# CAS-002

Number: CAS-002
Passing Score: 800
Time Limit: 120 min

**Exam A**

**QUESTION 1**
A network engineer wants to deploy user-based authentication across the company's wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user's network access be controlled based on the user's role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations. Which of the following are needed to implement these requirements? (Select TWO).

A. SAML
B. WAYF
C. LDAP
D. RADIUS
E. Shibboleth
F. PKI

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 2**
Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the

"Pass Any Exam. Any Time." - www.actualtests.com 108 CompTIA CAS-002 Exam
distributed login with centralized authentication and has wide compatibility among SaaS vendors?

A. Establish a cloud-based authentication service that supports SAML.
B. Implement a new Diameter authentication server with read-only attestation.
C. Install a read-only Active Directory server in the corporate DMZ for federation.
D. Allow external connections to the existing corporate RADIUS server.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 3**
The Chief Information Security Officer (CISO) at a large organization has been reviewing some security-related incidents at the organization and comparing them to current industry trends. The desktop security engineer feels that the use of USB storage devices on office computers has contributed to the frequency of security incidents. The CISO knows the acceptable use policy prohibits the use of USB storage devices. Every user receives a popup warning about this policy upon login. The SIEM system produces a report of USB violations on a monthly basis; yet violations continue to occur. Which of the following preventative controls would MOST effectively mitigate the logical risks associated with the use of USB storage devices?

A. Revise the corporate policy to include possible termination as a result of violations
B. Increase the frequency and distribution of the USB violations report
C. Deploy PKI to add non-repudiation to login sessions so offenders cannot deny the offense
D. Implement group policy objects

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 4**
The IT Security Analyst for a small organization is working on a customer's system and identifies a possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.
B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.
C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.
D. Refer the issue to management for handling according to the incident response process.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 5**
An IT manager is working with a project manager from another subsidiary of the same multinational organization. The project manager is responsible for a new software development effort that is being outsourced overseas, while customer acceptance testing will be performed in house. Which of the following capabilities is MOST likely to cause issues with network availability?

A. Source code vulnerability scanning
B. Time-based access control lists
C. ISP to ISP network jitter
D. File-size validation
E. End to end network encryption

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 107 CompTIA CAS-002 Exam

**QUESTION 6**
A finance manager says that the company needs to ensure that the new system can "replay" data, up to the minute, for every exchange being tracked by the investment departments. The finance manager also states that the company's transactions need to be tracked against this data for a period of five years for compliance. How would a security engineer BEST interpret the finance manager's needs?

A. Compliance standards
B. User requirements
C. Data elements

D. Data storage
E. Acceptance testing
F. Information digest
G. System requirements

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 7**
A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?

A. Insider threat
B. Network reconnaissance
C. Physical security
D. Industrial espionage

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 8**
A company is trying to decide how to manage hosts in a branch location connected via a slow WAN link. The company desires to provide the same level of performance and functionality to the branch office as it provides to the main campus. The company uses Active Directory for its directory service and host configuration management. The branch location does not have a datacenter, and the physical security posture of the building is weak. Which of the following designs is MOST appropriate for this scenario?

A. Deploy a branch location Read-Only Domain Controller in the DMZ at the main campus with a two-way trust.
B. Deploy a corporate Read-Only Domain Controller to the branch location.
C. Deploy a corporate Domain Controller in the DMZ at the main campus.
D. Deploy a branch location Read-Only Domain Controller to the branch office location with a one- way trust.
E. Deploy a corporate Domain Controller to the branch location.
F. Deploy a branch location Domain Controller to the branch location with a one-way trust.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 9**
DRAG DROP

A manufacturer is planning to build a segregated network. There are requirements to segregate development

and test infrastructure from production and the need to support multiple entry points into the network depending on the service being accessed. There are also strict rules in place to only permit user access from within the same zone. Currently, the following access requirements have been identified:

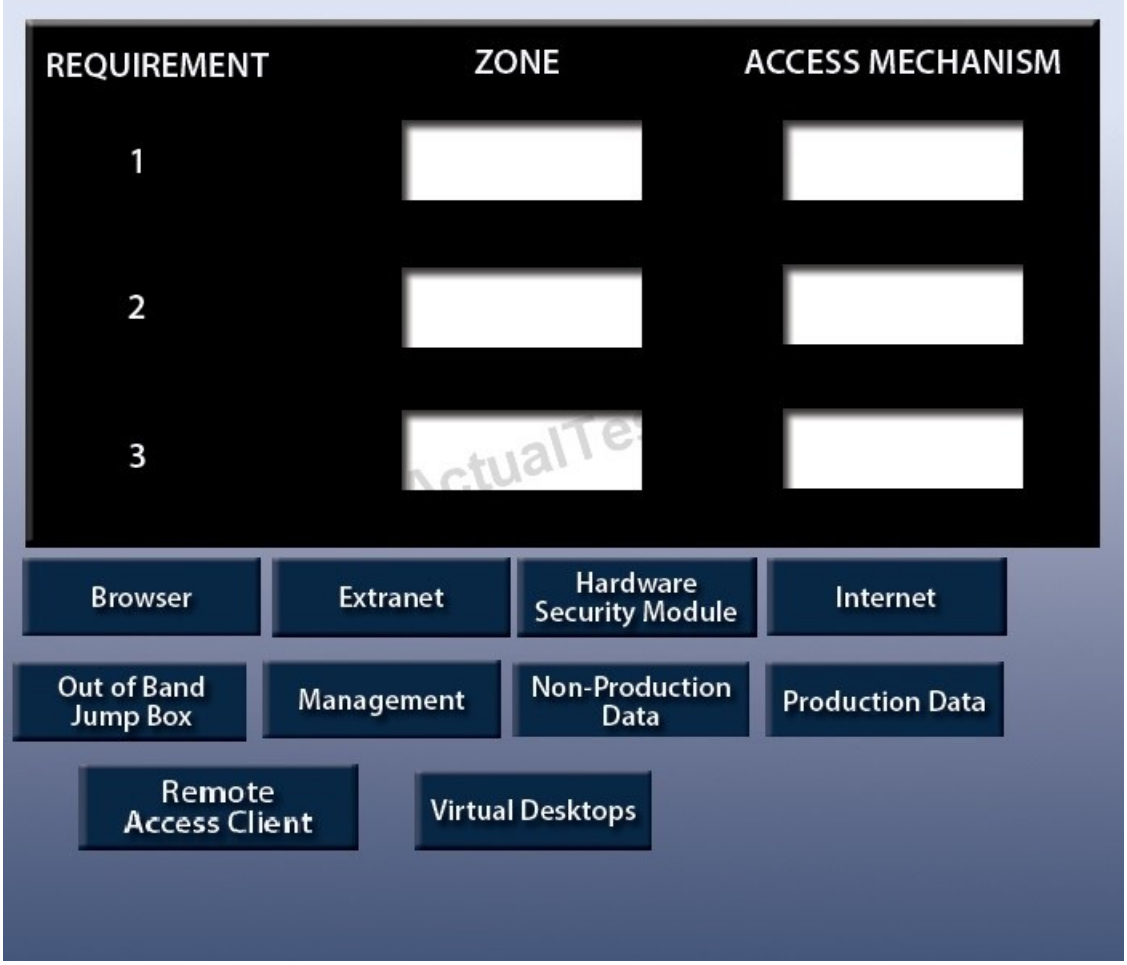
1. Developers have the ability to perform technical validation of development applications.

2. End users have the ability to access internal web applications.

3. Third-party vendors have the ability to support applications.

In order to meet segregation and access requirements, drag and drop the appropriate network zone that the user would be accessing and the access mechanism to meet the above criteria. Options may be used once or not at all. All placeholders must be filled.

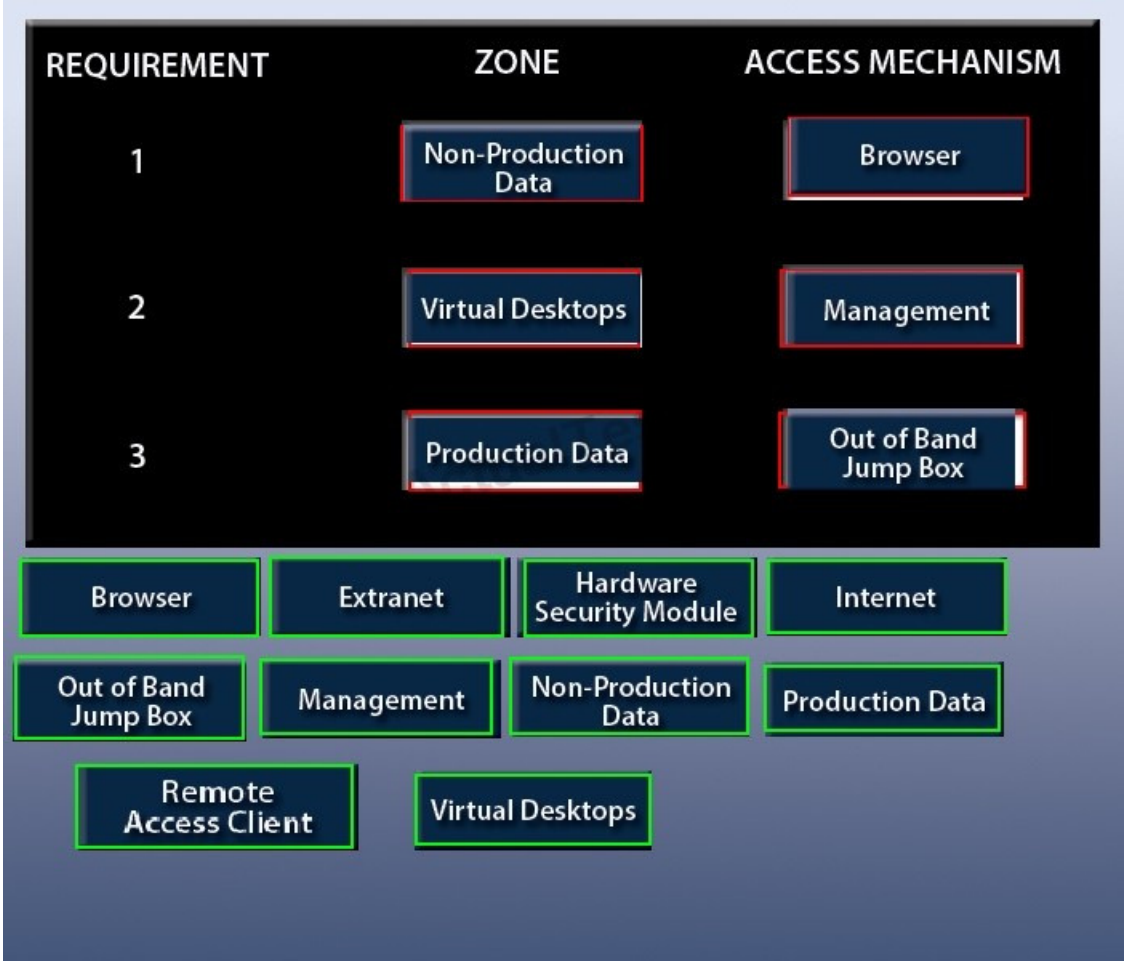
"Pass Any Exam. Any Time." - www.actualtests.com 122 CompTIA CAS-002 Exam




A.
B.
C.
D.

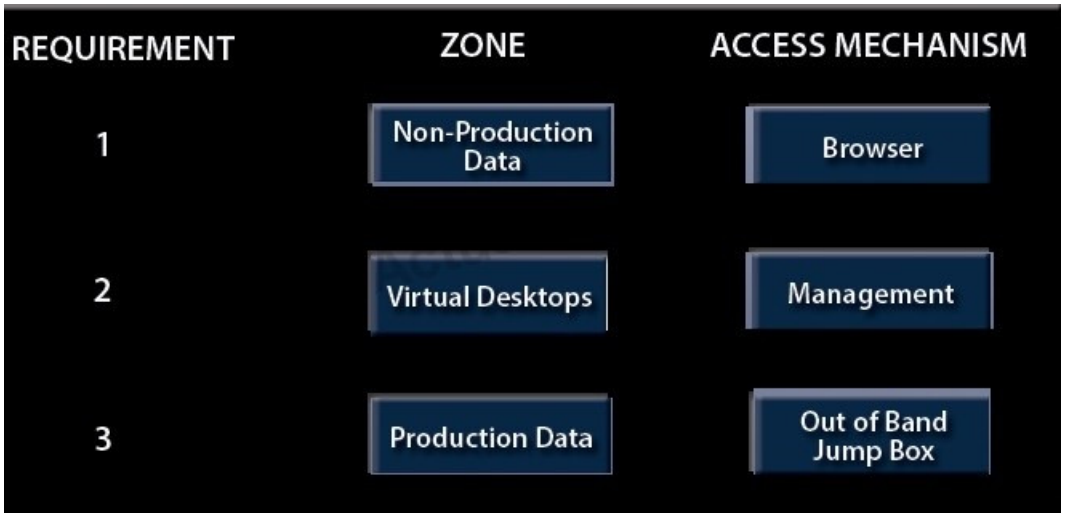
**Correct Answer:**
**Section: (none)**
**Explanation**

**Explanation/Reference:**




"Pass Any Exam. Any Time." - www.actualtests.com 123 CompTIA CAS-002 Exam

Explanation:




**QUESTION 10**
DRAG DROP

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

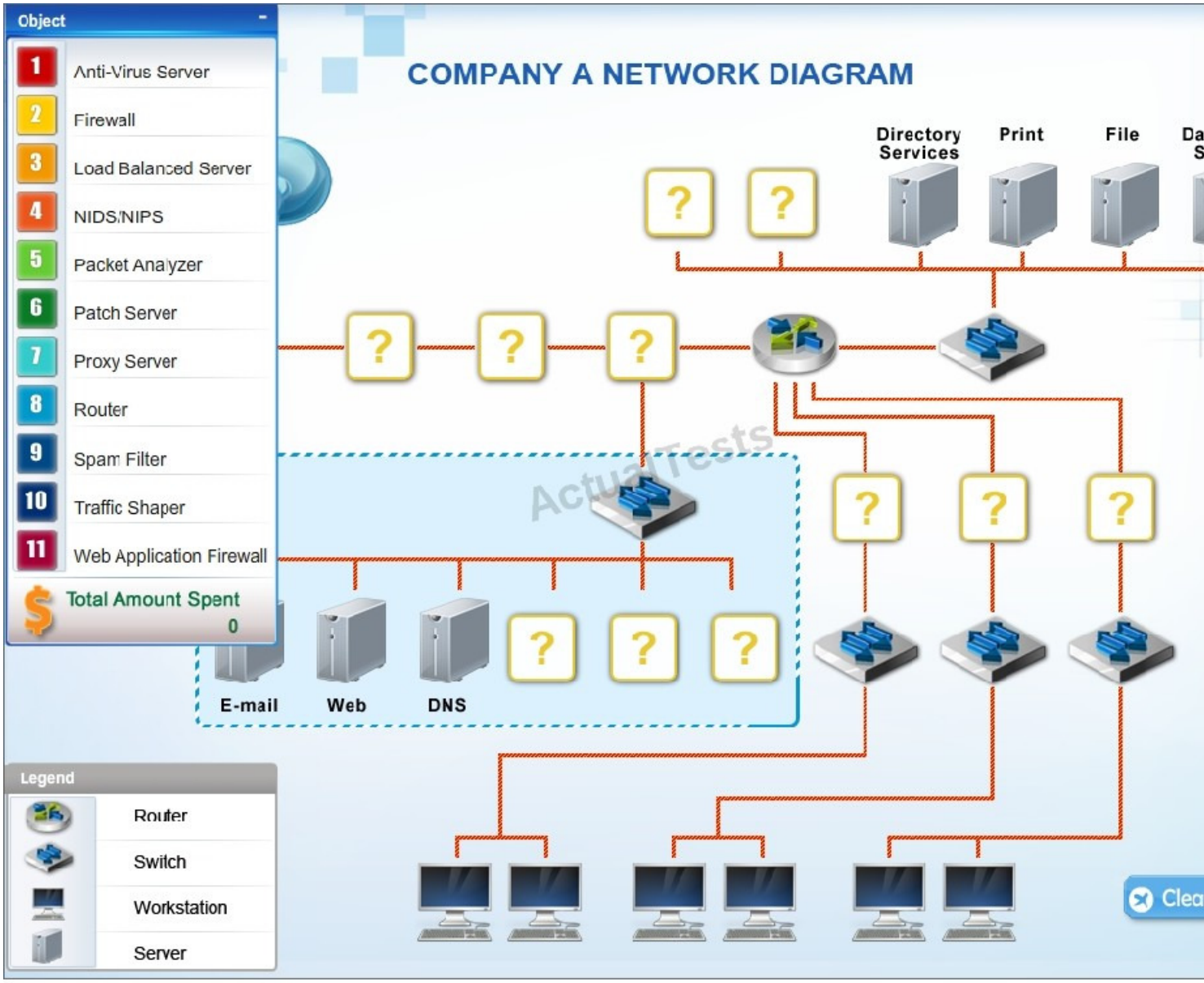
9. Spam Filter-$5,000

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.

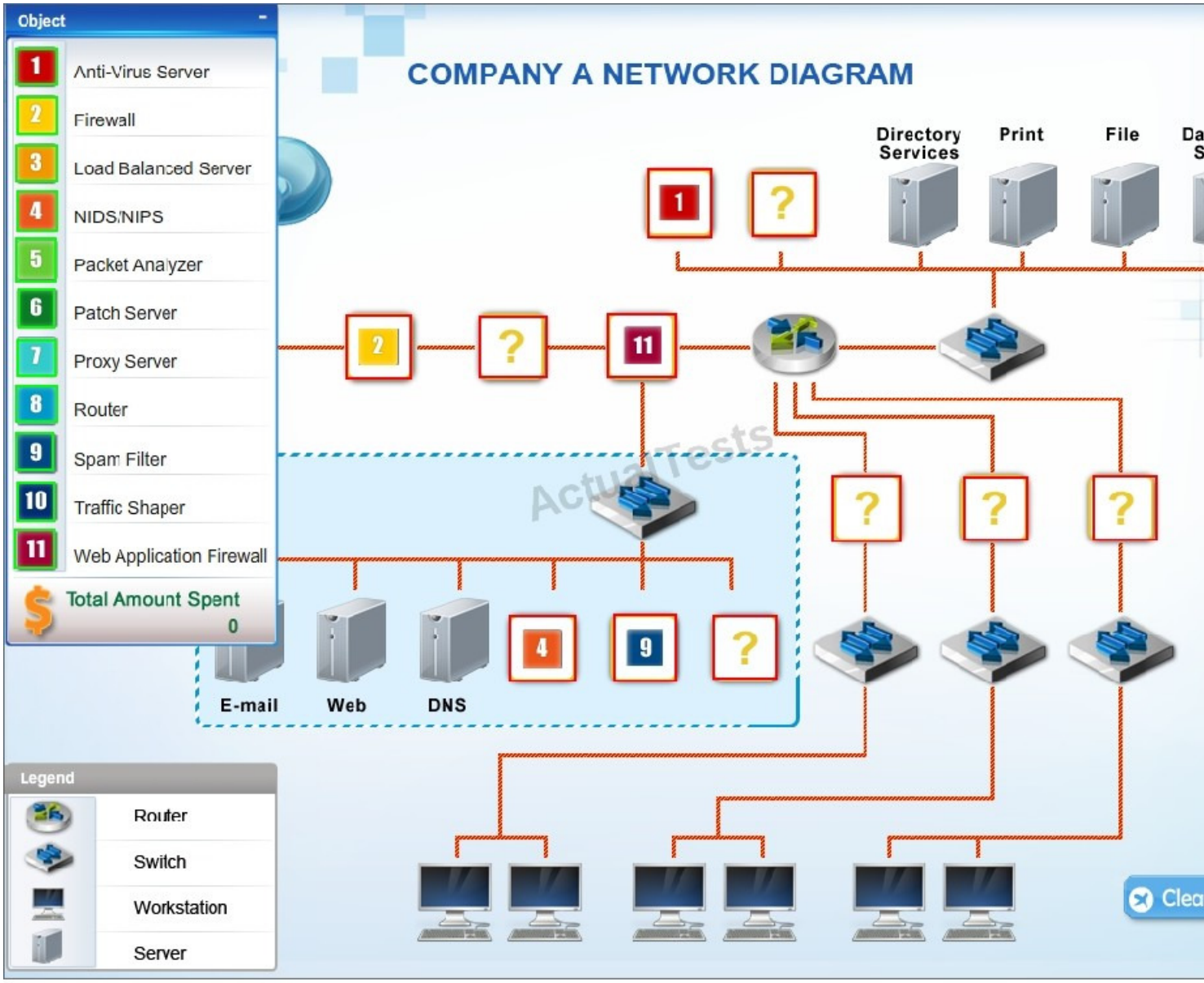
"Pass Any Exam. Any Time." - www.actualtests.com 120 CompTIA CAS-002 Exam
If you place an object on the network diagram, you can remove it by clicking the (x) in the upper right-hand of the object.




A.
B.
C.
D.

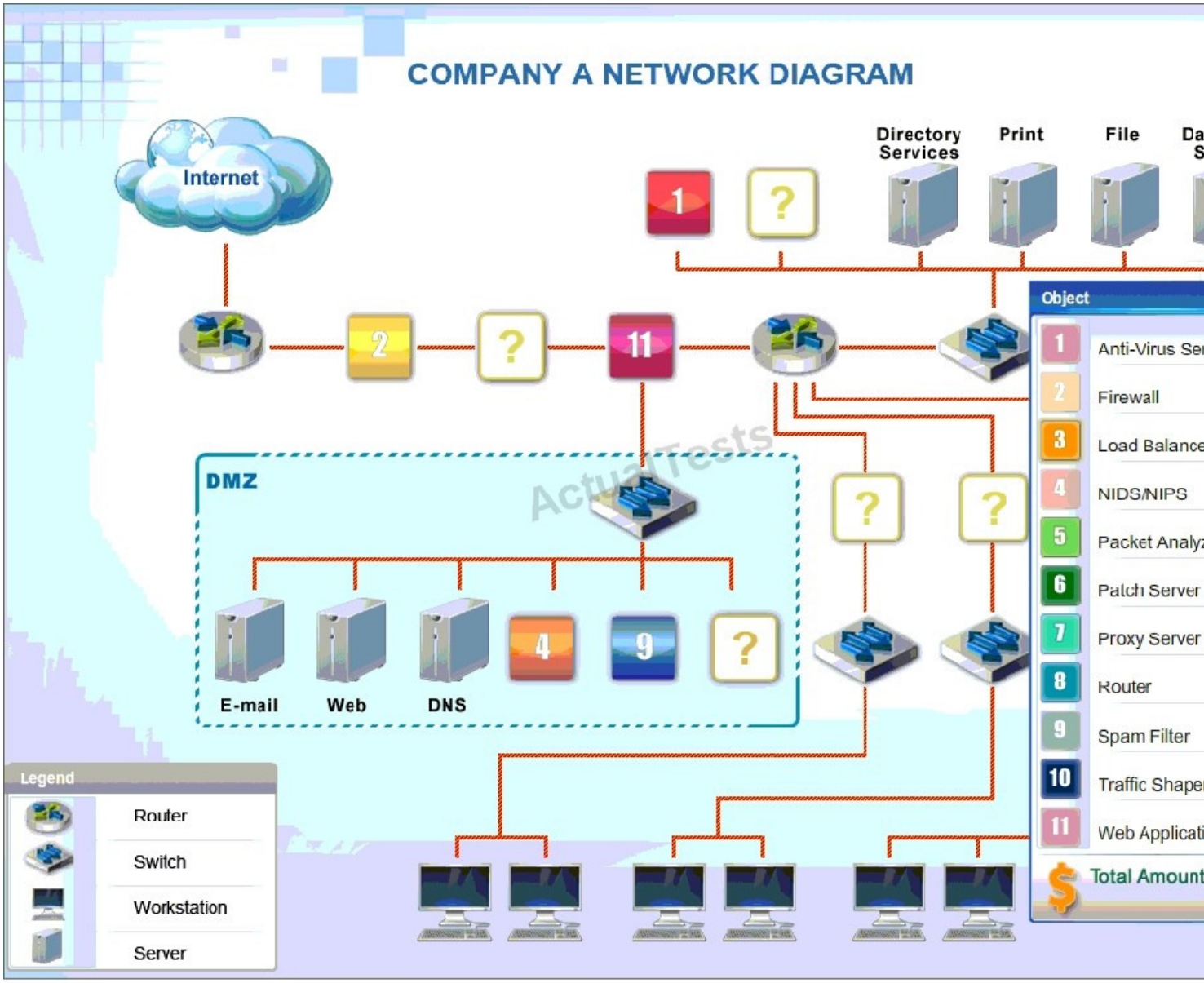
**Correct Answer:**
**Section: (none)**
**Explanation**

**Explanation/Reference:**




Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 121 CompTIA CAS-002 Exam




**QUESTION 11**
CORRECT TEXT

Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several Internal networks. The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:

User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet:192.168.3.0/24

Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down

Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.

Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.