

Exam : Cisco 642-533

**Title : Implementing Cisco
Intrusion Prevention
System (IPS)**

Version : Demo

Important Note, Please Read Carefully

Other TestInside products

[All TestInside.com IT Exam Products](#)

Our products of Offline Testing Engine

Use the offline Testing engine product to practice the questions in an exam environment.

Build a foundation of knowledge which will be useful also after passing the exam.

[TestInside Testing Engine](#)

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at TestInside and update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to <http://www.TestInside.com>
2. Log in the **Member Center**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

Feedback

If you spot a possible improvement then please let us know. We always interested in improving product quality.

Feedback should be send to sales(at)TestInside.com. You should include the following: Exam number, version, page number, question number, and your login Account.

Our experts will answer your mail promptly.

Explanations

This product does not include explanations at the moment. If you are interested in providing explanations for this exam, please contact sales(at)TestInside.com.

1. Refer to the exhibit. Which three statements correctly describe the configuration depicted in this Cisco IDM virtual sensors list? (Choose three.)

Virtual Sensors

The sensor monitors traffic that traverses interfaces, interface pairs, or VLAN pairs assigned to a virtual sensor. You can create a new virtual sensor by clicking Add. You can edit or delete an existing virtual sensor by selecting the row(s) and clicking Edit or Delete.

Name	Assigned Interfaces (or Pairs)	Sig Definition Policy	Event Action Rules Policy	Anomaly Detection Policy
vs0	GigabitEthernet0/2.0 (Promiscuous Interface) GigabitEthernet0/3.0 (Promiscuous Interface)	sig0	rules0	ad0
vs1	GigabitEthernet0/0.1 (Inline VLAN Pair: 102 <-> 201)	sig1	rules1	ad1

- A. inline dropping of packets can occur on the Gig0/0.1 sub-interface
- B. sub-interfaces Gig0/2.0 and Gig0/3.0 are operating in IPS mode
- C. the Cisco IPS Sensor appliance is configured for promiscuous (IDS) and inline (IPS) mode simultaneously
- D. the vs1 virtual sensor is misconfigured for inline operations since only one sub-interface is assigned to vs1
- E. inline dropping of packets can occur on the Gig0/2.0 sub-interface or Gig0/3.0 sub-interface or both
- F. the vs1 virtual sensor is operating inline between VLAN 102 and VLAN 201

Answer: ACF

2. Which two statements correctly describe Cisco ASA AIP-SSM based on Cisco IPS 6.0 and the ASA 7.x software release? (Choose two.)

- A. It supports up to four virtual sensors.
- B. It supports inline VLAN pairs.
- C. Its command and control interface is Gig0/0.
- D. It requires two physical interfaces to operate in inline mode.
- E. It does not have console port access.
- F. It has two sensing interfaces.

Answer: CE

3. A user with which user account role on a Cisco IPS Sensor can log into the native operating system shell for advanced troubleshooting purposes when directed to do so by Cisco TAC?

- A. administrator
- B. operator
- C. viewer
- D. service
- E. root
- F. super

Answer: D

4. What are the three roles of the Cisco IPS Sensor interface? (Choose three.)

- A. alternate TCP reset
- B. blocking
- C. command and control
- D. sensing (monitoring)
- E. logging
- F. bypass

Answer: ACD

5. In Cisco IDM, the Configuration > Sensor Setup > SSH > Known Host Keys screen is used for what purpose?

- A. to enable communications with the Master Blocking Sensor
- B. to enable communications with a blocking device
- C. to enable management hosts to access the Cisco IPS Sensor
- D. to regenerate the Cisco IPS Sensor SSH host key
- E. to regenerate the Cisco IPS Sensor SSL RSA key pair

Answer: B

6. Which three of these steps are used to initialize and verify the Cisco ASA AIP-SSM? (Choose three.)

- A. connect a management station directly to the AIP-SSM console port via a serial cable
- B. use the ASA#session 1 command to access the AIP-SSM CLI
- C. use the ASA#show module command to verify the AIP-SSM status

- D. access the Cisco IDM from a management station using `http://sensor-ip-address`
- E. use the `sensor#setup` command to configure the basic sensor settings
- F. use the `ASA#telnet sensor-ip-address` command to access the AIP-SSM to setup the basic configuration on the sensor

Answer: BCE

7. In which three of these ways can you achieve better Cisco IPS Sensor performance? (Choose three.)
- A. enable all anti-evasive measures to reduce noise
 - B. place the Cisco IPS Sensor behind a firewall
 - C. always enable unidirectional capture
 - D. disable unneeded signatures
 - E. have multiple Cisco IPS Sensors in the path and configure them to detect different types of events
 - F. enable selective packet capture using VLAN ACL on the Cisco IPS 4200 Series Sensors

Answer: BDE

8. Select the two correct general Cisco IPS Sensor tuning recommendations if the environment consists exclusively of Windows servers. (Choose two.)
- A. use "NT" IP fragment reassembly mode
 - B. use "Windows" TCP stream reassembly mode
 - C. disable deobfuscation for all HTTP signatures
 - D. enable all IIS signatures
 - E. enable all NFS signatures
 - F. enable all RPC signatures

Answer: AD

9. Which of the following statements best describes how IP logging should be used?
- A. only be used temporarily for such purposes as attack confirmation, damage assessment, or the collection of forensic evidence, because of its impact on performance
 - B. be used sparingly because there is a 4-GB limit on the amount of data that can be logged
 - C. always be enabled since it uses a FIFO buffer on the Cisco IPS Sensor flash memory

- D. be used to automatically correlate events with Cisco Security MARS for incident investigations
- E. only be used when you are also using inline IPS mode

Answer: A

10. Which type of signature engine is best suited for creating custom signatures that inspect data at Layer 5 and above?

- A. ATOMIC
- B. String
- C. Sweep
- D. Service
- E. AIC
- F. Flood

Answer: D

Testinside

Testinside.com was founded in 2002. The safer,easier way to help you pass any IT Certification exams . We provide high quality IT Certification exams practice questions and answers(Q&A). Especially [Adobe](#), [Apple](#), [Citrix](#), [Comptia](#), [EMC](#), [HP](#), [Juniper](#), [LPI](#), [Nortel](#), [Oracle](#), [SUN](#), [Vmware](#) and so on. And help you pass any IT Certification exams at the first try.

English	<u>http://www.testinside.com</u>
Chinese (Traditional)	<u>http:// www.testinside.net</u>
Chinese (Simplified)	<u>http:// www.testinside.cn</u>