Настройка nginx

Роль Nginx в решении для провайдеров состоит в следующем:

- отделение запросов к API от запросов к странице блокировки
- проксирование этих запросов на соответствующие веб-приложения
- ограничение доступа к API

Для корректного разделения запросов необходимо прописать доменное имя, используемое для управления фильтрацией через API, в директиву server_name в файле `/etc/nginx/sites-available/isp-go-api`, вместо значения api.ispgo, которое там прописано по умолчанию. Все остальные запросы пойдут на виртуальный хост, настроенный в файле `/etc/nginx/sites-available/isp-go-blocked`, за счет наличия там модификатора default_server в директиве listen. Допускается создавать другие виртуальные хосты, со следующими оговорками:

- в каждом виртуальном хосте должно быть прописано имя сервера с помощью директивы server_name;
- не допускается использование модификатора default_server;
- не рекомендуется использование протокола https - в этом случае, вместо сброса соединения, у пользователей, обращающихся к запрещенным сайтам по https, будет появляться предупреждение о невалидном сертификате, и неизбежно возникнут (необоснованные) обвинения от пользователей в перехвате защищенного траффика.

Для корректного проксирования необходимо, чтобы адреса и порты, упоминаемые в директиве proxy_pass в файлах `/etc/nginx/sites-available/isp-go-api` и `/etc/nginx/sites-available/isp-go-blocked`, соответствовали адресам и портам, которые прослушиваются соответствующими веб-приложениями. По умолчанию это так. См. ключи listen в секциях `[blockpage]` и `[api]` в файле `/etc/isp-go/config.ini`.

Доступ к API ограничивается с помощью директив allow и deny. Директивы обрабатываются по очереди сверху вниз до первого соответствия. Конфигурация по умолчанию разрешает доступ только с адреса 127.0.0.1. Следует разрешить доступ с сервера, на котором установлена биллинговая система. Ни в коем случае нельзя разрешать доступ к API с недоверенных (в том числе пользовательских) систем, т.к. при наличии доступа к API злоумышленник может изменять любые настройки фильтрации у любых пользователей.

Для применения настроек надо заставить Nginx перечитать конфигурационные файлы:

```
service nginx reload
```

Более подробную информацию о настройке nginx можно найти на странице проекта:

http://nginx.org/ru/docs/

Revision #2
Created 8 December 2023 12:19:04 by Виктор
Updated 8 December 2023 12:44:53 by Виктор