300-710Q&As

Securing Networks with Cisco Firepower (SNCF)

Pass Cisco 300-710 Exam with 100% Guarantee

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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?

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.

Correct Answer: A

Reference: https://community.cisco.com/t5/network-security/adding-eigrp-to-ftd-using-fmc/td-p/4284529

QUESTION 2

A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface. What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

A. The output format option for the packet logs is unavailable.

B. Only the UDP packet type is supported.

C. The destination MAC address is optional if a VLAN ID value is entered.

D. The VLAN ID and destination MAC address are optional.

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

QUESTION 3

An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down. What must be configured to accomplish this task?

A. redundant interfaces on the firewall cluster mode and switches

B. redundant interfaces on the firewall noncluster mode and switches

C. vPC on the switches to the interface mode on the firewall duster

D. vPC on the switches to the span EtherChannel on the firewall cluster

Correct Answer: D

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKSEC-2020.pdf

QUESTION 4

Which default action setting in a Cisco FTD Access Control Policy allows all traffic from an undefined application to pass without Snort Inspection?

A. Trust All Traffic

B. Inherit from Base Policy

C. Network Discovery Only

D. Intrusion Prevention

Correct Answer: A

The default action setting in a Cisco FTD Access Control Policy determines how the system handles and logs traffic that is not handled by any other access control configuration. The default action can block or trust all traffic without further inspection, or inspect traffic for intrusions and discovery data3. The Trust All Traffic option allows all traffic from an undefined application to pass without Snort inspection. This option also disables Security Intelligence filtering, file and malware inspection, and URL filtering for all traffic handled by the default action. This option is useful when you want to minimize the performance impact of access control on your network3. The other options are incorrect because: The Inherit from Base Policy option inherits the default action setting from the base policy. The base policy is the predefined access control policy that you use as a starting point for creating your own policies. Depending on which base policy you choose, the inherited default action setting can be different3. The Network Discovery Only option inspects all traffic for discovery data only. This option enables Security Intelligence filtering for all traffic handled by the default action, but disables file and malware inspection, URL filtering, and intrusion inspection. This option is useful when you want to collect information about your network before you configure access control rules3. The Intrusion Prevention option inspects all traffic for intrusions and discovery data. This option enables Security Intelligence filtering, file and malware inspection, URL filtering, and intrusion inspection for all traffic handled by the default action. This option provides the most comprehensive protection for your network, but also has the most performance impact3.

QUESTION 5

Which Cisco Firepower feature is used to reduce the number of events received in a period of time?

A. rate-limiting

B. suspending

C. correlation

D. thresholding

Correct Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Global-Threshold.html