500-285^{Q&As}

Securing Cisco Networks with FireSIGHT Intrusion Prevention System (SSFIPS)

Pass Cisco 500-285 Exam with 100% Guarantee

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

https://www.geekcert.com/500-285.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A user discovery agent can be installed on which platform?

A. OpenLDAP

B. Windows

C. RADIUS

D. Ubuntu

Correct Answer: B Testlet 1

TESTLET OVERVIEW

Title: Case Study

The following testlet will present a Case Study followed by [count] multiple choice question(s), [count]

create a tree question(s), [count] build list and reorder question(s) and [count] drop and connect question

(s).

You will have [count] minutes to complete the testlet.

For help on how to answer the questions, click the Instuctions button on the question screen.

QUESTION 2

Which option describes the two basic components of Sourcefire Snort rules?

A. preprocessor configurations to define what to do with packets before the detection engine sees them, and detection engine configurations to define exactly how alerting is to take place

B. a rule statement characterized by the message you configure to appear in the alert, and the rule body that contains all of the matching criteria such as source, destination, and protocol

C. a rule header to define source, destination, and protocol, and the output configuration to determine which form of output to produce if the rule triggers

D. a rule body that contains packet-matching criteria or options to define where to look for content in a packet, and a rule header to define matching criteria based on where a packet originates, where it is going, and over which protocol

Correct Answer: D

QUESTION 3

Other than navigating to the Network File Trajectory page for a file, which option is an alternative way of accessing the network trajectory of a file?

A. from Context Explorer

B. from the Analysis menu

C. from the cloud

D. from the Defense Center

Correct Answer: A

QUESTION 4

How do you configure URL filtering?

A. Add blocked URLs to the global blacklist.

B. Create a Security Intelligence object that contains the blocked URLs and add the object to the access control policy.

C. Create an access control rule and, on the URLs tab, select the URLs or URL categories that are to be blocked or allowed.

D. Create a variable.

Correct Answer: C

QUESTION 5

What is the maximum timeout value for a browser session?

A. 60 minutes

B. 120 minutes

C. 1024 minutes

D. 1440 minutes

Correct Answer: D

[500-285 VCE Dumps](#)   [500-285 Exam Questions](#)   [500-285 Braindumps](#)