SY0-501 Q&As

CompTIA Security+ Certification Exam

Pass CompTIA SY0-501 Exam with 100% Guarantee

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

https://www.lead4pass.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 bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions. in addition, the perimeter router can only handle 1Gbps of traffic. Which of the following should be implemented to prevent a DoS attacks in the future?

A. Deploy multiple web servers and implement a load balancer

B. Increase the capacity of the perimeter router to 10 Gbps

C. Install a firewall at the network to prevent all attacks

D. Use redundancy across all network devices and services

Correct Answer: D

QUESTION 2

Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security. Which of the following authentication methods should be deployed to achieve this goal?

A. PIN

B. Security Question:

C. Smart card

D. Passphrase

E. CAPTCHA

Correct Answer: C

QUESTION 3

An organization wants to ensure network access is granted only after a user or device has been authenticated. Which of the following should be used to achieve this objective for both wired and wireless networks?

A. CCMP

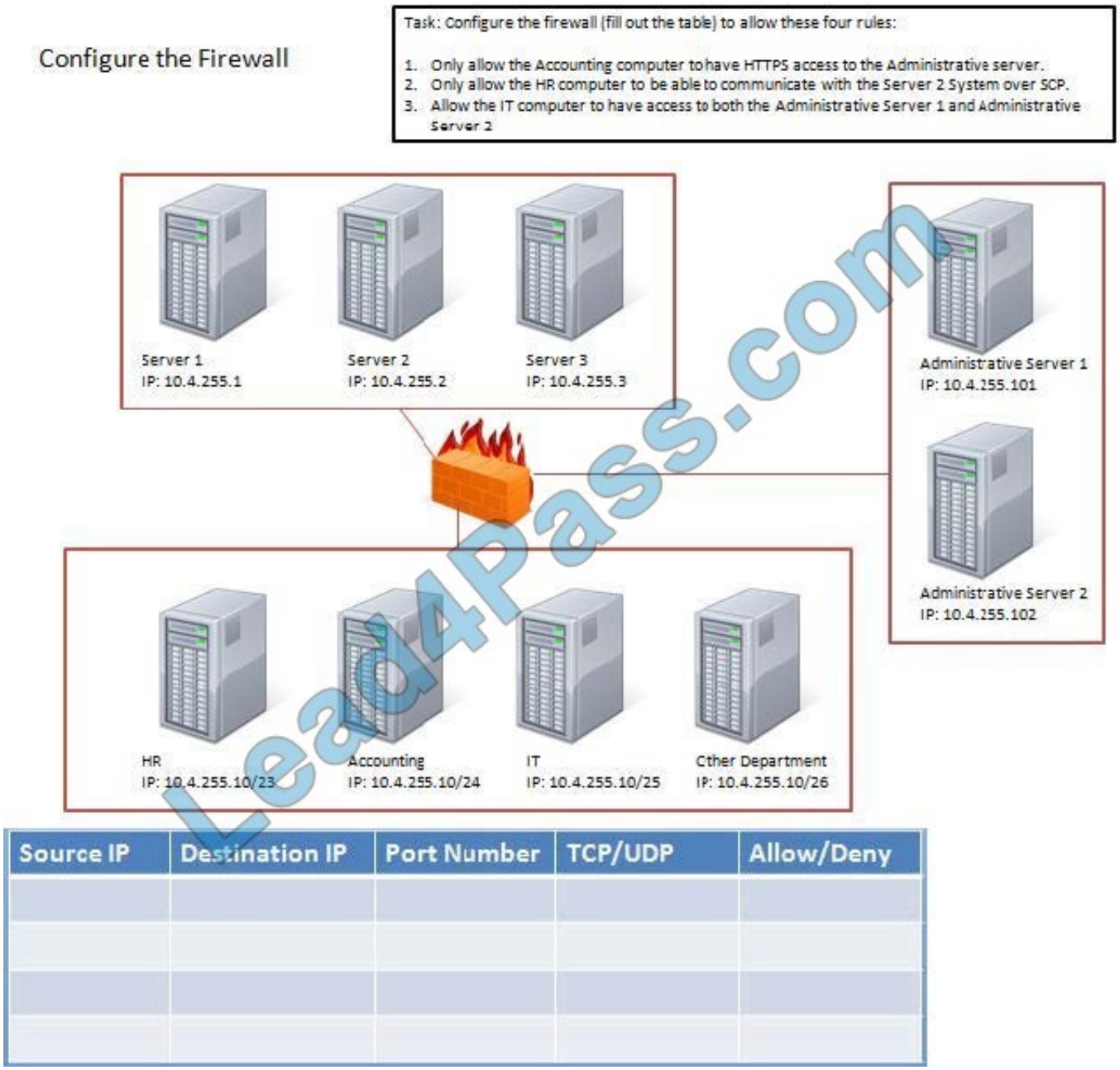
B. PKCS#12

C. IEEE 802.1X

D. OCSP

Correct Answer: C

QUESTION 4



Correct Answer:

Use the following answer for this simulation task:

Source IP

Destination IP

Port number

TCP/UDP

Allow/Deny

10.4.255.10/24

10.4.255.101

TCP

Allow

10.4.255.10/23

10.4.255.2

TCP

Allow

10.4.255.10/25

10.4.255.101

Any

Any

Allow

10.4.255.10/25

10.4.255.102

Any

Any

Allow

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule\\'s criteria:

Block the connection

Allow the connection

Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent. Two hosts communicate packet results with each other. TCP also

ensures that packets are decoded and sequenced properly. This connection is persistent during the session. When the session ends, the connection is torn down.

UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it\\'s considerably faster than TCP. The sessions don\\'t establish a synchronized session like the kind used in TCP,

and UDP doesn\\'t guarantee error-free communications. The primary purpose of UDP is to send small packets of

information. The application is responsible for acknowledging the correct reception of the data.

Port 22 is used by both SSH and SCP with UDP.

Port 443 is used for secure web connections

QUESTION 5

A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant. Which of the following represents the authentication architecture in use?

A. Open systems authentication

B. Captive portal

C. RADIUS federation

D. 802.1x

Correct Answer: D

QUESTION 6

A member of the admins group reports being unable to modify the "changes" file on a server.

The permissions on the file are as follows:

Permissions User Group File

-rwxrw-r--+ Admins Admins changes

Based on the output above, which of the following BEST explains why the user is unable to modify the "changes" file?

A. The SELinux mode on the server is set to "enforcing."

B. The SELinux mode on the server is set to "permissive."

C. An FACL has been added to the permissions for the file.

D. The admins group does not have adequate permissions to access the file.

Correct Answer: C

QUESTION 7

Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

A. LDAP

B. Kerberos

C. SAML

D. TACACS+

Correct Answer: D

QUESTION 8

During a recent audit, it was discovered that many services and desktops were missing security patches. Which of the following BEST describes the assessment that was performed to discover this issue?

A. Network mapping

B. Vulnerability scan

C. Port Scan

D. Protocol analysis

Correct Answer: B

QUESTION 9

An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

A. RTO

B. RPO

C. MTBF

D. MTTR

Correct Answer: A

QUESTION 10

A security administrator installed a new network scanner that identifies new host systems on the network. Which of the following did the security administrator install?

A. Vulnerability scanner

B. Network-based IDS

C. Rogue system detection

D. Configuration compliance scanner

Correct Answer: C

QUESTION 11

Phishing emails frequently take advantage of high-profile catastrophes reported in the news. Which of the following principles BEST describes the weakness being exploited?

A. Intimidation

B. Scarcity

C. Authority

D. Social proof

Correct Answer: D

QUESTION 12

Which of the following needs to be performed during a forensics investigation to ensure the data contained in a drive image has not been compromised?

A. Follow the proper chain of custody procedures.

B. Compare the image hash to the original hash.

C. Ensure a legal hold has been placed on the image.

D. Verify the time offset on the image file.

Correct Answer: B

Latest SY0-501 Dumps SY0-501 Practice Test SY0-501 Exam Questions

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

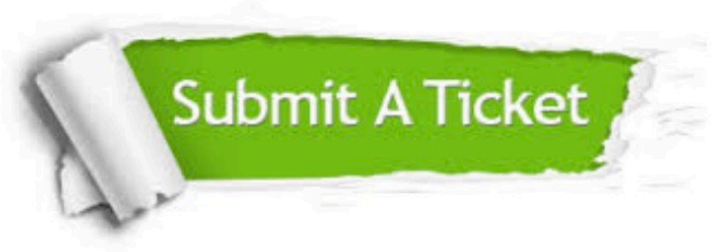
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.lead4pass.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © lead4pass, All Rights Reserved.