Microsoft

Exam 70-299

Implementing and Administering Security in a Microsoft Windows Server 2003 Network

Version: 4.2

[Total Questions: 56]

Question No : 1 HOTSPOT

You are a security administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003.

Your company uses the Internet to sell products. Customers place and view the status of orders by using a Web application named App1. App1 is hosted on a Windows Server 2003 computer that runs IIS. Users access App1 by using various Web browsers. You configure SSL for connections to App1.

The company's written security policy states the following requirements:

All users must enter a user name and password when they access App1.

All users must use the same authentication method.

All users must use credentials in the company's domain.

You need to configure IIS to support the required authentication.

What should you do?

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

Answer:

Question No : 2

You are a security administrator for your company. The network consists of a perimeter network that is configured as shown in the exhibit. (Click the Exhibit button.)

All computers in the perimeter network run Windows Server 2003. The company's written security policy states the following:

All computers must pass a security inspection before they are placed in the perimeter network.

Only computers that pass inspection are permitted to communicate with firewalls or other computers that pass inspection.

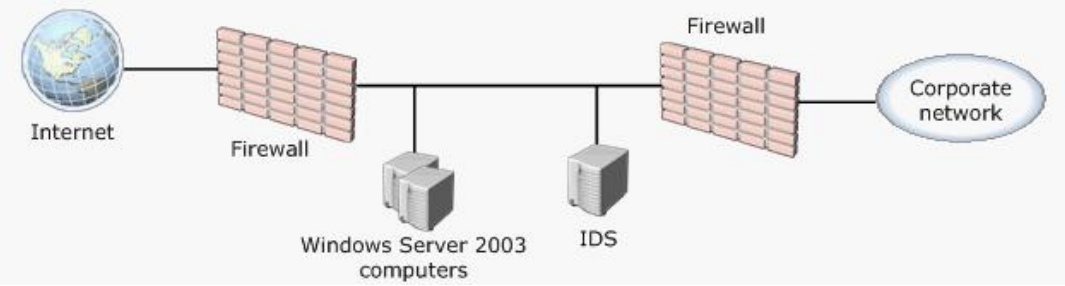
All communication in the perimeter network is inspected by a network-based intrusion-detection system (IDS).

Communication between computers in the perimeter network must use the strongest possible authentication methods.

You decide to deploy IPSec in the perimeter network to enforce the written security policy. You enable IPSec on the firewall computers.

You need to plan IPSec configuration for the Windows Server 2003 computers so that it meets the written security policy.

Which three actions should you perform to configure IPSec? (Each correct answer presents part of the solution. Choose three.)



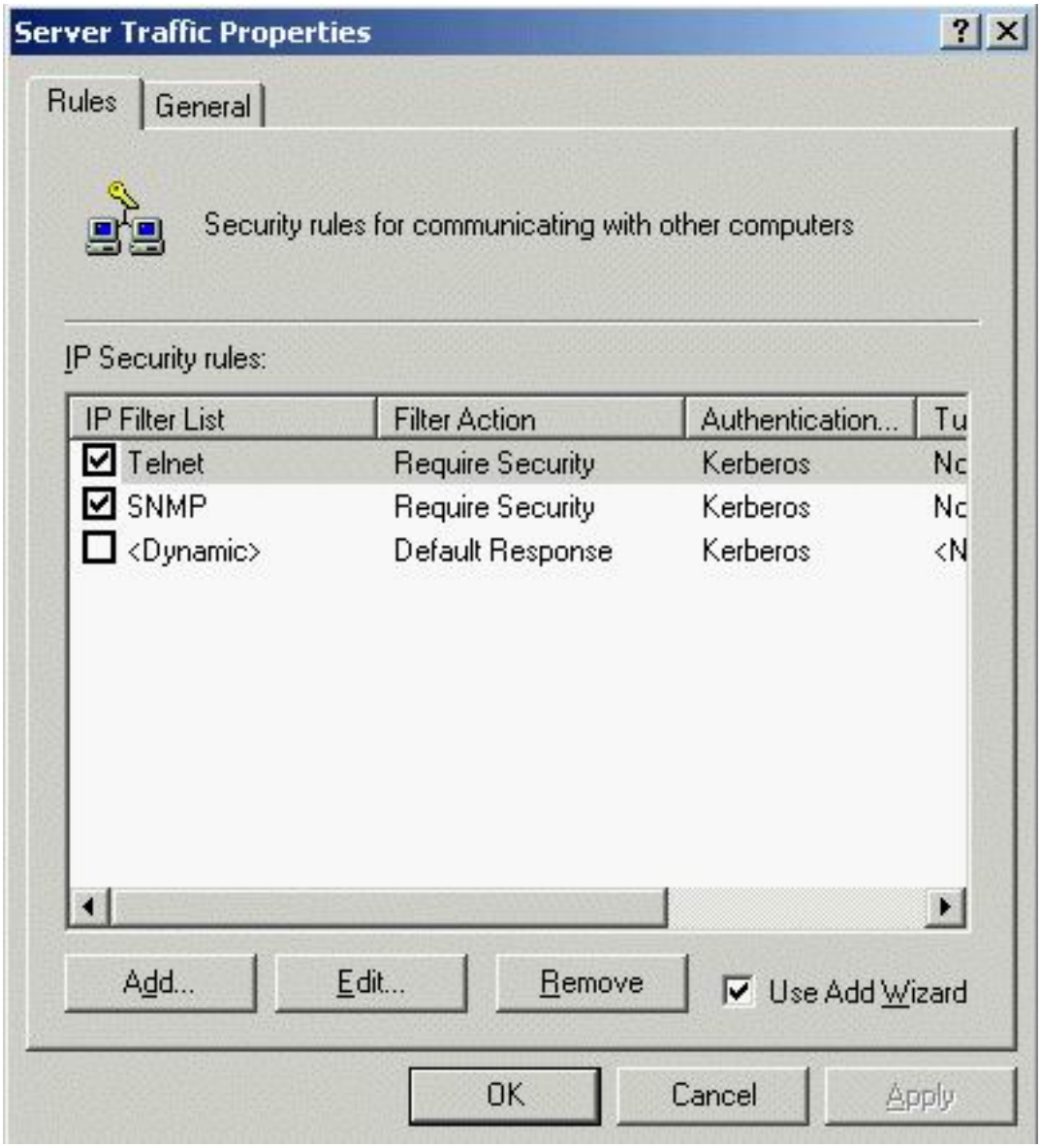
A. Use shared secret authentication.
B. Configure tunnel mode.
C. Enable Encapsulating Security Payload (ESP).
D. Enable Authentication Header (AH).
E. Use Kerberos authentication.
F. Configure transport mode.
G. Use certificate-based authentication.

Answer: D,E,F

Question No : 3

You are the security administrator of your network. The network consists of an Active Directory domain. All computers on the network are in the domain. The domain controllers and file servers on the network run Windows Server 2003. The client computers run Windows XP Professional. The file servers use a custom IPSec policy named Server Traffic. The Server Traffic policy contains rules to encrypt Telnet and SNMP traffic, as shown in the exhibit. (Click the Exhibit button.) All client computers use the Client (Respond

Only) IPSec policy. The default exemptions to IPSec filtering are disabled on the client computer. You want to configure the network so that Telnet, SNMP, and Kerberos traffic is encrypted by IPSec. You do not want to encrypt other network protocols. What should you do? (Each correct answer presents part of the solution. Choose two.)



A. On the client computers, enable the default exemptions to IPSec filtering.
B. Configure the rules in the Server Traffic policy to use an authentication method other than Kerberos.
C. On the file servers, enable the default exemptions to IPSec filtering.
D. Add a new rule to the Server Traffic policy to encrypt Kerberos traffic.
E. On the file servers, configure the IPSec policy in the local computer policy to encrypt Kerberos traffic.
F. Configure the Server Traffic policy to enable the Default Response rule.

Answer: B,D

Question No : 4

You are a security administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. All client computers run Windows XP Professional. Users are in the marketing, sales, or production department. A high-performance color print device named ColorPrinter1 is attached to a server named Server1. ColorPrinter1 is shared by the users in the marketing department. Only users in the marketing department are permitted to print documents on ColorPrinter1. Melanie is a user in the marketing department. Melanie is responsible for ensuring that print jobs on ColorPrinter1 print properly. She is also responsible for replacing paper and for general print device maintenance. Melanie is not permitted to modify the printer itself. You need to configure permissions for ColorPrinter1. You create a global group named Marketing. You add all marketing users to the Marketing global group. What else should you do?

A. Assign the global group the Allow - Print permission for ColorPrinter1. Create a local group on Server1. Add Melanie to the local group. Assign the local group the Allow - Manage Printers permission for ColorPrinter1.
B. Add the global group to a local group on Server1. Assign the local group the Allow - Manage Documents permission for ColorPrinter1. Assign Melanie the Allow - Manage Printers permission for ColorPrinter1.
C. Assign the global group the Allow - Manage Documents permission for ColorPrinter1. Assign Melanie the Allow - Manage Printers permission for ColorPrinter1.
D. Add the global group to a local group on Server1. Assign the local group the Allow - Print permission for ColorPrinter1. Create another local group on Server1. Add Melanie to the second local group. Assign the second local group the Allow - Manage Documents permission for ColorPrinter1.

Answer: D

Question No : 5

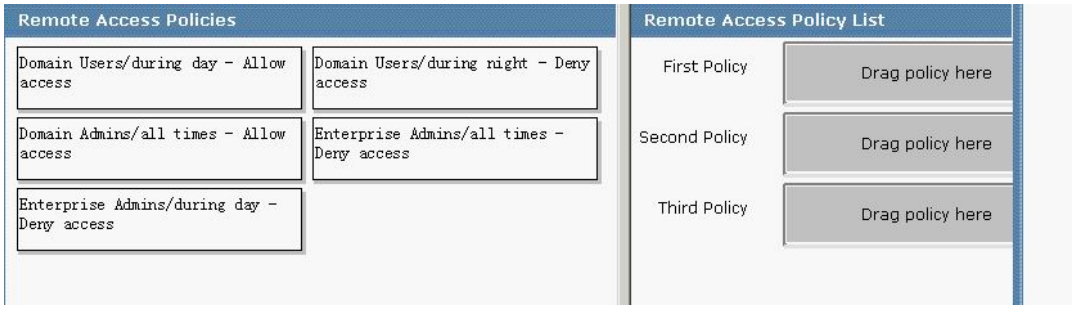
You are a security administrator for your company. The network consists of a single Active Directory domain. All servers run Windows 2003 Server. All client computers run Windows XP Professional. All computers are configured to use Automatic Updates to install updates without user intervention. Updates are scheduled to occur during off-peak hours. During a security audit, you notice some client computers are not receiving updates on a regular basis. You verify that Automatic Updates is running on all client computers, and you verify that users cannot modify the Automatic Updates settings. You need to ensure that computers on your network receive all updates. What should you do?

A. Disable the Specify intranet Microsoft update service location setting.
B. Enable the Reschedule Automatic Updates scheduled installations setting.
C. Enable the No auto-restart for scheduled Automatic Updates installations setting.
D. Enable the Remove access to use all Windows Update features setting.

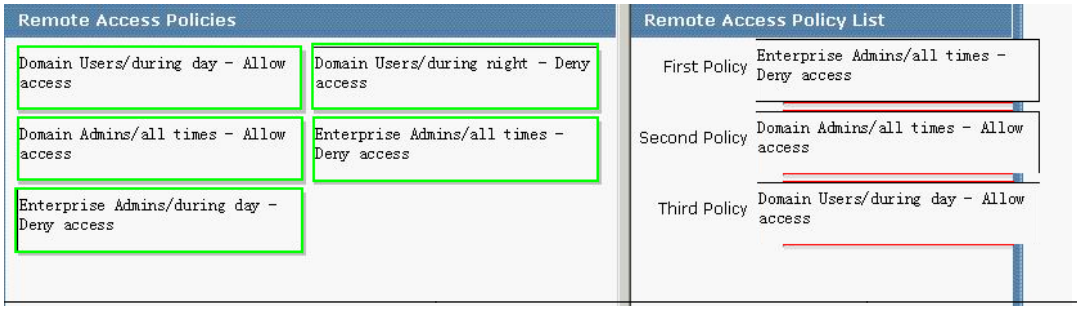
Answer: B

Question No : 6 DRAG DROP

You are a security administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. You plan to deploy remote access to the network for users that work from home. The company's written security policy states the following remote access requirements: Users are allowed to use remote access during the day only. Enterprise Admins are never allowed to use remote access. Domain Admins are always allowed to use remote access. A user who is a member of both the Enterprise Admins group and the Domain Admins group is not allowed to use remote access. You configure and enable Routing and Remote Access on a member server named Server1. You delete the predefined remote access policies. The remote access permission for all user accounts in the domain is set to use remote access policies. You need to ensure that the remote access policies on Server1 comply with the written security policy. What should you do? To answer, drag the remote access policy that should appear first in the remote access policy list to the First Policy box. Continue dragging the appropriate remote access policies to the corresponding numbered boxes until you list all required policies in the correct order. You might not need to use all numbered boxes.



Answer:



Question No : 7

You are a security administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. All client computers run Windows XP Professional. You manage the network by using a combination of Group Policy objects (GPOs) and scripts. File names for scripts have the .vbs file name extension. Scripts are stored in a shared folder named Scripts on a server named Server1. Users report that they accidentally run scripts that are received through e-mail and the Internet. They further report that these scripts cause problems with their client computers and often delete or change files. You discover that these scripts have .wsh, .wsf, .vbs, or .vbe file name extensions. You decide to use software restriction policies to prevent the use of unauthorized scripts. You need to configure a software restriction policy for your network. You want to achieve this goal without affecting management of your network. Which three rules should you include in your software restriction policy? (Each correct answer presents part of the solution. Choose three.)

A. a trusted sites rule that disallows the Internet zone
B. a path rule that disallows *.ws? files
C. a path rule that allows \\server1\scripts*.vb? files
D. a path rule that disallows *.vb? files
E. a trusted sites rule that allows the local intranet zone

Answer: B,C,D

Explanation:

Software Restriction Policy
By using the software restriction policy, you allow unknown code, which might contain viruses or code that conflicts with currently installed programs, to run only in a constrained environment (often called a sandbox) where it is disallowed from accessing any security-sensitive user privileges. For example, an e-mail attachment that contains a worm would be prohibited from automatically accessing your address book and therefore could not propagate itself. If the e-mail attachment contained a virus, the software restriction policy would restrict its ability to damage your system because it would be allowed to run only in a constrained environment.

The software restriction policy depends on assigning trust levels to the code that can run on a system. Currently, two trust levels exist: Unrestricted and Disallowed. Code that has an Unrestricted trust level is given unrestricted access to the user's privileges, so this trust level should be applied only to fully trusted code. Code with a Disallowed trust level is

disallowedfrom accessing any security-sensitive user privileges and can run only in a sandbox so that Unrestricted code cannot load the Disallowed code into its address space.

Configuring the software restriction policy for a system is done through the Local Security Policy administrative tool, while the restriction policy configuration of individual COM+ applications is done either programmatically or through the Component Services administrative tool. If the restriction policy trust level is not specified for a COM+ application, the systemwide settings are used to determine the application's trust level.

HOW TO: Use Software Restriction Policies in Windows Server 2003
SUMMARY
This article describes how to use software restriction policies in Windows Server 2003. When you use software restriction policies, you can identify and specify the software that is allowed to run so that you can protect your computer environment from untrusted code. When you use software restriction policies, you can define a default security level of Unrestricted or Disallowed for a Group Policy object (GPO) so that software is either allowed or not allowed to run by default. To create exceptions to this default security level, you can create rules for specific software. You can create the following types of rules:
Hash rules
Certificate rules
Path rules
Internet zone rules

How to Create a Path Rule
Click Start, click Run, type mmc, and then click OK.
Open Software Restriction Policies.
In either the console tree or the details pane, right-click Additional Rules, and then click New Path Rule.
In the Path box, type a path or click Browse to find a file or folder.
In the Security level box, click either Disallowed or Unrestricted.
In the Description box, type a description for this rule, and then click OK.IMPORTANT: On certain folders, such as the Windows folder, setting the security level to Disallowed can adversely affect the operation of your operating system. Make sure that you do not disallow a crucial component of the operating system or one of its dependent programs.
NOTES:
You may have to create a new software restriction policy setting for this GPO if you have not already done so.
If you create a path rule for a program with a security level of Disallowed, a user can still run the software by copying it to another location.
The wildcard characters that are supported by the path rule are the asterisk (*) and the