Kompatibilitätsmatrix für Intrusion Detection System

Inhalt

Einführung

Dieses Dokument enthält eine Hardware-/Software-Kompatibilitätsmatrix für die Cisco Intrusion Prevention System (IPS) Appliances (4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255), Adaptive Security Appliance Security Services Module (SSM). Router Module und Catalyst 6000 Intrusion Detection System Module (IDSM-1, IDSM-2). Dieses Dokument bietet auch eine Übersicht über die Verwaltungsoptionen. Es wird eine kurze Übersicht über jede Anwendung sowie eine Versionskompatibilitätsmatrix bereitgestellt. Die in jeder Kompatibilitätsmatrix aufgelisteten Versionen sind die einzigen unterstützten Versionen.

Das Cisco Intrusion Prevention System (IDS) wurde früher als Cisco Intrusion Detection System (IDS) oder NetRanger bezeichnet. Die Cisco Intrusion Prevention System Appliances werden auch als Sensoren bezeichnet. Weitere Informationen finden Sie in der entsprechenden Produktdokumentation und in den Versionshinweisen.

Hinweis: Beachten Sie die Spalte "Produktstatus" in den Tabellen in diesem Dokument. In dieser Spalte werden relevante Benachrichtigungen zum End-of-Life/End-of-Sale (EoS) aufgeführt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Kompatibilität von IPS-Hardware und -Software

Tabelle 1: Appliances

Appliance	Teilenummer	Hardware	Optionale Schnittstellen	Verfügbare zusätzliche Hardware	Kompatible Softwareversionen	Produktstatus
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	IDE-Festplatte mit CD-ROM für Software-Upgrades und Image-Recovery.		IDS-4210-MEM-U= Zusätzlicher Speicher von 256 MB für SmartNet-Kunden, der nur auf	3.1 bis aktuell *	**Vertriebsende:** 8. Dezember 2003 **Letzter Support-Tag:** 8. Dezember 2008

				Version 4.1 und höher aktualisiert werden kann. Kunden können den Speicher über das Product Upgrade Tool bestellen (nur registrierte Kunden).		
IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9	IDE-Festplatte und Compact Flash. Es ist kein CD-ROM-Laufwerk für Software-Upgrades und Image-Wiederherstellungszwecke verfügbar.	IDS-4FE-INT=		4,1 auf aktuelle *	Aktuell
IDS-4220	IDS-4220-E	IDE-Festplatte mit CD-ROM für Software-Upgrades und Image-Recovery.		IDS-4220-MEM-U= Zusätzlicher Speicher von 256 MB für SmartNet-Kunden, der nur auf	3,1 bis 4,1	**Vertriebsende:** 31. Juli 2002 **Letzter Support-Tag:** 31. Juli 2007

				Version 4.1 und höher aktualisiert werden kann. Kunden können den Speicher über das Product Upgrade Tool bestellen (nur registrierte Kunden).		
IDS-4230	IDS-4230-FE	IDE-Festplatte mit CD-ROM für Software-Upgrades und Image-Recovery.			3,1 bis 4,1	**Vertriebsende:** 31. Juli 2002 **Letzter Support-Tag:** 31. Juli 2007
IDS-4235	IDS-4235-K9	SCSI-Festplatte mit CD-ROM für Software-Upgrades und Image-Wiederherstellungszwecke verfügbar.	IDS-4FE-INT=	IDS-PWR= Ersatznetzteil	3.1 bis aktuell *	**Vertriebsende:** 31. Mai 2005 **Letzter Support-Tag:** 31. Mai 2010
IPS-4240	IPS-4240-K9 IPS-4240-DC-	Compact Flash Es ist kein CD-ROM-Laufwerk für Software-			4,1,4 bis zum aktuellen *	Aktuell

	K9 (Gleichstrom, nur NEBS-konform)	Upgrades und Image-Recovery verfügbar.				
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	SCSI-Festplatte mit CD-ROM für Software-Upgrades und Image-Wiederherstellungszwecke verfügbar.	IDS-4FE-INT= IDS-4250-SX-INT= IDS-XL-INT=	IDS-PWR= Ersatznetzteil IDS-SCSI= ErsatzSCSI-Festplatte	3.1 bis aktuell *	**Nur TX-Version Ende des Vertriebszeitraums:** 31. Mai 2005 Letzter Support-Tag für TX: 31. Mai 2010 Die beiden anderen IDS 4250-Plattformen sind von dieser EoL-Ankündigung nicht betroffen.
IPS-4255	IPS-4255-K9	Compact Flash Es ist kein CD-ROM-Laufwerk für Software-			4,1,4 bis zum aktuellen *	Aktuell

		Upgrades und Image-Recovery verfügbar.				

Tabelle 2 - Module

Modul	Teilenummer	Hardware	Optionale Schnittstellen	Verfügbare zusätzliche Hardware	Kompatible Softwareversionen	Produktstatus
SSM	ASA-SSM-AIP-10-K9 (ASA AIP Security Service Module-10) ASA-SSM-AIP-20-K9 (ASA AIP Security Service Module-20)	Compact Flash Es ist kein CD-ROM-Laufwerk für Software-Upgrades und Image-Recovery verfügbar.			5,0 auf aktuelles *	Aktuell
Router-Modul	NM-CIDS-K9 NM-CIDS-K9= (nur RMA-Teilenummer)	Compact Flash Es ist kein CD-ROM-Laufwerk für Software-Upgrades und Image-Recovery verfügbar.			Cisco IOS® Softwareversion 12.2(15)ZJ oder höher Cisco IOS Software Version 12.3(4)T oder höher	Aktuell

					IDS 4.1 auf aktuelle Version*	
IDS M-1	WS-X6381-IDS WS-X6381-IDS= (NUR RMA-Teilenummer)	IDE-Festplatte. Es ist kein CD-ROM-Laufwerk für Software-Upgrades oder Image-Wiederherstellungszwecke verfügbar.			2,5 bis 3,0	**Vertriebsende:** 20. April 2003 **Letzter Support-Tag:** 20. April 2008
IDS M-2	WS-SVC-IDS2-BUN-K9 WS-SVC-IDS2BUNK9= (nur RMA-Teilenummer)	IDE-Festplatte und Compact Flash. Es ist kein CD-ROM-Laufwerk für Software-Upgrades und Image-Recovery verfügbar.			4,0 auf aktuelles *	Aktuell

Hinweis: Die aktuelle Softwareversion, die zum Zeitpunkt der Veröffentlichung dieses Dokuments verfügbar ist, ist 5.1. Wenn Sie eine Softwareversion benötigen, die später als 5.1 ist, überprüfen Sie die Dokumentation für diese Codeversion, um die Kompatibilität sicherzustellen.

Management- und Konfigurationsoptionen

IPS-Sensoren können über die Befehlszeilenschnittstelle oder über eines der in diesen Abschnitten aufgeführten Konfigurations- oder Verwaltungstools verwaltet und konfiguriert werden.

CiscoWorks Management Center für IPS-Sensoren (IPS MC)

CiscoWorks Management Center für IPS-Sensoren ist ein Tool mit einer skalierbaren Architektur für die Konfiguration von Cisco Systems Network Sensors, Switch IPS Sensors, IPS-Netzwerkmodulen für Router und Inline Intrusion Prevention Software in Routern. Mit CiscoWorks Management Center für IPS-Sensoren können Administratoren durch die gleichzeitige Konfiguration mehrerer Sensoren mithilfe von Gruppenprofilen Zeit sparen. Darüber hinaus bietet sie eine leistungsstarke Funktion für das Signaturmanagement, die die Genauigkeit und Spezifität bei der Erkennung möglicher Netzwerkzugriffe erhöht.

Kompatibilitätsinformationen finden Sie in der Dokumentation Unterstützte Geräte und Softwareversionen für Management Center für IPS-Sensoren.

CiscoWorks Monitoring Center for Security (SecMon)

CiscoWorks Monitoring Center for Security ist ein Tool zum Erfassen, Speichern, Anzeigen, Korrelieren und Berichten von Sicherheitsereignissen von:

- Cisco Netzwerk-IPS
- Cisco Netzwerk-IDS
- Cisco Switch-IDS
- Cisco IOS-Router mit Inline-IPS-Funktionen
- Cisco IDS-Module für Router
- Cisco PIX-Firewalls
- Cisco Catalyst Firewall Services Module (FWSM) der Serie 6500
- CiscoWorks Management Center für Cisco Security Agents
- CiscoWorks Monitoring Center für Sicherheitsserver

Kompatibilitätsinformationen finden Sie in der Dokumentation Supported Devices and Software Versions for Monitoring Center for Security.

Cisco Security Monitoring, Analysis and Response System (MARS)

Das Cisco Security Monitoring Analysis and Response System (MARS) ist eine Produktfamilie von hochleistungsfähigen, skalierbaren Appliances für das Management, die Überwachung und die Eindämmung von Bedrohungen, die Kunden dabei unterstützen, Netzwerk- und Sicherheitsgeräte effektiver zu nutzen. Cisco Security MARS kombiniert die traditionelle Überwachung von Sicherheitsvorfällen mit Netzwerkintelligenz, Kontextkorrelation, Vektoranalyse, Anomalieerkennung, Hotspot-Erkennung und automatisierten Eindämmungsfunktionen. Cisco Security MARS kombiniert diese Funktionen, um Unternehmen bei der präzisen Identifizierung und Beseitigung von Netzwerkangriffen zu unterstützen und gleichzeitig die Netzwerkkonformität zu wahren.

MARS-Versionen	Unterstützte Appliance/Sensorsoftware
3,3,x	3.x und 4.x
3,4 x	3.x, 4.x, 5.x

Weitere Informationen finden Sie in den Versionshinweisen zum Produkt.

Cisco Threat Response (CTR)

Cisco Threat Response (CTR) bietet zusammen mit Cisco IPS-Sensoren eine effiziente Lösung für den Schutz vor Sicherheitsrisiken. Cisco Threat Response beseitigt Fehlalarme praktisch, eskaliert echte Angriffe und hilft bei der Beseitigung kostspieliger Angriffe.

Cisco Threat Response ist mit Cisco IPS ab Version 3.x kompatibel. Weitere Informationen finden Sie in den Versionshinweisen zum Produkt. Beachten Sie auch die End-of-Life-Ankündigung von Cisco Threat Response.

IDS Event Viewer (IEV)

IDS Event Viewer (IEV) ist eine Java-basierte Anwendung, mit der Sie Alarme für bis zu fünf Sensoren anzeigen und verwalten können. Mit IDS Event Viewer können Sie in Echtzeit oder in importierten Protokolldateien eine Verbindung herstellen und Alarme anzeigen. Sie können Filter und Ansichten konfigurieren, um die Alarme zu verwalten und Ereignisdaten für weitere Analysen zu importieren und zu exportieren. Die IDS Event Viewer bietet außerdem Zugriff auf die Network Security Database (NSDB) für Signaturbeschreibungen.

IEV wird von IDS Version 3.1 bis Version 4.x unterstützt. Die Version 5.x wird zwar nicht mehr unterstützt, kann aber zur Überwachung von Sensoren der Version 5.x verwendet werden. Die neuen 5.0-Funktionen werden jedoch nicht von IEV gemeldet. Weitere Informationen finden Sie in den Produktkonfigurationsbeispielen und technischen Hinweisen.

IDS Device Manager (IDM)

IDS Device Manager (IDM) ist eine webbasierte Anwendung, mit der Sie Ihren Sensor konfigurieren und verwalten können. Der Webserver für den IDS Device Manager befindet sich auf dem Sensor. Der Zugriff erfolgt über Netscape- oder Internet Explorer-Webbrowser.

IDM wird von IDS Version 3.1 unterstützt. Weitere Informationen finden Sie in den Produktkonfigurationsbeispielen und in technischen Hinweisen.

Cisco Secure Policy Manager (CSPM)

Cisco Secure Policy Manager (CSPM) bietet ein richtlinienbasiertes Sicherheitsmanagement für Cisco IDS-Sensoren, PIX-Firewalls und IPsec-VPN-Router.

Hinweis: CSPM hat seine EoL erreicht. Weitere Informationen finden Sie in der EoS/EoL-Ankündigung zu Cisco Secure Policy Manager 2.x und 3.x.

Modell	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 Intrustion Detecti	2.5 IDSM	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

on System Module (IDSM-1)					3.0(1)S6 IDSM

UNIX Director

UNIX Director bietet eine zentrale grafische Oberfläche für das Management von Sicherheit in einem verteilten Netzwerk. Darüber hinaus können andere wichtige Funktionen wie das Datenmanagement mithilfe von Drittanbieter-Tools, der Zugriff auf das NSDB, die Fernüberwachung und -verwaltung von Sensoren und IDSMs sowie das Senden von Seiten oder E-Mails an Sicherheitspersonal ausgeführt werden, wenn Sicherheitsereignisse auftreten. Die Director-Schnittstelle wird auf HP OpenView ausgeführt.

Hinweis: Softwareversion 2.2.x für den Cisco IDS-Appliance-Sensor hat seine EoL erreicht. Weitere Informationen finden Sie in der Dokumentation zum End of Life für die Cisco IDS 2.2.x Sensor-Software.

Director-Versionen	Unterstützte Appliance/Sensorsoftware
2,1/1	2,1/1
2,2/0	2,2/0
2,2/1	2,2/1
2,2/2	2.2.2 und 2.5
2,2/3*	2.2.3, 3.0, 3.1

* 2.2.3 ist die letzte verfügbare Version der IDS Director Software und unterstützt Sensor Software 3.1 und früher.

Obwohl der 2.2.x Director abwärtskompatibel mit den 2.2.x-Sensorversionen sein kann, kann es vorkommen, dass neuere Sensorfunktionen im Director nicht verfügbar sind, wenn Sie nicht mindestens dieselbe Softwareversion auf Directors und Sensoren haben. Dies erfordert eine manuelle Befehlszeilenkonfiguration. Weitere Informationen finden Sie in der Produktdokumentation.

Zugehörige Informationen

- Cisco Intrusion Prevention System
- Problemhinweise zu Sicherheitsprodukten (einschließlich CiscoSecure Intrusion Detection)