SSH: Устойчивый тоннель

Иногда бывает необходимо сделать тоннель подручными средствами. OpenVPN, Wireguard и прочее это все, конечно, здорово, но для некоторых случаев избыточно.

Есть возможность быстренько настроить устойчивый тоннель средствами SSH и спрятать в нем трафик или сделать доступ к определенному сервису.

Пример: заблокирован OpenVPN до определенного сервера, нужно пробросить локальный порт чтобы было подключение через ssh-тоннель.

Что и где:

- remote-user - наш пользователь, под которым будет осуществляться подключение. Авторизация по ключам, их необходимо создать заранее
- LOCAL-IP - локальный IP, на который будет приниматься подключение
- REMOTE-IP - удаленный сервер с OpenVPN

Ставим autossh:

```
sudo apt install autossh
```

Настраиваем подключение в файле /home/remote-user/.ssh/config:

```
Host REMOTE-IP
  HostName REMOTE-IP
  User remote-user
  IdentityFile ~/.ssh/id_remote-user
  IdentitiesOnly yes
```

Создаем файл сервиса /etc/systemd/system/ssh-tunnel.service со следующим содержимым:

```
[Unit]
Description=SSH Tunnel
After=network.target

[Service]
User=remote-user
ExecStart=/usr/bin/autossh -o ServerAliveInterval=30 -o "ServerAliveCountMax
3" -M 44444 -o ExitOnForwardFailure=yes -gnNT -L LOCAL-
IP:1194:localhost:1194 remote-user@REMOTE-IP
RestartSec=15
Restart=always
KillMode=mixed

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

Запускаем:

```
systemctl daemon-reload
systemctl start ssh-tunnel.service
```

ssh, autossh, tunnel, тоннель