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.pass4itsure.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

A company wants a solution to aggregate the capacity of two Cisco FTD devices to make the best use of resources such as bandwidth and connections per second. Which order of steps must be taken across the Cisco FTDs with Cisco FMC to meet this requirement?

A. Add members to the Cisco FMC, configure Cisco FTD interfaces, create the cluster in Cisco FMC, and configure cluster members in Cisco FMC

B. Add members to Cisco FMC, configure Cisco FTD interfaces in Cisco FMC, configure cluster members in Cisco FMC, create cluster in Cisco FMC, and configure cluster members in Cisco FMC

C. Configure the Cisco FTD interfaces, add members to FMC, configure cluster members in FMC, and create cluster in Cisco FMC

D. Configure the Cisco FTD interfaces and cluster members, add members to Cisco FMC, and create the cluster in Cisco FMC

Correct Answer: C

QUESTION 2

An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighbouring Cisco devices or use multicast in their environment. What must be done to resolve this issue?

A. Create a firewall rule to allow CDP traffic.

B. Create a bridge group with the firewall interfaces.

C. Change the firewall mode to transparent.

D. Change the firewall mode to routed.

Correct Answer: C

"In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule..." "The bridge group does not pass CDP packets packets..." https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/general/asa-913-general-config/intro-fw.html

Passing Traffic Not Allowed in Routed Mode

In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an access rule. The bridge group, however, can allow almost any traffic through using either an access rule (for IP traffic) or an EtherType rule (for non-

IP traffic):

IP traffic--In routed firewall mode, broadcast and "multicast traffic is blocked even if you allow it in an access rule," including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you

can allow this traffic with an access rule (using an extended ACL).

Non-IP traffic--AppleTalk, IPX, BPDUs, and MPLS, for example, can be configured to go through using an EtherType rule.

Note

"The bridge group does not pass CDP packets packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. An exception is made for BPDUs and IS- IS, which are supported. "

QUESTION 3

A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https:///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 HTTPS server and use HTTP instead.

B. Enable the HTTPS server for the device platform policy.

C. Disable the proxy setting on the browser.

D. Use the Cisco FTD IP address as the proxy server setting on the browser.

Correct Answer: B

QUESTION 4

An engineer wants to connect a single IP subnet through a Cisco FTD firewall and enforce policy. There is a requirement to present the internal IP subnet to the outside as a different IP address. What must be configured to meet these requirements?

A. Configure the downstream router to perform NAT.

B. Configure the upstream router to perform NAT.

C. Configure the Cisco FTD firewall in routed mode with NAT enabled.

D. Configure the Cisco FTD firewall in transparent mode with NAT enabled.

Correct Answer: C

QUESTION 5

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

A. ERSPAN

B. firewall

C. tap

D. IPS-only

Correct Answer: C

In Cisco Firepower Threat Defense (FTD) software, configuring an interface in "tap" mode is necessary to passively receive traffic that passes through the appliance. Tap mode allows the interface to act as a passive listening device, monitoring traffic between other devices without interfering or altering the traffic flow. This mode is used primarily for intrusion detection and monitoring purposes, enabling the appliance to analyze traffic for potential threats or anomalies while maintaining the integrity of the network\\'s operational status.