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.pass4itsure.com/300-710.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A network administrator discovers that a user connected to a file server and downloaded a malware file. The Cisco FMC generated an alert for the malware event, however the user still remained connected. Which Cisco AMP file rule action within the Cisco FMC must be set to resolve this issue?

A. Malware Cloud Lookup

B. Reset Connection

C. Detect Files

D. Local Malware Analysis

Correct Answer: B

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

QUESTION 2

A security engineer must integrate an external feed containing STIX/TAXII data with Cisco FMC. Which feature must be enabled on the Cisco FMC to support this connection?

A. Cisco Success Network

B. Cisco Secure Endpoint Integration

C. Threat Intelligence Director

D. Security Intelligence Feeds

Correct Answer: C

QUESTION 3

An engineer is setting up a new Firepower deployment and is looking at the default FMC policies to start the implementation. During the initial trial phase, the organization wants to test some common Snort rules while still allowing the majority of network traffic to pass. Which default policy should be used?

A. Balanced Security and Connectivity

B. Security Over Connectivity

C. Maximum Detection

D. Connectivity Over Security

Correct Answer: A

Balanced Security and Connectivity network analysis and intrusion policies

These policies are built for both speed and detection. Used together, they serve as a good starting point for most networks and deployment types. The system uses the Balanced Security and Connectivity network analysis policy as the default. https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdm-intrusion.html

QUESTION 4

An engineer is reviewing a ticket that requests to allow traffic for some devices that must connect to a server over 8699/udp. The request mentions only one IP address, 172.16.18.15, but the requestor asked for the engineer to open the port for all machines that have been trying to connect to it over the last week.

Which action must the engineer take to troubleshoot this issue?

A. Use the context explorer to see the application blocks by protocol.

B. Use the context explorer to see the destination port blocks

C. Filter the connection events by the source port 8699/udp.

D. Filter the connection events by the destination port 8699/udp.

Correct Answer: D

QUESTION 5

An organization has a compliance requirement to protect servers from clients, however, the clients and servers all reside on the same Layer 3 network. Without readdressing IP subnets for clients or servers, how is segmentation achieved?

A. Change the IP addresses of the servers, while remaining on the same subnet.

B. Deploy a firewall in routed mode between the clients and servers.

C. Change the IP addresses of the clients, while remaining on the same subnet.

D. Deploy a firewall in transparent mode between the clients and servers.

Correct Answer: B