DUMPSARENA

CompTIA Security+

CompTIA SY0-501

Version Demo

Total Demo Questions: 20

Total Premium Questions: 1132

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1 - (HOTSPOT)

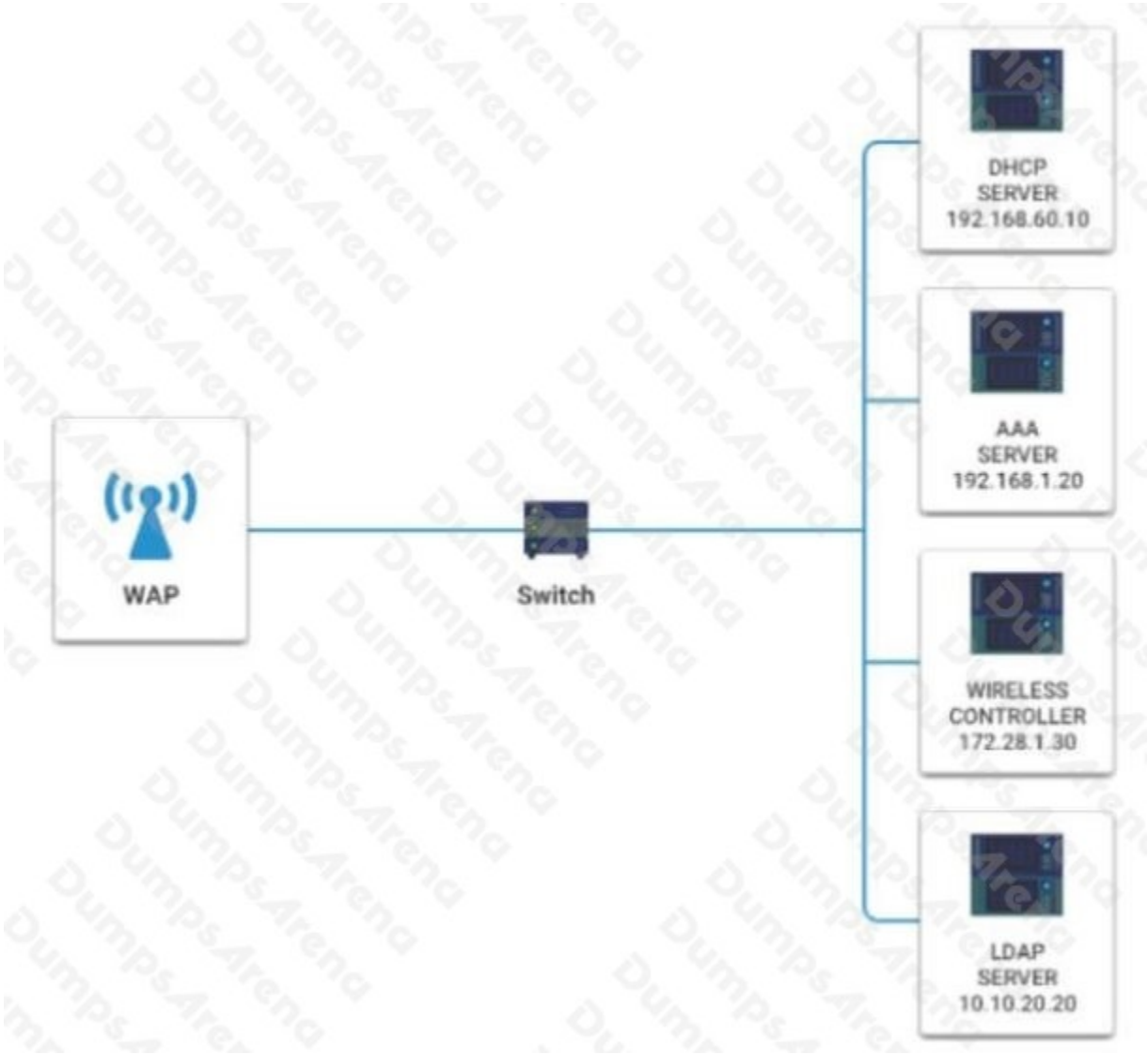
HOTSPOT

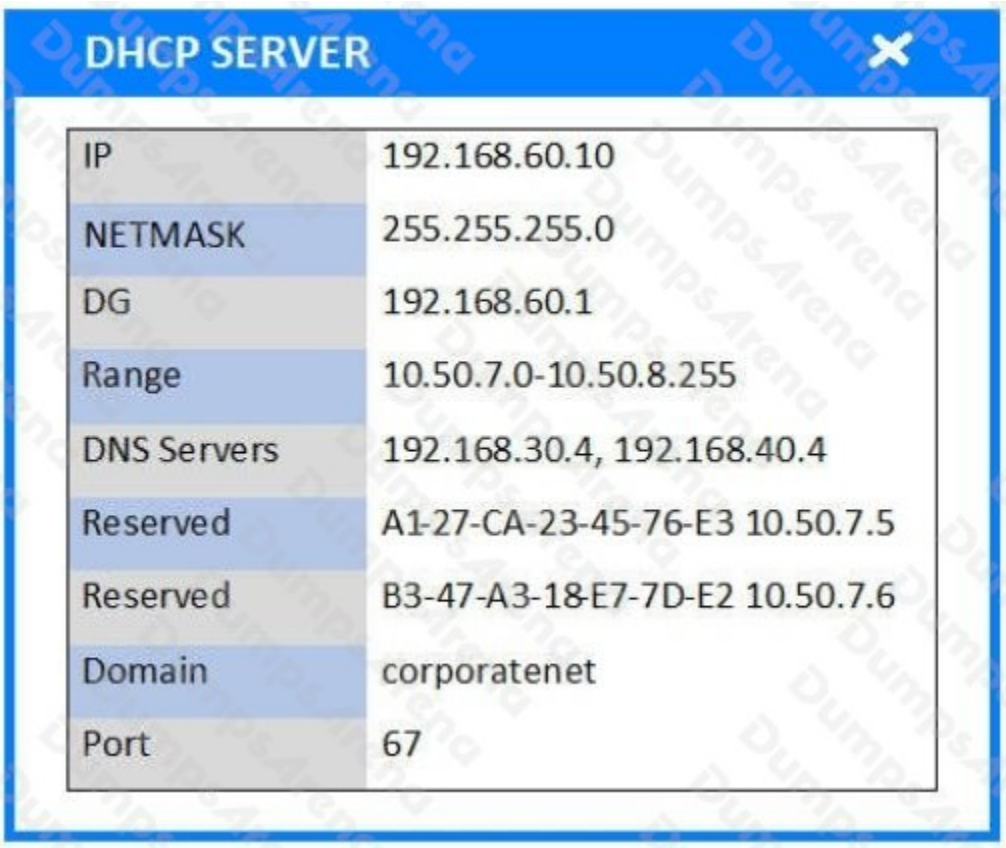
A newly purchased corporate WAP needs to be configured in the MOST secure manner possible. INSTRUCTIONS

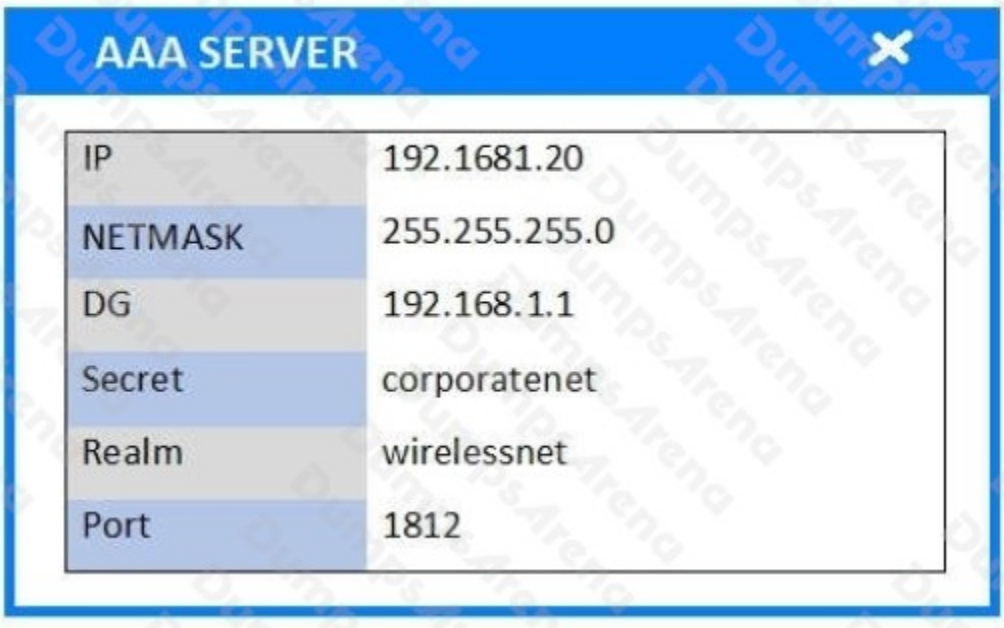
Please click on the below items on the network diagram and configure them accordingly:

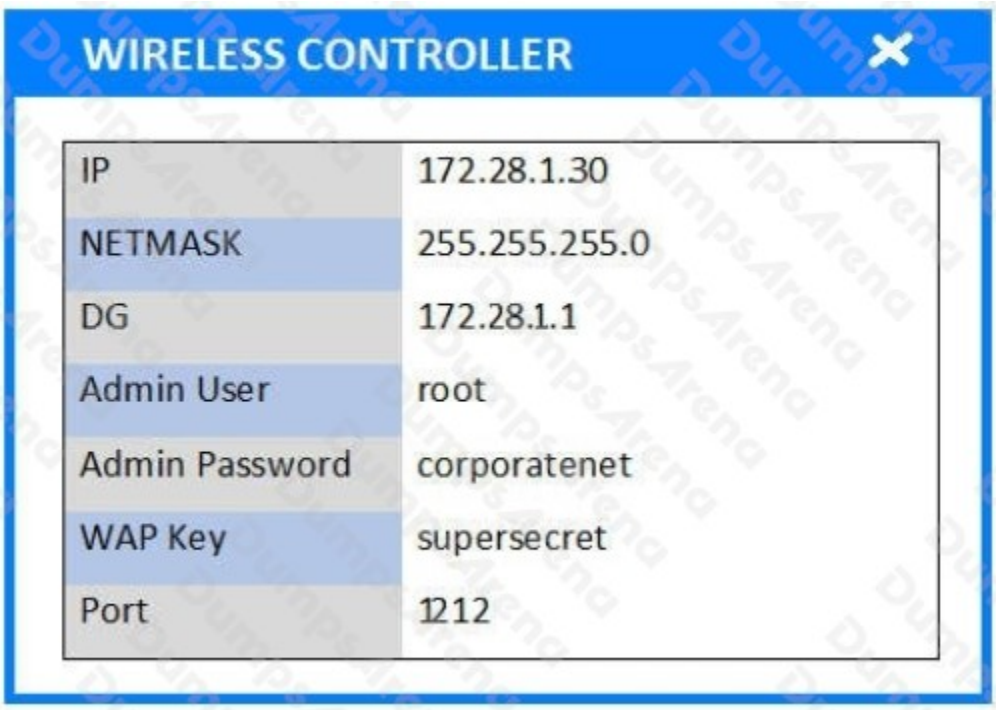
- WAP
- DHCP Server
- AAA Server
- Wireless Controller
- LDAP Server

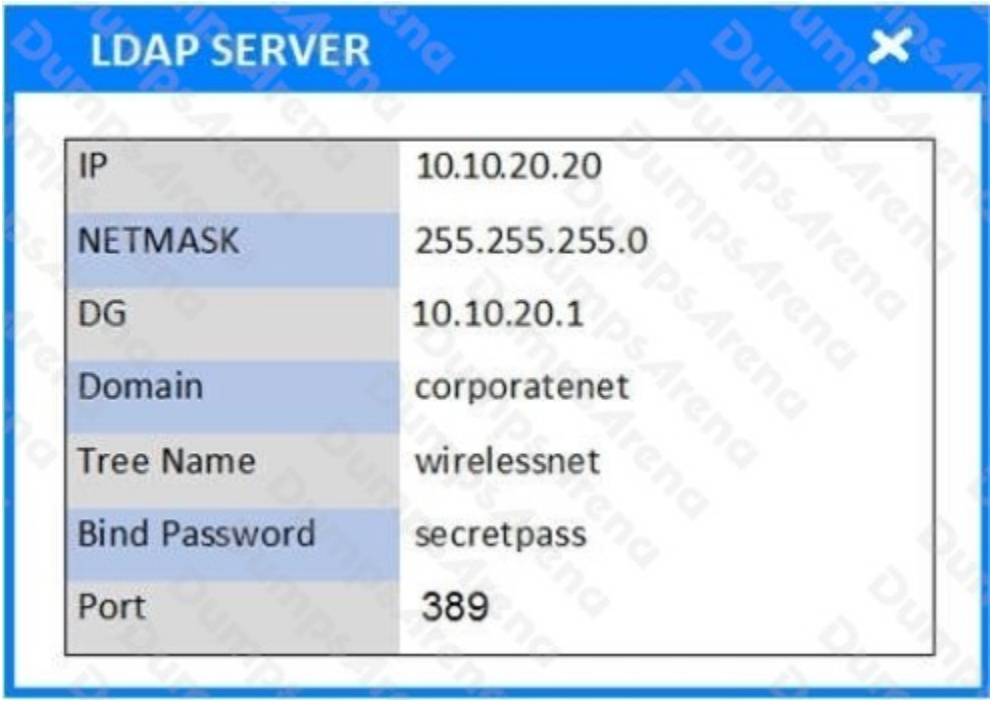
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


DHCP
SERVER
192.168.60.10
AAA
SERVER
192.168.1.20
WIRELESS
CONTROLLER
172.28.1.30
LDAP
SERVER
10.10.20.20
WAP
Switch


DHCP SERVER
IP
192.168.60.10
NETMASK
255.255.255.0
DG
192.168.60.1
Range
10.50.7.0-10.50.8.255
DNS Servers
192.168.30.4, 192.168.40.4
Reserved
A1-27-CA-23-45-76-E3 10.50.7.5
Reserved
B3-47-A3-18-E7-7D-E2 10.50.7.6
Domain
corporatenet
Port
67


AAA SERVER
IP
192.1681.20
NETMASK
255.255.255.0
DG
192.168.1.1
Secret
corporatenet
Realm
wirelessnet
Port
1812


WIRELESS CONTROLLER
IP
172.28.1.30
NETMASK
255.255.255.0
DG
172.28.1.1
Admin User
root
Admin Password
corporatenet
WAP Key
supersecret
Port
1212

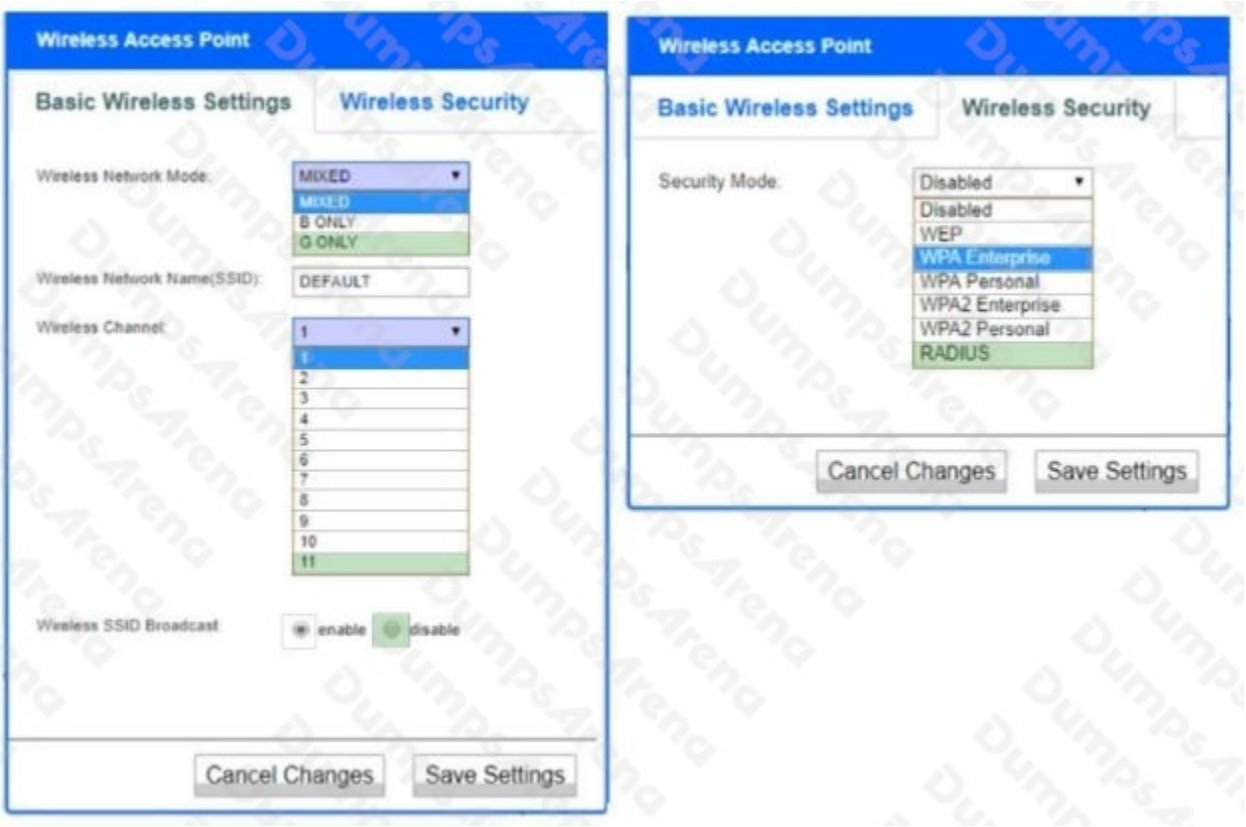

LDAP SERVER
IP
10.10.20.20
NETMASK
255.255.255.0
DG
10.10.20.1
Domain
corporatenet
Tree Name
wirelessnet
Bind Password
secretpass
Port
389

Hot Area:


Wireless Access Point
Basic Wireless Settings
Wireless Security
Wireless Network Mode:
MIXED
MIXED
B ONLY
G ONLY
Wireless Network Name(SSID):
DEFAULT
Wireless Channel:
1
1
2
3
4
5
6
7
8
9
10
11
Wireless SSID Broadcast
enable
disable
Cancel Changes
Save Settings


Wireless Access Point
Basic Wireless Settings
Wireless Security
Security Mode:
Disabled
Disabled
WEP
WPA Enterprise
WPA Personal
WPA2 Enterprise
WPA2 Personal
RADIUS
Cancel Changes
Save Settings

ANSWER:



Explanation:

QUESTION NO: 2

Which of the following AES modes of operation provide authentication? (Choose two.)

A. CCM

B. CBC

C. GCM

D. DSA

E. CFB

ANSWER: A C

QUESTION NO: 3

A penetration tester is checking to see if an internal system is vulnerable to an attack using a remote listener. Which of the following commands should the penetration tester use to verify if this vulnerability exists? (Choose two.)

A. tcpdump

B. nc

C. nmap

D. nslookup

E. tail

F. tracert

ANSWER: B C

QUESTION NO: 4

The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN.

Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted

B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance

C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files

D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

ANSWER: C

QUESTION NO: 5

Which of the following types of controls is a turnstile?

A. Physical

B. Detective

C. Corrective

D. Technical

ANSWER: A

QUESTION NO: 6

The security administrator has noticed cars parking just outside of the building fence line.

Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Choose two.)

A. Create a honeynet

B. Reduce beacon rate

C. Add false SSIDs

D. Change antenna placement

E. Adjust power level controls

F. Implement a warning banner

ANSWER: D E

QUESTION NO: 7

Which of the following are considered to be “something you do”? (Choose two.)

A. Iris scan

B. Handwriting

C. CAC card

D. Gait

E. PIN

F. Fingerprint

ANSWER: B D

QUESTION NO: 8

Which of the following implements two-factor authentication on a VPN?

A. Username, password, and source IP

B. Public and private keys

C. HOTP token and logon credentials

D. Source and destination IP addresses

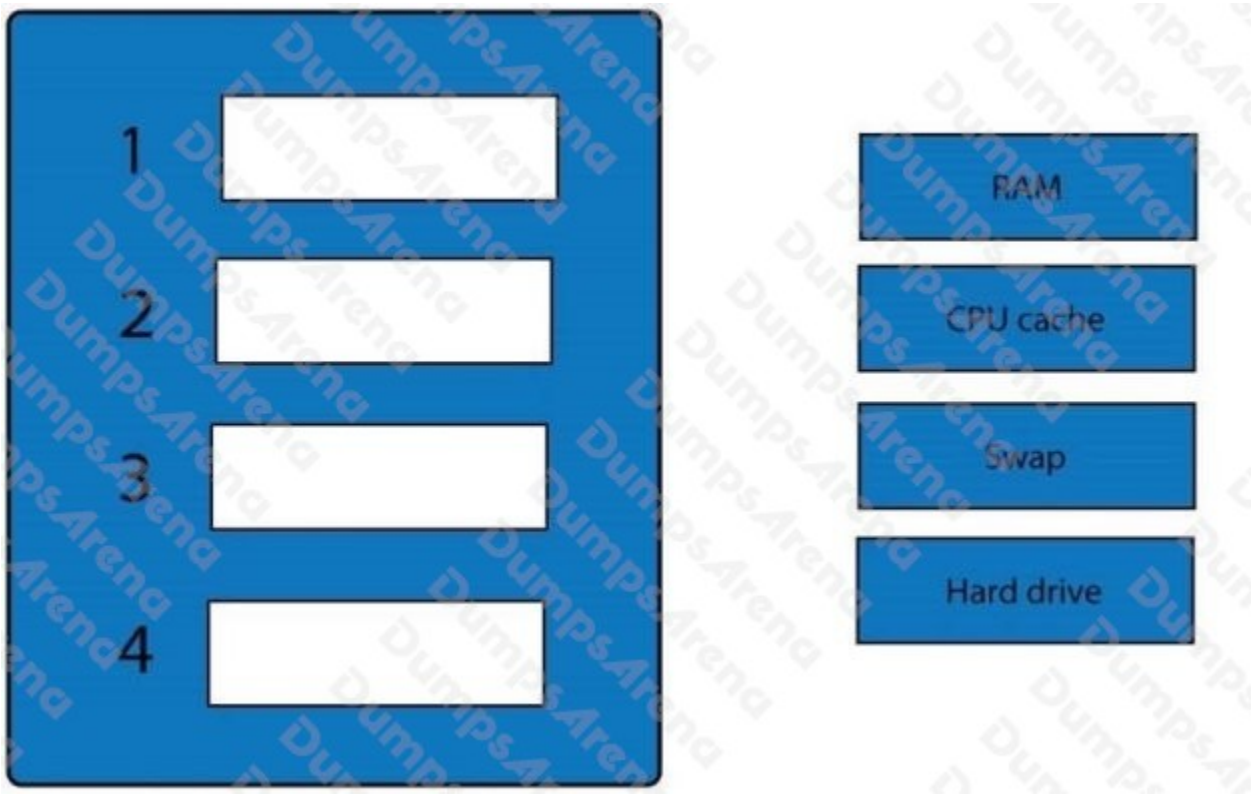
ANSWER: A

QUESTION NO: 9 - (DRAG DROP)

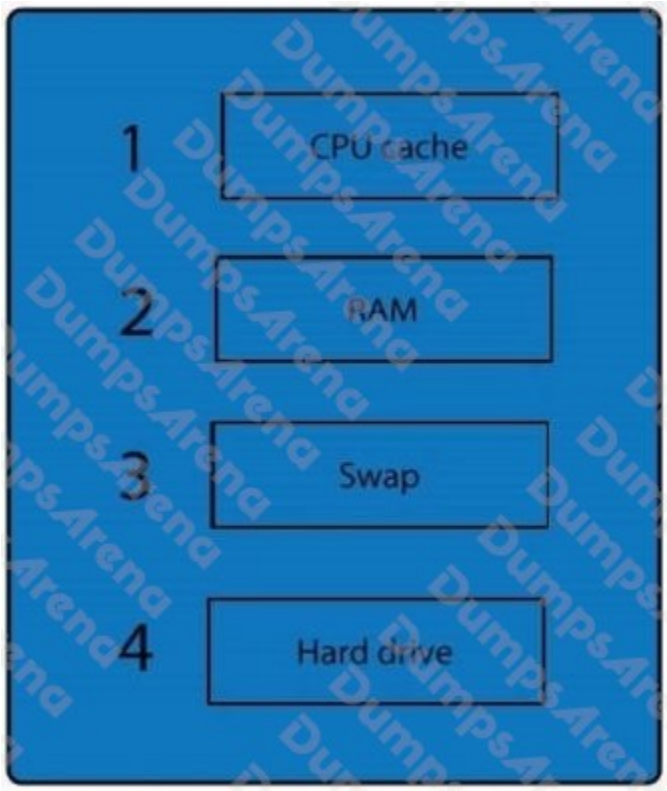
DRAG DROP

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

Select and Place:



ANSWER:



Explanation:

When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/ hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

QUESTION NO: 10

A systems administrator has been assigned to create accounts for summer interns. The interns are only authorized to be in the facility and operate computers under close supervision. They must also leave the facility at designated times each day. However, the interns can access intern file folders without supervision. Which of the following represents the BEST way to configure the accounts? (Choose two.)

A. Implement time-of-day restrictions.

B. Modify archived data.

C. Access executive shared portals.

D. Create privileged accounts.

E. Enforce least privilege.

ANSWER: A D

QUESTION NO: 11

Ann is the IS manager for several new systems in which the classifications of the systems' data are being decided. She is trying to determine the sensitivity level of the data being processed. Which of the following people should she consult to determine the data classification?

A. Steward

B. Custodian

C. User

D. Owner

ANSWER: D

QUESTION NO: 12

A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations.

Which of the following protocols would BEST facilitate secure file transfers? (Choose two.)

A. SCP

B. TFTP

C. SNMP

D. FTP

E. SMTP

F. FTPS

ANSWER: A F

QUESTION NO: 13

A systems administrator has installed a new UTM that is capable of inspecting SSL/TLS traffic for malicious payloads. All inbound network traffic coming from the Internet and terminating on the company’s secure web servers must be inspected. Which of the following configurations would BEST support this requirement?

A. The web servers’ CA full certificate chain must be installed on the UTM.

B. The UTM certificate pair must be installed on the web servers.

C. The web servers' private certificate must be installed on the UTM.

D. The UTM and web servers must use the same certificate authority.

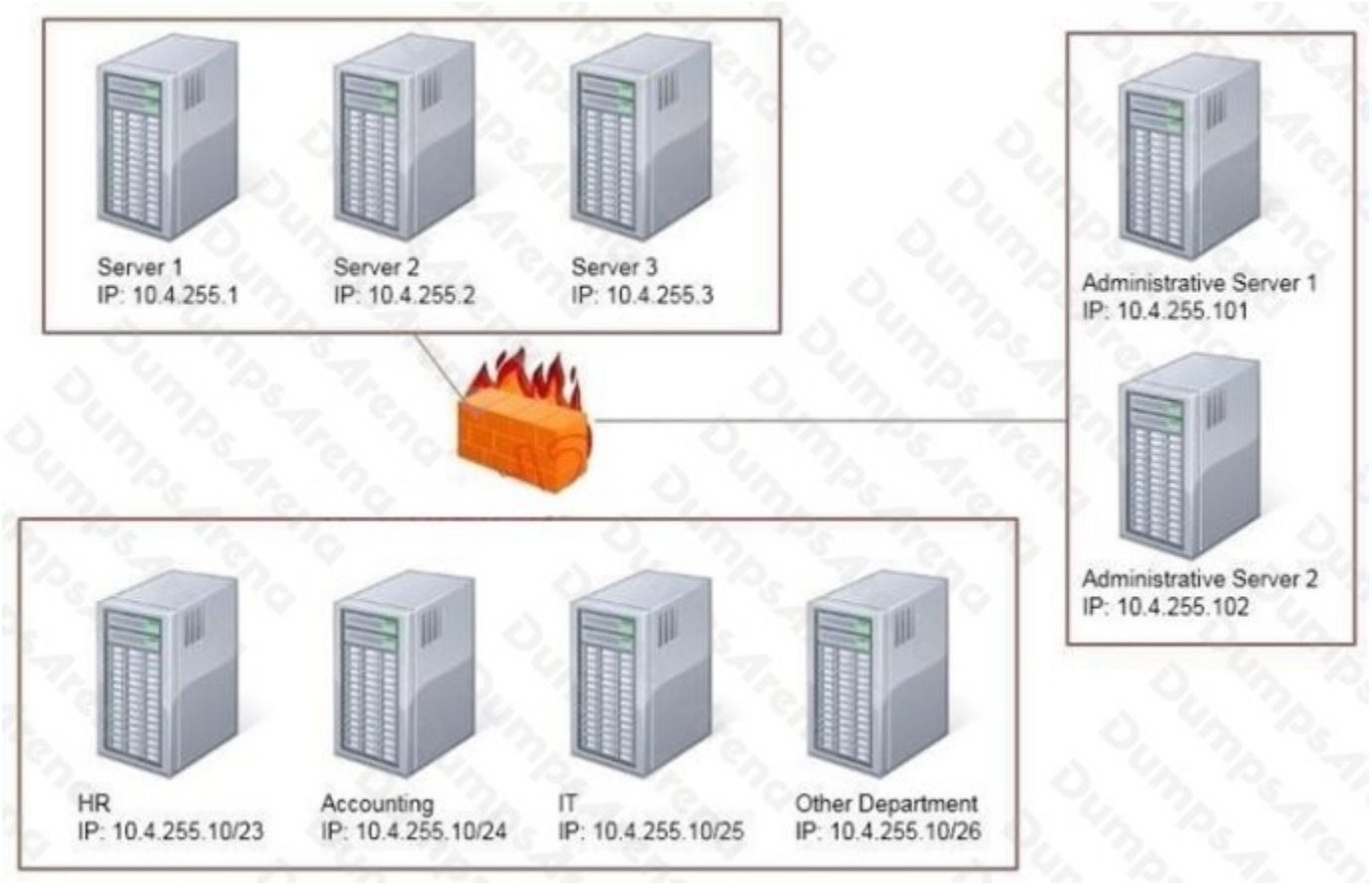
ANSWER: A

QUESTION NO: 14 - (SIMULATION)

SIMULATION

Task: Configure the firewall (fill out the table) to allow these four rules:

- Only allow the Accounting computer to have HTTPS access to the Administrative server.
- Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
- Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

ANSWER: See the solution below.

Explanation:

Use the following answer for this simulation task.

Below table has all the answers required for this question.

Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny
10.4.255.10/24	10.4.255.101	443	TCP	Allow
10.4.255.10/23	10.4.255.2	22	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? HTTPS and is a TCP port.

Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative

server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)

Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between:

10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)

10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

QUESTION NO: 15

A systems administrator wants to configure an enterprise wireless solution that supports authentication over HTTPS and wireless encryption using AES. Which of the following should the administrator configure to support these requirements? (Choose two.)

A. 802.1X

B. RADIUS federation

C. WPS

D. Captive portal

E. WPA2

F. WDS

ANSWER: A E

QUESTION NO: 16

Which of the following technologies employ the use of SAML? (Choose two.)

A. Single sign-on

B. Federation

C. LDAP

D. Secure token

E. RADIUS

ANSWER: A B

QUESTION NO: 17

A security analyst is working on a project that requires the implementation of a stream cipher. Which of the following should the analyst use?

A. Hash function

B. Elliptic curve

C. Symmetric algorithm

D. Public key cryptography

ANSWER: C

QUESTION NO: 18

Which of the following documents would provide specific guidance regarding ports and protocols that should be disabled on an operating system?

A. Regulatory requirements

B. Secure configuration guide

C. Application installation guides

D. User manuals

ANSWER: B

QUESTION NO: 19

Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

A. The recipient can verify integrity of the software patch.

B. The recipient can verify the authenticity of the site used to download the patch.

C. The recipient can request future updates to the software using the published MD5 value.

D. The recipient can successfully activate the new software patch.

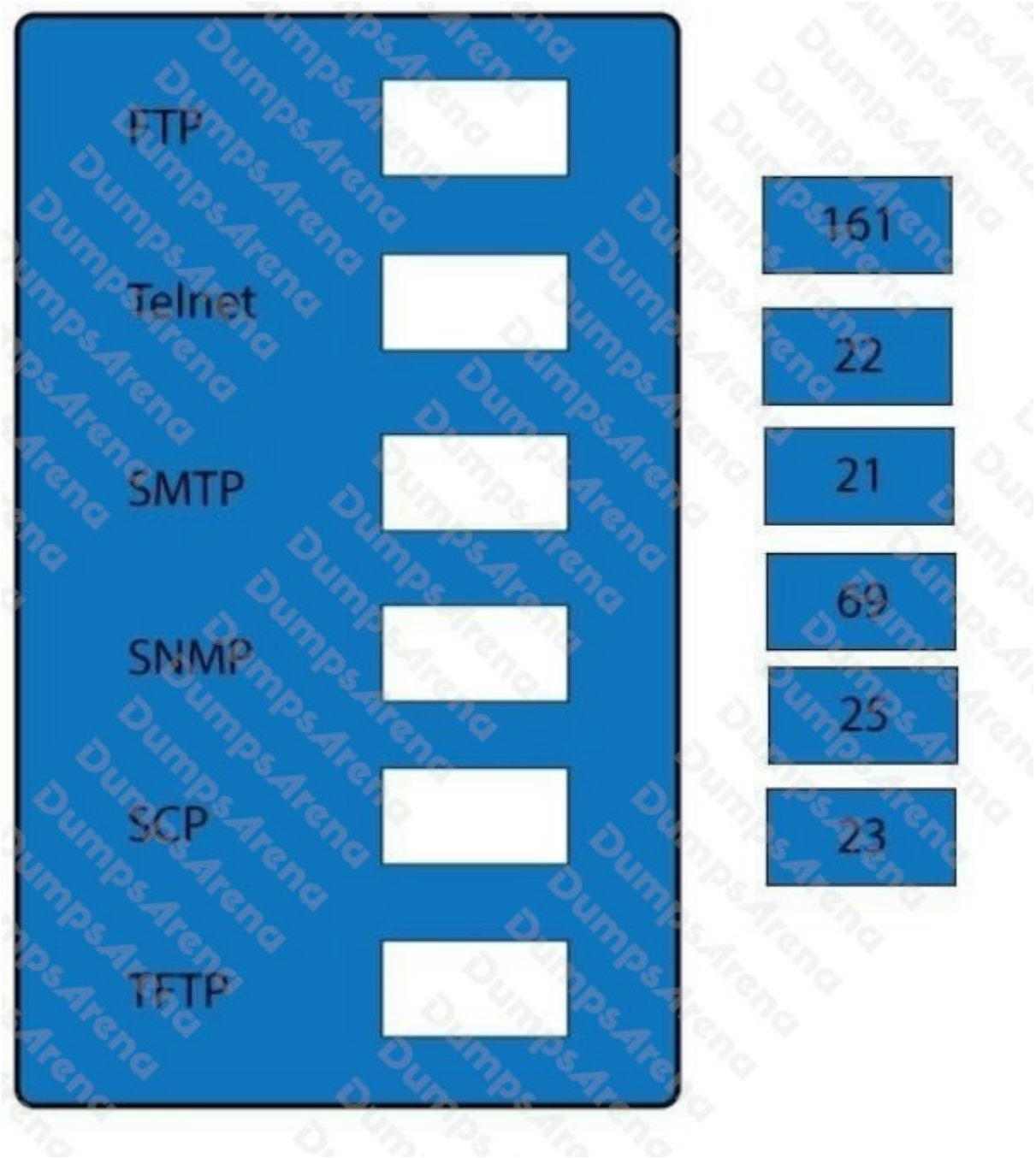
ANSWER: A

QUESTION NO: 20 - (DRAG DROP)

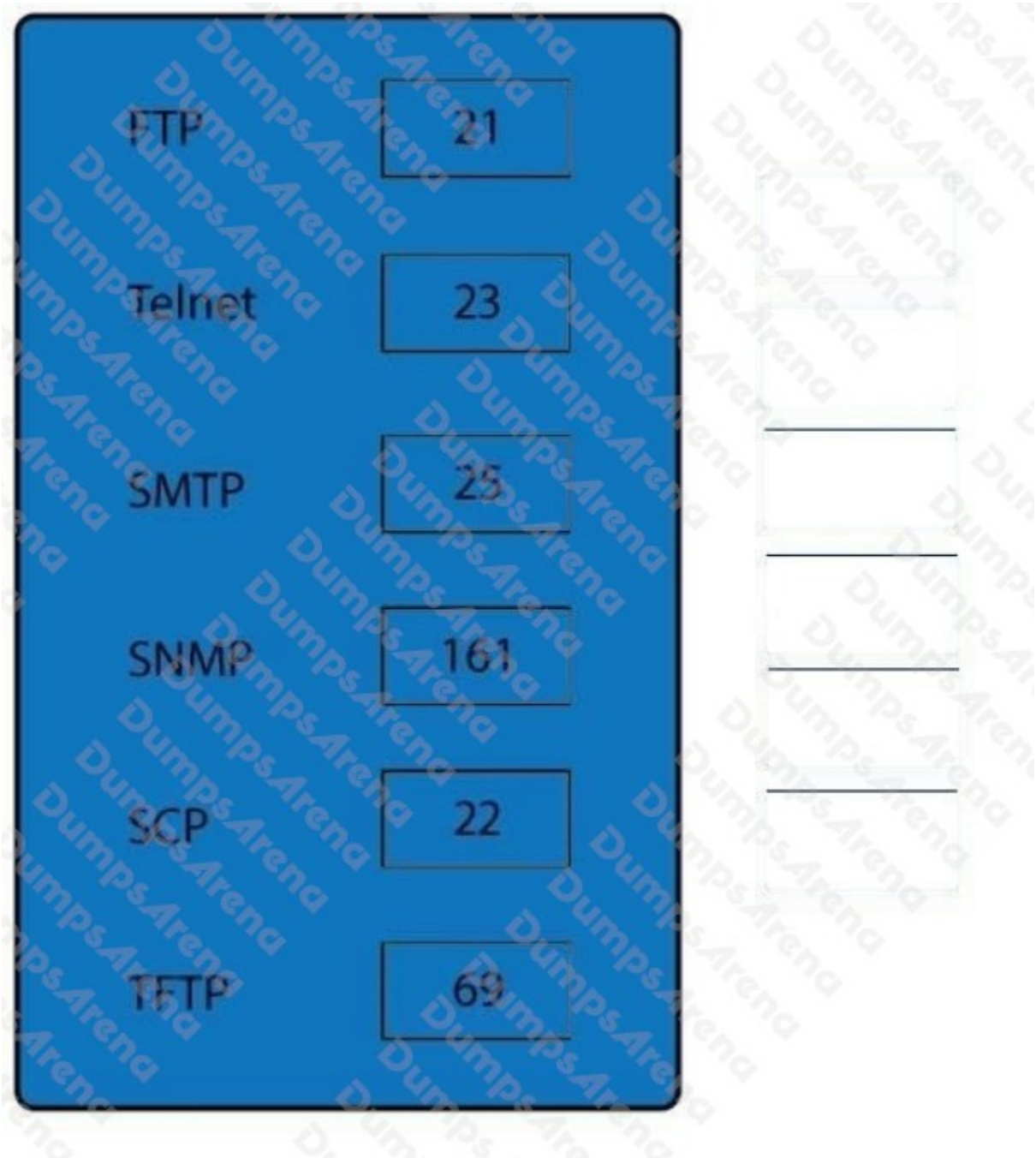
DRAG DROP

Drag and drop the correct protocol to its default port.

Select and Place:



ANSWER:



Explanation:

FTP uses TCP port 21. Telnet uses port 23.

SSH uses TCP port 22.

All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). SMTP uses TCP port 25. Port 69 is used by TFTP.

SNMP makes use of UDP ports 161 and 162. http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers