

# NSE6\_FWB-6.4<sup>Q&As</sup>

Fortinet NSE 6 - FortiWeb 6.4

## Pass Fortinet NSE6\_FWB-6.4 Exam with 100% Guarantee

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

[https://www.pass2lead.com/nse6\\_fwb-6-4.html](https://www.pass2lead.com/nse6_fwb-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**

What key factor must be considered when setting brute force rate limiting and blocking?

- A. A single client contacting multiple resources
- B. Multiple clients sharing a single Internet connection
- C. Multiple clients from geographically diverse locations
- D. Multiple clients connecting to multiple resources

Correct Answer: B

<https://training.fortinet.com/course/view.php?id=3363>

What is one key factor that you must consider when setting brute force rate limiting and blocking? Multiple clients sharing a single Internet connection

---

**QUESTION 2**

Which two statements about running a vulnerability scan are true? (Choose two.)

- A. You should run the vulnerability scan during a maintenance window.
- B. You should run the vulnerability scan in a test environment.
- C. Vulnerability scanning increases the load on FortiWeb, so it should be avoided.
- D. You should run the vulnerability scan on a live website to get accurate results.

Correct Answer: AB

Should the Vulnerability Scanner allow it, SVMS will set the scan schedule (or schedules) to run in a maintenance window. SVMS will advise Client of the scanner's ability to complete the scan(s) within the maintenance window. Vulnerabilities on live web sites. Instead, duplicate the web site and its database in a test environment.

Reference: [https://www.trustwave.com/media/17427/trustwave\\_mss\\_managed-3rd-party-vulnerability-scanning.pdf](https://www.trustwave.com/media/17427/trustwave_mss_managed-3rd-party-vulnerability-scanning.pdf)  
[https://help.fortinet.com/fweb/552/Content/FortiWeb/fortiweb-admin/vulnerability\\_scans.htm](https://help.fortinet.com/fweb/552/Content/FortiWeb/fortiweb-admin/vulnerability_scans.htm)

---

**QUESTION 3**

When the FortiWeb is configured in Reverse Proxy mode and the FortiGate is configured as an SNAT device, what IP address will the FortiGate's Real Server configuration point at?

- A. Virtual Server IP on the FortiGate
- B. Server's real IP
- C. FortiWeb's real IP

D. IP Address of the Virtual Server on the FortiWeb

Correct Answer: A

---

#### QUESTION 4

When generating a protection configuration from an auto learning report what critical step must you do before generating the final protection configuration?

- A. Restart the FortiWeb to clear the caches
- B. Drill down in the report to correct any false positives.
- C. Activate the report to create t profile
- D. Take the FortiWeb offline to apply the profile

Correct Answer: B

---

#### QUESTION 5

In which scenario might you want to use the compression feature on FortiWeb?

- A. When you are serving many corporate road warriors using 4G tablets and phones
- B. When you are offering a music streaming service
- C. When you want to reduce buffering of video streams
- D. Never, since most traffic today is already highly compressed

Correct Answer: A

<https://training.fortinet.com/course/view.php?id=3363> When might you want to use the compression feature on FortiWeb? When you are serving many road warriors who are using 4G tablets and phones

[Latest NSE6\\_FWB-6.4 Dumps](#)

[NSE6\\_FWB-6.4 VCE Dumps](#)

[NSE6\\_FWB-6.4 Study Guide](#)