Exam Questions NSE6_FWB-6.4

Fortinet NSE 6 - FortiWeb 6.4

https://www.2passeasy.com/dumps/NSE6_FWB-6.4/

NEW QUESTION 1
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 2
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

Answer: C

NEW QUESTION 3
When integrating FortiWeb and FortiAnalyzer, why is the selection for FortiWeb Version critical? (Choose two)

A. Defines Log file format
B. Defines communication protocol
C. Defines Database Schema
D. Defines Log storage location

Answer: AD

NEW QUESTION 4
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 5
You've configured an authentication rule with delegation enabled on FortiWeb. What happens when a user tries to access the web application?

A. FrotiWeb redirects users to a FortiAuthenticator page, then if the user authenticates successfully, FortiGate signals to FortiWeb to allow access to the web app
B. ForitWeb redirects the user to the web app's authentication page
C. FortiWeb forwards the HTTP challenge from the server to the client, then monitors the reply, allowing access if the user authenticates successfully
D. FortiWeb replies with a HTTP challenge of behalf of the server, the if the user authenticates successfully, FortiWeb allows the request and also includes credentials in the request that it forwards to the web app

Answer: A

NEW QUESTION 6
What other consideration must you take into account when configuring Defacement protection

A. Use FortiWeb to block SQL Injections and keep regular backups of the Database
B. Also incorporate a FortiADC into your network
C. Non
D. FortiWeb completely secures the site against defacement attacks
E. Configure the FortiGate to perform Anti-Defacement as well

Answer: A

NEW QUESTION 7
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 8
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 9
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 10
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 10
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 13
Refer to the exhibits.

Edit Virtual Server

Name	vserver1
Use Interface IP	◯
IPv4 Address	10.0.1.8/255.255.255.0
IPv6 Address	::/0
Interface	port1 ▼

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 14
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 19
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 20
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 22
True transparent proxy mode is best suited for use in which type of environment?

A. New networks where infrastructure is not yet defined
B. Flexible environments where you can easily change the IP addressing scheme
C. Small office to home office environments
D. Environments where you cannot change the IP addressing scheme

Answer: B

Explanation:
"Because blocking is not guaranteed to succeed in offline mode, this mode is best used during the evaluation and planning phase, early in implementation. Reverse proxy is the most popular operating mode. It can rewrite URLs, offload TLS, load balance, and apply NAT. For very large MSSP, true transparent mode has a significant advantage. You can drop it in without changing any schemes of limited IPv4 space–in transparent mode, you don't need to give IP addresses to the network interfaces on FortiWeb."

NEW QUESTION 27
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 30
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
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 38
When generating a protection configuration from an auto learning report what critical step must you do before generating the final protection configuration?

A. Restart the FortiWeb to clear the caches
B. Drill down in the report to correct any false positives.
C. Activate the report to create t profile
D. Take the FortiWeb offline to apply the profile

Answer: B

NEW QUESTION 43
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 47
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 48
Which algorithm is used to build mathematical models for bot detection?

A. HCM
B. SVN
C. SVM
D. HMM

Answer: C

Explanation:
FortiWeb uses SVM (Support Vector Machine) algorithm to build up the bot detection model

NEW QUESTION 51
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 53
A client is trying to start a session from a page that would normally be accessible only after the client has logged in.
When a start page rule detects the invalid session access, what can FortiWeb do? (Choose three.)

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

Answer: BCE

NEW QUESTION 57
The FortiWeb machine learning (ML) feature is a two-phase analysis mechanism. Which two functions does the first layer perform? (Choose two.)

A. Determines whether an anomaly is a real attack or just a benign anomaly that should be ignored
B. Builds a threat model behind every parameter and HTTP method
C. Determines if a detected threat is a false-positive or not
D. Determines whether traffic is an anomaly, based on observed application traffic over time

Answer: BD

Explanation:
The first layer uses the Hidden Markov Model (HMM) and monitors access to the application and collects data to build a mathematical model behind every parameter and HTTP method.

NEW QUESTION 58
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE6_FWB-6.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE6_FWB-6.4 Product From:

https://www.2passeasy.com/dumps/NSE6_FWB-6.4/

Money Back Guarantee

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