Prepare Smart for Success Free Fortinet NSE5_FWB_AD-8.0 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 5 - FortiWeb 8.0 Administrator exam PDF questions now. Get authentic NSE5_FWB_AD-8.0 dumps packed with verified answers and secure your certification success with PrepBolt NSE5_FWB_AD-8.0 exam pdf questions and answers.

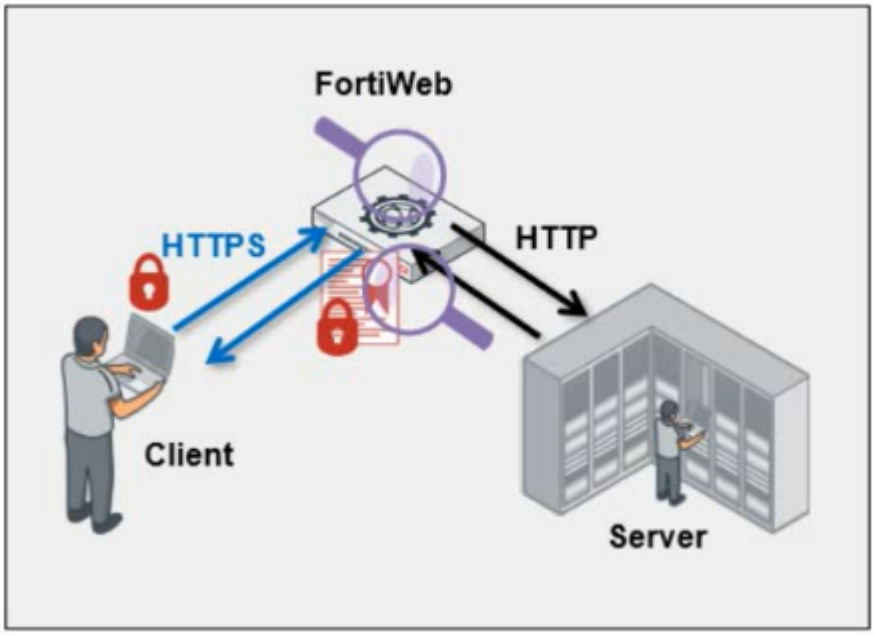
Thank you for Downloading NSE5_FWB_AD-8.0 exam PDF Demo

https://prepbolt.com/NSE5_FWB_AD-8.0.html

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



You are configuring SSL offloading on FortiWeb to protect a public-facing application. Clients connect using HTTPS, while FortiWeb forwards requests to the back-end server using HTTP.

You are reviewing certificate deployment and need to decide where to install the private key for the certificate used in client connections.

In this SSL offloading setup, which device is responsible for using the private key associated with the web server certificate?

Options:

A- FortiWeb, because it terminates the HTTPS session and decrypts traffic.
B- None. SSL offloading does not require a private key because FortiWeb only forwards traffic.
C- The server, because it always handles certificates regardless of SSL mode.
D- The client, because it initiates the TLS handshake and verifies the certificate.

Answer:

A

Explanation:

In SSL offloading, FortiWeb is the TLS endpoint for client connections. The client negotiates HTTPS with FortiWeb, not directly with the back-end web server. Therefore, FortiWeb must have the website

certificate and associated private key so it can complete the TLS handshake, decrypt inbound HTTPS traffic, inspect the HTTP content, and then forward the request to the server using HTTP or a separate back-end connection. Option B is wrong because TLS termination requires the private key. Option C describes SSL inspection or direct server termination, not offloading. Option D is wrong because clients verify the certificate but do not possess or use the server's private key. FortiWeb owns the private-key function in this design.

Question 2

Question Type: MultipleChoice

You are setting up a FortiWeb policy to protect a customer login portal. Users connect to https://login.training.lab, and you want FortiWeb to forward those requests to a load-balanced pool of back-end servers.

Which three components must you configure to complete the server policy?

Options:

A- Virtual server, server pool, and port settings (service).
B- Web application firewall (WAF) profile, DoS policy, and server name indication (SNI)-based certificate.
C- DNS resolver, URL rewrite rule, and HTTP health check.
D- Real server, IPsec tunnel, and static route.

Answer:

A

Explanation:

A FortiWeb server policy binds the listener, destination pool, and service handling required for traffic flow. The virtual server defines the public-facing listener where client traffic arrives. The server pool defines the real back-end servers or load-balanced pool where FortiWeb forwards accepted traffic. The service or port settings define whether FortiWeb handles HTTP, HTTPS, or another configured service. A WAF profile is important for security inspection, but the question asks for the three components needed to complete the forwarding policy. DNS resolver, URL rewrite, health checks, IPsec tunnels, and static routes may be useful in some deployments, but they are not the required core components of the server policy.

==========

Question 3

Question Type: DragDrop

You are configuring the FortiWeb client-side protection feature to defend against browser-based attacks.

Based on the layered defense strategy, drag and drop each control to the corresponding stage of defense.

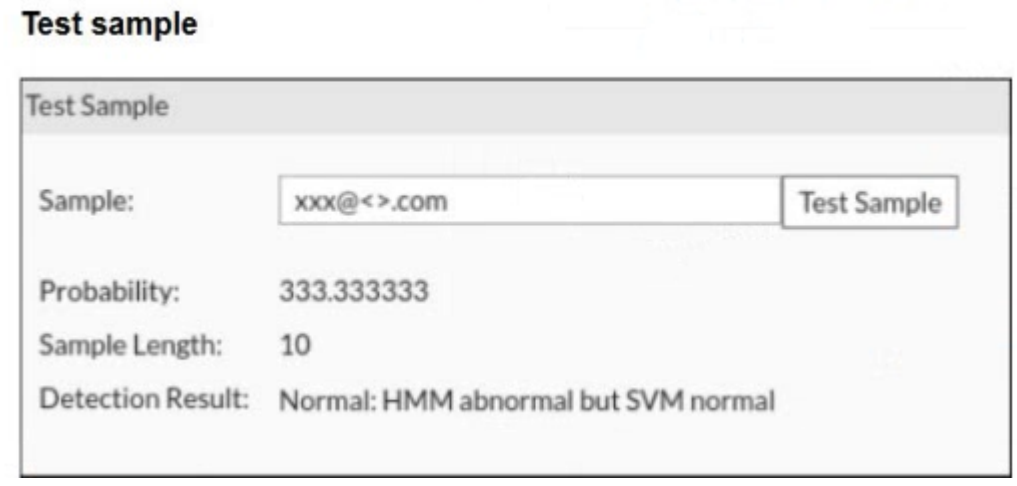
Answer:

See the Answer in the Premium Version!

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



A FortiWeb administrator tests a new form input value after training the machine learning (ML) anomaly detection system.

The hidden Markov model (HMM) flags the input as abnormal, while the support vector machine (SVM) model classifies it as normal. FortiWeb allows the request.

What does this result indicate about the FortiWeb ML anomaly detection behavior?

Options:

A- The anomaly detection thresholds are too low and must be increased.

B- One of the ML models should be disabled to avoid inconsistent results.
C- FortiWeb is correctly allowing an unusual but non-malicious input based on combined HMM and SVM evaluation.
D- FortiWeb failed to detect an attack and should have blocked the request.

Answer:

C

Explanation:

FortiWeb machine learning uses layered detection rather than treating every unusual value as malicious. The HMM layer models normal parameter behavior and can flag a value as abnormal when it falls outside the learned distribution. However, abnormal does not automatically mean hostile. FortiWeb then uses additional ML classification logic, including SVM-based evaluation, to determine whether the anomaly resembles an actual attack or simply a legitimate unusual input. In this case, HMM noticed that the value was uncommon, but SVM classified it as normal, so FortiWeb allowed the request. That is expected behavior. Raising thresholds, disabling models, or assuming FortiWeb failed would misunderstand the two-stage ML decision process.

==========

Question 5

Question Type: MultipleChoice

A FortiWeb administrator is deciding between using SAML SSO or HTML authentication. They want to minimize the number of credential prompts users receive across multiple Fortinet services.

Which statement accurately describes which option is best, and why?

Options:

A- SAML SSO, because it supports identity authentication on Fortinet devices.
B- SAML, because it blocks users from accessing anything not approved in FortiWeb policy.
C- HTML form authentication, because it's faster and doesn't need external systems.
D- HTML form, because it provides token-based access to remote services.

Answer:

A

Explanation:

SAML SSO is the correct choice when the goal is to reduce repeated credential prompts across multiple services. SAML uses a federated identity model, where users authenticate through an identity provider and then use assertions to access service providers without repeatedly entering credentials. This is exactly the value of single sign-on. HTML form authentication is more local and application-specific; it can authenticate users to a protected site, but it does not provide the same cross-service identity federation. Option B overstates SAML as a policy-blocking mechanism. Option C may be simpler but does not meet the SSO requirement. Option D incorrectly describes HTML form authentication as token-based remote-service access.

==========

Question 6

Question Type: MultipleChoice

You have configured parameter validation, file security, and machine learning (ML) anomaly detection for a web form, but some server-side request forgery tests are still succeeding. You need to advise the team on what to prioritize next to improve SSRF protection without compromising other parts of the application.

Which recommendation would best strengthen FortiWeb's ability to block remaining SSRF attempts?

Options:

A- Disable ML anomaly detection and rely solely on parameter inspection.
B- Review and refine input validation logic, as SSRF may be exploiting backend behavior or bypassing weak filters.
C- Offload all server-side request forgery (SSRF) protection to FortiGate and remove FortiWeb from the API flow.
D- Apply HTTPS inspection at the transport layer, which FortiWeb does not use to block SSRF.

Answer:

B

Explanation:

SSRF is an application-layer abuse case where attacker-controlled input causes the backend application to make unintended server-side requests. FortiWeb controls such as parameter validation, file security, and ML anomaly detection reduce risk, but SSRF often succeeds when the application accepts weakly validated URLs, hostnames, redirects, metadata endpoints, internal IP ranges, or

backend-only resources. Disabling ML would weaken protection. Moving SSRF protection to FortiGate is wrong because SSRF depends on HTTP/API logic, not only network-layer filtering. HTTPS inspection alone does not solve unsafe backend request behavior. The correct priority is to refine input validation and filtering logic so FortiWeb can better detect and block malicious URL, parameter, and backend-request patterns.

==========

Question 7

Question Type: DragDrop

You are hosting multiple secure web applications behind a single public IP address on FortiWeb.

When a client connects to a service, FortiWeb needs to:

Identify the correct SSL certificate.

Decrypt the request.

Route the request to the correct back-end server.

Match each FortiWeb function to the request handling step that performs the function.

FortiWeb function	Request handling step
Client-side connection initiation	Client sends HTTPS request with SNI field
SNI-based certificate selection	FortiWeb chooses the correct SSL certificate
SSL decryption	FortiWeb decrypts the HTTPS session
Content inspection (host and URL)	FortiWeb inspects host header and URL path
Intelligent traffic routing	FortiWeb routes request to correct back-end sever

Answer:

See the Answer in the Premium Version!

Question 8

Question Type: MultipleChoice

You need to monitor and respond to repeated suspicious activity from individual users who are accessing your web application.

Your goal is to evaluate each action the user takes and apply a response when their behavior becomes risky.

What can you configure on FortiWeb to track user behavior and respond automatically when risky activity continues?

Options:

A- Configure rate limiting on the IP reputation blocklist.
B- Add a custom signature to block suspicious URLs immediately.
C- Enable automatic cookie security under the server policy.
D- Set up scoring in the protection profile to track request behavior over time.

Answer:

D

Explanation:

The requirement is to track user behavior over time and respond when cumulative activity becomes risky. FortiWeb client management and threat scoring are built for that purpose. When enabled in the protection profile, FortiWeb can associate activity with a client, assign threat weights to suspicious behavior, and apply actions such as alerting, denying, or period blocking after a defined score threshold is exceeded. Rate limiting is useful for traffic volume, but it does not evaluate a user's full behavior pattern. A custom signature blocks a specific pattern immediately, not cumulative behavior. Cookie security protects session cookies but does not calculate behavioral risk. The correct configuration is scoring in the protection profile to track and respond to repeated risky actions.

==========

Thank You for trying NSE5_FWB_AD-8.0 PDF Demo

To try our NSE5_FWB_AD-8.0 practice exam software visit link below

https://prepbolt.com/NSE5_FWB_AD-8.0.html

Start Your NSE5_FWB_AD-8.0 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE5_FWB_AD-8.0 preparation with actual exam questions.