# Cisco IPS AIM


## Abstract

The Cisco® IPS Advanced Integration Module (AIM) for Cisco modular integrated services routers integrates a high-performance, feature-rich intrusion prevention system (IPS) into the operations of the hosting router. A port of Cisco industry-leading IPS sensors, the Cisco IPS AIM performs intrusion prevention by running Cisco IPS Software Version 6.0, providing feature parity with Cisco IPS sensors and other devices.


## Cisco IPS AIM Deployment, Benefits, and Capabilities

The Cisco IPS AIM installs into the AIM slot in the modular Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers. The AIM slot is an internal slot with no external interface capabilities. It functions in a coprocessor capability, offloading computationally intensive operations from the central CPU of the router, leaving additional CPU capacity for forwarding packets and other services.

The Cisco IPS AIM has its own dedicated CPU, memory, and storage architecture, discrete from the main operations of the router, allowing the card to offload all IPS inspection activities, store a full set of signature files, and send inspection results back to the router. The card is a separate entity within the router, allowing for independent management and configuration. By running Cisco IPS Software Version 6.0, the Cisco IPS AIM supports all signatures and features of the Cisco IPS 4200 Series appliances. Both promiscuous mode and inline mode are supported by Cisco IPS AIM.

## Cisco IPS AIM vs. Cisco IDS Network Module vs. Cisco IOS IPS Deployment Guidelines

Cisco IOS® IPS, the Cisco IDS Network Module, and the Cisco IPS AIM are all part of the Cisco Intrusion Prevention Solution. You can deploy all three technologies in the same network, but you can deploy only one in a single router. Because different IPS engines are not aware of each other's activities in the router, using more than one in a single router could cause each engine to react differently from the others when a signature match occurs. There is currently no mechanism for fail-back from one service to another.

Cisco IOS IPS is a Cisco IOS Software application that provides signature-based IPS. Packaged in a Cisco IOS Advanced Security image or later feature set, it is available on all Cisco integrated services router platforms beginning with the Cisco 871 Integrated Services Router. In Cisco IOS Software Release 12.4(11)T and later T-train releases, Cisco IOS IPS uses the Cisco IPS Version 5.0 signature format also used in the Cisco IPS 6.0 inspection engines running on standalone Cisco IPS appliances and modules. More than 2000 signatures are available for Cisco IOS IPS, but you need to deploy only a subset of these signatures simultaneously. Because Cisco IOS IPS is a Cisco IOS Software feature, it runs within the shared memory pool of the router and inspection is performed by the router CPU. Because active signatures are loaded in the main memory of the router, you may need to install additional memory in order to load more signatures. Even with additional memory, Cisco IOS IPS cannot load all supported signatures at the same time.

The Cisco IDS Network Module is a network-module version of the Cisco IPS 4200 Series appliances. Supported in Cisco 2811 Integrated Services Routers and later, the IDS network module runs Cisco IPS Version 5.0 and 6.0, but you can deploy it only in promiscuous mode. In promiscuous mode packets do not flow through the IPS; 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 IPS does not affect the packet flow with the forwarded traffic. The disadvantage of operating in promiscuous mode, however, is that the IPS 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 IPS devices are postevent responses such as connection shunning, and they often require assistance from other networking devices (for example, routers and firewalls) to respond to an attack. Although such response actions can prevent some classes of attacks, for atomic attacks the single packet has the potential to reach the target system before the promiscuous-based sensor can apply an access-control-list (ACL) modification on a managed device (such as a firewall, switch, or router).

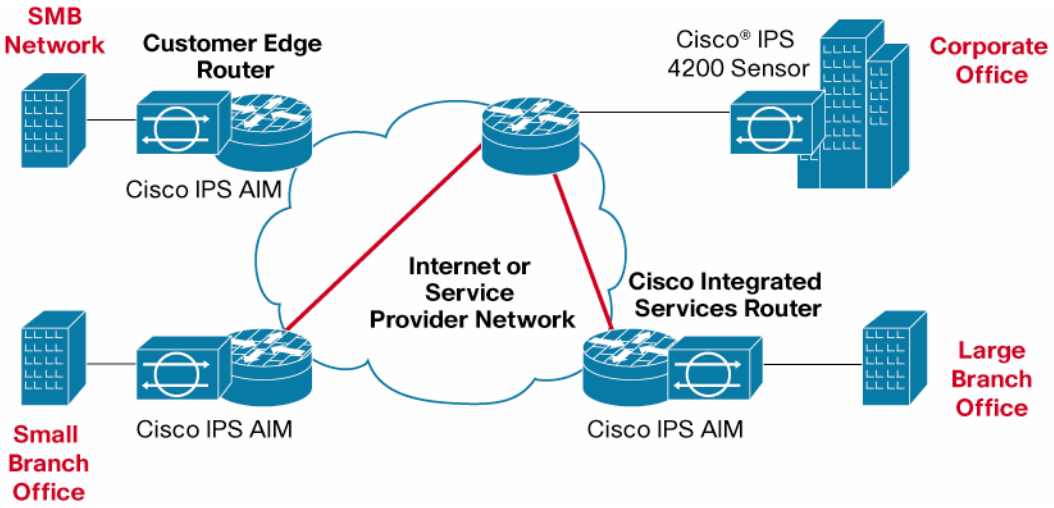
The Cisco IPS AIM is an evolutionary enhancement to the concept of porting a Cisco appliance to a card for a router. The Cisco IPS AIM provides dedicated resources (CPU and DRAM) to run Cisco IPS 6.0, store signatures, and trigger alerts. In contrast to the Cisco IDM Network Module, the Cisco IPS AIM can function in both promiscuous mode and inline mode, as mentioned previously. Inline mode inspects data in the packet-switching path; it checks all packets passing through it for intrusions and if it detects one, alerts the network administrator. In addition, it can block the intrusion from going any further. Typically, an inline IPS is placed at the perimeter of the network, behind the firewall or integrated inside the firewall.

## Deployment Scenarios

Cisco IPS AIM has two main deployment scenarios (Figure 1):

- Cisco IPS AIM protecting the Internet-facing (untrusted) interface
- Cisco IPS AIM within the internal (trusted) network

**Figure 1.** Deployments



### Cisco IPS AIM Protecting the Internet-Facing (Untrusted) Interface

The Internet is one of the major sources of attacks and exploits targeting today's corporate networks. Applying the IPS using the Cisco IPS AIM on router interfaces connected to the Internet helps defend the corporate network against such vulnerabilities. Cisco IOS Firewall and Cisco IPS AIM are complementary features to protect against malicious attacks. Cisco IOS Firewall restricts access from the untrusted Internet and prevents intruders from evading the perimeter router on the telecommuter side to gain access to the corporate network. However, common security attacks can include IP spoofing, man-in-the-middle attacks, and unauthorized access attempting to slip through the firewall. Telecommuter devices may have obtained exploits elsewhere that would then threaten the internal corporate network. To mitigate this threat, you can deploy IPS inspection in conjunction with the Cisco IOS Firewall at the incoming and outgoing interfaces of the perimeter router to monitor and discard malicious activity. In a typical network topology, the branch offices are the best places to enable IPS using the Cisco IPS AIM on both directions of the Internet-facing interface. A common scenario is to enable split tunneling while running VPN tunnels to the corporate network. Cisco recommends enabling IPS on the Internet traffic to protect the network from attacks and exploits that might come into the branch office or telecommuter personal computers, which could in turn affect the corporate network.

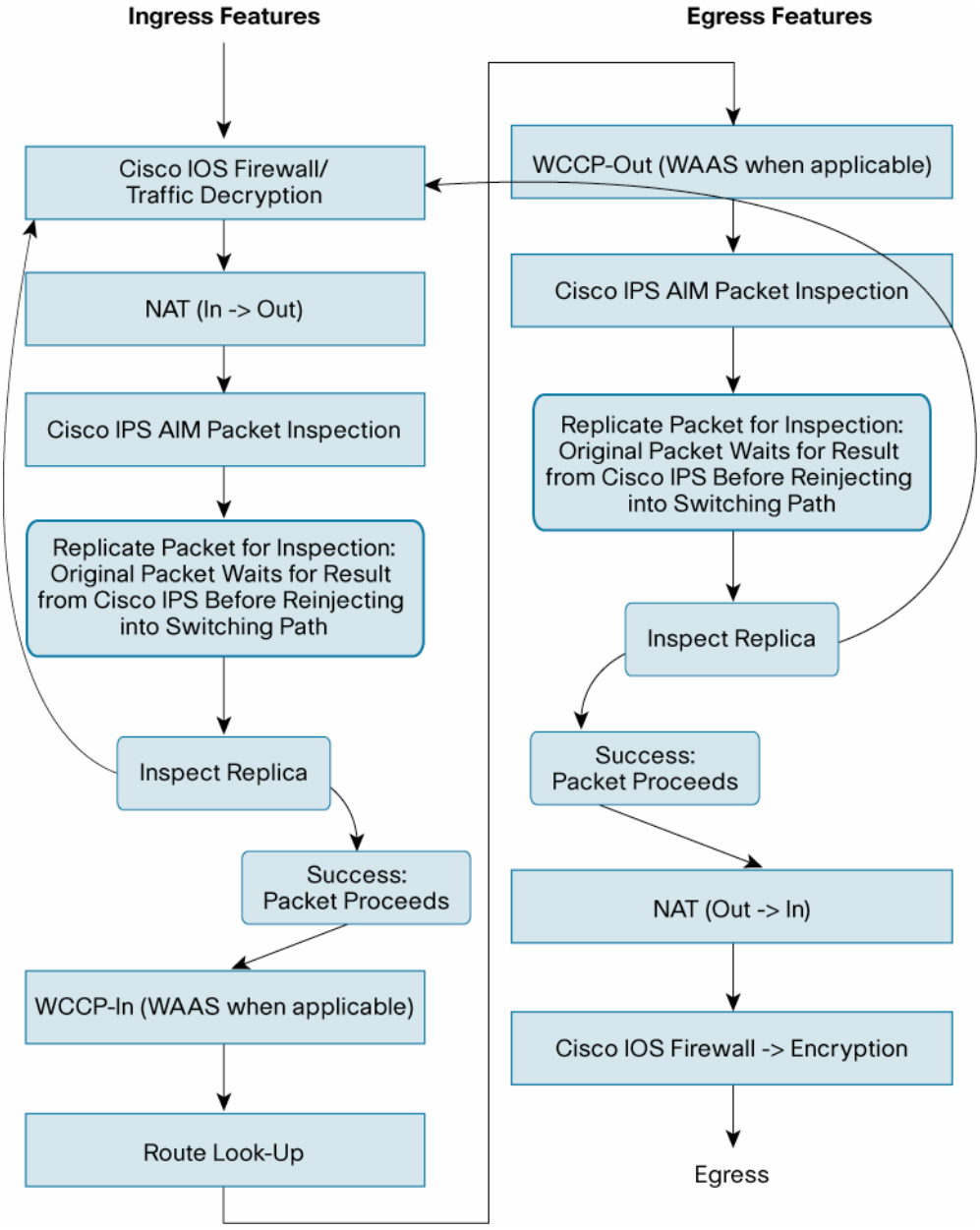
### Cisco IPS AIM Within the Internal (Trusted) Network

In today's corporate network environment, an increasing number of exploits and network attacks are coming from within the corporate network itself. These attacks or exploits may be deliberate or inadvertent (for example, an infected laptop brought into the office and connected to the corporate LAN). Deploying IPS within the corporate network helps mitigate attacks, and helps to prevent exploits from spreading within the network. Hub-and-spoke topologies are commonly used for networks. In a typical network topology, the Cisco IPS AIM on the spoke routers provides distributed protection for the network—attacks and exploits from one of the branch offices will not spread throughout the rest of the network. The WAN link is also spared from being congested by worms and denial-of-service (DoS) attacks, saving the valuable bandwidth for valid business traffic. In addition, the hub router does not have to process all attacks and exploits from all branch offices, thus leaving more CPU power and memory for other tasks. Deploying Cisco IPS as close to the entry point into the network as possible mitigates the attacks and exploits before they spread farther into the network. By facilitating Cisco IPS together with IP Security (IPsec) VPN, Cisco Network Admission Control (NAC), and Cisco IOS Firewall, a Cisco router can perform encryption, firewall, and traffic inspection at the point of entry into the network—an industry first. This setup reduces the additional devices needed to support the system, reduces operating and capital expenditures, and enhances security.

### Packet Flow

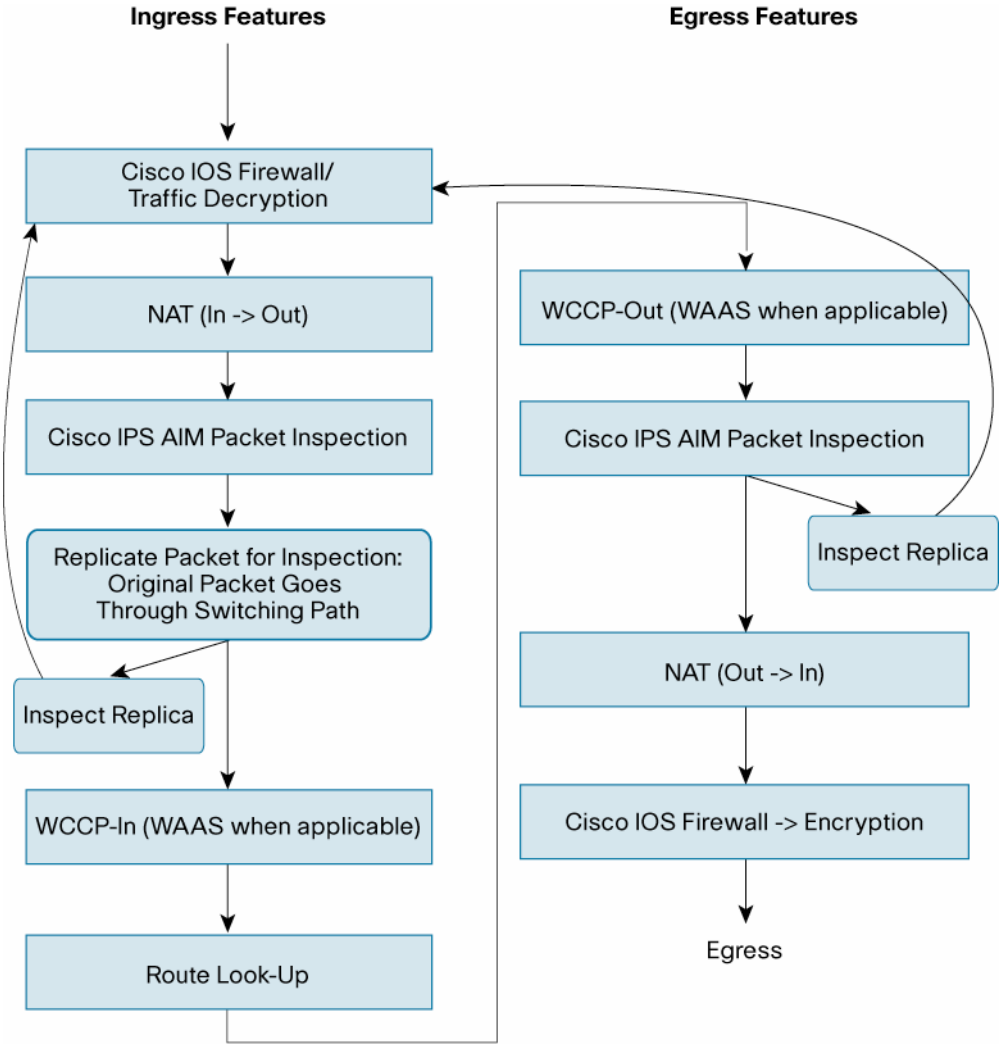
Packets traverse routers in a particular order, and services and features are executed in a specific sequence. Understanding this order and sequence is critical to successful deployment of IPS. Packet flow is slightly different between promiscuous and inline IPS modes, as well as for ingress and egress paths (Figures 2 and 3).

**Figure 2.** Packet Flow for Inline Mode




On ingress, all encapsulating technologies such as IPsec, Web Cache Control Protocol (WCCP), generic routing encapsulation (GRE), etc. must complete so that the original packet can be inspected.

**Figure 3.** Packet Flow for Promiscuous Mode




In promiscuous mode, a replica of the packet is created and sent to the Cisco IPS AIM for inspection.

### Filtering Packets for the Inspection Process

Care should be taken to send the sensor only traffic that it can inspect. In order to support the continuing development of IPS sensor inspection capabilities, Cisco IOS Software places no limits on which traffic can be sent to the sensor. Filtering sensor-bound traffic with an ACL reduces platform and sensor overhead, reduces bandwidth contention to the sensor, and helps eliminate extraneous messages from traffic the sensor may not be able to inspect.

Another type of traffic that should be filtered is any traffic that goes through a tunnel interface. Traffic destined for tunnel encapsulation or encryption should be inspected on the tunnel interface. However, that traffic should be specifically filtered from inspection on the physical egress interface to prevent the traffic from being sent to the inspection engine twice and potentially dropped.

### Deployment with Other Cisco IOS Software Services

- **Cisco IOS Firewall:** Within Cisco IOS Firewall deployments, the two technologies complement each other's abilities to create security zones in the network and inspect the traffic traversing those zones for attacks. However, because the Cisco IPS AIM and Cisco IOS Firewall operate independently, in some instances they are unaware of each other's activities. In a situation where Cisco IOS Firewall and the Cisco IPS AIM are deployed together, the Cisco IOS Firewall becomes the primary defense against a SYN flood attack.
- **Network Address Translation (NAT) and Port Address Translation (PAT):** Also known as NAT Overload, NAT and PAT occur outside the processing path of the Cisco IPS AIM. Thus, there are no dependencies between these services and the AIM.
- **Cisco IOS IPS and Cisco IDS Network Module:** As mentioned earlier, you can deploy only one IPS engine in a single router. Each IPS service separately inspects packets, comparing them to the unique signature set installed for that service. If one IPS service takes action on a match, any other service running would be unaware of that action. The Cisco IPS AIM provides the fastest performance and greatest number of features compared to the other two options, so this option is recommended when the Cisco IPS AIM is installed. You must disable all other IPS services.
- **Voice services:** IPS system performance is measured with TCP traffic, although User Datagram Protocol (UDP) and other protocols are inspected. If the traffic volume overwhelms the IPS engine, excess traffic will be dropped. This situation is an example of the fail-closed behavior, which ensures that no uninspected traffic passes the IPS engine to potentially endanger the protected network. In other words, if the dropped traffic consists of voice packets, voice quality can be compromised. Uniquely among the IPS engines, the Cisco IPS AIM offers the use of an ACL for selecting which traffic is inspected. In a situation where high traffic volumes affect voice quality, excluding that traffic from inspection eliminates the quality problem.
- **Cisco Wide Area Application Services (WAAS):** Cisco Wide Area Application Services, such as compression, WCCP, and TCP Optimization, offer significant performance improvements for running applications in a WAN environment. When combining Cisco WAAS with the Cisco IPS AIM, you should implement these services only on the ingress point of the router. For traffic using WCCP, you must apply inline IPS inspection to the same interface, with both services applied to inbound traffic. In other applications, the IPS cannot inspect the WAAS traffic.
- **Packet fragmentation:** IPS engines have a feature known as normalization, which addresses attacks that use fragmentation to evade IPS devices. The normalization engine collects all fragments of a TCP packet and reassembles that packet prior to inspection. The IPS engine then inspects the entire packet. For normalization using the Cisco IPS AIM, a copy of the packets stays in Cisco IOS Software buffers while a copy is forwarded to the card. When the packet passes inspection, the Cisco IPS AIM notifies Cisco IOS Software to release the buffered packets. The UDP and Internet Control Message Protocol (ICMP) protocols do not support fragmentation.
- **Encryption:** Encrypted traffic cannot be inspected. Inspection must occur before encryption or after decryption. This rule applies to both IPsec and Secure Sockets Layer (SSL) VPN encryption. You can apply both Cisco IPS AIM and encryption simultaneously on one router and in one data flow in cases where branch-office devices are granted direct Internet access and do not cross a corporate WAN where IPS is applied.

### Configuring the Cisco IPS AIM

In preparation for applying this IPS solution, you must configure both the Cisco IPS AIM and the router. Because the AIM has its own operating system, it acts as a separately configured entity. Configuration of the AIM occurs through a virtual console port accessible through a reverse Telnet session, which is initiated using the **session** command from the router command prompt. Router configuration involves the following steps:

1. Verify successful installation of the Cisco IPS AIM. Use the **show inventory** command from the router command line.

```
atg2851-21#sh inventory
NAME: "2851 chassis", DESCR: "2851 chassis"
PID: CISCO2851          , VID: V03 , SN: FTX1046A4CG

NAME: "AIM Packet Services Engine", DESCR: "AIM Packet Services
Engine"
PID: CISCO IPS AIM          , VID: V03, SN: FHH102300JG
```

2. Set up the interfaces. Installation of the Cisco IPS AIM creates a new interface in the router, which is labeled “interface IDS-Sensor”. This interface must have an IP address assigned to it, either shared with another interface through IP Unnumbered, or with its own routable address. You must also create a route to this IP address.

```
atg2851-21(config)#interface ids-sensor 0/0
atg2851-21(config-if)#ip address 12.0.0.1 255.255.255.252

or

atg2851-21(config-if)#ip unnumbered interface gi 0/0

atg2851-21#sh run int ids-sensor 0/0
interface IDS-Sensor0/0
 ip address 12.0.0.1 255.255.255.252
 service-module fail-open
 hold-queue 60 out
end
```

3. Set up the appropriate IP networking environment that fits network needs. Begin this process by executing the **session** command to access the Cisco IPS AIM command line. The default IP address of the sensor is 10.1.9.201/24. This address is easily changeable to meet the demands of the network. It is also possible to use the router NAT feature to direct traffic to the AIM and maintain the current interface IP addressing scheme, if you need to. Regardless of the IP address requirement, you must also set the network mask and default gateway to the AIM configuration parameters. Remember to apply changes that are made at this command-line interface.

```
atg2851-21#service-module ids-sensor 0/0 session
Trying 12.0.0.1, 2194 ... Open
sensor# conf t
sensor(config)# service host
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
```

```
sensor(config)# service host
sensor(config-hos)# network-setting
sensor(config-hos-net)# show setting
   network-settings
   -----------------------------------------------
      host-ip: 10.1.9.201/24,10.1.9.1 <defaulted>
      host-name: sensor <defaulted>
      telnet-option: disabled <defaulted>
      access-list (min: 0, max: 512, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text:  <defaulted>
   -----------------------------------------------
sensor(config-hos-net)# host-ip 12.0.0.2/30,12.0.0.1
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes?[yes]: yes
sensor(config)# exit
```

4. Verify status with the service-module ids-Sensor 0/x **status** command:

```
atg2851-21#service-module ids-Sensor 0/0 status
Service Module is Cisco IDS-Sensor0/0
Service Module supports session via TTY line 194
Service Module is in Steady state
Getting status from the Service Module, please wait..

Cisco Systems Intrusion Prevention System Network Module
  Software version:  0.0(0)S212.0
  Model:             AIM-IPS
  Memory:            890992 KB
  Mgmt IP addr:      10.1.9.201
  Mgmt web ports:    443
  Mgmt TLS enabled:  true
```

5. Enable IPS monitoring on the router interface. You can apply monitoring in either inline or promiscuous mode on any interface on the router. All interfaces on the router must have the same type of monitoring enabled, however. Because the Cisco IPS AIM functions on the CPU bus, it can monitor any interface installed in the router. Additionally, use an access list to control and identify which traffic is being inspected. Filtering traffic to those protocols supported by the currently deployed version of the IPS sensor helps eliminate spurious messages and reduce sensor bandwidth requirements.

6. Finally, configure the action the router should take if the card fails. The options are <fail-open>, meaning allow all traffic to pass, or <fail-closed>, meaning allow no traffic matching the ACL to pass.

```
atg2851-21(config)#interface GigabitEthernet0/0
atg2851-21(config-if)# ids-service-module monitoring ?
  inline       Configure Inline monitoring on the interface
  promiscuous  Configure Promiscuous monitoring on the interface
  <cr>
```

```
atg2851-21(config-if)# ids-service-module monitoring inline ?
  access-list  Apply standard or extended ACL to Inline monitoring
  <cr>

atg2851-21(config-if)# ids-service-module monitoring inline
atg2851-21(config-if)#end

atg2851-21# sh run int g0/0
Building configuration...

Current configuration : 135 bytes
!
interface GigabitEthernet0/0
ip address 100.0.0.1 255.255.255.0
ip access-group 10 in
duplex auto
speed auto
ids-service-module monitoring inline
end


atg2851-21#more ACL_only
!
!
interface GigabitEthernet0/0
mac-address 000b.000b.000b
!
access-list 10 permit udp any eq 2001 any eq 2001
access-list 10 permit udp any eq 2002 any eq 2002
access-list 10 permit udp 100.1.1.0 0.0.0.255 200.1.1.0 0.0.0.255 dscp
ef
access-list 10 permit ip 100.1.1.0 0.0.0.255 200.1.1.0 0.0.0.255 dscp
ef
access-list 10 permit udp any any eq 2005 dscp ef
access-list 10 permit ip 40.40.40.0 0.0.0.255 30.30.30.0 0.0.0.255
dscp ef
access-list 10 permit tcp any eq 2007 any eq 2007
access-list 10 permit tcp any eq 2008 any eq 2008
access-list 10 permit tcp any any
end
```

### Management

At first customer shipment (FCS), Cisco IPS Device Manager is built in with Cisco IPS AIM for device-level configuration, reporting, and event correlation.

Network management and configuration support is planned for Cisco Security Manager in a future release.

To coordinate events across the network with other devices, the Cisco IPS AIM supports the Security Device Event Exchange (SDEE) protocol. Recognition and configuration support from

Cisco Security Monitoring, Analysis and Response System (MARS) will be enabled shortly after FCS in an updated release of the Cisco Security MARS.

## For More Information

**Details about the Cisco IPS AIM card:** http://www.cisco.com/en/US/products/ps8395/index.html

**Cisco Intrusion Prevention System technology:** http://www.cisco.com/go/ips

**The deployment guide for Cisco IOS IPS in 5.0 signature format:** http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd8062acfb.shtml

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**



Printed in USA C11-452595-00 01/08