Fortinet.FCP_FWB_AD-7.4.by.Wick.20q

Number: FCP_FWB_AD-7.4
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: FCP_FWB_AD-7.4

Exam Name: FCP - FortiWeb 7.4 Administrator

Exam A

QUESTION 1
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.

Correct Answer: A
Section:
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 2
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

Correct Answer: B, D
Section:
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 3
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

Correct Answer: B, C, E
Section:
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 4
Which Layer 7 routing method does FortiWeb support?

A. URL policy routing
B. OSPF
C. BGP
D. HTTP content routing

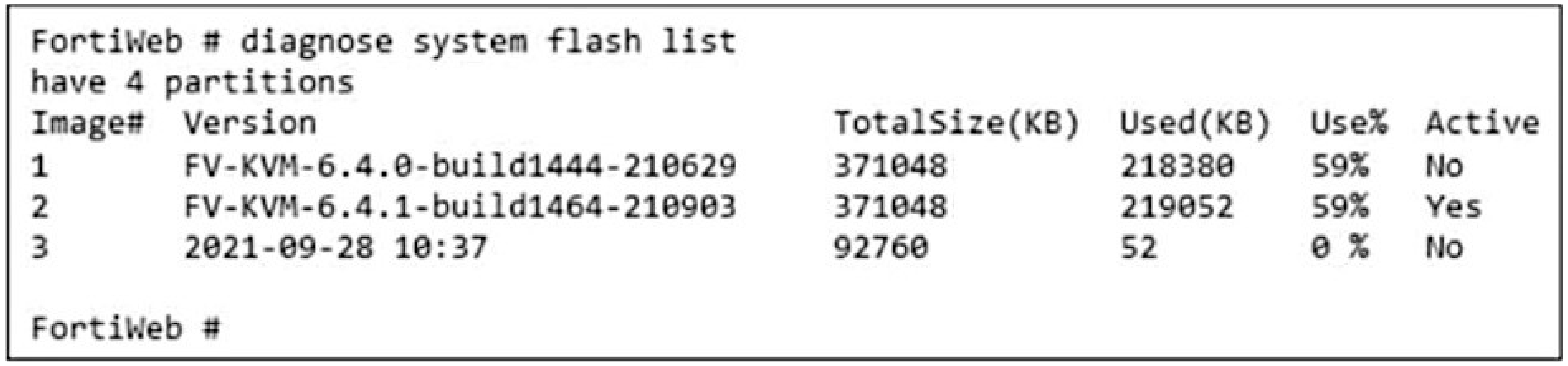
Correct Answer: D
Section:
Explanation:
FortiWeb is a Web Application Firewall (WAF) designed to protect web applications from various threats. Among its features, FortiWeb supports Layer 7 routing methods, which operate based on the content of the HTTP/HTTPS traffic.
HTTP Content Routing refers to the 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 URL-based 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.
FortiWeb 7.2.6 Administration Guide: 'FortiWeb provides advanced Layer 7 load balancing and authentication offload services.' cloud.orange-business.com
FortiWeb Data Sheet: 'FortiWeb provides advanced Layer 7 load balancing and authentication offload services.' Exclusive Networks
FortiWeb on OCB-FE - Installation and Deployment Guide: 'FortiWeb provides advanced Layer 7 load balancing and authentication offload services.' cloud.orange-business.com
These references confirm that FortiWeb supports HTTP content routing as a Layer 7 routing method.

QUESTION 5
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

Correct Answer: B
Section:
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 6
Refer to the exhibit.



```
FortiWeb # diagnose system flash list
have 4 partitions
Image#  Version                         TotalSize(KB)  Used(KB)  Use%  Active
1       FV-KVM-6.4.0-build1444-210629   371048         218380    59%   No
2       FV-KVM-6.4.1-build1464-210903   371048         219052    59%   Yes
3       2021-09-28 10:37                92760          52        0 %   No

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.

Correct Answer: B
Section:
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 7
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

Correct Answer: B
Section:
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 8
In SAML deployments, which server contains user authentication credentials (username/password)?

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

Correct Answer: A
Section:

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 9
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.

Correct Answer: B, C
Section:
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 10
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

Correct Answer: B, D
Section:
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 11
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.

Correct Answer: A, C
Section:
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

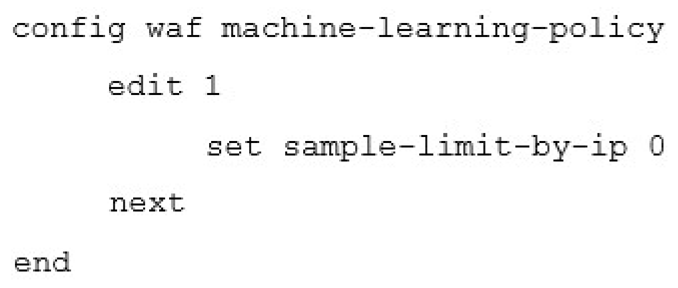
cause disruptions if run during peak hours or when the system is in use.
You should run the vulnerability scan in a test environment: It is important to run the vulnerability scan in a test environment first to avoid unintended disruptions on the live system. This helps to identify potential issues or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

QUESTION 12
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.

Correct Answer: B
Section:
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 13
Review the following configuration:



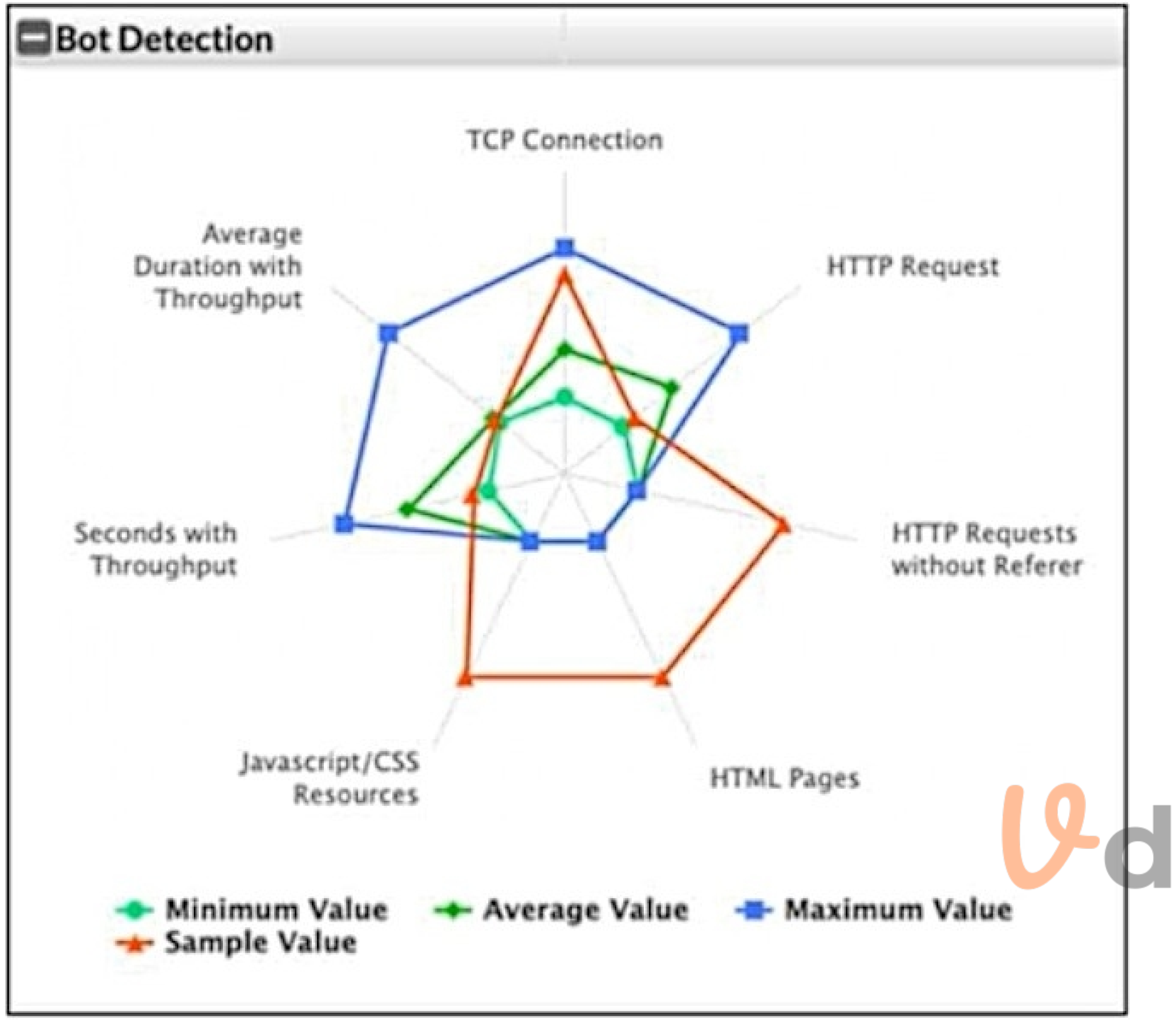
```
config waf machine-learning-policy
     edit 1
          set sample-limit-by-ip 0
     next
end
```

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.

Correct Answer: B
Section:
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 14
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.

Correct Answer: D
Section:
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 15
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

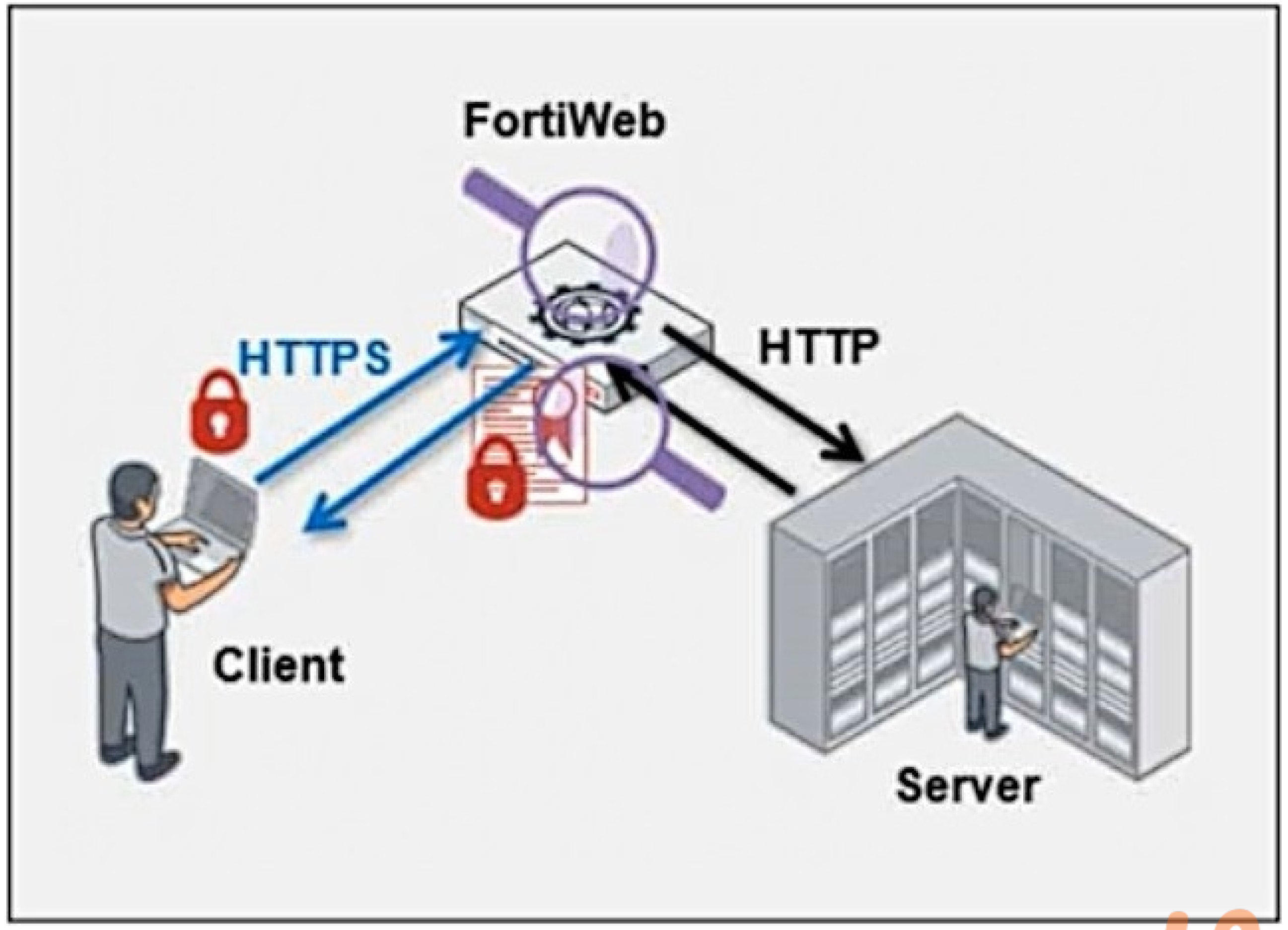
Correct Answer: B, C
Section:
Explanation:
Protected hostname: In reverse proxy mode, the protected hostname refers to the domain or hostname that FortiWeb will protect. It specifies which hostname FortiWeb is acting as a reverse proxy for, and is required for the server policy configuration.
Virtual 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 16
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

Correct Answer: C
Section:
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 17
Refer to the exhibit.



Which statement is true?

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

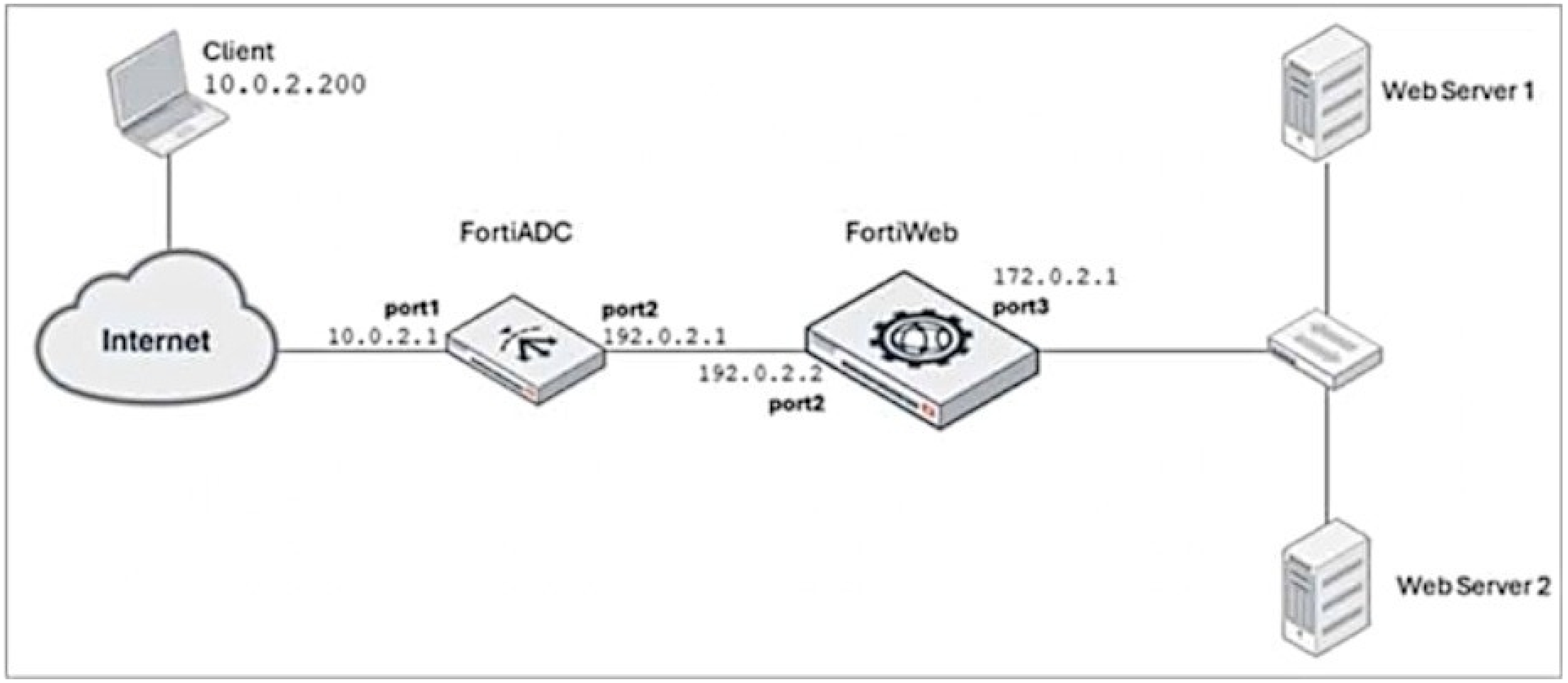
B. FortiWeb is decrypting and re-encrypting the traffic.

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

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

Correct Answer: B
Section:
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 offloading, 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 18
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.

Correct Answer: C, D
Section:
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.

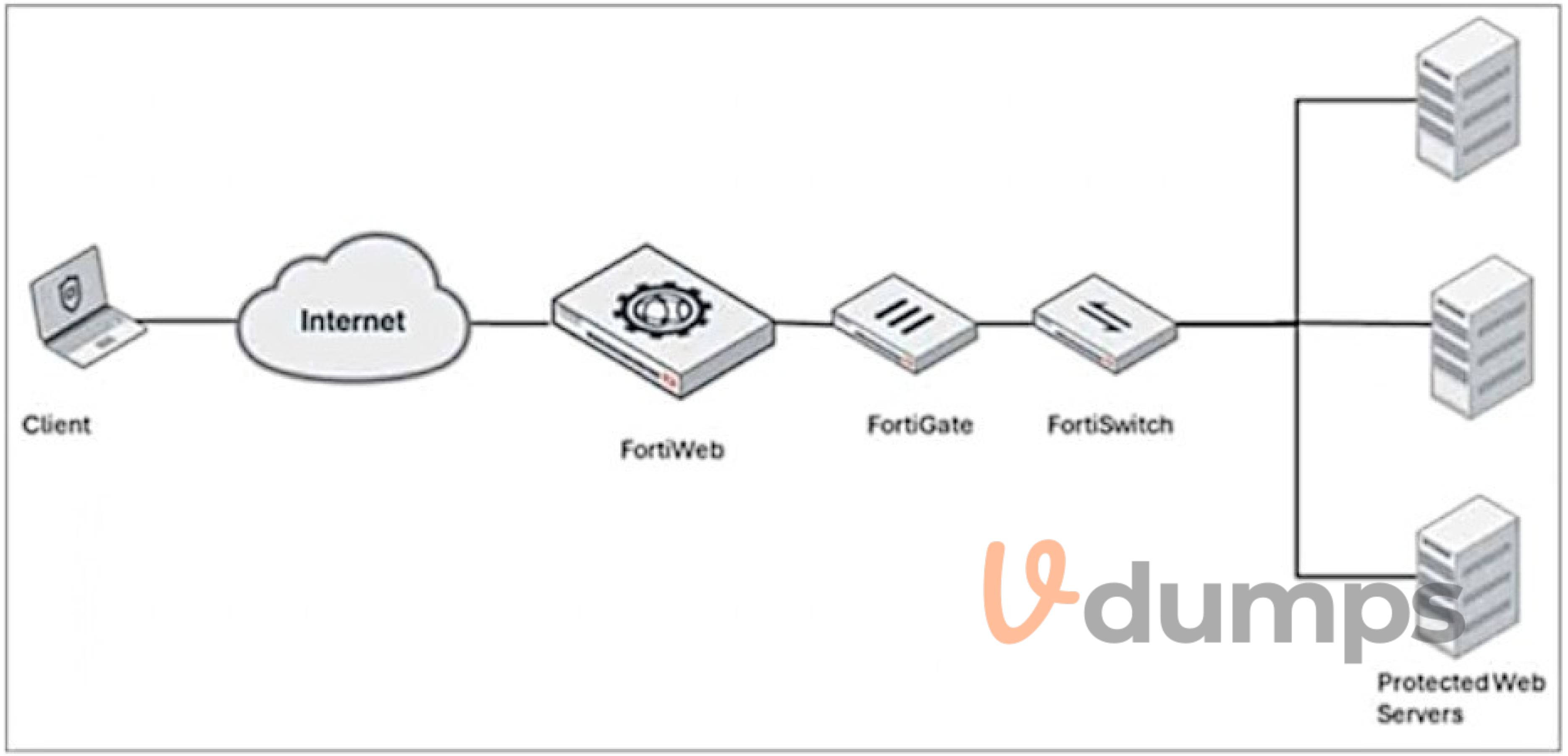
QUESTION 19
A customer wants to be able to index your websites for search and advertisement purposes.
What is the easiest way to allow this on a FortiWeb?

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.

Correct Answer: A

Section:
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 20
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.

Correct Answer: A
Section:
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.