



Free Questions for NSE6_FWB-6.4 by actualtestdumps

Shared by Vargas on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How does FortiWeb protect against defacement attacks?

Options:

- 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 2

Question Type: MultipleChoice

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

Options:

- 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 3

Question Type: MultipleChoice

Which three statements about HTTPS on FortiWeb are true? (Choose three.)

Options:

- 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:

C, D, E

Question 4

Question Type: MultipleChoice

When viewing the attack logs on FortiWeb, which client IP address is shown when you are using XFF header rules?

Options:

- 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.

Question 5

Question Type: MultipleChoice

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

Options:

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

Answer:

C, D

Question 6

Question Type: MultipleChoice

The FortiWeb machine learning (ML) feature is a two-phase analysis mechanism.

Which two functions does the first layer perform? (Choose two.)

Options:

- 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.

Question 7

Question Type: MultipleChoice

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

Options:

- 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

Question 8

Question Type: MultipleChoice

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

Options:

- 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

Question 9

Question Type: MultipleChoice

Refer to the exhibits.

Edit Server Pool

Name	<input type="text" value="server-pool1"/>
Protocol	HTTP
Type	<ul style="list-style-type: none">Reverse ProxyOffline ProtectionTrue Transparent ProxyTransparent InspectionWCCP
Single Server/Server Balance	<input type="radio"/> Single Server <input checked="" type="radio"/> Server Balance
Server Health Check	<input type="text" value="availability-check1"/> ▼
Load Balancing Algorithm	<input type="text" value="Round Robin"/> ▼
Persistence	<input type="text" value="session-persistence-cookie1"/> ▼
Comments	<input type="text"/> 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	<input type="text" value="vserver1"/>
Use Interface IP	<input type="checkbox"/>
IPv4 Address	<input type="text" value="10.0.1.8/255.255.255.0"/>
IPv6 Address	<input "::="" 0"="" type="text" value=""/>
Interface	<input type="text" value="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?

Options:

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

Answer:

D

Question 10

Question Type: MultipleChoice

What key factor must be considered when setting brute force rate limiting and blocking?

Options:

- 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

To Get Premium Files for NSE6_FWB-6.4 Visit

https://www.p2pexams.com/products/nse6_fwb-6.4

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/nse6-fwb-6.4>

