



300-710^{Q&As}

Securing Networks with Cisco Firepower (SNCF)

Pass Cisco 300-710 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

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

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

Refer to the exhibit.

```
Phase: IG
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Firewall: starting rule matching, zone 1 -> 1, geo 0 -> 0, vlan 0, sgt 0, src sgt type 0, dest_sgt_tag 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 0x0005562b0f8b7e0 flow (NA)/NA
```

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?

- 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.

Correct Answer: A

QUESTION 2

In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.)

- A. Traffic inspection can be interrupted temporarily when configuration changes are deployed.
- B. The system performs intrusion inspection followed by file inspection.
- C. They can block traffic based on Security Intelligence data.
- D. File policies use an associated variable set to perform intrusion prevention.
- E. The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters.

Correct Answer: AC

When deploying changes SNORT can restart causing traffic interruptions -->

<https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/>

[policy_management.html#reference_F11C552688424DEF85ED145FA97283B7](https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/policy_management.html#reference_F11C552688424DEF85ED145FA97283B7)

File policies don't make use of Variable sets, those are used for Intrusion policies.



Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Access_Control_Using_Intrusion_and_File_Policies.html

QUESTION 3

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

Correct Answer: C

QUESTION 4

What is the advantage of having Cisco Firepower devices send events to Cisco Threat Response via the security services exchange portal directly as opposed to using syslog?

- A. All types of Cisco Firepower devices are supported.
- B. An on-premises proxy server does not need to be set up and maintained.
- C. Cisco Firepower devices do not need to be connected to the Internet.
- D. Supports all devices that are running supported versions of Cisco Firepower.

Correct Answer: B

QUESTION 5

When deploying a Cisco ASA Firepower module, an organization wants to evaluate the contents of the traffic without affecting the network. It is currently configured to have more than one instance of the same device on the physical appliance. Which deployment mode meets the needs of the organization?

- A. inline tap monitor-only mode
- B. passive monitor-only mode
- C. passive tap monitor-only mode
- D. inline mode

Correct Answer: A



<https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config/access-sfr.html>

Inline tap monitor-only mode (ASA inline)--In an inline tap monitor-only deployment, a copy of the traffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode lets you see what the ASA FirePOWER module would have done to traffic, and lets you evaluate the content of the traffic, without impacting the network. However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.

[300-710 VCE Dumps](#)

[300-710 Practice Test](#)

[300-710 Braindumps](#)