300-710$^{\text{Q\&As}}$

Securing Networks with Cisco Firepower (SNCF)

Pass Cisco 300-710 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/300-710.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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.

Correct Answer: A

QUESTION 2

An engineer has been tasked with providing disaster recovery for an organization\\'s primary Cisco FMC. What must be done on the primary and secondary Cisco FMCs to ensure that a copy of the original corporate policy is available if the primary Cisco FMC fails?

A. Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device fails.

B. Connect the primary and secondary Cisco FMC devices with Category 6 cables of not more than 10 meters in length.

C. Configure high-availability in both the primary and secondary Cisco FMCs.

D. Place the active Cisco FMC device on the same trusted management network as the standby device.

Correct Answer: C

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

QUESTION 3

An administrator is attempting to remotely log into a switch in the data center using SSH and is unable to connect. How does the administrator confirm that traffic is reaching the firewall?

A. by performing a packet capture on the firewall

B. by attempting to access it from a different workstation

C. by running Wireshark on the administrator\\'s PC

D. by running a packet tracer on the firewall

Correct Answer: D

Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc16

QUESTION 4

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

Correct Answer: AB

QUESTION 5

Which interface type allows packets to be dropped?

A. passive

B. inline

C. ERSPAN

D. TAP

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring-firepower-threat-defense-int.html

QUESTION 6

A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface. What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

A. The output format option for the packet logs is unavailable.

B. Only the UDP packet type is supported.

C. The destination MAC address is optional if a VLAN ID value is entered.

D. The VLAN ID and destination MAC address are optional.

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guidev62/troubleshooting_the_system.html

QUESTION 7

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 y configured to provide visibility on the Cisco Firepower Dashboards?

A. Custom analysis.

B. Current Status

C. Current Sessions

D. Correlation Events

Correct Answer: D

QUESTION 8

Which report template field format is available in Cisco FMC?

A. box lever chart

B. arrow chart

C. bar chart

D. benchmark chart

Correct Answer: C

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

QUESTION 9

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

Correct Answer: D

Reference: https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits

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

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

---

QUESTION 11

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 register the device to Cisco FMC.

B. Update the IP addresses from IPV4 to IPV6 without deleting the device from cisco FMC.

C. Format and register the device to Cisco FMC.

D. Cisco FMC does not support devices that use IPv4 IP addresses.

Correct Answer: B

QUESTION 12

With Cisco Firepower Threat Defense software, which interface mode do you configure for an IPS deployment, where traffic passes through the appliance but does not require VLAN rewriting?

A. inline set

B. passive

C. inline tap

D. routed

E. transparent

Correct Answer: D

QUESTION 13

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.

Correct Answer: CD

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 14

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

Correct Answer: AB

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 15

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

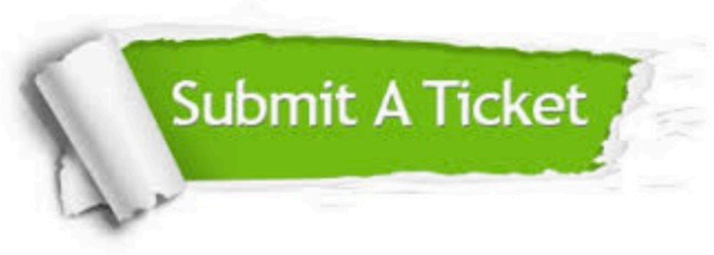
B. capacity handling

C. local malware analysis

D. dynamic analysis

Correct Answer: D

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



Submit A Ticket