

Автор:
27.12.14 20:10 -

Эксплуатация решения vGate R2 for Hyper-V с точки зрения администратора

Автор: Александр Самойленко
Дата: 27/12/2014

В прошлых статьях мы рассказывали о продукте [vGate R2 for Hyper-V](#), который позволяет проводить защищенную аутентификацию администраторов, разграничивать доступ к различным объектам инфраструктуры и проводить аудит событий безопасности. О возможностях этого продукта мы писали

[ТУТ](#)

, о настройке -

[ТУТ](#)

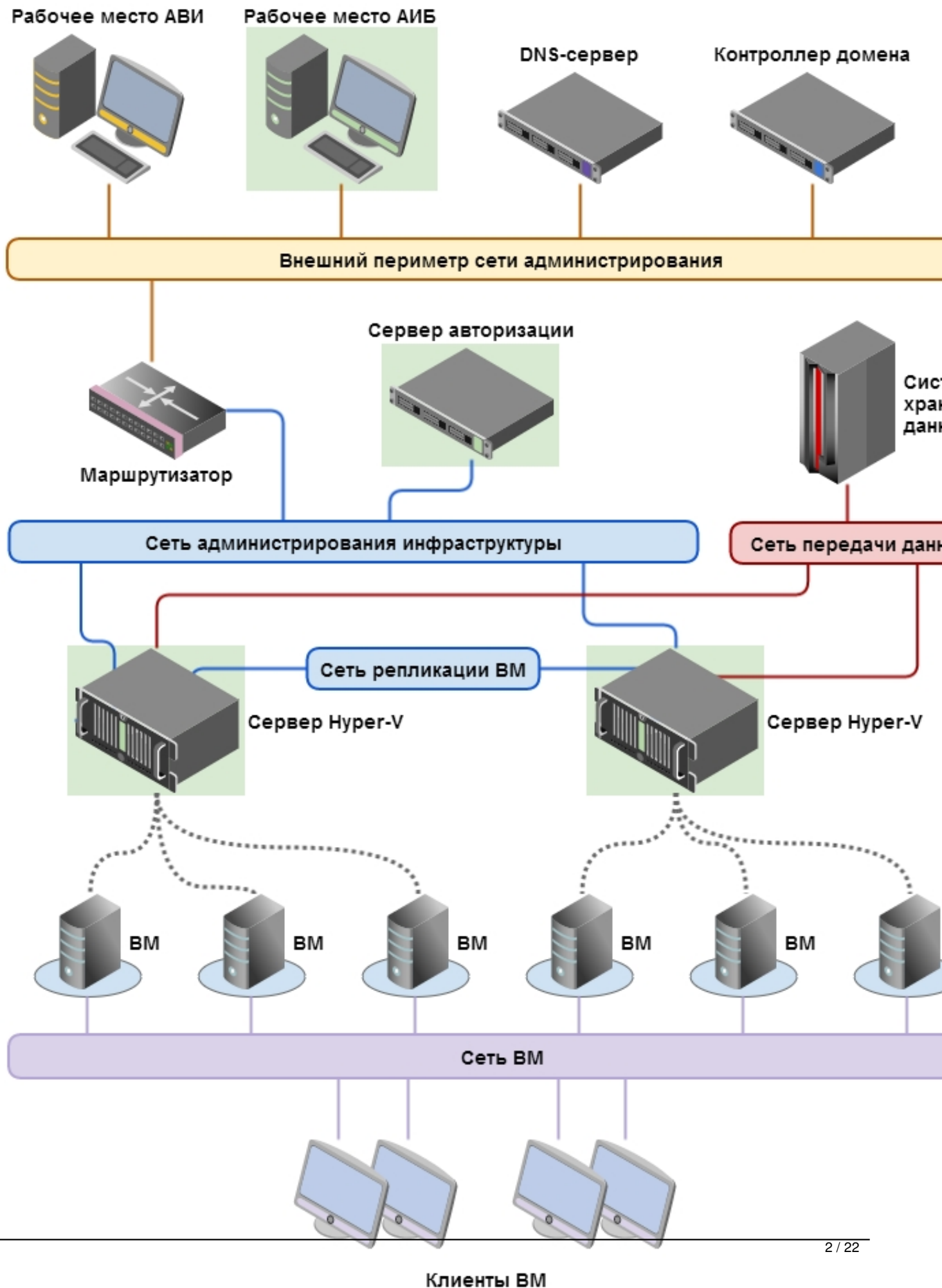
и

[ТУТ](#)

, а сегодня мы поговорим о том, как выглядит повседневная эксплуатация решения со стороны администратора ИБ, который является также и администратором решения vGate.

Итак, приведем сначала референсную архитектуру vGate R2 для инфраструктуры Hyper-V, к которой можно обращаться по ходу чтения статьи:

Автор:
27.12.14 20:10 -



Автор:
27.12.14 20:10 -

Выбор... Серверы

Аудит

Фильтрация событий

Типы событий <input checked="" type="checkbox"/> Успех <input checked="" type="checkbox"/> Уведомление <input checked="" type="checkbox"/> Предупреждение <input checked="" type="checkbox"/> Ошибка	Время событий:	с первого	17/04/2014	5:10:44 PM
		до последнего	17/04/2014	5:10:44 PM
	Компьютер:	*		
	Текст содержит:	*		
			Дополнительно...	Применить

Список событий:

Всего объектов: 2000

Тип	Время	Компьютер	Код события	Компонент	Категория
Предупреж...	17-04-2014 08:15:50	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Успех	17-04-2014 08:15:50	HVAUTHSERVER	16842763	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:15:24	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:15:03	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Успех	17-04-2014 08:15:03	HVAUTHSERVER	16842763	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:14:37	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:14:16	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Успех	17-04-2014 08:14:16	HVAUTHSERVER	16842763	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:13:50	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:13:29	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Успех	17-04-2014 08:13:29	HVAUTHSERVER	16842763	Служба аутентификации	Управление д

Выбор... Серверы

Автор:
27.12.14 20:10 -

Свойства события

Дата: 14-10-2014 18:38:31

Тип: Уведомление

Компьютер: SA

Код: 33558629

Компонент: vCenter

Категория: Виртуальные машины

Описание:
Виртуальная машина клонирована.
Виртуальная машина: WIN7
Новое имя: VM4
GUID: 4222abbb-d7f9-9594-7e5b-9693bc55ff29
Сервер: 192.168.100.104
URL: /vmfs/volumes/5405cd60-5d5874d4-e18f-000c29385f92

Копировать Закрыть

Свойства события

Дата: 14-10-2014 18:38:31

Тип: Уведомление

Компьютер: SA

Код: 33558629

Компонент: vCenter

Категория: Виртуальные машины

Описание:
GUID: 4222abbb-d7f9-9594-7e5b-9693bc55ff29
Сервер: 192.168.100.104
URL: /vmfs/volumes/5405cd60-5d5874d4-e18f-000c29385f92
Шаблон: Нет
Пользователь: avi1@VGATE
Компьютер пользователя: 192.168.2.205

Копировать Закрыть

Save As

Save in: Documents

Name	Date modified	Type	Size	Tags
No items match your search.				

File name: Event_log

Save as type: Текст (разделитель - табуляция) (*.txt)

Сохранить только выбранные строки

Save Cancel

Файл "Event_log" был сохранен в папке "Документы" ("C:\Users\avi1\Documents") и будет использоваться для дальнейшей работы.

Автор:
27.12.14 20:10 -

Очистка базы событий

Удалить события ранее:

Настройки генерации событий

Список генерируемых событий:

Строка поиска:

Код события	Состояние	Тип	Категория	Описание события
<input checked="" type="checkbox"/> 134219777	Аудит, SNMP	Ошибка	Целостность	Ошибка службы контроля цел...
<input checked="" type="checkbox"/> 134219782	Аудит	Ошибка	Целостность	Отмена изменений файла %1...
<input checked="" type="checkbox"/> 134219790	Аудит	Ошибка	Целостность	При подсчете контрольной су...
<input checked="" type="checkbox"/> 134219791	Аудит	Ошибка	Целостность	При проверке целостности вир...
<input checked="" type="checkbox"/> 134219792	Аудит	Ошибка	Целостность	При проверке целостности фа...
<input checked="" type="checkbox"/> 134219796	Аудит	Ошибка	Целостность	При подсчете контрольной су...
<input checked="" type="checkbox"/> 134219797	Аудит	Ошибка	Целостность	При проверке целостности гос...
<input checked="" type="checkbox"/> 134234113	Аудит, SNMP	Ошибка	Служба	Не удалось запустить службу ...
<input checked="" type="checkbox"/> 134234115	Аудит, SNMP	Ошибка	Служба	Не удалось остановить служб...
<input checked="" type="checkbox"/> 134234121	Аудит, SNMP	Ошибка	Служба	Не удалось запустить службу ...
<input checked="" type="checkbox"/> 134234123	Аудит, SNMP	Ошибка	Служба	Не удалось остановить служб...
<input checked="" type="checkbox"/> 134250499	Аудит	Ошибка	Развертывание	При установке агента vGate н...
<input checked="" type="checkbox"/> 134250500	Аудит	Ошибка	Развертывание	При удалении агента vGate с с...
<input checked="" type="checkbox"/> 134283266	Аудит	Ошибка	Управление доступом	Переименование защищаемого...
<input checked="" type="checkbox"/> 134283267	Аудит	Ошибка	Управление доступом	Создание защищаемого объек...

Включено: 426, выключено: 0.

Автор:
27.12.14 20:10 -

Защищаемые серверы

Список защищаемых серверов:

Всего объектов: 0

Имя	Тип	Версия	С...	Уровень	Катег...	Разре...	Поясн...
-----	-----	--------	------	---------	----------	----------	----------

- + Сервер виртуализации
- + Автономный сервер
- ✕ Удалить
- ✎ Редактировать
- ▣ Назначить метку
- ⇒ Экспорт
- ↻ Обновить

Обратитесь к меню серверов (Hyper-V виртуализация). На экране появится мастер

Мастер добавления нового сервера Hyper-V в список защищаемых серверов

Настройки соединения с сервером Hyper-V

Укажите полное доменное имя или IP-адрес сервера виртуальной инфраструктуры, имя (в формате 'domain\account') и пароль пользователя, обладающего правами администратора на этом сервере

Сервер будет добавлен в список защищаемых серверов. Агент vGate будет установлен автоматически

Сервер:

Пользователь:

Пароль:

Сохранить имя пользователя и пароль
Эти настройки будут использованы при добавлении следующих серверов

< Назад Далее > Отмена

На экране появится мастер добавления нового сервера Hyper-V в список защищаемых серверов. На экране появится мастер

Автор:
27.12.14 20:10 -

Мастер добавления нового Hyper-V сервера в список защищаемых серверов

Установка агента защиты на Hyper-V сервер

Происходит автоматическая установка агента защиты Hyper-V сервера

Установка агента успешно завершена. Сервер добавлен в список защищаемых серверов.

[< Назад](#) [Завершить](#)

Видео: [Обзор](#) [Обучение](#) [Помощь](#) [Дополнительно](#)

Развертывание

Список защищаемых серверов Всего объектов: 2

Имя	Статус агента	Версия агента	Сокеты	
192.168.2.20	Запущен	1.0.251.0	1	+ Переустановить
192.168.2.21	Запущен	1.0.251.0	1	✗ Удалить

[|| Приостановить контроль](#)

Видео: [Обзор](#) [Обучение](#) [Помощь](#) [Дополнительно](#)

Развертывание

Список защищаемых серверов Всего объектов: 2

Имя	Статус агента	Версия агента	Сокеты	
192.168.2.20	Установка		1	+ Установить
192.168.2.21	Запущен	1.0.251.0	1	✗ Удалить

[▶ Возобновить контроль](#)

агенту в браузере сервера при запуске и добавлении Hyper-V параметр "Статус

Автор:
27.12.14 20:10 -

Развертывание

Список защищаемых серверов

Всего объектов: 2

Имя	Статус агента	Версия агента	Сокеты
192.168.2.20	Запущен	1.0.251.0	1
192.168.2.21	Запущен	1.0.251.0	1

- + Установить
- ✗ Удалить
- ▶ Возобновить контроль

Используйте панель объектов параметров, чтобы управлять параметрами объектов и выполнять функции

Развертывание

Список защищаемых серверов

Всего объектов: 2

Имя	Статус агента	Версия агента	Сокеты
192.168.2.20	Приостановлен	1.0.251.0	1
192.168.2.21	Запущен	1.0.251.0	1

- + Переустановить
- ✗ Удалить
- ▶ Возобновить контроль

Используйте панель объектов параметров, чтобы управлять параметрами объектов и выполнять функции

Учетные записи

Список пользователей:

Всего объектов: 3

Имя пользователя	Уровень	Категории
admin@VGATE	Неконфиденциально	
u1@VGATE	Неконфиденциально	
u2@VGATE	Неконфиденциально	

- + Добавить
- ☀ Создать
- ✗ Удалить
- ✎ Редактировать
- 🔑 Изменить пароль
- 🏷 Назначить метку
- ➡ Экспорт
- 🔒 Политики паролей

Используйте панель объектов параметров, чтобы управлять параметрами объектов и выполнять функции

Автор:
27.12.14 20:10 -

Новый пользователь

Пользователь:

Пароль:

Подтверждение:

Полномочия учетной записи:

- Администратор информационной безопасности
- Оператор учетных записей
- Срок действия пароля неограничен
- Учетная запись отключена
- Сменить пароль при следующем входе в систему
- Разрешено скачивать файлы виртуальных машин

OK Отмена

Настройка параметров пользователя "OK" и "Отмена" задают параметры (Пароль

Автор:
27.12.14 20:10 -

Политики паролей пользователей

Максимальный срок действия пароля: 30 дней

Минимальная длина пароля: 1 символов

Хранить историю: 4 паролей

Разница при смене пароля: 4 символов

Минимальное количество классов символов: 1

Отключить учетную запись, неиспользуемую более:
90 дней


Отключить учетную запись после:
3 неуспешных попыток входа

OK Отмена

В настройках сети безопасности не рекомендуется использовать минимальную длину пароля






Автор:
27.12.14 20:10 -

Консоль управления vGate for Hyper-V






Метки безопасности

Категории конфиденциальности: Всего объектов: 5

Имя	Описание	Наборы политик безопасности
 Желтый		
 Зеленый		
 Красный		
 Оранжевый		
 Синий		

Уровни конфиденциальности: Всего объектов: 2

Имя	Описание	Наборы политик безопасности
 Неконфиденциально		
 Для служебного пользования		

 Настроить матрицу сочетаний уровней и категорий конфиденциальности

Защищаемые серверы
Развертывание
Виртуальные машины

Конфигурация
Политики безопасности
Метки безопасности
Учетные записи
О продукте

Аудит

- + Добавить
- ✗ Удалить
- ✎ Редактировать
- ✓ Назначить политику
- ⊖ Отменить назначение
- ↻ Обновить

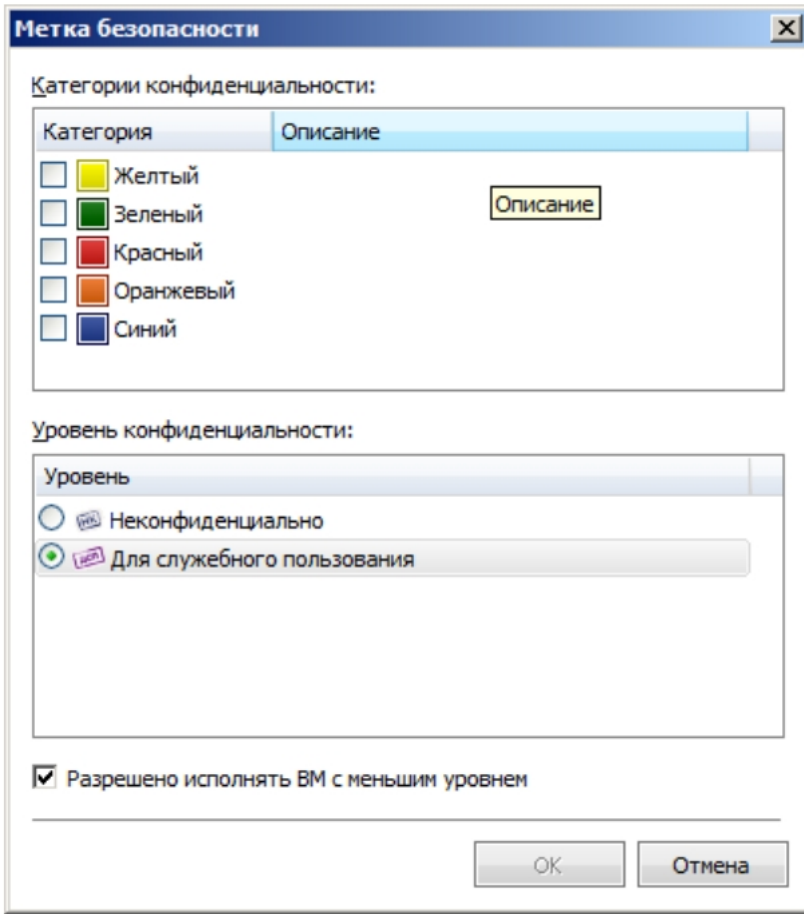
- ✎ Редактировать
- ✓ Назначить политику
- ⊖ Отменить назначение
- ↻ Обновить

Категория конфиденциальности: Желтый, Зеленый, Красный, Оранжевый, Синий

Уровни конфиденциальности: Неконфиденциально, Для служебного пользования

Настроить матрицу сочетаний уровней и категорий конфиденциальности

Автор:
27.12.14 20:10 -



Внимание! Данное изображение является частью документа, содержащего конфиденциальную информацию. Если вы обнаружили данное изображение в открытом доступе, пожалуйста, сообщите об этом по адресу: info@thin.kiev.ua. Все права защищены. © 2014 Thin Group.

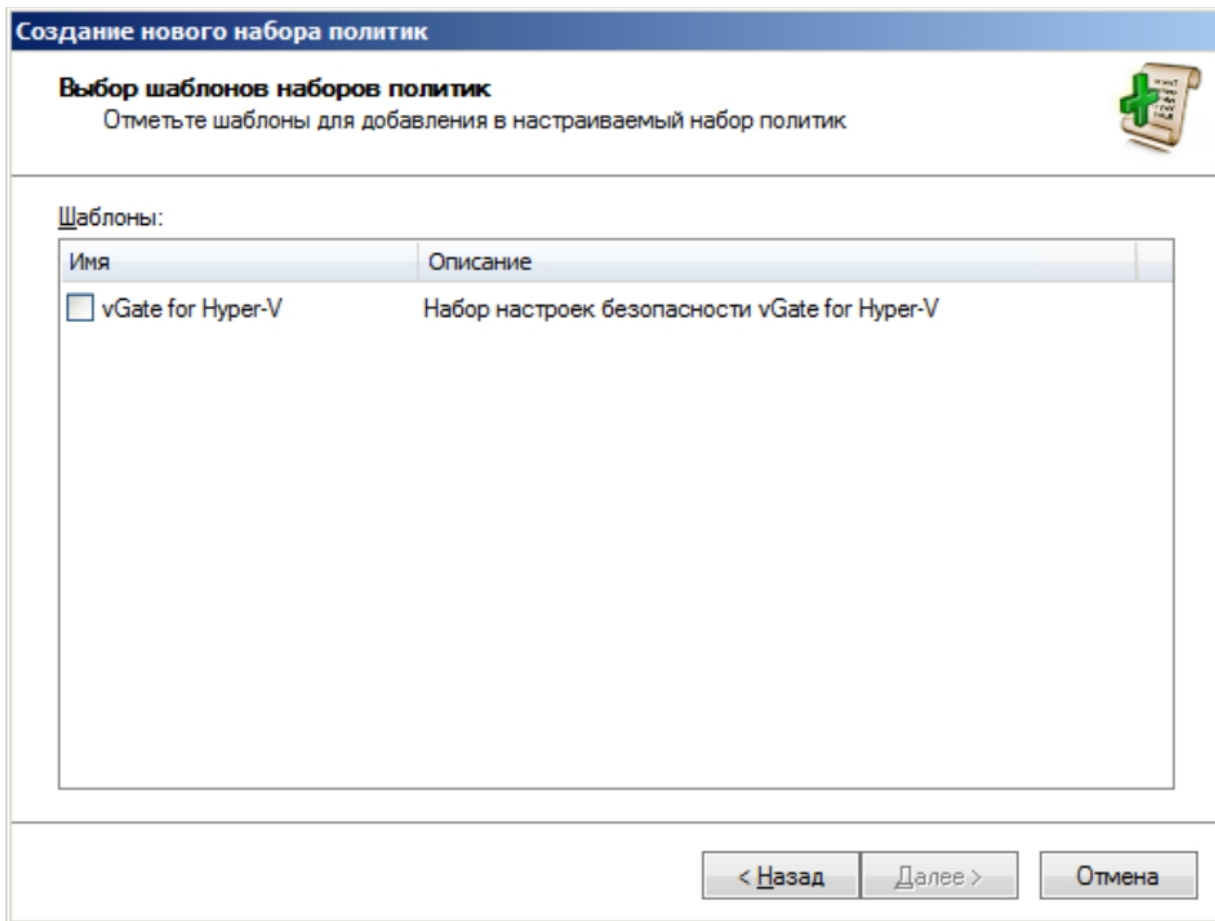
Автор:
27.12.14 20:10 -

The screenshot shows the 'vGate for Hyper-V' management console. The title bar reads 'Консоль управления vGate for Hyper-V'. The main header features the vGate logo and the text 'vGate for Hyper-V'. On the left, a navigation pane includes 'Защищаемые серверы', 'Развертывание', 'Виртуальные машины', 'Конфигурация', 'Политики безопасности' (highlighted), 'Метки безопасности', 'Учетные записи', 'О продукте', and 'Аудит'. The main area is titled 'Политики безопасности' and shows a list of security policy sets. The list has two columns: 'Имя' and 'Описание'. It contains one entry: 'vGate for Hyper-V' with the description 'Набор настроек безопасности vGate for Hyper-V'. To the right of the list are buttons: '+ Добавить', 'X Удалить', 'Изменить', and 'Переименовать'. At the bottom right of the list area is an 'Обновить' button.

Имя	Описание
vGate for Hyper-V	Набор настроек безопасности vGate for Hyper-V

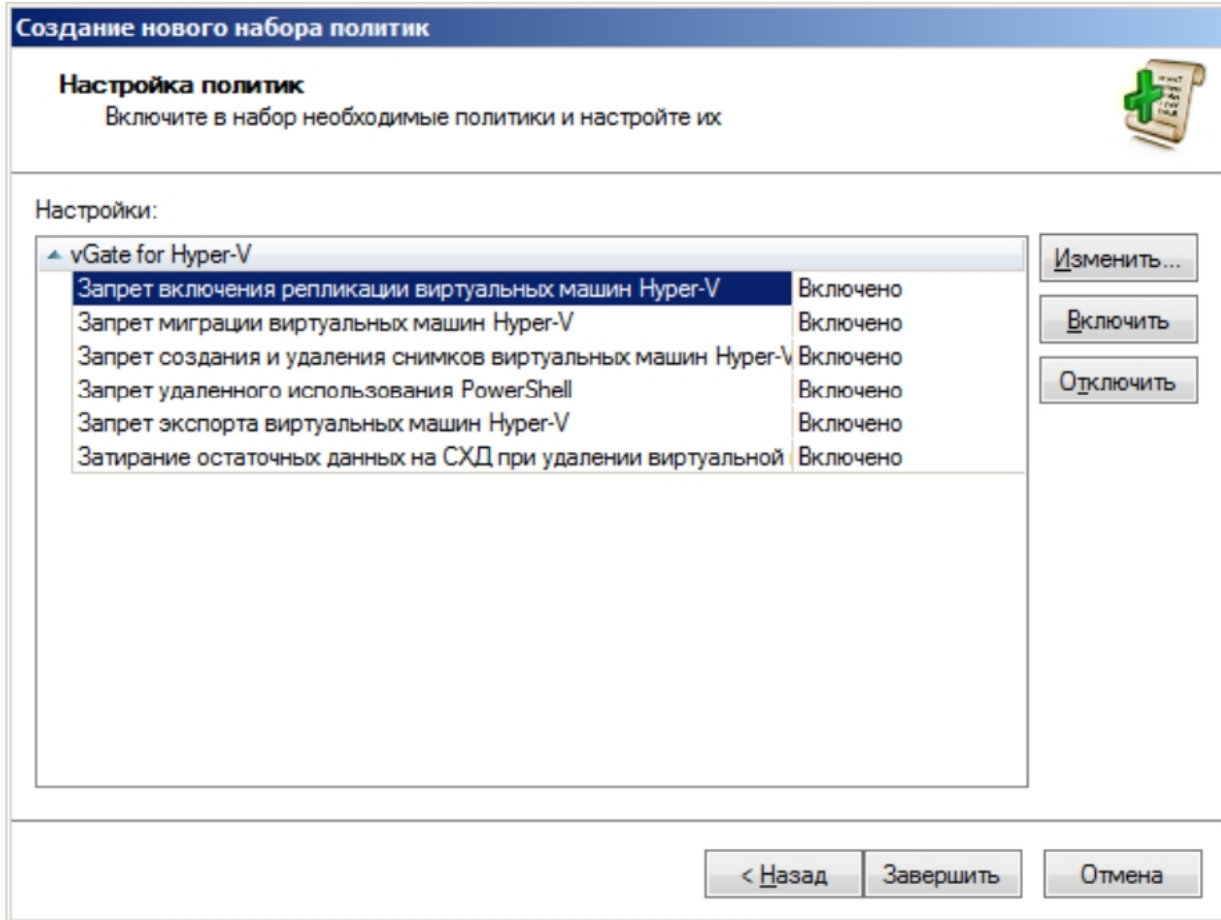
Далее нажмите кнопку "Добавить" и создайте новый шаблон политик на базе

Автор:
27.12.14 20:10 -



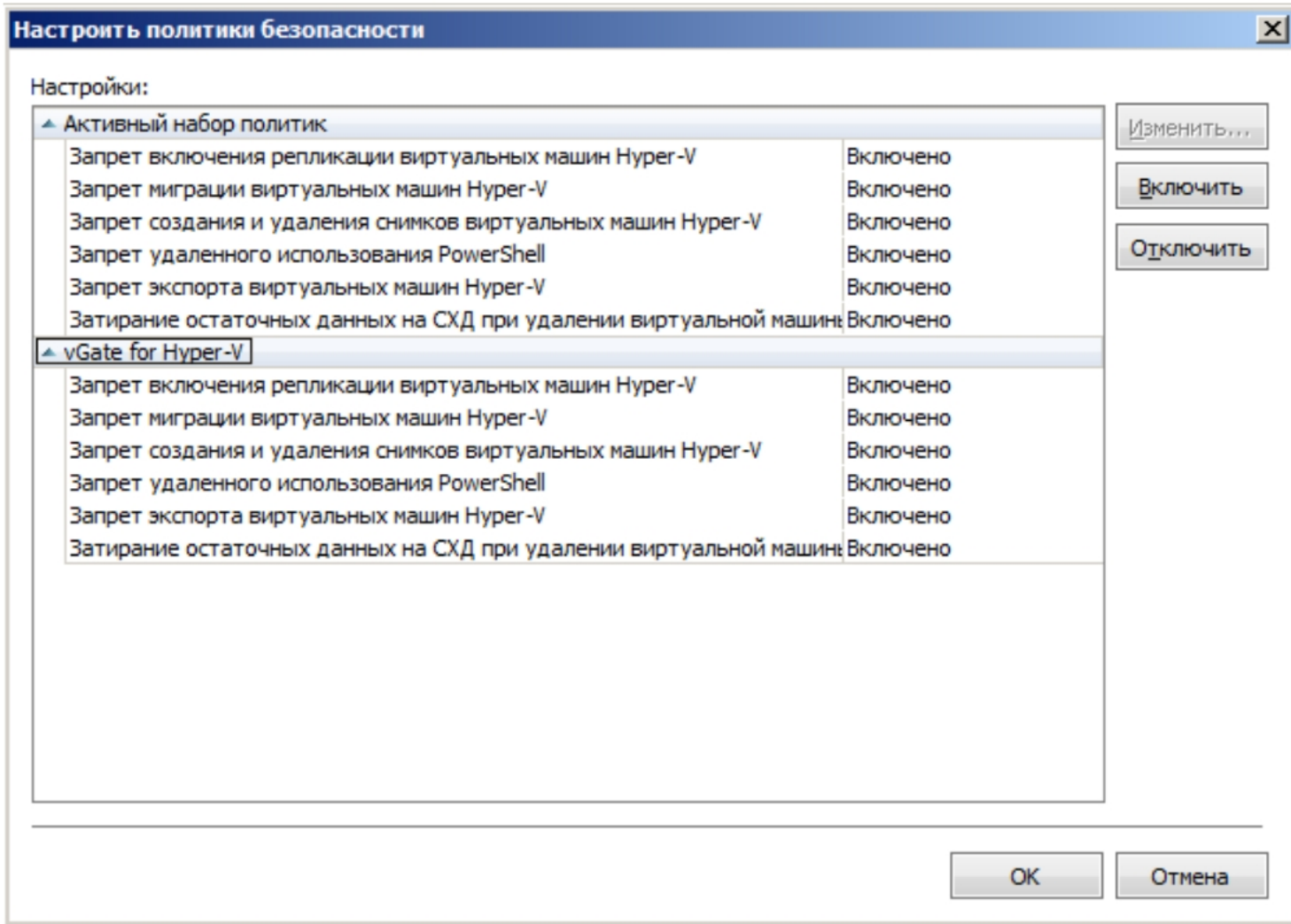
На экране появится диалог настройки политик:

Автор:
27.12.14 20:10 -



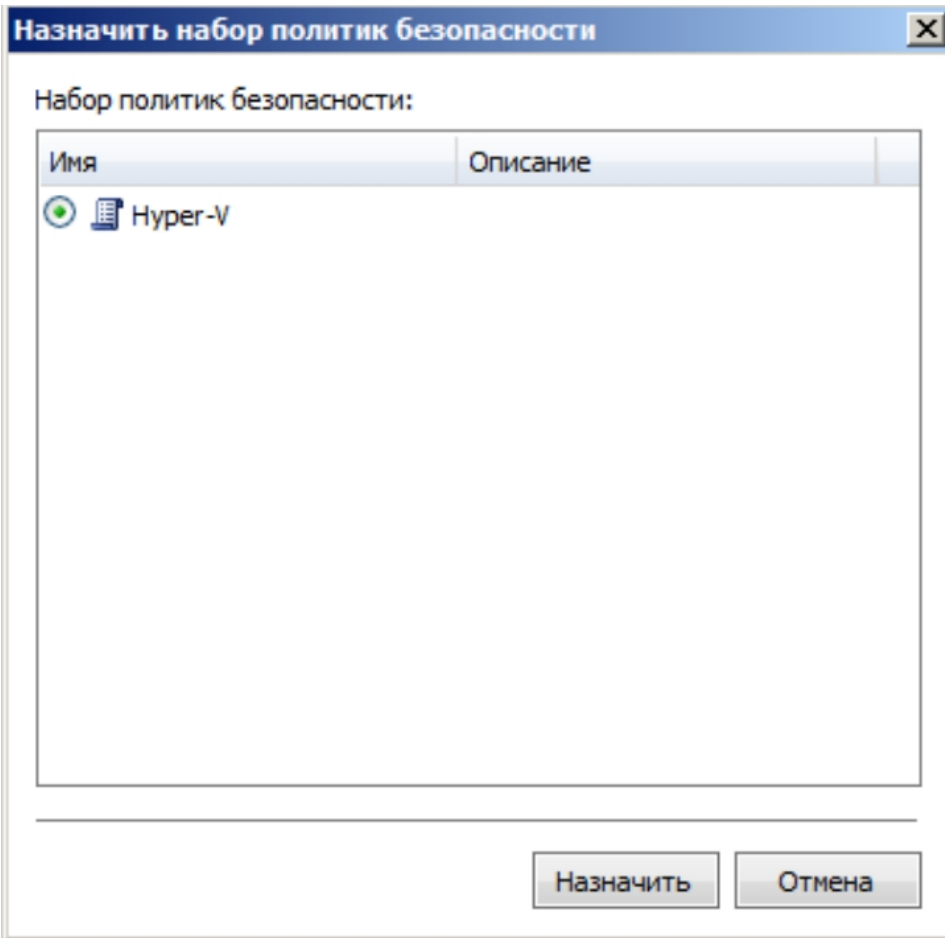
Виртуальные машины Hyper-V (vGate) - это виртуальные машины, которые работают под управлением гипервизора Hyper-V. Виртуальные машины Hyper-V (vGate) - это виртуальные машины, которые работают под управлением гипервизора Hyper-V.

Автор:
27.12.14 20:10 -



Файл | Правка | Вид | Сервис | Настройка | Справка | ...

Автор:
27.12.14 20:10 -



Назначение политик безопасности для виртуальной машины Hyper-V

Автор:
27.12.14 20:10 -

Защищаемые серверы

Список защищаемых серверов:

Всего объектов: 3

Имя	Тип	Версия	С...	Уровень	Катег...	Разре...	Поясн...
192.168.2.10	Автоно...						Сервер...
192.168.2.20	Сервер...	Windows Server 2...	1	Неконф...		Да	hVvM S...
192.168.2.21	Сервер...	Windows Server 2...	1	Неконф...		Да	hVvM S...

- Сервер вирту...
- Автономный с...
- Удалить
- Редактировать
- Назначить мет...
- Экспорт
- Обновить

Правила доступа для 192.168.2.10:

Всего правил: 5

Описание	Состо...	Пользоват...	Компьютер...	Прото...	Исход...	Порт н...
Доступ к вспомогатель...	Вкл	admin@VGATE	*	TCP	Любой	3908
Доступ к отчетам для ...	Вкл	admin@VGATE	*	TCP	Любой	5432
Доступ к службе управ...	Вкл	admin@VGATE	*	TCP	Любой	3802
Доступ к службе управ...	Вкл	admin@VGATE	*	TCP	Любой	3906
Статус операций по уп...	Вкл	admin@VGATE	*	TCP	Любой	3803

- Создать прави...
- Удалить
- Свойства
- Выключить
- Экспорт
- Обновить

Выбор правил для сервера 192.168.2.20: "Правила доступа для защищаемых серверов". В нижней

Правила доступа для 192.168.2.20:

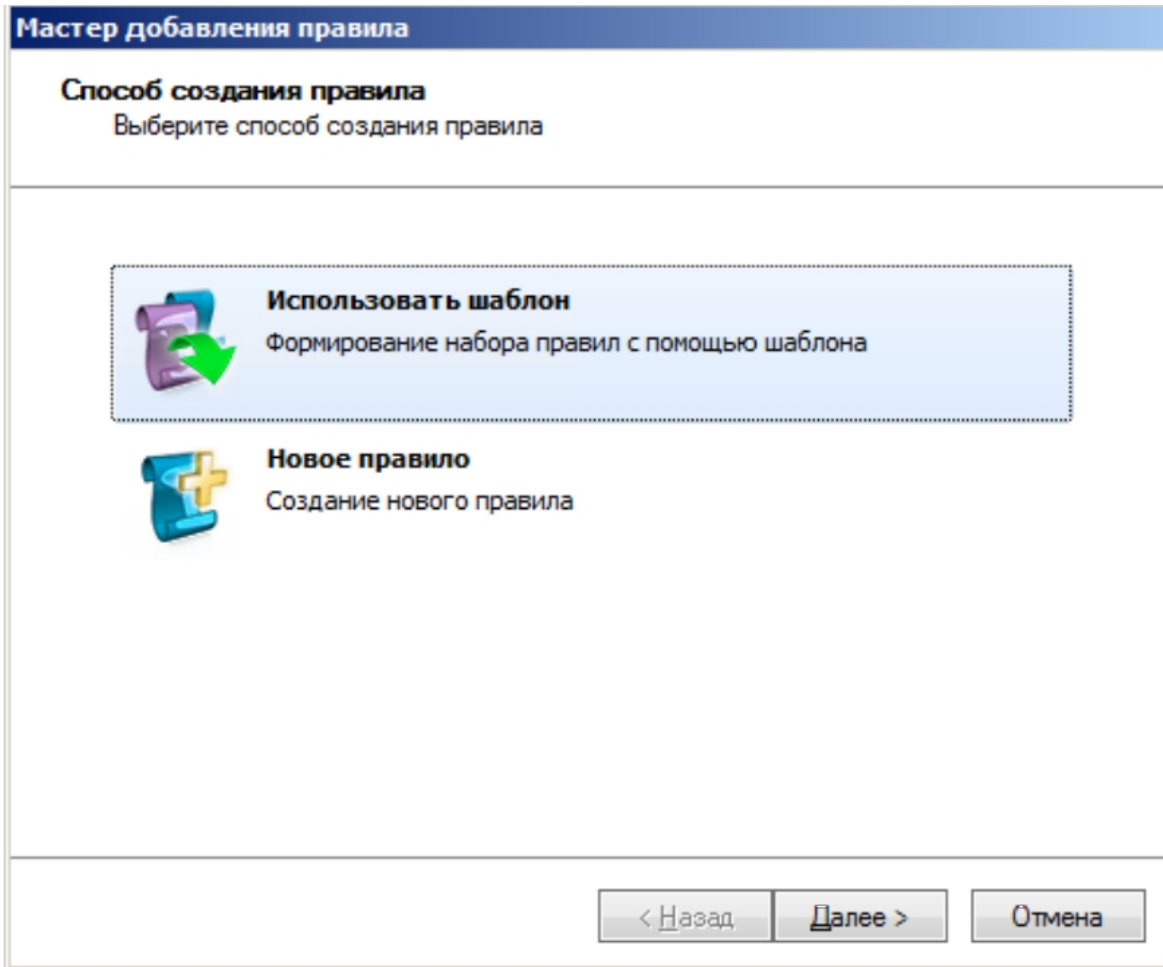
Всего правил: 3

Описание	Состо...	Пользоват...	Компьютер...	Прото...	Исход...	Порт н...
Доступ к консоли вирт...	Вкл	avi@VGATE	*	TCP	Любой	2179
Доступ к службе RPC	Вкл	avi@VGATE	*	TCP	Любой	135
Доступ к службе WMI	Вкл	avi@VGATE	*	TCP	Любой	3910

- Создать...
- Удалить
- Свойств...
- Выключ...
- Экспорт

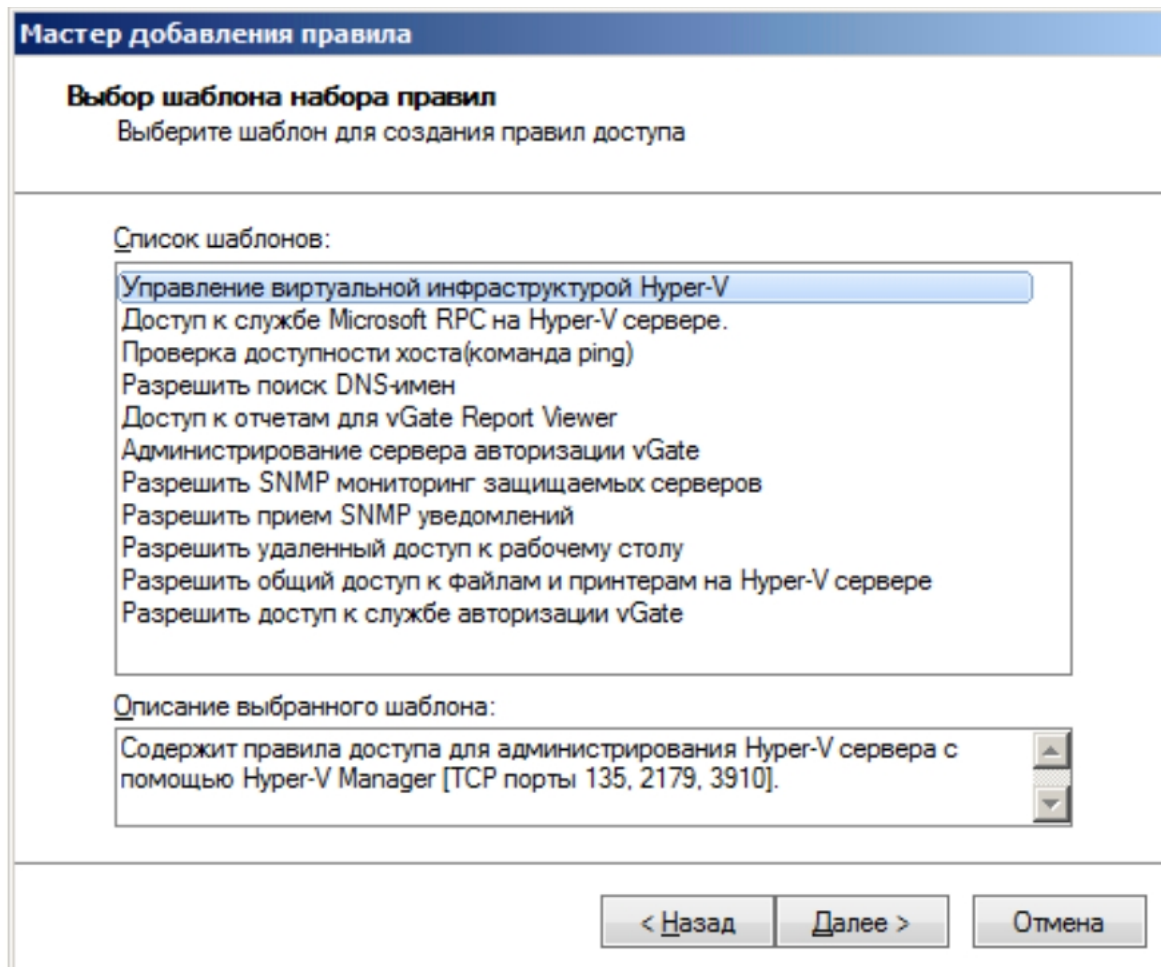
Для создания нового правила нажать кнопку-ссылку "Создать правило". На экране появится

Автор:
27.12.14 20:10 -



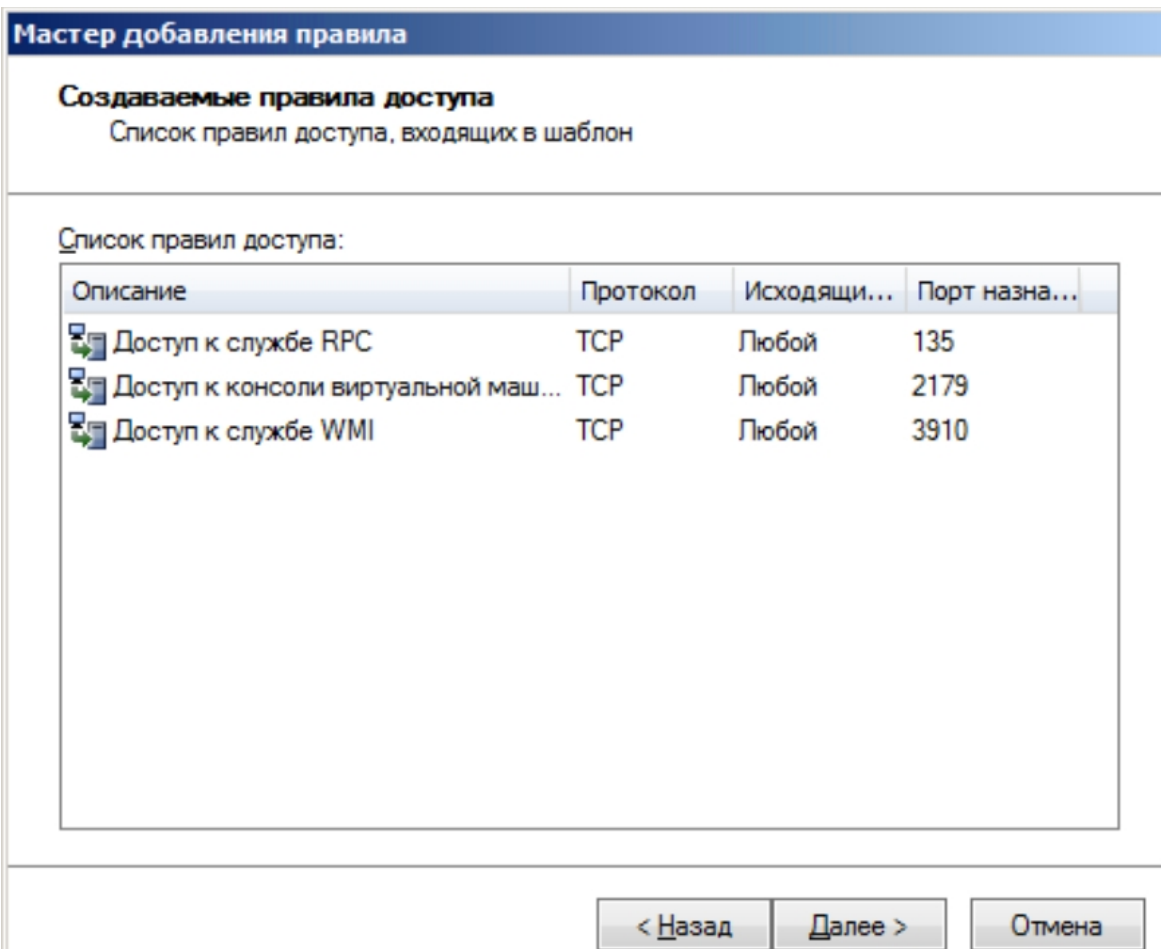
экран на первом этапе создания правил выбрать вариант "Использовать шаблон", на

Автор:
27.12.14 20:10 -



Выберите необходимый шаблон и нажмите кнопку "Далее". На экране появится

Автор:
27.12.14 20:10 -



~~Скриншоты, сделанные с помощью программы Snagit~~

Автор:
27.12.14 20:10 -

Мастер добавления правила

Новое правило
Настройте параметры нового правила

Имя:

Описание:

Тип протокола:

Исходящий порт:

Порт назначения:

< Назад **Далее >** Отмена

Укажите необходимые значения параметров и нажмите кнопку "Далее" (стрелка вправо) <http://www.thin.kiev.ua/vgate/ru/faq/faq.html>