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.pass4itsure.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

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.

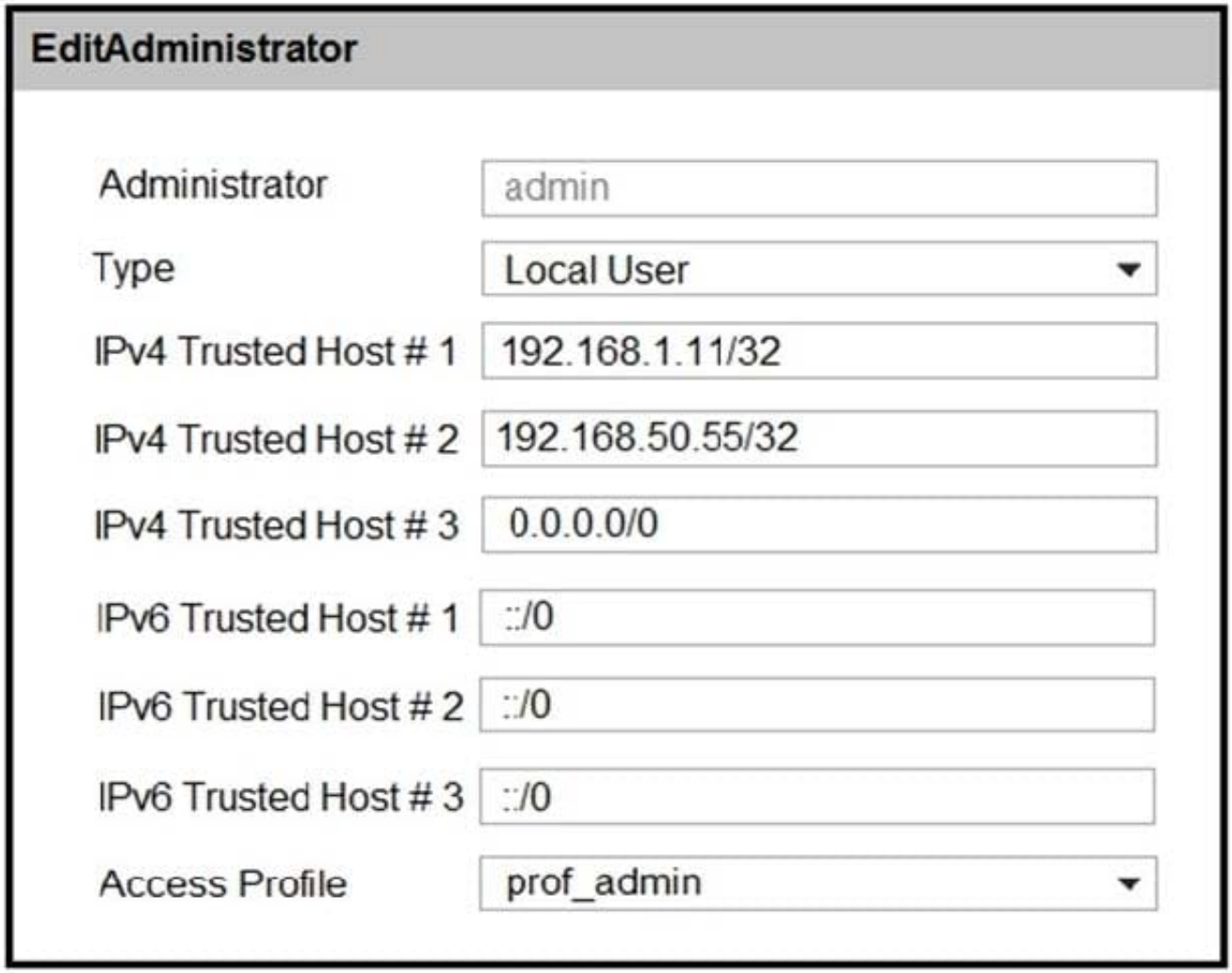
D. It keeps a live duplicate of the database.

Correct Answer: B

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. Reference: https://help.fortinet.com/fweb/551/Content/FortiWeb/fortiweb-admin/anti_defacement.htm

QUESTION 2

Refer to the exhibit.



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.

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortiweb/6.1.1/administration-guide/397469/preventing-brute-force-logins

QUESTION 3

Which of the following would be a reason for implementing rewrites?

A. Page has been moved to a new URL

B. Page has been moved to a new IP address

C. Replace vulnerable functions.

D. Send connection to secure channel

Correct Answer: C

QUESTION 4

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 5

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.

Correct Answer: C

QUESTION 6

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

Correct Answer: BCE

Reference: https://help.fortinet.com/fweb/607/Content/FortiWeb/fortiweb-admin/specify_urls_to_initiate.htm

QUESTION 7

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 8

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 9

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

Correct Answer: C

QUESTION 10

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