KillTest

質量更高　服務更好

學習資料

http://www.killtest.net

一年免費更新服務

Exam : **NSE5_FWB_AD-8.0**

Title : Fortinet NSE 5 - FortiWeb 8.0 Administrator

Version : DEMO

1.DRAG DROP

You are working on securing HTTPS communication across different services using FortiWeb. Your task is to configure and validate digital certificates for various traffic and communication needs.

Match each FortiWeb certificate feature to the certificate-related task that supports the feature.

FortiWeb certificate features		Certificate-related task
Online Certificate Status Protocol (OCSP)		Select the correct certificate based on the requested domain name.
Local Certificate Store		Automatically issue a free, signed certificate for a new public website.
Let's Encrypt		Check if a presented certificate has been revoked in real time.
Server Name Indication (SNI)		Import and store SSL/TLS certificates for use in server policies.
Public Key Pinning		Ensure a trusted public key is used to prevent man-in-the-middle (MITM) attacks.

Answer:

FortiWeb certificate features		Certificate-related task
Online Certificate Status Protocol (OCSP)	Server Name Indication (SNI)	Select the correct certificate based on the requested domain name.
Local Certificate Store	Public Key Pinning	Automatically issue a free, signed certificate for a new public website.
Let's Encrypt	Online Certificate Status Protocol (OCSP)	Check if a presented certificate has been revoked in real time.
Server Name Indication (SNI)	Local Certificate Store	Import and store SSL/TLS certificates for use in server policies.
Public Key Pinning	Let's Encrypt	Ensure a trusted public key is used to prevent man-in-the-middle (MITM) attacks.

2.Refer to the exhibit.

Exhibit

```
info:
 version: 1.0.0
 title: FortiGate Restrictions
 description: Very limited schema for FortiGate UI
 license:
  name: Fortinet
servers:
 - url: 'https://fortigate.com/'
paths:
 /ui:
  get:
   summary: Get UI items
   operationId: getui
   tags:
    - ui
   responses:
    "200":
     description: An array of UI information
     content:
      application/json:
       schema:
        type: string
```

What does the exhibit show?

A. The FortiGate UI interface in HTML.

B. A sample response returned by the FortiGate API at https://fortigate.com/ui.

C. The result of a show ui details command on a FortiWeb server.

D. An API schema file.

Answer: D

Explanation:

The exhibit is written in structured OpenAPI/YAML-style format. It includes fields such as info, version, title, servers, paths, HTTP method get, operationId, responses, content type application/json, and a schema definition. That is not HTML and it is not a live API response. It is also not CLI output from FortiWeb. FortiWeb OpenAPI validation uses OpenAPI description files in YAML or JSON to define API structure, endpoints, parameters, and expected data types. FortiWeb then uses that uploaded schema as a baseline to validate API requests and block requests that do not conform. So the exhibit is best identified as an API schema file

3.A FortiWeb administrator sees the following request:

GET /api/v1/data HTTP/1.1

Host: example.com

Authorization: ApiKey abc123def456

The API key belongs to a user in group B who is authorized to access only /api/v1/reports.

What should the administrator do to prevent this unauthorized access?
A. Restrict access to /api/v1/data using user group–based access control.
B. Block /api/v1/data for all user groups to avoid policy confusion.
C. Move the user to group A so they can access both endpoints.
D. Allow all valid API keys to access any API endpoint.
Answer: A
Explanation:
The problem is not that the API key is invalid; the key belongs to a real user. The issue is authorization scope: group B is allowed only to access /api/v1/reports, but the request targets /api/v1/data. The correct FortiWeb control is API gateway rule enforcement using API key verification and API user grouping. FortiWeb can restrict API access by user group, sub-URL, API key verification, and configured violation actions. Blocking the endpoint for every group is too broad, moving the user to another group grants unnecessary privilege, and allowing all API keys to access all endpoints destroys endpoint-level authorization. The correct fix is group-based access control on /api/v1/data.

4.While reviewing FortiWeb logs, you notice a suspicious login request that failed authentication. You suspect it may be part of an injection attack targeting the login form.
Which input pattern is an example of a typical SQL injection attempt that could bypass authentication checks?
A. '||(SELECT password FROM users WHERE role='admin')||'
B. <sql>select(ALL USERS);</sql>
C. <script>document.location='/steal?cookie='+document.cookie</script>
D. SELECT username FROM accounts WHERE username='admin';-- ' AND password='password';
Answer: D
Explanation:
Option D is the strongest SQL injection example because it uses SQL syntax with a comment marker -- to neutralize the password condition. In a vulnerable login query, that could cause the database to evaluate only the username portion and ignore the password check, creating an authentication bypass.
Option C is not SQL injection; it is cross-site scripting because it executes JavaScript in the browser.
Option B is fake XML-like markup and not a realistic SQL payload.
Option A contains a SQL-like subquery, but it is not the best authentication-bypass pattern shown.
FortiWeb's injection defenses are designed to detect SQL injection and XSS as malicious input patterns targeting application logic.

5.You are reviewing SSL-related issues on FortiWeb. An administrator reports that they receive a certificate warning when they access the FortiWeb GUI over HTTPS. Separately, your FortiWeb device also makes outbound HTTPS requests to a back-end API server.
In which two situations would FortiWeb use its own certificates to establish or secure the connection? (Choose two.)
A. When a client browser initiates an SSL session and FortiWeb is in transparent inspection mode.
B. When FortiWeb is routing an HTTPS connection to a FortiGate without decrypting it.
C. When an administrator connects to the FortiWeb GUI using HTTPS in a browser.
D. When FortiWeb connects to a back-end server over HTTPS as a client.
Answer: C D

Explanation:
The correct answers are C and D. FortiWeb uses its own built-in/self-signed or configured server certificate when an administrator connects to the FortiWeb GUI over HTTPS. FortiWeb can also authenticate as a client when it connects to protected back-end servers over HTTPS, and it may present its own certificate for client PKI authentication.
Option A is wrong because transparent inspection mode does not make FortiWeb the SSL endpoint in the same way; it inspects traffic without acting as the primary TLS termination point.
Option B is also wrong because simply routing HTTPS without decryption does not require FortiWeb to present its own certificate. FortiWeb certificates matter when FortiWeb is an HTTPS endpoint or an authenticated HTTPS client.