Perancangan Keamanan Jaringan Komputer Pada Router Dengan Metode ACL Pada PT. Aruna Sinar Jaya Jakarta

[1] Cahyo Candra Wijaya, [2] Ade Surya Budiman
[12] Teknologi Informasi, Universitas Bina Sarana Informatika, Jakarta Pusat
[1]cahyocandrawijaya56@gmail.com, [2]ade.aum@bsi.ac.id

Abstract - At PT. Aruna Sinar Jaya, the Internet network plays an important role in running the company's wheel. The problem is that some client computers that do not require an internet connection in their work still have access to the Internet, sometimes the Internet is overused that is not related to work. To solve the above problems, network security methods such as Access Control List (ACL) are needed to make Internet use in Aruna Sinar Jaya more controlled and efficient. In this case, the author recommends implementing ACL on Mikrotik routers using Winbox to restrict internet connections.

Keywords: Access Control List, Microtic Router, Winbox.

Abstrak - Pada PT. Aruna Sinar Jaya, jaringan internet berperan penting dalam menjalankan roda perusahaan. Masalah di temukan ialah beberapa komputer client yang tidak membutuhkan koneksi internet dalam pekerjaannya masih dapat mengakses internet, terkadang internet digunakan secara berlebihan yang tidak berkaitan dengan pekerjaan. Untuk mengatasi permasalahan di atas diperlukan metode keamanan jaringan seperti Access Control List (ACL) agar penggunaan internet pada PT. Aruna Sinar Jaya menjadi lebih terkontrol dan efesien. Dalam hal ini, penulis merekomendasikan untuk mengimplementasikan ACL pada router Mikrotik menggunakan Winbox untuk membatasi koneksi internet.

Kata kunci: Access Control List, Router Mikrotik, Winbox.

I. Pendahuluan

Seiring kemajuan teknologi, internet menjadi sarana jaringan komputer yang sangat bebas di akses, sehingga semua jaringan komputer yang ada membutuhkan model sistem keamanan demi menjaga jaringan baik dari dalam maupun luar. Perlu untuk memastikan keamanan jaringan komputer yang terhubung langsung ke Internet dari berbagai jenis aktivitas yang menganggu terjadi di internet [1]

PT. Aruna Sinar Jaya memiliki permasalahan dengan beberapa komputer *client* yang seharusnya tidak membutuhkan akses internet dalam pekerjaannya masih mengakses internet. Oleh karena itu, di balik permasalahan tersebut diperlukan suatu sistem keamanan jaringan untuk mengontrol akses antar jaringan yang terhubung dengan router atau menentukan lalu lintas tertentu yang diizinkan masuk dan keluar dari jaringan yang digunakan, yaitu penggunaan *Access Control List* (ACL) router perusahaan.

Untuk mengatur akses ke sumber daya jaringan dan melindungi jaringan dari akses yang tidak sah, Access Control List (ACL) adalah alat yang paling sering digunakan dalam situasi seperti ini. *Access Control List* (ACL) adalah alternatif yang aman untuk jaringan komputer. ACL sangat berguna untuk kontrol lalu lintas jaringan. ACL mengizinkan atau menolak paket ke tujuan tertentu. ACL terdiri dari aturan dan kondisi yang mendefinisikan dan mengendalikan lalu lintas jaringan router dan menunjukkan apakah paket dapat melewatinya atau tidak [2]. ACL yang tepat dapat memastikan bahwa sumber daya jaringan hanya dapat diakses oleh entitas yang berwenang dan meningkatkan efisiensi penggunaan internet.

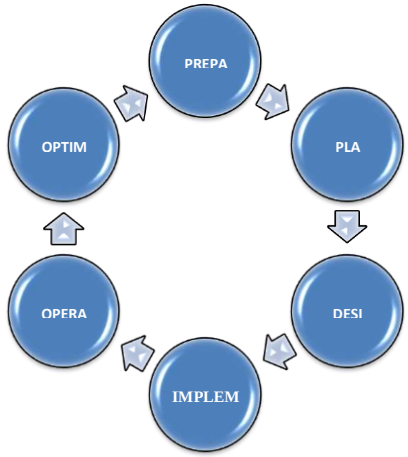
Meskipun ACL menawarkan banyak keuntungan, implementasinya dalam organiasi perusahaan menghadapi berbagai masalah saat menerapkan ACL, seperti menentukan kebijakan akses yang tepat, mengelola daftar akses yang besar, dan memastikan bahwa ACL tetap up-to-date dengan perubahan kebutuhan bisnis. Penulis melakukan penelitian bagaiamana cara menerapkan sistem keamanan jaringan pada router dengan menggunakan metode ACL serta mensimulasikan konfigurasi ACL pada *router* menggunakan perangkat lunak *Cisco Packet Tracer*.

II. Metode Penelitian

Metode penelitian ini didasarakan pada permasalahan terkait tidak adanya pengontrolan hak akses setiap pengguna jaringan internet serta kurangnya sistem keamanan jaringan komputer di setiap *router* perusahaan. Untuk itu peneliti mengembangkan model jaringan PPDIOO.

Model pengembangan jaringan PPDIOO adalah PPDIOO adalah metodologi desain jaringan untuk mendukung pengembangan jaringan. PPDIOO terdiri dari beberapa tahapan yaitu persiapan, perencanaan, perancangan, implementasi, pengoperasian dan optimalisasi. Seiring berkembangnya teknologi, dibutuhkan metode dan metodologi untuk mendukung perancangan jaringan komputer. Siklus PPDIOO menyajikan model siklus pada setiap tahapan, dan selalu terkait [3]. Ruang lingkup penelitian ini dibatasi oleh beberapa faktor yaitu membahas pembatasan hak akses, mengacu pada penerapan ACL pada router serta membahas implementasi ACL *Extended.*

Teknik pengumpulan data melibatkan observasi langsung, wawancara dengan tim IT dan pengguna jaringan, serta distribusi kuesioner untuk mendapatkan gambaran mendalam tentang kondisi jaringan saat ini dan kebutuhan pengguna. Sementara itu, Model Pengembangan Jaringan PPDIOO, yang terdiri dari tahapan *Prepare*, *Plan*, *Design*, *Implement*, *Operate*, dan *Optimize*, digunakan sebagai kerangka kerja untuk merencanakan, mendesain, menerapkan, dan mengoptimalkan solusi jaringan yang sesuai dengan kebutuhan dan tantangan yang dihadapi oleh PT. Aruna Sinar Jaya.



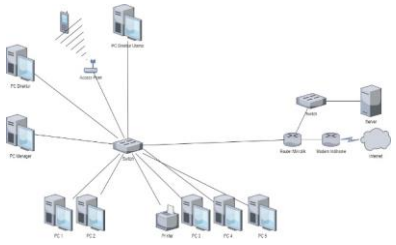
Gambar 1 Model Pengembangan Jaringan PPDIOO

III. Hasil dan Pembahasan

A. Analisis Permasalahan

Menurut pengamatan penulis, salah satu masalah yang dihadapi PT. Aruna Sinar Jaya adalah jaringan internet sering mengalami penurunan kinerja karena tindakan yang tidak berhubungan dengan pekerjaan yang dilakukan di beberapa komputer yang seharusnya tidak membutuhkan internet tetapi tetap dapat diakses secara bebas. Jaringan komputer yang digunakan oleh PT. Aruna Sinar Jaya adalah sistem jaringan WAN (Wide Area Network) yang terdiri dari perangkat keras dan perangkat lunak.

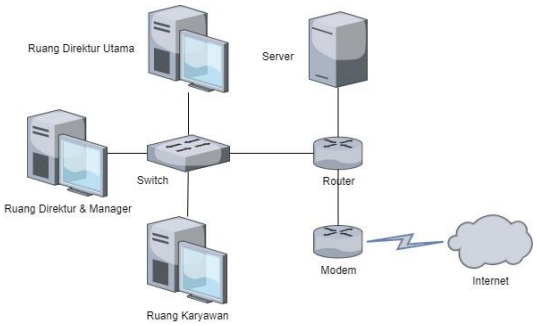
Keamanan jaringan komputer merupakan bagian integral dari perlindungan jaringan komputer, menjaga validitas dan integritas informasi, dan memastikan ketersediaan layanan untuk penggunaannya. Sistem keamanan jaringan komputer harus dilindungi dari setiap serangan atau upaya oleh orang yang tidak berwenang untuk menyusup atau memindai sistem [4]. Berikut adalah topologi, skema dan arsitektur jaringan:



Gambar 2 Topologi jaringan berjalan

Topologi jaringan komputer yang digunakan oleh PT. Aruna Sinar Jaya merupakan topologi *star* yang terdiri dari jaringan komputer yang terdiri dari beberapa komputer, *server*, *switch*, *router*, *printer*, *access point*, dan *modem*.

Setelah penulis melakukan penelitian di PT Aruna Sinar Jaya, penulis dapat mendeskripsikan topologi jaringan komputer di PT Aruna Sinar Jaya. Skema jaringan komputer di PT. Aruna Sinar Jaya, gambar sebagi berikut:



Gambar 3 Skema jaringan berjalan

Keamanan jaringan merupakan aspek penting dalam membangun jaringan internet, karena jaringan internal perusahaan membutuhkan keamanan untuk melindungi data penting, salah satunya memasang *firewall.* PT. Aruna Sinar Jaya masih belum memiliki keamanan lain selain mengandalkan *default firewall* yang menyebabkan jaringan masih rentan dalam menjaga data-data penting perusahaan.

Sistem operasi adalah garis pertahanan pertama melawan perilaku yang tidak diinginkan. Sistem operasi melindungi pengguna dari orang lain dengan memastikan bahwa area penting dari memori atau penyimpanan tidak diganti tanpa izin, melakukan identifikasi dan otentikasi orang dan operasi jarak jauh, dan memastikan distribusi yang adil dari sumber daya perangkat keras penting, karena kebijakan lalu lintas dan komputer yang efektif ini . sistem juga merupakan target serangan yang menarik, karena kompromi yang berhasil dari sistem operasi harganya adalah pemeriksaan penuh mesin dan semua bagiannya [5].

Spesifikasi *Hardware* dan *Software* dalam perangkat keras dan perangkat lunak jaringan membutuhkan perangkat keras untuk mendukung sistem jaringan komputer. Daftar spesifikasi perangkat keras dan perangkat lunak:

Tabel 1 Hardware IP Address

No	Hardware	IP Address	Subnet Mask
1	Client	192.168.2.2/24 – 192.168.2.254/24	255.255.255.0
2	Server	192.168.7.30	255.255.255.0
3	Modem	192.168.1.2	255.255.255.0
4	Router	192.168.2.1	255.255.255.0
5	Printer	192.168.2.20	255.255.255.0

Perangkat lunak yang digunakan meliputi sistem operasi jaringan dan aplikasinya, dalam hal ini penggunaan *Windows Server 2019*. Sistem operasi yang digunakan komputer *client*

berbasis Intel I3 menggunakan *Windows 10 64-bit*. Perangkat pemantauan keamanan menggunakan Winbox untuk sistem jaringan komputer.

Permasalahan yang terjadi di PT. Aruna Sinar Jaya, menurut pengamatan penulis adalah sering terjadinya penurunan kinerja jaringan internet akibat aktivitas yang tidak berhubungan dengan pekerjaan di beberapa komputer yang seharusnya tidak membutuhkan internet dan masih dapat mengaksesnya secara bebas.

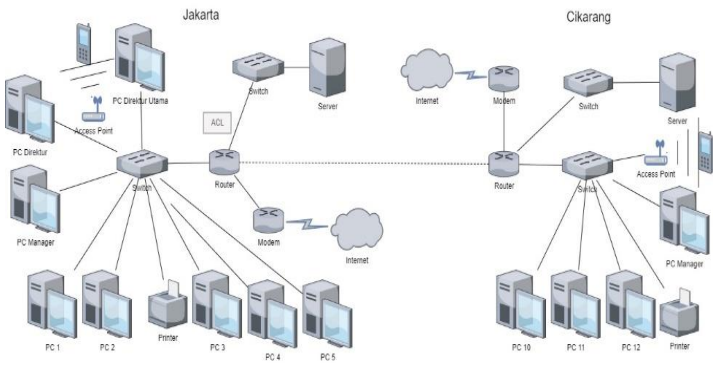
Untuk atasi permasalahan jaringan komputer di PT. Aruna Sinar Jaya, harus menggunakan metode *Access Control List* (ACL) agar meningkatkan kinerja jaringan internet dan membatasi beberapa komputer agar tidak leluasa mengakses internet dan tetap fokus mengerjakan pekerajaanya.

B. Implementasi Efisiensi menggunakan ACL

Access Control List (ACL) adalah aturan yang menentukan objek mana yang memiliki hak akses dan hak akses mana yang ingin mereka miliki. ACL telah menjadi salah satu teknik inspeksi paket yang paling umum. ACL pertama-tama memeriksa isi paket data dan menerapkan aturan untuk menentukan apakah paket tersebut ditolak atau diizinkan. Meskipun beberapa fungsi mungkin menggunakan header paket *TCP/IP* (misalnya *port*, protokol, dll.), pembahasan ini adalah tentang memfilter berdasarkan alamat *IP* sumber atau tujuan [6].

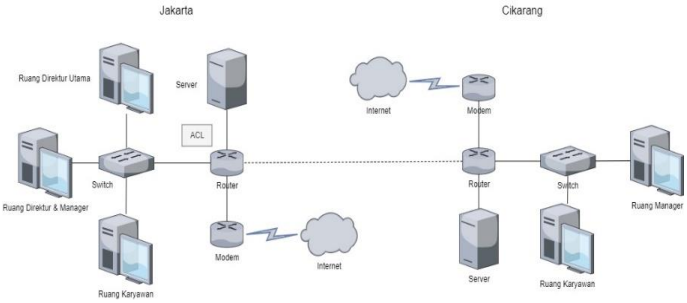
Intranet adalah jaringan komputer di dalam perusahaan yang menggunakan standar komunikasi data seperti internet, artinya pengguna dapat menggunakan semua fasilitas internet untuk keperluan perusahaan, yaitu internet dapat dikatakan berada pada lingkungan bisnis [7]

Setelah penulis melihat jaringan komputer PT, Aruna Sinar Jaya menyarankan untuk menggunakan jaringan keamanan Access Control List (ACL) dengan metode Extended ACL untuk mengontrol akses internet. Ini akan melibatkan implementasi konfigurasi sistem keamanan Access Control List (ACL) dengan router Mikrotik yang sudah ada dan mencegah beberapa komputer klien yang tidak membutuhkan internet di tempat kerja untuk mengakses internet. Berikut adalah topologi dan skema jaringan yang telah disarankan:



Gambar 4 Topologi jaringan disarankan

Dengan mengusulkan topologi jaringan untuk diterapkan di perusahaan, penulis mengembangkan topologi PT. Aruna Sinar Jaya untuk usulan membangun jaringan komputer baru di wilayah dekat pabrik produksi yang berada di Cikarang. Topologi jaringan yang digunakan adalah topologi *star*.



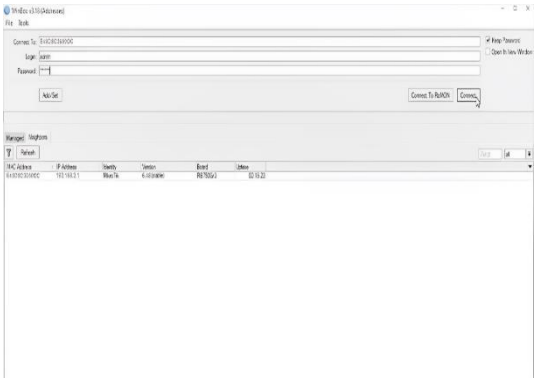
Gambar 5 Skema jaringan disarankan

Pada skema jaringan usulan diatas dapat dilihat bahwa hanya menambahkan *Access Control List* (ACL) pada PT. Aruna Sinar Jaya yang berfungsi untuk mengontrol pengunaan internet agar tidak digunakan secara bebas.

Jaringan komputer adalah sistem operasi yang terdiri dari beberapa komputer dan perangkat jaringan lainnya yang bekerja sama untuk mencapai tujuan bersama. Jaringan komputer adalah koneksi antara dua atau lebih jaringan, yang tujuan utamanya adalah pertukaran informasi. Jaringan komputer dapat saling terhubung menggunakan alat komunikasi yang memungkinkan informasi, data, program, dan perangkat (*printer*, *hard disk*, *webcam*) untuk dibagikan [8].

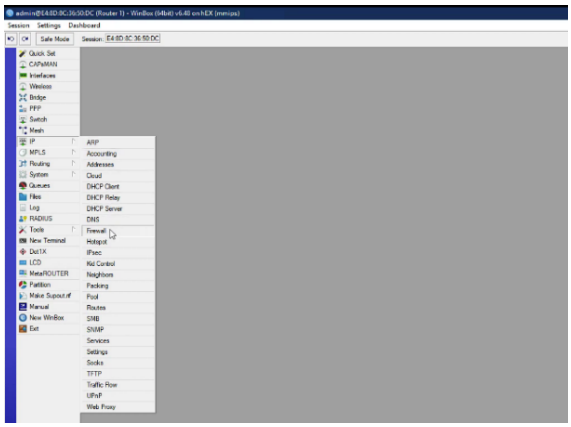
Penulis mengembangkan topologi PT. Aruna Sinar Jaya sebagai rekomendasi untuk topologi jaringan yang akan diterapkan di perusahaan. *Router* adalah perangkat keras yang digunakan untuk menghubungkan beberapa jaringan dengan menggunakan teknologi yang berbeda seperti jaringan dengan jaringan yang sama dan topologi *bus*, *star*, dan *ring*. *Router* dapat mengirimkan data atau informasi dari satu jaringan ke jaringan lainnya [9].

Topologi ini dimaksudkan untuk membangun jaringan komputer baru di daerah dekat pabrik produksi di Cikarang. Topologi bintang digunakan untuk topologi jaringan. Skema jaringan usulan di atas menunjukkan bahwa PT. Aruna Sinar Jaya hanya ditambahkan Access Control List (ACL), yang berfungsi untuk mengontrol akses internet agar tidak digunakan secara bebas. Penulis membuat dan menerapkan jaringan ACL dengan metode yang diperluas untuk mengontrol akses internet sehingga komputer di tempat kerja yang tidak membutuhkan internet tidak dapat mengakses internet secara bebas, berikut adalah perancangan aplikasi dalam WinBox:



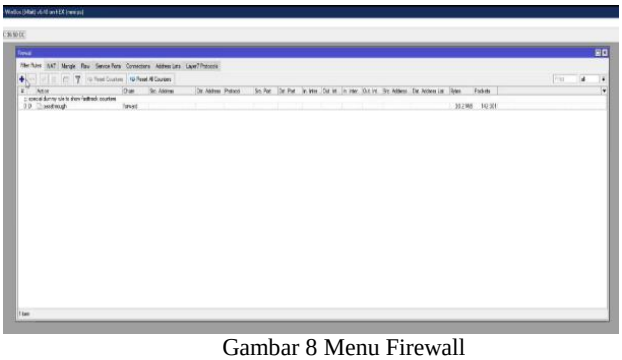
Gambar 6 Login WinBox

WinBox digunakan untuk mengkonfigurasikan IP Address dan memblokir beberapa port yang tidak diperlukan. Masukan login dan Password kemudian tekan tombol Connect untuk masuk ke menu WinBox.



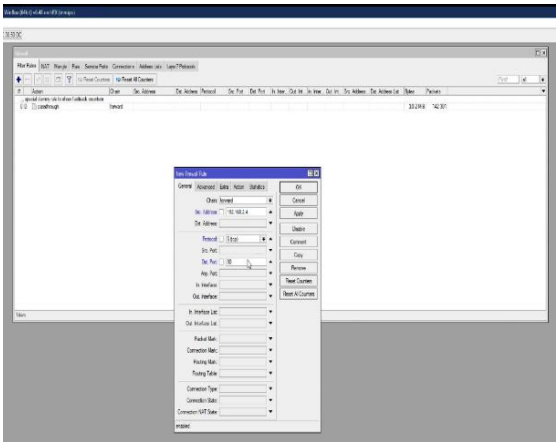
Gambar 7 Menu WinBox

Berikut adalah tampilan WinBox, pilih menu IP dan pilih Firewall.



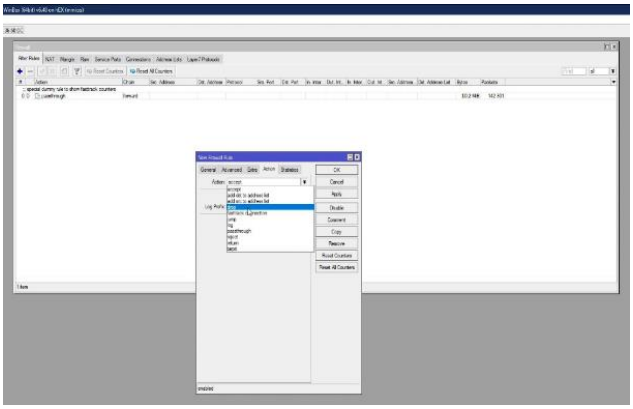
Gambar 8 Menu Firewall

Pada gambar diatas adalah tampilan dari menu Firewall, tekan icon + (Plus) untuk menambahkan Firewal Rule.



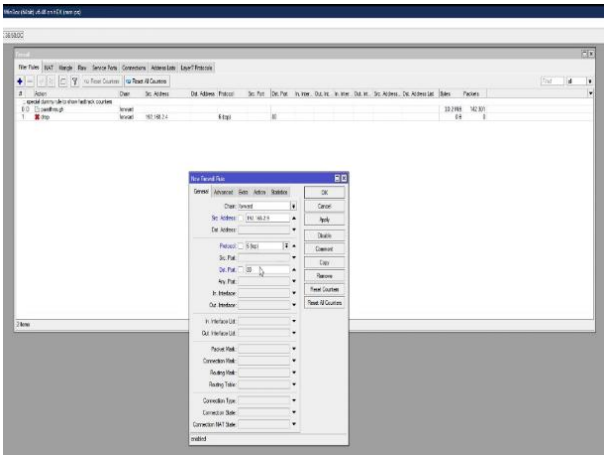
Gambar 9 Menambahkan Firewall Rule

Pada gambar tersebut memunculkan pop up berupa New Firewall Rule, pada tap General dikolom Chain biarkan diisi Forward da kolom Src. Address disi IP yang akan diblokir. Pada kasus ini penulis mengisi Src. Address dengan 192.168.2.4, pada kolom Protokol disikan dengan 6 (tcp) dan pada kolom Dst. Port diisikan 80, port 80 adalah akses untuk HTTP.



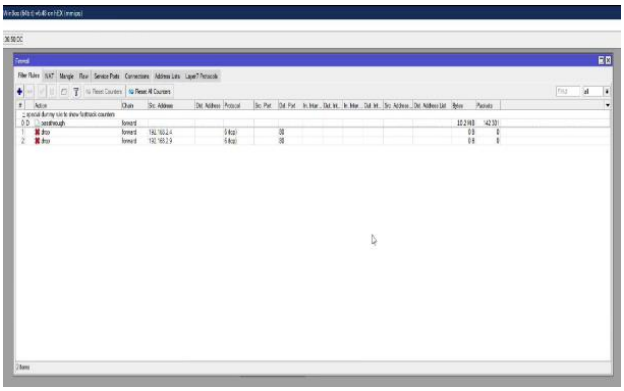
Gambar 10 Mengatur Action

Pindah pada kolom Action, pada kolom Action diganti dari accept menjadi drop untuk mematikan akses ke port yang dituju, dan pada Log di ceklis, kemudian tekan tombol Apply dan OK.



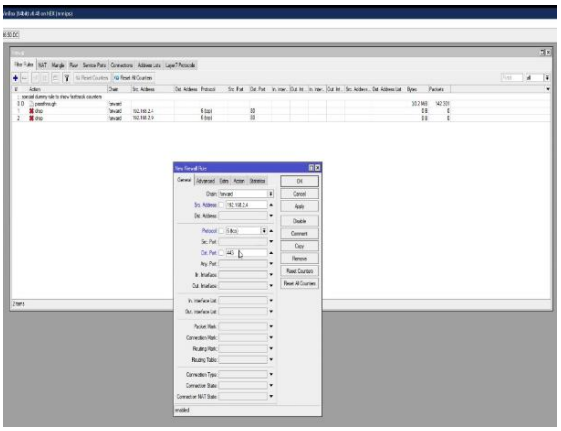
Gambar 11 Menambahkan Firewall Rule lainnya

Tambahkan 1 lagi IP Address sebagai bahan pengujian lainnya, penulis mengambil IP Address 192.168.2.9 dengan pengaturan yang sama dengan 192.168.2.4.



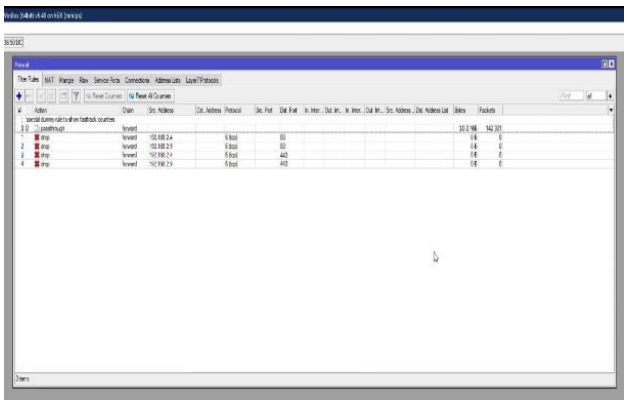
Gambar 12 Menambahkan IP Address Block Port 80

Pengaturan yang digunakan pada IP Address 192.168.2.9 sama dengan IP Address 192.168.2.4 pada tab General dan Action.



Gambar 13 Menambahkan IP Address Block Port 443

Pada gambar diatas, penulis menambahkan Firewall Rule dengan IP Address 192.168.2.4 dan 192.168.2.9, Protocol diisi dengan 6 (tcp) dan Dst. Port diisikan dengan 443. Port 443 adalah akses untuk HTTPS.



Gambar 14 Mengatur IP Address Block Port 80 dan 443

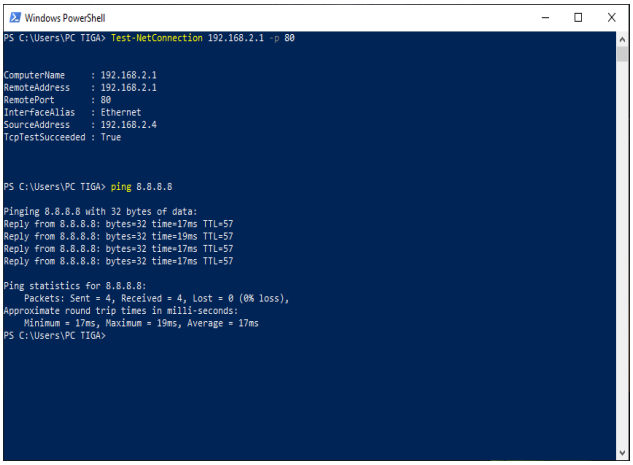
Gambar diatas menunjukan 2 IP Address, yaitu 192.168.2.4 dan 192.168.2.9 Port yang akan di blokir adalah 80 dan 443.

C. Pengujian Efisiensi Jaringan

Pengujian dibagi menjadi dua, awal dan akhir. Pengujian awal belum melibatkan implementasi ACL dan pengujian akhir sudah belum melibatkan implementasi ACL, lalu diujikan pada PC TIGA dan PC EMPAT. Beberapa tes melibatkan ping dari client ke router dengan port 80 dan 443, ping DNS 8.8.8.8 untuk mengecek koneksi jaringan internet, dan melacak trafik jaringan internet dengan alat Torch Mikrotik.

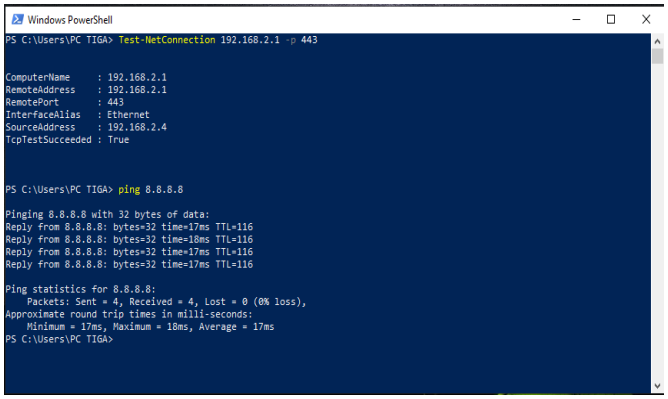
1) Pengujian Awal

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



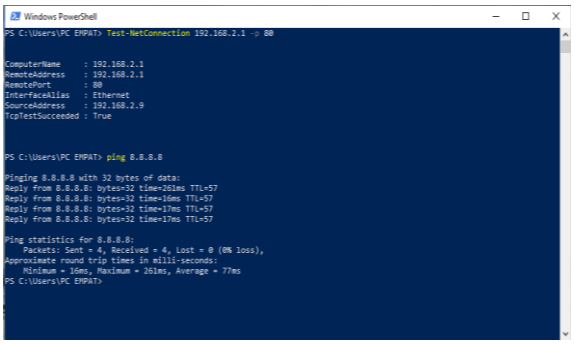
Gambar 15 Pengujian awal pada PC TIGA port 80

Pengujian awal dengan PC TIGA port 80 untuk melihat apakah PC TIGA masih ada akses internet atau tidak dan hasilnya adalah terdapat akses internet.



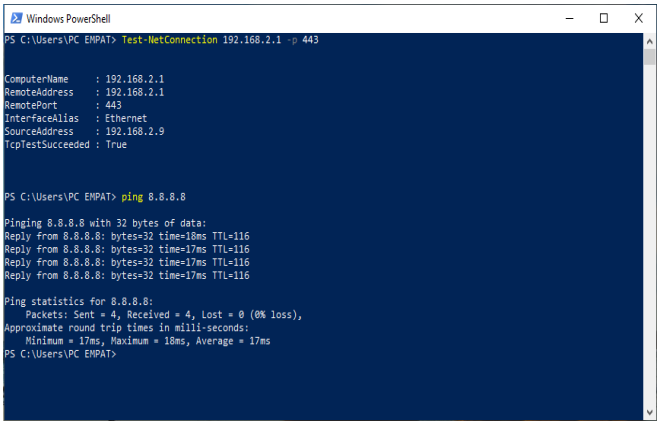
Gambar 16 Pengujian awal pada PC TIGA port 443

Pengujian awal dengan PC TIGA port 443 untuk melihat apakah PC TIGA masih ada akses internet atau tidak dan hasilnya adalah terdapat akses internet.



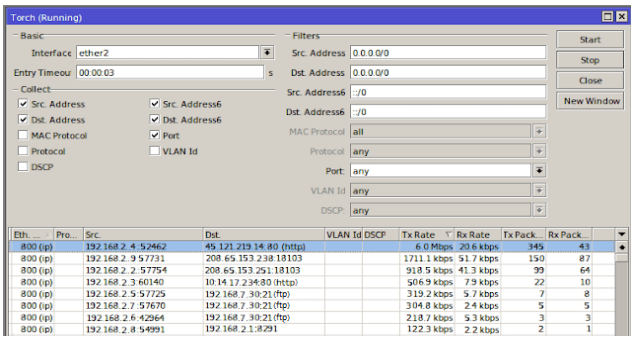
Gambar 17 Pengujian awal pada PC EMPAT port 80

Pengujian awal dengan PC EMPAT port 80 untuk melihat apakah PC EMPAT masih ada akses internet atau tidak dan hasilnya adalah terdapat akses internet.



Gambar 18 Pengujian awal pada PC EMPAT port 443

Pengujian awal dengan PC EMPAT port 443 untuk melihat apakah PC EMPAT masih ada akses internet atau tidak dan hasilnya adalah terdapat akses internet.

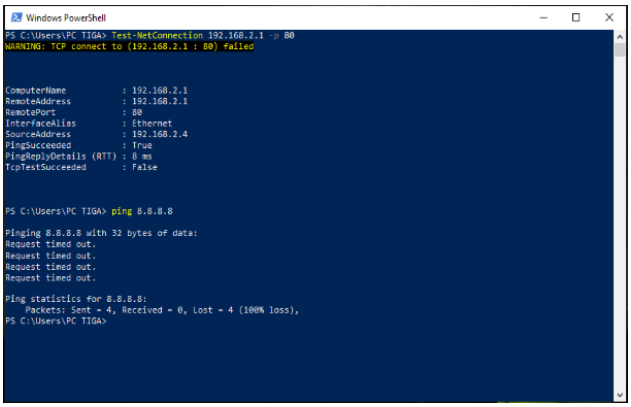


Gambar 19 Torch Mikrotik sebelum implementasi ACL

Dilihat dari alat Torch Mikrotik bahwa terdapat akses internet ke port 80 dan 443 karena belum dilakukan implementasi ACL.

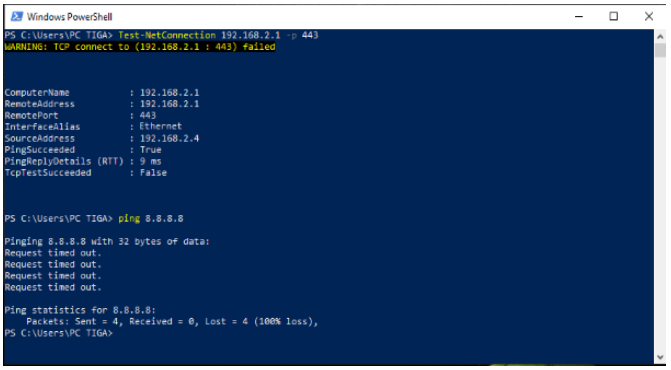
2) Pengujian Akhir

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



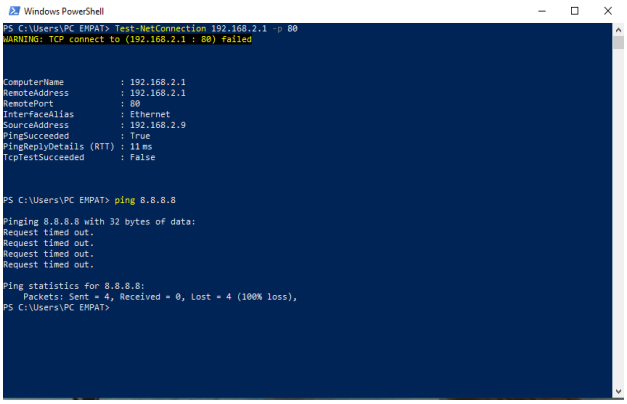
Gambar 20 Pengujian akhir pada PC TIGA port 80

Pengujian awal dengan PC TIGA port 443 untuk melihat apakah PC TIGA masih ada akses internet atau tidak dan hasilnya adalah tidak terdapat akses internet.



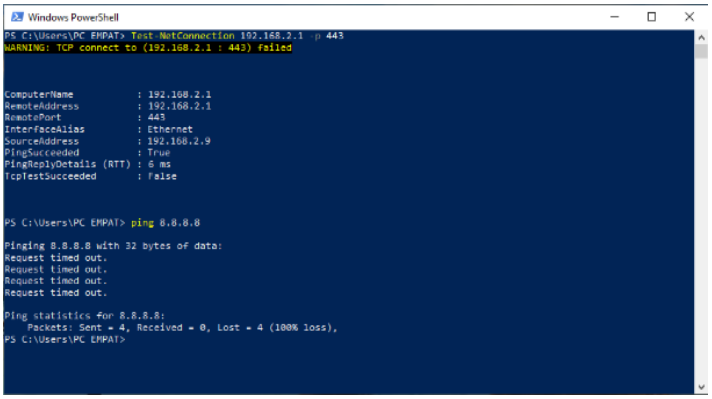
Gambar 21 Pengujian akhir pada PC TIGA port 443

Pengujian awal dengan PC TIGA port 443 untuk melihat apakah PC TIGA masih ada akses internet atau tidak dan hasilnya adalah tidak terdapat akses internet.



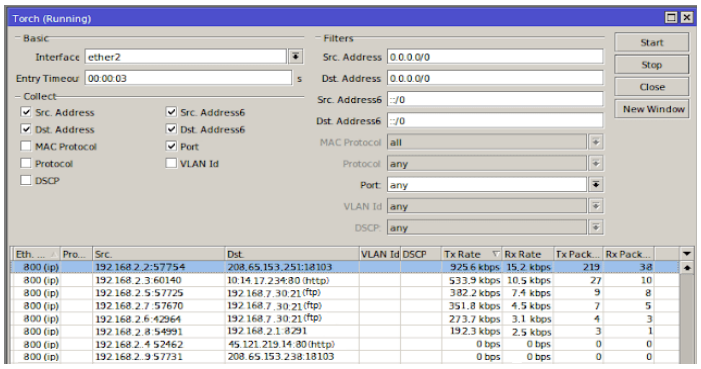
Gambar 22 Pengujian akhir pada PC EMPAT port 80

Pengujian awal dengan PC EMPAT port 80 untuk melihat apakah PC EMPAT masih ada akses internet atau tidak dan hasilnya adalah tidak terdapat akses internet.



Gambar 23 Pengujian akhir pada PC EMPAT port 443

Pengujian awal dengan PC EMPAT port 443 untuk melihat apakah PC EMPAT masih ada akses internet atau tidak dan hasilnya adalah tidak terdapat akses internet.



Gambar 24 Torch Mikrotik sesudah implementasi ACL

Tes monitoring *traffic* jaringan internet setelah implementasi ACL menggunakan *tool Torch* Mikrotik. Pada tampilan ini PC Tiga dan PC Empat tidak bisa lagi mengakses internet dikarenakan telah diblokir dari Port 80 dan 443.

IV. Kesimpulan

Dapat disimpulkan dari implementasi yang dilakukan di PT. Aruna Sinar Jaya adalah sebagai berikut:

1. Pembentukan Access Control List (ACL) sebagai sistem keamanan jaringan pada router di PT. Aruna Sinar Jaya memungkinkan penggunaan internet yang lebih sehat dan efisien.
2. Penerapan sistem ACL yang diperluas di dalam router memungkinkan beberapa komputer yang dimaksudkan tidak dapat mengakses internet.

V. Daftar Pustaka

[1] A. Muzakir dan M. Ulfa, "Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan," *Simetris J. Tek. Mesin Elektro Dan Ilmu Komput.*, vol. 10, no. 1, hlm. 15–20, Apr 2019, doi: 10.24176/simet.v10i1.2646.

[2] B. K. Sihotang, S. Sumarno, dan B. E. Damanik, "Implementasi Access Control List Pada Mikrotik dalam Mengamankan Koneksi Internet Koperasi Sumber Dana Mutiara," *JURIKOM J. Ris. Komput.*, vol. 7, no. 2, hlm. 229, Apr 2020, doi: 10.30865/jurikom.v7i2.2010.

[3] W. W. Purba dan R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *AITI*, vol. 17, no. 2, hlm. 143–158, Feb 2021, doi: 10.24246/aiti.v17i2.143-158.

[4] N. Hayaty, *Buku Ajar: Sistem Keamanan*. Tanjungpinang, 2020.

[5] A. Wibowo, *Keamanan Sistem Jaringan Komputer*. Semarang: Yayasan Prima Agus Teknik, 2021.

[6] F. Azmi, T. U. Kalsum, dan H. Alamsyah, "Analysis and Application of Access Control List (ACL) Methods on Computer Networks," *J. Komput. Inf. Dan Teknol. JKOMITEK*, vol. 2, no. 1, Jun 2022, doi: 10.53697/jkomitek.v2i1.642.

[7] A. Susanto dan L. J. Sitohang, "Analisis Keefektifan Jaringan Intranet Di Pt Pln (Persero) Ulpltu Tanjung Balai Karimun," *J. TIKAR*, vol. 3, no. 1, 2022.

[8] A. V. Mananggel, A. Mewengkang, dan A. C. Djamen, "Perancangan Jaringan Komputer Di Smk Menggunakan Cisco Packet Tracer," *Edutik J. Pendidik. Teknol. Inf. Dan Komun.*, vol. 1, no. 2, hlm. 119–131, Des 2021, doi: 10.53682/edutik.v1i2.1124.

[9] T. A. Mustofa, E. Sutanta, dan J. Triyono, "Perancangan Dan Implementasi Sistem Monitoring Jaringan Wi-Fi Menggunakan Mikhmon Online Di Wisma Muslim Klitren Gondokusuman Yogyakarta," vol. 7, no. 2, 2019.

[10]. Tittel, Ed. 2002. Schaum's Outline : Computer Networking (Jaringan Komputer). Jakarta : Penerbit Erlangga

[11]. Santos, Omar dan Stuppi, John. 2015. CCNA Security 210-260 Official Cert Guide. Cisco Press : IndianapolisUSA.

[12]. Iwan Kurnia.2007. Analisis Penggunaan Komputer Local Area Network. http://elib.unikom.ac.id 2007-08-20. Akses (11 Agustus 2014).

[13]. Perancangan keamanan jaringan komputer dengan menggunakan metode acl pada pt.tunas artha gardatama. Konferensi Nasional Ilmu Sosial & Teknologi (KNiST) Maret 2016, pp. 289 – 296.

[14]. Konfigurasi keamanan jaringan komputer Pada router dengan metode acl's. Rahmawati, ISSN 2442-2436. KONFIGURASI KEAMANAN JARINGAN VOL. 1 NO. 2. Jurnal Teknik Komputer AMIK BSI

[15]. Muhammad Ariq Istiqlal*, Linna Oktaviana Sari**, Irsan Taufik Ali**. Perancangan Sistem Keamanan Jaringan TCP/IP Berbasis Virtual LAN dan Access Control List. Jom FTEKNIK Volume 3 No. 1 Februari 2016