# Download Fortinet FCP_FWB_AD-7.4 Exam Dumps Free

**Shared by Nichols on 17-06-2026**

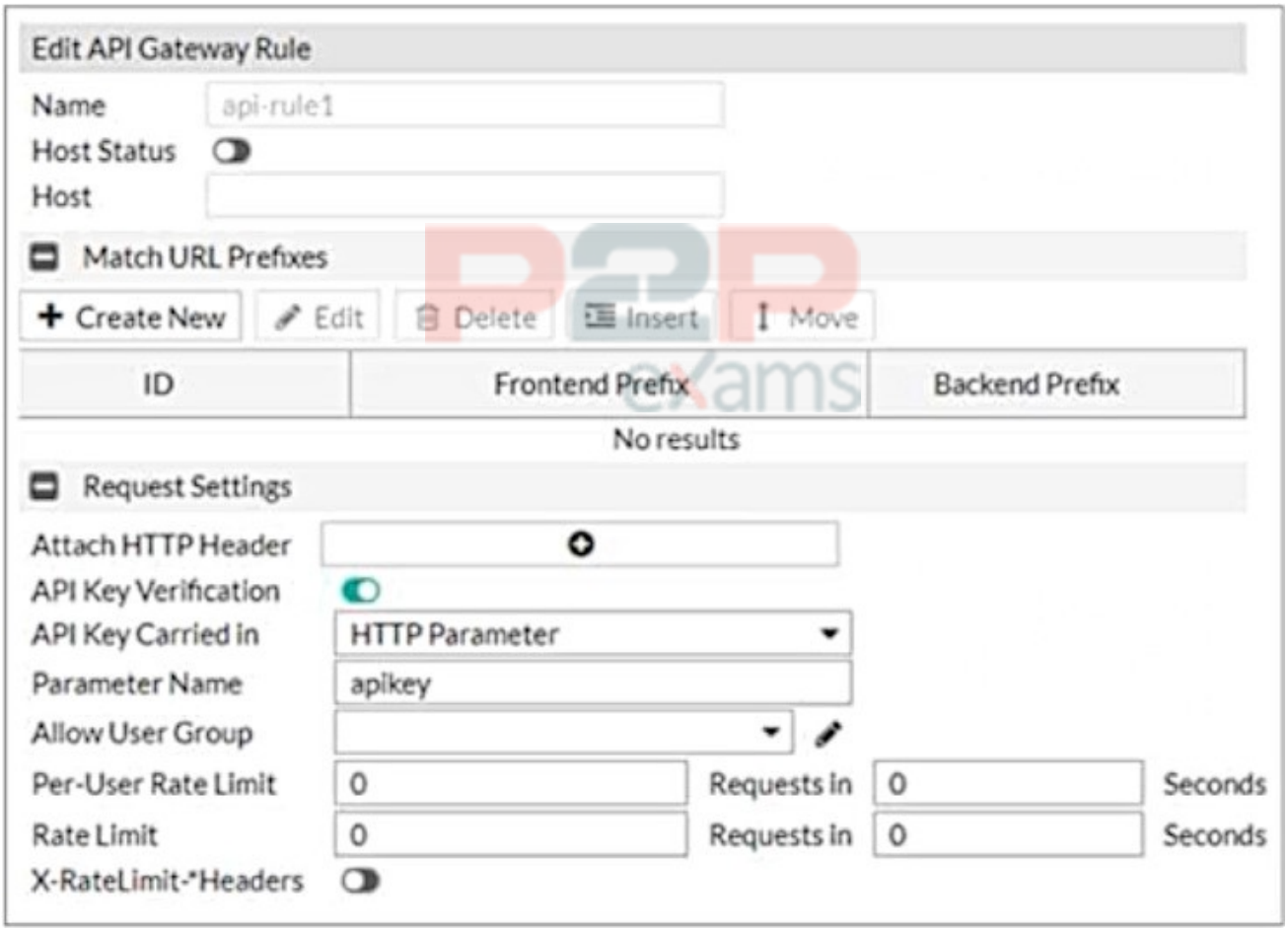
**For More Free Questions and Preparation Resources**

Check the Links on Last Page

# Question 1

Question Type: MultipleChoice

Refer to the exhibit.




What are two additional configuration elements that you must be configure for this API gateway? (Choose two.)

## Options:

A- You must define rate limits.
B- You must define URL prefixes.
C- You must select a setting in the Allow User Group field.
D- You must enable and configure Host Status.

## Answer:

A, B

## Explanation:

When configuring an API Gateway on a FortiWeb appliance, it's essential to include specific elements to ensure proper functionality and security. Two critical configuration elements are:

Defining Rate Limits: Implementing rate limits is crucial to control the number of requests a client can make to the API within a specified timeframe. This helps prevent abuse, such as denial-of-service attacks, by limiting excessive requests from clients.

Defining URL Prefixes: Specifying URL prefixes allows the FortiWeb appliance to identify and manage API requests accurately. By defining these prefixes, the appliance can route and process API calls correctly, ensuring that only legitimate traffic reaches the backend services.

These configurations align with Fortinet's best practices for setting up an API Gateway policy. While the exact steps may vary depending on the FortiWeb firmware version, the general process involves navigating to the Web Application Firewall section, selecting the API Gateway Policy tab, and configuring the necessary parameters, including rate limits and URL prefixes.

# Question 2

Question Type: MultipleChoice

What are two results of enabling monitor mode on FortiWeb? (Select two.)

## Options:

A- It does not affect denial-of-service (DoS) protection profile actions to rate limit traffic.
B- It uses the default action for all profiles and, depending on the configuration, blocks or allows traffic.
C- It does not affect any HTML rewriting or redirection actions in web protection profiles.
D- It overrides all usual profile actions. FortiWeb accepts all requests and generates alert email or log messages only for violations.

## Answer:

A, D

## Explanation:

It does not affect denial-of-service (DoS) protection profile actions to rate limit traffic: Monitor mode allows FortiWeb to monitor traffic without impacting the protection profile actions, including rate limiting in the DoS protection profiles. Traffic will still be subjected to DoS

protection actions like rate limiting, but FortiWeb will not block traffic unless a violation occurs.

It overrides all usual profile actions. FortiWeb accepts all requests and generates alert email or log messages only for violations: In monitor mode, FortiWeb will allow all traffic through and generate logs or alerts for any violations, but it will not take active actions like blocking requests or redirecting traffic. This allows you to observe the traffic patterns and potential threats without disrupting normal operations.

# Question 3

Question Type: MultipleChoice

An administrator notices multiple IP addresses attempting to log in to an application frequently, within a short time period. They suspect attackers are attempting to guess user passwords for a secure application.

What is the best way to limit this type of attack on FortiWeb, while still allowing legitimate traffic through?

## Options:

A- Blocklist any suspected IPs.
B- Configure a brute force login custom policy.
C- Rate limit all connections from suspected IP addresses.
D- Block the IP address at the border router.

## Answer:

B

## Explanation:

The best way to limit brute force login attacks on FortiWeb is to configure a brute force login custom policy. FortiWeb provides the ability to detect and mitigate brute force login attempts by automatically limiting the number of failed login attempts within a specific time period. This approach allows you to block or rate limit suspicious IP addresses while still allowing legitimate users access, based on your configuration.

# Question 4

Question Type: MultipleChoice

Which three security features must you configure on FortiWeb to protect API connections? (Choose three.)

## Options:

A- Single sign-on (SSO) authentication with Active Directory (AD)
B- Machine learning (ML)-based API protection
C- API schema validation
D- API user authentication with SAML
E- API user key enforcement

## Answer:

B, C, E

## Explanation:

Machine learning (ML)-based API protection: ML-based API protection helps detect and mitigate abnormal behavior in API traffic, such as bot attacks or abuse, by learning and adapting to normal traffic patterns.

API schema validation: API schema validation ensures that the API requests conform to the defined schema (e.g., checking the structure, fields, and types in the API calls). This helps prevent attacks like XML or JSON injection by ensuring only valid requests are processed.

API user key enforcement: Enforcing API user key authentication requires clients to provide valid API keys, ensuring only authorized users can access the API. This is crucial for controlling access to the API.

# Question 5

Question Type: MultipleChoice

Which two statements about running a vulnerability scan are true? (Choose two.)

## Options:

A- You should run the vulnerability scan during a maintenance window.
B- You should run the vulnerability scan multiple times so it can automatically update the scan parameters.
C- You should run the vulnerability scan in a test environment.
D- You should run the vulnerability scan on the live website to get accurate results.

## Answer:

A, C

## Explanation:

You should run the vulnerability scan during a maintenance window: Running a vulnerability scan during a maintenance window minimizes the risk of affecting normal operations. Scans can be resource-intensive and may cause disruptions if run during peak hours or when the system is in use.

You should run the vulnerability scan in a test environment: It is important to run the vulnerability scan in a test environment first to avoid unintended disruptions on the live system. This helps to identify potential issues or false positives without impacting production systems.

# Question 6

Question Type: MultipleChoice

Which implementation is most suited for a deployment that must meet PCI DSS compliance criteria?

## Options:

A- SSL offloading with FortiWeb in reverse proxy mode
B- SSL offloading with FortiWeb in PCI DSS mode
C- SSL offloading with FortiWeb in transparency mode
D- SSL offloading with FortiWeb in full transparent proxy mode

## Answer:

B

## Explanation:

The Payment Card Industry Data Security Standard (PCI DSS) sets forth security requirements to protect cardholder data. Requirement 6.6 specifically mandates that public-facing web applications be protected against known attacks by either:Exclusive Networks+3Gordion+3layer7solutions.com+3

Reviewing applications via manual or automated vulnerability security assessment tools or methods, at least annually and after any changes.

Installing an automated technical solution that detects and prevents web-based attacks, such as a web application firewall (WAF), in front of public-facing web applications to continually inspect all traffic.

FortiWeb, Fortinet's web application firewall, offers various deployment modes to protect web applications:

Reverse Proxy Mode: FortiWeb acts as an intermediary, terminating client sessions and initiating sessions to the backend servers. This mode provides comprehensive protection and allows for features like SSL offloading, URL rewriting, and advanced routing capabilities.

Transparent Mode: FortiWeb operates at Layer 2, inspecting traffic without modifying it, making it invisible to both clients and servers. This mode simplifies deployment as it doesn't require changes to the existing network topology.

Full Transparent Proxy Mode: Combines aspects of both reverse proxy and transparent modes, providing inspection and modification capabilities while remaining transparent to network devices.

PCI DSS Mode: A specialized deployment tailored to meet PCI DSS compliance requirements. This mode ensures that FortiWeb is configured with security policies and features aligned with PCI DSS standards, offering robust protection against threats targeting cardholder data.

Given the need to meet PCI DSS compliance criteria, deploying FortiWeb in PCI DSS mode is the most appropriate choice. This mode is specifically designed to align with PCI DSS requirements, ensuring that all necessary security measures are in place to protect cardholder data

# Question 7

Question Type: MultipleChoice

Which two items can be defined in a FortiWeb XML Protection Rule? (Choose two.)

## Options:

A- API key
B- IXML Schema
C- Web protection profile
D- Request URL

## Answer:

B, D

## Explanation:

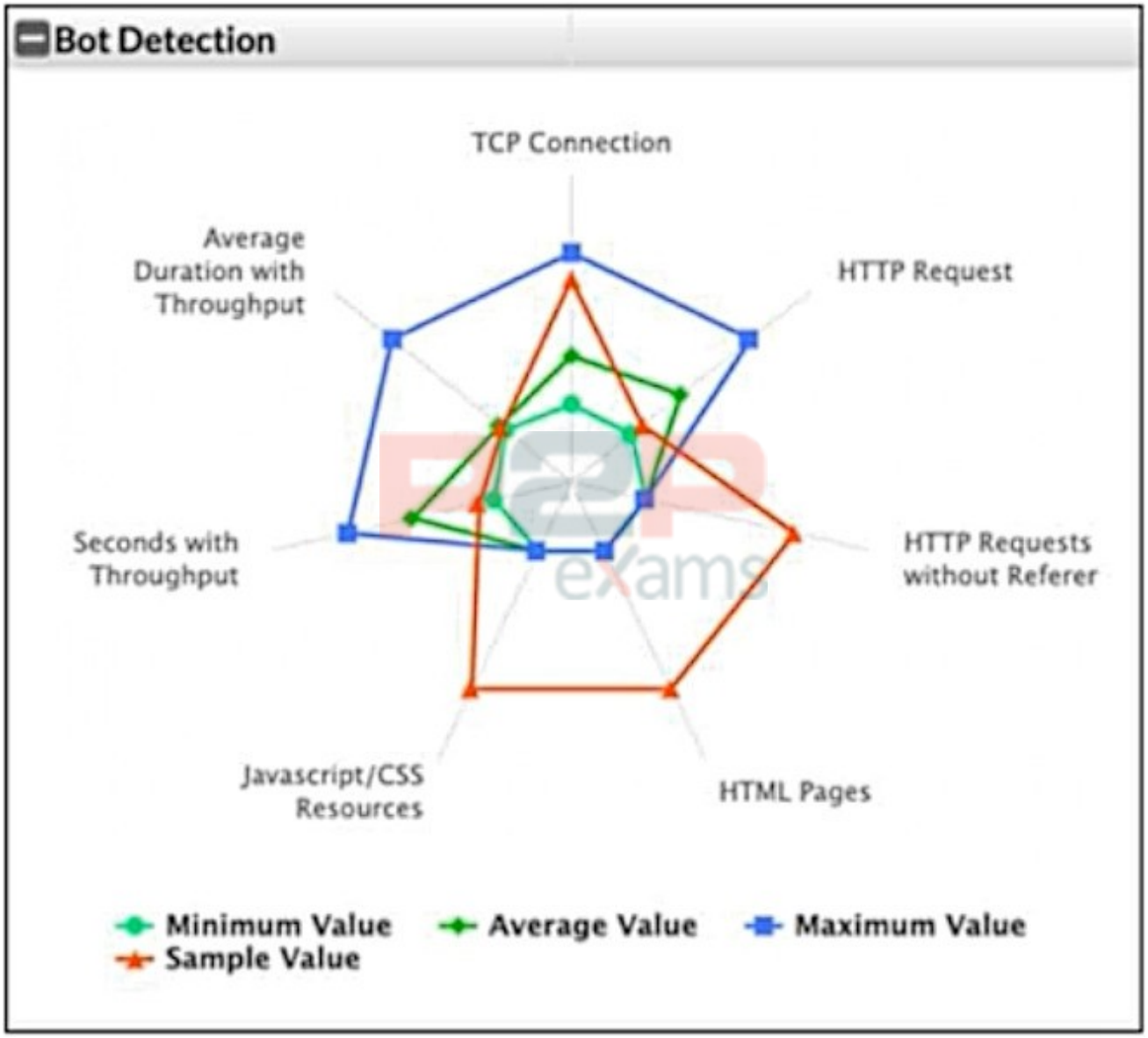
XML Schema: In FortiWeb, XML protection rules allow you to define an XML Schema to validate the structure and content of incoming XML documents. This helps protect against attacks like XML injection by ensuring that only well-formed XML requests are processed.

Request URL: You can define a request URL as part of an XML protection rule to specify the URL pattern for which the rule should apply. This allows you to apply different XML protection rules to different endpoints or resources based on the URL.

# Question 8

Question Type: MultipleChoice

Refer to the exhibit.




What can you conclude from this support vector machine (SVM) plot of a potential bot connection?

## Options:

A- The connection is normal and within the expected averages.
B- The connection uses too much bandwidth.
C- The connection uses an excessive amount of TCP connections, but is harmless.
D- The connection is possibly a bot.

## Answer:

D

## Explanation:

In the SVM plot of potential bot activity, you can see that the sample value (orange) is significantly different from the average value (green) and the maximum value (blue) in most of the metrics. This suggests unusual or abnormal behavior, indicating that the connection might be a bot. Typically, bots exhibit patterns that diverge from normal user activity, such as higher frequencies of certain types of requests, abnormal throughput, or an unusual pattern of HTTP requests (such as requests without referers or excessive TCP connections).

# Question 9

Question Type: MultipleChoice

Which high availability mode is commonly used to integrate with a traffic distributer like FortiADC?

## Options:

A- Cold standby
B- Load sharing
C- Active-Active
D- Active-Passive

## Answer:

C

## Explanation:

In Fortinet's high availability (HA) configurations, integrating FortiWeb with a traffic distributor like FortiADC is best achieved using the Active-Active HA mode. This mode allows multiple FortiWeb appliances to operate simultaneously, distributing traffic loads and enhancing both performance and redundancy.

FortiWeb supports several HA modes:

Active-Passive: One appliance actively handles all traffic, while the other remains on standby, ready to take over if the active unit fails.

Active-Active: Multiple appliances actively process traffic concurrently, sharing the load and providing redundancy.

High Volume Active-Active: An enhanced version of Active-Active, designed for environments with exceptionally high traffic volumes.

When integrating with a traffic distributor like FortiADC, the Active-Active mode is particularly advantageous. FortiADC can intelligently distribute incoming traffic across multiple active FortiWeb appliances, optimizing resource utilization and ensuring high availability. This setup not only balances the load but also provides fault tolerance; if one appliance becomes unavailable, FortiADC can redirect traffic to the remaining active units without service interruption.

This collaborative approach between FortiWeb and FortiADC ensures that web applications remain secure, performant, and resilient against failures.