Fortinet

Exam Questions NSE6_FWB-6.4

Fortinet NSE 6 - FortiWeb 6.4

NEW QUESTION 1
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.

NEW QUESTION 2
How does your FortiWeb configuration differ if the FortiWeb is upstream of the SNAT device instead of downstream of the SNAT device?

A. You must enable the "Use" X-Forwarded-For: option.
B. FortiWeb must be set for Transparent Mode
C. No special configuration required
D. You must enable "Add" X-Forwarded-For: instead of the "Use" X-Forwarded-For: option.

Answer: D

NEW QUESTION 3
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 4
How does an ADOM differ from a VDOM?

A. ADOMs do not have virtual networking
B. ADOMs improve performance by offloading some functions.
C. ADOMs only affect specific functions, and do not provide full separation like VDOMs do.
D. Allows you to have 1 administrator for multiple tenants

Answer: A

NEW QUESTION 5
What must you do with your FortiWeb logs to ensure PCI DSS compliance?

A. Store in an off-site location
B. Erase them every two weeks
C. Enable masking of sensitive data
D. Compress them into a .zip file format

Answer: C

NEW QUESTION 6
A client is trying to start a session from a page that should normally be accessible only after they have logged in.
When a start page rule detects the invalid session access, what can FortiWeb do? (Choose three.)

A. Reply with a "403 Forbidden" HTTP error
B. Allow the page access, but log the violation
C. Automatically redirect the client to the login page
D. Display an access policy message, then allow the client to continue, redirecting them to their requested page
E. Prompt the client to authenticate

Answer: ABC

NEW QUESTION 7
In which scenario might you want to use the compression feature on FortiWeb?

A. When you are serving many corporate road warriors using 4G tablets and phones

B. When you are offering a music streaming service
C. When you want to reduce buffering of video streams
D. Never, since most traffic today is already highly compressed

Answer: A

Explanation:
https://training.fortinet.com/course/view.php?id=3363
When might you want to use the compression feature on FortiWeb? When you are serving many road warriors who are using 4G tablets and phones

NEW QUESTION 8
Which of the following would be a reason for implementing rewrites?

A. Page has been moved to a new URL
B. Page has been moved to a new IP address
C. Replace vulnerable functions.
D. Send connection to secure channel

Answer: C

NEW QUESTION 9
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.

NEW QUESTION 10
An e-commerce web app is used by small businesses. Clients often access it from offices behind a router, where clients are on an IPv4 private network LAN. You need to protect the web application from denial of service attacks that use request floods.
What FortiWeb feature should you configure?

A. Enable "Shared IP" and configure the separate rate limits for requests from NATted source IPs.
B. Configure FortiWeb to use "X-Forwarded-For:" headers to find each client's private network IP, and to block attacks using that.
C. Enable SYN cookies.
D. Configure a server policy that matches requests from shared Internet connections.

Answer: C

NEW QUESTION 10
Refer to the exhibit.
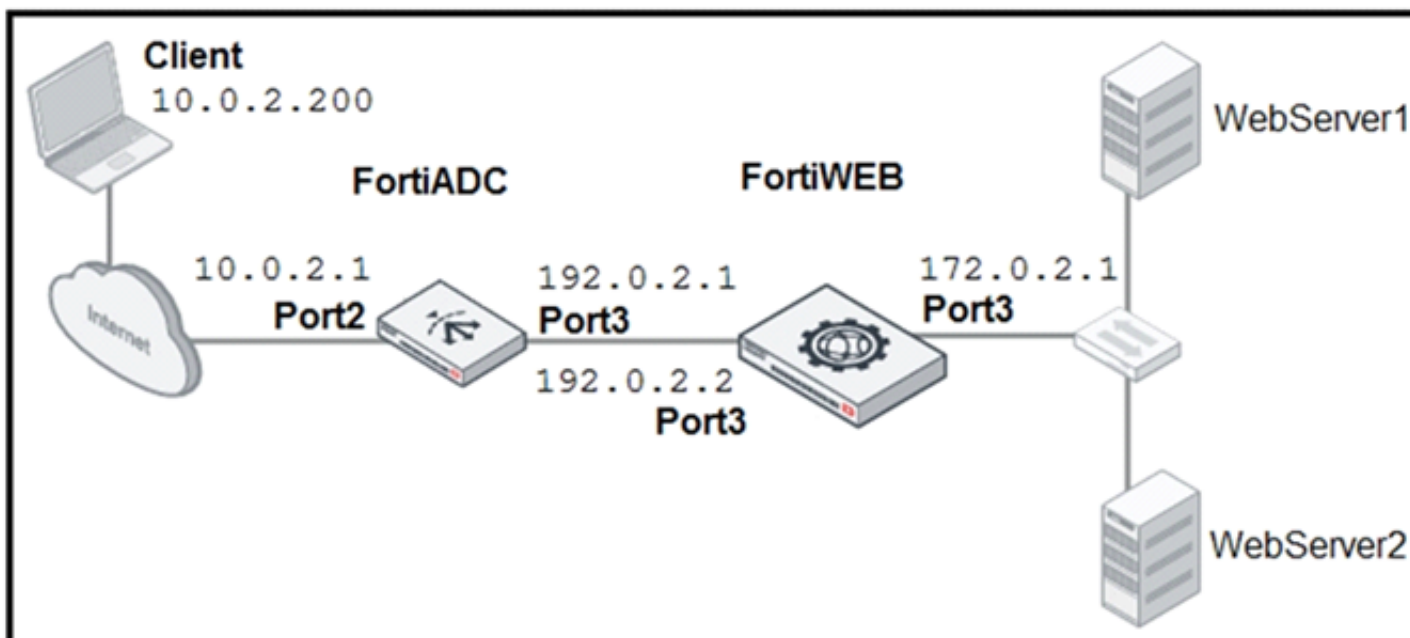
FortiADC is applying SNAT to all inbound traffic going to the servers. When an attack occurs, FortiWeb blocks traffic based on the 192.0.2.1 source IP address, which belongs to FortiADC. The setup is breaking all connectivity and genuine clients are not able to access the servers.
What must the administrator 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 12
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

Answer: B

NEW QUESTION 16
Refer to the exhibits.

FortiWeb is configured in reverse proxy mode and it is deployed downstream to FortiGate. Based on the configuration shown in the exhibits, which of the following statements is true?

A. FortiGate should forward web traffic to the server pool IP addresses.
B. The configuration is incorrec
C. FortiWeb should always be located upstream to FortiGate.
D. You must disable the Preserve Client IP setting on FotriGate for this configuration to work.
E. FortiGate should forward web traffic to virtual server IP address.

Answer: D

NEW QUESTION 18
Which three statements about HTTPS on FortiWeb are true? (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: CDE

NEW QUESTION 23
Which regex expression is the correct format for redirecting the URL http://www.example.com?

A. www\.example\.com
B. www.example.com
C. www\example\com
D. www/.example/.com

Answer: B

Explanation:
\1://www.company.com/\2/\3

NEW QUESTION 26
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 28
What key factor must be considered when setting brute force rate limiting and blocking?

A. A single client contacting multiple resources
B. Multiple clients sharing a single Internet connection
C. Multiple clients from geographically diverse locations
D. Multiple clients connecting to multiple resources

Answer: B

Explanation:
https://training.fortinet.com/course/view.php?id=3363 What is one key factor that you must consider when setting brute force rate limiting and blocking? Multiple clients sharing a single Internet connection

NEW QUESTION 32
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 35
When the FortiWeb is configured in Reverse Proxy mode and the FortiGate is configured as an SNAT device, what IP address will the FortiGate's Real Server configuration point at?

A. Virtual Server IP on the FortiGate
B. Server's real IP
C. FortiWeb's real IP
D. IP Address of the Virtual Server on the FortiWeb

Answer: A

NEW QUESTION 37
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 39
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 40
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 44
What role does FortiWeb play in ensuring PCI DSS compliance?

A. PCI specifically requires a WAF
B. Provides credit card processing capabilities
C. Provide ability to securely process cash transactions
D. Provides load balancing between multiple web servers

Answer: A

Explanation:
FortiWeb helps you meet all PCI requirements, but PCI now specifically recommends using a WAF, and developing remediations against the top 10 vulnerabilities, according to OWASP.

NEW QUESTION 48
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 52
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: AB

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.

NEW QUESTION 56
......

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

100% Actual & Verified — Instant Download, Please Click
[Order The NSE6_FWB-6.4 Practice Test Here](https://www.surepassexam.com/NSE6_FWB-6.4-exam-dumps.html)