642-627 Q&As

Implementing Cisco Intrusion Prevention System v7.0

Pass Cisco 642-627 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/642-627.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

What are the three valid options for configuring Cisco SensorBase participation? (Choose three.)

A. off

B. test

C. manual

D. automatic

E. partial

F. full

Correct Answer: AEF

QUESTION 2

What is a best practice to follow before tuning a Cisco IPS signature?

A. Disable all the alert actions on the signature to be tuned.

B. Disable the signature to be tuned.

C. Create a clone of the signature to be tuned.

D. Increase the number of events required to trigger the signature to be tuned.

E. Decrease the attention span (maximum inter-event interval) of the signature to be tuned

Correct Answer: C

http://www.cisco.com/web/about/security/intelligence/ips_custom_sigs_pdf.pdf, specifically:

Cloning a Signature

Administrators often find the need to modify a signature to meet the needs of a specific network, such as to reduce false positives or false negatives.

In such cases, the first approach should be to fine tune signature parameters such as event action filters and override policies. If these tunings are not sufficient, the last action that is available is to modify a signature. By default, signature

parameters such as the regular expression cannot be modified.

The signature must first be cloned in order to modify such signature parameters. The original signature can be retired or disabled if it is determined that it is no longer required.

ORIGINAL FROM CHIP:

Still Doubt here. 100% certain C is wrong.

A is best answer with B also possible.

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd8066d265.html

Official Guide - Chapter 13 Quiz - When tuning signatures it is recommended Answer: By removing harmful actions during the tuning phase we can have visibility.....without interfering with normal traffic "Do no harm" approach.

QUESTION 3

Refer to the exhibit of a Cisco IPS CLI configuration, which statement is true?

A. The IPS administrator should be able to use Telnet to connect to the IP appliance 172.26.26.1 IP address.

B. The IPS administrator should be able to use Telnet to connect to the IP appliance 172.26.26.2 IP address.

C. The IP appliance default gateway IP address is 172.26.26.1.

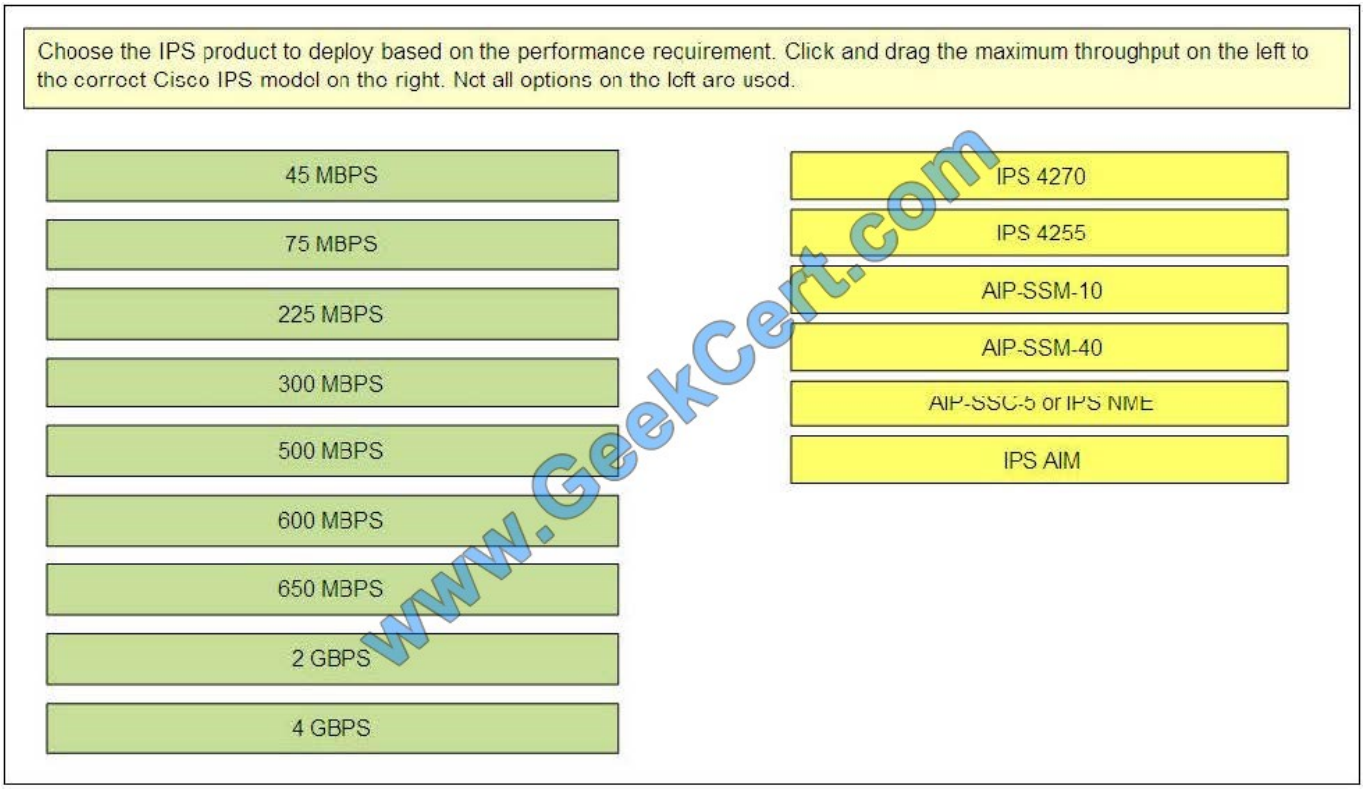
D. The IPS administrator will not be able to use Telnet to connect to the IP appliance.

E. The IP appliance primary IP address is 172.26.26.1 with a secondary IP address of 172.26.26.2.

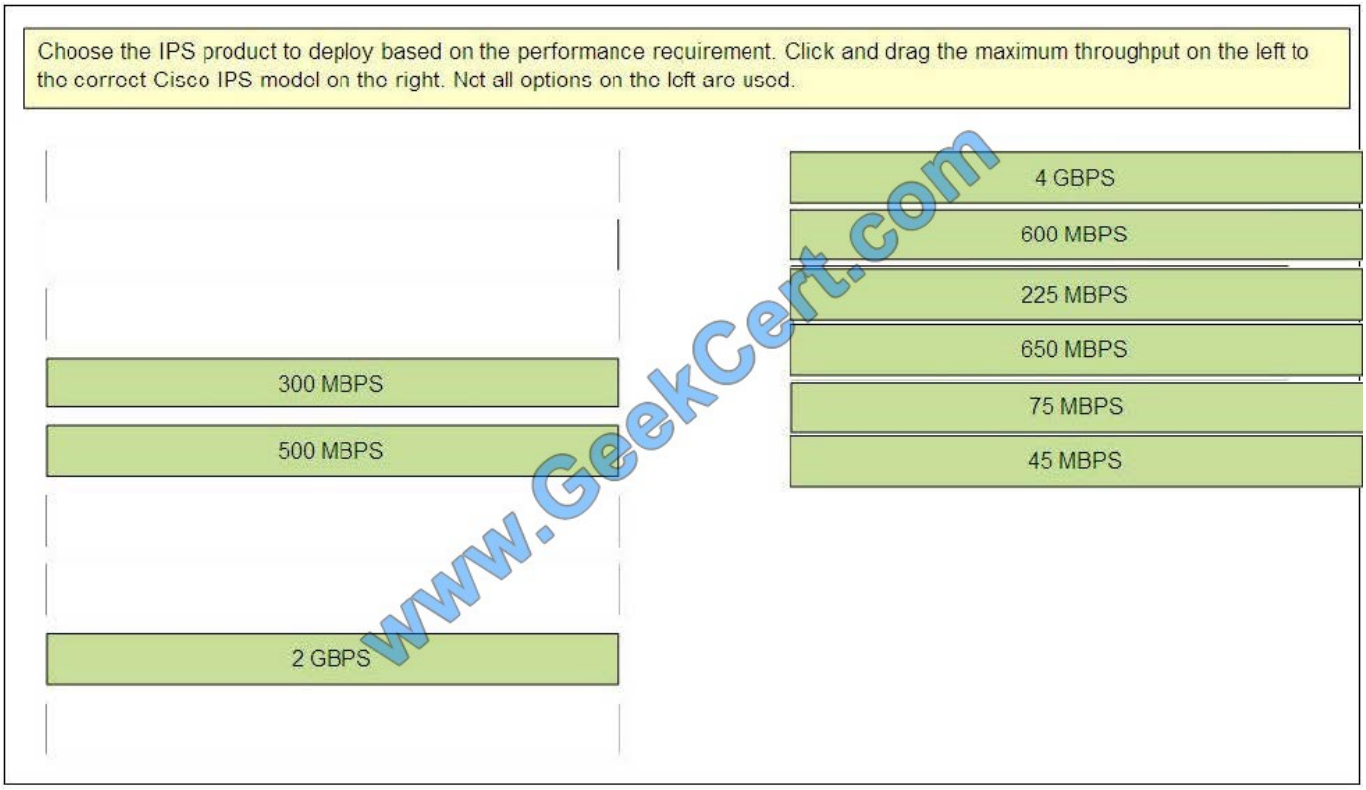
Correct Answer: D

QUESTION 4

Select and Place:



Correct Answer:



QUESTION 5

The AIP-SSM CLI can be accessed from the ASA CLI by using which command?

A. connect

B. telnet

C. hw-module

D. session

E. module

Correct Answer: D

http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/ssm.html#wp1096676