

## Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

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



#### NEW QUESTION 1

Which two conditions are necessary for high availability to function between two Cisco FTD devices? (Choose two.)

- A. The units must be the same version
- B. Both devices can be part of a different group that must be in the same domain when configured within the FMC.
- C. The units must be different models if they are part of the same series.
- D. The units must be configured only for firewall routed mode.
- E. The units must be the same model.

**Answer:** AE

#### 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

Which object type supports object overrides?

- A. time range
- B. security group tag
- C. network object
- D. DNS server group

**Answer:** C

#### NEW QUESTION 4

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

#### NEW QUESTION 5

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 6

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 7

Which group within Cisco does the Threat Response team use for threat analysis and research?

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

**Answer:** D

#### NEW QUESTION 8

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 9

Which command-line mode is supported from the Cisco Firepower Management Center CLI?

- A. privileged
- B. user
- C. configuration
- D. admin

**Answer:** C

#### NEW QUESTION 10

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:** B

#### NEW QUESTION 10

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 12

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

#### NEW QUESTION 16

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

#### NEW QUESTION 20

Which two statements about deleting and re-adding a device to Cisco FMC are true? (Choose two.)

- A. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re-apply the policies after registration is completed.
- B. Before re-adding the device in Cisco FMC, you must add the manager back in the device.
- C. No option to delete and re-add a device is available in the Cisco FMC web interface.
- D. The Cisco FMC web interface prompts users to re-apply access control policies.
- E. No option to re-apply NAT and VPN policies during registration is available, so users need to re-apply the policies after registration is completed.

**Answer:** DE

#### NEW QUESTION 21

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 24

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 29

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 31

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

#### NEW QUESTION 32

What is a valid Cisco AMP file disposition?

- A. non-malicious
- B. malware
- C. known-good
- D. pristine

**Answer:** B

#### NEW QUESTION 33

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 37

.....

## 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