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

QUESTION 1

A company has many Cisco FTD devices managed by a Cisco FMC. The security model requires that access control rule logs be collected for analysis. The security engineer is concerned that the Cisco FMC will not be able to process the volume of logging that will be generated. Which configuration addresses concern this?

A. Send Cisco FTD connection events directly to a SIEM system and forward security events from Cisco FMC to the SIEM system for storage and analysis

B. Send Cisco FTD connection events and security events directly to SIEM system for storage and analysis

C. Send Cisco FTD connection events and security events to a cluster of Cisco FMC devices for storage and analysis

D. Send Cisco FTD connection events and security events to Cisco FMC and configure it to forward logs to SIEM for storage and analysis

Correct Answer: D

QUESTION 2

There is an increased amount of traffic on the network and for compliance reasons, management needs visibility into the encrypted traffic. What is a result of enabling TLS/SSL decryption to allow this visibility?

A. It prompts the need for a corporate managed certificate.

B. It will fail if certificate pinning is not enforced.

C. It has minimal performance impact.

D. It is not subject to any Privacy regulations.

Correct Answer: A

QUESTION 3

An engineer is configuring a custom application detector for HTTP traffic and wants to import a file that was provided by a third party. Which type of flies are advanced application detectors creates and uploaded as?

A. Perl script

B. NBAR protocol

C. LUA script

D. Python program

Correct Answer: C

A custom application detector is a user-defined script that can detect web applications, clients, and application protocols

based on patterns in network traffic. Custom application detectors are written in LUA, which is a lightweight and

embeddable scripting language. LUA scripts can use predefined functions and variables provided by the Firepower System to access packet data and metadata, and to specify the detection criteria and the application information1.

To import a custom application detector file that was provided by a third party, you need to follow these steps1:

In the FMC web interface, navigate to Objects > Object Management > Application Detectors.

Click Import.

Browse to the location of the LUA script file and select it.

Click Upload.

Review the detector details and click Save.

The other options are incorrect because:

Perl script is not a supported format for custom application detectors. Perl is a general-purpose programming language that is not embedded in the Firepower System. NBAR protocol is not a file type, but a feature of Cisco IOS routers that

can classify and monitor network traffic based on application types. NBAR protocols are predefined and cannot be imported as custom application detectors. Python program is not a supported format for custom application detectors. Python

is a general-purpose programming language that is not embedded in the Firepower System.

QUESTION 4

An administrator is working on a migration from Cisco ASA to the Cisco FTD appliance and needs to test the rules without disrupting the traffic. Which policy type should be used to configure the ASA rules during this phase of the migration?

A. Prefilter

B. Intrusion

C. Access Control

D. Identity

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_01011.html

---

QUESTION 5

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-guide-v62/troubleshooting_the_system.html