

NSE6_FWB-6.1^{Q&As}

Fortinet NSE 6 - FortiWeb 6.1

Pass Fortinet NSE6_FWB-6.1 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse6_fwb-6-1.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

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

Correct Answer: ABC

QUESTION 3

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 4

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

QUESTION 5

How does your FortiWeb configuration differ if the FortiWeb is upstream of the SNAT device instead of downstream of the SNAT device?

- A. You must enable the "Use" X-Forwarded-For: option.
- B. FortiWeb must be set for Transparent Mode
- C. No special configuration required
- D. You must enable "Add" X-Forwarded-For: instead of the "Use" X-Forwarded-For: option.

Correct Answer: A

[Latest NSE6_FWB-6.1 Dumps](#)

[NSE6_FWB-6.1 VCE Dumps](#)

[NSE6_FWB-6.1 Study Guide](#)