Matriz de compatibilidad del sistema de la detección de intrusos

Contenido

Introducción

Este documento proporciona una matriz de compatibilidad de hardware o software para los Cisco Intrusion Prevention System (IPS) Appliances (4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255), Adaptive Security Appliance Security Services Module (SSM), Router Module y Catalyst 6000 Intrusion Detection System Modules (IDSM-1, IDSM-2). Este documento también proporciona una descripción general de las opciones de Management. Se proporciona una breve descripción general de cada aplicación, así como una matriz de compatibilidad de versiones. Las versiones enumeradas en cada matriz de compatibilidad son las únicas versiones admitidas.

El Cisco Intrusion Prevention System era conocido antes como el Sistema de detección de intrusos de Cisco (IDS) o Netranger. Los dispositivos del Cisco Intrusion Prevention System también se conocen como sensores. Refiera a la Documentación del Producto y a los Release Note relevantes para más información.

Nota: Sea consciente de la columna del Estado del producto en las tablas dentro de este documento. Esta columna denota las notificaciones relevantes del fin de vida (EoL) /End-of-Sale (FOE).

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivos del (IPS) del Cisco Intrusion Prevention System (4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255)
- Módulo de Servicios de seguridad adaptante del dispositivo de seguridad (SS)
- Módulo del router
- Módulos intrusion detection system del Catalyst 6000 (IDSM-1, IDSM-2)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

IPS de compatibilidad del hardware o software

Cuadro 1 — Dispositivos

Dispositivo	Parte N°	Hardware	Interfaces opcionales	Hardware adicional disponible	Versiones de software compatibles	Estado del producto
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	Unidad de disco duro IDE con el CD-ROM disponible para los propó		Memoria IDS-4210-MEM-U= adicional del 256 MB para los clientes del SmartNet a actualiza	3.1 a la corriente *	Final de la venta: 8 de diciembre de 2003 el día más pasado

		sitos de la actualización del software y de la recuperación de imagen.		r solamente a la versión 4.1 y posterior. Los clientes pueden pedir la memoria a través de la Herramienta de actualización del producto (clientes registrados solamente).		**de soporte:** 8 de diciembre de 2008
IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9	Unidad de disco duro y Flash compacta IDE. No hay lector CD-ROM disponible para los propósitos de la actualización del software y de la recuperación de	IDS-4FE-INT=		4.1 a la corriente *	Actual

		image n.				
IDS-4220	IDS-4220-E	Unidad de disco duro IDE con el CD-ROM disponible para los propósitos de la actualización del software y de la recuperación de image n.		Memoria IDS-4220-MEM-U= adicional del 256 MB para los clientes del SmartNet a actualizar solamente a la versión 4.1 y posterior. Los clientes pueden pedir la memoria a través de la Herramienta de actualización del producto (clientes registrados solamente).	3.1 a 4.1	**Final de la venta:** De julio el 31 de 2002 el **día más pasado de soporte:** De julio el 31 de 2007
IDS-4230	IDS-4230-FE	Unidad de disco duro IDE con el CD-ROM disponible para los propósitos			3.1 a 4.1	**Final de la venta:** De julio el 31 de 2002 el **día más pasado de sopo**

		de la actualización del software y de la recuperación de imagen.				**rte:** De julio el 31 de 2007
IDS-4235	IDS-4235-K9	Unidad de disco duro de SCSI con el CD-ROM disponible para los propósitos de la actualización del software y de la recuperación de imagen.	IDS-4FE-INT=	Fuente de alimentación IDS-PWR= de repuesto	3.1 a la corriente *	**Final de la venta:** Mayo 31, 2005 el **día más pasado de soporte:** Mayo 31, 2010
IPS-4240	IPS-4240-K9 IPS-4240-DC-K9 (DC accionado, Compatible con las normas NEBS	Flash compacta. Ningún lector CD-ROM disponible para los propó			4.1.4 a la corriente *	Actual

	solamente)	sitos de la actualización del software y de la recuperación de imagen.				
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	Unidad de disco duro de SCSI con el CD-ROM disponible para los propósitos de la actualización del software y de la recuperación de imagen.	IDS-4FE-INT= IDS-4250-SX-INT= IDS-XL-INT=	De la fuente de alimentación unidad de disco duro IDS-PWR= de repuesto de SCSI del repuesto IDS-SCSI=	3.1 a la corriente *	**Final de la versión TX solamente de la venta:** Mayo 31, 2005 el **día más pasado de soporte para el TX:** Mayo 31, 2010 las otras dos Plataformas IDS 4250 no son afectadas por

						este anuncio EOL.
IPS-4255	IPS-4255-K9	Flash compacta. Ningún lector CD-ROM disponible para los propósitos de la actualización del software y de la recuperación de imagen.			4.1.4 a la corriente *	Actual

Cuadro 2 — Módulos

Módulo	Parte N°	Hardware	Interfaces opcionales	Hardware adicional disponible	Versiones de software compatibles	Estado del producto
SS	ASA-SSM-AIP-10-K9 (servicio de seguridad Module-10 ASA AIP) ASA-SSM-AIP-20-K9 (servicio de seguridad Module-20 ASA AIP)	Flash compacta. Ningún lector CD-ROM disponible para los propósitos de			5.0 a la corriente *	Actual

		la actualización del software y de la recuperación de imagen.				
Módulo del router	NM-CIDS-K9 NM-CIDS-K9= (pieza RMA # solamente)	Flash compacta. Ningún lector CD-ROM disponible para la actualización del software y la recuperación de imagen purpose.			Cisco IOS Software Release 12.3(4)T o Posterior IDS 4.1 del Software Release 12.2(15)ZJ o Posterior de Cisco IOS® a la corriente *	Actual
IDSM-1	WS-X6381-IDS WS-X6381-IDS= (pieza RMA # SOLAMENTE)	Unidad de disco duro IDE. Ningún unidad de CD ROM disponible para los propósitos de la			2.5 al 3.0	**Final de la venta:** De abril el 20 de 2003 el **día más pasado de sopo**

		actualización del software o de la recuperación de imagen.				**rte:** De abril el 20 de 2008
IDSM-2	WS-SVC-IDS2-BUN-K9 WS-SVC-IDS2BUNK9= (pieza RMA # solamente)	Unidad de disco duro y Flash compacta IDE. Ningún lector CD-ROM disponible para los propósitos de la actualización del software y de la recuperación de imagen.			4.0 a la corriente *	Actual

Nota: La última versión de software disponible a la hora de la publicación de este documento es 5.1. Si usted necesita una versión de software que sea más adelante de 5.1, marque la documentación para que esa versión del código asegure la compatibilidad.

Administración y opciones de configuración

Usted puede manejar y configurar los sensores IPS vía la interfaz de línea de comando, o vía una de la configuración o de las herramientas de administración enumeradas en estas secciones.

CiscoWorks Management Center para IPS Sensors (IPS MC)

El CiscoWorks Management Center para IPS Sensors es una herramienta con una arquitectura con posibilidades de ampliación para la configuración de los sensores de la red de Cisco Systems, de los sensores IPS del Switch, de los módulos de red IPS para el Routers, y del software de prevención de intromisión en línea en el Routers. El CiscoWorks Management Center para IPS Sensors permite que los administradores salven el tiempo configurando los varios sensores simultáneamente usando los perfiles del grupo. Además, proporciona una función de administración potente de la firma que aumente la exactitud y la especificidad en la detección de intrusos en la red posibles.

Refiera a los dispositivos admitidos y a las versiones de software para el centro de administración para la documentación de sensores ips para la información sobre compatibilidad.

CiscoWorks que monitorean el centro para la Seguridad (SecMon)

El CiscoWorks Monitoring Center for Security es una herramienta a capturar, a salvar, a ver, a correlacionar, y a señalar sobre los eventos de seguridad de:

- Red de Cisco IPS
- Red de Cisco IDS
- Switch Cisco IDS
- Routers del Cisco IOS con las funciones en línea IPS
- Módulos para routers del Cisco IDS
- Firewall del Cisco PIX
- Módulos de servicios del Firewall de las Cisco Catalyst 6500 Series (FWSM)
- CiscoWorks Management Center for Cisco Security Agents
- Servidores del CiscoWorks Monitoring Center for Security

Refiera a los dispositivos admitidos y a las versiones de software para monitorear el centro para la documentación de la Seguridad para la información sobre compatibilidad.

Cisco Security Monitoring, Analysis and Response System (MARTE)

El Cisco Security que monitorea el análisis y el sistema de respuesta (MARTE) es una familia de dispositivos de alto rendimiento, scalable para la Administración de la amenaza, de supervisión, y de mitigación que ayude a los clientes a hacer un uso más eficaz de la red y de los dispositivos de seguridad. El Cisco Security MARTE combina la supervisión tradicional del evento de seguridad con la inteligencia de red, la correlación de contexto, el análisis de vector, la Detección de anomalías, la identificación de punto caliente, y las capacidades de mitigación automatizadas. Con la combinación de estas capacidades, compañías de las ayudas de MARTE del Cisco Security para identificar y para eliminar exactamente los ataques a la red mientras que mantiene la conformidad de la red.

Versiones de MARTE	Dispositivo/software sensor soportados
3.3.x	3.x y 4.x
3.4.x	3.x, 4.x, 5.x

Refiera a

Respuesta de Cisco ante amenazas (CTR)

La Respuesta de Cisco ante amenazas (CTR) trabaja con los sensores del IPS de Cisco para proporcionar una solución eficiente de la protección contra intrusos. La Respuesta de Cisco ante amenazas elimina virtualmente las alarmas falsas, extiende los ataques reales, y las ayudas en la corrección de intrusiones costosas.

La Respuesta de Cisco ante amenazas es compatible con la versión 3.x o posterior del IPS de Cisco. Refiera a También, sea consciente del anuncio de fin de vida útil para la Respuesta de Cisco ante amenazas.

IDS Event Viewer (IEV)

El IDS Event Viewer (IEV) es una aplicación de la Java basada que le permite para ver y para manejar las alarmas para hasta cinco sensores. Con el usted puede conectarse del IDS Event Viewer a y las alarmas de la visión en el tiempo real o en los archivos del registro importados. Usted puede configurar los filtros y las opiniones para ayudarle a manejar las alarmas y a importar y a exportar los datos de evento para el análisis adicional. El IDS Event Viewer también proporciona el acceso a la base de datos de la seguridad de la red (NSDB) para las descripciones de la firma.

El IEV se soporta del IDS versión 3.1 a la versión 4.x. Aunque esté soportado no más de la versión 5.x, pueda ser utilizado a los sensores de la versión de Monitor 5.x. Sin embargo, las nuevas 5.0 características no son señaladas por el IEV. Refiera a

IDS Device Manager (IDM)

El IDS Device Manager (IDM) es una aplicación basada en Web que permite que usted configure y que maneje su sensor. El servidor Web para el IDS Device Manager reside en el sensor. Usted puede accederlo a través de los buscadores Web de Netscape o del Internet Explorer.

El IDM se soporta del IDS versión 3.1. Refiera a

Cisco Secure Policy Manager (CSPM)

El Cisco Secure Policy Manager (CSPM) proporciona la Administración de seguridad del policy basado para los sensores del Cisco IDS, los Firewall PIX y el Routers del IPSec VPN.

Nota: El CSPM ha alcanzado su EoL. Refiera al FOE/al anuncio EOL para el Cisco Secure Policy Manager 2.x y 3.x.

Modelo	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	2.2.0.x 2.2.1.x 2.5.(0)S0	2.2.0.x 2.2.1.x 2.5.(0)S0 2.5(1)S0	2.2.0.x 2.2.1.x 2.5.(0)S0 2.5(1)S0	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

	2.5 (0)	0 2.5(1)S0 2.5(1)S2	2.5(1)S2 3.0(1)S3 3.0(1)S4	2.5(1)S2 3.0(1)S3 3.0(1)S4	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

Director de UNIX

El UNIX Director proporciona una interfaz gráfica centralizada para la administración de seguridad a través de una red distribuida. Puede también realizar otras funciones importantes tales como Administración de datos a través de las herramientas de tercera persona, acceso al NSDB, supervisión remota y administración de sensores y los IDSM, y envía las páginas o el email al personal de seguridad cuando ocurren los eventos de seguridad. Los funcionamientos de la interfaz del director encima del HP OpenView.

Nota: El Software Release 2.2.x para el Sensor del equipo del Cisco IDS ha alcanzado su EoL. Refiera al fin de la vida útil para la documentación de software sensor del Cisco IDS 2.2.x.

Versiones director	Dispositivo/software sensor soportados
2.1.1	2.1.1
2.2.0	2.2.0
2.2.1	2.2.1
2.2.2	2.2.2 y 2.5
2.2.3*	2.2.3, 3.0, 3.1

* 2.2.3 es la versión disponible más reciente del software y del software sensor de soportes 3.1 del director IDS y anterior.

Mientras que el director 2.2.x puede ser al revés compatible con las versiones Sensores 2.2.x, si usted no tiene por lo menos la misma versión de software en ambos directores y sensores, una más nueva funcionalidad del sensor puede no estar disponible en el director. Esto fuerza un comando line configuration manual. Refiera a la Documentación del Producto para más detalles.

Información Relacionada

- Cisco Intrusion Prevention System
- Field Notice de seguridad del producto (CiscoSecure Intrusion Detection incluyendo)