

# Latest Version: 17.0

## Question: 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: C**

Explanation:

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmconfig-guide-v64/clustering\\_for\\_the\\_firepower\\_threat\\_defense.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmconfig-guide-v64/clustering_for_the_firepower_threat_defense.html)

## Question: 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: AE**

Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/firepower-managementcenter/212699-configure-ftd-high-availability-on-firep.html>

## Question: 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: D**

Explanation:

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmconfig-guide-v64/inline\\_sets\\_and\\_passive\\_interfaces\\_for\\_firepower\\_threat\\_defense.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmconfig-guide-v64/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html)

### Question: 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: C**

Explanation:

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmconfig-guide-v65/ips\\_device\\_deployments\\_and\\_configuration.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmconfig-guide-v65/ips_device_deployments_and_configuration.html)

### Question: 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: A**