Free Cisco 300-745 SDSI Practice Questions

Shared by Cooley on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A bank experienced challenges with compromised endpoints gaining access to the internal network. To enhance security, the bank wants to ensure that all endpoints are scanned for compliance checks before being allowed to access the network. Which action achieves the level of security and control?

Options:

A- Use MFA using Cisco DUO.
B- Configure TrustSec using Cisco ISE.
C- Set up data loss prevention policy.
D- Implement Posture validation using Cisco ISE.

Answer:

D

Explanation:

In high-security environments like banking, simply verifying a user's identity is insufficient; the 'health' or security state of the device must also be validated. Posture validation, implemented through Cisco Identity Services Engine (ISE), is the specific architectural process used to ensure an endpoint meets the organization's security requirements---such as having an active antivirus, the latest OS patches, or disk encryption enabled---before it is granted access to the internal network.

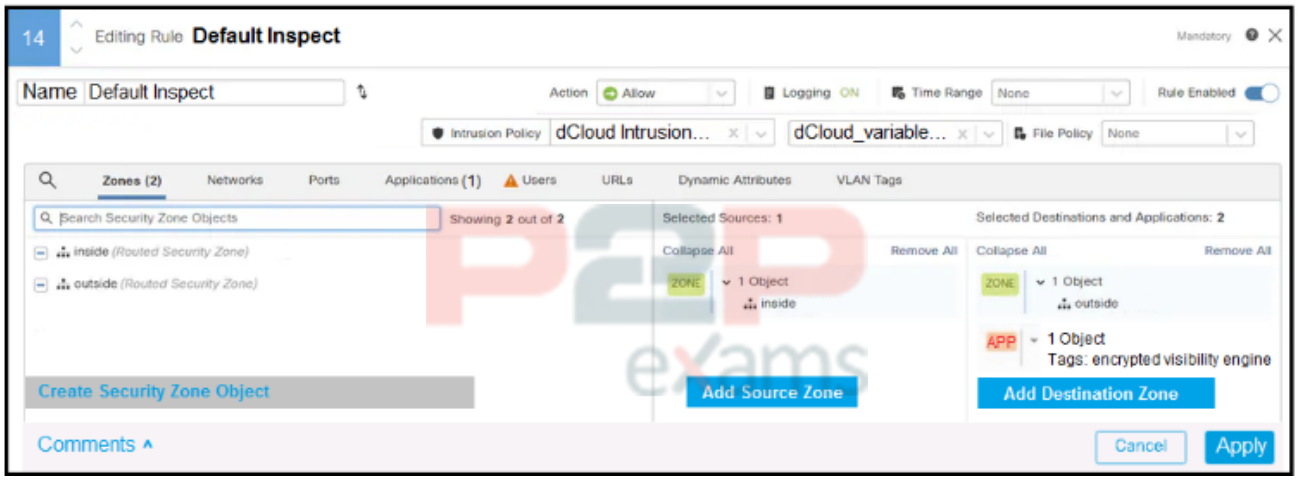
When an endpoint connects, Cisco ISE triggers a posture check (often via the Cisco Secure Client agent). If the device is found to be non-compliant (e.g., outdated signatures), ISE can move the endpoint into a restricted quarantine VLAN where it can only access remediation servers to update its software. Only after a successful re-scan shows the device is compliant is the network access policy updated to allow full internal connectivity. This effectively prevents compromised or 'dirty' endpoints from spreading threats laterally across the bank's network. While MFA (Option A) secures the user's identity and TrustSec (Option B) provides segmentation, only Posture validation addresses the technical compliance of the endpoint hardware and software itself. Data Loss Prevention (Option C) is focused on data transit rather than initial network admission control.

========

Question 2

Question Type: MultipleChoice

Refer to the exhibit.



In addition to SSL decryption, which firewall feature allows malware to be blocked?

Options:

A- DLP
B- SSL Offloading
C- URL Filtering
D- File Inspection

Answer:

D

Explanation:

Based on the provided exhibits, the correct firewall feature for blocking malware in this context is File Inspection.

In image_4c047c.png, we see a Cisco Secure Firewall Access Control Policy rule named 'Default Inspect'. This rule is configured to allow traffic from the 'inside' zone to the 'outside' zone while applying deep packet inspection. Crucially, the configuration includes a File Policy field, which is the mechanism used to perform malware analysis and file disposition lookups. By associating a File Policy with an Access Control rule, the firewall can inspect files as they transit the network, calculate their SHA-256 hash, and query the Cisco Collective Security Intelligence cloud to determine if the file is malicious, clean, or unknown.

The evidence of this feature in action is found in image_4b1ebe.png, which shows the Cisco

Secure Endpoint (formerly AMP for Endpoints) Device Trajectory. The 'Activity Details' pane specifically identifies a malicious file (iodnxvg.exe) categorized as W32.DFC.MalParent. While the log notes the file was not quarantined because it was in 'audit only mode,' the underlying technology performing the detection is File Inspection. This feature provides the necessary visibility into the contents of encrypted or unencrypted data streams to identify and---when properly configured in a 'Protect' or 'Block' mode---stop the execution of malware. This aligns with the Cisco SDSI objective of building a layered defense that combines perimeter traffic control with granular file-level security.

Question 3

Question Type: MultipleChoice

The network security team of a private university is conducting a comprehensive audit to evaluate the security posture across the network infrastructure. During the review, the security team found that a trusted vendor disclosed serious vulnerabilities identified in a product that plays a crucial role in the university's CI/CD pipeline. The security team must act promptly to mitigate the potential risks posed by these vulnerabilities. Which action must the security team take first in response to the disclosure?

Options:

A- Leverage IDS to measure the impact of the vulnerability.
B- Notify customers of the impact and its source.
C- Confirm impact by validating presence of the product in company's environment.
D- Patch the impacted product as soon as possible.

Answer:

C

Explanation:

According to the Cisco Security Incident Response lifecycle and the NIST SP 800-61 standards referenced in the SDSI objectives, the very first step in responding to a third-party vulnerability disclosure is Identification and Validation. Before a team can patch, notify stakeholders, or monitor for exploits, they must perform an asset inventory check to confirm whether the specific vulnerable version of the product is actually running within their environment.

In a complex CI/CD pipeline, multiple tools and versions coexist. Jumping straight to patching (Option D) without validation can lead to unnecessary downtime or 'breaking' integrated workflows if the vulnerability doesn't actually apply to the version in use. Similarly, using an IDS (Option A) is a detection/monitoring step that follows the confirmation of risk. Notifying

customers (Option B) is a later phase in the incident response process, usually reserved for confirmed breaches or significant service impacts. By confirming the presence and version of the software first, the security team can accurately assess the blast radius and prioritize remediation efforts based on the actual risk to the university's specific infrastructure. This systematic approach ensures that resources are allocated efficiently and that the security posture is managed based on verified data rather than assumptions.

========

Question 4

Question Type: MultipleChoice

Employees in a healthcare organization could not access their devices when they returned to work after the weekend. The security team discovered that a threat actor had encrypted the devices. Which security solution would mitigate the risk in future?

Options:

A- password policy enforcement
B- network configuration management
C- data loss prevention
D- endpoint detection and response

Answer:

D

Explanation:

In the scenario described, the healthcare organization fell victim to a ransomware attack, where devices were encrypted to extort the organization. To mitigate such risks in the future, Endpoint Detection and Response (EDR) is the essential architectural component. According to the Cisco SDSI Secure Infrastructure domain, protecting endpoints requires more than just traditional antivirus; it necessitates a solution that provides deep visibility into file behavior and process execution.

A robust EDR solution, such as Cisco Secure Endpoint, continuously monitors all activity on the device. When ransomware attempts to initiate its encryption process, the EDR can detect the malicious behavioral pattern in real-time. It can then take automated actions, such as isolating the infected host from the network and 'stopping' the encryption process before it spreads. Furthermore, Cisco's EDR provides retrospective security, allowing administrators to see how the malware arrived and which other devices it touched. While Option A (Password Policies)

helps prevent credential theft and Option C (DLP) prevents data theft, they do not stop the technical process of disk encryption. Only EDR provides the necessary detection and automated response capabilities to handle modern file-less and polymorphic malware threats effectively. This aligns with the Cisco SAFE goal of securing the endpoint layer against advanced persistent threats (APTs) and ransomware variants.

========

Question 5

Question Type: MultipleChoice

A manufacturing company recently experienced a network-down scenario due to malware spread on the management network. The company wants to implement a solution to detect and mitigate a similar threat in the future and protect the overall network. Which solution meets the requirements?

Options:

A- endpoint detection and response
B- RADIUS
C- encrypted threat analysis
D- IPsec VPN

Answer:

A

Explanation:

The spread of malware across a sensitive segment like the management network highlights a failure in host-level security and internal visibility. To detect and mitigate the spread of such threats and protect the overall network, Endpoint Detection and Response (EDR) is the most effective choice among the options. In the Cisco security ecosystem, the endpoint is often the last line of defense and the most critical source of telemetry for malware incidents.

By deploying an EDR solution like Cisco Secure Endpoint, the manufacturing company gains the ability to identify the 'patient zero' of the infection. EDR uses advanced features like Device Traversal and Lateral Movement detection to see how malware moves from one machine to another over the management network. Once detected, the security team can use the EDR platform to initiate a 'host isolation' command, effectively cutting off the infected device's communication with the rest of the network without physically unplugging it. While Encrypted Threat Analytics (ETA) (Option C) is a powerful network-based feature for detecting malware in

encrypted traffic without decryption, EDR provides the most granular control and response capabilities specifically for malware residing on and spreading between hosts. RADIUS (Option B) and IPsec VPNs (Option D) focus on access control and encryption of data in transit, respectively, but do not provide the behavioral analysis needed to stop a running malware outbreak once the network has already been accessed.

Question 6

Question Type: MultipleChoice

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?

Options:

A- traditional firewall
B- zone-based firewall
C- distributed firewall
D- host-based firewall

Answer:

C

Explanation:

In a multi-cloud architecture, traditional perimeter-based firewalls often create 'chokepoints' and fail to provide the granularity needed for east-west traffic between microservices across different providers. A distributed firewall is the architectural solution designed to meet these modern requirements. Unlike a centralized appliance, a distributed firewall is implemented as a software-defined layer that resides close to the workloads---often within the hypervisor or as part of a service mesh.

According to Cisco Security Infrastructure objectives, a distributed firewall allows for centralized management of a unified policy that is pushed out to all enforcement points,

regardless of whether the workload is in AWS, Azure, or an on-premises data center. This ensures consistent security policies across the entire footprint. Because the enforcement is decentralized, the solution scales automatically as new cloud platforms or workloads are added. While a Traditional Firewall (Option A) lacks the multi-cloud agility, a Zone-based Firewall (Option B) is typically tied to specific physical or logical interfaces on a router, and a Host-based Firewall (Option D) is managed at the individual OS level, which becomes difficult to coordinate centrally at scale. The distributed firewall model aligns with the Cisco SAFE architectural goal of pervasive security and simplified operations in highly dynamic, heterogeneous cloud environments.

========

Question 7

Question Type: MultipleChoice

How is generative AI used in securing networks?

Options:

A- to provide real-time load balancing
B- to improve resource consumption
C- to perform real-time audits to ensure regulatory compliance
D- to detect unusual patterns in network traffic

Answer:

D

Explanation:

The Cisco SDSI v1.0 blueprint highlights the transformative role of AI and Machine Learning in modern security operations. Generative AI and advanced behavioral analytics are primarily used to enhance Threat Detection by identifying 'unknown unknowns.' While traditional systems rely on static signatures, GenAI can analyze vast amounts of telemetry data to build a baseline of 'normal' behavior and then detect unusual patterns that signify a zero-day attack, data exfiltration, or lateral movement.

Generative AI models can synthesize complex log data and network flows to recognize subtle deviations that a human analyst might miss. For example, if a user account suddenly accesses an unusual set of servers at an odd hour, the AI can correlate this with other minor anomalies to flag a potential compromise. While AI can assist in compliance (Option C) by summarizing reports, its primary architectural value in securing the network lies in its predictive and

detective capabilities. Options A and B relate more to general network optimization and traffic engineering rather than the core security function of threat mitigation. By integrating AI-driven anomaly detection, organizations move toward a proactive security model, reducing the 'mean time to detect' (MTTD) and allowing automated systems to trigger defensive responses before a threat can escalate.

Question 8

Question Type: MultipleChoice

A manufacturing company experienced a security breach that resulted in sales data being compromised. An engineer participating in the investigation must identify who logged into the sales system during the affected period. Which approach must be used to gather the information?

Options:

A- SNMP
B- NACM
C- AAA
D- PKI

Answer:

C

Explanation:

In the aftermath of a security breach, forensic investigators rely on the Accounting portion of AAA (Authentication, Authorization, and Accounting) to reconstruct a timeline of events. While Authentication verifies identity and Authorization defines permissions, Accounting is the specific framework used to track user activity, including login/logout times and the specific commands executed during a session.

According to Cisco Security Infrastructure design objectives, implementing a centralized AAA solution (such as Cisco Identity Services Engine (ISE) or a TACACS+/RADIUS server) is critical for accountability. In this scenario, the engineer would query the AAA logs to identify exactly 'who' accessed the sales system during the compromise period. SNMP (Option A) is primarily for network monitoring and performance data, not granular user access logs. NACM (Option B) is an access control model for NETCONF but doesn't provide the broad auditing required here. PKI (Option D) provides the certificates used for digital signatures and encryption but does not log the historical 'session' data needed for the investigation. Therefore, AAA is the fundamental architectural requirement for ensuring non-repudiation and providing the audit trail necessary

to satisfy risk management and incident response requirements.

========