

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.leads4pass.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

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

Correct Answer: AD

QUESTION 2

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

Correct Answer: BD

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. Reference:
<https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/193258/machine-learning>

QUESTION 3

True transparent proxy mode is best suited for use in which type of environment?

- A. New networks where infrastructure is not yet defined
- B. Flexible environments where you can easily change the IP addressing scheme
- C. Small office to home office environments
- D. Environments where you cannot change the IP addressing scheme

Correct Answer: B

"Because blocking is not guaranteed to succeed in offline mode, this mode is best used during the evaluation and planning phase, early in implementation. Reverse proxy is the most popular operating mode. It can rewrite URLs, offload TLS, load balance, and apply NAT. For very large MSSP, true transparent mode has a significant advantage. You can drop it in without changing any schemes of limited IPv4 space?n transparent mode, you don't need to give IP

addresses to the network interfaces on FortiWeb."

QUESTION 4

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

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>

QUESTION 5

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

Correct Answer: C

[Latest NSE6_FWB-6.4 Dumps](#)

[NSE6_FWB-6.4 PDF Dumps](#)

[NSE6_FWB-6.4 Exam Questions](#)