Free Questions for 300-710 by certsinside

Shared by Craig on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An engainer must add DNS-specific rules to me Cisco FTD intrusion policy. The engineer wants to use the rules currently in the Cisco FTD Snort database that are not already enabled but does not want to enable more than are needed. Which action meets these requirements?

Options:

A- Change the dynamic state of the rule within the policy.

B- Change the base policy to Security over Connectivity.

C- Change the rule state within the policy being used.

D- Change the rules using the Generate and Use Recommendations feature.

Answer:

C

Question 2

Question Type: MultipleChoice

An administrator Is setting up a Cisco PMC and must provide expert mode access for a security engineer. The engineer Is permitted to use only a secured out-of-band network workstation with a static IP address to access the Cisco FMC. What must be configured to enable this access?

Options:

A- Enable SSH and define an access list.

B- Enable HTTP and define an access list.

C- Enable SCP under the Access List section.

D- Enable HTTPS and SNMP under the Access List section.

Answer:

A

Question 3

Question Type: MultipleChoice

A company is in the process of deploying intrusion protection with Cisco FTDs managed by a Cisco FMC. Which action must be selected to enable fewer rules detect only critical conditions and avoid false positives?

Options:

A- Connectivity Over Security

B- Balanced Security and Connectivity

C- Maximum Detection

D- No Rules Active

Answer:

A

Question 4

Question Type: **MultipleChoice**

An engineer is investigating connectivity problems on Cisco Firepower for a specific SGT. Which command allows the engineer to capture real packets that pass through the firewall using an SGT of 64?

Options:

A- capture CAP type inline-tag 64 match ip any any

B- capture CAP match 64 type inline-tag ip any any

C- capture CAP headers-only type inline-tag 64 match ip any any

D- capture CAP buffer 64 match ip any any

Answer:

A

Question 5

Question Type: MultipleChoice

Which Cisco FMC report gives the analyst information about the ports and protocols that are related to the configured sensitive network for analysis?

Options:

A- Malware Report

B- Host Report

C- Firepower Report

D- Network Report

Answer:

D

Question 6

Question Type: MultipleChoice

The CEO ask a network administrator to present to management a dashboard that shows custom analysis tables for the top DNS queries URL category statistics, and the URL reputation statistics.

Which action must the administrator take to quickly produce this information for management?

Options:

A- Run the Attack report and filter on DNS to show this information.

B- Create a new dashboard and add three custom analysis widgets that specify the tables needed.

C- Modify the Connection Events dashboard to display the information in a view for management.

D- Copy the intrusion events dashboard tab and modify each widget to show the correct charts.

Answer:

B

Question 7

Question Type: MultipleChoice

A network administrator is migrating from a Cisco ASA to a Cisco FTD.

EIGRP is configured on the Cisco ASA but it is not available in the Cisco FMC.

Which action must the administrator take to enable this feature on the Cisco FTD?

Options:

A- Configure EIGRP parameters using FlexConfig objects.

B- Add the command feature eigrp via the FTD CLI.

C- Create a custom variable set and enable the feature in the variable set.

D- Enable advanced configuration options in the FMC.

Answer:

A

Question 8

Question Type: MultipleChoice

An organization recently implemented a transparent Cisco FTD in their network.

They must ensure that the device does not respond to insecure SSL/TLS protocols.

Which action accomplishes the task?

Options:

A- Modify the device's settings using the device management feature within Cisco FMC to force only secure protocols.

B- Use the Cisco FTD platform policy to change the minimum SSL version on the device to TLS 1.2.

C- Enable the UCAPL/CC compliance on the device to support only the most secure protocols available.

D- Configure a FlexConfig object to disable any insecure TLS protocols on the Cisco FTD device.

Answer:

B

Question 9

Question Type: MultipleChoice

A network administrator cannot select the link to be used for failover when configuring an active/passive HA Cisco FTD pair.

Which configuration must be changed before setting up the high availability pair?

Options:

A- An IP address in the same subnet must be added to each Cisco FTD on the interface.

B- The interface name must be removed from the interface on each Cisco FTD.

C- The name Failover must be configured manually on the interface on each cisco FTD.

D- The interface must be configured as part of a LACP Active/Active EtherChannel.

Answer:

A