Vendor: Fortinet

Exam Code: NSE6_FWB-6.4

Exam Name: Fortinet NSE 6 - FortiWeb 6.4

Version: DEMO

QUESTION 1
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 2
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

QUESTION 3
What is one of the key benefits of the FortiGuard IP reputation feature?

A. It maintains a list of private IP addresses.
B. It provides a document of IP addresses that are suspect, so that administrators can manually update their blacklists.
C. It is updated once per year.
D. It maintains a list of public IPs with a bad reputation for participating in attacks.

Answer: D
Explanation:
FortiGuard IP Reputation service assigns a poor reputation, including virus-infected clients and

malicious spiders/crawlers.

QUESTION 4
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.

QUESTION 5
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

QUESTION 6
When generating a protection configuration from an auto learning report what critical step must you do before generating the final protection configuration?

A. Restart the FortiWeb to clear the caches
B. Drill down in the report to correct any false positives.
C. Activate the report to create t profile
D. Take the FortiWeb offline to apply the profile

Answer: B

QUESTION 7
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 8
You are configuring FortiAnalyzer to store logs from FortiWeb.

Which is true?

A. FortiAnalyzer will store antivirus and DLP archives from FortiWeb.
B. You must enable ADOMs on FortiAnalyzer.
C. To store logs from FortiWeb 6.4, on FortiAnalyzer, you must select "FrotiWeb 6.1".
D. FortiWeb will query FortiAnalyzer for reports, instead of generating them locally.

Answer: B

QUESTION 9
Which of the following would be a reason for implementing rewrites?

A. Page has been moved to a new URL
B. Page has been moved to a new IP address
C. Replace vulnerable functions.
D. Send connection to secure channel

Answer: C

QUESTION 10
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.)

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

Answer: ABC

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**