

NSE4_FGT-7.2^{Q&As}

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse4_fgt-7-2.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 two statements are correct about NGFW Policy-based mode? (Choose two.)

- A. NGFW policy-based mode does not require the use of central source NAT policy
- B. NGFW policy-based mode can only be applied globally and not on individual VDOMs
- C. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy
- D. NGFW policy-based mode policies support only flow inspection

Correct Answer: CD

QUESTION 2

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

- A. The interface has been configured for one-arm sniffer.
- B. The interface is a member of a virtual wire pair.
- C. The operation mode is transparent.
- D. The interface is a member of a zone.
- E. Captive portal is enabled in the interface.

Correct Answer: ABC

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

QUESTION 3

Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)

- A. DNS
- B. ping
- C. udp-echo
- D. TWAMP

Correct Answer: CD

QUESTION 4

You have enabled logging on a FortiGate device for event logs and all security logs, and you have set up logging to use the FortiGate local disk. What is the default behavior when the local disk is full?

- A. No new log is recorded after the warning is issued when log disk use reaches the threshold of 95%.
- B. No new log is recorded until you manually clear logs from the local disk.
- C. Logs are overwritten and the first warning is issued when log disk use reaches the threshold of 75%.
- D. Logs are overwritten and the only warning is issued when log disk use reaches the threshold of 95%.

Correct Answer: C

config log disk setting

```
set diskfull [ overwrite | nolog ]
```

Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full. (default --> overwrite)

config log memory global-setting

```
set full-first-warning-threshold {integer}
```

Log full first warning threshold as a percent. (default --> 75) Reference:

<https://docs.fortinet.com/document/fortigate/7.2.5/cli-reference/421620/config-log-disk-setting>

<https://docs.fortinet.com/document/fortigate/7.2.5/cli-reference/418620/config-log-memory-global-setting>

Logs are overwritten and the first warning is issued when log disk use reaches the threshold of 75%.

This is true because this is the default behavior of FortiGate when logging to the local disk. The local disk is the internal storage of FortiGate that can be used to store event logs and security logs. When the local disk is full, FortiGate will

overwrite the oldest logs with the newest ones, and issue warnings at different thresholds of disk usage. The first warning is issued when log disk use reaches 75%, the second warning is issued when log disk use reaches 85%, and the final

warning is issued when log disk use reaches 95%. The administrator can configure these thresholds and the action to take when the disk is full using the CLI command config log disk setting1

QUESTION 5

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.

What is the reason for the certificate warning errors?

- A. The matching firewall policy is set to proxy inspection mode.
- B. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
- C. The full SSL inspection feature does not have a valid license.

D. The browser does not trust the certificate used by FortiGate for SSL inspection.

Correct Answer: D

FortiGate Security 7.2 Study Guide (p.235): "If FortiGate receives a trusted SSL certificate, then it generates a temporary certificate signed by the built-in Fortinet_CA_SSL certificate and sends it to the browser. If the browser trusts the Fortinet_CA_SSL certificate, the browser completes the SSL handshake. Otherwise, the browser also presents a warning message informing the user that the site is untrusted. In other words, for this function to work as intended, you must import the Fortinet_CA_SSL certificate into the trusted root CA certificate store of your browser."

[Latest NSE4_FGT-7.2 Dumps](#)

[NSE4_FGT-7.2 VCE Dumps](#) [NSE4_FGT-7.2 Study Guide](#)