



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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





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?

```
!
service host
network<-settings
host-ip 172.26.26.1/24,172.26.26.2
host-name ips
telnet-option enabled
access-list 172.26.26.2/32
exit
exit
!
```

- 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:



Choose the IPS product to deploy based on the performance requirement. Click and drag the maximum throughput on the left to the correct Cisco IPS model on the right. Not all options on the left are used.

- 45 MBPS
- 75 MBPS
- 225 MBPS
- 300 MBPS
- 500 MBPS
- 600 MBPS
- 650 MBPS
- 2 GBPS
- 4 GBPS

- IPS 4270
- IPS 4255
- AIP-SSM-10
- AIP-SSM-40
- AIP-SSC-5 or IPS NME
- IPS AIM

Correct Answer:

Choose the IPS product to deploy based on the performance requirement. Click and drag the maximum throughput on the left to the correct Cisco IPS model on the right. Not all options on the left are used.

- 300 MBPS
- 500 MBPS
- 2 GBPS

- 4 GBPS
- 600 MBPS
- 225 MBPS
- 650 MBPS
- 75 MBPS
- 45 MBPS

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>

[642-627 PDF Dumps](#)

[642-627 VCE Dumps](#)

[642-627 Study Guide](#)



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.geekcert.com/allproducts>

Need Help

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



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © geekcert, All Rights Reserved.