

## NSE4\_FGT-6.2<sup>Q&As</sup>

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](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 temporarily 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.

**New SSL/SSH Inspection Profile**

Name:

Comments:  0/255

**SSL Inspection Options**

Enable SSL Inspection of: **Multiple Clients Connecting to Multiple Servers**  
Protecting SSL Server

Inspection Method: SSL Certificate Inspection **Full SSL Inspection**

CA Certificate ⚠️:  [Download Certificate](#)

Untrusted SSL Certificates: **Allow** Block [View Trusted CAs List](#)

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.

```
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=4497f0b077c742b5/0000000000000000 len=296
ike 0:4497f0b077c742b5/0000000000000000:8: responder: main mode get 1st message...
...
ike 0:4497f0b077c742b5/0000000000000000:8: SA proposal chosen, matched gateway Remote
ike 0: found Remote 172.20.186.222 2 -> 172.20.187.114:500
...
ike 0:Remote:8: sent IKE msg (ident_r1send): 172.20.186.222:500->172.20.187.114:500, len=160
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder:main mode get 2nd message...
....
ike 0:Remote:8: sent IKE msg (ident_r2send): 172.20.186.222:500->172.20.187.114:500, len=292
ike 0:Remote:8: ISAKMP SA 4497f0b077c742b5/fbbb59b259a0fc3e key 24:DCD18FBE7CFA138E27B06F
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder: main mode get 3rd message...
...
ike 0:Remote:8: PSK authentication succeeded
ike 0:Remote:8: authentication OK
ike 0:Remote:8: established IKE SA 4497f0b077c742b5/fbbb59b259a0fc3e
```

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

[Latest NSE4\\_FGT-6.2 Dumps](#)

[NSE4\\_FGT-6.2 VCE Dumps](#) [NSE4\\_FGT-6.2 Study Guide](#)