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.leads4pass.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

An engineer needs to configure remote storage on Cisco FMC. Configuration backups must be available from a secure location on the network for disaster recovery. Reports need to back up to a shared location that auditors can access with their Active Directory logins. Which strategy must the engineer use to meet these objectives?

A. Use SMB for backups and NFS for reports.

B. Use NFS for both backups and reports.

C. Use SMB for both backups and reports.

D. Use SSH for backups and NFS for reports.

Correct Answer: C

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/system_configuration.html#ID-2241-00000551 "You cannot send backups to one remote system and reports to another, but you can choose to send either to a remote system and store the other on the Firepower Management Center."

QUESTION 2

What is a limitation to consider when running a dynamic routing protocol on a Cisco FTD device in IRB mode?

A. Only link-stale routing protocols are supported.

B. Only distance vector routing protocols are supported.

C. Only EtherChannel interfaces are supposed.

D. Only nonbridge interfaces are supported.

Correct Answer: D

Integrated routing and bridging (IRB) is a feature that allows you to route between different bridge groups on a Cisco FTD device. A bridge group is a logical interface that acts as a container for one or more physical or logical interfaces that belong to the same layer 2 broadcast domain. You can assign an IP address to a bridge group interface (BVI) and enable routing protocols on it, just like a regular routed interface. However, when you run a dynamic routing protocol on a Cisco FTD device in IRB mode, you can only use nonbridge interfaces as routing peers. You cannot use bridge group interfaces or bridge group member interfaces as routing peers2. This is because the routing protocol packets are sent and received on the nonbridge interfaces, and the bridge group interfaces are used only for forwarding data traffic3.

QUESTION 3

A network administrator is deploying a Cisco IPS appliance and needs it to operate initially without affecting traffic flows. It must also collect data to provide a baseline of unwanted traffic before being reconfigured to drop it. Which Cisco IPS mode meets these requirements?

A. failsafe

B. inline tap

C. promiscuous

D. bypass

Correct Answer: B

QUESTION 4

Which two types of objects are reusable and supported by Cisco FMC? (Choose two.)

A. dynamic key mapping objects that help link HTTP and HTTPS GET requests to Layer 7 application protocols.

B. reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists

C. network-based objects that represent IP address and networks, port/protocols pairs, VLAN tags, security zones, and origin/destination country

D. network-based objects that represent FQDN mappings and networks, port/protocol pairs, VXLAN tags, security zones and origin/destination country

E. reputation-based objects, such as URL categories

Correct Answer: BC

SI feeds/lists and basic network objects are two common use cases for objects. Answer "A" is dynamic so you probably wouldn\\'t use a reusable object, same with answer "D". In E - you can store URLs in objects but not categories,

Reference:

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/730/management-center-device-config-73/objects-object-mgmt.html#ID-2243-0000045f https://www.cisco.com/c/en/us/td/docs/security/

firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-00000414

QUESTION 5

How many report templates does the Cisco Firepower Management Center support?

A. 20

B. 10

C. 5

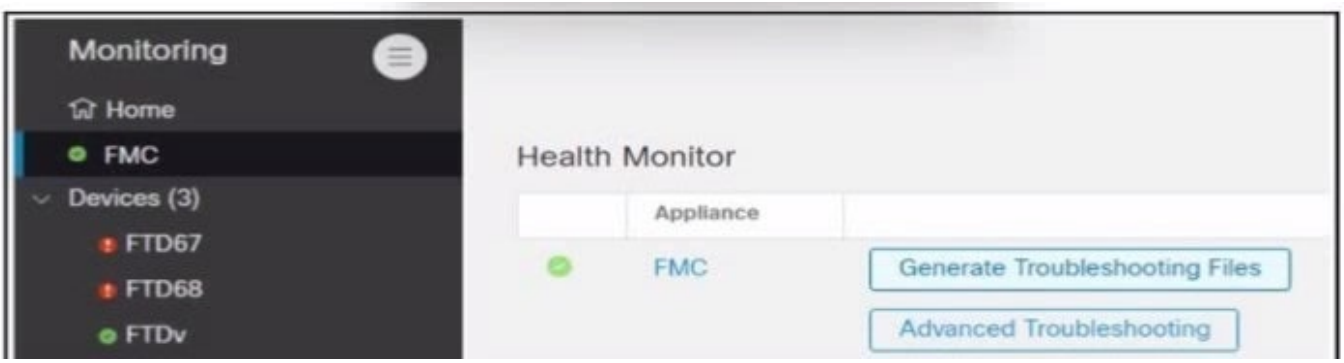
D. unlimited

Correct Answer: D

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

QUESTION 6

Refer to the exhibit.



An engineer generates troubleshooting files in Cisco Secure Firewall Management Center (FMC).

A successfully completed task Is removed before the files are downloaded.

Which two actions must be taken to determine the filename and obtain the generated troubleshooting files without regenerating them? (Choose two.)

A. Use an FTP client Hi expert mode on Secure FMC lo upload the files to the FTP server.

B. Go to the same screen as shown in the exhibit, click Advanced Troubleshooting, enter the rile name, and then start the download

C. Connect to CU on the FTD67 and FTD66 devices and copy the tiles from flash to the PIP server.

D. Go to expert mode on Secure FMC. list the contents of/Var/common, and determine the correct filename from the output

E. Click System Monitoring, men Audit to determine the correct filename from the line containing the Generate Troubleshooting Files string.

Correct Answer: DE

If a task to generate troubleshooting files in Cisco Secure Firewall Management Center (FMC) is completed successfully but removed before the files are downloaded, the following steps can be taken to determine the filename and obtain the

generated troubleshooting files without regenerating them:

Go to expert mode on Secure FMC:

Use the System Monitoring Audit logs:

These actions help identify and retrieve the generated troubleshooting files without the need to regenerate them, saving time and resources. References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on

Troubleshooting and File Management.

QUESTION 7

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

QUESTION 8

Which two dynamic routing protocols are supported in Cisco FTD without using FlexConfig? (Choose two.)

A. EIGRP

B. OSPF

C. static routing

D. IS-IS

E. BGP

Correct Answer: BE

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-routing.html

QUESTION 9

Refer to the exhibit.

What is the effect of the existing Cisco FMC configuration?

A. The remote management port for communication between the Cisco FMC and the managed device changes to port 8443.

B. The managed device is deleted from the Cisco FMC.

C. The SSL-encrypted communication channel between the Cisco FMC and the managed device becomes plain-text communication channel.

D. The management connection between the Cisco FMC and the Cisco FTD is disabled.

Correct Answer: D

QUESTION 10

An engineer currently has a Cisco FTD device registered to the Cisco FMC and is assigned the address of 10.10.50.12. The organization is upgrading the addressing schemes and there is a requirement to convert the addresses to a format

that provides an adequate amount of addresses on the network.

What should the engineer do to ensure that the new addressing takes effect and can be used for the Cisco FTD to Cisco FMC connection?

A. Delete and register the device to Cisco FMC.

B. Update the IP addresses from IPV4 to IPV6 without deleting the device from cisco FMC.

C. Format and register the device to Cisco FMC.

D. Cisco FMC does not support devices that use IPv4 IP addresses.

Correct Answer: A

QUESTION 11

A network administrator is seeing an unknown verdict for a file detected by Cisco FTD. Which malware policy configuration option must be selected in order to further analyze the file in the Talos cloud?

A. malware analysis

B. dynamic analysis

C. sandbox analysis

D. Spero analysis

Correct Answer: B

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

QUESTION 12

Cisco SecureX is classified as which type of threat detection and response solution?

A. MDR

B. EDR

C. XDR

D. NDR

Correct Answer: C

QUESTION 13

With Cisco Firepower Threat Defense software, which interface mode must be configured to passively receive traffic that passes through the appliance?

A. inline set

B. passive

C. routed

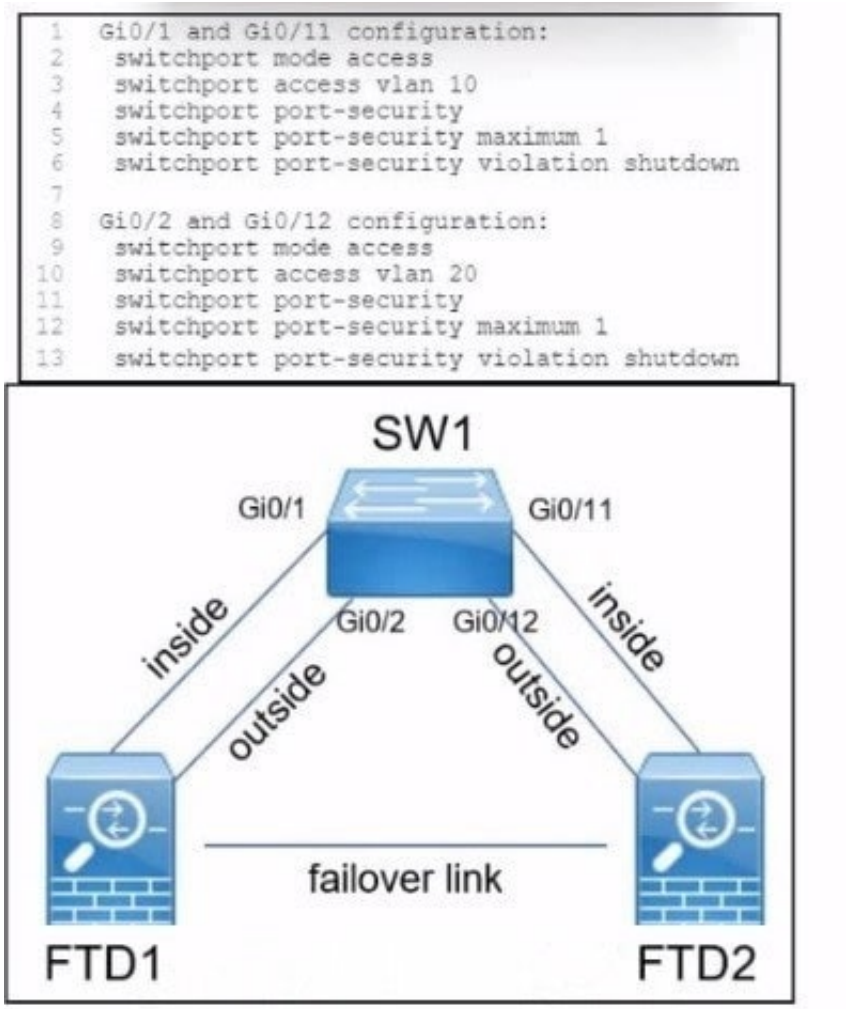
D. inline tap

Correct Answer: B

In Cisco Firepower Threat Defense (FTD) software, the "passive" interface mode must be configured to passively receive traffic that passes through the appliance. When set to passive mode, the interface listens to the network traffic but does not actively participate in the network; it does not transmit any packets. This configuration is typically used for monitoring and logging purposes without impacting the flow of traffic.

QUESTION 14

Refer to the exhibit.



A company is deploying a pair of Cisco Secure Firewall Threat defence devices named FTD1 and FTD2. FTD1 and FTD2 have been configured as an active/standby pair with a failover link but without a stateful link.

What must be implemented next to ensure that users on the internal network still communicate with outside devices if FTD1 fails?

A. Disable port security on the switch interfaces connected to FTD1 and FTD2.

B. Set maximum secured addresses to two on the switch interfaces on FTD1 and FTD2.

C. Connect and configure a stateful link and thon deploy the changes.

D. Configure the spanning-tree PortFasl feature on SW1 and FTD2

Correct Answer: C

In a failover configuration with Cisco Secure Firewall Threat Defense (FTD) devices, ensuring that users on the internal network can continue to communicate with outside devices if the primary device (FTD1) fails requires the implementation

of a stateful failover link. The stateful failover link allows the secondary device (FTD2) to maintain session information and state data, ensuring seamless failover and minimizing disruptions.

Steps to implement a stateful failover link:

Physically connect a stateful failover link between FTD1 and FTD2.

Configure the stateful failover link in the FMC.

Ensure that both devices are properly synchronized and that stateful failover is enabled.

Deploy the changes to both FTD devices.

By configuring a stateful link, the secondary FTD can take over active sessions without requiring users to re-establish their connections, thus ensuring continuous communication. References: Cisco Secure Firewall Threat Defense

Configuration Guide, Chapter on Failover Configuration.

QUESTION 15

An administrator is configuring the interface of a Cisco Secure Firewall Threat Defense firewall device in a passive IPS deployment. The device and interface have been identified. Which set of configuration steps must the administrator perform next to complete the implementation?

A. Set the interface mode to passive. Associate the interface with a security zone. Enable the interface. Set the MTU parameter.

B. Modify the interface to retransmit received traffic. Associate the interface with a security zone Set the MTU parameter

C. Set the interface mode to passive. Associate the interface with a security zone. Set the MTU parameter. Reset the interface.

D. Modify the interface to retransmit received traffic. Associate the interface with a security zone. Enable the interface. Set the MTU parameter.

Correct Answer: A

In a passive IPS deployment for a Cisco Secure Firewall Threat Defense (FTD) device, the administrator must configure the interface to operate in passive mode. This involves setting the interface mode, associating it with a security zone,

enabling the interface, and setting the MTU parameter.

Steps:

Set the interface mode to passive:

Associate the interface with a security zone:

Enable the interface:

Set the MTU parameter:

This ensures that the FTD device can inspect traffic passively without impacting the network flow.

References: Cisco Secure Firewall Management Center Device Configuration Guide, Chapter on Interface Settings