

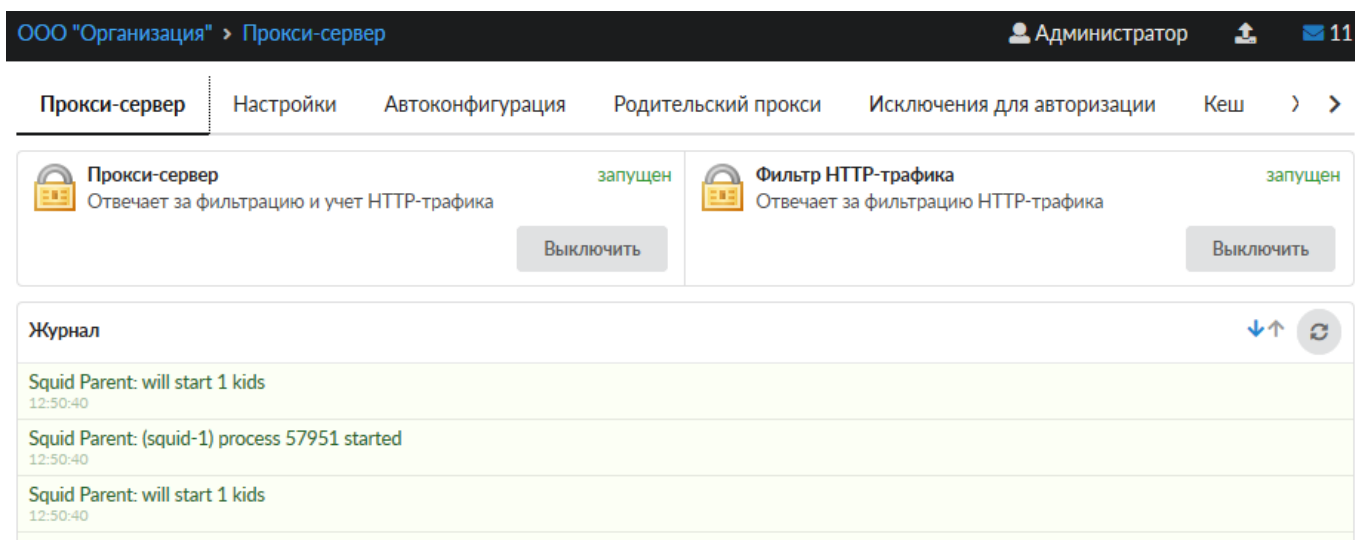
# Прокси

## Стартовая страница модуля

**Прокси-сервер** — служба, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо веб-ресурс, расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (если кто-то из клиентов уже обращался к этому ресурсу). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях.

Также, прокси-сервер позволяет анализировать проходящие через сервер HTTP-запросы клиентов, выполнять фильтрацию и учёт трафика по URL и time-типам. Кроме этого, прокси-сервер реализует механизм доступа в интернет по логину/паролю.

Прокси-сервер выполняет кеширование объектов, полученных пользователями из интернета и за счёт этого сокращает потребление трафика и увеличивает скорость загрузки страниц.



The screenshot shows the start page of the Proxies module. At the top, there is a breadcrumb "ООО 'Организация' > Прокси-сервер" and a user profile "Администратор" with a notification icon showing "11". Below this is a navigation menu with items: "Прокси-сервер", "Настройки", "Автоконфигурация", "Родительский прокси", "Исключения для авторизации", and "Кеш". The main content area contains two service status cards. The first card is for "Прокси-сервер" (Squid Parent) with a status of "запущен" (running) and a "Выключить" (Stop) button. The second card is for "Фильтр HTTP-трафика" (Squid Parent) with a status of "запущен" (running) and a "Выключить" (Stop) button. Below these cards is a "Журнал" (Log) section with a refresh icon and three log entries: "Squid Parent: will start 1 kids" (12:50:40), "Squid Parent: (squid-1) process 57951 started" (12:50:40), and "Squid Parent: will start 1 kids" (12:50:40).

При входе в модуль отображается состояние служб, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

## Настройки

Прокси-сервер **Настройки** Автоконфигурация Родительский прокси Исключения для авторизации Кеш > >

Порт\*  
3128

Автоматически создавать разрешающее правило

Доступ к прокси

Тип авторизации: По логину/паролю ИКС  
Порядок авторизации пользователей: По IP, затем по логину/паролю

Скрывать ip-адрес пользователя  
 Использовать кеш

Размер кеша\* 100 Мб  
Ограничивать размер ответа (не ограничивать) Мб

Обычно для работы через прокси-сервер, необходимо указать его адрес и порт в настройках браузера. Однако, в случае если не используется авторизация пользователей по логину/паролю, то можно использовать функцию прозрачного прокси.

При этом все запросы по протоколу HTTP из локальной сети автоматически направляются через прокси-сервер. Таким образом появляется возможность фильтрации и учёта трафика по URL независимо от настроек клиентских компьютеров.

Порт работы прокси-сервера по умолчанию 3128, в настройке модуля вы можете изменить его на любой свободный порт.

## Типы авторизации

Прокси-сервер ИКС поддерживает два способа авторизации: по ip-адресу пользователя, и по логину-паролю.

Авторизация по ip-адресу подходит для случаев, когда пользователь постоянно пользуется одним и тем же компьютером. Прокси определяет, какому пользователю принадлежит тот или иной трафик, исходя из ip-адреса его компьютера. Этот способ не подходит для терминальных серверов, так как в этом случае с одного ip-адреса работает несколько пользователей. Также этот способ не подходит для организаций, в которых пользователи постоянно перемещаются между рабочими местами. Кроме того, пользователь может сменить ip-адрес своего компьютера и, если не настроена привязка MAC-адреса к IP, ИКС примет его за кого-то другого.

Авторизация по логину/паролю решает проблему привязки пользователей к собственному компьютеру. В этом случае при первом обращении к любому интернет-ресурсу, браузер выдаст пользователю запрос логина/пароля для доступа в интернет. Если в вашей сети пользователи авторизуются в домене, вы можете установить тип авторизации «Через домен». В таком случае, если ИКС подключен к контроллеру домена и в из домена были импортированы пользователи, авторизация будет выполнена прозрачно, без запроса логина/пароля.

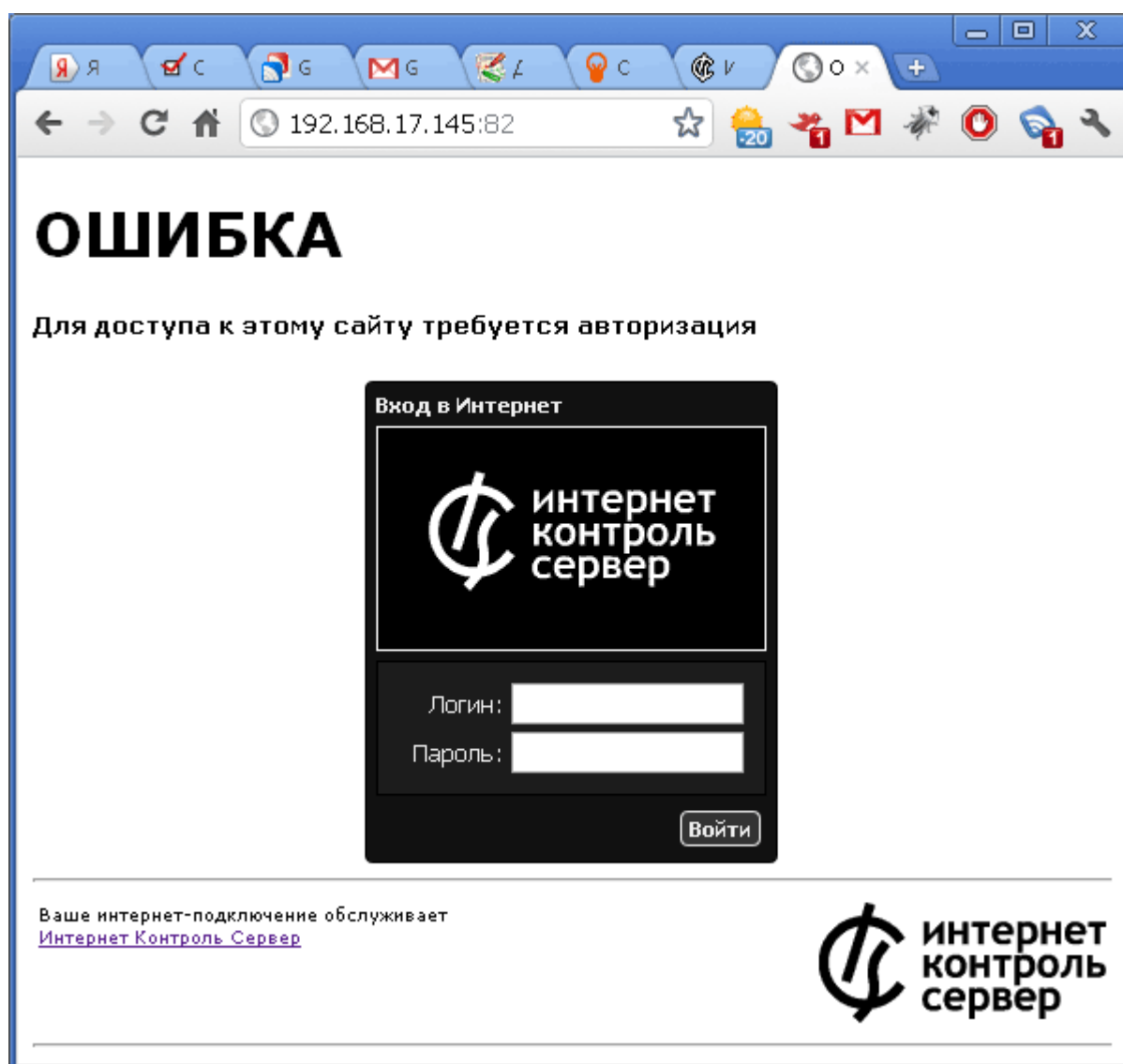
Недостаток этого способа авторизации заключается в том, что он не поддерживается прозрачным прокси, и во всех программах, обращающихся в интернет, необходимо прописывать адрес прокси-сервера.

Кроме того, следует помнить о том, что авторизация на прокси используется только для http-трафика пользователей. Доступ в интернет для программ, использующих протоколы, отличные от http, регулируется межсетевым экраном, который имеет только один способ авторизации: по ip-адресу. Другими словами, если пользователь использует только авторизацию по логину/паролю, он не сможет пользоваться почтой, jabber-клиентом, torrent-клиентом и другими программами, не поддерживающими работу через http-прокси.

## Веб-авторизация

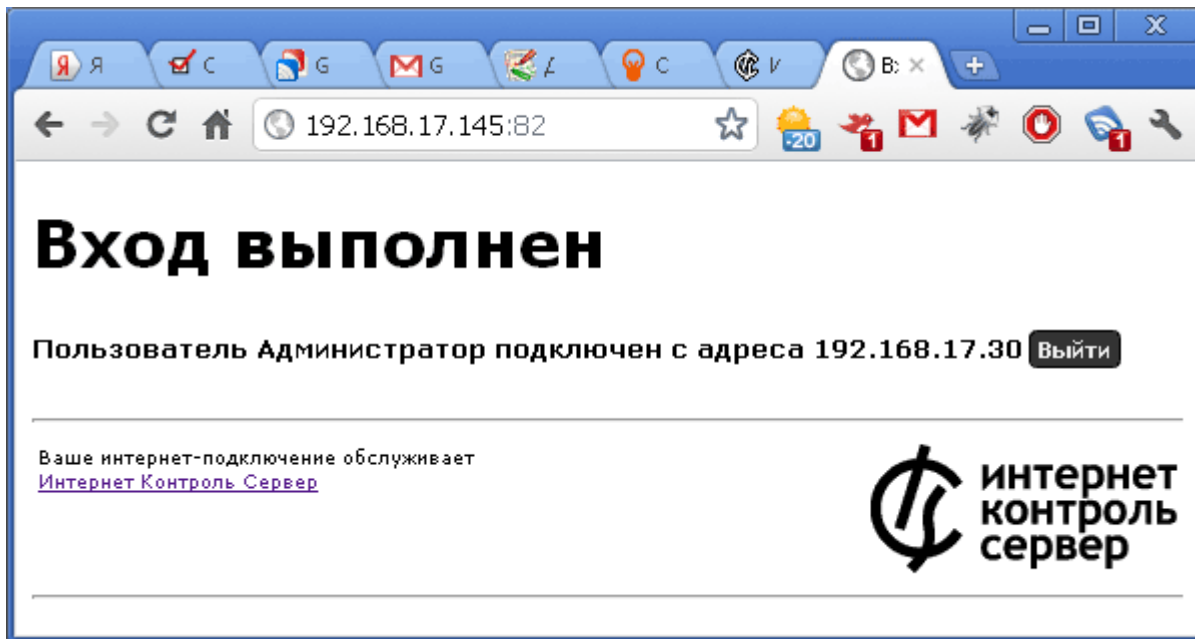
Для того, чтобы авторизовать пользователей без прописанного прокси-сервера по имени пользователя и паролю, вы можете использовать веб-авторизацию (captive portal), включив соответствующий флажок. Веб-авторизация позволяет, к примеру, интегрировать страницу авторизации в корпоративный портал, и использовать его в качестве страницы авторизации. По умолчанию порт веб-авторизации 82, вы также можете изменить его на любой свободный.

При переходе на страницу [http://ip\\_ics:82](http://ip_ics:82) вы получаете следующее сообщение:



Также, если включена веб-авторизация, то неавторизованные пользователи автоматически будут перенаправляться на страницу авторизации.

Для того, чтобы отключиться, нужно повторно зайти на страницу авторизации и нажать кнопку «Выйти».



Флажок «Только с одного ip-адреса» запрещает нескольким пользователям одновременно подключаться под одним и тем же логином.

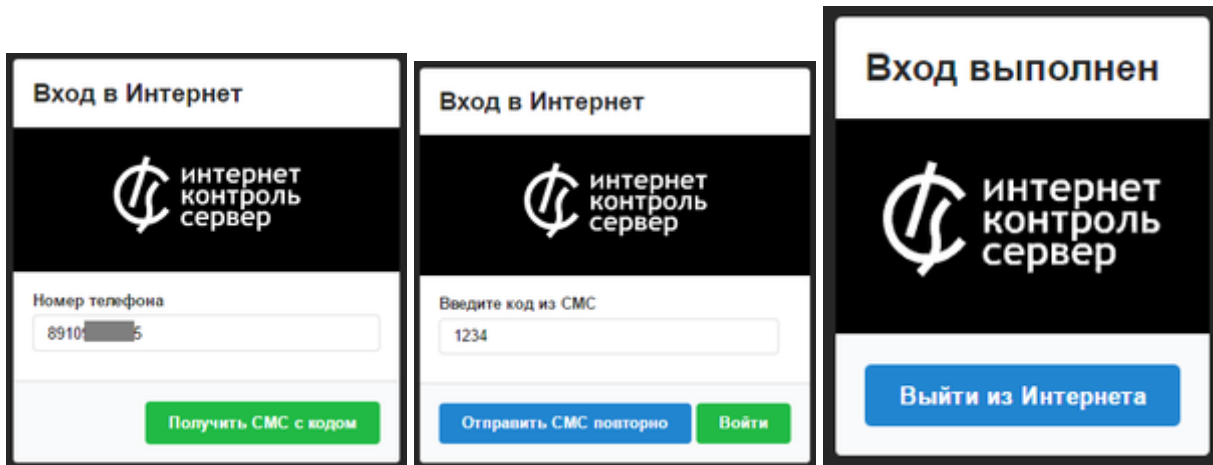
**Пользователь, авторизованный подобным способом, получит доступ ко всем протоколам (не только HTTP) в соответствии с назначенными ему правилами и ограничениями.**

## SMS-авторизация

В ИКС существует возможность SMS-авторизации пользователей для доступа в интернет.

### Принцип работы:

1. Пользователь подключается к вашей точке WiFi
2. Пользователь заходит в браузер, затем вводит свой номер телефона и нажимает кнопку «Получить СМС с кодом»
3. На указанный номер телефона приходит СМС с кодом
4. Полученный код пользователь вводит в форму авторизации и получает доступ к сети Интернет



На данный момент в ИКС используется сервис для отправки СМС [SMS.RU](https://sms.ru)

В дальнейшем планируется поддержка других сервисов отправки СМС. Если Вас интересует другой сервис отправки СМС-сообщений, [напишите нам об этом](#), мы попытаемся по возможности его добавить в ИКС.

Использовать SMS-авторизацию:

Порт SMS-авторизации:

API ID:

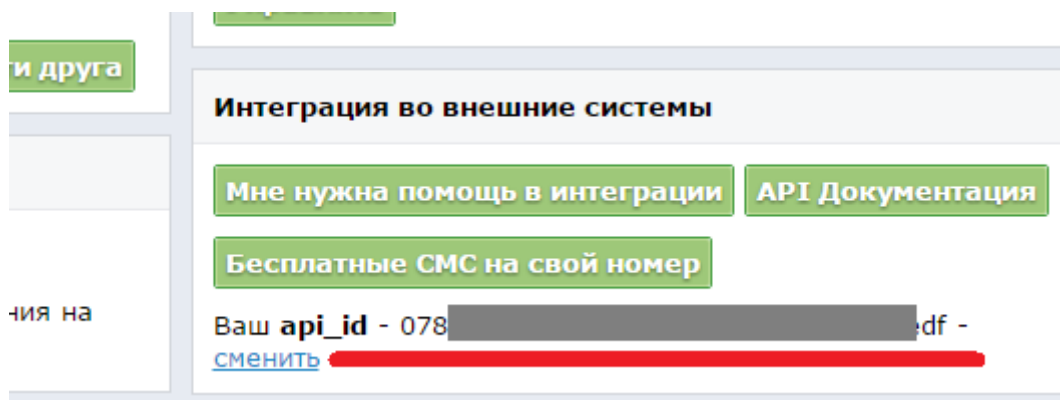
Назначать адреса пользователю:

**Использовать SMS-авторизацию** - Включает SMS-авторизацию.

**Порт SMS-авторизации** - порт, на который принимаются входящие соединения для доступа к графическому интерфейсу авторизации.

**API ID** - секретный ключ, который Вы получили на сайте [SMS.RU](https://sms.ru)

Данный ключ можно посмотреть прямо на главной странице Вашего профиля на сайте [sms.ru](https://sms.ru) справа-внизу:



**Назначать адреса пользователю** - Пользователь ИКС, которому будет выдан IP-адрес клиента, успешно прошедшего авторизацию через СМС.

## Кеширование страниц

Прокси-сервер выполняет кеширование веб-страниц и объектов, которые пользователи скачивают из интернета. Таким образом экономится интернет-трафик и увеличивается скорость доступа к веб-страницам.

Эффективность работы кеша зависит от его размера. Для организации с большим количеством пользователей, рекомендуется установить размер кеша в соответствующем поле в несколько гигабайт. Также, вы можете ограничить размер загружаемого файла в поле «Ограничивать размер ответа» (В мегабайтах).

Опция «Скрывать ip-адрес пользователя» позволяет отключить указание в отправляемом заголовке внутреннего ip-адреса пользователя (параметр `forwarded_for`).

Содержимое кеша прокси-сервера можно посмотреть на вкладке «содержимое кеша». Следует отметить, что веб-интерфейс отображает не все содержимое кэша, а только некоторые элементы, такие как изображения.

## Прозрачный прокси

Использовать прозрачный прокси

Порты *	Исключения для прозрачного прокси
<input type="text" value="80"/>	<input type="text" value="(нет)"/>
Порты для HTTPS *	<input type="checkbox"/> Перехватывать трафик из DMZ сетей
<input type="text" value="443"/>	<input checked="" type="checkbox"/> Перехватывать трафик между локальными сетями

В этом режиме ИКС вместо того, чтобы сразу принимать HTTP-запросы пользователя на порту прокси-сервера, сам перенаправляет их прокси-серверу. Прокси-сервер обрабатывает запрос (с возможной отдачей содержимого из кеша), это содержимое направляется к запросившему пользователю, для которого оно выглядит как «ответ» сервера, к которому адресовался запрос. Таким образом, пользователь может даже не знать, что все запросы и ответы прошли через прокси-сервер. По умолчанию прозрачный прокси перехватывает запросы по 80 порту (HTTP).

Вы можете включить или отключить прозрачное проксирование DMZ и локальных сетей, отметив соответствующие флажки в настройках. По умолчанию DMZ сети не проксируются, а локальные проксируются.

Некоторые программы могут негативно реагировать на изменения в пакетах, которые проходят через прокси-сервер. Вы можете прописать ip-адреса или имена сайтов, пакеты до которых не будут обрабатываться прокси-сервером в поле «Исключения для прозрачного прокси».

Для того, чтобы настроить [HTTPS-фильтрацию](#), нужно заполнить поле «Сертификат для SSL-фильтрации» ранее созданным корневым сертификатом. Адреса, которые не нужно фильтровать подменным сертификатом, могут быть добавлены в исключения.

## SOCKS5

**SOCKS** — сетевой протокол, который позволяет клиент-серверным приложениям прозрачно использовать сервисы за межсетевыми экранами. Клиенты за межсетевым экраном, нуждающиеся в доступе к внешним серверам, вместо этого могут соединиться с SOCKS прокси сервером. Такой прокси сервер контролирует права клиента для доступа к внешним ресурсам и передает запрос к серверу. SOCKS может использоваться и противоположным способом, разрешая внешним клиентам соединиться с серверами за межсетевым экраном (брандмауэром).

В отличие от HTTP прокси серверов, SOCKS передает все данные от клиента, ничего не добавляя от себя, то есть с точки зрения конечного сервера, SOCKS прокси является обычным клиентом. SOCKS более универсален — не зависит от конкретных протоколов уровня приложений (7-го уровня модели OSI) и базируется на стандарте TCP/IP — протоколе 4-го уровня. Зато HTTP прокси кэширует данные и может более тщательно фильтровать содержимое передаваемых данных.

Вы можете использовать SOCKS5-сервер, работающий в составе прокси-сервера для авторизации протоколов, отличных от HTTP. По умолчанию порт доступа 1080, вы также можете его изменить. Авторизация на сервере происходит по ip-адресу пользователя, установив соответствующий флажок, вы можете настроить авторизацию по логину/паролю.

## Антивирус

<input checked="" type="checkbox"/> Использовать антивирус Clamav	<input type="checkbox"/> Использовать внешний ICAP-сервер
<input type="checkbox"/> Использовать антивирус DrWeb	Сервис REQMOD URI
<input type="checkbox"/> Использовать антивирус Касперского	<input type="text" value="icap://192.168.1.1:1344/reqmod"/>
	<input type="checkbox"/> Разрешать доступ при недоступности сервиса
	Сервис RESPMOD URI
	<input type="text" value="icap://192.168.1.1:1344/respmo"/>
	<input type="checkbox"/> Разрешать доступ при недоступности сервиса

---

<input type="checkbox"/> Использовать DLP
<input type="checkbox"/> Использовать контент-фильтр
<input checked="" type="checkbox"/> Использовать SkyDNS
<input type="checkbox"/> Использовать веб-фильтр Касперского

Интернет Контроль Сервер поддерживает сканирование трафика, проходящего через прокси-сервер антивирусом. В версии 4 поддерживается 3 антивирусных модуля: бесплатный ClamAV и платные модули DrWeb и Касперский. Для работы антивируса, необходимо приобрести лицензию и установить её в соответствующем модуле.

Для того, чтобы включить антивирусное сканирование веб-трафика каким-либо антивирусным модулем, необходимо включить соответствующую опцию в настройках прокси. Параметр «Максимальный объем для сканирования» определяет максимальный размер файла, единовременно проходящего обработку антивирусом. Файлы, размер которых превышает

указанный, сканироваться не будут, что может повысить производительность.

Рекомендуется также включить проверку изображений, поскольку существуют вирусы, распространяющиеся через обычные изображения, однако сканирование изображений значительно увеличивает потребление системных ресурсов антивирусом, что при больших объемах графики способно сильно снизить быстродействие сервера.

## Разрешённые порты

Вы можете указать, к каким портам на внешних серверах можно подключаться через прокси-сервер. Список разрешённых портов для SSL определяет, к каким портам разрешён доступ с использованием метода CONNECT.

## ICAP

**ICAP** (Internet Content Adaptation Protocol) - протокол расширения для прокси-сервера. В большинстве случаев он используется для сканирования на вирусы проходящего трафика и применения к нему различных контент-фильтров. Вы можете подключить к прокси-серверу ИКС сторонний ICAP-сервер, отметив соответствующий флажок в настройках и указав его адрес.

Три последних флажка подключают к работе прокси-сервера соответственно, модули [DLP](#) и [контент-фильтра](#) и [skydns](#)

## Автоконфигурация прокси

Для того, чтобы не прописывать вручную прокси-сервер на каждой клиентской машине, вы можете воспользоваться автоконфигуратором. В браузере клиента должна быть выставлена опция «Автоматическая конфигурация прокси», все остальные настройки определит ИКС.

Прокси-сервер    Настройки    **Автоконфигурация**    Родительский прокси    Исключения для авторизации    Кеш    ) >

---

Создать скрипт автоконфигурации прокси

HTTP                       HTTPS                       FTP

Опубликовать по адресу

Создать виртуальный хост на веб-сервере

Создать запись на DNS-сервере

Публиковать скрипт автоконфигурации по DHCP



Он включается установкой флажка в соответствующей вкладке. Вы можете отметить один или несколько протоколов из доступных (HTTP, HTTPS, FTP).

Опция публикации скрипта автонастройки определяет, будет ли он доступен по ip-адресу сервера либо по созданному виртуальному хосту с доменным именем. При выборе виртуального хоста, он автоматически создается в системе. Флажок **«Создать запись на DNS-сервере»** автоматически добавит зону с нужными записями для этого виртуального хоста.

**Публиковать скрипт автоконфигурации по DHCP** - данный параметр передает настройки прокси всем DHCP-клиентам сервера.

## Родительский прокси

Если в вашей организации несколько проксирующих серверов, расположенных иерархично, то вышестоящий для ИКС прокси-сервер будет являться его **родительским прокси**. Кроме того, в качестве родительского прокси может выступать любой узел сети.

Прокси-сервер    Настройки    Автоконфигурация    **Родительский прокси**    Исключения для авторизации    Кеш    › >

Использовать родительский прокси

Адрес \*    Порт \*

192.168.5.6    3128

Использовать ICP

Порт ICP

3130

Использовать авторизацию

Логин \*    Пароль \*

root    ●●●●●●●●

Работать без DNS-сервера

Чтобы ИКС перенаправлял запросы, приходящие на его прокси-сервер, на родительский прокси, укажите его ip-адрес и порт назначения во вкладке «Родительский прокси».

Прокси-сервера могут обмениваться данными своих кэшей по протоколу ICP. В случае работы сети через несколько прокси это может значительно ускорить работу. Если родительский прокси поддерживает работу протокола, отметьте соответствующий флажок и укажите порт работы службы (по умолчанию 3130).

Если родительский прокси работает с авторизацией, то в нижеследующих полях укажите логин и пароль для подключения.

## Выданные ip-адреса

В этой вкладке находится список Ip-адресов и пользователей, которые авторизовались на



прокси-сервере с использованием веб-авторизации.

## Исключения для авторизации

Данная вкладка служит для настройки прокси сервера таким образом, чтобы он не требовал авторизации при: обработке запросов с определенного хоста в сети и/или при обращении на определенный хост. В основном окне отображаются кнопки «Добавить» и «Удалить», соответственно для добавления и удаления информации об исключениях для авторизации в прокси сервере. А также таблица, содержащая наборы исключений. При добавлении исключения доступны следующие поля:

- «Источник». Позволяет задать в качестве источника трафика IP-адрес или сеть, для которых не будет производиться аутентификация в прокси сервере. Это приведет к тому, что трафик идущий с указанных IP-адреса или сети не будет учитываться в статистике за определенными Пользователями. Но будет учитываться в общей статистике.
- «Назначение». В качестве назначения возможно указывать: IP-адрес; IP/mask; имя домена (например, ya.ru); поддомены исключая основной домен (например, ".google.com" – при обращении на drive.google.com авторизация не будет запрошена, но при обращении на google.com будет запрошена авторизация); регулярное выражение в формате - /regex/gi (например, /.\*.ai.\.ru/gi - разрешит домен mail.ru и его поддомены). Правила для заполнения данного поля также распространяются на поля содержащие URL, при создании запрещающего, разрешающего правила или исключения прокси.
- «Описание». Позволяет задать произвольное описание для создаваемого правила.
- «Выкл.». Позволяет выключить созданное правило.

## Содержимое кэша

Прокси-сервер	Настройки	Автоконфигурация	Родительский прокси	Исключения для авторизации	<b>Кеш</b>	>	>
 Очистить кеш				Поиск...			
URL	Объем	Последнее обращение					
<a href="http://testics.local:3128/squid-internal-periodic/store_digest">http://testics.local:3128/squid-internal-periodic/store_digest</a>	410	12:50:45					

Здесь вы можете просмотреть некоторые элементы веб-страниц (в основном изображения), которые сохранились в кэше, а также очистить его содержимое.

## Журнал

Настройки Автоконфигурация Родительский прокси Исключения для авторизации Кеш **Журнал**

07.05.2019 - 07.05.2019 **Сегодня** Неделя Месяц Другой период ↕

Экспорт Удалить логи

Поиск...

Squid Parent: will start 1 kids 12:50:40
Squid Parent: (squid-1) process 57951 started 12:50:40
Squid Parent: will start 1 kids 12:50:40
Squid Parent: (squid-1) process 57959 started 12:50:40

В закладке «Журнал» находится сводка всех системных сообщений от прокси-сервера. Журнал разделен на страницы, кнопками «вперед» и «назад» вы можете переходить со страницы на страницу, либо ввести номер страницы в поле и переключиться сразу на нее.

Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, обработка кэша) - зеленым, ошибки - красным.

В правом верхнем углу модуля находится строка поиска. С ее помощью вы можете искать в журнале нужные вам записи.

Журнал всегда отображает события за текущую дату. Чтобы посмотреть события в другой день, выберите нужную дату, используя календарь в левом верхнем углу модуля.

From:  
<https://doc-new.a-real.ru/> - **Документация**

Permanent link:  
<https://doc-new.a-real.ru/doku.php?id=proxy50>

Last update: **2020/01/27 16:28**

