300-710 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.pass2lead.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 Cisco Firepower rule action displays an HTTP warning page?

A. Monitor

B. Block

C. Interactive Block

D. Allow with Warning

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/AC-Rules-Tuning-Overview.html#76698

QUESTION 2

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.

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/Reports.html#87267

QUESTION 3

What is a result of enabling Cisco FTD clustering?

A. For the dynamic routing feature, if the master unit fails, the newly elected master unit maintains all existing connections.

B. Integrated Routing and Bridging is supported on the master unit.

C. Site-to-site VPN functionality is limited to the master unit, and all VPN connections are dropped if the master unit fails.

D. All Firepower appliances can support Cisco FTD clustering.

Correct Answer: C

"Remote access VPN is not supported with clustering. VPN functionality is limited to the control unit and does not take

advantage of the cluster high availability capabilities.

If the control unit fails, all existing VPN connections are lost, and VPN users will see a disruption in service. When a new control unit is elected, you must re-establish the VPN connections.

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/clustering_for_the_firepower_threat_defense.html

QUESTION 4

An engineer must deploy a Cisco FTD appliance via Cisco FMC to span a network segment to detect malware and threats. When setting the Cisco FTD interface mode, which sequence of actions meets this requirement?

A. Set to passive, and configure an access control policy with an intrusion policy and a file policy defined.

B. Set to passive, and configure an access control policy with a prefilter policy defined.

C. Set to none, and configure an access control policy with an intrusion policy and a file policy defined.

D. Set to none, and configure an access control policy with a prefilter policy defined.

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/fpmc-config-guide-v623_chapter_010000001.html

QUESTION 5

In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

A. unavailable

B. unknown

C. clean

D. disconnected

Correct Answer: A

Unavailable indicates that the system could not query the AMP cloud https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_malware_events_and_network_file_trajectory.html

QUESTION 6

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 7

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

Correct Answer: B

Click Advanced to set the following optional parameters:

CORRECT ANSWER (B) Tap Mode — Set to inline tap mode.

INCORRECT ANSWER Propagate Link State:

Link state propagation automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down. When the downed interface comes back up, the second interface automatically comes

back up, also. In other words, if the link state of one interface changes, the device senses the change and updates the link state of the other interface to match it. Note that devices require up to 4 seconds to propagate link state changes. Link

state propagation is especially useful in resilient network environments where routers are configured to reroute traffic automatically around network devices that are in a failure state.

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

QUESTION 8

An engineer is troubleshooting application failures through a FTD deployment. While using the FMC CLI, it has been determined that the traffic in question is not matching the desired policy. What should be done to correct this?

A. Use the system support firewall-engine-debug command to determine which rules the traffic matching and modify the rule accordingly.

B. Use the system support application-identification-debug command to determine which rules the traffic matching and modify the rule accordingly.

C. Use the system support firewall-engine-dump-user-f density-data command to change the policy and allow the application through the firewall.

D. Use the system support network-options command to fine tune the policy.

Correct Answer: A

QUESTION 9

The network administrator wants to enhance the network security posture by enabling machine learning tor malware detection due to a concern with suspicious Microsoft executable file types that were seen while creating monthly security reports for the CIO. Which feature must be enabled to accomplish this goal?

A. Spero

B. dynamic analysis

C. static analysis

D. Ethos

Correct Answer: A

QUESTION 10

A security engineer is configuring a remote Cisco FTD that has limited resources and internet bandwidth. Which malware action and protection option should be configured to reduce the requirement for cloud lookups?

A. Malware Cloud Lookup and dynamic analysis

B. Block Malware action and dynamic analysis

C. Block Malware action and local malware analysis

D. Block File action and local malware analysis

Correct Answer: C

QUESTION 11

A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire. How should this be implemented?

A. Specify the BVI IP address as the default gateway for connected devices.

B. Enable routing on the Cisco Firepower

C. Add an IP address to the physical Cisco Firepower interfaces.

D. Configure a bridge group in transparent mode.

Correct Answer: D

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place. Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.html

QUESTION 12

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. Multiple Deployment

B. single-context

C. Single deployment

D. multi-instance

Correct Answer: D

QUESTION 13

An analyst is reviewing the Cisco FMC reports for the week. They notice that some peer-to- peer applications are being used on the network and they must identify which poses the greatest risk to the environment. Which report gives the analyst this information?

A. Attacks Risk Report

B. User Risk Report

C. Network Risk Report

D. Advanced Malware Risk Report

Correct Answer: C

QUESTION 14

Which function is the primary function of Cisco AMP threat Grid?

A. It analyzes copies of packets from the packet flow

B. The device is deployed in a passive configuration

C. If a rule is triggered the device generates an intrusion event.

D. The packet flow traverses the device

E. If a rule is triggered the device drops the packet

Correct Answer: AC

QUESTION 15

With Cisco FTD integrated routing and bridging, which interface does the bridge group use to communicate with a routed interface?

A. subinterface

B. switch virtual

C. bridge virtual

D. bridge group member

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html