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.lead4pass.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 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 2

Which interface type allows for VLAN tagging?

A. inline

B. switched

C. high-availability link

D. passive

Correct Answer: B

QUESTION 3

Which list identifies the possible types of alerts that the Sourcefire System can generate as notification of events or policy violations?

A. logging to database, SMS, SMTP, and SNMP

B. logging to database, SMTP, SNMP, and PCAP

C. logging to database, SNMP, syslog, and email

D. logging to database, PCAP, SMS, and SNMP

Correct Answer: C

QUESTION 4

Which option is a remediation module that comes with the Sourcefire System?

A. Cisco IOS Null Route

B. Syslog Route

C. Nmap Route Scan

D. Response Group

Correct Answer: A

QUESTION 5

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 6

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

QUESTION 7

Context Explorer can be accessed by a subset of user roles. Which predefined user role is not valid for FireSIGHT event access?

A. Administrator

B. Intrusion Administrator

C. Security Analyst

D. Security Analyst (Read-Only)

Correct Answer: B

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

Correct Answer: C

QUESTION 9

Which interface type allows for bypass mode?

A. inline

B. switched

C. routed

D. grouped

Correct Answer: A

QUESTION 10

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 11

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 12

Which option is true regarding the $HOME_NET variable?

A. is a policy-level variable

B. has a default value of "all"

C. defines the network the active policy protects

D. is used by all rules to define the internal network

Correct Answer: C

QUESTION 13

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 14

Which statement represents detection capabilities of the HTTP preprocessor?

A. You can configure it to blacklist known bad web servers.

B. You can configure it to normalize cookies in HTTP headers.

C. You can configure it to normalize image content types.

D. You can configure it to whitelist specific servers.

Correct Answer: B

QUESTION 15

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.

Correct Answer: C

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.lead4pass.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: