



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.geekcert.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

In Reverse proxy mode, how does FortiWeb handle traffic that does not match any defined policies?

- A. Non-matching traffic is allowed
- B. non-Matching traffic is held in buffer
- C. Non-matching traffic is Denied
- D. Non-matching traffic is rerouted to FortiGate

Correct Answer: C

QUESTION 2

FortiWeb offers the same load balancing algorithms as FortiGate.

Which two Layer 7 switch methods does FortiWeb also offer? (Choose two.)

- A. Round robin
- B. HTTP session-based round robin
- C. HTTP user-based round robin
- D. HTTP content routes

Correct Answer: AD

Reference: <https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/399384/defining-your-web-servers>
http://fortinet.globalgate.com.ar/pdfs/FortiWeb/FortiWeb_DS.pdf

QUESTION 3

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

Correct Answer: A

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.



QUESTION 4

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.

Correct Answer: CDE

Reference: <https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/742465/supported-cipher-suites-protocol-versions>

QUESTION 5

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.

Correct Answer: C

[NSE6_FWB-6.4 VCE Dumps](#)

[NSE6_FWB-6.4 Practice Test](#)

[NSE6_FWB-6.4 Study Guide](#)