Matrice de compatibilité du système de détection des intrusions

Contenu

Introduction

Ce document fournit un matériel/matrice de compatibilité logicielle pour) des appareils du Système de protection contre les intrusions Cisco (IPS) 4220, 4230, 4235, 4240, 4250, 4255 (4210, 4215, le module de Services de sécurité d'appliance de sécurité adaptable (SSM), le module de routeur et les modules de système de détection d'intrusion du Catalyst 6000 (IDSM-1, IDSM-2). Ce document fournit également un aperçu des options d'administration. Une brève présentation de chaque application est fournie, aussi bien qu'une matrice de compatibilité de version. Les versions répertoriées dans chaque matrice de compatibilité sont les seules versions prises en charge.

Le Système de protection contre les intrusions Cisco a été autrefois connu comme Cisco Intrusion Detection System (ID) ou NetRanger. Les appliances de Système de protection contre les intrusions Cisco sont également connues comme capteurs. Référez-vous à la documentation du produit appropriée et au pour en savoir plus de notes de mise à jour.

Remarque: Rendez-vous compte de la colonne d'état de produit dans les tables dans ce document. Cette colonne dénote des notifications appropriées de fin de vie (EoL) /End-of-Sale (EOS).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliances du Système de protection contre les intrusions Cisco (IPS) (4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255)
- Module de Services de sécurité d'appliance de sécurité adaptable (SSM)
- Module de routeur
- Modules de système de détection d'intrusion du Catalyst 6000 (IDSM-1, IDSM-2)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

IPS de matériel/compatibilité logicielle

Tableau 1 — Appliances

Appliance	Partie #	Matériel	Interfaces facultatives	Matériel supplémentaire disponible	Versions de logiciel compatibles	État de produit
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	Disque dur ide avec le disque compact-ROM disponible pour des		Mémoire supplémentaire du Mo 256 IDS-4210-MEM-U= pour des clients de SmartNet à améliore	3.1 au courant *	Fin de vente : 8 décembre 2003 le jour passé du support :

		buts de mise à niveau de logiciel et de récupération d'image.		r seulement à la version 4.1 et ultérieures. Les clients peuvent commander la mémoire par l'outil de mise à jour d'un produit (clients enregistrés seulement).		8 décembre 2008
IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9	Disque dur et Compact Flash ide. Aucun lecteur de CD-ROM n'est disponible pour des buts de mise à niveau de logiciel et de récupération d'image.	IDS-4FE-INT=		4.1 au courant *	Courant
IDS-422	IDS-4220-E	Disque dur		Mémoire supplém	3.1 à 4.1	**Fin de**

0		ide avec le disque compact-ROM disponible pour des buts de mise à niveau de logiciel et de récupération d'image.		entaire du Mo 256 IDS-4220-MEM-U= pour des clients de SmartNet à améliorer seulement à la version 4.1 et ultérieures. Les clients peuvent commander la mémoire par l'outil de mise à jour d'un produit (clients enregistrés seulement).		**vente :** Juillet 31, 2002 le **jour passé du support :** Juillet 31, 2007
IDS-4230	IDS-4230-FE	Disque dur ide avec le disque compact-ROM disponible pour des buts de mise à niveau de logiciel et de			3.1 à 4.1	**Fin de vente :** Juillet 31, 2002 le **jour passé du support :** Juillet 31, 2007

		récupération d'image.				
IDS-4235	IDS-4235-K9	Disque dur SCSI avec le disque compact-ROM disponible pour des buts de mise à niveau de logiciel et de récupération d'image.	IDS-4FE-INT=	Bloc d'alimentation de pièce de rechange IDS-PWR=	3.1 au courant *	**Fin de vente :** Mai 31, 2005 **le jour passé du support :** Mai 31, 2010
IPS-4240	IPS-4240-K9 IPS-4240-DC-K9 (C.C actionné, NEB-conforme seulement)	Compact Flash. Aucun lecteur de CD-ROM disponible pour des buts de mise à niveau de logiciel et de récupération d'image.			4.1.4 au courant *	Courant
IDS-	IDS-	Disqu	IDS-	Disque	3.1	**Fin**

4250	4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	e dur SCSI avec le disque compact-ROM disponible pour des buts de mise à niveau de logiciel et de récupération d'image.	4FE-INT= IDS-4250-SX-INT= IDS-XL-INT=	dur de la pièce de rechange SCSI du bloc d'alimentation IDS-SCSI= de pièce de rechange IDS-PWR=	au courant *	**de version TX seulement de vente :** Mai 31, 2005 **le jour passé du soutien de TX :** Mai 31, 2010 les deux autres ID 4250 Plateformes ne sont pas affectés par cette annonce d'EoL.
IPS-4255	IPS-4255-K9	Compact Flash. Aucun lecteur de CD-ROM disponible pour des buts			4.1.4 au courant *	Courant

		de mise à niveau de logiciel et de récupération d'image.				

Tableau 2 — Modules

Module	Partie #	Matériel	Interfaces facultatives	Matériel supplémentaire disponible	Versions de logiciel compatibles	État de produit
SSM	ASA-SSM-AIP-10-K9 (service de sécurité AIP ASA Module-10) ASA-SSM-AIP-20-K9 (service de sécurité AIP ASA Module-20)	Compact Flash. Aucun lecteur de CD-ROM disponible pour des buts de mise à niveau de logiciel et de récupération d'image.			5.0 au courant *	Courant
Module de routeur	NM-CIDS-K9 NM-CIDS-K9= (pièce RMA # seulement)	Compact Flash. Aucun lecteur de CD-ROM disponible pour la			Logiciel Cisco IOS version 12.3(4)T de versio	Courant

		mise à niveau de logiciel et le but de récupération d'image.			n de logiciel 12.2(15)ZJ ou ultérieures de Cisco IOS® ou ID postérieurs 4.1 au courant *	
IDSM-1	WS-X6381-IDS WS-X6381-IDS= (pièce RMA # SEULEMENT)	Disque dur ide. Aucun lecteur disque compact-ROM disponible pour des buts de mise à niveau de logiciel ou de récupération d'image.			2.5 à 3.0	**Fin de vente :** Avril 20, 2003 le **jour passé du support :** Avril 20, 2008
IDSM-2	WS-SVC-IDS2-BUN-K9 WS-SVC-IDS2BUNK9= (pièce RMA # seulement)	Disque dur et Compact Flash ide. Aucun lecteur de CD-ROM disponible pour			4.0 au courant *	Courant

		des buts de mise à niveau de logiciel et de récupération d'image.				

Remarque: La dernière version du logiciel disponible au moment de la publication de ce document est 5.1. Si vous avez besoin d'une version de logiciel qui est plus tard que 5.1, vérifiez la documentation pour cette version de code pour assurer la compatibilité.

Options de Gestion et de configurations

Vous pouvez gérer et configurer des capteurs IPS par l'intermédiaire de l'interface de ligne de commande, ou par l'intermédiaire d'un de la configuration ou des outils de gestion répertoriés dans ces sections.

CiscoWorks Management Center pour détecteurs IPS (IPS MC)

Le CiscoWorks Management Center pour détecteurs IPS est un outil avec une architecture évolutive pour la configuration des capteurs de réseau de Cisco Systems, des capteurs IPS de commutateur, des modules réseau IPS pour des Routeurs, et du logiciel intégré de prévention des intrusions dans des Routeurs. Le CiscoWorks Management Center pour détecteurs IPS permet à des administrateurs pour épargner le temps en configurant de plusieurs capteurs simultanément utilisant des profils de groupe. Supplémentaire, il fournit une fonctionnalité de gestion puissante de signature qui augmente la précision et la spécificité dans la détection des intrusions possibles de réseau.

Référez-vous aux périphériques pris en charge et aux versions de logiciel pour le centre de Gestion pour la documentation de capteurs IPS pour information les informations sur la compatibilité.

CiscoWorks surveillant le centre pour la Sécurité (SecMon)

Le CiscoWorks Monitoring Center for Security est un outil au capturer, enregistrer, visualiser, le corréler, et rendre compte des événements de Sécurité de :

- Réseau IPS de Cisco
- ID de réseau de Cisco
- Cisco commutent des ID
- Routeurs Cisco IOS avec des fonctions IPS intégrées
- Modules IDS de Cisco pour des Routeurs
- Pare-feu de Cisco PIX
- Modules de services de Pare-feu de gamme Cisco Catalyst 6500 (FWSM)
- CiscoWorks Management Center pour Cisco Security Agents

- Serveurs de CiscoWorks Monitoring Center for Security

Référez-vous aux périphériques pris en charge et aux versions de logiciel pour surveiller le centre pour la documentation de Sécurité pour information les informations sur la compatibilité.

Système de sécurité pour la surveillance, l'analyse et l'intervention de Cisco (MARS)

L'analyse de surveillance de sécurité Cisco et le système de réponse (MARS) est une famille de haute performance, d'appliances extensibles pour la Gestion de menace, de surveillance, et de réduction qui aide des clients à faire une utilisation plus efficace du réseau et des périphériques de sécurité. La sécurité Cisco TROUBLE la surveillance traditionnelle d'événement de Sécurité de cartels avec l'intelligence réseau, la corrélation de contexte, l'analyse de vecteur, la détection d'anomalie, l'identification de point névralgique, et les capacités automatisées de réduction. Avec la combinaison de ces capacités, sociétés d'aides de MARS de sécurité Cisco exactement pour identifier et éliminer des attaques réseau tout en mettant à jour la conformité de réseau.

Versions de MARS	Logiciel pris en charge d'appareils/capteur
3.3.x	3.x et 4.x
3.4.x	3.x, 4.x, 5.x

Référez-vous au pour en savoir plus de notes de distribution du produit.

Solutions de sécurité pour neutraliser les menaces réseau Cisco (CTR)

Le Solutions de sécurité pour neutraliser les menaces réseau Cisco (CTR) fonctionne avec des capteurs de Cisco IPS pour fournir une solution efficace de protection contre les intrusions. Le Solutions de sécurité pour neutraliser les menaces réseau Cisco élimine presque entièrement des fausses alertes, fait suivre de vraies attaques, et aides dans la correction des intrusions coûteuses.

Le Solutions de sécurité pour neutraliser les menaces réseau Cisco est compatible avec la version 3.x ou ultérieures de Cisco IPS. Référez-vous au pour en savoir plus de notes de distribution du produit. En outre, rendez-vous compte de l'annonce de fin de vie pour le Solutions de sécurité pour neutraliser les menaces réseau Cisco.

Visualisateur d'événements d'ID (IEV)

Le visualisateur d'événements d'ID (IEV) est une application basée sur Java qui te permet de visualiser et gérer des alarmes pour jusqu'à cinq capteurs. Avec le visualisateur d'événements d'ID vous pouvez se connecter à et des alarmes de vue en temps réel ou dans des fichiers journal importés. Vous pouvez configurer des filtres et des vues pour vous aider à gérer les alarmes et à importer et exporter des données d'événement pour l'analyse approfondie. Le visualisateur d'événements d'ID permet d'accéder également à la base de données de sécurité des réseaux (NSDB) pour des descriptions de signature.

IEV est pris en charge de la version 3.1 d'ID à la version 4.x. Bien que plus non pris en charge de la version 5.x, il peut être utilisé pour surveiller des capteurs de version 5.x. Cependant, les nouvelles 5.0 caractéristiques ne sont pas signalées par IEV. Référez-vous au pour en savoir plus des exemples et de Technotes de configuration de produit.

Gestionnaire de périphériques d'ID (IDM)

Le gestionnaire de périphériques d'ID (IDM) est une application basée sur le WEB qui te permet pour configurer et gérer votre capteur. Le web server pour le gestionnaire de périphériques d'ID réside sur le capteur. Vous pouvez l'accéder à par Netscape ou navigateurs web internet explorers.

IDM est pris en charge de la version 3.1 d'ID. Référez-vous au pour en savoir plus des exemples et de TechNotes de configuration de produit.

Cisco Secure Policy Manager (CSPM)

Le Cisco Secure Policy Manager (CSPM) fournit la Gestion de la sécurité basée sur la politique pour des capteurs d'ID de Cisco, des Pare-feu PIX et des routeurs VPN d'IPsec.

Remarque: CSPM a atteint son EoL. Référez-vous à l'EOS/à annonce d'EoL pour le Cisco Secure Policy Manager 2.x et 3.x.

Modèle	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 Detection System Module (IDSM-1)	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 3.0(1)S6 IDSM

Directeur UNIX

Le directeur UNIX fournit une interface graphique centralisée pour la Gestion de la Sécurité à travers un réseau réparti. Il peut également remplir d'autres importantes fonctions telles que la gestion de données par des outils tiers, l'accès au NSDB, la télésurveillance et la Gestion des capteurs et l'IDSMs, et envoie les pages ou le courrier électronique au personnel de Sécurité quand les événements de Sécurité se produisent. Les passages d'interface de directeur sur le HP OpenView.

Remarque: La version de logiciel 2.2.x pour le capteur d'appareils d'ID de Cisco a atteint son EoL. Référez-vous à la fin de la vie pour la documentation du logiciel de capteur des ID 2.2.x de Cisco.

Versions de directeur	Logiciel pris en charge d'appareils/capteur
2.1.1	2.1.1
2.2.0	2.2.0
2.2.1	2.2.1
2.2.2	2.2.2 et 2.5
2.2.3*	2.2.3, 3.0, 3.1

* 2.2.3 est la dernière version disponible du logiciel d'IDS Director et prend en charge le logiciel 3.1 de capteur et plus tôt.

Tandis que le directeur 2.2.x peut être vers l'arrière compatible avec des versions du capteur 2.2.x, si vous n'avez pas au moins la même version du logiciel sur les deux directeurs et capteurs, une plus nouvelle fonctionnalité de capteur peut ne pas être disponible dans le directeur. Ceci force une configuration de ligne de commande manuelle. Référez-vous à la documentation du produit pour plus de détails.

Informations connexes

- Système de protection contre les intrusions Cisco
- Notes de terrain relatives aux produits de sécurité (détection y compris d'intrusion de CiscoSecure)