Perancangan Sistem Keamanan Jaringan Hotspot/Microtik OS

Romy Rajawali Nusantara Saifullah[1], Lola Sekar Arum[2], Joni Maulindar[3]

Teknik Informatika, Universitas Duta Bangsa Surakarta
Jl. Bhayangkara No. 55 Tipes Surakarta, Jawa Tengah

[1]202021085@mhs.udb.ac.id
[2]lolasa0807@gmail.com
[3]joni_maulindar@udb.ac.id

Abstrak—*Keamanan jaringan merupakan hal yang signifikan pada saat ini, keamanan jaringan, terutama di area hotspot WiFi. Sebagian besar ancaman yang menyerang jaringan Anda berasal dari pengguna internal jaringan hotspot itusendiri, sehingga keamanan jaringan nirkabel memerlukan perlakuan khusus. Oleh karena itu, perlu mengontrol akses ke setiap pengguna internal yang terhubung ke jaringan. Firewall merupakan salah satu solusi perlindungan jaringan komputer untuk mencegah tindakan tersebut. Metode yang berbeda digunakan, termasuk gateway level baris, gateway level aplikasi, dan firewall dengan pemfilteran paket. Contohnya adalah Contohnya adalah metode filter paket, yang menyaring lalu lintas pada lapisan jaringan seperti alamat IP dan port, tetapi karena persyaratan keamanan yang meningkat, keamanan dapat diterapkan dengan secara bersamaan memeriksa beberapa lapisan protokol jaringan dalam sistem. Ini membutuhkan infrastruktur dan peralatan yang tidak murah. Oleh karena itu, memerlukan perangkat dan sistem keamanan firewall yang ekonomis, efisien, dan berfungsi terbaik untuk melindungi jaringan computer. MetodePAT (Port Address Translation) adalah desain keamanan jaringan server yang memanfaatkan fungsi PATdari perangkat firewall.*

Kata kunci— **Perancangan, Sistem, Keamanan**

Abstract—*Network security is a significant thing at this time, especially network security in wireless hotspot areas. Wireless network security needs to get special handling, because most of the threats that attack the network come from the internal users of the hotspot network itself. Therefore, we need an access control for each internal user connected to the network. Firewall is one of the solutions to protect computer networks in preventing these actions. The methods applied also vary, including Circuit Level gateways, Application level gateways, and Packet Filtering firewalls. An example is the Packet Filtering method, data traffic will be filtered at the network layer including IP Address and Port, but the security needs are increasing, so we need a security that can inspect more than one layer of network protocols in one system, while to implement security This requires an infrastructure and equipment that is not cheap. So we need a firewall security device and system that is economical, efficient and able to work optimally to protect computer networks. The PAT (Port Address Translation) method is a server network security design that utilizes the PAT function on the firewall device.*

Keywords— **Security, System, Design**

I. PENDAHULUAN

[5] *Firewall* adalah solusi perlindungan jaringan komputer yang membahayakan kerahasiaan data dan mencegah serangan dan penyusup yang dapat merusak infrastruktur jaringan. Mekanisme yang diterapkan pada perangkat keras, perangkat lunak, atau sistem itu sendiri untuk melindungi beberapa atau semua hubungan antara segmen dalam jaringan pribadi dan jaringan eksternal di luarnya dengan menyaring, membatasi, atau melarangnya. Segmen dapat berupa*workstation*, *server*, *router*, atau *LAN (Local Area Network).*

Metode *firewall* ermasuk firewall packet filtering dan *NAT (Network Address Translation)*. Untuk memenuhi kebutuhan keamanan segmen jaringan komputer secara efektif dan aman, memerlukan firewall yang menerapkan pertahanan mendalam dan dapat memeriksa banyak lapisan protokol jaringan. *PAT (Port Address Translation)* sendiri merupakan salah satu fungsi dari *NAT (Network Address Translation)*, dan protokol *TCP* atau *UDP* yang dibuat antara host atau klien di jaringan lokal dapat ditransfer ke jaringan publik lain atau jaringan lokal. Mikrotik adalah sistem operasi router yang kaya fitur, salah satunya adalah sebagai *Router* dan *Firewall*. Berdasarkan latar belakang di atas, maka garis besar masalah adalah sebagai berikut :

a. Bagaimana menganalisa metode keamanan jaringan komputer saat menerapkan firewall menggunakan metode *PAT (Port Address Translation)* pada *OS* router Mikrotik.
b. Bagaimana menganalisa metode keamanan jaringan komputersaat menggunakan *firewall* dengan metode *packet filtering* (*access list*).
c. Bagaimana menganalisis perbandingan metode PAT (*Port Address Translation)* dengan metode *Packet Filter (access list)* sehingga didapatkan analisa dan metode terbaik.

Berdasarkan rumusan masalah di atas, tujuan yang dapat dicapai adalah:

a. Mampu menganalisa metode keamanan jaringan komputer dalam penerapan *firewall* menggunakan metodePAT (*Port Address Translation*) pada *Mikrotik Router OS*.

b. Mampu menganalisa metode keamanan jaringan komputer dalam penerapan *firewall* menggunakan metode *Packet Filter (*access list).
c. Mampu menganalisa perbandingan antara metode PAT (*Port Address Translation)* dengan metode *Packet Filter* (access list) sehingga didapatkan analisa dan metode terbaik.

Untuk menghindari pembahasan yang meluas, penulis melakukan analisis perbandingan *PAT (Port Address Translation)* dan *packet filtering* pada *Mikrotik Router OS*.

Manfaat dari penelitian ini adalah dengan menggunakan *OS router Mikrotik* sebagai firewall, Anda membangun keamanan di jaringan pribadi dengan mengancam infrastruktur jaringan dan memanfaatkan hak akses dari jaringan eksternal :

a. Manfaat Teoritis
   1) Dapat menjadi referensi untuk meningkatkan keamanan pada sebuah sistem.
   2) Sebagai penelitian yang berkaitan menggunakan penerapan *Firewall*yangmemakai metode *Port Address Translation (PAT)*dalam*Mikrotik Router OS*.
   3) Sebagai acuan untuk menganalisasistem firewall menggunakan metode Port Address Translation (PAT) pada*Mikrotik Router OS.*
b. Manfaat Praktis
   1) Dapat mendeteksi situs berbahaya dan dapat memblokir situs tertentu.
   2) Dapat dijadikan acuan dalam keamanan sistem sehingga dapat melindungi sistem dari ancaman-ancaman atau konten yang berbahaya dari luar sistem.

II. TINJAUAN PUSTAKA

Penelitian sebelumnya Pra penelitian merupakan salah satu referensi penulis sebagai sumber pendukung penelitian. Penelitian-penelitian sebelumnya dapat mencegah penulis untuk mengulangi penelitian-penelitian sebelumnya. Berikut ini adalah penelitian-penelitian sebelumnya yang berkaitan dengan penelitian-penelitian yang dilakukan.

Nama Penulis	Judul Penelitian	Hasil Penelitian
Efrahim Sinyo Rio Ola Balen Langobelen, Yuliana Rahmawati, Catur Iswahyudi (2019)	Analisis dan Optimasi dari Simulasi Keamanan Jaringan Menggunakan Firewall Microtik Studi Kasus di Taman Pintar Yogyakarta	Ananlisis dan Optimalisasi Sistem Keamanan Jarin gan pada Taman Pintar Yogyakarta
Joko Dwi Santoso (2020)	Analisis Perbandingan Metode Queue pada Mikrotik	Perbandingan Manajemen Bandwidth Dengan Metode Queue Simpel dan Queue Tree pada Jaringan Komputer Dengan Router Mikrotik
Lutfi Islami (2019)	Network Security with Mikrotik	Keamanan Jaringan Pada Mikrotik

Firewall sistem jaringan komputer diharapkan dapat melindungi informasi sensitif dan mengontrol akses lalu lintas dari dalam dan luar sistem. Untuk meningkatkan kinerja semua komponen terkait dan memanfaatkan koneksi atau jaringan internal atau eksternal untuk memberikan dampak positif bagi pengguna. Sebagai sistem keamanan jaringan dan komputer, firewall hanya cocok sebagai sistem keamanan dan tidak dapat digunakan sebagai satu-satunya sistem untuk melindungi jaringan itu sendiri. Oleh karena itu, harus dikombinasikan dengan beberapa metode keamanan lain untuk memperbaiki kekurangannya. Untuk meningkatkan keamanan jaringan, sistem harus memenuhi beberapa faktor, antara lain:

a. *Confidentiality* (kerahasiaan). Pembatasan akses hanya kepada *user* yang berhak atas suatu data atau informasi, dan mencegah akses dari *user* yang tidak memiliki hak.
b. *Integrity* (integritas).
   Keaslian data atau informasi yang dikirim dari sumber ke penerima melalui jaringan adalah lengkap tanpa modifikasi atau gangguan oleh orang yang tidak berwenang.
c. *Availability* (ketersediaan). Ketersediaan data atau informasi ketika dibutuhkan saat itu juga.

III. METODOLOGI PENELITIAN

a. Semua Jenis dan Sumber Data
   Pada penelitian ini, data yang digunakan untuk penelitian ini adalah data primer dan data sekunder. Dimana data yang diperoleh adalah hasil dari percobaan/pengalaman yang sudah pernah dipraktekan oleh penulis dan ada juga beberapa tambahan yang diperoleh dari sumber lain. Maka dari itu penulis menggunakan dua jenis sata dalam menyelesaikan penelitian ini. Dan selanjutnya untuk melakukan sebuah hasil penelitian ini maka penulis perlu menyiapkan beberapa device diantaranya yakni Laptop, Handphone, Mikrotik (Gateway), Kabel UTP, Aplikasi Winbox, Aplikasi TFGen.
b. Metode Pengumpulan Data
   Kumpulan alat dan bahan penelitian ini meliputi laptop sebagai alat untuk menjalankan perangkat lunak yang dibutuhkan seperti XAMPP v3.2.2, browser web Chrome, Winbox 2.2.16. Kumpulan alat dan sumber daya lainnya termasuk satu router firewall yang bertindak sebagai gateway server-ke-klien, firewall yang melakukan *translasi PAT (Port*

Address Translation) klien-ke-server, dan dua UTP 1 meter. Termasuk kabel. Spesifikasi minimum Cat5.

c. Metode Pengembangan Sistem

Pada metode *Port Address Translation*yang diterapkan pada sistem operasi router Mikrotik masih memerlukan pengembangan keamanan untuk menangani keamanan segmen aplikasi menggunakan metode *IPS (Intrusion Prevention System).*Pemfilteran dapat dilakukan tidak hanya pada*protocol port (layer transport)*tetapi juga pada lapisan aplikasi. Pada lapisan aplikasi, semakin banyak teknologi canggih yang dikembangkan yang dapat diserang kapan saja, di mana saja.

IV. KESIMPULAN

Dari keseluruhan materi yang telah dijelaskan pada analisis tersebut dapat disimpulkan bahwa :

a. Dengan menggunakan metode *Port Address Translation*, alamat *IP* yang sebenarnya di *server web* tidak ditampilkan ke klien, jaringan aman, dan terlindungi dari serangan peretas. Hal ini dibuktikan dengan analisis perbandingan traffic saat terjadi serangan *packet filter* dan kondisi serangan metode *PAT*.

b. Dengan menggunakan metode packet filtering yang digunakan yaitu metode Inspection masih memiliki kekurangan dalam menginspeksi paket data untuk traffic jaringan, sehingga harus dilakukan selective filtering agar benar-benar dapat dipilih saat melakukan filtering paket melalui traffic firewall. Untuk menghasilkan informasi log dan fungsionalitas sistem firewall, perlu adanya perbaikan lebih lanjut, baik dari segi metode yang digunakan maupun sistemnya.

REFERENSI

[1] A. Muzakir, M. U. (2019). *Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan*, 15-20.

[2] Abdullatteef, S. W. (2019). *An Implementation Of Firewall System Using Mikrotik* .

[3] Adani, R. M. (2021). *Sekawan Media*. Retrieved 4 4, 2022 from Firewall: Pengertian, Jenis, Fungsi, Manfaat, dan Cara Kerja: https://www.sekawanmedia.co.id/pengertian-firewall/

[4] Arifin, M. Agus Syamsul, Antoni Zulius. (2019). Bina Insan Linggau Menggunakan Teknik DMZ. *PERANCANGAN SISTEM KEAMANAN JARINGAN PADA UNIVERSITAS BINA INSAN LUBUKLINGGAU MENGGUNAKAN TEKNIK DEMILITARIZED ZONE (DMZ)*, 24.

[5] Buchari, A. (2019). *ANALISIS DAN IMPLEMENTASI FIREWALL DENGAN METODE PORT ADDRESS TRANSLATION PADA MIKROTIK OS*.

[6] Islami, L. (2019). *Keamanan Jaringan dengan Mikrotik - Laporan Praktikum Jaringan Komputer*. Retrieved 4 1, 2022 from Luizbuz: http://luisbuz.blogspot.com/2019/12/keamanan-jaringan-dengan-mikrotik_10.html

[7] Jejaring. (2021). *Berikut Ini Pengertian ISP, Fungsi, dan Cara Kerjanya*. Retrieved 4 1, 2022 from Jejaring: https://www.jejaring.web.id/pengertian-isp-fungsi-dan-cara-kerjanya/

[8] Santoso, J. D. (2020). *Analisis Perbandingan Metode Queue Pada Mikrotik*, 1-7.

[9] W. Purba, R. E. (2021). *Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT*, 143-158.