Free Cisco 300-710 SNCF Practice Questions

Shared by Hunt on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

* LAN 192.168.101.0724

* DMZ 192.168 200.0/24

* WAN 10.0.0.0/30

Which firewall mode must the engineer implement?

Options:

A- transparent
B- network
C- routed
D- gateway

Answer:

C

Explanation:

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.

Question 2

Question Type: MultipleChoice

A network administrator is configuring a site-to-site IPsec VPN to a router sitting behind a Cisco FTD. The administrator has configured an access policy to allow traffic to this device on UDP 500, 4500, and ESP VPN traffic is not working. Which action resolves this issue?

Options:

A- Set the allow action in the access policy to trust.
B- Enable IPsec inspection on the access policy.
C- Modify the NAT policy to use the interface PAT.
D- Change the access policy to allow all ports.

Answer:

B

Question 3

Question Type: MultipleChoice

A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?

Options:

A- Specify the BVl IP address as the default gateway for connected devices.
B- Enable routing on the Cisco Firepower
C- Add an IP address to the physical Cisco Firepower interfaces.
D- Configure a bridge group in transparent mode.

Answer:

D

Explanation:

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a ''bump in the wire,'' or a ''stealth firewall,'' and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place. Layer 2 connectivity is achieved by using a 'bridge group' where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.html

Question 4

Question Type: MultipleChoice

An administrator must fix a network problem whereby traffic from the inside network to a webserver is not getting through an instance of Cisco Secure Firewall Threat Defense. Which command must the administrator use to capture packets to the webserver that are dropped by Secure Firewall Throat Defense and resold the issue?

Options:

A- capture CAP int OUTSIDE match ip any host WEBSERVERIP
B- capture CAP type asp-drop all headers-only
C- capture CAP int INSIDE match ip any host WEBSERVERIP
D- capture CAP int INSIDE match tcp any 80 host WEBSERVERIP 80

Answer:

B

Explanation:

To capture packets that are dropped by Cisco Secure Firewall Threat Defense (FTD) and troubleshoot the issue of traffic from the inside network to a webserver not getting through, the administrator should use the command to capture packets dropped by the accelerated security path (ASP) engine. The correct command is:

capture CAP type asp-drop all headers-only

This command captures all packets dropped by the ASP engine, which includes packets that are

being blocked by access control policies, NAT issues, or other security checks.

Steps:

Access the FTD CLI.

Run the commandcapture CAP type asp-drop all headers-onlyto capture dropped packets.

Analyze the captured data to identify the cause of the drops.

This command provides detailed information on why packets are being dropped, helping the administrator resolve the issue.

Question 5

Question Type: MultipleChoice

Which CLI command is used to control special handling of clientHello messages?

Options:

A- system support ssl-client-hello-tuning
B- system support ssl-client-hello-display
C- system support ssl-client-hello-force-reset
D- system support ssl-client-hello-reset

Answer:

D

Question 6

Question Type: MultipleChoice

A network engineer wants to add a third-party threat feed into the Cisco FMC for enhanced threat detectionWhich action should be taken to accomplish this goal?

Options:

A- Enable Threat Intelligence Director using STIX and TAXII

B- Enable Rapid Threat Containment using REST APIs
C- Enable Threat Intelligence Director using REST APIs
D- Enable Rapid Threat Containment using STIX and TAXII

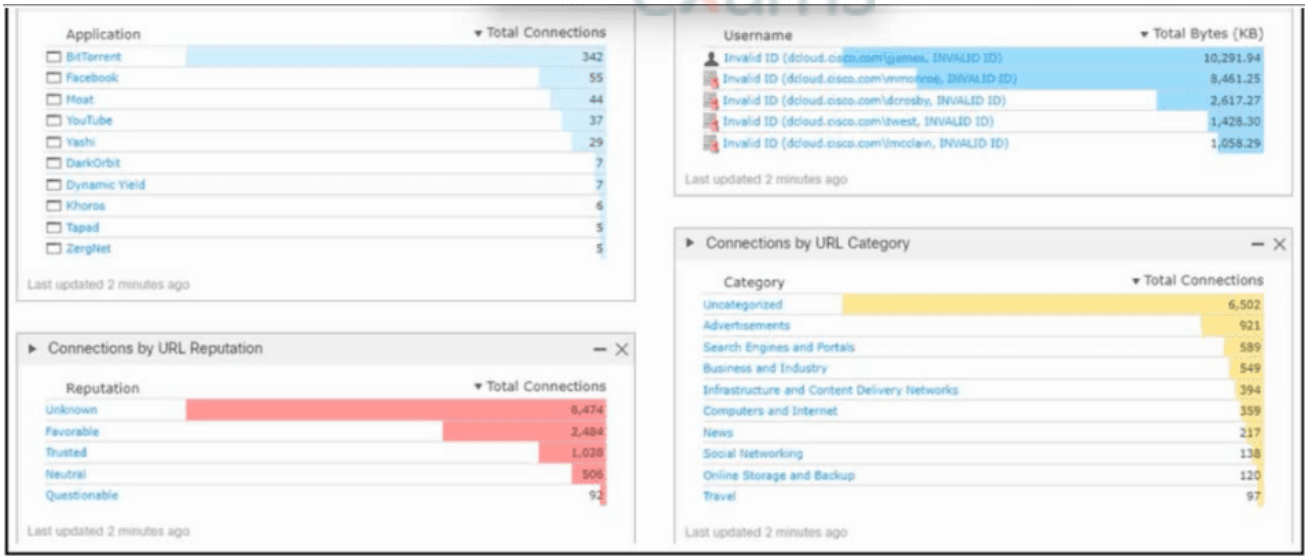
Answer:

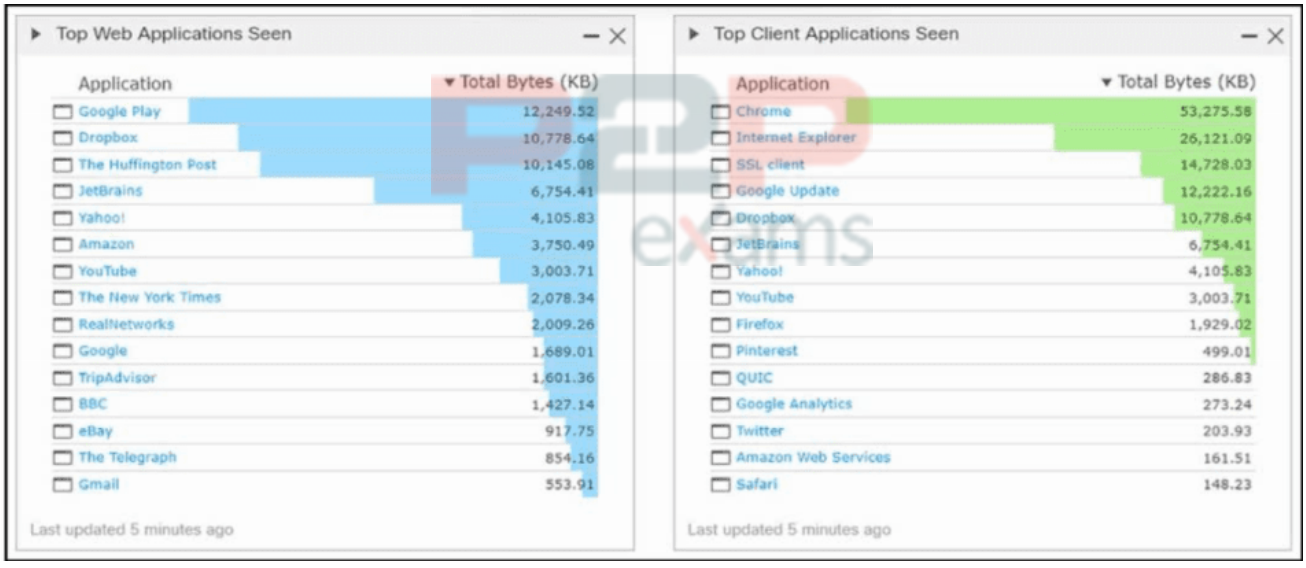
A

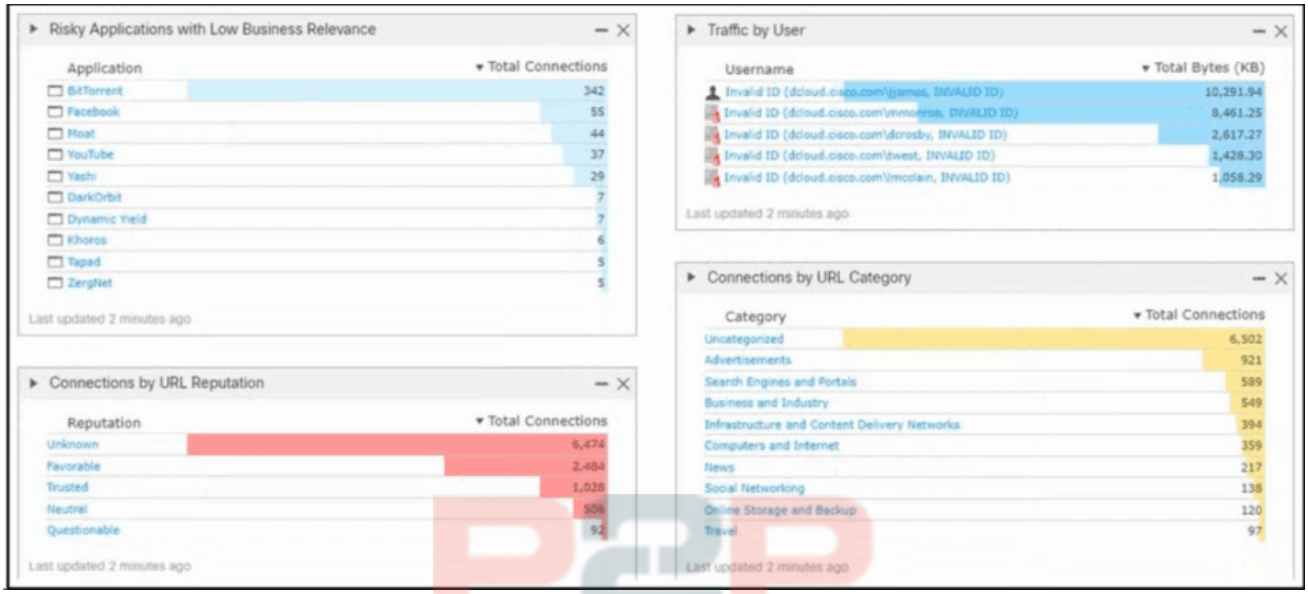
Question 7

Question Type: MultipleChoice

Refer to the exhibit.







Refer to the exhibit. An engineer analyzes a Cisco Firepower Management Center dashboard. Which action must be taken by the user to decrease the risk of data loss?

Options:

A- Stop all URLs that have an unknown reputation.
B- Block the use of Dropbox.
C- Stop all the URLs that are uncategorized.
D- Block all the BitTorrent applications.

Answer:

C

Question 8

Question Type: MultipleChoice

After using Firepower for some time and learning about how it interacts with the network, an administrator is trying to correlate malicious activity with a user Which widget should be configured to provide this visibility on the Cisco Firepower dashboards?

Options:

A- Custom Analysis
B- Current Status
C- Current Sessions
D- Correlation Events

Answer:

A

Question 9

Question Type: MultipleChoice

Remote users who connect via Cisco AnyConnect to the corporate network behind a Cisco FTD device report that they get no audio when calling between remote users using their softphones. These same users can call internal users on the corporate network without any issues. What is the cause of this issue?

Options:

A- The hairpinning feature is not available on FTD.
B- Split tunneling is enabled for the Remote Access VPN on FTD
C- FTDhas no NAT policy that allows outside to outside communication
D- The Enable Spoke to Spoke Connectivity through Hub option is not selected on FTD.

Answer:

A

Question 10

Question Type: MultipleChoice

An administrator configures the interfaces of a Cisco Secure Firewall Threat Defence device in an inline IPS deployment. The administrator completes these actions:

* identifies the device and the interfaces

* sets the interface mode to inline

* enables the interlaces

Which configuration step must the administrator take next to complete the implementation?

Options:

A- Enable spanning-tree PortFast on the interfaces.

B- Configure an inline set
C- Set the interface to Transparent mode.
D- Set the interface to routed mode.

Answer:

B

Explanation:

After setting the interface mode to inline and enabling the interfaces on a Cisco Secure Firewall Threat Defense (FTD) device in an inline IPS deployment, the next step is to configure an inline set. An inline set groups two interfaces that work together to inspect traffic passing between them.

Steps to configure an inline set:

In FMC, navigate toDevices > Device Management.

Select the FTD device and configure the interfaces.

Create a new inline set, adding the relevant interfaces that have been set to inline mode.

Deploy the configuration to the FTD device.

Configuring an inline set ensures that the traffic between the specified interfaces is inspected and processed according to the IPS policies, completing the implementation of the inline IPS deployment.

Question 11

Question Type: MultipleChoice

An engineer is tasked with deploying an internal perimeter firewall that will support multiple DMZs Each DMZ has a unique private IP subnet range. How is this requirement satisfied?

Options:

A- Deploy the firewall in transparent mode with access control policies.
B- Deploy the firewall in routed mode with access control policies.
C- Deploy the firewall in routed mode with NAT configured.
D- Deploy the firewall in transparent mode with NAT configured.

Answer:

C

P2P exams