LEAD2PASS

First Test, First Pass!

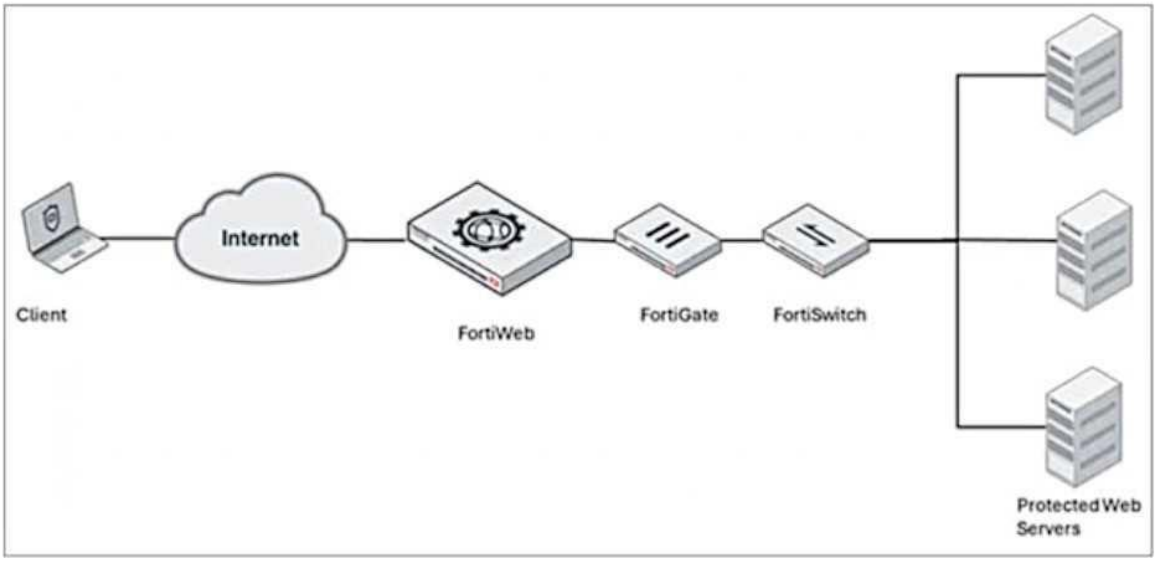
Vendor: Fortinet

Exam Code: FCP_FWB_AD-7.4

Exam Name: FCP - FortiWeb 7.4 Administrator

Version: DEMO

QUESTION 1
Refer to the exhibit. A FortiWeb device is deployed upstream of a device performing source network address translation (SNAT) or load balancing.

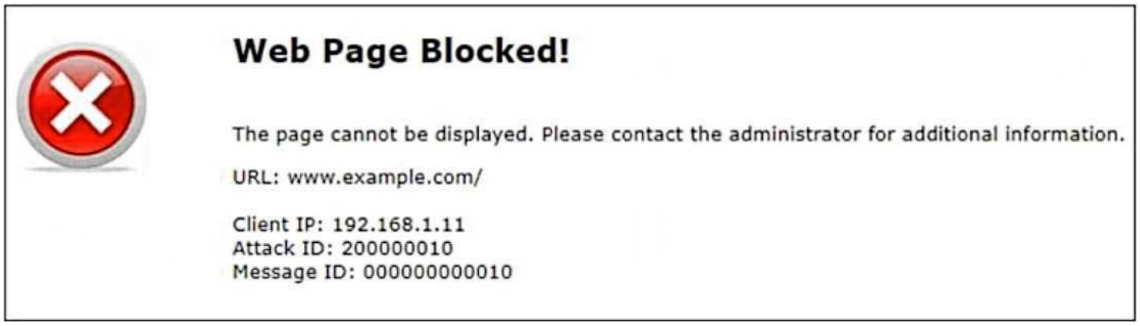


What configuration must you perform on FortiWeb to preserve the original IP address of the client?

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 2
Refer to the exhibit. Attack ID 20000010 is brute force logins.



Web Page Blocked!

The page cannot be displayed. Please contact the administrator for additional information.

URL: www.example.com/

Client IP: 192.168.1.11
Attack ID: 200000010
Message ID: 000000000010

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 3
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: ACD
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 4
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: BD
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 5

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 6
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 7
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: BC
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 8
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.

QUESTION 9
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.

QUESTION 10
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.