



# SY0-501<sup>Q&As</sup>

CompTIA Security+ Certification Exam

**Pass CompTIA SY0-501 Exam with 100% Guarantee**

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

<https://www.geekcert.com/sy0-501.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

A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops\' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?

- A. Put the desktops in the DMZ.
- B. Create a separate VLAN for the desktops.
- C. Air gap the desktops.
- D. Join the desktops to an ad-hoc network.

Correct Answer: C

---

### QUESTION 2

A security engineer is concerned about susceptibility to HTTP downgrade attacks because the current customer portal redirects users from port 80 to the secure site on port 443. Which of the following would be MOST appropriate to mitigate the attack?

- A. DNSSEC
- B. HSTS
- C. Certificate pinning
- D. OCSP

Correct Answer: B

---

### QUESTION 3

Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially. Which of the following would explain the situation?

- A. An ephemeral key was used for one of the messages
- B. A stream cipher was used for the initial email; a block cipher was used for the reply
- C. Out-of-band key exchange has taken place
- D. Asymmetric encryption is being used

Correct Answer: D

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.



#### QUESTION 4

A help desk technician is trying to determine the reason why several high-level officials' account passwords need to be reset shortly after implementing a self-service password reset process. Which of the following would BEST explain the issue?

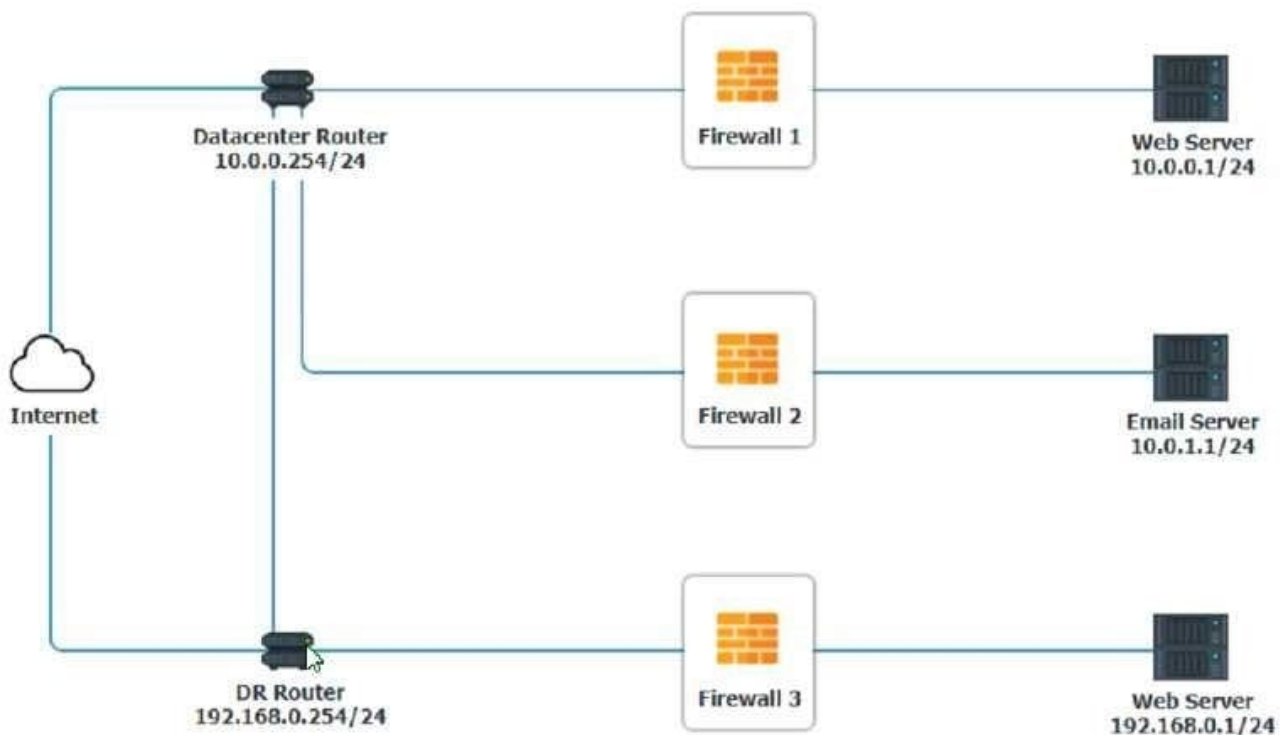
- A. The system asked for publicly available information
- B. The self-service system was compromised
- C. The account passwords expired
- D. A spear phishing attack occurred

Correct Answer: C

#### QUESTION 5

##### SIMULATION

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.



##### INSTRUCTIONS



Click on each firewall to do the following:

1.

Deny cleartext web traffic

2.

Ensure secure management protocols are used.

3.

Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints. At any time you would like to bring back the initial state of the simulation, please click the Reset All button.



**Firewall 1** ✕

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	PERMIT

Reset Answer Save Close

**Firewall 2** ✕

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	TELNET	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Reset Answer Save Close

**Firewall 3** ✕

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	PERMIT

Reset Answer Save Close



Correct Answer:

Check the answer in below In Firewall 1, HTTP inbound Action should be DENY. As shown below

Firewall 1						
Rule Name	Source	Destination	Service	Action		
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT		
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT		
Management	ANY	10.0.0.1/24	SSH	PERMIT		
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT		
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY		
<div>Reset Answer Save Close</div>						

In Firewall 2, Management Service should be DNS, As shown below.

Firewall 2						
Rule Name	Source	Destination	Service	Action		
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT		
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT		
Management	ANY	10.0.1.1/24	DNS	PERMIT		
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT		
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY		
<div>Reset Answer Save Close</div>						

In Firewall 3, HTTP Inbound Action should be DENY, as shown below



Firewall 3							
Rule Name	Source		Destination		Service		Action
DNS Rule	10.0.0.1/24	▼	ANY	▼	DNS	▼	PERMIT ▼
HTTPS Outbound	192.168.0.1/24	▼	ANY	▼	HTTPS	▼	PERMIT ▼
Management	ANY	▼	192.168.0.1/24	▼	SSH	▼	PERMIT ▼
HTTPS Inbound	ANY	▼	192.168.0.1/24	▼	HTTPS	▼	PERMIT ▼
HTTP Inbound	ANY	▼	192.168.0.1/24	▼	HTTP	▼	DENY ▼
<div>Reset Answer Save Close</div>							

[SY0-501 PDF Dumps](#)

[SY0-501 Study Guide](#)

[SY0-501 Exam Questions](#)