MODUL PRAKTIKUM SISTEM KEAMANAN JARINGAN

VERSI 1.0

OLEH

I PUTU HARIYADI

putu.hariyadi@stmikbumigora.ac.id

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER (STMIK) BUMIGORA MATARAM

BAB I

CISCO ACCESS CONTROL LIST (ACL)

Tujuan:

Mahasiswa memahami mengenai *Access Control List (ACL)* dan bagaimana menerapkannya di jaringan.

Materi:

1. Pengenalan Cisco Access Control List (ACL)

Cisco ACL digunakan untuk mengatur trafik IP dengan melakukan pemfilteran paket yang melalui router dan mengidentifikasi trafik untuk penanganan tertentu (klasifikasi). Pemfilteran menggunakan ACL dapat diterapkan untuk mengijinkan atau menolak paket yang melalui router, dan mengijinkan atau menolak akses telnet (vty) dari dan ke router. Router yang tidak memiliki konfigurasi ACL akan mentransmisikan semua paket ke semua bagian di jaringan. Klasifikasi menggunakan ACL dapat diterapkan untuk menangani trafik berdasarkan pengujian terhadap paket untuk tujuan seperti *Network Address Translation (NAT)*, *Virtual Private Network (VPN)*, dan lain sebagainya.

2. Jenis-jenis ACL.

ACL dibagi menjadi 2 jenis yaitu: *Standard ACL*, dan *Extended ACL*. *Standard ACL* digunakan untuk melakukan pemfilteran terhadap paket baik mengijinkan maupun menolak berdasarkan protokol secara keseluruhan, dan hanya melakukan pengujian pada alamat sumber. Sedangkan *Extended ACL* digunakan untuk melakukan pemfilteran terhadap paket baik mengijinkan maupun menolak berdasarkan protokol dan aplikasi secara spesifik, dan dapat melakukan pengujian pada alamat sumber, dan alamat tujuan, serta protokol tertentu.

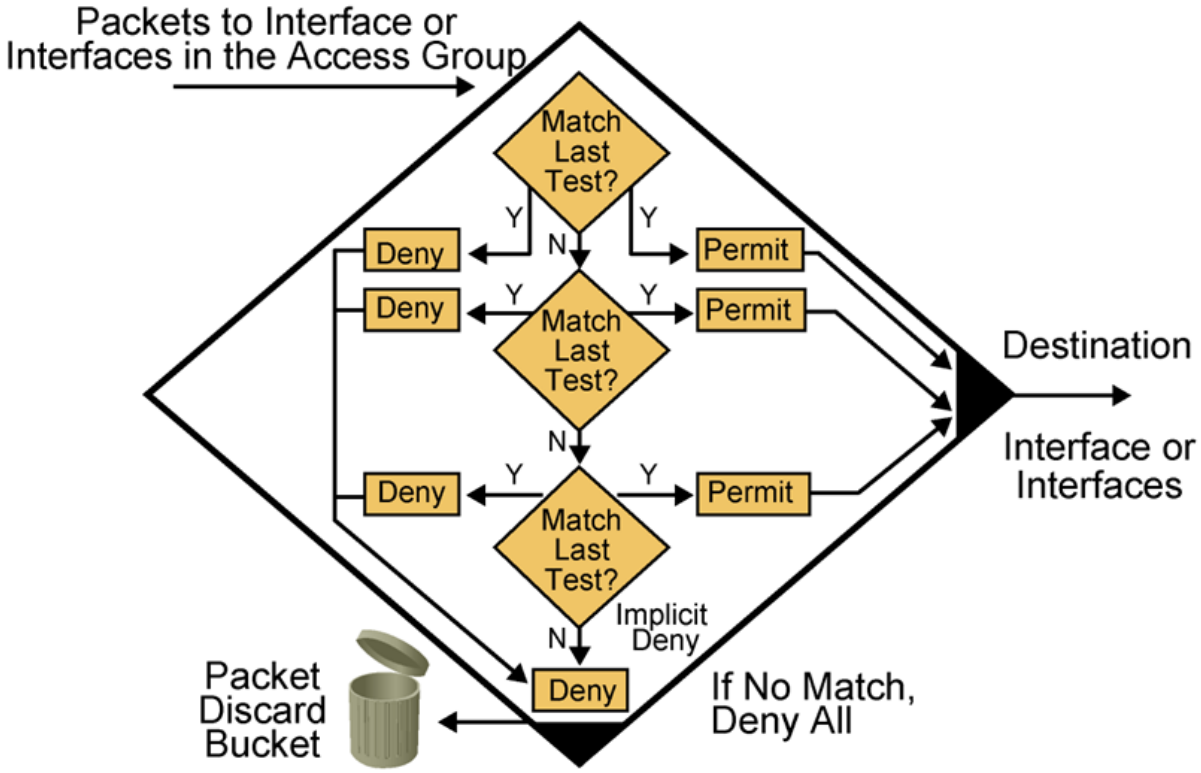
Terdapat dua metode yang digunakan untuk mengidentifikasi ACL dengan jenis standard dan extended yaitu *numbered ACL* dan *named ACL*. *Numbered ACL* menggunakan angka untuk mengidentifikasi ACL, sedangkan *Named ACL* menggunakan deskripsi nama untuk mengidentifikasi ACL.

Metode Identifikasi	Jenis ACL	Jangkauan Angka atau Penanda	Kondisi Pengujian
Numbered	**Standard**	1-99, 1300-1999	Seluruh paket IP berdasarkan alamat sumber.
	Extended	100-199, 2000-2699	Alamat sumber, alamat tujuan,

			protokol TCP/IP secara spesifik, dan nomor port sumber/tujuan.
Named	**Standard dan Extended**	Menggunakan nama berupa string alfanumerik.	Bergantung jenis ACL standard atau extended.

3. Pemrosesan ACL.

ACL melakukan pemrosesan dari atas ke bawah, dan dapat diatur untuk menguji trafik yang masuk (*incoming*) maupun keluar (*outgoing*), seperti terlihat pada gambar dibawah ini.



Gambar Alur Pemrosesan statement ACL (Sumber: Modul ICND2 CCNA)

Ketika sebuah router menerima paket pada interface tertentu (*incoming*) atau akan meneruskan paket keluar melalui interface tertentu (*outgoing*), maka router terlebih dahulu akan melakukan pengecekan apakah terdapat ACL yang diterapkan pada interface tersebut. Apabila tidak terdapat ACL yang diterapkan baik pada interface *incoming* maupun *outgoing* maka paket tersebut akan secara langsung dirutekan ke jaringan tujuan. Sebaliknya apabila terdapat ACL yang diterapkan pada interface tersebut maka akan dilakukan pengujian apakah paket tersebut cocok dengan salah satu statement ACL secara baris per baris dimulai dari atas ke bawah. Apabila cocok maka selanjutnya akan dilihat aksi yang dilakukan terhadap paket tersebut apakah ditolak atau diijinkan. Apabila ditolak maka paket tersebut

akan dibuang, sebaliknya apabila diijinkan maka paket tersebut akan diteruskan ke tujuan. Apabila tidak ada statement ACL yang sesuai atau cocok dengan paket tersebut maka dibaris paling akhir terdapat implicit deny any yang akan membuat paket tersebut dibuang atau tidak diteruskan.

4. Konsep Wildcard Mask pada ACL

Wildcard Mask digunakan untuk melakukan pengecekan bit alamat IP tertentu yang harus sesuai atau diabaikan. Wildcard Mask digunakan pada Access Control List (ACL). Wildcard Mask menggunakan bit 0 dan bit 1 untuk memperlakukan bit dari alamat IP, dimana:

a) **Bit 0**, bermakna cocok/sesuai/tepat dengan nilai bit pada alamat IP.
b) **Bit 1**, bermakna mengabaikan nilai bit pada alamat IP (diabaikan/nilainya dpt berupa apa saja).

Apabila 8 bit nilai wildcard mask diset dengan nilai bit 0 semua (00000000) maka nilai desimal dari wildcard mask tersebut adalah **0**. Sebaliknya apabila 8 bit nilai wildcard mask diset dengan nilai bit 1 semua (11111111) maka nilai desimal dari wildcard mask tersebut adalah **255**.

Terdapat 4 jenis Wildcard Mask yaitu:

a) **Wildcard mask "host"** digunakan untuk melakukan pencocokan dengan alamat IP (host) tertentu, dimana nilai wildcard masknya selalu **0.0.0.0**. Sebagai contoh harus tepat dengan alamat IP host **192.168.9.1**, maka nilai wildcard mask dalam format desimalnya adalah **0.0.0.0**. Nilai decimal 0 pada octet pertama menyatakan harus sesuai/tepat dengan nilai bit pada octet pertama dari alamat IP yaitu 192. Nilai decimal 0 pada octet kedua menyatakan harus sesuai/tepat dengan nilai bit pada octet kedua dari alamat IP yaitu 168. Nilai decimal 0 pada octet ketiga menyatakan harus sesuai/tepat dengan nilai bit pada octet ketiga dari alamat IP yaitu 9. Nilai decimal 0 pada octet ke-empat menyatakan harus sesuai/tepat dengan nilai bit pada octet ke-empat dari alamat IP yaitu 1.
b) **Wildcard mask "network"** digunakan untuk melakukan pencocokan dengan alamat network. Masing-masing alamat network berdasarkan **Class dari alamat IP** tersebut memiliki ketentuan nilai wildcard mask yang digunakan yaitu:
    - ✓ Class **A**: 0.255.255.255
    - ✓ Class **B**: 0.0.255.255
    - ✓ Class **C**: 0.0.0.255

c) **Wildcard mask "subnet"** digunakan untuk melakukan pencocokan dengan alamat subnet tertentu. Untuk menemukan nilai wildcard mask dari sebuah alamat subnet dapat menggunakan perhitungan nilai desimal dari wildcard mask tertinggi: 255.255.255.255 dikurangi dengan nilai decimal dari alamat subnetmask dari alamat subnet. Sebagai contoh terdapat sebuah alamat subnet 192.168.9.32/27, maka nilai wildcard mask adalah:

- ✓ Temukan terlebih dahulu alamat subnetmask dalam format *dotted decimal notation* dari alamat subnet 192.168.9.32 /27, yaitu /27 => 255.255.255.224.
- ✓ Selanjutnya lakukan **operasi pengurangan**:

  255.255.255.255
  255.255.255.224
  0. 0. 0. 31

  Sehingga nilai wildcard mask dari alamat subnet 192.168.9.32 adalah **0.0.0.31**.

d) **Wildcard Mask "Ranges"**, digunakan untuk melakukan pencocokan dengan jangkauan/block/jumlah tertentu dari alamat IP. Untuk menemukan nilai wildcard dari sebuah blok alamat IP tertentu digunakan perhitungan **nilai block size dikurangi dengan 1**. Sebagai contoh mencocokkan dengan jangkauan alamat IP dari 192.168.9.4, 192.168.9.5, 192.168.9.6, 192.168.9.7, maka nilai wildcard masknya adalah:

- ✓ Terlihat nilai decimal dari alamat IP pada octet pertama, kedua, dan ketiga memiliki nilai yang sama sehingga nilai decimal wildcard mask untuk masing-masing tiga octet pertama adalah 0.
- ✓ Selanjutnya terlihat untuk nilai decimal dari alamat IP pada octet 4, dimulai dari 4 yang terkecil dan yang tertinggi adalah 7, sehingga block size yang paling mendekati adalah 4 karena terdapat 4 alamat IP.
- ✓ Lakukan operasi perhitungan nilai block size dikurangi 1 yaitu 4-1 = 3.
- ✓ Wildcard mask adalah 192.168.9.4 0.0.0.3.

(**Catatan:** hanya berlaku ketika *ranges* (jangkauan) alamat yg dicocokkan berurut). Jika tidak berurut maka perhitungan dilakukan dengan menggunakan metode konversi ke biner & dicocokkan scr manual dg nilai wildcard mask bit.

Terdapat beberapa penanda yang digunakan pada wildcard yaitu:

a) Penanda untuk alamat wildcard mask host yang nilainya **0.0.0.0** bisa digantikan dengan kata kunci "**host**".

b) Penanda untuk alamat IP dengan nilai apapun alamat IP sumber/tujuannya ditandai dengan nilai: **0.0.0.0**.

c) Penanda untuk alamat wildcard mask yang nilainya dapat berupa apa saja ditandai dg nilai: **255.255.255.255**.

d) Pencocokan alamat IP berapapun dengan alamat wildcard mask berapapun yaitu: 0.0.0.0 255.255.255.255 dapat disingkat dengan kata kunci "**any**".

BAB II

KONFIGURASI STANDARD ACL

Tujuan:

Mahasiswa mampu mengkonfigurasi Standard ACL yang diterapkan pada interface dan line vty.

Materi:

1. Pengenalan Panduan Penulisan ACL

Terdapat beberapa panduan dalam penulisan ACL, antara lain:

a) Jenis ACL baik standard maupun extended menentukan apa yang akan difilter.
b) ACL dapat memfilter trafik yang melalui router, atau trafik dari dan ke router, bergantung bagaimana penerapannya.
c) Urutan dari statement ACL mengatur pengujian, dimana pemrosesan dilakukan dengan menguji dari baris atas ke bawah, sehingga sebaiknya menempatkan statement ACL yang lebih spesifik di baris yang lebih atas.
d) Baris paling bawah dari ACL terdapat *implicit deny any* sehingga minimal terdapat 1 baris yang mengijinkan (*permit*).
e) ACL dibuat secara global dan diterapkan ke interface atau *line vty* baik untuk trafik yang masuk (*inbound*) maupun keluar (*outbound*).
f) Hanya sebuah ACL yang dapat diijinkan untuk diterapkan per interface, per protocol, dan per arah
g) Menempatkan ACL jenis standard dekat dengan tujuan.
h) Menempatkan ACL jenis extended dekat dengan sumber.

2. Pengenalan Standard ACL & Sintak penulisannya

Standard ACL digunakan untuk melakukan pemfilteran terhadap paket baik mengijinkan atau menolak berdasarkan protokol secara keseluruhan, dan hanya melakukan pengujian pada alamat sumber. Adapun sintak penulisan dari Standard ACL adalah:

```
access-list nomor_acl aksi alamat_sumber wildcard_sumber
```

- *Nomor_acl* untuk Standard ACL adalah **1-99, 1300-1999**.
- *Aksi* yang dapat digunakan adalah **permit** untuk mengijinkan, **deny** untuk menolak, **remark** untuk memasukkan deskripsi mengenal ACL yang dibuat.

- *Alamat_sumber* adalah alamat IP dari sumber yang akan diatur hak aksesnya.
- *Wildcard_sumber* adalah nilai wildcard yang digunakan untuk mencocokkan dengan *alamat_sumber* yang diatur hak aksesnya.

Standard ACL yang telah dibuat selanjutnya diterapkan ke *interface* atau ke *line vty* (telnet) dari router menggunakan perintah berikut:

a) Menerapkan ACL pada interface

```
(config)# interface type number
(config-if)# ip access-group {nomor-acl|nama_acl} {in|out}
```

b) Menerapkan ACL pada line vty

```
(config)# line vty nomor-vty
(config-line)# access-class {nomor_acl|nama_acl} {in|out}
```

ACL yang telah dibuat dan penerapannya pada interface atau line vty dapat diverifikasi menggunakan perintah berikut:

a) Menampilkan informasi seluruh ACL yang terdapat pada router

```
# show ip access-list
```

b) Memverifikasi penerapan ACL pada interface

```
# show ip interface type number
```

Perhatikan output dari eksekusi perintah tersebut dibagian baris *incoming access-list* dan *outgoing access-list*.

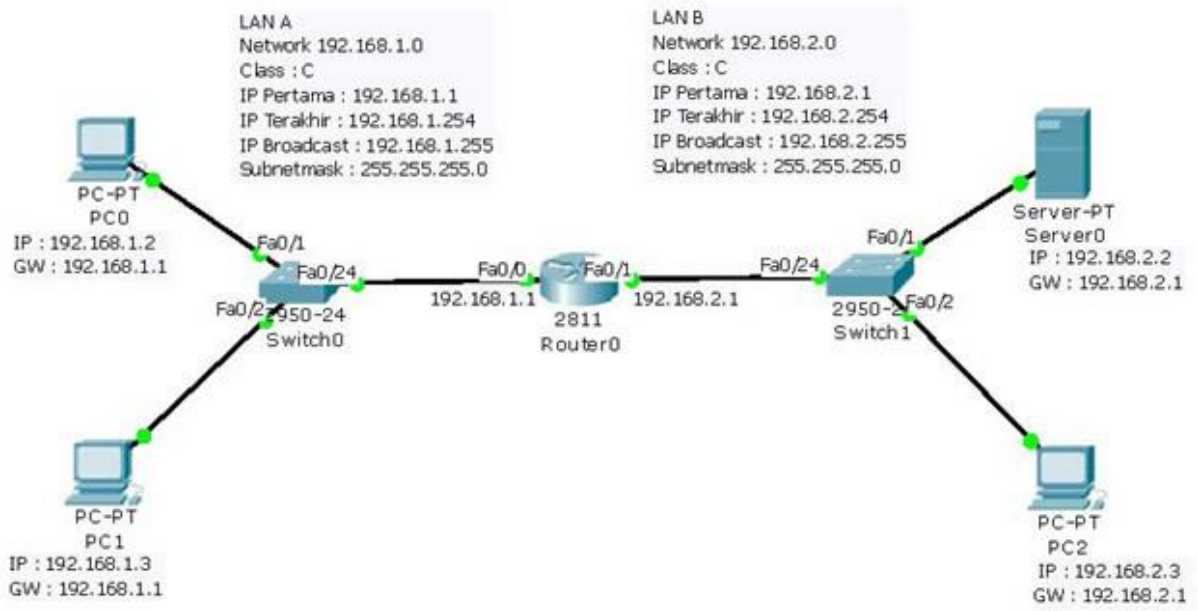
c) Memverifikasi penerapan ACL pada line vty

```
# show run
```

Perhatikan output dari eksekusi perintah tersebut dibagian line vty.

3. Studi Kasus penggunaan Standard ACL

Terdapat sebuah jaringan dengan gambar topologi dan pengalamatan IP seperti terlihat pada gambar dibawah ini:



Adapun beberapa skenario konfigurasi standard ACL yang akan diterapkan pada Router0 adalah menolak akses dari host PC1 di LAN A ke LAN B dan mengijinkan akses dari host lainnya, serta mengijinkan akses telnet ke Router0 hanya dari host-host LAN B.

Solusi:

Menolak akses dari host PC1 di LAN A ke LAN B dan mengijinkan akses dari host lainnya

a) Membuat ACL Standar:

```
(config)#access-list 2 deny 192.168.1.3 0.0.0.0

(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

b) Menerapkan ACL Standard yang dibuat ke interface FastEthernet0/1 menggunakan perintah berikut**:**

```
(config)# interface f0/1
(config-if)# ip access-group 2 out
(config-if)# end
```

c) Memverifikasi ACL yang telah dibuat

```
#show ip access-list
```

d) Memverifikasi penerapan ACL pada inteface f0/1

```
#show ip interface f0/1
```

Mengijinkan akses telnet ke Router 0 hanya dari host-host LAN B

e) Membuat ACL Standar:

```
(config)#access-list 1 permit 192.168.2.0 0.0.0.255
```

f) Menerapkan ACL Standard yang dibuat ke line vty menggunakan perintah **access-class:**

```
(config)#line vty 0 4

(config-line)#access-class 1 in
```

g) Memverifikasi ACL yang telah dibuat

```
#show ip access-list
```

h) Memverifikasi penerapan ACL pada line vty

```
#show run
```

Tugas:

Berdasarkan topologi jaringan pada studi kasus diatas, buatlah konfigurasi standard ACL dengan ketentuan sebagai berikut:

1. Menolak akses dari host PC2 ke LAN A.
2. Mengijinkan host PC0 dari LAN A untuk dapat melakukan telnet ke Router0.

BAB III

KONFIGURASI EXTENDED ACL

Tujuan:

Mahasiswa memahami penggunaan dan konfigurasi Extended ACL.

Materi:

1. Pengenalan Extended ACL & Sintak Penulisannya

Extended ACL digunakan untuk melakukan pemfilteran terhadap paket baik mengijinkan maupun menolak berdasarkan protokol dan aplikasi secara spesifik, dan dapat melakukan pengujian pada alamat sumber, dan alamat tujuan, serta protokol tertentu. Adapun sintak penulisan dari ACL Extended adalah:

```
access-list nomor_acl aksi protocol alamat_sumber wildcard sumber
alamat_tujuan wildcard_tujuan operator nomor_port
```

- Nomor_acl untuk ACL Extended adalah 100-199
- *Aksi* yang dapat digunakan adalah **permit** untuk mengijinkan, **deny** untuk menolak, **remark** untuk memasukkan deskripsi mengenal ACL yang dibuat.
- *Protocol* digunakan untuk menentukan metode transmisi yang digunakan di layer transport, seperti http – tcp, telnet – tcp, ftp – tcp, tftp – udp, dns – tcp & udp, ping – icmp.
- *Alamat_sumber* adalah alamat IP dari sumber yang akan diatur hak aksesnya.
- *Wildcard_sumber* adalah nilai wildcard yang digunakan untuk mencocokkan dengan alamat_sumber yang diatur hak aksesnya.
- *Alamat_tujuan* adalah alamat IP dari tujuan yang akan diatur hak aksesnya.
- *Wildcard_tujuan* adalah nilai wildcard yang digunakan untuk mencocokkan dengan alamat_tujuan yang diatur hak aksesnya.
- *Operator* digunakan untuk melakukan perbandingan, antara lain: **eq** (equal) untuk sama dengan, **neq** (not equal) untuk tidak sama dengan, **lt** (less than) untuk lebih kecil dari, dan **gt** (greater than) untuk lebih besar dari.
- *Nomor_port* dari layanan yang diatur, seperti http – 80, telnet -23, ftp – 20 & 21, smtp -25, pop3 – 110, tftp – 69, dns – 53.

Extended ACL yang telah dibuat selanjutnya diterapkan ke *interface* dari router menggunakan perintah berikut:

```
(config)# interface type number
(config-if)# ip access-group {nomor-acl|nama_acl} {in|out}
```

ACL yang telah dibuat dan penerapannya pada interface dapat diverifikasi menggunakan perintah berikut:

a) Menampilkan informasi seluruh ACL yang terdapat pada router

```
# show ip access-list
```

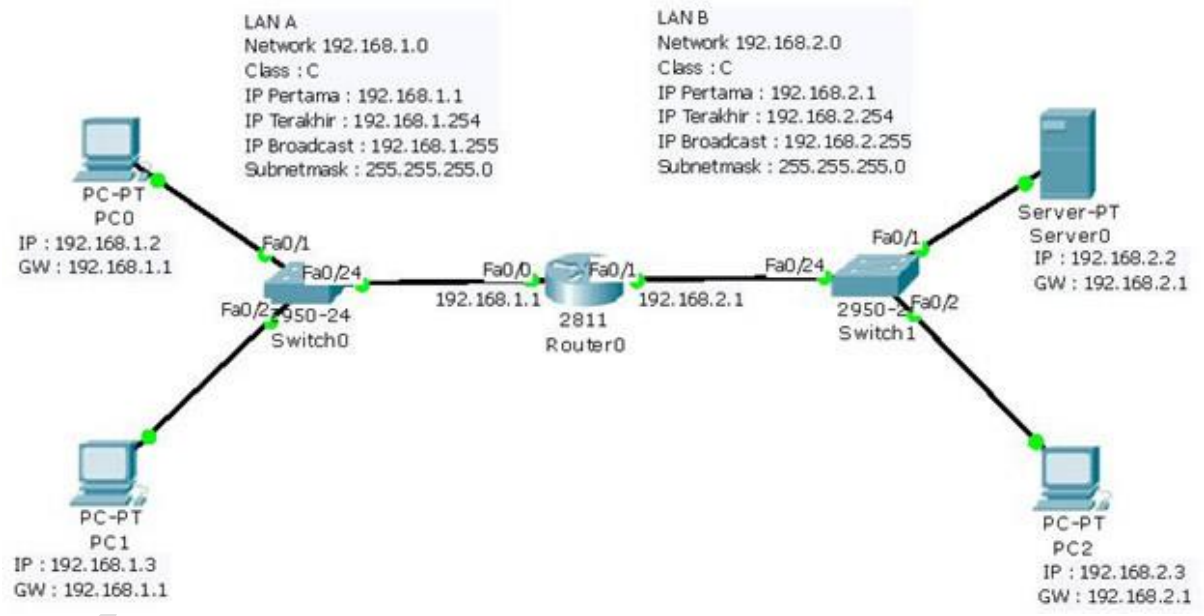
b) Memverifikasi penerapan ACL pada interface

```
# show ip interface type number
```

Perhatikan output dari eksekusi perintah tersebut dibagian baris *incoming access-list* dan *outgoing access-list*.

2. Studi Kasus penggunaan Extended ACL.

Terdapat sebuah jaringan dengan gambar topologi dan pengalamatan IP seperti terlihat pada gambar dibawah ini:



Adapun beberapa skenario konfigurasi Extended ACL yang akan diterapkan pada Router0 adalah mengijinkan akses dari LAN A hanya ke Server 0, dan mengijinkan akses http, ping dari LAN A ke Server 0, dan membalas permintaan ping dari PC 2 ke LAN A.

Solusi:

Mengijinkan akses dari LAN A hanya ke Server 0

a) Membuat ACL Extended untuk mengijinkan akses dari LAN A yaitu 192.168.1.0 ke Server 0 dengan alamat IP 192.168.2.2

```
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.2 0.0.0.0
```

b) Menerapkan ACL Extended yang telah dibuat pada interface fastethernet0/0 menggunakan perintah ip access-group.

```
interface f0/0

ip access-group 100 in
```

c) Memverifikasi ACL Extended yang telah dibuat menggunakan perintah:
```
show ip access-list
```
d) Memverifikasi penerapan ACL Extended pada interface fastethernet0/0 menggunakan perintah:
```
show ip interface fastethernet0/0
```

Mengijinkan akses http, ping dari LAN A ke Server 0, dan membalas permintaan ping dari PC 2 ke LAN A

a) Membuat ACL Extended untuk mengijinkan akses http dari LAN A yaitu 192.168.1.0 ke Server 0 dengan alamat IP 192.168.2.2

```
access-list 101 permit tcp 192.168.1.0 0.0.0.255 192.168.2.2 0.0.0.0 eq 80
```

b) Membuat ACL Extended untuk mengijinkan ping dari LAN A yaitu 192.168.1.0 ke Server 0 dengan alamat IP 192.168.2.2

```
access-list 101 permit icmp 192.168.1.0 0.0.0.255 192.168.2.2 0.0.0.0
```

c) Membuat ACL Extended untuk membalas permintaan ping dari PC2 dengan alamat 192.168.2.3 ke LAN A yaitu 192.168.1.0

```
access-list 101 permit icmp 192.168.1.0 0.0.0.255 192.168.2.3 0.0.0.0
```

d) Menerapkan ACL Extended yang telah dibuat ke interface fastethernet0/0 menggunakan perintah ip access-group:

```
int f0/0
ip access-group 101 in
```

e) Memverifikasi ACL Extended yang telah dibuat menggunakan perintah:

```
#show ip access-list
```

f) Memverifikasi penerapan ACL Extended pada interface fastethernet0/0 menggunakan perintah:

```
# show ip interface fastethernet0/0
```

Tugas:

Berdasarkan topologi jaringan pada studi kasus diatas, buatlah konfigurasi extended ACL dengan ketentuan sebagai berikut:

1. Mengijinkan akses FTP hanya dari host PC1 di LAN A ke Server0 di LAN B.
2. Mengijinkan akses SMTP, dan POP3 dari seluruh host di LAN A ke Server0 di LAN B.

BAB IV

STUDI KASUS FIREWALL I
ACL PADA SINGLE DUAL-HOMED FIREWALL

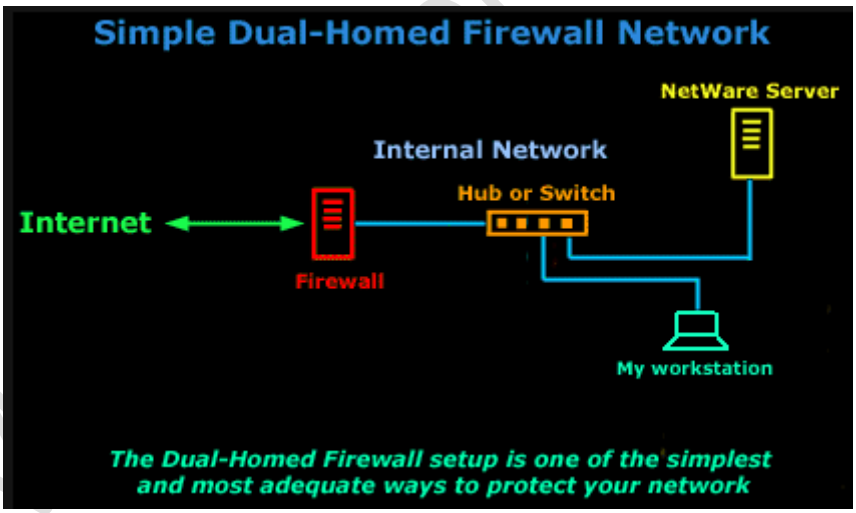
Tujuan:

Mahasiswa memahami penerapan ACL pada topologi Single Dual-Homed Firewall.

Materi:

1. Pengenalan Topologi Firewall Simple Dual-Homed

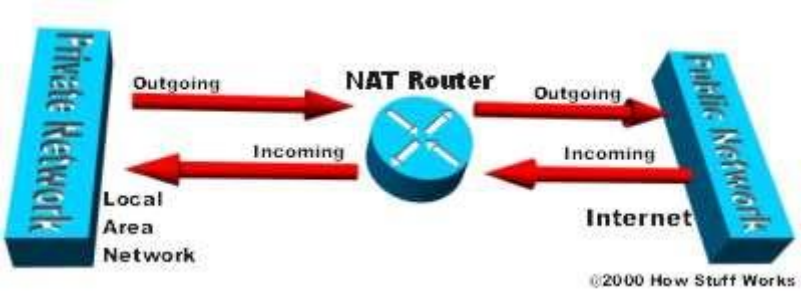
Dual-homed firewall merupakan salah satu dari firewall yang paling sederhana dan umum digunakan. Dual-homed mengacu pada dua jaringan dimana interface router terhubung secara langsung yaitu satu interface terhubung ke jaringan dalam, dan satu interface terhubung ke jaringan luar sebagai contoh Internet, seperti terlihat pada gambar berikut:



Gambar Dual Home Firewall (Sumber: www.firewall.cx)

Firewall yang diterapkan pada router akan menganalisa lalu lintas paket data diantara jaringan dalam (internal) ke Internet, dan sebaliknya. Jaringan internal pada LAN umumnya menggunakan pengalamatan IP Private, sedangkan jaringan Internet menggunakan alamat IP Publik. Agar dapat host-host di LAN yang menggunakan alamat IP Private dapat melakukan akses Internet maka diperlukan konfigurasi NAT pada router.

NAT merupakan proses untuk mentranslasikan sebuah alamat tertentu menjadi alamat lainnya. Router NAT mentranslasi trafik yang masuk dan yang meninggalkan jaringan private, seperti terlihat pada gambar berikut:



Menurut RFC 1631, pada dasarnya NAT memungkinkan sebuah perangkat seperti router bertindak sebagai perantara antara jaringan Internet dan local. Hal ini berarti hanya sebuah alamat IP unik yang dibutuhkan untuk merepresentasikan sekumpulan komputer ke jaringan luar. Terdapat beberapa alasan untuk menggunakan NAT yaitu:

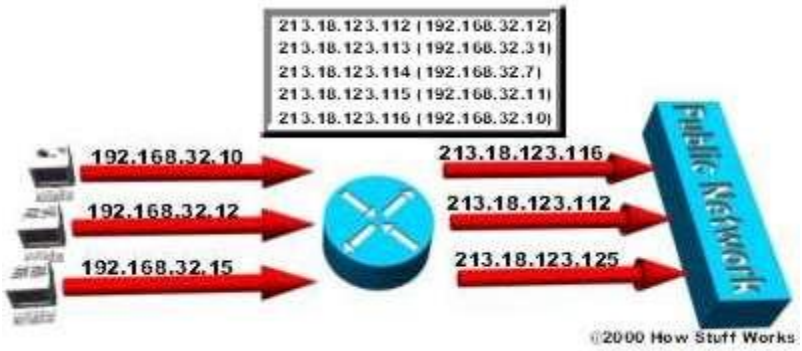
- Kekurangan alamat IP.
- Keamanan.
- Administrasi.

Terdapat 3 jenis NAT pada Cisco Router yaitu:

a) Static NAT (SNAT)
   Digunakan untuk memetakan satu alamat IP Private ke satu alamat IP Public (satu-ke-satu).

   Pada gambar static NAT diatas, terlihat komputer dengan alamat IP 192.168.32.10 akan ditranslasi menjadi 213.18.123.110.

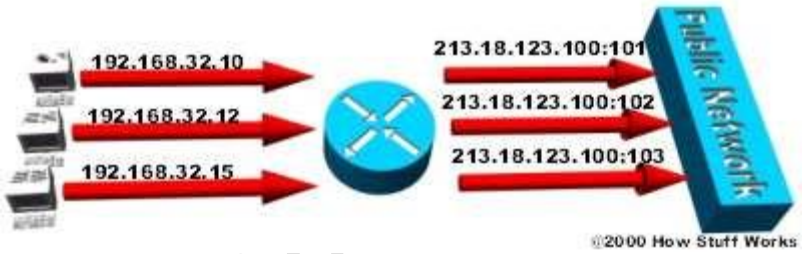
b) Dynamic NAT (DNAT)
   Digunakan untuk memetakan alamat IP Private ke alamat IP Public dari sekumpulan/sekelompok alamat IP Public. DNAT melakukan translasi satu-ke-satu antara alamat IP Private ke alamat IP Public sejumlah alamat IP Public yang terdapat pada pool (jangkauan alamat IP Public yang dimiliki).



Pada gambar dynamic NAT diatas terlihat komputer dengan alamat IP 192.168.32.10 akan ditranslasi ke alamat IP pertama yang terdapat pada jangkauan alamat 213.18.123.100 sampai dengan 213.18.123.150.

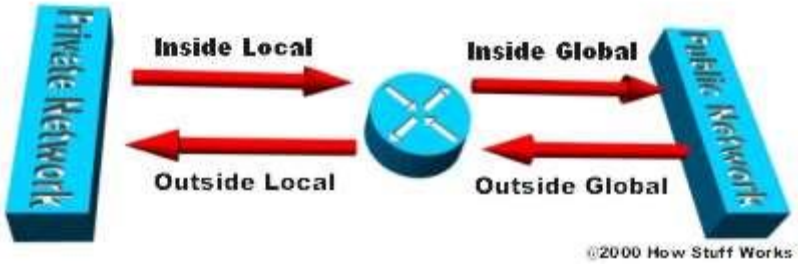
c) NAT Overload/Port Address Translation (PAT)

Merupakan bentuk dari Dynamic NAT yang memetakan seluruh alamat IP Private ke sebuah alamat IP Public dengan menggunakan nomor port yang berbeda.



Pada gambar NAT overload diatas, terlihat masing-masing komputer pada jaringan private akan ditranslasi menggunakan alamat IP yang sama yaitu 213.18.123.100, tetapi dengan nomor port yang berbeda.

Alamat IP memiliki penandaan berbeda bergantung pada apakah berada pada jaringan private, atau pada jaringan public (Internet), dan apakah trafik tersebut masuk atau keluar, seperti terlihat pada gambar berikut:



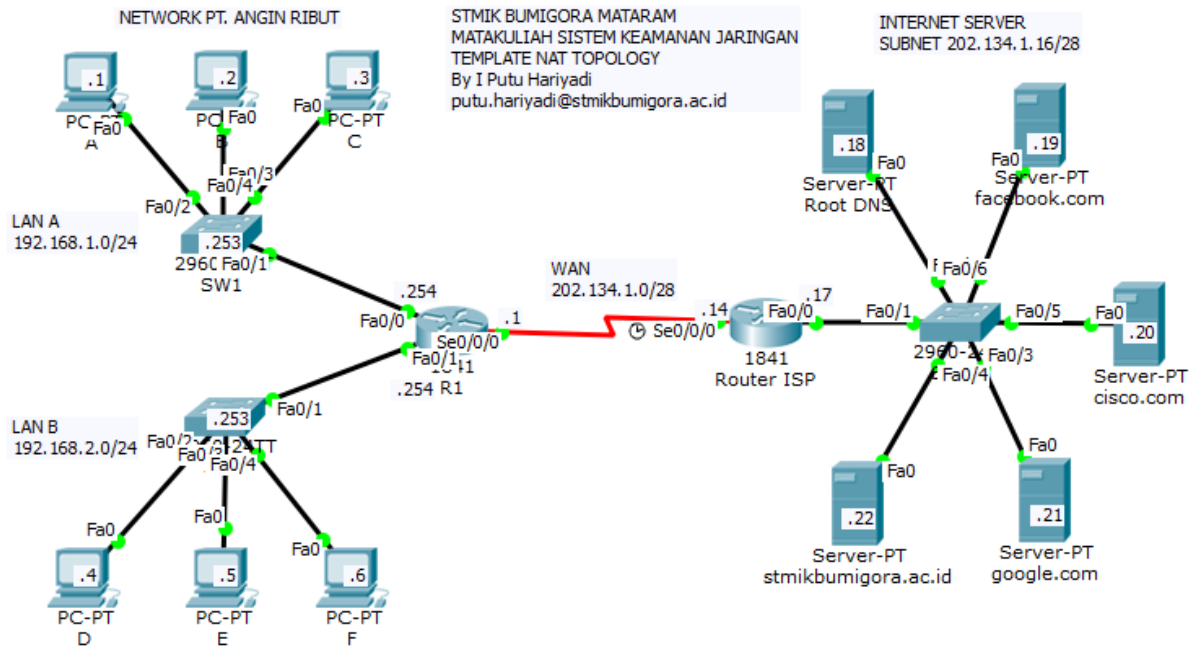
Cisco mendefinisikan menjadi 4 terminologi berikut:

- Inside local address, merupakan alamat IP yang diberikan ke host di jaringan dalam.

- Inside global address, merupakan alamat IP yang diberikan oleh Network Information Center (NIC) atau ISP yang merepresentasikan satu atau lebih dari satu alamat IP jaringan dalam ke jaringan luar.
- Outside local address, merupakan alamat IP dari host jaringan luar yang terlihat pada jaringan dalam.
- Outside global address, merupakan alamat IP yang diberikan ke host pada jaringan luar oleh pemilik host. Alamat dialokasikan dari alamat IP Public.

Sumber referensi: www.howstuffworks.com/nat.htm, dan www.cisco.com.

Praktikum NAT menggunakan topology dengan desain seperti terlihat pada gambar berikut:



File template topology dengan desain tersebut telah dibuatkan menggunakan Cisco Packet Tracer 6.2 yaitu dengan nama "*Template NAT Topology.pkt*". Sandi atau password login yang digunakan pada file template tersebut adalah sebagai berikut:

a) Console: cisco
b) Privilege: sanfran
c) Telnet: sanjose

PRAKTIKUM KONFIGURASI STATIC NAT PADA ROUTER R1

Static NAT digunakan untuk mengijinkan host-host tertentu pada jaringan PT. Angin Ribut agar dapat mengakses Internet dengan cara mentranslasikan satu alamat IP Private dari sebuah host ke satu alamat IP Public (satu-ke-satu), yaitu PC A pada LAN A dengan alamat

IP Private 192.168.1.2 ditranslasikan ke alamat IP Public 202.134.1.2, dan PC D pada LAN B dengan alamat IP Private 192.168.2.4 ditranslasikan ke alamat IP Public 202.134.1.3. Adapun tahapan-tahapan konfigurasinya adalah sebagai berikut:

1. Mengatur default route melalui global configuration mode.

   ```
   R1# conf t

   R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0
   ```

2. Mengaktifkan fitur NAT pada masing-masing interface yang terhubung ke jaringan yang diijinkan untuk mengakses Internet. Jaringan Dalam adalah **inside**, sedangkan jaringan luar adalah **outside**.
   a. Interface F0/0 yg terhubung ke LAN A

      ```
      R1(config)# int f0/0

      R1(config-if)# ip nat inside
      ```

   b. Interface f0/1 yg terhubung ke LAN B

      ```
      R1(config-if)# int f0/1

      R1(config-if)# ip nat inside
      ```

   c. Interface serial0/0/0 yg terhubung ke Internet

      ```
      R1(config-if)# int s0/0/0

      R1(config-if)# ip nat outside
      ```

      Berpindah ke satu mode sebelumnya:

      ```
      R1(config-if)# exit
      ```

3. Membuat static NAT untuk PC A dan PC D menggunakan perintah dengan sintak penulisan sebagai berikut:

   (config)# ip nat inside source static *alamat-ip-private alamat-ip-public*

   Dimana:

   - *alamat-ip-private* adalah alamat IP private dari host di jaringan dalam yang akan ditranslasi.
   - *alamat-ip-public* adalah alamat IP public untuk host di jaringan dalam agar dapat mengakses Internet.

Sehingga untuk membuat static NAT untuk PC A dengan alamat IP Private 192.168.1.1 yang ditranslasikan ke alamat IP Public 202.134.1.2, perintahnya adalah sebagai berikut:

```
R1(config)# ip nat inside source statis 192.168.1.1
202.134.1.2
```

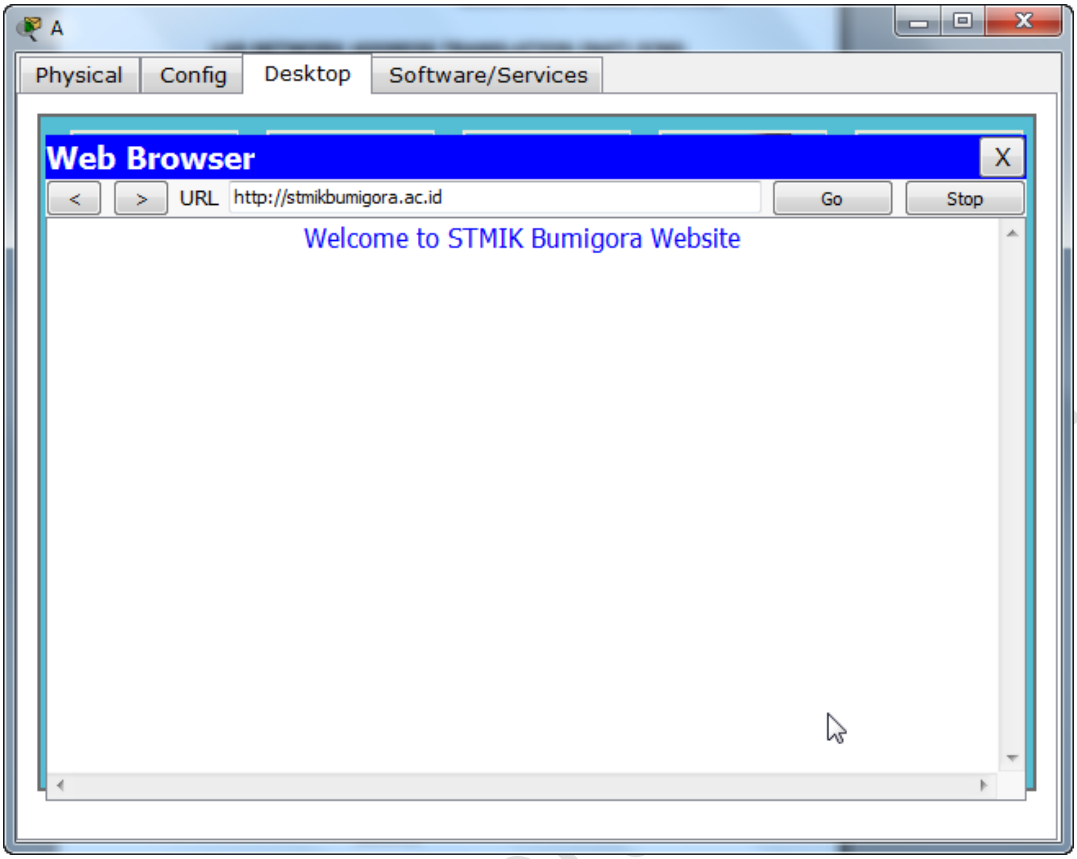
Selanjutnya untuk membuat static NAT untuk PC D dengan alamat IP Private 192.168.2.4 yang ditranslasikan ke alamat IP Public 202.134.1.3, perintahnya adalah sebagai berikut:

```
R1(config)# ip nat inside source statis 192.168.2.4
202.134.1.3
```

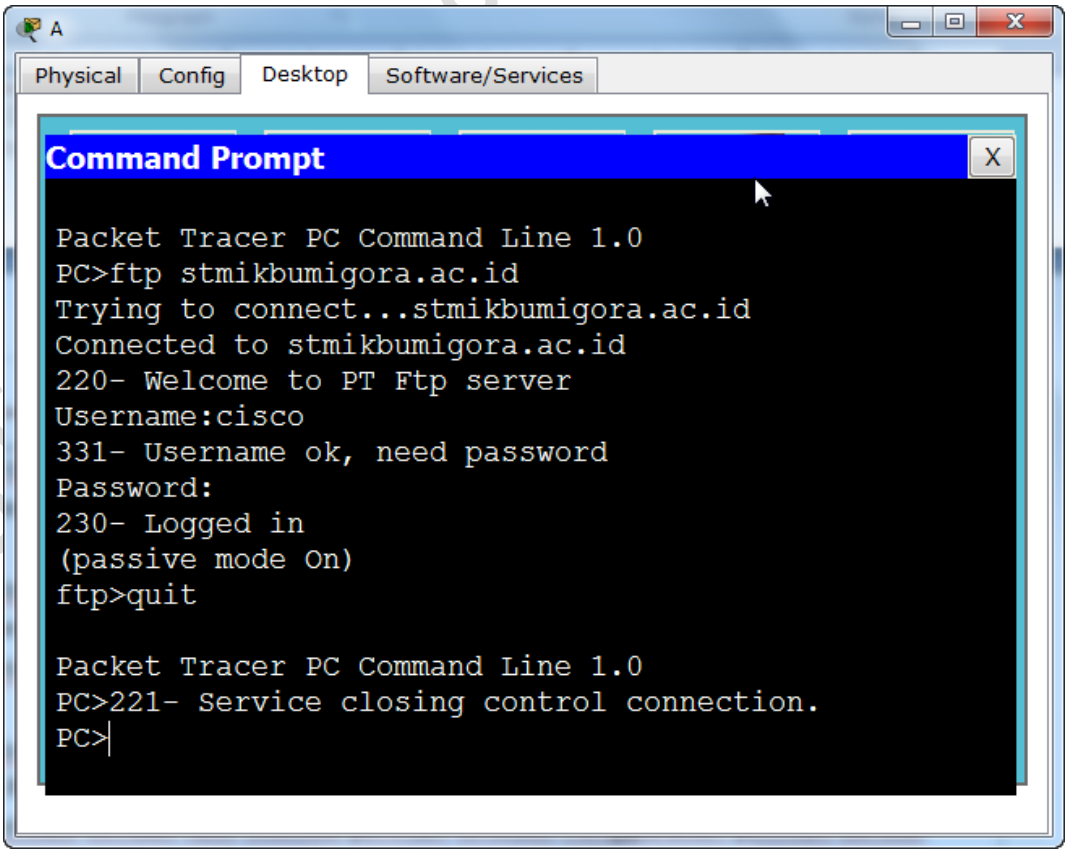
Berpindah ke privilege mode:

```
R1(config)# end
```

4. Verifikasi hasil konfigurasi menggunakan perintah berikut:
   ```
   R1# show run
   ```
5. Menampilkan informasi tabel translasi NAT
   ```
   R1#show ip nat translations
   Pro  Inside global     Inside local       Outside local      Outside global
   ---  202.134.1.2       192.168.1.1        ---                ---
   ---  202.134.1.3       192.168.2.4        ---                ---
   ```
   Terlihat tabel translasi NAT telah terbentuk untuk masing-masing host.
6. Melakukan ujicoba konfigurasi SNAT yang telah dilakukan sebelumnya dengan cara mengakses layanan-layanan dari server Internet sebagai contoh HTTP melalui browser dari PC A dan PC D ke situs *http://facebook.com, http://google.com, http://cisco.com,* atau *http://stmikbumigora.ac.id*. Apabila PC A, dan PC D dapat mengakses layanan HTTP dari server Internet tersebut maka konfigurasi telah berhasil ☺, salah satunya seperti terlihat pada gambar berikut:



Uji coba juga dapat dilakukan dengan mengakses layanan FTP dari masing-masing server Internet, salah satunya seperti terlihat pada gambar berikut:



Host-host selain PC A, dan D tidak akan dapat mengakses layanan Internet.

7. Informasi translasi NAT sebagai akibat dari pengaksesan layanan-layanan yang ada di Internet oleh PC A, dan PC D pada jaringan PT. Angin Ribut dapat dilihat menggunakan perintah berikut:

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
udp 202.134.1.2:1025   192.168.1.1:1025   202.134.1.18:53    202.134.1.18:53
udp 202.134.1.2:1026   192.168.1.1:1026   202.134.1.18:53    202.134.1.18:53
udp 202.134.1.3:1025   192.168.2.4:1025   202.134.1.18:53    202.134.1.18:53
---  202.134.1.2       192.168.1.1        ---                ---
---  202.134.1.3       192.168.2.4        ---                ---
tcp 202.134.1.2:1025   192.168.1.1:1025   202.134.1.21:80    202.134.1.21:80
tcp 202.134.1.2:1026   192.168.1.1:1026   202.134.1.21:80    202.134.1.21:80
tcp 202.134.1.3:1025   192.168.2.4:1025   202.134.1.22:80    202.134.1.22:80
```

8. Informasi statistic translasi NAT dapat dilihat menggunakan perintah berikut:

```
R1#show ip nat statistics
Total translations: 8 (2 static, 6 dynamic, 6 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: FastEthernet0/0 , FastEthernet0/1
Hits: 22  Misses: 6
Expired translations: 0
Dynamic mappings:
```

9. Informasi translasi NAT yang terbentuk dapat dihapus menggunakan perintah berikut:

```
R1# clear ip nat translation *
```

Verifikasi kembali hasil eksekusi perintah tersebut menggunakan perintah berikut:

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  202.134.1.2       192.168.1.1        ---                ---
---  202.134.1.3       192.168.2.4        ---                ---
```

PRAKTIKUM KONFIGURASI DYNAMIC NAT PADA ROUTER R1

Dynamic NAT digunakan untuk mengijinkan hanya 4 host pada jaringan PT. Angin Ribut baik dari LAN A 192.168.1.0/24 maupun LAN B 192.168.2.0/24 agar dapat mengakses Internet menggunakan 4 alamat IP Public yang dimiliki yaitu **202.134.1.2 - 202.134.1.5,** secara berkompetisi menggunakan metode **First-Come First-Served (FCFS)**. Hanya 4 host yang pertama kali melakukan koneksi ke Internet yang akan dapat melakukan akses Internet, sebaliknya yang lainnya ditolak karena alokasi alamat IP Public hanya tersedia 4 alamat. Adapun tahapan-tahapan konfigurasinya adalah sebagai berikut:

1. Mengatur default route melalui global configuration mode.

```
R1# conf t

R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0
```

2. Mengaktifkan fitur NAT pada masing-masing interface yang terhubung ke jaringan yang diijinkan untuk mengakses Internet
    a. Interface F0/0 yg terhubung ke LAN A

    ```
    R1(config)# int f0/0

    R1(config-if)# ip nat inside
    ```

    b. Interface f0/1 yg terhubung ke LAN B

    ```
    R1(config-if)# int f0/1

    R1(config-if)# ip nat inside
    ```

    c. Interface serial0/0/0 yg terhubung ke Internet

    ```
    R1(config-if)# int s0/0/0

    R1(config-if)# ip nat outside
    ```

    Berpindah ke satu mode sebelumnya:

    ```
    R1(config-if)# exit
    ```

3. Mengatur NAT POOL yang memuat jangkauan (*ranges*) alamat IP Public yang dialokasikan ke client menggunakan perintah dengan sintak penulisan sebagai berikut:
    `(config)#` **`ip nat pool`** *`nama-pool awal-alamat-ip-public akhir-alamat-ip-public`* **`netmask`** *`alamat-subnetmask`*
    Dimana:
    - *nama-pool*, adalah nama yang digunakan untuk mengidentifikasi jangkauan alamat IP Public yang dialokasikan ke host-host di jaringan dalam.
    - *awal-alamat-ip-public*, adalah alamat IP Public pertama yang dialokasikan.
    - *akhir-alamat-ip-public*, adalah alamat IP Public terakhir yang dialokasikan.
    - *alamat-subnetmask*, adalah alamat subnetmask dari alamat IP Public yang dialokasikan.

    Sehingga untuk membuat NAT Pool dengan nama "**allow_internet**" yang memuat 4 alamat IP Public yaitu **202.134.1.2-202.134.1.5** dengan subnetmask 255.255.255.240, perintahnya adalah sebagai berikut:
    ```
    (config)# ip nat pool allow_internet 202.134.1.2 202.134.1.5 netmask 255.255.255.240
    ```
4. Membuat ACL jenis standard yang mengijinkan host-host di LAN A & LAN B untuk mengakses Internet.
    a. Mengijinkan LAN A dengan alamat jaringan 192.168.1.0/24

```
R1(config)#   access-list   1   permit   192.168.1.0
0.0.0.255
```

b. Mengijinkan LAN B dengan alamat jaringan 192.168.2.0/24

```
R1(config)#   access-list   1   permit   192.168.2.0
0.0.0.255
```

5. Menerapkan ACL yang telah dibuat sebelumnya pada NAT menggunakan perintah dengan sintak penulisan sebagai berikut:

   (config)# ip nat inside source list *nomor-acl* **pool** *nama-pool*

   Dimana:

   - *nomor-acl* adalah nomor Access Control List yang akan diterapkan pada NAT.
   - *nama-pool* adalah nama pool yang memuat jangkauan alamat IP Public yang dapat digunakan untuk mentranslasikan alamat IP private dari host yang mengakses Internet.

   Sehingga untuk menerapkan ACL nomor 1 dan pool dengan nama "allow_internet" yang telah dibuat sebelumnya pada NAT, perintahnya adalah sebagai berikut:

   ```
   R1(config)#   ip   nat   inside   source   list   1   pool
   allow_internet
   ```

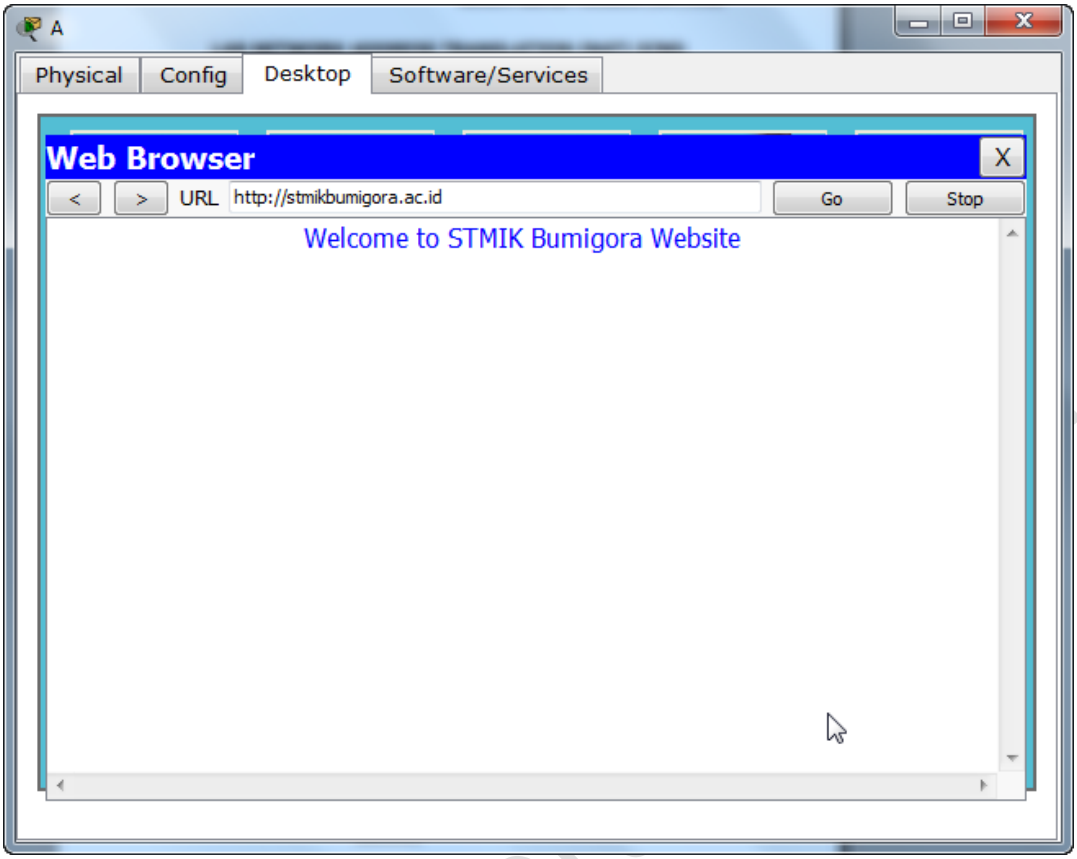
   Berpindah ke privilege mode:

   ```
   R1(config)# end
   ```

6. Verifikasi hasil konfigurasi menggunakan perintah berikut:
   ```
   R1# show run
   ```
7. Menampilkan informasi tabel translasi NAT

   ```
   R1# show ip nat translation
   ```

   Tabel translasi NAT akan terbentuk ketika terdapat host yang mengakses Internet.
8. Melakukan ujicoba konfigurasi Dynamic NAT yang telah dilakukan sebelumnya dengan cara mengakses layanan-layanan pada server Internet sebagai contoh HTTP melalui browser dari 4 host yaitu PC A, B, dan C yang berada di LAN A, dan PC D yang berada di LAN B. Apabila 4 host tersebut dapat mengakses layanan HTTP dari server Internet maka konfigurasi telah berhasil ☺, salah satunya seperti terlihat pada gambar berikut:



Selanjutnya lakukan percobaan akses Internet dari PC E/F, maka akan diperoleh hasil host tersebut tidak dapat melakukan akses Internet.

9. Informasi translasi NAT sebagai akibat dari pengaksesan layanan-layanan yang ada di Internet oleh host A, B, C, dan D pada jaringan PT. Angin Ribut dapat dilihat menggunakan perintah berikut:

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
udp 202.134.1.2:1025   192.168.1.1:1025   202.134.1.18:53    202.134.1.18:53
udp 202.134.1.2:1026   192.168.1.1:1026   202.134.1.18:53    202.134.1.18:53
udp 202.134.1.3:1025   192.168.1.2:1025   202.134.1.18:53    202.134.1.18:53
udp 202.134.1.3:1026   192.168.1.2:1026   202.134.1.18:53    202.134.1.18:53
udp 202.134.1.5:1025   192.168.1.3:1025   202.134.1.18:53    202.134.1.18:53
udp 202.134.1.4:1025   192.168.2.4:1025   202.134.1.18:53    202.134.1.18:53
tcp 202.134.1.2:1025   192.168.1.1:1025   202.134.1.21:80    202.134.1.21:80
tcp 202.134.1.2:1026   192.168.1.1:1026   202.134.1.21:80    202.134.1.21:80
tcp 202.134.1.3:1025   192.168.1.2:1025   202.134.1.19:80    202.134.1.19:80
tcp 202.134.1.3:1026   192.168.1.2:1026   202.134.1.19:80    202.134.1.19:80
tcp 202.134.1.5:1025   192.168.1.3:1025   202.134.1.20:80    202.134.1.20:80
tcp 202.134.1.4:1025   192.168.2.4:1025   202.134.1.22:80    202.134.1.22:80
```

Perhatian pada bagian kolom "Inside global", terlihat 4 alamat IP Public telah teralokasi masing-masing untuk PC A (202.134.1.2), PC B (202.134.1.3), PC C (202.134.1.4), PC D (202.134.1.5), sehingga host-host lainnya tidak akan dapat mengakses Internet.

10. Informasi statistic translasi NAT dapat dilihat menggunakan perintah berikut:

```
R1#show ip nat statistic
Total translations: 6 (0 static, 6 dynamic, 6 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: FastEthernet0/0 , FastEthernet0/1
Hits: 43  Misses: 12
Expired translations: 6
Dynamic mappings:
-- Inside Source
access-list 1 pool allow_internet refCount 6
 pool allow_internet: netmask 255.255.255.240
       start 202.134.1.2 end 202.134.1.5
       type generic, total addresses 4 , allocated 4 (100%), misses 0
```

11. Informasi translasi NAT yang terbentuk dapat dihapus menggunakan perintah berikut:

    ```
    R1# clear ip nat translation *
    ```

    Verifikasi kembali hasil eksekusi perintah tersebut menggunakan perintah berikut:

    ```
    R1# show ip nat translations
    ```

PRAKTIKUM KONFIGURASI PORT ADDRESS TRANSLATION (PAT) PADA ROUTER R1

PAT digunakan untuk mengijinkan seluruh host pada jaringan PT. Angin Ribut baik dari LAN A 192.168.1.0/24 maupun LAN B 192.168.2.0/24 agar dapat mengakses Internet menggunakan alamat IP Public dari interface **serial0/0/0** di router R1 yaitu 202.134.1.1. Adapun tahapan-tahapan konfigurasinya adalah sebagai berikut:

1. Mengatur default route melalui global configuration mode.

   ```
   R1# conf t

   R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0
   ```

2. Mengaktifkan fitur NAT pada masing-masing interface yang terhubung ke jaringan yang diijinkan untuk mengakses Internet
   a. Interface F0/0 yg terhubung ke LAN A

      ```
      R1(config)# int f0/0

      R1(config-if)# ip nat inside
      ```

   b. Interface f0/1 yg terhubung ke LAN B

      ```
      R1(config-if)# int f0/1

      R1(config-if)# ip nat inside
      ```

   c. Interface serial0/0/0 yg terhubung ke Internet

      ```
      R1(config-if)# int s0/0/0
      ```

```
R1(config-if)# ip nat outside
```

Berpindah ke satu mode sebelumnya:

```
R1(config-if)# exit
```

3. Membuat ACL jenis standard yang mengijinkan host-host di LAN A & LAN B untuk mengakses Internet.
   c. Mengijinkan LAN A dengan alamat jaringan 192.168.1.0/24

```
R1(config)# access-list 1 permit 192.168.1.0
0.0.0.255
```

   d. Mengijinkan LAN B dengan alamat jaringan 192.168.2.0/24

```
R1(config)# access-list 1 permit 192.168.2.0
0.0.0.255
```

4. Menerapkan ACL yang telah dibuat sebelumnya pada PAT menggunakan perintah dengan sintak penulisan sebagai berikut:

   (config)# ip nat inside source list *nomor-acl* **interface** *nama-interface* **overload**

   Dimana:

   - *nomor-acl* adalah nomor Access Control List.
   - *nama-interface* adalah nama interface yang memiliki alamat IP Public atau interface yang menghubungkan ke Internet.

   Sehingga untuk menerapkan ACL nomor 1 yan telah dibuat sebelumnya pada interface s0/0/0 yang merupakan interface dengan alamat IP public yang akan dibagi pakai untuk semua (*overload*):

```
R1(config)# ip nat inside source list 1 interface s0/0/0
overload
```

   Berpindah ke privilege mode:

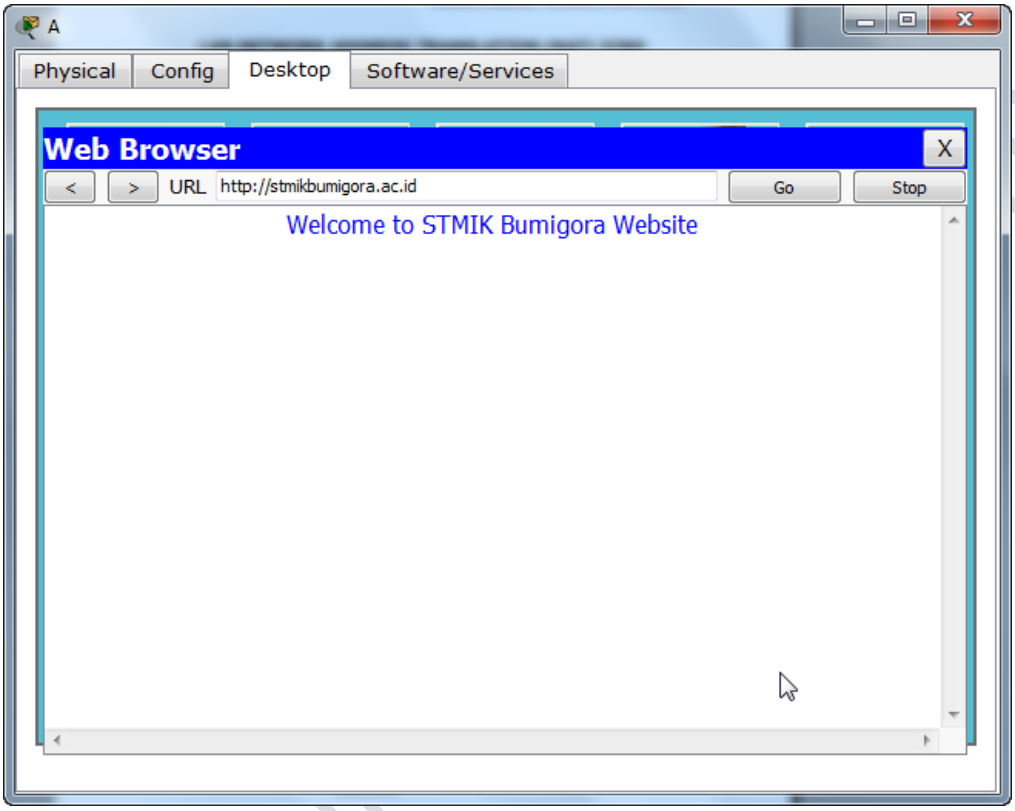
```
R1(config)# end
```

5. Verifikasi hasil konfigurasi menggunakan perintah berikut:
   `R1# show run`
6. Menampilkan informasi tabel translasi NAT

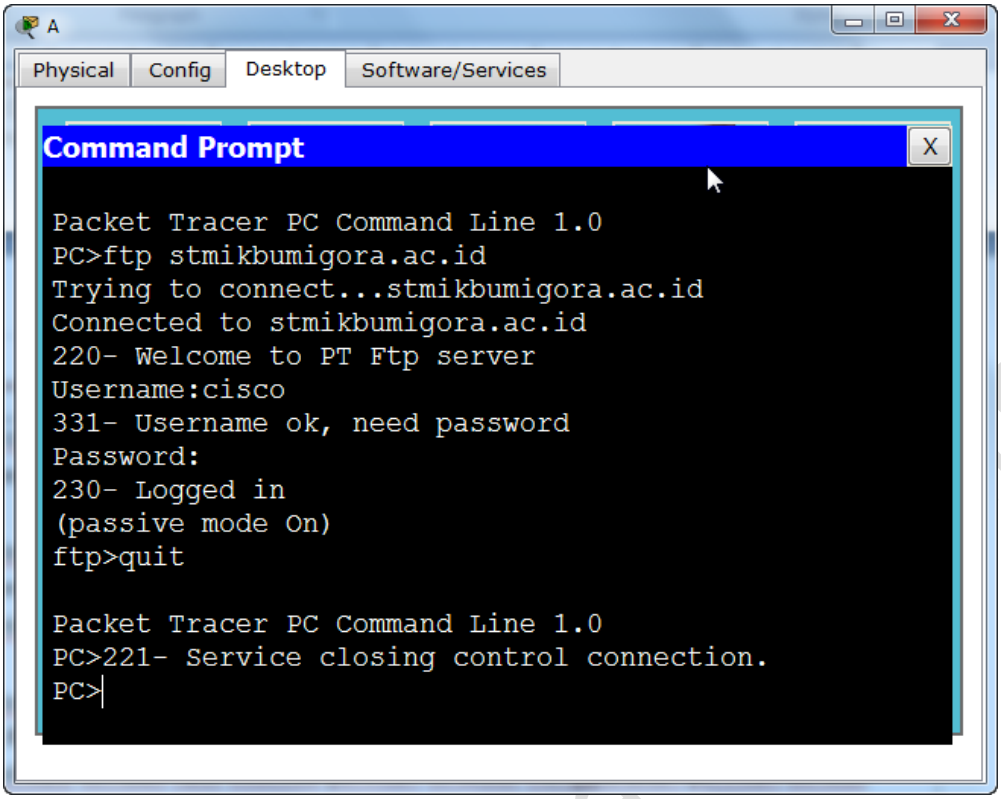
```
R1# show ip nat translation
```

   Tabel translasi NAT akan terbentuk ketika terdapat host yang mengakses Internet.

7. Melakukan ujicoba konfigurasi PAT yang telah dilakukan sebelumnya dengan cara mengakses layanan HTTP dari server Internet melalui browser dari masing-masing host baik di LAN A maupun B, yaitu ke situs *http://facebook.com, http://google.com, http://cisco.com, http://stmikbumigora.ac.id*. Apabila seluruh host dapat mengakses layanan HTTP dari server Internet maka konfigurasi telah berhasil ☺, salah satunya seperti terlihat pada gambar berikut:



Uji coba juga dapat dilakukan dengan mengakses layanan FTP dari masing-masing server Internet, salah satunya seperti terlihat pada gambar berikut:



8. Informasi translasi NAT sebagai akibat dari pengaksesan layanan-layanan yang ada di Internet oleh host-host pada jaringan PT. Angin Ribut dapat dilihat menggunakan perintah berikut:

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
udp 202.134.1.1:1025   192.168.1.1:1025   202.134.1.18:53    202.134.1.18:53
udp 202.134.1.1:1026   192.168.1.1:1026   202.134.1.18:53    202.134.1.18:53
udp 202.134.1.1:1027   192.168.1.1:1027   202.134.1.18:53    202.134.1.18:53
tcp 202.134.1.1:1025   192.168.1.1:1025   202.134.1.22:80    202.134.1.22:80
tcp 202.134.1.1:1026   192.168.1.1:1026   202.134.1.22:80    202.134.1.22:80
tcp 202.134.1.1:1027   192.168.1.1:1027   202.134.1.22:21    202.134.1.22:21
```

9. Informasi statistic translasi NAT dapat dilihat menggunakan perintah berikut:

```
R1#show ip nat statistics
Total translations: 4 (0 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: FastEthernet0/0 , FastEthernet0/1
Hits: 29  Misses: 6
Expired translations: 2
Dynamic mappings:
```

10. Informasi translasi NAT yang terbentuk dapat dihapus menggunakan perintah berikut:

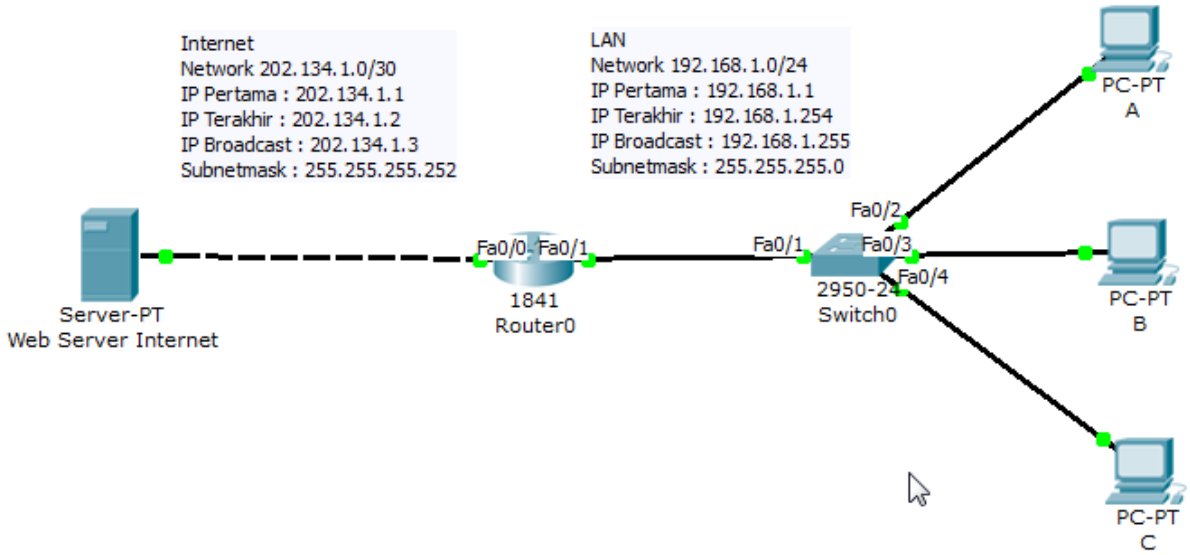
```
R1# clear ip nat translation *
```

Verifikasi kembali hasil eksekusi perintah tersebut menggunakan perintah berikut:

```
R1# show ip nat translations
```

2. Membangun topologi Simple Dual-Homed Firewall menggunakan Packet Tracer.

Buatlah topologi simple dual-homed firewall menggunakan program aplikasi Packet Tracer dengan ketentuan rancangan jaringan dan pengalamatan IP seperti terlihat pada gambar berikut:



Gambar Topologi Simple Dual-Homed Firewall

3. Konfigurasi & verifikasi ACL pada topologi Single Dual-Homed Firewall

Terdapat beberapa ketentuan pengaturan ACL yang harus dikonfigurasi pada Router0 sesuai dengan topologi yang digunakan yaitu mengijinkan akses Internet bagi seluruh host di LAN menggunakan alamat IP Publik dari interface Fastethernet0/0 dari router R0 yang dibagi pakai (*NAT Overload/PAT*).

```
(config)#int f0/0
(config-if)#ip nat outside
(config-if)#int f0/1
(config-if)#ip nat inside
(config-if)#exit
(config)#access-list 1 permit 192.168.1.0 0.0.0.255
(config)#ip nat inside source list 1 interface FastEthernet0/0
overload
```

Tugas:

Berdasarkan topologi jaringan diatas, buatlah konfigurasi ACL dengan ketentuan sebagai berikut:

1. Menolak akses Internet dari host dengan alamat IP 192.168.1.4-192.1681.7.
2. Mengijinkan akses telnet ke Router0 hanya dari LAN.

BAB V

STUDI KASUS FIREWALL II
ACL PADA TOPOLOGI FIREWALL TWO-LEGGED NETWORK WITH A FULLY EXPOSED DMZ

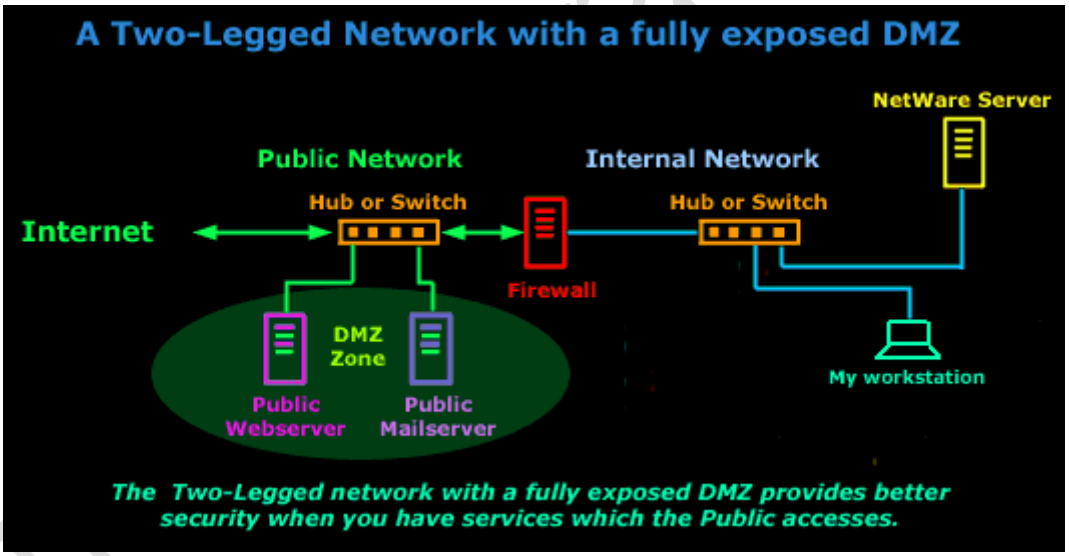
Tujuan:

Mahasiswa memahami penerapan ACL pada topologi Firewall Two-Legged Network with a Fully Exposed DMZ.

Materi:

1. Pengenalan Topologi Firewall Two-Legged Network with a Fully Exposed DMZ.

Pada topologi ini, router yang digunakan untuk mengakses ke Internet dihubungkan ke switch atau hub, seperti terlihat pada gambar berikut:

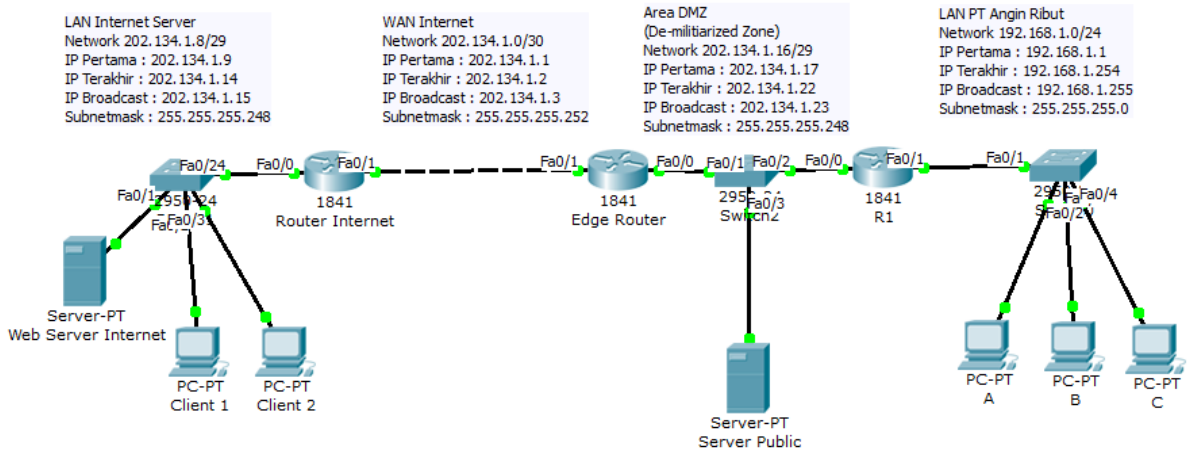


Gambar Two-Legged Network with a fully exposed DMZ (Sumber: www.firewall.cx)

Server-server yang terdapat di area DMZ dihubungkan langsung ke switch atau hub, dan tidak melalui pemfilteran oleh firewall, sehingga dapat diakses oleh pengguna dari Internet secara langsung. Firewall hanya memiliki dua interface yang terhubung ke Internal Network, dan ke Public Network melalui switch atau hub di area DMZ. Firewall hanya akan menganalisa lalu lintas paket data diantara jaringan dalam (internal) ke Internet, dan sebaliknya, tanpa melakukan pemfilteran atau pengaturan keamanan terkait server-server yang terdapat di area DMZ.

2. Membangun topologi firewall Two-Legged Network with a fully exposed DMZ menggunakan Packet Tracer.

Buatlah topologi firewall Two-Legged Network with a fully exposed DMZ menggunakan program aplikasi Packet Tracer dengan ketentuan rancangan jaringan dan pengalamatan IP seperti terlihat pada gambar berikut:



Gambar Topologi Firewall Two-Legged Network with a fully exposed DMZ

3. Konfigurasi & verifikasi ACL pada topologi Firewall Two-Legged Network with a fully exposed DMZ

Terdapat beberapa ketentuan pengaturan ACL yang harus dikonfigurasi pada router R1 sesuai dengan topologi yang digunakan yaitu mengijinkan akses Internet bagi seluruh host di LAN PT. Angin Ribut dengan menggunakan alamat IP Publik dari interface Fastethernet0/0 dari router R1 yang dibagi pakai (*NAT Overload/PAT*).

```
(config)#int f0/0
(config-if)#ip nat outside
(config-if)#int f0/1
(config-if)#ip nat inside
(config-if)#exit
(config)#access-list 1 permit 192.168.1.0 0.0.0.255
(config)#ip nat inside source list 1 interface FastEthernet0/0
overload
```

Tugas:

Berdasarkan topologi jaringan diatas, buatlah konfigurasi ACL dengan ketentuan sebagai berikut:

1. Mengijinkan akses Internet hanya bagi host dengan alamat IP Private 192.168.1.20 di LAN PT. Angin Ribut menggunakan alamat IP Publik 202.134.1.20 dengan metode Static NAT (SNAT).
2. Mengijinkan akses Internet hanya bagi 2 host di LAN PT. Angin Ribut secara berkompetisi menggunakan jangkauan alamat IP Publik 202.134.1.21-202.134.1.22 dengan metode Dynamic NAT (DNAT).

BAB VI

STUDI KASUS FIREWALL III
ACL PADA TOPOLOGI FIREWALL THREE-LEGGED NETWORK

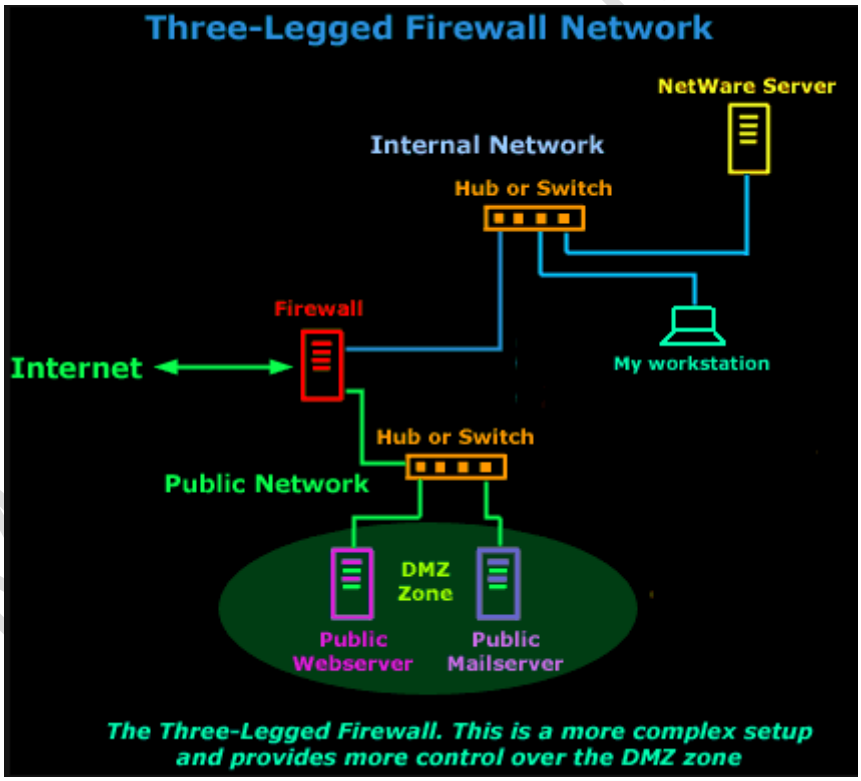
Tujuan:

Mahasiswa memahami penerapan ACL pada topologi Firewall Three-Legged Network.

Materi:

1. Pengenalan Topologi Three-Legged Firewall Network with DMZ.

Pada topologi ini, router memiliki 3 interface yang masing-masing terhubung ke jaringan Internal, jaringan DMZ, dan jaringan Internet, sehingga dikenal dengan istilah *Three-Legged*, seperti terlihat pada gambar berikut:

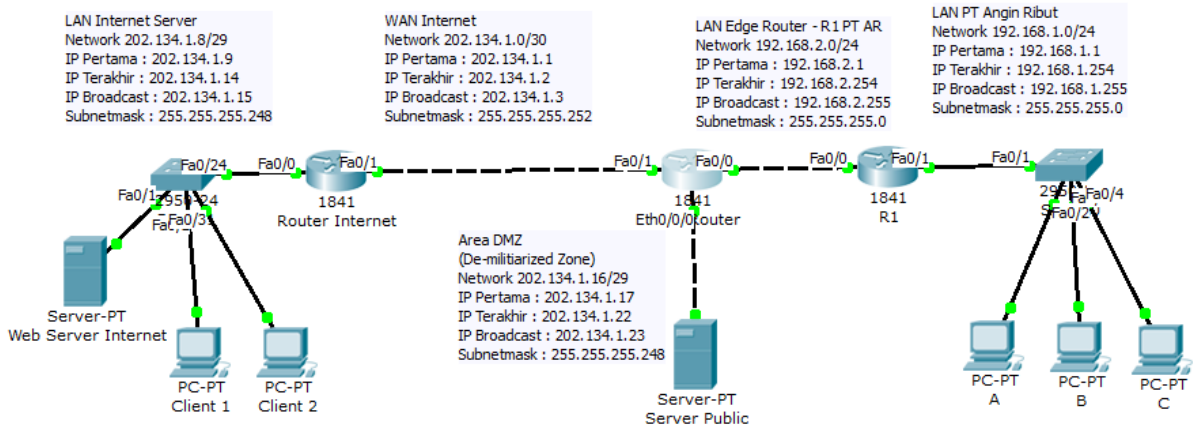


Gambar Three-Legged Firewall Network with DMZ (Sumber: www.firewall.cx)

Firewall dikonfigurasi untuk mengatur lalu lintas paket data dari jaringan internal ke jaringan Internet, dan jaringan DMZ.

2. Membangun topologi Three-Legged Firewall Network with DMZ menggunakan Packet Tracer.

Buatlah topologi Three-Legged firewall Network with DMZ menggunakan program aplikasi Packet Tracer dengan ketentuan rancangan jaringan dan pengalamatan IP seperti terlihat pada gambar berikut:



Gambar Topologi Three-Legged Firewall Network with DMZ

3. Konfigurasi & verifikasi ACL pada topologi Three-Legged Firewall Network DMZ

Terdapat beberapa ketentuan pengaturan ACL yang harus dikonfigurasi pada router yaitu sebagai berikut:

a) Mengatur default route pada Router Edge untuk merutekan paket dari jaringan internal ke Internet

```
Edge_Router(config)# ip route 0.0.0.0 0.0.0.0 202.134.1.2
```

b) Mengatur static route pada Router Edge untuk dapat mengakses LAN PT. Angin Ribut

```
Edge_Router(config)# ip route 192.168.1.0 255.255.255.0
192.168.2.2
```

c) Mengijinkan akses Internet bagi seluruh host di LAN PT. Angin Ribut

```
Edge_Router(config)# access-list 1 permit 192.168.1.0
0.0.0.255
Edge_Router(config)# ip nat inside source list 1 interface
fa0/1 overload
```

d) Mengijinkan akses layanan HTTP di Server Public PT. Angin Ribut dengan alamat IP 202.134.1.18 dari Internet dan LAN PT. Angin Ribut

```
Edge_Router(config)# access-list 100 permit tcp 0.0.0.0
255.255.255.255 202.134.1.18 0.0.0.0 eq 80
```

e) Menerapkan access-list 100 yang telah dibuat pada langkah sebelumnya pada *interface ethernet0/0/0* untuk arah "*outgoing*"

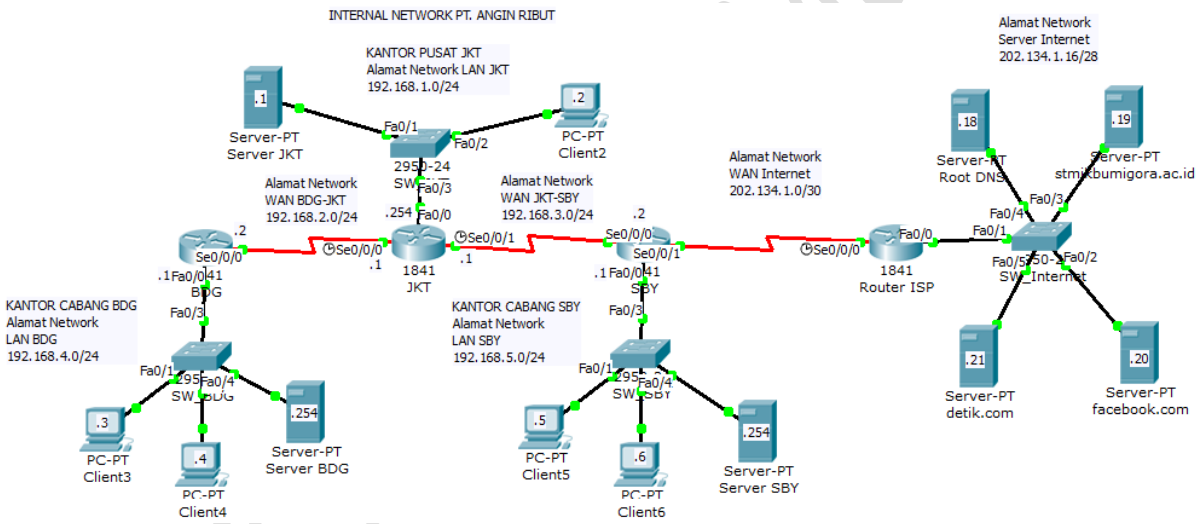
```
Edge_Router(config)# int e0/0/0
Edge_Router(config-if)# ip access-group 100 out
Edge_Router(config-if)# exit
```

f) Mengijinkan akses seluruh layanan di Server Public PT. Angin Ribut dari LAN PT. Angin Ribut

```
Edge_Router(config)# access-list 100 permit ip 192.168.1.0
0.0.0.255 202.134.1.18 0.0.0.0
```

Tugas:

Berdasarkan topologi jaringan seperti terlihat pada gambar dibawah ini, buat konfigurasi pada perangkat-perangkat terkait dengan ketentuan-ketentuan sebagai berikut:



1. Konfigurasi Routing Protokol RIP pada Router BDG, JKT, dan SBY agar antar jaringan internal kantor pusat dan cabang PT. Angin Ribut dapat saling berkomunikasi. Verifikasi komunikasi host antar jaringan menggunakan utilitas ping.
   Ping dari Client2 ke Client3 (192.168.4.3) -> SUKSES
   Ping dari Client2 ke Client5 (192.168.5.5) -> SUKSES
2. Konfigurasi NAT Overload/PAT pada Router SBY agar mengijinkan akses Internet hanya dari host-host pada LAN Kantor Cabang BDG. Verifikasi melalui browser dengan melakukan akses ke situs http://stmikbumigora.ac.id, http://facebook.com, http://detik.com. Akses Internet dari Client3, Client4, dan Server BDG di LAN Kantor Cabang BDG diijinkan, sebaliknya yang lainnya ditolak.
3. Konfigurasi ACL agar mengijinkan akses telnet pada masing-masing Router JKT, BDG, dan SBY dengan ketentuan sebagai berikut:

a) Router JKT

   Hanya mengijinkan telnet dari host Client2.

b) Router BDG

   Hanya mengijinkan telnet dari host Client2 dan Server BDG.

c) Router SBY

   Hanya mengijinkan telnet dari host Client2 dan Server SBY.

Verifikasi konfigurasi yang telah dilakukan dengan melakukan telnet dari masing-masing client yang diijinkan dan ditolak.

4. Konfigurasi ACL agar mengijinkan hanya host-host di LAN Kantor Cabang BDG dan LAN Kantor Cabang SBY yang dapat mengakses seluruh layanan HTTP, HTTPS, dan FTP pada Server BDG, sebaliknya menolak akses dari seluruh host di LAN Kantor Pusat JKT. Verifikasi konfigurasi yang telah dilakukan dengan melakukan akses HTTP, dan HTTPS melalui browser, serta FTP melalui command prompt baik dari host-host yang diijinkan maupun ditolak.
5. Konfigurasi ACL agar mengijinkan hanya host-host di LAN Kantor Cabang SBY dan LAN Kantor Cabang BDG yang dapat mengakses seluruh layanan HTTP, HTTPS, dan FTP pada Server SBY, sebaliknya menolak akses dari seluruh host di LAN Kantor Pusat JKT. Verifikasi konfigurasi yang telah dilakukan dengan melakukan akses HTTP, dan HTTPS melalui browser, serta FTP melalui command prompt baik dari host-host yang diijinkan maupun ditolak.

BAB VII

IPTABLES

IPTables digunakan untuk membuat, memelihara, dan menganalisa tabel-tabel aturan pemfilteran paket IP di kernel Linux. Fitur utama dari IPTables adalah *stateless packet filtering (IPv4 dan IPv6), stateful packet filtering (IPv4 dan IPv6), semua jenis Network Address dan Port Translation, memiliki infrastruktur yang fleksible dan dapat diperluas, memiliki beberapa lapisan API untuk ekstensi pihak ketiga, memiliki banyak plugin/modul*.

IPTables dapat digunakan untuk membangun firewall Internet berdasarkan pada stateless dan stateful packet filtering, untuk *Network Address Translation* (NAT) dan masquerading untuk berbagi pakai akses Internet, untuk implementasi transparent proxy, membantu utilitas *tc* dan *iproute2* untuk membangun *Quality of Services* (QoS) dan kebijakan pada router, melakukan manipulasi paket lanjutan (mangling) seperti mengubah bit TOS/DSCP/ECN dari header IP.

Pemrosesan Paket pada IPTables

Semua paket dianalisa oleh iptables melalui serangkaian tabel-tabel *built-in* (bawaan) untuk pemrosesan. Terdapat 3 tabel yaitu:

a) Tabel **Filter**, digunakan untuk melakukan pemfilteran paket. Terdapat 3 chain built-in, untuk menempatkan kebijakan aturan firewall, yaitu:
   ⇒ *Forward* Chain, memfilter paket ke server yang diproteksi oleh firewall.
   ⇒ *Input* Chain, memfilter paket yang ditujukan untuk firewall.
   ⇒ *Output* Chain, memfilter paket yang berasal dari firewall.
b) Tabel **NAT** (Network Address Translation), digunakan untuk melakukan translasi alamat jaringan. Tabel ini memiliki 2 chain bawaan, yaitu:
   ⇒ *Pre-routing* chain, melakukan NAT pada paket ketika alamat tujuan dari paket perlu diubah.
   ⇒ *Post-routing* chain, melakukan NAT pada paket ketika alamat sumber dari paket perlu diubah.

c) Tabel **Mangle**, digunakan untuk mengatur *Quality of Service (QoS)*.

Saat membuat aturan firewall menggunakan iptables, perlu ditentukan tipe tabel dan chain yang digunakan, defaultnya adalah tabel *filter*. Masing-masing aturan firewall menganalisa masing-masing paket IP dan selanjutnya mencoba untuk mengidentifikasi target. Setelah target diidentifikasi, paket perlu diproses lebih lanjut (jump).

Target yang digunakan oleh iptables antara lain:

Target	Keterangan
ACCEPT	IPTables menghentikan pemrosesan lanjutan, paket ditangani oleh aplikasi akhir, atau oleh system operasi untuk pemrosesan.
DROP	IPTables menghentikan pemrosesan lanjutan, dan paket akan ditolak.
REJECT	Sama seperti DROP, tetapi juga akan mengembalikan pesan kesalahan ke host yang mengirim paket yang ditolak.
LOG	Melakukan pencatatan (log) informasi paket ke daemon syslog
DNAT	Digunakan untuk melakukan translasi alamat IP tujuan, sebagai contoh menulis ulang alamat IP tujuan dari paket.
SNAT	Digunakan untuk melakukan translasi alamat IP sumber, sebagai contoh menulis ulang alamat IP sumber dari paket. Alamat IP sumber didefinisikan oleh sumber
MASQUERADE	Digunakan untuk melakukan translasi alamat jaringan sumber. Defaultnya alamat IP sumber adalah alamat IP yang digunakan oleh interface firewall.

Kriteria Pencocokan IPTables

IPTables Options	Keterangan
-t <-table->	Menentukan tipe table yaitu filter, nat, & mangle. Defaultnya adalah filter.
-j <target>	Jump ke target chain yang ditentukan ketika paket dicocokkan dengan aturan saat ini.
-A	Menambahkan aturan di akhir dari chain.

-F	Flush, menghapus semua aturan di table terpilih
-p <-jenis protocol->	Mencocokkan protocol, seperti tcp, udp, icmp, dan all (semuanya).
-s <-alamat-ip->	Mencocokkan alamat ip sumber
-d <-alamat-ip->	Mencocokkan alamat ip tujuan
-i <-interface->	Mencocokkan interface masuk dimana paket masuk
-o <-interface->	Mencocokkan interface keluar dimana paket keluar
-p tcp –sport <-port->	Port sumber adalah TCP, dapat berupa sebuah port atau jangkauan dengan format: *port-awal:port-akhir*
-p tcp –dport <-port->	Port tujuan adalah TCP, dapat berupa sebuah port atau jangkauan dengan format: *port-awal:port-akhir*
-p tcp –syn	Digunakan untuk mengidentifikasi permintaan koneksi TCP baru.
-p udp –sport <-port->	Port sumber adalah UDP, dapat berupa sebuah port atau jangkauan dengan format: *port-awal:port-akhir*
-p udp –dport <-port->	Port tujuan adalah UDP, dapat berupa sebuah port atau jangkauan dengan format: *port-awal:port-akhir*
-m state –state <-state->	Bagian (state) yang sering diuji adalah: **ESTABLISHED**, paket adalah bagian dari koneksi yang telah berlangsung. **NEW**, paket memulai koneksi yang baru. **RELATED**, paket memulai koneksi kedua yang baru. **INVALID**, paket tidak dapat diidentifikasi.

Menggunakan IPTables

Langkah pertama untuk menggunakan iptables adalah dengan menjalankan service iptables menggunakan perintah berikut:

```
# service iptables start
```

Catatan:

Service iptables saat dijalankan (start), akan mengeksekusi isi dari file /etc/sysconfig/iptables. Apabila file ini tidak ditemukan, maka service iptables tidak akan dapat dijalankan (status service tetap tidak aktif/stop). Untuk itu perlu dibuat file kosong dengan nama “iptables”

pada direktori /etc/sysconfig, dan mengatur ijin akses agar hanya user root yang dapat melakukan perubahan pada file tersebut.

```
# touch /etc/sysconfig/iptables

# chmod 600 /etc/sysconfig/iptables

# service iptables start
```

Untuk memverifikasi status service iptables telah aktif, eksekusi perintah berikut:

```
# service iptables status
```

Untuk menghentikan service iptables, eksekusi perintah berikut:

```
# service iptables stop
```

Untuk mengaktifkan service iptables saat booting, maka perlu dilakukan perubahan status runlevel ke mode on menggunakan utilitas *chkconfig*.

```
# chkconfig –level 345 iptables on
```

Untuk memverifikasi status service iptables telah aktif (mode on) pada run level 345, eksekusi perintah berikut:

```
# chkconfig –list iptables

iptables        0:off   1:off   2:on    3:on    4:on    5:on
6:off
```

Membuat Aturan IPTables

Membersihkan tabel filter

```
# iptables -F
```

Membersihkan tabel nat

```
# iptables -t nat -F
```

Membersihkan tabel mangle

```
# iptables -t mangle -F
```

Mengatur *default policy* untuk tabel INPUT dengan target DROP

```
# iptables -P INPUT DROP
```

Mengatur *default policy* untuk tabel FORWARD dengan target DROP

```
# iptables -P FORWARD DROP
```

Mengatur *default policy* untuk tabel OUTPUT dengan target ACCEPT

```
# iptables -P OUTPUT ACCEPT
```

Mengijinkan trafik dari interface *loopback*

```
# iptables -A INPUT -i lo -j ACCEPT
```

Mengijinkan trafik *DHCP Client Request*

```
# iptables -A INPUT -i eth0 -p udp --dport 67:68 --sport 67:68
-j ACCEPT
```

Mengijinkan permintaan *ping request*

```
# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

Mencatat paket apapun yang masuk pada eth0, yang berasal dari lokal atau jaringan yang tidak bisa dirutekan. Apabila salah satu dari alamat jaringan lokal berikut digunakan pada jaringan saat ini, abaikan aturan tersebut

```
# iptables -A INPUT -i eth0 -s 10.0.0.0/8 -j LOG --log-prefix
"IP DROP SPOOF A: "

# iptables -A INPUT -i eth0 -s 172.16.0.0/12 -j LOG --log-prefix
"IP DROP SPOOF B: "

# iptables -A INPUT -i eth0 -s 192.168.0.0/16 -j LOG --log-
prefix "IP DROP SPOOF C: "

# iptables -A INPUT -i eth0 -s 224.0.0.0/4 -j LOG --log-prefix
"IP DROP SPOOF D: "
```

```
# iptables -A INPUT -i eth0 -s 240.0.0.0/5 -j LOG --log-prefix
"IP DROP SPOOF E: "

# iptables -A INPUT -i eth0 -d 127.0.0.0/8 -j LOG --log-prefix
"IP DROP LOOPBACK "
```

Mengijinkan koneksi apapun yang telah terbentuk

```
# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j
ACCEPT
```

Mengijinkan akses WWW

```
#iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport
80 -j ACCEPT
```

Mengijinkan akses FTP

```
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport
21 -j ACCEPT
```

Mengijinkan akses FTP Data

```
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport
20 -j ACCEPT
```

Mengijinkan akses SSH

```
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport
22 -j ACCEPT
```

Mengijinkan akses Telnet

```
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport
23 -j ACCEPT
```

Mengijinkan akses TFTP

```
# iptables -A INPUT -m state --state NEW -m udp -p udp --dport
69 -j ACCEPT
```

Mengaktifkan pencatatan paket yang masuk (logging)

```
# iptables -A INPUT -j LOG
```

Mengaktifkan pencatatan hanya pada paket masuk yang tidak diinginkan

```
# iptables -A INPUT -j DROP
```

Menampilkan daftar aturan IPTables yang saat ini dijalankan

```
# service iptables status
```

Agar output dari hasil eksekusi perintah diatas ditampilkan dalam format layar per layar, gunakan perintah berikut:

```
# service iptables status | more
```

Untuk menampilkan daftar aturan IPTables yang saat ini dijalankan juga dapat menggunakan perintah berikut:

```
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Hasil output dari eksekusi perintah diatas hanya menampilkan daftar aturan untuk table filter.

Untuk menampilkan daftar aturan IPTables untuk table nat, eksekusi perintah berikut:

```
# iptables -L -t nat
```

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Untuk menampilkan daftar aturan IPTables untuk table mangle, eksekusi perintah berikut:

```
# iptables –L –t mangle
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
```

Menyimpan aturan IPTables

Aturan firewall disimpan pada file */etc/sysconfig/iptables*. File ini akan dieksekusi saat komputer booting, dan saat service iptables di-start atau direstart. Untuk menyimpan aturan IPTables, eksekusi perintah berikut:

```
# service iptables save
```

Aturan firewall IPTables perlu disimpan karena aturan tersebut hanya berlaku saat computer tersebut aktif (disimpan sementara di memory), sehingga apabila computer tersebut di-restart atau dimatikan, maka aturan tersebut akan dibersihkan.

Troubleshooting IPTables

Salah satu metode yang dapat digunakan untuk melakukan troubleshooting IPTables adalah dengan melakukan pencatatan (log) semua paket yang dibuang menggunakan target **LOG**. Target LOG dapat digunakan untuk melacak paket-paket yang bergerak melalui aturan IPTables. Semua trafik yang sesuai dengan aturan IPTables dimana ia ditempatkan akan di-log, dan disimpan pada file */var/log/messages*.

Untuk mencatat hanya trafik yang tidak diinginkan, perlu ditambahkan aturan yang sesuai dengan target **DROP** setelah aturan LOG.

Berikut adalah contoh penggunaan target LOG untuk mencatat paket pada table OUTPUT, INPUT, dan FORWARD, kemudian dilanjutkan dengan penggunaan target DROP untuk hanya mencatat (log) paket-paket yang dibuang atau tidak diinginkan pada table OUTPUT, INPUT, dan FORWARD:

```
iptables -A OUTPUT -j LOG
iptables -A INPUT -j LOG
iptables -A FORWARD -j LOG

iptables -A OUTPUT -j DROP
iptables -A INPUT -j DROP
iptables -A FORWARD -j DROP
```

BAB VIII
Studi Kasus Firewall I:
SINGLE DUAL-HOMED FIREWALL

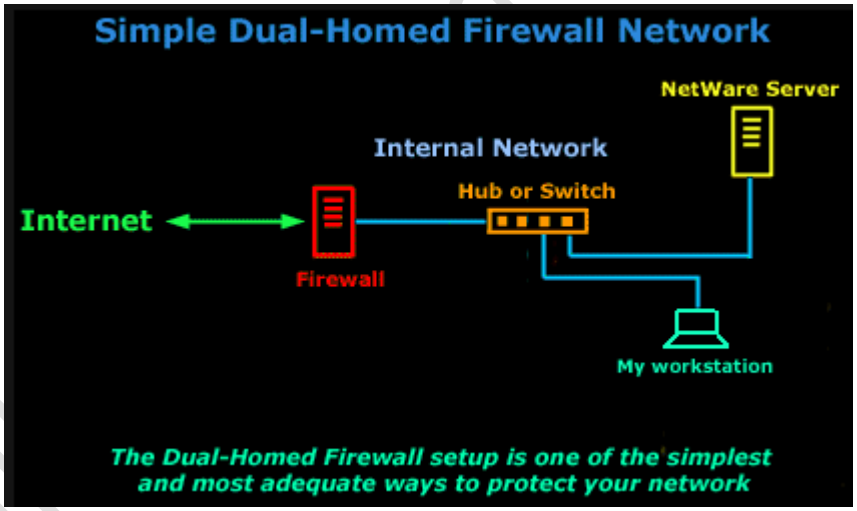
Tujuan:

Mahasiswa memahami penerapan IPTables pada topologi Single Dual-Homed Firewall.

Materi:

1. Pengenalan Topologi Single Dual-Homed Firewall.

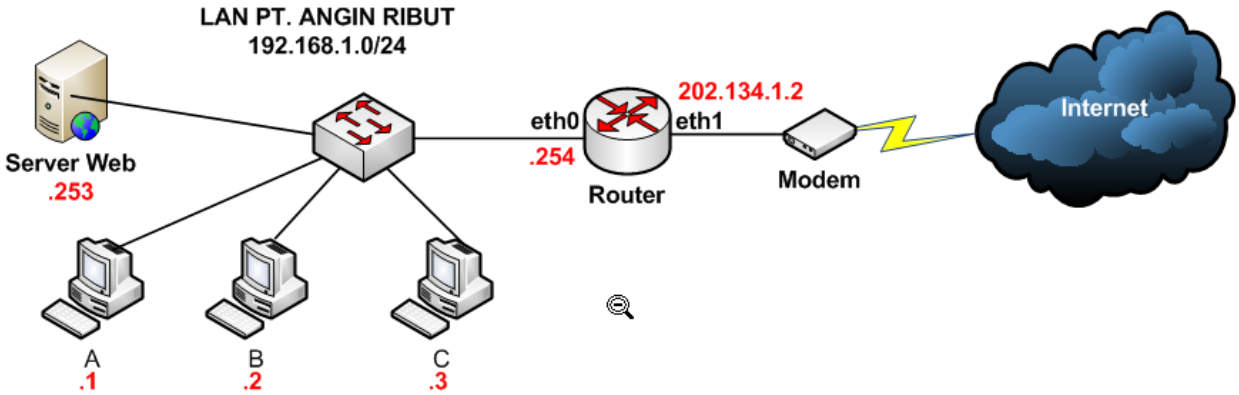
Dual-homed firewall merupakan salah satu dari firewall yang paling sederhana dan umum digunakan. Dual-homed mengacu pada dua jaringan dimana interface router terhubung secara langsung yaitu satu interface terhubung ke jaringan dalam, dan satu interface terhubung ke jaringan luar sebagai contoh Internet, seperti terlihat pada gambar berikut:



Gambar Dual Home Firewall (Sumber: www.firewall.cx)

Firewall yang diterapkan pada router akan menganalisa lalu lintas paket data diantara jaringan dalam (internal) ke Internet, dan sebaliknya. Jaringan internal pada LAN umumnya menggunakan pengalamatan IP Private, sedangkan jaringan Internet menggunakan alamat IP Publik. Agar dapat host-host di LAN yang menggunakan alamat IP Private dapat melakukan akses Internet maka diperlukan konfigurasi NAT pada router.

2. Membangun topologi Simple Dual-Homed Firewall menggunakan IPTables.



Gambar topologi jaringan Simple Dual-Home Firewall

3. Konfigurasi & verifikasi IPTables pada topologi Simple Dual-Homed Firewall.

Terdapat beberapa ketentuan pengaturan IPTables yang harus dikonfigurasi pada router yaitu sebagai berikut:

a) Mengijinkan akses Internet bagi seluruh host di LAN PT. Angin Ribut

```
# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth1 -j
SNAT --to-source 202.134.1.2
```

b) Mengijinkan akses Internet hanya bagi host C di LAN PT. Angin Ribut

```
# iptables -t nat -A POSTROUTING -s 192.168.1.3 -o eth1 -j SNAT -
-to-source 202.134.1.2
```

c) Menampilkan informasi seluruh aturan IPTables yang terdapat pada router

```
# service iptables status
```

Tugas:

Berdasarkan topologi jaringan sebelumnya, lakukan konfigurasi kebijakan keamanan pada router dengan ketentuan berikut:

1. Mengijinkan akses Internet hanya bagi host dengan jangkauan alamat IP 192.168.1.10-192.168.1.20.
2. Mengijinkan akses Internet bagi seluruh host untuk layanan HTTP.

BAB IX

Studi Kasus Firewall II:

Two Legged Network Firewall with a fully exposed DMZ

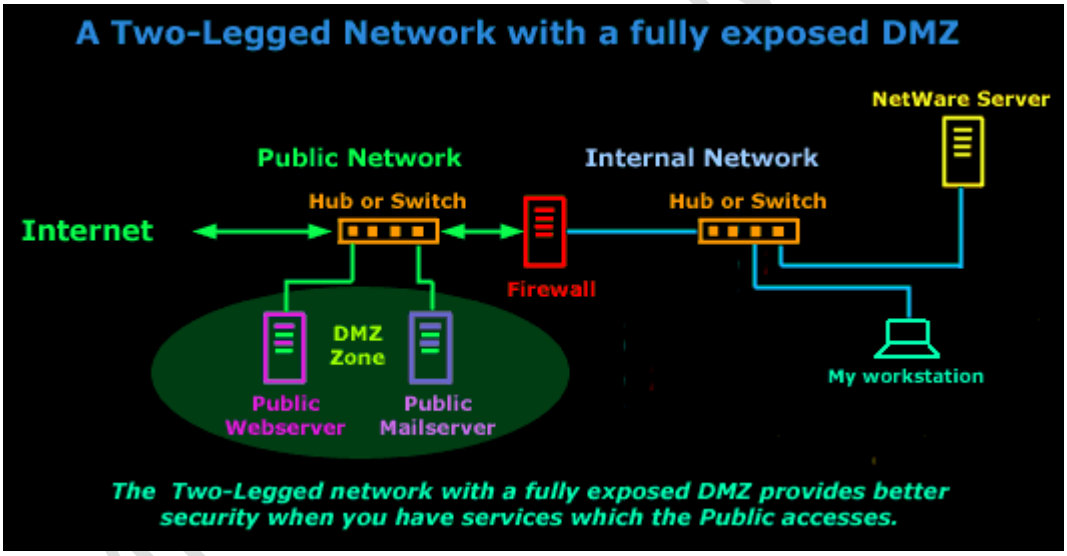
Tujuan:

Mahasiswa memahami penerapan IPTables pada topologi Two-Legged Network Firewall with a fully exposed DMZ.

Materi:

1. Pengenalan Topologi Two-Legged Network Firewall with a fully exposed DMZ

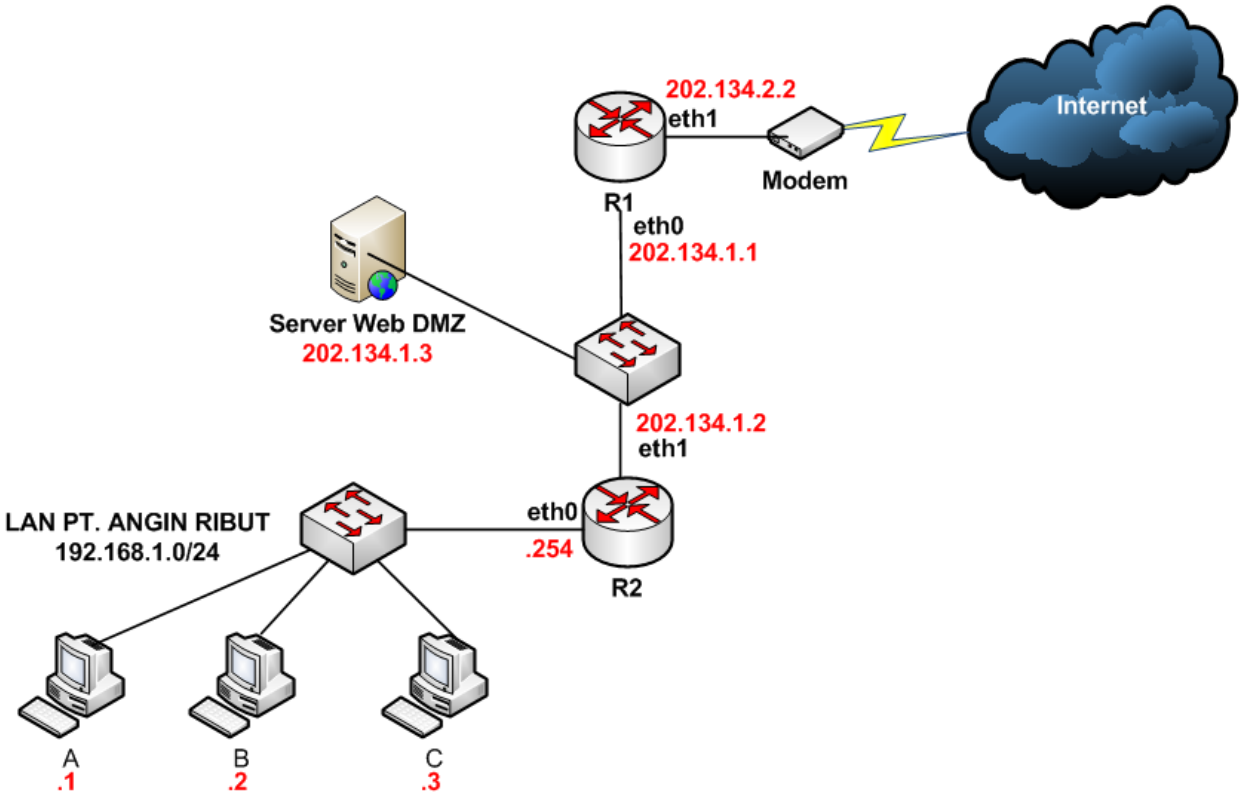
Pada topologi ini, router yang digunakan untuk mengakses ke Internet dihubungkan ke switch atau hub, seperti terlihat pada gambar berikut:



Gambar Two-Legged Network with a fully exposed DMZ (Sumber: www.firewall.cx)

Server-server yang terdapat di area DMZ dihubungkan langsung ke switch atau hub, dan tidak melalui pemfilteran oleh firewall, sehingga dapat diakses oleh pengguna dari Internet secara langsung. Firewall hanya memiliki dua interface yang terhubung ke Internal Network, dan ke Public Network melalui switch atau hub di area DMZ. Firewall hanya akan menganalisa lalu lintas paket data diantara jaringan dalam (internal) ke Internet, dan sebaliknya, tanpa melakukan pemfilteran atau pengaturan keamanan terkait server-server yang terdapat di area DMZ.

2. Membangun topologi Two-Legged Firewall with a fully exposed DMZ menggunakan IPTables



Gambar topologi jaringan Two-Legged Firewall with a fully exposed DMZ

3. Konfigurasi & verifikasi IPTables pada topologi Two-Legged Firewall with a fully exposed DMZ

Terdapat beberapa ketentuan pengaturan IPTables yang harus dikonfigurasi pada router yaitu sebagai berikut:

a) Mengijinkan akses Internet bagi seluruh host di LAN PT. Angin Ribut

```
# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth1 -j
SNAT --to-source 202.134.1.2
```

b) Menampilkan informasi seluruh aturan IPTables yang terdapat pada router

```
# service iptables status
```

Tugas:

Berdasarkan topologi jaringan sebelumnya, lakukan konfigurasi kebijakan keamanan dengan ketentuan berikut:

1. Konfigurasi pada Server Web agar default policy dari IPTables tabel Filter chain INPUT, OUTPUT adalah DROP.
2. Konfigurasi pada Server Web agar mengijinkan akses HTTP dari manapun.
3. Konfigurasi pada Server Web agar mengijinkan akses SSH hanya dari PC A di LAN.
4. Konfigurasi pada Server Web agar mengijinkan akses FTP hanya dari LAN.

BAB X

Studi Kasus Firewall III:

IPTables pada Three-Legged Network Firewall

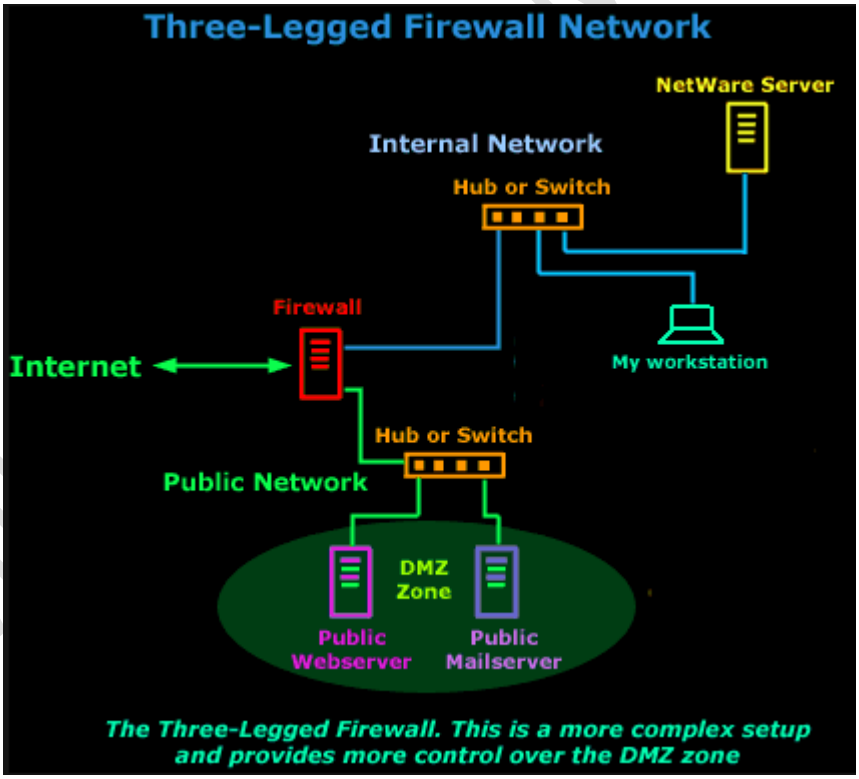
Tujuan:

Mahasiswa memahami penerapan IPTables pada topologi Three-Legged Network Firewall.

Materi:

1. Pengenalan Topologi Three-Legged Network Firewall.

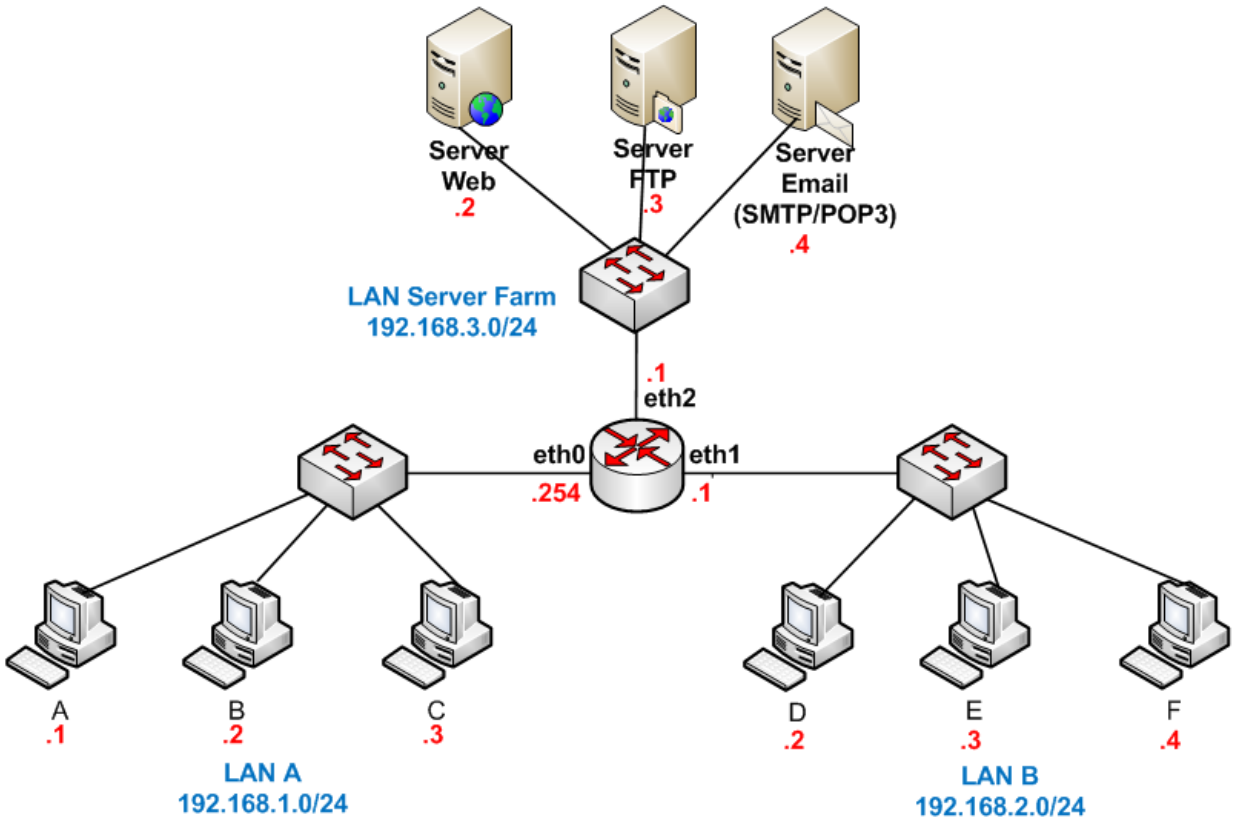
Pada topologi ini, router memiliki 3 interface yang masing-masing terhubung ke jaringan Internal, jaringan DMZ, dan jaringan Internet, sehingga dikenal dengan istilah *Three-Legged*, seperti terlihat pada gambar berikut:



Gambar Three-Legged Firewall Network with DMZ (Sumber: www.firewall.cx)

Firewall dikonfigurasi untuk mengatur lalu lintas paket data dari jaringan internal ke jaringan Internet, dan jaringan DMZ.

2. Membangun topologi Three-Legged Network Firewall menggunakan IPTables.



Gambar topologi jaringan Three-Legged Network Firewall

3. Konfigurasi & verifikasi IPTables pada topologi Three-Legged Network Firewall.

Terdapat beberapa ketentuan pengaturan IPTables yang harus dikonfigurasi pada router yaitu sebagai berikut:

a) Mengatur default policy untuk IPTables table Filter pada chain INPUT, OUTPUT maupun FORWARD menjadi DROP.

```
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -P FORWARD DROP
```

b) Mengijinkan hanya LAN A yang dapat mengakses layanan pada Server Web.

```
# iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.3.2 -p tcp --
dport 80 -j ACCEPT
# iptables -A FORWARD -s 192.168.3.2 -d 192.168.1.0/24 -p tcp --
sport 80 -j ACCEPT
```

c) Mengijinkan hanya LAN B yang dapat mengakses layanan pada Server FTP.

```
# iptables -A FORWARD -s 192.168.2.0/24 -d 192.168.3.3 -p tcp --
dport 21 -j ACCEPT
# iptables -A FORWARD -s 192.168.2.0/24 -d 192.168.3.3 -p tcp --
dport 20 -j ACCEPT
# iptables -A FORWARD -s 192.168.3.3 -d 192.168.2.0/24 -p tcp --
sport 21 -j ACCEPT
# iptables -A FORWARD -s 192.168.3.3 -d 192.168.2.0/24 -p tcp --
sport 20 -j ACCEPT
```

d) Mengijinkan baik LAN A maupun LAN B untuk dapat mengakses Server Email.

```
# iptables -A FORWARD -d 192.168.3.4 -p tcp --dport 25 -j ACCEPT
# iptables -A FORWARD -d 192.168.3.4 -p tcp --dport 110 -j ACCEPT
# iptables -A FORWARD -S 192.168.3.4 -p tcp --sport 25 -j ACCEPT
# iptables -A FORWARD -S 192.168.3.4 -p tcp --sport 110 -j ACCEPT
```

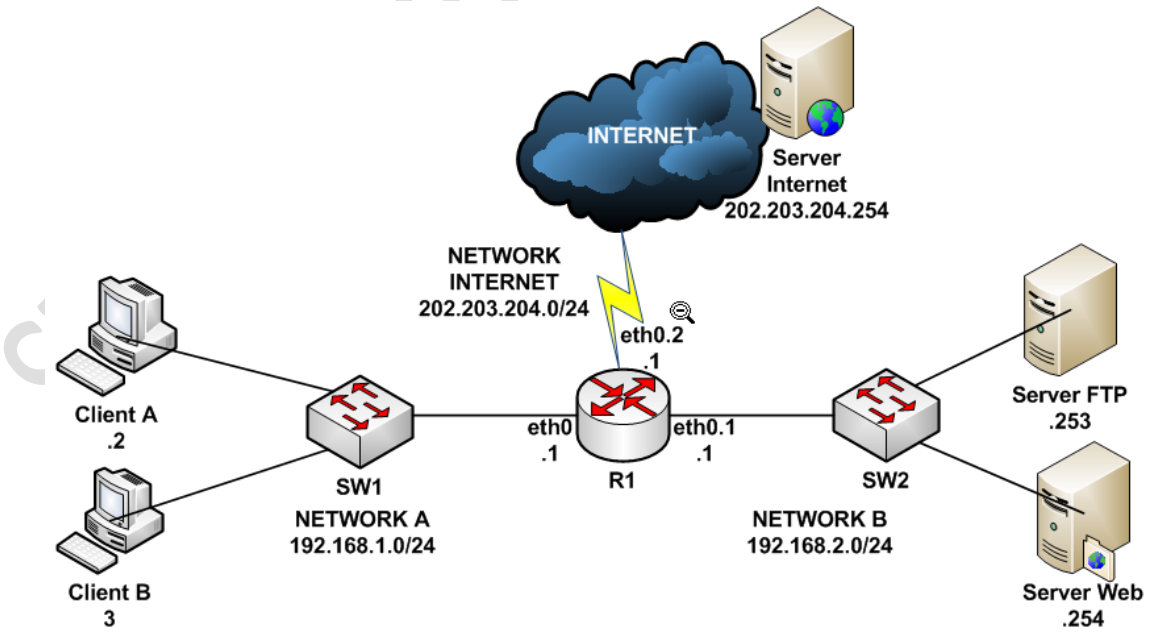
e) Mengijinkan hanya PC A pada LAN A untuk dapat mengakses PC D pada LAN B.

```
# iptables -A FORWARD -s 192.168.1.1 -d 192.168.2.2 -j ACCEPT
# iptables -A FORWARD -s 192.168.2.2 -d 192.168.1.1 -j ACCEPT
```

f) Menampilkan informasi seluruh aturan IPTables yang terdapat pada router

```
# service iptables status
```

Tugas:



Berdasarkan topologi jaringan seperti terlihat pada gambar diatas, lakukan konfigurasi kebijakan keamanan dengan ketentuan berikut pada Router R1:

1. Konfigurasi IPTables Tabel Filter untuk mengijinkan hanya Client A untuk dapat mengakses layanan Server FTP di Network B.
2. Konfigurasi IPTables Tabel Filter untuk mengijinkan hanya Client B untuk dapat mengakses layanan Server Web di Network B.
3. Konfigurasi IPTables Tabel Filter untuk menolak ping dari Network A ke Network B, sebaliknya ping dari Network B ke Network A diijinkan.
4. Konfigurasi NAT untuk mengijinkan hanya Client A yang dapat mengakses Internet.
5. Konfigurasi DNAT untuk mengijinkan pengguna di Internet mengakses Server Web di Network B yang menggunakan alamat IP Private 192.168.2.253 menggunakan alamat IP Publik dari interface eth0.2 yang digunakan oleh router R1 yaitu 202.203.204.1.

DAFTAR REFERENSI

Cisco Documentation, www.cisco.com

Firewall.CX, Firewall Topologies, http://www.firewall.cx/networking-topics/firewalls/209-firewall-topologies.html

Global Knowledge, Interconnecting Cisco Network Device Student Guide (ICND) 2

HowStuffWorks, How Network Address Translation Works, http://computer.howstuffworks.com/nat.htm

Linux Home Networking, Linux Firewalls Using IPTables, http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch14_:_Linux_Firewalls_Using_iptables#.V4XVZWh97IU