500-285 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.pass4itsure.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

A context box opens when you click on an event icon in the Network File Trajectory map for a file. Which option is an element of the box?

A. Scan

B. Application Protocol

C. Threat Name

D. File Name

Correct Answer: B

QUESTION 2

The collection of health modules and their settings is known as which option?

A. appliance policy

B. system policy

C. correlation policy

D. health policy

Correct Answer: D

QUESTION 3

One of the goals of geolocation is to identify which option?

A. the location of any IP address

B. the location of a MAC address

C. the location of a TCP connection

D. the location of a routable IP address

Correct Answer: D

QUESTION 4

Which statement describes the meaning of a red health status icon?

A. A critical threshold has been exceeded.

B. At least one health module has failed.

C. A health policy has been disabled on a monitored device.

D. A warning threshold has been exceeded.

Correct Answer: A

QUESTION 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

Correct Answer: B

QUESTION 6

Other than navigating to the Network File Trajectory page for a file, which option is an alternative way of accessing the network trajectory of a file?

A. from Context Explorer

B. from the Analysis menu

C. from the cloud

D. from the Defense Center

Correct Answer: A

QUESTION 7

What does packet latency thresholding measure?

A. the total elapsed time it takes to process a packet

B. the amount of time it takes for a rule to process

C. the amount of time it takes to process an event

D. the time span between a triggered event and when the packet is dropped

Correct Answer: A

QUESTION 8

Which statement is true in regard to the Sourcefire Security Intelligence lists?

A. The global blacklist universally allows all traffic through the managed device.

B. The global whitelist cannot be edited.

C. IP addresses can be added to the global blacklist by clicking on interactive graphs in Context Explorer.

D. The Security Intelligence lists cannot be updated.

Correct Answer: C

QUESTION 9

Which option is one of the three methods of updating the IP addresses in Sourcefire Security Intelligence?

A. subscribe to a URL intelligence feed

B. subscribe to a VRT

C. upload a list that you create

D. automatically upload lists from a network share

Correct Answer: C

QUESTION 10

Controlling simultaneous connections is a feature of which type of preprocessor?

A. rate-based attack prevention

B. detection enhancement

C. TCP and network layer preprocessors

D. performance settings

Correct Answer: A