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.geekcert.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

A network engineer is planning on replacing an Active/Standby pair of physical Cisco Secure Firewall ASAs with a pair of Cisco Secure Firewall Threat Defense Virtual appliances. Which two virtual environments support the current High Availability configuration? (Choose two.)

A. ESXi

B. Azure

C. Openstack

D. KVM

E. AWS

Correct Answer: AD

QUESTION 2

The security engineer reviews the syslog server events of an organization and sees many outbound connections to malicious sites initiated from hosts running Cisco Secure Endpoint. The hosts are on a separate network from the Cisco FTD device. Which action blocks the connections?

A. Modify the policy on Cisco Secure Endpoint to enable DFC.

B. Modify the access control policy on the Cisco FMC to block malicious outbound connections

C. Add the IP addresses of the malicious sites to the access control policy on the Cisco FMC

D. Add a Cisco Secure Endpoint policy with the Tetra and Spero engines enabled

Correct Answer: A

QUESTION 3

What is the difference between inline and inline tap on Cisco Firepower?

A. Inline tap mode can send a copy of the traffic to another device.

B. Inline tap mode does full packet capture.

C. Inline mode cannot do SSL decryption.

D. Inline mode can drop malicious traffic.

Correct Answer: D

INLINE TAP

Copies the data to the SNORT Engine to be checked but then dropped while the actual data flow continues

uninterrupted. Therefore, INLINE TAP does not send traffic to another device.

The Data is copied but not captured. You still would need to enable packet capture to capture packets (AKA Save PCAP).

INLINE:

Both inline and Inline Tap mode do not support SSL Decryption-resign... Although im a bit conflicted by this....

Truth is that Inline Mode can DROP malicious traffic but remember that Inline TAP mode CANNOT. Agan this is because tap mode sends a copy of the data to be inspected but not the actual data.

QUESTION 4

Which default action setting in a Cisco FTD Access Control Policy allows all traffic from an undefined application to pass without Snort Inspection?

A. Trust All Traffic

B. Inherit from Base Policy

C. Network Discovery Only

D. Intrusion Prevention

Correct Answer: A

The default action setting in a Cisco FTD Access Control Policy determines how the system handles and logs traffic that is not handled by any other access control configuration. The default action can block or trust all traffic without further inspection, or inspect traffic for intrusions and discovery data3. The Trust All Traffic option allows all traffic from an undefined application to pass without Snort inspection. This option also disables Security Intelligence filtering, file and malware inspection, and URL filtering for all traffic handled by the default action. This option is useful when you want to minimize the performance impact of access control on your network3. The other options are incorrect because: The Inherit from Base Policy option inherits the default action setting from the base policy. The base policy is the predefined access control policy that you use as a starting point for creating your own policies. Depending on which base policy you choose, the inherited default action setting can be different3. The Network Discovery Only option inspects all traffic for discovery data only. This option enables Security Intelligence filtering for all traffic handled by the default action, but disables file and malware inspection, URL filtering, and intrusion inspection. This option is useful when you want to collect information about your network before you configure access control rules3. The Intrusion Prevention option inspects all traffic for intrusions and discovery data. This option enables Security Intelligence filtering, file and malware inspection, URL filtering, and intrusion inspection for all traffic handled by the default action. This option provides the most comprehensive protection for your network, but also has the most performance impact3.

QUESTION 5

An engineer is troubleshooting connectivity to the DNS servers from hosts behind a new Cisco FTD device. The hosts cannot send DNS queries to servers in the DMZ. Which action should the engineer take to troubleshoot this issue using the real DNS packets?

A. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion policy as needed

B. Use the Connection Events dashboard to check the block reason and adjust the inspection policy as needed

C. Use the packet tracer tool to determine at which hop the packet is being dropped

D. Use the show blocks command in the Threat Defense CLI tool and create a policy to allow the blocked traffic

Correct Answer: A