**Руководство по развертывания и настройке VPN- сервера**

1. Для использования vpn-сервера необходима машина с установленной любым удобным способом ОС Linux с внутренним IP-адресом 10.128.0.11 и именем vpn, а так же должен быть развернут и настроен удостоверяющий центр. Еще нужно создать пару ssh-ключей и обменяться публичным ключом с каждой машиной (bkp1,bkp2, ca, monitoring).
2. Создаем в домашней директории пользователя (имя пользователя должно быть **user**) папку **artefacts**, куда копируем скрипты автоматизации и установочные пакеты.
3. Следующим шагом необходимо создать ssh-ключ и обменяться ним с удостоверяющим центром.
4. Для развертывания openVPN сервера необходимо запустить скрипт **vpnDeploy.sh** от имени суперпользователя. В процессе старта скрипт запросит имя пользователя и ip-адрес удостоверяющего центра.

Данный скрипт совершит следующие действия:

* Установит часовой пояс по Москве и синхронизирует с ним время.
* внесет правки в файл конфигурации ssh и установит правила: запрет входа от рута, подключение только по ключам, запрет на подключение по пустому паролю, запрет на подключение по паролю.
* Далее обновит кеш пакетов и установит пакет **Openvpn, prometheus-node-exporter, iptables и apache2-utils:**

**sudo apt update && sudo apt install -y openvpn prometheus-node-exporter iptables apache2-utils**

* Запустит скрипт **vpnIPtablesRules.sh**, который применит правила для фаервола.
* Перенесет корневой сертификат и сертификат сервера впн с машины удостоверяющего центра в домашнюю папку сервера впн командой scp

**scp user\_name@ip\_address:/home/user\_name/easy-rsa/pki/ca.crt /home/user\_name/**

**scp user\_name@ip\_address:/home/user\_name/easy-rsa/pki/issued/server.crt /home/user\_name/**

Затем эти файлы переместит в директорию **/etc/openvpn/server/**

* Для повышения уровня безопасности добавит дополнительный секретный ключ для использования tls-шифрования между клиентом и сервером vpn.

Команда **openvpn --genkey secret ta.key**

* Затем этот файл будет перемещен в директорию **/etc/openvpn/server/**
* Развернет файл конфигурации сервера из deb-пакета **openvpn-server-config.deb**
* Далее добавит vpn-сервер в автозагрузку: **systemctl enable openvpn,**

активируем сервис командой: **systemctl -f enable** [**openvpn-server@server.service**](mailto:openvpn-server@server.service) **,**

и запустит процесс: **systemctl start openvpn-server@server.service**

* Далее активирует демон для системы бекапа rsync - в файл **/etc/default/rsync** запишется строка

**RSYNC\_ENABLE=true,** создаст директорию для файлов rsync и сгенерирует файл конфигурации **/etc/rsyncd.conf** где указаны адреса в сети клиентов копирования rsync и директории для бекапа.

- Установит экспортер для openvpn **dpkg -i /home/$vpnUser/artefacts/openvpn-exporter\_0.1-1.deb**

**-** Запросит ввести DNS-адреса каждой машины в инфраструктуре. Например ca.ru-central1-a.ru

- Скопирует с машины центра сертификации ключ и сертификат для экспортера прометеус.

- Создаст директорию для экспортера прометеус **/opt/node\_exporter/,** перенесет в нее ключ и сертификат для локального экспортера и корневой сертификат, запросит логин и пароль для подключения к экспортеру (ввести логин admin и пароль), что и будет записано в файл конфигурации **/opt/node\_exporter/web.yml**

- Создаст юнит на автозапуск экспортеров и в конце перезапустит их.

После всего вышеописанного сервер впн будет готов к работе. Чтобы клиенты могли генерировать себе файл конфигурации необходимо каждому клиенту передать файлы **ta.key** и **ca.crt.**