Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

https://www.2passeasy.com/dumps/300-710/

NEW QUESTION 1
- (Exam Topic 5)
An engineer integrates Cisco FMC and Cisco ISE using pxGrid. Which role is assigned for Cisco FMC?

A. controller
B. publisher
C. client
D. server

Answer: C

NEW QUESTION 2
- (Exam Topic 5)
A network administrator is seeing an unknown verdict for a file detected by Cisco FTD. Which malware policy configuration option must be selected in order to further analyse the file in the Talos cloud?

A. Spero analysis
B. Malware analysis
C. Dynamic analysis
D. Sandbox analysis

Answer: B

NEW QUESTION 3
- (Exam Topic 5)
A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

A. The destination MAC address is optional if a VLAN ID value is entered
B. Only the UDP packet type is supported
C. The output format option for the packet logs unavailable
D. The VLAN ID and destination MAC address are optional

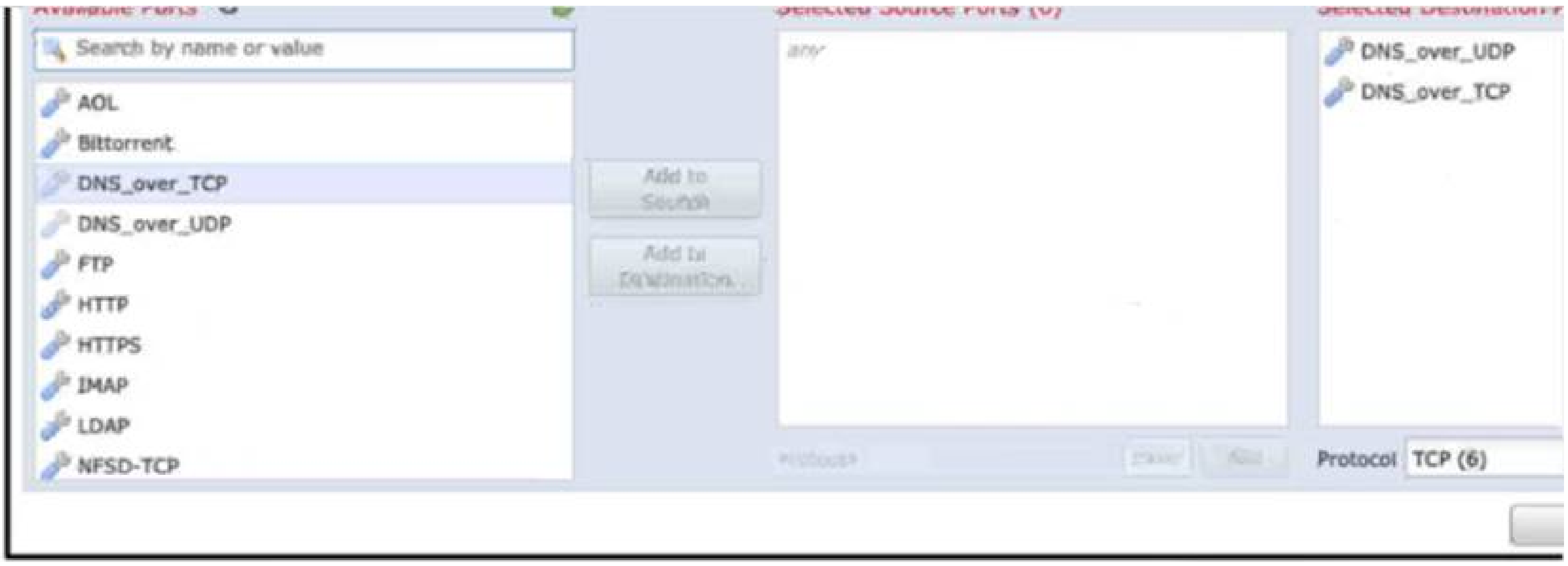
Answer: A

NEW QUESTION 4
- (Exam Topic 5)
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 "show tech" file for the device in question.
B. A "troubleshoot" file for the device in question.
C. A "troubleshoot" file for the Cisco FMC.
D. A "show tech" for the Cisco FMC.

Answer: B

NEW QUESTION 5
- (Exam Topic 5)
Refer to the exhibit.



Selected Source Ports (0)
any

Selected Destination Ports
DNS_over_UDP
DNS_over_TCP
Protocol TCP (6)

An engineer is modifying an access control policy to add a rule to Inspect all DNS traffic that passes it making the change and deploying the policy, they see that DNS traffic Is not being Inspected by the Snort engine. What is......

A. The action of the rule is set to trust instead of allow.
B. The rule must specify the security zone that originates the traffic.
C. The rule Is configured with the wrong setting for the source port.
D. The rule must define the source network for inspection as well as the port.

Answer: A

NEW QUESTION 6
- (Exam Topic 5)
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

Answer: A

NEW QUESTION 7
- (Exam Topic 5)
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 primary FMC currently has devices connected to it.
B. The code versions running on the Cisco FMC devices are different
C. The licensing purchased does not include high availability
D. There is only 10 Mbps of bandwidth between the two devices.

Answer: B

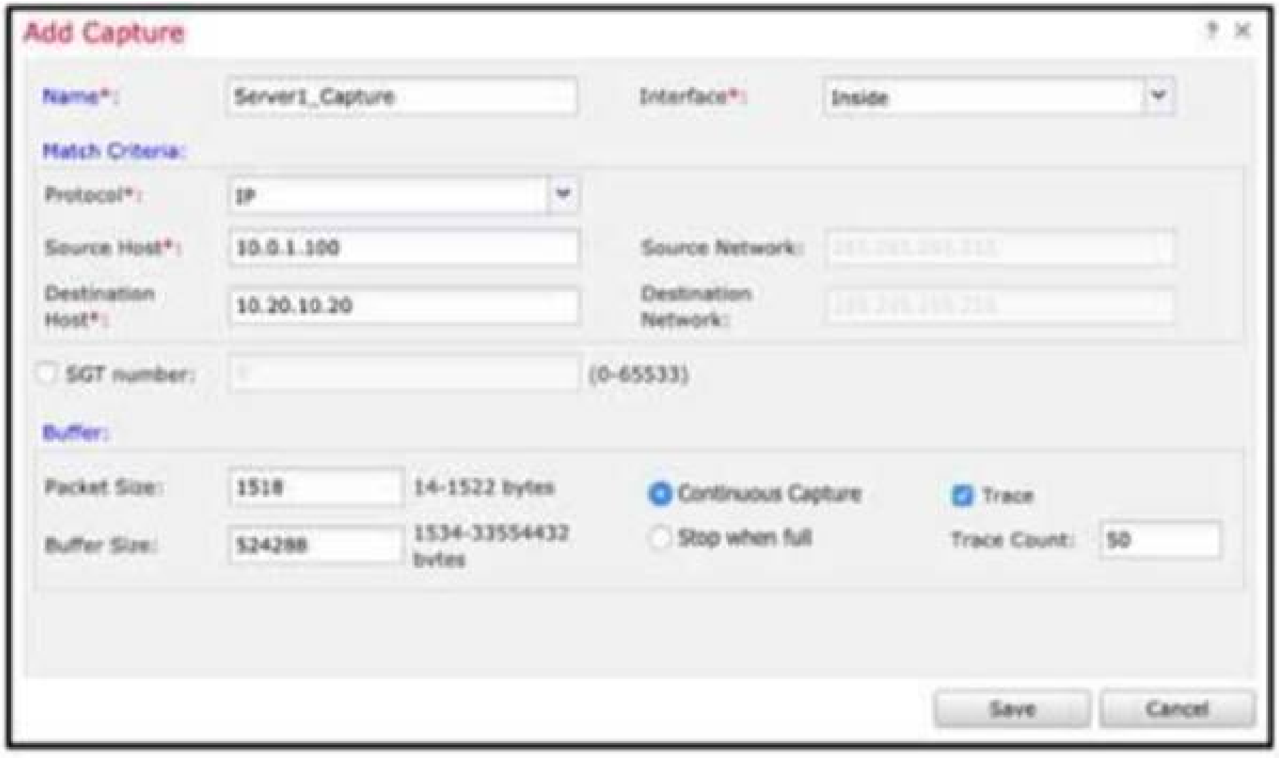
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firep

NEW QUESTION 8
- (Exam Topic 5)
Due to an Increase in malicious events, a security engineer must generate a threat report to include intrusion events, malware events, and security intelligence events. How Is this information collected in a single report?

A. Run the default Firepower report.
B. Export the Attacks Risk report.
C. Generate a malware report.
D. Create a Custom report.

Answer: D

NEW QUESTION 9
- (Exam Topic 5)
An engineer is troubleshooting a device that cannot connect to a web server. The connection is initiated from the Cisco FTD inside interface and attempting to reach 10.0.1.100 over the non-standard port of 9443 The host the engineer is attempting the connection from is at the IP address of 10.20.10.20. In order to determine what is happening to the packets on the network, the engineer decides to use the FTD packet capture tool Which capture configuration should be used to gather the information needed to troubleshoot this issue?
A)

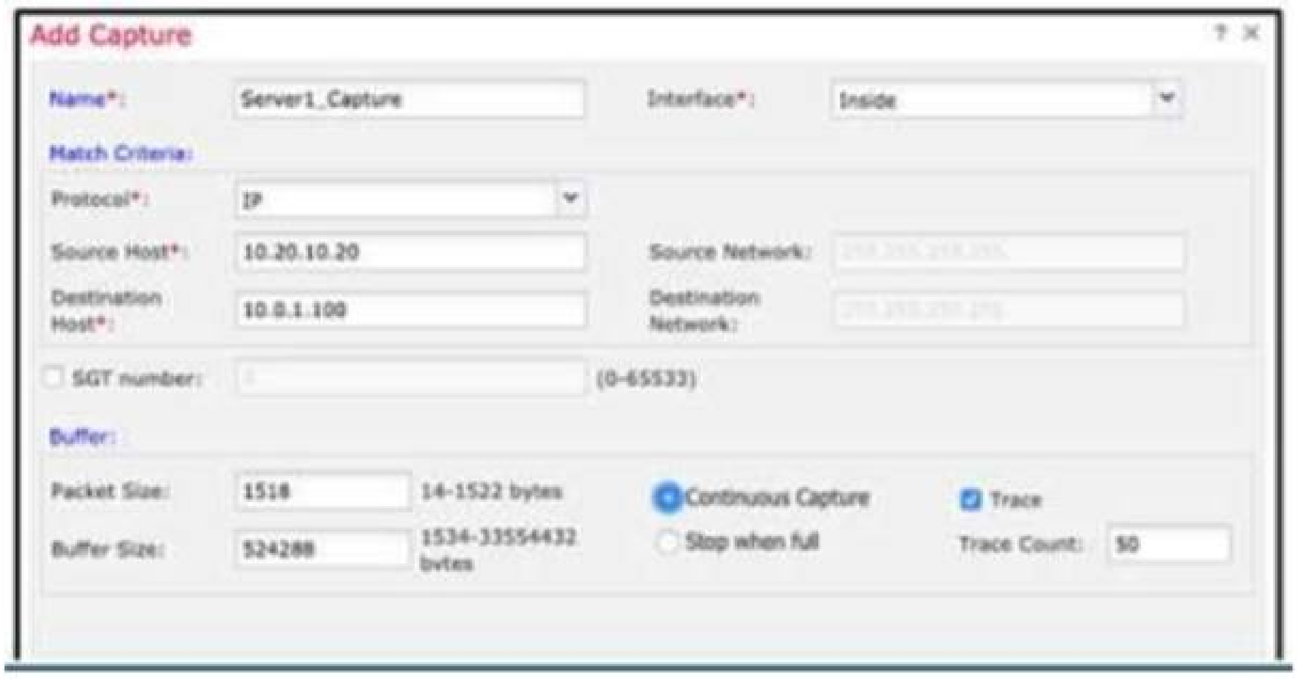

Add Capture

Name*: Server1_Capture
Interface*: Inside

Match Criteria:
Protocol*: IP
Source Host*: 10.0.1.100
Source Network:
Destination Host*: 10.20.10.20
Destination Network:
○ SGT number: (0-65533)

Buffer:
Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 bytes
● Continuous Capture
○ Stop when full
☑ Trace
Trace Count: 50

B)



Add Capture

Name*: Server1_Capture
Interface*: Inside

Match Criteria:

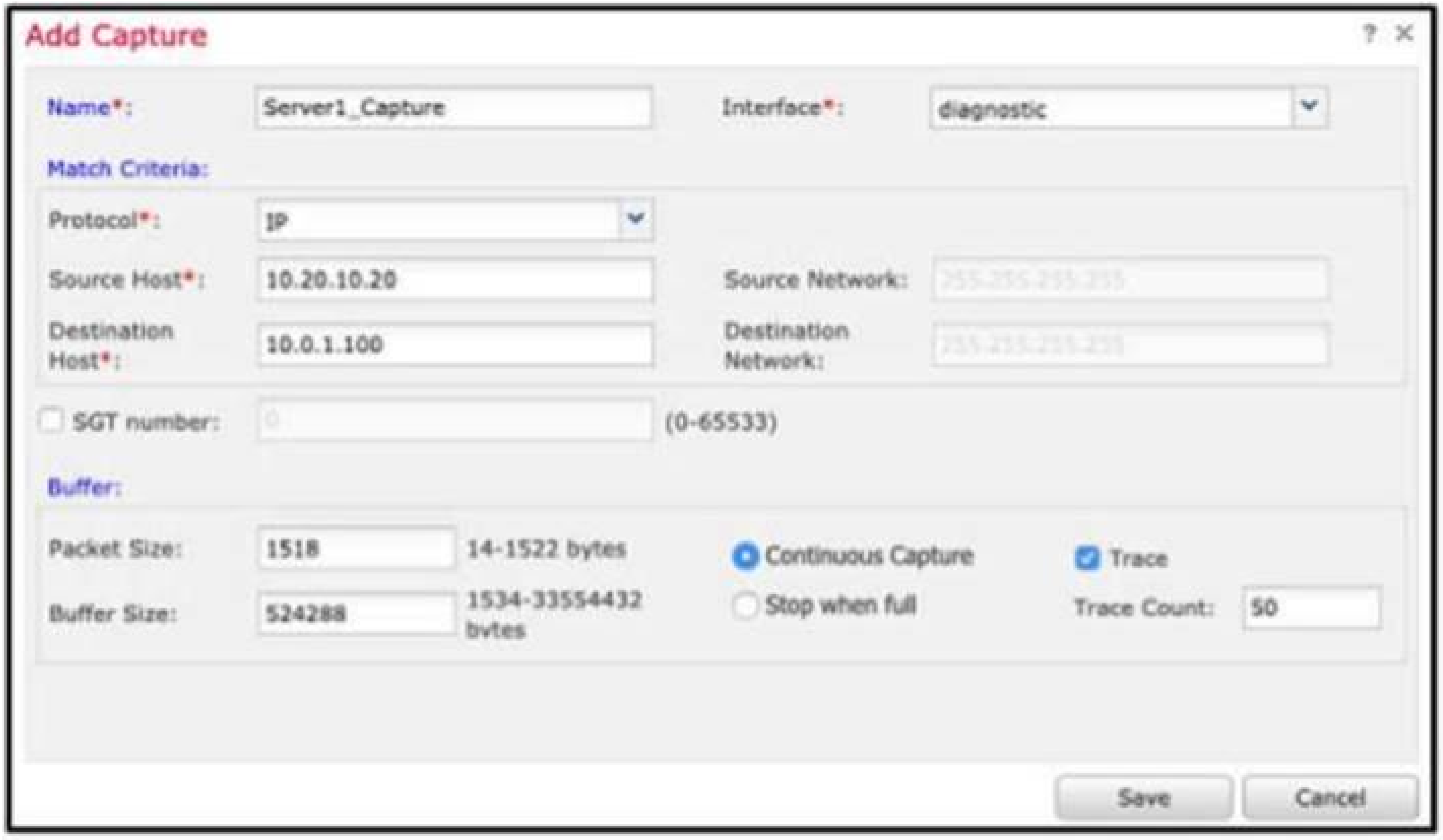
Protocol*: IP
Source Host*: 10.20.10.20
Source Network: 255.255.255.255
Destination Host*: 10.0.1.100
Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 bytes
● Continuous Capture
○ Stop when full
☑ Trace
Trace Count: 50

C)



Add Capture

Name*: Server1_Capture
Interface*: diagnostic

Match Criteria:

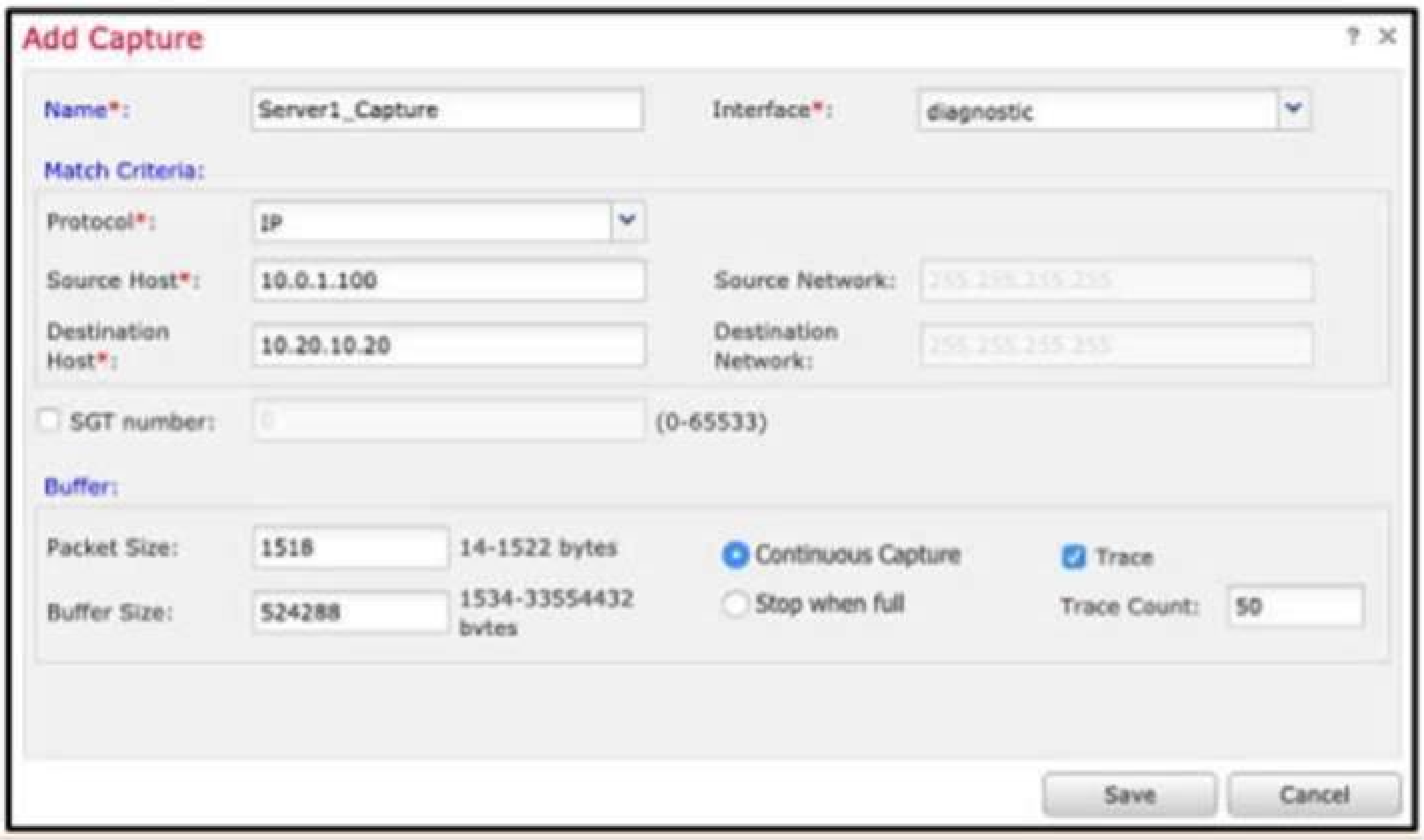
Protocol*: IP
Source Host*: 10.20.10.20
Source Network: 255.255.255.255
Destination Host*: 10.0.1.100
Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 bvtes
● Continuous Capture
○ Stop when full
☑ Trace
Trace Count: 50

D)



Add Capture

Name*: Server1_Capture
Interface*: diagnostic

Match Criteria:

Protocol*: IP
Source Host*: 10.0.1.100
Source Network: 255.255.255.255
Destination Host*: 10.20.10.20
Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 bvtes
● Continuous Capture
○ Stop when full
☑ Trace
Trace Count: 50

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 10
- (Exam Topic 5)
An engineer has been tasked with providing disaster recovery for an organization's primary Cisco FMC. What must be done on the primary and secondary Cisco FMCs to ensure that a copy of the original corporate policy is available if the primary Cisco FMC fails?

A. Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device fails.
B. Configure high-availability in both the primary and secondary Cisco FMCs.
C. Connect the primary and secondary Cisco FMC devices with Category 6 cables of not more than 10 meters in length.
D. Place the active Cisco FMC device on the same trusted management network as the standby device.

Answer: A

NEW QUESTION 10
- (Exam Topic 5)
An engineer is investigating connectivity problems on Cisco Firepower for a specific SGT. Which command allows the engineer to capture real packets that pass through the firewall using an SGT of 64?

A. capture CAP type inline-tag 64 match ip any any
B. capture CAP match 64 type inline-tag ip any any
C. capture CAP headers-only type inline-tag 64 match ip any any
D. capture CAP buffer 64 match ip any any

Answer: A

NEW QUESTION 14
- (Exam Topic 5)
An administrator is configuring their transparent Cisco FTD device to receive ERSPAN traffic from multiple switches on a passive port, but the Cisco FTD is not processing the traffic. What is the problem?

A. The switches do not have Layer 3 connectivity to the FTD device for GRE traffic transmission.
B. The switches were not set up with a monitor session ID that matches the flow ID defined on the CiscoFTD.
C. The Cisco FTD must be in routed mode to process ERSPAN traffic.
D. The Cisco FTD must be configured with an ERSPAN port not a passive port.

Answer: C

NEW QUESTION 15
- (Exam Topic 5)
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 Threat Intelligence Director using STIX and TAXII
B. Enable Rapid Threat Containment using REST APIs
C. Enable Threat Intelligence Director using REST APIs
D. Enable Rapid Threat Containment using STIX and TAXII

Answer: A

NEW QUESTION 17
- (Exam Topic 5)
A connectivity issue is occurring between a client and a server which are communicating through a Cisco Firepower device While troubleshooting, a network administrator sees that traffic is reaching the server, but the client is not getting a response Which step must be taken to resolve this issue without initiating traffic from the client?

A. Use packet-tracer to ensure that traffic is not being blocked by an access list.
B. Use packet capture to ensure that traffic is not being blocked by an access list.
C. Use packet capture to validate that the packet passes through the firewall and is NATed to the corrected IP address.
D. Use packet-tracer to validate that the packet passes through the firewall and is NATed to the correctedIP address.

Answer: D

NEW QUESTION 18
- (Exam Topic 5)
Which action must be taken on the Cisco FMC when a packet bypass is configured in case the Snort engine is down or a packet takes too long to process?

A. Enable Inspect Local Router Traffic
B. Enable Automatic Application Bypass
C. Configure Fastpath rules to bypass inspection
D. Add a Bypass Threshold policy for failures

Answer: B

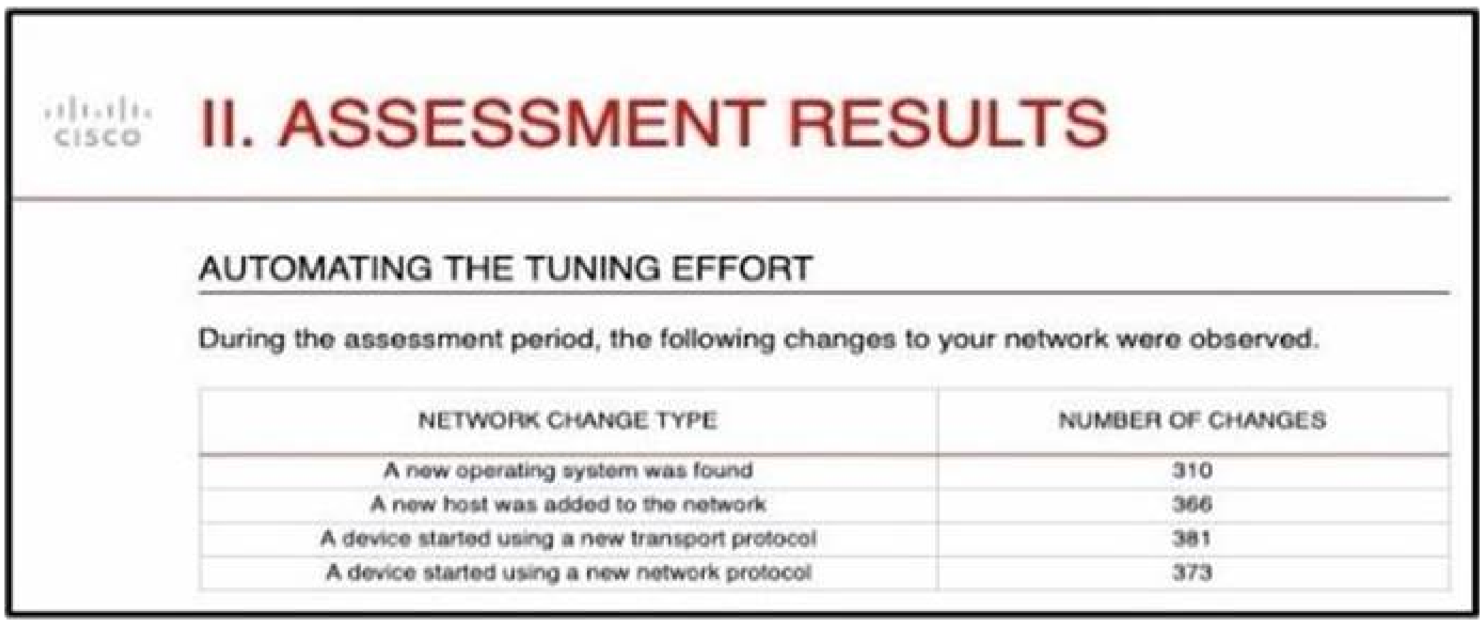
NEW QUESTION 23
- (Exam Topic 5)
When a Cisco FTD device is configured in transparent firewall mode, on which two interface types can an IP address be configured? (Choose two.)

A. Diagnostic
B. EtherChannel

C. BVI
D. Physical
E. Subinterface

Answer: AC

NEW QUESTION 27
- (Exam Topic 5)
Refer to the exhibit.



II. ASSESSMENT RESULTS

AUTOMATING THE TUNING EFFORT

During the assessment period, the following changes to your network were observed.

NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	310
A new host was added to the network	366
A device started using a new transport protocol	381
A device started using a new network protocol	373

And 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 recommendations to update the policies.
D. The administrator manually updates the policies.

Answer: C

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

NEW QUESTION 28
- (Exam Topic 5)
A hospital network needs to upgrade their Cisco FMC managed devices and needs to ensure that a disaster recovery process is in place. What must be done in order to minimize downtime on the network?

A. Configure a second circuit to an ISP for added redundancy
B. Keep a copy of the current configuration to use as backup
C. Configure the Cisco FMCs for failover
D. Configure the Cisco FMC managed devices for clustering.

Answer: B

NEW QUESTION 32
- (Exam Topic 5)
While integrating Cisco Umbrella with Cisco Threat Response, a network security engineer wants to automatically push blocking of domains from the Cisco Threat Response interface to Cisco Umbrella. Which API meets this requirement?

A. investigate
B. reporting
C. enforcement
D. REST

Answer: D

NEW QUESTION 33
- (Exam Topic 5)
An organization has seen a lot of traffic congestion on their links going out to the internet There is a Cisco Firepower device that processes all of the traffic going to the internet prior to leaving the enterprise. How is the congestion alleviated so that legitimate business traffic reaches the destination?

A. Create a flexconfig policy to use WCCP for application aware bandwidth limiting
B. Create a VPN policy so that direct tunnels are established to the business applications
C. Create a NAT policy so that the Cisco Firepower device does not have to translate as many addresses
D. Create a QoS policy rate-limiting high bandwidth applications

Answer: D

NEW QUESTION 37

- (Exam Topic 5)
An engineer must configure a Cisco FMC dashboard in a multidomain deployment Which action must the engineer take to edit a report template from an ancestor domain?

A. Add it as a separate widget.
B. Copy it to the current domain
C. Assign themselves ownership of it
D. Change the document attributes.

Answer: B

NEW QUESTION 39
- (Exam Topic 5)
An engineer is investigating connectivity problems on Cisco Firepower that is using service group tags.
Specific devices are not being tagged correctly, which is preventing clients from using the proper policies when going through the firewall How is this issue resolved?

A. Use traceroute with advanced options.
B. Use Wireshark with an IP subnet filter.
C. Use a packet capture with match criteria.
D. Use a packet sniffer with correct filtering

Answer: C

NEW QUESTION 42
- (Exam Topic 5)
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

Answer: D

NEW QUESTION 44
- (Exam Topic 5)
While configuring FTD, a network engineer wants to ensure that traffic passing through the appliance does not require routing or Vlan rewriting. Which interface mode should the engineer implement to accomplish this task?

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

Answer: B

NEW QUESTION 48
- (Exam Topic 5)
An engineer needs to configure remote storage on Cisco FMC. Configuration backups must be available from a secure location on the network for disaster recovery. Reports need to back up to a shared location that auditors can access with their Active Directory logins. Which strategy must the engineer use to meet these objectives?

A. Use SMB for backups and NFS for reports.
B. Use NFS for both backups and reports.
C. Use SMB for both backups and reports.
D. Use SSH for backups and NFS for reports.

Answer: C

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/syste "You cannot send backups to one remote system and reports to another, but you can choose to send either to a remote system and store the other on the Firepower Management Center."

NEW QUESTION 50
- (Exam Topic 5)
An organization has implemented Cisco Firepower without IPS capabilities and now wants to enable inspection for their traffic. They need to be able to detect protocol anomalies and utilize the Snort rule sets to detect malicious behaviour. How is this accomplished?

A. Modify the access control policy to redirect interesting traffic to the engine
B. Modify the network discovery policy to detect new hosts to inspect
C. Modify the network analysis policy to process the packets for inspection
D. Modify the intrusion policy to determine the minimum severity of an event to inspect.

Answer: D

NEW QUESTION 55

- (Exam Topic 5)
In a multi-tennent 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

Answer: B

NEW QUESTION 60
- (Exam Topic 5)
Which firewall design will allow It to forward traffic at layers 2 and 3 for the same subnet?

A. Cisco Firepower Threat Defense mode
B. routed mode
C. Integrated routing and bridging
D. transparent mode

Answer: C

Explanation:
Integrated routing and bridging (IRB) is a feature of Cisco Firepower Threat Defense (FTD) that allows the firewall to forward traffic at both layers 2 and 3 for the same subnet. In this mode, the firewall can act as a switch or a bridge to forward traffic at layer 2 and as a router to forward traffic at layer 3. This allows the firewall to maintain full control over the traffic, while still allowing it to forward traffic at both layers.
https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-config-guide/FTD-Config-Guide-v6/Integrated-Ro

NEW QUESTION 61
- (Exam Topic 5)
IT management is asking the network engineer to provide high-level summary statistics of the Cisco FTD appliance in the network. The business is approaching a peak season so the need to maintain business uptime is high. Which report type should be used to gather this information?

A. Malware Report
B. Standard Report
C. SNMP Report
D. Risk Report

Answer: B

NEW QUESTION 65
- (Exam Topic 5)
An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighbouring Cisco devices or use multicast in their environment. What must be done to resolve this issue?

A. Create a firewall rule to allow CDP traffic.
B. Create a bridge group with the firewall interfaces.
C. Change the firewall mode to routed.
D. Change the firewall mode to transparent.

Answer: C

NEW QUESTION 70
- (Exam Topic 5)
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. Maximum Detection
B. Security Over Connectivity
C. Balanced Security and Connectivity
D. Connectivity Over Security

Answer: C

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusio

NEW QUESTION 73
- (Exam Topic 5)
A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface. What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

A. Only the UDP packet type is supported.
B. The output format option for the packet logs is unavailable.
C. The destination MAC address is optional if a VLAN ID value is entered.
D. The VLAN ID and destination MAC address are optional.

Answer: C

NEW QUESTION 77
- (Exam Topic 5)
A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?

A. Add the hash to the simple custom deletion list.
B. Use regular expressions to block the malicious file.
C. Enable a personal firewall in the infected endpoint.
D. Add the hash from the infected endpoint to the network block list.

Answer: A

NEW QUESTION 80
- (Exam Topic 5)
What is the role of the casebook feature in Cisco Threat Response?

A. sharing threat analysts
B. pulling data via the browser extension
C. triage automaton with alerting
D. alert prioritization

Answer: A

Explanation:
The casebook and pivot menu are widgets available in Cisco Threat Response. Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables.
https://www.cisco.com/c/en/us/td/docs/se curity/ces/user_guide/esa_user_guide_13-5-1/b_ESA_Admin_Guide_ces
_13-5-1/b_ESA_Admin_Guide_13-0_chapter_0110001.pdf

NEW QUESTION 81
- (Exam Topic 5)
A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?

A. Use regular expressions to block the malicious file.
B. Add the hash from the infected endpoint to the network block list.
C. Add the hash to the simple custom detection list.
D. Enable a personal firewall in the infected endpoint.

Answer: C

NEW QUESTION 84
- (Exam Topic 5)
The CEO ask a network administrator to present to management a dashboard that shows custom analysis tables for the top DNS queries URL category statistics, and the URL reputation statistics.
Which action must the administrator take to quickly produce this information for management?

A. Run the Attack report and filter on DNS to show this information.
B. Create a new dashboard and add three custom analysis widgets that specify the tables needed.
C. Modify the Connection Events dashboard to display the information in a view for management.
D. Copy the intrusion events dashboard tab and modify each widget to show the correct charts.

Answer: B

NEW QUESTION 87
- (Exam Topic 5)
An administrator is configuring a transparent Cisco FTD device to receive ERSPAN traffic from multiple switches on a passive port but the FTD is not processing the traffic What is the problem?

A. The switches do not have Layer 3 connectivity to the FTD device for GRE traffic transmission.
B. The FTD must be configured with an ERSPAN port, not a passive port.
C. The FTD must &e in routed mode to process ERSPAN traffic.
D. The switches were not set up with a monitor session ID (hat matches the flow ID defined on the FTD

Answer: C

NEW QUESTION 88
- (Exam Topic 5)
Network traffic coining from an organization's CEO must never be denied. Which access control policy configuration option should be used if the deployment engineer is not permitted to create a rule to allow all traffic?

A. Configure firewall bypass.
B. Change the intrusion policy from security to balance.
C. Configure a trust policy for the CEO.
D. Create a NAT policy just for the CEO.

Answer: C

NEW QUESTION 92
- (Exam Topic 5)
A security engineer must configure a Cisco FTD appliance to inspect traffic coming from the internet. The Internet traffic will be mirrored from the Cisco Catalyst 9300 Switch. Which configuration accomplishes the task?

A. Set interface configuration mode to none.
B. Set the firewall mode to transparent.
C. Set the firewall mode to routed.
D. Set interface configuration mode to passive.

Answer: D

NEW QUESTION 95
- (Exam Topic 5)
Which feature within the Cisco FMC web interface allows for detecting, analyzing and blocking malware in network traffic?

A. intrusion and file events
B. Cisco AMP for Endpoints
C. Cisco AMP for Networks
D. file policies

Answer: C

NEW QUESTION 96
- (Exam Topic 5)
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 addresses globally in the quickest way possible and with the least amount of impact?

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

Answer: D

NEW QUESTION 97
- (Exam Topic 5)
An engineer attempts to pull the configuration for a Cisco FTD sensor to review with Cisco TAC but does not have direct access to the CU for the device. The CLI for the device is managed by Cisco FMC to which the engineer has access. Which action in Cisco FMC grants access to the CLI for the device?

A. Export the configuration using the Import/Export tool within Cisco FMC.
B. Create a backup of the configuration within the Cisco FMC.
C. Use the show run all command in the Cisco FTD CLI feature within Cisco FMC.
D. Download the configuration file within the File Download section of Cisco FMC.

Answer: A

NEW QUESTION 101
- (Exam Topic 5)
An organization has a compliancy 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. Deploy a firewall in transparent mode between the clients and servers.
B. Change the IP addresses of the clients, while remaining on the same subnet.
C. Deploy a firewall in routed mode between the clients and servers
D. Change the IP addresses of the servers, while remaining on the same subnet

Answer: A

NEW QUESTION 106
- (Exam Topic 5)
A security engineer is deploying a pair of primary and secondary Cisco FMC devices. The secondary must also receive updates from Cisco Talos. Which action achieves this goal?

A. Force failover for the secondary Cisco FMC to synchronize the rule updates from the primary.
B. Configure the secondary Cisco FMC so that it receives updates from Cisco Talos.
C. Manually import rule updates onto the secondary Cisco FMC device.
D. Configure the primary Cisco FMC so that the rules are updated.

Answer: D

NEW QUESTION 107
- (Exam Topic 5)
Upon detecting a flagrant threat on an endpoint, which two technologies instruct Cisco Identity Services Engine to contain the infected endpoint either manually or automatically? (Choose two.)

A. Cisco ASA 5500 Series

B. Cisco FMC
C. Cisco AMP
D. Cisco Stealthwatch
E. Cisco ASR 7200 Series

Answer: CD

NEW QUESTION 111
- (Exam Topic 5)
An engineer wants to change an existing transparent Cisco FTD to routed mode.
The device controls traffic between two network segments. Which action is mandatory to allow hosts to reestablish communication between these two segments after the change?

A. remove the existing dynamic routing protocol settings.
B. configure multiple BVIs to route between segments.
C. assign unique VLAN IDs to each firewall interface.
D. implement non-overlapping IP subnets on each segment.

Answer: D

NEW QUESTION 115
- (Exam Topic 5)
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. event viewer
B. reports
C. dashboards
D. context explorer

Answer: B

NEW QUESTION 116
- (Exam Topic 4)
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

Answer: CD

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

NEW QUESTION 117
- (Exam Topic 4)
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.

Answer: A

NEW QUESTION 118
- (Exam Topic 5)
An engineer must define a URL object on Cisco FMC. What is the correct method to specify the URL without performing SSL inspection?

A. Use Subject Common Name value.
B. Specify all subdomains in the object group.
C. Specify the protocol in the object.
D. Include all URLs from CRL Distribution Points.

Answer: B

NEW QUESTION 119
- (Exam Topic 5)
A network administrator discovers that a user connected to a file server and downloaded a malware file. The Cisc FMC generated an alert for the malware event, however the user still remained connected. Which Cisco APM file rule action within the Cisco FMC must be set to resolve this issue?

A. Detect Files
B. Malware Cloud Lookup
C. Local Malware Analysis

D. Reset Connection

Answer: D

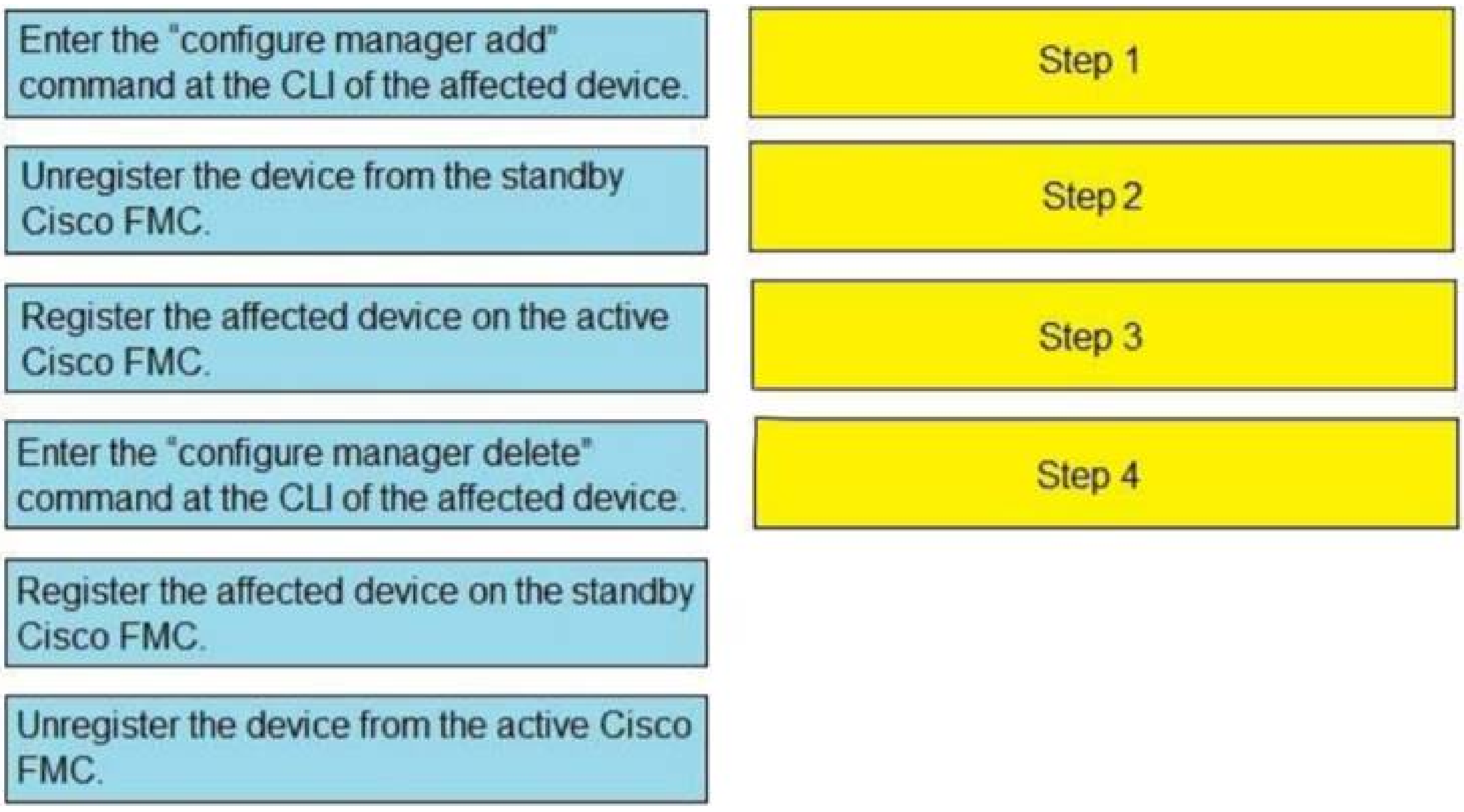
NEW QUESTION 123
- (Exam Topic 3)
After deploying a network-monitoring tool to manage and monitor networking devices in your organization, you realize that you need to manually upload an MIB for the Cisco FMC. In which folder should you upload the MIB file?

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

Answer: C

Explanation:
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

NEW QUESTION 128
- (Exam Topic 3)
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.



Enter the "configure manager add" command at the CLI of the affected device.

Unregister the device from the standby Cisco FMC.

Register the affected device on the active Cisco FMC.

Enter the "configure manager delete" command at the CLI of the affected device.

Register the affected device on the standby Cisco FMC.

Unregister the device from the active Cisco FMC.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
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

NEW QUESTION 131
- (Exam Topic 4)
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

Answer: AB

NEW QUESTION 136
- (Exam Topic 3)
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

Answer: C

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

NEW QUESTION 137
- (Exam Topic 3)
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

Answer: B

Explanation:
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

NEW QUESTION 141
- (Exam Topic 3)
Which limitation applies to Cisco Firepower Management Center dashboards in a multidomain environment?

A. Child domains can 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 can view dashboards.
D. Child domains cannot view dashboards that originate from an ancestor domain.

Answer: D

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

NEW QUESTION 144
- (Exam Topic 3)
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

Answer: D

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

NEW QUESTION 147
- (Exam Topic 3)
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-enabled

Answer: A

NEW QUESTION 149
- (Exam Topic 3)
Which two statements about deleting and re-adding a device to Cisco FMC are true? (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, you must add the manager back in the device.
C. No option to delete and re-add a device is available in the Cisco FMC web interface.
D. The Cisco FMC web interface prompts users to re-apply access control policies.
E. No option to re-apply NAT and VPN policies during registration is available, so users need to re-apply the policies after registration is completed.

Answer: DE

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

NEW QUESTION 153
- (Exam Topic 3)
What is the maximum bit size that Cisco FMC supports for HTTPS certificates?

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

Answer: C

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

NEW QUESTION 155
- (Exam Topic 3)
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

Answer: A

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

NEW QUESTION 156
- (Exam Topic 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

Answer: BE

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

NEW QUESTION 159
- (Exam Topic 2)
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 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.
B. 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.
C. 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.
D. 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.

Answer: A

NEW QUESTION 164
- (Exam Topic 2)
When creating a report template, how can the results be limited to show only the activity of a specific subnet?

A. Create a custom search in Firepower Management Center 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.

Answer: B

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

NEW QUESTION 167
- (Exam Topic 2)
A company has many Cisco FTD devices managed by a Cisco FMC. The security model requires that access control rule logs be collected for analysis. The security engineer is concerned that the Cisco FMC will not be able to process the volume of logging that will be generated. Which configuration addresses this concern?

A. Send Cisco FTD connection events and security events directly to SIEM system for storage and analysis.
B. Send Cisco FTD connection events and security events to a cluster of Cisco FMC devices for storage and analysis.
C. Send Cisco FTD connection events and security events to Cisco FMC and configure it to forward logs to SIEM for storage and analysis.
D. Send Cisco FTD connection events directly to a SIEM system and forward security events from Cisco FMC to the SIEM system for storage and analysis.

Answer: C

NEW QUESTION 169
- (Exam Topic 2)
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

Answer: D

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

NEW QUESTION 170
- (Exam Topic 2)
Which two statements about bridge-group interfaces in Cisco FTD are true? (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.

Answer: BE

Explanation:
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

NEW QUESTION 171
- (Exam Topic 1)
Which firewall design allows a firewall to forward traffic at layer 2 and layer 3 for the same subnet?

A. Cisco Firepower Threat Defense mode
B. transparent mode
C. routed mode
D. integrated routing and bridging

Answer: B

NEW QUESTION 176
- (Exam Topic 1)
An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic concurrently. How must the devices be implemented in this environment?

A. in active/active mode
B. in a cluster span EtherChannel
C. in active/passive mode
D. in cluster interface mode

Answer: C

NEW QUESTION 177
- (Exam Topic 1)
Within an organization's high availability environment where both firewalls are passing traffic, traffic must be segmented based on which department it is destined for. Each department is situated on a different LAN. What must be configured to meet these requirements?

A. span EtherChannel clustering
B. redundant interfaces
C. high availability active/standby firewalls
D. multi-instance firewalls

Answer: D

NEW QUESTION 182
- (Exam Topic 1)
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

Answer: CE

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

NEW QUESTION 184
- (Exam Topic 1)
Which interface type allows packets to be dropped?

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

Answer: B

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

NEW QUESTION 189
- (Exam Topic 1)
Which protocol establishes network redundancy in a switched Firepower device deployment?

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

Answer: A

Explanation:
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

NEW QUESTION 194
- (Exam Topic 1)
A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?

A. Specify the BVl IP address as the default gateway for connected devices.
B. Enable routing on the Cisco Firepower
C. Add an IP address to the physical Cisco Firepower interfaces.
D. Configure a bridge group in transparent mode.

Answer: D

Explanation:
Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place. Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.

NEW QUESTION 197
- (Exam Topic 1)
With Cisco Firepower Threat Defense 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

Answer: B

Explanation:
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

NEW QUESTION 200
- (Exam Topic 1)
An engineer is configuring a Cisco IPS to protect the network and wants to test a policy before deploying it. A copy of each incoming packet needs to be monitored while traffic flow remains constant. Which IPS mode should be implemented to meet these requirements?

A. Inline tap
B. passive
C. transparent
D. routed

Answer: A

NEW QUESTION 202
- (Exam Topic 1)
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.

Answer: AE

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

NEW QUESTION 203
......