300-710 Q&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.passapply.com/300-710.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What is a behavior of a Cisco FMC database purge?

A. User login and history data are removed from the database if the User Activity check box is selected.

B. Data can be recovered from the device.

C. The appropriate process is restarted.

D. The specified data is removed from Cisco FMC and kept for two weeks.

Correct Answer: C

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

QUESTION 2

A network administrator is configuring a site-to-site IPsec VPN to a router sitting behind a Cisco FTD. The administrator has configured an access policy to allow traffic to this device on UDP 500, 4500, and ESP VPN traffic is not working. Which action resolves this issue?

A. Set the allow action in the access policy to trust.

B. Enable IPsec inspection on the access policy.

C. Modify the NAT policy to use the interface PAT.

D. Change the access policy to allow all ports.

Correct Answer: B

QUESTION 3

Which two packet captures does the FTD LINA engine support? (Choose two.)

A. Layer 7 network ID

B. source IP

C. application ID

D. dynamic firewall importing

E. protocol

Correct Answer: BE

Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

QUESTION 4

An engineer is troubleshooting connectivity to the DNS servers from hosts behind a new Cisco FTD device. The hosts cannot send DNS queries to servers in the DMZ. Which action should the engineer take to troubleshoot this issue using the real DNS packets?

A. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion policy as needed

B. Use the Connection Events dashboard to check the block reason and adjust the inspection policy as needed

C. Use the packet tracer tool to determine at which hop the packet is being dropped

D. Use the show blocks command in the Threat Defense CLI tool and create a policy to allow the blocked traffic

Correct Answer: B

QUESTION 5

A company is in the process of deploying intrusion prevention with Cisco FTDs managed by a Cisco FMC. An engineer must configure policies to detect potential intrusions but not block the suspicious traffic Which action accomplishes this task?

A. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the “Drop when inline” option.

B. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the “Drop when inline” option.

C. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the “Drop when inline” option.

D. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the “Drop when inline” option.

Correct Answer: D

QUESTION 6

Which two features of Cisco AMP for Endpoints allow for an uploaded file to be blocked? (Choose two.)

A. application blocking

B. simple custom detection

C. file repository

D. exclusions

E. application whitelisting

Correct Answer: AB

configure custom malware detection policies and profiles for your entire organization, as well as perform flash and full scans on all your users' files perform malware analysis, including view heat maps, detailed file information, network file trajectory, and threat root causes configure multiple aspects of outbreak control, including automatic quarantines, application blocking to stop non-quarantined executables from running, and exclusion lists

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html#id_96014

QUESTION 7

What is a functionality of port objects in Cisco FMC?

A. to mix transport protocols when setting both source and destination port conditions in a rule

B. to represent protocols other than TCP, UDP, and ICMP

C. to represent all protocols in the same way

D. to add any protocol other than TCP or UDP for source port conditions in access control rules.

Correct Answer: B

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

QUESTION 8

With a recent summer time change, system logs are showing activity that occurred to be an hour behind real time. Which action should be taken to resolve this issue?

A. Manually adjust the time to the correct hour on all managed devices.

B. Configure the system clock settings to use NTP with Daylight Savings checked.

C. Configure the system clock settings to use NTP.

D. Manually adjust the time to the correct hour on the Cisco FMC.

Correct Answer: B

QUESTION 9

Which object type supports object overrides?

A. time range

B. security group tag

C. network object

D. DNS server group

Correct Answer: C

Object Overrides supported are: Network Port VLAN tag URL

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

QUESTION 10

Which Cisco Advanced Malware Protection for Endpoints policy is used only for monitoring endpoint actively?

A. Windows domain controller

B. audit

C. triage

D. protection

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214933-amp-for-endpoints-deployment-methodology.html

QUESTION 11

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?

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.

Correct Answer: A

QUESTION 12

Which action should you take when Cisco Threat Response notifies you that AMP has identified a file as malware?

A. Add the malicious file to the block list.

B. Send a snapshot to Cisco for technical support.

C. Forward the result of the investigation to an external threat-analysis engine.

D. Wait for Cisco Threat Response to automatically block the malware.

Correct Answer: A

QUESTION 13

A Cisco FMC administrator wants to configure fastpathing of trusted network traffic to increase performance. In which type of policy would the administrator configure this feature?

A. Network Analysis policy

B. Identity policy

C. Prefilter policy

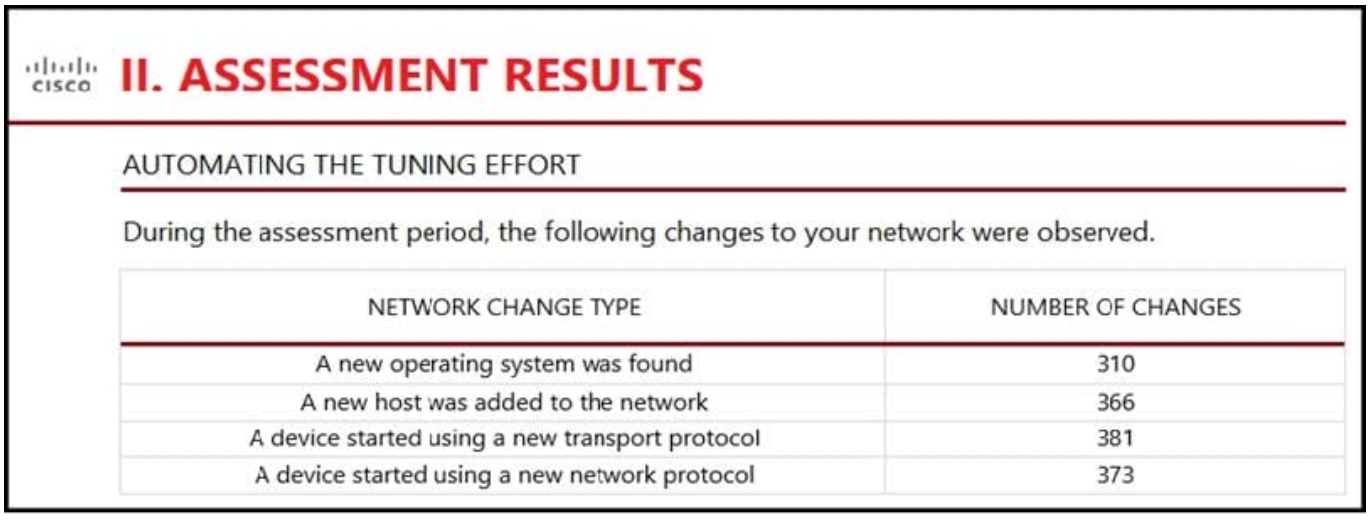
D. Intrusion policy

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/prefiltering_and_prefilter_policies.html

QUESTION 14

Refer to the exhibit.



An engineer is analyzing the Attacks Risk Report and finds that there are over 300 instances of new operating systems being seen on the network. How is the Firepower configuration updated to protect these new operating systems?

A. Cisco Firepower Automatically updates the policies.

B. The administrator requests a Remediation Recommendation Report from Cisco Firepower

C. Cisco Firepower gives recommendation to update the policies

D. The administrator manually updates the policies.

Correct Answer: C

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Tailoring_Intrusion_Protection_to_Your_Network_Assets.html

QUESTION 15

In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

A. unavailable

B. unknown

C. clean

D. disconnected

Correct Answer: A

Unavailable indicates that the system could not query the AMP cloud https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_malware_events_and_network_file_trajectory.html