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 deploying FortiWeb 6.4 in an Amazon Web Services cloud. Which 2 lines of this initial setup via CLI are incorrect? (Choose two.)

```
1 config system settings
2 set opmode transparent
3 set gateway 10.0.0.1
4 end
5 config system interface
6 set port1
7 set ip 10.0.0.5
8 set allowaccess https ssh ping
9 end
```

A. 6

B. 9

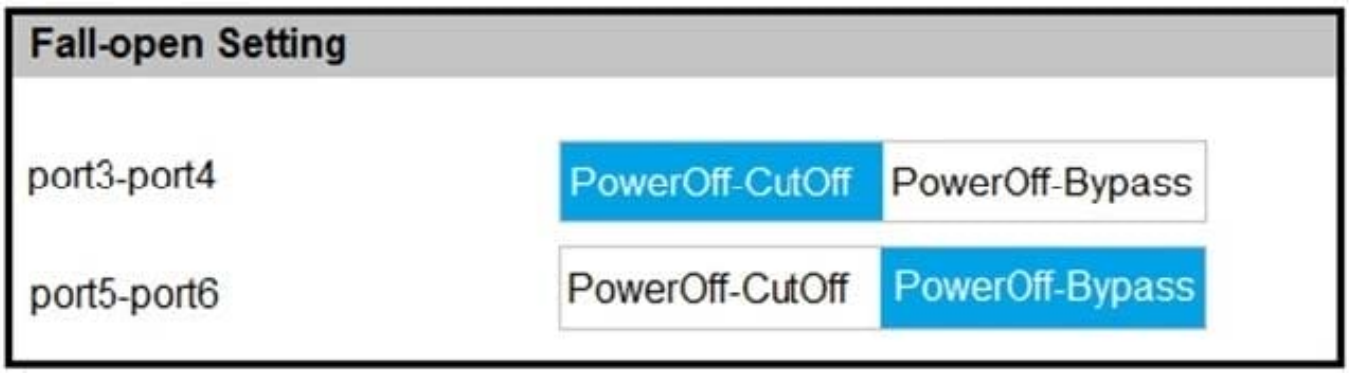
C. 3

D. 2

Correct Answer: AC

QUESTION 2

Refer to the exhibit.



Based on the configuration, what would happen if this FortiWeb were to lose power? (Choose two.)

A. Traffic that passes between port5 and port6 will be inspected.

B. Traffic will be interrupted between port3 and port4.

C. All traffic will be interrupted.

D. Traffic will pass between port5 and port6 uninspected.

Correct Answer: BD

Reference: https://docs.fortinet.com/document/fortiweb/6.3.10/administration-guide/33485/fail-to-wire-for-power-loss-reboots

QUESTION 3

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.

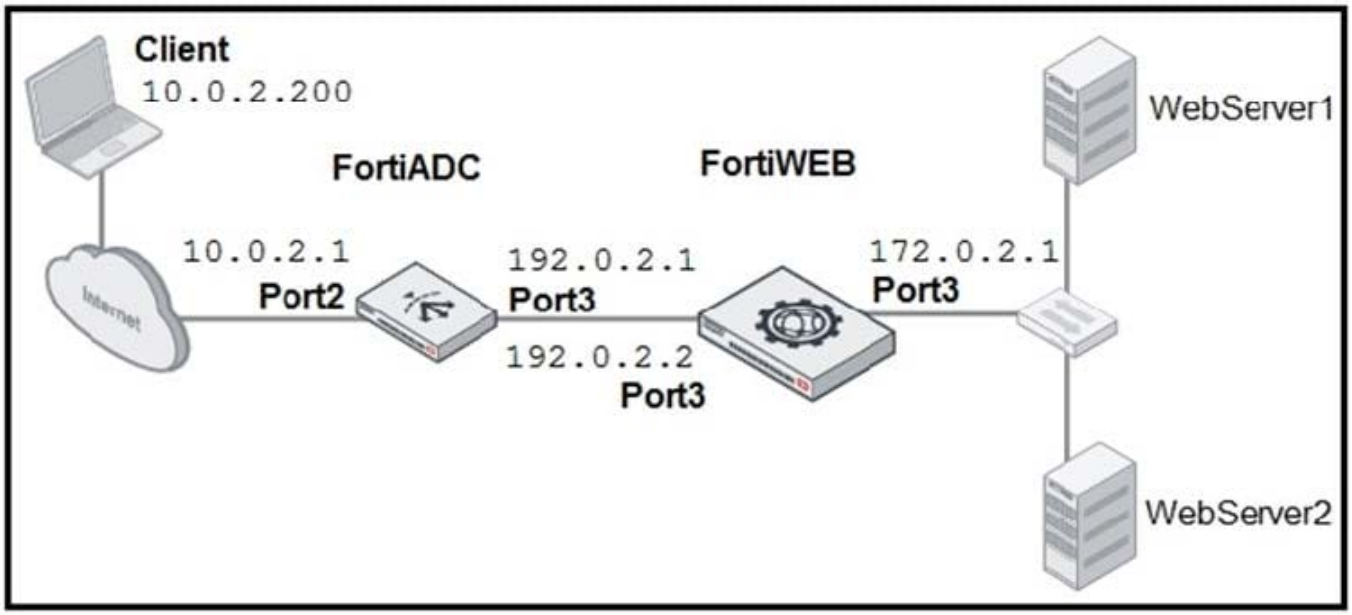
D. Disconnect the client from the network.

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 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.

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 5

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