



## **Fortinet**

### **Exam Questions NSE6\_FWB-6.4**

Fortinet NSE 6 - FortiWeb 6.4

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

What capability can FortiWeb add to your Web App that your Web App may or may not already have?

- A. Automatic backup and recovery
- B. High Availability
- C. HTTP/HTML Form Authentication
- D. SSL Inspection

**Answer: C**

#### NEW QUESTION 2

Which two statements about the anti-defacement feature on FortiWeb are true? (Choose two.)

- A. Anti-defacement can redirect users to a backup web server, if it detects a change.
- B. Anti-defacement downloads a copy of your website to RAM, in order to restore a clean image, if it detects defacement.
- C. FortiWeb will only check to see if there are changes on the web server; it will not download the whole file each time.
- D. Anti-defacement does not make a backup copy of your databases.

**Answer: CD**

#### Explanation:

Anti-defacement backs up web pages only, not databases.

If it detects any file changes, the FortiWeb appliance will download a new backup revision.

#### NEW QUESTION 3

How does an ADOM differ from a VDOM?

- A. ADOMs do not have virtual networking
- B. ADOMs improve performance by offloading some functions.
- C. ADOMs only affect specific functions, and do not provide full separation like VDOMs do.
- D. Allows you to have 1 administrator for multiple tenants

**Answer: A**

#### NEW QUESTION 4

When integrating FortiWeb and FortiAnalyzer, why is the selection for FortiWeb Version critical? (Choose two)

- A. Defines Log file format
- B. Defines communication protocol
- C. Defines Database Schema
- D. Defines Log storage location

**Answer: AD**

#### NEW QUESTION 5

In which two operating modes can FortiWeb modify HTTP packets? (Choose two.)

- A. Offline protection
- B. Transparent inspection
- C. True transparent proxy
- D. Reverse proxy

**Answer: CD**

#### NEW QUESTION 6

What other consideration must you take into account when configuring Defacement protection

- A. Use FortiWeb to block SQL Injections and keep regular backups of the Database
- B. Also incorporate a FortiADC into your network
- C. Non
- D. FortiWeb completely secures the site against defacement attacks
- E. Configure the FortiGate to perform Anti-Defacement as well

**Answer: A**

#### NEW QUESTION 7

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

**Answer: A**

**Explanation:**

<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

**NEW QUESTION 8**

Which of the following would be a reason for implementing rewrites?

- A. Page has been moved to a new URL
- B. Page has been moved to a new IP address
- C. Replace vulnerable functions.
- D. Send connection to secure channel

**Answer: C**

**NEW QUESTION 9**

An e-commerce web app is used by small businesses. Clients often access it from offices behind a router, where clients are on an IPv4 private network LAN. You need to protect the web application from denial of service attacks that use request floods.

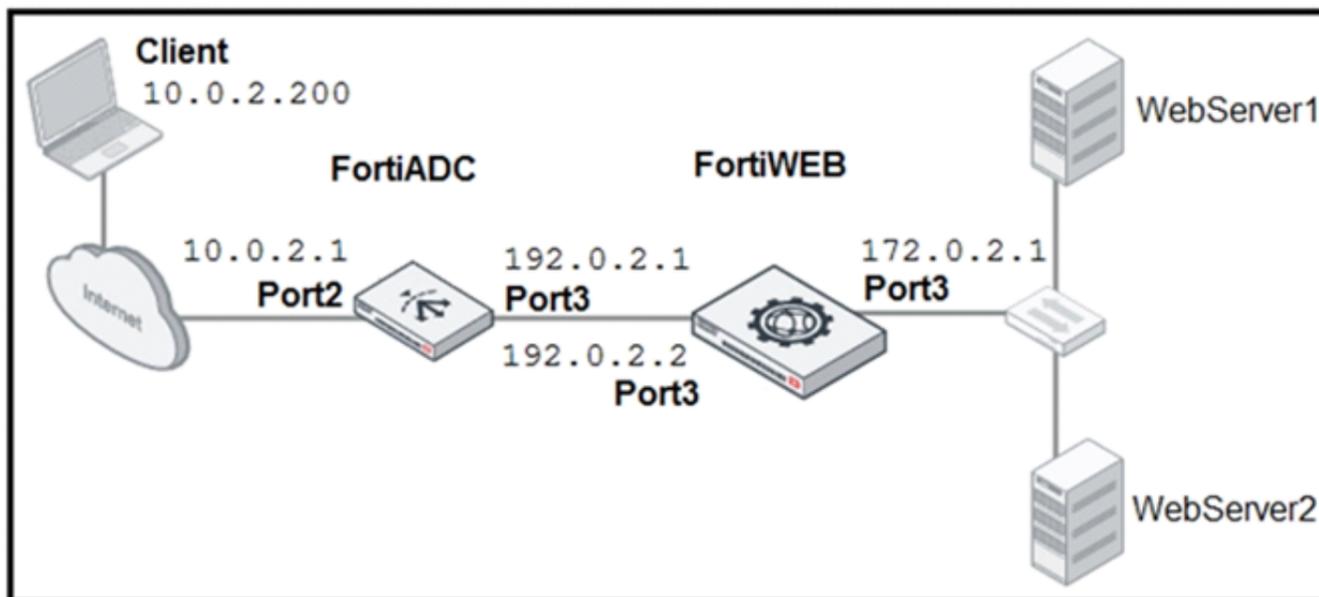
What FortiWeb feature should you configure?

- A. Enable "Shared IP" and configure the separate rate limits for requests from NATted source IPs.
- B. Configure FortiWeb to use "X-Forwarded-For:" headers to find each client's private network IP, and to block attacks using that.
- C. Enable SYN cookies.
- D. Configure a server policy that matches requests from shared Internet connections.

**Answer: C**

**NEW QUESTION 10**

Refer to the exhibit.



FortiADC is applying SNAT to all inbound traffic going to the servers. When an attack occurs, FortiWeb blocks traffic based on the 192.0.2.1 source IP address, which belongs to FortiADC. The setup is breaking all connectivity and genuine clients are not able to access the servers.

What must the administrator do to avoid this problem? (Choose two.)

- A. Enable the Use X-Forwarded-For setting on FortiWeb.
- B. No Special configuration is required; connectivity will be re-established after the set timeout.
- C. Place FortiWeb in front of FortiADC.
- D. Enable the Add X-Forwarded-For setting on FortiWeb.

**Answer: AC**

**Explanation:**

Configure your load balancer to insert or append to an X-Forwarded-For:, X-Real-IP:, or other HTTP X- header. Also configure FortiWeb to find the original attacker's or client's IP address in that HTTP header

**NEW QUESTION 10**

Under what circumstances would you want to use the temporary uncompress feature of FortiWeb?

- A. In the case of compression being done on the FortiWeb, to inspect the content of the compressed file
- B. In the case of the file being a .MP3 music file
- C. In the case of compression being done on the web server, to inspect the content of the compressed file.
- D. In the case of the file being an .MP4 video

**Answer: C**

**NEW QUESTION 15**

Which three statements about HTTPS on FortiWeb are true? (Choose three.)

- A. For SNI, you select the certificate that FortiWeb will present in the server pool, not in the server policy.
- B. After enabling HSTS, redirects to HTTPS are no longer necessary.
- C. In true transparent mode, the TLS session terminator is a protected web server.

- D. Enabling RC4 protects against the BEAST attack, but is not recommended if you configure FortiWeb to only offer TLS 1.2.
- E. In transparent inspection mode, you select which certificate that FortiWeb will present in the server pool, not in the server policy.

**Answer:** CDE

#### NEW QUESTION 16

What role does FortiWeb play in ensuring PCI DSS compliance?

- A. It provides the ability to securely process cash transactions.
- B. It provides the required SQL server protection.
- C. It provides the WAF required by PCI.
- D. It provides credit card processing capabilities.

**Answer:** C

#### NEW QUESTION 17

Which implementation is best suited for a deployment that must meet compliance criteria?

- A. SSL Inspection with FortiWeb in Transparency mode
- B. SSL Offloading with FortiWeb in reverse proxy mode
- C. SSL Inspection with FortiWeb in Reverse Proxy mode
- D. SSL Offloading with FortiWeb in Transparency Mode

**Answer:** C

#### NEW QUESTION 22

When viewing the attack logs on FortiWeb, which client IP address is shown when you are using XFF header rules?

- A. FortiGate public IP
- B. FortiWeb IP
- C. FortiGate local IP
- D. Client real IP

**Answer:** D

#### Explanation:

When an XFF header reaches Alteon from a client, Alteon removes all the content from the header and injects the client IP address. Alteon then forwards the header to the server.

#### NEW QUESTION 24

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

**Answer:** B

#### Explanation:

<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

#### NEW QUESTION 25

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 a profile
- D. Take the FortiWeb offline to apply the profile

**Answer:** B

#### NEW QUESTION 30

Review the following configuration:

```
config waf machine-learning-policy
edit 1
set sample-limit-by-ip 0
next
end
```

What is the expected result of this configuration setting?

- A. When machine learning (ML) is in its collecting phase, FortiWeb will accept an unlimited number of samples from the same source IP address.
- B. When machine learning (ML) is in its running phase, FortiWeb will accept an unlimited number of samples from the same source IP address.

- C. When machine learning (ML) is in its collecting phase, FortiWeb will not accept any samples from any source IP addresses.
- D. When machine learning (ML) is in its running phase, FortiWeb will accept a set number of samples from the same source IP address.

**Answer:** A

#### NEW QUESTION 31

Which algorithm is used to build mathematical models for bot detection?

- A. HCM
- B. SVN
- C. SVM
- D. HMM

**Answer:** C

#### Explanation:

FortiWeb uses SVM (Support Vector Machine) algorithm to build up the bot detection model

#### NEW QUESTION 34

A client is trying to start a session from a page that would normally be accessible only after the client has logged in. When a start page rule detects the invalid session access, what can FortiWeb do? (Choose three.)

- A. Display an access policy message, then allow the client to continue
- B. Redirect the client to the login page
- C. Allow the page access, but log the violation
- D. Prompt the client to authenticate
- E. Reply with a 403 Forbidden HTTP error

**Answer:** BCE

#### NEW QUESTION 35

Under which circumstances does FortiWeb use its own certificates? (Choose Two)

- A. Secondary HTTPS connection to server where FortiWeb acts as a client
- B. HTTPS to clients
- C. HTTPS access to GUI
- D. HTTPS to FortiGate

**Answer:** AC

#### NEW QUESTION 37

You are using HTTP content routing on FortiWeb. Requests for web app A should be forwarded to a cluster of web servers which all host the same web app. Requests for web app B should be forwarded to a different, single web server. Which is true about the solution?

- A. Static or policy-based routes are not required.
- B. To achieve HTTP content routing, you must chain policies: the first policy accepts all traffic, and forwards requests for web app A to the virtual server for policy C. It also forwards requests for web app B to the virtual server for policy D. Policy A and Policy B apply their app-specific protection profiles, and then distribute that app's traffic among all members of the server farm.
- E. You must put the single web server into a server pool in order to use it with HTTP content routing.
- F. The server policy applies the same protection profile to all its protected web apps.

**Answer:** B

#### NEW QUESTION 38

.....

## Relate Links

**100% Pass Your NSE6\_FWB-6.4 Exam with ExamBible Prep Materials**

[https://www.exambible.com/NSE6\\_FWB-6.4-exam/](https://www.exambible.com/NSE6_FWB-6.4-exam/)

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>