



NSE4_FGT-6.0^{Q&As}

Fortinet NSE 4 - FortiOS 6.0

Pass Fortinet NSE4_FGT-6.0 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse4_fgt-6-0.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**

What files are sent to FortiSandbox for inspection in flow-based inspection mode?

- A. All suspicious files that do not have their hash value in the FortiGuard antivirus signature database.
- B. All suspicious files that are above the defined oversize limit value in the protocol options.
- C. All suspicious files that match patterns defined in the antivirus profile.
- D. All suspicious files that are allowed to be submitted to FortiSandbox in the antivirus profile.

Correct Answer: C

QUESTION 2

An administrator wants to configure a FortiGate as a DNS server. FortiGate must use a DNS database first, and then relay all irresolvable queries to an external DNS server. Which of the following DNS methods must you use?

- A. Recursive
- B. Non-recursive
- C. Forward to primary and secondary DNS
- D. Forward to system DNS

Correct Answer: A

QUESTION 3

Which of the following SD-WAN load balancing method use interface weight value to distribute traffic? (Choose two.)

- A. Source IP
- B. Spillover
- C. Volume
- D. Session

Correct Answer: CD

QUESTION 4

Which is a requirement for creating an inter-VDOM link between two VDOMs?

- A. The inspection mode of at least one VDOM must be proxy-based.



B. At least one of the VDOMs must operate in NAT mode.

C. The inspection mode of both VDOMs must match.

D. Both VDOMs must operate in NAT mode.

Correct Answer: B

QUESTION 5

View the exhibit:



The client cannot connect to the HTTP web server. The administrator ran the FortiGate built-in sniffer and got the following output:

```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port 80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.755510 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
```

What should be done next to troubleshoot the problem?

A. Run a sniffer in the web server.

B. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10".

C. Capture the traffic using an external sniffer connected to port1.

D. Execute a debug flow.

Correct Answer: D

[NSE4_FGT-6.0 VCE Dumps](#) [NSE4_FGT-6.0 Study Guide](#) [NSE4_FGT-6.0 Braindumps](#)