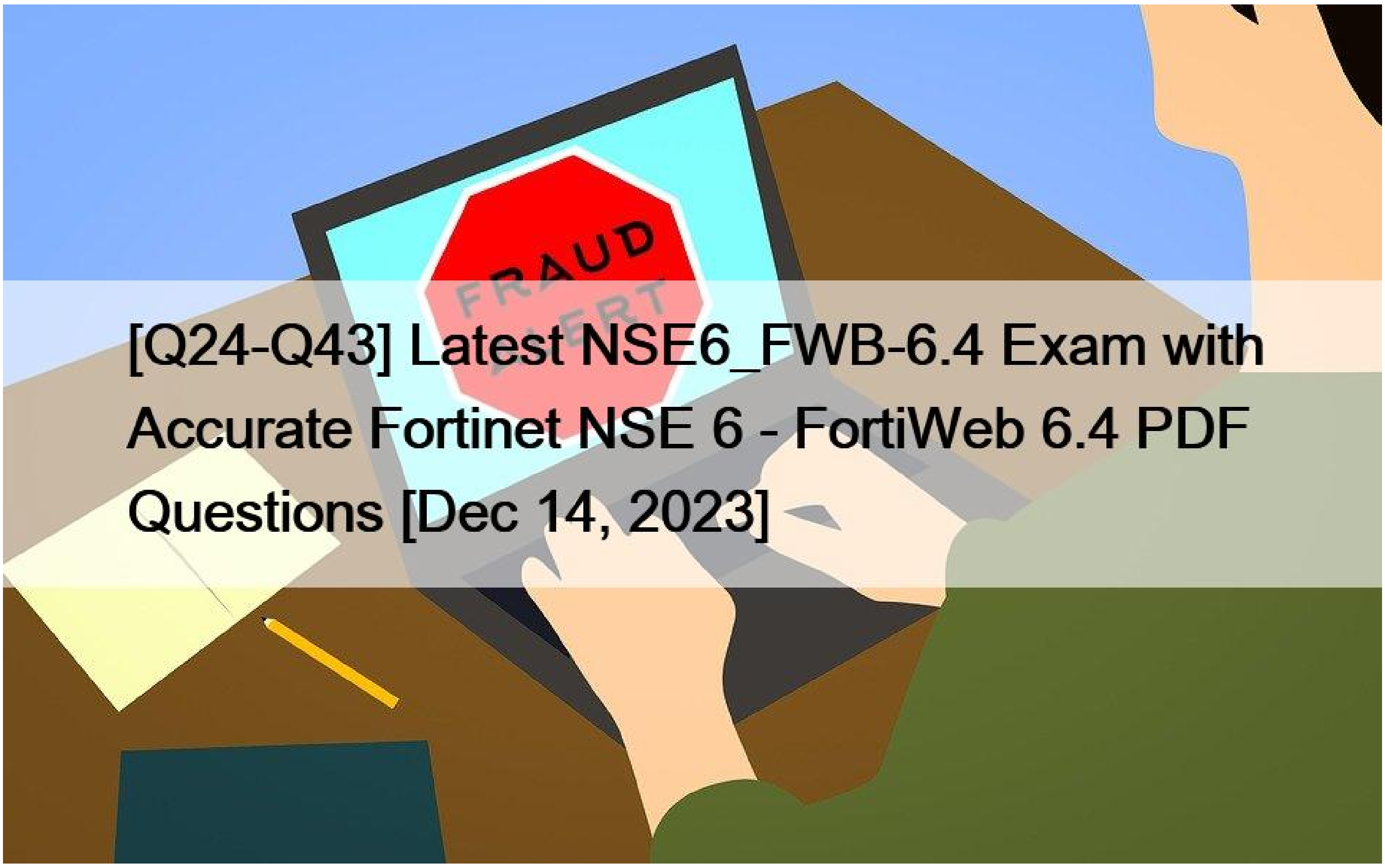
[Q24-Q43 Latest NSE6_FWB-6.4 Exam with Accurate Fortinet NSE 6 - FortiWeb 6.4 PDF Questions [Dec 14, 2023


FRAUD
ALERT
[Q24-Q43] Latest NSE6_FWB-6.4 Exam with Accurate Fortinet NSE 6 - FortiWeb 6.4 PDF Questions [Dec 14, 2023]

[Dec 14, 2023] Latest NSE6_FWB-6.4 Exam with Accurate Fortinet NSE 6 - FortiWeb 6.4 PDF Questions
Practice To NSE6_FWB-6.4 - Actualtests4sure Remarkable Practice On your Fortinet NSE 6 - FortiWeb 6.4 Exam

Fortinet is a renowned cybersecurity solution provider that offers a wide range of services for businesses looking to protect themselves from cyberattacks. The Fortinet NSE6_FWB-6.4 exam is the certification exam for the Fortinet NSE 6 - FortiWeb 6.4 solution. It is designed for cybersecurity professionals who want to validate their skills in deploying, managing, and maintaining the Fortinet FortiWeb 6.4 solution.

NEW QUESTION 24

What is one of the key benefits of the FortiGuard IP reputation feature?
* It maintains a list of private IP addresses.
* It provides a document of IP addresses that are suspect, so that administrators can manually update their blacklists.
* It is updated once per year.
* It maintains a list of public IPs with a bad reputation for participating in attacks.
Explanation

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

NEW QUESTION 25

In which two operating modes can FortiWeb modify HTTP packets? (Choose two.)
* Offline protection
* Transparent inspection
* True transparent proxy
* Reverse proxy

NEW QUESTION 26

Which implementation is best suited for a deployment that must meet compliance criteria?
* SSL Inspection with FortiWeb in Transparency mode
* SSL Offloading with FortiWeb in reverse proxy mode
* SSL Inspection with FrotiWeb in Reverse Proxy mode
* SSL Offloading with FortiWeb in Transparency Mode

NEW QUESTION 27

When is it possible to use a self-signed certificate, rather than one purchased from a commercial certificate authority?
* If you are a small business or home office
* If you are an enterprise whose employees use only mobile devices
* If you are an enterprise whose resources do not need security
* If you are an enterprise whose computers all trust your active directory or other CA server

NEW QUESTION 28

Under what circumstances would you want to use the temporary uncompress feature of FortiWeb?
* In the case of compression being done on the FortiWeb, to inspect the content of the compressed file
* In the case of the file being a .MP3 music file
* In the case of compression being done on the web server, to inspect the content of the compressed file.
* In the case of the file being an .MP4 video

NEW QUESTION 29

How does FortiWeb protect against defacement attacks?
* It keeps a complete backup of all files and the database.
* It keeps hashes of files and periodically compares them to the server.
* It keeps full copies of all files and directories.
* It keeps a live duplicate of the database.
Explanation

The anti-defacement feature examines a web site&#8217;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.

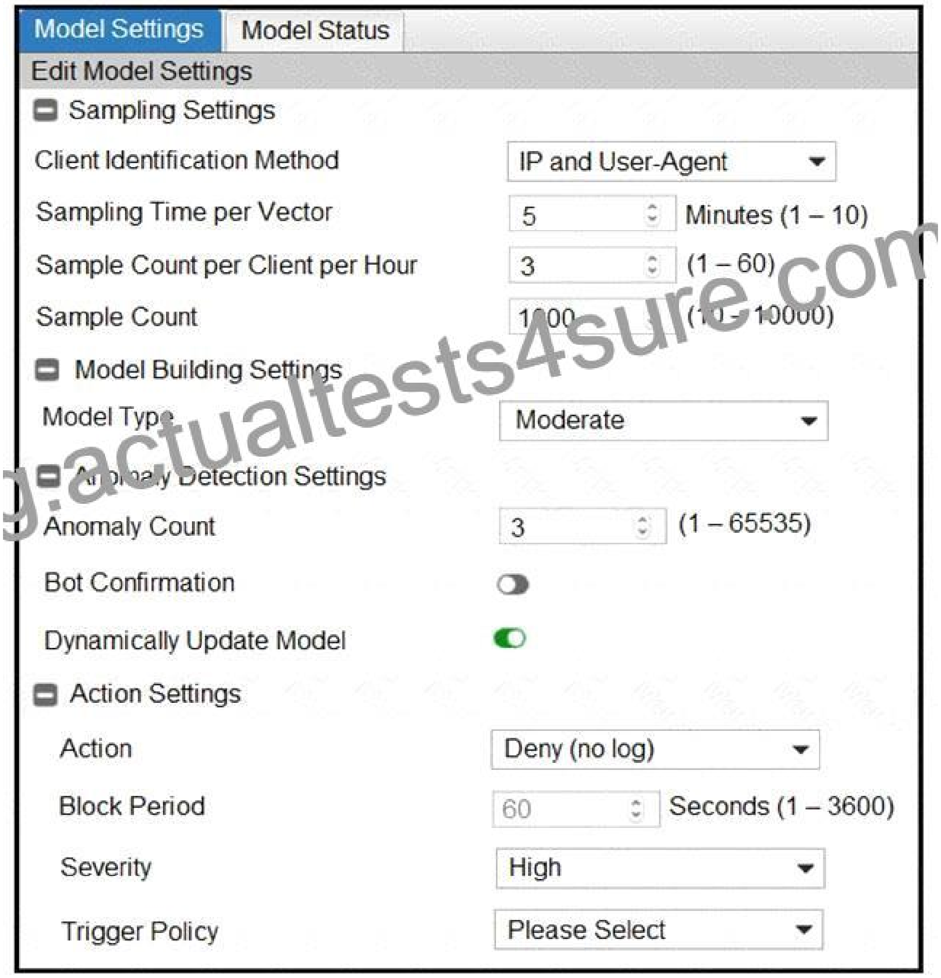
NEW QUESTION 30

What key factor must be considered when setting brute force rate limiting and blocking?
* A single client contacting multiple resources
* Multiple clients sharing a single Internet connection
* Multiple clients from geographically diverse locations
* Multiple clients connecting to multiple resources
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 31

Refer to the exhibit.



Edit Model Settings

Sampling Settings

Client Identification Method: IP and User-Agent
Sampling Time per Vector: 5 Minutes (1 – 10)
Sample Count per Client per Hour: 3 (1 – 60)
Sample Count: 1000 (10 – 10000)

Model Building Settings

Model Type: Moderate

Anomaly Detection Settings

Anomaly Count: 3 (1 – 65535)
Bot Confirmation: ○
Dynamically Update Model: ●

Action Settings

Action: Deny (no log)
Block Period: 60 Seconds (1 – 3600)
Severity: High
Trigger Policy: Please Select

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?
* Change Model Type to Strict
* Change Action under Action Settings to Alert

* Disable Dynamically Update Model
* Enable Bot Confirmation
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&#8217;s a real bot.

NEW QUESTION 32

When viewing the attack logs on FortiWeb, which client IP address is shown when you are using XFF header rules?
* FortiGate public IP
* FortiWeb IP
* FortiGate local IP
* Client real IP
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 33

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

NEW QUESTION 34

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.)
* Reply with a &#8220;403 Forbidden&#8221; HTTP error
* Allow the page access, but log the violation
* Automatically redirect the client to the login page
* Display an access policy message, then allow the client to continue, redirecting them to their requested page
* Prompt the client to authenticate

NEW QUESTION 35

Which two statements about the anti-defacement feature on FortiWeb are true? (Choose two.)
* Anti-defacement can redirect users to a backup web server, if it detects a change.

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

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 36

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?

- Enable &#8220;Shared IP&#8221; and configure the separate rate limits for requests from NATted source IPs.
- Configure FortiWeb to use &#8220;X-Forwarded-For:&#8221; headers to find each client&#8217;s private network IP, and to block attacks using that.
- Enable SYN cookies.
- Configure a server policy that matches requests from shared Internet connections.

NEW QUESTION 37

You are using HTTP content routing on FortiWeb. Requests for web app A should be forwarded to a cluster of web servers which all host the same web app. Requests for web app B should be forwarded to a different, single web server.

Which is true about the solution?

- Static or policy-based routes are not required.
- To achieve HTTP content routing, you must chain policies: the first policy accepts all traffic, and forwards requests for web app A to the virtual server for policy A. It also forwards requests for web app B to the virtual server for policy B. Policy A and Policy B apply their app-specific protection profiles, and then distribute that app&#8217;s traffic among all members of the server farm.
- You must put the single web server into a server pool in order to use it with HTTP content routing.
- The server policy applies the same protection profile to all its protected web apps.

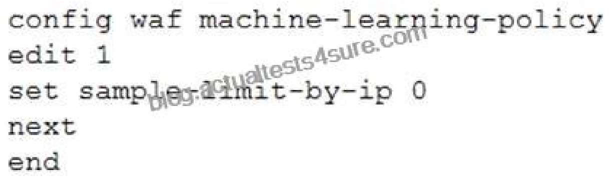
NEW QUESTION 38

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

- Defines Log file format
- Defines communication protocol
- Defines Database Schema
- Defines Log storage location

NEW QUESTION 39

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

NEW QUESTION 40

Under which circumstances does FortiWeb use its own certificates? (Choose Two)
* Secondary HTTPS connection to server where FortiWeb acts as a client
* HTTPS to clients
* HTTPS access to GUI
* HTTPS to FortiGate

NEW QUESTION 41

Which is true about HTTPS on FortiWeb? (Choose three.)
* For SNI, you select the certificate that FortiWeb will present in the server pool, not in the server policy.
* After enabling HSTS, redirects to HTTPS are no longer necessary.
* In true transparent mode, the TLS session terminator is a protected web server.
* Enabling RC4 protects against the BEAST attack, but is not recommended if you configure FortiWeb to only offer TLS 1.2.
* In transparent inspection mode, you select which certificate that FortiWeb will present in the server pool, not in the server policy.

NEW QUESTION 42

What can an administrator do if a client has been incorrectly period blocked?
* Nothing, it is not possible to override a period block.
* Manually release the ID address from the temporary blacklist.
* Force a new IP address to the client.
* Disconnect the client from the network.
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&#8217;s a temporary blacklist so you can manually release them from the blacklist.

NEW QUESTION 43

Which

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

- www.example.com
- www.example.com
- wwwexamplecom
- www/.example/.com

Explanation

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

The FortiWeb Web Application Firewall (WAF) is a part of the FortiGate security platform that's designed to secure web applications against several different types of vulnerabilities and attacks, including DoS attacks, SQL injection, cross-site scripting, and others. The Fortinet NSE6_FWB-6.4 certification exam focuses on assessing the candidate's knowledge of the FortiWeb WAF features, capabilities, and deployment, including the configuration and management of policies, authentication schemes, and other features. NSE6_FWB-6.4 exam also evaluates the candidate's understanding of how to integrate FortiWeb into a larger security architecture or into other Fortinet-based solutions.

Exam Questions and Answers for NSE6_FWB-6.4 Study Guide Questions and Answers!:
https://www.actualtests4sure.com/NSE6_FWB-6.4-test-questions.html]