GSNA$^{\text{Q\&As}}$

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

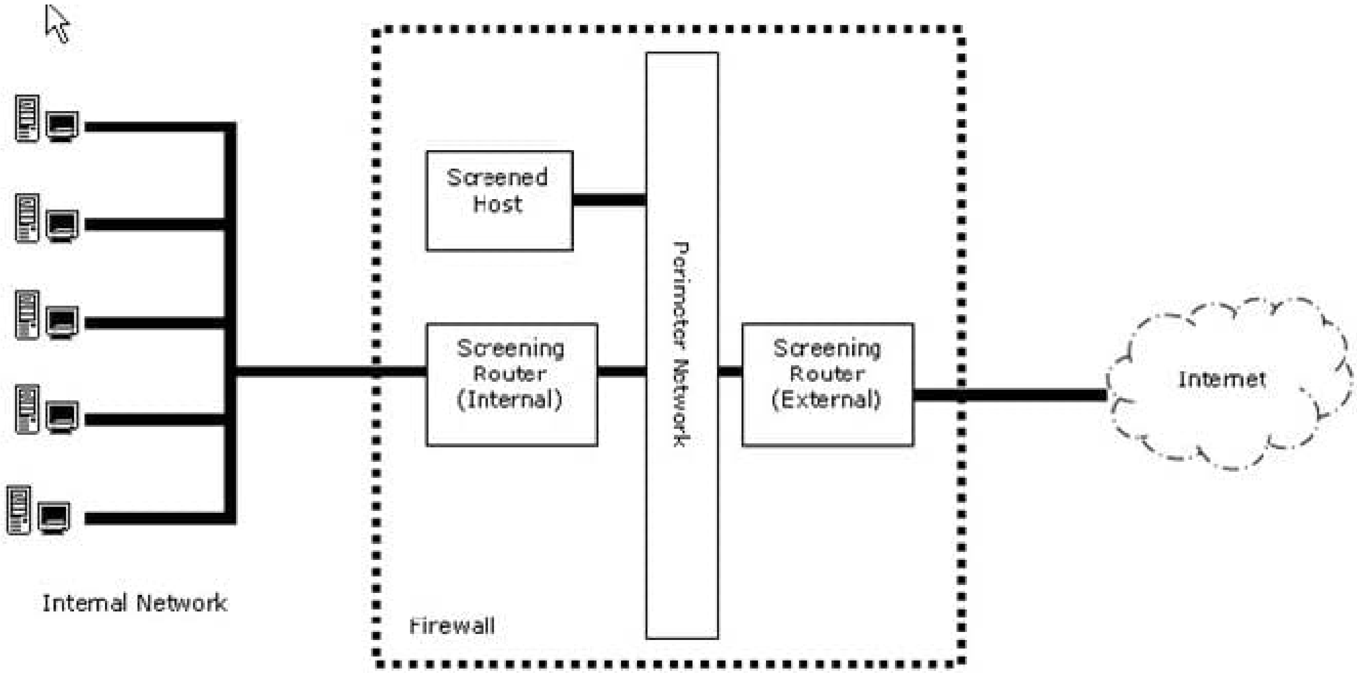
Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

HOTSPOT

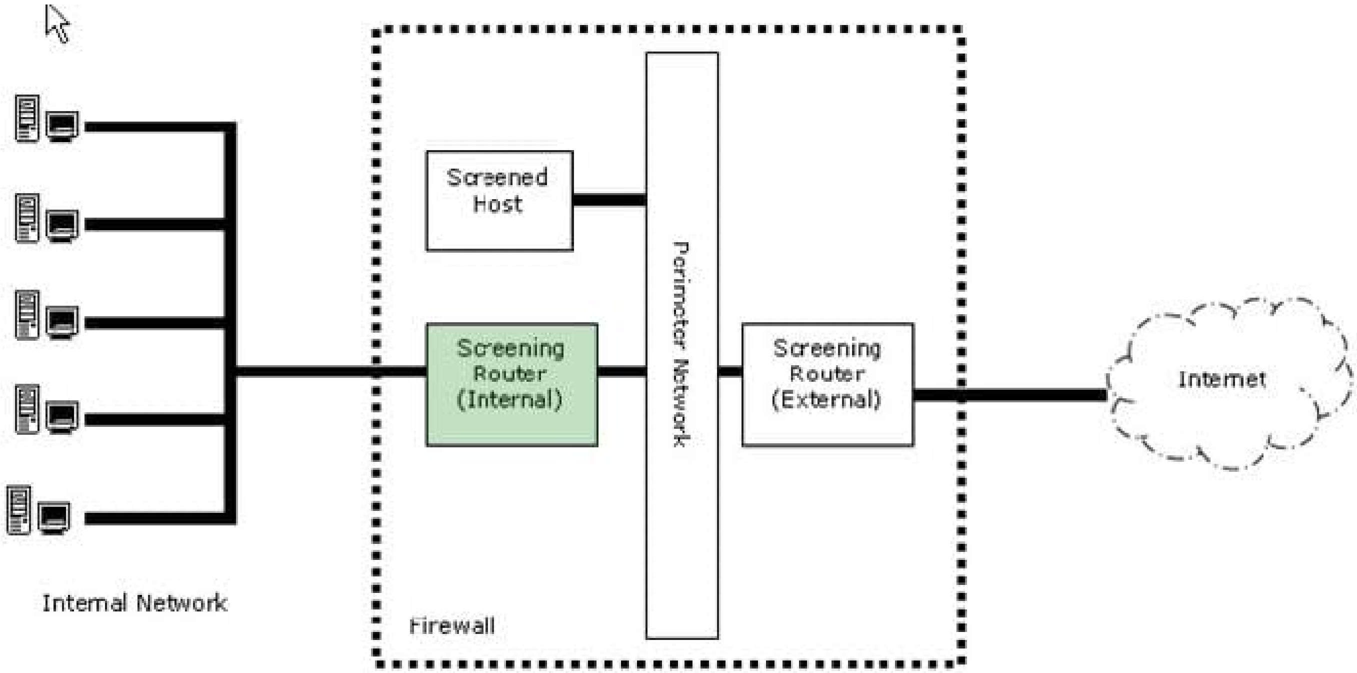
In the image of the Screened Host Firewall Architecture given below, select the element that is commonly known as the choke router.

Hot Area:



Screened Host Firewall Architecture

Correct Answer:



Screened Host Firewall Architecture

A choke router is an interior router present in the screened host firewall architecture. It is attached to the perimeter network and protects the internal network from the Internet and the perimeter net.

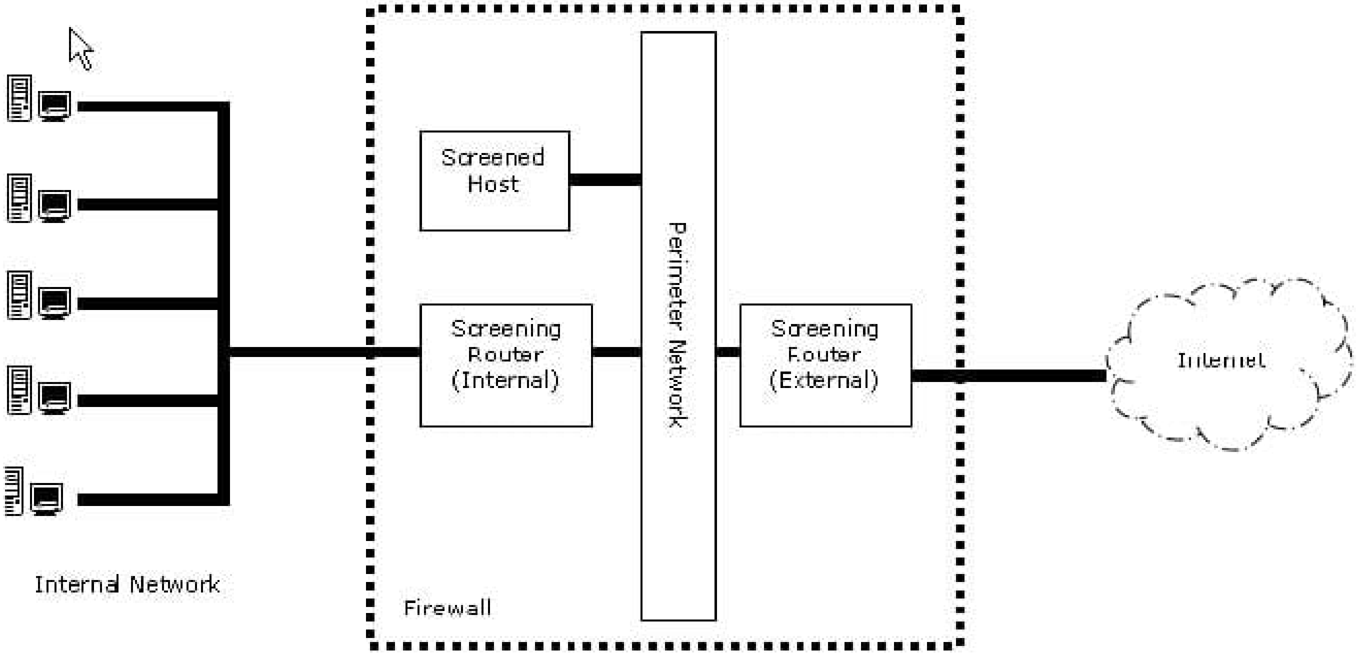
A choke router is basically employed for the job of packet filtering for the firewall. It is also used to provide access to selected services that are outbound from the internal net to the Internet. These services may include outgoing Telnet, FTP,

WAIS, Archie, Gopher, etc.

A Screened Host Firewall Architecture is used to provide services from a host that is attached only to the internal network by using a separate router. In this type of firewall architecture, the key security is provided by packet filtering.

The host exists in the internal network. The packet filtering on the screening router is configured in such a way that the bastion host is the only system in the internal network that is open to the Internet connections. If any external system tries

to access internal systems or services, then it will connect only to this host. The bastion host therefore needs to be at a high level of security.



Screened Host Firewall Architecture

QUESTION 2

Which of the following does an anti-virus program update regularly from its manufacturer\\'s Web site?

A. Hotfixes

B. Permissions

C. Service packs

D. Definition

Correct Answer: D

An anti-virus program updates the virus definition file regularly from the anti-virus manufacturer\\'s Web site. Antivirus (or anti-virus) software is used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware. Traditional antivirus software solutions run virus scanners on schedule, on demand and some run scans in real time. If a virus or malware is located, the suspect file is usually placed into a quarantine to terminate its chances of disrupting the system. Traditional antivirus solutions scan and compare against a publicized and regularly updated dictionary of malware otherwise known as a blacklist. Some antivirus solutions have additional options that employ a heuristic engine which further examines the file to see if it is behaving in a similar manner to previous examples of malware. A new technology utilized by a few antivirus solutions is whitelisting; this technology first checks if the file is trusted and only questions those that are not. With the addition of wisdom of crowds, antivirus solutions backup other antivirus techniques by harnessing the intelligence and advice of a community of trusted users to protect each other. Answer: C is incorrect. A service pack is a collection of Fixes and Patches in a single product. A service pack can be used to handle a large number of viruses and bugs or to update an operating system with advanced better capabilities. A service pack usually contains a number of file replacements. Answer: A is incorrect. Hotfix is a collection of files used by Microsoft for software updates that are released between major service pack releases. A hotfix is about a problem, occurring under specific circumstances, which cannot wait to be fixed till the next service pack release. Hotfixes are generally related to security problems. Hence, it is essential to fix these problems as soon as possible. Answer: B is incorrect. An anti-virus program does not update Permissions regularly from its manufacturer\\'s Web site.

QUESTION 3

You are concerned about attackers simply passing by your office, discovering your wireless network, and getting into your network via the wireless connection.

Which of the following are NOT steps in securing your wireless connection? (Choose two.)

A. Hardening the server OS

B. Using either WEP or WPA encryption

C. MAC filtering on the router

D. Strong password policies on workstations.

E. Not broadcasting SSID

Correct Answer: AD

Both hardening the server OS and using strong password policies on workstations are good ideas, but neither has anything to do with securing your wireless connection. Answer: B is incorrect. Using WEP or WPA is one of the most basic security steps in securing your wireless.

QUESTION 4

You work as a Security Administrator in Tech Perfect Inc. The company has a TCP/IP based network. The network has a vast majority of Cisco Systems routers and Cisco network switches. You want to take a snapshot of the router running configuration and archive running configuration of the router to persistent storage.

Which of the following steps will you take?

A. Secure the boot configuration

B. Restore an archived primary bootset

C. Verify the security of the bootset

D. Enable the image resilience

Correct Answer: A

In order to take a snapshot of the router running configuration and archive running configuration of the router to persistent storage, you should secure the boot configuration of the router using the secure boot- config command.

Answer: D is incorrect. You can enable the image resilience, if you want to secure the Cisco IOS image. Answer: C is incorrect. By verifying the security of bootset, you can examine whether or not the Cisco IOS Resilient Configuration is

enabled and the files in the bootset are secured. Answer: B is incorrect. By restoring an archived primary bootset, you can restore a primary bootset from a secure archive after an NVRAM has been erased or a disk has been formatted.

QUESTION 5

Which of the following backup sites takes the longest recovery time?

A. Mobile backup site

B. Warm site

C. Cold site

D. Hot site

Correct Answer: C

A cold backup site takes the longest recovery time. It is the most inexpensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. The lack of hardware contributes to the minimal startup costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster. Answer: D is incorrect. A hot site is a duplicate of the original site of the organization, with full computer systems as well as near- complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Ideally, a hot site will be up and running within a matter of hours or even less. Answer: A is incorrect. Although a mobile backup site provides rapid recovery, it does not provide full recovery in time. Hence, a hot site takes the shortest recovery time. Answer: B is incorrect. A warm site is, quite logically, a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.