
**Vendor:**Cisco

**Exam Code:**300-710

**Exam Name:**Securing Networks with Cisco Firepower (SNCF)

**Version:**Demo

**QUESTION 1**

Refer to the exhibit.

```
     6: 15:46:24.605132 192.168.40.11.65830 > 172.1.1.50.80:
SWE 1719837470:1719837470(0) win 8192 <mss 1460,nop,wscale
8,nop,nop,sackOK>
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC lookup resulted in egress ifc MGMT40_Outside1

Phase: 2
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_ advanced deny tcp any any object-group
HTTP rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY:
FTD Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: HTTP
object-group service HTTP tcp
 port-object eq www
Additional Information:

Result:
input-interface: MGMT40_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-
location: frame 0x00005587afa07120 flow (NA)/NA
```

What must be done to fix access to this website while preventing the same communication to all other websites?

A. Create an intrusion policy rule to have Snort allow port 80 to only 172.1.1 50.

B. Create an access control policy rule to allow port 80 to only 172.1.1 50.

C. Create an intrusion policy rule to have Snort allow port 443 to only 172.1.1.50

D. Create an access control policy rule to allow port 443 to only 172.1.1 50

Correct Answer: B

---

**QUESTION 2**

Which function is the primary function of Cisco AMP threat Grid?

A. It analyzes copies of packets from the packet flow

B. The device is deployed in a passive configuration

C. If a rule is triggered the device generates an intrusion event.

D. The packet flow traverses the device

E. If a rule is triggered the device drops the packet

Correct Answer: AC

---

**QUESTION 3**

Which action should be taken after editing an object that is used inside an access control policy?

A. Delete the existing object in use.

B. Refresh the Cisco FMC GUI for the access control policy.

C. Redeploy the updated configuration.

D. Create another rule using a different object name.

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/reusable_objects.html

---

**QUESTION 4**

An engineer is attempting to create a new dashboard within the Cisco FMC to have a single view with widgets from many of the other dashboards. The goal is to have a mixture of threat and security related widgets along with Cisco Firepower device health information. Which two widgets must be configured to provide this information? (Choose two.)

A. Intrusion Events

B. Correlation Information

C. Appliance Status

D. Current Sessions

E. Network Compliance

Correct Answer: AC

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/dashboards.html#ID-2206-00000283

---

**QUESTION 5**

A network security engineer must replace a faulty Cisco FTD device in a high availability pair. Which action must be taken while replacing the faulty unit?

A. Ensure that the faulty Cisco FTD device remains registered to the Cisco FMC

B. Shut down the active Cisco FTD device before powering up the replacement unit

C. Shut down the Cisco FMC before powering up the replacement unit

D. Unregister the faulty Cisco FTD device from the Cisco FMC

Correct Answer: D

---

**QUESTION 6**

When a Cisco FTD device is configured in transparent firewall mode, on which two interface types can an IP address be configured? (Choose two.)

A. Diagnostic

B. EtherChannel

C. BVI

D. Physical

E. Subinterface

Correct Answer: AC

---

**QUESTION 7**

An engineer must change the mode of a Cisco Secure Firewall Threat Defense (FTD) firewall in the Cisco Secure Firewall Management Center (FMC) inventory.

The engineer must take these actions:

1.

Register Secure FTD with Secure FMC.

2.

Change the firewall mode.

3.

Deregister the Secure FTD device from Secure FMC.

How must the engineer take FTD take the actions?

A. Reload the Secure FTD device.

B. Configure the management IP address.

C. Access the Secure FTD CLI from the console port.

D. Erase the Secure FTD configuration

Correct Answer: C

To change the mode of a Cisco Secure Firewall Threat Defense (FTD) device in the Cisco Secure Firewall Management Center (FMC) inventory, the engineer must follow these steps:

Register the Secure FTD with Secure FMC.

Change the firewall mode.

Deregister the Secure FTD device from Secure FMC. To perform these actions, accessing the Secure FTD CLI from the console port is necessary. This allows the engineer to execute the required commands to change the firewall mode and

manage the registration status of the FTD device.

Steps:

Connect to the Secure FTD device via the console port. Access the CLI and execute the command to change the firewall mode (configure firewall-mode).

Deregister the device from FMC if needed.

Register or re-register the device with FMC as required. References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Device Management and CLI Access.

---

**QUESTION 8**

The CIO asks a network administrator to present to management a dashboard that shows custom analysis tables for the top DNS queries URL category statistics, and the URL reputation statistics. Which action must the administrator take to quickly produce this information for management?

A. Run the Attack report and filter on DNS to show this information.

B. Create a new dashboard and add three custom analysis widgets that specify the tables needed.

C. Modify the Connection Events dashboard to display the information in a view for management.

D. Copy the intrusion events dashboard tab and modify each widget to show the correct charts.

Correct Answer: B

---

**QUESTION 9**

Which process should be checked when troubleshooting registration issues between Cisco FMC and managed devices to verify that secure communication is occurring?

A. fpcollect

B. dhclient

C. sfmgr

D. sftunnel

Correct Answer: D

---

**QUESTION 10**

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

---

**QUESTION 11**

A network administrator registered a new FTD to an existing FMC. The administrator cannot place the FTD in transparent mode. Which action enables transparent mode?

A. Add a Bridge Group Interface to the FTD before transparent mode is configured.

B. Dereglster the FTD device from FMC and configure transparent mode via the CLI.

C. Obtain an FTD model that supports transparent mode.

D. Assign an IP address to two physical interfaces.

Correct Answer: B

---

**QUESTION 12**

Which Cisco AMP for Endpoints policy is used only for monitoring endpoint activity?

A. Windows domain controller

B. audit

C. triage

D. protection

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214933-amp-for-endpoints-deployment-methodology.html