



Free Questions for 300-710 by dumpshq

Shared by Houston on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An engineer wants to perform a packet capture on the Cisco FTD to confirm that the host using IP address 192.168.100.100 has the MAC address of 0042.7734.103 to help troubleshoot a connectivity issue. What is the correct tcpdump command syntax to ensure that the MAC address appears in the packet capture output?

Options:

- A- `-nm src 192.168.100.100`
- B- `-ne src 192.168.100.100`
- D- `-w capture.pcap -s 1518 host 192.168.100.100 mac`
- D- `-w capture.pcap -s 1518 host 192.168.100.100 ether`

Answer:

B

Question 2

Question Type: MultipleChoice

Refer to the exhibit. An engineer is analyzing a Network Risk Report from Cisco FMC. Which application must the engineer take immediate action against to prevent unauthorized network use?

Options:

- A- Kerberos
- B- YouTube
- C- Chrome
- D- TOR

Answer:

D

Question 3

Question Type: DragDrop

Drag and drop the configuration steps from the left into the sequence on the right to enable external authentication on Cisco FMC to a RADIUS server.

Select Authentication Method and RADIUS.

step 1

Answer:

Configure the primary and secondary servers and user roles.

step 2

Question 4

Configure External Authentication.

step 3

Question Type: MultipleChoice

Add External Authentication Object.

step 4

An engineer must deploy a Cisco FTD appliance via Cisco FMC to span a network segment to detect malware and threats. When setting the Cisco FTD interface mode, which sequence of actions meets this requirement?

Options:

- A- Set to passive, and configure an access control policy with an intrusion policy and a file policy defined
- B- Set to passive, and configure an access control policy with a prefilter policy defined
- C- Set to none, and configure an access control policy with a prefilter policy defined
- D- Set to none, and configure an access control policy with an intrusion policy and a file policy defined

Answer:

A

Question 5

Question Type: MultipleChoice

An organization is configuring a new Cisco Firepower High Availability deployment. Which action must be taken to ensure that failover is as seamless as possible to end users?

Options:

- A- Set up a virtual failover MAC address between chassis.
- B- Use a dedicated stateful link between chassis.
- C- Load the same software version on both chassis.
- D- Set the same FQDN for both chassis.

Answer:

B

Question 6

Question Type: MultipleChoice

A network administrator wants to block traffic to a known malware site at <https://www.badsite.com> and all subdomains while ensuring no packets from any internal client are sent to that site. Which type of policy must the network administrator use to accomplish this goal?

Options:

- A- Prefilter policy
- B- SSL policy
- C- DNS policy
- D- Access Control policy with URL filtering

Answer:

D

Question 7

Question Type: MultipleChoice

A company is deploying intrusion protection on multiple Cisco FTD appliances managed by Cisco FMC. Which system-provided policy must be selected if speed and detection are priorities?

Options:

- A- Connectivity Over Security
- B- Security Over Connectivity
- C- Maximum Detection
- D- Balanced Security and Connectivity

Answer:

D

Question 8

Question Type: MultipleChoice

A security engineer must integrate an external feed containing STIX/TAXII data with Cisco FMC. Which feature must be enabled on the Cisco FMC to support this connection?

Options:

- A- Cisco Success Network
- B- Cisco Secure Endpoint Integration
- C- Threat Intelligence Director
- D- Security Intelligence Feeds

Answer:

C

Question 9

Question Type: MultipleChoice

When using Cisco Threat Response, which phase of the Intelligence Cycle publishes the results of the investigation?

Options:

- A- direction

B- dissemination

C- processing

D- analysis

Answer:

B

Explanation:

Disseminate: The dissemination phase publishes the results of the investigation or threat hunt. This information is disseminated with a focus on the receivers of the information. At the tactical level, this information feeds back into the beginning of the F3EAD model, Find. Figure 3 illustrates the F3EAD model.

To Get Premium Files for 300-710 Visit

<https://www.p2pexams.com/products/300-710>

For More Free Questions Visit

<https://www.p2pexams.com/cisco/pdf/300-710>

