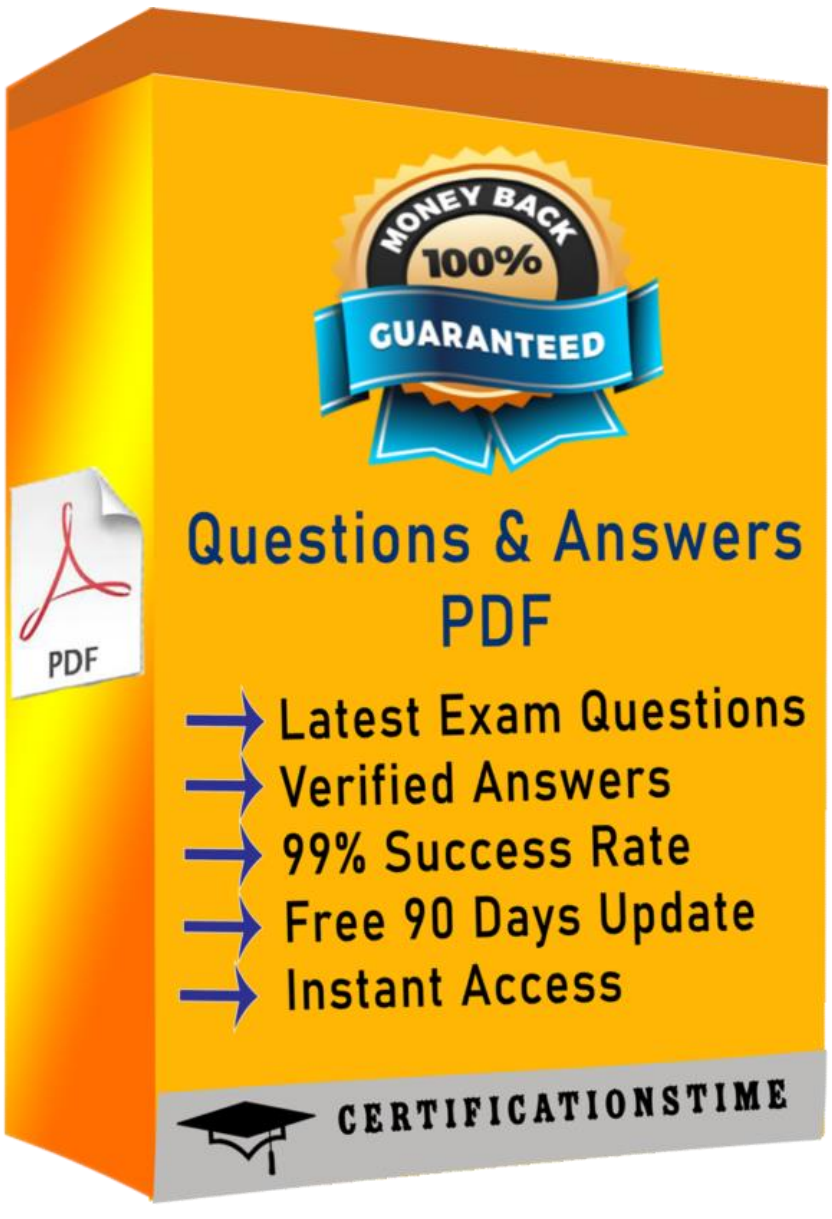
Cisco

Exam Questions 500-285

SSFIPS Securing Cisco Networks with Sourcefire Intrusion Prevention System

https://certificationstime.com/



QUESTION 1

- (Topic 1)
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
Topic 2, Access Control Policy

QUESTION 2

- (Topic 2)
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
Topic 3, Event Analysis

QUESTION 3

- (Topic 3)
Which option is not a characteristic of dashboard widgets or Context Explorer?
A. Context Explorer is a tool used primarily by analysts looking for trends across varying periods of time.
B. Context Explorer can be added as a widget to a dashboard.
C. Widgets offer users an at-a-glance view of their environment.
D. Widgets are offered to all users, whereas Context Explorer is limited to a few roles.
Answer: B
Topic 4, IPS Policy Basics

QUESTION 4

- (Topic 4)
Which option is used to implement suppression in the Rule Management user interface?
A. Rule Category
B. Global
C. Source
D. Protocol
Answer: C
Topic 5, FireSIGHT Technologies

QUESTION 5

- (Topic 5)
A user discovery agent can be installed on which platform?
A. OpenLDAP
B. Windows
C. RADIUS
D. Ubuntu
Answer: B

QUESTION 6

- (Topic 5)
Host criticality is an example of which option?
A. a default whitelist
B. a default traffic profile
C. a host attribute
D. a correlation policy

Answer: C
Topic 7, Basic Administration

QUESTION 7

- (Topic 7)
Where do you configure widget properties?
A. dashboard properties
B. the Widget Properties button in the title bar of each widget
C. the Local Configuration page
D. Context Explorer
Answer: B
Topic 9, Creating Snort Rules

QUESTION 8

- (Topic 9)
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.
Answer: B
Topic 11, Correlation Policies