

# Exam Questions SY0-601

CompTIA Security+ Exam

<https://www.2passeasy.com/dumps/SY0-601/>



#### NEW QUESTION 1

A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

- A. SPIM
- B. Vishing
- C. Spear phishing
- D. Smishing

**Answer:** D

#### NEW QUESTION 2

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

- > Check-in/checkout of credentials
- > The ability to use but not know the password
- > Automated password changes
- > Logging of access to credentials

Which of the following solutions would meet the requirements?

- A. OAuth 2.0
- B. Secure Enclave
- C. A privileged access management system
- D. An OpenID Connect authentication system

**Answer:** D

#### NEW QUESTION 3

Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

- A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
- B. The document is a backup file if the system needs to be recovered.
- C. The document is a standard file that the OS needs to verify the login credentials.
- D. The document is a keylogger that stores all keystrokes should the account be compromised.

**Answer:** A

#### NEW QUESTION 4

A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

- A. Segmentation
- B. Firewall whitelisting
- C. Containment
- D. isolation

**Answer:** A

#### NEW QUESTION 5

A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

- A. Implement open PSK on the APs
- B. Deploy a WAF
- C. Configure WIPS on the APs
- D. Install a captive portal

**Answer:** D

#### NEW QUESTION 6

A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

- A. Security
- B. Application
- C. Dump
- D. Syslog

**Answer:** C

#### NEW QUESTION 7

Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical

space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

- A. The employee's physical access card was cloned.
- B. The employee is colluding with human resources
- C. The employee's biometrics were harvested
- D. A criminal used lock picking tools to open the door.

**Answer:** A

#### NEW QUESTION 8

A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

- A. AH
- B. ESP
- C. SRTP
- D. LDAP

**Answer:** B

#### NEW QUESTION 9

Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

- A. SIEM
- B. CASB
- C. UTM
- D. DLP

**Answer:** D

#### NEW QUESTION 10

A startup company is using multiple SaaS and IaaS platform to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

- A. SIEM
- B. DLP
- C. CASB
- D. SWG

**Answer:** C

#### NEW QUESTION 10

A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

- A. Man-in-the middle
- B. Spear-phishing
- C. Evil twin
- D. DNS poisoning

**Answer:** D

#### NEW QUESTION 15

To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

- A. A password reuse policy
- B. Account lockout after three failed attempts
- C. Encrypted credentials in transit
- D. A geofencing policy based on login history

**Answer:** C

#### NEW QUESTION 16

Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and it has continued to evade detection. Which of the following should administrator implement to protect the environment from this malware?

- A. Install a definition-based antivirus.
- B. Implement an IDS/IPS
- C. Implement a heuristic behavior-detection solution.
- D. Implement CASB to protect the network shares.

**Answer:** C

#### NEW QUESTION 20

A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

- A. Perform a site survey
- B. Deploy an FTK Imager
- C. Create a heat map
- D. Scan for rogue access points
- E. Upgrade the security protocols
- F. Install a captive portal

**Answer:** AC

#### NEW QUESTION 21

A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes database resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

- A. Upgrade the bandwidth available into the datacenter
- B. Implement a hot-site failover location
- C. Switch to a complete SaaS offering to customers
- D. Implement a challenge response test on all end-user queries

**Answer:** B

#### NEW QUESTION 24

A worldwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

- A. Network location
- B. Impossible travel time
- C. Geolocation
- D. Geofencing

**Answer:** D

#### NEW QUESTION 26

Which of the following refers to applications and systems that are used within an organization without consent or approval?

- A. Shadow IT
- B. OSINT
- C. Dark web
- D. Insider threats

**Answer:** A

#### NEW QUESTION 27

A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

- A. The scan results show open ports, protocols, and services exposed on the target host
- B. The scan enumerated software versions of installed programs
- C. The scan produced a list of vulnerabilities on the target host
- D. The scan identified expired SSL certificates

**Answer:** B

#### NEW QUESTION 29

A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

- A. Dual power supply
- B. Off-site backups
- C. Automatic OS upgrades
- D. NIC teaming
- E. Scheduled penetration testing
- F. Network-attached storage

**Answer:** AB

#### NEW QUESTION 31

A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

- A. Credential harvesting
- B. Keylogger
- C. Brute-force
- D. Spraying

**Answer:** D

#### NEW QUESTION 36

Which of the following describes the ability of code to target a hypervisor from inside

- A. Fog computing
- B. VM escape
- C. Software-defined networking
- D. Image forgery
- E. Container breakout

**Answer:** B

#### NEW QUESTION 40

An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

- A. An external security assessment
- B. A bug bounty program
- C. A tabletop exercise
- D. A red-team engagement

**Answer:** C

#### NEW QUESTION 42

Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

- A. An ARO
- B. An MOU
- C. An SLA
- D. A BPA

**Answer:** B

#### NEW QUESTION 45

A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

- A. validate the vulnerability exists in the organization's network through penetration testing
- B. research the appropriate mitigation techniques in a vulnerability database
- C. find the software patches that are required to mitigate a vulnerability
- D. prioritize remediation of vulnerabilities based on the possible impact.

**Answer:** D

#### NEW QUESTION 47

A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?



- A. Configuring signature-based antivirus to update every 30 minutes
- B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.
- C. Implementing application execution in a sandbox for unknown software.
- D. Fuzzing new files for vulnerabilities if they are not digitally signed

**Answer:** C

#### NEW QUESTION 50

Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth to be provided to confirm Joe's identity before sending him the prize. Which of the following BEST describes this type of email?

- A. Spear phishing
- B. Whaling
- C. Phishing
- D. Vishing

**Answer:** C

#### NEW QUESTION 52

A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

- A. Loss of proprietary information
- B. Damage to the company's reputation
- C. Social engineering
- D. Credential exposure

**Answer:** C

#### NEW QUESTION 54

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

- A. Nmap
- B. Wireshark
- C. Autopsy
- D. DNSEnum

**Answer:** A

#### NEW QUESTION 59

Which of the following would MOST likely support the integrity of a voting machine?

- A. Asymmetric encryption
- B. Blockchain
- C. Transport Layer Security
- D. Perfect forward secrecy

**Answer:** D

#### NEW QUESTION 64

A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

- A. SDP
- B. AAA
- C. IaaS
- D. MSSP
- E. Microservices

**Answer:** D

#### NEW QUESTION 67

A security administrator checks the table of a network switch, which shows the following output:

VLAN	Physical address	Type	Port
1	001a:42ff:5113	Dynamic	GE0/5
1	0faa:abcf:ddee	Dynamic	GE0/5
1	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa:b6a3:1212	Dynamic	GE0/5
1	8025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

- A. MAC Flooding
- B. DNS poisoning
- C. MAC cloning
- D. ARP poisoning

**Answer:** A

#### NEW QUESTION 70

After entering a username and password, and administrator must gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

- A. Multifactor authentication
- B. Something you can do
- C. Biometric
- D. Two-factor authentication

**Answer:** D

#### NEW QUESTION 72

A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

- A. The GPS location
- B. When the file was deleted
- C. The total number of print jobs
- D. The number of copies made

**Answer:** A

#### NEW QUESTION 77

A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

- A. OAuth
- B. SSO
- C. SAML
- D. PAP

**Answer:** C

#### NEW QUESTION 80

A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

A)

```
http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
```

B)

```
http://sample.url.com/someotherpageonsite/../../../../etc/shadow
```

C)

```
http://sample.url.com/select-from-database-where-password-null
```

D)

```
http://redirect.sample.url.sampleurl.com/malicious-dns-redirect
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** B

#### NEW QUESTION 84

A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

- A. Security information and event management
- B. A web application firewall

- C. A vulnerability scanner
- D. A next-generation firewall

**Answer:** A

#### NEW QUESTION 85

Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?

- A. DDoS
- B. Man-in-the-middle
- C. MAC flooding
- D. Domain hijacking

**Answer:** A

#### NEW QUESTION 86

Which of the following disaster recovery tests is The LEAST time-consuming for the disaster recovery team?

- A. Tabletop
- B. Parallel
- C. Full interruption
- D. Simulation

**Answer:** D

#### NEW QUESTION 91

A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

- A. Corrective
- B. Physical
- C. Detective
- D. Administrative

**Answer:** C

#### NEW QUESTION 95

A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:

<http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us>

The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:

<http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us> Which of the following application attacks is being tested?

- A. Pass-the-hash
- B. Session replay
- C. Object deference
- D. Cross-site request forgery

**Answer:** B

#### NEW QUESTION 97

In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

- A. Identification
- B. Preparation
- C. Eradiction
- D. Recovery
- E. Containment

**Answer:** E

#### NEW QUESTION 98

In which of the following common use cases would steganography be employed?

- A. Obfuscation
- B. Integrity
- C. Non-repudiation
- D. Blockchain

**Answer:** A

#### NEW QUESTION 103

The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected



host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

- A. Updating the playbooks with better decision points
- B. Dividing the network into trusted and untrusted zones
- C. Providing additional end-user training on acceptable use
- D. Implementing manual quarantining of infected hosts

Answer: A

#### NEW QUESTION 105

A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

- A. OSINT
- B. SIEM
- C. CVSS
- D. CVE

Answer: D

#### NEW QUESTION 107

The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

- A. Limit the use of third-party libraries.
- B. Prevent data exposure queries.
- C. Obfuscate the source code.
- D. Submit the application to QA before releasing it.

Answer: D

#### NEW QUESTION 112

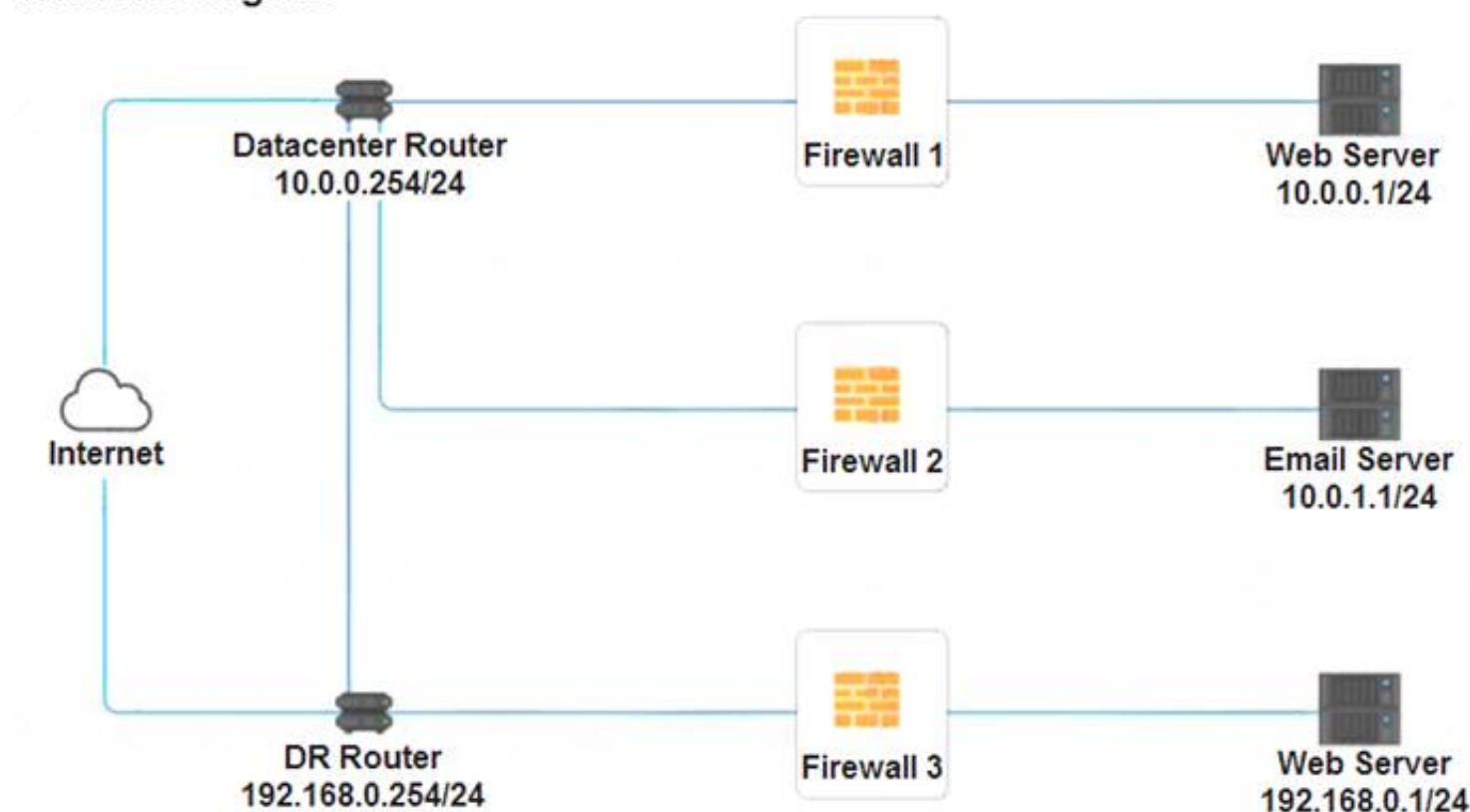
A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites. INSTRUCTIONS  
 Click on each firewall to do the following:

- > Deny cleartext web traffic.
- > Ensure secure management protocols are used.
- > Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

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 1

Rule Name	Source	Destination	Service	Action
DNS Rule	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  DNS  HTTP  HTTPS  TELNET  SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT  DENY </div>
HTTPS Outbound	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  DNS  HTTP  HTTPS  TELNET  SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT  DENY </div>
Management	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  DNS  HTTP  HTTPS  TELNET  SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT  DENY </div>
HTTPS Inbound	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  DNS  HTTP  HTTPS  TELNET  SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT  DENY </div>
HTTP Inbound	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  DNS  HTTP  HTTPS  TELNET  SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT  DENY </div>

Reset Answer
Save
Close

Firewall 2

Rule Name	Source	Destination	Service	Action
DNS Rule	<div> <div></div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div></div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div></div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div> <div></div> <div> PERMIT DENY </div> </div>
HTTPS Outbound	<div> <div></div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div></div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div></div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div> <div></div> <div> PERMIT DENY </div> </div>
Management	<div> <div></div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div></div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div></div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div> <div></div> <div> PERMIT DENY </div> </div>
HTTPS Inbound	<div> <div></div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div></div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div></div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div> <div></div> <div> PERMIT DENY </div> </div>
HTTP Inbound	<div> <div></div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div></div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div></div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div> <div></div> <div> PERMIT DENY </div> </div>

Reset Answer
Save
Close



Firewall 3

Rule Name	Source	Destination	Service	Action
DNS Rule	<div> <div></div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div> <div></div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div> <div></div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div> <div></div> <div>PERMIT DENY</div> </div>
HTTPS Outbound	<div> <div></div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div> <div></div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div> <div></div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div> <div></div> <div>PERMIT DENY</div> </div>
Management	<div> <div></div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div> <div></div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div> <div></div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div> <div></div> <div>PERMIT DENY</div> </div>
HTTPS Inbound	<div> <div></div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div> <div></div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div> <div></div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div> <div></div> <div>PERMIT DENY</div> </div>
HTTP Inbound	<div> <div></div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div> <div></div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div> <div></div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div> <div></div> <div>PERMIT DENY</div> </div>

Reset Answer
Save
Close

A.

**Answer:** A

**Explanation:**

See explanation below.

Explanation

Firewall 1:

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</div> <div>Save</div> <div>Close</div>				

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</div> <div>Save</div> <div>Close</div>				

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Firewall 2:

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</div> <div>Save</div> <div>Close</div>				



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

Firewall 3:

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

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

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

#### NEW QUESTION 117

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO).

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

Answer: AE

#### NEW QUESTION 118

Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

- A. Data encryption
- B. Data masking
- C. Anonymization
- D. Tokenization

**Answer:** A

#### NEW QUESTION 121

After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

- A. The vulnerability scan output
- B. The IDS logs
- C. The full packet capture data
- D. The SIEM alerts

**Answer:** A

#### NEW QUESTION 122

An organization just experienced a major cyberattack modern. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?

- A. Shadow IT
- B. An insider threat
- C. A hacktivist
- D. An advanced persistent threat

**Answer:** D

#### NEW QUESTION 125

A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

- A. One-time passwords
- B. Email tokens
- C. Push notifications
- D. Hardware authentication

**Answer:** C

#### NEW QUESTION 129

A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

- A. Containerization
- B. Geofencing
- C. Full-disk encryption
- D. Remote wipe

**Answer:** C

#### NEW QUESTION 130

A security administrator needs to create a RAIS configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drives will fail simultaneously. Which of the following RAID configurations should the administration use?

- A. RA1D 0
- B. RAID1
- C. RAID 5
- D. RAID 10

**Answer:** C

#### NEW QUESTION 133

Which of the following types of controls is a turnstile?

- A. Physical
- B. Detective
- C. Corrective
- D. Technical

**Answer:** A

#### NEW QUESTION 135

A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

- A. Mobile device management
- B. Full-device encryption
- C. Remote wipe
- D. Biometrics

**Answer:** A

#### NEW QUESTION 139

A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to account to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

- A. Create consultant accounts for each region, each configured with push MFA notifications.
- B. Create one global administrator account and enforce Kerberos authentication
- C. Create different accounts for each regio
- D. limit their logon times, and alert on risky logins
- E. Create a guest account for each regio
- F. remember the last ten passwords, and block password reuse

**Answer:** C

#### NEW QUESTION 141

A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices the following requirements must be met:

- Mobile device OSs must be patched up to the latest release
- A screen lock must be enabled (passcode or biometric)
- Corporate data must be removed if the device is reported lost or stolen

Which of the following controls should the security engineer configure? (Select TWO)

- A. Containerization
- B. Storage segmentation
- C. Posturing
- D. Remote wipe
- E. Full-device encryption
- F. Geofencing

**Answer:** DE

#### NEW QUESTION 145

A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

- A. Discretionary
- B. Rule-based
- C. Role-based
- D. Mandatory

**Answer:** D

#### NEW QUESTION 149

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

- A. VPN
- B. Drive encryption
- C. Network firewall
- D. File level encryption
- E. USB blocker
- F. MFA

**Answer:** BE

#### NEW QUESTION 150

Which of the following ISO standards is certified for privacy?

- A. ISO 9001
- B. ISO 27002
- C. ISO 27701
- D. ISO 31000

**Answer:** C

#### NEW QUESTION 155

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SY0-601 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SY0-601 Product From:

<https://www.2passeasy.com/dumps/SY0-601/>

## Money Back Guarantee

### **SY0-601 Practice Exam Features:**

- \* SY0-601 Questions and Answers Updated Frequently
- \* SY0-601 Practice Questions Verified by Expert Senior Certified Staff
- \* SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year