

➤ **Vendor: CompTIA**

➤ **Exam Code: SY0-601**

➤ **Exam Name: CompTIA Security+ Certification Exam**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [July/2021](#))**

[Visit Braindump2go and Download Full Version SY0-601 Exam Dumps](#)

QUESTION 315

A security operations analyst is using the company's SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an example of?

- A. Eradication 3
- B. Recovery
- C. Identification
- D. Preparation

Answer: C

QUESTION 316

A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?

- A. Fileless malware
- B. A downgrade attack
- C. A supply-chain attack
- D. A logic bomb
- E. Misconfigured BIOS

Answer: C

QUESTION 317

A hospital's administration is concerned about a potential loss of patient data that is stored on tablets. A security administrator needs to implement controls to alert the SOC any time the devices are near exits. Which of the following would BEST achieve this objective?

- A. Geotargeting
- B. Geolocation
- C. Geotagging
- D. Geofencing

Answer: D

QUESTION 318

A SOC is implementing an insider-threat-detection program. The primary concern is that users may be accessing

[SY0-601 Exam Dumps](#) [SY0-601 Exam Questions](#) [SY0-601 PDF Dumps](#) [SY0-601 VCE Dumps](#)

<https://www.braindump2go.com/sy0-601.html>

confidential data without authorization. Which of the following should be deployed to detect a potential insider threat?

- A. A honeyfile
- B. ADMZ
- C. DLP
- D. File integrity monitoring

Answer: A

QUESTION 319

A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

- A. A new firewall rule is needed to access the application.
- B. The system was quarantined for missing software updates.
- C. The software was not added to the application whitelist.
- D. The system was isolated from the network due to infected software.

Answer: C

QUESTION 320

A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?

- A. Dual power supplies
- B. A UPS
- C. A generator
- D. APDU

Answer: B

QUESTION 321

After a phishing scam for a user's credentials, the red team was able to craft a payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session. Which of the following types of attacks has occurred?

- A. Privilege escalation
- B. Session replay
- C. Application programming interface
- D. Directory traversal

Answer: A

QUESTION 322

A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted. Which of the following resiliency techniques was applied to the network to prevent this attack?

- A. NIC Teaming
- B. Port mirroring
- C. Defense in depth
- D. High availability

E. Geographic dispersal

Answer: C

QUESTION 323

A network administrator at a large organization is reviewing methods to improve the security of the wired LAN. Any security improvement must be centrally managed and allow corporate-owned devices to have access to the intranet but limit others to Internet access only. Which of the following should the administrator recommend?

- A. 802.1X utilizing the current PKI infrastructure
- B. SSO to authenticate corporate users
- C. MAC address filtering with ACLs on the router
- D. PAM for user account management

Answer: A

QUESTION 324

An organization is having difficulty correlating events from its individual AV, EDR, DLP, SWG, WAF, MOM, HIPS, and CASB systems. Which of the following is the BEST way to improve the situation?

- A. Remove expensive systems that generate few alerts.
- B. Modify the systems to alert only on critical issues.
- C. Utilize a SIEM to centralize logs and dashboards.
- D. Implement a new syslog/NetFlow appliance.

Answer: C

QUESTION 325

An attacker is attempting to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password, the login screen displays the following message:

`The username you entered does not exist.`

Which of the following should the analyst recommend be enabled?

- A. Input validation
- B. Obfuscation
- C. Error handling
- D. Username lockout

Answer: B

QUESTION 326

A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the MOST effective across heterogeneous platforms?

- A. Enforcing encryption
- B. Deploying GPOs
- C. Removing administrative permissions
- D. Applying MDM software

Answer: D

QUESTION 327

The cost of portable media and the security risks of transporting data have become too great for a laboratory. The laboratory has decided to interconnect with partner laboratories to make data transfers easier and more secure. The

[SY0-601 Exam Dumps](#) [SY0-601 Exam Questions](#) [SY0-601 PDF Dumps](#) [SY0-601 VCE Dumps](#)

<https://www.braindump2go.com/sy0-601.html>

Chief Security Officer (CSO) has several concerns about proprietary data being exposed once the interconnections are established.

Which of the following security features should the network administrator implement to prevent unwanted data exposure to users in partner laboratories?

- A. VLAN zoning with a file-transfer server in an external-facing zone
- B. DLP running on hosts to prevent file transfers between networks
- C. NAC that permits only data-transfer agents to move data between networks
- D. VPN with full tunneling and NAS authenticating through the Active Directory

Answer: B

QUESTION 328

A external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network.

Which of the following will BEST assist with this investigation?

- A. Perform a vulnerability scan to identify the weak spots.
- B. Use a packet analyzer to Investigate the NetFlow traffic.
- C. Check the SIEM to review the correlated logs.
- D. Require access to the routers to view current sessions.

Answer: C

QUESTION 329

The human resources department of a large online retailer has received multiple customer complaints about the rudeness of the automated chatbots It uses to interface and assist online shoppers. The system, which continuously learns and adapts, was working fine when it was installed a few months ago. Which of the following BEST describes the method being used to exploit the system?

- A. Baseline modification
- B. A fileless virus
- C. Tainted training data
- D. Cryptographic manipulation

Answer: C

QUESTION 330

Joe, a security analyst, recently performed a network discovery to fully understand his organization's electronic footprint from a "public" perspective. Joe ran a set of commands and received the following output:

```
Domain Name: COMPTIA.ORG
Registry Domain ID: 1234554321
Registrar Server: whois.networksolutions.com
Updated Date: 2018-12-01T05:08:11Z
Creation Date: 1998-02-26T05:00:00Z
Registrar Registration Expiration Date: 2021-02-25T05:00:00Z
Registrar: NETWORK SOLUTIONS, LLC
Registrar IANA ID: 2
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: YourBusiness Corporation
Registrant Organization: YourBusiness Corporation
Registrant Street: 500 Pennsylvania Ave
Registrant City: Downers Grove
Registrant State: IL
Registrant Postal Code: 11105
Registrant Country: US
Registrant Phone: 1 800 555 5555
Registrant Fax: 1 800 555 5556
Registrant Email: info@comptia.org
Admin: Jason Doe
Admin Organization: CompTIA
```

Which of the following can be determined about the organization's public presence and security posture? (Select TWO).

- A. Joe used Who is to produce this output.
- B. Joe used cURL to produce this output.
- C. Joe used Wireshark to produce this output
- D. The organization has adequate information available in public registration.
- E. The organization has too much information available in public registration.
- F. The organization has too little information available in public registration

Answer: AD

QUESTION 331

A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

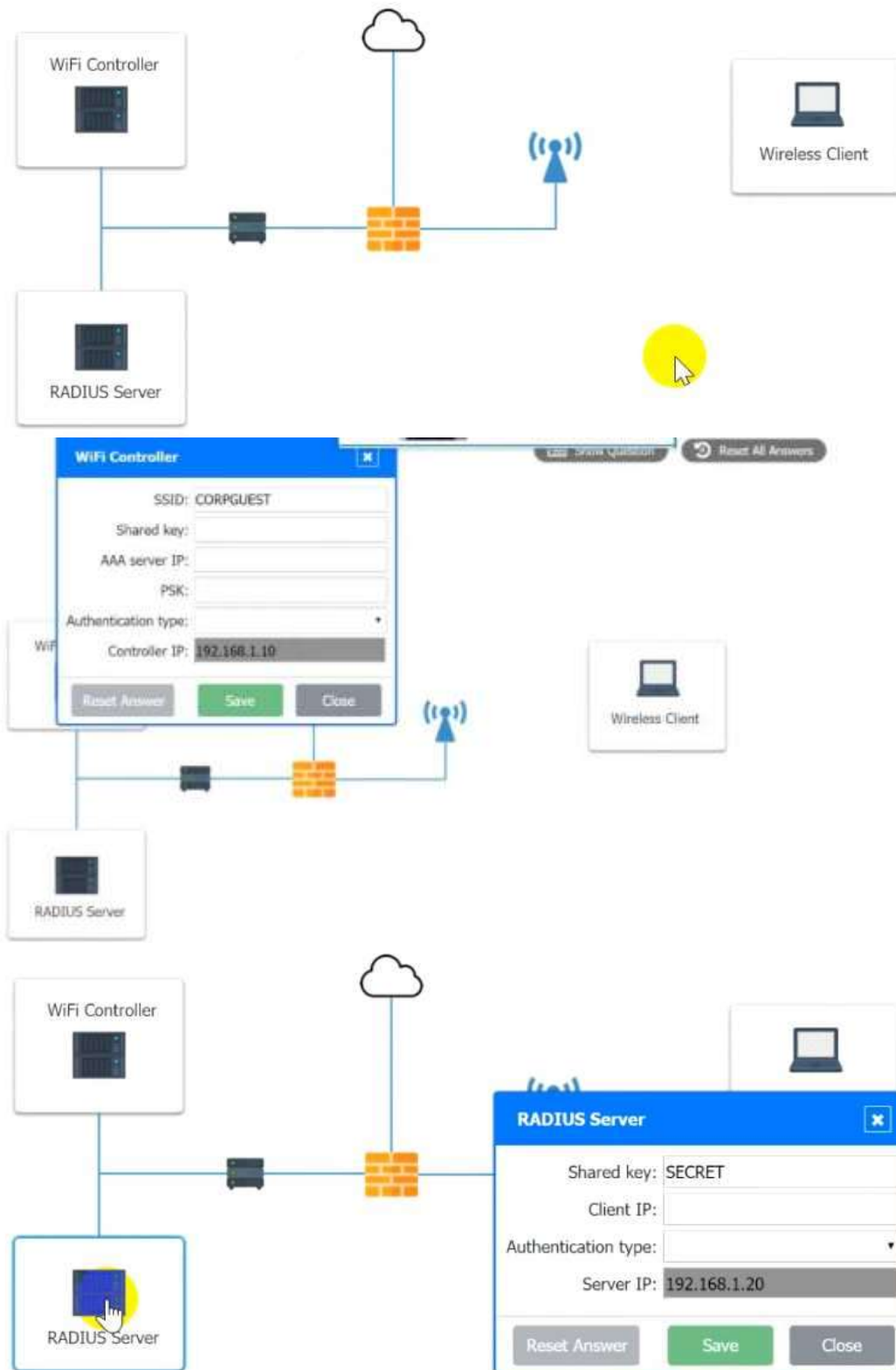
Perform the following steps:

1. Configure the RADIUS server.
2. Configure the WiFi controller.
3. Preconfigure the client for an incoming guest.

The guest AD credentials are:

User: guest01

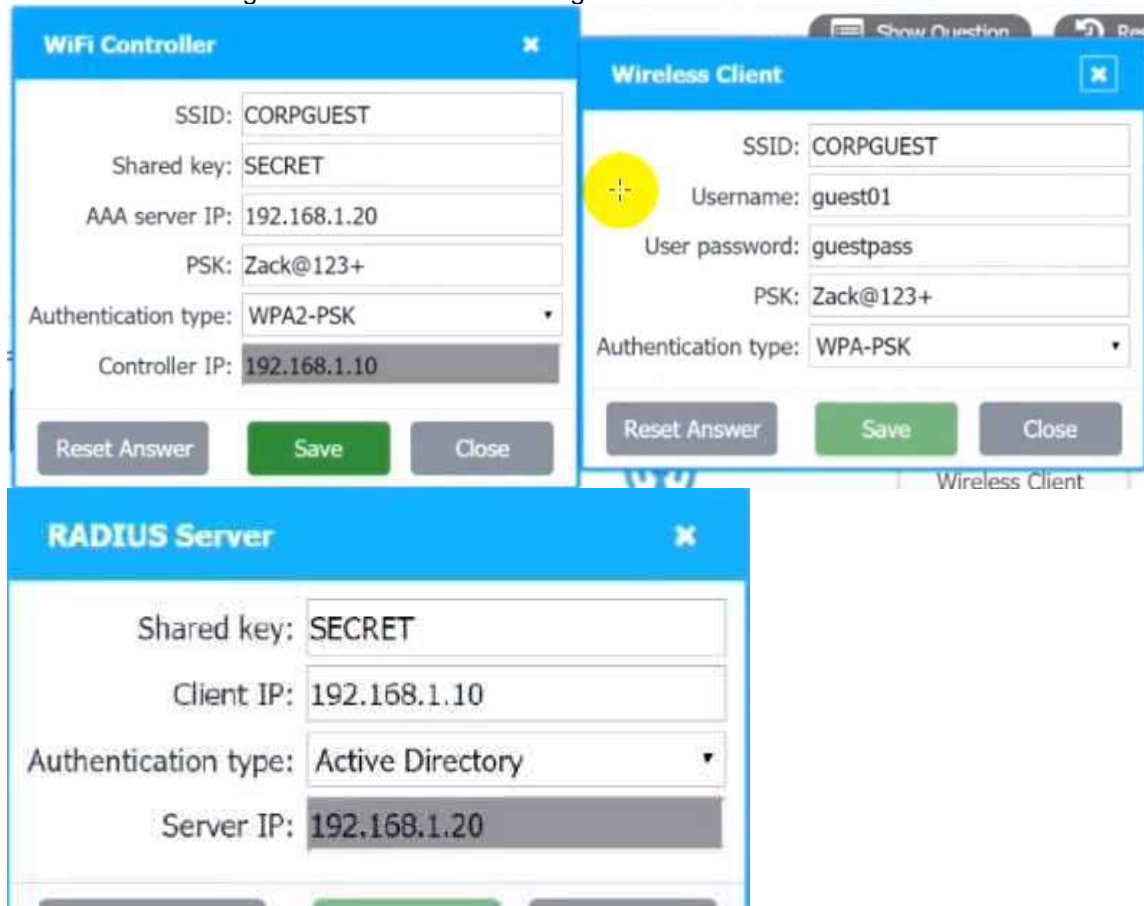
Password: guestpass





Answer:

Use the same settings as describe in below images.



WiFi Controller

SSID:	CORPGUEST
Shared key:	SECRET
AAA server IP:	192.168.1.20
PSK:	Zack@123+
Authentication type:	WPA2-PSK
Controller IP:	192.168.1.10

Wireless Client

SSID:	CORPGUEST
Username:	guest01
User password:	guestpass
PSK:	Zack@123+
Authentication type:	WPA-PSK

RADIUS Server

Shared key:	SECRET
Client IP:	192.168.1.10
Authentication type:	Active Directory
Server IP:	192.168.1.20

QUESTION 332

Hotspot Question

The security administration has installed a new firewall which implements an implicit DENY policy by default.

INSTRUCTIONS

Click on the firewall and configure it to allow ONLY the following communication:

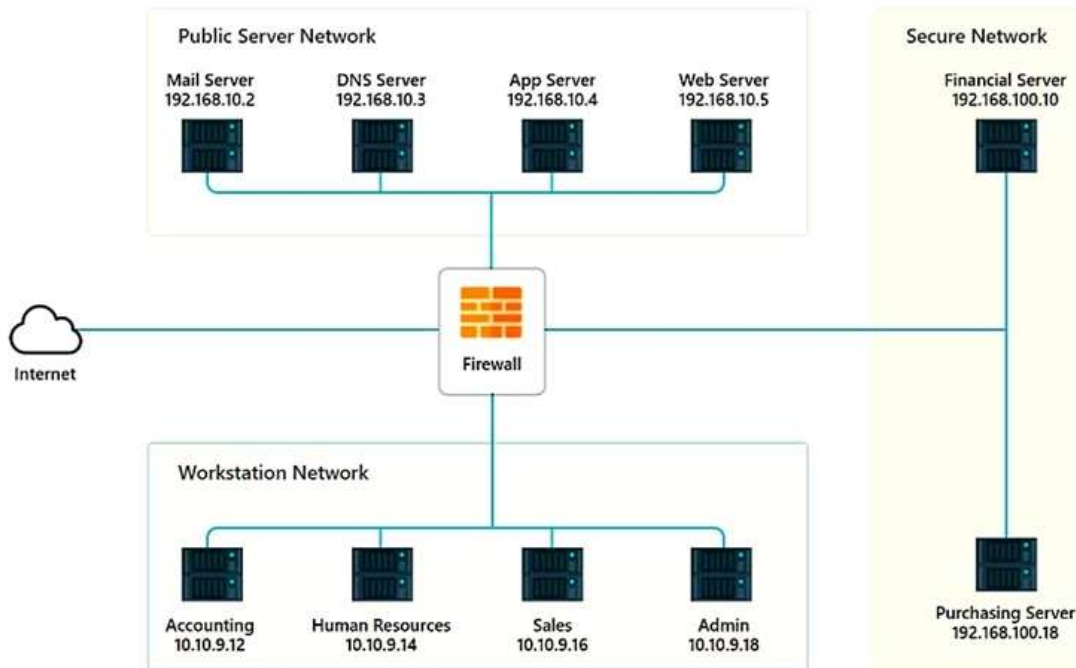
- The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
- The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port.
- The Admin workstation should ONLY be able to access the server on the secure network over the default TFTP port.

[SY0-601 Exam Dumps](#) [SY0-601 Exam Questions](#) [SY0-601 PDF Dumps](#) [SY0-601 VCE Dumps](#)

<https://www.braindump2go.com/sy0-601.html>

The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports.

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

Network Diagram

Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	<div>▼</div> <div>192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32</div>	<div>▼</div> <div>Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32</div>	<div>▼</div> <div>443 22 69</div>	<div>▼</div> <div>ANY TCP UDP</div>	<div>▼</div> <div>Permit Deny</div>
2	<div>▼</div> <div>192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32</div>	<div>▼</div> <div>Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32</div>	<div>▼</div> <div>443 22 69</div>	<div>▼</div> <div>ANY TCP UDP</div>	<div>▼</div> <div>Permit Deny</div>
3	<div>▼</div> <div>192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32</div>	<div>▼</div> <div>Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32</div>	<div>▼</div> <div>443 22 69</div>	<div>▼</div> <div>ANY TCP UDP</div>	<div>▼</div> <div>Permit Deny</div>
4	<div>▼</div> <div>192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32</div>	<div>▼</div> <div>Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32</div>	<div>▼</div> <div>443 22 69</div>	<div>▼</div> <div>ANY TCP UDP</div>	<div>▼</div> <div>Permit Deny</div>

Answer:

Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	192.168.10.2/32	Any	443	ANY	Permit
	192.168.10.3/32	192.168.10.2/32	22	TCP	Deny
	192.168.10.4/32	192.168.10.3/32	69	UDP	
	192.168.10.5/32	192.168.10.4/32			
	10.10.9.12/32	192.168.10.5/32			
	10.10.9.14/32	192.168.100.10/32			
	10.10.9.18/32	192.168.100.18/32			
2	192.168.10.2/32	Any	443	ANY	Permit
	192.168.10.3/32	192.168.10.2/32	22	TCP	Deny
	192.168.10.4/32	192.168.10.3/32	69	UDP	
	192.168.10.5/32	192.168.10.4/32			
	10.10.9.12/32	192.168.10.5/32			
	10.10.9.14/32	192.168.100.10/32			
	10.10.9.18/32	192.168.100.18/32			
3	192.168.10.2/32	Any	443	ANY	Permit
	192.168.10.3/32	192.168.10.2/32	22	TCP	Deny
	192.168.10.4/32	192.168.10.3/32	69	UDP	
	192.168.10.5/32	192.168.10.4/32			
	10.10.9.12/32	192.168.10.5/32			
	10.10.9.14/32	192.168.100.10/32			
	10.10.9.18/32	192.168.100.18/32			
4	192.168.10.2/32	Any	443	ANY	Permit
	192.168.10.3/32	192.168.10.2/32	22	TCP	Deny
	192.168.10.4/32	192.168.10.3/32	69	UDP	
	192.168.10.5/32	192.168.10.4/32			
	10.10.9.12/32	192.168.10.5/32			
	10.10.9.14/32	192.168.100.10/32			
	10.10.9.18/32	192.168.100.18/32			

Explanation:

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default.

Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443.

Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port 22

Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69.

QUESTION 333

An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization MOST likely consult?

[SY0-601 Exam Dumps](#) [SY0-601 Exam Questions](#) [SY0-601 PDF Dumps](#) [SY0-601 VCE Dumps](#)

<https://www.braindump2go.com/sy0-601.html>

- A. The business continuity plan
- B. The disaster recovery plan
- C. The communications plan
- D. The incident response plan

Answer: A

QUESTION 334

An organization recently recovered from a data breach. During the root cause analysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following solutions should the organization implement to reduce the likelihood of future data breaches?

- A. MDM
- B. MAM
- C. VDI
- D. DLP

Answer: A

QUESTION 335

An organization relies on third-party video conferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources.

Which of the following would BEST maintain high-quality video conferencing while minimizing latency when connected to the VPN?

- A. Using geographic diversity to have VPN terminators closer to end users
- B. Utilizing split tunneling so only traffic for corporate resources is encrypted
- C. Purchasing higher-bandwidth connections to meet the increased demand
- D. Configuring QoS properly on the VPN accelerators

Answer: D