Vendor: Cisco

Exam Code:500-285

Exam Name: Securing Cisco Networks with FireSIGHT Intrusion Prevention System (SSFIPS)

Version: Demo

QUESTION 1

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 2

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 3

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 4

Remote access to the Defense Center database has which characteristic?

A. read/write

B. read-only

C. Postgres

D. Estreamer

Correct Answer: B

QUESTION 5

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 6

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 7

When adding source and destination ports in the Ports tab of the access control policy rule editor, which restriction is in place?

A. The protocol is restricted to TCP only.

B. The protocol is restricted to UDP only.

C. The protocol is restricted to TCP or UDP.

D. The protocol is restricted to TCP and UDP.

Correct Answer: C

QUESTION 8

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 9

Which option describes the two basic components of Sourcefire Snort rules?

A. preprocessor configurations to define what to do with packets before the detection engine sees them, and detection engine configurations to define exactly how alerting is to take place

B. a rule statement characterized by the message you configure to appear in the alert, and the rule body that contains all of the matching criteria such as source, destination, and protocol

C. a rule header to define source, destination, and protocol, and the output configuration to determine which form of output to produce if the rule triggers

D. a rule body that contains packet-matching criteria or options to define where to look for content in a packet, and a rule header to define matching criteria based on where a packet originates, where it is going, and over which protocol

Correct Answer: D

QUESTION 10

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 11

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 12

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