Jika kamu ingin menggunakan **address list** untuk memfilter atau menambahkan IP publik melalui NAT pada MikroTik, kamu bisa menambahkan **address list** untuk menentukan IP yang boleh atau dilarang mengakses port tertentu atau memforwardkan trafik. Ini dapat meningkatkan fleksibilitas dalam pengaturan NAT, karena kamu bisa mengelompokkan IP atau jaringan IP tertentu dan memanipulasi trafik sesuai dengan kriteria yang sudah ditentukan.

Berikut adalah langkah-langkah untuk menambahkan **IP public melalui address list** dan kemudian mengonfigurasi NAT pada MikroTik:

1. **Menambahkan IP Publik ke Address List**

Misalnya, kita ingin menambahkan IP publik `36.94.33.94` ke dalam address list untuk tujuan NAT.

- Buka **Address List** dan tambahkan IP publik yang akan di-forward ke dalam list.
  - **Menambahkan IP ke Address List:**

    bash Copy

    ```
    /ip firewall address-list add list=public_ips address=36.94.33.94
    ```

    Penjelasan:

    - **list=public_ips**: Nama list yang kita buat (bisa kamu ganti dengan nama lain).
    - **address=36.94.33.94**: IP publik yang akan dimasukkan ke dalam list.

    Kamu bisa menambahkan lebih banyak IP publik atau subnet lainnya ke dalam address list yang sama sesuai kebutuhan.

  - Jika kamu ingin menambahkan lebih dari satu IP publik, misalnya:

    bash Copy

    ```
    /ip firewall address-list add list=public_ips address=36.94.33.95
    /ip firewall address-list add list=public_ips address=36.94.33.96
    ```

2. **Konfigurasi NAT dengan Address List**

Setelah menambahkan IP publik ke dalam address list, kita bisa memanfaatkan address list tersebut pada konfigurasi NAT untuk hanya meneruskan trafik dari IP yang terdaftar di dalam list tersebut.

A. **Port Forwarding (NAT) dengan Address List**

Kita akan menambahkan NAT rule untuk mem-forward port 80 dari IP publik yang ada dalam address list `public_ips` ke IP internal `192.168.100.115` di port 80.

- **Menambahkan Port Forwarding dengan Address List:**

  pgsql Copy

```
/ip firewall nat add chain=dstnat dst-address-list=public_ips protocol=tcp dst-port=80 a
```

Penjelasan:

- **chain=dstnat**: Ini adalah chain untuk destination NAT, yaitu trafik yang masuk.
- **dst-address-list=public_ips**: Menggunakan address list `public_ips` yang sudah kita buat sebelumnya. Hanya IP yang ada dalam address list ini yang akan diteruskan.
- **protocol=tcp**: Menentukan bahwa kita menggunakan protokol TCP (untuk port 80, HTTP).
- **dst-port=80**: Trafik yang datang pada port 80.
- **action=dst-nat**: Melakukan NAT pada trafik yang datang untuk diteruskan ke alamat tujuan.
- **to-addresses=192.168.100.115**: Mengarahkan trafik ke IP lokal internal (misalnya server web lokal).
- **to-ports=80**: Port tujuan yang diteruskan (port 80 di server lokal).

B. **Masquerading untuk IP Internal (Jika Diperlukan)**

Jika kamu ingin agar perangkat di jaringan internal dapat mengakses internet menggunakan IP publik melalui NAT, maka kamu bisa menambahkan aturan masquerade seperti sebelumnya.

- **Menambahkan Masquerade untuk Akses Internet:**

```csharp
/ip firewall nat add chain=srcnat out-interface=ether2 action=masquerade
```

Penjelasan:

- **chain=srcnat**: Aturan untuk source NAT (keluar).
- **out-interface=ether2**: Interface yang terhubung dengan ISP yang menyediakan IP publik (interface dengan IP publik).
- **action=masquerade**: Ini adalah tindakan NAT untuk mengganti sumber IP dengan IP publik yang tersedia.

3. **Menggunakan Address List untuk Filter Trafik (Optional)**

Kamu juga dapat menggunakan address list untuk membatasi akses ke server atau layanan tertentu hanya untuk IP yang ada dalam address list. Misalnya, kamu hanya ingin trafik dari IP dalam address list yang bisa mengakses port 80 di server internal.

- **Menambahkan Filter Firewall untuk Akses hanya dari Address List:**

```pgsql
```

```
/ip firewall filter add chain=input src-address-list=public_ips protocol=tcp dst-port=80
/ip firewall filter add chain=input protocol=tcp dst-port=80 action=drop
```

Penjelasan:

- **src-address-list=public_ips**: Menentukan bahwa hanya IP yang ada di address list `public_ips` yang bisa mengakses port 80.
- **protocol=tcp**: Protokol TCP untuk port 80.
- **action=accept**: Menerima trafik yang sesuai dengan kriteria.
- **action=drop**: Menjatuhkan trafik lainnya (mencegah akses selain IP yang ada di address list).

4. **Verifikasi Konfigurasi**

Pastikan untuk memverifikasi bahwa konfigurasi yang telah dilakukan berfungsi dengan baik.

- **Verifikasi Address List:**

bash Copy

```
/ip firewall address-list print
```

- **Verifikasi NAT Rules:**

bash Copy

```
/ip firewall nat print
```

- **Verifikasi Firewall Filter Rules:**

bash Copy

```
/ip firewall filter print
```

- **Tes Akses ke Port 80:** Cobalah mengakses IP publik `36.94.33.94:80` dan pastikan trafik diteruskan dengan benar ke IP internal `192.168.100.115:80`.

Kesimpulan:

Dengan menggunakan address list, kamu bisa memfilter dan mengontrol akses hanya untuk IP tertentu atau range IP yang sudah ada dalam daftar tersebut. Ini memberikan lebih banyak fleksibilitas dalam mengelola NAT dan akses ke jaringan internal kamu. Semoga langkah-langkah di atas membantu dalam konfigurasi NAT menggunakan address list di MikroTik!