Securing Cisco Networks with Sourcefire FireAMP Endpoints (500-275)

Exam Description: The Securing Cisco Networks with Sourcefire FireAMP Endpoints (500-275 SSFAMP) exam is a 75-minute exam with 45 to 55 questions. It is designed for technical professionals who need to demonstrate their skills and expertise in the deployment and management of Cisco Advanced Malware Protection in their network environment.

Exam takers will demonstrate knowledge of the powerful features and options of Cisco AMP technology and software, deployment tasks, management options, and analysis procedures.

The following topics are general guidelines for the content likely to be included on the exam. However, related topics may also appear on any specific version of the exam. To better reflect the contents of the exam, the guidelines below may change at any time without notice.

20% 1.0 Cisco Advanced Malware Protection Overview and Architecture

1.1 Describe the Cisco AMP technology and features that distinguish it from traditional malware solutions

1.2 Describe the Cisco AMP architecture, including the components of the cloud and connector

1.3 Describe the communication that occurs between the endpoints and Cisco AMP for the cloud

9% 2.0 Outbreak Control Menu Items

2.1 Understand the different types of custom detections (application blocking, advanced and simple detections) including the ways to create them

2.2 Define device flow control and describe its features

2.3 Describe whitelisting and how to create white lists

9% 3.0 Endpoint Policies

3.1 Describe the different policy elements under the General tab

3.2 Describe the settings contained in the file tab of a Cisco AMP policy

3.3 Describe the configuration options of device flow control

12% 4.0 Groups and Development

4.1 Understand the considerations one should take when planning the deployment of the Cisco AMP connector

4.2 Describe the requirements and procedures for installation of the connector

18% 5.0 Analysis and Reporting

5.1 Be familiar with general malware analysis tasks and terms for Cisco AMP

5.2 Describe the use of the dashboard including the indicators of compromise

5.3 Use the file and device trajectory feature of the Cisco AMP console

5.4 Use the file analysis features of the Cisco AMP console

5.5 Be familiar with the reporting features of Cisco AMP

10% 6.0 Private Cloud

6.1 Describe the communication that occurs between private and public clouds
6.2 Describe the items one should consider before installation of the Cisco AMP private cloud

6% 7.0 Accounts

7.1 Be familiar with the general features available in the Accounts menu
7.2 Describe the two-step authentication features of Cisco AMP

6% 8.0 Cisco AMP Connector

8.1 Describe the different scan types available to the Cisco AMP user
8.2 Describe the files used by the Cisco AMP connector
8.3 Be familiar with tools that may be used to help troubleshoot the connector

10% 9.0 Console Interface

9.1 Be familiar with the first-use interface
9.2 Describe the use and implementation of remote file fetch
9.3 Be familiar with the console interface features