Fortinet

Exam Questions NSE6_FWB-6.4

Fortinet NSE 6 - FortiWeb 6.4

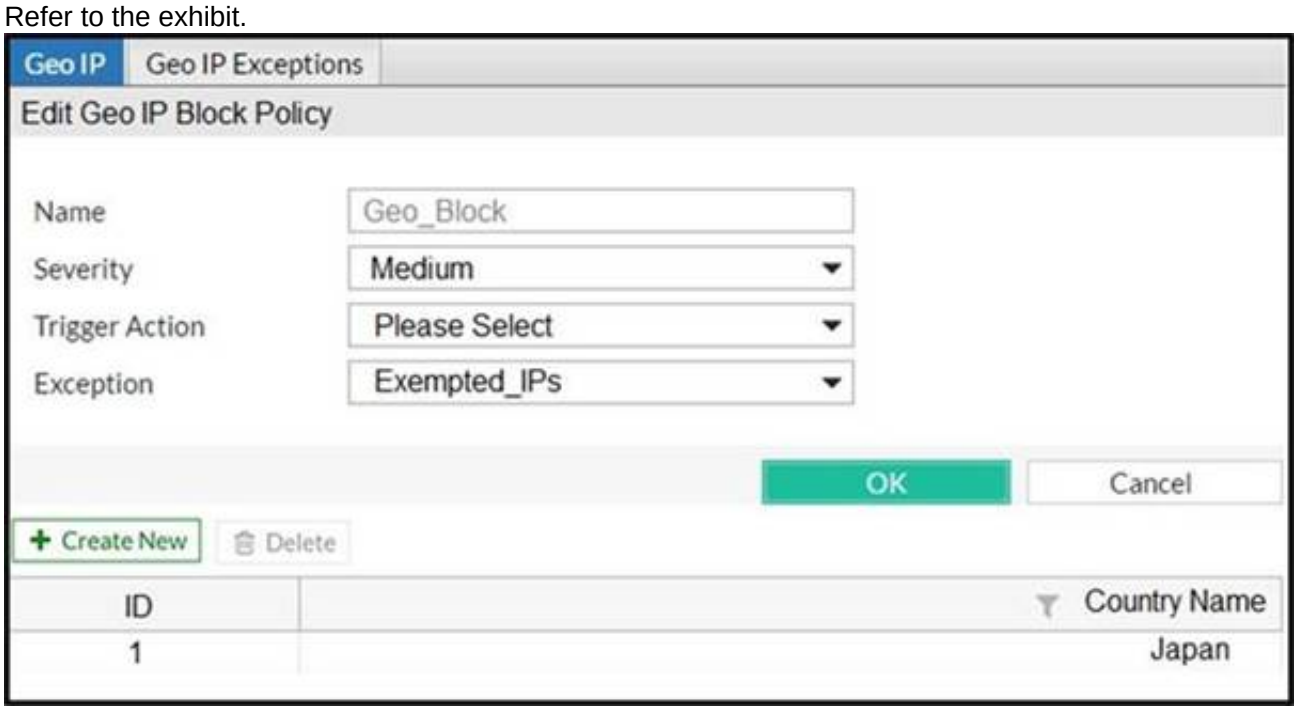
NEW QUESTION 1
Which two statements about the anti-defacement feature on FortiWeb are true? (Choose two.)

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.

Answer: CD

Explanation:
Anti-defacement backs up web pages only, not databases.
If it detects any file changes, the FortiWeb appliance will download a new backup revision.

NEW QUESTION 2
Refer to the exhibit.



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.

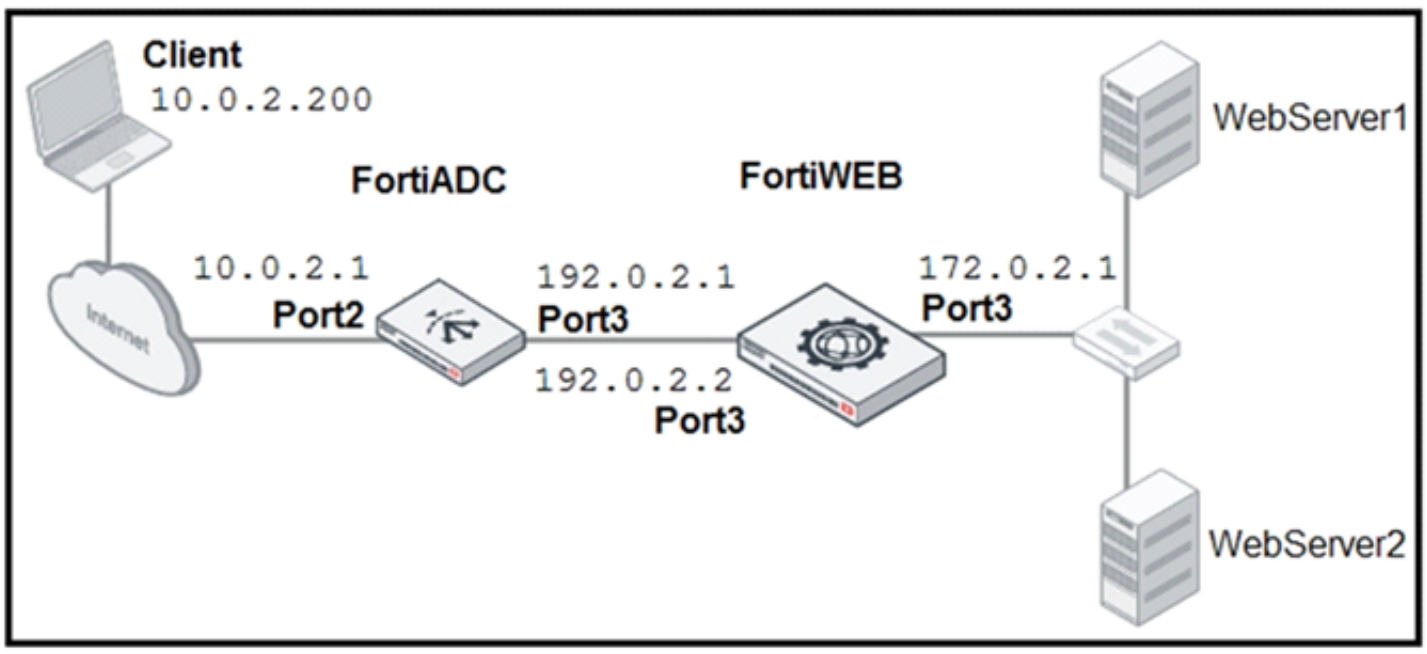
Answer: BC

NEW QUESTION 3
Which of the following is true about Local User Accounts?

A. Must be assigned regardless of any other authentication
B. Can be used for Single Sign On
C. Can be used for site publishing
D. Best suited for large environments with many users

Answer: C

NEW 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: AC

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

NEW QUESTION 5
Under what circumstances would you want to use the temporary uncompress feature of FortiWeb?

A. In the case of compression being done on the FortiWeb, to inspect the content of the compressed file
B. In the case of the file being a .MP3 music file
C. In the case of compression being done on the web server, to inspect the content of the compressed file.
D. In the case of the file being an .MP4 video

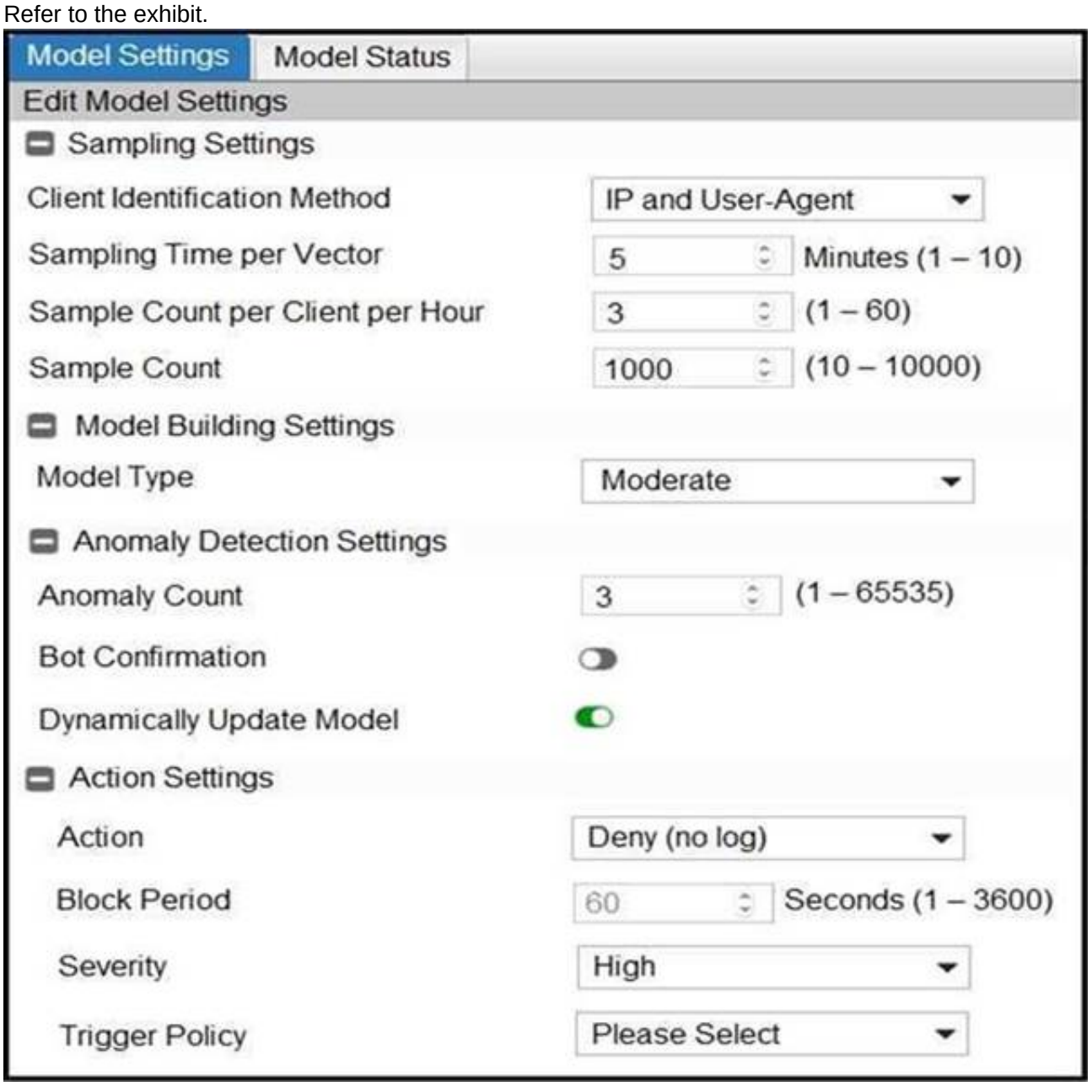
Answer: C

NEW QUESTION 6
How does offloading compression to FortiWeb benefit your network?

A. free up resources on the database server
B. Free up resources on the web server
C. reduces file size on the client's storage
D. free up resources on the FortiGate

Answer: B

NEW QUESTION 7
Refer to the exhibit.



Many legitimate users are being identified as bots. FortiWeb bot detection has been configured with the settings shown in the exhibit. The FortiWeb administrator has already verified that the current model is accurate.
What can the administrator do to fix this problem, making sure that real bots are not allowed through FortiWeb?

A. Change Model Type to Strict
B. Change Action under Action Settings to Alert
C. Disable Dynamically Update Model

D. Enable Bot Confirmation

Answer: D

Explanation:
Bot Confirmation
If the number of anomalies from a user has reached the Anomaly Count, the system executes Bot Confirmation before taking actions.
The Bot Confirmation is to confirm if the user is indeed a bot. The system sends RBE (Real Browser Enforcement) JavaScript or CAPTCHA to the client to double check if it's a real bot.

NEW QUESTION 8
What role does FortiWeb play in ensuring PCI DSS compliance?

A. It provides the ability to securely process cash transactions.
B. It provides the required SQL server protection.
C. It provides the WAF required by PCI.
D. It provides credit card processing capabilities.

Answer: C

NEW QUESTION 9
Which implementation is best suited for a deployment that must meet compliance criteria?

A. SSL Inspection with FortiWeb in Transparency mode
B. SSL Offloading with FortiWeb in reverse proxy mode
C. SSL Inspection with FrotiWeb in Reverse Proxy mode
D. SSL Offloading with FortiWeb in Transparency Mode

Answer: C

NEW QUESTION 10
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: AD

NEW QUESTION 10
Which is true about HTTPS on FortiWeb? (Choose three.)

A. For SNI, you select the certificate that FortiWeb will present in the server pool, not in the server policy.
B. After enabling HSTS, redirects to HTTPS are no longer necessary.
C. In true transparent mode, the TLS session terminator is a protected web server.
D. Enabling RC4 protects against the BEAST attack, but is not recommended if you configure FortiWeb to only offer TLS 1.2.
E. In transparent inspection mode, you select which certificate that FortiWeb will present in the server pool, not in the server policy.

Answer: ACE

NEW QUESTION 15
When is it possible to use a self-signed certificate, rather than one purchased from a commercial certificate authority?

A. If you are a small business or home office
B. If you are an enterprise whose employees use only mobile devices
C. If you are an enterprise whose resources do not need security
D. If you are an enterprise whose computers all trust your active directory or other CA server

Answer: D

NEW QUESTION 17
When viewing the attack logs on FortiWeb, which client IP address is shown when you are using XFF header rules?

A. FortiGate public IP
B. FortiWeb IP
C. FortiGate local IP
D. Client real IP

Answer: D

Explanation:
When an XFF header reaches Alteon from a client, Alteon removes all the content from the header and injects the client IP address. Alteon then forwards the header to the server.

NEW QUESTION 19
You are configuring FortiAnalyzer to store logs from FortiWeb. Which is true?

A. FortiAnalyzer will store antivirus and DLP archives from FortiWeb.
B. You must enable ADOMs on FortiAnalyzer.
C. To store logs from FortiWeb 6.4, on FortiAnalyzer, you must select “FrotiWeb 6.1”.
D. FortiWeb will query FortiAnalyzer for reports, instead of generating them locally.

Answer: B

NEW QUESTION 20
Which of the following FortiWeb features is part of the mitigation tools against OWASP A4 threats?

A. Sensitive info masking
B. Poison Cookie detection
C. Session Management
D. Brute Force blocking

Answer: C

NEW QUESTION 22
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

NEW QUESTION 25
Review the following configuration:

```
config waf machine-learning-policy
edit 1
set sample-limit-by-ip 0
next
end
```

What is the expected result of this configuration setting?

A. When machine learning (ML) is in its collecting phase, FortiWeb will accept an unlimited number of samples from the same source IP address.
B. When machine learning (ML) is in its running phase, FortiWeb will accept an unlimited number of samples from the same source IP address.
C. When machine learning (ML) is in its collecting phase, FortiWeb will not accept any samples from any source IP addresses.
D. When machine learning (ML) is in its running phase, FortiWeb will accept a set number of samples from the same source IP address.

Answer: A

NEW QUESTION 29
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.

NEW QUESTION 31
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.

Answer: BD

NEW QUESTION 35
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

Answer: AC

NEW QUESTION 39
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.

Answer: D

Explanation:
FortiGuard IP Reputation service assigns a poor reputation, including virus-infected clients and malicious spiders/crawlers.

NEW QUESTION 41
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

Answer: AC

NEW QUESTION 46
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE6_FWB-6.4 Practice Exam Features:

* NSE6_FWB-6.4 Questions and Answers Updated Frequently

* NSE6_FWB-6.4 Practice Questions Verified by Expert Senior Certified Staff

* NSE6_FWB-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE6_FWB-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year