Free Questions for 300-710 by ebraindumps

Shared by Johns on 05-09-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit An engineer is modifying an access control pokey to add a rule to inspect all DNS traffic that passes through the firewall After making the change and deploying the pokey they see that DNS traffic is not bang inspected by the Snort engine What is the problem?

Options:

A) The rule must specify the security zone that originates the traffic

B) The rule must define the source network for inspection as well as the port

C) The action of the rule is set to trust instead of allow.

D) The rule is configured with the wrong setting for the source port

Answer:

C

Question 2

Question Type: MultipleChoice

An engineer is vorlang on a LAN switch and has noticed that its network connection to the mime Cisco IPS has gone down Upon troubleshooting it is determined that the switch is working as expected What must have been implemented for this failure to occur?

Options:

A) The upstream router has a misconfigured routing protocol

B) Link-state propagation is enabled

C) The Cisco IPS has been configured to be in fail-open mode

D) The Cisco IPS is configured in detection mode

Answer:

D

Question 3

Question Type: MultipleChoice

In a multi-tenant deployment where multiple domains are in use. which update should be applied outside of the Global Domain?

Options:

A) minor upgrade

B) local import of intrusion rules

C) Cisco Geolocation Database

D) local import of major upgrade

Answer:

C

Question 4

Question Type: **MultipleChoice**

An engineer configures an access control rule that deploys file policy configurations to security zones, and it cause the device to restart. What is the reason for the restart?

Options:

A) Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.

B) The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.

C) Source or destination security zones in the source tunnel zone do not match the security zones that are associated with interfaces on the target devices.

D) The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.

Answer:

A

Question 5

Question Type: **MultipleChoice**

An engineer is vorlang on a LAN switch and has noticed that its network connection to the mime Cisco IPS has gone down Upon troubleshooting it is determined that the switch is working as expected What must have been implemented for this failure to occur?

Options:

A) The upstream router has a misconfigured routing protocol

B) Link-state propagation is enabled

C) The Cisco IPS has been configured to be in fail-open mode

D) The Cisco IPS is configured in detection mode

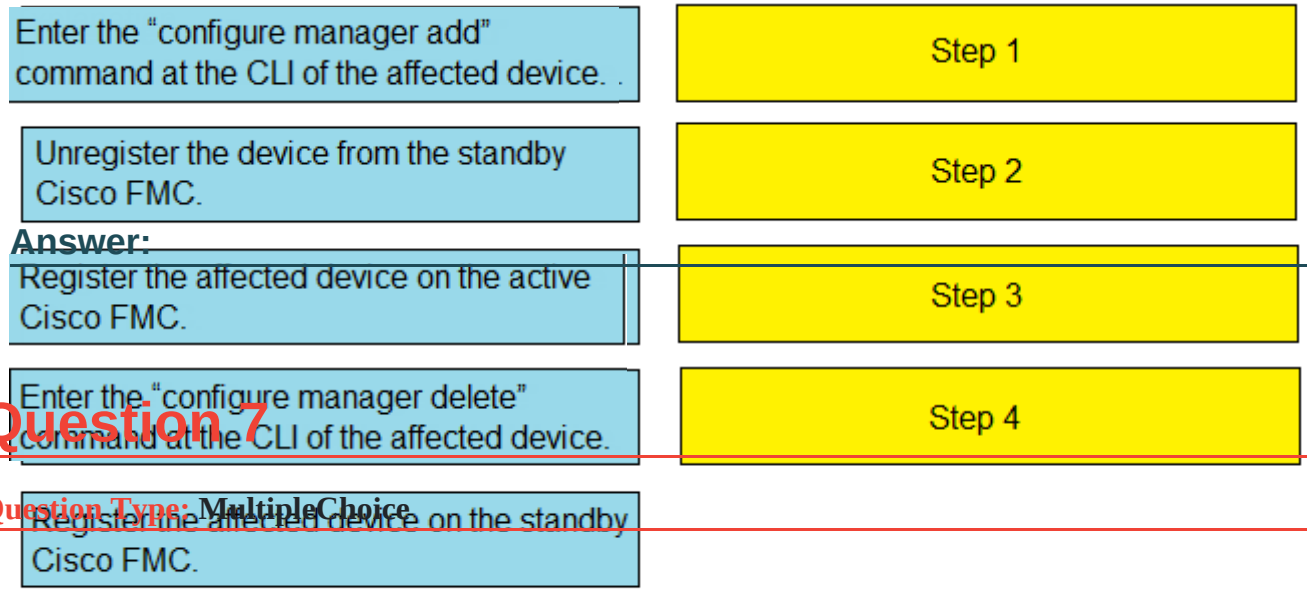
Answer:

D

Question 6

Question Type: **DragDrop**

Drag and drop the steps to restore an automatic device registration failure on the standby Cisco FMC from the left into the correct order on the right. Not all options are used.



Answer:

Question 7

Question Type: MultipleChoice

An engineer is attempting to create a new dashboard within the Cisco FMC to have a single view with widgets from many of the other dashboards. The goal is to have a mixture of threat and security related widgets along with Cisco Firepower device health information Which two widgets must be configured to provide this information? (Choose two.)

Options:

A) Intrusion Events

B) Correlation Information

C) Appliance Status

D) Current Sessions

E) Network Compliance

Answer:

A, B

Question 8

Question Type: MultipleChoice

An organization has implemented Cisco Firepower without IPS capabilities and now wants to enable inspection for their traffic. They need to be able to detect protocol anomalies and utilize the Snort rule sets to detect malicious behavior. How is this accomplished?

Options:

A) Modify the network discovery policy to detect new hosts to inspect.

B) Modify the access control policy to redirect interesting traffic to the engine.

C) Modify the intrusion policy to determine the minimum severity of an event to inspect.

D) Modify the network analysis policy to process the packets for inspection.

Answer:

D

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdmintrusion.

Html

Question 9

Question Type: MultipleChoice

An engineer configures an access control rule that deploys file policy configurations to security zone or tunnel zones, and it causes the device to restart. What is the reason for the restart?

Options:

A) Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.

B) The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.

C) Source or destination security zones in the source tunnel zone do not match the security zones that are associated with interfaces on the target devices.

D) The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.

Answer:

A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/policy_management.html

Question 10

Question Type: MultipleChoice

Refer to the exhibit An engineer is modifying an access control pokey to add a rule to inspect all DNS traffic that passes through the firewall After making the change and deploying the pokey they see that DNS traffic is not bang inspected by the Snort engine What is the

problem?

Options:

A) The rule must specify the security zone that originates the traffic

B) The rule must define the source network for inspection as well as the port

C) The action of the rule is set to trust instead of allow.

D) The rule is configured with the wrong setting for the source port

Answer:

C