RANCANG BANGUN APLIKASI *FIREWALL* PADA JARINGAN KOMPUTER

Novanda Ade Pratama, Joseph Dedy Irawan, FX. Ariwibisono
Program Studi Teknik Informatika S1, Fakultas Teknologi Industri
Institut Teknologi Nasional Malang, Jalan Raya Karanglo km 2 Malang, Indonesia
1818086@scholar.itn.ac.id

ABSTRAK

Kebebasan dalam mengakses internet telah terbukti dapat menimbulkan dampak *negative* pada anak usia 13 tahun, rasa ingin tahu akan dunia luar seperti pornografipun dengan mudah mereka akses di dunia maya lewat pemanfaatan internet. Kasus ini sering di jumpai di anak SMP jaman dulu juga yang sering membawa HP diam diam dan terdapat video pornografi di dalamnya, apalagi sekarang anak SMP pun sudah bisa membawa HP kesekolah dan mengakses internet secara bebas di sekolahannya. Penelitian ini ditujukan untuk siswa SMP 12 malang agar penggunaan internet di sekolah menjadi teratur dan siswanya dapat menggunakan internet secara sehat. Metode yang digunakan adalah menggunakan metode *address list* dimana *ip address* yang diizinkan sebagai *whitelist* maka akan dapat di akses Ketika *firewall* menyala. Hasil penelitian dari pembuatan aplikasi ini adalah *Administrator* dapat melakukan *filtering web* agar penggunaan internet dapat teratur. Pengujian aplikasi *firewall* pada jaringan komputer dengan menggunakan sistem *schedule* sebagai penjadwalan otomatis. Penerapan metode *addresslist* sebagai penentu *IP address* mana yang akan di perbolehkan mengakses internet Ketika *firewall* menyala. Pada pengujian pada *menu role*, jaringan dapat di blokir secara manual dan bisa memblokir *port* apa yang akan di izin kan seperti *port* UDP atau TCP.

Kata kunci : *firewall, web filtering, addresslist. jaringan computer, API*

1. PENDAHULUAN

Seiring dengan berkembangnya waktu teknologi pun ikut berkembang begitu juga dengan kebutuhan manusia, dimana setiap manusia perlu saling komunikasi satu sama lain. Salah satu teknologi yang terus berkembang adalah internet, Internet adalah salah satu teknologi yang dibutuhkan setiap manusia di kehidupan sehari hari. Sekolah Smp 12 Malang merupakan salah satu intansi atau sarana dalam melakukan proses belajar mengajar. Sebagai organisasi pendidikan yang formal sekolah mempunyai kewajiban untuk meningkatkan mutu Pendidikan.

Kebebasan dalam mengakses internet telah terbukti dapat menimbulkan dampak *negative* pada anak usia 13 tahun, rasa ingin tahu akan dunia luar seperti pornografipun dengan mudah mereka akses di dunia maya lewat pemanfaatan internet. Kasus ini sering di jumpai di anak SMP jaman dulu juga yang sering membawa HP diam diam dan terdapat video pornografi di dalamnya, apalagi sekarang anak SMP pun sudah bisa membawa HP kesekolah dan mengakses internet secara bebas di sekolahannya.

Untuk solusi di atas diperlukan suatu sistem yang efektif dan efisien dalam menyaring situs-situs negatif seperti pornografi, kekerasan, jejaring sosial, perjudian dll, Sehingga dapat tercipta penggunaan internet secara sehat. Berdasarkan masalah tersebut peneliti berniat membuat suatu sistem jaringan komputer mengenai *filtering* berbasis web agar tercipta *browsing* yang aman dan teratur bagi siswa siswi SMPN 12 Malang.

2. TINJAUAN PUSTAKA

2.1. Penelitian Sebelum

Pada penelitian yang berjudul "Perancangan *firewall* filtering dan manajemen *bandwidth* menggunakan router mikrotik pada jaringan komputer SMA NEGRI 1 Seputih banyak Lampung Tengah" Tujuan dari penelitian ini adalah Tujuan dari penelitian ini adalah memberikan perancangan *firewall filtering* dan manajemen *bandwidth* menggunakan MikroTik Router, memperluas ruang lingkup jaringan di SMA Negeri 1 Seputih Banyak, Dalam penyusunannya penulis menggunakan metode R&D (*Research and Development*) [1].

Pada penelitian yang berjudul "Implementasi *Firewall* Filtering Web dan Manajemen *Bandwith* Menggunakan Mikrotik" Tujuan dari penelitian ini adalah untuk memfilter situs negatif dan sistem *filtering* web dan pengaturan bandwidth dibutuhkan agar penggunakan internet lebih baik, cepat akses, efektif dan efesien. Sistem ini berguna untuk meningkatkan kecepatan akses pada SMK Multi Media Mandiri agar tercipta internet yang sehat dengan *filtering* web dengan mikrotik [2].

Pada penelitian yang berjudul "Implementasi *Firewall* Dan Web *Filtering* Pada Mikrotik Routeros Untuk Mendukung Internet Sehat Dan Aman (Insan)" Tujuan dari penelitian ini adalah Untuk mengurangi dampak konten tidak pantas internet maka perlu dilakukan upaya untuk mengurangi atau membatasi akses konten tidak pantas di internet. Salah satu upaya tersebut yaitu melalui program internet sehat dan aman (INSAN) yang dicanangkan oleh Kemkominfo dengan melibatkan seluruh komponen masyarakat [3].

Pada penelitian yang berjudul "Rancang Bangun Jaringan Internet Menggunakan Router Mikrotik Rb2011il-Rm Dengan Web *Filtering* Untuk Penggunaan Internet Sehat Di Smk Ma'arif Nu 1 Paguyangan". Tujuan dari penelitian ini adalah untuk membatasi atau memfilter situs situs yang sehat bagi siswa siswi agar tercipta jaringan internet di sekolah tersebut dapat terfilter dengan baik, dan hanya sistus situs sehat yang bisa diakses sementara situs yang berbau sara dan pornografi dapat di blokir di jaringan internet [4].

2.2. Firewall

Firewall adalah suatu perangkat keamanan jaringan yang memantau lalu lintas jaringan yang masuk maupun keluar dan *firewall* akan memutuskan paket data mana yang akan diizinkan atau di blokir berdasar kan peraturan yang telah di buat oleh *admin. Firewall* disebut juga sebagai benteng pertahanan lapisan pertama pada jaringan komputer, *firewall* akan membangun pembatas antara jaringan *local* yang terkendali dengan jaringan luar seperti internet dsb. (www.cisco.com, 2019) [3].

2.3. Web Filtering

Cara kerja *web filter* yaitu dengan cara memblokir akses web yang tidak terdaftar di *whitelist* sebagai *website* yang diizinkan pada jaringan tersebut. mikrotik juga menyediakan fitur itu dengan beberapa cara/teknik (Takeuchi, 2017). Fitur atau *policy* untuk memblock web yang dapat diterapkan pada MikroTik diantaranya yaitu *static* DNS, *web proxy*, *route policy*, *content filter*, *layer 7 firewall* dan *destination IP address/port block* (Takeuchi, 2017) [3].

2.4. API (Application Programming Interface)

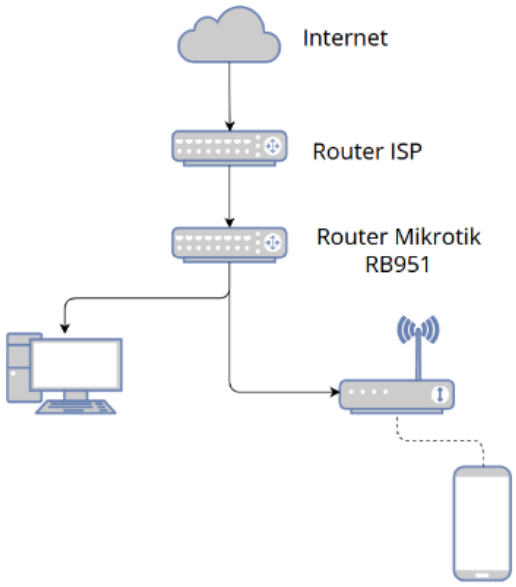
(API) adalah sekumpulan perintah, fungsi, dan *protocol* yang dapat digunakan oleh *programmer* saat membanguniperangkatilunakiuntuki sistemi operasi tertentu. iAPIidapatimenjelaskanicarai sebuahi tugas tertentuidilakukan. iiKarenaiitu, iAPIibiasanya menyertakani penjelasanidari ifungsi/rutini yang disediakannya. iAPIimenyediakanifungsiidan perintah denganibahasaiyangilebihiterstrukturidan lebih mudah untuk dipahami oleh *programer* bila dibandingkan dengan *System Calls*, hal ini penting untuk aspek *editing* dan pengembangan, sehingga *programer* dapat mengembangkan sistem dengan mudah. API juga dapat digunakan pada Sistem Operasi mana saja asalkan sudah ada paket-paket API nya [11].

2.5. Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri dari komputer - komputer yang didesain untuk dapat berbagi sumber data dan daya satu sama lain (printer, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban *web*). Tujuan dari jaringan komputer adalah suatu jaringan yang terdapat pada suatu lokasi dan bersifat *local* dan tujuan di buatnya jaringan komputer agar dapat berkomunikasi satu sama lain dalam jaringan local tersebut. Dalam jaringan komputer biasanya terdapat yang melayani dan di layanin, kedua nya itu di dalam jaringan komputer di sebut *client server* [6].

3. ANALISIS DAN PERANCANGAN

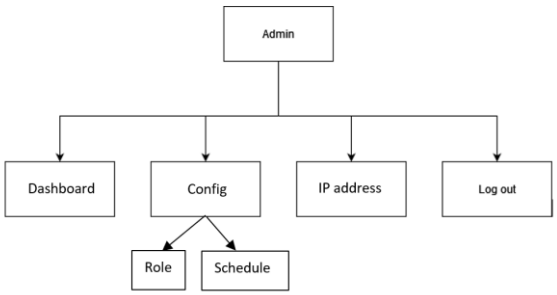
3.1. Diagram Blok



Gambar 1 Diagram Blok system network firewall control

Pada gambar 1 merupakan diagram blok yang digunakan untuk merancang *system filtering* jaringan berbasis web ini. diagram ini menggunakan Mikrotik yang terhung dengan internet dari ISP (*Internet Service Provider*) atau penyedia layanan internet untuk melakukan *filtering* jaringan. Terdapat 2 device yang terkoneksi dengan router menggunakan kabel UTP dan juga *wireless*. Komputer digunakan untuk mengkonfigurasi router menggunakan aplikasi *winbox*, Sedangkan HP digunakan sebagai *user* pengguna layanan.

3.2. Struktur Menu



Gambar 2 Struktur Menu aplikasi network firewall control

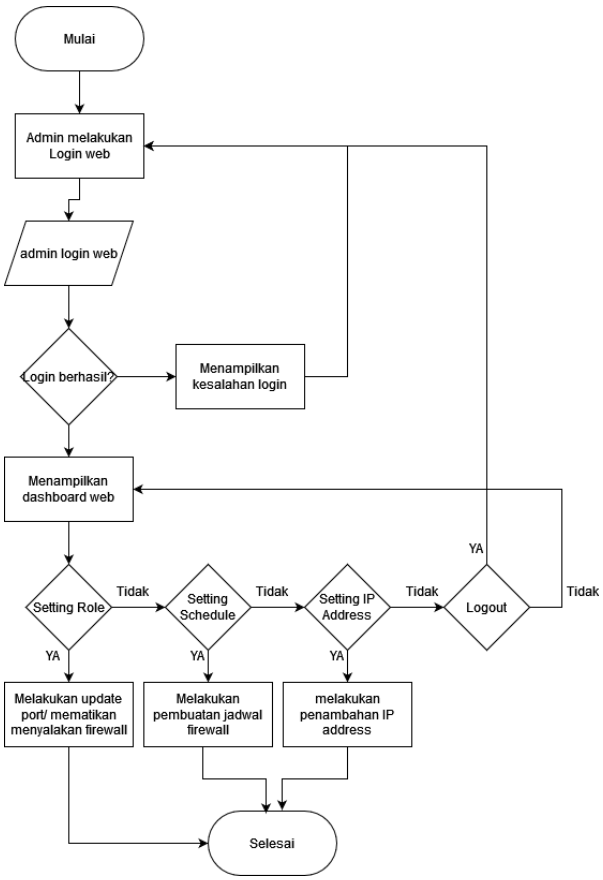
Pada gambar 2 merupakan struktur menu dari *system filtering* jaringan berbasis web yang terdiri dari 4 menu utama, yaitu:

1. Menu *Dashboard*, sebagai menu untuk menampilkan *user active* pada jaringan tersebut dan menampilkan data paket yang diakses.
2. Menu *Config*, dibagi menjadi 2 menu yaitu menu *role* dan menu *schedule*
3. Menu *Rol*e, sebagai pengatur jalannya *firewall* dan *port* yang bisa di akses oleh *user*
4. Menu *schedule*, sebagai pengatur jadwal kapan mati dan hidup *firewall* secara otomatis
5. Menu *ip address*, sebagai menu untuk melakukan penambahan *Ip address* yang akan di perbolehkan di buka oleh *user*.
6. Menu *Logout*, untuk keluar dari *system*.

3.3. Penjelasan API Mikrotik

Pada sistem ini menggunakan API sebagai koneksi antara *website* dengan *hardware* mikrotik RB951 , jadi alur dari api ini adalah, pertama mikrotik akan mengirimkan data dan akan di olah oleh *xampp* yang nantinya akan menjadi *website*, lalu tugas API ini adalah untuk penjembatan antara *software* dan *hardware*.

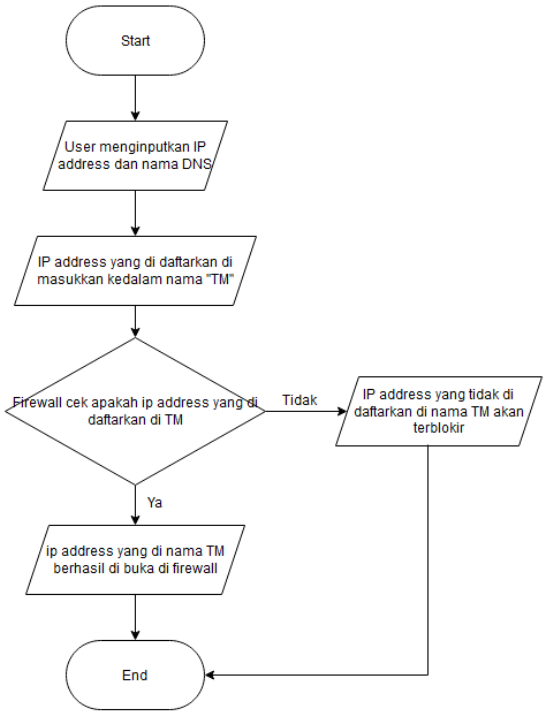
3.4. Flowchart sistem sistem network firewall control



Gambar 3 Flowchart sistem network firewall control

Pada gambar 3 merupakan *flowchart system network firewall control*. Pertama admin akan memasuki web dan melakukan *login* ke web tersebut, lalu jika berhasil maka akan menampilkan *dashboard* dimana isinya adalah tentang *active user* di jaringan tersebut, lalu akan ada menu *address list*, dimana isinya untuk menginputkan *Ip address* yang di perbolehkan di Ip tersebut jika tidak maka akan masuk ke menu selanjutnya yaitu ke pengaturan *role* jaringan setelah itu selesai.

3.5. Flowchart Address list



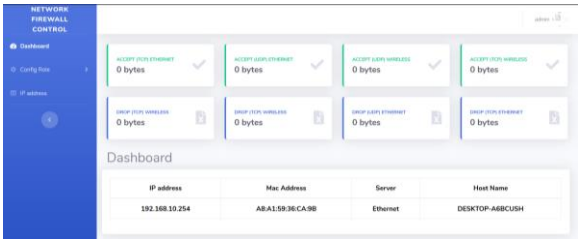
Gambar 4 Flowchart address list

Pada gambar 4 *flowchart* algoritma *address list* ini pertama *admin* akan memasukkan sebuah *IP address website* yang akan di izinkan dan akan di simpan di *whitelist* dengan nama "TM". Ketika *firewall* menyala, maka akan mengecek apakah ada *ip address* yang telah di daftarkan di nama TM tersebut terdaftar, jika ada maka *ip address* akan bisa di akses, dan jika tidak ada di nama TM maka *ip address* tersebut akan di blokir.

4. HASIL DAN PEMBAHASAN

4.1. Tampilan pada Menu dashboard

Pada Gambar 5 Tampilan *dashboard* di atas ini adalah tampilan *dashboard* yang dimana akan menampilkan data *user* yang *connect* dan data *packet* yang di akses ketika *firewall* menyala dan ketika *firewall* mati



Gambar 5 Tampilan Menu Dashboard

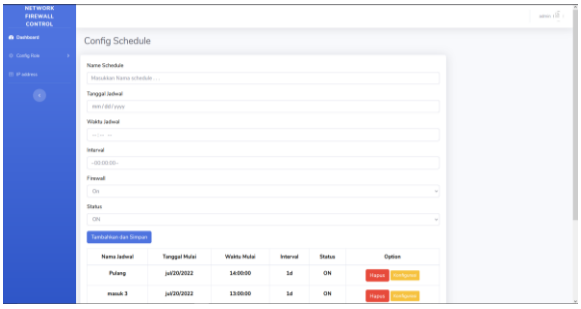
4.2. Tampilan menu IP address

Pada Gambar 6 Menu tambah *IP address* di atas ini adalah menu untuk menambah *ip address* yang akan diizinkan oleh sistem ketika kondisi *firewall* menyala.dan juga kita dapat mengganti data pada IP tersebut.

Gambar 6 Menu tambah IP address

4.3. Tampilan Schedule

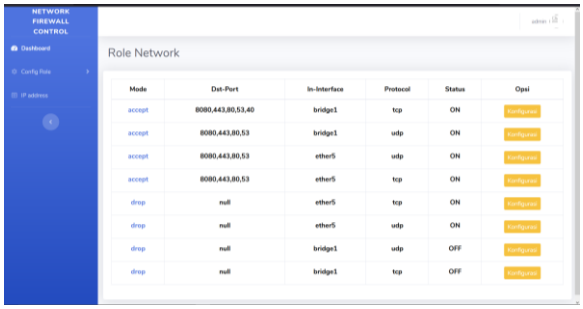
Pada Gambar 7 Tampilan *schedule* di atas ini adalah tampilan dari menu *schedule*, kita dapat mengatur jam berapa hari apa lalu kondisi untuk menyalakan *firewall* nya. dan fungsinya ini agar si *admin* tidak perlu repot dalam menyalakan *firewall* pada jam masuk sekolah dan mematikan *firewall* pada jam istirahat.



Gambar 7 Tampilan schedule

4.4. Tampilan *Config Role*

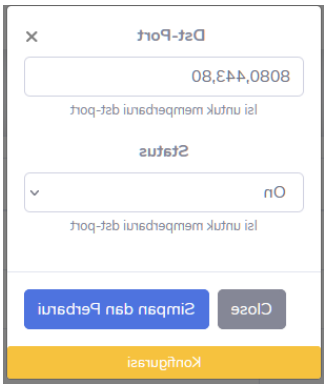
Pada Gambar 8 Tampilan menu *Config Role* di atas ini akan menampilkan *port port* mana yang akan di *enable* / disable , karena ketika *port* ini *enable* akan menjalankan fitur *firewall* dimana *client* tidak bisa mengakses internet dengan bebas kecuali *IP address* yang telah di daftarkan



Gambar 8 Tampilan menu Config Role

4.5. Tampilan Menambah port

Pada Gambar 9 Tampilan Menambahkan *port* di atas ini adalah tampilan ketika menambah dan mengatur *firewall*, kita bisa menambah *port* yang dapat diizinkan seperti HTTP atau HTTPS dan kita juga bisa menyalakan dan mematikan *firewall* secara manual



Gambar 9 Tampilan Menambahkan port

4.6. Pengujian Halaman awal website

Pengujian halaman *dashboard* ini akan mengecek apakah *user* yang *connect* dengan jaringan dapat terdeteksi, dan menu yang tersedia apakah dapat di akses dengan baik.

Table 1. Pengujian halaman awal *website*

No	Nama	Luaran yang diharapkan	Validitas	
			Y	N
1	*User Connect*	Menampilkan data *user* / *client* jaringan dengan lengkap	Y	
2	*Firewall data realtime*	Menampilkan paket yang di izinkan dan paket yang tidak di izinkan	Y	
3	*Role*	Membuka *sidebar* dan Masuk ke halaman *Configrole*	Y	
4	*Schedule*	Membuka sidebar dan Masuk ke halaman *Schedule*	Y	
5	*IP address*	Membuka sidebar dan Masuk ke halaman add *ipaddress*	Y	

Hasil dari pengujian halaman awal ini semua menu dapat di akses dengan baik dan menampilakn informasi yang dibutuhkan di setiap menu.

4.7. Pengujian menu configrole

Pengujian *firewall* ini dilakukan untuk mengetahui apakah *ip address* yang telah di daftarkan pada aplikasi dapat terbuka dengan baik atau tidak Hasil pengujian dapat di lihat dari beberapa data di bawah ini.

Tabel 2. Pengujian *Firewall*

No	Nama	Luaran yang diharapkan	Validitas	
			Y	N
1	Membuka spada spada.itn.ac.id	Dapat membuka *website* spada.itn.ac.id dengan kondisi *firewall* ON	Y	
2	Membuka spada Itn.ac.id	Dapat membuka *website* Itn.ac.id dengan kondisi *firewall* ON	Y	
3	Membuka youtube.com	Tidak dapat membuka *website* youtube.com dengan kondisi *firewall* ON	Y	
4	Membuka spada Instagram.com	Tidak dapat membuka *website* Instagram.com dengan kondisi *firewall* ON	Y	
5	Menambahkan dan menghapus data *port*	Menambahkan dan menghapus *port* pada menu *role*	Y	
6	Tombol *firewall*	Menyalakan menu *firewall*	Y	

Hasil dari pengujian menu *configrole* didapat bahwa *firewall* dapat di atur dengan cara menambahkan *port* tertentu dan juga bisa mengaktifkan *firewall* secara *customize*

Tabel 3. Pengujian *Firewall* ON dengan VPN

No	Nama	Luaran yang di harapkan	Validitas	
			Y	N
1	Membuka situs judi *online* dengan VPN	Situs yang dibuka tidak dapat di akses	Y	
2	Membuka situs web indoxx1 dengan VPN	Situs indoxx1 tidak dapat di buka/ diakses	Y	

Hasil dari pengujian Ketika *firewall on off* adalah *user/client* tidak dapat mengakses Ketika *firewall* dalam keadaaan on meskipun menggunakan VPN sekalipun.

4.8. Pengujian Schedule

Pengujian *schedule* ini dilakukan untuk mengetahui apakah *schedule* yang ditambahkan pada aplikasi dapat terbuka dan berjalan dengan baik atau tidak.

Tabel 4. Pengujian *Schedule*

No	Nama	Luaran yang di harapkan	Validitas	
			Y	N
1	Menambahkan jadwal	Dapat menambahkan jadwal	Y	
2	Mengubah data pada jadwal tertentu	Dapat mengubah data jadwal	Y	
3	Menghapus data jadwal	Dapat Menghapus jadwal yang dimaksut	Y	
4	Menambah data Dengan nama yang sama	Menampilkan notifikasi jika ada yang sama		N
5.	Mengatur jadwal on off	Jadwal menjadi on dan oFF	Y	

Hasil dari Pengujian *schedule* disini adalah jadwal dapat berjalan dengan baik dan jadwal bisa di *customize* namun masih ada kekurangan jika data ada yang sama jadi tidak bisa menampilkan notifikasi Ketika ada nama jadwal yang dobel.

4.9. Tampilan IP address

Pengujian menu *IP address* ini adalah untuk mengetahui apakah dengan kita menambahkan data dengan tidak lengkap atau berbeda bisa terakses Ketika *firewall* dalam keadaan ON.

Tabel 5. Pengujian *system menu IP address*

No	Nama	Luaran yang di harapkan	Validitas	
			Y	N
1	Menambahkan data dengan lengkap	*IP address* yang ditambahkan bisa membuka situs yang dimaksut	Y	
2	Menambahkan data yang berbeda	Situs dapat diakses dengan normal	Y	
3	Menambahkan data dengan *ip address* yang salah	Situs yang dimaksut tetap bisa di akses	Y	

Hasil dari pengujian IP address yang disini dapat menambahkan ip address sebagai Whitelist Ketika firewall menyala

Tabel 6. Pengujian beberapa *IP address* Ketika *firewall* menyala

No	Nama	Luaran yang di harapkan	Validitas	
			Y	N
1	Membuka spada.itn.ac.id	Dapat membuka web spada.itn.ac.id	Y	
2	Membuka ejournal.itn.ac.id	Dapat membuka web ejournal.itn.ac.id	Y	
3	Membuka smpn12malang.sch.id	Dapat membuka web smpn12malang.sch.id	Y	
4	Membuka jawapos.com	Dapat membuka web jawapos.com	Y	
5	Membuka wahyublahe.id	Dapat membuka web wahyublahe.id	Y	
6	Membuka *youtube.com*	Tidak dapat membuka web *youtube.com*	Y	
7	Membuka *Instagram.com*	Tidak dapat membuka web *Instagram.com*	Y	
8	Membuka *facebook.com*	Tidak dapat membuka web *facebook.com*	Y	
9	Membuka *judionline99.com*	Tidak dapat membuka web *judionline99.com*	Y	

No	Nama	Luaran yang di harapkan	Validitas	
			Y	N
10	Membuka *judibola91.com*	Tidak dapat membuka web *judibola91.com*	Y	

Pada Tabel 6 adalah beberapa *IP address* yang diizinkan dan ada yang tidak diizinkan seperti pada nomor 1-5 adalah *IP address* yang diizinkan untuk di akses Ketika *firewall* menyala dan untuk 6-10 adalah *IP address* yang tidak di izinkan untuk di akses atau tidak dapat di akses Ketika *firewall* menyala

5. KESIMPULAN DAN SARAN

Berdasarkan Hasil dari Rancang Bangun aplikasi *firewall* pada jaringan komputer yang telah dilakukan maka didapat beberapa kesimpulan sebagai berikut: *Administrator* dapat melakukan *filtering web* agar penggunaan internet dapat teratur. Pengujian aplikasi *firewall* pada jaringan komputer dengan menggunakan sistem *schedule* sebagai penjadwalan otomatis. Penerapan metode *addresslist* sebagai penentu *IP address* mana yang akan di perbolehkan mengakses internet Ketika *firewall* menyala. Pada pengujian pada *menu role*, jaringan dapat di blokir secara manual dan bisa memblokir *port* apa yang akan di izin kan seperti *port* UDP atau TCP. Pada pengujian *Schedule* data yang akan di tambahkan kedalam *schedule* dapat berjalan dan mengatur jalannya *firewall* namun masih belum bisa menampilkan notifikasi Ketika ada kesamaan nama jadwal. Pada pengujian *IP address* dapat berjalan dengan baik Ketika kondisi *firewall* menyala dan *ip address* yang di daftarkan DNS dari ip tersebut dapat di akses dan berjalan dengan lancer. Pada pengujian menggunakan VPN, *user* yang terkoneknsi dengan jaringan ini tetap tidak akan bisa mengakses *IP address* yang di blokir. Dan dari pengujian dari *firewall* ON didapatkan hasil *user* tidak dapat mengakses *website* yang diblokir meskipun menggunakan *VPN* sekalipun, dan untuk pengujian jadwal dapat di tambahkan danjuga dapat di customize sesuai selera dan untuk menu *configrole* dapat di *custom* dengan cara menambahkan *port* yang akan di atur seperti *port* yang akan diizinkan atau *port* mana yang akan diblokir. Adapun saran setelah melakukan pengujian, agar kedepannya sistem ini dapat berjalan lebih baik yaitu sebagai berikut :

Agar sistem dapat lebih mudah di pahami lagi oleh orang awam di buat untuk tampilan menambah *user* Ketika *login*, agar admin *login* sistem tidak hanya 1 saja. Menampilkan notifikasi Ketika data yang sama di tambahkan kedalam sebuah jadwal yang ada.

DAFTAR PUSTAKA

[1] Apriyanto, D., Sudarmaji, S. and Hidayat, A., 2021. PERANCANGAN FIREWALL FILTERING DAN MANAJEMEN BANDWIDTH MENGGUNAKAN ROUTER MIKROTIK PADA JARINGAN KOMPUTER SMA NEGERI 1 SEPUTIH BANYAK LAMPUNG TENGAH. *JIKI (Jurnal llmu Komputer & lnformatika)*, *2*(2), pp.141-147.

[2] Nurfauzi, A., Nainggolan, E.R., Khasanah, S.N. and Setiadi, A., 2018. Implementasi Firewall Filtering Web dan Manajemen Bandwith Menggunakan Mikrotik. *SNIT 2018*, *1*(1), pp.162-167.

[3] Jakaria, D.A. and Yulianeu, A., 2020. IMPLEMENTASI FIREWALL DAN WEB FILTERING PADA MIKROTIK ROUTEROS UNTUK MENDUKUNG INTERNET SEHAT DAN AMAN (INSAN). *JUTEKIN (Jurnal Teknik Informatika)*, *8*(2).

[4] Purnomo, J., Purbasari, W. and Sunaryono, S., 2020. RANCANG BANGUN JARINGAN INTERNET MENGGUNAKAN ROUTER MIKROTIK RB2011iL-RM DENGAN WEB FILTERING UNTUK PENGGUNAAN INTERNET SEHAT DI SMK MA'ARIF NU 1 PAGUYANGAN. *Teknikom: Teknologi Informasi, Ilmu Komputer dan Manajemen*, *3*(2), pp.25-29.

[5] Setiawan, D., 2017. *Buku Sakti Pemrograman Web: HTML, CSS, PHP, MySQL & Javascript*. Anak Hebat Indonesia.

[6] Yudianto, M.J.N., 2014. Jaringan komputer dan Pengertiannya. *Ilmukomputer. Com*, pp.1-10.

[7] Susianto, D., 2016. Implementasi queue tree untuk manajemen bandwidth menggunakan router board mikrotik. *Jurnal Cendikia*, *14*(1 April), pp.1-7.

[8] Novendri, M.S., Saputra, A. and Firman, C.E., 2019. Aplikasi Inventaris Barang Pada Mts Nurul Islam Dumai Menggunakan Php Dan Mysql. *lentera dumai*, *10*(2).

[9] Haerulah, E. and Ismiyatih, S., 2017. Aplikasi E-Commerce Penjualan Souvenir Pernikahan Pada Toko "XYZ". *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, *4*(1).

[10] Hidayanto, F., 2015. Pentingnya internet sehat. *Asian Journal of Innovation and Entrepreneursh*

[11] Jayanto, R.D., 2019. Rancang Bangun Sistem Monitoring Jaringan Menggunakan Mikrotik Router OS. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *3*(1), pp.391-395

[12] Pratama, R., Irawan, J.D. and Orisa, M., 2022. ANALISIS QUALITY OF SERVICE SISTEM MANAJEMEN BANDWIDTH PADA JARINGAN LABORATORIUM TEKNIK INFORMATIKA ITN MALANG. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *6*(1), pp.196-204