

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

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 3

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

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

Under what circumstances would you want to use the temporary uncompress feature of FortiWeb?

- A. In the case of compression being done on the FortiWeb, to inspect the content of the compressed file
- B. In the case of the file being a .MP3 music file
- C. In the case of compression being done on the web server, to inspect the content of the compressed file.
- D. In the case of the file being an .MP4 video

Answer: C

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 incorrect.
- C. FortiWeb should always be located upstream to FortiGate.
- D. You must disable the Preserve Client IP setting on FortiGate for this configuration to work.
- E. FortiGate should forward web traffic to virtual server IP address.

Answer: D

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

How does offloading compression to FortiWeb benefit your network?

- A. free up resources on the database server
- B. Free up resources on the web server
- C. reduces file size on the client's storage
- D. free up resources on the FortiGate

Answer: B

NEW QUESTION 9

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 10

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	<input type="checkbox"/>
Dynamically Update Model	<input checked="" type="checkbox"/>
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.

NEW QUESTION 10

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 13

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 14

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 16

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 19

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 22

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 26

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 31

What role does FortiWeb play in ensuring PCI DSS compliance?

- A. PCI specifically requires a WAF
- B. Provides credit card processing capabilities
- C. Provide ability to securely process cash transactions
- D. Provides load balancing between multiple web servers

Answer: A

Explanation:

FortiWeb helps you meet all PCI requirements, but PCI now specifically recommends using a WAF, and developing remediations against the top 10 vulnerabilities, according to OWASP.

NEW QUESTION 35

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.

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 39

.....

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](#)