

Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

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



NEW QUESTION 1

- (Exam Topic 5)

An engineer 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 2

- (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 3

- (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 4

- (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 5

- (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 6

- (Exam Topic 5)

A network administrator is configuring Snort inspection policies and is seeing failed deployment messages in Cisco FMC. What information should the administrator generate for Cisco TAC to help troubleshoot?

- A. A "show tech" file for the device in question.
- B. A "troubleshoot" file for the device in question.
- C. A "troubleshoot" file for the Cisco FMC.
- D. A "show tech" for the Cisco FMC.

Answer: B

NEW QUESTION 7

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 8

- (Exam Topic 5)

A VPN user is unable to connect to 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 thresholds to optimize the Snort processing.
- D. Decrypt the packet after the VPN flow so the DNS queries are not inspected

Answer: B

NEW QUESTION 9

- (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 10

- (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.

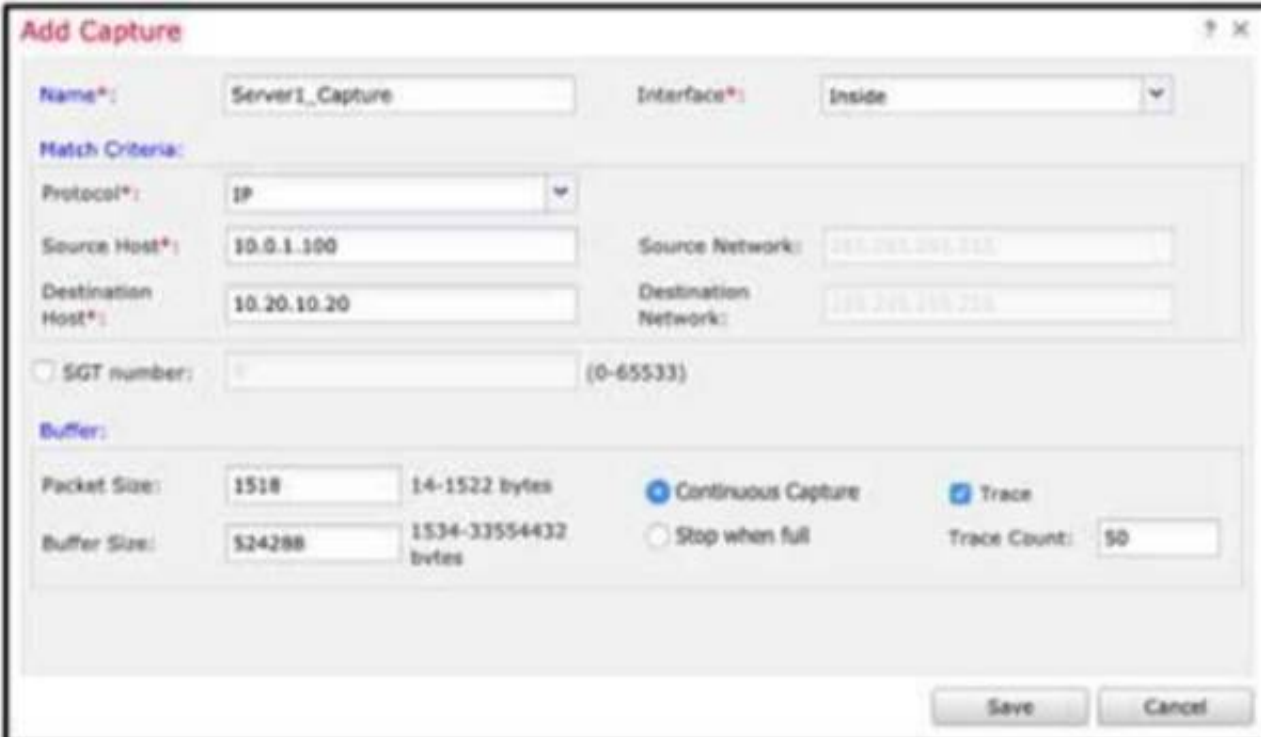
Answer: D

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)

Add Capture

Name*: Server1_Capture Interface*: Inside

Match Criteria:

Protocol*: IP

Source Host*: 10.20.10.20 Source Network: 255.255.255.255

Destination Host*: 10.0.1.100 Destination Network: 255.255.255.255

☐ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes ☒ Continuous Capture ☒ Trace

Buffer Size: 524288 1534-33554432 bytes ☐ Stop when full 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 ☒ Continuous Capture ☒ Trace

Buffer Size: 524288 1534-33554432 bytes ☐ Stop when full Trace Count: 50

Save Cancel

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 ☒ Continuous Capture ☒ Trace

Buffer Size: 524288 1534-33554432 bytes ☐ Stop when full Trace Count: 50

Save Cancel

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

Answer: B

NEW QUESTION 13

- (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 14

- (Exam Topic 5)

An organization is configuring a new Cisco Firepower High Availability deployment. Which action must be taken to ensure that failover is as seamless as possible to end users?

- A. Set up a virtual failover MAC address between chassis.
- B. Use a dedicated stateful link between chassis.
- C. Load the same software version on both chassis.
- D. Set the same FQDN for both chassis.

Answer: B

NEW QUESTION 16

- (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 19

- (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 23

- (Exam Topic 5)

A network engineer wants to add a third-party threat feed into the Cisco FMC for enhanced threat detection Which action should be taken to accomplish this goal?

- A. Enable Threat Intelligence Director using STIX and TAXII
- B. Enable Rapid Threat Containment using REST APIs
- C. Enable Threat Intelligence Director using REST APIs
- D. Enable Rapid Threat Containment using STIX and TAXII

Answer: A

NEW QUESTION 28

- (Exam Topic 5)

An organization is installing a new Cisco FTD appliance in the network. An engineer is tasked with configuring access between two network segments within the same IP subnet. Which step is needed to accomplish this task?

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

Answer: A

NEW QUESTION 32

- (Exam Topic 5)

Remote users who connect via Cisco AnyConnect to the corporate network behind a Cisco FTD device report that they get no audio when calling between remote users using their softphones. These same users can call internal users on the corporate network without any issues. What is the cause of this issue?

- A. The hairpinning feature is not available on FTD.
- B. Split tunneling is enabled for the Remote Access VPN on FTD
- C. FTD has no NAT policy that allows outside to outside communication

D. The Enable Spoke to Spoke Connectivity through Hub option is not selected on FTD.

Answer: A

NEW QUESTION 33

- (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 38

- (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 40

- (Exam Topic 5)

Refer to the exhibit.

II. ASSESSMENT RESULTS	
AUTOMATING THE TUNING EFFORT	
During the assessment period, the following changes to your network were observed.	
NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	310
A new host was added to the network	366
A device started using a new transport protocol	381
A device started using a new network protocol	373

And engineer is analyzing the Attacks Risk Report and finds that there are over 300 instances of new operating systems being seen on the network How is the Firepower configuration updated to protect these new operating systems?

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

Answer: C

Explanation:

Ref:

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

NEW QUESTION 42

- (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 47

- (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 52

- (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 53

- (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 58

- (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 61

- (Exam Topic 5)

An administrator is setting up Cisco Firepower to send data to the Cisco Stealthwatch appliances. The NetFlow_Set_Parameters object is already created, but NetFlow is not being sent to the flow collector. What must be done to prevent this from occurring?

- A. Add the NetFlow_Send_Destination object to the configuration
- B. Create a Security Intelligence object to send the data to Cisco Stealthwatch
- C. Create a service identifier to enable the NetFlow service
- D. Add the NetFlow_Add_Destination object to the configuration

Answer: B

NEW QUESTION 65

- (Exam Topic 5)

A security engineer needs to configure a network discovery policy on a Cisco FMC appliance and prevent excessive network discovery events from overloading the FMC database? Which action must be taken to accomplish this task?

- A. Change the network discovery method to TCP/SYN.
- B. Configure NetFlow exporters for monitored networks.
- C. Monitor only the default IPv4 and IPv6 network ranges.
- D. Exclude load balancers and NAT devices in the policy.

Answer: D

NEW QUESTION 68

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 70

- (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 75

- (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 76

- (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 81

- (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 85

- (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 87

- (Exam Topic 5)

The network administrator wants to enhance the network security posture by enabling machine learning for 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 89

- (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 91

- (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 94

- (Exam Topic 5)

An engineer is configuring multiple Cisco FTD appliances (or use in the network). Which rule must the engineer follow while defining interface objects in Cisco FMC for use with interfaces across multiple devices?

- A. An interface cannot belong to a security zone and an interface group
- B. Interface groups can contain multiple interface types
- C. Interface groups can contain interfaces from many devices.
- D. Two security zones can contain the same interface

Answer: C

NEW QUESTION 98

- (Exam Topic 5)

A network administrator has converted a Cisco FTD from using LDAP to LDAPS for VPN authentication. The Cisco FMC can connect to the LDAPS server, but the Cisco FTD is not connecting. Which configuration must be enabled on the Cisco FTD?

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

Answer: B

NEW QUESTION 101

- (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 104

- (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 108

- (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 109

- (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 111

- (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 112

- (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 115

- (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 118

- (Exam Topic 5)

A network administrator is configuring a Cisco AMP public cloud instance and wants to capture infections and polymorphic variants of a threat to help detect families of malware. Which detection engine meets this requirement?

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

Answer: C

NEW QUESTION 123

- (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 only secure 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 126

- (Exam Topic 5)

administrator is configuring SNORT inspection policies and is seeing failed deployment messages in Cisco FMC . What information should the administrator generate for Cisco TAC to help troubleshoot?

- A. A Troubleshoot" file for the device in question.
- B. A "show tech" file for the device in question
- C. A "show tech" for the Cisco FMC.
- D. A "troubleshoot" file for the Cisco FMC

Answer: A

NEW QUESTION 131

- (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 132

- (Exam Topic 5)

An organization has a Cisco IPS running in inline mode and is inspecting traffic for malicious activity. When traffic is received by the Cisco IPS, if it is not dropped, how does the traffic get to its destination?

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

Answer: A

NEW QUESTION 133

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 137

- (Exam Topic 5)

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 141

- (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 146

- (Exam Topic 5)

A network administrator is configuring an FTD in transparent mode. A bridge group is set up and an access policy has been set up to allow all IP traffic. Traffic is not passing through the FTD. What additional configuration is needed?

- A. The security levels of the interfaces must be set.
- B. A default route must be added to the FTD.
- C. An IP address must be assigned to the BVI.
- D. A mac-access control list must be added to allow all MAC addresses.

Answer: C

NEW QUESTION 147

- (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 152

- (Exam Topic 5)

An engineer is attempting to create a new dashboard within the Cisco FMC to have a single view with widgets from many of the other dashboards. The goal is to have a mixture of threat and security related widgets along with Cisco Firepower device health information. Which two widgets must be configured to provide this information? (Choose two).

- A. Intrusion Events
- B. Correlation Information
- C. Appliance Status
- D. Current Sessions
- E. Network Compliance

Answer: AE

NEW QUESTION 155

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 159

- (Exam Topic 5)

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 163

- (Exam Topic 5)

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

- A. Only the UDP packet type is supported.
- B. The output format option for the packet logs is unavailable.

- C. The destination MAC address is optional if a VLAN ID value is entered.
D. The VLAN ID and destination MAC address are optional.

Answer: C

NEW QUESTION 167

- (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 169

- (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 171

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 172

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 173

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 178

- (Exam Topic 5)

The CEO ask a network administrator to present to management a dashboard that shows custom analysis tables for the top DNS queries URL category statistics, and the URL reputation statistics.

Which action must the administrator take to quickly produce this information for management?

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

Answer: B

NEW QUESTION 180

- (Exam Topic 5)

Refer to the exhibit.



What is the effect of the existing Cisco FMC configuration?

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

Answer: D

NEW QUESTION 184

- (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 185

- (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 187

- (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 190

- (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 192

- (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 197

- (Exam Topic 5)

An administrator is working on a migration from Cisco ASA to the Cisco FTD appliance and needs to test the rules without disrupting the traffic. Which policy type should be used to configure the ASA rules during this phase of the migration?

- A. identity
- B. Intrusion
- C. Access Control
- D. Prefilter

Answer: C

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-M>

NEW QUESTION 201

- (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 202

- (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 206

- (Exam Topic 5)

An administrator must use Cisco FMC to install a backup route within the Cisco FTD to route traffic in case of a routing failure with the primary route. Which action accomplishes this task?

- A. Install the static backup route and modify the metric to be less than the primary route.
- B. Configure EIGRP routing on the FMC to ensure that dynamic routes are always updated.

- C. Use a default route on the FMC instead of having multiple routes contending for priority.
- D. Create the backup route and use route tracking on both routes to a destination IP address in the network.

Answer: A

NEW QUESTION 211

- (Exam Topic 5)

What is the RTC workflow when the infected endpoint is identified?

- A. Cisco ISE instructs Cisco AMP to contain the infected endpoint.
- B. Cisco ISE instructs Cisco FMC to contain the infected endpoint.
- C. Cisco AMP instructs Cisco FMC to contain the infected endpoint.
- D. Cisco FMC instructs Cisco ISE to contain the infected endpoint.

Answer: D

NEW QUESTION 213

- (Exam Topic 5)

Which license type is required on Cisco ISE to integrate with Cisco FMC pxGrid?

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

Answer: B

NEW QUESTION 218

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 219

- (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 223

- (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 228

- (Exam Topic 4)

What is a valid Cisco AMP file disposition?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 230

- (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 233

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 237

- (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 238

- (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: DE

NEW QUESTION 241

- (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 246

- (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 247

- (Exam Topic 4)

Which two features of Cisco AMP for Endpoints allow for an uploaded file to be blocked? (Choose two.)

- A. application blocking
- B. simple custom detection
- C. file repository
- D. exclusions
- E. application whitelisting

Answer: AB

NEW QUESTION 249

- (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 250

- (Exam Topic 3)

Which limitation applies to Cisco Firepower Management Center dashboards in a multidomain environment?

- A. Child domains can view but not edit dashboards that originate from an ancestor domain.
- B. Child domains have access to only a limited set of widgets from ancestor domains.
- C. Only the administrator of the top ancestor domain can view dashboards.
- D. Child domains cannot view dashboards that originate from an ancestor domain.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 255

- (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 260

- (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 263

- (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 264

- (Exam Topic 3)

Which command-line mode is supported from the Cisco Firepower Management Center CLI?

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

Answer: C

Explanation:

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

NEW QUESTION 265

- (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 268

- (Exam Topic 2)

Which two routing options are valid with Cisco Firepower Threat Defense? (Choose two.)

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

Answer: AC

Explanation:

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

NEW QUESTION 269

- (Exam Topic 2)

Which Cisco Firepower rule action displays an HTTP warning page?

- A. Monitor
- B. Block
- C. Interactive Block
- D. Allow with Warning

Answer: C

Explanation:

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

NEW QUESTION 270

- (Exam Topic 2)

An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events filling 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 275

- (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 279

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 283

- (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 287

- (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 289

- (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 290

- (Exam Topic 1)

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

- A. a default DMZ policy for which only a user can change the IP addresses.
- B. deny ip any
- C. no policy rule is included
- D. permit ip any

Answer: C

NEW QUESTION 295

- (Exam Topic 1)

Which interface type allows packets to be dropped?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 297

- (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 302

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 307

- (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 312

- (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.html>

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 317

- (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 319

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-710 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-710 Product From:

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

Money Back Guarantee

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