



**CertsMania**



**CertsMania**

## **Free Questions for SY0-701**

**Shared by Kendall on Apr 30, 2026**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**



**CertsMania**

## Questions # 1:

Which of the following is a directive managerial control?

### Options:

A.

Acceptable use policy

B.

Login warning banner

C.

Master service agreement

D.

No trespassing sign



CertsMania

### Answer

A

### Explanation

A directive managerial control provides guidance and expectations for behavior through policy and governance. An Acceptable Use Policy (AUP) is a classic example, as it defines how users may and may not use organizational systems and data. Security+ SY0-701 categorizes policies as managerial (administrative) controls that direct user behavior and establish accountability.

A login warning banner (B) is typically a deterrent/administrative control but is not managerial in nature. A master service agreement (C) is a contractual/legal document, not a managerial directive for internal users. A "No trespassing" sign (D) is a physical deterrent control.

Because an AUP formally directs behavior and is enforced through management processes, A: Acceptable use policy is correct.

## Questions # 2:

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.

Which of the following best describes the user's activity?

**Options:**

- A.  
Penetration testing
- B.  
Phishing campaign
- C.  
External audit
- D.  
Insider threat



CertsMania

**Answer**

D

**Explanation**

An insider threat is a security risk that originates from within the organization, such as an employee, contractor, or business partner, who has authorized access to the organization's data and systems. An insider threat can be malicious, such as stealing, leaking, or sabotaging sensitive data, or unintentional, such as falling victim to phishing or social engineering. An insider threat can cause significant damage to the organization's reputation, finances, operations, and legal compliance. The user's activity of logging in remotely after hours and copying large amounts of data to a personal device is an example of a malicious insider threat, as it violates the organization's security policies and compromises the confidentiality and integrity of the data. References = Insider Threats - CompTIA Security+ SY0-701: 3.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 133.

**Questions # 3:**

An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

**Options:**

A.

RDP server

B.

Jump server

C.

Proxy server

D.

Hypervisor



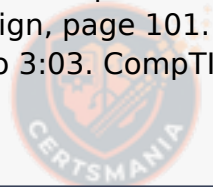
CertsMania

**Answer**

B

**Explanation**

= A jump server is a server that acts as an intermediary between a user and a target system. A jump server can provide an added layer of security by preventing unauthorized access to internal company resources. A user can connect to the jump server using a secure protocol, such as SSH, and then access the target system from the jump server. This way, the target system is isolated from the external network and only accessible through the jump server. A jump server can also enforce security policies, such as authentication, authorization, logging, and auditing, on the user's connection. A jump server is also known as a bastion host or a jump box. References = CompTIA Security+ Certification Exam Objectives, Domain 3.3: Given a scenario, implement secure network architecture concepts. CompTIA Security+ Study Guide (SY0-701), Chapter 3: Network Architecture and Design, page 101. Other Network Appliances - SY0-601 CompTIA Security+ : 3.3, Video 3:03. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 2.



CertsMania

Questions # 4:

Which of the following is the best way to improve the confidentiality of remote connections to an enterprise ' s infrastructure?

**Options:**

A.

Firewalls

B.

Virtual private networks

C.

Extensive logging

D.

Intrusion detection systems



CertsMania

## Answer

B

## Explanation

Confidentiality is primarily improved by preventing unauthorized parties from viewing data while it travels across untrusted networks. A Virtual Private Network (VPN) addresses this by creating a protected tunnel between endpoints, commonly using tunneling technologies such as IPSec or TLS for secure communications. The Study Guide explains the purpose of VPNs for remote access as: “A virtual private network (VPN) is a way to create a virtual network link across a public network that allows the endpoints to act as though they are on the same network.” It also notes the practical security value of full-tunnel VPNs when traversing untrusted networks: “A full-tunnel VPN sends all network traffic through the VPN tunnel, keeping it secure as it goes to the remote trusted network... [and] is a great way to ensure that traffic sent through an untrusted network... remains secure.”

Why the other options are less correct for confidentiality: Firewalls control traffic flow but do not inherently encrypt remote communications end-to-end; extensive logging improves detection/forensics, not confidentiality; and IDS detects suspicious activity but doesn't prevent eavesdropping on the connection. For confidentiality of remote connections, VPNs (implemented with secure tunneling like TLS/IPSec) are the best answer.

[References: Sybex CompTIA Security+ Study Guide (SY0-701) — VPN definition and role ; full-tunnel VPN guidance for securing traffic over untrusted networks . , , , , , ]

## Questions # 5:

A company ' s end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS servers, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the

following best describes what the security analyst is seeing?

**Options:**

A.

Concurrent session usage

B.

Secure DNS cryptographic downgrade

C.

On-path resource consumption

D.

Reflected denial of service

**Answer**

D

**Explanation**

A reflected denial of service (RDoS) attack is a type of DDoS attack that uses spoofed source IP addresses to send requests to a third-party server, which then sends responses to the victim server. The attacker exploits the difference in size between the request and the response, which can amplify the amount of traffic sent to the victim server. The attacker also hides their identity by using the victim's IP address as the source. A RDoS attack can target DNS servers by sending forged DNS queries that generate large DNS responses. This can flood the network interface of the DNS server and prevent it from serving legitimate requests from end users. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 1

**Questions # 6:**

A security analyst reviews firewall configurations and finds that firewalls are configured to fail-open mode in the event of a crash. Which of the following describes the security risk associated with this configuration?

**Options:**

A.

There may be increased latency during failover.

B.

Authentication tokens may be invalidated during an outage.

C.

Traffic will bypass inspection during a failure.

D.

All encrypted traffic will be blocked during an outage.

## Answer

C

## Explanation

The best answer is C. Traffic will bypass inspection during a failure.

A firewall configured to fail open will allow traffic to continue flowing if the device crashes or fails. This preserves availability, but it creates a security risk because traffic may pass through without being inspected or filtered.

That means malicious traffic, unauthorized connections, or prohibited traffic could traverse the network during the outage.

Why the other options are incorrect:

A. There may be increased latency during failover. This is not the main security risk associated with fail-open mode.

B. Authentication tokens may be invalidated during an outage. This is unrelated to firewall fail-open behavior.

D. All encrypted traffic will be blocked during an outage. Fail-open does the opposite of blocking traffic; it allows traffic to pass through.

From a SY0-701 perspective, fail-open prioritizes availability, but the tradeoff is that security inspection may be bypassed, making C the correct answer.

## Questions # 7:

Which of the following is a security benefit of an effective IT asset tracking system?

**Options:**

A.

Helping identify unauthorized or unmanaged devices connected to the network

B.

Preventing prohibited data exfiltration from endpoints on the network

C.

Assisting with automated root cause analysis for all security incidents on the network

D.

Ensuring proper data backup and recovery procedures are in place

**Answer**

A

**Explanation**

The best answer is A. Helping identify unauthorized or unmanaged devices connected to the network.

An effective IT asset tracking system maintains visibility into the hardware, software, and devices that are authorized to exist in the environment. One major security benefit is that it helps identify systems that are:

unauthorized

unmanaged

missing required security controls

unknown to administrators

This improves inventory control and helps security teams detect rogue or noncompliant devices.

Why the other options are incorrect:

B. Preventing prohibited data exfiltration from endpoints on the network Preventing exfiltration is more directly the role of DLP and related controls, not asset tracking alone.

C. Assisting with automated root cause analysis for all security incidents on the network Asset tracking can support investigations, but it does not automatically perform root cause analysis for all incidents.

D. Ensuring proper data backup and recovery procedures are in place Backup and recovery are separate operational processes, not a direct benefit of asset tracking itself.

From the SY0-701 perspective, maintaining an accurate asset inventory is foundational for identifying unauthorized or unmanaged devices, so A is the correct answer.

#### Questions # 8:

An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

#### Options:

A.

ACL

B.

DLP

C.

IDS

D.

IPS

#### Answer

D

#### Explanation

An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can also perform other functions, such as rate limiting, encryption, or redirection. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

## Questions # 9:

Which of the following best describes the main difference between an MOU and an SOW?

### Options:

A.

An MOU is usually not legally binding, while an SOW is usually legally binding about outcomes.

B.

An MOU identifies engagement details, while an SOW specifies who will engage.

C.

An MOU requires signatures from both parties, while an SOW only requires a signature from the service provider.

D.

An MOU is typically very detailed about tasks, while an SOW is typically high-level.

### Answer

A

### Explanation

The correct answer is A because the primary distinction between a Memorandum of Understanding (MOU) and a Statement of Work (SOW) lies in their legal enforceability and purpose. In the Security+ SY0-701 governance and third-party risk management context, an MOU is generally a formal but nonbinding agreement that outlines mutual expectations, responsibilities, and cooperation between parties. It establishes intent and alignment but typically does not impose enforceable obligations or penalties if terms are not met.

An SOW, on the other hand, is legally binding and serves as a contractual document that defines specific deliverables, timelines, performance metrics, and acceptance criteria. The SY0-701 study guide emphasizes that SOWs are critical in vendor and service provider relationships because they clearly define what work will be performed, how success is measured, and what happens if requirements are not met. This makes the SOW enforceable in legal and regulatory contexts, especially when dealing with sensitive systems or data.

Option B is incorrect because both MOUs and SOWs can identify engagement participants, but this is not their defining difference. Option C is incorrect because both documents

typically require agreement from all involved parties, and signature requirements vary by organization and jurisdiction. Option D is incorrect because it reverses the actual level of detail: MOUs are high-level and conceptual, while SOWs are detailed and task-specific.

In security programs, MOUs are often used for cooperative arrangements, such as information sharing between organizations or government entities. SOWs are used when accountability, compliance, and measurable outcomes are required. Understanding this distinction is essential for managing third-party risk, enforcing security requirements, and maintaining compliance with Security+ SY0-701 governance objectives.

#### Questions # 10:

A company that has a large IT operation is looking to better control, standardize, and lower the time required to build new servers. Which of the following architectures will best achieve the company's objectives?

#### Options:

A.

IoT

B.

IaC

C.

PaaS

D.

ICS

#### Answer

B

#### Explanation

Infrastructure as Code (IaC) enables organizations to automate the provisioning, configuration, and deployment of servers through machine-readable scripts rather than manual processes. SY0-701 emphasizes IaC as a key component of DevOps and secure deployment pipelines. By using IaC, server builds become repeatable, standardized, version-controlled, and much faster.

This directly addresses the company ' s goals:

Better control: IaC ensures predictable, consistent configuration across all servers.

Standardization: Scripts eliminate drift by applying identical configurations.

Lower build time: Automation significantly accelerates server creation and eliminates manual intervention.

IoT (A) refers to Internet-connected smart devices and is unrelated to server deployment. PaaS (C) offers development platforms but does not automate infrastructure builds. ICS (D) refers to industrial control systems, not IT server architecture.

Therefore, the only correct architecture that meets all objectives is IaC, a foundational technology for modern automated infrastructure.

#### Questions # 11:

A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

#### Options:

A.

Partition

B.

Asymmetric

C.

Full disk

D.

Database

#### Answer

C

#### Explanation

Full disk encryption (FDE) is a technique that encrypts all the data on a hard drive,

including the operating system, applications, and files. FDE protects the data from unauthorized access in case the laptop is lost, stolen, or disposed of without proper sanitization. FDE requires the user to enter a password, a PIN, a smart card, or a biometric factor to unlock the drive and boot the system. FDE can be implemented by using software solutions, such as BitLocker, FileVault, or VeraCrypt, or by using hardware solutions, such as self-encrypting drives (SEDs) or TrustedPlatform Modules (TPMs). FDE is a recommended encryption technique for laptops and other mobile devices that store sensitive data.

Partition encryption is a technique that encrypts only a specific partition or volume on a hard drive, leaving the rest of the drive unencrypted. Partition encryption is less secure than FDE, as it does not protect the entire drive and may leave traces of data on unencrypted areas. Partition encryption is also less convenient than FDE, as it requires the user to mount and unmount the encrypted partition manually.

Asymmetric encryption is a technique that uses a pair of keys, one public and one private, to encrypt and decrypt data. Asymmetric encryption is mainly used for securing communication, such as email, web, or VPN, rather than for encrypting data at rest. Asymmetric encryption is also slower and more computationally intensive than symmetric encryption, which is the type of encryption used by FDE and partition encryption.

Database encryption is a technique that encrypts data stored in a database, such as tables, columns, rows, or cells. Database encryption can be done at the application level, the database level, or the file system level. Database encryption is useful for protecting data from unauthorized access by database administrators, hackers, or malware, but it does not protect the data from physical theft or loss of the device that hosts the database.

References = Data Encryption - CompTIA Security+ SY0-401: 4.4, CompTIA Security+ Cheat Sheet and PDF | Zero To Mastery, CompTIA Security+ SY0-601 Certification Course - Cybr, Application Hardening - SY0-601 CompTIA Security+ : 3.2.

#### Questions # 12:

A systems administrator just purchased multiple network devices. Which of the following should the systems administrator perform to prevent attackers from accessing the devices by using publicly available information?

#### Options:

A.

Install endpoint protection

B.

Disable ports/protocols

C.

Change default passwords

D.

Remove unnecessary software

## Answer

C

## Explanation

Changing default passwords is a critical first step after acquiring new devices. Default credentials are widely known and publicly documented, so changing them prevents unauthorized access using this information.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 3.1: "Changing default passwords prevents attackers from exploiting publicly available device information.", Exam Objectives 3.1: "Implement secure network architecture concepts.", , , , , , , ]

## Questions # 13:

A systems administrator is concerned about vulnerabilities within cloud computing instances. Which of the following is most important for the administrator to consider when architecting a cloud computing environment?

### Options:

A.

SQL injection

B.

TOC/TOU

C.

VM escape

D.

Tokenization

E.

Password spraying

### Answer

C

### Questions # 14:

Which of the following describes when a user installs an unauthorized application by bypassing the authorized application store and installing a binary file?

### Options:

A.

Jailbreaking

B.

Sideloaded

C.

Memory injection

D.

VM escaping

### Answer

B

### Explanation

The best answer is B. Sideloaded.

Sideloaded is the installation of an application from outside the official or authorized application store, often by directly installing a binary package or application file. This bypasses standard review and distribution controls.

Why the other options are incorrect:

A. Jailbreaking Jailbreaking removes or bypasses manufacturer or operating system

restrictions, often on mobile devices. It may enable sideloading, but it is not the same thing as the act described.

C. Memory injectionMemory injection is a technique used to place code into another process's memory. It is unrelated to installing an app from an unauthorized source.

D. VM escapingVM escape is an attack in which code breaks out of a virtual machine into the host environment. It does not describe unauthorized app installation.

From a Security+ standpoint, bypassing the approved app store and directly installing a binary is the definition of sideloading.

#### Questions # 15:

Which of the following allows an exploit to go undetected by the operating system?

#### Options:

A.

Firmware vulnerabilities

B.

Side loading

C.

Memory injection

D.

Encrypted payloads

#### Answer

A

#### Questions # 16:

Which of the following threat actors would most likely deface the website of a high-profile music group?

**Options:**

- A.  
Unskilled attacker
- B.  
Organized crime
- C.  
Nation-state
- D.  
Insider threat



CertsMania

**Answer**

A

**Explanation**

Detailed Explanation: An unskilled attacker, often referred to as a script kiddie, is likely to engage in website defacement. This type of attack typically requires minimal expertise and is often conducted for notoriety. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: " Threat Actors and Motivations " .

Questions # 17:

Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company?

**Options:**

- A.  
Provisioning resources
- B.  
Disabling access
- C.

Reviewing change approvals

D.

Escalating permission requests

**Answer**

B

**Explanation**



CertsMania

Disabling access is an automation use case that would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company. Disabling access is the process of revoking or suspending the access rights of a user account, such as login credentials, email, VPN, cloud services, etc. Disabling access can prevent unauthorized or malicious use of the account by former employees or attackers who may have compromised the account. Disabling access can also reduce the attack surface and the risk of data breaches or leaks. Disabling access can be automated by using scripts, tools, or workflows that can trigger the action based on predefined events, such as employee termination, resignation, or transfer. Automation can ensure that the access is disabled in a timely, consistent, and efficient manner, without relying on manual intervention or human error.

[References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Identity and Access Management, page 2131. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Identity and Access Management, page 2132., , , , , , , , , , , ]

Questions # 18:

A security team installs an IPS on an organization ' s network and needs to configure the system to detect and prevent specific network attacks. Which of the following settings should the team configure first within the IPS?

**Options:**

A.

Allow list policies

B.

Packet Inspection

C.

Logging and reporting

D.

Firewall rules

**Answer**

B

**Explanation**



CertsMania

An Intrusion Prevention System (IPS) uses packet inspection (either signature-based, anomaly-based, or both) to analyze network traffic and detect malicious patterns. Configuring packet inspection is the first step to ensure the IPS can identify and respond to specific attack signatures.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 3.2: "IPS devices must be configured to inspect network packets for attack patterns.", Exam Objectives 3.2: "Summarize security implications of embedded and specialized systems.", , , , , , , , ]

Questions # 19:

Which of the following describes an executive team that is meeting in a board room and testing the company ' s incident response plan?

**Options:**

A.

Continuity of operations

B.

Capacity planning

C.

Tabletop exercise

D.

Parallel processing



CertsMania

## Answer

C

## Explanation

A tabletop exercise involves the executive team or key stakeholders discussing and testing the company's incident response plan in a simulated environment. These exercises are low-stress, discussion-based, and help to validate the plan's effectiveness by walking through different scenarios without disrupting actual operations. It is an essential part of testing business continuity and incident response strategies.

Continuity of operations refers to the ability of an organization to continue functioning during and after a disaster but doesn't specifically involve simulations like tabletop exercises.

Capacity planning is related to ensuring the infrastructure can handle growth, not incident response testing.

Parallel processing refers to running multiple processes simultaneously, which is unrelated to testing an incident response plan.

## Questions # 20:

An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions over the phone to use a new account. Which of the following would most likely prevent this activity in the future?

### Options:

A.

Standardizing security incident reporting

B.

Executing regular phishing campaigns

C.

Implementing insider threat detection measures

D.

Updating processes for sending wire transfers

## Answer

D

## Explanation

Updating wire transfer processes to include verification steps (such as requiring dual approval or verifying account changes via a secondary communication method) can prevent fraudulent transactions. Attackers often use business email compromise (BEC) or pretexting to trick employees into transferring funds to fraudulent accounts.

Standardizing security incident reporting is useful for tracking security events but does not prevent fraud in real time.

Executing regular phishing campaigns improves awareness but does not enforce a verification process for financial transactions.

Implementing insider threat detection focuses on internal risks but does not specifically prevent external fraud.

A more secure wire transfer process with additional verification steps is the most effective measure against fraudulent transactions.

## Questions # 21:

Which of the following is the best way to securely store an encryption key for a data set in a manner that allows multiple entities to access the key when needed?

### Options:

A.

Public key infrastructure

B.

Open public ledger

C.

Public key encryption

D.

Key escrow

## Answer

D

### Questions # 22:

A security analyst is evaluating a SaaS application that the human resources department would like to implement. The analyst requests a SOC 2 report from the SaaS vendor. Which of the following processes is the analyst most likely conducting?

#### Options:

A.

Internal audit

B.

Penetration testing

C.

Attestation

D.

Due diligence

## Answer

D

### Questions # 23:

While considering the organization 's cloud-adoption strategy, the Chief Information Security Officer sets a goal to outsource patching of firmware, operating systems, and applications to the chosen cloud vendor. Which of the following best meets this goal?

#### Options:

A.

Community cloud

B.

PaaS

C.

Containerization

D.

Private cloud

E.

SaaS

F.

IaaS



CertsMania

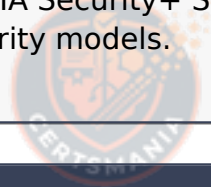
## Answer

E

## Explanation

Software as a Service (SaaS) is the cloud model that best meets the goal of outsourcing the management, including patching, of firmware, operating systems, and applications to the cloud vendor. In a SaaS environment, the cloud provider is responsible for maintaining and updating the entire software stack, allowing the organization to focus on using the software rather than managing its infrastructure.

References = CompTIA Security+ SY0-701 study materials, particularly the domains related to cloud security models.



CertsMania

## Questions # 24:

A security engineer configured a remote access VPN. The remote access VPN allows end users to connect to the network by using an agent that is installed on the endpoint, which establishes an encrypted tunnel. Which of the following protocols did the engineer most likely implement?

**Options:**

- A.  
GRE
- B.  
IPSec
- C.  
SD-WAN
- D.  
EAP



CertsMania

**Answer**

B

Questions # 25:

A service provider wants a cost-effective way to rapidly expand from providing internet links to managing them. Which of the following methods will allow the service provider to best scale its services while maintaining performance consistency?

**Options:**

- A.  
Escalation support
- B.  
Increased workforce
- C.  
Baseline enforcement
- D.  
Technical debt



CertsMania

## Answer

C

## Explanation

Baseline enforcement involves establishing standard configurations and operational baselines that allow a service provider to scale services efficiently while ensuring consistent performance and security. By enforcing baselines, automation can be applied, reducing manual intervention and variability, which supports rapid, cost-effective expansion.

Increasing workforce (B) adds operational cost and may introduce inconsistency. Escalation support (A) is reactive and does not inherently support scaling. Technical debt (D) refers to accumulated suboptimal design or quick fixes that hamper future scalability and is a negative factor.

Baseline enforcement is recognized as a best practice in the Security Program Management domain for scaling services reliably [6:Chapter 16†CompTIA Security+ Study Guide].

## Questions # 26:

A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken first?

### Options:

A.

Air gap the system.

B.

Move the system to a different network segment.

C.

Create a change control request.

D.

Apply the patch to the system.

## Answer

C

## Explanation

= A change control request is a document that describes the proposed change to a system, the reason for the change, the expected impact, the approval process, the testing plan, the implementation plan, the rollback plan, and the communication plan. A change control request is a best practice for applying any patch to a production system, especially a high-priority one, as it ensures that the change is authorized, documented, tested, and communicated. A change control request also minimizes the risk of unintended consequences, such as system downtime, data loss, or security breaches. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 235. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.1, page 13.

## Questions # 27:

Which of the following is a prerequisite for a DLP solution?

### Options:

A.

Data destruction

B.

Data sanitization

C.

Data classification

D.

Data masking



## Answer

C

## Explanation

Data classification is required before implementing a Data Loss Prevention (DLP) solution

because DLP policies depend on identifying and categorizing sensitive data to monitor, block, or encrypt it accordingly.

Data destruction (A) and sanitization (B) remove data, and masking (D) obscures data but classification is foundational for DLP effectiveness.

Data classification is emphasized in Security Program Management and Data Protection topics [6:Chapter 16+CompTIA Security+ Study Guide].

#### Questions # 28:

A company is changing its mobile device policy. The company has the following requirements:

Company-owned devices

Ability to harden the devices

Reduced security risk

Compatibility with company resources

Which of the following would best meet these requirements?

#### Options:

A.

BYOD

B.

CYOD

C.

COPE

D.

COBO

#### Answer

C

## Explanation

Detailed Explanation:COPE (Corporate-Owned, Personally Enabled) devices allow companies to manage and harden company-owned devices while still enabling limited personal use, reducing security risks while maintaining compatibility with corporate resources. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: " Mobile Device Deployment Models " .

## Questions # 29:

Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?

### Options:

- A.  
To track the status of patching installations
- B.  
To find shadow IT cloud deployments
- C.  
To continuously the monitor hardware inventory
- D.  
To hunt for active attackers in the network

## Answer

A

### Explanation

Running daily vulnerability scans on all corporate endpoints is primarily done to track the status of patching installations. These scans help identify any missing security patches or vulnerabilities that could be exploited by attackers. Keeping the endpoints up-to-date with the latest patches is critical for maintaining security.

Finding shadow IT cloud deployments and monitoring hardware inventory are better achieved through other tools.

Hunting for active attackers would typically involve more real-time threat detection methods than daily vulnerability scans.

### Questions # 30:

A small business initially plans to open common communications ports (21, 22, 25, 80, 443) on its firewall to allow broad access to its screened subnet. However, their security consultant advises against this action. Which of the following security principles is the consultant addressing?

#### Options:

A.

Secure access service edge

B.

Attack surface

C.

Least privilege

D.

Separation of duties

#### Answer

B

#### Explanation

The correct answer is Attack surface because opening multiple common service ports unnecessarily increases the number of potential entry points an attacker can target. In the Security+ SY0-701 exam objectives, the attack surface is defined as the total number of exposed interfaces, services, ports, protocols, and access points that an attacker could attempt to exploit. Each open port corresponds to a listening service, and every exposed service represents an opportunity for reconnaissance, exploitation, or abuse.

In this scenario, the business intends to open ports for FTP, SSH, SMTP, HTTP, and HTTPS without clearly limiting access. While some of these services may be required, opening all of them broadly—especially to a screened subnet—significantly expands the attack surface. If any of these services are misconfigured, unpatched, or vulnerable, attackers could exploit them to gain unauthorized access. The SY0-701 study guide emphasizes

minimizing exposed services as a foundational defensive strategy, often referred to as reducing attack surface area.

Option C, least privilege, is related but not the best answer. Least privilege focuses on granting users or systems only the minimum access required, whereas this question specifically concerns exposed network services rather than access rights. Option A, secure access service edge (SASE), is a cloud-based architecture model and is unrelated to basic firewall port exposure decisions. Option D, separation of duties, applies to role and responsibility distribution, not network exposure.

By advising against opening multiple common ports, the consultant is recommending a reduction in exposed services to limit opportunities for attack. This aligns directly with SY0-701 guidance on secure network design, firewall hardening, and minimizing externally accessible services.

In summary, limiting open ports reduces the organization's attack surface, making Attack surface the correct and best answer.

#### Questions # 31:

At the start of a penetration test, the tester checks OSINT resources for information about the client environment. Which of the following types of reconnaissance is the tester performing?

#### Options:

A.

Active

B.

Passive

C.

Offensive

D.

Defensive

#### Answer

B

## Explanation

Passive reconnaissance involves gathering publicly available information about a target without directly interacting with the target systems. Checking OSINT (Open Source Intelligence) sources is a typical passive technique used to collect data without alerting the target.

Active reconnaissance (A) involves direct interaction with the target. Offensive (C) and defensive (D) refer to broader security postures and are not specific reconnaissance types.

Passive reconnaissance is a foundational step in penetration testing and covered in the Threats and Vulnerabilities domain of SY0-701 [6:Chapter 2] CompTIA Security+ Study Guide [

## Questions # 32:

Which of the following concepts protects sensitive information from unauthorized disclosure?

### Options:

A.

Integrity

B.

Availability

C.

Authentication

D.

Confidentiality

## Answer

D

### Explanation

The best answer is D. Confidentiality.

In the CIA triad, confidentiality means protecting information from unauthorized

disclosure. It ensures that only authorized users, systems, or processes can view sensitive data.

The other choices are different security concepts:

A. Integrity means protecting data from unauthorized modification or destruction.

B. Availability means ensuring systems and data are accessible when needed.

C. Authentication means verifying the identity of a user, device, or process.

Since the question specifically asks about protecting sensitive information from unauthorized disclosure, confidentiality is the correct answer.

### Questions # 33:

An organization is evaluating new regulatory requirements associated with the implementation of corrective controls on a group of interconnected financial systems. Which of the following is the most likely reason for the new requirement?

#### Options:

A.

To defend against insider threats altering banking details

B.

To ensure that errors are not passed to other systems

C.

To allow for business insurance to be purchased

D.

To prevent unauthorized changes to financial data

#### Answer

B

#### Explanation

The primary goal of corrective controls in financial systems is to ensure that errors do not propagate across interconnected systems. Financial transactions are often interdependent,

meaning one incorrect or unauthorized change can affect multiple systems. Regulations often mandate these controls to maintain accuracy and prevent cascading failures.

A (insider threats altering banking details) is a concern, but this scenario focuses on corrective controls, not insider threats specifically.

C (business insurance) is unrelated to why corrective controls are implemented.

D (preventing unauthorized changes) falls under preventive, not corrective controls.

[Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain., , , , , , , , , ]

### Questions # 34:

Which of the following actions is best performed by ticketing automation to ensure that incidents receive the correct level of attention and response?

#### Options:

A.

Notification

B.

Creation

C.

Closure

D.

Escalation

#### Answer

D

#### Explanation

The key phrase is “ensure that incidents receive the correct level of attention and response.” In operations, that aligns most directly with escalation—moving high-severity or time-sensitive incidents to the right people/teams quickly and consistently, according to predefined criteria (severity, impacted systems, threat intel enrichment, SLA timers). The Study Guide lists ticketing and escalation explicitly as automation use cases: “Ticket

creation: Automation can streamline the ticketing process, enabling immediate creation and routing of issues to the right teams.” and, crucially for this question, “Escalation: In case of a major incident, scripts can automate the escalation process, alerting key personnel quickly.”

While automation can also handle notification and ticket creation, escalation is the control that most directly enforces that the incident gets the proper priority and response path (for example: paging on-call, invoking the IR lead, opening a bridge, and applying “major incident” workflows). Closure is typically less suitable because it often requires validation and human judgment to ensure containment, eradication, and recovery steps are complete.

[References: Automation use cases for ticketing, including escalation for major incidents ., . . . . ]

### Questions # 35:

A spoofed identity was detected for a digital certificate. Which of the following are the type of unidentified key and the certificate mat could be in use on the company domain?

#### Options:

A.

Private key and root certificate

B.

Public key and expired certificate

C.

Private key and self-signed certificate

D.

Public key and wildcard certificate

#### Answer

C

#### Explanation

A self-signed certificate is a certificate that is signed by its own private key rather than by a trusted certificate authority (CA). This means that the authenticity of the certificate relies solely on the issuer ' s own authority. If a spoofed identity was detected, it could

indicate that a private key associated with a self-signed certificate was compromised. Self-signed certificates are often used internally within organizations, but they carry higher risks since they are not validated by a third-party CA, making them more susceptible to spoofing.

References = CompTIA Security+ SY0-701 study materials, particularly the domains discussing Public Key Infrastructure (PKI) and certificate management.

### Questions # 36:

The Cruel Information Security Officer (CISO) asks a security analyst to install an OS update to a production VM that has a 99% uptime SLA. The CISO tells me analyst the installation must be done as quickly as possible. Which of the following courses of action should the security analyst take first?

#### Options:

A.

Log in to the server and perform a health check on the VM.

B.

Install the patch Immediately.

C.

Confirm that the backup service is running.

D.

Take a snapshot of the VM.

#### Answer

D

#### Explanation

Before applying any updates or patches to a production VM, especially one with a 99% uptime SLA, it is crucial to first take a snapshot of the VM. This snapshot serves as a backup that can be quickly restored in case the update causes any issues, ensuring that the system can be returned to its previous state without violating the SLA. This step mitigates risk and is a standard best practice in change management for critical systems.

References = CompTIA Security+ SY0-701 study materials, focusing on change

management and backup strategies.

### Questions # 37:

Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

#### Options:

A.

Software as a service

B.

Infrastructure as code

C.

Internet of Things

D.

Software-defined networking

#### Answer

B

#### Explanation

Infrastructure as code (IaC) is a method of using code and automation to manage and provision cloud resources, such as servers, networks, storage, and applications. IaC allows for easy deployment, scalability, consistency, and repeatability of cloud environments. IaC is also a key component of DevSecOps, which integrates security into the development and operations processes. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Cloud and Virtualization Concepts, page 294.

### Questions # 38:

While a school district is performing state testing, a security analyst notices all internet services are unavailable. The analyst discovers that ARP poisoning is occurring on the network

and then terminates access for the host. Which of the following is most likely responsible for this malicious activity?

**Options:**

- A.  
Unskilled attacker
- B.  
Shadow IT
- C.  
Credential stuffing
- D.  
DMARC failure



CertsMania

**Answer**

A

**Explanation**

ARP poisoning (also known as ARP spoofing) is a basic man-in-the-middle (MITM) attack that involves sending fake ARP responses to redirect traffic. This technique is not sophisticated and can be easily executed using freely available tools like Cain & Abel, Ettercap, or Wireshark.

Such attacks are often attempted by unskilled attackers (script kiddies) testing their abilities, especially in environments like schools. The term “unskilled attacker” fits best here, as credential stuffing and DMARC are unrelated to ARP poisoning.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - “Attack techniques: MITM, ARP poisoning; attacker types: Unskilled/script kiddie.”, , , , , , , , ]

**Questions # 39:**

Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?

**Options:**

A.

IDS

B.

ACL

C.

EDR

D.

NAC



CertsMania

**Answer**

C

**Explanation**

Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints, such as computers, laptops, mobile devices, and servers. EDR can help to detect and prevent malicious software, such as viruses, malware, and Trojans, from infecting the endpoints and spreading across the network. EDR can also provide visibility and response capabilities to contain and remediate threats. EDR is different from IDS, which is a network-based technology that monitors and alerts on network traffic anomalies. EDR is also different from ACL, which is a list of rules that control the access to network resources. EDR is also different from NAC, which is a technology that enforces policies on the network access of devices based on their identity and compliance status. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 2561



CertsMania

**Questions # 40:**

Which of the following will harden access to a new database system? (Select two)

**Options:**

A.

Jump server

B.

NIDS

C.

Monitoring

D.

Proxy server

E.

Host-based firewall

F.

WAF



CertsMania

## Answer

A, E

## Explanation

Hardening access to a new database system requires implementing controls that restrict and secure how administrators and applications connect to the database. A jump server (A) is a hardened intermediary system used to manage access to sensitive systems such as databases. By forcing administrators to authenticate through a controlled, monitored jump host instead of connecting directly, organizations reduce attack surfaces and prevent unauthorized lateral movement. Security+ SY0-701 identifies jump servers as critical in securing high-value systems.

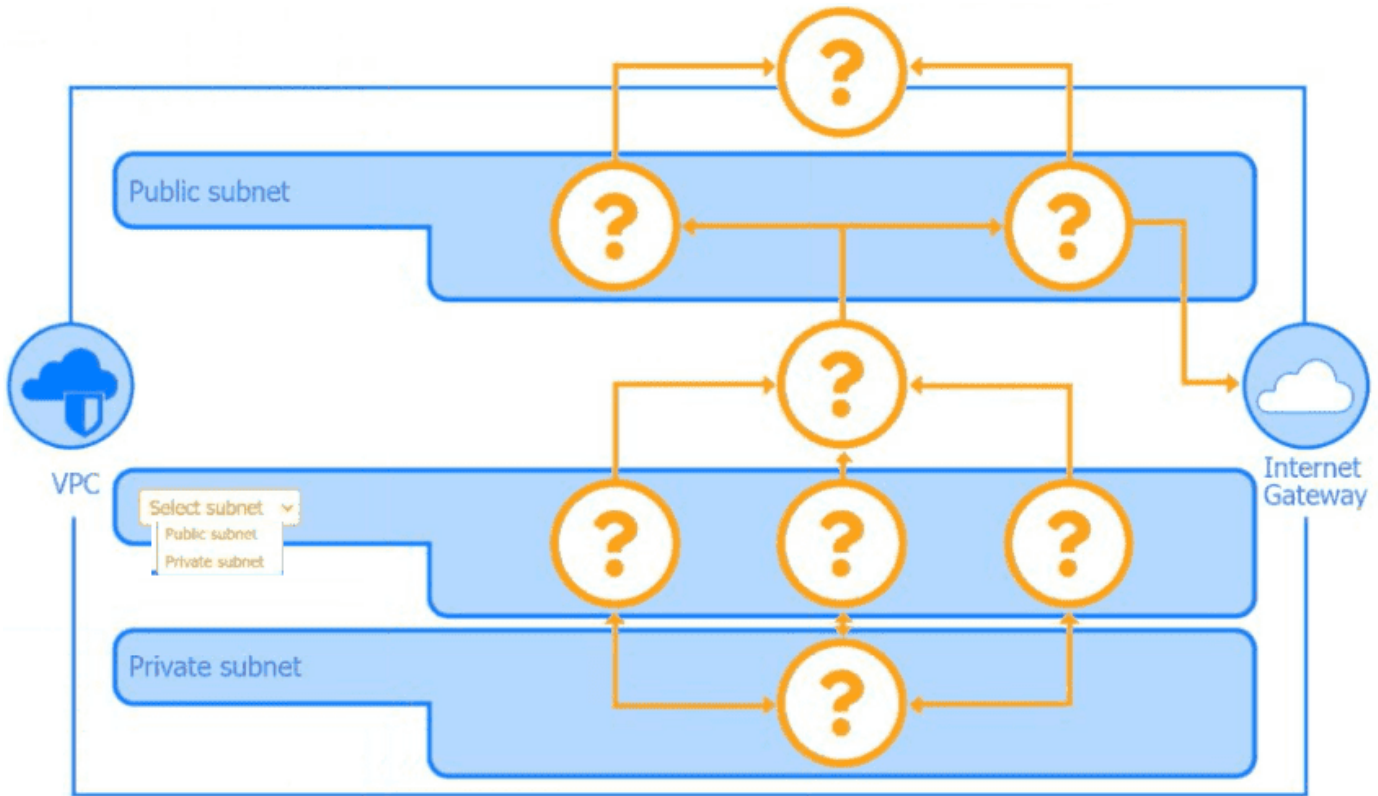
A host-based firewall (E) provides system-level traffic filtering directly on the database server. It allows only trusted IPs, ports, and services to communicate with the database, significantly reducing exposure. This is an essential hardening measure because databases should only accept connections from specific application servers or administrative hosts.

NIDS (B) monitors traffic but does not harden access. Monitoring (C) provides visibility but does not restrict access. A proxy server (D) is not typically used for database access. A WAF (F) protects web applications, not internal database systems.

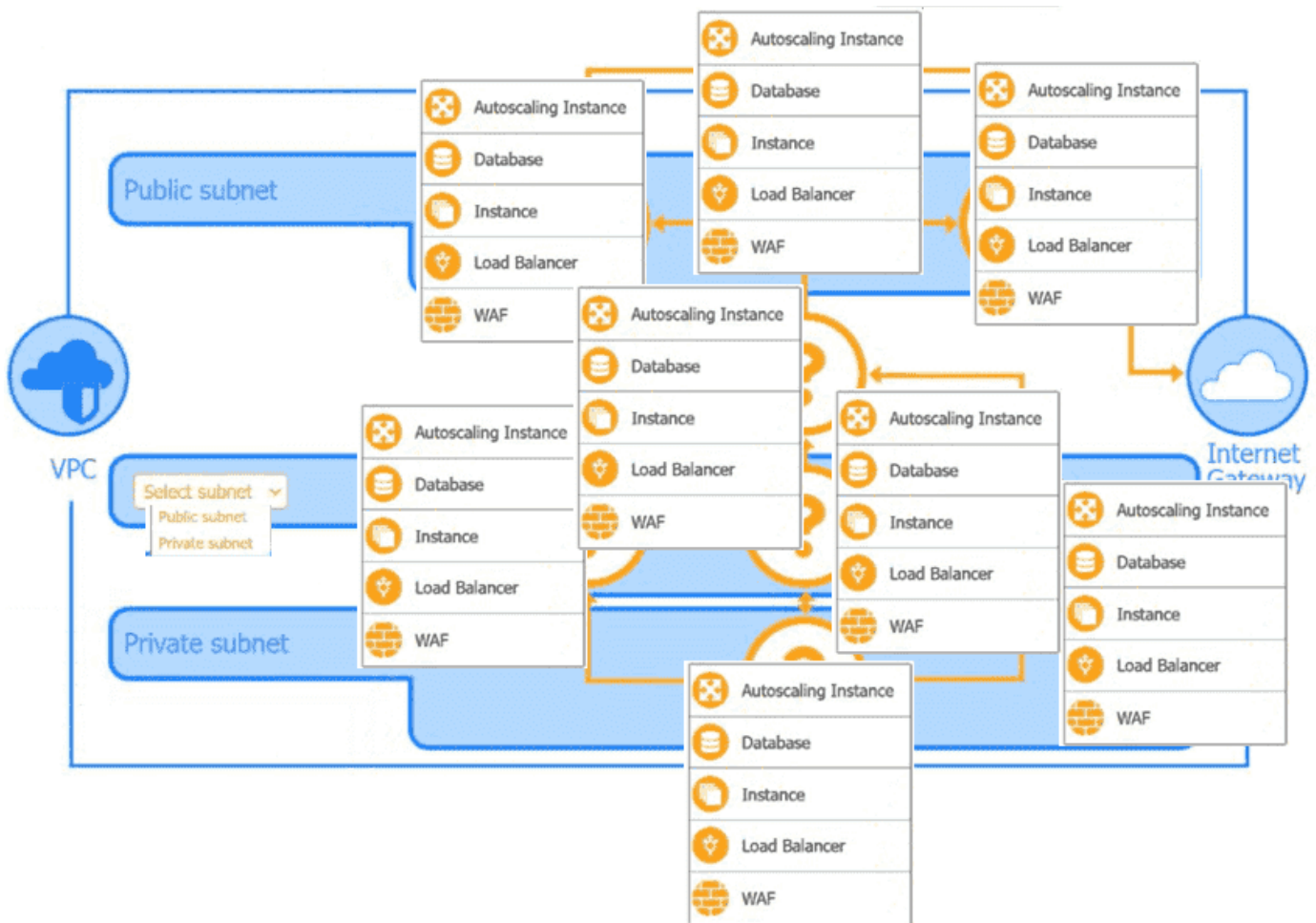
Thus, A (Jump server) and E (Host-based firewall) are the correct hardening controls.

Questions # 41:

A security analyst is creating the first draft of a network diagram for the company 's new customer-facing payment application that will be hosted by a third-party cloud service provider.



CertsMania



**Options:**

## Answer

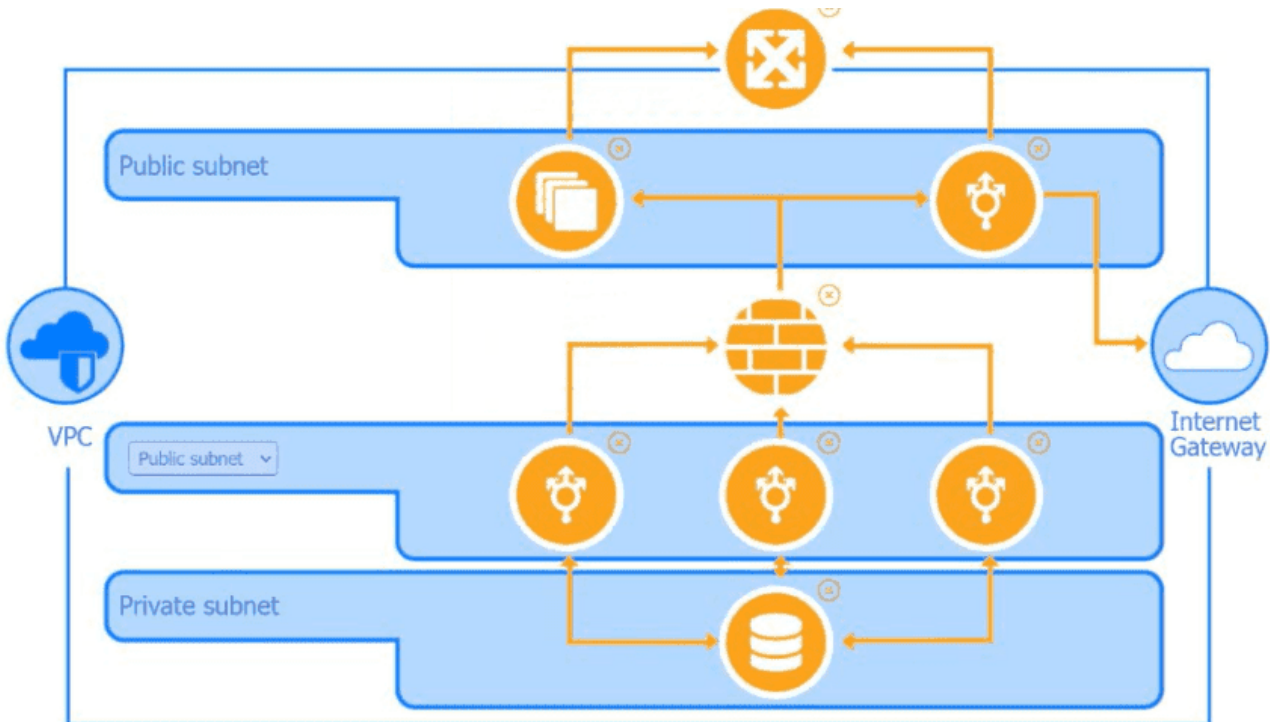
Answer:

See the Explanation for complete solution for this task.

## Explanation



CertsMania



A diagram of a computer AI-generated content may be incorrect.

### Step 1: Understand Requirements & Security Principles

Requirements:

Customer-facing payment application (PCI DSS compliance applies)

Hosted on third-party cloud (e.g., AWS)

Must segment public-facing and internal resources

Needs to be scalable and resilient

Must have strong security controls

### Step 2: Design the High-Level Network Layout

Core Components:

VPC (Virtual Private Cloud): Isolates your environment from other tenants in the cloud.

Subnets:

Public subnet: For resources that must communicate with the internet.

Private subnet: For internal resources, NOT directly exposed to the internet.

### Step 3: Place Resources in Appropriate Subnets

Public Subnet:

Internet-facing Load Balancer (LB): Distributes traffic to application servers.

Web Application Firewall (WAF): Protects against web exploits.

Autoscaling Instances: EC2 (or VM) servers running your web front-end, automatically scaling as traffic grows.

Private Subnet:

Application servers: Back-end logic, not exposed to internet directly.

Database: Sensitive data storage, only accessible by application servers.

Internal Load Balancer: Manages traffic among app servers.

WAF: Can be used internally as well for defense-in-depth.

Step 4: Add Connectivity and Security Controls

Internet Gateway: Allows resources in public subnet to communicate with the internet.

NAT Gateway: Allows outbound internet traffic from private subnet without exposing private IPs.

Security Groups: Firewalls at the instance level; allow only necessary traffic (e.g., LB to web server, web server to DB).

Network ACLs: Subnet-level firewalls for additional control.

Step 5: Network Diagram Explanation (Based on Your Images)

Public Subnet (Top Layer)

Load Balancer

Accepts HTTPS traffic from customers.

Sends only necessary HTTP/HTTPS to web servers in public subnet.

WAF (Web Application Firewall)

Sits in front of Load Balancer.

Filters malicious requests (SQLi, XSS, etc.).

Autoscaling Group

Multiple web servers for redundancy and scalability.

Placed in public subnet to respond to traffic spikes.

Private Subnet (Bottom Layer)

## Application Servers

Receive requests from public subnet's load balancer.

Not directly exposed to the internet.

## Database

Only accessible from application servers, never public.

Security groups restrict all inbound traffic except from app servers.

## Internal Load Balancer

Balances requests to application servers.

## Step 6: Flow of Data (Step-by-Step)

Client - > Internet Gateway - > WAF - > Load Balancer (Public Subnet): Customers initiate connections to your app over the internet.

Load Balancer - > Autoscaling Web Servers (Public Subnet): Load balancer routes requests to available web servers.

Web Servers - > Application Logic (Private Subnet): Web servers pass necessary requests to the internal application servers.

App Servers - > Database (Private Subnet): Application servers query/update customer payment data in the database.

Outbound (NAT Gateway): App servers may need to access updates or external APIs—use NAT Gateway for secure outbound connections.

## Step 7: Security Best Practices

Security Groups: Only allow necessary ports (e.g., 443 for HTTPS to LB, 3306 for MySQL between app server and DB).

Network ACLs: Add another layer of subnet-level restrictions.

Encryption: Use HTTPS for all external connections, encrypt data at rest and in transit (TLS, disk encryption).

IAM Roles/Policies: Principle of least privilege for accessing resources.

Monitoring/Logging: Enable VPC flow logs, cloud service logs, and application logging.

Patch Management: Automate patching for OS and applications.

Backups: Regular, secure backups of critical data.

## Step 8: Compliance Considerations

For payment applications (PCI DSS):

Isolate cardholder data environment (CDE).

Strong access controls (multi-factor authentication, role separation).

Regular vulnerability assessments and penetration testing.

Retain logs for auditing.

Step 9: Draw the Architecture (Summary)

Internet Gateway: Allows inbound/outbound internet access.

Public Subnet: WAF, Load Balancer, Autoscaling group.

Private Subnet: App servers, DB, internal LB.

NAT Gateway: Outbound access for private resources.

Security Groups/ACLs: Control all traffic flows.

Monitoring/Logging: Enabled at all levels.

Bonus: Sample Security Group Rules

Web Server (Public Subnet):

Inbound: 443 (HTTPS) from Internet

Outbound: 80/443 to App Servers

App Server (Private Subnet):

Inbound: 80/443 from Web Servers

Outbound: 3306 (MySQL) to Database

Database (Private Subnet):

Inbound: 3306 from App Servers

Outbound: None (unless replication required)

References to Security+ Domains

1.0 General Security Concepts: Principle of least privilege, defense in depth.

2.0 Threats, Vulnerabilities, Mitigations: WAF, segmentation, patching.

3.0 Security Architecture: Network segmentation, secure design.

4.0 Security Operations: Monitoring, logging, response.

Questions # 42:

Which of the following is prevented by proper data sanitization?

**Options:**

A.

Hackers ' ability to obtain data from used hard drives

B.

Devices reaching end-of-life and losing support

C.

Disclosure of sensitive data through incorrect classification

D.

Incorrect inventory data leading to a laptop shortage

**Answer**

A

**Explanation**

Detailed Explanation: Proper data sanitization ensures that sensitive data is securely erased from storage devices, preventing unauthorized access or recovery when the devices are disposed of or reused. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: " Data Sanitization and Disposal Methods " .

**To Get Premium Files for SY0-701 Visit**

**<https://www.certsmania.com/comptia/sy0-701-practice>**

**For More Free Questions Visit**

**<https://www.certsmania.com/comptia/pdf/sy0-701>**



**CertsMania**