300-710$^{Q\&As}$

Securing Networks with Cisco Firepower (SNCF)

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

Which limitation applies to Cisco FMC dashboards in a multi-domain environment?

A. Child domains are able to view but not edit dashboards that originate from an ancestor domain.

B. Child domains have access to only a limited set of widgets from ancestor domains.

C. Only the administrator of the top ancestor domain is able to view dashboards.

D. Child domains are not able to view dashboards that originate from an ancestor domain.

Correct Answer: D

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

QUESTION 3

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

A. minor upgrade

B. local import of intrusion rules

C. Cisco Geolocation Database

D. local import of major upgrade

Correct Answer: B

In a multidomain deployment, you can import local intrusion rules in any domain. You can view local intrusion rules imported in the current domain and ancestor domains.

QUESTION 4

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: D

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

QUESTION 5

Which protocol establishes network redundancy in a switched Firepower device deployment?

A. STP

B. HSRP

C. GLBP

D. VRRP

Correct Answer: A

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

QUESTION 6

Remote users who connect via Cisco AnyConnect to the corporate network behind a Cisco FTD device report that they get no audio when calling between remote users using their softphones. These same users can call internal users on the corporate network without any issues. What is the cause of this issue?

A. FTD has no NAT policy that allows outside to outside communication.

B. Split tunneling is enabled for the Remote Access VPN on FTD.

C. The hairpinning feature is not available on FTD.

D. The Enable Spoke to Spoke Connectivity through Hub option is not selected on FTD.

Correct Answer: A

QUESTION 7

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 8

With Cisco FTD integrated routing and bridging, which interface does the bridge group use to communicate with a routed interface?

A. subinterface

B. switch virtual

C. bridge virtual

D. bridge group member

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

QUESTION 9

Which feature is supported by IRB on Cisco FTD devices?

A. redundant interface

B. dynamic routing protocol

C. EtherChannel interface

D. high-availability cluster

Correct Answer: B

QUESTION 10

Which two TCP ports can allow the Cisco Firepower Management Center to communication with FireAMP cloud for file disposition information? (Choose two.)

A. 8080

B. 22

C. 8305

D. 32137

E. 443

Correct Answer: DE

QUESTION 11

An engineer integrates Cisco FMC and Cisco ISE using pxGrid. Which role is assigned for Cisco FMC?

A. server

B. controller

C. publisher

D. client

Correct Answer: D

Reference: https://www.ciscopress.com/articles/article.asp?p=2963461andseqNum=2

QUESTION 12

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 13

A network security engineer must replace a faulty Cisco FTD device in a high availability pair. Which action must be taken while replacing the faulty unit?

A. Ensure that the faulty Cisco FTD device remains registered to the Cisco FMC

B. Shut down the active Cisco FTD device before powering up the replacement unit

C. Shut down the Cisco FMC before powering up the replacement unit

D. Unregister the faulty Cisco FTD device from the Cisco FMC

Correct Answer: D

QUESTION 14

An organization has a compliance requirement to protect servers from clients, however, the clients and servers all reside on the same Layer 3 network. Without readdressing IP subnets for clients or servers, how is segmentation achieved?

A. Change the IP addresses of the servers, while remaining on the same subnet.

B. Deploy a firewall in routed mode between the clients and servers.

C. Change the IP addresses of the clients, while remaining on the same subnet.

D. Deploy a firewall in transparent mode between the clients and servers.

Correct Answer: B

QUESTION 15

A network administrator is implementing an active/passive high availability Cisco FTD pair. When adding the high availability pair, the administrator cannot select the secondary peer. What is the cause?

A. The second Cisco FTD is not the same model as the primary Cisco FTD.

B. An high availability license must be added to the Cisco FMC before adding the high availability pair.

C. The failover link must be defined on each Cisco FTD before adding the high availability pair.

D. Both Cisco FTD devices are not at the same software version.

Correct Answer: A