NSE6_FWB-6.4 Q&As

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.geekcert.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

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

Correct Answer: C

QUESTION 2

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 3

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.

Correct Answer: D

FortiGuard IP Reputation service assigns a poor reputation, including virus-infected clients and malicious spiders/crawlers. Reference: https://docs.fortinet.com/document/fortiweb/6.1.1/administration-guide/137271/blacklisting-whitelisting-clients

QUESTION 4

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

A. FrotiWeb redirects users to a FortiAuthenticator page, then if the user authenticates successfully, FortiGate signals to FortiWeb to allow access to the web app

B. ForitWeb redirects the user to the web app\\'s authentication page

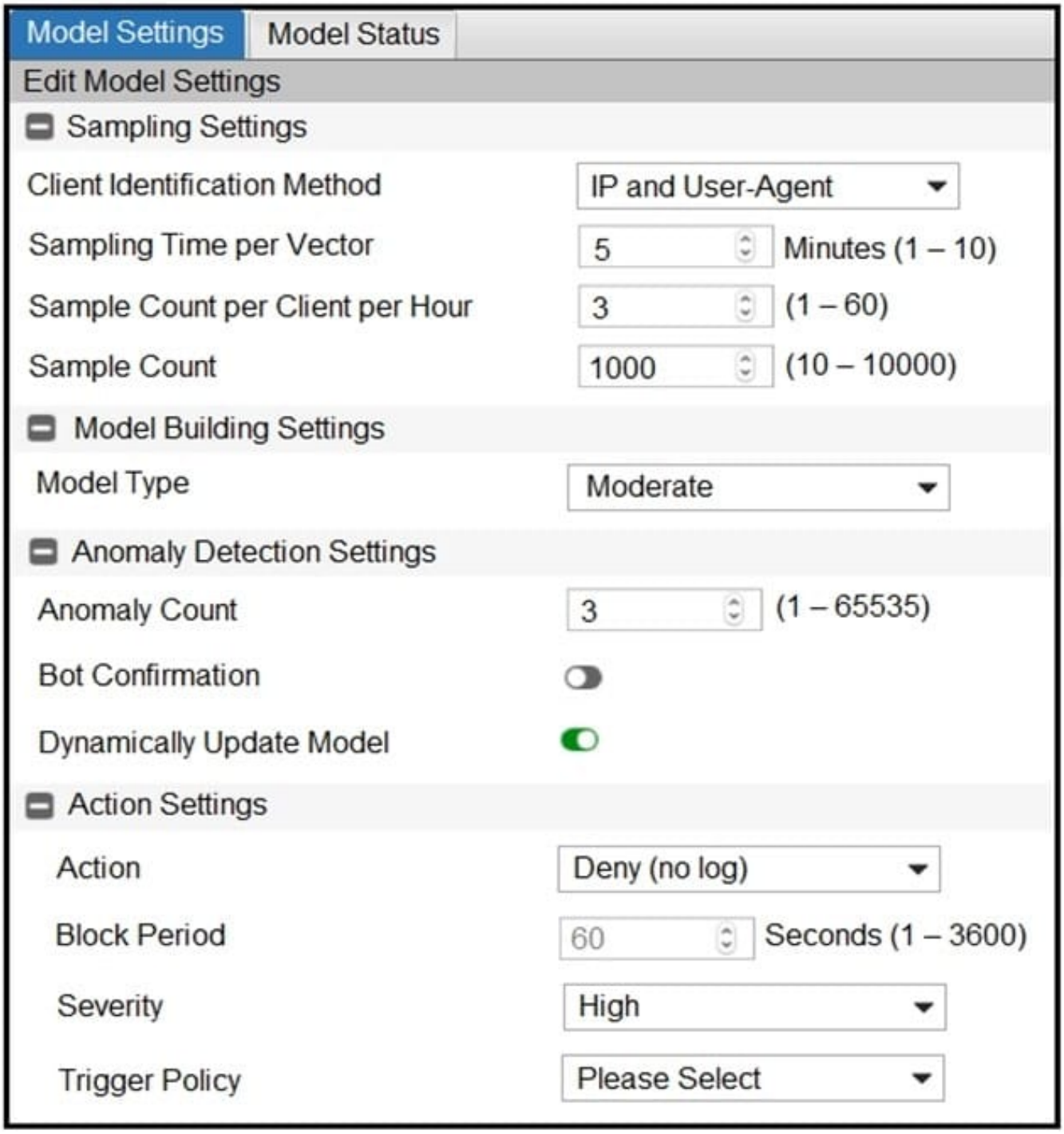
C. FortiWeb forwards the HTTP challenge from the server to the client, then monitors the reply, allowing access if the user authenticates successfully

D. FortiWeb replies with a HTTP challenge of behalf of the server, the if the user authenticates successfully, FortiWeb allows the request and also includes credentials in the request that it forwards to the web app

Correct Answer: A

QUESTION 5

Refer to the exhibit.



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

Correct Answer: D

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. Reference: https://docs.fortinet.com/document/fortiweb/6.3.1/administration-guide/600188/configuring-bot-detection-profiles