Fortinet

FCP_FWB_AD-7.4 Exam

FCP - FortiWeb 7.4 Administrator

Questions & Answers
Demo

Version: 4.0

Question: 1

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

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: 2

Review the following configuration:

```
config router setting
      set ip-forward enable
end
```

What are two routing behaviors that you can expect on FortiWeb after this configuration change? (Choose two.)

A. Non-HTTP traffic routed through the FortiWeb is allowed.

B. IPv6 routing is enabled.

C. Non-HTTP traffic destined to the FortiWeb virtual server IP address is dropped.

D. Only ICMP traffic is allowed. All other traffic is dropped.

Answer: A, C

Explanation:

FortiWeb is primarily designed to handle HTTP and HTTPS traffic, protecting web applications from various threats. By default, when operating in reverse proxy mode, FortiWeb does not forward non-HTTP/HTTPS protocols to protected servers. However, administrators can configure FortiWeb to handle non-HTTP/HTTPS traffic differently using the config router setting command. This command allows enabling IP-based forwarding (routing) for non-HTTP/HTTPS traffic. When enabled, FortiWeb can route non-HTTP traffic through itself to the appropriate backend servers.

Despite this capability, any non-HTTP/HTTPS traffic that is destined directly for a FortiWeb virtual server IP address is dropped. This means that while FortiWeb can be configured to forward non-HTTP/HTTPS traffic to backend servers, it will not process non-HTTP/HTTPS traffic targeted at its own virtual server IPs.

Regarding IPv6 routing, FortiWeb does support IPv6 in various operation modes, including reverse proxy, offline inspection, and transparent inspection. However, enabling IPv6 routing requires specific configurations and is not automatically enabled by default.

Question: 3

An attacker attempts to send an SQL injection attack containing the known attack string 'root'; -- through an API call.

Which FortiWeb inspection feature will be able to detect this attack the quickest?

A. API gateway rule

B. Known signatures

C. Machine learning (ML)-based API protection—anomaly detection

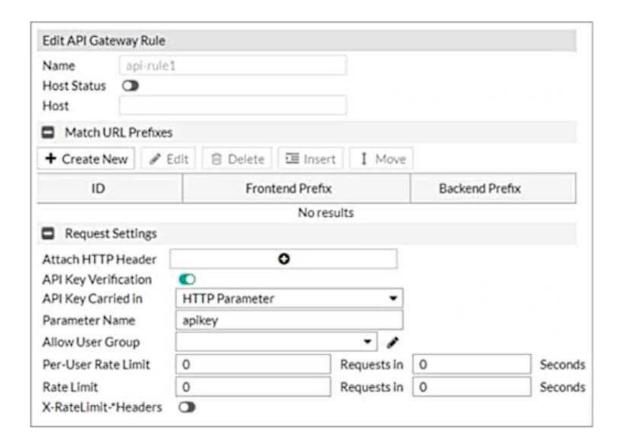D. ML-based API protection—threat detection

Answer: B

Explanation:

The quickest detection for an SQL injection attack like the one described ('root'; --) would be through known signatures. FortiWeb utilizes signature-based detection to match incoming traffic against predefined attack patterns. Since SQL injection attacks are commonly known and have specific patterns (such as 'root'; --), known signatures would immediately recognize and flag this type of attack.

Question: 4

Refer to the exhibit.

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

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.