CAS-005 Q&As

CompTIA SecurityX

Pass CompTIA CAS-005 Exam with 100% Guarantee

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

https://www.leads4pass.com/cas-005.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

After some employees were caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation.

Which of the following would the company most likely do to decrease this type of risk?

A. Improve firewall rules to avoid access to those platforms.

B. Implement a cloud-access security broker

C. Create SIEM rules to raise alerts for access to those platforms

D. Deploy an internet proxy that filters certain domains

Correct Answer: B

A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Implementing a CASB provides several benefits:

A. Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB. B. Implement a cloud-access security broker: A CASB can provide visibility into cloud application usage, enforce

data security policies, and protect against data leaks by monitoring and controlling access to cloud services. It also provides advanced features like data encryption, data loss prevention (DLP), and compliance monitoring.

C. Create SIEM rules to raise alerts for access to those platforms: This helps in monitoring but does not prevent data leaks.

D. Deploy an internet proxy that filters certain domains: This can block access to specific sites but lacks the granular control and visibility provided by a CASB. Implementing a CASB is the most comprehensive solution to decrease the risk of

data leaks by providing visibility, control, and enforcement of security policies for cloud services.

References:

CompTIA Security+ Study Guide

Gartner, "Magic Quadrant for Cloud Access Security Brokers" NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"

QUESTION 2

An organization has deployed a cloud-based application that provides virtual event services globally to clients. During a typical event, thousands of users access various entry pages within a short period of time. The entry pages include sponsor-related content that is relatively static and is pulled from a database. When the first major event occurs, users report poor response time on the entry pages. Which of the following features is the most appropriate for the company to implement?

A. Horizontal scalability

B. Vertical scalability

C. Containerization

D. Static code analysis

E. Caching

Correct Answer: E

Caching is the most appropriate feature for the company to implement in this scenario. Caching involves storing frequently accessed data closer to the user, reducing the need to retrieve data from the original source repeatedly. In the context of the virtual event services application, caching sponsor-related content on the entry pages can significantly improve response times for users. This approach leverages the static nature of the content and reduces the load on the database during peak usage times.

QUESTION 3

A software development company needs to mitigate third-party risks to its software supply chain. Which of the following techniques should the company use in the development environment to best meet this objective?

A. Performing software composition analysis

B. Requiring multifactor authentication

C. Establishing coding standards and monitoring for compliance

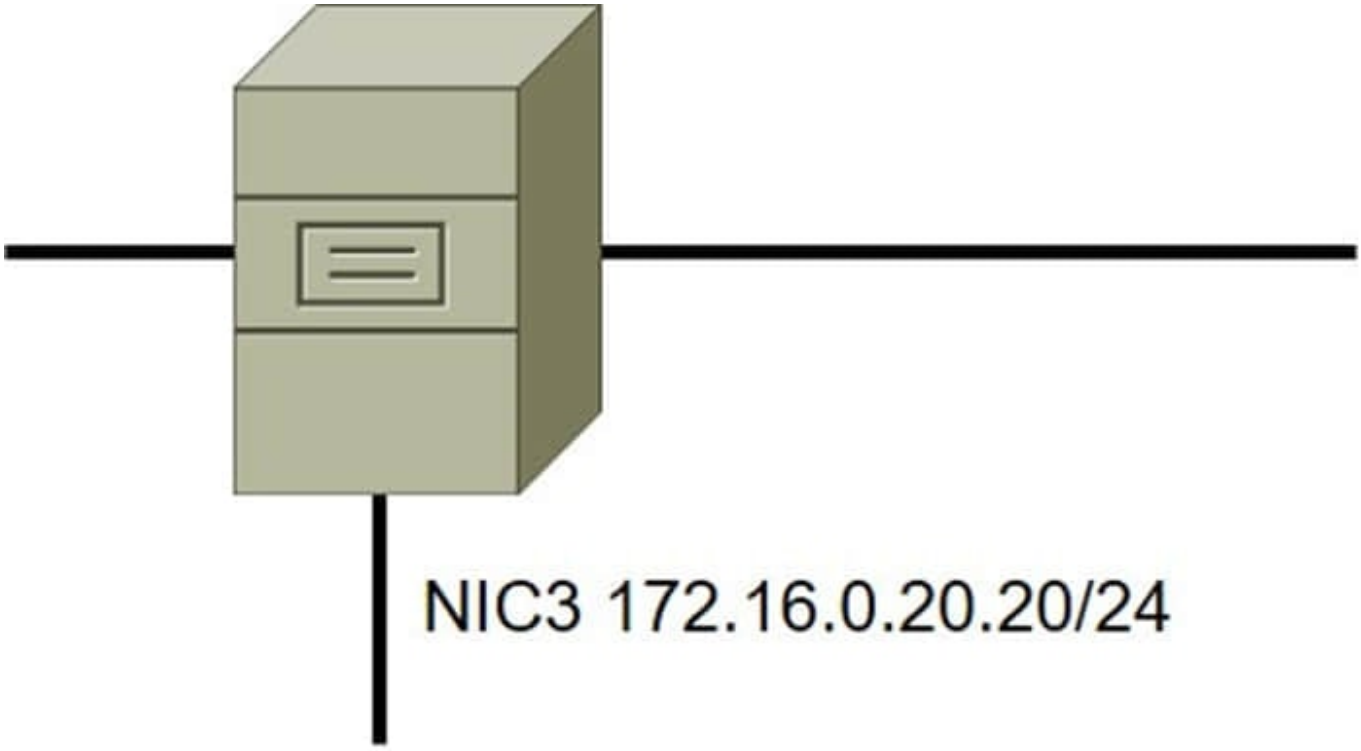
D. Implementing a robust unit and regression-testing scheme

Correct Answer: A

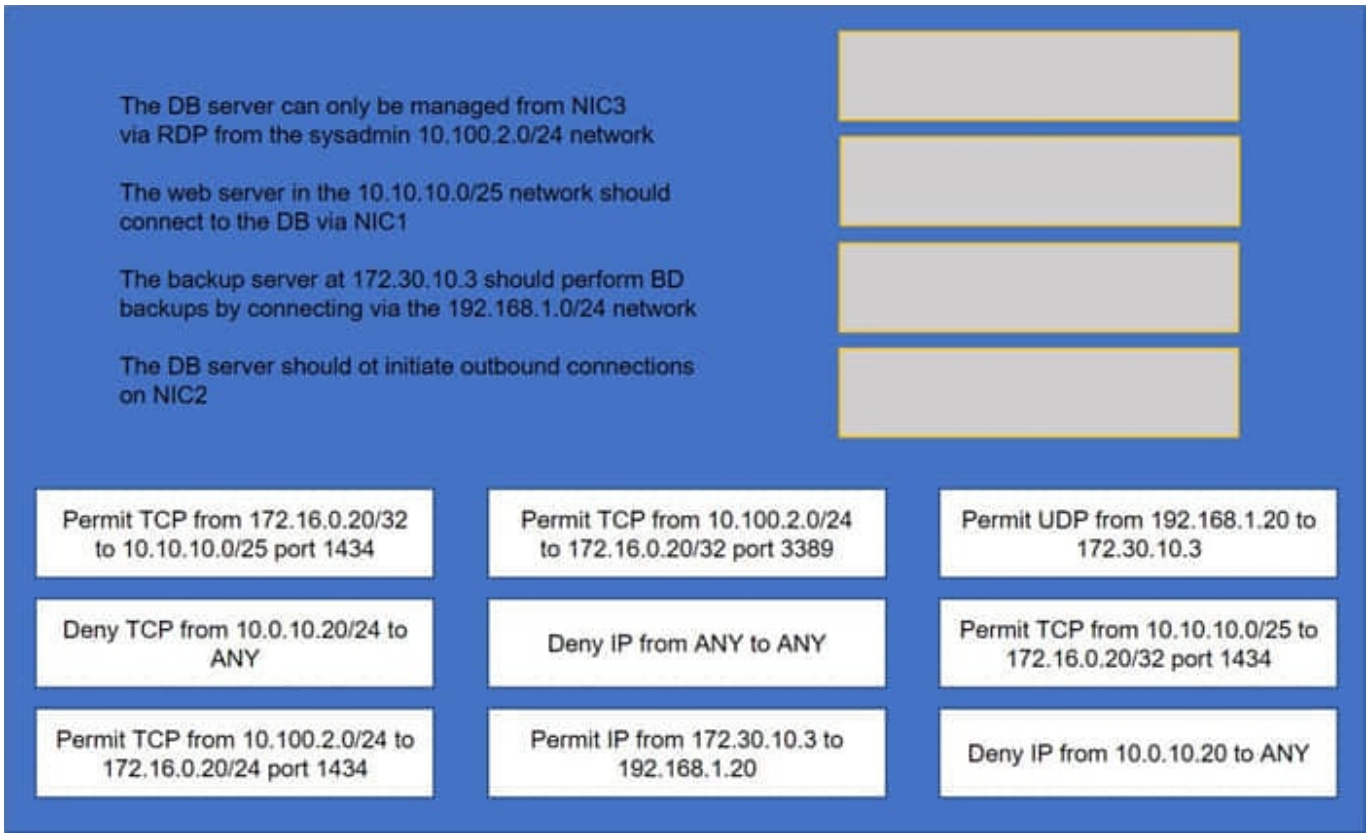
QUESTION 4

DRAG DROP

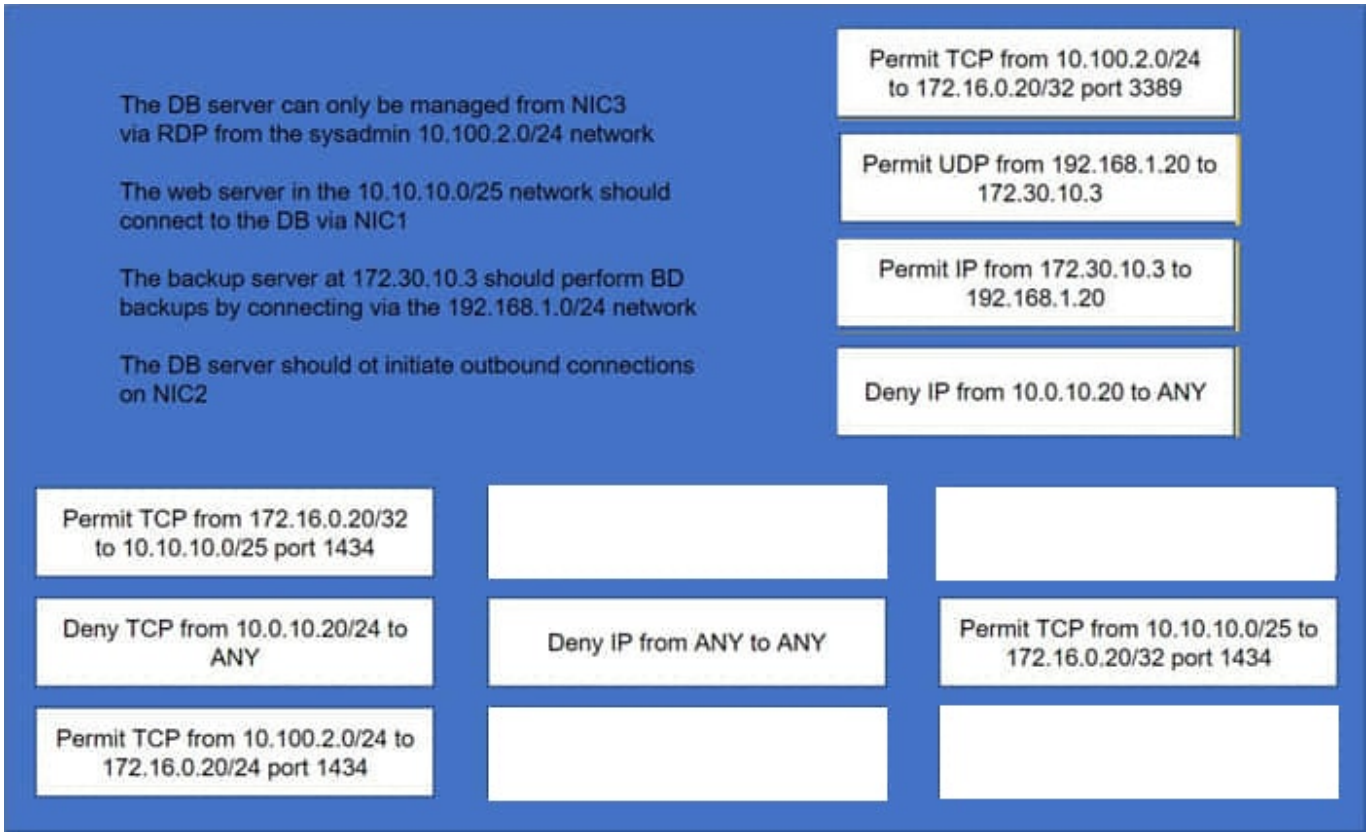
A security administrator must configure the database server shown below the comply with the four requirements listed. Drag and drop the appropriate ACL that should be configured on the database server to its corresponding requirement. Answer options may be used once or not at all.



Select and Place:



Correct Answer:



QUESTION 5

A security analyst is reviewing suspicious log-in activity and sees the following data in the SICM:

Account	Application	Authorization server	Status	Risk
SALES1	Customer manager	LDAP-US	Success	Low
SALES1	Payroll	LDAP-US	Success	Low
ADMIN	Email	LDAP-US	Failure	High
SALES1	Email	LDAP-EU	Unknown	Unknown
MARKET1	Customer manager	LDAP-US	Success	Low
FINANCE1	Payroll	LDAP-EU	Unknown	Unknown

Which of the following is the most appropriate action for the analyst to take?

A. Update the log configuration settings on the directory server that Is not being captured properly.

B. Have the admin account owner change their password to avoid credential stuffing.

C. Block employees from logging in to applications that are not part of their business area.

D. implement automation to disable accounts that nave been associated with high-risk activity.

Correct Answer: D

The log-in activity indicates a security threat, particularly involving the ADMIN account with a high-risk failure status. This suggests that the account may be targeted by malicious activities such as credential stuffing or brute force attacks.

Updating log configuration settings (A) may help in better logging future activities but does not address the immediate threat. Changing the admin account password (B) is a good practice but may not fully mitigate the ongoing threat if the

account has already been compromised. Blocking employees (C) from logging into non-business applications might help in reducing attack surfaces but doesn\\'t directly address the compromised account issue.

Implementing automation to disable accounts associated with high-risk activities ensures an immediate response to the detected threat, preventing further unauthorized access and allowing time for thorough investigation and remediation.

References:

CompTIA SecurityX guide on incident response and account management. Best practices for handling compromised accounts. Automation tools and techniques for security operations centers (SOCs).

QUESTION 6

Emails that the marketing department is sending to customers are pomp to the customers\\' spam folders. The security team is investigating the issue and discovers that the certificates used by the email server were reissued, but DNS records had not been updated.

Which of the following should the security team update in order to fix this issue? (Select three.)

A. DMARC

B. SPF

C. DKIM

D. DNSSEC

E. SASC

F. SAN

G. SOA

H. MX

Correct Answer: ABC

To prevent emails from being marked as spam, several DNS records related to email authentication need to be properly configured and updated when there are changes to the email server\\'s certificates:

A. DMARC (Domain-based Message Authentication, Reporting and Conformance):

DMARC records help email servers determine how to handle messages that fail SPF or DKIM checks, improving email deliverability and reducing the likelihood of emails being marked as spam. B. SPF (Sender Policy Framework): SPF

records specify which mail servers are authorized to send email on behalf of your domain. Updating the SPF record ensures that the new email server is recognized as an authorized sender. C. DKIM (DomainKeys Identified Mail): DKIM adds

a digital signature to email headers, allowing the receiving server to verify that the email has not been tampered with and is from an authorized sender. Updating DKIM records ensures that emails are properly signed and authenticated. D.

DNSSEC (Domain Name System Security Extensions): DNSSEC adds security to DNS by enabling DNS responses to be verified. While important for DNS security, it does not directly address the issue of emails being marked as spam. E.

SASC: This is not a relevant standard for this scenario. F. SAN (Subject Alternative Name): SAN is used in SSL/TLS certificates for securing multiple domain names, not for email delivery issues. G. SOA (Start of Authority): SOA records are

used for DNS zone administration and do not directly impact email deliverability.

H. MX (Mail Exchange): MX records specify the mail servers responsible for receiving email on behalf of a domain. While important, the primary issue here is the authentication of outgoing emails, which is handled by SPF, DKIM, and

DMARC.

References:

CompTIA Security+ Study Guide

RFC 7208 (SPF), RFC 6376 (DKIM), and RFC 7489 (DMARC) NIST SP 800-45, "Guidelines on Electronic Mail Security"

QUESTION 7

A company has data it would like to aggregate from its PLCs for data visualization and predictive maintenance purposes. Which of the following is the most likely destination for the tag data from the PLCs?

A. External drive

B. Cloud storage

C. System aggregator

D. Local historian

Correct Answer: D

PLCs (Programmable Logic Controllers) are commonly used in industrial automation to control machinery and processes. They generate a significant amount of data known as tag data, which includes real-time information about variables such as temperatures, pressures, and other operational parameters.

A local historian is a dedicated software or system component used in industrial automation environments to collect, store, and manage tag data from PLCs. The local historian typically resides on-site or within the industrial network environment. Its primary function is to capture and archive historical data from PLCs at a high frequency, providing insights into the operational history and trends of the industrial processes.

QUESTION 8

An organization wants to create a threat model to identity vulnerabilities in its infrastructure.

Which of the following, should be prioritized first?

A. External-facing Infrastructure with known exploited vulnerabilities

B. Internal infrastructure with high-seventy and Known exploited vulnerabilities

C. External facing Infrastructure with a low risk score and no known exploited vulnerabilities

D. External-facing infrastructure with a high risk score that can only be exploited with local access to the resource

Correct Answer: A

When creating a threat model to identify vulnerabilities in an organization\\'s infrastructure, prioritizing external-facing infrastructure with known exploited vulnerabilities is critical.

Here\\'s why:

Exposure to Attack: External-facing infrastructure is directly exposed to the internet, making it a primary target for attackers. Any vulnerabilities in this layer pose an immediate risk to the organization\\'s security. Known Exploited Vulnerabilities:

Vulnerabilities that are already known and exploited in the wild are of higher concern because they are actively being used by attackers. Addressing these vulnerabilities reduces the risk of exploitation significantly. Risk Mitigation: By

prioritizing external-facing infrastructure with known exploited vulnerabilities, the organization can mitigate the most immediate and impactful threats, thereby improving overall security posture.

QUESTION 9

A vulnerability can on a web server identified the following:

```
* TLS 1.2 Cipher Suites:
The server accepted the following 4 cipher suites:
TLS_RSA_WITH_DES_CBC_SHA                    56
TLS_RSA_WITH_AES_128_CBC_SHA                128
TLS_RSA_WITH_3DES_EDE_CBC_SHA               168
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA           168 DH (1024 bits)
```

Which of the following actions would most likely eliminate on path decryption attacks? (Select two).

A. Disallowing cipher suites that use ephemeral modes of operation for key agreement

B. Removing support for CBC-based key exchange and signing algorithms

C. Adding TLS_ECDHE_ECDSA_WITH_AE3_256_GCMS_HA256

D. Implementing HIPS rules to identify and block BEAST attack attempts

E. Restricting cipher suites to only allow TLS_RSA_WITH_AES_128_CBC_SHA

F. Increasing the key length to 256 for TLS_RSA_WITH_AES_128_CBC_SHA

Correct Answer: BC

On-path decryption attacks, such as BEAST (Browser Exploit Against SSL/TLS) and other related vulnerabilities, often exploit weaknesses in the implementation of CBC (Cipher Block Chaining) mode. To mitigate these attacks, the following actions are recommended:

B. Removing support for CBC-based key exchange and signing algorithms: CBC mode is vulnerable to certain attacks like BEAST. By removing support for CBC- based ciphers, you can eliminate one of the primary vectors for these attacks. Instead, use modern cipher modes like GCM (Galois/Counter Mode) which offer better security properties.

C. Adding TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256: This cipher suite uses Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for key exchange, which provides perfect forward secrecy. It also uses AES in GCM mode, which is not susceptible to the same attacks as CBC. SHA-256 is a strong hash function that ensures data integrity. References: CompTIA Security+ Study Guide NIST SP 800-52 Rev. 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations" OWASP (Open Web Application Security Project) guidelines on cryptography and secure communication

---

QUESTION 10

A network engineer must ensure that always-on VPN access is enabled Curt restricted to company assets

Which of the following best describes what the engineer needs to do\\'?

A. Generate device certificates using the specific template settings needed

B. Modify signing certificates in order to support IKE version 2

C. Create a wildcard certificate for connections from public networks

D. Add the VPN hostname as a SAN entry on the root certificate

Correct Answer: A

To ensure always-on VPN access is enabled and restricted to company assets, the network engineer needs to generate device certificates using the specific template settings required for the company\\'s VPN solution. These certificates

ensure that only authorized devices can establish a VPN connection.

Why Device Certificates are Necessary:

Authentication: Device certificates authenticate company assets, ensuring that only authorized devices can access the VPN.

Security: Certificates provide a higher level of security compared to username and password combinations, reducing the risk of unauthorized access. Compliance: Certificates help in meeting security policies and compliance requirements by

ensuring that only managed devices can connect to the corporate network.

Other options do not provide the same level of control and security for always-on VPN access:

B. Modify signing certificates for IKE version 2: While important for VPN protocols, it does not address device-specific

authentication. C. Create a wildcard certificate: This is not suitable for device-specific authentication and could introduce

security risks. D. Add the VPN hostname as a SAN entry: This is more related to certificate management and does not ensure device-specific authentication.

References:

CompTIA SecurityX Study Guide

"Device Certificates for VPN Access," Cisco Documentation NIST Special Publication 800-77, "Guide to IPsec VPNs"

QUESTION 11

A Chief Information Security Officer (CISO) received a call from the Chief Executive Officer (CEO) about a data breach from the SOC lead around 9:00 a.m. At 10:00 a.m. The CEO informs the CISO that a breach of the firm is being reported on national news. Upon investigation, it is determined that a network administrator has reached out to a vendor prior to the breach for information on a security patch that failed to be installed. Which of the following should the CISO do to

prevent this from happening again?

A. Properly triage events based on brand imaging and ensure the CEO is on the call roster.

B. Create an effective communication plan and socialize it with all employees.

C. Send out a press release denying the breach until more information can be obtained.

D. Implement a more robust vulnerability identification process.

Correct Answer: B

QUESTION 12

A security architect for a global organization with a distributed workforce recently received funding lo deploy a CASB solution

Which of the following most likely explains the choice to use a proxy-based CASB?

A. The capability to block unapproved applications and services is possible

B. Privacy compliance obligations are bypassed when using a user-based deployment.

C. Protecting and regularly rotating API secret keys requires a significant time commitment

D. Corporate devices cannot receive certificates when not connected to on-premises devices

Correct Answer: A

A proxy-based Cloud Access Security Broker (CASB) is chosen primarily for its ability to block unapproved applications and services. Here\\'s why:

Application and Service Control: Proxy-based CASBs can monitor and control the use of applications and services by

inspecting traffic as it passes through the proxy. This allows the organization to enforce policies that block unapproved

applications and services, ensuring compliance with security policies. Visibility and Monitoring: By routing traffic through the proxy, the CASB can provide detailed visibility into user activities and data flows, enabling better monitoring and

threat detection.

Real-Time Protection: Proxy-based CASBs can provide real-time protection against threats by analyzing and controlling traffic before it reaches the end user, thus preventing the use of risky applications and services.

QUESTION 13

A company has been the target of LDAP injections, as well as brute-force, whaling, and spear-phishing attacks. The company is concerned about ensuring continued system access. The company has already implemented a SSO system with strong passwords. Which of the following additional controls should the company deploy?

A. Two-factor authentication

B. Identity proofing

C. Challenge questions

D. Live identity verification

Correct Answer: A

QUESTION 14

Two companies that recently merged would like to unify application access between the companies, without initially merging internal authentication stores. Which of the following technical strategies would best meet this objective?

A. Federation

B. RADIUS

C. TACACS+

D. MFA

E. ABAC

Correct Answer: A

Federation (option A) is the best technical strategy for allowing two recently merged companies to unify application access while keeping their internal authentication stores separate. It provides a secure, seamless, and standardized approach to authentication and authorization across organizational boundaries, ensuring efficient and controlled access to shared applications and resources.

QUESTION 15

A security engineer is implementing DLP. Which of the following should the security engineer include in the overall DLP

strategy?

A. Tokenization

B. Network traffic analysis

C. Data classification

D. Multifactor authentication

Correct Answer: C