

DUMPS ARENA

Securing Networks with Cisco Firepower (300-710 SNCF)

Cisco 300-710

Version Demo

Total Demo Questions: 15

Total Premium Questions: 342

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

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 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.html>

QUESTION NO: 2

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**QUESTION NO: 3**

What are two features of bridge-group interfaces in Cisco FTD? (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: C D

Explanation:

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

QUESTION NO: 4

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: 5

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: A B

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>

QUESTION NO: 6

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**QUESTION NO: 7**

When a Cisco FTD device is configured in transparent firewall mode, on which two interface types can an IP address be configured? (Choose two.)

- A. Diagnostic
- B. EtherChannel
- C. BVI
- D. Physical
- E. Subinterface

ANSWER: A C**QUESTION NO: 8**

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. multi-instance
- B. multiple deployment
- C. single deployment

D. single-context

ANSWER: A

QUESTION NO: 9 - (DRAG DROP)

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:

Enter the "configure manager add" command at the CLI of the affected device.

Unregister the device from the standby Cisco FMC.

Register the affected device on the active Cisco FMC.

Enter the "configure manager delete" command at the CLI of the affected device.

Register the affected device on the standby Cisco FMC.

Unregister the device from the active Cisco FMC.

Step 1

Step 2

Step 3

Step 4

ANSWER:

Enter the "configure manager add" command at the CLI of the affected device.

Unregister the device from the active Cisco FMC.

Unregister the device from the standby Cisco FMC.

Enter the "configure manager delete" command at the CLI of the affected device.

Register the affected device on the active Cisco FMC.

Enter the "configure manager add" command at the CLI of the affected device.

Enter the "configure manager delete" command at the CLI of the affected device.

Register the affected device on the active Cisco FMC.

Register the affected device on the standby Cisco FMC.

Unregister the device from the active Cisco FMC.

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html#id_32288

QUESTION NO: 10

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: B E**Explanation:**

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

QUESTION NO: 11

A network administrator is configuring a Cisco AMP public cloud instance and wants to capture infections and polymorphic variants of a threat to help detect families of malware. Which detection engine meets this requirement?

- A. RBAC
- B. Tetra
- C. Ethos
- D. Spero

ANSWER: C**QUESTION NO: 12**

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**QUESTION NO: 13**

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 allow listing

ANSWER: A B**QUESTION NO: 14**

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

QUESTION NO: 15

A network administrator is implementing an active/passive high availability Cisco FTD pair. When adding the high availability pair, the administrator cannot select the secondary peer. What is the cause?

- A. The second Cisco FTD is not the same model as the primary Cisco FTD.
- B. An high availability license must be added to the Cisco FMC before adding the high availability pair.
- C. The failover link must be defined on each Cisco FTD before adding the high availability pair.
- D. Both Cisco FTD devices are not at the same software version.

ANSWER: A