**Memahami Konsep Network Address Translation (NAT)**

**Kita sering mendengar istilah Network Address Translation (NAT) dalam kaitannya dengan koneksi ke jaringan public atau koneksi ke internet. Kalau dalam bahasa teknik kita mungkin adalah "Terjemahan Alamat Jaringan", agak asing ditelinga kita rasanya.**

**Dalam kita merencanakan konektivity ke Internet dalam organisasi kita, anda harus mendefinisikan seberapa besar ukuran dari jaringan infrastruktur anda.**

**Untuk ukuran jaringan yang kecil yang tidak di routed, anda bisa menggunakan solusi NAT sederhana saja, akan tetapi solusi ini memberikan solusi keamanan minimum.**

**Untuk jaringan berskala besar, yang sangat kompleks anda membutuhkan suatu server ISA atau solusi firewall jadi – hardware firewall. Solusi server ISA atau hardware firewall memungkinkan anda mengkoneksikan beberapa routed jaringan ke Internet dan memberikan anda suatu system keamanan yang lebih advance dan lebih bisa leluasa mengendalikan akses resource jaringan.**

**Apa itu Network Address Translation (NAT)?**

**Network Address Translation (NAT) adalah suatu metoda pokok yang memungkinkan komputer yang mempunyai address yang tidak terdaftar atau komputer yang menggunakan address private, untuk bisa mengakses Internet. Ingat pada diskusi IP address sebelumnya bahwa IP address private tidak bisa di route ke internet (non-routed), hanya dipakai pada jaringan internal yang berada pada range berikut:**

**Class Type Start Address End Address**

**Class A 10.0.0.0 10.255.255.254**

**Class B 172.16.0.0 172.31.255.254**

**Class C 192.168.0.0 192.168.255.254**

**Untuk setiap paket yang dihasilkan oleh client, implementasi Network Address Translation (NAT) menggantikan IP address yang terdaftar kepada IP address client yang tidak terdaftar.**

**Ada tiga macam jenis dasar Network Address Translation (NAT):**

**1. Static NAT**

**Network Address Translation (NAT) menterjemahkan sejumlah IP address tidak terdaftar menjadi sejumlah IP address yang terdaftar sehingga setiap client dipetakkan kepada IP address terdaftar yang dengan jumlah yang sama.**

**NAT Static**

**Jenis NAT ini merupakan pemborosan IP address terdaftar, karena setiap IP address yang tidak terdaftar (un-registered IP) dipetakan kepada satu IP address terdaftar. Static NAT ini juga tidak seaman jenis NAT lainnya, karena setiap komputer secara permanen diasosiasikan kepada address terdaftar tertentu, sehingga memberikan kesempatan kepada para penyusup dari Internet untuk menuju langsung kepada komputer tertentu pada jaringan private anda menggunakan address terdaftar tersebut.**

**2. Dynamic NAT**

**Dynamic Network Address Translation dimaksudkan untuk suatu keadaan dimana anda mempunyai IP address terdaftar yang lebih sedikit dari jumlah IP address un-registered. Dynamic NAT menterjemahkan setiap komputer dengan IP tak terdaftar kepada salah satu IP address terdaftar untuk connect ke internet. Hal ini agak menyulitkan para penyusup untuk menembus komputer didalam jaringan anda karena IP address terdaftar yang diasosiasikan ke komputer selalu berubah secara dinamis, tidak seperti pada NAT statis yang dipetakan sama. Kekurangan utama dari dynamis NAT ini adalah bahwa jika jumlah IP address terdaftar sudah terpakai semuanya, maka untuk komputer yang berusaha connect ke Internet tidak lagi bisa karena IP address terdaftar sudah terpakai semuanya.**

**3. Masquerading NAT**

**Masquerading NAT ini menterjemahkan semua IP address tak terdaftar pada jaringan anda dipetakan kepada satu IP address terdaftar. Agar banyak client bisa mengakses Internet secara bersamaan, router NAT menggunakan nomor port untuk bisa membedakan antara paket-2 yang dihasilkan oleh atau ditujukan komputer-2 yang berbeda. Solusi Masquerading ini memberikan keamanan paling bagus dari jenis-2 NAT sebelumnya, kenapa? Karena asosiasi antara client dengan IP tak terdaftar dengan kombinasi IP address terdaftar dan nomor port didalam router NAT hanya berlangsung sesaat terjadi satu kesempatan koneksi saja, setelah itu dilepas.**

**NAT Masquerading**

**Keamanan NAT**

**Kebanyakan implementasi NAT sekarang ini mengandalkan pada teknik jenis Masquerading NAT karena meminimalkan jumlah kebutuhan akan IP address terdaftar dan memaksimalkan keamanan yang diberikan olen Network Address Translation (NAT).**

**Akan tetapi perlu dicatat bahwa NAT itu sendiri, walau memakai jenis NAT yang paling aman – Masquerading, bukanlah suatu firewall yang sebenarnya dan tidak memberikan suatu perisai besi keamanan untuk suatu situasi yang beresiko tinggi. NAT pada dasarnya hanya memblokir tamu tak diundang (unsolicited request) dan semua usaha penjajagan atau usaha scanning dari internet, yang berarti suatu pencegahan dari usaha para penyusup untuk mencari file share yang tidak di proteksi atau private Web ataupun FTP server. Akan tetapi, NAT tidak bisa mencegah user di Internet untuk meluncurkan suatu usaha serangan DoS (Denial of Services) terhadap komputer yang ada dijaringan private anda. Ataupun tidak bisa mencegah usaha-2 lain dengan teknik yang lebih kompleks untuk melakukan kompromi jaringan.**

**Network Address Translation dan Stateful Packet Inspection**

**Beberapa implementasi NAT juga melibatkan tambahan keamanan, biasanya secara umum menggunakan teknik yang disebut Stateful Packet Inspection (SPI). Stateful Packet Inspection adalah istilah generic pada proses dimana NAT router memeriksa paket yang datang dari internet dilakukan lebih teliti dan lebih seksama dari biasanya. Pada umumnya implementasi NAT, router hanya konsen pada IP address dan port dari paket yang melewatinya.**

**Suatu router NAT yang mendukung Stateful packet inspection memeriksa sampai ke header layer network dan layer transport juga, memeriksa pola yang mempunyai tingkah laku berbahaya, seperti IP spoofing, SYN floods, dan serangan teardrop. Banyak produsen router mengimplementasikan stateful packet inspection dalam berbagai bentuk dan cara, jadi tidak semua router NAT dengan kemampuan Stateful packet inspection ini mempunyai tingkat perlindungan keamanan yang sama.**

**Solusi NAT**

**Seperti didiskusikan sebelumnya, keputusan untuk design jaringan seharusnya mempertimbangkan berikut ini:**

**Ukuran besarnya jaringan private anda**

**Kebutuhan akan keamanan jaringan dalam organisasi**

**NAT adalah solusi yang memadai jika:**

**Akses ke internet dan akses ke jaringan tidak dibatasi berdasarkan user per user. Tentunya anda tidak memberikan akses internet ke semua user dalam jaringan anda bukan?**

**Jaringan private berisi user didalam lingkungan yang tidak bisa di routed.**

**Organisasi anda memerlukan address private untuk komputer-2 pada jaringan private.**

**Suatu server NAT memerlukan paling tidak 2 interface jaringan.**

**Setiap interface memerlukan IP address, range IP address yang diberikan haruslah berada dalam subnet yang sama dengan jaringan dimana ia terhubung.**

**Subnet mask juga harus sama dengan subnet mask yang diberikan pada segmen jaringan dimana dia terhubung**

**Suatu server NAT dapat diletakkan pada jaringan untuk melaksanakan tugas-2 tertentu:**

**Mengisolasi traffic jaringan pada segmen jaringan sumber, tujuan, dan segmen jaringan intermediate**

**Membuat partisi subnet didalam jaringan private, melindungi data confidential.**

**Pertukaran paket jaringan antara jenis segmen jaringan yang berbeda**

**Didalam design kebanyakan wireless router yang ada dipasaran sekarang ini, sudah banyak yang mengadopsi kemampuan Network Address Translation (NAT) dan Stateful Packet Inspection (SPI) ini kedalam piranti route.**