Настройка SSTP сервера на Almalinux 8

1. Подготовка окружения

Установим необходимые утилиты для компиляции и работы сервера:

```
sudo dnf install wget make gcc binutils tar -y
```

(При необходимости можно заранее включить EPEL-репозиторий для дополнительных пакетов:)

```
sudo dnf install epel-release -y
```

2. Скачивание и сборка SoftEther VPN Server

```
wget
"https://www.softether-download.com/files/softether/v4.41-9787-rtm-2023.03.14-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/softether-vpnserver-v4.41-9787-rtm-2023.03.14-linux-x64-64bit.tar.gz"
tar -xzf softether-vpnserver-*.tar.gz
cd vpnserver
make
cd ..
sudo mv vpnserver /usr/local/
```

3. Настройка прав и SELinux

```
sudo chmod -R 600 /usr/local/vpnserver/*
sudo chmod 700 /usr/local/vpnserver/vpnserver /usr/local/vpnserver/vpncmd
#sudo chcon -Rv -u system_u -t bin_t /usr/local/vpnserver/vpnserver
#sudo semanage fcontext -a -t bin_t '/usr/local/vpnserver/vpnserver'
#sudo restorecon -v '/usr/local/vpnserver/vpnserver'
sudo semanage fcontext -a -t bin_t '/usr/local/vpnserver(/.*)?'
sudo restorecon -Rv '/usr/local/vpnserver'
```

4. Создание systemd-сервиса

Создаём файл /etc/systemd/system/softether-vpnserver.service со следующим содержимым:

```
[Unit]
Description=SoftEther VPN server
After=network-online.target
```

```
[Service]
Type=forking
ExecStart=/usr/local/vpnserver/vpnserver start
ExecStop=/usr/local/vpnserver/vpnserver stop

[Install]
WantedBy=multi-user.target
```

Перезагрузим демона и включим автозапуск:

```
sudo systemctl daemon-reload
sudo systemctl enable softether-vpnserver
sudo systemctl start softether-vpnserver
```

5. Открытие порта в брандмауэре

SSTP работает поверх SSL/TLS на TCP 443:

```
sudo firewall-cmd --zone=public --add-port=443/tcp --permanent
sudo firewall-cmd --reload
```

6. Базовая настройка SSTP-сервера через vpncmd

Запускаем утилиту управления:

```
sudo /usr/local/vpnserver/vpncmd /SERVER
```

В интерфейсе:

- Создать виртуальный хаб для SSTP:

```
HubCreate SSTP
```

- Установить пароль администратора:

```
ServerPasswordSet
```

- Включить SecureNAT (встроенный NAT/DHCP):

```
SecureNatEnable
```

- Перейти в хаб и создать VPN-пользователя:

```
Hub SSTP
UserCreate <имя_пользователя>
UserPasswordSet <имя_пользователя>
```

- Сгенерировать SSL-сертификат (замените yourdomain.com):

```
ServerCertRegenerate yourdomain.com
ServerCertGet yourdomain.com.cer
```

- Включить SSTP:

```
SstpEnable yes
```

- Выйти:

```
exit
```

Перезапустить службу softether-vpnserver:

```
sudo systemctl restart softether-vpnserver
```

7. Включить маршрутизацию и настроить NAT (маскарадинг) в Firewalld

- Добавьте в /etc/sysctl.d/99-sysctl.conf:

```
net.ipv4.ip_forward = 1
```

- Применить настройку:

```
sudo sysctl --system
```

- Включите маскарадинг:

```
sudo firewall-cmd --zone=public --add-masquerade --permanent
```

- (Опционально) Если хотите ограничить маскарадинг только для SSTP-подсети:

```
sudo firewall-cmd --permanent --direct --add-rule ipv4 nat POSTROUTING 0 \
-s 192.168.30.0/24 -o eth0 -j MASQUERADE
```

- Перезагрузите firewalld:

```
sudo firewall-cmd --reload
```

Внешний сертификат

```
sudo dnf install nginx certbot python3-certbot-nginx -y
```

```
sudo systemctl enable --now nginx
```

```
sudo firewall-cmd --zone=public --add-service=http --permanent
#sudo firewall-cmd --zone=public --add-service=https --permanent
```

```
sudo firewall-cmd --reload
```

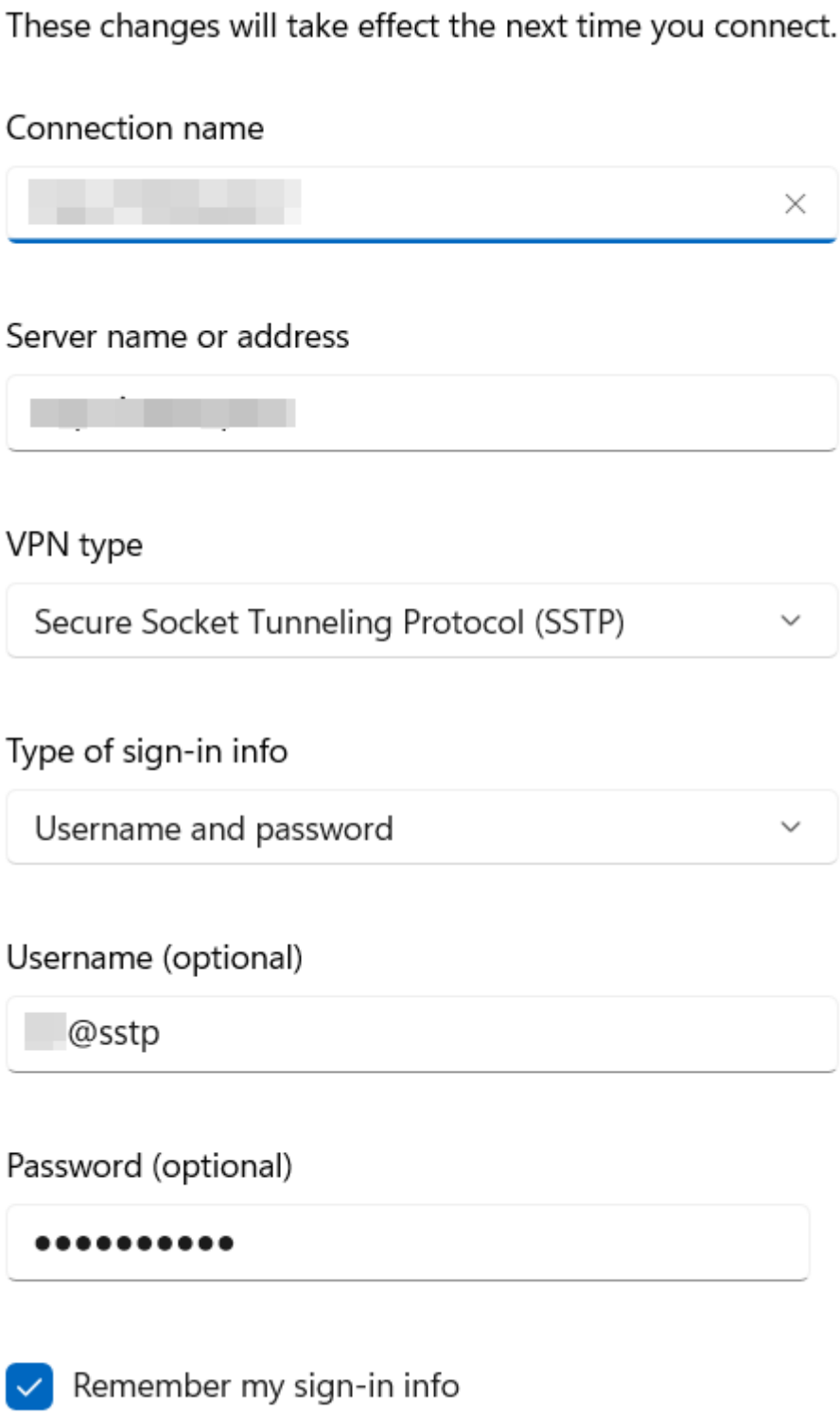
```
sudo certbot --nginx -d sstp.virtlab.space
```

```
sudo mkdir -p /etc/letsencrypt/renewal-hooks/deploy
sudo tee /etc/letsencrypt/renewal-hooks/deploy/softether-reload.sh >
/dev/null <<'EOF'
#!/bin/bash

LE_DIR="/etc/letsencrypt/live/sstp.virtlab.space"
VPN_DIR="/usr/local/vpnserver"

# Копируем свежий сертификат и ключ
cp "$LE_DIR/fullchain.pem" "$VPN_DIR/server.crt"
cp "$LE_DIR/privkey.pem"   "$VPN_DIR/server.key"

# Ставим правильные права
chmod 600 "$VPN_DIR/server.crt" "$VPN_DIR/server.key"
chown root:root "$VPN_DIR/server.crt" "$VPN_DIR/server.key"

# Перезапускаем SoftEther, чтобы он подхватил новые файлы
systemctl restart softether-vpnserver
EOF
sudo chmod +x /etc/letsencrypt/renewal-hooks/deploy/softether-reload.sh
```

```
sudo cp /etc/letsencrypt/live/sstp.virtlab.space/fullchain.pem
/usr/local/vpnserver/server.crt
sudo cp /etc/letsencrypt/live/sstp.virtlab.space/privkey.pem
/usr/local/vpnserver/server.key
sudo chmod 600 /usr/local/vpnserver/server.{crt,key}
sudo chown root:root /usr/local/vpnserver/server.{crt,key}
```

Настройка на стороне Windows клиента

1. Установить сертификат sstp.cer в хоанилище локальных доверенных корневых сертфиикатов.
2. Создать новое подключение SSTP, указав в качестве сервера dns-имя указанное в сертификате.
3. VPN type - SSTP
4. Указать имя пользователя в формате username@hub_name, т.е. username@sstp



5. В свойствах соединения на вкладке Security указать протоколы: PAP и MS-CHAPv2