Free Questions for 300-710 by go4braindumps

Shared by Frederick on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Due to an Increase in malicious events, a security engineer must generate a threat report to include intrusion in events, malware events, and security intelligence events. How Is this information collected in a single report?

Options:

A- Run the default Firepower report.

B- Export the Attacks Risk report.

C- Generate a malware report.

D- Create a Custom report.

Answer:

D

Question 2

Question Type: MultipleChoice

A network administrator registered a new FTD to an existing FMC. The administrator cannot place the FTD in transparent mode. Which action enables transparent mode?

Options:

A- Add a Bridge Group Interface to the FTD before transparent mode is configured.

B- Dereglster the FTD device from FMC and configure transparent mode via the CLI.

C- Obtain an FTD model that supports transparent mode.

D- Assign an IP address to two physical interfaces.

Answer:

B

Question 3

Question Type: **MultipleChoice**

A network administrator is configuring an FTD in transparent mode. A bridge group is set up and an access policy has been set up to allow all IP traffic. Traffic is not passing through the FTD. What additional configuration is needed?

Options:

A- The security levels of the interfaces must be set.

B- A default route must be added to the FTD.

C- An IP address must be assigned to the BVI.

D- A mac-access control list must be added to allow all MAC addresses.

Answer:

C

Question 4

Question Type: MultipleChoice

A network engineer must provide redundancy between two Cisco FTD devices. The redundancy configuration must include automatic configuration, translation, and connection updates. After the initial configuration of the two appliances, which two steps must be taken to proceed with the redundancy configuration? (Choose two.)

Options:

A- Configure the virtual MAC address on the failover link.

B- Disable hellos on the inside interface.

C- Configure the standby IP addresses.

D- Ensure the high availability license is enabled.

E- Configure the failover link with stateful properties.

Answer:

A, C

Question 5

Question Type: **MultipleChoice**

A network administrator is configuring a Cisco AMP public cloud instance and wants to capture infections and polymorphic variants of a threat to help detect families of malware. Which detection engine meets this requirement?

Options:

A- RBAC

B- Tetra

C- Ethos

D- Spero

Answer:

C

Question 6

Question Type: MultipleChoice

The network administrator wants to enhance the network security posture by enabling machine learning tor malware detection due to a concern with suspicious Microsoft executable file types that were seen while creating monthly security reports for the CIO. Which feature must be enabled to accomplish this goal?

Options:

A- Spero

B- dynamic analysis

C- static analysis

D- Ethos

Answer:

A

Question 7

Question Type: **MultipleChoice**

A security engineer must configure a Cisco FTD appliance to inspect traffic coming from the internet. The Internet traffic will be mirrored from the Cisco Catalyst 9300 Switch. Which configuration accomplishes the task?

Options:

A- Set interface configuration mode to none.

B- Set the firewall mode to transparent.

C- Set the firewall mode to routed.

D- Set interface configuration mode to passive.

Answer:

D

Question 8

Question Type: MultipleChoice

Refer to the exhibit.

```
Phase: 16
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Firewall: starting rule matching, zone 4 -> 1, geo 0 -> 0, vlan 0, sgt 0, src sgt type 0, dest_sgt_tag 0, dest sgt type 0, username 'No Authentication Required', , icmpType 8, icmpCode 0
Firewall: block rule,  'Ping' , drop
Snort: processed decoder alerts or actions queue, drop
Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST, Blocked by Firewall
Snort Verdict: (black-list) black list this flow

Result:
input-interface: ACCESS41_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame 0x000055d2b0f8b7e0 flow (NA)/NA
```

A systems administrator conducts a connectivity test to their SCCM server from a host machine and gets no response from the server. Which action ensures that the ping packets reach the destination and that the host receives replies?

Options:

A- Create an access control policy rule that allows ICMP traffic.

B- Configure a custom Snort signature to allow ICMP traffic after Inspection.

C- Modify the Snort rules to allow ICMP traffic.

D- Create an ICMP allow list and add the ICMP destination to remove it from the implicit deny list.

Answer:

A

Question 9

Question Type: **MultipleChoice**

A security engineer is deploying a pair of primary and secondary Cisco FMC devices. The secondary must also receive updates from Cisco Talos. Which action achieves this goal?

Options:

A- Force failover for the secondary Cisco FMC to synchronize the rule updates from the primary.

B- Configure the secondary Cisco FMC so that it receives updates from Cisco Talos.

C- Manually import rule updates onto the secondary Cisco FMC device.

D- Configure the primary Cisco FMC so that the rules are updated.

Answer:

D

Question 10

Question Type: **MultipleChoice**

Which feature is supported by IRB on Cisco FTD devices?

Options:

A- redundant interface

B- dynamic routing protocol

C- EtherChannel interface

D- high-availability cluster

Answer:

B

Question 11

Question Type: MultipleChoice

What is the RTC workflow when the infected endpoint is identified?

Options:

A- Cisco ISE instructs Cisco AMP to contain the infected endpoint.

B- Cisco ISE instructs Cisco FMC to contain the infected endpoint.

C- Cisco AMP instructs Cisco FMC to contain the infected endpoint.

D- Cisco FMC instructs Cisco ISE to contain the infected endpoint.

Answer:

D

Question 12

Question Type: MultipleChoice

A network administrator is trying to convert from LDAP to LDAPS for VPN user authentication on a Cisco FTD. Which action must be taken on the Cisco FTD objects to accomplish this task?

Options:

A- Add a Key Chain object to acquire the LDAPS certificate.

B- Create a Certificate Enrollment object to get the LDAPS certificate needed.

C- Identify the LDAPS cipher suite and use a Cipher Suite List object to define the Cisco FTD connection requirements.

D- Modify the Policy List object to define the session requirements for LDAPS.

Answer:

B