Job Sheet 5 - Mikrotik Firewall Filter Rules

1. Tujuan Praktikum / Capaian Pembelajaran Sub- Mata Kuliah (CPSMK)

- Mampu Melakukan konfigurasi serta Implementasi Firewall Filter Rules Chain Input, Output , Forward pada jaringan komputer

2. Referensi Terkait

1. I Putu Agus Eka Pratama Handbook Jaringan Komputer 'Teori Praktek berbasis open source ' Informatika Bandung 2014
2. Niall Mansfield, Practical TCP/IP Linux & Windows 1-2 , Andi Offset 2002
3. Rendra Towidjojo , Panduan Router Mikrotik #1-2-3 , Jasakom
4. Rendra Towidjojo, Konsep & Implementasi Routing dengan Router Mikrotik Jasakom
5. https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter

3. Dasar Teori / Informasi Pendukung

Firewall merupakan kombinasi perangkat keras [hardware] & perangkat lunak [software] dengan tujuan :

1. Untuk mengatur dan mengawasi lalu lintas paket data dalam jaringan komputer
2. Sebagai sistem keamanan untuk mengelola serta memantau trafik masuk dan keluar berdasarkan aturan keamanan (security rules) yang sudah ditentukan.
3. Mencegah akses yang tidak diinginkan dari atau ke dalam jaringan atau server

Pada *Firewall* Mikrotik terdapat Firewall Filter Rules untuk mengatur suatu kebijakan pada firewall serta mengatur trafik lalu lintas paket data dalam jaringan, berikut adalah beberapa aturan yang digunakan pada *Firewall filter rule*

- ✓ Menentukan paket data apa saja yang bisa masuk atau keluar dari jaringan tersebut
- ✓ Menentukan paket data mana yang akan diterima [*Accept*] atau dibuat [*Drop*] / ditolak [*Reject*]
- ✓ Firewall akan memeriksa *packet header* dari sebuah *IP Packet*, yang diperiksa adalah :
- ✓ Header -- > *IP Address* Pengirim [src-address], IP address tujuan [*dst-address*], jenis protokol, port pengirim [*src-port*], port tujuan [*dst-port*]
- ✓ Beberapa firewall juga melakukan pemeriksaan pada isi data yang dikirim [layer 7 *firewall*

Firewall bekerja sesuai dengan rule/aturan firewall.

- ✓ Untuk memeriksa *IP Packet*, maka paket yang masuk ke dalam firewall akan dicocokan dengan kesesuaian rule terhadap lalu lintas packet data [kondisi]
- ✓ Selanjutnya firewall akan menentukan tindakan yang akan dilakukan [action], apakah nantinya akan di terima [accept] atau dibuang/ditolak [drop/reject]
- ✓ Untuk melakukan konfigurasi firewall, harus terlebih dahulu diketahui asal packet dan tujuan packet
- ✓ Kesalahan dalam menentukan asal dan tujuan packet menjadikan filter terhadap packet tidak berfungsi
- ✓ Mikrotik firewall filtering dikelompokkan dalam chain, dengan mencocokkan pada satu kriteria dalam satu chain.

4. Perlengkapan/Alat & Bahan

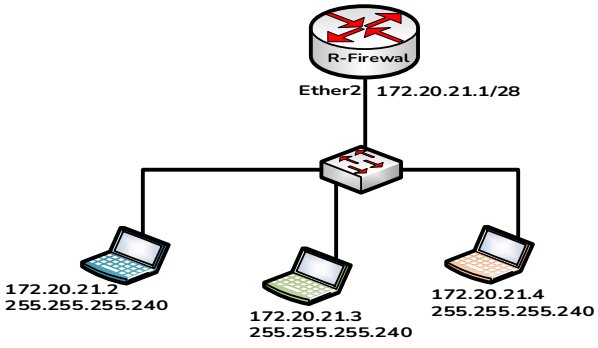
- ✓ Mikrotik - **RB951-2n/ RB750/ RB941-2nD/ RB952Ui-5ac2nD** 1 Unit
- ✓ Komputer PC / Laptop 3 Unit
- ✓ Kabel UTP / Patch Cord UTP Cat 5e 2/3 Meter 4 Set
- ✓ Utility Aplikasi : Winbox Ver 3.x.x / Telnet
- ✓ Switch unmanageable 1 Unit

5. Keselamatan Kerja

- ✓ Menggunakan peralatan lab & bahan praktikum sesuai fungsi serta petunjuk penggunaan
- ✓ Setelah menggunakan komputer/Notebook harus melakukan shutdown sesuai prosedur
- ✓ Sesuaikan pasangan power adaptor dengan perangkat router / switch yang akan digunakan

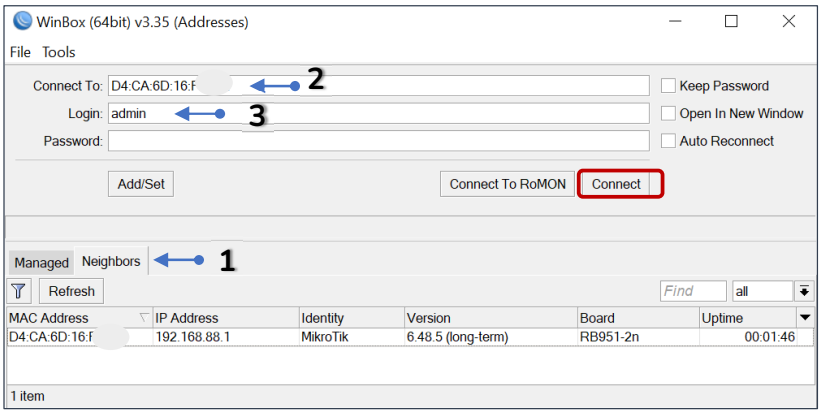
6. Langkah/Prosedur Kerja

A. Topologi konfigurasi Firewall Filter Rules



Koneksi Router Mikrotik & Komputer / Notebook

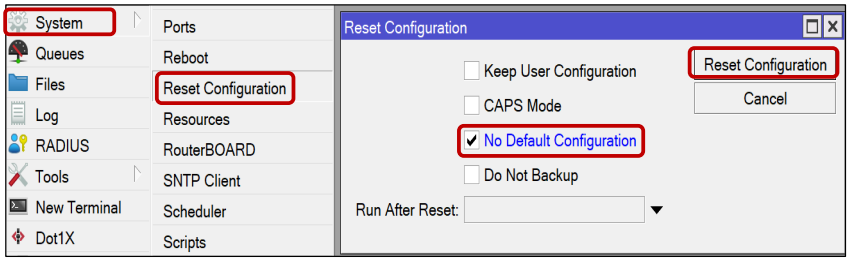
1. Aktifkan Aplikasi Winbox [pastikan aplikasi winbox sudah tersedia / diinstall di komputer/notebook, jika belum download pada link berikut : https://mikrotik.com/download.
2. Aktifkan / jalankan aplikasi winbox pada komputer/notebook, jika komputer sudah terkoneksi dengan baik ke Router akan tampil aplikasi program seperti gambar berikut :



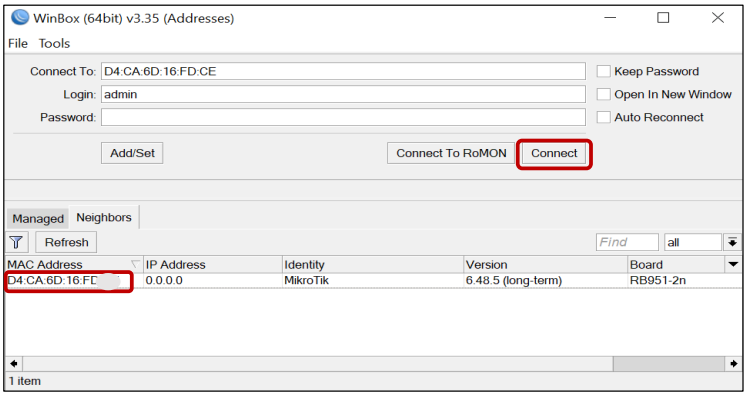
Setup Default Router/ Reset Router No Default Configuration

1. Pilih Menu Aplikasi winbox pada [Managed & Neighbors], pilihan **Neighbors** untuk menampilkan router yang terhubung ke jaringan perangkat komputer/notebook
2. Pada isian informasi Connect To : akan ditampikan pilihkan akses ke router [menggunakan MAC Address atau IP Address] pilih akses menggunakan **MAC Address**
3. Pada isian informasi Login : akan ditampikan secara default user login MikroTik adalah **admin**
4. Untuk isian informasi Password : isian password default mikrotik adalah kosong / blank

Setelah login dengan Winbox pastikan seluruh konfigurasi router dalam kondisi kosong, untuk itu pada Menu Winbox pilih Menu **System** sub menu **Reset Configuration** pada pilihan **√ No Default Configuration** lakukan centang dan pilih tombol **Reset Configuration [Untuk semua Router]**

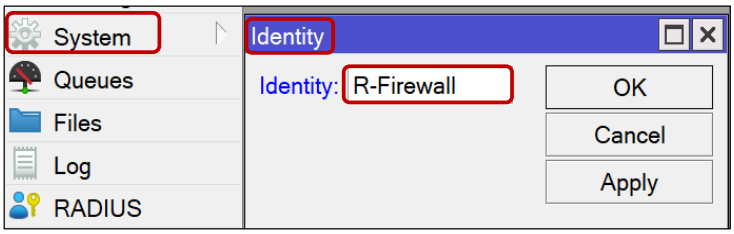


Tahapan selanjut akses kembali router seperti gambar berikut , dengan memilih tombol **Connect** [sesuai dengan tampilan informasi router pada menu **Neighbors**]



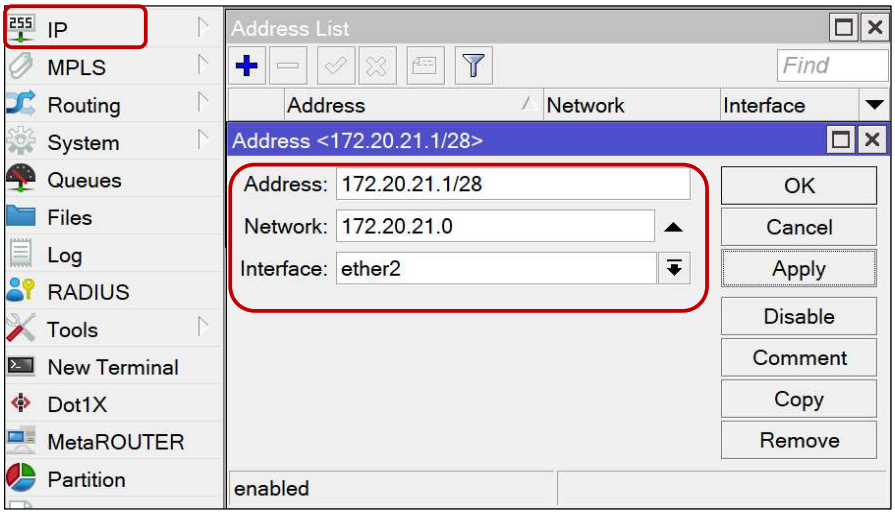
Set Identitas Router System Mikrotik

Set Identitas dengan memilih Menu System sub menu Identity , selanjutnya akan tampil nama router Default "**Mikrotik**", ganti dengan **R-Firewall,** seperti gambar berikut dilanjutkan dengan memilih tombol **OK**

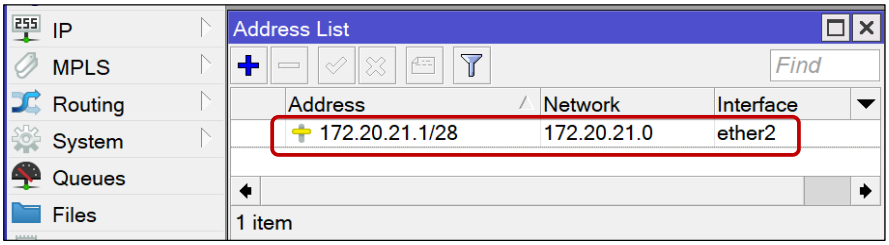


Menambahkan IP Address pada Interface Ether2 & Ether3

Untuk menambahkan IP Address pada interface, dapat dilakukan pada menu **IP** sub menu **Addresses,** selanjutnya akan tampil informasi address list, pilih icon **+** untuk menambahkan IP Address dan pilih Interface Ether2 dan pilih tombol **OK** seperti gambar berikut

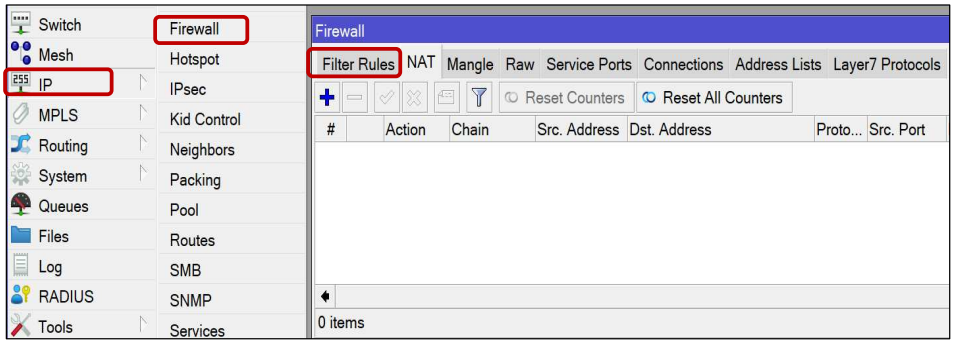


Setelah ditambahkan IP Address untuk Interface Ether2 dan Ether3, untuk menampilkan IP dan Interface yang telah dibuat dapat dilihat pada Menu **IP** Sub Menu **Address** seperti berikut

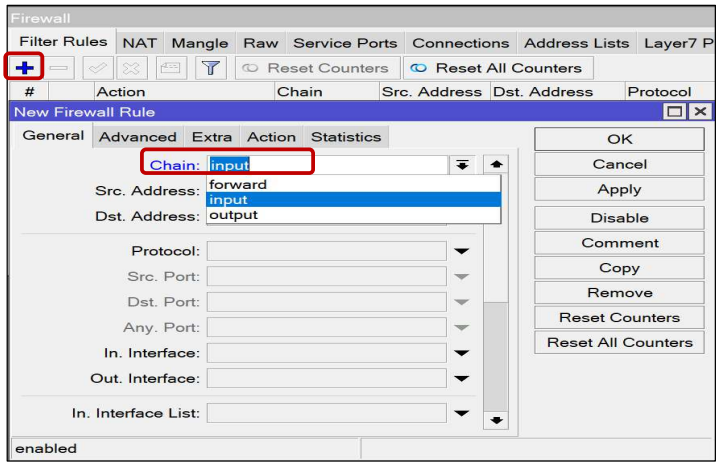


Setup Firewall Filter Rule Chain Input -Accept

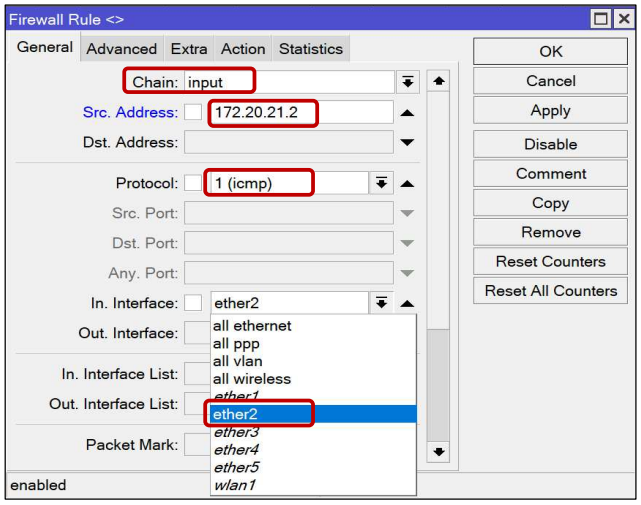
Untuk melakukan konfigurasi firewall filter rule dapat dilakukan dengan memilih Menu **IP** sub menu **Firewall**, selanjutnya pilih **Filter Rules** seperti gambar berikut :



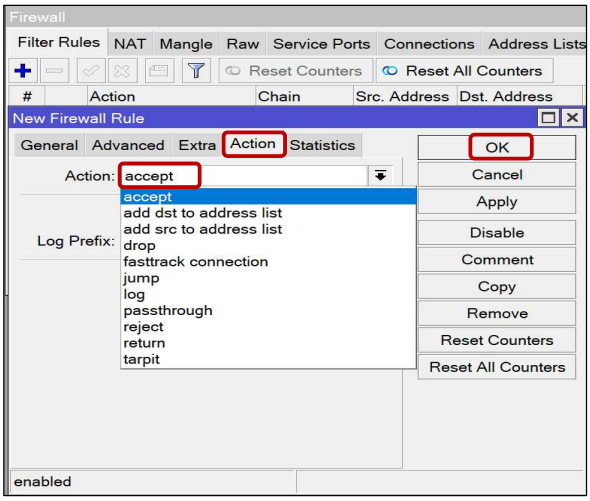
Tahapan selanjutnya pada Menu **Filter Rules** pilh Icon **+ ,** pada Tab Menu General Pilihan **Chain** pilih **Input** seperti gambar berikut



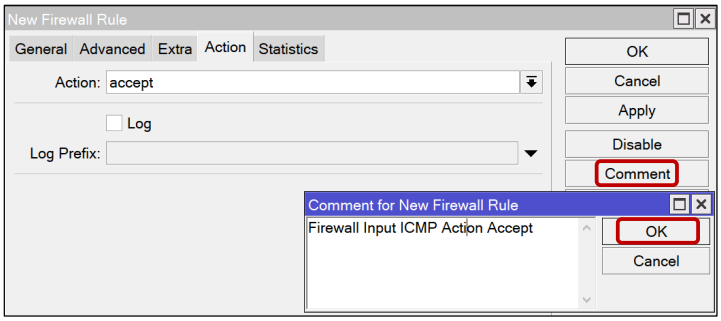
Setelah memilih **chain input** , selanjutnya adalah menambahkan source Address dengan IP **172.20.21.2** [IP Komputer/Notebook yang menuju / terhubung ke router **R-Firewall**] dan pilih protocol yang akan di filter yaitu **ICMP**, serta memilih input interface pada pilihan in.Interface, pada topologi Firewall Filter Rules komputer yang terhubung dengan Router melalui interface Ether2, pilih **Ether2** pada pilihan **in.Interface,** seperti pada gambar berikut



Tahapan selanjutnya pilih pada Tab Menu **Action ,** pada pilihan Action pilih **Accept** untuk mengizinkan IP pada **Src.Address** dan pilih tombol **OK,** seperti pada gambar berikut

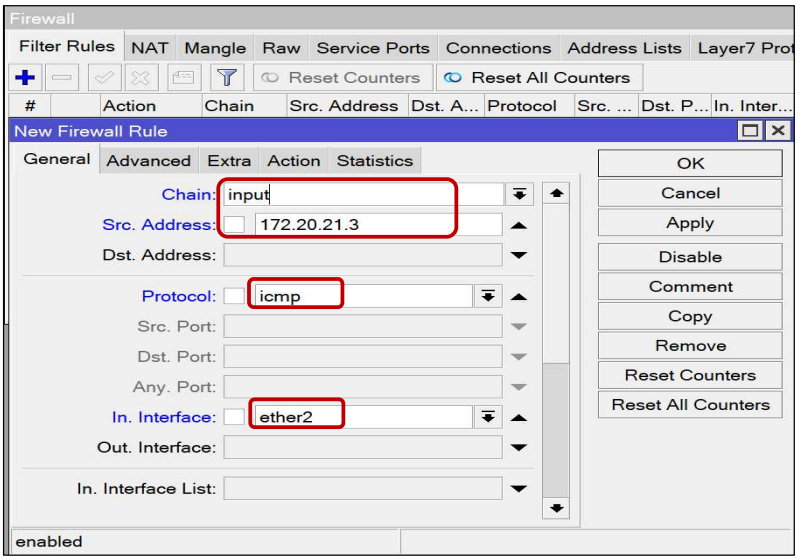


untuk memudahkan bagi network administrator mengetahui informasi setup Firewall Filter rules yang telah dilakukan, tambahkan **Comment** pada Tab Action Pilihan Tombol **Comment** dan memilih/klik tombol **OK** seperti gambar berikut

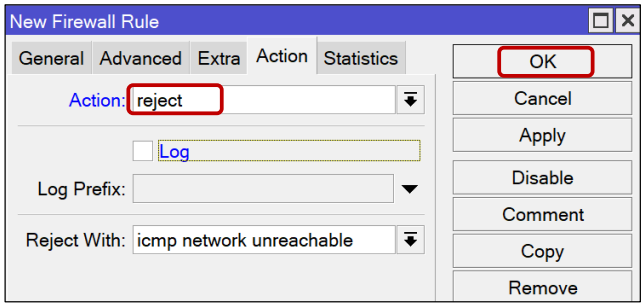


Setup Firewall Filter Rule Chain Input -Reject

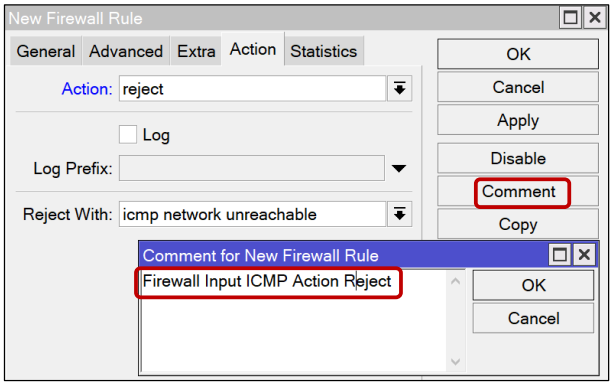
Untuk melakukan konfigurasi firewall filter rule Chain Input Reject Menu **Filter Rules** pilh Icon **+ ,** pada Tab Menu General Pilihan **Chain** pilih **Input** selanjutnya menambahkan source Address dengan IP **172.20.21.3** [IP Komputer/Notebook yang menuju / terhubung ke router **R-Firewall**] dan pilih protocol yang akan di filter yaitu **ICMP**, serta memilih input interface pada pilihan in.Interface sesuai topologi Firewall Filter Rules komputer yang terhubung dengan Router melalui interface **Ether2**, pilih **Ether2** pada pilihan **in.Interface,** seperti pada gambar berikut :



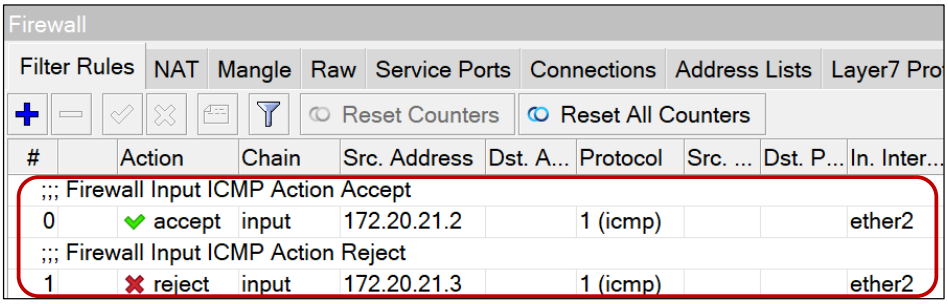
Tahapan selanjutnya pilih pada Tab Menu **Action ,** pada pilihan Action pilih **Reject** untuk menolak IP pada isian **Src.Address** untuk melakukan ping dan pilih tombol **OK,** seperti pada gambar berikut



untuk memudahkan bagi network administrator mengetahui informasi setup Firewall Filter rules yang telah dilakukan, tambahkan **Comment** pada Tab Action Pilihan Tombol **Comment** dan memilih/klik tombol **OK** seperti gambar berikut

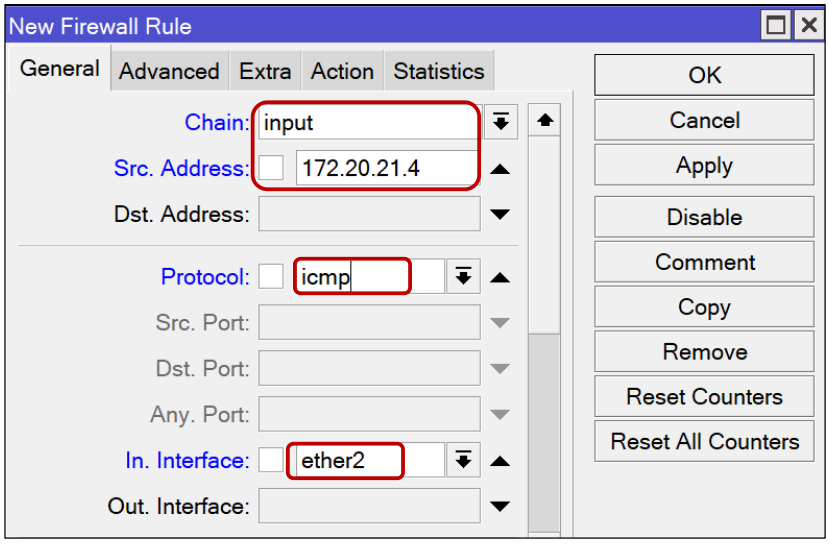


Untuk menampilkan Fiilter Rule yang telah dilakukan pilih Filter Rules seperti gambar berikut

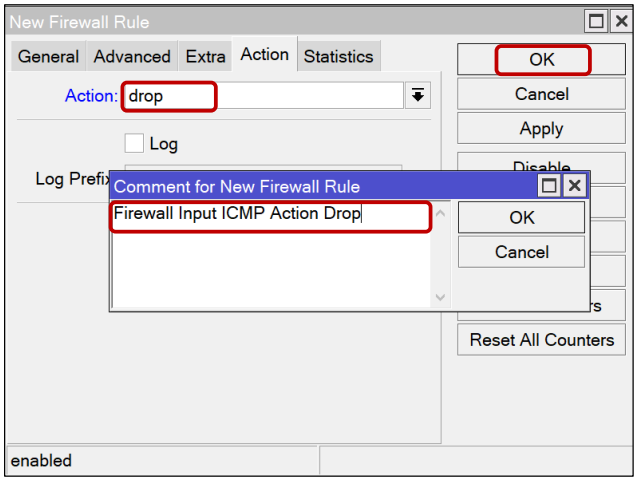


Setup Firewall Filter Rule Chain Input -Drop

Untuk melakukan konfigurasi firewall filter rule Chain Input Reject Menu **Filter Rules** pilh Icon **+ ,** pada Tab Menu General Pilihan **Chain** pilih **Input** selanjutnya menambahkan source Address dengan IP **172.20.21.3** [IP Komputer/Notebook yang menuju / terhubung ke router **R-Firewall**] dan pilih protocol yang akan di filter yaitu **ICMP**, serta memilih input interface pada pilihan in.Interface sesuai topologi Firewall Filter Rules komputer yang terhubung dengan Router melalui interface **Ether2**, pilih **Ether2** pada pilihan **in.Interface,** seperti pada gambar berikut :

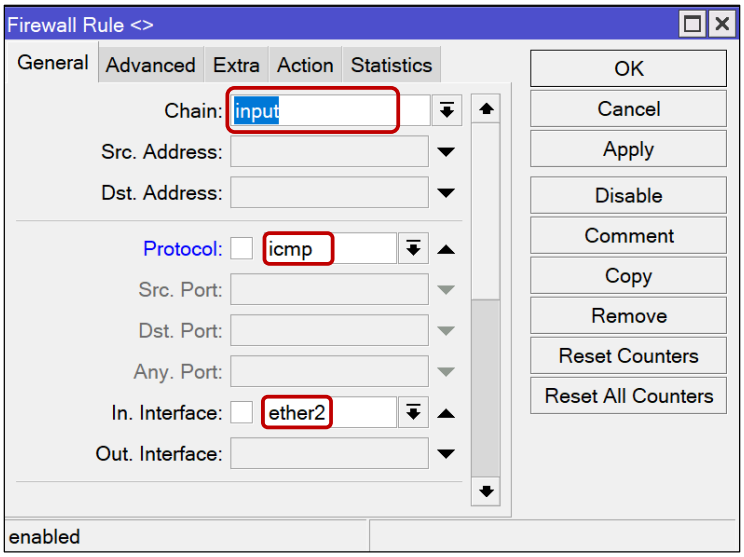


Tahapan selanjutnya pilih pada Tab Menu **Action** , pada pilihan Action pilih **Drop** untuk menolak IP pada isian **Src.Address** untuk melakukan ping, tambahkan **Comment** dan pilih tombol **OK,** seperti pada gambar berikut

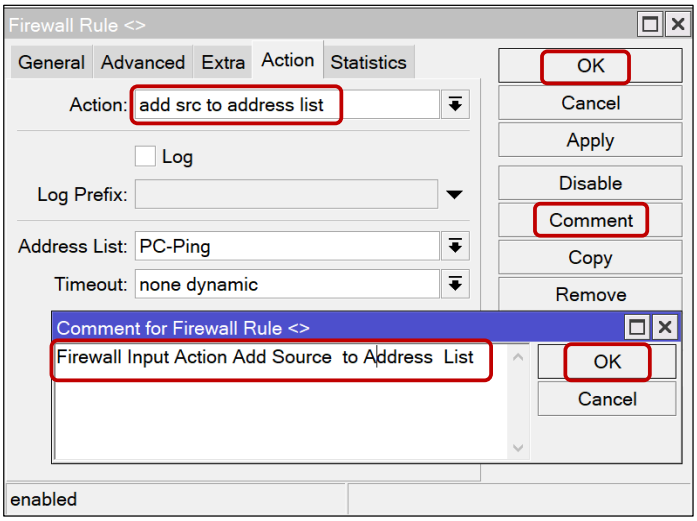


Setup Firewall Filter Rule Chain Input – add src to Address List

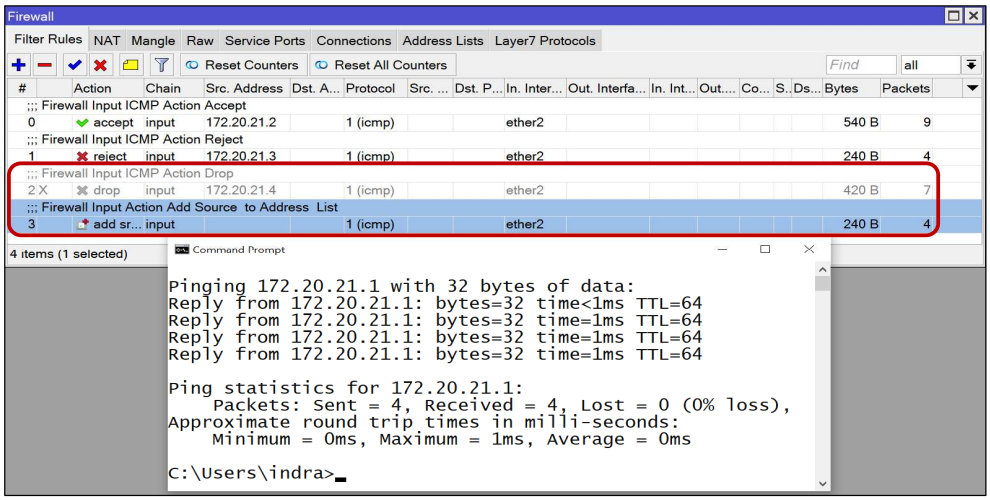
Untuk melakukan konfigurasi firewall filter rule Chain Input **add src to Address List** pilih Menu **Filter Rules** pilh Icon **+ ,** pada Tab Menu General Pilihan **Chain** pilih **Input** dan pilih protocol yang akan di filter yaitu **ICMP**, serta memilih input interface pada pilihan in.Interface dengan **Ether2** pada pilihan **in.Interface,** seperti pada gambar berikut :



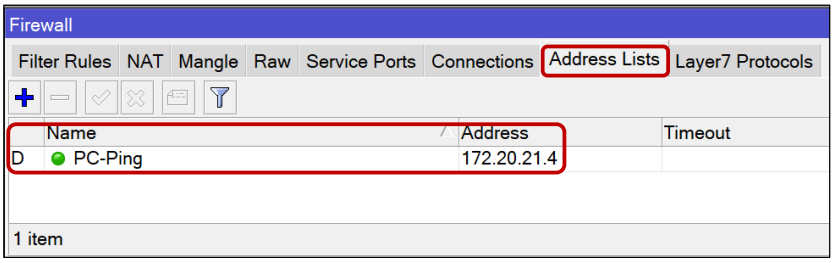
Tahapan selanjutnya pilih pada Tab Menu **Action ,** pada pilihan Action pilih **add src to address list** untuk nantinya akan ditambahkan pada address list dengan nama **PC-Ping**, sehingga setiap IP Address pada komputer yang melakukan ping akan ditambahkan pada address list, selanjutnya tuliskan nama address list PC-Ping, tambahkan **Comment** dan pilih tombol **OK,** seperti pada gambar berikut



Tahapan selanjutnya melakukan pengujian terhadap Action **add src to address list , dari komputer/notebook lakukan ping ke IP 172.20.21.1 [Ether2** Router **R-Firewall],** pada jobsheet ini karena dilakukan ping dari IP komputer **172.20.20.4** pastikan status action filter rule yang telah dilakukan sebelumnya [Action Drop] dinonaktikan terlebih dahulu **[disable]** dengan memilih baris script rule firewall index No. 2 **pilih Icon X [disable] seperti gambar berikut :**

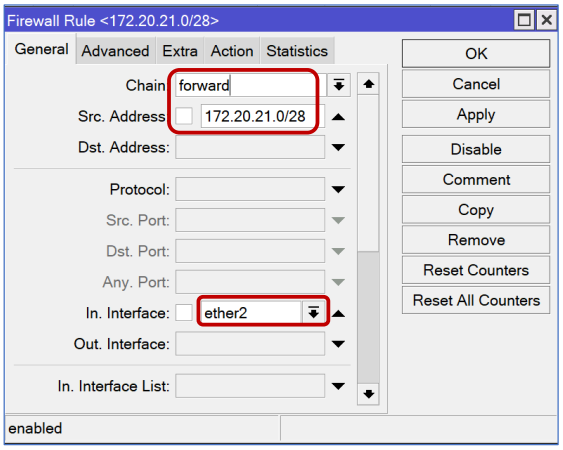


Selanjut pilih Tab Menu Addres List pada Firewall, maka akan ditampilkan IP Address dan komputer yang melakukan Ping , seperti pada gambar berikut :

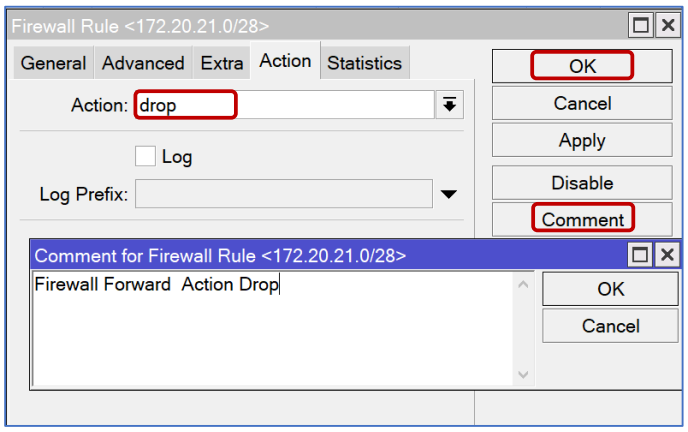


Setup Firewall Filter Rule Chain Forward -Drop

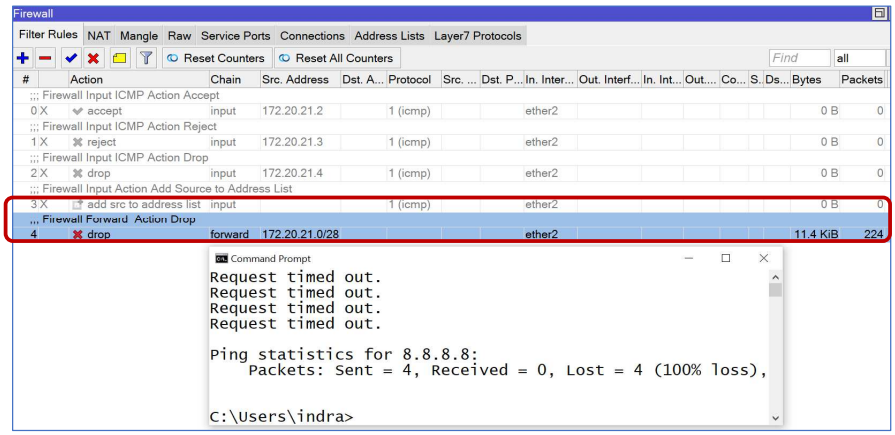
Untuk melakukan konfigurasi firewall filter rule Chain **Forward** Drop pada Menu **Filter Rules** pilh Icon **+ ,** pada Tab Menu General Pilihan **Chain** pilih **Forward** selanjutnya menambahkan source Address dengan IP **172.20.21.0/28** [IP Network pada interface Ether2 router **R-Firewall** terhubung ke Komputer/Notebook] serta memilih input interface pada pilihan **in.Interface** sesuai topologi Firewall Filter Rules komputer yang terhubung dengan Router melalui interface **Ether2**, pilih **Ether2** pada pilihan **in.Interface,** seperti pada gambar berikut :



Tahapan selanjutnya pada Tab Menu **Action** , pilihan Action pilih **drop, dengan tujuan untuk melakukan blok terhadap IP Network 172.20.21.0/28** sehingga tidak dapat diteruskan dari router **R-Firewall** untuk keluar dari router, selanjutnya tuliskan tambahkan **Comment** dan pilih tombol **OK,** seperti pada gambar berikut

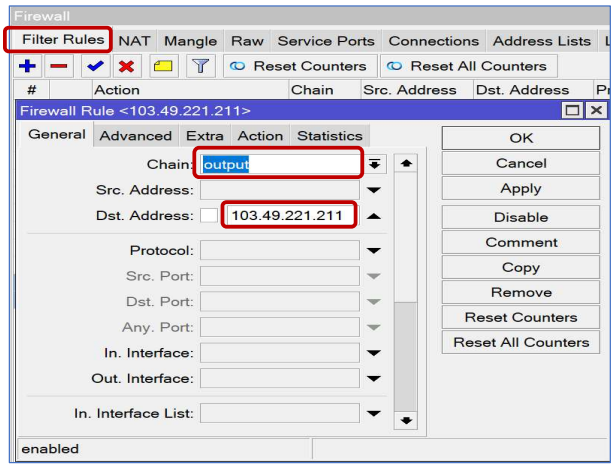


setelah dilakukan konfigurasi Firewall Chain Forward **Drop** tahapan selanjutnya melakukan pengujian terhadap Action **Drop,** dari komputer/notebook lakukan **ping** ke IP Public **8.8.8.8** [Melewati / forward Router **],** pada jobsheet ini jika dilakukan ping dari IP komputer **172.20.20.4** pastikan status action filter rule yang telah dilakukan sebelumnya [Action Drop] dinonaktikan terlebih dahulu **[disable]** dengan memilih baris script rule firewall index No. 2 **pilih Icon** X **[disable]**seperti gambar berikut **:**

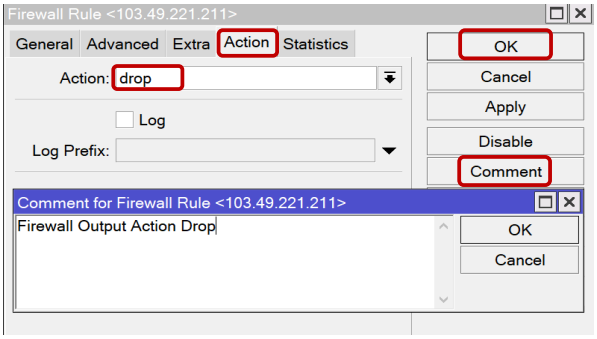


Setup Firewall Filter Rule Chain Output -Drop

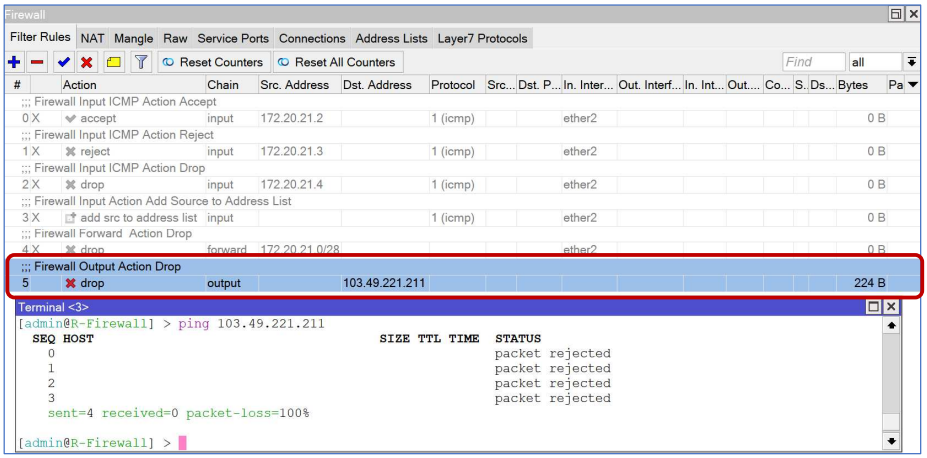
Untuk melakukan konfigurasi firewall filter rule Chain **Output Drop** pada Menu **Filter Rules** pilh Icon **+ ,** pada Tab Menu General Pilihan **Chain** pilih **Output** selanjutnya pilih **Dst.Address** isikan dengan IP Public **103.49.221.211** [dari router **R-Firewall** untuk menuju IP **103.49.221.211** tidak izinkan] seperti pada gambar berikut :



Tahapan selanjutnya pada Tab Menu **Action ,** pilihan Action pilih **drop,** dengan tujuan untuk melakukan blok terhadap IP Public **103.49.221.211**, selanjutnya tuliskan tambah **Comment** dan pilih tombol **OK,** seperti pada gambar berikut



Selanjutnya dilakukan pengujian konfigurasi Firewall Chain Output **Drop,** dari sisi **router** lakukan **ping** ke IP Public **103.49.221.211** seperti gambar berikut **:**



Simpulan

- Dengan melakukan praktek pada Job Sheet 5 mahasiswa dapat memahami cara kerja, penggunaan perintah serta dapat melakukan konfigurasi dasar router firewall filter rules [filter rules chain Input, Output , Forward, Action Accept/ Reject / Drop] pada Mikrotik Router.OS

7. Latihan Soal/Tugas

1. Buatlah Address List pada Firewall untuk melakukan pencatatan log user yang melakukan akses ke web itp.ac.id & detik.com
2. Tambahkan Firewall untuk menolak/reject IP **172.20.20.4** untuk akses MikroTik Router **R-Firewall** melalui Web, setelah ditambahkan lakukan pengujian akses IP Router melalui web browser dari komputer IP **172.20.20.4**

8. Penilaian

No.	Aspek Penilaian	Bobot	Poin Maksimal
1.	Sikap, Standar Perilaku Kerja	15%	20
2.	Hasil Kerja [standar konfigurasi]	85%	80
3.	Jumlah Bobot / Poin Maksimal	**100%**	**100**