Vendor: Cisco

Exam Code:300-710

Exam Name: Securing Networks with Cisco Firepower (SNCF)

Version: Demo

QUESTION 1

An engineer runs the command restore remote-manager-backup location 2.2.2.2 admin /Volume/home/admin FTD408566513.zip on a Cisco FMC. After connecting to the repository, the Cisco FTD device is unable to accept the backup file. What is the reason for this failure?

A. The backup file is not in .cfg format.

B. The wrong IP address is used.

C. The backup file extension was changed from .tar to .zip.

D. The directory location is incorrect.

Correct Answer: C

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC- 3455.pdf

---

QUESTION 2

A security engineer found a suspicious file from an employee email address and is trying to upload it for analysis, however the upload is failing. The last registration status is still active. What is the cause for this issue?

A. Cisco AMP for Networks is unable to contact Cisco Threat Grid on premise.

B. Cisco AMP for Networks is unable to contact Cisco Threat Grid Cloud.

C. There is a host limit set.

D. The user agent status is set to monitor.

Correct Answer: A

QUESTION 3

An engineer wants to connect a single IP subnet through a Cisco FTD firewall and enforce policy. There is a requirement to present the internal IP subnet to the outside as a different IP address. What must be configured to meet these requirements?

A. Configure the downstream router to perform NAT.

B. Configure the upstream router to perform NAT.

C. Configure the Cisco FTD firewall in routed mode with NAT enabled.

D. Configure the Cisco FTD firewall in transparent mode with NAT enabled.

Correct Answer: C

QUESTION 4

What is the advantage of having Cisco Firepower devices send events to Cisco Threat Response via the security services exchange portal directly as opposed to using syslog?

A. Firepower devices do not need to be connected to the Internet.

B. An on-premises proxy server does not need to set up and maintained.

C. All types of Firepower devices are supported.

D. Supports all devices that are running supported versions of Firepower

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower_and_Cisco_Threat_Response_Integration_Guide.pdf

---

QUESTION 5

In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.)

A. Traffic inspection is interrupted temporarily when configuration changes are deployed.

B. The system performs intrusion inspection followed by file inspection.

C. They block traffic based on Security Intelligence data.

D. File policies use an associated variable set to perform intrusion prevention.

E. The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters.

Correct Answer: AC

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

---

QUESTION 6

Which Cisco Firepower feature is used to reduce the number of events received in a period of time?

A. rate-limiting

B. suspending

C. correlation

D. thresholding

Correct Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Global-Threshold.html

---

QUESTION 7

Which two routing options are valid with Cisco Firepower Threat Defense? (Choose two.)

A. BGPv6

B. ECMP with up to three equal cost paths across multiple interfaces

C. ECMP with up to three equal cost paths across a single interface

D. BGPv4 in transparent firewall mode

E. BGPv4 with nonstop forwarding

Correct Answer: CE

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

---

QUESTION 8

What is a feature of Cisco AMP private cloud?

A. It disables direct connections to the public cloud.

B. It supports security intelligence filtering.

C. It support anonymized retrieval of threat intelligence.

D. It performs dynamic analysis.

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/products/collateral/security/fireamp-private-cloud-virtual-appliance/datasheet-c78-742267.html

---

QUESTION 9

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 10

An engineer is building a new access control policy using Cisco FMC. The policy must inspect a unique IPS policy as well as log rule matching. Which action must be taken to meet these requirements?

A. Configure an IPS policy and enable per-rule logging.

B. Disable the default IPS policy and enable global logging.

C. Configure an IPS policy and enable global logging.

D. Disable the default IPS policy and enable per-rule logging.

Correct Answer: C

There is no per-rule logging on the system. Also there would be no need to log the ACL rule as an Intrusion event will cause the rule to generate an event.

QUESTION 11

A company is deploying intrusion protection on multiple Cisco FTD appliances managed by Cisco FMC. Which system-provided policy must be selected if speed and detection are priorities?

A. Maximum Detection

B. Connectivity Over Security

C. Security Over Connectivity

D. Balanced Security and Connectivity

Correct Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/overview_of_network_analysis_and_intrusion_policies.html#ID-2247-00000144

QUESTION 12

An administrator is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of NAT001 and a password of Cisco0123456789. The private IP address of the FMC server is 192.168.45.45, which is being translated to the public IP address of 209.165.200.225/27. Which command set must be used in order to accomplish this task?

A. configure manager add 209.165.200.225 255.255.255.224

B. configure manager add 209.165.200.225

C. configure manager add 209.165.200.225/27

D. configure manager add 192.168.45.45

Correct Answer: B