

# GNSA<sup>Q&As</sup>

GIAC Systems and Network Auditor

## Pass GIAC GNSA Exam with 100% Guarantee

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

<https://www.pass2lead.com/gnsa.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

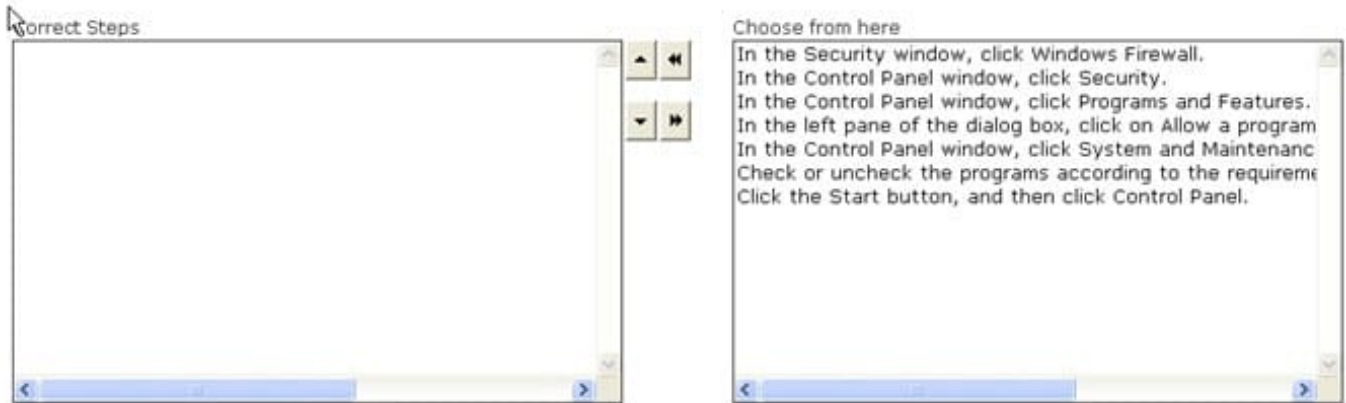


**QUESTION 1**

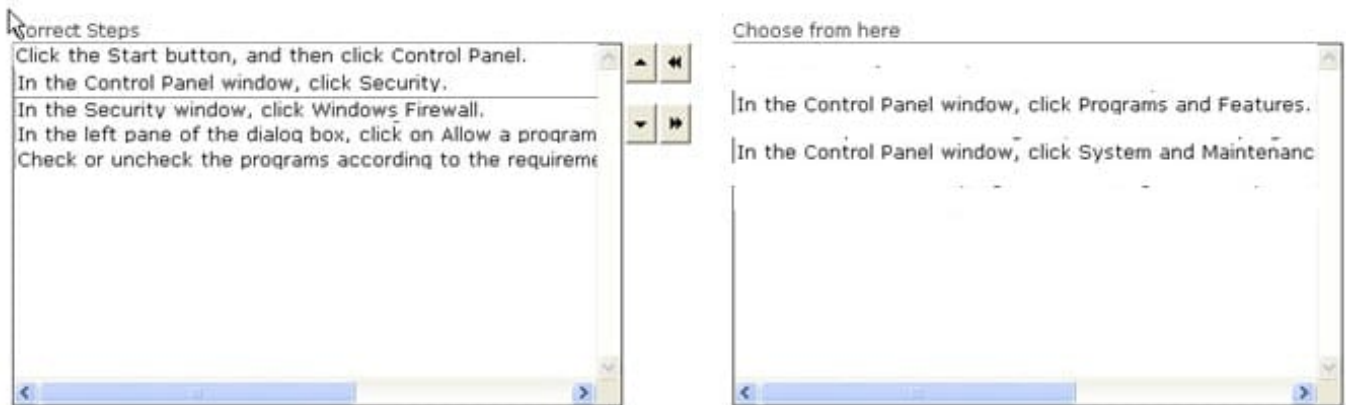
**DRAG DROP**

John works as a Network Administrator for Blue Well Inc. The company uses Windows Vista operating system. He wants to configure the firewall access for specific programs. What steps will he take to accomplish the task?

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**

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

- A. Incontrovertible
- B. Corroborating

C. Direct

D. Circumstantial

Correct Answer: D

Circumstantial evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person. Answer: B is incorrect. Corroborating evidence is evidence that tends to support a

proposition that is already supported by some evidence. Answer: A is incorrect. Incontrovertible evidence is a colloquial term for evidence introduced to prove a fact that is supposed to be so conclusive that there can be no other truth as to the

matter; evidence so strong, it overpowers contrary evidence, directing a fact-finder to a specific and certain conclusion.

Answer: C is incorrect. Direct evidence is testimony proof for any evidence, which expressly or straight-forwardly proves the existence of a fact.

---

### QUESTION 3

You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement? (Choose two)

A. Using WPA encryption

B. MAC filtering the router

C. Not broadcasting SSID

D. Using WEP encryption

Correct Answer: AD

With either encryption method (WEP or WPA) you can give the password to customers who need it, and even change it frequently (daily if you like). So this won't be an inconvenience for customers.

---

### QUESTION 4

In which of the following does a Web site store information such as user preferences to provide customized services to users?

A. Protocol

B. ActiveX control

C. Cookie

D. Keyword

Correct Answer: C

A cookie is a small bit of text that accompanies requests and pages as they move between Web servers and browsers. It contains information that is read by a Web application, whenever a user visits a site. Cookies are stored in the memory or hard disk of client computers. A Web site stores information, such as user preferences and settings in a cookie. This information helps in providing customized services to users. There is absolutely no way a Web server can access any private information about a user or his computer through cookies, unless a user provides the information. A Web server cannot access cookies created by other Web servers. Answer A is incorrect. A protocol is a set of predefined rules that govern how two or more processes communicate and interact to exchange data. Protocols are considered as the building blocks of network communication. Computer protocols are used by communicating devices and software services to format data in a way that all participants understand. It provides a context in which to interpret communicated information. Answer: B is incorrect. ActiveX controls are software components that can be integrated into Web pages and applications, within a computer or among computers in a network, to reuse the functionality. Reusability of controls reduces development time of applications and improves program interfaces. They enhance the Web pages with formatting features and animation. ActiveX controls can be used in applications written in different programming languages that recognize Microsoft's Component Object Model (COM). These controls always run in a container. ActiveX controls simplify and automate the authoring tasks, display data, and add functionality to Web pages. Answer: D is incorrect. Keywords are important terms used to search Web pages on a particular topic. For example, if a user enters a keyword "Networking" in a search engine form, all Web pages containing the term "Networking" will be displayed.

#### QUESTION 5

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to see the username, real name, home directory, encrypted password, and other information about a user.

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

- A. /etc/passwd
- B. /etc/printcap
- C. /etc/hosts
- D. /etc/inittab

Correct Answer: A

In Unix, the /etc/passwd file contains username, real name, home directory, encrypted password, and other information about a user.

Answer: C is incorrect. In Unix, the /etc/hosts file lists the hosts for name lookup use that are locally required.

Answer: D is incorrect. In Unix, the /etc/inittab file is the configuration file for init. It controls startup run levels and determines scripts to start with.

Answer: B is incorrect. In Unix, the /etc/printcap file is the configuration file for printers.

#### QUESTION 6

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to do RARP mapping from hardware mapping addresses to IP addresses.

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

- A. /etc/dhcpd.conf
- B. /etc/motd
- C. /etc/exports
- D. /etc/ethers

Correct Answer: D

In Unix, the /etc/ethers file is used by system administrators for RARP mapping from hardware mapping addresses to IP addresses.

Answer: A is incorrect. In Unix, the /etc/dhcpd.conf file is the configuration file for the DHCP server daemon.

Answer: C is incorrect. In Unix, the /etc/exports file describes exported file systems for NFS services.

Answer: B is incorrect. In Unix, the /etc/motd file automatically displays the message of the day after a successful login.

---

#### QUESTION 7

You are the Security Consultant and you frequently do vulnerability assessments on client computers. You want to have a standardized approach that would be applicable to all of your clients when doing a vulnerability assessment.

What is the best way to do this?

- A. Utilize OVAL.
- B. Create your own standard and use it with all clients.
- C. Utilize each client's security policies when doing a vulnerability assessment for that client.
- D. Utilize the Microsoft security recommendations.

Correct Answer: A

Open Vulnerability Assessment Language (OVAL) is a common language for security professionals to use when checking for the presence of vulnerabilities on computer systems. OVAL provides a baseline method for performing vulnerability

assessments on local computer systems.

Answer: D is incorrect. While Microsoft security standards will be appropriate for many of your clients, they won't help clients using Linux, Macintosh, or Unix. They also won't give you insight into checking your firewalls or routers.

Answer: C is incorrect. This would not fulfill the requirement of having a standardized approach applicable to all clients.

Answer: B is incorrect. This would not be the best way. You should use common industry standards, like OVAL.

---

#### QUESTION 8

You work as a Network Administrator for BetaTech Inc. You have been assigned the task of designing the firewall policy for the company.

Which of the following statements is unacceptable in the 'acceptable use statement' portion of the firewall policy?

- A. The computers and their applications should be used for organizational related activities only.
- B. Computers may not be left unattended with a user account still logged on.
- C. Applications other than those supplied or approved by the company can be installed on any computer.
- D. The installed e-mail application can only be used as the authorized e-mail service.

Correct Answer: C

Applications other than those supplied or approved by the company shall not be installed on any computer. Answer: A, B, D are incorrect. All of these statements stand true in the 'acceptable use statement' portion of the firewall policy.

---

### QUESTION 9

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. You want to use multiple security countermeasures to protect the integrity of the information assets of the company. To accomplish the task,

you need to create a complex and multi-layered defense system.

Which of the following components can be used as a layer that constitutes 'Defense in depth'? (Choose three)

- A. Backdoor
- B. Firewall
- C. Antivirus software
- D. Intrusion detection

Correct Answer: BCD

The components of Defense in depth include antivirus software, firewalls, anti-spyware programs, hierarchical passwords, intrusion detection, and biometric verification. In addition to electronic countermeasures, physical protection of business sites along with comprehensive and ongoing personnel training enhances the security of vital data against compromise, theft, or destruction. Answer A is incorrect. A backdoor is any program that allows a hacker to connect to a computer without going through the normal authentication process. The main advantage of this type of attack is that the network traffic moves from inside a network to the hacker's computer. The traffic moving from inside a network to the outside world is typically the least restrictive, as companies are more concerned about what comes into a network, rather than what leaves it. It, therefore, becomes hard to detect backdoors.

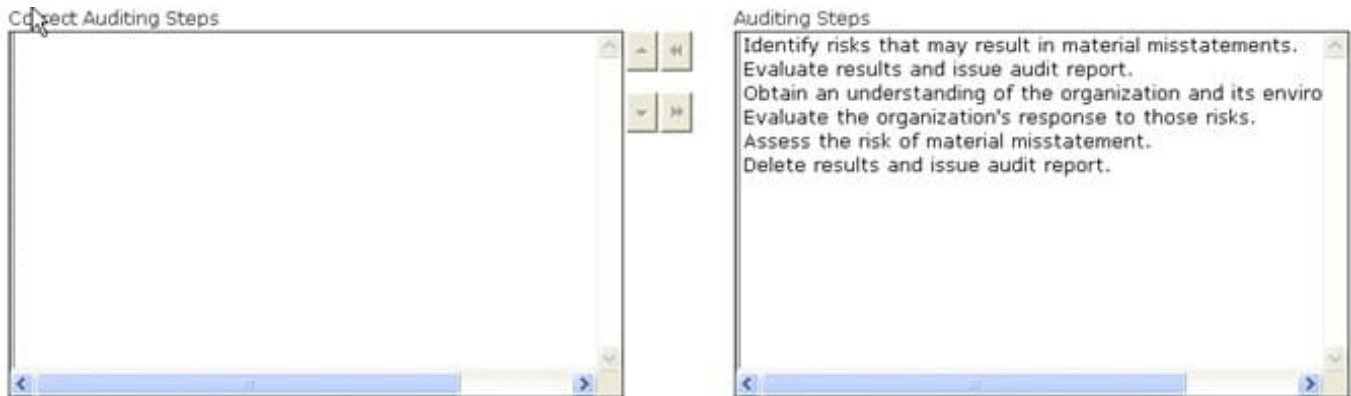
---

### QUESTION 10

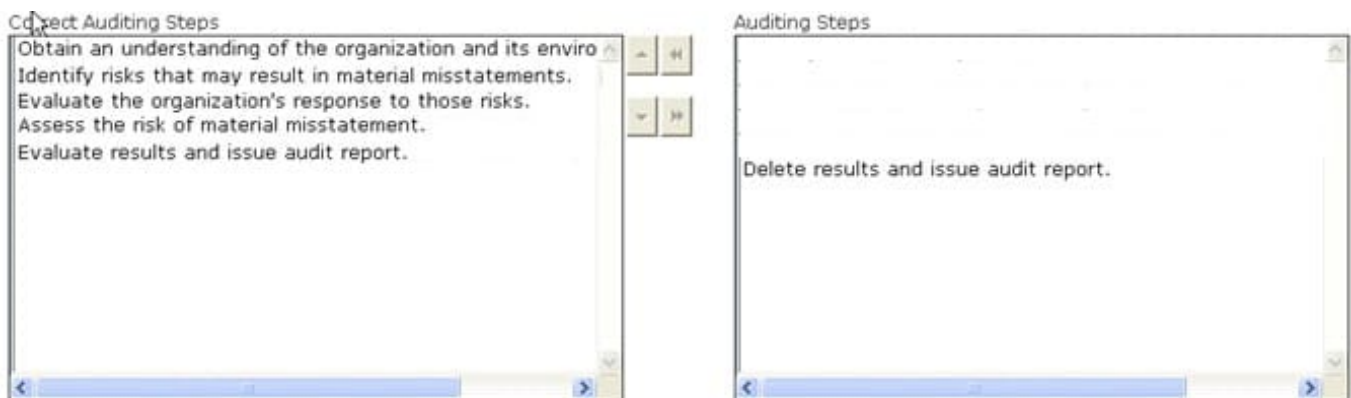
DRAG DROP

You work as a Network Auditor for Net Perfect Inc. The company has a Windows-based network. You need to audit the network of the company. You need to plan the audit process to minimize the audit risk. What steps will you take to minimize the possibility of audit risk?

Select and Place:



Correct Answer:



The auditor must plan and conduct the audit to ensure their audit risk (the risk of reaching an incorrect conclusion based on the audit findings) will be limited to an acceptable level. To eliminate the possibility of assessing audit risk too low, the

auditor should perform the following steps:

**Obtain an Understanding of the Organization and its Environment:** The understanding of the organization and its environment is used to assess the risk of material misstatement/weakness and to set the scope of the audit. The auditor's

understanding should include information on the nature of the entity, management, governance, objectives and strategies, and business processes.

**Identify Risks that May Result in Material Misstatements:** The auditor must evaluate an organization's business risks (threats to the organization's ability to achieve its objectives). An organization's business risks can arise or change due to

new personnel, new or restructured information systems, corporate restructuring, and rapid growth to name a few.

**Evaluate the Organization's Response to those Risks:** Once the auditor has evaluated the organization's response to the assessed risks, the auditor should then obtain evidence of management's actions toward those risks. The organization's

response (or lack thereof) to any business risks will impact the auditor's assessed level of audit risk.

**Assess the Risk of Material Misstatement:** Based on the knowledge obtained in evaluating the organization's responses to business risks, the auditor then assesses the risk of material misstatements and determines specific audit procedures

that are necessary based on that risk assessment.

Evaluate Results and Issue Audit Report: At this level, the auditor should determine if the assessments of risks were appropriate and whether sufficient evidence was obtained. The auditor will issue either an unqualified or qualified audit report

based on their findings.

---

#### QUESTION 11

What are the different categories of PL/SQL program units?

- A. Default
- B. Unnamed
- C. Primary
- D. Named

Correct Answer: BD

A named block is a PL/SQL block that Oracle stores in the database and can be called by name from any application. A named block is also known as a stored procedure. Named blocks can be called from any PL/SQL block. It has a declaration section, which is known as a header. The header may include the name of a block, type of the block, and parameter. The name and list of formal parameters are known as the signature of a subroutine. Once a named PL/SQL block is compiled, it gets permanently stored as p-code after compilation in the shared pool of the system global area. Therefore, the named block gets compiled only once. An anonymous block is a PL/SQL block that appears in a user's application and is neither named nor stored in the database. This block does not allow any mode of parameter. Anonymous block programs are effective in some situations. They are basically used when building scripts to seed data or perform one-time processing activities. They are also used when a user wants to nest activity in another PL/SQL block's execution section. Anonymous blocks are compiled each time they are executed.

---

#### QUESTION 12

You have made a program secure.c to display which ports are open and what types of services are running on these ports. You want to write the program's output to standard output and simultaneously copy it into a specified file.

Which of the following commands will you use to accomplish the task?

- A. cat
- B. more
- C. less
- D. tee

Correct Answer: D

You will use the tee command to write its content to standard output and simultaneously copy it into the specified file. The tee command is used to split the output of a program so that it can be seen on the display and also be saved in a file. It can also be used to capture intermediate output before the data is altered by another command or program. The



tee command reads standard input, then writes its content to standard output, and simultaneously copies it into the specified file

(s) or variables. The syntax of the tee command is as follows: tee [-a] [-i] [File] where, the -a option appends the output to the end of File instead of writing over it and the -i option is used to ignore interrupts. Answer: A is incorrect. The concatenate (cat) command is used to display or print the contents of a file. Syntax: cat filename For example, the following command will display the contents of the /var/log/dmesg file: cat /var/log/dmesg Note: The more command is used in conjunction with the cat command to prevent scrolling of the screen while displaying the contents of a file. Answer: C is incorrect. The less command is used to view (but not change) the contents of a text file, one screen at a time. It is similar to the more command. However, it has the extended capability of allowing both forward and backward navigation through the file. Unlike most Unix text editors/viewers, less does not need to read the entire file before starting; therefore, it has faster load times with large files. The command syntax of the less command is as follows: less [options] file\_name Where,

Option	Description
-g	Highlights just the current match of any searched string
-I	Performs case-insensitive searches
-M	Shows more detailed prompt, including file position
-N	Shows line numbers
-S	Disables line wrap

Answer B is incorrect. The more command is used to view (but not modify) the contents of a text file on the terminal screen at a time. The syntax of the more command is as follows: more [options] file\_name Where,

Option	Description
-num	It specifies an integer, which is the screen size (in lines).
-d	<b>more</b> will prompt the user with the message "[Press space to continue, 'q' to quit.]" and will display "[Press 'h' for instructions.]" instead of ringing the bell when an illegal key is pressed.
-l	<b>more</b> treats ^L as a special character, and pauses after any line that contains a form feed. The -l option prevents this behavior.
-f	It causes <b>more</b> to count logical, rather than screen lines (i.e., long lines are not folded).
-u	It suppresses underlining.
+/	It specifies a string that will be searched for before each file is displayed.
+num	<b>more</b> starts file at line number num.

### QUESTION 13

What does CSS stand for?

- A. Cascading Style Sheet
- B. Coded System Sheet
- C. Cyclic Style Sheet
- D. Cascading Style System

Correct Answer: A

A Cascading Style Sheet (CSS) is a separate text file that keeps track of design and formatting information, such as colors, fonts, font sizes, and margins, used in Web pages. CSS is used to provide Web site authors greater control on the appearance and presentation of their Web pages. It has codes that are interpreted and applied by the browser on to the Web pages and their elements. CSS files have .css extension. There are three types of Cascading Style Sheets:

External Style Sheet Embedded Style Sheet Inline Style Sheet

**QUESTION 14**

DRAG DROP

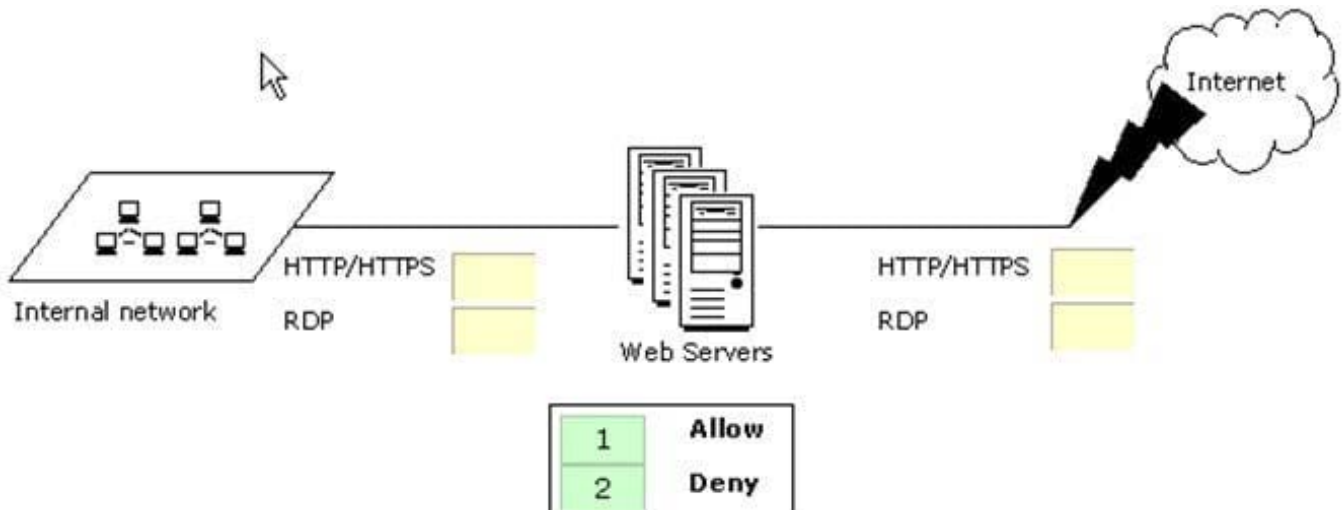
Your company has been hired to provide consultancy, development, and integration services for a company named Soul International. You have prepared a case study to plan the upgrade for the company.

You are designing policy settings for the Web servers at the headquarters.

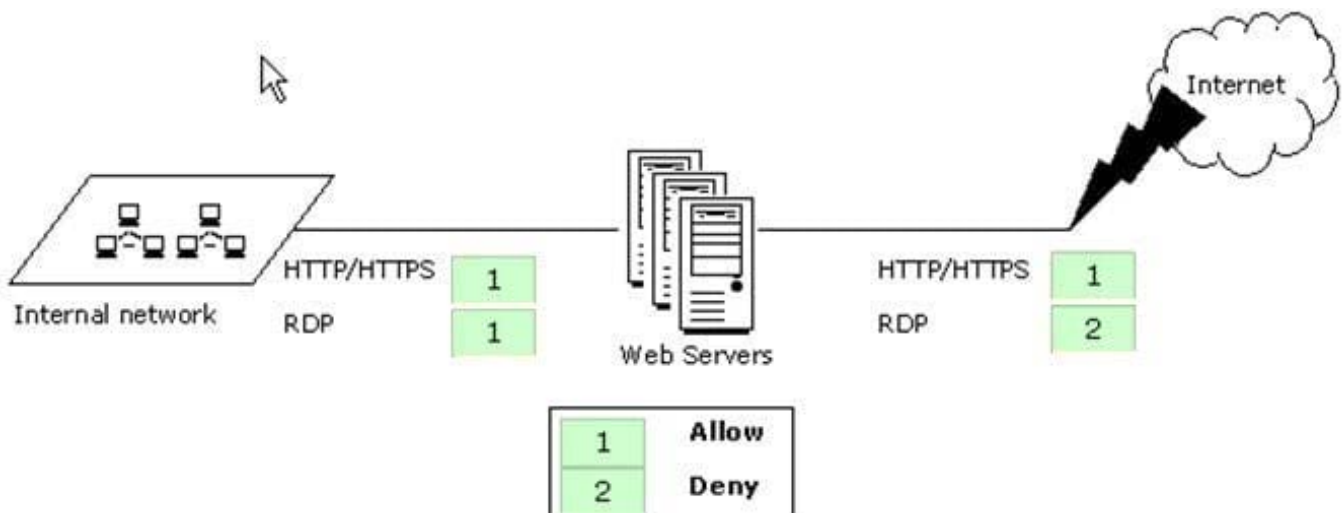
Place Allow or Deny in front of the type of traffic received by or sent to the Web servers from the internal clients and the Internet.

(Click the Exhibit button on the toolbar to see the case study.)

Select and Place:



Correct Answer:



HTTP/HTTPS is used for transferring HTML pages over the network. Hence, you should allow it for both the Internet and internal clients traffic.

The Remote Desktop Protocol (RDP) is used to connect to servers remotely. Allowing it for the Internet traffic is definitely a security threat. Hence, you should deny this for the Internet traffic. According to the case study, the administrators

must use RDP to connect to the servers in the perimeter network. Hence, you will have to allow it for the internal clients traffic.

**QUESTION 15**

**DRAG DROP**

Choose and select the information present in the header of a single IP packet that are helpful in packet filtering.

Select and Place:

Correct Answer:

An IP packet is a formatted unit of data carried by a packet mode computer network. A packet consists of two kinds of data:

control information and user data (also known as payload). The control information provides data the network needs to deliver the user data, for example: source and destination addresses, error detection codes like checksums, and

sequencing information. Typically, control information is found in packet headers and trailers, with user data in between.

IP packets are composed of a header and payload. Every IP packet has a set of headers containing certain information. The main information is as follows:

IP source address

IP destination address

Protocol (whether the packet is a TCP, UDP, or ICMP packet)

TCP or UDP source port TCP or UDP destination port ICMP message type The structure of an IP packet is as follows:

0	4	8	16	19	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time To Live		Protocol	Header Checksum		
Source IP Address					
Destination IP Address					
Options				Padding	

[GNSA PDF Dumps](#)

[GNSA VCE Dumps](#)

[GNSA Study Guide](#)