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 adding a network to an access control rule?

A. You can select only source networks.

B. You must have preconfigured the network as an object.

C. You can select the source and destination networks or network groups.

D. You cannot include multiple networks or network groups as sources or destinations.

Correct Answer: C

QUESTION 2

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

QUESTION 3

Which statement represents detection capabilities of the HTTP preprocessor?

A. You can configure it to blacklist known bad web servers.

B. You can configure it to normalize cookies in HTTP headers.

C. You can configure it to normalize image content types.

D. You can configure it to whitelist specific servers.

Correct Answer: B

QUESTION 4

Which option is true regarding the $HOME_NET variable?

A. is a policy-level variable

B. has a default value of "all"

C. defines the network the active policy protects

D. is used by all rules to define the internal network

Correct Answer: C

QUESTION 5

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