

# NSE7<sup>Q&As</sup>

Fortinet Troubleshooting Professional

## Pass Fortinet NSE7 Exam with 100% Guarantee

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

<https://www.pass2lead.com/nse7.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**

Examine the following partial output from a sniffer command; then answer the question below.

```
# diagnose sniff packet any 'icmp' 4
interfaces= [any]
filters = [icmp]
2.101199 wan2 in 192.168.1.110-> 4.2.2.2: icmp: echo request
2.101400 wan1 out 172.17.87.16-> 4.2.2.2: icmp: echo request
.....
2.123500 wan2 out 4.2.2.2-> 192.168.1.110: icmp: echo reply
244 packets received by filter
5 packets dropped by kernel
```

What is the meaning of the packets dropped counter at the end of the sniffer?

- A. Number of packets that didn't match the sniffer filter.
- B. Number of total packets dropped by the FortiGate.
- C. Number of packets that matched the sniffer filter and were dropped by the FortiGate.
- D. Number of packets that matched the sniffer filter but could not be captured by the sniffer.

Correct Answer: C

---

**QUESTION 2**

View the exhibit, which contains the output of a debug command, and then answer the question below.

```
#dia hardware sysinfo shm
SHM counter:          150
SHM allocated:        0
SHM total:            625057792
conserve mode: on - mem
system last entered: Mon Apr 24 16:36:37 2017
sys fd last entered: n/a
SHM FS total:        641236992
SHM FS free:         641208320
SHM FS avail:        641208320
SHM FS alloc:        28672
```

What statement is correct about this FortiGate?

- A. It is currently in system conserve mode because of high CPU usage.
- B. It is currently in FD conserve mode.
- C. It is currently in kernel conserve mode because of high memory usage.
- D. It is currently in system conserve mode because of high memory usage.

Correct Answer: D

### QUESTION 3

View the exhibit, which contains a screenshot of some phase-1 settings, and then answer the question below.

Name	Remote
Comments	Comments
<b>Network</b>	
IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Remote Gateway	Static IP address
IP Address	10.0.10.1
Interface	port1
Mode Config	<input type="checkbox"/>
NAT Traversal	<input checked="" type="checkbox"/>
Keepalive Frequency	10
Dead Peer Detection	<input checked="" type="checkbox"/>

The VPN is up, and DPD packets are being exchanged between both IPsec gateways; however, traffic cannot pass through the tunnel. To diagnose, the administrator enters these CLI commands:

```
diagnose vpn ike log-filter src-add4 10.0.10.1
diagnose debug application ike-1
diagnose debug enable
```

However, the IKE real time debug does not show any output. Why?

- A. The debug output shows phases 1 and 2 negotiations only. Once the tunnel is up, it does not show any more output.
- B. The log-filter setting was set incorrectly. The VPN's traffic does not match this filter.
- C. The debug shows only error messages. If there is no output, then the tunnel is operating normally.
- D. The debug output shows phase 1 negotiation only. After that, the administrator must enable the following real time debug: `diagnose debug application ipsec -1`.

Correct Answer: D

#### QUESTION 4

What events are recorded in the crashlogs of a FortiGate device? (Choose two.)

- A. A process crash.
- B. Configuration changes.

- C. Changes in the status of any of the FortiGuard licenses.
- D. System entering to and leaving from the proxy conserve mode.

Correct Answer: AD

---

#### QUESTION 5

An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer. If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

- A. diagnose sniffer packet any `udp port 500\`
- B. diagnose sniffer packet any `udp port 4500\`
- C. diagnose sniffer packet any `esp\`
- D. diagnose sniffer packet any `udp port 500 or udp port 4500\`

Correct Answer: C

[Latest NSE7 Dumps](#)

[NSE7 PDF Dumps](#)

[NSE7 Exam Questions](#)