Securing Networks with Cisco Firepower (300-710 SNCF)

1. What is a result of enabling Cisco FTD clustering?

A. For the dynamic routing feature, if the master unit fails, the newly elected master unit maintains all existing connections.

B. Integrated Routing and Bridging is supported on the master unit.

C. Site-to-site VPN functionality is limited to the master unit, and all VPN connections are dropped if the master unit fails.

D. All Firepower appliances can support Cisco FTD clustering.

Answer(s): C

---

2. Which two conditions are necessary for high availability to function between two Cisco FTD devices? (Choose two.)

- [ ] A. The units must be the same version
- [ ] B. Both devices can be part of a different group that must be in the same domain when configured within the FMC.
- [ ] C. The units must be different models if they are part of the same series.
- [ ] D. The units must be configured only for firewall routed mode.
- [ ] E. The units must be the same model.

Answer(s): A E

---

3. On the advanced tab under inline set properties, which allows interfaces to emulate a passive interface?

A. transparent inline mode

B. TAP mode

C. strict TCP enforcement

D. propagate link state

Answer(s): D

---

4. What are the minimum requirements to deploy a managed device inline?

A. inline interfaces, security zones, MTU, and mode

B. passive interface, MTU, and mode

C. inline interfaces, MTU, and mode

D. passive interface, security zone, MTU, and mode

Answer(s): C

---

5. What is the difference between inline and inline tap on Cisco Firepower?

A. Inline tap mode can send a copy of the traffic to another device.

B. Inline tap mode does full packet capture.

C. Inline mode cannot do SSL decryption.

D. Inline mode can drop malicious traffic.

Answer(s): A

---

6. With Cisco Firepower Threat Defense software, which interface mode must be configured to passively receive traffic that passes through the appliance?

A. inline set

B. passive

C. routed

D. inline tap

Answer(s): B

---

7. Which two deployment types support high availability? (Choose two.)

- [ ] A. transparent
- [ ] B. routed
- [ ] C. clustered
- [ ] D. intra-chassis multi-instance
- [ ] E. virtual appliance in public cloud

Answer(s): A B

---

8. Which protocol establishes network redundancy in a switched Firepower device deployment?

A. STP

B. HSRP

C. GLBP

D. VRRP

Answer(s): A

---

9. Which interface type allows packets to be dropped?

A. passive

B. inline

C. ERSPAN

D. TAP

Answer(s): B

---

10. Which Cisco Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two.)

- [ ] A. Redundant Interface
- [ ] B. EtherChannel
- [ ] C. Speed
- [ ] D. Media Type
- [ ] E. Duplex

Answer(s): C E

---

11. Which two dynamic routing protocols are supported in Firepower Threat Defense without using FlexConfig? (Choose two.)

- [ ] A. EIGRP
- [ ] B. OSPF

- [ ] C. static routing
- [ ] D. IS-IS
- [ ] E. BGP

Answer(s): B E

---

12. Which policy rule is included in the deployment of a local DMZ during the initial deployment of a Cisco NGFW through the Cisco FMC GUI?

A. a default DMZ policy for which only a user can change the IP addresses.

B. deny ip any

C. no policy rule is included

D. permit ip any

Answer(s): C

---

13. What are two application layer preprocessors? (Choose two.)

- [ ] A. CIFS
- [ ] B. IMAP
- [ ] C. SSL
- [ ] D. DNP3
- [ ] E. ICMP

Answer(s): B C

---

14. An engineer is tasked with deploying an internal perimeter firewall that will support multiple DMZs Each DMZ has a unique private IP subnet range. How is this requirement satisfied?

A. Deploy the firewall in transparent mode with access control policies.

B. Deploy the firewall in routed mode with access control policies.

C. Deploy the firewall in routed mode with NAT configured.

D. Deploy the firewall in transparent mode with NAT configured.

Answer(s): C

---

15. An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic concurrently. How must the devices be implemented in this environment?

A. in active/active mode

B. in a cluster span EtherChannel

C. in active/passive mode

D. in cluster interface mode

Answer(s): C

---

16. 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

Answer(s): A

---

17. 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.

Answer(s): C

---

18. A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?

A. Specify the BVl IP address as the default gateway for connected devices.

B. Enable routing on the Cisco Firepower

C. Add an IP address to the physical Cisco Firepower interfaces.

D. Configure a bridge group in transparent mode.

Answer(s): D

---

19. Which two conditions must be met to enable high availability between two Cisco FTD devices? (Choose two.)

- [ ] A. same flash memory size
- [ ] B. same NTP configuration
- [ ] C. same DHCP/PPoE configuration
- [ ] D. same host name
- [ ] E. same number of interfaces

Answer(s): B E

---

20. An engineer is building a new access control policy using Cisco FMC. The policy must inspect a unique IPS policy as well as log rule matching.
Which action must be taken to meet these requirements?

A. Configure an IPS policy and enable per-rule logging.

B. Disable the default IPS policy and enable global logging.

C. Configure an IPS policy and enable global logging.

D. Disable the default IPS policy and enable per-rule logging.

Answer(s): C
