JURNAL DEVICE, VOL. 11 NO.2, 21-29
ISSN: 0216-9185| eISSN: 2746-8984

IMPLEMENTASI FILTERING FIREWALL DAN HARDENING WEB SERVER UNTUK MENCEGAH SERANGAN HTTP DOS PADA DINAS LINGKUNGAN HIDUP PEMATANGSIANTAR

Rizki Josua Tampubolon[1)], Poningsih[2)], Solikhun[3)], Indra Gunawan[4)], Zulaini Masruro Nasution[5)]

[1,4,5)] STIKOM Tunas Bangsa,Pematangsiantar,Indonesia Jl.Jend.Sudirman Blok A-B No.1,2,3 Pematangsiantar, 21127, Indonesia

[2,3)] AMIK Tunas Bangsa, Jl.Jend.Sudirman Blok A-B No.1,2,3 Pematangsiantar, 21127, Indonesia

Email: rizkijosuatampubolon@gmail.com[1)], poningsih@amiktunasbangsa.ac.id[2)], solikhun@amiktunasbangsa.ac.id[3)], indra@amiktunasbangsa.ac.id[4)], zulaini@amiktunasbangsa.ac.id[5)]

ABSTRAK

Denial of Service (DoS) merupakan masalah keamanan jaringan yang saat ini sedang berkembang. Semakin tinggi kapasitas komputasi suatu komputer penyerang, serangan DoS yang dapat dihasilkan juga semakin berbahaya. Serangan ini dapat menyebabkan ketidakberdayaan *server* untuk melayani *service request* yang sah, karena itu serangan DoS sangat merugikan dan perlu diberikan antisipasi yang efektif agar keamanan *web server* aman dari serangan *Denial of Service* (DoS). Terkadang *internet* disalahgunakan dengan adanya waktu luang setelah kegiatan maupun saat kegiatan berlangsung seperti mengakses *browser*, media sosial serta mengakses *youtube*. Tanpa disadari kemungkinan adanya sebuah serangan muncul yang dapat mengakibatkan lambatnya internet sehingga terjadinya kegagalan akses pada *internet*. Maka diperlukan adanya penerapan *filtering firewall* serta *hardening web server* dengan menggunakan *mikrotik router* untuk memblokir akses *internet* untuk menunjang kegiatan pekerjaan pegawai Dinas Lingkungan Hidup Pematangsiantar lebih baik dan nyaman.

Kata Kunci : *Denial of Service* (DoS), *Hardening Web Server*, *Filtering Firewall*, *Mikrotik Router*

ABSTRACT

Denial of Service (DoS) is a network security problem that is currently developing. The higher the computing capacity of an attacker's computer, the DoS attacks that can be generated are also more dangerous. This attack can cause the server's powerlessness to serve legitimate service requests, therefore DoS attacks are very detrimental and need to be given effective anticipation so that web server security is safe from Denial of Service (DoS) attacks. Sometimes the internet is misused by having free time after activities or during activities such as accessing browsers, social media and accessing YouTube. Without realizing it, the possibility of an attack appears that can result in slow internet so that access to the internet fails. Therefore, it is necessary to implement firewall filtering and web server hardening using a proxy router to block internet access to support the work activities of Pematangsiantar Environmental Service employees better and more comfortably.

Keywords: *Denial of Service (DoS), Hardening Web Server, Filtering Firewall, Mikrotik Router*

1. PENDAHULUAN

Penyediaan informasi dalam bentuk halaman web pada layanan saat ini sudah merupakan sebuah kebutuhan, karena akan mempermudah dan mempercepat penyebaran informasi. Namun dalam prosesnya ternyata ada saja masalah yang dialami baik itu berasal dari dalam misalnya koneksi maupun dari luar misalnya serangan terhadap layanan yang bersumber dari *internet*. Jenis serangan yang sering mematikan layanan adalah serangan DOS (*Denial Of Service*). Serangan DoS merupakan ancaman keamanan dimana penyerang menghabiskan sumber daya jaringan *internet* pada *server*, oleh sebab itu *host* target menolak akses dari pengguna yang berhak dimana layanan dari *host* menjadi tidak tersedia, maka dengan itu serangan mengganggu ketersediaan sistem.

Berdasarkan observasi yang dikerjakan penulis pada Dinas Lingkungan Hidup Pematangsiantar terjadinya lambatnya mengakses pada layanan *internet* serta penggunaan *internet*. Masalah ini diakibatkan oleh adanya waktu luang setelah kegiatan maupun saat kegiatan sering kali dimanfaatkan pegawai untuk melakukan *browsing* situs, membuka situs pemutar audio maupun video serta membuka situs media sosial untuk mengisi waktu luang. Tanpa disadari adanya kemungkinan sebuah serangan muncul yang dapat terjadinya kegagalan akses serta lambatnya *internet*, sehingga pekerjaan yang dilakukan oleh pegawai-pegawai mengalami terkendala yang mengakibatkan performa Dinas Lingkungan Hidup Pematangsiantar Menurun. Pada Dinas Lingkungan Hidup Pematangsiantar sistem keamanannya masih ada celah untuk masuknya sebuah serangan yang mungkin terjadi. Untuk itu diperlukan adanya sistem keamanan yang dapat mengatasi masalah tersebut.

Berdasarkan latar belakang masalah yang telah diuraikan, maka terdapat beberapa masalah utama dalam penelitian yaitu bagaimana melakukan *filtering firewall* agar pegawai tidak dapat mengakses situs tertentu serta *hardening web server*.

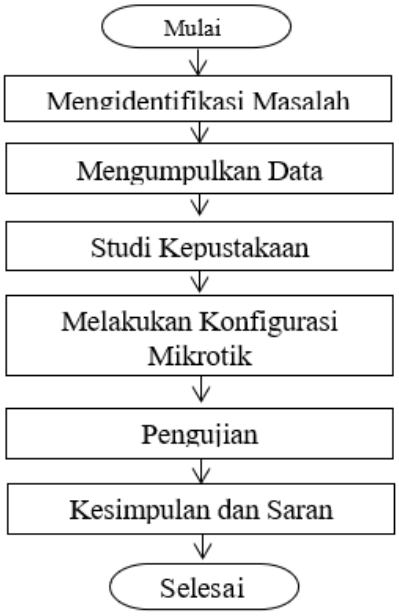
Tujuan Penelitian Ini ialah untuk membangun sistem *proxy server* pada *router mikrotik*, membangun sistem yang bisa memblokir situs serta membangun sistem *internet* yang baik untuk *user*

Berdasarkan masalah tersebut, penulis memberi solusi yaitu melakukan *firewall filter rule* akses *internet*, serta melakukan pemblokiran situs. Melalui konfigurasi mikrotik dapat mengatasi masalah diatas. *Mikrotik* adalah sistem operasi yang berbasis perangkat lunak (*software*) dimana digunakan untuk membuat komputer sebagai *router* suatu jaringan. *Router* merupakan sebuah alat dimana bisa menyambungkan dua atau lebih jaringan komputer yang berbeda. manfaat penelitian ini yaitu meningkatkan keamanan pada jaringan internet serta memfilter akses internet untuk blokir situs agar pekerjaan pegawai lebih terkendala.

2. METODE

Metode yang dipakai dalam penelitian ini adalah *filtering firewall* serta *hardening web sever*, dimana tujuan metode ini memblokir situs serta *hardening web server* dari serangan Dos.

2.1. Rancangan Penelitian



Gambar 2.1 Rancangan Penelitian

2.2. **Prosedur Pengumpulan Data**

Dalam melakukan penelitian ada beberapa prosedur dalam penumpulan data, yaitu:

1. Wawancara yaitu Melakukan wawancara dengan sekretaris Dinas Lingkungan Hidup Pematangsiantar untuk mendapatkan data maupun informasi yang berkaitan dengan penggunaan jaringan *internet* di Dinas Lingkungan Hidup Pematangsiantar.
2. Observasi (Pengamatan) yaitu penulis melakukan pengamatan atau observasi secara langsung ke Dinas Lingkungan Hidup Pematangsiantar untuk memperoleh data yang akan digunakan.
3. Penelitian Kepustakaan *(Library Research)* yaitu memanfaatkan perpustakaan, buku, prosiding atau jurnal sebagai media untuk bahan referensi dalam menentukan parameter yang dipakai dalam penelitian.
4. Sumber data penelitian diambil dari Kantor Dinas Lingkungan Hidup Pematangsiantar.

2.3. **Analisis Data**

Tahap ini adalah pengumpulan data untuk mengetahui perumusan masalah dengan cara menyelesaikan masalah tersebut. Dalam hal ini mengidentifikasi sistem sedang berjalan dan mencoba menganalisa pengembangan sistem seperti apa yang cocok di terapkan.

2.3.1. Alat Analisis Data

Bahan yang digunakan untuk penelitian ini adalah perangkat jaringan pada Dinas Lingkungan Hidup Pematangsiantar. Bahan tersebut akan digunakan sebagai sampel untuk ujicoba dalam pemblokiran menggunakan *Mikrotik.*

Dalam pengerjaan penelitian ini, alat penelitian yang digunakan untuk mendukung penelitian ini adalah *software* (*winbox*), *hardware* (laptop) serta *Mikrotik RB750r2.*

Gambar 2.2 Laptop dan *Mikrotik*

2.3.2. Instrumen Penelitian

Instrumen penelitian yang digunakan dalam penelitian ini berupa wawancara serta observasi terhadap Dinas Lingkungan Hidup Pematangsiantar tentang apa yang akan diamankan atau diblokir. Instrumen Penelitian merupakan alat ukur yang digunakan secara sistematis untuk mengumpulkan data penelitian.

Setelah melakukan wawancara serta observasi terhadap Dinas Lingkungan Hidup Pematangsiantar maka dilakukan pemblokiran. Untuk melakukan pemblokiran tersebut maka digunakan *mikrotik* dengan metode *filtering firewall* serta *hardening web server*.

2.3.3. Pemodelan Metode

Pada tahap ini, akan memecahkan model teknik *firewall* serta *hardening web server* yang biasa digunakan secara keseluruhan dalam pemfilteran satu layer, salah satunya adalah dengan menggunakan teknik *filtering firewall*. Jenis *firewall* ini memfilter paket data pada lokasi dan alternatif yang telah ditentukan untuk paket tersebut. Metode ini bekerja pada tingkat IP dari paket data dan menentukan pilihan akan tindakan berikutnya dilanjutkan atau tidak dilanjutkan tergantung pada kondisi paket tersebut. Metode ini dimaksukan untuk mengontrol aliran paket tergantung pada alamat asal, tujuan, *port* dan ciri informasi paket yang

terkandung dalam tiap paket. *Firewall* adalah sebuah cara atau komponen yang diterapkan pada *hardware* maupun *software* atau sistem dengan maksud untuk menjaga, baik dengan memisahkan, membatasi atau memutuskan sebagian koneksi/latihan pada jaringan dengan jaringan luar yang tidak ada dalam ruang lingkupnya.

3. HASIL DAN PEMBAHASAN

Pada bagian ini adalah hasil dalam penelitian terhadap perancangan berdasarkan hasil analisis. Tujuan penerapan rancangan metode *Filtering Firewall* dan *Hardening Web Server* pada Dinas Lingkungan Hidup Pematangsiantar adalah untuk mengimplementasikan rancangan yang telah dibuat untuk mempermudah pengguna dalam menggunakan *internet* dan pemblokiran situs. Pengujian rancangan jaringan ini menjelaskan tentang *filtering firewall* dan *hardening web server* dengan menggunakan perangkat keras dan perangkat lunak yang sudah disiapkan.

3.1. Implementasi Jaringan Mikrotik

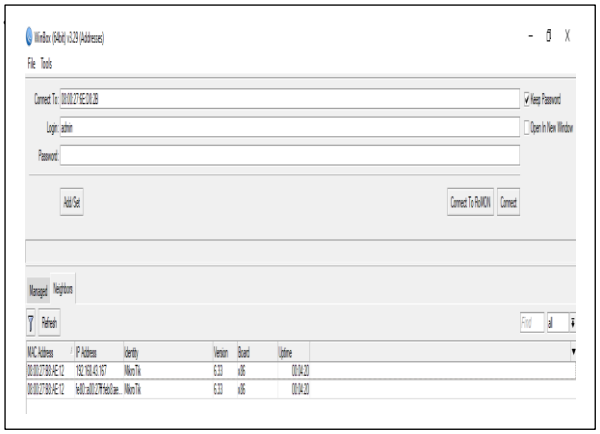
Rancangan yang digunakan dalam *Implementasi LAN Internet* pada Dinas Lingkungan Hidup Pematangsiantar yaitu menggunakan *router board* RB750r2 dan dilakukan pada 2 laptop, *modem 3G*, dan *Hub*. Tahap pertama yaitu menghubungkan *modem 3G* ke laptop, dengan *modem 3G* sebagai pusat *internet*, kemudian menghubungkan laptop (1) yang sudah terhubung *internet* ke *mikrotik* RB750r2, kemudian RB750r2 yang dihubungkan pada *Hub* dan menghubungkan laptop (2) ke *mikrotik* menggunakan kabel *UTP* untuk melakukan konfigurasi *mikrotik*. Pada penelitian ini aplikasi yang digunakan untuk mengkonfigurasi *mikrotik* yaitu aplikasi *winbox* dengan menggunakan aplikasi tersebut pada laptop.

Gambar 3.1 Gambar Perangkat Keras

3.2. Konfigurasi Mikrotik

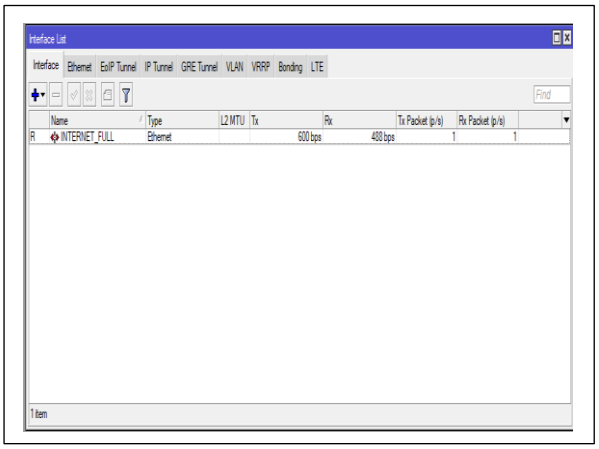
Konfigurasi *mikrotik* menggunakan aplikasi *winbox* dalam penerapan keamanan *internet* menggunakan model *filtering firewall* pada Dinas Lingkungan Hidup Pematangsiantar dan sistem operasi *mikrotik*. Dengan menggunakan *router board*, maka sistem operasi *mikrotik* secara otomatis sudah terinstal. Selanjutnya konfigurasi *mikrotik* dilakukan dengan menggunakan aplikasi *Winbox*. Berikut tampilan konfigurasi *mikrotik* menggunakan *winbox*.

Berikut konfigurasi *mikrotik* dengan menggunakan *Winbox*. *Setting Interface Mikrotik* dengan membuka *menu interface* maka akan tampil seperti Gambar 3.2 berikut ini.



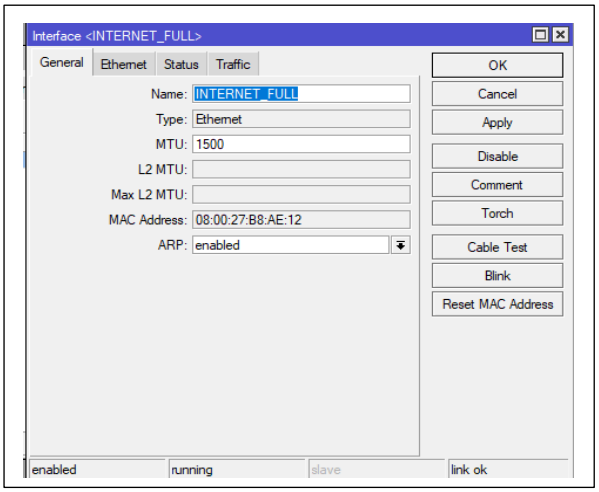
Gambar 3.2 Tampilan *Software Winbox*

Setelah masuk ke *menu interface* klik *MAC Addresss* yang sudah terdaftar di tampilan *winbox* tersebut, kemudian klik *connect* selanjutnya masuk ke interface list maka akan tampil seperti Gambar 3.3 dibawah ini :



Gambar 3.3 *Setingan Interface Mikrotik*

Selanjutnya ubah nama *interface Mikrotik* menjadi seperti gambar 3.4 dibawah ini :



Gambar 3.4 Tampilan *Interface Mikrotik*

Maka dapat dilihat seperti gambar diatas *setting* nama *Interface Mikrotik.*

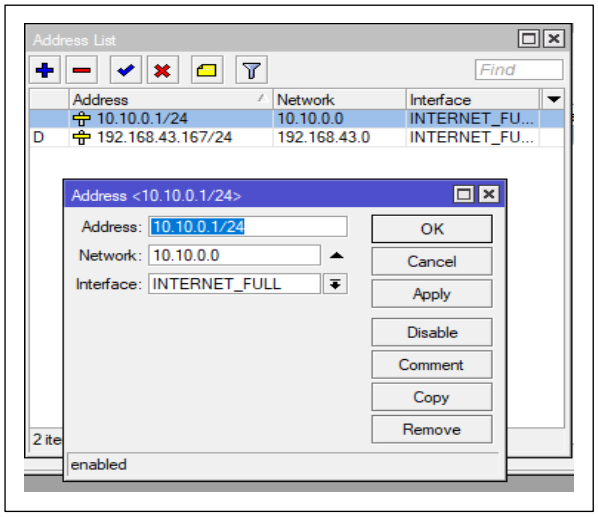
ether1 =====> Internet Dinas Lingkungan Hidup Pematangsiantar

Kemudian *Setting IP Address Mikrotik.* Dengan *IP Addresss* seperti berikut ini :

IP Addresss Modem = 192.168.43.167/24

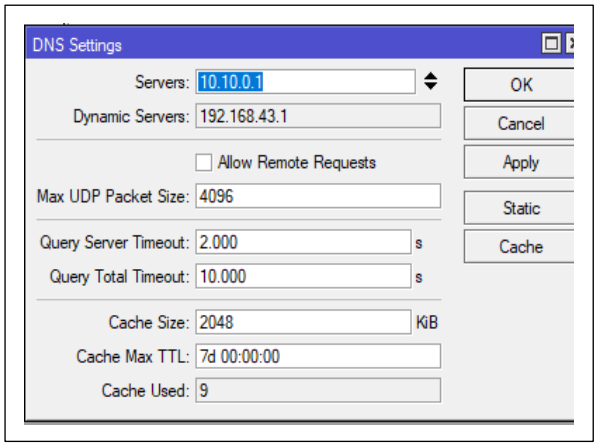
Di *Mikrotik* : *IP Addresss INTERNET_FULL* = 10.10.0.1/24

Dapat dilihat pada gambar 3.5 dibawah ini :



Gambar 3.5 Tampilan *Interface IP Address*

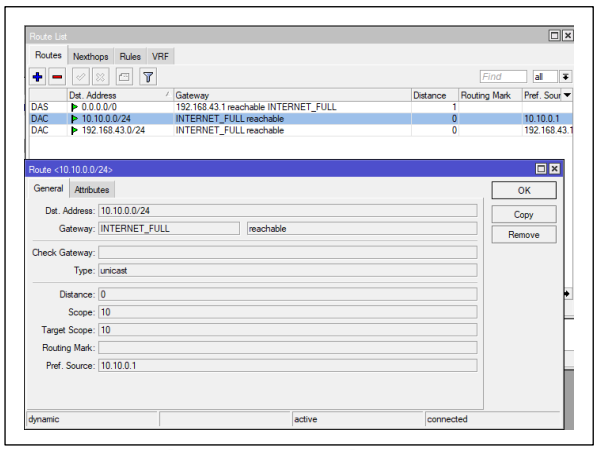
Setelah *IP Addresss mikrotik* diubah, selanjutnya berikan *DNS server* yang akan di isi dengan *IP Addresss* yang berasal dari modem. Dapat dilihat pada gambar 3.6 dibawah ini :



Gambar 3.6 Tampilan *DNS Server*

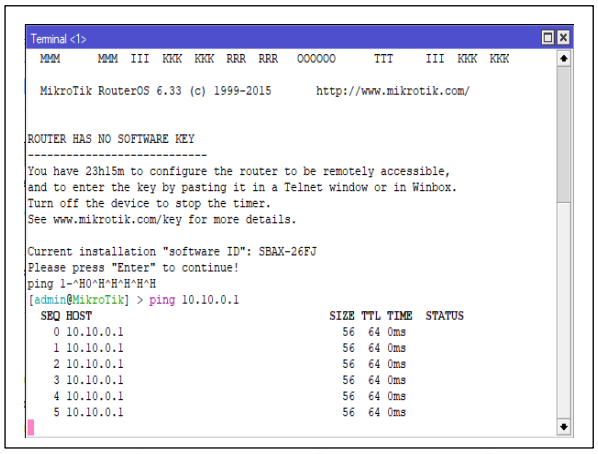
Setelah *DNS Server* sudah di konfigurasi lanjut ke konfigurasi *Routers*, memberikan *Default Gateway* dengan *IP*

Addresss Modem. Dapat dilihat pada gambar 3.7 dibawah ini :



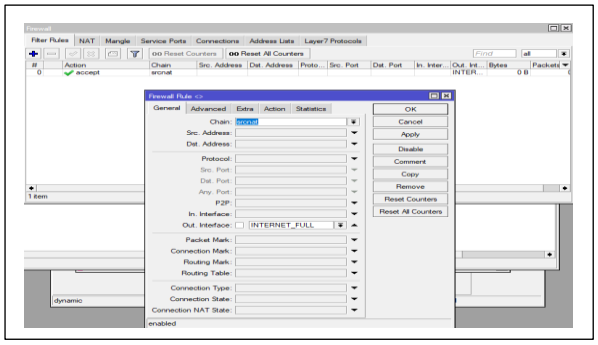
Gambar 3.7 Tampilan *Routers*

Setelah proses konfigurasi *Routers* selesai lakukan pengujian pada modem, modem memiliki *IPAddress* 10.10.0.1 seperti pada gambar 3.8 dibawah ini :



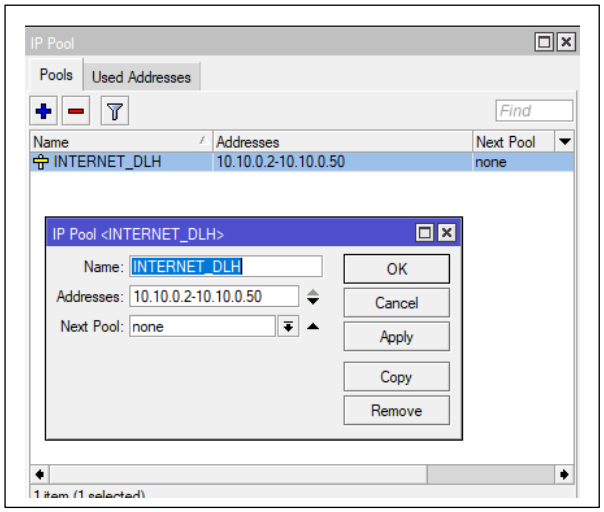
Gambar 3.8 Tampilan *Ping Modem*

Selanjutnya konfigurasi agar *Client* terhubung ke *internet*, yaitu dengan cara mengkonfigurasi *Firewall rules*. Seperti pada gambar 3.9 dibawah ini :



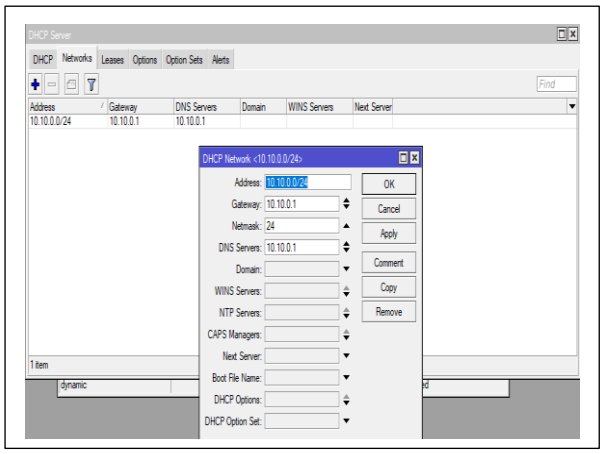
Gambar 3.9 Tampilan *Firewall rules*

Selanjutnya membuat *IP Pool* agar *Client* tidak mengisi *IP Addresss* secara manual. Dapat dilihat pada gambar 3.10 dibawah ini :



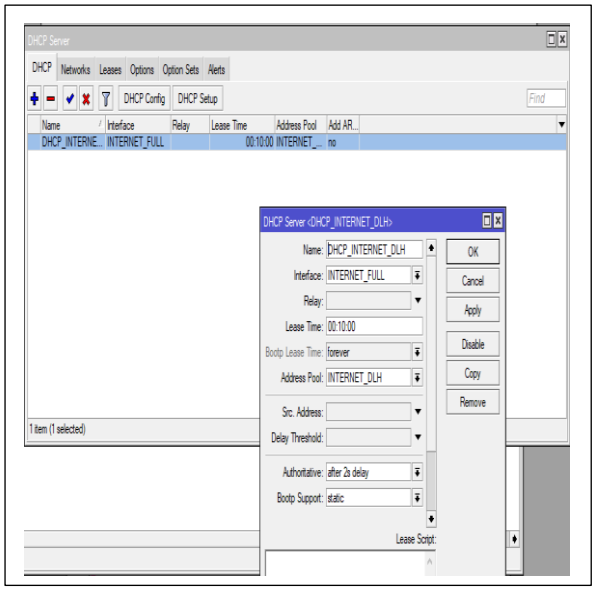
Gambar 3.10 Tampilan *IP Pool*

Setelah konfigurasi *IP Pool* selesai dilakukan selanjutnya konfigurasi *Network* yang ada di *DHCP server* seperti pada gambar 3.11 dibawah ini :



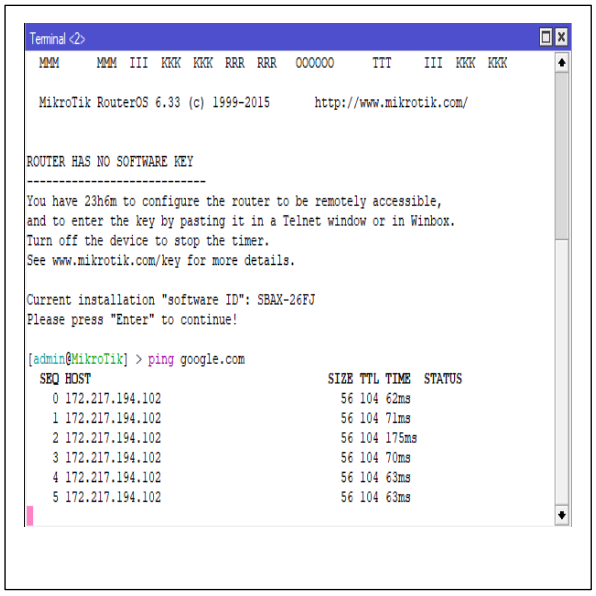
Gambar 3.11 Tampilan *DHCP Network*

Langkah selanjutnya melakukan tahapan konfigurasi *DHCP Server* dapat dilihat pada gambar 3.12. berikut.



Gambar 3.12 Tampilan *DHCP Server*

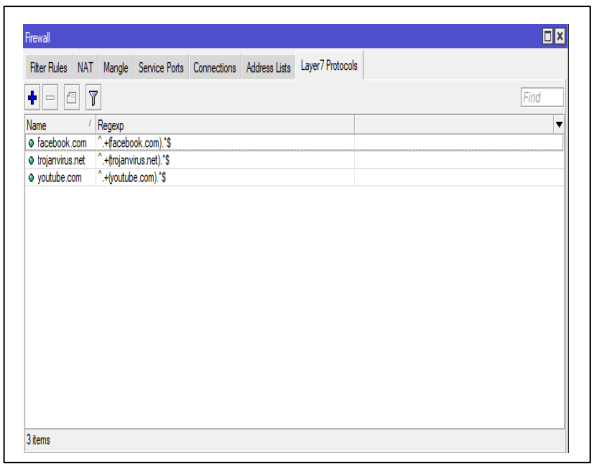
Konfigurasi *DHCP Server* sudah di buat, *Hub* sudah bisa terhubung ke *internet*. Selanjutnya dilakukan *test* dengan Ping *Google.com*. Dapat dilihat pada gambar 3.13 dibawah ini :



Gambar 3.13 Tampilan *Ping Google.Com*

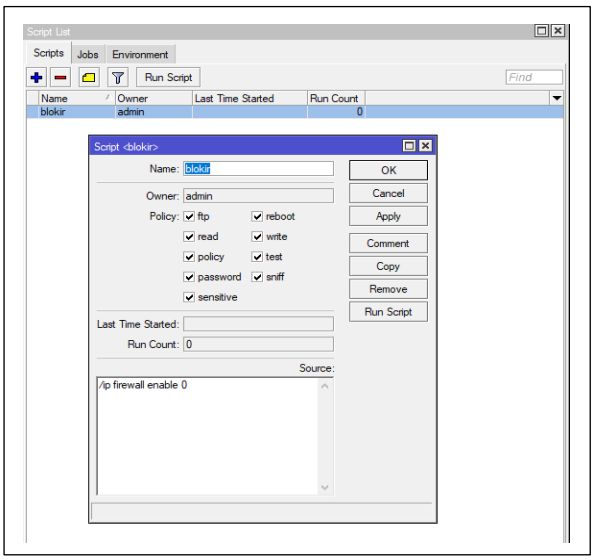
3.3. *Konfigurasi Filtering Firewall dan Hardening Server*

Selanjutnya dilakukan proses untuk mengkonfigurasi pemblokiran situs, seperti situs *Facebook*, *Youtube* yang di konfigurasi menggunakan *Layer 7 Protokol*, dapat dilihat pada gambar 3.14 dibawah ini :



Gambar 3.14 Tampilan *Layer 7 Protocol*

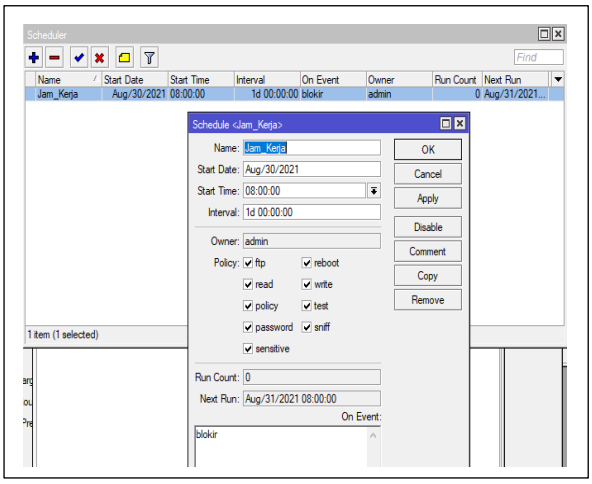
Setelah melakukan konfigurasi *Layer 7 Protokol* dilanjutkan dengan konfigurasi *Script List*. *Script List* berfungsi sebagai pintu apakah *Layer 7 Protokol* bisa melewati atau tidak. Dapat dilihat pada gambar 3.15 dibawah ini :



Gambar 3.15 Tampilan *Script List*

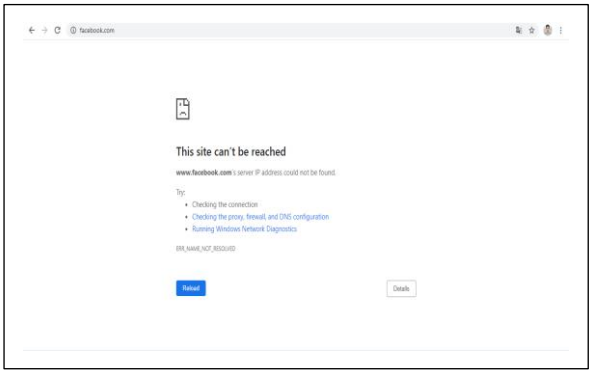
Selanjutnya konfigurasi *Scheduler* dalam hal ini untuk mengatur waktu. *Scheduler* digunakan untuk mengatur waktu mulai dilakukannya pengeblokan situs tertentu, waktunya bisa diatur sesuai keperluan

user. Dapat dilihat pada gambar 3.16 dibawah ini :



Gambar 3.16 Konfigurasi *Scheduler*

Selanjutnya melalukan pengujian pemblokiran pada *browser*. Dapat dilihat pada gambar 3.17 dibawah ini ;



Gambar 3.17 Hasil Blok *Facebook*

4. PENUTUP

4.1. Kesimpulan

Berdasarkan pengujian yang dilakukan dalam penelitian ini maka dapat disimpulkan bahwa:

1. Penggunaan perangkat *LAN Internet* yang didukung oleh *Mikrotik* memberikan kontribusi bagi upaya mengontrol situs akses dari pegawai dinas lingkungan hidup. Dengan adanya mikrotik lebih teratur dalam pengelolaan penggunaan internet.
2. Dengan penggunaan perangkat *LAN* yang didukung oleh *Mikrotik*, dapat mengawasi pengguna dalam pengaksesan situs menjadi lebih terkontrol dan pemakaian kuota jaringan internet menjadi tepat guna.
3. Penelitian ini diperuntukan pada Dinas lingkungan hidup pematangsiantar dengan memberikan sistem keamanan jaringan dengan memanfaatan *Mikrotik*, sehingga pegawai dapat menggunakan jaringan internet secara *free* yang aman dan terkontrol dengan baik. Serta mengamankan jaringan dari serangan Dos

4.2. Saran

Dengan mempertimbangkan keterbatasan waktu dan pengetahuan yang dimiliki oleh peneliti maka sangat diperlukan pengembangan selanjutnya di masa mendatang. Adapun saran pengembangan tersebut antara lain sebagai berikut:

1. Konfigurasi ini hanya memblokir akses internet seperti Facebook, Youtube serta melakukan *Scheduler* untuk akses internet.
2. Dapat dikembangkan dengan metode lain maupun software yang lain.

5. DAFTAR PUSTAKA

Andi, S. (n.d.). *Penanganan dan Pencegahan Insiden pada Serangan DoS di Jaringan Komputer Sesuai Rekomendasi NIST 800-61 EL6115 Secure Operation and Incident Response Syaiful Andy 13212050*. 1–17.

Anugrah, I., & Rahmanto, R. H. (2018). Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone. *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, *5*(2), 91–106. https://doi.org/10.33558/piksel.v5i2.271

Ardianto, F. (2020). Penggunaan mikrotik router sebagai jaringan server. *Penggunaan Router Mikrotik*, *1*, 26–31.

Arman, M. (2020). Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack. *JATISI (Jurnal Teknik Informatika*

Dan Sistem Informasi), *7*(1), 56–70. https://doi.org/10.35957/jatisi.v7i1.284

Hawari, M. S. (2016). Penerapan Iptables Firewall Pada Linux Dengan Menggunakan Fedora. *Jurnal Manajemen Informatika*, *6*, 198–207.

Informatika, D. M., Teknik, F., Surabaya, U. N., Informatika, T., Teknik, F., & Surabaya, U. N. (n.d.). *IMPLEMENTASI KEAMANAN JARINGAN INTRUSION DETECTION / PREVENTION SYSTEM MENGGUNAKAN PFSENSE Bima Putra Firdaus I Made Suartana*.

Muslim, B., & Dayana, L. (2016). Sistem Informasi Peraturan Daerah (Perda) Kota Pagar Alam Berbasis Web. *Jurnal Ilmiah Betrik*, *7*(01), 36–49. https://doi.org/10.36050/betrik.v7i01.11

Putri, A., Fatoni, & Solikin, I. (2016). Analisa Kinerja Koneksi Jaringan Komputer Pada Smk Teknologi Bistek Palembang. Universitas Bina Darma, 12, 1–11. https://ejournal.unsrat.ac.id/index.php/elekdankom/article/view/10400/9986

Putra, R. S., Mayasari, R., & Karna, N. B. A. (2018). Implementasi Dan Analisis Keamanan Jaringan Virtual HIPS Snort Pada Layanan Web Server Dengan Penyerangan DOS DAN DDOS. *E-Proceeding of Engineering*, *5*(3), 4958–4965.

Rahmatulloh, A., & MSN, F. (2017). Implementasi Load Balancing Web Server menggunakan Haproxy dan Sinkronisasi File pada Sistem Informasi Akademik Universitas Siliwangi. *Jurnal Nasional Teknologi Dan Sistem Informasi*, *3*(2), 241–248. https://doi.org/10.25077/teknosi.v3i2.2017.241-248

R, Mulyaman. (2020). Penjelasan pengertian hardening. *https://rifqimulyawan.com/*

Riska, P., Sugiartawan, P., & Wiratama, I. (2018). Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking. *Jurnal Sistem Informasi Dan Komputer Terapan Indonesia (JSIKTI)*, *1*(2), 53–64. https://doi.org/10.33173/jsikti.12

Saleh, S. B. (2019). *JURNAL GERBANG , VOLUME 9 No . 2 AGUSTUS 2019 Optimasi Bandwidth Hits Local Up To Dengan Transparent Proxy 2 . 7 Lusca Menggunakan Metode Network Development Life Cycle Amat Suroso Akses internet sekarang ini sudah menjadi suatu kebutuhan sebagian orang* ,. *9*(2), 26–34.

Sugiyono. (2016). Sistem keamanan jaringan komputer menggunakan metode watchguard firebox pada pt guna karya indonesia. *Jurnal CKI*, *9*(1), 1–8.

Supendar, H. (2016). Penerapan Linux Zentyal Sebagai Filtering Dan Bandwidth Management Pada Jaringan Pt . Anta Citra Arges. *Jurnal Teknik Komputer Amik Bsi*, *II*(24), 22–30.

Suyuti Ma'sum, M., Azhar Irwansyah, M., & Priyanto, H. (2017). Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. *Jurnal Sistem Dan Teknologi Informasi (JUSTIN)*, *5*(1), 56–60.

Tashia. (2017). Keamanan jaringan internet dan firewall. *https://aptika.kominfo.go.id/*

Tedyyana, A., & Kurniati, R. (2016). Membuat Web Server Menggunakan Dinamic Domain. *Jurnal Teknologi Informasi & Komunikasi Digital Zone*, *7*(1), 1–10. https://ejurnal.unilak.ac.id/index.php/dz/article/view/178

Walad, I., Ilmu, F., Dan, K., & Utara, U. S. (2020). *Analisis Denial of Service Attack Pada Sistem Keamanan Web*.