Vendor: Fortinet

Exam Code: NSE5_FWB_AD-8.0

Exam Name: Fortinet NSE 5 - FortiWeb 8.0 Administrator

Version: DEMO

QUESTION 1
FortiWeb is blocking groups of users behind your load balancer. In the logs, all users show the same source IP address. Which action should you take to restore proper client identification?

A. Add a bot detection rule in the protection profile.
B. Update the signature engine.
C. Enable caching for HTTPS traffic.
D. Reconfigure the load balancer to insert the original client IP address in an HTTP header.

Answer: D
Explanation:
When traffic passes through a load balancer, FortiWeb may see only the load balancer IP as the source. Inserting the original client IP address in an HTTP header, such as X-Forwarded-For, allows FortiWeb to identify individual clients correctly and avoid applying IP-based blocking to an entire group of users.

QUESTION 2
Your company hosts two different web applications: a shopping site and a blog. You want FortiWeb to apply different protection profiles and forwarding rules to each application. How should you configure FortiWeb to support this?

A. Use one server policy with different virtual IP addresses.
B. Use source network address translation (SNAT) with web caching to split the requests.
C. Configure one server pool but assign different firewall policies.
D. Create a separate server policy for each application.

Answer: D
Explanation:
Separate server policies allow FortiWeb to match each web application independently and apply its own protection profile, virtual server settings, server pool, and forwarding behavior. This is the correct approach when different applications require different security and routing requirements.

QUESTION 3
A FortiWeb administrator needs to allow a known web indexer to scan the website for search engine visibility. What is the easiest way to allow this on FortiWeb?

A. Add the web indexer IP address to the FortiGuard Known Search Engines category.
B. Add the web indexer user-agent string to a custom signature exemption rule.
C. Add the web indexer IP address to the trusted IP address list.
D. Add the web indexer IP address to an IP exception list inside the inline protection profile.

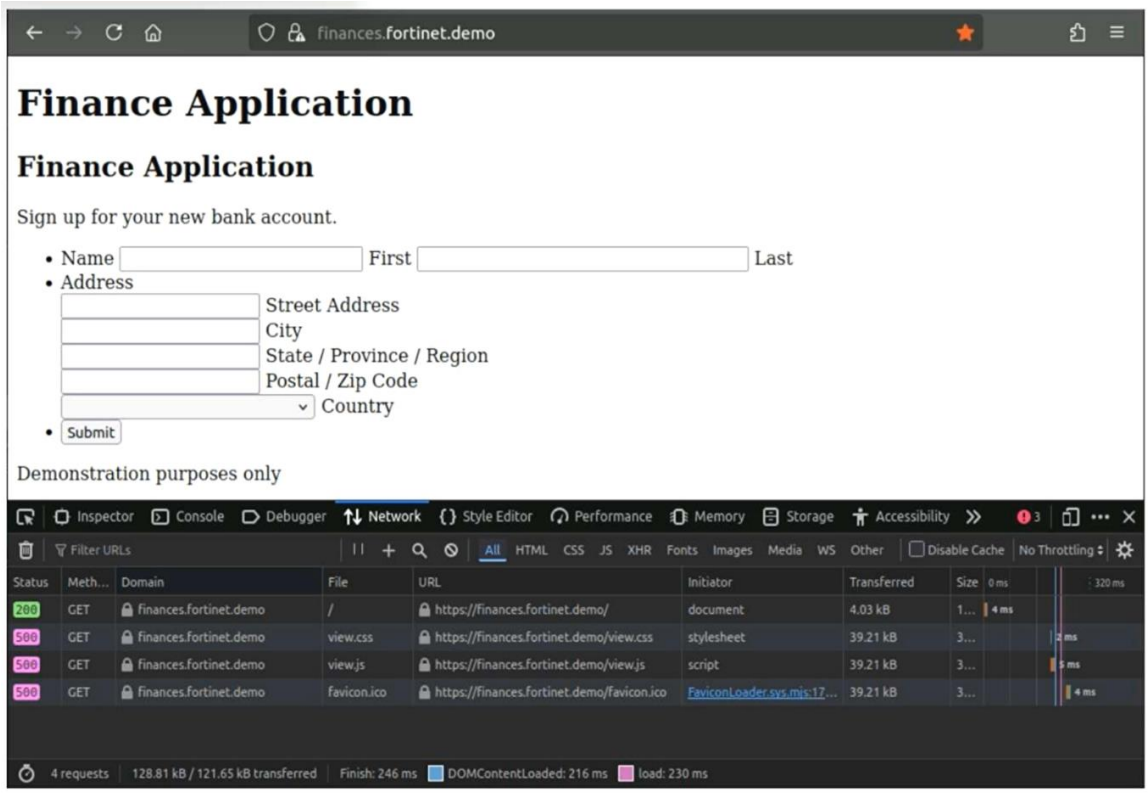
Answer: C
Explanation:
Adding the known web indexer IP address to the trusted IP address list is the simplest way to allow its scanning activity. FortiWeb treats traffic from trusted IPs as allowed, preventing the indexer from being blocked by bot, rate, or other protection controls during legitimate crawling.

QUESTION 4
Which action must a FortiWeb administrator take to enable FortiAppSec Cloud Advanced Bot Protection (ABP) service in a cloud deployment?

A. Deploy an internal intrusion detection system (IDS) to monitor incoming requests.
B. Activate Advanced Bot Protection in FortiWeb and bind it to a FortiAppSec Cloud Application ID.
C. Use browser fingerprinting to reject headless browsers.
D. Set rate-limiting rules for every user session.

Answer: B
Explanation:
FortiAppSec Cloud Advanced Bot Protection is enabled by activating the ABP feature in FortiWeb and associating it with the FortiAppSec Cloud Application ID. This links the FortiWeb deployment to the cloud-based bot protection service so it can analyze and enforce advanced bot detection for the protected application.

QUESTION 5
Refer to the exhibit.



Users complain that parts of the finances.fortinet.demo page fail to load. You see repeated 500 errors for view.js, view.css and favicon.ico.

What is the most likely cause?

A. The client browser does not support advanced caching headers.
B. The FortiWeb access rate limit is too low to allow all required page components to load.
C. The SSL certificate on FortiWeb is expired and blocks subresources.
D. The server is rejecting HTTPS traffic because it's misconfigured.

Answer: B
Explanation:
The page loads the main document successfully, but multiple required subresources fail immediately afterward. This pattern is consistent with FortiWeb rate limiting being set too aggressively, causing normal browser requests for page components such as JavaScript, CSS, and favicon files to be rejected before the full page can render properly.

QUESTION 6
You recently deployed two FortiWeb devices in an active-active (A-A) high availability (HA) cluster.

During routine maintenance, you want to confirm that the cluster is synchronizing the correct configuration areas and that both FortiWeb devices behave consistently in production.

As the FortiWeb administrator, which two configuration areas should you examine to verify that HA synchronization is functioning correctly? (Choose two.)

A. Check the network configuration on both FortiWeb devices-such as interfaces and static routes-to ensure they are aligned.
B. Verify whether firmware images and upgrade history are synchronized between the FortiWeb devices.
C. Review inspection and mitigation log files to determine if they are being replicated across both FortiWeb devices.
D. Review policy configurations, including server policies and protection profiles, to confirm they match across the cluster.

Answer: AD
Explanation:
In an active-active FortiWeb HA cluster, both appliances must have aligned network-related settings so traffic is handled consistently across members. Policy configurations such as server policies and protection profiles should also match, because these determine how FortiWeb forwards, inspects, and mitigates application traffic in production.

QUESTION 7
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 is does the exhibit show?

A. A sample response returned by the FortiGate API at https://fortigate.com/ui.
B. The result of a show ui details command on a FortiWeb server.
C. An API schema file.
D. The FortiGate UI interface in HTML.

Answer: C
Explanation:
The exhibit shows an OpenAPI-style API schema definition. It describes API metadata, server URL, available path, HTTP method, operation details, response code, content type, and expected response schema.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**