IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **NSE6_FWB-6.1**

Title : Fortinet NSE 6 - FortiWeb 6.1

Version : DEMO

1.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
Explanation:
FortiWeb protects against attacks that lead to sensitive data exposure such as SQL Injection and other injection types. Additionally, FortiWeb inspects all web server outgoing traffic for sensitive data such as Social Security numbers, credit card numbers and other predefined or custom based sensitive data.
Reference: https://www.gordion.de/fileadmin/user_upload/SG-PCI-Compliance.pdf

2.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.
Answer: B
Explanation:
Block Period
Enter the number of seconds that you want to block the requests. The valid range is 1–3,600 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

3.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

4.How does FortiWeb protect against defacement attacks?
A. It keeps a complete backup of all files and the database.
B. It keeps hashes of files and periodically compares them to the server.
C. It keeps full copies of all files and directories.
D. It keeps a live duplicate of the database.
Answer: B
Explanation:
The anti-defacement feature examines a web site's files for changes at specified time intervals. If it detects a change that could indicate a defacement attack,
the FortiWeb appliance can notify you and quickly react by automatically restoring the web site contents to the previous backup.
Reference: https://help.fortinet.com/fweb/551/Content/FortiWeb/fortiweb-admin/anti_defacement.htm

5.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.
Reference:
https://docs.fortinet.com/document/fortiweb/6.1.1/administration-guide/137271/blacklisting-whitelisting-clients