300-710$^{Q\&As}$

Securing Networks with Cisco Firepower (SNCF)

QUESTION 1

An organization recently implemented a transparent Cisco FTD in their network. They must ensure that the device does not respond to insecure SSL/TLS protocols. Which action accomplishes this task?

A. Modify the device\\'s settings using the device management feature within Cisco FMC to force only secure protocols.

B. Use the Cisco FTD platform policy to change the minimum SSL version on the device to TLS 1.2.

C. Enable the UCAPL/CC compliance on the device to support only the most secure protocols available.

D. Configure a FlexConfig object to disable any insecure TLS protocols on the Cisco FTD device.

Correct Answer: B

QUESTION 2

Which feature is supported by IRB on Cisco FTD devices?

A. redundant interface

B. high-availability cluster

C. dynamic routing protocol

D. EtherChannel interface

Correct Answer: C

QUESTION 3

Within Cisco Firepower Management Center, where does a user add or modify widgets?

A. dashboard

B. reporting

C. context explorer

D. summary tool

Correct Answer: A

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

QUESTION 4

An engineer is configuring a Cisco Secure Firewall Threat Defense device managed by Cisco Secure Firewall

Management Center. The device must have SSH enabled and be accessible from the inside interface for remote administration. Which type of policy must the engineer configure to accomplish this?

A. platform settings

B. access control

C. prefilter

D. identity

Correct Answer: A

To enable SSH access to a Cisco Secure Firewall Threat Defense (FTD) device from the inside interface for remote administration, the engineer needs to configure a Platform Settings policy in Cisco Secure Firewall Management Center

(FMC). The Platform Settings policy allows the configuration of various system-related settings, including enabling SSH, specifying the allowed interfaces, and defining the SSH access parameters.

Steps:

In FMC, navigate to Policies > Access Control > Platform Settings. Create a new Platform Settings policy or edit an existing one.

In the policy settings, go to the SSH section.

Enable SSH and specify the inside interface as the allowed interface for SSH access.

Define the SSH parameters such as allowed IP addresses, user credentials, and other security settings.

Save and deploy the policy to the FTD device.

This configuration ensures that SSH access is enabled on the specified interface, allowing secure remote administration.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Platform Settings.

QUESTION 5

A security analyst must create a new report within Cisco FMC to show an overview of the daily attacks, vulnerabilities, and connections. The analyst wants to reuse specific dashboards from other reports to create this consolidated one. Which action accomplishes this task?

A. Create a new dashboard object via Object Management to represent the desired views.

B. Modify the Custom Workflows within the Cisco FMC to feed the desired data into the new report.

C. Copy the Malware Report and modify the sections to pull components from other reports.

D. Use the import feature in the newly created report to select which dashboards to add.

Correct Answer: D

QUESTION 6

An engineer must configure a Cisco FMC dashboard in a multidomain deployment. Which action must the engineer take to edit a report template from an ancestor domain?

A. Copy it to the current domain.

B. Add it as a separate widget.

C. Change the document attributes.

D. Assign themselves ownership of it.

Correct Answer: A

QUESTION 7

An engineer is implementing Cisco FTD in the network and is determining which Firepower mode to use. The organization needs to have multiple virtual Firepower devices working separately inside of the FTD appliance to provide traffic

segmentation.

Which deployment mode should be configured in the Cisco Firepower Management Console to support these requirements?

A. Multiple Deployment

B. single-context

C. Single deployment

D. multi-instance

Correct Answer: D

QUESTION 8

An administrator is setting up a Cisco FMC and must provide expert mode access for a security engineer. The engineer is permitted to use only a secured out-of-band network workstation with a static IP address to access the Cisco FMC. What must be configured to enable this access?

A. Enable SSH and define an access list.

B. Enable HTTPS and SNMP under the Access List section.

C. Enable SCP under the Access List section.

D. Enable HTTP and define an access list.

Correct Answer: A

QUESTION 9

An administrator must use Cisco FMC to install a backup route within the Cisco FTD to route traffic in case of a routing failure with primary route. Which action accomplish this task?

A. Install the static backup route and modify the metric to be less than the primary route

B. Use a default route in the FMC instead of having multiple routes contending for priority

C. Configure EIGRP routing on the FMC to ensure that dynamic routes are always updated

D. Create the backup route and use route tracking on both routes to a destination IP address in the network

Correct Answer: D

QUESTION 10

An engineer integrates Cisco FMC and Cisco ISE using pxGrid. Which role is assigned for Cisco FMC?

A. server

B. controller

C. publisher

D. client

Correct Answer: D

Reference: https://www.ciscopress.com/articles/article.asp?p=2963461andseqNum=2

QUESTION 11

An organization must be able to ingest NetFlow traffic from their Cisco FTD device to Cisco Stealthwatch for behavioral analysis. What must be configured on the Cisco FTD to meet this requirement?

A. flexconfig object for NetFlow

B. interface object to export NetFlow

C. security intelligence object for NetFlow

D. variable set object for NetFlow

Correct Answer: A

QUESTION 12

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

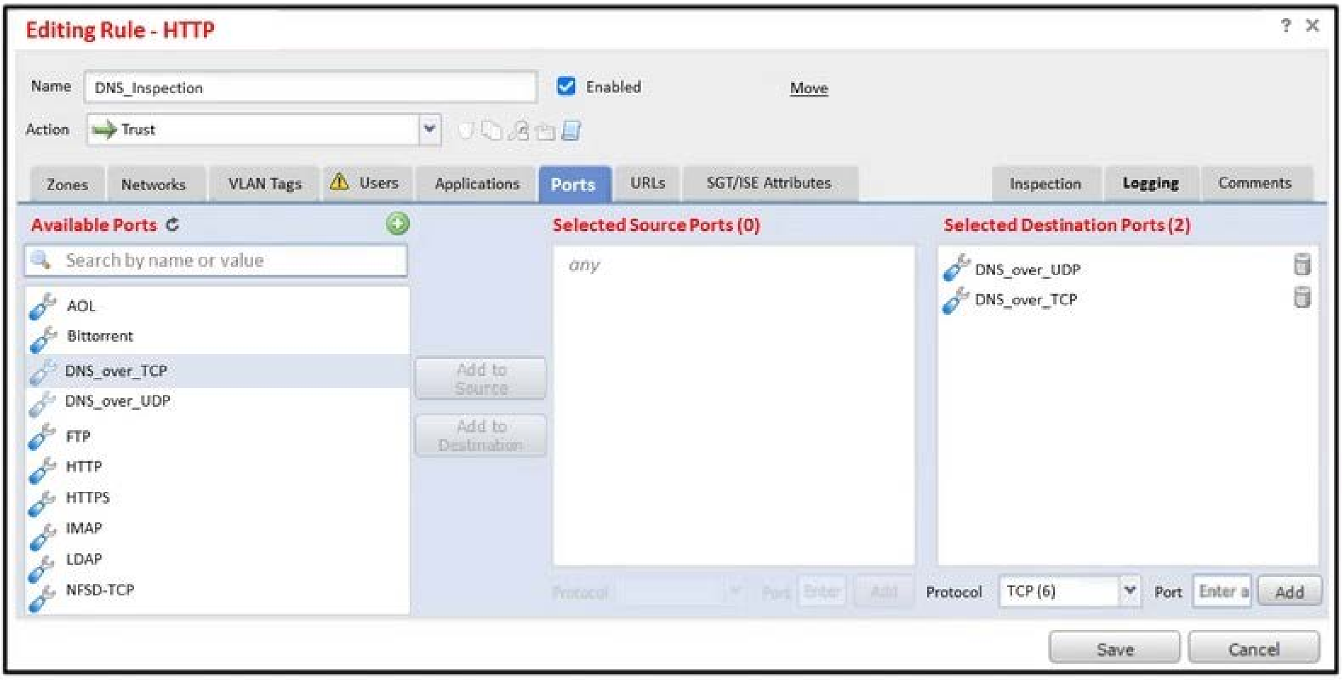
D. Identity

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 13

Refer to the exhibit



Editing Rule - HTTP

Name: DNS_Inspection

☑ Enabled

Action: Trust

Selected Source Ports (0): any

Selected Destination Ports (2): DNS_over_UDP, DNS_over_TCP

Protocol: TCP (6)

An engineer is modifying an access control pokey to add a rule to inspect all DNS traffic that passes through the firewall After making the change and deploying the pokey they see that DNS traffic is not bang inspected by the Snort engine What is the problem?

A. The rule must specify the security zone that originates the traffic.

B. The rule Is configured with the wrong setting for the source port.

C. The rule must define the source network for inspection as well as the port.

D. The action of the rule is set to trust instead of allow.

Correct Answer: D

QUESTION 14

A network engineer is deploying a pair of Cisco Secure Firewall Threat Defense devices managed by Cisco Secure Firewall Management Center for High Availability. Internet access is a high priority for the business and therefore they have invested in internet circuits from two different ISPs. The requirement from the customer is that internet access must be available to their users even if one of the ISPs is down. Which two features must be deployed to achieve this requirement? (Choose two.)

A. Route Tracking

B. Redundant interfaces

C. EtherChannel interfaces

D. SLA Monitor

E. BGP

Correct Answer: AD

To ensure high availability of internet access when deploying a pair of Cisco Secure Firewall Threat Defense (FTD) devices managed by Cisco Secure Firewall Management Center (FMC), the following features must be deployed:

Route Tracking: This feature monitors the reachability of a specified target (such as an external IP address) through the configured routes. If the route to the target is lost, the FTD can dynamically adjust the routing to use an alternate path,

ensuring continuous internet access.

SLA Monitor: Service Level Agreement (SLA) monitoring works alongside route tracking to continuously verify the status and performance of the internet links. If the SLA for one of the ISP links fails (indicating the link is down or

underperforming), the FTD can switch traffic to the secondary ISP link.

Steps to configure:

In FMC, navigate to Devices > Device Management.

Select the FTD device and configure route tracking to monitor the ISP links. Configure SLA monitors to continuously check the health and performance of the internet circuits.

These configurations ensure that internet access remains available to users even if one of the ISPs goes down.

References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on High Availability and SLA Monitoring.

QUESTION 15

An engineer is implementing a new Cisco Secure Firewall. The firewall must filler traffic between the three subnets:

1.

LAN 192.168.101.0724

2.

DMZ 192.168 200.0/24

3.

WAN 10.0.0.0/30

Which firewall mode must the engineer implement?

A. transparent

B. network

C. routed

D. gateway

Correct Answer: C

To filter traffic between multiple subnets, the engineer must implement the firewall in routed mode. In routed mode, the firewall operates as a Layer 3 device, capable of routing traffic between different IP subnets. This mode is appropriate for

filtering traffic between LAN, DMZ, and WAN subnets.

Steps to configure routed mode:

Access the firewall\\'s management interface.

Configure interfaces for each subnet (LAN, DMZ, WAN) with appropriate IP addresses and network masks.

Define security zones and apply access control policies to filter traffic as required. This ensures that the firewall can inspect and route traffic between the different subnets, providing the necessary security and control.

References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Routed Mode Configuration.