PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 6 - FortiADC 6.2

Fortinet NSE6_FAD-6.2

Version Demo

Total Demo Questions: 5

Total Premium Questions: 51

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, System configuration	9
Topic 2, Server load balancing	25
Topic 3, Link load balancing	2
Topic 4, Global server load balancing	5
Topic 5, Security	9
Topic 6, Troubleshooting	1
Total	51

QUESTION NO: 1

Which two remote destinations can FortiADC use for centralized log storage and analysis? (Choose two.)

A. FortiAnalyzer

B. Syslog server

C. FTP server

D. FortiCloud

ANSWER: A B

Explanation:

FortiAnalyzer is a supported centralized logging and analytics platform for Fortinet devices. Sending FortiADC logs to FortiAnalyzer allows administrators to retain, search, correlate, and report on system, traffic, and security events.

Syslog server is also a supported remote logging destination. A syslog server can receive FortiADC log messages for integration with an organization's existing monitoring or security-information and event-management infrastructure. FortiCloud and an FTP server are not FortiADC log destinations in this context. See the FortiADC 6.2 Handbook for logging configuration guidance.

QUESTION NO: 2

Which load balancing method requires the use of an SNMP health check?

A. Destination IP hash

B. Round robin

C. Dynamic load

D. Least connection

ANSWER: C

Explanation:

Dynamic load is correct because this FortiADC load-balancing method selects a real server according to load information that FortiADC obtains from the server itself. To make that decision, FortiADC needs an SNMP health check configured for the real servers in the pool. The health check polls the configured SNMP agent and retrieves the server-load values used by the dynamic-load algorithm. FortiADC can therefore direct new connections toward the available server reporting the most favorable current load, rather than distributing traffic solely from connection counts, a rotating sequence, or a client/destination address hash.

The SNMP health check is not merely an availability probe in this situation; it provides the dynamic metric on which server selection depends. Consequently, the SNMP agent must be reachable from FortiADC, the configured SNMP credentials and version must match the agent configuration, and the relevant load-related object values must be available for polling. This relationship between the Dynamic Load method and SNMP-based monitoring is documented in the FortiADC 6.2 handbook's server-load-balancing material and health-check configuration guidance. See the FortiADC 6.2 Handbook and the FortiADC 6.2 Administration Guide.

QUESTION NO: 3

An administrator is managing a web site that uses specialized servers for streaming, in addition to servers that handle HTTP traffic.

To make sure that specialized servers handle the streaming traffic, what FortiADC capacity should they use?

A. Persistence rules

B. Content routing

C. Dynamic load balancing

D. HTTP compression

ANSWER: B

Explanation:

Content routing is the appropriate FortiADC capability because it inspects relevant request characteristics and directs traffic to a selected server pool according to matching routing policies. An administrator can define criteria that identify streaming requests, such as a requested URL path or file extension, HTTP host, header, or other application-layer content, and associate that criterion with the pool containing the specialized streaming servers. Requests that match the streaming rule are therefore sent to those servers, while ordinary web requests can continue to be handled by the standard HTTP-server pool. This provides deliberate, application-aware traffic separation rather than merely distributing all connections across available servers. Content-routing rules are evaluated for traffic arriving at a virtual server, allowing FortiADC to select the appropriate real-server pool before normal load-balancing selection occurs within that pool. The result is that each request type reaches infrastructure designed to serve it, which is particularly important when streaming workloads require different protocols, resources, caching behavior, or performance characteristics from conventional HTTP content. Fortinet documents FortiADC content routing and its policy-based pool selection in the FortiADC 6.2 documentation and the FortiADC 6.2.1 Handbook.

QUESTION NO: 4

Which two statements about TCP and HTTP health checks are true? (Choose two.)

A. A TCP health check can verify that a TCP service is accepting connections.

B. An HTTP health check can validate an expected HTTP response.

C. A TCP health check evaluates WAF signatures on the real server.

D. An HTTP health check requires SNMP to retrieve server-load information.

ANSWER: A B

Explanation:

A **TCP health check** verifies basic TCP service availability by attempting to establish a TCP connection to the configured port on the real server. It is suitable when the administrator needs to confirm that a transport-layer service is listening and reachable.

An **HTTP health check** can validate application-layer behavior by sending an HTTP request and evaluating the server response against configured expectations. This provides more meaningful application availability monitoring than a TCP connection alone because FortiADC can verify that the web service responds as expected. Fortinet documents health-check methods in the FortiADC 6.2 Handbook.

QUESTION NO: 5

An administrator wants FortiADC to create and insert its own cookie to maintain persistence for HTTP clients.

Which persistence method should the administrator configure?

A. Insert cookie

B. Embedded cookie

C. Source IP

D. SSL session ID

ANSWER: A

Explanation:

Insert cookie is correct because FortiADC generates a persistence cookie and inserts it into the HTTP response sent to the client. When the client returns the cookie in a subsequent request, FortiADC uses the cookie value to identify the selected real server and maintain session affinity.

This method is appropriate when the application does not already provide a suitable cookie for persistence, or when the administrator wants FortiADC to manage session affinity independently of application cookies. It differs from embedded-cookie persistence, which adds FortiADC persistence information to an existing server-generated cookie. Fortinet documents persistence methods in the FortiADC 6.2 Handbook.