Fortinet

Exam Questions NSE6_FWB-6.4

Fortinet NSE 6 - FortiWeb 6.4

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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.

NEW QUESTION 2
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

NEW QUESTION 3
What must you do with your FortiWeb logs to ensure PCI DSS compliance?

A. Store in an off-site location
B. Erase them every two weeks
C. Enable masking of sensitive data
D. Compress them into a .zip file format

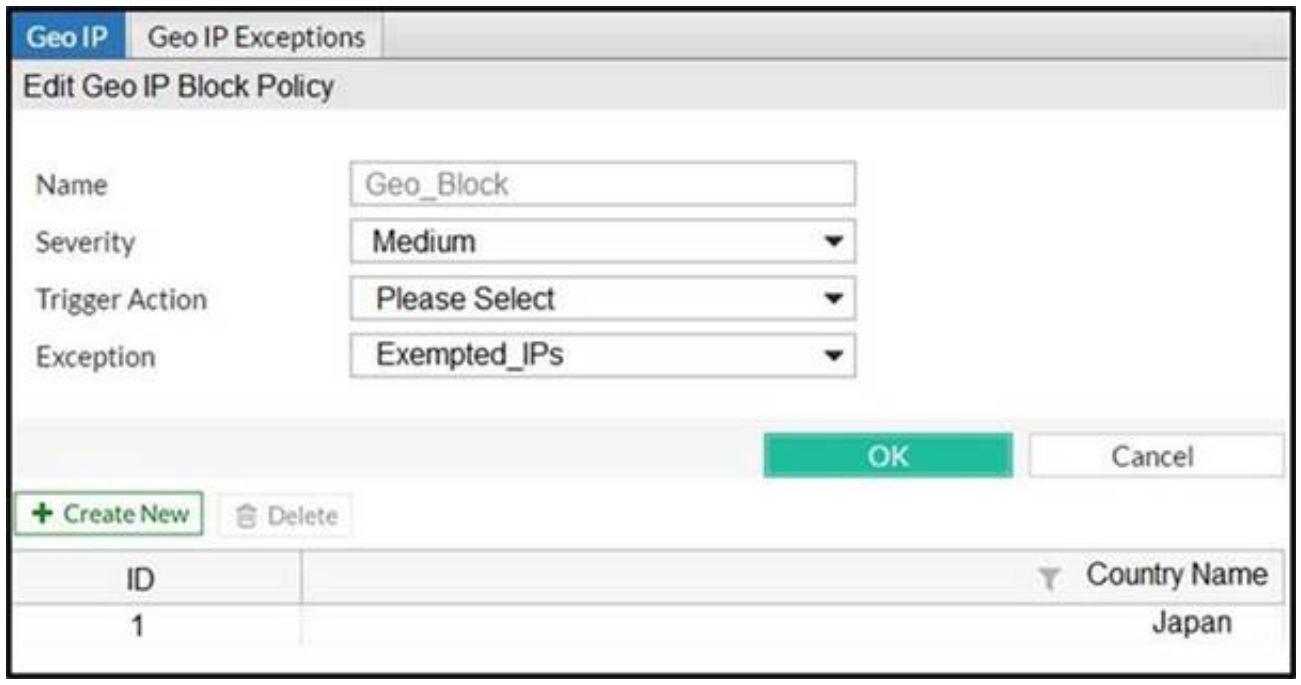
Answer: C

NEW QUESTION 4
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

NEW QUESTION 5
Refer to the exhibit.

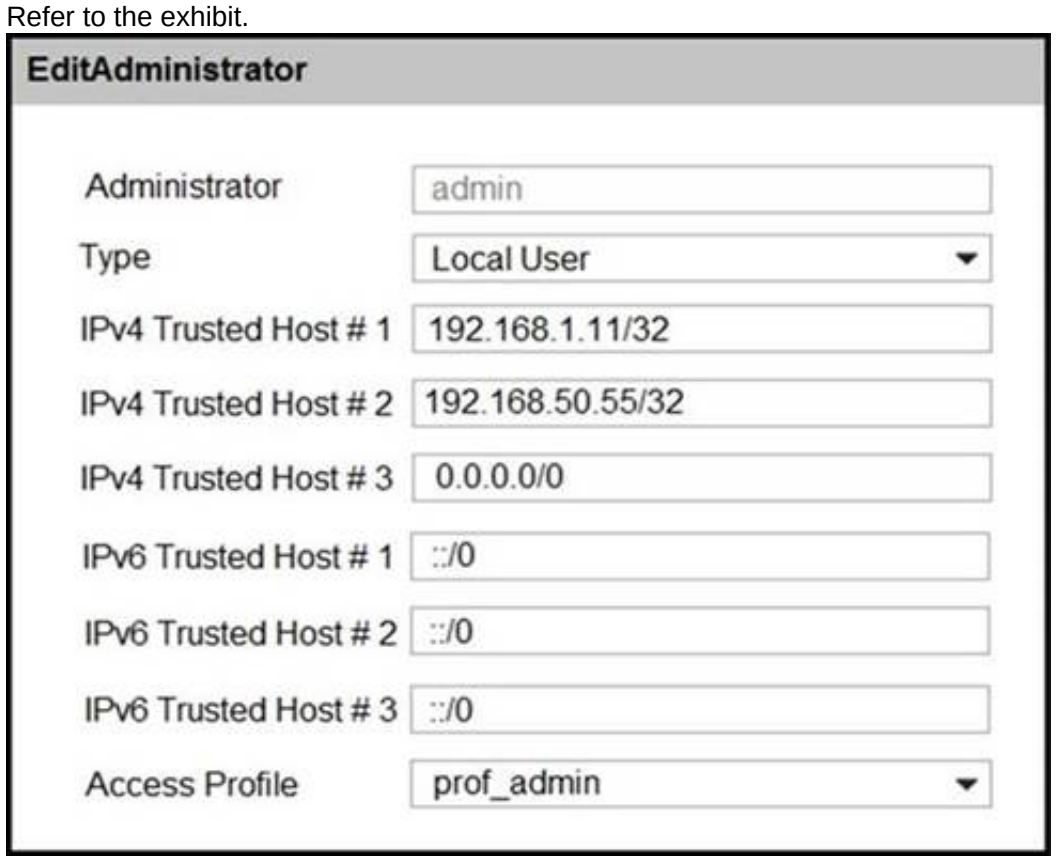


FortiWeb is configured to block traffic from Japan to your web application server. However, in the logs, the administrator is seeing traffic allowed from one particular IP address which is geo-located in Japan.
What can the administrator do to solve this problem? (Choose two.)

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: BC

NEW QUESTION 6
Refer to the exhibit.



There is only one administrator account configured on FortiWeb. What must an administrator do to restrict any brute force attacks that attempt to gain access to the FortiWeb management GUI?

A. Delete the built-in administrator user and create a new one.
B. Configure IPv4 Trusted Host # 3 with a specific IP address.
C. The configuration changes must be made on the upstream device.
D. Change the Access Profile to Read_Only.

Answer: B

NEW QUESTION 7
What other consideration must you take into account when configuring Defacement protection

A. Use FortiWeb to block SQL Injections and keep regular backups of the Database
B. Also incorporate a FortiADC into your network
C. Non
D. FortiWeb completely secures the site against defacement attacks
E. Configure the FortiGate to perform Anti-Defacement as well

Answer: A

NEW QUESTION 8
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

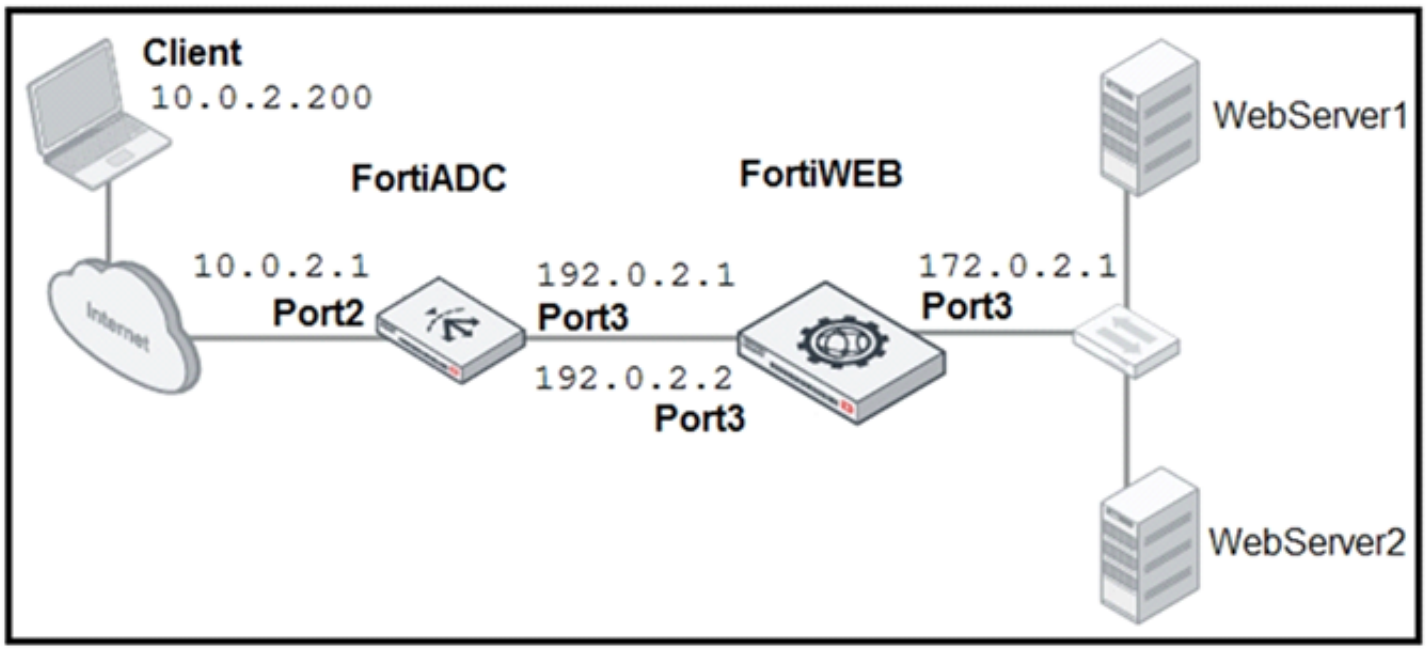
Explanation:
https://training.fortinet.com/course/view.php?id=3363
When might you want to use the compression feature on FortiWeb? When you are serving many road warriors who are using 4G tablets and phones

NEW QUESTION 9
When FortiWeb triggers a redirect action, which two HTTP codes does it send to the client to inform the browser of the new URL? (Choose two.)

A. 403
B. 302
C. 301
D. 404

Answer: BC

NEW QUESTION 10
Refer to the exhibit.



FortiADC is applying SNAT to all inbound traffic going to the servers. When an attack occurs, FortiWeb blocks traffic based on the 192.0.2.1 source IP address, which belongs to FortiADC. The setup is breaking all connectivity and genuine clients are not able to access the servers.
What must the administrator do to avoid this problem? (Choose two.)

A. Enable the Use X-Forwarded-For setting on FortiWeb.
B. No Special configuration is required; connectivity will be re-established after the set timeout.
C. Place FortiWeb in front of FortiADC.
D. Enable the Add X-Forwarded-For setting on FortiWeb.

Answer: AC

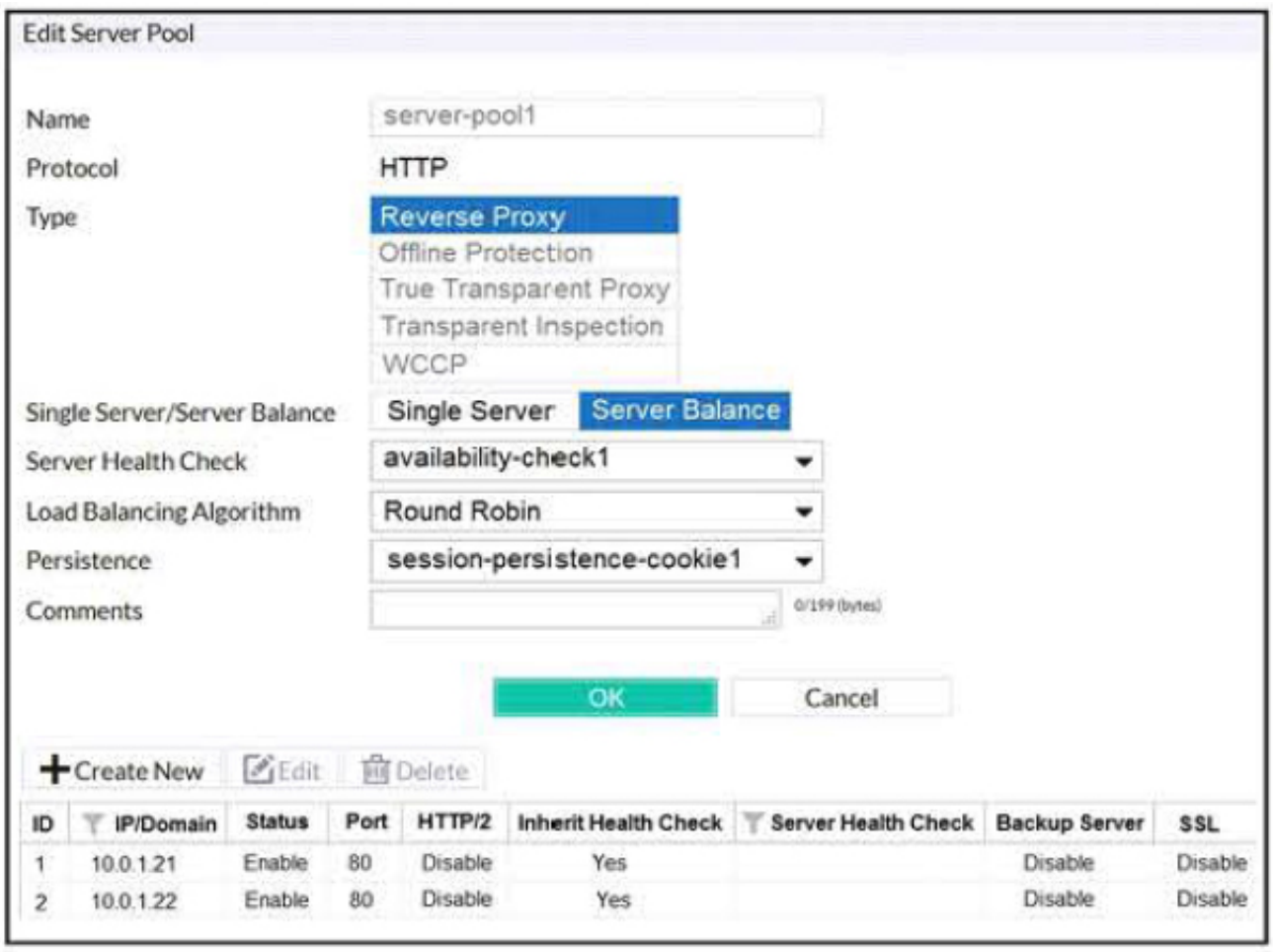
Explanation:
Configure your load balancer to insert or append to an X-Forwarded-For:, X-Real-IP:, or other HTTP
X- header. Also configure FortiWeb to find the original attacker's or client's IP address in that HTTP header

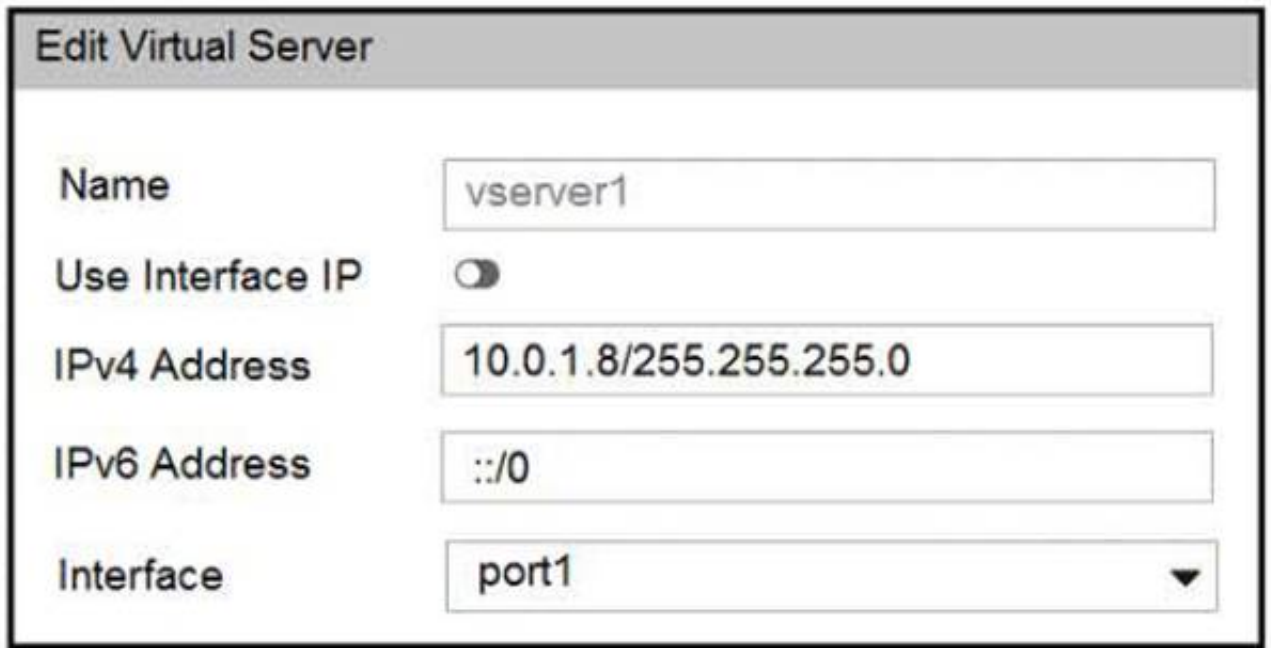
NEW QUESTION 10
Which operation mode does not require additional configuration in order to allow FTP traffic to your web server?

A. Offline Protection
B. Transparent Inspection
C. True Transparent Proxy
D. Reverse-Proxy

Answer: B

NEW QUESTION 15
Refer to the exhibits.





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 19
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 21
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 24
What benefit does Auto Learning provide?

A. Automatically identifies and blocks suspicious IPs
B. FortiWeb scans all traffic without taking action and makes recommendations on rules
C. Automatically builds rules sets
D. Automatically blocks all detected threats

Answer: C

NEW QUESTION 28
In which operation mode(s) can FortiWeb modify HTTP packets? (Choose two.)

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

Answer: CD

NEW QUESTION 29
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

NEW QUESTION 30
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 33
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 36
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 41
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 43
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 46
Which algorithm is used to build mathematical models for bot detection?

A. HCM
B. SVN
C. SVM
D. HMM

Answer: C

Explanation:
FortiWeb uses SVM (Support Vector Machine) algorithm to build up the bot detection model

NEW QUESTION 47
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 52
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 53
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: BCE

NEW QUESTION 54
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 57
.....

Relate Links

100% Pass Your NSE6_FWB-6.4 Exam with Exambible Prep Materials

https://www.exambible.com/NSE6_FWB-6.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/