Cisco

Exam Questions 500-285

SSFIPS Securing Cisco Networks with Sourcefire Intrusion Prevention System
1. When configuring FireSIGHT detection, an administrator would create a network discovery policy and set the action to "discover". Which option is a possible type of discovery?

A. host
B. IPS event
C. anti-malware
D. networks

Answer: A

2. FireSIGHT recommendations appear in which layer of the Policy Layers page?

A. Layer Summary
B. User Layers
C. Built-In Layers
D. FireSIGHT recommendations do not show up as a layer.

Answer: C

3. 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

4. Which statement is true when network traffic meets the criteria specified in a correlation rule?

A. Nothing happens, because you cannot assign a group of rules to a correlation policy.
B. The network traffic is blocked.
C. The Defense Center generates a correlation event and initiates any configured responses.
D. An event is logged to the Correlation Policy Management table.

Answer: C

5. In addition to the discovery of new hosts, FireSIGHT can also perform which function?

A. block traffic
B. determine which users are involved in monitored connections
C. discover information about users
D. route traffic

Answer: B

6. Context Explorer can be accessed by a subset of user roles. Which predefined user role is valid for FireSIGHT event access?

A. Administrator
B. Intrusion Administrator
C. Maintenance User
D. Database Administrator

Answer: A

7. What does the whitelist attribute value "not evaluated" indicate?

A. The host is not a target of the whitelist.
B. The host could not be evaluated because no profile exists for it.
C. The whitelist status could not be updated because the correlation policy it belongs to is not enabled.
D. The host is not on a monitored network segment.

Answer: A

8. Which statement regarding user exemptions is true?
A. Non-administrators can be made exempt on an individual basis.
B. Exempt users have a browser session timeout restriction of 24 hours.
C. Administrators can be exempt from any browser session timeout value.
D. By default, all users cannot be exempt from any browser session timeout value.

Answer: A
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

500-285 Practice Exam Features:

* 500-285 Questions and Answers Updated Frequently
* 500-285 Practice Questions Verified by Expert Senior Certified Staff
* 500-285 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 500-285 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 500-285 Practice Test Here