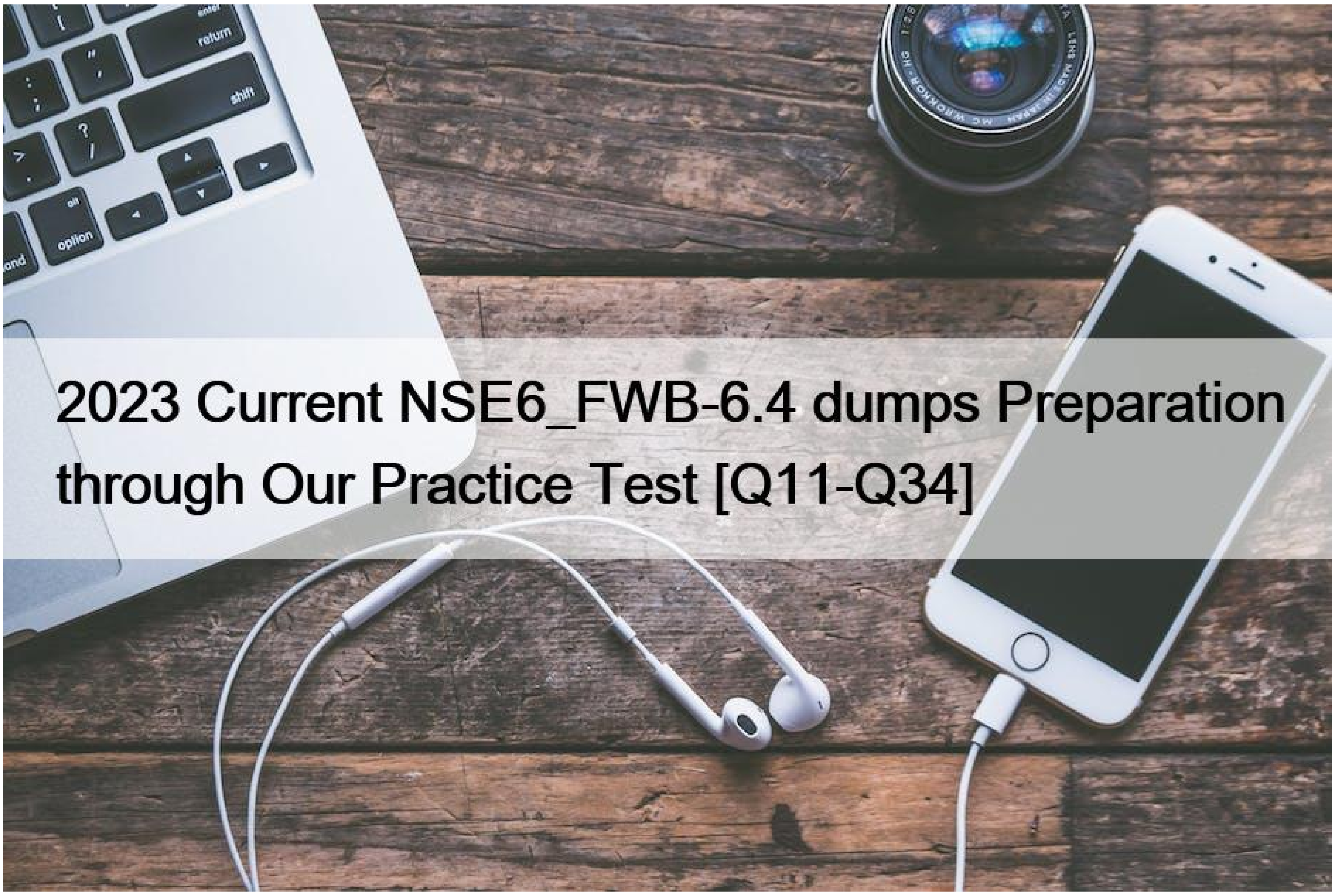
2023 Current NSE6_FWB-6.4 dumps Preparation through Our Practice Test [Q11-Q34



2023 Current NSE6_FWB-6.4 dumps Preparation through Our Practice Test
100% Reliable Microsoft NSE6_FWB-6.4 Exam Dumps Test Pdf Exam Material

QUESTION 11

What role does FortiWeb play in ensuring PCI DSS compliance?
* PCI specifically requires a WAF
* Provides credit card processing capabilities
* Provide ability to securely process cash transactions
* Provides load balancing between multiple web servers
Explanation

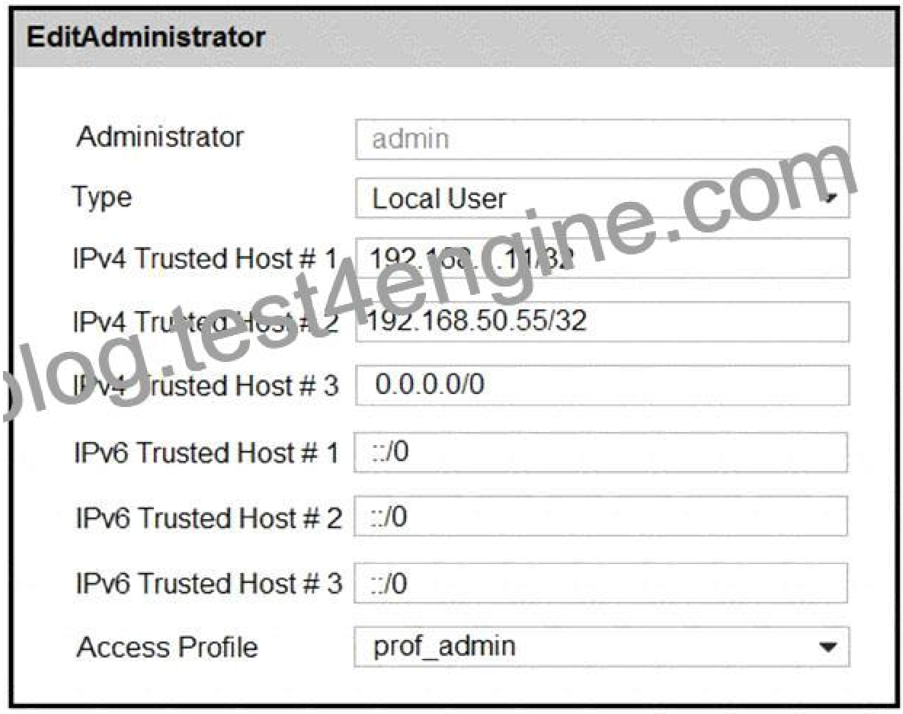
FortiWeb helps you meet all PCI requirements, but PCI now specifically recommends using a WAF, and developing remediations against the top 10 vulnerabilities, according to OWASP.

QUESTION 12

Which implementation is best suited for a deployment that must meet compliance criteria?
* SSL Inspection with FortiWeb in Transparency mode
* SSL Offloading with FortiWeb in reverse proxy mode
* SSL Inspection with FrotiWeb in Reverse Proxy mode
* SSL Offloading with FortiWeb in Transparency Mode

QUESTION 13

Refer to the exhibit.



EditAdministrator

Administrator	admin
Type	Local User
IPv4 Trusted Host # 1	192.168.[illegible].11/32
IPv4 Trusted Host # 2	192.168.50.55/32
IPv4 Trusted Host # 3	0.0.0.0/0
IPv6 Trusted Host # 1	::/0
IPv6 Trusted Host # 2	::/0
IPv6 Trusted Host # 3	::/0
Access Profile	prof_admin

There is only one administrator account configured on FortiWeb. What must an administrator do to restrict any brute force attacks that attempt to gain access to the FortiWeb management GUI?
* Delete the built-in administrator user and create a new one.
* Configure IPv4 Trusted Host # 3 with a specific IP address.
* The configuration changes must be made on the upstream device.
* Change the Access Profile to Read_Only.

QUESTION 14

In Reverse proxy mode, how does FortiWeb handle traffic that does not match any defined policies?
* Non-matching traffic is allowed
* non-Matching traffic is held in buffer
* Non-matching traffic is Denied
* Non-matching traffic is rerouted to FortiGate

QUESTION 15

You are configuring FortiAnalyzer to store logs from FortiWeb.

Which is true?

* FortiAnalyzer will store antivirus and DLP archives from FortiWeb.
* You must enable ADOMs on FortiAnalyzer.
* To store logs from FortiWeb 6.4, on FortiAnalyzer, you must select &#8220;FrotiWeb 6.1&#8221;.
* FortiWeb will query FortiAnalyzer for reports, instead of generating them locally.

QUESTION 16

How does FortiWeb protect against defacement attacks?

* It keeps a complete backup of all files and the database.
* It keeps hashes of files and periodically compares them to the server.
* It keeps full copies of all files and directories.
* It keeps a live duplicate of the database.

Explanation

The anti-defacement feature examines a web site&#8217;s files for changes at specified time intervals. If it detects a change that could indicate a defacement attack, the FortiWeb appliance can notify you and quickly react by automatically restoring the web site contents to the previous backup.

QUESTION 17

Which of the following would be a reason for implementing rewrites?

* Page has been moved to a new URL
* Page has been moved to a new IP address
* Replace vulnerable functions.
* Send connection to secure channel

QUESTION 18

How does offloading compression to FortiWeb benefit your network?

* free up resources on the database server
* Free up resources on the web server
* reduces file size on the client&#8217;s storage
* free up resources on the FortiGate

QUESTION 19

Which statement about local user accounts is true?

* They are best suited for large environments with many users.
* They cannot be used for site publishing.
* They must be assigned, regardless of any other authentication.
* They can be used for SSO.

QUESTION 20

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

* Offline protection
* Transparent inspection
* True transparent proxy

* Reverse proxy

QUESTION 21

An e-commerce web app is used by small businesses. Clients often access it from offices behind a router, where clients are on an IPv4 private network LAN. You need to protect the web application from denial of service attacks that use request floods.

What FortiWeb feature should you configure?
* Enable &#8220;Shared IP&#8221; and configure the separate rate limits for requests from NATted source IPs.
* Configure FortiWeb to use &#8220;X-Forwarded-For:&#8221; headers to find each client&#8217;s private network IP, and to block attacks using that.
* Enable SYN cookies.
* Configure a server policy that matches requests from shared Internet connections.

QUESTION 22

What other consideration must you take into account when configuring Defacement protection
* Use FortiWeb to block SQL Injections and keep regular backups of the Database
* Also incorporate a FortiADC into your network
* None. FortiWeb completely secures the site against defacement attacks
* Configure the FortiGate to perform Anti-Defacement as well

QUESTION 23

When integrating FortiWeb and FortiAnalyzer, why is the selection for FortiWeb Version critical? (Choose two)
* Defines Log file format
* Defines communication protocol
* Defines Database Schema
* Defines Log storage location

QUESTION 24

FortiWeb offers the same load balancing algorithms as FortiGate.

Which two Layer 7 switch methods does FortiWeb also offer? (Choose two.)
* Round robin
* HTTP session-based round robin
* HTTP user-based round robin
* HTTP content routes

QUESTION 25

Which three statements about HTTPS on FortiWeb are true? (Choose three.)
* For SNI, you select the certificate that FortiWeb will present in the server pool, not in the server policy.
* After enabling HSTS, redirects to HTTPS are no longer necessary.
* In true transparent mode, the TLS session terminator is a protected web server.
* Enabling RC4 protects against the BEAST attack, but is not recommended if you configure FortiWeb to only offer TLS 1.2.
* In transparent inspection mode, you select which certificate that FortiWeb will present in the server pool, not in the server policy.

QUESTION 26

When the FortiWeb is configured in Reverse Proxy mode and the FortiGate is configured as an SNAT device, what IP address will the FortiGate&#8217;s Real Server configuration point at?
* Virtual Server IP on the FortiGate
* Server&#8217;s real IP
* FortiWeb&#8217;s real IP
* IP Address of the Virtual Server on the FortiWeb

QUESTION 27

The FortiWeb machine learning (ML) feature is a two-phase analysis mechanism.

Which two functions does the first layer perform? (Choose two.)
* Determines whether an anomaly is a real attack or just a benign anomaly that should be ignored
* Builds a threat model behind every parameter and HTTP method
* Determines if a detected threat is a false-positive or not
* Determines whether traffic is an anomaly, based on observed application traffic over time
Explanation

The first layer uses the Hidden Markov Model (HMM) and monitors access to the application and collects data to build a mathematical model behind every parameter and HTTP method.

QUESTION 28

A client is trying to start a session from a page that would normally be accessible only after the client has logged in.

When a start page rule detects the invalid session access, what can FortiWeb do? (Choose three.)
* Display an access policy message, then allow the client to continue
* Redirect the client to the login page
* Allow the page access, but log the violation
* Prompt the client to authenticate
* Reply with a 403 Forbidden HTTP error

QUESTION 29

Which two statements about running a vulnerability scan are true? (Choose two.)
* You should run the vulnerability scan during a maintenance window.
* You should run the vulnerability scan in a test environment.
* Vulnerability scanning increases the load on FortiWeb, so it should be avoided.
* You should run the vulnerability scan on a live website to get accurate results.
Explanation

Should the Vulnerability Scanner allow it, SVMS will set the scan schedule (or schedules) to run in a maintenance window. SVMS will advise Client of the scanner&#8217;s ability to complete the scan(s) within the maintenance window.

Vulnerabilities on live web sites. Instead, duplicate the web site and its database in a test environment.

QUESTION 30

In which operation mode(s) can FortiWeb modify HTTP packets? (Choose two.)

* Transparent Inspection
* Offline protection
* True transparent proxy
* Reverse proxy

QUESTION 31

Which algorithm is used to build mathematical models for bot detection?
* HCM
* SVN
* SVM
* HMM
Explanation

FortiWeb uses SVM (Support Vector Machine) algorithm to build up the bot detection model

QUESTION 32

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

Which is true about the solution?
* Static or policy-based routes are not required.
* To achieve HTTP content routing, you must chain policies: the first policy accepts all traffic, and forwards requests for web app A to the virtual server for policy A. It also forwards requests for web app B to the virtual server for policy B. Policy A and Policy B apply their app-specific protection profiles, and then distribute that app&#8217;s traffic among all members of the server farm.
* You must put the single web server into a server pool in order to use it with HTTP content routing.
* The server policy applies the same protection profile to all its protected web apps.