ANCAMAN KEAMANAN JARINGAN PADA SERVER UNTUK MEMBATASI WEBSITE TERTENTU MENGGUNAKAN MIKROTIK

Heri Gunawan[1]
[1TM]Universitas ibn khaldun Bogor, Jl. KH sholeh Iskandar Km.2, Bogor, 0251-8380993
[3]Jurusan Teknik Informatika, NCC (jaringan)
e-mail: [1]herigoenawan16@gmail.com

Abstrak

Mikrotik RouterOs™ adalah sistem operasi dan perangakat lunak yang dapat di gunakan untuk menjadikan komputer menjadi router network yang handal, Didesain untuk memberikan kemudahan bagi penggunanya administrasinya bisa dilakukan melalui Windows application (Winbox,)Server adalah sebuah sistem komputer yang menyediakan jenis layanan (service) tertentu dalam sebuah jaringan komputer,server didukung dengan prosesor yang bersifat scalable dan ram yang besar juga di lengkapi dengan sistem operasi khusus, yang disebut sebagai (network operating system). Internet banyak memberikan konten yang bermanfaat apabila penggunanya menggunakan internet secara baik, disamping itu internet juga dapat memberikan dampak negatif bagi penggunanya apabila internet di gunakan untuk hal yang negatif yang akan berdampak pada generasi muda yang akan merangkul negeri ini untuk menjadi penerus bangsa ini digunakan diluar norma yang berlaku. Saat ini internet sudah banyak beragam jenis situs jejaring sosial yang telah digunakan oleh banyak orang, tujuannya atau Salah satu solusinya yaitu agar pengguna internet tidak mengakses yang berdampak negatif atau merugikan dirinya sendiri,menggunakan metode Scientific of Inquiry dengan membatasi akses terhadap website-website tertentu untuk upaya pencegahan dalam mengakses situs internet yang berbau negatif dalam hal ini mengandung konten pornografi adalah dengan memblokir situs-situs negatif tersebut secara permanen menggunakan web proxy yang berfungsi untuk memblokir beberapa website yang tidak boleh di akses oleh klien melalui browser pada router Mikrotik Fakultas teknik Universitas Ibn khaldun.

Kata kunci : Mikrotik, Web proxy, Blok Website

Abstrack

Mikrotik RouterOs ™ is an operating system and software that can be used to make a computer a reliable network router, designed to provide convenience for its users, the administration can be done through Windows application (Winbox), The server is a computer system that provides certain types of services (services) in a computer network, the server is supported by a processor that is scalable and a large ram is also equipped with a special operating system, called a (network operating system). The internet provides a lot of useful content if the user uses the internet well, besides that the internet can also have a negative impact on its users if the internet is used for negative things which will affect the young generation who will embrace this country to be the successor of this nation. outside the prevailing norms. Today the internet has many different types of social networking sites that have been used by many people, the goal or One of the solutions is that internet users do not access the negative or self-detrimental effects, using the Scientific of Inquiry method by limiting access to websites Specifically for prevention efforts in accessing negative internet sites in this case containing pornographic content is by blocking these negative sites permanently using a web proxy that serves to block some websites that cannot be accessed by clients through a browser on the Mikrotik Faculty of Engineering routers Ibn Khaldun Universit

Keywoard : *Mikrotik, Proxy Web, block website*

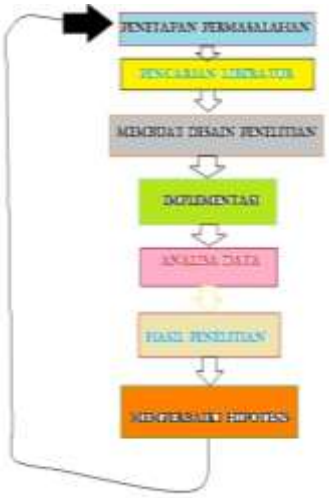
1.PENDAHULUAN

Dengan berkembangnya teknologi komputer dan komunikasi suatu model komputer tunggal yang melayani seluruh tugas-tugas komputasi suatu organisasi kini telah diganti dengan sekumpulan komputer yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya, sistem seperti ini disebut jaringan komputer. [1]

Server adalah sebuah sistem komputer yang menyediakan jenis layanan (*service*) tertentu dalam sebuah jaringan komputer, server didukung dengan prosesor yang bersifat scalable dan RAM yang besar, juga di lengkapi dengan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan (*network operating system*). Tugas utama *server* adalah melayani komputer *client.[2]*

Internet banyak manfaatnya apabila penggunanya menggunakan internet secara baik, di samping itu internet juga dapat memberi dampak negatif bagi penggunanya apabila digunakan norma yang berlaku.saat ini internet sudah banyak beragam jenis situs je-jaring sosial yang telah di gunakan oleh banyak orang, hal ini tentunya akan berdampak buruk bagi penggunanya jika di gunakan secara terus menerus, salah satu solusinya adalah dengan membatasi akses *website-website* tertentu agar tidak terjadi hal-hal yang tidak di inginkan. Upaya untuk pencegahan dalam mengakses situs internet yang berbau negatif dalam hal ini yang mengandung konten pornografi adalah dengan memblokir situs-situs negatif tersebut secara permanen menggunakan *web proxy* yang berfungsi untuk memblok beberapa *website* yang tidak boleh di akses oleh klien menggunakn *browser* pada *router mikrotik*. tujuan nya adalah untuk menerapkan internet sehat di area fakultas teknik dan terhindar dari dampak negatif yang berasal dari *website* pornografi.

2.METODE PENELITIAN



Gambar 1.Tahapan *Scientific of Inquiry*

1. Penetapan Permasalahan (*State General Problem*)
   Pada tahap awal yaitu mencari atau menentukan pokok permasalahan yang akan diamati.
2. Pencarianliteratur (*Conduct Literature Search*)
   Pada tahapan ini peneliti melakukan apa yang disebut dengan kajian pustaka.
3. Membuat Desain Penelitian (*Design Methodology*)
   Desain penelitian berisikan pengetahuan, bloking data, Dalam melakukan penelitian salah satu hal yang penting ialah membuat desain penelitian.
4. Implementasi
   Pada tahapan ini Implementasi merupakan tahapan yang sangat penting karena menentukan keberhasilan dalam suatu penelitian yang akan dibangun.
5. Analisa Data (*Analyze Data***)**
   Analisis sistem adalah telaah atas sistem berjalan dengan tujuan untuk mendesain sistem baru atau menyempurnakan sistem lama.
   Rincian tujuan dari tahapan analisis sistem adalah untuk:
6. Hasil Penelitian (*Report Results*)
   Dalam menulis laporan penelitian atau laporan akhir, kita harus berani mengemukakan dan menuliskan apa yang kita dapatkan selama melakukan penelitian tersebut.
7. Memperbaiki hipotesis
   Penarikan kesimpulan dilakukan setelah semua laporan hasil penelitian dilakukan.

Setiap kesimpulan yang dibuat oleh peneliti didasarkan pada data-data yang telah dikumpulkan. Kesimpulan yang diambil harus berupa jawaban dari permasalahan.[4]

3.HASIL DAN PEMBAHASAN

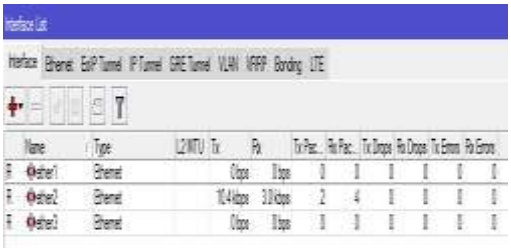
3.1 Konfigurasi Mikrotik Menggunakan Winbox

Dalam penulisan ini pengaksesan Mikrotik RouterOS akan menggunakan WinBox karena mudah dipahami dan mudah digunakan, adapun cara pengaksesan Mikrotik RouterOS melalui Winbox adalah sebagai berikut :

1. Buka aplikasi Winbox.
2. Klik lalu isikan *IP Address private* kampus yaitu 10.10.0.1 pada tampilan winbox, kemudian *login* dengan id yang sudah di buat dalam hal ini penulis memasukkan *login* dengan kata ***liat*** dan *password* yang tersedia.

Gambar 3.1: Tampilan awal aplikasi winbox

3. Kemudian cek status *interface* yang aktif pada menu *Interface List*, dalam hal ini menggunakan *interface* ether1, ether2, ether3



Gambar 3.2: Status interface yang tersedia

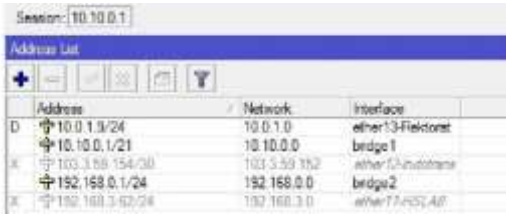
3.1.1 Konfigurasi DHCP *Client*

1. Pada menu IP klik DHCP *Client* lalu klik tanda + untuk memberikan *interface* ether1 konfigurasi DHCP dari server dan mendapatkan alamat *IP Address* serta DNS.

Gambar 3.3: DHCP *client* FT Teknik

3.1.2 Konfigurasi *IP Address*

1. Masukkan *IP Address* untuk Interface Internet dan LAN dengan cara pilih IP - Addresses.



Gambar 3.4: *IP addres list* yang tersedia

3.1.3 Konfigurasi DHCP server

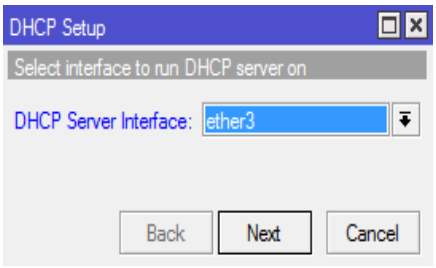
1. Buat DHCP SERVER yang tujuan adalah untuk memberikan *IP Address* secara otomatis kepada seluruh *client* yang berada pada *Interface LAN*. Klik IP – DHCP *server*.

Gambar 3.5: Tampilan untuk membuat dhcp *server*

2. DHCP *SERVER*

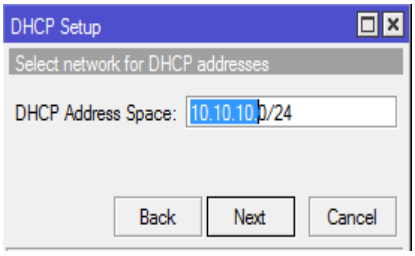
Gambar 3.6: dhcp *server* FT Teknik

3. Pilih *interface* yang akan digunakan sebagai DHCP *SERVER*.



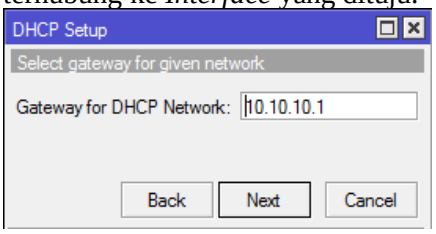
Gambar 3.7: Pilih *interface* untuk dhcp *server*

4. Masukkan IP untuk *Network* pada DHCP *Address Space*.



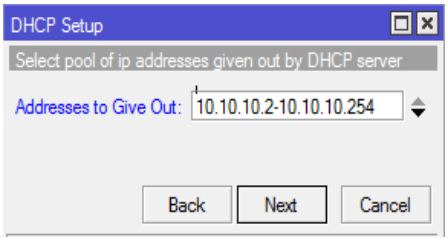
Gambar 3.8*: IP Network*

5. Masukkan *Gateway* sebagai gerbang atau alamat tujuan yang nantinya akan digunakan pada *Client* yang mendapatkan IP dari DHCP server tersebut agar terhubung ke *Interface* yang dituju.



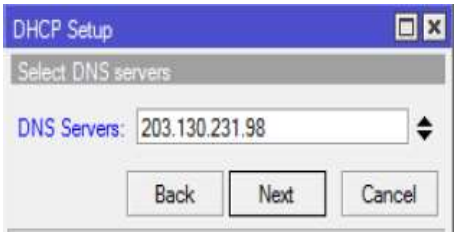
Gambar 3.9: Pemberian gateway

6. Masukkan *Range IP* untuk DHCP.



Gambar 3.10: pemberian *range* untuk *client*

7. Masukkan DNS *server*, dalam hal ini saya memasukkan DNS provider sebagai DNS *SERVER*.



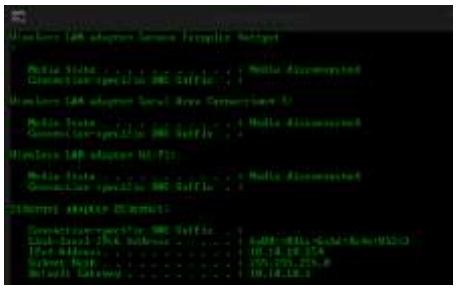
Gambar 3.11: DNS *server* FT Teknik

8. Konfigurasi DHCP telah berhasil dibuat.

Gambar 3.12: Dhcp *server* yang tersedia

3.2 Mengecek *IP Address* DHCP Pada *client*

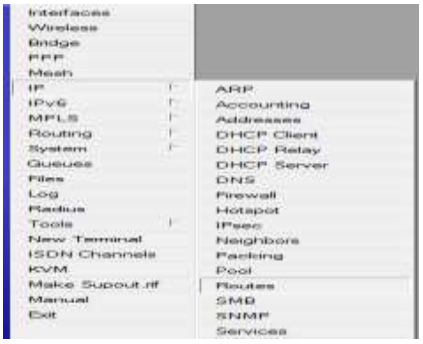
1. Cek apakah *client* yang berada dalam jaringan LAN telah berhasil mendapatkan *IP Address* dari Mikrotik. Buka CMD kemudian ketik *IPconfig*



Gambar 3.13: Mengecek *IP Client*

3.3 Konfigurasi Routing

1. Setting *routes* agar IP dapat mengetahui *gateway* yang berada pada *Switch* yang terhubung. Buka IP – pilih *Routes*.



Gambar 3.14: Menu *setting routing*

2. Karena menggunakan DHCP *Client*, maka konfigurasi *router* secara otomatis akan terbuat, namun apabila tidak menggunakan DHCP *Client*, Klik tanda + untuk membuat Konfigurasi baru dan masukan IP dari Dst. *Addres* yaitu 0.0.0.0/0 artinya adalah IP untuk seluruh *Network* dan masukan IP *gateway*
   Keterangan: D=*dynamic*, A=*Active*, C=*Connected*, S= *Static*

Gambar 3.15: *route* yang tersedia di Ft teknik

3.4 Konfigurasi *Domain Name System* (DNS)

Setting DNS pada Mikrotik dengan cara klik IP – pilih DNS.

Gambar 3.16: *Setting* DNS

Keterangan : Karena disini menggunakan DHCP *Client* maka untuk *setting* DNS tidak perlu dillakukan lagi. Namun apabila tidak menggunakan DHCP Client Maka penambahan Setting DNS perlu dilakukan agar dapat melakukan Koneksi menuju internet.

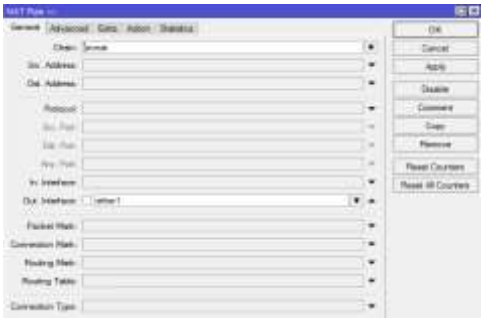
3.5 Konfigurasi *Firewall*

1. *setting Firewall* dengan cara klik IP – lalu pilih *Firewall*.

Gambar 3.17: Menu *setting Firewall*

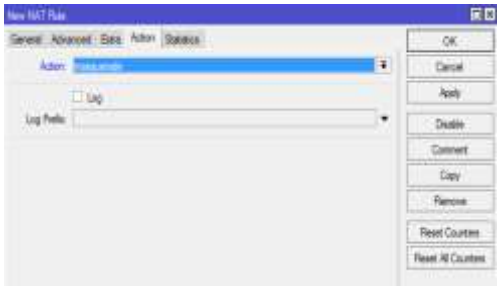
2. Pilih menu NAT untuk menghubungkan IP lebih dari satu Computer ke jaringan internet dengan menggunakan satu alamat IP. NAT bekerja dengan mengalihkan satu paket data dari satu alamat IP ke alamat IP yang lain. Saat satu paket diarahkan maka NAT akan mengingat dari Lokasi mana asal Paket serta kemana maksud paket itu. Klik tanda + untuk membuat Konfigurasi baru.

3. Pada *tab General* isikan *Chain* = Srcnat dan *Out. Interface* = internet.
   Keterangan: Srcnat(*Source NAT*) adalah pengalihan yang Dijalankan untuk paket data yang berasal dari Jaringan natted. NAT dapat merubah alamat IP asal Paket dari Jaringan natted dengan alamat IP umum. *Source* NAT selalu dikerjakan sesudah *Routing* saat Sebelum paket keluar menuju jaringan. *Masquerade* yaitu perumpamaan dari Srcnat.



Gambar 3.18: *setting* NAT pada *tab general*

4. Pada tab Action pilih *Masquerade* sebagai tindakan yang dilakukan untuk menghubungkan IP lokal menuju ke Jaringan internet (*Wide Area Network*) melalui perantara IP *Public*.



Gambar 3.19: setting NAT pada *tab action*

3.6 Tes Koneksi Dari Mikrotik Ke Gateway

1. Lakukan tes koneksi dari mikrotik ke *gateway* dengan perintah *PING* pada terminal.

Gambar 3.20: Tes Koneksi pada mikrotik

Keterangan:Tes koneksi antara mikrotik dengan *gateway* telah berhasil terhubung.

3.7 Konfigurasi web proxy

1. setting *Web Proxy* dengan cara klik IP – pilih *web proxy*.

Gambar 3.21: Tampilan *menu setting web proxy*

2. Pada Tab General ceklis kolom *Enabled* kemudian pilih *Access* agar masuk ke menu *web proxy Access*.

Gambar 3.22: *setting web proxy*

3. Klik + untuk membuat konfigurasi baru.

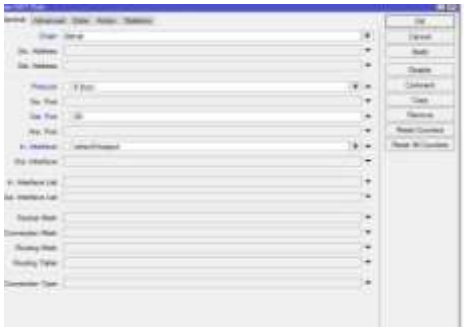
Gambar 3.23: Tampilan *awal web proxy acces*

4. Pada Src. *Address* Kosongkan saja karena *settingan* ini berfungsi untuk semua network. Pada Dst. *Address* kosongkan saja karena settingan ini berfungsi untuk semua *client.* Pada Dst. Host isikan konten *Website* yang akan dijadikan daftar *filter* pada *web Proxy*. Pada kolom Action isikan *Deny* untuk melakukan perintah menolak

3.8 Konfigurasi Firewall NAT Rule

1.Buat NAT *Rule* yang berada pada menu *Firewall.* Tujuanya adalah agar setiap ada *Request* terhadap *port* 80 yang berasal dari

client maka akan di *Filter* dan dialihkan ke *web proxy* yang berada di port 8080



Gambar 3.24: Konfigurasi NAT *rule*

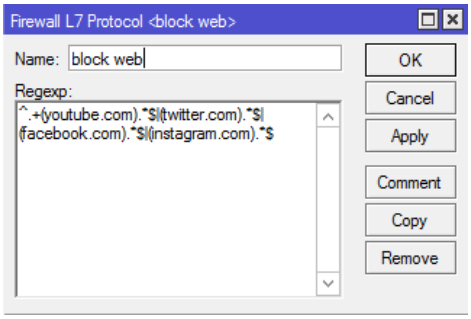
Keterangan:
Pada *tab Chain* piliih Dstnat yang artinya untuk merubah *Desstination Address* pada sebuah *Packet* data yang akan keluar dengan menggunakan Protocol TCP/IP yang ingin mengakses port 80 (HTTP) yang berasal dari *Interface* LAN.

2.Pada *tab Action* pilih *redirect* agar setiap *Request* yang akan keluar dialihkan terlebih dahulu ke *port* 8080 yaitu *Web proxy*.

Gambar 3.25: Konfigurasi pada *tab action*

3.9 *Firewall Layer 7 Protocol*

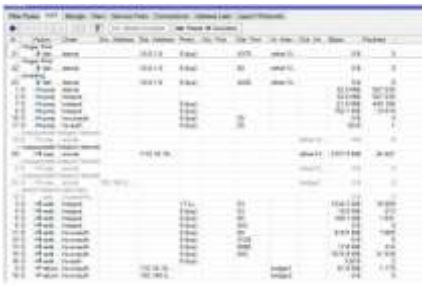
1. Buat *rules Layer* 7 dengan cara klik IP – *Firewall* – Pilih *Tab Layer 7 Protocol.*
   Kemudian buat *rules Layer* 7 untuk Memblok *Website* yang memiliki *protocol* 443 atau HTTPS.



Gambar 3.26: *setting* pada *Firewall layer 7 protocol*

^.+*(youtube.com).*$|(twitter.com).*$|(facebook.com).*$|(instagram.com).*$*
Isikan *name block web* dan isikan regexp yang akan di Blok

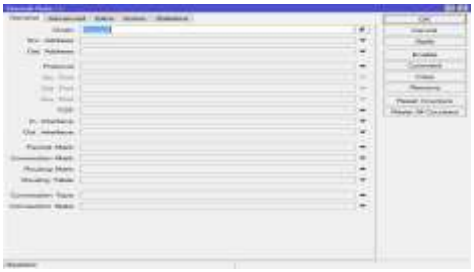
2. Buat *Addresses List* yang nantinya akan dijadikan sebagai Target dari *rules Layer 7 Protocol*



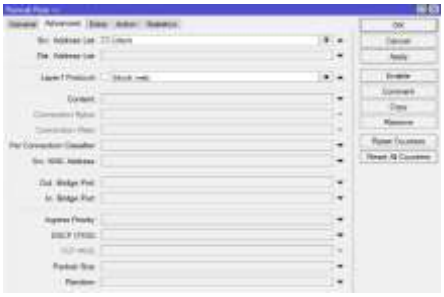
Gambar 3.27: Tampilan NAT pada FT teknik

3.10 Konfigurasi *Firewall Filter Rules* untuk *Layer 7 Protocol*

Klik tanda yang ada di colom chain dan pilih *Forward*

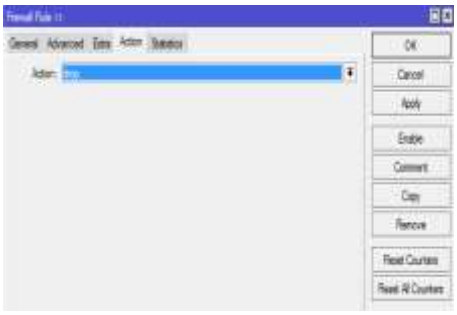


Gambar 3.28: Tampilan *setting* pada *tab general*



Gambar 3.29: Tampilan setting pada tab advanced

Di advanced pilih kolom Src. Address list pilih Client



Gambar 3.30: Tampilan *setting* pada *tab action*

Klik di *action* pilih *Drop* klik *apply* lalu oke

Tampilan Hasil Konfigurasi dari *Layer 7 Protocol*

Gambar 3.31: Tampilan *Instagram* yang di blok

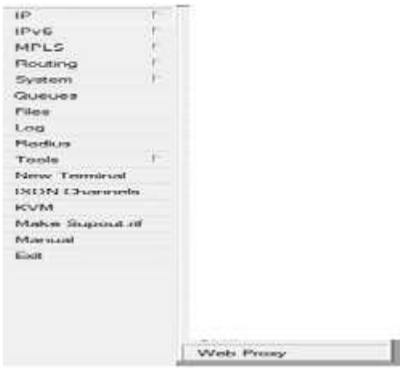
Gambar 3.32: tampilan *twitter* yang di blok

Gambar 3.33 Tampilan facebook yang di blok

Kemudian Buat *FIREWALL rules* baru dengan menambah kan *Port* yang Rentan terhadap Serangan virus. Contoh port 1, port 1-19, berbagai Protocol, Sebagian banyak *Port* ini tidak begitu di perlukan namun tidak dapat diganggu.membuat *Rules* pada beberapa Port

3.11 *Web proxy* Untuk menjadi perantara antara client dengan server.

Klik IP lalu pilih *web proxy*



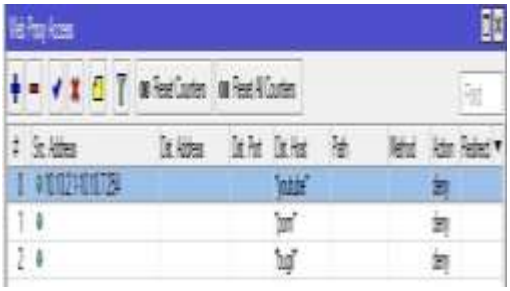
Gambar 3.34: *Menu setiing web proxy*

Gambar 3.35: *setting general* pada *web proxy*

Di *web Proxy setting* isikan centang pada *enable* dan isikan *port* 8080

3.12 Di *web Proxy*

Klik acces lalu pilih tanda + untuk membuat *website* yang akan di blok.



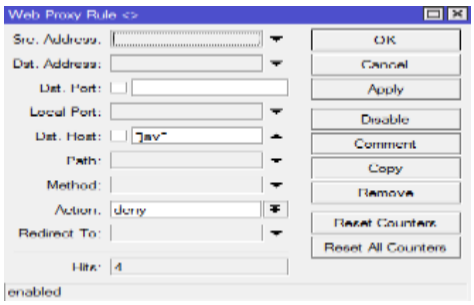
Gambar 3.36 *setting web proxy acces*

Gambar 3.37: *setting web proxy rule*

Pertama kita Blok *PORN*., pilih Dst *Host* tuliskan **porn**, di *Action* pilih *deny* klik *apply* lalu ok

Gambar 3.38: *setting web proxy rule* kedua

Kedua sama isikan Dst. *Host* "Bugil" lalu isikan *Action deny* klik *apply* lalu ok



Gambar 3.39: *setting web proxy rule* ketiga

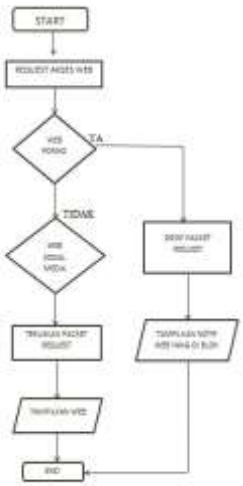
Selanjutnya pada *website porn* sama pilih Dst. *Host* ketik **JAV**. Dan pada *action* plih *deny*.

Gambar 3.40: mengakses *website* yang mengandung *porn*

Gambar 3.41: mengakses *website* yang mengandung *jav*

Gambar 3.42: mengakses web yang mengandung *jav*

3.13 Flowchart sistem



Gambar 3.42 *flowchart* pengakses *web*

4 KESIMPULAN

Berdasarkan analisis dan perancangan yang dilakukan dapat ditarik kesimpulan sebagai berikut:

Dari hasil uji coba di Fakultas Teknik Universitas ibn khaldun, maka dapat disimpulkan bahwa sistem *web proxy* untuk memblokir situs negatif di Fakultas teknik Universitas ibn khaldun telah berhasil dibuat. *Web proxy* mampu memblokir situs yang menggunakan port HTTPS. *Web proxy* dengan metode kata pencarian hanya memblokir situs berdasarkan nama domain website tersebut yang cocok dengan kata pencarian yang diinputkan di *web proxy*, sehingga *web proxy* tidak bisa melakukan pemblokiran terhadap isi atau content suatu halaman website hanya bisa memblok konten negatif.

5 SARAN

1. Di perlukan pengaturan atau penjadwalan untuk memblokir akses sosial media.

2. dalam pemblokiran ini harus banyak yang di kembangkan lebih jauh lagi sehingga tidak mengganggu koneksi internet di FT UIKA

DAFTAR PUSTAKA

[1]. Dwi Novia Lestari – 201243501151 DAN ILMU PENGETAHUAN ALAM UNIVERSITAS INDRAPRASTA PGRI 2013 ... Jakarta, 24 November 2013

[2]. Ilham efendi, Apa yanng di maksud dengan server, Pengertian server, jenis-jenis server, fungsi server, IT-Jurnal.com – 2018

[3]. Citraweb Solusi Teknologi,Blokir Website & File Extention Dengan Web Proxy PT Jalan Petung 31 Papringan Yogyakarta 55281 INDONESIA Telp:

[4]. Zainal A. Hasibuan, Ph.D metodologi penelitian pada bidang ilmu komputer dan teknologi informasi Depok, Agustus 2007

[5]. Hermawan Rudi (2015). ***Modul Network Security*.** Jakarta: G-Inova.

[6]. Rizky Agung, **Cara Memblokir Situs Menggunakan *Web Proxy* MikroTik,kumpulan tutorial mikrotik INDONESIA-2017**