

Cisco IDS 4200 Series Appliance Sensors

Cisco IDS(침입 탐지 시스템) 4200 장비 센서는 네트워크 전반에서 광범위한 보호 기능을 제공하는 업계 최고의 Cisco IDS Series 제품 계열입니다.

소개

Cisco IDS 4200 Series 장비 센서는 악의적인 목적을 가진 사용자가 네트워크에 무단으로 침입하여 탐색하는 것을 막기 위해 특별히 고안된 고성능 네트워크 보안 "장비"입니다. 따라서 Cisco IDS 센서는 실시간으로 네트워크 트래픽을 분석하여 사용자가 보안 공격에 신속히 대응할 수 있게 해줍니다.

Cisco의 저명한 Cisco C-CRT(Countermeasures Research Team)는 상태보유 패턴 인식, 프로토콜 구문 분석, 경험적 탐지(Heuristic Detection) 및 이상 상태 탐지를 비롯해 매우 혁신적이고 정교한 탐지 기술을 결합하여 사용함으로써 발생했거나 발생 가능성이 있는 다양하면서 광범위한 사이버 위협으로부터 광범위하게 보호해 줍니다. 더 나아가 특허 출원 중인 Cisco의 SME(Signature Micro-Engine) 기술을 사용하므로 정확하게 조절된 센서가 "오류" 발생률을 최소화할 수 있도록 센서 서명을 세밀하게 사용자 정의할 수 있습니다.

무단 행위가 탐지되면 센서는 관리 콘솔에게 탐지된 행위에 대한 상세 내용과 함께 알람 메시지를 보낼 수 있습니다. 또한 Cisco IDS Active Response System은 라우터, 방화벽, 스위치 등과 같은 다른

시스템을 제어하여 권한 없는 세션을 중단시키는 독보적인 보호 기능을 제공합니다. 웹 사용자 인터페이스, CLI(명령줄 인터페이스) 또는 Cisco의 고도로 확장 가능한 CiscoWorks VMS(VPN/Security Management Solution) 같은 다양한 관리 솔루션을 사용하여 이러한 Turn-key 장비를 쉽게 설치 및 관리할 수 있습니다.

애플리케이션

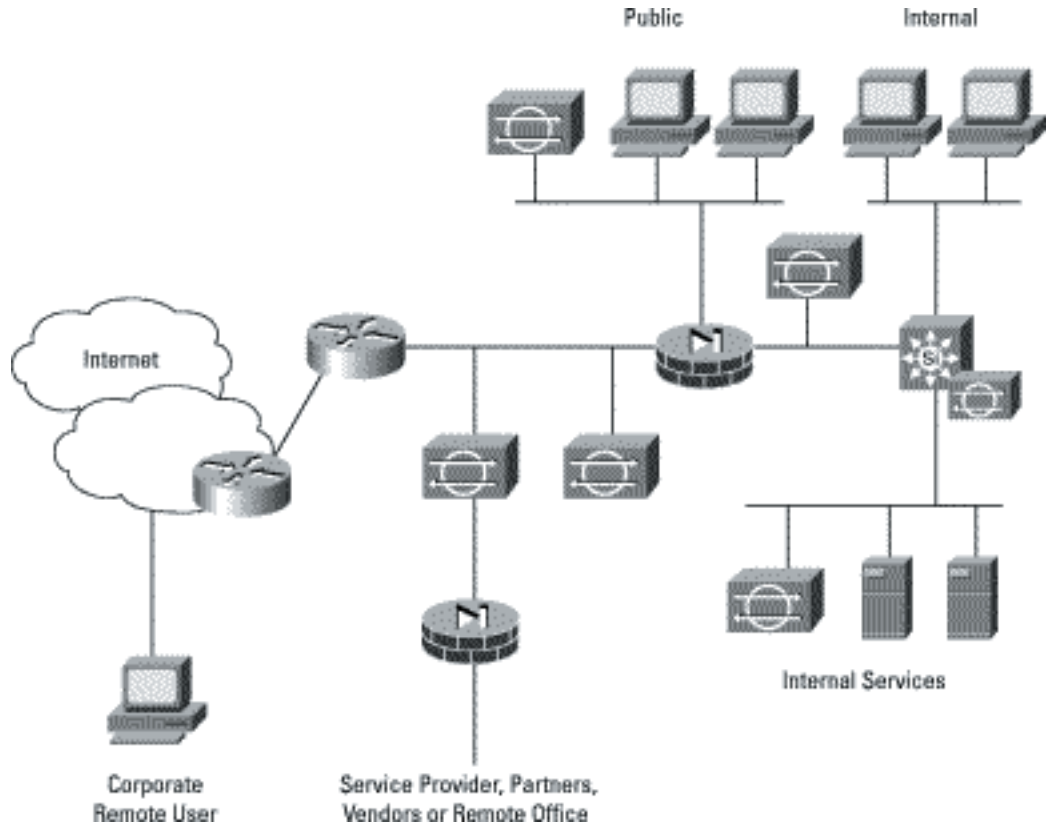
Cisco IDS 4200 Series 장비 센서는 Cisco IDS 4210, Cisco IDS 4235, Cisco IDS 4250 등 세 가지 제품으로 이루어져 있고 전체 Cisco IDS 장비 포트폴리오는 광범위한 솔루션을 제공해 주므로 기업 및 서비스 공급업체 환경을 포함하여 다양한 환경과 손쉽게 통합할 수 있습니다. 각 장비 센서는 45Mbps에서 기가비트까지 다양한 성능 표시 중 하나로 대역폭 요건을 처리합니다.

Cisco IDS 4210은 최대 45Mbps의 트래픽을 모니터링할 수 있고 T1/E1 및 T3 환경에 적합합니다.

다중 T3 서브넷의 스위칭 환경에 보호 기능을 제공하기 위해 Cisco IDS 4235를 200Mbps 속도로 구축할 수 있고 10/100/1000 인터페이스의 지원을 받으면 부분적으로 이용되는 기가비트 링크에도 구축할 수 있습니다.

Cisco IDS 4250은 500Mbps 속도에서 뛰어난 성능을 내며 수많은 서브넷에서 트래픽을 집중하는 데 사용되는 기가바이트 서브넷과 트래픽 탐색 스위치를 보호하기 위해 사용할 수 있습니다.

센서는 보안 감시가 필요한 기업 전체 네트워크의 거의 모든 세그먼트에 배치할 수 있습니다.



제품 사양

표 1 Cisco IDS 4210, 4235 및 4250 장비 센서 특성 비교표

	Cisco IDS 4210	Cisco IDS 4235	Cisco IDS 4250
			
성능	45Mbps	200Mbps ¹	500Mbps ²
표준 모니터링 인터페이스	10/100BASE-T	10/100/1000BASE-TX	10/100/1000BASE-TX
표준 명령 및 제어 인터페이스	10/1010/100BASE-T	10/100/1000BASE-TX	10/100/1000BASE-TX
선택 사양 인터페이스	없음	없음	1000BASE-SX(fiber)
성능 업그레이드	불가능	불가능	가능
폼 팩터(Form Factor)	1RU	1RU	1RU
고급 보호 알고리즘			
상태보유 패턴 인식	예	예	예
프로토콜 구문 분석	예	예	예
경험적 탐지	예	예	예
이상 상태 탐지	예	예	예
공격 방어			
스위프/초과	예	예	예
DoS ¹ 방지	예	예	예
웜/바이러스	예	예	예
CGI ² /WWW 공격	예	예	예
버퍼 오버플로 방지	예	예	예
RPC 공격 탐지	예	예	예
IP 단편화 공격	예	예	예
ICMP ³ 공격	예	예	예
SMTP ⁴ /Sendmail/IMAP ⁵ /POP ⁶ 공격	예	예	예
FTP ⁷ , SSH ⁸ , Telnet 및 rlogin 공격	예	예	예
DNS ⁹ 공격	예	예	예
TCP Hijacks	예	예	예
Windows/NetBIOS 공격	예	예	예

	Cisco IDS 4210	Cisco IDS 4235	Cisco IDS 4250
TCP 애플리케이션 보호	예	예	예
BackOrifice 공격	예	예	예
NTP¹⁰ 공격	예	예	예
SME 기술을 사용한 사용자 정의 서명	가능	가능	가능
자동 서명 업데이트	예	예	예
알림 요약	예	예	예
802.1q 트래픽 지원	예	예	예
보안 커뮤니케이션			
센서와 관리 콘솔 간 IPSec¹¹/SSL¹²	예	예	예
서명 패키지 암호화	예	예	예
원격 관리용 SSH	예	예	예
안전한 파일 전송을 위한 SCP¹³ 지원	예	예	예
IDS 회피 방지			
IP 단편화 리어셈블리	예	예	예
TCP 스트림 리어셈블리	예	예	예
유니코드 역난독처리	예	예	예
능동적 대응 작업			
라우터 ACL¹⁴ 수정	예	예	예
방화벽 정책 수정	예	예	예
스위치 ACL 수정	예	예	예
TCP 재설정을 통한 세션 종료	예	예	예
IP 세션 기록/세션 재생	예	예	예
능동적 알림 작업			
알림 메시지 표시	예	예	예
전자 메일 알림	예	예	예
전자 페이지 알림	예	예	예
스크립트 실행 사용자 정의	가능	가능	가능
복수 알림 대상(Destination)	예	예	예
타사 툴 통합	예	예	예
IDS 액티브 업데이트 게시판	예	예	예
관리			
웹 사용자 인터페이스(HTTPS¹⁵)	예	예	예
CLI(콘솔)	예	예	예

	Cisco IDS 4210	Cisco IDS 4235	Cisco IDS 4250
CLI (Telnet/SSH)	예	예	예
Cisco VMS 지원	예	예	예
고가용성			
중복 전원 공급 장치	없음	있음	있음
장애 탐지			
링크 오류 탐지 모니터링	예	예	예
커뮤니케이션 장애 탐지	예	예	예
서비스 장애 탐지	예	예	예
장치 장애 탐지	예	예	예
치수			
높이	4.32cm(1.7인치)	4.24cm(1.67인치)	4.24cm(1.67인치)
너비	42.54cm(16.8인치)	44.70cm(17.6인치)	44.70cm(17.6인치)
깊이	55.8cm(22인치)	68.58cm(27.0인치)	68.58cm(27.0인치)
중량	10.43kg(23lb)	15.88kg(35lb)	15.88kg(35lb)
랙 장착 가능	예	예	예
전원			
자동 전환	100VAC – 240VAC	110VAC – 220VAC	110VAC – 220VAC
주파수	50Hz – 60Hz	50Hz – 60Hz	50Hz – 60Hz
작동 전류	115V에서 2.0A 220V에서 1.3A	220V에서 1.0A 115V에서 2.7A	115V에서 2.7A 220V에서 1.3A
작동 환경			
작동 온도	10°C – 35°C(50°F – 95°F)	10°C – 35°C(50°F – 95°F)	10°C – 35°C(50°F – 95°F)
비작동 온도	-40°C – 70°C(-40°F – 158°F)	-40°C – 65°C(-40°F – 149°F)	-40°C – 65°C(-40°F – 149°F)
작동 상대습도	30°C에서 8% – 80%(비응결)	8% – 80%(비응결)	8% – 80%(비응결)
비작동 상대습도	5% – 95%(비응결)	5% – 95%(비응결)	5% – 95%(비응결)
열 소모량(최대 전력 사용 시)	898Btu/hr(최대)	983Btu/hr(최대)	983Btu/hr(최대)

¹DoS

²Common Gateway Interface

³Internet Control Message Protocol

⁴Simple Mail Transfer Protocol

⁵Internet Message Access Protocol

⁶Post Office Protocol

⁷File Transfer Protocol

⁸Secure Shell Protocol

⁹Domain Name System

¹⁰Network Timing Protocol

¹¹IP Security

¹²Secure Sockets Layer

¹³Serial Control Protocol

¹⁴액세스 제어 목록

¹⁵HTTP Secure

Cisco Systems, Inc.

All contents are Copyright © 1992-2002 Cisco Systems, Inc. All rights reserved. 중요 고지 사항 및 개인 정보 보호 정책

참고

- IDS 4235는 초당 2200개의 새로운 TCP 연결, 초당 2200개의 HTTP 트랜잭션, 평균 패킷 크기 438 바이트의 조건에서 1200Mbps 성능을 냅니다.
- IDS 4250은 초당 2700개의 새로운 TCP 연결, 초당 2700개의 HTTP 트랜잭션, 평균 패킷 크기 456 바이트의 조건에서 2500Mbps 성능을 냅니다.

기관 승인

- 방출 기준: 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
- 안전 기준: UL 1950, CSA 22.2 No.950, IEC 60950, EN 60950, AS/NZS 3260, CE Mark

표 2 Cisco IDS 4200 Series Appliance Sensor 주문 정보

제품 번호	제품 설명
IDS-4210	Cisco Secure IDS 45Mbps Sensor
IDS-4235-K9	Cisco IDS 4235 센서(새시, 소프트웨어, SSH, 10/100/1000BASE-T(RJ-45 커넥터 포함))
IDS-4250-TX-K9	Cisco IDS 4250 센서(새시, 소프트웨어, SSH, 10/100/1000BASE-T(RJ-45 커넥터 포함))
IDS-4250-SX-K9	Cisco IDS 4250 센서(새시, 소프트웨어, SSH, 1000BASE-SX(SC 커넥터 포함))
IDS-4250-SX-INT=	1000BASE-SX 모니터링 인터페이스(SC 커넥터 포함)
IDS-PWR=	Cisco IDS 4235/4250 장비 센서용 예비 전원 공급 장치
IDS-SCSI=	Cisco IDS 4250 장비 센서용 예비 SCSI ¹ 하드 디스크 드라이브
IDS-RAIL-2=	IDS 4235/4250 센서 플랫폼용 포스트 레일 키트 2개
IDS-RAIL-4=	Cisco IDS 4235/4250 센서 플랫폼용 포스트 레일 키트 4개
CON-SNT-IDS4210 CON-SNTE-IDS4210 CON-SNTP-IDS4210 CON-OS-IDS4210 CON-OSE-IDS4210 CON-OSP-IDS4210	Cisco SMARTnet [™] 8 x 5 x NBD ² 서비스(Cisco IDS 4210) Cisco SMARTnet 8 x 5 x 4 고급형 서비스(Cisco IDS 4210) Cisco SMARTnet 24 x 7 x 4 프리미엄 서비스(Cisco IDS 4210) Cisco SMARTnet 8 x 5 x NBD 방문(Onsite) 표준형 서비스 Cisco (IDS 4210) Cisco SMARTnet 8 x 5 x 4 방문 고급형 서비스 (Cisco IDS 4210) Cisco SMARTnet 24 x 7 x 4 방문 프리미엄 서비스 (Cisco IDS 4210)
CON-SNT-IDS4235K9 CON-SNTE-IDS4235K9 CON-SNTP-IDS4235K9 CON-OS-IDS4235K9 CON-OSE-IDS4235K9 CON-OSP-IDS4235K9	Cisco SMARTnet 지원 8 x 5 x NBD(Cisco IDS 4235) Cisco SMARTnet 지원 8 x 5 x 4(Cisco IDS 4235) Cisco SMARTnet 지원 24 x 7 x 4(Cisco IDS 4235) Cisco SMARTnet 방문 지원 8 x 5 x NBD(Cisco IDS 4235) Cisco SMARTnet 방문 지원 8 x 5 x 4(Cisco IDS 4235) Cisco SMARTnet 방문 지원 24 x 7 x 4(Cisco IDS 4235)
CON-SNT-IDS4250TK CON-SNTE-IDS4250TK CON-SNTP-IDS4250T CON-OS-IDS4250TK CON-OSE-IDS4250TK CON-OSP-IDS4250TK	Cisco SMARTnet 지원 8 x 5 x NBD(Cisco IDS 4250-TX) Cisco SMARTnet 지원 8 x 5 x 4(Cisco IDS 4250-TX) Cisco SMARTnet 지원 24 x 7 x 4 (Cisco IDS 4250-TX) Cisco SMARTnet 방문 지원 8 x 5 x NBD(Cisco IDS 4250-TX) Cisco SMARTnet 방문 지원 8 x 5 x 4 Cisco (IDS 4250-TX) Cisco SMARTnet 방문 지원 24 x 7 x 4(Cisco IDS 4250-TX)
CON-SNT-IDS4250SK CON-SNTE-IDS4250SK CON-SNTP-IDS4250SK CON-OS-IDS4250SK CON-OSE-IDS4250SK CON-OSP-IDS4250SK	Cisco SMARTnet 지원 8 x 5 x NBD Cisco (IDS 4250-SX) Cisco SMARTnet 지원 8 x 5 x 4(Cisco IDS 4250-SX) Cisco SMARTnet 지원 24 x 7 x 4(Cisco IDS 4250-SX) Cisco SMARTnet 방문 지원 8 x 5 x NBD(Cisco IDS 4250-SX) SMARTnet 방문 지원 8 x 5 x 4(Cisco IDS 4250-SX) SMARTnet 방문 지원 24 x 7 x 4(Cisco IDS 4250-SX)

¹Small Computer Serial Interface

²Next Business Day

수출 시 고려사항

Cisco IDS 4200 Series 장비 센서는 컨트롤을 수출할 수 있습니다.
 수출 관련 규정은 다음 사이트의 안내를 참조하십시오.
<http://www.cisco.com/www/export/crypto/>
 수출에 관한 문의는 export@cisco.com으로 보내주시기 바랍니다.

추가 정보

Cisco Intrusion Detection System:
<http://www.cisco.com/go/ids>
 Cisco VMS 솔루션 (IDS 관리):
<http://www.cisco.com/go/vms>



www.cisco.com/kr

2002-04-02

■ Gold 파트너	• ㈜데이콤아이엔	02-6747-4718	• 한국아이비엠(주)	02-3781-7187	• 쌍용정보통신(주)	02-2262-8496
	• ㈜데이터크레프트코리아	02-6256-7050	• ㈜콤텍시스템	02-3289-0190	• 에스넷시스템(주)	02-3469-2481
	• ㈜인네트	02-3451-5315				
■ Silver 파트너	• ㈜링네트	02-6675-1220	• ㈜인성정보	02-3400-7300	• 한국에이치피(주)	02-2199-0964
	• 케이디씨정보통신(주)	02-3459-0500				
■ Local SI 파트너	• 대우정보시스템	02-3708-8606	• ㈜시스폴	02-6009-6009	• 현대정보기술	02-2129-4285
	• 엘지전자(주)	02-818-4042	• 포스데이터주식회사	031-779-2630	• 이스텔시스템즈(주)	031-467-7100
	• SK씨앤씨(주)	02-2196-8342				
■ Global 파트너	• 이퀼트코리아	02-3782-2674	• 한국썬마이크로시스템즈	02-2193-5181	• 한국후지쯔(주)	02-3787-5510
	• 컴팩코리아(주)	02-6002-2223	• 한국유니시스(주)	02-768-1432	• 한국엔씨알	02-3279-4301
■ Local 디스트리뷰터	• ㈜소프트뱅크코리아	02-2187-0140	• ㈜인큐브테크(구)엘렉스 컴퓨터)	02-709-8127	• ㈜아이넷뱅크	02-3400-7083
■ Optical 전문 파트너	• 삼우통신공업	02-890-6410				
■ IPT 파트너	• 청호정보통신	02-3498-3114	• LG기공	02-2630-5156		
■ WLAN 전문 파트너	• ㈜에어커	02-541-1557	• ㈜텔레트론 아이엔씨	02-2105-2385		
■ Security 전문 파트너	• 코코넷	02-6007-0143	• TISS	051-743-5940		
■ NMS 전문 파트너	• ㈜넷브레인	02-568-4050				