GNSA$^{Q\&As}$

GIAC Systems and Network Auditor

Pass GIAC GNSA Exam with 100% Guarantee

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

https://www.leads4pass.com/gnsa.html

100% Passing Guarantee
100% Money Back Assurance

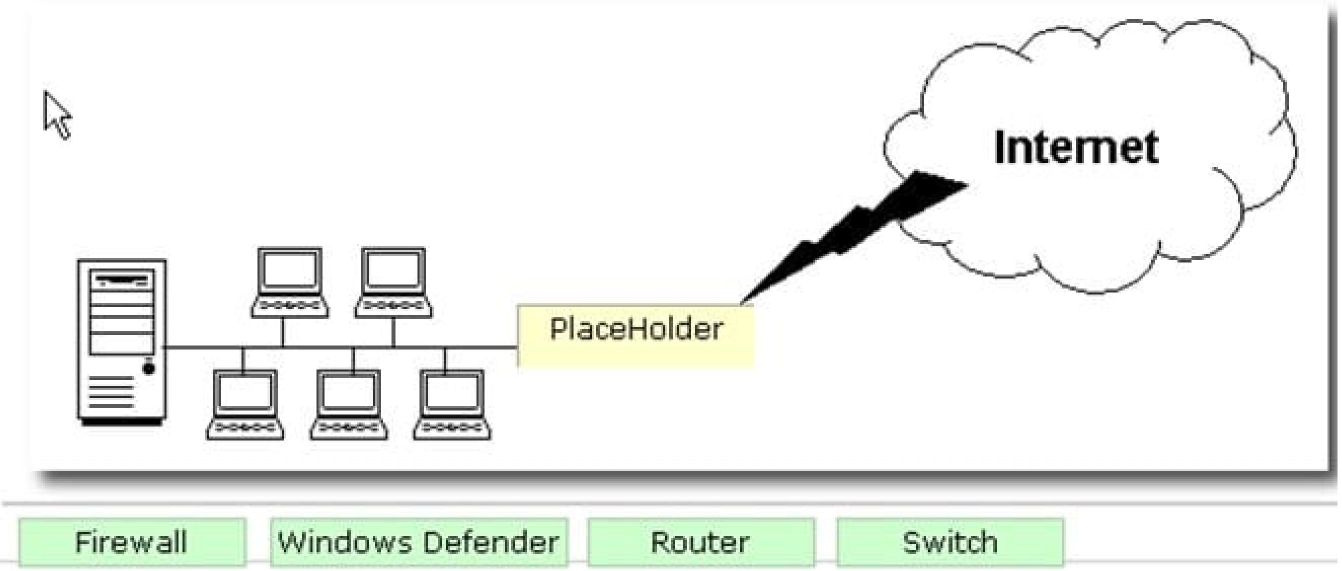
Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

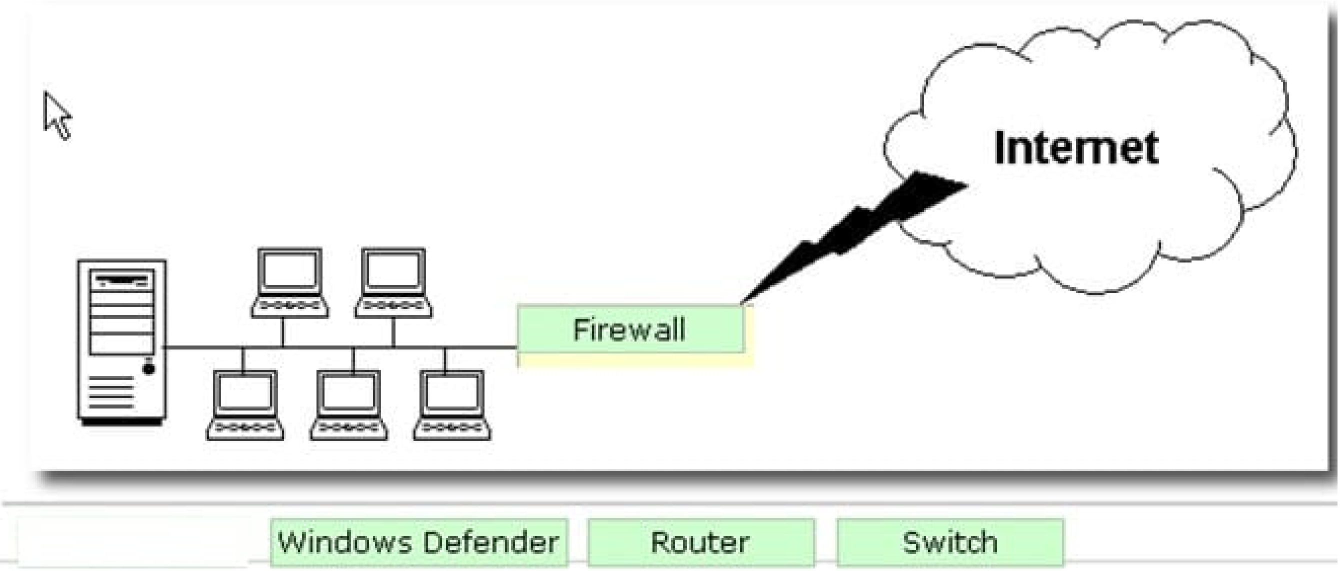
DRAG DROP

George works as a Network Administrator for Blue Soft Inc. The company uses Windows Vista operating system. The network of the company is continuously connected to the Internet. What will George use to protect the network of the company from intrusion?

Select and Place:



Correct Answer:



A firewall is a set of related programs configured to protect private networks connected to the Internet from intrusion. It is used to regulate the network traffic between different computer networks. It permits or denies the transmission of a network packet to its destination based on a set of rules. A firewall is often installed on a separate computer so that an incoming packet does not get into the network directly.

QUESTION 2

You work as a Network Administrator for Techpearl Inc. You are configuring the rules for the firewall of the company. You need to allow internal users to access secure external websites.

Which of the following firewall rules will you use to accomplish the task?

A. TCP 172.16.1.0/24 any any 80 HTTP permit

B. TCP 172.16.1.0/24 any any 25 SMTP permit

C. TCP 172.16.1.0/24 any any 80 HTTP deny

D. TCP 172.16.1.0/24 any any 443 HTTPs permit

Correct Answer: D

The TCP 172.16.1.0/24 any any 443 HTTPs permit rule is used to allow internal users to access secure external websites.

Answer: A is incorrect. The TCP 172.16.1.0/24 any any 80 HTTP permit rule is used to allow internal users to access external websites (secure and unsecure both). Answer: C is incorrect. The TCP 172.16.1.0/24 any any 80 HTTP deny rule is

used to deny internal users to access external websites. Answer: B is incorrect. The TCP 172.16.1.0/24 any any 25 SMTP permit rule is used to allow internal mail servers to deliver mails to external mail servers.

QUESTION 3

Data access auditing is a surveillance mechanism that watches over access to all sensitive information contained within the database.

What are the questions addressed in a perfect data access auditing solution?

A. Who accessed the data?

B. When was the data accessed?

C. For whom was the data accessed?

D. What was the SQL query that accessed the data?

Correct Answer: ABD

The perfect data access auditing solution would address the following six questions:

1. Who accessed the data? 2.

When was the data accessed?

3.Which computer program or client software was used to access the data?

4.From what location on the network was the data accessed?

5.What was the SQL query that accessed the data?

6.Was access to the data successfully done; and if so, how many rows of data were retrieved?

Answer: C is incorrect. In the perfect data access auditing solution, it cannot be determined for whom the data is being accessed. Only the person accessing the data can be identified.

QUESTION 4

Which of the following policies helps reduce the potential damage from the actions of one person?

A. CSA

B. Separation of duties

C. Internal audit

D. Risk assessment

Correct Answer: B

Separation of duties (SoD) is the concept of having more than one person required to complete a task. It is alternatively called segregation of duties or, in the political realm, separation of powers. Segregation of duties helps reduce the potential damage from the actions of one person. IS or end-user department should be organized in a way to achieve adequate separation of duties. According to ISACA\\'s Segregation of Duties Control matrix, some duties should not be combined into one position. This matrix is not an industry standard, just a general guideline suggesting which positions should be separated and which require compensating controls when combined. Answer: A is incorrect. Cisco Security Agent (CSA) is an endpoint intrusion prevention system. It is rule-based and examines system activity and network traffic, determining which behaviors are normal and which may indicate an attack. CSA uses a two or three-tier client-server architecture. The Management Center \\'MC\\' (or Management Console) contains the program logic; an MS SQL database backend is used to store alerts and configuration information; the MC and SQL database may be co-resident on the same system. The Agent is installed on the desktops and/or servers to be protected. The Agent communicates with the Management Center, sending logged events to the Management Center and receiving updates in rules when they occur. Answer: C is incorrect. Internal auditing is a profession and activity involved in helping organizations achieve their stated objectives. It does this by using a systematic methodology for analyzing business processes, procedures and activities with the goal of highlighting organizational problems and recommending solutions. Answer: D is incorrect. Risk assessment is a step in a risk management process.

QUESTION 5

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to allow direct access to the filesystems data structure.

Which of the following Unix commands can you use to accomplish the task?

A. debugfs

B. dosfsck

C. du

D. df

Correct Answer: A

In Unix, the debugfs command is used to allowdirect access to the filesystems data structure.

Answer: D is incorrect. In Unix, the df command shows the disk free space on one or more filesystems.

Answer: B is incorrect. In Unix, the dosfsck command checks and repairs MS-Dos filesystems.

Answer: C isincorrect. In Unix, the du command shows how much disk space a directory and all its files contain.