

300-710 Dumps

Securing Networks with Cisco Firepower (SNCF)

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



NEW QUESTION 1

- (Exam Topic 5)

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

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

Answer: C

Explanation:

When you configure the Cisco Firepower devices to bypass the access control policies for VPN traffic, the devices will not inspect the VPN traffic and thus will not waste resources on it. This is the best option to ensure that the VPN traffic is not wasting resources on the Cisco Firepower devices.

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the>

NEW QUESTION 2

- (Exam Topic 5)

An engineer is creating an URL object on Cisco FMC How must it be configured so that the object will match for HTTPS traffic in an access control policy?

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

Answer: B

NEW QUESTION 3

- (Exam Topic 5)

A network administrator is trying to convert from LDAP to LDAPS for VPN user authentication on a Cisco FTD. Which action must be taken on the Cisco FTD objects to accomplish this task?

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

Answer: B

NEW QUESTION 4

- (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 5

- (Exam Topic 5)

An engineer is monitoring network traffic from their sales and product development departments, which are on two separate networks What must be configured in order to maintain data privacy for both departments?

- A. Use a dedicated IPS inline set for each department to maintain traffic separation
- B. Use 802.1Q mime set Trunk interfaces with VLANs to maintain logical traffic separation
- C. Use passive IDS ports for both departments
- D. Use one pair of inline set in TAP mode for both departments

Answer: B

NEW QUESTION 6

- (Exam Topic 5)

A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address <https://<FMC IP>/capture/CAP1/pcap/test.pcap>, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

- A. Disable the HTTPS server and use HTTP instead.
- B. Enable the HTTPS server for the device platform policy.
- C. Disable the proxy setting on the browser.
- D. Use the Cisco FTD IP address as the proxy server setting on the browser.

Answer: B

NEW QUESTION 7

- (Exam Topic 5)

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

A)

Add Capture

Name*: Server1_Capture Interface*: Inside

Match Criteria:

Protocol*: IP

Source Host*: 10.0.1.100 Source Network: 10.0.0.0/24

Destination Host*: 10.20.10.20 Destination Network: 10.20.0.0/24

☐ SGT number: 0 (0-65533)

Buffer:

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

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

Save Cancel

B)

Add Capture

Name*: Server1_Capture Interface*: Inside

Match Criteria:

Protocol*: IP

Source Host*: 10.20.10.20 Source Network: 10.20.0.0/24

Destination Host*: 10.0.1.100 Destination Network: 10.0.0.0/24

☐ SGT number: 0 (0-65533)

Buffer:

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

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

Save Cancel

C)

Add Capture

Name*: Server1_Capture Interface*: diagnostic

Match Criteria:

Protocol*: IP

Source Host*: 10.20.10.20 Source Network: 10.20.0.0/24

Destination Host*: 10.0.1.100 Destination Network: 10.0.0.0/24

☐ SGT number: 0 (0-65533)

Buffer:

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

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

Save Cancel

D)

Add Capture

Name*: Server1_Capture Interface*: diagnostic

Match Criteria:

Protocol*: IP

Source Host*: 10.0.1.100 Source Network: 255.255.255.255

Destination Host*: 10.20.10.20 Destination Network: 255.255.255.255

☐ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes

Buffer Size: 524288 1534-33554432 bytes

☒ Continuous Capture ☐ Stop when full

☒ Trace Trace Count: 50

Save Cancel

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

Answer: B

NEW QUESTION 8

- (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 9

- (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 10

- (Exam Topic 5)

An engineer installs a Cisco FTD device and wants to inspect traffic within the same subnet passing through a firewall and inspect traffic destined to the internet. Which configuration will meet this requirement?

- A. transparent firewall mode with IRB only
- B. routed firewall mode with BVI and routed interfaces
- C. transparent firewall mode with multiple BVIs
- D. routed firewall mode with routed interfaces only

Answer: C

NEW QUESTION 10

- (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 11

- (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 12

- (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 14

- (Exam Topic 5)

An administrator is configuring their transparent Cisco FTD device to receive ERSPAN traffic from multiple switches on a passive port, but the Cisco 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 switches were not set up with a monitor session ID that matches the flow ID defined on the CiscoFTD.
- C. The Cisco FTD must be in routed mode to process ERSPAN traffic.
- D. The Cisco FTD must be configured with an ERSPAN port not a passive port.

Answer: C

NEW QUESTION 19

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 22

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 25

- (Exam Topic 5)

What is a characteristic of bridge groups on a Cisco FTD?

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

Answer: B

NEW QUESTION 30

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

Answer: C

NEW QUESTION 31

- (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 33

- (Exam Topic 5)

A network administrator cannot select the link to be used for failover when configuring an active/passive HA Cisco FTD pair. Which configuration must be changed before setting up the high availability pair?

- A. An IP address in the same subnet must be added to each Cisco FTD on the interface.
- B. The interface name must be removed from the interface on each Cisco FTD.
- C. The name Failover must be configured manually on the interface on each cisco FTD.
- D. The interface must be configured as part of a LACP Active/Active EtherChannel.

Answer: A

NEW QUESTION 36

- (Exam Topic 5)

Refer to the exhibit.

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

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

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

Answer: C

Explanation:

Ref:

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

NEW QUESTION 37

- (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 41

- (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 44

- (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 47

- (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 policies 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 50

- (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 55

- (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 56

- (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 58

- (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 63

- (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 65

- (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 70

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 71

- (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 75

- (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 77

- (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 78

- (Exam Topic 5)

An organization has implemented Cisco Firepower without IPS capabilities and now wants to enable inspection for their traffic. They need to be able to detect protocol anomalies and utilize the Snort rule sets to detect malicious behaviour. How is this accomplished?

- A. Modify the access control policy to redirect interesting traffic to the engine
- B. Modify the network discovery policy to detect new hosts to inspect
- C. Modify the network analysis policy to process the packets for inspection
- D. Modify the intrusion policy to determine the minimum severity of an event to inspect.

Answer: D

NEW QUESTION 79

- (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 82

- (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. Deregister 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 84

- (Exam Topic 5)

A network engineer is extending a user segment through an FTD device for traffic inspection without creating another IP subnet How is this accomplished on an FTD device in routed mode?

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

Answer: C

Explanation:

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

NEW QUESTION 88

- (Exam Topic 5)

In a multi-tenant deployment where multiple domains are in use. which update should be applied outside of the Global Domain?

- A. minor upgrade
- B. local import of intrusion rules
- C. Cisco Geolocation Database
- D. local import of major upgrade

Answer: B

NEW QUESTION 90

- (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 91

- (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 95

- (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 99

- (Exam Topic 5)

Refer to the exhibit.

```
Phase: 16
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packets: 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 0x00055d2b0f807e0 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 102

- (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 104

- (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. Which technique will retain the policy consistency at each location but allow only the locally significant network subnet within the applicable rules?

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

Answer: D

NEW QUESTION 105

- (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 108

- (Exam Topic 5)

An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighbouring Cisco devices or use multicast in their environment. What must be done to resolve this issue?

- A. Create a firewall rule to allow CDP traffic.
- B. Create a bridge group with the firewall interfaces.
- C. Change the firewall mode to routed.
- D. Change the firewall mode to transparent.

Answer: C

NEW QUESTION 113

- (Exam Topic 5)

An engineer is setting up a new Firepower deployment and is looking at the default FMC policies to start the implementation. During the initial trial phase, the organization wants to test some common Snort rules while still allowing the majority of network traffic to pass. Which default policy should be used?

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

Answer: C

Explanation:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusio>

NEW QUESTION 116

- (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 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)

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/securi/cy/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 124

- (Exam Topic 5)

A network administrator is concerned about the 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 127

- (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 128

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 131

- (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 133

- (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 134

- (Exam Topic 5)

An engineer is troubleshooting connectivity to the DNS servers from hosts behind a new Cisco FTD device. The hosts cannot send DNS queries to servers in the DMZ. Which action should the engineer take to troubleshoot this issue using the real DNS packets?

- A. Use the Connection Events dashboard to check the block reason and adjust the inspection policy as needed.
- B. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion policy as needed.
- C. Use the packet tracer tool to determine at which hop the packet is being dropped.
- D. Use the show blocks command in the Threat Defense CLI tool and create a policy to allow the blocked traffic.

Answer: A

NEW QUESTION 135

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 138

- (Exam Topic 5)

Network traffic coming 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 140

- (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 142

- (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 144

- (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 148

- (Exam Topic 5)

Which feature within the Cisco FMC web interface allows for detecting, analyzing and blocking malware in network traffic?

- A. intrusion and file events
- B. Cisco AMP for Endpoints
- C. Cisco AMP for Networks
- D. file policies

Answer: C

NEW QUESTION 149

- (Exam Topic 5)

A network administrator is troubleshooting access to a website hosted behind a Cisco FTD device. External clients cannot access the web server via HTTPS. The IP address configured on the web server is 192.168.7.46. The administrator is running the command `capture CAP interface outside match ip any 192.168.7.46 255.255.255.255` but cannot see any traffic in the capture. Why is this occurring?

- A. The capture must use the public IP address of the web server.
- B. The FTD has no route to the web server.
- C. The access policy is blocking the traffic.
- D. The packet capture shows only blocked traffic.

Answer: A

NEW QUESTION 154

- (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 addressed 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 156

- (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 160

- (Exam Topic 5)

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

- A. Install the static backup route and modify the metric to be less than the primary route.
- B. Configure EIGRP routing on the FMC to ensure that dynamic routes are always updated.
- C. Use a default route on the FMC instead of having multiple routes contending for priority.
- D. Create the backup route and use route tracking on both routes to a destination IP address in the network.

Answer: A

NEW QUESTION 161

- (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 164

- (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 167

- (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 169

- (Exam Topic 5)

An organization has a compliancy requirement to protect servers from clients, however, the clients and servers all reside on the same Layer 3 network Without readdressing IP subnets for clients or servers, how is segmentation achieved?

- A. Deploy a firewall in transparent mode between the clients and servers.
- B. Change the IP addresses of the clients, while remaining on the same subnet.
- C. Deploy a firewall in routed mode between the clients and servers
- D. Change the IP addresses of the servers, while remaining on the same subnet

Answer: A

NEW QUESTION 174

- (Exam Topic 5)

An engineer has been asked to show application usages automatically on a monthly basis and send the information to management What mechanism should be used to accomplish this task?

- A. event viewer
- B. reports
- C. dashboards
- D. context explorer

Answer: B

NEW QUESTION 178

- (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 180

- (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 182

- (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 186

- (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 188

- (Exam Topic 3)

When do you need the file-size command option during troubleshooting with packet capture?

- A. when capture packets are less than 16 MB
- B. when capture packets are restricted from the secondary memory
- C. when capture packets exceed 10 GB
- D. when capture packets exceed 32 MB

Answer: D

Explanation:

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

NEW QUESTION 192

- (Exam Topic 3)

Which command must be run to generate troubleshooting files on an FTD?

- A. system support view-files
- B. sudo sf_troubleshoot.pl
- C. system generate-troubleshoot all
- D. show tech-support

Answer: C

Explanation:

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

NEW QUESTION 194

- (Exam Topic 4)

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

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

Answer: AB

NEW QUESTION 195

- (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 200

- (Exam Topic 3)

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 201

- (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 203

- (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 207

- (Exam Topic 3)

Which CLI command is used to generate firewall debug messages on a Cisco Firepower?

- A. system support firewall-engine-debug
- B. system support ssl-debug
- C. system support platform
- D. system support dump-table

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212330-firepower- management-center-display-acc.html>

NEW QUESTION 208

- (Exam Topic 3)

Which command is entered in the Cisco FMC CLI to generate a troubleshooting file?

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

Answer: D

Explanation:

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

NEW QUESTION 209

- (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 213

- (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 215

- (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 217

- (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 221

- (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/Access.html>

NEW QUESTION 222

- (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 225

- (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 230

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 232

- (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/reuse.html> "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 234

- (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 239

- (Exam Topic 2)

A company has many Cisco FTD devices managed by a Cisco FMC. The security model requires that access control rule logs be collected for analysis. The security engineer is concerned that the Cisco FMC will not be able to process the volume of logging that will be generated. Which configuration addresses this concern?

- A. Send Cisco FTD connection events and security events directly to SIEM system for storage and analysis.
- B. Send Cisco FTD connection events and security events to a cluster of Cisco FMC devices for storage and analysis.
- C. Send Cisco FTD connection events and security events to Cisco FMC and configure it to forward logs to SIEM for storage and analysis.
- D. Send Cisco FTD connection events directly to a SIEM system and forward security events from Cisco FMC to the SIEM system for storage and analysis.

Answer: C

NEW QUESTION 241

- (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 243

- (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 245

- (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 247

- (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 248

- (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 250

- (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 255

- (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 257

- (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 262

- (Exam Topic 1)

An engineer is configuring a Cisco IPS to protect the network and wants to test a policy before deploying it. A copy of each incoming packet needs to be monitored while traffic flow remains constant. Which IPS mode should be implemented to meet these requirements?

- A. Inline tap
- B. passive
- C. transparent
- D. routed

Answer: A

NEW QUESTION 264

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 300-710 Exam with Our Prep Materials Via below:

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