FortiSandbox™

FortiSandbox 500F, 1000D, 2000E, 3000E, 3500D, виртуальная машина (VM), частная и общедоступная облачная сеть

Ключевым компонентом является продукт FortiSandbox («песочница») от компании Fortinet в составе решения Advanced Threat Protection (защита от продвинутых угроз) (ATP), которое интегрируется с архитектурой информационной безопасности Fortinet Security Fabric для противодействия быстроразвивающимся и таргетированным и цифровым атакам. В частности, FortiSandbox обеспечивает оперативное предоставление информации об угрозах в режиме реального времени благодаря автоматизации обнаружения и подавления уязвимостей нулевого дня и продвинутых вредоносных программ.

Полный охват всех видов атак с использованием Fortinet Security Fabric

Эффективная защита от продвинутых таргетированных атак посредством единой расширяемой архитектуры, предназначенной для защиты сетей, электронной почты, веб-приложений и конечных точек от предприятия до облака.

Обнаружение и подавление уязвимостей нулевого дня, продвинутых вредоносных программ

Встроенная интеграция и открытые интерфейсы прикладного программирования (API) обеспечивают автоматизированную передачу объектов от устройств Fortinet и точек защиты сторонних поставщиков, а также совместное использование данных об угрозах в режиме реального времени для немедленного реагирования на угрозу и снижения зависимости от недостаточных ресурсов безопасности.

Сертификация и высокие показатели

Постоянно подвергается строгому независимому тестированию в реальных условиях и стабильно получает высшие оценки в отношении известных и неизвестных угроз.

Режимы развертывания

- Изолированный режим (Standalone)
- Режим интеграции (Integrated)

Круглосуточная техническая поддержка службы FortiCare по всему миру

- support.fortinet.com

Службы безопасности FortiGuard

- www.fortiguard.com

Сертификаты сторонних организаций

ХАРАКТЕРИСТИКИ

Анализ вредоносных программ в «песочнице»

Дополнение организованной защиты с помощью двухэтапного анализа в «песочнице». Подозрительные файлы и файлы, находящиеся в группе риска, подвергаются первому этапу анализа с помощью отмеченного наградами антивирусного сканирования (AV engine) от компании Fortinet, глобального запроса данных об угрозах FortiGuard* и эмуляции кода. Второй этап анализа выполняется в замкнутой среде, с тем чтобы выявить полный жизненный цикл атаки с использованием действий операционной системы и обнаружением обратного вызова. На *Рис. 1* показаны новые угрозы, обнаруженные в режиме реального времени.

Помимо поддержки продуктов FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (агент ATP) и продуктов партнеров в рамках программы Fabric-Ready Partner, обеспечивается поддержка сторонних поставщиков услуг безопасности с помощью четко определенного набора открытых интерфейсов прикладного программирования (API).

Рис. 1: Панель мониторинга статуса угрозы на основе виджета

* в режиме реального времени проверка индикаторов компрометации (IoC) возникающих угроз (заведомо хороших и плохих) осуществляется в рамках информационно-аналитического сервиса FortiGuard

Инструменты для отчета и анализа

Отчеты с перехваченными пакетами, исходным файлом, журналом трассировки и скриншотами предоставляют обширную информацию об угрозах и важнейшие сведения после просмотра файлов (см. *Рис. 2*). Ускоряют восстановление.

Рис. 2: Подробный отчет о вредоносных программах с помощью встроенных инструментов

Подавление угроз

Способность различных продуктов от компании Fortinet к интеграции с FortiSandbox («песочницей») посредством Fortinet Security Fabric обеспечивает автоматическую защиту с исключительно простой настройкой. После идентификации вредоносного кода «песочница» (FortiSandbox) выполняет возврат показателей рисков, а местные данные об угрозах используются в режиме реального времени совместно с устройствами от компании Fortinet, устройствами от сторонних зарегистрированных поставщиков и клиентами для устранения и предотвращения новых продвинутых угроз. Местные данные об угрозах могут совместно использоваться исследовательской группой Fortinet и командой специалистов FortiGuard Labs для обеспечения глобальной защиты организаций. На *Рис. 3* показаны этапы выполнения автоматизированного процесса подавления угроз.

Запрос

1 Передача файла на анализ, возвращение результатов

Подавление

2a Блокировка объектов на устройстве передачи файла или помещение файлов в карантин в конечной точке

2b Помещение в карантин конечных точек

2c Дальнейшее исследование и реагирование

Update

3a Совместное использование индикаторов компрометации (IoC) на интегрированных устройствах

3b Дополнительный совместный анализ службами FortiGuard

4 Усовершенствованная защита всех пользователей/устройств

Рис. 3: Процесс подавления угрозы в FortiSandbox («песочнице»)

ВАРИАНТЫ РАЗВЕРТЫВАНИЯ

Простое развертывание

FortiSandbox представляет собой единое решение, поддерживающее проверку множества протоколов, что упрощает инфраструктуру сети и операции. Кроме того, FortiSandbox интегрируется в архитектуру Fortinet Security Fabric, добавляя уровень защиты от продвинутых угроз в существующую архитектуру безопасности пользователя.

FortiSandbox представляет собой самый гибкий инструмент анализа угроз на рынке, поскольку он предлагает различные варианты развертывания в соответствии с уникальной конфигурацией и требованиями пользователей. Организации могут комбинировать варианты развертывания устройства.

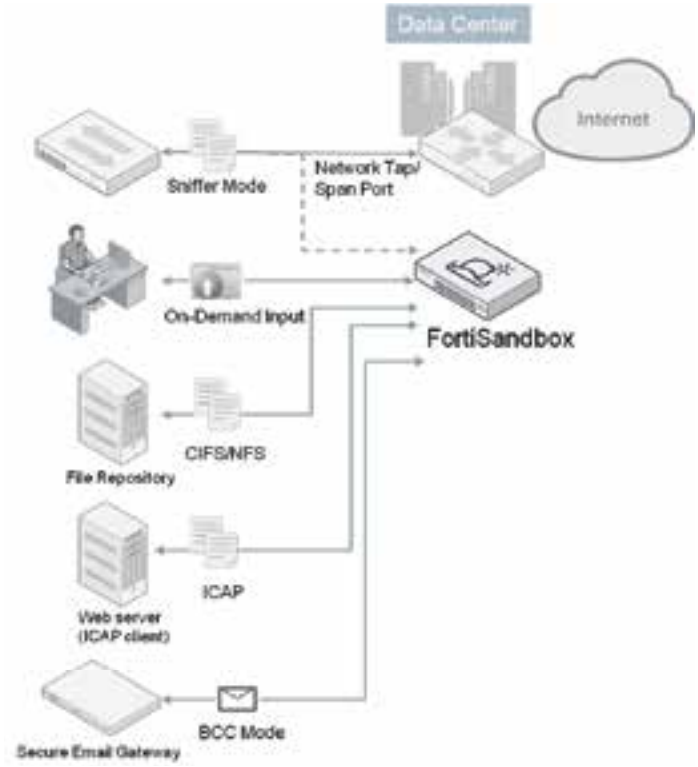


Рис. 4: Развертывание в изолированном режиме (Standalone)

Изолированный режим (Standalone)

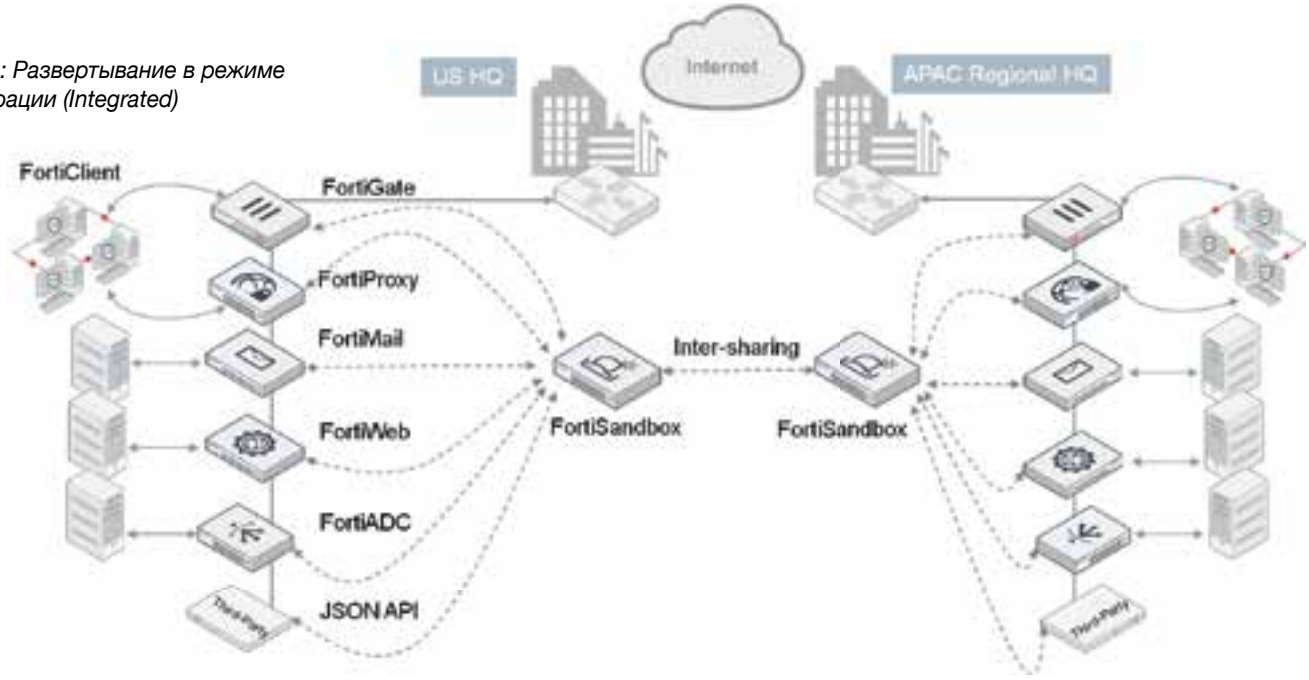
В данном режиме развертывания «песочница» FortiSandbox принимает входные сигналы как сервер, реализующий протокол ICAP (Протокол проверки и контроля трафика), или через подключенные порты коммутатора или сетевые отводы. В данном режиме администратор также может загружать или сканировать файлы из репозитория файлов через протокол файлового доступа CIFs или NFS с помощью графического интерфейса. Данный вариант является идеальным для усовершенствования существующей процедуры защиты от угроз в случае с несколькими поставщиками.

Режим интеграции (Integrated)

Такие продукты компании Fortinet, как FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy и FortiClient (поставщик ATP), а также продукты сторонних поставщиков услуг безопасности могут перехватывать и передавать FortiSandbox подозрительный контент в том случае, когда их конфигурация позволяет взаимодействовать с FortiSandbox. Интеграция обеспечивает своевременное восстановление и генерацию отчетности для этих устройств.

Также возможна интеграция с другими устройствами FortiSandbox для обеспечения мгновенного одновременного реагирования на данные об угрозах в режиме реального времени. Данное свойство удобно для крупных предприятий, развертывающих несколько устройств FortiSandbox в разных филиалах. Данная модель автоматического развертывания идеально подходит для глобальной защиты вне зависимости от государства и часового пояса.

Рис. 5: Развертывание в режиме интеграции (Integrated)



ХАРАКТЕРИСТИКИ

Администрирование

Поддержка конфигурации веб-интерфейса пользователя (WebUI) и интерфейса командной строки (CLI)

Создание нескольких учетных записей администратора

Резервное копирование и восстановление файла конфигурации

Электронное письмо с уведомлением при обнаружении вредоносного файла

Еженедельный отчет для глобального списка адресов электронной почты и администраторов FortiGate

Страница централизованного поиска, которая позволяет администраторам создавать индивидуальные условия поиска

Частые автоматические обновления сигнатур

Автоматическая проверка и загрузка новых изображений виртуальной машины

Мониторинг состояния виртуальной машины

Аутентификация Radius для администраторов

Сеть/развертывание

Поддержка статической маршрутизации

Ввод файла: Онлайн режим/режим анализатора трафика, загрузка файлов по запросу, передача файла из интегрированного устройства (в)

Возможность создания моделируемой сети для сканирования файла доступа к среде закрытой сети

Поддержка кластеризации высокой доступности

Проверка портов на самовосстановление в кластере

Интеграция систем

Ввод передаваемого файла: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy и FortiClient (агент ATP)

Обратная связь и отчет с информацией о статусе файла: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy и FortiClient (агент ATP)

Динамическое обновление базы данных угроз: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy и FortiClient (агент ATP)
- Периодическая рассылка динамической базы данных зарегистрированным организациям
- Контрольная сумма файла и база данных с вредоносными URL-адресами

Обновление прокси-сервера базы данных: FortiManager

Дистанционная регистрация данных: FortiAnalyzer, сервер syslog

Интерфейс обмена данными JSON API для автоматизации процесса загрузки образцов и выгрузки действующих индикаторов вредоносных программ для восстановления

Интеграция с сертифицированными сторонними организациями: CarbonBlack, Ziften, SentinelOne

Совместное использование индикаторов компрометации (IoC) устройствами FortiSandbox

Защита от продвинутых атак

Проверка новых угроз, включая вредоносные программы, целью которых является вымогательство, и подавление вредоносных программ, защищенных паролем

Статический анализ кода, определяющий возможные угрозы в невыполняемом коде

Эвристический/характеристический/репутационный анализ

«Песочница» с виртуальной операционной системой
- Одновременные экземпляры
- Поддерживаемый тип операционной системы: Windows XP*, Windows 7, Windows 8.1, Windows 10, macOS и Android
- Техники обхода Anti-evasion: вызовы в спящем режиме, процессы и запросы реестров
- Обнаружение обратного вызова: переход по ссылке вредоносного URL-адреса, взаимодействие с ботнет-сетями (управление и контроль), трафик злоумышленников посредством активированного вредоносного программного обеспечения
- Выгрузка перехваченных пакетов, исходного файла, журнала трассировки и скриншотов
- Интерактивный режим «песочницы»

* Поддерживается в виртуальной машине пользователя

Поддержка типов файлов: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip

Поддержка протоколов/приложений:
- Режим анализатора трафика: HTTP, FTP, POP3, IMAP, SMTP, SMB
- Режим скрытой копии (BCC): SMTP
- Режим интеграции с FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM и аналогичные версии с шифрованием SSL
- Режим интеграции с FortiMail: SMTP, POP3, IMAP
- Режим интеграции с FortiWeb: HTTP
- Режим интеграции с ICAP клиент HTTP

Настройка виртуальных машин для поддержки различных типов файлов

Трафик изображения виртуальной машины изолирован от системного трафика

Обнаружение угроз сети в режиме анализатора трафика: Идентификация действий ботнет, сетевые атаки, переход по ссылке вредоносного URL-адреса

Сканирование протоколов SMB/NFS общей сети и помещение подозрительных файлов в карантин. Сканирование может проводиться с определенными интервалами

Сканирование URL-адресов, встроенных внутрь текстовых файлов

Возможность интеграции с Yara-правилами сторонних организаций

Возможность автоматической передачи подозрительных файлов в облачную службу для ручного анализа и создания сигнатуры

Возможность пересылки файлов в общую сеть для дальнейшего сканирования сторонними организациями

Возможность использования белых и черных списков с контрольными суммами файлов

Передача URL-адресов для сканирования и запроса из электронных писем и файлов

Мониторинг и отчеты

Виджеты мониторинга в режиме реального времени (возможность просмотра на основании источника и периода времени): Scanning result statistics, scanning activities (в течение выбранного периода времени), top targeted hosts, top malware, top infectious urls, top callback domains

Средство просмотра для детализации событий: Динамическая таблица с информацией о событии, имени вредоносной программы, рейтинге, типе, источнике, месте назначения, времени обнаружения и пути загрузки

Регистрация данных – графический интерфейс, загрузка файла журнала в формате RAW (необработанный файл)

Генерация отчета по вредоносным файлам: Подробные отчеты о характеристиках и поведении файлов – изменение файла, поведение процесса, поведение реестра, поведение сети, снимок файловой системы (снапшот) виртуальной машины, диаграмма хронологии поведения

Дополнительный анализ: Загружаемые файлы – образец файла, журналы трассировки «песочницы», перехват с использованием библиотеки PCAP и индикаторы в формате STIX

ХАРАКТЕРИСТИКИ

	FSA-500F	FSA-1000D	FSA-2000E
Аппаратное обеспечение			
Исполнение	1U	2U	2U
Количество сетевых интерфейсов	Порты 4x GE RJ45	Порты 6x GE RJ45, слоты 2x GE SFP	Порты 4x GE RJ45, слоты 2x 10 GE SFP+
Встроенная память	1x 1 Тбайт	2x 2 Тбайт	2x 2 Тбайт
Источники питания	1x источник питания	2x резервных источника питания	2x резервных источника питания
Производительность системы			
Кол-во виртуальных машин	6***	8	24***
Пропускная способность в ходе предварительной фильтрации в «песочнице» (файл/час)[1]	4500	6000	12000
Пропускная способность виртуальной «песочницы» (файл/час)	120	160	480
Эффективная пропускная способность в реальных условиях (файл/час)	6002, 3603	8002, 4803	24002, 14403
Пропускная способность анализатора трафика	500 Мбит/с	1 Гбит/с	4 Гбит/с
Размеры			
Высота × ширина × длина (дюймы)	1,73 x 17,24 x 12,63	3,5 x 17,2 x 14,5	3,46 x 17,24 x 20,87
Высота × ширина × длина (мм)	44 x 438 x 320	89 x 437 x 368	88 x 438 x 530
Вес	18,72 фунта (8,5 кг)	27,60 фунта (12,52 кг)	27 фунтов (12,25 кг)
Условия эксплуатации			
Потребляемая мощность (средняя/максимальная)	30,1 / 76,3 Вт	115 / 138 Вт	164,7 / 175,9 Вт
Максимальный ток	100 В / 8 А, 240 В / 4 А	100 В / 5 А, 240 В / 3А	100 В / 8 А, 240 В / 4 А
Тепловыделение	260,34 БТЕ/ч	471 БТЕ/ч	600,17 БТЕ/ч
Источник питания	100–240 В~, 60–50 Гц	100–240 В~, 60–50 Гц	100–240 В~, 60–50 Гц
Влажность	От 5 до 90 % (без конденсата)	От 5 до 95 % (без конденсата)	От 5 до 90 % (без конденсата)
Диапазон рабочей температуры	32…104 °F (0…40 °C)	32…104 °F (0…40 °C)	32…104 °F (0…40 °C)
Диапазон температуры хранения	-4…158 °F (-20…70 °C)	-13…158 °F (-25…70 °C)	-4…158 °F (-20…70 °C)
Совместимость			
Сертификация	FCC часть 15 класс A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, ГОСТ		

	FSA-3000E	FSA-3500D
Аппаратное обеспечение		
Исполнение	2U	3U (5 узлов предусмотрено по умолчанию, 8 узлов максимум)
Количество сетевых интерфейсов	Порты 4x GE RJ45, слоты 2x 10 GE SFP+	Порты 20x GE RJ45, слоты 10x 10 GE SFP+ (Порты 4x GE RJ45, слоты 2x 10 GE SFP+ на узел)
Встроенная память	4x 2 Тбайт	5x 2 Тбайт (2 Тбайт на узел)
Источники питания	2x резервных источника питания	2x резервных источника питания
Производительность системы		
Кол-во виртуальных машин	56***	36* (С возможностью расширения** до 60) (8 на узел)
Пропускная способность в ходе предварительной фильтрации в «песочнице» (файл/час)[1]	15000	30000* (С возможностью увеличения** до 48000) (6000 на узел)
Пропускная способность виртуальной «песочницы» (файл/час)	1120	720* (С возможностью увеличения** до 1200) (160 на узел)
Эффективная пропускная способность в реальных условиях (файл/час)	5600[2], 3360[3]	3600 (С возможностью увеличения** до 6000) (800 на узел)[2] 2160 (С возможностью увеличения до 3600) (480 на узел)[3]
Пропускная способность анализатора трафика	8 Гбит/с	2 Гбит/с
Размеры		
Высота × ширина × длина (дюймы)	3,5 x 17,2 x 29	5,2 x 17,5 x 29,5
Высота × ширина × длина (мм)	89 x 437 x 738	133 x 445 x 749
Вес	43 фунта (19,52 кг)	88 фунтов (39,92 кг)
Условия эксплуатации		
Потребляемая мощность (средняя /максимальная)	538,6 / 549,6 Вт	625 / 735,6 Вт
Максимальный ток	100 В / 9,8 А, 240 В / 5 А	12 А при 100 В / 12 А, 240 В / 8 А
Тепловыделение	1943,82 БТЕ/ч	2728,9 БТЕ/ч
Источник питания	100–240 В~, 60–50 Гц	100–240 В~, 60–50 Гц
Влажность	От 8 до 90 % (без конденсата)	От 8 до 90 % (без конденсата)
Диапазон рабочей температуры	50…95 °F (10…35 °C)	50…95 °F (10…35 °C)
Диапазон температуры хранения	-40…158 °F (-40…70 °C)	-40…158 °F (-40…70 °C)
Совместимость		
Сертификация	FCC Часть 15, Класс A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, ГОСТ	

Примечание: Все указанные величины являются максимальными и могут изменяться в зависимости от условий окружающей среды и конфигурации системы.

[1] Предварительная фильтрация в устройстве FortiSandbox осуществляется при поддержке информационно-аналитического сервиса FortiGuard.
[2] Измерения основаны на веб-трафике и трафике электронных писем в реальных условиях при последовательном использовании предварительной фильтрации и динамического анализа.
[3] Измерения основаны на трафике электронных писем в реальных условиях при последовательном использовании предварительной фильтрации и динамического анализа.

* На основании предположения, что 1 блейд-сервер будет использоваться в качестве первичного в режиме кластера с высокой доступностью
** При добавлении 3 и более узлов SAM-3500D на то же самое шасси
*** Лицензии включают в себя 2(FSA-500F)/4(FSA-2000E)/8(FSA-3000E) виртуальные машины Windows, в том числе аппаратное обеспечение, остальное приобретается в рамках расширения лицензии

ХАРАКТЕРИСТИКИ

	FORTISANDBOX-VM		FORTISANDBOX CLOUD
Требования к аппаратному обеспечению			
Поддержка гипервизора	VMware ESXi версия 5.1 или более поздняя, Linux KVM CentOS 7.2 или более поздняя версия, AWS (по запросу и с поддержкой собственных лицензий (BYOL))		Не применяется
Виртуальные процессоры (мин./макс.)	4/неограниченно (компания Fortinet рекомендует, чтобы количество процессоров соответствовало количеству виртуальных машин Windows +4)		Не применяется
Поддержка памяти (мин /макс.)	8 Гбайт / без ограничения		Не применяется
Объем виртуального хранилища (мин./макс.)	30 Гбайт/ 16 Тбайт		Не применяется
Количество виртуальных сетевых интерфейсов (мин.)	6		Не применяется
Производительность системы			
Пропускная способность анализатора трафика	1 Гбит/с		Не применяется
Пропускная способность в ходе предварительной фильтрации в «песочнице» (файл/час)[1]	В зависимости от аппаратного обеспечения		****
	Виртуальные машины для локальной сети	Виртуальные машины в облаке	
Кол-во виртуальных машин	8 виртуальных машин/узел, до 99 узлов/кластер	5 (до 200 виртуальных машин Windows в облаке)	****
Пропускная способность виртуальной «песочницы» (файл/час)	В зависимости от аппаратного обеспечения	100 (до 4000)	****
Эффективная пропускная способность в реальных условиях (файл/час)[2]	В зависимости от аппаратного обеспечения	500 (до 20 000)2, 300 (до 12 000)3	****

Примечание: Все указанные величины являются максимальными и могут изменяться в зависимости от условий окружающей среды и конфигурации системы.

[1] Предварительная фильтрация в устройстве FortiSandbox осуществляется при поддержке информационно-аналитического сервиса FortiGuard.
[2] Измерения основаны на веб-трафике и трафике электронных писем в реальных условиях при последовательном использовании предварительной фильтрации и динамического анализа.
[3] Измерения основаны на трафике электронных писем в реальных условиях при последовательном использовании предварительной фильтрации и динамического анализа.
****** См. описание облачного сервиса FortiSandbox.

FortiSandbox 500F

FortiSandbox 1000D

FortiSandbox 2000E

FortiSandbox 3000E

FortiSandbox 3500D

МАТРИЦА ИНТЕГРАЦИИ

		FORTIGATE	FORTICLIENT	FORTIMAIL	FORTIWEB	FORTIADC	FORTIPROXY
Устройство FSA и виртуальная машина	**Передача файла**	*OC FortiOS V5.0.4+	FortiClient для Windows OC V5.4+	FortiMail OC V5.1+	FortiWeb OC V5.4+	FortiADC OC V5.0+	FortiProxy OC V1.0+
	Обратная связь с информацией о статусе файла	*OC FortiOS V5.0.4+	FortiClient для Windows OC V5.4+	FortiMail OC V5.1+	FortiWeb OC V5.4+	FortiADC OC V5.0+	FortiProxy OC V1.0+
	Подробный отчет с информацией о файле	*OC FortiOS V5.4+	FortiClient для Windows OC V5.4+	FortiMail OC V5.1+	-	FortiADC OC V5.0+	FortiProxy OC V1.0+
	Динамическое обновление базы данных угроз	*OC FortiOS V5.4+	FortiClient для Windows OC V5.4+	FortiMail OC V5.3+	FortiWeb OC V5.4+	FortiADC OC V5.0+	FortiProxy OC V1.0+
FortiSandbox Cloud	**Передача файла**	*OC FortiOS V5.2.3+	-	FortiMail OC V5.3+	FortiWeb OC V5.5.3+	-	FortiProxy OC V1.0+
	Обратная связь с информацией о статусе файла	*OC FortiOS V5.2.3+	–	FortiMail OC V5.3+	FortiWeb OC V5.5.3+	–	FortiProxy OC V1.0+
	Подробный отчет с информацией о файле	*OC FortiOS V5.2.3+	–	–	–	–	FortiProxy OC V1.0+
	Динамическое обновление базы данных угроз	*OC FortiOS V5.4+	–	FortiMail OC V5.3+	FortiWeb OC V5.5.3+	–	FortiProxy OC V1.0+

*для некоторых режимов может потребоваться конфигурация интерфейса командной строки (CLI)

Информация для заказа

Изделие	Код товара (SKU)	Описание
FortiSandbox 500F	FSA-500F	Система Advanced Threat Protection (Система защиты от продвинутых угроз) – порты 4x GE RJ45, 2 лицензированные виртуальные машины, в комплект входят лицензии на Win7, Win10 и (1) MS office. С максимальной возможностью расширения до 6 виртуальных машин.
FortiSandbox 1000D	FSA-1000D	Система Advanced Threat Protection (Система защиты от продвинутых угроз) – порты 6x GE RJ45, слоты 2x GE SFP, резервный источник питания, 8 виртуальных машин, в комплект входят лицензии на Win7 и (1) MS Office. Соответствует TAA (закону о торговых соглашениях).
FortiSandbox 2000E	FSA-2000E	Система Advanced Threat Protection (Система защиты от продвинутых угроз) – порты 4x GE RJ45, слоты 2x 10 GE SFP+, резервный источник питания, 4 виртуальных машины, в комплект входят лицензии на Win7, Win8, Win10 и (1) MS Office. С максимальной возможностью расширения до 24 лицензированных виртуальных машин.
FortiSandbox 3000E	FSA-3000E	Система Advanced Threat Protection (Система защиты от продвинутых угроз) – порты 4x GE RJ45, слоты 2x 10 GE SFP+, резервный источник питания, 8 виртуальных машин, в комплект входят лицензии на Win7, Win8, Win10 и (1) MS Office. С максимальной возможностью расширения до 56 лицензированных виртуальных машин. Соответствует TAA (закону о торговых соглашениях).
FortiSandbox 3500D	FSA-3500D	Система Advanced Threat Protection (Система защиты от продвинутых угроз) – шасси 3U с 8 слотами и резервным источником питания, 5 блейд-серверов x SAM-3500D, порты 20x GE RJ45, слоты 10x 10 GE SFP+, 36 виртуальных машин, в комплект входят лицензии на WIn7, Win8, Win10 и (5) MS Office. С максимальной возможностью до 60 лицензированных виртуальных машин.
SandboxModule 3500D	SAM-3500D	Блейд-сервер Advanced Threat Protection (блейд-сервер защиты от продвинутых угроз) – порты 4x GE RJ45, слоты 2x 10 GE SFP+, 8 виртуальных машин, в комплект входят лицензии на Win7, Win8, Win10 и (1) MS Office.
FortiSandbox-VM	FSA-VM-00	Виртуальное устройство FortiSandbox-VM без виртуальных машин и с максимально возможным расширением до 8 виртуальных машин на узел, до 99 узлов на кластер.
FortiSandbox Windows Cloud VM	FC-10-FSA01-195-02-DD	Облачный сервис для виртуальных машин FortiSandbox Windows Cloud VM на (5) виртуальных машин Windows с максимально возможным расширением до (200) виртуальных машин Windows в облаке на одно виртуальное устройство FortiSandbox VM.
FortiSandbox macOS Cloud VM	FC-10-FSA01-192-02-DD	Облачный сервис для виртуальных машин macOS Cloud VM на (2) виртуальные машины macOS X с максимально возможным расширением до (8) виртуальных машин macOS X на устройство / виртуальную машину FortiSandbox.
FortiSandbox Cloud Service	FC-10-XXXXX-123-02-12	Подписка на облачный сервис Sandbox Cloud Service (код товара изменяется для различных моделей FortiGate/FortiMail/FortiProxy/FortiWeb).
Вспомогательное оборудование		
Модульный трансивер 1 GE SFP SX	FG-TRAN-SX	Модульный трансивер 1 GE SFP LX для всех систем со слотами SFP и SFP/SFP+.
Модульный трансивер 1 GE SFP LX	FG-TRAN-LX	Модульный трансивер 1 GE SFP LX для всех систем со слотами SFP и SFP/SFP+.
Модульный трансивер 10 GE SFP+ малой дальности	FG-TRAN-SFP+SR	Модульный трансивер 10 GE SFP+ малой дальности для всех систем со слотами SFP+ и SFP/SFP+.
Модульный трансивер 10 GE SFP+ большой дальности	FG-TRAN-SFP+LR	Модульный трансивер 10 GE SFP+ большой для всех систем со слотами SFP+ и SFP/SFP+.

ВСЕМИРНАЯ ШТАБ-КВАРТИРА
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States (США)
Тел.: +1.408.235.7700
www.fortinet.com/sales

ОФИС ПРОДАЖ В ЕВРОПЕ, НА БЛИЖНЕМ ВОСТОКЕ И В АФРИКЕ
905 rue Albert Einstein
Valbonne 06560
Alpes-Maritimes,
France (Франция)
Тел.: +33.4.8987.0500

ОФИС ПРОДАЖ В АЗИАТСКО-ТИХООКЕАНСКОМ РЕГИОНЕ
8 Temasek Boulevard
#12-01 Suntec Tower
Three
Singapore 038988
(Сингапур)
Тел.: +65.6395.2788

ОФИС В РОССИИ И СНГ
Пресненская
набережная д.10
Блок С 123317
Москва, Россия
www.fortinet.com/ru
russia@fortinet.com

FST-PROD-DS-GT1HS2 FG-100E-DAT-R12-201807