

Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

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



NEW QUESTION 1

On the advanced tab under inline set properties, which allows interfaces to emulate a passive interface?

- A. transparent inline mode
- B. TAP mode
- C. strict TCP enforcement
- D. propagate link state

Answer: D

NEW QUESTION 2

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: D

NEW QUESTION 3

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

- A. inline set
- B. passive
- C. routed
- D. inline tap

Answer: B

NEW QUESTION 4

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 5

Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)

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

Answer: BD

NEW QUESTION 6

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

NEW QUESTION 7

Which two statements about bridge-group interfaces in Cisco FTD are true? (Choose two.)

- A. The BVI IP address must be in a separate subnet from the connected network.
- B. Bridge groups are supported in both transparent and routed firewall modes.
- C. Bridge groups are supported only in transparent firewall mode.
- D. Bidirectional Forwarding Detection echo packets are allowed through the FTD when using bridge-group members.
- E. Each directly connected network must be on the same subnet.

Answer: CD

NEW QUESTION 8

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

NEW QUESTION 9

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

NEW QUESTION 10

Which Cisco Firepower rule action displays an HTTP warning page?

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

Answer: C

NEW QUESTION 10

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

NEW QUESTION 11

In which two places can thresholding settings be configured? (Choose two.)

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

Answer: AC

NEW QUESTION 12

Which two types of objects are reusable and supported by Cisco FMC? (Choose two.)

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

Answer: BC

NEW QUESTION 13

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

NEW QUESTION 16

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

NEW QUESTION 17

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: B

NEW QUESTION 22

Which Cisco Firepower feature is used to reduce the number of events received in a period of time?

- A. rate-limiting
- B. suspending
- C. correlation
- D. thresholding

Answer: D

NEW QUESTION 26

DRAG DROP

Drag and drop the steps to restore an automatic device registration failure on the standby Cisco FMC from the left into the correct order on the right. Not all options are used.

Select and Place:

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 31

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

NEW QUESTION 35

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

NEW QUESTION 38

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

NEW QUESTION 39

What is a behavior of a Cisco FMC database purge?

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

Answer: C

NEW QUESTION 42

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

NEW QUESTION 45

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 47

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 50

.....

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