



# EndExam

## QUESTION & ANSWER

Accurate study guides, High passing rate!



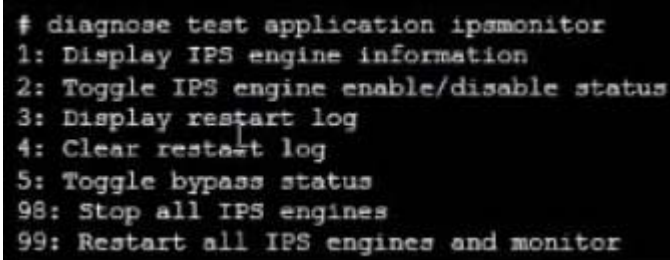
We offer free update service for one year!  
<http://www.endexam.com>

**Exam : NSE4\_FGT-6.4**

**Title : Fortinet NSE 4 - FortiOS 6.4**

**Version : DEMO**

1.Refer to the exhibit.



```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

- A. The IPS engine was inspecting high volume of traffic.
- B. The IPS engine was unable to prevent an intrusion attack.
- C. The IPS engine was blocking all traffic.
- D. The IPS engine will continue to run in a normal state.

**Answer: A**

2.Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

- A. hard-timeout
- B. auth-on-demand
- C. soft-timeout
- D. new-session
- E. Idle-timeout

**Answer: A,D,E**

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221>

3.FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.

Which two other security profiles can you apply to the security policy? (Choose two.)

- A. Antivirus scanning
- B. File filter
- C. DNS filter
- D. Intrusion prevention

**Answer: A,D**

4.When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

- A. Log ID
- B. Universally Unique Identifier
- C. Policy ID
- D. Sequence ID

**Answer: B**

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies>

5.Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

- A. The subject field in the server certificate
- B. The serial number in the server certificate
- C. The server name indication (SNI) extension in the client hello message
- D. The subject alternative name (SAN) field in the server certificate
- E. The host field in the HTTP header

**Answer:** ACD

**Explanation:**

Reference: <https://checkthefirewall.com/blogs/fortinet/ssl-inspection>