BAB III
METODE PENELITIAN

3.1 Alat dan Bahan *(Hardware dan Software)*

Penelitian ini menggunakan beberapa peralatan dan bahan sebagai berikut:

A. Perangkat Keras (*Hardware*)

Perangkat keras (*hardware*) yang digunakan oleh dalam analisa dan penelitian ini adalah sebagai berikut:

1. Kabel UTP Cat 6 AMP
2. *Switch* dan *Hub D-Link*
3. Routerboard Mikrotik RB750
4. *PC Server HP* Proliant Gen9
5. Laptop/PC Core i3 sebanyak 5 uniy sebagai percobaan
6. *Access Point D-Link*

B. Perangkat Lunak (*Software*)

Perangkat lunak (*software*) yang digunakan oleh dalam analisa dan penelitian ini adalah sebagai berikut:

1. Winbox

   Winbox merupakan aplikasi *remote* yang dikeluarkan mikrotik sendiri yang berfungsi untuk mempermudah konfigurasi *remote* dengan tampilan *windows*.

2. Mikrotik OS

   Mikrotik *router OS*™ adalah sistem operasi berbasis linux yang digunakan untuk menjadikan *PC* berbasis *intel* atau *AMD* mampu melakukan beberapa fungsi di dalamnya yaitu *router, bridge, firewall*, pengaturan *bandwidth, wireless access point* atau *client* dan fungsi *networking* serta beberapa fungsi *server*, sehingga cocok untuk routing jaringan atau *internet* di perkantoran bahkan juga digunakan oleh ISP dan *provider hotspot*.

3. *Windows Operating System*

   Windows Operating System merupakan sistem operasi yang dilengkapi dengan antar muka pengguna grafis *(GUI)* dengan *desktop* yang

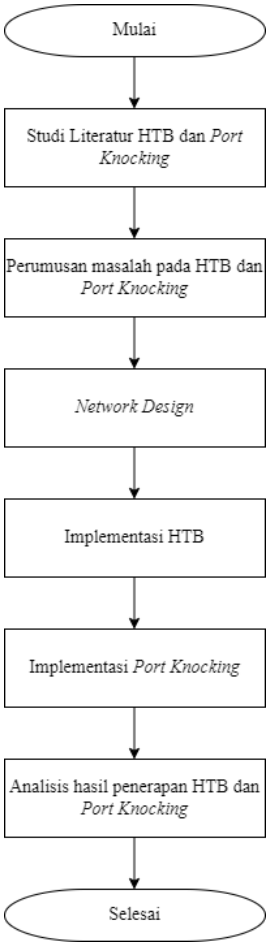
memungkinkan pengguna untuk melihat semua *file* dn *video*. Sistem operasi ini dirancag untuk berjalan pad perangkat keras x86 seperti *intel* dan *AMD*.

4. Aplikasi *Wireshark*

   Wireshark yaitu sebuah aplikasi *capture* paket data berbasis *open-source* yang berguna untuk memindai dan menangkap trafik data pada jaringan *internet*. Aplikasi ini umum digunakan sebagai alat *troubleshoot* pada jaringan yang bermasalah.

3.2 Alur Penelitian

Adapun alur penelitian terdiri dari beberapa tahap meliputi studi literatur *hierarchical token bucket* dan *port knocking*, perumusan masalah, *network design*, implementasi HTB, implementasi *port knocking*, dan analisis hasil penerapan HTB dan *port knocking* seperti ditunjukkan pada gambar 3.1.

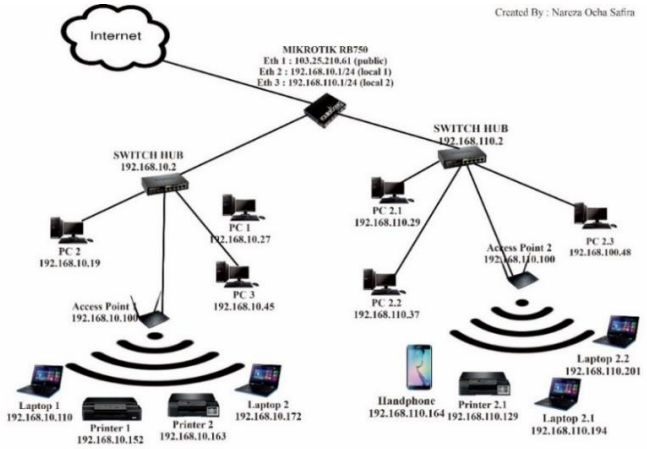


Gambar 3. 1 Diagram Alir Penelitian

Pada gambar 3.1 merupakan penjelasan yang sesuai dengan diagram alir penelitian, penelitian ini dilakukan dengan beberapa tahapan proses pengerjaan yaitu dari identifikasi masalah: melakukan beberapa identifikasi beberapa masalah dengan penelitian yaitu bagaimana melakukan manajemen bandwidth dan kemanan jaringan. Studi literatur: melakukan studi literatur yang berkaitan dengan penelitian yaitu dengan pencarian informasi topik yang berhubungan dengan penelitian manajemen *bandwidth* dan keamanan jaringan yang didapatkan dari jurnal, buku, dan *internet*. Selanjutnya analisis: melakukan analisis dari studi literatur yang telah dilakukan sehingga dapat mengetahui penelitian yang akan dilakukan. Desain: membuat konfigurasi atau perancangan jaringan sesuai dengan penelitian yang dilakukan dan nanti pada saat *maintenance* mudah dilakukan. Implementasi: tahap implementasi merupakan tahap paling penting dimana tahap ini menentukan berhasil tidaknya perancangan jaringan yang sudah dibuat sebelumnya. Menganalisis hasil: Analisa ini dilakukan untuk mengetahui tingkat kinerja dari sisi manajemen *bandwidth* dan keamanan jaringan yang telah dilakukan apakah metode yang diterapkan sudah berjalan dengan baik.

3.2.1 Perancangan Jaringan

Topologi jaringan yang umum digunakan saat ini merupakan jenis topologi *star extend*. *Access point* yang berfungsi sebagai *hotspot*, kabel *UTP* sebagai media transmisi yang menghubungkan seluruh komputer ke jaringan, *Hub* berfungsi juga sebagai *media internet* bagi pengguna *LAN* dan penghubung antara *server* ke jaringan. Berikut adalah analogi desain jaringan atau *network diagram* yang dapat dilihat pada gambar 3.2.



Gambar 3. 2 *Network Diagram*

Penelitian ini mengambil contoh penggunaan *Routerboard* Mikrotik *RB750* menjelaskan analogi perancangan jaringan. *Routerboard* Mikrotik bertindak sebagai pembagi koneksi ke jaringan LAN dan jaringan WLAN. Dalam tahap ini yang dilakukan adalah merancang desain topologi jaringan komputer, baik topologi fisik maupun topologi logis sesuai dengan ketersediaan teknologi yang ada. Penelitian ini melakukan desain terhadap sistem yang akan dibangun dengan tujuan memaksimalkan penggunaan *bandwidth* yang ada.

Pada desain jaringan penelitian ini melakukan perancangan sebuah *router* mikrotik untuk diletakkan diantara *access point* dan *switch* utama yang difungsikan sebagai *gateway*, *firewall*, dan *bandwidth controller*. Berikut adalah tabel pembagian alamat IP pada jaringan menggunakan mikrotik yang dapat digambarkan pada tabel 3.1.

Tabel 3. 1 *Pembagian Kelas IP*

Alat	*Inter face*	*IP*	*Subnet mask*	*Gateway*	Keterangan
Mikro tik RB 750	*Eth 1*	103.25.210.61	255.255.255.0	103.25.210.61	*Internet Public*
	Eth 2	192.168.10.1/24	255.255.255.0	192.168.10.1	*Kelas Lan 10*
	Eth 3	192.168.110.18/24	255.255.255.0	192.168.110.1	*Kelas Lan 110*
	Access Point 1	192.168.10.100/24	255.255.255.0	192.168.10.100	*WLAN 10*
	Access Point 2	192.168.110.100/24	255.255.255.0	192.168.110.100	*WLAN 110*

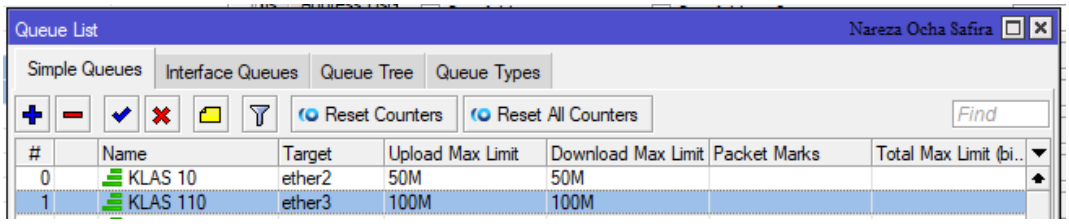
Keterangan pembagian alamat IP pada tabel 3.1:

1. *Eth1 IP* 103.25.210.61 adalah *IP* yang diterima dari *ISP Internet* yang masuk ke Mikrotik.
2. *Eth 2* menggunakan IP 192.168.10.1/24 adalah pembagian IP untuk *switch hub* yang nanti akan di sebut dengan *Kelas 10.* Yang nanti semua yang terhubung dengan *switch hub* ini akan mendapatkan IP dengan range 192.168.10.2 – 192.168.10.255.
3. *Eth 3* menggunakan IP 192.168.110.1/24 adalah IP yang di setting di mikrotik untuk switch hub yang nanti di sebut dengan Kelas 110. Dan *client* yang nanti terhubung dengan switch hub tersebut akan mendapatkan *IP* di *range* 192.168.110.2 – 192.168.110.255.

4. *Access Point 1* mendapatkan IP 192.168.10.100 karena terhubung dengan *switch hub* yang keluar dari mikrotik *Interface 1 (eth 1)*. Namun *client* yang nanti terhubung dengan *access point* tersebut akan mendapatkan range IP 192.168.10.101 – 192.168.10.255. Dikarenakan *gateway* yang terpasang di *access point* tersebut adalah 192.168.10.100.
5. *Access Point 1* mendapatkan IP 192.168.110.100 karena terhubung dengan *switch hub* yang keluar dari mikrotik *Interface 1 (eth 2)*. Namun *client* yang nanti terhubung dengan access point tersebut akan mendapatkan *range IP* 192.168.110.101 – 192.168.110.255. Dikarenakan *gateway* yang terpasang di *access point* tersebut adalah 192.168.110.

3.2.2 Penerapan Metode *Hierarchical Token Bucket*

Pada dasarnya semua r*outerboard* mikrotik sudah menggunakan *Hierarchical Token Bucket (HTB).* Penelitian ini mengambil contoh penerapan *Hierarchical Token Bucket (HTB)* yang sudah dilakukan di salah satu Badan Usaha Milik Daerah Perumdam Tirta Satria. Di Perumdam Tirta Satria memiliki alokasi *bandwidth* dari *Internet Service Provider* sebesar 150*Mbps*. Namun dari bagian Teknologi Informasi nya memberi *limit* kepada *client* atau *user* secara keseluruhan dalam penggunaan nya sesuai dengan prioritas dan bagian seperti gambar 3.3 berikut.

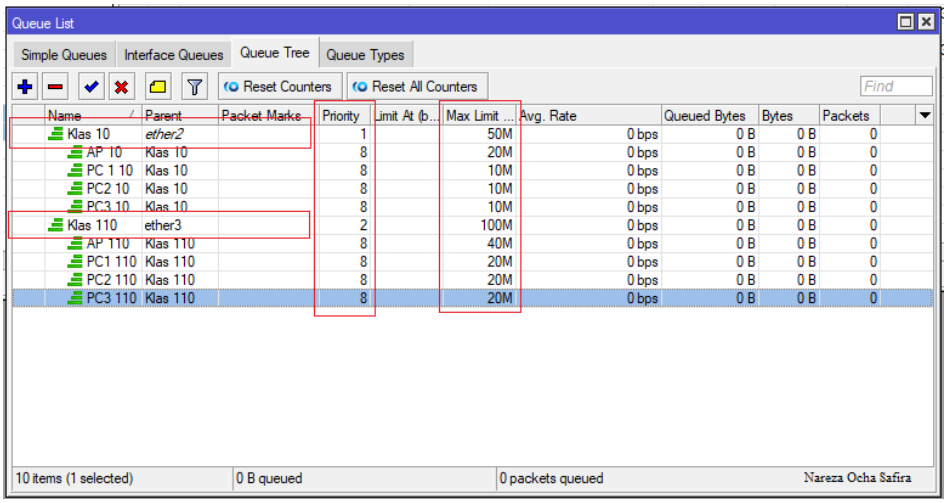


Gambar 3. 3 Penerapan *HTB*

Berdasarkan gambar 3.3 menjelaskan bahwa dari Bagian Teknologi Informasi Perumdam Tirta Satria menerapkan metode *Hierarchical Token Bucket* untuk pembagian koneksi pada klas 110 adalah Maksimal 100*Mbps*. Dan alokasi bandwidth untuk klas 10 adalah sebesar 50*Mbps*.

Penerapan metode *Hierarchical Token Bucket* pada *client* atau *user* yang sudah di tentukan prioritasnya dengan membuat *parent queue* yang dapat dilihat pada gambar 3.4 dimana *Max-Limit* yang merupakan angka dari MIR (*Maximum*

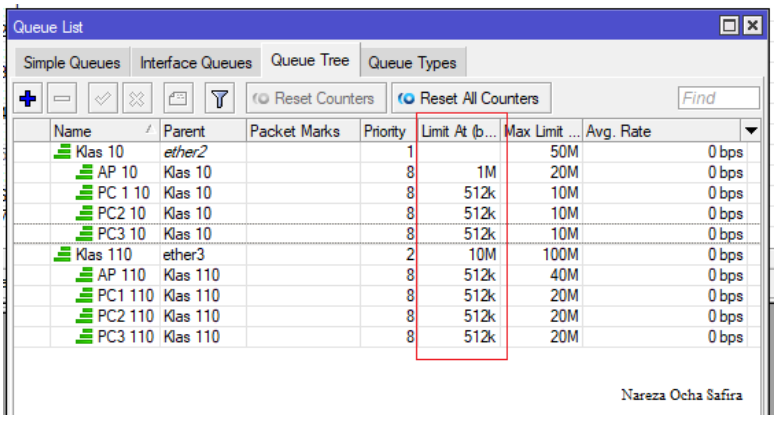
Information Rate), kecepatan maksimum yang mungkin didapatkan saat jaringan **tidak sibuk** berdasarkan prioritas *user* yang sudah ditentukan seperti gambar 3.4.



Gambar 3. 4 Penerapan *parent queue* dan *max limit*

Dalam penerapan metode *Hierarchical Token Bucket* perlu memasang parameter *max-limit* pada *parent queue*, barulah prioritas pada *client* akan berjalan.

Selain itu perlu dilakukan penerapan nilai *limit-at* yang merupakan angka dari CIR (*Committed Information Rate*), angka yang menunjukkan *bandwidth* yang akan didapatkan saat jaringan **paling sibuk** pada masing-masing *client*. Nilai *limit-at* ini adalah kecepatan *minimal* yang akan di dapatkan oleh *client*, dan tidak akan terganggu oleh *client* lainnya, seberapa besarpun *client* lainnya mengambil *bandwidth*, ataupun berapapun prioritasnya seperti gambar 3.5.



Gambar 3. 5 Penerapan *limit-at*

Dari penjelasan gambar 3.5 dapat dijabarkan sebagai berikut :

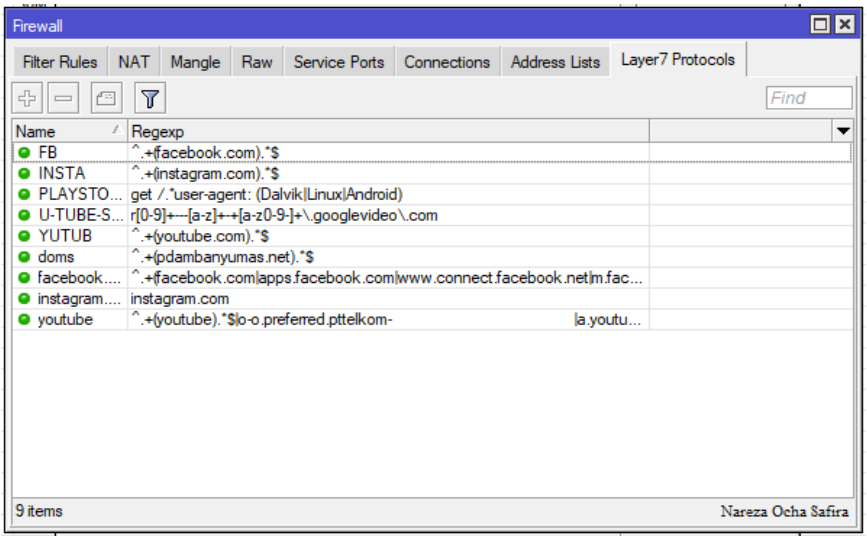
a. *User / Client* yang berada di klas IP address 192.168.10.0/24 memiliki maksimal koneksi 50*Mbps* dan *user/client* yang berada di *range* klas *IP address* 192.168.110.0/24 adalah sebesar 100*Mbps.*
b. Klas 10 merupakan prioritas pertama dalam mendapatkan *bandwidth* yang diaolikasikan sebesar 50*Mbps* dan Klas 110 menjadi prioritas kedua dengan alokasi *bandwidth* sebesar 100*Mbps* dari 150 yang tersedia.
c. Masing – masing *user/client* mendapatkan *limit-at* yang merupakan angka dari *Committed Information Rate* (CIR), angka yang menunjukkan *bandwidth* yang akan didapatkan saat jaringan **paling sibuk** pada masing-masing *client*.
d. Dan masing – masing *user/client* mendapatkan *Max-Limit* yang merupakan angka dari *Maximum Information Rate* (MIR), kecepatan maksimum yang mungkin didapatkan saat jaringan **tidak sibuk** berdasarkan *parent queue* yang sudah di tetapkan dengan rincian seperti gambar 3.5.

3.2.3 Penerapan *Port Knocking* dan *Port Blocking*

Port Knocking adalah metode yang dilakukan untuk membuka akses ke *port* tertentu yang telah di*block* oleh *firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Dengan cara ini, perangkat jaringan seperti *router* akan lebih aman, sebab *admin* jaringan bisa melakukan *blocking* terhadap *port-port* yang telah ditentukan seperti winbox (tcp 8291), SSH (tcp 22), *Telnet* (tcp 23) atau webfig (tcp 80). Penelitian ini mengambil contoh penerapan metode *port knocking* dan *port blocking* di Perumda Tirta Satria yang sudah di terapkan oleh Bagian Teknologi Informasi.

Dalam hal ini Perumdam Tirta Satria menerapkan aturan bahwa selama dalam jam kerja, *user/client* tidak boleh mengakses *social media* yang dilarang seperti *Facebook*, *Instagram* ataupun *Youtube*. Dikarenakan dalam hal tersebut dapat mengganggu fokus kerja karyawan. Oleh karena itu Bagian IT Perumdam Tirta Satria menerapkan metode *port knocking* dan *port blocking* terhadap jaringan lokal agar user/client yang sudah di tentukan tidak dapat mengakses *social media* yang dilarang.

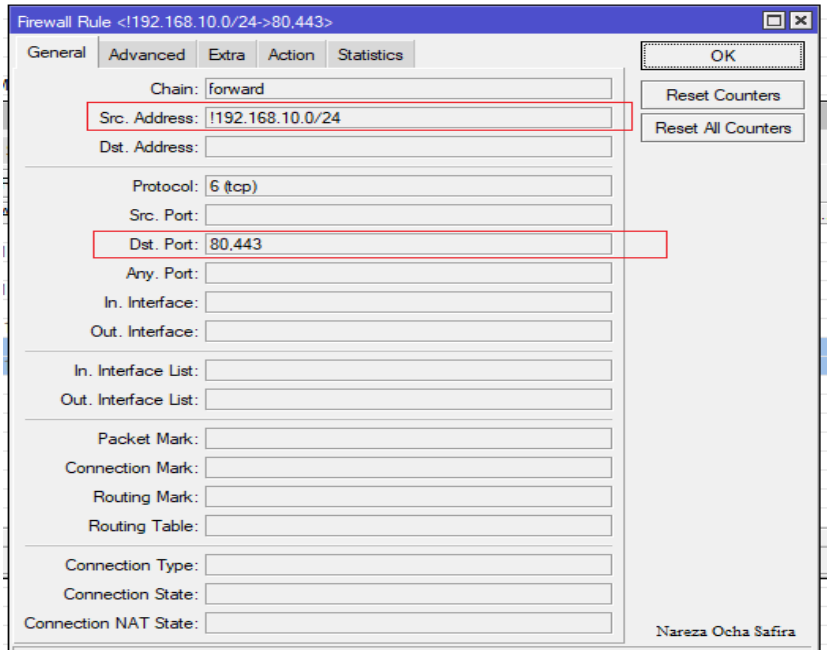
Untuk dapat menerapkan metode *port knocking* sederhana, dapat memanfaatkan *Layer7 Protocol* pada *Router*. Fitur *Layer7 Protocol* dapat digunakan untuk melakukan pengelompokan / *grouping* yang selanjutnya group tersebut dapat digunakan pada fitur lain seperti *Firewall Filter, NAT* atau *Mangle*. *Layer7 Protocol* dapat ditambahkan secara *manual* ataupun secara *dynamic*. Penambahan secara *manual* dapat dilakukan pada menu ***IP -> Firewall -> Layer7 Protocol***. Yang nanti nya akan muncul tampilan seperti gambar 3.6.



Gambar 3. 6 *layer7 protocols*

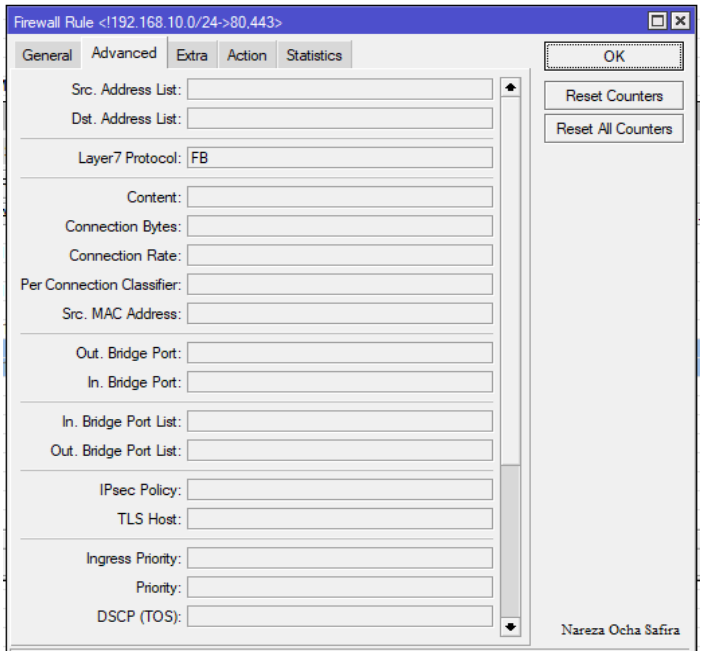
Contoh gambar 3.6 *setting* ***Simple Port Knocking*** inilah, akan digunakan *Layer7 protocols* tersebut. Bagian IT Perumdam Tirta Satria memilih menggunakan *Layer7 Protocols* dalam penerapan port blocking karena *Layer7 Protocol* adalah metode pencarian pola terhadap paket data yang melewati jalur ICMP, TCP dan UDP. Firewall layer 7 merupakan firewall yang sangat bagus dan komples dibandingkan firewall – firewall lain yang ada pada mikrotik. Penerapan *port blocking* pada layer 7 protokol menggunakan firewall filter. Jadi dengan penggunaan fitur tersebut tidak perlu lagi menentukan satu per satu port mana saja yang harus di block. Hal tersebut juga meminimalisir user/client yang berusaha mengakses situ tersebut menggunakan aplikasi pihak ke 3.

Untuk alasan sekuritas maka pengujian ini tidak dapat menampilkan konfigurasi atau settingan *Firewall* yang berada di Mikrotik Perumdam Tirta Satria secara banyak



Gambar 3. 7 *Src Address*

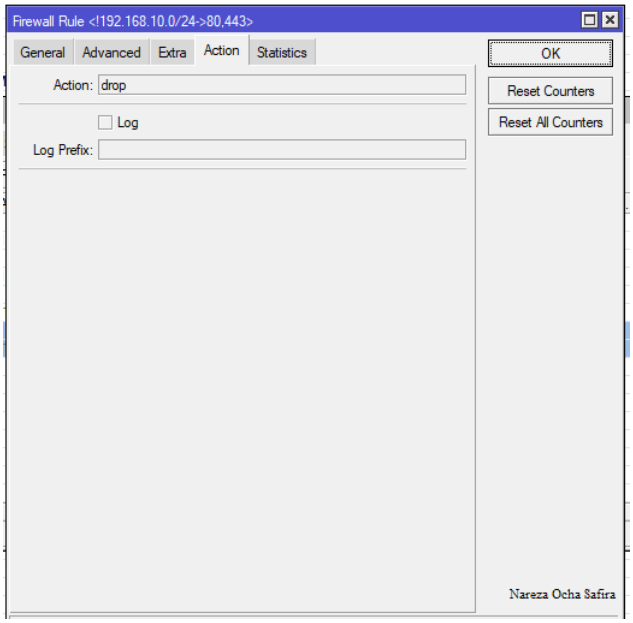
Berdasarkan gambar 3.7 dapat dijelaskan bahwa, dari Bagian Teknologi Informasi Perumdam Tirta Satria menerapkan metode *Port Knocking* pada Klas IP 192.168.10.0/24 pada *port* 80 dan *port* 443 dalam melakukan akses ke *Facebook*.



Gambar 3. 8 Penerapan *Port knocking*

Berdasarkan gambar 3.8 tersebut juga dapat dilihat bahwa metode *Port Blocking* juga berlaku pada IP **selain** klas IP 192.168.10.0/24 karena ada logika

NOT (!) pada *Scr. Address* (ip tujuan) nya. Hal tersebut dikarenakan adanya *action* ***drop*** pada *tab action firewall* mikrotik tersebut seperti gambar 3.9.



Gambar 3. 9 *Action drop*