# 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.geekcert.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 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 2**

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 3**

Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides (client and server) have terminated the session?

A. To remove the NAT operation.

B. To generate logs

C. To finish any inspection operations.

D. To allow for out-of-order packets that could arrive after the FIN/ACK packets.

Correct Answer: D

**QUESTION 4**

An administrator wants to configure Dead Peer Detection (DPD) on IPSEC VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.

Which DPD mode on FortiGate will meet the above requirement?

A. Disabled

B. On Demand

C. Enabled

D. On Idle

Correct Answer: D

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD40813

**QUESTION 5**

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

1.

All traffic must be routed through the primary tunnel when both tunnels are up

2.

The secondary tunnel must be used only if the primary tunnel goes down

3.

In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover

Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two,)

A. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

B. Enable Dead Peer Detection.

C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.

D. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

Correct Answer: BC

Study Guide IPsec VPN IPsec configuration Phase 1 Network.

When Dead Peer Detection (DPD) is enabled, DPD probes are sent to detect a failed tunnel and bring it down before its IPsec SAs expire. This failure detection mechanism is very useful when you have redundant paths to the same

destination, and you want to failover to a backup connection when the primary connection fails to keep the connectivity between the sites up.

There are three DPD modes. On demand is the default mode.

Study Guide IPsec VPN Redundant VPNs.

Add one phase 1 configuration for each tunnel. DPD should be enabled on both ends.

Add at least one phase 2 definition for each phase 1.

Add one static route for each path. Use distance or priority to select primary routes over backup routes (routes for the primary VPN must have a lower distance or lower priority than the backup). Alternatively, use dynamic routing.

Configure FW policies for each IPsec interface.