Designing Cisco Security Infrastructure (SDSI) v1.0

Cisco 300-745

Version Demo

Total Demo Questions: 7

Total Premium Questions: 77

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Strategy and Design	20
Topic 2, Network Security Segmentation	3
Topic 3, Secure Connectivity	5
Topic 4, Security of Cloud and Data Center	13
Topic 5, Endpoint Protection and Detection	9
Topic 6, Secure Network Access, Visibility, and Enforcement	27
Total	77

QUESTION NO: 1

Which benefit does AI provide in network security?

A. It speeds up network data transmission rates.

B. It replaces comprehensive defense in depth.

C. It provides complete protection from DDoS attacks.

D. It identifies vulnerabilities associated with weak TLS algorithms.

ANSWER: D

Explanation:

It identifies vulnerabilities associated with weak TLS algorithms. AI provides security teams with scalable analysis of network telemetry, including encrypted-traffic metadata and TLS session characteristics. Rather than requiring an analyst to manually inspect every connection, AI and machine-learning models can correlate patterns across a large environment and highlight traffic that uses outdated protocol versions, weak cipher suites, or other cryptographic configurations that do not meet an organization's security policy. This improves visibility into exposure that may otherwise be difficult to find in busy networks, especially where payload decryption is impractical, undesirable, or unavailable.

This capability supports a proactive security workflow: identify systems with obsolete encryption settings, prioritize them according to context and risk, and remediate the configuration before the weakness can contribute to a compromise. Cisco's encrypted-traffic analytics approach demonstrates how security telemetry can be analyzed to provide useful detection and visibility without relying solely on decrypting traffic. Cisco also describes AI-driven security capabilities as helping organizations analyze security signals and prioritize threats at scale. See Cisco Encrypted Traffic Analytics and Cisco AI Defense.

QUESTION NO: 2

A technology company recently onboarded a new customer in the medical space. The customer needs a solution to provide data integrity across remote sites. Which solution must be used to meet this requirement?

A. hashing

B. data masking

C. preshared key

D. authentication

ANSWER: A

Explanation:

hashing is the appropriate solution because it provides a dependable mechanism for detecting whether data has changed. A cryptographic hash function processes data and produces a fixed-length digest. The sending site generates this digest for the original data, and the receiving site independently calculates a digest after receipt. Matching digests demonstrate that the received content is the same as the content on which the original digest was calculated. Because a cryptographic hash is highly sensitive to input changes, even a very small modification produces a substantially different digest.

For medical data shared among remote locations, this verification is important because clinical records, diagnostic results, and other sensitive information must remain accurate throughout transmission and handling. In practice, integrity protection is commonly delivered through secure protocols and VPN mechanisms that use secure hash algorithms or message-authentication codes. These mechanisms bind integrity verification to protected communications and allow a receiving endpoint to detect modification. Cisco documents the use of integrity algorithms in IPsec to ensure that packets are not altered in transit, including HMAC-based SHA algorithms: Cisco IPsec Integrity Configuration Guide. The foundational behavior and security properties of SHA-2 hash functions are specified by NIST in FIPS PUB 180-4.

QUESTION NO: 3

A furniture company recently discovered that the endpoint detection and response configuration flagged several malicious files on company-managed laptops. The company must enhance security to prevent known malicious files from being delivered to the network and endpoints. The new solution must enhance the company's ability to inspect and filter incoming traffic effectively. Which security product must be used to accomplish this goal?

A. next-generation firewall

B. traditional firewall

C. host-based firewall

D. eBPF

ANSWER: A

Explanation:

The **next-generation firewall** is the appropriate product because it provides application-aware, deep inspection of traffic entering the organization and can enforce security policy beyond basic IP address, port, and protocol filtering. In a Cisco security design, a next-generation firewall such as Cisco Secure Firewall can inspect network flows, identify applications, and integrate intrusion prevention and malware defenses to detect and block threats before content reaches internal systems. This gives the company a preventive network control that complements its endpoint detection and response deployment.

For the stated requirement, the important capability is inspection of inbound traffic and filtering based on threat intelligence and file or malware indicators. Cisco Secure Firewall's malware-defense capabilities can use file reputation information to identify known malicious files and block their transfer, reducing the likelihood that those files are delivered to managed laptops. Policies can be applied at the network perimeter or other enforcement points so that potentially harmful content is stopped before endpoint execution and subsequent EDR alerts. This layered approach improves both visibility and prevention by combining endpoint telemetry with inline network inspection and enforcement. Cisco describes these capabilities in its Next-Generation Firewall overview and Cisco Secure Firewall product information.

QUESTION NO: 4

A software development company uses multiple cloud providers to host applications. The company is designing a scalable firewall solution that must meet the requirements:

Consistent security policies across multiple cloud environments.

Centralized visibility and management.

Scalability to accommodate different cloud platforms.

Which type of firewall meets the requirements?

A. traditional firewall

B. zone-based firewall

C. distributed firewall

D. host-based firewall

ANSWER: C

Explanation:

distributed firewall is the appropriate choice because it distributes enforcement close to workloads while allowing security teams to define and manage policy centrally. This model is well suited to applications spread across separate cloud environments because policy is based on workload identity, application context, and desired communications rather than

being dependent on a single physical perimeter. As workloads are created, moved, scaled, or retired, the distributed enforcement model can apply the same centrally governed segmentation policy at each relevant enforcement point.

Centralized policy management also gives operations teams a unified way to define allowed application flows, monitor policy implementation, and maintain consistent controls across a heterogeneous environment. This supports scalable east-west security for dynamic application components while avoiding a design in which all traffic must traverse one fixed inspection location. Cisco describes workload-centric segmentation and policy enforcement as core capabilities of Cisco Secure Workload, including visibility into application dependencies and centralized policy management for workloads across data centers and cloud environments. These capabilities align directly with the stated requirements for consistent multi-cloud policy, centralized visibility, and scalable enforcement. See Cisco Secure Workload and Cisco Secure Firewall.

QUESTION NO: 5

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?

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:

Static Application Security Testing tools, such as Checkmarx, Fortify, SonarQube is correct because static application security testing analyzes application source code, bytecode, or binaries without needing the application to be running. This makes it well suited to CI/CD integration: scans can run automatically when developers commit code, open pull requests, or build an artifact, and findings can be returned before the software reaches a deployment stage. For recurring SQL injection issues, static analysis can trace potentially untrusted input through application code and identify unsafe database-query construction or missing parameterization. Developers can then remediate the vulnerable code while the change is still small, reviewable, and inexpensive to fix. Security gates can also enforce organizational policy by failing a build or preventing promotion when findings meet a defined severity threshold. OWASP describes static testing as reviewing source code or compiled code for security weaknesses and identifies it as a useful activity early in the software development life cycle. This approach supports the requested proactive, shift-left workflow by placing vulnerability detection directly in the development pipeline rather than relying on detection after release. See the OWASP Static Application Security Testing guidance and Cisco's Secure Application overview.

QUESTION NO: 6

A telecommunications company recently introduced a hybrid working model. Based on the new policy, employees can work remotely for 2 days per week if corporate equipment is used. The IT department is preparing corporate laptops to support users during the remote working days. Which solution must the IT department implement that provides secure connectivity to corporate resources and protects sensitive corporate data even if a laptop is stolen?

A. Secure Client

B. Cisco Duo

C. ISE Posture

D. Umbrella

ANSWER: A

Explanation:

Secure Client is the appropriate endpoint solution because it provides the remote-access VPN capability needed to establish authenticated, encrypted connectivity from a corporate laptop to private corporate resources. Cisco Secure Client supports SSL/TLS and IPsec/IKEv2 VPN connections, allowing the organization to apply remote-access policy consistently for hybrid workers. It is also a modular endpoint agent: alongside the VPN module, organizations can deploy posture-related capabilities that assess endpoint compliance, including whether required security controls such as disk encryption are enabled. This lets the organization restrict or remediate access for devices that do not meet its corporate security baseline. For the stolen-laptop scenario, the required endpoint data-protection controls, particularly full-disk encryption and centrally enforced device policy, protect locally stored corporate information from offline access; Secure Client helps enforce the access and posture model around that managed corporate endpoint. Its Always-On VPN capabilities can further ensure that corporate traffic is sent through the organization's protected security infrastructure whenever the device has network connectivity. Cisco documents Secure Client as its unified VPN and endpoint-security client, with modules for secure connectivity and posture assessment. See Cisco Secure Client and Cisco Secure Client feature information.

QUESTION NO: 7

A financial company uses a remote access solution that directs all traffic over a secure tunnel. The company recently received some large ISP bills from the headquarter location. According to traffic analysis during the investigation, most of the network traffic was due to employees spending a lot of time on video conferences provided by a SaaS collaboration company. What must the company modify to reduce the cost without negatively impacting security or employee experience?

A. Reduce the video resolution size permitted within the SaaS application.

B. Split-exclude the video SaaS application from the VPN.

C. Block the video conferencing app when connected on VPN.

D. Suggest users to disconnect from the VPN when on video calls.

ANSWER: B

Explanation:

Split-exclude the video SaaS application from the VPN is correct because the existing full-tunnel remote-access design backhauls all employee traffic, including high-bandwidth real-time video, through the headquarters Internet connection. This unnecessarily consumes centralized WAN/Internet capacity and drives ISP usage costs upward. A split-exclude policy identifies the approved collaboration SaaS application, typically by its documented destination domains, IP ranges, or application-aware policy, and sends that traffic directly from the user's local Internet connection rather than through the VPN headend.

This approach preserves the employee experience because video conferencing follows a shorter, lower-latency path to the SaaS provider instead of traversing the VPN concentrator and headquarters egress link. It can preserve security when the exception is tightly scoped to the trusted SaaS service and is combined with endpoint protection, DNS-layer security, secure web controls, and the provider's encrypted application sessions. Cisco Secure Client supports split-tunneling policy, including excluding defined traffic from the VPN tunnel; the organization should validate the SaaS provider's current network requirements before deployment and monitor the resulting policy. See Cisco's Secure Client Administrator Guide and Cisco's SASE guidance.