

# NSE4\_FGT-6.4<sup>Q&As</sup>

Fortinet NSE 4 - FortiOS 6.4

## Pass Fortinet NSE4\_FGT-6.4 Exam with 100% Guarantee

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

[https://www.pass2lead.com/nse4\\_fgt-6-4.html](https://www.pass2lead.com/nse4_fgt-6-4.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 settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

- A. System time
- B. FortiGuard update servers
- C. Operating mode
- D. NGFW mode

Correct Answer: CD

C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.

D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM"  
Page 125 of FortiGate\_Infrastructure\_6.4\_Study\_Guide

---

**QUESTION 2**

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: CD

---

**QUESTION 3**

How does FortiGate act when using SSL VPN in web mode?

- A. FortiGate acts as an FDS server.
- B. FortiGate acts as an HTTP reverse proxy.
- C. FortiGate acts as DNS server.
- D. FortiGate acts as router.

Correct Answer: B

Reference: [https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate\\_v4.0MR3/fortigatesslvpn-40-mr3.pdf](https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigatesslvpn-40-mr3.pdf)

---

**QUESTION 4**

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'. The 'Name' field is filled with 'WINDOWS\_SERVERS'. Below it, there are buttons for '+ Add Signatures', 'Delete', and 'Edit IP Exemptions'. A table with columns 'Name', 'Exempt IPs', 'Severity', 'Target', 'Service', 'OS', 'Action', and 'Packet Logging' is shown, with the message 'No matching entries found' below it. Under the 'IPS Filters' section, there are buttons for '+ Add Filter', 'Edit Filter', and 'Delete'. A table with columns 'Filter Details', 'Action', and 'Packet Logging' is shown, with the following entry: 'Location:server', 'OS:Windows', 'Block' (with a red circle and slash icon), and a red circle icon. An 'Apply' button is at the bottom.

The screenshot shows the 'Forward Traffic Logs' section. It has a table with columns: '#', 'Date/Time', 'Source', 'Destination', 'Application Name', 'Result', and 'Policy'. The table contains 10 rows of log entries, all showing 'HTTPS' traffic from '10.200.1.254' to '10.200.1.200' with a result of '1.30kB/2.65 kB' and a policy of '2(Web-Server-Access-IPS)'. There are icons for refresh, download, and add filter at the top left of the table.

#	Date/Time	Source	Destination	Application Name	Result	Policy
1	10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
2	10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
3	10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
4	10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
5	10:09:01	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
6	10:08:59	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
7	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
8	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
9	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
10	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)

An administrator has configured the WINDOWS\_SERVERS IPS sensor in an attempt to determine whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic.

What is a possible reason for this?

- A. The IPS filter is missing the Protocol: HTTPS option.
- B. The HTTPS signatures have not been added to the sensor.
- C. A DoS policy should be used, instead of an IPS sensor.

- D. A DoS policy should be used, instead of an IPS sensor.
- E. The firewall policy is not using a full SSL inspection profile.

Correct Answer: E

---

#### QUESTION 5

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

\*

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

\*

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

\*

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

[NSE4\\_FGT-6.4 PDF Dumps](#) [NSE4\\_FGT-6.4 VCE Dumps](#) [NSE4\\_FGT-6.4 Braindumps](#)