GSNA Q&As

GIAC Systems and Network Auditor

Pass GIAC GSNA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gsna.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

You work as the Network Administrator for a company. You configure a Windows 2000-based computer as the Routing and Remote Access server, so that users can access the company\\'s network, remotely. You want to log a record of all the users who access the network by using Routing and Remote Access.

What will you do to log all the logon activities?

A. On the Routing and Remote Access server, enable log authentication requests in auditing, and define the path for the log file in Remote Access Logging.

B. On the Routing and Remote Access server, enable log authentication requests in Remote Access Logging.

C. On the Routing and Remote Access server, enable log authentication requests in auditing.

D. Do nothing as the Windows 2000-based Routing and Remote Access server automatically creates a log record for each connection attempt.

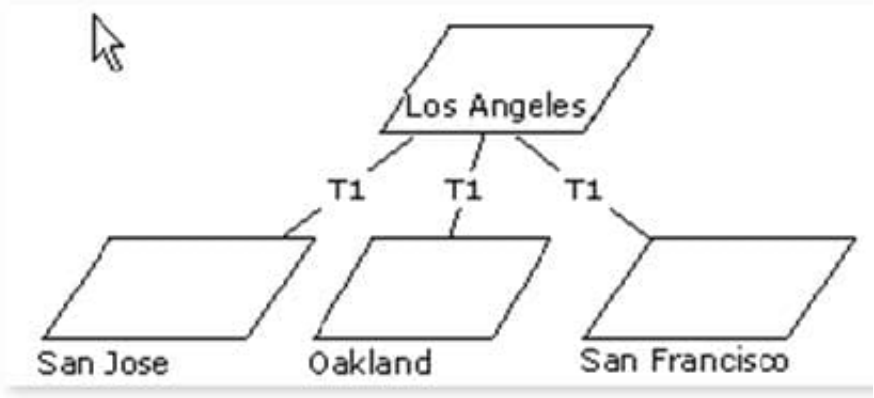
Correct Answer: B

The Routing and Remote Access service can log all the records of authentication and accounting information for connection attempts when Windows authentication or accounting is enabled. This can be done by enabling the log authentication requests in the properties of the RemoteAccess Logging folder, in the Routing and Remote Access snap-in, where you can configure the type of activity to log, i.e., accounting or authentication activity and log file settings. This information is stored in the form of a log file in \\'%SystemRoot%System32LogFiles\\' folder. For each authentication attempt, the name of the remote access policy, that either accepted or rejected the connection attempt, is recorded. The logged information is useful to track remote access usage, and authentication attempts.

QUESTION 2

DRAG DROP

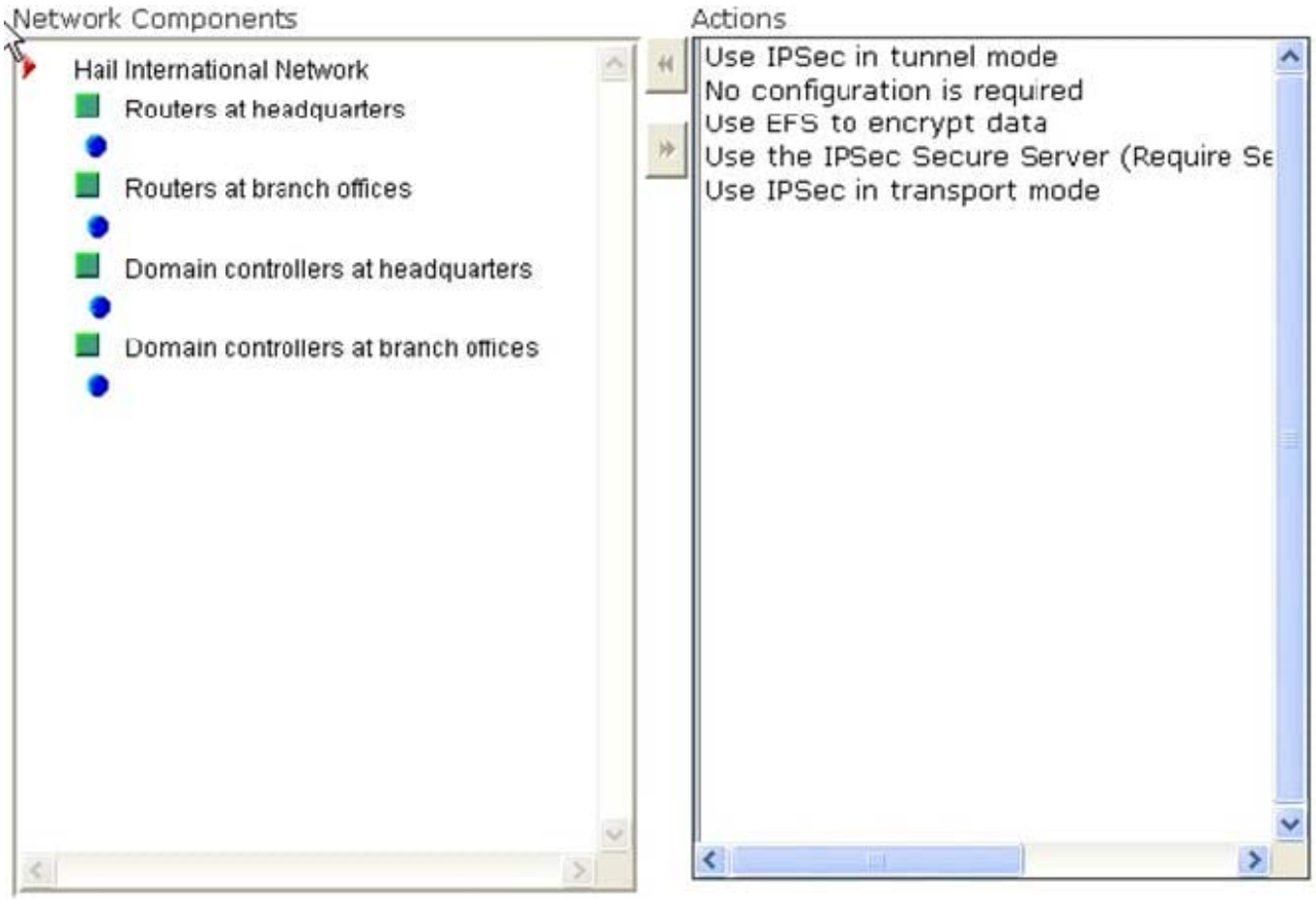
You work as a Network Administrator for Hail International. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. The company\\'s headquarters is located at Los Angeles. The company has branch offices in San Jose, Oakland, and San Francisco. All branch offices are connected to the headquarters by using T1 leased lines. The fragment of the company\\'s network is shown below:



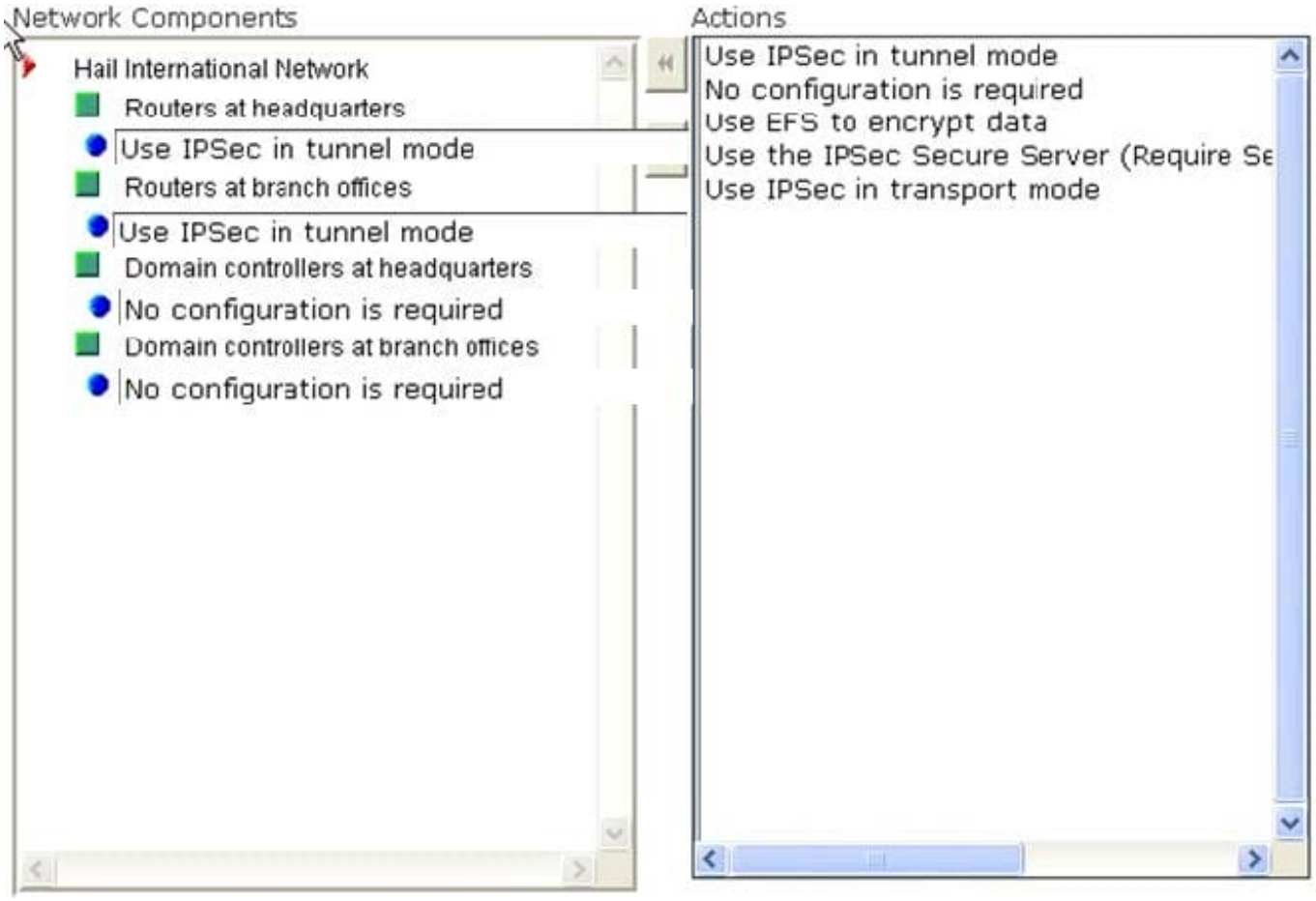
The routers are used to connect to the T1 lines to configure the private network. Each router at each location is a server that is running Microsoft Windows Server 2008. The management of the company wants to secure the WAN communication between the offices. The solution provided by you must not be expensive.

Choose and place the correct actions required to configure the necessary components of the network in order to accomplish the task.

Select and Place:



Correct Answer:



In order to accomplish the task, you will have to configure the routers at all locations to use IPSec in tunnel mode. Tunnel mode protects the WAN traffic. If you configure IPSec on routers, no security for the WAN communication is required on other servers and workstations.

QUESTION 3

You work as a Security manager for Qualoxizz Inc. Your company has number of network switches in the site network infrastructure. Which of the following actions will you perform to ensure the security of the switches in your company?

A. Open up all the unused management ports.

B. Set similar passwords for each management port.

C. Set long session timeouts.

D. Ignore usage of the default account settings.

Correct Answer: D

A switch with a management port using a default user account permits an attacker to intrude inside by making connections using one or more of the well-known default user accounts (e.g., administrator, root, security). Therefore, the default

account settings should not be used. Answer: A is incorrect. The unused management ports on a switch should always be blocked to prevent port scanning attacks from the attackers.

Answer: B is incorrect. Setting similar passwords on all management ports increases the vulnerability of password cracking. The matching passwords on all ports can be used by the attacker to break into all ports once the password of one of

the ports is known.

Answer: C is incorrect. Short timeout sessions should always be set to reduce the session period. If the connections to a management port on a switch do not have a timeout period set or have a large timeout period (greater than 9 minutes),

then the connections will be more available for an attacker to hijack them.

QUESTION 4

Which of the following tools can be used to perform tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing?

A. L0phtcrack

B. Obiwan

C. Cain

D. John the Ripper

Correct Answer: C

Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks:

1.

Dictionary attack

2.

Bruteforce attack

3.

Rainbow attack

4.

Hybrid attack Answer: A is incorrect. L0phtcrack is a tool which identifies and remediate security vulnerabilities that result from the use of weak or easily guessed passwords. It recovers Windows and Unix account passwords to access user and administrator accounts. Answer: D is incorrect. John the Ripper is a fast password cracking tool that is available for most versions of UNIX, Windows, DOS, BeOS, and Open VMS. It also supports Kerberos, AFS, and Windows NT/2000/ XP/2003 LM hashes. John the Ripper requires a user to have a copy of the password file. Answer: B is incorrect. Obiwan is a Web password cracking tool that is used to perform brute force and hybrid attacks. It is effective against HTTP connections for Web servers that allow unlimited failed login attempts by the user. Obiwan uses wordlists as well as alphanumeric characters as possible passwords.

QUESTION 5

Mark works as a Network Administrator for Infonet Inc. The company has a Windows 2000 Active Directory domain-based network. The domain contains one hundred Windows XP Professional client computers. Mark is deploying an 802.11 wireless LAN on the network. The wireless LAN will use Wired Equivalent Privacy (WEP) for all the connections. According to the company\\'s security policy, the client computers must be able to automatically connect to the wireless LAN. However, the unauthorized computers must not be allowed to connect to the wireless LAN and view the wireless network. Mark wants to configure all the wireless access points and client computers to act in accordance with the company\\'s security policy.

What will he do to accomplish this? (Choose three)

A. Configure the authentication type for the wireless LAN to Shared Key

B. On each client computer, add the SSID for the wireless LAN as the preferred network

C. Install a firewall software on each wireless access point

D. Disable SSID Broadcast and enable MAC address filtering on all wireless access points

E. Configure the authentication type for the wireless LAN to Open system

F. Broadcast SSID to connect to the access point (AP)

Correct Answer: ABD

To configure all the wireless access points and client computers to act in accordance with the company\\'s security policy, Mark will take the following actions:

1.

Configure the authentication type for the wireless LAN to Shared Key.

2.

Shared Key authentication provides access control.

3.

Disable SSID Broadcast and enable MAC address filtering on all the wireless access points.

4.

Disabling SSID Broadcast and enabling MAC address filtering will prevent unauthorized wireless client computers from connecting to the access point (AP).

5.

Only the computers with particular MAC addresses will be able to connect to the wireless access points.

6.

On each client computer, add the SSID for the wireless LAN as the preferred network. Answer: E is incorrect. Setting the authentication type for the wireless LAN to Open System will disable Wired Equivalent Privacy (WEP). This level of WEP will not provide security.

Latest GSNA Dumps GSNA Practice Test GSNA Braindumps