NSE6_FWB-6.4 $^{Q\&As}$

Fortinet NSE 6 - FortiWeb 6.4

Pass Fortinet NSE6_FWB-6.4 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse6_fwb-6-4.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which is true about HTTPS on FortiWeb? (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.

Correct Answer: ACE

QUESTION 2

Refer to the exhibit.

EditAdministrator

Administrator	admin
Type	Local User ▼
IPv4 Trusted Host # 1	192.168.1.11/32
IPv4 Trusted Host # 2	192.168.50.55/32
IPv4 Trusted Host # 3	0.0.0.0/0
IPv6 Trusted Host # 1	::/0
IPv6 Trusted Host # 2	::/0
IPv6 Trusted Host # 3	::/0
Access Profile	prof_admin ▼

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.

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortiweb/6.1.1/administration-guide/397469/preventing-brute-force-logins

QUESTION 3

What can an administrator do if a client has been incorrectly period blocked?

A. Nothing, it is not possible to override a period block.

B. Manually release the ID address from the temporary blacklist.

C. Force a new IP address to the client.

D. Disconnect the client from the network.

Correct Answer: B

Block Period Enter the number of seconds that you want to block the requests. The valid range is 1?,600 seconds. The default value is 60 seconds. This option only takes effect when you choose Period Block in Action. Note: That\\'s a temporary blacklist so you can manually release them from the blacklist. Reference: https://docs.fortinet.com/document/fortiweb/6.3.1/administration-guide/600188/configuring-bot-detection-profiles

QUESTION 4

You\\'ve configured an authentication rule with delegation enabled on FortiWeb. What happens when a user tries to access the web application?

A. FrotiWeb redirects users to a FortiAuthenticator page, then if the user authenticates successfully, FortiGate signals to FortiWeb to allow access to the web app

B. ForitWeb redirects the user to the web app\\'s authentication page

C. FortiWeb forwards the HTTP challenge from the server to the client, then monitors the reply, allowing access if the user authenticates successfully

D. FortiWeb replies with a HTTP challenge of behalf of the server, the if the user authenticates successfully, FortiWeb allows the request and also includes credentials in the request that it forwards to the web app

Correct Answer: A

QUESTION 5

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

Correct Answer: C

Reference: https://docplayer.net/8466775-Fortiweb-web-application-firewall-ensuring-compliance-for-pci-dss-requirement-6-6-solution-guide.html

[NSE6_FWB-6.4 PDF Dumps](#)   [NSE6_FWB-6.4 Exam Questions](#)   [NSE6_FWB-6.4 Braindumps](#)