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.pass2lead.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

Which option is used to implement suppression in the Rule Management user interface?

A. Rule Category

B. Global

C. Source

D. Protocol

Correct Answer: C

QUESTION 2

Which mechanism should be used to write an IPS rule that focuses on the client or server side of a TCP communication?

A. the directional operator in the rule header

B. the "flow" rule option

C. specification of the source and destination ports in the rule header

D. The detection engine evaluates all sides of a TCP communication regardless of the rule options.

Correct Answer: B

QUESTION 3

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 4

FireSIGHT uses three primary types of detection to understand the environment in which it is deployed. Which option is one of the detection types?

A. protocol layer

B. application

C. objects

D. devices

Correct Answer: B

QUESTION 5

Which option is a remediation module that comes with the Sourcefire System?

A. Cisco IOS Null Route

B. Syslog Route

C. Nmap Route Scan

D. Response Group

Correct Answer: A