PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 6 - FortiWeb 6.4

Fortinet NSE6_FWB-6.4

Version Demo

Total Demo Questions: 7

Total Premium Questions: 78

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Deployment and Configuration	29
Topic 2, WAF Configuration	7
Topic 3, Authentication and Access Control	13
Topic 4, Advanced Protection	28
Topic 5, Troubleshooting	1
Total	78

QUESTION NO: 1

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:

FortiWeb anti-defacement protects website content by maintaining known-good copies of monitored web pages and checking the protected site at configured intervals. To reduce bandwidth and processing overhead during routine monitoring, FortiWeb first checks whether content has changed rather than downloading every complete file on every polling cycle. When it identifies a change, FortiWeb can retrieve the affected content and compare it with its protected revision so that an unauthorized modification can be detected and handled according to the anti-defacement policy. This makes the statement that FortiWeb checks for changes without downloading the whole file each time accurate. Anti-defacement is specifically a web-content protection and restoration capability: it backs up and restores website files/pages, not application databases. Database contents require separate backup, replication, and recovery controls implemented by the database platform or other backup tooling. Therefore, the statement that anti-defacement does not make a backup copy of databases is also accurate. Fortinet's anti-defacement documentation describes the feature's website-content backup and monitoring behavior: FortiWeb Anti-defacement documentation. Additional FortiWeb documentation is available from the Fortinet Documentation Library.

QUESTION NO: 2

You've configured an authentication rule with delegation enabled on FortiWeb.

What happens when a user tries to access the web application?

A. FortiWeb redirects users to a FortiAuthenticator page, then, if the user authenticates successfully, FortiAuthenticator signals 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

ANSWER: A

Explanation:

With delegation enabled, FortiWeb delegates the user-authentication process to FortiAuthenticator rather than performing the credential challenge itself or relying on the protected application's login page. When the user requests the protected web application, FortiWeb redirects the user to the FortiAuthenticator authentication page. FortiAuthenticator applies its configured authentication policy, which can include directory-based authentication and additional controls such as two-factor authentication. After the user successfully authenticates, FortiAuthenticator returns the delegated-authentication result to FortiWeb. FortiWeb then recognizes the authenticated session and permits the user to access the protected web application according to the matching authentication rule and any associated access policy. This design centralizes identity verification in FortiAuthenticator while allowing FortiWeb to remain the enforcement point in front of the web application. The corrected wording identifies FortiAuthenticator, rather than FortiGate, as the component that performs the delegated authentication and communicates the successful result back to FortiWeb. Fortinet's FortiWeb administration documentation describes authentication and authentication-rule behavior, while the FortiAuthenticator documentation covers its centralized identity and authentication role. See the FortiWeb 6.4 Administration Guide and the FortiAuthenticator 6.4 Administration Guide.

QUESTION NO: 3

Which of the following is true about Local User Accounts?

A. Must be assigned regardless of any other authentication

B. Can be used for Single Sign On

C. Can be used for site publishing

D. Best suited for large environments with many users

ANSWER: C

Explanation:

Can be used for site publishing is correct. In FortiWeb, local user accounts are accounts maintained directly on the FortiWeb appliance and can be selected as an authentication source when configuring access control for published applications. Site publishing uses an authentication policy to determine how users authenticate before FortiWeb permits access to protected content. A locally defined user or local user group can therefore provide the identity store for a site-publishing authentication policy, which is useful when an external directory service is not required for that protected site or when only a limited set of users needs access.

After the local accounts are created, administrators can organize them into local groups and reference the relevant user/group configuration in the authentication and site-publishing policy. FortiWeb then validates the credentials supplied by the client as part of the access workflow and applies the configured publishing rules to the request. This capability makes local accounts an appropriate built-in authentication source for site-publishing deployments. Fortinet's FortiWeb 6.4 documentation describes configuration of authentication users, groups, and policies in the FortiWeb 6.4 Administration Guide; the associated configuration material is also available through the FortiWeb 6.4 documentation portal.

QUESTION NO: 4

You have created a custom attack signature on FortiWeb.

What must you do before FortiWeb can use the signature to inspect traffic?

A. Add the signature to the signature policy used by the protection profile.

B. Install the signature as a local TLS certificate.

C. Configure the signature as a server-pool health check.

D. Export the signature to FortiAnalyzer before enabling it.

ANSWER: A

Explanation:

A custom signature must be included in the signature configuration that is applied by the protection profile used in the matching server policy. Creating the signature object alone does not cause FortiWeb to inspect protected traffic with it. After the signature is enabled in the applicable signature policy and that protection profile is associated with the server policy, FortiWeb can detect matching requests and apply the configured action. See the FortiWeb 6.4 Administration Guide.

QUESTION NO: 5

Which two types of request characteristics can FortiWeb HTTP constraints validate? (Choose two.)

A. URL length

B. HTTP request body size

C. Backend server operating system version

D. Client browser bookmark count

ANSWER: A B

Explanation:

HTTP constraints can enforce limits on request characteristics such as the length of a requested URL and the size of an HTTP request body. These limits help FortiWeb reject malformed or unexpectedly large requests before they consume unnecessary application resources or reach the protected server. Values must be tuned for the application, especially where legitimate file uploads or long URLs are expected. See the FortiWeb 6.4 Administration Guide.

QUESTION NO: 6

An organization wants to observe web attacks before deploying FortiWeb inline. It can provide FortiWeb with a copy of traffic from a network switch mirror port.

Which operating mode is appropriate?

A. Transparent Inspection

B. Reverse Proxy

C. True Transparent Proxy

D. SSL offloading

ANSWER: A

Explanation:

Transparent Inspection is correct. In this mode, FortiWeb receives and analyzes a copy of traffic from a SPAN or mirror port instead of acting as an inline proxy. This enables monitoring and attack detection without changing the live client-to-server traffic path.

Because FortiWeb is not inline in Transparent Inspection mode, it cannot directly block or modify the original live request. Administrators can use the visibility obtained during this phase to tune policies before deploying an inline protection mode. See the FortiWeb 6.4 Administration Guide.

QUESTION NO: 7

Which two statements about cookie security flags are true? (Choose two.)

A. The HttpOnly attribute prevents client-side scripts from accessing the cookie.

B. The Secure attribute causes the browser to send the cookie only over HTTPS.

C. The Secure attribute encrypts the cookie value before it is stored in the browser.

D. The HttpOnly attribute prevents FortiWeb from inspecting the cookie.

ANSWER: A B

Explanation:

The **HttpOnly** cookie attribute instructs compatible browsers not to expose the cookie to client-side scripts. This reduces the risk that a script injected through a cross-site scripting vulnerability can read a session cookie. The **Secure** attribute instructs the browser to send the cookie only over HTTPS connections. FortiWeb can add applicable cookie-security attributes when it

is operating as a proxy and processing HTTP responses. See the FortiWeb 6.4 Administration Guide and MDN Web Docs: HTTP cookies.