Содержание

Введение

Этот документ предоставляет матрицу программной и аппаратной совместимости для системы предотвращения вторжений Cisco (IPS) (IPS) Устройства (4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255), модуль служб безопасности (SSM) Устройства адаптивной безопасности, Модуль маршрутизатора и модули Catalyst 6000 Системы обнаружения проникновения (IDSM-1, IDSM-2). Этот документ также предоставляет обзор Параметров управления. Краткий обзор каждого приложения предоставлен, а также матрица совместимости версий. Версии, перечисленные в каждой матрице совместимости, являются единственными поддерживаемыми версиями.

Система предотвращения вторжений Cisco (IPS) была раньше известна как Cisco Intrusion Detection System (IDS) или NetRanger. Устройства системы предотвращения вторжений Cisco (IPS) также известны как Датчики. См. документацию соответствующего продукта и Комментарии к выпуску для получения дополнительной информации.

Примечание: Знайте о столбце состояния продукта в таблицах в этом документе. Этот столбец обозначает соответствующую поддержку закончена (EoL)/End-of-Sale (EoS) уведомления.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Система предотвращения вторжений Cisco (IPS) (IPS) устройства (4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255)
- Модуль служб безопасности (SSM) устройства адаптивной безопасности
- Модуль маршрутизатора
- Модули Catalyst 6000 системы обнаружения проникновения (IDSM-1, IDSM-2)

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Программная и аппаратная совместимость IPS

Таблица 1? Устройства

Устройство	Часть #	Аппаратные средства	Дополнительные интерфейсы	Доступные дополнительные аппаратные средства	Совместимые версии программного обеспечения	Состояние продукта
IDS 4210	IDS-4210, IDS-4210-K9, IDS-4210-NFR	Жесткий диск с интерфейсом IDE с CDROM, доступным для обновления програ		IDS-4210-MEM-U = Дополнительная память на 256 МБ для клиентов SmartNet только для обновле	3.1 к току *	Конец продажи: 8 декабря 2003 В последний день

		ммного обеспечения и целей восстановления образа.		ния к версии 4.1 и позже. Клиенты могут упорядочить память через Средство обновления продукта (только зарегистрированные клиенты).		**поддержки:** 8 декабря 2008
IDS-4215	IDS-4215-K9, IDS-4215-4FE-K9	Жесткий диск с интерфейсом IDE и стандарт Compact Flash. Никакой дисковод для компакт-дисков не доступен для целей восстановления образа и обновления програ	IDS-4FE-INT =		4.1 к току *	Текущий

		ммного обеспечения.				
IDS 4220	IDS-4220-E	Жесткий диск с интерфейсом IDE с CDROM, доступным для обновления программного обеспечения и целей восстановления образа.		IDS-4220-MEM-U = Дополнительная память на 256 МБ для клиентов SmartNet только для обновления к версии 4.1 и позже. Клиенты могут упорядочить память через Средство обновления продукта (только зарегистрированные клиенты).	3.1 к 4.1	**Конец продажи:** 31 июля 2002 **Последний день поддержки:** 31 июля 2007
IDS 4230	IDS-4230-FE	Жесткий диск с интерфейсом IDE с CDROM, доступным			3.1 к 4.1	**Конец продажи:** 31 июля 2002 **Пос**

		для обновления программного обеспечения и целей восстановления образа.				**последний день поддержки:** 31 июля 2007
IDS 4235	IDS-4235-K9	Жесткий диск SCSI с CDROM, доступным для обновления программного обеспечения и целей восстановления образа.	IDS-4FE-INT =	PWR IDS = Запасной источник питания	3.1 к току *	**Конец продажи:** 31 мая 2005 **В последний день поддержки:** 31 мая 2010
IPS 4240	IPS-4240-K9 IPS-4240-DC-K9 (DC, приведенный в действие, соответствующий	Стандарт Compact Flash. Никакой дисковод для компакт-дисков, доступ			4.1.4 к току *	Текущий

	NEBS только)	ный для обновления программного обеспечения и целей восстановления образа.				
IDS 4250	IDS-4250-TX-K9, IDS-4250-SX-K9, IDS-4250-XL-K9	Жесткий диск SCSI с CDROM, доступным для обновления программного обеспечения и целей восстановления образа.	IDS-4FE-INT = IDS-4250-SX-INT = IDS-XL-INT =	PWR IDS = Запасной SCSI IDS источника питания = Запасной Жесткий диск SCSI	3.1 к току *	**Версия TX только Конец Продажи:** 31 мая 2005 **В последний день поддержки TX:** 31 мая 2010 На другие два IDS 4250 платформ

						не влияет это извещение EoL.
IPS 4255	IPS-4255-K9	Стандарт Compact Flash. Никакой дисковод для компакт-дисков, доступный для обновления программного обеспечения и целей восстановления образа.			4.1.4 к току *	Текущий

Таблица 2? Модули

Модуль	Часть #	Аппаратные средства	Дополнительные интерфейсы	Доступные дополнительные аппаратные средства	Совместимые версии программного обеспечения	Состояние продукта

SSM	ASA-SSM-AIP-10-K9 (модуль 10 сервиса безопасности AIP ASA) ASA-SSM-AIP-20-K9 (модуль 20 сервиса безопасности AIP ASA)	Стандарт Compact Flash. Никакой дисковод для компакт-дисков, доступный для обновления программного обеспечения и целей восстановления образа.			5.0 к току *	Текущий
Модуль маршрутизатора	NM-CIDS-K9 NM-CIDS-K9= (Часть RMA # только)	Стандарт Compact Flash. Никакой дисковод для компакт-дисков, доступный для обновления программ			Релиз 12.2 Программного обеспечения Cisco IOS (15) ZJ или более позднее программное	Текущий

		ого обеспечения и целивосстановления образа.			обеспечение Cisco IOS версии 12.3(4)T или более поздний IDS 4.1 к току *	
IDSM-1	WS-X6381-IDS WS-X6381-IDS = (часть RMA # ONLY)	Жесткий диск с интерфейсом IDE. Никакой CD-ROM-привод, доступный для обновления программного обеспечения или целей восстановления образа.			2.5 к 3.0	**Конец продажи:** 20 апреля 2003 **В последний день поддержки:** 20 апреля 2008
IDSM-2	WS-SVC-IDS2-BUN-K9 WS-	Жесткий диск с интерфейс			4.0 к току *	Текущий

	SVC-IDS2BUNK9 = (Часть RMA # только)	ом IDE и стандарт Compact Flash. Никакой дисковод для компакт-дисков, доступный для обновления программного обеспечения и целей восстановления образа.				

Примечание: Последняя версия программного обеспечения, доступного во время публикации этого документа, 5.1. Если вам нужна версия программного обеспечения, которая является позже, чем 5.1, проверьте документацию для той версии кода для обеспечения совместимости.

Менеджмент и параметры настройки

Можно управлять и настроить Сенсоры IPS через интерфейс командной строки, или через одну из конфигурации или средств управления, перечисленных в этих разделах.

Центр управления сенсорами IPS для CiscoWorks (MC IPS)

Центр управления сенсорами IPS для CiscoWorks является программным средством с масштабируемой архитектурой для конфигурации Сетевых датчиков Cisco Systems, Сенсоров IPS коммутатора, сетевых модулей IPS для маршрутизаторов и программного обеспечения предотвращения внутреннего проникновения в маршрутизаторах. Центр управления сенсорами IPS для CiscoWorks позволяет администраторам экономить время

путем настройки несколько сенсоров одновременно использования профилей группы. Кроме того, это предоставляет мощную функцию управления подписи, которая увеличивает точность и специфику в обнаружении возможных несанкционированных доступов в сеть.

См. Поддерживаемые устройства и Версии программного обеспечения для документации Центра управления сенсорами IPS для Информации о совместимости.

Центр мониторинга ИБ для CiscoWorks (SecMon)

Центр мониторинга ИБ для CiscoWorks является программным средством, чтобы перехватить, сохранить, просмотреть, коррелировать, и сообщить относительно событий связанное с безопасностью от:

- IPS сети Cisco
- IDS сети Cisco
- IDS коммутатора Cisco
- Маршрутизаторы Cisco IOS со встроенными функциями IPS
- Модули для маршрутизаторов Cisco IDS
- Межсетевые экраны Cisco PIX
- Сервисные модули межсетевого экрана Cisco Catalyst серии 6500 (FWSM)
- CiscoWorks Management Center for Cisco Security Agents
- Серверы Центра мониторинга ИБ для CiscoWorks

См. Поддерживаемые устройства и Версии программного обеспечения для документации Центра мониторинга ИБ для Информации о совместимости.

Система Cisco Security Monitoring, Analysis and Response System (MARS)

Cisco Security, Контролирующий Анализ и Систему ответа (MARS), является семейством высокоэффективных, масштабируемых устройств для управления угрозами, мониторинга и смягчения, которое помогает клиентам делать более эффективное использование сети и устройств безопасности. Cisco Security MARS комбинирует традиционное событие связанное с безопасностью, контролирующее с сетевой логикой, контекстной корреляцией, векторным анализом, обнаружением отклонения, идентификацией пункта подключения к беспроводной сети и автоматизированными Возможностями ослабления. С комбинацией этих возможностей Cisco Security MARS помогает компаниям точно определять и устранять сетевые атаки при поддержании сетевого соответствия.

Версии MARS	Поддерживаемое программное обеспечение Устройства/Датчика
3.3. x	3.x и 4. x
3.4. x	3.x, 4.x, 5. x

См. Комментарии к выпуску продукта для получения дополнительной информации.

Решения Cisco для защиты от угроз (CTR)

Решения Cisco для защиты от угроз (CTR) работают с датчиками Cisco IPS для предоставления эффективного решения для защиты от проникновения. Решения Cisco для защиты от угроз фактически устраняют ошибочные сигналы тревоги, передают реальные

атаки и способствуют ликвидации последствий вторжений с серьезными материальными последствиями.

Решения Cisco для защиты от угроз совместимы с версией 3.x Cisco IPS или позже. См. Комментарии к выпуску продукта для получения дополнительной информации. Кроме того, знать об Уведомлении об окончании срока службы для решений Cisco для защиты от угроз.

IDS Event Viewer (IEV)

IDS Event Viewer (IEV) на основе Java приложение, которое позволяет вам просмотреть и управлять сигналами тревоги максимум для пяти Датчиков. С помощью IDS Event Viewer осуществляется просмотр событий в режиме реального времени или в импортированных файлах журналов. Можно настроить фильтры и представления, чтобы помочь вам управлять сигналами тревоги и импортом и экспортировать данные события для дальнейшего анализа. Через IDS Event Viewer организован доступ к базе данных сетевой безопасности (NSDB), в которой хранятся описания цифровых подписей.

IEV поддерживается от Версии IDS 3.1 до версии 4. x . Несмотря на то, что больше не поддерживаемый от версии 5.x, это может использоваться к Датчикам версии монитора 5.x. Однако о новых 5.0 функциях не сообщает IEV. См. Примеры конфигурации продукта и Технические примечания для получения дополнительной информации.

IDS Device Manager (IDM)

IDS Device Manager (IDM) является приложением на основе технологии WWW, которое позволяет вам настраивать и управлять своим Датчиком. Веб-сервер для IDS Device Manager обеспечивается датчиком. Можно обратиться к нему через web-браузеры Netscape или Internet Explorer.

IDM поддерживается от Версии IDS 3.1. См. Примеры конфигурации продукта и технические примечания для получения дополнительной информации.

Cisco Secure Policy Manager (CSPM)

Cisco Secure Policy Manager (CSPM) предоставляет на основе политики управление системой безопасности для Датчиков Cisco IDS, межсетевых экранов PIX и маршрутизаторов IPSec VPN.

Примечание: CSPM достиг своего EoL. См. EOS/ИЗВЕЩЕНИЕ EOL для Cisco Secure Policy Manager 2.x и 3. x .

Модель	CSPM 2.2	CSPM 2.3i	CSPM 2.3.1i	CSPM 2.3.2i	CSPM 2.3.3i

UNIX Director

UNIX Director предоставляет централизованный графический интерфейс для управления безопасностью через распределенную сеть. Когда события связанное с безопасностью происходят, это может также выполнить другие важные функции, такие как управление данными через сторонние программные средства, доступ к NSDB, удаленному мониторингу и управлению датчиками и IDSM, и передать страницы или электронную почту персоналу

службы безопасности. Интерфейс Управляющего узла выполняется поверх HP OpenView.

Примечание: Выпуск ПО 2.2.x для Датчика устройства Cisco IDS достиг своего EoL. См. Окончание срока службы для Cisco IDS 2.2.x Документация к программному обеспечению Датчика.

Версии Director	Поддерживаемое программное обеспечение Устройства/Датчика
2.1.1	2.1.1
2.2.0	2.2.0
2.2.1	2.2.1
2.2.2	2.2.2 и 2.5
2.2.3*	2.2.3, 3.0, 3.1

* 2.2.3 последняя доступная версия программного обеспечения IDS Director и поддерживает программное обеспечение Датчика 3.1 и ранее.

В то время как 2.2.x Управляющий узел может быть назад совместим с 2.2.x Версии датчика, если у вас нет, по крайней мере, той же версии ПО и на Управляющих узлах и на Датчиках, более новая Функция sensor может не быть доступной в Управляющем узле. Это вызывает ручную конфигурацию командной строки. См. Документацию по продукту для получения дополнительной информации.

Дополнительные сведения

- Cisco Intrusion Prevention System
- Уведомления о дефекте для специалистов по продуктам безопасности (включая обнаружение несанкционированного доступа CiscoSecure)
- Cisco Systems – техническая поддержка и документация