Cisco

Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

NEW QUESTION 1
- (Exam Topic 5)
Which Cisco FMC report gives the analyst information about the ports and protocols that are related to the configured sensitive network for analysis?

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

Answer: D

NEW QUESTION 2
- (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

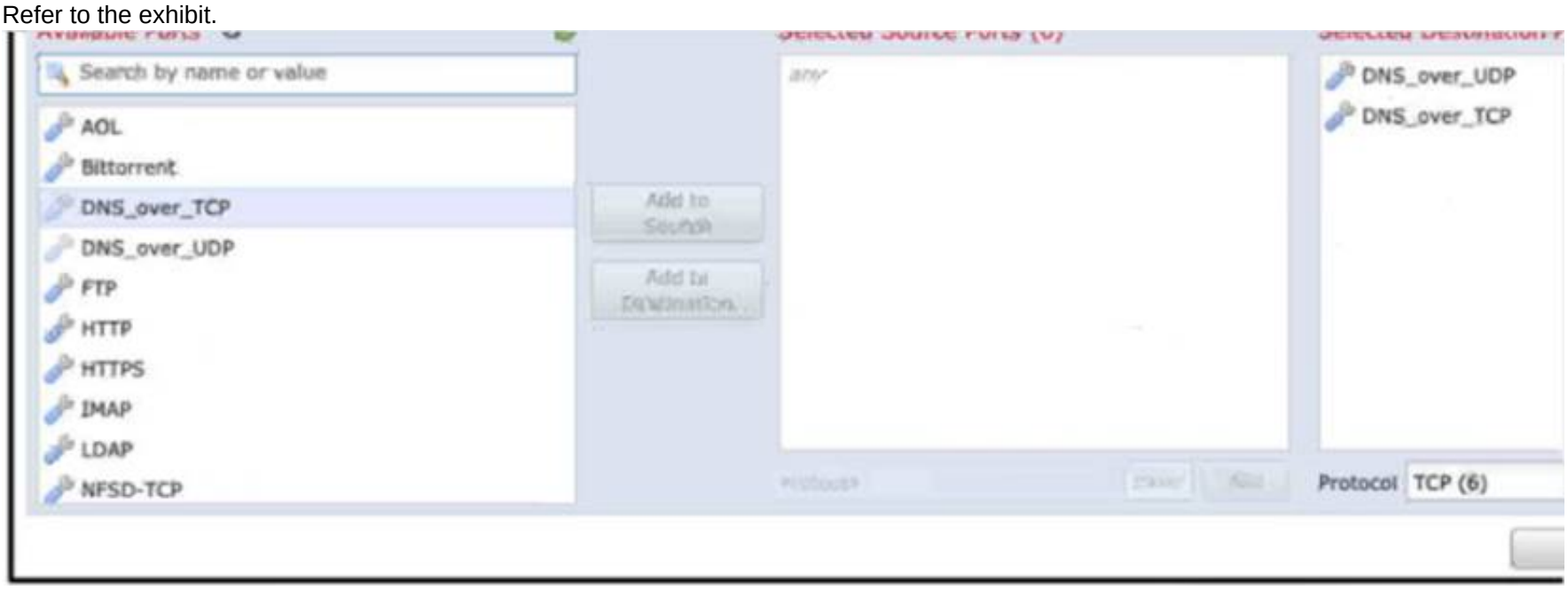
Answer: B

NEW QUESTION 3
- (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 4
- (Exam Topic 5)
Refer to the exhibit.



An engineer is modifying an access control policy to add a rule to Inspect all DNS traffic that passes it making the change and deploying the policy, they see that DNS traffic Is not being Inspected by the Snort engine. What is.....

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

Answer: A

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

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

Answer: B

NEW QUESTION 6
- (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 7
- (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 8
- (Exam Topic 5)
An engineer has been tasked with providing disaster recovery for an organization's primary Cisco FMC. What must be done on the primary and secondary Cisco FMCs to ensure that a copy of the original corporate policy is available if the primary Cisco FMC fails?

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

Answer: A

NEW QUESTION 9
- (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 10
- (Exam Topic 5)
Which feature is supported by IRB on Cisco FTD devices?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 5)
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 14
- (Exam Topic 5)
An engineer is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of ACME001 and a password of Cisco388267669. Which command set must be used in order to accomplish this?

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

Answer: D

NEW QUESTION 16
- (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 21
- (Exam Topic 5)
A network engineer sets up a secondary Cisco FMC that is integrated with Cisco Security Packet Analyzer What occurs when the secondary Cisco FMC synchronizes with the primary Cisco FMC?

A. The existing integration configuration is replicated to the primary Cisco FMC
B. The existing configuration for integration of the secondary Cisco FMC the Cisco Security Packet Analyzer is overwritten.
C. The synchronization between the primary and secondary Cisco FMC fails
D. The secondary Cisco FMC must be reintegrated with the Cisco Security Packet Analyzer after the synchronization

Answer: B

NEW QUESTION 26
- (Exam Topic 5)
An engineer configures an access control rule that deploys file policy configurations to security zones or tunnel zones, and it causes the device to restart. What is the reason for the restart?

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

Answer: A

NEW QUESTION 27
- (Exam Topic 5)
An organization must be able to ingest NetFlow traffic from their Cisco FTD device to Cisco Stealthwatch for behavioral analysis. What must be configured on the Cisco FTD to meet this requirement?

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

Answer: A

NEW QUESTION 28
- (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 31
- (Exam Topic 5)

An engineer is configuring Cisco FMC and wants to limit the time allowed for processing packets through the interface However if the time is exceeded the configuration must allow packets to bypass detection What must be configured on the Cisco FMC to accomplish this task?

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

Answer: D

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

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

Answer: D

NEW QUESTION 34
- (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

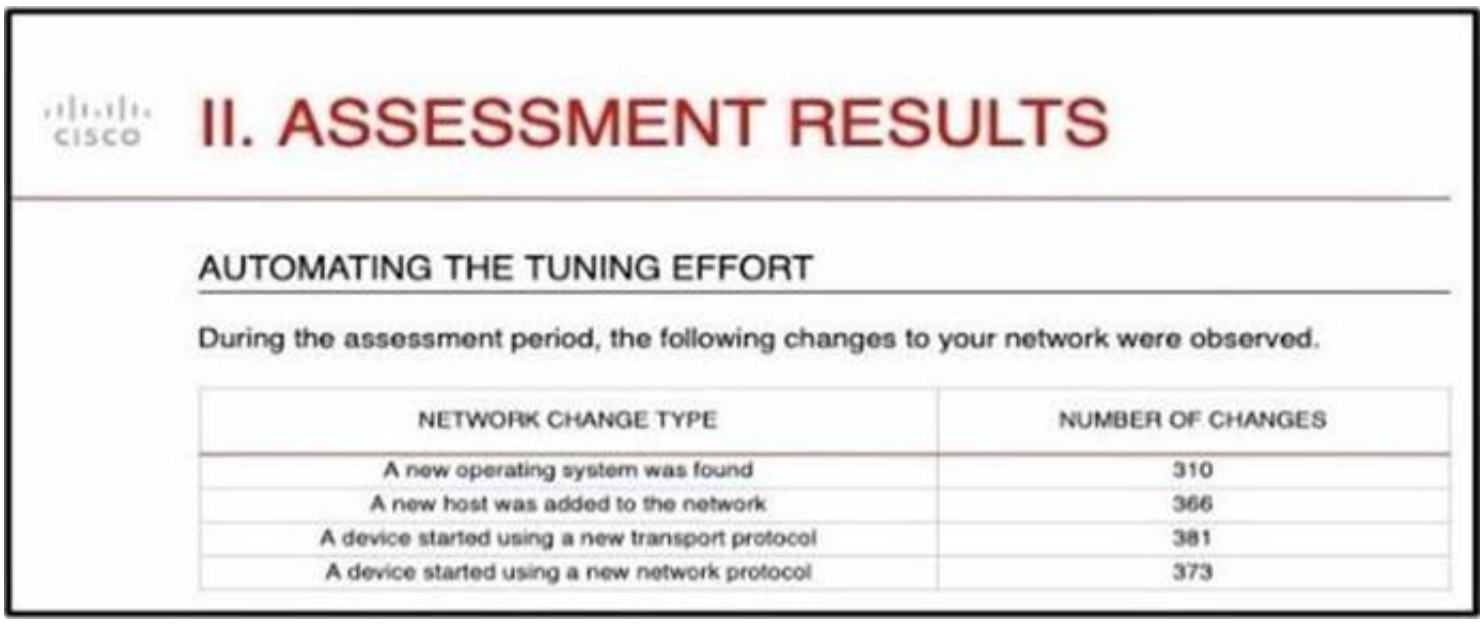
Answer: B

NEW QUESTION 36
- (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 39
- (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 44
- (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 49
- (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 54
- (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 58
- (Exam Topic 5)
An engineer must configure a Cisco FMC dashboard in a multidomain deployment Which action must the engineer take to edit a report template from an ancestor domain?

A. Add it as a separate widget.
B. Copy it to the current domain
C. Assign themselves ownership of it
D. Change the document attributes.

Answer: B

NEW QUESTION 63
- (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 66
- (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 71

- (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 72
- (Exam Topic 5)
An engineer wants to add an additional Cisco FTD Version 6.2.3 device to their current 6.2.3 deployment to create a high availability pair.
The currently deployed Cisco FTD device is using local management and identical hardware including the available port density to enable the failover and stateful links required in a proper high availability deployment. Which action ensures that the environment is ready to pair the new Cisco FTD with the old one?

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

Answer: A

NEW QUESTION 77
- (Exam Topic 5)
A network administrator has converted a Cisco FTD from using LDAP to LDAPS for VPN authentication. The Cisco FMC can connect to the LDAPS server, but the Cisco FTD is not connecting. Which configuration must be enabled on the Cisco FTD?

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

Answer: B

NEW QUESTION 80
- (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 needs to configure remote storage on Cisco FMC. Configuration backups must be available from a secure location on the network for disaster recovery. Reports need to back up to a shared location that auditors can access with their Active Directory logins. Which strategy must the engineer use to meet these objectives?

A. Use SMB for backups and NFS for reports.
B. Use NFS for both backups and reports.
C. Use SMB for both backups and reports.
D. Use SSH for backups and NFS for reports.

Answer: C

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/syste “You cannot send backups to one remote system and reports to another, but you can choose to send either to a remote system and store the other on the Firepower Management Center.”

NEW QUESTION 88
- (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 92
- (Exam Topic 5)
What is the advantage of having Cisco Firepower devices send events to Cisco Threat response via the security services exchange portal directly as opposed to using syslog?

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

Answer: D

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

NEW QUESTION 93
- (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 98
- (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 103
- (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 106
- (Exam Topic 5)
A network engineer must provide redundancy between two Cisco FTD devices. The redundancy configuration must include automatic configuration, translation, and connection updates. After the initial configuration of the two appliances, which two steps must be taken to proceed with the redundancy configuration? (Choose two.)

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

Answer: AC

NEW QUESTION 111
- (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 112
- (Exam Topic 5)
An engineer wants to connect a single IP subnet through a Cisco FTD firewall and enforce policy. There is a requirement to present the internal IP subnet to the outside as a different IP address. What must be configured to meet these requirements?

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

Answer: C

NEW QUESTION 116
- (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 121
- (Exam Topic 5)
An administrator is attempting to remotely log into a switch in the data centre using SSH and is unable to connect. How does the administrator confirm that traffic is reaching the firewall?

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

Answer: B

NEW QUESTION 123
- (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 128
- (Exam Topic 5)
A network engineer is receiving reports of users randomly getting disconnected from their corporate applications which traverses the data center FTD appliance Network monitoring tools show that the FTD appliance utilization is peaking above 90% of total capacity. What must be done in order to further analyze this issue?

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

Answer: B

NEW QUESTION 130
- (Exam Topic 5)
With a recent summer time change, system logs are showing activity that occurred to be an hour behind real time Which action should be taken to resolve this issue?

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

Answer: B

NEW QUESTION 135
- (Exam Topic 5)
An administrator is adding a QoS policy to a Cisco FTD deployment. When a new rule is added to the policy and QoS is applied on 'Interfaces in Destination Interface Objects", no interface objects are available What is the problem?

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

Answer: C

NEW QUESTION 140
- (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 141
- (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 142
- (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 146
- (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 151
- (Exam Topic 5)
What is the role of the casebook feature in Cisco Threat Response?

A. sharing threat analysts
B. pulling data via the browser extension
C. triage automaton with alerting
D. alert prioritization

Answer: A

Explanation:
The casebook and pivot menu are widgets available in Cisco Threat Response. Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables.
https://www.cisco.com/c/en/us/td/docs/se curity/ces/user_guide/esa_user_guide_13-5-1/b_ESA_Admin_Guide_ces_13-5-1/b_ESA_Admin_Guide_13-0_chapter_0110001.pdf

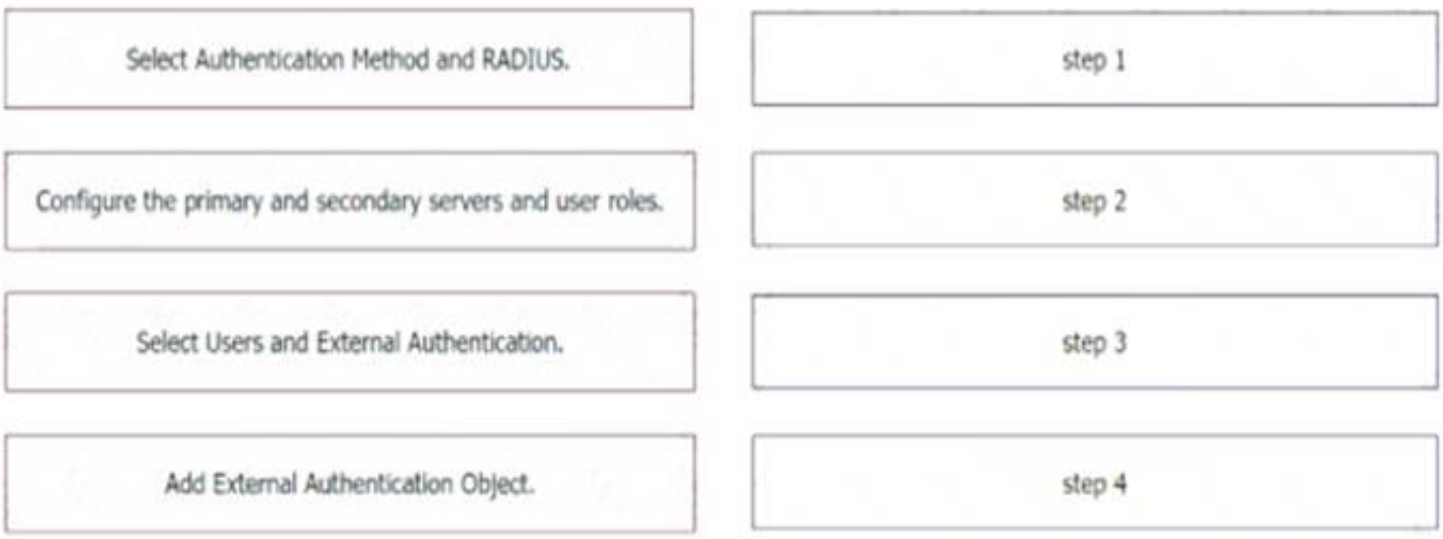
NEW QUESTION 156

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

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

Answer: D

NEW QUESTION 159
- (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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
4, 1, 2, 3

NEW QUESTION 163
- (Exam Topic 5)
Which protocol is needed to exchange threat details in rapid threat containment on Cisco FMC?

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

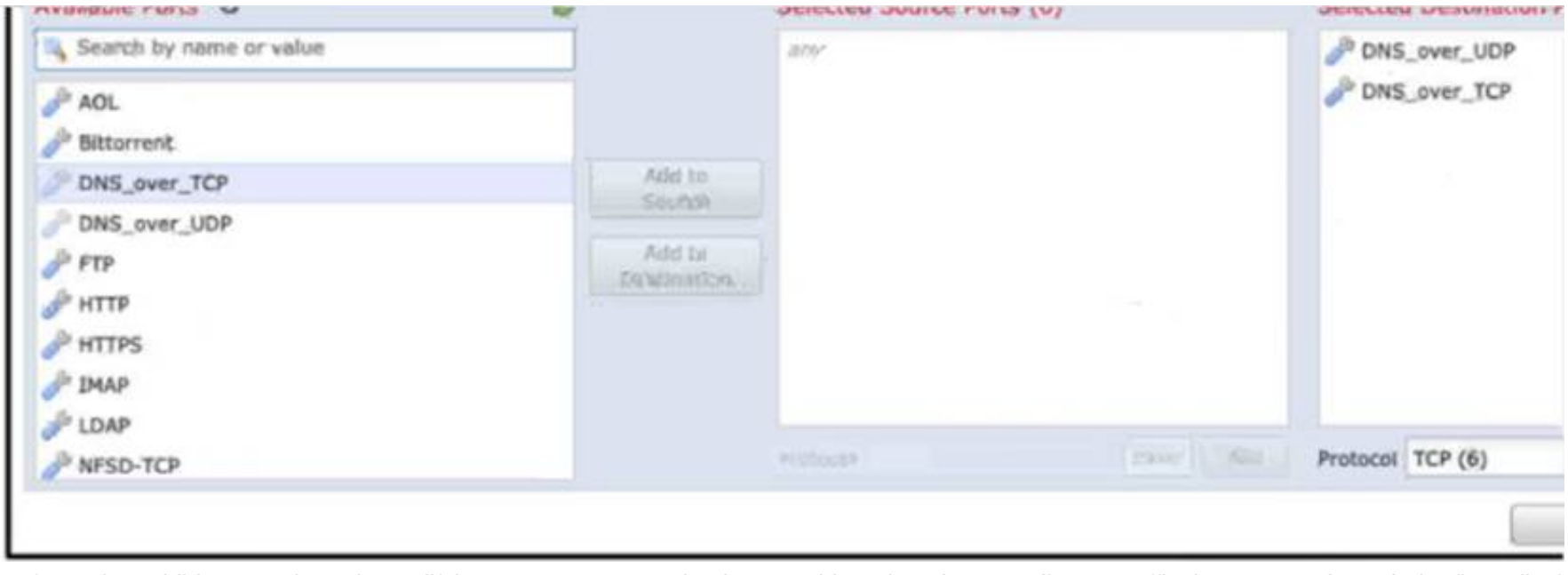
Answer: D

NEW QUESTION 166
- (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 169
- (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 174
- (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 175
- (Exam Topic 5)
An administrator is configuring a transparent Cisco FTD device to receive ERSPAN traffic from multiple switches on a passive port but the FTD is not processing the traffic What is the problem?

A. The switches do not have Layer 3 connectivity to the FTD device for GRE traffic transmission.
B. The FTD must be configured with an ERSPAN port, not a passive port.
C. The FTD must &e in routed mode to process ERSPAN traffic.
D. The switches were not set up with a monitor session ID (hat matches the flow ID defined on the FTD

Answer: C

NEW QUESTION 178
- (Exam Topic 5)
An engineer is 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 180
- (Exam Topic 5)
Network traffic coining from an organization's CEO must never be denied. Which access control policy configuration option should be used if the deployment engineer is not permitted to create a rule to allow all traffic?

A. Configure firewall bypass.
B. Change the intrusion policy from security to balance.
C. Configure a trust policy for the CEO.
D. Create a NAT policy just for the CEO.

Answer: C

NEW QUESTION 181
- (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 183
- (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 185
- (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 186
- (Exam Topic 5)
An engineer runs the command restore remote-manager-backup location 2.2.2.2 admin /Volume/home/admin FTD408566513.zip on a Cisco FMC. After connecting to the repository, the Cisco FTD device is unable to accept the backup file. What is the reason for this failure?

A. The backup file is not in .cfg format.
B. The wrong IP address is used.
C. The backup file extension was changed from .tar to .zip.
D. The directory location is incorrect.

Answer: C

Explanation:
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3455.pdf

NEW QUESTION 188
- (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 191
- (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 196
- (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 200
- (Exam Topic 5)
A network administrator is configuring a site-to-site IPsec VPN to a router sitting behind a Cisco FTD. The administrator has configured an access policy to allow traffic to this device on UDP 500, 4500, and ESP VPN traffic is not working. Which action resolves this issue?

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

Answer: B

NEW QUESTION 203
- (Exam Topic 5)
Upon detecting a flagrant threat on an endpoint, which two technologies instruct Cisco Identity Services Engine to contain the infected endpoint either manually or automatically? (Choose two.)

A. Cisco ASA 5500 Series
B. Cisco FMC
C. Cisco AMP
D. Cisco Stealthwatch
E. Cisco ASR 7200 Series

Answer: CD

NEW QUESTION 207
- (Exam Topic 4)
Which two remediation options are available when Cisco FMC is integrated with Cisco ISE? (Choose two.)

A. dynamic null route configured
B. DHCP pool disablement
C. quarantine
D. port shutdown
E. host shutdown

Answer: CD

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524-configure- firepower-6-1-pxgrid-remediati.html

NEW QUESTION 212
- (Exam Topic 4)
What is the maximum SHA level of filtering that Threat Intelligence Director supports?

A. SHA-1024
B. SHA-4096
C. SHA-512
D. SHA-256

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisc

NEW QUESTION 213
- (Exam Topic 4)
Which connector is used to integrate Cisco ISE with Cisco FMC for Rapid Threat Containment?

A. pxGrid
B. FTD RTC
C. FMC RTC
D. ISEGrid

Answer: A

NEW QUESTION 215
- (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 219
- (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 221
- (Exam Topic 5)
A network administrator discovers that a user connected to a file server and downloaded a malware file. The Cisc FMC generated an alert for the malware event, however the user still remained connected. Which Cisco APM file rule action within the Cisco FMC must be set to resolve this issue?

A. Detect Files
B. Malware Cloud Lookup
C. Local Malware Analysis
D. Reset Connection

Answer: D

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

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

Answer: DE

NEW QUESTION 229
- (Exam Topic 3)
After deploying a network-monitoring tool to manage and monitor networking devices in your organization, you realize that you need to manually upload an MIB for the Cisco FMC. In which folder should you upload the MIB file?

A. /etc/sf/DCMIB.ALERT

B. /sf/etc/DCEALERT.MIB
C. /etc/sf/DCEALERT.MIB
D. system/etc/DCEALERT.MIB

Answer: C

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-External-Responses.pdf

NEW QUESTION 231
- (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 232
- (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 236
- (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 239
- (Exam Topic 3)
Which command is typed at the CLI on the primary Cisco FTD unit to temporarily stop running high- availability?

A. configure high-availability resume
B. configure high-availability disable
C. system support network-options
D. configure high-availability suspend

Answer: B

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 240
- (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 245
- (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 248
- (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 251
- (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 256
- (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 259
- (Exam Topic 2)
A company is in the process of deploying intrusion prevention with Cisco FTDs managed by a Cisco FMC. An engineer must configure policies to detect potential intrusions but not block the suspicious traffic. Which action accomplishes this task?

A. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the "Drop when inline" option.
B. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the "Drop when inline" option.
C. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the "Drop when inline" option.
D. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the "Drop when inline" option.

Answer: A

NEW QUESTION 261
- (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 263
- (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 265
- (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 267
- (Exam Topic 2)
An engineer is using the configure manager add <FMC IP> Cisc402098527 command to add a new Cisco FTD device to the Cisco FMC; however, the device is not being added. Why Is this occurring?

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

Answer: A

NEW QUESTION 270
- (Exam Topic 2)
In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.)

A. Traffic inspection can be interrupted temporarily when configuration changes are deployed.
B. The system performs intrusion inspection followed by file inspection.
C. They can block traffic based on Security Intelligence data.
D. File policies use an associated variable set to perform intrusion prevention.
E. The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters.

Answer: AC

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

NEW QUESTION 275
- (Exam Topic 2)
An engineer is configuring Cisco FMC and wants to allow multiple physical interfaces to be part of the same VLAN. The managed devices must be able to perform Layer 2 switching between interfaces, including
sub-interfaces. What must be configured to meet these requirements?

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

Answer: C

NEW QUESTION 279
- (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 280
- (Exam Topic 2)
An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events filing the database and overloading the Cisco FMC. A monitored NAT device is executing multiple updates of its operating system in a short period of time. What configuration change must be made to alleviate this issue?

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

Answer: D

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

NEW QUESTION 282
- (Exam Topic 2)
In which two places can thresholding settings be configured? (Choose two.)

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

Answer: AC

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

NEW QUESTION 283
- (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 285
- (Exam Topic 2)
Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)

A. OSPFv2 with IPv6 capabilities
B. virtual links
C. SHA authentication to OSPF packets
D. area boundary router type 1 LSA filtering
E. MD5 authentication to OSPF packets

Answer: BE

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

NEW QUESTION 287
- (Exam Topic 2)
Which two types of objects are reusable and supported by Cisco FMC? (Choose two.)

A. dynamic key mapping objects that help link HTTP and HTTPS GET requests to Layer 7 application protocols.
B. reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists
C. network-based objects that represent IP address and networks, port/protocols pairs, VLAN tags, security zones, and origin/destination country
D. network-based objects that represent FQDN mappings and networks, port/protocol pairs, VXLAN tags, security zones and origin/destination country
E. reputation-based objects, such as URL categories

Answer: BC

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/reusable_objects.html#ID-2243-00000414

NEW QUESTION 289
- (Exam Topic 1)
Which firewall design allows a firewall to forward traffic at layer 2 and layer 3 for the same subnet?

A. Cisco Firepower Threat Defense mode
B. transparent mode
C. routed mode
D. integrated routing and bridging

Answer: B

NEW QUESTION 291
- (Exam Topic 1)
An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic concurrently. How must the devices be implemented in this environment?

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

Answer: C

NEW QUESTION 293
- (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 296
- (Exam Topic 1)
A network security engineer must replace a faulty Cisco FTD device in a high availability pair. Which action must be taken while replacing the faulty unit?

A. Shut down the Cisco FMC before powering up the replacement unit.
B. Ensure that the faulty Cisco FTD device remains registered to the Cisco FMC.
C. Unregister the faulty Cisco FTD device from the Cisco FMC
D. Shut down the active Cisco FTD device before powering up the replacement unit.

Answer: C

NEW QUESTION 300
- (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 304
- (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 308
- (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 309
- (Exam Topic 1)
A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?

A. Specify the BVI IP address as the default gateway for connected devices.
B. Enable routing on the Cisco Firepower
C. Add an IP address to the physical Cisco Firepower interfaces.
D. Configure a bridge group in transparent mode.

Answer: D

Explanation:
Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place. Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.

NEW QUESTION 313
- (Exam Topic 1)
An organization is migrating their Cisco ASA devices running in multicontext mode to Cisco FTD devices. Which action must be taken to ensure that each context on the Cisco ASA is logically separated in the Cisco FTD devices?

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

Answer: C

NEW QUESTION 314

- (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 317
- (Exam Topic 1)
Which two conditions must be met to enable high availability between two Cisco FTD devices? (Choose two.)

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

Answer: BE

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

NEW QUESTION 319
- (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 321
.....

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