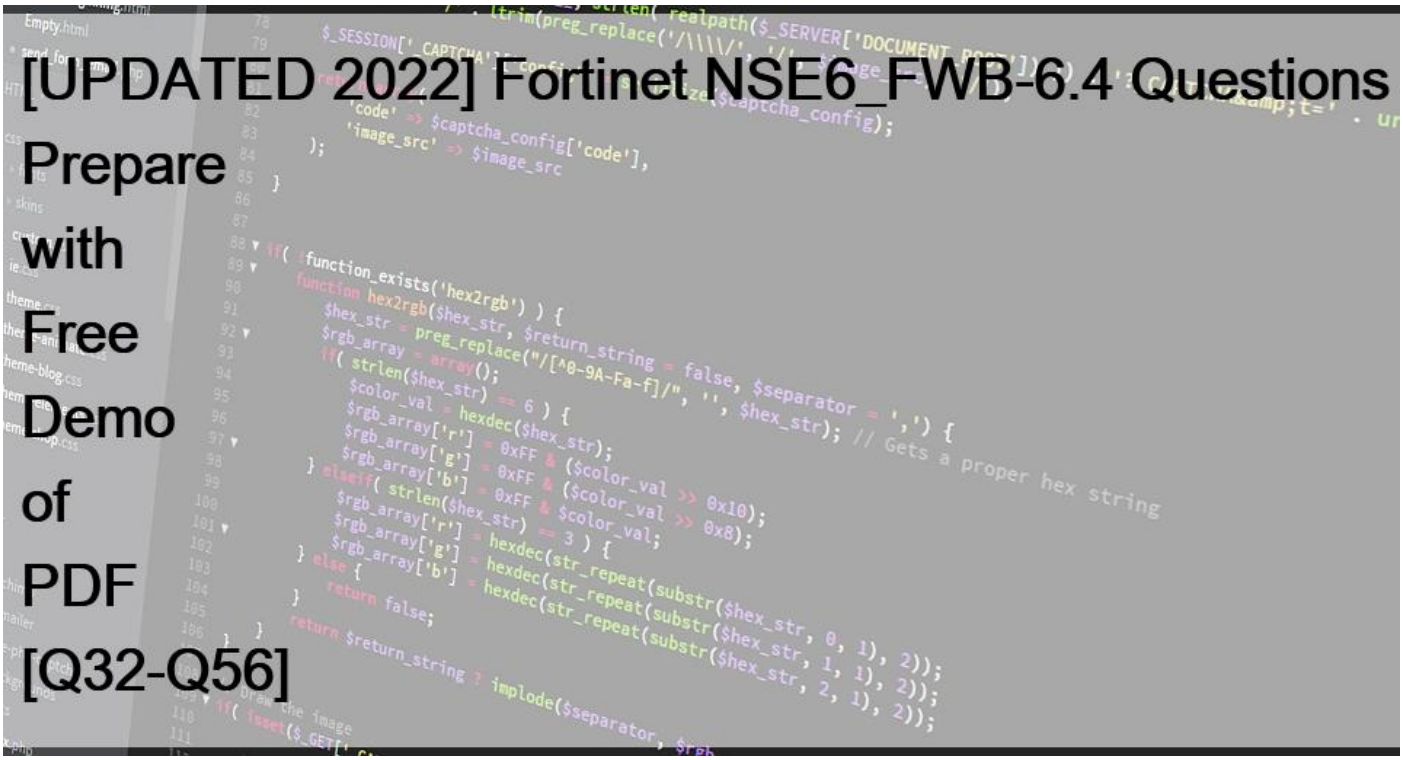
[UPDATED 2022 Fortinet NSE6_FWB-6.4 Questions Prepare with Free Demo of PDF [Q32-Q56



[UPDATED 2022] Fortinet NSE6_FWB-6.4 Questions Prepare with Free Demo of PDF
NEW 2022 Certification Sample Questions NSE6_FWB-6.4 Dumps & Practice Exam

Fortinet NSE6_FWB-6.4 Exam Syllabus Topics:

TopicDetailsTopic 1- Configure various access control and tracking methods- Troubleshoot deployment and system related issues
Topic 2- Troubleshoot threat detection and mitigation related issues- Identify FortiWeb deployment requirementsTopic 3- Encryption, Authentication, and Compliance- Mitigate web application vulnerabilitiesTopic 4- Configure HTTP content routing, rewriting, and redirection- Mitigate attacks on authentication

QUESTION 32

You’ve configured an authentication rule with delegation enabled on FortiWeb.

What happens when a user tries to access the web application?
* FrotiWeb redirects users to a FortiAuthenticator page, then if the user authenticates successfully, FortiGate signals to FortiWeb to allow access to the web app
* ForitWeb redirects the user to the web app’s authentication page
* FortiWeb forwards the HTTP challenge from the server to the client, then monitors the reply, allowing access if the user authenticates successfully
* 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

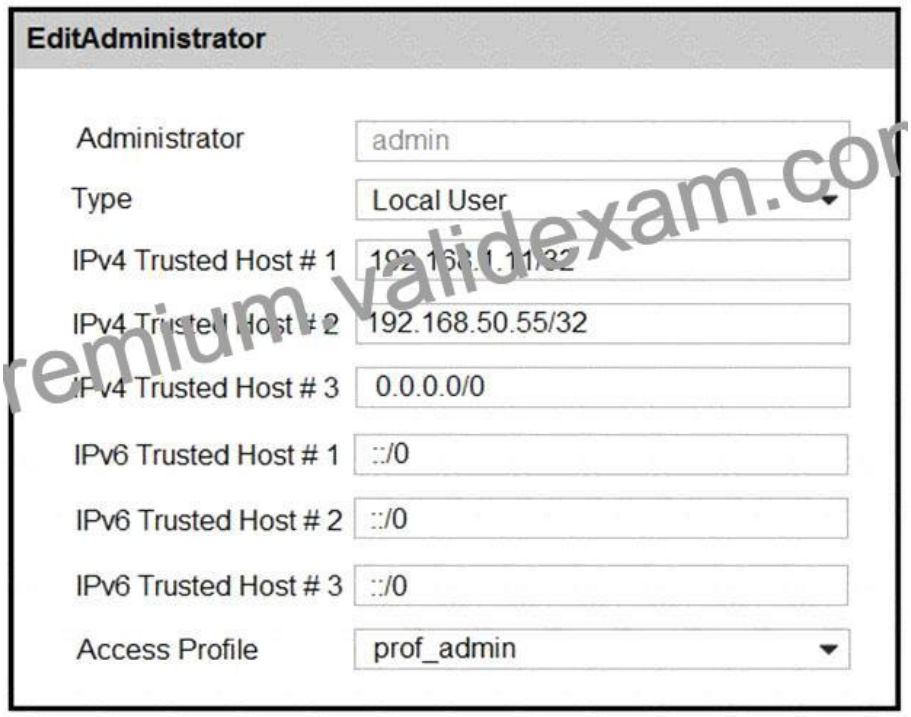
QUESTION 33

FortiWeb offers the same load balancing algorithms as FortiGate.

Which two Layer 7 switch methods does FortiWeb also offer? (Choose two.)
* Round robin
* HTTP session-based round robin
* HTTP user-based round robin
* HTTP content routes

QUESTION 34

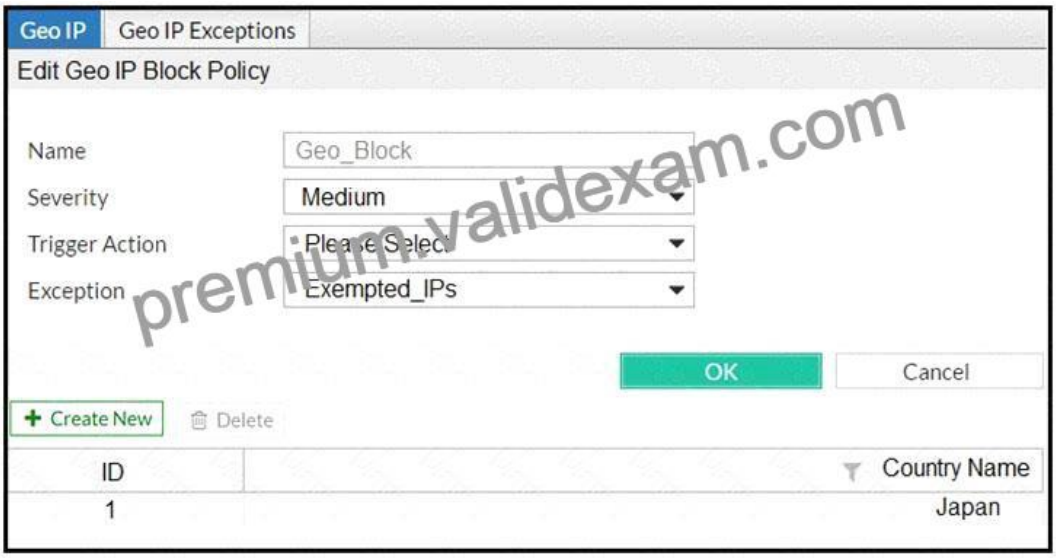
Refer to the exhibit.



There is only one administrator account configured on FortiWeb. What must an administrator do to restrict any brute force attacks that attempt to gain access to the FortiWeb management GUI?
* Delete the built-in administrator user and create a new one.
* Configure IPv4 Trusted Host # 3 with a specific IP address.
* The configuration changes must be made on the upstream device.
* Change the Access Profile to Read_Only.

QUESTION 35

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.)
* Manually update the geo-location IP addresses for Japan.
* If the IP address is configured as a geo reputation exception, remove it.
* Configure the IP address as a blacklisted IP address.
* If the IP address is configured as an IP reputation exception, remove it.

QUESTION 36

Refer to the exhibit.

Based on the configuration, what would happen if this FortiWeb were to lose power? (Choose two.)
* Traffic that passes between port5 and port6 will be inspected.
* Traffic will be interrupted between port3 and port4.
* All traffic will be interrupted.
* Traffic will pass between port5 and port6 uninspected.

QUESTION 37

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

QUESTION 38

When FortiWeb triggers a redirect action, which two HTTP codes does it send to the client to inform the browser of the new URL? (Choose two.)
* 403
* 302
* 301
* 404

QUESTION 39

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 “403 Forbidden” 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

QUESTION 40

Which operation mode does not require additional configuration in order to allow FTP traffic to your web server?
* Offline Protection
* Transparent Inspection
* True Transparent Proxy
* Reverse-Proxy

QUESTION 41

How does offloading compression to FortiWeb benefit your network?
* free up resources on the database server
* Free up resources on the web server
* reduces file size on the client’s storage
* free up resources on the FortiGate

QUESTION 42

What must you do with your FortiWeb logs to ensure PCI DSS compliance?
* Store in an off-site location
* Erase them every two weeks
* Enable masking of sensitive data
* Compress them into a .zip file format

QUESTION 43

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.

QUESTION 44

How does an ADOM differ from a VDOM?
* ADOMs do not have virtual networking
* ADOMs improve performance by offloading some functions.
* ADOMs only affect specific functions, and do not provide full separation like VDOMs do.
* Allows you to have 1 administrator for multiple tenants

QUESTION 45

Which two statements about running a vulnerability scan are true? (Choose two.)
* You should run the vulnerability scan during a maintenance window.
* You should run the vulnerability scan in a test environment.
* Vulnerability scanning increases the load on FortiWeb, so it should be avoided.
* You should run the vulnerability scan on a live website to get accurate results.

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.

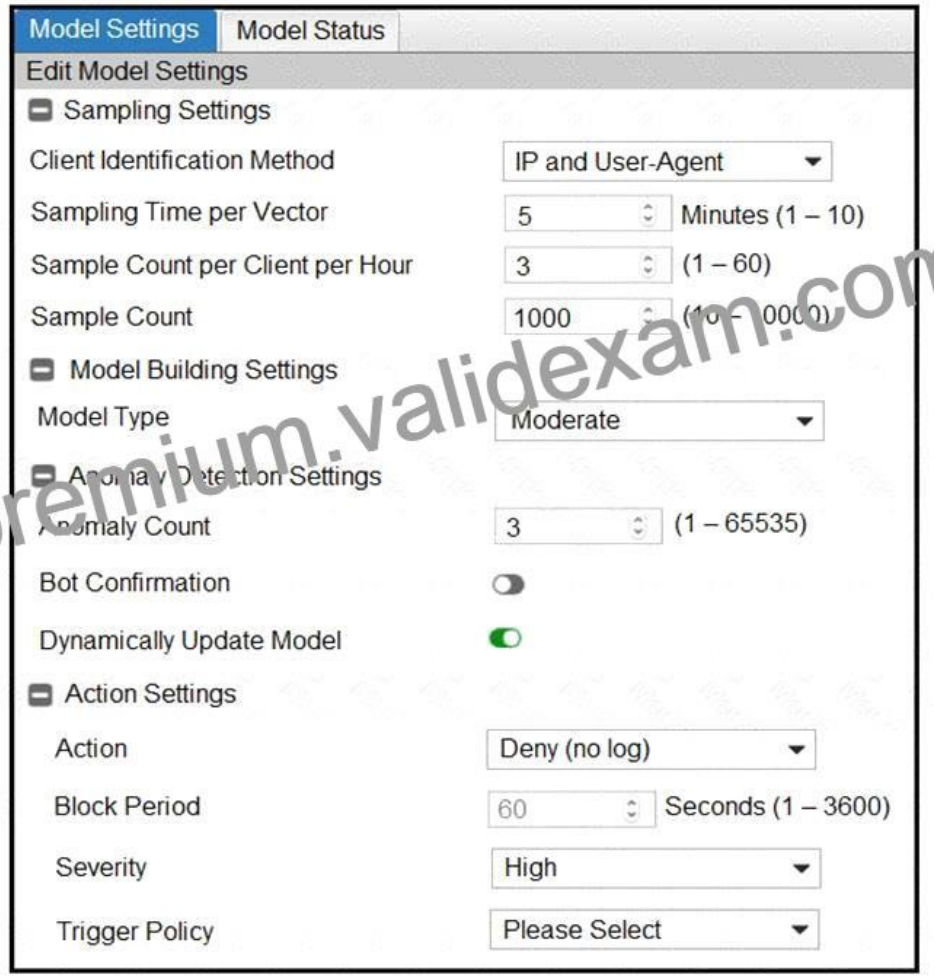
Vulnerabilities on live web sites. Instead, duplicate the web site and its database in a test environment.

QUESTION 46

Which three statements about HTTPS on FortiWeb are true? (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.

QUESTION 47

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?
* 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’s a real bot.

QUESTION 48

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

QUESTION 49

What role does FortiWeb play in ensuring PCI DSS compliance?
* It provides the ability to securely process cash transactions.
* It provides the required SQL server protection.
* It provides the WAF required by PCI.
* It provides credit card processing capabilities.

QUESTION 50

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

QUESTION 51

In which scenario might you want to use the compression feature on FortiWeb?
* When you are serving many corporate road warriors using 4G tablets and phones
* When you are offering a music streaming service
* When you want to reduce buffering of video streams
* Never, since most traffic today is already highly compressed

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

QUESTION 52

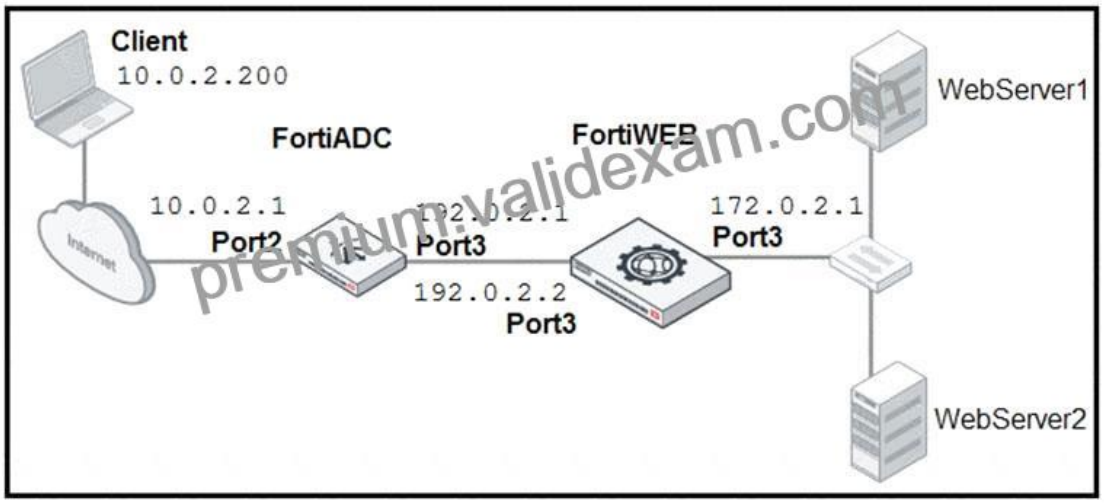
You are using HTTP content routing on FortiWeb. You want requests for web application A to be forwarded to a cluster of web servers, which all host the same web application. You want requests for web application B to be forwarded to a different, single web server.

Which statement about this solution is true?
* The server policy applies the same protection profile to all of its protected web applications.
* You must put the single web server in to a server pool, in order to use it with HTTP content routing.
* You must chain policies so that requests for web application A go to the virtual server for policy A, and requests for web

application B go to the virtual server for policy B.
* Static or policy-based routes are not required.

QUESTION 53

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.)
* Enable the Use X-Forwarded-For setting on FortiWeb.
* No Special configuration is required; connectivity will be re-established after the set timeout.
* Place FortiWeb in front of FortiADC.
* Enable the Add X-Forwarded-For setting on FortiWeb.

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

NSE6_FWB-6.4 Deluxe Study Guide with Online Test Engine: https://www.validexam.com/NSE6_FWB-6.4-latest-dumps.html]