Архитектура и системные требования

Решение для провайдеров состоит из трех компонентов:

- фильтрующего DNS-сервера,
- веб-приложения **страничка блокировки**
- веб-приложения **ISP Go API** для управления настройками пользователей

Имеются зависимости от следующих внешних программных продуктов:

- `nginx` используется как reverse proxy для странички блокировки и ISP Go API
- `redis` является хранилищем данных
- `rsync` нужен для скачивания обновлений фильтра с серверов SkyDNS

Пользователям, включивших у провайдера услугу фильтрации контента, средствами самого провайдера выдается адрес фильтрующего DNS-сервера или производится перенаправление на него их DNS запросов. С помощью ISP Go API (т.е. путем особых HTTP-запросов, выполняющихся из скриптов провайдера) этот DNS-сервер информируется о том, какие категории сайтов не надо показывать пользователю. Также в API поддерживаются индивидуальные пользовательские черный и белый списки и их глобальные варианты, действующие для всех пользователей.

Если пользователь наберет в браузере адрес запрещенного сайта, то фильтрующий DNS-сервер ответит на DNS-пакет от браузера IP-адресом страницы блокировки, и браузер загрузит именно ее. На странице блокировки можно прочитать, почему доступ к данному домену заблокирован. Дизайн страницы блокировки при желании можно изменить.

Машина, на которой наше решение можно протестировать (и даже использовать с сотней пользователей), должна удовлетворять следующим минимальным требованиям:

Рекомендуемые системные требования:
Среднее использование службы фильтрации ISP-Go охватывает несколько тысяч запросов в секунду. Для обеспечения этой производительности необходимо соответствие рекомендуемым системным требованиям.

- Архитектура x86-64
- Установлен Debian 8, 9 или 10 amd64
- 2 ГБ ОЗУ

- 2 ГГц 4-ядерный процессор
- 80 ГБ свободного места на диске
- Сетевая карта 1 Гбит\с

Высокопроизводительные системные требования:
Высокопроизводительное использование службы фильтрации ISP-Go охватывает ~0,5 миллиона запросов в секунду или более. Для обеспечения этой производительности необходимо соответствие рекомендуемым системным требованиям.

- Архитектура x86-64
- Установлен Debian 8, 9 или 10 amd64
- 8 или более ГБ ОЗУ
- 2 ГГц 8-ядерный процессор или более
- 160 ГБ или более свободного места на диске
- Сетевая карта 2,5 Гбит\с или две сетевые карты 1 Гбит\с

Решение распространяется в виде deb-пакета для архитектуры amd64.

Для функционирования нашего решения у провайдера уже должен существовать обычный рекурсивный кеширующий DNS-сервер. Bind 9 или Unbound с настройками по умолчанию на другой машине вполне подходит, или можно поставить один из этих DNS-серверов на ту же машину и сконфигурировать, чтобы он слушал только адрес 127.0.0.1.

Фильтрующий DNS-сервер (`isp-go-dnsproxy`) передает все незаблокированные запросы кеширующему, а сам кешированием не занимается. Имеется возможность пропускать все запросы всех пользователей (даже тех, для которых услуга фильтрации выключена) через фильтрующий DNS-сервер без фильтрации запросов.

Веб-приложения **страничка блокировки** и **ISP Go API** выполнены в виде отдельных демонов, каждый из которых слушает свой порт на адресе 127.0.0.1. Для передачи запросов из внешней сети к этим веб-приложениям используется nginx, он слушает порт 80 на внешнем сетевом интерфейсе. Распределение запросов по этим веб-приложениям осуществляется, исходя из заголовка Host: в HTTP-запросах. Запросы, поступающие на выделенное для ISP Go API доменное имя, передаются в это веб-приложение, а все остальные запросы попадают на страничку блокировки.

У провайдера должна существовать какая-либо сущность (биллинг, система авторизации), которая "знает" соответствие между IP-адресами и пользователями. Необходимым условием для внедрения решения SkyDNS для провайдеров является возможность в существующем биллинговом решении запуска скриптов при выдаче IP-адреса пользователю и (желательно) при отключении пользователя, а также наличие специалиста, способного написать скрипты, обращающиеся к веб-приложению ISP Go API по HTTP при этих событиях.

Для использования продукта конечным пользователем необходимо поменять настройки DNS на конечном устройстве. Специальных требований к конечным устройствам нет.

Сервер, на котором установлен `isp-go-dnsproxy`, должен иметь возможность отправлять HTTP POST запросы на сервер www.skydns.ru

Revision #3
Created 8 December 2023 12:17:34 by Виктор
Updated 15 October 2024 05:15:11 by Leo