

➤ **Vendor: Cisco**

➤ **Exam Code: 300-710**

➤ **Exam Name: Securing Networks with Cisco Firepower (SNCF)**

➤ **New Updated Questions from Braindump2go (Updated in June/2022)**

Visit Braindump2go and Download Full Version 300-710 Exam Dumps

QUESTION 212

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 HTTP and define an access list.
- C. Enable SCP under the Access List section.
- D. Enable HTTPS and SNMP under the Access List section.

Answer: A

QUESTION 213

An engineer must add DNS-specific rules to the Cisco FTD intrusion policy. The engineer wants to use the rules currently in the Cisco FTD Snort database that are not already enabled but does not want to enable more than are needed. Which action meets these requirements?

- A. Change the dynamic state of the rule within the policy.
- B. Change the base policy to Security over Connectivity.
- C. Change the rule state within the policy being used.
- D. Change the rules using the Generate and Use Recommendations feature.

Answer: C

QUESTION 214

A network administrator is trying to convert from LDAP to LDAPS for VPN user authentication on a Cisco FTD. Which action must be taken on the Cisco FTD objects to accomplish this task?

- A. Add a Key Chain object to acquire the LDAPS certificate.
- B. Create a Certificate Enrollment object to get the LDAPS certificate needed.
- C. Identify the LDAPS cipher suite and use a Cipher Suite List object to define the Cisco FTD connection requirements.
- D. Modify the Policy List object to define the session requirements for LDAPS.

Answer: B

QUESTION 215

What is the RTC workflow when the infected endpoint is identified?

[300-710 Exam Dumps](#) [300-710 Exam Questions](#) [300-710 PDF Dumps](#) [300-710 VCE Dumps](#)

<https://www.braindump2go.com/300-710.html>

- A. Cisco ISE instructs Cisco AMP to contain the infected endpoint.
- B. Cisco ISE instructs Cisco FMC to contain the infected endpoint.
- C. Cisco AMP instructs Cisco FMC to contain the infected endpoint.
- D. Cisco FMC instructs Cisco ISE to contain the infected endpoint.

Answer: D

QUESTION 216

Which feature is supported by IRB on Cisco FTD devices?

- A. redundant interface
- B. dynamic routing protocol
- C. EtherChannel interface
- D. high-availability cluster

Answer: B

QUESTION 217

A security engineer is deploying a pair of primary and secondary Cisco FMC devices. The secondary must also receive updates from Cisco Talos. Which action achieves this goal?

- A. Force failover for the secondary Cisco FMC to synchronize the rule updates from the primary.
- B. Configure the secondary Cisco FMC so that it receives updates from Cisco Talos.
- C. Manually import rule updates onto the secondary Cisco FMC device.
- D. Configure the primary Cisco FMC so that the rules are updated.

Answer: D

QUESTION 218

Refer to the exhibit. A systems administrator conducts a connectivity test to their SCCM server from a host machine and gets no response from the server. Which action ensures that the ping packets reach the destination and that the host receives replies?

```
Phase: 16
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Firewall: starting rule matching, zone 4 -> 1, geo 0 -> 0, vlan 0, src sgt type 0, dest sgt type 0, username 'No Authentication Required', , icmpType 8, icmpCode 0
Firewall: block rule, 'ping', drop
Snort: processed decoder alerts or actions queue, drop
Snort id 0, MAP id 2, IPS id 0, Verdict BLACKLIST, Blocked by Firewall
Snort Verdict: (black-list) black list this flow

Result:
Input-Interface: ACCESS41_Inside1
Input-status: up
Input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame 0x000055d2b0f8b7e0 flow (NA)/NA
```

- A. Create an access control policy rule that allows ICMP traffic.
- B. Configure a custom Snort signature to allow ICMP traffic after Inspection.
- C. Modify the Snort rules to allow ICMP traffic.
- D. Create an ICMP allow list and add the ICMP destination to remove it from the implicit deny list.

Answer: A

QUESTION 219

A security engineer must configure a Cisco FTD appliance to inspect traffic coming from the internet. The Internet traffic will be mirrored from the Cisco Catalyst 9300 Switch.

Which configuration accomplishes the task?

- A. Set interface configuration mode to none.

[300-710 Exam Dumps](#) **[300-710 Exam Questions](#) **[300-710 PDF Dumps](#) **[300-710 VCE Dumps](#)******

<https://www.braindump2go.com/300-710.html>

- B. Set the firewall mode to transparent.
- C. Set the firewall mode to routed.
- D. Set interface configuration mode to passive.

Answer: D

QUESTION 220

The network administrator wants to enhance the network security posture by enabling machine learning for malware detection due to a concern with suspicious Microsoft executable file types that were seen while creating monthly security reports for the CIO. Which feature must be enabled to accomplish this goal?

- A. Spero
- B. dynamic analysis
- C. static analysis
- D. Ethos

Answer: A