

Exam Questions NSE6_FWB-6.4

Fortinet NSE 6 - FortiWeb 6.4

https://www.2passeasy.com/dumps/NSE6_FWB-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

In Reverse proxy mode, how does FortiWeb handle traffic that does not match any defined policies?

- A. Non-matching traffic is allowed
- B. non-Matching traffic is held in buffer
- C. Non-matching traffic is Denied
- D. Non-matching traffic is rerouted to FortiGate

Answer: C

NEW QUESTION 4

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 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

Which operation mode does not require additional configuration in order to allow FTP traffic to your web server?

- A. Offline Protection
- B. Transparent Inspection
- C. True Transparent Proxy
- D. Reverse-Proxy

Answer: B

NEW QUESTION 7

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 8

Which regex expression is the correct format for redirecting the URL <http://www.example.com>?

- A. `www\.example\.com`
- B. `www.example.com`
- C. `www\example\com`
- D. `www/.example/.com`

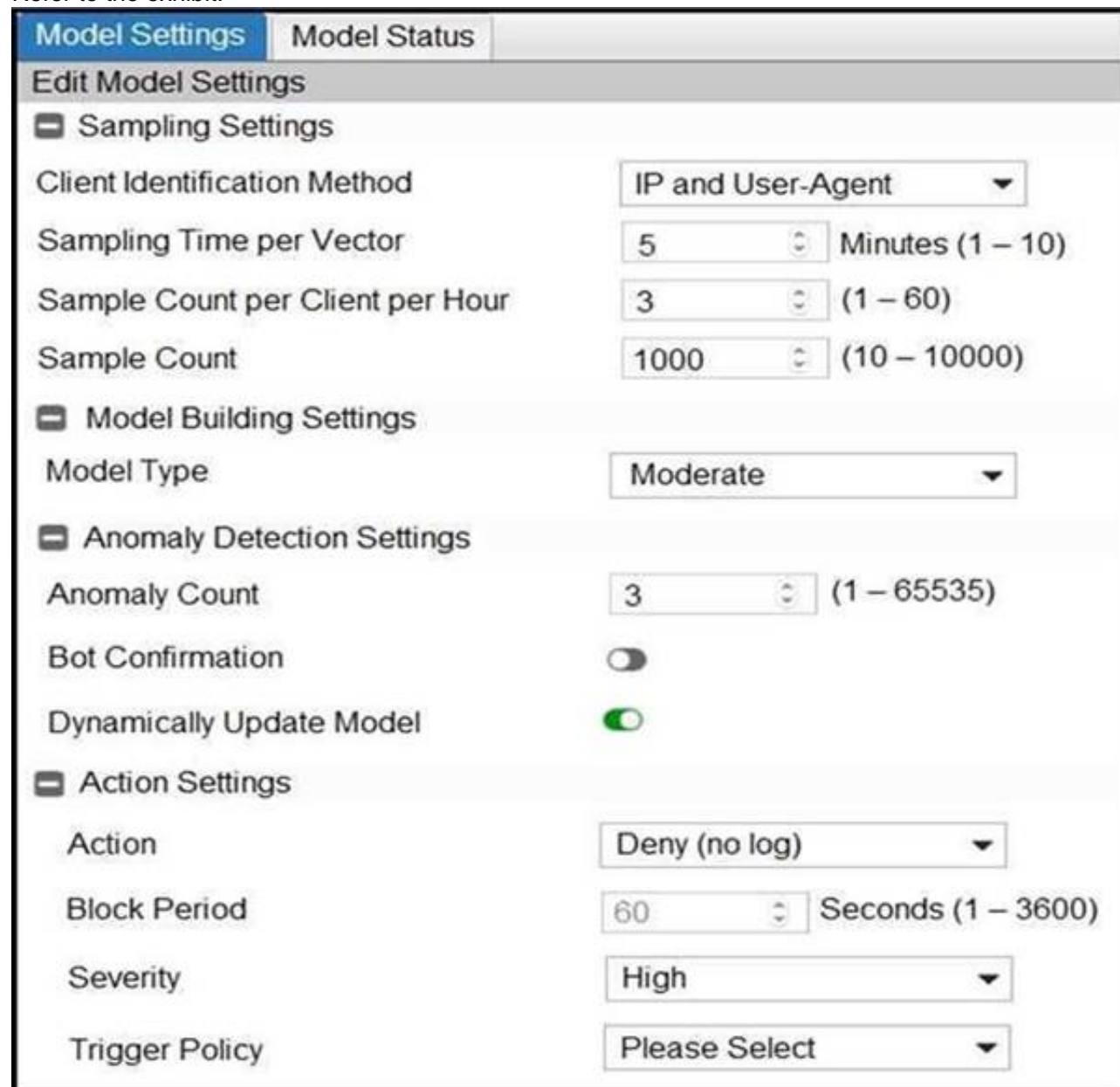
Answer: B

Explanation:

`\1://www.company.com\2\3`

NEW QUESTION 9

Refer to the exhibit.



The screenshot shows the 'Model Settings' tab in the FortiWeb configuration interface. The 'Edit Model Settings' section is expanded, showing the following configurations:

- 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: Disabled (toggle)
 - Dynamically Update Model: Enabled (toggle)
- 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 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

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 12

Which is true about HTTPS on FortiWeb? (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: ACE

NEW QUESTION 17

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 20

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 23

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 25

Which statement about local user accounts is true?

- A. They are best suited for large environments with many users.
- B. They cannot be used for site publishing.
- C. They must be assigned, regardless of any other authentication.
- D. They can be used for SSO.

Answer: B

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

Answer: B

NEW QUESTION 32

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 33

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 36

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 39

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 44

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 46

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 49

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.

Answer: AB

Explanation:

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.

NEW QUESTION 52

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE6_FWB-6.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE6_FWB-6.4 Product From:

https://www.2passeasy.com/dumps/NSE6_FWB-6.4/

Money Back Guarantee

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 FirstTry
- * NSE6_FWB-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year