

OpenVPN и маршруты в клиентские сети

Иногда при использовании OpenVPN бывает необходимо попадать с сервера в клиентские сети. Например, к серверу OpenVPN подключается два клиента с подсетями 192.168.100.0/24 и 192.168.101.0/24 и с сервера необходимо добавить маршруты в подсети этих клиентов. Стандартными настройками это не делается, нужно прикручивать скрипты.

Устанавливаем утилиту ipcalc:

```
sudo apt install ipcalc
```

Создаем скрипты /etc/openvpn/client-connect.sh и /etc/openvpn/client-disconnect.sh

/etc/openvpn/client-connect.sh

```
#!/bin/bash
# Скрипт выполняется при подключении каждого клиента

# Логируем запуск
logger -t openvpn "Client $common_name connected with IP $ifconfig_pool_remote_ip"

# Проверяем CCD файл клиента
if [ -f "/etc/openvpn/ccd/$common_name" ]; then
    # Ищем iroute директивы
    while IFS= read -r line; do
        if [[ "$line" =~ ^iroute[[:space:]]+([0-9\.]+)[[:space:]]+([0-9\.]+) ]]; then
            network="${BASH_REMATCH[1]}"
            netmask="${BASH_REMATCH[2]}"

            # Конвертируем в CIDR
            cidr=$(ipcalc "$network" "$netmask" | grep 'Netmask' | awk {'print $4'})

            if [ -n "$cidr" ]; then
                # Добавляем маршрут на сервере
                sudo ip route add "$network/$cidr" via "$ifconfig_pool_remote_ip" dev "$dev" 2>/dev/null

                # Логируем действие
                logger -t openvpn "Added route $network/$cidr via $ifconfig_pool_remote_ip (client: $common_name)"

                # Выводим в лог OpenVPN
                echo "$(date): Added route $network/$cidr via $ifconfig_pool_remote_ip for client $common_name"
            fi
        fi
    done
```

```
done < "/etc/openvpn/ccd/$common_name"
fi

exit 0
```

/etc/openvpn/client-disconnect.sh

```
#!/bin/bash
# Скрипт выполняется при отключении клиента

# Проверяем CCD файл клиента
if [ -f "/etc/openvpn/ccd/$common_name" ]; then
    while IFS= read -r line; do
        if [[ "$line" =~ ^iroute[[:space:]]+([0-9\.]+)[[:space:]]+([0-9\.]+)
    ]]; then
            network="${BASH_REMATCH[1]}"
            netmask="${BASH_REMATCH[2]}"

            cidr=$(ipcalc "$network" "$netmask" | grep 'Netmask' | awk
{'print $4'})

            if [ -n "$cidr" ]; then
                # Удаляем маршрут
                sudo ip route del "$network/$cidr" 2>/dev/null

                # Логируем
                logger -t openvpn "Removed route $network/$cidr (client:
$common_name disconnected)"
            fi
        fi
    done < "/etc/openvpn/ccd/$common_name"
fi

exit 0
```

Так же необходимо добавить в конфиг OpenVPN несколько строк, которые добавят вызов скриптов при подключении/отключении клиента.

```
script-security 3 # или 2, если 3 не работает
client-connect /etc/openvpn/client-connect.sh
client-disconnect /etc/openvpn/client-disconnect.sh
```

Добавляем в конфигурационный файл клиента:

```
ifconfig-push 172.16.1.10 255.255.255.0
iroute 192.168.100.0 255.255.255.0
```

172.16.1.10 - IP который будет назначен клиенту при подключении

iroute 192.168.100.0 255.255.255.0 - добавляет адрес подсети клиента, который и будет добавляется в маршруты

From:

<https://wiki.rtzra.ru/> - RTzRa's hive

Permanent link:

<https://wiki.rtzra.ru/software/openvpn/openvpn-routes-to-client-network>

Last update: **2025/12/26 17:11**

