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.leads4pass.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

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.

Correct Answer: D

QUESTION 2

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

QUESTION 3

What are the two categories of variables that you can configure in Object Management?

A. System Default Variables and FireSIGHT-Specific Variables

B. System Default Variables and Procedural Variables

C. Default Variables and Custom Variables

D. Policy-Specific Variables and Procedural Variables

Correct Answer: C

QUESTION 4

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 5

Which Sourcefire feature allows you to send traffic directly through the device without inspecting it?

A. fast-path rules

B. thresholds or suppressions

C. blacklist

D. automatic application bypass

Correct Answer: A

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

Suppose an administrator is configuring an IPS policy and attempts to enable intrusion rules that require the operation of the TCP stream preprocessor, but the TCP stream preprocessor is turned off. Which statement is true in this situation?

A. The administrator can save the IPS policy with the TCP stream preprocessor turned off, but the rules requiring its operation will not function properly.

B. When the administrator enables the rules and then attempts to save the IPS policy, the administrator will be prompted to accept that the TCP stream preprocessor will be turned on for the IPS policy.

C. The administrator will be prevented from changing the rule state of the rules that require the TCP stream preprocessor until the TCP stream preprocessor is enabled.

D. When the administrator enables the rules and then attempts to save the IPS policy, the administrator will be prompted to accept that the rules that require the TCP stream preprocessor will be turned off for the IPS policy.

Correct Answer: B

QUESTION 8

Stacking allows a primary device to utilize which resources of secondary devices?

A. interfaces, CPUs, and memory

B. CPUs and memory

C. interfaces, CPUs, memory, and storage

D. interfaces and storage

Correct Answer: B

QUESTION 9

Which option transmits policy-based alerts such as SNMP and syslog?

A. the Defense Center

B. FireSIGHT

C. the managed device

D. the host

Correct Answer: C

QUESTION 10

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.

Correct Answer: C