NSE5 $^{\text{Q\&As}}$

Fortinet Network Security Expert 5 Written Exam (500)

Pass Fortinet NSE5 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse5.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following DLP actions will override any other action?

A. Exempt

B. Quarantine Interface

C. Block

D. None

Correct Answer: A

QUESTION 2

Which one of the following statements is correct about raw log messages?

A. Logs have a header and a body section. The header will have the same layout for every log message. The body section will change layout from one type of log message to another.

B. Logs have a header and a body section. The header and body will change layout from one type of log message to another.

C. Logs have a header and a body section. The header and body will have the same layout for every log message.

Correct Answer: A

QUESTION 3

Data Leak Prevention archiving gives the ability to store files and message data onto a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.)

A. SNMP

B. IPSec

C. SMTP

D. POP3

E. HTTP

Correct Answer: CDE

QUESTION 4

Which of the following statements correctly describe Transparent Mode operation? (Select all that apply.)

A. The FortiGate unit acts as transparent bridge and routes traffic using Layer-2 forwarding.

B. Ethernet packets are forwarded based on destination MAC addresses NOT IPs.

C. The device is transparent to network hosts.

D. Permits inline traffic inspection and firewalling without changing the IP scheme of the network.

E. All interfaces must be on different IP subnets.

Correct Answer: ABCD

QUESTION 5

An administrator is examining the attack logs and notices the following entry:

```
device_id=FG100A3907508962 log_id=18432 subtype=anomaly type=ips timestamp=1270017358 pri=alert
itime=1270017893 severity=critical src=192.168.1.52 dst=64.64.64.64 src_int=internal serial=0 status=clear_session
proto=6 service=http vd=root count=1 src_port=35094 dst_port=80 attack_id=100663402 sensor=protect- servers
ref=http://www.fortinet.com/ids/VID100663402 msg="anomaly: tcp_src_session, 2 > threshold 1" policyid=0
carrier_ep=N/A profile=N/A dst_int=N/A

user=N/A group=N/A
```

Based solely upon this log message, which of the following statements is correct?

A. This attack was blocked by the HTTP protocol decoder.

B. This attack was caught by the DoS sensor "protect-servers".

C. This attack was launched against the FortiGate unit itself rather than a host behind the FortiGate unit.

D. The number of concurrent connections to destination IP address 64.64.64.64 has exceeded the configured threshold.

Correct Answer: B