



[Cisco 642-533](#)

Exam Name: *Implementing Cisco Intrusion Prevention System (IPS)*

Q & A : 136 Q&As

Pdf Demo

Quality and Value for the 642-533 Exam

[Just4Exams Practice Exams](#) for Cisco VPN and Security 642-533 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

100% Guarantee to Pass Your 642-533 Exam

If you do not pass the VPN and Security 642-533 exam on your first attempt using our Just4Exams **642-533 testing engine and pdf study guide**, we will give you a FULL REFUND of your purchasing fee.

Downloadable, Interactive 642-533 Testing engines and PDF Version

Our Exam Preparation Material provides you everything you will need to take a [VPN and Security certification](#) examination. Details are researched and produced by [Cisco Certification](#) Experts who are constantly using industry experience to produce precise, and logical.

Free 642-533 Exams:

This is demo only, this pdf do not include the questions and answers picture

Exam : Cisco 642-533

Title : Implementing Cisco Intrusion Prevention System (IPS)

1. 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

2. 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

3. 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

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

- 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

5. 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

6. 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

7. 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

8. 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

9. 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

10. 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

More [642-533 Braindumps](#) Information

Related 642-533 Exams

642-533 646-301 642-511 642-541

Other Cisco Exams

350-021 642-243 642-502 642-821 642-552
646-561 642-511 642-359 646-223 642-531
642-112 642-654 646-056 642-452 642-973
640-861 646-671 642-241 642-515 642-681