

NSE4^{Q&As}

Fortinet Network Security Expert 4 Written Exam (400)

Pass Fortinet NSE4 Exam with 100% Guarantee

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

<https://www.leads4pass.com/nse4.html>

100% Passing Guarantee
100% Money Back Assurance

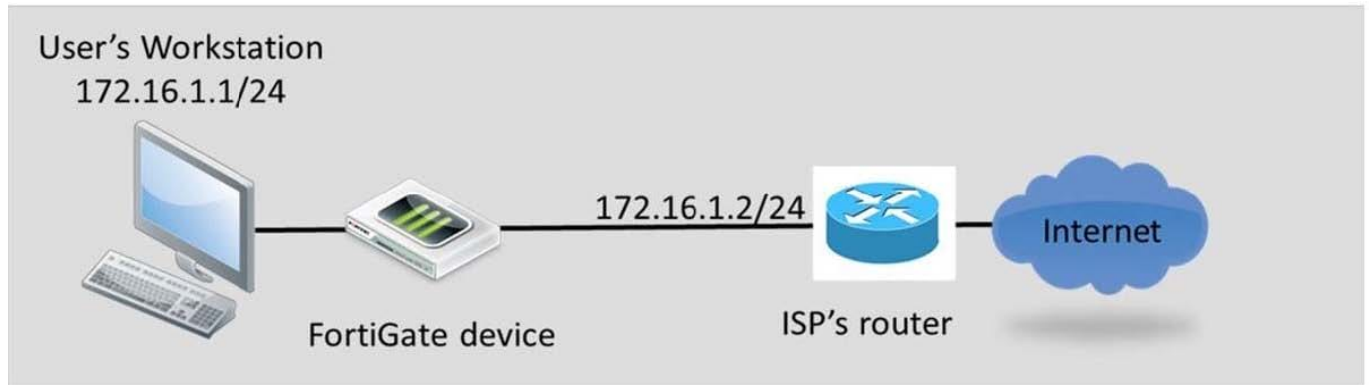
Following Questions and Answers are all new published by Fortinet
Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



QUESTION 1

Review to the network topology in the exhibit.



The workstation, 172.16.1.1/24, connects to port2 of the FortiGate device, and the ISP router, 172.16.1.2, connects to port1. Without changing IP addressing, which configuration changes are required to properly forward users traffic to the Internet? (Choose two)

- A. At least one firewall policy from port2 to port1 to allow outgoing traffic.
- B. A default route configured in the FortiGuard devices pointing to the ISP's router.
- C. Static or dynamic IP addresses in both FortiGate interfaces port1 and port2.
- D. The FortiGate devices configured in transparent mode.

Correct Answer: AD

QUESTION 2

Which of the following statements are correct concerning IKE mode config? (Choose two)

- A. It can dynamically assign IP addresses to IPsec VPN clients.
- B. It can dynamically assign DNS settings to IPsec VPN clients.
- C. It uses the ESP protocol.
- D. It can be enabled in the phase 2 configuration.

Correct Answer: AB

QUESTION 3

Which of the following statements are correct concerning layer 2 broadcast domains in transparent mode VDOMs?(Choose two)

- A. The whole VDOM is a single broadcast domain even when multiple VLAN are used.
- B. Each VLAN is a separate broadcast domain.
- C. Interfaces configured with the same VLAN ID can belong to different broadcast domains.
- D. All the interfaces in the same broadcast domain must use the same VLAN ID.

Correct Answer: BC

QUESTION 4

What are the requirements for a HA cluster to maintain TCP connections after device or link failover? (Choose two.)

- A. Enable session pick-up.
- B. Enable override.
- C. Connections must be UDP or ICMP.
- D. Connections must not be handled by a proxy.

Correct Answer: AD

QUESTION 5

A FortiGate administrator with the super_admin profile configures a virtual domain (VDOM) for a new customer. After creating the VDOM, the administrator is unable to reassign the dmz interface to the new VDOM as the option is greyed out in the GUI in the management VDOM.

What would be a possible cause for this problem?

- A. The administrator does not have the proper permissions the dmz interface.
- B. The dmz interface is referenced in the configuration of another VDOM.
- C. Non-management VDOMs cannot reference physical interfaces
- D. The dmz interface is in PPPoE or DHCP mode.

Correct Answer: B

QUESTION 6

Which statement concerning IPS is false?

- A. IPS packages contain an engine and signatures used by both IPS and other flow-based scans.
- B. One-arm topology with sniffer mode improves performance of IPS blocking.
- C. IPS can detect zero-day attacks.

D. The status of the last service update attempt from FortiGuard IPS is shown on System>Config>FortiGuard and in output from `\\diag autoupdate version\\`

Correct Answer: D

QUESTION 7

Which of the following statements are correct concerning the FortiGate session life support protocol? (Choose two)

- A. By default, UDP sessions are not synchronized.
- B. Up to four FortiGate devices in standalone mode are supported.
- C. only the master unit handles the traffic.
- D. Allows per-VDOM session synchronization.

Correct Answer: AD

QUESTION 8

Which of the following statements best describe the main requirements for a traffic session to be offload eligible to an NP6 processor? (Choose three.)

- A. Session packets do NOT have an 802.1Q VLAN tag.
- B. It is NOT multicast traffic.
- C. It does NOT require proxy-based inspection.
- D. Layer 4 protocol must be UDP, TCP, SCTP or ICMP.
- E. It does NOT require flow-based inspection.

Correct Answer: CDE

QUESTION 9

Alert emails enable the FortiGate unit to send email notifications to an email address upon detection of a pre-defined event type.

Which of the following are some of the available event types in Web Config?

- A. Intrusion detected.
- B. Successful firewall authentication.
- C. Oversized file detected.
- D. DHCP address assigned.

E. FortiGuard Web Filtering rating error detected.

Correct Answer: A

QUESTION 10

What are required to be the same for two FortiGate units to form an HA cluster? (Choose two)

- A. Firmware.
- B. Model.
- C. Hostname.
- D. System time zone.

Correct Answer: AB

QUESTION 11

Which of the following statements are correct regarding a master HA unit? (Choose two)

- A. There should be only one master unit in each HA virtual cluster.
- B. The Master synchronizes cluster configuration with slaves.
- C. Only the master has a reserved management HA interface.
- D. Heartbeat interfaces are not required on a master unit.

Correct Answer: AB

QUESTION 12

Which is true of FortiGate's session table?

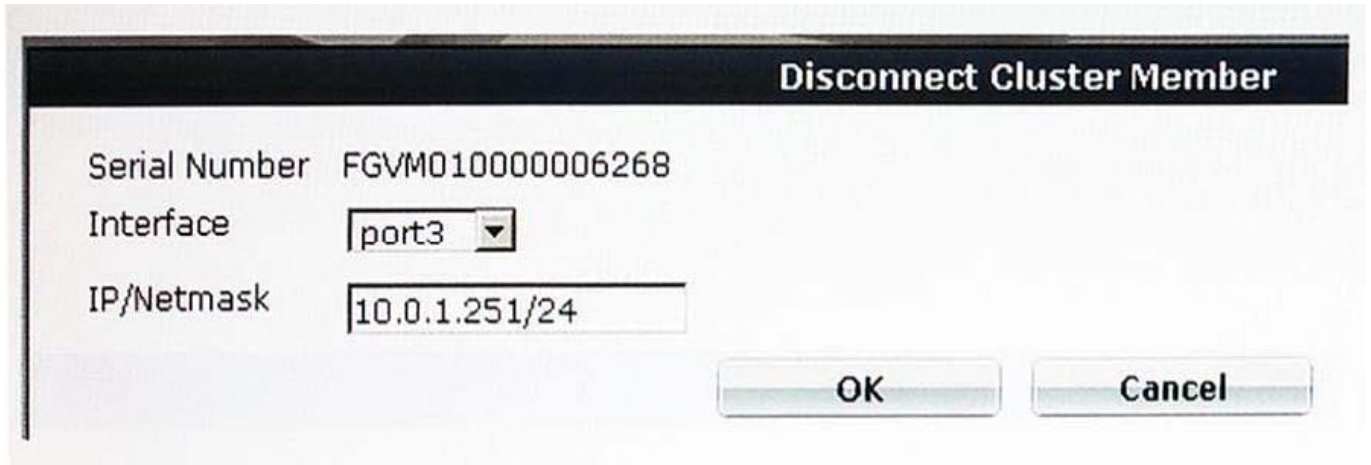
- A. NAT/PAT is shown in the central NAT table, not the session table.
- B. It shows TCP connection states.
- C. It shows IP, SSL, and HTTP sessions.
- D. It does not show UDP or ICMP connection state codes, because those protocols are connectionless.

Correct Answer: B

QUESTION 13

The exhibit shows the Disconnect Cluster Member command in a FortiGate unit that is part of a HA cluster with two HA

members.



What is the effect of the Disconnect Cluster Member command as given in the exhibit. (Choose two.)

- A. Port3 is configured with an IP address management access.
- B. The firewall rules are purged on the disconnected unit.
- C. The HA mode changes to standalone.
- D. The system hostname is set to the unit serial number.

Correct Answer: AC

QUESTION 14

Which FSSO agents are required for a FSSO agent-based polling mode solution?

- A. Collector agent and DC agents
- B. Polling agent only
- C. Collector agent only
- D. DC agents only

Correct Answer: A

QUESTION 15

What actions are possible with Application Control? (Choose three.)

- A. Warn
- B. Allow
- C. Block

D. Traffic Shaping

E. Quarantine

Correct Answer: BCD

[NSE4 PDF Dumps](#)

[NSE4 Practice Test](#)

[NSE4 Exam Questions](#)