PEMERINTAH PROVINSI SUMATERA BARAT
DINAS PENDIDIKAN
SMK NEGERI 4 PAYAKUMBUH
Jl. Koto Kociak,Kel.PadangSikabu,
KecLamposiTigoNagori (26219) – Payakumbuh
NPSN : 69947085 Email : smkn4pyk@gmail.com

RENCANA PELAKSANAAN PEMBELAJARAN

Sekolah Pendidikan	: SMK N 4 Payakumbuh
Bidang Studi Keahlian	: Teknologi Informasi Dan Komunikasi
Program Studi Keahlian	: Teknik Komputer Dan Informatika
Paket Keahlian	: TKJ, MM, RPL
Mata Pelajaran	: Administrasi Infrastruktur Jaringan
Kelas/Semester	: XII/I
Alokasi Waktu	: 42 x45 menit (5x pertemuan)
Kompetensi Dasar	: 3.8. Mengevaluasi Firewall Jaringan
	4.8 Mengkonfigurasi Firewall Jaringan

A. Tujuan Pembelajaran

Melalui model pembelajaran Discovery Learning peserta didik mampu menjelaskan tentang terminology jaringan dasar mengamati (Observing), menanya (Questioning), menalar (Assosiating), mencoba (Experimenting) dan mengaitkan (Networking) antar konsep dalam pembelajaran, dengan tujuan siswa dapat :

1. Menjelaskan Firewall jaringan
2. Menentukan cara konfigurasi Firewall jaringan

Setelah mempraktikan, peserta didik akan dapat:

1. Melakukan konfigurasi Firewall jaringan
2. Menguji hasil konfigurasi Firewall jaringan
3. Membuat laporan konfigurasi Firewall jaringan

B. Langkah-langkah Pembelajaran

Pertemuan 1

1. Guru memberikan gambaran awal tentang materi yang akan dipelajari pada pertemuan tersebut. (rasa ingin tahu)
2. Guru membagi peserta didik menjadi 4 kelompok untuk berdiskusi (kerjasama dan saling menghargai)
3. Peserta didik saling berdiskusi dan saling berkomunikasi serta berkolaborasi dengan anggota sekelompok tentang materi firewall (kerjasama)
4. Guru memperhatikan dan menjadi fasilisator dalam kegiatan diskusi kelompok belajar siswa
5. Setelah diskusi selesai guru memberikan kuis untuk mengukur sejauh mana kemampuan siswa memahami materi yang telah di diskusikan
6. Guru memeriksa hasil kuis dan memberikan penghargaan kepada siswa yang menjawab dengan benar serta kelompok dengan memperoleh skor tertinggi dan memberi apresiasi pada kelompok lain,

Pertemuan 2

1. Guru memberikan pokok materi yang akan dipelajari (rasa ingin tahu)
2. Guru melakukan demonstrasi metode konfigurasi firewall.
3. Peserta didik melakukan konfigurasi firewall sesuai dengan metode yang disampaikan.
4. Setelah selesai peserta didik melakukan konfigurasi firewall, guru menugaskan perserta didik untuk membuat laporan pelaksanaan pekerjaan.
5. Peserta didik melakukan metode konfigurasi firewall dengan kreatif dan percaya diri
7. Setelah konfigurasi firewall selesai, guru memberikan kuis untuk mengukur sejauh mana kemampuan siswa dalam memahami konfigurasi firewall.
6. Guru memeriksa hasil kuis dan memberikan penghargaan kepada siswa yang menjawab dengan benar dan memberi apresiasi pada siswa lain.

Pertemuan 3

1. Guru memberikan pokok materi yang akan dipelajari (rasa ingin tahu)
2. Guru melakukan demonstrasi cara konfigurasi firewall.

3. Peserta didik melakukan konfigurasi firewall sesuai dengan petunjuk.
4. Setelah selesai peserta didik melakukan konfigurasi firewall, guru menugaskan perserta didik untuk membuat laporan pelaksanaan pekerjaan.
5. Peserta didik melakukan konfigurasi firewall dengan kreatif dan percaya diri
8. Setelah konfigurasi firewall selesai, guru memberikan kuis untuk mengukur sejauh mana kemampuan siswa dalam memahami konfigurasi firewall.
6. Guru memeriksa hasil kuis dan memberikan penghargaan kepada siswa yang menjawab dengan benar dan memberi apresiasi pada siswa lain.

Pertemuan 4

1. Guru memberikan pokok materi yang akan dipelajari (rasa ingin tahu)
2. Guru melakukan demonstrasi cara menguji konfigurasi firewall.
3. Peserta didik melakukan konfigurasi firewall sesuai dengan petunjuk.
4. Setelah selesai peserta didik melakukan konfigurasi firewall, guru menugaskan perserta didik untuk melakukan pengujian konfigurasi firewall.
5. Peserta didik melakukan pengujian konfigurasi firewall dengan kreatif dan percaya diri
9. Setelah pengujian konfigurasi firewall selesai, guru memberikan kuis untuk mengukur sejauh mana kemampuan siswa dalam memahami konfigurasi firewall.
6. Guru memeriksa hasil kuis dan memberikan penghargaan kepada siswa yang menjawab dengan benar dan memberi apresiasi pada siswa lain.

Pertemuan 5

1. Guru memberikan pokok materi yang akan dipelajari (rasa ingin tahu)
2. Guru menjelaskan tentang teknik penyusunan laporan praktek.
3. Peserta didik melakukan konfigurasi firewall sesuai dengan petunjuk.
4. Setelah selesai peserta didik melakukan konfigurasi dan pengujian firewall, guru menugaskan perserta didik untuk membuat laporan pelaksanaan pekerjaan.
5. Peserta didik menyusun laporan praktek konfigurasi firewall
6. Setelah laporan selesai, guru memberikan kesepampatan kepada siswa untuk mempresentasikan laporan tersebut.

7. Guru memeriksa laporan dan memberikan penghargaan kepada siswa yang melakukan pekerjaan dengan baik dan memberi apresiasi pada siswa lain.

C. Asesmen

1. Pengetahuan :

   Tes tertulis : dalam bentuk essay tentang teori dasar firewall

2. Keterampilan :

   Tes Kinerja tentang konfigurasi firewall

Mengetahui, Kepala SMK N 4 Payakumbuh	Telah diperiksa oleh, Waka Kurikulum	Payakumbuh, Mei 2020 Guru Bidang Studi
Drs. Aizur Hedi, MM Nip. 19640402 198903 1 008	**Nazwita, M.Kom** NIP. 19770115 200901 2 002	**Ilham Ilahi, S.Pd** Nip. 198505182009011002

LAMPIRAN PENILAIAN

1. Teknik dan Bentuk Penilaian

TeknikPenilaian	**BentukPenilaian**
✓ Penilaian Sikap : observasi	Lembar Jurnal
✓ Penilaian Pengetahuan : tes tulis	Essay
✓ Penilaian Keterampilan : tes kinerja	Lembar Kinerja (proses)

2. Instrumen Penilaian

Sikap :

Pedoman Pengamatan Sikap

Kelas **:**

Hari, tanggal **:**

Pertemuan ke **:**

Materi pokok **:** Konfigurasi Firewall

Lembar Observasi

No	**NAMA**	**Religius**	**Integritas**	**Nasionalis**	**Mandiri**	**Gotong royong**
1						
2						
3						
4						
5						
dst						

Skor penilaian menggunakan skala 1 – 4, yaitu :

Skor 1 apabila peserta didik tidak pernah sesuai aspek sikap yang dinilai

Skor 2 apabila peserta didik kadang-kadang sesuai aspek sikap yang dinilai

Skor 3 apabila peserta didik sering sesuai aspek sikap yang dinilai

Skor 4 apabila peserta didik selalu sesuai aspek sikap yang dinilai

$$\text{Nilai} = \frac{\text{Skor Perolehan}}{20} \times 4$$

Pengetahuan :

✓ Kisi-kisi soal

No.	Kompetensi Dasar	Materi	Indikator Soal	No Soal	Bentuk Soal
1	Mengevaluasi Firewall jaringan	Dasar Firewall	Menjelaskan pengertian firewall	1	Essay
2	Mengkonfigurasi Firewall jaringan.		Menjelaskan manfaat firewall	2	Essay
3	Mengevaluasi Firewall jaringan		Menjelaskan jenis jenis firewall	3	Essay
4	Mengkonfigurasi Firewall jaringan.		Menjelaskan konfigurasi firewall	4	Essay
5	Mengkonfigurasi Firewall jaringan.		Menguji firewall	5	Essay

✓ Soal

No	Soal	Bobot
1.	Jelaskanlah definisi firewall dalam jaringan	20
2.	Jelaskan manfaat firewall dalam jaringan	20
3.	Sebutkan jenis-jenis firewall dalam jaringan	20
4.	Uraikan langkah-langkah melakukan filrtering terhadap port 21,22 dan ICMP	20
5.	Jelaskan bagaimana langkah langkah dalam menguji konfigurasi firewall sesuai soal nomor 4	20
	Total Skor	100

Kunci Jawaban

1. Firewall adalah salah satu cara untuk mengamankan jaringan dari akses yang tidak diizinkan. Mengamankan akses dari traffic yang masuk (input) dari dalam jaringan (forward) maupun menuju client (output).
2. Manfaat firewall dalam jaringan adalah untuk mengamankan sumber daya jaringan dari akses yang tidak diiizinkan. Membatasi akses user kedalam jaringan agar proses pertukaran informasi menjadi lebih maksimal.
3. Beberapa jenis firewall yang ada antara lain >
   - Filter Rule
   - NAT
   - Address List
   - Mangle
4. Langkah -langkah konfigurasi firewall untuk bloking port 21.22
   - Chain = input
   - Src-address= Lokal
   - DST-port = 21,22
   - Action = drop
5. Pengujuan client adalah dengan melakukan akses ftp ke router jika ditolak, maka konfigurasi firewall berhasil.

Penilaian Ketarampilan

✓ **Instrumen**

Petunjuk :Berilah tanda check (v) pakai kolom skor

No	Komponen/Sub Komponen	Skor		
		1	2	3
A	**Persiapan**			
	Hadir tepat waktu, berseragam lengkapdanrapi			
	Alat dipersiapan dengan lengkap dan rapi			
B	**Proses Kerja**			
	Konfigurasi Firewall			
C	**Hasil**			
	Konfigurasi firewall			
D	**SikapKerja**			
	Sikap kerja saat melakukan konfigurasi			
E	**Waktu**			
	Ketepatan waktu kerja			

Rubrik Penilaian

No	Komponen/Sub Komponen	Indikator/KriteriaUnjukKerja	Skor
A	**Persiapan**		
	Hadir tepat waktu, berseragam lengkap dan rapi	✓ Hadir tepat waktu, berseragam lengkap dan rapi ✓ Hadir tepat waktu, berseragam lengkap ✓ Hadir tepat waktu, berseragam tidak lengkap	3 2 1
	Mempersiapkan kebutuhan praktek dengan baik.	• Alat dipersiapan dengan lengkap dan rapi • Alat dipersiapan dengan lengkap	3 2 1

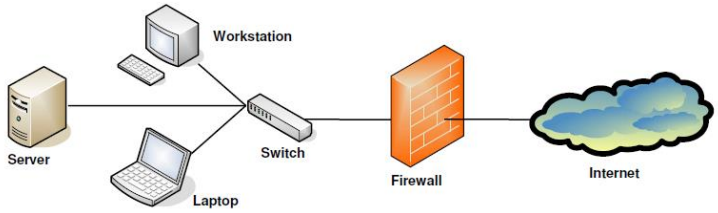
		• Alat dipersiapan dengan tidak lengkap	
B	**Proses Kerja**		
	Prosedur melakukan konfigurasi firewall.	• Menunjukkan Prosedur konfigurasi firewall dengan baik • Menunjukkan Prosedur pembuatan rule firewall dengan baik • Menunjukkan hasil konfigurasi yang dibuat	3 2 1
C	**Hasil**		
	Pengujian Firewall	• Akses ke port 21 diblok • Akses ke port 22 diblok • Client tidak bisa ping ke router	3 2 1
D	**SikapKerja**		
	Sikapkerjasaatmembuat peta minda	• Tertib dan rapi saat mempersiapkan, dan melaksanakan dan melaporkan • Tertib dan rapi saat mempersiapkan, dan melaksanakan • Tertib dan rapi saat mempersiapkan, melaksanakan, atau melaporkan	3 2 1
	Waktu		
	Ketepatanwaktukerja	Kurang dari 15 menit 15 – 30 menit Lebih dari 30 menit	3 2 1

LAMPIRAN MATERI

FIREWALL

A. MENGENAL FIREWALL MIKROTIK

Firewall adalah sistem keamanan jaringan yang digunakan untuk melindungi jaringan dari akses yang tidak diizinkan serta mengendalikan lalu lintas jaringan berdasarkan aturan keamanan yang telah ditentukan. Fungsi dari *Firewall* secara umum digunakan untuk memeriksa dan menentukan aliran paket data yang masuk dan keluar dalam jaringan. Mengontrol dan mengawasi aliran paket data di jaringan. Mengawasi paket data yang diizinkan masuk dari jaringan public ke jaringan local.

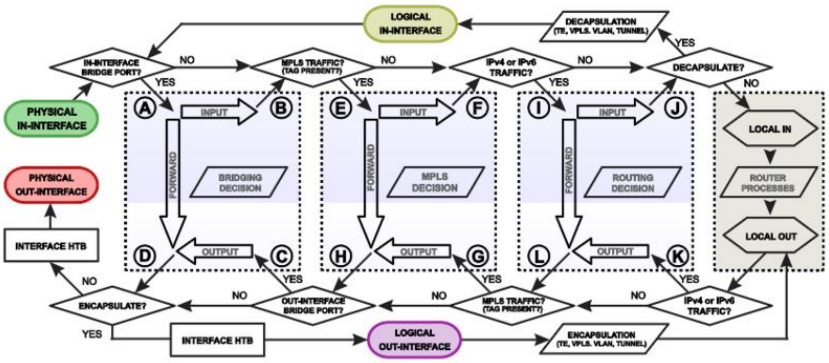


Gambar 4..1. Firewall

Untuk dapat mempelajari *Firewall* dengan baik, maka kita seharusnya sudah memiliki pengetahuan mengenai IP packet yang meliputi informasi mengenai IP address pengirim (*source address*), IP address penerima (*destination address*), port pengirim dan port tujuan. Selain itu kita juga sebaiknya sudah mengetahui jenis *protocol* yang digunakan dalam aplikasi jaringan internet seperti *protocol* tcp, UDP, ICMP. Pembahasan lebih lanjut mengenai protocol tcp/udp bisa didapatkan di berbagai buku yang membahasa dasar jaringan komputer. Pengetahuan mengenai IP Packet inilah yang menjadi pedoman dalam menentukan logika *Firewall* rule yang akan digunakan di mikrotik.

Firewall di Router mikrotik dapat melakukan filtering akses (*filter rule*), *forwarding packet* (NAT) serta menandai paket yang masuk dan keluar router (*mangle*). Agar fitur *Firewall* ini berjalan dengan baik maka diperlukan aturan (rule) yang tepat.

Parameter utama dalam membuat rule *Firewall* ini diatur dalam *chain*. Parameter *chain* digunakan untuk menentukan jenis lalu lintas data yang akan diatur dalam *Firewall*. Parameter chain pada *Firewall* filter rule, NAT dan Mangel memiliki pilihan chain yang berbeda. Pengisian parameter chain mengacu pada traffic flow routerOS. Setiap versi RouterOS memiliki skema traffic flow yang berbeda. Sebelum kita melakukan filter paket data yang masuk dan keluar di router kita harus mengenali terlebih dahulu jenis paket data yang akan kita atur menggunakan *Firewall*. Chain dianalogikan sebagai tempat untuk mencegat sebuah traffic data dan melakukan filtering sesuai kebutuhan. Berikut ini adalah skema traffic flow di RouterOs versi 6.

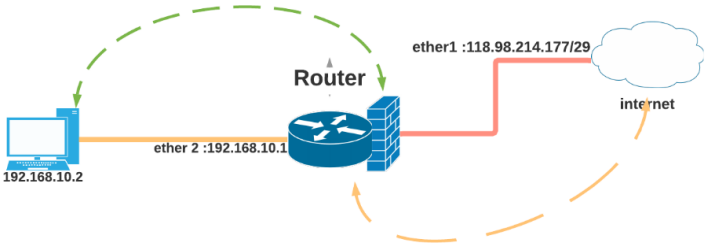


Gambar 4.2. Packet Flow Diagram

B. FILTER RULE

Filter rule adalah *Firewall* yang digunakan untuk melakukan kebijakan hak akses sebuah traffic yang ada dalam jaringan. Setiap *Firewall* filer rule yang disusun diorganisir dalam bentuk *chain* (rantai). Dalam menu *Firewall-filter rule* ada 3 chain yaitu *input, output, forward*. Setiap aturan rule chain yang dibuat akan dibaca oleh router dari rule paling atas ke bawah.

Chain input, digunakan untuk mengelola paket yang masuk menuju router melalui salah satu interface router dan alamat IP yang dimiliki router. Jenis traffic rule ini bisa berasal dari jaringan public maupun jaringan local. Contoh akses ke router menggunakan winbox,ssh,telnet dari jaringan public dan local. Kita tidak menginginkan adanya akses yang tidak diizinkan kedalam router.



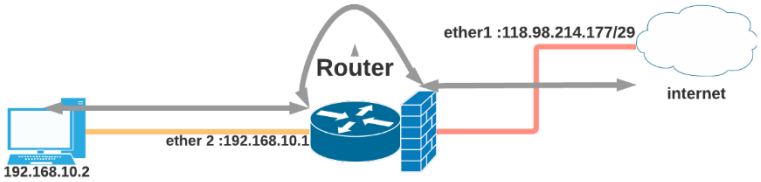
Gambar 4.3.Chain Chain

Chain input seperti gambar diatas diberikan pada interface ether 1 untuk melakukan perlindungan dari akses yang berasal dari luar/internet, sedangkan input di ether2 merupakan perlindungan akses yang berasal dari jaringan local. Penerapan chain input dalam jaringan digunakan untuk membatasi akses terhadap beberapa port router yang terbuka baik dari dalam maupun dari luar. Secara default port yang terbuka di router mikrotik seperti ssh 22, telnet 23, ftp 21, winbox 8291, webfig 80.

Kita tentunya tidak menginginkan jika ada pengguna tak dikenal bisa askes masuk ke router dari port yang terbuka tersebut. Untuk itu salah satu metode keaman yang digunakan untuk mencegah akses tersebut adalah dengan menutup port tersebut di *Firewall* rule.

```
/ip Firewall filter add chain=input in-interface=ether 1 protocol=tcp dst-port=21,22,23,80,8291 action=drop
```

Chain forward, digunakan untuk mengelola paket yang masuk ke router dan kemudian diteruskan ke tujuan dengan cara melewati router. Misalnya traffic dari jaringan public ke jaringan local. Contohnya ketika melakukan browsing internet maka *Firewall* filter akan mengelola paket dengan chain forward.

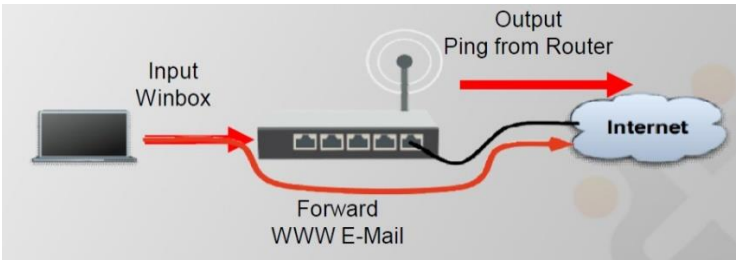


Gambar 4.5.Chain Forward

Cara kerja chain *forward* hampir sama dengan *filrewall nat*, Client 192.168.10.2 ketika akan melakukan akses ke google.com maka paket data akan dkirimkan ke router melakui interface ether2.

Di router sesuai dengan *filter rule* yang ditetapkan, maka paket akan diteruskaN NAT untuk dilakukan perubahan IP local menjadi IP public dan selanjunya diteruskan ke internet. Selain itu kita bisa menggunakan *chain forward* untuk melakukan filter terhadap konten website dan ekstensi file yang diakses client.

Chain output, digunakan untuk mengelola traffic yang keluar dari router ke alamat tujuan. Jadi traffic berasal dari dalam router ke *destination network*. Misalnya adalah akses ping, Penerapan chain output salah satunya adalah dengan pengaturan jika ada percobaan login ke router salah sebanyak beberapa kali maka router akan melakukan blokir terhadap IP address tersebut. Konfigurasi ini selanjutnya akan dibahas di studi kasus.



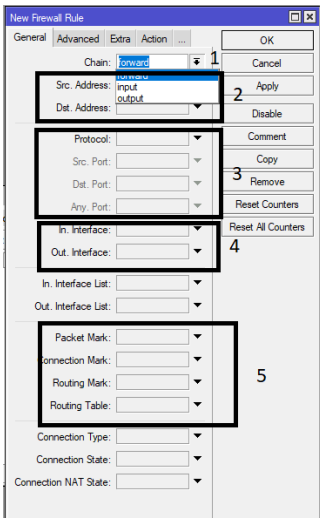
Gambar 4.6. Chain Output

Untuk menentukan *rule* pada *Firewall* rule menggunakan prinsip logika **IF..Then..** dimana **IF** (jika) adalah kondisi packet memenuhi syarat pada rule yang akan dibuat. Dan **Then** (maka) adalah kondisi filter yang akan dilakukan terhadap packet data tadi. Kriteris parameter IF seperti chain yang digunakan, asal IP address (*source address*) kondisi port dan protocol yang akan di filter.

Kemudian parameter **Then** adalah kondisi tindakan yang dilakukan untuk parameter **IF** sebelumnya, misalnya contoh kondisi **IF** adalah paket IP address 10.10.1.0/24 dengan protocol tcp akan diberikan tindakan seperti *drop* yang merupakan parameter kondisi **Then**. Penentuan *filter rule* jika tidak

memenuhi kondisi seperti diatas maka tidak akan dapat diproses oleh router. Kemudian router juga melakukan proses filter dengan skema urutan *top to down*, artinya rule paling atas yang akan diproses terlebih dahulu kemudian disusul dengan proses di rule selanjutnya sampai ke rule terakhit. Keberhasilan filter juga ditentukan dari urutan rule yang dibuat sebelumnya.

Kondisi parameter IF..



1. Chain = pilihan metode chain filter yaitu input, forward,output

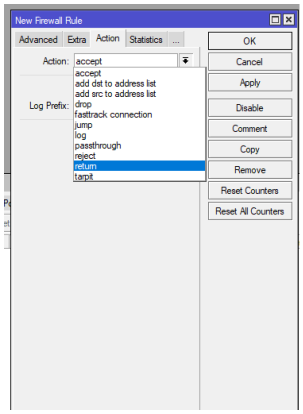
2. Source address = IP sumber client
   Destination IP = IP tujuan client

3. Protocol = tcp, udp, icmp
   Source port = port asal protocol
   destination port = port tujuan

4. Interface = pilihan interface yang akan difilter

5. Packet mark pilihan untuk menandai paket yang akan difilter

Parameter Then..



2. add dst to address list = menambahkan network tujuan ke address list dengan parameter tertentu
3. add src to address list= menambahkan IP asal (source) ke daftar address list

4. drop = menolak paket secara diam diam
5. jump = lompat ke rule berikutnya atau rule target berikutnya.

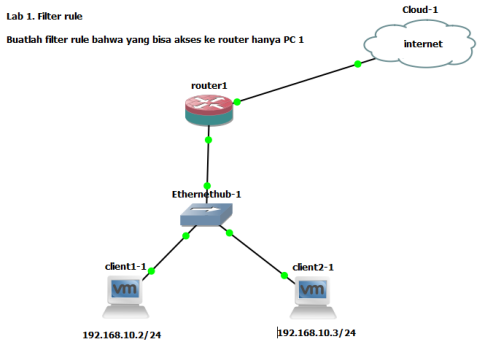
6. log = tambahkan pesan ke daftar logc/catatan
7. passtrough = abaikan rule dan maju ke rule berikutnya.
8. reject = tolak paket dengan mengirim pesan penolakan.
9. return = kembali ke rule yang ditentukan
10. tarpit = memberikan pesan tcp connection dan menjaga status ACK

Selanjutnya strategi yang kita lakukan dalam pembuatan filter rule adalah dengan menggunakan pendekatan antara lain :

a. Drop beberapa, terima lainnya (drop few, accept any)
b. Terima beberapa, drop lainnya (accept few, drop any).

Misalnya kita buat pengecualian bahwa hanya IP 10.10.1.2 yang bisa akses router, maka semua IP selain itu kita tolak. Untuk lebih jelasnya penerapan filter rule, kita akan lakukan lab filter *Firewall* pada beberapa kondisi yang umum digunakan di jaringan komputer.

Lab 1. Filter rule - Membatasi akses ke router



Konfigurasi agar yang bisa akses dan ping ke router 1 hanya IP 192.168.10.2

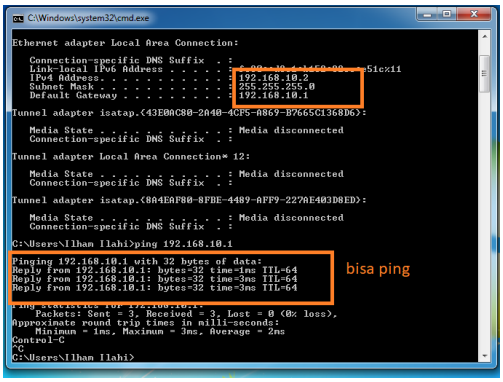
/ip *Firewall* filter add chain=inpur src-address=192.168.10.2 action=accept

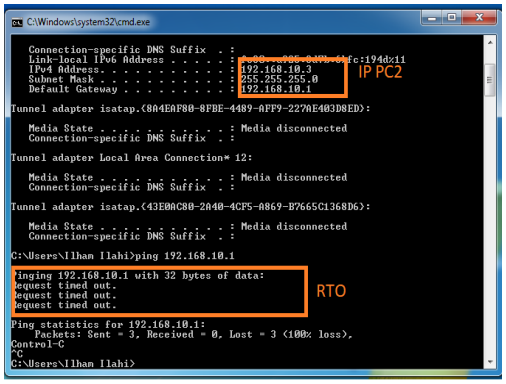
/ip *Firewall* filter add chain=input action=drop

```
[admin@router1] > ip firewall filter add chain=input src-address=192.168.10.2 action=accept
[admin@router1] > ip firewall filter add chain=input action=drop
[admin@router1] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=input action=accept src-address=192.168.10.2

 1    chain=input action=drop
[admin@router1] >
```

Hasilnya adalah PC 1 192.168.10.2 bisa melakukan ping ke router dan IP PC2 192.168.10.2 tidak bisa ping ke router.





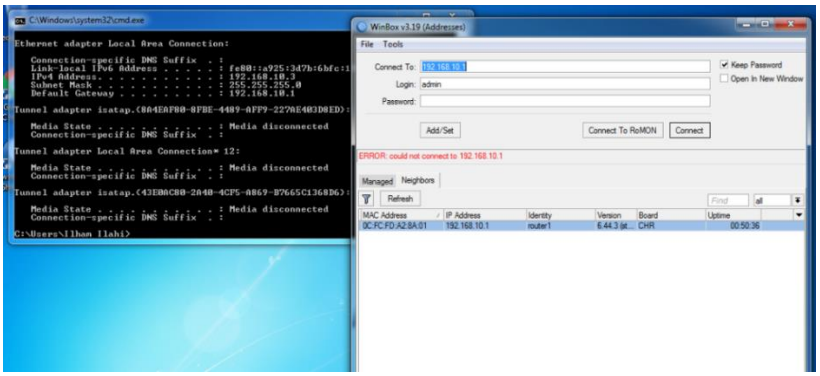
Jika kita melihat filter rule print, maka ada 2 rule yang dibuat sesuai urutan pertama dengan index 0 adalah mengizinkan IP 192.168.10.2 untuk akses ke router, kemudian rule kedua dengan index 1 artinya melakukan drop paket kepada semua input IP yang masuk ke router. Jadi penerapan metode ini disebut dengan metode *accept few,drop any*.

Filter yang kita buat sebelumnya hanya melakukan drop ping, namun jika dicoba PC 2 192.168.10.3 bisa melakukan akses ke winbox. Bagaimana caranya agar PC 2 tidak bisa akses ke winbox router?

Untuk melakukan filter akses ke winbox ada beberapa cara, kali ini kita gunakan filter rulenya saja. Sama seperti kondisi filter sebelumnya hanya di rule drop tambahkan port winbox = 8291 dan definisikan interface yang digunakan.

```
/ip filrewall filter add chain=input src-address=192.168.10.2 action=accept
/ip Firewall filter add chain=input protocol=tcp dst-port=8291 in-interface=ether2 action=drop
```

Hasilnya adalah client PC2 tidak bisa login ke winbox.



Kita ingin agar router kita tidak bisa di ping dari client intenet , maka penerapan rule filternya adalah

```
/ip Firewall filter add chain=input in-interface=ether1 protocol=icmp action=drop
```

Ada kalanya kita ingin melakukan remote router dari intenet, namun berdasarkan rule diatas kita sudah melakukan blokir akses kesemua port router sehingga tidak memungkinkan untuk melakukan akses ke router dari luar. Untuk kasus seperti ini bisa kita atasi dengan menambakan alamat IP yang diizinkan untuk melakukan akses ke router dari internet. Rule yang kita gunakan

```
/ip Firewall filter add chain=input action=accept protocol=tcp src-address=alamat_ip_public in-interface=ether1
```

Filter Rule – Address list filter

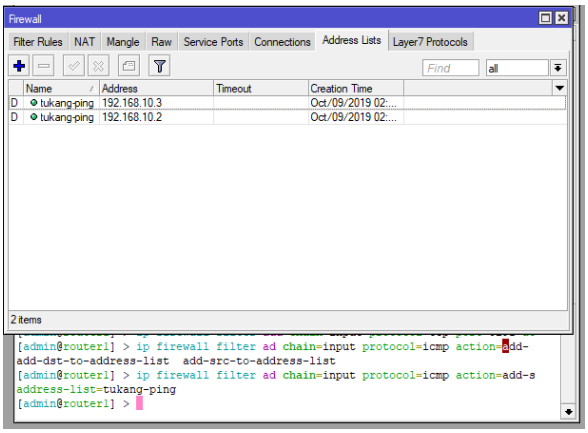
Ada kalanya kita ingin melakukan filter terhadap sekelompok IP address di dalam jaringan. Mikrotik mempunyai fitur address list untuk mengelompokkan IP address tertentu berdasarkan metworknya kedalam system penamaan yang kita inginkan. Address list digunakan untuk melakukan filter terhadap group IP dengan 1 *Firewall* rule.Addres List juga merupakan hasil dari rule *Firewall* dengan action=add to address list. Untuk satu address list bisa memuat subnet, range IP, atau 1 host IP address.

Lab 2 filter rule – address list

Buatlah rule *Firewall* yang akan memasukkan setiap IP address yang melakukan ping ke router ke dalam table address list.

/ip *Firewall* filter add chain=input protocol=icmp action=add-src-to-address-list addres=list=tukangping

Kemudian cobalah untuk melakukan ping dari pc client ke IP router

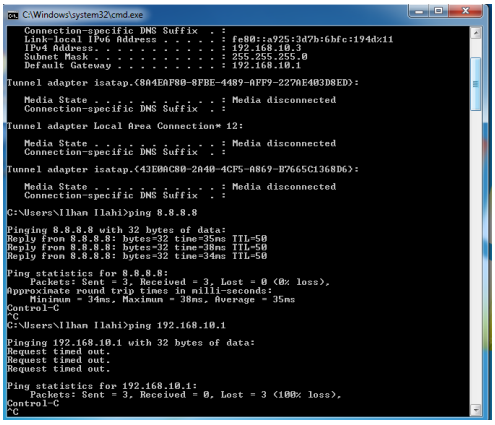


Terlihat secara otomatis IP address yang melakukan ping akan masuk ke table address list dengan kelompok nama=tukang-ping.

Kemudian buat rule yang memblokir akses tukang ping ke router.

/ip *Firewall* filter add chain=input src-address-list=tukang-ping action=drop

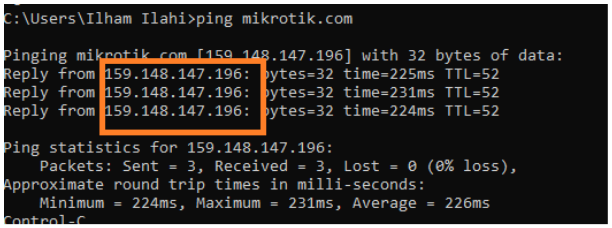
Maka hasilnya semua IP yang ada di table address list tidak bisa lagi ping ke router.



Filter akses ke website dengan filter rule

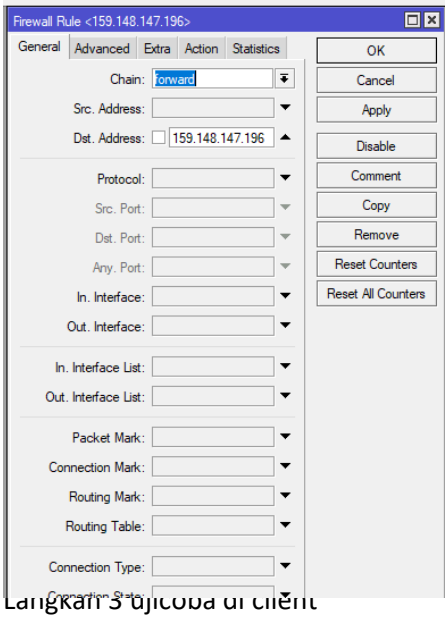
Administrator ingin agar client dijaringannya tidak dapat melakukan akses ke website tertentu, missal ke situs porno,situs judi dan lain lainnya. Untuk melakukan filter tersebut dapat dilakukan salah satunya dengan filter rule *Firewall*. Lab kali ini kita akan filter akses ke mikrotik.com

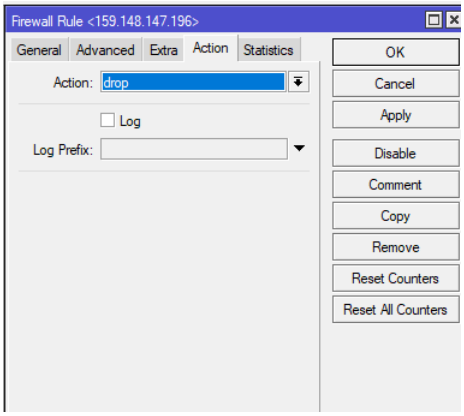
Langkah 1. Mengetahui IP server domain yang akan diblok, bisa dengan menggunakan ping domain.



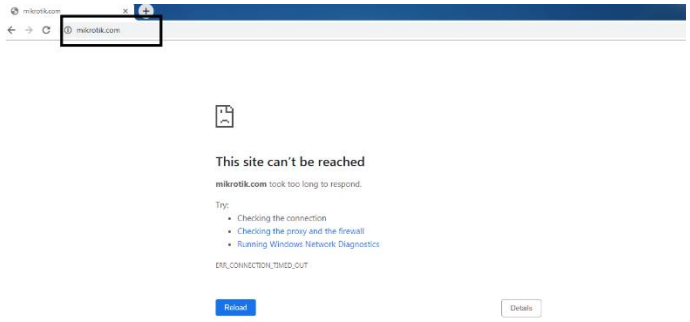
Langkah 2. Tambahkan filter rule di *Firewall*

/ip *Firewall* filter add chain=forward dst-address=159.148.147.196 action=drop





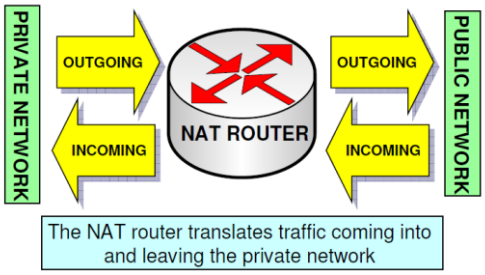
Langkah 3 ujicoba di client



Terlihat di client browser tidak dapat menampilkan halaman web mikrotik.com. Permasalah yang muncul dari menggunakan filter ini adalah ada beberapa website besar seperti facebook.com, youtube,com dll yang memiliki puluhan alamat IP server yang berbeda. Tentunya administrator akan kesulitan untuk melakukan filter seperti ini. Cara yang digunakan jika IP servernya banyak bisa menggunakan Teknik *add-to-address-list*. Kita mengelompokkan IP server youtube.com di address list yang akan terdata secara otomatis di table address list kemudian lakukan drop dengan parameter address list seperti yang sudah dilakukan di lab sebelumnya.

C. NAT

NAT *(Network Address translation*) adalah salah satu konfigurasi yang dilakukan untuk menghubungkan jaringan local yang memiliki IP Private ke internet. Sebelumnya kita sudah menjelaskan bahwa jaringan internet berkomunikasi dengan IP *Public* yang teregistrasi dan sudah terdaftar oleh ISP. Tetapi tidak mungkin rasanya jika di jaringan local semua host menggunakan *IP public* untuk berkomunikasi karena IPv4 memiliki jumlah yang terbatas. Untuk itu agar client dengan IP Private bisa akses intenet maka digunakan Teknik NAT Masquerade.



Pada *Firewall* Nat ada 2 chain yang digunakan yaitu **srcnat** (*source nat*) dan **dstnat** (*destination nat*).

Srcnat digunakan untuk mengubah paket asal (*source*) address yang berasal dari jaringan yang akan diubah yaitu jaringan local/private. Dengan *srcnat* maka IP private akan disembunyikan dan digantikan dengan IP Public (masquerade).