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.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

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 2

Which interface type allows for VLAN tagging?

A. inline

B. switched

C. high-availability link

D. passive

Correct Answer: B

QUESTION 3

Which statement is true when adding a network to an access control rule?

A. You can select only source networks.

B. You must have preconfigured the network as an object.

C. You can select the source and destination networks or network groups.

D. You cannot include multiple networks or network groups as sources or destinations.

Correct Answer: C

QUESTION 4

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 5

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

QUESTION 6

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

QUESTION 7

Correlation policy rules allow you to construct criteria for alerting on very specific conditions. Which option is an example of such a rule?

A. testing password strength when accessing an application

B. limiting general user access to administrative file shares

C. enforcing two-factor authentication for access to critical servers

D. issuing an alert if a noncompliant operating system is detected or if a host operating system changes to a noncompliant operating system when it was previously profiled as a compliant one

Correct Answer: D

QUESTION 8

When configuring an LDAP authentication object, which server type is available?

A. Microsoft Active Directory

B. Yahoo

C. Oracle

D. SMTP

Correct Answer: A

QUESTION 9

Which interface type allows for bypass mode?

A. inline

B. switched

C. routed

D. grouped

Correct Answer: A

QUESTION 10

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 11

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 12

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 13

Which option is a valid whitelist evaluation value?

A. pending

B. violation

C. semi-compliant

D. not-evaluated

Correct Answer: D

QUESTION 14

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.

Correct Answer: B

QUESTION 15

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