ООО «СкайДНС» ИНН 6670326961
620109, Россия, Свердловская обл., город Екатеринбург,
г. Екатеринбург, ул. Токарей , д. 40, офис 348
тел.: 8-800-333-33-72
web: www.skydns.ru
e-mail: info@skydns.ru

Как подключить фильтрацию SkyDNS

Шаг №1: Зарегистрировать личный кабинет

Для активации промокода, необходимо перейти по ссылке регистрации, ввести промокод, электронную почту учреждения и создать пароль. После заполнения формы регистрации нужно обязательно подтвердить почту, перейдя по ссылке из письма. Если письмо не пришло – проверьте папку «Спам».

Шаг №2: Настроить правила фильтрации

1. Внести свои внешние IP-адреса в разделе «Настройки». Также можно добавить туда DynDNS-адреса, если у вас нет статического IP-адреса.
   - Это поможет нам отличить ваши запросы от запросов других клиентов.
   - Если у вас большой список адресов, воспользуйтесь кнопкой «Добавить списком».

2. В разделе «Категории» выбрать то, что нужно заблокировать. Закрытый замок означает, что сайты этой тематики будут недоступны.
   - Опция «**Работать по разрешающему списку**» означает, что заблокировано будет вообще всё, кроме того, что явно прописано в «Белом Списке».
   - Опция «**Блокировать неизвестные сайты**» означает, что заблокировано будет всё, что ещё не категоризировано нами. Это кратно увеличивает безопасность в отношении свежих фишинговых сайтов, но осложняет работу с облачными сервисами, т.к. CDN плохо поддаются категоризации из-за отсутствия каких-либо публичных данных.
   - Опция «**Использовать безопасный поиск**» будет перенаправлять на безопасный поиск SkyDNS при открытии любого поискового сервиса. Однако для того, чтобы это работало по https, нужно добавить сертификат SkyDNS. Сам сертификат и инструкция доступны здесь.

3. В разделе «Списки» вы можете добавить то, что должно быть доступно независимо от заблокированных категорий и то, что должно быть принудительно заблокировано, независимо от категорий. Обратите внимание, что сначала вы создаете сам список и даете ему название

(например «Мои рабочие сайты»), а потом уже добавляете один или несколько доменов в этот список.

Шаг №3: Перенаправить DNS-трафик на наши сервера (193.58.251.251)

Важно: Перед тем, как приступить к этому шагу, подождите минимум 5 минут с момента, когда на предыдущем шаге вы внесли IP-адрес. При большом трафике, наша система, не идентифицировав вас, может заблокировать вас за высокий анонимный трафик.

Теперь измените сетевые настройки в вашей сети таким образом, чтобы DNS трафик отправлялся нам вместо вашего текущего DNS-резолвера. Варианты:

- Если вы используете локальный DNS-сервер, то в качестве внешнего источника данных укажите наш IP-адрес. Если ваш DNS-сервер поддерживает приоритезацию, можете не заменить текущий, а добавить наш и поставить его первым приоритетом.
- Если DNS-пакеты обрабатываются вашим маршрутизатором, то в качестве DNS Forwarder укажите наш IP вместо того, которым вы пользуетесь сейчас.
- Если конечные DNS вы прописываете на каждом конечном устройстве, замените в настройках DHCP-сервера текущие адреса DNS на наш.

Важно: На конечном устройстве должен быть указан только один DNS-адрес, который напрямую или опосредованно ведет на нас. Если указано несколько IP-адресов, то нужно убедиться, что при запросе на каждый из них, DNS-запрос попадет именно на наш сервер.

Диагностические команды (для IT-специалистов)

Чтобы перед переключением трафика убедиться, что всё настроено правильно и переключение не вызовет проблем, нужно выполнить следующую команду:

```
nslookup -q=txt black.skydns.ru 193.58.251.251
```

Эта команда посылает DNS-запрос напрямую на наш сервер, игнорируя текущие настройки DNS.

Если всё настроено, пример ответа должен выглядеть так:

```
"{"ip": "176.215.11.249", "t": 0, "p": 327865}"
```

Самое главное, что нас тут интересует, это поле «p». Если в нём указано любое число, отличное от нуля, значит мы правильно идентифицировали вас.

Это число – ID профиля фильтрации. Проверить свой ID профиля можно здесь. Нужно мышкой навести на название профиля и во всплывающей подсказе будет его номер.

Если же в этом поле стоит «0», значит мы получили ваш запрос, но не можем его идентифицировать. Скорее всего это связано с тем, что запрос пришел с IP, который не добавлен в настройки вашего Личного Кабинета. Здесь нам как раз поможет поле «ip» в выводе диагностической команды, потому что ваш запрос к нам пришел именно с этого IP. Добавьте его в кабинет и подождите до 5 минут, чтобы изменения были доставлены до всех наших серверов.

В случае, если в ответе вы вообще не увидели JSON, то это означает, что этот DNS-запрос не дошел до нас, а был обработан кем-то другим. Скорее всего, это связано с тем, что кто-то перехватывает DNS-трафик в вашей сети (DNAT). Обратитесь к нашим специалистам.

Если, согласно диагностике, вы получили номер профиля фильтрации, то можно смело переключать трафик в вашей сети (Шаг №3). Но после того, как переключили, мы рекомендуем проверить правильность переключения следующей командой:

```
nslookup -q=txt black.skydns.ru
```

Она отличается тем, что мы не указали принудительно наш IP-адрес, а значит, DNS-запрос пойдет согласно вашим настройкам маршрутизации. Если настроено всё правильно, то вы увидите тот же результат, что и в первой диагностической команде. Если вы не увидели JSON вообще (будет информация о TTL и прочем), значит, настройки пересылки DNS настроены неверно. Обратитесь к нашим специалистам за помощью.