

Fortinet

Exam Questions NSE6_FWB-6.4

Fortinet NSE 6 - FortiWeb 6.4



NEW QUESTION 1

How does your FortiWeb configuration differ if the FortiWeb is upstream of the SNAT device instead of downstream of the SNAT device?

- A. You must enable the “Use” X-Forwarded-For: option.
- B. FortiWeb must be set for Transparent Mode
- C. No special configuration required
- D. You must enable “Add” X-Forwarded-For: instead of the “Use” X-Forwarded-For: option.

Answer: D

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

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 on 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 6

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 7

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 8

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 9

When FortiWeb triggers a redirect action, which two HTTP codes does it send to the client to inform the browser of the new URL? (Choose two.)

- A. 403
- B. 302
- C. 301
- D. 404

Answer: BC

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 10

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 11

Refer to the exhibit.

| Model Settings | | Model Status |
|-----------------------------------|-------------------------------------|--------------------|
| Edit Model Settings | | |
| Sampling Settings | | |
| 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) |
| Model Building Settings | | |
| Model Type | Moderate | |
| Anomaly Detection Settings | | |
| Anomaly Count | 3 | (1 – 65535) |
| Bot Confirmation | <input type="checkbox"/> | |
| Dynamically Update Model | <input checked="" type="checkbox"/> | |
| Action Settings | | |
| 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 14

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 18

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 20

When is it possible to use a self-signed certificate, rather than one purchased from a commercial certificate authority?

- A. If you are a small business or home office
- B. If you are an enterprise whose employees use only mobile devices
- C. If you are an enterprise whose resources do not need security

D. If you are an enterprise whose computers all trust your active directory or other CA server

Answer: D

NEW QUESTION 23

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 25

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 26

Which of the following FortiWeb features is part of the mitigation tools against OWASP A4 threats?

- A. Sensitive info masking
- B. Poison Cookie detection
- C. Session Management
- D. Brute Force blocking

Answer: C

NEW QUESTION 27

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 29

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

Answer: A

NEW QUESTION 31

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 34

Which would be a reason to implement HTTP rewriting?

- A. The original page has moved to a new URL
- B. To replace a vulnerable function in the requested URL
- C. To send the request to secure channel
- D. The original page has moved to a new IP address

Answer: B

Explanation:

Create a new URL rewriting rule.

NEW QUESTION 38

You are deploying FortiWeb 6.4 in an Amazon Web Services cloud. Which 2 lines of this initial setup via CLI are incorrect? (Choose two.)

```
1 config system settings
2 set opmode transparent
3 set gateway 10.0.0.1
4 end
5 config system interface
6 set port1
7 set ip 10.0.0.5
8 set allowaccess https ssh ping
9 end
```

- A. 6
- B. 9
- C. 3
- D. 2

Answer: AC

NEW QUESTION 43

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 47

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 52

What is one of the key benefits of the FortiGuard IP reputation feature?

- A. It maintains a list of private IP addresses.
- B. It provides a document of IP addresses that are suspect, so that administrators can manually update their blacklists.
- C. It is updated once per year.
- D. It maintains a list of public IPs with a bad reputation for participating in attacks.

Answer: D

Explanation:

FortiGuard IP Reputation service assigns a poor reputation, including virus-infected clients and malicious spiders/crawlers.

NEW QUESTION 53

The FortiWeb machine learning (ML) feature is a two-phase analysis mechanism. Which two functions does the first layer perform? (Choose two.)

- A. Determines whether an anomaly is a real attack or just a benign anomaly that should be ignored
- B. Builds a threat model behind every parameter and HTTP method
- C. Determines if a detected threat is a false-positive or not
- D. Determines whether traffic is an anomaly, based on observed application traffic over time

Answer: BD

Explanation:

The first layer uses the Hidden Markov Model (HMM) and monitors access to the application and collects data to build a mathematical model behind every parameter and HTTP method.

NEW QUESTION 58

.....

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](#)