

入侵檢測系統相容性矩陣

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[IPS硬體/軟體相容性](#)

[管理和配置選項](#)

[適用於IPS感應器的CiscoWorks管理中心\(IPS MC\)](#)

[CiscoWorks安全監控中心\(SecMon\)](#)

[思科安全監控、分析及回應系統\(MARS\)](#)

[思科威脅回應\(CTR\)](#)

[IDS事件檢視器\(IEV\)](#)

[IDS裝置管理員\(IDM\)](#)

[思科安全原則管理員\(CSPM\)](#)

[UNIX Director](#)

[相關資訊](#)

簡介

本文檔提供了思科入侵防禦系統(IPS)裝置(4210、4215、4220、4230、4235、4240、4250、4255)、自適應安全裝置安全服務模組(SSM)、路由器模組和Catalyst 6000入侵檢測系統模組(IDSM-1、IDSM-2)的硬體/軟體相容性矩陣。本文檔還提供了管理選項的概述。提供了每個應用程式的簡要概述以及版本相容性矩陣。每個相容性矩陣中列出的版本是唯一受支援的版本。

思科入侵防禦系統以前稱為思科入侵檢測系統(IDS)或NetRanger。思科入侵防禦系統裝置也稱為感測器。有關詳細資訊，請參閱相關產品文檔和發行說明。

注意：請注意本文檔中表格中的「產品狀態」列。此列表示相關的壽命終止(EoL)/銷售終止(EoS)通知。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科入侵防禦系統(IPS)裝置(4210、4215、4220、4230、4235、4240、4250、4255)
- 調適型安全裝置安全服務模組(SSM)
- 路由器模組
- Catalyst 6000入侵偵測系統模組(IDSM-1、IDSM-2)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

IPS硬體/軟體相容性

表1 — 裝置

裝置	部件號	硬體	可選介面	可用的其他硬體	相容的軟體版本	產品狀態
IDS-4210-4210-24210-10	IDS-4210-4210-K9	帶有CDROM的IDE硬碟可用於軟體升級和映像恢復。		IDS-4210-MEM-U= SmartNet客戶僅需升級到版本4.1及更高版本即可獲得額外256 MB記憶體。客戶可以通過 產品升級工具 訂購記憶體(僅限 註冊 客戶)。	3.1到當前*	銷售結束：二〇〇三年十二月八日 最後支援日期：二零零八年十二月八日
IDS-4215-4215-15	IDS-4215-K9	IDE硬碟和快閃記憶體。沒有CDROM驅動器可用於軟體升級和映像恢復。	ID S-4F E-IN T=		4.1到當前*	當前
ID-4220-E	IDS-4220-E	帶有CDROM的		IDS-4220-MEM-U=	3.1	銷售結束

S-4220		IDE硬碟可用於軟體升級和映像恢復。		SmartNet客戶僅需升級到版本4.1及更高版本即可獲得額外256 MB記憶體。客戶可以通過 產品升級工具 訂購記憶體(僅限 註冊 客戶)。	-4.1	: 2002年七月三十一日 最後支援日期 : 2007年七月三十一日
IDS-4230	IDS-4230-FE	帶有CDROM的IDE硬碟可用於軟體升級和映像恢復。			3.1-4.1	銷售結束 : 2002年七月三十一日 最後支援日期 : 2007年七月三十一日
IDS-4235	IDS-4235-K9	帶有CDROM的SCSI硬碟可用於軟體升級和映像恢復。	IDS-4FE-INT=	IDS-PWR=備用電源	3.1到當前*	銷售結束 : 2005年5月31日 最後支援日期 : 2002年五月三十一日
IPS-4240	IPS-4240-K9 IPS-4240-DC-K9 (直流	快閃記憶體。沒有光碟機可用於軟體升級和映像恢復。			4.1.4到當前	當前

240	供電，僅符合NEBS標準)				前*	
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	帶有CDROM的SCSI硬碟可用於軟體升級和映像恢復。	ID S-4F E-IN T= ID S-42 50 - SX - IN T= ID S-XL - IN T=	IDS-PWR=備用電源 IDS-SCSI=備用SCSI硬碟	3.1到當前*	TX版本僅銷售結束 : 2005年5月31日 TX支援的最後一天 : 2010年5月31日 其他兩個IDS 4250平台不受此EoL公告的影響。
IPS-4255	IPS-4255-K9	快閃記憶體。沒有光碟機可用於軟體升級和映像恢復。			4.1.4到當前*	當前

表2 — 模組

模組	部件號	硬體	可選介面	可用的其他硬體	相容的軟體版本	產品狀態
SSM	ASA-SSM-AIP-10-K9 (ASA	快閃記憶體。沒有光碟機可用於軟體升級和映像			5.0到當前*	當前

	AIP安全服務模組 -10) ASA-SSM-AIP-20-K9 (ASA AIP安全服務模組 -20)	恢復。			
路由器模組	NM-CIDS-K9 NM-CIDS-K9= (僅限RMA部件號)	快閃記憶體。沒有光碟機可用於軟體升級和映像恢復。		Cisco IOS®軟體版本 12.2(15)Z J或更新版本 Cisco IOS軟體版本 12.3(4)T 或更新版本 IDS 4.1到最新版本*	當前
IDS M-1	WS-X6381-IDS WS-X6381-IDS= (僅限RMA部件號)	IDE硬碟。沒有光碟機可用於軟體升級或映像恢復。		2.5 - 3.0	銷售結束：二〇〇三年四月二十日 最後支援日期：二零零八年四月二十日
IDS M-2	WS-SVC-IDS2-BUN-K9 WS-SVC-IDS2BUNK9= (僅限RMA部件號)	IDE硬碟和快閃記憶體。沒有光碟機可用於軟體升級和映像恢復。		4.0到當前*	當前

附註： 本文檔發佈時可用的最新軟體版本是5.1。如果您需要高於5.1的軟體版本，請檢視文檔中的該版本代碼，以確保相容性。

管理和配置選項

您可以通過命令列介面或通過以下部分列出的配置或管理工具來管理和配置IPS感測器。

適用於IPS感應器的CiscoWorks管理中心(IPS MC)

CiscoWorks Management Center for IPS Sensors (IPS感測器管理中心) 是一個具有可擴展架構的工具，用於在路由器中配置Cisco Systems網路感測器、交換機IPS感測器、IPS網路模組以及內聯入侵防禦軟體。CiscoWorks Management Center for IPS Sensors允許管理員通過使用組配置檔案同時配置多個感測器來節省時間。此外，它還提供強大的簽名管理功能，可提高檢測可能的網路入侵的準確性和特異性。

有關相容性資訊，請參閱[Management Center for IPS Sensors支援的裝置和軟體版本](#)文檔。

CiscoWorks安全監控中心(SecMon)

CiscoWorks Monitoring Center for Security是一個用於捕獲、儲存、檢視、關聯和報告安全事件的工具，來自：

- Cisco網路IPS
- Cisco網路IDS
- Cisco交換器IDS
- 具有內嵌IPS功能的Cisco IOS路由器
- 適用於路由器的Cisco IDS模組
- Cisco PIX防火牆
- Cisco Catalyst 6500系列防火牆服務模組(FWSM)
- 適用於思科安全代理的CiscoWorks管理中心
- 適用於安全伺服器的CiscoWorks監控中心

有關相容性資訊，請參閱[Monitoring Center for Security支援的裝置和軟體版本](#)。

思科安全監控、分析及回應系統(MARS)

思科安全監控分析和響應系統(MARS)是一系列高效能、可擴展的裝置，用於威脅管理、監控和緩解，可幫助客戶更有效地利用網路和安全裝置。Cisco Security MARS將傳統安全事件監控與網路智慧、情景關聯、向量分析、異常檢測、熱點識別和自動緩解功能相結合。藉助這些功能的組合，Cisco Security MARS可幫助公司準確識別和消除網路攻擊，同時保持網路合規性。

MARS版本	支援的裝置/感測器軟體
3.3.x	3.x和4.x
3.4.x	3.x、4.x、5.x

有關詳細資訊，請參閱產品[發行說明](#)。

思科威脅回應(CTR)

Cisco Threat Response(CTR)與Cisco IPS感測器配合使用，可提供高效的入侵防護解決方案。思科威脅響應實際上消除了誤報，升級了真正的攻擊，並有助於補救昂貴的入侵。

Cisco Threat Response與Cisco IPS 3.x版或更高版本相容。有關詳細資訊，請參閱產品[發行說明](#)。此外，請注意思科[威脅響應的終止生命公告](#)。

[IDS事件檢視器\(IEV\)](#)

IDS事件檢視器(IEV)是一個基於Java的應用程式，可用於檢視和管理最多五個感測器的警報。通過IDS事件檢視器，您可以即時連線並檢視警報，也可以在匯入的日誌檔案中檢視警報。您可以配置過濾器 and 檢視，以幫助您管理警報以及匯入和匯出事件資料以進行進一步分析。IDS事件檢視器還提供對網路安全資料庫(NSDB)的訪問，以瞭解特徵碼說明。

從IDS 3.1版到4.x版支援IEV。雖然版本5.x不再支援，但可用於監控版本5.x感測器。但是，IEV未報告新的5.0特性。如需詳細資訊，請參閱[產品組態範例和Technotes](#)。

[IDS裝置管理員\(IDM\)](#)

IDS裝置管理器(IDM)是一個基於Web的應用程式，可用於配置和管理感測器。IDS裝置管理器的Web伺服器位於感測器上。您可以通過Netscape或Internet Explorer Web瀏覽器訪問它。

IDS 3.1版支援IDM。有關詳細資訊，請參閱[產品配置示例和TechNotes](#)。

[思科安全原則管理員\(CSPM\)](#)

Cisco Secure Policy Manager(CSPM)為Cisco IDS感測器、PIX防火牆和IPsec VPN路由器提供基於策略的安全管理。

註： CSPM已達到其停產許可證。請參閱[Cisco Secure Policy Manager 2.x和3.x的EoS/EoL公告](#)。

型號	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. x	2.2. 0.x 2.2. 1.x 2.5. (0)S	2.2.0.x 2.2.1.x 2.5.(0) S0 2.5(1)S 0	2.2.0.x 2.2.1.x 2.5.(0) S0 2.5(1)S 0	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
IDS 4220	2.2 .1. x	2.5. (0)S 0	2.5(1)S 2	2.5(1)S 2	2.2.1.2 2.5(1)S0 3.0(1)S6
IDS 4230	2.5 (1)S0 (0)	2.5(1)S0 2.5(1)S2	3.0(1)S 3 3.0(1)S 4	3.0(1)S 3 3.0(1)S 4	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 Director](#)

UNIX Director提供了一個集中化的圖形介面，用於管理分散式網路中的安全性。它還可以執行其他重要功能，例如通過第三方工具進行資料管理、訪問NSDB、遠端監控和管理感測器和IDSM，以及在發生安全事件時向安全人員傳送頁面或電子郵件。Director介面運行在HP OpenView之上。

注意： Cisco IDS裝置感測器的軟體版本2.2.x已達到其停產日期。請參閱[Cisco IDS 2.2.x感測器軟體生命週期結束文檔](#)。

控制器版本	支援的裝置/感測器軟體
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 Director軟體的最後可用版本，支援感測器軟體3.1及更低版本。

雖然2.2.x導向器可能會向後相容2.2.x感測器版本，但如果您在導向器和感測器上都沒有至少相同版本的軟體，則較新的感測器功能可能在Director中不可用。這會強制進行手動命令列配置。如需詳細資訊，請參閱[產品檔案](#)。

[相關資訊](#)

- [思科入侵防禦系統](#)
- [安全產品現場通知 \(包括CiscoSecure Intrusion Detection \)](#)