DATA SHEET

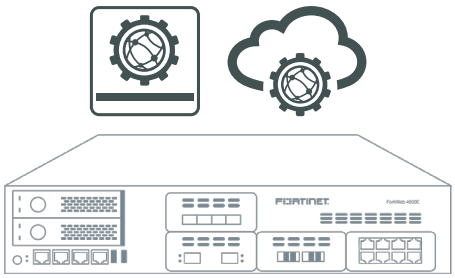
FortiWeb™

Исполнение:

Устройство | Виртуальная машина | SaaS | Облако | Контейнер

Защита веб-приложений и API

FortiWeb 100E, 400E, 600E, 1000E, 2000E, 3000E, 4000E, ВМ и Контейнер



FortiWeb представляет собой межсетевой экран уровня веб-приложений (WAF), который реализует защиту от атак, направленных на эксплуатацию известных и неизвестных уязвимостей, и помогает соответствовать требованиям отраслевых стандартов.

Благодаря использованию многоуровневой системы обнаружения угроз на базе искусственного интеллекта, а также методов корреляции событий FortiWeb обеспечивает защиту приложений от известных уязвимостей и угроз нулевого дня.

Защита веб-приложений

Защита веб-приложений от десяти наиболее распространенных угроз по версии OWASP, в том числе от межсайтового скриптинга и внедрения SQL-кода.

Защита API

Защита API от эксплуатации злоумышленниками, фильтрация на основе политик. Бесшовная интеграция безопасности API в процесс разработки и пайплайн CI/CD.

Противодействие ботам

Защита веб-сайтов, мобильных приложений и API от автоматизированных атак, точно разделяя хороших и плохих ботов, блокируя последних. Механизмы противодействия ботам предоставляют инструменты контроля и визуализации запросов без необходимости ввода CAPTCHA или ответов на вопросы.

Особенности

- Механизмы машинного обучения для повышения эффективности и снижения ложных срабатываний
- Механизмы противодействия ботам без негативного влияния на легитимных пользователей
- Защита API, включая используемые для мобильных приложений
- Расширенная защита за счет интеграции с Fortinet Security Fabric
- Инструменты визуальной аналитики
- Виртуальный патчинг и интеграции

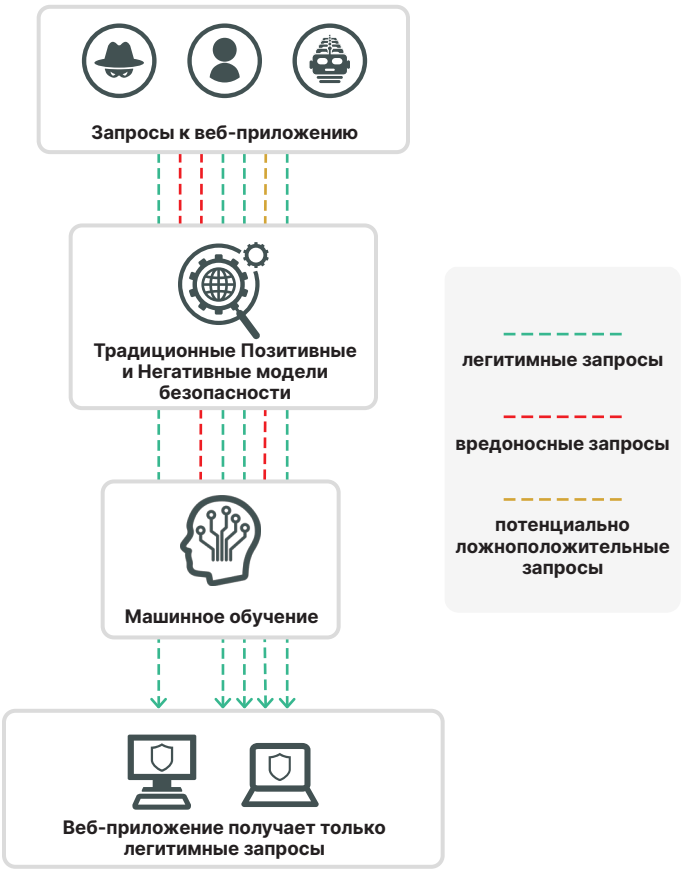
Круглосуточная техническая поддержка FortiCare
support.fortinet.com

Сервисы безопасности FortiGuard
www.fortiguard.com

Сертификация отраслевых лабораторий

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ



FortiWeb уходит вперед от традиционных позитивных и негативных моделей безопасности (сигнатуры атак, репутация IP адресов, валидация протокола и т.д.) и реализует дополнительный эшелон защиты с помощью интеллектуального механизма машинного обучения и аналитики, детектируя и блокируя вредоносные аномалии, минимизируя количество ложных срабатываний.

Машинное обучение улучшает обнаружение атак и увеличивает операционную эффективность.

Способность FortiWeb обнаруживать поведенческие аномалии в запросах к конкретному защищаемому приложению позволяет блокировать ранее неизвестные эксплойты и предотвращать атаки нулевого дня, нацеленные на приложение.

В операционном плане машинное обучение FortiWeb избавляет вас от трудоемких задач, таких как устранение ложных срабатываний или ручная настройка правил WAF. FortiWeb постоянно обновляет математическую модель запросов по мере развития вашего приложения, поэтому нет необходимости вручную обновлять правила при каждом обновлении. FortiWeb позволяет вам быстрее выпускать в релиз новые функции веб-приложений, а также экономит ресурсы специалистов, повышая операционную эффективность.

Защита от атак нулевого дня

Безопасность веб-приложений

FortiWeb обеспечивает многоуровневую защиту веб-приложений от всего спектра угроз, включая 10 наиболее распространенных и опасных типов атак по версии OWASP. На первом уровне используются традиционные механизмы для обнаружения и блокировки вредоносных запросов: сигнатуры, IP репутация, валидация протокола и т.д. На втором уровне FortiWeb использует механизмы машинного обучения для обнаружения аномалий, опираясь на генерируемую FortiWeb математическую модель защищаемого приложения. Модель формируется и обновляется решением самостоятельно, исключая необходимость в ручной донастройке правил фильтрации.

Защита API

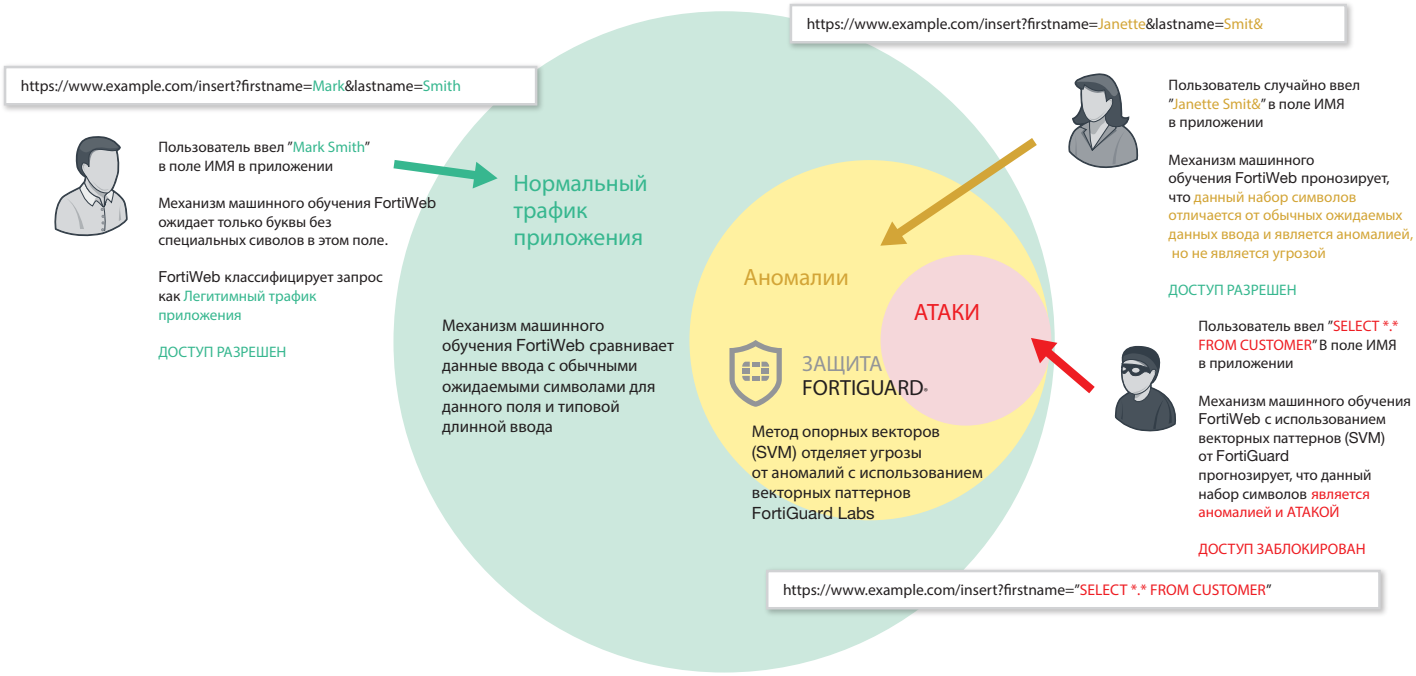
В условиях активной цифровой трансформации API интерфейсы стали еще более популярными. Они являются неотъемлемой частью инфраструктуры мобильных приложений и интеграции бизнес систем. Доступность, распространенность и важность выполняемых функций делает API привлекательной целью для злоумышленников. Защита API веб-приложений является одним из ключевых предназначений FortiWeb. FortiWeb позволяет импортировать схему API веб-приложения (OpenAPI, XML или JSON) и автоматически сформировать позитивную модель безопасности для защиты от API эксплойтов. Механизм валидации схемы API FortiWeb может быть интегрирован в конвейер разработки и доставки приложений (CI/CD) для автоматической перегенерации позитивной модели безопасности при каждом обновлении API приложения.

Противодействие ботам

FortiWeb защищает веб-ресурсы, API, приложения, пользователей и чувствительную информацию от автоматизированных ботов, автосборщиков данных с сайтов и других инструментальных атак. Сочитая механизмы машинного обучения, политики пороговых значений для запросов, ловушек для ботов, биометрический анализ, FortiWeb эффективно блокирует атаки ботов, сводя к нулю негативное воздействие на легитимных пользователей. Составляя профиль пользователя, FortiWeb может отличить запросы человека, бота и злоумышленника, минимизируя необходимость использования CAPTCHA. Инструменты графической аналитики FortiWeb позволяют компаниям легко дифференцировать атаки, хороших ботов и легитимных пользователей.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Машинное обучение FortiWeb точно обнаруживает аномалии и определяет, какие из них являются атаками. В отличие от существующих моделей обнаружения, используемых другими поставщиками WAF, которые воспринимают каждую аномалию, как угрозу, FortiWeb с высокой точностью исключает ложноположительные срабатывания и перехватывает типы атак, которые недоступны аналогичным устройствам.

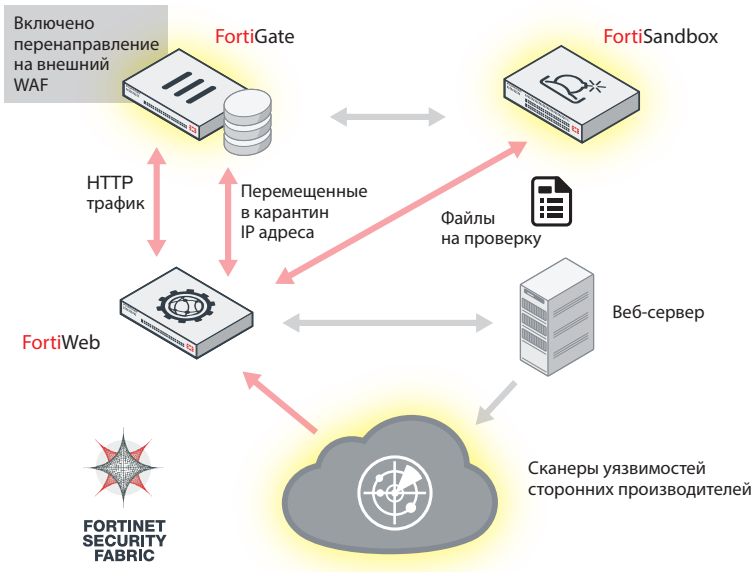


Интелектуальный механизм машинного обучения FortiWeb оценивает запросы к приложению и определяет, являются ли они легитимными, неопасными аномалиями или аномалиями, представляющими собой угрозу.

Тесная интеграция с Fortinet Security Fabric и сканерами уязвимостей сторонних производителей

По мере развития ландшафта угроз многие новые угрозы требуют комплексного подхода к защите веб-приложений. Развитые устойчивые угрозы, нацеленные на организации, могут принимать различные формы по сравнению с традиционными одновекторными атаками, и могут обойти защиту, осуществляемую только одним устройством. Интеграция FortiWeb с FortiGate и FortiSandbox расширяет основные возможности защиты WAF посредством синхронизации и обмена информацией об угрозах как в случае глубокого сканирования подозрительных файлов, так и в случае распространения зараженных внутренних источников.

FortiWeb обеспечивает интеграцию со сканерами уязвимостей от сторонних производителей, включая Acunetix, HP WebInspect, IBM AppScan, Qualys, IBM QRadar и WhiteHat для формирования виртуальных патчей. Уязвимости, обнаруженные сканером, автоматически превращаются в правила безопасности FortiWeb для защиты приложения до того момента, пока разработчики не смогут внести их в код приложения.



Интеграция с другими элементами архитектуры информационной безопасности Fortinet Security Fabric, в том числе с FortiGate и FortiSandbox, обеспечивает защиту от развитых устойчивых угроз (APT) и расширяет возможности сканеров уязвимостей сторонних производителей

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Решение проблемы ложных срабатываний

Ложноположительные срабатывания могут иметь крайне разрушительные последствия и часто приводят к тому, что многие администраторы ослабляют правила безопасности межсетевых экранов для веб-приложений до такой степени, что многие из них становятся средством мониторинга, а не надежной платформой для предотвращения угроз.

Механизмы искусственного интеллекта FortiWeb исключают ложные срабатывания без необходимости трудоемкого управления белыми списками и тонкой настройки политик. При обеспечении практически 100 % точности, двухуровневые обучаемые механизмы обнаруживают аномалии, а затем определяют, являются ли они атаками, в отличие от других производителей, которые блокируют все аномалии независимо от их сути. В сочетании с другими защитными механизмами FortiWeb практически исключает ложные срабатывания.

Отчетность и расширенная графическая аналитика

FortiWeb включает в себя набор инструментов графической аналитики FortiView. Он визуализирует ключевые элементы конфигурации, карту атаки, категорирует события безопасности в соответствии с классификацией OWASP, технические параметры клиентских запросов. FortiView позволяет в режиме реального времени обнаруживать источники подозрительной активности и атак, агрегировать вспомогательную информацию о пользователе и клиентском устройстве.

Защита с помощью FortiGuard

Отмеченные наградами сервисы FortiGuard Labs от компании Fortinet являются основой FortiWeb при обеспечении безопасности приложений. Служба репутации IP-адресов FortiWeb защищает вас от известных источников атак, таких как ботнеты, спамеры, анонимные прокси-серверы и источники, замеченные в распространении вредоносного ПО.

Для FortiWeb разработаны специализированные сервисы FortiGuard: сигнатуры прикладного уровня, модели угроз машинного обучения, подозрительные шаблоны URL, вредоносные боты, обновления сканера уязвимостей, модуль антивирусной фильтрации. Сервис защиты учетных данных (Credential Stuffing Defense) проверяет попытки входа в соответствии со списком скомпрометированных учетных данных FortiGuard и может блокировать вход с использованием украденных идентификаторов. Подписка на облачный сервис FortiSandbox Cloud позволяет FortiWeb интегрироваться с облачным сервисом-песочницей от Fortinet для глубокого анализа поведения подозрительных файлов.

Поддержка публичных и частных облаков

FortiWeb максимально гибок с точки зрения поддержки инфраструктуры публичных и частных облаков. Виртуальные FortiWeb поддерживают все функции аппаратной реализации и доступны в средах виртуализации VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, Docker, AWS, Azure, Google Cloud, а также как сервис WAF в AWS, Azure и Google Cloud. Подробнее на портале fortiweb-cloud.com.

Интерфейс FortiView для FortiWeb

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Варианты развертывания
- Обратный прокси-сервер (Reverse Proxy)
- Прозрачный режим «в разрыв» (Inline Transparent)
- Расширенный прозрачный режим (True Transparent Proxy)
- Анализ копии трафика (Offline Sniffing)
- WCCP (протокол перенаправления контента)

Веб-безопасность
- Машинное обучение на основе искуственного интеллекта
- Автоматическое профилирование (белый список)
- Веб-сервер и сигнатуры приложений (черный список)
- Репутация IP
- Геолокация IP
- Соответствие RFC HTTP
- Встроенная поддержка HTTP/2
- Поддержка спецификации OpenAPI 3.0
- Защита WebSocket с применением сигнатур
- Защита от атак Man in the Browser (MiTB)

Защита приложений от атак
- 10 наиболее распространенных угроз по версии OWASP
- Межсайтовые сценарии
- Внедрение SQL-кода
- Межсайтовая подделка запроса
- Перехват сеанса
- Встроенный сканер уязвимостей
- Интеграция со сканерами сторонних производителей (виртуальные патчи)
- Сканирование загружаемых файлов с помощью антивируса и песочницы

Службы безопасности
- Сигнатуры веб-сервисов
- Соответствие форматам XML и JSON
- Обнаружение вредоносного ПО
- Виртуальные патчи
- Валидация протокола
- Защита от атак методом перебора
- Подпись и шифрование файлов cookie
- Обнаружение внедрения SQL-кода
- Защита заголовка HTTP
- Обработка кодов возврата и информации об ошибках
- Сигнатуры атак на операционную систему
- Защита от известных угроз и атак нулевого дня
- Межсетевой экран с контролем состояния сеансов L4
- Предотвращение DoS-атак
- Корреляция событий безопасности
- Защита от утечки данных (DLP)
- Защита от искажения внешнего вида веб-сайта

Доставка приложений
- Балансировка нагрузки L7
- Перезапись URL-адресов
- Маршрутизация контента
- HTTPS/SSL Offloading (перенос HTTPS/SSL на FortiWeb)
- Сжатие HTTP
- Кэширование

Authentication
- Явная и прозрачная аутентификация
- Публикация сайта и использование технологии единого входа (SSO)
- Доступ с использованием криптографического алгоритма RSA для двухфакторной аутентификации
- Поддержка протоколов LDAP, RADIUS и SAML
- Поддержка SSL-сертификата клиента
- Тест Капча и функция Real Browser Enforcement (RBE) (принудительное подтверждение реального браузера)

Управление и отчетность
- Веб-интерфейс управления
- Интерфейс командной строки
- Инструменты графического анализа и отчетности
- Централизованное управление несколькими устройствами FortiWeb
- Кластеризация высокой доступности активный/активный
- Поддержка API для управления
- Централизованный сбор логов и отчетность
- Отслеживание пользователя/устройства
- Панели мониторинга в режиме реального времени
- Панель мониторинга ботов
- Анализ геолокации IP
- Поддержка протоколов SNMP, Syslog, SMTP
- Административные домены с ролевой моделью контроля доступа

Другое
- Поддержка протокола IPv6
- Конвертация HTTP/2 в HTTP 1.1
- Поддержка аппаратного модуля безопасности (HSM)
- Поддержка инфраструктуры открытых ключей (PKI)
- Сканирование вложений для приложений ActiveSync/MAPI, веб-клиента OWA и протокола FTP
- Высокая доступность с синхронизацией конфигурации по активным устройствам
- Параметры автоматической настройки и конфигурации по умолчанию для упрощенного развертывания
- Преднастроенные шаблоны для Microsoft Exchange, SharePoint, OWA, Drupal, Wordpress
- Поддержка OpenStack для виртуальных машин FortiWeb
- Поддержка протокола WebSocket

ХАРАКТЕРИСТИКИ



	FORTIWEB 100E	FORTIWEB 400E	FORTIWEB 600E
Параметры оборудования			
Интерфейсы 10/100/1000 (RJ-45)	4	4 GE RJ45, 4 SFP GE	4 GE RJ45 (2 bypass), 4 SFP GE
Порты 10G BASE-SR SFP+	—	—	—
Обработка SSL/TLS	Программная	Программная	Программная
USB интерфейсы	2	2	2
Объем диска	32 Гбайт SSD	480 Гбайт SSD	480 Гбайт SSD
Исполнение	Desktop	1U	1U
Блок питания	Один	Один	Два
Производительность системы			
Пропускная способность	50 Мбит/с	250 Мбит/с	750 Мбит/с
Задержка	<5мс	<5мс	<5мс
Высокая доступность	Кластеризация Активный/Пассивный, Активный/Активный	Кластеризация Активный/Пассивный, Активный/Активный	Кластеризация Активный/Пассивный, Активный/Активный
Лицензии на приложение	Неограниченные	Неограниченные	Неограниченные
Административные домены	—	32	32
Все указанные величины являются максимальными и могут изменяться в зависимости от конфигурации системы.			
Габариты			
Высота x Ширина x Длина (дюймы)	1.61 × 8.27 × 5.24	1.73 × 17.24 × 16.38	1.73 × 17.24 × 16.38
Высота x Ширина x Длина (мм)	41 × 210 × 133	44 × 438 × 416	44 × 438 × 416
Высота	2.3 фунта (1.1 кг)	22 фунта (9.97 кг)	22 фунта (9.97 кг)
Монтаж в стойку	Дополнительно	Да	Да
Условия эксплуатации			
Требования к электропитанию	100–240В~, 50–60 Гц	100–240 В~, 50–60 Гц	100–240 В~, 50–60 Гц
Максимальный ток	110V/1.2A, 220V/1.2A	100V/5A, 240V/3A	100V/5A, 240V/3A
Потребляемая мощность (средняя)	18 Вт	109 Вт	109 Вт
Тепловыделение	74 БТЕ/ч	446.3 БТЕ/ч	446.3 БТЕ/ч
Рабочая температура	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
Температура хранения	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)
Влажность	10–90% без конденсата	10–90% без конденсата	10–90% без конденсата
Соответствие требованиям			
Сертификаты безопасности	FCC Class A Part 15, RCM, VCCI, CE, UL/cUL, CB	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL

ХАРАКТЕРИСТИКИ




	FORTIWEB 1000E	FORTIWEB 2000F	FORTIWEB 3000F	FORTIWEB 4000F
Параметры оборудования				
Интерфейсы 10/100/1000 (RJ-45)	6 (4 bypass), 4x SFP GE (non-bypass)	4GE (4 bypass), 4 SFP GE	8 GE (bypass)	8 GE (bypass)
Порты 10G BASE-SR SFP+	2	4	10 (2 bypass)	10 (2 bypass)
Порты 40G QSFP	–	–	–	2 bypass
Обработка SSL/TLS	Аппаратная	Аппаратная	Аппаратная	Аппаратная
USB интерфейсы	2	2	2	2
Объем диска	2× 1 Тбайт	2×480 Гбайт SSD	2× 960 Гбайт SSD	2× 960 Гбайт SSD
Исполнение	2U	2U	2U	2U
Блок питания	Два с горячей заменой	Два с горячей заменой	Два с горячей заменой	Два с горячей заменой
Производительность системы				
Пропускная способность	1.3 Гбит/с	5 Гбит/с	10 Гбит/с	70 Гбит/с
Задержка	<5мс	<5мс	<5мс	<5мс
Высокая доступность	Кластеризация Активный/Пассивный, Активный/Активный	Кластеризация Активный/Пассивный, Активный/Активный	Кластеризация Активный/Пассивный, Активный/Активный	Кластеризация Активный/Пассивный, Активный/Активный
Лицензии на приложение	Неограниченные	Неограниченные	Неограниченные	Неограниченные
Административные домены	64	96	96	192
Все указанные величины являются максимальными и могут изменяться в зависимости от конфигурации системы.				
Габариты				
Высота x Ширина x Длина (дюймы)	3.46 × 16.93 × 19.73	3.5 × 17.2 × 20.8	3.5 × 17.5 × 22.6	3.5 × 17.5 × 22.6
Высота x Ширина x Длина (мм)	88 × 430 × 501.20	88 × 438 × 530	88 × 444 × 574	88 × 444 × 574
Высота	28 фунта (12.8 кг)	33 фунта (15 кг)	56.2 фунта (22.5 кг)	56.2 фунта (22.5 кг)
Монтаж в стойку	Да	Да	Да	Да
Условия эксплуатации				
Требования к электропитанию	100–240 В~, 50–60 Гц	100–240 В~, 60–50 Гц	100–240 В~, 60–50 Гц	100–240 В~, 60–50 Гц
Максимальный ток	100В/5А, 240В/3А	120В/6А, 240В/3А	120В/2.6А, 240В/1.3А	120В/3А, 240В/1.5А
Потребляемая мощность (средняя)	140 Вт	200 Вт	200 Вт	248.5 Вт
Тепловыделение	471 БТЕ/ч	1433 БТЕ/ч	1045.5 БТЕ/ч	1219.8 БТЕ/ч
Рабочая температура	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
Температура хранения	-4–158°F (-20–70°C)	-4–158°F (-20–70°C)	-4–158°F (-20–70°C)	-4–158°F (-20–70°C)
Влажность	5–90% без конденсата	5–90% без конденсата	5–90% без конденсата	5–90% без конденсата
Соответствие требованиям				
Сертификаты безопасности	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL

ХАРАКТЕРИСТИКИ

ВИРТУАЛЬНЫЕ МАШИНЫ	FORTIWEB-VM (1 VCPU)	FORTIWEB-VM (2 VCPU)	FORTIWEB-VM (4 VCPU)	FORTIWEB-VM (8 VCPU)
Производительность системы				
Пропускная способность для HTTP	25 Мбит/с	100 Мбит/с	500 Мбит/с	3 Гбит/с
Лицензии на приложение	Неограниченные	Неограниченные	Неограниченные	Неограниченные
Административные домены	от 4 до 64 в зависимости от объема выделенной памяти			
Виртуальная машина				
Поддержка гипервизоров	VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and Oracle Cloud. Please see FortiWeb VM Installation Guide for versions supported.			
Поддержка vCPU (Мин./ Макс.)	1	2	2 / 4	2 / 8
Поддержка сетевых интерфейсов (Мин./ Макс.)	1 / 10	1 / 10	1 / 10	1 / 10
Размер дисковой подсистемы (Мин./ Макс.)	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB
Оперативная память (Мин./ Макс.)	1,024 Мба1т / Неограниченная для 64-бит	1,024 Мба1т / Неограниченная для 64-бит	1,024 Мба1т / Неограниченная для 64-бит	1,024 Мба1т / Неограниченная для 64-бит
Рекомендованный объем оперативной памяти	8 Гбайт	8 Гбайт	8 Гбайт	8 Гбайт
Поддержка высокой доступности	Да	Да	Да	Да

Указанные значения могут изменяться в зависимости от параметров сетевого трафика и конфигурации системы. Фактические показатели были получены при использовании сервера Dell PowerEdge R710 (2 процессора Intel Xeon E5504, 2,0 ГГц, Кэш 4 Мбайт), с установленной платформой VMware ESXi 5.5, включающего в себя оперативную память (vRAM) на 4 Гбайт для FortiWeb Virtual Appliance на 4 и 8 виртуальных процессоров, и оперативную память (vRAM) на 4 Гбайт для FortiWeb Virtual Appliance на 2 виртуальных процессора.

УСТРОЙСТВА В ВИДЕ КОНТЕЙНЕРА	FORTIWEB-VMC01	FORTIWEB-VMC02	FORTIWEB-VMC04	FORTIWEB-VMC08
Производительность системы				
Пропускная способность для HTTP (макс.)	25 Мбит/с	100 Мбит/с	500 Мбит/с	3 Гбит/с
Лицензии на приложение	Неограниченные	Неограниченные	Неограниченные	Неограниченные
Административные домены	от 4 до 64 в зависимости от объема выделенной памяти			
Виртуальная машина				
Поддержка ПО контейнеризации	Docker			
Поддержка сетевых интерфейсов (Мин./ Макс.)	1 / 10	1 / 10	1 / 10	1 / 10
Размер дисковой подсистемы (Мин./ Макс.)	30 Гбайт / 500 Гбайт	30 Гбайт / 500 Гбайт	30 Гбайт / 500 Гбайт	30 Гбайт / 500 Гбайт
Оперативная память (Мин./ Макс.)	4 Гбайт	4 Гбайт	4 Гбайт	4 Гбайт
Рекомендованный объем оперативной памяти	8 Гбайт	8 Гбайт	8 Гбайт	8 Гбайт
Поддержка высокой доступности	Нет	Нет	Нет	Нет

Производительность и другие показатели представляют собой максимальные значения, разрешенные для каждой версии. Фактические указанные величины могут изменяться в зависимости от сетевого трафика и конфигурации системы.

ИНФОРМАЦИЯ ДЛЯ ЗАКАЗА

Продукт	Код товара (SKU)	Описание
FortiWeb 100E	FWB-100E	Межсетевой экран для веб-приложений — порты 4x GE RJ45, память 4 Гбайт RAM, 1 SSD диск x 32 Гбайт.
FortiWeb 400E	FWB-400E	Межсетевой экран для веб-приложений — порты 4x GE RJ45, 4x GE SFP, 480 Гбайт SSD.
FortiWeb 600E	FWB-600E	Межсетевой экран для веб-приложений — порты 4x GE RJ45 (2x bypass), 4x GE SFP, 480 Гбайт SSD.
FortiWeb 1000E	FWB-1000E	Межсетевой экран для веб-приложений — порты 2× 10 GE SFP+, 2x GE RJ45, 4x GE RJ45 bypass, 4x GE SFP, два блока питания, 2 Тбайт хранилище.
FortiWeb 2000F	FWB-2000F	Межсетевой экран для веб-приложений — порты 4 × 10GE SFP+, 4 x GE RJ45 bypass, 4 x GE SFP, 2 x GE порта управления, два блока питания, 2×480 Гбайт SSD.
FortiWeb 3000F	FWB-3000F	Межсетевой экран для веб-приложений — порты 10 × 10GE SFP+ (2 bypass), 8 x GE RJ45 bypass, 2 x GE порта управления, два блока питания, 2×960 Гбайт SSD.
FortiWeb 4000F	FWB-4000F	Межсетевой экран для веб-приложений — порты 2 × 40GE bypass, 10 × 10GE SFP+ (2 bypass), 8 x GE RJ45 bypass, 2 x GE порта управления, два блока питания, 2×960 Гбайт SSD.
FortiWeb-VM01	FWB-VM01	FortiWeb-VM, поддержка 1 vCPU и 64-бит операционной системы.
FortiWeb-VM02	FWB-VM02	FortiWeb-VM, поддержка до 2 vCPU и 64-бит операционной системы.
FortiWeb-VM04	FWB-VM04	FortiWeb-VM, поддержка до 4 vCPU и 64-бит операционной системы.
FortiWeb-VM08	FWB-VM08	FortiWeb-VM, поддержка до 8 vCPU и 64-бит операционной системы.
FortiWeb-VMC01	FWB-VMC01	FWB-VMC01 для сред на базе контейнеров. Пропускная способность до 25 Мбит/с.
FortiWeb-VMC02	FWB-VMC02	FWB-VMC02 для сред на базе контейнеров. Пропускная способность до 100 Мбит/с.
FortiWeb-VMC04	FWB-VMC04	FWB-VMC04 для сред на базе контейнеров. Пропускная способность до 500 Мбит/с.
FortiWeb-VMC08	FWB-VMC08	FWB-VMC08 для сред на базе контейнеров. Пропускная способность до 2 Гбит/с.
Central Manager 10	FWB-CM-BASE	Лицензия FortiWeb Central Manager, управление максимум 10 устройствами FortiWeb, VMware vSphere.
Central Manager Unlimited	FWB-CM-UL	Лицензия FortiWeb Central Manager, управление неограниченным количеством устройств FortiWeb, VMware vSphere.

Ниже приведены SKUs для схемы лицензирования по срочной подписке:

Product	SKU	Description
FortiWeb-VM01-S Standard	FC1-10-WBVMS-916-02-DD	Подписка на FortiWeb-VM (1 CPU) со стандартным набором сервисов безопасности.
FortiWeb-VM01-S Advanced	FC1-10-WBVMS-633-02-DD	Подписка на FortiWeb-VM (1 CPU) со расширенным набором сервисов безопасности.
FortiWeb-VM02-S Standard	FC2-10-WBVMS-916-02-DD	Подписка на FortiWeb-VM (2 CPU) со стандартным набором сервисов безопасности.
FortiWeb-VM02-S Advanced	FC2-10-WBVMS-633-02-DD	Подписка на FortiWeb-VM (2 CPU) со расширенным набором сервисов безопасности.
FortiWeb-VM04-S Standard	FC3-10-WBVMS-916-02-DD	Подписка на FortiWeb-VM (4 CPU) со стандартным набором сервисов безопасности.
FortiWeb-VM04-S Advanced	FC3-10-WBVMS-633-02-DD	Подписка на FortiWeb-VM (4 CPU) со расширенным набором сервисов безопасности.
FortiWeb-VM08-S Standard	FC4-10-WBVMS-916-02-DD	Подписка на FortiWeb-VM (8 CPU) со стандартным набором сервисов безопасности.
FortiWeb-VM08-S Advanced	FC4-10-WBVMS-633-02-DD	Подписка на FortiWeb-VM (8 CPU) со расширенным набором сервисов безопасности.