Matrice di compatibilità del sistema di rilevamento intrusioni

Sommario

Introduzione

Questo documento fornisce una matrice di compatibilità hardware/software per i seguenti moduli: Cisco Intrusion Prevention System (IPS) (4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255), Adaptive Security Appliance Security Services Module (SSM), Router Module e Catalyst 6000 Intrusion Detection System Module (IDSM-1, IDSM-2). Questo documento fornisce anche una panoramica delle opzioni di gestione. Viene fornita una breve panoramica di ogni applicazione, nonché una matrice di compatibilità delle versioni. Le versioni elencate in ogni matrice di compatibilità sono le uniche versioni supportate.

Cisco Intrusion Prevention System era noto in precedenza come Cisco Intrusion Detection System (IDS) o NetRanger. Le appliance del sistema di prevenzione delle intrusioni Cisco sono note anche come sensori. Per ulteriori informazioni, consultare la documentazione del prodotto e le note di rilascio pertinenti.

Nota: tenere presente la colonna relativa allo stato del prodotto nelle tabelle di questo documento. Questa colonna indica le notifiche rilevanti di fine del ciclo di vita (EoL)/fine vendita (EoS).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Appliance Cisco Intrusion Prevention System (IPS) (4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255)
- Adaptive Security Appliance Security Services Module (SSM)
- Modulo router
- Moduli del sistema di rilevamento intrusioni Catalyst 6000 (IDSM-1, IDSM-2)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Compatibilità hardware/software IPS

Tabella 1 - Appliance

Appliance	N. parte	Hardware	Interfacce opzionali	Hardware aggiuntivo disponibile	Versioni software compatibili	Stato del prodotto
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	Disco rigido IDE con CD-ROM disponibile per l'aggiornamento del software e il ripristin		IDS-4210-MEM-U= 256 MB di memoria aggiuntiva per i clienti SmartNet solo per l'aggiornamento alla	da 3.1 a corrente *	Fine vendita: 8 dicembre 2003 Ultimo giorno di supporto: 8 dice

		o dell'immagine.		versione 4.1 e successive. I clienti possono ordinare la memoria tramite lo strumento di aggiornamento del prodotto (solo utenti registrati).		mbre 2008
IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9	disco rigido IDE e Compact Flash. Nessuna unità CD-ROM disponibile per l'aggiornamento del software e il ripristino dell'immagine.	IDS-4FE-INT=		4.1 al corrente *	Corrente
IDS-4220	IDS-4220-E	Disco rigido IDE con CD-ROM disponibile per l'aggiornament		IDS-4220-MEM-U= 256 MB di memoria aggiuntiva per i clienti SmartNe	da 3.1 a 4.1	**Fine vendita:** 31 luglio 2002 **Ultimo giorn**

		o del software e il ripristino dell'immagine.		t solo per l'aggiornamento alla versione 4.1 e successive. I clienti possono ordinare la memoria tramite lo strumento di aggiornamento del prodotto (solo utenti registrati).		o di supporto: 31 luglio 2007
IDS-4230	IDS-4230-FE	Disco rigido IDE con CD-ROM disponibile per l'aggiornamento del software e il ripristino dell'immagine.			da 3.1 a 4.1	Fine vendita: 31 luglio 2002 Ultimo giorno di supporto: 31 luglio 2007
IDS-4235	IDS-4235-K9	Disco rigido SCSI con CD-ROM disponibile per l'aggiornament	IDS-4FE-INT=	IDS-PWR= alimentatore di riserva	da 3.1 a corrente *	Fine vendita: 31 mag 2005 Ultimo giorno di

		o del software e il ripristino dell'immagine.				supporto: 31 mag 2010
IPS-4240	IPS-4240-K9 IPS-4240-DC-K9 (alimentato a corrente continua, solo conforme a NEBS)	Scheda Compact Flash Nessuna unità CD-ROM disponibile per l'aggiornamento del software e il ripristino dell'immagine.			4.1.4 al corrente *	Corrente
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	Disco rigido SCSI con CD-ROM disponibile per l'aggiornamento del software e il ripristino dell'immagine.	IDS-4FE-INT= IDS-4250-SX-INT= IDS-XL-INT=	IDS-PWR= Alimentatore di riserva IDS-SCSI= Disco rigido di riserva SCSI	da 3.1 a corrente *	Solo versione TX Fine vendita: 31 maggio 2005 Ultimo giorno di supporto per TX: 31 maggio 2010 Le

						altre due piattaforme IDS 4250 non sono interessate da questo annuncio di fine ciclo di vita.
IPS-4255	IPS-4255-K9	Scheda Compact Flash Nessuna unità CD-ROM disponibile per l'aggiornamento del software e il ripristino dell'immagine.			4.1.4 al corrente *	Corrente

Tabella 2 - Moduli

Modulo	N. parte	Hardware	Interfacce opzionali	Hardware aggiuntivo disponibile	Versioni software compatibili	Stato del prodotto
SS	ASA-SSM-	Scheda			5.0 al	Corre

M	AIP-10-K9 (ASA AIP Security Service Module-10) ASA-SSM-AIP-20-K9 (ASA AIP Security Service Module-20)	Compact Flash Nessuna unità CD-ROM disponibile per l'aggiornamento del software e il ripristino dell'immagine.			corrente *	nte
Modulo router	NM-CIDS-K9 NM-CIDS-K9= (solo numero parte RMA)	Scheda Compact Flash Nessuna unità CD-ROM disponibile per l'aggiornamento del software e il ripristino dell'immagine.			Software Cisco IOS® versione 12.2(15)ZJ o successive Software Cisco IOS versione 12.3(4)T o successive IDS 4.1 fino alla versione attuale *	Corrente
IDSM-1	WS-X6381-IDS WS-X6381-IDS= (SOLO N. parte RMA)	disco rigido IDE. Nessuna unità CD-ROM			da 2,5 a 3,0	Fine vendita: 20 aprile 2003 Ultimo giorno

		disponibile per l'aggiornamento del software o il ripristino dell'immagine.				di supporto: 20 aprile 2008
IDSM-2	WS-SVC-IDS2-BUN-K9 WS-SVC-IDS2BUNK9= (solo parte RMA n.)	disco rigido IDE e Compact Flash. Nessuna unità CD-ROM disponibile per l'aggiornamento del software e il ripristino dell'immagine.			4.0 al corrente *	Corrente

Nota: L'ultima versione del software disponibile al momento della pubblicazione del presente documento è la 5.1. Se è necessaria una versione del software successiva alla 5.1, consultare la documentazione della versione del codice per verificare la compatibilità.

Opzioni di gestione e configurazione

Èpossibile gestire e configurare i sensori IPS tramite l'interfaccia della riga di comando o uno degli strumenti di configurazione o gestione elencati in queste sezioni.

CiscoWorks Management Center per sensori IPS (IPS MC)

CiscoWorks Management Center per i sensori IPS è uno strumento con un'architettura scalabile per la configurazione dei sensori di rete Cisco Systems, dei sensori IPS di switch, dei moduli di rete IPS per router e del software di prevenzione delle intrusioni nei router. CiscoWorks Management Center per i sensori IPS consente agli amministratori di risparmiare tempo configurando più sensori contemporaneamente utilizzando i profili di gruppo. Offre inoltre una potente funzione di gestione delle firme che aumenta l'accuratezza e la specificità nel rilevamento di possibili intrusioni nella rete.

Per informazioni sulla compatibilità, consultare la documentazione relativa ai dispositivi supportati e alle versioni software per i sensori IPS di Management Center.

CiscoWorks Monitoring Center for Security (SecMon)

CiscoWorks Monitoring Center for Security è uno strumento per l'acquisizione, l'archiviazione, la visualizzazione, la correlazione e la creazione di report sugli eventi relativi alla sicurezza da:

- Cisco Network IPS
- Cisco Network IDS
- Cisco Switch IDS
- Router Cisco IOS con funzioni IPS inline
- Moduli Cisco IDS per router
- Cisco PIX firewall
- Cisco Catalyst serie 6500 Firewall Services Module (FWSM)
- CiscoWorks Management Center per gli agenti di sicurezza Cisco
- CiscoWorks Monitoring Center per server di sicurezza

Per informazioni sulla compatibilità, consultare la documentazione relativa ai dispositivi supportati e alle versioni software per il Monitoring Center for Security.

Cisco Security Monitoring, Analysis and Response System (MARS)

Cisco Security Monitoring Analysis and Response System (MARS) è una famiglia di appliance scalabili e ad alte prestazioni per la gestione, il monitoraggio e la mitigazione delle minacce che aiuta i clienti a utilizzare in modo più efficiente i dispositivi di rete e di sicurezza. Cisco Security MARS combina il monitoraggio degli eventi di sicurezza tradizionale con le funzionalità di intelligence di rete, correlazione di contesto, analisi vettoriale, rilevamento delle anomalie, identificazione degli hotspot e funzionalità di mitigazione automatizzate. Grazie alla combinazione di queste funzionalità, Cisco Security MARS consente alle aziende di identificare ed eliminare accuratamente gli attacchi alla rete, mantenendo al contempo la conformità alla rete.

Versioni MARS	Software di accessorio/sensore supportato
3.3.x	3.x e 4.x
3.4 x	3,x, 4,x, 5,x

Fare riferimento alle note sulla versione del prodotto per ulteriori informazioni.

Cisco Threat Response (CTR)

Cisco Threat Response (CTR) funziona con i sensori Cisco IPS per fornire una soluzione efficiente per la protezione dalle intrusioni. Cisco Threat Response consente di eliminare virtualmente i falsi allarmi, intensificare gli attacchi e contribuire a correggere costose intrusioni.

Cisco Threat Response è compatibile con Cisco IPS versione 3.x o successive. Fare riferimento alle note sulla versione del prodotto per ulteriori informazioni. Presta attenzione anche all'annuncio di fine del ciclo di vita per Cisco Threat Response.

Visualizzatore eventi IDS (IEV)

IDS Event Viewer (IEV) è un'applicazione basata su Java che consente di visualizzare e gestire gli allarmi per un massimo di cinque sensori. Con il Visualizzatore eventi IDS è possibile connettersi e visualizzare gli allarmi in tempo reale o nei file di registro importati. È possibile configurare filtri e visualizzazioni per gestire gli allarmi e importare ed esportare i dati degli eventi per ulteriori analisi. Il Visualizzatore eventi IDS consente inoltre di accedere al database di sicurezza di rete (NSDB, Network Security Database) per le descrizioni delle firme.

IEV è supportato dalla versione IDS 3.1 alla versione 4.x. Sebbene non più supportato dalla versione 5.x, può essere utilizzato per monitorare la versione 5.x dei sensori. Tuttavia, le nuove funzionalità della versione 5.0 non sono riportate da IEV. Fare riferimento agli esempi di configurazione del prodotto e alle note tecniche per ulteriori informazioni.

IDS Device Manager (IDM)

IDS Device Manager (IDM) è un'applicazione basata sul Web che consente di configurare e gestire il sensore. Il server Web per IDS Device Manager risiede sul sensore. È possibile accedervi tramite Netscape o Internet Explorer.

IDM è supportato da IDS versione 3.1. Per ulteriori informazioni, fare riferimento agli esempi di configurazione del prodotto e alle note tecniche.

Cisco Secure Policy Manager (CSPM)

Cisco Secure Policy Manager (CSPM) fornisce una gestione della sicurezza basata su policy per i sensori Cisco IDS, i firewall PIX e i router VPN IPsec.

Nota: CSPM ha raggiunto il proprio EoL. Fare riferimento all'annuncio EoS/EoL per Cisco Secure Policy Manager 2.x e 3.x.

Modello	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	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

(IDSM-1)					

UNIX Director

UNIX Director fornisce un'interfaccia grafica centralizzata per la gestione della sicurezza in una rete distribuita. Può inoltre svolgere altre importanti funzioni, come la gestione dei dati tramite strumenti di terze parti, l'accesso al NSDB, il monitoraggio e la gestione remota di Sensori e IDSM, e inviare pagine o e-mail al personale di sicurezza quando si verificano eventi di sicurezza. L'interfaccia Director viene eseguita su HP OpenView.

Nota: il software versione 2.2.x per il sensore dell'accessorio Cisco IDS ha raggiunto il proprio EoL. Fare riferimento alla documentazione del software sensore Cisco IDS 2.2.x alla fine del ciclo di vita.

Versioni Director	Software di accessorio/sensore supportato
2.1.1	2.1.1
2.2.0	2.2.0
2.2.1	2.2.1
2.2.2	2.2.2 e 2.5
2.2.3*	2.2.3, 3.0, 3.1

* La versione 2.2.3 è l'ultima versione disponibile del software IDS Director e supporta il software sensore 3.1 e versioni precedenti.

Sebbene Director 2.2.x possa essere compatibile con le versioni precedenti dei sensori 2.2.x, se non si dispone almeno della stessa versione del software sia su Director che su Sensori, le nuove funzionalità dei sensori potrebbero non essere disponibili in Director. In questo modo viene forzata una configurazione manuale della riga di comando. Fare riferimento alla documentazione del prodotto per ulteriori dettagli.

Informazioni correlate

- Cisco Intrusion Prevention System
- Avvisi sui prodotti per la sicurezza (incluso Cisco Secure Intrusion Detection)