Cisco 300-745 Practice Test

Shared by Martin on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A pharmaceutical company needs a hub-and-spoke VPN topology. The design must be capable of building either partial or full mesh overlay networks. Which VPN solution must be implemented in the environment?

Options:

A- DMVPN
B- L2TP
C- crypto maps
D- SSL VPN

Answer:

A

Explanation:

In the context of the Designing Cisco Security Infrastructure (300-745 SDSI) blueprint, Dynamic Multipoint VPN (DMVPN) is the specialized architectural solution designed for scalable hub-and-spoke topologies that require the flexibility to evolve into partial or full mesh overlays. DMVPN leverages a combination of Multipoint GRE (mGRE) tunnels, Next Hop Resolution Protocol (NHRP), and IPsec encryption to create a dynamic environment.

The primary advantage of DMVPN is its ability to establish 'on-demand' tunnels between spoke sites. In a traditional hub-and-spoke model, traffic between two spokes must transit the hub, which introduces latency and increases hub resource consumption. With DMVPN, spokes can use NHRP to discover the public IP addresses of other spokes and build direct tunnels between them automatically. This allows the pharmaceutical company to maintain a simple hub-and-spoke management model while benefiting from the performance of a full mesh when traffic patterns demand it.

While SSL VPNs (Option D) and L2TP (Option B) are excellent for individual remote access, they are not designed for site-to-site mesh scalability. Crypto maps (Option C) represent the legacy method of building IPsec tunnels, which requires static, manual configuration of every peer relationship---making a full mesh practically impossible to manage at scale. DMVPN fulfills the Cisco SDSI objective of designing highly available and flexible secure infrastructure by automating the complexity of large-scale tunnel management.

Question 2

Question Type: MultipleChoice

A company recently discovered that a former employee, who left to join a competitor, continued to access and exfiltrate sensitive data over several weeks after leaving. The breach highlighted vulnerabilities in the organization's data security and access management practices. To prevent such incidents in the future, the organization must adopt measures that detect and restrict unauthorized data access and transfer. Which mitigation strategy must be implemented to address the issue?

Options:

A- Implement web application firewall.
B- Upgrade network policy access.
C- Implement data loss prevention strategy.
D- Deploy audit logging and monitoring solution.

Answer:

C

Explanation:

The scenario describes a typical 'insider threat' involving data exfiltration. While the initial failure was likely in the off-boarding process (Identity Management), the technical control required to specifically 'detect and restrict unauthorized data access and transfer' is a Data Loss Prevention (DLP) strategy. DLP solutions are designed to monitor, detect, and block sensitive data from leaving the organization's control.

A robust DLP strategy---integrated across Cisco platforms like Email Security (ESA), Web Security (WSA), and Cisco Umbrella---works by identifying sensitive content (such as customer lists, proprietary code, or financial data) using techniques like fingerprinting or keyword matching. If an unauthorized attempt is made to upload this data to a personal cloud drive or send it via email, the DLP engine intercepts and blocks the transfer. While Audit Logging (Option D) is essential for forensic investigation after the fact, it does not 'restrict' the transfer in real-time. WAFs (Option A) protect against external attacks on web servers, and Network Policies (Option B) control traffic flow but generally lack the content-awareness required to identify sensitive business data. Implementing DLP ensures that the organization's intellectual property remains protected even if an account remains active or a user has legitimate network access.

Question 3

Question Type: MultipleChoice

A company has been facing recurring issues with SQL injection vulnerabilities affecting the products, leading to significant disruptions for customers. To address the security concerns proactively, the company wants to integrate a tool into the CI/CD pipeline. The tool must be capable of identifying vulnerabilities such as SQL injection early in the development process, which allows developers to rectify issues before the code is deployed. Which solution must be implemented to meet the requirement?

Options:

A- Static Application Security Testing tools, such as Checkmarx, Fortify, SonarQube
B- build log observability tools, such as Splunk, Datadog
C- workflow automation tools, such as GitHub Actions, Azure
D- Dynamic Application Security Testing tools, such as OWASP ZAP, Veracode, Burp Suite

Answer:

A

Explanation:

In the framework of the Designing Cisco Security Infrastructure (300-745 SDSI) curriculum, the 'Shift-Left' security strategy is fundamental to modern DevSecOps. To identify vulnerabilities like SQL injection at the earliest possible stage---specifically before the code is even compiled or deployed---Static Application Security Testing (SAST) is the required solution. SAST tools analyze the application's source code, byte code, or binaries without actually executing the program.

By integrating SAST tools like Checkmarx or SonarQube into the CI/CD pipeline, the security team can automate the scanning of every code commit or pull request. These tools use sophisticated algorithms to trace data flows and identify dangerous patterns, such as user-controlled input being concatenated directly into SQL queries without proper sanitization or parameterization. This proactive approach allows developers to receive immediate feedback within their native workflow, enabling them to fix security flaws before they progress into later, more expensive stages of the development lifecycle.

In contrast, Dynamic Application Security Testing (DAST) (Option D) requires a running instance of the application and typically occurs much later in the pipeline, such as during the testing or staging phase. While DAST is excellent for finding runtime vulnerabilities, it does not meet the requirement of identifying issues 'early in the development process' as effectively as SAST. Build log observability tools (Option B) and workflow automation platforms (Option C) provide

infrastructure and visibility but do not possess the specialized engine required to perform deep code analysis for application-layer vulnerabilities like SQL injection. Implementing SAST ensures that security is a foundational element of the code-writing phase, aligning with Cisco's vision for a secure, automated software supply chain.

Question 4

Question Type: MultipleChoice

An IT company operates an application in a SaaS model. The administrative tasks, such as customer onboarding, within the application must be restricted to users who are on the corporate network where admins can access those functions via a web browser or a smartphone application. Which application technology must be used to provide granular control based on function?

Options:

A- VPC
B- RBAC
C- security group
D- Service Mesh

Answer:

B

Explanation:

The requirement to restrict administrative tasks like 'customer onboarding' to specific users based on their job function is a classic use case for Role-Based Access Control (RBAC). In the context of application security design, RBAC is the mechanism that maps a user's identity to a specific set of permissions within the application.

According to Cisco Security Infrastructure principles, RBAC ensures the principle of least privilege by ensuring that an 'Admin' role has access to onboarding functions, while a 'Support' or 'Standard User' role does not. This control is independent of the network layer and is enforced at the application or identity provider level. While a VPC (Option A) or Security Groups (Option C) provide network-layer isolation and can ensure the user is on the corporate network (by filtering IP ranges), they cannot distinguish between different functions or actions performed within the application once the connection is established. A Service Mesh (Option D) is used for microservices communication and can provide some authorization, but RBAC is the primary

architectural approach for defining 'who can do what' within an application interface. Implementing RBAC allows the SaaS provider to secure sensitive administrative workflows, ensuring that only authorized personnel can modify customer data or system configurations.

========

Question 5

Question Type: MultipleChoice

A global marketing firm, based in California with customers on every continent, suffered a data breach that exposed employee and customer PII. Which regulations is the company in danger of violating?

Options:

A- ISO SP800-53
B- FedRamp
C- GDPR
D- ISO27001

Answer:

C

Explanation:

The General Data Protection Regulation (GDPR) is a comprehensive data privacy law in the European Union (EU) that has a significant global reach. For a California-based marketing firm with customers on every continent, any breach involving the Personally Identifiable Information (PII) of European residents triggers immediate and severe legal exposure under GDPR. This regulation is unique because of its extraterritorial application; it mandates that any entity---regardless of its physical headquarters---must comply if they offer goods or services to, or monitor the behavior of, individuals located within the EU.

In the event of a data breach, GDPR requires organizations to notify the relevant supervisory authority within 72 hours and, in cases of high risk, notify the affected individuals without undue delay. Failure to implement adequate technical and organizational measures to protect data can result in astronomical fines of up to 20 million or 4% of annual global turnover, whichever is higher. While other frameworks like NIST SP 800-53 (often confused with ISO in Option A) or ISO 27001 (Option D) provide the architectural standards and controls to prevent such incidents, they

are voluntary standards or frameworks, not legally binding regulations that a company 'violates' in the same sense as GDPR. FedRAMP (Option B) is specific to US federal government cloud service providers and would not typically apply to a private marketing firm's global operations. Thus, GDPR represents the primary regulatory threat for a global firm handling international PII.

========

Question 6

Question Type: MultipleChoice

A technology company has many remote workers who access corporate resources from various locations. The company must ensure that security policies are managed and enforced directly on endpoints, and endpoints are protected from threats regardless of location. Which firewall architecture meets the requirements?

Options:

A- next-generation firewall
B- host-based firewall
C- web application firewall
D- traditional firewall

Answer:

B

Explanation:

As organizations shift toward a 'borderless' or hybrid work model, the traditional perimeter-based security model becomes insufficient. When employees work from home, coffee shops, or airports, they are no longer behind the enterprise's physical Next-Generation Firewall (NGFW) (Option A). To ensure that security policies are enforced 'regardless of location,' the security must move with the device.

A host-based firewall is a software-defined firewall that resides directly on the endpoint (laptop, workstation, or server). In the Cisco ecosystem, this is often a component of Cisco Secure Client or Cisco Secure Endpoint. Because the firewall is local to the operating system, it can enforce strict inbound and outbound traffic rules even when the user is not connected to a VPN. This protects the device from lateral movement threats on untrusted local networks (like a public Wi-Fi) and ensures that only authorized applications can communicate over the network.

While an NGFW (Option A) provides superior deep packet inspection for the corporate perimeter, and a Web Application Firewall (WAF) (Option C) protects web servers from application-layer attacks, neither provides the local, location-independent protection required for a distributed remote workforce. Implementing a host-based firewall aligns with the Zero Trust architecture promoted by Cisco, where the endpoint itself becomes a micro-perimeter capable of self-protection.