

# Fortinet

## Exam Questions NSE6\_FWB-6.4

Fortinet NSE 6 - FortiWeb 6.4



#### NEW QUESTION 1

How does FortiWeb protect against defacement attacks?

- A. It keeps a complete backup of all files and the database.
- B. It keeps hashes of files and periodically compares them to the server.
- C. It keeps full copies of all files and directories.
- D. It keeps a live duplicate of the database.

**Answer: B**

#### Explanation:

The anti-defacement feature examines a web site's files for changes at specified time intervals. If it detects a change that could indicate a defacement attack, the FortiWeb appliance can notify you and quickly react by automatically restoring the web site contents to the previous backup.

#### NEW QUESTION 2

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 3

What must you do with your FortiWeb logs to ensure PCI DSS compliance?

- A. Store in an off-site location
- B. Erase them every two weeks
- C. Enable masking of sensitive data
- D. Compress them into a .zip file format

**Answer: C**

#### NEW QUESTION 4

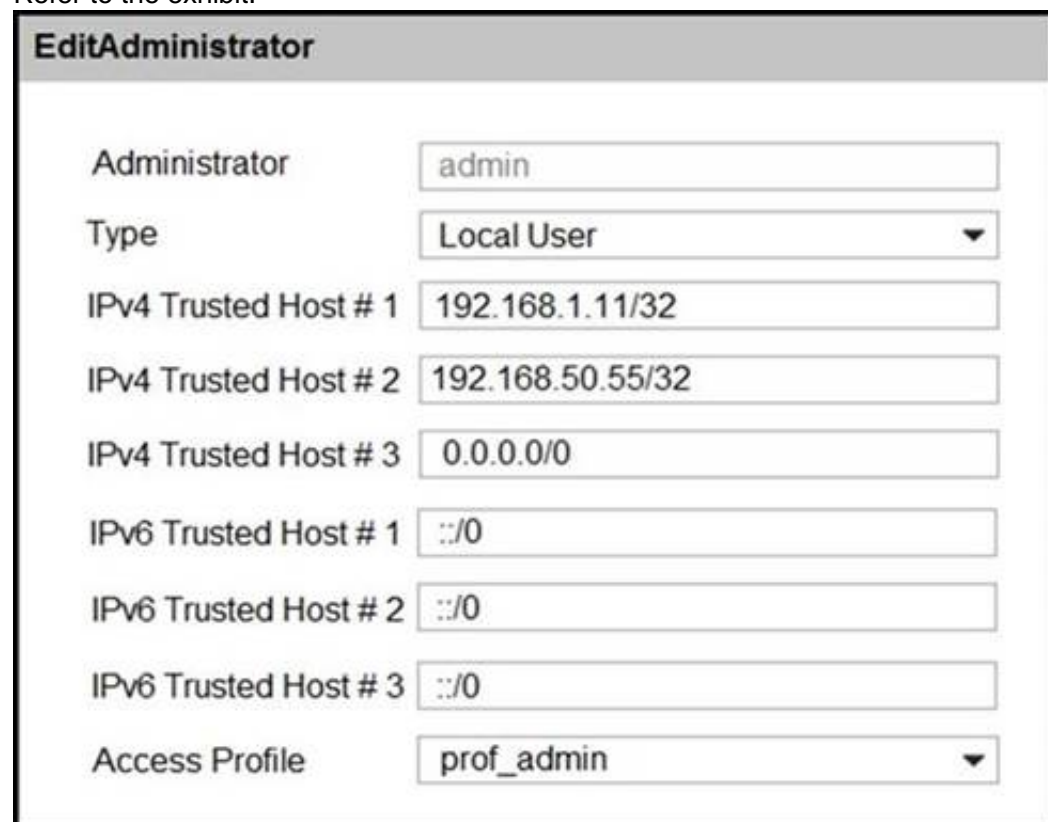
When integrating FortiWeb and FortiAnalyzer, why is the selection for FortiWeb Version critical? (Choose two)

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

**Answer: AD**

#### NEW QUESTION 5

Refer to the exhibit.



EditAdministrator	
Administrator	admin
Type	Local User
IPv4 Trusted Host # 1	192.168.1.11/32
IPv4 Trusted Host # 2	192.168.50.55/32
IPv4 Trusted Host # 3	0.0.0.0/0
IPv6 Trusted Host # 1	::/0
IPv6 Trusted Host # 2	::/0
IPv6 Trusted Host # 3	::/0
Access Profile	prof_admin

There is only one administrator account configured on FortiWeb. What must an administrator do to restrict any brute force attacks that attempt to gain access to the FortiWeb management GUI?

- A. Delete the built-in administrator user and create a new one.
- B. Configure IPv4 Trusted Host # 3 with a specific IP address.
- C. The configuration changes must be made on the upstream device.
- D. Change the Access Profile to Read\_Only.

**Answer:** B

#### NEW QUESTION 6

You've configured an authentication rule with delegation enabled on FortiWeb. What happens when a user tries to access the web application?

- A. FortiWeb redirects users to a FortiAuthenticator page, then if the user authenticates successfully, FortiGate signals to FortiWeb to allow access to the web app
- B. FortiWeb redirects the user to the web app's authentication page
- C. FortiWeb forwards the HTTP challenge from the server to the client, then monitors the reply, allowing access if the user authenticates successfully
- D. FortiWeb replies with a HTTP challenge of behalf of the server, then if the user authenticates successfully, FortiWeb allows the request and also includes credentials in the request that it forwards to the web app

**Answer:** A

#### NEW QUESTION 7

What can an administrator do if a client has been incorrectly period blocked?

- A. Nothing, it is not possible to override a period block.
- B. Manually release the IP address from the temporary blacklist.
- C. Force a new IP address to the client.
- D. Disconnect the client from the network.

**Answer:** B

#### Explanation:

Block Period

Enter the number of seconds that you want to block the requests. The valid range is 1–3,600 seconds. The default value is 60 seconds.

This option only takes effect when you choose Period Block in Action.

Note: That's a temporary blacklist so you can manually release them from the blacklist.

#### NEW QUESTION 8

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 9

Refer to the exhibit.

Model Settings	Model Status
<b>Edit Model Settings</b>	
<b>Sampling Settings</b>	
Client Identification Method	IP and User-Agent
Sampling Time per Vector	5 Minutes (1 – 10)
Sample Count per Client per Hour	3 (1 – 60)
Sample Count	1000 (10 – 10000)
<b>Model Building Settings</b>	
Model Type	Moderate
<b>Anomaly Detection Settings</b>	
Anomaly Count	3 (1 – 65535)
Bot Confirmation	<input type="checkbox"/>
Dynamically Update Model	<input checked="" type="checkbox"/>
<b>Action Settings</b>	
Action	Deny (no log)
Block Period	60 Seconds (1 – 3600)
Severity	High
Trigger Policy	Please Select

Many legitimate users are being identified as bots. FortiWeb bot detection has been configured with the settings shown in the exhibit. The FortiWeb administrator has already verified that the current model is accurate.

What can the administrator do to fix this problem, making sure that real bots are not allowed through FortiWeb?

- A. Change Model Type to Strict
- B. Change Action under Action Settings to Alert
- C. Disable Dynamically Update Model
- D. Enable Bot Confirmation

**Answer:** D

**Explanation:**

Bot Confirmation

If the number of anomalies from a user has reached the Anomaly Count, the system executes Bot Confirmation before taking actions.

The Bot Confirmation is to confirm if the user is indeed a bot. The system sends RBE (Real Browser Enforcement) JavaScript or CAPTCHA to the client to double check if it's a real bot.

**NEW QUESTION 10**

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 10**

In which operation mode(s) can FortiWeb modify HTTP packets? (Choose two.)

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

**Answer:** CD

**NEW QUESTION 14**

FortiWeb offers the same load balancing algorithms as FortiGate.

Which two Layer 7 switch methods does FortiWeb also offer? (Choose two.)

- A. Round robin
- B. HTTP session-based round robin
- C. HTTP user-based round robin
- D. HTTP content routes

**Answer:** AD

**NEW QUESTION 15**

You are configuring FortiAnalyzer to store logs from FortiWeb. Which is true?

- A. FortiAnalyzer will store antivirus and DLP archives from FortiWeb.
- B. You must enable ADOMs on FortiAnalyzer.
- C. To store logs from FortiWeb 6.4, on FortiAnalyzer, you must select "FortiWeb 6.1".
- D. FortiWeb will query FortiAnalyzer for reports, instead of generating them locally.

**Answer:** B

**NEW QUESTION 17**

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 20**

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 25**

Refer to the exhibit.



Based on the configuration, what would happen if this FortiWeb were to lose power? (Choose two.)

- A. Traffic that passes between port5 and port6 will be inspected.
- B. Traffic will be interrupted between port3 and port4.
- C. All traffic will be interrupted.
- D. Traffic will pass between port5 and port6 uninspected.

**Answer:** BD

**NEW QUESTION 27**

What role does FortiWeb play in ensuring PCI DSS compliance?

- A. PCI specifically requires a WAF
- B. Provides credit card processing capabilities
- C. Provide ability to securely process cash transactions
- D. Provides load balancing between multiple web servers

**Answer:** A

**Explanation:**

FortiWeb helps you meet all PCI requirements, but PCI now specifically recommends using a WAF, and developing remediations against the top 10 vulnerabilities, according to OWASP.

**NEW QUESTION 32**

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 34**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### NSE6\_FWB-6.4 Practice Exam Features:

- \* NSE6\_FWB-6.4 Questions and Answers Updated Frequently
- \* NSE6\_FWB-6.4 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE6\_FWB-6.4 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* NSE6\_FWB-6.4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE6\\_FWB-6.4 Practice Test Here](#)**