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

QUESTION 1

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

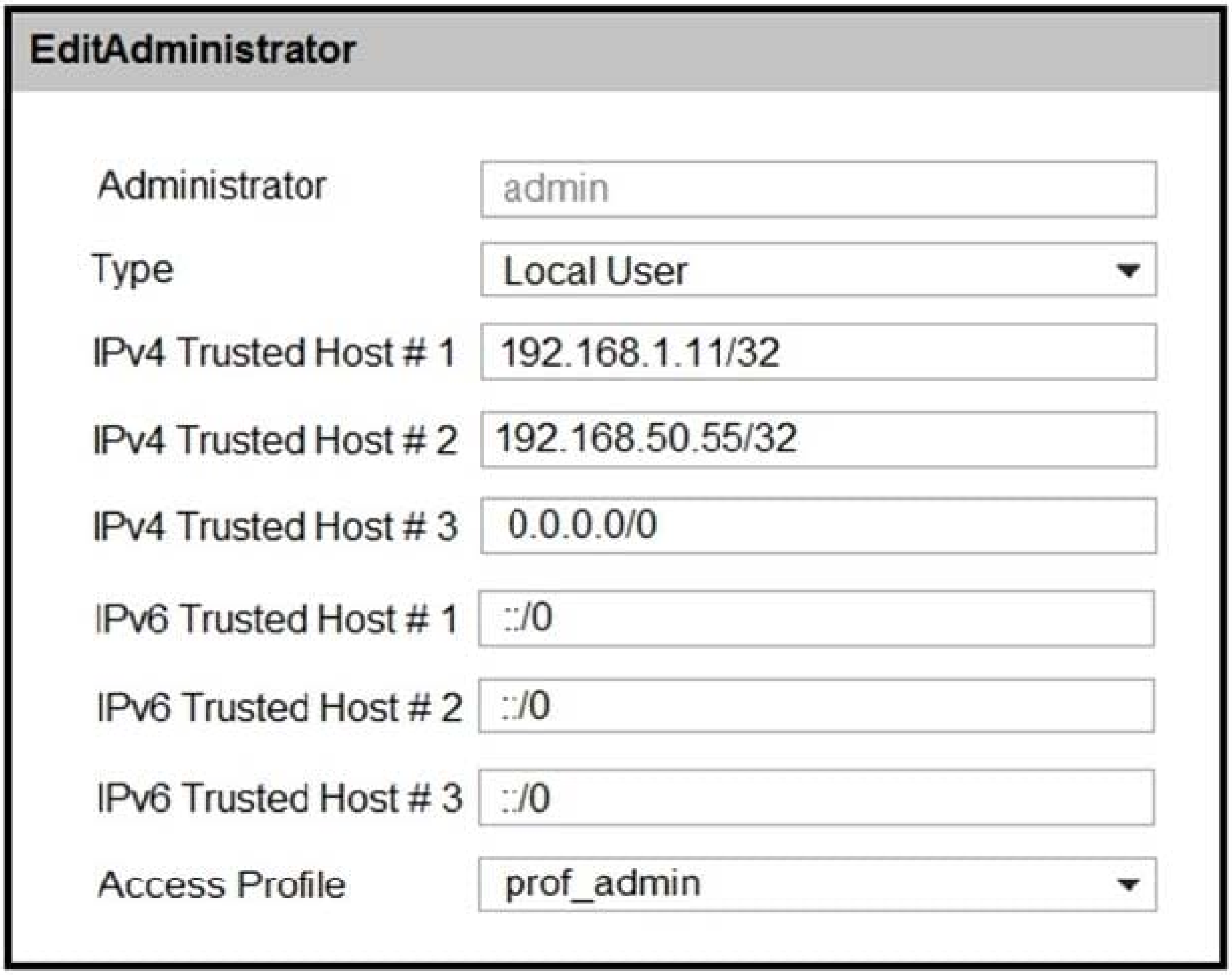
D. Determines whether traffic is an anomaly, based on observed application traffic over time

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 2

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.

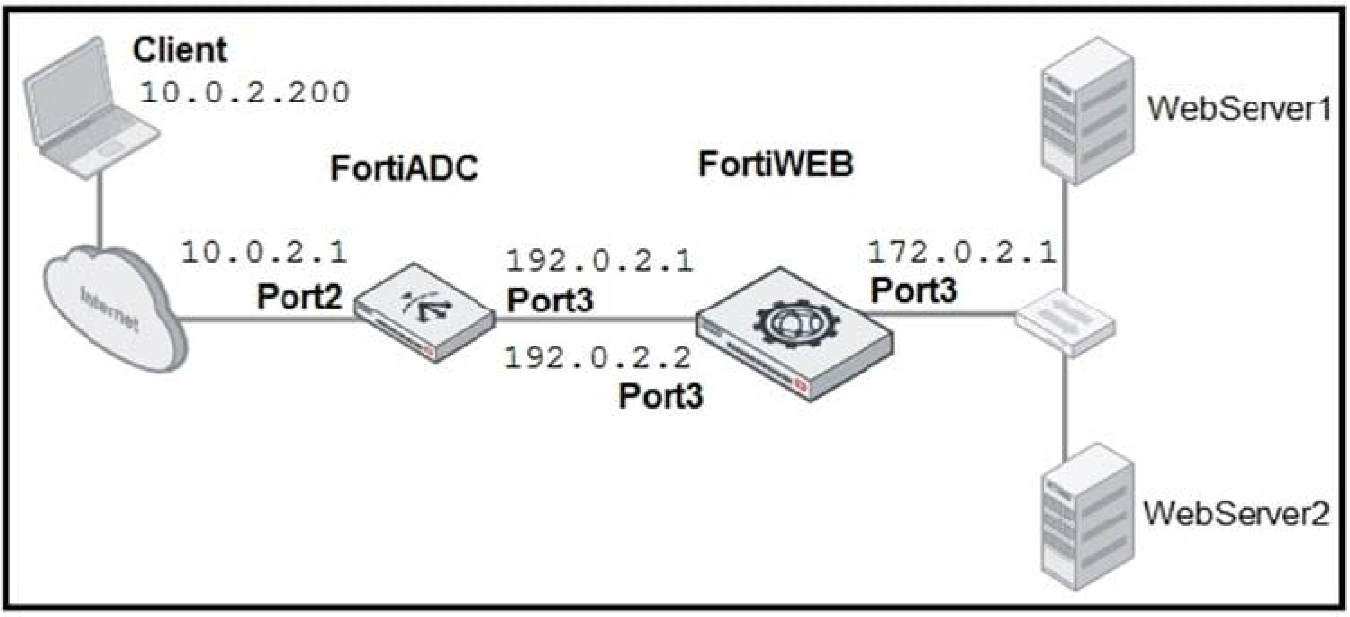
D. Change the Access Profile to Read_Only.

Correct Answer: B

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

QUESTION 3

Refer to the exhibit.



FortiADC is applying SNAT to all inbound traffic going to the servers. When an attack occurs, FortiWeb blocks traffic based on the 192.0.2.1 source IP address, which belongs to FortiADC. The setup is breaking all connectivity and genuine clients are not able to access the servers.

What must the administrator do to avoid this problem? (Choose two.)

A. Enable the Use X-Forwarded-For setting on FortiWeb.

B. No Special configuration is required; connectivity will be re-established after the set timeout.

C. Place FortiWeb in front of FortiADC.

D. Enable the Add X-Forwarded-For setting on FortiWeb.

Correct Answer: AC

Configure your load balancer to insert or append to an X-Forwarded-For:, X-Real-IP:, or other HTTP X-header. Also configure FortiWeb to find the original attacker\\'s or client\\'s IP address in that HTTP header Reference: https://help.fortinet.com/fweb/560/Content/FortiWeb/fortiweb-admin/planning_topology.htm

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

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

Correct Answer: AC