DUMPSQUEEN

Securing Networks with Cisco Firepower (300-710 SNCF)

Cisco 300-710

Version Demo

Total Demo Questions: 15

Total Premium Questions: 342

Buy Premium PDF

dumpsqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, New Update	148
Topic 2, Deployment	53
Topic 3, Configuration	47
Topic 4, Management and Troubleshooting	69
Topic 5, Integration	25
Total	342

QUESTION NO: 1

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: D E

QUESTION NO: 2

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. Current Sessions

B. Correlation Events

C. Current Status

D. Custom Analysis

ANSWER: B

QUESTION NO: 3

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

QUESTION NO: 4

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

A. Cisco ASA 5500 Series

B. Cisco FMC

C. Cisco AMP

D. Cisco Stealthwatch

E. Cisco ASR 7200 Series

ANSWER: C D

QUESTION NO: 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-cisco-firepow.html

QUESTION NO: 6

Which two routing options are valid with Cisco FTD? (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: A C

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

---

QUESTION NO: 7

A network engineer is configuring URL Filtering on Cisco FTD. Which two port requirements on the FMC must be validated to allow communication with the cloud service? (Choose two.)

A. outbound port TCP/443

B. inbound port TCP/80

C. outbound port TCP/8080

D. inbound port TCP/443

E. outbound port TCP/80

ANSWER: A E

Explanation:

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

---

QUESTION NO: 8

In which two places are thresholding settings 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: A C

Explanation:

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

---

QUESTION NO: 9

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

QUESTION NO: 10

In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.)

A. Traffic inspection is interrupted temporarily when configuration changes are deployed.

B. The system performs intrusion inspection followed by file inspection.

C. They 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: A C

Explanation:

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

---

QUESTION NO: 11

An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events are 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. Exclude load balancers and NAT devices.

B. Leave default networks.

C. Increase the number of entries on the NAT device.

D. Change the method to TCP/SYN.

ANSWER: A

Explanation:

Reference:

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

QUESTION NO: 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

Explanation:

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

QUESTION NO: 13

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. Spero analysis

B. capacity handling

C. local malware analysis

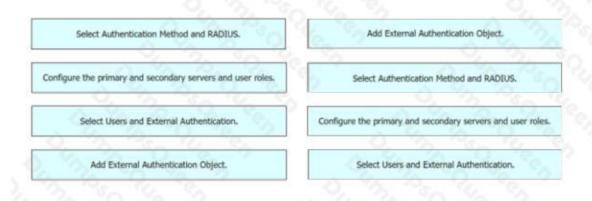**D.** dynamic analysis

ANSWER: D

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_policies_and_advanced_malware_protection.html#ID-2199-000005d8

QUESTION NO: 14 - (DRAG DROP)

Drag and drop the configuration steps from the left into the sequence on the right to enable external authentication on Cisco FMC to a RADIUS server.

Select Authentication Method and RADIUS.	step 1
Configure the primary and secondary servers and user roles.	step 2
Select Users and External Authentication.	step 3
Add External Authentication Object.	step 4

ANSWER:

Select Authentication Method and RADIUS.	Add External Authentication Object.
Configure the primary and secondary servers and user roles.	Select Authentication Method and RADIUS.
Select Users and External Authentication.	Configure the primary and secondary servers and user roles.
Add External Authentication Object.	Select Users and External Authentication.

Explanation:

4, 1, 2, 3

QUESTION NO: 15

Which two conditions must be met to enable high availability between two Cisco FTD devices? (Choose two.)

A. same flash memory size

B. same NTP configuration

C. same DHCP/PPoE configuration

D. same host name

E. same number of interfaces

ANSWER: B E