**РАЗРАБОТКА ГЛАВНОГО СЕРВЕРА**

Главный сервер представляет собой docker-compose сборку, реализующую связь пользователей с серверами WG. Для авторизации пользователей используется JWT – access и refresh. Приватный ключ подписи предлагается генерировать прямо в контейнере. Главный сервер может управлять VPN-серверами, которые, скорее всего будут вовсе отклонять все TCP-соединения помимо запросов с IP-адреса главного сервера, что обеспечивает высочайшую устойчивость к DoS-атакам, в то время как сам Wireguard, работающий через UDP, также устойчив к DoS архитектурно:

*In fact, the server does not even respond at all to an unauthorized client; it is silent and invisible. The handshake avoids a denial of service vulnerability created by allowing any state to be created in response to packets that have not yet been authenticated.  
 -* wireguard.com/protocol

Главному серверу в виде файла передаются списки серверов с ключами доступа к ним, названиями, необходимым уровнем пользователя для подключения. Предлагается на VPN-серверах отключить очищение пиров, а делать это вручную, регулярно получая их список, тем самым и проверяя состояние серверов.

Главный сервер оперирует базой данных, за которую предлагается выбрать PgSQL в связи с наличием опыта. Она запускается в отдельном контейнере на базе образа postgres:alpine.

Третьим контейнером является nginx. Его функция будет состоять в ограничении запросов в минуту, управлении TLS и прочие.

**Выработка политики подключения**

Базовой единицей подключения является устройство пользователя. Идентификатором устройства является публичный ключ Wireguard. Каждому пользователю выдаётся лимит устройств. Предлагает бесплатным пользователям выдать лимит в 1 устройство, платным – в 5 устройств. Для удобства каждому устройству выдаётся имя. В качестве имени предлагается выбрать два случайных слова: цвет и животное, чтобы облегчить запоминание. Если пользователь пытается войти на новом устройстве, но лимит уже исчерпан, ему предлагается удалить одно из устройств.