Cisco IPS 4300 Series

사용자와 데이터가 기업 경계를 넘어가고 있습니다. 이에 따라 네트워크 액세스 계층의 투과성이 점점 커지고 있으며, 디지털 서명만을 사용하는 감지 제품은 일차원적 응답으로 이어질 수 있습니다. Cisco 만이 공격 대상 OS, 회피 기법, 디지털 서명 전반에 걸친 공격 상태, 그리고 업계 최초의 공격자 ID 및 동작을 포함하는 모든 분석 단계의 폭넓은 네트워크 컨텍스트를 사용합니다.

Cisco® ntrusion Prevention Sensor(IPS) 4300 Series 는 소규모 사무실과 지사 사업장에서 대기업 데이터 센터 아키텍처까지 광범위한 배치 시나리오에 맞게 확장이 가능합니다. 처리량 속도가 1Gbps~10Gbps 에 이르는 각 IPS 4300 Series 모델은 일관된 보호 수준을 제공합니다. Cisco IPS 4300 Series 는 1-RU 폼 팩터에서 하드웨어 가속 검사 성능, 높은 포트 밀도 및 에너지 효율성을 제공합니다(그림 1). 효율성과 함께 이미 탑재된 보안과 위협 관리 자동화를 통해 주요 데이터 센터 자산이 몇 분 만에 바로 보호됩니다.

그림 1. Cisco IPS 4345 및 4360 Sensor

고급 위협 방지

Cisco IPS 솔루션은 다음과 같은 이점을 제공합니다.

- 5 천 5 백개 이상되는 디지털 서명을 통한 광범위하면서도 심층성 있는 보호 기능
- 특허 획득 회피 방지 기술을 통한 웜, 바이러스, 트로이 목마, 정찰 공격, 스파이웨어, 봇네트, 원하지 않는 애플리케이션, 악성 코드 등의 방어 및 모니터링
- 최종 위협 결정을 위한 프로토콜 및 동작 분석
- DoS(denial of service), DDoS(distributed denial of service), SYN 플러딩 및 암호화된 공격의 소스를 식별하고 이러한 공격을 차단할 수 있도록 해주는 Cisco Global Correlation
- Cisco 인프라 보호에 도움이 되는 유니파이드 커뮤니케이션, WLAN, 라우팅 및 스위칭에 대한 전용 보호 방식

규정 준수 보장

Cisco IPS 솔루션은 고객이 다음과 같은 개인정보 및 데이터 보호 규정을 준수할 수 있도록 지원합니다.

- PCI(Payment Card Industry) 표준
- 유럽 연합 개인정보 보호 규칙
- 미국 SOX(Sarbanes-Oxley Act)

- 미국 GLBA(Gramm-Leach-Bliley Act)
- NERC CIP(Critical Infrastructure Protection)
- HIPAA(Health Insurance Portability and Accountability Act)

원활한 네트워크 통합

Cisco IPS 기술은 업계에서 가장 앞선 네트워크 인식 기능을 제공합니다. 데이터 센터, 코어, 에지 등 무엇을 방어하든 Cisco IPS 솔루션은 레이어 7 까지 위협 방지를 제공합니다. Cisco IPS 솔루션은 설비 투자를 줄일 수 있도록 라우팅, 스위칭, 방화벽 플랫폼 등 Cisco 네트워크 어디에서나 배포를 가능하게 하는 공용 소프트웨어 아키텍처를 기반으로 하고 있습니다. 일관된 정책 및 운영 프레임워크를 통해 시스템을 통합하여 보다 적은 운영 비용으로 규정을 준수하고 위험을 관리할 수 있습니다.

최상의 Global Correlation

APT(Advanced Persistent Threat), 봇네트 및 기타 복합적 위협이 진화하고 있습니다. 이제 디지털 서명 기반 콘텐츠 검사만으로는 부족합니다. Cisco IPS 는 지난 10 년간 축적된 평판 기술의 유산을 이용해 디지털 서명 기반 공격뿐 아니라 소스 평판을 기반으로 공격을 식별하고 완화할 수 있는 유일한 IPS 입니다. Cisco Security Intelligence Operations(SIO)가 지원되는 Cisco IPS Global Correlation 과 함께 Cisco IPS 를 사용하면 수백 개의 추가 보안 매개변수와 수백만 개의 규칙의 열람이 가능하며, 업계 선두를 달리고 있는 이메일, 웹, 방화벽 및 IPS 장치를 통해 하루 8TB 의 위협을 측정할 수 있습니다.

이미 준비된 네트워크 기능

가장 까다로운 네트워크 요구를 충족하기 위해 Cisco IPS 기술을 방화벽에 직접 통합했습니다. 수 기가비트의 성능, 짧은 대기 시간 및 고가용성 기능 제공이 가능합니다. 하드웨어 가속 심층 패킷 분석 기능이 포함된 Cisco IPS 4300 Series 는 다양한 애플리케이션과 배포를 지원할 수 있도록 750Mbps~1.25Gbps 범위의 성능을 제공합니다. Cisco 에서 IPS 성능 계산에 사용하는 고유 방법론에 대한 자세한 내용은 Cisco IPS 4500 및 4300 Series Sensor 의 성능을 참조하십시오. 유연한 고가용성 배포 옵션에는 작동-작동 및 작동-대기 구성, 실패-열기 또는 실패-닫기 모드, IDS 및 IPS 모드 그리고 예비 전원 공급 장치가 포함됩니다. IPS 4300 Series 는 또한 GRE, MPLS, 802.1q, IPv4 in IPv4, IPv4 in IPv6, Q-in-Q double VLAN 을 비롯 캡슐화된 트래픽을 검사할 수 있는 기능도 제공합니다.

이미 입증된 위협 방지

1 억 달러가 넘는 보안 연구 부문 투자와 5 백여명의 위협 분석가, 매일마다 Cisco SensorBase™에는 테라바이트 규모의 위협 데이터가 공급됩니다. 이러한 데이터의 분석을 통해 Cisco 는 고객 네트워크에 신뢰를 제공합니다. Cisco IPS 가 세계에서 가장 널리 배포된 상용 IPS 기술이 된 것도, 독립 테스트 기관에서 Cisco IPS 를 권장하는 배경에는 바로 이런 이유가 존재합니다.

완벽한 제어와 실시간 가시성

Cisco 는 소규모 배포용 관리 솔루션은 물론 엔터프라이즈급 관리 솔루션도 제공합니다. Cisco IPS Manager Express 는 최대 10 개의 장치를 위한 올인원 IPS 관리 및 리포팅 애플리케이션입니다. Cisco Security Manager 는 이론 상만의 보안이 아닌 이미 수천 개 기업에 배포된 실제상황에서 사용되고 있는 엔터프라이즈급 보안 관리 애플리케이션입니다.

두개의 솔루션 모두 Cisco IPS 4300 Series 는 물론 기타 Cisco 센서 어플라이언스, Cisco ISR(Integrated Services Router) 및 Cisco IDSM(Intrusion Detection Services Module)을 지원합니다.

Cisco IPS Manager Express 는 다음과 같은 기능을 제공합니다.

- 프로비저닝, 모니터링 및 문제 해결
- 드래그 앤 드롭 대시보드 도구를 통한 용이한 사용자 지정과 개인화된 사용자 설정을 기억하는 맞춤형 보기로 설정 시간 최소화
- 맞춤형 리포트 및 규정 준수 리포트를 몇 초 만에 생성하는 유연한 리포팅 툴

Cisco Security Manager 4.x 는 다음과 같은 기능을 제공합니다.

- 새로운 디지털 서명과 업데이트된 서명의 점증적인 프로비저닝 및 해당 디지털 서명에 대한 IPS 정책 생성과 장치 간의 정책 공유가 가능한 유연한 프로세스
- Cisco IPS Global Correlation 등 Cisco 최신 IPS 기능을 지원하는 향상된 리포팅 및 이벤트 관리 지원
- 오류 없는 배포 및 프로세스 규정 준수를 위한 RBAC(역할 기반 액세스 제어) 및 워크플로

표 1 과 2 에는 Cisco IPS 4300 Series Sensor 의 사양이 나열되어 있습니다.

표 1. Cisco IPS 4300 Series 사양

기능	Cisco IPS 4345	Cisco IPS 4360
평균 검사 처리량	750Mbps	1.25Gbps
최대 검사 처리량	1.8Gbps	2.4Gbps
최대 연결 수	750,000	1,700,000
초당 연결 수	30,000	45,000
평균 대기 시간	<150µ	<150µ
위협 방지	25,000 개가 넘는 위협	25,000 개가 넘는 위협
프로토콜 이상 감지	예	예
회피 식별 및 완화	예	예
애플리케이션 이상 감지	예	예
수동 OS 핑거프린팅	예	예
글로벌 연관성	예	예
검사 전 평판 블랙 리스트	예	예
평판 중심의 완화 선택	예	예
복합적 서명 분석(서로 다른 알림이 결합되어 ID 가 높은 순서로 위협이 열거됨)	예	예
사용자 지정 가능한 서명 등급: 심각도, 신뢰도	예	예
맞춤형 디지털 서명 지원	예	예

표 2. Cisco IPS 사양

기능	Cisco IPS 4345	Cisco IPS 4360
관리 및 모니터링 인터페이스	이더넷 10/100 포트 1 개	이더넷 10/100 포트 1 개
CPU	멀티코어	멀티코어
메모리	8GB	16GB
데이터 포트	8 x 1GE	8 x 1GE
최소 플래시	8GB	8GB
온도	-4~45ºC(24.5~113ºF)	-4~45ºC(24.5~113ºF)
상대 습도(작동)	10 - 90% 비응결	10 - 90% 비응결
고도(작동)	3024m(0~9,921 피트)	3024m(0~9,921 피트)
최대 사용	최대 30W	최대 90W

기능	Cisco IPS 4345	Cisco IPS 4360
MTBF(Mean Time Between Failure)	874,070 시간(100 년)	299,588 시간(31 년)
크기(HxWxD)	4.24 x 42.9 x 39.5cm (1.67 x 16.9 x 15.5 인치)	4.24 x 42.9 x 48.4cm (1.67 x 16.7 x 19.1 인치)
무게	6.77kg(14.92lb)	7.63kg(16.82lb)
안전	UL 1950, CSA C22.2 No. 950, EN 60950 IEC 60950, AS/NZS3260, TS001	UL 1950, CSA C22.2 No. 950, EN 60950 IEC 60950, AS/NZS3260, TS001
전자기 호환성(EMC)	CE marking, FCC Part 15 Class A, AS/NZS 3548 Class A, VCCI Class A, EN55022 Class A, CISPR22 Class A, EN61000-3-2, EN61000-3-3	CE marking, FCC Part 15 Class A, AS/NZS 3548 Class A, VCCI Class A, EN55022 Class A, CISPR22 Class A, EN61000-3-2, EN61000-3-3

주문 정보

제품 주문은 Cisco 주문 홈 페이지를 방문하십시오. 주문 정보는 표 3 을 참조하십시오.

표 3. 주문 정보

제품 이름	제품 번호
Cisco IPS 4300 Series	
Cisco IPS 4345 Sensor	IPS-4345-K9
Cisco IPS 4360 Sensor	IPS-4360-K9
Cisco IPS 4345 Sensor(DC 전원 버전)	IPS-4345-DC-K9
Cisco IPS 4360 Sensor(DC 전원 버전)	IPS-4360-DC-K9

서비스 및 지원

Cisco 는 고객이 보다 빠른 시일 내에 성공을 거둘 수 있도록 다양한 서비스 프로그램을 제공합니다. Cisco 의 혁신적인 프로그램은 인력, 프로세스, 툴, 파트너의 독특하고 독창적인 조합을 통해 제공되며 높은 수준의 고객 만족을 실현합니다. Cisco 서비스는 고객의 네트워크 투자를 보호하고 네트워크 운영을 최적화하며 새로운 애플리케이션에 맞는 네트워크의 준비를 통해 네트워크 인텔리전스와 고객의 비즈니스 능력 강화에 기여합니다. Cisco 보안 서비스에 관한 자세한 내용은 http://www.cisco.com/go/services/securit 를 참조하십시오.

Cisco Services for IPS

Cisco Services for IPS 는 Cisco IPS 4300 Series 솔루션에 포함되어 있으며, 운영자가 디지털 서명 파일과 알림 등 시간임계적인 정보를 전송합니다. Cisco Services for IPS 는 Cisco Technical Support Services 포트폴리오의 일부분으로써, Cisco IPS 4300 Series Sensor 가 항상 최근의 위협에 관해 업데이트를 받아 악의적이거나 손상을 일으키는 트래픽을 정확하게 파악하고 분류 및 중단시킵니다. Cisco Services for IPS 기능에는 다음이 포함됩니다.

- 디지털 서명 파일 업데이트 및 알림
- 글로벌 위협 상관관계 신뢰도 피드
- 온라인 툴 및 기술 지원을 받기 위해 Cisco.com 에 등록을 통한 액세스
- Cisco 기술 지원 센터(Technical Assistance Center) 액세스
- Cisco IPS 소프트웨어 업데이트
- 고장 난 하드웨어의 선 교체

Cisco Services for IPS 에 대한 자세한 내용은 http://www.cisco.com/en/US/products/ps6076/serv_group_home.html 을 참조하십시오.

수출 시 고려 사항

Cisco IPS 4300 Series 제품은 수출 관리 대상입니다. 자세한 내용은 수출 규정 준수 웹 사이트 http://www.cisco.com/wwl/export/crypto/를 참조하십시오. 수출과 관련된 구체적인 질문은 export@cisco.com 으로 문의하십시오.

추가 정보

자세한 내용은 다음 링크를 참조하십시오.

- Cisco Intrusion Prevention System: http://www.cisco.com/go/ips
- Cisco IDS 및 IPS 센서 그리고 판매 중지 상태의 소프트웨어 버전에 대한 자세한 내용은 http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_eol_notices_list.html 을 참조하십시오.
- Cisco Security Manager: http://www.cisco.com/go/csmanager
- Cisco IPS Manager Express: http://www.cisco.com/go/ime

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

인쇄지: 미국 C78-701659-00 03/12