

[сервисы](#), [табуретка](#), [демо](#)

Сервис Пользовательский VPN

[Пользовательский VPN](#)

Заказчик

[Александров Назар Иванович](#)

Назначение

Предоставить возможность пользователям подключаться удаленно к внутренним ресурсам компании с разграничением доступности ресурсов для каждого пользователя

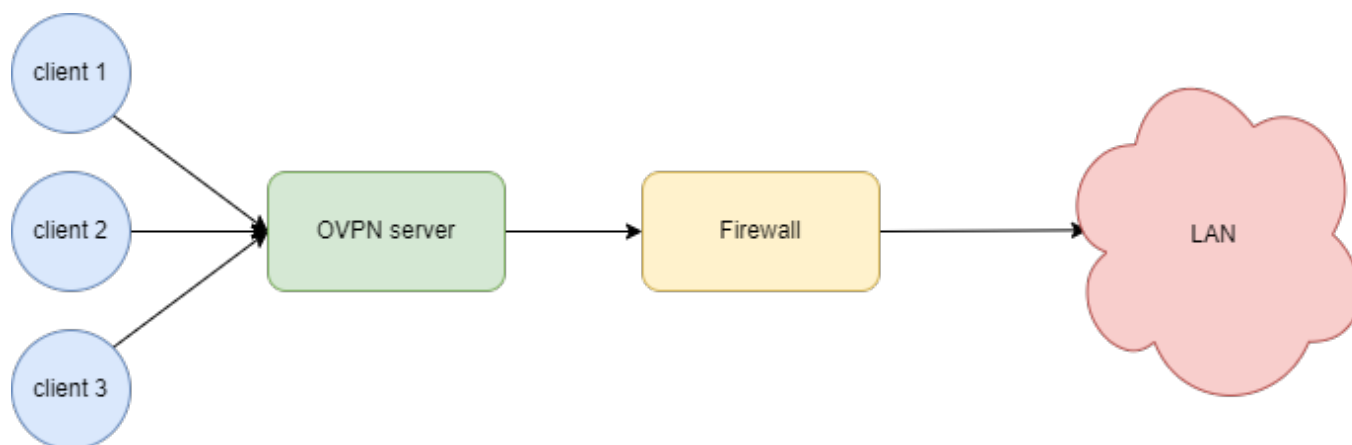
Описание

- OpenVPN сервер и скрипт выпуска клиентских конфигов.
- IP адреса клиентам выдаются статические через CCD файлы, что позволяет четко идентифицировать каждого клиента по IP и управлять его доступом на FW
- Учет свободных и занятых адресов ведется скриптом автоматически в инвентори/сети [10.50.50.0/24 \(CHL_OVPN_LAN\)](#) - челябинские клиенты, [10.20.50.0/24 \(MSK_OVPN_LAN\)](#) - московские: скрипт закрепляет за новым конфигом первый свободный IP

Если при генерации нового конфига скрипт найдет одноименного пользователя в инвентори - закрепит за ним выделенный IP (иначе просто сделает описание к IP адресу в виде ovpn-username)

Доступ

Доступ отзывается/активируется удалением/восстановлением CCD файлов: сервер настроен так, что на каждый конфиг должен присутствовать одноименный CCD файл, удаление CCD деактивирует конфиг (правда не рвет активную сессию) Дополнительно индивидуальный сетевой доступ клиентов регулируется на FW [MSK-GW](#) и [CHL-GW](#)



Инструкция

```
/etc/openvpn/usr.new pupkin_ii
```

Создает новый конфиг для *pupkin_ii*. Конфиг располагается в папке **/etc/openvpn/clients/taburetk-pupkin_ii**

- taburetk-pupkin_ii.conf - для linux
- taburetk-pupkin_ii.ovpn - для windows клиента

Содержимое файлов ничем не отличается, просто в разных окружениях по умолчанию используются разные расширения. При создании смотрит какой первый адрес свободен в подсети местной площадки.

- прописывает его в CCD для пользователя pupkin_ii
- прописывает в инвентори комментарий для занятого IP (название VPN конфига) - тем самым «занимая его» во избежание коллизий
- если в инвентори есть пользователь pupkin_ii - привязывает к нему занятый IP

Созданный CCD находится в папке с конфигом и называется **ccd**, по умолчанию туда прописывается только назначение IP адреса клиенту, но содержание можно изменить по своему усмотрению.

Активация доступа

По умолчанию новый конфиг не активирован

```
/etc/openvpn/usr.enable pupkin_ii
```

или **_enable** в папке конфига. Конфигурация сервера такова, что при подключении он ищет файл /etc/openvpn/ccd/pupkin_ii, а скрипт делает линк /etc/openvpn/clients/taburetk-pupkin_ii/ccd → /etc/openvpn/ccd/pupkin_ii

Отзыв доступа

```
/etc/openvpn/usr.disable pupkin_ii
```

или **_disable** в папке конфига а скрипт удаляет линк /etc/openvpn/clients/taburetk-pupkin_ii/ccd → /etc/openvpn/ccd/pupkin_ii

Пересборка CCD

Может понадобиться при появлении новых сетей Удалить существующий ccd файл и

```
/etc/openvpn/usr.new pupkin_ii
```

или **_renew** в папке конфига

При этом закрепленный за пользователем IP сохранится

Отказоустойчивость

Не предусмотрена

Резервное копирование

RPO - достаточно ежедневной копии папки /etc/openvpn RTO - на усмотрение заказчика

Мониторинг

В zabbix-agent зарегистрирована метрика **ovpn.users.online**

/etc/zabbix/zabbix_agentd.d/userparam_ovpn.conf

```
UserParameter=ovpn.users.online[*],/etc/zabbix/scripts/ovpn.userlist.sh  
/var/log/openvpn.status
```

Который парсит файл /var/log/openvpn.status скриптом

[/etc/zabbix/scripts/ovpn.userlist.sh](#)

```
#!/bin/bash  
  
f=$1  
  
userlist=`cat $f | sed -n '/^Common Name/,/^ROUTING TABLE/ p' | tail -n +2  
| head -n -1`  
rtable=`cat $f | sed -n '/^ROUTING TABLE$/,/^GLOBAL STATS$/ p`  
  
echo "$userlist" | \  
while read userline; do
```

```
username=`echo $userline|cut -d, -f1`  
since=`echo $userline|cut -d, -f5`  
utcsince=`date --date="$since" +%s`  
localutc=$(( $utcsince + 18000 ))  
localsince=`date --date="@$localutc" +%Y-%m-%d %H:%M:%S`  
localip=`echo "$rtable"|grep $username|cut -d, -f1`  
echo $username,$localip,$localsince  
done
```

Логирование

Логи расположены по пути /var/log/openvpn-server.log /var/log/openvpn-status Хранить не менее 60 дней

Отказоустойчивость

Предусмотрена ли, если предусмотрена то как реализуется

Резервное копирование

Как делается, какие предъявлены требования по RPO и RTO

Логирование

Требования предъявленные к логированию (глубина хранения, подробность) Детали логротейта

Мониторинг

Задача

Что нужно мониторить Кого нужно оповещать

Реализация

Как настроены метрики, триггеры, оповещения

Журнал изменений доступа

если доступ к сервису не контролируется, то эту секцию нужно убрать за ненадобностью

Дата	Изменение	Комментарий
------	-----------	-------------

30.06.2020	Добавлен доступ Ревякину А.А.	СЗ №12345 в ELMA (Утверждена Бондаревой и Комиссаровым)
01.07.2020	Добавлен доступ из подсети 10.10.30.0/24	Письмо комиссарова по почте (Тема FW:Доступ из сети ИТ)

From:

<http://wiki.reviakin.net/> - Wiki

Permanent link:

http://wiki.reviakin.net/%D1%81%D0%B5%D1%80%B2%D0%B8%D1%81%D1%88:%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%B8%D1%8C%D1%81%D0%BA%D0%B8%D0%B9_vpn

Last update:

2023/09/18 15:13

