Сегодня хочу рассказать о необычном продукте росскийской разработки — интернет шлюзе ИКС. Ранее мне не приходилось о нем ничего слышать, тем более пробовать в деле, но после тестов могу сказать, что решение мне в целом понравилось. Это платный продукт с freebsd под капотом, но все управление только через web-интерфейс. В консоль лазить не надо.

> Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую по программе, основанной на информации из официального курса **MikroTik Certified Network Associate**. Курс стоящий, все подробности читайте по ссылке. Есть бесплатные курсы.

Содержание:

Цели статьи

1. Рассказать об интернет-шлюзе, который позиционирует себя как коробочное решение для настройки безопасного шлюза с ограничением доступа к ресурсам интернета, контентной фильтрацией в том числе https трафика с подменой сертификата.
2. Настроить фильтрацию https трафика в том числе по содержимому web страниц.

3. Потестировать остальной функционал продукта — voip, почтовый, файловый, jabber сервер.
4. Поделиться своим мнением о шлюзе.

Введение

Эта статья заказная. Ко мне обратились авторы продукта и предложили оценить его и написать по нему статью. Требований никаких не предъявляли. С сайта скачивается полнофункциональный триал на 35 дней. Я посмотрел описание, меня заинтересовал функционал, поэтому я согласился. У меня есть пара очень старых статей, которые описывают заявленный в ИКС функционал, но делают это не очень хорошо, поэтому под статьями десятки комментариев. Функционал востребованный, статьи популярны, с множеством комментариев и вопросов. Вот эти статьи:

- Настройка прокси сервера на CentOS 7 (squid+AD+sams2)
- Как заблокировать сайт микротиком

Мне показалось, что готовое коробочное решение, которое решает схожие задачи, будет полезно и интересно. Забегая вперед скажу, что это так и есть. Продукт в целом мне понравился, сделан добротно. Заявленный функционал работает нормально.

Для прокси серверов сейчас практически нет альтернатив, везде используют squid. К нему колхозят всякие авторизации, статистики, отчеты и т.д. Получается всегда так себе. Обслуживать неудобно. Я сам лично использовал шлюзы на базе описанного sams + squid с авторизацией по ip. Так же настраивал squid на работу в AD с доступом к ресурсам по группам домена. Работало вполне нормально, но не очень удобно.

Со временем перестал работать с этими продуктами, потому что мне надоело обслуживать все это. Надоели наколенные поделки. Готовые платные шлюзы сам не использовал никогда, потому что заказчики чаще всего не хотят платить за то, что можно настроить бесплатно, а я не любил это настраивать. В итоге просто исключил этот сегмент из своей сферы деятельности.

Что такое Интернет Контроль Сервер (ИКС)

Переходим теперь к ИКС. Сами разработчики позиционируют свой продукт как безопасный интернет-шлюз в связи с тем, что он соответствует требованиям ФСТЭК России. В чем именно состоят эти требования и насколько это влияет на безопасность я судить не берусь, потому что с сертификацией не знаком вообще.

Тем не менее, с безопасностью, по идее, проблем быть не должно, потому что под капотом этого решения стандартные проверенные временем инструменты. В основе операционная система **Freebsd**, которую традиционно любят использовать в сборках под шлюзы. Например, самый популярный

шлюз с веб интерфейсом — pfsense использует freebsd.

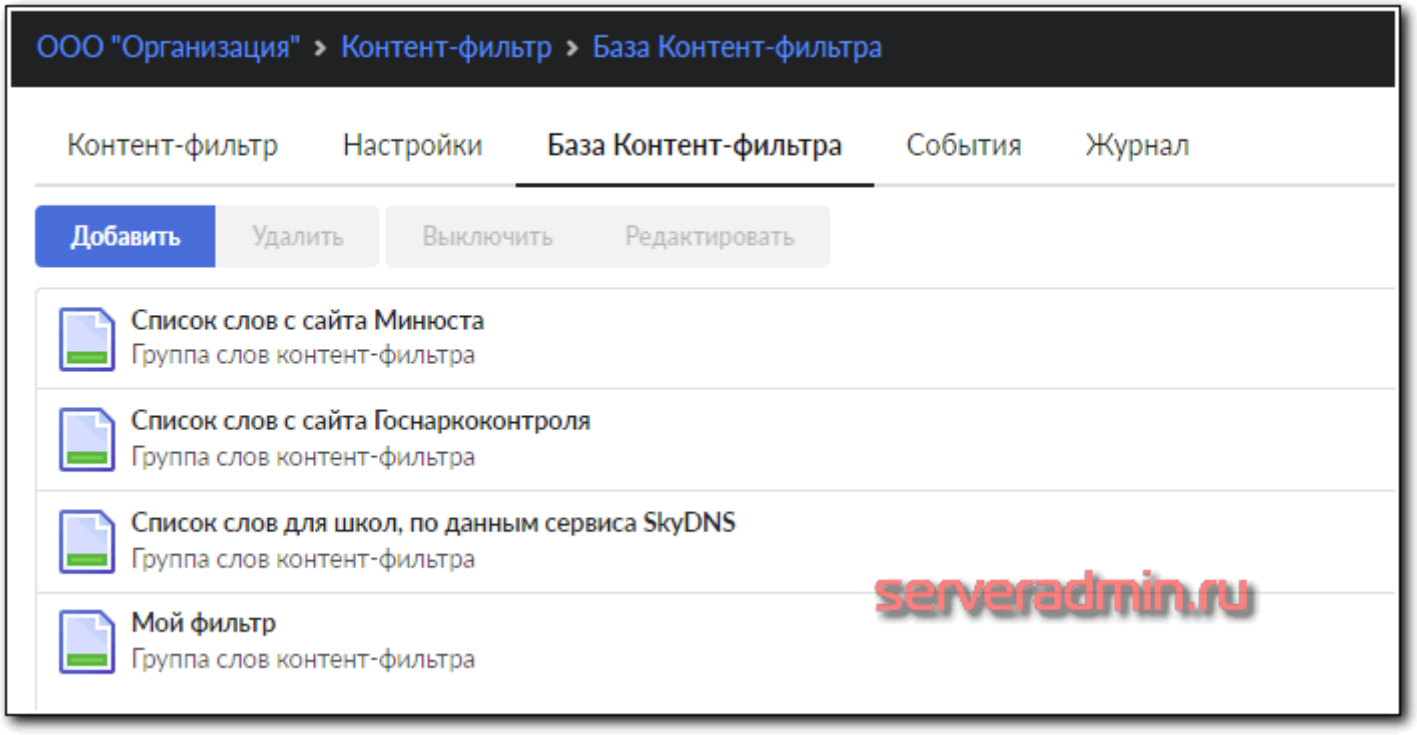
В качестве firewall используется традиционные для bsd систем **ipfw** и **pf**, в качестве прокси все тот же **squid**, в качестве телефонии **asterisk**, файлового сервера **samba** и т.д. То есть все стандартное, но завернутое в единый web интерфейс. Мне сам интерфейс понравился. Выглядит современно, красиво, работает шустро. В процессе настройки у меня к нему претензий не было.

Среди преимуществ разработчики выделяют следующее:

- Отечественная разработка, зарегистрированная в едином реестре российских программ для ЭВМ и БД. Соответствует ФЗ №188 и статье 14 ФЗ №44. Может использоваться в бюджетных учреждениях и коммерческих организациях любого уровня.
- Объединение в одном продукте практически всех служб, которые требуются для функционирования современной локальной сети — шлюз, почта, телефония, файловый сервер, чат.
- Простая и интуитивная (тут у меня есть сомнения) настройка, с которой справится любой эникей.
- Льготные цены для учебных заведений и библиотек.

После изучения функционала, просмотра цен и тестирования, я понял, в какую нишу в основном метят разработчики — бюджетные учреждения, в том числе школы. Смысл в том, что сейчас все больше и больше всяких законодательных требований к контролю за интернетом и трафиком. Бюджетные учреждения обязаны как-то заниматься этим вопросом, а не пускать его на самотек и доверять своим админам, которые, как известно, не очень, из-за низких зарплат бюджетников.

В целом, продукт отвечает на поставленные вопросы. Он действительно прост в управлении и имеет под капотом все необходимые инструменты для выполнения требований закона по контролю за интернет активностью. Он автоматом обновляет списки Минюста и Госнаркоконтроля и ограничивает доступ в интернет в соответствии с этими списками.



Когда я изучал сайт и читал описание, думал, что это очередная поделка с лейблом «отечественное», созданное под распил бюджетных денег. Когда уже потестировал, могу сказать, что продукт в целом качественный и решает вопросы не только бюджетников, но и коммерческих организаций. Я бы такой купил и поставил в организацию. Думаю, после описания возможностей и демонстрации отчетов, вам тоже его захочется. Это я для тех, кто настраивал отчеты сквида в Sams или LightSquid и им подобным панелям. В ИКС все гораздо удобнее и нагляднее.

Ну и помимо собственно функционала прокси-сервера с анализом трафика там есть мультиван, объединение сетей, отказоустойчивость на основе CARP и многое другое. То есть продукт вполне функциональный с претензией на enterprise.

Некоторые полезные ссылки:

- Описание и основные преимущества
- Видеоуроки и прошедшие вебинары
- Документация в wiki и pdf
- Загрузка (данные можно казать любые, проверки нет) и стоимость.

О ценах судить не берусь. У каждого свои представления. Если все настраивать самостоятельно, то нужен будет админ с зарплатой каждый месяц выше, чем единоразовая покупка, скажем, на 100 пользователей. Сужу по зарплатам в Москве. Этим же шлюзом сможет управлять любой эникей, посмотрев обучающие ролики и обратившись в тех поддержку.

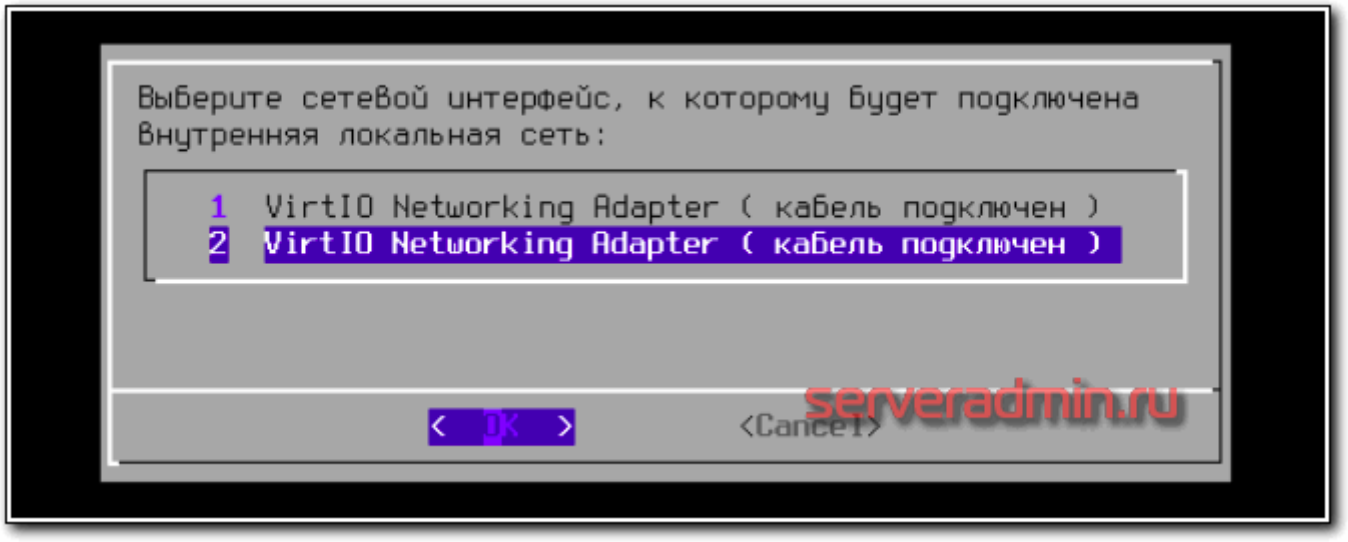
Установка российского интернет-шлюза ИКС

С установкой российского интернет-шлюза ИКС никаких сложностей нет. Инсталлятор очень простой с минимумом настроек, плюс на русском языке. Поставить сможет практически любой и не возникнет вопросов, а как разбить диск на разделы, сколько выделить под /var, /home и т.д. :)

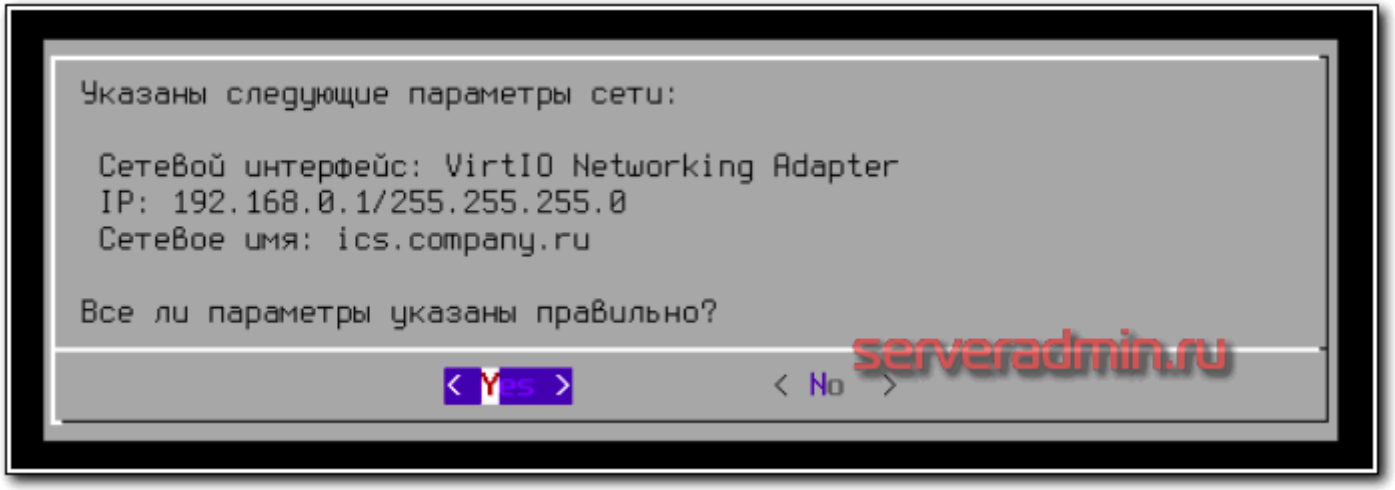
Системные требования тоже очень скромные. На сайте они указаны, но понятно, что это все очень условно. Внутри неприхотливая freebsd, которая в качестве шлюза требует очень скромных ресурсов. А вот если вы развернетесь на полную с установкой почтового и файлового сервера, то ресурсов потребуется уже побольше. Для простого шлюза начать можно с 1 ядра и 2 Гб памяти. Если есть возможность, я бы начал с 2 ядра, 4 гига оперативы. Диск подбирать по потребностям, начиная 50 Гб. Я буду ставить на виртуальную машину KVM.

Установщик нас встречает выбором языка.

Дальше принимаете лицензионное соглашение и переходите к настройке сети.

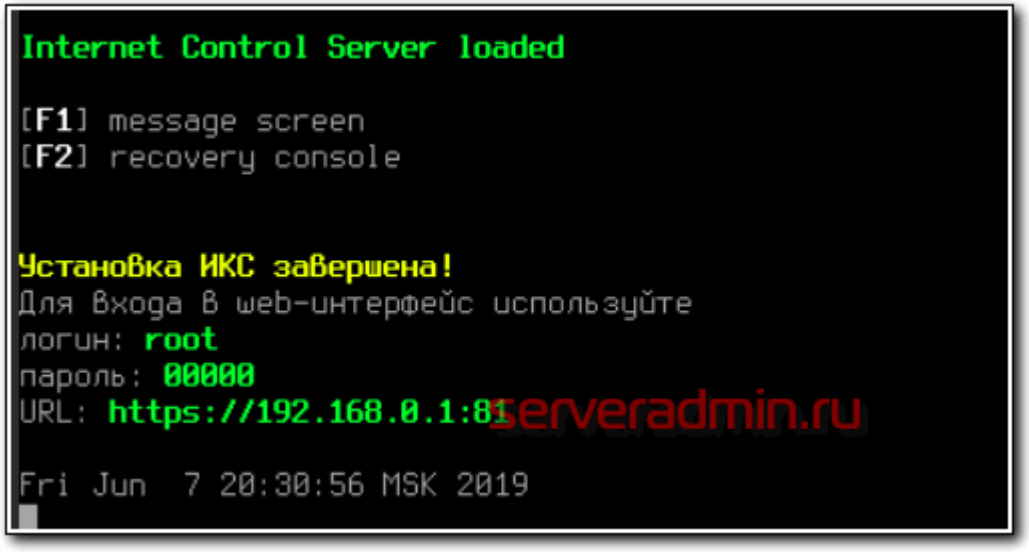


Выбрать нужно интерфейс, который будет смотреть в локалку. Указываем ему ip адрес, маску и имя сервера. Я все выбрал дефолтное — 192.168.0.1/24.

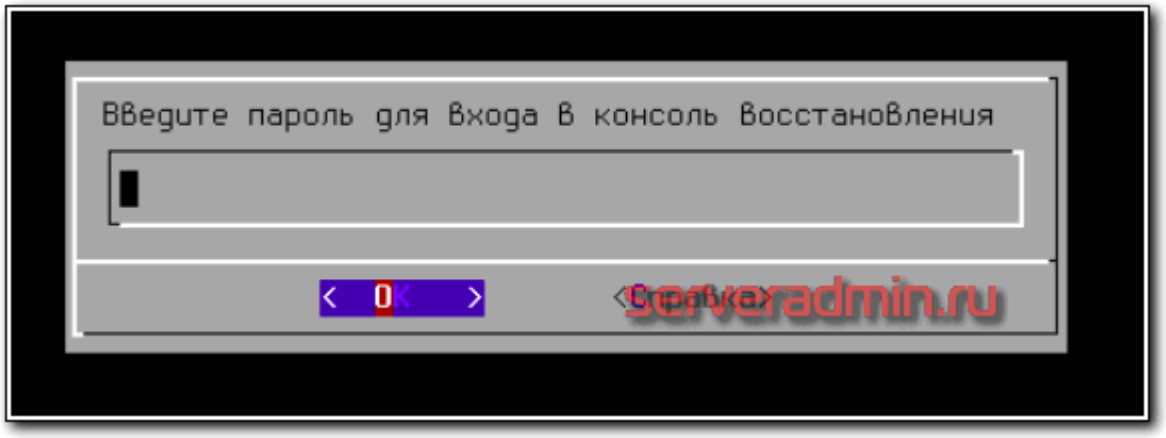


Дальше выбираем диск, часовой пояс и начинается установка. Не буду на этом задерживаться, там нечего выбирать, все оставляем дефолтное. После завершения установки извлекаем установочный диск и перезагружаем сервер.

После загрузки сервера видим информацию для подключения к web интерфейсу. Учетная запись root и пароль 00000 (пять нулей).



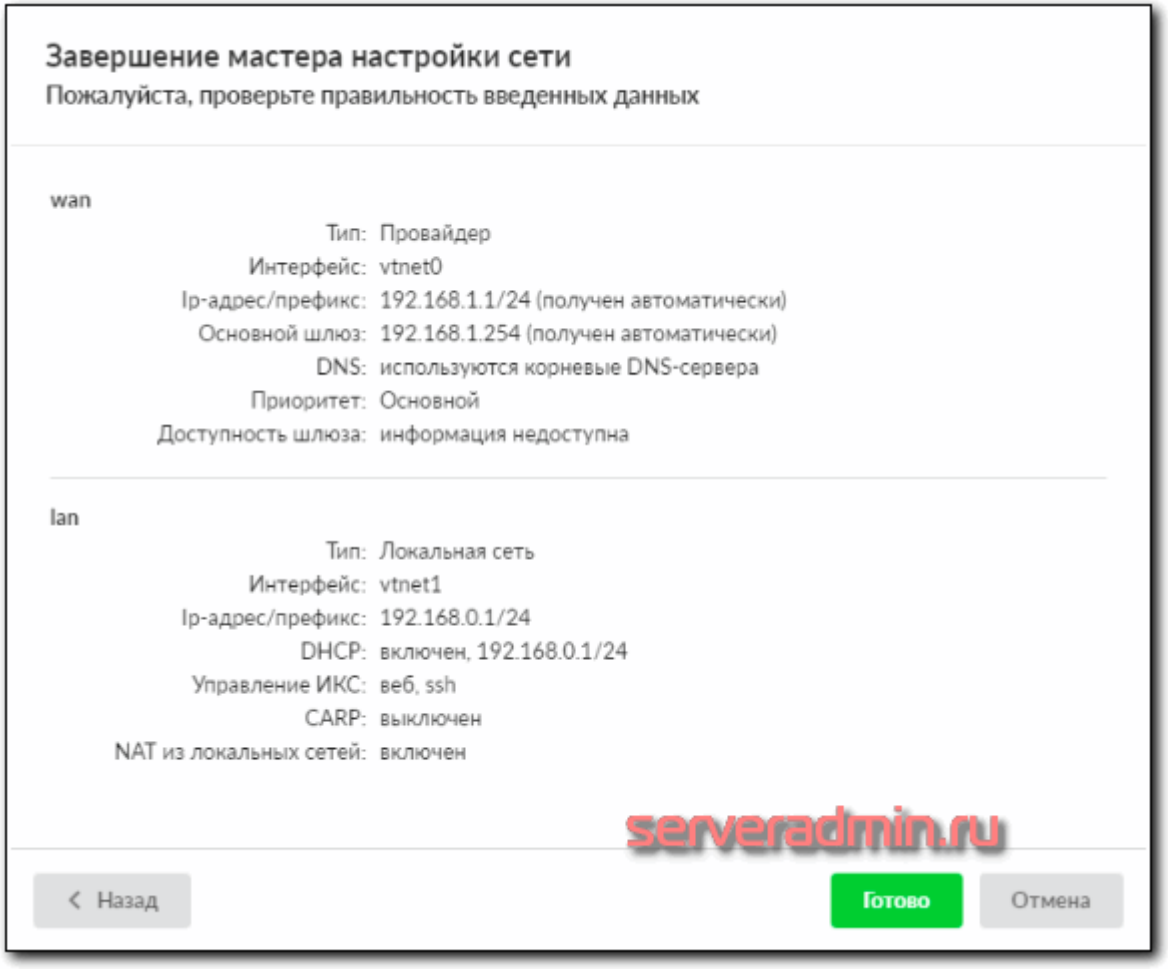
У меня иногда почему-то сразу же загружалась консоль восстановления, через которую можно так же управлять сервером. Если что, ее дефолтный пароль **recovery**. Эта инфа есть в документации, но я не сразу понял, что это вообще такое и какой нужен пароль.



Теперь можно отправляться по адресу *https://192.168.0.1:81* и начинать настройку безопасного интернет шлюза.

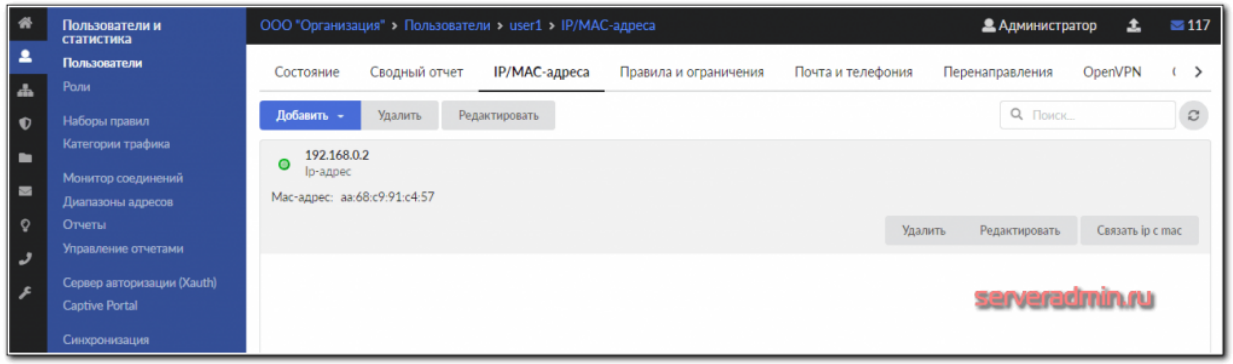
Настройка доступа в интернет

В принципе, шлюз уже сейчас практически готов к работе. Нам нужно только выполнить начальную настройку сетевых адаптеров. Для этого идем в раздел **Сеть -> Мастер настройки сети**. Указываем параметры для WAN и LAN интерфейсов и применяем их. Рекомендую осмысленно называть интерфейсы. По именам потом проще будет оперировать в настройке firewall.



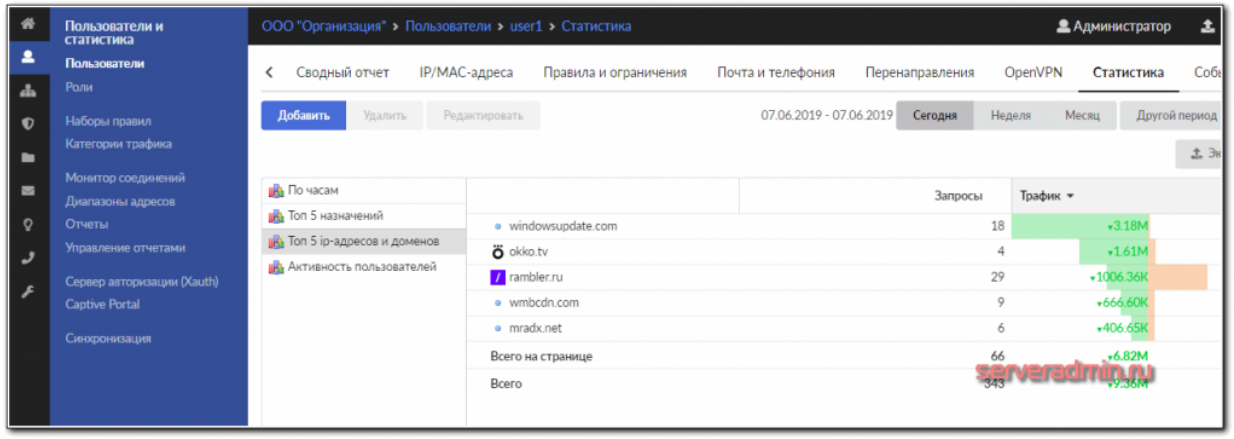
У меня получилось примерно так. Теперь нам нужно создать пользователя, на котором будем тренироваться. Если я правильно понял подход к организации доступа в интернет, то он выдается только тем, кому разрешено. То есть по умолчанию, сейчас шлюз в интернет никого не пускает. Добавим нового пользователя и назначим ему IP адрес.

Идем в раздел **Пользователи и Статистика -> Пользователи** и добавляем нового пользователя. В настройках пользователя на вкладке IP/MAC-адреса указываем ip адрес этого пользователя.

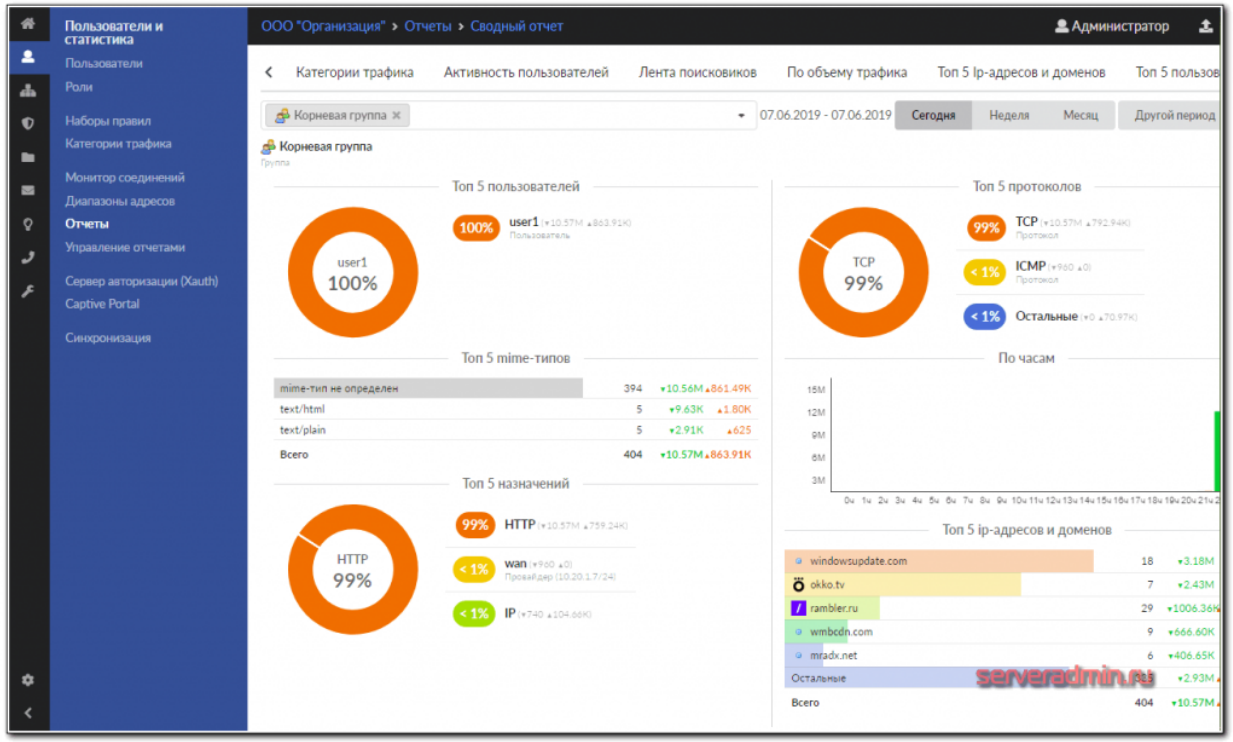


Теперь идем на компьютер пользователя и прописываем ему адрес прокси сервера. В данном случае 192.168.0.1 и порт 3128. После этого у пользователя появится доступ в интернет. Концепция такая, что неконтролируемого доступа в сеть нет ни у кого. Разрешено только тому, кого вы сами добавите и разрешите доступ.

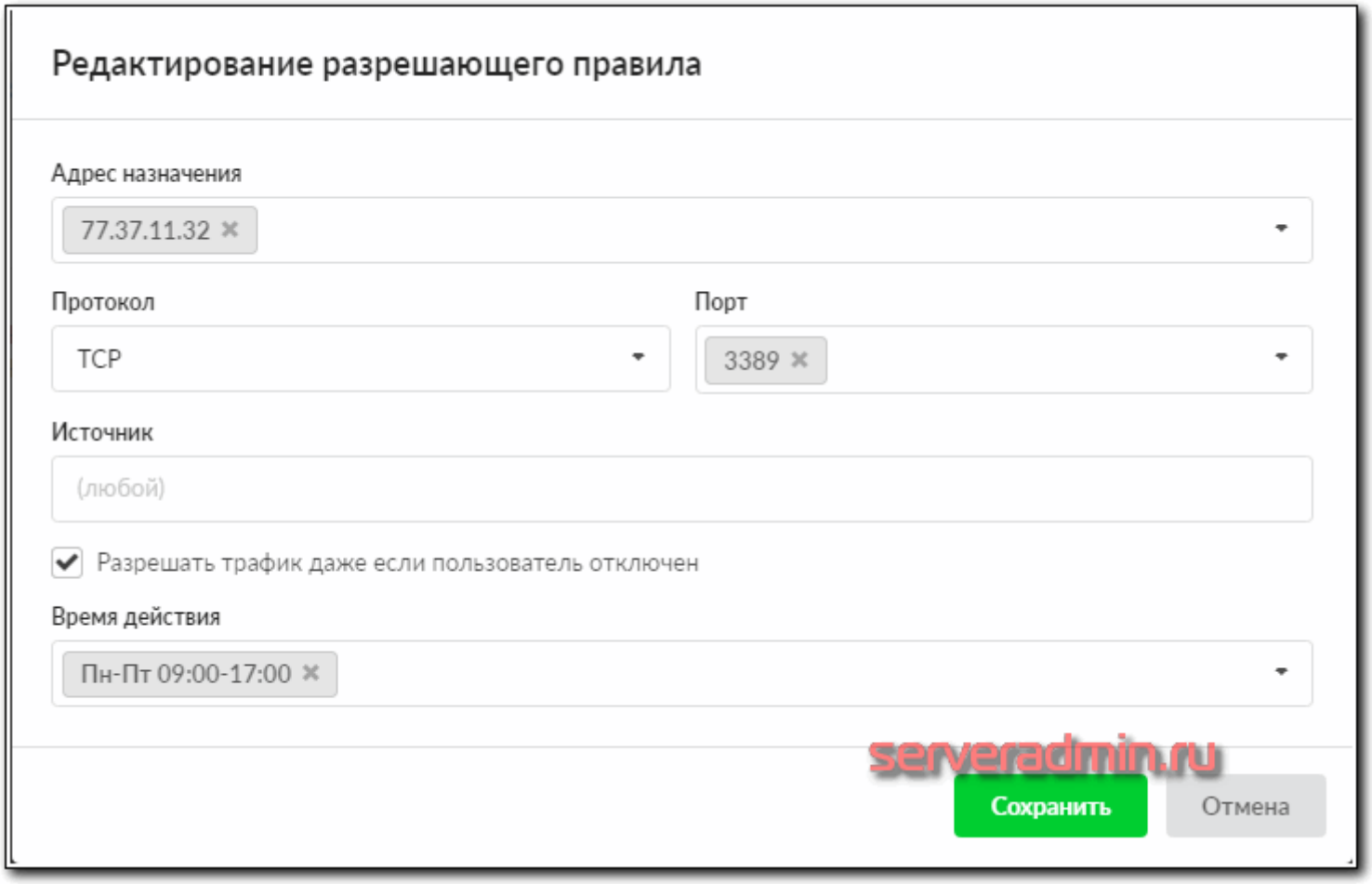
По пользователю доступна полная статистка в удобном виде. Ее можно посмотреть как в разрезе самого пользователя, так и в целом по системе. Вот пример статистики пользователя.

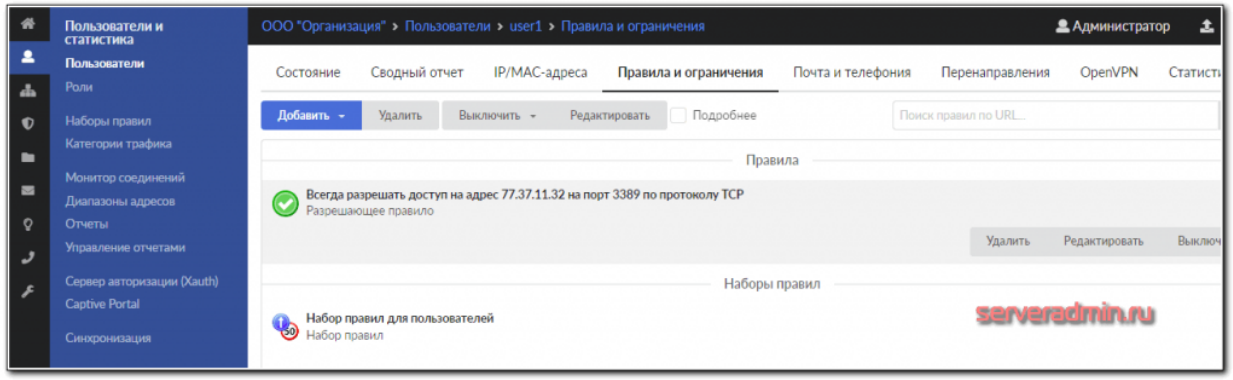


А вот системный отчет по всем пользователям.



Если пользователю нужно отдельно открывать что-то еще, кроме http, то можно добавить правила фаервола либо конкретно пользователю, либо всей группе, в которой он состоит. Удобный подход, причем делается это все через веб интерфейс с наглядной визуализацией.

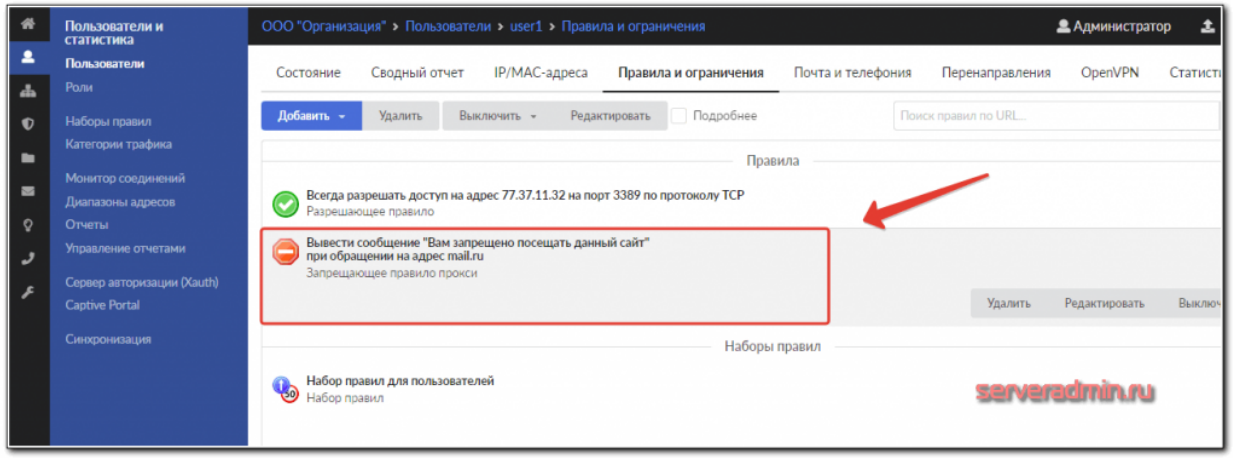

Редактирование разрешающего правила
Адрес назначения
77.37.11.32
Протокол
TCP
Порт
3389
Источник
(любой)
Разрешать трафик даже если пользователь отключен
Время действия
Пн-Пт 09:00-17:00
serveradmin.ru
Сохранить
Отмена



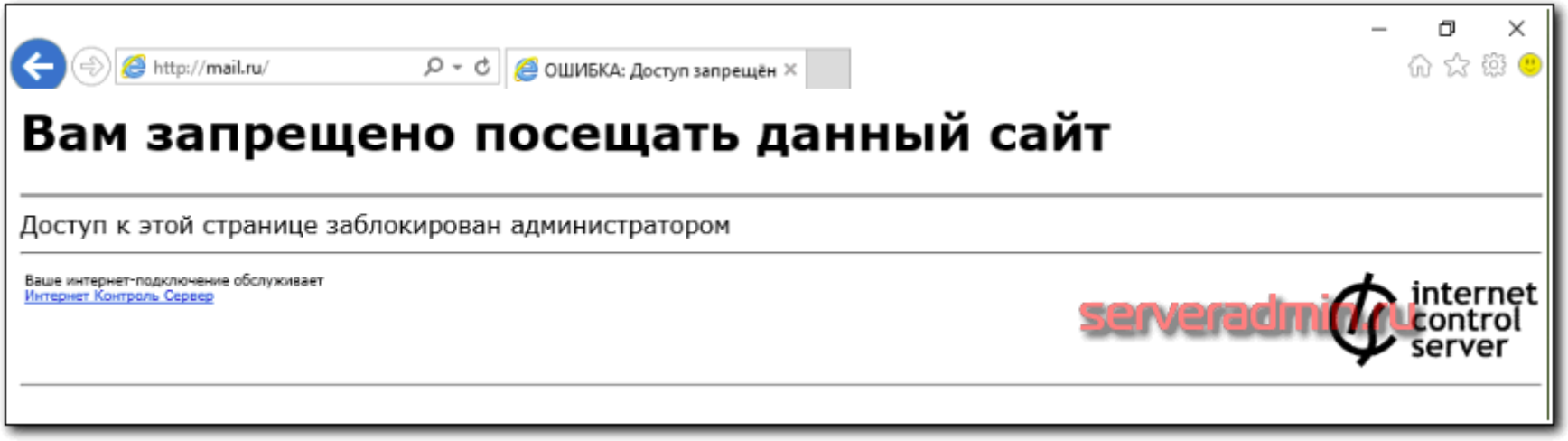
С простым доступом в интернет закончили. Переходим к более интересным штукам, таким как ограничение доступа.

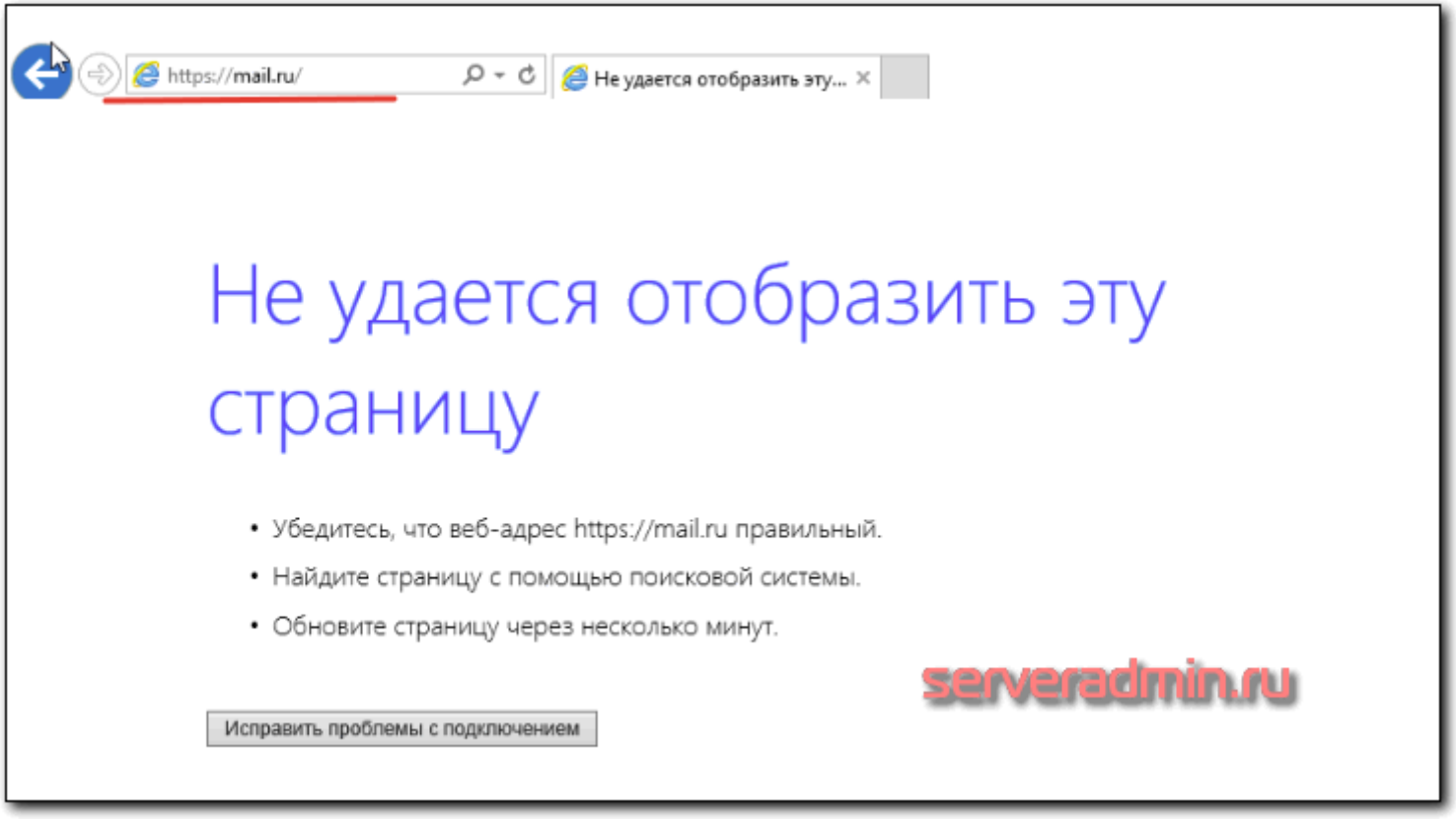
Фильтрация HTTPS трафика в интернет-шлюзе ИКС

Рассмотрим теперь ситуацию, когда нам нужно запретить пользователю или группе пользователей доступ к какому-то сайту. Пусть это будет mail.ru. Идем в настройки правил пользователя и добавляем **Запрещающее правило прокси**.

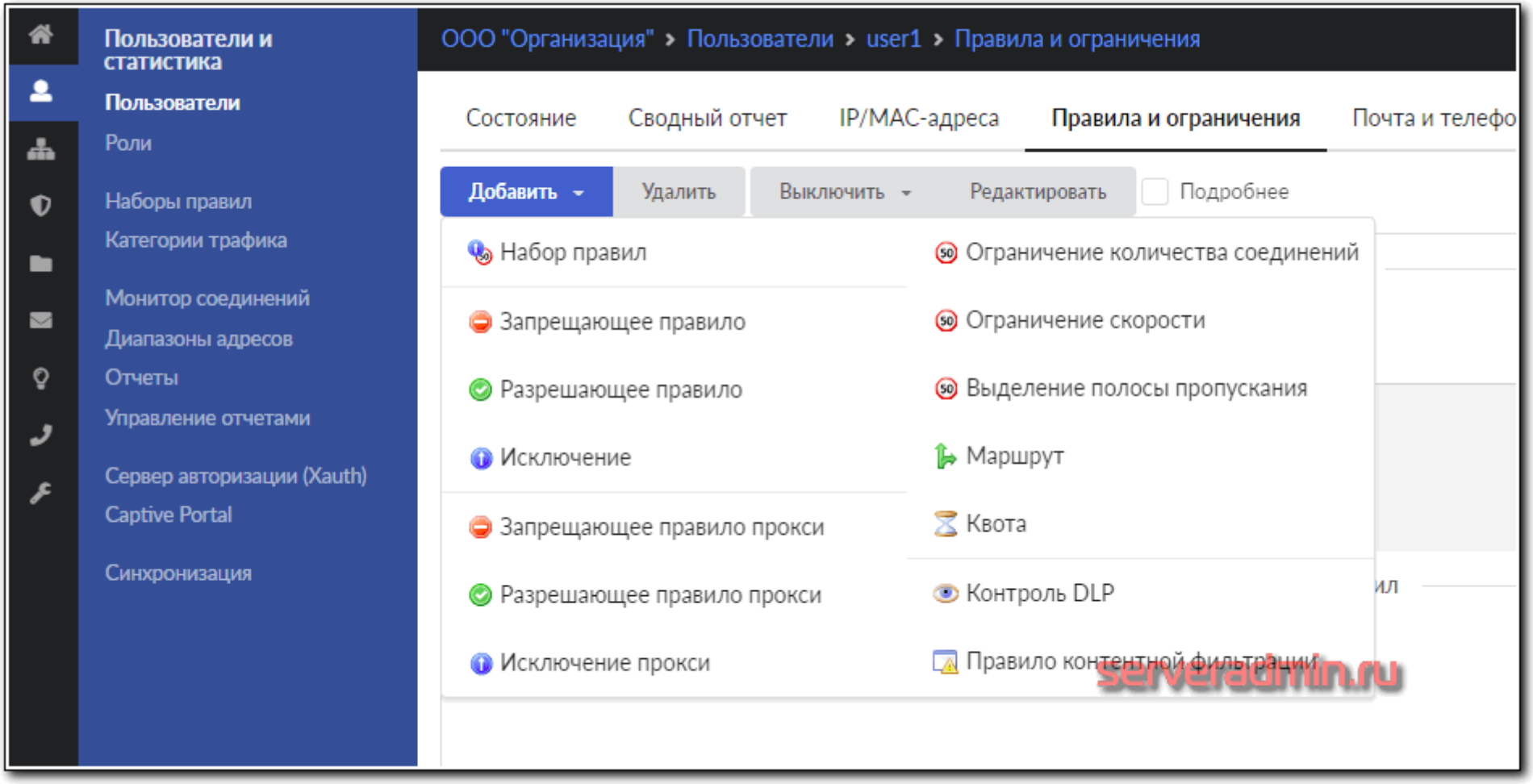


Идем к пользователю и проверяем. Если сайт открыть по http, то будет видно запрещающее сообщение. Если сайт https, то никакого сообщения не будет, он просто не откроется.

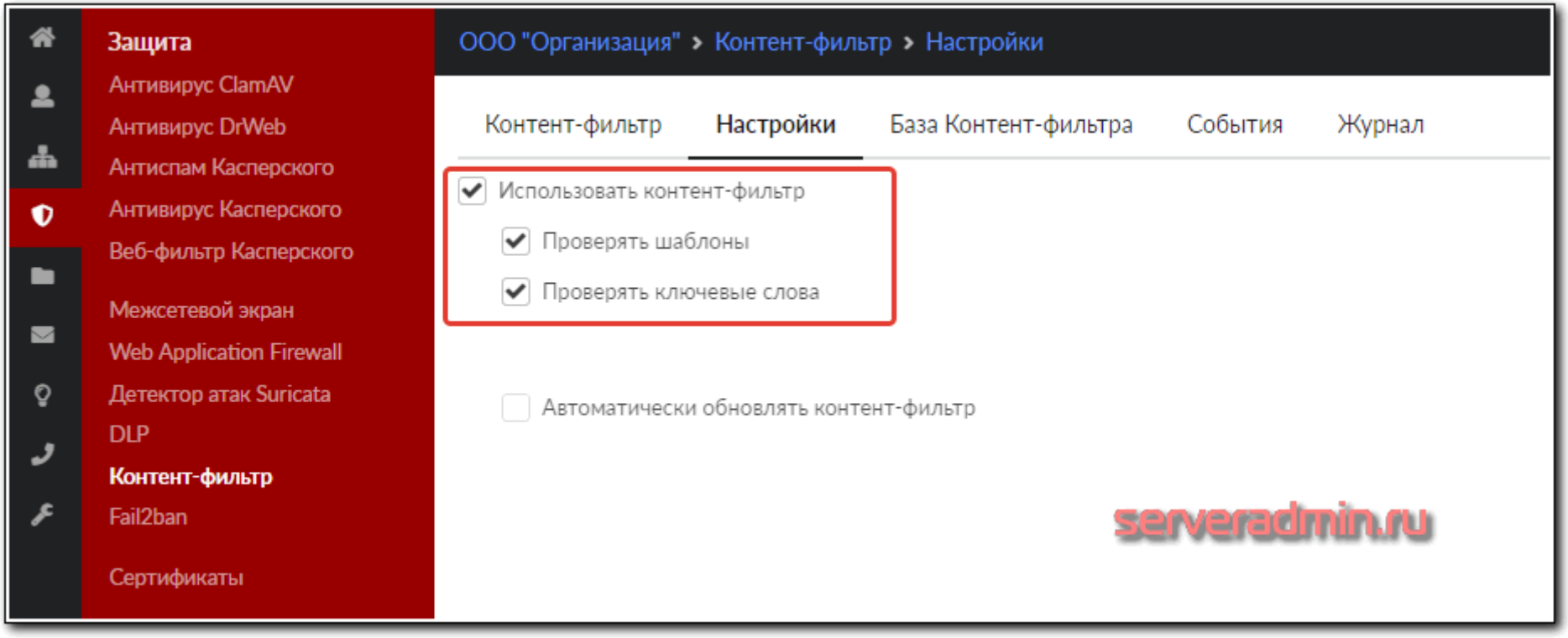

http://mail.ru/
ОШИБКА: Доступ запрещён
Вам запрещено посещать данный сайт
Доступ к этой странице заблокирован администратором
Ваше интернет-подключение обслуживает
Интернет Контроль Сервер
serveradmin.ru
internet
control
server



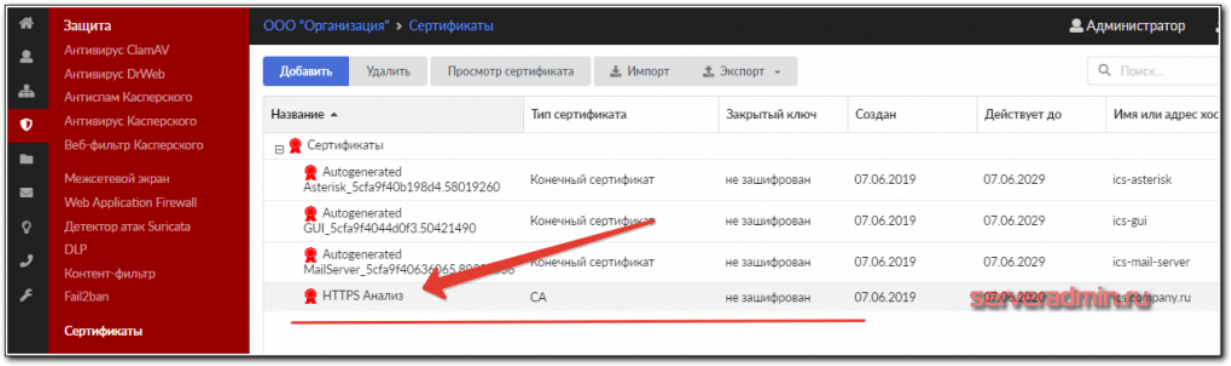
Пользователей можно объединять в группы и настраивать запреты по группам. Помимо ограничений по адресам сайтов, можно настроить и другие правила запретов и разрешений.



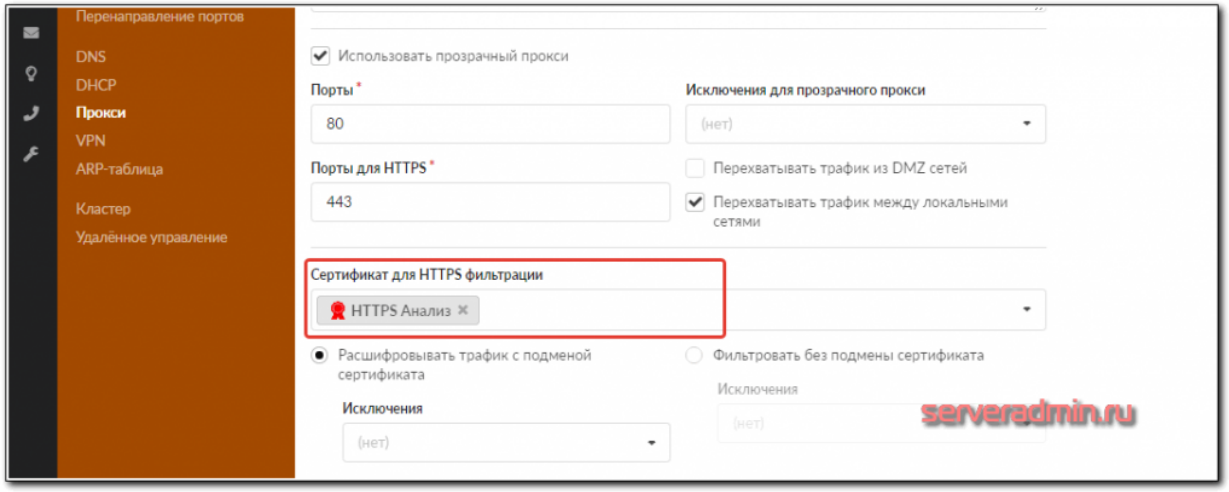
Давайте теперь включим контентный фильтр и настроим ограничения доступа на основе содержимого https страниц. Фильтровать можно будет как по готовым спискам от госорганов, так и создавать свои. Для этого нам надо включить **Контент-фильтр** в разделе **Защита**.



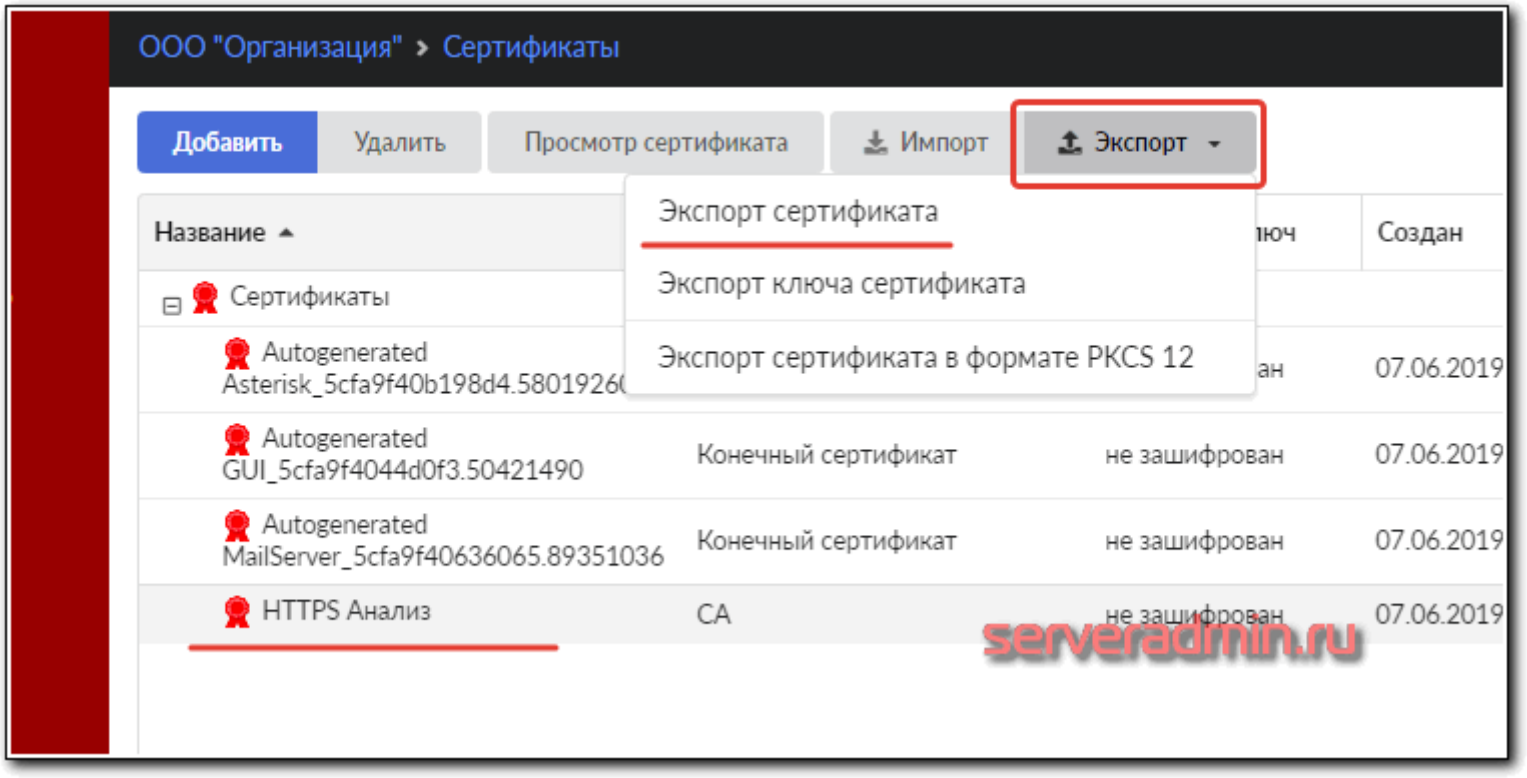
Далее нужно создать сертификат, который будет использоваться для MITM. То есть нам надо этот сертификат поместить на прокси сервер и в доверенные сертификаты клиента. Только в таком случае возможно анализировать и разбирать https трафик. Других способов нет. Создаем сертификат в разделе **Защита -> Сертификаты**.



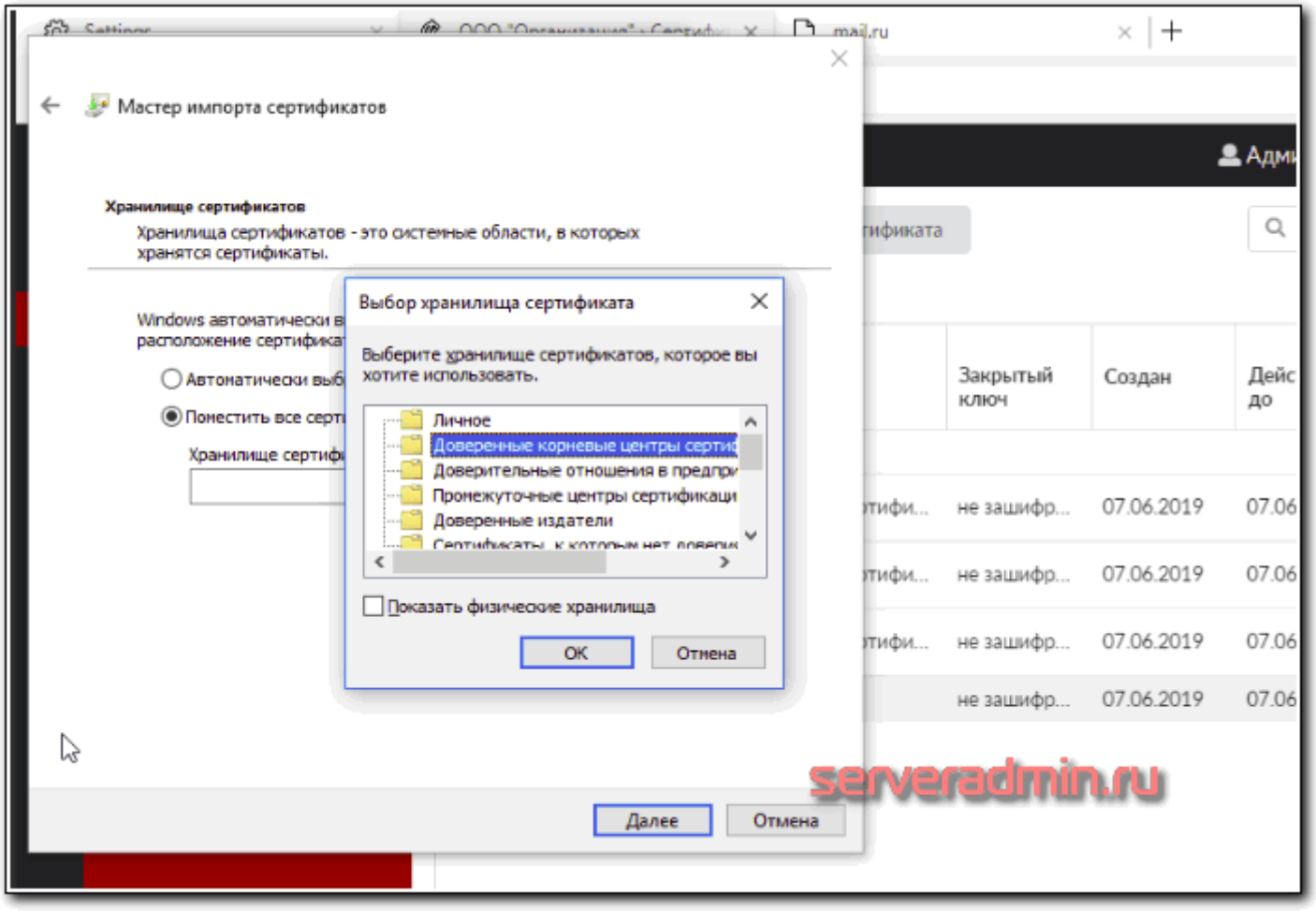
Теперь указываем прокси серверу использовать этот сертификат. Идем в раздел **Сеть -> Прокси -> Настройки**.



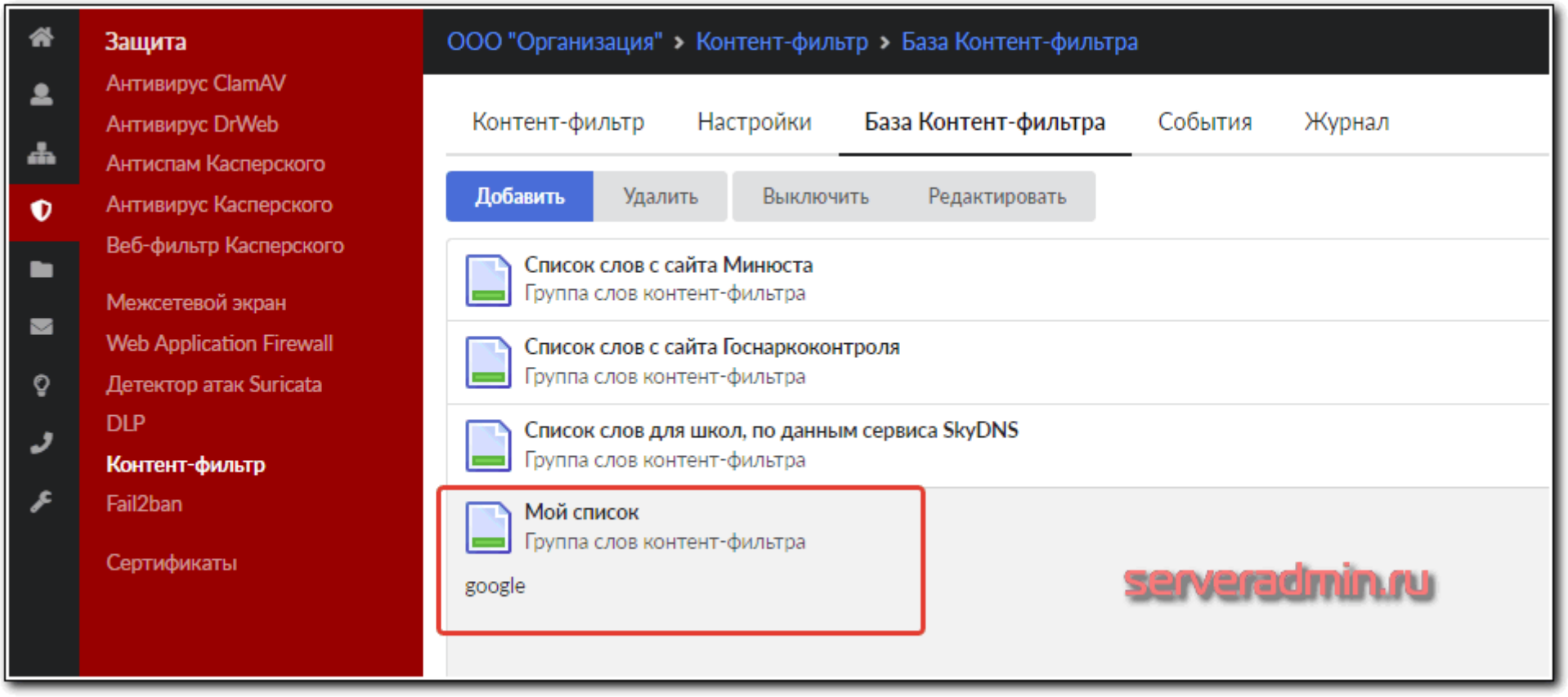
Делаем экспорт этого сертификата и передаем его на компьютер клиента.



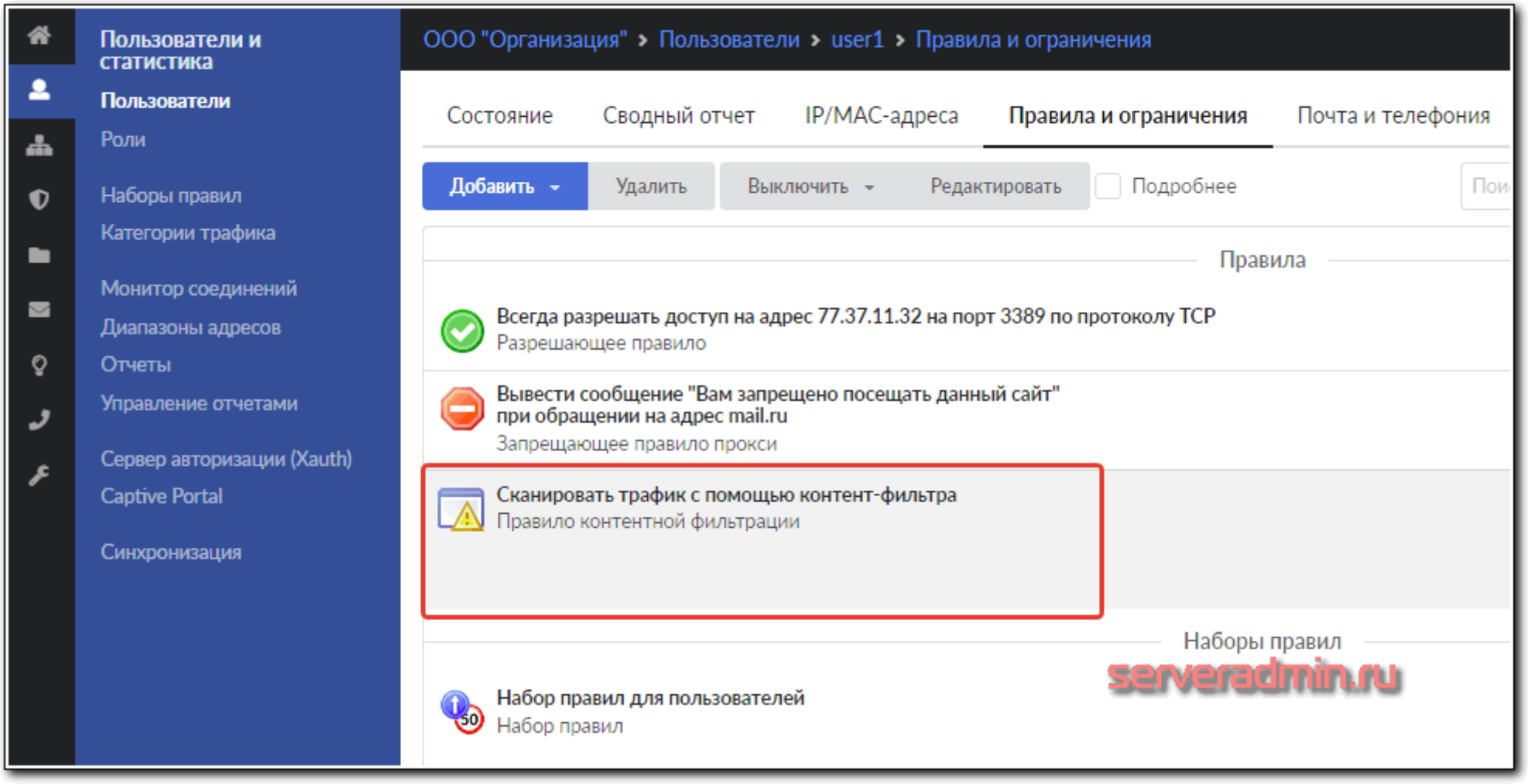
На компьютере клиента устанавливаем этот сертификат в хранилище **Доверенные корневые центры сертификации**.



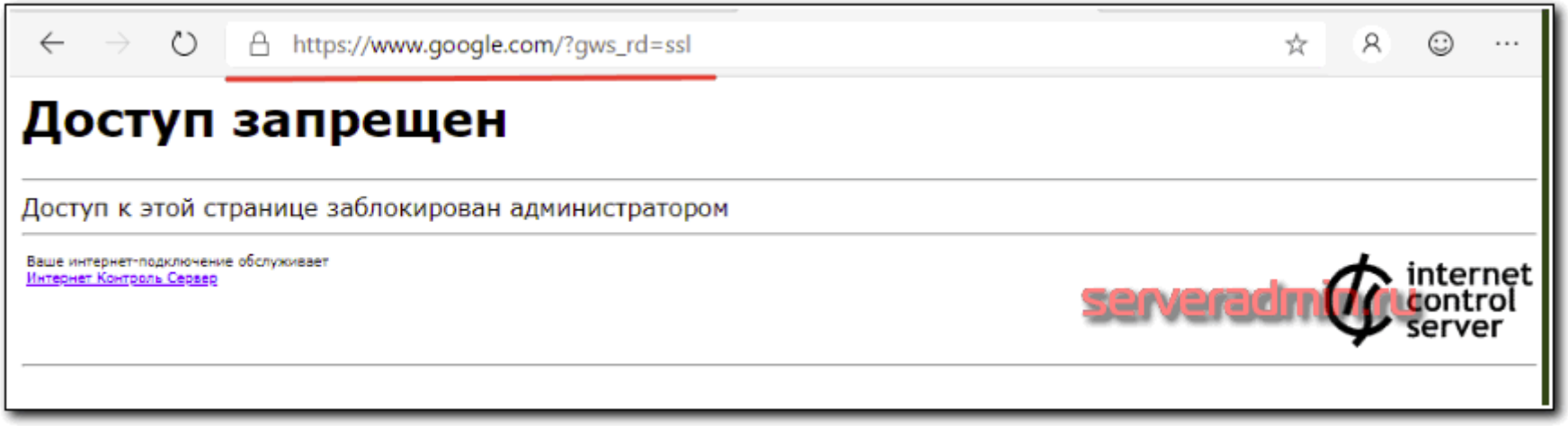
Теперь нам можно создать свой список в Контент-фильтре. Я назвал его *Мой список* и добавил туда слово google, которое фильтр будет искать в содержимом страницы.



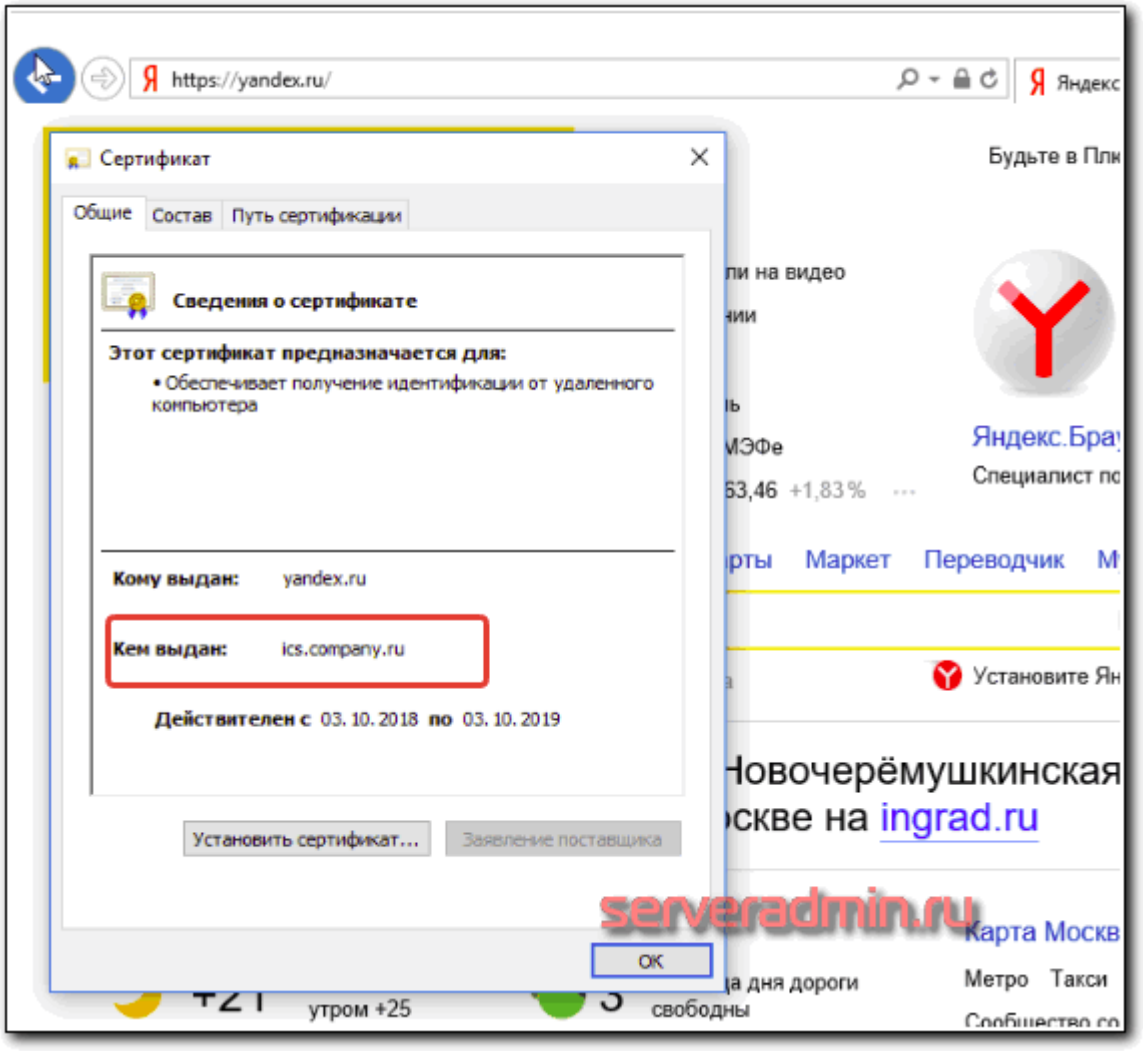
Добавляем пользователю правило **Сканировать трафик с помощью контент-фильтра**.



Теперь идем на компьютер пользователя и пробуем открыть сайт google.com, где на странице точно встречается слово google.



Если на каком-то сайте будет встречаться слово google, открываться он не будет. Можно убедиться, что MITM работает, проверив сертификат любого https сайта. Там будет стоять метка нашего CA.



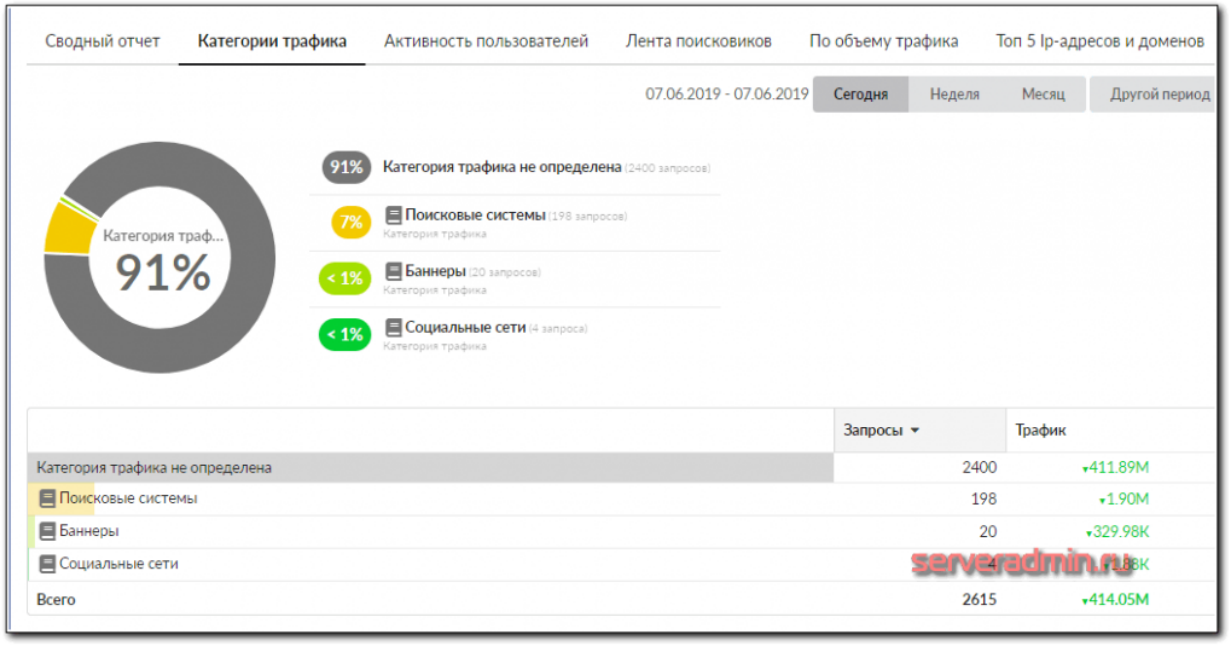
Если браузер использует не системное хранилище сертификатов, а свое, например Firefox, то сертификат нужно добавить отдельно в браузер через его

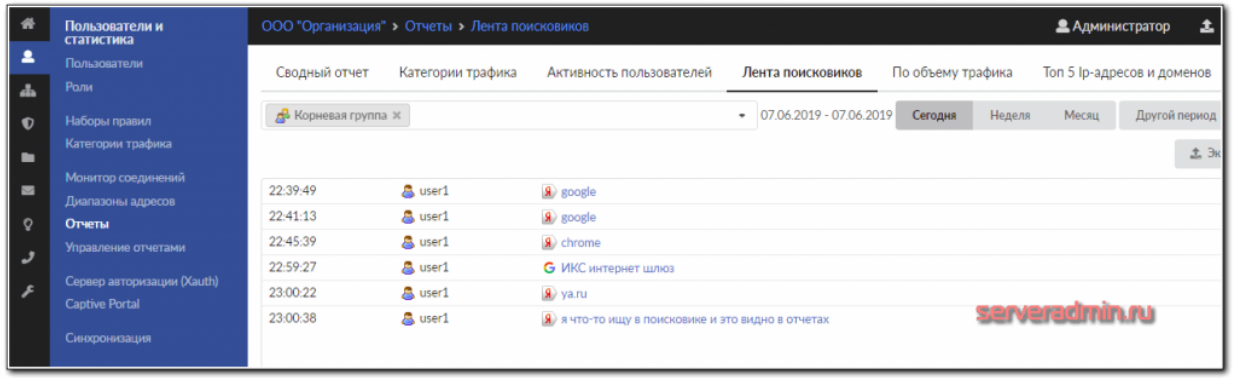
настройки.

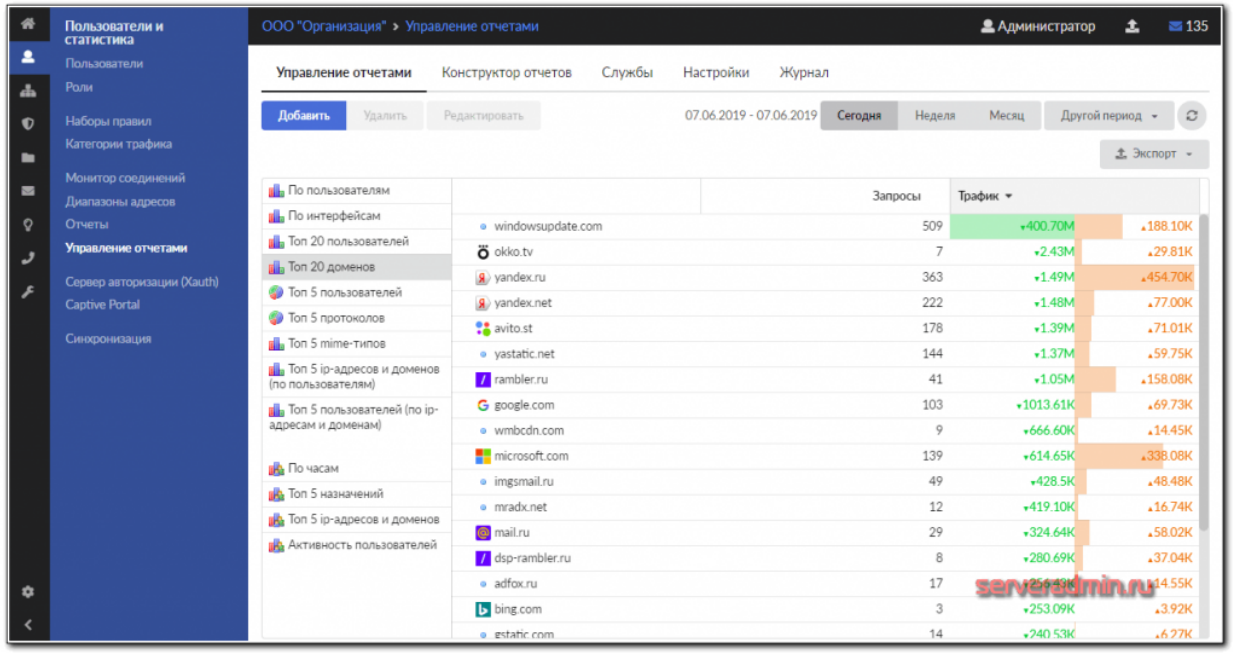
Таким образом **фильтруется https трафик**. С помощью подмены сертификата можно смотреть подробную статистику по всем посещенным страницам пользователя. Срабатывание контент-фильтра логируется.

Отчеты по трафику

Отдельно хочу показать вам отчеты, которые рисует ИКС шлюз. Мне они очень понравились. Сами по себе информативны, плюс возможность гибких настроек. Я такого нигде больше не видел. Вот несколько примеров.


Сводный отчет
Категории трафика
Активность пользователей
Лента поисковиков
По объему трафика
Топ 5 Ip-адресов и доменов
07.06.2019 - 07.06.2019
Сегодня
Неделя
Месяц
Другой период
Категория траф...
91%
91% Категория трафика не определена (2400 запросов)
7% Поисковые системы (198 запросов)
Категория трафика
< 1% Баннеры (20 запросов)
Категория трафика
< 1% Социальные сети (4 запроса)
Категория трафика
Запросы
Трафик
Категория трафика не определена 2400 411.89M
Поисковые системы 198 1.90M
Баннеры 20 329.98K
Социальные сети
Всего 2615 414.05M
serveradmin.ru


Пользователи и статистика
Пользователи
Роли
Наборы правил
Категории трафика
Монитор соединений
Диапазоны адресов
Отчеты
Управление отчетами
Сервер авторизации (Xauth)
Captive Portal
Синхронизация
ООО "Организация" › Отчеты › Лента поисковиков
Администратор
Сводный отчет
Категории трафика
Активность пользователей
Лента поисковиков
По объему трафика
Топ 5 Ip-адресов и доменов
Корневая группа
07.06.2019 - 07.06.2019
Сегодня
Неделя
Месяц
Другой период
22:39:49 user1 google
22:41:13 user1 google
22:45:39 user1 chrome
22:59:27 user1 ИКС интернет шлюз
23:00:22 user1 ya.ru
23:00:38 user1 я что-то ищу в поисковике и это видно в отчетах
serveradmin.ru

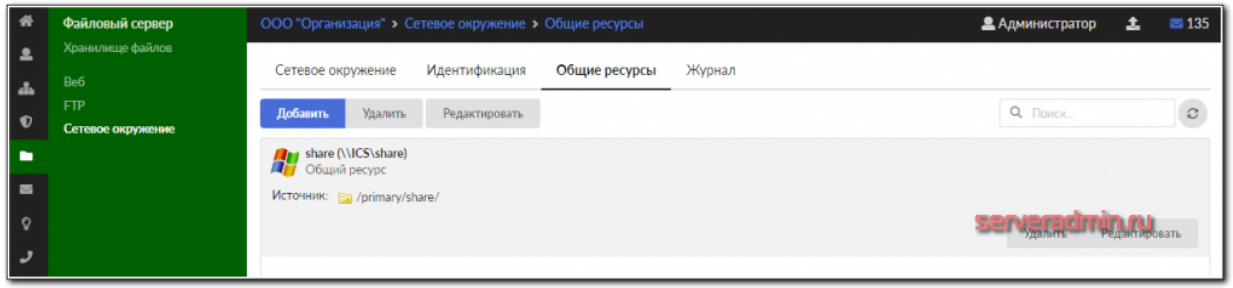


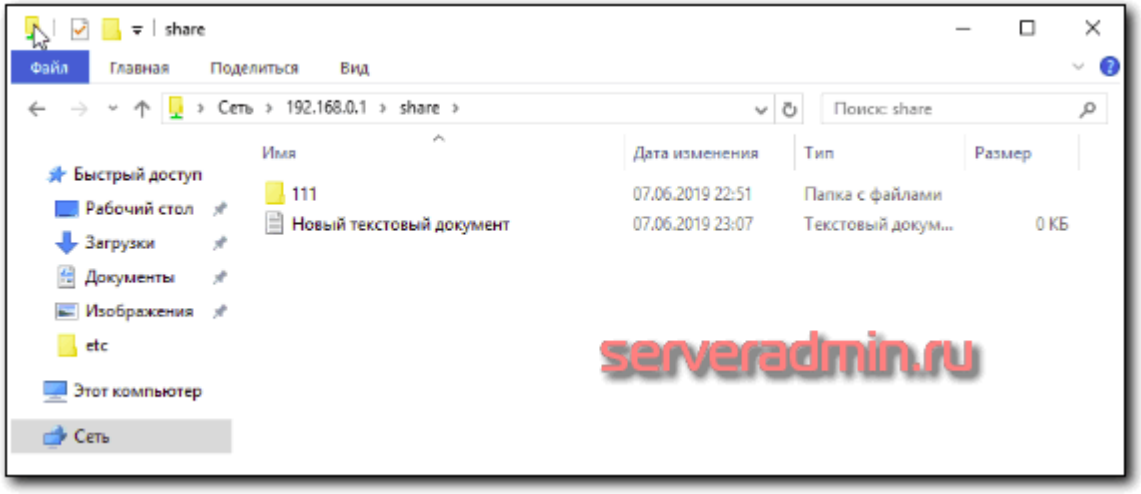
И так далее. Отчеты реально удобные и наглядные. Можно строить свои через конструктор. Работает экспорт.

Что еще умеет интернет шлюз ИКС

Функционал этого шлюза огромен. Куча всяких модулей, списков доступа и т.д. Половина из этого платное с отдельной подпиской. Я все не проверял, так как надо тестовый доступ запрашивать, да и долго все проверять.

Из того, что я проверил и это работало — файловый сервер и почтовый сервер. Под капотом файлового сервера samba. Я просто расшарил папку и настроил в ней доступ по пользователям. Авторизация была по паролю. Работает просто и надежно.

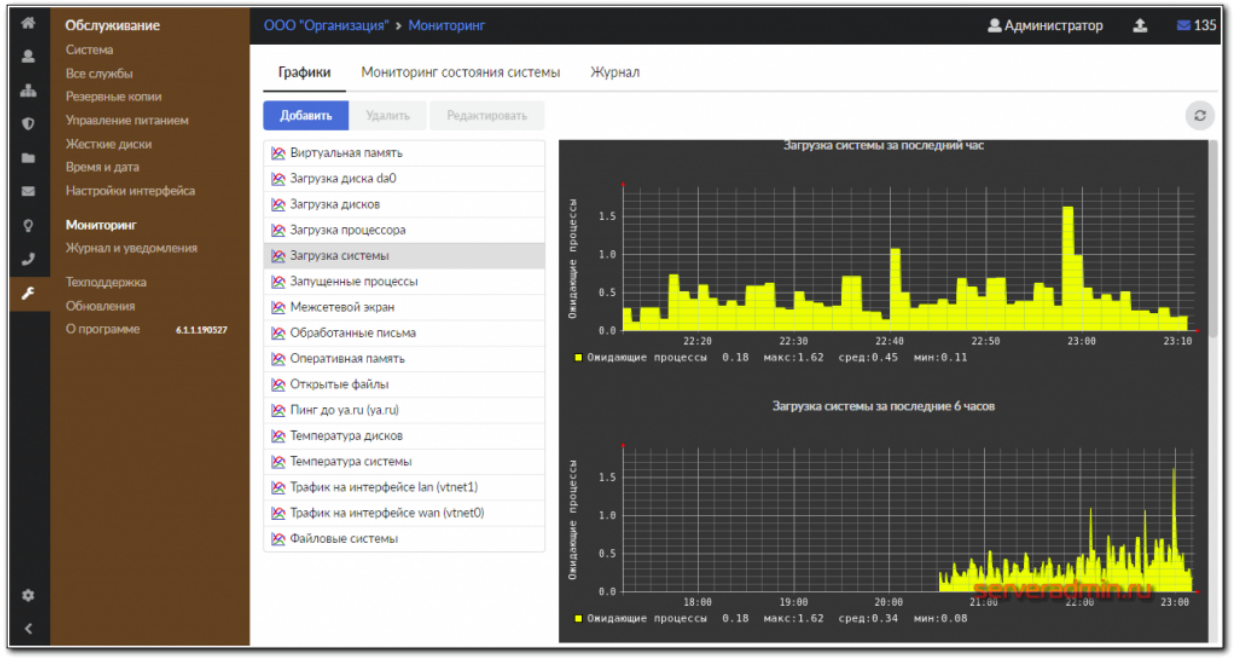

Файловый сервер
Хранилище файлов
Веб
FTP
Сетевое окружение
ООО "Организация" › Сетевое окружение › Общие ресурсы
Администратор
135
Сетевое окружение
Идентификация
Общие ресурсы
Журнал
Добавить
Удалить
Редактировать
Поиск...
share (\\ICS\share)
Общий ресурс
Источник:
/primary/share/
serveradmin.ru
Удалить
Редактировать



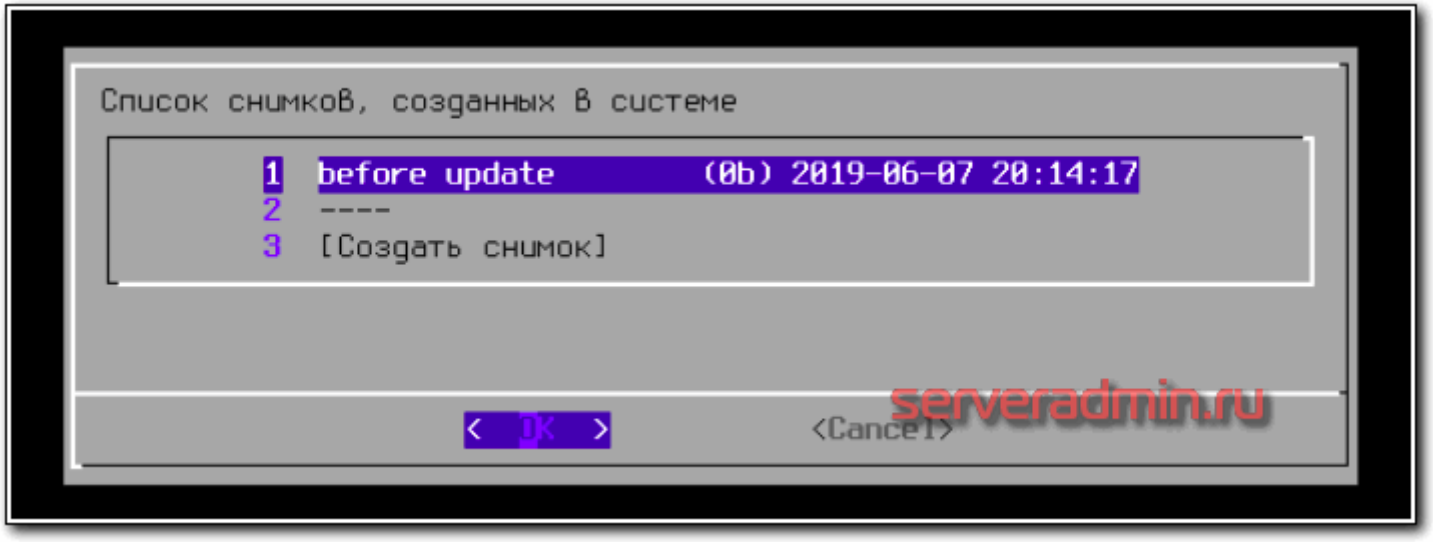
Попробовал почтовый сервер. Что там внутри не проверял, думаю, что postfix. Функционал понравился. Сразу интегрировано несколько spam фильтров, как платный от Kaspersky (он хорошо, я его много где использую и всегда рекомендую), так и бесплатные. В принципе, для настройки почтового сервера в нем не обязательно разбираться, все настраивается через web интерфейс. Сравните это с ручной настройкой примерно такого же функционала.

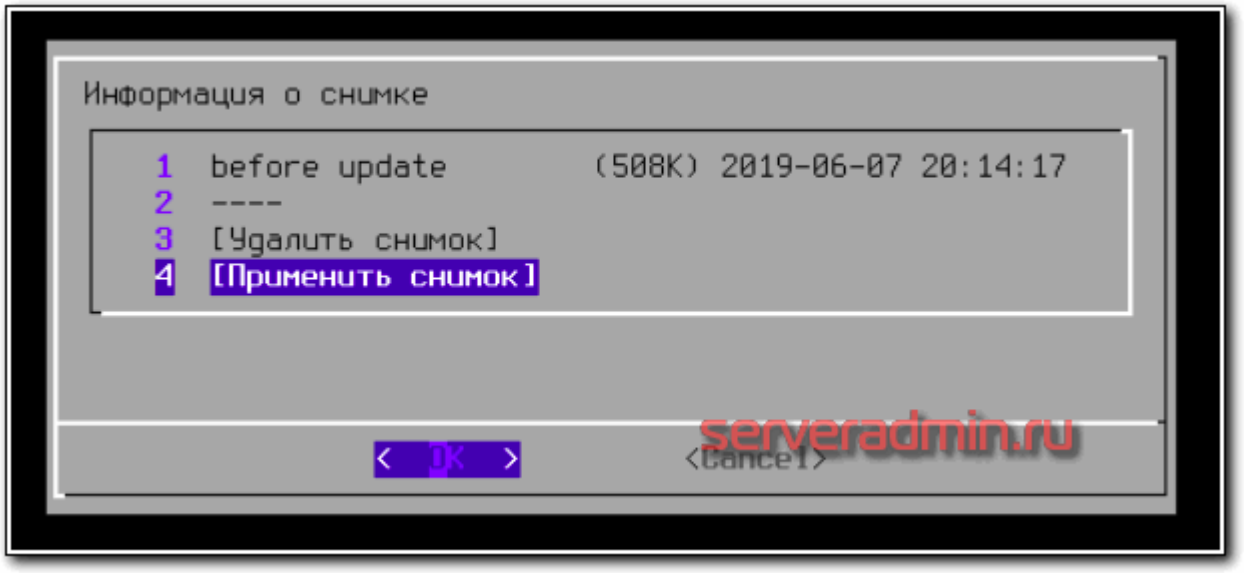
Jabber и сервер телефонии не пробовал настраивать. Судя по тому, что все предыдущее работало без плясок с бубном, подозреваю, что и это будет работать.

У сервера встроенный простенький мониторинг.



Я забыл упомянуть, что в качестве файловой системы **используется zfs** со всеми ее фишками — софтовый рейд, снепшоты и т.д.


Список снимков, созданных в системе
1 before update (0b) 2019-06-07 20:14:17
2 ----
3 [Создать снимок]
< OK >
<Cancel>
serveradmin.ru



Сервер умеет слать уведомления на почту, в ICQ и Jabber. Не хватает тут Telegram. Я лично не знаю людей, которые пользуются ICQ в наше время.

Данный шлюз может выступать в качестве web и ftp сервера. Просто невероятный комбайн :) Я такого еще не видел. Ах да, забыл сказать про VPN. Он умеет PPTP и OpenVPN. Я не тестировал, но не думаю, что там могут быть проблемы. OpenVPN все интернет шлюзы умеют настраивать.

Интересные записи:
Шутки для сисадминов
Мои программы для системного администрирования
Монетизация ИТ блога, сколько можно заработать на информационном сайте

Еще забыл сказать, что он интегрируется с AD. Может брать пользователей оттуда.

Заключение

Я потратил целый день на исследование и настройку сертифицированного интернет шлюза ИКС от российских разработчиков. И он мне понравился. В голове даже план созрел, как это все можно отладить, настроить, проработать стратегию внедрения и ставить в госы или малые и средние компании.

Взять два бюджетных сервера или простых компьютера. Настроить отказоустойчивость с помощью CARP, чтобы не потерять связь при выходе одного из строя, и внедрять в организации. У разработчиков есть готовые видеоролики по управлению и неплохая документация. Соответственно, надо внедрить и обучить местный персонал. Реально этот шлюз покрывает большинство потребностей малого и среднего бизнеса по ИТ инфраструктуре.

А уж тем, кому нужно соблюдать требования закона в плане ограничения доступа к информации в интернете это может стать настоящей находкой и простым способом закрытия вопроса за вполне приемлемую цену. Так что берите на вооружение, кому интересно, и внедряйте. Сам я уже давно этим не занимаюсь.

Я тестировал множество различных комбайнов с web панелями в свое время, когда занимался обслуживанием офисов. Идея была внедрить и оставить на обслуживание местным специалистам. Нужно было максимально простое и стабильное решение. В бесплатных сборках функционала, подобного ИКС, нет нигде, это точно. С платными я не знаком вообще, не тестировал ни один. Наверняка есть какие-то аналоги. Интересно было бы сравнить.

- Которые хотят освободить продуктовые команды от части задач администрирования и автоматизации и сфокусировать их на развитии продукта.

Проверьте себя на вступительном тесте и смотрите программу детальнее по .