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

QUESTION 155
Within an organization's high availability environment where both firewalls are passing traffic, traffic must be segmented based on which department it is destined for. Each department is situated on a different LAN. What must be configured to meet these requirements?

A. redundant interfaces
B. span EtherChannel clustering
C. high availability active/standby firewalls
D. multi-instance firewalls

Answer: D

QUESTION 156
An engineer is configuring a Cisco IPS to protect the network and wants to test a policy before deploying it. A copy of each incoming packet needs to be monitored while traffic flow remains constant. Which IPS mode should be implemented to meet these requirements?

A. routed
B. passive
C. transparent
D. inline tap

Answer: D

QUESTION 157
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

Answer: A

QUESTION 158
An administrator is optimizing the Cisco FTD rules to improve network performance, and wants to bypass inspection for certain traffic types to reduce the load on the Cisco FTD. Which policy must be configured to accomplish this goal?

A. intrusion
B. prefilter
C. URL filtering
D. identity

Answer: B

QUESTION 159
A company is in the process of deploying intrusion prevention with Cisco FTDs managed by a Cisco FMC. An engineer must configure policies to detect potential intrusions but not block the suspicious traffic Which action accomplishes this task?

A. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the “Drop when inline” option.
B. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the “Drop when inline” option.
C. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the “Drop when inline” option.
D. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the “Drop when inline” option.

Answer: B

QUESTION 160
An engineer is using the **configure manager add <FMC IP> Cisc404225383** command to add a new Cisco FTD device to the Cisco FMC; however, the device is not being added. Why is this occurring?

A. **DONOTRESOLVE** must be added to the command
B. The IP address used should be that of the Cisco FTD, not the Cisco FMC
C. The registration key is missing from the command
D. The NAT ID is required since the Cisco FMC is behind a NAT device

Answer: D

QUESTION 161
An engineer is configuring Cisco FMC and wants to allow multiple physical interfaces to be part of the same VLAN. The managed devices must be able to perform Layer 2 switching between interfaces, including sub-interfaces. What must be configured to meet these requirements?

A. inter-chassis clustering VLAN
B. Cisco ISE Security Group Tag
C. interface-based VLAN switching
D. integrated routing and bridging

Answer: D

QUESTION 162
An organization does not want to use the default Cisco Firepower block page when blocking HTTP traffic. The organization wants to include information about its policies and procedures to help educate the users whenever a block occurs. Which two steps must be taken to meet these requirements? (Choose two.)

A. Edit the HTTP request handling in the access control policy to customized block
B. Modify the system-provided block page result using Python
C. Create HTML code with the information for the policies and procedures

D. Change the HTTP response in the access control policy to custom
E. Write CSS code with the information for the policies and procedures

Answer: AD

QUESTION 163
A company has many Cisco FTD devices managed by a Cisco FMC. The security model requires that access control rule logs be collected for analysis. The security engineer is concerned that the Cisco FMC will not be able to process the volume of logging that will be generated. Which configuration addresses concern this?

A. Send Cisco FTD connection events directly to a SIEM system and forward security events from Cisco FMC to the SIEM system for storage and analysis
B. Send Cisco FTD connection events and security events directly to SIEM system for storage and analysis
C. Send Cisco FTD connection events and security events to a cluster of Cisco FMC devices for storage and analysis
D. Send Cisco FTD connection events and security events to Cisco FMC and configure it to forward logs to SIEM for storage and analysis

Answer: B

QUESTION 164
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

Answer: D

QUESTION 165
A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https://<FMC IP>/capture/CAPI/pcap/test.pcap, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

A. Disable the proxy setting on the browser
B. Disable the HTTPS server and use HTTP instead
C. Use the Cisco FTD IP address as the proxy server setting on the browser
D. Enable the HTTPS server for the device platform policy

Answer: D