



МАРАТ ДАВЛЕТХАНОВ, программист, системный администратор  
и независимый журналист в одном лице

## Подключаем сеть к Интернету с помощью UserGate Proxy&Firewall

В современных условиях задача подключения корпоративной сети к Интернету вышла за рамки простой организации совместного доступа к нему сотрудников. А поэтому решить ее без использования дополнительного ПО невозможно

Сегодня бизнес (обычно в лице руководства организации) предъявляет особые требования к подключению корпоративной информационной системы к Интернету. Если раньше задача, которая ставилась перед системными администраторами, часто выражалась словосочетанием «лишь бы почта ходила», то теперь она сильно усложнилась. Так произошло и в нашем случае. Пока к Интернету были подключены буквально пять руководящих сотрудников, можно было обойтись простейшим бесплатным прокси-сервером. Однако когда было принято решение подключить к Сети всех офисных сотрудников (более 50 человек), пришлось задуматься о реорганизации системы доступа.

Руководство компаний не хочет допускать неограниченного и неконтролируемого использования Интернета. И его можно понять. Ничем не сдерживаемые сотрудники способны скачивать фильмы, загружая интернет-канал, устанавливать и запускать на своих компьютерах подозрительные программы, посещать потенциально опасные сайты, часами сидеть в «Одноклассниках», забывая про свои обязанно-

сти. Все это становится причиной дополнительных затрат и уменьшения производительности труда.

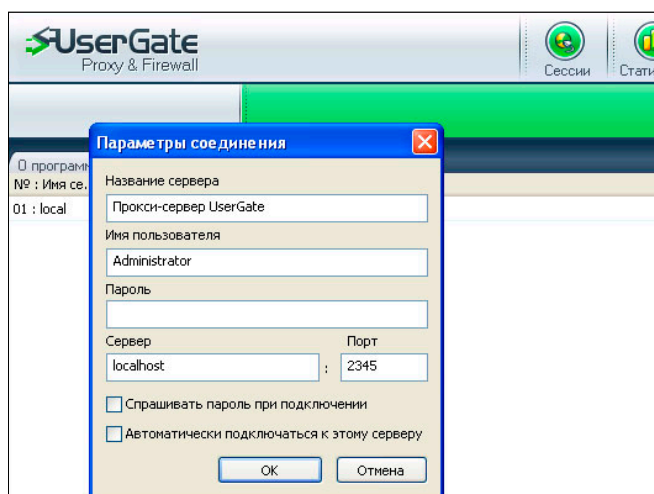
Поэтому задача была поставлена следующая – организовать подключение к Интернету всех рабочих станций компании, предусмотрев возможность расширения системы (в надежде на рост бизнеса и числа сотрудников в будущем). Прокси-сервер должен интегрироваться в Active Directory (администрировать вручную две сотни сотрудников просто-напросто нереально), а также иметь возможность авторизации пользователей по их AD-логинам. При этом, помимо технической стороны, необходимо предусмотреть целый ряд организационных вопросов, а именно ограничить потребляемый трафик и занимаемую полосу пропускания для отдельных пользователей и групп, пресечь нецелевое использование глобальной Сети, обеспечить защиту от проникновения извне вирусов и другого вредоносного ПО.

Сегодня на рынке присутствует немало прокси-серверов. Наиболее известными из них являются UserGate Proxy&Firewall, Kerio Control, Traffic Inspector и WinGate. Из этого перечня был выбран первый вариант. На решение повлиял в первую очередь набор функциональных возможностей, в частности, возможность интеграции с Active Directory, система фильтрации сайтов по категории, возможность контроля сетевой активности разных приложений, наличие интегрированных антивирусных модулей и пр.

Еще одним важным отличием продукта UserGate Proxy&Firewall является наличие версии, сертифицированной ФСТЭК России. Причем можно сначала приобрести обычный вариант, а потом, если потребуется (например, в связи с началом проверок информационных систем на соответствие ФЗ «О защите персональных данных»), доплатить и апгрейдить продукт до сертифицированного.

Нельзя не отметить простоту внедрения UserGate Proxy&Firewall. Данный прокси-сервер может развертываться в существующую инфраструктуру без ее изменения. Практически вся настройка осуществляется на интернет-шлюзе. В некоторых случаях может потребоваться определенная работа с клиентскими машинами. Однако прозрачный режим работы прокси-серверов, DNS-форвардинг

Рисунок 1. Создание подключения к прокси-серверу



и использование NAT позволяют свести необходимость вмешательства в ИС к минимуму.

Что касается недостатков UserGate Proxy&Firewall, то здесь можно отметить только необходимость ежегодного обновления лицензии на систему фильтрации сайтов по категориям и антивирусных модулей. С технической точки зрения возможностей продукта вполне достаточно для решения поставленной задачи.

Лицензия на сам продукт UserGate Proxy&Firewall бессрочная в пределах одной версии. Ее стоимость зависит от количества сессий и колеблется в очень широких пределах – от 4,5 (до 5 сессий) до 57 000 рублей (неограниченное количество сессий).

### Установка UserGate Proxy&Firewall

UserGate Proxy&Firewall состоит фактически из трех модулей. Первый – непосредственно сам прокси-сервер. Его необходимо установить на компьютер, играющий роль интернет-шлюза. В идеале это отдельный ПК, к которому подключена линия (или линии) связи от провайдера. Данный компьютер должен обладать как минимум двумя сетевыми интерфейсами (при наличии нескольких подключений к Интернету их может быть больше), один из которых необходимо присоединить к локальной сети. В небольших сетях прокси-сервер может быть запущен на контроллере домена. Хотя это и не совсем корректное решение с точки зрения информационной безопасности.

Вторая часть UserGate Proxy&Firewall – консоль управления. Именно с ее помощью сотрудники ИТ-отдела осуществляют администрирование системы совместного использования Интернета. Консоль управления UserGate Proxy&Firewall

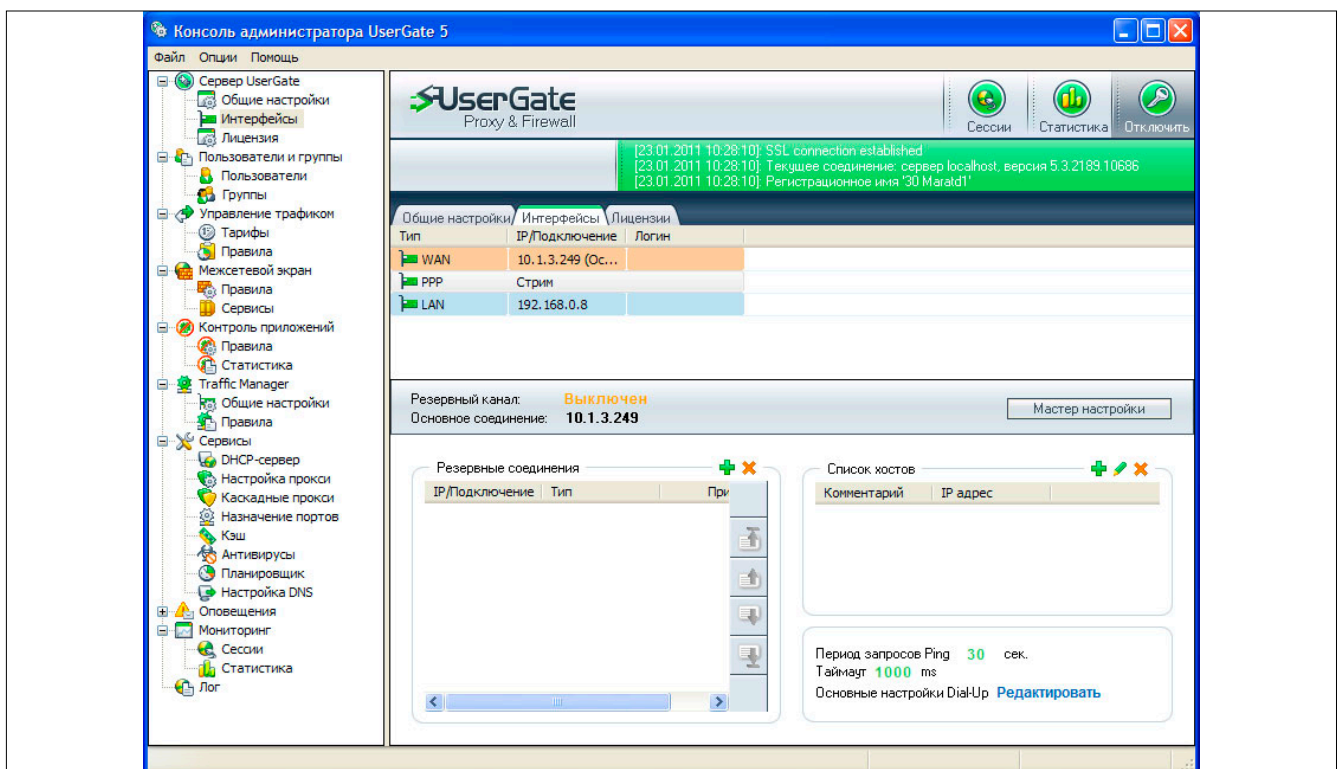
способна работать как локально, так и удаленно. То есть ее можно установить и запустить на любом компьютере сети и оттуда администрировать прокси-сервер, что весьма удобно. Третья часть отвечает за просмотр статистики использования глобальной сети. С ее помощью осуществляются мониторинг работы сотрудников и прочие подобные задачи.

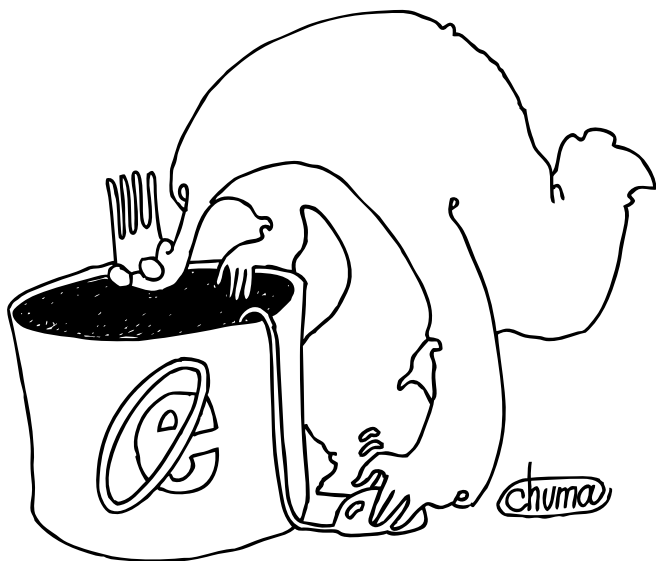
Дистрибутив прокси-сервера можно загрузить непосредственно с сайта разработчика или получить его на диске (при покупке «коробки»). Сама процедура установки в принципе ничем особым не выделяется. Единственный момент, на который стоит обратить внимание, – выбор устанавливаемых компонентов.

Во-первых, именно на этом происходит разделение трех модулей. То есть непосредственно на интернет-шлюз можно установить все части (чтобы обеспечить возможность локального администрирования). При установке продукта на компьютер системного администратора достаточно оставить только консоль управления и статистику. Дополнительно последний модуль можно установить на ПК руководителя или ответственного сотрудника, дабы он мог самостоятельно проверять использование Интернета работниками компании.

Во-вторых, при установке прокси-сервера на интернет-шлюз можно выбрать набор доступных компонентов. Так, например, если была приобретена версия без антивирусов (а их в системе два, причем они могут работать как каждый по отдельности, так и совместно, что обеспечивает максимальную степень защиты), то их не стоит устанавливать. Также можно отключить веб-статистику (система, позволяющая просматривать статистику использования Интернета прямо через браузер), если использовать ее не планируется.

Рисунок 2. Настройка сетевых интерфейсов





UserGate Proxy&Firewall,  
несмотря на весьма и весьма  
широкие возможности,  
очень прост в управлении

В ходе инсталляции основной части прокси-сервера происходит установка драйверов, необходимых для работы NAT. Соответственно если на компьютере есть какая-то система проактивной защиты, то нужно дать процессу соответствующее разрешение.

### Базовая настройка прокси-сервера

Все операции по настройке работы прокси-сервера выполняются с помощью консоли управления. В первую очередь необходимо установить подключение к серверу. Если консоль запущена на том же компьютере, что и основная часть UserGate Proxy&Firewall, то в ней сразу после установки будет готовое соединение с именем local. Так что остается только дважды щелкнуть по нему мышкой и начать работу.

Если консоль используется на удаленном ПК, то предварительно требуется создать подключение. Для этого правой кнопкой мыши вызываем контекстное меню и выбираем в нем пункт «Добавить соединение». В открывшемся окне вводим его название, имя пользователя и пароль (по умолча-

нию Administrator и пустой пароль), а также адрес или сетевое имя интернет-шлюза и порт подключения (по умолчанию 2345). После создания подключения установить соединение с прокси-сервером можно в любой момент.

При первом подключении к серверу необходимо выполнить процедуру активации, для чего нужно ввести в открывшемся окне полученный от продавца ключ. Если же вы хотите только попробовать прокси-сервер в действии, то требуется активировать демонстрационный режим. Для этого устанавливаем переключатель в режим «Получить временный ключ», выбираем способ подключения компьютера к Интернету и нажимаем на кнопку «Продолжить».

После активации можно переходить к настройке самого прокси-сервера, то есть основных его сервисов. В UserGate Proxy&Firewall реализовано два способа установки этих параметров. Первый из них – Мастер настройки UserGate. Это пошаговый мастер, на каждом этапе которого задаются определенные параметры. С его помощью в большинстве случаев можно быстро настроить прокси-сервер и подгото-

Рисунок 3. Список прокси-серверов

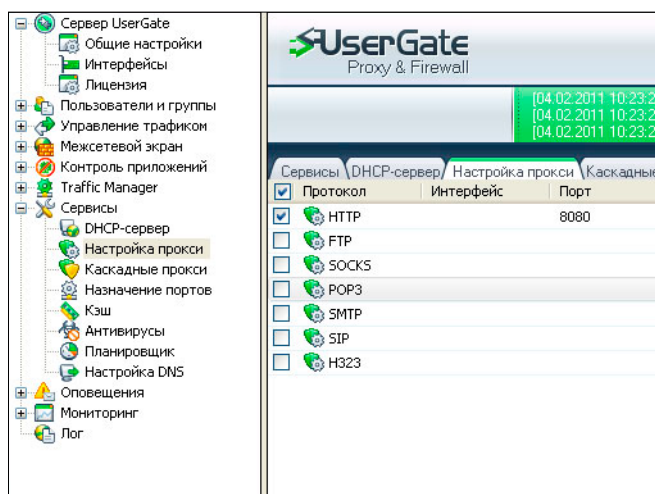
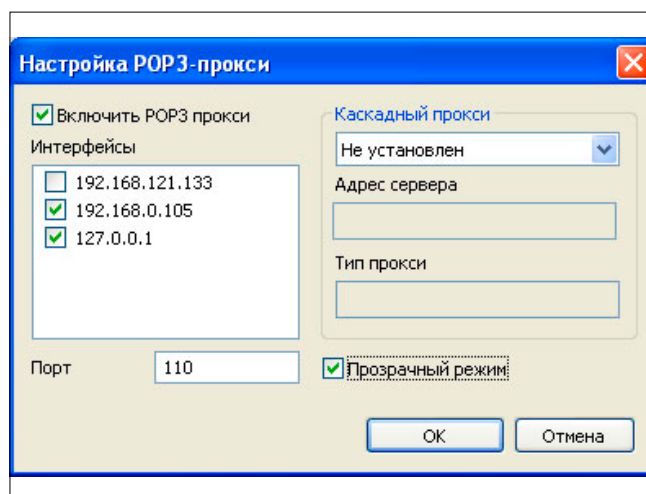


Рисунок 4. Настройка прокси-сервера



вить его к работе. Однако мы рассмотрим другой вариант – ручную установку параметров. Во-первых, такой способ обеспечивает большую гибкость настройки. А во-вторых, зная его, с мастером будет разобратся проще простого.

В первую очередь нужно настроить сетевые интерфейсы. Сделать это можно в разделе «Сервер UserGate → Интерфейсы». На вкладке перечислены все доступные сетевые интерфейсы. На каждом из них дважды щелкаем мышкой и выбираем их тип: WAN – Интернет, LAN – локальная сеть. Здесь же можно активировать резервный канал (если у вас есть второе подключение к Интернету). При этом нужно будет указать его сетевой интерфейс, а также список хостов, при недоступности которых будет включаться перенаправление трафика.

Далее выбираем способ обеспечения совместной работы пользователей в Интернете и настраиваем все необходимые для этого параметры. Здесь нужно сделать небольшое отступление. Сегодня для организации совместного доступа обычно используется либо технология NAT, либо прокси-сервер. Первая обеспечивает большую скорость работы и простоту внедрения (при ее применении нет необходимости перенастройки приложений на клиентских компьютерах). Однако при этом NAT весьма ограничена в настройках. С прокси-сервером же все точно наоборот. Работает он немного медленнее (впрочем, это заметно только в больших группах пользователей) и требует перенастройки клиентского ПО (браузеров, почтовых клиентов, IM-клиентов и пр.). Но зато обладает широкими дополнительными возможностями: фильтрацией сайтов по категориям, ограничением скорости и пр.

Кроме них в UserGate Proxy&Firewall реализован еще один способ – так называемый прозрачный прокси-сервер. При его выборе драйвер NAT перехватывает кли-

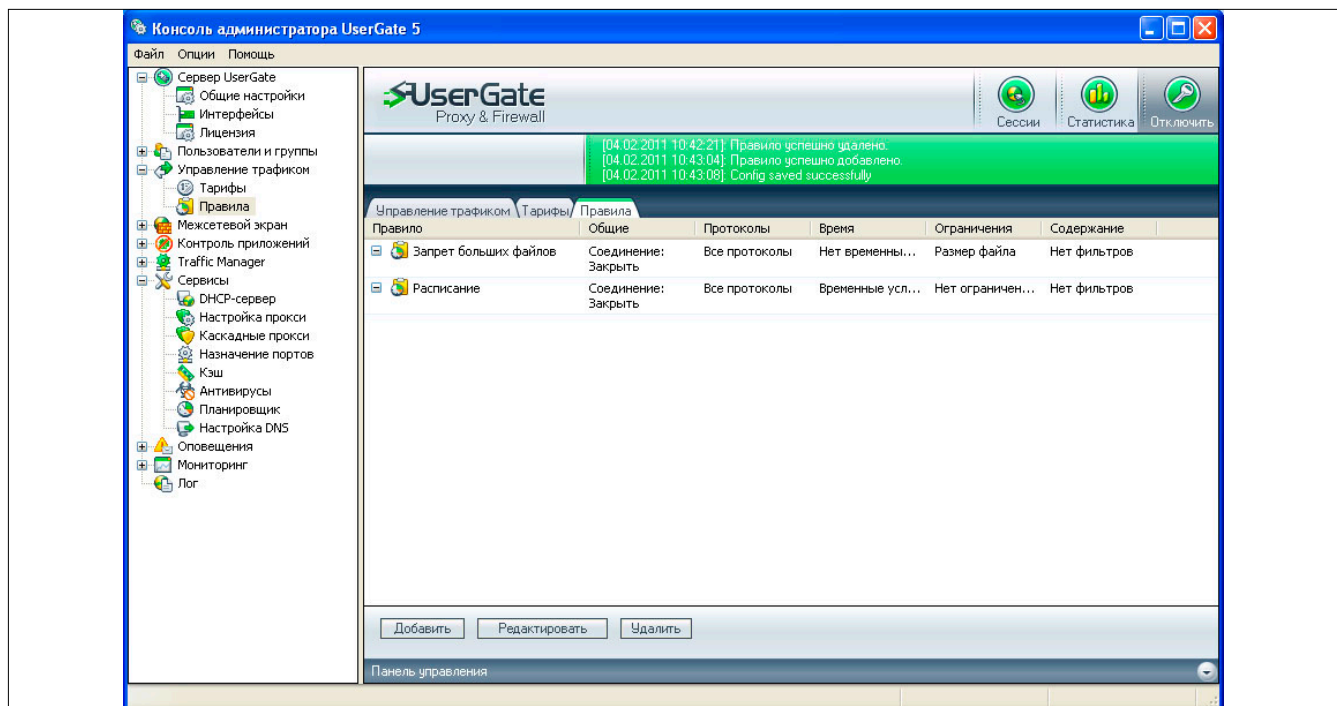
ентские запросы по определенным портам и пересылает их на порт UserGate. Это позволяет избежать необходимости настройки клиентских приложений и предоставляет доступ ко всем дополнительным возможностям. Во многих случаях, особенно в небольших локальных сетях, именно прозрачные прокси-серверы являются оптимальным способом обеспечения совместной работы пользователей в Интернете.

Безусловно, нельзя сказать, что данный режим является своеобразной панацеей. Нет, решение об использовании того или иного варианта должно приниматься в каждом конкретном случае отдельно с учетом существующей инфраструктуры. Подробно останавливаться на этом мы не будем, благо в Интернете можно найти множество информации по данной теме. Отметим только, что в нашем примере мы будем использовать именно прозрачные прокси-серверы.

Определившись со способом совместной работы, переходим в консоли управления в раздел «Сервисы» и выбираем вкладку «Настройка прокси». На ней перечислены все прокси-серверы, реализованные в UserGate Proxy&Firewall. Всего их семь: HTTP, FTP, POP3, SMTP SOCKS, а также SIP и H323 (два последних предназначены для систем IP-телефонии).

Настройка осуществляется очень просто. Щелкаем правой кнопкой мыши на нужном прокси-сервере и выбираем в открывшемся контекстном меню пункт «Редактировать». В первую очередь в открывшемся окне отмечаем в списке с помощью переключателей локальные сетевые интерфейсы. Если этого не сделать, то прокси-сервер будет работать и «наружу». А поскольку при его активации автоматически будет создано нужное правило в брандмауэре, это создаст потенциальную опасность для корпоративной сети. Далее

Рисунок 5. Список правил трафика



включаем прозрачный режим (активируем одноименный переключатель) и нажимаем на кнопку «ОК».

Теперь необходимо настроить систему DNS. Наиболее удобный способ – использование DNS-форвардинга, при котором происходит перенаправление DNS-запросов с прокси-сервера на DNS-сервер провайдера. Для его включения переходим в том же разделе на вкладку «Настройка DNS» и нажимаем напротив надписи «DNS форвардинг» на ссылку «Выключен». При этом она меняет свой статус на «Включен». Если DNS-сервер провайдера указан в настройках TCP/IP-подключения, то можно больше ничего не делать. В противном случае устанавливаем переключатель в положение «Использовать DNS-сервер из списка» и вводим адрес необходимого DNS-сервера вручную.

Последний этап – настройка рабочих станций. Вообще, поскольку мы использовали прозрачные прокси-серверы, изменять параметры приложений (браузер, почтовый клиент и пр.) нет необходимости. Все эти программы будут работать и со старыми настройками. Единственное, что необходимо сделать, – изменить параметры сетевого подклю-

чения. В них необходимо в качестве шлюза и DNS-сервера указать IP-адрес нашего интернет-шлюза.

### Дополнительная настройка прокси-сервера

Использование продуктов класса UserGate Proxy&Firewall для организации корпоративного доступа к Интернету хорошо тем, что они предоставляют весьма широкие дополнительные возможности. С их помощью можно реализовать полноценную политику по применению Интернета сотрудниками компании. А это, в свою очередь, сокращает прямые издержки предприятия (за счет сокращения выплат провайдеру), способствует увеличению производительности труда (путем запрета доступа к социальным сетям, развлекательным проектам и пр.), увеличивает общую безопасность информационной системы (за счет запрета посещения нежелательных сайтов, использования потенциально опасных приложений и т.д.).

Настройка корпоративной политики использования Интернета – процесс сугубо индивидуальный: конкретные условия, правила и ограничения в каждой компании свои. Тем не менее мы можем рассмотреть в качестве примера

Рисунок 6. Правило, ограничивающее доступную полосу пропускания

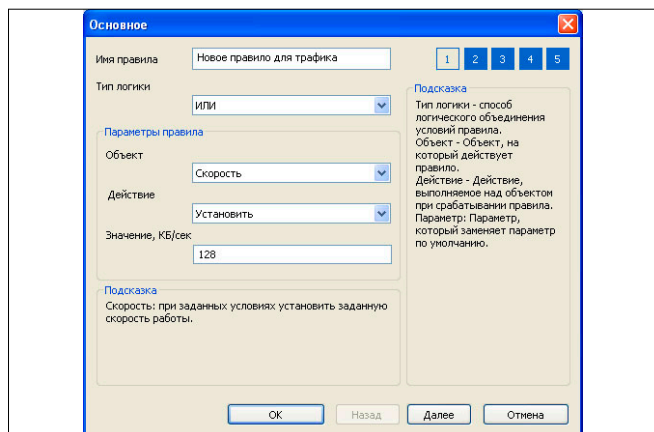


Рисунок 8. Ввод основных параметров группы пользователей

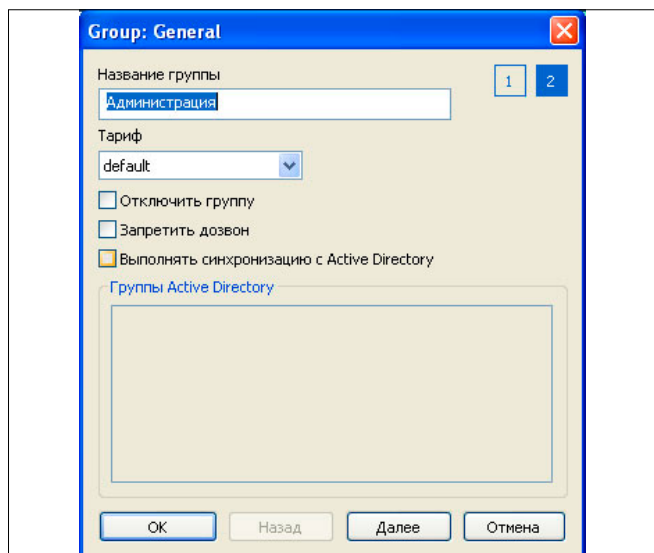


Рисунок 7. Запрет доступа к сайтам по категориям

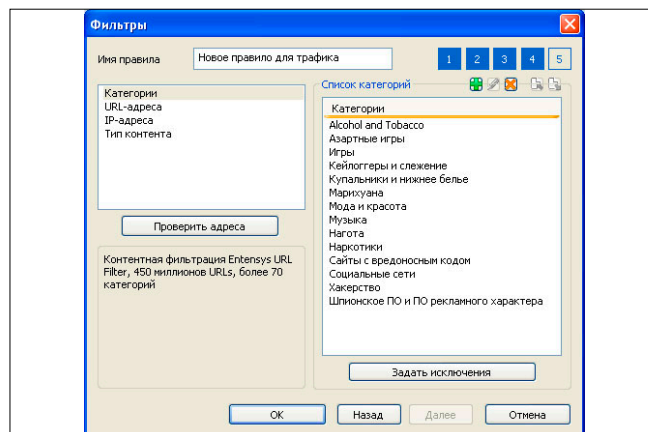
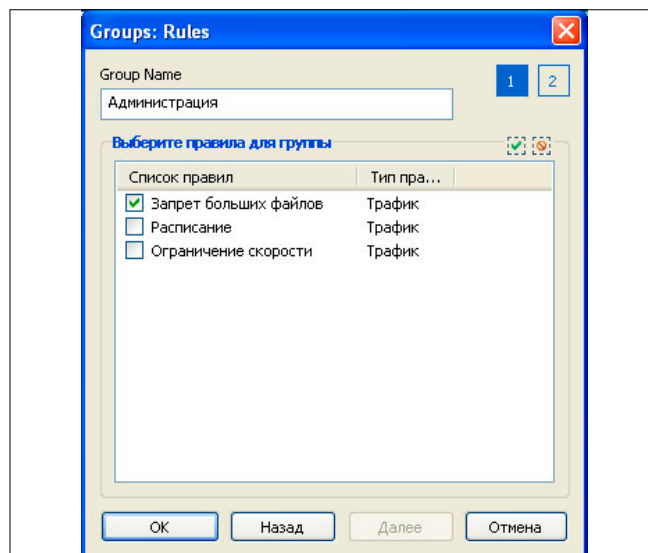


Рисунок 9. Присвоение группе правил обработки трафика



ряд наиболее часто употребляемых параметров, которые наши читатели легко смогут «подстроить» под себя.

Основная масса «тонкой» настройки осуществляется с помощью так называемых правил для трафика. Они определяют поведение системы при выполнении одного или нескольких условий. Правил можно создать сколько угодно, после чего назначать их как отдельным пользователям, так и целым их группам. Такая система обеспечивает высокую гибкость настройки. Для работы с правилами используется одноименная вкладка раздела «Управления трафиком».

Процедура создания правила выполнена в виде пошагового мастера, состоящего из пяти пунктов. Для его запуска достаточно нажать на кнопку «Добавить». На каждом этапе системный администратор может настроить определенные условия и/или действия, связанные с ними. Стоит отметить, что шаги не обязательно выполнять последовательно. Если в правиле не предполагается, к примеру, использовать ограничение, то данный шаг можно пропустить.

Для внесения полной ясности в данный вопрос давайте рассмотрим несколько примеров. Допустим, нам нужно создать для некоторых пользователей ограничение на доступную полосу пропускания. Делается это следующим образом. На первом экране мастера создания правила вводим его название (желательно осмысленное, в противном случае впоследствии будет тяжело присваивать правила), выбираем объект «Скорость», действие – «Установить», после чего вводим в поле «Значение» полосу пропускания (в Кб/с).

Если мы хотим, чтобы ограничение действовало только на просмотр сайтов, а почта загружалась и отправлялась на максимальной скорости, то дополнительно переходим ко второму шагу и снимаем «галочки» с протоколов POP3 и SMTP. Это правило можно еще немного усложнить. К при-

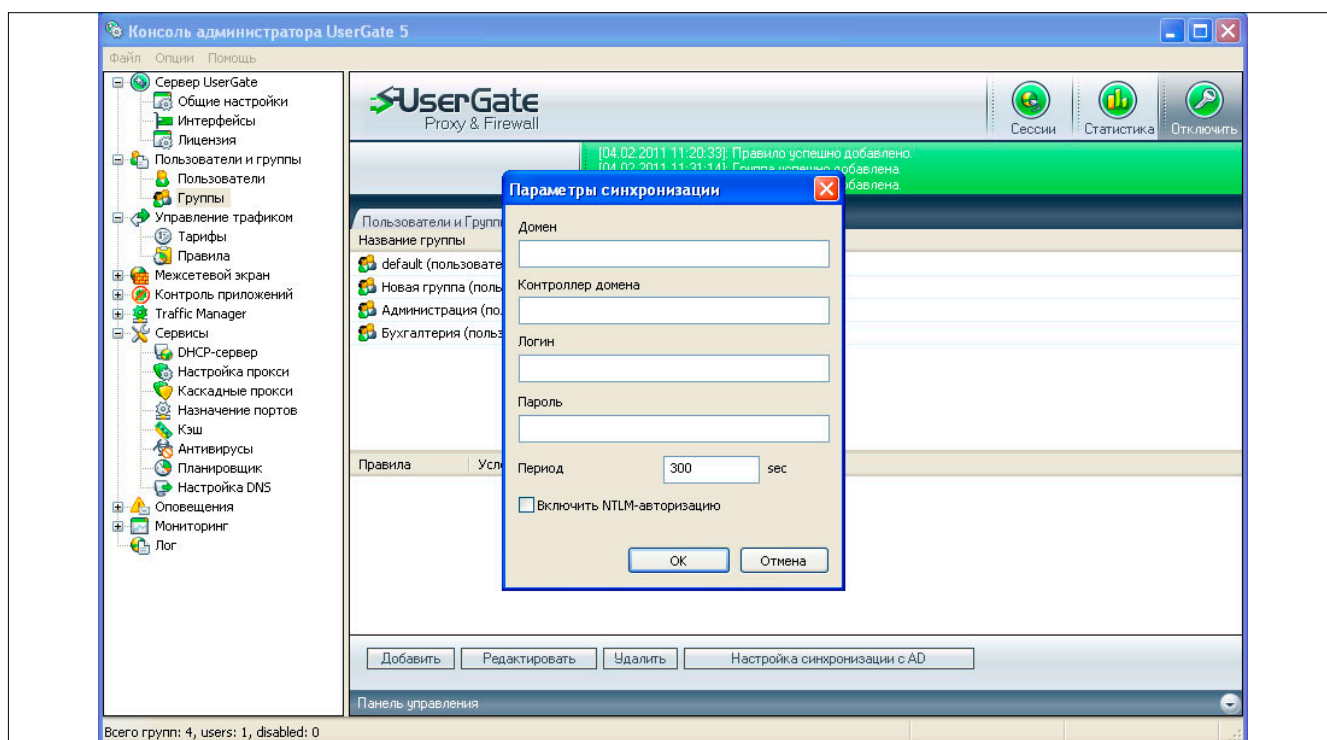
меру, разрешить пользователю работать на максимальной возможной скорости, но только до тех пор, пока он не потребит определенный объем трафика за день, неделю или месяц. Или же сделать так, чтобы правило применялось только во время загрузки больших файлов. Для реализации этой задачи открываем четвертый шаг мастера и вводим либо нужный нам лимит, либо размер файла, с которого будет вступать в силу ограничение.

Можно взять другой пример. Одной из важных особенностей продукта UserGate Proxy&Firewall является поддержка облачной технологии Entensys URL Filtering, которая используется для фильтрации сайтов по категориям. В ее основе лежит огромная (по данным разработчиков, более 500 млн сайтов), адаптированная для русскоязычных пользователей и постоянно обновляющаяся база данных. Данная технология используется в работе – создадим правило, запрещающее доступ к социальным сетям и развлекательным порталам. Для этого на первом этапе мастера введем название нового правила, выберем в списке «Объект» значение «Соединение», а в списке «Действие» – пункт «Закрыть». После этого перейдем на пятый шаг, установим среди типов фильтрации «Категории» и добавим в список те из них, посещение которых сотрудникам не нужно для выполнения их трудовых обязанностей.

Можно сделать работникам некоторое послабление – разрешить им доступ к социальным сетям, но, к примеру, только во время обеденного перерыва. Для этого переходим на третий шаг мастера и с помощью наглядной таблицы указываем часы действия правила – все рабочее время.

На этом разговор о «тонкой» настройке прокси-сервера мы завершим. Хотя, если говорить откровенно, мы не рассмотрели еще целый ряд возможностей UserGate

Рисунок 10. Настройка синхронизации с Active Directory



Proxy&Firewall: ограничение сетевой активности разных приложений, сервер IP-телефонии, систему распределения нагрузки между несколькими внешними каналами, перенаправление портов и пр. Просто разобрать их все в одной статье совершенно нереально.

### Работа со списком пользователей

В целом наш прокси-сервер готов к работе. Осталось только разобраться с пользователями. Сразу отметим, что в UserGate Proxy&Firewall возможно управление как отдельными учетными записями, так и целыми их группами. Понятно, что если речь идет о небольшой компании с 10 сотрудниками, то можно настройки устанавливать персонально для каждого. Но вот в большой информационной системе без разделения сотрудников на группы с разными правами и настройками явно не обойтись.

Сначала создаем нужные группы. Для этого открываем раздел «Пользователи и группы» и переходим на вкладку «Группы». Поочередно нажимаем на кнопку «Добавить» и вводим в открывшемся окне название. После этого переходим на вторую вкладку и с помощью переключателей отмечаем в списке заранее созданных правил те, которые должны действовать на эту группу.

Далее заполняем список сотрудников, имеющих право на использование Интернета. В большинстве случаев удобнее всего синхронизировать UserGate Proxy&Firewall с Active Directory, чтобы данные об учетных записях загружались автоматически. Для этого переходим в раздел «Пользователи и группы», открываем вкладку «Группы», нажимаем на кнопку «Настройка синхронизации с AD» и в открывшемся окне вводим данные домена. Затем переходим к свойствам введенных нами групп, активируем в каждой из них параметр «Выполнять синхронизацию с Active Directory», после чего выбираем в списке те группы домена, пользователи из которых будут «присвоены» текущей группе доступа прокси-сервера.

В UserGate Proxy&Firewall предусмотрен и ручной ввод учетных записей пользователей с помощью специального пошагового мастера. Давайте рассмотрим его и заодно разберем, какие свойства есть у аккаунтов в UserGate Proxy&Firewall.

Итак, на первом этапе нужно ввести имя пользователя, группу, к которой он принадлежит, и параметры авторизации. И вот на последних стоит остановиться подробно. В UserGate Proxy&Firewall реализовано девять различных способов аутентификации пользователей. Есть среди них достаточно простые, например, по IP-адресу компьютера, MAC-адресу сетевой карты или по ним обоим сразу (IP+MAC). При их выборе нужно просто ввести необходимые значения. Другие варианты более сложны. Например, можно отметить HTTP-авторизацию. При ее выборе пользователь должен будет ввести созданные системным администратором логин и пароль. Также авторизация может осуществляться по логину Active Directory. Все способы имеют достоинства и недостатки, и использование каждого из них оправдано в той или иной ситуации.

На втором этапе вводятся дополнительные параметры: адрес электронной почты, роль в веб-статистике (обычно простой пользователь, который может просматривать только свои данные), номер IP-телефона. Кроме того, здесь же задаются ограничения на доступную пользователю полосу пропускания.

На третьем шаге можно указать различные правила, которые будут действовать для данного пользователя: ограничения трафика, использование NAT и приложений. Делать это необходимо, если настройки данной учетной записи должны отличаться от групповых (по умолчанию на аккаунт действуют все правила, определенные в параметрах группы).

\*\*\*

Мы подробно рассмотрели процедуру внедрения и первоначальной настройки UserGate Proxy&Firewall. Как видно, данный прокси-сервер, несмотря на весьма и весьма широкие возможности, очень прост в управлении. Запустить его сможет любой системный администратор или даже опытный пользователь. В статье разобран только самый распространенный способ настройки прокси-сервера. В некоторых корпоративных системах процедура внедрения может несколько отличаться от описанной. Все зависит от конкретной ситуации: существующей инфраструктуры, количества пользователей и их потребностей. **BOX**

Рисунок 11. Настройка основных параметров пользователя

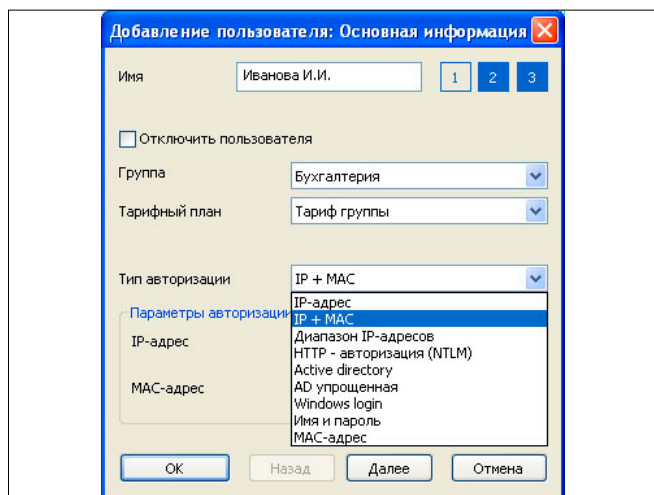


Рисунок 12. Выбор правил для пользователя

