Судя по вводным у нас молодая компания сотрудники которой не работают с конфиденциальной и критически важной информацией, соответственно можно допустить размещение удостоверяющего центра и VPN сервера на одной ВМ. Как временаня мера: Файл с ключем удостоверяющего центра ( /usr/share/easy-rsa/pki/private/ca.key) следует зашифровать программой gpg

В процессе развития инфраструктуры можно запланировать разведение сервисов по разным ВМ.

На сервере необходимо создать нового юзера, отличного от root, дав ему группу прав sudo, доступ к серверу есть только у администратора.

**Установка Удостоверяющего Центра и создание сертификата Центра**

Процедура развертывания удостоверяющего центра реализована скриптом и прилагающимся к нему deb-пакетом, который несет нужные конфигурационные файлы. Скрипт inst\_easy\_rsa.sh и пакет rsa\_0.1-1\_all.deb кладутся в папку /tmp сервера. Если необходимо изменить пути – необходимо поправить соответствующие переменные в начале скрипта.

**Установка VPN Сервера, создание сертификатов сервера и клиента, сетевые настройки, запуск службы**

Вся процедура реализована скриптом inst\_openvpn.sh и прилагающимся к нему deb-пакетом vpn-cl-conf\_0.1-1\_all.deb, который несет нужные конфигурационные файлы. В этом же скрипте производятся необходимые настройки портов и маршрутизации трафика, производится запуск сервиса vpn-сервера.

Процедура генерации ключа и сертификата клиента подразумевается на стороне сервера.

Администратор любым способом получает от клиента его данные (ФИО и т.д) и генерирует комплект ключ\сертификат. После формирует файл конфигурации \*.ovpn и передает этот файл клиенту с соответствующими комментариями по подключению VPN-клиента.

Создание первого клиентского пакета уже включено в скрипт установки VPN сервера inst\_openvpn.sh

Секретный ключ как сервера так и сертификата перемещается в соответствующую папку VPN сервера, тем самым изолируется от Центра сертификации (имитация разделения сервисов по двум серверам)

Последующие генерации клиентских ключей и конфигурационных файлов осуществляются скриптом client-maker.sh Путь к конечному файлу \*.ovpn задается в $OUTPUT\_DIR

В перспективе с ростом нагрузки процесс будет автоматизирован так, чтобы клиент на своей стороне генерировал ключ, создавал запрос на сертификат \*.csr и передавал на флешке системному администратору .

**Все скрипты и deb-пакеты кладутся в папку /tmp сервера. Если необходимо изменить пути – необходимо поправить соответствующие переменные в начале скрипта.**