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.pass4itsure.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 when network traffic meets the criteria specified in a correlation rule?

A. Nothing happens, because you cannot assign a group of rules to a correlation policy.

B. The network traffic is blocked.

C. The Defense Center generates a correlation event and initiates any configured responses.

D. An event is logged to the Correlation Policy Management table.

Correct Answer: C

QUESTION 2

Controlling simultaneous connections is a feature of which type of preprocessor?

A. rate-based attack prevention

B. detection enhancement

C. TCP and network layer preprocessors

D. performance settings

Correct Answer: A

QUESTION 3

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 4

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 5

Which Sourcefire feature allows you to send traffic directly through the device without inspecting it?

A. fast-path rules

B. thresholds or suppressions

C. blacklist

D. automatic application bypass

Correct Answer: A

Latest 500-285 Dumps   500-285 Practice Test   500-285 Study Guide