CAS-002^{Q&As}

CompTIA Advanced Security Practitioner Exam

Pass CompTIA CAS-002 Exam with 100% Guarantee

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

https://www.passapply.com/cas-002.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Company A is purchasing Company B. Company A uses a change management system for all IT processes while Company B does not have one in place. Company B\\'s IT staff needs to purchase a third party product to enhance production. Which of the following NEXT steps should be implemented to address the security impacts this product may cause?

A. Purchase the product and test it in a lab environment before installing it on any live system.

B. Allow Company A and B\\'s IT staff to evaluate the new product prior to purchasing it.

C. Purchase the product and test it on a few systems before installing it throughout the entire company.

D. Use Company A\\'s change management process during the evaluation of the new product.

Correct Answer: D

QUESTION 2

The Information Security Officer (ISO) is reviewing a summary of the findings from the last COOP tabletop exercise. The Chief Information Officer (CIO) wants to determine which additional controls must be implemented to reduce the risk of an extended customer service outage due to the VoIP system being unavailable. Which of the following BEST describes the scenario presented and the document the ISO is reviewing?

A. The ISO is evaluating the business implications of a recent telephone system failure within the BIA.

B. The ISO is investigating the impact of a possible downtime of the messaging system within the RA.

C. The ISO is calculating the budget adjustment needed to ensure audio/video system redundancy within the RFQ.

D. The ISO is assessing the effect of a simulated downtime involving the telecommunication system within the AAR.

Correct Answer: D

QUESTION 3

After reviewing a company\\'s NAS configuration and file system access logs, the auditor is advising the security administrator to implement additional security controls on the NFS export. The security administrator decides to remove the no_root_squash directive from the export and add the nosuid directive. Which of the following is true about the security controls implemented by the security administrator?

A. The newly implemented security controls are in place to ensure that NFS encryption can only be controlled by the root user.

B. Removing the no_root_squash directive grants the root user remote NFS read/write access to important files owned by root on the NAS.

C. Users with root access on remote NFS client computers can always use the SU command to modify other user\\'s files on the NAS.

D. Adding the nosuid directive disables regular users from accessing files owned by the root user over NFS even after

using the SU command.

Correct Answer: C

QUESTION 4

An organization recently upgraded its wireless infrastructure to support WPA2 and requires all clients to use this method. After the upgrade, several critical wireless clients fail to connect because they are only WEP compliant. For the foreseeable future, none of the affected clients have an upgrade path to put them into compliance with the WPA2 requirement. Which of the following provides the MOST secure method of integrating the non-compliant clients into the network?

A. Create a separate SSID and WEP key to support the legacy clients and enable detection of rogue APs.

B. Create a separate SSID and WEP key on a new network segment and only allow required communication paths.

C. Create a separate SSID and require the legacy clients to connect to the wireless network using certificate-based 802.1x.

D. Create a separate SSID and require the use of dynamic WEP keys.
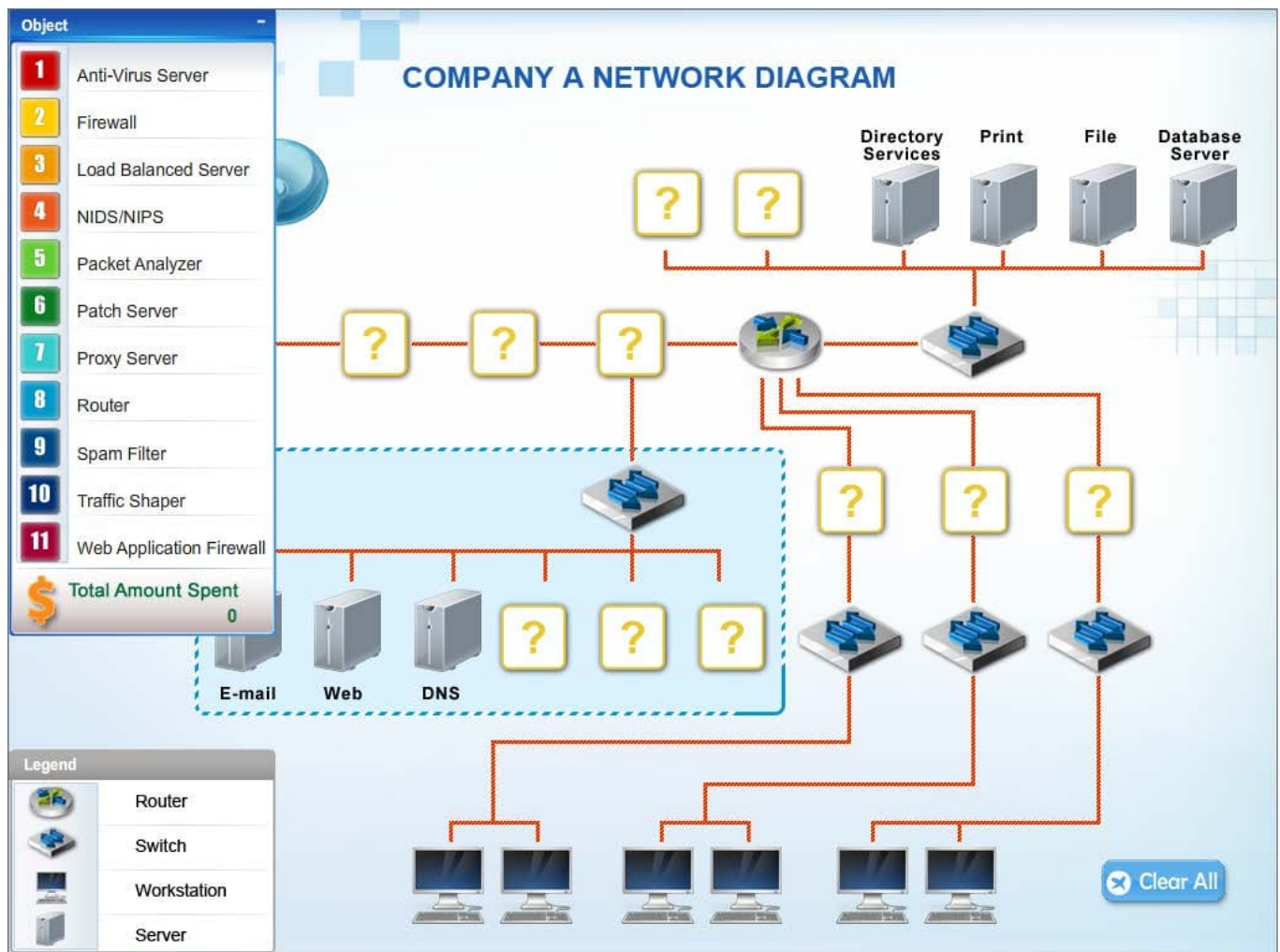
Correct Answer: B

QUESTION 5

Company A has experienced external attacks on their network and wants to minimize the attacks from reoccurring. Modify the network diagram to prevent SQL injections, XSS attacks, smurf attacks, e-mail spam, downloaded malware, viruses and ping attacks. The company can spend a MAXIMUM of $50,000 USD. A cost list for each item is listed below:

1.

 Anti-Virus Server - $10,000

2.

 Firewall-$15,000

3.

 Load Balanced Server - $10,000

4.

 NIDS/NIPS-$10,000

5.

 Packet Analyzer - $5,000

6.

 Patch Server-$15,000

7.

Proxy Server-$20,000

8.

Router-$10,000

9.

Spam Filter-$5,000

10.

Traffic Shaper - $20,000

11.

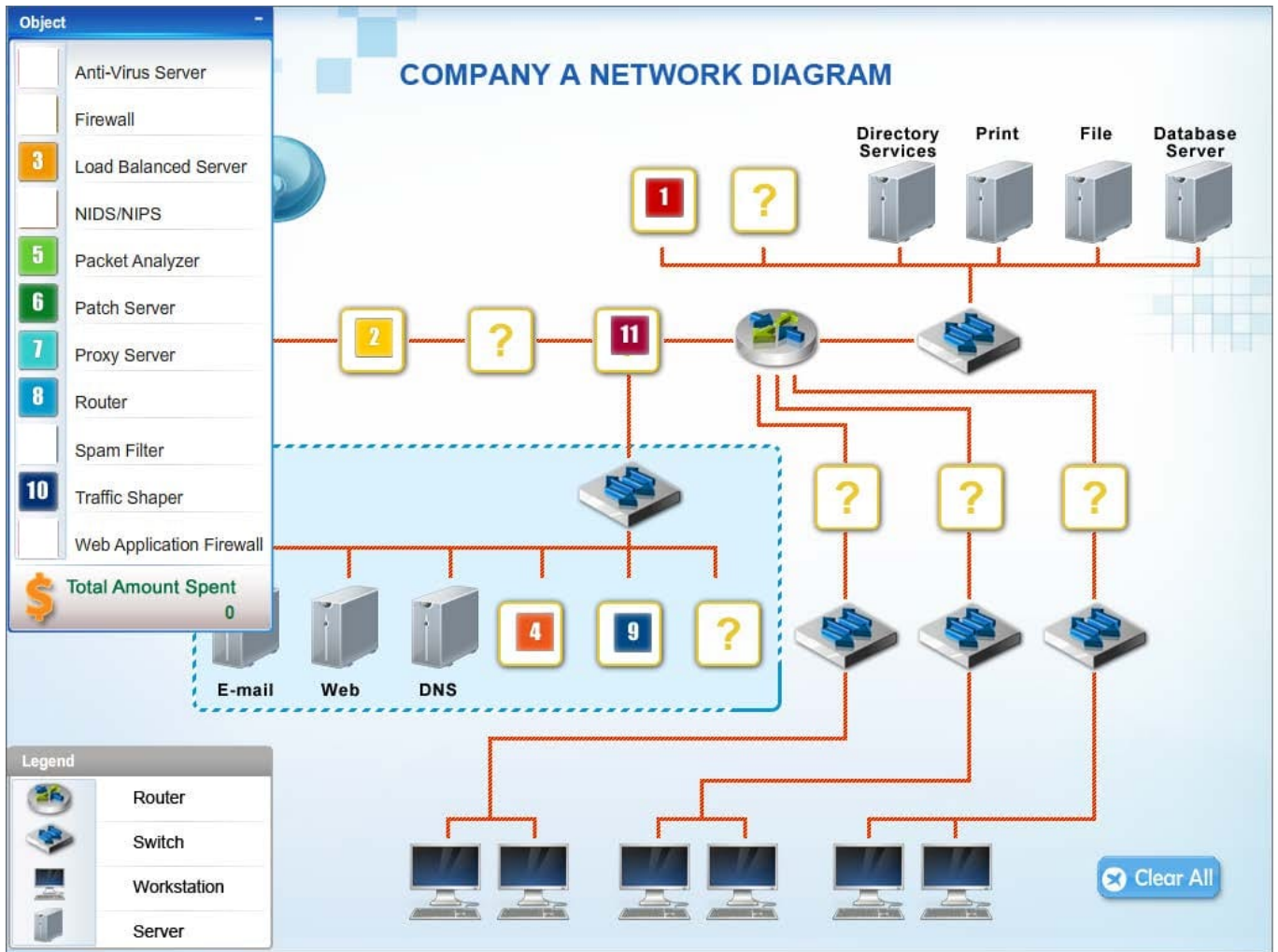Web Application Firewall - $10,000

Instructions: Not all placeholders in the diagram need to be filled and items can only be used once. If you place an object on the network diagram, you can remove it by clicking the (x) in the upper right-hand of the object.

Select and Place:

Correct Answer: