

Fortinet

Exam Questions NSE6_FWB-6.4

Fortinet NSE 6 - FortiWeb 6.4



NEW QUESTION 1

How does your FortiWeb configuration differ if the FortiWeb is upstream of the SNAT device instead of downstream of the SNAT device?

- A. You must enable the “Use” X-Forwarded-For: option.
- B. FortiWeb must be set for Transparent Mode
- C. No special configuration required
- D. You must enable “Add” X-Forwarded-For: instead of the “Use” X-Forwarded-For: option.

Answer: D

NEW QUESTION 2

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

NEW QUESTION 3

When integrating FortiWeb and FortiAnalyzer, why is the selection for FortiWeb Version critical? (Choose two)

- A. Defines Log file format
- B. Defines communication protocol
- C. Defines Database Schema
- D. Defines Log storage location

Answer: AD

NEW QUESTION 4

In which two operating modes can FortiWeb modify HTTP packets? (Choose two.)

- A. Offline protection
- B. Transparent inspection
- C. True transparent proxy
- D. Reverse proxy

Answer: CD

NEW QUESTION 5

In which scenario might you want to use the compression feature on FortiWeb?

- A. When you are serving many corporate road warriors using 4G tablets and phones
- B. When you are offering a music streaming service
- C. When you want to reduce buffering of video streams
- D. Never, since most traffic today is already highly compressed

Answer: A

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

NEW QUESTION 6

Refer to the exhibits.

Edit Server Pool

Name

server-pool1

Protocol

HTTP

Type

Reverse Proxy

Offline Protection

True Transparent Proxy

Transparent Inspection

WCCP

Single Server/Server Balance

Single Server

Server Balance

Server Health Check

availability-check1

Load Balancing Algorithm

Round Robin

Persistence

session-persistence-cookie1

Comments

0/199 (bytes)

OK

Cancel

+ Create New

Edit

Delete

| ID | IP/Domain | Status | Port | HTTP/2 | Inherit Health Check | Server Health Check | Backup Server | SSL |
|----|-----------|--------|------|---------|----------------------|---------------------|---------------|---------|
| 1 | 10.0.1.21 | Enable | 80 | Disable | Yes | | Disable | Disable |
| 2 | 10.0.1.22 | Enable | 80 | Disable | Yes | | Disable | Disable |

Edit Virtual Server

Name

vserver1

Use Interface IP

IPv4 Address

10.0.1.8/255.255.255.0

IPv6 Address

::/0

Interface

port1

FortiWeb is configured in reverse proxy mode and it is deployed downstream to FortiGate. Based on the configuration shown in the exhibits, which of the following statements is true?

- A. FortiGate should forward web traffic to the server pool IP addresses.
- B. The configuration is incorrec
- C. FortiWeb should always be located upstream to FortiGate.
- D. You must disable the Preserve Client IP setting on FotriGate for this configuration to work.
- E. FortiGate should forward web traffic to virtual server IP address.

Answer: D

NEW QUESTION 7

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 8

When is it possible to use a self-signed certificate, rather than one purchased from a commercial certificate authority?

- A. If you are a small business or home office
- B. If you are an enterprise whose employees use only mobile devices
- C. If you are an enterprise whose resources do not need security
- D. If you are an enterprise whose computers all trust your active directory or other CA server

Answer: D

NEW QUESTION 9

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 10

True transparent proxy mode is best suited for use in which type of environment?

- A. New networks where infrastructure is not yet defined
- B. Flexible environments where you can easily change the IP addressing scheme
- C. Small office to home office environments
- D. Environments where you cannot change the IP addressing scheme

Answer: B

Explanation:

"Because blocking is not guaranteed to succeed in offline mode, this mode is best used during the evaluation and planning phase, early in implementation. Reverse proxy is the most popular operating mode. It can rewrite URLs, offload TLS, load balance, and apply NAT. For very large MSSP, true transparent mode has a significant advantage. You can drop it in without changing any schemes of limited IPv4 space—in transparent mode, you don't need to give IP addresses to the network interfaces on FortiWeb."

NEW QUESTION 10

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 15

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.

NEW QUESTION 17

Refer to the exhibit.



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: BD

NEW QUESTION 20

You are deploying FortiWeb 6.4 in an Amazon Web Services cloud. Which 2 lines of this initial setup via CLI are incorrect? (Choose two.)

```
1 config system settings
2 set opmode transparent
3 set gateway 10.0.0.1
4 end
5 config system interface
6 set port1
7 set ip 10.0.0.5
8 set allowaccess https ssh ping
9 end
```

- A. 6
- B. 9
- C. 3
- D. 2

Answer: AC

NEW QUESTION 23

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 27

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 30

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 35

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions 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 First Try
- * NSE6_FWB-6.4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE6_FWB-6.4 Practice Test Here](#)