300-710Q&As

Securing Networks with Cisco Firepower (SNCF)

Pass Cisco 300-710 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/300-710.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

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.

Correct Answer: D

QUESTION 2

An engineer wants to connect a single IP subnet through a Cisco FTD firewall and enforce policy. There is a requirement to present the internal IP subnet to the outside as a different IP address. What must be configured to meet these requirements?

A. Configure the downstream router to perform NAT.

B. Configure the upstream router to perform NAT.

C. Configure the Cisco FTD firewall in routed mode with NAT enabled.

D. Configure the Cisco FTD firewall in transparent mode with NAT enabled.

Correct Answer: C

QUESTION 3

A network administrator configured a NAT policy that translates a public IP address to an internal web server IP address. An access policy has also been created that allows any source to reach the public IP address on port 80. The web server is still not reachable from the Internet on port 80.

Which configuration change is needed?

A. The intrusion policy must be disabled for port 80.

B. The access policy rule must be configured for the action trust.

C. The NAT policy must be modified to translate the source IP address as well as destination IP address.

D. The access policy must allow traffic to the internal web server IP address.

Correct Answer: D

QUESTION 4

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?

A. Cisco Success Network

B. Cisco Secure Endpoint Integration

C. Threat Intelligence Director

D. Security Intelligence Feeds

Correct Answer: C

QUESTION 5

An organization created a custom application that is being flagged by Cisco Secure Endpoint. The application must be exempt from being flagged. What is the process to meet the requirement?

A. Configure the custom application to use the information-store paths.

B. Add the custom application to the DFC list and update the policy.

C. Precalculate the hash value of the custom application and add it to the allowed applications.

D. Modify the custom detection list to exclude the custom application.

Correct Answer: C

To exempt a custom application from being flagged by Cisco Secure Endpoint, the organization must precalculate the hash value of the custom application and add it to the allowed applications list. This process involves creating a hash of the

executable file, which uniquely identifies it, and then configuring Cisco Secure Endpoint to recognize this hash as trusted.

Steps:

Calculate the hash value (e.g., SHA-256) of the custom application executable. In the Cisco Secure Endpoint management console, navigate to the policy configuration.

Add the calculated hash value to the list of allowed applications or exclusions.

Save and deploy the updated policy.

By adding the hash value to the allowed applications, Cisco Secure Endpoint will recognize the custom application as trusted and will no longer flag it. References: Cisco Secure Endpoint User Guide, Chapter on Policy Configuration and

Application Whitelisting.

QUESTION 6

A network engineer wants to add a third-party threat feed into the Cisco FMC for enhanced threat detection. Which action should be taken to accomplish this goal?

A. Enable Rapid Threat Containment using REST APIs.

B. Enable Rapid Threat Containment using STIX and TAXII.

C. Enable Threat Intelligence Director using REST APIs.

D. Enable Threat Intelligence Director using STIX and TAXII.

Correct Answer: D

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

QUESTION 7

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?

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.

Correct Answer: B

QUESTION 8

An engineer is tasked with configuring a custom intrusion rule on Cisco Secure Firewall Management Center to detect and block the malicious traffic pattern with specific payload containing string "|04 68 72 80 87 ff ed cq fg he qm pn|". Which action must the Engineer configure on the IPS policy?

A. reset

B. drop

C. alert

D. disable

E. quarantine

Correct Answer: B

QUESTION 9

After using Firepower for some time and learning about how it interacts with the network, an administrator is trying to correlate malicious activity with a user. Which widget should be configured to provide this visibility on the Cisco Firepower Dashboards?

A. Custom analysis.

B. Current Status

C. Current Sessions

D. Correlation Events

Correct Answer: C

QUESTION 10

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.)

A. Intrusion Events

B. Correlation Information

C. Appliance Status

D. Current Sessions

E. Network Compliance

Correct Answer: AC

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/dashboards.html#ID-2206-00000283

QUESTION 11

A network administrator is configuring SNORT inspection policies and is seeing failed deployment messages in Cisco FMC. What information should the administrator generate for Cisco TAC to help troubleshoot?

A. A "troubleshoot" file for the device in question.

B. A "show tech" file for the device in question.

C. A "troubleshoot" file for the Cisco FMC.

D. A "show tech" for the Cisco FMC.

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 12

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?

A. Ethos

B. Tetra

C. RBAC

D. Spero

Correct Answer: A

QUESTION 13

What is the maximum bit size that Cisco FMC supports for HTTPS certificates?

A. 1024

B. 8192

C. 4096

D. 2048

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/system_configuration.html

QUESTION 14

An organization wants to secure traffic from their branch office to the headquarters building using Cisco Firepower devices. They want to ensure that their Cisco Firepower devices are not wasting resources on inspecting the VPN traffic. What must be done to meet these requirements?

A. Configure the Cisco Firepower devices to bypass the access control policies for VPN traffic.

B. Tune the intrusion policies in order to allow the VPN traffic through without inspection.

C. Configure the Cisco Firepower devices to ignore the VPN traffic using prefilter policies.

D. Enable a flexconfig policy to re-classify VPN traffic so that it no longer appears as interesting traffic.

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-ravpn.html

QUESTION 15

A network engineer must configure an existing firewall to have a NAT configuration. The new configuration must support more than two interfaces per context. The firewall has previously been operating in transparent mode. The Cisco Secure Firewall Threat Defense (FTD) device has been deregistered from Cisco Secure Firewall Management Center (FMC). Which set of configuration actions must the network engineer take next to meet the requirements?

A. Run the configure firewall routed command from the Secure FTD device CLI, and reregister with Secure FMC.

B. Run the configure manager add routed command from the Secure FMC CLI. and reregister with Secure FMC.

C. Run the configure manager add routed command from the Secure FTD device CLI, and reregister with Secure FMC.

D. Run the configure firewall routed command from the Secure FMC CLI. and reregister with Secure FMC.

Correct Answer: A

To support more than two interfaces per context and enable NAT configurations, the firewall must operate in routed mode. Since the firewall was previously in transparent mode, the network engineer needs to change it to routed mode.

Steps:

Access the CLI of the Secure FTD device.

Run the command configure firewall routed to switch the firewall from transparent mode to routed mode.

Reregister the FTD device with the FMC by running the configure manager add command from the FTD device CLI. This will ensure that the firewall can support the required NAT configurations and more than

two interfaces per context.

References: Cisco Secure Firewall Management Center Device Configuration Guide, Chapter on Routed Mode Configuration.