IT Security

- iptables setup
- WireGuard VPN Client/Server
- RSA Keys Setup

iptables setup

Настройка межсетевого экрана iptables

????????? iptables

```
sudo apt install iptables-persistent -y
```

Создание файла правил iptables

```
#!/sbin/iptables-restore
#Таблица filter и её цепочки
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p tcp -m multiport --dports 2202,80,443,587 -j ACCEPT
COMMIT
```

??????? ?????????? iptables

Применение правил из файла

```
sudo sh -c "iptables-restore < /etc/iptables/rules.v4"
```

Сохранение конфигурации в boot-правила

```
sudo sh -c 'iptables-save > /etc/iptables/rules.v4'
```

Добавление новых правил без очистки текущих

```
sudo iptables-restore -n < /etc/iptables/rules.v4
```

Очистка всех правил INPUT

```
sudo iptables -t filter -F INPUT
```

Просмотр статуса правил iptables

```
sudo iptables -n -L -v --line-numbers
```

WireGuard VPN Client/Server

Настройка WireGuard VPN Клиент/Сервер

????????? VPN ???????

```
sudo apt install resolvconf -y
sudo apt install wireguard -y
sudo touch /etc/wireguard/wg0.conf && sudo chmod 600 -R /etc/wireguard/
```

Создание конфигурационного файла

```
sudo tee /etc/wireguard/wg0.conf << 'EOF'
[Interface]
PrivateKey = <>
Address = 10.8.0.3/24
DNS = 1.1.1.1

[Peer]
PublicKey = <>
PresharedKey = <>
AllowedIPs = 0.0.0.0/0, ::/0
PersistentKeepalive = 0
Endpoint = x.x.x.x:51820
EOF
```

> Значения `PrivateKey`, `PublicKey`, `PresharedKey` берутся из файла конфигурации, созданного средствами VPN сервера.

Запуск VPN клиента

```
sudo wg-quick up wg0
```

> После запуска VPN клиента активируется сетевой интерфейс и у ВМ изменится IP адрес.
> Мы потеряем текущее SSH подключение и к ВМ и нужно будет подключиться по локальному IP внутри VPN сети.

Проверка статуса VPN

```
sudo wg show
```

Отключение VPN канала

```
sudo wg-quick down wg0
```

> Мы вновь потеряем текущее SSH подключение и к ВМ и нужно будет подключиться по публичному IP.

????????? wg-easy VPN Server Docker

Github Repo

Остановка/Удаление старых контейнеров/образов

```
docker stop wg-easy docker rm wg-easy docker pull ghcr.io/wg-easy/wg-easy docker rmi
```

Генерация bcrypt hash для создания пароля к Web Интерфейсу

```
docker run -it ghcr.io/wg-easy/wg-easy wgpw Password
```

```
PASSWORD_HASH='<pass>'
```

Первичный запуск и преднастройка нового VPN сервера

```
docker run -d \
  --name=wg-easy \
  -e LANG=en \
  -e WG_HOST=x.x.x.x \
  -e PASSWORD_HASH='<pass>' \
  -e PORT=51821 \
  -e WG_PORT=51820 \
  -v ~/.wg-easy:/etc/wireguard \
  -p 51820:51820/udp \
  -p 51821:51821/tcp \
  --cap-add=NET_ADMIN \
  --cap-add=SYS_MODULE \
  --sysctl="net.ipv4.conf.all.src_valid_mark=1" \
  --sysctl="net.ipv4.ip_forward=1" \
```

```
  --restart unless-stopped \
  ghcr.io/wg-easy/wg-easy
```

Проверка корректности отправки docker скрипта и HASH-а пароля

```
docker inspect \
 --format "$(curl -s
https://gist.githubusercontent.com/efrecon/8ce9c75d518b6eb863f667442d7bc679/raw/run.tpl)" \
 wg-easy
```

Расположение конфигурации клиентов

```
/home/xeon/.wg-easy/wg0.conf
```

RSA Keys Setup

Настройка RSA ключей

????????? RSA ?????? (??????)

RSA ????? (nix/mac)

git-scm.com Guide

```
ssh-keygen -o -t rsa -b 4096 -C xeonmp22@gmail.com
```

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/xeon/.ssh/id_rsa): home
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in home
Your public key has been saved in home.pub
```

Сгенерируется 2 файла:

- Приватный ключ `~/.ssh/home`
- Публичный ключ `~/.ssh/home.pub`

> Необходимо скопировать (в буфер обмена) текст файла публичного ключа - **home.pub**
> На клиенте достаточно оставить только приватный ключ - **home**

RSA ????? (win)

learn.microsoft.com Guide

Запустите `C:\Windows\System32\cmd.exe` от имени Администратора

```
mkdir C:\Users\%USERNAME%\.ssh cd C:\Users\%USERNAME%\.ssh
```

```
ssh-keygen -m PEM -t rsa -b 4096
```

```
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\xeon/.ssh/id_rsa): home
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in home.
Your public key has been saved in home.pub.
```

> Необходимо скопировать (в буфер обмена) текст файла публичного ключа - **home.pub**
> На клиенте достаточно оставить только приватный ключ - **home**

????????? ????????? ?????? (??????)

????????? ???? (nix/mac)

```
mkdir ~/.ssh chmod 0700 ~/.ssh
```

Создание файла публичного ключа

```
sudo tee ~/.ssh/my_key1.pub << 'EOF'
***
Вставить код публичного ключа - home.pub (из буфера обмена)
***
EOF
```

```
chmod 0600 ~/.ssh/my_key1.pub
```

Изменение конфигурации службы SSH

```
sudo tee /etc/ssh/sshd_config << 'EOF'
# Путь до публичных ключей
AuthorizedKeysFile      .ssh/my_key1.pub
# Разрешить аутентификацию по ключу
RSAAuthentication yes
PubkeyAuthentication yes
# Запрет подключатся к SSH серверу по паролю
PasswordAuthentication no
EOF
```

```
sudo service sshd restart
```

???. ????????? ???? (nix/mac)

> Необходимо скопировать (в буфер обмена) текст**НОВОГО** файла публичного ключа

```
sudo tee ~/.ssh/my_key2.pub << 'EOF'
***
Вставить код публичного ключа - home2.pub (из буфера обмена)
***
EOF
```

Изменение конфигурации службы SSH

```
chmod 0600 ~/.ssh/my_key2.pub
```

```
sudo tee /etc/ssh/sshd_config << 'EOF'
# Путь до публичных ключей
# Можно указывать несколько ключей через пробел
AuthorizedKeysFile      .ssh/my_key1.pub .ssh/my_key2.pub
EOF
```

```
sudo service sshd restart
```

?????????? ?? SSH (? ???????)

SSH (nix/mac)

```
ssh user@server-ip
# Ввести парольную фразу
```

Получение fingerprint ключа из body ключа

```
ssh-keygen -E md5 -lf ~/.ssh/.pub | awk '{print $2}'
```

SSH (win)

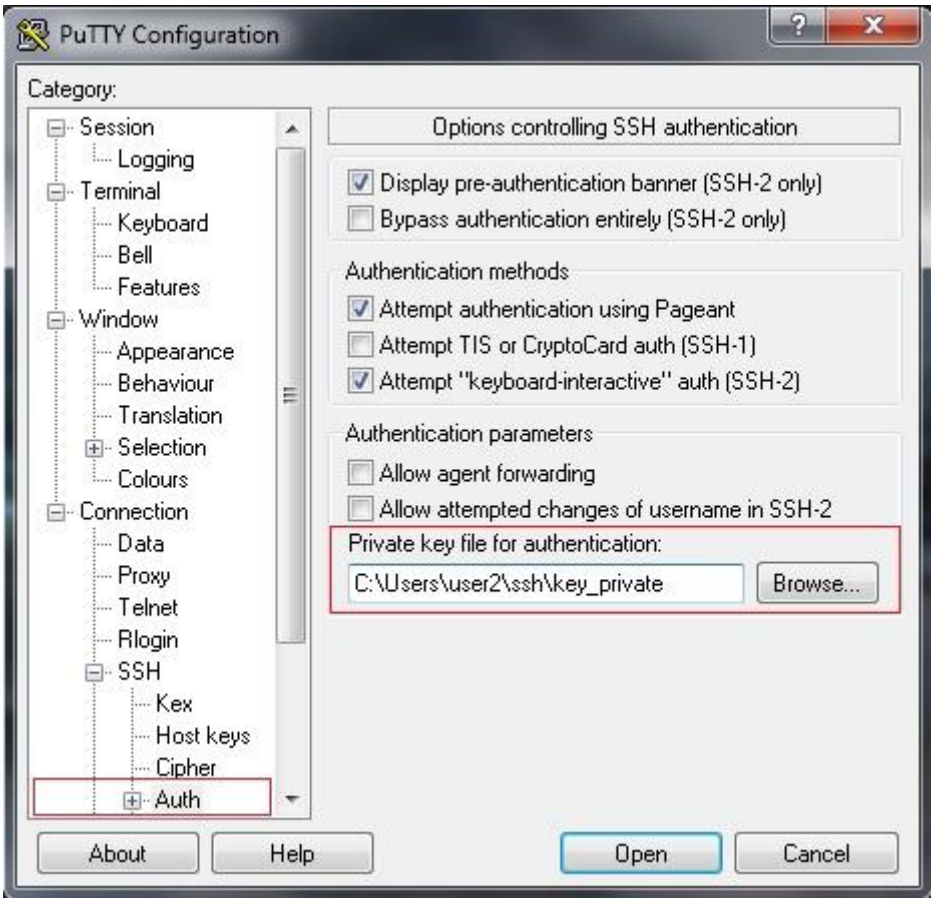
Загрузка и Установка пакета PuTTY

- Putty (файл *installer.msi)
- Либо установить ПО генерации ключей: puttygen (64-bit)

Настройка подключения к серверу в PuTTY

- Необходимо запустить PuTTY.
- Находясь в категории Session ввести данные нового сервера:

- `Host Name (or IP address)` - указываем IP (либо домен сайта)
- `Saved Sessions` - Указываем удобное вам имя сервера (может совпадать с Host Name)
- Нажимаем кнопку `Save`
- Переходим в категорию `SSH/Auth` и указываем путь до нашего приватного ключа:



- Возвращаемся в категорию `Session` и нажимаем кнопку `Save` (важно чтоб был выделен наш новый сервер)
- Нажимаем кнопку `Open`
- В открывшемся окне консоли вводим логин и нашу `парольную фразу`