Cisco

300-745 Exam

Designing Cisco Security Infrastructure

Questions & Answers
Demo

Version: 4.0

Question: 1

A restaurant distribution center recently suffered a password spray attack targeting the Cisco Secure Firepower Threat Defense VPN headend. The attack attempts to gain unauthorized access by trying common passwords across many accounts. The attack poses a significant security threat to the organization's remote access infrastructure. To enhance the security of the VPN setup and minimize the risk of similar attacks in the future, the IT security team must implement effective mitigation measures. Which technique effectively reduces the risk of this type of attack?

A. Implement an access list to block addresses from the previous password spray attack.

B. Disable group aliases in the connection profiles.

C. Change the AAA authentication method from RADIUS to TACACS+.

D. Enable AAA authentication for the DefaultWEBVPN and DefaultRAGroup Connection Profiles.

Answer: D

Explanation:

In the context of Designing Cisco Security Infrastructure, protecting Remote Access VPN (RAVPN) against brute-force and password spray attacks is a critical objective. On Cisco Firepower Threat Defense (FTD) and Adaptive Security Appliance (ASA) platforms, the DefaultWEBVPNGroup and

DefaultRAGroup are the landing points for any connection request that does not specify a valid Group Alias or Group URL. Attackers frequently target these default profiles because they are often left with "None" as the authentication method, allowing the attacker to probe for valid usernames without immediate rejection.

By selecting Option D, the security designer ensures that any attempt to access the VPN via these default profiles requires valid AAA credentials. According to Cisco's hardened design guides, it is best practice to point these default profiles to a "sinkhole" AAA server or a local database with no users. This forces the password spray attack to fail at the initial authentication phase before any sensitive information is leaked or unauthorized access is granted. While Option A (ACLs) provides a temporary fix, it is ineffective against distributed attacks using rotating IP addresses. Option B (Disabling aliases) is a good obfuscation technique but doesn't stop an attacker from hitting the default profile. Option D provides a structural mitigation that aligns with the Cisco SAFE architectural principle of reducing the attack surface by securing every possible entry vector into the private infrastructure.

Question: 2

A product manager is focused on maintaining the security integrity of a microservice-based application as new features are developed and integrated. To ensure that known software vulnerabilities are not introduced into the product, it is crucial to implement a robust application security technique. The technique must be applied during the build phase of the software development lifecycle, which allows the team to proactively identify and address vulnerability risks before deployment. Which application security technique must be applied to accomplish the goal?

A. secret detection

B. container scanning

C. infrastructure as code scanning

D. Open API specification analysis

Answer: B

Explanation:

In a microservices-based architecture, applications are typically packaged into containers to ensure

consistency across different environments. According to the Designing Cisco Security Infrastructure (SDSI) objectives, securing the software development lifecycle (SDLC) requires integrating security checks as far "left" as possible. Container scanning is the specific technique used during the build phase to inspect container images for known software vulnerabilities (CVEs) within the bundled libraries, binaries, and dependencies.

When a developer initiates a build, the container scanning tool cross-references the layers of the image against vulnerability databases. If a high-risk vulnerability is detected in a base image or a third-party library, the build can be automatically failed, preventing the vulnerable code from ever reaching the registry or production environment. This directly addresses the product manager's goal of ensuring known vulnerabilities are not introduced. While Secret Detection (Option A) is vital for finding leaked API keys or passwords, and Infrastructure as Code (IaC) scanning (Option C) ensures the environment configuration is secure, neither specifically targets the software vulnerabilities within the application package itself. Similarly, Open API specification analysis (Option D) focuses on the contract and security of the interface rather than the underlying software vulnerabilities. By implementing container scanning, organizations align with Cisco's DevSecOps framework, which emphasizes automated, policy-driven security within the CI/CD pipeline to maintain the integrity of cloud-native applications.

Question: 3

A financial company is in the process of upgrading network access across the entire company. The solution must ensure: least privilege access control access across different network segments and increased security for employees. Which solution approach must the company take?

A. NetFlow

B. SNMP

C. PKI

D. RBAC

Answer: D

Explanation:

In the architecture of a modern secure infrastructure, achieving least privilege is a foundational requirement, especially for a financial institution where data sensitivity is high. Role-Based Access Control (RBAC) is the specific methodology used to restrict network access based on the roles of individual users within an enterprise. By implementing RBAC, the security team can ensure that employees only have access to the specific network segments and resources necessary for their job functions, effectively minimizing the internal attack surface.

Within the Cisco Security ecosystem, RBAC is often operationalized through tools like Cisco Identity Services Engine (ISE) using Scalable Group Tags (SGTs). Instead of relying on static IP addresses or complex Access Control Lists (ACLs) that are difficult to maintain across different segments, RBAC allows for dynamic policy enforcement. For example, a "Financial Auditor" role would automatically be granted access to the accounting segment but blocked from the development segment, regardless of where they plug into the network. While PKI (Option C) provides strong authentication and encryption, and NetFlow (Option A) provides visibility, neither inherently defines the "least privilege" permission structure. RBAC is the architectural approach that directly maps business requirements to technical access policies, ensuring that security is maintained across segmented environments as required by the Cisco SDSI objectives for secure infrastructure design.

========

Question: 4

A security engineer on an application design team must choose a framework of attack patterns to evaluate during threat modeling. Which framework provides the common set of attacks?

A. Cisco SAFE

B. GDPR

C. MITRE CAPEC

D. SOC2

Answer: C

Explanation:

In the "Risk, Events, and Requirements" domain of the Cisco SDSI curriculum, understanding how to systematically identify and mitigate threats is essential. MITRE CAPEC (Common Attack Pattern Enumeration and Classification) is a comprehensive dictionary and classification scheme for known attack patterns used by adversaries. It is specifically designed to help security engineers, developers, and designers understand how an attacker might exploit a system. By using CAPEC during the threat modeling phase, an engineer can look at specific "attack patterns"—such as SQL injection, Cross-Site Scripting (XSS), or Man-in-the-Middle—to see if the application's architecture is resilient against them.

Unlike Cisco SAFE (Option A), which is an architectural guide providing best practices for designing secure networks, or GDPR (Option B) and SOC2 (Option D), which are regulatory and compliance frameworks focused on privacy and operational auditing, CAPEC is purely technical and focused on the "how" of an attack. It provides the granular data necessary to simulate attacks and build robust defenses into the application design. Integrating CAPEC into the development lifecycle allows teams to move beyond broad risks and address the specific methods attackers use to bypass security controls. This alignment with the MITRE knowledge base ensures that the security infrastructure is designed with a realistic understanding of modern adversarial tactics, which is a core objective for Cisco security professionals.

Question: 5

A manufacturing company implemented IoT devices throughout their smart factory and needs a security solution that meets these requirements:

Protect IoT devices from network-based attacks.

Visibility into communication patterns.

Anomaly detection for IoT traffic.

Which firewall technology or feature should be recommended?

A. zone-based firewall

B. transparent firewall

C. traditional firewall

D. IPS/IDS

Answer: D

Explanation:

In a smart factory environment, IoT devices often use specialized industrial protocols (like Modbus, PROFINET, or EtherNet/IP) and have limited built-in security. To meet the requirements of protecting these devices from network-based attacks while gaining visibility into communication patterns and detecting anomalies, an IPS/IDS (Intrusion Prevention/Detection System) is the most effective solution.

Modern Cisco Secure Firewall (NGFW) systems integrate advanced IPS/IDS capabilities that go beyond simple port-based filtering. They provide deep packet inspection (DPI) to identify specific IoT protocols and baseline "normal" behavior. When an IoT device suddenly begins communicating with an unknown external IP or attempts to use a command it has never used before, the IPS/IDS can trigger an alert or block the traffic as an anomaly.

While a Zone-Based Firewall (Option A) or a Traditional Firewall (Option C) can segment traffic and control access between zones, they generally lack the granular visibility and behavior-based anomaly detection required for IoT security. A Transparent Firewall (Option B) is a deployment mode that makes the firewall "invisible" at Layer 2, which is useful for insertion into existing networks but does not inherently provide the required anomaly detection. Therefore, IPS/IDS is the primary technology within the Cisco Security Infrastructure that addresses the need for signature-based protection combined with behavioral visibility for specialized IoT traffic.