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.passapply.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 statement is true in regard to the Sourcefire Security Intelligence lists?

A. The global blacklist universally allows all traffic through the managed device.

B. The global whitelist cannot be edited.

C. IP addresses can be added to the global blacklist by clicking on interactive graphs in Context Explorer.

D. The Security Intelligence lists cannot be updated.

Correct Answer: C

QUESTION 2

What are the two categories of variables that you can configure in Object Management?

A. System Default Variables and FireSIGHT-Specific Variables

B. System Default Variables and Procedural Variables

C. Default Variables and Custom Variables

D. Policy-Specific Variables and Procedural Variables

Correct Answer: C

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

Correlation policy rules allow you to construct criteria for alerting on very specific conditions. Which option is an example

of such a rule?

A. testing password strength when accessing an application

B. limiting general user access to administrative file shares

C. enforcing two-factor authentication for access to critical servers

D. issuing an alert if a noncompliant operating system is detected or if a host operating system changes to a noncompliant operating system when it was previously profiled as a compliant one

Correct Answer: D

QUESTION 5

The gateway VPN feature supports which deployment types?

A. SSL and HTTPS

B. PPTP and MPLS

C. client and route-based

D. point-to-point, star, and mesh

Correct Answer: D