Industrial Security Appliance 3000 데이터 시트

가장 혹독한 산업 환경에서도 견딜 수 있게 특별히 개발된 ISA 3000 보안 디바이스는 산업 설계 및 운영을 고려한 최고 성능의 엔드 투 엔드 보안을 제공합니다.

제품 개요

Cisco® Industrial Security Appliance 는 검증된 엔터프라이즈급 보안을 기반으로 OT 대상 보호를 제공하는 진정한 산업용 어플라이언스입니다.

4 개의 데이터 링크가 포함된 ISA 3000 은 내구성을 강화한(ruggedized) DIN 레일 마운트 어플라이언스로서 가장 혹독하고 까다로운 산업 환경을 위해 가장 광범위한 액세스, 위협 및 애플리케이션 제어 기능을 제공합니다.

ISA 3000 Series 는 IE 4000 스위치 하드웨어 설계와 마찬가지로, 강력한 산업용 솔루션일 뿐만 아니라 Cisco ASA 및 SourceFire 소프트웨어의 검증된 보안 기능도 갖추고 있습니다. ISA 3000 은 고객의 네트워크 현대화 프로젝트에 안전과 보안을 모두 제공할 수 있는 이상적인 솔루션입니다. 또한 산업 운영 방식에 방해가 되지 않으면서 IT 및 OT 보안 가시성을 통합하기 위한 기준점을 제공합니다. 이 보안 어플라이언스는 전반적인 IT 네트워크 설계, 규정준수, 성능 요건을 준수하는 동시에 극한의 환경을 견디고 산업 설계를 반영하도록 구축되었습니다.

ISA 3000 Series 는 내구성이 강화된 제품이 필요한 산업용 이더넷 애플리케이션에 매우 적합합니다. 여기에는 유틸리티 산업, 제조, 에너지 및 프로세스 제어, ITS(Intelligent Transportation System), 유전 및 가스 산지 현장, 도시 감시 프로그램, 광업이 포함됩니다. 단일 디바이스 내에서 의심스러운 파일 전파, 코일 설정 지점, 비정상적 트래픽 패턴, 권한 에스컬레이션을 모두 동시에 추적할 수 있는 기능 덕분에 그 어느 때보다 뛰어난 보안 및 안전 가시성이 구현됩니다. Cisco 보안 네트워킹 포트폴리오의 이러한 산업 요소는 다른 산업 등급의 Cisco 솔루션과 협력적으로 상호 작용할 뿐만 아니라, 로컬 셀과 IT 조직, 외부 벤더 또는 계약업체 활동 간의 상호 작용에 대해 완벽한 가시성을 제공합니다.

사용자 친화적인 온박스(on-box) 시스템 매니저 또는 전사적인 보안 관리를 통해 관리되는 ISA 3000 에서는 산업 환경에 초점을 맞춘 아웃-오브-더-박스(out-of-the-box) 컨피그레이션과 간소화된 운영 관리 용이성이 제공됩니다. 이러한 고도의 맞춤형 관리 옵션을 사용하여 산업 기능과 IT 기능의 불가피한 혼합을 위해 로컬 운영 인식을 간소화하고 더 높은 수준의 IT/OT 보안 통합을 구현할 수 있습니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

기능 및 혜택

표 1. Cisco ISA 3000 의 기능 및 혜택

기능	혜택
강력한 산업 설계	● 혹독한 환경과 온도 범위(-40°~70°C)를 위한 설계 ● 모든 ISA 3000 은 절연 방수 코팅(conformal coating) 처리 ● 진동, 충격, 서지(surge), 전기적 잡음 내성을 위해 내구성 강화 ● 4 개의 1 기가비트 이더넷 업링크 포트를 통해 복원력을 갖춘 여러 설계 옵션 제공(4 copper 또는 2cu/2 fiber) ● 산업 자동화, ITS, 변전소 환경을 위한 다중 산업 사양 준수 ● 산업 시스템 및 장비의 가동 시간, 성능, 안전 향상 ● 산업 LED 기능을 갖춘 컴팩트한 DIN 레일 유닛 설계를 통해 간편하게 모니터링 가능 ● 내구성 확장을 위해 가동부(moving part)를 사용하지 않는, 팬이 없는 대류 냉각 방식 ● IEEE 1588v2 PTP(파워 프로필과 기본 프로필 모두 지원) ● 외부 장비에 대한 모니터링 및 신호 전달을 위한 경보 I/O (향후 릴리스에서 사용 가능) ● 컨피그레이션 백업 및 부팅용 SD 카드 (향후 릴리스에서 사용 가능)
사용자 친화적 GUI 디바이스 매니저	● 로컬 인식 즉시 제어를 위한 온디바이스(on-device) 관리 ● 다중 디바이스 관리를 통해 수백 개의 디바이스 처리 가능 ● 사용자별 액세스 및 제어 맞춤화
트래픽 연속성/보호	● 풀(full) “정전” 트래픽 바이패스 카퍼 포트 ● 기본 패시브 구축 학습 모드 ● 트래픽 손실 없이 소프트웨어 업데이트 가능 ● 연결 제한을 통해 트래픽을 유발하는 DOS 로부터 보호 ● 레이턴시 탐지 및 완화 기능 ● QoS(Quality of Service) 정책
검증된, 확장 가능한 액세스 제어	● ISA-95/IEC 62264 세그멘테이션 요구사항 집행 ● 풀(full) 스테이트풀 인스펙션 ● Layer 2 및 Layer 3 방화벽 운영 모드 ● 다운로드 가능한 ACL(Access Control List) ● 신원 기반 액세스 제어 정책 ● 사용자/사용자 그룹 ● 정책 기반 라우팅 ACL ● 확장된 ACL ● WebVPN ACL ● Dynamic ACLs ● TrustSec ACL
최고의 위협 탐지 기능	● 서드파티 테스트에서 검증된 가장 효과적인 위협 탐지 기능 ● 25,000 개가 넘는 규칙을 통해 어디서나 가장 광범위한 보호 제공 ● 수백 개의 산업 중심 규칙 ● 산업 장비 익스플로잇 공격 차단 규칙 ● 프로토콜 남용 파악 ● 웹 기반 제어 시스템 보호 ● 네트워크 동작 분석 ● 패시브 디바이스 검색
애플리케이션 제어	● 모든 DMZ 인프라의 가시성 및 제어 ● 산업 애플리케이션의 가시성 및 제어 ● 개별 프로토콜 명령과 값의 가시성 및 제어

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

기능	혜택
원격 액세스 지원/제어	• Cisco AnyConnect 를 통한 네트워크 액세스 제어 • ISE(Identity Services Engine) 지원 • 사이트 대 사이트 VPN • 원격 액세스 VPN • 클라이언트리스(clientless) SSL VPN 오퍼링 • Cisco Secure Desktop • Citrix 및 VMware 클라이언트리스 연결 지원
DMZ 인프라	• DNS 서비스 • DHCP 서비스 • AAA 지원 • IP 라우팅

산업 환경을 위해 내구성을 강화한 솔루션

Cisco Industrial Security Appliance 3000 Series 는 다음을 제공합니다.

- 셀 및 변전소 레벨에서 ISP 연결성에 이르는 제어된 액세스
- 유연한 엔터프라이즈급 원격 액세스
- DNS, DHCP 등의 기본 네트워크 인프라 서비스 제공
- 스위치, 라우터, OS, 컴퓨팅 인프라에서 산업 제어 시스템에 이르는 모든 네트워킹 및 컴퓨팅 레벨에 탁월한 위협 차단 기능 구현
- 산업 환경에서 다른 제품보다 더 많은 트래픽 연속성 안전 레벨 제공
- 산업 및 엔터프라이즈 환경에서 모든 애플리케이션 레벨에 애플리케이션 가시성 및 제어 기능 구현

그림 1 은 ISA 3000 이고, 표 2 는 사용 가능한 ISA 3000 주문 PID 이며, 표 3 은 Cisco Industrial Security Appliance 3000 Series 용 SFP 모듈입니다.

그림 1. ISA 3000

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

표 2. Cisco Industrial Security Appliance 3000 Series 모델 및 옵션:

제품 번호	Copper 10/100/1000(모든 바이패스 지원)	SFP 파이버 포트
ISA3000-4C-K9	4	0
ISA3000-2C2F-K9	2	2
	주문 가능한 선택적 기능	
L-ISA3000SEC+-K9	HA 지원, SSL VPN, 더 많은 연결 수, VLAN 트렁킹	

표 3. 지원되는 Cisco Ruggedized SFP

제품 번호	유형
GLC-SX-MM-RGD=	1000 BASE-SX Ruggedized
GLC-LX-SM-RGD=	1000 BASE-LX/LH Ruggedized
GLC-FE-100FX-RGD=	100 BASE-FX Ruggedized
GLC-FE-100LX-RGD=	100 BASE-LX Ruggedized

제품 사양

표 4 는 물리적 사양이고, 표 5 는 디바이스 성능 및 확장성에 대한 정보이며, 표 6 과 7 은 일부 중요한 소프트웨어 기능입니다. 또한 표 8 은 규정준수 사양이고, 표 9 는 Cisco ISA 3000 Series 의 관리 및 표준에 대한 정보입니다.

표 4. 물리적 사양

설명	사양
하드웨어	• 4 Core Intel Rangely(I-temp) • 8GB DRAM(soldered down) • 16GB 온보드 플래시 메모리 • mSATA 64Gb • 1GB 이동식 SD 플래시 메모리 카드 - 산업 온도(향후 릴리스에서 사용 가능) • 콘솔용 미니 USB 커넥터 • RJ-45 전통적 콘솔 커넥터 • 전용 10/100/1000 관리 포트 • 하드웨어 기반 위/변조 방지 칩 • 공장 초기화 옵션
경보	• 경보 I/O: 드라이 컨택(dry contact)이 열려 있거나 닫혀 있는 것을 탐지하는 4 개의 경보 입력, 1 개의 Form C 경보 출력 릴레이(향후 릴리스에서 사용 가능)
크기(H x W x D)	• 11.2cm(너비) x 13cm(높이) x 16cm(깊이)
무게	• 1.9kg
전원 공급 장치 및 범위	• 듀얼 내부 DC • 공칭 전압 ± 12Vdc, 24Vdc 또는 48Vdc • 최대 범위 9.6Vdc ~ 60Vdc • 전력 소비량 24 와트
MTBF(Mean Time Between Failure)	• ISA-3000-4C 398,130 시간 • ISA-3000-2C2F 376,580 시간

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

표 5. 디바이스 확장성

설명	사양
처리량	최대 2Gbps - 최소 22Mbps 트래픽 유형과 보안 활동에 따라 다름 (트래픽 프로필을 알아보려면 Cisco SE 와 협력하여 주십시오.)
IPSec VPN 터널	5, 25(SecPlus 라이센스의 경우)
정의된 인터페이스	200, 400(SecPlus 라이센스의 경우)
VLAN 수	5, 25(SecPlus 라이센스의 경우)
IPv4 MAC 보안 ACE	기본 TCAM 템플릿의 경우 1,000
NAT 변환	올바르게 설계될 경우 수만 개의 변환된 항목으로 확장될 수 있는 128 개의 고유한 양방향 서브넷 NAT 변환 엔트리

표 6. Cisco ISA 3000 의 주요 네트워크 지원 기능

LAN Base 라이센스(기본값)	기능
NAT	• Static NAT 포트 변환, 일대다, 비표준 포트의 경우 • Dynamic NAT • Dynamic PAT • Identity NAT
Layer 2 IPv6	IPv6 호스트 지원, HTTP over IPv6, SNMP over IPv6
Layer 3 라우팅	IPv4 Static 라우팅
유틸리티	IEEE 1588 v2 PTP 파워 프로필
관리 트래픽에 대한 별도의 라우팅	데이터와 관리 트래픽 라우팅 분리
트렁킹	802.1q 트렁크 지원됨

표 7. Cisco ISA 3000 의 주요 보안 소프트웨어 기능

보안 영역	기능
TrustSec 제어	• 대역 내(in-band) 및 대역 외(out of band) 신원 • Active Directory 통합 • 보안 그룹 태그 기반 정책 • 802.1x 지원 • MACSec 및 MAB 지원 • 원격 액세스를 위한 엔드포인트 보안 상태 집행
다중 레벨 액세스 제어	• 글로벌 블랙리스트 - 자동 또는 수동 • 글로벌 화이트리스트 • 서드파티 인텔리전스 피드 활용 • 파일 화이트리스트 • 파일 블랙리스트 • 애플리케이션 레벨 액세스 제어 • 802.1x 지원
위협 네트워크 매핑	• 패시브 디바이스 식별 • 모바일 디바이스 식별 • 애플리케이션 호스트 네트워크 매핑 • 취약성/호스트 네트워크 매핑 • 사용자/호스트 네트워크 매핑

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

보안 영역	기능
위협 검색	• IoC(Indicators of Compromise, 침해지표) 추적 • OpenAppID - 개방형 커뮤니티 ID 시스템 • 상관관계 정책 및 응답 • 트래픽 변동 탐지 • 라우터 기반 치료 조치 • Netflow 추적 • 25,000 개 이상의 위협 식별자 • 맞춤형 식별자 • 완전히 새로운 식별자 생성 가능 • 가장 광범위한 식별자 기여자 역할
파일 추적	• 승인된 파일 추적 • 의심스러운 파일 추적 • 악성코드 일치

표 8. 규정준수 사양

유형	표준
전자기 방사	FCC 47 CFR Part 15 Class A EN 55022A Class A VCCI Class A AS/NZS CISPR 22 Class A CISPR 11 Class A CISPR 22 Class A ICES 003 Class A CNS13438 Class A KN22
전자기 내성	EN55024 CISPR 24 AS/NZS CISPR 24 KN24 EN 61000-4-2 Electro Static Discharge EN 61000-4-3 Radiated RF EN 61000-4-4 Electromagnetic Fast Transients EN 61000-4-5 Surge EN 61000-4-6 Conducted RF EN 61000-4-8 Power Frequency Magnetic Field EN 61000-4-9 Pulse Magnetic Field EN 61000-4-18 Damped Oscillatory Wave EN-61000-4-29 DC Voltage Dips and Interruptions
업계 표준	EN 61000-6-1 Immunity for Light Industrial Environments EN 61000-6-2 Immunity for Industrial Environments EN 61000-6-4 Emission Standard for Industrial Environments EN 61326 Industrial Control EN 61131-2 Programmable Controllers IEEE 1613 Electric Power Stations Communications Networking IEC 61850-3 Electric Substations Communications Networking

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

유형	표준
안전 표준 및 인증	**정보 기술 장비:** UL/CSA 60950-1 EN 60950-1 CB to IEC 60950-1(모든 국가별 편차 포함) NOM to NOM-019-SCFI(파트너 및 총판사를 통해) **산업 플로어(제어 장비):** UL 508 CSA C22.2, No 142 EN/IEC 61010-2-201(transitional) **위험 장소** ANSI/ISA 12.12.01(Class I, Div 2 A-D) CSA 213(Class 1, Div 2 A-D) UL/CSA 60079-0, -15 IEC 60079-0, -15 (IECEx test report Class I, Zone 2, group II gases) EN 60079-0, -15 ATEX certification (Class I, Zone 2, group II gases)
작동 환경	작동 온도: -40C ~ +74C ● -40C ~ +70C (Vented Enclosure Operating) ● -40C ~ +60C (Sealed Enclosure Operating) ● -34C ~ +75C (Fan or Blower equipped Enclosure Operating) EN 60068-2-21 EN 60068-2-2 EN 61163
보관 환경	온도: -40 ~ +85°C 고도: 0~15,000 피트 IEC 60068-2-14
습도	상대 습도 5% ~ 95%(비응축) IEC 60068-2-30
충격 및 진동	● IEC60068-2-6 및 IEC60068-2-27 ● MIL-STD-810, Method 514.4 ● Marine EN60945 ● Industrial EN61131-2/IEC61131-2 ● Railway EN50155 ● Smart Grid EN61850-3 ● IEEE 1613
부식	ISO 9223: Corrosion class C3-Medium class C4-High EN 60068-2-52 (Salt Fog) (Pending) EN 60068-2-60 (Flowing Mixed Gas) (Pending)
기타	RoHS Compliance 중국 RoHS Compliance TAA(정부) CE(유럽)
워런티	모든 ISA 3000 PIDS 에 대한 5 년 제한적 HW 워런티 에 대한 자세한 내용은 데이터 시트 끝부분의 링크를 참조하시기 바랍니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

표 9. 관리 및 표준

설명	사양	
IEEE 표준	• IEEE 802.1D MAC Bridges, STP • IEEE 802.1p Layer2 COS prioritization • IEEE 802.1q VLAN • IEEE 802.1s Multiple Spanning-Trees • IEEE 802.1w Rapid Spanning-Tree • IEEE 802.1x Port Access Authentication • IEEE 802.1AB LLDP • IEEE 802.3ad Link Aggregation (LACP)	• IEEE 802.3ah 100BASE-X SMF/MMF only • IEEE 802.3x full duplex on 10BASE-T • IEEE 802.3 10BASE-T 사양 • IEEE 802.3u 100BASE-TX 사양 • IEEE 802.3ab 1000BASE-T 사양 • IEEE 802.3z 1000BASE-X 사양 • IEEE 1588v2 PTP Precision Time Protocol
RFC 규정준수	• RFC 768: UDP • RFC 783: TFTP • RFC 791: IPv4 protocol • RFC 792: ICMP • RFC 793: TCP • RFC 826: ARP • RFC 854: Telnet • RFC 951: BOOTP • RFC 959: FTP • RFC 1157: SNMPv1 • RFC 1901,1902-1907 SNMPv2 • RFC 2273-2275: SNMPv3 • RFC 2571: SNMP Management • RFC 1166: IP Addresses • RFC 1256: ICMP Router Discovery	• RFC 1305: NTP • RFC 1492: TACACS+ • RFC 1493: Bridge MIB Objects • RFC 1534: DHCP and BOOTP interoperation • RFC 1542: Bootstrap Protocol • RFC 1643: Ethernet Interface MIB • RFC 1757: RMON • RFC 2068: HTTP • RFC 2131, 2132: DHCP • RFC 2236: IGMP v2 • RFC 3376: IGMP v3 • RFC 2474: DiffServ Precedence • RFC 3046: DHCP Relay Agent Information Option • RFC 3580: 802.1x RADIUS • RFC 4250-4252 SSH Protocol

[1] 지원되는 SFP 모델의 전체 목록은 http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html 을 참조하십시오.
[2] MMF = Multi-Mode Fiber
[3] SMF = Single-Mode Fiber

워런티 정보

ISA 3000 의 워런티 정보는 http://www.cisco-servicefinder.com/warrantyfinder.aspx 에서 확인할 수 있습니다.

Cisco 및 파트너 서비스

Cisco 는 고객의 TCO 를 최소화하기 위해 최선을 다하고 있으며, 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. 시스코 서비스는 고객의 네트워크 투자를 보호하고, 네트워크 운영을 최적화하며, 새로운 애플리케이션에 맞는 네트워크의 준비를 통해 네트워크 인텔리전스와 고객의 비즈니스 역량 강화에 기여합니다. Cisco 고객이 시스코 서비스로부터 얻을 수 있는 주요 혜택 중 일부는 다음과 같습니다.

- 사전 대응적 문제 해결 또는 더 신속한 문제 해결을 통해 위험 완화
- Cisco 의 전문성과 지식을 활용하여 TCO 절감
- 네트워크 다운타임 최소화
- 기존 지원 인력이 다른 생산적인 활동에 주력할 수 있도록 지원

시스코 서비스에 대한 자세한 내용은 http://www.cisco.com/web/services/에서 Cisco Technical Support Services 또는 Cisco Advanced Services 를 참조하시기 바랍니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Cisco Capital

목표 달성을 지원하는 파이낸싱

Cisco Capital 이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI 를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한 예측 가능한 비용 결제가 단 한 번뿐입니다. Cisco Capital 은 100 여 개 국가에서 이용할 수 있습니다. 자세히 보기.

추가 정보

Cisco ISA 3000 Series 에 대한 자세한 내용은 http://www.cisco.com/go/isa3000 을 참조하시거나 현지 어카운트 담당자에게 문의하시기 바랍니다.

이 제품에는 Eric Young(eay@cryptsoft.com)이 작성한 암호화 소프트웨어가 포함되어 있습니다. 이 제품에는 US Naval Research Laboratory 의 Information Technology Division 에서 개발한 소프트웨어가 포함되어 있습니다. 이 제품에는 DAV Explorer 프로젝트(http://www.ics.uci.edu/~webdav/)에 사용하기 위해 University of California, Irvine 에서 개발한 소프트웨어가 포함되어 있습니다. 이 제품에는 Boris Popov 가 개발한 소프트웨어가 포함되어 있습니다. 이 제품에는 OpenSSL 툴킷에 사용하기 위해 OpenSSL 프로젝트를 통해 개발된 소프트웨어가 포함되어 있습니다. (http://www.openssl.org/). 이 제품에는 Tim Hudson(tjh@cryptsoft.com)이 작성한 소프트웨어가 포함되어 있습니다.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C78-735839-00 10/15

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.