Correct Answer: D

QUESTION 67
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

QUESTION 68
Which command should be used on the Cisco FTD CLI to capture all the packets that hit an interface?

A. configure coredump packet-engine enable
B. capture-traffic
C. capture
D. capture WORD

Correct Answer: C

QUESTION 69
Which group within Cisco does the Threat Response team use for threat analysis and research?

A. Cisco Deep Analytics
B. OpenDNS Group
C. Cisco Network Response
D. Cisco Talos

Correct Answer: D

QUESTION 70
Within Cisco Firepower Management Center, where does a user add or modify widgets?

A. dashboard
B. reporting
C. context explorer
D. summary tool

Correct Answer: A

QUESTION 71
Which command-line mode is supported from the Cisco Firepower Management Center CLI?

A. privileged
B. user

C. configuration
D. admin

Correct Answer: C

QUESTION 72
After deploying a network-monitoring tool to manage and monitor networking devices in your organization, you realize that you need to manually upload an MIB for the Cisco FMC. In which folder should you upload the MIB file?

A. /etc/sf/DCMIB.ALERT
B. /sf/etc/DCEALERT.MIB
C. /etc/sf/DCEALERT.MIB
D. system/etc/DCEALERT.MIB

Correct Answer: C

QUESTION 73
Which command must be run to generate troubleshooting files on an FTD?

A. system support view-files
B. sudo sf_troubleshoot.pl
C. system generate-troubleshoot all
D. show tech-support

Correct Answer: C

QUESTION 74
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

QUESTION 75
Which action should be taken after editing an object that is used inside an access control policy?

A. Delete the existing object in use.
B. Refresh the Cisco FMC GUI for the access control policy.
C. Redeploy the updated configuration.
D. Create another rule using a different object name.

Correct Answer: C

QUESTION 76
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 77
What is a valid Cisco AMP file disposition?

A. non-malicious
B. malware
C. known-good
D. pristine
Correct Answer: B

QUESTION 78
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

QUESTION 79
Which two remediation options are available when Cisco FMC is integrated with Cisco ISE? (Choose two.)

A. dynamic null route configured
B. DHCP pool disablement
C. quarantine
D. port shutdown
E. host shutdown

Correct Answer: CD

QUESTION 80
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

QUESTION 81
Which connector is used to integrate Cisco ISE with Cisco FMC for Rapid Threat Containment?

A. pxGrid
B. FTD RTC
C. FMC RTC
D. ISEGrid

Correct Answer: A

QUESTION 82
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

QUESTION 83
What is the maximum SHA level of filtering that Threat Intelligence Director supports?

A. SHA-1024
B. SHA-4096
C. SHA-512
D. SHA-256

Correct Answer: D

QUESTION 84
A network administrator cannot select the link to be used for failover when configuring an active/passive HA Cisco FTD pair. Which configuration must be changed before setting up the high availability pair?

A. An IP address in the same subnet must be added to each Cisco FTD on the interface.
B. The interface name must be removed from the interface on each Cisco FTD.
C. The name Failover must be configured manually on the interface on each cisco FTD.
D. The interface must be configured as part of a LACP Active/Active EtherChannel.

Correct Answer: A

QUESTION 85
An engineer is configuring a cisco FTD appliance in IPS-only mode and needs to utilize fail-to-