데이터 시트

Cisco Catalyst 6500 Series IDSM-2 (Intrusion Detection System Services Module)

시스코 통합 네트워크 보안 솔루션을 사용하여 조직에서는 생산성을 향상시키고 운영 비용을 절감할 수 있습니다.

그림 1. Cisco IDSM-2

Cisco IDSM-2는 Cisco IPS(Intrusion Prevention System)의 일부분으로, 다른 구성요소와 함께 작동하여 데이터 인프라를 효율적으로 보호합니다. 보안의 위협이 점점 더 복잡해짐에 따라 높은 수준의 보호를 유지하기 위해서는 효율적인 네트워크 침입 보안 솔루션을 구현하는 것이 필수적입니다. 적절한 보호는 비즈니스의 연속성을 보장하고 침입으로 인한 막대한 영향을 최소화합니다.

Cisco IDS/IPS(Intrusion Detection System/Intrusion Prevention System)에 대한 자세한 내용은 http://www.cisco.com/go/ids를 방문하십시오. 시스코 통합 네트워크 보안 솔루션을 통해 조직에서는 위협으로부터 비즈니스 자산을 보호하고 침입 차단 시스템을 보다 효율적으로 운영할 수 있습니다. 이 솔루션 중에는 널리 배치된 Cisco Catalyst® 섀시에 사용되는 Cisco IDS/IPS 모듈의 차세대 모듈인 IDSM-2가 있습니다. 전 세계 수십 만 개가 설치되어 있는 Catalyst 섀시는 방화벽, 가상 사설망(VPN) 및 침입 탐지/방지 시스템(IDS/IPS) 서비스와 같은 추가적인 서비스를 위한 지능형 플랫폼입니다. 이러한 접근 방식의 필요성을 인식한 시스코는 악의적인 공격으로부터 고객 데이터 인프라를 안전하게 보호하기 위하여 시스코의 차세대 모듈 IDSM-2를 출시했습니다.

기능 및 이점

Cisco IDSM-2는 다음과 같은 기능과 이점을 제공합니다.

- 시스코는 VLAN 기반의 접근 제어 목록(VACL) 캡처를 통해 데이터 스트림을 분석 가능하게 하는 IDS/IPS 솔루션을 유일하게 공급하는 업체입니다.
- 인라인(IPS) 모드와 수동 작동(IDS) 모드를 둘 다 지원합니다.
- 수동 모드에서 IDSM-2는 VACL 캡처 및 SPAN(Switch Port Analyzer)/RSPAN(Remote SPAN)을 통해 다양한 방식으로 패킷을 검사합니다.
- 수동 모드에서는 IDSM-2가 스위치 전송 경로에 있지 않으므로 네트워크 성능이 저하되거나 다운타임이 발생하지 않습니다.
- 인라인으로 사용할 경우 IDSM-2의 이상 동작으로 인한 네트워크 운영에 영향을 미치지 않도록 소프트웨어 방식의 바이패스 기능을 지원합니다.
- PET(Prevention Enablement Technologies)와 같은 고급 오류 탐지 기능을 사용하여 패킷 작업의 신뢰도를 극대화합니다. PET는 또한 사용자 조정이 가능한 Risk Rating 및 Meta Event Generator를 사용하여 내부 네트워크에 전달되는 데이터의 신뢰도를 극대화합니다.
- Cisco Catalyst 6500 또는 Catalyst 7600 섀시에 1 랙 유닛(RU) 크기로 장착되어 슬롯 한 개만을 차지하게 되므로, 최대 8개의 IDSM-2를 동시에 설치하여 트래픽 검사와 보호를 제공할 수 있습니다.

- IDSM-2 최대 8개의 모듈을 통해 4Gbps의 IDS/IPS 검사를 통해 고속 패킷 검사기능을 제공하고 더욱 다양한 종류의 네트워크와 트래픽을 보호 합니다.
- 고객이 SPAN/RSPAN 및 VACL 캡처를 비롯한 여러 캡처 기술을 사용하여 다양한 네트워크 세그먼트와 트래픽을 모니터링하고 적절한 조치를 취하여 위협을 완화할 수 있습니다.
- Cisco IDS/IPS 네트워크 어플라이언스와 동일한 IPS 코드를 사용하므로, 사용자가 단일 관리 기술을 표준화하여 더 쉽고 빠르게 설치, 교육, 운영 및 지원을 수행할 수 있으며 Cisco IDS/IPS의 광범위한 공격 인식 및 서명 범위를 활용할 수 있습니다.
- Trend Micro를 통한 시그니쳐 통합 – 시스코와 Trend Micro의 협력을 통해 시스코 고유의 서명 개발을 촉진하고 가장 완벽한 시그니쳐 업데이트를 제공함으로써 공격을 적시에 탐지하고 방지합니다.
- 텔넷, 보안 CLI, IDM 로컬 구성 브라우저, SecMon 모니터링 애플리케이션, CTR(Cisco Threat Response) 및 SNMP를 통해 유연한 관리 옵션이 제공될 뿐 아니라, VMS와 타사 관리 애플리케이션을 통해서도 제공됩니다.
- Catalyst 65xx 및 76xx 섀시상에서 다양한 수퍼바이저를 통해 Catalyst Hybrid Supervisor OS와 Native IOS Supervisor를 지원하므로 광범위한 설치 기반 네트워크 상에서 분배가 가능합니다.
- MPLS 디코드를 비롯한 대부분의 TCP/IP 및 ARP 프로토콜을 지원합니다.

기술 사양

Cisco IDSM-2 부품 번호

- Catalyst 시스템의 일부로 구입하는 경우 WS-SVC-IDS2-BUN-K9
- "예비용"으로 별도 구입하는 경우 WS-SVC-IDS2BUNK9=

Cisco IDSM-2 서비스 부품 번호

- CON-xxxx-WS-IDSM2-K9

부품 번호에서 "xxxx"의 서비스 키는 다음과 같습니다.

• SNT = 8x5x 다음 영업일	• SNTE = 8x5x4 시간 서비스
• SNTP = 24x7x4 시간 서비스	• OS = 8x5x 다음 영업일
• OSE = 8x5x4 시간 서비스 온사이트	• SP = 24x7x4 시간 서비스 온사이트

폼 팩터

1 랙 유닛 모듈이 Cisco Catalyst 6500/7600 섀시에서 한 개의 슬롯을 사용합니다.

LED 및 스위치

단일 표시기(LED)

- OFF-전원 없음
- 노랑-부팅 중/대기
- 녹색-애플리케이션 실행 중
- 적색-모듈 장애 탐지

섀시에서 모듈을 제거하기 전에 스위치를 끄십시오.

핫스왑 요구사항
- 제거하기 전에 모듈을 꺼야 합니다.
- 모듈을 삽입/제거하더라도 Cisco Catalyst 스위치에는 영향을 미치지 않습니다.

프로세서
메인보드상의 이중 Pentium P3 1.13 GHz(가속기상에 232 MHz IXP 32비트 StrongARM 정책 프로세서가 있음)

메모리 및 하드 드라이브
- 20 GB (모두 사용되지 않음)
- 2 GB RAM
- IDSv5.0의 경우 32 MB 이벤트 스토리지
- 64 MB 플래시 메모리

운영 체제
GNU Linux 커널 버전 2.4.26

섀시 당 모듈의 최대 수
- 섀시 당 8개
- 슬롯 제한 없음

트래픽 캡처 방식(수동 모드)
- VACL 캡처
- SPAN
- RSPAN(2)
- ERSPAN(4) (Supervisor 720 전용)

최소 코드 수정
- 릴리스 4.x, S47
- 현재 릴리스: 5.x S14x

Catalyst 수퍼바이저 소프트웨어 요구사항
- Catalyst OS 7.6(1) (최소)
- 기본 Cisco IOS Software 릴리스 12.1(19)E (최소)

표 1. IDSM-2의 경우 Catalyst 수퍼바이저 하드웨어 옵션

수퍼바이저	인라인 작동 시 기본 IOS 브랜치	인라인 작동 시 Catalyst OS 브랜치
Sup 720(모든 버전)	TBD	8.4(1)
Sup 1a(PFC 없음, PFC 포함, MSFC20 포함)	TBD	8.4(1)
Sup 2(PFC 없음, PFC 포함 및 MSFC2 포함)	TBD	8.4(1)
수퍼바이저	**수동 모드에서 기본 IOS 브랜치**	**수동 모드에서 Catalyst OS 브랜치**
Sup 720(MSFC3 있음) (모든 버전)	12.2(18)SXD1	8.2(1), 8.3(1), 8.4(1)
Sup 720(MSFC3 없음)	해당 없음	해당 없음
Sup 32 "W"	해당 없음	8.4(1)
Sup 2(MSFC2 있음)	12.1(13)E, 12.1(19)E, 12.2(14)SX, 12.2(18)SXD1	7.5(1), 7.6(1), 8.1(1), 8.2(1), 8.3(1), 8.4(1)
Sup 2(MSFC2 없음)	해당 없음	7.5(1), 7.6(1), 8.1(1), 8.2(1), 8.3(1), 8.4(1)
Sup 2(PFC2 없음)	해당 없음	해당 없음
Sup 1a(MSFC2 있음)	12.1(19)E1, 12.1(20)	7.5(1), 7.6(1), 8.1(1), 8.2(1),8.3(1), 8.4(1); 유효 MSFC2 브랜치 12.1(13)E, 12.1(19)E, 12.1(20)
Sup 1a(MSFC2 없음)	해당 없음	7.5(1), 7.6(1), 8.1(1), 8.2(1), 8.3(1), 8.4(1)
Sup 1a(PFC 없음)	해당 없음	해당 없음
Sup 1a(MSFC1 있음)	지원 않음	7.5(1), 7.6(1), 8.1(1), 8.2(1),8.3(1), 8.4(1); 유효 MSFC1 브랜치 12.1(13)E, 12.1(19)E, 12.1(20)
Sup 1a(MSFC1 없음)	해당 없음	7.5(1), 7.6(1), 8.1(1), 8.2(1), 8.3(1), 8.4(1)

상호운용성

7.6(1), 8.1(1) Catalyst OS 또는 12.1(19)E를 사용하는 다른 모든 서비스 모듈과 호환됩니다(VPNSM 제외). VPNSM과 함께 작동하려면, Cat 6500이 있는 12.2(17d)SXB이나 Cat 7600이 있는 12.2(18)SXD1을 사용하십시오. VPNSM에 대해서는 다른 제한이 적용될 수 있습니다.

표 2. WAN 상호운용성 지원

WAN 호환성 지원	Catalyst 6500	Catalyst 7600
IDSM-2	지원	지원
IDSM-2(FlexWAN2 포함)*	지원하지 않음	지원

* FlexWAN1은 Catalyst 6500 또는 Catalyst 7600에서 지원되지 않습니다.

수동 모드 및 인라인 모드의 차이점

표 3. 수동 모드 및 인라인 모드의 차이점

	IDSM-2 수동 모드(4.x)	IDSM-2 수동 모드(5.x)	IDSM-2 인라인 모드(5.x)
Cat 6500 지원	지원	지원	지원
Cat 7600 지원	지원	지원(IOS 12.2(17)SXD1 전용)	지원하지 않음
Cat OS 지원	지원 (다양)	지원 (다양)	지원 (8.4(1) 전용)
Cat IOS 지원	지원	지원	지원하지 않음
모니터링되는 VLAN	무제한	무제한	단일 쌍
성능(FCS의 경우)	600 Mbps 양방향	500 Mbps	500 Mbps
지연 시간	없음, 해당 없음	없음, 해당 없음	~1 Ms/패킷 이하
동작	TCP 재설정, 회피, IP 로그, 트리거 패킷 캡처	TCP 재설정, 회피, IP 로그, 트리거 패킷 캡처	패킷 폐기, TCP 재설정, 회피, IP 로그, 트리거 패킷 캡처
장치 장애의 영향	장치 장애가 트래픽에 영향을 미치지 않음	장치 장애가 트래픽에 영향을 미치지 않음	장치 장애가 트래픽에 영향을 미칠 수 있음, 소프트웨어 바이패스, SNMP가 영향을 감소시킴
모든 공격을 중단할 수 있음	지원하지 않음 (단일 패킷 공격만이 성공할 수 있음)	지원하지 않음(단일 패킷 공격만이 성공할 수 있음)	지원(탐지된 모든 공격 트래픽을 분석하고 폐기할 수 있음)
SecMon/IDSMC 지원	VMS 2.3	VMS 2.3	VMS 2.3

참고: 고객이 적절한 버전과 수퍼바이저를 사용하여 수동 모드에서 IPSv5.0과 함께 IDSM-2를 실행할 수 있지만, 인라인 작동을 위해 이번에는 Cat OS 8.4(1)만 지원됩니다.

성능 기준(수동 모드)

- 초당 5000개의 새로운 TCP 연결과 50,000개의 동시 연결에서 450바이트 패킷의 경우 500 Mbps
- 최대 500,000개의 동시 연결 지원
- 100% 경보 속도
- Cisco Catalyst 새시에 VLAN이나 장치를 추가하더라도 Catalyst 성능에는 영향을 미치지 않음
- 패브릭 활성화됨
- 오버 샘플링 경보가 "993 Bandwidth Exceeded" 경보를 발생
- 무제한 VLAN 지원

성능 기준(인라인 모드)

- 초당 5000개의 새로운 TCP 연결과 50,000개의 동시 연결에서 450바이트 패킷을 사용하여 500 Mbps
- 최대 500,000개의 동시 연결 지원
- 100% 경보 속도
- 1개의 VLAN 쌍

VLANS의 최대 수(802.1q 태깅)

- 수동 모드에서는 무제한
- IDSM-2 인라인의 경우 1개의 VLAN 쌍

장애 복구 보호

- 수동 모드: IDSM-2는 장애 발생 시 Cisco Catalyst 섀시에 영향을 미치지 않는 수동 방식입니다.
- 인라인 모드: 소프트웨어 바이패스 기능을 사용하여 IDSM-2에 장애가 발생하는 것을 막을 수 있습니다. SNMP를 통해 유닛 상태를 모니터링할 수 있습니다.

관리

- CLI-텔넷 또는 SSHv3.0을 통해 CLI를 로컬이나 원격으로 사용하여 IDSM-2를 구성할 수 있습니다.
- IDM-로컬 사용을 위한 구성 관리자입니다. IDM은 IDSM-2에서 다운로드되는 애플릿이며 PC에서 실행됩니다. 이 애플리케이션은 TLS v1.0 또는 SSL v1.5/2.0을 통해 보호됩니다.
- IEV-IEV는 중단되었으며 더 이상 IDSM-2에서 지원되지 않습니다.
- CTR-CTR은 중단되었으며 더 이상 IDSM-2에 사용할 수 없습니다.
- SNMP-IDSv5.0은 IDSM-2용 Cisco CIDS MIB를 비롯한 SNMPv2c를 지원하며 Gets와 Traps은 제공하지만 Sets는 제공하지 않습니다. 즉, SNMP를 통해 IDSM-2를 구성할 수 없습니다. Trap에서 경보를 전송합니다. IDSM-2상에 SNMP 데몬을 켜고 커뮤니티를 구성한 시그니쳐를 구성하여 경보와 함께 SNMP Traps을 생성합니다. 센서가 생성하는 SNMP Traps을 수신하도록 SNMP 관리 스테이션을 구성해야 합니다. SNMP 관리 스테이션은 경보를 수신할 뿐만 아니라 다른 여러 통계와 상태(CPU 사용량, 메모리 사용량 등)를 센서에 질의할 수 있습니다.
- VMS 2.3은 Cisco VPN, 방화벽 및 IDS 장치와 CSA HIDS를 관리하는 애플리케이션 번들입니다. 이 번들은 VMS Basic, VMS-R(제한) 및 VMS-UR(제한 없음)을 비롯한 세 가지 형태로 제공됩니다. VMS Basic은 최대 5대의 장치를 관리하며 무료로 포함됩니다. VMS-R은 최대 20대의 장치를 관리하며, VMS-UR은 장치를 무제한으로 관리합니다. VMS 2.3에는 Cisco IOS IPS 가능 라우터를 비롯한 IDSv3.x 및 IDSv4.x 장치를 모니터링하고 관리할 수 있는 SecMon 2.0 및 IDSMC 2.0이 포함됩니다. IDSv5.0 장치 모니터링 및 관리를 위해 SecMon 2.1 및 IDSMC 2.1이 향후 출시될 예정입니다.
- IDSMC 2.0-VMS의 한 구성요소로, IDSMC의 새로운 버전인 IDSMC 2.0은 사람의 개입이 없이도 서명을 센서에 자동으로 업데이트할 수 있습니다. IDSMC는 예정된 주기마다 Cisco CCO 사이트를 검사하여 시그니쳐 업데이트가 있는 경우 이 업데이트를 IDSMC 플랫폼에 다운로드한 후 해당 어플라이언스로 자동으로 전달합니다.
- SecMon 2.0-IDSv5.0은 IDSv4.0 형식으로 메시지를 전달하기 때문에 SecMon 2.0에서 이 메시지를 식별할 수 있습니다.
- Third Party Managers를 사용하여 IDSM-2를 모니터링할 수 있습니다. 단, 이번에는 구성을 위해서는 사용할 수 없습니다. 이 타사 관리자는 SDEE(Secure Data Event Exchange) 프로토콜을 사용하여 IDSM-2에서 이벤트와 경보를 모니터링하고 검사합니다. IDSM-2 모니터링을 지원하는 공급업체로는 Protego, NetForensics, Tivoli Risk Manager, Arcsight, Intellitactics, Arbor, Solsoft 등이 있습니다.

물리적 치수

- 높이: 3.0 cm (1.2 인치)
- 가로: 35.6 cm (14.4 인치)
- 세로: 40.6 cm (16 인치)
- 중량: 2.27 kg (5 파운드)

전원

- 앰프: 2.5
- 와트: 105
- 열 손실: 450 BTU

동작 환경

- 동작 온도: 0 ~ 40°C (32 ~ 104.5ºF)
- 비동작 온도: –40 ~ 70°C (–40 ~ 158ºF)
- 동작 상대 습도: 10 ~ 90%(비응축)
- 비동작 상대 습도: 5 ~ 95%(비응축)
- 동작 및 비동작 고도: 해발 3050m (10,000 피트)

정부 승인

전자파 방출

FCC Part 15 (CFR 47) Class A, ICES–003 Class A, EN55022 Class A, CISPR22 Class A, AS/NZS 3548 Class A, VCCI Class A with UTP cables, EN55022 Class B, CISPR22 Class B, AS/NZS 3548 Class B, VCCI Class B with FTP cables

안전성

UL 1950, CSA 22.2 No. 950, EN 60950, IEC 60950, TS 001, AS/NZS 3260을 준수하는 CE marking

인증

- NEBS Level 3 대기 중(Catalyst 7600의 경우)
- Common Criteria Level 2 인증 획득

수출 규제

Cisco IDSM–2는 "강력한 암호화" 제품으로 분류되며 수출이 규제됩니다. 자세한 내용은 http://www.cisco.com/wwl/export/crypto/tool/을 참조하십시오.

추가 정보

설명서는 http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm을 참조하십시오.
Cisco Catalyst 6500 스위치에 대한 자세한 내용은 http://www.cisco.com/go/6000을 참조하십시오.
Cisco Secure IDS(Intrusion Detection System)에 대한 자세한 내용은 http://www.cisco.com/go/ids/를 참조하십시오.

www.cisco.com/kr

2005-06-07

■ Gold 파트너	• (주)데이타크레프트코리아	02-6256-7000	• (주)인네트	02-3451-5300	• (주)인성정보	02-3400-7000
	• 한국아이비엠(주)	02-3781-7800	• (주)콤텍시스템	02-3289-0114	• 쌍용정보통신(주)	02-2262-8114
	• 에스넷시스템(주)	02-3469-2400	• (주)링네트	02-6675-1216	• 한국후지쯔(주)	02-3787-6000
	• 한국휴렛팩커드(주)	02-2199-0114	• (주)LG씨엔에스	02-6363-5000		
■ Silver 파트너	• 한국NCR	02-3279-4423	• (주)시스폴	02-6009-6009	• 포스데이타주식회사	031-779-2114
	• SK씨앤씨(주)	02-2196-7114/8114				
■ Local 디스트리뷰터	• (주)소프트뱅크커머스코리아	02-2187-0176	• (주)아이넷뱅크	02-3400-7490	• (주)SK 네트웍스	02-3788-3673
■ IPT 전문파트너	• 에스넷시스템(주)	02-3469-2900	• (주)인성정보	02-3400-7000	• 크리스넷주식회사	1566-3827
	• LG기공	02-2630-5280	• (주)컴웨어	02-2629-2700		
■ IP/VC(Video Conferencing)	• (주)컴웨어	02-2629-2700				
■ IPCC전문파트너	• 한국아이비엠(주)	02-3781-7114	• 한국휴렛팩커드(주)	02-2199-4272	• LG기공	02-2630-5280
	• (주)인성정보	02-3400-7000	• (주)삼성네트웍스	02-3415-6754		
■ WLAN 전문 파트너	• (주)에어키	02-584-3717	• (주)해창시스템	031-389-0780		
■ Security 전문 파트너	• 나래시스템	02-2190-5533	• (주)데이터크레프트코리아	02-6256-7000	• (주)링네트	080-822-6675
	• 에스넷시스템(주)	02-3469-2900	• (주)인성정보	02-3400-7000	• 인포섹(주)	02-2104-5114
	• UNNET Systems	02-565-7034	• 코코넛	02-6007-0133	• (주)토탈인터넷시큐리티시스템	051-743-5940
■ Optical 전문 파트너	• (주)LG씨엔에스	02-6363-5000	• 에스넷시스템(주)	02-3469-2900	• 미리넷주식회사	02-2142-2800
■ CN 전문 파트너	• (주)메버릭시스템	02-845-4280				
■ Storage 전문 파트너	• (주)패킷시스템즈코리아	02-558-7170	• 매크로임팩트	02-3446-3508		