Использование VPN может быть хорошим решением для проблемы портов

WireGuard

Для настройки WireGuard на Ubuntu выполните следующие шаги:

На мастер-ноде:

1. Установите WireGuard:

    ```bash
    sudo apt update
    sudo apt install wireguard
    ```
1.1 Сгенерируйте ключи на каждой машине:

```bash
wg genkey | tee privatekey | wg pubkey > publickey

```
2. Создайте конфигурационный файл. Назовем его `wg0.conf`:

    ```bash
    sudo nano /etc/wireguard/wg0.conf
    ```

3. Добавьте следующие строки, заменяя ключи и IP-адреса на реальные:

    ```ini
    [Interface]
    Address = 10.0.0.1/24
    PrivateKey = [MasterPrivateKey]
    ListenPort = 51820

    [Peer]
    PublicKey = [WorkerPublicKey]
    AllowedIPs = 10.0.0.2/32
    ```

4. Поднимите интерфейс:

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

На воркер-ноде:

1. Установите WireGuard так же, как и на мастер-ноде.

2. Создайте конфигурационный файл `wg0.conf`:

    ```bash
    sudo nano /etc/wireguard/wg0.conf
    ```

3. Добавьте следующие строки:

    ```ini
    [Interface]
    Address = 10.0.0.2/24
    PrivateKey = [WorkerPrivateKey]

    [Peer]
    PublicKey = [MasterPublicKey]
    AllowedIPs = 10.0.0.1/32
    Endpoint = [MasterPublicOrLocalIP]:51820
    ```

4. Поднимите интерфейс:

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

Теперь у машин должны быть уникальные IP-адреса в VPN (10.0.0.1 для мастера и 10.0.0.2 для воркера). Используйте эти адреса для инициализации и присоединения к Docker Swarm.

```bash
# На мастере
docker swarm init --advertise-addr 10.0.0.1

# На воркере
docker swarm join --token [TOKEN] 10.0.0.1:2377
```

Таким образом, машины будут частью одного Swarm кластера, даже если они находятся в разных физических или виртуальных сетях.