Информационный бюллетень

Cisco Firepower Management Center

Решение Cisco Firepower™ Management Center повышает эффективность ваших решений сетевой безопасности Cisco® благодаря централизованному, интегрированному и оптимизированному управлению.

Обзор продукта

Решение Cisco Firepower Management Center (ранее решение называлось FireSIGHT Management Center) — это административный центр для целого ряда продуктов безопасности Cisco, выполняемых на самых разных платформах. Решение обеспечивает полное, унифицированное управление межсетевыми экранами, контролем приложениями, предотвращением вторжений, фильтрацией URL-адресов и защитой от усовершенствованного вредоносного ПО. Центр управления — это центральная точка для управления событиями и политиками следующих решений:

- межсетевой экран нового поколения Cisco Firepower Next-Generation Firewall (NGFW);
- Cisco ASA с сервисами FirePOWER;
- Cisco Firepower Next-Generation IPS (NGIPS)
- Cisco FirePOWER Threat Defense for ISR
- Cisco Advanced Malware Protection (AMP)

Решение Cisco Firepower Management Center позволяет получить подробную аналитическую информацию о пользователях, приложениях, устройствах, угрозах и уязвимостях, существующих в вашей сети. Это решение использует эту информацию для анализа уязвимостей вашей сети, а затем предоставляет адаптированные рекомендации о том, какие политики безопасности следует внедрить, а какие события безопасности изучить и расследовать.

Центр управления предоставляет удобные в использовании экраны политик для контроля доступа и защиты от известных атак. Решение интегрируется с защитой от усовершенствованного вредоносного ПО и «песочницей», а также предоставляет инструменты для отслеживания инфицированного вредоносного ПО по всей вашей сети. Все эти возможности объединены в одном интерфейсе управления. Вы легко и просто можете переходить от управления межсетевым экраном к управлению приложениями или расследованию и устранению вторжений со стороны вредоносного ПО.

Рисунок 1. Централизованное управление политиками, событиями и устройствами

© Корпорация Cisco и/или ее дочерние компании, 2017. Все права защищены. В данном документе содержится общедоступная информация Cisco.

Управление корпоративного класса

Cisco Firepower Management Center получает оперативную информацию обо всех изменениях сетевых ресурсов и операций и предоставляет полную контекстную базу для принятия обоснованных решений (см. рис. 1). Помимо предоставления широкого набора аналитических решений, Firepower Management Center обеспечивает высокий уровень детализации, в том числе следующие данные:

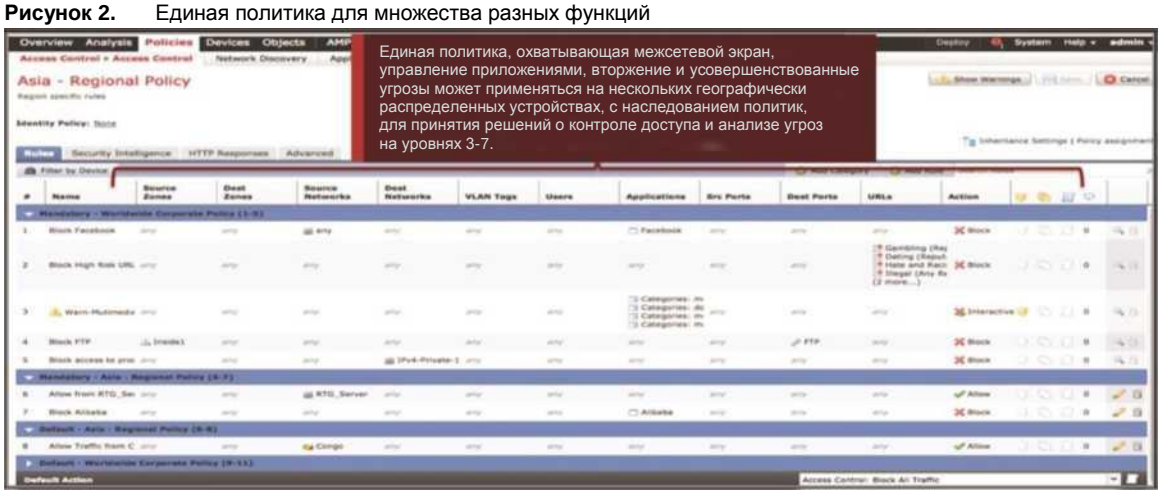
- **Тенденции и обобщенные статистические данные** Эти данные позволяют понять состояние безопасности в каждый момент времени, а также тенденцию его изменения — в лучшую или худшую сторону.
- **Подробная информация о событиях, соответствие нормативным требованиям и экспертиза.** Это позволяет понять, что происходило во время события, связанного с безопасностью, а также оптимизировать защиту, обеспечить поддержку мер по нейтрализации угроз и содействовать принудительному выполнению политик.
- **Данные потока.** Могут быть легко экспортированы в другие решения для улучшения управления реагирования на инциденты.

Функции и преимущества

Функция	Преимущество
Унифицированное управление разными функциями безопасности на разных платформах	Облегчает централизованное управление средой безопасности Cisco, включающей следующие решения: • межсетевой экран нового поколения Cisco Firepower Next-Generation Firewall (NGFW); • Cisco ASA с сервисами FirePOWER; • Cisco Firepower NGIPS; • Cisco FirePOWER Threat Defense for ISR • Cisco AMP.
Интегрированное управление политиками для разных функций безопасности	Конфигурирует настройки доступа к межсетевому экрану, контроля приложений, предотвращения угроз, фильтрации URL-адресов и защиты от усовершенствованного вредоносного ПО в единой политике. Облегчает управление политиками, уменьшает количество ошибок и обеспечивает целостность и единообразие. Позволяет применять одну политику сразу к нескольким решениям по безопасности.
Интеграция управления политиками доступа с Cisco Identify Services Engine	Управляет доступом на основе меток группы безопасности ISE, типа устройств и местоположения IP, а также обеспечивает быстрое сдерживание угроз Обеспечивает соответствие нормативным требованиям, повышает безопасность инфраструктуры и оптимизирует работу сервисов
Высочайший уровень аналитики сетевых угроз	Интегрирует аналитические данные по безопасности, угрозам и уязвимостями, предоставленные группой Cisco Talos, для обеспечения защиты от угроз за считанные минуты. Использует новые методы защиты от атак на основе данных безопасности по IP- и URL-адресам Включает Cisco Umbrella для мониторинга угроз за пределами периметра сети. Обеспечивает получение и сопоставление аналитических данных об угрозах из каналов данных об угрозах и платформ анализа угроз третьих сторон в форматах STIX/TAXII или простых файлов
Мониторинг и контроль приложений	Сокращает число угроз для вашей сети за счет точного контроля более 4000 коммерческих приложений. Использует OpenAppID на основе открытых стандартов для подробной идентификации и управления пользовательскими приложениями
Многопользовательское управление и наследование политик	Создает до 50 доменов управления с отдельными данными событий, отчетностью и сопоставлением сетей, реализованными через управление доступом на основе ролей. Обеспечивает целостное и эффективное управление благодаря своей иерархической структуре политик, в которой каждый уровень наследует политики вышестоящего уровня.
Отчеты и информационные панели	Обеспечивает необходимый уровень мониторинга за счет создания настраиваемых информационных панелей с пользовательскими отчетами на основе шаблонов Предоставляет всеобъемлющие отчеты и предупреждения по общим и целевым данным. Отображает контекстную информацию и информацию о событиях в виде таблиц, графиков и диаграмм с гиперссылками для удобства использования в аналитических целях Контролирует поведение сети и производительность на предмет обнаружения аномалий и поддержания работоспособности системы.
Защищенная загрузка	Защищенная загрузка (Secure boot) — это механизм для подтверждения целостности и подлинности программного обеспечения Cisco, выполняемого на оборудовании FMC при загрузке системы. Если сигнатура отсутствует, или программное обеспечение недействительно, оно не будет загружаться, и самозрагрузки системы не произойдет. (только FMC 1000, FMC 2500, FMC 4500)

© Корпорация Cisco и/или ее дочерние компании, 2017. Все права защищены. В данном документе содержится общедоступная информация Cisco.

Рисунок 2. Единая политика для множества разных функций



Непревзойденный мониторинг и подробный анализ

Нельзя защищать то, что нельзя увидеть. Решение Cisco Firepower Management Center автоматически собирает, сопоставляет и отображает контекстную информацию обо всем, что происходит в вашей среде. В таблице 1 представлен весь диапазон контекстных данных, которые можно получить о векторах угроз, и которые не в состоянии обнаружить стандартные технологии обеспечения безопасности. Такие подробные данные анализа сети можно использовать для определения политик защиты и обеспечения такого высокого уровня защиты, которые не могут предоставить другие решения.

Таблица 1. Полная прозрачность инфраструктуры

Категория	Cisco Firepower Management Center	Обычная система обнаружения вторжений	Обычный межсетевой экран нового поколения
Угрозы	Да	Да	Да
Пользователи	Да	Да	Да
Веб-приложения	Да	Нет	Да
Протоколы приложений	Да	Нет	Да
Передача файлов	Да	Нет	Да
Вредоносное ПО	Да	Нет	Нет
Серверы команд и управления	Да	Нет	Нет
Клиентские приложения	Да	Нет	Нет
Сетевые серверы	Да	Нет	Нет
Операционные системы	Да	Нет	Нет
Маршрутизаторы и коммутаторы	Да	Нет	Нет
Мобильные устройства	Да	Нет	Нет
Принтеры	Да	Нет	Нет
Телефоны VoIP	Да	Нет	Нет
Виртуальные машины	Да	Нет	Нет
Информация об уязвимостях	Да	Нет	Нет

Управление на всем протяжении атаки — до, во время и после

Решение Cisco Firepower Management обеспечивает унифицированное управление на всем протяжении атаки — до, во время и после.

До

- Обеспечивает непревзойденный мониторинг того, что происходит в вашей сети, чтобы вы могли увидеть угрозу и принять соответствующие меры.
- Создает правила для МСЭ и контролирует более 4000 коммерческих и пользовательских приложений, выполняемых в вашей среде.

© Корпорация Cisco и/или ее дочерние компании, 2017. Все права защищены. В данном документе содержится общедоступная информация Cisco.

Во время

- Определяет уровни предотвращения вторжений, правила репутации URL-адресов и компоненты защиты от усовершенствованного вредоносного ПО, которые необходимо установить.
- Применяет такие политики, как: «Если трафик приходит из этой страны с использованием этого конкретного приложения с прикрепленным файлом, я будут применять этот уровень проверки на предмет наличия вторжения и анализировать этот файл на предмет наличия вредоносного ПО, и даже, при необходимости, отправлять его в песочницу».

После

- Создает графическое представление всех устройств, которые были инфицированы в результате конкретной атаки.
- Обеспечивает возможность легко создавать пользовательское правило для остановки атаки и предотвращения ее распространения.
- Предоставляет подробные аналитические данные о конкретном вредоносном ПО для его безопасного удаления.

Автоматическая безопасность для динамической защиты

Решение Cisco Firepower Management Center постоянно следит за изменениями в сети. Оно оптимизирует работу сети и обеспечивает ее безопасность благодаря следующим возможностям:

- Автоматическая корреляция событий новых атак с уязвимостями вашей сети для того, чтобы предупреждать вас об атаках, которые могут оказаться удачными. Ваша команда специалистов по безопасности сможет сфокусировать свое внимание на событиях, которые важнее всего;
- Анализ уязвимостей вашей сети и автоматическое предоставление рекомендаций о политиках безопасности, которые следует внедрить. Вы можете адаптировать ваши механизмы защиты к меняющимся условиям и внедрить меры безопасности, подходящие конкретно для вашей сети.
- Корреляция отдельных событий из сети, оконечного устройства, системы обнаружения вторжений и анализа безопасности. В случае если отдельные узлы проявляют признаки компрометации, связанные с неизвестными атаками, вы получаете предупреждение.
- Применение критериев политик. Если эти политики удовлетворены, система автоматически анализирует файл на предмет выявления известного вредоносного ПО и (или) отправляет этот файл во встроенную песочницу для определения неизвестного вредоносного ПО.

Открытые API-интерфейсы для удобной интеграции

Решение Cisco Firepower Management Center делает возможным интеграцию с технологиями третьих фирм благодаря использованию четырех прикладных программных интерфейсов с мощным и эффективным функционалом Эти API-интерфейсы представляют собой точки подключения для реализации перечисленных ниже задач.

- Перемещение данных событий из решения Management Center на другую платформу, например, решение по управлению информацией и событиями безопасности (SIEM)
- Пополнение информации, содержащейся в базе данных Cisco Firepower, данными третьих фирм. Такие данные могут включать данные систем управления уязвимостями и информацией об операционных системах из активных сканеров.
- Запуск рабочих процессов и реализация шагов по восстановлению, которые инициируются правилами корреляции, определяемыми пользователями. Например, можно интегрировать рабочий процесс с решением контроля сетевого доступа (NAC) для помещения в карантин инфицированного оконечного устройства, или запустить процесс цифрового расследования.
- Поддержка возможностей по созданию отчетности и аналитики третьих фирм благодаря предоставлению возможности этим решениям отправлять запросы в базу данных Management Center.

© Корпорация Cisco и/или ее дочерние компании, 2017. Все права защищены. В данном документе содержится общедоступная информация Cisco.

Эти API-интерфейсы также используются для интеграции с отдельными продуктами и рабочими операциями Cisco по обеспечению безопасности. Среди них: Cisco AMP Threat Grid для песочницы; Cisco Identity Services Engine для идентификации данных и сегментации сети и Cisco Umbrella для мониторинга доменов по всей сети Интернет.

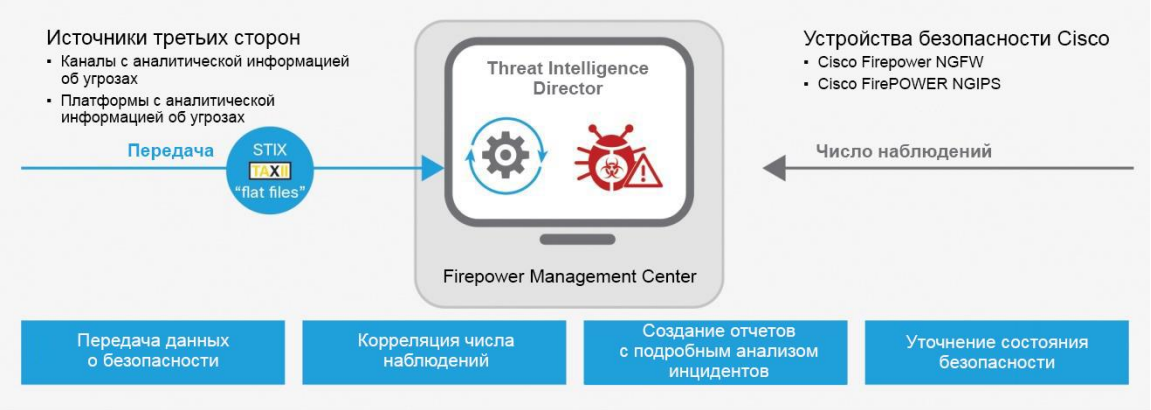
Threat Intelligence Director

Функция Threat Intelligence Director теперь доступна в решении Cisco Firepower Management Center (v6.2.1). Используя открытые API-интерфейсы, функция Threat Intelligence Director облегчает получение аналитических данных об угрозах третьих сторон из таки источников, как каналы с данными об угрозах и платформы анализа угроз (threat intelligence platforms, TIP). Эта функция поддерживает стандарты Structured Threat Information Expression (STIX) и Trusted Automated Exchange of Indicator Information (TAXII) или отдельные форматы простых (неотформатированных) файлов. Threat Intelligence Director раскладывает получаемые аналитические данные на компоненты, которые можно изучать (IoCs), включая IP (IPv4, IPv6), домены, URL-адреса и SHA-256. Все эти данные передаются на устройства безопасности Cisco, которые могут автоматически блокировать действия злоумышленников изнутри или осуществлять мониторинг сети с целью быстрого реагирования на угрозы.

Threat Intelligence Director может обрабатывать доступные аналитические данные об угрозах для следующих устройств безопасности Cisco:

- Межсетевой экран нового поколения Cisco Firepower NGFW
- Система защита от вторжений нового поколения Cisco Firepower NGIPS

Рисунок 3. Threat Intelligence Director позволяет интегрировать аналитические данные безопасности третьих сторон



Последний список партнеров TIP и каналов аналитических данных кибербезопасности третьих сторон см. по ссылке: Cisco Technical Alliance Partners Listing.

Варианты развертывания

Решение Cisco Firepower Management Center можно развертывать как физическое или виртуальное устройство или из облака (таблица 2), поэтому вы сможете выбрать тот вариант, который лучше всего подойдет для вашей среды. Физические устройства обычно могут управлять большим числом сенсоров и предоставляют больше емкости для хранения событий, чем их виртуальные аналоги. Удобство виртуальных устройств заключается в возможности использования существующей инфраструктуры виртуальных машин. Для хостинга Management Center можно также использовать облачные вычислительные сервисы. Эти сервисы обеспечиваю управление безопасностью без необходимости дополнительных инвестиций в вычислительные мощности и хранилище базы данных. Кроме того, они дают возможность гибкого и быстрого масштабирования по мере потребности.

© Корпорация Cisco и/или ее дочерние компании, 2017. Все права защищены. В данном документе содержится общедоступная информация Cisco.

При использовании функции Threat Intelligence Director на виртуальных МСЭ нового поколения для оптимальной производительности рекомендуется устанавливать на оборудование память объемом 15 Гбайт.

Таблица 2. Варианты развертывания

Платформа развертывания	Минимальная версия
Гипервизоры VMware ESX и ESXi	Версия 5.x
Гипервизор KVM	Версия 6.1
Облачная платформа веб-сервисов Amazon	Версия 6.0

Технические характеристики платформы

Решение Cisco Firepower Management Center предлагается в виде нескольких разных моделей. Выберите модель, наилучшим образом подходящую для вашей организации, в зависимости от количества сенсорных устройств, подлежащих мониторингу (оба варианта - и физические, и виртуальные), числа хостов в вашей среде и ожидаемому числу событий безопасности (см. таблицу 3). Все модели предоставляют следующие одинаковые возможности управления:

- Централизованное управление устройствами, лицензиями, событиями и политиками
- Управление на основе ролей (сегментированные и отдельные представления и обязанности в зависимости от роли администратора или группы)
- Настраиваемые информационные панели с отчетами на основе шаблонов и настраиваемые в соответствии с потребностями пользователей
- Всеобъемлющие отчеты и предупреждения по общим и целевым данным
- Контекстная информация и информация о событиях в виде таблиц, графиков и диаграмм с гиперссылками
- Поведение сети и контроль производительности
- Надежные функции высокой доступности для гарантии отсутствия сбоев
- Функции корреляции и восстановления для реагирования на угрозы в реальном времени
- Открытые API-интерфейсы для интеграции с решениями третьих фирм и пользовательскими рабочими потоками, такими как межсетевые экраны, сетевая инфраструктура, управление журналами, SIEM, журналы неисправности и управление исправлениями

В таблице 3 приводится сравнение емкости и пропускной способности доступных устройств Cisco Firepower Management Center (физических и виртуальных).

Таблица 3. Модели устройств Cisco Firepower Management Center

Производительность и функциональность	FMC 750	FMC 1000	FMC 2000	FMC 2500	FMC 4000	FMC 4500	FMCv
Максимальное число управляемых сенсоров	10	50	250	300	500	750	25 10 2
Макс. число событий IPS	20 млн	60 млн	60 млн	60 млн	300 млн	300 млн	10 млн
Интерфейс управления	100/100/1000 RJ-45						
Сетевые интерфейсы	2 x 1 Гбит/с	2 x 1 Гбит/с	2 x 1 Гбит/с 2 x 10 Гбит/с SFP+	2 x 1 Гбит/с 2 x 10 Гбит/с SFP+	2 x 1 Гбит/с 2 x 10 Гбит/с SFP+	2 x 1 Гбит/с 2 x 10 Гбит/с SFP+	
Память	8 Гбайт (поставляется в настоящее время)	32 Гбайт	64 Гбайт	64 Гбайт	128 Гбайт	128 Гбайт	–
ЦП	4-х ядерный Xeon	8-ми ядерный Xeon	6-ти ядерный Xeon	2 восьмиядерных процессора Xeon	2 десятиядерных процессора Xeon	2 десятиядерных процессора Xeon	—

© Корпорация Cisco и/или ее дочерние компании, 2017. Все права защищены. В данном документе содержится общедоступная информация Cisco.

Производительность и функциональность	FMC 750	FMC 1000	FMC 2000	FMC 2500	FMC 4000	FMC 4500	FMCv
Система хранения событий	100 Гбайт	900 Гбайт	1,8 Тбайт	1,8 Тбайт	3,2 Тбайт	3,2 Тбайт	250 Гбайт
Максимальное соотношение в сети хостов к пользователям	2 000/2 000	50 000/50 000	150 000/150 000	150 000/150 000	600 000/600 000	600 000/600 000	50 000/50 000
Максимальная частота потока (число потоков в секунду)	2 000 потоков/сек	5 000 потоков/сек	12 000 потоков/сек	12 000 потоков/сек	20 000 потоков/сек	20 000 потоков/сек	Различается
Сетевые интерфейсы	2 x 1 Гбит/с	2 x 10 Гбит/с 2 порта	2 x 1 Гбит/с 2 x 10 Гбит/с (можно заказать дополнительные модули SFP на портале Cisco Commerce)	1 x 10 Гбит/с 2 порта 1 двойной порт 10 Гбит/с SFP+	2 x 1 Гбит/с 2 x 10 Гбит/с (можно заказать дополнительные модули SFP на портале Cisco Commerce)	1 x 10 Гбит/с 2 порта 1 двойной порт 10 Гбит/с SFP+	1 x 1 Гбит/с
Защищенная загрузка	—	Да	—	Да	—	Да	—
Возможности резервирования							
Поддержка высокой доступности	Нет	Да	Да	Да	Да	Да	Нет
2 блока питания	Нет	Да	Да	Да	Да	Да	—
Поддержка RAID	Нет	HDD RAID 1	HDD RAID 5	HDD RAID 1	SSD RAID 6	SSD RAID 6	—
Физические характеристики и требования к окружающей среде							
Форм-фактор	1RU	1RU	1RU	1RU	1RU	1RU	—
Размеры глубина x ширина x высота (дюймы)	27,19 x 16,9 x 1,7 (69 x 43 x 4,3 см)	29,8 x 16,9 x 1,7 (75,7 x 43 x 4,3 см)	28,5 x 16,9 x 1,7 (72,3 x 43 x 4,3 см)	29,8 x 16,9 x 1,7 (75,7 x 43 x 4,3 см)	28,5 x 16,9 x 1,7 (72,3 x 43 x 4,3 см)	29,8 x 16,9 x 1,7 (75,7 x 43 x 4,3 см)	—
Масса комплекта поставки	33 фунта (15 кг)	39 фунтов (17,7 кг)	35,6 фунтов (16,2 кг)	39 фунтов (17,7 кг)	35,6 фунтов (16,2 кг)	39 фунтов (17,7 кг)	—
Вт (макс.)	350 Вт	770 Вт	650 Вт	770 Вт	650 Вт	770 Вт	—
Электропитание	макс. 9,5 А при 110 В, 50/60 Гц макс. 4,75 А при 220 В, 50/60 Гц	100-240 В перем. тока (номинальное значение) 90-264 В перем. тока (мин./макс. значение) макс. 9,5 А при 100 В перем. тока макс. 4,5 А при 208 В перем. тока	От 90 до 264 В перем. тока (саморегулировка). 100-120 В перем. тока (номинальное значение) 200-240 В перем. тока (номинальное значение) Пиковое значение 7,6 А при 100 В перем. тока Пиковое значение 3,65 А при 208 В перем. тока	100-240 В перем. тока (номинальное значение) 90-264 В перем. тока (мин./макс. значение) 9.5 макс. 9,5 А при 100 В перем. тока 4.5 макс. 4,5 А при 208 В перем. тока	От 90 до 264 В перем. тока (саморегулировка). 100-120 В перем. тока (номинальное значение) 200-240 В перем. тока (номинальное значение) Пиковое значение 7,6 А при 100 В перем. тока Пиковое значение 3,65 А при 208 В перем. тока	100-240 В перем. тока (номинальное значение) 90-264 В перем. тока (мин./макс. значение) 9.5 макс. 9,5 А при 100 В перем. тока 4.5 макс. 4,5 А при 208 В перем. тока	
Обдув	От передней панели к задней	От передней панели к задней	От передней панели к задней	От передней панели к задней	От передней панели к задней	От передней к задней панели	—
Рабочая температура	от 10°C до 35°C	от 5°C до 35°C	от 5°C до 40°C	от 5°C до 35°C	от 5°C до 40°C	от 5°C до 35°C	—

Производительность виртуального устройства Cisco Firepower Management Center сильно зависит от выбранной виртуальной среды: ЦП, память, хранилище и т.д.

Общие функции

- Встроенное внешнее сетевое управление (LOM)
- Централизованное управление решениями Cisco по безопасности нового поколения: NGIPS, NGIPS плюс контроль приложений, NGFW

Примечание. При работе с продуктами Cisco ASA с сервисами FirePOWER, все устройствaCisco Firepower Management Centers управляют только той частью развертываемого решения, которая относится к FirePOWER.

© Корпорация Cisco и/или ее дочерние компании, 2017. Все права защищены. В данном документе содержится общедоступная информация Cisco.

В таблице 4 перечислены поддерживаемые версии продуктов Cisco Firepower, которыми может управлять устройство Cisco Firepower Management Center, а также представлены связанные аппаратные платформы.

Таблица 4. Поддерживаемые версии Firepower и связанные с ними платформы

Платформа управления	Версия ПО	Аппаратная платформа
Cisco Firepower Management Center	**Cisco Firepower Threat Defense 6.x (NGFW)**	**ASA 5500-X (кроме ASA 5585-X)** Cisco Firepower 4100 Series Cisco Firepower 9300
	Сервисы FirePOWER 6.x	**ASA 5500-X**
	Cisco Firepower NGIPS 6.x	**Cisco Firepower серии 7000** Cisco Firepower серии 8000
	FirePOWER Threat Defense для ISR 6.x (сервисы Cisco FirePOWER)	**4000 серия ISR** ISR G2
	Сервисы FirePOWER 5.4.x	**ASA 5500-X**
	Cisco Firepower NGIPS 5.4.x	**Cisco Firepower 7000** **Cisco Firepower 8000**

Совместимость с гипервизорами

Виртуальное устройство Cisco Firepower Management Center поддерживает версии гипервизоров, перечисленные в таблице 5.

Таблица 5. Поддержка гипервизора виртуальным устройством

Гипервизор	Версия и описание	Версия виртуального устройства Cisco Firepower Management Center
VMware vSphere	5.1,5.5:, 6.0 • Сервер ESXi • Сервер vCenter (дополнительно) • Веб-клиент vSphere, клиент vSphere или инструмент OVF для Windows или Linux	5.4, 6.0
KVM	Ubuntu 14.04 LTS Red Hat Enterprise Linux (RHEL), версия 7.1	6.1
Веб-сервисы Amazon	Типы экземпляров AWS: c3.xlarge и c3.2xlarge	6.0.1,6.1

Информация для заказа

Лицензирование

Начиная с версии 6.0, лицензионные ключи для пользования Cisco Firepower Management Center больше не нужны. Для версий 5.4 и более ранних по-прежнему требуется ключ авторизации продукта (PAK) или smart-ключ. При обновлении до версии 6.0 это требование отпадает.

Поддержка услуги Cisco Smart Net Total Care

Услуга Cisco Smart Net Total Care™ - это прекрасно зарекомендовавшая себя услуга технической поддержки, благодаря которой ваши ИТ-специалисты получают прямой круглосуточный доступ к инженерам центра технической поддержки Cisco Technical Assistance Center (TAC) и ресурсам Cisco.com. Вы получаете быструю экспертную поддержку и выделенные ресурсы, необходимые для быстрого решения критически важных проблем.

Smart Net Total Care обеспечивает следующую поддержку для устройств:

- Круглосуточный доступ 365 дней в году из любой точки мира к квалифицированным инженерам центра поддержки Cisco TAC
- Доступ в любое время к расширенным онлайн-возможностям сайта Cisco.com - базе знаний, ресурсам и инструментам
- Варианты замены оборудования - замена оборудования через 2, 4 часа или на следующий день (NDB), а также возможность возврата оборудования на ремонт (RFR)

© Корпорация Cisco и/или ее дочерние компании, 2017. Все права защищены. В данном документе содержится общедоступная информация Cisco.

- Постоянные обновления ПО операционной системы, в том числе основные и вспомогательные версии в рамках вашего набора лицензионных функций
- Проактивная диагностика и предупреждения в реальном времени по выбранным устройствам с помощью услуги Cisco Smart Call Home

Кроме того, услуга Cisco Smart Net Total Care Onsite Service, предоставляемая на местах, предусматривает выезд инженера, который установит заменяемые детали в вашем офисе и гарантирует, что ваша сеть будет работать на самом высоком уровне.
Более подробную информацию об услуге Smart Net Total Care см. по ссылке:
http://www.cisco.com/c/en/us/services/portfolio/product- technical-support/smart-net-total-care.html.

Информация для заказа

В таблице 6 представлена информация для заказа виртуальных и физических устройств Cisco Firepower Management Center и запасного оборудования. Дополнительную информацию по возможностям конфигурации и аксессуарам см. в руководстве по заказу продуктов безопасности Cisco Network Security Ordering Guide .

Таблица 6. Информация для заказа

Устройства Cisco Firepower Management Center (оборудование)	
Номер по каталогу	**Описание продукта**
FS750-K9	Шасси Cisco Firepower Management Center 750, 1 RU
FMC1000-K9	Шасси Cisco Firepower Management Center 1000, 1RU
FS2000-K9	Шасси Cisco Firepower Management Center 2000, 1RU
FMC2500-K9	Шасси Cisco Firepower Management Center 2500, 1 RU
FS4000-K9	Шасси Cisco Firepower Management Center 4000, 1RU
FMC4500-K9	Шасси Cisco Firepower Management Center 4500, 1 RU
Устройства Cisco Firepower Management Center (оборудование), запасные части	
FS-PWR-AC-650W=	Блок питания переменного тока Cisco Firepower 650 Вт для FS2000, FS4000
FS-PWR-AC-779W=	Блок питания переменного тока Cisco 770 Вт для FMC1000, FMC2500, FMC4500
Виртуальное устройство Cisco Firepower Management Center (программное обеспечение)	
FS-VMW-SW-K9	Лицензия на виртуальное устройство Cisco Firepower Management Center, (VMware) Firepower
FS-VMW-10-SW-K9	Лицензия Cisco Firepower Management Center, (VMware) Firepower на 10 виртуальных устройства
FS-VMW-2-SW-K9	Лицензия Cisco Firepower Management Center, (VMware) Firepower на 2 виртуальных устройства

Для размещения заказа перейдите на главную страницу заказов Cisco.

Гарантийные обязательства

Информацию о гарантии можно найти на странице Гарантия на продукты веб-сайта Cisco.com.

Услуги Cisco

Cisco предлагает целый ряд программ обслуживания для ускорения успешного развертывания решений заказчиков. Эти инновационные сервисные программы представляют собой уникальное сочетание опыта наших специалистов с хорошо организованными процессами, ценными инструментами и широкой партнерской сетью, что в итоге дает высокий уровень удовлетворенности заказчиков. Предлагаемые компанией Cisco услуги позволят защитить инвестиции в сетевую инфраструктуру, оптимизировать эксплуатацию сети и подготовить сеть к внедрению новых приложений, призванных расширить использование интеллектуальных функций и вывести ваш бизнес на новый уровень. Более подробную информацию об услугах Cisco по информационной безопасности см. по ссылке
http://www.cisco.com/go/services/security.

© Корпорация Cisco и/или ее дочерние компании, 2017. Все права защищены. В данном документе содержится общедоступная информация Cisco.

Cisco Capital

Возможности финансирования, которые помогут в достижении поставленных целей

Программы финансирования Cisco Capital помогут вам приобрести технологии, необходимые для достижения поставленных целей и обеспечения конкурентоспособности. Мы поможем вам снизить капитальные затраты. Ускорить развитие бизнеса. И оптимизировать инвестиции и их окупаемость. Программы финансирования Cisco Capital обеспечивают гибкие возможности при приобретении оборудования, программного обеспечения, сервисов и дополнительного оборудования сторонних производителей. И это всего лишь за один прогнозируемый платеж. Программами Cisco Capital можно воспользоваться более чем в 100 странах. Подробнее.

Дополнительная информация

Для получения дополнительной информации пройдите по следующим ссылкам:

- Cisco Firepower Management Center
- Cisco Firepower Next-Generation Firewalls
- Cisco Firepower Next-Generation IPS (NGIPS)
- Cisco Advanced Malware Protection (AMP)
- Cisco FirePOWER Threat Defense for ISR
- Cisco Security Services

Для получения дополнительной информации о решении Cisco Firepower в средах операторов связи пройдите по следующим ссылкам: http://www.cisco.com/c/en/us/solutions/enterprise-networks/service-provider-security-solutions/

Россия, 121614, Москва,
ул. Крылатская, д.17, к.4 (Krylatsky Hills)
Телефон: +7 (495) 961-1410, факс: +7 (495) 961-1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313-6230, факс: +7 (812) 313-6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391-3600, факс: +38 (044) 391-3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269-1691, факс: +375 (17) 269-1699
www.cisco.ru, www.cisco.com

Казахстан, 050059, Алматы, бизнес-центр «Самал Тауэрс», ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244-2101, факс: +7 (727) 244-2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, «Лэндмарк» здание III, 3 этаж
Телефон: +994 (12) 437-4820, факс: +994 (12) 437-4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998 (71) 140-4460, факс: +998 (71) 140-4465

© 2015 Cisco и (или) ее дочерние компании. Все права защищены. Cisco, логотип Cisco и Cisco Systems являются зарегистрированными товарными знаками или товарными знаками Cisco и (или) ее дочерних компаний в США и некоторых других странах. Все прочие товарные знаки, упомянутые в этом документе или на сайте, являются собственностью соответствующих владельцев. Использование слова «партнер» не означает наличия партнерских отношений компании Cisco с какой-либо другой компанией. (1002R)

© Cisco Systems, Inc, 2015. С сохранением всех прав. В данном документе содержится информация, свободно распространяемая компанией Cisco.