprise Configuration Storage server. ISA1 and ISA2 are members of a single enterprise array.

A Web server named Web1 resides in the perimeter network. You publish an external Web site on Web1. You publish an internal Web site on the array.

ISA1 and ISA2 are each configured with a RAID-5 volume. You enable a cache drive on ISA1. You enable Cache Array Routing Protocol (CARP) on the Internal network on ISA1 and ISA2.

Users report that access to Web1 is very slow. You discover that physical disk usage is extremely high on ISA1 and Web1.

You need to configure ISA Server 2006 to allow faster access to Web1.

What should you do?

A. On ISA1, increase the HTTP caching Time to Live (TTL) setting to 50.

B. On ISA1, increase the size of the cache drive.

C. On ISA2, enable a content download job for the Web sites on Web1.

D. On ISA2, configure a cache drive.

Answer: D

8. Your network contains two ISA Server 2006 Enterprise Edition computers named ISA1 and ISA2. ISA1 and ISA2 are configured as members of an ISA Server 2006 array.

You configure the array to cache outgoing Web requests. You configure the array so that the cached Web content is distributed between ISA1 and ISA2.

You want to minimize the traffic on the intra-array network.

What should you do?

A. Enable Cache Array Routing Protocol (CARP) on the Local Host network.

B. Enable the client computers to download the automatic configuration script.

C. Configure a content download job on the array.

D. Configure Network Load Balancing on the Internal network.

Answer: B

9. You are the administrator of an ISA Server 2006 computer named ISA1. ISA1 is connected to the Internet. All client computers are configured as SecureNAT clients.

The company's new written security policy states that only Web-based traffic will be permitted through the ISA Server. In the past, all instant messaging traffic was allowed.

You need to configure ISA1 to block all instant messaging traffic and all other non-Web traffic.

What should you do?

A. Delete all current access rules.

Create a new access rule that has only HTTP and HTTPS as the allowed protocols.

Configure HTTP filtering and add signatures for instant messaging applications.

B. Create a new access rule that denies all instant messaging protocols.

Create a new access rule that has only HTTP and HTTPS as the allowed protocols.

C. Create a new access rule that has only HTTP and HTTPS as the allowed protocols.

Configure HTTP filtering and add signatures for instant messaging applications.

Unbind the HTTP filter from the HTTP protocol definition.

D. Create a computer set definition for instant messaging servers on the Internet.

Create a new access rule that denies all instant messaging protocols to the computer set you defined.

Create a new access rule that has only HTTP and HTTPS as the allowed protocols.

Answer: A

10. You are the network administrator for your company. The network contains an ISA Server 2006 computer named ISA1, which was recently installed.

The company's written security policy states that all HTTP traffic must go through ISA1.

The human resources (HR) department creates a new HR Web site, which employees use to access and manage their benefits. The HR Web site has its own Windows Server 2003 Web server and its own server publishing rule on ISA1.

Security requirements dictate that employees must not be able to access the HR Web site from an

untrusted client computer.

You need to configure the server publishing rule to meet the security requirements.

Which network object should you enable?

A. External

B. Local Host

C. Quarantined VPN Clients

D. All Protected Networks

Answer: D