- **Vendor: Cisco**
- **Exam Code: 300-710**
- **Exam Name: Securing Networks with Cisco Firepower (SNCF)**
- **New Updated Questions from Braindump2go (Updated in April/2021)**

QUESTION 93
An organization has implemented Cisco Firepower without IPS capabilities and now wants to enable inspection for their traffic.
They need to be able to detect protocol anomalies and utilize the Snort rule sets to detect malicious behavior. How is this accomplished?

A. Modify the network discovery policy to detect new hosts to inspect.
B. Modify the access control policy to redirect interesting traffic to the engine.
C. Modify the intrusion policy to determine the minimum severity of an event to inspect.
D. Modify the network analysis policy to process the packets for inspection.

Answer: D
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdmintrusion.html

QUESTION 94
A hospital network needs to upgrade their Cisco FMC managed devices and needs to ensure that a disaster recovery process is in place. What must be done in order to minimize downtime on the network?

A. Configure a second circuit to an ISP for added redundancy
B. Keep a copy of the current configuration to use as backup
C. Configure the Cisco FMCs for failover
D. Configure the Cisco FMC managed devices for clustering.

Answer: C

QUESTION 95
An engineer is monitoring network traffic from their sales and product development departments, which are on two separate networks.
What must be configured in order to maintain data privacy for both departments?

A. Use a dedicated IPS inline set for each department to maintain traffic separation
B. Use 802 1Q mime set Trunk interfaces with VLANs to maintain logical traffic separation
C. Use passive IDS ports for both departments
D. Use one pair of inline set in TAP mode for both departments

Answer: D
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-

v64/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

QUESTION 96
With Cisco FTD software, which interface mode must be configured to passively receive traffic that passes through the appliance?

A. ERSPAN
B. IPS-only
C. firewall
D. tap

Answer: A
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/interface_overview_for_firepower_threat_defense.html

QUESTION 97
A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface.
What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

A. The destination MAC address is optional if a VLAN ID value is entered
B. Only the UDP packet type is supported
C. The output format option for the packet logs unavailable
D. The VLAN ID and destination MAC address are optional

Answer: A
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

QUESTION 98
What is a characteristic of bridge groups on a Cisco FTD?

A. In routed firewall mode, routing between bridge groups must pass through a routed interface.
B. In routed firewall mode, routing between bridge groups is supported.
C. In transparent firewall mode, routing between bridge groups is supported
D. Routing between bridge groups is achieved only with a router-on-a-stick configuration on a connected router

Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.pdf

QUESTION 99
Network traffic coining from an organization's CEO must never be denied.
Which access control policy configuration option should be used if the deployment engineer is not permitted to create a rule to allow all traffic?

A. Configure firewall bypass.
B. Change the intrusion policy from security to balance.
C. Configure a trust policy for the CEO.
D. Create a NAT policy just for the CEO.

Answer: C

QUESTION 100

An organization has a compliancy 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. Deploy a firewall in transparent mode between the clients and servers.
B. Change the IP addresses of the clients, while remaining on the same subnet.
C. Deploy a firewall in routed mode between the clients and servers
D. Change the IP addresses of the servers, while remaining on the same subnet

Answer: C

QUESTION 101
In a multi-tenant deployment where multiple domains are in use. Which update should be applied outside of the Global Domain?

A. minor upgrade
B. local import of intrusion rules
C. Cisco Geolocation Database
D. local import of major upgrade

Answer: C

QUESTION 102
A mid-sized company is experiencing higher network bandwidth utilization due to a recent acquisition. The network operations team is asked to scale up their one Cisco FTD appliance deployment to higher capacities due to the increased network bandwidth.
Which design option should be used to accomplish this goal?

A. Deploy multiple Cisco FTD appliances in firewall clustering mode to increase performance.
B. Deploy multiple Cisco FTD appliances using VPN load-balancing to scale performance.
C. Deploy multiple Cisco FTD HA pairs to increase performance
D. Deploy multiple Cisco FTD HA pairs in clustering mode to increase performance

Answer: A
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept_C8502505F840451C9E600F1EED9BC18E

QUESTION 103
An organization has seen a lot of traffic congestion on their links going out to the internet There is a Cisco Firepower device that processes all of the traffic going to the internet prior to leaving the enterprise. How is the congestion alleviated so that legitimate business traffic reaches the destination?

A. Create a flexconfig policy to use WCCP for application aware bandwidth limiting
B. Create a VPN policy so that direct tunnels are established to the business applications
C. Create a NAT policy so that the Cisco Firepower device does not have to translate as many addresses
D. Create a QoS policy rate-limiting high bandwidth applications

Answer: D

QUESTION 104
An engineer configures an access control rule that deploys file policy configurations to security zone or tunnel zones, and it causes the device to restart. What is the reason for the restart?

A. Source or destination security zones in the access control rule matches the security zones that

are associated with interfaces on the target devices.
B. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.
C. Source or destination security zones in the source tunnel zone do not match the security zones that are associated with interfaces on the target devices.
D. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.

Answer: A
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/policy_management.html

QUESTION 105
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

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

QUESTION 106
An organization is setting up two new Cisco FTD devices to replace their current firewalls and cannot have any network downtime. During the setup process, the synchronization between the two devices is failing.
What action is needed to resolve this issue?

A. Confirm that both devices have the same port-channel numbering
B. Confirm that both devices are running the same software version
C. Confirm that both devices are configured with the same types of interfaces
D. Confirm that both devices have the same flash memory sizes

Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/firepower_threat_defense_high_availability.html#Cisco_Reference.dita_cc8821d8-a5a5-49c0-97fddc9b6f7dbad2