

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.leads4pass.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

FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.

In this scenario, what are two requirements for the VLAN ID? (Choose two.)

- A. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.
- B. The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs.
- C. The two VLAN subinterfaces must have different VLAN IDs.
- D. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

Correct Answer: BC

<https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-use-vmac-vlan-to-share-the-same-VLAN/tag/192843?externalID=FD43883>

When FortiGate is operating in NAT mode, it means that it uses network address translation (NAT) to modify the source or destination IP addresses of the traffic passing through it¹. NAT mode allows FortiGate to hide the IP addresses of the internal network from the external network, and to conserve IP addresses by using a single public IP address for multiple private IP addresses¹. A virtual LAN (VLAN) subinterface is a logical interface that allows traffic from different VLANs to enter and exit the FortiGate unit². A VLAN subinterface is created by adding a VLAN ID to a physical interface or an aggregate interface². A VLAN ID is a numerical identifier that distinguishes one VLAN from another². In this scenario, there are two requirements for the VLAN ID of the VLAN subinterfaces added to the same physical interface: The two VLAN subinterfaces must have different VLAN IDs. This is because the VLAN ID is used to tag the traffic with the appropriate VLAN information, and to separate the traffic into different VLANs². If the two VLAN subinterfaces have the same VLAN ID, they will not be able to distinguish the traffic from each other, and they will not be able to forward the traffic to the correct destination. The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs. This is because VDOMs are virtual instances of FortiGate that can have their own interfaces, policies, and routing tables³. Each VDOM operates independently from other VDOMs, and can have its own VLAN subinterfaces with different or identical VLAN IDs³. However, this requires inter-VDOM links to allow traffic between different VDOMs³.

QUESTION 2

An employee needs to connect to the office through a high-latency internet connection.

Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

- A. idle-timeout
- B. login-timeout
- C. udp-idle-timer
- D. session-ttl

Correct Answer: B

FortiGate Infrastructure 7.2 Study Guide (p.222):

"When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under config vpn ssl

settings have been added to address this. The first command allows you to set up the login timeout, replacing the previous hard timeout value. The second command allows you to set up the maximum DTLS hello timeout for SSL VPN connections."

QUESTION 3

Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

- A. Web filter in flow-based inspection
- B. Antivirus in flow-based inspection
- C. DNS filter
- D. Web application firewall
- E. Application control

Correct Answer: ABE

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/739623/dns-filter-handled-by-ips-engine-in-flow-mode>

QUESTION 4

If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source field of a firewall policy?

- A. IP address
- B. Once Internet Service is selected, no other object can be added
- C. User or User Group
- D. FQDN address

Correct Answer: B

Reference: <https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-in-policy>

QUESTION 5

An administrator has a requirement to keep an application session from timing out on port 80.

What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)

- A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
- B. Create a new service object for HTTP service and set the session TTL to never
- C. Set the TTL value to never under config system-ttl
- D. Set the session TTL on the HTTP policy to maximum

Correct Answer: BC

[Latest NSE4_FGT-7.2 Dumps](#)

[NSE4_FGT-7.2 Practice Test](#)

[NSE4_FGT-7.2 Study Guide](#)