500-285$^{\text{Q\&As}}$

Securing Cisco Networks with FireSIGHT Intrusion Prevention System (SSFIPS)

Pass Cisco 500-285 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/500-285.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which event source can have a default workflow configured?

A. user events

B. discovery events

C. server events

D. connection events

Correct Answer: B

QUESTION 2

Which option is true when configuring an access control rule?

A. You can use geolocation criteria to specify source IP addresses by country and continent, as well as destination IP addresses by country and continent.

B. You can use geolocation criteria to specify destination IP addresses by country but not source IP addresses.

C. You can use geolocation criteria to specify source and destination IP addresses by country but not by continent.

D. You can use geolocation criteria to specify source and destination IP addresses by continent but not by country.

Correct Answer: A

QUESTION 3

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.

Correct Answer: B

QUESTION 4

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

Correct Answer: C

QUESTION 5

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.

Correct Answer: A

QUESTION 6

Which interface type allows for bypass mode?

A. inline

B. switched

C. routed

D. grouped

Correct Answer: A

QUESTION 7

Which policy controls malware blocking configuration?

A. file policy

B. malware policy

C. access control policy

D. IPS policy

Correct Answer: A

QUESTION 8

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

Correct Answer: A

QUESTION 9

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

Correct Answer: B

QUESTION 10

The gateway VPN feature supports which deployment types?

A. SSL and HTTPS

B. PPTP and MPLS

C. client and route-based

D. point-to-point, star, and mesh

Correct Answer: D