Free Questions for 350-701 by go4braindumps

Shared by Aguilar on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which term describes when the Cisco Secure Firewall downloads threat intelligence updates from Cisco Tables?

Options:

A- analysis

B- sharing

C- authoring

D- consumption

Answer:

D

Explanation:

When the Cisco Secure Firewall downloads threat intelligence updates from Cisco Talos, it is engaged in 'consumption.' This term refers to the process of receiving and utilizing threat intelligence data to enhance security measures. Cisco Talos provides comprehensive threat intelligence that Cisco Secure Firewall consumes to update its threat detection and prevention capabilities.

Question 2

Question Type: MultipleChoice

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.

Question 3

Question Type: MultipleChoice

What must be configured on Cisco Secure Endpoint to create a custom detection tile list to detect and quarantine future files?

Options:

A- Use the simple custom detection feature and add each detection to the list.

B- Add a network IP block allowed list to the configuration and add the blocked files.

C- Create an advanced custom detection and upload the hash of each file

D- Configure an application control allowed applications list to block the files

Answer:

C

Explanation:

In Cisco Secure Endpoint, to create a custom detection file list for detecting and quarantining future files, an advanced custom detection should be created, and the hash of each file to be detected and quarantined should be uploaded. This allows the system to uniquely identify and take action on files based on their hash values, providing a precise method for targeting specific malicious or unwanted files.

Question 4

Question Type: MultipleChoice

A network administrator has configured TACACS on a network device using the key Cisc0467380030 tor authentication purposes. However, users are unable to authenticate. TACACS server is reachable, but authentication is tailing. Which configuration step must the administrator complete?

Options:

A- Implement synchronized system clock on TACACS server that matches the network device.

B- Install a compatible operating system version on the TACACS server.

C- Configure the TACACS key on the server to match with the network device.

D- Apply an access control list on TACACS server to allow communication with the network device.

Answer:

C

Explanation:

For TACACS authentication to work, the key configured on the network device must match the key configured on the TACACS server. If users are unable to authenticate despite the TACACS server being reachable, it is likely due to a mismatch in the keys. Ensuring that both the network device and the TACACS server have the same key configured is crucial for successful authentication.

Question 5

Question Type: MultipleChoice

What is a difference between GRE over IPsec and IPsec with crypto map?

Options:

A- Multicast traffic is supported by IPsec with crypto map.

B- GRE over IPsec supports non-IP protocols.

C- GRE provides its own encryption mechanism.

D- IPsec with crypto map oilers better scalability.

Answer:

B

Explanation:

The difference between GRE over IPsec and IPsec with crypto map is that GRE (Generic Routing Encapsulation) over IPsec can encapsulate and transport non-IP protocols across an IP network, whereas IPsec with crypto map is typically used for IP traffic. GRE tunnels wrapped in IPsec provide a way to transport multicast traffic and other protocol types across an IPsec VPN, offering greater flexibility in the types of traffic that can be secured.

Question 6

Question Type: MultipleChoice

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

Options:

A- ADC

B- ERSPAN

C- Cisco ASA

D- NetFlow

E- Cisco Secure Workload

Answer:

D, E

Explanation:

In a Cisco Secure Workload implementation, telemetry data can be generated from IPFIX (Internet Protocol Flow Information Export) records using NetFlow connectors and Cisco Secure Workload itself. NetFlow provides insights into network traffic flow and volume, while Cisco Secure Workload uses this data for visibility, segmentation, and security analytics within the data center.

Question 7

Question Type: MultipleChoice

Which two devices support WCCP for traffic redirection? (Choose two.)

Options:

A- Cisco Secure Web Appliance

B- Cisco IOS

C- proxy server

D- Cisco ASA

E- Cisco IPS

Answer:

B, D

Explanation:

Web Cache Communication Protocol (WCCP) is supported on Cisco IOS routers and Cisco ASA firewalls. WCCP allows these devices to redirect traffic to a WCCP-capable device, such as a web cache or a Cisco Secure Web Appliance, for processing. This redirection

can be used for tasks like content filtering, web caching, and load balancing.

Question 8

Question Type: MultipleChoice

Which technology must De used to Implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

Options:

A- GET VPN

B- IPsec DVTI

C- DMVPN

D- FlexVPN

Answer:

A

Explanation:

Group Encrypted Transport VPN (GET VPN) is used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity. GET VPN provides a way to encrypt traffic between sites without the need for point-to-point tunnels, supporting efficient, scalable, and secure communication across a broad network infrastructure.

Question 9

Question Type: MultipleChoice

Which method must be used to connect Cisco Secure Workload to external orchestrators at a client site when the client does not allow incoming connections?

Options:

A- source NAT

B- reverse tunnel

C- GRE tunnel

D- destination NAT

Answer:

B

Explanation:

To connect Cisco Secure Workload to external orchestrators at a client site where incoming connections are not allowed, a reverse tunnel must be used. A reverse tunnel initiates the connection from the inside of the client's network out to the external orchestrator, thereby bypassing restrictions on incoming connections and enabling secure communication.