Cisco

Exam 500-285

Securing Cisco Networks with Sourcefire IPS

Verson: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 1: Object Management	1
Topic 2: Access Control Policy	1
Topic 3: Event Analysis	1
Topic 4: IPS Policy Basics	1
Topic 5: FireSIGHT Technologies	2
Topic 7: Basic Administration	1
Topic 9: Creating Snort Rules	1
Topic 11: Correlation Policies	2

Topic 1, Object Management

Question No : 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 No : 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 No : 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 No : 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 No : 5 - (Topic 5)

A user discovery agent can be installed on which platform?

A. OpenLDAP
B. Windows
C. RADIUS
D. Ubuntu

Answer: B

Question No : 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 No : 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 No : 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

Question No : 9 - (Topic 11)

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

Answer: A

Question No : 10 - (Topic 11)

Which list identifies the possible types of alerts that the Sourcefire System can generate as notification of events or policy violations?

A. logging to database, SMS, SMTP, and SNMP
B. logging to database, SMTP, SNMP, and PCAP
C. logging to database, SNMP, syslog, and email
D. logging to database, PCAP, SMS, and SNMP

Answer: C