

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[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\(火星\)](#)

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

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

[IDS服务管理器\(IDM\)](#)

[Cisco Secure Policy Manager](#)

[UNIX Director](#)

[相关信息](#)

简介

本文为思科入侵防御系统(IPS)伊莱克斯(4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255), 可适应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)提供硬件/软件兼容性矩阵。本文也提供管理选项的概述。提供每应用程序简要概述, 以及版本兼容性矩阵。在每兼容性矩阵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伊莱克斯是传感器。参考相关产品文档和版本注释欲知更多信息。

注意： 注意产品Status (状态)列在本文内的表里。此列表示相关到期(EOL) /End销售(EoS)通知。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

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)伊莱克斯(4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255)
- 可适应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)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

IPS硬件/软件兼容性

表1?Appliances

设备	部分 #	硬件	可选接口	可用的另外的硬件	兼容软件版本	产品状态
ID S-4210	ID S-4210	有CD-ROM联机的IDE硬盘驱动器软件升级和镜像恢复目的。		SmartNet 客户的IDS-4210-MEM-U=另外的256 MB内存只升级对版本4.1和以上。客户能通过 产品升级工具(仅限注册用户) 订购内存。	3.1 对当前*	销售终止：十二月8 ，支持2003年 最后一天：十二月8 ，2008
ID S-4215	ID S-4215	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-4FE-INT=		4.1 对当前*	当前
ID	ID	有CD-ROM联机		SmartNet	3.	销售终

DS-4220-E		的IDE硬盘驱动器软件升级和镜像恢复目的。		客户的IDS-4220-MEM-U=另外的256MB内存只升级对版本4.1和以上。客户能通过 产品升级工具(仅限注册用户) 订购内存。	1到4.1	止：七月31，支持2002年最后一天：七月31，2007
IDS-4230-FE		有CD-ROM联机的IDE硬盘驱动器软件升级和镜像恢复目的。			3.1到4.1	销售终止：七月31，支持2002年最后一天：七月31，2007
IDS-4235-K9		有CD-ROM联机的SCSI硬盘驱动器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*	销售终止：2005年5月31日支持最后一天：2010年5月31日
IPS-4240-K9	IP S-4240-D C-K9 (D C 只供给	微型闪存。软件升级和镜像恢复目的没有光盘驱动器联机。			4.1.4对当前*	当前

	动力, NEBS兼容)					
IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	有CD-ROM联机的SCSI硬盘驱动器软件升级和镜像恢复目的。	IDS-4250-SX-K9 IDS-4250-XL-K9	IDS-PWR=节省电源IDS-SCSI=备件SCSI硬盘驱动器	3.1对当前*	TX仅版本销售终止 : 2005年5月31日支持最后一天 TX的 : 2010年5月31日另外两IDS 4250平台没有影响的是受此EoL通告的。	
IPS-4250-K9	微型闪存。软件升级和镜像恢复目的没有光盘驱动器联机。			4.1.4对当前*	当前	

表2?Modules

模块	部分#	硬件	可选接口	可用的另外的硬件	兼容软件版本	产品状态
S	ASA-	微型闪存。软件升级			5.0对当	当

SSM	SSM-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)	和镜像恢复目的没有光盘驱动器联机。			前*	前
路由模块	NM-CIDS-K9 NM-CIDS-K9= (RMA 零件 #只)	微型闪存。软件升级的光盘驱动器联机和镜像恢复不目的。			Cisco IOS软件版本 12.2(15) ZJ或以上 Cisco IOS软件版本 12.3(4)T 或以上 IDS 4.1对当前*	当前
IDSM-1	WS-X6381-IDS WS-X6381-IDS= (RMA 零件 #只)	IDE硬盘驱动器。软件升级或镜像恢复目的没有光驱联机。			2.5到3.0	销售终止：April 2003 支持 2003 年最后

						二天 : April 20 + 2008
IDS M-2	WS-SVC-IDS2-BUN-K9 WS-SVC-IDS2BUNK9 =(RMA零件#只)	IDE硬盘驱动器和微型闪存。软件升级和镜像恢复目的没有光盘驱动器联机。			4.0对当前*	当前

注意： 软件联机新版本在本文的出版物的时是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

您能管理和配置IPS传感器通过命令行界面，或者通过这些部分或管理工具列出的其中一配置。

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Cisco系统网络传感器、交换机IPS传感器、IPS网络模块路由器的和在路由器的轴向入侵防御软件的配置的。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。

参考[支持的设备和软件版本管理中心的IPS传感器](#)文档的兼容性信息。

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
- 思科PIX防火墙
- Cisco Catalyst 6500系列防火墙服务模块(FWSM)
- CiscoWorks Management Center for Cisco Security Agents
- CiscoWorks Monitoring Center for Security服务器

参考[支持的设备和软件版本监控的中心安全](#)文档的兼容性信息。

[思科安全检测、分析及响应系统\(火星\)](#)

Cisco安全监听分析和答复系统(火星)是高性能，可扩展设备，监听和缓解家族帮助客户做更加有效的使用网络和安全设备的威胁管理的。Cisco安全火星结合传统安全事件监听以网络智能、上下文相关性、向量分析、异常情况检测、热点识别和自动化的缓解功能。使用这些功能的组合，Cisco安全火星帮助公司准确地识别和排除网络攻击，当维护网络标准时。

火星版本	支持的设备/传感器软件
3.3.x	3.x和4.x
3.4.x	3.x , 4.x , 5.x

参考[产品版本注释](#)欲知更多信息。

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

Cisco Threat Response (CTR)与思科IPS传感器一起使用提供一高效入侵保护解决方案。Cisco Threat Response实际上排除假告警，升级实时攻击和帮助在昂贵的入侵的修正。

Cisco Threat Response是与Cisco IPS版本3.x或以上兼容。参考[产品版本注释](#)欲知更多信息。并且，请注意Cisco Threat Response的[生命终止通知](#)。

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

IDS Event Viewer (IEV)是使您查看和管理五个传感器的报警的一基于Java的应用程序。使用IDS Event Viewer您能连接对和查看报警在实时或在已导入日志文件。您能配置过滤器和视图帮助您管理报警和导入和出口事件数据进一步分析的。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，它可以用于监控程序版本5.x传感器。然而，新的5.0功能没有由IEV报告。参考[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。

注意： CSPM到达了其EoL。参考[EoS/EoL通告Cisco Secure Policy Manager 2.x & 3.x的](#)。

型号	CSPM 2.2	CSPM 2.3i	CSPM 2.3.1i	CSPM 2.3.2i	CSPM 2.3.3i

UNIX Director

UNIX向导为安全的管理在间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和IDSM和发送页或者电子邮件到保安。导向器接口运行在它上面HP OpenView。

注意： Cisco IDS设备传感器的软件版本2.2.x到达了其EoL。参考[Cisco IDS 2.2.x传感器软件文档的生命周期终止](#)。

导向器版本	支持的设备/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是最后可用的版本IDS控制器软件和传感器软件3.1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，如果没有在两个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参考[产品文档](#)。

相关信息

- [Cisco Intrusion Prevention System](#)
- [安全产品的问题信息通告 \(Field Notice \) \(包括CiscoSecure Intrusion Detection\)](#)
- [技术支持和文档 - Cisco Systems](#)