Cisco

Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

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)
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 4
- (Exam Topic 5)
An engineer integrates Cisco FMC and Cisco ISE using pxGrid. Which role is assigned for Cisco FMC?

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

Answer: C

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

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

Answer: B

NEW QUESTION 6
- (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 7
- (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 8
- (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 9
- (Exam Topic 5)
An engineer is configuring a second Cisco FMC as a standby device but is unable to register with the active unit. What is causing this issue?

A. The primary FMC currently has devices connected to it.
B. The code versions running on the Cisco FMC devices are different
C. The licensing purchased does not include high availability
D. There is only 10 Mbps of bandwidth between the two devices.

Answer: B

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

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

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

Answer: A

NEW QUESTION 14
- (Exam Topic 5)
With Cisco FTD integrated routing and bridging, which interface does the bridge group use to communicate with a routed interface?

A. switch virtual
B. bridge group member
C. bridge virtual
D. subinterface

Answer: C

Explanation:

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

NEW QUESTION 16
- (Exam Topic 5)
A security engineer found a suspicious file from an employee email address and is trying to upload it for analysis, however the upload is failing. The last registration status is still active. What is the cause for this issue?

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

Answer: B

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

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

Answer: A

NEW QUESTION 21
- (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 25
- (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 27
- (Exam Topic 5)
A network engineer is tasked with minimising traffic interruption during peak traffic limes. When the SNORT inspection engine is overwhelmed, what must be configured to alleviate this issue?

A. Enable IPS inline link state propagation
B. Enable Pre-filter policies before the SNORT engine failure.
C. Set a Trust ALL access control policy.
D. Enable Automatic Application Bypass.

Answer: D

NEW QUESTION 29
- (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 33
- (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

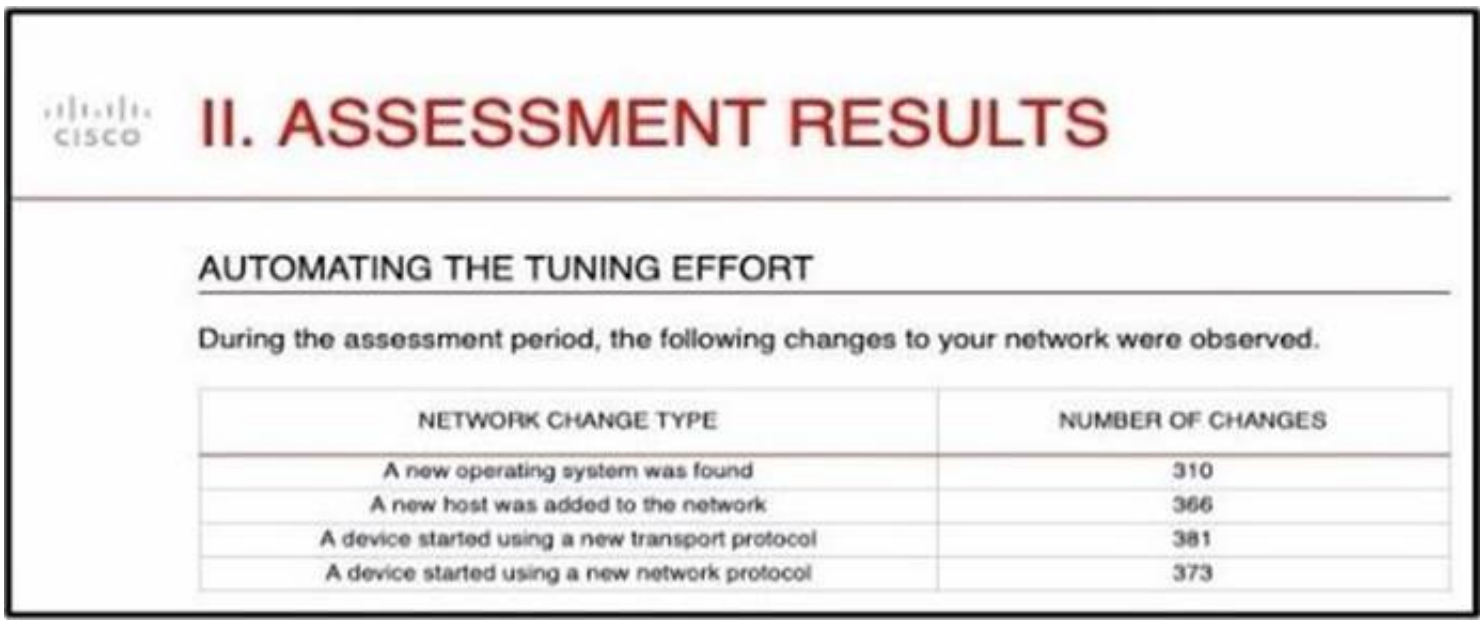
Answer: B

NEW QUESTION 38
- (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 41
- (Exam Topic 5)
Refer to the exhibit.



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

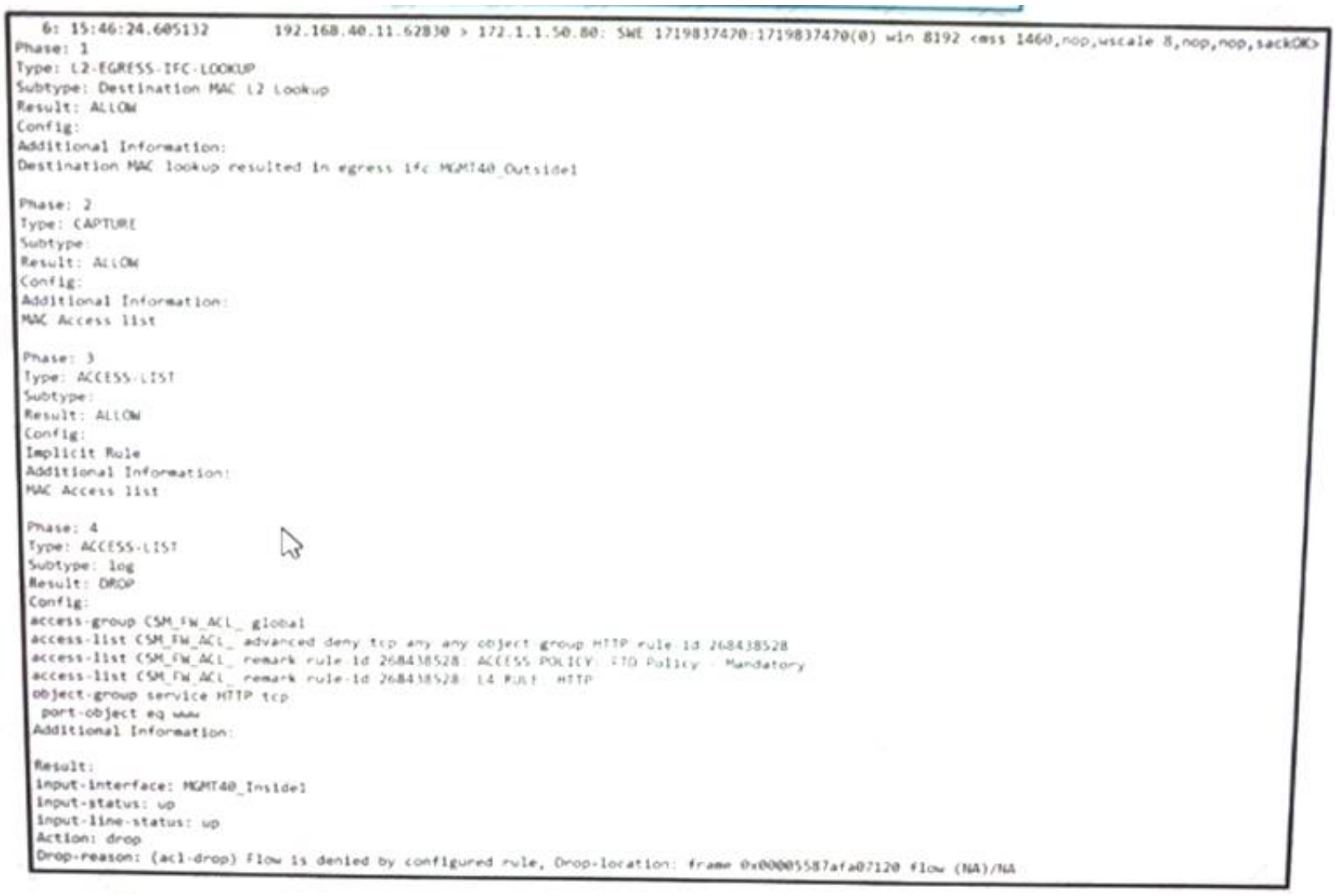
Explanation:
Ref:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Tailor

NEW QUESTION 42
- (Exam Topic 5)
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 45
- (Exam Topic 5)
Refer to the exhibit.



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 48
- (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 50
- (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 52
- (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 53
- (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 58
- (Exam Topic 5)
Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC (Choose two).

A. Before re-adding the device In Cisco FMC, the manager must be added back.
B. The Cisco FMC web interface prompts users to re-apply access control policies.
C. Once a device has been deleted, It must be reconfigured before it is re-added to the Cisco FMC.
D. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re-apply the polices after registration is completed.
E. There is no option to re-apply NAT and VPN policies during registration is available, so users need to re-apply the policies after registration is completed.

Answer: BE

NEW QUESTION 63
- (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 64
- (Exam Topic 5)
An administrator is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of NAT001 and a password of Cisco0420l06525. The private IP address of the FMC server is 192.168.45.45. which is being translated to the public IP address of 209.165.200.225/27. Which command set must be used in order to accomplish this task?

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

Answer: A

NEW QUESTION 67
- (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 68
- (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 73
- (Exam Topic 5)
An administrator needs to configure Cisco FMC to send a notification email when a data transfer larger than 10 MB is initiated from an internal host outside of standard business hours. Which Cisco FMC feature must be configured to accomplish this task?

A. file and malware policy
B. application detector

C. intrusion policy
D. correlation policy

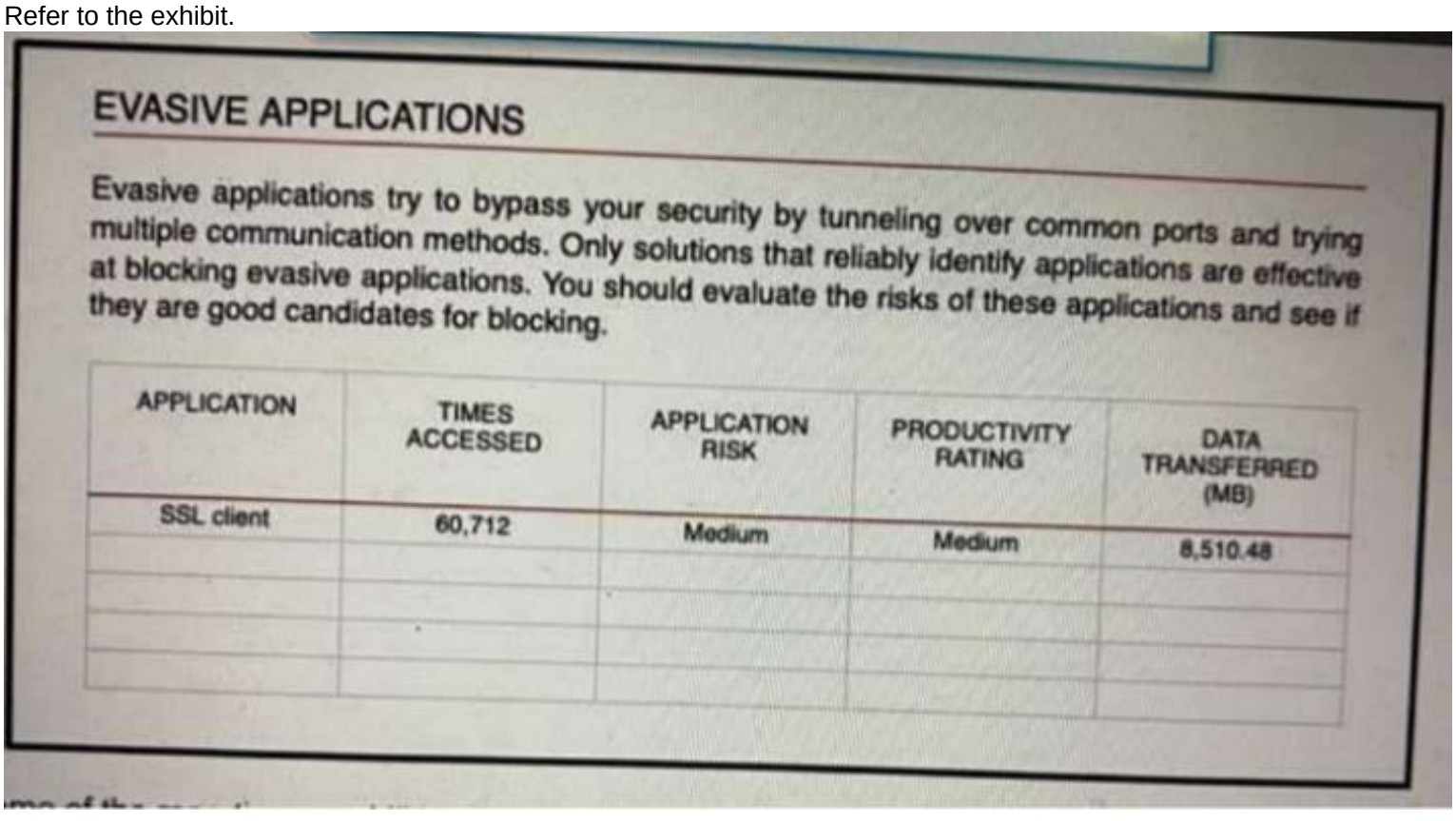
Answer: A

NEW QUESTION 74
- (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 79
- (Exam Topic 5)
Refer to the exhibit.



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

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

Answer: A

NEW QUESTION 82
- (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 85
- (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 90
- (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 93
- (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 95
- (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 97
- (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 101
- (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 102
- (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 104
- (Exam Topic 5)
A network administrator registered a new FTD to an existing FMC. The administrator cannot place the FTD in transparent mode. Which action enables transparent mode?

A. Add a Bridge Group Interface to the FTD before transparent mode is configured.
B. Dereglster the FTD device from FMC and configure transparent mode via the CLI.
C. Obtain an FTD model that supports transparent mode.
D. Assign an IP address to two physical interfaces.

Answer: B

NEW QUESTION 105
- (Exam Topic 5)
An organization recently implemented a transparent Cisco FTD in their network. They must ensure that the device does not respond to insecure SSL/TLS protocols. Which action accomplishes the task?

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

Answer: B

NEW QUESTION 107
- (Exam Topic 5)
An organization is setting up two new Cisco FTD devices to replace their current firewalls and cannot have any network downtime During the setup process, the synchronization between the two devices is failing What action is needed to resolve this issue?

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

Answer: B

NEW QUESTION 111
- (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 113
- (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 118
- (Exam Topic 5)
Refer to the exhibit.

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

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

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

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

Answer: A

NEW QUESTION 119
- (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 122
- (Exam Topic 5)
A network administrator is migrating from a Cisco ASA to a Cisco FTD. EIGRP is configured on the Cisco ASA but it is not available in the Cisco FMC. Which action must the administrator take to enable this feature on the Cisco FTD?

A. Configure EIGRP parameters using FlexConfig objects.
B. Add the command feature eigrp via the FTD CLI.
C. Create a custom variable set and enable the feature in the variable set.
D. Enable advanced configuration options in the FMC.

Answer: A

NEW QUESTION 127
- (Exam Topic 5)
A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?

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

Answer: A

NEW QUESTION 132
- (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.

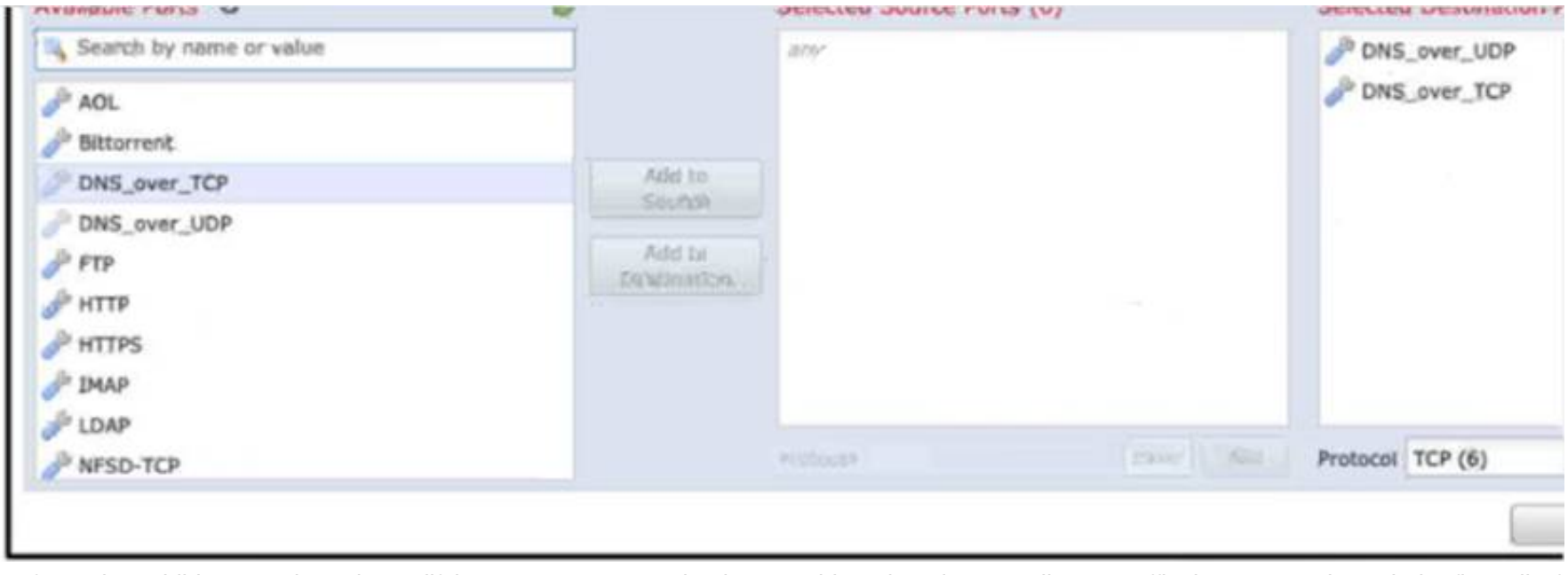
Answer: C

NEW QUESTION 133
- (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 138
- (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 139
- (Exam Topic 5)
An engineer is configuring a cisco FTD appliance in IPS-only mode and needs to utilize fail-to-wire interfaces. Which interface mode should be used to meet these requirements?

A. transparent
B. routed
C. passive
D. inline set

Answer: D

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

NEW QUESTION 144
- (Exam Topic 5)
A security engineer must deploy a Cisco FTD appliance as a bump in the wire to detect intrusion events without disrupting the flow of network traffic. Which two features must be configured to accomplish the task? (Choose two.)

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

Answer: BC

NEW QUESTION 149
- (Exam Topic 5)
Which two routing options are valid with Cisco FTD? (Choose Two)

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

Answer: AC

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

NEW QUESTION 153
- (Exam Topic 5)
An analyst using the security analyst account permissions is trying to view the Correlations Events Widget but is not able to access it. However, other dashboards are accessible. Why is this occurring?

A. An API restriction within the Cisco FMC is preventing the widget from displaying.
B. The widget is configured to display only when active events are present.
C. The widget is not configured within the Cisco FMC.
D. The security analyst role does not have permission to view this widget.

Answer: C

NEW QUESTION 157
- (Exam Topic 5)
Which process should be checked when troubleshooting registration issues between Cisco FMC and managed devices to verify that secure communication is occurring?

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

Answer: D

NEW QUESTION 162
- (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 163
- (Exam Topic 5)
An organization has noticed that malware was downloaded from a website that does not currently have a known bad reputation. How will this issue be addresses globally in the quickest way possible and with the least amount of impact?

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

Answer: D

NEW QUESTION 166
- (Exam Topic 5)
An engineer must configure the firewall to monitor traffic within a single subnet without increasing the hop count of that traffic. How would the engineer achieve this?

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

Answer: A

NEW QUESTION 167
- (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 170
- (Exam Topic 5)
An engineer must investigate a connectivity issue and decides to use the packet capture feature on Cisco FTD. The goal is to see the real packet going through the Cisco FTD device and see the Snort detection actions as a part of the output. After the capture-traffic command is issued, only the packets are displayed. Which action resolves this issue?

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

Answer: B

NEW QUESTION 175
- (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 180
- (Exam Topic 5)
A security engineer is configuring a remote Cisco FTD that has limited resources and internet bandwidth. Which malware action and protection option should be configured to reduce the requirement for cloud lookups?

A. Malware Cloud Lookup and dynamic analysis
B. Block Malware action and dynamic analysis
C. Block Malware action and local malware analysis
D. Block File action and local malware analysis

Answer: C

NEW QUESTION 181
- (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 183
- (Exam Topic 5)
The event dashboard within the Cisco FMC has been inundated with low priority intrusion drop events, which are overshadowing high priority events. An engineer has been tasked with reviewing the policies and reducing the low priority events. Which action should be configured to accomplish this task?

A. generate events
B. drop packet
C. drop connection
D. drop and generate

Answer: B

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

NEW QUESTION 187
- (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 192
- (Exam Topic 3)
A network engineer is configuring URL Filtering on Firepower Threat Defense. Which two port requirements on the Firepower Management Center must be validated to allow communication with the cloud service? (Choose two.)

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

D. inbound port TCP/443
E. outbound port TCP/80

Answer: AE

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

NEW QUESTION 196
- (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 201
- (Exam Topic 3)
What is a functionality of port objects in Cisco FMC?

A. to mix transport protocols when setting both source and destination port conditions in a rule
B. to represent protocols other than TCP, UDP, and ICMP
C. to represent all protocols in the same way
D. to add any protocol other than TCP or UDP for source port conditions in access control rules.

Answer: B

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

NEW QUESTION 205
- (Exam Topic 3)
Which action should be taken after editing an object that is used inside an access control policy?

A. Delete the existing object in use.
B. Refresh the Cisco FMC GUI for the access control policy.
C. Redeploy the updated configuration.
D. Create another rule using a different object name.

Answer: C

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

NEW QUESTION 209
- (Exam Topic 3)
Which group within Cisco does the Threat Response team use for threat analysis and research?

A. Cisco Deep Analytics
B. OpenDNS Group
C. Cisco Network Response
D. Cisco Talos

Answer: D

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

NEW QUESTION 214
- (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 216
- (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 221
- (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 224
- (Exam Topic 3)
What is the maximum bit size that Cisco FMC supports for HTTPS certificates?

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

Answer: C

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

NEW QUESTION 225
- (Exam Topic 3)
What is a behavior of a Cisco FMC database purge?

A. User login and history data are removed from the database if the User Activity check box is selected.
B. Data can be recovered from the device.
C. The appropriate process is restarted.
D. The specified data is removed from Cisco FMC and kept for two weeks.

Answer: C

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

NEW QUESTION 229
- (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 230
- (Exam Topic 3)
Which two packet captures does the FTD LINA engine support? (Choose two.)

A. Layer 7 network ID
B. source IP

C. application ID
D. dynamic firewall importing
E. protocol

Answer: BE

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

NEW QUESTION 233
- (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 238
- (Exam Topic 2)
A network administrator reviews the file report for the last month and notices that all file types, except exe. show a disposition of unknown. What is the cause of this issue?

A. The malware license has not been applied to the Cisco FTD.
B. The Cisco FMC cannot reach the Internet to analyze files.
C. A file policy has not been applied to the access policy.
D. Only Spero file analysis is enabled.

Answer: C

Explanation:
A file policy defines the actions that the Cisco Firepower Threat Defense (FTD) device should take when it
encounters different types of files. The file policy is applied as part of an access control policy. If an access control policy does not include a file policy, the FTD device will not take any action on the files it encounters, resulting in a disposition of "unknown" for all file types except exe.
Reference:
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the

NEW QUESTION 239
- (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 242
- (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 244
- (Exam Topic 2)
An administrator is creating interface objects to better segment their network but is having trouble adding interfaces to the objects. What is the reason for this

failure?

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

Answer: D

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

NEW QUESTION 245
- (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 249
- (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 250
- (Exam Topic 2)
Which Firepower feature allows users to configure bridges in routed mode and enables devices to perform Layer 2 switching between interfaces?

A. FlexConfig
B. BDI
C. SGT
D. IRB

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/relnotes/Firepower_System_Release_Notes_Version_620/new_features_and_functionality.html

NEW QUESTION 251
- (Exam Topic 2)
Which command is run on an FTD unit to associate the unit to an FMC manager that is at IP address 10.0.0.10, and that has the registration key Cisco123?

A. configure manager local 10.0.0.10 Cisco123
B. configure manager add Cisco123 10.0.0.10
C. configure manager local Cisco123 10.0.0.10
D. configure manager add 10.0.0.10 Cisco123

Answer: D

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

NEW QUESTION 253
- (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 255
- (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 259
- (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 262
- (Exam Topic 1)
What is the difference between inline and inline tap on Cisco Firepower?

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

Answer: A

NEW QUESTION 265
- (Exam Topic 1)
An engineer is tasked with deploying an internal perimeter firewall that will support multiple DMZs Each DMZ has a unique private IP subnet range. How is this requirement satisfied?

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

Answer: C

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

NEW QUESTION 269
- (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 274
- (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 279
- (Exam Topic 1)
Which two deployment types support high availability? (Choose two.)

A. transparent
B. routed
C. clustered
D. intra-chassis multi-instance
E. virtual appliance in public cloud

Answer: AB

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

NEW QUESTION 280
- (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 285
- (Exam Topic 1)
An administrator is optimizing the Cisco FTD rules to improve network performance, and wants to bypass inspection for certain traffic types to reduce the load on the Cisco FTD. Which policy must be configured to accomplish this goal?

A. prefilter
B. intrusion
C. identity
D. URL filtering

Answer: A

NEW QUESTION 290
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

300-710 Practice Exam Features:

* 300-710 Questions and Answers Updated Frequently

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

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

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