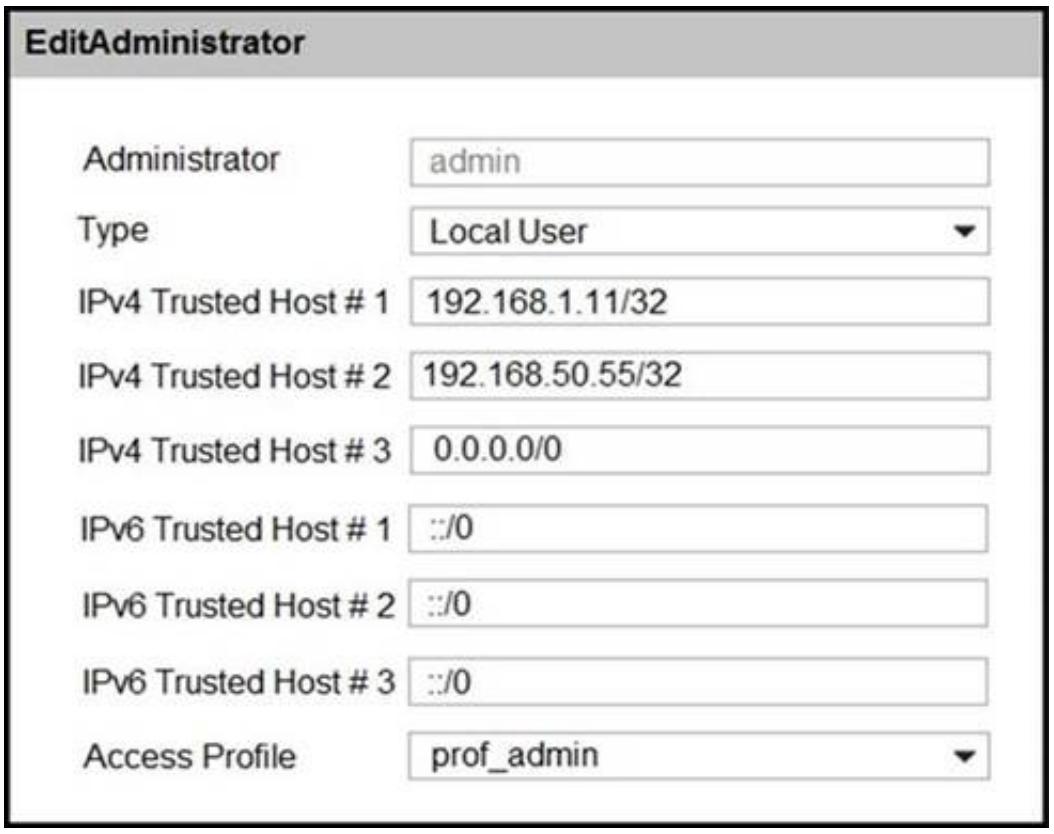
Fortinet

Exam Questions NSE6_FWB-6.4

Fortinet NSE 6 - FortiWeb 6.4

NEW QUESTION 1
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?

A. Delete the built-in administrator user and create a new one.
B. Configure IPv4 Trusted Host # 3 with a specific IP address.
C. The configuration changes must be made on the upstream device.
D. Change the Access Profile to Read_Only.

Answer: B

NEW QUESTION 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.

NEW QUESTION 3
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.)

A. 403
B. 302
C. 301
D. 404

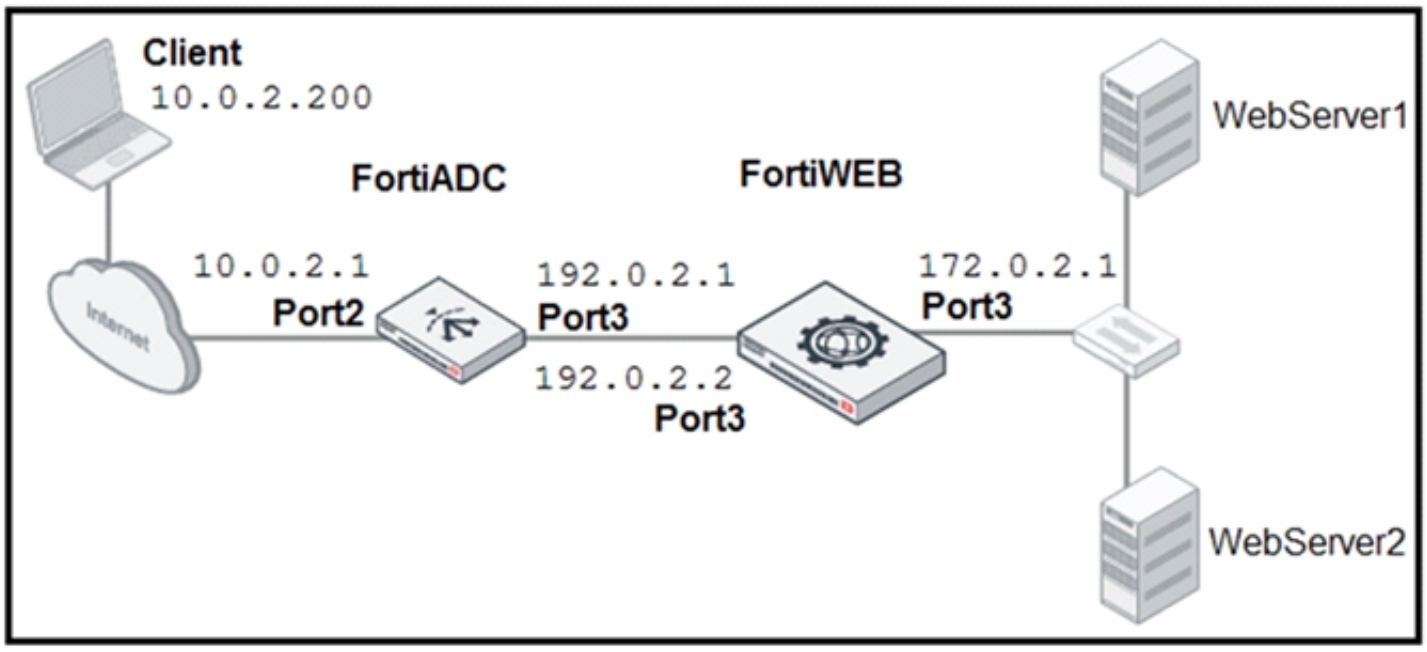
Answer: BC

NEW QUESTION 4
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 5
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 6
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 7
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

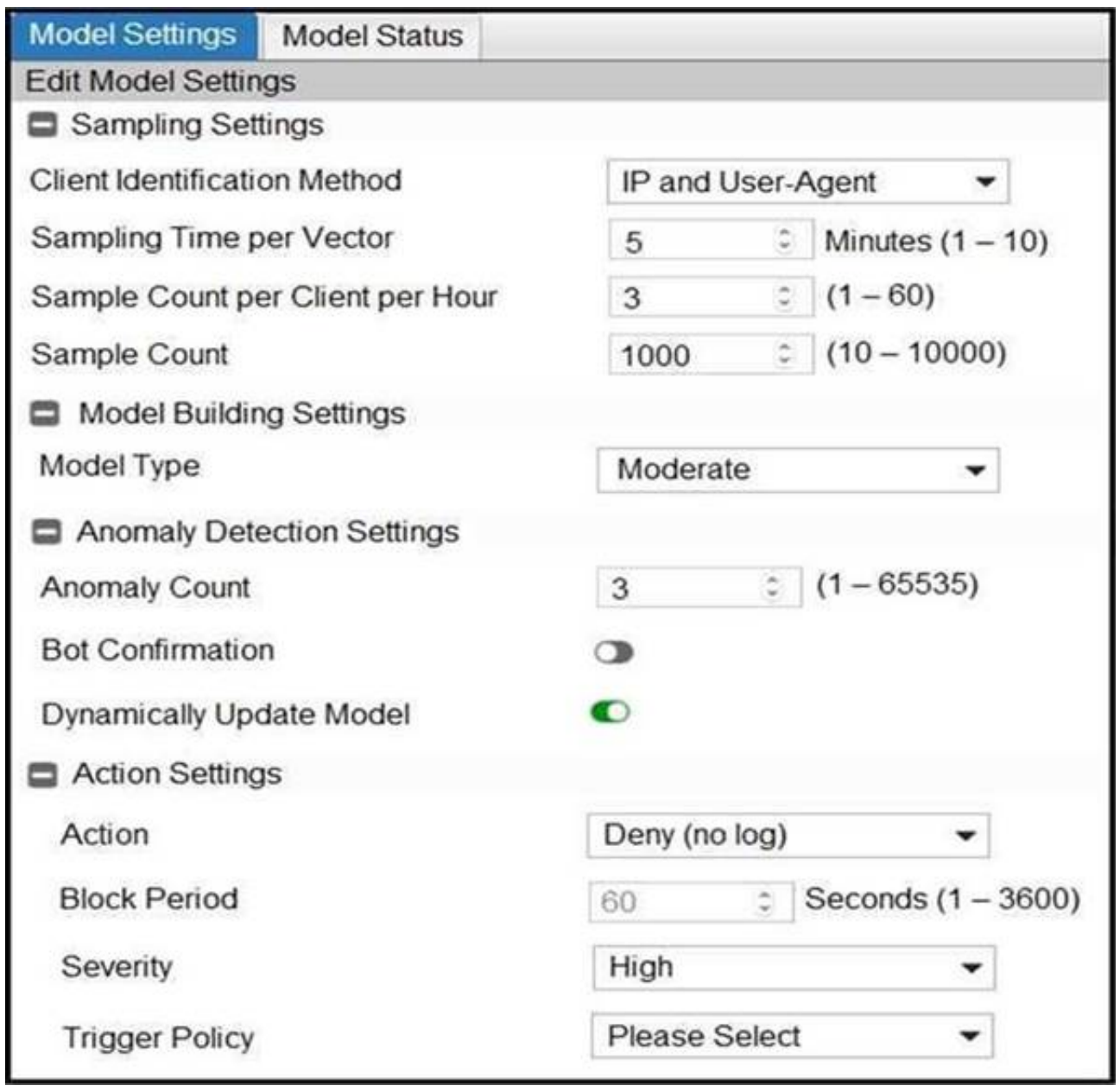
NEW QUESTION 8
Which regex expression is the correct format for redirecting the URL http://www.example.com?

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 9
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?

A. Change Model Type to Strict
B. Change Action under Action Settings to Alert
C. Disable Dynamically Update Model
D. Enable Bot Confirmation

Answer: D

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.

NEW QUESTION 10
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

NEW QUESTION 10
Which implementation is best suited for a deployment that must meet compliance criteria?

A. SSL Inspection with FortiWeb in Transparency mode
B. SSL Offloading with FortiWeb in reverse proxy mode
C. SSL Inspection with FrotiWeb in Reverse Proxy mode
D. SSL Offloading with FortiWeb in Transparency Mode

Answer: C

NEW QUESTION 11
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?

A. The server policy applies the same protection profile to all of its protected web applications.
B. You must put the single web server in to a server pool, in order to use it with HTTP content routing.

C. 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.
D. Static or policy-based routes are not required.

Answer: D

NEW QUESTION 14
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 19
When viewing the attack logs on FortiWeb, which client IP address is shown when you are using XFF header rules?

A. FortiGate public IP
B. FortiWeb IP
C. FortiGate local IP
D. Client real IP

Answer: D

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 23
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 24
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 26
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 27
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 32
Under which circumstances does FortiWeb use its own certificates? (Choose Two)

A. Secondary HTTPS connection to server where FortiWeb acts as a client
B. HTTPS to clients
C. HTTPS access to GUI
D. HTTPS to FortiGate

Answer: AC

NEW QUESTION 33
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?

A. Static or policy-based routes are not required.
B. 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
C. It also forwards requests for web app B to the virtual server for policy
D. Policy A and Policy B apply their app-specific protection profiles, and then distribute that app's traffic among all members of the server farm.
E. You must put the single web server into a server pool in order to use it with HTTP content routing.
F. The server policy applies the same protection profile to all its protected web apps.

Answer: B

NEW QUESTION 38
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 43
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 46
.....

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