



Vendor: Cisco

Exam Code: 500-285

Exam Name: Securing Cisco Networks with Sourcefire
Intrusion Prevention System

Version: DEMO

QUESTION 1

Which option is true of the Packet Information portion of the Packet View screen?

- A. provides a table view of events
- B. allows you to download a PCAP formatted file of the session that triggered the event
- C. displays packet data in a format based on TCP/IP layers
- D. shows you the user that triggered the event

Answer: C

QUESTION 2

Which option is used to implement suppression in the Rule Management user interface?

- A. Rule Category
- B. Global
- C. Source
- D. Protocol

Answer: C

QUESTION 3

When you are editing an intrusion policy, how do you know that you have changes?

- A. The Commit Changes button is enabled.
- B. A system message notifies you.
- C. You are prompted to save your changes on every screen refresh.
- D. A yellow, triangular icon displays next to the Policy Information option in the navigation panel.

Answer: D

QUESTION 4

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

QUESTION 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

QUESTION 6

FireSIGHT uses three primary types of detection to understand the environment in which it is deployed. Which option is one of the detection types?

- A. protocol layer
- B. application
- C. objects
- D. devices

Answer: B

QUESTION 7

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

QUESTION 8

Which option is derived from the discovery component of FireSIGHT technology?

- A. connection event table view
- B. network profile
- C. host profile
- D. authentication objects

Answer: C

QUESTION 9

The IP address ::/0 is equivalent to which IPv4 address and netmask?

- A. 0.0.0.0
- B. 0.0.0.0/0
- C. 0.0.0.0/24
- D. The IP address ::/0 is not valid IPv6 syntax.

Answer: B

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>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives[®]

10% Discount Coupon Code: ASTR14