Compatibiliteitsmatrix voor inbraakdetectiesysteem

Inhoud

Inleiding

Dit document biedt een hardware/software-compatibiliteitsmatrix voor Cisco IPS-applicaties (4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255) adaptieve security servicesmodule (SSM)), routermodule en Catalyst 6000 modules voor inbraakdetectiesysteem (IDSM-1, IDSM-2). Dit document geeft ook een overzicht van de beheeropties. Er wordt een kort overzicht van elke toepassing gegeven, evenals een matrixprinter voor de compatibiliteit van de versie. De versies in elke compatibiliteitsmatrix zijn de enige ondersteunde versies.

Het Cisco-inbraakpreventiesysteem was voorheen bekend als Cisco Inbraakdetectiesysteem (IDS) of NetRanger. De applicaties van Cisco voor inbraakpreventiesysteem zijn ook bekend als sensoren. Raadpleeg de relevante productdocumentatie en releaseopmerkingen voor meer informatie.

N.B.: Let op de kolom productstatus in de tabellen in dit document. In deze kolom worden de relevante meldingen end-of-life (EoL)/end-of-sale (EoS) aangegeven.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IPS-applicaties (4210, 4215, 4220, 4230, 4235, 4240, 4250, 42555)
- Adaptieve security applicatie security servicesmodule (SSM)
- Routermodule
- Catalyst 6000 modules voor inbraakdetectiesysteem (IDSM-1, IDSM-2)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

IPS hardware/software-compatibiliteit

Tabel 1-applicaties

Applicatie	Onderdeel nr.	Hardware	Optionele interfaces	Beschikbare extra hardware	Compatibele softwareversies	Productstatus
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	IDE harde schijf met CD-ROM beschikbaar voor software-upgrade en beeldherstel.		IDS-4210-MEM-U= Aanvullende 256 MB geheugen voor SmartNet-klanten alleen voor upgrade naar versie 4.1 en hoger. Klanten	3.1. huidige *	End-of-sale: 8 december 2003 Laatste dag van ondersteuning: 8 december 2008

				kunnen het geheugen bestellen via het product upgrade-programma (alleen geregistreerde klanten).		
IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9	IDE harde schijf en compacte Flitser. Er is geen CD-ROM-station beschikbaar voor software-upgrades en beeldherstel.	IDS-4FE-INT=		4.1. huidige *	huidig
IDS-4220	IDS-4220-E switch	IDE harde schijf met CD-ROM beschikbaar voor software-upgrade en beeldh		IDS-4220-MEM-U= Aanvullende 256 MB geheugen voor SmartNet-klanten alleen voor	3,1 t/m 4,1	**End-of-sale:** 31 juli 2002 **Laatste dag van ondersteuning:** 31

		erstel.		upgrade naar versie 4.1 en hoger. Klanten kunnen het geheugen bestellen via het product upgrade-programma (alleen geregistreerde klanten).		juli 2007
IDS-4230	IDS-4230-FE	IDE harde schijf met CD-ROM beschikbaar voor software-upgrade en beeldherstel.			3,1 t/m 4,1	**End-of-sale:** 31 juli 2002 **Laatste dag van ondersteuning:** 31 juli 2007
IDS-4235	IDS-4235-K9	SCSI-harde schijf met CD-ROM beschikbaar voor doeleinden van softwar	IDS-4FE-INT=	IDS-PWR= Stroomtoevoer	3.1. huidige *	**End-of-sale:** 31 mei 2005 **Laatste dag van ondersteuning:**

		eupgrade en beeldherstel.				31 mei 2010
IPS-4240 sensor	IPS-4240-K9 IPS-4240-DC-K9 (DC-voeding, alleen NEBS-conform)	Compacte flitser. Er is geen CD-ROM-station beschikbaar voor software-upgrades en beeldherstel.			4.1.4. huidige *	huidig
IDS-4250-software	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	SCSI-harde schijf met CD-ROM beschikbaar voor doeleinden van softwareupgrade en beeldherstel.	IDS-4FE-INT= IDS-4250-SX-INT= IDS-XL-INT= IDS-X-INT	IDS-PWR= reserve-voeding IDS-SCSI= reserve-SCSI harde schijf	3.1. huidige *	**Alleen TX-versie van End-of-sale:** 31 mei 2005 Laatste dag **van steun voor TX:** 31 mei 2010 De andere twee IDS 4250-platforms worden

						niet beïnvloed door deze aankondiging van de EoL.
IPS-4255 switch	IPS-4255-K9 switch	Compacte flitser. Er is geen CD-ROM-station beschikbaar voor software-upgrades en beeldherstel.			4.1.4. huidige *	huidig

Tabel 2—modules

Module	Onderdeel nr.	Hardware	Optionele interfaces	Beschikbare extra hardware	Compatibele softwareversies	Productstatus
SSM	ASA 5500-X-AIP-10-K9 (ASA security servicemodule-10) ASA-SM-AIP-20-K9 (ASA AIP security servicemodule-20)	Compacte flitser. Er is geen CD-ROM-station beschikbaar voor software-upgrades en			5,0 op huidige *	huidig

		beeldherstel.				
Routermodule	NM-CIDS-K9 NM-CIDS-K9= (RMA Onderdeel # alleen)	Compacte flitser. Er is geen CD-ROM-station beschikbaar voor software-upgrade en herstel van afbeeldingen.			Cisco IOS® software release 12.2(15) ZJ of later Cisco IOS-software release 12.3(4)T of later IDS 4.1 naar huidige *	huidig
IDSM-1	WS-X6381-IDS WS-X6381-IDS= (ALLEEN RMA-ONDERDEEL)	IDE harde schijf. Er is geen CD-ROM-station beschikbaar voor software-upgrades of beeldherstel.			2,5 t/m 3,0	End-of-sale: 20 april 2003 Laatste dag van ondersteuning: 20 april 2008
IDSM-2	WS-SVC-IDS2-BUN-K9 WS-SVC-IDS2BUNK9= (RMA-onderdeel nr. alleen)	IDE harde schijf en compacte Flitser. Er is geen CD-ROM-station beschikbaar voor			4.0. huidige *	huidig

		softwar e-upgrad es en beeldhe rstel.				

Opmerking: De meest recente versie van de software die op het tijdstip van de publicatie van dit document beschikbaar is, is 5.1. Als u een softwareversie nodig hebt die later is dan 5.1, controleer dan de documentatie voor die versie van de code om de compatibiliteit te waarborgen.

Opties voor beheer en configuratie

U kunt IPS-sensoren beheren en configureren via de interface van de opdrachtregel of via een van de configuratie- of beheertools die in deze secties worden genoemd.

CiscoWorks Management Center voor IPS-sensoren (IPS MC)

CiscoWorks Management Center voor IPS Sensors is een tool met een schaalbare architectuur voor de configuratie van Cisco Systems Network Sensors, switch IPS Sensors, IPS-netwerkmodules voor routers en inline inbraakpreventiesoftware in routers. CiscoWorks Management Center voor IPS Sensors stelt beheerders in staat tijd te besparen door meerdere sensoren tegelijk te configureren met gebruik van groepsprofielen. Daarnaast biedt het een krachtige functie voor het beheer van handtekeningen die de nauwkeurigheid en specificiteit bij de detectie van mogelijke netwerkstoringen vergroot.

Raadpleeg de Ondersteunde apparaten en softwareversies voor Management Center voor IPS Sensors documentatie voor compacte informatie.

CiscoWorks Monitoring Center for Security (SEC)

CiscoWorks Monitoring Center for Security is een tool voor het opnemen, opslaan, weergeven, correleren en rapporteren over beveiligingsgebeurtenissen van:

- Cisco-netwerkIPS
- Cisco-netwerkIDS
- Cisco Switch IDS
- Cisco IOS-routers met inline IPS-functies
- Cisco IDS-modules voor routers
- Cisco PIX-firewalls
- Cisco Catalyst 6500 Series firewallservicesmodules (FWSM)
- CiscoWorks Management Center voor Cisco security agenten
- CiscoWorks Monitoring Center voor security servers

Raadpleeg de Ondersteunde apparaten en softwareversies voor de documentatie van het Monitoring Center for Security voor informatie over de compatibiliteit.

Cisco-systeem voor beveiligingsbewaking, analyse en respons (MARS)

Het Cisco Security Monitoring Analysis and Response System (MARS) is een reeks

hoogwaardige, schaalbare apparaten voor bedreigingsbeheer, bewaking en beperking die klanten helpen om effectiever gebruik te maken van netwerk- en beveiligingsapparaten. Cisco Security MARS combineert traditionele security gebeurtenissen met controle van netwerkintelligentie, contextcorrelatie, vectoranalyse, anomalie-detectie, hotspot-identificatie en geautomatiseerde limietmogelijkheden. Met de combinatie van deze mogelijkheden, helpt Cisco Security MARS bedrijven om netwerkaanvallen nauwkeurig te identificeren en te elimineren met behoud van netwerkconformiteit.

MARS-versies	Ondersteunde software voor applicatie/sensor
3,3,x	3,x en 4,x
3,4,x	3.x, 4.x, 5.x

Raadpleeg de opmerkingen bij de productrelease voor meer informatie.

Cisco Threat Response (CTR)

Cisco Threat Response (CTR) werkt met Cisco IPS Sensoren om een efficiënte inbraakbeschermingsoplossing te bieden. Cisco Threat Response heft valse alarm af, escaleert echte aanvallen en hulp bij het herstellen van kostbare inbreuken.

Cisco Threat Response is compatibel met Cisco IPS versie 3.x of hoger. Raadpleeg de opmerkingen bij de productrelease voor meer informatie. Let ook op de mededeling End-of-life voor Cisco Threat Response.

IDS Event Viewer (IEV)

IDS Event Viewer (IEV) is een op Java gebaseerde toepassing die u in staat stelt alarmen te bekijken en te beheren voor maximaal vijf sensoren. In het DIS Event Viewer kunt u in real-time of in geïmporteerde logbestanden verbinding maken met en alarmen weergeven. U kunt filters en meningen configureren om u te helpen de alarmen te beheren en gebeurtenissen gegevens in te voeren en te exporteren voor verdere analyse. IDS Event Viewer biedt ook toegang tot de Network Security Database (NSDB) voor kenmerkende beschrijvingen.

IEV wordt ondersteund door IDS versie 3.1 naar versie 4.x. Hoewel niet langer ondersteund worden door versie 5.x, kan deze gebruikt worden om versie 5.x-sensoren te controleren. De nieuwe 5.0 kenmerken worden echter niet door IEV gerapporteerd. Raadpleeg de voorbeelden van productconfiguratie en de technische opmerkingen voor meer informatie.

IDS-apparaatbeheer (IDM)

IDS Devices Manager (IDM) is een op internet gebaseerde toepassing waarmee u uw sensor kunt configureren en beheren. De webserver voor IDS Devices Manager bevindt zich op de sensor. U kunt de breedbeeldmodus benaderen via webbrowsers van Netscape of Internet Explorer.

IDM wordt ondersteund door IDS versie 3.1. Raadpleeg de voorbeelden van productconfiguratie en TechNotes voor meer informatie.

Cisco Secure Policy Manager (CSPM)

Cisco Secure Policy Manager (CSPM) biedt op beleid gebaseerd beveiligingsbeheer voor Cisco IDS-sensoren, PIX-firewalls en IPsec VPN-routers.

Opmerking: CSPM heeft zijn EoL bereikt. Raadpleeg de bekendmaking EoS/EoL voor Cisco Secure Policy Manager 2.x en 3.x.

Model	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

UNIX-directeur

De UNIX-directeur biedt een gecentraliseerde grafische interface voor het beheer van de beveiliging in een gedistribueerd netwerk. Het kan ook andere belangrijke functies uitvoeren, zoals gegevensbeheer door middel van hulpmiddelen van derden, toegang tot de NSDB, controle op afstand en beheer van sensoren en IDSM's, en pagina's of e-mail naar het beveiligingspersoneel versturen wanneer zich beveiligingsgebeurtenissen voordoen. De Director interface loopt boven HP OpenView.

Opmerking: softwarerelease 2.2.x voor Cisco IDS-applicatie Sensor heeft zijn EoL bereikt. Raadpleeg het Einde van de levensduur van Cisco IDS 2.2.x Sensor-softwaredocumentatie.

Director-versies	Ondersteunde software voor applicatie/sensor
2.1.1	2.1.1
2.2.0	2.2.0
2.2.1	2.2.1
2.2.2	2.2.2 en 2.5
2,2,3*	2.2.3, 3.0, 3.1

* 2.2.3 is de laatste beschikbare versie van IDS Director-software en ondersteunt Sensor Software 3.1 en hoger.

Terwijl de 2.2.x Director mogelijk retrospectief compatibel is met 2.2.x Sensor-versies, en als u niet ten minste dezelfde versie van software hebt op zowel directeuren als sensoren, is er mogelijk geen nieuwere Sensor-functionaliteit beschikbaar in de Director. Dit dwingt een handmatige configuratie van de opdrachtregel. Raadpleeg de productdocumentatie voor meer informatie.

Gerelateerde informatie

- Cisco-inbraakpreventiesysteem
- Security meldingen uit het veld (inclusief Cisco Secure Inbraakdetectie)