EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : **500-285**

Title : Securing Cisco Networks with Sourcefire IPS

Version : DEMO

1.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
Answer: C

2.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
Answer: C

3.Which option is one of the three methods of updating the IP addresses in Sourcefire Security Intelligence?
A. subscribe to a URL intelligence feed
B. subscribe to a VRT
C. upload a list that you create
D. automatically upload lists from a network share
Answer: C

4.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.
Answer: C

5.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.
Answer: C