Free Questions for NSE6_FWB-6.4 by go4braindumps

Shared by Fitzgerald on 22-07-2024

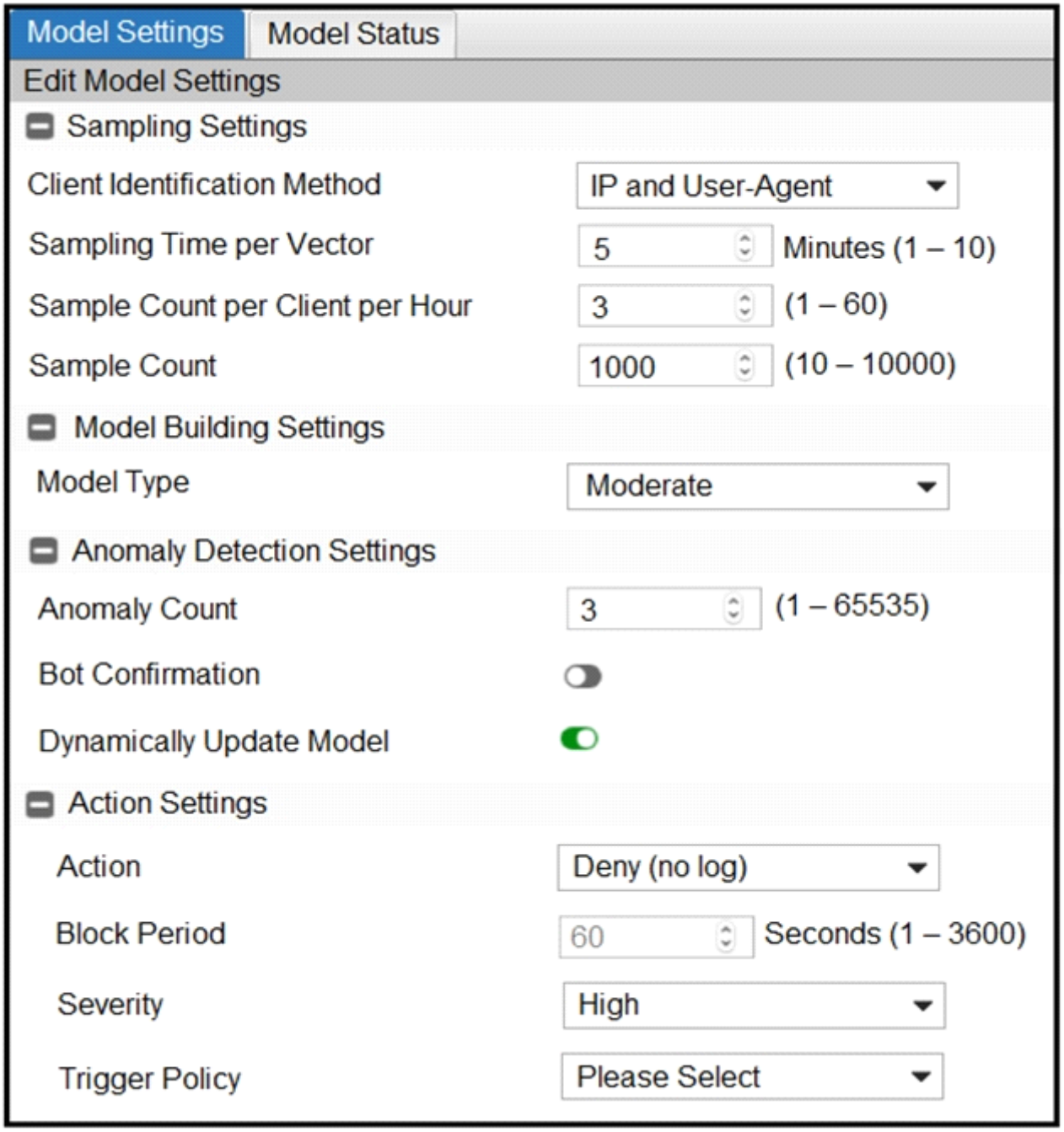
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.


Model Settings
Model Status
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?

Options:

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 theAnomaly Count, the system executesBot Confirmationbefore taking actions.

TheBot Confirmationis 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 2

Question Type: MultipleChoice

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.)

Options:

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:

B, C, E

Question 3

Question Type: MultipleChoice

Which algorithm is used to build mathematical models for bot detection?

Options:

A- HCM

B- SVN

C- SVM

D- HMM

Answer:

C

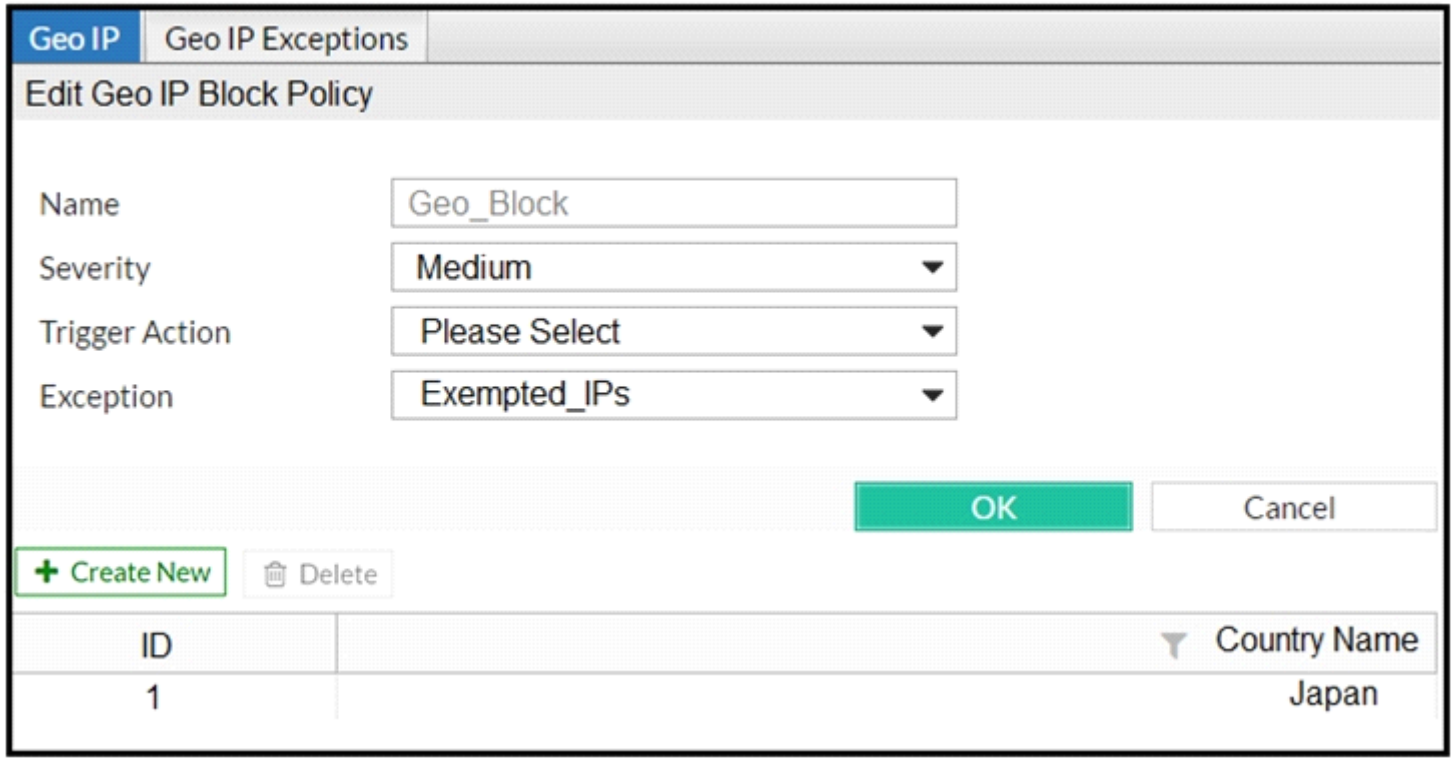
Explanation:

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

Question 4

Question Type: MultipleChoice

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.)

Options:

A- Manually update the geo-location IP addresses for Japan.

B- If the IP address is configured as a geo reputation exception, remove it.

C- Configure the IP address as a blacklisted IP address.

D- If the IP address is configured as an IP reputation exception, remove it.

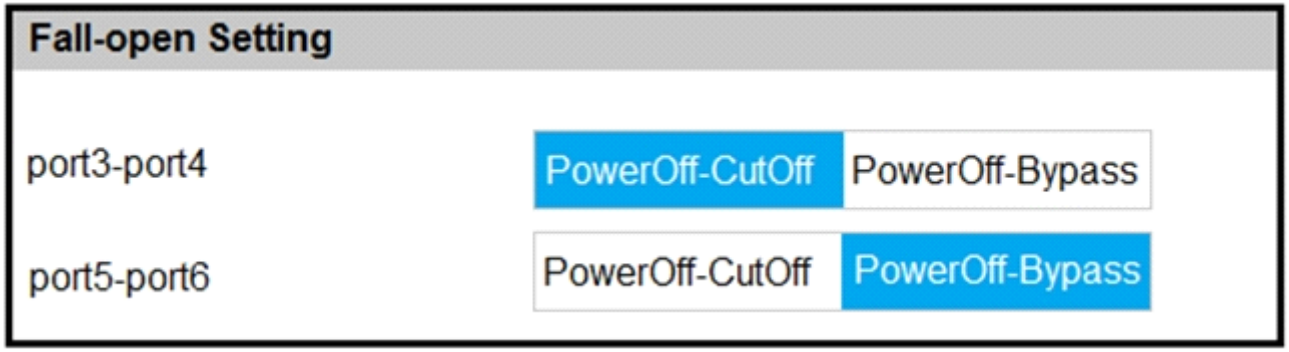
Answer:

B, C

Question 5

Question Type: MultipleChoice

Refer to the exhibit.



Based on the configuration, what would happen if this FortiWeb were to lose power? (Choose two.)

Options:

A- Traffic that passes between port5 and port6 will be inspected.

B- Traffic will be interrupted between port3 and port4.

C- All traffic will be interrupted.

D- Traffic will pass between port5 and port6 uninspected.

Answer:

B, D

Question 6

Question Type: MultipleChoice

Which statement about local user accounts is true?

Options:

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.

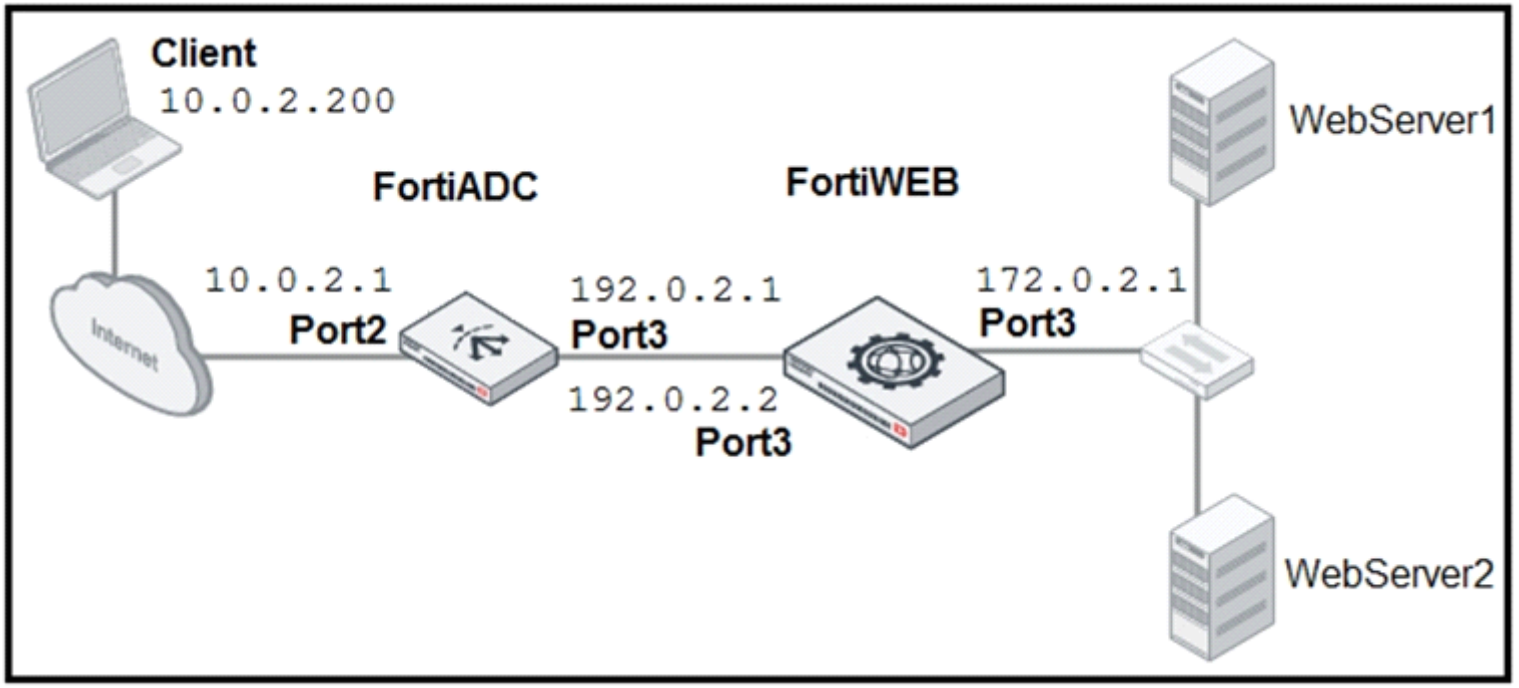
Answer:

B

Question 7

Question Type: MultipleChoice

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.)

Options:

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:

A, C

Explanation:

Configure your load balancer to insert or append to anX-Forwarded-For:,X-Real-IP:, or other HTTP X-header. Also configureFortiWebto find the original attacker's or client's IP address in that HTTP header

Question 8

Question Type: **MultipleChoice**

Which would be a reason to implement HTTP rewriting?

Options:

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.

Question 9

Question Type: **MultipleChoice**

FortiWeb offers the same load balancing algorithms as FortiGate.

Which two Layer 7 switch methods does FortiWeb also offer? (Choose two.)

Options:

A- Round robin

B- HTTP session-based round robin

C- HTTP user-based round robin

D- HTTP content routes

Answer:

A, D

Explanation:

http://fortinet.globalgate.com.ar/pdfs/FortiWeb/FortiWeb_DS.pdf

Question 10

Question Type: **MultipleChoice**

Which two statements about running a vulnerability scan are true? (Choose two.)

Options:

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:

A, B

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.

https://help.fortinet.com/fweb/552/Content/FortiWeb/fortiweb-admin/vulnerability_scans.htm