Решение потенциальных проблем

Блокировка серверов обновления Windows

С помощью нашего контент-фильтра Вы можете заблокировать доступ к серверам обновления Windows, заблокировав доменные имена, которые используются ОС Windows для обновления.

Для полной блокировки обновлений Windows, необходимо внести в Ваш **запрещающий список** следующие записи:

- windowsupdate.com
- activation-v2.sls.microsoft.com
- b1.download.windowsupdate.com
- ctldl.windowsupdate.com
- data.microsoft.com
- displaycatalog.mp.microsoft.com
- download.windowsupdate.com
- fe2.update.microsoft.com
- go.microsoft.com
- licensing.mp.microsoft.com
- purchase.mp.microsoft.com
- settings-win.data.microsoft.com
- sls.update.microsoft.com
- update.microsoft.com
- urs.microsoft.com
- v10.vortex-win.data.microsoft.com
- validation-v2.sls.microsoft.com
- wdcp.microsoft.com
- wdcpalt.microsoft.com
- win10.ipv6.microsoft.com

Если что-то работает не так, как ожидалось

Если фильтрация не работает, как ожидалось, то до обращения в техническую поддержку выполните следующие действия:

1. Если вы являетесь администратором сети организации, то в первую очередь обратитесь к разделу Настройка использования DNS-фильтрации SkyDNS в локальной (корпоративной) сети.
2. Отключите любую фильтрацию, в том числе фильтрацию SkyDNS.
3. Убедитесь, что выход в интернет осуществляется через соединение, которое вы собираетесь защитить сервисом SkyDNS. Например, убедитесь, что со смартфона выход осуществляется по Wi-Fi через роутер, а не через сотового оператора. Удостоверьтесь, что настройки DNS получаются в автоматическом режиме с Wi-Fi роутера в этом случае.
4. В командной строке ОС Windows выполните команду **ping 193.58.251.251**. Убедитесь, что получаете ответы от узла с указанным IP-адресом через вашего провайдера в данный момент времени. Возможно, в сети вашего провайдера существуют проблемы, и часть ресурсов в интернет недоступна в данный момент времени, в том числе один из наших серверов, на который маршрутизируются ваши запросы DNS. Обратитесь в техническую поддержку вашего провайдера.
5. В командной строке выполните команду **nslookup -q=txt black.skydns.ru 193.58.251.251**. В результате должны получить ответ **black.skydns.ru text ="{"ip": "*", "t": *, "p": *}"**, где в "ip" будет указан ваш IP-адрес, а "t" и "p" будут иметь какое-то значение или 0. Если полученный ответ не имеет вид "{"ip": "*", "t": *, "p": *}", то это означает, что ваши запросы DNS не доходят до наших серверов, а перенаправляются на какой-либо другой сервер DNS, скорее всего, вашим провайдером. Вы можете обратиться к вашему провайдеру с просьбой, открыть доступ к публичным DNS серверам в интернете. Или попробуйте воспользоваться сервисом SkyDNS, установив агент SkyDNS или активировав модуль SkyDNS в роутерах серии Zyxel Keenetic. Агент SkyDNS и модуль SkyDNS в роутерах Zyxel Keenetic с последними версиями прошивок используют нестандартный порт 1253 для запросов DNS. На Linux можно настроить обращение к нестандартному порту для запросов DNS по инструкции Настройка средствами iptables использования нестандартного порта для запросов DNS.
6. Если вы используете Агент SkyDNS или модуль SkyDNS в роутерах Zyxel Keenetic, то убедитесь, что на шлюзе доступа в интернет, если он имеется, и провайдером открыт доступ к сайту https://www.skydns.ru и портам 1253 tcp и udp на адресе

193.58.251.251.

7. На время установки или удаления Агента SkyDNS отключите антивирус.
8. Проверьте, что на вашем компьютере не используется DNS сервер для протокола IPv6. Соответствующая опция DNS в настройках протокола, должна быть выставлена в ручное получение DNS и адрес DNS не должен быть заполнен. Либо произведите отключение протокола IPv6.
9. Проверьте, что на вашем компьютере не включены программы перехватывающие DNS трафик, такие как Avast Internet Security или Avast Premier. Эти программы производят перехват DNS запросов, их шифрацию и нарушают работу нашего фильтра. Если у вас используются такие программы, то необходимо в них выключить соответствующие опции (Secure DNS в Avast), нарушающие работу нашего фильтра.
10. Включите фильтрацию SkyDNS.
11. Если вы используете агент SkyDNS, то запустите графический интерфейс управления агентом. Затем перейдите **Настройки, Общие настройки, Соединения интернет. Проверьте, что выбраны все необходимые сетевые соединения.**
12. Отключите расписание на всех профилях (если использовали) и убедитесь, что используете нужный профиль фильтрации.
13. Очистите кэш DNS. Для этого выключите и включите роутер (если используется) и перезагрузите компьютер (мобильное устройство).
14. Убедитесь, что файл hosts (обычно расположен по пути C:\Windows\System32\drivers\etc\hosts) не содержит лишних записей. Для этого откройте его в текстовом редакторе типа **Блокнот** и убедитесь, что все строки либо пустые, либо начинаются со знака # (решетка).
15. В командной строке ОС Windows выполните команду **nslookup paypai.com.** (без указания адреса сервера DNS). Домен paypai.com должен разрешиться в IP-адрес из сети 193.58.251.0/24.
16. На странице узнайте к какой категории относится какой-либо домен (например, youtube.com). Заблокируйте эту категорию. Подождите 5 минут пока изменения в настройках вступят в действие на наших серверах. В командной строке ОС Windows выполните команду **nslookup youtube.com**. Домен youtube.com должен разрешиться в IP-адрес из сети 193.58.251.0/24. Зайдите на сайт youtube.com и убедитесь, что отображается страница блокировки.
17. Если ваш компьютер находится за прозрачным прокси-сервером (не под вашим управлением), то активируйте опцию **Пустой DNS-ответ** в настройках страницы блокировки в Личном кабинете на сайте www.skydns.ru. В этом случае сайт не будет доступен. Страница блокировки так же отображаться не будет.

Очистка системного кэша DNS и кэша браузеров

Перед началом использования сервиса или после изменения настроек SkyDNS рекомендуется очистить системный кэш DNS и кэш DNS браузера, чтобы исключить ложное несрабатывание фильтра или наоборот ложную блокировку. В противном случае, вы можете наблюдать отсутствие блокировки для некоторых ресурсов в течение некоторого времени, хотя при этом наш сервис будет выдавать вашей системе правильную блокирующую информацию.

Все команды рекомендуется запускать от имени пользователя с администраторскими правами

Windows (все версии)

В режиме командной строки необходимо выполнить команду **ipconfig /flushdns**

OS X

В режиме терминала необходимо от имени администратора выполнить команду соответствующую вашей версии системы

10.4 TIGER: **lookupd -flushcache**

10.5 и 10.6 LEOPARD: **dscacheutil -flushcache**

10.7 и 10.8 Lion: **sudo killall -HUP mDNSResponder**

10.9 и 10.10.4 Yosemite: **dscacheutil -flushcache;sudo killall -HUP mDNSResponder**

10.10 Yosemite (не 10.10.4): **sudo discoveryutil mdnsflushcache; sudo discoveryutil udnsflushcaches; say flushed**

Linux (основные дистрибутивы)

Откройте терминал и выполните команду
sudo /etc/init.d/nscd restart или **/etc/init.d/nscd restart**

Ubuntu Linux

Откройте терминал и выполните команду

sudo service network-manager restart

sudo systemd-resolve --flush-caches

Очистка кэша DNS в браузере

Internet Explorer: Войдите в свойства браузера - Общие - Журнал браузера - Удалить. Включите все галочки кроме опций Файлы cookie и Пароли и нажмите Удалить.

Mozilla Firefox: Войдите в меню Журнал - Удалить недавнюю историю. В выпадающем списке с временным периодом выберите Всё, а в Подробности выберите все кроме Куки, Журнал форм и поиска. Нажмите кнопку Удалить сейчас.

Apple Safari: Войдите в настройки браузера (шестеренка в правом верхнем углу) и выберите Сбросить Safari. Уберите галочки для тех данных которые хотите сохранить (например данные форм) и нажмите Сброс.

Google Chrome: Войдите в меню (гамбургер в правом верхнем углу) и выберите История. Нажмите Очистить историю. Выберите За все время и поставьте галочки на всех пунктах кроме Файлы cookie и Пароли. Нажмите Очистить историю.

Отключение опции Secure DNS в антивирусах Avast Internet Security и Avast Premier

При одновременном использовании контент-фильтра SkyDNS и некоторых антивирусов может наблюдаться отсутствие фильтрации. Это связано с функциями таких программ по перехвату DNS трафика, которые в итоге приводят к неправильной работе нашего фильтра.

Для восстановления корректной работы фильтра SkyDNS в этой ситуации необходимо отключить такие функции, тем более что при одновременном использовании с нашим фильтром они не добавляют дополнительной защиты, дублируя уже имеющиеся защитные системы в нашем фильтре.

Ознакомьтесь с данной инструкцией, чтобы узнать как отключить такую функцию Secure DNS в антивирусных продуктах компании Avast.

Откройте интерфейс антивирусной программы и нажмем меню настроек (значок шестеренки справа сверху):

Image not found or type unknown

В меню настроек нужно перейти на вкладку **Активная защита**:

Image not found or type unknown

Здесь нужно выключить опцию **Secure DNS** нажав на нее:

Image not found or type unknown

И выбрать пункт **Остановить навсегда**:

Image not found or type unknown

На вопрос антивируса, действительно ли мы хотим отключить защиту, отвечаем утвердительно:

Image not found or type unknown

Опция станет серым цветом. Нажимаем **OK**:

Image not found or type unknown

Настройка закончена. Перезагружаем компьютер и проверяем, что фильтрация SkyDNS работает корректно.

Как правильно описать проблему при обращении в техническую поддержку SkyDNS

Для того, чтобы Ваш вопрос в техническую поддержку был рассмотрен и решен как можно быстрее, хотим обратить Ваше внимание на составление самого запроса.

Постарайтесь максимально полно описать возникшую проблему, следуя перечисленным ниже пунктам:

1. Укажите Ваши контактные данные - e-mail регистрации в SkyDNS и контактный e-mail, если он отличается от регистрации. Также если вам требуется очень срочная поддержка, вы можете указать контактный телефон.
2. Постарайтесь как можно подробнее описать схему Вашей локальной сети, какие устройства или ПО Вы используете. Важно указать, какую операционную систему Вы используете на устройстве, где возникла проблема.
3. Опишите Вашу схему подключения к интернету. Могут быть разные варианты: провод провайдера напрямую к компьютеру, через роутер или другой шлюз, используется ли прокси сервер в Вашей сети. Будет плюсом, если укажите Вашего провайдера, через которого подключаетесь к интернет.
4. Укажите каким образом настроена фильтрация и подключение к сервису SkyDNS. Это может быть агент SkyDNS, установленный на компьютер, роутер Zyxel Keenetic с плагином SkyDNS, или же через роутер другого производителя с привязкой IP адреса в личном кабинете. В последнем случае укажите, используете ли Вы статический или динамический IP адрес. Используется ли Active Directory в Вашей сети, как настроен Ваш DNS сервер в этом случае. Для роутеров укажите точную модель устройства и марку, а для роутеров ZyXEL желательно указать текущую версию прошивки.
5. Опишите непосредственно саму проблему, на каком сайте вы видите проблему, на каком профиле настроек она возникла и примерное время возникновения проблемы. В случае проблем наблюдаемых в браузере, будет не лишним написать какие именно ошибки показывает браузер. Скриншоты к описанию проблемы будут всегда плюсом. Дополнительно можете прислать вывод команд:

```
ipconfig /all
nslookup site.com
nslookup site.com 193.58.251.251
#где site.com - имя сайта, заблокированного фильтром (например у меня заблокированы
соц. сети,
#можно указать такую команду nslookup vk.com). Вторая команда отличается от первой
тем, что
#проверяется по конкретному серверу. Приведенные команды необходимо запускать в
режиме командной строки.
```

Пример корректного запроса в техническую поддержку:

Мой аккаунт moi-email@email.ru. У меня дома используется роутер Zyxel Keenetic Lite III с модулем SkyDNS. Дома 1 стационарный компьютер и 1 ноутбук. На компьютере фильтрация работает, на ноутбуке не фильтруется ни один сайт. ОС ноутбука Windows 8.1. Профиль настроек для ноутбука "Детский".

Вывод команд из п.5 прикладывается.

Инструкция по работе с WireShark

В этом руководстве показано, как устранять проблемы, когда приложение или домен не работают должным образом и не имеют доступ по сети.

Установка

Загрузите и установите Wireshark. Выберите версию x32, если вы не знаете архитектуру своей операционной системы: https://www.wireshark.org/download.html

Согласно требованиям Wireshark, вам необходимо будет установить драйвер захвата WinPcap или Npcap. Пожалуйста, выберите наиболее подходящий для вас вариант.

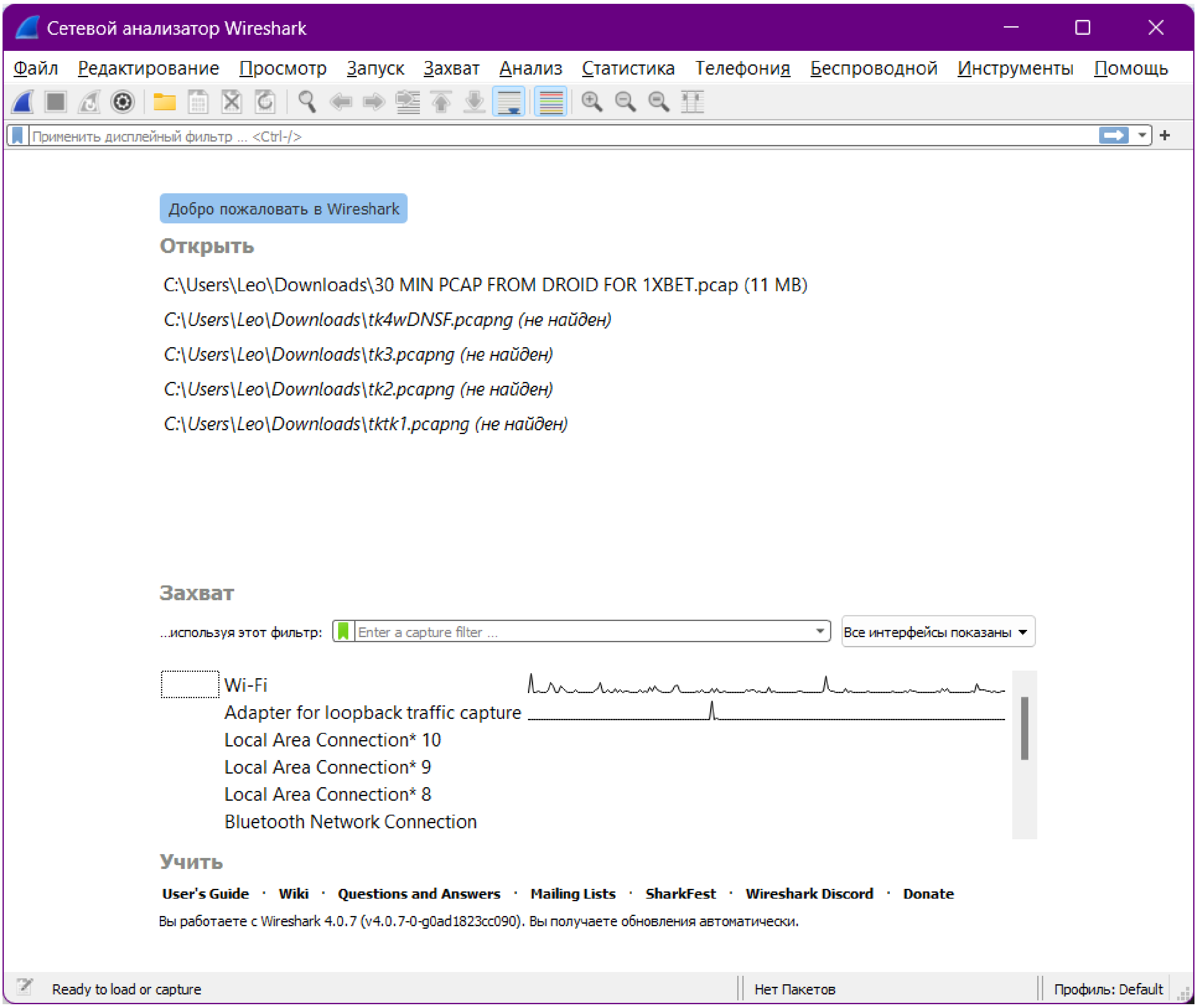
Как использовать приложение

После установки Wireshark систему следует перезагрузить.

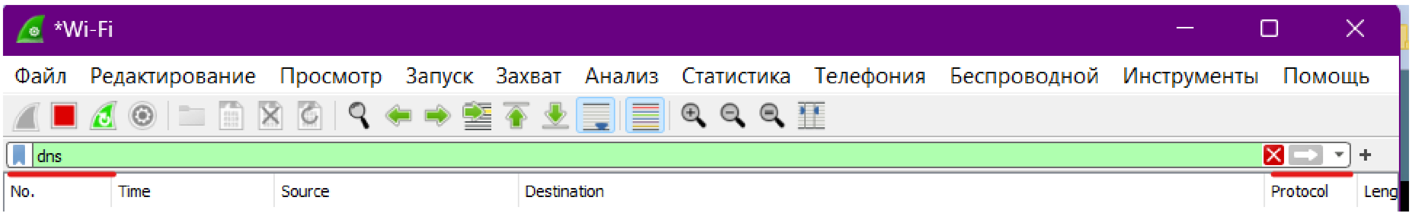
Пожалуйста, запустите приложение Wireshark с правами администратора. При первом запуске вам будет предложено выбрать интерфейс для захвата трафика. Пожалуйста, выберите один из сетевых адаптеров:

Adapter for loopback traffic capture - если вы используете агент SkyDNS.

Wi-Fi или Local Area Connection - если фильтрация настроена на сетевом уровне.



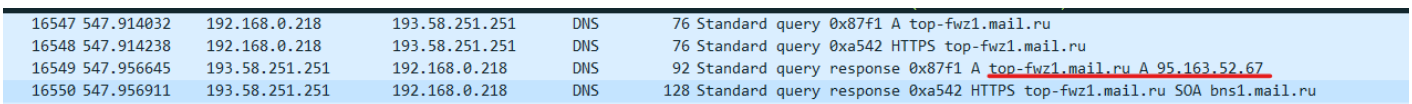
После запуска процесса отслеживания пакетов, настройте протокол захвата, введя DNS в поле **Фильтр отображения** и нажав кнопку **Ввод**.



На этом шаге все сетевые запросы будут фильтроваться, чтобы отображались только DNS-запросы.

Запустите приложение, требующее устранения неполадок.

На экране Wireshark отобразится список адресов имен хостов, соответствующие им IP-адреса и дополнительная служебная информация.



В приведенном выше примере, домен top-fwz1.mail.ru был разрешен в IP-адрес 95.163.52.67 - адрес запрашиваемого ресурса. Это означает, что вышеуказанный домен сервиса Mail.ru успешно резолвится через сервера фильтрации СкайДНС. Если вместо реального адреса запрашиваемого ресурса вы увидите адрес страницы блокировки СкайДНС, это означает что доступ к запрашиваемому ресурсу был заблокирован.

Ниже указаны адреса страниц блокировок СкайДНС:

```
193. 58. 251. 1
193. 58. 251. 2
193. 58. 251. 3
193. 58. 251. 4
193. 58. 251. 12
```

Как решить проблему?

Найдите категорию домена с помощью онлайн-инструмента SkyDNS:
https://www.skydns.ru/check/

После этого проверьте, не заблокирована ли эта категория на панели управления SkyDNS или нет ли домена в списке запрещенных.

Использование Wireshark для захвата DNS-запросов обычно достаточно для решения любых проблем, связанных с веб-фильтрацией DNS. Однако вы также можете попробовать расширенные функции Wireshark — захват сетевых пакетов, анализатор пакетов и захват USB-трафика.