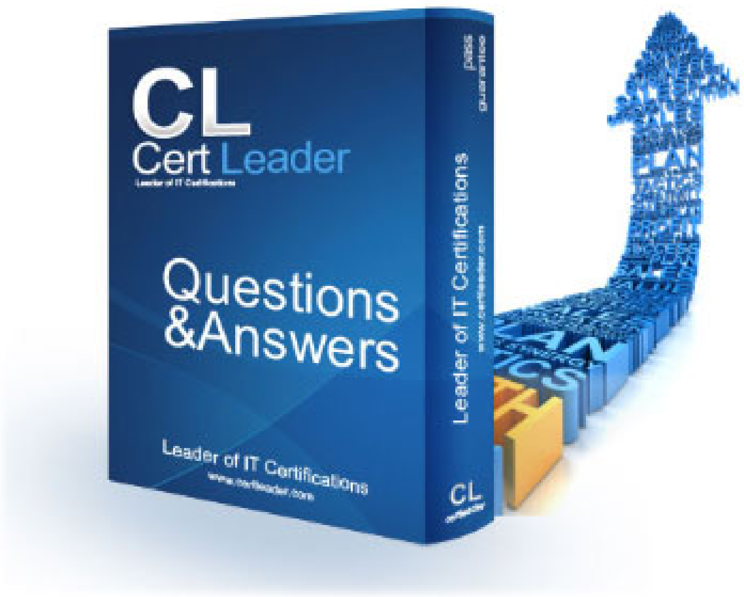
300-710 Dumps

Securing Networks with Cisco Firepower (SNCF)

https://www.certleader.com/300-710-dumps.html



NEW QUESTION 1
- (Exam Topic 5)
An organization wants to secure traffic from their branch office to the headquarter building using Cisco Firepower devices, They want to ensure that their Cisco Firepower devices are not wasting resources on inspecting the VPN traffic. What must be done to meet these requirements?

A. Configure the Cisco Firepower devices to ignore the VPN traffic using prefilter policies
B. Enable a flexconfig policy to re-classify VPN traffic so that it no longer appears as interesting traffic
C. Configure the Cisco Firepower devices to bypass the access control policies for VPN traffic.
D. Tune the intrusion policies in order to allow the VPN traffic through without inspection

Answer: C

Explanation:
When you configure the Cisco Firepower devices to bypass the access control policies for VPN traffic, the devices will not inspect the VPN traffic and thus will not waste resources on it. This is the best option to ensure that the VPN traffic is not wasting resources on the Cisco Firepower devices.
Reference:
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the

NEW QUESTION 2
- (Exam Topic 5)
An engineer is creating an URL object on Cisco FMC How must it be configured so that the object will match for HTTPS traffic in an access control policy?

A. Specify the protocol to match (HTTP or HTTPS).
B. Use the FQDN including the subdomain for the website
C. Define the path to the individual webpage that uses HTTPS.
D. Use the subject common name from the website certificate

Answer: B

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 Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

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

Answer: A

NEW QUESTION 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

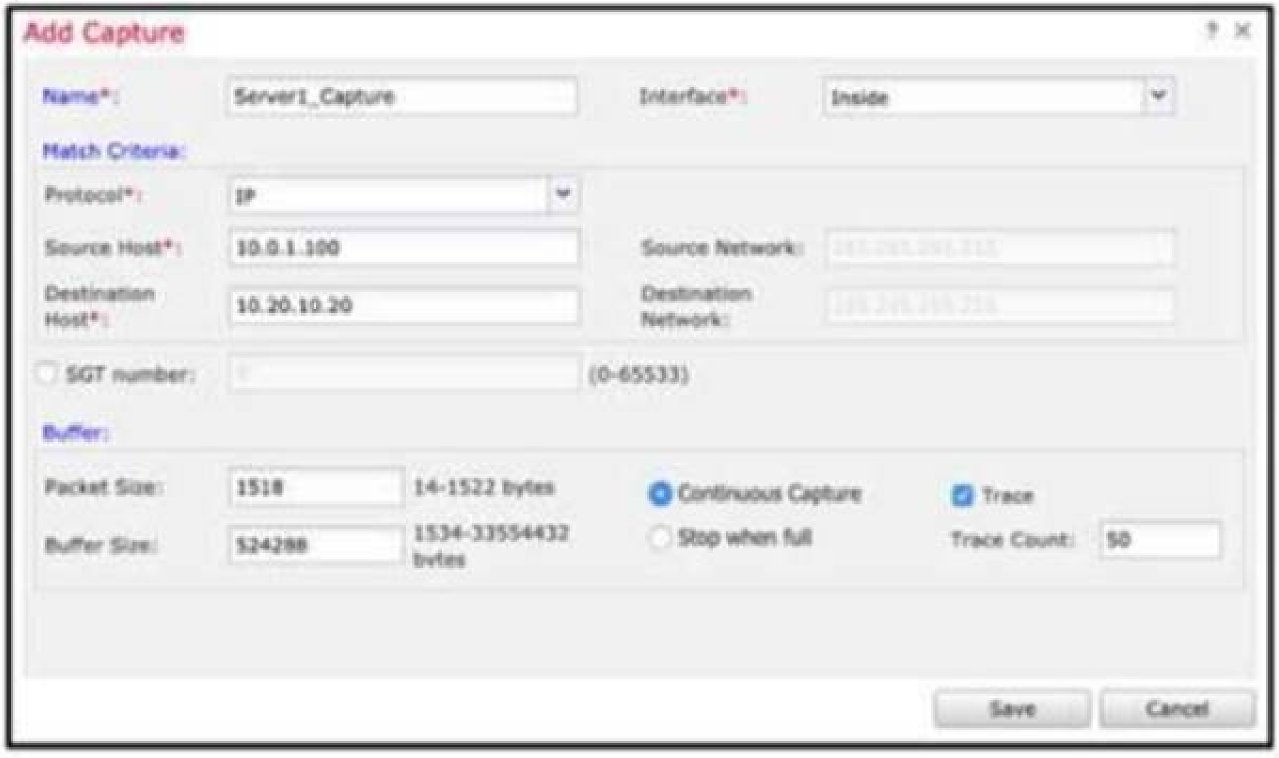
Answer: B

NEW QUESTION 7
- (Exam Topic 5)
A 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

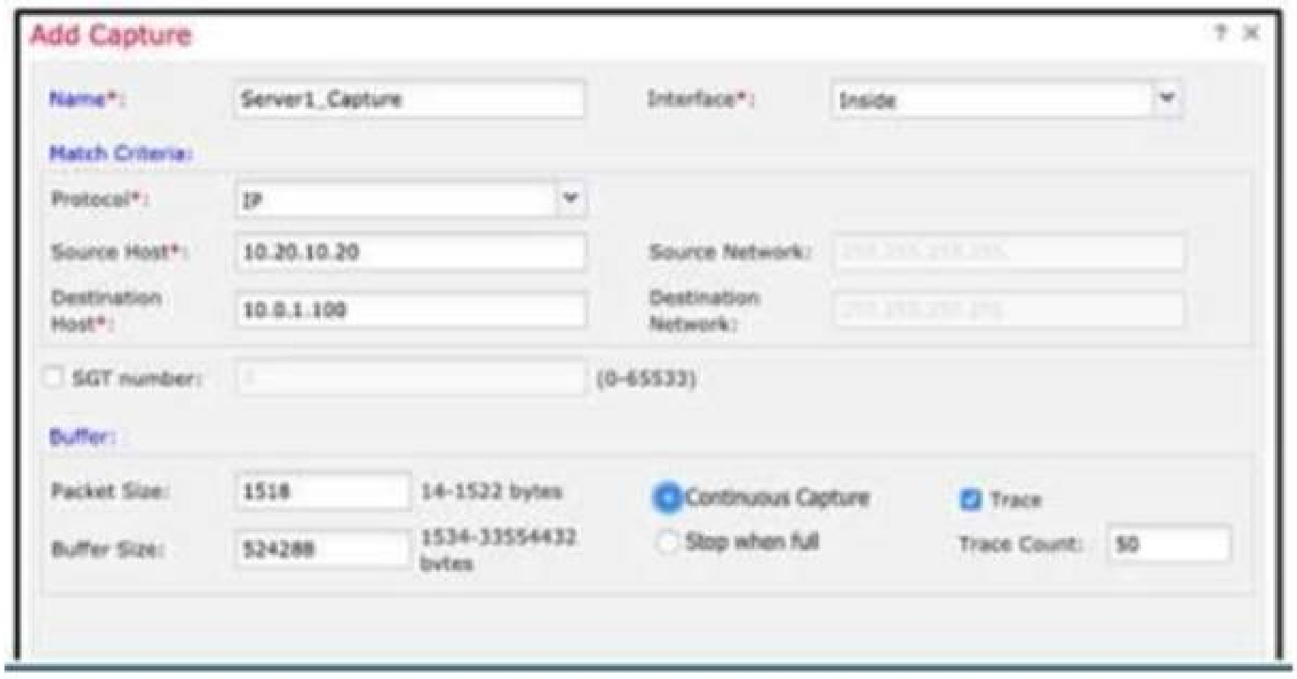
NEW QUESTION 8
- (Exam Topic 5)
An engineer is troubleshooting a device that cannot connect to a web server. The connection is initiated from the Cisco FTD inside interface and attempting to reach 10.0.1.100 over the non-standard port of 9443 The host the engineer is attempting the connection from is at the IP address of 10.20.10.20. In order to determine what is happening to the packets on the network, the engineer decides to use the FTD packet capture tool Which capture configuration should be used to gather the information needed to troubleshoot this issue?
A)



Add Capture

Name*: Server1_Capture
Interface*: Inside
Match Criteria:
Protocol*: IP
Source Host*: 10.0.1.100
Source Network:
Destination Host*: 10.20.10.20
Destination Network:
□ SGT number: (0-65533)
Buffer:
Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 bytes
● Continuous Capture
○ Stop when full
☑ Trace
Trace Count: 50

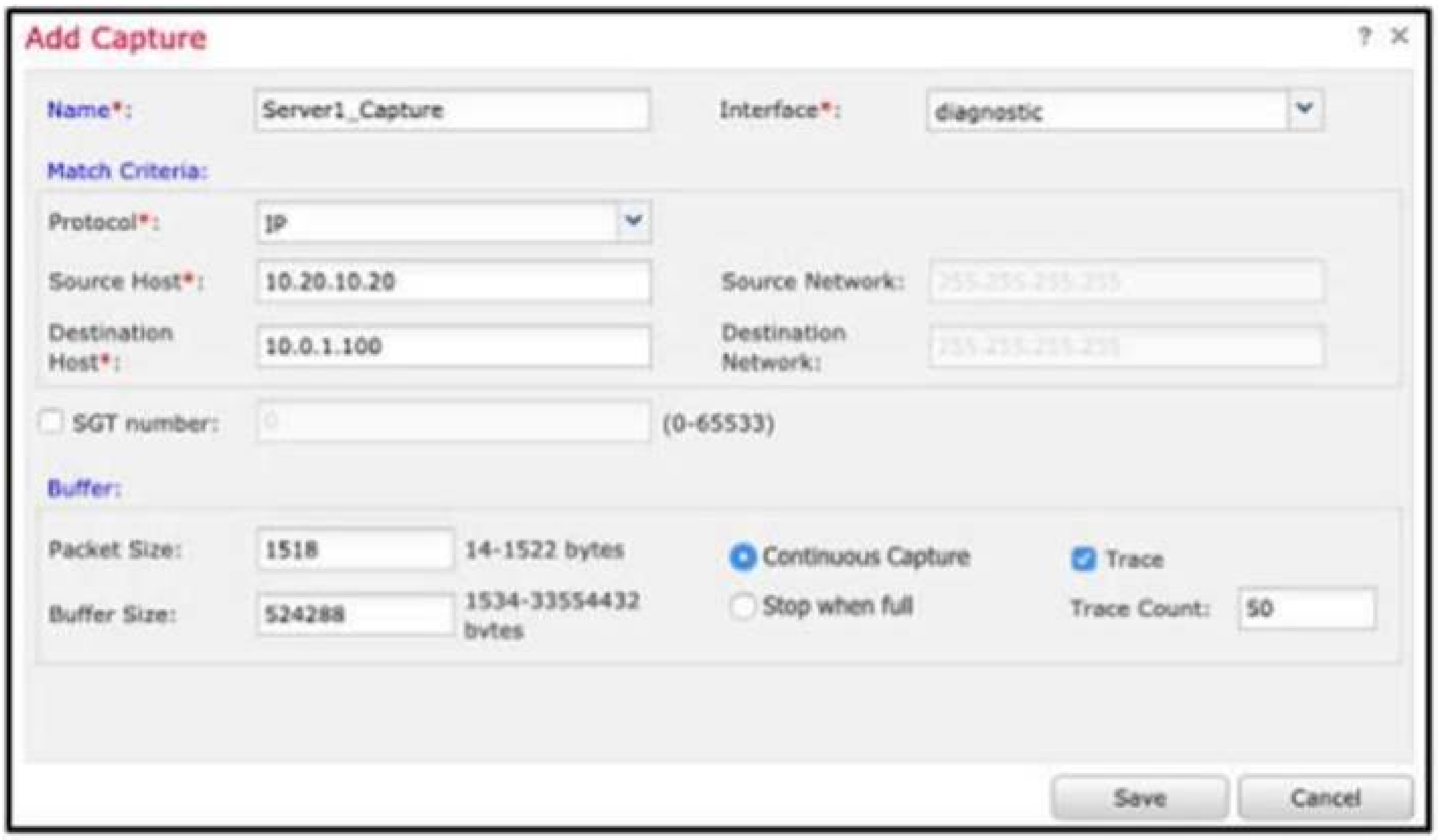
B)



Add Capture

Name*: Server1_Capture
Interface*: Inside
Match Criteria:
Protocol*: IP
Source Host*: 10.20.10.20
Source Network:
Destination Host*: 10.0.1.100
Destination Network:
□ SGT number: (0-65533)
Buffer:
Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 bytes
● Continuous Capture
○ Stop when full
☑ Trace
Trace Count: 50

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)

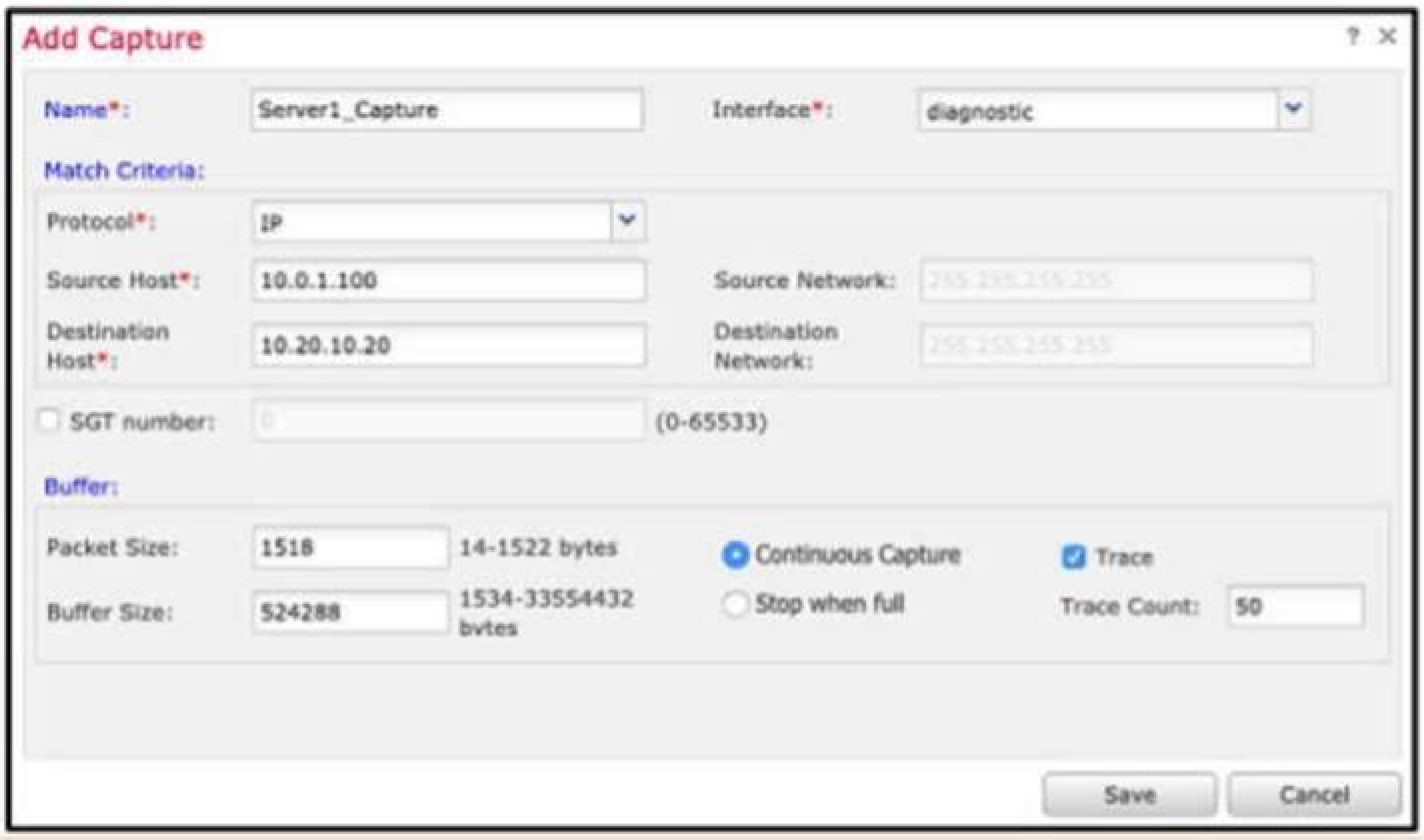
Buffer:

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 9
- (Exam Topic 5)
What is an advantage of adding multiple inline interface pairs to the same inline interface set when deploying an asynchronous routing configuration?

A. Allows the IPS to identify inbound and outbound traffic as part of the same traffic flow.
B. The interfaces disable autonegotiation and interface speed is hard coded set to 1000 Mbps.
C. Allows traffic inspection to continue without interruption during the Snort process restart.
D. The interfaces are automatically configured as a media-independent interface crossover.

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpm

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

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

Answer: A

NEW QUESTION 10
- (Exam Topic 5)
An engineer is 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 11
- (Exam Topic 5)
What is a feature of Cisco AMP private cloud?

A. It supports anonymized retrieval of threat intelligence
B. It supports security intelligence filtering.
C. It disables direct connections to the public cloud.
D. It performs dynamic analysis

Answer: C

NEW QUESTION 12
- (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 13
- (Exam Topic 5)
What is a characteristic of bridge groups on a Cisco FTD?

A. In routed firewall mode, routing between bridge groups must pass through a routed interface.
B. In routed firewall mode, routing between bridge groups is supported.
C. In transparent firewall mode, routing between bridge groups is supported
D. Routing between bridge groups is achieved only with a router-on-a-stick configuration on a connected router

Answer: B

NEW QUESTION 16
- (Exam Topic 5)
An engineer is configuring Cisco FMC and wants to limit the time allowed for processing packets through the interface However if the time is exceeded the configuration must allow packets to bypass detection What must be configured on the Cisco FMC to accomplish this task?

A. Fast-Path Rules Bypass
B. Cisco ISE Security Group Tag
C. Inspect Local Traffic Bypass
D. Automatic Application Bypass

Answer: D

NEW QUESTION 21
- (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 25
- (Exam Topic 5)
Which action must be taken on the Cisco FMC when a packet bypass is configured in case the Snort engine is down or a packet takes too long to process?

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

Answer: B

NEW QUESTION 27
- (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 31
- (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 32
- (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

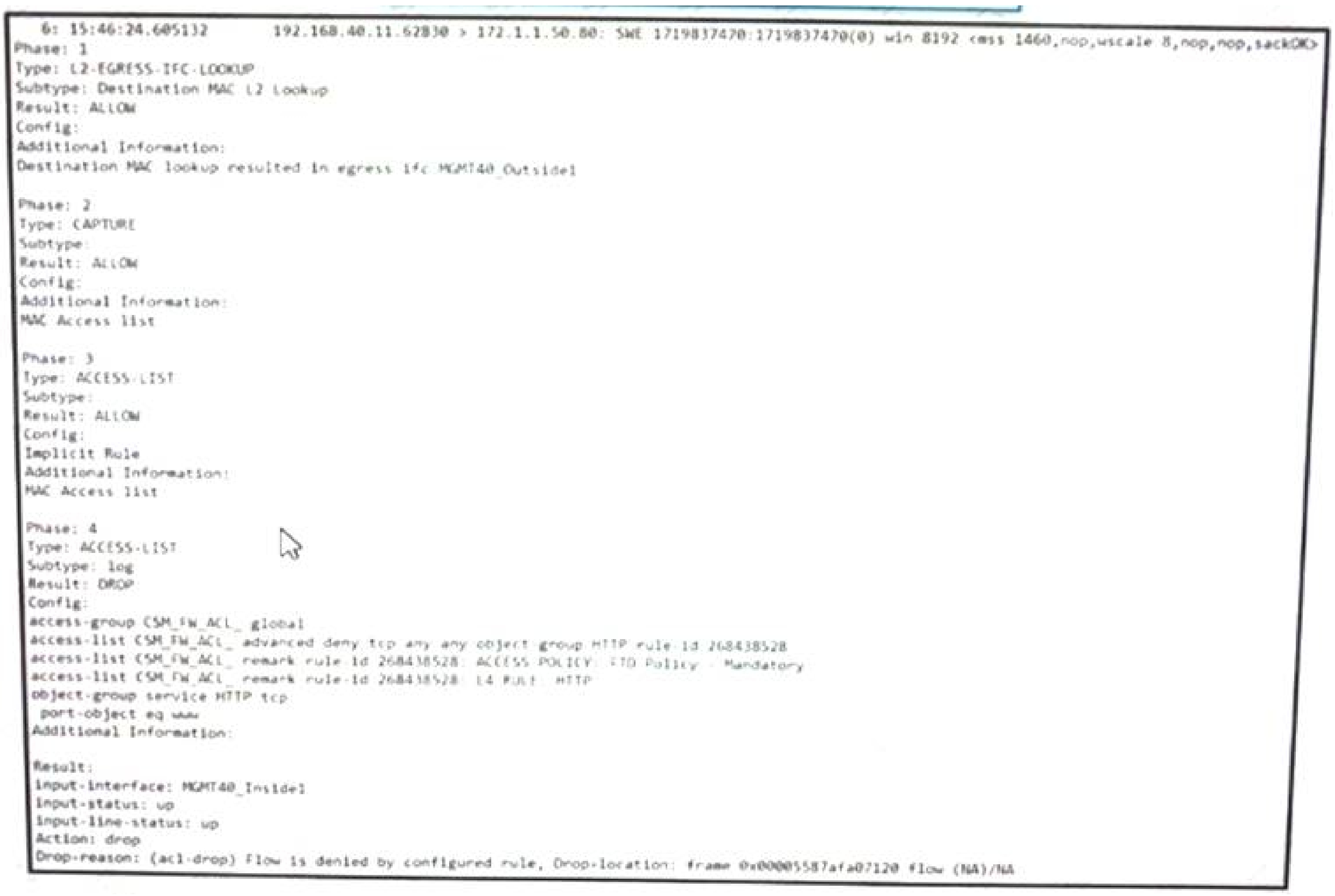
NEW QUESTION 36
- (Exam Topic 5)
An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down. What must be configured to accomplish this task?

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 38
- (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 43
- (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 44
- (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 49
- (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 53
- (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 57
- (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 Cisco0420I06525. 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 59
- (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 64
- (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 66
- (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 71
- (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 72
- (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 76
- (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 81
- (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 86
- (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 91
- (Exam Topic 5)
An engineer must deploy a Cisco FTD appliance via Cisco FMC to span a network segment to detect malware and threats. When setting the Cisco FTD interface mode, which sequence of actions meets this requirement?

A. Set to passive, and configure an access control policy with an intrusion policy and a file policy defined
B. Set to passive, and configure an access control policy with a prefilter policy defined
C. Set to none, and configure an access control policy with a prefilter policy defined
D. Set to none, and configure an access control policy with an intrusion policy and a file policy defined

Answer: A

NEW QUESTION 92
- (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 97
- (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 100
- (Exam Topic 5)
An engineer is setting up a remote access VPN on a Cisco FTD device and wants to define which traffic gets sent over the VPN tunnel. Which named object type in Cisco FMC must be used to accomplish this task?

A. split tunnel
B. crypto map
C. access list
D. route map

Answer: A

NEW QUESTION 103
- (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 104
- (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 tasks 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: BE

NEW QUESTION 109
- (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 114
- (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

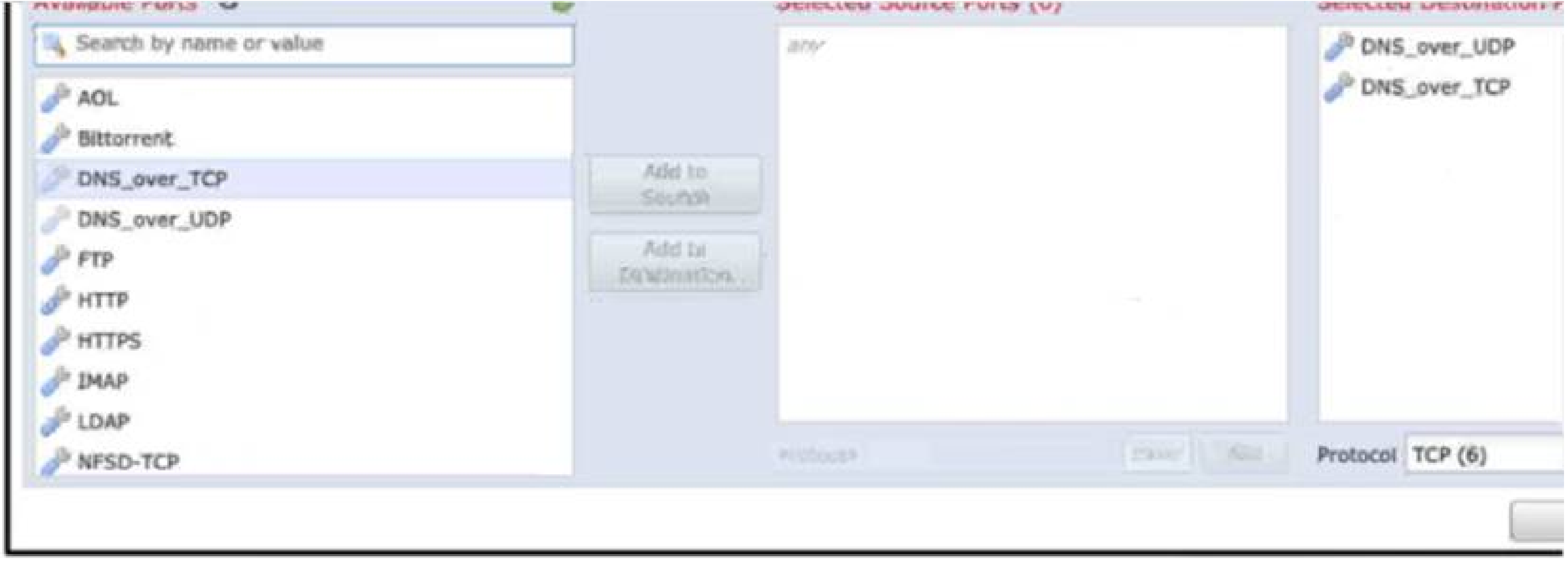
NEW QUESTION 117
- (Exam Topic 5)
A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?

A. Use regular expressions to block the malicious file.

B. Add the hash from the infected endpoint to the network block list.
C. Add the hash to the simple custom detection list.
D. Enable a personal firewall in the infected endpoint.

Answer: C

NEW QUESTION 120
- (Exam Topic 5)



Refer to the exhibit An engineer is modifying an access control pokey to add a rule to inspect all DNS traffic that passes through the firewall After making the change and deploying the pokey they see that DNS traffic is not bang inspected by the Snort engine What is the problem?

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

Answer: C

NEW QUESTION 122
- (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 127
- (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 128
- (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 132
- (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 135
- (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 140
- (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 142
- (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 146
- (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 151
- (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 155
- (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 159
- (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 164
- (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 168
- (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 169
- (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 172
- (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 175
- (Exam Topic 3)
What is the benefit of selecting the trace option for packet capture?

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

Answer: A

NEW QUESTION 177
- (Exam Topic 3)
Within Cisco Firepower Management Center, where does a user add or modify widgets?

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

Answer: A

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

NEW QUESTION 180
- (Exam Topic 4)
In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

A. unavailable
B. unknown
C. clean
D. disconnected

Answer: A

NEW QUESTION 183
- (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 186
- (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 190
- (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 193
- (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 196
- (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 200
- (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 205
- (Exam Topic 3)
Which Cisco Firepower feature is used to reduce the number of events received in a period of time?

A. rate-limiting
B. suspending
C. correlation
D. thresholding

Answer: D

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

NEW QUESTION 210
- (Exam Topic 2)
An engineer is using the configure manager add <FMC IP> Cisc402098527 command to add a new Cisco FTD device to the Cisco FMC; however, the device is not being added. Why Is this occurring?

A. The NAT ID is required since the Cisco FMC is behind a NAT device.
B. The IP address used should be that of the Cisco FT
C. not the Cisco FMC.
D. DONOTRESOLVE must be added to the command
E. The registration key is missing from the command

Answer: A

NEW QUESTION 213
- (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 218
- (Exam Topic 2)
An engineer is configuring Cisco FMC and wants to allow multiple physical interfaces to be part of the same VLAN. The managed devices must be able to perform Layer 2 switching between interfaces, including
sub-interfaces. What must be configured to meet these requirements?

A. interface-based VLAN switching
B. inter-chassis clustering VLAN
C. integrated routing and bridging
D. Cisco ISE Security Group Tag

Answer: C

NEW QUESTION 222
- (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 224
- (Exam Topic 2)
In which two places can thresholding settings be configured? (Choose two.)

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

Answer: AC

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

NEW QUESTION 227
- (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 228
- (Exam Topic 2)
An organization does not want to use the default Cisco Firepower block page when blocking HTTP traffic. The organization wants to include information about its policies and procedures to help educate the users whenever a block occurs. Which two steps must be taken to meet these requirements? (Choose two.)

A. Modify the system-provided block page result using Python.
B. Create HTML code with the information for the policies and procedures.
C. Edit the HTTP request handling in the access control policy to customized block.
D. Write CSS code with the information for the policies and procedures.
E. Change the HTTP response in the access control policy to custom.

Answer: BE

NEW QUESTION 233
- (Exam Topic 2)
Which object type supports object overrides?

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

Answer: C

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

NEW QUESTION 234
- (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 239
- (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 241
- (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 246
- (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 247
- (Exam Topic 1)
An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic

concurrently. How must the devices be implemented in this environment?

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

Answer: C

NEW QUESTION 249
- (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 250
- (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 253
- (Exam Topic 1)
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 transparent.
D. Change the firewall mode to routed.

Answer: C

Explanation:
"In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule..." "The bridge group does not pass CDP packets packets..." https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/general/asa-913-general-config/intro-f
Passing Traffic Not Allowed in Routed Mode
In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an access rule. The bridge group, however, can allow almost any traffic through using either an access rule (for IP traffic) or an EtherType rule (for non-IP traffic):
IP traffic—In routed firewall mode, broadcast and "multicast traffic is blocked even if you allow it in an access rule," including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you can allow this traffic with an access rule (using an extended ACL).
Non-IP traffic—AppleTalk, IPX, BPDUs, and MPLS, for example, can be configured to go through using an EtherType rule.
Note
"The bridge group does not pass CDP packets packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. An exception is made for BPDUs and IS-IS, which are supported. "

NEW QUESTION 256
- (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 260
- (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 265
- (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 268
......