Jurnal Teknologi Terpadu

https://journal.nurulfikri.ac.id/index.php/JTT
ISSN : 2477-0043 ISSN ONLINE : 2460-7908

PENERAPAN LIMIT AKSES *BROWSING* INTERNET PADA SAAT JAM KERJA DI PT XYZ

Zaenal Mutaqin Subekti[1], Kikim Mukiman[2], Ahmad Fikri Adluwal Fadil[3], Muhammad Asyrofi[4]

[1, 4]Teknik Komputer, Sekolah Tinggi Manajemen In*for*matika dan Komputer Bani Saleh
[2]Sistem Informasi, Sekolah Tinggi Manajemen In*for*matika dan Komputer Bani Saleh
[3]Teknik Informatika, Sekolah Tinggi Manajemen In*for*matika dan Komputer Bani Saleh
Jl. M Hasibuan No 68, Bekasi, Indonesia 17113
zms.stmikbanisaleh@gmail.com, kikimmukiman@gmail.com, ahmad.fikrinew2801@gmail.com, asyrofimail@gmail.com

Abstract

One of the engineering companies located in the Cikarang area has a rule that every employee is not allowed to access the internet through a browser during working hours, i.e., from 08.00 AM to 12.00 AM and 1.00 to 5.00 PM, only during break time which is between 12.00 AM until 1.00 PM, employees are allowed to access the internet through a browser. The company can apply this rule by implementing its policies on router firewalls to be followed by all employees thoroughly. This research will analyze and implement the process of configuring the router firewalls for the applied case. The first stage of this research starts from analyzing the software and hardware requirements, analyzing the network topology designs, implement the company's policies on firewall configuration, and the last stage is by doing the testing. From this implementation, we get the results that all users cannot access the internet through a browser except for authorized users. These results are applied based on the company's rules and policies proposed above that employees only able to access the internet through a browser during break time and before and after working hours.

Keywords: *access limit, browser, working hours, firewall, internet*

Abstrak

Salah satu perusahaan *engineering* yang terletak di kawasan Cikarang, mempunyai aturan bahwa setiap karyawan tidak boleh akses internet melalui *browser* pada jam kerja, yaitu jam 08.00 pagi sampai jam 12.00 dan jam 13.00 sampai jam 17.00 pada saat jam istirahat yaitu jam 12.00 – 13.00 karyawan dapat mengakses internet melalui *browser*, dengan menerapkan kebijakan perusahaan untuk diimplementasikan pada *firewall router*, sehingga kebijakan perusahaan tersebut dapat diikuti oleh semua karyawan dengan baik. Tahapan penelitian dimulai dari Analisa untuk menganalisa kebutuhan *software* dan *hardware*, kedua desain topologi jaringan, ketiga implementasi kebijakan melalui konfigurasi yang diterapkan pada *firewall*, keempat melakukan *testing*. Hasil *testing* yaitu semua pengguna tidak dapat melakukan akses internet melalui *browser* pada jam kerja pagi yaitu jam 08.00 sampai jam12.00 dan jam kerja siang jam 13.00 sampai jam 17.00, kecuali bagi *user* yang dibolehkan, dan semua pengguna dapat mengakses internet, sebelum jam kerja pagi, istirahat makan siang yaitu jam 12.00 sampai jam 13.00 dan setelah jam 17.00 yaitu setelah jam kerja pulang.

Kata kunci: limit akses, *browser*, jam kerja, *firewall*, internet

1. PENDAHULUAN

Berkembangnya teknologi semakin hari semakin cepat, kebutuhan infrastruktur jaringan dibutuhkan dalam menunjang pekerjaan pada salah satu perusahaan *engineering* di kawasan *Hyundai* Cikarang, seperti untuk akses data ke *server* lokal, menyimpan data pekerjaan pada *server* lokal seperti *drawing engineering* dan administrasi perkantoran menggunakan aplikasi *Office Word* atau *Excell*, serta *input* data pada sistem gudang. *Sharing* [1] data komputer [2], akses *sharing* printer, akses ke sistem gudang untuk *input* barang masuk dan barang keluar, akses ke sistem produksi lokal, dan penggunaan *email* [3] *client* berbasis *desktop* seperti *Ms. Outlook*.

Perusahaan mempunyai aturan bahwa setiap karyawan tidak boleh akses *browsing* internet pada jam kerja yaitu jam 08.00 pagi sampai jam 12.00 dan jam 13.00 sampai jam 17.00 kecuali bagi karyawan yang diperbolehkan. Aturan perusahaan juga mewajibkan karyawan menggunakan *email*

Diterima 07 Juni 2021, Direvisi 01 Juli 2021, Diterima untuk publikasi 13 Juli 2021

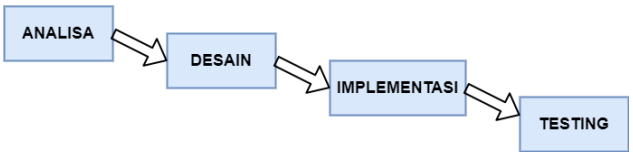
berbasis *desktop* untuk berkomunikasi dengan *supplier* dan *client* perusahaan untuk keperluan pekerjaan.

Untuk mengatasi beberapa permasalahan tersebut dengan menerapkan layanan *Quality Of Service* (QoS) [4], menerapkan limit akses *browsing* berupa *filter* [5] pada *firewall* untuk *drop* komunikasi dari *inbond* ke *outbond* pada port 80 dan 443, kecuali *user* yang mendapatkan akses *browsing* internet.

Penelitian terdahulu perancangan pembangunan *firewall* dan *proxy server* untuk membatasi hak akses internet dengan menggunakan *proxy squid* yang terinstall pada Linux Ubuntu 16.10 dengan melakukan *Access Control List* dapat *filter* IP *address* yang boleh akses internet dan memblokir situs-situs tertentu [6]. Implementasi *Access Control List* menggunakan *mikrotik* pada SMK Budi Mulia Tanggerang, dengan menerapkan *Access Control List* dapat membatasi akses media sosial dan *streaming video* pada saat jam pelajaran [7], pemanfaatan pada *web proxy* untuk pengoptimalkan keamanan jaringan *wireless*, dengan menggunakan *web proxy* pada *router mikrotik* pada *hotspot* untuk membatasi akses media sosial dan *streaming* pada saat jam kerja [8], limitasi pengguna akses internet berdasarkan kuota waktu dan data menggunakan PC *router* sistem operasi *mikrotik* dengan mengatur pembagian *bandwidth* pada setiap pengguna dan pembatasan *download* maupun *upload* [9], implementasi *Mikrotik Router Board* 750 sebagai *firewall* blok situs pada jaringan LAN untuk melakukan *filter* terhadap situs-situs *web* yang berkonten *negative* hasilnya web yang telah diblokir tidak dapat dibuka oleh pengguna [10]. Tujuan dari penelitian ini adalah pengguna yang masuk pada *list* IP *address* blok *browsing* tidak dapat akses *browsing* internet pada saat jam kerja dan pengguna yang masuk *list* IP *address allow browsing* dapat akses *browsing* internet pada saat jam kerja.

2. METODE PENELITIAN

Tahapan pada penelitian ini ada empat tahapan, pertama di awali dengan melakukan analisa kebutuhan. Kedua dengan melakukan *design*, yaitu merancang topologi jaringan. Selanjutnya pada tahap ketiga, implementasi menerapkan konfigurasi pada *device* seperti *router*. Dan tahapan yang terakhir yaitu *testing*, melakukan uji coba dari hasil implementasi dan menghasilkan data-data yang dapat digunakan sebagai acuan untuk mendapatkan kesimpulan.



Gambar 1. Tahapan Penelitian

2.1 Analisa

Tahapan pertama melakukan analisa. Langkah awal dengan melakukan analisa untuk kebutuhan baik perangkat keras atau perangkat lunak yang akan digunakan pada penelitian ini, kebutuhan perangkat keras meliputi:

Tabel 1. Kebutuhan Perangkat Keras

Nama Perangkat	Fungsi
Router	Untuk menerapkan konfigurasi IP *address* pada internet dan *local area network* (LAN), *network address* translation, memisahkan penggunaan *bandwidth* internet dan lokal, melakukan *filter* IP *address* yang tidak boleh akses ke internet dan yang dibolehkan serta menambahkan waktu pada *user* yang tidak boleh akses internet/*browsing*.
Switch	Perangkat *intermediary* yang digunakan untuk menghubungkan dari PC pengguna ke PC pengguna yang lain atau ke perangkat *router*.
Kabel UTP	Merupakan media atau penghubung dari pengakat komputer ke *switch* atau ke *router*, media yang digunakan menggunakan tembaga yang balut pada kabel *unshield twisted pair* (UTP)
PC	Perangkat yang digunakan pengguna dalam melakukan pekerjaan baik *drawing*, administrasi dengan aplikasi *office*, *input* data ke sistem aplikasi, kirim dan terima *email*.
Server	Sebuah perangkat yang digunakan untuk menyimpan data terpusat dari pengguna.

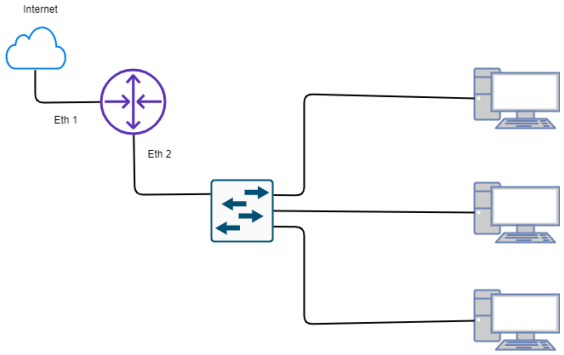
Selanjutnya kebutuhan perangkat lunak, meliputi:

Tabel 2. Kebutuhan Perangkat Lunak

Nama Perangkat	Fungsi
Winbox	Sebuah aplikasi yang digunakan untuk melakukan konfigurasi pada *mikrotik* melalui *Grafik User Browsing* (GUI).

2.2 Desain

Tahapan kedua yaitu desain, pada tahap ini desain topologi jaringan dirancang sesuai dengan kebutuhan dan tata letak pengguna, sehingga topologi jaringan dapat memudahkan dalam menggambarkan dan persiapan untuk mengkonfigurasi *router* sesuai dengan kebutuhan.



Gambar 2. Topologi Jaringan

2.3 Implementasi

Tahapan ketiga di tahapan penelitian ini adalah implementasi, melakukan konfigurasi atau *setting* pada *device router* sesuai dengan kebutuhan, berikut beberapa langkah implementasinya :

- Konfigurasi IP *address* internet dan *local area network*
- Konfigurasi *Network Address Translation* (NAT)
- Konfigurasi DHCP *server* untuk LAN
- Konfigurasi *filter* pada *firewall* untuk IP *address* yang tidak bisa *browsing*.

2.4 *Testing*

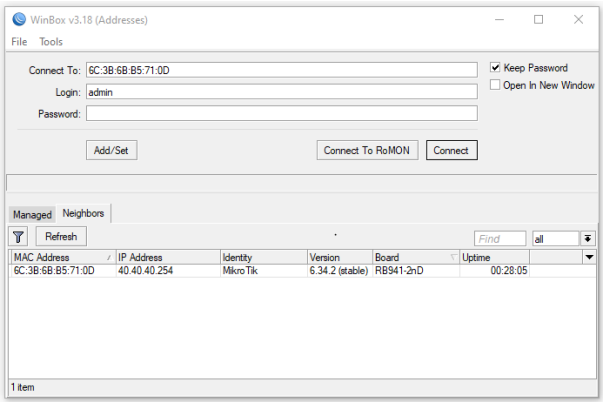
Tahapan keempat yaitu *testing* atau pengujian merupakan tahapan untuk melakukan pengujian, setelah melaksanakan analisa, desain, dan implementasi penerapan konfigurasi, serta pengujian akan dilakukan *testing bandwidth* internet dan *bandwidth* lokal, pengujian akses *browsing* pada saat jam kerja dan di luar jam kerja.

3. HASIL DAN PEMBAHASAN

Pembahasan dimulai dengan menerapkan konfigurasi pada router sesuai dengan topologi.

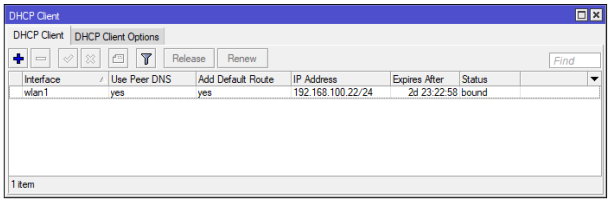
3.1 Konfigurasi *Router*

Akses *router mikrotik* dengan menggunakan *Winbox* untuk memudahkan konfigurasi berbasis *grafik user browsing* atau *console* teks.



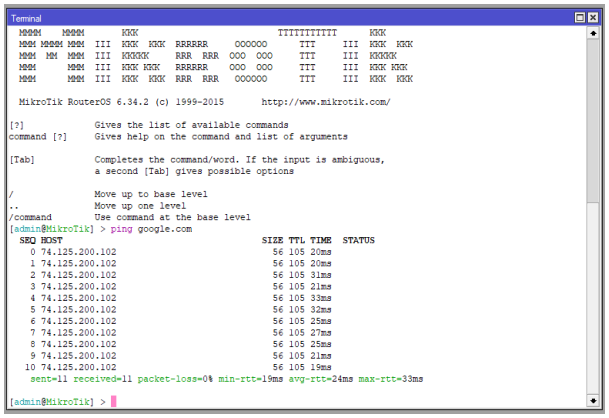
Gambar 3. *Winbox*

Konfigurasi IP *address* pada *browsing* ether1 untuk mendapatkan internet dengan menggunakan layanan DHCP *client*.



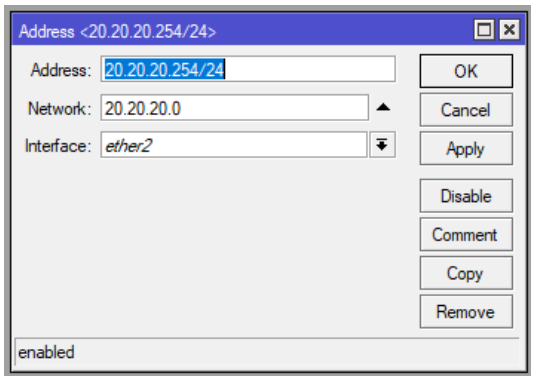
Gambar 4. *DHCP Client*

Pada DHCP *client* di tab status mendapatkan status *bound* menjelaskan bahwa IP *address* dari internet sudah di dapatkan, selanjutnya, dapat di lakukan *testing* apakah internet sudah mengalir ke *router* atau belum. Lakukan dengan klik tab *new terminal* dan *ping* ke *google.com*



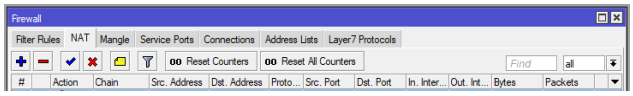
Gambar 5. Pengujian Akses Internet pada *Router*

Setelah *testing* berhasil dilajutkan dengan konfigurasi IP *address* untuk *Local Area Network*. Klik pada tab IP dan sub tab *address*, kemudian klik tanda *plus* dan isi alamat *network* dan *browsing* dan klik OK.



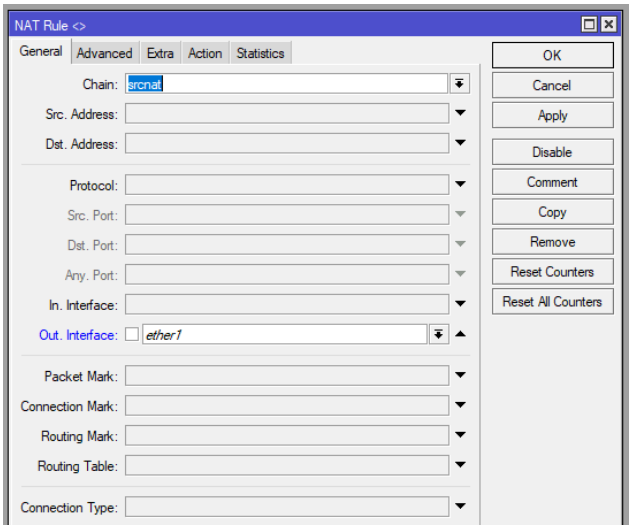
Gambar 6. Pengisian IP *Address*

Selanjutnya konfigurasi *Network Address Translation* (NAT) klik pada tab IP dan pilih *firewall*.



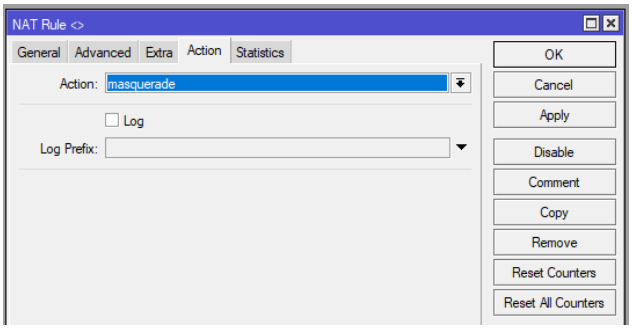
Gambar 7. *Firewall*

Klik pada tab NAT dan untuk menambah konfigurasi pilih tanda plus, sehingga muncul *pop up form new* NAT *rule*, pada *chain* isi dengan *srcnat* dan *out browsing* diisi dengan ether1.



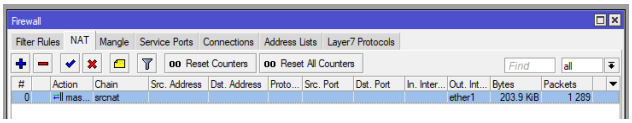
Gambar 8. NAT *Rule*

Pilih tab *action* dan pada *action* pilih masquerade dan klik OK.



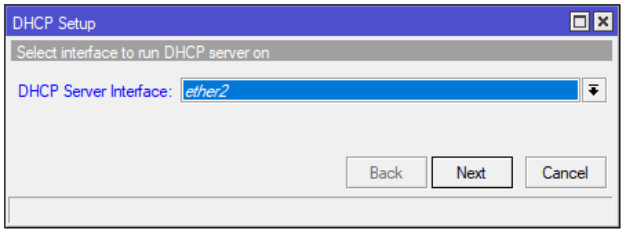
Gambar 9. *Action Masquerade*

Sehingga menghasilkan baris *firewall* dengan nomor 0 yang menandakan bahwa baris ini memmpunyai priorotas yang utama.



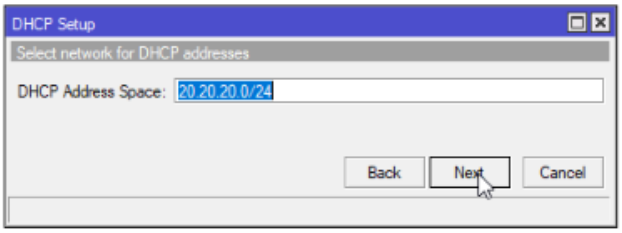
Gambar 10. *Firewall* NAT

Konfigurasi selanjutnya *setup* DHCP (*Dynamic Host Configuration Protocol*) *server* untuk mensuplay IP *address* secara otomatis pada ether2 yang terhubung ke LAN. Klik IP dan pilih DHCP *server* kemudian klik DHCP *setup*. Selanjutnya pada DHCP *setup* pilih *browsing* yang akan di konfigurasi DHCP *server*, di sini pilih ether2.



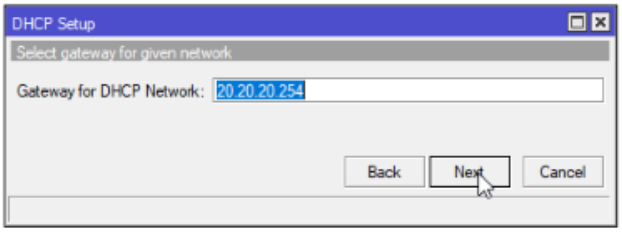
Gambar 11. DHCP *Setup*

Selanjutnya DHCP *address space* diisi dengan 20.20.20.0/24.



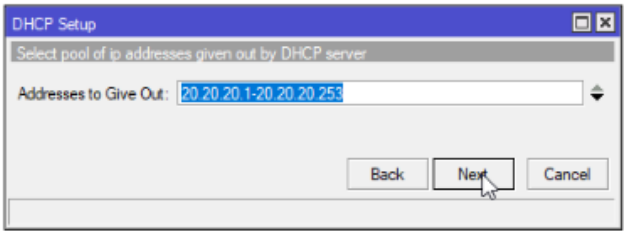
Gambar 12. DHCP *Address Space*

Setelah *next*, pengisian IP *gateway* untuk DHCP *network* diisi dengan = 20.20.20.254.



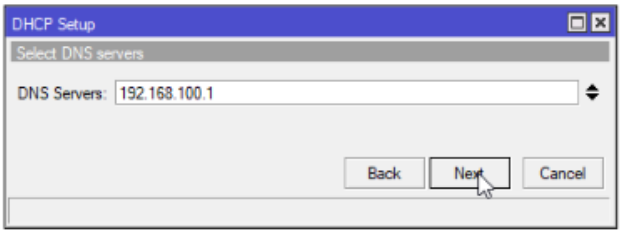
Gambar 13. *Gateway for* DHCP *Network*

Klik *next*, *form* pengisian selanjutnya mengenai alamat IP *address* yang akan diisi secara otomatis pada DHCP *server*, dan setelah diisi klik *Next.*



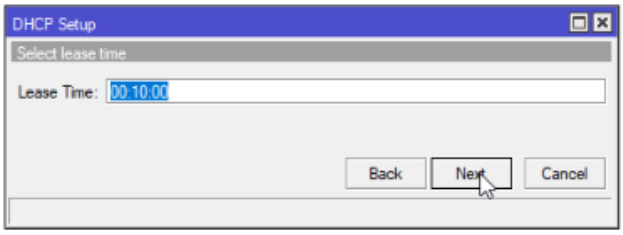
Gambar 14. *Address to Give Out*

Selanjutnya pengisian pada *setup* DHCP *server* untuk DNS *server* dan klik *Next.*



Gambar 15. DNS *Server*

Yang terakhir pengisian *lease time.*



Gambar 16. *Lease Time*

Setelah selesai akan muncul *pop up setup has completed successfully*, menandakan bahwa *setup* DHCP *server* telah selesai.

Berikut *list* IP *address* yang dibolehkan untuk akses *browsing* internet.

Tabel 3. *List IP Address Allow Browsing*

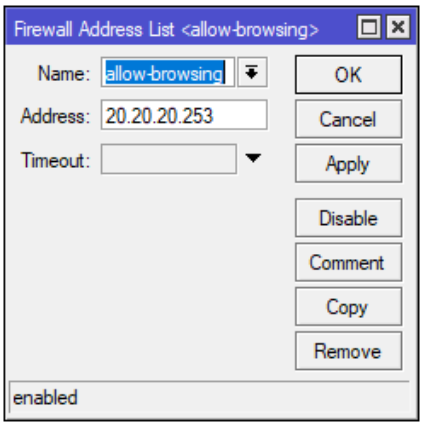
No	Ip *Address*	Nama Bagian
1	20.20.20.253	Direktur
2	20.20.20.252	Manager *Marketing*
3	20.20.20.251	Manager Produksi
4	20.20.20.250	Manager *Engineering*
5	20.20.20.249	Spv *Accounting*
6	20.20.20.248	Spv *Engineering*
7	20.20.20.247	Spv Produksi
8	20.20.20.246	Staff *Marketing*
9	20.20.20.245	Staff *Purchasing*
10	20.20.20.244	Staff HRD

Tabel 4. *List IP Address Block Browsing*

No	Ip *Address*	Nama Bagian
1	20.20.20.243	Staff Produksi
2	20.20.20.242	Staff Produksi
3	20.20.20.241	Staff *Engineering*
4	20.20.20.240	Staff *Engineering*
5	20.20.20.239	Staff *Accounting*
6	20.20.20.238	Staff *Accounting*
7	20.20.20.237	Sstaff administrasi
8	20.20.20.236	Staff Gudang

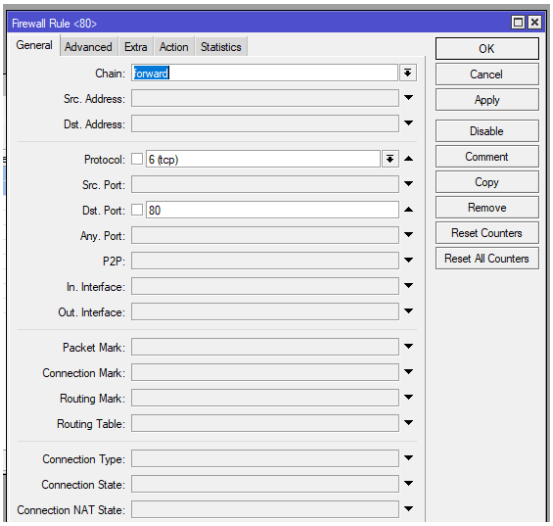
Tahap selanjutnya konfigurasi *filter firewall* untuk menerapkan kebijakan bahwa karyawan tidak boleh akses internet melalui *browser* pada jam kerja mulai jam 08.00 – 12.00 dan jam 13.00 – 17.00.

Klik pada tab IP dan pilih *firewall* nanti akan muncul *form firewall*. Pada tab *address list* dan klik tanda *plus* untuk menambahkan *list* baru. Pada *address list* akan digunakan untuk mendaftarkan IP *address* yang boleh mengakses internet via *browsing*. Pada *name*, isi dengan *allow-browsing*. Dan pada *address*, isi dengan IP *address* yang boleh akses internet contoh di sini 20.20.20.253 dan klik OK.



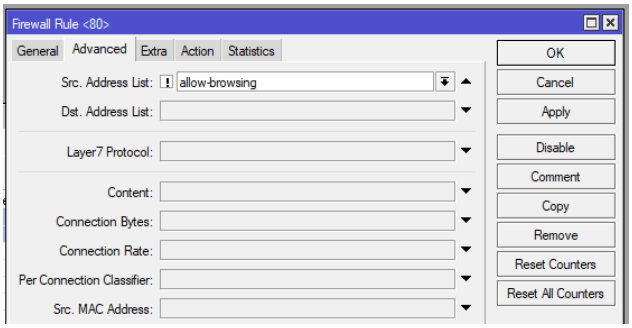
Gambar 17. *Firewall Address List*

Pada tab *filter rule*s klik icon tanda *plus* untuk menambahkan *rule firewall* baru. Setelah muncul *form firewall rule* pada tab *general chain* pilih *for*ward, dan *protocol* pilih 6(tcp) serta pada *destination* port ketik 80 *rule* ini akan mengeblok jika pengguna akan mengakses internet via *browser* dan yang diakses menggunakan HTTP.



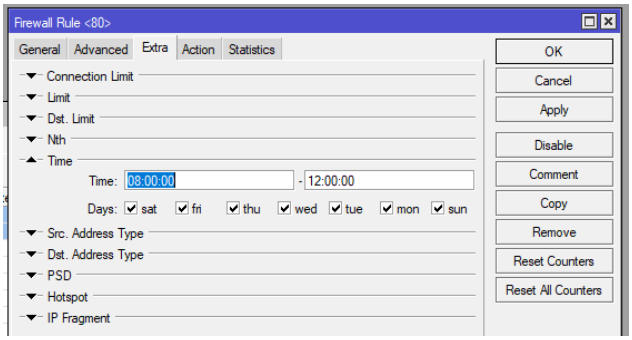
Gambar 18. *Tab General Firewall Rule*

Pada tab *advanced* pada *source address list*, klik tanda seru pada kolom dan pilih *allow-browsing*. *Rule* ini akan memberikan IP *address* yang termasuk pada *allow blocking* dapat diperbolehkan akses *browsing* internet.



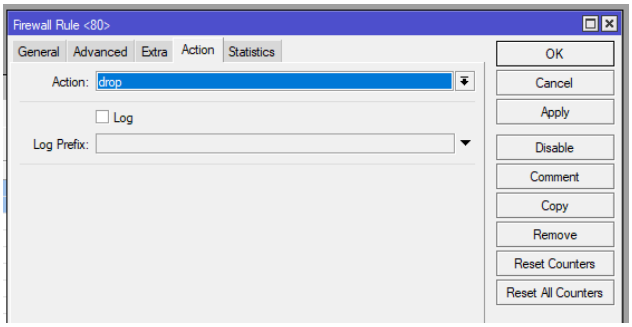
Gambar 19. *Tab Advanced Firewall Rule*

Pada tab *extra*, *time* diisi dengan waktu bloking *browsing* akses intenet, pada *rule* ini mengakibatkan pada jam 08.00 – 12.00 akan diblok untuk *browsing* akses internet.



Gambar 20. Tab *Extra Firewall Rule*

Pada tab *action*, pilih *drop* untuk mengeblok jika ada *user* akan mengakses ke HTTP atau port 80 kecuali jika IP *address* yang masuk ke dalam *allow browser*.



Gambar 20. Tab *Action Firewall Rule*

Lakukan setting *filter firewall* seperti Langkah-langkah diatas lagi dengan *destination* port 443 atau HTTPS, dan *extra* jam 08.00 – 12.00 sehingga dapat mengblok pengguna yang akan mengakses https pada waktu jam 08.00 – 12.00 kecuali IP *address* yang di *allow browsing*.

Kemudian lakukan setting *filter firewall* seperti langkah-langkah seperti di atas dengan *destination port* 80 atau HTTP dengan *extra time* 13.00 – 17.00 sehingga dapat melakukan blok pengguna yang akan mengakses HTTP pada waktu, jam 13.00 – 17.00 kecuali IP *address* yang dibolehkan akses *browsing*.

Selanjutnya lakukan *setting filter firewall* seperti langkah-langkah *filter rule* seperti di atas dengan *destination port* 443 dan *extra time* jam 13.00 – 17.00. Sehingga, jika ada pengguna mengakses HTTPS pada jam 13.00 – 17.00 dapat diblok akses internet kecuali IP *address* yang dibolehkan akses internet.

3.2 Pengujian

Pada pengujian dilakukan sebelum menerapkan konfigurasi blok akses *browsing* internet, dan sesudah menerapkan, berikut hasil pengujian sebelum menerapkan blok akses *browsing* internet.

Tabel 5. Hasil Pengujian sebelum menerapkan *Block Browsing*.

No	IP *Address*	Nama Bagian	Akses *Browsing* Internet
1	20.20.20.253	Direktur	Berhasil
2	20.20.20.252	Manager *Marketing*	Berhasil
3	20.20.20.251	Manager Produksi	Berhasil
4	20.20.20.250	Manager *Engineering*	Berhasil
5	20.20.20.249	Spv *Accounting*	Berhasil
6	20.20.20.248	Spv *Engineering*	Berhasil
7	20.20.20.247	Spv Produksi	Berhasil
8	20.20.20.246	Staff *Marketing*	Berhasil
9	20.20.20.245	Staff *Purchasing*	Berhasil
10	20.20.20.244	Staff HRD	Berhasil
11	20.20.20.243	Staff Produksi	Berhasil
12	20.20.20.242	Staff Produksi	Berhasil
13	20.20.20.241	Staff *Engineering*	Berhasil
14	20.20.20.240	Staff *Engineering*	Berhasil
15	20.20.20.239	Staff *Accounting*	Berhasil
16	20.20.20.238	Staff *Accounting*	Berhasil
17	20.20.20.237	Sstaff Administrasi	Berhasil
18	20.20.20.236	Staff Gudang	Berhasil

Pada pengujian tabel 5 diatas, yaitu pengujian sebelum menerapkan *block browsing* mendapatkan bahwa semua pengguna dapat melakukan akses *browsing* ke internet pada sebelum jam kerja.

Tabel 6. Hasil Pengujian setelah menerapkan *Block Browsing* Waktu Pengujian sekitar jam 08.00 – 12.00

No	Ip *Address*	Nama Bagian	Akses *Browsing* Internet
1	20.20.20.253	Direktur	Berhasil
2	20.20.20.252	Manager *Marketing*	Berhasil
3	20.20.20.251	Manager Produksi	Berhasil
4	20.20.20.250	Manager *Engineering*	Berhasil
5	20.20.20.249	Spv *Accounting*	Berhasil
6	20.20.20.248	Spv *Engineering*	Berhasil
7	20.20.20.247	Spv Produksi	Berhasil
8	20.20.20.246	Staff *Marketing*	Berhasil
9	20.20.20.245	Staff *Purchasing*	Berhasil
10	20.20.20.244	Staff HRD	Berhasil
11	20.20.20.243	Staff Produksi	Gagal
12	20.20.20.242	Staff Produksi	Gagal
13	20.20.20.241	Staff *Engineering*	Gagal
14	20.20.20.240	Staff *Engineering*	Gagal
15	20.20.20.239	Staff *Accounting*	Gagal
16	20.20.20.238	Staff *Accounting*	Gagal
17	20.20.20.237	Sstaff administrasi	Gagal
18	20.20.20.236	Staff Gudang	Gagal

Pada pengujian tabel 6 di atas, yaitu pengujian setelah menerapkan *block browsing* waktu pengujian sekitar jam 08.00 – 12.00 mendapatkan pengguna yang terdapat pada *list* IP *address block browsing* tidak dapat akses *browsing* internet pada jam 08.00 – 12.00, dan pengguna yang terdapat *list* IP *address allow browsing* dapat mengakses internet melalui *browser*.

Tabel 7. Hasil Pengujian setelah menerapkan Blok *Browsing* Waktu Pengujian sekitar jam 12.00 – 13.00 atau Waktu Istirahat Makan Siang

No	Ip *Address*	Nama Bagian	Akses *Browsing* Internet
1	20.20.20.253	Direktur	Berhasil
2	20.20.20.252	Manager *Marketing*	Berhasil
3	20.20.20.251	Manager Produksi	Berhasil
4	20.20.20.250	Manager *Engineering*	Berhasil
5	20.20.20.249	Spv *Accounting*	Berhasil
6	20.20.20.248	Spv *Engineering*	Berhasil
7	20.20.20.247	Spv Produksi	Berhasil
8	20.20.20.246	Staff *Marketing*	Berhasil
9	20.20.20.245	Staff *Purchasing*	Berhasil
10	20.20.20.244	Staff HRD	Berhasil
11	20.20.20.243	Staff Produksi	Berhasil
12	20.20.20.242	Staff Produksi	Berhasil
13	20.20.20.241	Staff *Engineering*	Berhasil
14	20.20.20.240	Staff *Engineering*	Berhasil
15	20.20.20.239	Staff *Accounting*	Berhasil
16	20.20.20.238	Staff *Accounting*	Berhasil
17	20.20.20.237	Staff administrasi	Berhasil
18	20.20.20.236	Staff Gudang	Berhasil

Pada pengujian tabel 7 di atas, yaitu setelah menerapkan blok *browsing* waktu pengujian sekitar jam 12.00 – 13.00 atau waktu istirahat makan siang mendaptkan semua pengguna dapat mengakses *browsing* ke internet, karena pada jam tersebut dibolehkan semua karyawan dapat mengakses internet.

Tabel 8. Hasil Pengujian setelah menerapkan *Block Browsing* Waktu Pengujian sekitar jam 13.00 – 17.00

No	IP *Address*	Nama Bagian	Akses *Browsing* Internet
1	20.20.20.253	Direktur	Berhasil
2	20.20.20.252	Manager *Marketing*	Berhasil
3	20.20.20.251	Manager Produksi	Berhasil
4	20.20.20.250	Manager *Engineering*	Berhasil
5	20.20.20.249	Spv *Accounting*	Berhasil
6	20.20.20.248	Spv *Engineering*	Berhasil
7	20.20.20.247	Spv Produksi	Berhasil
8	20.20.20.246	Staff *Marketing*	Berhasil
9	20.20.20.245	Staff *Purchasing*	Berhasil
10	20.20.20.244	Staff HRD	Berhasil
11	20.20.20.243	Staff Produksi	Gagal
12	20.20.20.242	Staff Produksi	Gagal
13	20.20.20.241	Staff *Engineering*	Gagal
14	20.20.20.240	Staff *Engineering*	Gagal
15	20.20.20.239	Staff *Accounting*	Gagal
16	20.20.20.238	Staff *Accounting*	Gagal
17	20.20.20.237	Sstaff Administrasi	Gagal
18	20.20.20.236	Staff Gudang	Gagal

Pada pengujian tabel 8 di atas, yaitu pengujian setelah menerapkan *block browsing* waktu pengujian sekitar jam 13.00 – 17.00 mendapatkan pengguna yang terdapat pada *List* IP *address block browsing* tidak dapat akses *browsing* internet pada jam 13.00 – 17.00, dan pengguna yang terdapat *list* IP *address allow browsing* dapat mengakses internet melalui *browser*.

4. KESIMPULAN

Dari tabel hasil pengujian di atas, sebelum menerapkan *blocking browsing* akses internet dari semua pengguna dapat mengakses *browsing* internet. Pada hasil pengujian setelah menerapkan *block browsing* waktu pengujian sekitar jam 08.00 sampai jam 12.00 pengguna yang termasuk pada *list* IP *address allow browsing* dapat mengakses internet, sedangkan pangguna yang tidak masuk pada *list allow browsing* tidak dapat *browsing* internet. Hasil pengujian setelah menerapkan blok *browsing* waktu pengujian sekitar jam 12.00 sampai jam 13.00 atau waktu istirahat makan siang, semua karyawan dapat mengakses *browsing* internet, hasil pengujian yang terakhir pengujian setelah menerapkan blok *browsing* waktu pengujian sekitar jam 13.00 sampai jam 17.00, karyawan yang masuk pada *list* IP *address allow browsing* dapat mengakses *browsing* internet dan karyawan yang IP *address* nya tidak masuk pada *list allow browsing*

tidak dapat akses *browsing* internet, ini menunjukkan dengan metode *filter* pada *firewall router mikrotik* dapat melakukan limit akses *browsing* internet pada jam kerja di salah satu perusahaan *engineering* di Cikarang. Tentunya kebijakan ini hanya digunakan untuk bekerja pada kantor atau *work form office*.

Ucapan Terima Kasih

Terima kasih kepada LPPM STMIK Bani Saleh yang memberikan kesempatan untuk melaksanakan penelitian dosen internal di STMIK Bani Saleh.

DAFTAR PUSTAKA

[1] A. Nugroho and Y. Handrianto, "File *Sharing Server* menggunakan Samba *Server* dan Linux Ubuntu 12.04 Server," *Paradig. - J. Komput. dan Inform.*, vol. 18, no. 2, pp. 11–17, 2016.

[2] Z. M. Subekti, "Implementasi Keamanan Akses *Sharing* Folder pada Windows 10," vol. 11, no. 1, 2021.

[3] M. A. Sutisna, M. T. Informasi, U. A. Dahlan, I. Riadi, M. Kom, and J. Soepomo, "Analisa Forensik pada *Email Spoofing*," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 38–43, 2018.

[4] R. Muzawi, and R. Hardianto, "Perancangan Server dan Analisis *Quality of Service* (QoS) Jaringan Diskless PXE Linux pada Laboratorium Komputer STMIK-Amik-Riau," *J. INOVTEK POLBENG-Seri Informatika*, vol. 1, no. 1, 2016.

[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.

[6] N. Suryana, "Perancangan Penggunaan *Firewall* dan *Proxy Server* untuk Membatasi Hak Akses Internet," *J. Sutet*, vol. 8, no. 1, pp. 44-53, 2019.

[7] I. W. D. Alfian Aji Saputra, "Implementasi *Access Control List* menggunakan *Mikrotik* pada SMK Budi Mulia Tangerang," *Jurnal IDEALIS*, vol. 1, no. 5, pp. 401–408, 2019.

[8] Noviansyah, "Pemanfaatan *Web Proxy* sebagai Pengoptimal Keamanan," *J. KhatuListiwa Inform.*, vol. 8, no. 1, pp. 34–39, 2020.

[9] R. D. H. Ontoseno, M. N. Haqqi, and M. Hatta, "Limitasi Pengguna Akses Internet berdasarkan Kuota Waktu dan Data menggunakan PC *Router Os Mikrotik*," *Tek. Eng. Sains J.*, vol. 1, no. 2, p. 125, 2017.

[10] M. Siddik, "Implementasi *Mikrotik Router Board* 750 sebagai *Firewall* Blok Situs pada Jaringan LAN," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 3, no. 2, pp. 70–75, 2019.