Microsoft 70-351

Microsoft 70-351 TS: MS Internet Security & Acceleration Server 2006, Configuring

Practice Test

Version: 2.2

QUESTION NO: 1

Your network consists of a single Active Directory domain named contoso.com. The network contains an ISA Server 2000 computer named ISAL.
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 2006 Migration Tool. When you use Network Monitor on ISA1, you discover that client requests for App1 and App2 are being passed through ISAL
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, P0P3, and SMTP access rules on ISAL
B. Configure an Application.ini file on the client computers.
C. Redeploy the ISA Server 2006 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

QUESTION NO: 2

Your network contains an ISA Server 2006 computer named ISAL ISA1 is configured as a remote access VPN server and as a DHCP server.
VPN client computers need to be assigned the following DHCP options:
DNS
WINS
Domain name
On the DHCP server, you create a DHCP scope that includes the three DHCP options.
VPN users report that they cannot connect to file shares after logging on to the network. You

discover that no WINS or DNS server address is assigned to the VPN clients, and no primary domain name is listed.
You need to ensure that the DHCP options are assigned to the VPN client computers.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Remove the DHCP server from ISA1 and place it on a computer that is behind ISAL
B. Configure the Routing and Remote Access internal network adapter as a DHCP client.
C. In the ISA Server Management console, configure VPN address assignment to use the Internal network for the DHCP, DNS, and WINS services.
D. Install a DHCP Relay Agent on ISAL

Answer: A,D

QUESTION NO: 3

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 NO: 4

Your network contains a single ISA Server 2006 computer named ISAL
The company's written security policy states that ISA1 must authenticate users before users on the Internet are allowed to access corporate Web servers.
You install a new Web server on the Internal network. Partners and customers will access the Web pages hosted by this Web server only from the Internet.
You need to configure ISA1 to publish the Web site hosted by this Web server, and you need to adhere to the company's security policy.

What should you do?

A. Create a Web publishing rule. Configure the rule to require user authentication.
B. Create a Web publishing rule. Configure the rule to perform link translation.
C. Create an HTTP server publishing rule. Configure the rule to specify that requests appear to come from ISAL
D. Create an HTTP access rule. Configure the rule to allow connections from the External network to the Internal network.

Answer: A

QUESTION NO: 5

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 NO: 6

Your network contains an ISA Server 2006 computer named ISAL
The company deploys a new secure Web site. The Web site hosts an application named Appl.
Appl must record the client IP source address in the Appl logs for every request.
You need to configure ISA1 to publish the new Web site. First, you create an SSL Web publishing rule. Now, you need to configure the rule to meet the requirements.
What should you do?

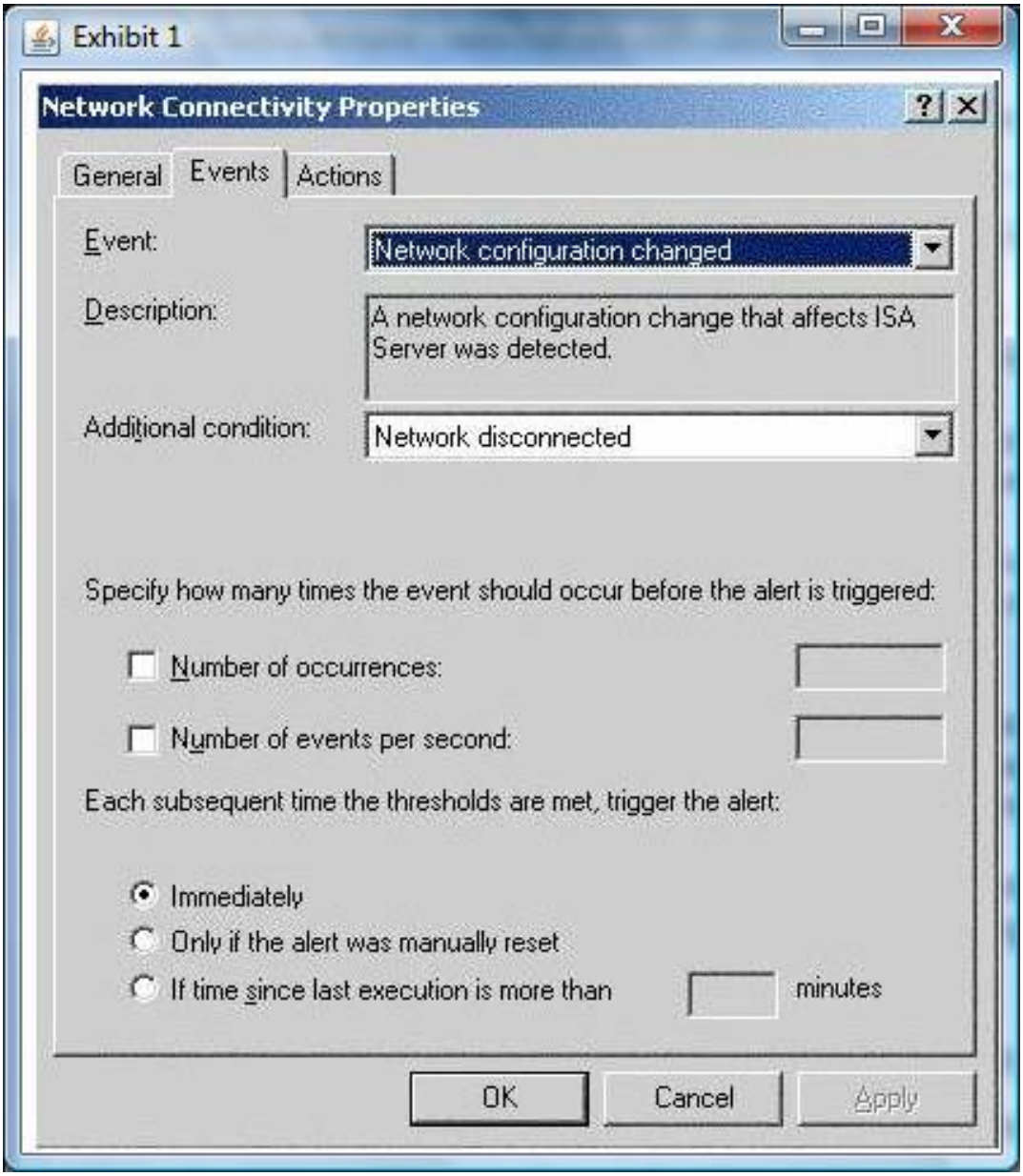
A. Configure the rules link translation to replace absolute links in all Web pages.

B. Configure the rule to forward the original host header to the published Web server.
C. Configure the rule to forward the requests so that they appear to come from ISA1.
D. Configure the rule to forward the requests so that they appear to come from the original client.

Answer: D

QUESTION NO: 7

Your network contains an ISA Server 2006 computer named ISA1, which runs Windows Server 2003.
ISA1 has three network adapters. Each adapter is connected to one of the following: Internal network, perimeter network, and Internet. All administrative hosts exist in the Internal network.
You create a file named C:\Alerts\NetworkAlert.cmd. The NetworkAlert.cmd uses net.exe to send the following message to all administrative computers: Problem with network connectivity on ISA1.
You enable the default Network configuration changed alert. You add a custom alert named Network Connectivity.
The properties of the Network Connectivity alert are configured as shown in the Alert Events exhibit and the Alert Actions exhibit. (Click the Exhibit button.)



You test the Network Connectivity alert by disabling the ISA1 network adapter that is connected to the perimeter network. You see the corresponding alert in both the Alerts view and the application log of Event Viewer.

However, the message is not received on any of the administrative computers.
You need to ensure that the administrative computers receive the text message when the Network Connectivity alert is triggered. You also need to be able to test the alert by disabling the perimeter network adapter on ISAL
What should you do?

A. Disable the default Network configuration changed alert.
B. Enable and start the messenger service and the alert service on ISA1 and on your administrative computer.
C. On ISA1 configure the DisableDHCPMediaSense entry with a value of 1.
D. Configure the Network Connectivity alert actions to run NetworkAlert.cmd by using an account that has the Log on as a batch job right.

Answer: D

QUESTION NO: 8

Your network contains a server that runs ISA Server. The ISA Server is a member of an Active Directory domain. The ISA Server provides Internet access and is the default gateway for all computers on the network.
Your company uses Web Proxy Automatic Discovery (WPAD) to configure the Web browsers' proxy settings.

You create the following objects on the server:
Two user sets named Internet Users and Admin Internet Users
a URL set named Blocked Sites that contains the URLs of Internet sites to which users should be blocked
You need to configure the Firewall Policy rules on the ISA Server to meet the following requirements:

Members of Internet Users must be able to access Internet Web sites, except for the sites in the Blocked Sites URL set.

Members of Admin Internet Users must be able to access all Internet Web sites.
HTTP, HTTPS, and FTP must be available for all allowed sites.

Which set of access rules should you create?

A. Rule 1: Allow HTTP, HTTPS, and FTP protocols from the Internal network to the External network, except for the Blocked Sites URL set, for the Internet Users user set.
Rule 2: Allow HTTP, HTTPS, and FTP protocols from the Internal network to the External network for the All Authenticated Users user set, except for the Internet Users user set.
B. Rule 1: Allow HTTP, HTTPS, and FTP protocols from the Internal network to the External network, except for the Blocked Sites URL set, for the Internet Users user set, and the Admin Internet Users user set.
Rule 2: Allow HTTP, HTTPS, and FTP protocols from the Internal network to the Blocked Sites URL set for the Admin Internet Users user set.
C. Rule 1: Allow HTTP, HTTPS, and FTP protocols from the External network to the Internal network, except for the Blocked Sites URL set, for the Internet Users user set.
Rule 2: Allow HTTP, HTTPS, and FTP protocols from the Internal network to the External network for the Admin Internet Users user set.
D. Rule 1: Allow HTTP, HTTPS, and FTP protocols from the External network to the Internal network, except for the Blocked Sites URL set, for the Internet Users user set, and the Admin Internet Users user set.
Rule 2: Allow HTTP, HTTPS, and FTP protocols from the Internal network to the Blocked Sites

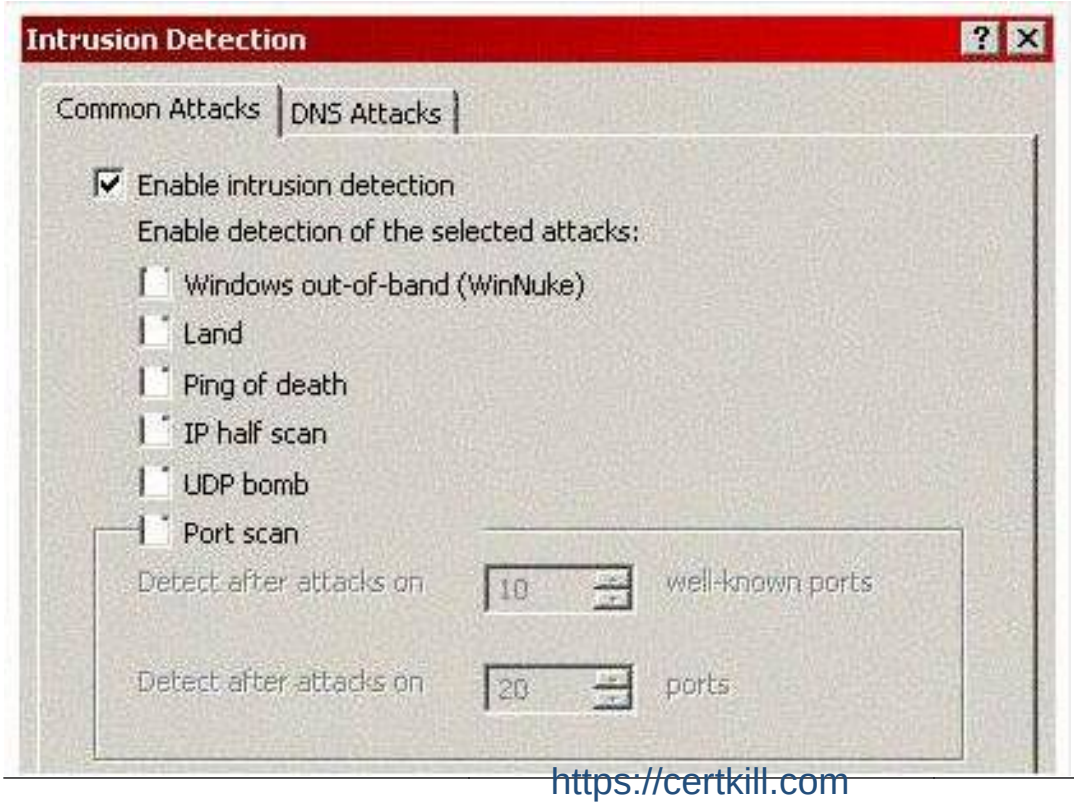
URL set for the Admin Internet Users user set.

Answer: B

QUESTION NO: 9 HOTSPOT

)Your network contains an ISA Server 2006 computer named ISAL
You use Network Monitor to capture and analyze inbound traffic from the Internet to ISAL You notice a high volume of TCP traffic that is sent in quick succession to
random TCP ports on ISAL
The flag settings of the raffle are shown in the following example.
TCP: Flags = 0x00:.....
TCP: ..0.....= No urgent data
TCP: ...0.... = Acknowledgement field not significant TCP: ....0... = No Push function
TCP:.....0.. = No Reset
TCP:.....0. = No Synchronize
TCP:.....0 = No Fin
This traffic slows the performance of ISAL
You want to be able to create a custom alert that is triggered whenever ISA1 experiences traffic that uses invalid flag settings to discover open ports. You do not want the alert to be triggered by traffic that uses valid flag settings in an attempt to discover open ports. You want to accomplish this goal by selecting only the minimum number of options in the Intrusion Detection dialog box.
What should you do?

To answer, configure the appropriate option or options in the dialog box in the answer area.



Answer:

Explanation:

QUESTION NO: 10

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 NO: 11

Your network contains a VPN server that runs ISA Server 2006.
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 NO: 12

Your network contains an ISA Server 2006 computer named ISA1, which is configured as a remote access VPN server. You configure ISA1 to accept both PPTP and L2TP over IPSec VPN connections from remote access clients.
Several users report that they cannot connect to the network. You review the log files on ISA1 and