

# QUESTIONS & ANSWERS

Kill your exam at first Attempt



300-710 Dumps  
300-710 Braindumps  
300-710 Real Questions  
300-710 Practice Test  
300-710 dumps free



**Cisco**

# 300-710

*Securing Networks with Cisco Firepower*

<http://killexams.com/pass4sure/exam-detail/300-710>



### Question: 273

When creating a report template, how can the results be limited to show only the activity of a specific subnet?

- A. Create a custom search in Firepower Management Center and select it in each section of the report.
- B. Add an Input Parameter in the Advanced Settings of the report, and set the type to Network/I
- D. Add a Table View section to the report with the Search field defined as the network in CIDR format.
- E. Select IP Address as the X-Axis in each section of the report.

**Answer: B**

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/piresight/541/user-guide/FireSIGHT-SystemUserGuide-v5401/Reports.html#87267>

### Question: 274

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 FM
- D. The units must be different models if they are part of the same series.
- E. The units must be configured only for firewall routed mode.
- F. The units must be the same model.

**Answer: AE**

Explanation:

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

### Question: 275

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: C**

### Question: 276

Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)

- A. OSPFv2 with IPv6 capabilities
- B. virtual links
- C. SHA authentication to OSPF packets
- D. area boundary router type 1 LSA filtering
- E. MD5 authentication to OSPF packets

**Answer: BD**

Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/ospf\\_for\\_firepower\\_threat\\_defense.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/ospf_for_firepower_threat_defense.html)

### Question: 277

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:** D

**Question:** 278

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:** B

Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/interface\\_overview\\_for\\_firepower\\_threat\\_defense.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/interface_overview_for_firepower_threat_defense.html)

**Question:** 279

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:** AB

Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-configguide-v61/firepower\\_threat\\_defense\\_high\\_availability.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-configguide-v61/firepower_threat_defense_high_availability.html)

**Question:** 280

Which two actions can be used in an access control policy rule? (Choose two.)

- A. Block with Reset
- B. Monitor
- C. Analyze
- D. Discover
- E. Block ALL

**Answer:** AB

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asafirepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html#71854>

**Question:** 281

Which two statements about bridge-group interfaces in Cisco FTD are true? (Choose two.)

- A. The BVI IP address must be in a separate subnet from the connected network.
- B. Bridge groups are supported in both transparent and routed firewall modes.
- C. Bridge groups are supported only in transparent firewall mode.
- D. Bidirectional Forwarding Detection echo packets are allowed through the FTD when using bridge-group members.
- E. Each directly connected network must be on the same subnet.

**Answer:** CD

Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/transparent\\_or\\_routed\\_firewall\\_mode\\_for\\_firepower\\_threat\\_defense.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html)

### Question: 282

Which two routing options are valid with Cisco Firepower Threat Defense? (Choose two.)

- A. BGPv6
- B. ECMP with up to three equal cost paths across multiple interfaces
- C. ECMP with up to three equal cost paths across a single interface
- D. BGPv4 in transparent firewall mode
- E. BGPv4 with nonstop forwarding

**Answer:** AC

Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-configguide-v601/fpmc-config-guide-v60\\_chapter\\_01100011.html#ID-2101-0000000e](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-configguide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e)

### Question: 283

Which command is run on an FTD unit to associate the unit to an FMC manager that is at IP address 10.0.0.10, and that has the registration key Cisco123?

- A. configure manager local 10.0.0.10 Cisco123
- B. configure manager add Cisco123 10.0.0.10
- C. configure manager local Cisco123 10.0.0.10
- D. configure manager add 10.0.0.10 Cisco123

**Answer:** D

Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmtnw.html#id\\_106101](https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmtnw.html#id_106101)

### Question: 284

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/fpmc-configguide-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/fpmc-configguide-v64/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html)

### Question: 285

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:** CE

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-routing.html>

**Question: 286**

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

- A. STP
- B. HSRP
- C. GLBP
- D. VRRP

**Answer: A**

Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/firepower\\_threat\\_defense\\_high\\_availability.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/firepower_threat_defense_high_availability.html)

**Question: 287**

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

**Question: 288**

Which interface type allows packets to be dropped?

- A. passive
- B. inline
- C. ERSPAN
- D. TAP

**Answer: B**

Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuringfirepower-threat-defense-int.html>

**Question: 289**

What is the disadvantage of setting up a site-to-site VPN in a clustered-units environment?

- A. VPN connections can be re-established only if the failed master unit recovers.
- B. Smart License is required to maintain VPN connections simultaneously across all cluster units.
- C. VPN connections must be re-established when a new master unit is elected.
- D. Only established VPN connections are maintained when a new master unit is elected.

**Answer: C**

Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-clustersolution.html#concept\\_g32\\_yml\\_y2b](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-clustersolution.html#concept_g32_yml_y2b)

For More exams visit <https://killexams.com/vendors-exam-list>



*Kill your exam at First Attempt....Guaranteed!*