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

You are using HTTP content routing on FortiWeb. You want requests for web application A to be forwarded to a cluster of web servers, which all host the same web application. You want requests for web application B to be forwarded to a different, single web server.

Which statement about this solution is true?

A. The server policy applies the same protection profile to all of its protected web applications.

B. You must put the single web server in to a server pool, in order to use it with HTTP content routing.

C. You must chain policies so that requests for web application A go to the virtual server for policy A, and requests for web application B go to the virtual server for policy B.

D. Static or policy-based routes are not required.

Correct Answer: D

QUESTION 2

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 3

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 4

What can an administrator do if a client has been incorrectly period blocked?

A. Nothing, it is not possible to override a period block.

B. Manually release the ID address from the temporary blacklist.

C. Force a new IP address to the client.

D. Disconnect the client from the network.

Correct Answer: B

Block Period Enter the number of seconds that you want to block the requests. The valid range is 1?,600 seconds. The default value is 60 seconds. This option only takes effect when you choose Period Block in Action. Note: That\\'s a temporary blacklist so you can manually release them from the blacklist. Reference: https://docs.fortinet.com/document/fortiweb/6.3.1/administration-guide/600188/configuring-bot-detection-profiles

QUESTION 5

An e-commerce web app is used by small businesses. Clients often access it from offices behind a router, where clients are on an IPv4 private network LAN. You need to protect the web application from denial of service attacks that use request floods.

What FortiWeb feature should you configure?

A. Enable "Shared IP" and configure the separate rate limits for requests from NATted source IPs.

B. Configure FortiWeb to use "X-Forwarded-For:" headers to find each client\\'s private network IP, and to block attacks using that.

C. Enable SYN cookies.

D. Configure a server policy that matches requests from shared Internet connections.

Correct Answer: C