Exam Code: 070-350
Implementing Microsoft Internet Security and Acceleration (ISA) Server 2004

QUESTION 1:

You are a network administrator for Itexamworld .com. You plan to implement ISA Server 2004 as a SecureNAT firewall for client computers on the network. The implementation will consist of a Windows Server 2003 Network Load Balancing cluster.
External client computers that connect to resources published by ISA Server must be load balanced across the Network Load Balancing cluster when they connect by using DNS.
You need to plan the external DNS implementation before you deploy ISA Server 2004.
What should you do?

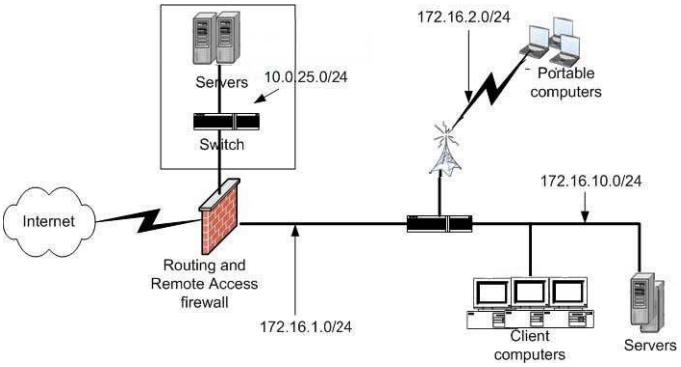
A. Create three service locater (SRV) resource records.
Configure each record to use the _HTTP service and to reference the IP address of one of the internal interfaces of the Network Load Balancing cluster nodes.
B. Create three host (A) resource records.
Configure each record with the IP address of one of the external interfaces of the Network Load Balancing cluster nodes.
C. Create one host (A) resource record.
Configure the record with the virtual IP address that is assigned to the external interface of the Network Load Balancing cluster.
D. Create one host (A) resource record.
Configure the record with the virtual IP address that is assigned to the internal interface of the Network Load Balancing cluster.

Answer: C

Explanation:
Network Load Balancing (NLB) is a Windows service that enables network traffic to be shared between multiple servers, while appearing to the client to be captured and processed by a single server's IP address. It provides for load sharing between NLB cluster members, and also provides for redundancy if one of the NLB members becomes unavailable. Only the Enterprise version of ISA Server 2004 natively supports NLB.
In this scenario we are publishing resources for external clients, therefore we need to configure publishing rules that are configured to use the external interface of the isa server.

QUESTION 2:

You are a network administrator for Itexamworld .com. The network is configured as shown in the exhibit.



You are upgrading the Routing and Remote Access server to ISA Server 2004. You need to configure the Internal network.
You need to create a access rules that are specific for each subnet.
Which three IP address ranges should you use? (Each correct answer presents part of the solution. (Choose three)

A. 10.0.25.1 - 10.0.25.255
B. 172.16.1.0 - 172.16.1.255
C. 172.16.2.0 - 172.16.2.255
D. 172.16.10.0 - 172.16.10.255
E. 192.168.1.0 - 192.168.255.255

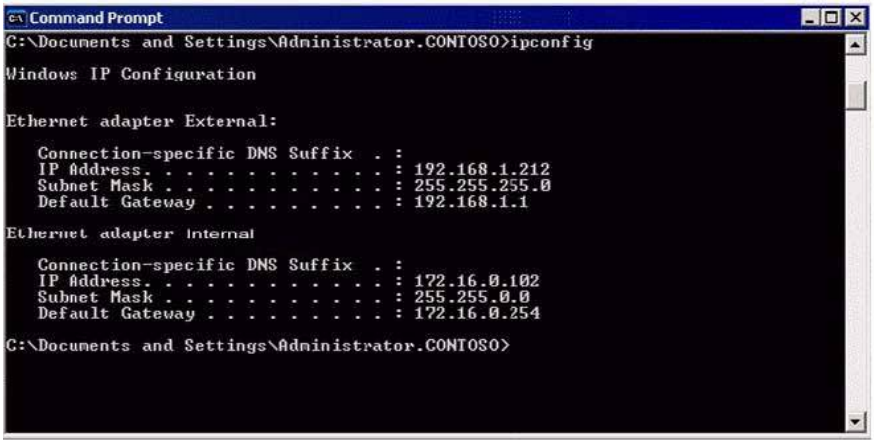
Answer: B, C, D

Explanation:
The term network in ISA server should not be confused with the concepts of subnets; the two terms are distinct in the ISA world. An ISA network is defined as the grouping of physical subnets that form a network topology that is attached to a single ISA Server network adapter. So, a single ISA "network" could be composed of multiple physical networks. Even though there are four physical subnets, all connected to each other with switches, ISA sees these individual subnets as only two networks, an internal network and a perimeter network (also called DMZ) because it has network adapters attached to only a single subnet on each of the network. To further illustrate, a uni-homed (single NIC) server would see the range of all IP addresses on the Internet as a single ISA network. In our scenario the internal network consists of 172.16.1.0 - 172.16.1.255, 172.16.2.0 - 172.16.2.255 and 172.16.10.0 - 172.16.10.255. A perimeter network, also known as a demilitarized zone (DMZ), or screened subnet, is a network that you set up separately from an internal network and the
Internet. Perimeter networks allow external users to gain access to specific servers that are located on the perimeter network while preventing direct access to the internal network. In this way, even if an attacker penetrates the perimeter network security, only the perimeter network servers are compromised.
In our scenario the DMZ consists 10.0.25.1 - 10.0.25.255.

QUESTION 3:

You are a network administrator for Itexamworld .com. Client computers on the

internal network are divided among several subnets by using routers.
You install an ISA Server 2004 computer named ISA1. ISA1 will be used to allow users to access Web sites on the Internet. You configure TCP/IP on ISA1 as shown in the exhibit.



After ISA1 is installed, 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)

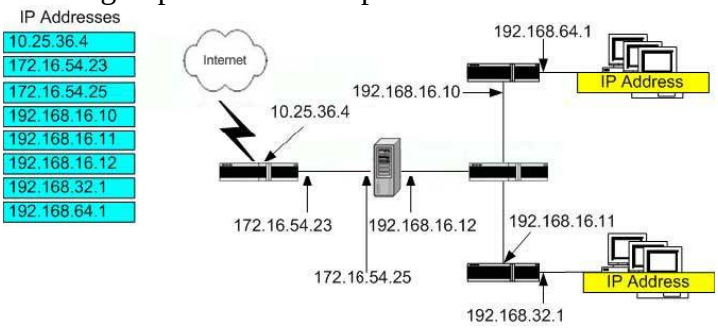
A. Configure the internal default gateway to match the external default gateway. B. Configure a static route to each subnet.
C. Add the IP address of the internal default gateway to the Remote Management Computers computer set.
D. Configure the internal network adapter with a blank default gateway. E.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

Answer: B, D
Explanations:
The routing table on the ISA firewall machine should be configured before you install the ISA firewall software. The routing table should include routes to all networks that are not local to the ISA firewall's network interfaces. These routing table entries are required because the ISA firewall can have only a single default gateway. Normally, the default gateway is configured on the network interface that is used for the External Network. Therefore, if you have an internal or or other Network that contains multiple subnets, you should configure routing table entries that ensure the ISA firewall can communicate with the computers and other IP devices on the appropriate subnets. The network interface with the default gateway is the one used to connect to the Internet, either direction or via upstream routers. After knowing this we should remove the default gateway IP Address from the internal network card and we should configure static routes to each subnet.

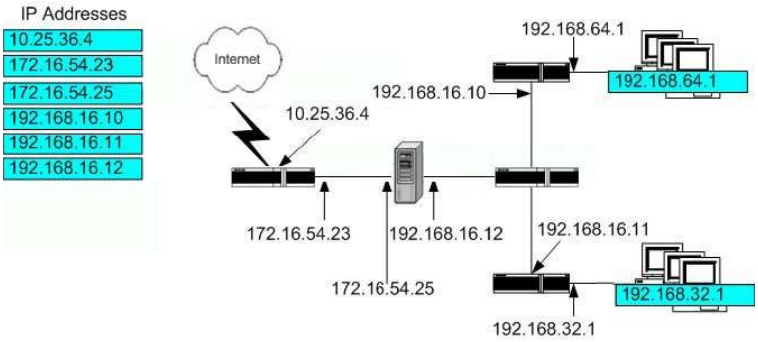
QUESTION 4:

You are a network administrator for Itexamworld .com. You plan to deploy one ISA

Server 2004 computer, three routers, and one switch to provide Internet access to client computers on the network. This planned network is shown in the answer area. You must ensure that client computers can access the Internet as SecureNAT clients after ISA Server is deployed. You examine several client computers and discover that the default gateway is not configured.
You need to configure the correct default gateway for client computers.
What should you do?
To answer, drag the appropriate default gateway IP address or addresses to the correct groups of client computers in the answer area.



Answer:



Explanation:
In the simple network scenario, the default gateway of the SecureNAT client is configured as the IP address of the Internal interface of the ISA 2004 firewall. You can manually configure the default gateway address, or you can use DHCP to automatically assign addresses to the SecureNAT clients. The DHCP server can be on the ISA 2004 firewall itself, or it can be located on a separate machine on the Internal network. In the 'complex network scenario,' the Internal network consists of multiple network IDs that are managed by a router or series of routers or layer 3 switch(s). In the case of the complex network, the default gateway address assigned to each SecureNAT client depends on the location of the SecureNAT client computer. The gateway address for the SecureNAT client will be a router that allows the SecureNAT client access to other networks within the organization, as well as the Internet. The routing infrastructure must be configured to support the SecureNAT client so that Internet-bound requests are forwarded to the Internal interface of the ISA 2004 firewall.

QUESTION 5:

You are a network administrator for Itexamworld .com. Itexamworld has a main office and

three branch offices.
You are planning to deploy ISA Server 2004 in the branch offices to provide users which access to the Internet. The ISA Server computers will be configured as stand-alone servers. The Firewall Client installation share will be placed on an existing file server in each branch office.
You install Windows Server 2003 on the computers that will run ISA Server 2004.
You need to configure additional security for the ISA Server computers.
What are three possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose three)

A. Grant the Allow log on locally right to only the Administrators group.
B. Disable the external network adapter.
C. Enable the Secure Server (Require Security) IPSec policy.
D. Disable the Server service.
E. Remove all users from the Access this computer from the network right.

Answer: A, D, E
Explanations:
Secure Server (Require Security) policy - This policy is only appropriate for servers that require all communications to be secure. Once this policy has been applied, the server will neither send or accept insecure communications. Any client wanting to communicate with the server must use at least the minimum level of security described by the policy. In this scenario it will not work because the clients do not have Ipsec installed.
Allow log on locally - This logon right determines which users can interactively log on to this computer. Logons initiated by pressing CTRL+ALT+DEL sequence on the attached keyboard requires the user to have this logon right.
Access this computer from the network - This user right determines which users and groups are allowed to connect to the computer over the network. This would still be needed if the firewall client installation share resided on the isa server. In this scenario the ISA Server2004 Client Installation Share resides on another server, so we can remove the users from the list.
Disable the Server service - You need the Server service if you : You install ISA Server2004 Client Installation Share or use the Routing and Remote Access Management, rather than ISA Server Management, to configure a VPN. In this scenario we are not using both.
Disable the external network adapter - In this scenario the external adapter has been connected to the internet. If we disable that adapter then nobody would we able to connect to the internet and no VPN could be set up.

QUESTION 6:

You are a network administrator for Itexamworld .com. The 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 Itexamworld 1. 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.
1. Employees must be allowed access to only Itexamworld 1, three file servers, and an internal Web server named Web1.
2. Employees must have installed all current software updates and antivirus software before connecting to any internal resources.
3. Partners must be allowed access to only Itexamworld 1.
4. You must not install any software other than the App1 client on any partner computers.
You need to plan the VPN configuration for Itexamworld
. 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 for 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

Explanation:
VPN quarantine control allows you to screen VPN client machines before allowing them access to the organization's network. To enable VPN quarantine, you create a Connection Manager Administration Kit (CMAK) package that includes a VPN client profile and a VPN-quarantine client-side script. This
script runs on the client and checks the security configuration of the remote access client and reports the results to the VPN server. If the client passes the security configuration check, the client is granted access to the organizations network.
If you are using ISA Server as the VPN server, and the script reports that the client meets

the software requirements for connecting to the network, the VPN client is moved from the VPN Quarantine network to the VPN Clients network. You can set different access policies for hosts on the VPN Quarantine network
compared to the VPN Clients network. The partners do not need to be quarantined so we exclude them from the Quarantine Control. ISA Server uses these networks just like it uses any other directly connected networks. That means that you can use network rules and access rules to define the conditions under which network packets will be passed from one network to another.

QUESTION 7:

You are the network administrator for Itexamworld .com. The network consists of a single Active Directory domain named Itexamworld .com. The network contains an ISA Server 2004 computer named ISA1.
ISA1 is configured as a VPN server and allows only VPN connections that use PPTP. ISA1 is configured to use a RADIUS server named Itexamworld 1 to provide authentication and authorization for VPN client connections.
You want to configure ISA1 to also allow VPN connections that use L2TP. For testing purposes, you want VPN clients to be able to use preshared keys for authentication.
You perform the following actions on ISA1:
1. In the Routing and Remote Access console, you enable the Allow custom IPSec policy for L2TP connection option and enter a value for a preshared key.
2. In the ISA Server Management console, you enable L2TP over IPSec settings in the VPN Clients Properties dialog box.
You test L2TP functionality by configuring a VPN connection object on a computer named Workstation1, which runs Windows XP Professional with Service Pack 2.
The VPN connection object is configured to use the same preshared key that you configured on ISA1. However, when you try to connect to ISA1 by using L2TP, you receive the following error message: "Error 792: The L2TP connection failed because security negotiation timed out."
You need to configure ISA1 to support L2TP connections that use preshared keys.
What should you do?

A. In the ISA Server Management console, enable the use of a custom IPSec policy and configure a preshared key in the Virtual Private Networks (VPN) Properties dialog box.
B. In the ISA Server Management console, enable EAP in the Virtual Private Networks (VPN) Properties dialog box.
C. In the RADIUS remote access policy profile for the VPN connection, add MD5-Challenge as an authentication method.
D. In the RADIUS remote access policy profile for the VPN connection, add Protected Extensible Authentication Protocol (PEAP) as an authentication method.

Answer: A

Explanation:
Error 792 can be caused by :
* You have a preshared key that is configured on the client, but the key is not configured on the Routing and Remote Access Service server.
* VPN server is not a valid machine certificate or is missing.
* The IPSec Policy Agent service is stopped and started without stopping and starting the Routing and Remote Access service on the remote computer.
* The IPSec Policy Agent service is not running when you start the Routing and Remote Access service.
* The ISA Server computer is configured to block IP fragments.
In this scenario we need to : In the ISA Server Management console, enable the use of a custom IPSec policy and configure a preshared key in the Virtual Private Networks (VPN) Properties dialog box and NOT in the RRAS console. VPN properties should be configured in the ISA Console and not in the RRAS console because the ISA console overrides RRAS settings.

QUESTION 8:

You are the network administrator for Itexamworld .com. The network contains an ISA Server 2004 computer named ISA1. ISA1 functions as a remote access VPN server for the network. Remote access VPN clients can use either PPTP or L2TP over IPSec to connect to ISA1.
Users report that after connecting to the corporate network, they cannot access file shared on the network file server without first being presented with an authentication prompt.
You need to ensure that users are not asked for credentials when they access file shares.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Instruct the users to log on by using their domain credentials via dial-up networking.
B. Configure ISA1 as a RADIUS client.
C. Create an access rule to enable the LDAP and LDAP5 protocols form the Local Host network to the Internal network.
D. Join ISA1 to the domain.

Answer: A, D

Explanation:
The placement of the ISA VPN server ultimately governs how user accounts are accessed during authentication. The following authentication methods are available:
* Authenticating directly against Active Directory - If the ISA VPN server is installed as a domain member server, users can be authenticated directly against the internal Active Directory domain without any additional configuration.
* Implement RADIUS Authentication - A RADIUS server, such as Microsoft's IAS, included with both the Windows 2000 Server and Windows Server 2003, can allow the

stand-alone ISA VPN server to authenticate users against the internal domain. This service is very useful when the ISA VPN server has been implemented in a DMZ configuring.
* Authenticate against local users - It is possible to configure local users on the ISA VPN server. This type of configuration is usually not recommended in a production environment, but may be acceptable in specific lab scenarios.
In this scenario we need to join the ISA server to the domain. After that we can simply instruct the users to logon by using their domain credentials via dial-up networking. Now they won't be prompted anymore to access the files.

QUESTION 9:

You are the network administrator for Itexamworld .com. Itexamworld 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. ISA1 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. Change the Phase II IPsec configuration on both ISA1 and ISA2 to use Message Digest 5 (MD5) as its integrity algorithm.
D. Create a new protocol definition for TCP port 80 outbound and use the definition in the access rule.

Answer: D

Explanation:
As the scenario stated : Users at the branch office report that they can connect to file shares at the main office.
Therefore we can assume that the VPN tunnel has been correctly setup and is fully functional. All we need to do is create a rule that allow the branch office users to connect to the OWA website. We can achieve this by creating a new protocol definition for TCP port 80 outbound and use the definition in the access rule.

QUESTION 10:

You are the network administrator for Itexamworld .com. The network contains an ISA Server 2004 computer named IS1, 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 discover that the users with failed connection attempts are all using L2TP over IPSec.
You need to ensure that the users can connect to the network.
What should you do?

A. Disable IP fragment blocking.
B. Disable IP routing.
C. Disable IP options filtering
D. Disable verification of incoming client certificates.

Answer: A

Explanation:
You can also configure ISA Server to drop all IP fragments. A single IP datagram can be divided into multiple datagrams of smaller sizes known as IP fragments. If you enable this option, then all fragmented packets are dropped when ISA Server filters packet fragments. A common attack that uses IP fragments is the teardrop. In this attack, multiple IP fragments are sent to a server. However, the IP fragments are modified so that the offset fields within the packet overlap. When the destination computer tries to reassemble these packets, it is unable to do so. It may fail, stop responding, or restart. Enabling IP fragment filtering can interfere with streaming audio and video. In addition, Layer Two Tunneling Protocol (L2TP) over IPSec connections may not be successfully established because packet fragmentation may take place during certificate exchange. This scenario has IP fragment blocking enabled, therefor we must disable it to allow L2TP over Ipsec communication.

QUESTION 11:

You are the network administrator for Itexamworld .com. The network contains an ISA Server 2004 computer named ISA1.
You enable VPN Quarantine Control on ISA1. You create a Connection Manager (CM) profile and install it on VPN client computers.
The CM profile contains a script named quarantine.vbs that performs several tests on VPN client computers to ensure conformance with Itexamworld policy. If a computer passes the tests, the script executes the following command:
RQC %1 %2 %3 %4 SV1.
The variables in the command represent the parameters inherited from the CM profile. The parameters are shown in the following table.

Variable	Parameter
%1	%DialRasEntry%
%2	%TunnelRasEntry%

%3	%Domain%
%4	%UserName%

Users report that after they establish a VPN connection with ISA1, they receive a message stating that their computer has been placed in quarantine mode. The VPN connection is terminated, and they are prompted to reconnect. You verify that the client computer configurations conform to Itexamworld policies and pas the tests on the quarantine.vbs script.
The System log displays a large number of instance of the following warning message: "A remote access client at IP address w.x.y.z connected by Itexamworld \username has been rejected because it presented the following unrecognized quarantine string: SV1"
You need to ensure that VPN client computers can be moved out of the Quarantined VPN Clients network when the quarantine.vbs script executes successfully.
What should you do?

A. Create a new CM profile by using the Connection Manager Administration Kit (CMAK). Append the text string "SV1" to the lost of parameters for the custom action.
B. Edit the quarantine.vbs scipt so that it used the following command:
RQC %DialRasEntry% %TunnelRasEntry% 7250 %Domain% %UserName%
C. On ISA1, configure the AllowedSets values for the RQS service by including the text string "SV1".
D. Use the Connection Manager Administration Kit (CMAK) to change the post-connect action to Rqc.exe.

Answer: C

Explanation:
The VPN quarantine control feature allows you to screen VPN client machines before allowing them access to the organizations network. VPN quarantine control can delay normal remote access to a private network until the remote access client configuration has been validated by a client-side script. Configuring quarantine control on ISA Server requires a number of configuration steps. Before you enable quarantine mode, you must complete the following steps:
* Create a client-side script that validates client configuration information.
* Use CMAK to create a CM profile that includes a notification component and the client-side script.
* Create and install a listener component on the ISA Server.
* Enable quarantine control on ISA Server.
* Configure network rules and access rules for the Quarantined VPN Clients network.
The Network Quarantine Service (Rqs.exe) provides the listener service for computers running ISA Server to support VPN Quarantine. This component must be installed on all computers running ISA Server that will provide quarantine services.
The easiest way to install the Network Quarantine Service and configure ISA Server to support listener network traffic is to use the ConfigureRQSForISA.vbs script provided with ISA Server 2004. The syntax to use this script is:

Cscript ConfigureRQSForISA.vbs /install SharedKey1\0SharedKey2
* The /install command line switch installs the listener service. To uninstall the listener service, use /remove.
* The SharedKey value is the key that the notification component will send to the listener component. The notification message sent by Rqc.exe contains a text string that indicates the version of the quarantine script being run. This string is configured for Rqc.exe as part of its command-line parameters, as run from the quarantine script. Rqs.exe compares this text string to a set of text strings stored in the registry of the computer running ISA Server. If there is a match, the quarantine conditions are removed from the connection. If the client provides a shared key that is not in the allowed set, it will be disconnected. There can be more than one shared key, separated by \0".
* defines where the listener executable is located.
However in this scenario we can see that the scriptversion name is SV1. This script will be executed on the client side. On the ISA server there must be a registry entry called allowedsets with a value SV1. otherwise we will get the error mentioned in the scenario.

QUESTION 12:

You are the network administrator for Itexamworld .com. Itexamworld has a main office and one branch office.
The main office has one ISA Server 2004 computer named ISA1, which runs Windows Server 2003. The branch office has one ISA Server 2004 computer named ISA2, which runs Windows 2000 Server.
You create a site-to-site VPN connection between ISA1 and ISA2. You configure IPSec tunnel mode for the site-to-site connection.
When you test the site-to-site site VPN connection, the connection attempt fails.
You need to enable the IPSec tunnel mode site-to-site VPN connection between the main office and the branch office.
What should you do?

A. Install the IPSecPol tool on ISA1.
B. Install the IPSecPol tool on ISA2.
C. Configure a custom IPSec policy on ISA1.
D. Configure a custom IPSec policy on ISA2.

Answer: B

Explanation:
IPSec tunnel mode - Tunneling is the entire process of encapsulation, routing, and decapsulation. Tunneling wraps, or encapsulates, the original packet inside a new packet. This new packet might have new addressing and routing information, which enables it to travel through a network. When tunneling is combined with data confidentiality, the original packet data (as well as the original source and destination) is not revealed to those listening to traffic on the network. After the encapsulated packets reach their destination, the encapsulation is removed, and the original packet header is used to route

the packet to its final destination.
The tunnel itself is the logical data path through which the encapsulated packets travel. To the original source and destination peer, the tunnel is usually transparent and appears as just another point-to-point connection in the network path. The peers are unaware of any routers, switches, proxy servers, or other security gateways between the tunnels beginning point and the tunnels endpoint. When tunneling is combined with data confidentiality, it can be used to provide a VPN.
The encapsulated packets travel through the network inside the tunnel. In this example, the network is the Internet. The gateway might be an edge gateway that stands between the outside Internet and the private network. The edge gateway can be a router, firewall, proxy server, or other security gateway. Also, two gateways can be used inside the private network to protect traffic across untrusted parts of the network.
When Internet Protocol security (IPSec) is used in tunnel mode, IPSec itself provides encapsulation for IP traffic only. The primary reason for using IPSec tunnel mode is interoperability with other routers, gateways, or end systems that do not support L2TP over IPSec or PPTP VPN tunneling.
To create a remote site network that uses the IPSec protocol tunneling mode on a computer running Windows 2000 (ISA2 in our scenario), you must install the IPSecPol tool, available on the Microsoft website.

QUESTION 13:

You are the network administrator for Itexamworld .com. Itexamworld has a main office and is adding a branch office.
You are connecting the main office and branch office networks. You install ISA Server 2004 on a computer at each office, and you create a site-to-site VPN connection between the ISA Server computers.
You create remote site networks on the ISA Server computers at both offices. You choose the L2TP over IPSec VPN protocol. You want to use a preshared key for the IPSec authentication. You open the Routing and Remote Access console and enter the preshared key in the Properties dialog box for the Routing and Remote Access server.
The site-to-site L2TP over IPsec connection is successful. You then restart the ISA Server computers and discover that the site-to-site connection fails.
You need to ensure that the L2TP over IPSec site-to-site VPN connections continue to function properly after the ISA Server computers are restarted.
What should you do?

A. Re-enter the preshared keys on the ISA Server computers at both offices. Chang the preshared keys so that they include mixed-case letters, numbers, and symbols.
B. Remove all certificates for the ISA Server computers at both offices.
C. On the ISA Server computers at both offices, remove the preshared key from the Routing and Remote Access console, and enter the key on the Authentication tab of the Virtual Private Networks (VPN) Properties dialog box.
D. Install user certificates on the ISA Server computers in both offices and enable EAP user authentication for the demand-dial accounts.

Answer: C

Explanation:
Error 792 or pre-shared key issues can be caused by :
* You have a preshared key that is configured on the client, but the key is not configured on the Routing and Remote Access Service server.
* VPN server is not a valid machine certificate or is missing.
* The IPSec Policy Agent service is stopped and started without stopping and starting the Routing and Remote Access service on the remote computer.
* The IPSec Policy Agent service is not running when you start the Routing and Remote Access service.
* The ISA Server computer is configured to block IP fragments.
In this scenario we need to : In the ISA Server Management console, enable the use of a custom IPSec policy and configure a preshared key in the Virtual Private Networks (VPN) Properties dialog box and NOT in the RRAS console. VPN properties should be configured in the ISA Console and not in the RRAS console because the ISA console overrides RRAS settings.

QUESTION 14:

You are the network administrator for Itexamworld .com. Itexamworld has a main office and is adding a branch office.
The main office and the new branch each have an ISA Server 2004 computer. You want to connect the main office and the branch office networks by using a site-to-site VPN.
You create a site-to-site VPN connection that connects the office networks by using the L2TP over IPSec VPN protocol. Computer certificates are installed on the ISA Server computer at each office. When you create the remote site network on each ISA Server computer, you configure it to use certificates and a preshared key. At each office, the preshared key is configured as the office name on the ISA Server computer at that office.
From the ISA Server computer at the main office, you repeatedly run the ping command to a host on the branch office network. The site-to-site VPN fails. You open the Routing and Remote Access console and manually dial the demand-dial interface. You receive the following error message: "The last connection attempt failed because: The L2TP connection attempt failed because the security layer encountered a processing error during initial negotiations with the remote computer."
You need to enable the site-to-site VPN connection by using the most secure IPSec authentication method possible.
What should you do?

A. Restart the ISA Server computer at both offices.
B. Re-enter the preshard keys on the ISA Server computer at both offices. Change the preshared keys so that they include mixed-case letters, numbers, and symbols.

C. Remove the preshared key from the remote site network configuration on the ISA Server computer at both offices.
D. Delete the remote site network on the ISA Server computer at both offices, and re-create the remote site networks with the original parameters.

Answer: C

Explanation:
Layer Two Tunneling Protocol (L2TP) over Internet Protocol security (IPSec) - Layer Two Tunneling Protocol (L2TP) is an industry-standard Internet tunneling protocol that provides encapsulation for sending Point-to-Point Protocol (PPP) across IP networks. The Microsoft implementation of the L2TP protocol uses Internet Protocol security (IPSec) encryption to protect the data stream from the VPN client to the VPN server. L2TP/IPSec connections require user-level authentication and, in addition, computerlevel authentication using computer certificates OR a pre-shared key. In this scenario we are using both, thus we need to remove the per-shared keys to achieve highest possible security.

QUESTION 15:

You are the network administrator for Itexamworld .com. The network contains an ISA Server 2004 computer named ISA1. ISA1 functions as a VPN remote access server. Remote access VPN clients use either PPTP or L2TP over IPSec to connect to ISA1. All remote access VPN client computers are configured as both Web Proxy and Firewall clients of ISA1.
You create an access rule to allow domain users on the VPN Clients network access to all protocols and Web sites on the Internet.
A user named Bob logs on to his portable computer by using a local user account and establishes a VPN connection to ISA1 by using his domain credentials. You discover that Bob cannot connect to the Internal network when the VPN connection to ISA1 is active.
You need to ensure that Bob can access the Internet network while maintaining a VPN connection to ISA1.
What should you do?

A. Disable the Firewall client before establishing the VPN connection.
B. Disable the Web Proxy configuration before establishing the VPN connection.
C. Create an access rule to allow connections from the VPN Clients network to the Internal network.
D. Remote the authentication requirement on the access rule that allows VPN Clients access to the Internet.

Answer: C

Explanation:
As the scenario stated : A user named Bob logs on to his portable computer by using a

local user account and establishes a VPN connection to ISA1 by using his domain credentials.
Therefore we can assume that the VPN tunnel has been correctly setup and is fully functional. All we need to do is create a rule that allow Bob to connect to the internal network. We can achieve this by creating n access rule to allow connections from the VPN Clients network to the Internal network.

QUESTION 16:

You are the network administrator for Itexamworld .com. The network contains an ISA Server 2004 computer named ISA1. ISA1 provides Internet access for all users on Itexamworld 's network.
All computers on the network are configured as SecureNAT clients. You create an access rule on ISA1 that allows all users access to all protocols on the External network.
You view the Firewall log and the Web Proxy filter log on ISA1 and notice that the URLs of Web sites visited by Itexamworld users are not displayed.
You need to ensure that the URLs of Web sites visited by Itexamworld users are displayed in the ISA1 log files.
What should you do?

A. Configure all network computers as Web Proxy clients.
B. Configure all network computers as Firewall clients.
C. Configure ISA1 to require authentication for Web requests.
D. Configure ISA1 to require authentication for all protocols.

Answer: A

Explanation:
The user name is only included in Firewall and Web Proxy logs when a client sends that information to the ISA firewall. A client piece is always required to send user information to the firewall since there are no provisions in the layer 1 through 6 headers to provide this information. Only the Firewall client and Web Proxy client configurations can send user information to the ISA firewall and have this information included in the log files. SecureNAT client connections allow for logging of the source IP address, but user information is never recorded for machines configured as only SecureNAT clients.
Note that there is no option to log the URL in the Firewall Logging Properties. The reason for this is that the Firewall client doesn't send the URL for Web sites accessed via the Firewall client. However you can fix this by correctly setting up the Web proxy client configuration.

QUESTION 17:

You are the network administrator for Itexamworld .com. The network contains an ISA Server 2004 computer named ISA1. ISA1 is configured to provide forward Web caching for users on the Internet network.

During periods of peak usage, users report that it takes longer than usual for Web pages to appear. You suspect that insufficient memory is the source of the slow performance of ISA1.
You need to verify whether insufficient memory is the source of the slow performance.
Which two System Monitor performance counters should you add? (Each correct answer presents part of the solution. Choose two)

A. Memory\Pages/sec
B. Process(W3Prefch)\Pool Nonpaged Bytes
C. ISA Server Cache\Memory Usage Ratio Percent (%)
D. Physical Disk\Avg. Disk Queue Length
E. ISA Server Cache\Disk Write Rate (writes/sec)
F. Memory\Pool Nonpaged Bytes

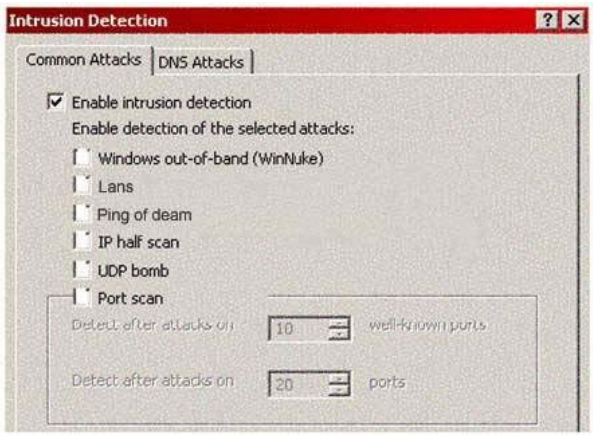
Answer: A, C

Explanation:
The ISA Server installation configures several new performance objects that you can use to monitor system performance on the computer running ISA Server. You view the performance objects and their associated
performance counters in real time in System Monitor. System Monitor is a monitoring tool that is included with Windows 2000 and Windows Server 2003.
Memory\Pages/sec - Pages/sec is the rate at which pages are read from or written to disk to resolve hard page faults. This counter is a primary indicator of the kinds of faults that cause system-wide delays. Process(W3Prefch)\Pool Nonpaged Bytes - Pool Nonpaged Bytes is the size, in bytes, of the nonpaged pool, an area of system memory (physical memory used by the operating system) for objects that cannot be written to disk, but must remain in physical memory as long as they are allocated.
ISA Server Cache\Memory Usage Ratio Percent (%) - Shows the percentage of the total amount of cache fetches that are from the memory cache. A high percentage may indicate that it is worthwhile allocating more available memory resources to the cache. A low percentage may indicate that memory resources may be better used elsewhere.
Physical Disk\Avg. Disk Queue Length - Is the average number of both read and write requests that were queued for the selected disk during the sample interval.
ISA Server Cache\Disk Write Rate (writes/sec) - Measures the number of writes per second to the disk cache for the purpose of writing URL content to the cache disk.
Memory\Pool Nonpaged Bytes - Pool Nonpaged Bytes is the size, in bytes, of the nonpaged pool, an area of system memory (physical memory used by the operating system) for objects that cannot be written to disk, but must remain in physical memory as long as they are allocated.

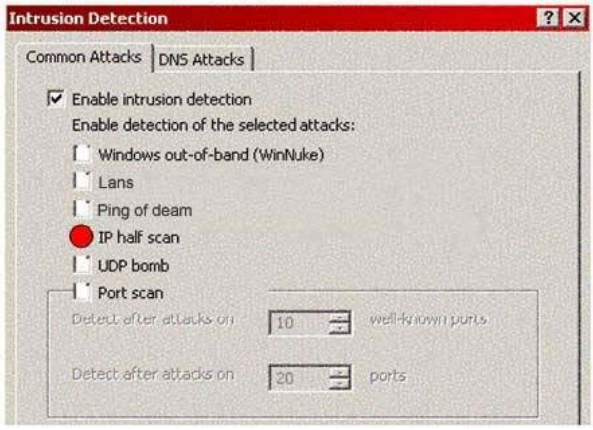
QUESTION 18:

You are the network administrator for Itexamworld .com. The network contains an ISA Server 2004 computer names ISA1.

You use Network Monitor to capture and analyze inbound traffic from the Internet to ISA1. You notice a high volume of TCP traffic that is sent in quick succession to random TCP ports on ISA1. The flag settings of the traffic are shown in the following example.
TCP: Flags = 0x00 : .....
TCP: ..0..... = No urgent data
TCP: ...0.... = Acknowledgment 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 ISA1.
You want to be able to create a custom alert that is triggered whenever ISA1 experience 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:

Windows out-of-band attack - This alert notifies you that there was an out-of-band denial-ofservice attack attempted against a computer protected by ISA Server. An out-of-band attack occurs when a Windows system receives a packet with the URGENT flag set. The system expects data will follow that flag. The exploit consists of setting the URGENT flag, but not following it with data. The port most susceptible is TCP Port 139, the Netbios Session Service port. If mounted successfully, this attack causes the computer to fail or causes a loss of network connectivity on vulnerable computers.
Land attack - This alert notifies you that a TCP SYN packet was sent with a spoofed source IP address and port number that match those of the destination IP address and port. If the attack is successfully mounted, it can cause some TCP implementations to go into a loop that causes the computer to fail.
Ping-of-death attack - This alert notifies you that an IP fragment was received with more data than the maximum IP packet size. If the attack is successfully mounted, a kernel buffer overflows, which causes the computer to fail.
Port scan - This alert notifies you that an attempt was made to access more than the preconfigured number of ports. You can specify a threshold, indicating the number of ports that can be accessed.
IP half scan - This alert notifies you that repeated attempts to send TCP packets with invalid flags were made. During an IP half scan attack, the attacking computer does not send the final ACK packet during the TCP three-way handshake. Instead, it sends other types of packets that can elicit useful responses from the target host without causing a connection to be logged. This is also known as a stealth scan, because it does not generate a log entry on the scanned host. If this alert occurs, log the address from which the scan occurs. If appropriate, configure the ISA Server rules to block traffic from the source of the scans.
UDP bomb - This alert notifies you that there is an attempt to send an illegal User Datagram Protocol (UDP) packet. These UDP packets will cause some older operating systems to fail when the packet is received. If the target machine does fail, it is often difficult to determine the cause.

QUESTION 19:

You are the administrator of an ISA Server 2004 computer named ISA1. ISA1 is configured to publish two Web sites named www.fabrikam.com and www. Itexamworld .com. Both Web sites are located on a Windows Server 2003 computer named Itexamworld 1. The IP address of Itexamworld 1 is 10.0.0.2.
The Web publishing rules are configured as shown in the following display.

Order	Name	Action	Protocols	From / Listener	To	Condition
1	Web Publish 1	Allow	HTTP	WebListener1	10.0.0.2	All Users
2	Web Publish 2	Allow	HTTP	WebListener1	10.0.0.2	All Users

Both the www.fabrikam.com/info and www. Itexamworld .com/info virtual point to a common share file.
The default log view does not allow you to easily distinguish between requests for www.fabrikam.com/info and requests for www. Itexamworld .com/info. A sample of the log with the relevant entries is shown in the following table.

Destination IP Rule URL
10.0.0.2 Web Publish 1 10.0.0.2/info
10.0.0.2 Web Publish 2 10.0.0.2/info
You need to ensure that the log viewer displays the fully qualified domain names (FQDNs) for the Web site requests. In addition, you need to filter the log viewer to display only the requests for both the www. Itexamworld .com/info and the www.fabrikam.com/info virtual subdirectories.
What should you do?

A. On ISA1, configure two Hosts file entries that resolve both FQDNs to 10.0.0.2.
Configure each Web publishing rule to use the FQDN of its respective Web site on the To tab.
In the log viewer, add to the default log filter expression a condition where the URL contains the text string "info".
B. On ISA1 configure two Hosts file entries that resolve both FQDNs to the external IP address of ISA1.
Configure each Web publishing rule so that requests appear to come from the original client computer.
In the log viewer, add a column to display the destination host name.
In the log viewer, add to the default log filter expression a condition where the URL contains the text string "info".
C. In the log viewer, add two conditions to the default log filter expression.
Configure the first condition so that the Rule equals Web Publish 1.
Configure the second condition so that the Rule equals Web publish 2.
In the log viewer, add a column to display the destination host name.
D. In the log viewer, add two conditions to the default log filter expression.
Configure the first condition so that Server contains Fabrikam.
Configure the second condition so that Server contains Itexamworld .
In the log viewer, add a column to display the destination host name.

Answer: A

Explanation:
The ISA firewall's Web Proxy filter handles all incoming Web connections made through Web Publishing Rules. Even when you unbind the Web Proxy filter from the HTTP protocol definition, the Web Proxy filter is always enabled for Web Publishing Rules.
We can see in the exhibit that there is an web publishing rule created by using using ip addresses in the to column, but we should use FQDN instead. One of the primary advantages of using a FQDN in the Computer name or IP address field is that the Web site name shows up in the URL field in the ISA firewall's Web Proxy log. If you use an IP address, only the IP address of the published server will appear in this field and make log analysis more difficult to perform efficiently. The ISA Server should know that www. Itexamworld .com and www.fabrikam.com are webservers residing on the internal network, otherwise the isa server will try to resolve the DNS name and the request will loopback through the firewall. We can resolve this issue by creating entries in the ISA's

hostfile. The hostfile will be checked first by the ISA Server before it tries to resolve the DNS queries by other DNS servers.

QUESTION 20:

You are the network administrator for Itexamworld .com. The network contains an ISA Server 2004 computer named ISA1 and a Windows Server 2003 computer named Itexamworld 1. Both ISA1 and Itexamworld 1 are members of an Active Directory domain named Itexamworld .com
You configure ISA1 to generate daily reports and automatically publish them to a shared folder named DailyReports on Itexamworld 1. You create an account named Itexamworld \IsaReports. You configure ISA to create reports in the security context
of the Itexamworld \IsaReports account.
The current permissions on the DailyReports folder are shown in the following table.

Group or user name	Allow permissions
Itexamworld 1\Administrators	Full Control
System	Full Control
	Read
Itexamworld \Manageers	List Folder Contents
	Read & Execute
Itexamworld \IsaReports	Full Control

You need to configure the minimum NTFS permissions on the DailyReports folder.
What should you do?

A. Change the allowed permissions for the system object from Full Control to Modify.
B. Change the allowed permissions for the Itexamworld \IsaReports object from Full Control to Read.
C. Change the allowed permissions for the Itexamworld \IsaReports object from Full Control to Write.
D. Change the allowed permissions for the system object from Full Control to Read and Write.
Answer: C
Explanation:
Reports are collections of information generated from data collected from the ISA Server log files. You can use the reporting feature to summarize and analyze common usage patterns such as:
* Internet users and the Web sites that are accessed.
* The protocols and applications most often used.
* General traffic patterns.
* The cache hit ratio.
You can also use reports to monitor the security of your network, such as attempts to

access internal resources or the number of connections to a published server. You can generate a report immediately or you can schedule reports to generate on a recurring basis. The report can include daily, weekly, monthly, or yearly data.
The Microsoft ISA Server Job Scheduler service must be running to create a report and if you publish the report to a shared folder, be sure to supply credentials that will be used by the reporting engine for publishing. These credentials should have write permissions in the specified folder. To allow others to view the published report, give them read permissions to that folder. In this scenario we are using the Itexamworld \IsaReports account, therefore we should remove the FULL Control permissions and change it to write permissions.