IMPLEMENTASI ACCESS CONTROL LIST (ACL) DALAM PERANCANGAN VIRTUAL LOCAL AREA NETWORK PADA SMKN 1 AL-MUBARKEYA

Andi Al-furqan Abra, Aulia Syarif Aziz
Pendidikan Teknologi Informasi, Universitas Islam Negeri Ar-Raniry
Jl. Syeikh Abdul Rauf Darussalam Banda Aceh, Indonesia
andifurqan38@gmail.com

ABSTRAK

Sekolah sebagai lembaga pendidikan memiliki peran penting dalam membekali siswa dengan berbagai ilmu pengetahuan dan keterampilan, termasuk dalam bidang teknologi informasi dan komunikasi. Dalam mendukung proses belajar mengajar, jaringan yang handal dan memadai menjadi salah satu kebutuhan utama. SMKN 1 AL-Mubarkeya, sebagai sekolah yang memiliki jurusan Teknik Komputer Jaringan (TKJ) dan Rekayasa Perangkat Lunak (RPL), tentu saja sangat bergantung pada sistem jaringan komputer untuk memperlancar kegiatan pembelajaran.Namun, dengan semakin banyaknya penggunaan internet di kalangan siswa dan guru, muncul tantangan baru berupa potensi gangguan keamanan jaringan, atau mengakses data secara tidak sah. Oleh karena itu, pengamanan jaringan menjadi salah satu aspek yang sangat penting untuk diperhatikan dalam pengelolaan jaringan sekolah. Untuk itu, penerapan metode keamanan menjadi langkah yang diperlukan agar jaringan internet yang digunakan tetap aman dan stabil.Penelitian ini bertujuan untuk mengimplementasikan pengamanan jaringan di SMKN 1 AL-Mubarkeya dengan menggunakan metode *Access Control List* (ACL) pada router Mikrotik melalui aplikasi Winbox. Metode ACL pada Mikrotik memungkinkan pengaturan akses internet secara selektif dan terbatas untuk setiap klien di jaringan, yang bertujuan untuk memastikan hanya perangkat yang berhak yang dapat mengakses internet sesuai dengan kebutuhan masing-masing. Dengan penerapan ACL, diharapkan sekolah dapat membatasi penggunaan internet oleh siswa sesuai dengan peruntukannya, sehingga meningkatkan keamanan dan kestabilan jaringan.

Kata kunci : *Access Control List (ACL),Mikrotik,Winbox*

1. PENDAHULUAN

Internet adalah jaringan komputer global yang telah menjadi kebutuhan utama di berbagai bidang, terutama di lingkungan kerja dan pendidikan. Internet memungkinkan perangkat seperti komputer, smartphone, dan alat komunikasi lainnya untuk terhubung dan berinteraksi dalam jaringan global melalui internet. Dengan berkembangnya teknologi jaringan komputer, muncul pula tantangan baru terkait keamanan[1].

Teknologi ini berkembang pesat, mencakup penggunaan sumber daya jaringan bersama, baik perangkat keras maupun perangkat lunak. Sejalan dengan itu, muncul kebutuhan untuk menyempurnakan jaringan guna mengoptimalkan efisiensi dan keamanan. Salah satu solusi yang dihadirkan adalah *Virtual Local Area Network* (VLAN), yang memungkinkan pemisahan dan segmentasi jaringan komputer menjadi beberapa bagian tanpa perubahan fisik. VLAN memberikan fleksibilitas dan efisiensi dalam mengelola jaringan, termasuk menghubungkan LAN tanpa batasan lokasi geografis, memanfaatkan DHCP untuk distribusi IP, serta NAT untuk menghubungkan host dengan jaringan berbeda tanpa mengganggu VLAN lainnya.

Namun, seiring dengan peningkatan kebutuhan jaringan yang kompleks, diperlukan kontrol lebih lanjut terhadap akses dan keamanan. *Access Control List* (ACL) menawarkan solusi dalam mengelola lalu lintas antara VLAN. ACL berfungsi sebagai pengendali akses, mengizinkan atau menolak aliran data berdasarkan kebijakan yang diterapkan[2].

Implementasi ACL dalam perancangan VLAN memungkinkan administrator jaringan untuk membatasi akses antar-VLAN secara efektif, memperkuat keamanan, dan membatasi akses hanya kepada pengguna yang diizinkan. Selain itu, ACL membantu dalam segregasi lalu lintas, memastikan bahwa setiap departemen atau kelompok pengguna memiliki jalur lalu lintas yang aman dan terpisah. Hal ini penting untuk menghindari potensi serangan dan menjaga kinerja jaringan tetap andal[3].

Berdasarkan alasan-alasan tersebut, penelitian ini bertujuan untuk mengevaluasi implementasi ACL dalam perancangan VLAN di SMKN 1 Al-Mubarkeya guna meningkatkan keamanan dan kinerja jaringan sekolah tersebut.

2. TINJAUAN PUSTAKA

Penelitian ini memperoleh referensi dari beberapa dokumen dan jurnal dalam membantu penelitian sehingga dapat memposisikan penelitian serta menujukkan orsinalitas dari penelitian yaitu:

Jurnal dengan implementasi *Access Control List* Dalam Perancangan *Virtual Local Area Network* pada PT Cakramedia Indocyber yang ditulis oleh Reza Aditya Pratama pada tahun (2019). Pada tulisan ini dibahas bagaimana penerapan *Virtual Local Area Network* (VLAN) dan keamanan *switch port* dapat dilakukan untuk membatasi akses pengguna antar jaringan perusahaan, *Access Control List* (ACL)

digunakan untuk menerapkan peran akses sehingga jaringan hanya dapat mengirimkan data yang diizinkan sesuai dengan kebutuhan komunikasi perusahaan. Penelitian ini menggunakan ACL router standar karena belum diketahui kebutuhan khusus pembatasan data TCP dan UDP untuk perusahaan[4].

Judul dengan implementasikan Implementasi Keamanan Jaringan Komputer *Local Area Network* Menggunakan *Access Control List* pada Perusahaan X yang ditulis oleh M. Alvian Habib Nasution pada tahun (2020). Pada tulisan ini dibahas bagaimana penerapan metode Vlan *Access Control List* adalah salah satu metode untuk meminta akses jaringan internet atau komunikasi data dan mengirimkan sejumlah paket data dari satu komputer ke komputer lainnya. Hasil reset penulis menunjukkan bahwa dengan menggunakan metode *filtering* dan pembagian pengguna koneksi internet, Vlan *Access Control List* dapat menyaring dan mengidentifikasi pengguna yang telah di batasi aksesnya, sehingga mereka dapat mendapatkan akses ke pengguna lain atau ke server di Perusahaan X[5].

Jurnal dengan judul Implementasi PCI- DSS untuk keamanan data kartu pembayaran pada PT Dharma Lautan Nusantara yang di tulis oleh Fahrizal, dkk pada tahun (2022). Tulisan ini membahas cara mengidentifikasi perangkat yang melakukan proses, mengirim (transmit), menerima (receive), dan menyimpan (save) informasi dan komunikasi data. Fokus pengamanan tulisan ini adalah informasi kartu kredit karena memperkecil ruang lingkup pengamanan melalui pembagian jaringan VLAN, penggunaan Router ACL untuk mengatur jalur komunikasi data di jaringan, dan penggunaan[6].

2.1. Jaringan Komputer

Jaringan komputer adalah "jaringan kombinasi perangkat keras, perangkat lunak, dan pengkabelan (cabling), yang memungkinkan berbagai alat komputasi berkomunikasi satu sama lain." Salah satu perangkat berfungsi untuk menghubungkan jaringan komputer dengan perangkat "tanpa kabel", yang merupakan teknologi komunikasi yang menggunakan gelombang radio untuk bertukar data. Jaringan tanpa kabel ini dikenal sebagai jaringan telekomunikasi, jaringan telekomunikasi adalah jenis jaringan yang banyak digunakan dalam jaringan komputer. Ini digunakan untuk jarak kurang dari tiga meter dengan bluetooth dan sangat jauh dengan satelit[7].

2.2. Mikrotik

Mikrotik router memiliki berbagai fitur jaringan dan nirkabel yang lengkap, menjadikannya salah satu sistem operasi yang dapat diandalkan untuk router jaringan (Pamuji et al., 2020). Mikrotik juga memiliki kemampuan untuk berfungsi sebagai firewall. Paket filtering adalah metode yang akan digunakan firewall untuk mengatur paket yang menuju, melewati, atau dituju. Ini mengatur apakah paket diterima, diteruskan, atau ditolak[8].

2.3. Access Control List

Salah satu cara untuk melakukan packet filtering adalah dengan menggunakan *Access Control List* (ACL). *Access Control List* memberi network administrator kemampuan untuk mengontrol paket-paket yang dapat diakses melalui proxy server. Dalam aplikasi winbox, ACL dapat digabungkan dengan perintah http_access untuk menentukan apakah paket-paket akan ditolak atau diterima masuk ke sistem. Daftar kontrol akses adalah dasar *filtering* untuk aplikasi Winbox[9].

2.4. Winbox

Winbox adalah aplikasi manajemen berbasis GUI yang digunakan untuk konfigurasi dan pemantauan perangkat jaringan MikroTik. Aplikasi ini memudahkan administrator jaringan dalam mengelola pengaturan router dan *switch* MikroTik dengan antarmuka yang mudah dipahami, baik melalui koneksi langsung maupun jarak jauh[10].

3. METODE PENELITIAN

3.1. Metode Pengumpulan data

Metode ini bertujuan untuk mendukung dalam mendapatkan informasi dalam mencapai tujuan penelitian. Tahapan dalam pengumpulan data bisa dilakukan dengan berbagai macam cara, dibawah ini adalah tahapan-tahapan dalam pengumpulan data yang dilakukan.

3.2. Observasi

Penulis melakukan pengamatan langsung di SMKN 1 Al-Mubarkeya yang berkaitan dengan masalah yang diambil dan mencatat hasilnya secara langsung. Pengamatan tersebut termasuk penerapan *Access Control List* dalam perancangan *Virtual Local Area Network*. Kegiatan observasi menunjukkan skema jaringan SMKN 1 Al-Mubarkeya saat ini.

3.3. Wawancara

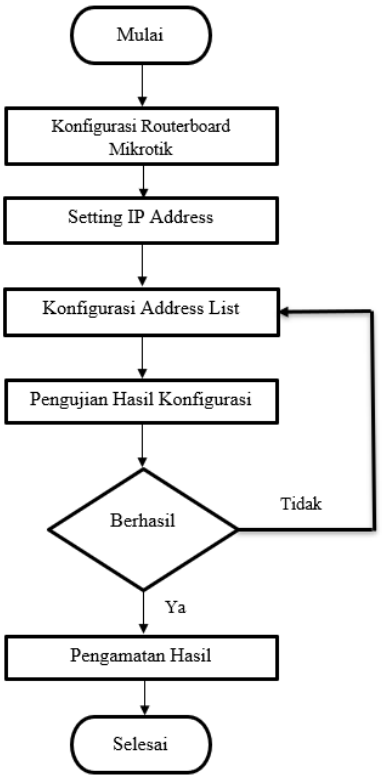
Penulis melakukan tanya jawab dengan orang-orang yang terlibat dalam kegiatan sistem jaringan komputer untuk mendapatkan gambaran lengkap tentang subjek penelitian.

3.4. Studi Literatur

Selain aktivitas di atas, penulis juga melakukan penelitian kepustakaan dengan melihat referensi-referensi dari karya penelitian sebelumnya, jurnal-jurnal yang membahas masalah serupa, dan informasi dari internet.

3.5. Rancangan Penelitian

Adapun rancangan alur penelitian ditunjukkan pada gambar di bawah**:**



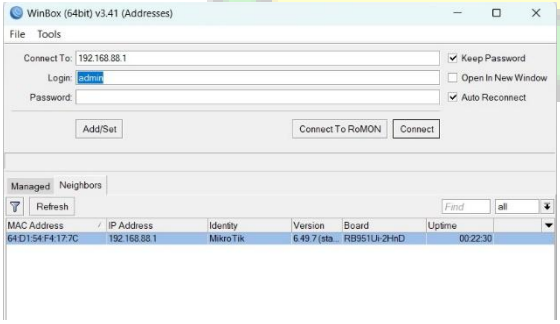
Gambar 1. Flowchat perancangan penelitian

Dari *flowchat* gambar 1 dapat dilihat langkah pertama yang harus dilakukan adalah konfigurasi routerboard MikroTik, kemudian melakukan setting IP *address* pada winbox untuk menentukan IP *address* mana saja yang diperbolehkan mengakses internet. Kemudian melakukan konfigurasi *address list* untuk menentukan IP mana saja yang tidak akan mendapat akses internet. Setelah melakukan konfigurasi, tahap selanjutnya adalah melakukan pengujian untuk memastikan bahwa konfigurasi berfungsi dengan baik. Setelah itu, penulis memeriksa hasil konfigurasi untuk memastikan bahwa hanya IP *address* yang terdaftar di *address list* yang dapat mengakses internet, dan IP *address* yang tidak terdaftar di *address list* tidak dapat mengakses internet.

4. HASIL DAN PEMBAHASAN

4.1. Konfigurasi Mikrotik

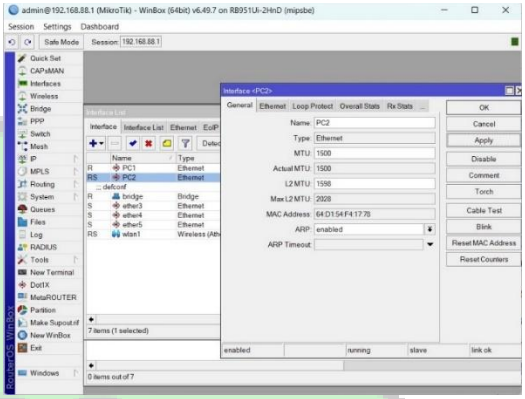
a. Login aplikasi winbox



Gambar 2. Login winbox

Sebelum memulai konfigurasi, buka aplikasi Winbox untuk masuk ke server Mikrotik. Klik pada bagian "Connect To" untuk memilih perangkat Mikrotik yang akan kita akses. Untuk login menggunakan admin, masukkan password yang telah diatur. Setelah masuk, masuk berhasil.

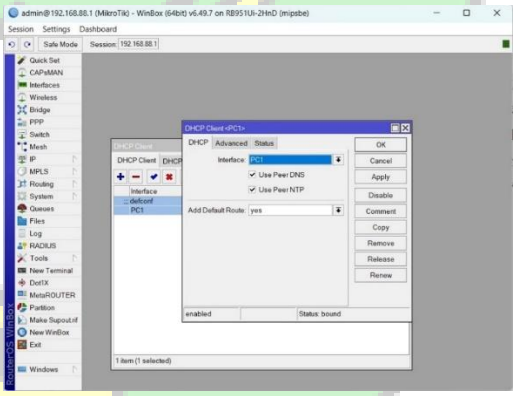
b. Konfigurasi Interface



Gambar 3. Menu setting interface

Pada gambar 3 ada tampilan menu *Interface* lalu kita kasih nama pada Ether-1 yaitu PC1 untuk WAN dan PC2 untuk LAN.

c. Setting DHCP client

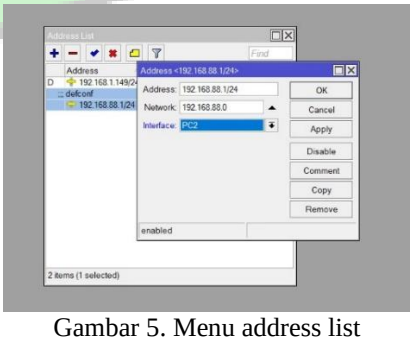


Gambar 4. Menu setting dhcp client

Pada gambar 4 kita setting dhcp client pada menu IP kita setting dhcp client, lalu pada kolom *interface* ubah menjadi PC1 lalu apply.

4.2. Setting IP Address

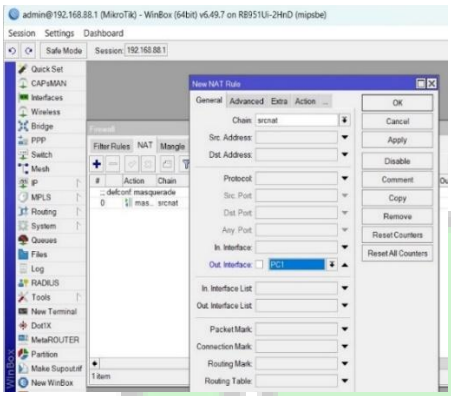
a. Masukan IP *address*



Gambar 5. Menu address list

Setelah setting dhcp client kita lanjut ke menu IP dan *address* masukkan IP private lalu *interface* nya ubah jadi PC2.

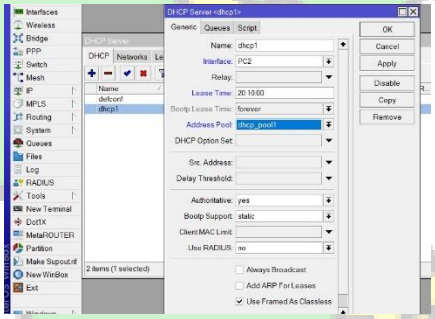
b. Setting NAT



Gambar 6. Menu setting nat

Pada gambar 6 menunjukkan bagaimana *firewall* menyamarkan IP lokal menjadi IP publik agar dapat terhubung ke internet. Dalam menu IP, *firewall* memilih kolom NAT. Lalu tambahkan kolom baru di menu General masukan pada kolom *chain* = *scrnat* kemudian *Out Interface* = PC1, kemuadian di menu *Action* = *masquerade*.

c. Setting DHCP Server

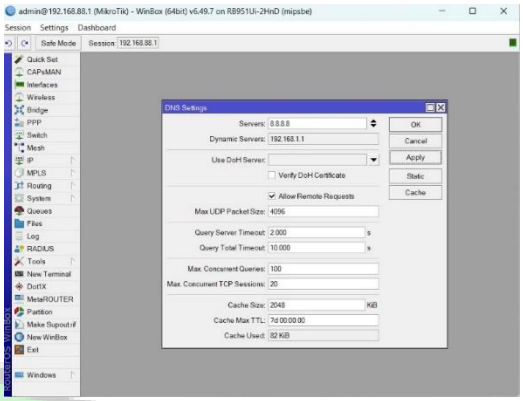


Gambar 7. Menu setting dhcp client

Pada bagian menu IP,DHCP Server pilih DHCP Setup, selanjutnya di name pilih dhcp1, kemudian di *interface* pilih PC2 dan di *address* pool pilih dhcp_pool1 seperti gambar di atas.

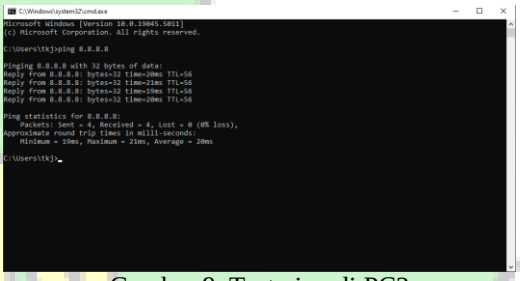
d. Setting DNS Server

Selanjutnya setting DNS pilih pada menu IP,DNS Setting masukan Server 8.8.8.8 seperti gambar di bawah.



Gambar 8. Menu setting dns server

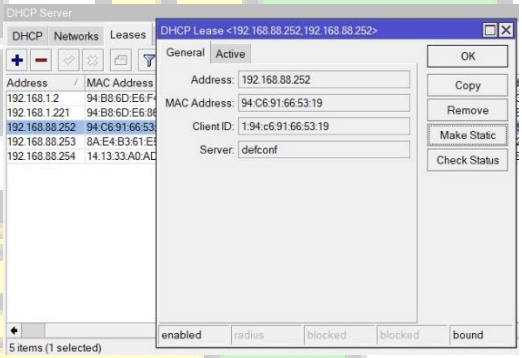
e. Test Koneksi Internet dari Client



Gambar 9. Test ping di PC2

Pada gambar 9 kita test ping di PC2 apakah internet nya berjalan, ya seperti gambar di atas bahwa setelah kita ping internet nya berjalan.

f. Setting IP Static Client

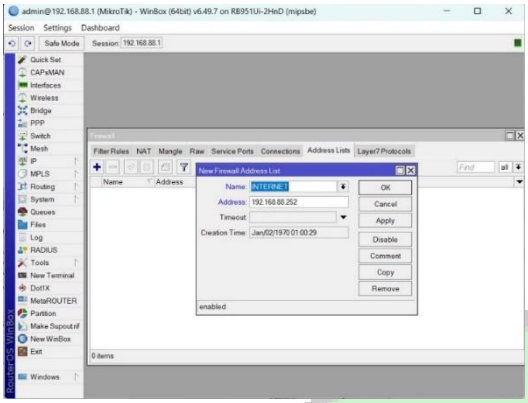


Gambar 10. Setting IP static

Pada gambar 10 kita setting IP static di bagian menu IP, DHCP Server, Leases lalu ubah IP Client menjadi static dengan klik “make static”.

4.3. Konfigurasi Address List

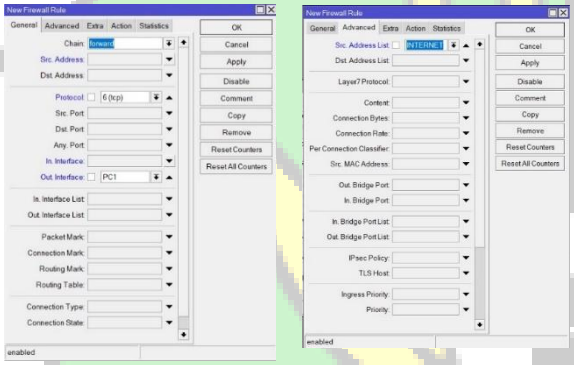
a. Setting *Address List*



Gambar 11. Menu setting address list

Pada gambar 11 setting *address list* di bagian menu *Firewall* lalu *Address List* masukan nama disini saya isikan nama INTERNET, lalu isi IP *Address* yang ingin di daftarkan lalu “apply”

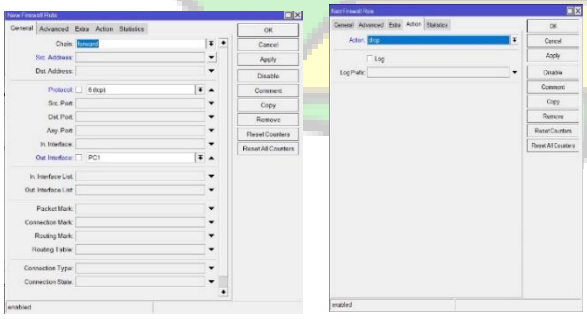
b. Konfigurasi Filter Rule Accept Internet



Gambar 12. Konfigurasi filter rule

Pada gambar 12 konfigurasi filter rule di bagian menu IP, *Firewall* lalu Filter Rule Klik “+” di kolom *Chain* isi *forward*, Protocol (6TCP), lalu di *Out Interface* pilih (PC1), selanjutnya di bagian *advanced Src Address* (INTERNET), di bagian *Action* (Accept).

c. Konfigurasi Filter Rule Drop Internet

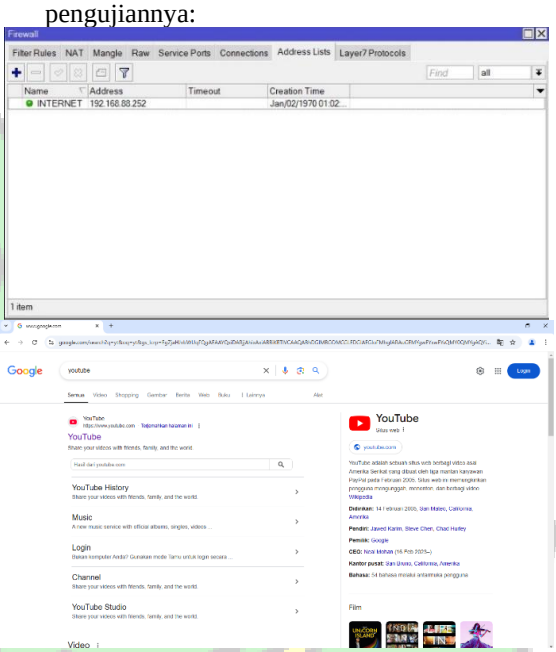


Gambar 13. Konfigurasi Filter Rule Drop

Pengujian dibagi menjadi dua, awal dan akhir. Pengujian awal belum melibatkan implementasi ACL dan pengujian akhir sudah melibatkan implementasi ACL, lalu diujikan pada PC2.

1. Pengujian Awal

Pengujian awal dilakukan sebelum implementasi ACL, berikut adalah hasil pengujiannya:

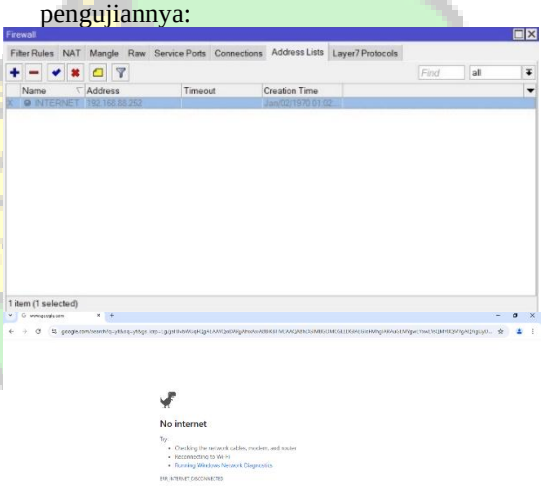


Gambar 14. Hasil pengujian awal

Pengujian awal dengan PC2 untuk melihat apakah masih ada akses internet atau tidak dan hasilnya adalah terdapat akses internet.

2. Pengujian Akhir

Pengujian akhir dilakukan sesudah implementasi ACL, berikut adalah hasil pengujiannya:



Gambar 15. Hasil pengujian akhir

4.4. Pengujian Hasil

Pengujian akhir dengan PC2 untuk melihat apakah PC2 masih ada akses internet atau tidak dan hasilnya adalah tidak terdapat akses internet.

Konfigurasi di atas menunjukkan bahwa pengujian kami dengan metode *Packet Filtering* menggunakan menu *Access Control List* (ACL) di *Firewall* berhasil. Metode ini memungkinkan kami untuk memfilter paket internet, dengan hanya IP *Address* yang terdaftar pada *Address List* yang dapat mengakses internet, dan IP *Address* yang tidak terdaftar pada *Address List* tidak dapat mengakses internet.

5. KESIMPULAN

Setelah proses penelitian dan analisis dilakukan di lab SMKN 1 AL-Mubarkeya, beberapa kesimpulan yang dihasilkan adalah sebagai berikut:

1. Sebelum ini, SMKN 1 AL-Mubarkeya tidak memfilter paket internet. Akibatnya, siswa yang tidak membutuhkan internet dalam proses belajar mengajar dapat menggunakan internet untuk melakukan hal-hal seperti mendownload film atau menghidupkan YouTube.

2. Pengujian kami berhasil setelah konfigurasi keamanan jaringan dengan *Packet Filtering* melalui metode *Access Control List* (ACL) yang tersedia di menu Firewall. Ini memungkinkan kami untuk memfilter paket internet, dengan hanya IP *Address* yang terdaftar pada *Address List* yang dapat mengakses internet, dan IP *Address* yang tidak terdaftar pada *Address List* tidak dapat mengakses internet.

DAFTAR PUSTAKA

[1] S. Prayoga, “Analisa Manajemen Bandwith Simple Queue Dan Queue Tree,” vol. 3, no. 3, pp. 95–101, 2021.

[2] F. Amarudin. Ulum, “Desain Keamanan Jaringan Pada Mikrotik Router Os Menggunakan Metode Port Knocking,” *J. teknoinfo*, vol. 12, no. 2, pp. 72–75, 2018.

[3] C. C. Wijaya and A. S. Budiman, “Perancangan Keamanan Jaringan Komputer Pada Router Dengan Metode ACL Pada PT. Aruna Sinar Jaya Jakarta,” *J. Zetroem*, vol. 5, no. 2, pp. 180–186, 2023, doi: 10.36526/ztr.v5i2.3077.

[4] Reza Aditya Pratama, “Perancangan Jaringan LAN dan Keamanan Wireless Internet Hotspot Berbasis Mikrotik Router Pada CV. Gemilang,” *eprints.udb.ac.id*, 2019, [Online]. Available: https://eprints.udb.ac.id/id/eprint/67

[5] A. T. Laksono and M. A. H. Nasution, “Implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X,” *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 83, 2020, doi: 10.30865/json.v1i2.1920.

[6] P. Pada, P. T. Dharma, and L. Nusantara, “SWADHARMA (JEIS),” vol. 02, 2022.

[7] M. J. N. Yudianto, “Jaringan Komputer dan Pengertiannya,” *Ilmukomputer.Com*, vol. Vol.1, pp. 1–10, 2014.

[8] B. Cahya, F. Rizki, A. Sutiyo, Y. El Saputra, and M. Elfarizi, “Implementasi *Firewall* Pada Mikrotik Untuk Keamanan Jaringan,” *J. JOCOTIS-Journal Sci. Inform. Robot. E*, vol. 1, no. 2, pp. 63–80, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[9] M. R. Amar, S. Anwar, and O. Nurdiawan, “Optimalisasi Menggunakan Access Control List Berbasis Mikrotik pada Amami Event Organizer,” *MEANS (Media Inf. Anal. dan Sist.*, vol. 7, no. 1, pp. 117–123, 2022, doi: 10.54367/means.v7i1.1800.

[10] Candra A.M, Jupriyadi, and Samsugi.S, “Perancangan dan Implementasi Controller Access Point System Manager (CAPsMAN) Mikrotik Menggunakan Aplikasi Winbox,” *J. Telemat. Inf. Technol.*, vol. 02, no. 2, pp. 26–32, 2021, [Online]. Available: https://ejurnal.teknokrat.ac.id/index.php/teleftortech/article/view/1990