ISSN: 2614-1205

Implementasi Firewall Static Network Address Translation (NAT) Menggunakan Packet Tracer

Rizqia Salsabila[1]

[1]Jurusan Ilmu Komputer, FMIPA, Universitas Negeri Semarang
Email: [1]rizqiasalsabila88@gmail.com

Abstrak

Pesatnya perkembangan internet dapat memberikan banyak kemudahan terutama dalam penyediaan informasi dan sarana komunikasi, tetapi hal itu juga mempunyai dampak negatif, yaitu banyaknya kriminalitas dalam dunia internet. Untuk itu perlu pembatasan jaringan internet dengan menggunakan *firewall*. NAT adalah salah satu jenis *firewall* yang digunakan untuk menyaring IP dengan menerjemahkan IP untuk mendapat jalan masuk dari jaringan yang berbeda, NAT juga dapat memasukan *host* ke jaringan yang berbeda tanpa izin tuan rumah. Tujuan dari simulasi ini adalah untuk menerapkan *static network address translation* dengan menggunakan *packet tracer*. Pada penelitian ini simulasi jaringan dirancang menggunakan beberapa perangkat berbeda seperti satu server, dua *router*, dua *swich*, dan delapan komputer yang saling terhubung satu sama lain. Hasil yang didapat melalui simulasi tersebut berupa melalui pengimplementasian NAT maka jaringan komputer lebih aman karena hanya IP *address* terdaftar yang dapat masuk ke jaringan.
Kata Kunci: Jaringan, *Firewall*, *Static* NAT

Abstract

The rapid development of the internet can provide many conveniences, especially in providing information and means of communication, but it also has a negative impact, namely the number of crimes committed in the internet world. For this reason, it is necessary to limit the internet network by using a firewall. NAT is one type of firewall that is used to filter IP by translating IP to get access from different networks. NAT can also enter hosts into different networks without the host's permission. The purpose of this simulation is to implement static network address translation using a packet tracer. In this research, the network simulation is designed using several different devices, such as one server, two routers, two switches, and eight computers that are connected to each other. The results obtained through the simulation are that, through the implementation of NAT, the computer network is safer because only registered IP addresses can enter the network.
***Keyword**: Network, Firewall, Static NAT*

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer saat ini sangatlah pesat. Jaringan komputer didefinisikan sebagai sambungan beberapa perangkat komputer yang dapat berkomunikasi. Selain itu jaringan komputer juga diartikan sebagai kumpulan komputer yang terhubung satu sama lain melalui media perantara sehingga dapat berbagi aplikasi dan informasi bersama-sama [1]. Dengan terus berkembangnya keamanan jaringan komputer, tingkat kriminalitas dari para penjahat ini juga terus menerus berkembang [2].

Cyber-crime adalah salah satu contoh tindak kejahatan pada keamanan jaringan komputer. *Cyber-crime* adalah penggunaan komputer dengan tujuan yang tidak baik dan merusak melalui penyalahgunaan kemudahan teknologi digital [3]. *Cyber-crime* juga dapat disebut sebagai perbuatan melanggar hukum yang dilakukan dengan memakai komputer sebagai objek dan jaringan komputer untuk sarana dengan niat yang tidak baik dan dapat merugikan pihak lain [4]. Biasanya bentuk dari *cyber-crime* yang merusak keamanan jaringan disebut dengan *cracking*.

Cracking adalah kegiatan untuk merusak sistem keamanan komputer. Orang yang melakukan *cracking* disebut *cracker.* Definisi *cracker* adalah seseorang yang merusak keamanan sistem atau jaringan setelah mendapatkan akses untuk masuk serta biasanya *cracker* juga melakukan tindakan pencurian data dan tindakan lain yang menyebabkan kerugian [5]. Masyarakat biasanya menyebut *cracking* sebagai *hacking*, namun kedua hal tersebut sebetulnya cukup berbeda karena memiliki tujuan yang berbeda walaupun tindakan yang dilakukan sama. Mengacu pada tujuannya tindakan *hacking* bertujuan untuk masuk ke dalam sistem komputer sehingga dapat mengetahui dimana letak kelemahan pada keamanan sistem tersebut.

Kejahatan *cyber-crime* bisa lebih luas daripada tindak pidana konvensional karena para pelaku bisa bertindak kapan saja dan dimana saja. Oleh karena itu, lingkup wilayah terjadinya tidak hanya mencangkup secara lokal atau nasional, tetapi juga internasional. Salah satu jenis *cyber-crime* berdasarkan bentuk aktivitas yang dilakukan adalah *Unauthorized Access*. *Unauthorized Access* adalah tindakan yang bertujuan untuk masuk secara paksa ke dalam sistem jaringan komputer tanpa mendapat izin dari pemiliknya [6]. Ancaman keamanan yang paling menakutkan untuk LAN berjenis *wirreless* adalah *Unauthorized access point* karena melibatkan pemasangan titik akses eksternal yang tidak sah [7].

Salah satu cara untuk menanggulangi *cyber-crime* adalah dengan mengamankan sistem jaringan komputer. Hal ini bertujuan untuk memblokir seseorang yang tidak diinginkan masuk kedalam sistem [6]. *Firewall* adalah sistem atau perangkat yang berfungsi untuk mengamankan lalu lintas jaringan komputer [8]. *Firewall* bertujuan untuk mengontrol akses sehingga dapat menolak atau mengijinkan koneksi tertentu sebagai tindak pengamanan jaringan [9]. Umumnya *firewall* diimplementasikan pada *gateway* yang berada di antara jaringan lokal dan jaringan internet. *Firewall* mengontrol lalu lintas jaringan lokal (LAN) pada tingkat yang paling dasar. Secara umum tidak ada jaminan bahwa setiap sistem jaringan komputer yang terhubung memiliki keamanan jaringan publik (Internet). Ada berbagai macam jenis *firewall*, namun *packet filtering* adalah metode yang paling dasar pada *firewall*. *Packet filtering* berfungsi untuk memilah paket data yang akan melalui jaringan.

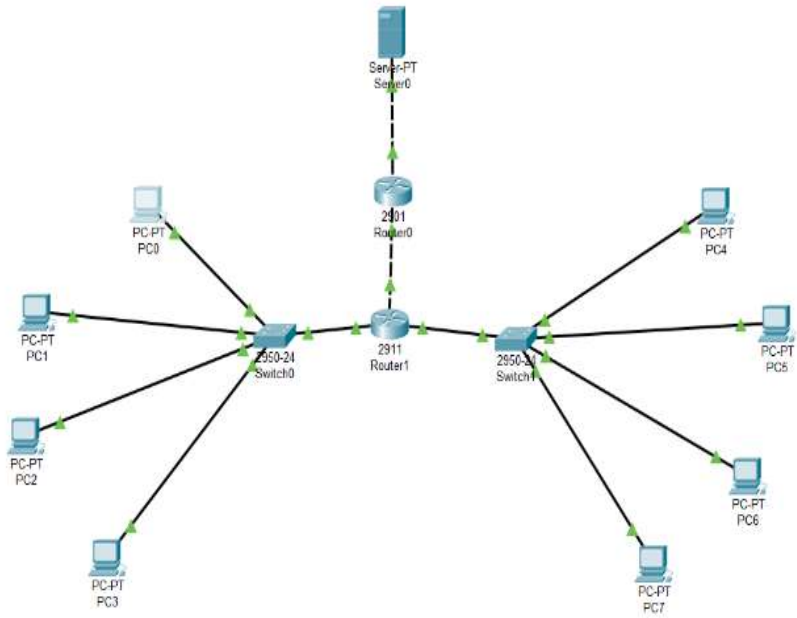
Salah satu contoh *packet filtering* adalah NAT *(Network Address Translation)* yang digunakan untuk membatasi akses secara langsung dan melindungi *traffic* yang keluar dari *router*. NAT dapat membuat *IP address* publik di jaringan dapat digunakan untuk mengakses alamat *host* di Internet dengan menerjemahkan *IP address* pribadi [10]. Tanpa NAT, IP pribadi di jaringan lokal tidak akan dapat mengakses Internet. NAT merupakan pemetaan *IP address*, perangkat di jaringan lokal akan mendapat alamat IP publik agar dapat mengekses jaringan publik. NAT memiliki model ganda yaitu NAT

dinamis dan NAT statis. NAT dinamis menggunakan logika manajemen beban, di mana tabel itu sendiri memiliki logika probabilitas dan solusi yang disematkan. Sedangkan NAT statis menggunakan translasi tetap dimana *IP address* yang ditetapkan sesuai dengan alamat asal. Sesuai dengan aturan yang telah ditabelkan dalam sebuah NAT, NAT statis akan melakukan *request* atau pengambilan dan pengiriman paket data [11]. NAT statis menggunakan dua *router*, yakni *router* luar dengan IP yang terhubung dengan internet serta *router* dalam yang memiliki IP yang terhubung dengan LAN [12].

Tujuan utama dari implementasi NAT menggunakan *packet tracer* adalah memetakan *IP address* jaringan lokal menjadi *IP address* jaringan internet pada komputer tertentu supaya dapat membatasi siapa saja yang dapat mengakses jaringan internet. Selain itu, tujuan lainnya guna menunjukkan hasil perbedaan antara IP *address* lokal yang diubah menjadi *IP address* jaringan internet yang tidak dapat diubah.

2. METODE

Simulasi jaringan ini dilakukan di Cisco Packet Tracer. Perangkat yang digunakan adalah sebuah server, 2 *router*, 2 *switch* dan 8 komputer. Perangkat-perangkat tersebut digunakan untuk membuat rancangan topologi jaringan menjadi seperti Gambar 1.



Gambar 1. Rancangan topologi jaringan

Pada topologi jaringan diatas diketahui bahwa Router1 bekerja sebagai NAT router. Setelah membuat rancangan topologi jaringan, Langkah selanjutnya adalah memberi *IP address* pada server dan masing-masing komputer. Pemberian *IP address* tersebut dilakukan sesuai data pada table berikut.

Tabel 1. Pemetaan *IP address*

Perangkat	IP Addreess	Subnet Mask	Gatway
Server	8.8.8.8	255.255.255.0	8.8.8.1
PC0	196.168.1.10	255.255.255.0	196.168.1.1
PC1	196.168.1.11	255.255.255.0	196.168.1.1
PC2	196.168.1.12	255.255.255.0	196.168.1.1
PC3	196.168.1.13	255.255.255.0	196.168.1.1
PC4	196.168.2.10	255.255.255.0	196.168.2.1
PC5	196.168.2.11	255.255.255.0	196.168.2.1
PC6	196.168.2.12	255.255.255.0	196.168.2.1
PC7	196.168.2.13	255.255.255.0	196.168.2.1

Selanjutnya akan terlihat perbedaan antara *IP address* yang terdaftar sebagai IP NAT dan yang tidak. Munculnya perbedaan tersebut dapat terlihat melalui perangkat pada PC5 dan PC6.

3. HASIL DAN PEMBAHASAN

Setelah pemberian *IP address* pada server dan masing-masing komputer dilakukan, langkah selanjutnya adalah mengkonfigurasi kedua router, memetakan *IP address* lokal dengan *IP address* publik, menentukan *interface* yang mengarah ke IP lokal dan IP publik pada Router1, serta langkah terakhir yang perlu dilakukan adalah melakukan pengaturan pada *router ISP* atau Router0.

3.1. Konfigurasi *Router*

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip address 25.25.25.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,

Router(config-if)#exit
Router(config)#int g0/1
Router(config-if)#ip address 8.8.8.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,

Router(config-if)#exit
Router(config)#
```

Gambar 2. Konfigurasi *Router0*

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip address 25.25.25.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#int g0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#int g0/2
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Gambar 3. Konfigurasi *Router1*

3.2. Memetakan IP Jaringan Lokal ke IP Publik

Pada tahap ini dilakukan pengaturan pada Router1 agar dapat mengubah IP lokal 192.168.1.10 menjadi IP publik yang terhubung dengan server yaitu 25.25.25.10. Konfigurasi ini sengaja tidak memetakan *IP address* dari PC5 dan PC6 agar nanti ketika dilakukan pengujian dapat terlihat perbedaannya.

```
Router(config)#ip nat inside source static 192.168.1.10
25.25.25.10
Router(config)#ip nat inside source static 192.168.1.11
25.25.25.20
Router(config)#ip nat inside source static 192.168.1.12
25.25.25.30
Router(config)#ip nat inside source static 192.168.1.13
25.25.25.40
Router(config)#
Router(config)#ip nat inside source static 192.168.2.10
25.25.25.50
Router(config)#ip nat inside source static 192.168.2.13
25.25.25.100
```

Gambar 4. Pemetaan IP *address* pada *Router1*

3.3. Menentukan *Inside* dan *Outside Interface*

Dilihat dari *design* dan konfigurasi *router*, *interface* pada g0/0 merupakan *interface* yang mengarah pada *global address* yaitu 25.25.25.0, sedangkan g0/1 dan g0/2 merupakan *local address.* Oleh karena itu, perlu dimasukkan perintah seperti gambar 5 pada *Router1*.

```
Router(config)#int g0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#int g0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int g0/2
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#
```

Gambar 5. Menentukan *inside* dan *outside interface* pada *Router1*

3.4. Mengatur *Router ISP*

Tujuan dari dilakukannya pengaturan pada *router ISP* adalah untuk mengenalkan *IP address* yang berada pada *Router1* atau *router NAT* pada *router ISP* atau *Router0*.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 25.25.25.1
```

Sintak 5. Menentukan *inside* dan *outside interface* pada *Router1*

Setelah menyelesaikan semua langkah diatas selanjutnya akan dilakukan uji pada NAT statis dengan cara masing-masing PC melakukan ping pada server dan *router ISP* sehingga diperoleh hasil sebagai berikut.

Tabel 2. Hasil uji coba ping

Perangkat	Server	Router ISP
PC0	V	V
PC2	V	V
PC3	V	V
PC4	V	V
PC5	X	X
PC6	X	X
PC7	V	V

Berdsarkan Tabel 2 terlihat bahwa PC dengan *IP address* yang tidak di petakan pada IP Publik tidak dapat mengakses server maupun *router ISP*. Langkah yang terakhir yaitu melihat NAT statis berjalan atau tidak dengan cara membuka Router1 dan memasukan perintah seperti berikut

```
Router1>enable
Router1#show ip nat translation
```

Jika Static NAT berhasil maka akan muncul keterangan seperti dibawah ini.

Tabel 2. Keterangan NAT statis yang berhasil

Pro	Inside global	Inside local	Outside local	Outside global
icmp	25.25.25.100: 21	192.168.2.13: 21	8.8.8.8:21	8.8.8.8:21
icmp	25.25.25.100: 22	192.168.2.13: 22	8.8.8.8:22	8.8.8.8:22
icmp	25.25.25.100: 23	192.168.2.13: 23	8.8.8.8:23	8.8.8.8:23
icmp	25.25.25.100: 24	192.168.2.13: 24	8.8.8.8:24	8.8.8.8:24

Ketika muncul keterangan seperti diatas artinya NAT statis berjalan dengan lancar. *Inside global* adalah *IP address* yang menerjemahkan IP lokal. *Inside local* adalah *IP address* lokal pada PC 7. *Outside local* adalah *IP address* yang menjadi tujuan saat dilakukan ping. *Outside Global* adalah IP Address tujuan.

4. SIMPULAN

Setelah melakukan percobaan seperti diatas, dapat disimpulkan bahwa uji coba yang dilakukan berhasil. PC yang tidak didaftarkan atau tidak di petakan *IP address*-nya tidak bisa masuk ke server atau ke internet. Oleh karena itu, hanya PC terpilih saja yang IP lokalnya sudah dipetakan ke IP global yang dapat mengakses server. Implementasi NAT statis ini tidak diragukan lagi serta mampu menjadikan jaringan komputer lebih aman dari *IP address* yang tidak dikenal yang ingin memasuki jaringan.

5. REFERENSI

[1] Iswati, H., dan Retnoningrum, E. 2019. Mengukur Layanan Website E-Govqual terhadap Kepuasan Masyarakat dalam Mengakses Rekap E-KTP. *Jurnal Serasi*, Vol. 17(2): 101-110.,

[2] Munawar, Z., and Putri, N. I. 2020. Keamanan Jaringan Komputer Pada Era Big Data. *J-SIKA| Jurnal Sistem Informasi Karya Anak Bangsa.* Vol. 2(01): 14–20.

[3] Arifah, D. A. 2011. Kasus Cybercrime di Indonesia. *Jurnal Bisnis Dan Ekonomi.* Vol. 18(2): 185–195.

[4] Setiawan, D. 2018. Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Budaya. *JURNAL SIMBOLIKA: Research and Learning in Communication Study.* Vol. 4(1): 62-72

[5] Natali, J., Fajrillah, F., dan Diansyah, T. M. 2016. Implementasi Static Nat Terhadap Jaringan Vlan Menggunakan Ip Dynamic Host Configuration Protocol (Dhcp). *Jurnal Ilmiah Informatika. Vol. 1*(1): 51–58.

[6] Abidin, D. Z. 2015. Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Ilmiah Media Processor.* Vol. 10(2): 1–8.

[7] Paramita, F., Alvina, O., Sentia, R. E., dan Kurniawan, A. 2021. Menggunakan Teknik Network Forensics. Jurnal Telematika. Vol. 14(2): 63-72.

[8] Purwoko, M., dan Hilal, H. 2019. Analisis Penerapan Firewall Nftables Sebagai Sistem Keamanan Server Pada Mesin Virtualisasi. *Jurnal Telekomunikasi Dan Komputer*. Vol. 9(1): 1-22.

[9] Suryana, N., dan Saputra, D. D. 2018. Perancangan Penggunaan Firewall dan Proxy Server Untuk. *Jurnal Sutet.* Vol. 8(1): 44–53.
[10] Dinata, M. 2020. Penerapan Metode Nat Dan Acls dengan Menggunakan Router di jaringan Lan pada Dinas Kominfo Oki. Universitas Bina Darma: Palembang.
[11] Sofana. (2012). *Penerapan Teknik Kriptografi Stream*. Informatika: Bandung
[12] Tujni, B. (2019). Implementasi Dynamic NAT dan IP DHCP Pada Jaringan Vlan Menggunakan Simulasi Packet Tracer. *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok).* Vol. 1(1): 109-116.