DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified



Technology Provider: Fortinet

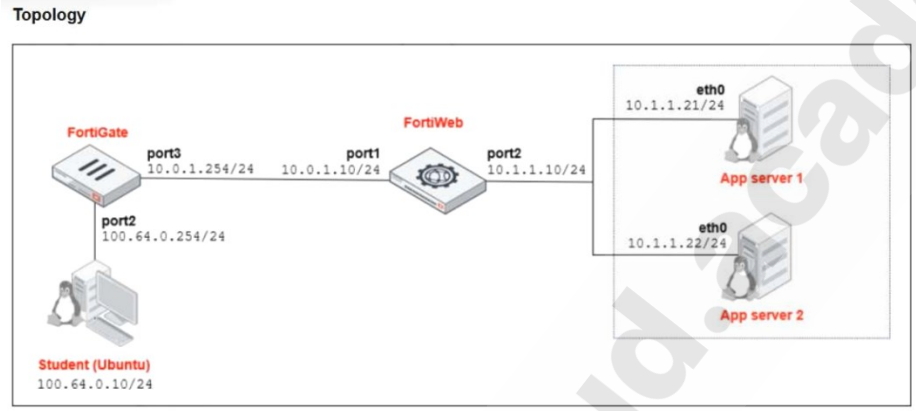
Exam: Fortinet NSE 5 - FortiWeb 8.0 Administrator

Number of questions in the database: 60

Exam Version: NOV.2026

Question #1 Topic 1

Refer to the exhibit.



You are a FortiWeb administrator. FortiWeb is deployed between a FortiGate and two back-end web servers, as shown in the diagram. No server policies are currently configured on FortiWeb. While testing, you notice that a student system in the 100.64.0.0/24 network is still able to access the back-end servers in 10.1.1.0/24, even though FortiWeb is not logging or inspecting the traffic. Which action should you take to ensure FortiWeb blocks or inspects all traffic before it reaches the back-end servers?

A. Configure FortiWeb in transparent mode to force traffic inspection.

B. Enable network address translation (NAT) mode on FortiWeb to hide the backend server IP addresses.

C. Add static routes on FortiGate to route traffic back through the FortiWeb internal interface.

D. Disable ip-forward to prevent traffic from passing through FortiWeb without a matching server policy.

Correct Answer: D

https://dbcloud.academy/

Question #2Topic 1

Which URL should you rewrite to reduce security risk?

A. https://www.example.com/25.3.6/Browse/MediaData

B. https://www.example.com/wordpress/?feed=rss2

C. https://www.example.com/products/today

D. https://www.example.com/about/team

Correct Answer: A

Question #3Topic 1

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?

A. Real server, IPsec tunnel, and static route

B. Web application firewall (WAF) profile, DoS policy, and server name indication (SNI)-based certificate

C. Virtual server, server pool, and port settings (service)

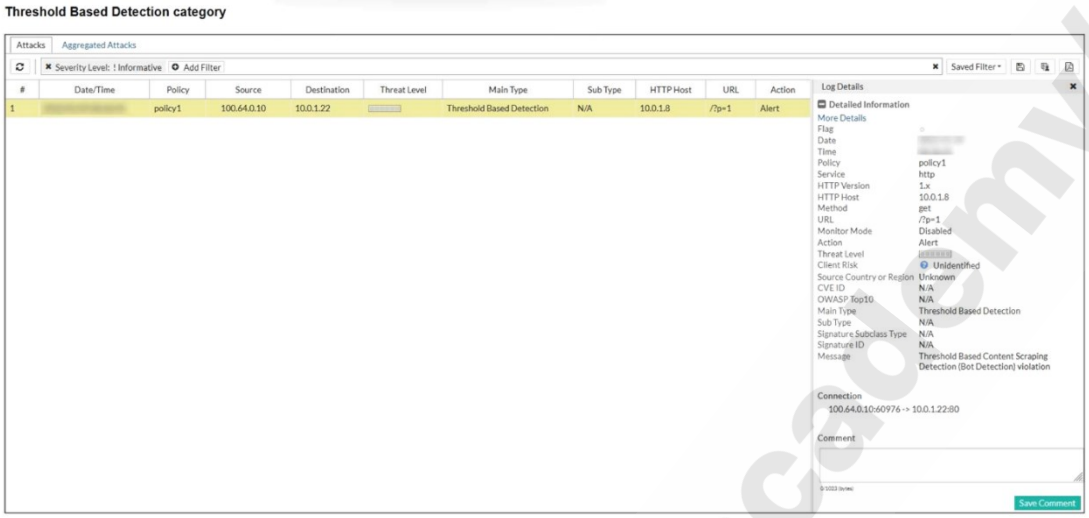
D. DNS resolver, URL rewrite rule, and HTTP health check

Correct Answer: C

https://dbcloud.academy/

Question #4*Topic 1*

Refer to the exhibit.



A FortiWeb administrator notices an alert triggered under the Threshold Based Detection category, with the message: Threshold Based Content Scraping Detection (Bot Detection) violation.
Based on the log details, what is the most likely cause of this alert?

A. An automated script or bot systematically accessing multiple pages to extract web content

B. A layer 4 SYN flood attack overwhelming the web server

C. A client sending malformed HTTP requests due to browser incompatibility

D. A vulnerability scanner triggering rate limits by simulating browser behavior

Correct Answer: A

Question #5Topic 1

Your e-commerce platform is experiencing frequent SQL injection attempts. You need FortiWeb to actively inspect, enforce, and block attacks inline before traffic reaches the web servers.

The deployment must support the full FortiWeb security feature set without operational limitations, including protocol validation, attack detection, and policy enforcement.

Which FortiWeb operation mode should you configure to proactively intercept and block threats such as SQL injection attempts?

A. Reverse proxy

B. Web Cache Communication Protocol (WCCP) integration mode

C. Transparent bridge mode

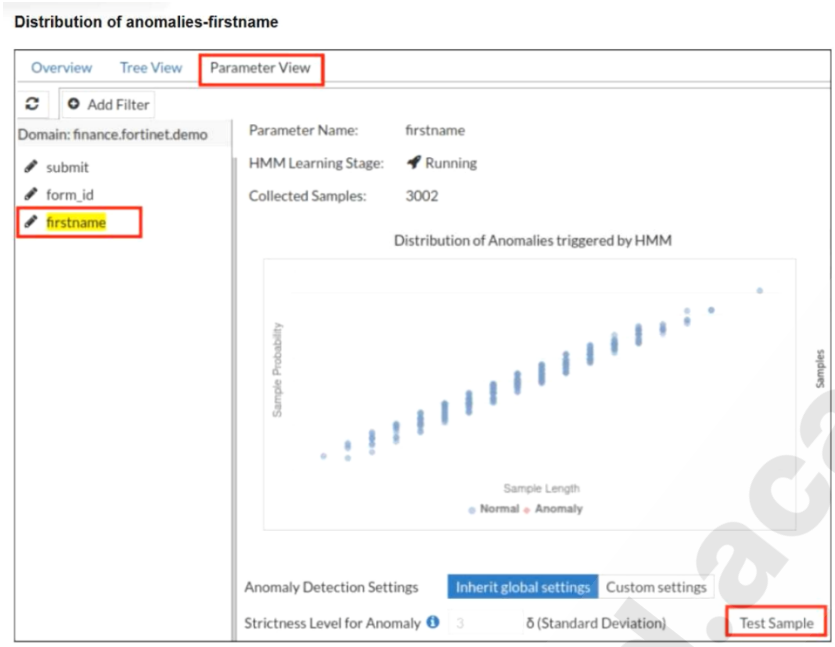
D. Offline protection

Correct Answer: A

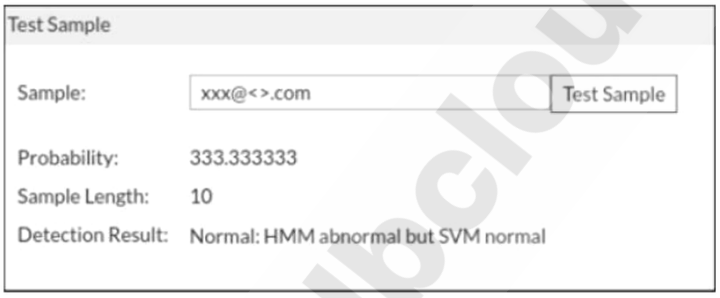
https://dbcloud.academy/

Question #6*Topic 1*

Refer to the exhibit.



Test sample



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?

A. FortiWeb is correctly allowing an unusual but non-malicious input based on combined HMM and SVM evaluation.

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

C. FortiWeb failed to detect an attack and should have blocked the request.

D. One of the ML models should be disabled to avoid inconsistent results.

Correct Answer: A

https://dbcloud.academy/

Question #7Topic 1

A third-party penetration test reveals that users can bypass login controls through a mobile API. Your current FortiWeb configuration includes zero trust network access (ZTNA) profiles and cookie security, but API protection and client management are not enabled. The security team asks you to recommend the most effective way to close this gap.

Which FortiWeb adjustment would best prevent future unauthorized API access?

A. Switch to a reverse-proxy mode to bypass cookie-based controls.

B. Enable API protection and client management to enforce identity checks on mobile API traffic.

C. Log only API traffic and rely on FortiAnalyzer for future alerts.

D. Replace ZTNA with bot protection to reduce false positives.

Correct Answer: B

Question #8Topic 1

Which statement best describes the difference between SAML authentication and HTML authentication in FortiWeb site publishing?

A. SAML authentication delegates login to an external system, while HTML authenticates directly on FortiWeb.

B. SAML authentication is used for internal apps while HTML authentication is used for cloud apps.

C. SAML authentication encrypts passwords while HTML authentication sends passwords in cleartext format.

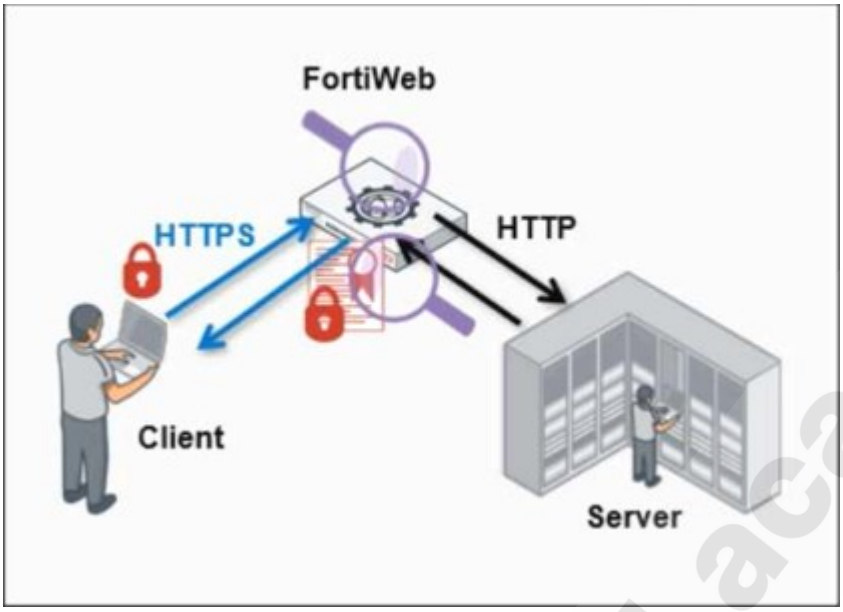
D. SAML authentication uses a passwordless login, while HTML authentication uses tokens.

Correct Answer: A

https://dbcloud.academy/

Question #9*Topic 1*

Refer to the exhibit.



You are deploying FortiWeb to handle HTTPS traffic from clients and forward cleartext traffic to a back-end server.
You want FortiWeb to decrypt the HTTPS session, inspect the traffic, and then send the traffic to the server using HTTP.
What can you configure on FortiWeb to make this behavior happen?

A. Enable reencryption on the back-end interface so the server receives HTTPS traffic.

B. Configure passive SSL inspection so FortiWeb analyzes encrypted packets without terminating SSL.

C. Configure FortiWeb to reuse the same certificate for inbound and outbound HTTPS traffic without decrypting traffic.

D. Enable SSL offloading so FortiWeb terminates the client's HTTPS session and forwards decrypted HTTP traffic to the back-end server.

Correct Answer: D

https://dbcloud.academy/