



NSE4_FGT-6.4^{Q&As}

Fortinet NSE 4 - FortiOS 6.4

Pass Fortinet NSE4_FGT-6.4 Exam with 100% Guarantee

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

https://www.geekcert.com/nse4_fgt-6-4.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

Which two statements are true about the Security Fabric rating? (Choose two.)

- A. It provides executive summaries of the four largest areas of security focus.
- B. Many of the security issues can be fixed immediately by clicking Apply where available.
- C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.
- D. The Security Fabric rating is a free service that comes bundled with all FortiGate devices.

Correct Answer: BC

FortiGate_Security_6.4_Study_Guide-Online. page 89

QUESTION 2

An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

- A. The strict RPF check is run on the first sent and reply packet of any new session.
- B. Strict RPF checks the best route back to the source using the incoming interface.
- C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
- D. Strict RPF allows packets back to sources with all active routes.

Correct Answer: B

QUESTION 3

What is the primary FortiGate election process when the HA override setting is disabled?

- A. Connected monitored ports > System uptime > Priority > FortiGate Serial number
- B. Connected monitored ports > HA uptime > Priority > FortiGate Serial number
- C. Connected monitored ports > Priority > HA uptime > FortiGate Serial number
- D. Connected monitored ports > Priority > System uptime > FortiGate Serial number

Correct Answer: B

Reference: <http://myitmicroblog.blogspot.com/2018/11/what-should-you-know-about-ha-override.html>

QUESTION 4

Which three methods are used by the collector agent for AD polling? (Choose three.)



- A. FortiGate polling
- B. NetAPI
- C. Novell API
- D. WMI
- E. WinSecLog

Correct Answer: BDE

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

QUESTION 5

Refer to the exhibit.

```
1: date=2020-08-14 time=06:28:24 logid= "0316013056" type= "utm" subtype= "webfilter"
eventtype= "ftgd_blk" level= "warning" vd= "root" eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= "port3" srcintfrole=
"undefined" dstip=159.65.216.232 dstport=443 dstintf= "port1" dstintfrole= "wan" proto=6
service= "HTTPS" hostname= "etp-experiment-1.dummytracker.org" profile= "default"
action= "blocked" rectype= "direct" url= "https://etp-experiment-1.dummytracker.org/"
sentbyte=517 rcvbyte=0 direction= "outgoing" msg= "URL belongs to a denied category in
policy" method= "domain" cat=26 catdesc= "Malicious Websites" crscore=30 craction=
4194304 crlevel= "high"
```

Based on the raw log, which two statements are correct? (Choose two.)

- A. Traffic is blocked because Action is set to DENY in the firewall policy.
- B. Traffic belongs to the root VDOM.
- C. This is a security log.
- D. Log severity is set to error on FortiGate.

Correct Answer: AC

[Latest NSE4_FGT-6.4 Dumps](#)

[NSE4_FGT-6.4 Study Guide](#) [NSE4_FGT-6.4 Braindumps](#)