침입 탐지 시스템 호환성 매트릭스

목차

소개

이 문서에서는 Cisco IPS(Intrusion Prevention System) 어플라이언스(4210, 4215, 4220, 4230, 4235, 4240, 4250, 4250, 4255), Adaptive Security Appliance SSM(Security Services Module), Catalyst Module 및 Catalyst Router0600 어플라이언스에 대한 하드웨어/소프트웨어 호환성 매트릭스를 제공합니다. 0 Intrusion Detection System Module(IDSM-1, IDSM-2). 이 문서에서는 관리 옵션에 대한 개요도 제공합니다.각 애플리케이션에 대한 간략한 개요와 버전 호환성 매트릭스가 제공됩니다.각 호환성 매트릭스에 나열된 버전만 지원됩니다.

Cisco Intrusion Prevention System은 이전에 Cisco IDS(Intrusion Detection System) 또는 NetRanger로 알려져 있었습니다.Cisco Intrusion Prevention System Appliance는 Sensor라고도 합니다.자세한 내용은 관련 제품 설명서 및 릴리스 정보를 참조하십시오.

참고: 이 문서의 테이블에 있는 제품 상태 열에 유의하십시오.이 열은 관련 EoL(End-of-Life)/EoS(End-of-Sale) 알림을 나타냅니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IPS(Intrusion Prevention System) 어플라이언스(4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255)
- SSM(Adaptive Security Appliance Security Services Module)
- 라우터 모듈
- Catalyst 6000 Intrusion Detection System Module(IDSM-1, IDSM-2)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

IPS 하드웨어/소프트웨어 호환성

표 1 - 어플라이언스

어플라이언스	부품 번호	하드웨어	선택적 인터페이스	사용 가능한 추가 하드웨어	호환 소프트웨어 버전	제품 상태
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	소프트웨어 업그레이드 및 이미지 복구를 위해 CDROM이 포함된 IDE 하드 드라이브를 사용할 수 있습니다.		IDS-4210-MEM-U= SmartNet 고객이 버전 4.1 이상으로 업그레이드하도록 지원하는 추가 256MB 메모리.고객은 Product Upgrade Tool을 통해 메모리를 주문할 수 있습	3.1에서 현재 *	판매종료:2003년 12월 8일 지원종료일:2008년 12월 8일

				니다(등록된 고객만 해당).		
IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9	IDE 하드 드라이브 및 컴팩트 플래시 .소프트웨어 업그레이드 및 이미지 복구를 위해 사용할 수 있는 CDROM 드라이브가 없습니다.	IDS-4FE-INT=		4.1 - 현재 *	현재
IDS-4220	IDS-4220-E	소프트웨어 업그레이드 및 이미지 복구를 위해 CDROM이 포함된 IDE 하드 드라이브를 사용할 수 있습니다.		IDS-4220-MEM-U= SmartNet 고객이 버전 4.1 이상으로 업그레이드하도록 지원하는 추가 256MB 메모리 .고객은 Product Upgrade Tool을 통해 메모리를 주문할 수 있습니다(등록된 고객만 해당).	3.1 ~ 4.1	**판매종료**:2002년 7월 31일 **지원종료일**:2007년 7월 31일
IDS-	IDS-	소프트			3.1	**판**

4230	4230-FE	웨어 업그레이드 및 이미지 복구를 위해 CDROM이 포함된 IDE 하드 드라이브를 사용할 수 있습니다.			~ 4.1	**매종료**:2002년 7월 31일 **지원종료일**:2007년 7월 31일
IDS-4235	IDS-4235-K9	소프트웨어 업그레이드 및 이미지 복구를 위해 CDROM이 포함된 SCSI 하드 드라이브를 사용할 수 있습니다.	IDS-4FE-INT=	IDS-PWR= 예비 전원 공급 장치	3.1에서 현재 *	**판매종료**:2005년 5월 31일 **지원종료일**:2010년 5월 31일
IPS-4240	IPS-4240-K9 IPS-4240-DC-K9(DC 전원, NEBS 호환 전용)	컴팩트 플래시.소프트웨어 업그레이드 및 이미지 복구 용도로 사용할 수 있는			4.1.4 - 현재 *	현재

		CDROM 드라이브가 없습니다.				
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	소프트웨어 업그레이드 및 이미지 복구를 위해 CDROM이 포함된 SCSI 하드 드라이브를 사용할 수 있습니다.	IDS-4FE-INT= IDS-4250-SX-INT= IDS-XL-INT=	IDS-PWR= 예비 전원 공급 장치 IDS-SCSI= 예비 SCSI 하드 드라이브	3.1 에서 현재 *	**TX 버전 전용 판매 종료** :2005 년 5월 31 일 **TX 지원 종료 일** :2010 년 5월 31 일 다른 두 IDS 4250 플랫폼은 이 EoL 발표에 영향을 받지

						않습니다.
IPS-4255	IPS-4255-K9	컴팩트 플래시.소프트웨어 업그레이드 및 이미지 복구 용도로 사용할 수 있는 CDROM 드라이브가 없습니다.			4.1.4 - 현재 *	현재

표 2 - 모듈

모듈	부품 번호	하드웨어	선택적 인터페이스	사용 가능한 추가 하드웨어	호환 소프트웨어 버전	제품 상태
SSM	ASA-SSM-AIP-10-K9(ASA AIP 보안 서비스 모듈-10) ASA-SSM-AIP-20-K9(ASA AIP 보안 서비스 모듈-20)	컴팩트 플래시.소프트웨어 업그레이드 및 이미지 복구 용도로 사용할 수 있는 CDROM 드라이브가 없습니다.			5.0에서 현재 *	현재
라우터 모듈	NM-CIDS-K9 NM-CIDS-K9= (RMA 부품 번호 전용)	컴팩트 플래시.소프트웨어 업그레이드 및 이미지 복구 용도로 사용할 수 있는 CDROM 드라이브가 없습니다.			Cisco IOS® Software 릴리스 12.2(15)ZJ 이상 Cisco IOS Softw	현재

					are 릴리스 12.3(4)T 이상 IDS 4.1 - 최신 *	
IDSM-1	WS-X6381-IDS WS-X6381-IDS= (RMA 부품 번호 전용)	IDE 하드 드라이브 .소프트웨어 업그레이드 또는 이미지 복구 용도로 사용할 수 있는 CD ROM 드라이브가 없습니다.			2.5 ~ 3.0	**판매종료:2003년 4월 20일 지원종료일:2008년 4월 20일**
IDSM-2	WS-SVC-IDS2-BUN-K9 WS-SVC-IDS2BUNK9= (RMA 부품 번호 전용)	IDE 하드 드라이브 및 컴팩트 플래시.소프트웨어 업그레이드 및 이미지 복구 용도로 사용할 수 있는 CDROM 드라이브가 없습니다.			4.0에서 현재 *	현재

참고: 이 문서를 게시할 때 사용할 수 있는 최신 버전의 소프트웨어는 5.1입니다. 5.1 이상의 소프트웨어 버전이 필요한 경우 해당 버전의 코드 설명서를 참조하여 호환성을 확인하십시오.

관리 및 구성 옵션

명령줄 인터페이스를 통해 또는 이 섹션에 나열된 컨피그레이션 또는 관리 툴 중 하나를 통해 IPS

센서를 관리하고 구성할 수 있습니다.

CiscoWorks Management Center for IPS Sensor(IPS MC)

CiscoWorks Management Center for IPS Sensor는 Cisco Systems Network Sensor, 스위치 IPS Sensor, 라우터용 IPS 네트워크 모듈, 라우터용 인라인 침입 방지 소프트웨어 구성을 위한 확장 가능한 아키텍처를 갖춘 툴입니다.관리자는 CiscoWorks Management Center for IPS Sensor를 사용하여 그룹 프로필을 사용하여 여러 센서를 동시에 구성하여 시간을 절약할 수 있습니다.또한 강력한 시그니처 관리 기능을 제공하여 가능한 네트워크 침입을 탐지하는 정확성과 특성을 향상시킵니다.

호환성 정보는 Management Center for IPS Sensors 설명서를 참조하십시오.

CiscoWorks Monitoring Center for Security(SecMon)

CiscoWorks Monitoring Center for Security는 보안 이벤트를 캡처, 저장, 보기, 상관 관계 분석 및 보고하는 툴입니다.

- Cisco 네트워크 IPS
- Cisco 네트워크 IDS
- Cisco 스위치 IDS
- 인라인 IPS 기능이 있는 Cisco IOS 라우터
- 라우터용 Cisco IDS 모듈
- Cisco PIX 방화벽
- Cisco Catalyst 6500 Series FWSM(Firewall Services Module)
- Cisco Security Agent용 CiscoWorks Management Center
- 보안 서버용 CiscoWorks Monitoring Center

호환성 정보는 Monitoring Center for Security 설명서에 대한 지원되는 디바이스 및 소프트웨어 버전을 참조하십시오.

Cisco MARS(Security Monitoring, Analysis and Response System)

Cisco MARS(Security Monitoring Analysis and Response System)는 위협 관리, 모니터링 및 완화를 위한 고성능, 확장 가능한 어플라이언스 제품군으로, 고객이 네트워크 및 보안 장치를 보다 효과적으로 사용할 수 있도록 지원합니다.Cisco Security MARS는 기존의 보안 이벤트 모니터링과 네트워크 인텔리전스, 컨텍스트 상관관계, 벡터 분석, 이상 징후 탐지, 핫스팟 식별 및 자동화된 완화 기능을 결합합니다.Cisco Security MARS는 이러한 기능을 결합하여 네트워크 규정 준수를 유지하면서 네트워크 공격을 정확하게 식별하고 제거할 수 있도록 지원합니다.

MARS 버전	지원되는 어플라이언스/센서 소프트웨어
3.3.x	3.x 및 4.x
3.4.x	3.x, 4.x, 5.x

자세한 내용은 제품 릴리스 정보를 참조하십시오.

CTR(Cisco Threat Response)

Cisco CTR(Threat Response)은 Cisco IPS Sensor와 연동하여 효율적인 침입 방지 솔루션을 제공합니다.Cisco Threat Response는 오탐(false alarms)을 사실상 제거하고, 실제 공격을 에스컬레이

션하며, 비용이 많이 드는 침입을 해결하는 데 도움이 됩니다.

Cisco Threat Response는 Cisco IPS 버전 3.x 이상과 호환됩니다.자세한 내용은 제품 릴리스 정보를 참조하십시오.또한 Cisco Threat Response에 대한 End-of-Life 공지를 숙지하십시오.

IDS 이벤트 뷰어(IEV)

IDS Event Viewer(IEV)는 최대 5개의 센서에 대한 경보를 보고 관리할 수 있는 Java 기반 애플리케이션입니다.IDS 이벤트 뷰어를 사용하면 실시간으로 또는 가져온 로그 파일에 연결하여 경보를 볼 수 있습니다.경보를 관리하고 추가 분석을 위해 이벤트 데이터를 가져오고 내보낼 수 있도록 필터 및 보기를 구성할 수 있습니다.IDS 이벤트 뷰어는 시그니처 설명을 위해 NSDB(Network Security Database)에 대한 액세스도 제공합니다.

IEV는 IDS 버전 3.1에서 버전 4.x로 지원됩니다.버전 5.x에서는 더 이상 지원되지 않지만 버전 5.x 센서를 모니터링하는 데 사용할 수 있습니다.그러나 새로운 5.0 기능은 IAV에서 보고하지 않습니다.자세한 내용은 제품 구성 예 및 기술 노트를 참조하십시오.

IDM(IDS Device Manager)

IDM(IDS Device Manager)은 센서를 구성하고 관리할 수 있는 웹 기반 애플리케이션입니다.IDS 장치 관리자용 웹 서버는 센서에 상주합니다.Netscape 또는 Internet Explorer 웹 브라우저를 통해 액세스할 수 있습니다.

IDM은 IDS 버전 3.1에서 지원됩니다. 자세한 내용은 제품 구성 예 및 기술 노트를 참조하십시오.

Cisco CSPM(Secure Policy Manager)

Cisco CSPM(Secure Policy Manager)은 Cisco IDS Sensor, PIX 방화벽 및 IPsec VPN 라우터에 대한 정책 기반 보안 관리를 제공합니다.

참고: CSPM이 EoL에 도달했습니다.Cisco Secure Policy Manager 2.x & 3.x에 대한 EoS/EoL 공지를 참조하십시오.

모델	CSPM 2.2	CSPM 2.3i	CSPM 2.3.1i	CSPM 2.3.2i	CSPM 2.3.3i
IDS 4210 IDS 4220 IDS 4230	2.2.0.x 2.2.1.x 2.5(0)	2.2.0.x 2.2.1.x 2.5.(0)S0 2.5(1)S0 2.5(1)S2	2.2.0.x 2.2.1.x 2.5.(0)S0 2.5(1)S0 2.5(1)S2 3.0(1)S3 3.0(1)S4	2.2.0.x 2.2.1.x 2.5.(0)S0 2.5(1)S0 2.5(1)S2 3.0(1)S3 3.0(1)S4	2.2.0.x 2.2.1.5 2.5(1)S3 2.2.1.0 2.2.1.6 3.0(1)S4 2.2.1.1 2.5(0)S0 3.0(1)S5 2.2.1.2 2.5(1)S0 3.0(1)S6 2.2.1.3 2.5(1)S1 3.0(1)S7 2.2.1.4 2.5(1)S2 3.0(1)S8
Catalyst 6000	2.5 IDS	2.5 IDSM	2.5 IDSM	2.5 IDSM	2.5(0)S0 IDSM 2.5(1)S2 IDSM

Intrustion Detection System Module (IDSM-1)	M		3.0 IDSM	3.0 IDSM	2.5(1)S0 IDSM 3.0(1)S4 IDSM 2.5(1)S1 IDSM 3.0(1)S6 IDSM

UNIX 디렉터

UNIX Director는 분산된 네트워크 전반의 보안 관리를 위한 중앙 집중식 그래픽 인터페이스를 제공합니다.또한 타사 툴을 통한 데이터 관리, NSDB 액세스, 센서 및 IDSM의 원격 모니터링 및 관리, 보안 이벤트가 발생할 경우 보안 담당자에게 페이지 또는 e-메일을 보낼 수 있습니다.Director 인터페이스는 HP OpenView 위에서 실행됩니다.

참고: Cisco IDS Appliance Sensor용 소프트웨어 릴리스 2.2.x가 EoL에 도달했습니다.Cisco IDS 2.2.x Sensor 소프트웨어의 단종 설명서를 참조하십시오.

디렉터 버전	지원되는 어플라이언스/센서 소프트웨어
2.1.1	2.1.1
2.2.0	2.2.0
2.2.1	2.2.1
2.2.2	2.2.2 및 2.5
2.2.3*	2.2.3, 3.0, 3.1

* 2.2.3은 IDS Director 소프트웨어의 최신 버전이며 센서 소프트웨어 3.1 이하를 지원합니다.

2.2.x Director는 2.2.x Sensor 버전과 역호환될 수 있지만, 디렉터 및 센서에 동일한 소프트웨어 버전이 없을 경우, Director에서 최신 Sensor 기능을 사용할 수 없습니다.이렇게 하면 수동 명령줄 구성이 실행됩니다.자세한 내용은 제품 문서를 참조하십시오.

관련 정보

- Cisco 침입 방지 시스템
- 보안 제품 필드 알림(CiscoSecure Intrusion Detection 포함)