Vendor: Cisco

Exam Code: 500-290

Exam Name: IPS Express Security for Engineers

Version: DEMO

QUESTION 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

QUESTION 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

QUESTION 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

QUESTION 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

QUESTION 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

QUESTION 6
When adding source and destination ports in the Ports tab of the access control policy rule editor, which restriction is in place?

A. The protocol is restricted to TCP only.
B. The protocol is restricted to UDP only.
C. The protocol is restricted to TCP or UDP.
D. The protocol is restricted to TCP and UDP.

Answer: C

QUESTION 7
Access control policy rules can be configured to block based on the conditions that you specify in each rule. Which behavior block response do you use if you want to deny and reset the connection of HTTP traffic that meets the conditions of the access control rule?

A. interactive block with reset
B. interactive block
C. block
D. block with reset

Answer: D

QUESTION 8
Which option transmits policy-based alerts such as SNMP and syslog?

A. the Defense Center
B. FireSIGHT
C. the managed device
D. the host

Answer: C

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**