300-710.premium. 76q - DEMO

Number: 300-710
Passing Score: 800
Time Limit: 120 min

300-710

Securing Networks with Cisco Firepower

Exam A

QUESTION 1

What is a result of enabling Cisco FTD clustering?

A. For the dynamic routing feature, if the master unit fails, the newly elected master unit maintains all existing connections.
B. Integrated Routing and Bridging is supported on the master unit.
C. Site-to-site VPN functionality is limited to the master unit, and all VPN connections are dropped if the master unit fails.
D. All Firepower appliances support Cisco FTD clustering.

Correct Answer: C
Section: Deployment
Explanation

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

QUESTION 2 Which two conditions are necessary for high availability to function between two Cisco FTD devices?
(Choose two.)

A. The units must be the same version
B. Both devices can be part of a different group that must be in the same domain when configured within the FMC.
C. The units must be different models if they are part of the same series.
D. The units must be configured only for firewall routed mode.
E. The units must be the same model.

Correct Answer: AE
Section: Deployment
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html

QUESTION 3 On the advanced tab under inline set properties, which allows interfaces to emulate a
passive interface?

A. transparent inline mode
B. TAP mode
C. strict TCP enforcement
D. propagate link state

Correct Answer: D
Section: Deployment
Explanation

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

QUESTION 4 What are the minimum requirements to deploy a managed
device inline?

A. inline interfaces, security zones, MTU, and mode
B. passive interface, MTU, and mode
C. inline interfaces, MTU, and mode
D. passive interface, security zone, MTU, and mode

Correct Answer: C

Section: Deployment
Explanation
Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/ips_device_deployments_and_configuration.html

QUESTION 5 What is the difference between inline and inline tap on Cisco Firepower?

A. Inline tap mode can send a copy of the traffic to another device.
B. Inline tap mode does full packet capture.
C. Inline mode cannot do SSL decryption.
D. Inline mode can drop malicious traffic.

Correct Answer: D
Section: Deployment
Explanation

Explanation/Reference:

QUESTION 6 With Cisco FTD software, which interface mode must be configured to passively receive traffic that passes through the appliance?

A. inline set
B. passive
C. routed
D. inline tap

Correct Answer: B
Section: Deployment
Explanation

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

QUESTION 7 Which two deployment types support high availability? (Choose two.)

A. transparent
B. routed
C. clustered
D. intra-chassis multi-instance
E. virtual appliance in public cloud

Correct Answer: AB
Section: Deployment
Explanation

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

QUESTION 8 Which protocol establishes network redundancy in a switched Firepower device deployment?

A. STP
B. HSRP
C. GLBP
D. VRRP

Correct Answer: A
Section: Deployment
Explanation

Explanation/Reference:
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 9 Which interface type allows packets to be dropped?

A. passive
B. inline
C. ERSPAN
D. TAP

Correct Answer: B
Section: Deployment
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring-firepower-threat-defense-int.html

QUESTION 10 Which Cisco Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two.)

A. Redundant Interface
B. EtherChannel
C. Speed
D. Media Type
E. Duplex

Correct Answer: CE
Section: Deployment
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm-interfaces.html

QUESTION 11 Which two dynamic routing protocols are supported in Cisco FTD without using FlexConfig? (Choose two.)

A. EIGRP
B. OSPF
C. static routing
D. IS-IS
E. BGP

Correct Answer: CE
Section: Deployment
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-routing.html

QUESTION 12 Which policy rule is included in the deployment of a local DMZ during the initial deployment of a Cisco NGFW through the Cisco FMC GUI?

A. a default DMZ policy for which only a user can change the IP addresses.

B. deny ip any
C. no policy rule is included
D. permit ip any

Correct Answer: C
Section: Deployment
Explanation

Explanation/Reference:

QUESTION 13 What are two application layer preprocessors? (Choose two.)

A. CIFS
B. IMAP
C. SSL
D. DNP3
E. ICMP

Correct Answer: BC
Section: Deployment
Explanation

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

QUESTION 14
An engineer is implementing Cisco FTD in the network and is determining which Firepower mode to use. The organization needs to have multiple virtual Firepower devices working separately inside of the FTD appliance to provide traffic segmentation. Which deployment mode should be configured in the Cisco Firepower Management Console to support these requirements?

A. multi-instance
B. multiple deployment
C. single deployment
D. single-context

Correct Answer: A
Section: Deployment
Explanation

Explanation/Reference:

QUESTION 15 A network engineer is extending a user segment through an FTD device for traffic inspection without creating another IP subnet. How is this accomplished on an FTD device in routed mode?

A. by assigning an inline set interface
B. by using a BVI and creating a BVI IP address in the same subnet as the user segment
C. by leveraging the ARP to direct traffic through the firewall
D. by bypassing protocol inspection by leveraging pre-filter rules

Correct Answer: A
Section: Deployment
Explanation

Explanation/Reference:

QUESTION 16
An engineer is configuring a Cisco FTD appliance in IPS-only mode and needs to utilize fail-to-wire interfaces. Which interface mode should be used to meet these requirements?
A. passive
B. routed
C. transparent
D. inline set

Correct Answer: D
Section: Deployment
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

QUESTION 17 An organization has noticed that malware was downloaded from a website that does not currently have a known bad reputation. How will this issue be addressed globally in the quickest way possible and with the least amount of impact?

A. by creating a URL object in the policy to block the website.
B. Cisco Talos will automatically update the policies.
C. by denying outbound web access
D. by isolating the endpoint

Correct Answer: B
Section: Deployment
Explanation

Explanation/Reference:

QUESTION 18
The event dashboard within the Cisco FMC has been inundated with low priority intrusion drop events, which are overshadowing high priority events. An engineer has been tasked with reviewing the policies and reducing the low priority events. Which action should be configured to accomplish this task?

A. drop packet
B. generate events
C. drop connection
D. drop and generate

Correct Answer: B
Section: Deployment
Explanation

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

QUESTION 19
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
Section: Deployment
Explanation

Explanation/Reference:

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 20
An engineer is setting up a new Firepower deployment and is looking at the default FMC policies to start the implementation. During the initial trial phase, the organization wants to test some common Snort rules while still allowing the majority of network traffic to pass. Which default policy should be used?

A. Balanced Security and Connectivity
B. Security Over ConnectivityC. Maximum Detection
D. Connectivity Over Security

Correct Answer: D
Section: Deployment
Explanation

Explanation/Reference:

QUESTION 21
An engineer is configuring a second Cisco FMC as a standby device but is unable to register with the active unit. What is causing this issue?

A. The code versions running on the Cisco FMC devices are different.
B. The licensing purchased does not include high availability.
C. The primary FMC currently has devices connected to it.
D. There is only 10 Mbps of bandwidth between the two devices.

Correct Answer: A
Section: Deployment
Explanation

Explanation/Reference:

QUESTION 22 While configuring FTD, a network engineer wants to ensure that traffic passing though the appliance does not require routing or VLAN rewriting. Which interface mode should the engineer implement to accomplish this task?

A. inline set
B. passive
C. transparent
D. inline tap

Correct Answer: B
Section: Deployment
Explanation

Explanation/Reference:

QUESTION 23
Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)

A. OSPFv2 with IPv6 capabilities
B. virtual links
C. SHA authentication to OSPF packets
D. area boundary router type 1 LSA filtering
E. MD5 authentication to OSPF packets

Correct Answer: BE
Section: Configuration

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

QUESTION 24 When creating a report template, how are the results limited to show only the activity of a specific subnet?

A. Create a custom search in Cisco FMC and select it in each section of the report.
B. Add an Input Parameter in the Advanced Settings of the report, and set the type to Network/IP.
C. Add a Table View section to the report with the Search field defined as the network in CIDR format.
D. Select IP Address as the X-Axis in each section of the report.

Correct Answer: B
Section: Configuration
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/Reports.html#87267

QUESTION 25 What is the disadvantage of setting up a site-to-site VPN in a clustered-units environment?

A. VPN connections can be re-established only if the failed master unit recovers.
B. Smart License is required to maintain VPN connections simultaneously across all cluster units.
C. VPN connections must be re-established when a new master unit is elected.
D. Only established VPN connections are maintained when a new master unit is elected.

Correct Answer: C
Section: Configuration
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept_g32_yml_y2b

QUESTION 26 What are two features of bridge-group interfaces in Cisco FTD? (Choose two.)

A. The BVI IP address must be in a separate subnet from the connected network.
B. Bridge groups are supported in both transparent and routed firewall modes.
C. Bridge groups are supported only in transparent firewall mode.
D. Bidirectional Forwarding Detection echo packets are allowed through the FTD when using bridge-group members.
E. Each directly connected network must be on the same subnet.

Correct Answer: CD
Section: Configuration
Explanation

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

QUESTION 27
Which command is run on an FTD unit to associate the unit to an FMC manager that is at IP address 10.0.0.10, and that has the registration key Cisco123?

A. configure manager local 10.0.0.10 Cisco123
B. configure manager add Cisco123 10.0.0.10
C. configure manager local Cisco123 10.0.0.10
D. configure manager add 10.0.0.10 Cisco123

Correct Answer: D
Section: Configuration
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#id_106101

QUESTION 28 Which two actions can be used in an access control policy rule? (Choose two.)

A. Block with Reset
B. Monitor
C. Analyze
D. Discover
E. Block ALL

Correct Answer: AB
Section: Configuration
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html#71854

QUESTION 29 Which two routing options are valid with Cisco FTD? (Choose two.)

A. BGPv6
B. ECMP with up to three equal cost paths across multiple interfaces
C. ECMP with up to three equal cost paths across a single interface
D. BGPv4 in transparent firewall mode
E. BGPv4 with nonstop forwarding

Correct Answer: AC
Section: Configuration
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

QUESTION 30 Which object type supports object overrides?

A. time range
B. security group tag
C. network object
D. DNS server group

Correct Answer: C
Section: Configuration
Explanation

Explanation/Reference:
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 31 Which Cisco Firepower rule action displays an HTTP warning page?

A. Monitor

B. Block
C. Interactive Block
D. Allow with Warning

Correct Answer: C
Section: Configuration
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/AC-Rules-Tuning-Overview.html#76698

QUESTION 32 What is the result a specifying of QoS rule that has a rate limit that is greater than the maximum throughput of an interface?

A. The rate-limiting rule is disabled.
B. Matching traffic is not rate limited.
C. The system rate-limits all traffic.
D. The system repeatedly generates warnings.

Correct Answer: B
Section: Configuration
Explanation

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

QUESTION 33
Which Firepower feature allows users to configure bridges in routed mode and enables devices to perform Layer 2 switching between interfaces?

A. FlexConfig
B. BDI
C. SGT
D. IRB

Correct Answer: D
Section: Configuration
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/relnotes/Firepower_System_Release_Notes_Version_620/new_features_and_functionality.html

QUESTION 34 In which two places are thresholding settings configured? (Choose two.)

A. on each IPS rule
B. globally, within the network analysis policy
C. globally, per intrusion policy
D. on each access control rule
E. per preprocessor, within the network analysis policy

Correct Answer: AC
Section: Configuration
Explanation

Explanation/Reference:
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.pdf

QUESTION 35 In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.) A. Traffic inspection is interrupted temporarily when configuration changes are deployed.

B. The system performs intrusion inspection followed by file inspection.
C. They block traffic based on Security Intelligence data.
D. File policies use an associated variable set to perform intrusion prevention.
E. The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters.

Correct Answer: AC
Section: Configuration
Explanation

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

QUESTION 36 Which two types of objects are reusable and supported by Cisco FMC? (Choose two.)

A. dynamic key mapping objects that help link HTTP and HTTPS GET requests to Layer 7 application protocols.
B. reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists
C. network-based objects that represent IP addresses and networks, port/protocol pairs, VLAN tags, security zones, and origin/destination country
D. network-based objects that represent FQDN mappings and networks, port/protocol pairs, VXLAN tags, security zones and origin/destination country
E. reputation-based objects, such as URL categories

Correct Answer: BC
Section: Configuration
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-00000414

QUESTION 37
A security engineer is configuring an Access Control Policy for multiple branch locations. These locations share a common rule set and utilize a network object called INSIDE_NET which contains the locally significant internal network subnets at each location. What technique will retain the policy consistency at each location but allow only the locally significant network subnet within the application rules?

A. utilizing a dynamic ACP that updates from Cisco Talos
B. creating a unique ACP per device
C. utilizing policy inheritance
D. creating an ACP with an INSIDE_NET network object and object overrides

Correct Answer: D
Section: Configuration
Explanation

Explanation/Reference:

QUESTION 38 What is the benefit of selecting the trace option for packet capture?

A. The option indicates whether the packet was dropped or successful.
B. The option indicates whether the destination host responds through a different path.
C. The option limits the number of packets that are captured.
D. The option captures details of each packet.

Correct Answer: C

Section: Management and Troubleshooting Explanation

Explanation/Reference:
QUESTION 39 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.MIBC. /etc/sf/DCEALERT.MIB
D. system/etc/DCEALERT.MIB

Correct Answer: C
Section: Management and Troubleshooting Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-External-Responses.pdf

QUESTION 40
Which command is run at the CLI when logged in to an FTD unit, to determine whether the unit is managed locally or by a remote FMC server?

A. system generate-troubleshoot
B. show configuration session
C. show managers
D. show running-config | include manager

Correct Answer: C
Section: Management and Troubleshooting Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/c_3.html

QUESTION 41 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: B
Section: Management and Troubleshooting Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/ac_1.html

QUESTION 42 How many report templates does the Cisco Firepower Management Center support?

A. 20
B. 10
C. 5
D. unlimited

Correct Answer: D
Section: Management and Troubleshooting Explanation

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

QUESTION 43 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
Section: Management and Troubleshooting Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/reusable_objects.html

QUESTION 44 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
Section: Management and Troubleshooting Explanation

Explanation/Reference:
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

QUESTION 45 Which report template field format is available in Cisco FMC?

A. box lever chart
B. arrow chart
C. bar chart
D. benchmark chart

Correct Answer: C
Section: Management and Troubleshooting Explanation

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

QUESTION 46 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
Section: Management and Troubleshooting Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits

QUESTION 47
DRAG DROP

Drag and drop the steps to restore an automatic device registration failure on the standby Cisco FMC from the left into the correct order on the right. Not all options are used.

Select and Place:

Correct Answer:

Section: Management and Troubleshooting Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html#id_32288

QUESTION 48 Which CLI command is used to generate firewall debug messages on a Cisco Firepower?

A. system support firewall-engine-debug
B. system support ssl-debug
C. system support platform
D. system support dump-table

Correct Answer: A
Section: Management and Troubleshooting Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212330-firepower-management-center-display-acc.html

QUESTION 49
Which command-line mode is supported from the Cisco FMC CLI?

A. privileged
B. user
C. configuration
D. admin

Correct Answer: C
Section: Management and Troubleshooting Explanation

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

QUESTION 50 Which command is entered in the Cisco FMC CLI to generate a troubleshooting file?

A. show running-config
B. show tech-support chassis
C. system support diagnostic-cli
D. sudo sf_troubleshoot.pl

Correct Answer: D
Section: Management and Troubleshooting Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

QUESTION 51 Which CLI command is used to control special handling of ClientHello messages?

A. system support ssl-client-hello-tuning
B. system support ssl-client-hello-display

C. system support ssl-client-hello-force-reset
D. system support ssl-client-hello-reset

Correct Answer: A
Section: Management and Troubleshooting Explanation

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

QUESTION 52 Which command is typed at the CLI on the primary Cisco FTD unit to temporarily stop running high-availability?

A. configure high-availability resume
B. configure high-availability disable
C. system support network-options
D. configure high-availability suspend

Correct Answer: B
Section: Management and Troubleshooting Explanation

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

QUESTION 53 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: B
Section: Management and Troubleshooting Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

QUESTION 54 When is the **file-size** command needed while troubleshooting with packet capture?

A. when capture packets are less than 16 MB
B. when capture packets are restricted from the secondary memory
C. when capture packets exceed 10 GB
D. when capture packets exceed 32 MB

Correct Answer: D
Section: Management and Troubleshooting
Explanation
Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

QUESTION 55 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
Section: Management and Troubleshooting Explanation

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

QUESTION 56 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
Section: Management and Troubleshooting Explanation

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

QUESTION 57
A network engineer is configuring URL Filtering on Cisco FTD. Which two port requirements on the FMC must be validated to allow communication with the cloud service? (Choose two.)

A. outbound port TCP/443
B. inbound port TCP/80
C. outbound port TCP/8080
D. inbound port TCP/443
E. outbound port TCP/80

Correct Answer: AE
Section: Management and Troubleshooting Explanation

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

QUESTION 58 What is the maximum bit size that Cisco FMC supports for HTTPS certificates?

A. 1024
B. 8192
C. 4096
D. 2048

Correct Answer: D
Section: Management and Troubleshooting
Explanation

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

QUESTION 59 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
Section: Management and Troubleshooting Explanation

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

QUESTION 60 Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC?
(Choose two.)

A. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re-apply the policies after registration is completed.
B. Before re-adding the device in Cisco FMC, the manager must be added back.
C. Once a device has been deleted, it must be reconfigured before it is re-added to the Cisco FMC.
D. The Cisco FMC web interface prompts users to re-apply access control policies.
E. There is no option to re-apply NAT and VPN policies during registration available, so users need to re-apply the policies after registration is completed.

Correct Answer: DE
Section: Management and Troubleshooting Explanation

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

QUESTION 61 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 is 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
Section: Management and Troubleshooting Explanation

Explanation/Reference:
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 62 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
Section: Management and Troubleshooting Explanation

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

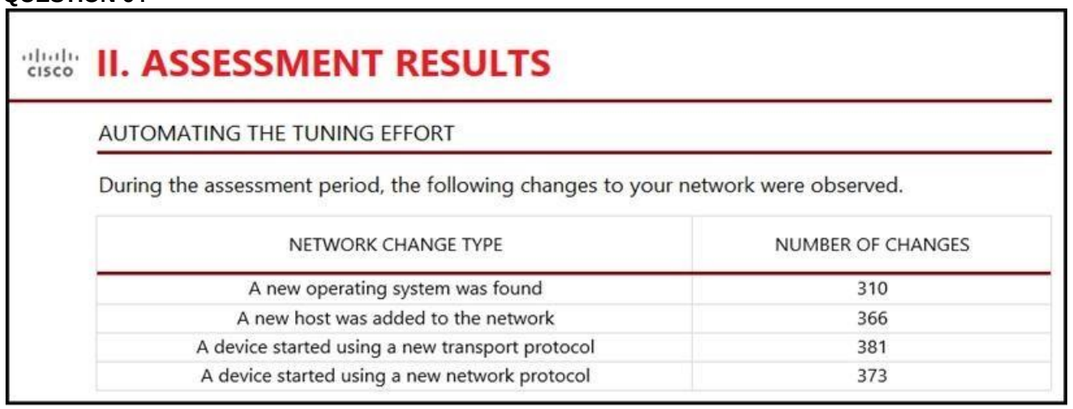
QUESTION 63
An engineer currently has a Cisco FTD device registered to the Cisco FMC and is assigned the address of 10.10.50.12. The organization is upgrading the addressing schemes and there is a requirement to convert the addresses to a format that provides an adequate amount of addresses on the network. What should the engineer do to ensure that the new addressing takes effect and can be used for the Cisco FTD to Cisco FMC connection?

A. Update the IP addresses from IPv4 to IPv6 without deleting from Cisco FMC.
B. Format and reregister the device to Cisco FMC.
C. Cisco FMC does not support devices that use IPv4 IP addresses.
D. Delete and reregister the device to Cisco FMC.

Correct Answer: A
Section: Management and Troubleshooting Explanation

Explanation/Reference:

QUESTION 64



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. The administrator manually updates the policies.
B. The administrator requests a Remediation Recommendation Report from Cisco Firepower.
C. Cisco Firepower gives recommendations to update the policies.
D. Cisco Firepower automatically updates the policies.

Correct Answer: C
Section: Management and Troubleshooting Explanation

Explanation/Reference:

QUESTION 65
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. Current Sessions
B. Correlation Events
C. Current Status
D. Custom Analysis

Correct Answer: B
Section: Management and Troubleshooting Explanation

Explanation/Reference:

QUESTION 66
An engineer is troubleshooting application failures through an FTD deployment. While using the FMC CLI, it has been determined that the traffic in question is not matching the desired policy. What should be done to correct this?

A. Use the **system support firewall-engine-debug** command to determine which rules the traffic matching and modify the rule accordingly.
B. Use the **system support firewall-engine-dump-user-identity-data** command to change the policy and allow the application though the firewall.
C. Use the **system support application-identification-debug** command to determine which rules the traffic matching and modify the rule accordingly.

D. Use the **system support network-options** command to fine tune the policy.

Correct Answer: A
Section: Management and Troubleshooting Explanation

Explanation/Reference:

QUESTION 67 An engineer has been asked to show application usages automatically on a monthly basis and send the information to management. What mechanism should be used to accomplish this task?

A. reports
B. context explorer
C. dashboards
D. event viewer

Correct Answer: A
Section: Management and Troubleshooting Explanation

Explanation/Reference:

QUESTION 68 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 allow listing

Correct Answer: AB
Section: Integration
Explanation

Explanation/Reference:
QUESTION 69 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
Section: Integration
Explanation

Explanation/Reference:

QUESTION 70 Which Cisco AMP for Endpoints policy is used only for monitoring endpoint activity?

A. Windows domain controller
B. audit
C. triage
D. protection

Correct Answer: B
Section: Integration
Explanation

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

QUESTION 71 What is a valid Cisco AMP file disposition?

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

Correct Answer: B
Section: Integration
Explanation

Explanation/Reference:
Reference: 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

QUESTION 72 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
Section: Integration
Explanation
Explanation/Reference:

QUESTION 73 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
Section: Integration
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524-configure-firepower-6-1-pxgrid-remediati.html

QUESTION 74 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
Section: Integration
Explanation

Explanation/Reference:

QUESTION 75 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
Section: Integration
Explanation

Explanation/Reference:
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 76
What is the advantage of having Cisco Firepower devices send events to Cisco Threat Response via the security services exchange portal directly as opposed to using syslog?

A. Firepower devices do not need to be connected to the Internet.
B. An on-premises proxy server does not need to set up and maintained.
C. All types of Firepower devices are supported.
D. Supports all devices that are running supported versions of Firepower

Correct Answer: B
Section: Integration
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower_and_Cisco_Threat_Response_Integration_Guide.pdf