NSE4_FGT-6.2 Q&As

Fortinet NSE 4 - FortiOS 6.2

Pass Fortinet NSE4_FGT-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse4_fgt-6-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.

B. Only secondary FortiGate devices are rebooted.

C. Uninterruptable upgrade is enabled by default.

D. Traffic load balancing is temporally disabled while upgrading the firmware.

Correct Answer: BD

QUESTION 2

If traffic matches a DLP filter with the action set to Quarantine IP Address, what action does FortiGate take?

A. It notifies the administrator by sending an email.

B. It provides a DLP block replacement page with a link to download the file.

C. It blocks all future traffic for that IP address for a configured interval.

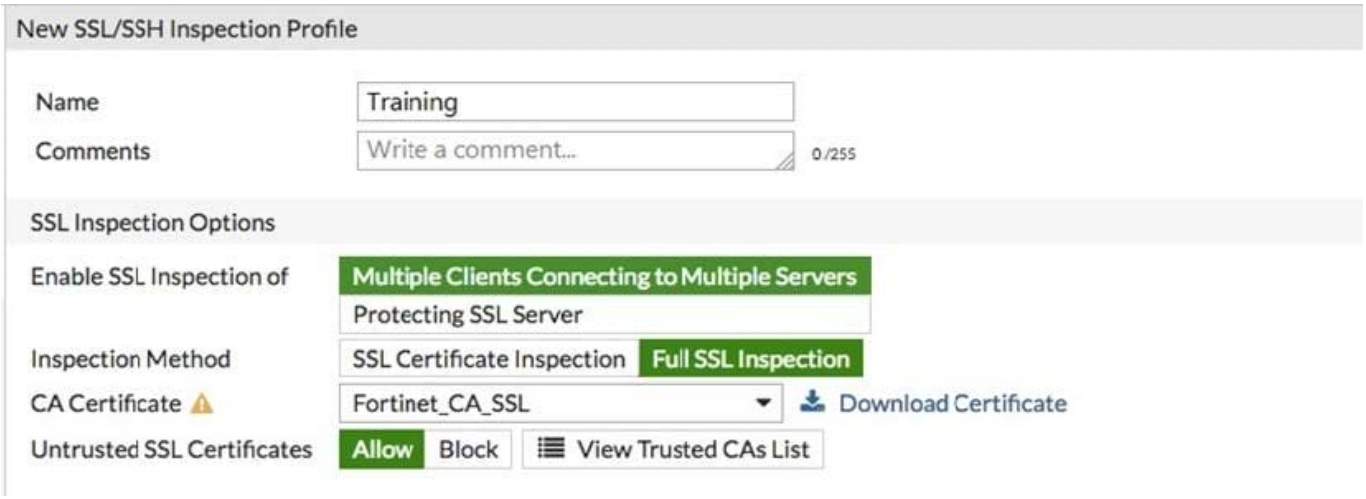
D. It archives the data for that IP address.

Correct Answer: C

QUESTION 3

An employee connects to the https://example.com on the Internet using a web browser. The web server\\'s certificate was signed by a private internal CA. The FortiGate that is inspecting this traffic is configured for full SSL inspection.

This exhibit shows the configuration settings for the SSL/SSH inspection profile that is applied to the policy that is invoked in this instance. All other settings are set to defaults. No certificates have been imported into FortiGate. View the exhibit and answer the question that follows.



Which certificate is presented to the employee\\'s web browser?

A. The web server\\'s certificate.

B. The user\\'s personal certificate signed by a private internal CA.

C. A certificate signed by Fortinet_CA_SSL.

D. A certificate signed by Fortinet_CA_Untrusted.

Correct Answer: D

QUESTION 4

An administrator needs to strengthen the security for SSL VPN access. Which of the following statements are best practices to do so? (Choose three.)

A. Configure split tunneling for content inspection.

B. Configure host restrictions by IP or MAC address.

C. Configure two-factor authentication using security certificates.

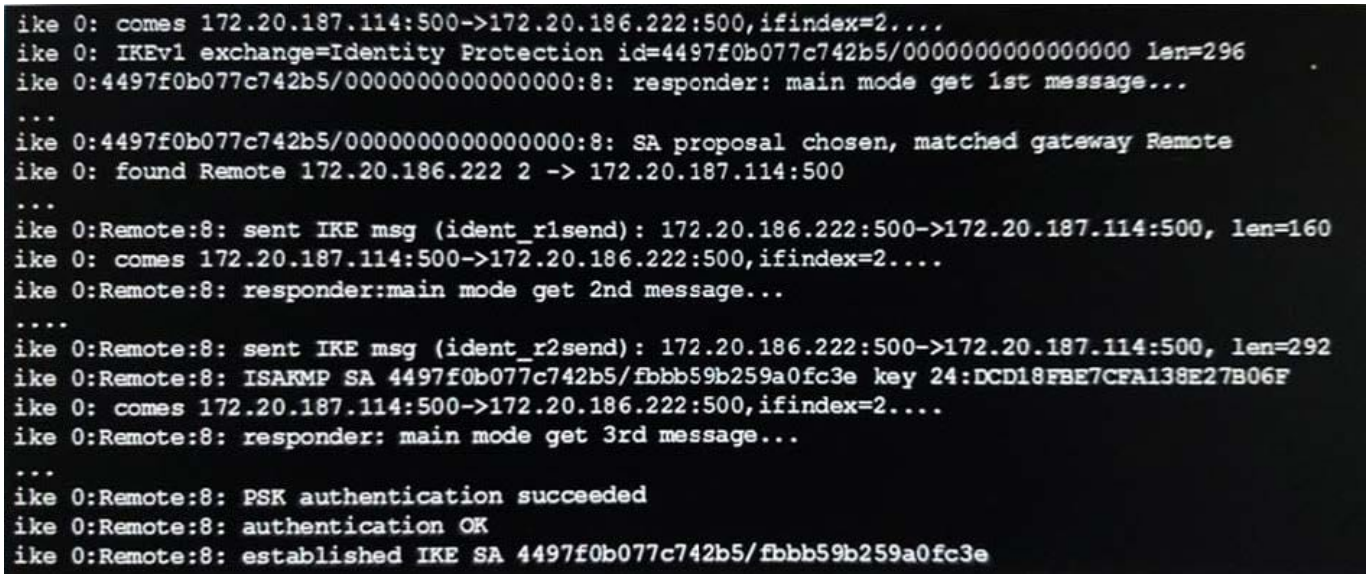
D. Configure SSL offloading to a content processor (FortiASIC).

E. Configure a client integrity check (host-check).

Correct Answer: CDE

QUESTION 5

Examine the exhibit, which shows the partial output of an IKE real-time debug.



Which of the following statement about the output is true?

A. The VPN is configured to use pre-shared key authentication.

B. Extended authentication (XAuth) was successful.

C. Remote is the host name of the remote IPsec peer.

D. Phase 1 went down.

Correct Answer: A