



70-299

**Implementing and Administering Security in a Microsoft
Windows Server 2003 Network**

Q&A

DEMO Version

Important Note Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website.

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

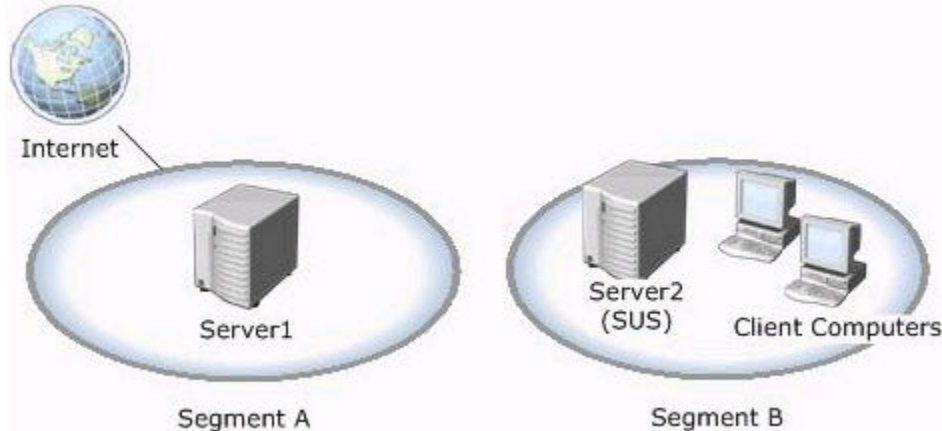
Technical and Support Team
Chinatag LLC.

A	Implementing, Managing, and Troubleshooting Security Policies
B	Implementing, Managing, and Troubleshooting Patch Management Infrastructure
C	Implementing, Managing, and Troubleshooting Security for Network Communications
D	Planning, Configuring, and Troubleshooting Authentication, Authorization, and PKI

Relevant objective of each question is mentioned along with question number.

Question: 1. (C)

You are the security administrator for Company. The network consists of two segments named Segment A and Segment B. The client computers on the network run Windows XP Professional. The servers run Windows Server 2003. Segment A contains a single server named Server1. Segment B contains all other computers, including a server named Server2. Company's written security policy states that Segment B must not be connected to the Internet. Segment A is allowed to connect to the Internet. There is no network connection between Segment A and Segment B. You can copy files from Segment A to Segment B only by using a CD-ROM to transport the files between the two segments. The network topology is displayed in the exhibit.



You are planning a patch management infrastructure. On Segment B, you install Software Update Services (SUS) on Server2. You configure Automatic Updates on all computers in Segment B to use <http://Server2> and to install security patches. You need to ensure that all computers in Segment B automatically install security patches. What should you do?

- A. Install SUS on Server1.
Periodically copy the files in the Content folder and in the SUS root folder from Server1 to Server2.
- B. Install SUS on Server1.
Periodically copy the files in the Content folder from Server1 to Server2. Copy the Approveditems.txt file from Server1 to the Windows folder on Server2.
- C. On Server1, periodically connect to the Microsoft Windows Update Catalog Web site and download new security patches. Copy the files to the Content folder on Server2.
- D. On Server1, configure Automatic Updates to use the URL of the Microsoft Windows Update Web site. Periodically copy the downloaded files and the Mssecure.xml file to the Content folder on Server2.

Answer: A

Explanation:

B – You must copy all items in the Content and SUS root folder.

C – This is possible, but you would have to install the patches manually.

D – Turning on AU would update Server1 does not provide files for Server2. The MBSA uses an XML-based catalog file, MSSecure.xml, to determine the security updates that are available. The catalog file is compressed and is stored in the MSSecure.cab file.

If SUS is used to approve updates, it retrieves the Approveditems.txt file from the root of the IIS/SUS default website (<http://server2>) not the Windows folder.

If you do not install SUS on Server1 there will be no Content folder (distribution point) on Server1.

Automatic Updates should not be turned on, on the SUS servers.

SUS is a server component that, when installed on a server running Windows 2000, allows small and medium enterprises to bring critical updates from Windows Update inside their firewalls to distribute to Windows 2000 and Windows XP computers. The same Automatic Updates component that can direct Windows 2000 and Windows XP computers to Windows Update can be directed to a SUS server inside your firewall to install critical updates.

Automatic Updates retrieves all critical updates and Microsoft Security Response Center security updates that are classified as moderate or important.

Automatic Updates scans only for critical updates, but if its server that runs SUS contains updates other than critical ones, Automatic Updates receives and applies those as well. SUS receives critical and moderate security updates.

Creating Distribution Points When you install a server that runs SUS, a distribution point is created on that server. When you synchronize the server with a parent server or with an external Web site, all the content on the Web site is downloaded to the distribution point. If new updates are downloaded, this distribution point is updated during every synchronization. During Setup, the distribution point is created in a virtual root (Vroot) named /Content.

If you choose to maintain content on the public Web site instead of downloading the patches to the local server running SUS, this distribution point is empty except for the AUCatalog.cab file. AUCatalog.cab defines the updates that have been approved for deployment to clients.

You can also create a distribution point on a server that is not running SUS. Such a server must be running IIS 5.0 or later. You can download and test packages on servers running SUS, and then download approved and tested packages to distribution points for client access.

If your SUS design includes distribution points, perform the following tasks to create a distribution point:

1. Confirm that IIS is present.
2. Create a folder named \Content.
3. Copy all of the following items from the source server running SUS to the newly created \Content folder:
 - <root of the SUS Web site>\Aucatalog1.cab
 - <root of the SUS Web site>\Aurtf1.cab
 - <root of the SUS Web site>\approveditems.txt
 - All the files and folders under the \Content\cabs
4. Create an IIS Vroot called http://<Servername>/Content that points to the \content folder.

Question: 2. (B)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. Company's written security policy states that security patches must be manually installed on servers by administrators. You need to configure the network to comply with the written security policy. You need to maintain security patches by using the minimum amount of administrative effort. What should you do?

- A. Create a new organizational unit (OU) to contain all server computers.
Create a new Group Policy object (GPO) and link it to the OU. Configure the GPO to disable Automatic Updates. Allow only administrators to start Automatic Updates.
- B. Create a new organizational unit (OU) to contain all server computers. Create a new Group Policy object (GPO) and link it to the OU. Configure the GPO to automatically download updates and notify when they are ready to be installed.
- C. Create a new organizational unit (OU) named Admins to contain all administrators.
Create a second OU named Servers to contain all server computers. Create a new Group Policy object (GPO) and link it to the Admins OU. Configure the GPO to disable Automatic Updates.
- D. Modify the Default Domain Policy Group Policy object (GPO) to disable Windows

Update and to disable Automatic Updates. Create a new organizational unit (OU) named Admins. Place all administrator accounts in the Admins OU. Block GPO inheritance on the Admins OU.

Answer: B

Explanation:

A – Cannot be done using Network Neighborhood.

C – Scanning the finance subnet would report on all computers on the subnet, including non-finance computers.

D – This option again would scan all systems in the domain, not just the finance once. The scan should be done from an administrative machine, not a users' machine.

Objective: Implementing, Managing, and Troubleshooting Security for Network Communications

Sub-Objective: 3.4.1 Monitor IPsec policies by using IP Security Monitor.

1. Planning a Host Name Resolution Strategy MCSA/MCSE Self-Paced Training Kit (Exams 70-292 and 70-296): Upgrading Your Certification to Microsoft Windows Server 2003, Microsoft Press Chapter 7,

The correct syntax is `mbsacl /hf -i hosts.txt` syntax. The `-i` flag is used to scan one or more Internet Protocol (IP) addresses.

The `mbsacl /hf -fh hosts.txt`. The `-fh` flag causes the tool to scan the NetBIOS computer names specified in the named text file. You must specify one computer name on each line in the `.txt` file, up to a maximum of 256 names.

The `mbsacl /hf -r hosts.txt` syntax. The `-r` flag is used to specify a range of IP addresses to be scanned.

<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q320454&ID=KB;EN-US;Q320454&&FR=1>

Switches available with `/hf` flag

`mbsacl /hf [-h hostname] [-fh filename] [-i ipaddress] [-fip filename] [-r ipaddressrange] [-d domainname] [-n]`

`[-sus SUS server|SUS filename] [-b] [-fq filename] [-s 1] [-s 2] [-nosum] [-sum] [-z] [-v] [-history level] [-nvc]`

`[-o option] [-f filename] [-unicode] [-t] [-u username] [-p password] [-x] [-?]`

To Select Which Computer to Scan

`-h hostname` - Scans the named NetBIOS computer name. The default location is the local host. To scan multiple hosts, separate the host names with a comma (,).

`-fh filename` - Scans the NetBIOS computer names that are specified in the text file that you named. Specify one computer name on each line in the `.txt` file, to a maximum of 256 names.

`-i xxx.xxx.xxx.xxx` - Scans the named IP address. To scan multiple IP addresses, separate each IP address with a comma.

`-fip filename` - Scans the IP addresses that you specified in the text file that you named. Specify one IP address on each line in the `.txt` file, with a maximum of 256 IP addresses.

`-r xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx` - Scans a specified range of IP addresses.

Note You can use the previous switches in combination. For example, you can use a command-line with the following format: `mbsacl /hf -h hostname1,hostname2 -i xxx.xxx.xxx.xxx -fip ipaddresses.txt -r yyy.yyy.yyy.yyy-zzz.zzz.zzz.zzz`

`-d domainname` - Scans a specified domain.

`-n` - Scans all the computers on the local network. All computers from all domains in Network Neighborhood (or My Network Places) are scanned

Question: 3. (B)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The Company.com Active Directory domain contains 150 Windows Server 2003 computers and 7,500 Windows XP Professional client computers. The network is made up of 64 class C IP subnets that range from 172.16.0.0 through 172.16.63.0.

The finance department uses 135 computers on the 172.16.9.0 /24 IP subnet. This subnet also contains computers that belong to other departments in the company. All finance department computers are members of the Company.com Active Directory domain. You need to produce a report that identifies which Microsoft security patches are not installed on the computers in the finance department. The report must contain information about only the finance department computers. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. Run Mbsacl.exe on a finance department computer with the option to scan computers in the Network Neighborhood.
- B. Run Mbsacl.exe on a finance department computer with the option to scan computers by using a list of individual IP addresses on the finance department computers.
- C. Run Mbsacl.exe on a finance department computer with the option to scan computers on the finance department IP subnet.
- D. Run Mbsacl.exe on a finance department computer with the option to scan computers in the Company.com Active Directory domain.

Answer: B

Explanation:

Since there are non-accounting computers on the subnet, the scan needs to be performed by individual IP. Objective: Implementing, Managing, and Troubleshooting Security for Network Communications Sub-Objective: 3.4.1 Monitor IPsec policies by using IP Security Monitor.

1. Planning a Host Name Resolution Strategy

MCSA/MCSE Self-Paced Training Kit (Exams 70-292 and 70-296): Upgrading Your Certification to Microsoft Windows Server 2003, Microsoft Press Chapter 7,

The correct syntax is mbsacl /hf -fh hosts.txt. The -fh flag causes the tool to scan the NetBIOS computer names specified in the named text file. You must specify one computer name on each line in the .txt file, up to a maximum of 256 names. You should not use the mbsacl /hf -i hosts.txt syntax. The -i flag is used to scan one or more Internet Protocol (IP) addresses. You should not use the mbsacl /hf -r hosts.txt syntax. The -r flag is used to specify a range of IP addresses to be scanned. Switches available with /hf flag mbsacl /hf [-h hostname] [-fh filename] [-i ipaddress] [-fip filename] [-r ipaddressrange] [-d domainname] [-n] [-sus SUS server|SUS filename] [-b] [-fq filename] [-s 1] [-s 2] [-nosum] [-sum] [-z] [-v] [-history level] [-nvc] [-o option] [-f filename] [-unicode] [-t] [-u username] [-p password] [-x] [-?] To Select Which Computer to Scan -h hostname - Scans the named NetBIOS computer name. The default location is the local host. To scan multiple hosts, separate the host names with a comma (.). -fh filename - Scans the NetBIOS computer names that are specified in the text file that you named. Specify one computer name on each line in the .txt file, to a maximum of 256 names. -i xxx.xxx.xxx.xxx - Scans the named IP address. To scan multiple IP addresses, separate each IP address with a comma. -fip filename - Scans the IP addresses that you specified in the text file that you named. Specify one IP address on each line in the .txt file, with a maximum of 256 IP addresses. -r xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx - Scans a specified range of IP addresses. Note You can use the previous switches in combination. For example, you can use a command-line with the following format:mbsacl /hf -h hostname1,hostname2 -i xxx.xxx.xxx.xxx -fip ipaddresses.txt -r yyy.yyy.yyy.yyy-zzz.zzz.zzz.zzz -d domainname - Scans a specified domain. -n - Scans all the computers on the local network. All computers from all domains in Network Neighborhood (or My Network Places) are scanned

Reference:

Microsoft Baseline Security Analyzer (MBSA) version 1.2 is available, Microsoft Knowledge Base Article – 320454

Question: 4.(B)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional. Company has a main office and 150 branch offices located throughout the United States and Canada. The company does not use disk-imaging software. In the past, newly installed client computers were exploited by malicious Internet worms before you applied all security patches. You need to build and deploy client computers that will always have the least service packs, updates, and security patches. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

- A. Install the operating system on the computers by using the original installation media. Use Windows Update immediately after the installation to apply updates and security patches.
- B. Install the operating system on the computers by using the original installation media. Configure Automatic Updates to immediately install updates and security patches.
- C. Create slipstream installation media that has the latest service pack. Install the operating system from the slipstream installation media. Implement a Software Update Services (SUS) server to install approved updates and security patches on client computers.
- D. Create slipstream installation media that has the latest service pack and includes Microsoft Baseline Security Analyzer (MBSA). Install the operating system from the slipstream installation media. Run MBSA immediately after installing the operating system.

Answer: C**Explanation:**

A – This would allow for exploitation as the system is new and therefore unpatched and would have to download all patches.

B – This is the same as the aforementioned.

D – This does nothing to install patches. This is still a new install and a check just to see what patches are needed.

Objective: Implementing, Managing, and Troubleshooting Patch Management Infrastructure

Sub-Objective: 2.3.1 Deploy service packs and hotfixes on new servers and client computers.

Considerations include slipstreaming, custom scripts, and isolated installation or test networks.

Objective: Implementing, Managing, and Troubleshooting Patch Management Infrastructure

Sub-Objective: 2.3.2 Deploy service packs and hotfixes to existing client and server computers.

Question: 5.(B)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computers are members of the domain. Company has a main office and six branch offices. Each branch office is connected to the main office by a dedicated leased line. All offices are connected to the Internet. Each office contains multiple servers and hundreds of client computers. You are planning a security patch management infrastructure. You install a Software Update Services (SUS) server in the main office and in each branch office. You configure the main office SUS server to store updates locally. You need to ensure that all client computers automatically install the latest security patches. You want to minimize the network traffic on the leased lines between the offices and on the connections to the Internet. Which two actions should you perform?

(Each correct answer presents part of the solution. Choose two)

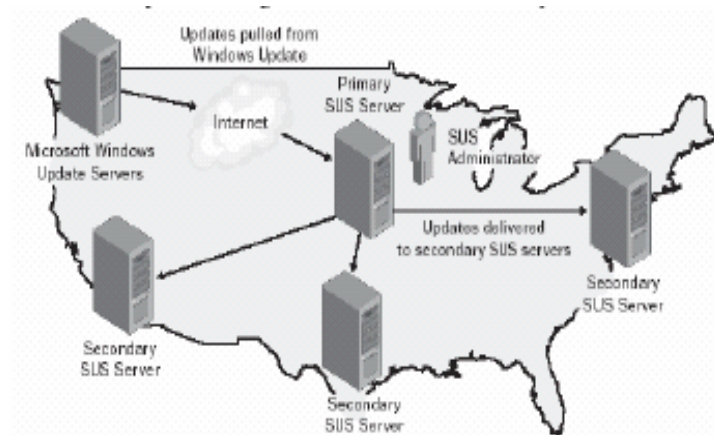
- A. Configure the branch office SUS servers to maintain updates on the Microsoft Windows Update servers.

- B. Configure Automatic Updates on the branch office SUS servers to use the main office SUS server.
- C. Configure the branch office SUS servers to obtain updates from the main office SUS server.
- D. Configure Automatic Updates on the client computers to use the SUS server in the local office.
- E. Configure Automatic Updates on the client computers to use the main office SUS server.

Answer: C, D

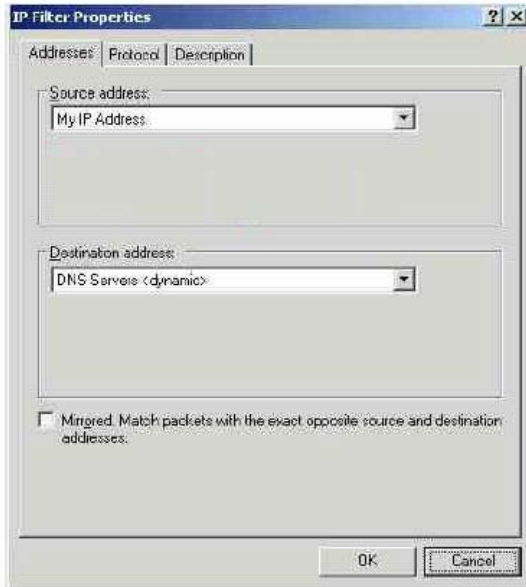
Explanation:

MCSA/MCSE Training Kit 70-299 5-20 Chapter: 5 Planning an Update Management Infrastructure Approval of updates using Software Update Services SUS is designed to be used in large organizations. Almost every aspect of the behavior can be customized. For example, the SUS server can download updates from Microsoft automatically, manually, or on a schedule specified by an administrator. SUS servers can be tiered as shown in Figure 5.4, with multiple SUS servers synchronizing updates between each other. This optimizes the use of your Internet connection by only requiring each update to be downloaded once for the entire organization. It also optimizes traffic on your wide area networks by allowing clients to download updates from a local SUS server.



Question: 6.(C)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The network contains Windows Server 2003 computers and Windows XP Professional client computers. The Active Directory domain consists of 10 Active Directory sites. Each Active Directory site contains a Windows Server 2003 computer that functions as a domain controller and a DNS server. A Windows Server 2003 computer named Company1 is a member of the Active Directory domain. Company1 is used to store confidential data in a Microsoft SQL Server 2000 database. You set up IP filters by using IPsec to control the types of inbound and outbound IP traffic that are allowed to and from Company1. After you configure the IP filters, you cannot resolve DNS names from Company1. The Addresses tab on the IP Filter Properties dialog box is shown in the exhibit.



This is the only rule in the IPsec policy that is relevant to DNS traffic. You need to enable Company1 to resolve DNS names. What should you do?

- A. Create an additional rule that allows DNS responses from the DNS servers to Company1.
- B. Change the Source address list to Any IP Address.
- C. Change the Destination Address list to A specific IP Subnet and type the IP subnet address That matches the IP subnet on Company1.
- D. Change the Destination address list to A specific IP Address and type an IP address of a DNS Server in the same IP subnet as Company1.

Answer: A

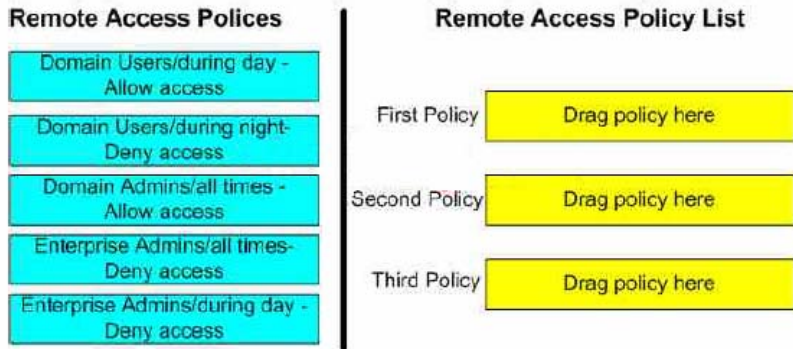
Question: 7.(C)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. You plan to deploy remote access to the network for users that work from home. Company's written security policy states the following remote access requirements:

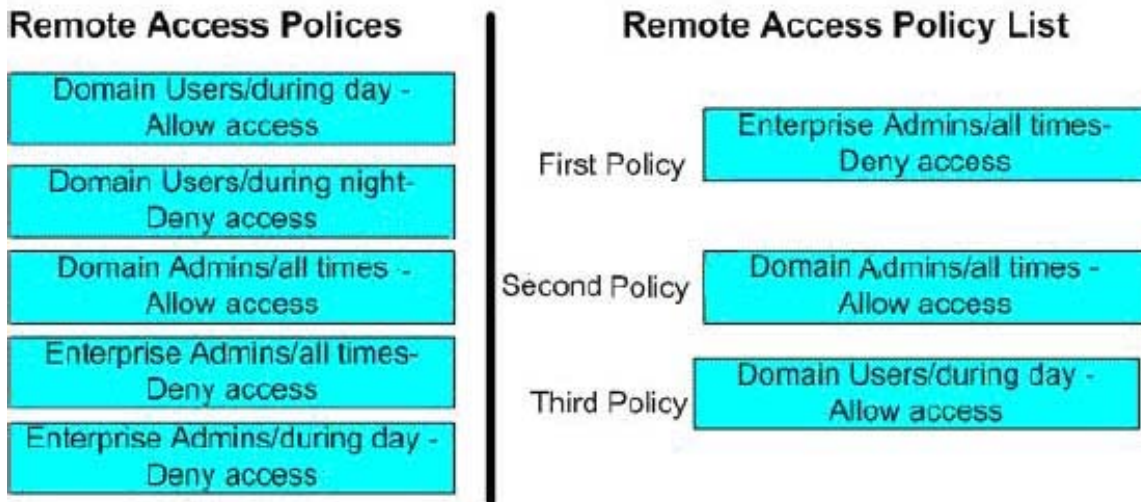
- A. Users are allowed to use remote access during the day only.
- B. Enterprise Admins are never allowed to use remote access.
- C. Domain Admins are always allowed to use remote access.
- D. A user who is a member of both the Enterprise Admins group and the Domains Admins group is not allowed to use remote access.

You configure and enable Routing and Remote Access on a member server named Company1. You delete the predefined remote access policies. The remote access permission for all user accounts in the domains is set to use remote access policies.

You need to ensure that the remote access policies on Company1 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 in the correct order. You might not need to use all numbered boxes.



Answer:



Explanation:

The remote access polices are tried in order. The more specific remote access policies are placed in order ahead of the more general remote access policies. If the first policy in the ordered list of remote access policies does not match the connection attempt, the next policy is tried. The most specific policy is Enterprise Admins/all times Deny acces, so it should be placed first. The next most specific policy is Domain Admins/all times Allow access. This policy should be placed second. The most general remote access policy is Domain Users/during day – Allow Access. This policy should be placed last. The reason for this is that everyone by default is part of the Domain Users group. If this was first or second, Enterprise Adminis would be allowed to connect and Domain Admins would only be able to connect during the day.

To process a connection attempt, the parameters of the connection attempt are compared to the user name, password, and dial-in properties of the user account and the configured remote access policies.

Some general characteristics of remote access connection attempt processing are:

If a connection attempt does not use a valid user name and password, then the connection attempt is denied.

If there are no configured policies, then all connection attempts are denied.

If the connection attempt does not match any of the remote access policies, then the connection attempt is denied.

If the remote access permission of the user account for the remote access user is set to Deny Access, the connection attempt is always denied for that remote access user.

The only time that a connection attempt is allowed is when it matches the conditions of a remote access policy, and remote access permission is enabled either through the dial-in properties of the user account or through the remote access permission of the remote access policy (assuming the user's remote access permission is set to control access through remote access policies), and the parameters of the connection attempt match or conform to the parameters and conditions of the dial-in properties of the user account and the remote access policy profile properties.

The figure depicts the specific processing of remote access connection attempts using the dial-in properties of the user account and remote access policies. Figure 7.15 assumes that the user name and password sent during the authentication process match a valid user account.

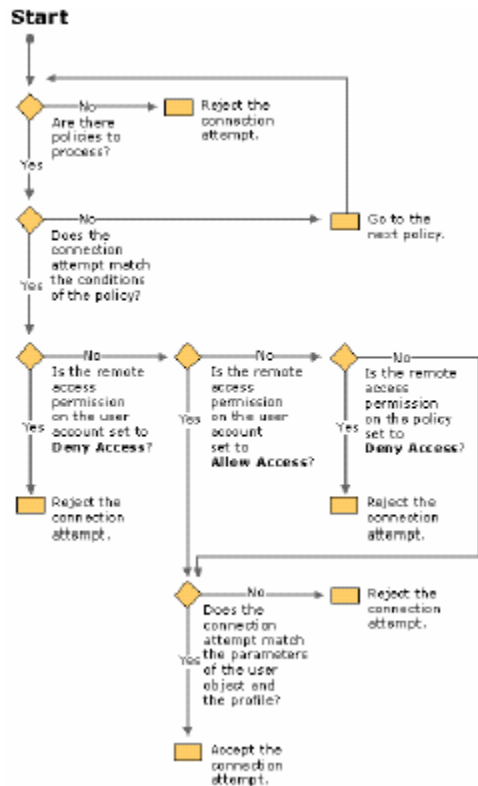


Figure Connection Attempt Processing
Accepting a connection attempt

When a user attempts a connection, the connection attempt is accepted or rejected, based on the following logic:

The first policy in the ordered list of remote access policies is checked. If there are no policies, reject the connection attempt.

If all conditions of the policy do not match the connection attempt, go to the next policy. If there are no more policies, reject the connection attempt.

If all conditions of the policy match the connection attempt, check the value of the Ignore-User-Dialin- Properties attribute.

If the Ignore-User-Dialin-Properties attribute is set to False, check the remote access permission setting for the user attempting the connection.

If Deny access is selected, reject the connection attempt.

If Allow access is selected, apply the user account and profile properties.

If the connection attempt does not match the settings of the user account and profile properties, reject the connection attempt.

If the connection attempt matches the settings of the user account and profile properties, accept the connection attempt.

If the remote access permission is not set to Allow access or Deny access, the remote access permission must be set to Control access through Remote Access Policy. Check the remote access permission setting of the policy.

If Deny remote access permission is selected, reject the connection attempt.

If Grant remote access permission is selected, apply the user account and profile properties.

If the connection attempt does not match the settings of the user account and profile properties, reject the connection attempt.

If the connection attempt matches the settings of the user account properties and profile, accept the connection attempt.

If the Ignore-User-Dialin-Properties attribute is set to True, check the remote access permission setting of the policy.

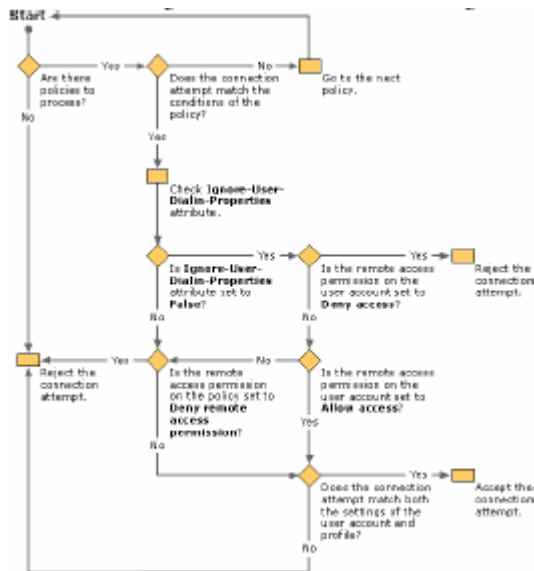
If Deny remote access permission is selected, reject the connection attempt.

If Grant remote access permission is selected, apply the profile properties.

If the connection attempt does not match the settings of the profile properties, reject the connection attempt.

If the connection attempt matches the settings of the profile properties, accept the connection attempt.

The following illustration shows the logic of remote access policies.



Notes

The profile and user account settings for the first matching policy are applied to the connection. If a connection does not match the profile or user account settings of the remote access policy, the additional remote access policies are not tried.

A connection attempt might not match any of the remote access policies. If this is the case, the connection attempt is rejected regardless of the remote access permission setting on the user account.

The remote access policies are tried in order. The more specific remote access policies are typically placed in order ahead of the more general remote access policies.

The Ignore-User-Dialin-Properties attribute is a new feature for Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition that allows you to ignore all of the dial-in properties of a user account. For more information, see New features.

You can configure IAS in Windows Server 2003, Standard Edition, with a maximum of 50 RADIUS clients and a maximum of 2 remote RADIUS server groups. You can define a RADIUS client using a fully qualified domain name or an IP address, but you cannot define groups of

RADIUS clients by specifying an IP address range. If the fully qualified domain name of a RADIUS client resolves to multiple IP addresses, the IAS server uses the first IP address returned in the DNS query. With IAS in Windows Server 2003, Enterprise Edition, and Windows Server 2003, Datacenter Edition, you can configure an unlimited number of RADIUS clients and remote RADIUS server groups. In addition, you can configure RADIUS clients by specifying an IP address range.

For examples of how different connection attempts are processed, see Remote access policies examples.

Question: 8.(C)

You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All client computers run Windows XP Professional. All servers run Windows Server 2003. All computers on the network are members of the domain. Traffic on the network is encrypted by IPSec. The domain contains a custom IPSec policy named Lan Security that applies to all computers in the domain. The Lan Security policy does not allow unsecured communication with non-IPSec-aware computers. Company's written security policy states that the configuration of the domain and the configuration of the Lan Security policy must not be changed. The domain contains a multihomed server named Company1. Company1 is connected to the company network, and Company1 is also connected to a test network. Currently, the Lan Security IPSec policy applies to the network traffic on both network adapters on Company1. You need to configure Company1 so that it communicates on the test network without IPSec security. Company1 must still use the Lan Security policy when it communicates on the company network. How should you configure Company1?

- A. Configure a packet filter for the network adapter on the test network to block the Internet Key Exchange (IKE) port.
- B. Configure the network adapter on the test network to disable IEEE 802.1x authentication.
- C. Configure the network adapter on the test network to enable TCP/IP filtering, and then permit all traffic.
- D. Use the netsh command to assign a persistent IPSec policy that permits all traffic on the Network adapter on the test network.
- E. Assign an IPSec policy in the local computer policy that permits all traffic on the network adapter on the test network.

Answer: D

Explanation:

Assigning IPSec Policies Locally Each computer running Windows Server 2003 has one local GPO, which is also known as the local computer policy. When this local GPO is used, Group Policy settings can be stored on individual computers regardless of whether they are members of an Active Directory domain. The local GPO can be overridden by GPOs assigned to sites, domains, or OUs in an Active Directory environment that have higher precedence. On a network without an Active Directory domain (that is, a domain that does not have a domain controller running Windows 2000 or Windows Server 2003), the local GPO settings determine IPSec behavior because they are not overridden by other GPOs. Local policy assignment is a way to enable IPSec for computers that are not members of a domain. You can also create and assign persistent IPSec policy, which secures a computer even if a local IPSec policy or an Active Directory-based IPSec policy cannot be applied.

This policy adds to or overrides the local or Active Directory policy, and remains in effect regardless of whether other policies are applied or not. Persistent IPSec policies enhance security by providing a secure transition from computer startup to IPSec policy enforcement. Persistent policy also provides backup security in the event of an IPSec policy corruption, or if errors occur during the application of local or domain-based IPSec policy. To configure persistent

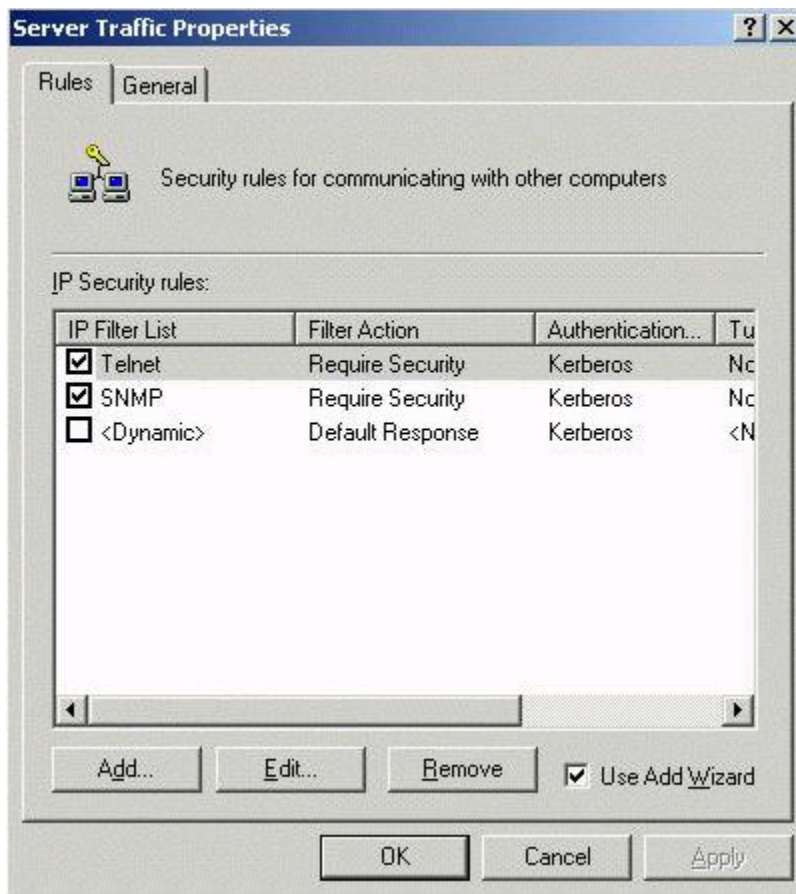
policies, you must use the `netsh ipsec static set store location=persistent` command. When designing persistent IPsec policy, it is important to consider the potential impact of persistent policy on remote management. If local or domain-based IPsec policy is not applied and the persistent IPsec policy is the only policy that is applied, attempts to remotely diagnose an issue might be blocked by the persistent IPsec policy. To allow for remote management in case troubleshooting is required, it is recommended that you create appropriate permit filters when configuring persistent IPsec policy.

Question: 9.(C)

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.



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. On the file servers, enable the default exemptions to IPsec filtering.

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

Answer: D, F

Question: 10.(C)

You are a security administrator for Company. Company consists of two divisions. One division is named Company Winery and is located in San Francisco. The other division is named Company Vineyard and is located in Paris. Each division is connected to the Internet by a 1.544 Mbps WAN connection. Company Winery consists of a single Active Directory forest named Companywinery.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Company Winery has a Microsoft SQL Server 2000 database that contains customer information. The SQL Server 2000 database is hosted on a Windows Server 2003 computer named Company1. Company Vineyard consists of a single Active Directory forest named Companyvineyard.com. All servers run Windows 2000 Server. All client computers run Windows 2000 Professional or Windows NT Workstation. All computers run the latest service packs.

To enable data replication, you configure a new Windows Server 2003 computer named Company2 in the Companyvineyard.com forest. You install SQL Server 2000 on Company2. Your database administrator configures the database on Company1 to replicate to Company2 every night. Management reports that a competitor acquired confidential customer data. You determine that the competitor intercepted customer data as it replicated from Company1 to Company2. You decide to use IPSec to protect customer data as it replicates.

You need to configure an IPSec policy to protect customer data as it replicates. What should you do?

- A. Configure the IPSec policy to use Authentication Header (AH) in transport mode with Kerberos authentication.
- B. Configure the IPSec policy to use Encapsulating Security Payload (ESP) with certificate-based authentication in tunnel mode.
- C. Configure the IPSec policy to use Authentication Header (AH) with certificate-based authentication in transport mode.
- D. Configure the IPSec policy to use Encapsulating Security Payload (ESP) with Kerberos authentication in tunnel mode.

Answer: B

Explanation:

IPSec can operate in two different modes: transport mode and tunnel mode. Typically, you should use transport mode to protect host-to-host communications. In transport mode, IPSec tunnels traffic starting at the transport layer, also known as layer 4. Therefore, IPSec in transport mode can encrypt the User Datagram Protocol/Transmission Control Protocol (UDP/TCP) protocol header and the original data, but the IP header itself cannot be protected. IPSec transports an application's data by adding an IPSec header and trailer to outgoing packets. Depending on the IPSec protocol used, the original contents of the outgoing packets will be encrypted. IPSec's position in the packet when functioning in transport mode is shown in Figure 8.1. The diagram shows IPSec using the ESP protocol. ESP is the most common of the two IPSec protocols

because it provides both authentication and encryption. When you protect traffic sent directly between two hosts, you will almost always use IPSec transport mode.

When you protect traffic between a host and a network, or between two networks, you must use IPSec tunnel mode. Although transport mode stores the UDP/TCP header and the application data between an IPSec header and trailer, tunnel mode stores the entire original packet. The IP header, including the source and destination addresses, must be stored within the IPSec packet because the traffic is destined for a computer other than the computer to which the IPSec connection was established. If hosts on two networks are communicating across the Internet and all clients are IPSec enabled, transport mode can be used to encrypt traffic between individual hosts, or tunnel mode can be used to encrypt all traffic sent between the two networks. Naturally, tunnel mode is more convenient because it doesn't require every host to have IPSec enabled—but which is more secure? Tunnel mode is more secure than transport mode, in theory. Use transport mode when you communicate with one computer, and use tunnel mode when you communicate with an entire network, so when the decision calls for encapsulating or tunneling the IP header, use tunnel mode.