Practice Exam Questions

FORTINET

NSE6_FWB-6.4

Fortinet NSE 6 - FortiWeb 6.4

Fortinet

Exam NSE6_FWB-6.4

Fortinet NSE 6 - FortiWeb 6.4

Version: 3.0

[Total Questions: 56]

Question No : 1

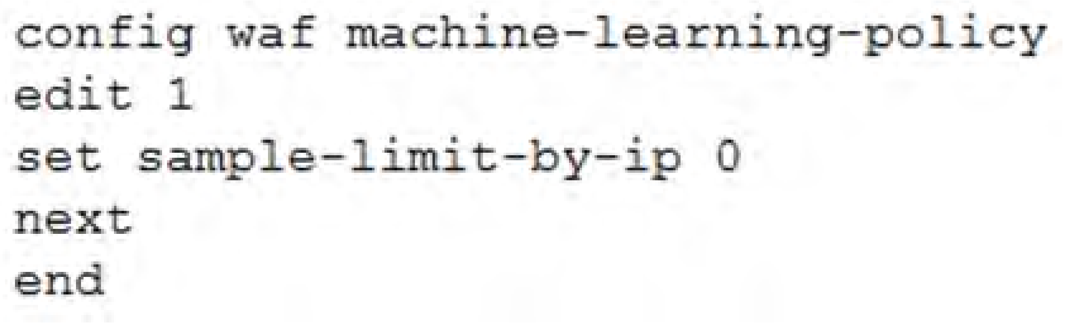
What capability can FortiWeb add to your Web App that your Web App may or may not already have?

A. Automatic backup and recovery
B. High Availability
C. HTTP/HTML Form Authentication
D. SSL Inspection

Answer: C

Question No : 2

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

Question No : 3

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

Question No : 4

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

Question No : 5

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

Question No : 6

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

Question No : 7

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

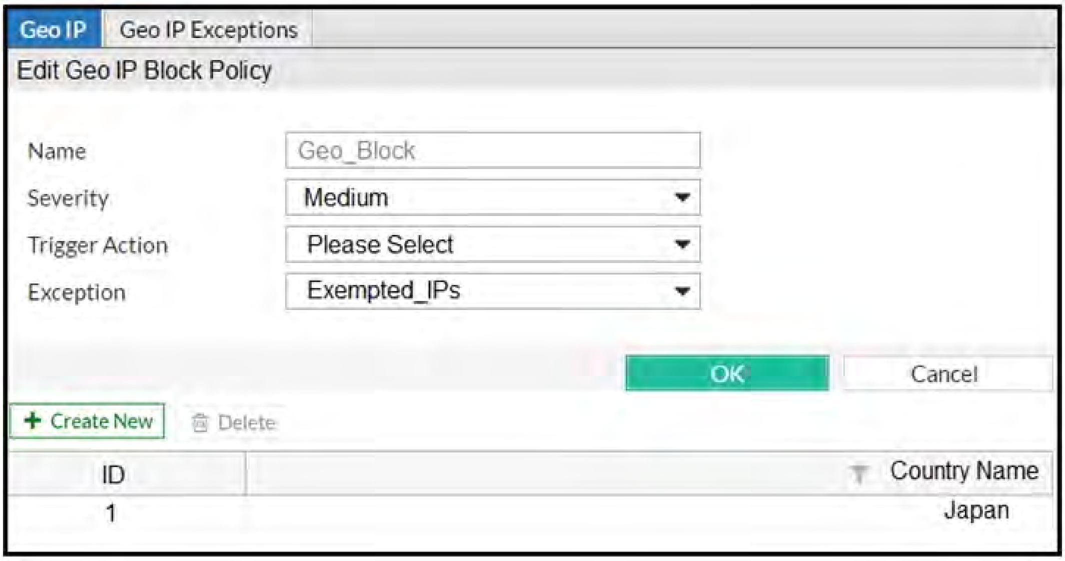
Answer: D

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.
Reference:
https://support.radware.com/app/answers/answer_view/a_id/20925/~/modifying-the-client-ip-address-in-the-xff-header-using-httpmod

Question No : 8

Refer to the exhibit.



Name: Geo_Block
Severity: Medium
Trigger Action: Please Select
Exception: Exempted_IPs

ID	Country Name
1	Japan

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.)

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 No : 9

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

Question No : 10

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.
Reference: https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/961303/rewriting-redirecting

Question No : 11

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.)

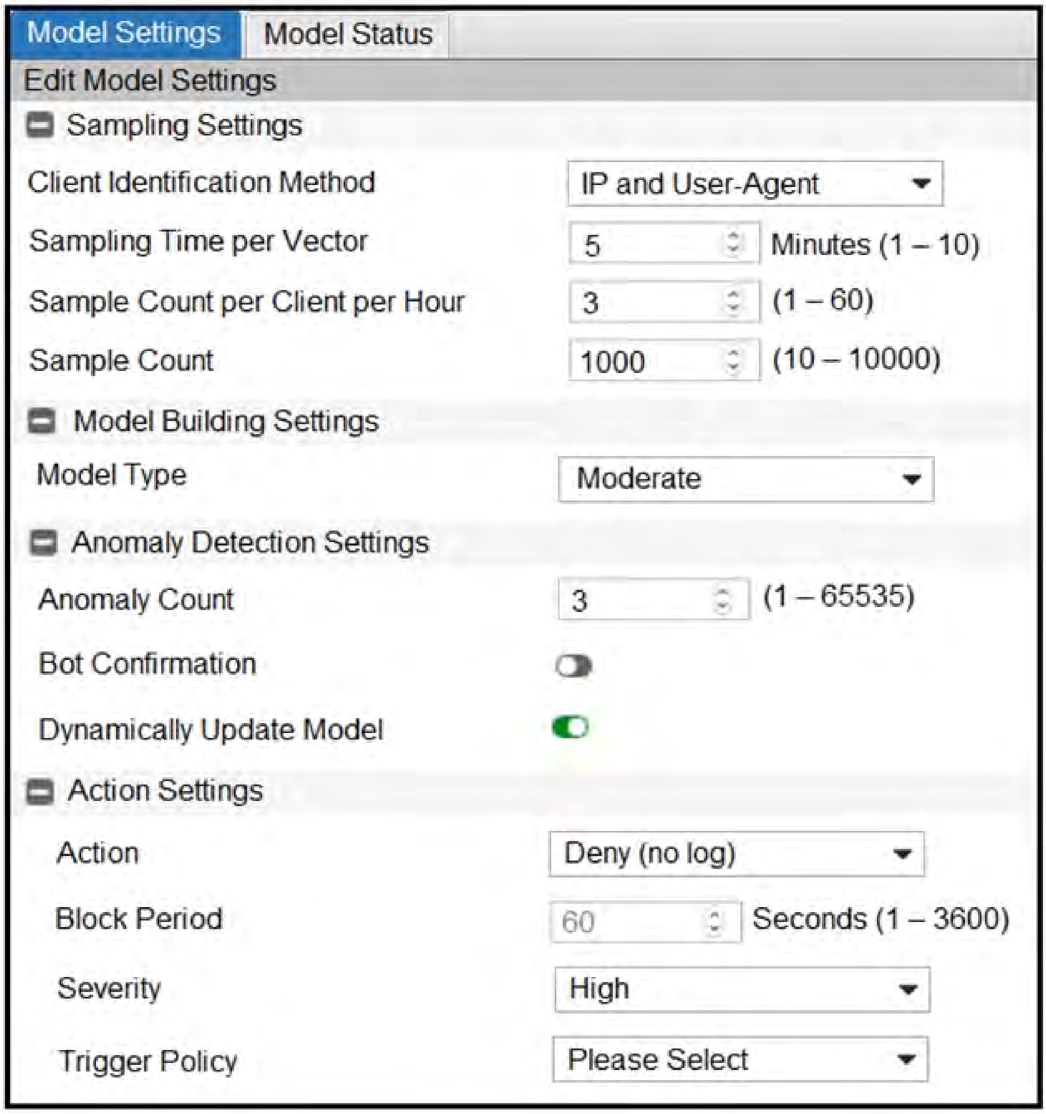
A. Display an access policy message, then allow the client to continue
B. Redirect the client to the login page
C. Allow the page access, but log the violation
D. Prompt the client to authenticate
E. Reply with a 403 Forbidden HTTP error

Answer: B,C,E

Reference: https://help.fortinet.com/fweb/607/Content/FortiWeb/fortiweb-admin/specify_urls_to_initiate.htm

Question No : 12

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?

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

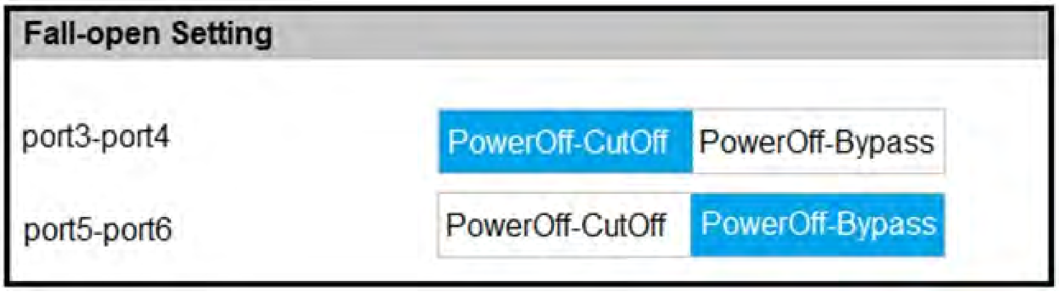
If the number of anomalies from a user has reached the Anomaly Count, the system executes Bot Confirmation before taking actions.

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.

Reference: https://docs.fortinet.com/document/fortiweb/6.3.1/administration-guide/600188/configuring-bot-detection-profiles

Question No : 13

Refer to the exhibit.



Fall-open Setting

port3-port4 [✓ PowerOff-CutOff] PowerOff-Bypass

port5-port6 PowerOff-CutOff [✓ PowerOff-Bypass]

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

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

Reference: https://docs.fortinet.com/document/fortiweb/6.3.10/administration-guide/33485/fail-to-wire-for-power-loss-reboots

Question No : 14

How does FortiWeb protect against defacement attacks?

A. It keeps a complete backup of all files and the database.
B. It keeps hashes of files and periodically compares them to the server.

C. It keeps full copies of all files and directories.
D. It keeps a live duplicate of the database.

Answer: B

Explanation:

The anti-defacement feature examines a web site'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.
Reference: https://help.fortinet.com/fweb/551/Content/FortiWeb/fortiweb-admin/anti_defacement.htm

Question No : 15

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: B,D

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.
Reference: https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/193258/machine-learning

Question No : 16

Which two statements about the anti-defacement feature on FortiWeb are true? (Choose two.)