

Free Share Lead2pass Cisco 500-285 Exam Dumps and Questions

Lead2pass new Cisco 500-285 study guides that you use have been rigorously tested by International experts. Choose Lead2pass both save your time and money . And our products will satisfy you. 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 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 Lead2pass 500-285 PDF Format Exam Questions and Answers provides: 100% Accurate and Verified Answers. Comprehensive explanations of all the questions (when available). Questions with exhibits (when available). Printable PDF format questions and answers. Complete coverage of exam objectives. <http://www.lead2pass.com/500-285.html>