



NSE6_FWB-6.0^{Q&As}

Fortinet NSE 6 - FortiWeb 6.0

Pass Fortinet NSE6_FWB-6.0 Exam with 100% Guarantee

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

https://www.passapply.com/nse6_fwb-6-0.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

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: B

QUESTION 2

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

Correct Answer: B

QUESTION 3

How does an ADOM differ from a VDOM?

- A. ADOMs do not have virtual networking
- B. ADOMs improve performance by offloading some functions.
- C. ADOMs only affect specific functions, and do not provide full separation like VDOMs do.
- D. Allows you to have 1 administrator for multiple tenants

Correct Answer: D

QUESTION 4

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 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-6.0 Practice Test](#)

[NSE6_FWB-6.0 Study Guide](#)

[NSE6_FWB-6.0 Braindumps](#)