DUMPSBOSS.

Implementing and Operating Cisco Security Core Technologies (SCOR 350-701)

Cisco 350-701

Version Demo

Total Demo Questions: 78

Total Premium Questions: 782

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Concepts	79
Topic 2, Network Security	153
Topic 3, Securing the Cloud	82
Topic 4, Content Security	127
Topic 5, Endpoint Protection and Detection	80
Topic 6, Secure Network Access, Visibility, and Enforcement	257
Topic 7, Mix Questions	4
Total	782

QUESTION NO: 1

What are two functions of TAXII in threat intelligence sharing? (Choose two.)

A. determines the "what" of threat intelligence

B. Supports STIX information

C. allows users to describe threat motivations and abilities

D. exchanges trusted anomaly intelligence information

E. determines how threat intelligence information is relayed

ANSWER: B E

Explanation:

TAXII (Trusted Automated eXchange of Indicator Information) is the transport mechanism used to move cyber threat intelligence between systems and organizations. In practice, it defines the services and message exchanges used to request, push, and pull threat intelligence over HTTPS, enabling automated sharing at scale. A core function of TAXII is that it supports STIX information by providing a standardized way to exchange STIX-formatted content (for example, indicators, malware, threat actor, and campaign objects) between a TAXII client and TAXII server. Another core function is that it determines how threat intelligence information is relayed, meaning it specifies the transport and API model (collections, channels/endpoints, and request/response patterns) used to distribute the intelligence. This separation of concerns is fundamental: STIX focuses on the structure and semantics of the intelligence itself, while TAXII focuses on how that intelligence is communicated and accessed. Together, they enable interoperable threat-intel sharing across vendors and platforms without custom integrations.

References: OASIS CTI TAXII Introduction, OASIS CTI STIX Introduction

QUESTION NO: 2

What are two DDoS attack categories? (Choose two.)

A. protocol

B. source-based

C. database

D. sequential

E. volume-based

ANSWER: A E

Explanation:

DDoS attacks are commonly categorized by what resource they aim to exhaust and where in the network stack they operate. One major category is *volume-based* attacks, which attempt to saturate bandwidth with massive traffic rates (often measured in bps). Typical examples include UDP floods and amplification/reflection attacks (such as DNS or NTP amplification), where the goal is to overwhelm upstream links and edge capacity rather than a specific application.

Another widely used category is *protocol* attacks (often called state-exhaustion attacks). These target weaknesses or resource limits in Layer 3/4 protocols and network devices by consuming connection/state tables or control-plane resources. Examples include SYN floods (exhausting TCP connection state) and other floods that stress firewalls, load balancers, or routers by forcing them to track large numbers of half-open or malformed sessions.

These two categories are standard in Cisco-aligned security discussions and also align with industry taxonomy that separates bandwidth saturation from protocol/state exhaustion. For additional background, see Cloudflare's overview of DDoS categories and Cisco's DDoS protection resources: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ and https://www.cisco.com/c/en/us/products/security/ddos-protection/index.html.

QUESTION NO: 3

Which two kinds of attacks are prevented by multifactor authentication? (Choose two.)

A. phishing

B. brute force

C. man-in-the-middle

D. DDOS

E. tear drop

ANSWER: A B

Explanation:

Multifactor authentication is designed to reduce the risk of account compromise when a password is guessed, reused, or otherwise obtained. It is particularly effective against *brute force* attacks because even if an attacker successfully guesses or cracks the password, they still cannot authenticate without the additional factor (for example, a one-time code, push approval, or hardware token). This directly breaks the "single secret" failure mode that brute-force and password-spraying attacks rely on.

Multifactor authentication also helps prevent many *phishing*-driven compromises. In common phishing scenarios, the attacker's goal is to steal a user's password and then log in as that user. MFA adds a second requirement that the attacker typically cannot satisfy, so stolen credentials alone are insufficient. While advanced real-time phishing can sometimes proxy MFA, MFA still materially mitigates standard credential-harvesting phishing and is widely recommended as a primary control to reduce phishing impact.

These protections align with industry guidance that MFA mitigates password-based attacks and reduces the success of credential theft. See CISA: Implementing Phishing-Resistant MFA and MITRE ATT&CK Mitigation M1032 (Multi-factor Authentication).

QUESTION NO: 4

When a next-generation endpoint security solution is selected for a company, what are two key

deliverables that help justify the implementation? (Choose two.)

A. signature-based endpoint protection on company endpoints

B. macro-based protection to keep connected endpoints safe

C. continuous monitoring of all files that are located on connected endpoints

D. email integration to protect endpoints from malicious content that is located in email

E. real-time feeds from global threat intelligence centers

ANSWER: C E

Explanation:

Next-generation endpoint security is typically justified by capabilities that materially improve detection and response beyond traditional antivirus. A core deliverable is **continuous monitoring of all files that are located on connected endpoints**, which aligns with modern EPP/EDR behavior: ongoing visibility into endpoint activity, file/process telemetry, and continuous assessment rather than periodic or purely on-access scanning. This continuous monitoring supports faster detection, investigation, and containment, and it provides the operational evidence (telemetry, timelines, and indicators) needed to demonstrate risk reduction and improved incident response outcomes.

Another key deliverable is **real-time feeds from global threat intelligence centers**. Modern endpoint platforms commonly integrate cloud-delivered threat intelligence to rapidly identify emerging threats, enrich detections with reputation/IOC context, and improve prevention and detection efficacy without waiting for local signature updates. This helps justify implementation by showing improved protection against new and evolving malware and by reducing mean time to detect/respond through better context and automated correlation.

These deliverables map directly to widely documented EDR/EPP expectations: continuous endpoint telemetry/monitoring and cloud-based threat intelligence to keep protections current against fast-changing adversary techniques.

References: Cisco Secure Endpoint (AMP for Endpoints) overview, Cisco Talos threat intelligence

QUESTION NO: 5

In which two ways does a system administrator send web traffic transparently to the Cisco WSA? (Choose two.)

A. use Web Cache Communication Protocol

B. configure AD Group Policies to push proxy settings

C. configure the proxy IP address in the web-browser settings

D. configure policy-based routing on the network infrastructure

E. reference a Proxy Auto Config file

ANSWER: A D

Explanation:

Transparent redirection to Cisco Web Security Appliance means users do not have to explicitly configure a proxy in their browser; instead, the network steers HTTP/HTTPS flows to the WSA. Two common approaches are Web Cache Communication Protocol and policy-based routing. Web Cache Communication Protocol allows a router/switch to intercept web requests and redirect them to the WSA (and optionally receive “return” information), enabling proxy services without endpoint configuration. Policy-based routing achieves a similar outcome by matching web traffic (for example, TCP/80 and TCP/443) and forcing the next hop toward the WSA, which is a standard way to implement transparent proxying when WCCP is not used or not supported on a given platform. Both methods are implemented on network infrastructure and are designed specifically to redirect traffic transparently, rather than relying on user/browser proxy settings or PAC files (which are explicit proxy discovery/configuration mechanisms). See Cisco WSA deployment guidance and WCCP/PBR redirection concepts in Cisco documentation: Cisco Web Security Appliance configuration guides and Cisco WCCP support documentation.

QUESTION NO: 6

An organization wants to secure users, data, and applications in the cloud. The solution must be API-based on operate as a cloud-native CASB. Which solution must be used for this implementation?

A. Cisco Cloud Email Security

B. Cisco Cloudlock

C. Cisco Umbrella

D. Cisco Firepower Nest-Generation Firewall

ANSWER: B

Explanation:

Cisco Cloudlock is the correct choice because it is Cisco’s cloud-native, API-based Cloud Access Security Broker (CASB). Cloudlock connects to SaaS platforms (for example, Microsoft 365, Google Workspace, Salesforce, Box, and others) using vendor APIs rather than inline proxying. This API-based approach allows it to continuously monitor cloud application activity, assess risk, and enforce security controls directly within the SaaS environment. Typical CASB capabilities delivered by Cloudlock include discovery and governance of cloud apps, user and entity behavior analytics, data loss prevention for sensitive data stored in SaaS, and automated remediation workflows (for example, quarantining content, revoking sharing links, or disabling risky third-party OAuth applications). These functions align precisely with the requirement to secure users, data, and applications in the cloud using an API-based, cloud-native CASB model. Cisco positions Cloudlock specifically for SaaS security posture, compliance, and threat protection via API integrations, which is distinct from DNS-layer security or network firewalls.

References: Cisco Cloudlock (product overview), Cisco CASB overview

QUESTION NO: 7

Why is it important to have logical security controls on endpoints even though the users are trained to spot security threats and the network devices already help prevent them?

A. because defense-in-depth stops at the network

B. because human error or insider threats will still exist

C. to prevent theft of the endpoints

D. to expose the endpoint to more threats

ANSWER: B

Explanation:

because human error or insider threats will still exist is correct because endpoint security is a necessary layer in a defense-in-depth strategy, not something that can be replaced by training or network controls alone. Even well-trained users make mistakes (clicking a convincing phishing link, approving an MFA prompt, misconfiguring software, or reusing passwords), and those mistakes can directly execute on the endpoint where malware, credential theft, and lateral movement begin. In addition, insider threats—malicious or negligent—operate from legitimate access and can bypass many perimeter-focused protections. Endpoint logical controls (EDR/AV, host firewall, application control, disk encryption, least privilege, patching, and continuous monitoring) reduce the blast radius when something slips past training and network defenses, and they provide visibility and response capabilities at the point of execution. Cisco's security guidance emphasizes layered controls and endpoint detection/response as part of an overall architecture because threats can originate from email, web, removable media, or already-compromised internal hosts, all of which ultimately impact endpoints. See Cisco Secure Endpoint overview and Cisco defense-in-depth.

QUESTION NO: 8

What is a functional difference between a Cisco ASA and Cisco IOS router with Zone-Based Policy Firewall?

A. The Cisco ASA can be configured for high availability, whereas the Cisco IOS router with Zone-Based Policy Firewall cannot.

B. The Cisco IOS router with Zone-Based Policy Firewall can be configured for high availability, whereas the Cisco ASA cannot.

C. The Cisco ASA denies all traffic by default, whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces.

D. The Cisco IOS router with Zone-Based Policy Firewall denies all traffic by default, whereas Cisco ASA starts out by allowing traffic until rules are added.

ANSWER: C

Explanation:

The Cisco ASA denies all traffic by default, whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces. This reflects the different default security postures of the two platforms. ASA is a stateful firewall appliance with a "default deny" stance between interfaces of the same security level (and it also blocks lower-to-higher by default), requiring explicit policy (ACLs, inspection policies, NAT rules, etc.) to permit flows. In contrast, Cisco IOS Zone-Based Policy Firewall (ZBFW) is a feature added to a router; until you define zones and apply a zone-pair policy, the router behaves like a normal router and forwards traffic based on routing and any existing interface ACLs. Once interfaces are assigned to zones, IOS will not allow inter-zone traffic unless a zone-pair with a policy is configured, but that is a configured state—not the out-of-the-box behavior. This "router forwards by default unless you configure firewall policy" versus "firewall blocks by default unless you permit" is a key functional difference often tested in SCOR.

References: Cisco ASA security levels and default behavior, Cisco IOS Zone-Based Policy Firewall design guide

QUESTION NO: 9

Which two products are used to forecast capacity needs accurately in real time? (Choose two.)

A. Cisco Secure Workload

B. Cisco Umbrella

C. Cisco Workload Optimization Manager

D. Cisco AppDynamics

ANSWER: C D

Explanation:

Cisco Workload Optimization Manager is designed specifically for real-time resource optimization and capacity planning across on-prem and cloud environments. It continuously analyzes supply and demand for compute, storage, and network resources and can project future capacity requirements based on observed utilization and application needs, which aligns directly with “forecast capacity needs accurately in real time.” Cisco AppDynamics complements this by providing real-time application performance monitoring and business transaction visibility, which helps correlate application demand with underlying infrastructure consumption. That end-to-end insight supports more accurate capacity forecasting because you can see how application behavior drives resource usage and predict when scaling will be required to maintain performance and SLOs.

Together, these tools provide both infrastructure-level optimization/forecasting (Workload Optimization Manager) and application-driven demand visibility (AppDynamics), enabling accurate, real-time capacity planning decisions. This pairing is commonly positioned in Cisco’s full-stack observability and optimization story for ensuring performance while right-sizing resources.

References: Cisco Workload Optimization Manager, Cisco AppDynamics

QUESTION NO: 10

Which two protocols must be configured to authenticate end users to the Cisco WSA? (Choose two.)

B. CHAP

C. NTLMSSP

D. RADIUS

E. Kerberos

ANSWER: C E

Explanation:

Cisco Web Security Appliance (WSA) end-user authentication is commonly implemented using integrated authentication methods that allow the appliance to identify users transparently in enterprise environments. Two key protocols used for this

purpose are NTLMSSP and Kerberos. NTLMSSP (NT LAN Manager Security Support Provider) enables WSA to perform Windows Integrated Authentication, typically via explicit proxy settings (or with appropriate network design), allowing domain users to be authenticated without repeatedly prompting for credentials. Kerberos provides a stronger, ticket-based integrated authentication mechanism with mutual authentication and avoids sending reusable password material across the network; it is widely used in Active Directory environments and is supported by WSA for authenticating users when properly joined/configured with the domain and service principal requirements. In practice, organizations choose between NTLMSSP and Kerberos depending on client support, domain configuration, and security requirements, and both are standard, documented approaches for WSA end-user authentication workflows. These protocols align with Cisco's guidance for acquiring end-user credentials and integrating WSA with enterprise identity infrastructure for user/group-based policy enforcement.

References: Cisco Web Security Appliance - User Guides, Cisco WSA Technical Documentation

QUESTION NO: 11

Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?

A. RADIUS-based REAP

B. fingerprinting

C. Dynamic ARP Inspection

D. multifactor authentication

ANSWER: D

Explanation:

Multifactor authentication is the best technology to help prevent attackers from successfully stealing and reusing usernames and passwords. Even if an attacker captures a user's credentials through phishing, keylogging, password spraying, or a database leak, multifactor authentication adds an additional, independent verification factor (something the user has, is, or does) that the attacker typically cannot replicate. This significantly reduces the likelihood that stolen passwords alone can be used to authenticate to corporate applications, VPNs, cloud services, or administrative portals. In Cisco security architectures, multifactor authentication is commonly integrated with AAA and identity services (for example, via RADIUS/TACACS+ with an MFA provider, or SAML/OIDC for web applications), providing a practical control against credential compromise and account takeover. While it does not stop the act of credential capture itself in every case, it is a primary compensating control that prevents stolen usernames and passwords from being sufficient for access, which is the core security objective implied by the question.

References: https://www.cisa.gov/resources-tools/resources/multi-factor-authentication-mfa, https://www.nist.gov/itl/tig/projects/special-publication-800-63

QUESTION NO: 12

Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two.)

A. Patch for cross-site scripting.

B. Perform backups to the private cloud.

C. Protect against input validation and character escapes in the endpoint.

D. Install a spam and virus email filter.

E. Protect systems with an up-to-date antimalware program.

ANSWER: D E

Explanation:

Installing a spam and virus email filter helps reduce exposure to phishing by detecting and blocking malicious messages, suspicious links, and dangerous attachments before they reach the user's inbox. Since many social engineering campaigns are delivered via email, improving email hygiene at the endpoint (or via integrated endpoint email security controls) directly lowers the likelihood that a user will interact with a phishing lure. In addition, protecting systems with an up-to-date antimalware program is a key endpoint control because phishing often aims to deliver malware (for example, droppers, ransomware, or credential stealers). Modern antimalware/endpoint protection platforms use signatures plus behavioral and reputation-based detection to stop malicious payloads even when a user clicks a link or opens an attachment. Keeping antimalware current is critical because attackers frequently change indicators and techniques, and updated engines/content improve detection and prevention. Together, these two measures reduce both the probability of successful delivery and the impact of user interaction, which is why they are commonly recommended baseline controls for phishing and social engineering risk reduction.

References: Cisco Secure Email, Cisco Secure Endpoint

QUESTION NO: 13

What are two characteristics of the RESTful architecture used within Cisco DNA Center? (Choose two.)

A. REST uses methods such as GET, PUT, POST, and DELETE.

B. REST codes can be compiled with any programming language.

C. REST is a Linux platform-based architecture.

D. The POST action replaces existing data at the URL path.

E. REST uses HTTP to send a request to a web service.

ANSWER: A E

Explanation:

Cisco DNA Center exposes capabilities through RESTful APIs, which follow standard web-service conventions. A key characteristic is that REST relies on standard HTTP methods to operate on resources; common methods include GET for retrieval, POST for creation/triggering actions, PUT for full updates, and DELETE for removal. Another core characteristic is that REST uses HTTP (typically HTTPS in production) as the transport protocol to send requests to the API endpoints and receive responses, commonly encoded as JSON. These traits are fundamental to REST and are exactly how Cisco DNA Center's Intent APIs are consumed by external clients and automation tools: clients authenticate, then issue HTTP requests using these verbs against specific resource URLs (endpoints) to read or change controller-managed network state. This consistent use of HTTP and its verbs is what enables broad interoperability with many tools and languages, and it aligns with Cisco's published DNA Center API usage patterns and DevNet guidance.

References: Cisco DNA Center APIs (Cisco DevNet), Cisco DNA Center User Guides

QUESTION NO: 14

How does Cisco Umbrella protect clients when they operate outside of the corporate network?

A. by modifying the registry for DNS lookups

B. by using Active Directory group policies to enforce Cisco Umbrella DNS servers

C. by using the Cisco Umbrella roaming client

D. by forcing DNS queries to the corporate name servers

ANSWER: C

Explanation:

Cisco Umbrella protects users off the corporate network by using the Cisco Umbrella roaming client. The roaming client (and the newer Umbrella Roaming Security module within Cisco Secure Client) ensures that DNS requests from endpoints are sent to Umbrella's resolvers even when the device is on untrusted networks like home Wi-Fi, hotels, or public hotspots. This maintains consistent policy enforcement (blocking malicious domains, phishing, and command-and-control lookups) regardless of where the endpoint is located. In practice, the roaming client runs on the endpoint and intercepts/redirects DNS traffic so that Umbrella can apply the organization's security policies and provide visibility into DNS activity outside the perimeter. This is the key mechanism Umbrella uses for "roaming" protection, as opposed to relying on on-premises network controls that only apply when a device is connected to the corporate LAN/VPN. Umbrella's documentation describes the roaming client/roaming module as the method to extend Umbrella protection beyond the corporate network by enforcing DNS-layer security from the endpoint itself.

References: Cisco Umbrella User Guide – Roaming Clients, Cisco Umbrella User Guide – Cisco Secure Client (Umbrella module)

QUESTION NO: 15

Which VPN technology can support a multivendor environment and secure traffic between sites?

A. SSL VPN

B. GET VPN

C. FlexVPN

D. DMVPN

ANSWER: B

Explanation:

GET VPN is the correct choice because it is designed for site-to-site encryption in a way that scales well and interoperates across different vendors using standards-based IPsec. GET VPN (Group Encrypted Transport VPN) uses a group keying model (via a key server) so that multiple sites can share common security policies and keys while encrypting traffic end-to-end across a private WAN or MPLS network. A key advantage is that it preserves the original IP header (no tunnel encapsulation), which helps maintain routing visibility and supports services that rely on the original addressing while still providing confidentiality and integrity between sites. Because it is built on standard IPsec mechanisms and group key

management concepts, it can be deployed in environments where not every device is the same vendor, making it a strong fit for multivendor site-to-site protection. Cisco positions GET VPN specifically for securing traffic between sites over a service-provider core while keeping the network “tunnel-less” and scalable for many branches. See Cisco’s GET VPN overview and configuration guidance for details on its group IPsec model and use cases: Cisco GET VPN support page and Cisco IOS XE GET VPN Configuration Guide.

QUESTION NO: 16

Under which two circumstances is a CoA issued? (Choose two.)

A. A new authentication rule was added to the policy on the Policy Service node.

B. An endpoint is deleted on the Identity Service Engine server.

C. A new Identity Source Sequence is created and referenced in the authentication policy.

D. An endpoint is profiled for the first time.

E. A new Identity Service Engine server is added to the deployment with the Administration persona.

ANSWER: B D

Explanation:

In Cisco ISE, a Change of Authorization (CoA) is used to force an active session to be reauthorized so that new policy results can be applied without waiting for the session to naturally end. CoA is commonly triggered by endpoint-related events that change the authorization outcome for an already-authenticated device. When an endpoint is profiled for the first time, ISE can determine a new endpoint identity (for example, printer, IP phone, workstation) and then issue a CoA so the network access device re-runs authorization and applies the correct authorization profile (such as VLAN, dACL, or SGT). Similarly, when an endpoint is deleted on the Identity Service Engine server, the endpoint’s stored identity/attributes are removed, which can change how the endpoint should be authorized; issuing a CoA allows the session to be re-evaluated immediately against current policy and identity data. These are classic “session-impacting” identity changes where CoA provides near real-time enforcement of updated authorization decisions. For background on CoA and how ISE uses RADIUS Change of Authorization for dynamic reauthorization, see Cisco ISE Change of Authorization (CoA) overview and Cisco ISE Admin Guide (RADIUS CoA / reauthentication).

QUESTION NO: 17

Which factor must be considered when choosing the on-premise solution over the cloud-based one?

A. With an on-premise solution, the provider is responsible for the installation and maintenance of the product, whereas with a cloud-based solution, the customer is responsible for it

B. With a cloud-based solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.

C. With an on-premise solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.

D. With an on-premise solution, the customer is responsible for the installation and maintenance of theproduct, whereas with a cloud-based solution, the provider is responsible for it.

ANSWER: D

Explanation:

The key factor to consider is the operational responsibility split between customer and provider. With an on-premise solution, the organization typically owns the full lifecycle: it must deploy the hardware/software, integrate it into the environment, patch and upgrade it, monitor health and capacity, and handle break/fix and backups. In contrast, with a cloud-based (SaaS) solution, the provider generally operates the underlying infrastructure and the application platform, including installation, scaling, and ongoing maintenance/patching, while the customer focuses more on configuration, user/access administration, and using the service. This responsibility model directly impacts staffing, skills, change windows, risk tolerance, and total cost of ownership—on-prem often requires more internal operational overhead but can offer greater control and customization, whereas cloud reduces day-to-day maintenance burden. Cisco commonly frames this as a shared responsibility model where cloud providers manage the service operation and customers manage their data, identities, and configurations. See Cisco's cloud security/shared responsibility discussions and general SaaS responsibility guidance: https://www.cisco.com/c/en/us/solutions/security/what-is-cloud-security.html and https://www.cisco.com/c/en/us/solutions/cloud/what-is-saas.html.

QUESTION NO: 18

Which two descriptions of AES encryption are true? (Choose two.)

A. AES is less secure than 3DES.

B. AES is more secure than 3DES.

C. AES can use a 168-bit key for encryption.

D. AES can use a 256-bit key for encryption.

E. AES encrypts and decrypts a key three times in sequence.

ANSWER: B D

Explanation:

AES is a symmetric block cipher standardized by NIST (FIPS 197) and is widely used in modern VPNs and IPsec deployments. It is generally considered more secure than 3DES because it supports larger key sizes, has a more modern design, and avoids the practical limitations and deprecation concerns surrounding 3DES (including its effective security reduction and industry guidance to move away from it). AES supports three standardized key lengths—128, 192, and 256 bits—so the statement that it can use a 256-bit key for encryption is accurate. In Cisco security technologies (including IPsec/IKE), AES-256 is a common strong cipher choice when policy allows, balancing strong security with good performance on hardware that supports AES acceleration. These properties are why AES has become the preferred replacement for older ciphers like 3DES in most security baselines and compliance frameworks. For the authoritative standard and key-size details, see NIST FIPS 197. For current guidance on transitioning away from older algorithms like 3DES, see NIST recommendations on acceptable algorithms and key lengths.

References: https://csrc.nist.gov/publications/detail/fips/197/final, https://csrc.nist.gov/projects/key-management/key-length-recommendations

QUESTION NO: 19

Which two types of connectors are used to generate telemetry data from IPFIX records in a Cisco Secure Workload implementation? (Choose two.)

A. ADC

B. ERSPAN

C. Cisco ASA

D. NetFlow

E. Cisco Secure Workload

ANSWER: D E

Explanation:

Telemetry derived from IPFIX records in Cisco Secure Workload is collected through flow-export mechanisms and then ingested by Secure Workload for analysis. NetFlow is the commonly referenced Cisco flow technology that aligns with IPFIX (IPFIX is the IETF standard, and NetFlow v9 is the basis for IPFIX), so a NetFlow-type connector is used to receive and interpret exported flow records from network devices. Cisco Secure Workload also provides its own connector/ingestion capability to consume these flow records and convert them into the application dependency and policy-relevant telemetry used for visibility and segmentation analytics. In practice, Secure Workload can ingest IPFIX/NetFlow data streams and correlate them with workloads, labels, and policy constructs to build communication maps and support enforcement planning. This is why the correct connector types are the ones explicitly tied to flow telemetry ingestion and Secure Workload's processing pipeline rather than packet-mirroring or unrelated device types.

References: https://www.ietf.org/rfc/rfc7011.html, https://www.cisco.com/c/en/us/products/security/secure-workload/index.html

QUESTION NO: 20

What is a difference between GETVPN and IPsec?

A. GETVPN is used to build a VPN network with multiple sites without having to statically configure all devices.

B. GETVPN is based on IKEv2 and does not support IKEv1.

C. GETVPN provides key management and security association management.

D. GETVPN reduces latency and provides encryption over MPLS without the use of a central hub.

ANSWER: D

Explanation:

GETVPN (Group Encrypted Transport VPN) is designed for encrypting traffic in a private WAN—commonly MPLS—while preserving the original IP header, which allows the provider core to continue using routing/QoS features based on the customer's addressing. A key architectural difference is that GETVPN enables any-to-any encryption among multiple sites without requiring a hub-and-spoke topology for data traffic. Instead, a key server distributes group security associations and keys so that spokes can encrypt/decrypt directly with each other, avoiding the "trombone" effect through a central hub. This typically reduces latency and improves bandwidth efficiency compared to many traditional site-to-site IPsec deployments that are often built as hub-and-spoke to simplify keying and policy. In other words, GETVPN is purpose-built to provide encryption

over MPLS without forcing a central hub for forwarding, while still using IPsec ESP for the actual data-plane protection. This is the practical difference captured by the statement about reducing latency and providing encryption over MPLS without the use of a central hub.

References: Cisco Group Encrypted Transport VPN (GETVPN) overview, Cisco GETVPN technical documentation (support)

QUESTION NO: 21

A network engineer is tasked with configuring a Cisco ISE server to implement external authentication against Active Directory. What must be considered about the authentication requirements? (Choose two.)

A. RADIUS communication must be permitted between the ISE server and the domain controller.

B. The ISE account must be a domain administrator in Active Directory to perform JOIN operations.

C. Active Directory only supports user authentication by using MSCHAPv2.

D. LDAP communication must be permitted between the ISE server and the domain controller.

E. Active Directory supports user and machine authentication by using MSCHAPv2.

ANSWER: D E

Explanation:

When Cisco ISE is integrated with Microsoft Active Directory, ISE joins the AD domain and then uses standard AD protocols to validate credentials and retrieve identity/group information. This requires allowing directory communications between ISE and the domain controllers; in practice this is LDAP/LDAPS (and related AD join/kerberos/RPC ports), so permitting LDAP communication between the ISE server and the domain controller is a key requirement to plan for. In addition, for 802.1X/EAP methods where ISE must validate a user password against AD, ISE commonly uses MSCHAPv2-based inner authentication (for example, PEAP-MSCHAPv2 or EAP-TTLS with MSCHAPv2) because AD natively supports validating MSCHAPv2 credentials. That MSCHAPv2 capability is also used for machine authentication scenarios (computer accounts) in domain environments, enabling both user and machine authentications when endpoints use those EAP methods. These considerations directly affect which EAP types you can deploy and which firewall rules/ports must be opened between ISE and AD for successful authentication and authorization lookups.

References: Cisco Identity Services Engine Configuration Guides, Microsoft Windows authentication and credential processing

QUESTION NO: 22

How is ICMP used as an exfiltration technique?

A. by flooding the destination host with unreachable packets

B. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address

C. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host

D. by overwhelming a targeted host with ICMP echo-request packets

ANSWER: C

Explanation:

ICMP can be abused for data exfiltration by tunneling information inside ICMP messages—most commonly ICMP echo-request/echo-reply—because many environments allow ICMP through firewalls for troubleshooting. In this technique, an attacker embeds (often encrypts/encodes) stolen data or command-and-control content into the ICMP payload field and sends it out of the network as a stream of ICMP packets. On the receiving side, a listener reconstructs the payloads to recover the exfiltrated data or to exchange C2 instructions. This is frequently described as “ICMP tunneling,” and tools/malware families have used it specifically to bypass egress controls that focus on TCP/UDP ports and application-layer inspection. The key idea is not denial-of-service behavior, but covertly carrying data in a protocol that is commonly permitted and less scrutinized. This aligns with the option describing encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host, which is a typical mechanism used to support exfiltration and remote control over ICMP.

References: MITRE ATT&CK: Exfiltration Over Alternative Protocol (ICMP), Cisco Secure Malware Analytics (Threat Grid)

QUESTION NO: 23

A user has a device in the network that is receiving too many connection requests from multiple machines. Which type of attack is the device undergoing?

A. SYN flood

B. slowloris

C. phishing

D. pharming

ANSWER: A

Explanation:

SYN flood is the best match for a situation where a device is receiving an abnormally high number of connection requests from many different machines. In a SYN flood, attackers send large volumes of TCP SYN packets (often from multiple sources in a distributed attack), forcing the target to allocate resources and maintain many half-open TCP connections while it waits for the final ACK that never arrives. This can exhaust the target’s connection table and CPU/memory resources, leading to degraded performance or denial of service for legitimate users. The key clue in the prompt is “too many connection requests,” which aligns directly with the TCP connection establishment process being abused at scale. This is a classic denial-of-service technique against TCP-based services and is commonly discussed in Cisco security fundamentals and DoS/DDoS mitigation topics.

References: https://en.wikipedia.org/wiki/SYN_flood, https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/13669-5.html

QUESTION NO: 24

Which industry standard is used to integrate Cisco ISE and pxGrid to each other and with other

interoperable security platforms?

A. IEEE

B. IETF

C. NIST

D. ANSI

ANSWER: B

Explanation:

The industry standard used for integrating Cisco ISE and pxGrid with other interoperable security platforms is IETF. pxGrid is built around widely adopted, open IETF standards for exchanging identity, context, and security events between systems. In particular, pxGrid uses XMPP (Extensible Messaging and Presence Protocol) as the messaging bus, which is standardized by the IETF and commonly used for publish/subscribe style communications. pxGrid also relies on standard TLS for transport security and uses certificate-based authentication to establish trusted connections between ISE and pxGrid clients. Because these are IETF-defined protocols, third-party security tools (for example, SIEM, EDR, NAC integrations, and network security platforms) can implement the same standards to interoperate with ISE via pxGrid without requiring proprietary transport mechanisms. Cisco's pxGrid documentation explicitly references XMPP and TLS as foundational technologies, aligning pxGrid interoperability with IETF standards rather than bodies like IEEE, NIST, or ANSI.

References: https://datatracker.ietf.org/doc/html/rfc6120, https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html

QUESTION NO: 25

What are two functions of IKEv1 but not IKEv2? (Choose two)

A. NAT-T is supported in IKEv1 but rot in IKEv2.

B. With IKEv1, when using aggressive mode, the initiator and responder identities are passed cleartext

C. With IKEv1, mode negotiates faster than main mode

D. IKEv1 uses EAP authentication

E. IKEv1 conversations are initiated by the IKE_SA_INIT message

ANSWER: B C

Explanation:

With IKEv1, aggressive mode is a distinct Phase 1 exchange that can send the initiator and responder identities before an encrypted channel is fully established, which means identities can be exposed in cleartext on the wire. IKEv2 removed the concept of "main mode vs aggressive mode" entirely and instead uses a fixed set of exchanges designed to provide identity protection by encrypting identities within the IKE_AUTH exchange after keys are established. Also, IKEv1 supports a "faster" Phase 1 negotiation mode compared to main mode—this is the practical purpose of aggressive mode: fewer messages and quicker setup (at the cost of reduced identity protection and some negotiation flexibility). These are behaviors specific to IKEv1's mode-based Phase 1 design and are not present as separate functions in IKEv2's streamlined exchange model. For additional protocol details, see the IKEv2 specification in RFC 7296 and the IKEv1 base specification in RFC 2409, which describe the exchange structures and identity handling differences. References: https://www.rfc-editor.org/rfc/rfc7296, https://www.rfc-editor.org/rfc/rfc2409

QUESTION NO: 26

```
RouterA(config) crypto key generate rsa general-keys label SSH modulus 2048
RouterA(config) ip ssh keypair-name SSH
RouterA(config) ip ssh version2
```

Refer to the exhibit. An engineer must enable secure SSH protocols and enters this configuration. What are two results of running this set of commands on a Cisco router? (Choose two.)

A. Labels the key pair to be used for SSH

B. Uses the FQDN with the label command

C. Generates AES key pairs on the router

D. Generates RSA key pair on the router

E. Enables SSHv1 on the router

ANSWER: A D

Explanation:

This configuration is the standard IOS workflow to prepare a router for SSH by ensuring the device has the identity information required for key generation and then creating the SSH key material. Setting the device's domain name is significant because IOS uses the hostname plus the configured domain name to form an FQDN, which is then used as part of the RSA key pair generation process for SSH. After that prerequisite is met, the command to create SSH keys generates an RSA public/private key pair locally on the router, which is what SSH uses for server authentication and to establish encrypted sessions. In other words, the practical outcomes are that the router now has an RSA key pair available for SSH operations and that the key pair is created and stored on the device for subsequent SSH connections. These are core requirements for enabling SSHv2 securely on Cisco IOS devices, and they align with Cisco's documented SSH configuration steps (domain name + RSA key generation). For additional context on IOS SSH prerequisites and RSA key generation, see Cisco's guidance on configuring SSH and the IOS crypto key generation behavior.

References: Cisco Secure Shell (SSH) Configuration Example, Cisco IOS XE Secure Shell (SSH) Configuration Guide

QUESTION NO: 27

What is a benefit of a Cisco Secure Email Gateway Virtual as compared to a physical Secure Email Gateway?

A. simplifies the distribution of software updates

B. provides faster performance

C. provides an automated setup process

D. enables the allocation of additional resources

ANSWER: D

Explanation:

“enables the allocation of additional resources ” is correct because the virtual form factor of Cisco Secure Email Gateway (formerly Email Security Appliance) allows you to scale the appliance by adjusting the virtual machine’s allocated CPU, memory, and disk resources (within supported limits) without needing to replace or physically upgrade hardware. This is a key operational advantage of virtual appliances in general: you can right-size capacity for changing mail volume, feature usage (for example, outbreak filters, encryption, or DLP processing), and performance needs by modifying VM resources and, when required, rebooting the VM—often much faster and with less procurement lead time than upgrading a physical appliance. Cisco’s virtual appliance deployment guidance emphasizes that the virtual edition runs as a VM on supported hypervisors and relies on the underlying virtualization platform for resource assignment, making scaling and capacity planning more flexible than fixed hardware models. See Cisco’s Secure Email Gateway documentation landing page for deployment and virtualization references: https://www.cisco.com/c/en/us/support/security/email-security-appliance/series.html and the Secure Email and Web Manager guides index: https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-and-configuration-guides-list.html.

QUESTION NO: 28

Refer to the exhibit.

Refer to the exhibit. Traffic is not passing through IPsec site-to-site VPN on the Secure Firewall Threat Defense appliance. What is causing this issue?

A. No split-tunnel policy is defined on the Secure Firewall Threat Defense appliance.

B. Site-to-site VPN preshared keys are mismatched.

C. The access control policy is not allowing VPN traffic in.

D. Site-to-site VPN peers are using different encryption algorithms.

ANSWER: C

Explanation:

The issue is that the access control policy is not allowing VPN traffic in. On Cisco Secure Firewall Threat Defense (FTD), even if the IPsec site-to-site VPN negotiation succeeds, the decrypted (cleartext) traffic must still be permitted by the Access Control Policy (ACP) to traverse the device. FTD evaluates traffic against the ACP based on the post-decryption flow, so if there is no rule permitting the inside-to-inside (or VPN-to-inside) traffic that results from the tunnel, packets will be dropped and “traffic not passing” is observed despite an apparently healthy tunnel. In practice, you typically need an explicit ACP rule allowing the relevant source/destination networks and applications (often with logging enabled for verification). This is a common operational difference for engineers coming from ASA, where crypto ACLs and interface ACLs behave differently; on FTD, the ACP is the primary policy gate for transit traffic, including VPN-decrypted flows. Verifying this involves checking ACP hit counts, connection events, and intrusion/file/malware policies applied to the matching rule.

References: Cisco Secure Firewall Threat Defense configuration guides, Cisco Secure Firewall (Firepower/FTD) technical documentation

QUESTION NO: 29

Which two mechanisms are used to control phishing attacks? (Choose two.)

A. Enable browser alerts for fraudulent websites.

B. Define security group memberships.

C. Revoke expired CRL of the websites.

D. Use antispyware software.

E. Implement email filtering techniques.

ANSWER: A E

Explanation:

Phishing is primarily an email- and web-based social-engineering attack, so the most effective controls focus on reducing delivery of malicious messages and warning users before they interact with fraudulent sites. Implementing email filtering techniques is a core anti-phishing mechanism because it can block or quarantine messages based on sender reputation, authentication results (SPF/DKIM/DMARC), URL rewriting/detonation, attachment sandboxing, and known-bad indicators. This directly reduces the likelihood that phishing emails reach end users and is a standard control in secure email gateways and cloud email security services.

Enable browser alerts for fraudulent websites is also a valid control because modern browsers and endpoint security integrations use reputation services (for example, Google Safe Browsing / Microsoft SmartScreen-like capabilities) to warn users when they attempt to visit known phishing or deceptive domains. These interstitial warnings and URL reputation checks help prevent credential submission even when a user clicks a phishing link.

These two mechanisms align with common security best practices for phishing defense: block at the email layer and protect at the web browsing layer with reputation-based warnings.

References: Cisco Secure Email (Email Security) overview, Google Chrome Safe Browsing protections

QUESTION NO: 30

What are two workloaded security models? (Choose two)

A. SaaS

B. IaaS

C. on-premises

D. off-premises

E. PaaS

ANSWER: B C

Explanation:

Workload security models commonly align to where the workload runs and who is responsible for securing the underlying components (the shared responsibility model). In Cisco security architecture discussions (including cloud workload protection and segmentation use cases), two foundational workload deployment/security models are cloud-based infrastructure and customer-owned infrastructure. Infrastructure as a Service (IaaS) is a core cloud workload model where the provider supplies compute, storage, and networking, while the customer secures the guest OS, applications, identities, and configurations for the workloads they deploy. On-premises is the traditional workload model where the organization owns and operates the full stack (hardware through applications), so the organization retains end-to-end responsibility for workload security controls such as segmentation, host hardening, patching, and monitoring. These two models are frequently contrasted because they drive different control points, visibility, and operational responsibilities for protecting workloads. Cisco Secure Workload (formerly Tetration) explicitly targets workload protection/segmentation across on-premises and cloud environments, reinforcing these as primary workload security contexts. For additional background on Cisco's workload security approach and general cloud responsibility boundaries, see Cisco Secure Workload and CISA Cloud Security Technical Reference Architecture.

QUESTION NO: 31

What are two differences between a Cisco Secure Web Appliance that is running in transparent mode and one running in explicit mode? (Choose two.)

A. The Cisco Secure Web Appliance responds with its own IP address only if it is running in transparent mode.

B. When the Cisco Secure Web Appliance is running in transparent mode, it uses the Secure Web Appliance's own IP address as the HTTP request destination.

C. The Cisco Secure Web Appliance responds with its own IP address only if it is running in explicit mode.

D. The Cisco Secure Web Appliance is configured in a web browser only if it is running in transparent mode.

ANSWER: C E

Explanation:

In explicit mode, client devices are aware of the proxy and are configured (manually, via PAC/WPAD, or via group policy/MDM) to send HTTP/HTTPS proxy requests directly to the Cisco Secure Web Appliance. Because the client is explicitly targeting the proxy, the proxy is the destination IP address for the TCP connection, and the appliance therefore responds using its own IP address in that proxy conversation. This is a key behavioral difference from transparent mode, where the client is not configured for a proxy and instead attempts to connect to the origin server; the network then intercepts and redirects that traffic to the appliance.

In transparent mode, the redirection typically relies on network infrastructure (commonly a Layer 3 device such as a router/switch using WCCP or policy-based routing) to steer web traffic to the Secure Web Appliance without changing endpoint proxy settings. This dependency on an upstream redirection mechanism is another practical difference between transparent and explicit deployments.

References: Cisco Secure Web Appliance configuration guides, Cisco Secure Web Appliance support documentation.

QUESTION NO: 32

Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

A. OpenC2

B. OpenIOC

C. CybOX

D. STIX

ANSWER: D

Explanation:

STIX is the open standard designed specifically to structure and represent cyber threat intelligence so it can be shared and processed in a machine-digestible way. It defines a common language and data model for describing threat actors, indicators, malware, attack patterns, vulnerabilities, observed data, relationships between objects, and more. This standardized representation enables consistent exchange of CTI across tools and organizations, improving automation for detection, correlation, enrichment, and response workflows. In practice, STIX content is commonly transported using TAXII, but STIX itself is the framework/data model that makes the intelligence portable and machine-readable. This aligns with how Cisco and the broader industry describe modern threat-intel sharing: STIX provides the structured format, while complementary standards handle transport and orchestration. For official background, see OASIS's STIX overview and specification resources, which describe STIX as a standardized language for cyber threat intelligence representation and sharing in a machine-readable form: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti and https://oasis-open.github.io/cti-documentation/stix/intro.

QUESTION NO: 33

Which two protocols must be configured to authenticate end users to the Cisco WSA? (Choose two.)

A. TACACS+

B. CHAP

C. NTLMSSP

D. RADIUS

E. Kerberos

ANSWER: C E

Explanation:

For Cisco Web Security Appliance (WSA) end-user authentication, the appliance commonly integrates with Microsoft Active Directory environments using browser-based authentication mechanisms. Two key protocols used for this are NTLMSSP and Kerberos. NTLMSSP (NTLM Security Support Provider) enables “transparent” authentication where the browser can automatically respond to an NTLM challenge from the proxy, allowing the WSA to identify and authenticate the user without prompting for credentials in many enterprise setups. Kerberos is used for Integrated Windows Authentication (IWA) as well, typically via SPNEGO/Negotiate, providing stronger mutual authentication and better security properties than NTLM when properly configured with AD, service principals, and time synchronization.

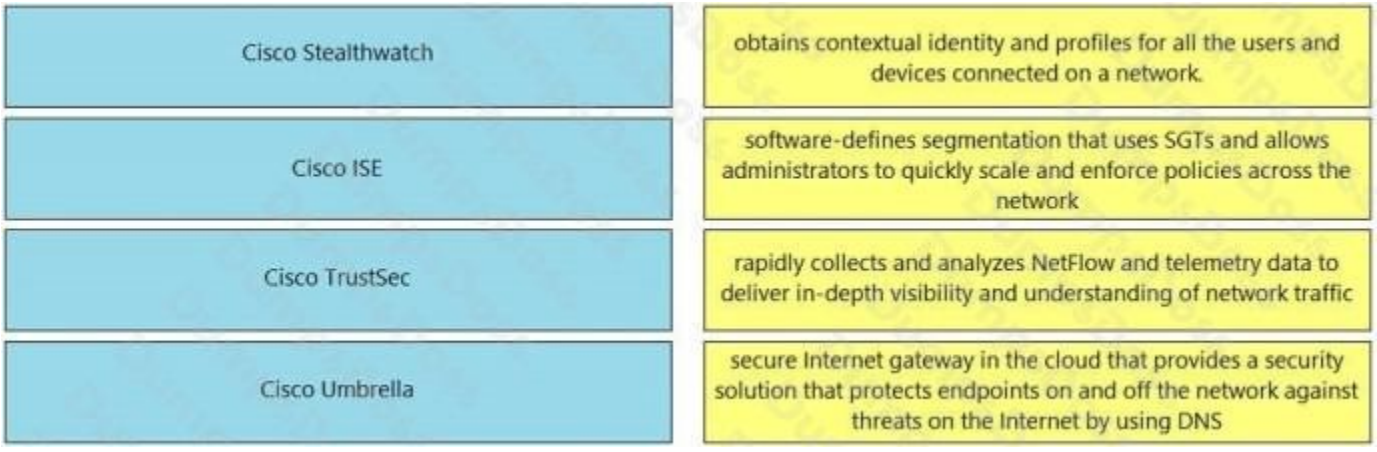
In contrast, TACACS+ and RADIUS are primarily AAA protocols used for network device administration and network access control (for example, authenticating administrators to infrastructure devices or authenticating 802.1X/VPN users), not the standard mechanisms WSA relies on for authenticating web proxy end users at the browser/proxy layer. Therefore, the protocols that must be configured for WSA end-user authentication in typical deployments are NTLMSSP and Kerberos.

References: Cisco WSA configuration guides, Microsoft Kerberos authentication overview

QUESTION NO: 34 - (DRAG DROP)

Drag and drop the solutions from the left onto the solution’s benefits on the right.

Select and Place:



ANSWER:

Explanation:

This matching is correct because each Cisco solution is being paired with the capability it is designed to deliver in Cisco security architectures. Cisco ISE is the platform that builds “who/what is on the network” context by authenticating users and profiling endpoints, then sharing that identity and posture information for policy decisions. That directly aligns with obtaining contextual identity and profiles for users and devices. Cisco TrustSec is Cisco’s policy and segmentation approach that uses Security Group Tags (SGTs) to classify traffic and enforce scalable access policies consistently across the network fabric, which matches the software-defined segmentation benefit. Cisco Stealthwatch (now commonly positioned as Cisco Secure Network Analytics) is centered on collecting and analyzing network telemetry such as NetFlow to provide deep visibility into traffic behaviors and to detect anomalies, which aligns with rapidly collecting and analyzing NetFlow/telemetry for in-depth traffic understanding. Cisco Umbrella is a cloud-delivered security service that includes DNS-layer protection and secure internet gateway capabilities to protect users on and off the corporate network from internet threats, matching the cloud secure internet gateway/DNS protection description.

References: Cisco Identity Services Engine (ISE), Cisco TrustSec, Cisco Secure Network Analytics (Stealthwatch), Cisco Umbrella.

QUESTION NO: 35

Which two tasks allow NetFlow on a Cisco ASA 5500 Series firewall? (Choose two.)

A. Define a NetFlow collector by using the flow-export command

B. Create a class map to match interesting traffic

C. Create an ACL to allow UDP traffic on port 9996

D. Enable NetFlow Version 9

E. Apply NetFlow Exporter to the outside interface in the inbound direction

ANSWER: A E

Explanation:

On Cisco ASA 5500 Series, enabling NetFlow Secure Event Logging (NSEL) export requires configuring where flow records will be sent and enabling flow creation/export on an interface. Defining a NetFlow collector by using the flow-export

command is a core step because the ASA must know the destination (collector IP/port) and transport parameters to export NSEL/NetFlow records. Without an export destination, the device can generate events but has nowhere to send them for analysis.

In addition, you must enable NetFlow/NSEL on an interface so the ASA will create flow events for traffic seen on that interface. Applying the NetFlow Exporter to the outside interface in the inbound direction is a valid way to activate flow monitoring for traffic entering that interface, which is a common deployment pattern for observing flows traversing the firewall. Together, these tasks establish both the export target and the interface-level activation needed for NetFlow operation on ASA.

References: Cisco ASA NetFlow Secure Event Logging (NSEL) configuration example, Cisco ASA Command Reference (flow-export and related NetFlow/NSEL commands).

QUESTION NO: 36

For which type of attack is multifactor authentication an effective deterrent?

A. Ping of death

B. Teardrop

C. SYN flood

D. Phishing

ANSWER: D

Explanation:

Phishing is an attack that commonly aims to steal user credentials (usernames/passwords) by tricking a victim into entering them into a fake login page or disclosing them via email, SMS, or voice. Multifactor authentication is an effective deterrent in this scenario because it reduces the value of a stolen password: even if an attacker successfully captures the victim's primary credential, they still typically cannot complete authentication without the additional factor (such as a one-time code, push approval, hardware token, or biometric). This makes account takeover significantly harder and often stops opportunistic phishing campaigns that rely on password reuse and single-factor logins. While advanced adversaries can attempt real-time "adversary-in-the-middle" phishing to capture session tokens or relay MFA prompts, MFA still materially raises the bar and is widely recommended as a core control to mitigate credential phishing risk. Cisco security best practices and general industry guidance consistently position MFA as a key protection against credential theft and unauthorized access stemming from phishing.

References: https://www.cisa.gov/secure-our-world/use-strong-passwords, https://www.cisa.gov/resources-tools/resources/implementing-phishing-resistant-mfa

QUESTION NO: 37

What are two reasons for implementing a multifactor authentication solution such as Cisco Duo Security provide to an organization? (Choose two.)

A. single sign-on access to on-premises and cloud applications

B. identification and correction of application vulnerabilities before allowing access to resources

C. secure access to on-premises and cloud applications

D. integration with 802.1x security using native Microsoft Windows supplicant

E. flexibility of different methods of 2FA such as phone callbacks, SMS passcodes, and push notifications

ANSWER: A C E

Explanation:

Implementing a multifactor authentication (MFA) solution like Cisco Duo is primarily about reducing the risk of account takeover by requiring an additional verification factor beyond a password. This directly enables secure access to on-premises and cloud applications because even if credentials are phished, reused, or otherwise compromised, an attacker still must satisfy the second factor to gain access. In practice, Duo is commonly deployed to protect VPN, VDI, Windows/macOS logons, and web/SaaS applications via SAML/SSO integrations and application gateways, improving the overall security posture for both internal and cloud-hosted resources.

A second key reason is the flexibility of different methods of 2FA such as phone callbacks, SMS passcodes, and push notifications. Organizations benefit from offering multiple factor options to match user needs, device availability, and risk tolerance. For example, push-based approval through Duo Mobile is convenient for most users, while passcodes or phone callbacks can serve as alternatives when push is unavailable. This flexibility improves adoption and usability while maintaining strong authentication controls.

References: https://duo.com/product/multi-factor-authentication-mfa, https://duo.com/docs

QUESTION NO: 38

What does endpoint isolation in Cisco AMP for Endpoints security protect from?

A. an infection spreading across the network E

B. a malware spreading across the user device

C. an infection spreading across the LDAP or Active Directory domain from a user account

D. a malware spreading across the LDAP or Active Directory domain from a user account

ANSWER: A

Explanation:

Endpoint isolation in Cisco AMP for Endpoints (Cisco Secure Endpoint) is designed to contain a potentially compromised host by cutting off its network communications, thereby preventing the threat on that endpoint from reaching other systems. When an endpoint is isolated, the connector enforces network restrictions so the device cannot communicate with other hosts (except for explicitly allowed traffic such as to the Secure Endpoint cloud and any administrator-defined allow lists). This containment capability is primarily about stopping lateral movement and limiting propagation beyond the infected machine—i.e., preventing an infection from spreading across the network. It is not a control that specifically targets directory services (LDAP/Active Directory) propagation from a user account; rather, it broadly blocks network connectivity to reduce the blast radius while investigation and remediation occur. This is why the best match is the option describing prevention of an infection spreading across the network.

References: Cisco Secure Endpoint (AMP for Endpoints) product page, Cisco Community: AMP Endpoint Isolation

QUESTION NO: 39

Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?

A. PaaS

B. XaaS

C. IaaS

D. SaaS

ANSWER: A

Explanation:

PaaS is the cloud service model that provides a complete application development and deployment environment while abstracting away the underlying infrastructure management. With Platform as a Service, the cloud provider manages the servers, storage, networking, virtualization, operating system, and often middleware/runtime components (for example, web servers, databases, language runtimes, and scaling mechanisms). The cloud consumer focuses on building, testing, deploying, and operating their applications and data, typically using provider-supplied tools, APIs, CI/CD integrations, and managed services. This matches the requirement of enabling development and deployment “without needing to manage or maintain the underlying cloud infrastructure,” which is the defining characteristic of PaaS in standard cloud service model definitions. In contrast to infrastructure-focused offerings, PaaS is specifically designed to accelerate application delivery by removing the operational burden of maintaining the platform layers beneath the application code. For commonly accepted definitions of PaaS and the shared responsibility boundaries, see https://www.nist.gov/publications/nist-definition-cloud-computing and https://aws.amazon.com/types-of-cloud-computing/.

QUESTION NO: 40

In which two ways does the Cisco Advanced Phishing Protection solution protect users? (Choose two.)

A. It prevents use of compromised accounts and social engineering.

B. It prevents all zero-day attacks coming from the Internet.

C. It automatically removes malicious emails from users' inbox.

D. It prevents trojan horse malware using sensors.

E. It secures all passwords that are shared in video conferences.

ANSWER: A C

Explanation:

Cisco Advanced Phishing Protection (AAP) is designed to reduce business email compromise (BEC) and identity-deception phishing by analyzing who the sender claims to be and whether that identity makes sense in context. It does this by applying behavioral analysis and relationship modeling (for example, typical communication patterns between executives, finance staff, vendors, and partners) to detect impersonation attempts and other social-engineering tactics. That directly supports the protection outcome described as preventing use of compromised accounts and social engineering, because the solution

focuses on detecting anomalous or deceptive sender behavior and display-name/domain spoofing patterns commonly used in BEC.

AAP also supports post-delivery protection through retrospective verdicting and remediation workflows. As new intelligence or analytics determine that a previously delivered message is malicious or part of an ongoing deception campaign, the solution can enable automated remediation actions so that malicious messages are removed from user mailboxes, reducing dwell time and limiting the chance a user acts on the email. These capabilities align with the protection outcome of automatically removing malicious emails from users' inbox.

References: Cisco Secure Email (Email Security) overview, Cisco Secure Email product information.

QUESTION NO: 41

Which Cisco security solution secures public, private, hybrid, and community clouds?

A. Cisco ISE

B. Cisco ASAv

C. Cisco Cloudlock

D. Cisco pxGrid

ANSWER: C

Explanation:

Cisco Cloudlock is the Cisco security solution designed to secure cloud services across deployment models, including public, private, hybrid, and community clouds, by operating as a cloud access security broker (CASB). As a cloud-native CASB, it focuses on protecting SaaS usage and cloud-resident data through capabilities such as visibility into cloud application activity, policy enforcement, compliance reporting, and detection of risky or anomalous behavior. Cloudlock integrates with major cloud applications and platforms using APIs to monitor configurations and user actions, identify sensitive data exposure, and help enforce governance controls without requiring inline traffic redirection. This makes it well-suited for organizations that consume multiple cloud services and need consistent security controls and compliance posture across them. Cisco positions Cloudlock within its cloud and application security portfolio specifically for securing cloud applications and cloud environments, aligning with the requirement to cover multiple cloud deployment types. For additional context on Cisco's cloud security and CASB approach, see Cisco's cloud security overview and Cloudlock/CASB resources: https://www.cisco.com/c/en/us/products/security/cloud-security/index.html and https://www.cisco.com/c/en/us/products/security/cloudlock/index.html.

QUESTION NO: 42

What are two benefits of workload security? (Choose two.)

A. Tracked application security

B. Automated patching

C. Reduced attack surface

D. Scalable security policies

ANSWER: C D

Explanation:

Workload security focuses on protecting compute workloads (VMs, containers, and cloud instances) by applying consistent controls close to where applications run. A key benefit is **Reduced attack surface**, because workload security commonly includes hardening, segmentation/microsegmentation, and limiting unnecessary exposure between workloads. By restricting east-west traffic and enforcing least-privilege communications, there are fewer reachable paths for lateral movement and fewer exploitable services exposed.

Another major benefit is **Scalable security policies**. In modern data centers and cloud environments, workloads are dynamic (autoscaling, ephemeral containers, frequent redeployments). Workload security platforms typically use centralized policy definitions with automation and orchestration integrations so controls can be applied consistently as workloads are created, moved, or scaled. This improves operational consistency and reduces configuration drift across environments (on-prem, hybrid, and multi-cloud).

These benefits align with Cisco's broader data center and cloud security approach, where policy-based segmentation and centrally managed controls help reduce risk while supporting rapid workload changes. See Cisco's Secure Workload overview and guidance on segmentation and workload protection: Cisco Secure Workload and Cisco ACI Security.

QUESTION NO: 43

A company discovered an attack propagating through their network via a file. A custom file detection policy was created in order to track this in the future and ensure no other endpoints execute to infected file. In addition, it was discovered during testing that the scans are not detecting the file as an indicator of compromise. What must be done in order to ensure that the policy created is functioning as it should?

A. Create an IP block list for the website from which the file was downloaded.

B. Block the application that the file was using to open.

C. Upload the hash for the file into the policy.

D. Send the file to Cisco Threat Grid for dynamic analysis.

ANSWER: C

Explanation:

Uploading the hash for the file into the policy is required because custom file detection/blocking in Cisco Secure Endpoint (AMP for Endpoints) and related Cisco security controls is commonly implemented using file trajectory/IOC matching based on cryptographic hashes (for example, SHA-256). If testing shows the file is not being detected as an indicator of compromise, the most direct way to make the custom policy reliably match the exact malicious sample is to add the file's hash to the custom detection list/policy so the endpoint connector can identify it regardless of filename, path, or delivery method. Hash-based indicators are deterministic and are a standard method for enforcing "block this exact file everywhere" behavior across endpoints once the policy is deployed and the connector receives the updated policy. This aligns with Cisco's general guidance around using file hashes as IOCs for endpoint detection and response workflows and for creating custom detections/exclusions based on known file identities.

References: Cisco Secure Endpoint (AMP for Endpoints) overview, Cisco Secure Endpoint product page

QUESTION NO: 44

What are two characteristics of Cisco DNA Center APIs? (Choose two.)

A. They are Cisco proprietary.

B. They do not support Python scripts.

C. They view the overall health of the network.

D. They quickly provision new devices.

E. Postman is required to utilize Cisco DNA Center API calls.

ANSWER: C D

Explanation:

Cisco DNA Center APIs are designed to expose DNA Center's intent-based networking capabilities programmatically. A key characteristic is that they can be used to view the overall health of the network, because DNA Center provides REST endpoints for assurance/analytics that return device, client, and site health, issues, and trends—enabling external tools or scripts to query and visualize network health without using the GUI. Another core characteristic is that they can quickly provision new devices, since DNA Center's intent and automation workflows (such as discovery, inventory, and provisioning) are exposed through APIs that allow you to trigger and orchestrate onboarding and configuration at scale. These APIs are RESTful and commonly consumed by automation tools and scripts (including Python), and they do not require a specific client like Postman—Postman is simply a convenient testing tool. Cisco documents these capabilities in the DNA Center Platform documentation, including API categories for Assurance (health/insights) and Provisioning/Device Onboarding, which align directly to network health visibility and rapid provisioning use cases.

References: Cisco DNA Center Platform (Developer) Documentation, Cisco DNA Center product overview

QUESTION NO: 45

What is an advantage of the Cisco Umbrella roaming client?

A. the ability to see all traffic without requiring TLS decryption

B. visibility into IP-based threats by tunneling suspicious IP connections

C. the ability to dynamically categorize traffic to previously uncategorized sites

D. visibility into traffic that is destined to sites within the office environment

ANSWER: B

Explanation:

The Cisco Umbrella roaming client (often deployed via the Umbrella Roaming Security module in Cisco Secure Client/AnyConnect) extends Umbrella protection to endpoints when they are off-network or not connected to a corporate VPN. A key advantage is visibility into IP-based threats by tunneling suspicious IP connections to the Umbrella cloud for inspection and enforcement. This matters because not all malicious activity is purely DNS-based; malware and command-and-control can use direct IP connections or nonstandard ports/protocols. By selectively forwarding (tunneling) these risky IP flows to Umbrella, the roaming client enables cloud-based detection and blocking even when users are roaming, helping

prevent callbacks and connections to known-bad infrastructure outside the enterprise perimeter. This capability complements DNS-layer enforcement and helps maintain consistent security policy for remote users without requiring all traffic to hairpin through a central VPN concentrator. Cisco documents this behavior as part of Umbrella's roaming/endpoint protection features, including IP-layer enforcement for suspicious destinations. See: https://docs.umbrella.com/umbrella-user-guide/docs/roaming-client and https://docs.umbrella.com/deployment-umbrella/docs/roaming-security-module.

QUESTION NO: 46

When configuring ISAKMP for IKEv1 Phase1 on a Cisco IOS router, an administrator needs to input the

command crypto isakmp key cisco address 0.0.0.0. The administrator is not sure what the IP addressing in this command issued for. What would be the effect of changing the IP address from 0.0.0.0 to 1.2.3.4?

A. The key server that is managing the keys for the connection will be at 1.2.3.4

B. The remote connection will only be allowed from 1.2.3.4

C. The address that will be used as the crypto validation authority

D. All IP addresses other than 1.2.3.4 will be allowed

ANSWER: B

Explanation:

In IKEv1 Phase 1 using pre-shared keys on Cisco IOS, the `crypto isakmp key` command binds a specific pre-shared key to a specific peer identity, most commonly the peer's IP address. Using `address 0.0.0.0` (typically with a mask such as `0.0.0.0 0.0.0.0` on many IOS versions) acts as a "match any peer" entry, meaning the router will accept that pre-shared key for any remote peer address that does not have a more specific match. If you change the address to `1.2.3.4`, you are no longer defining a universal key; you are defining a key that applies only when the remote IKE peer is identified as `1.2.3.4`. Practically, this restricts successful IKE authentication with that particular key to the peer at `1.2.3.4` (unless additional `crypto isakmp key` statements exist for other peers). This is a common way to tighten PSK usage so that a shared secret is not accepted from arbitrary source addresses. See Cisco IOS IKE/ISAKMP PSK configuration guidance in the IPsec VPN configuration documentation: Cisco IPsec/IKE troubleshooting and concepts and Cisco IOS IKE/IPsec VPN Configuration Guide.

QUESTION NO: 47

Which two commands are required when configuring a flow-export action on a Cisco ASA? (Choose two.)

A. flow-export event-type

B. policy-map

C. access-list

D. flow-export template timeout-rate 15

E. access-group

ANSWER: A B

Explanation:

On Cisco ASA, NetFlow Secure Event Logging (NSEL) flow export is configured using the Modular Policy Framework (MPF). That means you must build a policy framework that can apply an inspection/action to matching traffic. The *policy-map* command is required because the flow-export action is applied under a policy map (typically a global policy) where you define what to do with the matched traffic. In addition, the *flow-export event-type* command is required because it specifies which NSEL event records the ASA should export (for example, flow-create, flow-teardown, and related event types). Without defining the event type, the ASA has no instruction on which flow events to generate and export as NetFlow/NSEL records. Other items like ACLs and access-groups are used for traffic filtering and interface policy enforcement, but they are not inherently required just to define the flow-export action itself within MPF. Template timeout tuning can be configured, but it is not mandatory for a basic, valid flow-export action configuration. For ASA NSEL/NetFlow export configuration concepts and MPF usage, see Cisco's ASA NetFlow/NSEL documentation and MPF overview: Cisco ASA configuration examples and Cisco ASA CLI reference.

QUESTION NO: 48

A company is experiencing exfiltration of credit card numbers that are not being stored on-premise. The company needs to be able to protect sensitive data throughout the full environment. Which tool should be used to accomplish this goal?

A. Cisco ISE

B. Web Security Appliance

C. Security Manager

D. Cloudlock

ANSWER: D

Explanation:

Cloudlock is the right tool because it is a cloud access security broker (CASB) designed to discover, monitor, and protect sensitive data in cloud applications and across users' cloud activity—exactly what you need when credit card numbers are being exfiltrated and the data is not stored on-premises. A CASB provides visibility into cloud app usage (including sanctioned and unsanctioned/SaaS usage), applies data loss prevention (DLP) policies to detect regulated data such as PCI/credit card numbers, and can take enforcement actions like blocking sharing, quarantining content, alerting, or applying remediation workflows. This aligns with the requirement to protect sensitive data "throughout the full environment," including cloud services where the data resides or traverses. Cloudlock's strengths are in SaaS security posture, user behavior analytics, and DLP controls for cloud data and cloud app interactions, which directly addresses exfiltration scenarios beyond the on-prem perimeter.

References: Cisco Cloudlock (product overview), Cisco Cloudlock FAQ

QUESTION NO: 49

Which two methods must be used to add switches into the fabric so that administrators can control how switches are added into DCNM for private cloud management? (Choose two.)

A. Cisco Cloud Director

B. Cisco Prime Infrastructure

C. PowerOn Auto Provisioning

D. Seed IP

E. CDP AutoDiscovery

ANSWER: C D

Explanation:

In Cisco DCNM (now evolved into Nexus Dashboard Fabric Controller in newer releases), controlled onboarding of switches into a fabric is typically done using discovery and provisioning workflows that let administrators explicitly define what devices are brought under management and how they are configured. “Seed IP” is a core discovery approach: you provide one or more reachable management IP addresses as starting points, and DCNM uses that information to discover and inventory the fabric devices in a controlled manner. “PowerOn Auto Provisioning” is the complementary method used to automate initial device bring-up and bootstrap configuration so that newly racked switches can be onboarded predictably (for example, ensuring management reachability and baseline settings) before they are incorporated into the fabric management domain. Together, these methods support private-cloud operational models where you want repeatable, policy-driven onboarding while still retaining administrative control over which switches are admitted and how they are initialized. For additional context on Cisco’s fabric management and device onboarding concepts, see Cisco’s Nexus Dashboard Fabric Controller overview and documentation landing pages: Cisco Nexus Dashboard Fabric Controller and NDFC Documentation and Support.

QUESTION NO: 50

Which ESA implementation method segregates inbound and outbound email?

A. one listener on a single physical Interface

B. pair of logical listeners on a single physical interface with two unique logical IPv4 addresses and one IPv6 address

C. pair of logical IPv4 listeners and a pair Of IPv6 listeners on two physically separate interfaces

D. one listener on one logical IPv4 address on a single logical interface

ANSWER: B

Explanation:

The correct method is using a pair of logical listeners on a single physical interface with separate IP identities so the appliance can apply different mail flow policies to inbound versus outbound SMTP connections. In Cisco Email Security Appliance (ESA), a “listener” is the SMTP service bound to a specific interface/IP/port combination. By creating separate listeners (commonly one for inbound mail from the Internet to your mail servers and another for outbound/relay mail from your internal mail servers), you cleanly separate policy enforcement, sender groups, relay controls, TLS requirements, and anti-spam/AV behaviors per direction of mail flow. This design is a standard best practice because it avoids mixing inbound and outbound trust models on the same listener and makes it easier to apply distinct access controls (for example, only allowing internal hosts to use the outbound listener for relaying). Cisco documentation and configuration guidance for ESA listeners and mail flow supports deploying multiple listeners on the same physical interface using different IP addresses to logically separate traffic and policies. See Cisco’s ESA user/configuration guidance around listeners and mail flow: Cisco Email Security Appliance configuration guides and an example of outbound relay/mail flow configuration concepts: ESA Outbound Traffic Relay Configuration Example.

QUESTION NO: 51

A network engineer has entered the snmp-server user andy myv3 auth sha cisco priv aes 256 cisc0383320506 command and needs to send SNMP information to a host at 10.255.254.1. Which command achieves this goal?

A. snmp-server host inside 10.255.254.1 snmpv3 andy

B. snmp-server host inside 10.255.254.1 version 3 myv3

C. snmp-server host inside 10.255.254.1 snmpv3 myv3

D. snmp-server host inside 10.255.254.1 version 3 andy

ANSWER: D

Explanation:

To send SNMP notifications (traps/informs) to a remote manager, you must configure an SNMP host destination and tie it to the SNMPv3 security model being used. The user creation command shown defines an SNMPv3 user named andy and associates that user with the SNMPv3 group myv3, including authentication (SHA) and privacy (AES-256) parameters. When configuring the destination host, the device needs to know which SNMP version and which SNMPv3 user credentials to use when generating notifications toward 10.255.254.1. The command that accomplishes this is the one that specifies the host IP address and explicitly sets SNMP version 3 along with the SNMPv3 user that will be used for secure communication. This aligns with Cisco IOS/IOS XE SNMP configuration where the snmp-server host command includes a version 3 keyword and the username for SNMPv3 notifications. See Cisco SNMP host configuration guidance here: Cisco IOS XE SNMP Notifications Configuration and SNMPv3 user/host usage examples here: Cisco SNMPv3 Configuration Example.

QUESTION NO: 52

Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)

A. It must include the current date.

B. It must reside in the trusted store of the WSA.

C. It must reside in the trusted store of the endpoint.

D. It must have been signed by an internal CA.

E. it must contain a SAN.

ANSWER: B C

Explanation:

For Cisco Web Security Appliance (WSA) HTTPS decryption, the appliance must be able to validate the server certificate chain and also present a trusted signing chain to clients when it performs man-in-the-middle decryption. First, the certificate chain used to validate the origin server must be trusted by the WSA, which is why the relevant CA certificates must reside in the trusted store of the WSA. Without a trusted CA chain, WSA cannot reliably authenticate the upstream server certificate during the TLS handshake and therefore cannot proceed with decryption in a secure/validated manner.

Second, when WSA dynamically generates (or presents) a substitute certificate to the client during decryption, the client must trust the CA that signed that substitute certificate. Practically, this means the WSA's HTTPS decryption CA (or the

enterprise CA used to sign the WSA's signing certificate) must reside in the trusted store of the endpoint; otherwise, endpoints will see certificate warnings or fail the TLS connection, preventing successful decrypted access. These two trust requirements—WSA trust of upstream server CAs and endpoint trust of the WSA's signing CA—are foundational to operational HTTPS inspection on WSA.

References: Cisco Web Security Appliance configuration guides, Cisco WSA support documentation.

QUESTION NO: 53

Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)

A. Cisco Umbrella

B. Cisco ISE

C. Cisco DNA Center

D. Cisco TrustSec

E. Cisco Duo Security

ANSWER: A E

Explanation:

Cisco Umbrella and Cisco Duo Security both directly reduce the success rate of phishing and social engineering by protecting users at the point where they click links, resolve domains, and authenticate. Cisco Umbrella provides DNS-layer security (and optional secure web gateway capabilities) that can block access to known malicious domains, command-and-control infrastructure, and phishing sites before a connection is established. This is particularly effective for endpoints both on and off the corporate network because enforcement can occur via roaming clients and DNS policies, limiting the impact of a user being tricked into clicking a malicious link.

Cisco Duo Security helps by hardening the authentication step that attackers often target after harvesting credentials through phishing. By enforcing multi-factor authentication, device health checks, and adaptive access policies, Duo can prevent stolen usernames/passwords from being sufficient to access VPNs, SaaS apps, and internal resources. In practice, even if a user is socially engineered into revealing credentials, strong MFA and risk-based controls significantly reduce account takeover. These two solutions complement each other: Umbrella reduces exposure to phishing destinations, while Duo reduces the blast radius if credentials are compromised.

References: Cisco Umbrella, Cisco Duo

QUESTION NO: 54

Which Cisco DNA Center RESTful PNP API adds and claims a device into a workflow?

A. api/v1/fie/config

B. api/v1/onboarding/pnp-device/import

C. api/v1/onboarding/pnp-device

D. api/v1/onboarding/workflow

ANSWER: B

Explanation:

The endpoint

api/v1/onboarding/pnp-device/import

is the Cisco DNA Center Plug and Play (PnP) API used to bring devices into the PnP inventory by importing device details (for example, PID/serial, device info, and site parameters) and associating them to an onboarding workflow so they can be claimed/provisioned through that workflow. In Cisco DNA Center, “claiming” a device is the act of assigning it to a specific workflow (which can include image, template/config, and other onboarding actions) so that when the device contacts PnP, DNA Center knows exactly how to onboard it. The import operation is the practical REST entry point for adding devices into the PnP database and tying them to the workflow context used during provisioning. This aligns with Cisco DNA Center Platform PnP API usage patterns where device import/claim actions are performed via the PnP device import endpoint rather than generic workflow listing or base device collection endpoints. References: Cisco DNA Center Platform APIs, Cisco DNA Center Plug and Play APIs.

QUESTION NO: 55

An organization recently installed a Cisco Secure Web Appliance and would like to take advantage of the AVC engine to allow the organization to create a policy to control application-specific activity.

After enabling the AVC engine, what must be done to implement this?

A. Use an access policy group to configure application control settings.

B. Use security services to configure the traffic monitor.

C. Use URL categorization to prevent the application traffic.

ANSWER: A

Explanation:

Use an access policy group to configure application control settings is correct because on Cisco Secure Web Appliance (formerly WSA), Application Visibility and Control (AVC) is enforced through the web access policy framework. After the AVC engine is enabled, you must apply AVC-based controls within an Access Policy Group so the appliance can evaluate web requests against application classifications and then take actions (for example, allow, block, monitor, or apply additional controls) based on the identified application. In other words, enabling AVC turns on the capability to detect and classify application traffic, but policy enforcement happens where web access decisions are made: the Access Policies (and their associated policy groups). This is the operational step that actually “implements” application-specific control for users/identities/networks governed by that policy group. Cisco documents AVC on Secure Web Appliance as an application-layer classification feature integrated with access policies for control and reporting. See Cisco Secure Web Appliance documentation for policy configuration and AVC concepts: Cisco Secure Web Appliance User Guides and Cisco Secure Web Appliance overview resources: Cisco Secure Web Appliance.

QUESTION NO: 56

What is a benefit of using a multifactor authentication strategy?

A. It provides visibility into devices to establish device trust.

B. It provides secure remote access for applications.

C. It provides an easy, single sign-on experience against multiple applications

D. It protects data by enabling the use of a second validation of identity.

ANSWER: D

Explanation:

It protects data by enabling the use of a second validation of identity is correct because multifactor authentication (MFA) strengthens access control by requiring users to prove their identity using two or more independent factors (typically something you know, something you have, and/or something you are). This directly reduces the likelihood that a stolen or guessed password alone can be used to access systems and sensitive information. In practical security operations, MFA is one of the most effective compensating controls against credential theft, phishing, password spraying, and reuse of breached passwords, because an attacker must also compromise an additional factor (for example, a hardware token, authenticator app push approval, or biometric). By improving the assurance level of authentication, MFA helps protect data and applications from unauthorized access even when primary credentials are exposed. This is a core best practice in zero trust and modern identity security architectures, where identity is treated as the new perimeter and stronger authentication is a foundational control. See Cisco's overview of MFA concepts and benefits in identity security guidance and NIST's digital identity authentication recommendations: https://www.cisco.com/c/en/us/products/security/duo-multifactor-authentication-mfa/index.html and https://pages.nist.gov/800-63-3/sp800-63b.html.

QUESTION NO: 57

Which Cisco security solution protects remote users against phishing attacks when they are not connected to the VPN?

A. Cisco Umbrella

B. Cisco Firepower NGIPS

C. Cisco Stealthwatch

D. Cisco Firepower

ANSWER: A

Explanation:

Cisco Umbrella is designed to protect users wherever they are, including when they are off-network and not connected to a corporate VPN. Umbrella provides cloud-delivered DNS-layer security (and optional secure web gateway capabilities) that can block access to known malicious domains, command-and-control callbacks, and many phishing destinations before a connection is fully established. For roaming users, Umbrella can be enforced using the Umbrella Roaming Client (or AnyConnect Umbrella Roaming Security module), which redirects DNS requests to Umbrella's resolvers and applies the organization's security policies even on public Wi-Fi or home networks. This makes it a strong fit for preventing phishing-related domain lookups and web access outside the VPN, reducing reliance on backhauling traffic to a central security stack. Cisco positions Umbrella specifically for "secure internet gateway" and "DNS security" use cases that extend protection beyond the perimeter to remote endpoints. See Cisco's Umbrella overview and roaming/off-network protection details here: https://www.cisco.com/c/en/us/products/security/umbrella/index.html and https://docs.umbrella.com/umbrella-user-guide/docs/roaming-client.

QUESTION NO: 58

What is the purpose of the My Devices Portal in a Cisco ISE environment?

A. to register new laptops and mobile devices

B. to manage and deploy antivirus definitions and patches on systems owned by the end user

C. to provision userless and agentless systems

D. to request a newly provisioned mobile device

ANSWER: A

Explanation:

The My Devices Portal in Cisco ISE is an end-user self-service portal used to view and manage the endpoints associated with a user account, most commonly for BYOD scenarios. A primary purpose is allowing users to register (onboard) their personal endpoints—such as laptops, tablets, and smartphones—so those devices can be identified by ISE and granted the appropriate network access based on policy. In practice, this portal supports workflows like adding a new device, seeing previously registered devices, and (depending on configuration) removing or renaming devices. This helps organizations scale endpoint onboarding without requiring help-desk intervention for every new personal device, while still maintaining visibility and control through ISE's identity-based access policies. The portal is not intended for endpoint security operations like patching/AV management, nor is it specifically for "userless/agentless" provisioning; it is focused on user-associated device registration and management within ISE's BYOD and endpoint identity capabilities.

References: Cisco Identity Services Engine (ISE) Install and Configure Guides, Cisco Identity Services Engine product page

QUESTION NO: 59

Which two behavioral patterns characterize a ping of death attack? (Choose two.)

A. The attack is fragmented into groups of 16 octets before transmission.

B. The attack is fragmented into groups of 8 octets before transmission.

C. Short synchronized bursts of traffic are used to disrupt TCP connections.

D. Malformed packets are used to crash systems.

E. Publicly accessible DNS servers are typically used to execute the attack.

ANSWER: B D

Explanation:

A ping of death is a classic denial-of-service technique that abuses ICMP Echo Request/Reply handling by sending an IP packet that becomes larger than the maximum allowed size once it is reassembled by the target. Because IPv4 has a maximum total length of 65,535 bytes, an attacker can craft oversized ICMP payloads and then rely on IP fragmentation so the packet traverses the network in smaller fragments, but reassembles into an invalid (oversized) datagram at the destination. This is why fragmentation behavior is commonly associated with the attack. The key impact is that the target's IP stack or ICMP processing code encounters an invalid/oversized or otherwise malformed reassembled packet, which

historically led to crashes, hangs, or reboots—hence the characterization that malformed packets are used to crash systems. Modern systems generally mitigate this, but the defining behavioral pattern remains: fragmented ICMP traffic that reassembles into an illegal size and triggers faulty handling. For background on IP fragmentation/reassembly limits and the nature of the ping of death, see https://en.wikipedia.org/wiki/Ping_of_death and the IPv4 specification details in https://www.rfc-editor.org/rfc/rfc791.

QUESTION NO: 60

Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two.)

A. SIP

B. inline normalization

C. SSL

D. packet decoder

E. modbus

ANSWER: A C

Explanation:

Firepower NGIPS (Snort-based inspection in Firepower) uses application-layer preprocessors to understand and normalize specific protocols before rule evaluation, so signatures can match reliably and evasions are reduced. SIP is one of these preprocessors; it parses Session Initiation Protocol signaling, tracks dialogs, and exposes protocol fields to detection logic. SSL is also implemented as an application-layer preprocessor in this context; it identifies and processes SSL/TLS sessions (for example, tracking handshakes and session state) so the engine can apply relevant detection and policy behaviors around encrypted traffic handling. These are explicitly listed among Firepower's application-layer preprocessors in Cisco documentation for the Firepower Management Center configuration guide.

In contrast, items like packet decoding and normalization are foundational inspection functions rather than application-layer preprocessors, and industrial protocols such as Modbus are handled under different inspection components depending on platform/version and licensing. For the exam objective, the key is recognizing the named application-layer preprocessors that Snort/Firepower exposes as preprocessors for protocol-aware inspection.

References: Cisco Firepower Management Center Configuration Guide – Application Layer Preprocessors, Snort Documentation.

QUESTION NO: 61

An engineer is configuring Cisco WSA and needs to enable a separated email transfer flow from the Internet and from the LAN. Which deployment mode must be used to accomplish this goal?

A. single interface

B. multi-context

C. transparent

D. two-interface

ANSWER: D

Explanation:

The correct deployment mode is *two-interface* because it physically and logically separates traffic flows by using different network interfaces for different sides of the mail flow. In a typical email security gateway design, you want one interface facing the untrusted/external network (Internet/DMZ side) and another interface facing the trusted/internal network (LAN side). This separation supports distinct routing, access control, and policy enforcement per side, and it aligns with common best practices for placing an email security appliance between the Internet and the internal mail infrastructure. Using two interfaces also simplifies designing inbound and outbound mail paths (for example, inbound SMTP from the Internet to the gateway on the external interface, then relayed to internal mail servers via the internal interface; and outbound SMTP from internal mail servers to the gateway on the internal interface, then relayed to the Internet via the external interface). Cisco's email security deployment guidance describes using separate interfaces to segment and control mail traffic between internal and external networks. See Cisco Email Security documentation and deployment guidance: Cisco Email Security Appliance configuration guides and Cisco Secure Email (ESA) product documentation.

QUESTION NO: 62

An engineer must deploy Cisco Secure Email with Cloud URL Analysis and must meet these requirements:

To protect the network from large-scale virus outbreaks

To protect the network from non-viral attacks such as phishing scams and malware distribution To provide active analysis of the structure of the URL and information about the domain and page contents

Which two prerequisites must the engineer ensure are configured? (Choose two.)

A. Scanning enabled for each Verdict, Prepend Subject and Deliver.

B. Outbreak Filters must be enabled globally.

C. Enable TLS by setting to Preferred to the Default Domain.

D. Service Logs must be enabled.

ANSWER: A B

Explanation:

To meet the stated requirements, the deployment must use the Cisco Secure Email features that specifically address outbreak-style malware events and URL-based threats. Enabling Outbreak Filters globally is a prerequisite because Outbreak Filters are the mechanism Cisco Secure Email uses to detect and mitigate large-scale, rapidly spreading malware outbreaks by applying outbreak intelligence and rules at the system level. Without Outbreak Filters enabled, the system cannot provide the intended "large-scale virus outbreak" protection.

Cloud URL Analysis requires that URL scanning be enabled in the relevant mail policies so that messages containing URLs are actually submitted for analysis and verdicting. The prerequisite captured by "Scanning enabled for each Verdict, Prepend Subject and Deliver." aligns with enabling URL scanning actions based on verdict outcomes (for example, appending verdict information to the subject and delivering/quarantining according to policy). This ensures the platform performs active URL inspection and returns domain/page intelligence as part of message handling.

These two configurations directly map to the requirements: outbreak protection and active URL analysis for phishing/malware distribution. Reference: Cisco Secure Email (Email Security), Cisco Secure Email user guides.

QUESTION NO: 63

Which two commands are required when configuring a flow-export action on a Cisco ASA? (Choose

two.)

A. flow-export event-type

B. policy-map

C. access-list

D. flow-export template timeout-rate 15

E. access-group

ANSWER: A B

Explanation:

On Cisco ASA, NetFlow Secure Event Logging (NSEL) export is implemented through Modular Policy Framework (MPF). To create a flow-export action, you must define the event(s) that will generate NSEL records and then attach that action to traffic via a policy. The *flow-export event-type* command is required because it specifies which NSEL event types (for example, flow-create, flow-teardown, flow-denied, etc.) will be exported; without selecting an event type, there is no trigger for exporting records. The *policy-map* command is also required because the flow-export action is configured under a policy map (typically within a class-map match), and that policy is later applied with a service-policy to activate the behavior. Together, these are the essential building blocks for defining the export action and associating it with traffic processing on the ASA. Other items like ACLs may be used to match traffic classes, and template timeout tuning may be recommended, but they are not strictly required to define the flow-export action itself. References: Cisco ASA configuration guides (NSEL/NetFlow sections), Cisco ASA NetFlow Secure Event Logging (NSEL) overview and configuration (support doc).

QUESTION NO: 64

Which two key and block sizes are valid for AES? (Choose two.)

A. 64-bit block size, 112-bit key length

B. 64-bit block size, 168-bit key length

C. 128-bit block size, 192-bit key length

D. 128-bit block size, 256-bit key length

E. 192-bit block size, 256-bit key length

ANSWER: C D

Explanation:

AES (Advanced Encryption Standard), standardized by NIST as FIPS 197, is a symmetric block cipher with a fixed block size of 128 bits. Unlike older ciphers such as DES/3DES that use 64-bit blocks, AES does not support any block size other than 128 bits. AES supports three standardized key lengths: 128 bits, 192 bits, and 256 bits. Therefore, valid AES “key and block size” pairings must always include a 128-bit block size combined with one of the supported key lengths.

From the available choices, the combinations that match the AES standard are the 128-bit block size with a 192-bit key length and the 128-bit block size with a 256-bit key length. These correspond to AES-192 and AES-256, respectively, and are widely used in Cisco security technologies (for example, in IPsec/IKE and TLS cipher suites) where AES is negotiated with one of these key sizes while retaining the fixed 128-bit block size.

References: NIST FIPS 197 (AES), NIST Block Ciphers overview.

QUESTION NO: 65

Which type of attack is MFA an effective deterrent for?

A. ping of death

B. phishing

C. teardrop

D. syn flood

ANSWER: B

Explanation:

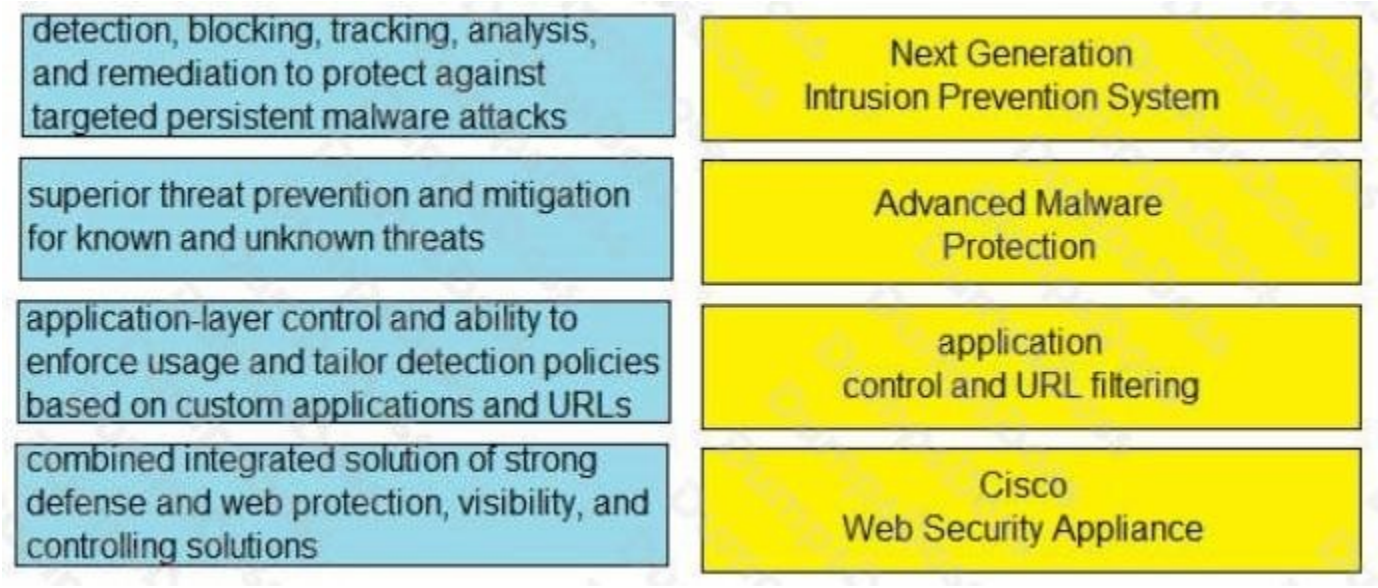
phishing is the best answer because multi-factor authentication (MFA) is specifically designed to reduce the impact of stolen credentials, which are commonly obtained through phishing. In a typical phishing attack, an attacker tricks a user into entering a username and password on a fake login page. If the attacker only gains the password, MFA can prevent account takeover by requiring an additional factor (such as a push approval, TOTP code, or hardware security key) that the attacker does not possess. While MFA is not a complete solution against advanced real-time phishing (for example, adversary-in-the-middle proxying that relays MFA prompts), it is still widely recognized as an effective deterrent and mitigation against the most common credential-phishing scenarios and password reuse attacks. In contrast, network-layer denial-of-service or malformed-packet attacks are not addressed by MFA because they do not rely on interactive user authentication. Cisco security best practices commonly position MFA as a core control for strengthening identity and access management and reducing successful credential-based intrusions. References: https://www.cisa.gov/resources-tools/resources/implementing-phishing-resistant-mfa, https://www.nist.gov/itl/tig/projects/special-publication-800-63

QUESTION NO: 66 - (DRAG DROP)

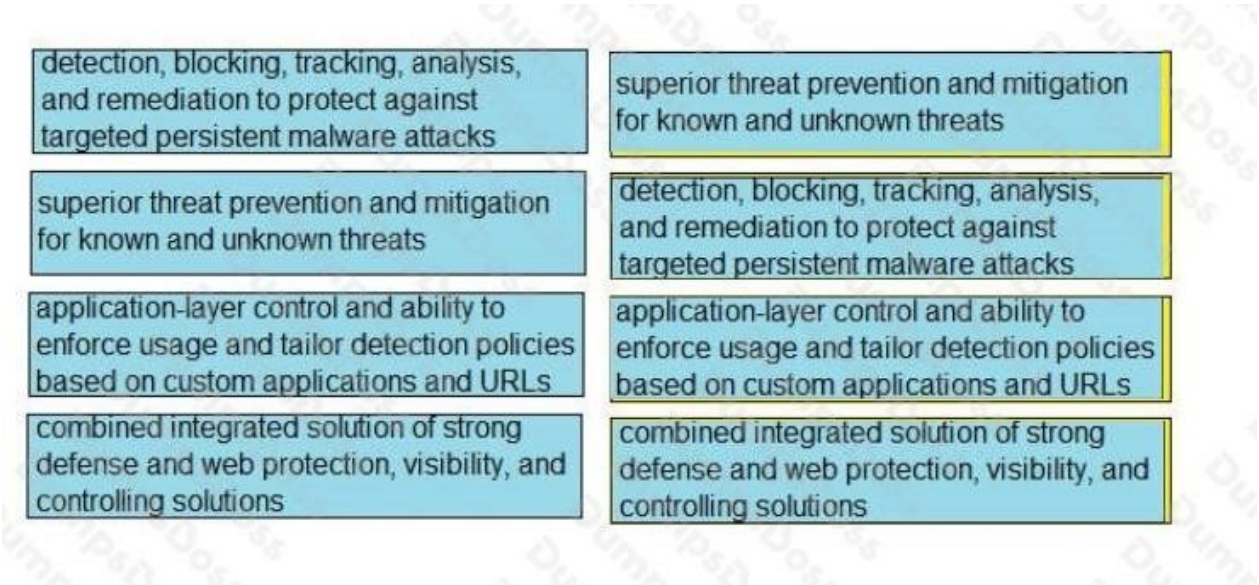
DRAG DROP

Drag and drop the capabilities from the left onto the correct technologies on the right.

Select and Place:



ANSWER:



Explanation:

The correct matching is based on what each Cisco security technology is designed to do in an enterprise security architecture. A Next Generation Intrusion Prevention System focuses on identifying and stopping exploits and network-based attacks by using signatures, reputation, and contextual awareness, which aligns with “superior threat prevention and mitigation for known and unknown threats.” This is the core promise of NGIPS platforms: prevent intrusions by detecting malicious activity and blocking it inline. Cisco’s NGIPS capabilities are described as providing advanced threat protection and intrusion prevention at the network level (Cisco NGIPS).

Advanced Malware Protection is centered on malware-centric controls such as continuous file analysis, retrospective security, and the ability to track a file’s trajectory and remediate after detection. That directly matches “detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks,” which is the classic AMP value proposition (file disposition, sandboxing/analysis, and post-compromise response). Cisco’s AMP/secure malware analytics messaging emphasizes detection plus ongoing analysis and remediation workflows (Cisco Advanced Malware Protection).

"Application control and URL filtering" is explicitly about controlling application-layer usage and web destinations, including creating policies based on specific applications and URLs. That maps cleanly to "application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs," which describes application visibility/control and URL category/policy enforcement commonly implemented on Cisco security platforms (Cisco Secure Firewall (application visibility/control)).

Finally, Cisco Web Security Appliance is a web proxy/security gateway designed to provide integrated web protection, visibility into user web activity, and centralized control over web access. That aligns with "combined integrated solution of strong defense and web protection, visibility, and controlling solutions," which is the typical description of a secure web gateway's role (Cisco Web Security Appliance).

QUESTION NO: 67

What is the result of the ACME-Router(config)#login block-for 100 attempts 4 within 60 command on a Cisco IOS router?

A. If four log in attempts fail in 100 seconds, wait for 60 seconds to next log in prompt.

B. After four unsuccessful log in attempts, the line is blocked for 100 seconds and only permit IP addresses are permitted in ACL

C. After four unsuccessful log in attempts, the line is blocked for 60 seconds and only permit IP addresses are permitted in ACL1

D. If four failures occur in 60 seconds, the router goes to quiet mode for 100 seconds.

ANSWER: D

Explanation:

The command `login block-for 100 attempts 4 within 60` enables Cisco IOS login enhancements that protect against brute-force login attacks by placing the device into "quiet mode" when too many failed login attempts occur in a defined time window. Specifically, it tracks failed login attempts and, if the router sees four failed login attempts within 60 seconds, it triggers quiet mode for 100 seconds. During quiet mode, the router blocks further login attempts (for example, on VTY lines) except from sources explicitly allowed via a configured quiet-mode access list (using `login quiet-mode access-class`). This mechanism is designed to slow down password-guessing attempts and reduce exposure during an active attack while still allowing administrative access from trusted management networks if configured. The key elements are the threshold (four failures), the observation window (within 60 seconds), and the lockout duration (block-for 100 seconds). For details, see Cisco IOS Security Command Reference for login enhancements and quiet mode behavior: Cisco IOS Login Enhancements and Cisco guidance on login block-for/quiet mode.

QUESTION NO: 68

Which feature does the IaaS model provide?

A. granular control of data

B. dedicated, restricted workstations

C. automatic updates and patching of software

D. software-defined network segmentation

ANSWER: D

Explanation:

In the Infrastructure as a Service (IaaS) model, the cloud provider delivers the underlying infrastructure components—compute (VMs), storage, and networking—while the customer is responsible for managing the operating system, middleware, and applications running on top of that infrastructure. A key feature associated with IaaS is the ability to build and control networking constructs in a software-defined way, such as virtual networks, subnets, routing, security groups/ACLs, and segmentation between workloads. This aligns with the idea of "software-defined network segmentation," where segmentation is implemented using virtualized networking controls rather than physical network changes.

This is distinct from Platform as a Service (PaaS) and Software as a Service (SaaS), where the provider typically takes on more responsibility for patching and updating the platform or application stack. In IaaS, automatic updates and patching of software are not inherently provided as a core feature because the customer generally controls and maintains the guest OS and installed software. Therefore, the most accurate feature to associate with IaaS in this question is the capability to implement segmentation using software-defined networking constructs exposed by the cloud provider.

References: NIST SP 800-145 (Definition of Cloud Computing), AWS – Types of Cloud Computing (IaaS/PaaS/SaaS)

QUESTION NO: 69

Which two Cisco ISE components must be configured for BYOD? (Choose two.)

A. local WebAuth

B. central WebAuth

C. null WebAuth

D. guest

E. dual

ANSWER: B D

Explanation:

For Cisco ISE BYOD, you must configure the web-based onboarding flow that redirects endpoints to ISE so users can authenticate and complete device registration/provisioning. This relies on Central Web Authentication (CWA), where the network access device (for example, WLC or switch) performs the initial interception/redirect and ISE hosts the portal and completes the authentication/authorization exchange. CWA is the standard mechanism used by ISE for both guest and BYOD portals because it provides a consistent redirect and portal experience across wired and wireless deployments and integrates cleanly with ISE authorization policies.

In addition, the Guest services component in ISE is required because BYOD onboarding uses ISE portals and workflows that are built on the ISE Guest/BYOD portal framework (even when the use case is employee BYOD rather than visitor guest access). Enabling and configuring Guest/BYOD portals (including the BYOD portal, certificate provisioning, and related policy sets) is a prerequisite to deliver the BYOD onboarding experience.

References: Cisco Identity Services Engine Configuration Guides, Cisco ISE Technical Documentation

QUESTION NO: 70

How does a cloud access security broker function?

A. It is an authentication broker to enable single sign-on and multi-factor authentication for a cloud solution

B. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution

C. It acts as a security information and event management solution and receives syslog from other cloud solutions.

D. It scans other cloud solutions being used within the network and identifies vulnerabilities

ANSWER: B

Explanation:

A cloud access security broker (CASB) functions as a security control point between cloud service consumers and cloud service providers, enforcing an organization's security policies as users access cloud applications. A core way many CASBs operate is through API-based integrations with SaaS providers (for example, Microsoft 365, Google Workspace, Salesforce). With API access, the CASB can continuously inspect cloud activity and data at rest, detect risky behavior (such as anomalous logins, mass downloads, or suspicious sharing), apply governance controls (like quarantining content or revoking sharing links), and generate alerts/incidents based on events observed in the cloud service. This aligns directly with the idea that it "integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution." CASBs may also support other deployment modes (like forward/reverse proxy) for inline control, but API integration is a fundamental and widely used CASB function for visibility and policy enforcement in SaaS environments. For additional background, see Cisco's overview of CASB concepts and capabilities and the Cloud Security Alliance's CASB guidance: https://www.cisco.com/c/en/us/products/security/what-is-a-casb.html and https://cloudsecurityalliance.org/artifacts/what-is-a-casb/.

QUESTION NO: 71

What are two functionalities of SDN Northbound APIs? (Choose two.)

A. Northbound APIs provide a programmable interface for applications to dynamically configure the network.

B. Northbound APIs form the interface between the SDN controller and business applications.

C. OpenFlow is a standardized northbound API protocol.

D. Northbound APIs use the NETCONF protocol to communicate with applications.

E. Northbound APIs form the interface between the SDN controller and the network switches or routers.

ANSWER: A B

Explanation:

SDN northbound APIs are the controller-facing interfaces exposed upward to software consumers, enabling applications and higher-level systems to interact with the SDN controller. A key functionality is providing a programmable interface so applications can request network services and drive policy/intent, which the controller then translates into network behavior. This is how orchestration platforms, automation tools, and custom apps can dynamically influence connectivity, segmentation, QoS, and security policies without directly configuring each device. Another core functionality is serving as the integration point between the SDN controller and business/IT applications (for example, ITSM, orchestration, or analytics systems), allowing those systems to query topology/state and push desired outcomes via APIs (commonly RESTful APIs, though implementations vary). These northbound capabilities are distinct from southbound interfaces, which connect the

controller to network devices using device/control protocols. For additional context on SDN architecture and the role of northbound APIs, see Open Networking Foundation SDN definition and Cisco's overview of SDN concepts at Cisco Software-Defined Networking overview.

QUESTION NO: 72

What are two functions of IKEv1 but not IKEv2? (Choose two)

B. With IKEv1, when using aggressive mode, the initiator and responder identities are passed cleartext

C. With IKEv1, mode negotiates faster than main mode

D. IKEv1 uses EAP authentication

E. IKEv1 conversations are initiated by the IKE_SA_INIT message

ANSWER: B C

Explanation:

In IKEv1, Phase 1 can be negotiated using two distinct exchange types: main mode and aggressive mode. This "two-mode" Phase 1 behavior is specific to IKEv1; IKEv2 replaces it with a single, standardized initial exchange (IKE_SA_INIT followed by IKE_AUTH) rather than offering separate main/aggressive modes. A key characteristic of IKEv1 aggressive mode is that peer identities can be sent without identity protection during the exchange, meaning the initiator and responder identities may be exposed in cleartext on the wire. This is a well-known tradeoff of aggressive mode: it reduces the number of messages and completes faster than main mode, but at the cost of weaker identity protection. Therefore, the statements about aggressive mode passing identities in cleartext and aggressive mode negotiating faster than main mode describe IKEv1-specific behaviors that do not exist as "functions/modes" in IKEv2. For additional detail on IKEv1 main/aggressive mode behavior and IKEv2 exchange structure, see Cisco IPsec/IKE documentation and an overview of IKEv2 exchanges at RFC 7296 (IKEv2).

QUESTION NO: 73

Why is it important to patch endpoints consistently?

A. Patching reduces the attack surface of the infrastructure.

B. Patching helps to mitigate vulnerabilities.

C. Patching is required per the vendor contract.

D. Patching allows for creating a honeypot.

ANSWER: B

Explanation:

Patching helps to mitigate vulnerabilities because software flaws are routinely discovered in operating systems and applications, and attackers quickly weaponize public disclosures into reliable exploits. Consistent patching ensures endpoints receive security fixes in a predictable, repeatable way, reducing the window of exposure between vulnerability

disclosure and remediation. In enterprise security operations, this is foundational to vulnerability management: you identify weaknesses, prioritize risk, and then remediate—most commonly by applying vendor patches that correct the underlying defect. When patching is inconsistent, you end up with “weakest-link” endpoints that can be compromised and then used for lateral movement, credential theft, or persistence, even if most of the fleet is up to date. Consistency also supports measurable compliance and operational hygiene (for example, being able to prove patch levels and reduce variance across endpoint baselines), which improves incident response and reduces the likelihood that known, preventable vulnerabilities are the root cause of a breach. Cisco security best practices align with this approach by emphasizing timely remediation of known vulnerabilities as a core control in endpoint and infrastructure hardening.

References: https://www.cisa.gov/known-exploited-vulnerabilities-catalog, https://www.cisco.com/c/en/us/products/security/what-is-vulnerability-management.html

QUESTION NO: 74

A network administrator is configuring a rule in an access control policy to block certain URLs and selects the “Chat and Instant Messaging” category. Which reputation score should be selected to accomplish this goal?

A. 5

B. 10

C. 3

D. 1

ANSWER: B

Explanation:

In Cisco Secure Firewall (FTD) URL filtering, each URL can have both a category (such as “Chat and Instant Messaging”) and a reputation score. The reputation score is a risk indicator used to decide how aggressively to control access: lower scores represent more trustworthy sites, while higher scores represent more suspicious or potentially harmful sites. To block “certain URLs” within a selected category using reputation, you choose a threshold that targets the worst reputations. Selecting reputation score 1 would represent the most trustworthy content and would not align with the intent of blocking risky destinations. Instead, you would select the highest reputation score available so the rule matches and blocks the most suspicious URLs in that category. In the Cisco URL reputation model used by Secure Firewall, the highest score is 10, which corresponds to the poorest reputation and therefore is the appropriate selection when the goal is to block URLs based on reputation within a category.

References: Cisco Secure Firewall Threat Defense URL Filtering Configuration, Cisco Firepower/FTD URL Filtering Overview

QUESTION NO: 75

An engineer wants to automatically assign endpoints that have a specific OUI into a new endpoint group. Which probe must be enabled for this type of profiling to work?

A. SNMP

B. NMAP

C. DHCP

D. NetFlow

ANSWER: C

Explanation:

For profiling based on a specific OUI (Organizationally Unique Identifier), the key requirement is that Cisco ISE must learn the endpoint's MAC address. The OUI is simply the first 24 bits of the MAC address, so any data source that reliably provides the client MAC to ISE can be used to classify endpoints and then apply an Endpoint Identity Group assignment rule (for example, matching the MAC address prefix). Enabling the DHCP probe is a common and supported way to do this because ISE can passively listen to DHCP traffic and extract the client hardware address (MAC) from DHCP messages, then use that attribute for profiling and group assignment.

This is distinct from NMAP, which is used for active scanning and OS/service discovery, not for deriving OUI-based identity from the MAC prefix. With DHCP probe enabled, ISE can build/refresh endpoint attributes automatically as endpoints obtain leases, making it practical to dynamically place devices into a new endpoint group based on their OUI.

References: Cisco Identity Services Engine (ISE) Install and Configure Guides, Cisco ISE Admin Guide – Profiling

QUESTION NO: 76

Which two parameters are used for device compliance checks? (Choose two.)

A. endpoint protection software version

B. Windows registry values

C. DHCP snooping checks

D. DNS integrity checks

E. device operating system version

ANSWER: A E

Explanation:

In Cisco identity and access control designs (such as Cisco ISE posture/compliance), "device compliance checks" focus on endpoint posture attributes that can be measured on the device itself and compared to policy. Common posture conditions include verifying the device operating system version (for example, ensuring a minimum Windows/macOS build level or that a mobile OS is not jailbroken/rooted) and validating endpoint protection status, including the endpoint protection software version, to ensure the required security agent is installed and up to date. These parameters are directly tied to endpoint risk and are typical inputs to posture policies that determine whether an endpoint is compliant, noncompliant, or unknown, and then apply network access controls accordingly (for example, full access vs. quarantine/remediation). This aligns with Cisco ISE posture's use of posture agents and conditions to assess antivirus/anti-malware presence and versioning as well as OS characteristics as part of compliance decisions.

References: Cisco Identity Services Engine (ISE) product page, Cisco ISE Installation and Configuration Guides

QUESTION NO: 77

Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware? (Choose two.)

A. Sophos engine

B. white list

C. RAT

D. outbreak filters

E. DLP

ANSWER: A D

Explanation:

Cisco Email Security Appliance (ESA) uses a layered anti-malware design that combines signature-based scanning with behavior/epidemic-style detection to reduce both known and emerging threats. The Sophos engine is one of the supported anti-virus scanning engines on ESA and provides traditional malware detection using signatures and heuristics, forming a core layer of protection for inbound and outbound mail. Outbreak filters add another layer by detecting and controlling new or rapidly spreading malware outbreaks before traditional signatures are available, using Cisco Talos intelligence and outbreak rules to quarantine, drop, or modify messages that match outbreak characteristics. Using both together is a classic "multilayer" approach: one layer focuses on known malware via AV scanning, while the other focuses on zero-day/fast-moving campaigns via outbreak intelligence and policy actions. This combination is specifically aligned to ESA's anti-malware strategy and is commonly referenced in Cisco guidance for configuring comprehensive email threat defense.

References: Cisco Email Security Appliance (product overview), Cisco ESA configuration guides (support)

QUESTION NO: 78

Which attack is preventable by Cisco ESA but not by the Cisco WSA?

A. buffer overflow

B. DoS

C. SQL injection

D. phishing

ANSWER: D

Explanation:

phishing
is the correct answer because Cisco Email Security Appliance (ESA) is purpose-built to inspect and control email-borne threats, including phishing and business email compromise techniques that arrive via SMTP and are delivered to user mailboxes. ESA provides anti-spam/anti-phishing engines, URL and attachment reputation, and advanced phishing protections (for example, detecting display-name spoofing, lookalike domains, and other social-engineering patterns in email headers and content). In contrast, Cisco Web Security Appliance (WSA) primarily protects web browsing traffic (HTTP/HTTPS) by enforcing acceptable use, blocking malicious sites, and scanning downloads; it is not an email gateway and does not sit inline for inbound/outbound SMTP to prevent phishing emails from being delivered. While WSA can reduce

user exposure to phishing websites when users click links, the question asks which attack is preventable by ESA but not by WSA—email phishing is the canonical case where ESA provides direct prevention at the email layer.

References: Cisco Secure Email (Email Security) overview, Cisco ESA Advanced Phishing Protection documentation