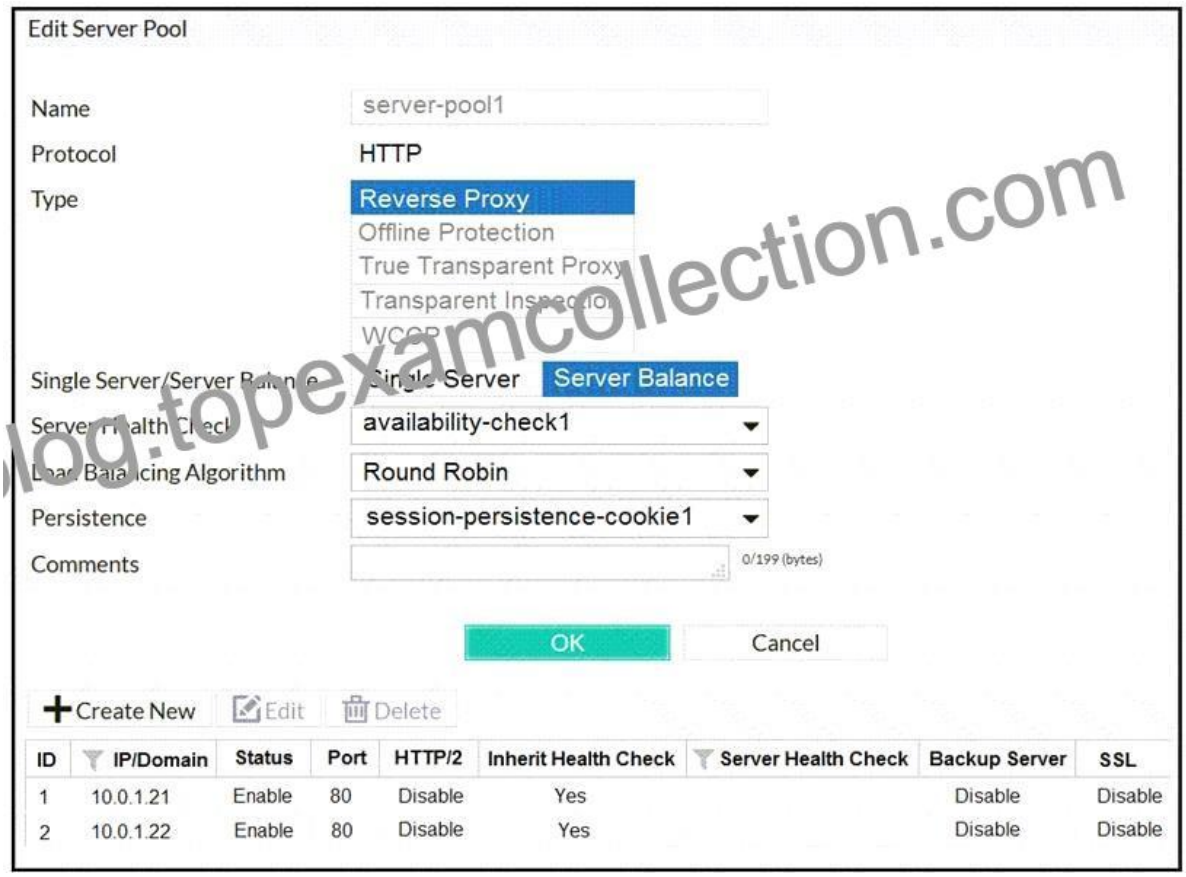
[2023 Use Valid New Free NSE6_FWB-6.4 Exam Dumps & Answers [Q22-Q40

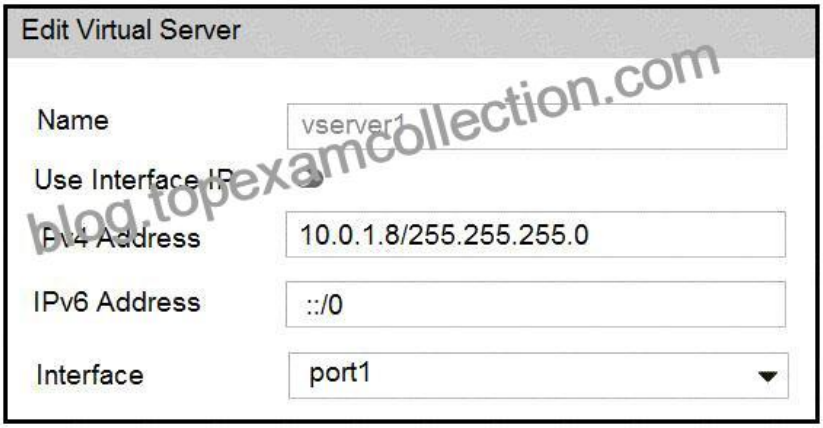
[2023] Use Valid New Free NSE6_FWB-6.4 Exam Dumps & Answers
NSE6_FWB-6.4 Braindumps PDF, Fortinet NSE6_FWB-6.4 Exam Cram

Fortinet NSE6_FWB-6.4 Exam Syllabus Topics:

TopicDetailsTopic 1- Configure server pools, policies, and protected hostnames- Trobleshoot encryption and authentication related issuesTopic 2- Troublehsoot application delivery related issues- Configure various threat mitigation featuresTopic 3- Configure machine learning and bot detection- Configure SSL inspection and offloadingTopic 4- Configure various access control and tracking methods- Troubleshoot deployment and system related issuesTopic 5- Configure API protection and bot mitigation- Configure caching and compressionTopic 6- Configure HTTP content routing, rewriting, and redirection- Mitigate attacks on authenticationTopic 7- Encryption, Authentication, and Compliance- Mitigate web application vulnerabilities

Q22. Refer to the exhibits.





FortiWeb is configured in reverse proxy mode and it is deployed downstream to FortiGate. Based on the configuration shown in the exhibits, which of the following statements is true?

* FortiGate should forward web traffic to the server pool IP addresses.
* The configuration is incorrect. FortiWeb should always be located upstream to FortiGate.
* You must disable the Preserve Client IP setting on FotriGate for this configuration to work.
* FortiGate should forward web traffic to virtual server IP address.

Q23. When viewing the attack logs on FortiWeb, which client IP address is shown when you are using XFF header rules?

* FortiGate public IP

* FortiWeb IP
* FortiGate local IP
* Client real IP

Explanation

When an XFF header reaches Alteon from a client, Alteon removes all the content from the header and injects the client IP address. Alteon then forwards the header to the server.

Q24. Which operation mode does not require additional configuration in order to allow FTP traffic to your web server?
* Offline Protection
* Transparent Inspection
* True Transparent Proxy
* Reverse-Proxy

Q25. Which of the following is true about Local User Accounts?
* Must be assigned regardless of any other authentication
* Can be used for Single Sign On
* Can be used for site publishing
* Best suited for large environments with many users

Q26. What benefit does Auto Learning provide?
* Automatically identifies and blocks suspicious IPs
* FortiWeb scans all traffic without taking action and makes recommendations on rules
* Automatically builds rules sets
* Automatically blocks all detected threats

Q27. In which scenario might you want to use the compression feature on FortiWeb?
* When you are serving many corporate road warriors using 4G tablets and phones
* When you are offering a music streaming service
* When you want to reduce buffering of video streams
* Never, since most traffic today is already highly compressed

Explanation

https://training.fortinet.com/course/view.php?id=3363

When might you want to use the compression feature on FortiWeb? When you are serving many road warriors who are using 4G tablets and phones

Q28. When generating a protection configuration from an auto learning report what critical step must you do before generating the final protection configuration?
* Restart the FortiWeb to clear the caches
* Drill down in the report to correct any false positives.
* Activate the report to create t profile
* Take the FortiWeb offline to apply the profile

Q29. What is one of the key benefits of the FortiGuard IP reputation feature?
* It maintains a list of private IP addresses.
* It provides a document of IP addresses that are suspect, so that administrators can manually update their blacklists.
* It is updated once per year.
* It maintains a list of public IPs with a bad reputation for participating in attacks.

Explanation

FortiGuard IP Reputation service assigns a poor reputation, including virus-infected clients and malicious spiders/crawlers.

Q30. Which would be a reason to implement HTTP rewriting?
* The original page has moved to a new URL
* To replace a vulnerable function in the requested URL
* To send the request to secure channel
* The original page has moved to a new IP address

Explanation

Create a new URL rewriting rule.

Q31. How does an ADOM differ from a VDOM?
* ADOMs do not have virtual networking
* ADOMs improve performance by offloading some functions.
* ADOMs only affect specific functions, and do not provide full separation like VDOMs do.
* Allows you to have 1 administrator for multiple tenants

Q32. Under what circumstances would you want to use the temporary uncompress feature of FortiWeb?
* In the case of compression being done on the FortiWeb, to inspect the content of the compressed file
* In the case of the file being a .MP3 music file
* In the case of compression being done on the web server, to inspect the content of the compressed file.
* In the case of the file being an .MP4 video

Q33. A client is trying to start a session from a page that should normally be accessible only after they have logged in.

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

Q34. 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’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.

Q35. What must you do with your FortiWeb logs to ensure PCI DSS compliance?
* Store in an off-site location
* Erase them every two weeks
* Enable masking of sensitive data

* Compress them into a .zip file format

Q36. Refer to the exhibit.

Based on the configuration, what would happen if this FortiWeb were to lose power? (Choose two.)
* Traffic that passes between port5 and port6 will be inspected.
* Traffic will be interrupted between port3 and port4.
* All traffic will be interrupted.
* Traffic will pass between port5 and port6 uninspected.

Q37. 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

Q38. You’ve configured an authentication rule with delegation enabled on FortiWeb.

What happens when a user tries to access the web application?
* FrotiWeb redirects users to a FortiAuthenticator page, then if the user authenticates successfully, FortiGate signals to FortiWeb to allow access to the web app
* ForitWeb redirects the user to the web app’s authentication page
* FortiWeb forwards the HTTP challenge from the server to the client, then monitors the reply, allowing access if the user authenticates successfully
* FortiWeb replies with a HTTP challenge of behalf of the server, the if the user authenticates successfully, FortiWeb allows the request and also includes credentials in the request that it forwards to the web app

Q39. 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

Q40. 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

Feel Fortinet NSE6_FWB-6.4 Dumps PDF Will likely be The best Option:
https://www.topexamcollection.com/NSE6_FWB-6.4-vce-collection.html]