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)
Which Cisco FMC report gives the analyst information about the ports and protocols that are related to the configured sensitive network for analysis?

A. Malware Report
B. Host Report
C. Firepower Report
D. Network Report

Answer: D

NEW QUESTION 3
- (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 4
- (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 5
- (Exam Topic 5)
A network administrator is trying to convert from LDAP to LDAPS for VPN user authentication on a Cisco FTD. Which action must be taken on the Cisco FTD objects to accomplish this task?

A. Add a Key Chain object to acquire the LDAPS certificate.
B. Create a Certificate Enrollment object to get the LDAPS certificate needed.
C. Identify the LDAPS cipher suite and use a Cipher Suite List object to define the Cisco FTD connection requirements.
D. Modify the Policy List object to define the session requirements for LDAPS.

Answer: B

NEW QUESTION 6
- (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 7
- (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 8
- (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

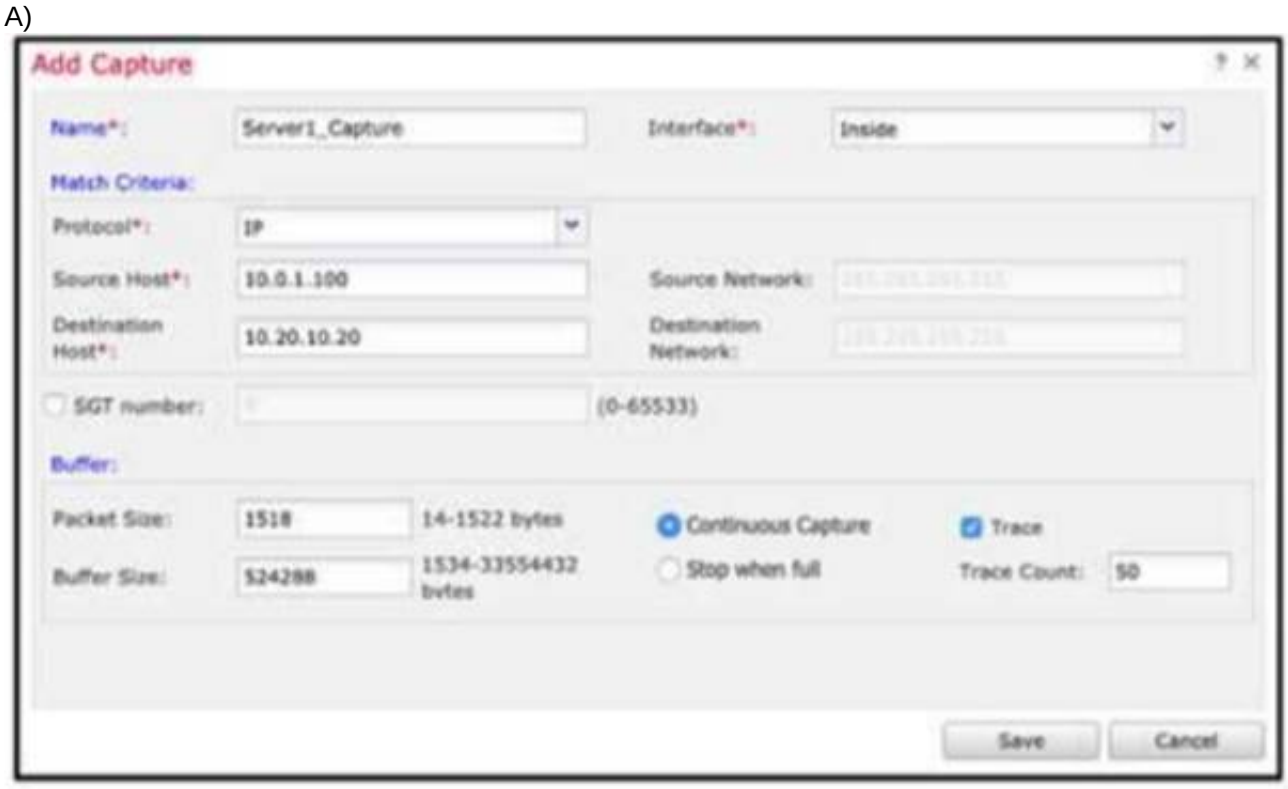
Answer: A

NEW QUESTION 9
- (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?

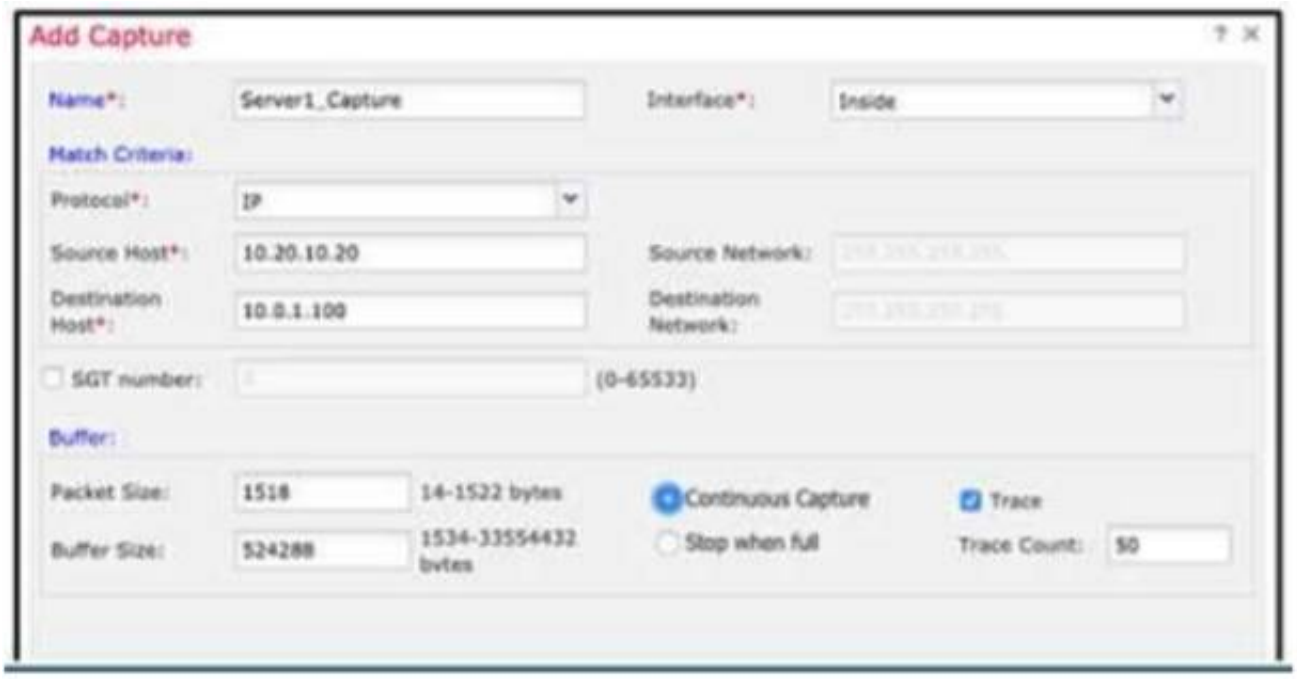
A. Run the default Firepower report.
B. Export the Attacks Risk report.
C. Generate a malware report.
D. Create a Custom report.

Answer: D

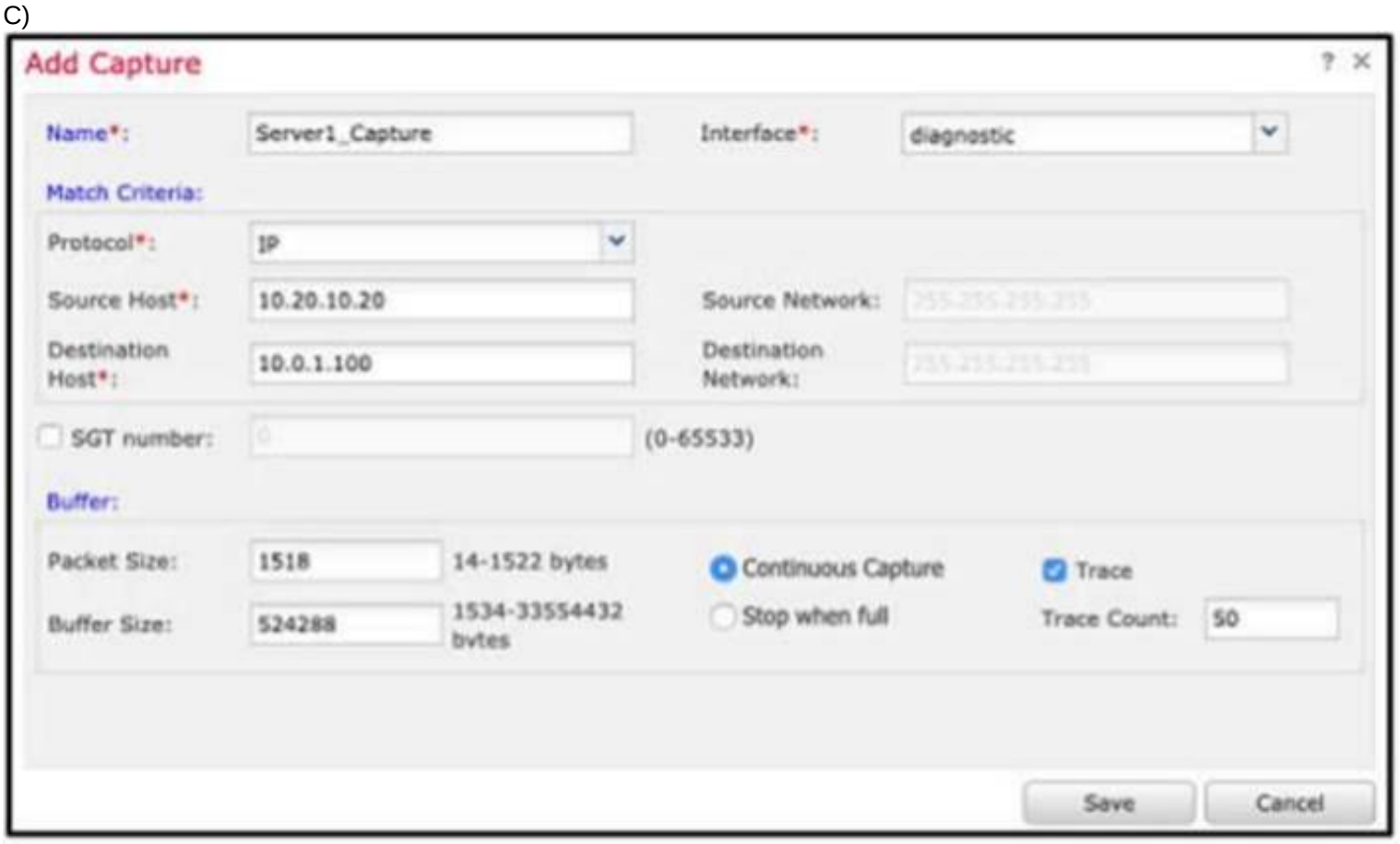
NEW QUESTION 10
- (Exam Topic 5)
An engineer is troubleshooting a device that cannot connect to a web server. The connection is initiated from the Cisco FTD inside interface and attempting to reach 10.0.1.100 over the non-standard port of 9443 The host the engineer is attempting the connection from is 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)



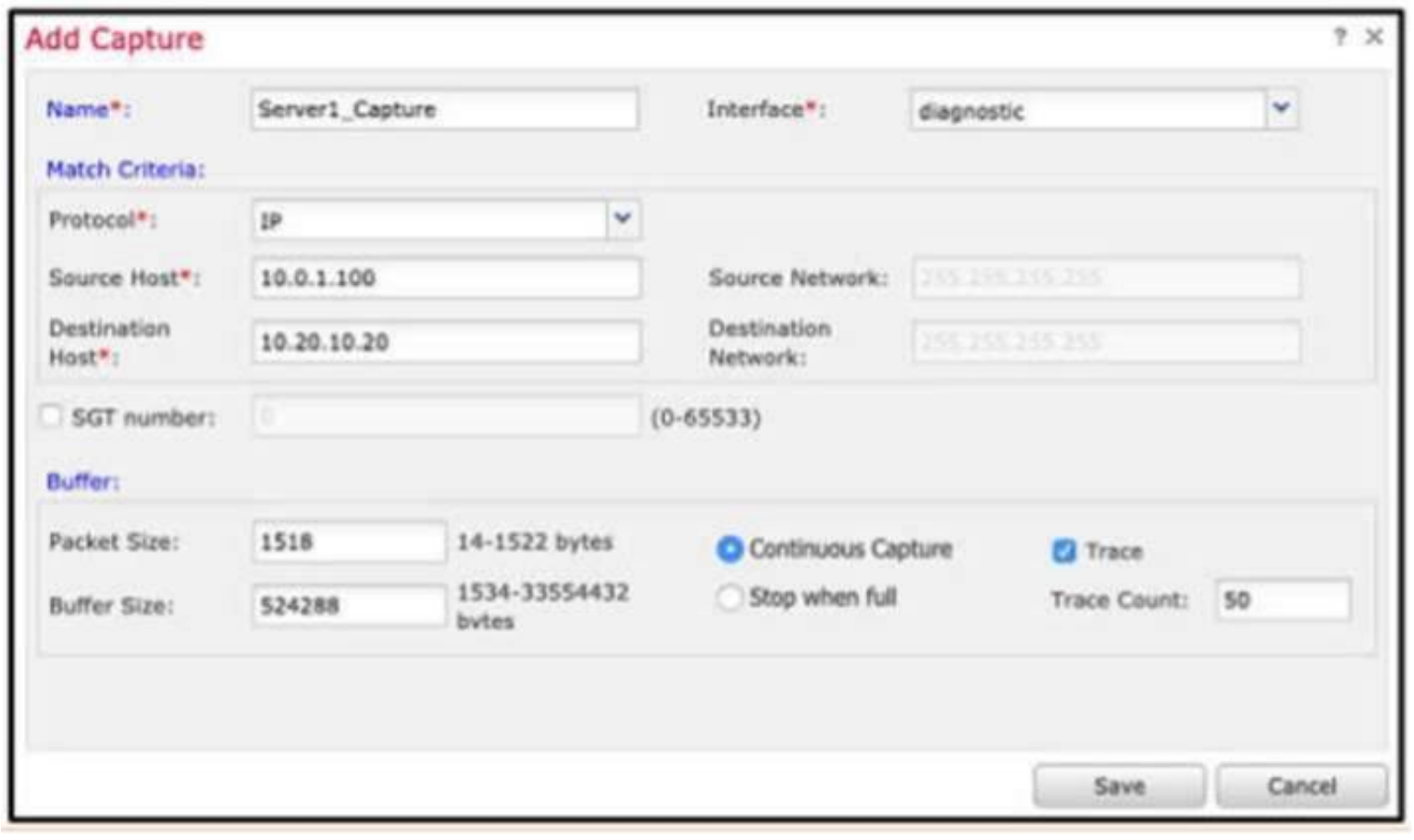
B)



C)



D)



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

Answer: B

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 12
- (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 14
- (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 18
- (Exam Topic 5)
A security engineer found a suspicious file from an employee email address and is trying to upload it for analysis, however the upload is failing. The last registration status is still active. What is the cause for this issue?

A. Cisco AMP for Networks is unable to contact Cisco Threat Grid on premise.
B. Cisco AMP for Networks is unable to contact Cisco Threat Grid Cloud.
C. There is a host limit set.
D. The user agent status is set to monitor.

Answer: B

NEW QUESTION 19
- (Exam Topic 5)
The administrator notices that there is malware present with an .exe extension and needs to verify if any of the systems on the network are running the executable file. What must be configured within Cisco AMP for Endpoints to show this data?

A. prevalence
B. threat root cause
C. vulnerable software
D. file analysis

Answer: A

NEW QUESTION 24
- (Exam Topic 5)
A company is in the process of deploying intrusion protection with Cisco FTDs managed by a Cisco FMC. Which action must be selected to enable fewer rules detect only critical conditions and avoid false positives?

A. Connectivity Over Security
B. Balanced Security and Connectivity
C. Maximum Detection
D. No Rules Active

Answer: A

NEW QUESTION 28
- (Exam Topic 5)
An engineer is restoring a Cisco FTD configuration from a remote backup using the command restore remote-manager-backup location 1.1.1.1 admin /volume/home/admin BACKUP_Cisc394602314.zip on a
Cisco FMG. After connecting to the repository, an error occurred that prevents the FTD device from accepting the backup file. What is the problem?

A. The backup file is not in .cfg format.
B. The backup file is too large for the Cisco FTD device
C. The backup file extension was changed from tar to zip
D. The backup file was not enabled prior to being applied

Answer: C

NEW QUESTION 33
- (Exam Topic 5)
A network administrator wants to block traffic to a known malware site at https://www.badsite.com and all subdomains while ensuring no packets from any internal client are sent to that site. Which type of policy must the network administrator use to accomplish this goal?

A. Prefilter policy
B. SSL policy
C. DNS policy
D. Access Control policy with URL filtering

Answer: D

NEW QUESTION 34
- (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 37
- (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 38
- (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 39
- (Exam Topic 5)
A security engineer is adding three Cisco FTD devices to a Cisco FMC. Two of the devices have successfully registered to the Cisco FMC. The device that is unable to register is located behind a router that translates all outbound traffic to the router's WAN IP address. Which two steps are required for this device to register to the Cisco FMC? (Choose two.)

A. Reconfigure the Cisco FMC lo use the device's private IP address instead of the WAN address.
B. Configure a NAT ID on both the Cisco FMC and the device.
C. Add the port number being used for PAT on the router to the device's IP address in the Cisco FMC.
D. Reconfigure the Cisco FMC to use the device's hostname instead of IP address.
E. Remove the IP address defined for the device in the Cisco FMC.

Answer: BE

NEW QUESTION 43
- (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 44
- (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 46
- (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 50
- (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 58
- (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 63
- (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 64
- (Exam Topic 5)
An engineer defines a new rule while configuring an Access Control Policy. After deploying the policy, the rule is not working as expected and the hit counters associated with the rule are showing zero. What is causing this error?

A. Logging is not enabled for the rule.
B. The rule was not enabled after being created.
C. The wrong source interface for Snort was selected in the rule.
D. An incorrect application signature was used in the rule.

Answer: B

NEW QUESTION 69
- (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 72
- (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 75
- (Exam Topic 5)
An engineer is configuring two new Cisco FTD devices to replace the existing high availability firewall pair in a highly secure environment. The information exchanged between the FTD devices over the failover link must be encrypted. Which protocol supports this on the Cisco FTD?

A. IPsec
B. SSH
C. SSL
D. MACsec

Answer: A

NEW QUESTION 76
- (Exam Topic 5)
An administrator is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of NAT001 and a password of Cisco0420l06525. The private IP address of the FMC server is 192.168.45.45. which is being translated to the public IP address of 209.165.200.225/27. Which command set must be used in order to accomplish this task?

A. configure manager add 209.165.200.225 <reg_key> <nat_id>
B. configure manager add 192.168.45,45 <reg_key> <nat_id>
C. configure manager add 209.165.200.225 255.255.255.224 <reg_key> <nat_id>
D. configure manager add 209.165.200.225/27 <reg_key> <nat_id>

Answer: A

NEW QUESTION 78
- (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 81
- (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 84
- (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 87
- (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 88
- (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 93
- (Exam Topic 5)
A company is deploying intrusion protection on multiple Cisco FTD appliances managed by Cisco FMC. Which system-provided policy must be selected if speed and detection are priorities?

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

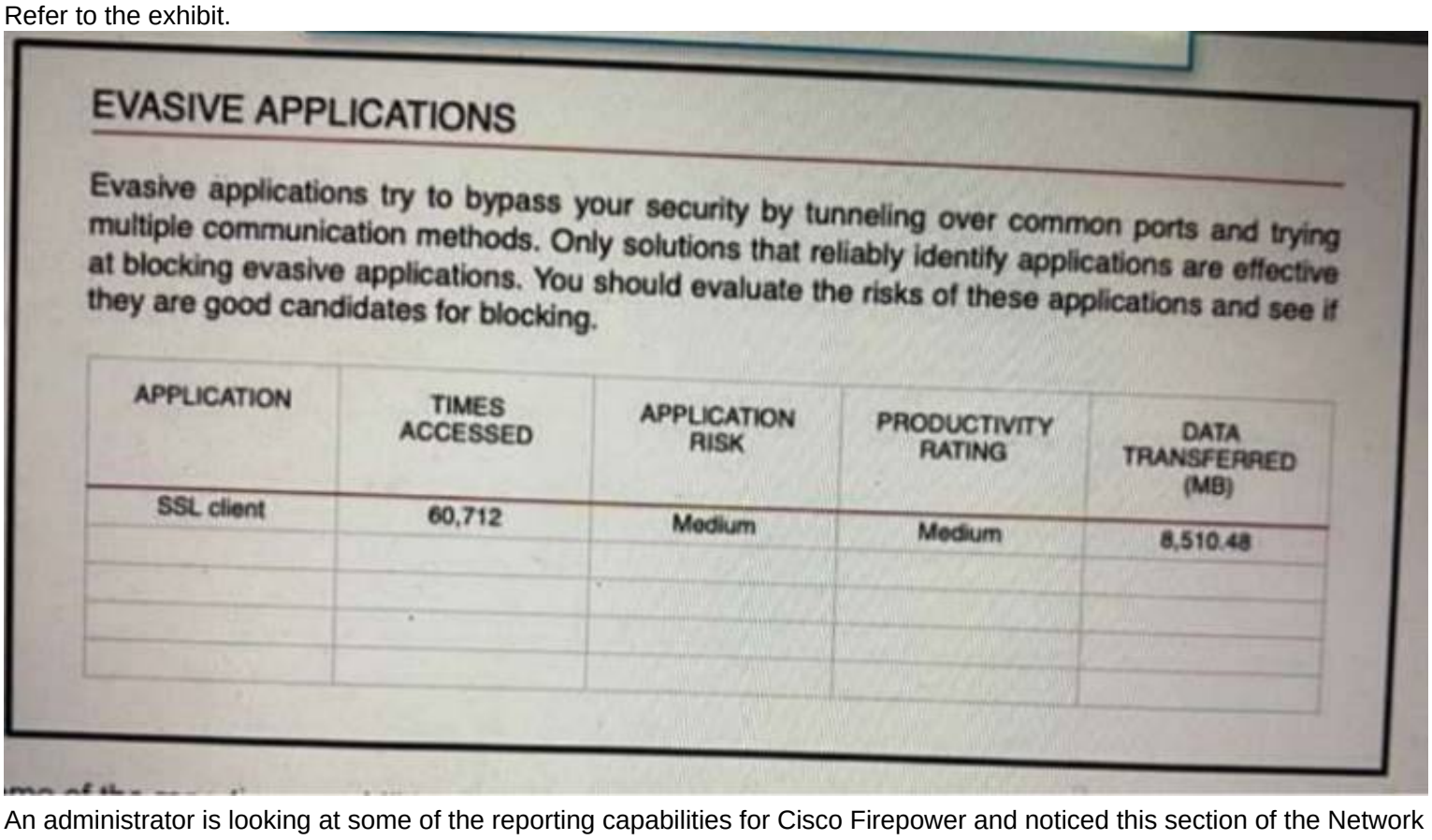
Answer: D

NEW QUESTION 97
- (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 101
- (Exam Topic 5)
Refer to the exhibit.



An administrator is looking at some of the reporting capabilities for Cisco Firepower and noticed this section of the Network Risk report showing a lot of SSL activity that cloud be used for evasion. Which action will mitigate this risk?

A. Use SSL decryption to analyze the packets.
B. Use encrypted traffic analytics to detect attacks
C. Use Cisco AMP for Endpoints to block all SSL connection
D. Use Cisco Tetration to track SSL connections to servers.

Answer: A

NEW QUESTION 103
- (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 108
- (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 110
- (Exam Topic 5)
An engineer is working on a LAN switch and has noticed that its network connection to the mime Cisco IPS has gone down Upon troubleshooting it is determined that the switch is working as expected What must have been implemented for this failure to occur?

A. The upstream router has a misconfigured routing protocol
B. Link-state propagation is enabled
C. The Cisco IPS has been configured to be in fail-open mode
D. The Cisco IPS is configured in detection mode

Answer: D

NEW QUESTION 113
- (Exam Topic 5)
An engineer currently has a Cisco FTD device registered to the Cisco FMC and is assigned the address of 10.10.50.12. The organization is upgrading the addressing schemes and there is a requirement to convert the addresses to a format that provides an adequate amount of addresses on the network What should the engineer do to ensure that the new addressing takes effect and can be used for the Cisco FTD to Cisco FMC connection?

A. Delete and reregister the device to Cisco FMC
B. Update the IP addresses from IFV4 to IPv6 without deleting the device from Cisco FMC
C. Format and reregister the device to Cisco FMC.
D. Cisco FMC does not support devices that use IPv4 IP addresses.

Answer: A

NEW QUESTION 115
- (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. Firepower devices do not need to be connected to the internet.
B. All types of Firepower devices are supported.
C. Supports all devices that are running supported versions of Firepower
D. An on-premises proxy server does not need to set up and maintained

Answer: D

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

NEW QUESTION 120
- (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 125
- (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 129
- (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 130
- (Exam Topic 5)
A network engineer is extending a user segment through an FTD device for traffic inspection without creating another IP subnet How is this accomplished on an FTD device in routed mode?

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

Answer: C

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

NEW QUESTION 132
- (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 133
- (Exam Topic 5)
A Cisco FMC administrator wants to configure fastpathing of trusted network traffic to increase performance. In which type of policy would the administrator configure this feature?

A. Identity policy
B. Prefilter policy
C. Network Analysis policy
D. Intrusion policy

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 140
- (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 145
- (Exam Topic 5)
Refer to the exhibit.

```
Phase: 16
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Firewall: starting rule matching, zone 4 -> 1, geo 0 -> 0, vlan 0, sgt 0, src sgt type 0, dest_sgt_tag 0, dest sgt type 0, username 'No Authentication Required', , icmpType 8, icmpCode 0
Firewall: block rule,  'Ping' , drop
Snort: processed decoder alerts or actions queue, drop
Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST, Blocked by Firewall
Snort Verdict: (black-list) black list this flow

Result:
input-interface: ACCESS41_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame 0x000055d2b0f8b7e0 flow (NA)/NA
```

A systems administrator conducts a connectivity test to their SCCM server from a host machine and gets no response from the server. Which action ensures that the ping packets reach the destination and that the host receives replies?

A. Create an access control policy rule that allows ICMP traffic.
B. Configure a custom Snort signature to allow ICMP traffic after Inspection.
C. Modify the Snort rules to allow ICMP traffic.
D. Create an ICMP allow list and add the ICMP destination to remove it from the implicit deny list.

Answer: A

NEW QUESTION 148
- (Exam Topic 5)
A network engineer is receiving reports of users randomly getting disconnected from their corporate applications which traverses the data center FTD appliance Network monitoring tools show that the FTD appliance utilization is peaking above 90% of total capacity. What must be done in order to further analyze this issue?

A. Use the Packet Export feature to save data onto external drives
B. Use the Packet Capture feature to collect real-time network traffic
C. Use the Packet Tracer feature for traffic policy analysis
D. Use the Packet Analysis feature for capturing network data

Answer: B

NEW QUESTION 152
- (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 154
- (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 157
- (Exam Topic 5)
After using Firepower for some time and learning about how it interacts with the network, an administrator is trying to correlate malicious activity with a user Which widget should be configured to provide this visibility on the Cisco Firepower dashboards?

A. Custom Analysis
B. Current Status
C. Current Sessions
D. Correlation Events

Answer: A

NEW QUESTION 161
- (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 164
- (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 167
- (Exam Topic 5)
A network administrator is concerned about (he high number of malware files affecting users' machines. What must be done within the access control policy in Cisco FMC to address this concern?

A. Create an intrusion policy and set the access control policy to block.
B. Create an intrusion policy and set the access control policy to allow.
C. Create a file policy and set the access control policy to allow.
D. Create a file policy and set the access control policy to block.

Answer: D

NEW QUESTION 168
- (Exam Topic 5)
Drag and drop the configuration steps from the left into the sequence on the right to enable external authentication on Cisco FMC to a RADIUS server.

Select Authentication Method and RADIUS.	step 1
Configure the primary and secondary servers and user roles.	step 2
Select Users and External Authentication.	step 3
Add External Authentication Object.	step 4

A. Mastered
B. Not Mastered

Answer: A

Explanation:
4, 1, 2, 3

NEW QUESTION 171
- (Exam Topic 5)
An engineer is reviewing a ticket that requests to allow traffic for some devices that must connect to a server over 8699/udp. The request mentions only one IP address, 172.16.18.15, but the requestor asked for the engineer to open the port for all machines that have been trying to connect to it over the last week. Which action must the engineer take to troubleshoot this issue?

A. Use the context explorer to see the application blocks by protocol.
B. Use the context explorer to see the destination port blocks
C. Filter the connection events by the source port 8699/udp.
D. Filter the connection events by the destination port 8699/udp.

Answer: D

NEW QUESTION 176

- (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 177
- (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 178
- (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 181
- (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 182
- (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. Configure high-availability in both the primary and secondary Cisco FMCs
B. Connect the primary and secondary Cisco FMC devices with Category 6 cables of not more than 10 meters in length.
C. Place the active Cisco FMC device on the same trusted management network as the standby device
D. Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device fails

Answer: D

NEW QUESTION 185
- (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 189
- (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)
Which two routing options are valid with Cisco FTD? (Choose Two)

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

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 198
- (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 199
- (Exam Topic 5)
An analyst is investigating a potentially compromised endpoint within the network and pulls a host report for the endpoint in question to collect metrics and documentation. What information should be taken from this report for the investigation?

A. client applications by user, web applications, and user connections
B. number of attacked machines, sources of the attack, and traffic patterns
C. intrusion events, host connections, and user sessions
D. threat detections over time and application protocols transferring malware

Answer: C

NEW QUESTION 202
- (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 204
- (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 206
- (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 208
- (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 210
- (Exam Topic 5)
A network administrator is configuring a site-to-site IPsec VPN to a router sitting behind a Cisco FTD. The administrator has configured an access policy to allow traffic to this device on UDP 500, 4500, and ESP VPN traffic is not working. Which action resolves this issue?

A. Set the allow action in the access policy to trust.
B. Enable IPsec inspection on the access policy.
C. Modify the NAT policy to use the interface PAT.
D. Change the access policy to allow all ports.

Answer: B

NEW QUESTION 212
- (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 216
- (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 218
- (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 219
- (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 221
- (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 223
- (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 226
- (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 229
- (Exam Topic 5)
An engineer has been tasked with using Cisco FMC to determine if files being sent through the network are malware. Which two configuration takes must be performed to achieve this file lookup? (Choose two.)

A. The Cisco FMC needs to include a SSL decryption policy.
B. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.
C. The Cisco FMC needs to connect to the Cisco ThreatGrid service directly for sandboxing.
D. The Cisco FMC needs to connect with the FireAMP Cloud.
E. The Cisco FMC needs to include a file inspection policy for malware lookup.

Answer: DE

NEW QUESTION 231
- (Exam Topic 3)
When do you need the file-size command option during troubleshooting with packet capture?

A. when capture packets are less than 16 MB
B. when capture packets are restricted from the secondary memory

C. when capture packets exceed 10 GB
D. when capture packets exceed 32 MB

Answer: D

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

NEW QUESTION 232
- (Exam Topic 3)
A network engineer is configuring URL Filtering on Firepower Threat Defense. Which two port requirements on the Firepower Management Center must be validated to allow communication with the cloud service? (Choose two.)

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

Answer: AE

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

NEW QUESTION 233
- (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 236
- (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 237
- (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 240
- (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 245
- (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 250
- (Exam Topic 3)
Which command is entered in the Cisco FMC CLI to generate a troubleshooting file?

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

Answer: D

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

NEW QUESTION 252
- (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 254
- (Exam Topic 2)
An organization is using a Cisco FTD and Cisco ISE to perform identity-based access controls. A network administrator is analyzing the Cisco FTD events and notices that unknown user traffic is being allowed through the firewall. How should this be addressed to block the traffic while allowing legitimate user traffic?

A. Modify the Cisco ISE authorization policy to deny this access to the user.
B. Modify Cisco ISE to send only legitimate usernames to the Cisco FTD.
C. Add the unknown user in the Access Control Policy in Cisco FTD.
D. Add the unknown user in the Malware & File Policy in Cisco FTD.

Answer: C

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

NEW QUESTION 255
- (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 256
- (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 258
- (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 259
- (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 261
- (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 266
- (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 268
- (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 270
- (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 272
- (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 275
- (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 280
- (Exam Topic 1)
What is the difference between inline and inline tap on Cisco Firepower?

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

Answer: A

NEW QUESTION 284
- (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 286
- (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 287
- (Exam Topic 1)
What are two application layer preprocessors? (Choose two.)

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

Answer: BC

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

NEW QUESTION 289
- (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 294
- (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 299
- (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 302
- (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 303
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

300-710 Practice Exam Features:

* 300-710 Questions and Answers Updated Frequently

* 300-710 Practice Questions Verified by Expert Senior Certified Staff

* 300-710 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 300-710 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year