# 642-532

## Cisco

### *Implementing Cisco Intrusion Prevention Systems*

*Visit: http://www.pass4sureofficial.com/exams.asp?examcode=642-532*

*Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your 642-532 exam in first attempt, but also you can get a high score to acquire Cisco certification.*

*If you use pass4sureofficial 642-532 Certification questions and answers, you will experience actual 642-532 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Cisco exam prep covers over 95% of the questions and answers that may be appeared in your 642-532 exam. Every point from pass4sure 642-532 PDF, 642-532 review will help you take Cisco 642-532 exam much easier and become Cisco certified. All the Questions/Answers are taken from real exams.*

*Here's what you can expect from the Pass4sureOfficial Cisco 642-532 course:*

** Up-to-Date Cisco 642-532 questions taken from the real exam.*
** 100% correct Cisco 642-532 answers you simply can't find in other 642-532 courses.*
** All of our tests are easy to download. Your file will be saved as a 642-532 PDF.*
** Cisco 642-532 brain dump free content featuring the real 642-532 test questions.*

*Cisco 642-532 certification exam is of core importance both in your Professional life and Cisco certification path. With Cisco certification you can get a good job easily in the market and get on your path for success. Professionals who passed Cisco 642-532 exam training are an absolute favorite in the industry. You will pass Cisco 642-532 certification test and career opportunities will be open for you.*

**QUESTION:** 1
A new IDSM2 module was installed in the Companys network. Which of the following features regarding the IDSM2 is true?

A. IDSM2 needs a separate management package
B. IDSM2 is limited to 62 signatures
C. IDSM2 can drop offending packets
D. IDSM2 makes use of the same code as the network appliance
E. None of the above

**Answer:** D

**Explanation:**
IDSM-2 provides the following capabilities or features:
- Merged switching and security into a single chassis
- Ability to monitor multiple VLANs
- Does not impact switch performance
- Attacks and signatures equal to appliance sensor
- Uses the same code base of the appliance sensor
- Support for improved management techniques such as IDM

**Reference:**
Cisco Press CCSP CSIDS Guide, 2nd edition page 199

**QUESTION:** 2
A new NM-CIDS module is being inserted into the Companys network. Which versions of Cisco IOS software is needed to support the NM-CIDS module?

A. 3.1 and above.
B. 4.1 and above
C. 4.0 and above
D. 2.0 and above
E. None of the above

**Answer:** B

**Explanation:**

| Series | Devices Supported | Software |
|---|---|---|
| Cisco Network IDS Sensor Appliances | NRS-2E | IDS 3.0 and IDS 3.1 |
| | NRS-2FE | IDS 3.0 and IDS 3.1 |
| | NRS-TR | IDS 3.0 and IDS 3.1 |
| | NRS-SFDDI | IDS 3.0 and IDS 3.1 |
| | NRS-DFDDI | IDS 3.0 and IDS 3.1 |
| | IDS-4210 | IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1 |
| | IDS-4215 | IDS 4.1 |
| | IDS-4220 | IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1 |
| | IDS-4230 | IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1 |
| | IDS-4235 | IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1 |
| | IDS-4250-TX and IDS-4250-SX | IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1 |
| | IDS-4250-XL | IDS 4.0 and IDS 4.1 |
| Cisco Switch IDS Sensor Modules | IDSM | IDSM 3.0(5) and IDSM 3.0(6) |
| | IDSM2 | IDS 4.0 and IDS 4.1 |
| Cisco IOS Router IDS Sensor Module | NM-CIDS | IDS 4.1 |

**QUESTION:** 3
A new Companys IPS sensor is being configured for inline operation. Which three steps must you perform to prepare sensor interfaces for inline operations? (Choose three)

A. Disable all interfaces except the inline pair
B. Add the inline pair to the default virtual sensor
C. Enable two interfaces for the pair
D. Disable any interfaces that are operating in promiscuous mode.
E. Create the interface pair
F. Configure an alternate TCP-reset interface.

**Answer:** B, C, E

**Explanation:**
Operating in inline interface mode puts the IPS directly into the traffic flow and affects packet-forwarding rates making them slower by adding latency. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service.Not only is the inline device processing information on layers 3 and 4, but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (layers 3 to 7). This deeper analysis lets the system identify and stop and/or block attacks that would normally pass through a traditional firewall device.In inline interface mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.To configure the interfaces for inline operation, you will need to create the interface pair, enable the two interfaces, and add the inline interface pair to the default sensor.

**Reference:**
Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1, Cisco Documentation, page 5-11.

**QUESTION:** 4
The Companys security administrator is determining whether to configure a new sensor in inline or promiscuous mode. What are three differences between inline and promiscuous sensor functionality? (Choose three)

A. A sensor that is operating in inline mode can drop the packet that triggers a signature before it reaches its target, but a sensor that is operating in promiscuous mode cannot.
B. A sensor that is operating in inline mode supports more signatures than a sensor that operates in promiscuous mode.
C. Deny actions are available only to inline sensors, but blocking actions are available only to promiscuous mode sensors.
D. A sensor that is operating in promiscuous mode can perform TCP resets, but a sensor that is operating in inline mode cannot.

E. Inline operation provides more protection from Internet worms than promiscuous mode does. F. Inline operation provides more protection from atomic attacks than promiscuous mode does.

**Answer:** A, E, F

**Explanation:**
In promiscuous mode, packets do not flow through the sensor. The sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating in promiscuous mode is that the sensor does not affect the packet flow with the forwarded traffic. The disadvantage of operating in promiscuous mode, however, is the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response actions implemented by promiscuous sensor devices are post-event responses and often require assistance from other networking devices, for example, routers and firewalls, to respond to an attack. While such response actions can prevent some classes of attacks, in atomic attacks the single packet has the chance of reaching the target system before the promiscuous-based sensor can apply an ACL modification on a managed device (such as a firewall, switch, or router).Operating in inline interface mode puts the IPS directly into the traffic flow and affects packet-forwarding rates making them slower by adding latency. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service. Not only is the inline device processing information on layers 3 and 4, but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (layers 3 to7). This deeper analysis lets the system identify and stop and/or block attacks that would normally pass through a traditional firewall device.In inline interface mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.

**Reference:**
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008055

**QUESTION:** 5
New Cisco IPS sensors are being deployed within the Companys network. Which of the following are appropriate installation points for a Cisco IPS sensor? (Choose two)

A. On publicly accessible servers
B. On critical network servers
C. At network entry points
D. On user desktops

## Pass4SureOfficial.com Lifetime Membership Features;

- Pass4SureOfficial Lifetime Membership Package includes over **2500** Exams.
- **All** exams Questions and Answers are included in package.
- **All** Audio Guides are included **free** in package.
- **All** Study Guides are included **free** in package.
- **Lifetime** login access.
- Unlimited download, no account expiry, no hidden charges, just one time $99 payment.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) downloads
http://www.pass4sureofficial.com/allexams.asp

View list of All Study Guides (SG) downloads
http://www.pass4sureofficial.com/study-guides.asp

View list of All Audio Exams (AE) downloads
http://www.pass4sureofficial.com/audio-exams.asp

Download All Exams Samples
http://www.pass4sureofficial.com/samples.asp

To purchase $99 Lifetime Full Access Membership click here
http://www.pass4sureofficial.com/purchase.asp

| | | | | | | |
|---|---|---|---|---|---|---|
| 3COM | CompTIA | Filemaker | IBM | LPI | OMG | Sun |
| ADOBE | ComputerAssociates | Fortinet | IISFA | McAfee | Oracle | Sybase |
| APC | CWNP | Foundry | Intel | McData | PMI | Symantec |
| Apple | DELL | Fujitsu | ISACA | Microsoft | Polycom | TeraData |
| BEA | ECCouncil | GuidanceSoftware | ISC2 | Mile2 | RedHat | TIA |
| BICSI | EMC | HDI | ISEB | NetworkAppliance | Sair | Tibco |
| CheckPoint | Enterasys | Hitachi | ISM | Network-General | SASInstitute | TruSecure |
| Cisco | ExamExpress | HP | Juniper | Nokia | SCP | Veritas |
| Citrix | Exin | Huawei | Legato | Nortel | See-Beyond | Vmware |
| CIW | ExtremeNetworks | Hyperion | Lotus | Novell | SNIA | |