Free Questions for 350-701

Shared by Evelyn on Jun 27, 2025

For More Free Questions and Preparation Resources

Check the Links on Last Page

Questions # 1:

What is the most common type of data exfiltration that organizations currently experience?

Options:

○ A.

HTTPS file upload site

○ B.

Microsoft Windows network shares

○ C.

SQL database injections

○ D.

encrypted SMTP

Answer

B

Explanation

[Reference: https://blogs.cisco.com/security/sensitive-data-exfiltration-and-the-insider, , ,]

Questions # 2:

A security engineer must create a policy based on the reputation verdict of a file from a Cisco Secure Email Gateway. The file with an undetermined verdict must be dropped. Which action must the security engineer take to meet the requirement?

Options:

○ A.

Configure threshold settings for files with no score to be allowed.

○ B.

Set up a policy to automatically drop files with no reputation score.

○ C.

Implement a policy to disable file analysis.

○ D.

Create a policy to send a file to quarantine.

Answer

B

CertsMania

Questions # 3:

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

authenticated?

Options:

○ A.

Authorization

○ B.

Accounting

○ C.

Authentication

○ D.

CoA

CertsMania

Answer

D

Explanation

CoA stands for Change of Authorization, which is a feature that allows a RADIUS server to adjust an active client session after it is authenticated. For example, CoA can be used to reauthenticate a client, terminate a client session, or change the VLAN or group policy of a

client. CoA is supported by several RADIUS vendors, including Cisco ISE. CoA is defined in RFC 5176 and uses a pushed model, where the request originates from the RADIUS server and is sent to the network device that acts as a listener. CoA requests can have two possible response codes: CoA-ACK (acknowledgment) or CoA-NAK (non-acknowledgment). References :=

Some possible references are:

RADIUS Change of Authorization

Change of Authorization with RADIUS (CoA) on MR Access Points

Change of Authorization with RADIUS (CoA) on MS Switches

Technical Tip: Radius COA behavior

Questions # 4:

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?

Options:

○ A.

map SNMPv3 users to SNMP views

○ B.

set the password to be used for SNMPv3 authentication

○ C.

define the encryption algorithm to be used by SNMPv3

○ D.

specify the UDP port used by SNMP

Answer

A

Explanation

SNMPv3 is a security model that uses authentication and encryption to provide secure access to devices. SNMPv3 requires the configuration of SNMP groups, users, and views. SNMP groups define the security model, security level, and access rights for a set of users. SNMP users are members of SNMP groups and have passwords for authentication and encryption. SNMP views define the subset of the MIB tree that a group of users can access. To facilitate access to the SNMP views, the network administrator must map the SNMPv3 users to the SNMP views using the snmp-server group command with the v3 and view keywords. This command assigns a view to a group of users and specifies the security model and level for that group. For example, the following command maps the SNMPv3 users in the group admin to the view all using the authPriv security level:

snmp-server group admin v3 authPriv read all write all

This command allows the users in the group admin to access all the MIB objects in the view all using authentication and encryption. The other options are not correct because they are not related to the SNMP views. Option B is incorrect because the password for SNMPv3 authentication is configured for each user using the snmp-server user command with the auth keyword. Option C is incorrect because the encryption algorithm for SNMPv3 is also configured for each user using the snmp-server user command with the priv keyword. Option D is incorrect because the UDP port used by SNMP is not configurable and is always 161 for queries and 162 for traps. References :=

Some possible references for this question are:

SNMP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) - SNMP Version 3

Configuration Template for SNMPv3 - Cisco Community

Configure ESXi for SNMP v3 - VMware Docs

How to Configure SNMPv3 and How It Works - CBT Nuggets

Questions # 5:

Why is it important for the organization to have an endpoint patching strategy?

Options:

○ A.

so the organization can identify endpoint vulnerabilities

○ B.

so the internal PSIRT organization is aware of the latest bugs

○ C.

so the network administrator is notified when an existing bug is encountered

○ D.

so the latest security fixes are installed on the endpoints

Answer

D

Questions # 6:

Which endpoint solution protects a user from a phishing attack?

Options:

○ A.

Cisco Identity Services Engine

○ B.

Cisco AnyConnect with ISE Posture module

○ C.

Cisco AnyConnect with Network Access Manager module

○ D.

Cisco AnyConnect with Umbrella Roaming Security module

CertsMania

Answer

D

Explanation

Cisco AnyConnect with Umbrella Roaming Security module protects a user from a phishing attack by enforcing security at the DNS layer and blocking malicious domains that are used for phishing campaigns. The Umbrella Roaming Security module integrates with the Cisco AnyConnect client and provides always-on security even when no VPN is active. The Umbrella Roaming Security module can replace the existing Cisco Umbrella roaming client or be part of a new AnyConnect deployment12.

Cisco Identity Services Engine (ISE) is not an endpoint solution, but a network access control and policy enforcement platform that can integrate with AnyConnect for posture assessment and compliance3. Cisco AnyConnect with ISE Posture module is used to check the compliance status of the endpoint device and apply the appropriate network access policy based on the posture result4. Cisco AnyConnect with Network Access Manager module is used to manage the network connections and profiles of the endpoint device and support various authentication methods5. Neither of these modules directly protect the user from a phishing attack.

References :=

Roaming Client: Umbrella Roaming Security (Integration with AnyConnect)

Secure Umbrella Roaming: Cisco Secure Client (Formerly AnyConnect)

Cisco Identity Services Engine

[Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.9 - Posture Module]

[Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.9 - Network Access Manager Module]

CertsMania

Questions # 7:

What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and

Response?

Options:

○ A.

EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.

○ B.

EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.

○ C.

EPP focuses on network security, and EDR focuses on device security.

○ D.

EDR focuses on network security, and EPP focuses on device security.

Answer

A

Explanation

Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) are both important components of an endpoint security strategy, but they have different goals and capabilities. EPP is designed to act as a preventive security measure, blocking known and unknown malware and malicious activity on endpoint devices using various techniques such as antivirus, data encryption, and data loss prevention. EPP solutions are mainly cloud-managed and assisted by cloud data, and use multiple detection engines such as signature-based, machine learning, and behavioral analysis. EPP solutions prevent breaches by leveraging threat intelligence and sandboxing capabilities to continuously protect endpoints from emerging threats12.

EDR, on the other hand, focuses on detecting and responding to advanced threats that have already evaded the front-line defenses and infiltrated the environment. EDR solutions provide continuous and comprehensive visibility into endpoint activity in real time, allowing security teams to quickly and effectively identify and remediate cyberattacks such as ransomware and fileless malware. EDR solutions offer advanced threat detection, investigation, and response capabilities, including incident data search and investigation, alert triage, suspicious activity validation, threat hunting, and malicious activity detection and containment. EDR solutions serve as a safety net to capture threats that go undetected by traditional antivirus software and uncover incidents that would otherwise remain invisible34.

Therefore, the primary difference between an EPP and an EDR is that EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses. References: 1: Endpoint Protection Platform (EPP) Definition - Cisco 2: EPP vs. EDR: Why You Need Both - CrowdStrike 3: Endpoint Detection and Response (EDR) Definition - Cisco 4: EDR vs EPP: Why Should You Have to Choose? - Check Point Software

Questions # 8:

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

devices?

Options:

○ A.

health policy

○ B.

system policy

○ C.

correlation policy

○ D.

access control policy

○ E.

health awareness policy

Answer

A

Explanation

On Cisco Firepower Management Center, a health policy is used to collect health modules alerts from managed devices. A health policy is a collection of tests, or health modules, that monitor the health status of the hardware and software in the system. You can apply a health policy to one or more appliances and configure the frequency and conditions for running the health modules and generating alerts. The health monitor on the Firepower Management Center tracks the health events based on the health policy settings and displays them on the Health Monitor page and the event views. You can also use external alerting mechanisms, such as SNMP traps or syslog messages, to notify you of health events. References :=

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Health_Monitoring.html

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/710/management-center-admin-71/health-health.html

Questions # 9:

A network engineer is deciding whether to use stateful or stateless failover when configuring two ASAs for high availability. What is the connection status in both cases?

Options:

○ A.

need to be reestablished with stateful failover and preserved with stateless failover

○ B.

preserved with stateful failover and need to be reestablished with stateless failover

○ C.

preserved with both stateful and stateless failover

○ D.

need to be reestablished with both stateful and stateless failover

Answer

B

Explanation

Stateful failover means that the connection state information is replicated from the active ASA to the standby ASA, so that in the event of a failover, the connections are preserved and do not need to be reestablished. Stateless failover means that the connection state information is not replicated, so that in the event of a failover, the connections are dropped and need to be reestablished by the end hosts. Stateful failover provides a smoother transition and less disruption to the network traffic, while stateless failover is simpler and less resource-intensive. References:

Failover for High Availability - Cisco

Failover Types / ASA Failover Addresses / Failover Requirements | Cisco …

Questions # 10:

Refer to the exhibit. When creating an access rule for URL filtering, a network engineer adds certain categories and individual URLs to block. What is the result of the configuration?

Options:

○ A.

Only URLs for botnets with reputation scores of 1-3 will be blocked.

○ B.

Only URLs for botnets with a reputation score of 3 will be blocked.

○ C.

Only URLs for botnets with reputation scores of 3-5 will be blocked.

○ D.

Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked.

Answer

B

Explanation

The exhibit shows an access rule for URL filtering that has the following conditions:

The action is Block

The URL category is Botnets

The URL reputation is 3

The URL list is empty

This means that the rule will block any URL that matches the category and reputation criteria, regardless of the individual URL. According to the Cisco documentation1, the URL reputation is a score from 1 to 5 that indicates the risk level of a URL, where 1 is the most risky and 5 is the least risky. Therefore, a reputation score of 3 means a moderate risk level. The rule will not block URLs for botnets with reputation scores of 1, 2, 4, or 5, nor will it block any other URL category or list. The rule will also not allow any URL, as the

action is Block, not Allow.

References := 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Securing the Cloud, Lesson 4.3: Cloud Application Security, Topic 4.3.2: Cisco Umbrella, page 4-58.

Questions # 11:

Which Cisco security solution stops exfiltration using HTTPS?

Options:

○ A.

Cisco FTD

○ B.

Cisco AnyConnect

○ C.

Cisco CTA

○ D.

Cisco ASA

Answer

C

Explanation

https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf

Questions # 12:

Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize

applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application traffic?

Options:

○ A.

Cisco Security Intelligence

○ B.

Cisco Application Visibility and Control

○ C.

Cisco Model Driven Telemetry

○ D.

Cisco DNA Center

Answer

B

Explanation

Explanation

Explanation

The Cisco Application Visibility and Control (AVC) solution leverages multiple technologies to recognize,

analyze, and control over 1000 applications, including voice and video, email, file sharing, gaming, peer-to-peer

(P2P), and cloud-based applications. AVC combines several Cisco IOS/IOS XE components, as well as

communicating with external tools, to integrate the following functions into a powerful solution...

[Reference: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/guide/avc-user-guide/avc_tech_overview.html, ,]

Questions # 13:

Which two request of REST API are valid on the Cisco ASA Platform? (Choose two)

Options:

○ A.

put

○ B.

options

○ C.

get

○ D.

push

○ E.

connect

Answer

A, C

Explanation

Explanation

The ASA REST API gives you programmatic access to managing individual ASAs through a Representational State Transfer (REST) API. The API allows external clients to perform CRUD (Create, Read, Update, Delete) operations on ASA resources; it is based on the HTTPS protocol and REST methodology.

All API requests are sent over HTTPS to the ASA, and a response is returned.

Request Structure

Available request methods are:

GET – Retrieves data from the specified object.

PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist.

POST – Creates the object with the supplied information.

DELETE – Deletes the specified object

PATCH – Applies partial modifications to the specified object.

[Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html,]

Questions # 14:

When planning a VPN deployment, for which reason does an engineer opt for an active/active FlexVPN

configuration as opposed to DMVPN?

Options:

○ A.

Multiple routers or VRFs are required.

○ B.

Traffic is distributed statically by default.

○ C.

Floating static routes are required.

○ D.

HSRP is used for faliover.

Answer

A

Explanation

An active/active FlexVPN configuration allows for multiple routers or VRFs to act as hubs for different VPN groups, providing load balancing and redundancy1. This is useful when the VPN deployment has a large number of spokes or different security policies for different groups of spokes. DMVPN, on the other hand, only supports a single hub or a pair of hubs in active/standby mode for each VPN group2. This limits the scalability and flexibility of DMVPN deployments. Therefore, an engineer would opt for an active/active FlexVPN configuration as opposed to DMVPN when multiple routers or VRFs are required. References :=

Cisco FlexVPN: Benefits and Best Practices

Cisco DMVPN Design Guide

Questions # 15:

An engineer must deploy a Cisco Secure Web Appliance. Antimalware scanning must use the Outbreak Heuristics antimalware category on files identified as malware before performing any other processes. What must be configured on the Secure Web Appliance to meet the requirements?

Options:

○ A.

Sophos scanning engine

○ B.

Webroot scanning engine

○ C.

McAfee scanning engine

○ D.

Adaptive Scanning

Answer

D

Questions # 16:

Refer to the exhibit.

```
Gateway of last resort is 1.1.1.1 to network 0.0.0.0

S*   0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C        1.1.1.0 255.255.255.0 is directly connect, outside
S        172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C        192.168.100.0 255.255.255.0 is directly connected, inside
C        172.16.10.0 255.255.255.0 is directly connected, dmz
S          10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz
```

```
access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
 match access-list redirect-acl

policy-map inside-policy
 class redirect-class
 sfr fail-open

service-policy inside-policy global
```

What is a result of the configuration?

Options:

○ A.

Traffic from the DMZ network is redirected

○ B.

Traffic from the inside network is redirected

○ C.

All TCP traffic is redirected

○ D.

Traffic from the inside and DMZ networks is redirected

Answer

D

Explanation

Explanation

The purpose of above commands is to redirect traffic that matches the ACL “redirect-acl” to the Cisco

FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and

any other actions that are applied by policy are performed, the traffic is returned to the ASA for further

processing and ultimate transmission.

The command “service-policy global_policy global” applies the policy to all of the interfaces.

[Reference: https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.html, ,]

CertsMania

Questions # 17:

An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1 1 11 using the flow record Stea!thwatch406397954 command Which additional command is required to complete the flow record?

Options:

○ A.

transport udp 2055

○ B.

match ipv4 ttl

○ C.

cache timeout active 60

○ D.

destination 1.1.1.1

Answer

D

Explanation

The destination command is required to complete the flow record and specify the IP address of the Stealthwatch collector that will receive the NetFlow data. The transport udp 2055 command is also needed, but it is part of the flow exporter configuration, not the flow record. The match ipv4 ttl and cache timeout active 60 commands are optional and can be used to customize the flow record, but they are not mandatory. The flow record defines the fields that are collected and exported for each flow, such as source and destination IP addresses, ports, protocols, etc. The flow exporter defines the destination, source, transport protocol, and port for sending the NetFlow data. The flow monitor binds the flow record and the flow exporter together and applies them to an interface. The following is an example of a complete NetFlow configuration for sending data to Stealthwatch:

flow exporter EXPORTER description Export NetFlow to Stealthwatch destination 1.1.1.1 export-protocol netflow-v9 source Vlan100 transport udp 2055 ! flow record RECORD description NetFlow record match datalink mac source address input match datalink mac destination address input match datalink vlan input match ipv4 ttl match ipv4 tos match ipv4 protocol match ipv4 source address match ipv4 destination address match transport source-port match transport destination-port match interface input collect interface output collect counter bytes long collect counter packets long collect timestamp absolute first collect timestamp absolute last ! flow monitor IPv4_NETFLOW record RECORD exporter EXPORTER cache timeout active 60 ! interface <> ip flow monitor IPv4_NETFLOW input ! References : Configuring and Troubleshooting NetFlow for Stealthwatch, Cisco NetFlow Configuration, Building a Better Monitoring Solution with Flexible Netflow

Questions # 18:

A company identified a phishing vulnerability during a pentest What are two ways the company can protect employees from the attack? (Choose two.)

Options:

○ A.

using Cisco Umbrella

○ B.

using Cisco ESA

○ C.

using Cisco FTD

○ D.

using an inline IPS/IDS in the network

○ E.

using Cisco ISE

CertsMania

Answer

A, B

Explanation

Phishing is a type of cyberattack that uses fraudulent emails or other communications to trick users into providing sensitive information or installing malware on their devices1. Phishing can lead to identity theft, data breaches, ransomware infections, and financial losses. To protect employees from phishing attacks, a company can use various solutions that can detect, block, and remediate phishing threats. Two of these solutions are:

Cisco Umbrella: Cisco Umbrella is a cloud-based security platform that provides the first line of defense against threats on the internet, including phishing2. Cisco Umbrella uses DNS-layer security, which can identify and block malicious domains, IPs, and URLs before they can reach the user's device2. Cisco Umbrella also integrates with Cisco Email Security to provide additional protection against phishing emails that may bypass the email gateway3.

Cisco Email Security Appliance (ESA): Cisco ESA is an email gateway that protects inbound and outbound email traffic from spam, malware, phishing, and other threats4. Cisco ESA uses multiple layers of defense, such as reputation filtering, antivirus scanning, outbreak filters, and content filtering, to prevent malicious emails from reaching the user's inbox4. Cisco ESA also leverages Cisco Advanced Phishing Protection, which uses machine learning and threat intelligence to identify and block sophisticated phishing attacks that use identity deception techniques5.

References := 1: What Is Phishing? Examples and Phishing Quiz - Cisco 2: Cisco Umbrella - Cloud Delivered Enterprise Security 3: Cisco Umbrella and Cisco Email Security Integration 4: Cisco Secure Email - Cisco 5: Cisco Advanced Phishing Protection - Cisco Video Portal

Questions # 19:

Which CLI command is used to enable URL filtering support for shortened URLs on the Cisco ESA?

Options:

○ A.

webadvancedconfig

○ B.

websecurity advancedconfig

○ C.

outbreakconfig

○ D.

websecurity config

Answer

B

Questions # 20:

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?

Options:

○ A.

FilterAction

○ B.

ScreenAction

○ C.

Quarantine

○ D.

Defang

Answer

D

Questions # 21:

A network engineer entered the snmp-server user asmith myv7 auth sha cisco priv aes 256

cisc0xxxxxxxxx command and needs to send SNMP information to a host at 10.255.255.1. Which

command achieves this goal?

Options:

○ A.

snmp-server host inside 10.255.255.1 version 3 myv7

○ B.

snmp-server host inside 10.255.255.1 snmpv3 myv7

○ C.

snmp-server host inside 10.255.255.1 version 3 asmith

○ D.

snmp-server host inside 10.255.255.1 snmpv3 asmith

Answer

C

Questions # 22:

What is a key difference between Cisco Firepower and Cisco ASA?

Options:

○ A.

Cisco ASA provides access control while Cisco Firepower does not.

○ B.

Cisco Firepower provides identity-based access control while Cisco ASA does not.

○ C.

Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not.

○ D.

Cisco ASA provides SSL inspection while Cisco Firepower does not.

Answer

C

Explanation

Cisco Firepower is a unified security solution that combines firewall, intrusion prevention system (IPS), advanced malware protection (AMP), and threat intelligence features. Cisco ASA is a traditional firewall that focuses on network traffic control based on packet filtering and stateful inspection. One of the key differences between Cisco Firepower and Cisco ASA is that Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not. Intrusion prevention is the process of detecting and blocking malicious network traffic before it reaches the intended target. Cisco Firepower uses a combination of signature-based and behavior-based detection methods to identify and stop known and unknown attacks. Cisco ASA, on the other hand, does not have built-in intrusion prevention capabilities. It can only perform basic packet inspection and filtering based on predefined rules. To enable intrusion prevention on Cisco ASA, an additional module called FirePOWER Services is required. This module integrates Cisco Firepower features into Cisco ASA, but it is not the same as Cisco Firepower itself. Cisco Firepower offers more advanced and integrated security features than Cisco ASA with FirePOWER Services123. References: 1: Cisco ASA vs Cisco Firepower | What are the differences? - StackShare 2: Cisco FTD vs ASA: Difference and Comparison 3: CISCO FIREPOWER VS. ASA - Critical Design

Questions # 23:

What is the default action before identifying the URL during HTTPS inspection in Cisco Secure Firewall Threat Defense software?

Options:

○ A.

reset

○ B.

buffer

○ C.

pass

○ D.

drop

Answer

C

Explanation

Before identifying the URL during HTTPS inspection in Cisco Secure Firewall Threat Defense software, the default action is to "pass." This means that the traffic is allowed through without inspection until the URL can be identified, at which point appropriate security policies can be applied based on the URL categorization and reputation.

Questions # 24:

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

Options:

○ A.

single interface

○ B.

multi-context

○ C.

transparent

○ D.

two-interface

Answer

D

Explanation

To enable a separated email transfer flow from the Internet and from the LAN, the engineer must use the two-interface deployment mode on the Cisco WSA. This mode allows the WSA to have two separate network interfaces, one for the Internet traffic and one for the LAN traffic. This way, the WSA can apply different policies and settings for each interface, and isolate the email flows from each other. The two-interface mode also provides better performance and security than the single-interface mode, which uses only one network interface for both Internet and LAN traffic12. The other deployment modes, such as multi-context, transparent, or single-interface, do not support a separated email transfer flow from the Internet and from the LAN. References:

Two-interface mode, section “Deployment”.

WSA network configuration, section “Interfaces”.

Questions # 25:

An organization is trying to implement micro-segmentation on the network and wants to be able to gain visibility on the applications within the network. The solution must be able to maintain and force compliance. Which product should be used to meet these requirements?

Options:

○ A.

Cisco Umbrella

○ B.

Cisco AMP

○ C.

Cisco Stealthwatch

○ D.

Cisco Tetration

Answer

D

Explanation

Explanation

Micro-segmentation secures applications by expressly allowing particular application traffic and, by default,

denying all other traffic. Micro-segmentation is the foundation for implementing a zero-trust security model for

application workloads in the data center and cloud.

Cisco Tetration is an application workload security platform designed to secure your compute instances across

any infrastructure and any cloud. To achieve this, it uses behavior and attribute-driven microsegmentation

policy generation and enforcement. It enables trusted access through automated, exhaustive context from

various systems to automatically adapt security policies.

To generate accurate microsegmentation policy, Cisco Tetration performs application dependency mapping to

discover the relationships between different application tiers and infrastructure services. In addition, the

platform supports “what-if” policy analysis using real-time data or historical data to assist in the validation and risk assessment of policy application pre-enforcement to ensure ongoing application availability. The

normalized microsegmentation policy can be enforced through the application workload itself for a consistent approach to workload microsegmentation across any environment, including virtualized, bare-metal, and container workloads running in any public cloud or any data center. Once the microsegmentation policy is enforced, Cisco Tetration continues to monitor for compliance deviations, ensuring the segmentation policy is up to date as the application behavior change.

[Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf,]

Questions # 26:

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

Options:

○ A.

FlexVPN

○ B.

DMVPN

○ C.

SSL VPN

○ D.

GET VPN

Answer

A

Questions # 27:

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?

Options:

○ A.

Cisco ISE

○ B.

Cisco NAC

○ C.

Cisco TACACS+

○ D.

Cisco WSA

Answer

A

Explanation

Cisco ISE is a platform that can onboard 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. Cisco ISE has an internal CA service that can validate and sign certificate requests from endpoints, generate and store keys and certificates, and provide an OCSP responder to check the validity of certificates. Cisco ISE also supports Enrollment over Secure Transport (EST), which is a protocol that allows endpoints to securely enroll with a CA and obtain certificates. Cisco ISE can use EST to provision certificates to endpoints and configure their network settings to use EAP-TLS authentication. Cisco ISE can also use BYOD workflows to onboard endpoints and issue certificates to them. References:

Understand ISE Internal Certificate Authority Services

Endpoint On-boarding using Internal ISE CA

Cisco ISE BYOD Prescriptive Deployment Guide

Questions # 28:

A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to

ensure that bandwidth is available for VPN users needing access to corporate resources on the10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the

network?

Options:

○ A.

Use split tunneling to tunnel traffic for the 10.0.0.0/24 network only.

○ B.

Configure VPN load balancing to distribute traffic for the 10.0.0.0/24 network,

○ C.

Configure VPN load balancing to send non-corporate traffic straight to the internet.

○ D.

Use split tunneling to tunnel all traffic except for the 10.0.0.0/24 network.

Answer

A

Explanation

Split tunneling is a feature that allows VPN users to access both the corporate network and the internet at the same time. By using split tunneling, only the traffic destined for the 10.0.0.0/24 network will be encrypted and sent through the VPN tunnel, while the rest of the traffic will be sent directly to the internet. This reduces the VPN bandwidth load on the headend Cisco ASA and ensures that bandwidth is available for VPN users needing access to corporate resources. Split tunneling can be configured on the ASA by using the split-tunnel-network-list value command under the group-policy attributes. The network list should include the 10.0.0.0/24 network as the only entry. References: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 5: Secure Connectivity, Lesson 5.1: Implementing Site-to-Site VPNs on Cisco Routers and ASA Firewalls, Topic 5.1.3: Configuring Site-to-Site VPNs on Cisco ASA Firewalls, Subtopic 5.1.3.2: Configuring Split Tunneling.

CertsMania

Questions # 29:

A switch with Dynamic ARP Inspection enabled has received a spoofed ARP response on a trusted interface.

How does the switch behave in this situation?

Options:

○ A.

It forwards the packet after validation by using the MAC Binding Table.

○ B.

It drops the packet after validation by using the IP & MAC Binding Table.

○ C.

It forwards the packet without validation.

○ D.

It drops the packet without validation.

Answer

B

Explanation

Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets on untrusted interfaces by comparing the MAC address to IP address bindings in the DHCP snooping database or an ARP access-list. If the ARP packet contains invalid or spoofed information, it is dropped and logged. DAI also inspects ARP packets on trusted interfaces, but it does not drop them if they are invalid. Instead, it forwards them to the destination without validation. This allows the switch to support devices that use static IP addresses or have legitimate reasons to send ARP packets with different MAC address to IP address bindings. However, this also means that if a spoofed ARP packet is received on a trusted interface, it will bypass the DAI validation and be forwarded to the destination. This could allow an attacker to poison the ARP cache of other devices and perform a man-in-the-middle attack. Therefore, the correct answer is option B. The switch drops the packet after validation by using the IP & MAC Binding Table. References:

Understanding and Configuring Dynamic ARP Inspection

DAI (Dynamic ARP Inspection)

Dynamic ARP Inspection (DAI) Explanation & Configuration

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

Questions # 30:

Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?

Options:

○ A.

Cisco Umbrella

○ B.

Cisco AMP for Endpoints

○ C.

Cisco ISE

○ D.

Cisco Stealthwatch

Answer

C

Explanation

Cisco ISE is a solution that allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard. Cisco ISE integrates with Mobile Device Management (MDM) servers to provide necessary insight into the posture of mobile devices and enforce network access policies. Cisco ISE can also perform device registration, remediation, and periodic compliance checks on mobile devices. Cisco ISE can also issue remote actions on the device through the MDM server, such as full wipe, corporate wipe, and PIN lock. Cisco ISE can also augment endpoint data with information from the MDM server that cannot be gathered using the Cisco ISE profiling services. References:

Integrate XenMobile Mobile Device Management (MDM) with Cisco Identity Services Engine (ISE)

Cisco Identity Services Engine Administrator Guide, Release 2.4 - Mobile Device Manager Interoperability with Cisco ISE

Cisco ISE Integration with Mobile Device Management (MDM)

Questions # 31:

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?

CertsMania

Options:

○ A.

Adaptive Network Control Policy List

○ B.

Context Visibility

○ C.

Accounting Reports

○ D.

RADIUS Live Logs

Answer

D

Explanation

Explanation

Explanation

How To Troubleshoot ISE Failed Authentications & Authorizations

Check the ISE Live Logs

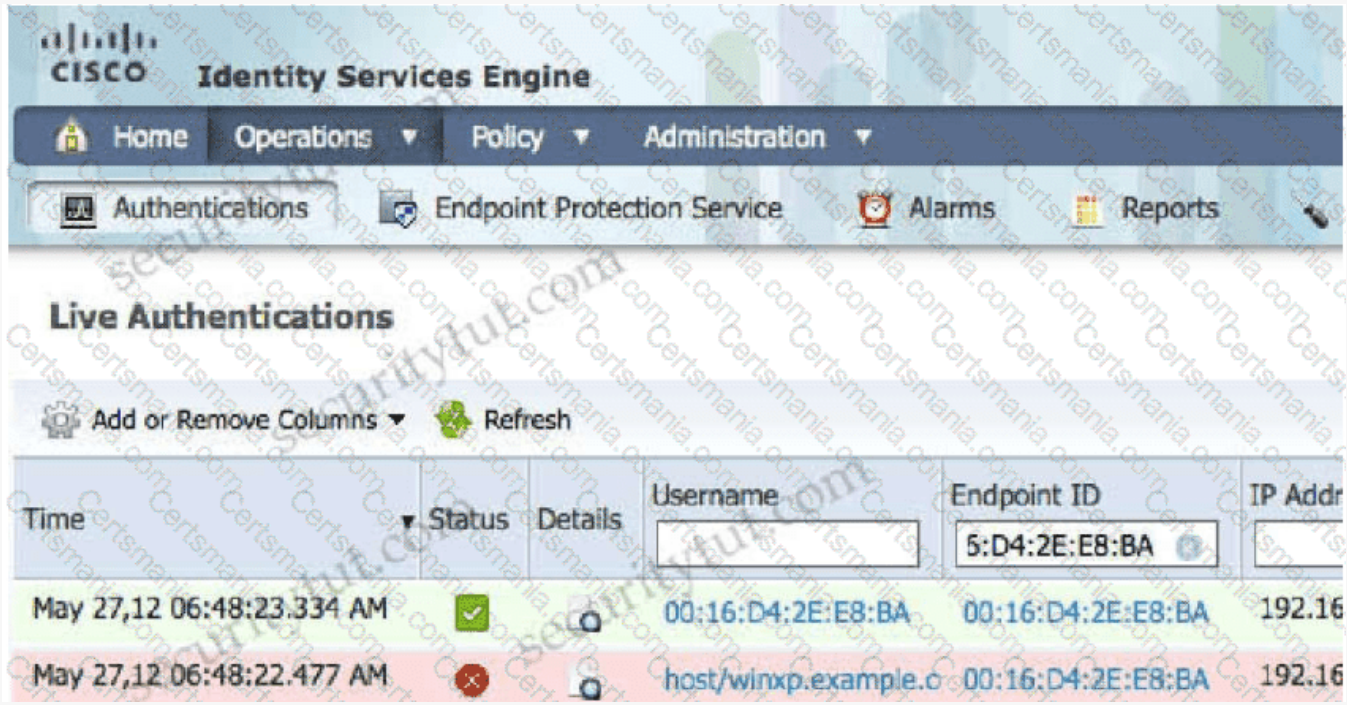
Login to the primary ISE Policy Administration Node (PAN).

Go to Operations > RADIUS > Live Logs

(Optional) If the event is not present in the RADIUS Live Logs, go to Operations > Reports > Reports >

Endpoints and Users > RADIUS Authentications

Check for Any Failed Authentication Attempts in the Log



[Reference: https://community.cisco.com/t5/security-documents/how-to-troubleshoot-ise-failed-authentications amp/ta-p/3630960,]

Questions # 32:

Which Cisco security solution provides patch management in the cloud?

Options:

○ A.

Cisco Umbrella

○ B.

Cisco ISE

○ C.

Cisco CloudLock

○ D.

Cisco Tetration

CertsMania

Answer

D

Explanation

Cisco Tetration is a Cisco security solution that provides patch management in the cloud. Patch management is the process of identifying, acquiring, installing, and verifying patches for products and systems to correct security and functionality problems in software and firmware1. Cisco Tetration is a cloud-native platform that delivers comprehensive workload protection for multicloud data centers by enabling a zero-trust model using segmentation2. One of the features of Cisco Tetration is software vulnerability detection and patch management, which allows users to identify software vulnerabilities on workloads, prioritize patching based on risk scores, and automate patch deployment using orchestration tools3. Cisco Tetration leverages the National Vulnerability Database (NVD) and Cisco Talos Intelligence Group to provide up-to-date information on software vulnerabilities and their severity levels3. Cisco Tetration also supports patch management for both Windows and Linux operating systems, as well as third-party applications such as Apache, Java, MySQL, and Oracle4. Therefore, the correct answer is D. Cisco Tetration. References: 1: RFC 9232: Network Telemetry Framework - Internet Engineering Task Force 2: Cisco Tetration - Workload Protection - Cisco 3: Cisco Tetration Software Vulnerability Detection and Patch Management - Cisco 4: Cisco Tetration Platform Data Sheet - Cisco

Questions # 33:

An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally

manage cloud policies across these platforms. Which software should be used to accomplish this goal?

Options:

○ A.

Cisco Defense Orchestrator

○ B.

Cisco Secureworks

○ C.

Cisco DNA Center

○ D.

Cisco Configuration Professional

Answer

A

Explanation

Explanation

Explanation

Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies

and device configurations with ease across multiple Cisco and cloud-native security platforms.

Cisco Defense Orchestrator features:

....

Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki

MX software is now easy, with the ability to share policy elements across platforms.

[Reference: https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html,]

Questions # 34:

Which encryption algorithm provides highly secure VPN communications?

Options:

○ A.

3DES

○ B.

AES 256

○ C.

AES 128

○ D.

DES

Answer

B

Explanation

AES (Advanced Encryption Standard) is a symmetric encryption algorithm that uses the same key to encrypt and decrypt data. It turns plain text into a code that only the intended recipient can read. AES has different key sizes, such as 128, 192, and 256 bits. The larger the key size, the more secure and complex the encryption is. AES 256 is the most secure encryption algorithm for VPN communications, as it uses a 256-bit key that would take an enormous amount of time and computing power to crack. AES 256 is widely used by VPN providers, as it offers a high level of security and performance for VPN tunnels. AES 256 is also recommended by the U.S. government for protecting classified information. References :=

How Does a VPN Securely Encrypt Your Connection?

What Is VPN Encryption, Types, Protocols And Algorithms Explained

What is AES (Advanced Encryption Standard)?

What is VPN Encryption & How Does it Work?

Questions # 35:

Which term describes when the Cisco Firepower downloads threat intelligence updates from Cisco Talos?

Options:

○ A.

consumption

○ B.

sharing

○ C.

analysis

○ D.

authoring

Answer

A

Explanation

Explanation

Explanation

... we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's Firepower

Management Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intellige ncedirector

Questions # 36:

After a recent breach, an organization determined that phishing was used to gain initial access to the network before regaining persistence. The information gained from the phishing attack was a result of users visiting known malicious websites. What must be done in order to prevent this from happening in the future?

Options:

○ A.

Modify an access policy

○ B.

Modify identification profiles

○ C.

Modify outbound malware scanning policies

○ D.

Modify web proxy settings

Answer

D

Explanation

URL conditions in access control rules allow you to limit the websites that users on your network can access. This feature is called URL filtering. There are two ways you can use access control to specify URLs you want to block (or, conversely, allow):

– With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic.

– With a URL Filtering license, you can also control access to websites based on the URL's general

classification, or category, and risk level, or reputation. The system displays this category and reputation data in connection logs, intrusion events, and application details.

Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies.

[Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html, , ,]

Questions # 37:

Which technology must be used to implement secure VPN connectivity among company branches over a

private IP cloud with any-to-any scalable connectivity?

Options:

○ A.

DMVPN

○ B.

FlexVPN

○ C.

IPsec DVTI

○ D.

GET VPN

Answer

D

Explanation

Explanation

Cisco's Group Encrypted Transport VPN (GETVPN) introduces the concept of a trusted group to eliminate

point-to-point tunnels and their associated overlay routing. All group members (GMs) share a common security

association (SA), also known as a group SA. This enables GMs to decrypt traffic that was encrypted by any

other GM.

GETVPN provides instantaneous large-scale any-to-any IP connectivity using a group IPsec security paradigm.

[Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_version_2_0_External.pdf,]

Questions # 38:

Which solution for remote workers enables protection, detection, and response on the endpoint against known and unknown threats?

Options:

○ A.

Cisco AMP for Endpoints

○ B.

Cisco AnyConnect

○ C.

Cisco Umbrella

○ D.

Cisco Duo

CertsMania

Answer

A

Explanation

Cisco AMP for Endpoints is a solution that enables protection, detection, and response on the endpoint against known and unknown threats. It provides continuous visibility and analysis of endpoint activity, as well as automated threat prevention and response capabilities. It leverages cloud-based intelligence, sandboxing, and machine learning to block malware, fileless attacks, ransomware, and other advanced threats. It also allows security teams to quickly investigate and remediate incidents, as well as hunt for indicators of compromise across all endpoints. Cisco AMP for Endpoints is part of the Cisco SecureX platform, which integrates with other Cisco security solutions to provide a unified and simplified security experience. The other options are not correct because they do not offer the same level of endpoint protection, detection, and response as Cisco AMP for Endpoints. Cisco AnyConnect is a VPN solution that provides secure access to the network for remote workers, but it does not monitor or respond to endpoint threats. Cisco Umbrella is a DNS security solution that blocks malicious domains, IPs, and URLs, but it does not analyze or remediate endpoint activity. Cisco Duo is a multi-factor authentication solution that verifies the identity of users and devices, but it does not protect or detect endpoint attacks. References :=

Some possible references are:

Cisco AMP for Endpoints

Cisco SecureX

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 - Module 5: Endpoint Protection and Detection

Questions # 39:

What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is

deleted from an identity group?

Options:

○ A.

posture assessment

○ B.

CoA

○ C.

external identity source

○ D.

SNMP probe

Answer

B

Explanation

Explanation

Explanation

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration

page that enables the profiling service with more control over endpoints that are already authenticated.

One of the settings to configure the CoA type is “Reauth”. This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.

[Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13

/b_ise_admin_guide_sample_chapter_010101.html,]

Questions # 40:

How does the Cisco WSA enforce bandwidth restrictions for web applications?

Options:

○ A.

It implements a policy route to redirect application traffic to a lower-bandwidth link.

○ B.

It dynamically creates a scavenger class QoS policy and applies it to each client that connects through the WSA.

○ C.

It sends commands to the uplink router to apply traffic policing to the application traffic.

○ D.

It simulates a slower link by introducing latency into application traffic.

Answer

D

Explanation

The Cisco WSA can enforce bandwidth restrictions for web applications by using the Application Visibility and Control (AVC) engine. The AVC engine allows the WSA to identify and control application activity on the network, and to apply bandwidth limits to certain application types or individual applications. The WSA dynamically creates a scavenger class QoS policy and applies it to each client that connects through the WSA. The scavenger class QoS policy assigns a low priority to the application traffic and limits the bandwidth usage based on the configured settings. This way, the WSA can prevent congestion and ensure fair allocation of bandwidth among different applications and users. References:

User Guide for AsyncOS 11.8 for Cisco Web Security Appliances - GD (General Deployment) - Managing Access to Web Applications

WSA - limit bandwidth - Cisco Community

Questions # 41:

What is a characteristic of traffic storm control behavior?

Options:

○ A.

Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level withinthe interval.

○ B.

Traffic storm control cannot determine if the packet is unicast or broadcast.

○ C.

Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.

○ D.

Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet isunicast or broadcast.

Answer

D

Explanation

Traffic storm control is a feature that prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces. Traffic storm control monitors the level of each traffic type for which it is enabled in 1-second intervals and compares it with the configured threshold, which is a percentage of the total available bandwidth of the port. When the ingress traffic reaches the threshold, traffic storm control drops the traffic until the end of the interval. Traffic storm control uses the Individual/Group bit in the packet destination address to determine if the packet is unicast or broadcast. This bit is set to 0 for unicast addresses and 1 for multicast or broadcast addresses. Traffic storm control does not use the source address to classify the traffic type. References := Configuring Traffic Storm Control - Cisco, Understanding Cisco Traffic Storm Control - NetCraftsmen

Questions # 42:

What is the purpose of a NetFlow version 9 template record?

Options:

○ A.

It specifies the data format of NetFlow processes.

○ B.

It provides a standardized set of information about an IP flow.

○ C.

It defines the format of data records.

○ D.

It serves as a unique identification number to distinguish individual data records

Answer

C

Explanation

A NetFlow version 9 template record is a record that contains information about the fields that will be present in the data records that follow the template. A template record consists of a template ID, a field count, and a list of field types and lengths. A template record is sent periodically by the NetFlow exporter to the NetFlow collector, so that the collector can parse and interpret the data records correctly. A template record can also be requested by the collector using an options template record. The purpose of a template record is to define the format of data records, which contain the actual information about the IP flows1234.

A. It specifies the data format of NetFlow processes. - This is incorrect, because a template record does not specify the data format of NetFlow processes, but rather the data format of data records. NetFlow processes are the functions that perform flow creation, aggregation, export, and analysis on the NetFlow device or the collector. B. It provides a standardized set of information about an IP flow. - This is incorrect, because a template record does not provide any information about an IP flow, but rather the information about the fields that will be present in the data records. The data records are the ones that provide the information about an IP flow, such as source and destination IP addresses, ports, protocols, bytes, packets, timestamps, and so on. C. It defines the format of data records. - This is correct, because a template record defines the format of data records by specifying the field types and lengths that will be present in the data records. A template record allows the NetFlow collector to parse and interpret the data records correctly, and

also enables the NetFlow exporter to use different formats for different types of flows. D. It serves as a unique identification number to distinguish individual data records. - This is incorrect, because a template record does not serve as a unique identification number, but rather as a description of the fields. A template record has a template ID, which is a 16-bit value that identifies the template record uniquely within an export packet, but this ID is not used to distinguish individual data records. The data records are distinguished by their position within the export packet and their association with a template record.

References := 1: NetFlow Version 9 Flow-Record Format [IP Application Services] - Cisco ... 2: NetFlow V9 formats - IBM 3: Netflow :: Version 9 - Caligare 4: NetFlow Versions > NetFlow for Cybersecurity | Cisco Press

CertsMania

Questions # 43:

What is a difference between GETVPN and IPsec?

Options:

○ A.

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

○ B.

GETVPN provides key management and security association management

○ C.

GETVPN is based on IKEv2 and does not support IKEv1

○ D.

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

CertsMania

Answer

C

Questions # 44:

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

Options:

○ A.

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

○ B.

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

○ C.

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

○ D.

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

Answer

D

Explanation

The login block-for command sets a limit on the maximum number of failed login attempts allowed within a defined period of time. If this limit is exceeded, no further logins are allowed for the specified period of time. This feature is designed to protect the router from denial-of-service and dictionary attacks. The syntax of the command is as follows:

login block-for attempts within

The parameter specifies the duration of the quiet period in seconds. The parameter specifies the number of failed attempts that trigger the quiet period. The parameter specifies the time window in seconds for counting the failed attempts.

In this question, the command login block-for 100 attempts 4 within 60 means that if four failures occur in 60 seconds, the router goes to quiet mode for 100 seconds. During the quiet period, no login attempts are accepted, and the router responds with the message “Login disabled for seconds due to too many failed login attempts.” After the quiet period expires, the router resumes normal login operations.

The other options are incorrect because they do not match the command syntax or the expected behavior of the login block-for feature.

References :=

Some possible references for this question are:

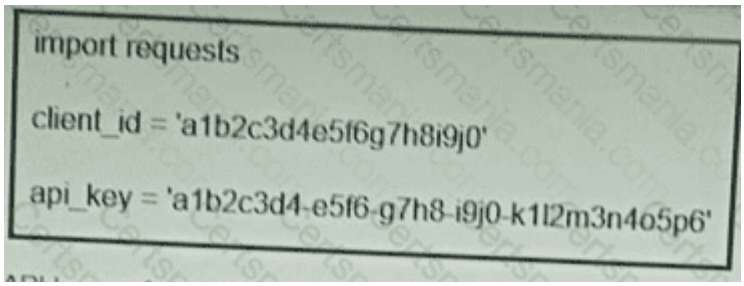
User Security Configuration Guide - Cisco IOS Login Enhancements-Login Block

Configuring Login Block

Restrict login attempts : login block-for command

When applied to a router, which command would help mitigate brute-force password attacks against the router?

Questions # 45:



Refer to the exhibit. What function does the API key perform while working with https://api.amp.cisco.com/v1/computers?

Options:

○ A.

imports requests

○ B.

HTTP authorization

○ C.

HTTP authentication

○ D.

plays dent ID

Answer

C

Explanation

The API key is a secret token that is used to authenticate the client to the server. It is functionally equivalent to a username and password, and should be treated as such. The API key is passed as part of the HTTP header in the request, using the Authorization: Basic scheme. The API key is combined with the client ID and encoded in base64 format. For example, if the client ID is d16aff14860af496e848 and the API key is d01ed435-b00d-4a4d-a299-1806ac117e72, the HTTP header would look like this:

Authorization: Basic ZDE2YWZmMTQ4NjBhZjQ5NmU4NDg6ZDAxZWQ0MzUtYjAwZC00YTRkLWEyOTktMTgwNmFjMTE3ZTcy

The server then decodes the header and verifies the credentials. If the credentials are valid, the server grants access to the requested resource. If the credentials are invalid, the server returns an HTTP 401 Unauthorized error.

The API key performs the function of HTTP authentication, which is the process of verifying the identity of the client. HTTP authentication is different from HTTP authorization, which is the process of determining the permissions of the client. HTTP authorization is based on the scope of the API credential, which can be either read-only or read & write. The scope determines what actions the client can perform on the Cisco AMP for Endpoints data.

Importing requests is not a function of the API key, but rather a Python module that allows sending HTTP requests. Playing dent ID is not a meaningful term in this context. Therefore, the correct answer is C. References:

Secure Endpoint API - Cisco DevNet

Overview of the Cisco AMP for Endpoints API - Cisco

Configure AMP for Endpoints Event Stream Feature - Cisco

Questions # 46:

When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

Options:

○ A.

Application Control

○ B.

Security Category Blocking

○ C.

Content Category Blocking

○ D.

File Analysis

CertsMania

Answer

B

Explanation

Cisco Umbrella groups harmful destinations into categories of security threat, such as Malware, Command Control Callbacks, Phishing Attacks, Dynamic DNS, Potentially Harmful Domains, DNS Tunneling VPN, and Cryptomining1. When web policies are configured in Cisco Umbrella, the security category blocking provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats. By enabling or disabling these categories, the administrator can control the identity access to these destinations and protect the network from malicious traffic2. References: 1: Security Categories - Umbrella User Guide 2: Manage Security Settings - Umbrella User Guide

Questions # 47:

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

CertsMania

Options:

○ A.

local WebAuth

○ B.

central WebAuth

○ C.

null WebAuth

○ D.

guest

○ E.

dual

Answer

B, D

Explanation

Cisco ISE supports two types of WebAuth for BYOD: central WebAuth and local WebAuth. Central WebAuth is the default method and it uses the ISE portal to authenticate the users and redirect them to the BYOD portal. Local WebAuth is an alternative method that uses the network access device (NAD) portal to authenticate the users and then redirects them to the ISE BYOD portal. Both methods require the configuration of a guest component on ISE, which is used to create the BYOD portal and the guest user accounts. The guest component also provides the self-service onboarding and registration features for the BYOD users. The dual component is not related to BYOD, but rather to the dual-SSID method, which uses two separate SSIDs for provisioning and access. The null WebAuth component is not a valid option for BYOD. References :=

Some possible references are:

Cisco ISE BYOD Prescriptive Deployment Guide

Configure Single SSID Wireless BYOD on Windows and ISE

Cisco ISE for BYOD and Secure Unified Access, 2nd Edition

Questions # 48:

Refer to the exhibit.

```
> show crypto ipsec sa
interface: Outside
    Crypto map tag: CSM_Outside_map, seq num: 1, local addr:
209.165.200.225

      access-list CSM_IPSEC_ACL_1 extended permit ip 10.0.11.0
255.255.255.0 10.0.10.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.0.11.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.0.10.0/255.255.255.0/0/0)
      current_peer: 209.165.202.129


      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 17
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp
failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.200.225/500, remote crypto endpt.:
209.165.202.129/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: B6F5EA53
      current inbound spi : 84348DEE
```

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

Options:

○ A.

No split-tunnel policy is defined on the Firepower Threat Defense appliance.

○ B.

The access control policy is not allowing VPN traffic in.

○ C.

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

○ D.

Site-to-site VPN preshared keys are mismatched.

Answer

A

Explanation

Explanation

Explanation

If sysopt permit-vpn is not enabled then an access control policy must be created to allow the VPN traffic through the FTD device. If sysopt permit-vpn is enabled skip creating an access control policy.

[Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html,]

Questions # 49:

What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?

Options:

○ A.

Telemetry uses a pull mehod, which makes it more reliable than SNMP

○ B.

Telemetry uses push and pull, which makes it more scalable than SNMP

○ C.

Telemetry uses push and pull which makes it more secure than SNMP

○ D.

Telemetry uses a push method which makes it faster than SNMP

Answer

D

Explanation

Explanation

SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts.

The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data.

Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc.

Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Referfence: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming telemetry

Questions # 50:

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

Options:

○ A.

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

○ B.

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

○ C.

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

○ D.

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

Answer

D

Explanation

The main difference between an on-premise solution and a cloud-based solution is the distribution of responsibilities between the customer and the provider. With an on-premise solution, the customer has full control over the installation, configuration, maintenance, and security of the product, but also bears the costs and risks associated with it. With a cloud-based solution, the provider takes care of most of these aspects, while the customer pays a subscription fee and accesses the product over the internet. Therefore, when choosing between the two options, the customer must consider factors such as cost, scalability, performance, availability, security, compliance, and customization. For example, an on-premise solution may be preferred if the customer has strict security or regulatory requirements, or needs a high level of customization. A cloud-based solution may be preferred if the customer wants to reduce capital expenditure, or needs a flexible and scalable solution that can adapt to changing demands. References :=

Some possible references are:

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Security Concepts, Lesson 1: Describing Information Security Concepts, Topic: Cloud Security

350-701 SCOR - Cisco, Exam Topics, 1.0 Security Concepts, 1.6 Compare and contrast the characteristics of a data center and the cloud

Cloud vs. On-Premise Software Comparison

Questions # 51:

Refer to the exhibit.

CertsMania

Interface	MAC Address	Method	Domain	Status	Fg	Session I
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth		0A021982000
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth		0A021982000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth		0A021982000
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth		0A021982000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth		0A021982000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth		0A021982000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth		0A021982000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth		0A021982000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth		0A021982000
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth		0A021982000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth		0A021982000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth		0A021982000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth		0A021982000
Gi7/4	54ee.75db.d766	dot1x	DATA	Auth		0A021982000
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth		0A021982000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth		0A021982000
Gi9/22	0007.b00c.8c35	mab	DATA	Auth		0A021982000

Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

Options:

○ A.

show authentication registrations

○ B.

show authentication method

○ C.

show dot1x all

○ D.

show authentication sessions

CertsMania

Answer

D

Explanation

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137

Displaying the Summary of All Auth Manager Sessions on the Switch

Enter the following:

Switch# show authentication sessions

Interface MAC Address Method Domain Status Session ID

Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C

Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58

Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

Questions # 52:

Which attribute has the ability to change during the RADIUS CoA?

Options:

○ A.

NTP

○ B.

Authorization

○ C.

Accessibility

○ D.

Membership

Answer

B

Explanation

Explanation

The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an

authentication, authorization, and accounting (AAA) session after it is authenticated.

[Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html,]

Questions # 53:

Which technology reduces data loss by identifying sensitive information stored in public computing

environments?

Options:

○ A.

Cisco SDA

○ B.

Cisco Firepower

○ C.

Cisco HyperFlex

○ D.

Cisco Cloudlock

Answer

D

Explanation

Cisco Cloudlock is a cloud-native security platform that provides data loss prevention (DLP) capabilities for public cloud environments, such as SaaS, IaaS, and PaaS. Cisco Cloudlock can discover, classify, and protect sensitive data stored in cloud applications, such as Office 365, Google Workspace, Salesforce, Dropbox, and AWS. Cisco Cloudlock uses advanced techniques, such as regular expressions, keywords, dictionaries, and machine learning, to identify and monitor data based on predefined or custom policies. Cisco Cloudlock can also enforce actions, such as encryption, quarantine,

deletion, or notification, to prevent data leakage or exposure12. References := 1: Cisco Cloudlock Data Sheet 2: Cloud Data Loss Prevention (Cloud DLP) Overview

Questions # 54:

Which Cisco ISE service checks the compliance of endpoints before allowing the endpoints to connect to

the network?

Options:

○ A.

posture

○ B.

profiler

○ C.

Cisco TrustSec

○ D.

Threat Centric NAC

Answer

A

Explanation

Posture is a service in Cisco ISE that allows you to check the compliance, also known as posture, of endpoints, before allowing them to connect to your network. A posture agent, such as the AnyConnect ISE Posture Agent or Network Admission Control (NAC) Agent, runs on the endpoint and collects information about the endpoint’s security posture, such as antivirus, antispyware, firewall, and patch status. The posture agent then communicates with the ISE server, which evaluates the posture information against the posture policy and determines the compliance state of the endpoint. Based on the compliance state, the ISE server can grant or deny network access to the endpoint, or apply remediation actions to bring the endpoint into compliance. Posture service is part of the ISE solution for network access control (NAC), which aims to secure the network from unauthorized or compromised endpoints. References:

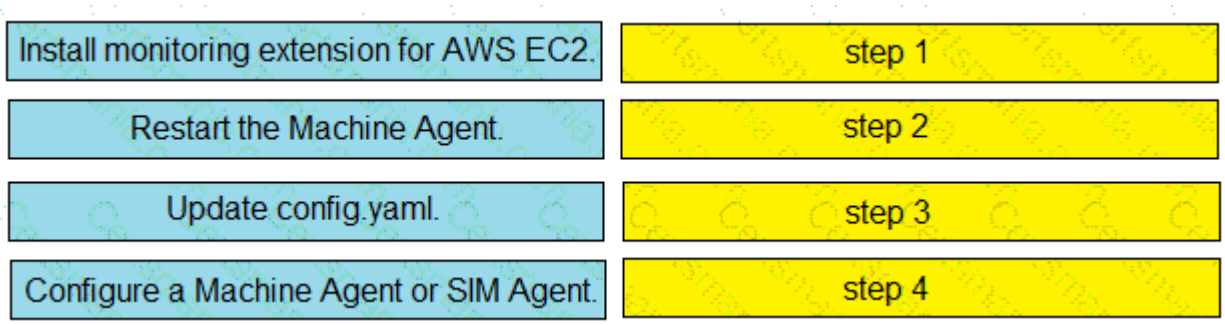
Cisco Identity Services Engine Administrator Guide, Release 2.2 - Configure Client Posture Policies

Configuring posture services with the Cisco Identity Services Engine - Cisco Community

Cisco Content Hub - Configure Client Posture Policies

Questions # 55:

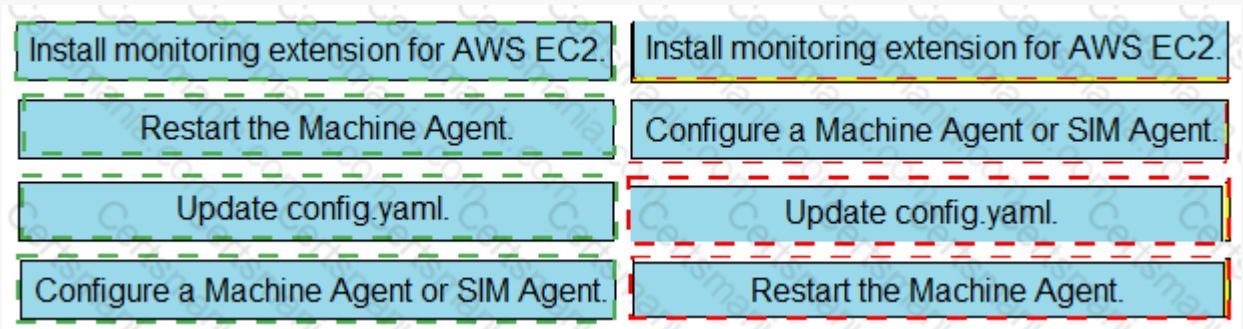
Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.



Options:

Answer

Answer:



Questions # 56:

What is a functional difference between Cisco AMP for Endpoints and Cisco Umbrella Roaming Client?

Options:

○ A.

The Umbrella Roaming client stops and tracks malicious activity on hosts, and AMP for Endpoints tracks only URL-based threats.

○ B.

The Umbrella Roaming Client authenticates users and provides segmentation, and AMP for Endpoints allows only for VPN connectivity

○ C.

AMP for Endpoints authenticates users and provides segmentation, and the Umbrella Roaming Client allows only for VPN connectivity.

○ D.

AMP for Endpoints stops and tracks malicious activity on hosts, and the Umbrella Roaming Client tracks only URL-based threats.

Answer

D

Explanation

Cisco AMP for Endpoints and Cisco Umbrella Roaming Client are both security solutions that protect mobile users from threats, but they have different functions and features. Cisco AMP for Endpoints is a cloud-managed endpoint security solution that stops and tracks malicious activity on hosts, such as malware execution, file behavior, and command-and-control callbacks. It also provides threat intelligence, sandboxing, and retrospective analysis to detect and respond to advanced threats. Cisco Umbrella Roaming Client is a lightweight DNS client that tracks only URL-based threats, such as phishing, ransomware, and botnets. It prevents connections to malicious domains and IP addresses, and provides visibility and enforcement for off-network devices. It also integrates with Cisco AnyConnect VPN client to provide seamless protection for VPN and non-VPN traffic. Therefore, the functional difference between Cisco AMP for Endpoints and Cisco Umbrella Roaming Client is that AMP for Endpoints stops and tracks malicious activity on hosts, and the Umbrella Roaming Client tracks only URL-based threats. References :=

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.1: Cisco AMP for Endpoints Overview

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.2: Cisco AMP for Endpoints Architecture and Components

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.3: Cisco AMP for Endpoints Installation and Configuration

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.4: Cisco AMP for Endpoints Analysis and Response

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.5: Cisco Umbrella Overview

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.6: Cisco Umbrella Architecture and Components

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.7: Cisco Umbrella Roaming Client

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Endpoint Protection and Detection, Lesson 3.8: Cisco Umbrella Policies and Reporting

Best Mobile Cybersecurity Solution - Cisco Umbrella

Questions # 57:

How does a cloud access security broker function?

Options:

○ A.

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

○ B.

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

○ C.

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

○ D.

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

Answer

B

Explanation

A cloud access security broker (CASB) is a security solution that helps protect cloud-hosted services and applications from cyberattacks and data breaches. A CASB acts as an intermediary between cloud users and cloud providers, and enforces the organization's security policies and compliance requirements. A CASB integrates with other cloud solutions via APIs and monitors the cloud activity and data across multiple platforms and devices. A CASB can also create incidents based on events from the cloud solution, such as unauthorized access, data leakage, malware infection, or policy violation. A CASB can then alert the administrators, block the malicious actions, or remediate the issues. A CASB provides visibility, control, and protection for the organization's cloud environment12.

References :=

What Is a Cloud Access Security Broker (CASB)? | Microsoft

What is a CASB Cloud Access Security Broker? - CrowdStrike

Questions # 58:

What are two ways that Cisco Container Platform provides value to customers who utilize cloud service providers? (Choose two.)

Options:

○ A.

Allows developers to create code once and deploy to multiple clouds

○ B.

helps maintain source code for cloud deployments

○ C.

manages Docker containers

○ D.

manages Kubernetes clusters

○ E.

Creates complex tasks for managing code

Answer

A, D

Explanation

Cisco Container Platform (CCP) is a solution that simplifies the deployment and management of containerized applications across multiple clouds. It provides the following benefits to customers who utilize cloud service providers12:

Allows developers to create code once and deploy to multiple clouds. CCP is based on open source components, such as Kubernetes and Docker, that are compatible with various cloud platforms. This enables developers to write code once and run it anywhere, without worrying about the underlying infrastructure or vendor lock-in. CCP also supports hybrid and multicloud scenarios, allowing customers to leverage the best features of different cloud providers and optimize their costs and performance.

Manages Kubernetes clusters. CCP automates the installation, configuration, and maintenance of Kubernetes clusters, which are groups of nodes that run containerized applications. CCP provides a simple GUI-driven menu system to deploy clusters, as well as automated monthly updates for bug fixes, feature enhancements, and security patches. CCP also offers a choice of networking solutions, such as Cisco ACI, Calico, or Contiv, to connect and secure the clusters. CCP also integrates with Cisco AppDynamics and Prometheus for visibility and monitoring of the clusters and applications. References:

Cisco Container Platform - Cisco

Cisco Container Platform - At-a-Glance - Cisco

CertsMania

Questions # 59:

An engineer is configuring cloud logging using a company-managed Amazon S3 bucket for Cisco Umbrella logs. What benefit does this configuration provide for accessing log data?

Options:

○ A.

It is included m the license cost for the multi-org console of Cisco Umbrella

○ B.

It can grant third-party SIEM integrations write access to the S3 bucket

○ C.

No other applications except Cisco Umbrella can write to the S3 bucket

○ D.

Data can be stored offline for 30 days.

Answer

B

Explanation

Using a company-managed Amazon S3 bucket for Cisco Umbrella logs allows the administrator to have full control over the access and lifecycle of the log data. This configuration can grant third-party SIEM integrations write access to the S3 bucket, which can enable more advanced analysis and correlation of the log data with other sources. This configuration also provides more flexibility in terms of how long the data can be stored offline, as opposed to the Cisco-managed S3 bucket, which has a fixed retention period of 30 days. References:

Enable Logging to Your Own S3 Bucket

Centralized Umbrella Log Management with Amazon’s S3 service for MSP, MSSP, and Multi-org customers

Questions # 60:

Which method of attack is used by a hacker to send malicious code through a web application to an unsuspecting user to request that the victim's web browser executes the code?

Options:

○ A.

buffer overflow

○ B.

browser WGET

○ C.

SQL injection

○ D.

cross-site scripting

Answer

D

Explanation

Cross-site scripting (XSS) is the method of attack that is used by a hacker to send malicious code through a web application to an unsuspecting user to request that the victim's web browser executes the code. XSS is a type of injection attack that exploits the lack of input validation or output encoding in a web application. An attacker can craft a malicious script and embed it in a web page or a URL that is sent to the user. When the user visits the web page or clicks the URL, the script is executed by the user's browser, which may not be able to distinguish it from legitimate code. The script can then perform various actions, such as stealing cookies, session tokens, or other sensitive information, redirecting the user to a malicious site, or performing actions on behalf of the user12. The other options are not correct, because they are not methods of attack that use web applications to execute malicious code on the user's browser. Buffer overflow is a type of attack that exploits a memory vulnerability in a program or system, where an attacker can overwrite the memory beyond the allocated buffer and execute arbitrary code3. Browser WGET is a command-line tool that can be used to download files from the web, but it is not an attack method by itself4. SQL injection is a type of attack that exploits a database vulnerability in a web application, where an attacker can inject malicious SQL statements into a user input field and execute them on the database server5. References:

1: What is Cross-Site Scripting (XSS)? - Cisco

2: Cross-Site Scripting (XSS) - OWASP

3: What is a Buffer Overflow? - Cisco

4: GNU Wget 1.21.1 Manual

5: What is SQL Injection (SQLi)? - Cisco

Questions # 61:

In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint Protection Platform?

Options:

○ A.

When there is a need to have more advanced detection capabilities

○ B.

When there is a need for traditional anti-malware detection

○ C.

When there is no need to have the solution centrally managed

○ D.

When there is no firewall on the network

Answer

A

Questions # 62:

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?

Options:

○ A.

records

○ B.

flow exporter

○ C.

flow sampler

○ D.

flow monitor

CertsMania

Answer

D

Explanation

A flow monitor is a component of Flexible NetFlow that is used to store and export flow data. A flow monitor consists of a record, an optional exporter, and a cache. The cache is a section of memory that stores flow entries before they are exported to an external collector. The cache is created by the flow monitor when NetFlow is applied to an interface. The cache collects traffic based on the key and nonkey fields in the configured record. The key fields are used to identify a flow uniquely, while the nonkey fields are used to provide additional information about the flow. The cache can be configured with various parameters, such as the number of entries, the timeout values, and the type of cache. The cache can also be viewed and cleared using show and clear commands. References :=

Some possible references are:

Flexible Netflow Configuration Guide, Cisco IOS Release 15M&T

ASR9000/XR Netflow Architecture and overview

Cisco IOS Flexible NetFlow Command Reference - cache (Flexible NetFlow) through match flow

CertsMania

Questions # 63:

A network engineer is deciding whether to use stateful or stateless failover when configuring two Cisco ASAs for high availability. What is the connection status in both cases?

Options:

○ A.

Need to be reestablished with both stateful and stateless failover

○ B.

Need to be reestablished with stateful failover and preserved with stateless failover

○ C.

Preserved with both stateful and stateless failover

○ D.

Preserved with stateful failover and need to be reestablished with stateless failover

Answer

D

CertsMania

CertsMania

To Get Premium Files for 350-701 Visit

https://www.certsmania.com/cisco/350-701-practice

For More Free Questions Visit

https://www.certsmania.com/cisco/pdf/350-701

CertsMania