

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 mime-тиปам. 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 main interface of the Proxy module. At the top, there is a navigation bar with tabs: Прокси-сервер (selected), Настройки, Родительский прокси, Выданные Ip-адреса, Содержимое кеша, and Журнал. Below the navigation bar are two service status cards:

- Прокси-сервер**: Shows a lock icon with a green checkmark, indicating it is running (запущен). It also says "Отвечает за фильтрацию и учет HTTP-трафика". There is a "Выключить" (Shutdown) button to its right.
- Фильтр HTTP-трафика**: Shows a lock icon with a green checkmark, indicating it is running (запущен). It also says "Отвечает за фильтрацию HTTP-трафика". There is a "Выключить" (Shutdown) button to its right.

Below these cards is a large area labeled "Журнал" (Log) containing a list of log entries:

```
13:11:40 Adding nameserver 127.0.0.1 from squid.conf
13:11:40 helperOpenServers: Starting 8/32 'nc' processes
13:11:40 helperOpenServers: Starting 2/32 'basic_ncsa_auth' processes
13:11:40 HTCP Disabled.
13:11:40 Loaded Icons.
13:11:40 Ready to serve requests.
13:11:40 Accepting interceptedHTTP Socket connections at FD 36 on 0.0.0.0:3128
```

At the bottom of the log area, a message says "Показаны последние 20 записей за сегодня" (Showing the last 20 records for today).

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	Выданные Ip-адреса	Содержимое кеша	Журнал
<p>Порт: 3128</p> <p>Тип авторизации: По логину/паролю ИКС</p> <p>Порядок авторизации пользователей: По IP, затем по логину/паролю</p> <p>Скрывать ip-адрес пользователя: <input type="checkbox"/></p> <p>Размер кеша: 100 Мб</p> <p>Ограничивать размер ответа: (не ограничивать) Мб</p> <p>Сообщение о запрете доступа: Доступ запрещен</p> <p>Использовать веб-авторизацию: <input checked="" type="checkbox"/></p> <p>Порт веб-авторизации: 82</p> <p>Только с одного ip-адреса: <input checked="" type="checkbox"/></p>						

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

<input checked="" type="checkbox"/> Использовать прозрачный прокси	Исключения для прозрачного прокси	
Порты*	80	(нет)
Порты для HTTPS*	443	<input type="checkbox"/> Перехватывать трафик из DMZ сетей <input checked="" type="checkbox"/> Перехватывать трафик между локальными сетями
Сертификат для HTTPS фильтрации		
<input checked="" type="radio"/> Расшифровывать трафик с подменой сертификата	<input type="radio"/> Фильтровать без подмены сертификата	Расшифровывать трафик с подменой сертификата для
Не фильтровать HTTPS для	(нет)	(нет)
Разрешенные порты*	Порты для метода CONNECT*	
80, 21, 443, 563, 70, 210, 1025-65535, 280, 488, !	443, 563	

Использовать socks5 сервер
Порт socks5 сервера *
1080 Авторизация на socks5 сервере по логину/
паролю
 Автоматически создавать разрешающее правило

Использовать антивирус Clamav Использовать внешний ICAP-сервер
Сервис REQMOD URI
icap://192.168.1.1:1344/reqmod
 Разрешать доступ при недоступности
сервиса
Сервис RESPMOD URI
icap://192.168.1.1:1344/respmod
 Разрешать доступ при недоступности
сервиса

Использовать DLP
 Использовать контент-фильтр
 Использовать SkyDNS
 Использовать веб-фильтр Касперского

Использовать DNS
127.0.0.1

Сохранить **Обновить**

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.

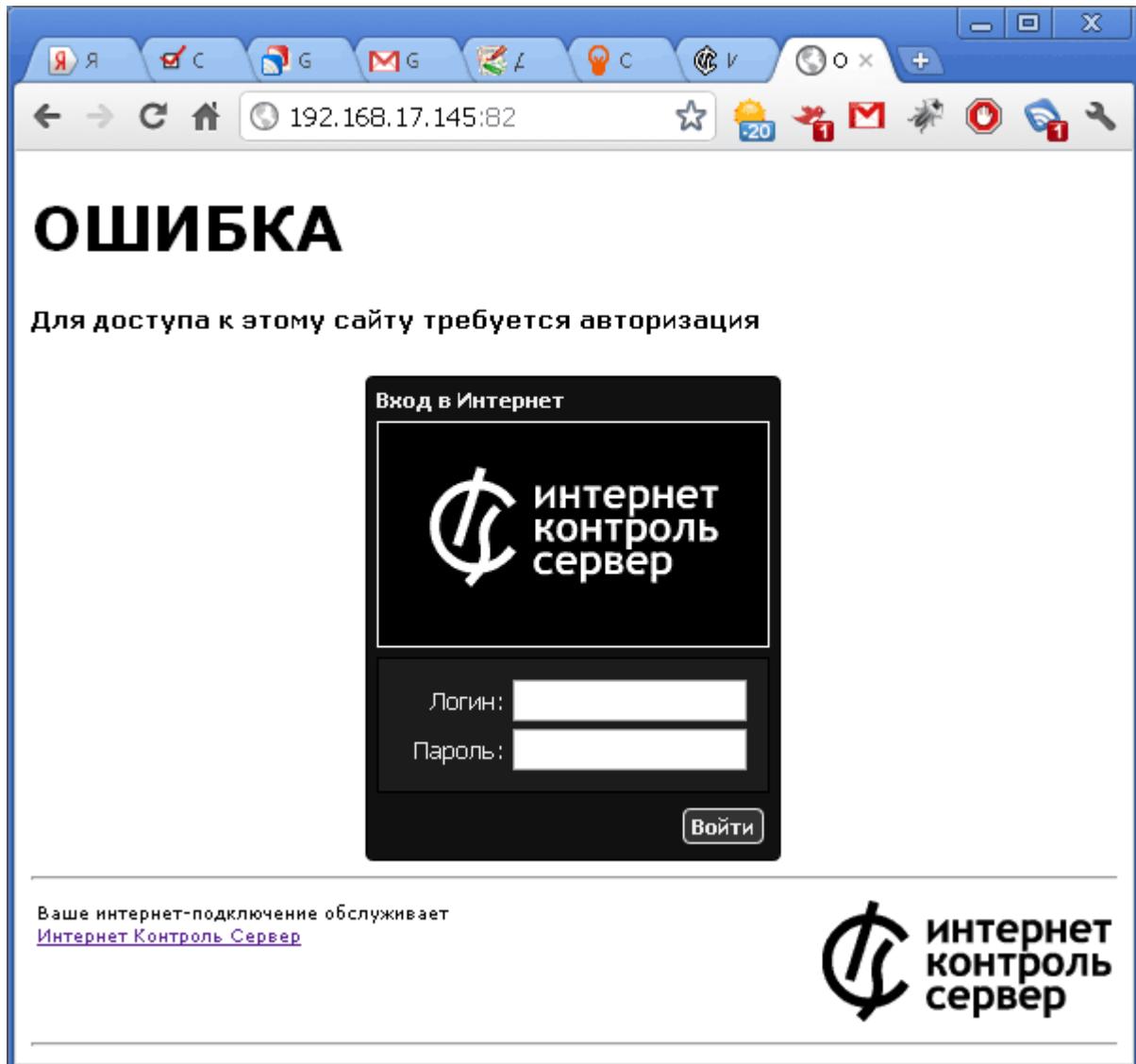
Кроме того, следует помнить о том, что авторизация на прокси используется только для http-трафика пользователей. Доступ в интернет для программ, использующих протоколы, отличные от http, регулируется межсетевым экраном, который имеет только один способ авторизации: по ip-адресу. Другими словами, если 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

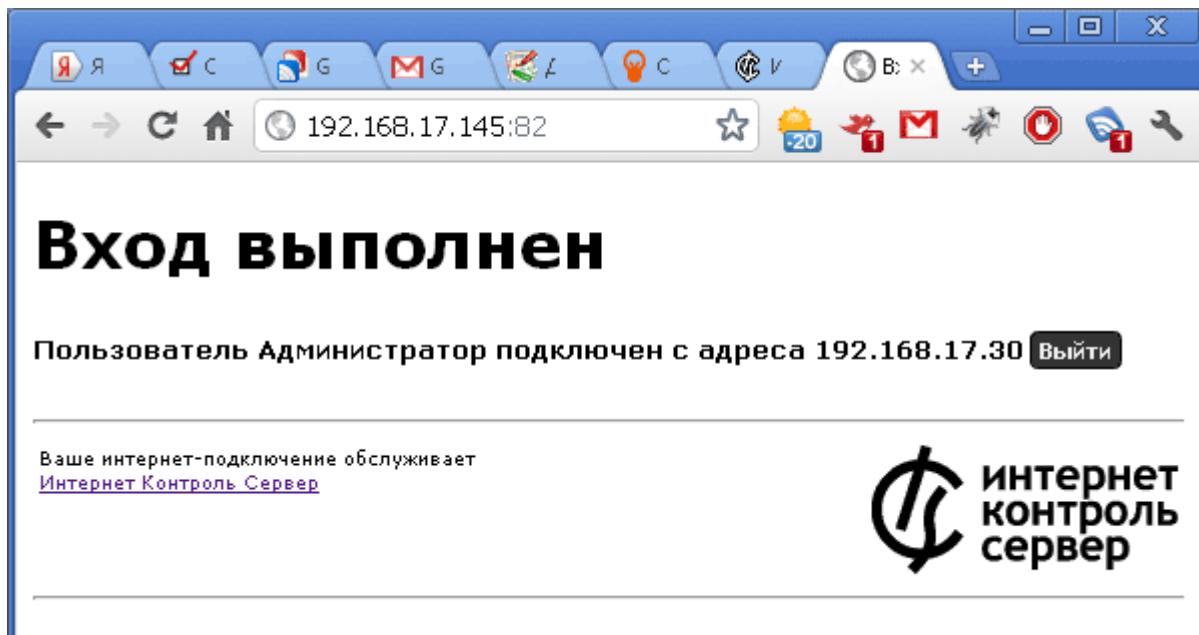
Для того, чтобы авторизовать пользователей без прописанного прокси-сервера по имени пользователя и паролю, вы можете использовать веб-авторизацию (captive portal), включив соответствующий флажок. Веб-авторизация позволяет, к примеру, интегрировать страницу авторизации в корпоративный портал, и использовать 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 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 некоторым 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.

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

Прокси-сервер Настройки Автоконфигурация Родительский прокси Выданные Ip-адреса Содержимое кеша Журнал

Использовать прозрачный прокси:

Порты: 80

Порты для HTTPS: 443

Исключения для прозрачного прокси: (нет) ...

Перехватывать трафик из DMZ сетей:

Перехватывать трафик между локальными сетями:

Сертификат для ssl-фильтрации: (нет) ...

Исключения для HTTPS: (нет) ...

Разрешенные порты: 80, 21, 443, 563, 70, 210, 1025-65535, 280, 488, 591, 777

Порты для метода CONNECT: 443, 563

Порт socks5 сервера: 1080

Авторизация на socks5 сервере по логину/паролю:

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 флаги 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 соединяться с SOCKS прокси сервером. Такой прокси сервер контролирует права клиента для доступа к внешним ресурсам и передаёт запрос к серверу. SOCKS может использоваться и противоположным способом, разрешая внешним клиентам соединяться с серверами за межсетевым экраном

(брандмауэром).

В отличие от HTTP прокси серверов, SOCKS передаёт 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

Использовать антивирус Clamav:

Использовать антивирус DrWeb:

Использовать антивирус Касперского:

Использовать внешний ICAP-сервер:

Сервис REQMOD:
URI: icap://192.168.1.1:1344/reqmod

Разрешать доступ при недоступности сервиса:

Сервис RESPMOD:
URI: icap://192.168.1.1:1344/respmode

Разрешать доступ при недоступности сервиса:

Использовать DLP:

Использовать контент-фильтр:

Использовать SkyDNS:

Сохранить **Обновить**

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

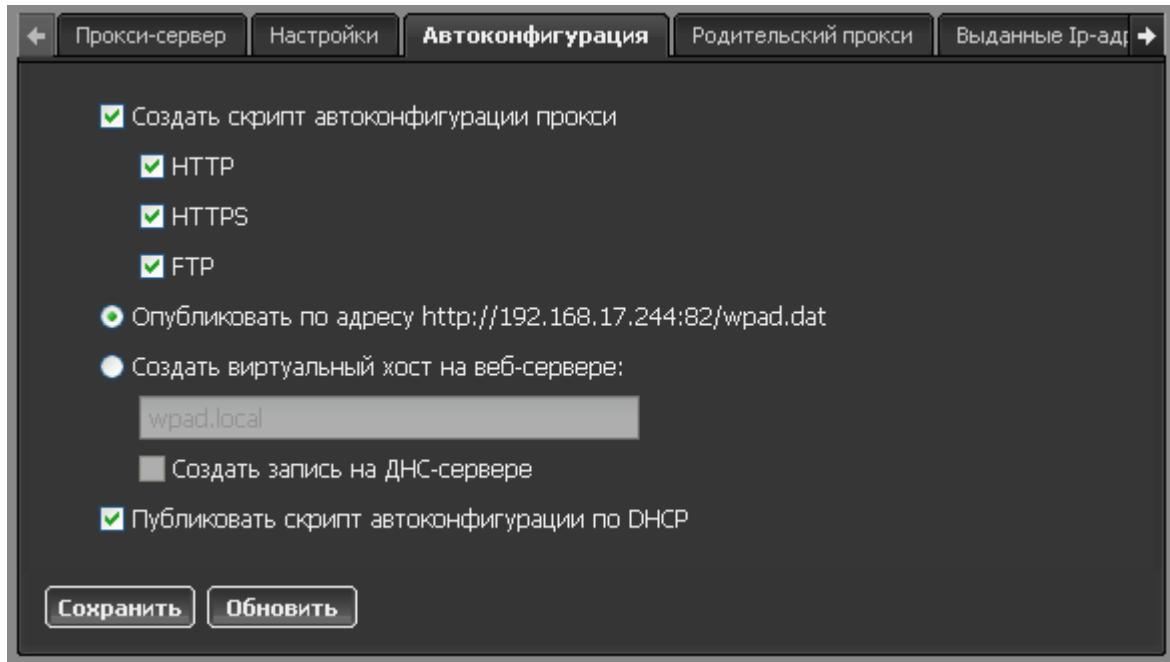
Вы можете указать, к каким портам на внешних серверах можно подключаться через прокси-сервер. Список разрешённых портов для SSL определяет, к каким портам разрешён доступ с использованием метода CONNECT.

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 флагок в настройках и указав его адрес.

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

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.

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

Опция публикации скрипта автонастойки определяет, будет ли он доступен по ip-адресу

сервера либо по созданному виртуальному хосту с доменным именем. При выборе виртуального хоста, он автоматически создастся в системе. Флажок «**Создать запись на ДНС-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

The screenshot shows the 'Parent Proxy' configuration page. At the top, there is a navigation bar with tabs: 'Прокси-сервер', 'Настройки', 'Родительский прокси' (which is selected and highlighted in blue), 'Выданные Ир-адреса', 'Содержимое кеша', and 'Журнал'. The main area contains several configuration sections:

- Использовать родительский прокси:** A checked checkbox. Below it are input fields for 'Адрес:' (192.168.5.6) and 'Порт:' (3128).
- Использовать ICP:** A checked checkbox. Below it is an input field for 'Порт ICP:' (3130).
- Использовать авторизацию:** A checked checkbox. Below it are input fields for 'Логин:' (root) and 'Пароль:' (redacted).
- Работать без ДНС-сервера:** An unchecked checkbox.

At the bottom left are two buttons: 'Сохранить' (Save) and 'Обновить' (Update).

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.

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.

Содержимое кэша

Очистить кеш			
URL	Объем	Последнее обращение	
http://testics.local:3128/squid-internal-static/icons/anthony-script.gif	373	31.01.2011 12:13	
http://testics.local:3128/squid-internal-static/icons/anthony-xpm.gif	386	31.01.2011 12:13	
http://testics.local:3128/squid-internal-static/icons/anthony-image.gif	445	31.01.2011 12:13	
http://mcs2:3128/squid-internal-static/icons/anthony-ps.gif	380	31.01.2011 06:30	
http://testics.local:3128/squid-internal-static/icons/anthony-compress...	387	31.01.2011 12:13	
http://mcs2:3128/squid-internal-static/icons/anthony-script.gif	373	31.01.2011 06:30	
http://mcs2:3128/squid-internal-static/icons/anthony-binhex.gif	384	31.01.2011 06:30	
http://mcs2:3128/squid-internal-static/icons/anthony-image2.gif	422	31.01.2011 06:30	
http://mcs2:3128/squid-internal-static/icons/anthony-portal.gif	390	31.01.2011 06:30	
http://mcs2:3128/squid-internal-static/icons/anthony-movie.gif	369	31.01.2011 06:30	
http://testics.local:3128/squid-internal-static/icons/anthony-xbm.gif	372	31.01.2011 12:13	

Стр 1 из 1 | Показаны записи 1 - 50 из 50

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

Журнал

Прокси-сервер | Настройки | Родительский прокси | Выданные Ир-адреса | Содержимое кеша | Журнал

14.09.2011 | Экспорт

Время	Сообщение
13:02:58	WARNING: redirector #3 (FD 17) exited
13:02:58	Too few redirector processes are running (need 4/32)
13:02:58	Starting new helpers
13:02:58	helperOpenServers: Starting 4/32 'nc' processes
13:02:58	WARNING: redirector #4 (FD 19) exited
13:02:58	Too few redirector processes are running (need 4/32)
13:02:58	Starting new helpers
13:02:58	helperOpenServers: Starting 4/32 'nc' processes
13:02:58	WARNING: redirector #7 (FD 25) exited
13:02:58	Too few redirector processes are running (need 3/32)
13:02:58	Starting new helpers
13:02:58	helperOpenServers: Starting 3/32 'nc' processes
13:02:58	WARNING: redirector #1 (FD 11) exited
13:02:58	Too few redirector processes are running (need 1/32)

| < | Стр 1 из 2 | > | | Показаны записи 1 - 100 из 151 |

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-old.a-real.ru/> - Документация

Permanent link:
<https://doc-old.a-real.ru/doku.php?id=%D0%BF%D1%80%D0%BE%D0%BA%D1%81%D0%B8&rev=1573395752>

Last update: 2020/01/27 16:28

