



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.passapply.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**

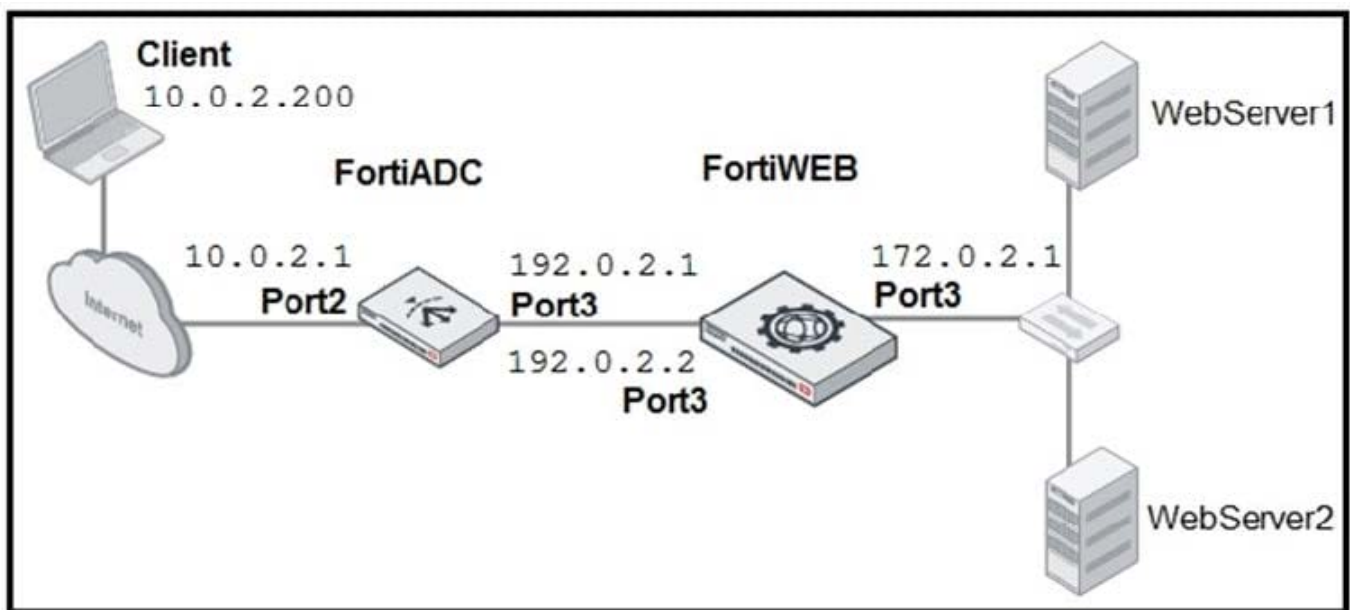
Which operation mode does not require additional configuration in order to allow FTP traffic to your web server?

- A. Offline Protection
- B. Transparent Inspection
- C. True Transparent Proxy
- D. Reverse-Proxy

Correct Answer: B

QUESTION 2

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.)

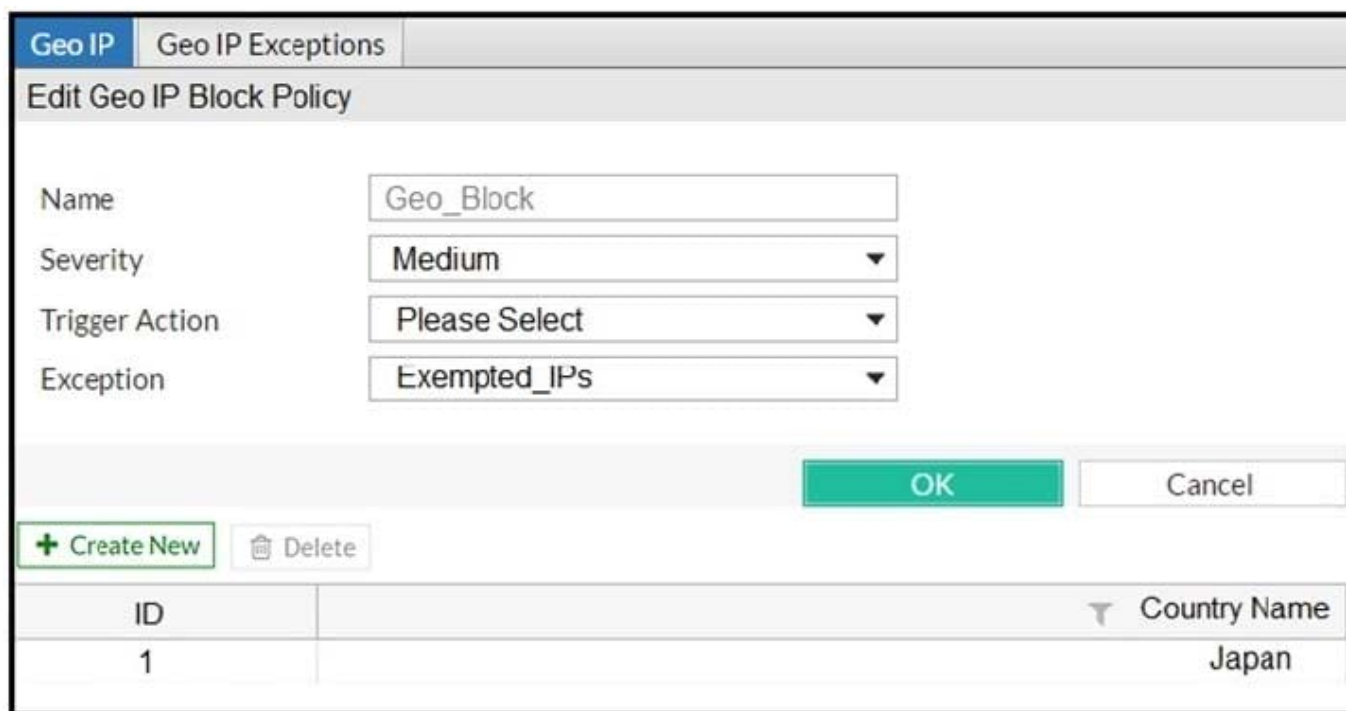
- A. Enable the Use X-Forwarded-For setting on FortiWeb.
- B. No Special configuration is required; connectivity will be re-established after the set timeout.
- C. Place FortiWeb in front of FortiADC.
- D. Enable the Add X-Forwarded-For setting on FortiWeb.

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 3

Refer to the exhibit.



ID	Country Name
1	Japan

FortiWeb is configured to block traffic from Japan to your web application server. However, in the logs, the administrator is seeing traffic allowed from one particular IP address which is geo-located in Japan. What can the administrator do to solve this problem? (Choose two.)

- A. Manually update the geo-location IP addresses for Japan.
- B. If the IP address is configured as a geo reputation exception, remove it.
- C. Configure the IP address as a blacklisted IP address.
- D. If the IP address is configured as an IP reputation exception, remove it.

Correct Answer: BC

QUESTION 4

Which two statements about the anti-defacement feature on FortiWeb are true? (Choose two.)

- A. Anti-defacement can redirect users to a backup web server, if it detects a change.



- B. Anti-defacement downloads a copy of your website to RAM, in order to restore a clean image, if it detects defacement.
- C. FortiWeb will only check to see if there are changes on the web server; it will not download the whole file each time.
- D. Anti-defacement does not make a backup copy of your databases.

Correct Answer: CD

Anti-defacement backs up web pages only, not databases. If it detects any file changes, the FortiWeb appliance will download a new backup revision. Reference: https://help.fortinet.com/fweb/551/Content/FortiWeb/fortiweb-admin/anti_defacement.htm

QUESTION 5

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>

[Latest NSE6 FWB-6.4 Dumps](#)

[NSE6 FWB-6.4 PDF Dumps](#)

[NSE6 FWB-6.4 Exam Questions](#)