PassQueen
a.k.a dumpsqueen.com

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

Cisco 350-701

Version Demo

Total Demo Questions: 95

Total Premium Questions: 955

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security Concepts	119
Topic 2, Network Security	193
Topic 3, Securing the Cloud	124
Topic 4, Content Security	149
Topic 5, Endpoint Protection and Detection	96
Topic 6, Secure Network Access, Visibility, and Enforcement	271
Topic 7, Mix Questions	3
Total	955

QUESTION NO: 1

Which two Cisco Secure Client modules can help enforce endpoint compliance and provide endpoint network telemetry? (Choose two.)

A. ISE Posture

B. Network Visibility Module

C. Diagnostics and Reporting Tool

D. VPN module

E. Start Before Logon

ANSWER: A B

Explanation:

ISE Posture is correct because the Cisco Secure Client ISE Posture module communicates with Cisco ISE to assess endpoint compliance. The module can evaluate requirements such as antivirus state, operating-system updates, disk encryption, and required endpoint software. Cisco ISE can use the result to assign restricted access, direct a user to remediation, or authorize normal network access.

Network Visibility Module is also correct because it collects endpoint network-flow telemetry. The module records flow-related information that can provide visibility into endpoint communications and can be exported to supported analytics platforms. This helps security teams investigate endpoint activity and identify suspicious connections without relying solely on perimeter telemetry.

The VPN module establishes remote-access VPN connectivity, while the Diagnostics and Reporting Tool is primarily used to collect diagnostic information. See the Cisco Secure Client Administrator Guide.

QUESTION NO: 2

A company has 5000 Windows users on its campus. Which two precautions should IT take to prevent WannaCry ransomware from spreading to all clients? (Choose two.)

A. Segment different departments to different IP blocks and enable Dynamic ARp inspection on all VLANs

B. Ensure that noncompliant endpoints are segmented off to contain any potential damage.

C. Ensure that a user cannot enter the network of another department.

D. Perform a posture check to allow only network access to those Windows devices that are already patched.

E. Put all company users in the trusted segment of NGFW and put all servers to the DMZ segment of the Cisco NGFW. ni

ANSWER: B D

Explanation:

“Ensure that noncompliant endpoints are segmented off to contain any potential damage.” is an effective containment control for a wormable threat such as WannaCry. WannaCry spread laterally by exploiting the Microsoft SMB vulnerability addressed in MS17-010. Isolating endpoints that do not meet required security conditions restricts their ability to communicate with other internal hosts, reducing the potential blast radius if an endpoint is vulnerable or already infected. Cisco Identity Services Engine can apply endpoint compliance and network-access policies, including restricted or remediation access, to support this type of segmentation.

“Perform a posture check to allow only network access to those Windows devices that are already patched.” addresses the underlying exposure before a device receives normal campus access. Posture assessment can validate that required operating-system updates and endpoint-security conditions are present. Devices missing critical updates can be redirected to remediation resources or limited to restricted connectivity until they comply. Combining patch-based admission control with isolation of noncompliant devices prevents vulnerable systems from freely reaching peers over SMB and limits

propagation opportunities across a large Windows environment. Microsoft's MS17-010 bulletin is available at Microsoft Security Bulletin MS17-010; Cisco ISE product and posture capabilities are described at Cisco Identity Services Engine.

QUESTION NO: 3

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:

Sophos engine and **outbreak filters** provide complementary layers of malware protection on Cisco Email Security Appliance. The Sophos anti-virus engine is an anti-malware scanning layer that examines email messages and attachments for malicious content. It applies anti-virus detection technologies to identify known malware and suspicious file content before messages are delivered or leave the organization. This scanning capability is a fundamental component of ESA's email malware defenses.

Outbreak filters provide an additional intelligence-driven layer for rapidly emerging email threats. They use Cisco threat intelligence and rules designed to identify characteristics associated with active malware, phishing, and spam outbreaks, including campaigns that may begin spreading before conventional anti-virus detections are broadly available. Administrators can configure actions such as quarantining, dropping, or modifying messages that match an outbreak-filter rule. Combining anti-virus scanning with outbreak filtering gives ESA both content-level malware inspection and campaign/outbreak-based protection, which is the intended multilayer strategy for defending email traffic against viruses and malware. Cisco documents ESA as providing layered email threat protection and describes anti-malware and outbreak-filter capabilities in its product and configuration documentation.

References: Cisco Email Security Appliance; Cisco ESA installation and configuration guides.

QUESTION NO: 4

Which command is used to log all events to a destination colector 209.165.201.107?

A. CiscoASA(config-pmap-c)#flow-export event-type flow-update destination 209.165.201.10

B. CiscoASA(config-cmap)# flow-export event-type all destination 209.165.201.

C. CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.10

D. CiscoASA(config-cmap)#flow-export event-type flow-update destination 209.165.201.10

E. CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.107

ANSWER: E

Explanation:

`CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.107` is the correct command because Cisco ASA NetFlow Secure Event Logging (NSEL) is configured through the Modular Policy Framework within policy-map class configuration mode, indicated by the `config-pmap-c` prompt. The `flow-export` action defines the NSEL records that the ASA exports to a collector. Using `event-type all` instructs the appliance to export every

supported NSEL event category, rather than limiting export to a particular event such as flow updates. The `destination` parameter then identifies the receiving collector, and it must exactly match the specified address, `209.165.201.107`. This command therefore satisfies both requirements at once: exporting all events and sending them to the requested collector host. NSEL provides event-based flow information that can be consumed by a NetFlow/NSEL-capable collector for monitoring and security analysis. Cisco documents the `flow-export event-type all destination` syntax as an MPF policy-map class action for configuring NSEL export. See the Cisco ASA flow-export command reference and Cisco ASA NSEL configuration guide.

QUESTION NO: 5

Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?

A. quality of service

B. time synchronization

C. network address translations

D. intrusion policy

ANSWER: B

Explanation:

time synchronization is configured through a Platform Settings policy in Cisco Firepower Management Center. Platform Settings policies centrally define device-level operational and management-plane settings for managed Firepower Threat Defense devices, rather than traffic-handling rules or inspection policies. The time synchronization section enables the administrator to configure Network Time Protocol settings, including NTP server information, so the FMC can deploy consistent time settings to one or more managed devices.

Accurate and consistent time is fundamental to security operations. It ensures that connection events, intrusion events, malware events, audit records, and system logs have reliable timestamps. Consistent clocks also improve event correlation across multiple devices and external log-management systems, support certificate-validity checks, and make incident investigation and troubleshooting more dependable. Applying these settings through a reusable Platform Settings policy provides centralized administration and consistent deployment across the selected managed devices.

Cisco documents time synchronization as a configurable setting in Platform Settings policies for managed devices. See the Cisco Secure Firewall Management Center Platform Settings documentation and the Cisco Secure Firewall Management Center Device Configuration Guide.

QUESTION NO: 6

A Cisco FirePower administrator needs to configure a rule to allow a new application that has never been seen on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose two.)

A. permit

B. allow

C. reset

D. trust

E. monitor

F. fastpath

ANSWER: D F

Explanation:

The correct actions are **trust** and **fastpath**. Both are access-control actions designed to permit matching traffic while bypassing normal deep inspection, which is appropriate when the administrator explicitly needs a flow to pass without being evaluated by the Snort inspection engine. The **trust** action permits the traffic and exempts it from further access-control inspection. It is suitable for traffic that has been identified as trusted and does not require security-policy evaluation. The **fastpath** action also permits matching traffic without inspection, processing the traffic as efficiently as possible and avoiding the overhead associated with detailed inspection. This can be particularly useful where an application is new or cannot yet be reliably identified by application detection, but business requirements require that its sessions be passed immediately. In both cases, the rule should be scoped as narrowly as practical, using available network, host, port, or zone criteria, because bypassing inspection means that intrusion, file, malware, and application-control evaluation is not applied to the matching traffic. Cisco documents Trust and Fastpath as access-control rule actions that allow traffic without further inspection. See the Cisco Secure Firewall Management Center access-control rules documentation and the Cisco prefilter and Fastpath documentation.

QUESTION NO: 7

What are two list types within Cisco AMP for Endpoints Outbreak Control? (Choose two.)

A. blocked ports

B. simple custom detections

C. command and control

D. allowed applications

E. URL

ANSWER: B D

Explanation:

Within Cisco AMP for Endpoints, now Cisco Secure Endpoint, Outbreak Control provides centrally managed controls that security teams can use to react quickly to newly identified threats across deployed endpoint connectors. **simple custom detections** are an Outbreak Control list type intended for rapid creation and deployment of targeted file detections. Administrators can use these detections to identify or block a known malicious artifact using available file-identification criteria, helping contain an outbreak while investigation and longer-term policy decisions continue.

allowed applications are also an Outbreak Control list type. This list establishes known, trusted applications that should be permitted, including when broader outbreak-response controls could otherwise affect them. Maintaining an allow list helps organizations apply urgent protections without unnecessarily interrupting approved business software. Together, simple custom detections and allowed applications support the operational goal of Outbreak Control: quickly enforcing focused containment while preserving the execution of explicitly trusted applications. Cisco identifies Secure Endpoint as the current name for AMP for Endpoints and provides product and support documentation through its Secure Endpoint resources: Cisco Secure Endpoint product page and Cisco Secure Endpoint support documentation.

QUESTION NO: 8

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 helps defend against business email compromise and identity-based phishing, attacks that commonly rely on impersonating a trusted executive, employee, supplier, or business partner. It analyzes sender identity and communication context, including relationships and normal interaction patterns, to identify suspicious anomalies such as display-name impersonation, lookalike domains, and unusual requests. This capability helps prevent use of compromised accounts and social engineering by identifying deceptive messages before a recipient acts on a fraudulent payment, credential request, or other manipulation attempt.

The solution also supports post-delivery protection. Email threat intelligence and analysis can change after a message has reached a mailbox; therefore, remediation capabilities are important for limiting user exposure. When a message is subsequently determined to be malicious, automated remediation can remove malicious emails from users' inboxes. This reduces the time that phishing content remains available to users and helps contain campaigns as additional evidence is discovered. These protections combine contextual identity analysis with mailbox remediation to address both initial delivery and threats identified after delivery. Cisco describes phishing and business-email-compromise protections within its Secure Email portfolio at Cisco Secure Email and documents phishing-defense capabilities at Cisco Email Security.

QUESTION NO: 9

```
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:

The `crypto key generate rsa` command creates an RSA public/private key pair locally on the Cisco IOS router. SSH requires this asymmetric RSA key material so that the router can authenticate itself as the SSH server and establish protected management sessions. The key pair is retained in the device configuration/key storage and is subsequently available to the SSH process.

Including the `label` keyword assigns the specified name to the generated RSA key pair. A label is useful when a device has, or may later have, multiple RSA key pairs because it provides an explicit identifier for the pair intended for a particular use, such as SSH. The configured domain name is a normal prerequisite for IOS SSH key generation when no explicit key label is used; IOS can derive a default key name from the device identity. Here, the explicit label names the RSA key pair while the RSA-generation command performs the actual key creation.

Cisco documents RSA key generation as a required SSH server configuration step and documents the optional `label` parameter for naming generated RSA keys. See Cisco Secure Shell Configuration Example and Cisco IOS XE Secure Shell Configuration Guide.

QUESTION NO: 10

A network administrator is setting up Cisco FMC to send logs to Cisco Security Analytics and Logging (SaaS). The network administrator is anticipating a high volume of logging events from the firewalls and wants lo limit the strain on firewall resources. Which method must the administrator use to send these logs to Cisco Security Analytics and Logging?

A. SFTP using the FMCCLI

B. syslog using the Secure Event Connector

C. direct connection using SNMP traps

D. HTTP POST using the Security Analytics FMC plugin

ANSWER: B

Explanation:

syslog using the Secure Event Connector is the required method. Cisco Security Analytics and Logging (SaaS) uses the Secure Event Connector as an on-premises intermediary between the Secure Firewall deployment and Cisco's cloud logging service. The firewall sends its event messages to the connector using syslog, and the connector securely forwards the collected telemetry to the SaaS platform. This design is particularly appropriate for a high event rate because cloud-delivery processing is handled by the dedicated connector rather than requiring each firewall to independently maintain the cloud-facing logging connection. The connector also provides a centralized ingestion point for firewall telemetry, which helps reduce operational and resource overhead on managed devices while supporting reliable delivery of security events for cloud-based storage, search, and analytics. The FMC is used to configure the firewall syslog destination and logging behavior so that relevant events are exported to the Secure Event Connector. Cisco documents Security Analytics and Logging (SaaS) as a cloud-delivered logging and analytics service for Secure Firewall environments, with the Secure Event Connector providing the supported secure connectivity component for event forwarding. See Cisco's Security Analytics and Logging overview and the Secure Firewall Management Center configuration guides.

QUESTION NO: 11

Which component of Cisco umbrella architecture increases reliability of the service?

A. Anycast IP

B. AMP Threat grid

C. Cisco Talos

D. BGP route reflector

ANSWER: A

Explanation:

Anycast IP increases the reliability of Cisco Umbrella because the same recursive DNS resolver addresses are announced from multiple geographically distributed Umbrella data centers. A client sends DNS requests to a single configured Umbrella IP address, while normal Internet routing selects an available and efficient Umbrella location advertising that address. This provides inherent resilience: if a particular data center or network path is unavailable, routing can converge on another operational location that advertises the same Anycast address. The customer does not need to reconfigure endpoint or network DNS settings during that failure condition.

In addition to availability, the distributed Anycast design generally helps direct DNS queries to a nearby or well-connected service location, which supports responsive DNS resolution at global scale. This architecture is particularly suited to a cloud-delivered DNS security service because it avoids dependence on one centralized resolver site and reduces the impact of localized outages. Cisco documents its Umbrella recursive DNS resolvers and identifies the Anycast addresses used to reach the globally distributed service. See the Cisco Umbrella DNS resolvers documentation and the Cisco Umbrella product overview.

QUESTION NO: 12

Refer to the exhibit When configuring this access control rule in Cisco FMC, what happens with the traffic destined to the DMZjnside zone once the configuration is deployed?

A. All traffic from any zone to the DMZ_inside zone will be permitted with no further inspection

B. No traffic will be allowed through to the DMZ_inside zone regardless of if it's trusted or not

C. All traffic from any zone will be allowed to the DMZ_inside zone only after inspection

D. No traffic will be allowed through to the DMZ_inside zone unless it's already trusted

ANSWER: A

Explanation:

All traffic from any zone to the DMZ_inside zone will be permitted with no further inspection. The exhibited access-control rule uses the *Trust* action and identifies DMZ_inside as the destination security zone. In Cisco Secure Firewall Management Center, a Trust rule permits matching traffic while exempting it from access-control inspection. Therefore, connections matching this rule are allowed without invoking the deeper inspection mechanisms normally associated with an Allow rule, such as intrusion inspection, file control, malware inspection, or Security Intelligence processing in the access-control path. Because the source-zone condition is set to match any zone, the rule applies to traffic arriving from any source security zone as long as its destination matches DMZ_inside and any other configured rule conditions are met. The policy processes access-control rules in order, so this behavior applies when the Trust rule is the first matching rule for the connection. The change takes effect after the access-control policy is successfully deployed to the managed Secure Firewall device. Cisco documents Trust as an action intended for traffic that should be explicitly allowed without further access-control inspection; it should consequently be used only for flows that are appropriate to exempt from those security controls. See Cisco's Access Control Rules documentation and the Secure Firewall Management Center user guides.

QUESTION NO: 13

What is the difference between EPP and EDR?

A. EPP focuses primarily on threats that have evaded front-line defenses that entered the environment.

B. Having an EPP solution allows an engineer to detect, investigate, and remediate modern threats.

C. EDR focuses solely on prevention at the perimeter.

D. Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior.

ANSWER: D

Explanation:

Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior because endpoint detection and response continuously collects endpoint telemetry and evaluates activity for suspicious behavioral indicators. Rather than relying exclusively on a known file signature, an EDR capability can correlate process execution, parent-child process relationships, command-line activity, file writes, registry or configuration changes, network connections, and persistence attempts. This visibility helps identify malicious behavior as it emerges, including activity associated with previously unknown or modified threats.

The “flag” action is an important distinction: EDR provides security teams with high-fidelity detections and investigation context, allowing them to examine the affected endpoint and take response actions such as isolating a device, terminating a malicious process, or quarantining a file. Cisco Secure Endpoint provides endpoint telemetry, detection, investigation, and response workflows intended to help analysts rapidly identify and contain endpoint threats. Cisco describes EDR as a capability that enables continuous monitoring and response using endpoint data, which directly supports detecting an offending file or process when its behavior first becomes malicious. See Cisco Secure Endpoint and Cisco: What Is Endpoint Detection and Response (EDR)?.

QUESTION NO: 14

Which parameter is required when configuring a Netflow exporter on a Cisco Router?

A. DSCP value

B. Source interface

C. Exporter name

D. Exporter description

ANSWER: C

Explanation:

Exporter name is required because Cisco Flexible NetFlow defines an exporter as a named configuration object. The configuration process begins in global configuration mode with `flow exporter <exporter-name>`; the name supplied to that command creates and identifies the exporter instance. Cisco IOS and IOS XE then enter flow-exporter configuration mode, where the administrator can configure the collector destination, source interface, transport protocol and port, DSCP marking, template settings, and other export behavior. The same name is also how a flow monitor associates itself with the exporter through the `exporter <exporter-name>` command. Thus, the exporter name is the required parameter that establishes the object and provides the reference used by the Flexible NetFlow configuration model. Cisco’s Flexible NetFlow command reference documents the named form of the `flow exporter` command and its exporter configuration submode, while the configuration guide shows exporters being created and subsequently attached to monitors by name. See the Cisco IOS Flexible NetFlow Command Reference and the Cisco IOS XE Flexible NetFlow Configuration Guide.

QUESTION NO: 15

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: C D

Explanation:

Cisco ASA and **NetFlow** are the connector types used for this IPFIX-derived telemetry use case. A NetFlow connector is designed to receive exported flow records, including the NetFlow v9/IPFIX-style, template-based records used to represent observed communications. Secure Workload uses those records to build flow telemetry that can be associated with workloads and used for application-dependency visibility and segmentation analysis. IPFIX is the IETF standard for exporting Internet Protocol flow information; its information-model and template-based export approach are defined in RFC 7011.

A Cisco ASA connector supports telemetry from Cisco ASA firewalls through NetFlow Secure Event Logging. ASA can export connection and security-event information as NetFlow Secure Event Logging records, supplying the flow-oriented data required by Secure Workload's telemetry pipeline. Cisco documents the ASA configuration and export behavior in its NetFlow Secure Event Logging configuration guide. Together, these connector types enable Secure Workload to consume flow-export telemetry from both general NetFlow/IPFIX exporters and ASA-specific security-event flow exports.

QUESTION NO: 16

Which solution should be leveraged for secure access of a CI/CD pipeline?

A. Duo Network Gateway

B. remote access client

C. SSL WebVPN

D. Cisco FTD network gateway

ANSWER: A

Explanation:

Duo Network Gateway is the appropriate solution because it provides identity-based, application-level remote access for internal resources that commonly support a CI/CD pipeline, including build servers, source-control interfaces, artifact repositories, administrative dashboards, and related web applications. Rather than granting a user broad access to an internal network, it places an access gateway in front of protected applications and requires the user to complete Duo authentication before reaching the resource. This supports a zero-trust approach in which access decisions are based on verified user identity and Duo policy controls, such as multifactor authentication and device-related checks.

CI/CD environments contain highly sensitive assets: source code, credentials, deployment controls, build outputs, and release-management interfaces. Limiting remote connectivity to the specific applications a developer or administrator needs helps enforce least privilege and reduces exposure of the wider environment. Duo Network Gateway was designed to securely publish internal web applications and selected internal services without making those resources directly reachable from the internet. This makes it well suited to protecting access paths used to operate and administer a CI/CD pipeline. Cisco describes the product's application-access architecture in the Duo Network Gateway documentation and provides broader trusted-access guidance in the Cisco Duo overview.

QUESTION NO: 17

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

A. TACACS+
Reference:
User Guide for AsyncOS 11.0 for Cisco Web Security Appliances (Acquire End-User Credentials)
Cisco WSA Authentication WSA Authentication

B. CHAP

C. NTLMSSP

D. RADIUS

E. Kerberos

ANSWER: C E

Explanation:

NTLMSSP and Kerberos are the integrated Windows authentication protocols used by Cisco Web Security Appliance (WSA) to acquire and validate end-user identities for identity-based access and web-use policies. NTLMSSP supports NTLM-based authentication, allowing the WSA to challenge clients and validate credentials through the configured Microsoft Active Directory environment. This is commonly used for transparent or explicit proxy deployments where Windows clients can respond to an NTLM challenge.

Kerberos provides ticket-based integrated authentication. With the necessary Active Directory, DNS, service principal name, and browser/client configuration in place, clients can obtain and present Kerberos service tickets to the WSA without repeatedly prompting users for credentials. This lets the appliance associate requests with authenticated directory users and apply the relevant user- and group-based policies. Cisco documents both NTLMSSP and Kerberos under the end-user credential acquisition and authentication capabilities of AsyncOS for WSA. See the Cisco Web Security Appliance user guides and Cisco WSA technical documentation.

QUESTION NO: 18

Which Cisco solution extends network visibility, threat detection, and analytics to public cloud environments?

A. Cisco Umbrella

B. Cisco Stealthwatch Cloud

C. Cisco Appdynamics

D. Cisco CloudLock

ANSWER: B

Explanation:

Cisco Stealthwatch Cloud is the correct solution because it was specifically designed to deliver network detection and response capabilities for public-cloud infrastructure. The service collects and analyzes cloud-native telemetry, such as flow-log data and cloud-provider activity, to establish behavioral baselines for workloads, users, and network communications. This visibility enables security teams to detect anomalous traffic, suspicious connections, policy violations, and potential account compromise that may otherwise be difficult to identify in dynamic cloud deployments. The product also provides investigation context and analytics that help teams understand how cloud resources are communicating and prioritize security events. Cisco later used the Secure Cloud Analytics name for this cloud-focused capability, while Stealthwatch branding is associated with Cisco's broader network-analytics portfolio. Therefore, Cisco Stealthwatch Cloud directly matches the requirement to extend network visibility, threat detection, and analytics into public-cloud environments. Cisco's Secure Network Analytics information provides context for the broader network-visibility platform at Cisco Secure Network Analytics. Cisco's cloud-security portfolio information is available at Cisco Cloud Security.

QUESTION NO: 19

A malicious user gained network access by spoofing printer connections that were authorized using MAB on

four different switch ports at the same time. What two catalyst switch security features will prevent further

violations? (Choose two)

A. DHCP Snooping

B. 802.1AE MacSec

C. Port security

D. IP Device track

E. Dynamic ARP inspection

F. Private VLANs

ANSWER: B C

Explanation:

802.1AE MacSec and **Port security** provide complementary protections in this situation. MAC Authentication Bypass authorizes a device based on its presented MAC address, so a copied printer address can be used to impersonate that printer unless an additional control establishes cryptographic trust. IEEE 802.1AE MACsec protects Ethernet traffic with integrity validation and optional confidentiality between MACsec peers. MACsec uses the MACsec Key Agreement protocol to establish secure connectivity association keys, so merely presenting a printer's MAC address does not provide the cryptographic material needed to participate as an authenticated peer. Cisco describes MACsec as providing Layer 2 data confidentiality, integrity, and origin authentication.

Port security limits the MAC addresses permitted on a physical switch interface. It can be configured with a small maximum secure-MAC count and with static or sticky secure MAC-address bindings, allowing each printer-facing interface to be restricted to its expected endpoint. A violation action such as restrict or shutdown then stops unauthorized MAC-address activity and generates operational visibility. Together, cryptographic Layer 2 protection and per-port MAC admission enforcement address repeated attempts to exploit MAB-authorized printer identities. See Cisco's MACsec configuration guide and Port Security configuration guide.

QUESTION NO: 20

A network administrator is using the Cisco ESA with AMP to upload files to the cloud for analysis. The network

is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?

A. AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.

B. The file is queued for upload when connectivity is restored.

C. The file upload is abandoned.

D. The ESA immediately makes another attempt to upload the file.

ANSWER: C

Explanation:

The file upload is abandoned. Cisco ESA file analysis submits eligible attachments to Cisco's cloud analysis service, but it does not maintain a persistent local upload queue for failures caused by communication or connectivity conditions. Therefore, when network congestion prevents the appliance from successfully uploading a file for analysis, that particular submission is not retained and retried later merely because connectivity improves. The message-processing path can continue according to the configured file-analysis and mail-policy behavior, but cloud analysis for that failed upload is unavailable.

This behavior is important operationally: reliable connectivity between the Secure Email Gateway and the cloud-analysis infrastructure is required if administrators expect consistent analysis coverage. Cisco documents file analysis as a cloud-based capability of Secure Email Gateway/AMP and describes the appliance's interaction with the analysis service, including submission behavior and result handling. Administrators should monitor network reachability, DNS resolution, firewall policy, and available bandwidth to minimize upload failures during periods of congestion. See Cisco's Secure Email Gateway Administration Guide: File Analysis and the Cisco Secure Email product documentation portal.

QUESTION NO: 21

What is a difference between an XSS attack and an SQL injection attack?

A. SQL injection is a hacking method used to attack SQL databases, whereas XSS attacks can exist in many different types of applications

B. XSS is a hacking method used to attack SQL databases, whereas SQL injection attacks can exist in many different types of applications

C. SQL injection attacks are used to steal information from databases whereas XSS attacks are used toredirect users to websites where attackers can steal data from them

D. XSS attacks are used to steal information from databases whereas SQL injection attacks are used toredirect users to websites where attackers can steal data from them

ANSWER: C

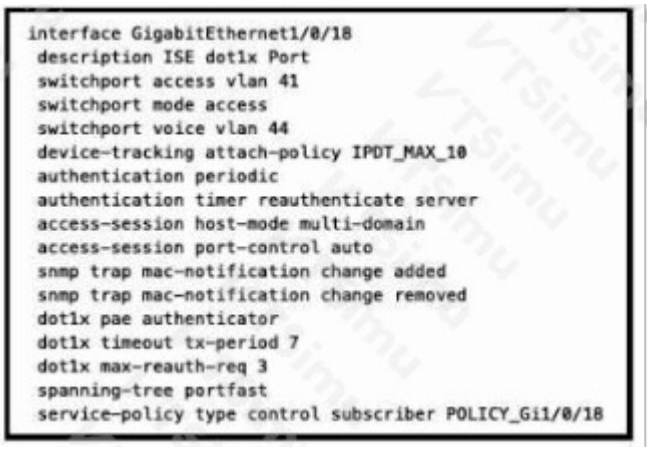
Explanation:

SQL injection attacks are used to steal information from databases whereas XSS attacks are used toredirect users to websites where attackers can steal data from them is the correct distinction in the context of these choices. SQL injection is a server-side web application vulnerability in which an attacker manipulates application input so that it changes an SQL command sent to a relational database. If the application does not safely parameterize its queries and the database permissions allow it, the attacker may retrieve sensitive records, alter data, or bypass application controls. The key target is therefore the application's database-query processing and the data held by that database.

Cross-site scripting (XSS) instead causes attacker-supplied client-side script to be interpreted by a victim's browser in the security context of a trusted site. The script can steal session identifiers or tokens, act as the victim within the application, display deceptive content, or redirect the victim to an attacker-controlled destination where further data theft can occur. Thus, the meaningful difference is the primary target and execution context: SQL injection manipulates backend database operations, while XSS executes in users' browsers. OWASP describes the respective attack classes at OWASP SQL Injection and OWASP Cross Site Scripting.

QUESTION NO: 22

Refer to the exhibit.



```
interface GigabitEthernet1/0/18
 description ISE dot1x Port
 switchport access vlan 41
 switchport mode access
 switchport voice vlan 44
 device-tracking attach-policy IPDT_MAX_10
 authentication periodic
 authentication timer reauthenticate server
 access-session host-mode multi-domain
 access-session port-control auto
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 spanning-tree portfast
 service-policy type control subscriber POLICY_Gi1/0/18
```

What will occur when this device tries to connect to the port?

A. 802.1X will not work, but MAB will start and allow the device on the network.

B. 802.1X will not work and the device will not be allowed network access

C. 802 1X will work and the device will be allowed on the network

D. 802 1X and MAB will both be used and ISE can use policy to determine the access level

ANSWER: B

Explanation:

802.1X will not work and the device will not be allowed network access is correct because the depicted endpoint does not support an 802.1X supplicant. Wired 802.1X authentication requires the endpoint, acting as the supplicant, to initiate and

participate in an EAP over LAN (EAPOL) exchange with the switch. The switch acts as the authenticator and relays the authentication exchange to Cisco ISE or another RADIUS server. Without supplicant support, the endpoint cannot provide the EAPOL communication and credentials required to complete 802.1X authentication.

On an access port using 802.1X only, successful authentication is required before the switch authorizes normal data traffic. Therefore, the port remains unauthorized for the endpoint and the device does not receive production network access. Devices such as many printers, cameras, and other headless endpoints commonly require an alternative identity method, such as MAC Authentication Bypass, when they cannot run an 802.1X supplicant. That alternative must be explicitly configured on the switchport and supported by the ISE authorization policy; it is not automatically available merely because 802.1X fails. Cisco's wired access documentation describes the distinct supplicant, authenticator, and authentication-server roles in this process. See Cisco's 802.1X wired authentication overview and Cisco's ISE MAB configuration concepts.

QUESTION NO: 23

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, the Trusted Automated eXchange of Indicator Information, is an application-layer protocol for the automated sharing of cyber threat intelligence. Its central role is to define how intelligence is exchanged between participating systems, rather than defining the intelligence's meaning or data model. Therefore, TAXII supports STIX information by providing a standardized RESTful HTTPS-based API through which systems can discover API roots, access collections, and retrieve or publish STIX objects. This allows products from different vendors to share structured intelligence such as indicators, malware details, threat actors, relationships, and sightings without requiring a proprietary integration. TAXII also determines how threat intelligence information is relayed: its specification defines client-server interactions and resources used to request, deliver, and manage threat-intelligence content. In TAXII 2.x, collections organize objects available from a server, and API endpoints provide the method by which a client obtains or adds content, subject to authorization. This clear separation is important in a threat-intelligence architecture: STIX supplies the standardized language and object model for expressing cyber-observable and adversary information, while TAXII supplies the interoperable transport mechanism that communicates it. See the OASIS TAXII introduction and the TAXII 2.1 REST API specification.

QUESTION NO: 24

Which attack is commonly associated with C and C++ programming languages?

A. cross-site scripting

B. water holing

C. DDoS

D. buffer overflow

ANSWER: D

Explanation:

Buffer overflow is commonly associated with C and C++ because these languages allow direct memory access and, particularly in traditional code, do not automatically perform bounds checking for array and buffer operations. A buffer

overflow occurs when software writes more input data to a fixed-size memory buffer than it was allocated to hold. The excess data can overwrite adjacent memory locations, potentially corrupting application state, causing a crash, or altering control-flow data such as a return address or function pointer. If an attacker can precisely control the overwritten data, the condition may permit arbitrary code execution in the security context of the vulnerable process. This risk is especially relevant when C or C++ programs use unsafe memory-handling patterns or fail to validate input lengths. Secure coding practices use explicit length validation, bounds-aware APIs, and memory-safe design patterns to prevent these flaws. Platform defenses such as stack canaries, address space layout randomization, and non-executable memory protections can make exploitation more difficult, but they do not eliminate the underlying coding weakness. MITRE classifies out-of-bounds writes as CWE-787 and describes their potential impact on integrity, availability, and code execution. See MITRE CWE-787: Out-of-bounds Write and CISA guidance on memory-management vulnerabilities.

QUESTION NO: 25

An engineer is implementing Cisco CES in an existing Microsoft Office 365 environment and must route inbound email to Cisco CE.. record must be modified to accomplish this task?

A. CNAME

B. MX

C. SPF

D. DKIM

ANSWER: B

Explanation:

MX is correct because an MX (Mail Exchanger) DNS record identifies the mail host responsible for receiving inbound email for a domain. When Cisco Cloud Email Security (CES) is deployed in front of an existing Microsoft 365 environment, the organization updates its public MX records so that external mail is delivered first to the Cisco CES cloud service. CES can then apply its inbound email-security controls, such as anti-spam, anti-malware, message and URL analysis, and policy enforcement, before relaying accepted messages to the organization's Microsoft 365 mail environment. This mail-flow design ensures inbound Internet email is inspected by Cisco CES rather than being sent directly to Microsoft 365. Cisco's Microsoft 365 integration guidance specifically directs administrators to update the domain's MX record to the Cisco Secure Email cloud-delivery hostname supplied during provisioning. MX records are published in authoritative public DNS because sending mail servers use DNS MX lookups to determine the destination for SMTP delivery. The precise MX target is tenant- and region-specific, so the value must be the one assigned in the Cisco Secure Email administration portal. See Cisco's Microsoft 365 with Secure Email configuration guidance and the SMTP DNS MX lookup requirements in RFC 5321.

QUESTION NO: 26

An administrator is configuring N I P on Cisco ASA via ASDM and needs to ensure that rogue NTP servers cannot insert themselves as the authoritative time source Which two steps must be taken to accomplish this task? (Choose two)

A. Specify the NTP version

B. Configure the NTP stratum

C. Set the authentication key

D. Choose the interface for syncing to the NTP server

E. Set the NTP DNS hostname

ANSWER: C D

Explanation:

Set the authentication key is required because NTP authentication lets the ASA validate time packets using a configured shared key and key identifier. The authentication key is the basis for confirming that NTP information came from the intended, authenticated time source rather than from an injected or spoofed source. In a complete ASA configuration, the relevant key must also be trusted and NTP authentication enabled so that the ASA enforces this validation for its NTP association.

Choose the interface for syncing to the NTP server explicitly binds the ASA's NTP-server communication to the appropriate ASA interface. ASDM exposes this selection when an NTP server is configured, and the corresponding ASA NTP server configuration can specify the source interface used for communication with that server. Selecting the expected interface ensures the appliance reaches the intended NTP infrastructure through the correct network path and uses the intended ASA source address. Combined with authenticated NTP, this provides both peer validation and controlled association connectivity, protecting the clock that is essential for accurate logging, certificate validation, VPN operation, and security-event correlation.

See Cisco's ASA NTP configuration guidance and the Cisco ASA command reference for NTP commands.

QUESTION NO: 27

Which RADIUS feature provides a mechanism to change the AAA attributes of a session after it is

authenticated?

A. Authorization

B. Accounting

C. Authentication

D. CoA

ANSWER: D

Explanation:

CoA is correct because RADIUS Change of Authorization provides a standardized way for an authorized RADIUS server to alter the authorization state or AAA attributes associated with an already active, authenticated client session. The server sends a CoA-Request to the network access device that is enforcing access, enabling policy to be updated dynamically rather than requiring the client to disconnect and perform a completely new authentication process. In Cisco security deployments, this capability is central to adaptive network access control. For example, Cisco ISE can use CoA after a posture assessment, guest-flow event, identity-group change, or other policy event to apply revised access permissions to a live endpoint. Depending on the access device and configured policy, the updated session can receive attributes such as a different VLAN assignment, a downloadable access control list, a security group tag, or a web-redirection policy. CoA can also request session reauthentication when that is the appropriate enforcement action. RFC 5176 defines Change-of-Authorization messages and explains that they enable a RADIUS server to communicate authorization changes to a NAS for an existing session. Cisco documents CoA as the mechanism used by ISE to dynamically apply authorization changes to connected endpoints. See RFC 5176: Dynamic Authorization Extensions to RADIUS and Cisco ISE Administrator Guide.

QUESTION NO: 28

How does Cisco Advanced Phishing Protection protect users?

A. It utilizes sensors that send messages securely.

B. It uses machine learning and real-time behavior analytics.

C. It validates the sender by using DKIM.

D. It determines which identities are perceived by the recipient.

ANSWER: D

Explanation:

Cisco Advanced Phishing Protection protects users by determining the identity that an email is attempting to present to the recipient. This identity-focused approach is essential for detecting impersonation attacks, including messages that appear to come from executives, trusted business partners, vendors, or recognized brands. Such attacks commonly use display-name spoofing, deceptive reply-to information, and lookalike domains to establish trust and persuade a recipient to disclose information, transfer funds, or take another risky action. By analyzing the perceived sender identity in the context of the recipient, the service can recognize when a message is misrepresenting a legitimate person or organization and apply the appropriate phishing-protection policy before delivery. This helps protect against business email compromise and other socially engineered attacks that may not contain malware or a clearly malicious link. Cisco describes its Secure Email capabilities as providing protection against phishing and impersonation threats, including advanced defenses that identify deceptive sender identities and suspicious messages. See the Cisco Secure Email overview and Cisco's Email Security product information.

QUESTION NO: 29

Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain

aware of the ongoing and most prevalent threats?

A. PSIRT

B. Talos

C. CSIRT

D. DEVNET

ANSWER: B

Explanation:

Talos is correct. Cisco Talos is Cisco's threat-intelligence organization, combining threat researchers, analysts, and engineers who investigate malicious activity and publish actionable intelligence for defenders. Its weekly *Threat Source* newsletter is specifically intended to keep cybersecurity professionals informed about significant and prevalent threats observed during the prior week, along with relevant security developments. The newsletter distills Talos research and telemetry into an accessible update that helps security teams understand the active threat landscape and use that awareness to prioritize defensive activity. Talos also publishes detailed threat research, vulnerability analysis, malware coverage, and indicators that support Cisco security products and the wider security community. This role—producing recurring intelligence on current threats—is directly aligned with the question's description of a weekly newsletter focused on ongoing and prevalent cybersecurity threats. Cisco Talos describes the Threat Source newsletter and provides subscription information at Cisco Talos Newsletters. Additional information about Talos research and threat-intelligence capabilities is available at Cisco Talos Intelligence Group.

QUESTION NO: 30

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

A. It must be within its validity period.

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: A C

Explanation:

For HTTPS/application-traffic decryption, the certificate authority certificate used by the Cisco Web Security Appliance must be currently valid and trusted by the client endpoints. A certificate with valid dates is required because certificates are usable only within their configured validity period. The WSA uses the configured certificate and private key to dynamically generate and sign certificates presented during the TLS interception process. If that signing certificate is expired or not yet valid, it cannot be used reliably for this purpose.

The certificate authority also must reside in the trusted certificate store of the endpoint. During decryption, the WSA effectively acts as an intermediary TLS endpoint and presents a certificate signed by its configured decryption CA. The endpoint validates the presented certificate chain against its local trust store. Deploying the WSA decryption root or intermediate CA certificate to managed clients is therefore necessary for clients to establish trusted TLS sessions while inspection occurs. Cisco's HTTPS-decryption guidance describes installing the decryption certificate on client systems, while standard TLS certificate processing requires that certificates be within their validity dates. See the Cisco AsyncOS HTTPS decryption documentation and RFC 5280 certificate validity requirements.

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.

E. The Cisco Secure Web Appliance uses a Layer 3 device to redirect traffic only if it is running in transparent mode.

ANSWER: C E

Explanation:

"The Cisco Secure Web Appliance responds with its own IP address only if it is running in explicit mode" is correct because explicit proxy operation requires clients to be proxy-aware. A browser or endpoint proxy setting directs the client's HTTP or HTTPS proxy connection to the Secure Web Appliance itself. The appliance is therefore the TCP/proxy peer for that client connection and uses its own address when responding in the proxy exchange. Explicit deployment can be configured directly in browsers or distributed through mechanisms such as PAC files, WPAD, group policy, or endpoint-management tooling.

"The Cisco Secure Web Appliance uses a Layer 3 device to redirect traffic only if it is running in transparent mode" is also correct. Transparent operation does not require clients to be configured to use a proxy. Instead, the endpoint initially attempts to reach the requested web destination, and network infrastructure transparently steers qualifying traffic to the appliance. Cisco deployments commonly use a Layer 3 redirection mechanism, such as Web Cache Communication Protocol or policy-based routing, to perform this interception and forwarding. This network-based traffic steering is what allows the appliance to apply web-security policy without endpoint proxy configuration. Cisco's Secure Web Appliance documentation and configuration-guide catalog describe the available proxy deployment and traffic-redirection models: Cisco Secure Web Appliance configuration guides and Cisco Secure Web Appliance support documentation.

QUESTION NO: 32

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

A. Postman is required to utilize Cisco Catalyst Center API calls.

B. They are Cisco proprietary.

C. They do not support Python scripts.

D. They view the overall health of the network.

E. They quickly provision new devices.

ANSWER: D E

Explanation:

Cisco Catalyst Center APIs expose the platform's assurance and automation capabilities through REST-based interfaces. "They view the overall health of the network" is correct because the Assurance APIs provide programmatic access to network health and related telemetry, including health summaries for the network, devices, clients, and applications. This allows external applications, dashboards, and operational workflows to retrieve the same type of assurance information used to identify performance and connectivity issues in the Catalyst Center interface.

"They quickly provision new devices." is also correct because Catalyst Center provides APIs for automation workflows around device discovery, inventory, site assignment, template deployment, and device provisioning. By invoking these API-driven workflows, an organization can consistently onboard and configure devices at scale rather than performing repetitive manual configuration. The APIs therefore support both operational visibility through assurance data and rapid deployment through automated provisioning processes.

Cisco documents these capabilities in its Catalyst Center API resources, including Assurance API endpoints and device onboarding and provisioning workflows. See the Cisco Catalyst Center API documentation and the Cisco Catalyst Center product page.

QUESTION NO: 33

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 exploits IP fragmentation and reassembly handling by delivering an ICMP Echo packet whose reassembled size exceeds the maximum IP datagram size supported by the receiving host. "The attack is fragmented into groups of 8 octets before transmission" accurately describes the relevant IPv4 fragmentation behavior: the IPv4 Fragment Offset field is expressed in units of 8 octets, and, except for the final fragment, fragment data must be sized on an 8-octet boundary. An attacker can use individually valid fragments to cause the destination to attempt reassembly of an invalid oversized datagram. RFC 791 specifies both the 65,535-octet maximum IPv4 total length and the 8-octet units used by Fragment Offset: RFC 791.

"Malformed packets are used to crash systems" describes the intended result and historical vulnerability condition. Once the target reassembles or processes the crafted ICMP datagram, defective IP-stack implementations could mishandle its illegal size, causing memory corruption, a hang, reboot, or denial of service. Thus, the defining pattern is not ordinary ICMP reachability testing, but deliberately malformed fragmented traffic designed to trigger a failure during packet handling. Cisco describes denial-of-service attacks as attempts to exhaust resources or interrupt service availability: Cisco: What Is a Denial-of-Service Attack?.

QUESTION NO: 34

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:

Device compliance, commonly implemented through Cisco ISE Posture, evaluates security-relevant attributes reported by the endpoint and compares them with the organization's posture policy. **endpoint protection software version** is a valid compliance parameter because posture policy can verify that endpoint anti-malware or antivirus protection is present, enabled as required, and running an approved product/version level. This helps ensure that a device seeking network access has the expected baseline endpoint defenses.

device operating system version is also a core compliance parameter. Policies can assess the endpoint operating system and version against an approved baseline, enabling the organization to restrict or remediate devices that are running unsupported, obsolete, or otherwise noncompliant platform versions. These endpoint-derived checks support an access decision such as granting normal access, applying restricted access, or directing the device to remediation. Cisco documents ISE Posture as the mechanism for assessing endpoint posture requirements and enforcing the resulting access policy. See the Cisco Identity Services Engine product page and Cisco's ISE installation and configuration guides.

QUESTION NO: 35

When wired 802.1X authentication is implemented, which two components are required? (Choose two.)

A. authentication server: Cisco Identity Service Engine

B. supplicant: Cisco AnyConnect ISE Posture module

C. authenticator: Cisco Catalyst switch

D. authenticator: Cisco Identity Services Engine

E. authentication server: Cisco Prime Infrastructure

ANSWER: A C

Explanation:

Wired IEEE 802.1X uses a port-based access-control model in which the network device at the edge acts as the authenticator and a RADIUS-based authentication service validates the endpoint's credentials. **authentication server: Cisco Identity Service Engine** is correct because Cisco Identity Services Engine (ISE) can provide the authentication-server role. ISE receives the authentication request from the network access device over RADIUS, evaluates the presented identity and credentials according to configured policy, and returns the authentication and authorization result. It can also send authorization attributes, such as downloadable access-control lists, VLAN assignments, or security group tags.

authenticator: Cisco Catalyst switch is correct because an access switch performs the authenticator role for a wired endpoint. The switch controls the physical access port, exchanges EAP over LAN (EAPOL) messages with the endpoint, and encapsulates and relays the relevant EAP information to ISE using RADIUS. It then enforces the authorization result received from ISE on that port. Together, the Catalyst switch and ISE supply the network-enforcement and centralized authentication functions needed for a Cisco wired 802.1X deployment. Cisco describes these roles and message flows in its IEEE 802.1X overview and documents ISE's RADIUS-based access-control capabilities.

QUESTION NO: 36

Which solution detects threats across a private network, public clouds, and encrypted traffic?

A. Cisco Stealthwatch

B. Cisco CTA

C. Cisco Encrypted Traffic Analytics

D. Cisco Umbrella

ANSWER: A

Explanation:

Cisco Stealthwatch, now named Cisco Secure Network Analytics, is the solution that provides network detection and response across on-premises private networks, public-cloud environments, and encrypted traffic. It collects and analyzes network telemetry such as NetFlow, IPFIX, and cloud flow logs, then applies behavioral analytics to identify suspicious communications, compromised hosts, lateral movement, and data-exfiltration activity. This telemetry-based approach allows the platform to maintain visibility even when traffic payloads are not available for inspection.

For encrypted traffic, Secure Network Analytics can use Cisco Encrypted Traffic Analytics capabilities. ETA evaluates observable characteristics of encrypted sessions, including flow behavior and TLS-related metadata, to identify potentially malicious encrypted communications without requiring decryption of the payload. The same analytics platform can ingest relevant telemetry from cloud deployments as well as enterprise network infrastructure, providing correlated threat detection across these environments. Therefore, Cisco Stealthwatch is the best match because it is the overarching solution that combines broad network visibility, cloud telemetry analysis, and encrypted-traffic threat detection. Cisco documents these capabilities under Cisco Secure Network Analytics and Cisco Encrypted Traffic Analytics.

QUESTION NO: 37

An engineer notices traffic interruptions on the network. Upon further investigation, it is learned that broadcast packets have been flooding the network. What must be configured, based on a predefined threshold, to address this issue?

A. Storm Control

B. embedded event monitoring

C. access control lists

D. Bridge Protocol Data Unit guard

ANSWER: A

Explanation:

Storm Control is the appropriate feature because it provides threshold-based protection against excessive broadcast traffic on Layer 2 switch interfaces. A broadcast storm can consume available link bandwidth and switch resources, disrupting normal traffic across the VLAN. Storm control monitors the amount of broadcast traffic received on an interface and compares it with a configured rising threshold, typically expressed as a percentage of the interface's total bandwidth. When the measured traffic exceeds that threshold, the switch suppresses traffic above the allowed level. Depending on the platform and configuration, the interface can also be configured to generate a trap or to enter an error-disabled state for more restrictive mitigation. This makes Storm Control directly suited to the stated requirement: responding to broadcast flooding according to a predefined threshold, at the affected switchport, before the excess traffic causes broader network interruption. Cisco documents storm control as a mechanism for limiting broadcast, multicast, and unknown-unicast traffic levels on switch ports. See Cisco: Understanding and Configuring Storm Control and Cisco Catalyst 9300: Configuring Storm Control.

QUESTION NO: 38

What is the purpose of joining Cisco WSAs to an appliance group?

A. All WSAs in the group can view file analysis results.

B. The group supports improved redundancy

C. It supports cluster operations to expedite the malware analysis process.

D. It simplifies the task of patching multiple appliances.

E. It simplifies centralized management by allowing consistent policy and configuration deployment across multiple appliances.

ANSWER: E

Explanation:

It simplifies centralized management by allowing consistent policy and configuration deployment across multiple appliances. In Cisco Secure Web Appliance (formerly Web Security Appliance) deployments, an appliance group logically associates multiple appliances so an administrator can manage shared configuration settings from a central location. This reduces repetitive administrative work and helps maintain consistent web-security enforcement when several appliances are deployed, such as across sites or to accommodate larger traffic volumes. Group-level administration is intended for configuration and policy consistency; after appliances are joined, eligible configuration changes can be applied to group members rather than recreated separately on every device. This makes operational management more efficient and reduces the likelihood of configuration drift between appliances that should enforce the same organizational requirements. The appliance group is therefore a management construct, supporting coordinated administration of multiple WSAs rather than serving as a malware-analysis cluster or a mechanism for patch distribution. Cisco documentation for Secure Web Appliance describes appliance groups and centralized configuration management in its administration and configuration materials. See the Cisco Secure Web Appliance User Guide and Cisco's Secure Web Appliance support resources.

QUESTION NO: 39

Which security solution is used for posture assessment of the endpoints in a BYOD solution?

A. Cisco FTD

B. Cisco ASA

C. Cisco Umbrella

D. Cisco ISE

ANSWER: D

Explanation:

Cisco ISE is used for endpoint posture assessment in a BYOD deployment. As Cisco's network access control platform, ISE evaluates whether an endpoint complies with the organization's defined security policy before and, when required, after it receives network access. Posture conditions can include the state of antimalware and personal-firewall software, operating-system updates, disk encryption, and other endpoint-security requirements. Cisco ISE commonly performs these checks through the Cisco Secure Client posture module, formerly called the AnyConnect posture module, and can use the assessment outcome to drive authorization policy.

For BYOD, this lets an organization apply access appropriate to both the user identity and the device's compliance state. A compliant device can receive the intended authorization result, while a device requiring remediation can be directed to a limited-access or remediation workflow until it meets policy. ISE can also integrate device-management information and enforce policy through network infrastructure using capabilities such as 802.1X authentication and change of authorization. This makes posture assessment a core ISE function for controlling access by personally owned endpoints. Cisco documents ISE posture services in its Identity Services Engine product overview and its ISE configuration guides.

QUESTION NO: 40

A network administrator is configuring a switch to use Cisco ISE for 802.1X. An endpoint is failing authentication and is unable to access the network. Where should the administrator begin troubleshooting to verify the authentication details?

A. Context Visibility

B. Accounting Reports

C. Adaptive Network Control Policy List

D. RADIUS Live Logs

ANSWER: D

Explanation:

RADIUS Live Logs is the appropriate starting point because Cisco ISE records each RADIUS authentication request as it is processed and presents the resulting decision for the individual endpoint session. For an 802.1X failure, the administrator can locate the event using identifying details such as the username, endpoint MAC address, switch/NAD IP address, or time of the attempt. Opening the detailed report shows the authentication status and failure reason, the EAP method in use, the identity submitted by the supplicant, RADIUS attributes received from the switch, and the policy set and authentication/authorization rules evaluated by ISE. This makes it possible to verify whether the request reached ISE, whether it matched the intended policy, and which authentication detail prevented successful access. The report also provides the session-level evidence needed to investigate certificate validation, identity-store lookups, authorization results, or RADIUS attribute values in the proper context. Cisco documents RADIUS Live Logs as the area for viewing RADIUS authentication and accounting activity and drilling into individual log messages for details. See the Cisco ISE Monitoring and Troubleshooting documentation and Cisco ISE User Guides.

QUESTION NO: 41

An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the endpoint to apply a new or updated policy from ISE.

Which CoA type achieves this goal?

A. Port Bounce

B. CoA Terminate

C. CoA Reauth

D. CoA Session Query

ANSWER: C

Explanation:

CoA Reauth is the appropriate Cisco ISE Change of Authorization action when an active endpoint must be authenticated and authorized again so that ISE can evaluate its current state against the latest policy. ISE sends a RADIUS CoA request to the network access device that owns the session, such as a switch or wireless controller. The device then initiates reauthentication for the existing session and obtains a new authorization result from ISE. This enables updated authorization controls, such as downloadable ACLs, security group tags, VLAN assignments, URL redirection, or other authorization attributes, to be applied based on the endpoint's newly evaluated identity, posture, or authorization conditions.

This is particularly useful following a posture-status change, a change in group membership, or an authorization-policy update, because it refreshes the session's policy treatment without requiring an administrator to physically reset the connection. The underlying RADIUS Change of Authorization framework is defined by RFC 5176. Cisco also documents Change of Authorization behavior and configuration for ISE-integrated network devices in its Cisco ISE Administrator Guide.

QUESTION NO: 42

What are the two most commonly used authentication factors in multifactor authentication? (Choose two.)

A. biometric factor

B. time factor

C. confidentiality factor

D. knowledge factor

E. encryption factor

ANSWER: A D

Explanation:

biometric factor and **knowledge factor** are valid authentication-factor categories used in multifactor authentication. A knowledge factor establishes identity through something the user knows, commonly a password, PIN, or memorized passphrase. It is widely deployed because authentication services can validate it without requiring a physical device or specialized sensor. A biometric factor, also called an inherence factor, establishes identity using something the user is, such as a fingerprint, facial recognition, or an iris pattern. Modern laptops and mobile devices commonly include biometric sensors, making this factor practical for user verification and passwordless or step-up authentication flows.

MFA requires evidence from distinct factor categories rather than repeated evidence of the same type. Cisco describes MFA as combining verification methods such as a password with a biometric or a device-based approval. Therefore, knowledge and biometric factors are both recognized, commonly implemented factor types and are the applicable selections from the choices provided. Cisco Duo's overview of MFA is available at Cisco Duo Multi-Factor Authentication; NIST's definition and terminology are available at NIST CSRC Multi-Factor Authentication.

QUESTION NO: 43

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:

Cisco ISE BYOD onboarding requires **central WebAuth** because the endpoint must be redirected to an ISE-hosted portal before it can complete the onboarding workflow. The network access device initially permits only the necessary pre-authentication access and redirects the user's web traffic to ISE. At the portal, ISE authenticates the user, applies authorization policy, registers the device, and can initiate certificate-based provisioning. This centralized portal model allows the same ISE policy and onboarding experience to be used consistently across supported wired and wireless access deployments.

The **guest** component must also be configured because ISE's portal services provide the framework used for self-service web workflows, including the BYOD portal experience. Although BYOD users are normally employees rather than visitor guests, BYOD onboarding relies on ISE portal capabilities for device registration, acceptable-use presentation, identity authentication, and certificate provisioning. Administrators configure the relevant BYOD portal settings and authorization policies so that a successfully onboarded endpoint receives the intended access after registration.

Cisco documents BYOD as an ISE portal-based onboarding workflow that uses Central Web Authentication and certificate provisioning. See the Cisco ISE Administrator Guide and Cisco ISE installation and configuration guides.

QUESTION NO: 44

Which VMware platform does Cisco ACI integrate with to provide enhanced visibility, provide policy integration and deployment, and implement security policies with access lists?

A. VMware APIC

B. VMwarevRealize

C. VMware fusion

D. VMware horizons

E. VMware vSphere Distributed Switch (VDS/vDS)

ANSWER: E

Explanation:

VMware vSphere Distributed Switch (VDS/vDS) is correct because Cisco ACI integrates with the VMware virtual networking layer through a Virtual Machine Manager domain associated with a vSphere Distributed Switch. In this model, Cisco APIC connects to vCenter Server and uses the distributed switch to coordinate virtual-network constructs, including port groups, VLAN pools, and endpoint-group associations, for workloads attached to the virtual switch. This integration gives the fabric visibility into virtual-machine endpoints and their locations while allowing centrally defined ACI policy to be deployed consistently for those workloads. ACI contracts express the permitted communication between endpoint groups. Depending on the selected enforcement model and where traffic is forwarded, the contract policy is enforced through rules that function as access-control entries, including enforcement at the virtual-switch or fabric level. The distributed-switch integration is therefore the VMware platform that combines virtualization-aware visibility, policy mapping and deployment, and security-policy enforcement for ACI-connected virtual machines. Cisco documents this architecture under its VMware vCenter/vSphere VMM integration guidance, and VMware describes the vSphere Distributed Switch as a switch spanning multiple hosts and centrally managed through vCenter Server. See Cisco APIC Virtualization Guide: VMware vCenter integration and VMware vSphere Distributed Switch documentation.

QUESTION NO: 45

Which two RADIUS accounting messages are used to record the beginning and end of a user session? (Choose two.)

A. Accounting-Start

B. Accounting-Stop

C. Access-Request

D. Access-Accept

E. Change of Authorization

ANSWER: A B

Explanation:

Accounting-Start is correct because a network access device sends this RADIUS accounting message when it begins providing service to a user. The record can include information such as the username, session identifier, network access device, port, and time at which the session began.

Accounting-Stop is also correct because it is sent when the user session ends. It records the termination time and can include session duration, input and output octets, and a termination cause. Authentication and authorization systems use these accounting records for auditing, usage reporting, troubleshooting, and billing-related workflows.

Access-Request and Access-Accept are authentication and authorization messages. Change of Authorization is a dynamic authorization mechanism used to modify an active session rather than a standard accounting start or stop record. See RFC 2866: RADIUS Accounting.

QUESTION NO: 46

Which two methods can a client use to check whether a certificate has been revoked? (Choose two.)

A. Certificate revocation lists

B. Online Certificate Status Protocol

C. Subject alternative names

D. Certificate pinning

E. Extended key usage

ANSWER: A B

Explanation:

Certificate revocation lists are correct because a CRL is a list published by a certificate authority that identifies certificates revoked before their normal expiration date. A client can retrieve the CRL from the distribution point included in the certificate and verify whether the certificate serial number appears on the list.

Online Certificate Status Protocol is also correct because OCSP enables a client to request the revocation status of a specific certificate from an OCSP responder. Compared with downloading an entire CRL, OCSP can provide more targeted and potentially more current status information for an individual certificate.

Certificate pinning is an application trust-control technique and does not provide CA revocation status. Subject alternative names identify valid names for a certificate but do not identify whether it has been revoked. See RFC 5280 and RFC 6960.

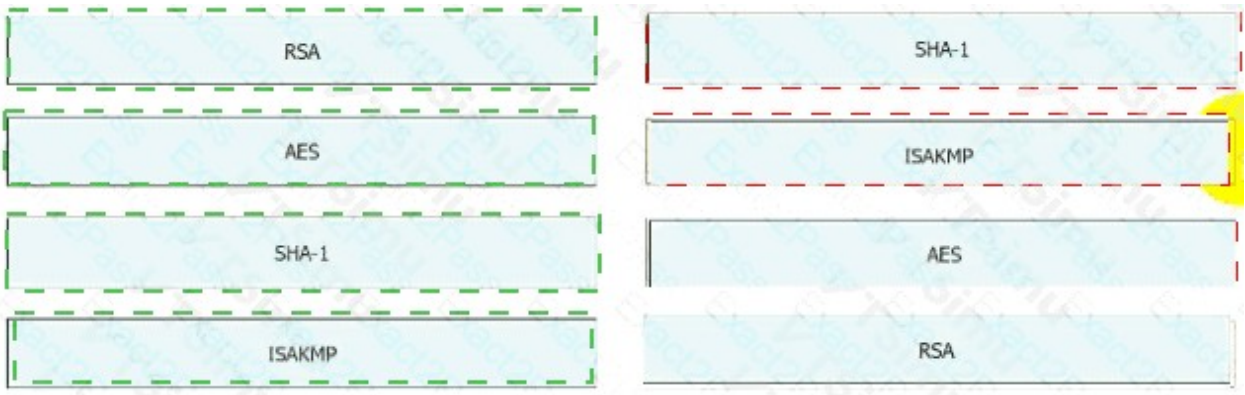
QUESTION NO: 47 - (DRAG DROP)

Drag and drop the VPN functions from the left onto the descriptions on the right.

ANSWER:

Answer:

Answer:



Explanation:

IPsec VPN operation uses separate mechanisms for confidentiality, integrity, authentication, and Security Association negotiation, and the mappings shown correctly align each technology with its role. AES is the symmetric encryption algorithm that protects the contents of packets from disclosure while they traverse an untrusted network. Its function in a VPN is therefore to ensure data confidentiality. SHA-1 is a cryptographic hash algorithm. In IPsec-era integrity mechanisms, a hash is used with a keyed construction such as HMAC so that the receiving peer can validate that protected traffic was not modified in transit. This makes SHA-1 the function that ensures data integrity.

RSA is an asymmetric public-key cryptographic system and supports identity authentication through digital signatures. A peer can validate a signature using the corresponding public key, providing assurance about the identity of the entity participating in the exchange. RSA therefore provides authentication in this mapping. ISAKMP, the Internet Security Association and Key Management Protocol, supplies the framework and message formats used to establish, negotiate, modify, and delete Security Associations for secure communications. Within the IKE/IPsec architecture, it is associated with defining and managing IKE Security Associations. Cisco's overview of IPsec and IKE describes IKE as the protocol used to establish the secure associations needed by IPsec: Cisco: IKE and IPsec Overview. The role of AES as a confidentiality algorithm is also consistent with NIST's AES standard: NIST FIPS 197: Advanced Encryption Standard. Thus, the displayed pairings correctly separate encryption, hashing for integrity, public-key authentication, and Security Association negotiation functions.

QUESTION NO: 48

Which Cisco platform onboards the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing the endpoint to gain network access?

A. Cisco ISE

B. Cisco NAC

C. Cisco TACACS+

D. Cisco WSA

ANSWER: A

Explanation:

Cisco ISE is the correct platform because its BYOD onboarding service is designed to register endpoints, provision identity certificates, and configure the endpoint for certificate-based network authentication. In a typical workflow, a user connects to an onboarding portal, ISE identifies and registers the device, and the onboarding process installs the required configuration profile or supplicant settings. ISE can use its internal certificate authority to issue the endpoint certificate, or it can integrate with an external public key infrastructure. The resulting certificate and trust chain support an EAP-TLS authentication method for wired or wireless 802.1X access. Crucially, the onboarding workflow can automatically deploy the network profile that selects and uses that certificate, rather than requiring the user to manually configure authentication settings. When the endpoint subsequently connects, ISE evaluates the certificate-based authentication and authorization policy, enabling the appropriate network access. This combination of device onboarding, certificate enrollment, and automated endpoint network-profile configuration is a core Cisco ISE capability. Cisco documents BYOD provisioning and certificate-based onboarding in its ISE administrator guidance and product documentation. See Cisco ISE BYOD Administration Guide and Cisco Identity Services Engine.

QUESTION NO: 49

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: A B

Explanation:

Before the Cisco Web Security Appliance (WSA) decrypts TLS application traffic, it evaluates the certificate presented by the destination server as part of certificate validation. The certificate must include the current date within its validity period: its *Not Before* date must already have started and its *Not After* date must not have expired. This time-validity check helps ensure that the WSA does not establish its inspection workflow using a certificate that is not presently valid.

The certificate chain must also terminate at a certificate authority that the WSA trusts. Accordingly, the relevant root CA certificate, and any required intermediate CA certificates, must reside in the WSA trusted certificate store. This enables the appliance to build and validate the server certificate chain before applying decryption to the session. These checks are core parts of certificate verification for HTTPS proxy and decryption deployments, where the WSA acts as the TLS-intercepting proxy while preserving validation of the upstream server identity.

Cisco documents HTTPS decryption and certificate-management behavior in its Web Security Appliance User Guide and provides the related configuration documentation through the Cisco WSA configuration guides.

QUESTION NO: 50

What are two functionalities of northbound and southbound APIs within Cisco SDN architecture? (Choose two.)

A. Southbound APIs are used to define how SDN controllers integrate with applications.

B. Southbound interfaces utilize device configurations such as VLANs and IP addresses.

C. Northbound APIs utilize RESTful API methods such as GET, POST, and DELETE.

D. Southbound APIs utilize CLI, SNMP, and RESTCONF.

E. Northbound interfaces utilize OpenFlow and OpFlex to integrate with network devices.

ANSWER: C D

Explanation:

Northbound APIs utilize RESTful API methods such as GET, POST, and DELETE because northbound interfaces connect SDN controller capabilities to applications, automation tools, and orchestration platforms. Through a controller's REST-based API, an application can retrieve topology, inventory, and assurance information, submit intent or policy, and create, modify, or delete managed objects. These interfaces make controller functions consumable by software rather than requiring direct, device-by-device administration.

Southbound APIs utilize CLI, SNMP, and RESTCONF because southbound communication is directed from the SDN controller toward network infrastructure. A controller needs mechanisms to discover devices, obtain operational information, and apply configuration or policy to physical and virtual network devices. Cisco controller platforms support a range of device-facing protocols and adapters according to platform and device capabilities; RESTCONF is a model-driven management interface, while CLI and SNMP can support configuration integration and monitoring of devices that use traditional management mechanisms. This separation allows applications to interact with the controller through northbound APIs while the controller translates desired outcomes into device-level operations through southbound interfaces. Cisco's SDN overview describes the controller's role between applications and infrastructure, and Cisco Catalyst Center publishes REST APIs for application integration. See Cisco Software-Defined Networking Overview and Cisco Catalyst Center Platform APIs.

QUESTION NO: 51

When NetFlow is applied to an interface, which component creates the flow monitor cache that is used

to collect traffic based on the key and nonkey fields in the configured record?

A. records

B. flow exporter

C. flow sampler

D. flow monitor

ANSWER: D

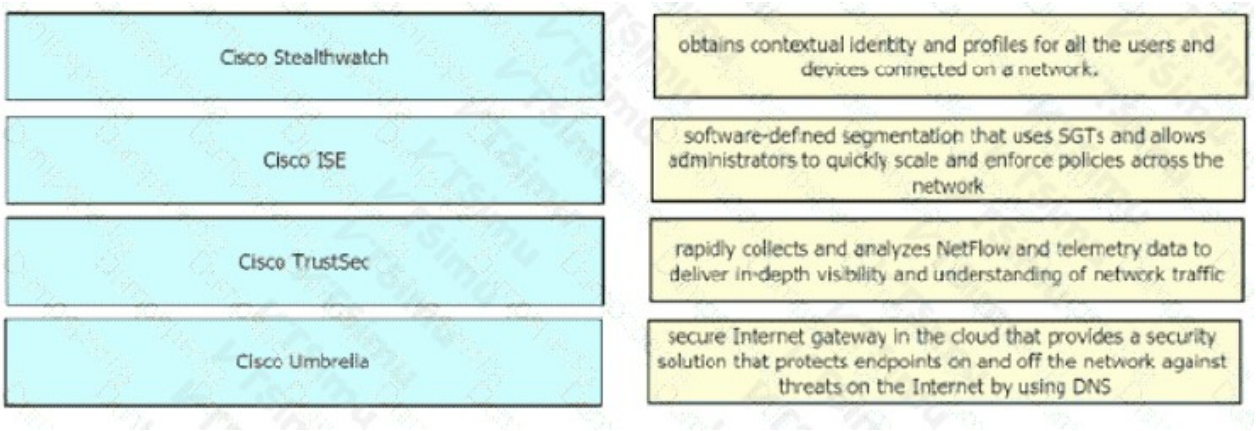
Explanation:

The correct answer is **flow monitor**. In Cisco Flexible NetFlow, a flow monitor is the operational component applied to an interface. It references a configured flow record, which specifies the fields used to identify a flow (key fields) and the additional information to collect for that flow (nonkey fields). Once the monitor is attached to an interface, it creates and maintains the monitor cache for traffic observed at that attachment point. Packets are classified according to the associated record, and matching packets update the corresponding cache entry until the flow is exported or aged out under the configured cache timers.

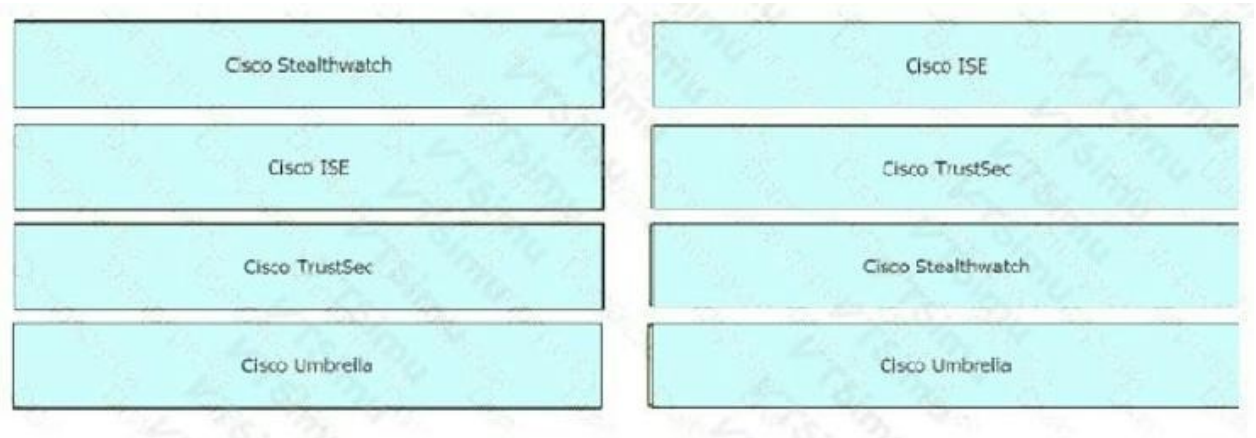
A flow monitor can also reference an exporter to send completed flow information to an external collector and, where required, a sampler to determine which packets are processed. However, the monitor is the object that binds these Flexible NetFlow elements into an interface-specific operational configuration and owns the cache used for flow accounting. Cisco documentation describes the monitor as the component applied to interfaces and identifies its cache as the location where flow information is stored. See the Cisco Flexible NetFlow Configuration Guide and Cisco's NetFlow overview.

QUESTION NO: 52 - (DRAG DROP)

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



ANSWER:



Explanation:

Cisco ISE provides the identity-based context needed to understand who and what is connecting to the network. It gathers and uses information about users, endpoints, device types, and posture, which supports the benefit of obtaining contextual identity and profiling information for all connected users and devices. Cisco TrustSec is Cisco's policy-based segmentation architecture. Its policy model uses Security Group Tags, commonly called SGTs, so access policy can be consistently enforced as traffic moves through the network without relying solely on address-based segmentation.

Cisco Stealthwatch, now associated with Cisco Secure Network Analytics, is the visibility and analytics solution in this set. It consumes flow records such as NetFlow along with telemetry to build an understanding of network communications, detect anomalous behavior, and provide network traffic visibility. That directly matches the benefit focused on rapidly collecting and analyzing NetFlow and telemetry. Cisco Umbrella is delivered from the cloud and acts as a secure Internet gateway. Its DNS-layer security capability helps stop connections to known malicious or risky Internet destinations before endpoints establish those connections, matching the DNS-based Internet threat protection benefit. Cisco documentation describes the TrustSec segmentation model at Cisco TrustSec, identity services at Cisco ISE, cloud-delivered protection at Cisco Umbrella, and network analytics at Cisco Secure Network Analytics.

QUESTION NO: 53

What is the primary benefit of deploying an ESA in hybrid mode?

A. You can fine-tune its settings to provide the optimum balance between security and performance for your environment

B. It provides the lowest total cost of ownership by reducing the need for physical appliances

C. It provides maximum protection and control of outbound messages

D. It provides email security while supporting the transition to the cloud

ANSWER: D

Explanation:

"It provides email security while supporting the transition to the cloud" is correct because hybrid email security is designed for organizations that need to protect email across both on-premises infrastructure and cloud-delivered security services. Rather than requiring a complete, immediate migration, a hybrid deployment lets an organization use on-premises Email Security Appliances alongside Cisco's cloud email-security capabilities. This supports phased adoption of cloud services while maintaining continuity for existing mail flows, policies, operational processes, and security controls.

The defining benefit is deployment flexibility: organizations can shift protected users between on-premises and cloud coverage as their business, compliance, infrastructure, or migration requirements evolve, while retaining comprehensive email threat protection. This model is particularly valuable when a company is moving messaging workloads to the cloud gradually, has a mixed environment, or needs to preserve local controls during a transition. Cisco describes Hybrid Email Security as an approach that combines on-premises and cloud email-security deployments and enables adjustment of user allocation between them during the subscription term. See Cisco's Email Security overview and the Cisco Hybrid Email Security at-a-glance for deployment context.

QUESTION NO: 54

Email security has become a high-priority task for a security engineer at a large multi-national organization due to ongoing phishing campaigns. To help control this, the engineer has deployed an Incoming Content Filter with a URL reputation of (-10.00 to -6.00) on the Cisco Secure Email Gateway. Which action will the system perform to disable any links in messages that match the filter?

A. FilterAction

B. ScreenAction

C. Quarantine

D. Defang

ANSWER: D

Explanation:

Defang is the Cisco Secure Email Gateway content-filter action designed to disable URLs found in a message. When an incoming content filter matches URLs with the specified poor reputation range, the Defang action modifies the URI so that it is not usable as an active hyperlink. This allows the email to be delivered while reducing the risk that a recipient can inadvertently follow a phishing or malicious link. The original URL information remains visible in a safely altered form, which preserves useful message context for the recipient, help desk, or incident-response team.

This behavior is particularly appropriate for reputation-based phishing controls. Rather than necessarily discarding the entire message, it neutralizes the risky web destination identified by URL reputation analysis. Cisco documents URL filtering and message actions, including URL defanging, as controls available for handling unwanted or malicious URLs in mail processed by the Secure Email Gateway. See Cisco's AsyncOS for Cisco Secure Email Gateway User Guide and the Cisco Secure Email Gateway product documentation portal.

QUESTION NO: 55

An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch was not installed, which left the endpoint vulnerable to WannaCry ransomware.

Which two solutions mitigate the risk of this ransomware infection? (Choose two.)

A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.

B. Set up a profiling policy in Cisco Identity Services Engine to check an endpoint patch level before allowing access on the network.

C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.

D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.

E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.

ANSWER: C E

Explanation:

Configuring a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network is an appropriate access-control mitigation. Cisco ISE Posture evaluates endpoint compliance through the Cisco Secure Client posture module and can use authorization results to restrict a noncompliant device's connectivity until it is remediated. In this case, the organization can define the required Microsoft update or an equivalent compliant operating-system patch level, then prevent an endpoint that does not meet that requirement from receiving normal network access. This limits the opportunity for an unpatched host to be exploited or to spread ransomware laterally.

Setting up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion addresses the underlying exposure across the endpoint estate. MS17-010 resolves the Microsoft SMB vulnerability exploited by WannaCry; therefore, prompt, centrally managed deployment of the applicable security update removes the vulnerable condition rather than merely detecting it at connection time. Combining timely patch deployment with ISE compliance enforcement provides both remediation and admission control for devices that have not yet been updated. Microsoft documents the affected SMB vulnerability and required updates in Microsoft Security Bulletin MS17-010. Cisco describes its endpoint compliance capabilities in the Cisco Identity Services Engine product documentation.

QUESTION NO: 56

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), now Cisco Secure Email, is designed to inspect email traffic and stop malicious messages before they reach users' mailboxes. It applies email-specific controls to inbound and outbound SMTP messages, including anti-spam and anti-phishing analysis, sender and domain reputation, authentication checks, malicious URL evaluation, attachment inspection, and detection of impersonation techniques. These capabilities allow the appliance to identify social-engineering emails that attempt to trick recipients into disclosing credentials, transferring funds, or opening malicious content.

Cisco ESA's advanced phishing protections are particularly relevant because phishing campaigns commonly rely on forged identities, deceptive display names, lookalike domains, and suspicious links embedded in messages. By analyzing the message envelope, headers, body, URLs, and attachments at the mail gateway, ESA can quarantine, block, or otherwise prevent delivery of the phishing email. Cisco Web Security Appliance (WSA) is focused on controlling and securing web access rather than acting as an SMTP email-security gateway. Cisco documentation describes Secure Email's phishing-defense capabilities and the specific advanced phishing protections available for email processing: Cisco Secure Email overview and Cisco ESA Advanced Phishing Protection documentation.

QUESTION NO: 57

Which two email authentication mechanisms are used by DMARC to evaluate alignment with a domain in the From header? (Choose two.)

A. SPF

B. DKIM

C. TLS

D. S/MIME

E. SNMP

ANSWER: A B

Explanation:

SPF is correct because Sender Policy Framework authorizes the mail servers that can send email for a domain. During DMARC evaluation, the receiving system can determine whether the domain validated by SPF aligns with the domain displayed in the RFC 5322 From header.

DKIM is also correct because DomainKeys Identified Mail applies a cryptographic signature to an email message. The receiving server validates the signature by retrieving the signer's public key from DNS. DMARC evaluates whether the validated DKIM signing domain aligns with the domain in the From header.

DMARC uses the results and alignment of SPF and DKIM to determine whether a message passes DMARC and then applies the sender's requested disposition policy, such as none, quarantine, or reject. TLS protects the transport path between mail systems, while S/MIME provides end-to-end message signing or encryption and is not a DMARC alignment mechanism. See RFC 7489: DMARC.

QUESTION NO: 58

Which open source tool does Cisco use to create graphical visualizations of network telemetry on Cisco IOS XE devices?

A. InfluxDB

B. Splunk

C. SNMP

D. Grafana

ANSWER: D

Explanation:

Grafana is the correct tool because it is an open-source observability and visualization platform used to create dashboards, charts, and graphs from telemetry data. In a typical Cisco IOS XE model-driven telemetry deployment, the router or switch exports operational data through a telemetry subscription to a collector and time-series data store. Grafana provides the presentation layer: it queries the stored telemetry and renders it in customizable visual panels. This makes it well suited to displaying continuously changing operational metrics such as interface throughput and errors, CPU and memory utilization, environmental status, QoS counters, and routing information. Cisco IOS XE telemetry documentation describes the telemetry pipeline and its use with external collectors and visualization systems, while Grafana documentation describes its dashboard-based visualization capabilities and support for time-series data sources. The pairing enables network teams to turn streamed device-state data into actionable, near-real-time operational views. See Cisco's IOS XE telemetry documentation and the Grafana product documentation.

QUESTION NO: 59

Which two activities can be done using Cisco DNA Center? (Choose two.)

A. DHCP

B. design

C. accounting

D. DNS

E. provision

ANSWER: B E

Explanation:

Cisco DNA Center, now branded Cisco Catalyst Center, supports an intent-based network lifecycle that includes designing the network and provisioning its devices and services. The design activity lets administrators define the hierarchical site structure, such as areas, buildings, and floors, and associate network settings including IP address pools, wireless settings, device credentials, and network profiles. These design settings provide the reusable intent and foundational data needed for consistent enterprise-network deployments.

The provision activity applies that intent to the infrastructure. Cisco DNA Center can discover and onboard supported devices, use Plug and Play for zero-touch device onboarding, assign devices to sites, deploy configurations, and provision services such as wired, wireless, or SD-Access fabric connectivity. This automation enables repeatable deployment while maintaining centralized control of configuration and operational intent.

These functions are core elements of the Cisco DNA Center workflow, alongside policy and assurance. Cisco documents the platform as providing automation and assurance across the network lifecycle, with design and provisioning workflows used to prepare sites and deploy managed infrastructure. See the Cisco Catalyst Center product overview and Cisco's Catalyst Center User Guide.

QUESTION NO: 60

Which two capabilities are provided by Cisco Secure Malware Analytics? (Choose two.)

A. Dynamic analysis of suspicious files

B. Threat intelligence and behavioral indicators

C. Centralized mobile device enrollment

D. RADIUS authentication for network devices

E. DNS recursion for internal clients

ANSWER: A B

Explanation:

Dynamic analysis of suspicious files is correct because Cisco Secure Malware Analytics executes submitted files in a controlled analysis environment and observes their behavior. The resulting analysis can reveal actions such as process creation, registry changes, network communications, and attempts to evade detection.

Threat intelligence and behavioral indicators is also correct. The analysis report provides behavioral evidence and threat context that analysts can use to determine whether a file is malicious and to investigate affected systems. Secure Malware Analytics complements reputation-based detection by providing deeper inspection of files whose disposition is unknown or suspicious. Cisco describes its malware-analysis capabilities at Cisco Secure Malware Analytics.

QUESTION NO: 61

[Security Operations]

Which security solution uses NetFlow to provide visibility across the network, data center, branch offices, and cloud?

A. Cisco CTA

B. Cisco Encrypted Traffic Analytics

C. Cisco Umbrella

D. Cisco Secure Network Analytics

ANSWER: D

Explanation:

Cisco Secure Network Analytics is the correct solution because it collects and analyzes network telemetry, including NetFlow and IPFIX records, to establish broad visibility into communications throughout distributed enterprise environments. Formerly called Cisco Stealthwatch, it functions as a network detection and response platform: routers, switches, firewalls, and cloud sources export flow telemetry, which Secure Network Analytics correlates to model normal behavior and identify anomalies, suspicious connections, policy violations, and possible threats. This telemetry-centric approach supports visibility across campus and enterprise networks, data centers, branch sites, and cloud deployments without depending solely on packet payload inspection. It is particularly valuable for investigating encrypted traffic and east-west movement, because flow metadata still describes who communicated, when, how much data was transferred, and which protocols were used. Cisco documentation describes Secure Network Analytics as providing security analytics and visibility using pervasive network telemetry, including NetFlow, across on-premises and cloud environments. See Cisco Secure Network Analytics and the Cisco Secure Network Analytics data sheet.

QUESTION NO: 62

What is a difference between FlexVPN and DMVPN?

A. DMVPN uses only IKEv1. FlexVPN uses only IKEv2

B. FlexVPN uses IKEv2. DMVPN uses IKEv1 or IKEv2

C. DMVPN uses IKEv1 or IKEv2. FlexVPN only uses IKEv1

D. FlexVPN uses IKEv1 or IKEv2. DMVPN uses only IKEv2

ANSWER: B

Explanation:

FlexVPN uses IKEv2 as its control-plane and tunnel-establishment framework. Cisco designed FlexVPN around IKEv2 constructs, including IKEv2 profiles, authorization policies, and virtual tunnel interfaces, to provide a common VPN architecture that can support site-to-site and remote-access use cases. This IKEv2 foundation is a defining characteristic of FlexVPN configuration and operation.

DMVPN, by comparison, is an overlay VPN architecture based on multipoint GRE, NHRP, and IPsec. Traditional DMVPN deployments commonly use IKEv1, but Cisco platforms also support IKEv2 for DMVPN in supported releases and configurations. Therefore, the statement “FlexVPN uses IKEv2. DMVPN uses IKEv1 or IKEv2” accurately describes the practical protocol distinction: FlexVPN is inherently IKEv2-based, whereas DMVPN can be deployed with either Internet Key Exchange version. This distinction affects the configuration model, supported design choices, and the way peers authenticate and establish IPsec security associations. Cisco identifies FlexVPN as an IKEv2-based VPN solution and documents DMVPN support for both IKEv1 and IKEv2. See the Cisco FlexVPN support documentation and the Cisco DMVPN support documentation.

QUESTION NO: 63

An organization has a Cisco Stealthwatch Cloud deployment in their environment. Cloud logging is working as expected, but logs are not being received from the on-premise network, what action will resolve this issue?

A. Configure security appliances to send syslogs to Cisco Stealthwatch Cloud

B. Configure security appliances to send NetFlow to Cisco Stealthwatch Cloud

C. Deploy a Cisco FTD sensor to send events to Cisco Stealthwatch Cloud

D. Deploy a Cisco Stealthwatch Cloud sensor on the network to send data to Cisco Stealthwatch Cloud

ANSWER: D

Explanation:

Deploy a Cisco Stealthwatch Cloud sensor on the network to send data to Cisco Stealthwatch Cloud. The sensor provides the essential on-premises telemetry collection and forwarding function for Secure Cloud Analytics, formerly named Stealthwatch Cloud. It is deployed within the local environment where it can observe network traffic and generate the flow-based visibility required by the cloud analytics service. The sensor then establishes an outbound, secure connection to the Cisco cloud service and transmits the collected telemetry for analysis. This architecture is particularly appropriate when cloud-source integrations are already functioning but the organization lacks visibility into traffic traversing its physical site, branch, or data center. After the sensor is deployed, registered, and able to reach the service, Secure Cloud Analytics can analyze the on-premises traffic alongside cloud telemetry, enabling detection and investigation across both environments. Cisco describes Secure Cloud Analytics as a cloud-delivered network detection and response service, with sensors used to extend monitoring to private networks. Additional product and deployment information is available from Cisco Secure Cloud Analytics and the Cisco Secure Cloud Analytics data sheet.

QUESTION NO: 64

What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?

A. It decrypts HTTPS application traffic for unauthenticated users.

B. It alerts users when the WSA decrypts their traffic.

C. It decrypts HTTPS application traffic for authenticated users.

D. It provides enhanced HTTPS application detection for AsyncOS.

ANSWER: D

Explanation:

It provides enhanced HTTPS application detection for AsyncOS. HTTPS encrypts the HTTP content that ordinarily supplies useful application-identification data, such as request paths, headers, and other Layer 7 attributes. The Decrypt for Application Detection setting enables Cisco Secure Web Appliance (formerly WSA) AsyncOS to decrypt applicable HTTPS traffic so that it can inspect this content and identify the application more accurately. This provides the visibility needed to distinguish applications that may otherwise be visible only as generic encrypted web traffic. After AsyncOS identifies the application, administrators can use that identity in access-policy controls and reporting, allowing policy decisions to be based on the actual application being used rather than solely on destination information or TLS metadata. The feature's purpose is therefore application visibility and classification within the HTTPS-decryption workflow; it is not a setting intended to categorize decryption by a user's authentication status or merely notify users of inspection. Cisco documents HTTPS decryption configuration and behavior in the Cisco Secure Web Appliance User Guide: HTTPS Decryption. Additional release-specific guides are available through the Cisco Web Security Appliance User Guides page.

QUESTION NO: 65

Which Cisco security solution determines if an endpoint has the latest OS updates and patches installed on the system?

A. Cisco Endpoint Security Analytics

B. Cisco AMP for Endpoints

C. Endpoint Compliance Scanner

D. Security Posture Assessment Service

E. Cisco Identity Services Engine (ISE) Posture

ANSWER: E

Explanation:

Cisco Identity Services Engine (ISE) Posture is the Cisco solution that evaluates endpoint compliance, including whether the endpoint meets defined operating-system update and patch requirements. ISE uses its posture service together with the Cisco Secure Client (formerly AnyConnect) posture module to collect endpoint attributes and compare them with the organization's posture policy before or while granting network access. Administrators can define requirements for Windows Update status and other endpoint-security conditions, then apply authorization results based on the assessment. This makes the patch and update check part of a network-access-control workflow rather than merely an inventory or malware-detection function. If the device does not satisfy the required posture, ISE can restrict access, redirect the user for remediation, or provide limited access until the endpoint becomes compliant. Cisco identifies ISE as its platform for policy enforcement and secure network access, while its posture capabilities assess endpoint security state. See the Cisco Identity Services Engine product page and Cisco's ISE Administrator Guide for ISE policy and posture-related documentation.

QUESTION NO: 66

What provides visibility and awareness into what is currently occurring on the network?

A. CMX

B. WMI

C. Cisco Prime Infrastructure

D. Telemetry

ANSWER: D

Explanation:

Telemetry provides the real-time visibility and situational awareness needed to understand current network conditions. Network devices continuously generate operational data such as interface utilization and errors, CPU and memory use, routing and protocol state, flow records, security events, and application performance metrics. Telemetry exports this information to collectors and analytics platforms, where it can be correlated, visualized, and used to identify changes or anomalies as they occur.

In modern Cisco environments, model-driven telemetry commonly uses structured YANG-modeled data and supports efficient, scalable push-based delivery rather than relying solely on periodic polling. This enables operations and security teams to observe the present state of infrastructure, recognize emerging issues quickly, and supply timely data to monitoring, automation, SIEM, and network-detection systems. The resulting near-real-time insight supports faster troubleshooting and more informed operational decisions. Cisco describes model-driven telemetry as a mechanism for streaming operational data from devices and gaining actionable network visibility. See Cisco Model-Driven Telemetry and Cisco DevNet IOS XE Telemetry documentation.

QUESTION NO: 67

Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two.)

A. RADIUS

B. TACACS+

C. DHCP

D. sFlow

E. SMTP

ANSWER: A C

Explanation:

RADIUS and **DHCP** are Cisco Identity Services Engine profiling probes that gather endpoint attributes used to classify connected devices. The RADIUS probe uses information that ISE receives during RADIUS authentication, authorization, and accounting activity. This can provide valuable endpoint and connection context, including the endpoint MAC address, assigned network details, network-access-device information, and other RADIUS attributes. Because ISE commonly serves as the policy and RADIUS service for access control, these exchanges are a useful source of profiling data.

The DHCP probe gathers data from DHCP requests and lease-related traffic. DHCP messages expose attributes such as the client hardware address, requested parameters, vendor class information, host name, and other DHCP option values. ISE correlates this information with data obtained by other enabled probes to build endpoint profiles and apply authorization policy appropriate to the discovered device type. Cisco documents both RADIUS and DHCP among the probes available for ISE profiling, and administrators enable the probes that match the traffic and infrastructure visibility available in their deployment. See Cisco's ISE Profiling documentation and Cisco ISE installation and configuration guides.

QUESTION NO: 68

Which characteristic is unique to a Cisco WSAv as compared to a physical appliance?

A. supports VMware vMotion on VMware ESXi

B. requires an additional license

C. performs transparent redirection

D. supports SSL decryption

ANSWER: A C

Explanation:

supports VMware vMotion on VMware ESXi is applicable because the Cisco Web Security Virtual Appliance is deployed as a virtual machine. When it is hosted on a suitably configured VMware ESXi environment, the VM can use VMware infrastructure capabilities such as vMotion for live workload migration between hosts. This virtual-machine mobility supports maintenance and host-evacuation workflows without requiring a separate appliance replacement process.

performs transparent redirection is also a supported WSAv deployment capability. Transparent deployment enables web traffic to be redirected to the virtual security appliance for inspection without requiring clients to be explicitly configured with the appliance as their proxy. In a virtualized network, this can be implemented through the available network-redirection design, allowing the WSAv to receive and enforce web-security policy on redirected traffic while remaining transparent to endpoint users. Cisco documents transparent-proxy operation and the traffic-redirection mechanisms supported by Secure Web Appliance deployments. VMware documents vMotion as a live-migration capability for workloads running on ESXi hosts.

References: Cisco Secure Web Appliance User Guide; VMware vMotion

QUESTION NO: 69

A company has 5000 Windows users on its campus. Which two precautions should IT take to prevent WannaCry ransomware from spreading to all clients? (Choose two.)

A. Segment different departments to different IP blocks and enable Dynamic ARp inspection on all VLANs

B. Ensure that noncompliant endpoints are segmented off to contain any potential damage.

C. Ensure that a user cannot enter the network of another department.

D. Perform a posture check to allow network access only to those Windows devices that are already patched.

E. Put all company users in the trusted segment of NGFW and put all servers to the DMZ segment of the Cisco NGFW. ni

ANSWER: B D

Explanation:

Ensuring that noncompliant endpoints are segmented off to contain any potential damage is an effective containment measure. Dynamic segmentation can apply access controls based on endpoint identity and security status, placing devices that do not meet policy into a restricted network segment. This limits their ability to communicate laterally with other user devices and critical resources, which is essential when containing a rapidly propagating worm such as WannaCry. Cisco Identity Services Engine can use endpoint context and policy to enforce this type of controlled access and remediation workflow.

Performing a posture check to allow network access only to Windows devices that are already patched directly addresses the underlying exposure exploited by WannaCry. The malware abused the Microsoft SMB vulnerability addressed by the MS17-010 security update. A posture policy can assess whether required operating-system patches and endpoint-security controls are present before granting normal network access. Compliant systems receive appropriate connectivity, while unpatched systems can be quarantined or directed to remediation services until the required updates are installed. Combining patch-based posture validation with segmentation provides both preventive control and blast-radius reduction. Microsoft documents the SMB vulnerability update in MS17-010, and Cisco describes policy-based endpoint access and segmentation through Cisco Identity Services Engine.

QUESTION NO: 70

What are two benefits of using an MDM solution? (Choose two.)

A. grants administrators a way to remotely wipe a lost or stolen device

B. provides simple and streamlined login experience for multiple applications and users

C. native integration that helps secure applications across multiple cloud platforms or on-premises environments

D. encrypts data that is stored on endpoints

E. allows for centralized management of endpoint device applications and configurations

ANSWER: A E

Explanation:

Mobile device management (MDM) gives an organization centralized, policy-based control over enrolled mobile endpoints throughout their lifecycle. “grants administrators a way to remotely wipe a lost or stolen device” is a core MDM benefit because an administrator can issue a remote erase command when a device is lost, stolen, retired, or no longer compliant. This protects organizational information without requiring physical possession of the endpoint. Depending on the ownership and management model, the action can remove only managed corporate data or reset the entire device.

“allows for centralized management of endpoint device applications and configurations” is also fundamental to MDM. From a central console, administrators can enroll devices; distribute, configure, update, or remove managed applications; and deploy configuration profiles for settings such as Wi-Fi, VPN, email, certificates, passcodes, and device restrictions. Centralized control promotes consistent security settings across a device fleet, reduces manual administration, and helps demonstrate compliance with organizational policy. Cisco’s endpoint-security guidance recognizes device management and policy enforcement as important controls for protecting endpoints, while Microsoft’s MDM documentation provides practical examples of remote actions, application deployment, and configuration-policy management. See Cisco Secure Endpoint and Microsoft Intune documentation.

QUESTION NO: 71

Which type of data exfiltration technique encodes data in outbound DNS requests to specific servers

and can be stopped by Cisco Umbrella?

A. DNS tunneling

B. DNS flood attack

C. cache poisoning

D. DNS hijacking

ANSWER: A

Explanation:

DNS tunneling is the technique that embeds data within DNS queries, commonly in the subdomain portion of a queried domain name. A host can encode data into a series of query labels and send those queries to a domain controlled by an attacker. The attacker-controlled domain’s authoritative DNS server receives the encoded labels and reconstructs the transmitted information. This approach can provide a covert exfiltration or command-and-control channel because DNS resolution is widely required by normal network activity and is often permitted through outbound firewalls.

Cisco Umbrella operates at the DNS layer, applying security intelligence and policy enforcement before a client connects to a destination. Its DNS security capabilities can block requests to known or suspicious malicious domains and help identify DNS activity associated with threats, including anomalous query behavior characteristic of tunneling. By preventing resolution of attacker-controlled destinations or enforcing DNS-layer policy for suspicious domains, Umbrella can disrupt this outbound channel before the encoded requests reach the intended DNS infrastructure. Cisco describes Umbrella as a cloud-delivered security service that blocks requests to malicious internet destinations at the DNS layer. See the Cisco Umbrella documentation and Cisco’s Umbrella product overview.

QUESTION NO: 72

An attacker needs to perform reconnaissance on a target system to help gain access to it. The system has weak passwords, no encryption on the VPN links, and software bugs on the system's applications. Which vulnerability allows the attacker to see the passwords being transmitted in clear text?

A. unencrypted links for traffic

B. weak passwords for authentication

C. improper file security

D. software bugs on applications

ANSWER: A

Explanation:

Unencrypted links for traffic allow an attacker who can observe network communications to read data transmitted across those links, including usernames and passwords, directly in clear text. Encryption provides confidentiality for data in transit: a properly configured VPN normally encapsulates traffic in an encrypted tunnel, so a packet capture exposes encrypted ciphertext rather than readable credential values. When the VPN link has no encryption, however, an attacker positioned to capture the traffic—for example, on a compromised network device, a hostile wireless network, or another point along the communication path—can inspect the packets and view any credentials that the application or authentication protocol sends. This exposure is a passive confidentiality issue; the attacker can obtain the transmitted password without needing to guess it or exploit an application defect. Cisco describes IPsec VPNs as providing confidentiality by encrypting IP traffic, protecting communications as they traverse an untrusted network. Using strong VPN encryption and secure application protocols such as TLS prevents credentials and other sensitive content from being readable to traffic observers. See Cisco's IPsec overview and the Cisco VPN security overview.

QUESTION NO: 73

What are two facts about WSA HTTP proxy configuration with a PAC file? (Choose two.)

A. It is defined as a Transparent proxy deployment.

B. In a dual-NIC configuration, the PAC file directs traffic through the two NICs to the proxy.

C. The PAC file, which references the proxy, is deployed to the client web browser.

D. It is defined as an Explicit proxy deployment.

E. It is defined as a Bridge proxy deployment.

ANSWER: C D

Explanation:

The PAC file, which references the proxy, is deployed to the client web browser because Proxy Auto-Configuration is a client-side mechanism. A browser or operating system downloads or receives the PAC file through a configured PAC URL, enterprise endpoint-management policy, or Web Proxy Auto-Discovery. It evaluates the file's JavaScript `FindProxyForURL()` function for each requested URL. That function can return a directive such as `PROXY wsa.example.com:8080`, identifying the Cisco Web Security Appliance address and listening port to use; it can also return `DIRECT` for destinations that should bypass the proxy. Therefore, the client must possess and use the PAC configuration for its requests to be routed according to the file's rules.

It is defined as an Explicit proxy deployment because the endpoint deliberately sends web requests to the WSA based on its configured proxy-selection behavior. PAC-based configuration is a common scalable method for configuring explicit forward-proxy use while allowing rules for internal destinations, trusted sites, and proxy failover. This behavior is distinct from a deployment in which network infrastructure intercepts traffic without endpoint proxy configuration. Cisco's WSA documentation is available through the Cisco Web Security Appliance configuration guides. The standardized PAC format and the role of `FindProxyForURL()` are also documented by MDN's PAC file guide.

QUESTION NO: 74

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. teardrop

ANSWER: A B

Explanation:

phishing and **brute force** are the intended credential-based attack types addressed by multifactor authentication. MFA requires a user to prove identity with more than a password, combining factors such as knowledge, possession, or inherence. Consequently, a stolen, disclosed, or guessed password alone is insufficient to complete authentication.

For phishing, an attacker may obtain a victim's username and password through a fraudulent site or message, but MFA adds a separate verification step. Phishing-resistant methods, particularly FIDO2/WebAuthn security keys or platform authenticators, bind authentication to the legitimate site and provide stronger protection against credential-harvesting phishing. Cisco recommends MFA as an identity-security control for reducing the impact of compromised credentials.

For brute force, an attacker attempts many password values until one succeeds. Even if this process reveals a valid password, the attacker still needs the required additional factor, such as a registered authenticator, hardware token, biometric verification, or approved push challenge. MFA therefore substantially reduces the value of passwords obtained through guessing attacks, while rate limiting and account-lockout controls provide complementary protection. See Cisco's overview of multifactor authentication and the CISA guidance on implementing phishing-resistant MFA.

QUESTION NO: 75

On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed

devices?

A. health policy

B. system policy

C. correlation policy

D. access control policy

E. health awareness policy

ANSWER: A

Explanation:

The correct policy is **health policy**. In Cisco Firepower Management Center, a health policy defines the health-monitoring configuration that is assigned to managed devices. It contains health modules, which are individual tests that monitor operational conditions affecting appliance hardware, software, and services. Examples include resource utilization, interface status, process status, disk usage, time synchronization, and other platform-specific operational checks. The configured policy controls which modules run and their alert thresholds or reporting behavior for each assigned device. When a module detects a condition meeting its alert criteria, the managed device reports the health event to Firepower Management Center. Administrators can then review these events and the device's health status through the Health Monitor and related health-event views. This centralized policy model lets administrators apply consistent health monitoring to multiple managed devices while tailoring module settings where necessary. Cisco documents health policies as the mechanism for configuring

health monitoring and collecting health alerts from devices managed by FMC. See Cisco's Health Monitoring documentation and the Cisco Secure Firewall Management Center Health Policy API documentation.

QUESTION NO: 76

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:

PowerOn Auto Provisioning and Seed IP are the controlled switch-onboarding methods used with Cisco DCNM fabric deployment. PowerOn Auto Provisioning (POAP) enables a newly powered-on Nexus switch to obtain its initial configuration automatically, typically through DHCP and a provisioning script or configuration file. This provides a repeatable way to establish required management connectivity and baseline settings before the switch participates in the managed fabric. Cisco documents POAP as a zero-touch deployment mechanism for bringing up Nexus switches in a consistent manner.

Seed IP onboarding starts with an administrator-supplied, reachable management address for a switch already connected to the management network. DCNM can use that initial address as the discovery starting point to identify and add applicable devices under management. Supplying the seed explicitly preserves administrative control over where discovery begins rather than relying on an unrestricted, automatic network-discovery process. Used together, these approaches support predictable private-cloud fabric expansion: POAP prepares switches at initial boot, while a seed IP provides a deliberate point from which DCNM discovers and manages fabric devices. Cisco's DCNM documentation and Nexus switch provisioning guidance provide additional details: Cisco DCNM LAN Fabric Configuration Guide and Cisco Nexus POAP documentation.

QUESTION NO: 77

Which two preventive measures are used to control cross-site scripting? (Choose two)

A. Enable client-side scripts on a per-domain basis.

B. Incorporate contextual output encoding/escaping.

C. Disable cookie inspection in the HTML inspection engine.

D. Run untrusted HTML input through an HTML sanitization engine.

E. Same Site cookie attribute should not be used.

ANSWER: B D

Explanation:

Incorporate contextual output encoding/escaping and **Run untrusted HTML input through an HTML sanitization engine** are core preventive controls for cross-site scripting (XSS). Contextual output encoding ensures that untrusted data is treated as data rather than executable browser content when it is placed into a response. The appropriate encoding must match the output location, such as an HTML element, HTML attribute, JavaScript value, URL, or CSS context. Using a framework or a well-maintained encoding library helps consistently apply the required context-specific handling before content reaches the browser.

When an application intentionally accepts a limited subset of HTML, output encoding alone is not sufficient to preserve approved markup safely. An HTML sanitization engine parses the untrusted input and removes or neutralizes unsafe tags, attributes, protocols, and executable constructs while allowing an explicitly permitted set of harmless formatting elements. This is especially important for features such as rich-text comments or profile descriptions. These practices reduce the likelihood that attacker-controlled input can introduce script execution into pages viewed by other users. OWASP identifies output encoding and HTML sanitization as primary XSS defenses; see the OWASP Cross Site Scripting Prevention Cheat Sheet and the OWASP XSS guidance.

QUESTION NO: 78

Which two methods can be used to authenticate IKEv2 peers for an IPsec VPN? (Choose two.)

A. Pre-shared keys

B. Digital certificates

C. DH group selection

D. ESP integrity algorithms

E. NAT traversal

ANSWER: A B

Explanation:

Pre-shared keys and **digital certificates** are supported methods for authenticating IKEv2 peers. With pre-shared key authentication, both peers are configured with the same secret and use it to prove knowledge of the shared value during IKE authentication. This method is common in smaller or static VPN deployments, although key management becomes more difficult as the number of peers increases.

Digital certificates authenticate a peer by using a certificate and associated private key. The receiving peer validates the certificate chain, identity information, validity dates, and applicable revocation status. Certificate-based authentication is often preferred for scalable VPN deployments because it avoids configuring a unique shared secret on every peer and supports stronger identity lifecycle management through a public key infrastructure. See the Cisco IOS XE IKEv2 configuration guide.

QUESTION NO: 79

Which two Cisco Secure Firewall actions require a network analysis policy to be enabled? (Choose two.)

A. Detecting network-based malware with file inspection

B. Detecting intrusion events with intrusion rules

C. Translating an inside address with dynamic NAT

D. Assigning an interface IP address

E. Authenticating an administrator with TACACS+

ANSWER: A B

Explanation:

Detecting network-based malware with file inspection is correct because Secure Firewall network analysis policy settings control advanced inspection functions, including file-related malware detection workflows. The policy determines how the device processes applicable traffic and files for further analysis.

Detecting intrusion events with intrusion rules is also correct because intrusion policies are associated through the network analysis policy. The intrusion policy supplies the rules and detection settings used to inspect matching traffic for exploits, policy violations, and other suspicious activity. Access control policy determines whether traffic is allowed and can

associate deeper inspection policies, while the network analysis policy controls the advanced traffic-analysis functions. Cisco documents these policies in the Cisco Secure Firewall Management Center Network Analysis Policy documentation.

QUESTION NO: 80

Which two preventive measures are used to control cross-site scripting? (Choose two.)

A. Enable client-side scripts on a per-domain basis.

B. Incorporate contextual output encoding/escaping.

C. Disable cookie inspection in the HTML inspection engine.

D. Run untrusted HTML input through an HTML sanitization engine.

E. SameSite cookie attribute should not be used.

ANSWER: B D

Explanation:

Incorporate contextual output encoding/escaping is a fundamental XSS preventive control because browsers interpret data differently depending on whether it is placed in an HTML element, attribute, URL, JavaScript, or CSS context. Encoding untrusted values for their specific output context ensures characters such as angle brackets, quotation marks, and ampersands are treated as displayed data rather than as markup or executable code. This prevents attacker-controlled input from changing the document structure or introducing script into a rendered page.

Run untrusted HTML input through an HTML sanitization engine is appropriate when the application intentionally accepts rich-text content. A robust sanitizer uses a tightly controlled allowlist of safe elements, attributes, and URL schemes, while removing executable constructs such as script-capable attributes and unsafe URI values. Sanitization complements context-aware encoding by making user-supplied HTML safer before it is rendered. These controls address the core XSS risk: untrusted data reaching an execution-capable browser context. OWASP identifies output encoding as a primary XSS defense and recommends HTML sanitization for user-authored HTML content. See the OWASP Cross Site Scripting Prevention Cheat Sheet and the OWASP XSS overview.

QUESTION NO: 81

A network administrator is configuring SNMPv3 on a new router. The users have already been created, however an additional configuration is needed to facilitate access to the SNMP views. What must the administrator do to accomplish this?

A. define the encryption algorithm to be used by SNMPv3

B. set the password to be used for SNMPv3 authentication

C. Associate SNMPv3 users with an SNMP group that is configured with the required SNMP views.

D. specify the UDP port used by SNMP

ANSWER: C

Explanation:

Associate SNMPv3 users with an SNMP group that is configured with the required SNMP views. Cisco SNMPv3 authorization is based on a user, group, and view relationship. An SNMP view defines the permitted portion of the MIB object tree, such as the objects that may be read, written, or used for notifications. The view does not independently grant access merely because an SNMPv3 user exists. Instead, the administrator configures an SNMP group with the appropriate security model and security level, then assigns the desired read, write, and/or notify view to that group. The SNMPv3 user must belong to that group so that requests authenticated under that user inherit the group's authorized MIB scope. For example, a group can be configured with a read view and a user can be assigned to that group; the user can then retrieve only the objects included by that read view. This group-based association provides the access-control binding required for SNMPv3

and allows administrators to apply consistent permissions to multiple users. Cisco documents the configuration flow and the use of group read/write/notify views in its SNMP configuration and troubleshooting guide and Cisco IOS SNMP Configuration Guide.

QUESTION NO: 82

An engineer has enabled LDAP accept queries on a listener. Malicious actors must be prevented from quickly identifying all valid recipients. What must be done on the Cisco ESA to accomplish this goal?

A. Configure Directory Harvest Attack Prevention

B. Bypass LDAP access queries in the recipient access table.

C. Use Bounce Verification.

D. Configure incoming content filters.

ANSWER: A

Explanation:

Configure Directory Harvest Attack Prevention because LDAP accept queries cause the Email Security Appliance to check recipient validity during the SMTP transaction. Although this recipient verification is useful for blocking mail addressed to nonexistent users, an abusive SMTP client can attempt large numbers of recipient addresses and use the resulting responses to enumerate the organization's valid mailboxes. This behavior is a directory harvest attack.

Directory Harvest Attack Prevention is the ESA control intended to limit this recipient-enumeration risk. It monitors recipient-validation activity for patterns associated with harvesting, particularly excessive invalid-recipient attempts from an SMTP client. When configured thresholds are exceeded, the ESA applies protective action to the suspicious sender, reducing the rate at which it can continue probing recipients. Consequently, attackers cannot rapidly use LDAP-backed recipient validation as an oracle for discovering valid addresses, while ordinary legitimate SMTP traffic can continue to be processed.

The feature should be enabled and tuned for the organization's normal recipient and connection patterns, especially on listeners that use LDAP accept queries. Cisco documents directory harvesting protection as part of the ESA listener and mail-flow security configuration. See the Cisco Email Security Appliance user-guide library and Cisco Email Security Appliance documentation.

QUESTION NO: 83

Which command is used to log all events to a destination colector 209.165.201.107?

A. CiscoASA(config-pmap-c)#flow-export event-type flow-update destination 209.165.201.10

B. CiscoASA(config-cmap)# flow-export event-type all destination 209.165.201.

C. CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.10

D. CiscoASA(config-cmap)#flow-export event-type flow-update destination 209.165.201.10

E. CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.107

ANSWER: E

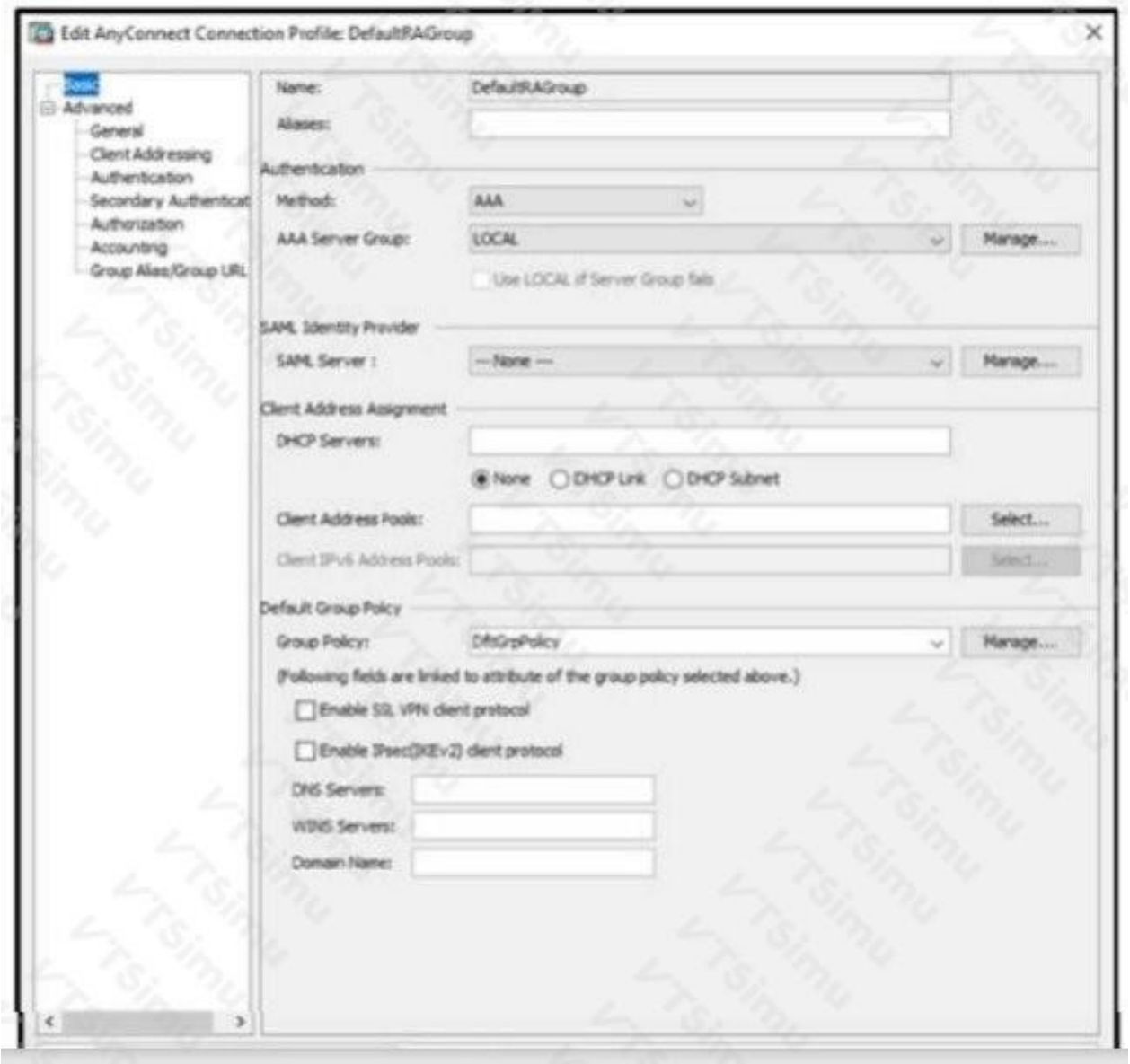
Explanation:

`CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.107` is the appropriate command because it configures Cisco ASA NetFlow Secure Event Logging (NSEL) flow export within a policy-map class configuration context. The `event-type all` keyword selects every supported NSEL event category for export, including flow-create, flow-deny, flow-teardown, and flow-update records. The `destination` parameter identifies the collector that will receive the exported records, so it must exactly match `209.165.201.107`. NSEL export is configured under the class of

an inspected traffic policy because the policy determines which traffic is subject to flow logging. This command therefore both enables comprehensive event selection and sends those events to the required collector address. Cisco documents NSEL configuration as a `flow-export` action under policy-map class configuration, with `event-type all` available to export all event types. See Cisco's ASA command reference for flow-export and the Cisco ASA NSEL monitoring guide.

QUESTION NO: 84

Refer to the exhibit.



When configuring a remote access VPN solution terminating on the Cisco ASA, an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication using machinecertificates. Which configuration item must be modified to allow this?

A. Group Policy

B. Method

C. SAML Server

D. DHCP Servers

ANSWER: B

Explanation:

Method must be modified because it controls the authentication flow that the ASA applies to connections using the relevant remote-access VPN connection profile. The required flow combines certificate authentication with AAA authentication: the ASA validates the client machine certificate and also sends the user authentication request to the configured external AAA service, such as a RADIUS server that supports token-based authentication. This is commonly configured as certificate-and-AAA authentication, rather than choosing only a certificate or only a AAA method.

Using the combined method is important because machine certificates identify and validate the endpoint, while the external token mechanism provides the additional user-authentication factor through AAA. The ASA connection profile therefore needs an authentication method that invokes both processes for the same VPN establishment attempt. Cisco documents certificate authentication and AAA authentication as connection-profile authentication mechanisms for remote-access VPNs, including configurations in which certificate authentication is used together with AAA. See the Cisco ASA Remote Access VPN Configuration Guide and Cisco's ASA VPN AAA Configuration documentation.

QUESTION NO: 85

Which two cryptographic algorithms are used with IPsec? (Choose two)

A. AES-BAC

B. AES-ABC

C. HMAC-SHA1/SHA2

D. Triple AMC-CBC

E. AES-CBC

ANSWER: C E

Explanation:

HMAC-SHA1/SHA2 and **AES-CBC** are cryptographic algorithms used by IPsec. IPsec protects IP traffic through the Authentication Header and, more commonly, Encapsulating Security Payload. HMAC used with SHA-1 or SHA-2 provides packet integrity and data-origin authentication: it enables the receiving peer to verify that protected traffic was not modified in transit and was generated by a party possessing the shared key. Cisco IPsec configurations use HMAC integrity algorithms as part of an IPsec transform set or proposal, subject to the platform and configured security policy.

AES in Cipher Block Chaining mode provides confidentiality for IPsec Encapsulating Security Payload by encrypting the packet payload. AES-CBC has historically been a widely deployed ESP encryption choice, including in Cisco IPsec configurations. The encryption algorithm and integrity algorithm can be negotiated together in an IPsec security association, allowing AES-CBC to provide encryption while HMAC-SHA provides integrity and authentication. Modern deployments may instead use authenticated-encryption suites such as AES-GCM, but that does not change the validity of AES-CBC and HMAC-SHA algorithms for IPsec. See Cisco's IOS XE Security Configuration Guide and the IETF's ESP specification.

QUESTION NO: 86

[Security Operations]

An engineer is configuring cloud logging on Cisco ASA and needs events to compress. Which component must be configured to accomplish this goal?

A. CDO event viewer

B. SWC service

C. Cisco analytics

D. SDC VM

ANSWER: D

Explanation:

SDC VM is the component that must be configured because the Secure Device Connector is the virtual-machine-based on-premises service that receives cloud-logging events from the ASA and securely forwards them to Cisco Defense Orchestrator cloud logging. It provides the transport path between the appliance and the cloud service, including connection management, local event handling, and compression of the log payload before it is sent across the WAN to Cisco's cloud infrastructure. This placement is important: compression is a forwarding and transport function, so it occurs at the connector that brokers the ASA-to-cloud connection rather than after events have arrived in a cloud interface.

For ASA cloud logging, the firewall is configured to use the Secure Device Connector as its logging destination. The SDC VM is deployed and registered from Cisco Defense Orchestrator, then the ASA forwards its selected syslog events to that connector. Configuring the SDC appropriately enables the connector to optimize the event stream, including compression, while maintaining secure delivery and buffering behavior as needed. Cisco's ASA configuration documentation describes cloud logging and its Secure Device Connector integration, and Cisco Defense Orchestrator documentation covers the cloud logging workflow: Cisco ASA Cloud Logging Configuration Guide and Cisco Defense Orchestrator Documentation.

QUESTION NO: 87

In which two ways does Easy Connect help control network access when used with Cisco TrustSec? (Choose two)

A. It allows multiple security products to share information and work together to enhance security posture in the network.

B. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.

C. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.

D. It integrates with third-party products to provide better visibility throughout the network.

E. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).

ANSWER: C E

Explanation:

Easy Connect extends Cisco TrustSec policy enforcement to endpoints and access environments where deploying conventional 802.1X authentication is impractical. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint. This lets Cisco ISE associate an endpoint with a TrustSec Security Group Tag, which is then used by the network to apply identity-based segmentation and Security Group ACL policy. The result is that access decisions can be based on the assigned security group rather than solely on IP address or VLAN placement.

Easy Connect also allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID). By using passive identity information obtained from Active Directory authentication activity, Cisco ISE can correlate a user identity with an endpoint and map that identity to the appropriate TrustSec security group. This supports consistent group-based policy for managed devices without requiring an 802.1X supplicant workflow. Together, SGT assignment without 802.1X and PassiveID-based AD identity mapping provide practical methods to extend TrustSec access control and segmentation. Cisco describes TrustSec as an architecture for policy-based access control using security group tags: Cisco TrustSec. Cisco ISE documentation and configuration guides are available at Cisco Identity Services Engine documentation.

QUESTION NO: 88

What are two workload security models? (Choose two.)

A. SaaS

B. PaaS

C. off-premises

D. on-premises

E. IaaS

ANSWER: C D

Explanation:

off-premises and **on-premises** are workload security models because they identify the environment in which an application workload operates and establish the associated security-responsibility boundary. An on-premises workload runs in infrastructure owned or directly controlled by the organization, such as its data center or private-cloud environment. The organization therefore manages protection across the environment, including the compute platform, network controls, operating systems, application configuration, identities, and data. An off-premises workload runs in externally hosted infrastructure, typically a public-cloud or managed-hosting environment. Security is governed through a shared-responsibility approach: the provider protects the underlying physical facilities and core cloud infrastructure, while the customer remains responsible for securing workload configurations, identities, applications, access policies, and data. Identifying whether a workload is on-premises or off-premises helps security teams select appropriate segmentation, visibility, policy enforcement, and incident-response controls. Cisco workload-security capabilities are designed to provide application-context visibility and consistent protection across both data-center and cloud-hosted workloads. See Cisco Secure Workload and Cisco: What Is Cloud Security?.

QUESTION NO: 89

What must be enabled to secure SaaS-based applications?

A. modular policy framework

B. two-factor authentication

C. application security gateway

D. end-to-end encryption

ANSWER: C

Explanation:

An application security gateway must be enabled to apply consistent security controls to users accessing software-as-a-service applications. SaaS services are internet-hosted and are often accessed directly by users from managed offices, remote locations, and unmanaged networks. An application security gateway provides a cloud-delivered policy-enforcement point between users and SaaS destinations, allowing an organization to identify the applications in use and control how they are accessed.

In Cisco’s security architecture, this function is commonly delivered through Secure Service Edge capabilities, including secure web gateway and cloud access security broker controls. These capabilities provide visibility into sanctioned and unsanctioned SaaS use, enforce web and application access policy, inspect relevant traffic, and apply data-protection controls such as restricting sensitive-data uploads. This is especially important for controlling shadow IT and protecting organizational data when the SaaS provider and the user are outside the traditional enterprise network perimeter.

Cisco Secure Access integrates these cloud-delivered security functions to protect access to internet and SaaS applications regardless of user location. See the Cisco Secure Access overview and Cisco’s Umbrella security overview.

QUESTION NO: 90

In an IaaS cloud services model, which security function is the provider responsible for managing?

A. Internet proxy

B. firewalling virtual machines

C. CASB

D. hypervisor OS hardening

ANSWER: D

Explanation:

In an infrastructure-as-a-service model, **hypervisor OS hardening** is managed by the cloud provider because it is part of the underlying virtualization platform used to deliver compute resources to customers. The provider operates the physical data centers, physical servers, storage, networking, and the hypervisor layer that isolates tenants and allows virtual machines to run. Securing that layer includes applying relevant platform patches, securely configuring and maintaining hypervisor hosts, controlling privileged administrative access, and monitoring the infrastructure for threats that could affect tenant isolation or service availability.

This division reflects the shared-responsibility model: the provider is accountable for security *of* the cloud, while a customer using IaaS remains responsible for security *in* the cloud. In practice, the customer configures and protects its guest operating systems, deployed applications, identities, data, and workload-level network controls; however, it cannot directly administer the provider's hypervisor environment. Cisco security professionals should recognize the virtualization layer as foundational infrastructure and therefore a provider-operated responsibility in IaaS. See the AWS Shared Responsibility Model and Microsoft Azure shared responsibility guidance.

QUESTION NO: 91

Which two protocols must be configured to authenticate end users to the Web Security Appliance? (Choose two.)

A. NTLMSSP

B. Kerberos

C. CHAP

D. TACACS+

E. RADIUS

ANSWER: A B

Explanation:

NTLMSSP and Kerberos are the Windows integrated-authentication protocols used by Cisco Web Security Appliance to identify end users transparently and apply identity- and group-based web-access policies. NTLMSSP uses a Windows challenge-response exchange, allowing the appliance to validate a user's domain identity without sending the password as clear text. This is commonly used when browsers are configured for integrated proxy authentication or where Kerberos cannot be used.

Kerberos provides ticket-based authentication through Active Directory. With the appropriate service principal name, DNS configuration, and browser trust settings, a browser can present a Kerberos service ticket to the proxy without prompting the user for credentials. This supports a seamless single sign-on experience and gives the appliance the authenticated identity needed for access policies, decryption controls, reporting, and other directory-aware enforcement.

Cisco documents NTLMSSP and Kerberos as authentication methods available for identifying users in web-proxy deployments. The platform's authentication configuration and deployment guidance is available in the Cisco Web Security Appliance configuration guides. Kerberos ticket-based identity validation is further described in the Microsoft Kerberos authentication overview.

QUESTION NO: 92

An administrator has been tasked with configuring the Cisco Secure Email Gateway to ensure there are no viruses before quarantined emails are delivered. In addition, delivery of mail from known bad mail servers must be prevented. Which two actions must be taken in order to meet these requirements? (Choose two.)

A. Deploy the Secure Email Gateway in the DMZ.

B. Use outbreak filters from Cisco Talos.

C. Configure a recipient access table.

D. Enable a message tracking service.

E. Scan quarantined emails using AntiVirus signatures.

ANSWER: B E

Explanation:

Scanning quarantined emails using AntiVirus signatures ensures that a message is evaluated for malware before it is released from quarantine and delivered. This is important because the security status of a held message can change as Cisco updates malware detections and antivirus signatures. Applying the current antivirus scanning capability at release helps ensure that attachments and message content containing newly identified threats are not delivered to recipients.

Using outbreak filters from Cisco Talos provides intelligence-driven protection against messages associated with active malicious email campaigns and suspicious sending infrastructure. Cisco Talos continuously analyzes global email and threat telemetry, allowing Secure Email to identify emerging outbreaks and take the configured action, such as blocking or quarantining affected messages. This provides timely protection when known-bad or compromised mail servers participate in a malicious campaign, rather than relying solely on static administrative rules. Together, these controls apply malware inspection to quarantined content and Talos-backed outbreak intelligence to inbound mail sources and campaigns. Cisco describes Secure Email's threat defense capabilities at Cisco Secure Email, and Talos threat intelligence information is available at Cisco Talos Intelligence.

QUESTION NO: 93

A Cisco Firepower administrator needs to configure a rule to allow a new application that has never been seen

on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose

two)

A. permit

B. trust

C. reset

D. allow

E. monitor

ANSWER: B E

Explanation:

trust and **monitor** are the access-control actions that permit matching traffic to traverse the Firepower device without applying the normal deep inspection policies. A trust rule is appropriate when the administrator wants to exempt a known and trusted traffic flow from further Firepower inspection. The connection is allowed, but the system does not apply intrusion, file, malware, or other access-control inspection to that flow. This is commonly used where inspection is unnecessary or where a traffic type must be bypassed.

A monitor rule also permits the traffic without inspection, while retaining connection visibility through logging and connection events. It is useful for a newly introduced application because it enables the administrator to observe that the application is using the rule and collect traffic information, without subjecting the flow to security-policy inspection that could affect the application. Cisco documents Monitor and Trust as the non-inspecting permit actions, with Monitor providing event logging and Trust providing a bypass for trusted traffic. See Cisco's Secure Firewall Management Center access-control rule documentation and the access-control rule components reference.

QUESTION NO: 94

How does Cisco Stealthwatch Cloud provide security for cloud environments?

A. It delivers visibility and threat detection.

B. It prevents exfiltration of sensitive data.

C. It assigns Internet-based DNS protection for clients and servers.

D. It facilitates secure connectivity between public and private networks.

ANSWER: A

Explanation:

Cisco Stealthwatch Cloud, now known as Cisco Secure Cloud Analytics, provides cloud-environment security through network detection and response capabilities: it delivers visibility into network communications and detects threats by analyzing cloud network telemetry. The service collects sources such as AWS VPC Flow Logs, Azure NSG flow logs, and other cloud telemetry, then applies behavioral analytics to establish expected communication patterns and identify suspicious deviations. This gives security teams useful context about workload-to-workload, workload-to-Internet, and hybrid-cloud traffic, even when cloud assets are dynamic and traditional network boundaries are less defined. Its detections can reveal behaviors associated with reconnaissance, command-and-control communications, lateral movement, cryptomining, and anomalous data transfers. The resulting alerts and investigation context enable analysts to prioritize risk and respond to potentially malicious activity. Therefore, “It delivers visibility and threat detection.” accurately describes the core security function of the product. Cisco describes Secure Cloud Analytics as a cloud-native network detection and response solution that uses cloud telemetry and behavioral modeling to identify threats across public-cloud and hybrid environments. See Cisco Secure Cloud Analytics and Cisco Stealthwatch.

QUESTION NO: 95

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 helps prevent *phishing* and *brute force* attacks by ensuring that a password alone is not sufficient to authenticate. In a typical credential-phishing attack, an attacker captures a user’s password through a fraudulent email, website, or message. Requiring an additional factor, such as a push approval, time-based one-time password, or hardware security key, means the stolen password cannot ordinarily be used by itself to access the account. Phishing-resistant implementations, especially FIDO2/WebAuthn security keys, provide stronger protection by binding authentication to the legitimate site and reducing the opportunity for credential replay.

Multifactor authentication also mitigates brute-force and password-guessing attacks. Even if an attacker successfully discovers, guesses, or cracks a password, authentication still requires possession of or access to the additional factor. This removes the password as the single point of failure and substantially reduces the value of compromised credentials. Cisco security designs commonly combine MFA with strong password controls, account lockout or rate-limiting measures, and identity monitoring for layered protection. CISA recommends phishing-resistant MFA as a key control for protecting accounts from credential theft, while MITRE identifies MFA as a mitigation for valid-account abuse. See CISA guidance on phishing-resistant MFA and MITRE ATT&CK: Multi-factor Authentication.