



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.pass4itsure.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**

FSSO provides a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows active directory.

Which of the following statements are correct regarding FSSO in a Windows domain environment when DC-agent mode is used? (Choose two.)

- A. An FSSO collector agent must be installed on every domain controller.
- B. An FSSO domain controller agent must be installed on every domain controller.
- C. The FSSO domain controller agent will regularly update user logon information on the FortiGate unit.
- D. The FSSO collector agent will receive user logon information from the domain controller agent and will send it to the FortiGate unit.

Correct Answer: BD

QUESTION 2

Which of the following authentication methods are supported in an IPsec phase 1? (Choose two.)

- A. Asymmetric Keys
- B. CA root digital certificates
- C. RSA signature
- D. Pre-shared keys

Correct Answer: CD

QUESTION 3

Which statement describes how traffic flows in sessions handled by a slave unit in an active-active HA cluster?

- A. Packet are sent directly to the slave unit using the slave physical MAC address.
- B. Packets are sent directly to the slave unit using the HA virtual MAC address.
- C. Packets arrived at both units simultaneously, but only the salve unit forwards the session.
- D. Packets are first sent to the master unit, which then forwards the packets to the slave unit.

Correct Answer: D

QUESTION 4



Which IPSec mode includes the peer id information in the first packet?

- A. Main mode.
- B. Quick mode.
- C. Aggressive mode.
- D. IKEv2 mode.

Correct Answer: C

QUESTION 5

Which of the following statements is true regarding the differences between route-based and policy-based IPsec VPNs? (Choose two.)

- A. The firewall policies for policy-based are bidirectional. The firewall policies for route-based are unidirectional.
- B. In policy-based VPNs the traffic crossing the tunnel must be routed to the virtual IPsec interface. In route-based, it does not.
- C. The action for firewall policies for route-based VPNs may be Accept or Deny, for policy-based VPNs it is Encrypt.
- D. Policy-based VPN uses an IPsec interface, route-based does not.

Correct Answer: AC

QUESTION 6

What functions can the IPv6 Neighbor Discovery Protocol accomplish? (Choose two.)

- A. Negotiate the encryption parameters to use.
- B. Auto-adjust the MTU setting.
- C. Autoconfigure addresses and prefixes.
- D. Determine other nodes reachability.

Correct Answer: CD

QUESTION 7

You have configured the DHCP server on a FortiGate's port1 interface (or internal, depending on the model) to offer IPs in a range of 192.168.1.65-192.168.1.253.

When the first host sends a DHCP request, what IP will the DHCP offer?

- A. 192.168.1.99



B. 192.168.1.253

C. 192.168.1.65

D. 192.168.1.66

Correct Answer: C

QUESTION 8

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 9

Which of the following are operating mode supported in FortiGate devices? (Choose two)

A. Proxy

B. Transparent

C. NAT/route

D. Offline inspection

Correct Answer: BC

QUESTION 10

Which commands are appropriate for investigating high CPU? (Choose two.)

A. diag sys top

B. diag hardware sysinfo mem

C. diag debug flow

D. get system performance status

Correct Answer: AD

**QUESTION 11**

With FSSO DC-agent mode, a domain user could authenticate either against the domain controller running the collector agent and domain controller agent, or a domain controller running only the domain controller agent.

If you attempt to authenticate with a domain controller running only the domain controller agent, which statements are correct? (Choose two.)

- A. The login event is sent to a collector agent.
- B. The FortiGate receives the user information directly from the receiving domain controller agent of the secondary domain controller.
- C. The domain collector agent may perform a DNS lookup for the authenticated client's IP address.
- D. The user cannot be authenticated with the FortiGate in this manner because each domain controller agent requires a dedicated collector agent.

Correct Answer: AC

QUESTION 12

Which of the following statements are correct about the HA command diagnose sys ha reset-uptime? (Choose two.)

- A. The device this command is executed on is likely to switch from master to slave status if override is disabled.
- B. The device this command executed on is likely to switch from master to slave status if override is enabled.
- C. The command has no impact on the HA algorithm.
- D. This commands resets the uptime variable used in the HA algorithm so it may cause a new master to become elected.

Correct Answer: AD

QUESTION 13

Which best describes the authentication timeout?

- A. How long FortiGate waits for the user to enter his or her credentials.
- B. How long a user is allowed to send and receive traffic before he or she must authenticate again.
- C. How long an authenticated user can be idle (without sending traffic) before they must authenticate again.
- D. How long a user-authenticated session can exist without having to authenticate again.

Correct Answer: C

QUESTION 14



Which IPsec configuration mode can be used for implementing GRE-over-IPsec VPNs?

- A. Policy-based only.
- B. Route-based only.
- C. Either policy-based or route-based VPN.
- D. GRE-based only.

Correct Answer: B

QUESTION 15

In which process states is it impossible to interrupt/kill a process? (Choose two.)

- A. S-Sleep
- B. R-Running
- C. D-Uninterruptable Sleep
- D. Z-Zombie

Correct Answer: CD

[Latest NSE4 Dumps](#)

[NSE4 PDF Dumps](#)

[NSE4 Practice Test](#)