

NSE4_FGT-6.0^{Q&As}

Fortinet NSE 4 - FortiOS 6.0

Pass Fortinet NSE4_FGT-6.0 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse4_fgt-6-0.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 of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

- A. The public key of the web server certificate must be installed on the browser.
- B. The web-server certificate must be installed on the browser.
- C. The CA certificate that signed the web-server certificate must be installed on the browser.
- D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Correct Answer: C

QUESTION 2

Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.

The screenshot shows the configuration for an IPS sensor named 'WINDOWS_SERVERS'. It includes sections for 'IPS Signatures' and 'IPS Filters'. The 'IPS Signatures' table shows a signature for 'A32S.Botnet' with a severity of 5 (indicated by 5 red bars) and an action of 'Monitor'. The 'IPS Filters' table shows a filter for 'Location:server' and 'OS:Windows' with an action of 'Block' and packet logging disabled.

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
A32S.Botnet	0	5	Server.Client	TCP	All	Monitor	✓

Filter Details	Action	Packet Logging
Location:server OS:Windows	Block	✗

What are the expected actions if traffic matches this IPS sensor? (Choose two.)

- A. The sensor will gather a packet log for all matched traffic.
- B. The sensor will not block attackers matching the A32S.Botnet signature.
- C. The sensor will block all attacks for Windows servers.
- D. The sensor will reset all connections that match these signatures.

Correct Answer: AC

QUESTION 3

Which of the following features is supported by web filter in flow-based inspection mode with NGFW mode set to profile-based?

- A. FortiGuard Quotas
- B. Static URL
- C. Search engines
- D. Rating option

Correct Answer: B

QUESTION 4

Which statements about HA for FortiGate devices are true? (Choose two.)

- A. Sessions handled by proxy-based security profiles cannot be synchronized.
- B. Virtual clustering can be configured between two FortiGate devices that have multiple VDOMs.
- C. HA management interface settings are synchronized between cluster members.
- D. Heartbeat interfaces are not required on the primary device.

Correct Answer: BC

QUESTION 5

Which statements about antivirus scanning mode are true? (Choose two.)

- A. In proxy-based inspection mode antivirus buffers the whole file for scanning before sending it to the client.
- B. In flow-based inspection mode, you can use the CLI to configure antivirus profiles to use protocol option profiles.
- C. In proxy-based inspection mode, if a virus is detected, a replacement message may not be displayed immediately.
- D. In quick scan mode, you can configure antivirus profiles to use any of the available signature data bases.

Correct Answer: AB

[Latest NSE4_FGT-6.0 Dumps](#)

[NSE4_FGT-6.0 VCE Dumps](#) [NSE4_FGT-6.0 Braindumps](#)