

DUMPSQUEEN

Fortinet NSE 6 - FortiWeb 6.4

Fortinet NSE6 FWB-6.4

Version Demo

Total Demo Questions: 10

Total Premium Questions: 56

Buy Premium PDF

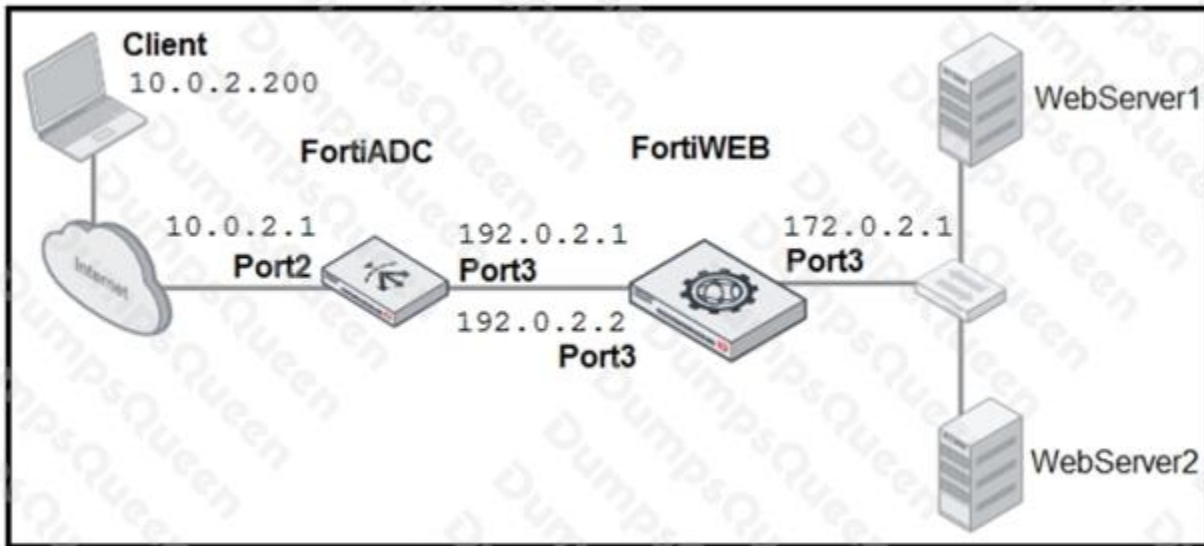
<https://dumpsqueen.com>

support@dumpsqueen.com

dumpsqueen.com

QUESTION NO: 1

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: A C

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

Reference: https://help.fortinet.com/fweb/560/Content/FortiWeb/fortiweb-admin/planning_topology.htm

QUESTION NO: 2

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.

ANSWER: A C E

QUESTION NO: 3

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

ANSWER: C

QUESTION NO: 4

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 FortiWeb in Reverse Proxy mode
- D. SSL Offloading with FortiWeb in Transparency Mode

ANSWER: C

QUESTION NO: 5

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.

ANSWER: C D E

Explanation:

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

QUESTION NO: 6

Which two statements about the anti-defacement feature on FortiWeb are true? (Choose two.)

- A. Anti-defacement can redirect users to a backup web server, if it detects a change.
- B. Anti-defacement downloads a copy of your website to RAM, in order to restore a clean image, if it detects defacement.
- C. FortiWeb will only check to see if there are changes on the web server; it will not download the whole file each time.
- D. Anti-defacement does not make a backup copy of your databases.

ANSWER: C D

Explanation:

Anti-defacement backs up web pages only, not databases.

If it detects any file changes, the FortiWeb appliance will download a new backup revision.

Reference: https://help.fortinet.com/fweb/551/Content/FortiWeb/fortiweb-admin/anti_defacement.htm

QUESTION NO: 7

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

QUESTION NO: 8

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: B C E

Explanation:

Reference: https://help.fortinet.com/fweb/607/Content/FortiWeb/fortiweb-admin/specify_urls_to_initiate.htm

QUESTION NO: 9

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

QUESTION NO: 10

What role does FortiWeb play in ensuring PCI DSS compliance?

- A. It provides the ability to securely process cash transactions.
- B. It provides the required SQL server protection.
- C. It provides the WAF required by PCI.
- D. It provides credit card processing capabilities.

ANSWER: C