Network Address Translation

Network Address Translation atau yang lebih biasa disebut dengan NAT adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP, merupakan teknologi yang memungkinkan jaringan IP Private dapat membagi koneksi akses internet jaringan yang didisain untuk menyederhanakan IP address dan berperan juga untuk melindungi jaringan dan kemudahan serta fleksibilitas dalam administrasi jaringan. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas.

Saat ini, protokol IP yang banyak digunakan adalah IP version 4 (IPv4). Dengan panjang alamat 4 bytes berarti terdapat 2 pangkat 32 = 4.294.967.296 alamat IP yang tersedia. Jumlah ini secara teoretis adalah jumlah komputer yang dapat langsung koneksi ke internet. Karena keterbatasan inilah sebagian besar ISP (Internet Service Provider) hanya akan mengalokasikan satu alamat untuk satu user dan alamat ini bersifat dinamik, dalam arti alamat IP yang diberikan akan berbeda setiap kali user melakukan koneksi ke internet. Hal ini akan menyulitkan untuk bisnis golongan menengah ke bawah. Di satu sisi mereka membutuhkan banyak komputer yang terkoneksi ke internet, akan tetapi di sisi lain hanya tersedia satu alamat IP yang berarti hanya ada satu komputer yang bisa terkoneksi ke internet. Hal ini bisa diatasi dengan metode NAT. Dengan NAT gateway yang dijalankan di salah satu komputer, satu alamat IP tersebut dapat dishare dengan beberapa komputer yang lain dan mereka bisa melakukan koneksi ke internet secara bersamaan.

NAT berlaku sebagai penerjemah antara dua jaringan. Dalam beberapa kasus pada jaringan rumahan, posisi NAT diantara jaringan internet dan jaringan lokal Anda. Internet sebagai sisi “Public” dan jaringan lokal Anda sebagai sisi “Private”. Ketika komputer pada jaringan private menginginkan data dari jaringan public (internet), maka perangkat NAT membuka sedikit saluran antara komputer Anda dan komputer tujuan. Ketika komputer pada jaringan internet membalikkan hasil dari permintaan, yang dilewati melalui perangkat NAT kepada komputer peminta, sehingga paket tersebut dapat diteruskan melewati jaringan public.

Ketika suatu komputer terkoneksi ke internet, komputer tersebut tidak saja dapat mengakses, misal ke server suatu web tertentu. Akan tetapi komputer tersebut juga sangat mungkin untuk diakses oleh komputer lain yang juga terkoneksi ke internet. Jika disalahgunakan, hal tersebut bisa sangat berbahaya. Data-data penting bisa saja dilihat atau bahkan dicuri oleh orang yang tak bertanggungjawab. NAT secara otomatis akan memberikan proteksi seperti halnya firewall dengan hanya mengizinkan koneksi yang berasal dari dalam jaringan. Hal ini berarti tingkat keamanan suatu jaringan akan meningkat, karena kemungkinan koneksi dari luar ke dalam jaringan menjadi relatif sangat kecil.

Dengan NAT, suatu jaringan yang besar dapat dipecah-pecah menjadi jaringan yang lebih kecil. Bagian-bagian kecil tersebut masing-masing memiliki satu alamat IP, sehingga dapat menambahkan atau mengurangi jumlah komputer tanpa mempengaruhi jaringan secara keseluruhan. Selain itu, pada gateway NAT modern terdapat server DHCP yang dapat mengkonfigurasi komputer client secara otomatis. Hal ini sangat menguntungkan bagi admin jaringan karena untuk mengubah konfigurasi jaringan, admin hanya perlu mengubah pada komputer server dan perubahan ini akan terjadi pada semua komputer client. Gateway NAT juga mampu membatasi akses ke internet, selain juga mampu mencatat semua traffic baik dari dan ke internet. Overall, dengan segala kelebihan gateway NAT tersebut, admin jaringan akan sangat terbantu dalam melakukan tugas-tugasnya. Selain itu beberapa keuntungan lain dalam menggunakan NAT, diantaranya :

1. Menghemat IP legal yang diberikan oleh ISP (Internet service provider)
2. Mengurangi terjadinya duplikasi IP address pada jaringan
3. Menghindari proses pengalamatan kembali pada saat jaringan berubah
4. Meningkatkan fleksibilitas untuk koneksi ke internet

Static NAT dan Dinamik NAT

Dua Tipe NAT Dua tipe NAT adalah Static dan Dinamik yang keduanya dapat digunakan secara terpisah maupun bersamaan.

- Static NAT one-to one mapping Statik Translasi Static terjadi ketika sebuah alamat lokal (inside) di petakan ke sebuah alamat global/internet (outside). Setiap ip private host ke sebuah ip public Alamat lokal dan global dipetakan satu lawan satu secara Statik.
- Dynamic NAT di sediakan pool ip public yang direserved untuk di gunakan. oleh client. Dinamik NAT dengan Pool (kelompok) Translasi Dinamik terjadi ketika router NAT diset untuk memahami alamat lokal yang harus ditranslasikan, dan kelompok (pool) alamat global yang akan digunakan untuk terhubung ke internet. Proses NAT Dinamik ini dapat memetakan bebarapa kelompok alamat lokal ke beberapa kelompok alamat global. NAT Overload Sejumlah IP lokal/internal dapat ditranslasikan ke satu alamat IP global/outside.

Selain kemudahan dan keuntungan menggunakan NAT, kerugian menggunakan NAT diantaranya :

1. Proses translasi menimbulkan keterlambatan karena data harus melalui perangkat NAT (software atau hardware).
2. Terdapat beberapa aplikasi yang tidak dapat berjalan ketika menggunakan jaringan NAT, khususnya NAT yang menggunakan software.
3. Menghilangkan kemampuan untuk melacak data karena melewati firewall.

Sewaktu Internet terus mengalami laju peningkatan, NAT menawarkan cara cepat dan efektif untuk memperluas akses internet yang aman ke dalam jaringan yang sudah ada dan maupun jaringan-jaringan lokal yang baru. NAT menawarkan keluesan dan performa dibandingkan aplikasi alternatif setingkat proxy, dan menjadikan ukuran standar untuk akses internet yang dibagi-bagi (connection sharing).

Mikrotik Router OS mendukung

- Open Shortest Path First (OSPF)
- Routing information Protokol (RIP)
- Border Gateway Protokol (BGP)

Mikrotik router OS tidak mendukung

- Interior gateway routing protokol (IGRP)
- Enchanced interior gateway routing protokol (EIGRP)

Membangun NAT dengan Firewall

Firewall atau lebih dikenal dengan aturan aturan adalah untuk melakukan fungsi keamanan yang digunakan untuk control pengelolaan akses yang berjalan data dari sebuah router. NAT dan Firewall secara otomatis menyediakan proteksi terhadap sistem yang berada di balik firewall karena NAT Firewall hanya mengizinkan koneksi yang datang dari jaringan yang berada di balik firewall. Tujuan dari NAT adalah untuk melakukan multiplexing terhadap lalu lintas dari jaringan internal untuk kemudian menyampaikannya kepada jaringan yang lebih luas (MAN, WAN atau Internet) seolah-olah paket tersebut datang dari sebuah alamat IP atau beberapa alamat IP. NAT Firewall membuat tabel dalam memori yang mengandung informasi mengenai koneksi yang dilihat oleh firewall

Firewall diposisikan di pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya mengizinkan lalu lintas jaringan yang aman untuk dilalui, dan mencegah lalu lintas jaringan yang tidak aman.

Karakteristik dari Routing terdiri dari tiga yaitu NAT, MANGLE dan FILTER. Penggunannya disesuaikan dengan sifat dan karakteristik masing-masing. Fungsi dari masing-masing tabel tersebut sebagai berikut :

1. NAT : Secara umum digunakan untuk melakukan Network

   Address Translation. NAT adalah penggantian field alamat asal atau alamat tujuan dari sebuah paket.

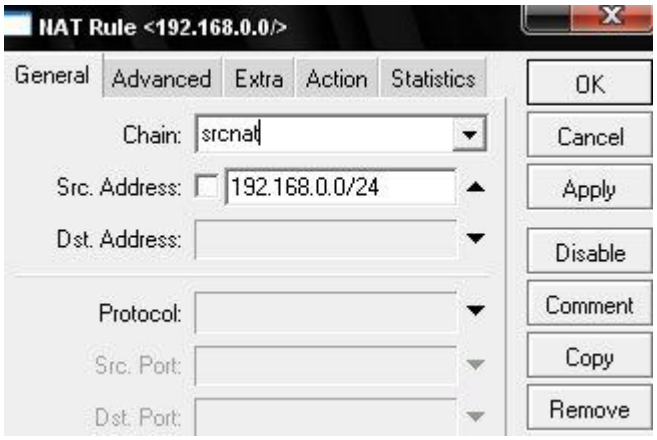
2. MANGLE : Digunakan untuk melakukan penghalusan (mangle) paket, seperti TTL, TOS dan MARK.
3. FILTER : Secara umum, inilah pemfilteran paket yang sesungguhnya.. Di sini bisa dintukan apakah paket akan di-DROP, LOG, ACCEPT atau REJECT

Struktur logika dari NAT

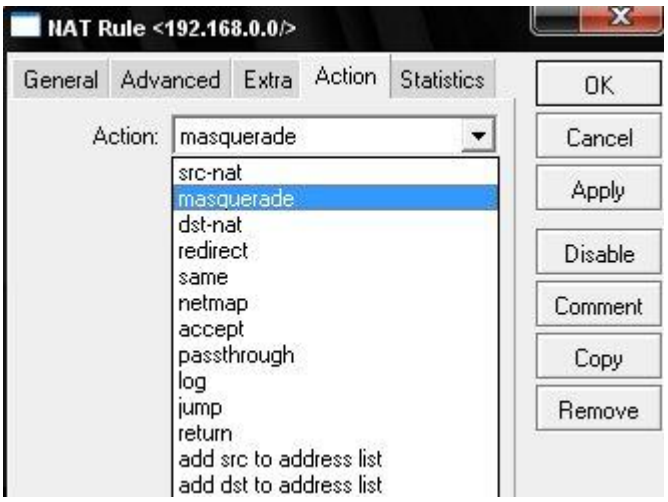
“ jika <kondisi> selanjutnya <aksi>“

Untuk mengaktifkan NAT dapat dilakukan dengan :

1. Klik **IP —> Firewall**, Kemudian pilih **NAT,** dari tab General pilih chain srcnat, src.Address 192.168.0.0/24 IP network address lokal router kita 192.168.0.0/24 yg merupakan semua host di internal network. Network pada jaringan ini sebagai network yang akan di NAT



2. Dari tab Action pilih masquerade. Masquerade NAT dipergunakan untuk membolehkan jaringan private bersembunyi di belakang, merubah/mentransformasikan ip private menjadi ip public. Sebaik sebagai diwakili oleh perangkat external yang menuju internet



Pada tab **General** pada **Chain** pilih **srcnat** pada **Out. Interface** pilih **ether1** pada tab **Action** pilih **masquerade** Kemudian klik **Apply** dan **OK.**

- **SRCNAT** melakukan perubahan alamat asal dari paket (Source Network Address Translation). Target ini berlaku untuk tabel nat pada chain POSTROUTING, dan di sinilah SRCNAT bisa dilakukan. Jika paket pertama dari sebuah koneksi mengalami SRCNAT, maka paket-paket berikutnya dalam koneksi tersebut juga akan mengalami hal yang sama yakni menyembunyikan alamat IP yang sifatnya private berada di belakang menjadi satu atau lebih alamat IP external. Dalam Srcnat kita juga dapat mengaktifkan dst-nat dan redirect.
- **DSTNAT** digunakan untuk merubah alamat tujuan, port dan kemudian membentuk kembali perjalan paket. Dst-nat membolehkan alamat tujuan dan port dirubah menjadi alamat local.
- **MASQUERADE** bekerja dengan cara yang hampir sama seperti target SNAT, tetapi target ini tidak memerlukan option –to-source. MASQUERADE memang didesain untuk bekerja pada komputer dengan koneksi yang tidak tetap seperti dial-up atau DHCP yang akan kita mendapatkan IP yang berubah-ubah.
- **ACCEPT** Mengijinkan paket. Tidak ada operasi yang dilakukan, sebagai contoh paket paket di dibiarkan dan tidak ada aturan yang diaplikasikan.
- **Add-dst-to-address-list** menambahkan tujuan dari sebuah alamat IP.
- **Add-src-to-address-list** menambahkan alamat asal dari sebuah alamat IP.

- **Drop** memberhentikan paket tanpa mengirimkan pesan penolakan ICMP
- **Jump** beralih ke aturan parameter yang telah di definisikan oleh nilai parameter dari target loncatan.
- **Passthrogh** mengabaikan aturan dan beralih ke aturan selanjutnya.
- **Reject** menolak dan mengembalikan paket dengan mengirimkan ICMP sebagai pesan penolakan.

Untuk melihat konfigurasi NAT yang ada di router dapat dilakukan dengan cara :

[admin@workshop]/ip firewall nat print

```
[adrian@workshop] > ip firewall nat pr
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=srcnat src-address=192.168.0.0/24 action=masquerade

 1   chain=srcnat src-address=192.168.1.0/24 action=masquerade

 2   chain=srcnat src-address=192.168.2.0/24 action=masquerade

 3   chain=dstnat src-address=192.168.0.0/24 protocol=tcp dst-port=80 action=redirect
     to-ports=3188

 4   chain=dstnat src-address=192.168.1.0/24 protocol=tcp dst-port=80 action=redirect
     to-ports=3188

 5   chain=dstnat src-address=192.168.2.0/24 protocol=tcp dst-port=80 action=redirect
     to-ports=3188
[adrian@workshop] >
```

Mapping

Jika kita menginginkan menghubungkan IP Publick dengan subnet 11.11.11.0/24 ke local 2.2.2.0/24, kita harus mendeskripsikan alamat tujuan NAT dan alamat sumber dengan parameter **action=netmap**:

[admin@workshop]//ip firewall nat add chain=dstnat dst-address=11.11.11.1-11.11.11.254 action=netmap to-addresses=2.2.2.1-2.2.2.254

[admin@workshop]//ip firewall nat add chain=srcnat src-address=2.2.2.1-2.2.2.254 action=netmap to-addresses=11.11.11.1-11.11.11.254

Bloking Mikrotik dari Scan Winbox dan Neighbour

Kadang kala para ISP atau penyedia jasa layanan tidak terlalu jeli untuk melindungi customernya. Terutama ketika melindungi router pelanggan yang menggunakan Mikrotik RouterOS(tm). Dengan menjalankan IP >> Neighbor kita bisa melihat router mikrotik lainnya yang secara fisik terhubung dengan router kita melalui jaringan di provider kita.

Untuk itu kita bisa melindunginya dengan berbagai cara misalnya memblok scan dari winbox dan neighbor kita. Berikut adalah cara yang paling mudah :

Code:

[admin@mikrotik] interface bridge> filter print

Flags: X - disabled, I - invalid, D - dynamic

0 ;;; block discovery mikrotik

chain=forward in-interface=ether1 mac-protocol=ip dst-port=5678

ip-protocol=udp action=drop

1 ;;; block discovery mikrotik

chain=input in-interface=ether1 mac-protocol=ip dst-port=5678

ip-protocol=udp action=drop

2 ;;; block discovery mikrotik

chain=output mac-protocol=ip dst-port=5678 ip-protocol=udp action=drop

3 ;;; block discovery mikrotik

chain=input in-interface=ether1 mac-protocol=ip dst-port=8291

ip-protocol=tcp action=drop

4 ;;; block winbox mikrotik

chain=forward in-interface=ether1 mac-protocol=ip dst-port=8291

ip-protocol=tcp action=drop

5 ;;; block request DHCP

chain=input mac-protocol=ip dst-port=68 ip-protocol=udp action=drop

6 ;;; block request DHCP

chain=forward mac-protocol=ip dst-port=68 ip-protocol=udp action=drop

7 ;;; block request DHCP

chain=output mac-protocol=ip dst-port=68 ip-protocol=udp action=drop

Dengan perintah tersebut kita bisa menutup beberapa scan terutama yang menggunakan winbox dan ip neighbor. Port diatas adalah bagian dari share Mikrotik RouterOS yang memang di perlukan untuk monitoring.