Автор:
30.11.14 18:24 -

Настройка локальной сети для решения vGate R2 for Hyper-V и использован

Автор: Александр Самойленко
Дата: 30/11/2014

Продолжаем вас знакомить с решением vGate R2 от компании Код Безопасности, предназначенным для защиты виртуальной инфраструктуры Hyper-V от несанкционированного доступа, а также для ее безопасной настройки средствами политик. В этой статье мы расскажем о том, как правильно настроить локальную сеть в соответствии с рефернсной архитектурой vGate, а также установить продукт с использованием различных конфигураций (способы маршрутизации и варианты развертывания с основным и резервным сервером).

Перед установкой сервера авторизации vGate R2

Чтобы обеспечить надежный уровень защиты, необходимо до установки компонентов vGate R2 выполнить конфигурирование сети, руководствуясь следующими правилами:

- Сеть администрирования виртуальной инфраструктуры и сеть виртуальных машин рекомендуется отделить от остальных сетей ИТ-инфраструктуры.
- Если в виртуальной инфраструктуре используются функции динамической миграции (Live Migrations) и репликации, то рекомендуется организовать отдельную сеть репликации виртуальных машин, отделив ее от сетей администрирования и сетей виртуальных машин.
- Если данные виртуальных машин хранятся за пределами серверов Hyper-V в отдельной системе хранения, то рекомендуется создать сеть передачи данных на основе технологии Ethernet (iSCSI) или SMB 3.0. При необходимости сеть передачи данныхи сеть репликации виртуальныхмашин могут быть совмещены.

Для работы в сети, сконфигурированной таким образом, серверы Hyper-V должны иметь необходимое число независимых Ethernet-интерфейсов.

Если вы будете вводить сервер авторизации в домен Active Directory, выполните следующие рекомендации:

- Не размещайте контроллер домена внутри защищаемого периметра виртуальной инфраструктуры.
- Сервер авторизации не поддерживает автоматическую смену паролей для служебных учетных записей vGate в домене Windows. Поэтому необходимо создать отдельное организационное подразделение (Organization Units — OU), в котором будут размещаться такие учетные записи, и отключить для него автоматическую смену паролей.
- Для этого:
- назначьте данному OU групповую политику, в которой в ветви "**Computer ConfigurationPoliciesWindows SettingsSecurity SettingsLocal PoliciesSecurity Options** "

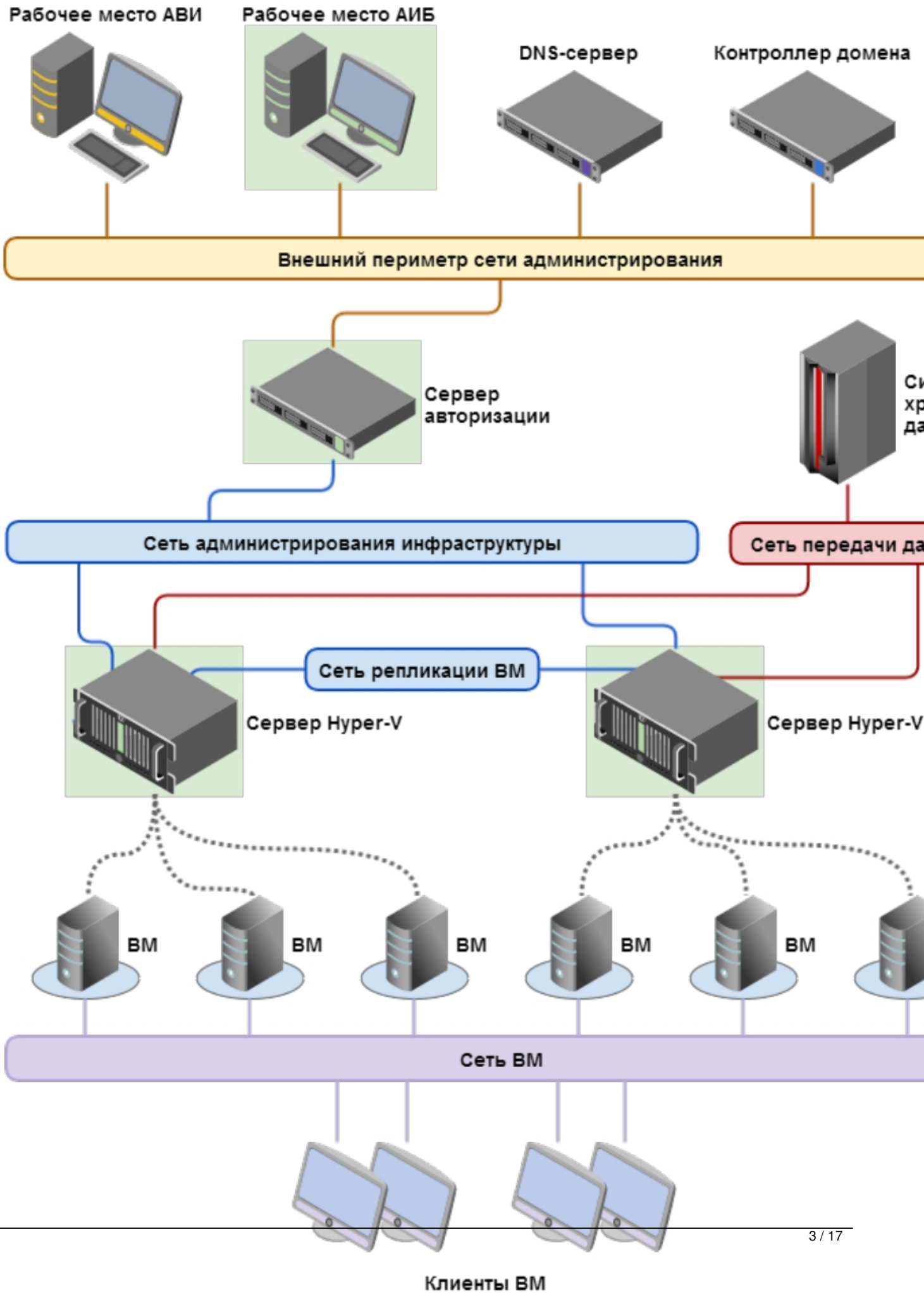
- присвойте параметру "**Domain member: Disable machine account password changes** " значение "**Enabled**" или параметру "**Domain member:maximum machine accountpassword age** " — значение " **999 days** ". Данное OU выбирается на определенномшаге установки сервера авторизации.

Перед конфигурированием локальной сети вам, возомжно, потребуется дополнительно ознакомиться с документацией к продукту Microsoft Hyper-V.

Итак, возможно несколько вариантов развертывания решения vGate R2 в локальной сети.

1. Сервер vGate выступает как маршрутизатор трафика из внешней сети администрирования (рабочие места администраторов, а также DNS-серверы, контроллеры домена и т.п.):

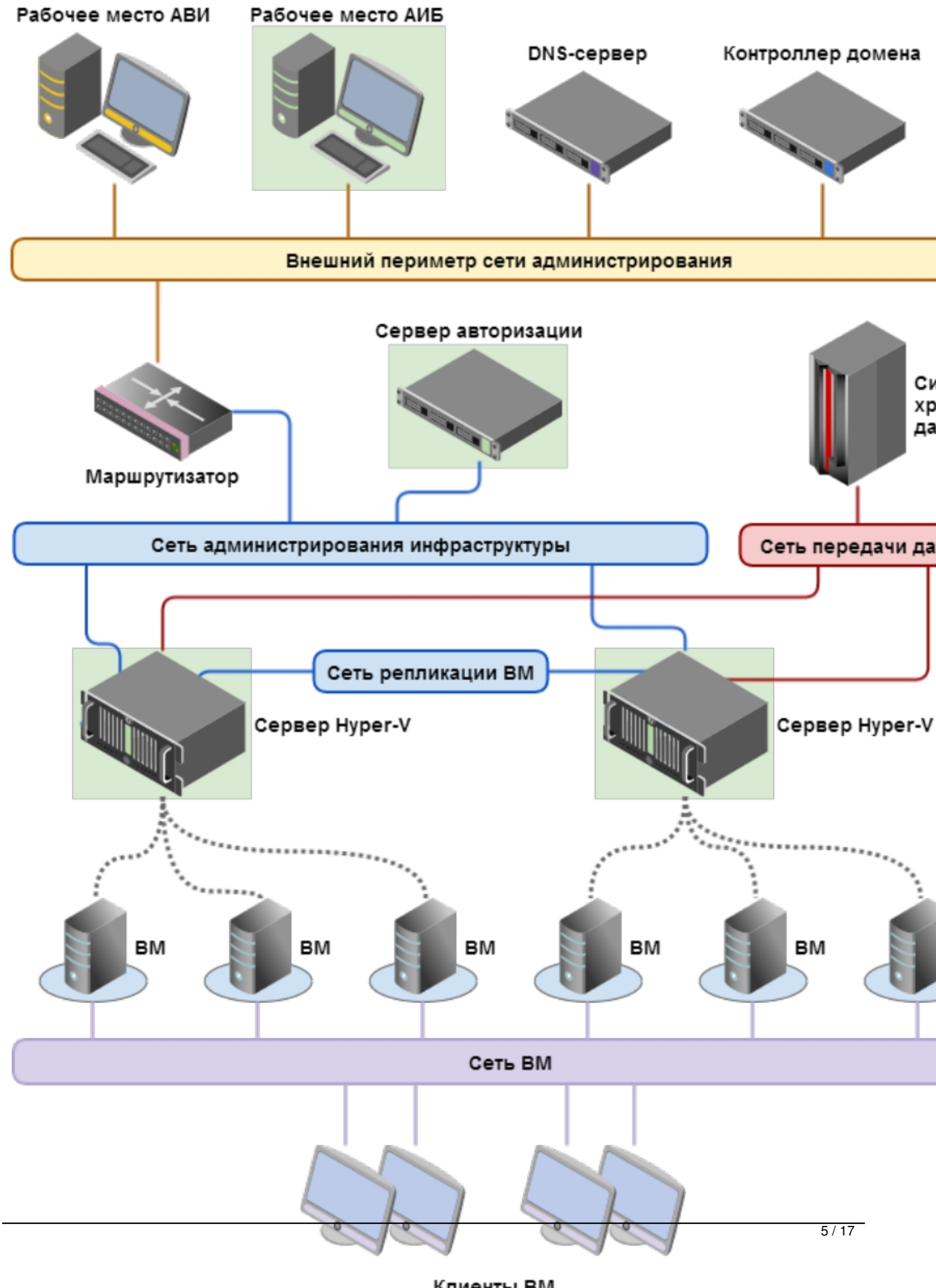
Автор:
30.11.14 18:24 -



Автор:
30.11.14 18:24 -

[illegible]

Автор:
30.11.14 18:24 -



Во время установки сервера авторизации vGate R2

Установка и последующая работа сервера авторизации vGate различаются в зависимости от рассмотренного выше способа маршрутизации управляющего трафика между внешним и защищаемым периметрами сети администроирования:

- **С помощью существующего маршрутизатора в сети.**

Режим не требует реконфигурации существующей сети и предусматривает наличие во внешней сети администрирования сертифицированного межсетевого экрана (маршрутизатора), фильтрующего сетевой трафик к защищаемым серверам. На маршрутизаторе необходимо закрыть доступ с рабочих мест администратора виртуальной инфраструктры (АВИ) и администратора информационной безопасности (АИБ, он же администратор vGate) в защищаемую подсеть или к серверам по отдельности и разрешить доступ к серверу авторизации.

- **Через сервер авторизации vGate.**

При выборе этого способа защищаемые серверы должны быть расположены в отдельной подсети. На всех компьютерах защищаемого периметра (серверах Hyper-V) в качестве шлюза по умолчанию следует указать IP-адрес

адаптера защищаемого периметра сервера авторизации. На всех рабочих местах АВИ в качестве шлюза по умолчанию следует указать IP- адрес сетевого адаптера сервера авторизации во внешней сети. При выборе данного режима не требуется дополнительная настройка маршрутизатора.

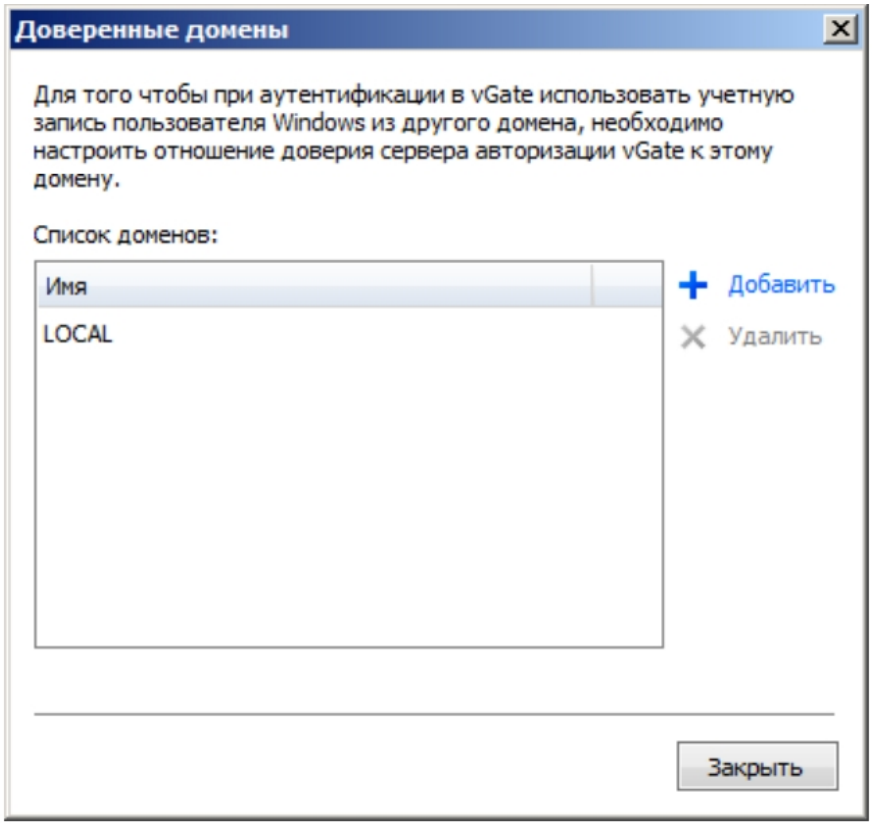
На компьютере, предназначенном для сервера авторизации vGate, необходимо предварительно установить компонент Microsoft Visual C++ 2005 Redistributable. Для этого запустите с установочного диска из каталога RedistributablesMicrosoft Visual C++ 2005 Redistributable файл vcredist_x86.exe и следуйте указаниям мастера установки.

Примечание. Если на компьютере, предназначенном для сервера авторизации vGate, эксплу-
атируется ПО Security Studio Endpoint Protection (SSEP), то перед началом установки необходимо
отключить брандмауэр SSEP.

Важно! Если предполагается использование Active Directory, необходимо ввести компьютер, предназначенный для сервера vGate, в домен. Если компьютер сервера авторизации был добавлен в домен после установки ПО vGate, то необходимо добавить этот домен в список доверенных доменов в консоли управления vGate.

Для этого уже после установки vGate откройте группу параметров "Дополнительные настройки". В области параметров нажмите кнопку-ссылку "Настроить" рядом с заголовком "Доверенные домены".

На экране появится диалог для добавления и удаления доверенных доменов:



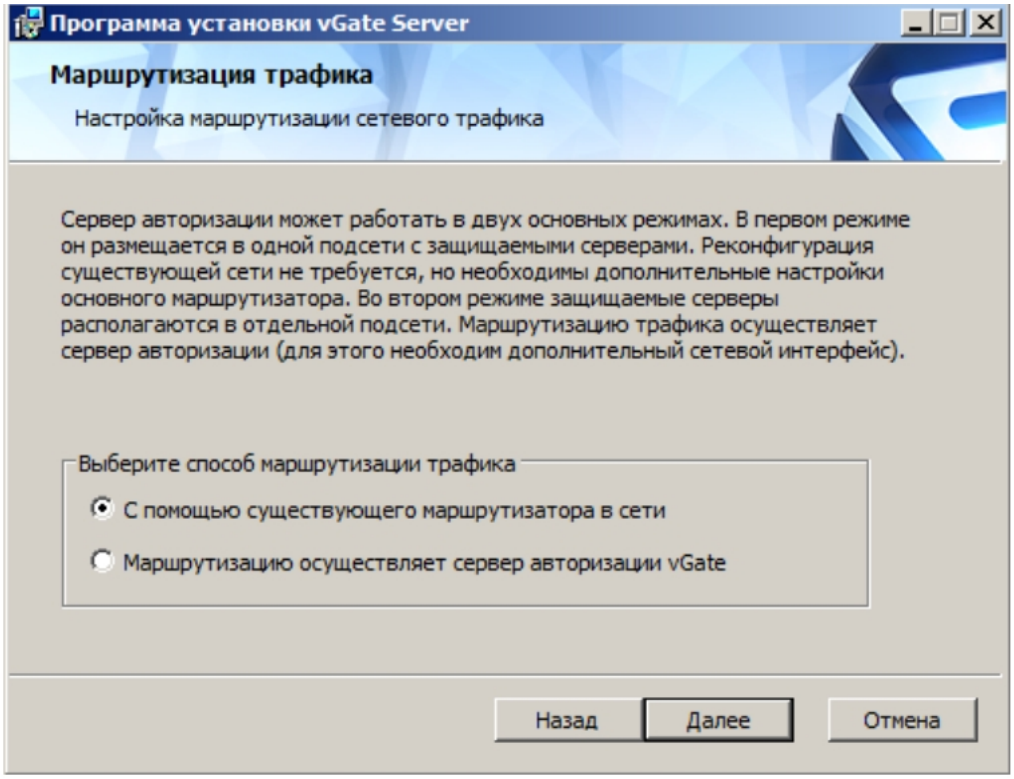
Автор:
30.11.14 18:24 -

Установка при использовании маршрутизатора

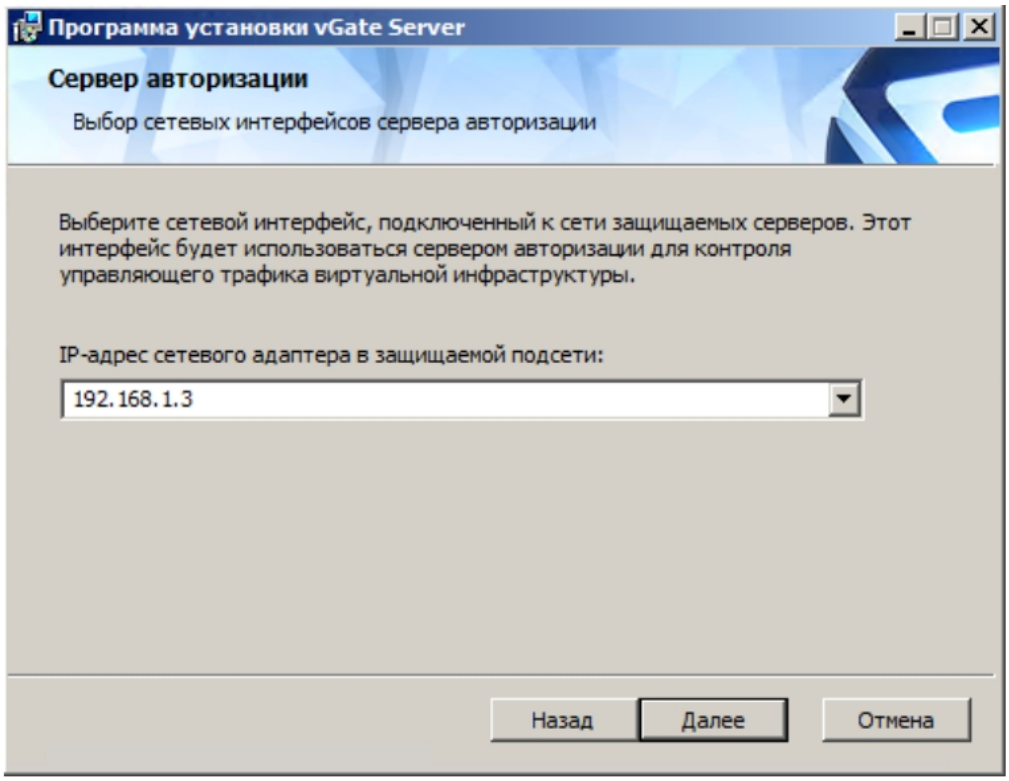
Настройте на компьютере, предназначенном для сервера авторизации, одно соединение локальной сети.

Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	IP-адрес, используемый серверами Hyper-V для конфигурации и аудита. В примерах используется IP-адрес **192.168.1.3**

Далее запустите установку и выберите способ маршрутизации трафика "С помощью существующего маршрутизатора в сети":

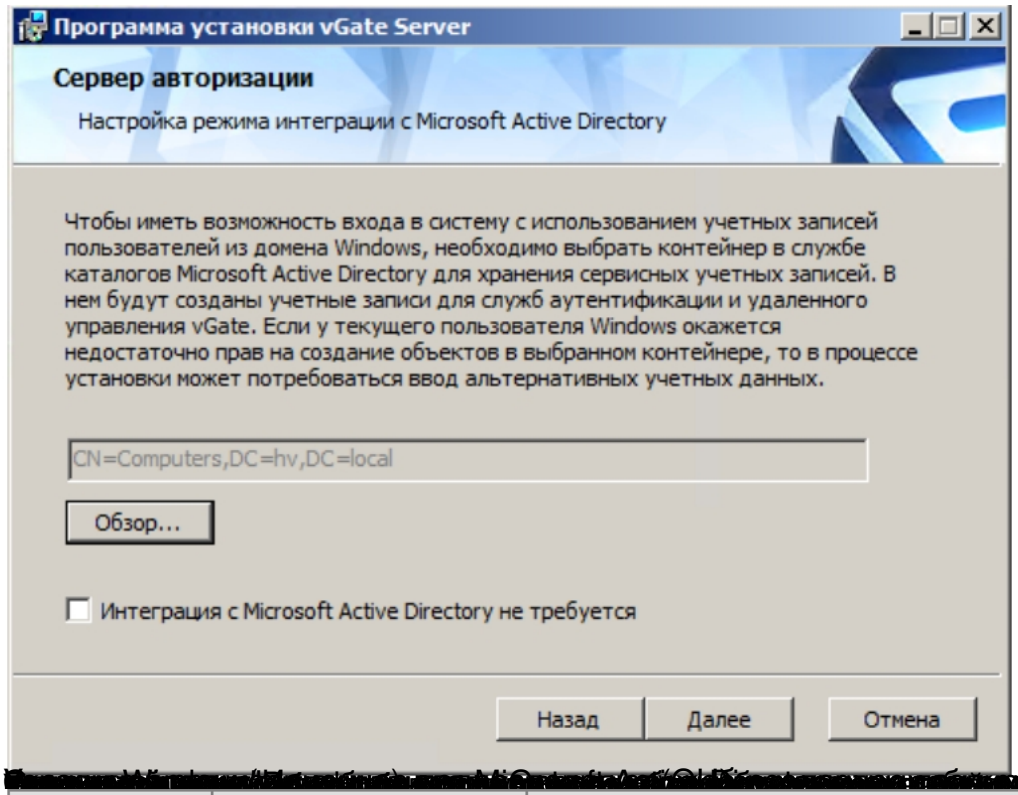


Затем укажите IP-адрес адаптера 1 сервера авторизации, через который будут проходить маршруты в защищаемый периметр и из него:



Если учетная запись данного компьютера входит в домен Windows, на одном из следующих шагов появится следующий диалог (если же используется учетная запись локального администратора,то на экране появится сообщение об ошибке "Не удалось поключиться к службе каталогов". Поле выбора контейнера для учетных записей vGate будет пустым, а кнопка "Обзор" недоступна):

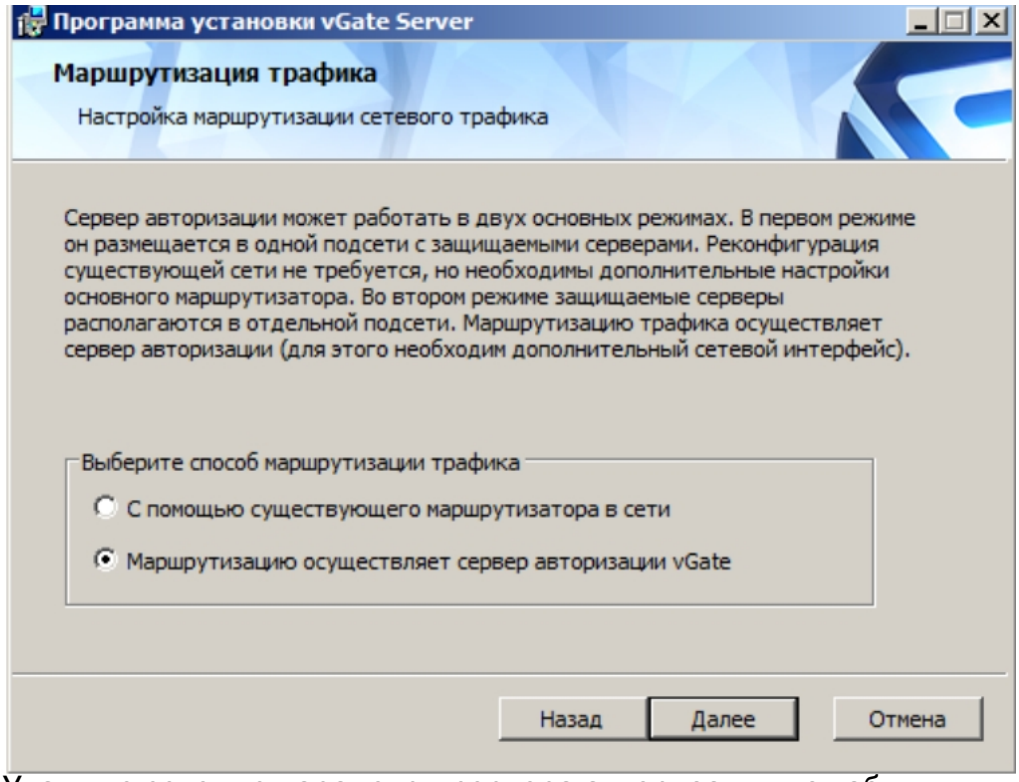
Автор:
30.11.14 18:24 -



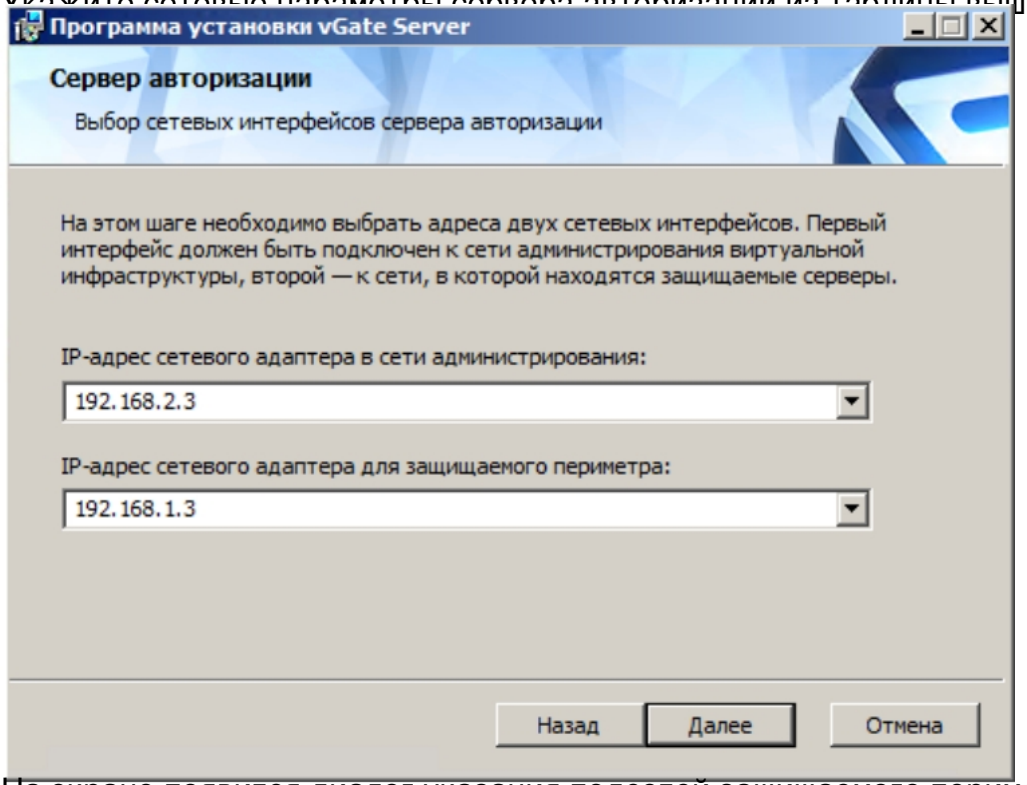
Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	IP-адрес из диапазона адресов защищаемого периметра, используемый серверами Hyper-V для конфигурации и аудита. В примерах используется IP-адрес **192.168.1.3**
Адаптер 2	Сеть внешнего периметра администрирования	IP-адрес из диапазона адресов внешней сети, используемый для соединения с рабочими местами АВИ и АИБ. В примерах используется IP-адрес **192.168.2.3**

Выбираем способ маршрутизации трафика "Маршрутизацию осуществляет сервер

Автор:
30.11.14 18:24 -

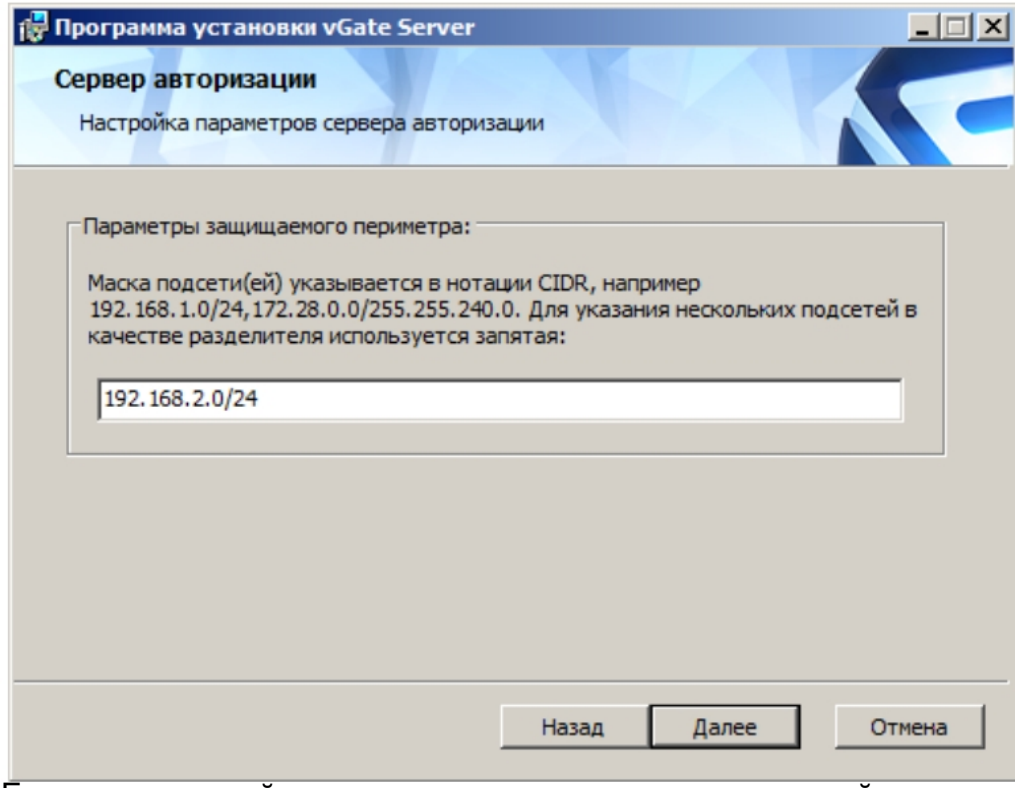


Укажите сетевые параметры сервера авторизации из таблицы выше:

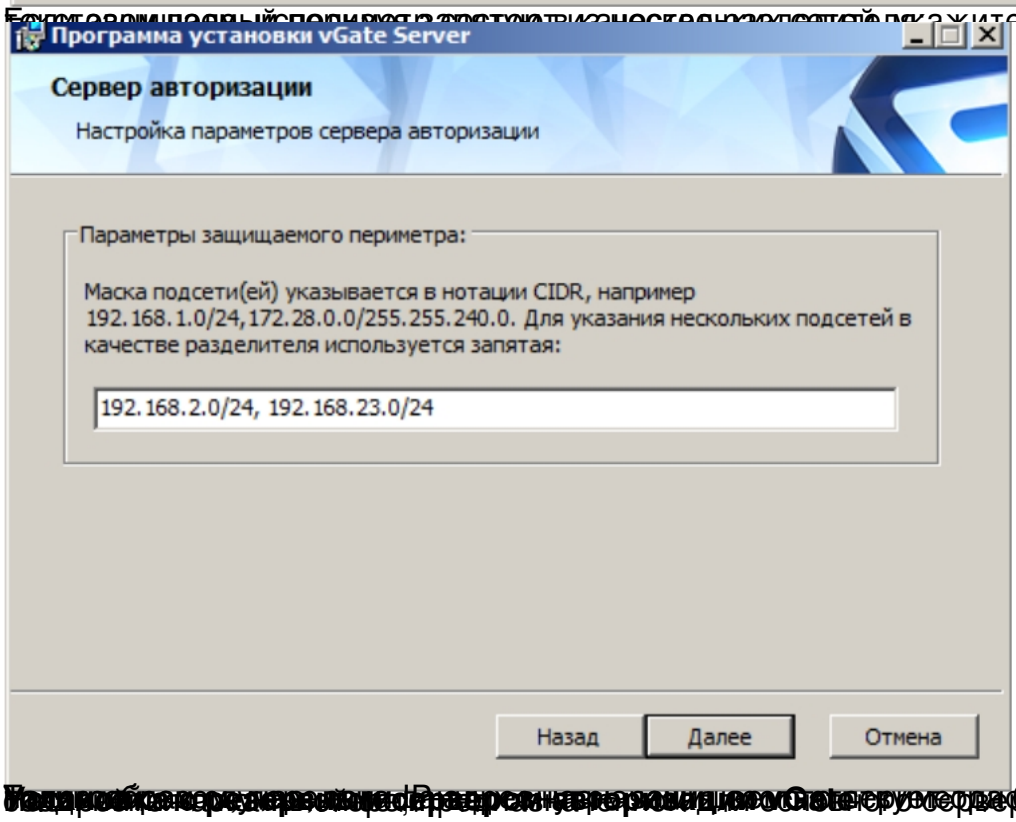


На экране появится диалог указания подсетей защищаемого периметра:

Автор:
30.11.14 18:24 -



Если в вашей сети присутствуют несколько подсетей, укажите их IP-адреса в



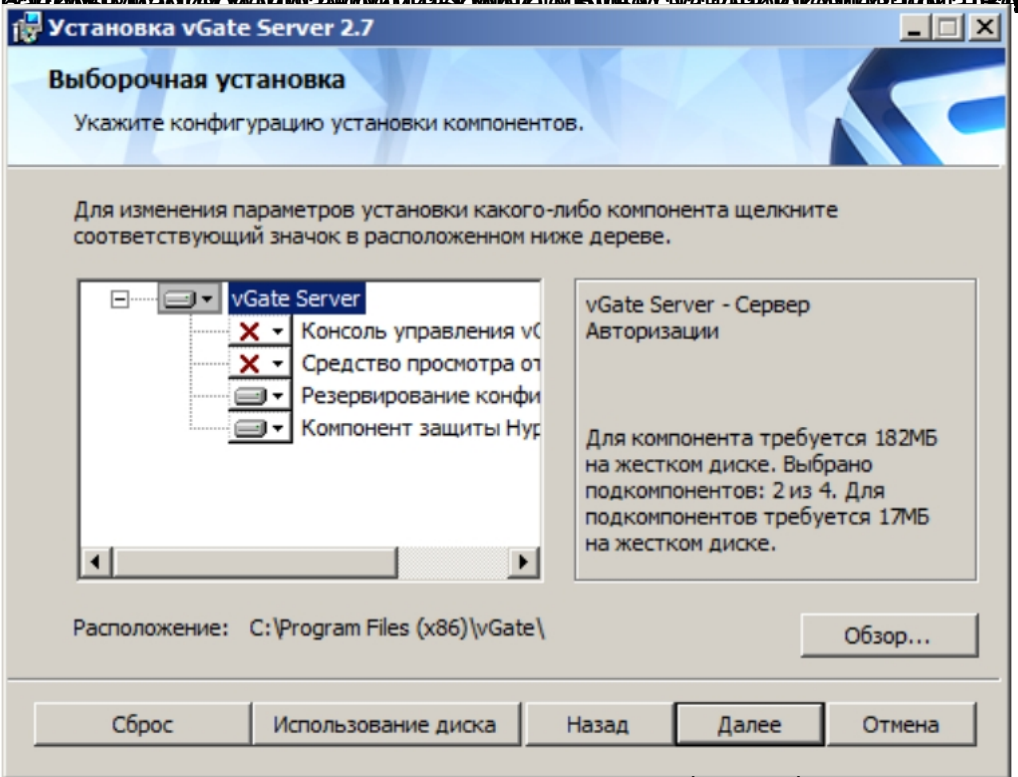
Для обеспечения отказоустойчивости системы vGate рекомендуется развернуть два

Автор:
30.11.14 18:24 -

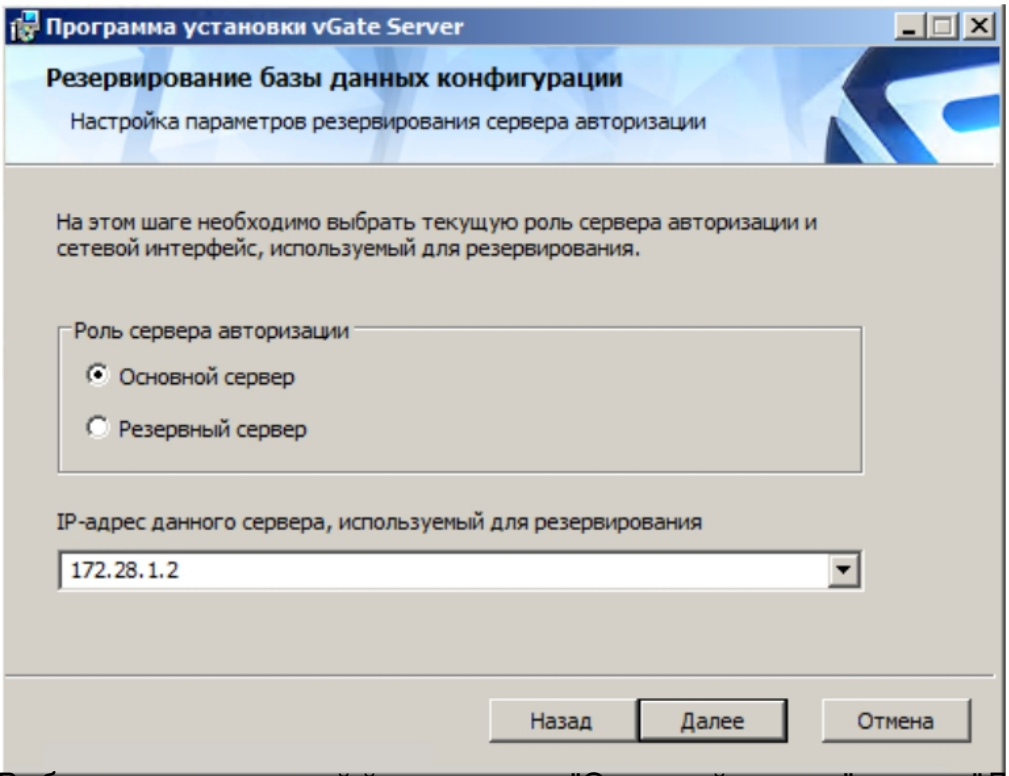
Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	• Основной IP-адрес, используемый серверами Hyper-V для конфигурации и аудита. В примерах используется IP-адрес **192.168.1.3**. • Дополнительный IP-адрес, используемый при сбое сервера. В примерах используется IP-адрес **192.168.1.5**
Адаптер 2	Сеть резервирования	IP-адрес из диапазона адресов сети резервирования, по которому будет осуществляться репликация данных между основным и резервным серверами авторизации. В примерах используется IP-адрес **172.28.1.2**

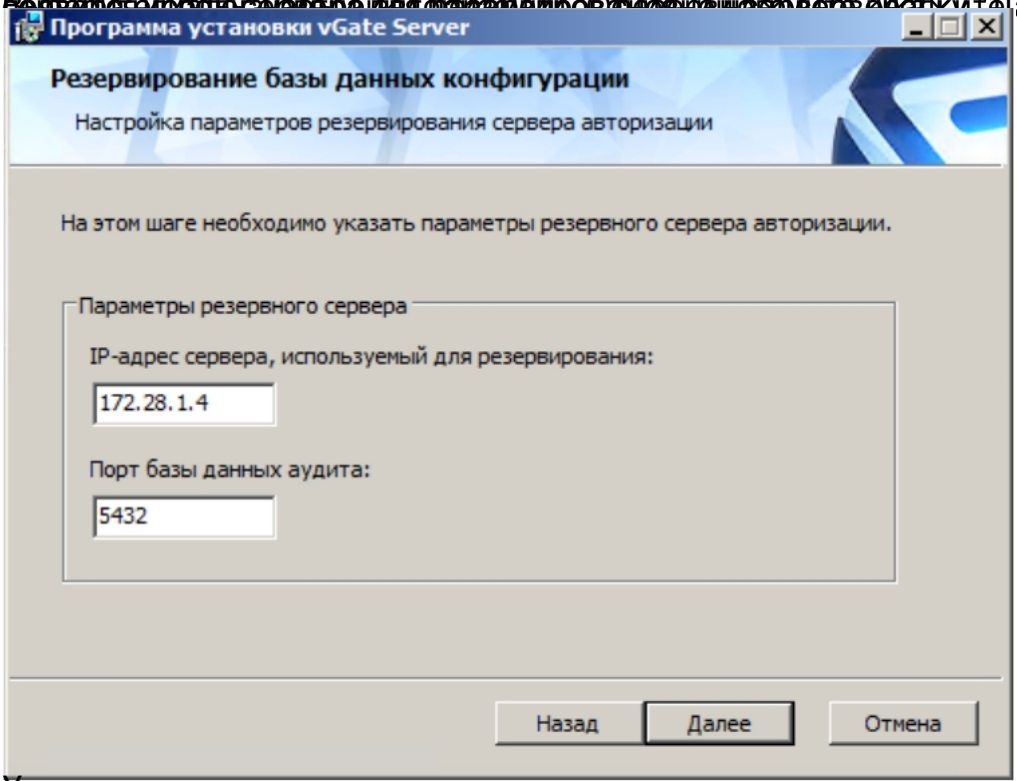
можно

Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	IP-адрес, используемый серверами Hyper-V для конфигурации и аудита. В примерах используется IP-адрес **192.168.1.4**
Адаптер 2	Сеть резервирования	IP-адрес из диапазона адресов сети резервирования, используемый для соединения с основным сервером авторизации. В примерах используется IP-адрес **172.28.1.4**



Автор:
30.11.14 18:24 -

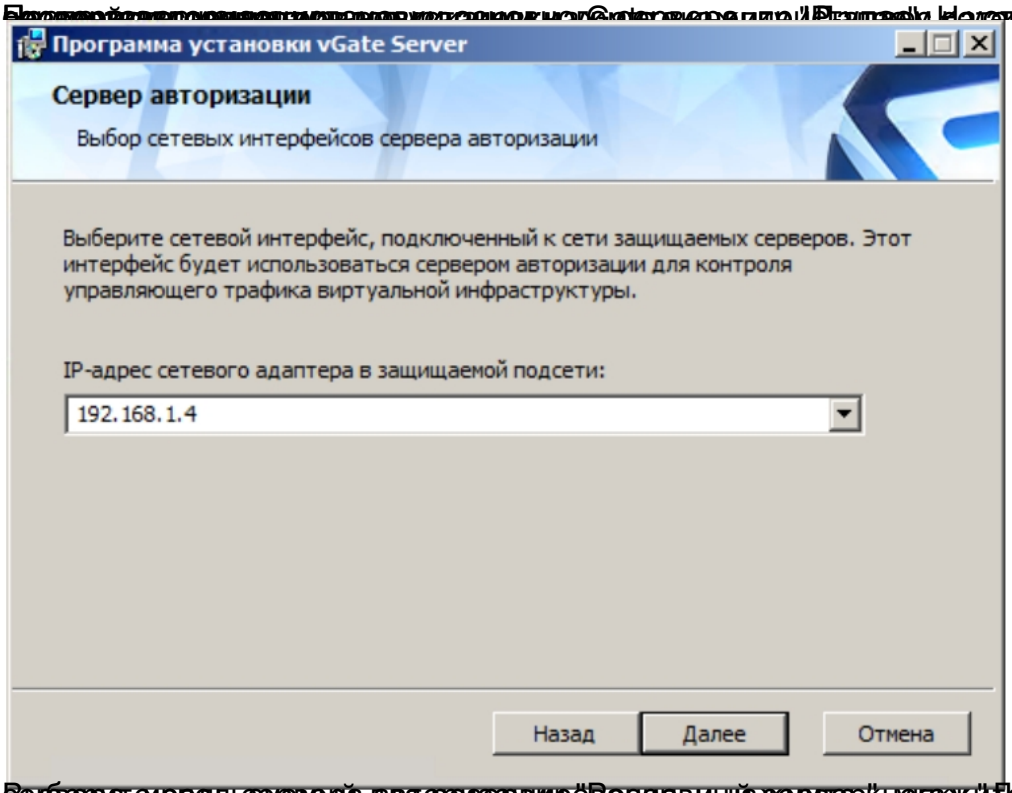




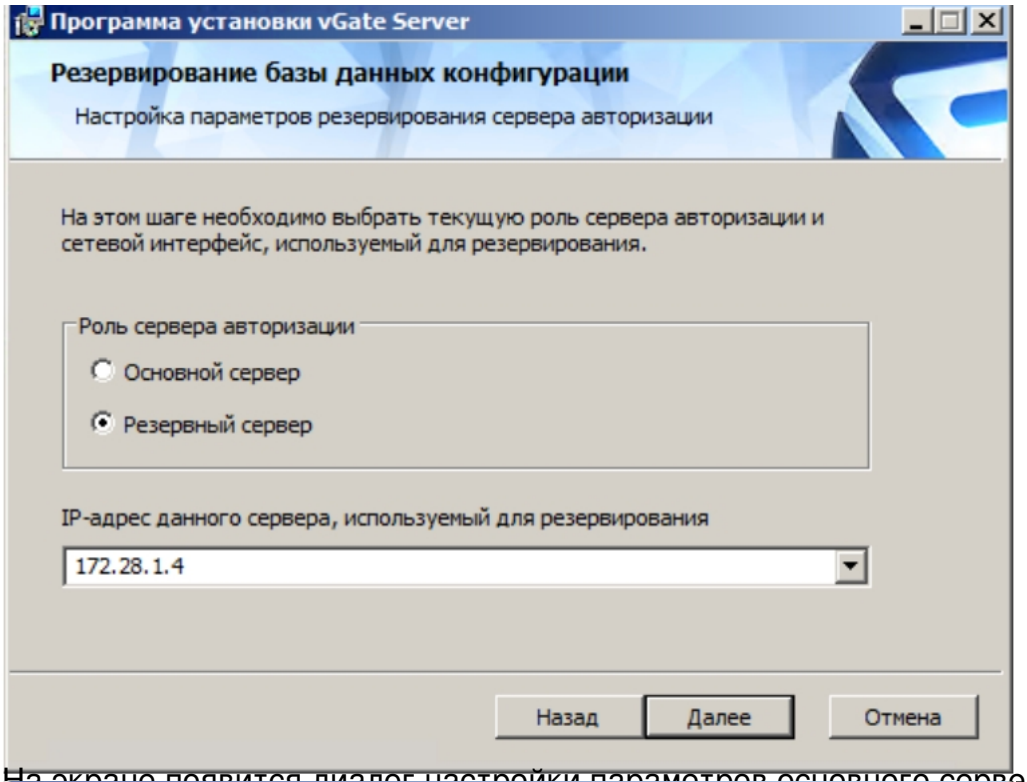
Укажите параметры репликации для резервного сервера авторизации, используя

Автор:
30.11.14 18:24 -

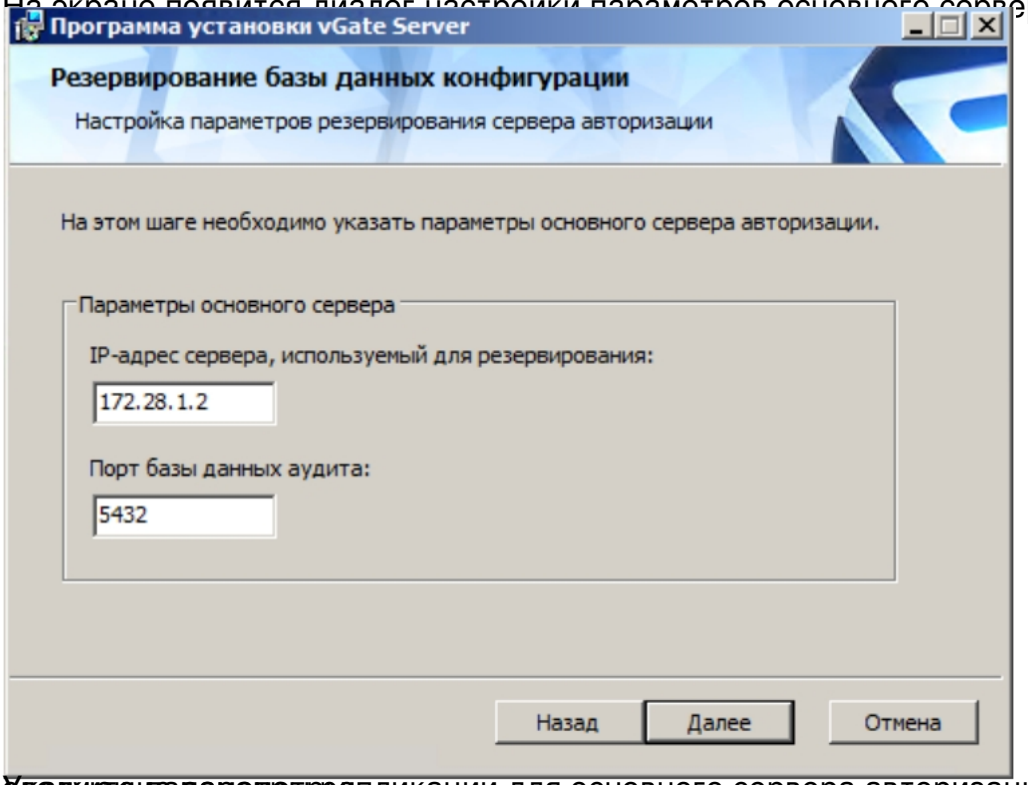
Параметр	Описание
IP-адрес сервера, используемый для резервирования	IP-адрес резервного сервера авторизации в сети резервирования
Порт базы данных аудита	Порт сервера авторизации, используемый для соединения с базой данных аудита на сервере PostgreSQL. Измените значение, если используется номер порта, отличный от стандартного



Автор:
30.11.14 18:24 -



На экране появится диалог настройки параметров основного сервера:



Укажите параметры репликации для основного сервера авторизации, используя следующие параметры:

Автор:
30.11.14 18:24 -

Параметр	Описание
IP-адрес сервера, используемый для резервирования	IP-адрес основного сервера авторизации в сети резервирования
Порт базы данных аудита	Порт сервера авторизации, используемый для соединения с базой данных аудита на сервере PostgreSQL. Измените значение, если используется номер порта, отличный от стандартного