BAB III

METODOLOGI PENELITIAN

3.1 PERANGKAT YANG DIGUNAKAN

Perangkat yang digunakan dalam penelitian ini terdiri dari dua bagian, yaitu perangkat keras *(Hardware)* dan perangkat lunak *(Software)*.

3.1.1 Perangkat Keras *(Hardware)*

Perangkat keras yang dibutuhkan yaitu sebuah laptop serta satu buah *routerboard* mikrotik sebagai media untuk merealisasikan sistem yang akan dibangun dan dua buah laptop yang digunakan untuk melakukan serangan *DoS* dan *Brute Force*. Untuk spesifikasi perangkat keras (*Hardware)* yang digunakan ditunjukkan pada Tabel 3.1 yang akan digunakan untuk media dalam membangun sistem jaringan, sementara pada Tabel 3.2 spesifikasi perangkat keras laptop yang akan digunakan untuk serangan *Denial of Service* (DoS), dan pada Tabel 3.3 adalah spesifikasi dari perangkat *routerboard* mikrotik.

Tabel 3.1 Spesifikasi Perangkat Keras *(Hardware)* Laptop

OS	Windows 10
Processor	7th Gen AMD® APU FX^{TM}-9830P, *Clook Speed* 3.0 GHz – 3.7 GHz
RAM	8GB DDR4 2133MHz *up to* 16GB *(Dual Channel Support)*
Harddisk	500 GB

Tabel 3.2 Spesifikasi Perangkat Keras *(Hardware)* Laptop untuk serangan DoS

OS	Windows 10
Processor	Intel Core i5-3320M 2.6 GHz
RAM	4 GB
Harddisk	500 GB

Tabel 3.3 Spesifikasi Perangkat Keras *(Hardware) Mikrotik Router Board RB941-2nD (hAP-Lite)*

OS	RouterOS
CPU	QCA9531-BL3A-R 650MHz
Main Storage	16 MB
RAM	32 MB
LAN *Ports*	4
Dimentions	113x89x28mm

3.1.2 Perangkat Lunak *(Software)*

Berikut untuk perangkat lunak yang digunakan dalam penelitian ini berserta dengan spesifikasinya: (gambar di hapus)

A. *Winbox* versi 6.48.6 (*long-term*)

Software yang digunakan untuk *remote router* mikrotik pada penelitian ini yaitu *winbox* versi 6.48.6 yang mempunyai kegunaan untuk me-*remote* sebuah mikrotik kedalam *mode Graphical User Interface* (GUI) melalui *operating system windows*. Kebanyakan teknisi melakukan konfigurasi mikrotik os atau mikrotik routerboard menggunakan winbox dibandingkan dengan konfigurasi langsung lewat *mode Command Line Interface* (CLI), hal ini dikarenakan dalam menggunakan winbox dirasa lebih mudah dan simple dibandingkan melalui browser dan hasilnya pun juga lebih cepat.

B. *Wireshark*

Wireshark adalah 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, selain itu juga biasa digunakan untuk pengujian *software* karena kemampuannya untuk membaca konten dari tiap paket trafik data. *Wireshark* berguna untuk pekerjaan analisis jaringan. Cara kerjanya yaitu dengan ‘menangkap’ paket-paket data dari protokol-protokol yang berbeda dari berbagai tipe jaringan yang umum ditemukan di dalam trafik jaringan internet. Paket-

paket data tersebut ‘ditangkap’ lalu ditampilkan di jendela hasil *capture* secara *real-time*.

C. *Low Orbit Ion Cannon (LOIC)*

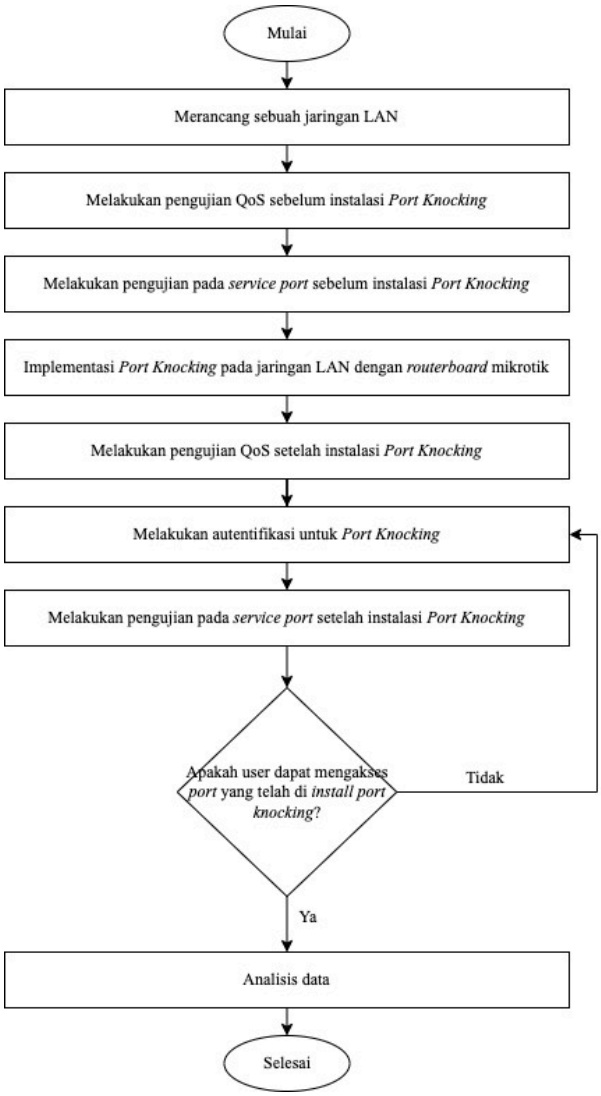
Low Orbit Ion Cannon (LOIC) merupakan aplikasi pengujian layanan dan penolakan layanan sumber terbuka yang ditulis dalam C#. *Low Orbit Ion Cannon* melakukan serangan *Denial of Service* (DoS) atau *Distributed Denial of Service* (DDoS) yang ditujukan pada situs target dengan membanjiri server dengan paket TCP, UDP, atau HTTP pada suatu sistem sehingga mengakibatkan sistem *overload* dan tidak dapat diakses atau dengan kata lain bertujuan untuk mengganggu layanan *host* tertentu.

D. *Network Mapper (NMAP)*

Network Mapper atau yang dapat disebut dengan NMAP merupakan sebuah *tool* yang bersifat *open source*. NMAP memiliki peran penting dalam audit dan juga eksplorasi yang berkaitan dengan keamanan jaringan. Fungsi utama NMAP adalah mengecek dan memeriksa sebuah jaringan. Pengecekan oleh NMAP dapat dilakukan sekalipun pada jaringan yang besar dan kurun waktu yang singkat, selain itu fungsi NMAP juga berfungsi untuk melakukan *scanning* pada *port* jaringan. *Port* itu sendiri merupakan nomor yang digunakan dalam membedakan aplikasi satu dengan yang lainnya yang ada dalam satu jaringan komputer. Dengan fungsi *scanning* pada masing – masing *port* dapat mengetahui aplikasi apa saja yang sudah terpasang pada suatu perangkat.

3.2 ALUR PENGUJIAN

Penelitian dijalankan secara bertahap berdasarkan *flowchart,* dimana tahapan penelitian terdiri dari perancangan sistem yang terdiri dari instalasi *Winbox*, *Wireshark*, dan *Low Orbit Ion Cannon (LOIC)* tahap pembuatan jaringan, tahap pengujian, implementasi *Port Knocking* dan yang terakhir adalah melakukan analisis dan menarik kesimpulan.



Gambar 3.1 *Flowchart* Pengujian

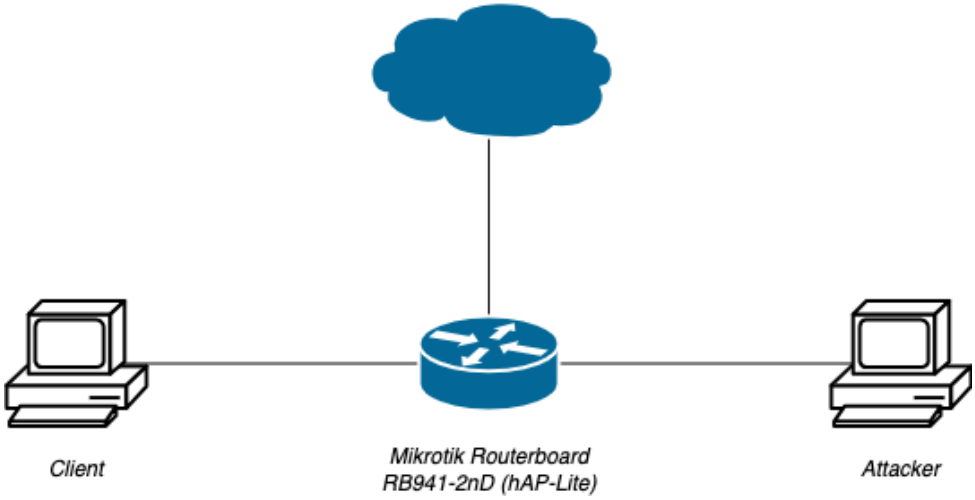
Flowchart pada Gambar 3.1 dimulai dengan melakukan instalasi *software winbox*, *wireshark*, *Low Orbit Ion Cannon (LOIC),* dan *Netwok Mapper (NMAP)* selanjutnya untuk perancangan jaringan LAN dengan menggunakan beberapa perangkat yaitu kabel LAN, laptop dan *Routerboard* Mikrotik.

Alur selanjutnya adalah tahap melakukan pengujian QoS sebelum instalasi *port knocking* untuk parameter QoS-nya terdiri dari *throughtput, packet loss, delay* dan *jitter*, seletah itu dilakukan pengujian pada *service port* sebelum instalasi *port knocking*. Pada tahap selanjutnya yaitu melakukan implementasi *port knocking* pada jaringan LAN dengan *routerboard* mikrotik, melakukan pengujian QoS serta autentifikasi untuk

port knocking dan pengujian pada *service port* setelah dilakukan instalasi *port knocking.* Tahap berikutnya yaitu tahap yang paling penting di mana tahap ini menentukan berhasil atau tidaknya perancangan jaringan yang sudah dibuat sebelumnya, pada tahap ini jika penerapan *port knocking* berhasil maka akan diberi akses untuk mengakses *port* 8291, *port* 80, dan *port* 23 sementara jika dalam penerapan metoda *port knocking* gagal maka tidak diizinkan untuk mengakses *port* 8291, *port* 80, dan *port* 23 akan melakukan *looping* pada alur autentifikasi untuk *port knocking.*

Tahap terakhir yaitu melakukan analisis dan menarik kesimpulan, analisis dilakukan untuk mengetahui tingkat kinerja dari sisi keamanan jaringan yang telah dilakukan apakah metoda yang diterapkan sudah berjalan dengan baik.

3.3 TOPOLOGI JARINGAN

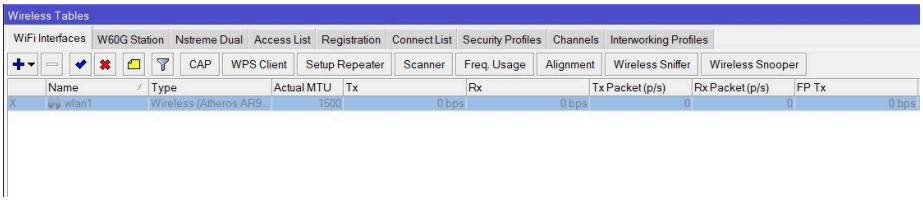


Gambar 3.2 Topologi Jaringan

Pada Gambar 3.2 merupakan topologi yang akan digunakan dalam penelitian ini, topologi jaringan yang digunakan pada penelitian ini terdiri dari 2, PC *client* digunakan untuk *remote* serta melakukan simulasi pengujian data IP pada *client* adalah 10.10.10.2, selanjutnya PC attacker digunakan untuk melakukan serangan dengan IP 10.10.10.3, dan 1 *routerboard mikrotik* digunakan untuk membangun sistem keamanan jaringan mikrotik, pada perancangan sistem dilakukan dengan menambahkan pengamanan pada mikrotik dengan menutup *port* yang terbuka dengan menambahkan metode *port knocking* untuk mengakses

router, dalam menentukan alamat IP yang akan dipakai ada beberapa *rules* yang harus diterapkan melalui aplikasi *winbox* agar bisa terhubung ke internet, yaitu:

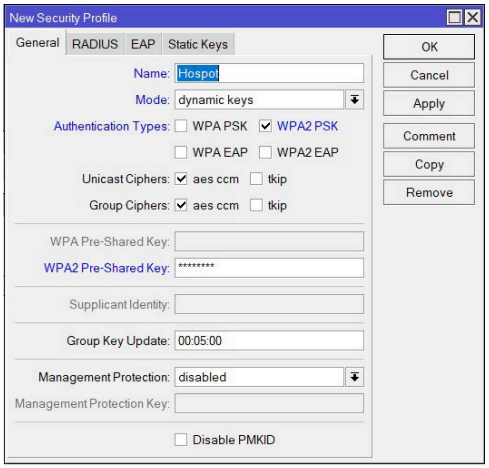
A. Mengaktifkan *Wireless*



Gambar 3.3 Mengaktifkan *Wireless*

Pada Gambar 3.3 ini dilakukan jika konfigurasi *wireless* yang masih *default* atau masih dalam keadaan mati, maka langkah yang dilakukan penulis dalam mengaktifkannya, masuk ke halaman utama mikrotik dibagian *menu wireless* terdapat *tab interface*, setelah itu penulis memilih *wireless* yang ada di *list* dan mengaktifkan tanda *check list* biru untuk mengaktifkannya.

B. *Security Profiles*

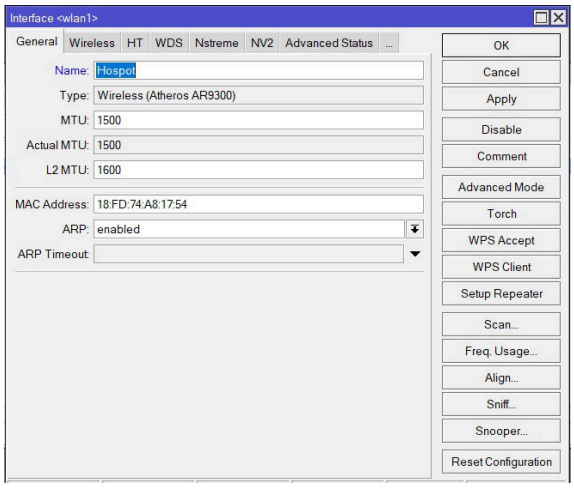


Gambar 3.4 *Security Profile*

Selanjutnya pada Gambar 3.4 merupakan *security profile* yang mana *wifi* akan dihubungkan menggunakan *password*, dimana penulis menambahkan sebuah konfigurasi untuk membuka *password* dengan melakukan berbagai cara yaitu pada halaman *wireless* dibagian *tab security profile* penulis mengaktifkan tanda + biru untuk menambahkan.

Kemudian pada halaman *security profiles* di bagian *tab general* penulis mengisikan kolom-kolom yang tertera pada Gambar 3.4.

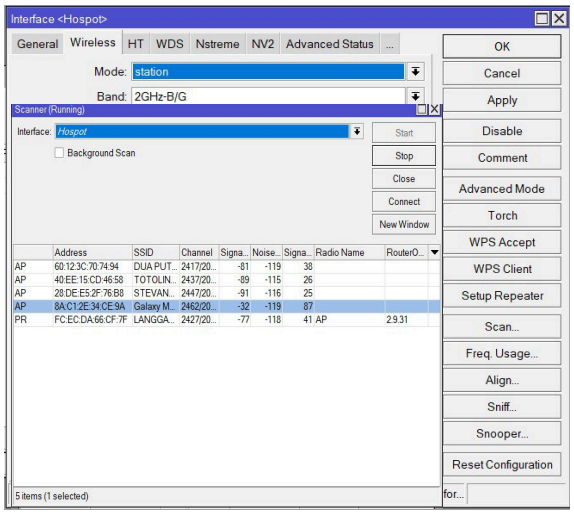
C. Konfigurasi *Wireless*



Gambar 3.5 Konfigurasi *Wireless*

Pada Gambar 3.5 jika *wireless* sudah aktif, langkah selanjutnya kembali ke *tab interface* lalu *double klik wireless*, dan di *tab general* ubah kolom *name* yang tadinya wlan1 menjadi nama untuk *interface wlan* sesuai dengan keinginan kita, konfigurasi ini bertujuan untuk merubah nama *interface wlan* saja yang nantinya akan mempermudah kita di konfigurasi-konfigurasi selanjutnya, langkah ini optional bisa dilakukan dan bisa juga tidak.

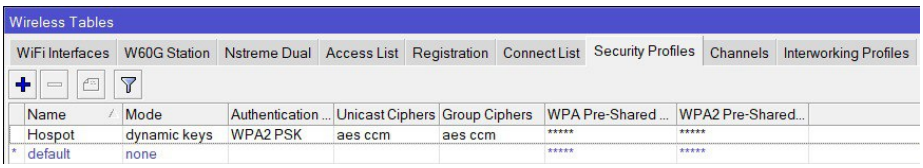
D. *Scan Wifi*



Gambar 3.6 *Scan WiFi*

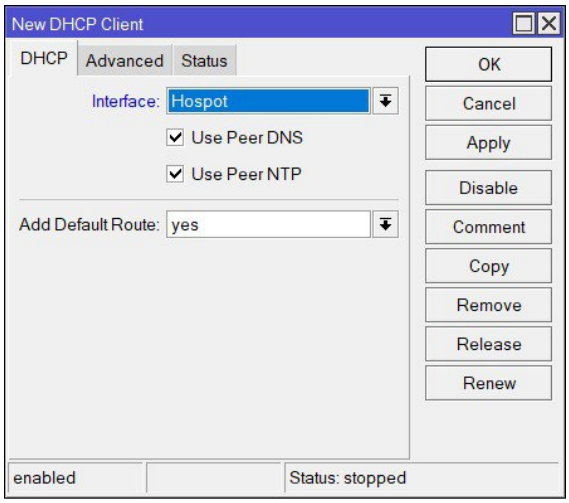
Pada *tab interface* dibagian *wireless*, penulis menghubungkan *wireless* mikrotik dengan jaringan *wifi* yang ada disekitar, dimana yang dilakukan penulis adalah merubah *wireless* menjadi *station,* selanjutnya terdapat opsi *navigasi scan*. Sehingga akan muncul tampilan baru, pada halaman *scanner* penulis mengisi kolom *interface* dengan nama *interface hospot*, penulis melalukan perintah *start* sehingga mikrotik akan melakukan *scan* terhadap sinyal *wifi* yang ada disekitarnya yang akan menampilkan hasilnya dibawah seperti yang tertera pada Gambar 3.6, jika hasil scannya sudah muncul, selanjutnya penulis memilih *wifi* yang akan digunakan kemudian penulis akan melakukan konektivitas pada perintah *connect*.

E. Konfigurasi IP – DHCP *Client*



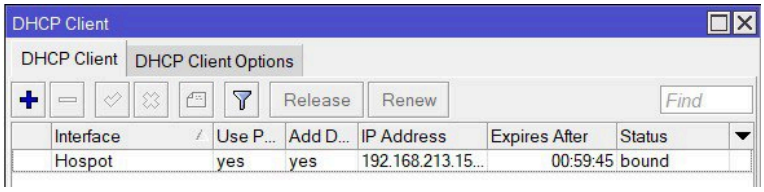
Gambar 3.7 Konfigurasi IP – DHCP *Client* (1)

Karena penulis tidak tahu IP yang digunakan, untuk menghubungkan dengan internet, maka akan menambahkan konfigurasi DHCP *Client*, dimana mikrotik nantinya akan mendapatkan IP secara otomatis dari *wifi* yang teleh terhubung. Pada *menu* IP dibagian DHCP *Client* penulis mengaktifkan tanda + untuk menambahkan seperti yang tertera pada Gambar 3.7.



Gambar 3.8 Konfigurasi IP – DHCP *Client* (2)

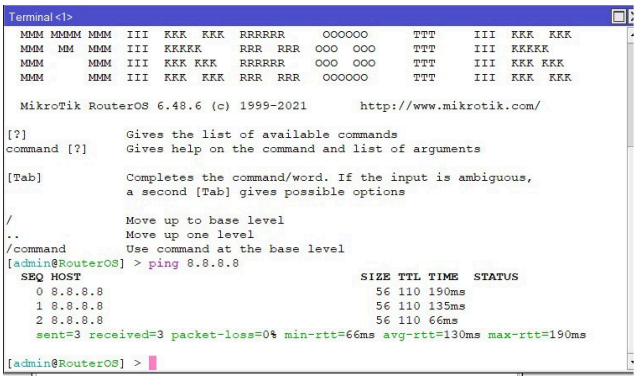
Di bagian halaman *New* DHCP *Client*, pada kolom *interface* penulis memilih *interface* dengan nama yang sudah ditentukan sebelumnya dan tandai *Use Peer* DNS dan *Use Peer* NTP, jika semua sudah memberikan perintah OK, seperti yang tertera pada Gambar 3.8.



Gambar 3.9 Konfigurasi IP – DHCP *Client* (3)

Jika statusnya sudah *bound* maka mikrotik sudah mendapatkan IP, maka konfigurasi *wireless station* sudah berhasil contohnya seperti pada Gambar 3.9.

F. *Ping*

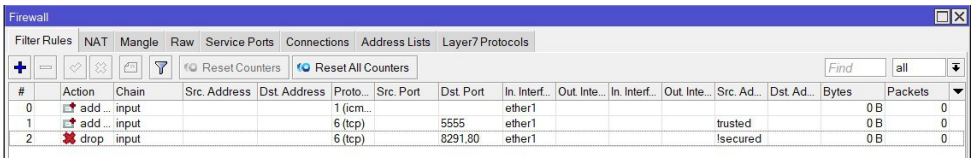


Gambar 3.10 *Test PING*

Pada Gambar 3.10 merupakan langkah terakhir yaitu menguji konektifitas, apakah sudah terhubung dengan internet atau belum terhubung caranya yaitu dengan menuliskan *script* "*ping* 8.8.8.8".

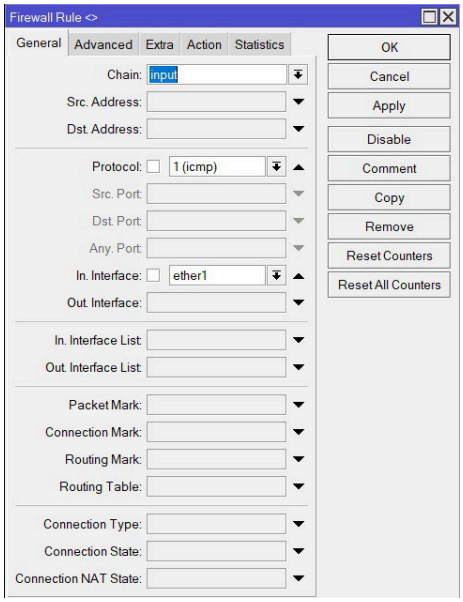
3.4 PENERAPAN *PORT KNOCKING*

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, pada penelitian ini penulis akan menggunakan *port* seperti *winbox* (8291), dan *webfig* (80).

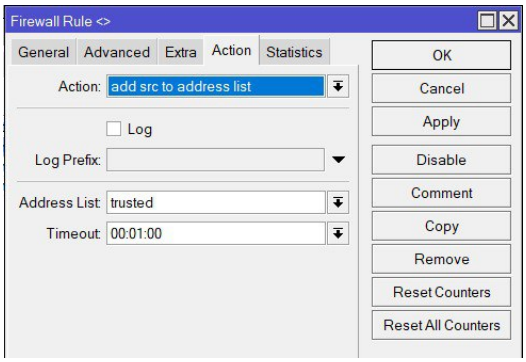


Gambar 3.11 *Rules* Penelitian

Pada Gambar 3.11 merupakan rules penelitian yang akan dilakukan, untuk rules yang akan diuji coba diantaranya, *rules* identifikasi alamat IP yang ingin mengakses mikrotik, *rules Port Knocking* 5555, dan *rules drop.*

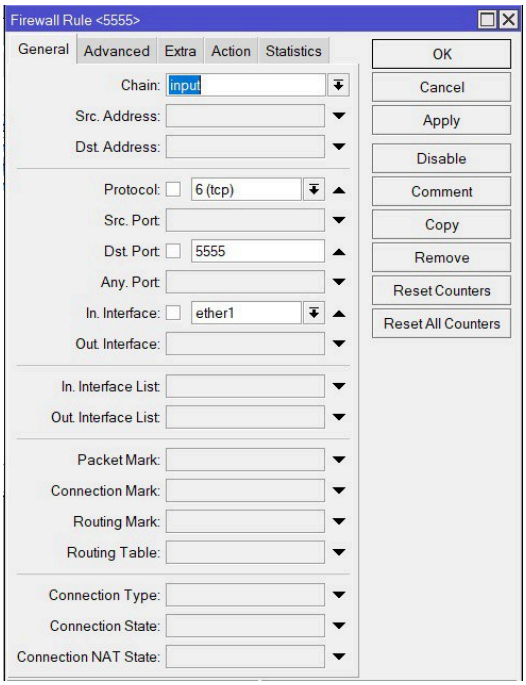


Gambar 3.12 *Rules* Identifikasi Alamat IP (1)

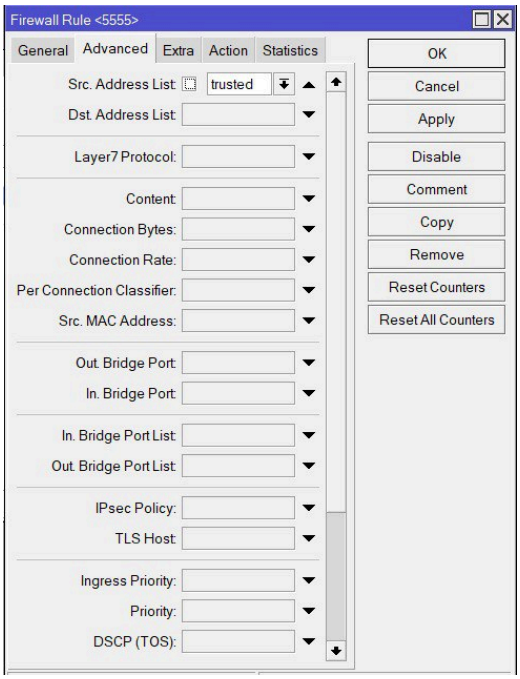


Gambar 3.13 *Rules* Identifikasi Alamat IP (2)

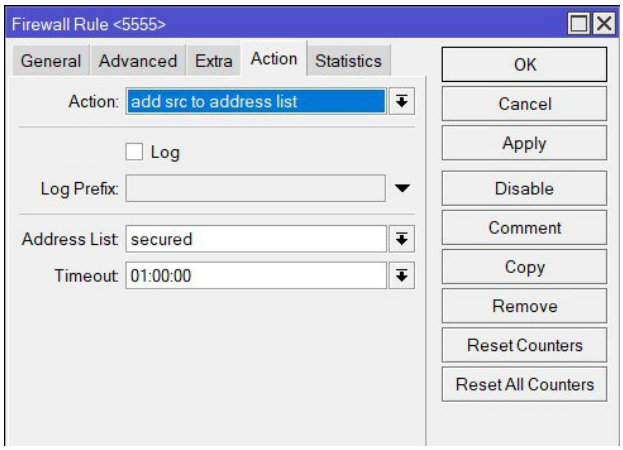
Untuk Gambar 3.12 menjelaskan apabila ada seseorang melakukan *remote* ke mikrotik dengan *protocol icmp*, dimana untuk *input interface*-nya adalah *ether* 1. *Rules* ini akan memasukkan alamat IP tersebut ke dalam *address list trusted* dengan *timeout* yang diberikan selama 1 menit seperti pada gambar 3.13, yang akan diberikan akses menuju *rules* yang kedua.



Gambar 3.14 *Rules Port Knocking* 5555 (1)

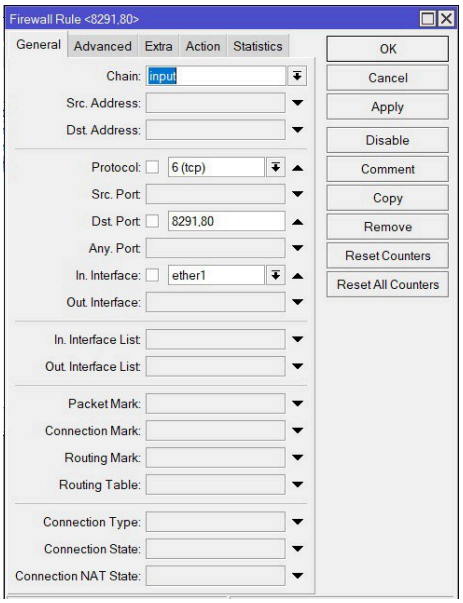


Gambar 3.15 *Rules Port Knocking* 5555 (2)

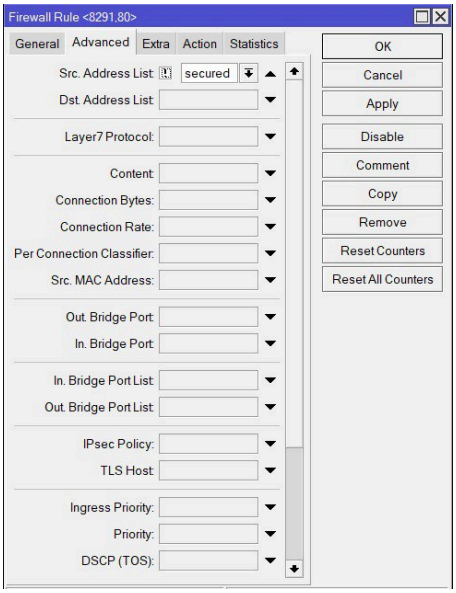


Gambar 3.16 *Rules Port Knocking* 5555 (3)

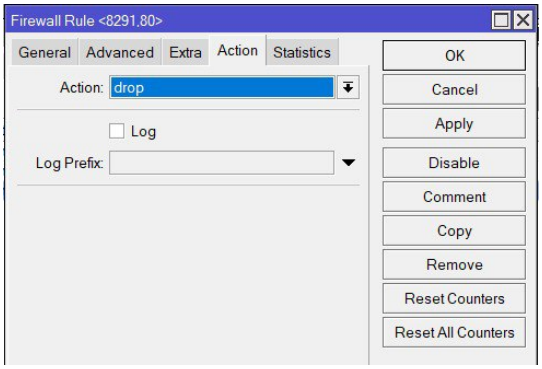
Pada Gambar 3.14 menjelaskan untuk *rules port knocking* 5555 dengan *protocol tcp* dan *input interface ether* 1, mempunyai fungsi sebagai tanda pengenal apabila ada alamat IP yang ingin mengakses ke dalam mikrotik yang sudah terdaftar pada *source address list trusted* yang tertera pada Gambar 3.15, maka orang tersebut harus mengetuk *port* 5555 terlebih dahulu untuk dapat dikenali oleh mikrotik dan dimasukan ke dalam *address list* dengan nama *secured* dan akan diberikan *timeout* selama 60 menit seperti yang tertera pada Gambar 3.16.



Gambar 3.17 *Rules Drop* (1)



Gambar 3.18 *Rules Drop* (2)



Gambar 3.19 *Rules Drop* (3)

Pada *rules* terakhir yang tertera pada Gambar 3.17 menjelaskan apabila ada alamat IP yang ingin mengakses ke dalam mikrotik dengan dengan *protocol tcp*, lalu mengakses salah satu *port* misalnya *winbox* (8291), atau *webfig* (80), dengan input interface ether 1, sementara pada Gambar 3.18 menjelaskan jika ternyata alamat *IP* tersebut tidak termasuk ke dalam *source address list secured*, maka alamat *IP* tersebut akan di *drop* seperti pada penjelasan Gambar 3.19, akan tetapi apabila IP tersebut masuk ke dalam *source address list secured* dan berhasil melakukan *rules port knocking* maka untuk alamat *IP* tersebut akan diberikan izin mengakses ke *winbox* (8291), atau *webfig* (80).