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.

Revision #6
Created 22 November 2023 11:49:56 by Виктор
Updated 14 February 2024 05:40:02 by Виктор