

Tips réseaux (brige et wireguard)

Second bridge

```
cat /etc/network/interface
```

```
auto vmbr1
```

```
iface vmbr1 inet static
```

```
address 192.168.122.1
```

```
netmask 255.255.255.0
```

```
bridge_ports none
```

```
bridge_stp off
```

```
bridge_fd 0
```

```
post-up echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
post-up iptables -t nat -A POSTROUTING -s '192.168.122.0/24' -o vmbr0 -j MASQUERADE
```

```
post-down iptables -t nat -D POSTROUTING -s '192.168.122.0/24' -o vmbr0 -j MASQUERADE
```

VPN Wireguard entre deux cluster (via un bridge)

LE BRIGE:

```
cat /etc/network/interface
```

```
auto vmbr2
```

```
iface vmbr2 inet static
```

```
address 10.24.100.1/24
```

```
netmask 255.255.255.0
```

```
bridge_ports none
```

```
bridge-stp off
```

```
bridge-fd 0
```

```
post-up echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
post-up iptables -t nat -A POSTROUTING -s '10.24.100.0/24' -o wg0 -j MASQUERADE
```

```
post-down iptables -t nat -D POSTROUTING -s '10.24.100.0/24' -o wg0 -j MASQUERADE
```

SERVER WIREGARD:

```
apt-get install wireguard wireguard-tools net-tools linux-headers-`uname -r`  
cd /etc/wireguard/  
umask 077; wg genkey | tee private.key | wg pubkey > public.key
```

fichier de conf:

```
cat /etc/wireguard/wg0.conf  
  
[Interface]  
Address = 10.24.10.1/24  
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o vmbr0 -j MASQUERADE;  
ip6tables -A FORWARD -i wg0 -j ACCEPT; ip6tables -t nat -A POSTROUTING -o eth0 -j MASQUERADE  
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o vmbr0 -j MASQUERADE;  
ip6tables -D FORWARD -i wg0 -j ACCEPT; ip6tables -t nat -D POSTROUTING -o eth0 -j MASQUERADE  
ListenPort = 51194  
PrivateKey = QGWisdgdsgd=====UJAAi/wjvqvW6IOX1Q= (clé privé server)  
  
[Peer]  
PublicKey = 7vBH7GjalaKnqsfqfsqfsq6T1YXw= (clé public client)  
AllowedIPs = 10.24.10.0/24, 10.24.100.1/32  
Endpoint = ip_public_client:52443
```

Client WIREGARD

```
cat /etc/wireguard/conf.fr.conf  
  
[Interface]  
PrivateKey = UMWuzzVMXj3+tP+IYmi4zsdgsdgsg!!! (clé privé client)  
Address = 10.24.10.2/24  
DNS = 192.168.0.1  
  
[Peer]  
PublicKey = 5knFixic7i/ghreg//qfhgqdf// (clé public server)  
AllowedIPs = 10.24.10.1/24, 10.24.100.1/24 #AllowedIPs 0.0.0.0/0 représente l'ensemble de l'Internet, ce qui
```

signifie que tout le trafic vers Internet doit être acheminé via le VPN. Sinon spécifier la classe d'IP du réseau VPN : ex 192.168.10.0/24

Endpoint = ip_public_server:51194

PersistentKeepalive = 20 #PersistentKeepalive: Envoyez un paquet vide authentifié au pair toutes les 25 secondes pour maintenir la connexion active. Si PersistentKeepalive n'est pas activé, le serveur VPN ne pourra peut-être pas envoyer une requête ping au client VPN.

wg-quick up conf.fr.conf

Revision #8

Created 12 July 2022 21:18:12 by garfi

Updated 12 July 2022 22:00:05 by garfi