КОД безопасности

Средство защиты информации

vGate R2

Руководство администратора

Быстрый старт

RU.88338853.501410.012 91 3-1

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений

AD	Active Directory — служба каталогов MS Windows
DNS	Domain Name System (система доменных имен)
iSCSI	Internet Small Computer System Interface — протокол для управления системами хранения и передачи данных на основе TCP/IP
vCenter	Централизованное средство управления ESXi-серверами и виртуальными машинами
vCSA	vCenter Server Appliance — виртуальный модуль с установленным сервером vCenter и связанными с ним службами
PSC	Platform Services Controller — компонент, обеспечивающий работу служб виртуальной инфраструктуры VMware
АВИ	Администратор виртуальной инфраструктуры
АИБ	Администратор информационной безопасности
АС	Автоматизированная система
БД	База данных
ВМ	Виртуальная машина (англ. — VM)
Главный АИБ	Главный администратор информационной безопасности
ИБ	Информационная безопасность
КЦ	Контроль целостности
НСД	Несанкционированный доступ
ОС	Операционная система
ОЗУ	Оперативное запоминающее устройство
ПО	Программное обеспечение
ПРД	Правила разграничения доступа
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СХД	Система хранения данных (англ. — SAN)
ЦПУ	Центральное процессорное устройство

Введение

Актуальная версия эксплуатационной документации на изделие "Средство защиты информации vGate R2" находится на сайте компании по адресу https://www.securitycode.ru/products/vgate/.

Последнюю версию Release Notes можно запросить по электронной почте vgateinfo@securitycode.ru.

Данное руководство предназначено для администраторов изделия "Средство защиты информации vGate R2" RU.88338853.501410.012 (далее — vGate). В документе содержатся сведения, необходимые для первоначальной настройки и эксплуатации vGate.

Данное руководство предназначено для администраторов изделия "Средство защиты информации vGate R2" RU.88338853.501410.012 (далее — vGate). В документе содержатся сведения, необходимые для установки компонента vGate Service Pack 1.

Документ предназначен для vGate версии 4.5.

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.

- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.

- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в интернете. Вы можете посетить сайт компании "Код Безопасности" (https://www.securitycode.ru/) или связаться с представителями компании по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training-courses/.

Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Назначение vGate

vGate предназначен для обеспечения безопасности виртуальной инфраструктуры, развернутой с использованием системы виртуализации VMware vSphere.

Компоненты vGate

При развертывании компоненты vGate располагаются согласно схеме:

Компоненты vGate выполняют следующие функции.

Компонент	Функции
Сервер авторизации	Основной сервер авторизации выполняет следующие функции: • Аутентификация пользователей и компьютеров. • Разграничение доступа к средствам управления виртуальной инфраструктурой. • Хранение данных. • Регистрация событий безопасности. • Автоматическое развертывание компонентов защиты vGate на ESXi-серверах. • Репликация данных (при наличии резервного сервера)
Резервный сервер авторизации	При сбое основного сервера резервный сервер берет на себя все функции сервера авторизации. Осуществляет репликацию данных и хранение информации о пользователях и настройках
Агент аутентификации	Выполняет функцию идентификации и аутентификации пользователей и компьютеров
Компонент защиты ESXi-сервера	Выполняет контроль целостности ВМ и осуществляет защиту от НСД внутри сети администрирования. Контролирует целостность модулей и настроек vGate
Компонент защиты vCenter	Осуществляет управление фильтрацией входящего трафика и защиту от НСД внутри сети администрирования
Компонент защиты PSC	Осуществляет защиту от НСД внутри сети администрирования
Консоль управления	Осуществляет централизованное управление vGate
Веб-консоль	Позволяет выполнять централизованное управление vGate, настройку правил фильтрации сетевого трафика и осуществлять мониторинг событий безопасности через веб-интерфейс
Сервер мониторинга	Выполняет сбор и корреляцию событий виртуальной инфраструктуры
Сервер анализа	Выполняет анализ сетевого трафика виртуальных машин в рамках функции "Контроль прикладных протоколов"
Средство просмотра отчетов	Позволяет формировать отчеты о состоянии параметров безопасности виртуальной инфраструктуры, произошедших событиях и внесенных в конфигурацию изменениях
Служба развертывания vGate	Осуществляет установку агентов vGate на защищаемые ESXi-серверы

Ввод в эксплуатацию vGate

Для развертывания и настройки vGate:

1. Ознакомьтесь с ограничениями использования продукта (см. Release Notes).
2. Ознакомьтесь с требованиями к программному и аппаратному обеспечению (см. раздел "Системные требования" в документе [2]).
3. Настройте сеть администрирования, отделив ее от сети защищаемых компьютеров и сети виртуальных машин (см. раздел "Правила конфигурирования локальной сети" в документе [2]).
4. Выберите способ маршрутизации трафика (см. раздел "Настройка маршрутизации между подсетями" в документе [2]):
   - с помощью сервера авторизации;
   - с помощью отдельного маршрутизатора.
5. При необходимости подготовьте резервный сервер авторизации.
6. Выполните установку сервера авторизации vGate, консоли управления и средства просмотра отчетов (см. раздел "Установка и настройка сервера авторизации" в документе [2]).
7. При использовании резервирования выполните установку ПО vGate на резервном сервере авторизации (см. раздел "Установка и настройка сервера авторизации с резервированием" в документе [2]).
8. Установите компонент "Агент аутентификации" на компьютер АИБ.
9. Установите компонент "Агент аутентификации" на рабочем месте АВИ.
10. В консоли управления зарегистрируйте имеющуюся лицензию на использование vGate для защиты ESXi-серверов (см. раздел "Регистрация лицензии" в документе [2]).
11. Добавьте в список защищаемых объектов серверы vCenter и ESXi (см. раздел "Регистрация защищаемых серверов" в документе [2]).
12. Установите компоненты vGate на защищаемые серверы vCenter (vCSA) и ESXi (см. раздел "Развертывание компонентов защиты" в документе [2]).
13. Создайте учетные записи пользователей (см. раздел "Управление учетными записями пользователей" в документе [2]).
14. Настройте метки безопасности (см. раздел "Настройка меток безопасности" в документе [2]) и назначьте их учетным записям и объектам виртуальной инфраструктуры (см. раздел "Настройка полномочного управления доступом к конфиденциальным ресурсам" в документе [2]).
15. Назначьте наборы политик безопасности защищаемым объектам или группам объектов (см. раздел "Настройка политик безопасности" в документе [2]).
16. Настройте правила разграничения доступа к защищаемым серверам (см. раздел "Управление доступом к защищаемым серверам" в документе [2]).
17. Настройте правила фильтрации сетевого трафика между защищаемыми серверами (см. раздел "Сегментирование" в документе [2]).

Устранение неисправностей

Распространенные ошибки

Список проблем, которые могут возникнуть при работе с ПО vGate, и способы их решения находятся в документе Troubleshooting.html (расположен на установочном диске в папке \Documentation).
Особенности работы vGate и возможные ошибки описаны в документе ReleaseNotes.html (расположен на установочном диске в папке \Documentation\vSphere).

Ответы на вопросы

Данный раздел содержит список частых вопросов и ответы на них.

Вопрос	Ответ
В vGate 4.5 поддерживается работа с несколькими серверами vCenter?	Да. Для этого необходимо объединить серверы vCenter с помощью режима VMware vCenter Linked Mode
Как переустановить служебные учетные записи vGate 4.5 в Active Directory?	1. Удалите служебные учетные записи vGate из Active Directory. 2. Запустите программу установки сервера авторизации vGate. 3. В диалоге изменения параметров установки нажмите кнопку "Изменить" и следуйте указаниям мастера. Все текущие настройки vGate при этом сохраняются. 4. По окончании установки будут созданы новые служебные учетные записи vGate в Active Directory. 5. Отключите автоматическую смену паролей для служебных учетных записей
Почему установка агента аутентификации на компьютере в сети защищаемых серверов завершается ошибкой?	Установка агента аутентификации внутри защищаемого периметра не поддерживается (см. раздел "Конфигурирование локальной сети" в документе [2])

Документация

1.	Средство защиты информации vGate R2. Руководство администратора. Принципы функционирования	RU.88338853.501410.012 91 1-1
2.	Средство защиты информации vGate R2. Руководство администратора. Установка, настройка и эксплуатация	RU.88338853.501410.012 91 2-1
3.	Средство защиты информации vGate R2. Руководство администратора. Быстрый старт	RU.88338853.501410.012 91 3-1
4.	Средство защиты информации vGate R2. Руководство пользователя. Работа в защищенной среде	RU.88338853.501410.012 92 1