Инструкции по настройке сервиса

Рекомендации по усилению защиты от обхода фильтрации

Общие рекомендации

1. Заблокируйте категорию **Прокси и анонимайзеры**.
2. Убедитесь, что **пользователи используют ограниченную учетную запись** в операционной системе. Использование ограниченной учетной записи и отсутствие доступа пользователей к учетной записи администратора лишает пользователей возможности удалить агент SkyDNS, установить стороннее программное обеспечение, изменить файл hosts или изменить сетевые настройки, в том числе возможности изменить адрес сервера DNS.
3. **Запретите доступ к другим DNS**. Если доступ в интернет осуществляется через шлюз или бытовой роутер, то, по возможности, запретите доступ к любым другим серверам DNS кроме 193.58.251.251 или кэширующего сервера DNS на вашем шлюзе/роутере. Для этого в настройках firewall на роутере запретите прохождение пакетов по протоколам TCP и UDP на порт 53 на любые IP-адреса, кроме 193.58.251.251.
4. **Запретите доступ к HTTP прокси серверам**. Для этого в настройках firewall на роутере запретите прохождение пакетов по протоколам TCP и UDP на наиболее популярные порты 3128 и 8080 на любые IP-адреса.
5. **Отключите опцию DNS Crypt** в браузерах, также эта опция может называться **Использовать безопасный DNS сервер**.

Рекомендации для администраторов корпоративных сетей

1. Настройте перенаправление DNS запросов на адрес серверов SkyDNS или на кэширующий сервер DNS в корпоративной сети.
2. Запретите доступ к внешним прокси серверам.
3. Ограничите доступ к сайтам с обращением к ним по прямому IP адресу, без ввода имени сайта.
4. Ограничьте пользователям возможность создавать и осуществлять подключения к неизвестным внешним серверам VPN.
5. Ограничьте пользователям возможность запускать стороннее программное обеспечение.
6. Ограничьте пользователям возможность подключать стороннее оборудование к рабочим станциям.

FAQ — список частых вопросов

1. Следит ли SkyDNS за моим трафиком?

SkyDNS не является провайдером и не имеет доступа к вашему трафику. Мы не знаем, какие именно странички вы посещаете, так как по протоколу DNS передаются только названия доменов, а не полные ссылки.

Соответственно, мы не желаем и не имеем никакой технической возможности отслеживать такую информацию, как передаваемые на сайты логины и пароли, вашу электронную почту, сообщения в мессенджерах и так далее.

О нашей политике защиты личных данных вы можете узнать из документа Политика конфиденциальности.

2. Зачем нужна регистрация?

Зарегистрировавшись на нашем сайте, вы сможете выбирать категории ресурсов, которые желаете заблокировать, а также вести собственные белые и черные списки доменов.

Работать через SkyDNS можно и без регистрации, но в этом случае мы будем защищать вас только от наиболее опасных сайтов, распространяющих вирусы, а также от фишинговых ресурсов, которые открывают мошенники, чтобы воровать логины и пароли пользователей.

Кроме того, без регистрации могут обойтись те пользователи, которые пользуются нашим сервисом, как обычной DNS-службой. Это может быть актуально в случаях, когда DNS-серверы вашего провайдера или сотового оператора не справляются с нагрузкой, периодически падают или работают нестабильно.

Также в режиме без регистрации для повышения безопасности использования заблокирован доступ к фишинговым и вирусным сайтам.

3. Что делать, если сайты не блокируются?

Для нормальной работы SkyDNS необходимо выполнить два шага.

Во-первых, зарегистрируйтесь на сайте, перейдите на вкладку фильтр, и установите галочки напротив всех категорий, которые необходимо заблокировать.

Во-вторых, если вы пользуетесь операционной системой Windows, то скачайте из личного кабинета и установите программу SkyDNS Agent. Если вы используете другую систему или аппаратный роутер/firewall, то настройте сетевое подключение вашего компьютера или роутера на работу со SkyDNS согласно указаниям руководства.

Если вы выполнили оба шага, но фильтрация не работает, обратитесь в нашу поддержку.

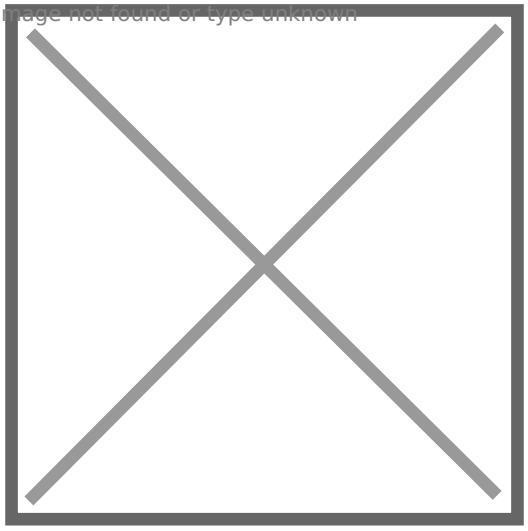
Для пользователей, находящихся за прозрачным прокси, фильтрация SkyDNS работать не будет, но мы постараемся устранить эту проблему в будущем.

4. Как отказаться от использования сервиса?

Для того, чтобы полностью исключить влияние SkyDNS на работу в Интернет, необходимо вернуть сетевые настройки вашего компьютере в исходное состояние. Смените адрес DNS-сервера, а также деинсталлируйте SkyDNS Agent, если вы им пользуетесь.

Для смены DNS-сервера откройте диалоговое окно настроек сети согласно инструкции, но вместо адреса наших серверов установите галочку «Получить адрес DNS-сервера автоматически» или впишите настройки предоставленные вам провайдером.

Image not found or type unknown



На сайте Microsoft вы можете ознакомиться с альтернативным описанием.

5. Можно ли удалить мой аккаунт из сервиса SkyDNS?

Мы не удаляем аккаунты пользователей. Если вы желаете отказаться от услуг сервиса, смените адрес наших DNS-серверов на адрес вашего провайдера, или другой публичной службы DNS (см. пункт 4).

6. Откуда вы взялись в моем компьютере, я к вам не подключался?

Если вы самостоятельно не регистрировались в нашем сервисе и увидели блокировку каких-либо сайтов нашим сервисом, обратитесь к вашему провайдеру, администратору компании или родителям за разъяснениями и для получения доступа.

Чтобы наш сервис интернет-фильтрации мог работать на вашем компьютере у вас должна быть установлена программа SkyDNS Agent или же сделаны изменения в настройках DNS (на вашем компьютере или роутере). Всё это могут сделать только лица, имеющие соответствующий доступ к этому оборудованию.

7. Снимите запрет с сайта ВКонтакте, Одноклассники и т.п.

Если вы пользуетесь нашей системой дома и являетесь зарегистрированным пользователем, то вы можете самостоятельно настроить правила фильтрации в личном кабинете.

В противном случае вам необходимо обратиться к тому, кто поставил блокировку (провайдер, работодатель, родители).

8. У меня блокируются сайты и категории, другие чем настроены в личном кабинете

Если у вас заблокировался сайт из какой-то другой категории (показывается на странице блокировки), то, скорее всего, вы сделали привязку своего IP адреса как статического в личном кабинете сервиса, но на самом деле ваш IP адрес динамический.

В этом случае вы можете при очередной смене динамического IP адреса, попасть под настройки другого пользователя вашего провайдера, также сделавшего привязку IP адреса как статического. Для исправления снимите привязку статического IP и установите SkyDNS Agent.

9. Я хочу пожаловаться на плохой сайт или неправильную категорию блокируемого сайта

Вы можете сделать это, воспользовавшись сервисом проверки.

10. Могу ли я настроить ваш сервис на роутере?

Да, наш сервис может быть настроен на аппаратном роутере. В большинстве случаев достаточно указать в настройках наш DNS-сервер и сделать привязку статического IP адреса роутера в личном кабинете на сайте.

11. Можно ли сделать разные настройки фильтрации для разных компьютеров в локальной сети?

Если ваши компьютеры работают под ОС Windows, то вы можете установить SkyDNS Agent и выбрать, какой профиль фильтрации использовать на конкретном компьютере. Для всех

прочих компьютеров будет действовать профиль по умолчанию.

12. SkyDNS Agent выдает ошибку идентификации и пишет **токен не доступен**

Обновите агент до последней версии. Если вы используете агента до версии 2.2 и не имеете возможности его обновить, тогда сделайте следующее: войдите в агент - **Настройки** - **Сменить пользователя** (ссылка справа под списком подключений) и нажмите кнопку **Вход**.

13. У меня не работает фильтрация, я пользуюсь услугами провайдера Акадо

Данный провайдер блокирует обращения к сторонним DNS-серверам при использовании внутренних IP-адресов. Более подробно можно посмотреть на сайте Акадо.

Чтобы воспользоваться нашими услугами вам нужно получить внешний IP у провайдера.

14. Фильтрация то работает, то не работает

Такая ситуация возможна в следующих случаях:

- Вы оставили в настройках DNS вторичный DNS-сервер вашего провайдера. В этом случае часть запросов может обслуживаться DNS-сервером провайдера, который соответственно ничего не фильтрует. Для исправления - удалите все альтернативные DNS-серверы из настроек.
- Ваш компьютер поддерживает IPv6 и настроен на автоматическое получение IPv6-адреса DNS-сервера. В этом случае часть запросов может обслуживаться DNS-сервером, который доступен по IPv6 (т.е. не нашим). Естественно, он ничего не фильтрует. Для исправления в настройках протокола IPv6 (если он включен) вместо "Получить адрес DNS-сервера автоматически" установите "Использовать следующие адреса DNS-серверов", а поля с адресами DNS-серверов оставьте пустыми.
- Вы сделали привязку своего IP адреса как статического в личном кабинете сервиса, но на самом деле ваш IP адрес динамический. В этом случае вы можете при очередной смене динамического IP адреса, попасть под настройки другого пользователя вашего провайдера, также сделавшего привязку IP адреса как статического. Для исправления — снимите привязку статического IP и установите SkyDNS Agent.

15. Добавляю Вконтакте, Youtube, Facebook, skype.com или другой сайт в белый список, но сайт показывается неправильно или программа (например, skype) не работает.

Многие сайты в целях повышения производительности используют несколько разных адресов для загрузки своих данных. Например, Вконтакте использует адрес vk.com для загрузки страниц, а картинки и прочие элементы страницы грузятся с домена userapi.com.

Если вы заблокировали категорию, но хотите разблокировать отдельные такие сайты из этой категории, то необходимо внести в белый список все домены, которые используют эти сайты.

Чтобы найти блокируемые домены на странице выполните действия:

1. Очистите историю (журнал) в браузере (Google Chrome или Firefox), перезапустите браузер.
2. В Google Chrome нажмите клавишу F12, выберите Console, перезагрузите страницу и посмотрите в консоли строки с ошибкой 403 (FORBIDDEN). Аналогично в Firefox - Веб-разработка & Веб-консоль.
3. Добавьте нужные домены в белый список в личном кабинете на skydns.ru

Ниже приведены примеры для некоторых сайтов, которые используют несколько адресов. Разработчики таких сайтов могут в любое время изменить или добавить служебные адреса, используемые для работы сайтов.

Чтобы разблокировать ВКонтакте полностью, вам нужно добавить в белый список следующие записи:

- vk.com (без www)
- userapi.com
- vk-portal.net
- vk.me
- vkadre.ru
- vkdownloader.net
- vkuser.net
- vkuseraudio.net
- vkuserlive.com
- vkuservideo.net

Чтобы разблокировать YouTube полностью, вам нужно добавить в белый список следующие записи:

- youtube.com (без www)
- googlevideo.com
- wide-youtube.l.google.com
- youtube-nocookie.com
- youtube.googleapis.com
- youtube.l.google.com
- youtubei.googleapis.com
- ytimg.com

- ytimg.l.google.com

Чтобы разблокировать Skype полностью, вам нужно добавить в белый список следующие записи:

- skype.com (без www)
- azureedge.net
- browser.pipe.aria.microsoft.com
- c-msedge.net
- cloudapp.net
- download.skype.com
- dr.skype-cr.akadns.net
- edgecastdns.net
- get.skype.com
- login.live.com
- messenger.live.com
- mobile.pipe.aria.microsoft.com
- msedge.net
- msftconnecttest.com
- msn.com.akadns.net
- s-msedge.net
- skype-dsn.akadns.net
- skype.net
- skypeassets.com
- skypedata.akadns.net
- trafficmanager.net
- v0cdn.net
- web.skype.com

Чтобы разблокировать WhatsApp полностью, вам нужно добавить в белый список следующие записи:

- whatsapp.com
- whatsapp.net

Чтобы разблокировать Viber полностью, вам нужно добавить в белый список следующие записи:

- viber.com

Чтобы разблокировать Google Drive полностью, вам нужно добавить в белый список следующие записи:

- google.com
- gstatic.com
- googleusercontent.com
- googleapis.com

Чтобы разблокировать Hamachi полностью, вам нужно добавить в белый список следующие записи:

- hamachi.cc
- logmein-gateway.com
- logmein.com

Чтобы разблокировать Zoom полностью, вам нужно добавить в белый список следующие записи:

- zoom.us
- zoom.com

16. Я внес/внесла изменения в настройки фильтрации, но ничего не изменилось.

Изменения в настройках распространяются по серверам SkyDNS в течение нескольких минут. Проверьте через 10-15 минут, что изменения вступили в силу.

Кроме того, если вы ранее заходили на сайты, относительно которых вы меняли настройки, то ответы DNS серверов скорее всего, находятся в кэше браузера, клиента DNS на локальном компьютере, кэширующем DNS (если запущен) на точке доступа/маршрутизаторе/роутере (если используется для выхода в интернет).

Для скорейшего вступления в действие изменения настроек может понадобиться перезапустить браузер. В большинстве случаев этого достаточно.

Если после перезапуска браузера изменений нет, то выполните команду ipconfig /flushdns на локальном компьютере, которая очистит кэш клиента DNS Windows.

В еще более редких случаях может понадобиться очистить кэш DNS на точке доступа/маршрутизаторе/роутере (если используется).

17. Я открыл/открыла доступ к сайту, но выдается сообщение вида Доступ всё ещё закрыт.

Сообщение вида **Доступ всё ещё закрыт!** может выдаваться в случае, если на нашем DNS сервере данный сайт для вас разблокирован, но ваш браузер на основании информации в его кэше или кэше какого-либо промежуточного сервера у вас по прежнему обращается к странице блокировки.

Для скорейшего вступления в действие изменения настроек может понадобиться перезапустить браузер. В большинстве случаев этого достаточно.

Если после перезапуска браузера изменений нет, то выполните команду ipconfig /flushdns на локальном компьютере, которая очистит кэш клиента DNS Windows.

В еще более редких случаях может понадобиться очистить кэш DNS на точке доступа/маршрутизаторе/роутере (если используется).

У пользователей в организациях такое сообщение может выдаваться в случае, если запросы DNS приходят с одного IP адреса, а HTTP запросы с другого IP адреса, который не добавлен в профиле в личном кабинете. Убедитесь что оба IP адреса привязаны к вашему профилю.

18. После установки агента SkyDNS или при вводе в сетевых настройках адреса DNS сервера SkyDNS 193.58.251.251 пропадает интернет.

Наиболее вероятно, что ваш провайдер блокирует доступ к DNS серверам отличным от своих и адреса сайтов не могут быть разрешены в IP-адреса. В таком случае, при вводе в качестве адреса DNS сервера 8.8.8.8 (DNS сервер Google), скорее всего, будет наблюдаться та же картина.

Вы можете обратиться к вашему провайдеру с просьбой открыть доступ к DNS серверам в интернете или сменить провайдера.

19. Не работает фильтрация при установке агента и замене прописанного после установки DNS 127.0.0.1 на 193.58.251.251 или адрес другого сервера DNS.

При установленном агенте SkyDNS адрес DNS в настройках должен оставаться 127.0.0.1. Если вы изменили адрес на какой-то другой, то верните 127.0.0.1

20. Не работает DNS сервер и агент SkyDNS на одном сервере.

Агент SkyDNS привязывается к порту 53, который используется серверами DNS, на локальном адресе 127.0.0.1 и прописывает этот адрес в качестве адреса DNS сервера в сетевых настройках при установке. Поэтому работа на одном компьютере агента SkyDNS и сервера DNS невозможна. В вашей организации необходимо запускать сервер DNS и агент SkyDNS на разных физических серверах или виртуальных машинах.

21. Работает ли фильтрация SkyDNS с прокси-сервером?

Да, работает.

Для этого необходимо настроить прокси-сервер на использование DNS-сервера SkyDNS с IP адресом 193.58.251.251. Укажите в настройках прокси-сервера DNS-сервер 193.58.251.251. Если прокси-сервер использует системный клиент DNS операционной системы или получает список серверов DNS из настроек ОС, то в сетевых настройках ОС пропишите DNS-сервер SkyDNS с IP адресом 193.58.251.251.

Для SQUID используйте список DNS серверов из ОС или параметр dns_nameservers.

При использовании прокси-сервера запросы к серверам DNS осуществляет прокси-сервер. Для всех пользователей, использующих прокси-сервер, будут применяться единые настройки фильтрации, которые действуют для прокси-сервера.

На ОС Windows также возможно использование агента SkyDNS и прокси-сервера на одном хосте. Для такой конфигурации настройте прокси-сервер на использование DNS 127.0.0.1.

> При использовании такого решения не будет отображаться страница блокировки. Вместо страницы блокировки браузер будет показывать, что сайт недоступен.

> Невозможна работа на одном хосте агента SkyDNS и DNS сервера, который может идти в составе ПО совместно с прокси-сервером.

22. Работает ли фильтрация SkyDNS с Active Directory?

Да, работает.

Для этого настройте Службу DNS на пересылку запросов внешних DNS-имен на DNS-сервер SkyDNS с IP адресом 193.58.251.251.

23. Как я могу использовать локальные ресурсы моего провайдера невидимые из интернет (например, music.local)?

Если у вашего провайдера используются локальные ресурсы невидимые из интернет (например, music.local), то доступа к ним в настройке по умолчанию не будет.

Для решения этого вопроса у нас есть функция **Алиасов**, когда вы сообщаете нашей системе о подобных ресурсах.

На странице Исключения в личном кабинете необходимо настроить Алиас для такого ресурса, указав имя локального ресурса (music.local) и его IP адрес.

Узнать IP адрес ресурса можно следующим образом:

1. Временно отключите агент - кликните правой клавишей на иконке агента возле часов и выберите **Выключить фильтрацию до перезагрузки**.
2. Нажмите **Пуск** и выполните команду cmd.
3. В открывшемся черном окне напишите nslookup music.local
4. Запишите IP адрес из последней выданной строки с названием Address.
5. В личном кабинете на странице Исключения в подразделе Алиасы укажите имя music.local и записанный IP адрес.
6. Включите фильтрацию в агенте.

После этого локальный ресурс будет вам доступен.

24. Почему в интерфейсе агента и на сайте в личном кабинете отображаются разные настройки фильтрации?

Если настройки фильтрации были изменены на сайте SkyDNS в личном кабинете, то в интерфейсе агента могут отображаться не актуальные настройки. В течение часа в агенте SkyDNS станут отображаться те же настройки, что и в личном кабинете на сайте SkyDNS.

25. Я включаю блокировку социальных сетей, но vk.com остается доступен.

Это может быть вызвано теми же причинами, что и пункт 14.

26. Я подключаюсь через провайдера Yota и включаю фильтрацию SkyDNS на роутере Zyxel Keenetic или использую агент SkyDNS, но фильтрация не работает.

У нас имеется информация по данным обращений пользователей Yota, что Yota модифицирует запросы DNS и очищает дополнительную секцию в запросе DNS, в которой находится идентификационный токен. В результате наш сервер не имеет данных для того, чтобы применить ваши настройки фильтрации при ответе на запрос DNS. Вы можете использовать сервис SkyDNS с привязкой статического IP-адреса или имени хоста и использования одного из сервисов динамического DNS как описано в этом примере.

27. В нашей организации используется кэширующий DNS bind9, который разрешает домены через сервера SkyDNS. Некоторые домены оказываются заблокированными, хотя находятся в разрешенных категориях или в белом списке.

В используемой Вами схеме нужно учитывать следующие особенности:

1. Ответы нашего сервера DNS кеширует ваш DNS. Для очистки кэша bind9 можно воспользоваться командой "rndc flush". После этого в логах bind9 должны появиться записи "received control channel command 'flush'" и "flushing caches in all views succeeded".
2. Когда bind9 (ваш DNS) в ответ на запрос получает запись CNAME (в ответе также содержаться IP-адреса, в которые разрешился домен), то он на IP-адреса в ответе не смотрит и пытается самостоятельно разрешить каноническое имя в IP-адреса. Если каноническое имя не находится в разрешенных, то оно разрешается в IP-адрес страницы блокировки.

Подробнее по второму пункту на примере.

Имеем запись

```
bar.example.com.        CNAME   foo.example.com.
```

Слева записан алиас. Справа - каноническое имя.

Клиент запрашивает **bar.example.com**, в ответ получает **foo.example.com** и IP-адреса, в которые разрешается **foo.example.com**. Но bind9 в таком случае на IP-адреса не смотрит и пытается разрешить **foo.example.com**, делая еще один запрос. Если **bar.example.com** находится в разрешенных сервере, а **foo.example.com** находится в заблокированных, то bind9 получит от нашего сервера в ответ адрес страницы блокировки и вернет его конечному клиенту.

Хотя, если бы конечный клиент запрашивал **bar.example.com** у нашего сервера напрямую, а не у кеширующего bind9, то получил бы в ответ действительный IP-адрес **bar.example.com**.

Учитывая, что домены принадлежащие Яндекс, Google, Microsoft и другим глобальным организациям часто разрешаются в CNAME, которые часто входят в CDN (content delivery network), то нужно добавлять в белый список не только алиасы, но и канонические имена.

28. Вместо персональной страницы блокировки отображается стандартная страница блокировки с сообщением вида **Доступ всё ещё закрыт!**.

Это может быть вызвано теми же причинами, что и пункт 17.

29. При использовании фильтрации SkyDNS на роутере Zyxel Keenetic применяется не тот профиль фильтрации, который выбран для устройства в локальной сети.

Убедитесь, что на роутере Zyxel Keenetic установлена последняя версия прошивки.

Убедитесь, что устройство подключено к роутеру Zyxel Keenetic напрямую, а не через какой-либо маршрутизатор.

Убедитесь, что устройство использует только одно подключение к роутеру, а не подключено, например, через проводное подключение и через Wi-Fi к роутеру Zyxel Keenetic.

Убедитесь, что в вашей локальной сети не используется прокси-сервер, кэширующий DNS или Active Directory, т.к. в этом случае запросы DNS на роутер Zyxel Keenetic приходят с MAC-адреса используемого сервера и применяется профиль фильтрации, назначенный серверу.

30. При блокировке доступа к, например, Youtube, доступ через браузер блокируется, а через приложение Youtube доступен.

Для блокировки доступа необходимо очистить кэш DNS и перезапустить приложение, через которое осуществляется доступ. На планшетах, телефонах или в ОС Windows 8 приложения могут не закрываться, а сворачиваться и оставаться в памяти. Для очистки кэша DNS и закрытия приложения перезагрузите устройство.

31. Как заблокировать Skype?

Клиент Skype при первом удачном подключении скачивает список IP-адресов супернод и в дальнейшем подключается к ним даже если не может разрешить имя домена в IP.

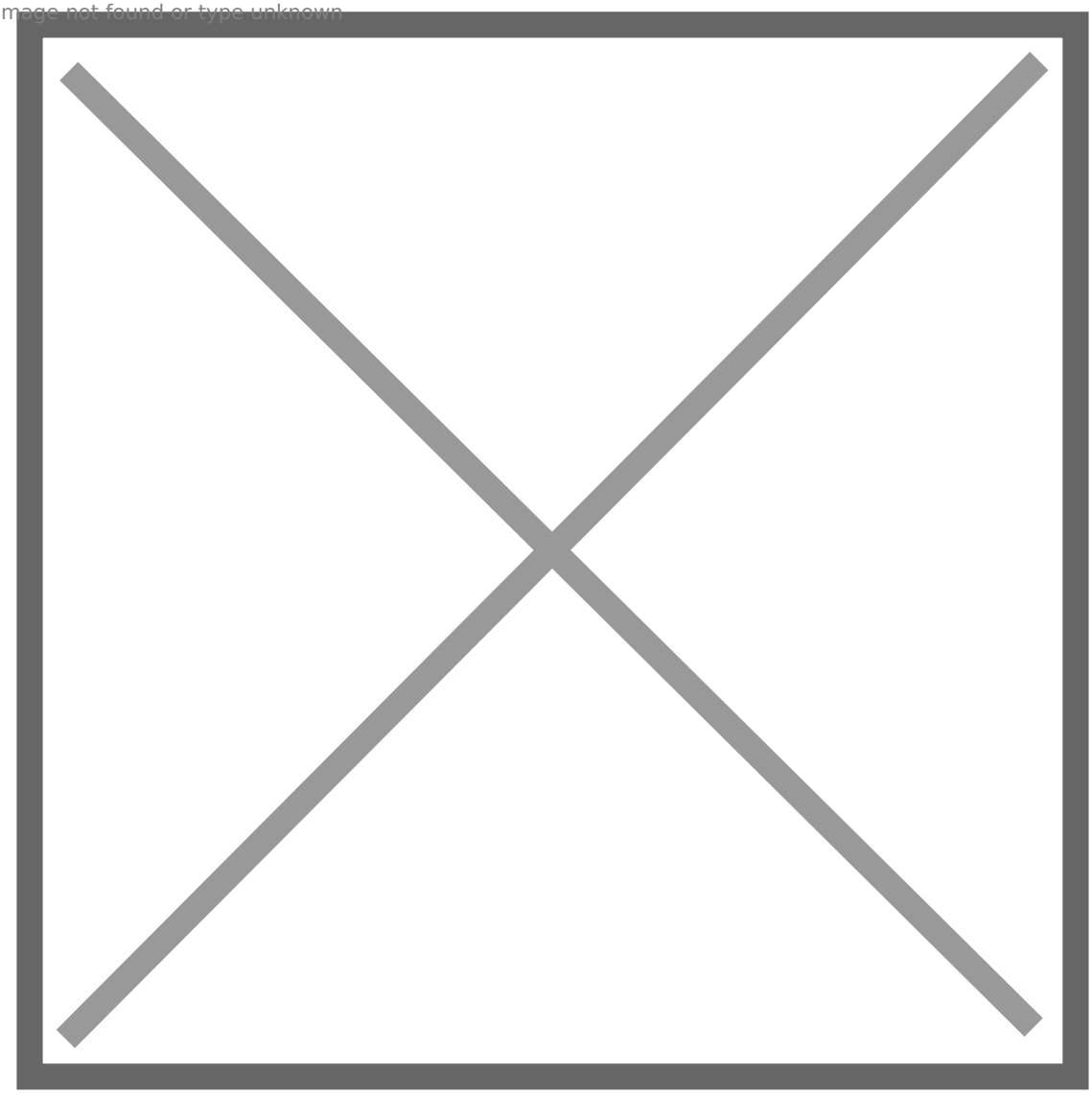
Заблокируйте категорию **Чаты и мессенджеры**. Попробуйте удалить каталог Skype в папке AppData/Roaming каждого профиля пользователя на каждом компьютере и очистить кэш DNS командой ipconfig /flushdns.

Настройка профилей фильтрации

По умолчанию на все компьютеры, подключаемые к сервису, действует профиль **Основной**. Данный профиль нельзя удалить, в отличии от профилей создаваемых пользователем.

1. Для создания нового профиля перейдите на вкладку **Настройки** и далее **Профили**. На этой странице отображаются все созданные вами профили и перечень адресов, на которые они действуют. Для создания нового профиля введите его имя и нажмите **Добавить**.

Image not found or type unknown



2. После создания нового профиля необходимо назначить этому профилю адреса на которые распространяется его действие. Это можно сделать на вкладке **Настройки - Устройства** и

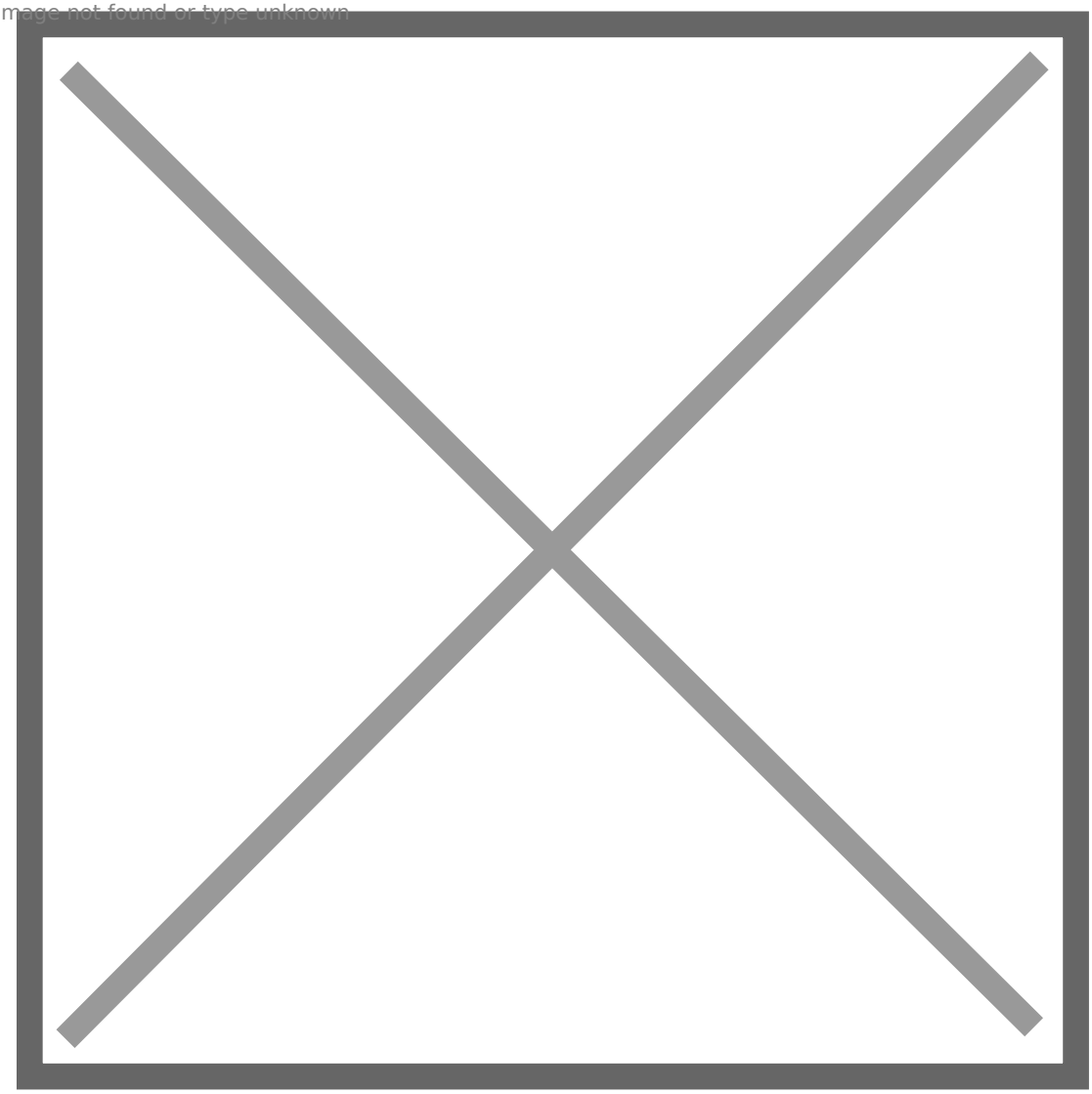
далее **IP-адреса/DynDNS**.

Профиль назначается при добавлении нового IP адреса или DynDNS хоста. По умолчанию на все ранее введенные адреса и динамические IP адреса действует профиль **Основной**. Для смены профиля необходимо отредактировать добавленный адрес или удалить адрес и добавить его снова к нужному профилю.

> Если Вы используете агент SkyDNS, то привязывать адреса к профилям фильтрации не нужно. Вы можете выбрать нужный профиль фильтрации в агенте SkyDNS.

3. После создания профиля и назначения его необходимым адресам нужно настроить правила фильтрации для созданных профилей и профиля **Основной**. Зайдите на вкладку **Категории** и в выпадающем списке в блоке сверху выберите настраиваемый профиль.

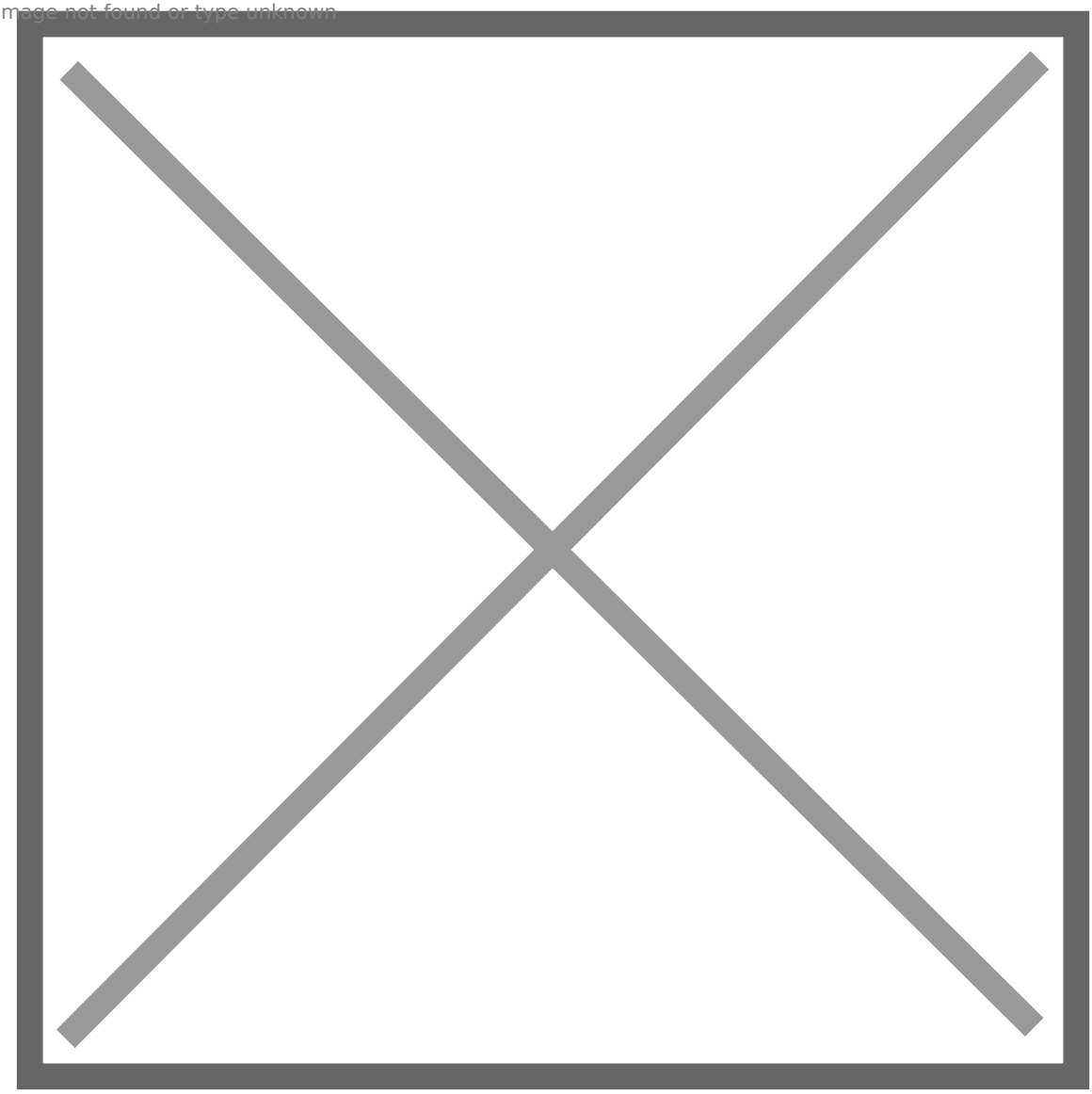
Image not found or type unknown



После настройки блокируемых категорий нажмите кнопку **Сохранить.**

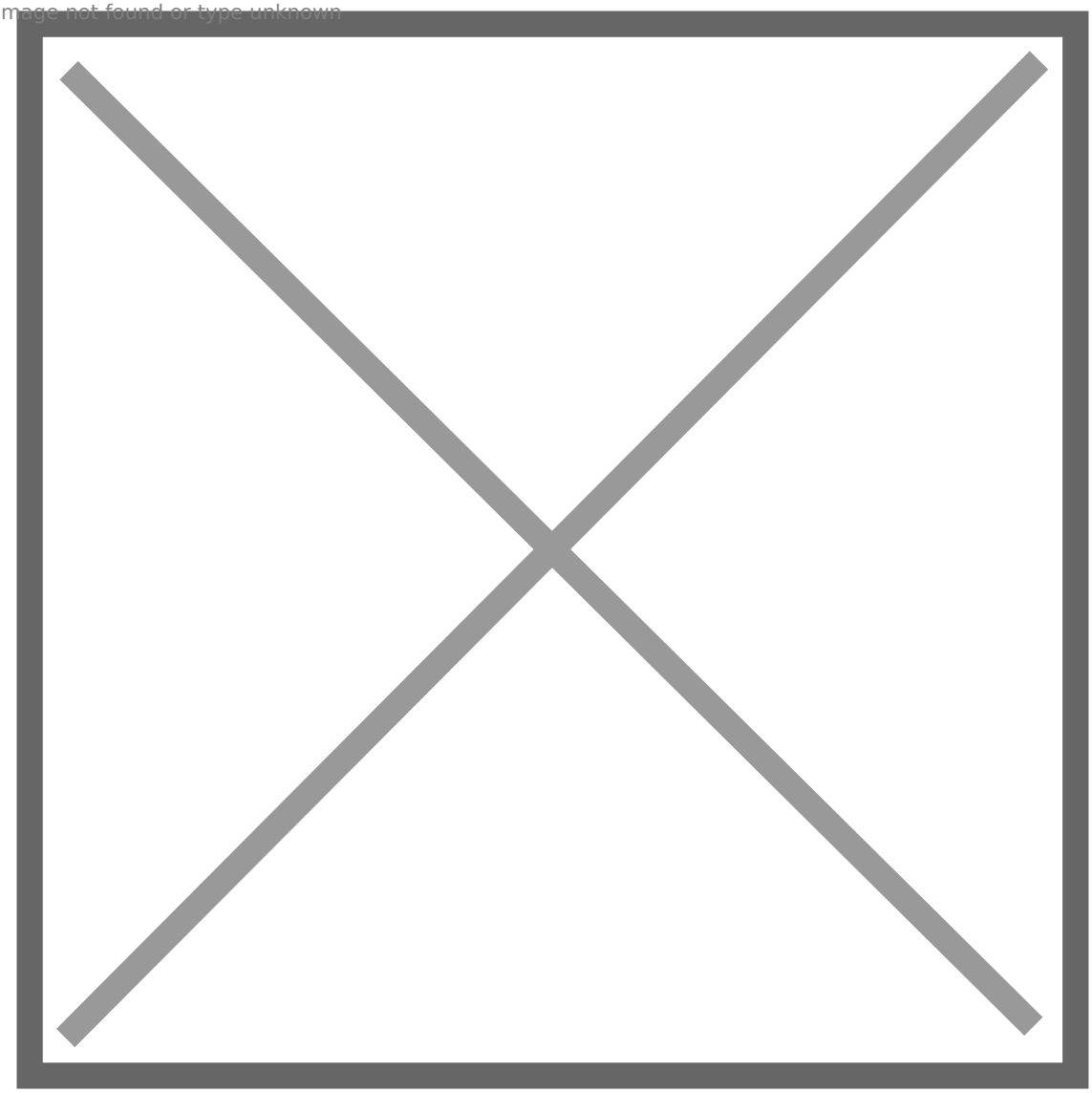
Аналогичным образом настраиваются алиасы, разрешающие и запрещающие списки для профиля на странице **Списки**.

Image not found or type unknown



4. Для настройки расписания действия профилей отличных от профиля **Основной** перейдите на вкладку **Настройки** и далее **Расписание**. Из выпадающего списка выберите профиль, для которого нужно настроить расписание. Установите галочку **Расписание включено**. Настройте периоды, в которые будет включен профиль. В периоды, когда профиль выключен, будет действовать профиль **Основной**.

Image not found or type unknown



Если Вы используете агент SkyDNS, то все описанные настройки можно выполнить следуя инструкции по работе с агентом SkyDNS.

Настройка расписания работы фильтрации

Расписание в сервисе реализуется через дополнительные профили настроек. Каждому профилю можно задать свой график включения и отключения. В то время когда вы указываете активность профиля с расписанием будут соответственно действовать все настройки этого профиля, в остальное же время, когда согласно расписания установлено выключение профиля, будет активен профиль по умолчанию **Основной**.

Система расписания позволяет гибко настраивать время и режимы фильтрации под любые сценарии работы, такие как:

1. Отключение интернета по расписанию, с фильтрованным защищенным интернетом в остальное время. Такой вариант часто используется родителями для ограничения школьников в учебные часы.
2. Фильтрация социальных сетей в рабочее время, со свободным доступом в обеденный перерыв, а также до начала рабочего дня и после его окончания. Очевидно, что такой вариант удобен для использования в организациях.
3. Более строгая фильтрация в часы, когда за компьютером находится ребенок, и более слабая фильтрация или её отсутствие в часы, когда за компьютером начинают работать взрослые.

Сейчас мы рассмотрим, как включить и настроить расписание. Далее рассмотрим настройку типовых сценариев фильтрации по расписанию дома и в организации.

Для настройки расписания необходимо создать дополнительный профиль настроек, на котором мы и будем включать расписание.

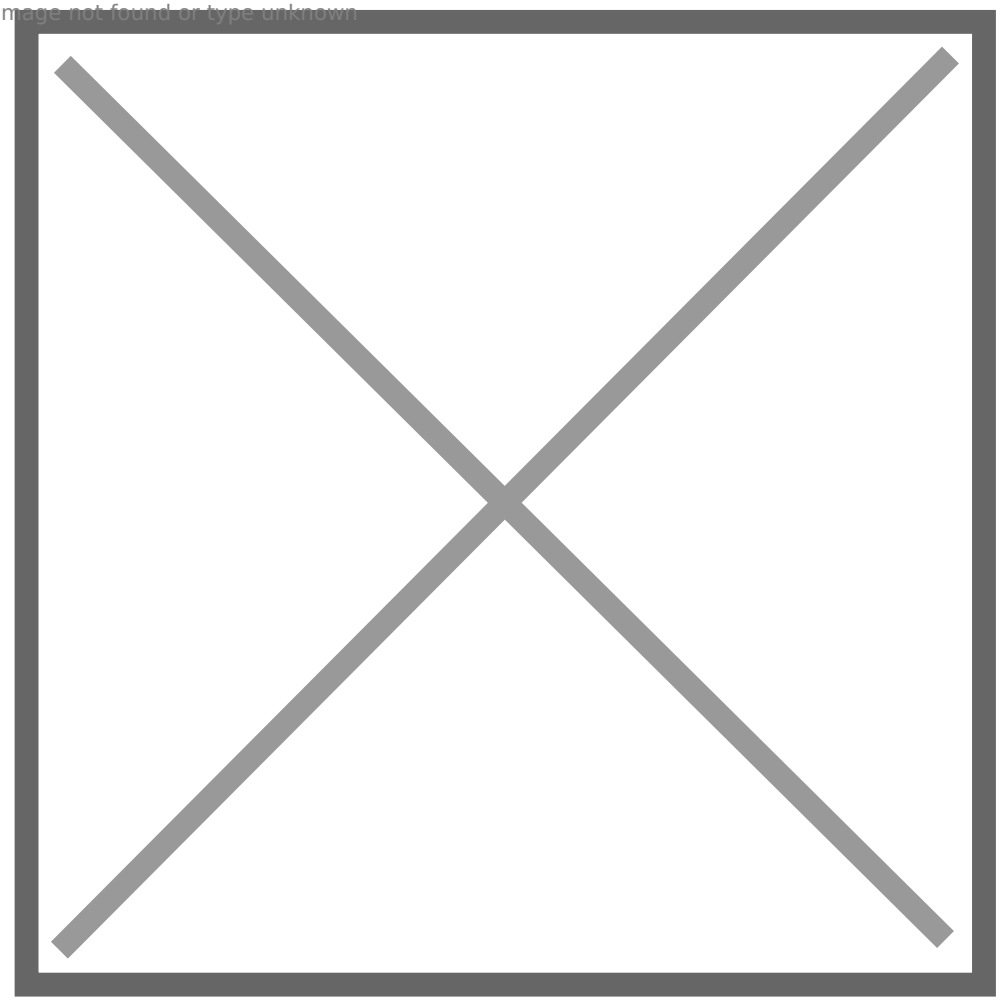
1. Войдите в личный кабинет
2. Войдите в раздел **Настройки** - **Профили**
3. Введите название профиля (например, Блокировка) и нажмите **Добавить**.

После создания профиля можно приступать к настройке расписания.

1. Войдите в раздел **Настройки** - **Расписание**
2. В списке профилей (в левом верхнем углу) выберите только что созданный профиль Блокировка для настройки расписания. Заметьте, что профиль Основной в списке не отображается, поскольку для него отдельно расписание не настраивается.
3. Установите нужное время, в которое должен быть активен профиль Блокировка. В остальное время будет активен профиль Основной.

4. Поставьте галочку в чек-боксе **Расписание включено** по расписанию для этого профиля.
5. Нажмите кнопку **Сохранить**.

Image not found or type unknown



После настройки расписания необходимо выполнить действия, чтобы это расписание применялось к вашей сети или отдельным компьютерам.

Если вы используете программу агент, то вам необходимо войти в программу и выбрать созданный профиль Блокировка и установить его как используемый по умолчанию. Сделать это можно в разделе **Настройки** - **Настройки контент-фильтрации**, выбрав требуемый профиль в списке профилей и нажав кнопку **Применить**.

Если вы использовали скрытую установку агента по компьютерам в корпоративной сети, то вам потребуется заново запустить установку с ключом, в котором передать название профиля с расписанием.

Если у вас настроена фильтрация на уровне роутера, прокси-сервера или шлюза, то вам необходимо произвести привязку вашего внешнего адреса на профиль с расписанием.

1. Войдите в раздел **Настройки** - **Устройства**
2. Отвяжите внешний IP-адрес вашей сети от профиля Основной

3. Привяжите этот же IP-адрес на профиль с расписанием (Блокировка)

Если ваш внешний IP-адрес динамический и вы используете сторонний сервис динамического DNS то вместо IP-адреса вы должны привязать динамический хост. После применения всех настроек расписание начнет работу.

Вы можете иметь несколько профилей с разными расписаниями для разных пользователей и сетей, но обратите внимание, что переключение всегда будет между текущим профилем и профилем Основной.

Возможные проблемы при настройке расписания

Расписание переключает настройки в неправильное время.

Проверьте, что у вас правильно выставлена временная зона. Войдите в раздел **Аккаунт** - **Персональные данные**, выберите правильную временную зону и нажмите **Сохранить**.

Расписание работает, но блокировка и разблокировка происходят с задержкой.

Из-за кэширования DNS запросов на системном уровне и в браузере ваш компьютер может не сразу отреагировать на выданную нашей системой блокировку или разблокировку. Чтобы исключить это, мы рекомендуем отключать автоматическое управление кэшем браузера.

Расписание совсем не работает.

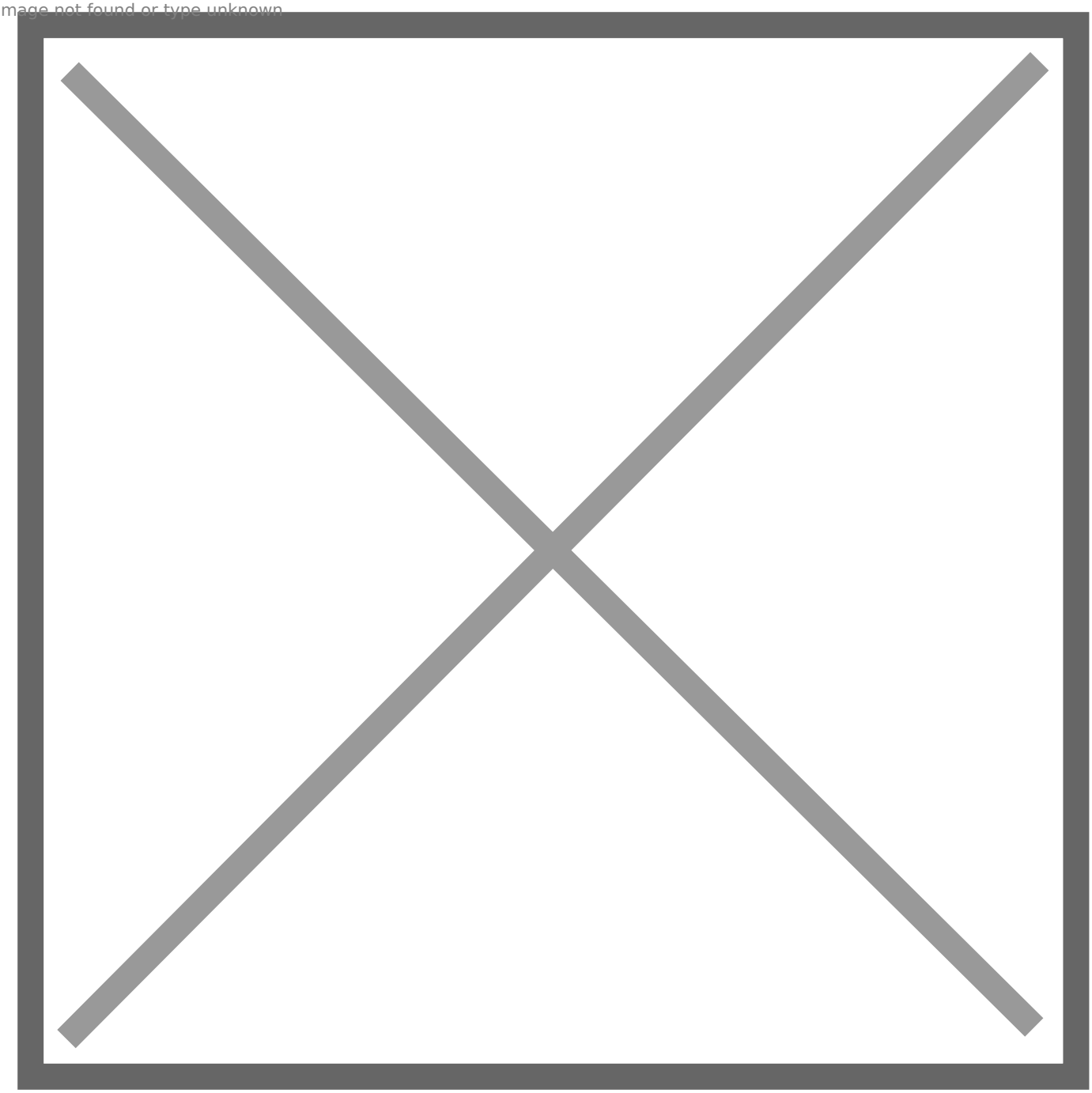
Проверьте, что вы правильно выполнили описанные выше шаги по настройке расписания.

Если все сделано правильно и проблема сохраняется, обратитесь в техническую поддержку.

Настройка разрешающих и запрещающих списков

Для создания разрешающий и запрещающих списков необходимо перейти в раздел **Списки**. Далее необходимо ввести имя списка и выбрать профили, к которым он будет применен, и нажать кнопку **Добавить**.

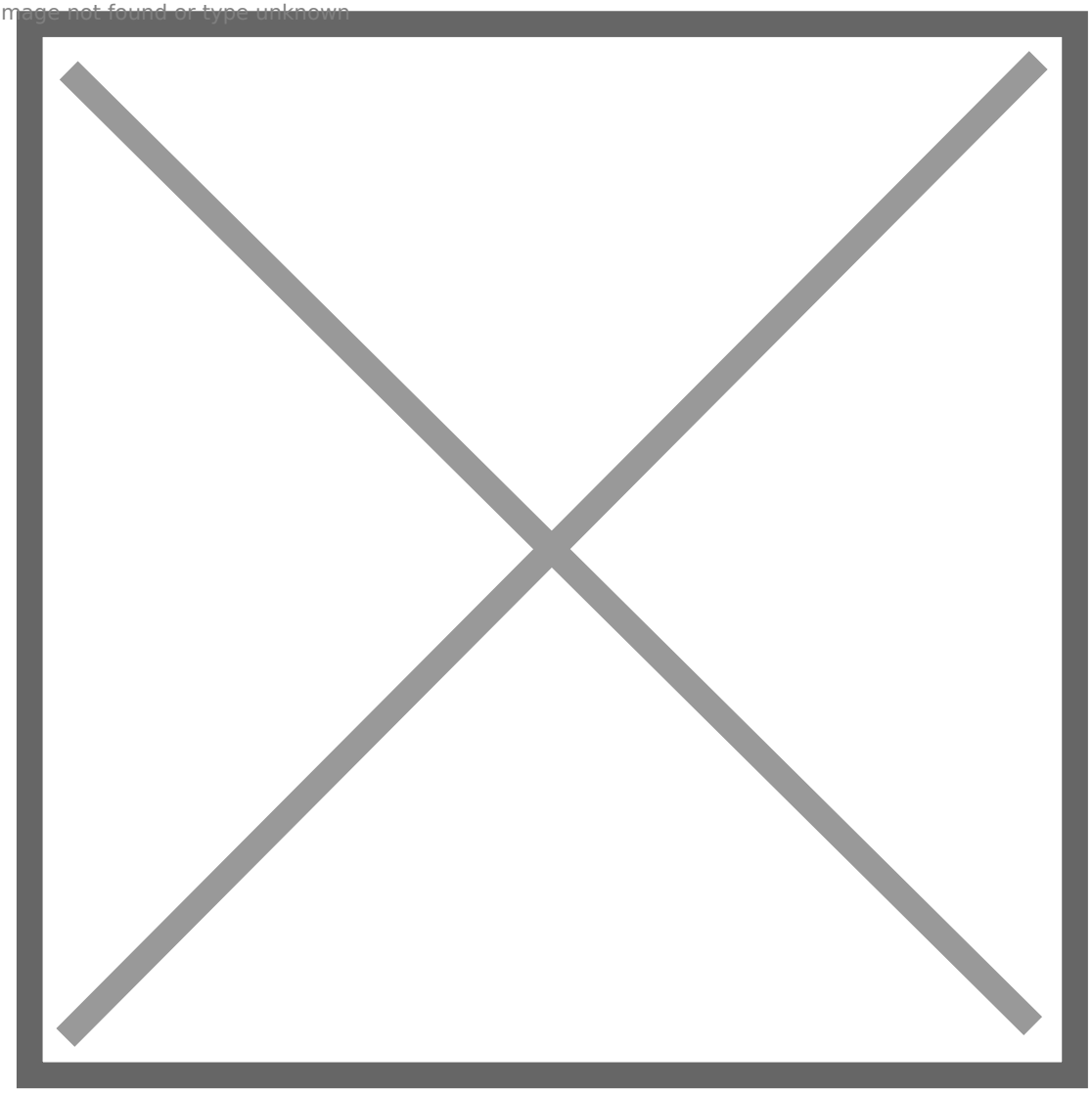
Image not found or type unknown



После создания списка можно добавить в него необходимые домены, введя доменное имя и нажав кнопку **Добавить**.

Редактируя уже созданный список можно изменить его имя или профили к которым он будет применен.

Image not found or type unknown



При необходимости к домену можно добавить комментарий.
Доменное имя нужно вводить без https:// или www.

Функция **Редактировать списком** недоступна на тарифах **Домашний** и **Домашний+**

Создание и управление дополнительными страницами блокировки

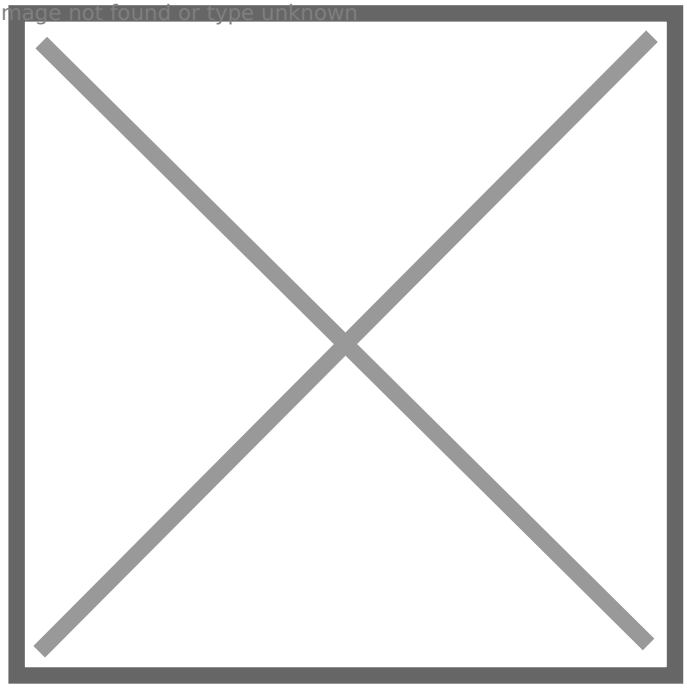
В данной инструкции дано пошаговое описание создания и управления дополнительными страницами блокировки.

Для создания дополнительной страницы блокировки необходимо:

1. Перейти в **Настройки** - **Дополнительно**.
2. В блоке **Страница блокировки** введите название страницы блокировки.
3. Введите текст, который будет отображаться на странице блокировки.
4. Нажмите кнопку **Добавить**.

> При необходимости добавьте изображение для его отображения на странице блокировки

Image not found or type unknown

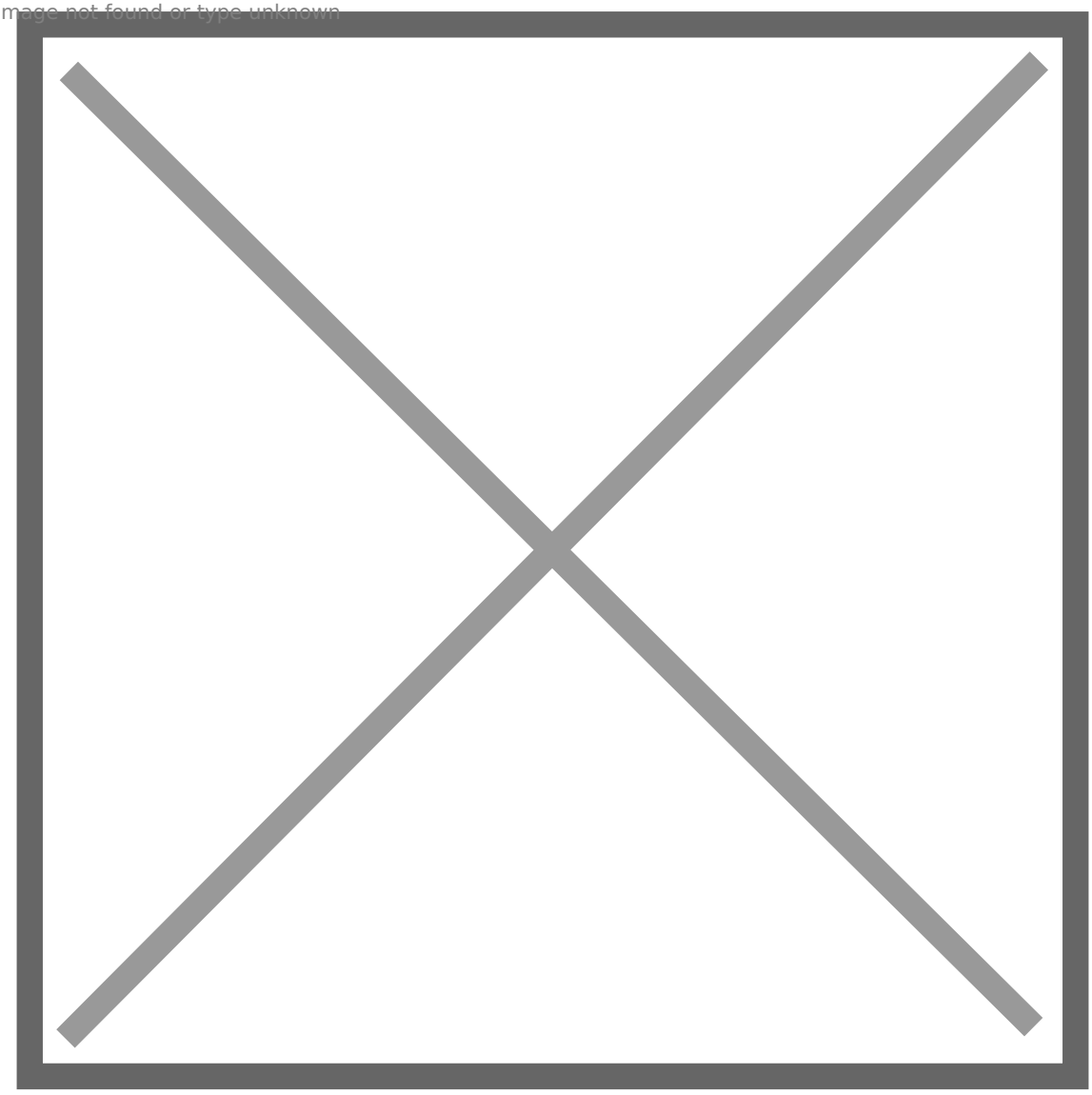


Для применения страницы блокировки к существующему профилю необходимо:

1. Перейти в **Настройки** - **Профили.**

2. Нажать кнопку редактирования справа от профиля.
3. Нажать на выпадающий список и выбрать созданную ранее страницу.
4. Нажать на копку применения изменений справа от профиля.

Image not found or type unknown



Установка корневого сертификата SkyDNS

Корневой сертификат или **сертификат SSL** - одна из частей системы безопасности сайтов. Сертификат SSL необходим для корректной работы сайтов с безопасным соединением (https). Если у Вас возникают проблемы с отображением страницы блокировки SkyDNS (браузер выдает сообщение **Не удается получить доступ к сайту**), то Вам необходимо скачать сертификат SkyDNS и настроить его использование в Вашем браузере.

Скачать корневой сертификат SkyDNS

Если при нажатии кнопки браузер открывает окно установки сертификата, отмените установку, кликните по кнопке правой клавишей мыши и выберите пункт **Сохранить объект как...**
Чтобы проверить работу страницы блокировки в https воспользуйтесь следующей инструкцией в конце статьи.

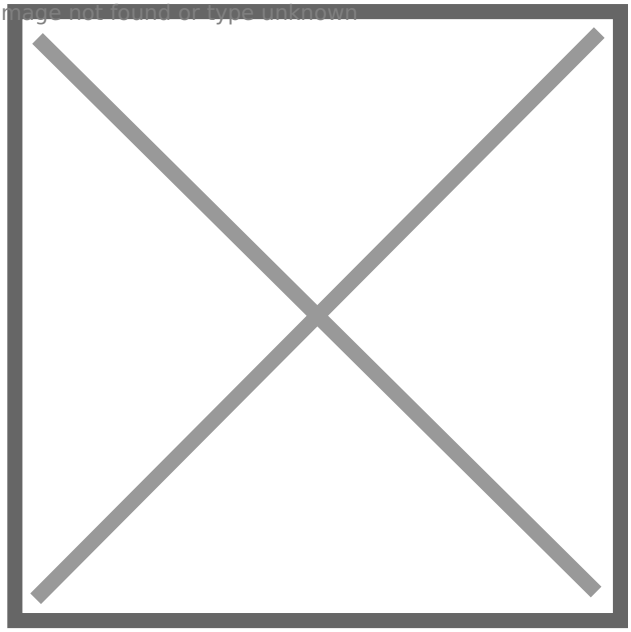
Сертификат не поддерживается в Yandex браузере.
Браузер Mozilla Firefox не использует системные настройки, для установки сертификата воспользуйтесь инструкцией ниже.

Установка сертификата SkyDNS для Windows (браузеры Internet Explorer, Edge, Opera, Google Chrome)

Установка сертификата для браузеров **Internet Explorer, Edge, Opera, Google Chrome** производится через системные настройки.

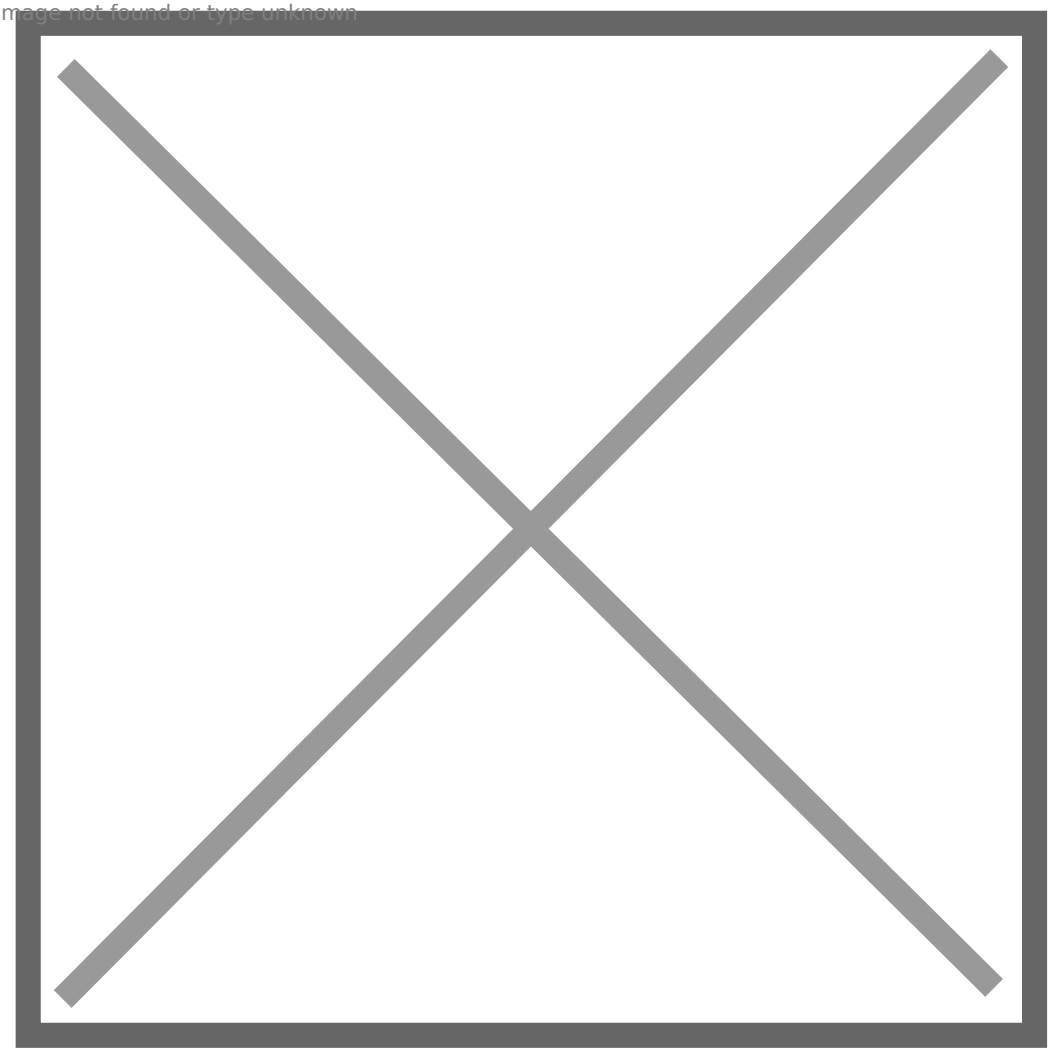
1. Нажмите кнопку **Пуск** и начните вводить словосочетание **Панель управления**. Когда появится иконка Панели Управления нажмите на нее.

Image not found or type unknown



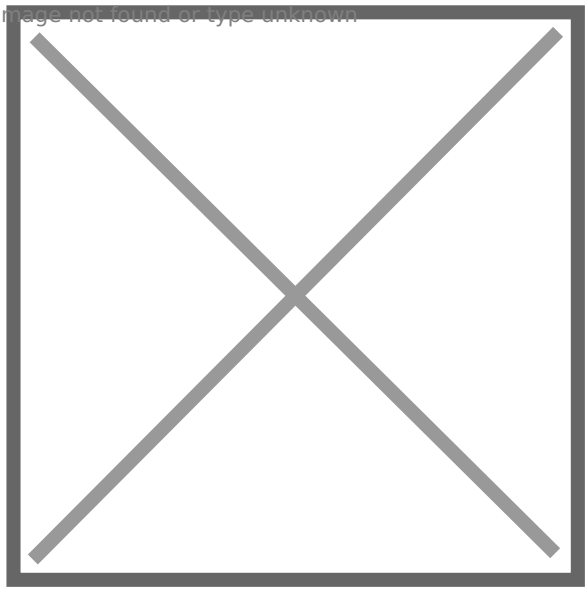
2. В поиске панели управления введите **Свойства браузера** и нажмите появившуюся иконку.

Image not found or type unknown



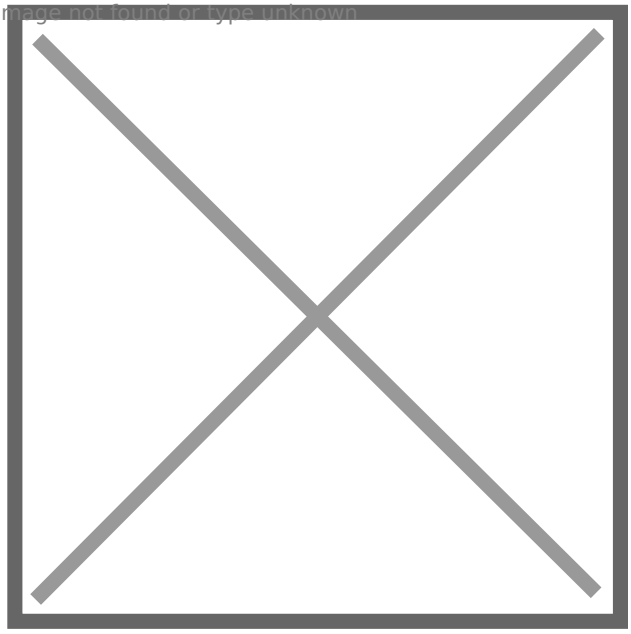
3. В Свойствах браузера перейдите на вкладку **Содержание** и нажмите кнопку **Сертификаты**.

Image not found or type unknown



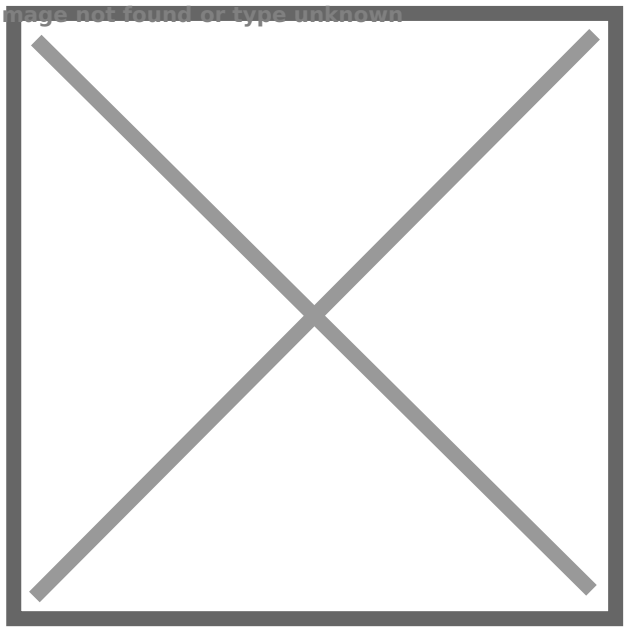
4. В окне Сертификаты перейдите на вкладку **Доверенные корневые центры сертификации** и нажмите кнопку **Импорт**.

Image not found or type unknown



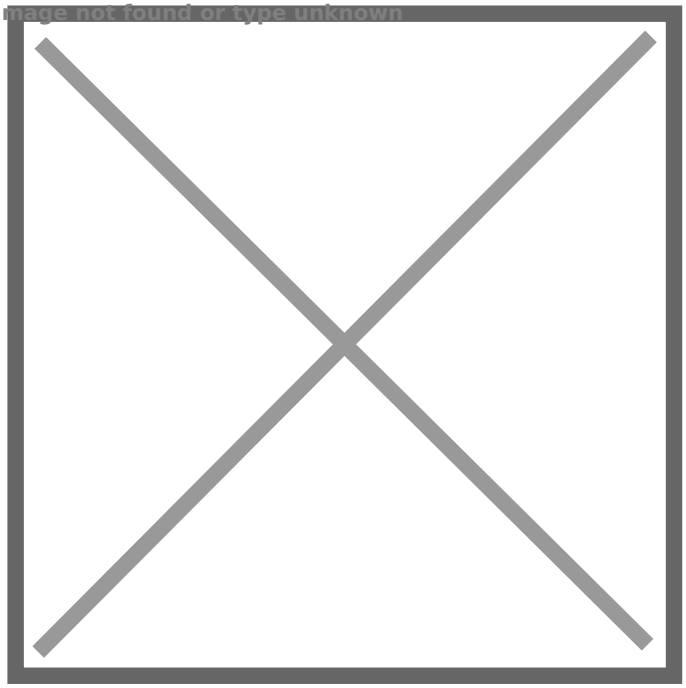
5. В окне мастера импорта сертификатов на первом шаге нажмите кнопку **Далее**.

Image not found or type unknown



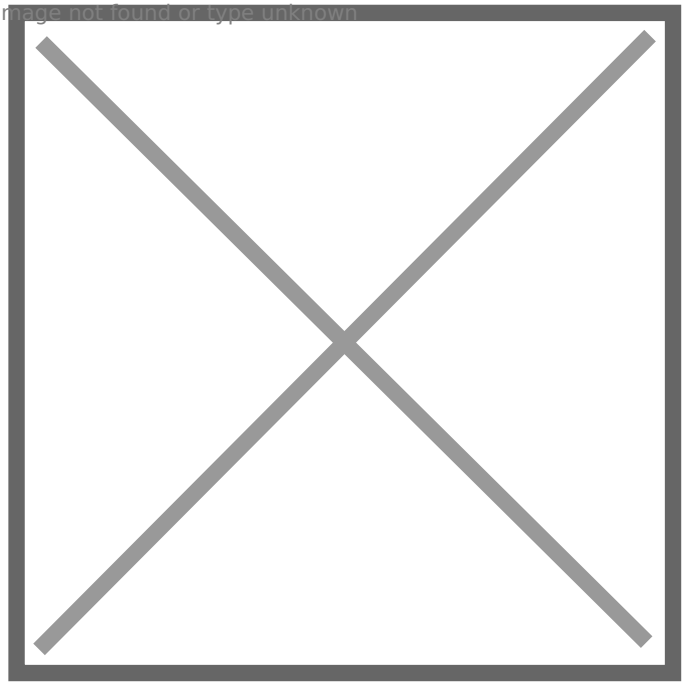
6. На втором шаге нажмите кнопку **Обзор** и выберите заранее загруженный файл сертификата SkyDNS.

Image not found or type unknown



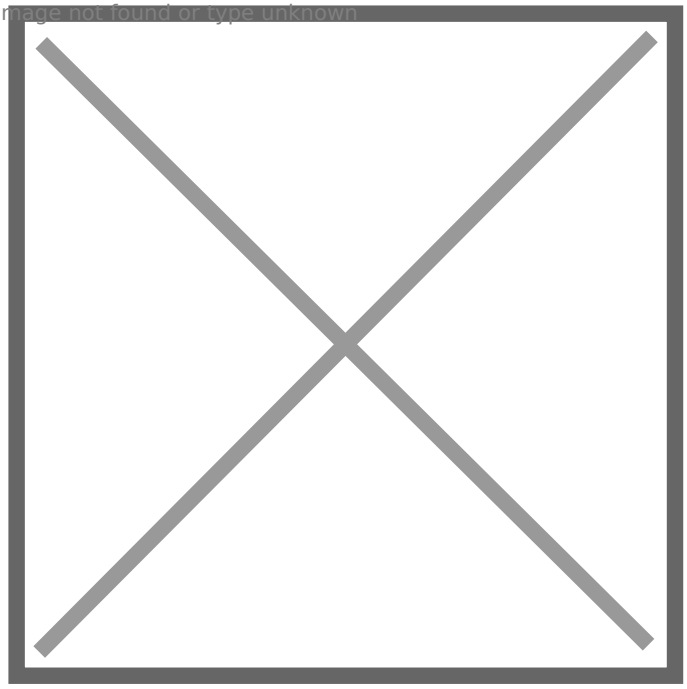
7. На третьем шаге убедитесь, что сертификат помещается в хранилище **Доверенных корневых центров сертификации.**

Image not found or type unknown



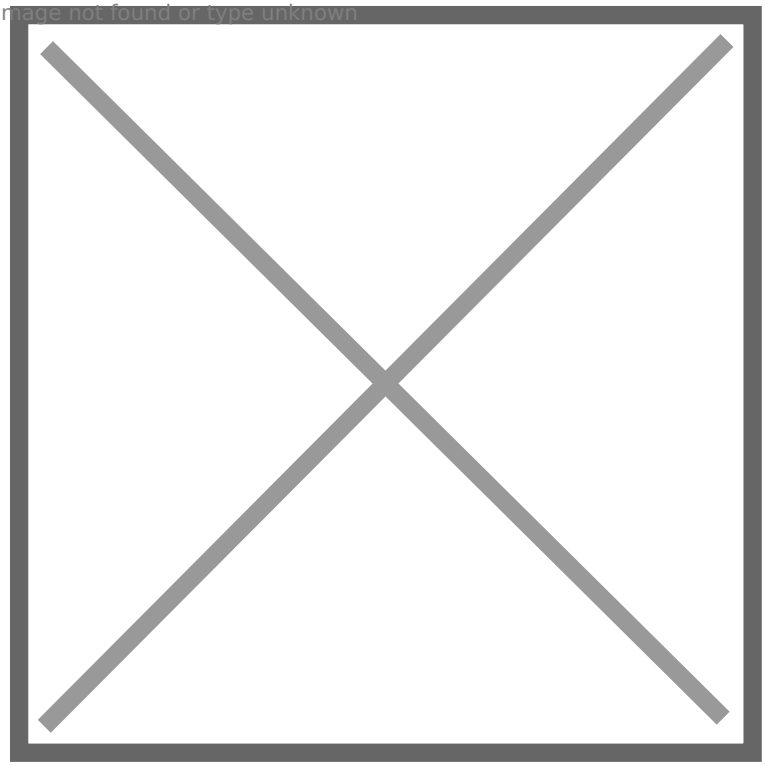
8. Подтвердите ранее проделанные действия, нажав на кнопку **Готово**.

Image not found or type unknown



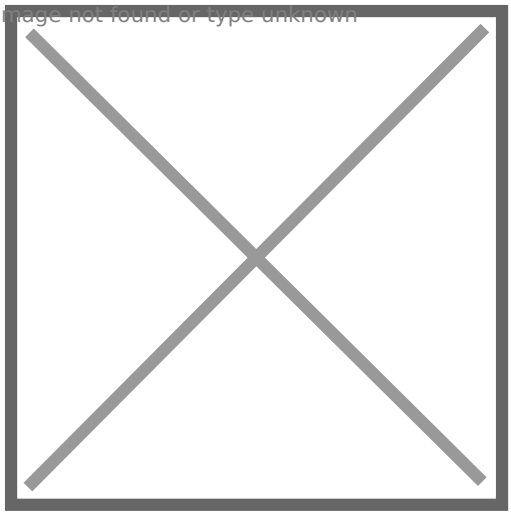
9. На вопрос системы нужно ответить **Да**.

Image not found or type unknown



10. Закрыть мастер импорта сертификатов, нажав **Ок**.

Image not found or type unknown

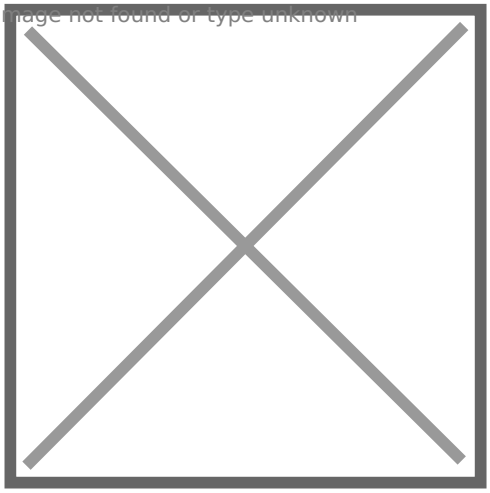


Установка сертификата SkyDNS в браузере Mozilla Firefox для всех платформ

Браузер Mozilla Firefox не использует системные настройки, поэтому установка сертификата в нем отличается от других браузеров.

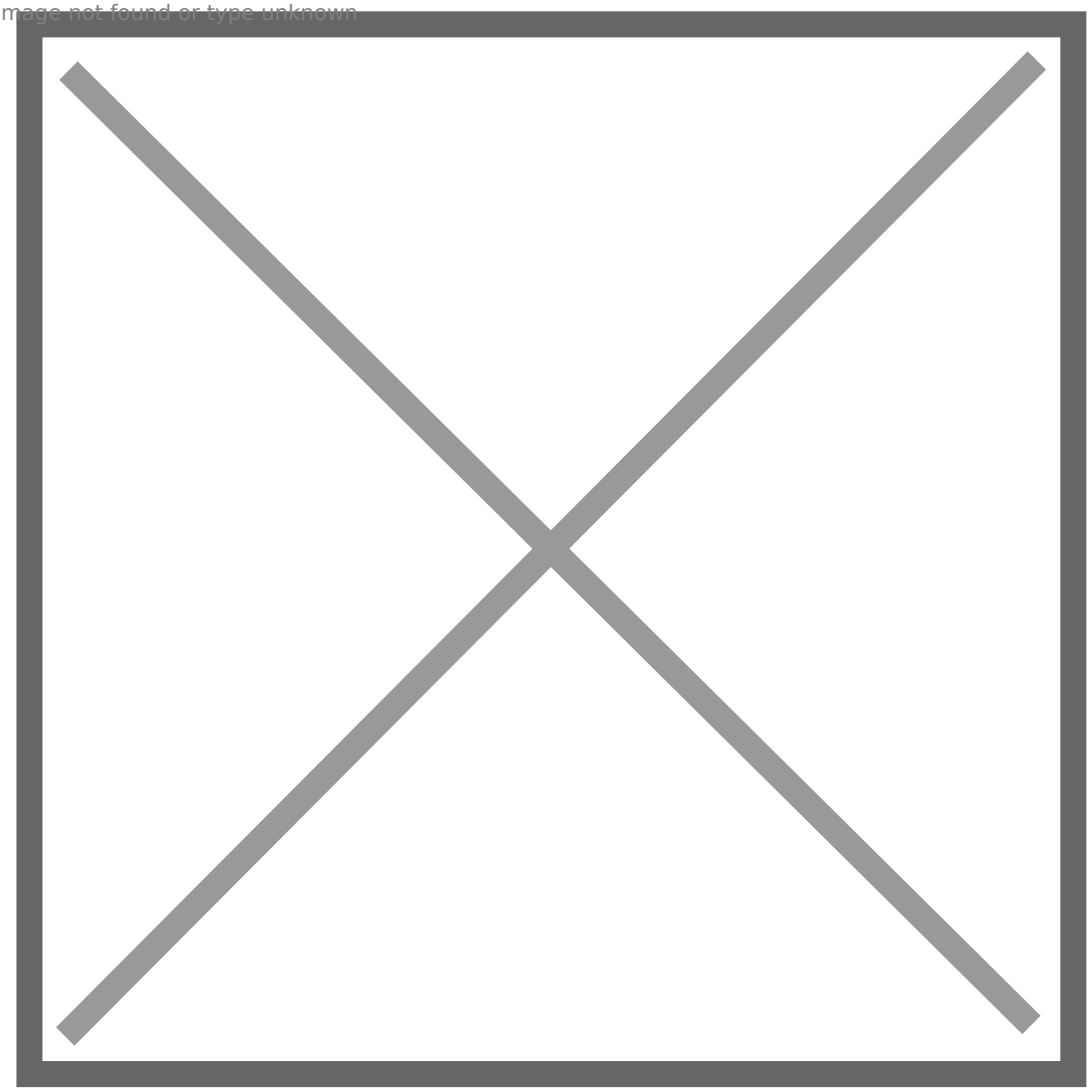
1. Щелкните по иконке настроек в правом верхнем углу браузера и выберите пункт меню **Настройки**.

Image not found or type unknown



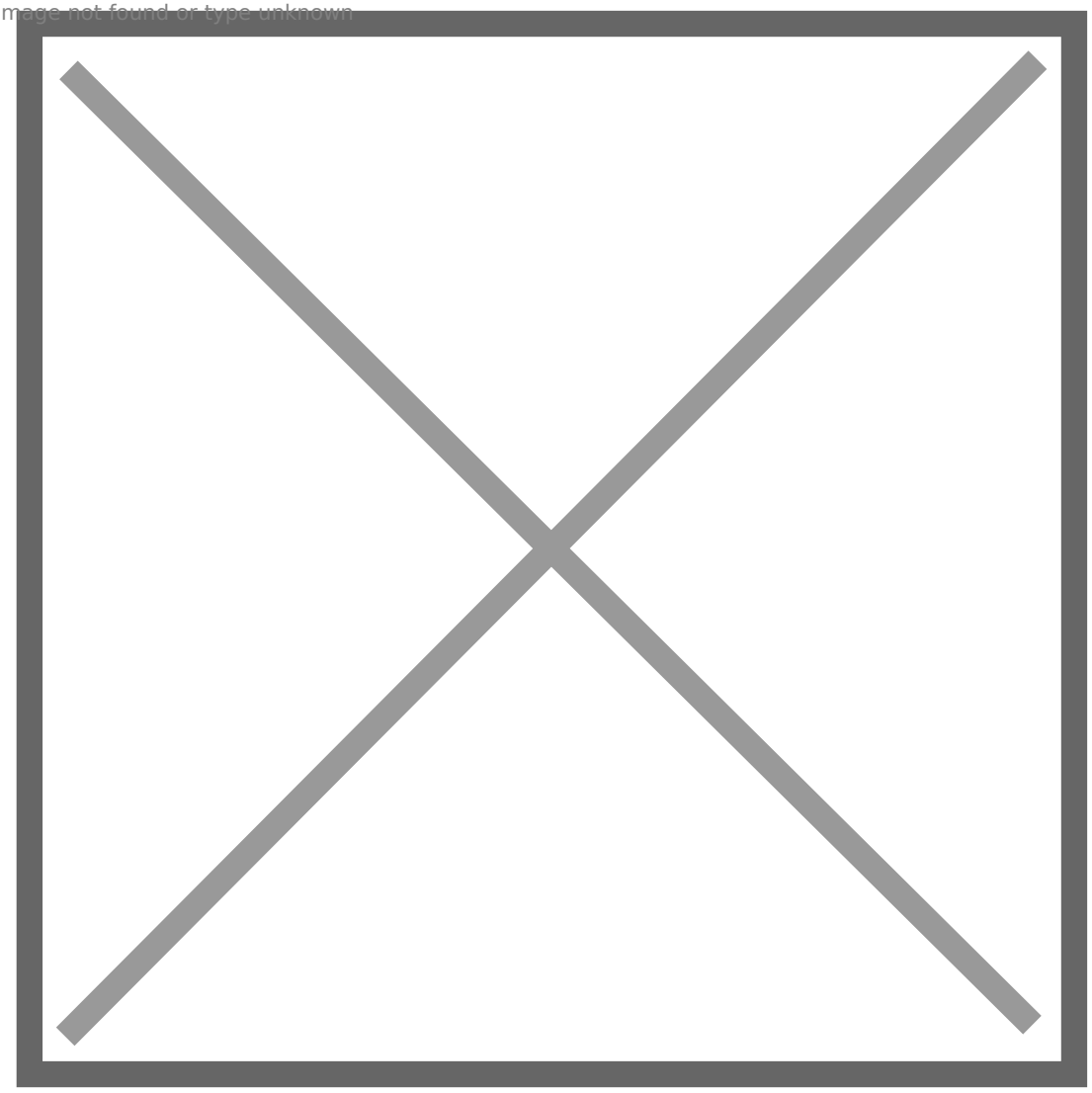
2. В левом меню выберите **Приватность и защита** затем прокрутите в самый низ страницы и нажмите кнопку **Просмотр сертификатов**.

Image not found or type unknown



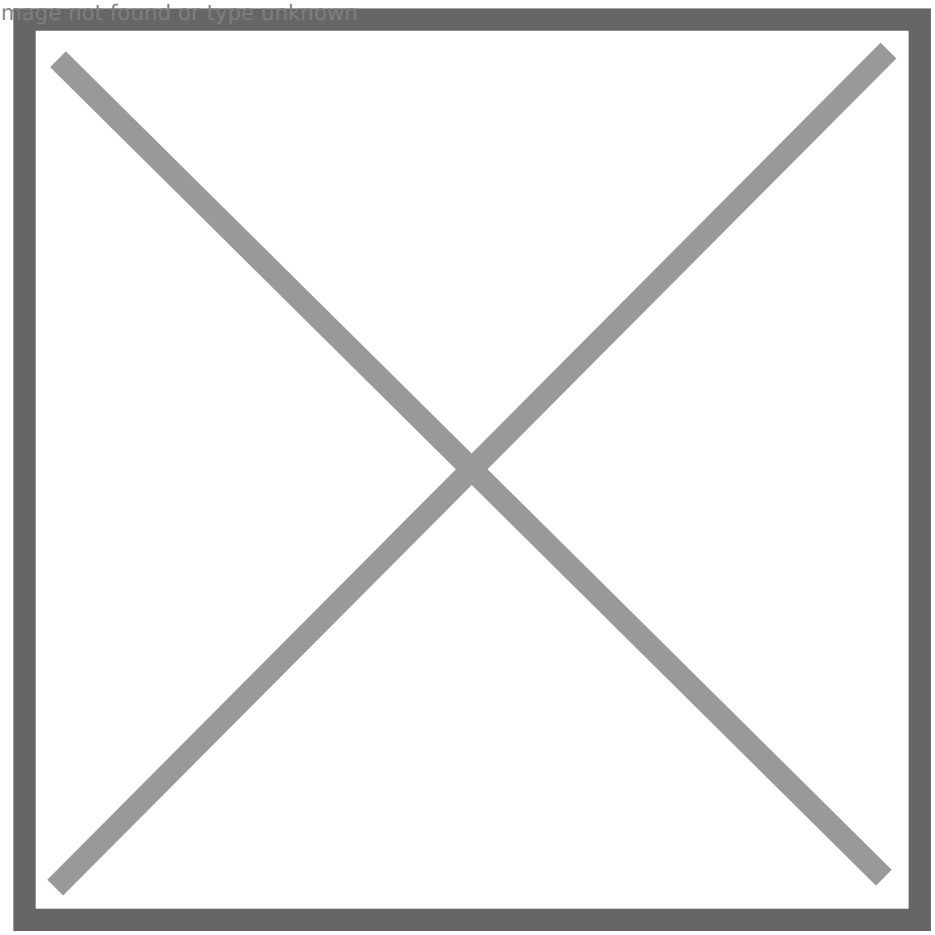
3. В окне Сертификатов выберите вкладку **Центры сертификации** и нажмите кнопку **Импортировать**.

Image not found or type unknown



4. Выберите заранее загруженный сертификат SkyDNS. В окне загрузки сертификата установите галочку **Доверять при идентификации веб-сайтов** и нажмите кнопку **OK**.

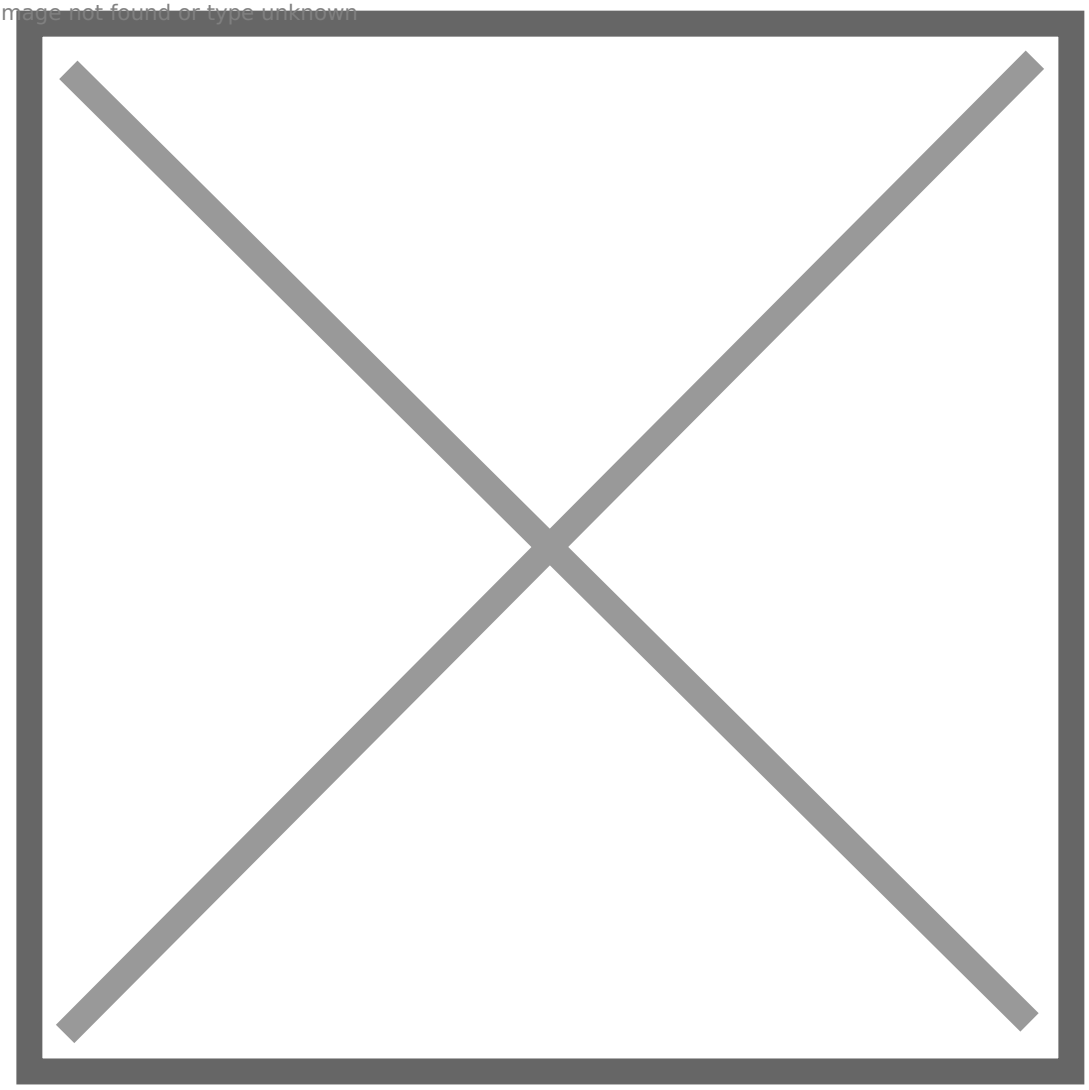
Image not found or type unknown



Установка сертификата SkyDNS в Mac OSX

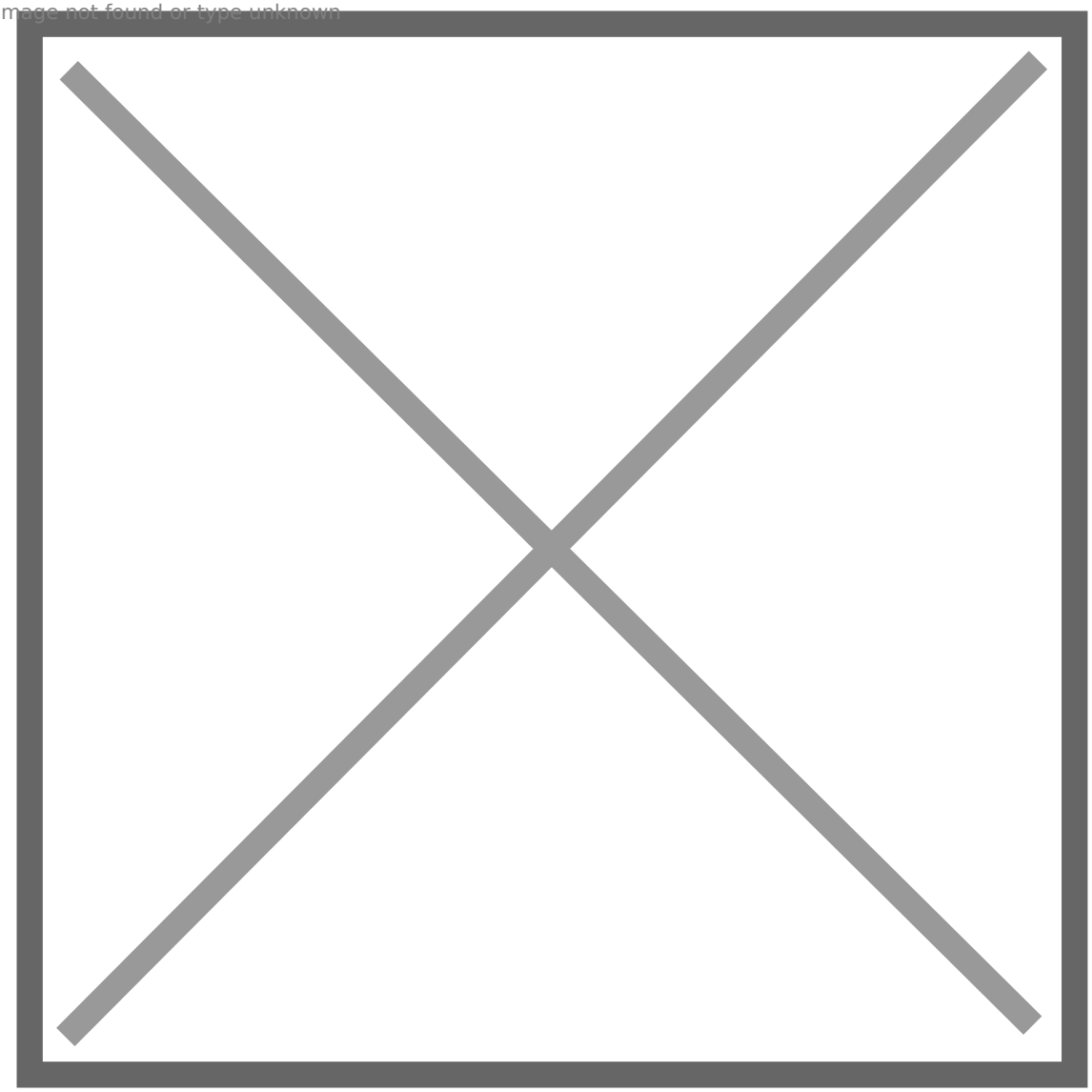
1. Нажмите сочетание клавиш **CTRL+SPACE** и в поиске Spotlight введите **Связка ключей**. Откройте приложение Связка ключей.

Image not found or type unknown



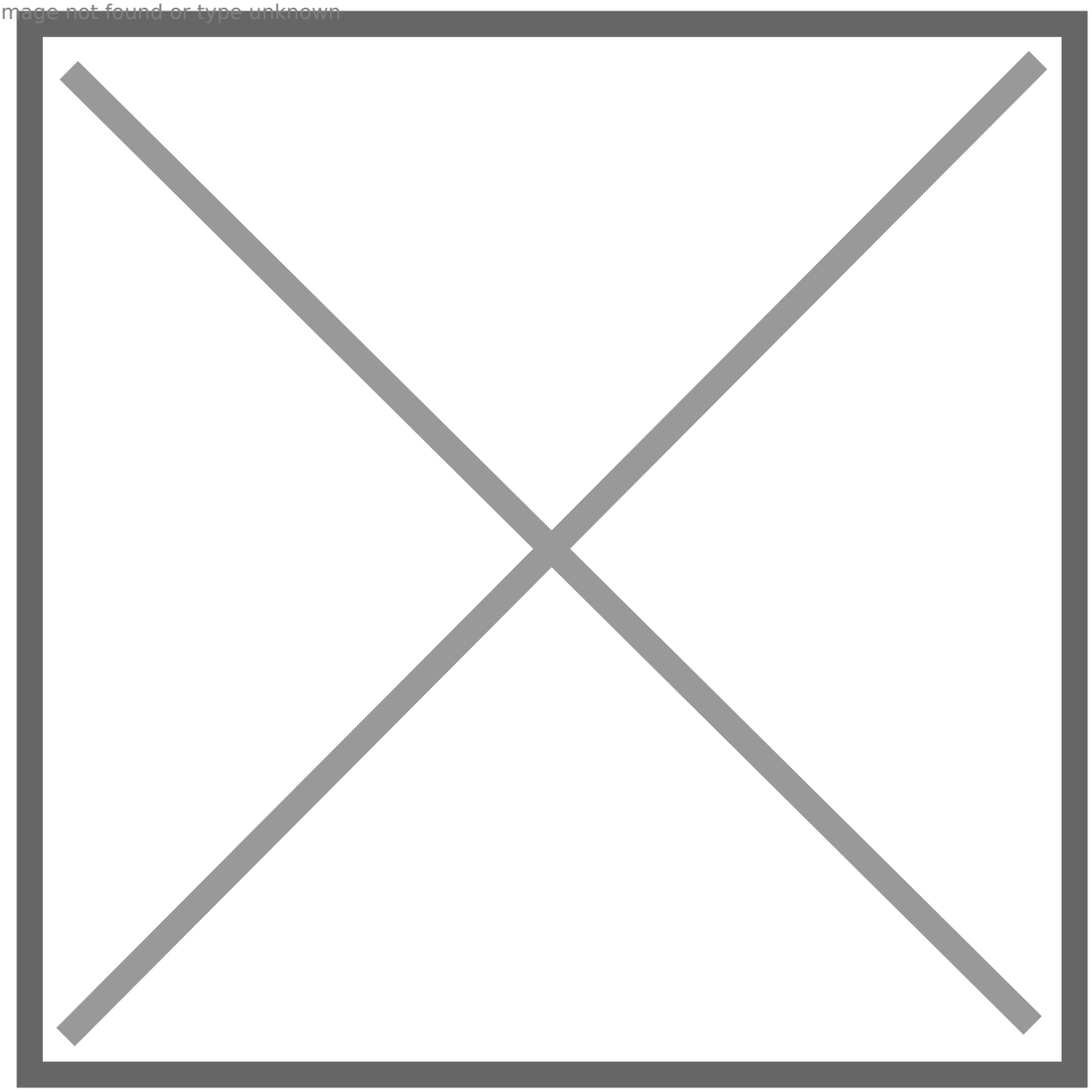
2. В приложении Связка ключей выберите параметр **Вход** и категорию **Сертификаты**.

Image not found or type unknown



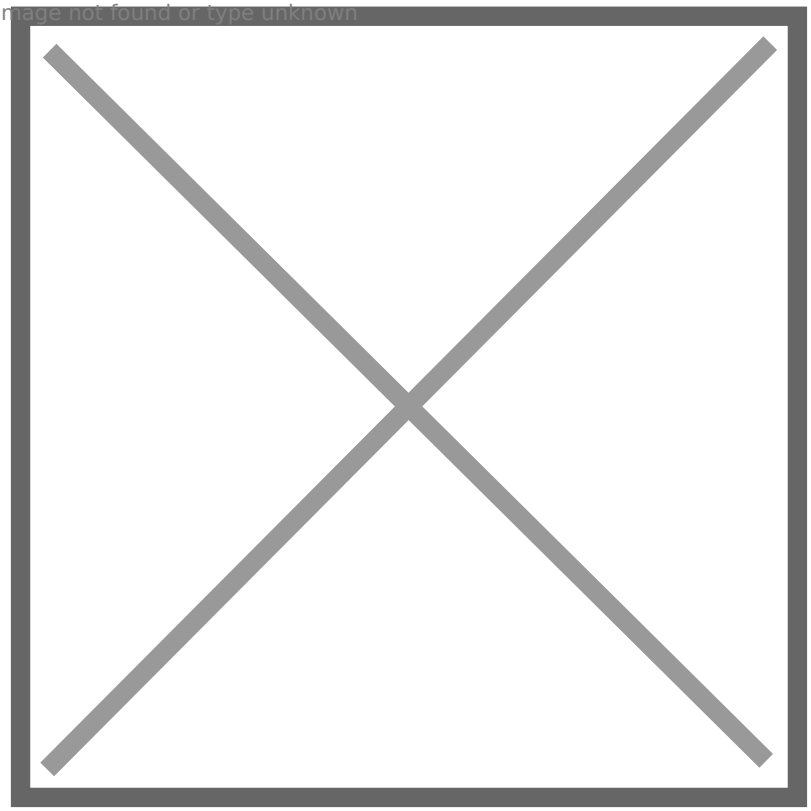
3. Перетащите заранее загруженный сертификат SkyDNS в правую часть окна приложения Связка ключей, где хранятся остальные сертификаты.

Image not found or type unknown



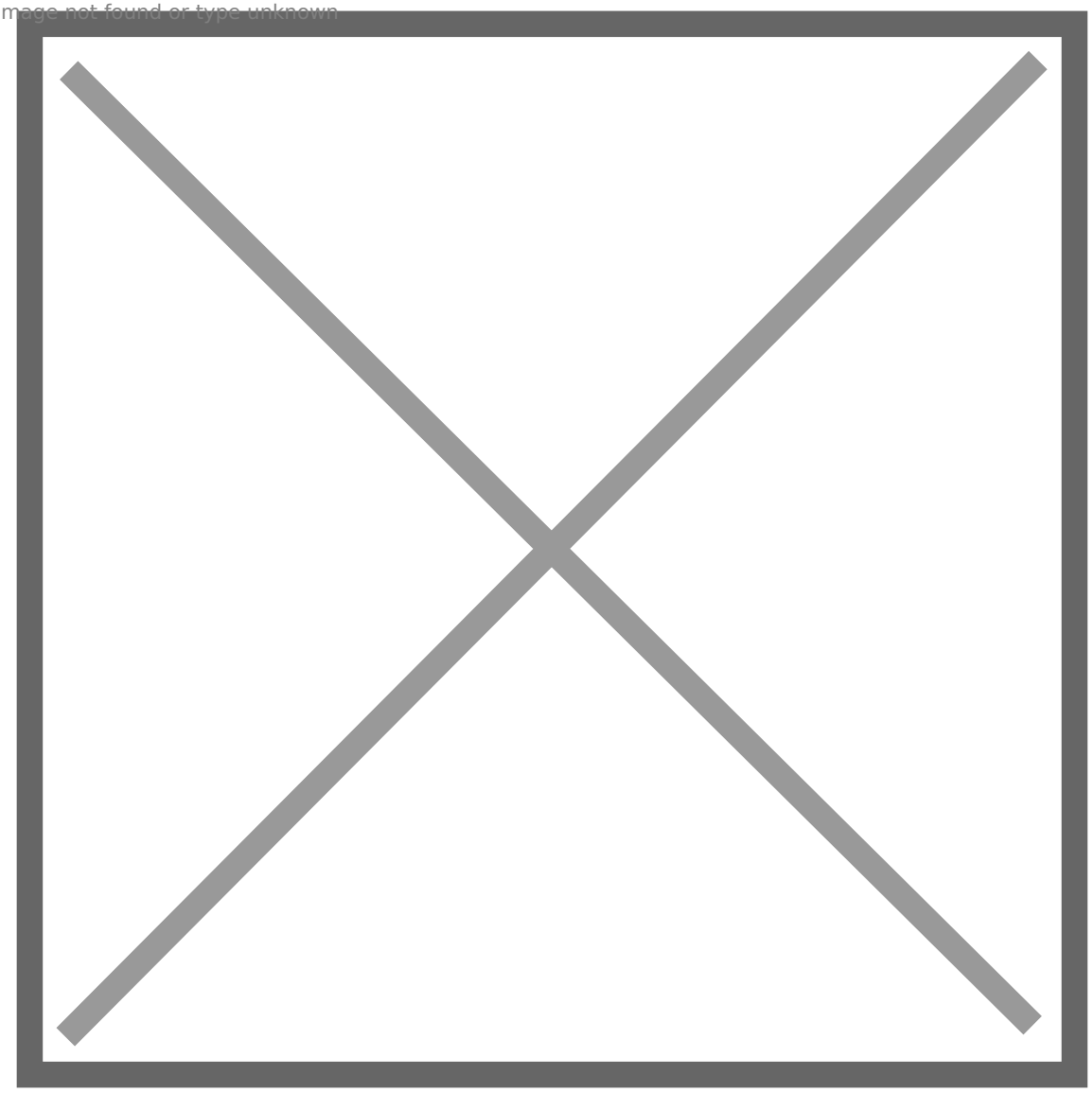
4. Щелкните правой кнопкой мыши по сертификату SkyDNS и выберите пункт меню **Свойства сертификата**. В открывшемся окне разверните пункт **Доверие** и в **Параметрах использования сертификата** выберите **Всегда доверять**. Закройте окно сертификата.

Image not found or type unknown



5. В приложении Связка ключей убедитесь, что сертификат SkyDNS помечен как надежный для данной учетной записи.

Image not found or type unknown



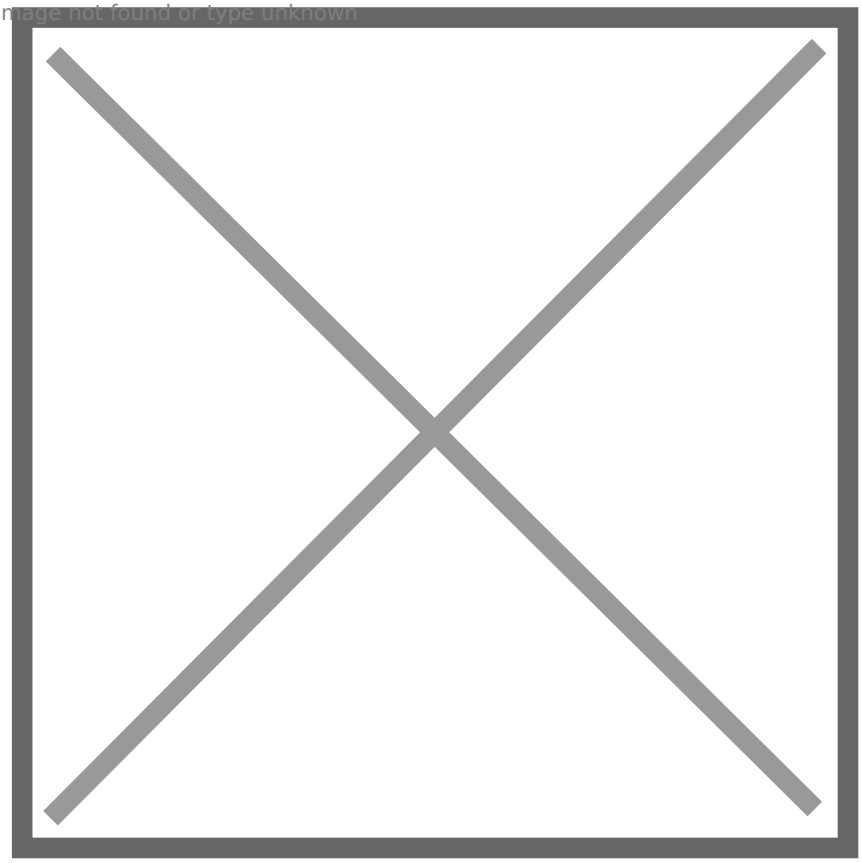
Установка корневого сертификата SkyDNS на устройства под управлением OS Android и iOS

Установка сертификата SkyDNS в Android:

1. Скачать сертификат. После скачивания автоматически откроется окно добавления сертификата.

2. Ввести название сертификата, в поле "**Использовать аккаунт**" выбрать "**VPN и приложения**". Нажать "**OK**".

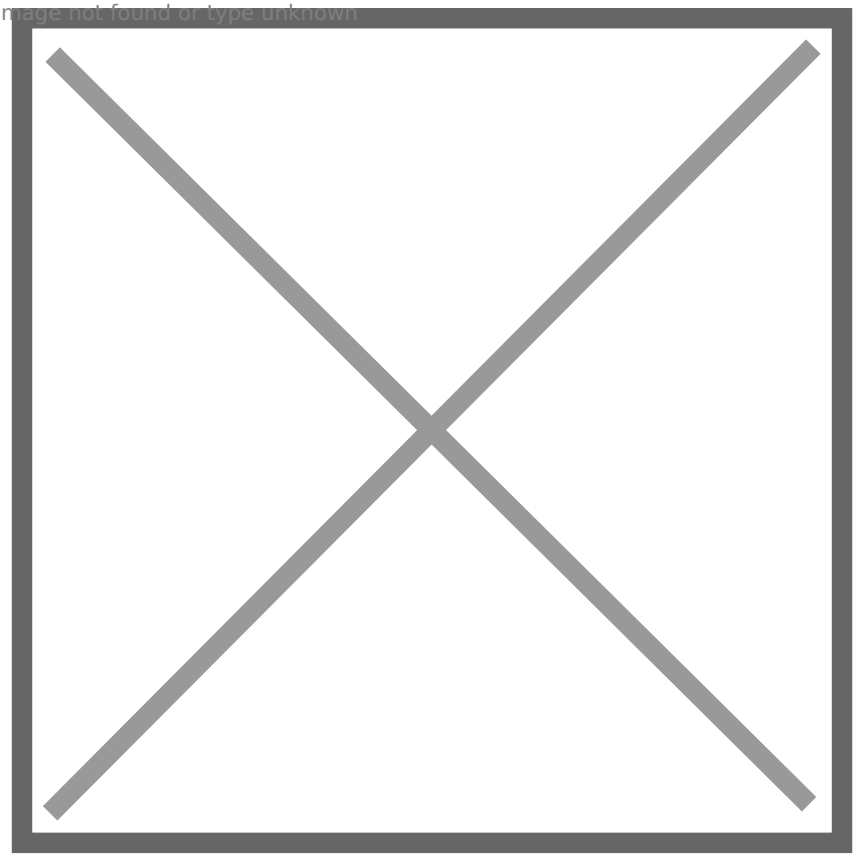
Image not found or type unknown



Установка сертификата SkyDNS в iOS:

1. Скачать сертификат на устройство. Открыть скачанный файл.

Image not found or type unknown



2. Нажать **Установить** в открывшемся окне установки сертификата, затем в появившемся предупреждении, затем в окне установки профиля.

Image not found or type unknown

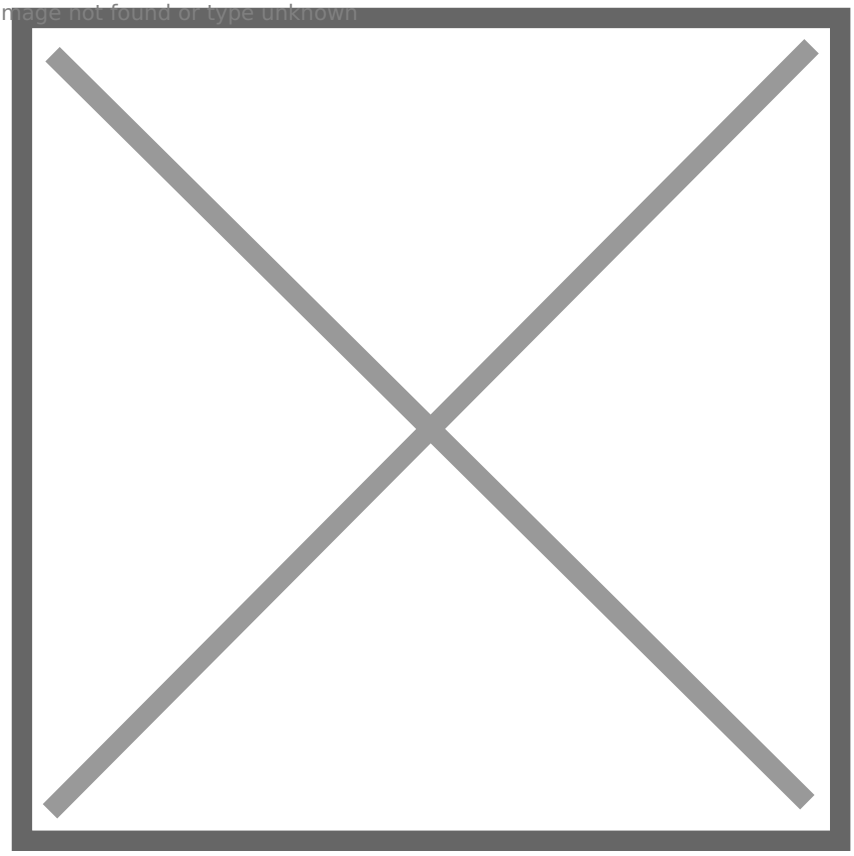
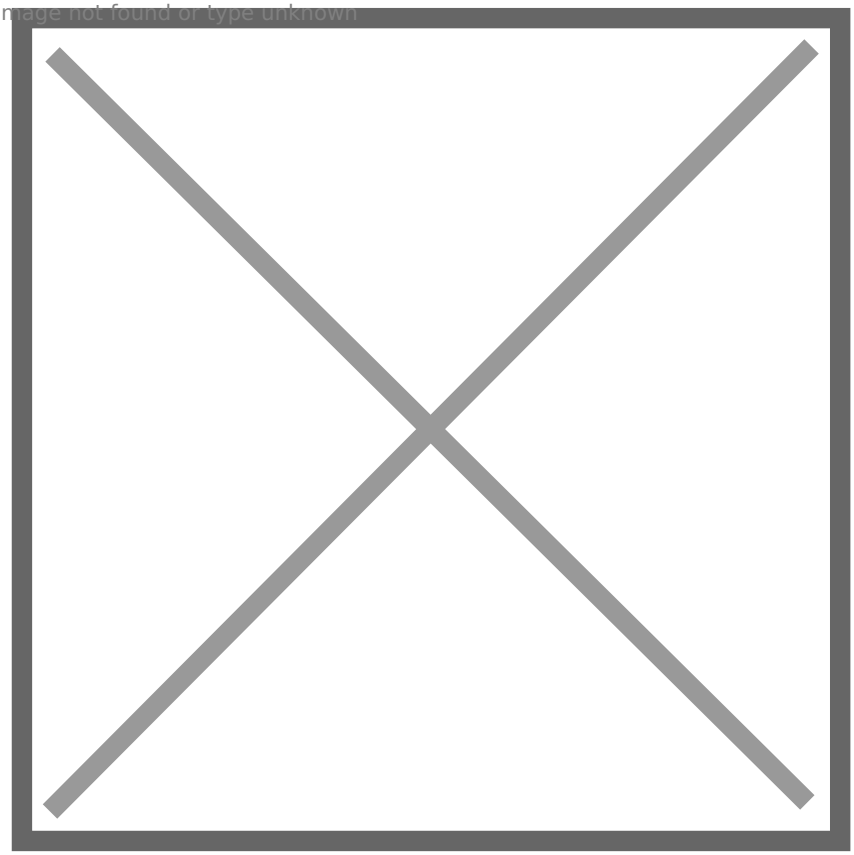
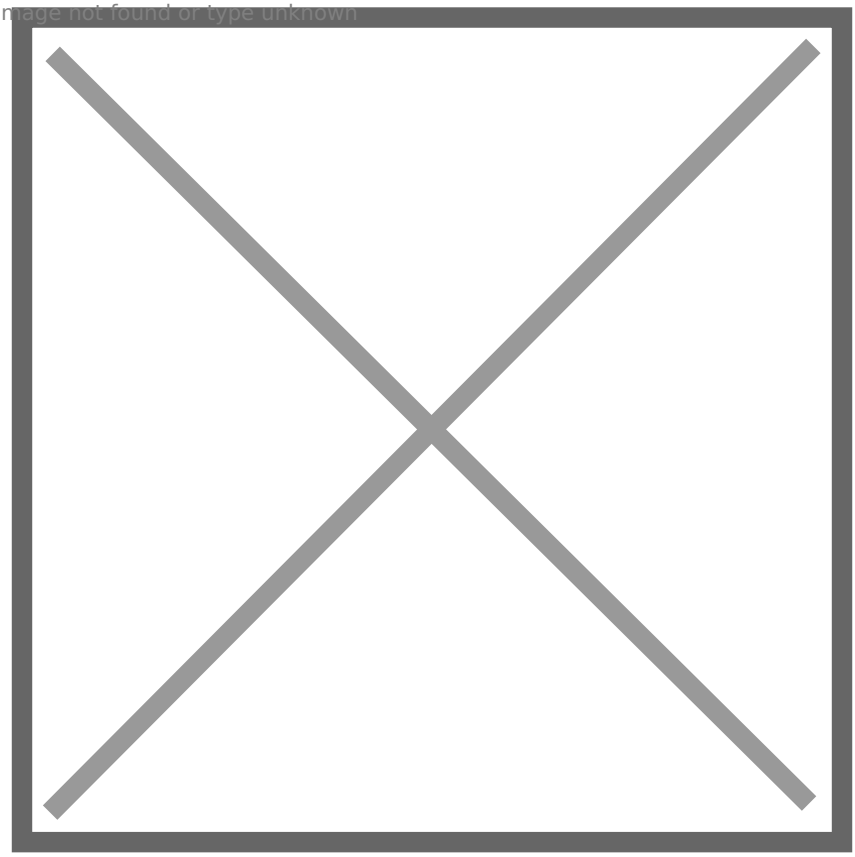


Image not found or type unknown



3. Нажать **Готово** для завершения установки.

Image not found or type unknown



4. Перейти в Настройки - Об этом устройстве - Управление сертификатами. Включить переключатель **Доверять сертификату**.

Image not found or type unknown

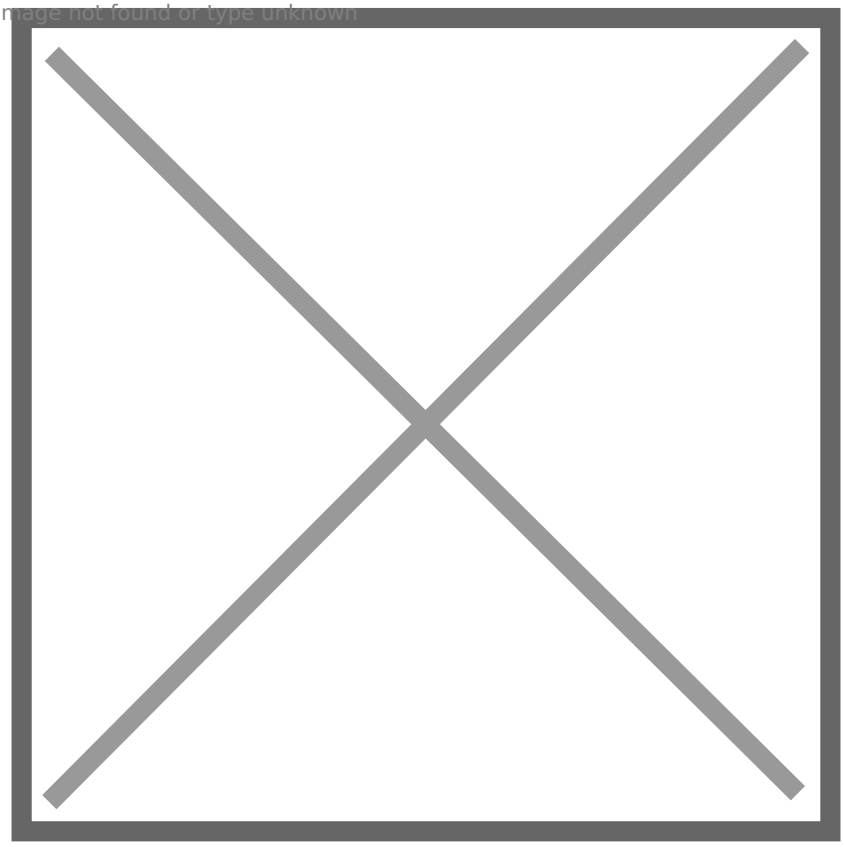


Image not found or type unknown

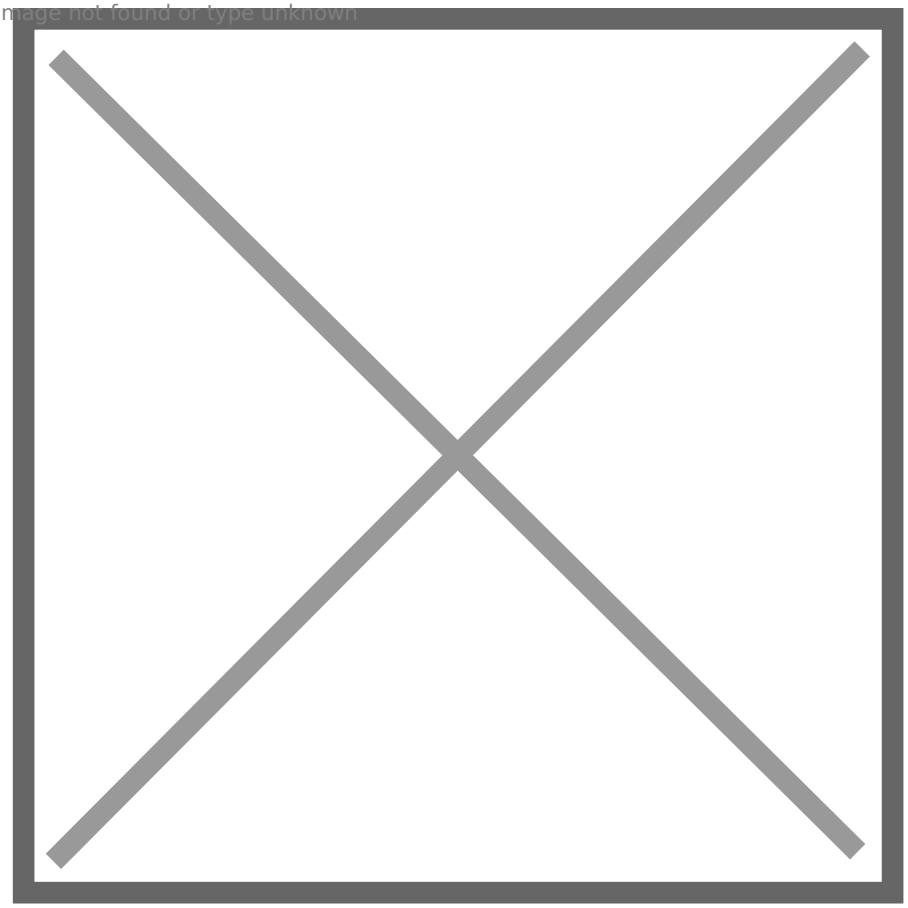
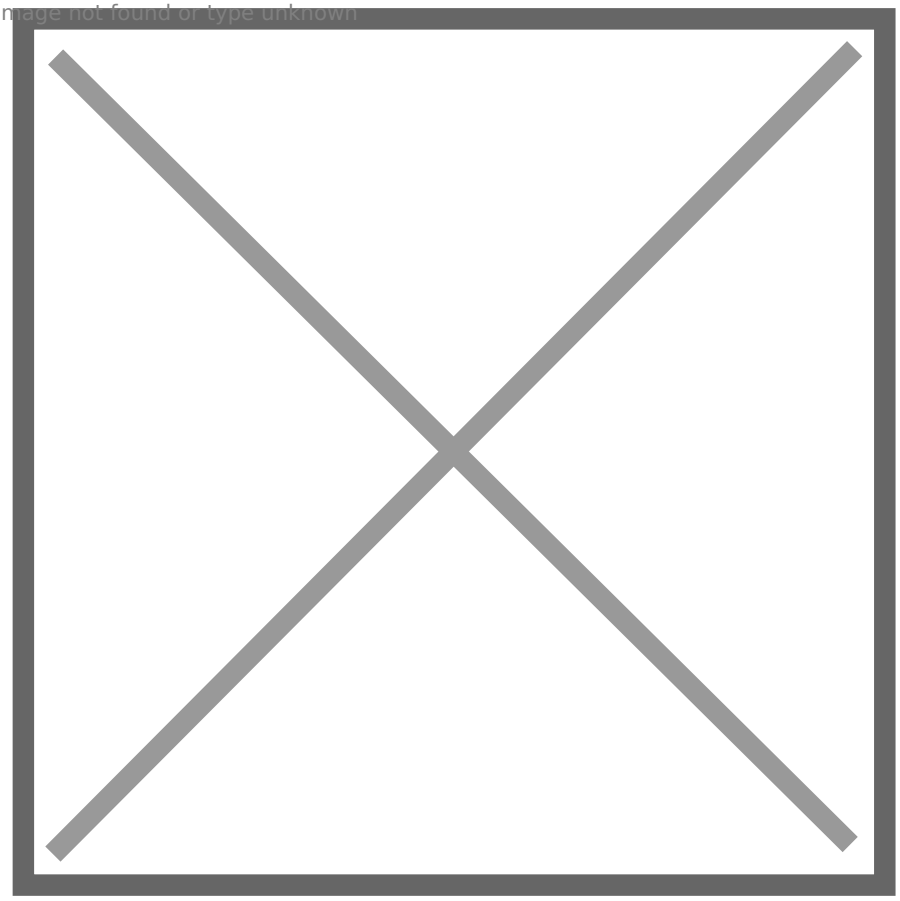


Image not found or type unknown



Ручная установка сертификата с помощью консоли

Установка сводится к двум шагам:

1. Скопировать файл с сертификатом в определенный каталог.
2. Запустить команду для импорта сертификата.

Для Deb (Debian / Ubuntu / Astra Linux)

Копируем файл в каталог **/usr/local/share/ca-certificates**:

```
cp /foo/bar/cert.crt /usr/local/share/ca-certificates/
```

Выполняем установку:

```
update-ca-certificates
```

Для RPM (Rocky Linux / РЕД ОС / RHEL / CentOS / Fedora)

Копируем файл в каталог **/etc/pki/ca-trust/source/anchors**:

```
cp /foo/bar/cert.crt /etc/pki/ca-trust/source/anchors/
```

Выполняем установку:

```
update-ca-trust
```

Проверка корректности работы страницы блокировки после установки сертификата

Теперь можно проверить блокировку сайтов по протоколу **https**. При попытке зайти на заблокированный сайт у Вас должна отобразиться страница блокировки. Если страница блокировки не отображается, либо отображается оповещение браузера о недействительном сертификате - повторите шаги по установке сертификата.

Если после повторной настройки останутся нерешенные вопросы или проблемы - обращайтесь в нашу службу технической поддержки.

Распределение ролей в управлении контент-фильтрацией SkyDNS

В этой инструкции объясняется как настроить распределение ролей в управлении вашим аккаунтом. Если вы используете тарифы SkyDNS.Бизнес+, SkyDNS.Wi-Fi или SkyDNS.Вуз.

В личном кабинете есть возможность назначать администраторам аккаунта различные роли:

- **Аудитор** - обладает правом просматривать и загружать любую статистику аккаунта сервиса SkyDNS. Аудитор не может изменять настройки или использующиеся профили фильтрации.
- **Администратор** - имеет такие же права как владелец аккаунта, кроме возможности добавления администраторов.

Чтобы добавить администратора аккаунта SkyDNS войдите в **Личный кабинет** и пройдите во вкладку **Аккаунт**. Затем выберите пункт **Администраторы** в левом меню.

Затем введите учетные данные создаваемого администратора (логин и пароль), назначьте ему необходимую роль и нажмите кнопку **Добавить**.

Ниже находится список уже добавленных администраторов и их роль в управлении аккаунтом. Здесь вы можете редактировать или удалять аккаунты администраторов.

Настройка использования DNS-фильтрации SkyDNS в локальной (корпоративной) сети

Для того, чтобы начать использовать сервис DNS-фильтрации SkyDNS необходимо:

1. Определить, какие настройки фильтрации требуются одинаковые или различные для каждого компьютера (группы компьютеров)
2. Выяснить, какой внешний IP адрес предоставил провайдер — статический или динамический
3. Составить логическую схему локальной сети, в том числе:

- Определить, через какой шлюз осуществляется выход в интернет
- Определить, какие службы (Active Directory, DNS, proxy, DHCP) на каких серверах выполняются, какие IP адреса используются для этих служб и компьютеров пользователей
- Определить, каким образом получают сетевые настройки компьютеры (по DHCP или прописаны вручную)
- Привязать внешний статический IP адрес к профилю в аккаунте SkyDNS
- Если внешний IP-адрес динамический, то:
    - либо установить на компьютеры пользователей SkyDNS Agent
    - либо использовать сервис динамического DNS (типа DynDNS или no-ip.com) и привязать имя хоста, зарегистрированное в сервисе динамического DNS, к профилю в аккаунте SkyDNS
    - использовать для разрешения внешних DNS-имен DNS-сервер SkyDNS 193.58.251.251.

Привязка внешнего IP адреса или имени хоста, зарегистрированного в сервисе динамического DNS, к профилю в аккаунте SkyDNS необходима для идентификации запросов к нашим DNS серверам и применения заданных вами настроек фильтрации.

Если провайдер предоставил вам внешний IP адрес из одной из подсетей для частных сетей (т.е. IP адрес не является внешним), то возможными решениями будут являться установка агента SkyDNS на компьютеры в локальной сети, использование роутера ZyXEL Keenetic или привязка того IP адреса, который определился для вас нашим сервисом. Но в последнем случае возможен конфликт настроек с другими пользователями нашего сервиса на том же IP адресе, поэтому мы рекомендуем делать это с осторожностью. Список подсетей для частных (не маршрутизируемых) сетей следующий: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, 100.64.0.0/10.

Централизованное управление настройками фильтрации

Администратор может создавать/удалять/изменять различные профили фильтрации через веб-интерфейс (личный кабинет на сайте SkyDNS) или агент SkyDNS.

После ввода логина и пароля в агенте SkyDNS администратор может выбрать, какой профиль фильтрации будет использовать данный агент. Последующая настройка профиля фильтрации может быть сделана через личный кабинет на сайте SkyDNS или через другой экземпляр агента.

В случае удаления используемого профиля фильтрации агент SkyDNS будет использовать профиль фильтрации Основной.

При смене профиля в агенте SkyDNS настройки выбранного профиля фильтрации вступают в действие немедленно, но необходимо учитывать существование кеширования на уровне браузера и клиента DNS операционной системы.

Если требуются раздельные настройки фильтрации для каждого компьютера (группы компьютеров)

В этом случае установите агент SkyDNS на компьютеры в локальной сети, создайте и примените в агенте необходимые профили фильтрации.

Если в локальной сети развернуты службы Active Directory, то:

- пропишите в аккаунте SkyDNS адрес домена контроллера и пропишите алиасы для локальных ресурсов (создаются только A записи)
- либо установите специальную версию агента SkyDNS CS (данная версия предоставляется пользователям платных тарифов по запросу в техническую поддержку).

Стандартный агент SkyDNS принимает DNS запросы на локальном для каждого компьютера IP адресе 127.0.0.1 и осуществляет запросы DNS к серверам SkyDNS 193.58.251.251.

При использовании прокси-сервера запросы к серверам DNS осуществляет прокси-сервер. На компьютерах с установленным агентом SkyDNS необходимо отказаться от

использования прокси-сервера, если он использовался, или включить спец.режим страницы блокировки **Пустой DNS-ответ** в личном кабинете. В противном случае будут действовать те настройки фильтрации DNS, которые применяются к прокси-серверу.

Если требуются одинаковые настройки фильтрации для всех или основной части компьютеров в сети

Ниже приведены примеры настройки использования DNS-сервера SkyDNS для разрешения внешних DNS-имен.

Пример №1. В локальной сети отсутствуют серверы DNS, прокси-серверы и т.п. Компьютеры используют серверы DNS в интернете.

Привяжите внешний статический IP адрес или имя хоста, зарегистрированное в сервисе динамического DNS, к профилю в аккаунте SkyDNS.

Настройте компьютеры на использование DNS-сервера SkyDNS с IP адресом **193.58.251.251**.

Пример №2. В локальной сети имеется сервер DNS, который используют все компьютеры в сети.

Привяжите внешний статический IP адрес или имя хоста, зарегистрированное в сервисе динамического DNS, к профилю в аккаунте SkyDNS.

Настройте существующий сервер DNS на пересылку запросов внешних DNS-имен на DNS-сервер SkyDNS с IP адресом **193.58.251.251**.

Пример №3. В локальной сети используется сервис DHCP для выдачи компьютерам сетевых настроек.

Настройте сервис DHCP для выдачи адреса DNS сервера **193.58.251.251** тем компьютерам, на которых требуется фильтрация.

Привяжите внешний статический IP адрес или имя хоста, зарегистрированное в сервисе динамического DNS, к профилю в аккаунте SkyDNS.

Пример №4. В локальной сети имеется прокси-сервер, который используют все компьютеры в сети.

Привяжите внешний статический IP адрес или имя хоста, зарегистрированное в сервисе динамического DNS, к профилю в аккаунте SkyDNS.

Настройте прокси-сервер на использование DNS-сервера SkyDNS с IP адресом 193.58.251.251. Укажите в настройках прокси-сервера DNS-сервер 193.58.251.251. Если прокси-сервер использует системный клиент DNS операционной системы или получает

список серверов DNS из настроек ОС, то в сетевых настройках ОС пропишите DNS-сервер SkyDNS с IP адресом 193.58.251.251.

Пример №5. В локальной сети имеется прокси-сервер запущенный на ОС Windows, который используют все компьютеры в сети. Внешний IP адрес динамический.

Настройте прокси-сервер на использование DNS-сервера с IP адресом 127.0.0.1. Укажите в настройках прокси-сервера DNS-сервер 127.0.0.1. Если прокси-сервер использует системный клиент DNS операционной системы или получает список серверов DNS из настроек ОС, то дополнительных настроек не требуется.

Установите на компьютер, на котором запущен прокси-сервер агент SkyDNS.

> При использовании такого решения не будет отображаться страница блокировки. Вместо страницы блокировки браузер будет показывать, что сайт недоступен.

> Невозможна работа на одном хосте агента SkyDNS и DNS сервера, который может идти в составе ПО совместно с прокси-сервером.

Пример №6. В локальной сети имеется сервер DNS и прокси-сервер, которые используют все компьютеры в сети.

Привяжите внешний статический IP адрес или имя хоста, зарегистрированное в сервисе динамического DNS, к профилю в аккаунте SkyDNS.

Настройте существующий сервер DNS на пересылку запросов внешних DNS-имен на DNS-сервер SkyDNS с IP адресом 193.58.251.251.

Настройте прокси-сервер на использование имеющегося DNS-сервера или на использование DNS-сервера SkyDNS с IP адресом 193.58.251.251 (в последнем случае будут недоступны внутренние веб-ресурсы, если они имеются в локальной сети). Если в локальной сети имеются внутренние веб-ресурсы и прокси-сервер, то имеет смысл внедрить использование Web Proxy Autodiscovery Protocol и/или файл proxy auto-config (PAC), что позволяет тонко настраивать браузеры пользователей в каких случаях использовать прокси-сервер, а в каких обращаться к веб-ресурсам напрямую.

Пример №7. В локальной сети развернуты службы Active Directory.

Привяжите внешний статический IP адрес или имя хоста, зарегистрированное в сервисе динамического DNS, к профилю в аккаунте SkyDNS.

Если у вас в организации развернуты службы Active Directory, то также существует внутренний для организации сервер DNS.

Настройте существующий сервер DNS на пересылку запросов внешних DNS-имен на DNS-сервер SkyDNS с IP адресом 193.58.251.251.

Подробнее про настройку Службы DNS здесь.

Пример №8. В локальной сети развернуты службы Active Directory, имеется прокси-сервер, на части компьютеров пользователей установлены ОС Windows, на другой части — Linux. Внешний IP-адрес динамический. Требуется для разных компьютеров применять различные настройки фильтрации.

В данном случае раздельные настройки фильтрации для компьютеров с Linux не будут применяться. Но возможно для компьютеров с Linux и части компьютеров с Windows применять одни настройки фильтрации и различные настройки фильтрации для других компьютеров с Windows.

1. Используйте сервис динамического DNS (типа DynDNS или no-ip.com) и привяжите имя хоста, зарегистрированное в сервисе динамического DNS, к профилю в аккаунте SkyDNS.
2. Настройте существующий сервер DNS на пересылку запросов внешних DNS-имен на DNS-сервер SkyDNS с IP адресом 193.58.251.251. Подробнее про настройку Службы DNS здесь.
3. Настройте прокси-сервер на использование имеющегося DNS-сервера или на использование DNS-сервера SkyDNS с IP адресом 193.58.251.251 (в последнем случае будут недоступны внутренние веб-ресурсы, если они имеются в локальной сети).
4. Настройте компьютеры с Linux на использование существующего сервера DNS и прокси-сервера.
5. Настройте компьютеры с Windows, на которых должны применяться те же настройки фильтрации, на использование существующего сервера DNS и прокси-сервера.
6. Установите на другие компьютеры с Windows агент SkyDNS или SkyDNS CS. Создайте и примените необходимые профили фильтрации. Отключите использование прокси-сервера на данных компьютерах.

Пример №9. В локальной сети развернуты службы Active Directory, на части компьютеров пользователей установлены ОС Windows, на другой части Linux. Имеется подсеть внешних IP адресов с маской 28 (14 внешних IP адресов). Требуется для разных компьютеров применять различные настройки фильтрации.

1. Создайте до 14 включительно профилей фильтрации в аккаунте SkyDNS.
2. Привяжите к каждому профилю по IP адресу из имеющихся внешних IP адресов.
3. Запустите до 14 включительно серверов DNS (например bind9) принимающих запросы от компьютеров в локальной сети каждый на своем IP. Можно запустить DNS серверы с различными конфигурационными файлами или использовать виртуализацию и запустить каждый экземпляр в отдельной виртуальной машине.

4. Настройте каждый экземпляр как slave для зон в DNS сервере, используемом службами Active Directory.
5. Настройте на каждом DNS сервере пересылку запросов внешних DNS-имен на DNS-сервер SkyDNS с IP адресом 193.58.251.251 с индивидуального сокета для этого сервера DNS.
6. На шлюзе доступа в интернет настройте Source NAT на каждый из имеющихся 14 внешних IP для каждого из сокетов, с которых DNS серверы осуществляют запросы.
7. Разбейте компьютеры в локальной сети на 14 групп и каждой группе выдайте с помощью DHCP один из созданных DNS серверов.

Настройка различных профилей фильтрации в сетях с трансляцией сетевых адресов (NAT)

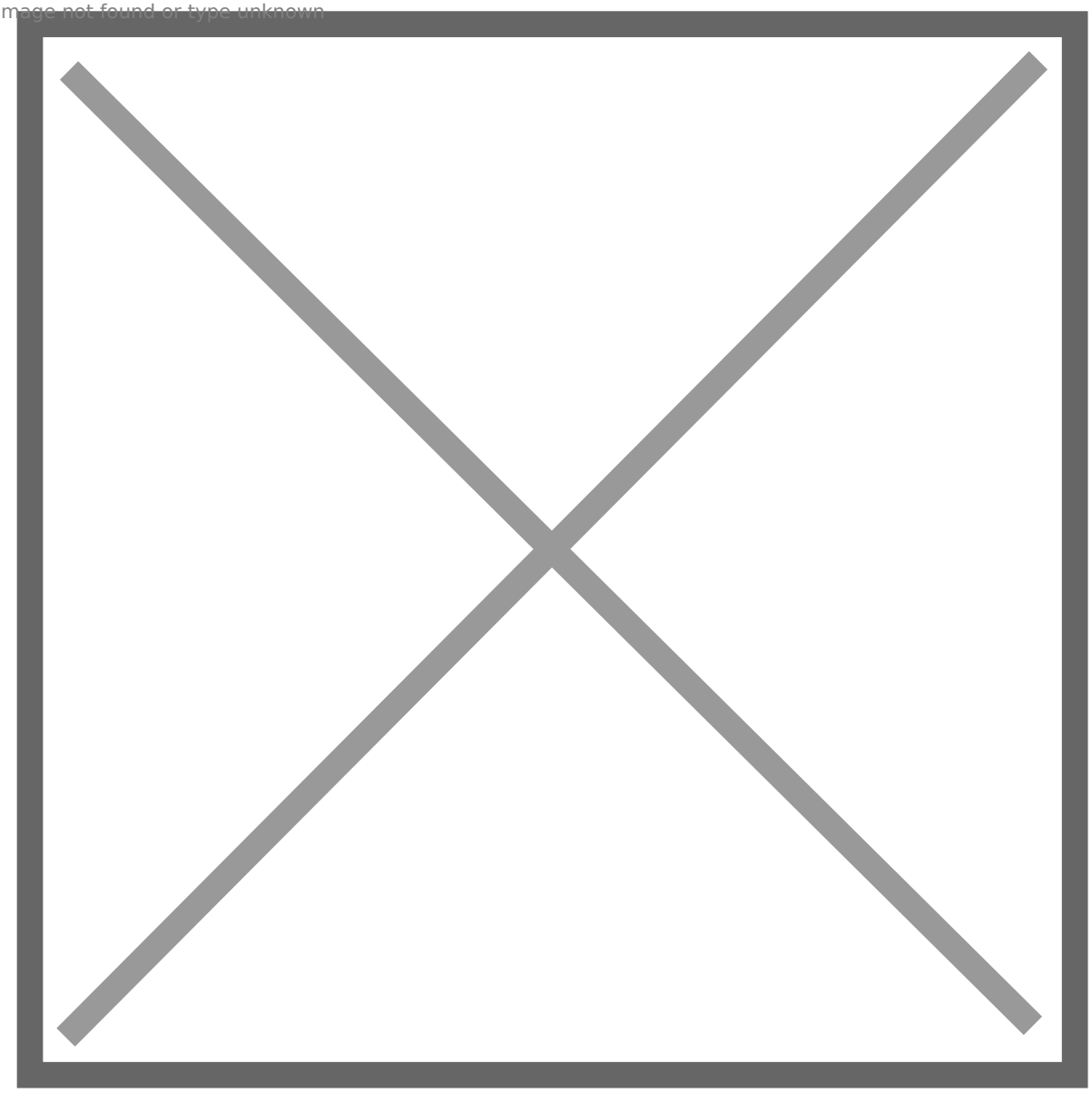
Сетевая технология NAT активно применяется в корпоративных и гостевых сетях и предназначена для:

- экономии количества статических IP-адресов,
- обеспечения безопасности устройств внутри локальной сети,
- предотвращения обращений извне к внутренним хостам,
- позволяет скрыть внутреннюю структуру корпоративной сети от внешнего наблюдателя.

Функция NAT DNS служит для привязки разных профилей фильтрации сервиса SkyDNS к разным устройствам за NAT (роутерам, точкам доступа, интернет-шлюзам и т. д.).

> Для корректной работы функции ваш роутер или интернет-шлюз должен быть настроен согласно инструкциям, расположенным на нашем сайте.

Image not found or type unknown



Пример организации контент-фильтрации в корпоративной сети с использованием опции NAT DNS

Настройка NAT DNS:

1. Зайдите в личный кабинет SkyDNS и привяжите **внешний IP** для роутера или интернет-шлюза с NAT к любому из профилей фильтрации (для настройки функции NAT DNS вам необходимо иметь не менее 2 профилей).

2. На конечных устройствах (отдельные роутеры, интернет-шлюзы в сети за NAT) стандартными средствами (вручную, через DHCP и т. п.) установите соответствующие нужным профилям фильтрации **целевые адреса DNS серверов**.

Список целевых адресов DNS:

- 193.58.251.101
- 193.58.251.102

- 193.58.251.103
- 193.58.251.104
- 193.58.251.105

3. В личном кабинете SkyDNS перейдите в: **Настройки** - **Устройства**, выберите профиль соответственно **целевому IP адресу** (один IP адрес - один профиль). После того, как необходимые профили фильтрации выбраны, сохраните настройки.

image-1700654355370.png

Image not found or type unknown

4. После сохранения настроек устройства будут фильтроваться согласно установленным правилам.

5. Статистика запросов и блокировок будет отображаться на соответствующих профилях.

> Опция предназначена только для настройки в сетях с NAT. При наличии прокси-сервера фильтрация по настройкам NAT DNS производиться **не будет**, так как в этом случае применяются только настройки, установленные для прокси-сервера.

Взаимодействие SkyDNS и корпоративных систем

В корпоративной системе существует набор сервисов, использование которых упрощает администрирование сети, а на некоторые из них возлагают и функцию ограничения доступа пользователей к нежелательным ресурсам Интернета.

К являющимся частью инфраструктуры многих корпоративных систем можно отнести такие сервисы как **DHCP**, **DNS** и **контроллер домена**.

Одна из целей использования сервиса **DHCP** заключается в назначении сетевых реквизитов пользовательским системам.

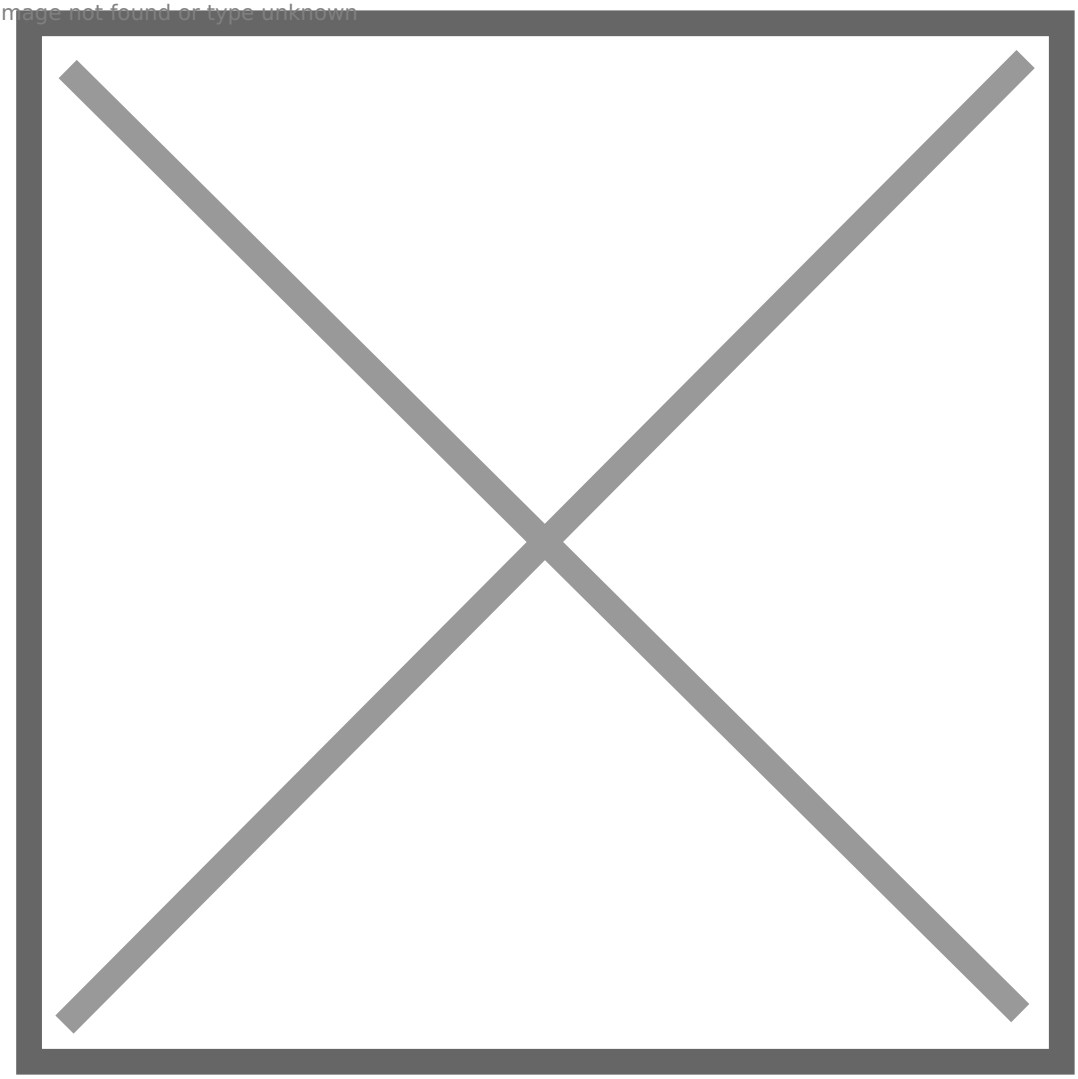
В задачи **контроллера домена** входит обеспечение централизованного управления ресурсами домена компании. К таким ресурсам относятся и доменные имена пользовательских и иных систем компании.

Разрешение доменных имён систем компании в их IP адреса для сетевого взаимодействия возлагается на **сервер DNS**. Кроме этого, DNS-сервер отвечает за обработку запросов, касающихся интернет доменов.

Дополнительно к вышеприведённым сервисам может применяться и **прокси-сервер**. Его основной функцией является транзит Веб-трафика (и трафика некоторых других протоколов) из Интернет в локальную сеть компании. Для выполнения запросов пользователей прокси-сервер выполняет разрешение имён используя сервис DNS.

Интернет-шлюз занимается маршрутизацией трафика между сетью компании и интернет. Очень часто на него возложены функции защиты локальной сети и блокировки нежелательных видов трафика в сторону Интернет.

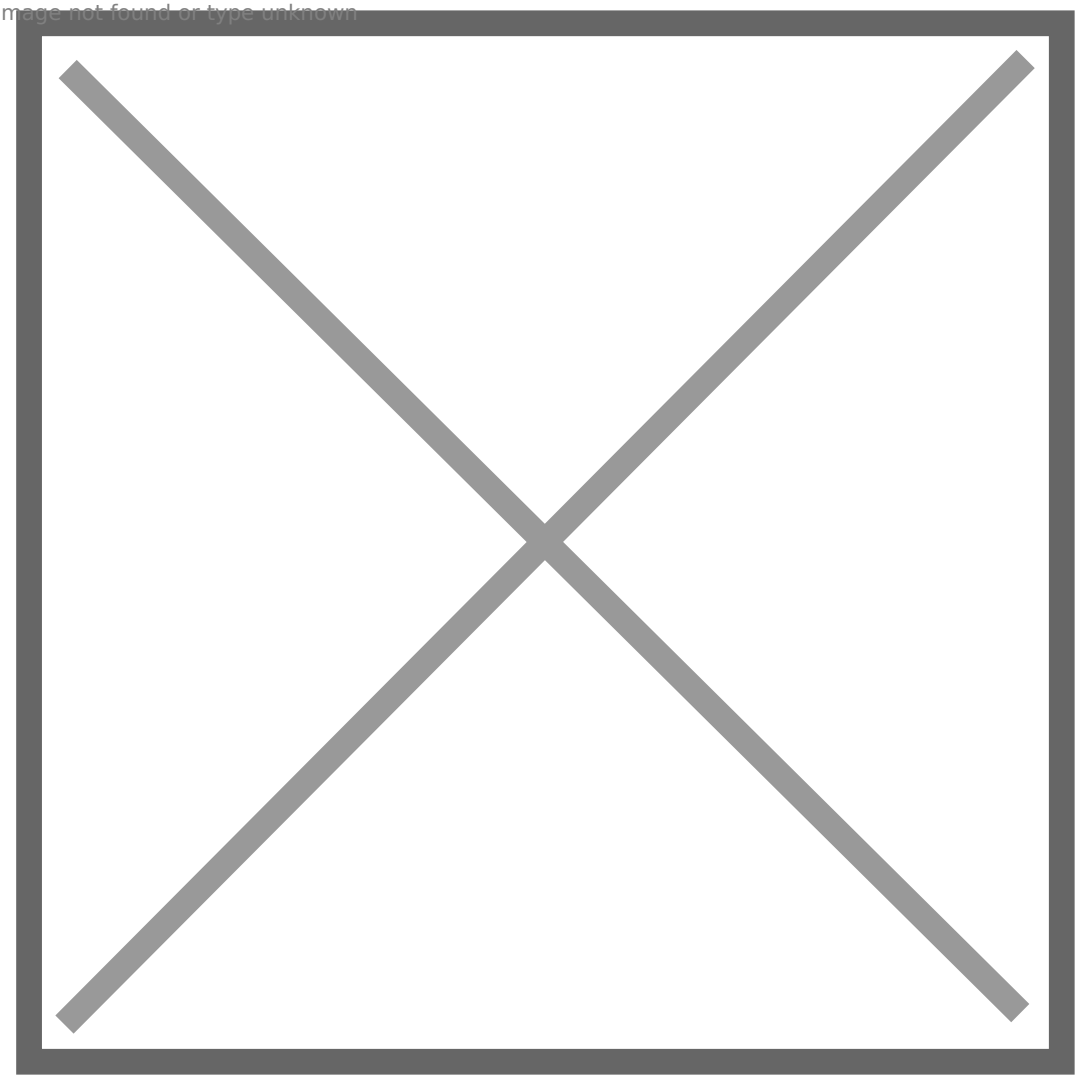
Image not found or type unknown



Рассмотрим варианты взаимодействия сервиса **SkyDNS** с каждым из вышеприведённых компонентов корпоративной системы.

DNS сервер компании: как правило, такие серверы настроены на передачу запросов соответствующим серверам провайдера и самостоятельным разрешением имён занимаются только в рамках корпоративного домена. Если для такого сервера в качестве сервиса реализующего фактическое разрешение имён для интернет указать **SkyDNS**, то в ответ на запросы, содержащиеся в заблокированных категориях, будет выдаваться один из адресов **SkyDNS**. Если при этом целью запроса к DNS-серверу компании было получение IP-адреса веб-страницы, то в браузере появится страница блокировки сервисом **SkyDNS** обращения к сайту. В данной конфигурации взаимодействия корпоративных систем со **SkyDNS** пользователи, использующие **DNS сервер** компании, будут вынуждены подчиняться тем или иным правилам политики безопасности или контроля использования интернет. А отражение правил будет установлено в личном кабинете сервиса **SkyDNS**.

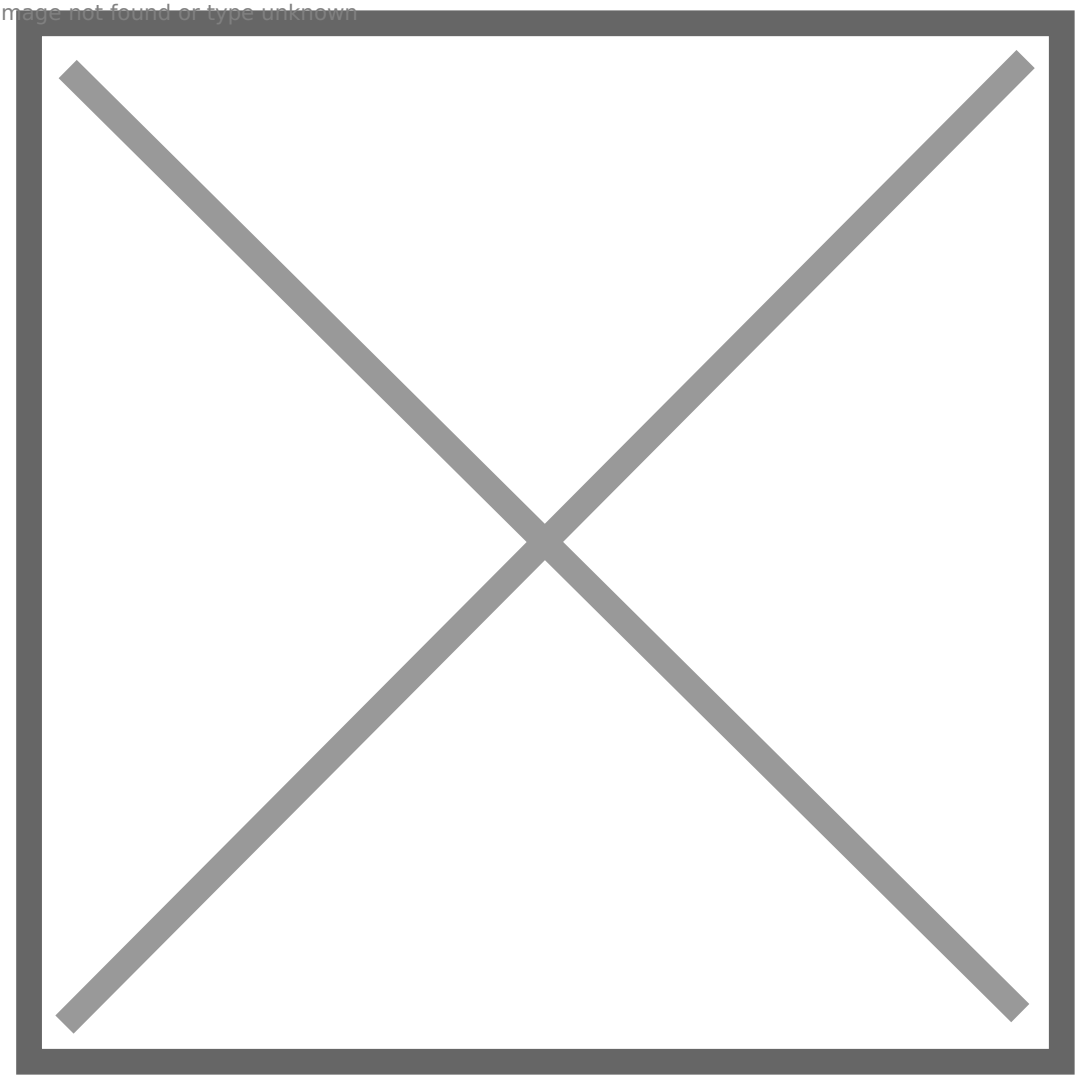
Image not found or type unknown



При этом, при правильной настройке разрешение имён корпоративного домена будет происходить только на стороне DNS-сервера компании.

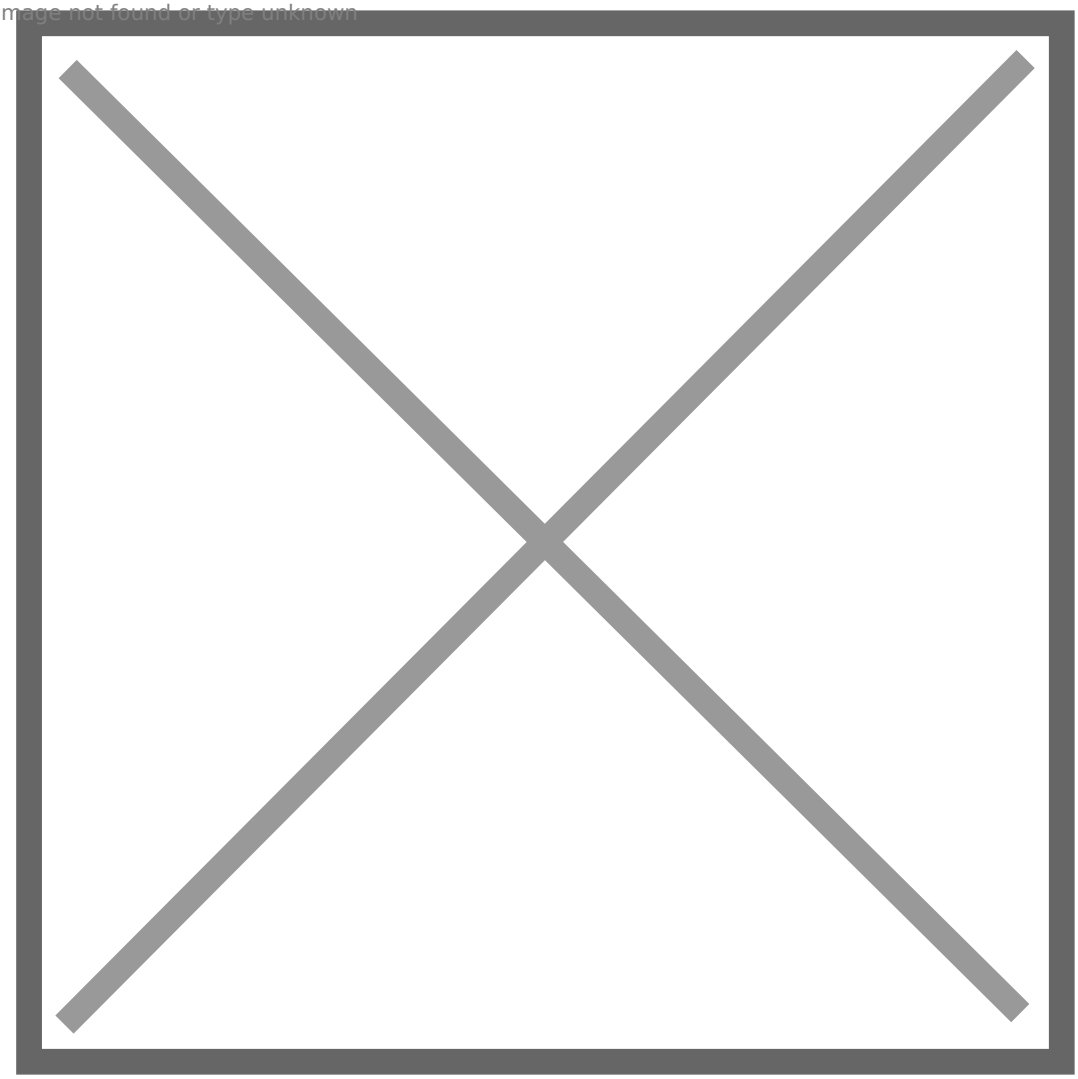
Далее рассмотрим конфигурирование **DHCP** таким образом, чтобы пользователям в качестве **DNS сервера** для компании выдавался адрес **SkyDNS**. При этом запросы тех пользователей, чьи системы используют **DHCP** для получения сетевых реквизитов, будут получать ответы напрямую от сервиса **SkyDNS**. Это ограничивает возможности использования корпоративного домена. Лучше такая конфигурация подходит когда он не используется в локальной сети компании. При возможности гибкой настройки **DHCP-сервера** можно назначать пользователям DNS без фильтрации или с ней.

Image not found or type unknown



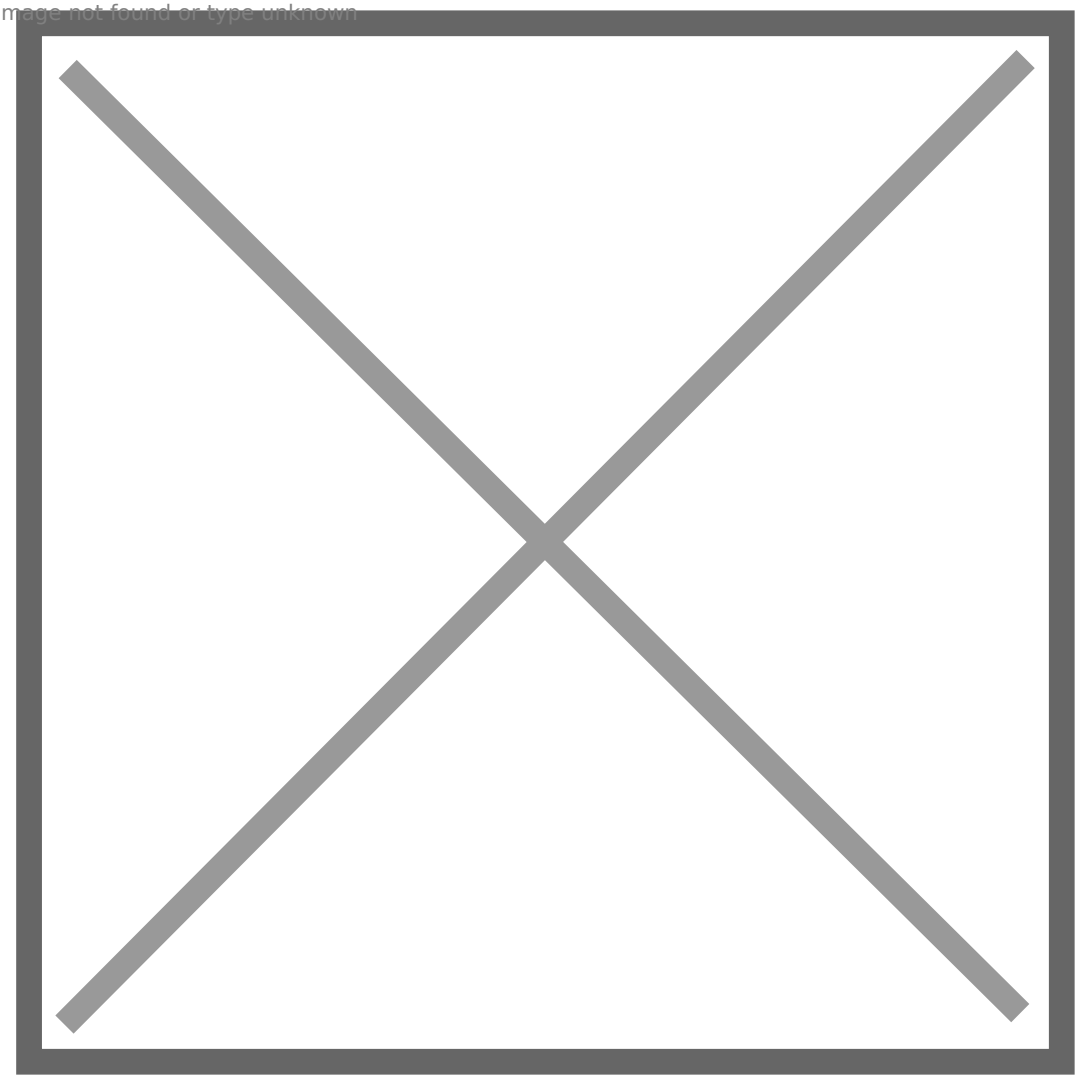
Если используется **прокси-сервер**, то настроив разрешение имён в нём через сервис **SkyDNS** можно получить аналогичный по своему эффекту взаимодействия **DNS** сервера компании с сервисом **SkyDNS** результат.

Image not found or type unknown



Лучший контроль над **DNS** запросами пользователей и соответствующую политике безопасности или ограничений реализацию взаимодействия с сервисом **SkyDNS** можно получить комплексным подходом, включающим в себя и настройку **интернет-шлюза** компании или филиала. При этом, в брандмауэре надо задать перенаправление **DNS** запросов на сервис **SkyDNS**. При желании можно и исключить те машины в сети, которые не должны проходить фильтрацию запросов.

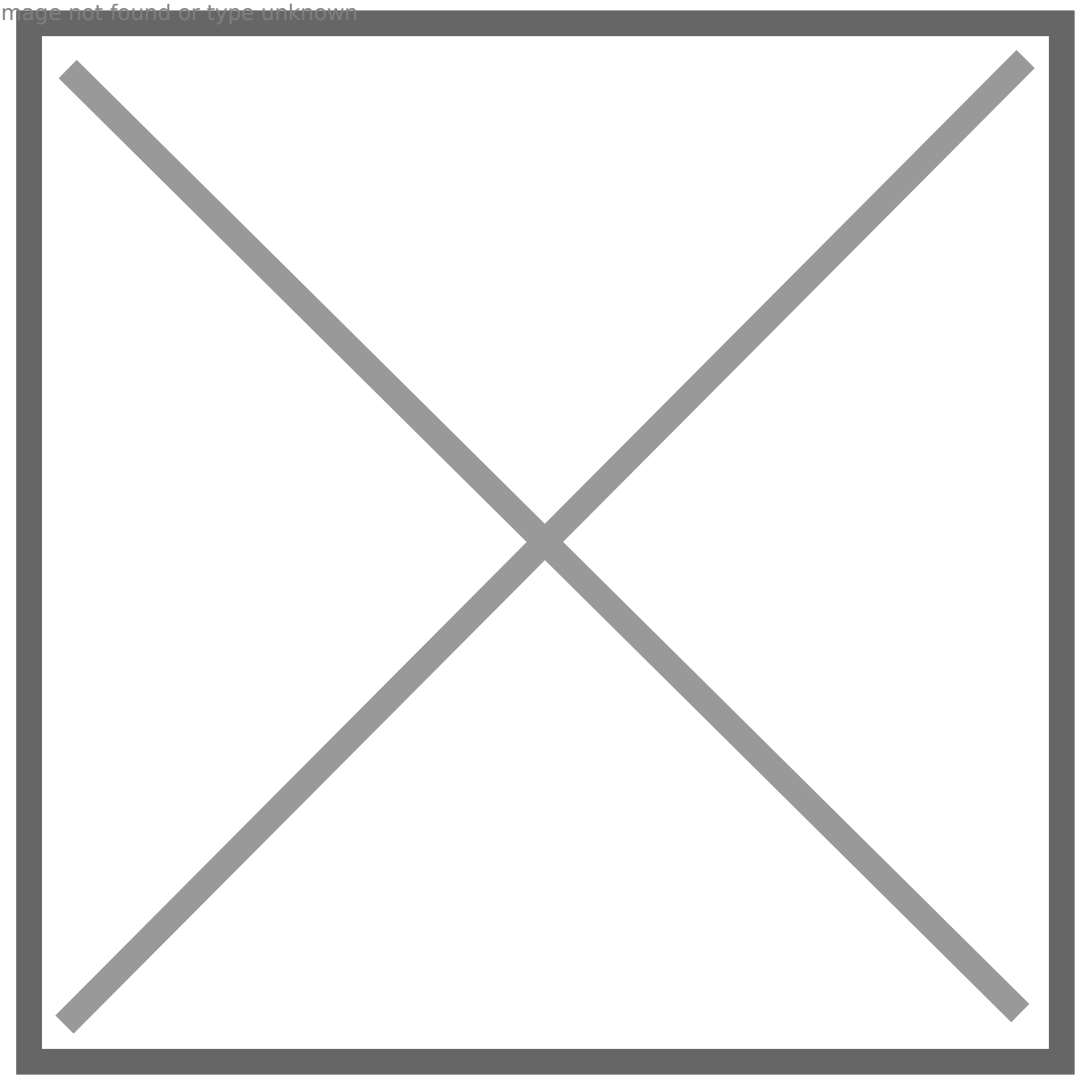
Image not found or type unknown



В качестве заключения можно привести вариант сценария взаимодействия с сервисом **SkyDNS**:

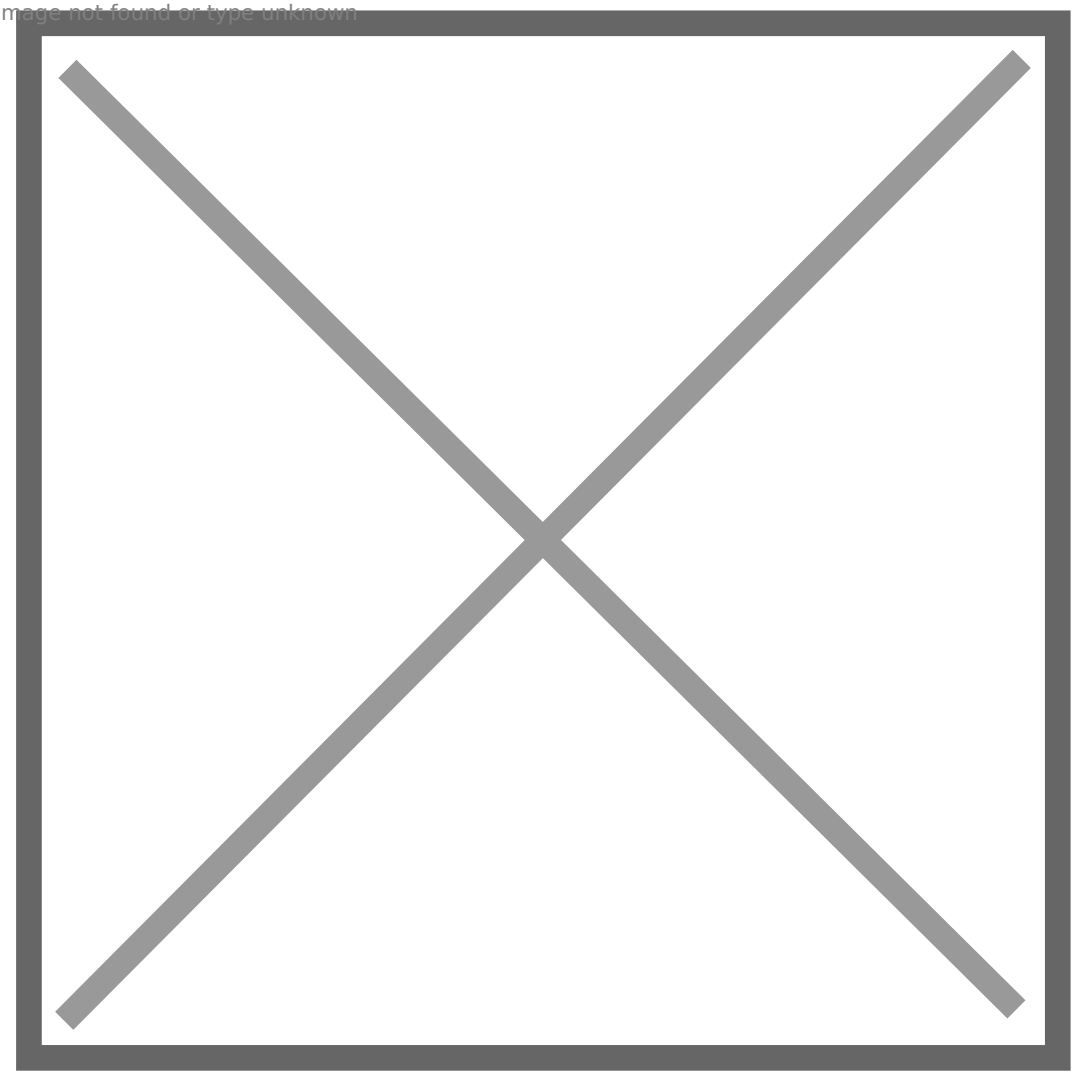
Среди сетевых реквизитов, получаемых по **DHCP** в качестве адреса **DNS-сервера**, пользовательская система получает адрес корпоративного **DNS сервера**.

Image not found or type unknown



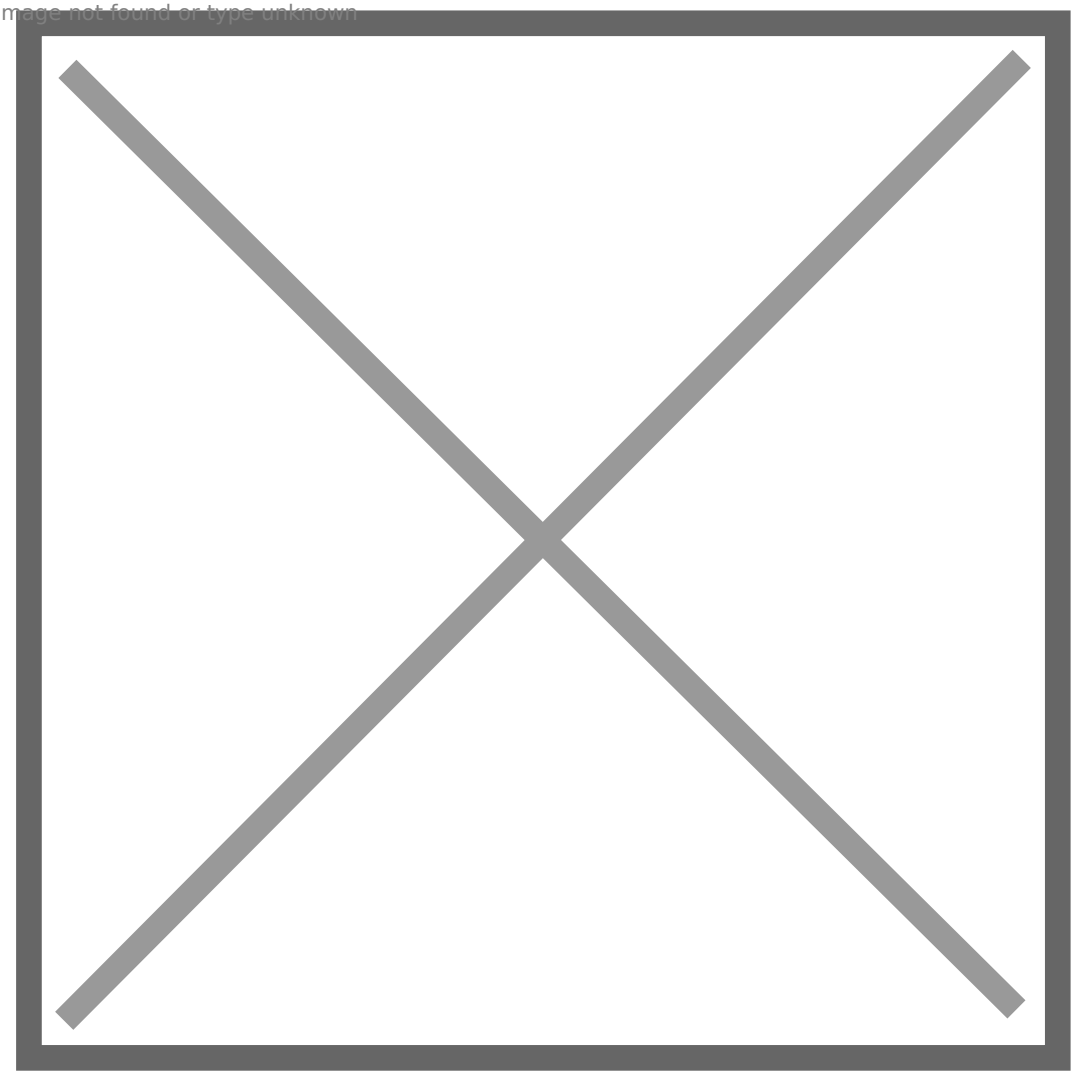
На корпоративном **DNS-сервере** запросы, касающиеся доменов интернет, передаются сервису **SkyDNS**. Ответы отфильтрованы в соответствии с настройками сервиса.

Image not found or type unknown



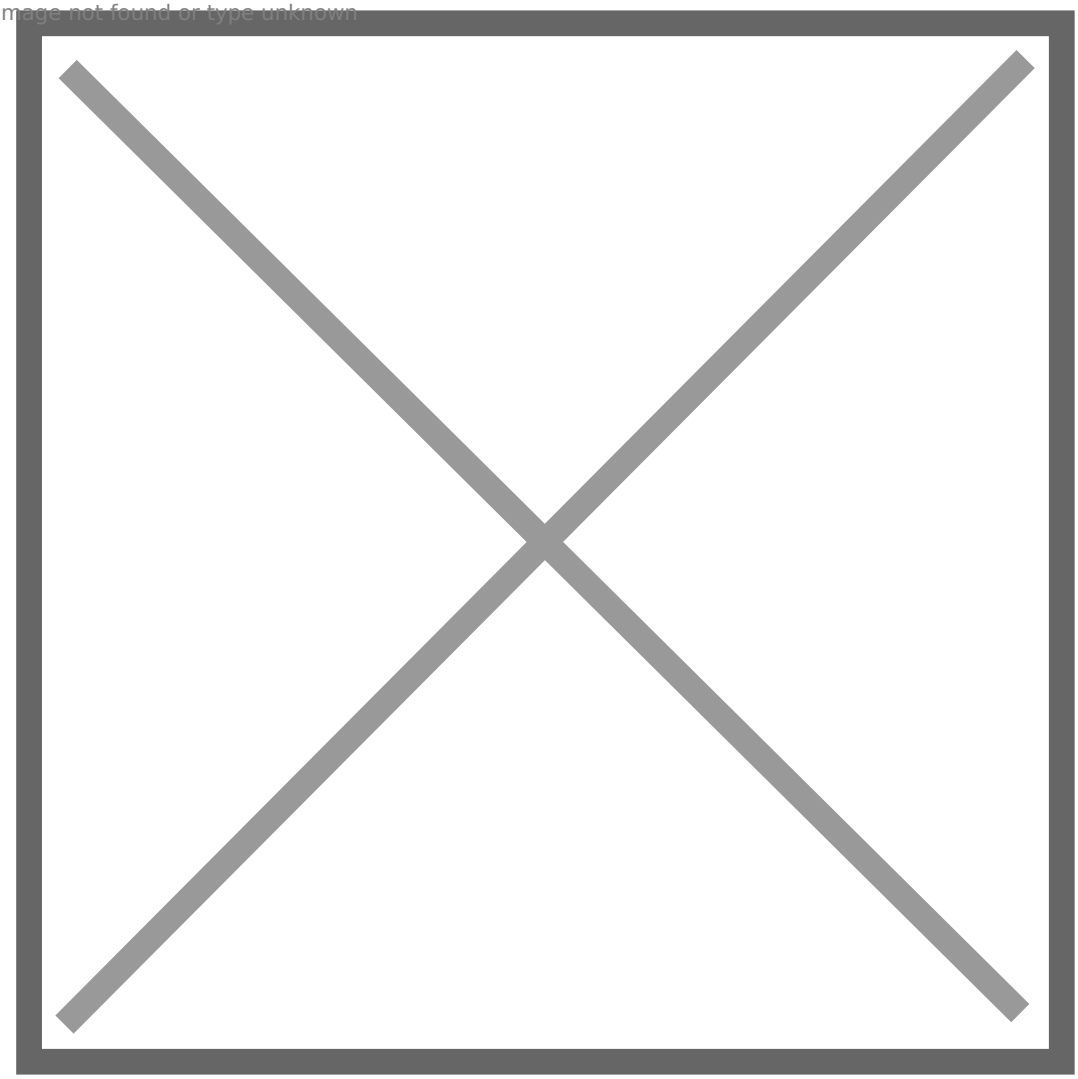
Преобразование адресов на **прокси-сервере** настроено на корпоративный **DNS сервер**. Запросы к веб-серверам в сети проходят без изменений, а к Интернет-сайтам фильтруются на уровне **DNS**.

Image not found or type unknown



Дополнительно, или как вариант, на **Интернет-шлюзе** запросы, направляющиеся по протоколу **DNS**, перенаправляются в сторону сервиса **SkyDNS**.

Image not found or type unknown



Для успешного применения некоторых политик безопасности обязательно закрытие доступа пользователей к другим **DNS** на **Интернет-шлюзе**. При этом, если у компании есть несколько белых IP-адресов (например, для NAT), то возможно разделение профилей фильтрации.

API обновления динамического IP адреса

Для того что бы обновить ваш привязанный в системе динамический IP адрес необходимо отправить HTTP запрос на следующий URL:

https://www.skydns.ru/nic/update

Пример минимального запроса с передачей авторизационных данных в запросе в явном виде (поддерживается роутерами с прошивкой DD-WRT, OPEN-WRT и другими системами)

```
https://username:password@www.skydns.ru/nic/update?hostname=home
```

Пример сырого HTTP запроса с передачей авторизационных данных в закодированном виде

```
GET /nic/update?hostname=home HTTP/1.0
Host: www.skydns.ru
Authorization: Basic base64-encoded-auth-string
```

Авторизация при использовании сырых HTTP запросов

Для сырых HTTP запросов нужно использовать Basic Authorization.

Нужно передавать специальный HTTP заголовок Authorization в каждом запросе, в котором передавать строку username:password, закодированную методом base64. При этом следует явно указывать базовый (Basic) метод авторизации.

Пример заголовка:

```
Authorization: Basic NDc2MDE4N2Q4MWJjNGI3Nzk5NDc2YjQycjUxMDM3MTM6ZjI1YmViZjk5MWZmNDE5ODkzZGIyNTU
```

Параметры URL

Поле	Обязательный	Описание
username:password	Да	Логин и пароль аккаунта. В качестве логина используется email адрес.

hostname	Да	Указывает имя хоста, добавляется для идентификации. Например, если привязывается несколько IP адресов на один профиль.
profile	Нет	Указывает числовой идентификатор профиля на который будет привязан IP адрес. Идентификаторы можно увидеть в личном кабинете в разделе Профили.
myip	Нет	Обновляемый динамический IP адрес. В целях безопасности данный параметр игнорируется и обновляемый адрес берется не из параметра, а определяется на стороне нашего сервера.

Коды ответа

Код	Статус	Описание
Authentication required	Ошибка	Требуется авторизация, указаны неправильные данные в заголовке Authorization
badprofile	Ошибка	Указан неверный профиль
!yours	Ошибка	Данный IP адрес уже используется, для большей информации можете посмотреть статус в кабинете
good IP_ADDRESS	Успех	Адрес успешно привязан