ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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

A. SSL ofloading with FortiWeb in reverse proxy mode

B. SSL ofloading with FortiWeb in PCI DSS mode

C. SSL ofloading with FortiWeb in transparency mode

D. SSL ofloading 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 ofloading, 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, ofline 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

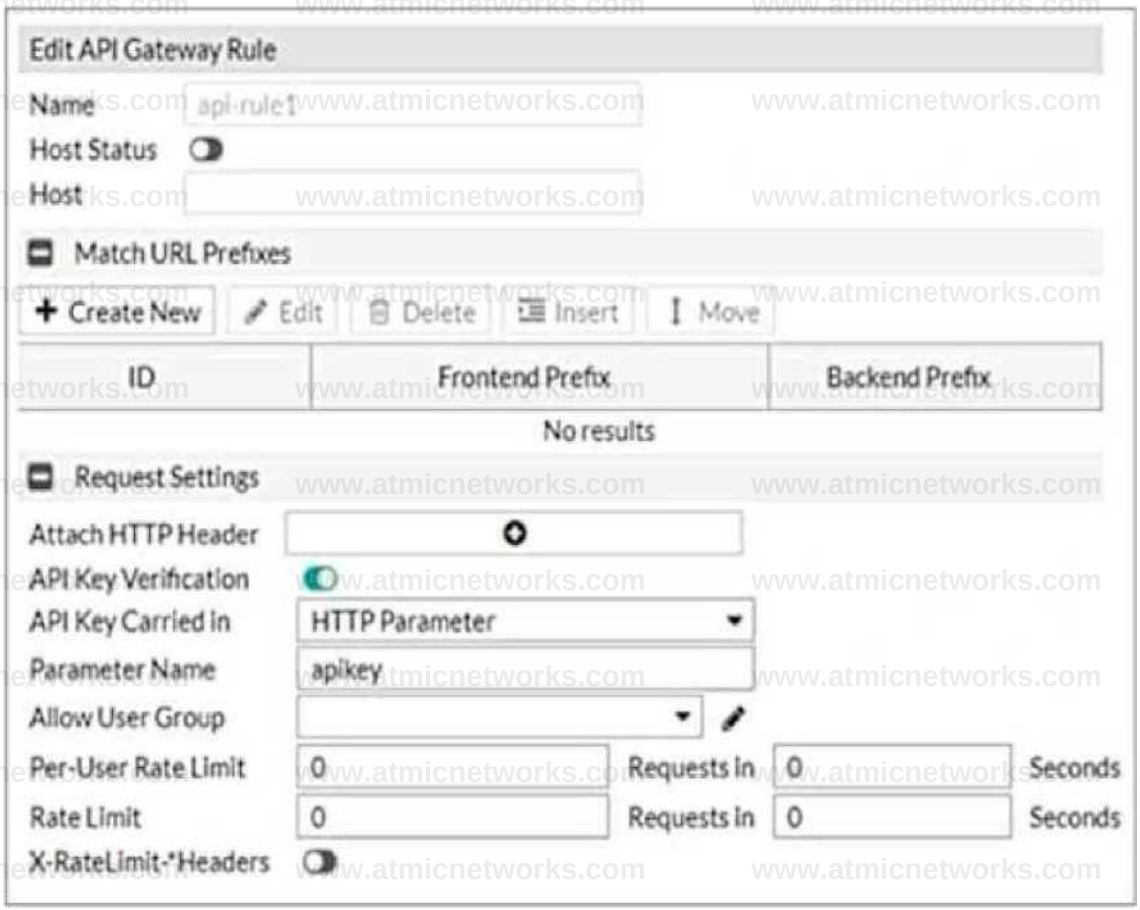
Answer: B

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.

Question: 5

Which would be a reason to implement HTTP rewriting?

A. To redirect HTTP to HTTPS.

B. To implement load balancing.

C. To replace a vulnerable element in a requested URL.

D. The original page has moved to a new URL.

Answer: A

Explanation:

HTTP rewriting is a feature in FortiWeb that allows administrators to modify HTTP requests and responses for various purposes, including security enhancements, user experience improvements, and application functionality. One common use case for HTTP rewriting is to redirect HTTP traffic to HTTPS, ensuring that all communications between clients and the server are encrypted and secure.

Explanation of Options:

A . To redirect HTTP to HTTPS: This is a valid reason to implement HTTP rewriting. By rewriting incoming HTTP requests to HTTPS, administrators can enforce secure connections, protecting data integrity and confidentiality. FortiWeb supports this functionality, allowing seamless redirection from HTTP to HTTPS.

B . To implement load balancing: Load balancing is not typically achieved through HTTP rewriting. Instead, it involves distributing network traffic across multiple servers to ensure availability and reliability. FortiWeb provides load balancing features, but these are separate from HTTP rewriting capabilities.

C . To replace a vulnerable element in a requested URL: While HTTP rewriting can modify URLs, its primary purpose is not to replace vulnerable elements within URLs. Addressing vulnerabilities typically involves input validation, sanitization, and other security measures rather than rewriting URLs.

D . The original page has moved to a new URL: This is another valid reason to implement HTTP rewriting. When a webpage's URL changes, rewriting rules can redirect requests from the old URL to the new one, ensuring users can still access the content without encountering errors.

In summary, both options A and D are correct reasons to implement HTTP rewriting. However, in the context of FortiWeb's functionalities, redirecting HTTP to HTTPS (option A) is a common and significant use case, as it enhances security by ensuring encrypted connections.

Question: 6

What is the difference between an API gateway protection schema and a machine learning (ML) API protection schema?

A. An API gateway protection schema does not allow authentication.

B. An API gateway protection schema handles response bodies.

C. An API gateway protection schema supports data types other than string.

D. An API gateway protection schema cannot change without administrator intervention.

Answer: C

Explanation:

In FortiWeb's API protection mechanisms, there are distinctions between the traditional API gateway protection schema and the machine learning (ML) based API protection schema:

Data Type Support: The API gateway protection schema has the capability to support various data types beyond just strings, allowing for more comprehensive validation and enforcement of API schemas.

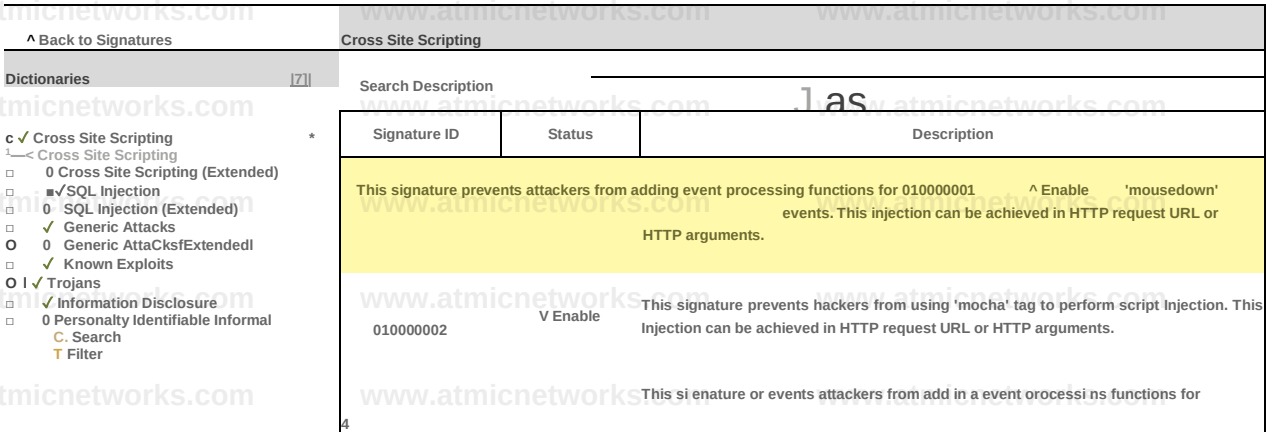
Schema Adaptability: The ML-based API protection schema is designed to automatically learn and adapt to changes in the API structure without requiring manual intervention from administrators. This dynamic learning process enables FortiWeb to identify and

protect against anomalies and potential threats in real-time.

Question: 7

Refer to the exhibits.

Signature details



Signature exception

Signature ID: 010000001
Match Sequence: (1)

Exception Threat Weight

+ Create Nev/ / Edit 8 Delete ^ Insert

ID	Element Type	Name	Value	Operation
1	Full URL		http:\A/my\.blog\.orgVuserl\/	00

What will happen when a client attempts a mousedown cross-site scripting (XSS) attack against the site http://my.blog.org/userl1/blog.php and FortiWeb is enforcing the highlighted signature?

A. The connection will be stripped of the mousedown JavaScript code.

B. The connection will be blocked as an XSS attack.

C. FortiWeb will report the new mousedown attack to FortiGuard.

D. The connection will be allowed.

Answer: D

Explanation:

In the provided configuration, the signature exception has been set for the URL http://my.blog.org/user1V. This means that any request to this specific URL will bypass the signature ID 01000001, which is designed to block cross-site scripting (XSS) attacks using the mousedown event. As the request comes from the URL http://my.blog.org/userl1/blog.php, which does not match the exception rule for http://my.blog.org/user1V, the attack will be allowed through.

Therefore, the connection will be allowed because the exception rule bypasses protection for the specified URL.

Question: 8

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

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.

Question: 9

A customer wants to be able to index your websites for search and advertisement purposes.

What is the easiest way to allow this on a FortiWeb?

A. Add the indexer IP address to the trusted IP list on the FortiWeb.

B. Add the indexer IP address to the FortiGuard "Known Search Engines" category.

C. Create a firewall rule to bypass the FortiWeb entirely for the indexer IP address.

D. Do not allow any external sites to index your websites.

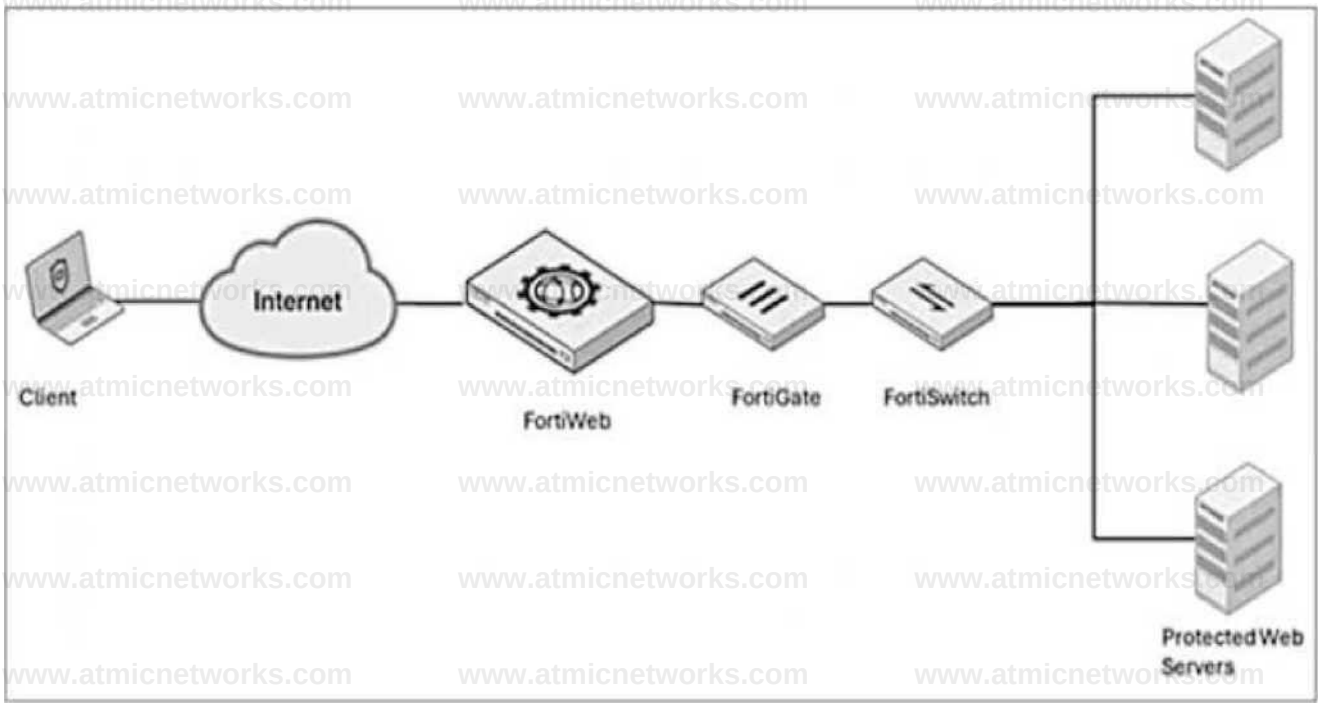
Answer: A

Explanation:

The easiest way to allow a search engine indexer (such as Googlebot or Bingbot) to index your website on a FortiWeb is to add the indexer's IP address to the trusted IP list. This ensures that traffic from trusted indexers is allowed through without being blocked or interfered with by FortiWeb's security features like bot protection.

Question: 10

Refer to the exhibit.



A FortiWeb device is deployed upstream of a device performing source network address translation (SNAT) or load balancing.

What configuration must you perform on FortiWeb to preserve the original IP address of the client?

A. Enable and configure the Preserve Client IP setting.

B. Use a transparent operating mode on FortiWeb.

C. Enable and configure the Add X-Forwarded-For setting.

D. Turn off NAT on the FortiWeb.

Answer: A

Explanation:

When FortiWeb is deployed upstream of a device performing source network address translation (SNAT) or load balancing, the original client IP address may be lost. To preserve the original client IP address, you must enable and configure the Preserve Client IP setting on FortiWeb. This allows FortiWeb to retain and pass the client's original IP address to the backend servers for accurate

logging and processing.

Question: 11

Refer to the exhibit.

Attack ID 20000010 is brute force logins.

Which statement is accurate about the potential attack?

A. The attacker has successfully retrieved the credentials to www.example.com.

B. www.example.com is running attacks against the client 192.168.1.11.

C. The attack has happened 10 times.

D. 192.168.1.11 is sending suspicious traffic to FortiWeb.

Answer: D

Explanation:

The Attack ID of 20000010 refers to a brute force login attempt, which typically indicates that the client IP (192.168.1.11) is sending suspicious or malicious traffic to the FortiWeb. FortiWeb detected and blocked this suspicious activity, which is why the page is shown as blocked.

Question: 12

Which three stages are part of creating a machine learning (ML) bot detection algorithm? (Choose three.)

A. Model building

B. Model running

C. Model verification

D. Sample collecting

E. Model Bayesian analysis

Answer: A, C, D

Explanation:

Model building: In this stage, you design and develop the ML model, which involves selecting appropriate algorithms and features to detect bot activity.

Model verification: This is where you test and evaluate the model's performance to ensure it can accurately detect bots without false positives or negatives.

Sample collecting: Gathering relevant data samples (e.g., bot and non-bot traffic) to train the machine learning model is crucial to ensure it can learn from various scenarios.

Question: 13

Under which two circumstances does FortiWeb use its own certificates? (Choose two.)

A. Connecting to browser clients using SSL

B. Making a secondary HTTPS connection to a server where FortiWeb acts as a client

C. Routing an HTTPS connection to a FortiGate

D. An administrator session connecting to the GUI using HTTPS

Answer: B, D

Explanation:

Making a secondary HTTPS connection to a server where FortiWeb acts as a client: When FortiWeb needs to connect to an external server via HTTPS (acting as a client), it may use its own certificates for that connection.

An administrator session connecting to the GUI using HTTPS: FortiWeb uses its own certificates to secure the HTTPS connection between the administrator and the FortiWeb GUI. This ensures secure access for management purposes.

Question: 14

You are using HTTP content routing on FortiWeb. You want requests for web application A to be forwarded to a cluster of web servers, which all host the same web application. You want requests for web application B to be forwarded to a different, single web server.

Which statement regarding this solution is true?

A. You must chain policies so that all requests go to the virtual server for policy A first, and then redirect requests for web application B to go to the virtual server for policy B

B. You must create static routes on the FortiWebto allow these requests.

C. You must put the single web server for application B into a server pool and use it with HTTP content routing.

D. The server policy always applies the same web protection profile to both web application A and web application B.

Answer: C

Explanation:

To forward requests for web application B to a single web server, you would configure FortiWeb to use HTTP content routing and create a server pool specifically for web application B. In FortiWeb, server pools are used to group servers together based on application requirements, and you can configure the pool to contain only a single web server for application B.

Question: 15

What can a FortiWeb administrator do if a client has been incorrectly period blocked?

A. Allow the period block to expire on its own, you cannot override it.

B. Manually release the IP address from the blocklist.

C. Disable and re-enable the server policy.

D. Force a new IP address to the client.

Answer: B

Explanation:

If a client has been incorrectly blocked due to a period block, the FortiWeb administrator can manually release the IP address from the blocklist. This allows the client to access the application again before the block expires naturally.

Question: 16

Which two functions does the first layer of the FortiWeb anomaly machine learning (ML) analysis mechanism perform? (Choose two.)

A. Determines whether an anomaly is a real attack or just a harmless anomaly that should be ignored

B. Determines a probability model behind every parameter and HTTP method passing through FortiWeb

C. Determines whether traffic is an anomaly, based on observable features overtime

D. Determines if a detected threat is a false-positive or not

Answer: B, C

Explanation:

The first layer of the FortiWeb anomaly machine learning (ML) analysis mechanism focuses on analyzing traffic and creating a probability model for parameters and HTTP methods to detect potential anomalies. It also assesses traffic patterns over time to determine whether certain behavior is anomalous. These functions are key to understanding and classifying traffic before further analysis is done.

Question: 17

Which is an example of a cross-site scripting (XSS) attack?

A. SELECT username FROM accounts WHERE username='admin';-- ' AND password='password';

B. <img src="http://badfile/nothere" onerror=alert(document.cookie);>

C. SELECT username FROM accounts WHERE username='XSS' ' AND password='alert("http://badurl.com")';

D. <IMG SRC="xss.png">

Answer: B

Explanation:

Cross-Site Scripting (XSS) is a type of web security vulnerability that allows attackers to inject malicious scripts into web pages viewed by users. This can lead to session hijacking, credential theft, or redirection to malicious sites. XSS attacks typically exploit vulnerabilities in web applications that fail to properly sanitize user input.

Here's an analysis of the given options:

A . SELECT username FROM accounts WHERE username='admin';-- ' AND password='password';

This is an example of SQL Injection (SQLi) rather than XSS. It manipulates SQL queries to bypass authentication, not execute JavaScript in a user's browser.

B . <img src="http://badfile/nothere" onerror=alert(document.cookie);>

This is a classic XSS attack.

It uses an <img> tag with a non-existent src attribute.

The onerror event triggers when the image fails to load, executing alert(document.cookie);, which can expose session cookies.

This method is commonly used for stealing cookies or executing arbitrary scripts.

C . SELECT username FROM accounts WHERE username='XSS' ' AND password='alert("http://badurl.com")';

This is neither a valid SQL injection nor a valid XSS attack.

The syntax suggests an incorrect SQL query rather than JavaScript execution in a browser.

D . <IMG SRC="xss.png">

This is not a valid XSS attack unless there is an additional event handler like onload, onerror, or onmouseover executing JavaScript.

By itself, it just loads an image and does not execute any malicious script.

Thus, Option B is the correct answer as it represents a real-world XSS attack technique.

Reference:

OWASP XSS Guide: https://owasp.org/www-community/attacks/xss/

Fortinet XSS Protection Documentation: https://docs.fortinet.com/

Question: 18

Which Layer 7 routing method does FortiWeb support?

A. URL policy routing

B. OSPF

C. BGP

D. HTTP content routing

Answer: D

Explanation:

FortiWeb is a Web Application Firewall (WAF) designed to protect web applications from various threats. Among its features, FortiWeb supports Layer 7 routing methods, which operate based on the content of the HTTP/HTTPS traffic.

HTTP Content Routing refers to the capability of directing incoming web traffic to specific backend servers based on characteristics found within the HTTP requests, such as URL paths, headers, or other content. This allows for more granular and efficient distribution of traffic, ensuring that requests are handled by the appropriate servers based on their content.

Analysis of Options:

A . URL policy routing: While this term suggests routing decisions based on URL policies, it is not a standard term used in FortiWeb's documentation. FortiWeb's content routing encompasses URLbased decisions, making this option less precise.

B . OSPF (Open Shortest Path First): This is a Layer 3 routing protocol used for IP routing within an Autonomous System. It operates at the network layer and is not related to Layer 7 routing methods.

C . BGP (Border Gateway Protocol): Another Layer 3 routing protocol, BGP is used for routing between Autonomous Systems on the internet. It does not pertain to Layer 7 or application-layer routing.

D . HTTP content routing: This aligns with FortiWeb's capabilities to make routing decisions based on the content of HTTP requests, such as URL paths, headers, or other application-layer data. This is a Layer 7 routing method supported by FortiWeb.

Therefore, the correct answer is D. HTTP content routing.

Reference:

FortiWeb 7.2.6 Administration Guide: "FortiWeb provides advanced Layer 7 load balancing and authentication ofload services." cloud.orange-business.com

FortiWeb Data Sheet: "FortiWeb provides advanced Layer 7 load balancing and authentication ofload services." Exclusive Networks

FortiWeb on OCB-FE - Installation and Deployment Guide: "FortiWeb provides advanced Layer 7 load balancing and authentication ofload services." cloud.orange-business.com

These references confirm that FortiWeb supports HTTP content routing as a Layer 7 routing method.

Question: 19

Which command will enable debugging for the FortiWeb user tracking feature?

A. debug enable user-tracking 7

B. diagnose debug application user-cracking 7

C. debug application user-cracking 7

D. diagnose debug enable user-cracking 7

Answer: B

Explanation:

To enable debugging for the user tracking feature in FortiWeb, you would use the command diagnose debug application user-tracking 7. This command enables debugging for the user-tracking application and sets the debug level to 7, providing detailed logs for troubleshooting.

Question: 20

Refer to the exhibit.

```
FortiWeb ³ diagnose system flash list
have 4 partitions
Image# Version                          TotalSize(KB) Us
1      FV-KVH-6.4.0-build1444-210629    371048          21
2      FV-KVM-6.4.1-build1464-210903    371048          21
3      2021-09-28 10:37                 92760           52

FortiWeb #
```

What is true about this FortiWeb device? (Choose two.)

A. It has 41% of the disk available for logging.

B. It was upgraded to a different version after initial installation.

C. It is currently running version 6.4.0.

D. It is currently running version 6.4.1.

Answer: B

Explanation:

It was upgraded to a different version after initial installation: The device has multiple partitions with different firmware versions (6.4.0 and 6.4.1), indicating that it was upgraded after the initial installation from version 6.4.0 to 6.4.1.

Question: 21

Which high availability (HA) mode uses gratuitous Address Resolution Protocol (ARP) to advertise a failover event to neighboring network devices?

A. Passive-Passive
B. Active-Passive
C. Active-Active
D. Passive-Active

Answer: B

Explanation:

In Active-Passive high availability (HA) mode, the active unit is responsible for handling traffic while the passive unit remains idle, ready to take over in case of a failure. When a failover occurs, the active unit sends out gratuitous ARP messages to notify neighboring devices about the change in the active unit's IP address. This ensures that the network devices update their ARP tables and can forward traffic to the new active unit.

Question: 22

In SAML deployments, which server contains user authentication credentials (username/password)?

A. Identity provider
B. Service provider
C. User database
D. Authentication client

Answer: A

Explanation:

In SAML (Security Assertion Markup Language) deployments, the Identity Provider (IdP) is responsible for storing and managing user authentication credentials, such as usernames and passwords. The IdP authenticates the user and then issues a SAML assertion to the Service Provider (SP), which allows the user to access services without needing to re-enter credentials.

Question: 23

What are two possible impacts of a DoS attack on your web server? (Choose two.)

A. The web application starts accepting unencrypted traffic.

B. The web application is unable to accept any more connections because of network socket exhaustion.

C. The web application server is unable to accept new client sessions due to memory exhaustion.

D. The web application server database is compromised with data theft.

Answer: B, C

Explanation:

The web application is unable to accept any more connections because of network socket exhaustion: A Denial of Service (DoS) attack often floods the web server with an overwhelming number of requests, leading to network socket exhaustion. This can prevent the server from accepting new legitimate connections, effectively disrupting service.

The web application server is unable to accept new client sessions due to memory exhaustion: DoS attacks can consume a significant amount of server memory, causing memory exhaustion. This results in the web application being unable to accept new client sessions or handle requests properly.

Question: 24

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

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: 25

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

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: 26

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?

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: 27

Review the following configuration:

```
config waf ma.chine—learning—policy edit 1

        set sainple-limit-by-ip 0 next

end
```

Which result would you expect from this configuration setting?

A. When machine learning (ML) is in its running phase, FortiWeb will accept a set number of samples from the same source IP address.

B. When ML is in its running phase, FortiWeb will accept an unlimited number of samples from the same source IP address.

C. When ML is in its collecting phase, FortiWeb will accept an unlimited number of samples from the same source IP address.

D. When ML is in its collecting phase, FortiWeb will not accept any samples from any IP addresses.

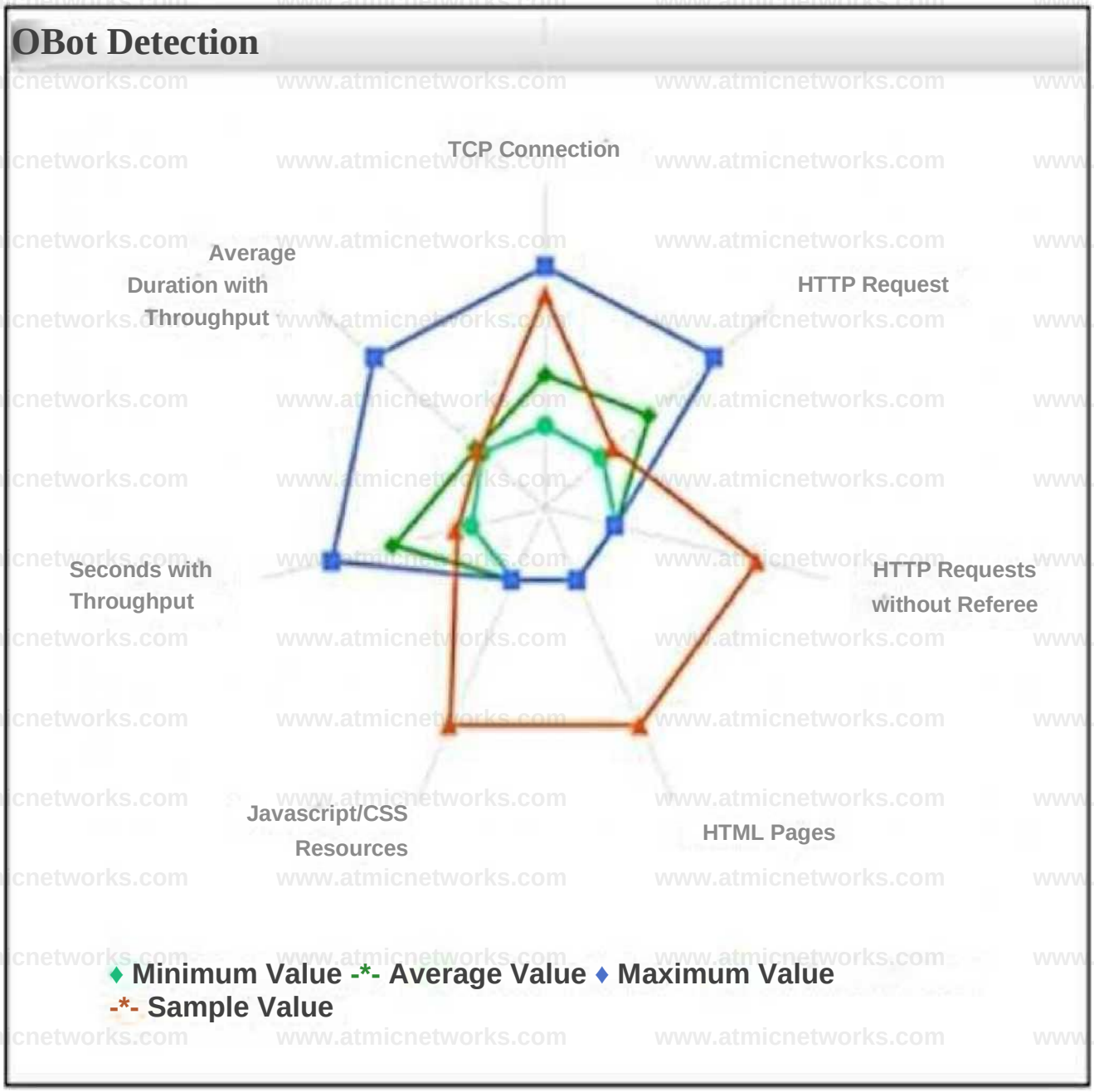
Answer: B

Explanation:

In the configuration, the command set sample-limit-by-ip 0 disables the sample limit for any specific IP address. This means that during the machine learning (ML) running phase, FortiWeb will not limit the number of samples it accepts from the same IP address. Setting this to 0 effectively removes any restrictions on the number of samples from a given IP address.

Question: 28

Refer to the exhibit.



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

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: 29

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

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: 30

Which two objects are required to configure a server policy in reverse proxy mode without content routing? (Choose

two.)

A. Site publishing

B. Protected hostname

C. Virtual server

D. Server pool

Answer: B, C

Explanation:

Protected hostname: In reverse proxy mode, the protected hostname refers to the domain or hostname that FortiWeb will protect. It specifies which hostname FortiWeb is acting as a reverse proxy for, and is required for the server policy configuration.

Virtual server: A virtual server is a logical representation of a web server that FortiWeb handles. It's required to configure how traffic is routed to the protected resources in reverse proxy mode.

Question: 31

When is it possible to use a self-signed certificate, rather than one purchased from a commercial certificate authority?

A. If you are an enterprise whose employees use only mobile devices

B. If you are a small business or home office

C. If you are an enterprise whose computers all trust the active directory or CA server that signed the certificate

D. If you are an enterprise whose resources do not need security or https connections

Answer: C

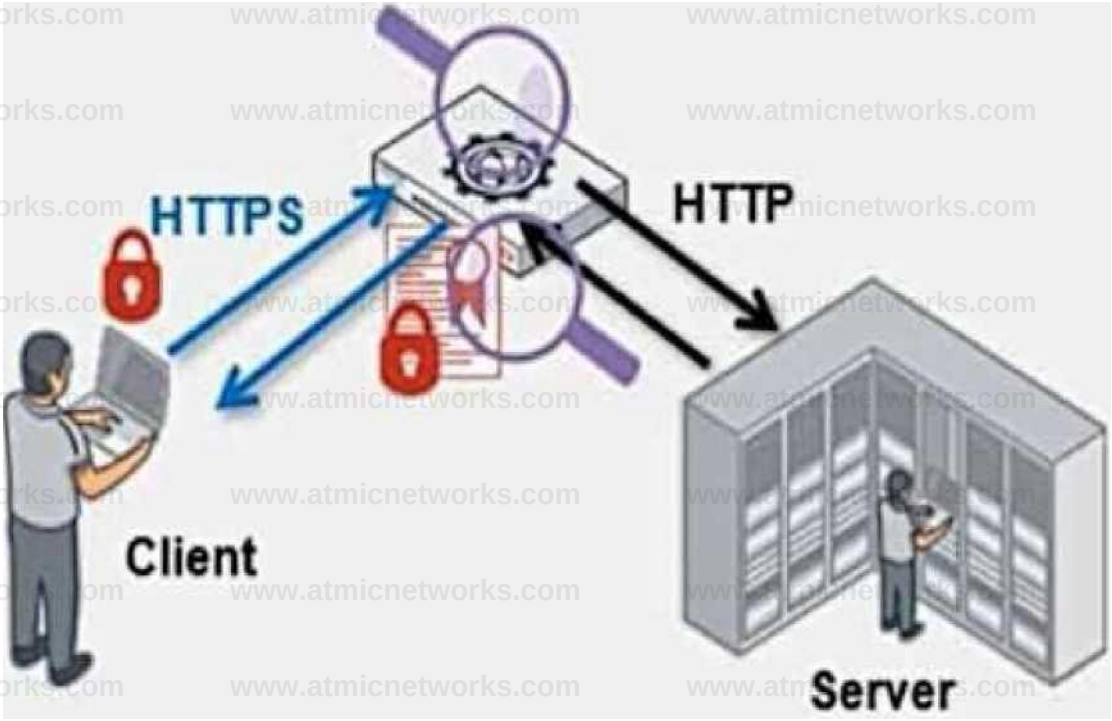
Explanation:

A self-signed certificate is useful when all the devices in your network can be configured to trust it. In this case, if your enterprise's computers trust the internal Active Directory or Certificate Authority (CA) server that signed the certificate, the self-signed certificate can be used internally for HTTPS connections without raising trust issues.

Question: 32

Refer to the exhibit.

FortiWeb



Which statement is true?

A. FortiWeb cannot perform content inspection on the traffic because it is encrypted.

B. FortiWeb is decrypting and re-encrypting the traffic.

C. The server is not performing any cryptography on the traffic.

D. The server is encrypting traffic being sent to the client.

Answer: B

Explanation:

In the diagram, FortiWeb is positioned between the client and the server, handling encrypted HTTPS traffic from the client and sending unencrypted HTTP traffic to the server. This indicates that FortiWeb is performing SSL ofloading, which means it is decrypting the HTTPS traffic from the client, inspecting it, and then re-encrypting the traffic before forwarding it to the server.

Question: 33

How are bot machine learning (ML) models different from API or anomaly detection models?

A. Bot ML models analyze multiple connections overtime instead analyzing each connection as a single unit.

B. Bot ML models detect only anomalies and not actual threats.

C. Bot ML models inspect more types of connection properties.

D. Bot ML models do not update models periodically from new data.

Answer: A

Explanation:

Bot ML models analyze multiple connections over time instead of analyzing each connection as a single unit: This is the key distinction. Bot ML models focus on analyzing patterns over a period of time, looking at behavioral patterns across multiple requests or connections from the same source to identify potential bot activity. Unlike traditional anomaly detection or API models that may focus on single connections or individual transactions, bot detection typically examines aggregated behavior to identify patterns indicative of bots, such as high-frequency requests or unusual traffic flows.

Question: 34

In which two operating modes can FortiWeb modify HTTP packets? (Choose two.)

A. True transparent proxy

B. Virtual proxy

C. Transparent inspection

D. Reverse proxy

Answer: B, D

Explanation:

Virtual proxy: In virtual proxy mode, FortiWeb acts as an intermediary between clients and the server, and it can modify HTTP packets. It performs various security checks, such as inspecting and filtering HTTP traffic before forwarding it to the web server.

Reverse proxy: In reverse proxy mode, FortiWeb sits between the client and the server, handling incoming requests from clients, modifying or inspecting HTTP packets as needed, and forwarding them to the backend servers.

Question: 35

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

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:

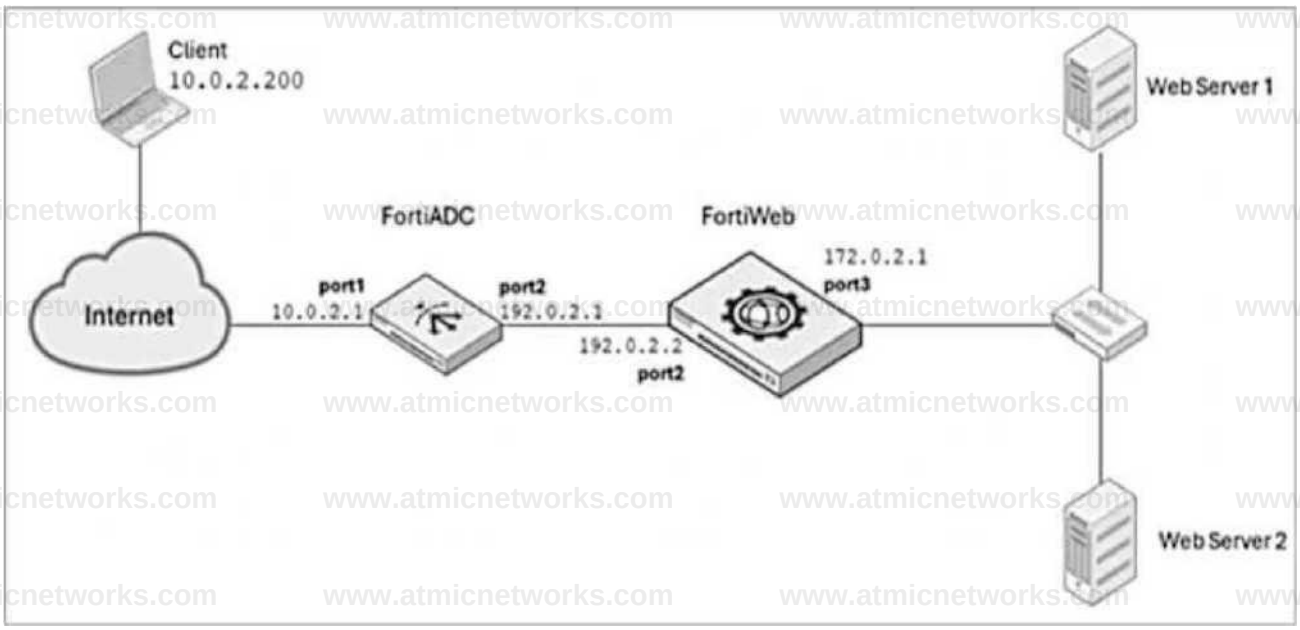
Machine learning (ML)-based API protection: ML-based API protection helps detect and mitigate abnormal behavior in API traffic, such as bot attacks or abuse, by learning and adapting to normal traffic patterns.

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: 36

Refer to the exhibit.



FortiADC is applying SNAT to all inbound traffic going to the servers.
When an attack occurs, FortiWeb blocks traffic based on the 192.0.2.1 source IP address, which belongs to FortiADC. This setup is breaking all connectivity and genuine clients are not able to access the servers.

What can the administrator do to avoid this problem? (Choose two.)

A. Enable and configure the Preserve Client IP setting on the client.

B. No special configuration is required; connectivity will be re-established for all clients after the set timeout.

C. Place FortiWeb in front of FortiADC.

D. Enable and configure the Use X-Forwarded-For setting on FortiWeb.

Answer: C, D

Explanation:

Place FortiWeb in front of FortiADC: This configuration change places FortiWeb between the client and FortiADC, so that FortiWeb can directly inspect and protect the incoming traffic before FortiADC applies SNAT (Source Network Address Translation). By placing FortiWeb in front, it will have access to the real client IP addresses, and it will be able to properly identify and handle attack traffic without blocking legitimate client traffic.

Enable and configure the Use X-Forwarded-For setting on FortiWeb: This setting allows FortiWeb to extract the original client IP address from the X-Forwarded-For header in the HTTP request, which is inserted by FortiADC when performing SNAT. With this setting enabled, FortiWeb will be able to block traffic based on the original client IP address rather than the SNATed IP address (192.0.2.1), preserving the accuracy of the security measures.