500-275^{Q&As}

Securing Cisco Networks with Sourcefire FireAMP Endpoints (SSFAMP)

Pass Cisco 500-275 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/500-275.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

When discussing the FireAMP product, which term does the acronym DFC represent?

A. It means Detected Forensic Cause.

B. It means Duplicate File Contents.

C. It means Device Flow Correlation.

D. It is not an acronym that is associated with the FireAMP product.

Correct Answer: C

QUESTION 2

What is the default clean disposition cache setting?

A. 3600

B. 604800

C. 10080

D. 1 hour

Correct Answer: B

QUESTION 3

Which of these can you use for two-step authentication?

A. the Apple Authenticator app

B. the Google Authenticator app

C. a SecurID token

D. any RFC 1918 compatible application

Correct Answer: B

QUESTION 4

For connector-to-FireAMP Private Cloud communication, which port number is used for lower- overhead communication?

A. 22

B. 80

C. 443

D. 32137

Correct Answer: D

QUESTION 5

Which statement is true about the Device Trajectory feature?

A. It shows where the endpoint devices have moved in your environment by displaying each IP address that a device has had over time.

B. A "plus" sign on the File Trajectory map indicates that you can execute the file inside FireAMP.

C. In the File Trajectory map, you can view the parent process for a file by selecting the infected system.

D. It shows hosts that display Indications of Compromise.

Correct Answer: C