

Cisco.300-710.v2024-11-21.q123

□□□□:	300-710
□□□□:	Securing Networks with Cisco Firepower
□□□:	Cisco
□□ □□ □□□:	123
□□:	v2024-11-21
# □□ □:	881
# □□ □□□:	1230
https://www.krdump.com/Cisco.300-710.v2024-11-21.q123.html	

NEW QUESTION: 1

□□ □□□□□ □□□ □□□ □□□□□ □□□ □□□□ □□□, □ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□□ □□ □ □□ □□□□□□ □□□□□. □□□□□ □ □□□□□ □□□□□ □□ □□ □□□ □□□ □□□□?

- A. Secure FMC□□ Cisco Secure Endpoint □□□ □□□□ Cisco Secure Endpoint □□□□ □□□ □□□□□.
- B. Cisco Secure Endpoint □□□□ Croats□ □□□□ API □□ □□□□ Cisco Secure AMP □□ □□□□□□.
- C. AMP □□ □□□□ Secure FMC□□ Secure FMC□ Cisco Secure Endpoint □□ □□□ □□□□□.
- D. Cisco Secure Endpoint □□□□ □□□ GUID□ □□□□ Cisco Secure Firewall Management Center(FMC) AMP □□ □□□□□□.

Answer: C (LEAVE A REPLY)

□□□ □□□ □□□□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□□ □□□□□□ □□ □□□□□□ Secure FMC□ AMP □□ □□□□□ □□□□□ □□□□□ Cisco Secure Endpoint(□□□ AMP for Endpoints) □□ □□□ □□□□□ □□□.

□□:

- * FMC□□ □□ > □□ □□□ □□□□□.
- * □□□ □□□□□ AMP □□□ □□□□□.
- * □□□ API □□ □□□ □□□□□ FMC□ Cisco Secure Endpoint □□□ □□□□ □□□ □□□□□.
- * □□□ □□□ □□ □□ □□□□□ □□□□□ □□□□ □□ FMC□□ □□ □□ □□□ □□□ □ □□ □□ □□□ □□□ □ □□□ □.

□□□ □□ □□□ □□□□□ □□□□□ □□□ □□□□ □□ □□□□□□ □□□□ □□□□□ □□□□□, □□ □□□□ □□□ □□□□ □ □□□ □□□ □□□ □□□□□.


□□ □□: Cisco Secure Firewall Management Center □ Cisco Secure Endpoint Integration Guide.

NEW QUESTION: 2

□□□□ □□□□ □□ □□ □□ □□ □□□□ □□□□ □□ □□ 2 □□□□ □□□□ □□□ □□□□ □□□□□□. □□□□ □ □□ □□□ □□ □ □□□ □□ □□□ □□ □□ □□ □□ □□ Cisco FMC □□□ □□□ □□□□ □□□?

- A. □□ > □□ > Whols
- B. □□ > □□□□ > □□□□ □□□
- C. □□ > □□□ > □□□
- D. □□ > □□□ > □□□ □□

Enter the "configure manager add" command at the CLI of the affected device.	Unregister the device from the active Cisco FMC.
Unregister the device from the standby Cisco FMC.	Enter the "configure manager delete" command at the CLI of the affected device.
Register the affected device on the active Cisco FMC.	Enter the "configure manager add" command at the CLI of the affected device.
Enter the "configure manager delete" command at the CLI of the affected device.	Register the affected device on the active Cisco FMC.
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	



NEW QUESTION: 5

Which two actions should be performed to migrate a Cisco Firepower device to a new Cisco FMC? (Choose two.)

- A. Configure the device with a BVI IP address.
- B. Cisco Firepower device to the new FMC.
- C. Configure the device with a new IP address.
- D. Unregister the device from the active FMC.

Answer: (SHOW ANSWER)

The correct answers are B and D. To migrate a Cisco Firepower device to a new Cisco FMC, you must first unregister the device from the active FMC. Then, you must configure the device to connect to the new FMC. This is done by configuring the device with a BVI IP address and setting the management interface to the new FMC. The other options are incorrect because you do not need to configure a new IP address for the device, and you do not need to configure the device with a BVI IP address before migrating it to the new FMC.

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.h>

NEW QUESTION: 6

Which two actions should be performed to migrate a Cisco Firepower device to a new Cisco FMC? (Choose two.)

- A. Configure the device with a BVI IP address.
- B. Cisco Firepower device to the new FMC.
- C. Configure the device with a new IP address.
- D. Unregister the device from the active FMC.
- E. Register the device on the new FMC.

Answer: (SHOW ANSWER)

□□:

Which of the following is a Cisco Firepower module feature? (Choose two.)

- A. IPS signature sets
- B. Global threshold
- C. Signature sets
- D. Signature sets
- E. Signature sets

Answer: (SHOW ANSWER)

00: 00

00/00: <https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Global-Threshold.pdf>

NEW QUESTION: 12

Which of the following is a Cisco Firepower module feature? (Choose two.)

- A. Signature sets
- B. Signature sets
- C. Signature sets
- D. Signature sets

Answer: D (LEAVE A REPLY)

00:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdmintrusion.html>

NEW QUESTION: 13

Which of the following is a Cisco IPS module feature? (Choose two.)

- A. Signature sets
- B. Signature sets
- C. Signature sets
- D. Signature sets

Answer: A (LEAVE A REPLY)

NEW QUESTION: 14

Which of the following is a Cisco FTD module feature? (Choose two.)

- A. Snort signature sets
- B. Signature sets
- C. VPN signature sets
- D. VPN signature sets

Answer: (SHOW ANSWER)

NEW QUESTION: 15

Which two Cisco FTD configurations are required to allow traffic from 10.50.120.0/24 to reach the Cisco FTD? (Choose two.)

- A. Cisco FTD IPv4 IP address configuration.
- B. Cisco FTD IPv4 IP address configuration.
- C. Cisco FTD IPv4 IP address configuration.
- D. Cisco FTD IPv4 IP address configuration and IPv6 IP address configuration.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 16

Which two Cisco ASA configurations are required to allow traffic from the Cisco ASA to reach the Cisco FTD? (Choose two.)

- A. Cisco ASA IPv4 IP address configuration and Cisco FTD IPv4 IP address configuration.
- B. Cisco ASA IPv4 IP address configuration and Cisco FTD IPv4 IP address configuration.
- C. Cisco FTD IPv4 IP address configuration and Cisco ASA IPv4 IP address configuration.
- D. Cisco FTD IPv4 IP address configuration and Cisco ASA IPv4 IP address configuration.

Answer: B (LEAVE A REPLY)

300-710 Cisco dumps and questions available at DumpTop. Visit <https://www.dumptop.com/Cisco/300-710-dump.html> (445 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 17

Which two Cisco Firepower 9300 configurations are required to allow traffic from the Cisco Firepower 9300 to reach the Cisco FTD? (Choose two.)

- A. FMC CLI
- B. FTD CLI
- C. FXOS CLI
- D. FMC GUI

Answer: C (LEAVE A REPLY)

Which two Cisco Firepower 9300 configurations are required to allow traffic from the Cisco Firepower 9300 to reach the Cisco FTD? (Choose two.)

- A. Cisco Firepower 9300 IPv4 IP address configuration and Cisco FTD IPv4 IP address configuration.
- B. Cisco Firepower 9300 IPv4 IP address configuration and Cisco FTD IPv4 IP address configuration.
- C. Cisco Firepower 9300 IPv4 IP address configuration and Cisco FTD IPv4 IP address configuration.
- D. Cisco Firepower 9300 IPv4 IP address configuration and Cisco FTD IPv4 IP address configuration.

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html

NEW QUESTION: 21

Which two Cisco FTD components are used to manage the configuration of the Cisco FTD devices? (Choose two.)

- A. Cisco FTD configuration files
- B. Cisco FTD configuration database
- C. Cisco FTD configuration templates
- D. Cisco FTD configuration scripts

Answer: (SHOW ANSWER)

NEW QUESTION: 22

Which two Cisco FTD components are used to manage the configuration of the Cisco FTD devices? (Choose two.)

- A. Cisco FTD configuration files
- B. Cisco FTD configuration database
- C. Cisco FTD configuration templates
- D. Cisco FTD configuration scripts

Answer: D (LEAVE A REPLY)

NEW QUESTION: 23

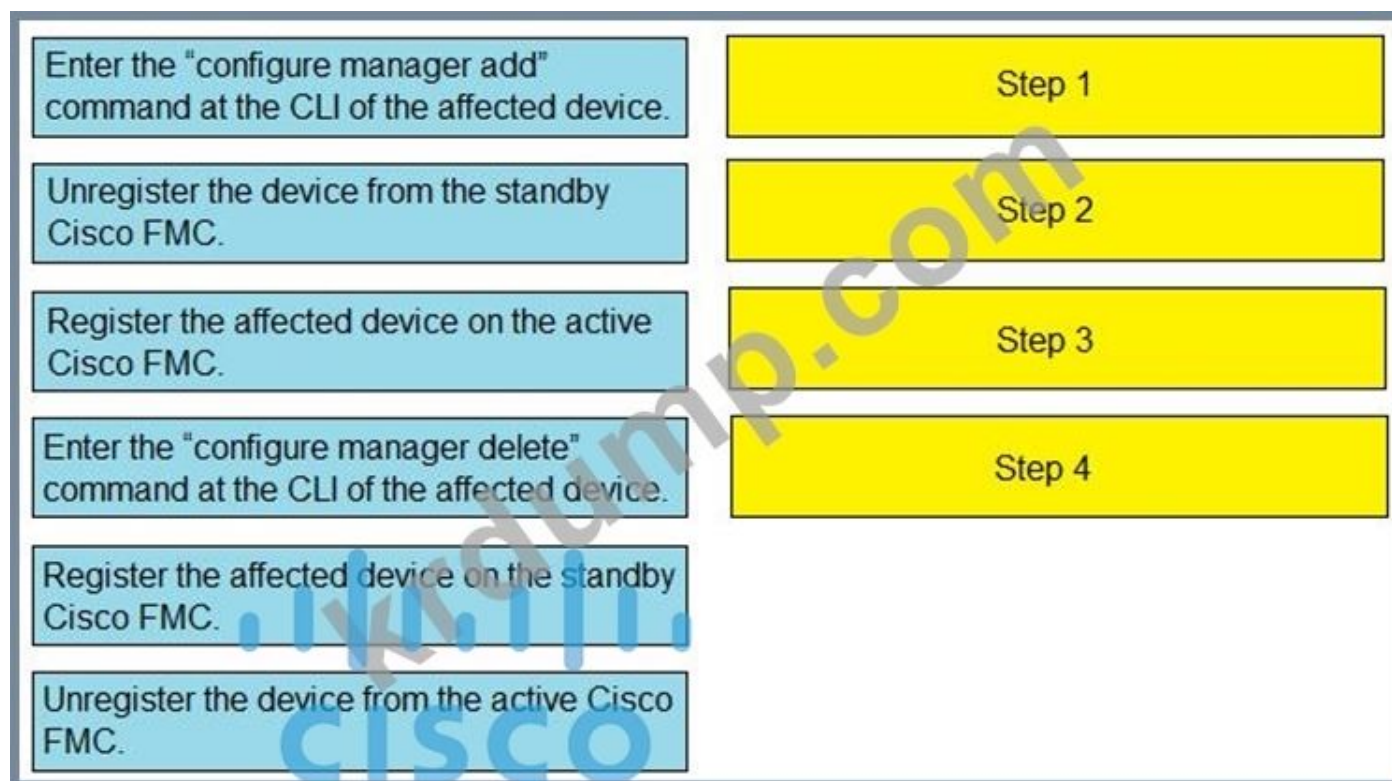
Which two Cisco FTD components are used to manage the configuration of the Cisco FTD devices? (Choose two.)

- A. Cisco FTD configuration files
- B. Cisco FTD configuration database
- C. Cisco FTD configuration templates
- D. Cisco FTD configuration scripts

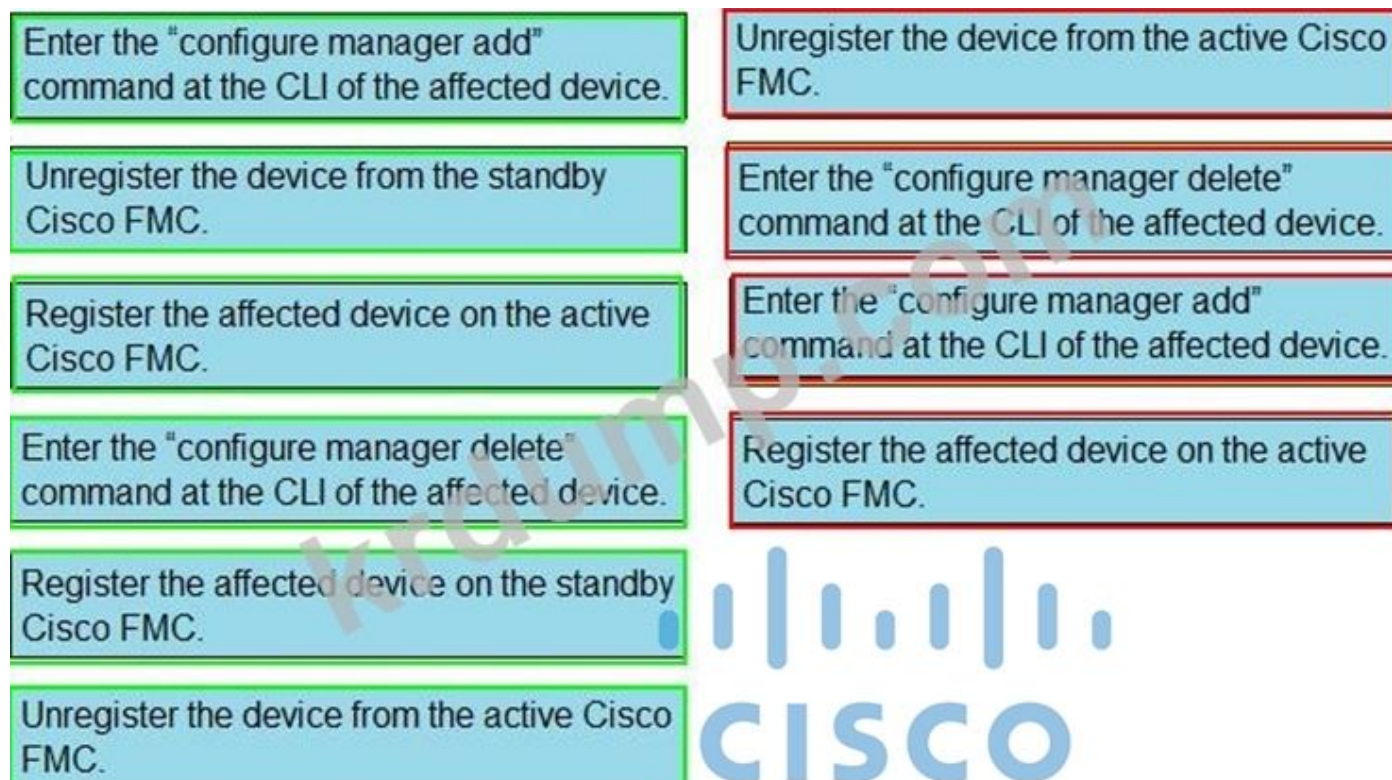
Answer: (SHOW ANSWER)

NEW QUESTION: 24

Which two Cisco FTD components are used to manage the configuration of the Cisco FTD devices? (Choose two.)



Answer:



NEW QUESTION: 25

□□ □□□ □□□ □□□□ □□ □□□□ □□ 2□□□ 3□□□□ □□□□ □□□ □ □□□□?

A. Cisco Firepower Threat Defense □□

B. □□□ □□

C. □□ □□□ □ □□□

D. □□ □□

Answer: C (LEAVE A REPLY)

Which of the following is a valid configuration for Cisco Firepower Threat Defense (FTD) in Integrated Routing and Bridging (IRB) mode? (Choose two.)

A. interface eth0/23 ip address 10.10.10.1 255.255.255.0

B. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects

C. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables

D. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables no ip redirects

<https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-config-guide/FTD-Config-Guide-v6/Integrated-Routing-and-Bridging.html>

NEW QUESTION: 26

Which of the following is a valid configuration for Cisco FTD CLI in bridge mode?

- A. interface eth0/23 ip address 10.10.10.1 255.255.255.0
- B. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects
- C. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables
- D. WORD

Answer: (SHOW ANSWER)

CC:

https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/ac_1.html

NEW QUESTION: 27

Which of the following is a valid configuration for Cisco Firepower Threat Defense (FTD) in bridge mode? (Choose two.)

A. interface eth0/23 ip address 10.10.10.1 255.255.255.0

B. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects

C. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables

D. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables no ip redirects

- A. interface eth0/23 ip address 10.10.10.1 255.255.255.0
- B. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects
- C. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables
- D. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables no ip redirects

Answer: C (LEAVE A REPLY)

<https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusion.html>

NEW QUESTION: 28

Which of the following is a valid configuration for Cisco FTD in bridge mode? (Choose two.)

- A. interface eth0/23 ip address 10.10.10.1 255.255.255.0
- B. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects
- C. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables
- D. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables no ip redirects
- E. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables no ip redirects no ip redirects

Answer: (SHOW ANSWER)

Which of the following is a valid configuration for Cisco FTD in bridge mode? (Choose two.)

CC:

Which of the following is a valid configuration for Cisco FTD in bridge mode? (Choose two.)

A. interface eth0/23 ip address 10.10.10.1 255.255.255.0

B. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects

C. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables

D. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables no ip redirects

E. interface eth0/23 ip address 10.10.10.1 255.255.255.0 no ip redirects no ip unreachables no ip redirects no ip redirects

FTD can connect to FMC GUI via REST API. FTD can connect to FMC via REST API.
FTD can connect to FMC via REST API.

FTD can connect to FMC via REST API. FTD can connect to FMC via REST API.
FTD can connect to FMC via REST API. FTD can connect to FMC via REST API.
FTD can connect to FMC via REST API. FTD can connect to FMC via REST API.

NEW QUESTION: 29

Cisco FTD can connect to FMC via REST API. FTD can connect to FMC via REST API.
Cisco FTD can connect to FMC via REST API. FTD can connect to FMC via REST API.

- A. BVI IP address is configured on the interface.
- B. BVI IP address is configured on the interface.
- C. BVI IP address is configured on the interface.
- D. BVI IP address is configured on the interface.
- E. BVI IP address is configured on the interface.

Answer: C,D (LEAVE A REPLY)

URL: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

NEW QUESTION: 30

FTD can connect to FMC via REST API. FTD can connect to FMC via REST API.
FTD can connect to FMC via REST API. FTD can connect to FMC via REST API.

- A. PC can capture traffic on the interface.
- B. PC can capture traffic on the interface.
- C. PC can capture traffic on the interface.
- D. PC can capture traffic on the interface.

Answer: C (LEAVE A REPLY)

URL:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc16>

NEW QUESTION: 31

FTD can connect to FMC via REST API. FTD can connect to FMC via REST API.
FTD can connect to FMC via REST API. FTD can connect to FMC via REST API.

- A. Cisco FMC can connect to Cisco FMC via REST API.
- B. Cisco FMC can connect to Cisco Security Packet Analyzer via REST API.
- C. Cisco FMC can connect to Cisco FMC via REST API.
- D. Cisco Security Packet Analyzer can connect to Cisco FMC via REST API.

Answer: D (LEAVE A REPLY)

300-710 <https://www.dumptop.com/Cisco/300-710-dump.html> (445 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 32

Cisco FMC restore remote-manager-backup location 2.2.2.2 admin /Volume/home/admin FTD408566513.zip

- A. .tar .zip
- B.
- C. .cfg
- D. IP

Answer: A (LEAVE A REPLY)

NEW QUESTION: 33

Cisco FTD

- A.
- B. Cisco
- C.
- D.

Answer: (SHOW ANSWER)

NEW QUESTION: 34

Cisco FTD

- A.
- B.
- C.
- D.

Answer: (SHOW ANSWER)

NEW QUESTION: 35

Cisco FMC

- A.
- B. Cisco FMC GUI
- C.
- D.

Answer: C (LEAVE A REPLY)

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/reusable_objects.html

NEW QUESTION: 36

Which Cisco FMC component is used to manage Cisco FTD devices? A. Cisco ISE B. Cisco ICM C. Cisco ISE D. Cisco ICM

- A. Cisco ISE
 - B. Cisco ICM
 - C. Cisco ISE
 - D. Cisco ICM
- Answer: D (LEAVE A REPLY)

NEW QUESTION: 37

Which Cisco FMC component is used to manage Cisco FTD devices? A. Cisco ISE B. Cisco ICM C. Cisco ISE D. Cisco ICM

- A. Cisco ISE
 - B. Cisco ICM
 - C. FMC EIGRP
 - D. Cisco ICM
- Answer: D (LEAVE A REPLY)

NEW QUESTION: 38

Which protocol is used for redundancy in a Firepower cluster? A. STP B. HSRP C. GLBP D. VRRP

- A. STP
 - B. HSRP
 - C. GLBP
 - D. VRRP
- Answer: (SHOW ANSWER)

00:00

00/00: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_threat_defense_high_availability.html

NEW QUESTION: 39

Which Cisco Firepower component is used to manage Cisco FTD devices? A. Cisco ISE B. Cisco ICM C. Cisco ISE D. Cisco ICM

- A. Cisco ISE
 - B. Cisco ICM
 - C. Cisco ISE
 - D. Cisco ICM
- Answer: (SHOW ANSWER)

NEW QUESTION: 40

Which Cisco Firepower component is used to manage Cisco FTD devices? A. Cisco ISE B. Cisco ICM C. Cisco ISE D. Cisco ICM

- A. Cisco ISE

Which of the following is a Cisco ASA feature? Cisco FTD is a Cisco ASA feature. Cisco FTD is a Cisco ASA feature. Cisco FTD is a Cisco ASA feature.

- A. Cisco FTD is a Cisco ASA feature.
- B. Cisco ASA is a Cisco FTD feature.
- C. Cisco FTD is a Cisco ASA feature.
- D. Cisco FTD is a Cisco ASA feature.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 44

Which of the following is a Cisco Firepower feature? Cisco FMC is a Cisco Firepower feature. Cisco FMC is a Cisco Firepower feature. Cisco FMC is a Cisco Firepower feature.

- A. Cisco FMC is a Cisco Firepower feature.

<https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusion.html>

- B. Cisco FMC is a Cisco Firepower feature.
- C. Cisco FMC is a Cisco Firepower feature.
- D. Cisco FMC is a Cisco Firepower feature.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 45

Which of the following is a Cisco Firepower feature?

<e ip="72b21ba7b43895c49d775efef3fb0ff1.jpg"></ e>

Which of the following is a Cisco Firepower feature? Cisco Firepower is a Cisco Firepower feature. Cisco Firepower is a Cisco Firepower feature. Cisco Firepower is a Cisco Firepower feature.

- A. Cisco Firepower is a Cisco Firepower feature.
- B. Cisco Firepower is a Cisco Firepower feature.
- C. Cisco Firepower is a Cisco Firepower feature.
- D. Cisco Firepower is a Cisco Firepower feature.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 46

ClientHello is a Cisco ASA feature. ClientHello is a Cisco ASA feature. ClientHello is a Cisco ASA feature.

- A. ClientHello is a Cisco ASA feature.
- B. ClientHello is a Cisco ASA feature.
- C. ClientHello is a Cisco ASA feature.
- D. ClientHello is a Cisco ASA feature.

Answer: D (LEAVE A REPLY)

300-710 <https://www.dumpstoc.com/Cisco/300-710-dump.html> (445 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 47

Which of the following is a valid configuration for Cisco Firepower 2130 FMC? (Choose two.)

- A. FTD on ASA and FMC on FTD
- B. FTD on ASA and FMC on FTD
- C. FTD on ASA and FMC on FTD
- D. FTD on ASA and FMC on FTD

Answer: B (LEAVE A REPLY)

Which of the following is a valid configuration for Cisco Firepower 2130 FMC? (Choose two.)

Which of the following is a valid configuration for Cisco Firepower 2130 FMC? (Choose two.)

NEW QUESTION: 48

Which of the following is a valid configuration for Cisco Firepower Management Center? (Choose two.)

- A. FTD on ASA and FMC on FTD
- B. FTD on ASA and FMC on FTD
- C. FTD on ASA and FMC on FTD
- D. FTD on ASA and FMC on FTD

Answer: B (LEAVE A REPLY)

NEW QUESTION: 49

Which of the following is a valid configuration for Cisco FMC? (Choose two.)

- A. FTD on ASA and FMC on FTD
- B. TCP, UDP, ICMP on FTD
- C. FTD on ASA and FMC on FTD
- D. FTD on ASA and FMC on FTD

Answer: B (LEAVE A REPLY)

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html

NEW QUESTION: 50

Which of the following is a valid configuration for Cisco FTD? (Choose two.)

- A. FTD on ASA and FMC on FTD
- B. FTD on ASA and FMC on FTD

C. □□□ □□□□□□ □□□□ □□□

D. □□□ □□ □□□□□□ □□ □□□ □□□□

Answer: B ([LEAVE A REPLY](#))

□□

□□□ □□ □□□ □□□□ Cisco FTD □□□ □□□□□ □□□□□ □□ □□□□□□ □□ □□ □□□ □□□□ □□□. □□ □□ □ FTD □□□ "□□ □ □ □□□" □□ "□□□□ □□□" □□□ □□ □□□ □□□ □□ □□□ □□□ □□ □□□ □□□□ □□ □□□ □□□□. □□ □□□□ FTD □□□ IP □□ □□ □□□ □□1□ □□□□ □□ □□ □□ □□□□ □□□□ □□□□ □□ □□ □□□□ □ □□ □□□□□□. □□ □□□□□□ FTD □□□ □□□□ □□ □□□□ □□□ □□□□□ □□□□ □□ □□□□□□□□ □□ □□□□□□ □□ □□□ □□ SSH □□□□ □□□□□ □□□ □ □□□, □□ Telnet2□□ □ □□□□□□.

□□ □□□ □□□ □□ □□□ □□□□ □□□□.

□□□ □□□ FTD □□□ □□□ □□□ □□ □□□ □□□□□ □□ □□ □□ □ □□□□ □□□□ □□□ □□□□□□. □□□ □□ □ IP □□ □□ □□□ □□1□ □□□□ □□ □□ □□ □□□□ □□□ □ □□ □□□□ □□□ □□□□□□. □□ □□□□□□ FTD □□□□ □□ □□ □ □□□ □□□ □□□□□□□□□□. □□ □□□□□□ □□ □□□□ □□□ □□□□□□ □□□□ □ □□ □□□ □□ SSH □□□□ □□□□ □□□□.

□□□ □□□□□□ □□ □□ □□□ □□ □□□□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□□. □□□ □□□□□□ FTD □□□□ □□□□ □□□□ □□□□ □ □□□□ □□ □□□□□□□□□□. □□□ □□□□□□ □□ □□□ □□ SSH □□□□ □ □□□ □□□□2.

□□□ □□ □□□□□(BVI)□ □□ □□□ □□□ □□ □□□□ □□□ □□□□ □□ □□ □□□□ □□□□ □□ □□□ □□□□ □ □□□. BVI□ □□□ □□□ 2 □□□□□□□ □□□□ □□□ □□ □□□ □□□ □□ □□□ □□□□□□ □□ □□□□ □□□ □□ □□□ □□□□□□□□□□. BVI□ □□□□ FTD □□□ □□□□ □□ □□/□□□□□ □□ □□□ □□ □□ □□□□ □ □□□□□. □□□ □ □□ □□□ □□□ IP □□ □□ □□□ □□ □□□ □□ □□ □□□□ □□□ □ □□ □□□□ □□□ □□□□□□.

NEW QUESTION: 51

□□ □□ □□□□ □□□□□□□□□□ □□ □□□ □□□□, □□ □□ □□□□□□ □□□□ □□□ □□□□□□□□. □□□□□ □□□□□□ □□□□ □□□□□□ □□ □□□□□□□□ Cisco FMC □□□ □□□ □□□□ □□□□?

- A. □□ □□
- B. □□ □□□ □□
- C. □□ □□
- D. □□ □□

Answer: D ([LEAVE A REPLY](#))

□□□:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_policies_and_advanced_malware_protection.html#ID-2199-000005d8

NEW QUESTION: 52

Cisco Firepower□□ □□□□ □□□ □□ □□□□ □□□□□□?

- A. □□□ □ □□□ □□□ □□□ □□ □□□ □□□ □ □□□□□.
- B. □□□ □ □□□ □□ □□□ □□□□□□.
- C. □□□ □□□ □□ □□□□ □□□ □ □□□□□.
- D. □□□ □□□□□□ SSL □□ □□□ □ □ □□□□□.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 53

- □□ □□□ □□□□ Cisco FTD□ □□ □□ □□□ □□□□□□.
- Cisco FTD □□□ □□□□ □□ □□□ □□ □□□ □□□ Short □□ □□□ □□ □□□□. capture-traffic □□□ □□□ □□ □□□ □□□□□. □□ □□□ □ □□□ □□□□□?
- A. □□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□□.
 - B. capture-traffic □□ □□ -T □□□ □□□□ □□□ □□□□□.
 - C. Cisco FTD CLI □□ Cisco FMC GUI□□ □□□ □□□□□.
 - D. capture-traffic □□□ □□□ verbose □□□ □□□□□.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 54

- □□ Cisco FMC□ □□□ Cisco FTD □□□ □□□ □□□ 10□ □□□ □□□□ □□□□.
- 10.50.12. □□□□ □□ □□ □□□ □□□□□□□□ □□□, □□□□□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□ □□ □□□□ □□□□. □□□□□ □□□ □□ □□□ □□□□ Cisco FTD□□ Cisco FMC□□ □□□ □□□ □ □□□ □□ □□ □□ □□ □□ □□□?
- A. Cisco FMC□ IPv4 IP □□□ □□□□ □□□ □□□□ □□□□.
 - B. Cisco FMC□ □□□ □□□□ □□ □□□□□.
 - C. Cisco FM□ □□□ □□□□ □□□□□□.
 - D. Cisco FMC□□ □□□ □□□□ □□ IFV4□□ IPv6□ IP □□□ □□□□□□□.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 55

- Cisco Threat Response□□ AMP□ □□□ □□□□ □□□□□ □□□ □□□ □□ □□□ □□□ □□□?
- A. □□ □□□ □□ □□□ □□□□□.
 - B. □□ □□□ □□ Cisco□ □□□□ □□□□.
 - C. □□ □□□ □□ □□ □□ □□□□ □□□□□.
 - D. Cisco Threat Response□ □□□□ □□□□ □□□ □□□ □□□□□.

Answer: ([SHOW ANSWER](#))

□□: □□

NEW QUESTION: 56

□□□ □□□□□.

II. ASSESSMENT RESULTS

AUTOMATING THE TUNING EFFORT

During the assessment period, the following changes to your network were observed.

NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	310
A new host was added to the network	366
A device started using a new transport protocol	381
A device started using a new network protocol	373

- □□ □□ □□□□ □□□ □□ □□□□□□ □□□ □□ □□□ 300□ □□ □□□□□□□□. □□□ □□□ □□ □□□ □ □□□ □□ □□□□□□□□?
- A. Cisco Firepower□ □□□ □□□□ □□□□□□□□.
 - B. □□□□ Cisco Firepower□□ □□ □□ □□ □□□□ □□□□□□.
 - C. Cisco Firepower□ □□□ □□□□□□□ □□ □□ □□□ □□□□□□.
 - D. □□□□ □□□□ □□□ □□□□□□□□.

Answer: (SHOW ANSWER)

□□
□□:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Tailori>

NEW QUESTION: 57

□□ □□□ □□□ □□ □□□ □□ □□□□ □□□ □□□□ □□□□□□□□. □□□□ □□ □□ □□□□ □□□□ □□□□ □□□ □□□ □□□□□□ □□□ □ □□ □□□□ □□□□□ □□□ □□□□□□. □ □□□ □□□□ □□ □□ □□ □□□ □□□□ □□□□ □□□?

- A. □□□ □□□ □□ □□□ □□□□□ □□□□ □□ Cisco FTD □□□□□□□□ □□□□□□.
- B. VPN □□ □□□ □□□□ □□ Cisco FTD □□□□□□□□ □□□□ □□□ □□□□□□.
- C. □□ □□□ □□ □□ Cisco FTD HA □□ □□□□□□.
- D. □□ □□□ □□ □□□□□ □□□□ □□ Cisco FTD HA □□ □□□□□□.

Answer: A (LEAVE A REPLY)

□□:

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept_C8502505F840451C9E600F1EED9BC18E

NEW QUESTION: 58

□□□□□ Cisco FMC□□ Cisco FTD □□□ □□ URL □□□□ □□□□ □□□□. □□□□ http://www.Dac'additstte.com□ □□□□ □ □□□ □□□ □□, □□□ □□ □□□□□ □□ □□□ □ □□ □□□ □□□□□□. □□ □□□□□ □□□□□□□□ □ □□□. □□□□□ □□□ □□ □□□ □□□□ □□ □□□ □□ □ □□ □□□ □□□□□□? (□ □□ □□□□□.)

- A. □□□ □□ □□ □□□□ HTTP □□ □□□ □□ □□ □□□□ □□□ □□□□ □□□□□□.
- B. □□□ □□ □□ □□□□ HTTP □□ □□□ □□□ □□ □□ □□□□ □□□ □□□□□ □□□□□□.

C. Cisco AMP can be configured to block traffic to and from specific URLs.

D. Cisco AMP can be configured to block traffic to and from specific URLs.

E. <http://www.badadultsite.com> URL can be configured to block traffic to and from specific URLs.

Answer: B,E (LEAVE A REPLY)

CC

Cisco FMC can be configured to block traffic to and from specific URLs.

Cisco AMP can be configured to block traffic to and from specific URLs.

Cisco AMP can be configured to block traffic to and from specific URLs.

1. Cisco AMP can be configured to block traffic to and from specific URLs.

CC

<http://www.badadultsite.com> URL can be configured to block traffic to and from specific URLs.

URL can be configured to block traffic to and from specific URLs.

1. Cisco AMP can be configured to block traffic to and from specific URLs.

Cisco AMP can be configured to block traffic to and from specific URLs.

Cisco AMP can be configured to block traffic to and from specific URLs.

. Block Response Page can be configured to block traffic to and from specific URLs.

Cisco AMP can be configured to block traffic to and from specific URLs.

Cisco AMP can be configured to block traffic to and from specific URLs.

URL can be configured to block traffic to and from specific URLs.

1. Cisco AMP can be configured to block traffic to and from specific URLs.

CC

<http://www.badadultsite.com> URL can be configured to block traffic to and from specific URLs.

1.

NEW QUESTION: 59

Cisco AMP can be configured to block traffic to and from specific URLs?

A. Cisco AMP can be configured to block traffic to and from specific URLs.

B. Cisco AMP can be configured to block traffic to and from specific URLs.

C. Cisco AMP can be configured to block traffic to and from specific URLs.

D. Cisco AMP can be configured to block traffic to and from specific URLs.

Answer: B (LEAVE A REPLY)

CC: CC

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

NEW QUESTION: 60

Cisco Firepower High Availability can be configured to block traffic to and from specific URLs.

Cisco Firepower High Availability can be configured to block traffic to and from specific URLs?

A. Cisco Firepower High Availability can be configured to block traffic to and from specific URLs.

B. Cisco Firepower High Availability can be configured to block traffic to and from specific URLs.

- C. □ □□□ □□□ □□□□□ □□□ □□□□□.
- D. □□ □ □□ □□ □□ MAC □□□ □□□□□.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 61

□□ Firepower □□□ □□□□ □□□□ □□□ □□□□ □□□□ □□□ □□□□□ □□ □□□ 2 □□□ □□□ □ □□□ □?

- A. FlexConfig
- B. □□□□□
- C. BDI
- D. □□

Answer: B ([LEAVE A REPLY](#))

300-710 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ 300-710 □□! DumpTop □ □□ **300-710** □□ □□□ □□□□ □□, DumpTop 300-710 □□ □□□ □□□□□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop 300-710 □ □□ □□□□□. <https://www.dumptop.com/Cisco/300-710-dump.html> (445 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 62

□□□□□ Cisco FTD □□□□□□□ IPS □□ □□□ □□□□ □□□ fail-to-wire □□□□□□ □□□□ □□□. □□□ □□ □□□ □□□□□ □□ □□□□□ □□□ □□□□ □□□?

- A. □□
- B. □□□□
- C. □□□
- D. □□□ □□

Answer: D ([LEAVE A REPLY](#))

□□: <https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/inline>

NEW QUESTION: 63

□□ Cisco FTD □□□ CLI□□ □□□□ □□□ □□□□□ □□□□ □□ □□□□ □□□ □□□□□?

- A. □□□□ □□ □□
- B. □□□□ □□□□ □□
- C. □□□ □□ □□□□ □□
- D. □□□□ □□ □□ □□

Answer: B ([LEAVE A REPLY](#))

□□: https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_threat_defense_high_availability.html

NEW QUESTION: 64

Which of the following is the correct sequence of steps to migrate a device from a standby Cisco FMC to an active Cisco FMC?

Enter the "configure manager add" command at the CLI of the affected device.	Step 1
Unregister the device from the standby Cisco FMC.	Step 2
Register the affected device on the active Cisco FMC.	Step 3
Enter the "configure manager delete" command at the CLI of the affected device.	Step 4
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	

Answer:

Enter the "configure manager add" command at the CLI of the affected device.	Unregister the device from the active Cisco FMC.
Unregister the device from the standby Cisco FMC.	Enter the "configure manager delete" command at the CLI of the affected device.
Register the affected device on the active Cisco FMC.	Enter the "configure manager add" command at the CLI of the affected device.
Enter the "configure manager delete" command at the CLI of the affected device.	Register the affected device on the standby Cisco FMC.
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	

NEW QUESTION: 65

Which of the following is the correct sequence of steps to migrate a device from a standby Cisco Firepower IPS to an active Cisco Firepower IPS?

- A. Unregister the device from the active Cisco Firepower IPS, enter the "configure manager delete" command at the CLI of the affected device, register the affected device on the standby Cisco Firepower IPS, and enter the "configure manager add" command at the CLI of the affected device.
- B. Register the affected device on the standby Cisco Firepower IPS, enter the "configure manager delete" command at the CLI of the affected device, unregister the device from the active Cisco Firepower IPS, and enter the "configure manager add" command at the CLI of the affected device.
- C. Enter the "configure manager delete" command at the CLI of the affected device, register the affected device on the standby Cisco Firepower IPS, unregister the device from the active Cisco Firepower IPS, and enter the "configure manager add" command at the CLI of the affected device.
- D. Register the affected device on the standby Cisco Firepower IPS, unregister the device from the active Cisco Firepower IPS, enter the "configure manager delete" command at the CLI of the affected device, and enter the "configure manager add" command at the CLI of the affected device.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 66

Which command is used to configure NAT on a Cisco IOS router? (Choose two.)

- A. ip nat inside
- B. ip nat outside
- C. ip nat enable
- D. ip nat configuration

Answer: B ([LEAVE A REPLY](#))

Which command is used to configure NAT on a Cisco IOS router? (Choose two.)

NEW QUESTION: 67

Which command is used to configure NAT on a Cisco IOS router? (Choose two.)

- A. ip nat inside
- B. ip nat outside
- C. ip nat enable
- D. ip nat configuration
- E. ip nat configuration

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 68

Which command is used to configure NAT on a Cisco IOS router? (Choose two.)

- A. ip nat inside
- B. capture-traffic
- C. capture-traffic
- D. Cisco FTD CLI

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 69

Which command is used to configure NAT on a Cisco IOS router? (Choose two.)

- A. 64MB
- B. 1GB
- C. 10GB

D. 100GB

Answer: (SHOW ANSWER)

Which of the following is a valid configuration for a Cisco Secure Firewall Threat Defense (FTD) device with a 24-core processor and 32MB of RAM?

Options:

* FTD device with 1GB of RAM and 24-core processor.

* FTD device with 1GB of RAM and 24-core processor.

* FTD device with 1GB of RAM and 24-core processor.

* FTD device with 1GB of RAM and 24-core processor.

NEW QUESTION: 70

Which of the following is a valid configuration for a Cisco Secure Firewall Threat Defense (FTD) device with a 24-core processor and 32MB of RAM? (Choose two.)

A. 1GB of RAM, 24-core processor

B. 1GB of RAM, 24-core processor

C. 1GB of RAM, 24-core processor

D. 1GB of RAM, 24-core processor

E. 1GB of RAM, 24-core processor

Answer: (SHOW ANSWER)

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

NEW QUESTION: 71

Which of the following is a valid configuration for a Cisco FMC device with a 24-core processor and 32MB of RAM?

A. 1GB of RAM, 24-core processor

B. 1GB of RAM, 24-core processor

C. 1GB of RAM, 24-core processor

D. 1GB of RAM, 24-core processor

Answer: D (LEAVE A REPLY)

Options: 1GB of RAM, 24-core processor

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

NEW QUESTION: 72

Which of the following is a valid configuration for a Cisco FMC device with a 24-core processor and 32MB of RAM? (Choose two.)

A. 1GB of RAM, 24-core processor

B. 1GB of RAM, 24-core processor

C. Cisco FMC with 1GB of RAM and 24-core processor.

D. Cisco FMC with 1GB of RAM and 24-core processor.

Answer: (SHOW ANSWER)

□□:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

NEW QUESTION: 73

□□□□ □□□ □□□ □□□□ Cisco IPS□ □□ □□ □□□ □□ □□□□ □□□□ □□□□. Cisco IRS□□ □□□□ □□□□ □, □□□□ □□□ □□□□ □□□□ □□□ □□□□□?

- A. □□□ □□□□ □□□□ □□□□ □□□□□.
- B. Cisco IPS □□ □□□□□□□ □□□□□.
- C. Cisco IPS □□□ □□□□ □□ □□□□□.
- D. □□□ □□ Cisco ASA □□□□□□□ □□ □□□□□□□.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 74

Cisco FTD □□□□□□□ □□□□□□ □□ □□□ □□□□□□?

- A. □□ □□□ □□□ □□ □□□ □□□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□□□.
- B. □□□ □□□□ □□ □□□ □ □□□□ □□□□□.
- C. □□□ □ VPN □□□ □□□ □□□□ □□□□□, □□□ □□□ □□□ □□□□ □□ VPN □□□ □□□□□.
- D. □□ Firepower □□□□□□□□ Cisco FTD □□□□□□□ □□□ □ □□□□.

Answer: ([SHOW ANSWER](#))

□□:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/□□□□□□□□ □□ □□□□□ □.html>

NEW QUESTION: 75

□□□□ □□□□□ Active/Standby □□ □□□ Cisco Secure Firewall ASA□ Cisco Secure Firewall Threat Defense Virtual □□□□□ □ □□□ □□□ □□□□□. □□ □□□□ □□□ □□□□ □ □□ □□ □□□ □□□□□? (□ □□□ □□□□□.)

- A. KVM
- B. Azure
- C. ESXi
- D. AWS
- E. □□□□

Answer: C,D ([LEAVE A REPLY](#))

Cisco Secure Firewall Threat Defense Virtual(FTDv) □□□□□□□ □□ □□ □□□□ □□□□(HA) □□□ □□□□□. HA □□□ □ □□□ □□□ □□□ □□□□.

* ESXi: VMware□ ESXi□ HA □□□□□ FTDv □□□□□□□□ □□□□ □ □□ □□□□ □□□□□□□.

* AWS: Amazon Web Services(AWS)□ FTDv □□□□□□□□ □□□□□ HA □□□ □□□□ □□□□ □□ □ □□□□ □□□□ □□□ □□□.

□□□ □□□ FTDv □□□□□□□□ □□□□ □□ □□□ □□□□ □ □□□ □□□□ □□□ □□□□□.

□□ □□: Cisco Secure Firewall Threat Defense Virtual Configuration Guide, □□□□ □ □□ □□□□□ □□ □□.

NEW QUESTION: 76

Which of the following are supported by Cisco Firepower Threat Defense?

- A. IPv6
- B. IPv4
- C. Cisco Firepower Threat Defense
- D. IPv4

Answer: C ([LEAVE A REPLY](#))

300-710 Cisco Security Fundamentals Exam DumpTop Cisco Security Fundamentals Exam 300-710! DumpTop Cisco Security Fundamentals Exam **300-710** Cisco Security Fundamentals Exam, DumpTop 300-710 Cisco Security Fundamentals Exam Cisco Security Fundamentals Exam. Cisco Security Fundamentals Exam DumpTop 300-710 Cisco Security Fundamentals Exam. <https://www.dumptop.com/Cisco/300-710-dump.html> (445 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 77

Which of the following is a feature of Cisco Secure Firewall Management Center (FMC) 6.2.3? (Choose two.)

- A. REST API
- B. TAXII URL
- C. 7GB RAM
- D. TAXII

Answer: ([SHOW ANSWER](#))

Threat Intelligence Director (TID) is a feature of Cisco Secure Firewall Management Center (FMC) 6.2.3.

- * FMC 6.6: FMC Threat Intelligence Director (TID) is a feature of FMC 6.6.
- * TAXII URL: Threat Intelligence Director (TID) TAXII (Trusted Automated eXchange of Indicator Information) URL is a feature of FMC TID.
- * FMC 6.6: FMC 6.6 is a feature of FMC 6.6.
- * FMC 6.6: FMC 6.6 is a feature of FMC 6.6.
- * TAXII URL: TAXII URL is a feature of TAXII.

NEW QUESTION: 78

Which of the following is a feature of Cisco FTD?

- A. BVI
- B. IPv6

- C.
- D.
- E.

Answer: A,C ([LEAVE A REPLY](#))

NEW QUESTION: 79

Which of the following Cisco Firepower Layer 7 protocols are supported by the Cisco Firepower Management Center (FMC)?

- A. HTTP
- B. FTP
- C. SMTP
- D. TCP

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 80

Which of the following Cisco Threat Response features are supported by the Cisco Firepower Management Center (FMC)?

- A. Signature-based detection
- B. Anomaly-based detection
- C. Behavior-based detection
- D. Signature-based detection and anomaly-based detection

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 81

Which of the following Cisco Firepower Management Center (FMC) features are supported by the Cisco Firepower Management Center (FMC)?

- A. Signature-based detection
- B. Anomaly-based detection
- C. Behavior-based detection
- D. Signature-based detection and anomaly-based detection

Answer: D ([LEAVE A REPLY](#))

URL:

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

NEW QUESTION: 82

Which of the following Cisco Firepower Management Center (FMC) features are supported by the Cisco Firepower Management Center (FMC)?

- A. Signature-based detection
- B. Anomaly-based detection
- C. Behavior-based detection
- D. Signature-based detection and anomaly-based detection

Answer: ([SHOW ANSWER](#))

URL:

NEW QUESTION: 83

Which two actions can be performed by the Cisco Firepower Threat Defense (FTD) engine? (Choose two.)

- A. IPS
- B. Sniff
- C. Packet capture
- D. NetFlow
- E. NetFlow

Answer: **A,C** ([LEAVE A REPLY](#))

👤:

<https://www.cisco.com/c/en/us/td/docs/security/piresight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/541-0101.pdf>

NEW QUESTION: 84

Cisco FMC can be used to manage which of the following? (Choose two.)

- A. Cisco FTD
- B. Cisco ISE
- C. Cisco Duo
- D. Cisco Duo

Answer: **(SHOW ANSWER)**

NEW QUESTION: 85

Which two actions can be performed by the Cisco FTD engine? (Choose two.)

- A. Cisco FTD can be used to manage Cisco ISE.
- B. Cisco FTD can be used to manage Cisco Duo.
- C. Cisco FTD can be used to manage Cisco Duo.
- D. Cisco FMC can be used to manage Cisco Duo.

Answer: **A** ([LEAVE A REPLY](#))

NEW QUESTION: 86

Which two actions can be performed by the Cisco Secure Firewall Threat Defense (FTD) engine? (Choose two.)

- A. Sniff
- B. NetFlow
- C. NetFlow
- D. NetFlow

Answer: **B** ([LEAVE A REPLY](#))

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 89

Configure a Cisco FTD to capture traffic for a specific IP address. The configuration includes the following commands:
`ip address 192.168.7.46 255.255.255.255`
`capture CAP interface outside match ip any 192.168.7.46 255.255.255.255`
Which of the following is true regarding this configuration?

- A. The IP address 192.168.7.46 is not a valid IP address.
- B. The FTD will capture traffic for all IP addresses.
- C. The FTD will capture traffic for the IP address 192.168.7.46 only.
- D. The FTD will capture traffic for the IP address 192.168.7.46 and all other IP addresses.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 90

Which of the following is a valid configuration for a Cisco Firepower module to capture traffic for a specific IP address?

- A. `capture CAP interface outside match ip any 192.168.7.46 255.255.255.255`
- B. `capture CAP interface outside match ip any 192.168.7.46 255.255.255.255`
- C. ERSPAN
- D. `capture CAP interface outside match ip any 192.168.7.46 255.255.255.255`

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 91

Which of the following is a valid configuration for a Cisco Firepower module to capture traffic for a specific IP address?

- A. `capture CAP interface outside match ip any 192.168.7.46 255.255.255.255`
- B. `capture CAP interface outside match ip any 192.168.7.46 255.255.255.255`
- C. ERSPAN
- D. `capture CAP interface outside match ip any 192.168.7.46 255.255.255.255`

Answer: D ([LEAVE A REPLY](#))

URL: <https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/cap.html>

300-710 Cisco 300-710 dumps **DumpTop** Cisco 300-710 dumps! **DumpTop** Cisco 300-710 dumps, **DumpTop** 300-710 dumps **DumpTop** Cisco 300-710 dumps. <https://www.dumptop.com/Cisco/300-710-dump.html> (445 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 92

Cisco FTD 100 BVI 1000 1000 1000 1000000 10000. 10000000 1000 10000 100 VLAN 1000000. Cisco FTD 100 1000 1000 1000000 10000 100000?

- A. 100
- B. 10000
- C. 10000 100000
- D. 100/100 100 100

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 93

10000 1000 100000 100000 10 100 100000 100000 Cisco FMC 100000 1000. 10MB 100 100 100 100 100 1000000 1000000. 10000 1000000 100 Cisco FMC 1000 100000 10000?

- A. 100 10000 100
- B. 100 100
- C. 10000000 1000
- D. 10000 100

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 94

Cisco FTD 1000 100 100000 100 100 100 1000 100000 100000 100 1000000000 100 100000 Snort 100 100 1000 100000?

- A. 100 100000 1000000
- B. 100 100000 100
- C. 100000 100 100
- D. 100 100

Answer: A ([LEAVE A REPLY](#))

Cisco FTD 1000 100 1000 100 100 1000 100000 100 1000 100 100000 100000 100 100000 100000 10000 100000. 100 1000 100 100 100 100 100000 1000000 1000000 100 100 100000 100 100000 1000 10000003. 100 1000 100 1000 100000 100000 100 1000000000 100 100000 Snort 100 100 1000 100000. 100 1000 100 100 100000 100000 100 100000 100 100 1000000 1000, 100 100000 100, URL 100000 1000000000. 100 1000 1000000000 1000 1000 100 1000 1000000000 1000 100000003. 100 1000 1000 100 1000 100000 100000.

* 100 100000 100 1000 100 100000 100 100 1000 1000000. 100 1000 100000 1000 1000 1000 1000000 1000 100 1000 1000 100 1000000. 1000 100 1000 100 1000 100 100 1000 100 10000003.

* Network Discovery Only 1000 100 1000000 Discovery 100000 1000000. 100 1000 100 100000 100000 100 100000 100 Security Intelligence 100000 1000000000 100 100000 100, URL 1000 100 100 1000 1000000000. 100 1000 1000 100 100 100000 100 1000000000 100 1000 1000000000 1000 1000000000 1000 100000003.

* 100 100 1000 100 1000000 100 100 100000 1000000. 100 1000 100 100000 100000 100 100000 100 100 1000 100000, 100 100000 100, URL 1000 100 100 1000 1000000000. 100 1000 1000000000 100 100000 1000 1000000000 100 100 100 1000 100000003.

NEW QUESTION: 95

Which two Cisco FMC components can be used to monitor and protect endpoints? (Choose two.)

- A. Cisco FMC Cisco AMP for Endpoints
- B. Cisco FMC FireAMP Cloud
- C. Cisco FMC SSL
- D. Cisco FMC
- E. Cisco FMC Cisco ThreatGrid

Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 96

Which two Cisco FMC components can be used to monitor and protect endpoints? (Choose two.)

- A.
- B.
- C.
- D.

Answer: (SHOW ANSWER)

NEW QUESTION: 97

Which two Cisco FMC components can be used to monitor and protect endpoints? (Choose two.)

- A. Cisco FMC
- B. NAT VPN
- C. Cisco FMC
- D. Cisco FMC
- E. NAT VPN

Answer: (SHOW ANSWER)

NEW QUESTION: 98

Which two Cisco FMC components can be used to monitor and protect endpoints? (Choose two.)

- A.
- B. OpenDNS
- C. Cisco
- D.

Answer: D (LEAVE A REPLY)

URL:

URL: <https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits>

NEW QUESTION: 99

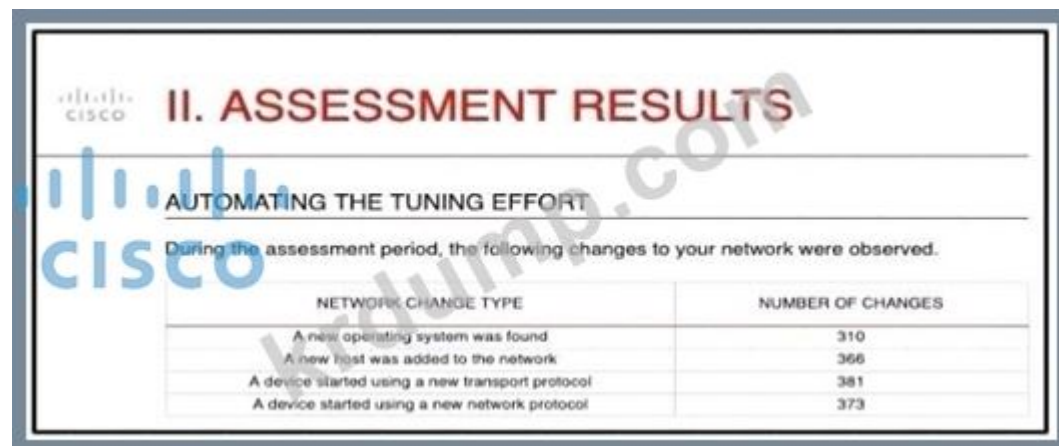
Cisco FMC □□□□ □□□ □□□ □□ □□□ □ □□ □□□□ □□□□ □□ □□□ □□□□□ □□□. □□□□ □□ □□□ □□□ □ □□□ □□□□ □□□?

- A. □□ □□
- B. □□ □□
- C. □□□□ □□ □□
- D. □□ □□ □□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 100

□□□ □□□□□.



The screenshot shows a slide titled "II. ASSESSMENT RESULTS" with the subtitle "AUTOMATING THE TUNING EFFORT". Below the subtitle, it states: "During the assessment period, the following changes to your network were observed." A table follows with two columns: "NETWORK CHANGE TYPE" and "NUMBER OF CHANGES".

NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	310
A new host was added to the network	366
A device started using a new transport protocol	381
A device started using a new network protocol	373

□□□□□ □□ □□ □□□□ □□□ □□ □□□□□□ □□□ □□ □□□ □□□□□□□□. □□□ □□□ □□ □□□ □ □□□□□ □□ □□ □□ □□□□□□□□?

- A. Cisco Firepower□ □□□ □□□□ □□□□□□□□.
- B. □□□□ Cisco Firepower□□ □□ □□ □□ □□□□ □□□□□.
- C. Cisco Firepower□ □□□ □□□□□□ □□ □□ □□□ □□□□□.
- D. □□□□ □□□□ □□□ □□□□□□□□.

Answer: (SHOW ANSWER)

□□
□□:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Tailori>

NEW QUESTION: 101

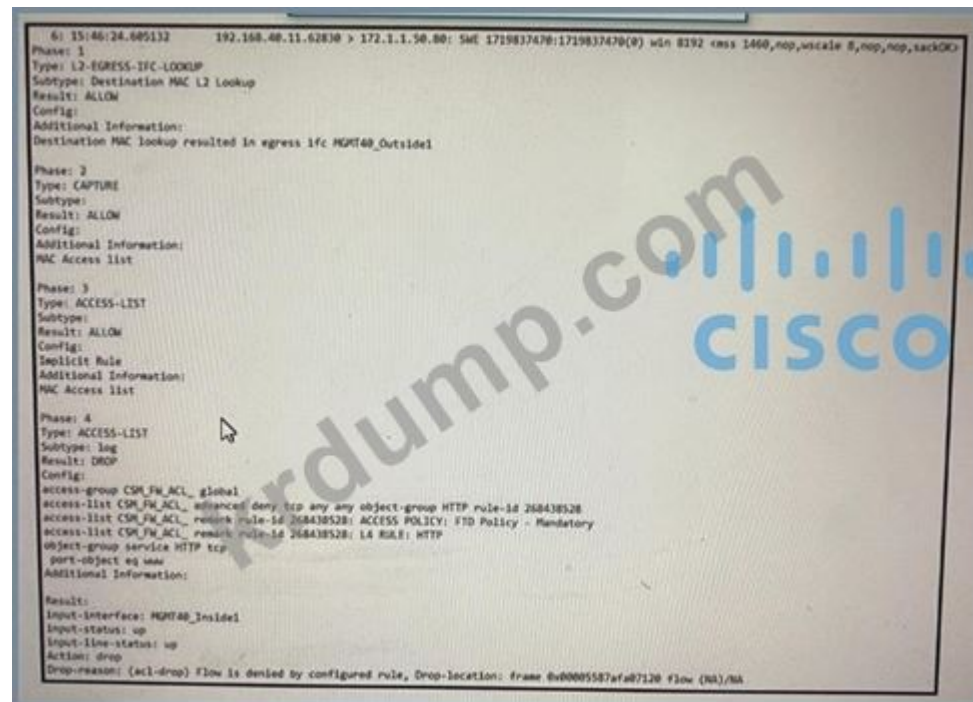
□□□□□ □□□ □□ □□□ □□□□ □□ □ □□□ □□□□□. □□□ □□□ □ □□□ □□□□ □□□□ □□ □□□ □□□ □ □□□□ □□□□□□□□. □ □□□ □□□ □□□□□□?

- A. □□□ □□□ □ □□□□□ □□□□□.
- B. □□□ □□□ □□□□□□ □□□ □□□□□□□□.
- C. □□□ □□ □□□ □□□□□ □□ □□□□.
- D. □□□□ Snort□ □□ □□□ □□ □□□□□□ □□□□□□□□.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 102

□□□ □□□□□.



□□ □□ □□□□□□ □□ □□ □□□□ □□ □□ □□□□ □□ □□ □□□□ □□ □□ □□□□

- A. □□ 80□□ 172.1.1 50□□□ □□□ □□□□ □□ □□ □□ □□□□.
- B. Snort□ □□ 443□ 172.1.1.50□□ □□□□□ □□ □□ □□ □□□□.
- C. □□ 443□ □□□□ 172.1.1 50□ □□□□ □□□ □□ □□ □□ □□□□.
- D. Snort□ □□ 80□□ 172.1.1 50□□□ □□ □□□□□ □□ □□ □□ □□□□□.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 103

□□□□□ □ □□ □□ □□□□□ □□ □□ □ □□ □□ □□□□ □□□□ □□□□□□ □□□□□ □□□□ □□□ □□ □ □□□□□ □□□ □□□□ □□□?

- A. □ □□□ □□ IPS □□□ □□□ □□□□ □□□ □□□□□.
- B. VLAN□ □□ 802 1Q MIME □□ □□□ □□□□□□ □□□□ □□□ □□□ □□□□□.
- C. □ □□ □□□ □□ IDS □□□ □□□□□.
- D. □ □□ □□□ □□ TAP □□□□ □□□ □□ □ □□ □□□□□.

Answer: (SHOW ANSWER)

□□:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/> □□ □□ □□□ □□ □□□ □ □ □ □ □□□□□.html

NEW QUESTION: 104

Syslog□ □□□□ □□ □□ Cisco Firepower □□□ □□ □□□ □□ □□□ □□ Cisco Threat Response□ □□□□ □□ □□□□ □ □□ □□ □□□□□?

- A. □□□□□ □□□ □□□ □□ □ □□ □□□ □□□□ □□□□.
- B. □□□□ Firepower □□□ □□□□ □□ □□□ □□□□□.
- C. □□ □□□ □□□□ □□□ □□□ □□□□.

D. Cisco Firepower Management Center.

Answer: (SHOW ANSWER)

NEW QUESTION: 105

Which Cisco Secure Firewall Management Center (FMC) configuration is required to allow Cisco Secure Firewall Threat Defense (FTD) devices to be managed via SSH? A. Configure the FMC to allow SSH connections from the FTD devices. B. Configure the FMC to allow SSH connections from the FTD devices. C. Configure the FMC to allow SSH connections from the FTD devices. D. Configure the FMC to allow SSH connections from the FTD devices.

A. Cisco

B. Cisco

C. Cisco

D. Cisco

Answer: D (LEAVE A REPLY)

Which Cisco Secure Firewall Threat Defense (FTD) configuration is required to allow Cisco Secure Firewall Management Center (FMC) devices to be managed via SSH? A. Configure the FTD to allow SSH connections from the FMC. B. Configure the FTD to allow SSH connections from the FMC. C. Configure the FTD to allow SSH connections from the FMC. D. Configure the FTD to allow SSH connections from the FMC.

Answer:

* FMC IP > Cisco > Cisco

* Cisco Cisco Cisco Cisco Cisco Cisco

* Cisco Cisco SSH Cisco Cisco

* SSH Cisco Cisco SSH Cisco Cisco Cisco Cisco Cisco Cisco

* Cisco IP Cisco, Cisco Cisco Cisco Cisco Cisco Cisco SSH Cisco Cisco

* Cisco Cisco FTD Cisco Cisco

Cisco Cisco Cisco Cisco Cisco Cisco SSH Cisco Cisco Cisco Cisco Cisco

Answer: Cisco Secure Firewall Management Center Cisco Cisco, Cisco Cisco

NEW QUESTION: 106

Cisco Security Analytics and Logging (SaaS) provides a cloud-based solution for security analytics. How many days of data are retained by default?

A. 60

B. 365

C. 90

D. 120

Answer: C (LEAVE A REPLY)

Cisco Security Analytics and Logging (SaaS) provides a cloud-based solution for security analytics. How many days of data are retained by default?

A. Cisco Security Analytics and Logging (SaaS) provides a cloud-based solution for security analytics. How many days of data are retained by default? B. Cisco Security Analytics and Logging (SaaS) provides a cloud-based solution for security analytics. How many days of data are retained by default? C. Cisco Security Analytics and Logging (SaaS) provides a cloud-based solution for security analytics. How many days of data are retained by default? D. Cisco Security Analytics and Logging (SaaS) provides a cloud-based solution for security analytics. How many days of data are retained by default?

Answer: Cisco Security Analytics and Logging (SaaS) provides a cloud-based solution for security analytics. How many days of data are retained by default?

300-710 CCNAs dumps Cisco 300-710! DumpTop 300-710 dumps, DumpTop 300-710 CCNAs dumps. <https://www.dumpst.com/Cisco/300-710-dump.html> (445 Q&As Dumps, 30%OFF Special Discount: **KrDump**)

NEW QUESTION: 107

IP 10.0.0.10 Cisco123 FMC FTD

- A. 10.0.0.10 Cisco123
- B. Cisco123 10.0.0.10
- C. Cisco123 10.0.0.10
- D. 10.0.0.10 Cisco123

Answer: D (LEAVE A REPLY)

https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#id_106101

NEW QUESTION: 108

QoS

- A.
- B.
- C.
- D.

Answer: B (LEAVE A REPLY)

CC: CC

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/quality_of_service_qos.pdf

NEW QUESTION: 109

()

- A.
- B.
- C.
- D.
- E.

Answer: A,B (LEAVE A REPLY)

CC:

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

NEW QUESTION: 110

Cisco FTD

- A.

- B.
- C.
- D.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 111

Which configuration command is used to enable the Cisco Firepower Threat Defense (FTD) device to receive updates from the Cisco Security Intelligence Center (SIC)?

- A. `IPS update enable`
- B. `update enable 1000Mbps`
- C. `Snort update enable`
- D. `update enable`

Answer: A ([LEAVE A REPLY](#))

<https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpm>

NEW QUESTION: 112

Which configuration command is used to enable the Cisco Firepower Threat Defense (FTD) device to receive updates from the Cisco Security Intelligence Center (SIC)?

- A. `VPN update enable`
- B. `update enable`
- C. `Cisco FTD HA update enable`
- D. `update enable`

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 113

Which configuration command is used to enable the Cisco Firepower Threat Defense (FTD) device to receive updates from the Cisco Security Intelligence Center (SIC)?

- A. `update enable`
- B. `update enable`
- C. `update enable`
- D. `update enable`

Answer: ([SHOW ANSWER](#))

Which configuration command is used to enable the Cisco Firepower Threat Defense (FTD) device to receive updates from the Cisco Security Intelligence Center (SIC)?

- A. `update enable`
- B. `update enable`
- C. `update enable`
- D. `update enable`

Which of the following is a valid IPv6 address?

 A. 2001:0db8:0000:0000:0000:0000:0000:0000

 B. 2001:0db8:0000:0000:0000:0000:0000:0000:7

 C. 2001:0db8:0000:0000:0000:0000:0000:0000

 D. 2001:0db8:0000:0000:0000:0000:0000:0000

NEW QUESTION: 114

Which of the following protocols is used by Cisco FTD devices to discover neighboring devices?

- A. ARP
- B. CDP
- C. LLDP
- D. STP

Answer: D (LEAVE A REPLY)

NEW QUESTION: 115

Which of the following devices is not a Cisco Identity Services Engine (ISE) component?

- A. AMP
- B. Cisco ASR 7200
- C. ISE
- D. FMC
- E. ASA 5500

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 116

Which of the following is not a Cisco FMC supported protocol?

- A. NAT
- B. Cisco FMC
- C. Cisco FMC
- D. Cisco FMC
- E. NAT

Answer: D,E (LEAVE A REPLY)

Question ID: 116

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

NEW QUESTION: 117

Cisco Firepower Management Center (FMC) can be deployed in which of the following modes?

- A. 10

- B. 5
- C. 20
- D. 100

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 118

Which of the following is a valid IP address for the Management Interface on a Cisco FTD?



- A. 192.168.1.44
- B. 192.168.1.1
- C. 192.168.1.254
- D. 192.168.1.100

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 119

Which of the following is a valid IP address for the Management Interface on a Cisco FTD?

- A. 192.168.1.1
- B. 192.168.1.254
- C. 192.168.1.100
- D. 192.168.1.44

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 120

Which of the following is a valid IP address for the Management Interface on a Cisco FTD?

- A. 192.168.1.1
- B. 192.168.1.254
- C. 192.168.1.100
- D. 192.168.1.44

Answer: C ([LEAVE A REPLY](#))

□□:

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

NEW QUESTION: 121

□□□ □□□□□.



□□□□□ Cisco Secure Firewall Management Center(FMC)□□ □□ □□ □□□ □□□□□. □□□□□ □□□ □□□ □□□ □□□ □□□ □□ □□□□□. □□ □□□ □□□□ □□□ □□ □□ □□□ □□□□□ □□□ □□□ □□ □□ □□□ □□□ □□□□? (□ □□□ □□□□□.)

- A. Secure FMC□ FTP □□□□□ Hi □□□ □□□ □□□□ □□□ FTP □□□ □□□□□□.
- B. □□□ □□□ □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□ □□ □□□□ □□□□□.
- C. FTD67 □ FTD66 □□□□ CU□ □□□□ □□□□□ PIP □□□ □□□ □□□□□.
- D. Secure FMC□□ □□□ □□□ □□□□□. /Var/common□ □□□ □□□□ □□□□ □□□ □□ □□□ □□□□□.
- E. □□□ □□□□, □□□ □□□□ □□ □□ □□ □□ □□□□ □□□ □□□ □□□ □□ □□□ □□□□□.

Answer: D,E (LEAVE A REPLY)

Cisco Secure Firewall Management Center(FMC)□□ □□ □□ □□□ □□□□ □□□ □□□□□ □□□□□ □□□ □□□□□□ □□ □□□ □□, □□ □□□ □□□□ □□ □□□ □□□□ □□□ □□ □□ □□□ □□ □□□□ □□□ □□□ □ □□□□.

- * Secure FMC□□ □□□ □□□ □□:
- * SSH □□ □□□ □□ FMC□□ □□□ □□□ □□□□□□.
- * □□□ □□ □□ □□□ □□□□ □□□□ /var/common□ □□□ □□□□□. Is /var/common □□□ □□□□□.
- * □□□ □□□□ □□ □□ □□:
- * FMC□□ □□□ > □□□□ > □□□ □□□□□.
- * "□□ □□ □□ □□" □□□□ □□□ □□ □□ □□□ □□ □□□ □□□□□.

□□□ □□□ □□□□ □□□ □□ □□ □□□ □□ □□□□ □□□ □□□□ □□□□ □□□ □□□□ □□□ □ □□□□. □□ □□: Cisco Secure Firewall Management Center □□□ □□□, □□ □□ □ □□ □□ □□.

300-710 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ 300-710 □□! DumpTop □ □□ **300-710** □□ □□□ □□□□ □□, DumpTop 300-710 □□ □□□ □□□□□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop 300-710 □ □□ □□□□□. <https://www.dumpst.com/Cisco/300-710-dump.html> (445 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 122

□□□□□ □ □□ Cisco FMC□ □□ □□□ □□□□ □□□ □□ □□□ □□□ □ □□□□. □ □□□ □□□ □□□□□? A. □□ □□ FMC□ □□□ □□□□ □□□□.

B. 10Mbps.

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html

C.

D. Cisco FMC.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 123

Cisco FMC. IPS. ?

A. IPS.

B. IPS.

C. IPS.

D. IPS.

Answer: (SHOW ANSWER)

300-710 DumpTop 300-710! DumpTop 300-710, DumpTop 300-710. DumpTop 300-710. <https://www.dumptop.com/Cisco/300-710-dump.html> (445 Q&As Dumps, 30%OFF Special Discount: **KrDump**)