Configuração de WireGuard p/ acesso à HamNet nos Ubiquiti Unifi Security Gateway (USG, USG Pro 4, etc)

É necessário acesso SSH, portanto, deve-se configurar uma conta SSH. Para isso, no Unifi manager, em **System > Network Device SSH Authentication** deve-se activar o "Device SSH Authentication" e definir um nome de utilizador e password.

- Actualizar a gateway para a última versão (4.4.57 na altura deste documento).
- Fazer um backup da configuração da vossa rede (utilizar o Unifi manager para isso).

Instalar o WireGuard pela consola

Usar um cliente SSH para se ligar à gateway (PuTTY / ssh na linha de comandos ou outro) e instalar o wireguard. Fazer o download do package para o equipamento em: https://github.com/WireGuard/wireguard-vyatta-ubnt/releases

Nesse local, há uma descrição de qual o nome do ficheiro a fazer download para cada equipamento. Neste caso, como estou a utilizar um USG 4 Pro, deve-se fazer o download do ficheiro com o nome `ugw4-v1-v1.0.20220627-v1.0.20210914.deb`. A versão e data de compilação podem ser diferentes, fazer download sempre da mais recente.

Depois de efectuar o login na gateway por SSH, fazer o download e instalar o wireguard. Substituir `ugw4-v1-v1.0.20220627-v1.0.20210914.deb` pelo mais recente presente no local de download:

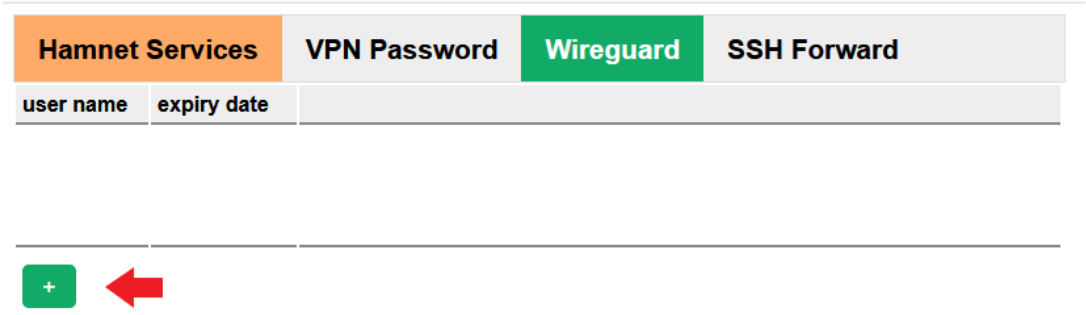
```
curl -OL https://github.com/WireGuard/wireguard-vyatta-
ubnt/releases/download/1.0.20220627-1/ugw4-v1-v1.0.20220627-v1.0.20210914.deb
sudo dpkg -i ugw4-v1-v1.0.20220627-v1.0.20210914.deb
```

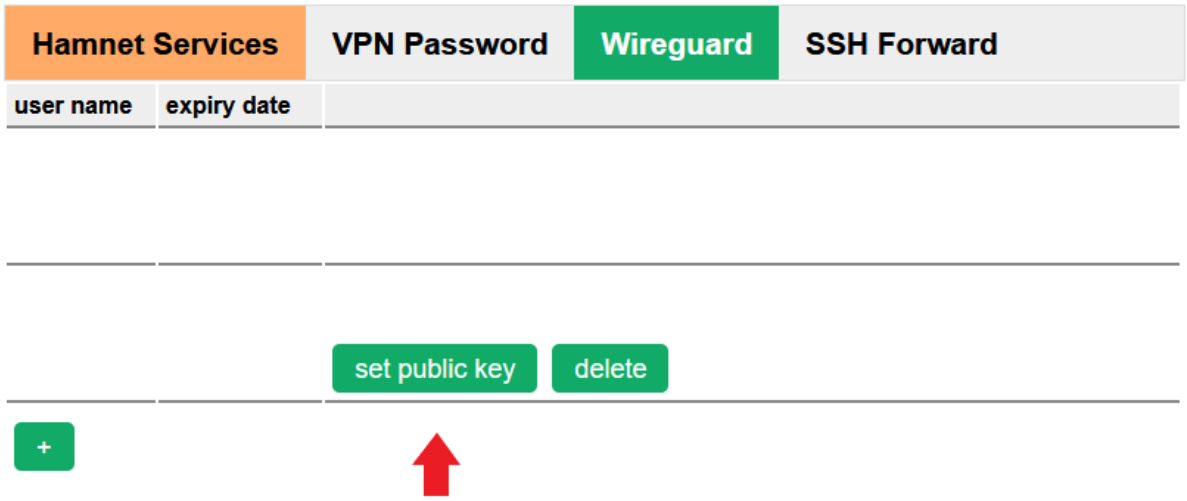
Após instalar, é necessário criar uma chave pública e privada para o cliente da vpn, com o seguinte comando (que cria ambas de uma vez só):

```
cd /config/auth
wg genkey | tee /config/auth/private.key | wg pubkey > public.key
```

Configurar o WireGuard

Na página da HamNet services (para quem vai por lotw: https://lotw.services.hamnet.network/services/index.php), escolher Wireguard e adicionar uma nova ligação por wireguard. Clicar em "set public key" para colocar a chave de encriptação pública que acabámos de gerar.

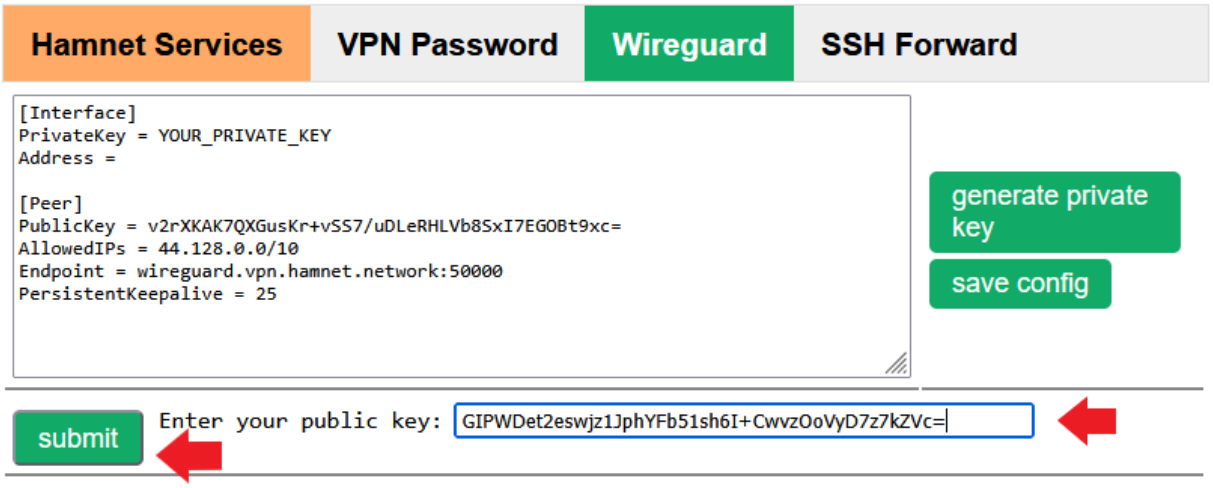




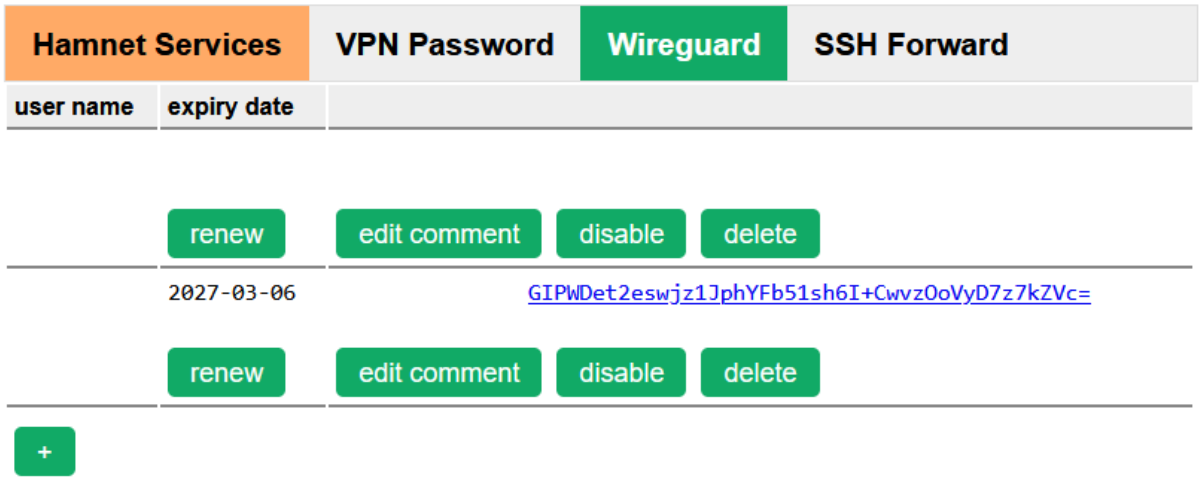
Para visualizar a nossa chave pública:
(NOTA!!! Chave pública!!! NUNCA partilhar em lado algum a privada!!!)

```
cat /config/auth/public.key
```

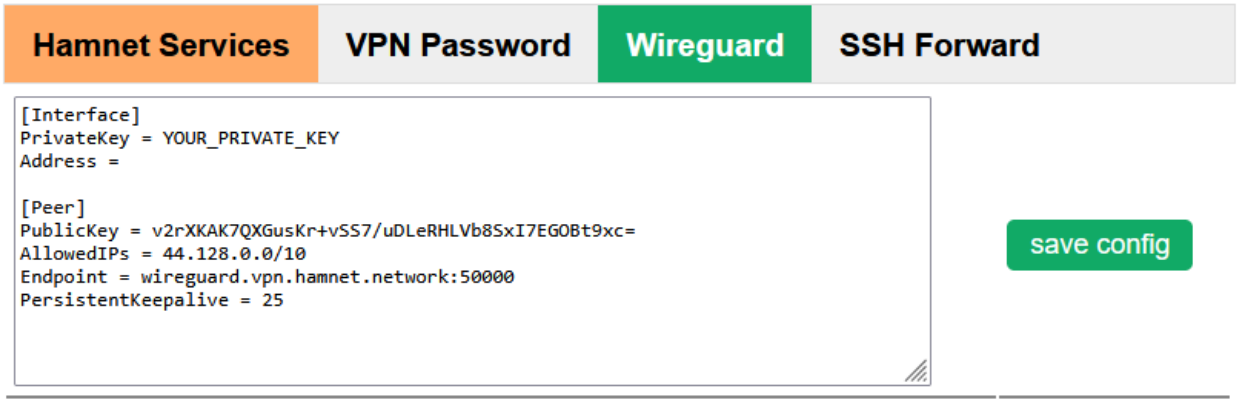
O comando mostra na consola o conteúdo da nossa chave pública. Fazer copy & paste para o campo "Enter your public key:" no website da hamnet, na nova configuração de wireguard que se acabou de adicionar.



Em seguida, irão visualizar algo parecido com:



O campo com as letras aparentemente aleatórias é a nossa chave pública. Se lá se clicar, uma página com os seguintes dados é apresentada:



A secção `[Interface]` define a configuração do nosso ponto de rede local (cliente

wireguard). A secção `[Peer]` define os dados do servidor onde o wireguard se irá ligar. O Address está vazio na imagem, porque muda para cada utilizador, utilizar o que lhe for atribuído.

Voltando novamente para a linha de comandos na gateway, configurar o interface de rede para o wireguard, utilizando como exemplo os dados apresentados acima:

```
configure
set interfaces wireguard wg0 address 44.148.209.???/32
set interfaces wireguard wg0 listen-port 51820
set interfaces wireguard wg0 route-allowed-ips true
set interfaces wireguard wg0 private-key /config/auth/private.key

set interfaces wireguard wg0 peer
aBaxDzgsyDk58eax6lt3CLedDt6SlVHnDxLG2K5UdV4= endpoint
wireguard.vpn.hamnet.network:50000
set interfaces wireguard wg0 peer
aBaxDzgsyDk58eax6lt3CLedDt6SlVHnDxLG2K5UdV4= allowed-ips 44.128.0.0/10
set interfaces wireguard wg0 peer
aBaxDzgsyDk58eax6lt3CLedDt6SlVHnDxLG2K5UdV4= persistent-keepalive 25

set service nat rule 5000 description "Masquerade for Hamnet"
set service nat rule 5000 outbound-interface wg0
set service nat rule 5000 type masquerade
set service nat rule 5000 protocol all
set service nat rule 5000 source address 192.168.1.0/24
```

Verificar com muita atenção todos os dados inseridos. Substituir o address `44.148.209.???/32` pelo endereço atribuído à vossa configuração, e verificar a chave pública do endpoint (onde se vai ligar) que aqui se está a utilizar `aBaxDzgsyDk58eax6lt3CLedDt6SlVHnDxLG2K5UdV4=`. Utilizar a chave que vos foi atribuída.

Após confirmar todos os dados, confirmar a configuração e submeter com o seguinte comando:

```
commit
```

Após este comando, a configuração fica activa. Em caso de erro podemos corrigir, ou se necessário, reiniciar a gateway para restaurar a configuração antiga caso algo tenha corrido mal, pois ainda não se encontra definitiva.

Testar a Ligação

Testar se a ligação foi efectuada com sucesso e se há tráfego a circular entre a rede interna e a vpn. Para isso pode-se utilizar o seguinte comando:

```
sudo wg show
```

Se tudo estiver correcto, deverá mostrar algo similar a:

```
interface: wg0
  public key: GIPWDet2eswjz1JphYFb51sh6I+CwvzOoVyD7z7kZVc=
  private key: (hidden)
  listening port: 51820

peer: aBaxDzgsyDk58eax6lt3CLedDt6SlVHnDxLG2K5UdV4=
  endpoint: 192.68.17.22:50000
  allowed ips: 44.128.0.0/10
  latest handshake: 1 minute, 52 seconds ago
  transfer: 35.13 MiB received, 25.71 MiB sent
  persistent keepalive: every 25 seconds
```

Na gateway, pingar um ip dentro da vpn para testar acesso entre gateway <-> vpn:

```
ping 44.146.1.105
```

(Exemplo de resposta esperada)

```
PING 44.146.1.105 (44.146.1.105) 56(84) bytes of data.
64 bytes from 44.146.1.105: icmp_req=3 ttl=59 time=150 ms
64 bytes from 44.146.1.105: icmp_req=4 ttl=59 time=167 ms
64 bytes from 44.146.1.105: icmp_req=5 ttl=59 time=158 ms
```

Se não tiver 'replies', a ligação não se encontra bem sucedida. Rever o processo e todos os comandos. Para limpar a configuração veja abaixo em "Remover configuração".

Se estiver tudo bem, falta testar os computadores na rede interna, se têm acesso à vpn. Para isso, basta no browser aceder a algum site, como:
`http://web.ct7afy.ampr.org/`

Se visualizar a página com sucesso, tudo está a funcionar.

Para gravar definitivamente as configurações desta sessão, termine com:

```
save
exit
```

> **Nota:** No caso de haver necessidade de restaurar a gateway pelo unifi manager, estas configurações não ficarão gravadas. É necessário adicionar estas configurações ao ficheiro de 'provisioning' típico da ubiquiti, com o nome `config.gateway.json`. Esses passos não estão aqui explicados, mas encontram-se facilmente pela internet, procurar no google sobre como o fazer.

Remover a configuração

Para apagar a configuração efectuada acima, se não estiver já em modo de configuração, deve entrar com o comando:

```
configure
```

(se já estiver, ignore o comando acima)

Apague o interface e a configuração de masquerading da seguinte forma:

```
delete interfaces wireguard
delete service nat rule 5000
commit
save
exit
```

Os comandos acima apagam o interface wireguard, removem o masquerading para a vpn, aplicam a configuração, gravam na sessão e saem do modo de configuração.

Actualizar o wireguard

Para actualizar é necessário apagar a configuração que está em curso, remover o driver do kernel, actualizar e recarregar a configuração gravada do sistema.

Fazer primeiro o download da nova versão:

```
curl -OL https://github.com/WireGuard/wireguard-vyatta-
ubnt/releases/download/1.0.20220627-1/ugw4-v1-v1.0.20220627-v1.0.20210914.deb
```

Executar os seguintes comandos:

```
configure
set interfaces wireguard wg0 route-allowed-ips false
commit
```

```
delete interfaces wireguard
commit
sudo rmmod wireguard
sudo dpkg -i ugw4-v1-v1.0.20220627-v1.0.20210914.deb
sudo modprobe wireguard
load
commit
exit
```

Substituir o nome do ficheiro pelo ficheiro do qual se fez download, e desta forma, permite efectuar um upgrade sem fazer um reboot à gateway.

WireGuard Configuration for HamNet access on Ubiquiti Unifi Security Gateway (USG, USG Pro 4, etc.)

Language: English

SSH access is required; therefore, you must configure an SSH account. To do this, in the Unifi manager, go to **System > Network Device SSH Authentication**, enable "Device SSH Authentication", and define a username and password.

- Update the gateway to the latest version (4.4.57 at the time of this document).
- Backup your network configuration (use the Unifi manager for this).

Install WireGuard via the console

Use an SSH client to connect to the gateway (PuTTY / ssh in the command line or another) and install WireGuard. Download the package for your device at: https://github.com/WireGuard/wireguard-vyatta-ubnt/releases

On that site, there is a description of the file name to download for each device. In this case, since I am using a USG 4 Pro, you should download the file named `ugw4-v1-v1.0.20220627-v1.0.20210914.deb`. The version and compilation date may differ; always download the most recent one.

After logging into the gateway via SSH, download and install WireGuard, replacing the filename below with the most recent one found at the download location:

```
curl -OL https://github.com/WireGuard/wireguard-vyatta-ubnt/releases/download/1.0.20220627-1/ugw4-v1-v1.0.20220627-v1.0.20210914.deb
sudo dpkg -i ugw4-v1-v1.0.20220627-v1.0.20210914.deb
```

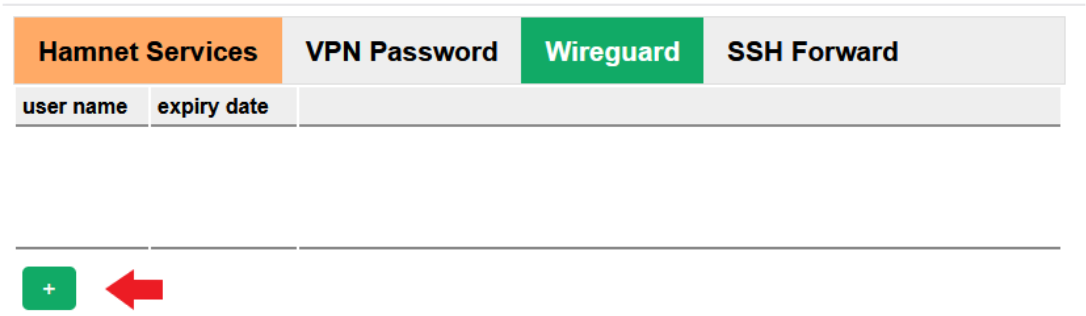
After installing, it is necessary to create a public and private key for the VPN client with the following (which creates both at once):

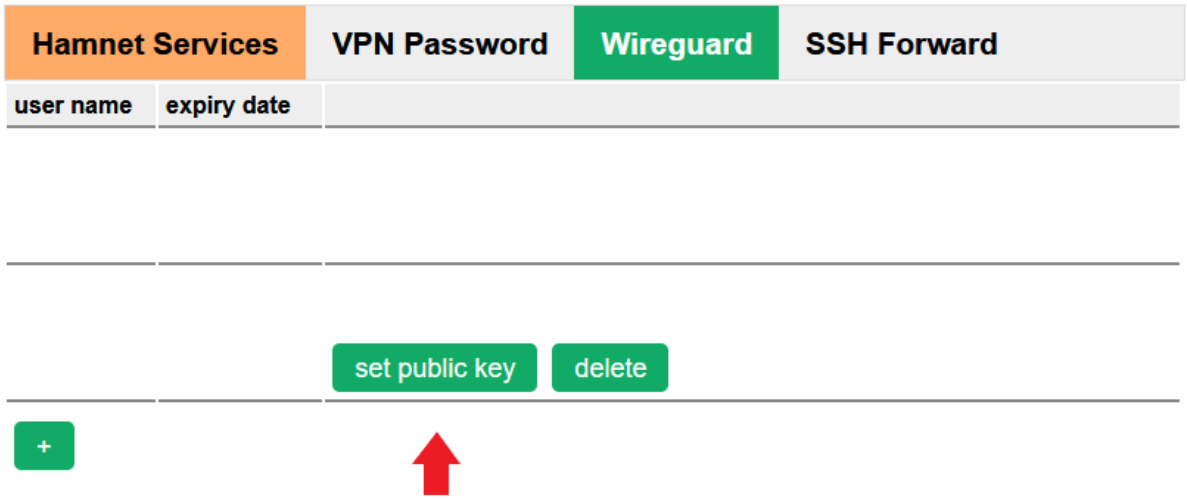
```
cd /config/auth
wg genkey | tee /config/auth/private.key | wg pubkey > public.key
```

Configure WireGuard

Now, configure WireGuard. On the HamNet services page (for those using LoTW: https://lotw.services.hamnet.network/services/index.php), choose WireGuard and add a

new connection. Click on "set public key" to input the public encryption key we just generated.

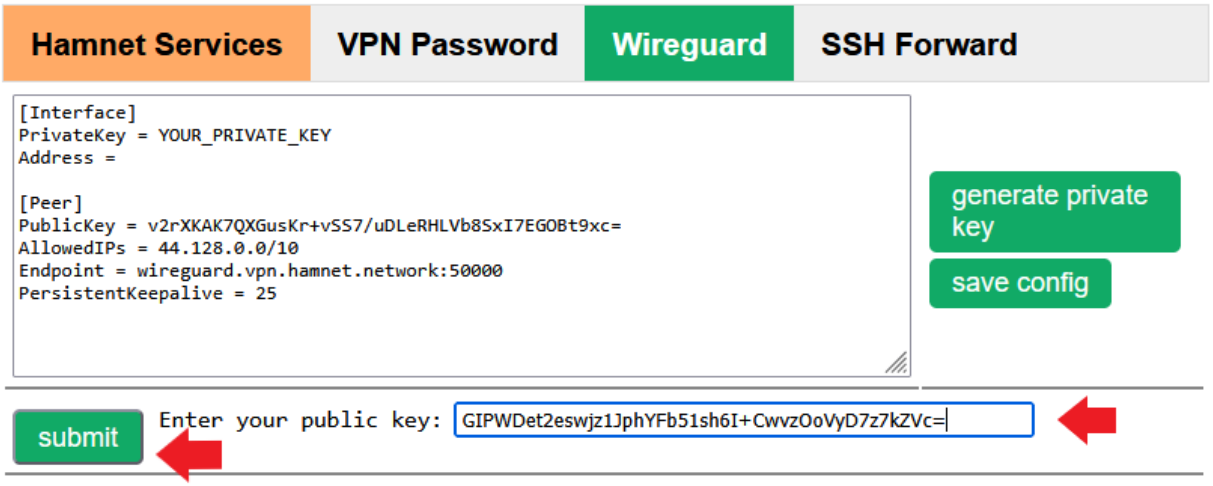




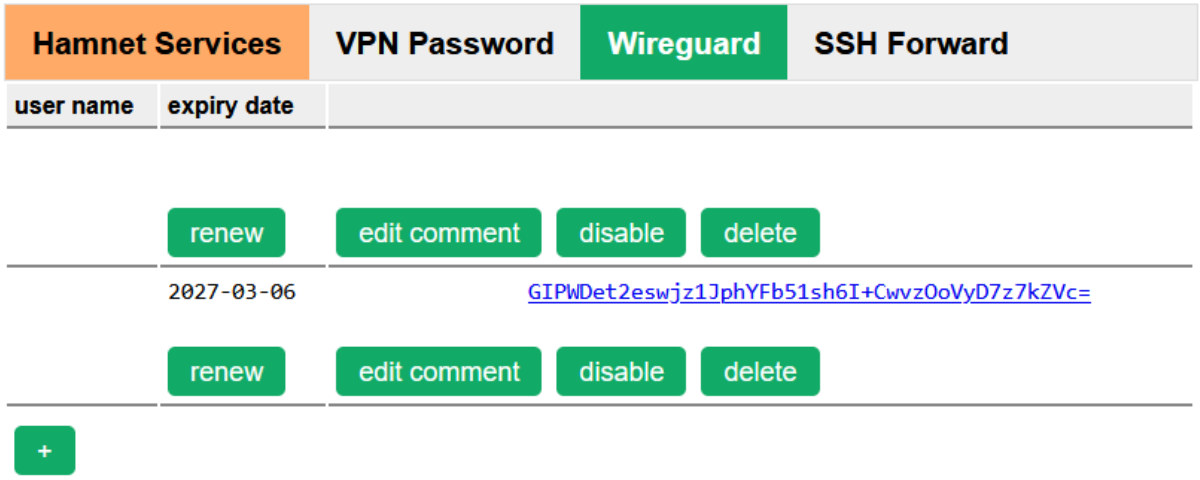
View your public key:
(NOTE!!! Public key!!! NEVER share the private one anywhere!!!)

```
cat /config/auth/public.key
```

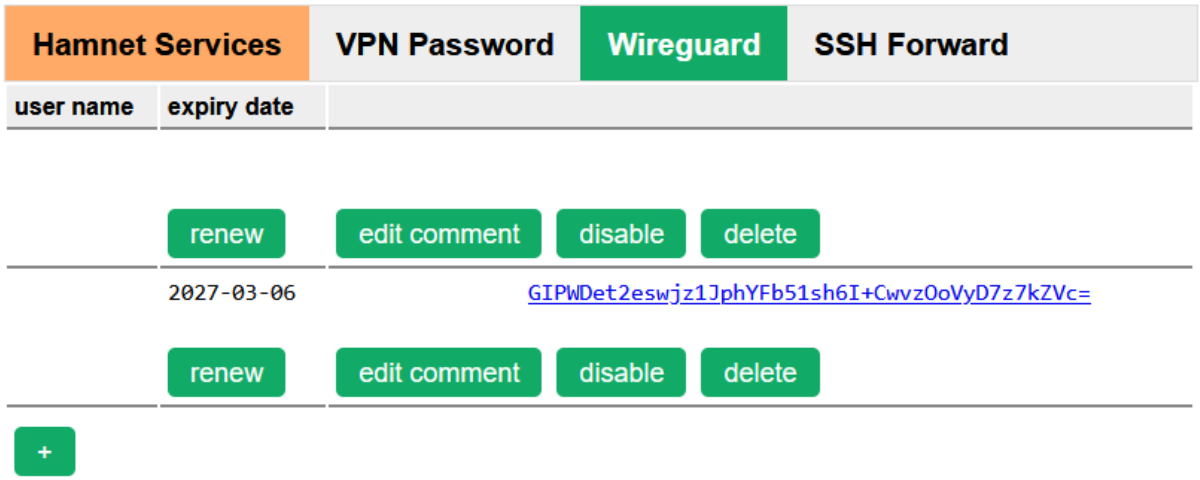
This displays the content of your public key in the console. Copy & paste it into the "Enter your public key:" field on the HamNet website for the new WireGuard configuration you just added.



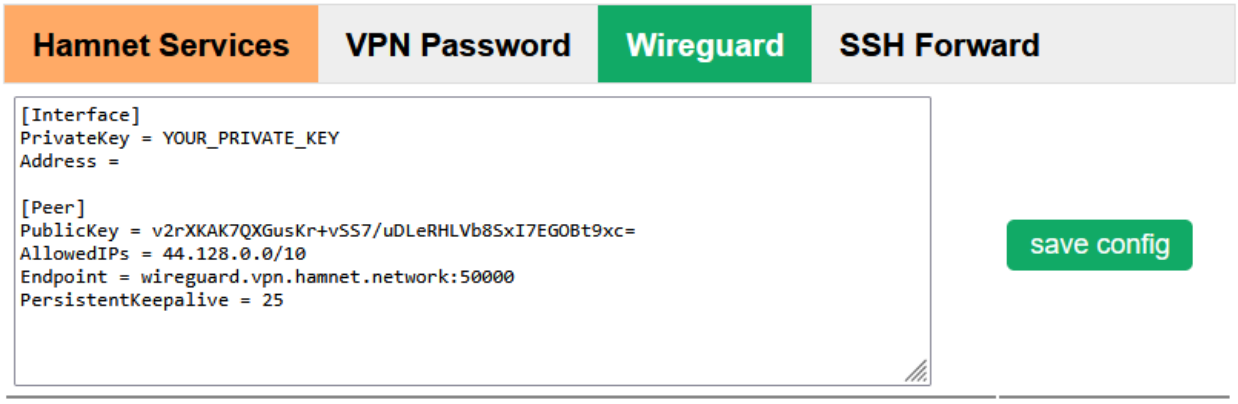
Em seguida, irão visualizar algo parecido com:



Next, you will see something similar to:



The field with apparently random letters is our public key. If you click there, a page with the following data is presented:



The `[Interface]` section defines the configuration of our local network point (WireGuard client). The `[Peer]` section defines the data for the server where WireGuard will connect. The Address in the image is empty because it changes for each user; use the one assigned to you.

Returning to the gateway command line, configure the network interface for WireGuard, using the data presented above as an example:

```
configure
set interfaces wireguard wg0 address 44.148.209.???/32
set interfaces wireguard wg0 listen-port 51820
set interfaces wireguard wg0 route-allowed-ips true
set interfaces wireguard wg0 private-key /config/auth/private.key

set interfaces wireguard wg0 peer
aBaxDzgsyDk58eax6lt3CLedDt6SlVHnDxLG2K5UdV4= endpoint
wireguard.vpn.hamnet.network:50000
set interfaces wireguard wg0 peer
aBaxDzgsyDk58eax6lt3CLedDt6SlVHnDxLG2K5UdV4= allowed-ips 44.128.0.0/10
set interfaces wireguard wg0 peer
aBaxDzgsyDk58eax6lt3CLedDt6SlVHnDxLG2K5UdV4= persistent-keepalive 25

set service nat rule 5000 description "Masquerade for Hamnet"
set service nat rule 5000 outbound-interface wg0
set service nat rule 5000 type masquerade
set service nat rule 5000 protocol all
set service nat rule 5000 source address 192.168.1.0/24
```

Carefully check all entered data. Replace the address `44.148.209.???/32` with the address assigned to your configuration, and verify the endpoint's public key (where you are connecting) used here `aBaxDzgsyDk58eax6lt3CLedDt6SlVHnDxLG2K5UdV4=`. Use the key assigned to you.

After confirming all data, commit the configuration and submit it with the following command:

```
commit
```

After this command, the configuration becomes active. In case of an error, you can correct it or, if necessary, restart the gateway to restore the old configuration if something went wrong, as it is not yet permanent.

Test the Connection

Test if the connection was successful and if traffic is flowing between the internal network and the VPN using the following command:

```
sudo wg show
```

If everything is correct, it should show something similar to:

```
interface: wg0
  public key: GIPWDet2eswjz1JphYFb51sh6I+CwvzOoVyD7z7kZVc=
  private key: (hidden)
  listening port: 51820

peer: aBaxDzgsyDk58eax6lt3CLedDt6SlVHnDxLG2K5UdV4=
  endpoint: 192.68.17.22:50000
  allowed ips: 44.128.0.0/10
  latest handshake: 1 minute, 52 seconds ago
  transfer: 35.13 MiB received, 25.71 MiB sent
  persistent keepalive: every 25 seconds
```

On the gateway, ping an IP inside the VPN to test access between gateway <-> VPN:

```
ping 44.146.1.105
```

If you do not get "replies," the connection is not successful. Review the process and all commands. To clear the configuration, see below under "Remove configuration."

If everything is fine, you need to test the computers on the internal network to see if they have access to the VPN. To do this, simply access a site in your browser, such as: `http://web.ct7afy.ampr.org/`

If you view the page successfully, everything is working. To permanently save the configurations for this session, finish with:

```
save
exit
```

> **Note:** In the event that the gateway needs to be restored via Unifi manager, these configurations will not be saved. It is necessary to add these configurations to the typical Ubiquiti provisioning file named `config.gateway.json`. These steps are not explained here, but can easily be found online; search Google on how to do it.

Remove configuration

To delete the configuration performed above, if you are not already in configuration mode, enter the command:

```
configure
```

(If you already are, ignore the above command)

Delete the interface and the masquerading configuration as follows:

```
delete interfaces wireguard
delete service nat rule 5000
commit
save
exit
```

The above commands delete the WireGuard interface, remove the masquerading for the VPN, apply the configuration, save it to the session, and exit configuration mode.

Update WireGuard

To update, it is necessary to delete the current configuration, remove the kernel driver, update, and reload the saved system configuration.

First, download the new version:

```
curl -OL https://github.com/WireGuard/wireguard-vyatta-
ubnt/releases/download/1.0.20220627-1/ugw4-v1-v1.0.20220627-v1.0.20210914.deb
```

Execute the following commands:

```
configure
set interfaces wireguard wg0 route-allowed-ips false
commit
delete interfaces wireguard
commit
sudo rmmod wireguard
sudo dpkg -i ugw4-v1-v1.0.20220627-v1.0.20210914.deb
sudo modprobe wireguard
load
commit
exit
```

Replace the filename with the file you downloaded. This allows you to perform an upgrade without rebooting the gateway.