

入侵检测系统兼容性矩阵

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[IPS硬件/软件兼容性](#)

[管理和配置选项](#)

[CiscoWorks Management Center for IPS Sensors \(IPS MC\)](#)

[监控安全\(SecMon\)的CiscoWorks中心](#)

[思科安全检测、分析及响应系统\(MARS\)](#)

[Cisco Threat Response \(CTR\)](#)

[IDS Event Viewer \(IEV\)](#)

[IDS服务管理器\(IDM\)](#)

[Cisco Secure Policy Manager](#)

[UNIX导向器](#)

[Related Information](#)

[Introduction](#)

本文为思科入侵防御系统(IPS)工具(4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255), 可适应的安全工具安全服务模块(SSM), 路由模块和Catalyst 6000入侵检测系统模块(IDSM-1, IDSM-2)提供一个硬件/软件兼容性矩阵。本文也提供管理选项概述。提供每个应用程序简要概述, 以及版本兼容性矩阵。在每张兼容表列出的版本是唯一的支持的版本。

思科入侵防御系统以前叫作Cisco入侵检测系统(IDS)或NetRanger。亦称思科入侵防御系统工具是传感器。请参见相关产品文档和版本注释欲知更多信息。

Note: 注意产品Status (状态)列在本文内的表里。此列表示相关End-of -生活(EoL) /End销售(EoS)通知。

[Prerequisites](#)

[Requirements](#)

There are no specific requirements for this document.

[Components Used](#)

本文档中的信息基于以下软件和硬件版本：

- 思科入侵防御系统(IPS)工具(4210 , 4215 , 4220 , 4230 , 4235 , 4240 , 4250 , 4255)
- 可适应的安全工具安全服务模块(SSM)
- 路由模块
- Catalyst 6000入侵检测系统模块(IDSM-1 , IDSM-2)

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

IPS硬件/软件兼容性

表1 —工具

工具	部分 #	硬件	可选的接口	可用的另外的硬件	兼容的软件版本	产品状态
ID S- 42 - 10 ID S- 42 - 10- K9 ID S- 42 - 10- NF R		IDE硬盘驱动器用CD-ROM可用为软件升级和镜像恢复目的。		SmartNet用户的IDS-4210-MEM-U=另外的256MB内存只升级到版本4.1和以上。用户能通过 产品升级工具(仅限注册用户) 订购内存。	3.1 对当前*	销售结尾 : 2003年12月8日 技术支持最后一天 : 2008年12月8日
ID S- 42 - 15- K9 ID S- 42 - 15- 4F		IDE硬盘驱动器和微型闪存。光盘驱动器为软件升级和镜像恢复目的不是可用的。	ID S- 4F E- IN T=		4.1 对当前*	当前

	E-K9					
IDS-4220E	IDE硬盘驱动器用CD-ROM可用为软件升级和镜像恢复目的。		SmartNet用户的IDS-4220-MEM-U=另外的256MB内存只升级到版本4.1和以上。用户能通过 产品升级工具(仅限注册用户) 订购内存。	3.1到4.1	销售结尾 : 2002年7月31日 技术支持最后一天 : 2007年7月31日	
IDS-4230FE	IDE硬盘驱动器用CD-ROM可用为软件升级和镜像恢复目的。			3.1到4.1	销售结尾 : 2002年7月31日 技术支持最后一天 : 2007年7月31日	
IDS-4235K9	SCSI硬盘驱动器用CD-ROM可用为软件升级和镜像恢复目的。	IDS-4FE-INT=	IDS-PWR=节省电源	3.1对当前*	销售结尾 : 2005年5月31日 技术支持最后一天 : 2010年5月31日	
IPS-4240K9 IPS-4240DC-K9(DC)	微型闪存。没有光盘驱动器可用为软件升级和镜像恢复目的。			4.1.4对当前*	当前	

	只供给动力，NEBS兼容)				
IDS-4250-SX-K9	SCSI硬盘驱动器用CD-ROM可用为软件升级和镜像恢复目的。	IDS-4FE-INT=IDS-4250-SX-INT=IDS-XL-INT=	IDS-PWR=节省电源IDS-SCSI=备件SCSI硬盘驱动器	3.1对当前*	TX销售仅版本结尾 : 2005年5月31日技术支持最后一天TX的 : 2010年5月31日另外两IDS 4250平台没有影响的是受此EoL公告的。
IPS-4255-K9	微型闪存。光盘驱动器可用为软件升级和镜像恢复不目的。			4.1.4对当前*	当前

表2—模块

模块	部分#	硬件	可选的接口	可用的另外的硬件	兼容的软件版本	产品状态
SS	ASA-SSM-	微型闪存。光盘驱动器可用为软件升级和			5.0对当前*	当前

M	AIP-10-K9 (ASA AIP安全性服务 Module-10) ASA-SSM-AIP-20-K9 (ASA AIP安全性服务 Module-20)	镜像恢复不目的。				
路由模块	NM-CIDS-K9 NM-CIDS-K9= (RMA 零件 #只)	微型闪存。光盘驱动器可用为软件升级和镜像恢复不目的。			Cisco IOS软件版本 12.2(15) ZJ或以上 Cisco IOS Software Release 12.3(4)T 或以上 IDS 4.1对当前*	当前
IDS M-1	WS-X6381-IDS WS-X6381-IDS= (RMA 零件 #只)	IDE硬盘驱动器。光驱可用为软件升级或镜像恢复不目的。			2.5到3.0	销售结尾 : 2003年4月20日技术支持最后一天 : 2008年4月20日
ID	WS-SVC-	IDE硬盘驱动器和微型闪存。没有光盘驱			4.0对当前*	当前

S M - 2	IDS2- BUN- K9 WS- SVC- IDS2B UNK9 = (RMA 零件 #只)	动器可用为软件升级 和镜像恢复目的。				
------------------	---	-----------------------	--	--	--	--

Note: 软件新版本可用在本文的出版物时是5.1。如果需要比5.1以后的软件版本，请检查文档该编码版本保证兼容性。

管理和配置选项

您能管理，并且通过line命令配置IPS传感器请通过这些部分列出的其中一配置或管理工具建立接口，或者。

CiscoWorks Management Center for IPS Sensors (IPS MC)

CiscoWorks Management Center for IPS Sensors是有可扩展的体系结构的一个工具的Cisco系统网络传感器、交换机IPS传感器、IPS网络模块的路由器和在路由器的轴向入侵防御软件的配置。使用组配置文件，CiscoWorks Management Center for IPS Sensors允许管理员通过并发配置多个传感器节省时间。另外，它提供增加准确性和特异性在可能的网络入侵的检测的一个强大的签名管理功能。

请参见[支持的设备和软件版本管理中心的IPS传感器](#)文档兼容性信息。

监控安全(SecMon)的CiscoWorks中心

CiscoWorks Monitoring Center for Security是捕获，存储，查看，关联和报告的工具关于安全事件从：

- Cisco网络IPS
- Cisco网络IDS
- Cisco交换机IDS
- 有轴向IPS功能的Cisco IOS路由器
- 路由器的Cisco IDS模块
- Cisco PIX防火墙
- Cisco Catalyst 6500 Series防火墙服务模块(FWSM)
- CiscoWorks Management Center for Cisco Security Agents
- CiscoWorks Monitoring Center for Security服务器

请参见[支持的设备和软件版本监控的中心安全](#)文档兼容性信息。

思科安全检测、分析及响应系统(MARS)

Cisco安全监控分析和回应系统(MARS)是帮助用户做更加有效的使用网络和安全设备高性能，可升

级的工具，监控和缓解的家族威胁管理的。Cisco安全MARS结合传统安全事件监控以网络智能、上下文相关性、向量分析、异常情况检测、热点证明和自动化的缓解功能。使用这些功能的组合，Cisco安全MARS准确地识别和排除网络攻击的帮助公司，当维护网络标准时。

MARS版本	支持的工具/传感器软件
3.3.x	3.x和4.x
3.4.x	3.x , 4.x , 5.x

请参见产品[版本注释](#)欲知更多信息。

[Cisco Threat Response \(CTR\)](#)

Cisco Threat Response (CTR)与Cisco IPS传感器一起使用提供一个高效的入侵保护解决方案。Cisco Threat Response实际上排除假告警，升级实际攻击和帮助在昂贵的闯入的修正。

Cisco Threat Response是与Cisco IPS版本3.x或以上兼容。请参见产品[版本注释](#)欲知更多信息。并且，请注意[End-of - Cisco Threat Response的生活公告](#)。

[IDS Event Viewer \(IEV\)](#)

IDS Event Viewer (IEV)是enable (event)查看和管理五个传感器的警报的您的一个基于Java的应用程序。使用IDS Event Viewer您能连接对和视图警报在实时或在被导入的日志文件。您能配置过滤器和视图帮助您管理警报和导入和导出进一步分析的事件数据。IDS Event Viewer为签名说明也提供存取对于网络安全数据库(NSDB)。

IEV从IDS版本3.1支持到版本4.x。虽然不再支持从版本5.x，它可以用于监控版本5.x传感器。然而，新的5.0功能没有由IEV报告。请参见[产品配置示例和Technotes](#)欲知更多信息。

[IDS服务管理器\(IDM\)](#)

IDS服务管理器(IDM)是允许您配置与管理您的传感器的基于Web的应用。IDS服务管理器的Web服务器在传感器驻留。您能通过Netscape或Internet Explorer Web浏览器访问它。

IDM从IDS版本3.1支持。参考[产品配置示例和TechNotes](#)欲知更多信息。

[Cisco Secure Policy Manager](#)

Cisco Secure Policy Manager为Cisco IDS传感器、PIX防火墙和IPSec VPN路由器提供基于策略的安全管理。

Note: CSPM到达了其EoL。请参见[EoS/EoL公告Cisco Secure Policy Manager 2.x & 3.x的](#)。

型号	CS P M 2.2	CSP M 2.3i	CSPM 2.3.1i	CSPM 2.3.2i	CSPM 2.3.3i
IDS 4210	2.2 .0.	2.2. 0.x	2.2.0.x 2.2.1.x	2.2.0.x 2.2.1.x	2.2.0.x 2.2.1.5 2.5(1)S3
IDS	x	2.2.	2.5.(0)	2.5.(0)	2.2.1.0 2.2.1.6

4220 IDS 4230	2.2 .1. x 2.5 (0)	1.x 2.5. (0)S 0 2.5(1)S0 2.5(1)S2	S0 2.5(1)S 0 2.5(1)S 2 3.0(1)S 3 3.0(1)S 4	S0 2.5(1)S 0 2.5(1)S 2 3.0(1)S 3 3.0(1)S 4	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
Catalys t 6000 Intrust ion Detecti on System Module (IDSM- 1)	2.5 IDS M	2.5 IDSM	2.5 IDSM 3.0 IDSM	2.5 IDSM 3.0 IDSM	2.5(0)S0 IDSM 2.5(1)S2 IDSM 2.5(1)S0 IDSM 3.0(1)S4 IDSM 2.5(1)S1 IDSM 3.0(1)S6 IDSM

UNIX导向器

UNIX导向器为安全的管理在间一个分布式网络的提供一个集中化图形界面。当安全事件发生时，它可通过第三方工具也执行其他重要功能例如对NSDB的数据管理，访问，传感器的远程监控和管理 and IDSM，并且发送页或电子邮件到保安。导向器接口运行在它上面HP OpenView。

Note: Cisco IDS工具传感器的软件版本2.2.x到达了其EoL。请参见[生活结尾Cisco IDS 2.2.x传感器软件文档](#)的。

导向器版本	支持的工具/传感器软件
2.1.1	2.1.1
2.2.0	2.2.0
2.2.1	2.2.1
2.2.2	2.2.2和2.5
2.2.3*	2.2.3, 3.0, 3.1

* 2.2.3是IDS控制器软件和传感器软件3.1的最后可用的版本和前。

当2.2.x导向器可能向后是与2.2.x传感器版本兼容时，如果没有在导向器和传感器的至少同一个软件版本，更新的传感器功能可能不取得到在导向器。这强制一手工的line configuration命令。欲了解更详细的信息请参见[产品文档](#)。

Related Information

- [思科入侵防御系统](#)
- [安全产品售后通知\(包括CiscoSecure Intrusion Detection\)](#)