Cisco

Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

NEW QUESTION 1
- (Exam Topic 5)
An administrator Is setting up a Cisco PMC and must provide expert mode access for a security engineer. The engineer Is permitted to use only a secured out-of-band network workstation with a static IP address to access the Cisco FMC. What must be configured to enable this access?

A. Enable SSH and define an access list.
B. Enable HTTP and define an access list.
C. Enable SCP under the Access List section.
D. Enable HTTPS and SNMP under the Access List section.

Answer: A

NEW QUESTION 2
- (Exam Topic 5)
A user within an organization opened a malicious file on a workstation which in turn caused a ransomware attack on the network. What should be configured within the Cisco FMC to ensure the file is tested for viruses on a sandbox system?

A. Capacity handling
B. Local malware analysis
C. Spere analysis
D. Dynamic analysis

Answer: D

NEW QUESTION 3
- (Exam Topic 5)
An engineer is monitoring network traffic from their sales and product development departments, which are on two separate networks What must be configured in order to maintain data privacy for both departments?

A. Use a dedicated IPS inline set for each department to maintain traffic separation
B. Use 802 1Q mime set Trunk interfaces with VLANs to maintain logical traffic separation
C. Use passive IDS ports for both departments
D. Use one pair of inline set in TAP mode for both departments

Answer: B

NEW QUESTION 4
- (Exam Topic 5)
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 applicable rules?

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

Answer: D

NEW QUESTION 5
- (Exam Topic 5)
A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https://<FMC IP>/capture/CAPI/pcap/test.pcap. an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

A. Disable the HTTPS server and use HTTP instead.
B. Enable the HTTPS server for the device platform policy.
C. Disable the proxy setting on the browser.
D. Use the Cisco FTD IP address as the proxy server setting on the browser.

Answer: B

NEW QUESTION 6
- (Exam Topic 5)
A VPN user is unable to conned lo web resources behind the Cisco FTD device terminating the connection. While troubleshooting, the network administrator determines that the DNS responses are not getting through the Cisco FTD What must be done to address this issue while still utilizing Snort IPS rules?

A. Uncheck the "Drop when Inline" box in the intrusion policy to allow the traffic.
B. Modify the Snort rules to allow legitimate DNS traffic to the VPN users.
C. Disable the intrusion rule threshes to optimize the Snort processing.
D. Decrypt the packet after the VPN flow so the DNS queries are not inspected

Answer: B

NEW QUESTION 7

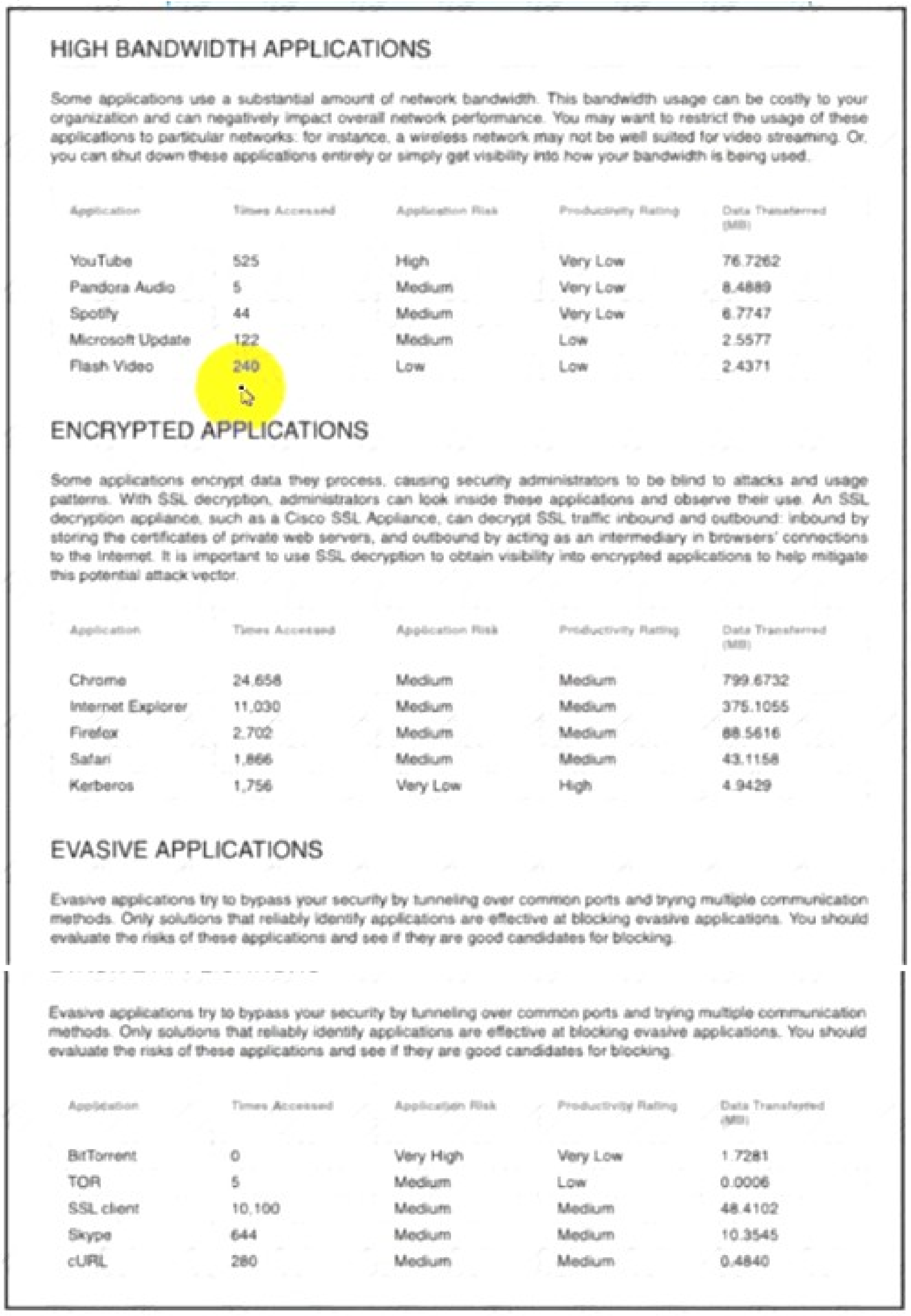
- (Exam Topic 5)
An engineer is configuring a second Cisco FMC as a standby device but is unable to register with the active unit. What is causing this issue?

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)



HIGH BANDWIDTH APPLICATIONS

Some applications use a substantial amount of network bandwidth. This bandwidth usage can be costly to your organization and can negatively impact overall network performance. You may want to restrict the usage of these applications to particular networks: for instance, a wireless network may not be well suited for video streaming. Or, you can shut down these applications entirely or simply get visibility into how your bandwidth is being used.

Application	Times Accessed	Application Risk	Productivity Rating	Data Transferred (MB)
YouTube	525	High	Very Low	76.7262
Pandora Audio	5	Medium	Very Low	8.4889
Spotify	44	Medium	Very Low	6.7747
Microsoft Update	122	Medium	Low	2.5577
Flash Video	240	Low	Low	2.4371

ENCRYPTED APPLICATIONS

Some applications encrypt data they process, causing security administrators to be blind to attacks and usage patterns. With SSL decryption, administrators can look inside these applications and observe their use. An SSL decryption appliance, such as a Cisco SSL Appliance, can decrypt SSL traffic inbound and outbound: inbound by storing the certificates of private web servers, and outbound by acting as an intermediary in browsers' connections to the Internet. It is important to use SSL decryption to obtain visibility into encrypted applications to help mitigate this potential attack vector.

Application	Times Accessed	Application Risk	Productivity Rating	Data Transferred (MB)
Chrome	24,658	Medium	Medium	799.6732
Internet Explorer	11,030	Medium	Medium	375.1055
Firefox	2,702	Medium	Medium	88.5616
Safari	1,866	Medium	Medium	43.1158
Kerberos	1,756	Very Low	High	4.9429

EVASIVE APPLICATIONS

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

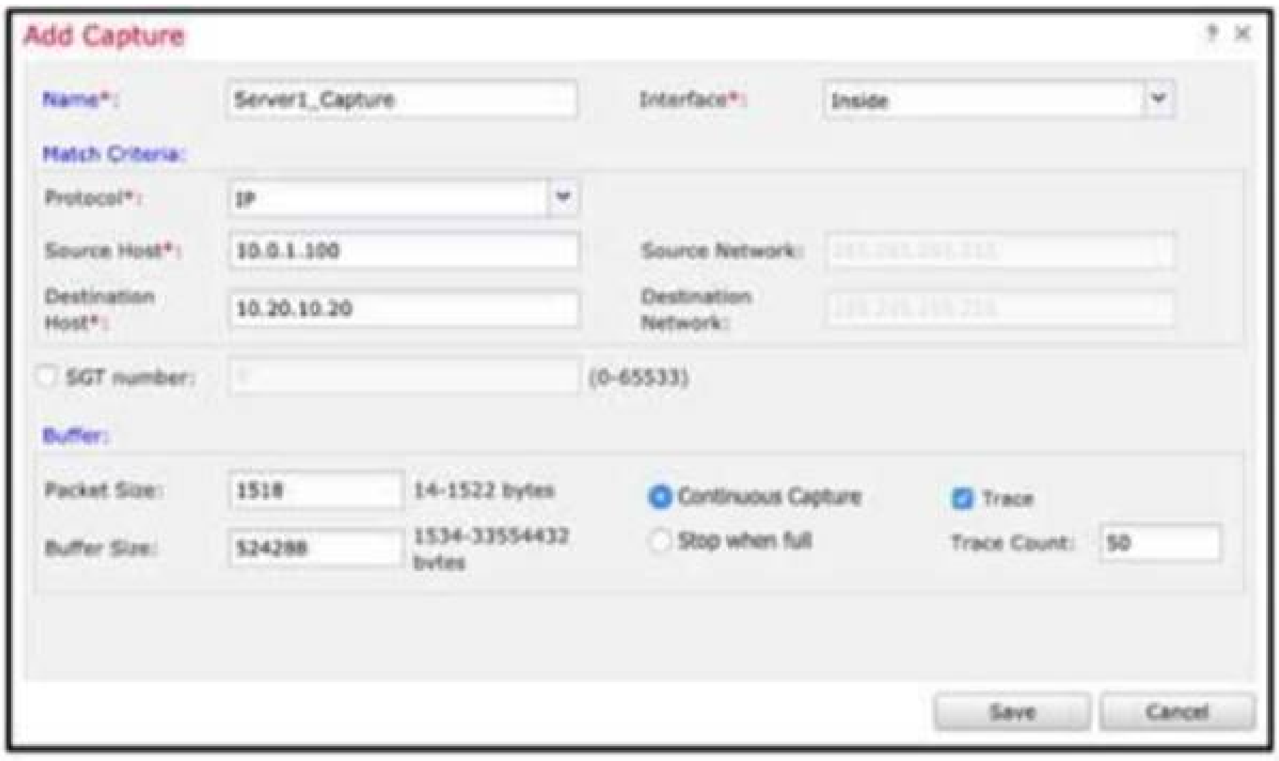
Application	Times Accessed	Application Risk	Productivity Rating	Data Transferred (MB)
BitTorrent	0	Very High	Very Low	1.7281
TOR	5	Medium	Low	0.0006
SSL client	10,100	Medium	Medium	48.4102
Skype	644	Medium	Medium	10.3545
cURL	280	Medium	Medium	0.4840

Refer to the exhibit. An engineer is analyzing a Network Risk Report from Cisco FMC. Which application must the engineer take immediate action against to prevent unauthorized network use?

A. Kerberos
B. YouTube
C. Chrome
D. TOR

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: 255.255.255.255
Destination Host*: 10.20.10.20
Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

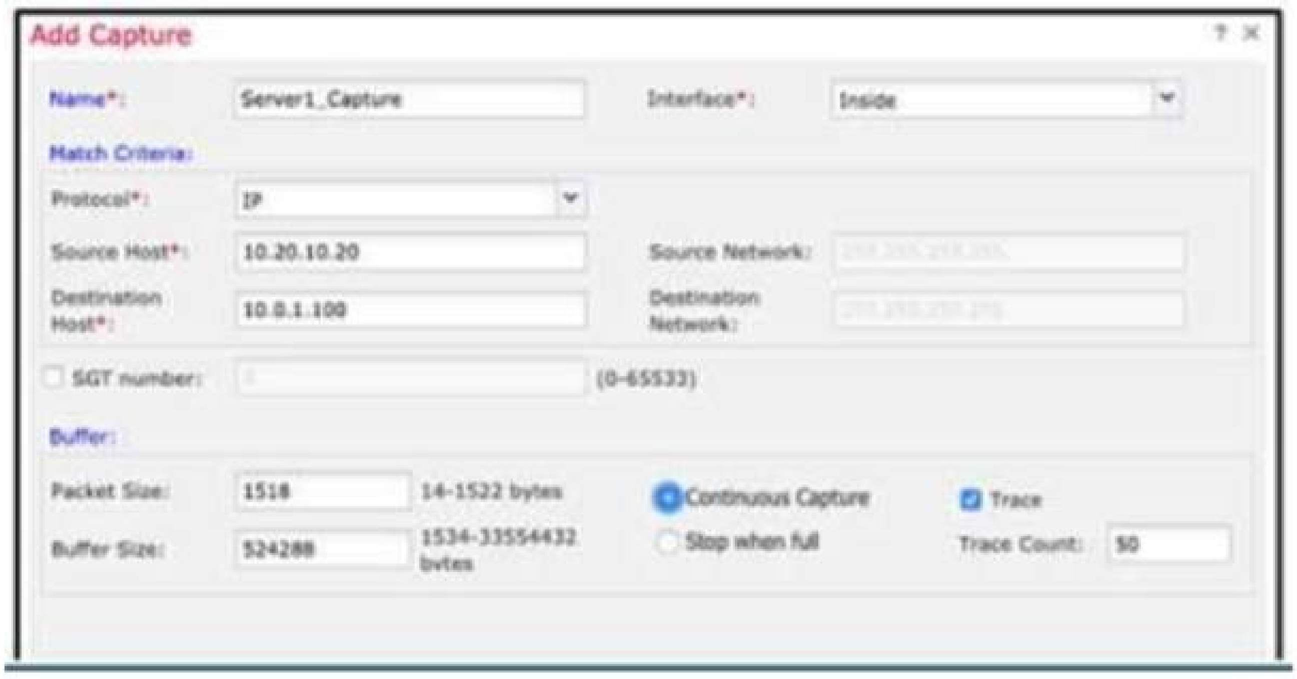
Buffer:

Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 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)

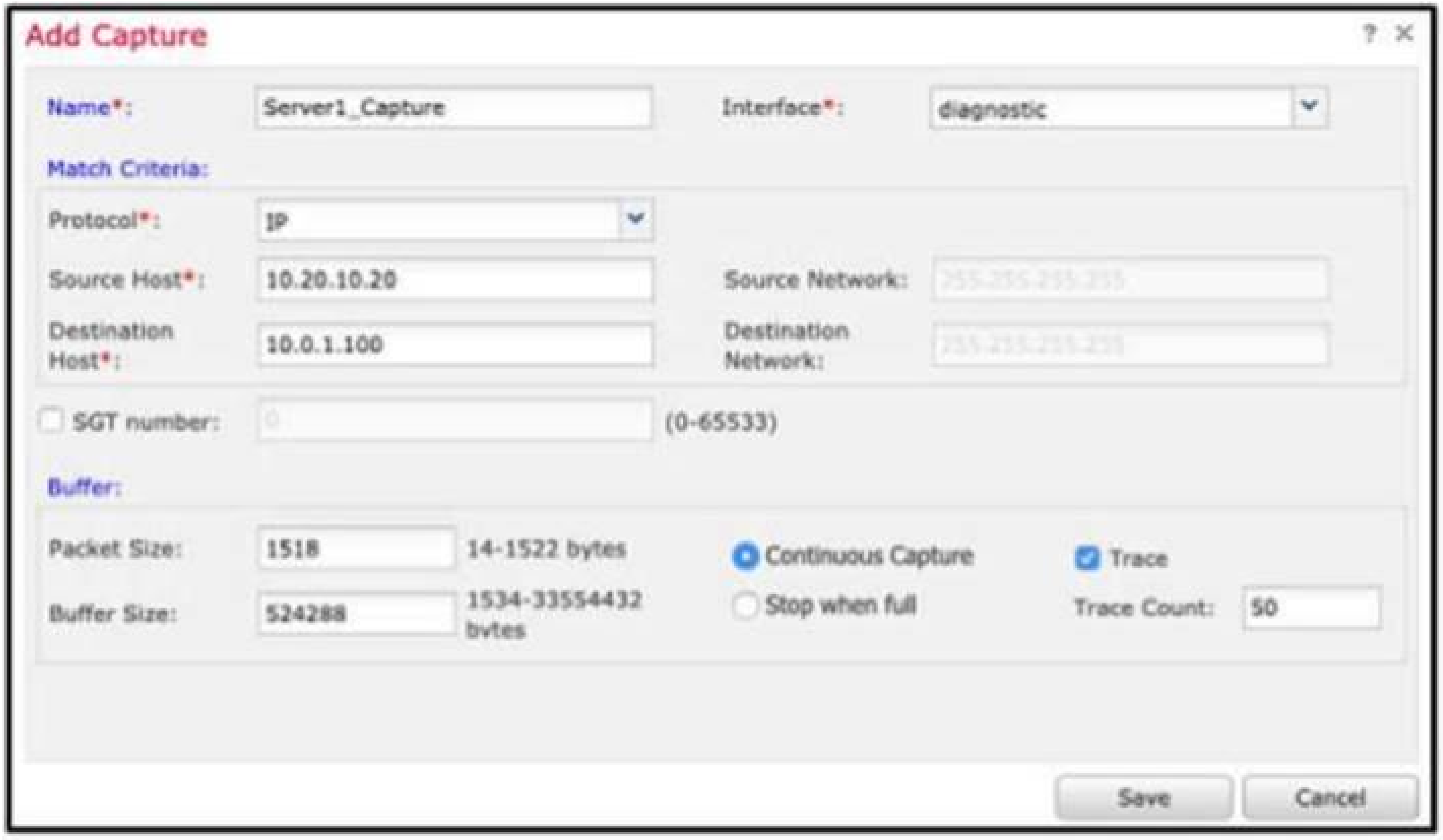
Buffer:

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)

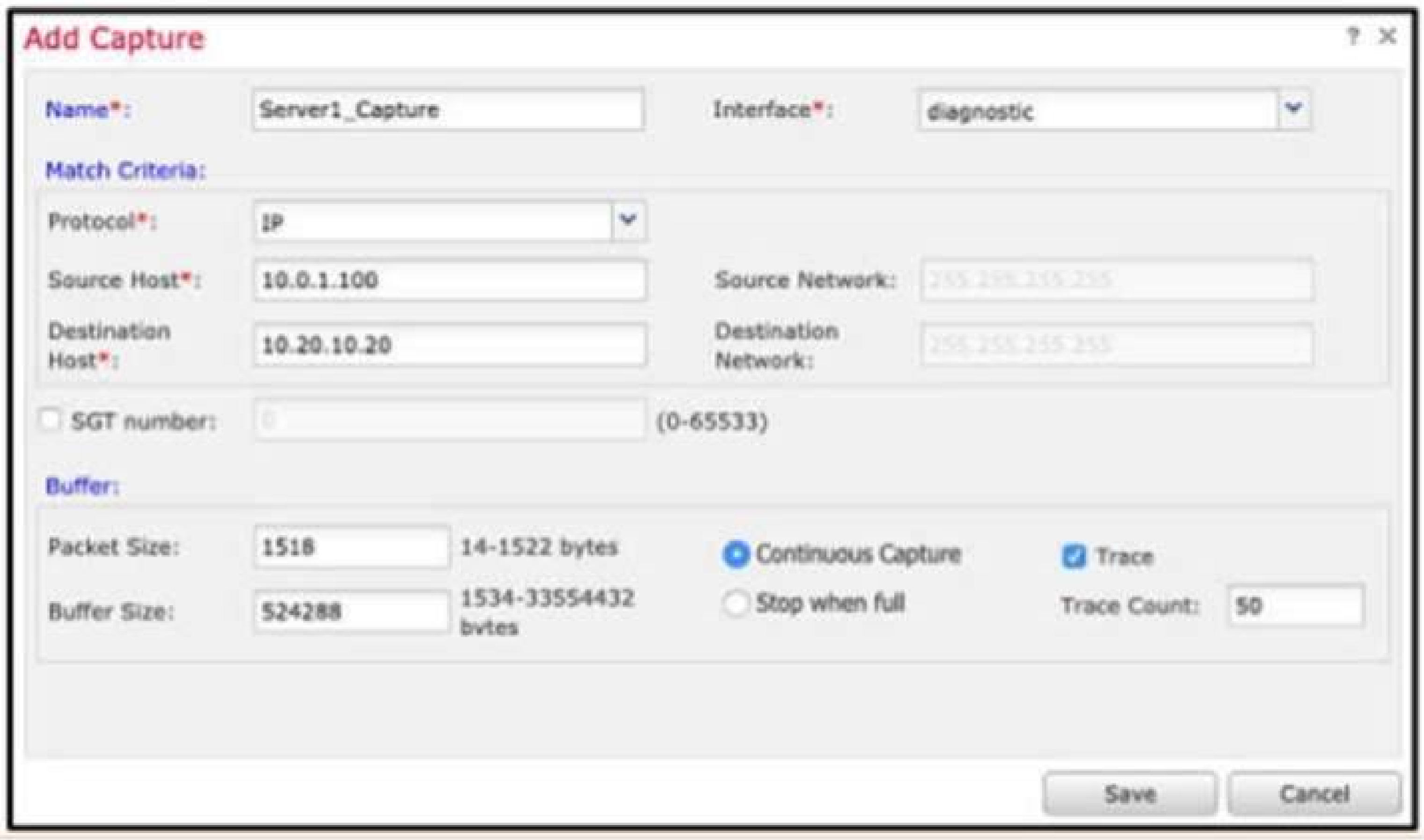
Buffer:

Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 bytes

● 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 bytes
● 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)
Which feature is supported by IRB on Cisco FTD devices?

A. redundant interface
B. dynamic routing protocol
C. EtherChannel interface
D. high-availability cluster

Answer: B

NEW QUESTION 10
- (Exam Topic 5)
An engineer is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of ACME001 and a password of Cisco388267669. Which command set must be used in order to accomplish this?

A. configure manager add ACME001 <registration key> <FMC IP>
B. configure manager add <FMC IP> ACME0O1 <registration key>
C. configure manager add DONTRESOLVE <FMC IP> AMCE001 <registration key>
D. configure manager add <FMC IP> registration key> ACME001

Answer: D

NEW QUESTION 12
- (Exam Topic 5)
An engineer installs a Cisco FTD device and wants to inspect traffic within the same subnet passing through a firewall and inspect traffic destined to the internet. Which configuration will meet this requirement?

A. transparent firewall mode with IRB only
B. routed firewall mode with BVI and routed interfaces
C. transparent firewall mode with multiple BVIs
D. routed firewall mode with routed interfaces only

Answer: C

NEW QUESTION 15
- (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 18
- (Exam Topic 5)
An engineer configures an access control rule that deploys file policy configurations to security zones or tunnel zones, and it causes the device to restart. What is the reason for the restart?

A. Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.
B. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.
C. Source or destination security zones in the source tunnel zone do not match the security zones that are associated with interfaces on the target devices.
D. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.

Answer: A

NEW QUESTION 19
- (Exam Topic 5)
An organization must be able to ingest NetFlow traffic from their Cisco FTD device to Cisco Stealthwatch for behavioral analysis. What must be configured on the Cisco FTD to meet this requirement?

A. flexconfig object for NetFlow
B. interface object to export NetFlow
C. security intelligence object for NetFlow
D. variable set object for NetFlow

Answer: A

NEW QUESTION 24
- (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 25
- (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 30
- (Exam Topic 5)
An organization is installing a new Cisco FTD appliance in the network. An engineer is tasked with configuring access between two network segments within the same IP subnet. Which step is needed to accomplish this task?

A. Assign an IP address to the Bridge Virtual Interface.
B. Permit BPDU packets to prevent loops.
C. Specify a name for the bridge group.
D. Add a separate bridge group for each segment.

Answer: A

NEW QUESTION 33
- (Exam Topic 5)
A network administrator configured a NAT policy that translates a public IP address to an internal web server IP address. An access policy has also been created that allows any source to reach the public IP address on port 80. The web server is still not reachable from the Internet on port 80. Which configuration change is needed?

A. The intrusion policy must be disabled for port 80.
B. The access policy rule must be configured for the action trust.
C. The NAT policy must be modified to translate the source IP address as well as destination IP address.
D. The access policy must allow traffic to the internal web server IP address.

Answer: D

NEW QUESTION 35

- (Exam Topic 5)
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.

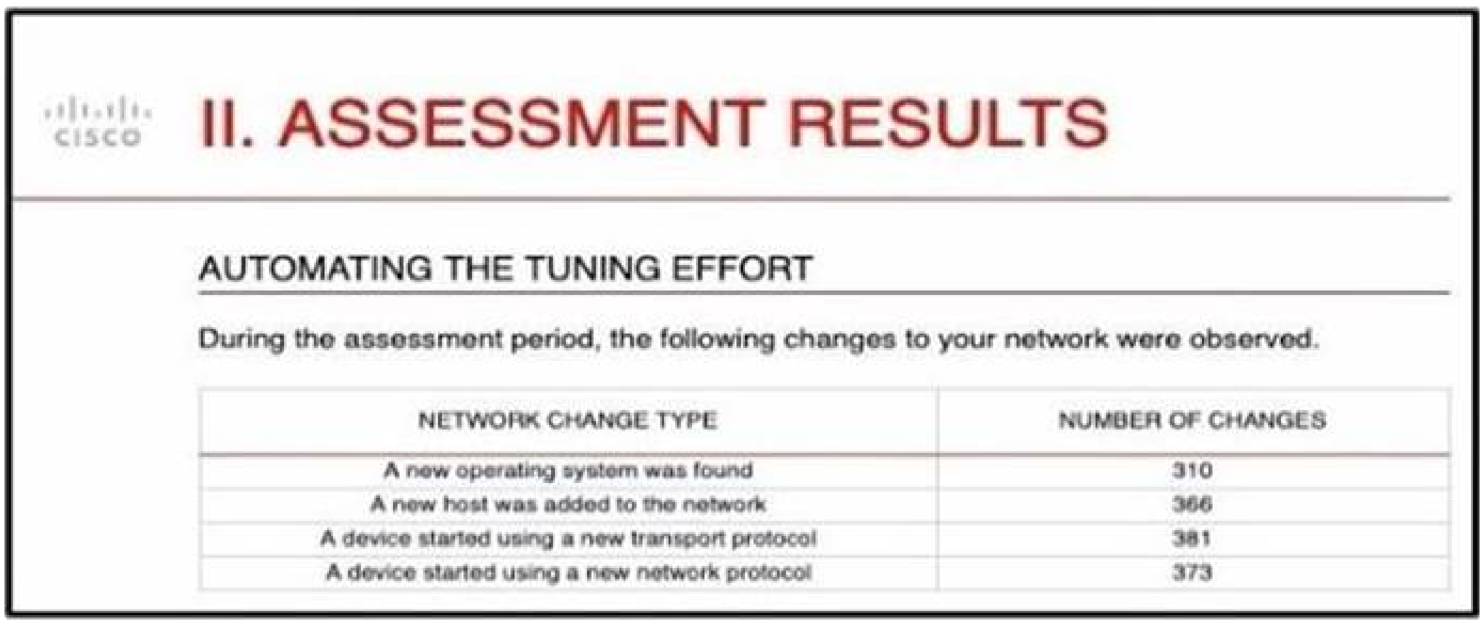
Answer: A

NEW QUESTION 39
- (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 44
- (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 45
- (Exam Topic 5)
An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down. What must be configured to accomplish this task?

A. redundant interfaces on the firewall cluster mode and switches
B. redundant interfaces on the firewall noncluster mode and switches
C. vPC on the switches to the interface mode on the firewall duster
D. vPC on the switches to the span EtherChannel on the firewall cluster

Answer: D

Explanation:
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKSEC-2020.pdf

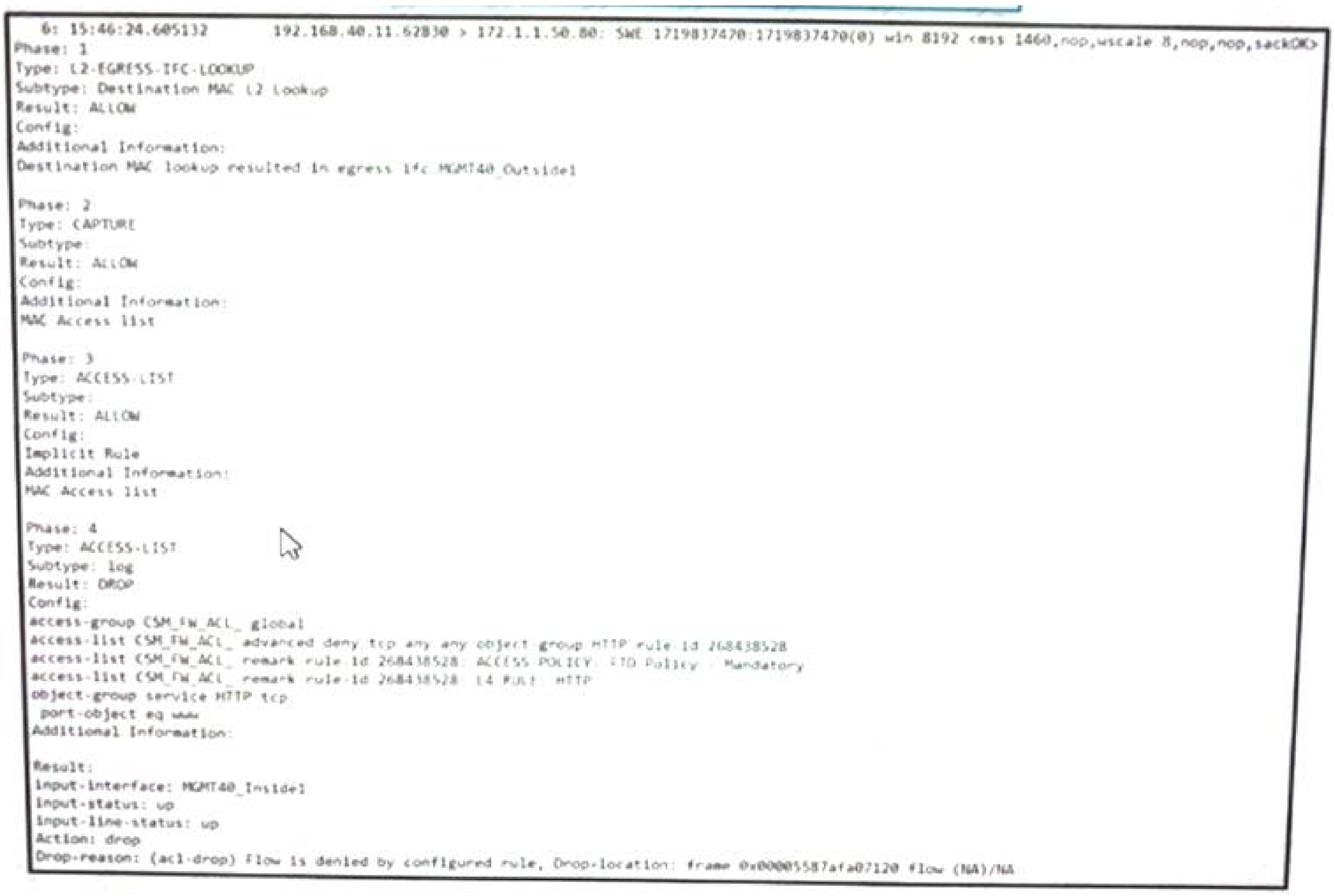
NEW QUESTION 48
- (Exam Topic 5)
A security analyst must create a new report within Cisco FMC to show an overview of the daily attacks, vulnerabilities, and connections. The analyst wants to reuse specific dashboards from other reports to create this consolidated one. Which action accomplishes this task?

A. Create a new dashboard object via Object Management to represent the desired views.

B. Modify the Custom Workflows within the Cisco FMC to feed the desired data into the new report.
C. Copy the Malware Report and modify the sections to pull components from other reports.
D. Use the import feature in the newly created report to select which dashboards to add.

Answer: D

NEW QUESTION 49
- (Exam Topic 5)
Refer to the exhibit.



```
   6: 15:46:24.605132       192.168.40.11.62830 > 172.1.1.50.80: SWE 1719837470:1719837470(0) win 8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC lookup resulted in egress ifc MGMT40_Outside1

Phase: 2
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny tcp any any object-group HTTP rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: HTTP
object-group service HTTP tcp
 port-object eq www
Additional Information:

Result:
input-interface: MGMT40_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x00005587afa07120 flow (NA)/NA
```

What must be done to fix access to this website while preventing the same communication to all other websites?

A. Create an intrusion policy rule to have Snort allow port 80 to only 172.1.1 50.
B. Create an access control policy rule to allow port 80 to only 172.1.1 50.
C. Create an intrusion policy rule to have Snort allow port 443 to only 172.1.1.50
D. Create an access control policy rule to allow port 443 to only 172.1.1 50

Answer: B

NEW QUESTION 53
- (Exam Topic 5)
An organization is implementing Cisco FTD using transparent mode in the network. Which rule in the default Access Control Policy ensures that this deployment does not create a loop in the network?

A. ARP inspection is enabled by default.
B. Multicast and broadcast packets are denied by default.
C. STP BPDU packets are allowed by default.
D. ARP packets are allowed by default.

Answer: B

NEW QUESTION 55
- (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 57
- (Exam Topic 5)
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. All types of Cisco Firepower devices are supported.

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

Answer: B

NEW QUESTION 60
- (Exam Topic 5)
Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC (Choose two).

A. Before re-adding the device In Cisco FMC, the manager must be added back.
B. The Cisco FMC web interface prompts users to re-apply access control policies.
C. Once a device has been deleted, It must be reconfigured before it is re-added to the Cisco FMC.
D. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re-apply the polices after registration is completed.
E. There is 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: BE

NEW QUESTION 65
- (Exam Topic 5)
An engineer is troubleshooting application failures through a 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 application-identification-debug command to determine which rules the traffic matching and modify the rule accordingly
C. Use the system support firewall-engine-dump-user-f density-data command to change the policy and allow the application through the firewall.
D. Use the system support network-options command to fine tune the policy.

Answer: A

NEW QUESTION 66
- (Exam Topic 5)
An administrator needs to configure Cisco FMC to send a notification email when a data transfer larger than 10 MB is initiated from an internal host outside of standard business hours. Which Cisco FMC feature must be configured to accomplish this task?

A. file and malware policy
B. application detector
C. intrusion policy
D. correlation policy

Answer: A

NEW QUESTION 71
- (Exam Topic 5)
The network administrator wants to enhance the network security posture by enabling machine learning tor malware detection due to a concern with suspicious Microsoft executable file types that were seen while creating monthly security reports for the CIO. Which feature must be enabled to accomplish this goal?

A. Spero
B. dynamic analysis
C. static analysis
D. Ethos

Answer: A

NEW QUESTION 76
- (Exam Topic 5)
An engineer wants to perform a packet capture on the Cisco FTD to confirm that the host using IP address 192 168.100.100 has the MAC address of 0042 7734.103 to help troubleshoot a connectivity issue What is the correct tcpdump command syntax to ensure that the MAC address appears in the packet capture output?

A. -nm src 192.168.100.100
B. -ne src 192.168.100.100
C. -w capture.pcap -s 1518 host 192.168.100.100 mac
D. -w capture.pcap -s 1518 host 192.168.100.100 ether

Answer: B

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

NEW QUESTION 80
- (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 85
- (Exam Topic 5)
An engineer wants to add an additional Cisco FTD Version 6.2.3 device to their current 6.2.3 deployment to create a high availability pair.
The currently deployed Cisco FTD device is using local management and identical hardware including the available port density to enable the failover and stateful links required in a proper high availability deployment. Which action ensures that the environment is ready to pair the new Cisco FTD with the old one?

A. Change from Cisco FDM management to Cisco FMC management on both devices and register them to FMC.
B. Ensure that the two devices are assigned IP addresses from the 169 254.0.0/16 range for failover interfaces.
C. Factory reset the current Cisco FTD so that it can synchronize configurations with the new Cisco FTD device.
D. Ensure that the configured DNS servers match on the two devices for name resolution.

Answer: A

NEW QUESTION 88
- (Exam Topic 5)
A network administrator has converted a Cisco FTD from using LDAP to LDAPS for VPN authentication. The Cisco FMC can connect to the LDAPS server, but the Cisco FTD is not connecting. Which configuration must be enabled on the Cisco FTD?

A. SSL must be set to a use TLSv1.2 or lower.
B. The LDAPS must be allowed through the access control policy.
C. DNS servers must be defined for name resolution.
D. The RADIUS server must be defined.

Answer: B

NEW QUESTION 92
- (Exam Topic 5)
A network administrator notices that inspection has been interrupted on all non-managed interfaces of a device. What is the cause of this?

A. The value of the highest MTU assigned to any non-management interface was changed.
B. The value of the highest MSS assigned to any non-management interface was changed.
C. A passive interface was associated with a security zone.
D. Multiple inline interface pairs were added to the same inline interface.

Answer: A

NEW QUESTION 94
- (Exam Topic 5)
An administrator is adding a new URL-based category feed to the Cisco FMC for use within the policies. The intelligence source does not use STIX. but instead uses a .txt file format. Which action ensures that regular updates are provided?

A. Add a URL source and select the flat file type within Cisco FMC.
B. Upload the .txt file and configure automatic updates using the embedded URL.
C. Add a TAXII feed source and input the URL for the feed.
D. Convert the .txt file to STIX and upload it to the Cisco FMC.

Answer: A

NEW QUESTION 96
- (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 101
- (Exam Topic 5)
An administrator receives reports that users cannot access a cloud-hosted web server. The access control policy was recently updated with several new policy additions and URL filtering. What must be done to troubleshoot the issue and restore access without sacrificing the organization's security posture?

A. Create a new access control policy rule to allow ports 80 and 443 to the FQDN of the web server.

B. Identify the blocked traffic in the Cisco FMC connection events to validate the block, and modify the policy to allow the traffic to the web server.
C. Verify the blocks using the packet capture tool and create a rule with the action monitor for the traffic.
D. Download a PCAP of the traffic attempts to verify the blocks and use the flexconfig objects to create a rule that allows only the required traffic to the destination server.

Answer: B

NEW QUESTION 104
- (Exam Topic 5)
What must be implemented on Cisco Firepower to allow multiple logical devices on a single physical device to have access to external hosts?

A. Add at least two container instances from the same module.
B. Set up a cluster control link between all logical devices
C. Add one shared management interface on all logical devices.
D. Define VLAN subinterfaces for each logical device.

Answer: C

NEW QUESTION 106
- (Exam Topic 5)
A network administrator is deploying a Cisco IPS appliance and needs it to operate initially without affecting traffic flows.
It must also collect data to provide a baseline of unwanted traffic before being reconfigured to drop it. Which Cisco IPS mode meets these requirements?

A. failsafe
B. inline tap
C. promiscuous
D. bypass

Answer: B

NEW QUESTION 108
- (Exam Topic 5)
A security engineer must integrate an external feed containing STIX/TAXII data with Cisco FMC. Which feature must be enabled on the Cisco FMC to support this connection?

A. Cisco Success Network
B. Cisco Secure Endpoint Integration
C. Threat Intelligence Director
D. Security Intelligence Feeds

Answer: C

NEW QUESTION 109
- (Exam Topic 5)
A network administrator is configuring a Cisco AMP public cloud instance and wants to capture infections and polymorphic variants of a threat to help detect families of malware. Which detection engine meets this requirement?

A. RBAC
B. Tetra
C. Ethos
D. Spero

Answer: C

NEW QUESTION 112
- (Exam Topic 5)
When using Cisco Threat Response, which phase of the Intelligence Cycle publishes the results of the investigation?

A. direction
B. dissemination
C. processing
D. analysis

Answer: B

Explanation:
Disseminate: The dissemination phase
publishes the results of the investigation or threat hunt. This
information is disseminated with a focus on the receivers of the information. At the tactical level, this information feeds back into the beginning of the F3EAD model, Find. Figure 3 illustrates the F3EAD model.

NEW QUESTION 114
- (Exam Topic 5)
A network engineer must provide redundancy between two Cisco FTD devices. The redundancy configuration must include automatic configuration, translation, and connection updates. After the initial configuration of the two appliances, which two steps must be taken to proceed with the redundancy configuration? (Choose two.)

A. Configure the virtual MAC address on the failover link.
B. Disable hellos on the inside interface.
C. Configure the standby IP addresses.
D. Ensure the high availability license is enabled.
E. Configure the failover link with stateful properties.

Answer: AC

NEW QUESTION 119
- (Exam Topic 5)
An organization recently implemented a transparent Cisco FTD in their network. They must ensure that the device does not respond to insecure SSL/TLS protocols. Which action accomplishes the task?

A. Modify the device's settings using the device management feature within Cisco FMC to force onlysecure protocols.
B. Use the Cisco FTD platform policy to change the minimum SSL version on the device to TLS 1.2.
C. Enable the UCAPL/CC compliance on the device to support only the most secure protocols available.
D. Configure a FlexConfig object to disable any insecure TLS protocols on the Cisco FTD device.

Answer: B

NEW QUESTION 120
- (Exam Topic 5)
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 Troubleshoot" file for the device in question.
B. A "show tech" file for the device in question
C. A "show tech" for the Cisco FMC.
D. A "troubleshoot" file for the Cisco FMC

Answer: A

NEW QUESTION 124
- (Exam Topic 5)
An organization is setting up two new Cisco FTD devices to replace their current firewalls and cannot have any network downtime During the setup process, the synchronization between the two devices is failing What action is needed to resolve this issue?

A. Confirm that both devices have the same port-channel numbering
B. Confirm that both devices are running the same software version
C. Confirm that both devices are configured with the same types of interfaces
D. Confirm that both devices have the same flash memory sizes

Answer: B

NEW QUESTION 127
- (Exam Topic 5)
An engineer wants to connect a single IP subnet through a Cisco FTD firewall and enforce policy. There is a requirement to present the internal IP subnet to the outside as a different IP address. What must be configured to meet these requirements?

A. Configure the downstream router to perform NAT.
B. Configure the upstream router to perform NAT.
C. Configure the Cisco FTD firewall in routed mode with NAT enabled.
D. Configure the Cisco FTD firewall in transparent mode with NAT enabled.

Answer: C

NEW QUESTION 128
- (Exam Topic 5)
An organization has a Cisco IPS running in inline mode and is inspecting traffic for malicious activity. When traffic is received by the Cisco IRS, if it is not dropped, how does the traffic get to its destination?

A. It is retransmitted from the Cisco IPS inline set.
B. The packets are duplicated and a copy is sent to the destination.
C. It is transmitted out of the Cisco IPS outside interface.
D. It is routed back to the Cisco ASA interfaces for transmission.

Answer: A

NEW QUESTION 131
- (Exam Topic 5)
An administrator is attempting to remotely log into a switch in the data centre using SSH and is unable to connect. How does the administrator confirm that traffic is reaching the firewall?

A. by running Wireshark on the administrator's PC
B. by performing a packet capture on the firewall.
C. by running a packet tracer on the firewall.
D. by attempting to access it from a different workstation.

Answer: B

NEW QUESTION 134
- (Exam Topic 5)
A network administrator needs to create a policy on Cisco Firepower to fast-path traffic to avoid Layer 7 inspection. The rate at which traffic is inspected must be optimized. What must be done to achieve this goal?

A. Enable lhe FXOS for multi-instance.
B. Configure a prefilter policy.
C. Configure modular policy framework.
D. Disable TCP inspection.

Answer: B

NEW QUESTION 137
- (Exam Topic 5)
An engineer is troubleshooting a file that is being blocked by a Cisco FTD device on the network. The user is reporting that the file is not malicious.
Which action does the engineer take to identify the file and validate whether or not it is malicious?

A. identify the file in the intrusion events and submit it to Threat Grid for analysis.
B. Use FMC file analysis to look for the file and select Analyze to determine its disposition.
C. Use the context explorer to find the file and download it to the local machine for investigation.
D. Right click the connection event and send the file to AMP for Endpoints to see if the hash is malicious.

Answer: A

NEW QUESTION 142
- (Exam Topic 5)
With Cisco FTD software, which interface mode must be configured to passively receive traffic that passes through the appliance?

A. ERSPAN
B. IPS-only
C. firewall
D. tap

Answer: A

NEW QUESTION 143
- (Exam Topic 5)
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. Which technique will retain the policy consistency at each location but allow only the locally significant network subnet within the applicable rules?

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

Answer: D

NEW QUESTION 148
- (Exam Topic 5)
With a recent summer time change, system logs are showing activity that occurred to be an hour behind real time Which action should be taken to resolve this issue?

A. Manually adjust the time to the correct hour on all managed devices
B. Configure the system clock settings to use NTP with Daylight Savings checked
C. Manually adjust the time to the correct hour on the Cisco FMC.
D. Configure the system clock settings to use NTP

Answer: B

NEW QUESTION 151
- (Exam Topic 5)
An administrator is adding a QoS policy to a Cisco FTD deployment. When a new rule is added to the policy and QoS is applied on 'Interfaces in Destination Interface Objects", no interface objects are available What is the problem?

A. The FTD is out of available resources lor us
B. so QoS cannot be added
C. The network segments that the interfaces are on do not have contiguous IP space
D. QoS is available only on routed interfaces, and this device is in transparent mode.
E. A conflict exists between the destination interface types that is preventing QoS from being added

Answer: C

NEW QUESTION 153

- (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 155
- (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 159
- (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 163
- (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 164
- (Exam Topic 5)
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. multiple deployment
B. single-context
C. single deployment
D. multi-instance

Answer: D

NEW QUESTION 166
- (Exam Topic 5)
Which protocol is needed to exchange threat details in rapid threat containment on Cisco FMC?

A. SGT
B. SNMP v3
C. BFD
D. pxGrid

Answer: D

NEW QUESTION 170
- (Exam Topic 5)
An engainer must add DNS-specific rules to me Cisco FTD intrusion policy. The engineer wants to use the rules currently in the Cisco FTD Snort database that are not already enabled but does not want to enable more than are needed. Which action meets these requirements?

A. Change the dynamic state of the rule within the policy.
B. Change the base policy to Security over Connectivity.
C. Change the rule state within the policy being used.
D. Change the rules using the Generate and Use Recommendations feature.

Answer: C

NEW QUESTION 173
- (Exam Topic 5)
An engineer is troubleshooting HTTP traffic to a web server using the packet capture tool on Cisco FMC. When reviewing the captures, the engineer notices that there are a lot of packets that are not sourced from or destined to the web server being captured. How can the engineer reduce the strain of capturing packets for irrelevant traffic on the Cisco FTD device?

A. Use the host filter in the packet capture to capture traffic to or from a specific host.
B. Redirect the packet capture output to a .pcap file that can be opened with Wireshark.
C. Use the -c option to restrict the packet capture to only the first 100 packets.
D. Use an access-list within the packet capture to permit only HTTP traffic to and from the web server.

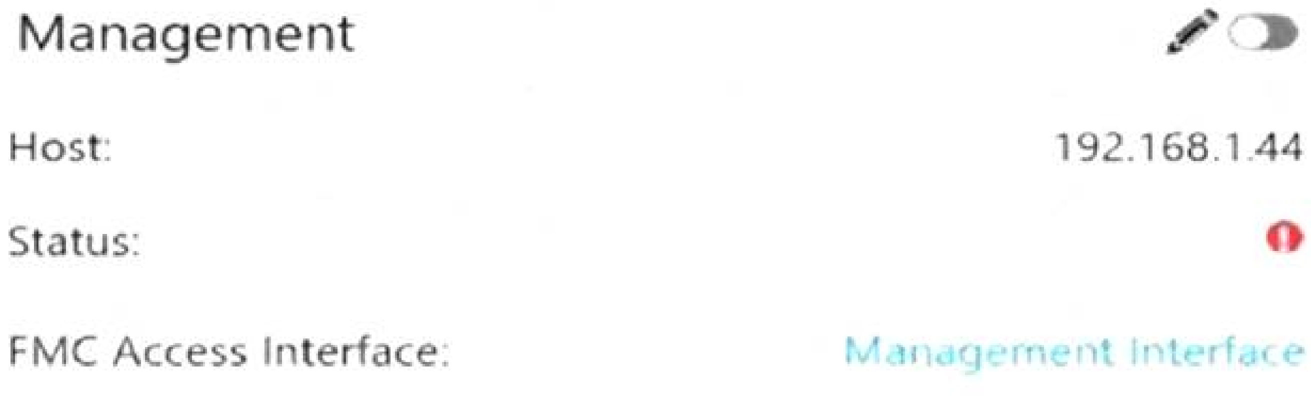
Answer: A

NEW QUESTION 177
- (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 180
- (Exam Topic 5)
Refer to the exhibit.



Management

Host:	192.168.1.44
Status:	●
FMC Access Interface:	Management Interface

What is the effect of the existing Cisco FMC configuration?

A. The remote management port for communication between the Cisco FMC and the managed device changes to port 8443.
B. The managed device is deleted from the Cisco FMC.
C. The SSL-encrypted communication channel between the Cisco FMC and the managed device becomes plain-text communication channel.
D. The management connection between the Cisco FMC and the Cisco FTD is disabled.

Answer: D

NEW QUESTION 181
- (Exam Topic 5)
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 Connection Events dashboard to check the block reason and adjust the inspection policy as needed.
B. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion 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 blockedtraffic.

Answer: A

NEW QUESTION 182
- (Exam Topic 5)
A company wants a solution to aggregate the capacity of two Cisco FTD devices to make the best use of resources such as bandwidth and connections per second. Which order of steps must be taken across the Cisco FTDs with Cisco FMC to meet this requirement?

A. Configure the Cisco FTD interfaces, add members to FMC, configure cluster members in FMC, and create cluster in Cisco FMC.
B. Add members to Cisco FMC, configure Cisco FTD interfaces in Cisco FM
C. configure cluster members in Cisco FMC, create cluster in Cisco FM
D. and configure cluster members in Cisco FMC.
E. Configure the Cisco FTD interfaces and cluster members, add members to Cisco FM
F. and create the cluster in Cisco FMC.
G. Add members to the Cisco FMC, configure Cisco FTD interfaces, create the cluster in Cisco FMC, and configure cluster members in Cisco FMC.

Answer: D

NEW QUESTION 187
- (Exam Topic 5)
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. transparent
B. routed
C. passive
D. inline set

Answer: D

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

NEW QUESTION 188
- (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 192
- (Exam Topic 5)
A security engineer must deploy a Cisco FTD appliance as a bump in the wire to detect intrusion events without disrupting the flow of network traffic. Which two features must be configured to accomplish the task? (Choose two.)

A. inline set pair
B. transparent mode
C. tapemode
D. passive interfaces
E. bridged mode

Answer: BC

NEW QUESTION 197
- (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 201
- (Exam Topic 5)
Which process should be checked when troubleshooting registration issues between Cisco FMC and managed devices to verify that secure communication is occurring?

A. fpcollect
B. dhclient
C. sfmgr
D. sftunnel

Answer: D

NEW QUESTION 205
- (Exam Topic 5)
An engineer must configure the firewall to monitor traffic within a single subnet without increasing the hop count of that traffic. How would the engineer achieve this?

A. Configure Cisco Firepower as a transparent firewall
B. Set up Cisco Firepower as managed by Cisco FDM
C. Configure Cisco Firepower in FXOS monitor only mode.
D. Set up Cisco Firepower in intrusion prevention mode

Answer: A

NEW QUESTION 207
- (Exam Topic 5)
There is an increased amount of traffic on the network and for compliance reasons, management needs visibility into the encrypted traffic What is a result of enabling TLS'SSL decryption to allow this visibility?

A. It prompts the need for a corporate managed certificate
B. It has minimal performance impact
C. It is not subject to any Privacy regulations
D. It will fail if certificate pinning is not enforced

Answer: A

NEW QUESTION 211
- (Exam Topic 5)
A mid-sized company is experiencing higher network bandwidth utilization due to a recent acquisition The network operations team is asked to scale up their one Cisco FTD appliance deployment to higher capacities due to the increased network bandwidth. Which design option should be used to accomplish this goal?

A. Deploy multiple Cisco FTD appliances in firewall clustering mode to increase performance.
B. Deploy multiple Cisco FTD appliances using VPN load-balancing to scale performance.
C. Deploy multiple Cisco FTD HA pairs to increase performance
D. Deploy multiple Cisco FTD HA pairs in clustering mode to increase performance

Answer: A

NEW QUESTION 212
- (Exam Topic 5)
An engineer must investigate a connectivity issue and decides to use the packet capture feature on Cisco FTD. The goal is to see the real packet going through the Cisco FTD device and see the Snort detection actions as a part of the output. After the capture-traffic command is issued, only the packets are displayed. Which action resolves this issue?

A. Use the verbose option as a part of the capture-traffic command
B. Use the capture command and specify the trace option to get the required information.
C. Specify the trace using the -T option after the capture-traffic command.
D. Perform the trace within the Cisco FMC GUI instead of the Cisco FTD CLI.

Answer: B

NEW QUESTION 216
- (Exam Topic 5)
Which license type is required on Cisco ISE to integrate with Cisco FMC pxGrid?

A. mobility
B. plus
C. base
D. apex

Answer: B

NEW QUESTION 220
- (Exam Topic 5)
A network administrator notices that SI events are not being updated The Cisco FTD device is unable to load all of the SI event entries and traffic is not being blocked as expected. What must be done to correct this issue?

A. Restart the affected devices in order to reset the configurations
B. Manually update the SI event entries to that the appropriate traffic is blocked
C. Replace the affected devices with devices that provide more memory
D. Redeploy configurations to affected devices so that additional memory is allocated to the SI module

Answer: D

NEW QUESTION 223

- (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 224
- (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 227
- (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 229
- (Exam Topic 4)
What is a valid Cisco AMP file disposition?

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

Answer: B

Explanation:
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

NEW QUESTION 233
- (Exam Topic 5)
An analyst is reviewing the Cisco FMC reports for the week. They notice that some peer-to-peer applications are being used on the network and they must identify which poses the greatest risk to the environment. Which report gives the analyst this information?

A. Attacks Risk Report
B. User Risk Report
C. Network Risk Report
D. Advanced Malware Risk Report

Answer: C

NEW QUESTION 236
- (Exam Topic 5)
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. generate events
B. drop packet
C. drop connection
D. drop and generate

Answer: B

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

NEW QUESTION 238
- (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 240
- (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 245
- (Exam Topic 3)
How many report templates does the Cisco Firepower Management Center support?

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

Answer: D

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

NEW QUESTION 246
- (Exam Topic 3)
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.

Answer: B

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

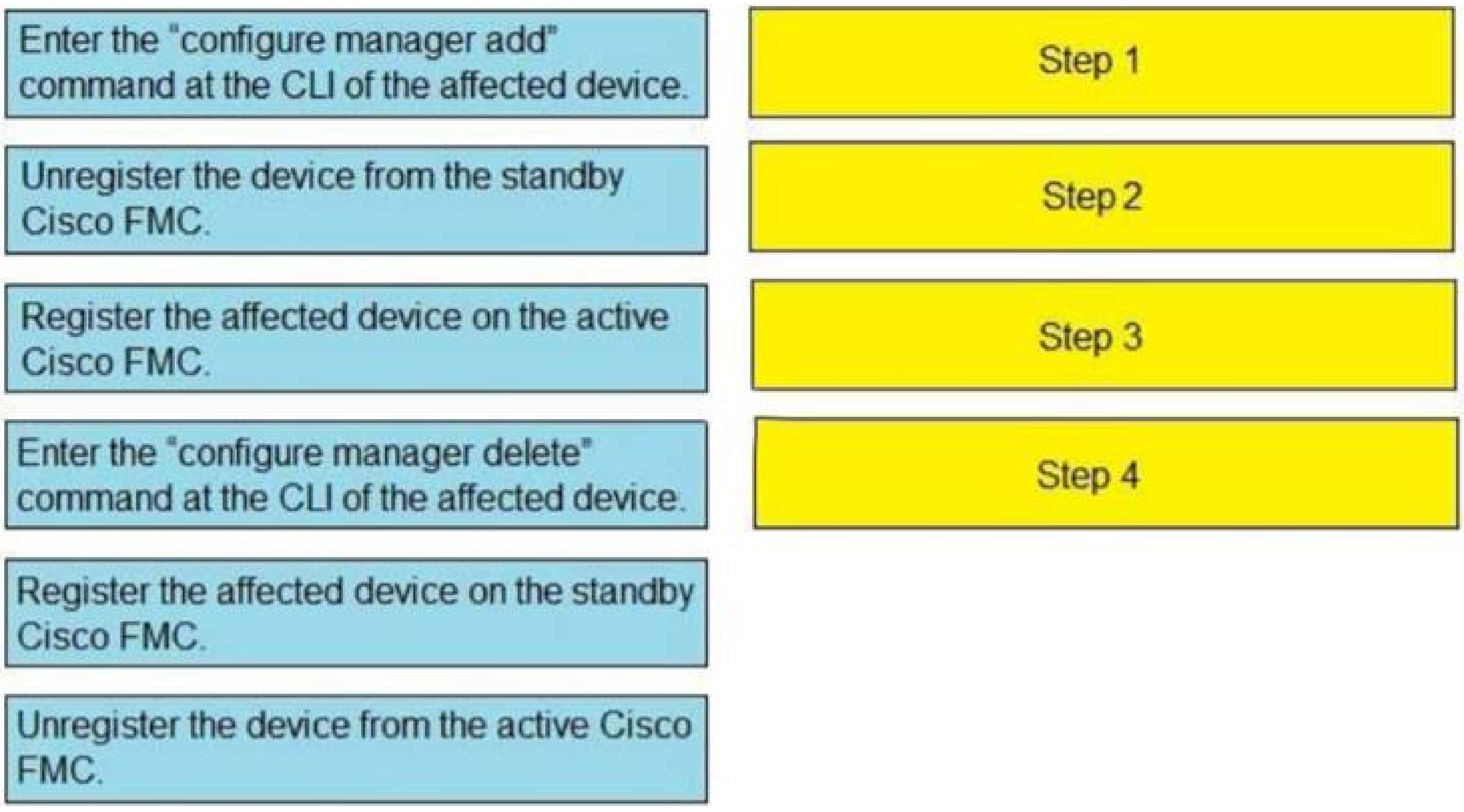
NEW QUESTION 248
- (Exam Topic 3)
Which command must be run to generate troubleshooting files on an FTD?

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

Answer: C

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

NEW QUESTION 251
- (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.

Step 1

Step 2

Step 3

Step 4

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 256
- (Exam Topic 4)
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

Answer: B

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

NEW QUESTION 260
- (Exam Topic 3)
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.

Answer: C

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

NEW QUESTION 265
- (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 266

- (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 267
- (Exam Topic 3)
Which report template field format is available in Cisco FMC?

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

Answer: C

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

NEW QUESTION 270
- (Exam Topic 2)
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

Answer: AB

Explanation:
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

NEW QUESTION 271
- (Exam Topic 3)
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.

Answer: C

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

NEW QUESTION 273
- (Exam Topic 2)
Which two routing options are valid with Cisco Firepower Threat Defense? (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

Answer: AC

Explanation:
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

NEW QUESTION 278
- (Exam Topic 2)
In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.)

A. Traffic inspection can be interrupted temporarily when configuration changes are deployed.
B. The system performs intrusion inspection followed by file inspection.

C. They can 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.

Answer: AC

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

NEW QUESTION 280
- (Exam Topic 2)
An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events filing the database and overloading the Cisco FMC. A monitored NAT device is executing multiple updates of its operating system in a short period of time. What configuration change must be made to alleviate this issue?

A. Leave default networks.
B. Change the method to TCP/SYN.
C. Increase the number of entries on the NAT device.
D. Exclude load balancers and NAT devices.

Answer: D

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

NEW QUESTION 282
- (Exam Topic 2)
An administrator is creating interface objects to better segment their network but is having trouble adding interfaces to the objects. What is the reason for this failure?

A. The interfaces are being used for NAT for multiple networks.
B. The administrator is adding interfaces of multiple types.
C. The administrator is adding an interface that is in multiple zones.
D. The interfaces belong to multiple interface groups.

Answer: D

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusa "All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains."

NEW QUESTION 287
- (Exam Topic 2)
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.

Answer: C

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

NEW QUESTION 288
- (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 293
- (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 298
- (Exam Topic 2)
What is the result of 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.

Answer: B

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

NEW QUESTION 299
- (Exam Topic 2)
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

Answer: BE

Explanation:
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

NEW QUESTION 300
- (Exam Topic 2)
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 address and networks, port/protocols 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

Answer: BC

Explanation:
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

NEW QUESTION 305
- (Exam Topic 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 can support Cisco FTD clustering.

Answer: C

Explanation:
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

NEW QUESTION 309
- (Exam Topic 1)
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

Answer: D

Explanation:
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

NEW QUESTION 314
- (Exam Topic 2)
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

Answer: D

Explanation:
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

NEW QUESTION 316
- (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 321
- (Exam Topic 1)
A Cisco FTD has two physical interfaces assigned to a BVI. Each interface is connected to a different VLAN on the same switch. Which firewall mode is the Cisco FTD set up to support?

A. active/active failover
B. transparent
C. routed
D. high availability clustering

Answer: B

NEW QUESTION 322
- (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 325
- (Exam Topic 1)
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. Shut down the Cisco FMC before powering up the replacement unit.
B. Ensure that the faulty Cisco FTD device remains registered to the Cisco FMC.
C. Unregister the faulty Cisco FTD device from the Cisco FMC
D. Shut down the active Cisco FTD device before powering up the replacement unit.

Answer: C

NEW QUESTION 330
- (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 335
- (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 338
- (Exam Topic 1)
An engineer is tasked with deploying an internal perimeter firewall that will support multiple DMZs Each DMZ has a unique private IP subnet range. How is this requirement satisfied?

A. Deploy the firewall in transparent mode with access control policies.
B. Deploy the firewall in routed mode with access control policies.
C. Deploy the firewall in routed mode with NAT configured.
D. Deploy the firewall in transparent mode with NAT configured.

Answer: C

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general-config/intro-fw.

NEW QUESTION 341
- (Exam Topic 1)
An engineer is building a new access control policy using Cisco FMC. The policy must inspect a unique IPS policy as well as log rule matching. Which action must be taken to meet these requirements?

A. Configure an IPS policy and enable per-rule logging.
B. Disable the default IPS policy and enable global logging.
C. Configure an IPS policy and enable global logging.
D. Disable the default IPS policy and enable per-rule logging.

Answer: C

NEW QUESTION 342
- (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 347
- (Exam Topic 1)
When deploying a Cisco ASA Firepower module, an organization wants to evaluate the contents of the traffic without affecting the network. It is currently configured to have more than one instance of the same device on the physical appliance Which deployment mode meets the needs of the organization?

A. inline tap monitor-only mode
B. passive monitor-only mode
C. passive tap monitor-only mode
D. inline mode

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config/access Inline tap monitor-only mode (ASA inline)—In an inline tap monitor-only deployment, a copy of the traffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode lets you see what the ASA FirePOWER module would have done to traffic, and lets you evaluate the content of the traffic, without impacting the network. However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.

NEW QUESTION 350
- (Exam Topic 1)
An organization is migrating their Cisco ASA devices running in multicontext mode to Cisco FTD devices. Which action must be taken to ensure that each context on the Cisco ASA is logically separated in the Cisco FTD devices?

A. Add a native instance to distribute traffic to each Cisco FTD context.
B. Add the Cisco FTD device to the Cisco ASA port channels.
C. Configure a container instance in the Cisco FTD for each context in the Cisco ASA.
D. Configure the Cisco FTD to use port channels spanning multiple networks.

Answer: C

NEW QUESTION 354
- (Exam Topic 1)
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

Answer: C

Explanation:
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

NEW QUESTION 355
- (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 357
- (Exam Topic 1)
Which two conditions must be met to enable high availability between two Cisco FTD devices? (Choose two.)

A. same flash memory size
B. same NTP configuration
C. same DHCP/PPoE configuration
D. same host name
E. same number of interfaces

Answer: BE

Explanation:
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high- Conditions
In order to create an HA between 2 FTD devices, these conditions must be met: Same model
Same version (this applies to FXOS and to FTD - (major (first number), minor (second number), and maintenance (third number) must be equal))
Same number of interfaces
Same type of interfaces
Both devices as part of same group/domain in FMC
Have identical Network Time Protocol (NTP) configuration Be fully deployed on the FMC without uncommitted changes Be in the same firewall mode: routed or transparent.
Note that this must be checked on both FTD devices and FMC GUI since there have been cases where the FTDs had the same mode, but FMC does not reflect this.
Does not have DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configured in any of the interface Different hostname (Fully Qualified Domain Name (FQDN)) for both chassis. In order to check the chassis
hostname navigate to FTD CLI and run this command

NEW QUESTION 359
- (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 363
- (Exam Topic 1)
Which two dynamic routing protocols are supported in Firepower Threat Defense without using FlexConfig? (Choose two.)

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

Answer: BE

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

NEW QUESTION 366
- (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 370
......