

Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

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



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)

A user within an organization opened a malicious file on a workstation which in turn caused a ransomware attack on the network. What should be configured within the Cisco FMC to ensure the file is tested for viruses on a sandbox system?

- A. Capacity handling
- B. Local malware analysis
- C. Spere analysis
- D. Dynamic analysis

Answer: D

NEW QUESTION 3

- (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 4

- (Exam Topic 5)

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

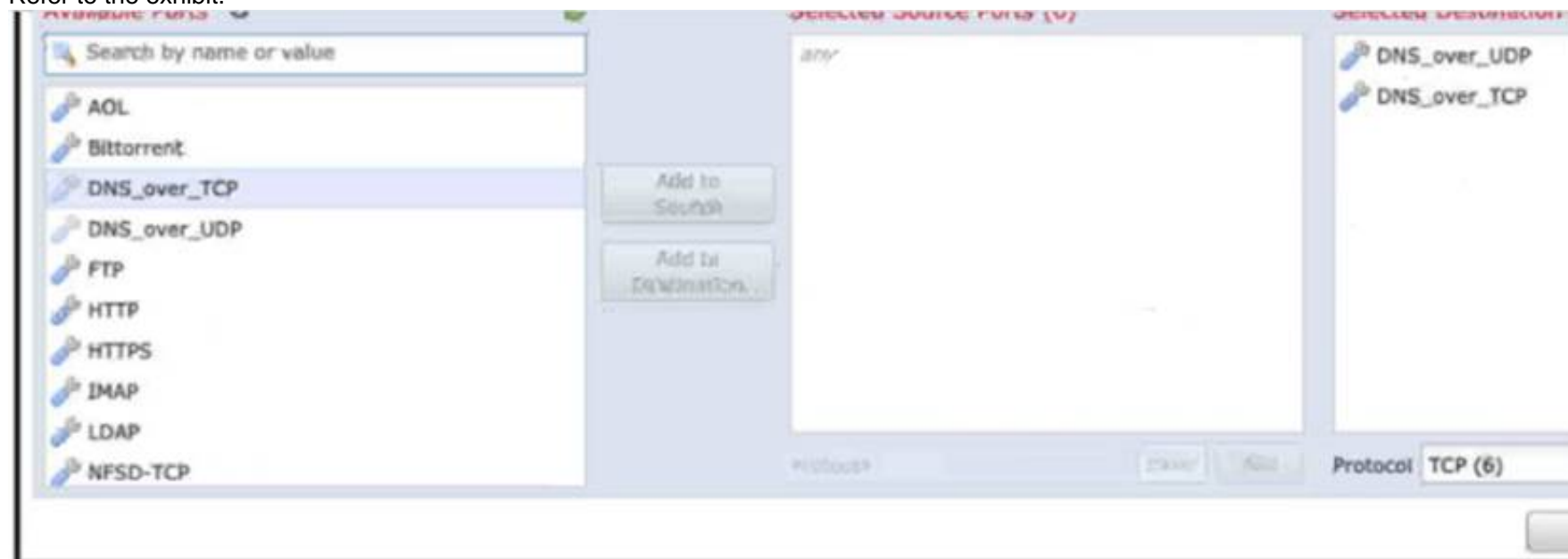
- A. A "show tech" file for the device in question.
- B. A "troubleshoot" file for the device in question.
- C. A "troubleshoot" file for the Cisco FMC.
- D. A "show tech" for the Cisco FMC.

Answer: B

NEW QUESTION 5

- (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 6

- (Exam Topic 5)

A VPN user is unable to connect to web resources behind the Cisco FTD device terminating the connection. While troubleshooting, the network administrator determines that the DNS responses are not getting through the Cisco FTD. What must be done to address this issue while still utilizing Snort IPS rules?

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

Answer: B

NEW QUESTION 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)

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)

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 10

- (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 15

- (Exam Topic 5)

A network administrator wants to block traffic to a known malware site at <https://www.badsite.com> and all subdomains while ensuring no packets from any internal client are sent to that site. Which type of policy must the network administrator use to accomplish this goal?

- A. Prefilter policy
- B. SSL policy
- C. DNS policy
- D. Access Control policy with URL filtering

Answer: D

NEW QUESTION 18

- (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 20

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 23

- (Exam Topic 5)

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 27

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 31

- (Exam Topic 5)

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

- A. The hairpinning feature is not available on FTD.
- B. Split tunneling is enabled for the Remote Access VPN on FTD
- C. FTD has no NAT policy that allows outside to outside communication
- D. The Enable Spoke to Spoke Connectivity through Hub option is not selected on FTD.

Answer: A

NEW QUESTION 33

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 35

- (Exam Topic 5)

An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down. What must be configured to accomplish this task?

- A. redundant interfaces on the firewall cluster mode and switches
- B. redundant interfaces on the firewall noncluster mode and switches
- C. vPC on the switches to the interface mode on the firewall duster
- D. vPC on the switches to the span EtherChannel on the firewall cluster

Answer: D

Explanation:

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKSEC-2020.pdf>

NEW QUESTION 40

- (Exam Topic 5)

A hospital network needs to upgrade their Cisco FMC managed devices and needs to ensure that a disaster recovery process is in place. What must be done in order to minimize downtime on the network?

- A. Configure a second circuit to an ISP for added redundancy
- B. Keep a copy of the current configuration to use as backup
- C. Configure the Cisco FMCs for failover
- D. Configure the Cisco FMC managed devices for clustering.

Answer: B

NEW QUESTION 42

- (Exam Topic 5)

While integrating Cisco Umbrella with Cisco Threat Response, a network security engineer wants to automatically push blocking of domains from the Cisco Threat Response interface to Cisco Umbrella. Which API meets this requirement?

- A. investigate
- B. reporting
- C. enforcement
- D. REST

Answer: D

NEW QUESTION 46

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 48

- (Exam Topic 5)

An engineer defines a new rule while configuring an Access Control Policy. After deploying the policy, the rule is not working as expected and the hit counters associated with the rule are showing zero. What is causing this error?

- A. Logging is not enabled for the rule.
- B. The rule was not enabled after being created.
- C. The wrong source interface for Snort was selected in the rule.
- D. An incorrect application signature was used in the rule.

Answer: B

NEW QUESTION 53

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

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

Answer: A

NEW QUESTION 59

- (Exam Topic 5)

An engineer is investigating connectivity problems on Cisco Firepower that is using service group tags.

Specific devices are not being tagged correctly, which is preventing clients from using the proper policies when going through the firewall How is this issue resolved?

- A. Use traceroute with advanced options.
- B. Use Wireshark with an IP subnet filter.
- C. Use a packet capture with match criteria.
- D. Use a packet sniffer with correct filtering

Answer: C

NEW QUESTION 60

- (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 61

- (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 65

- (Exam Topic 5)

An engineer wants to perform a packet capture on the Cisco FTD to confirm that the host using IP address 192 168.100.100 has the MAC address of 0042 7734.103 to help troubleshoot a connectivity issue What is the correct tcpdump command syntax to ensure that the MAC address appears in the packet capture output?

- A. -nm src 192.168.100.100
- B. -ne src 192.168.100.100
- C. -w capture.pcap -s 1518 host 192.168.100.100 mac
- D. -w capture.pcap -s 1518 host 192.168.100.100 ether

Answer: B

Explanation:

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-de>

NEW QUESTION 66

- (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 70

- (Exam Topic 5)

An engineer currently has a Cisco FTD device registered to the Cisco FMC and is assigned the address of 10.10.50.12. The organization is upgrading the addressing schemes and there is a requirement to convert the addresses to a format that provides an adequate amount of addresses on the network What should the engineer do to ensure that the new addressing takes effect and can be used for the Cisco FTD to Cisco FMC connection?

- A. Delete and reregister the device to Cisco FMC
- B. Update the IP addresses from IPv4 to IPv6 without deleting the device from Cisco FMC
- C. Format and reregister the device to Cisco FMC.
- D. Cisco FMC does not support devices that use IPv4 IP addresses.

Answer: A

NEW QUESTION 71

- (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 74

- (Exam Topic 5)

What must be implemented on Cisco Firepower to allow multiple logical devices on a single physical device to have access to external hosts?

- A. Add at least two container instances from the same module.
- B. Set up a cluster control link between all logical devices
- C. Add one shared management interface on all logical devices.
- D. Define VLAN subinterfaces for each logical device.

Answer: C

NEW QUESTION 77

- (Exam Topic 5)

A network administrator is deploying a Cisco IPS appliance and needs it to operate initially without affecting traffic flows.

It must also collect data to provide a baseline of unwanted traffic before being reconfigured to drop it. Which Cisco IPS mode meets these requirements?

- A. failsafe
- B. inline tap
- C. promiscuous
- D. bypass

Answer: B

NEW QUESTION 81

- (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 86

- (Exam Topic 5)

An engineer must deploy a Cisco FTD appliance via Cisco FMC to span a network segment to detect malware and threats. When setting the Cisco FTD interface mode, which sequence of actions meets this requirement?

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

Answer: A

NEW QUESTION 90

- (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 91

- (Exam Topic 5)

An organization recently implemented a transparent Cisco FTD in their network. They must ensure that the device does not respond to insecure SSL/TLS protocols. Which action accomplishes the task?

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

Answer: B

NEW QUESTION 96

- (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 98

- (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 99

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 103

- (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 105

- (Exam Topic 5)

With Cisco FTD software, which interface mode must be configured to passively receive traffic that passes through the appliance?

- A. ERSPAN
- B. IPS-only
- C. firewall
- D. tap

Answer: A

NEW QUESTION 106

- (Exam Topic 5)

Refer to the exhibit.

```
Phase: 16
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Firewall: starting rule matching, zone 4 => 1, geo 0 => 0, vlan 0, sgt 0, src sgt type 0, dest_sgt_tag 0, dest sgt type 0, username 'No Authentication Required', , icmpType 8, icmpCode 0
Firewall: block rule, 'Ping', drop
Snort: processed decoder alerts or actions queue, drop
Snort id 0, NMAP 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 0x00055e208f8b7e0 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 110

- (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/security/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 114

- (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 119

- (Exam Topic 5)

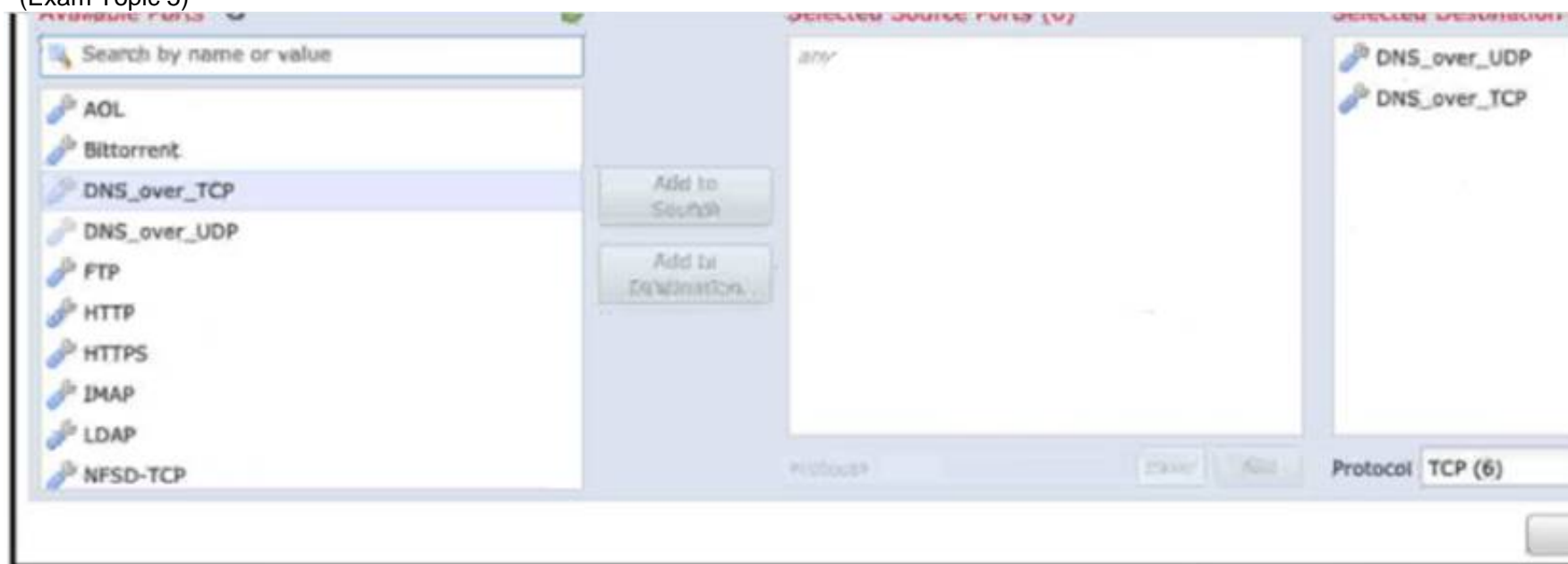
An engineer is implementing Cisco FTD in the network and is determining which Firepower mode to use. The organization needs to have multiple virtual Firepower devices working separately inside of the FTD appliance to provide traffic segmentation. Which deployment mode should be configured in the Cisco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

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

Answer: D

NEW QUESTION 121

- (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 through the firewall After making the change and deploying the policy they see that DNS traffic is not being 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 125

- (Exam Topic 5)

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

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

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

Answer: B

NEW QUESTION 126

- (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 129

- (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 130

- (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 131

- (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 132

- (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 135

- (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 138

- (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 139

- (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 141

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 144

- (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 146

- (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 147

- (Exam Topic 5)

A security engineer is deploying a pair of primary and secondary Cisco FMC devices. The secondary must also receive updates from Cisco Talos. Which action achieves this goal?

- A. Force failover for the secondary Cisco FMC to synchronize the rule updates from the primary.
- B. Configure the secondary Cisco FMC so that it receives updates from Cisco Talos.
- C. Manually import rule updates onto the secondary Cisco FMC device.
- D. Configure the primary Cisco FMC so that the rules are updated.

Answer: D

NEW QUESTION 151

- (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 155

- (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-remediate.html>

NEW QUESTION 159

- (Exam Topic 4)

Which action should you take when Cisco Threat Response notifies you that AMP has identified a file as malware?

- A. Add the malicious file to the block list.
- B. Send a snapshot to Cisco for technical support.
- C. Forward the result of the investigation to an external threat-analysis engine.
- D. Wait for Cisco Threat Response to automatically block the malware.

Answer: A

NEW QUESTION 161

- (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 163

- (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 167

- (Exam Topic 5)

An engineer must define a URL object on Cisco FMC. What is the correct method to specify the URL without performing SSL inspection?

- A. Use Subject Common Name value.
- B. Specify all subdomains in the object group.
- C. Specify the protocol in the object.
- D. Include all URLs from CRL Distribution Points.

Answer: B

NEW QUESTION 170

- (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/piresight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-External-Responses.pdf>

NEW QUESTION 172

- (Exam Topic 3)

What is the benefit of selecting the trace option for packet capture?

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

Answer: A

NEW QUESTION 174

- (Exam Topic 3)

What is a functionality of port objects in Cisco FMC?

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

Answer: B

Explanation:

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

NEW QUESTION 178

- (Exam Topic 3)

Which command should be used on the Cisco FTD CLI to capture all the packets that hit an interface?

- A. configure coredump packet-engine enable
- B. capture-traffic
- C. capture
- D. capture WORD

Answer: C

Explanation:

Reason: the command "capture-traffic" is used for SNORT Engine Captures. To capture a LINA Engine Capture, you use the "capture" command. Since the Lina Engine represents the actual physical interface of the device, "capture" is the only reasonable choice Reference:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-de>

The command is firepower# capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100 firepower# capture INSIDE interface inside trace detail match ip host 192.168.76.14 host 192.168.75.14

NEW QUESTION 180

- (Exam Topic 4)

In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

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

Answer: A

NEW QUESTION 185

- (Exam Topic 4)

Which Cisco Advanced Malware Protection for Endpoints policy is used only for monitoring endpoint actively?

- A. Windows domain controller
- B. audit
- C. triage
- D. protection

Answer: B

Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214933-amp-for-endpoints-deployment-methodology.html>

NEW QUESTION 187

- (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 190

- (Exam Topic 3)

Which CLI command is used to control special handling of ClientHello messages?

- A. system support ssl-client-hello-tuning
- B. system support ssl-client-hello-display
- C. system support ssl-client-hello-force-reset
- D. system support ssl-client-hello-enabled

Answer: A

NEW QUESTION 194

- (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 197

- (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 200

- (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 201

- (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 206

- (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-v601_chapter_01100011.html#ID-2101-0000000e

NEW QUESTION 207

- (Exam Topic 2)

An administrator is creating interface objects to better segment their network but is having trouble adding interfaces to the objects. What is the reason for this

failure?

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

Answer: D

Explanation:

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

NEW QUESTION 211

- (Exam Topic 2)

What is the disadvantage of setting up a site-to-site VPN in a clustered-units environment?

- A. VPN connections can be re-established only if the failed master unit recovers.
- B. Smart License is required to maintain VPN connections simultaneously across all cluster units.
- C. VPN connections must be re-established when a new master unit is elected.
- D. Only established VPN connections are maintained when a new master unit is elected.

Answer: C

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept_g32_yml_y2b

NEW QUESTION 216

- (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 217

- (Exam Topic 1)

What is a result of enabling Cisco FTD clustering?

- A. For the dynamic routing feature, if the master unit fails, the newly elected master unit maintains all existing connections.
- B. Integrated Routing and Bridging is supported on the master unit.
- C. Site-to-site VPN functionality is limited to the master unit, and all VPN connections are dropped if the master unit fails.
- D. All Firepower appliances can support Cisco FTD clustering.

Answer: C

Explanation:

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

NEW QUESTION 218

- (Exam Topic 2)

Which Firepower feature allows users to configure bridges in routed mode and enables devices to perform Layer 2 switching between interfaces?

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

Answer: D

Explanation:

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

NEW QUESTION 221

- (Exam Topic 2)

Which command is run on an FTD unit to associate the unit to an FMC manager that is at IP address 10.0.0.10, and that has the registration key Cisco123?

- A. configure manager local 10.0.0.10 Cisco123
- B. configure manager add Cisco123 10.0.0.10

- C. configure manager local Cisco123 10.0.0.10
- D. configure manager add 10.0.0.10 Cisco123

Answer: D

Explanation:

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

NEW QUESTION 223

- (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 227

- (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 228

- (Exam Topic 1)

An engineer is tasked with deploying an internal perimeter firewall that will support multiple DMZs Each DMZ has a unique private IP subnet range. How is this requirement satisfied?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 233

- (Exam Topic 1)

Which protocol establishes network redundancy in a switched Firepower device deployment?

- A. STP
- B. HSRP
- C. GLBP
- D. VRRP

Answer: A

Explanation:

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

NEW QUESTION 237

- (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 239

- (Exam Topic 1)

Which two dynamic routing protocols are supported in Firepower Threat Defense without using FlexConfig? (Choose two.)

- A. EIGRP
- B. OSPF
- C. static routing
- D. IS-IS
- E. BGP

Answer: BE

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-routing.html>

NEW QUESTION 243

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

300-710 Practice Exam Features:

- * 300-710 Questions and Answers Updated Frequently
- * 300-710 Practice Questions Verified by Expert Senior Certified Staff
- * 300-710 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 300-710 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year