Data Sheet

Cisco IDS 4200 Series Sensors

Cisco integrated network security solutions enable organizations to protect productivity gains and reduce operating costs.

The Cisco IDS 4200 Series sensors are used in the Cisco Intrusion Protection System. These intrusion detection system sensors work in concert with the other components to efficiently protect your data and information infrastructure. With the increased complexity of security threats, achieving efficient network intrusion security solutions is critical to maintaining a high level of protection. Vigilant protection ensures business continuity and minimizes the effect of costly intrusions.

Please refer to Table 1 for information on the characteristics of the Cisco IDS 4200 Series Sensors.

For details on the complete Cisco Intrusion Protection System, go to http://www.cisco.com/go/ids.

Deploying the Cisco IDS 4200 Series Sensors

The Cisco IDS 4200 Series includes four products: the Cisco IDS 4210, IDS 4235, IDS 4250 and IDS 4250-XL sensors. The Cisco IDS product line delivers a broad range of solutions that allow easy integration into many different environments, including enterprise and service provider environments. Each sensor addresses the bandwidth requirements at one of several speeds, from 45 Mbps to gigabits per second.

The Cisco IDS 4210 can monitor up to 45 Mbps of traffic and is suitable for T1/E1 and T3 environments.

At 200 Mbps, the Cisco IDS 4235 can be deployed to provide protection in switched environments, on multiple T3 subnets, and with the support of 10/100/1000 interfaces it can also be deployed on partially utilized gigabit links.

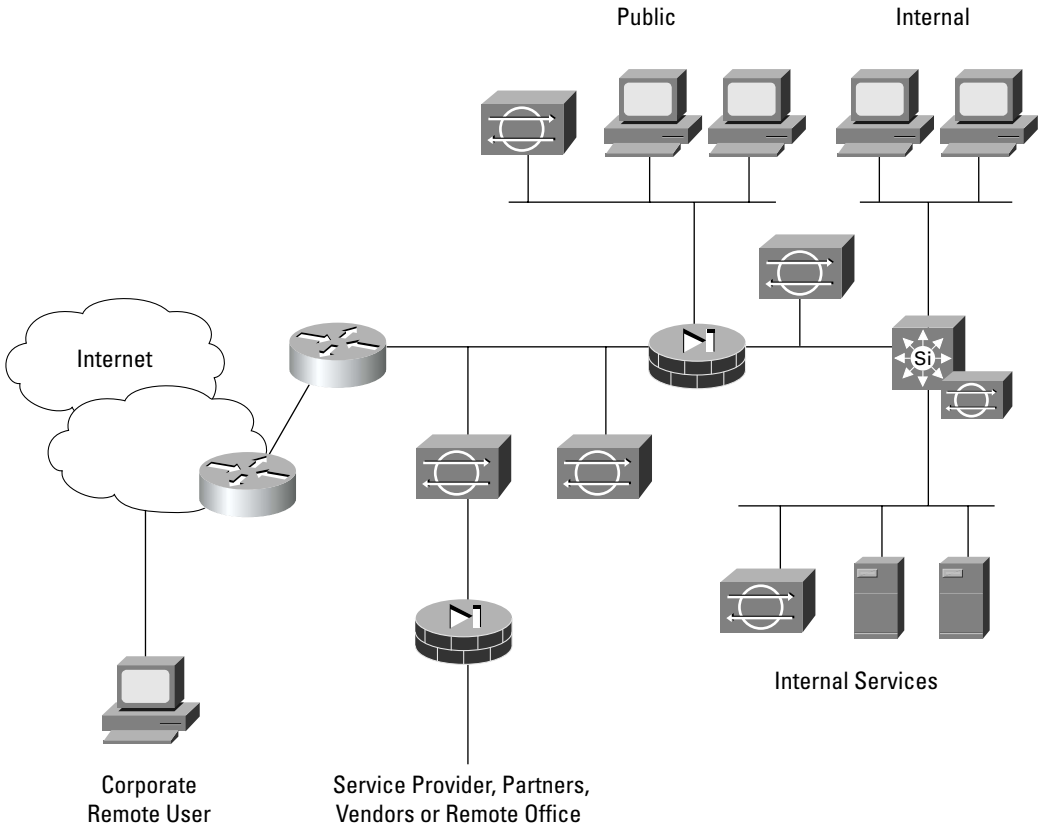
The Cisco IDS 4250 supports a 500 Mbps speed and can be used to protect gigabit subnets and traffic traversing switches that are being used to aggregate traffic from numerous subnets. In addition, the Cisco IDS 4250 provides the flexibility to accommodate a simple hardware upgrade to scale to full line-rate gigabit performance.

At 1 Gbps, the Cisco IDS 4250-XL provides unprecedented performance by providing customized hardware acceleration to protect fully-saturated gigabit links as well as multiple partially-utilized gigabit subnets.

As shown in Figure 1, sensors can be placed on almost any network segment of the enterprise-wide network where security visibility is required.

Please refer to Table 2 for ordering information for the Cisco IDS 4200 Series Sensors.

Figure 1
Deployment Scenarios for the 4200 Series Appliance Sensors



Product Specifications

Table 1 Characteristics of Cisco IDS 4210, 4235, 4250, and 4250-XL Sensors

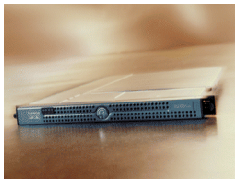
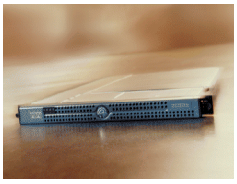
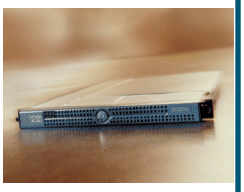
	Cisco IDS 4210	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
				
Performance	45 Mbps	200 Mbps	500 Mbps	1000 Mbps
Standard monitoring interface	10/100BASE-T	10/100/1000BASE-TX	10/100/1000BASE-TX	Dual 1000BASE-SX interface with MTRJ
Standard command and control interface	10/1010/100BASE-T	10/100/1000BASE-TX	10/100/1000BASE-TX	10/100/1000BASE-TX
Optional interface	No	No	1000BASE-SX (fiber)	1000BASE-SX (fiber)
Performance upgradable	No	No	Yes	No
Form factor	One rack unit	One rack unit	One rack unit	One rack unit
Advanced protection algorithms				
Stateful pattern recognition	Yes	Yes	Yes	Yes
Protocol parsing	Yes	Yes	Yes	Yes
Heuristic detection	Yes	Yes	Yes	Yes
Anomaly detection	Yes	Yes	Yes	Yes
Attack protection				
Sweeps or floods	Yes	Yes	Yes	Yes
Denial-of-service (DoS) mitigation	Yes	Yes	Yes	Yes
Worms or viruses	Yes	Yes	Yes	Yes
Common gateway interface (CGI) or WWW attacks	Yes	Yes	Yes	Yes
Buffer overflow protection	Yes	Yes	Yes	Yes
Remote-procedure call (RPC) attack detection	Yes	Yes	Yes	Yes
IP fragmentation attacks	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4210, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4210	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Internet Control Message Protocol (ICMP) attacks	Yes	Yes	Yes	Yes
Simple Message Transfer Protocol (SMTP), Sendmail, Internet Message Access Protocol (IMAP), or Post Office Protocol (POP) attacks	Yes	Yes	Yes	Yes
File Transfer Protocol (FTP), Secure Shell Protocol (SSH), Telnet, and rlogin attacks	Yes	Yes	Yes	Yes
Domain Name System (DNS) attacks	Yes	Yes	Yes	Yes
TCP hijacks	Yes	Yes	Yes	Yes
Windows or NetBios attacks	Yes	Yes	Yes	Yes
TCP application protection	Yes	Yes	Yes	Yes
BackOrifice attacks	Yes	Yes	Yes	Yes
Network Timing Protocol (NTP) attacks	Yes	Yes	Yes	Yes
Customizable signatures using Signature Micro-Engine technology	Yes	Yes	Yes	Yes
Automated signature updates	Yes	Yes	Yes	Yes
Alarm summarization	Yes	Yes	Yes	Yes
Support for 802.1q traffic	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4210, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4210	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Secure communication				
IP Security (IPSec) or Secure Sockets Layer (SSL) between sensor and management console	Yes	Yes	Yes	Yes
Encrypted signature packages	Yes	Yes	Yes	Yes
SSH for remote administration	Yes	Yes	Yes	Yes
Serial Control Protocol (SCP) support for secure file transfer	Yes	Yes	Yes	Yes
IDS evasion protection				
IP fragmentation re-assembly	Yes	Yes	Yes	Yes
TCP stream re-assembly	Yes	Yes	Yes	Yes
Unicode deobfuscation	Yes	Yes	Yes	Yes
Active response actions				
Router access-control-list (ACL) modifications	Yes	Yes	Yes	Yes
Firewall policy modifications	Yes	Yes	Yes	Yes
Switch ACL modifications	Yes	Yes	Yes	Yes
Session termination via TCP resets	Yes	Yes	Yes	Yes
IP session logging or session replay	Yes	Yes	Yes	Yes
Active notification actions				
Alarm display	Yes	Yes	Yes	Yes
E-mail alerts	Yes	Yes	Yes	Yes
E-page alerts	Yes	Yes	Yes	Yes
Customizable script execution	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4210, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4210	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Multiple alarm destinations	Yes	Yes	Yes	Yes
Third-party tool integration	Yes	Yes	Yes	Yes
IDS active update bulletins	Yes	Yes	Yes	Yes
Administration				
Web user interface (Secure Hypertext Transfer Protocol [HTTPS])	Yes	Yes	Yes	Yes
Command-line interface (CLI) (console)	Yes	Yes	Yes	Yes
CLI (Telnet or SSH)	Yes	Yes	Yes	Yes
CiscoWorks VPN Security Management Solution (VMS) support	Yes	Yes	Yes	Yes
High availability				
Redundant power supply	No	Yes	Yes	Yes
Failure detection				
Monitoring link failure detection	Yes	Yes	Yes	Yes
Communications failure detection	Yes	Yes	Yes	Yes
Services failure detection	Yes	Yes	Yes	Yes
Device failure detection	Yes	Yes	Yes	Yes
Dimensions				
Height	1.7 in. (4.32 cm)	1.67 in. (4.24 cm)	1.67 in. (4.24 cm)	1.67 in. (4.24 cm)
Width	16.8 in. (42.54 cm)	17.6 in. (44.70 cm)	17.6 in. (44.70 cm)	17.6 in. (44.70 cm)
Depth	22 in. (55.8 cm)	27.0 in. (68.58 cm)	27.0 in. (68.58 cm)	27.0 in. (68.58 cm)
Weight	23 lb (10.43 kg)	35 lb (15.88 kg)	35 lb (15.88 kg)	35 lb (15.88 kg)
Rack-mountable	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4210, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4210	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Power				
Autoswitching	100–240 VAC	110–220 VAC	110–220 VAC	110–220 VAC
Frequency	50–60 Hz	50–60 Hz	50–60 Hz	50–60 Hz
Operating current	2.0A at 115V 1.0A at 220V	2.7A at 115V 1.3A at 220V	2.7A at 115V 1.3A at 220V	2.7A at 115V 1.3A at 220V
Operating environment				
Operating temperature	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)
Nonoperating temperature	–40 to 70°C (–40 to 158°F)	–40 to 65°C (–40 to 149°F)	–40 to 65°C (–40 to 149°F)	–40 to 65°C (–40 to 149°F)
Operating relative humidity	8 to 80% at 30°C (noncondensing)	8 to 80% (noncondensing)	8 to 80% (noncondensing)	8 to 80% (noncondensing)
Nonoperating relative humidity	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)
Heat dissipation (most severe case with full power usage)	898 Btu/hr (maximum)	983 Btu/hr (maximum)	983 Btu/hr (maximum)	983 Btu/hr (maximum)

Notes:

- This 45-Mbps performance for the Cisco IDS 4210 is based on the following conditions:
  - 500 new TCP connections per second
  - 500 HTTP transactions per second
  - Average packet size of 445 bytes,
  - Running Cisco IDS 4.0 Sensor Software
- This 200-Mbps performance for the Cisco IDS 4235 is based on the following conditions:
  - 2000 new TCP connections per second
  - 2000 HTTP transactions per second
  - Average packet size of 445 bytes
  - Running Cisco IDS 4.0 Sensor Software
- This 500-Mbps performance for the Cisco IDS 4250 is based on the following conditions:
  - 2700 new TCP connections per second
  - 2700 HTTP transactions per second
  - Average packet size of 595 bytes
  - Running Cisco IDS 4.0 Sensor Software

- This 1000-Mbps performance for the Cisco IDS 4250-XL is based on the following conditions:
  - 5000 new TCP connections per second
  - 5000 HTTP transactions per second
  - Average packet size of 595 bytes
  - Running Cisco IDS 4.0 Sensor Software

Agency Approvals

- Emissions—FCC (CFR 47 Part 15) Class A, CISPR 22 Class A, EN 55022 Class A, EN 55024, EN61000-3-2, EN61000-3-3, VCCI Class A, AS/NZS 3548 Class A, CE mark
- Safety—UL 1950, CSA 22.2 No.950, IEC 60950, EN 60950, AS/NZS 3260, CE mark

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
Cisco IDS-4210-K9	Cisco IDS 4210 Sensor (chassis, software, SSH, 10/100BASE-T with RJ-45 connector), 45-Mbps
Cisco IDS-4235-K9	Cisco IDS 4235 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector)
Cisco IDS-4250-TX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector)
Cisco IDS-4250-SX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 1000BASE-SX with SC connector)
Cisco IDS-4250-XL-K9	Cisco IDS 4250-XL Sensor (chassis, software, SSH, hardware accelerator, with dual 1000BASE-SX and MTRJ connectors)
Cisco IDS-XL-INT=	Cisco IDS Accelerator Card with dual 1000BASE-SX interfaces and MTRJ connectors
IDS-4250-SX-INT=	1000BASE-SX monitoring interface with SC connector
IDS-PWR=	Spare power supply for the Cisco IDS 4235 and 4250 sensors
IDS-SCSI=	Spare Small Computer Systems Interface (SCSI) hard disk drive for Cisco IDS 4250 Sensor
IDS-RAIL-2=	Two post rail kits for the Cisco IDS 4235 and 4250 sensor platforms
IDS-RAIL-4=	Four post rail kits for the Cisco IDS 4235 and 4250 sensor platforms
CON-SNT-IDS4210	Cisco SMARTnet™ 8 x 5 x next business day (NBD) service (Cisco IDS 4210)
CON-SNTE-IDS4210	Cisco SMARTnet 8 x 5 x 4 enhanced service (Cisco IDS 4210)
CON-SNTP-IDS4210	Cisco SMARTnet 24 x 7 x 4 premium service (Cisco IDS 4210)
CON-OS-IDS4210	Cisco SMARTnet 8 x 5 x NBD onsite standard service Cisco (IDS 4210)
CON-OSE-IDS4210	Cisco SMARTnet 8 x 5 x 4 onsite enhanced service (Cisco IDS 4210)
CON-OSP-IDS4210	Cisco SMARTnet 24 x 7 x 4 onsite premium service (Cisco IDS 4210)

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
CON-SNT-IDS4235K9	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4235)
CON-SNTE-IDS4235K9	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4235)
CON-SNTP-IDS4235K9	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4235)
CON-OS-IDS4235K9	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4235)
CON-OSE-IDS4235K9	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4235)
CON-OSP-IDS4235K9	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4235)
CON-SNT-IDS4250TK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4250-TX)
CON-SNTE-IDS4250TK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-TX)
CON-SNTP-IDS4250T	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-TX)
CON-OS-IDS4250TK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-TX)
CON-OSE-IDS4250TK	Cisco SMARTnet onsite support 8 x 5 x 4 Cisco (IDS 4250-TX)
CON-OSP-IDS4250TK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-TX)
CON-SNT-IDS4250SK	Cisco SMARTnet support 8 x 5 x NBD Cisco (IDS 4250-SX)
CON-SNTE-IDS4250SK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-SX)
CON-SNTP-IDS4250SK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-SX)
CON-OS-IDS4250SK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-SX)
CON-OSE-IDS4250SK	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4250-SX)
CON-OSP-IDS4250SK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-SX)
CON-SNT-IDS4250XK	Cisco SMARTnet support 8 x 5 x NBD Cisco (IDS 4250-XL)
CON-SNTE-IDS4250XK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-XL)
CON-SNTP-IDS4250XK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-XL)
CON-OS-IDS4250XK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-XL)
CON-OSE-IDS4250XK	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4250-XL)
CON-OSP-IDS4250XK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-XL)
CON-SNT-IDSXL	Cisco SMARTnet support 8 x 5 x NBD (IDS-XL-INT=)
CON-SNTE-IDSXL	Cisco SMARTnet support 8 x 5 x 4 (IDS-XL-INT=)
CON-SNTP-IDSXL	Cisco SMARTnet support 24 x 7 x 4 (IDS-XL-INT=)
CON-OS-IDSXL	Cisco SMARTnet onsite support 8 x 5 x NBD (IDS-XL-INT=)
CON-OSE-IDSXL	SMARTnet onsite support 8 x 5 x 4 (IDS-XL-INT=)
CON-OSP-IDSXL	SMARTnet onsite support 24 x 7 x 4 (IDS-XL-INT=)

Export Considerations

The Cisco IDS 4200 Series sensors are subject to export controls. Refer to the export compliance Web site for guidance at: http://www.cisco.com/wwl/export/crypto/.

For specific export questions, contact export@cisco.com.

Additional Information

For more information about the Cisco Intrusion Protection System, go to: http://www.cisco.com/go/ids

For more information about the CiscoWorks VMS Solutions (IDS management), go to: http://www.cisco.com/go/vms

Corporate 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: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

RD/LW4099 01/03