**ПРОЕКТИРОВАНИЕ VPN-СЕРВЕРА**

Данная глава описывает прототипирование базовой единицы разрабатываемого проекта. Сам VPN сервер представляет из себя Wireguard сервис и ASP-приложение, которое, по запросу, выполняет с ним определенные манипуляции – добавляет и удаляет пиры. Данные приложения запускаются в одном контейнере, основывающемся на docker-образе linux.

Функционал ASP-приложения состоит в принятии запросов от удаленного сервера, проверке действительности API-ключа (возможно написание авторизации по API-ключу с дальнейшим использованием JWT, хотя данный функционал не кажется существенно полезным, т.к. все подключения должны гарантировать TLS), выполнении действия. Само приложение, как предполагается, должно хранить ключи в виде их SHA512-хеша, не храня оригиналы, т.к. это не имеет смысла, при этом создаёт концептуальную уязвимость в связи с наличием ключей в открытом виде как таковых, что не соответствует принципу secure-by-design. Приложение должно быть способно изменять конфигурацию Wireguard посредствам выполнения CL-команд.

Функционал Wireguard является стандартным и состоит в прослушивании порта 51820 (стандартный порт wg), маскировании трафика (англ. masquerade), перенаправлении на внешний адрес. Пиры должны добавляться и удаляться по CL-команде от ASP-приложения. Поскольку Wireguard работает в контейнере, существует два варианта перехвата из внешней сети: непосредственное прослушивание докером порта 51820, либо перехват UDP-трафика с помощью NGINX с дальнейшим перенаправлением. На текущем этапе не видно существенных причин для использования прокси помимо унификации, т.к. весь остальное трафик (исходя их опыта разработки), передаваемый, как правило, через TCP, всё-таки всегда перехватывает с помощью NGINX.