- **Vendor:** Cisco
- **Exam Code:** 300-710
- **Exam Name:** Securing Networks with Cisco Firepower (SNCF)
- **New Updated Questions from Braindump2go**
- **(Updated in December/2023)**

QUESTION 298
A network administrator reviews the attack risk report and notices several low-impact attacks. What does this type of attack indicate?

A. All attacks are listed as low until manually recategorized.
B. The host is not vulnerable to those attacks.
C. The host is not within the administrator's environment.
D. The attacks are not dangerous to the network.

Answer: D

QUESTION 299
What is a limitation to consider when running a dynamic routing protocol on a Cisco Secure Firewall Threat Defense device in IRB mode?

A. Only link-state routing protocols are supported.
B. Only nonbridge interfaces are supported.
C. Only EtherChannel interfaces are supported.
D. Only distance vector routing protocols are supported.

Answer: B

QUESTION 300
An engineer is configuring URL filtering for a Cisco FTD device in Cisco FMC. Users must receive a warning when they access http://www.badadultsite.com with the option of continuing to the website if they choose to. No other websites should be blocked. Which two actions must the engineer take to meet these requirements? (Choose two.)

A. On the HTTP Responses tab of the access control policy editor, set the Interactive Block Response Page to System-provided.
B. Configure the default action for the access control policy to Interactive Block.
C. Configure an access control rule that matches an URL object for http://www.badadultsite.com/ and set the action to Interactive Block.
D. Configure an access control rule that matches the Adult URL category and set the action to Interactive Block.
E. On the HTTP Responses tab of the access control policy editor, set the Block Response Page to Custom.

Answer: AC

QUESTION 301
The security engineer reviews the syslog server events of an organization and sees many outbound connections to malicious sites initiated from hosts running Cisco Secure Endpoint. The hosts are on a separate network from the Cisco FTD device. Which action blocks the connections?

A. Modify the policy on Cisco Secure Endpoint to enable DFC.
B. Modify the access control policy on the Cisco FMC to block malicious outbound connections
C. Add the IP addresses of the malicious sites to the access control policy on the Cisco FMC
D. Add a Cisco Secure Endpoint policy with the Tetra and Spero engines enabled

Answer: C

QUESTION 302
An engineer has been tasked with performing an audit of network objects to determine which objects are duplicated across the various firewall models (Cisco Secure Firewall Threat Defense, Cisco Secure Firewall ASA, and Meraki MX Series) deployed throughout the company. Which tool will assist the engineer in performing that audit?

A. Cisco Firepower Device Manager
B. Cisco Defense Orchestrator
C. Cisco Secure Firewall Management Center
D. Cisco SecureX

Answer: B

QUESTION 303
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

Answer: AD

QUESTION 304
A network engineer is planning on replacing an Active/Standby pair of physical Cisco Secure Firewall ASAs with a pair of Cisco Secure Firewall Threat Defense Virtual appliances. Which two virtual environments support the current High Availability configuration? (Choose two.)

A. ESXi
B. Azure
C. Openstack
D. KVM
E. AWS

Answer: AD

QUESTION 305
A company is deploying AMP private cloud. The AMP private cloud instance has already been deployed by the server

administrator. The server administrator provided the hostname of the private cloud instance to the network engineer via email. What additional information does the network engineer require from the server administrator to be able to make the connection to the AMP private cloud in Cisco FMC?

A. SSL certificate for the AMP private cloud instance
B. Username and password to the AMP private cloud instance
C. IP address and port number for the connection proxy
D. Internet access for the AMP private cloud to reach the AMP public cloud

Answer: B

QUESTION 306
A security engineer is deploying Cisco Secure Endpoint to detect a zero day malware attack with an SHA-256 hash of 47ea931f3e9dc23ec0b0885a80663e30ea013d493f8e88224b570a0464084628. What must be configured in Cisco Secure Endpoint to enable the application to take action based on this hash?

A. access control rule
B. correlation policy
C. transform set
D. custom detection list

Answer: D

QUESTION 307
A security engineer must create a malware and file policy on a Cisco Secure Firewall Threat Defense device. The solution must ensure that PDF, DOCX, and XLSX files are not sent to Cisco Secure Malware Analytics. What must be configured to meet the requirements?

A. Spero analysis
B. local malware analysis
C. capacity handling
D. dynamic analysis

Answer: B

QUESTION 308
Encrypted Visibility Engine (EVE) is enabled under which tab on an access control policy in Cisco Secure Firewall Management Center?

A. Network Analysis Policy
B. SSL
C. Advanced
D. Security Intelligence

Answer: C

QUESTION 309
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

Answer: B

QUESTION 310
What is the result when two users modify a VPN policy at the same time on a Cisco Secure Firewall Management Center managed device?

A. Both users can edit the policy and the last saved configuration persists.
B. The changes from both users will be merged together into the policy.
C. The first user locks the configuration when selecting edit on the policy.
D. The system prevents modifications to the policy by multiple users.

Answer: A

QUESTION 311
A network administrator is configuring a BVI interface on a routed FTD. The administrator wants to isolate traffic on the interfaces connected to the bridge group and not have the FTD route this traffic using the routing table. What must be configured?

A. A new VRF must be created for the BVI interface
B. An IP address must be configured on the BVI
C. IP routing must be removed from the physical interfaces connected to the BVI
D. The BVI interface must be configured for transparent mode

Answer: D

QUESTION 312
Which file format can standard reports from Cisco Secure Firewall Management Center be downloaded in?

A. doc
B. ppt
C. csv
D. xls

Answer: C