



**Vendor:** Fortinet

**Exam Code:** NSE6

**Exam Name:** Fortinet Advanced Products Professional

**Version:** DEMO

### QUESTION 1

When an administrator attempts to manage FortiGate from an IP address that is not a trusted host, what happens?

- A. FortiGate will still subject that person's traffic to firewall policies; it will not bypass them.
- B. FortiGate will drop the packets and not respond.
- C. FortiGate responds with a block message, indicating that it will not allow that person to log in.
- D. FortiGate responds only if the administrator uses a secure protocol. Otherwise, it does not respond

**Answer: B**

### QUESTION 2

A backup file begins with this line:

```
#config-version=FGVM64-5.02-FW-build589-140613:opmode=0:vdom=0:user=admin  
#conf_file_ver=3881503152630288414 #buildno=0589 #global_vdom=1 Can you restore it to a  
FortiWiFi 60D?
```

- A. Yes
- B. Yes, but only if you replace the "#conf\_file\_ver" line so that it contains the serial number of that specific FortiWiFi 60D.
- C. Yes, but only if it is running the same version of FortiOS, or a newer compatible version.
- D. No

**Answer: D**

### QUESTION 3

Examine this log entry.

What does the log indicate? (Choose three.)

```
date=2013-12-04 time=09:30:18 logid=0100032001 type=event  
subtype=system level=information vd="root" user="admin"  
ui=http(192.168.1.112) action=login status=success reason=none  
profile="super_admin" msg="Administrator admin logged in successfully  
from http(192.168.1.112)"
```

- A. In the GUI, the log entry was located under "Log & Report > Event Log > User".
- B. In the GUI, the log entry was located under "Log & Report > Event Log > System".
- C. In the GUI, the log entry was located under "Log & Report > Traffic Log > Local Traffic".
- D. The connection was encrypted.
- E. The connection was unencrypted.
- F. The IP of the FortiGate interface that "admin" connected to was 192.168.1.112.
- G. The IP of the computer that "admin" connected from was 192.168.1.112.

**Answer: BEG**

### QUESTION 4

Where are most of the security events logged?

- A. Security log

- B. Forward Traffic log
- C. Event log
- D. Alert log
- E. Alert Monitoring Console

**Answer:** C

**QUESTION 5**

What determines whether a log message is generated or not?

- A. Firewall policy setting
- B. Log Settings in the GUI
- C. 'config log' command in the CLI
- D. Syslog
- E. Webtrends

**Answer:** A

**QUESTION 6**

Which of the following are considered log types? (Choose three.)

- A. Forward log
- B. Traffic log
- C. Syslog
- D. Event log
- E. Security log

**Answer:** BDE

**QUESTION 7**

What attributes are always included in a log header? (Choose three.)

- A. policyid
- B. level
- C. user
- D. time
- E. subtype
- F. duration

**Answer:** BDE

**QUESTION 8**

What log type would indicate whether a VPN is going up or down?

- A. Event log
- B. Security log
- C. Forward log
- D. Syslog

**Answer: A**

**QUESTION 9**

Which correctly define "Section View" and "Global View" for firewall policies? (Choose two.)

- A. Section View lists firewall policies primarily by their interface pairs.
- B. Section View lists firewall policies primarily by their sequence number.
- C. Global View lists firewall policies primarily by their interface pairs.
- D. Global View lists firewall policies primarily by their policy sequence number.
- E. The 'any' interface may be used with Section View.

**Answer: AD**

**QUESTION 10**

What protocol cannot be used with the active authentication type?

- A. Local
- B. RADIUS
- C. LDAP
- D. RSO

**Answer: D**

**QUESTION 11**

When configuring LDAP on the FortiGate as a remote database for users, what is not a part of the configuration?

- A. The name of the attribute that identifies each user (Common Name Identifier).
- B. The user account or group element names (user DN).
- C. The server secret to allow for remote queries (Primary server secret).
- D. The credentials for an LDAP administrator (password).

**Answer: C**

**QUESTION 12**

In "diag debug flow" output, you see the message "Allowed by Policy-1: SNAT". Which is true?

- A. The packet matched the topmost policy in the list of firewall policies.
- B. The packet matched the firewall policy whose policy ID is 1.
- C. The packet matched a firewall policy, which allows the packet and skips UTM checks
- D. The policy allowed the packet and applied session NAT.

**Answer: B**

## Thank You for Trying Our Product

### Braindump2go Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.braindump2go.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives<sup>®</sup>

**10% Discount Coupon Code: BDNT2014**