Fortinet

NSE6_FWB-6.4 Exam

Fortinet NSE 6 - FortiWeb 6.4

Questions & Answers
Demo

Version: 4.0

Question: 1

Which two statements about running a vulnerability scan are true? (Choose two.)

A. You should run the vulnerability scan during a maintenance window.
B. You should run the vulnerability scan in a test environment.
C. Vulnerability scanning increases the load on FortiWeb, so it should be avoided.
D. You should run the vulnerability scan on a live website to get accurate results.

Answer: A, B

Explanation:

Should the Vulnerability Scanner allow it, SVMS will set the scan schedule (or schedules) to run in a maintenance window. SVMS will advise Client of the scanner's ability to complete the scan(s) within the maintenance window.
Vulnerabilities on live web sites. Instead, duplicate the web site and its database in a test environment.
Reference: https://www.trustwave.com/media/17427/trustwave_mss_managed-3rd-party-vulnerability-scanning.pdf
https://help.fortinet.com/fweb/552/Content/FortiWeb/fortiweb-admin/vulnerability_scans.htm

Question: 2

FortiWeb offers the same load balancing algorithms as FortiGate.
Which two Layer 7 switch methods does FortiWeb also offer? (Choose two.)

A. Round robin
B. HTTP session-based round robin
C. HTTP user-based round robin
D. HTTP content routes

Answer: A, D

Explanation:

Reference: https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/399384/defining-your-web-servers

http://fortinet.globalgate.com.ar/pdfs/FortiWeb/FortiWeb_DS.pdf

Question: 3

Which would be a reason to implement HTTP rewriting?

A. The original page has moved to a new URL
B. To replace a vulnerable function in the requested URL
C. To send the request to secure channel
D. The original page has moved to a new IP address

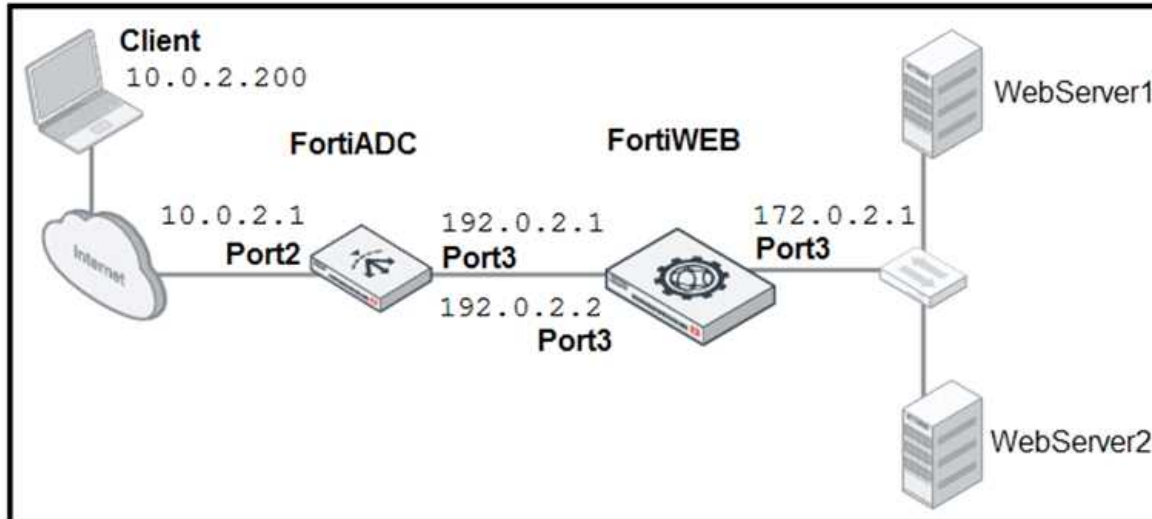**Answer: B**

Explanation:

Create a new URL rewriting rule.
Reference: https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/961303/rewriting-redirecting

Question: 4

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.

Answer: A, C

Explanation:

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: 5

Which statement about local user accounts is true?

A. They are best suited for large environments with many users.
B. They cannot be used for site publishing.
C. They must be assigned, regardless of any other authentication.
D. They can be used for SSO.

Answer: B