FIREWALL DENGAN IPTABLES

Tujuan

Setelah mengikuti materi ini diharapkan siswa mampu:

- Memahami konsep dasar keamanan jaringan
- Memahami teknik penyerangan jaringan
- Memahami teknik pengamanan jaringan
- Memahami Manajemen Resiko Keamanan Jaringan
- Mengetahui Aspek Hukum/Legal Keamanan Jaringan

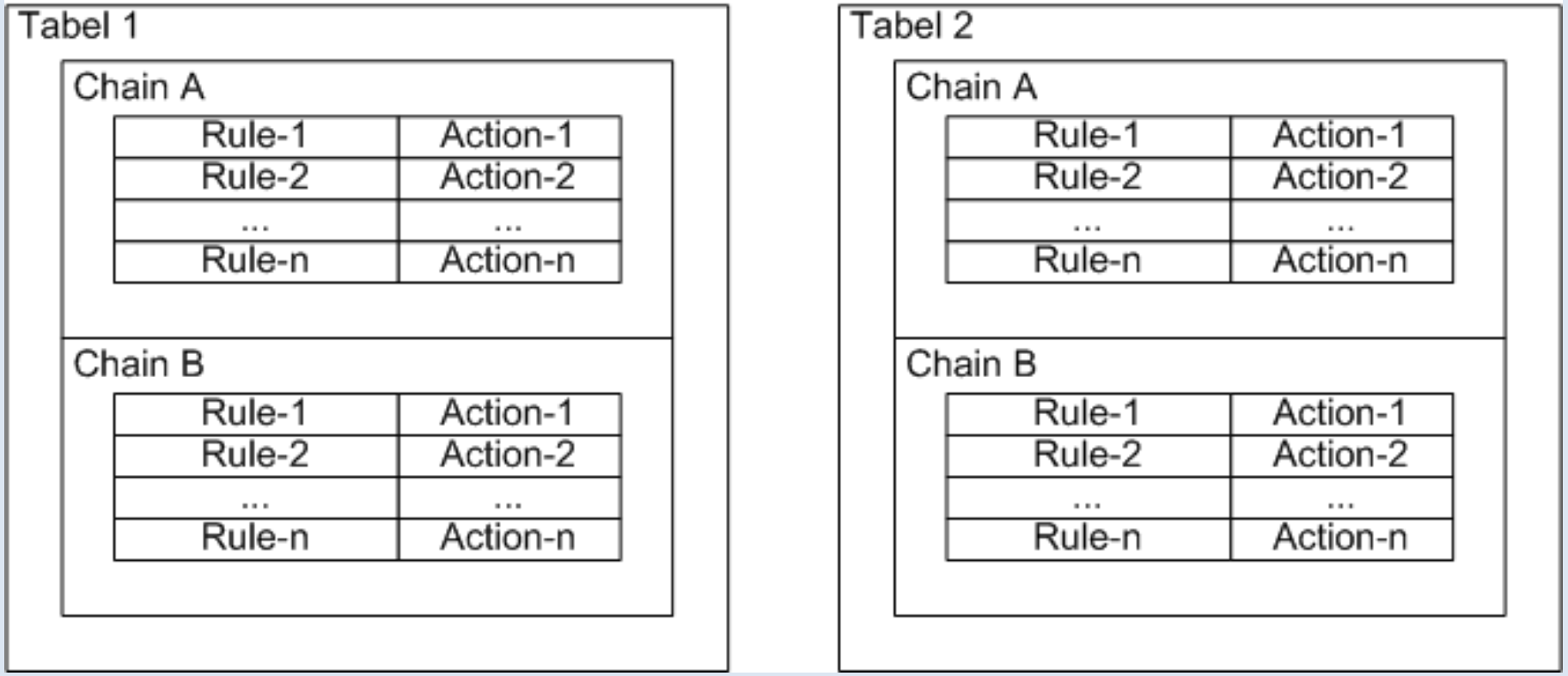
IPTABLES

- iptables adalah tool administrasi untuk fitur packet filtering and NAT IPv4 yang disediakan oleh sistem operasi linux.
- digunakan untuk membuat, mengelola dan melihat tabel aturan (**table**) packet filtering yang digunakan oleh kernel.

Tables, Chain, Rules, Target, Action

- Tabel aturan (**table**) dapat lebih dari satu dan masing2nya terdiri dari beberapa **chain**
- **chain** dapat berupa *chain built-in pada kernel* atau *chain yang didefinisikan sendiri*
- setiap **chain** terdiri dari satu set aturan (**rule)** yang cocok dengan jenis packet tertentu
- packet-packet yang cocok dengan aturan (**rule**) disebut dengan **target**.
- setiap **rule** harus menetapkan tindakan (action) yang akan dilakukan terhadap **target**.

Tables, Chain, Rules, Target, Action



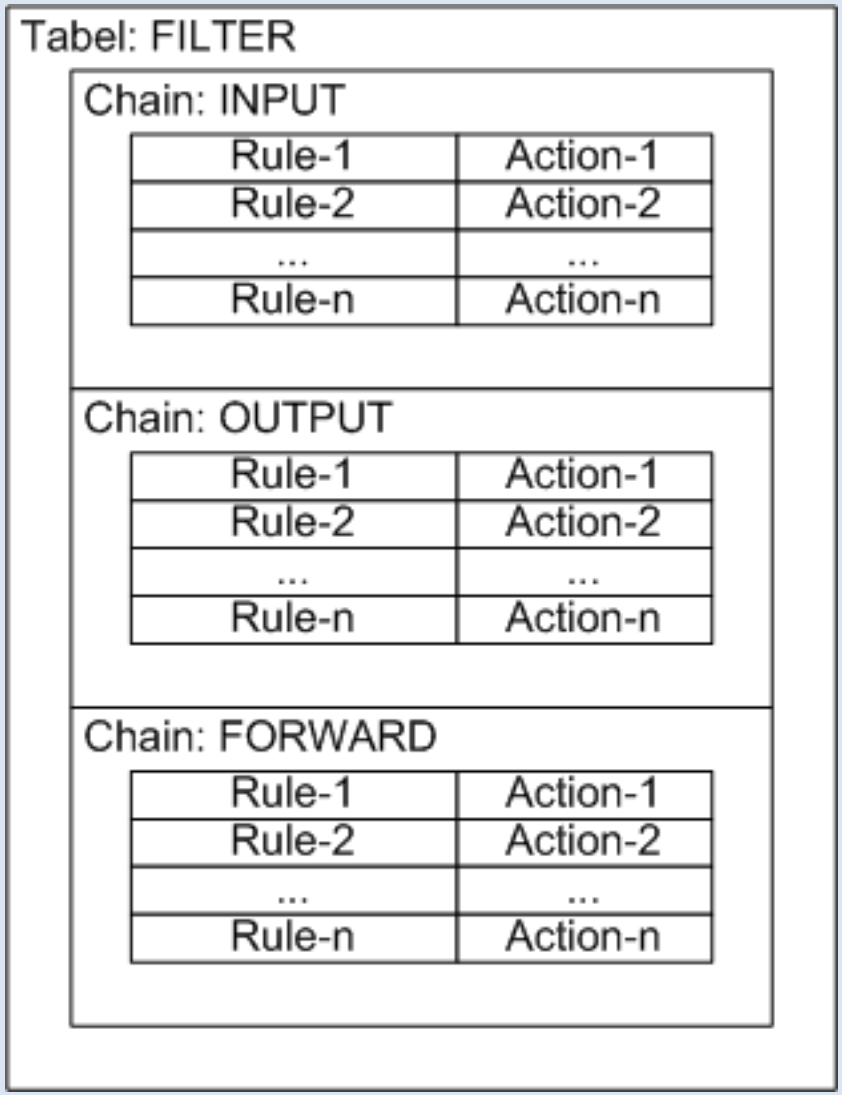
Jenis Tabel

- **Filter** : Pengaturan pengolahan paket yang masuk dan keluar dari sebuah host.
- **NAT** : Pengaturan pengolahan paket yang terkait dengan Translasi Alamat (NAT).
- **Mangle**: Pengaturan pengolahan paket yang terkait dengan pelabelan header/status packet.

Tabel Filter

Terdiri dari 3 built-in chains:

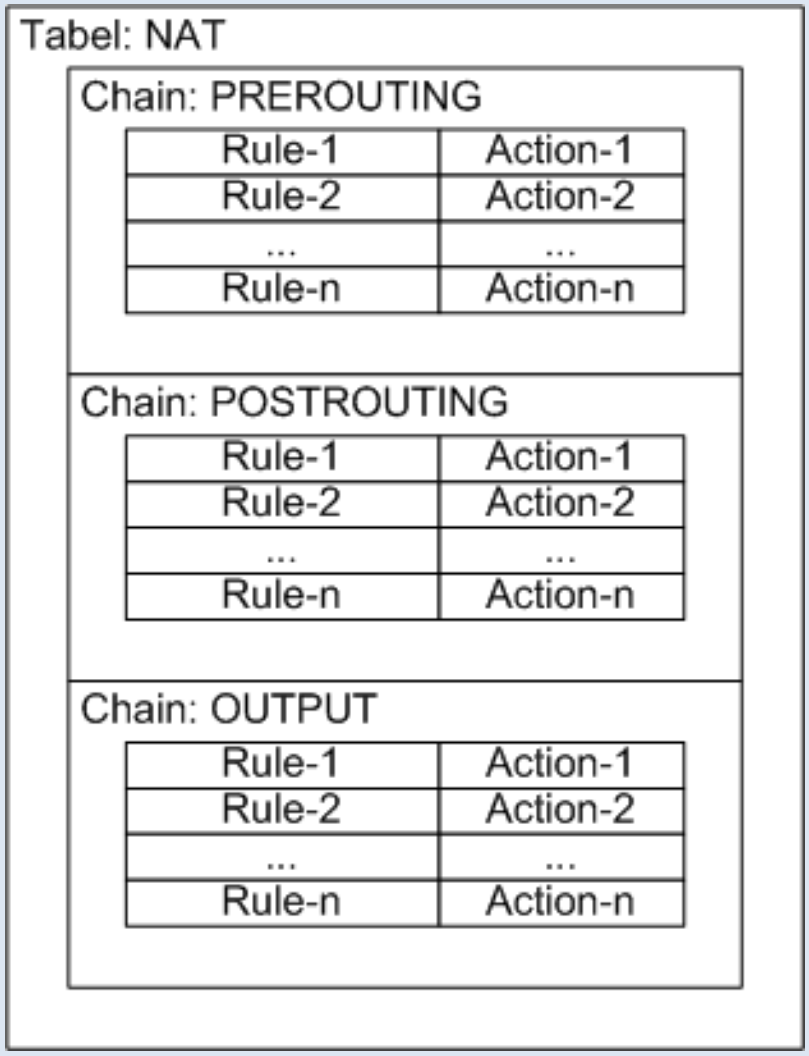
- INPUT
- OUTPUT
- FORWARD



Tabel NAT

Terdiri dari 3 built-in chains:

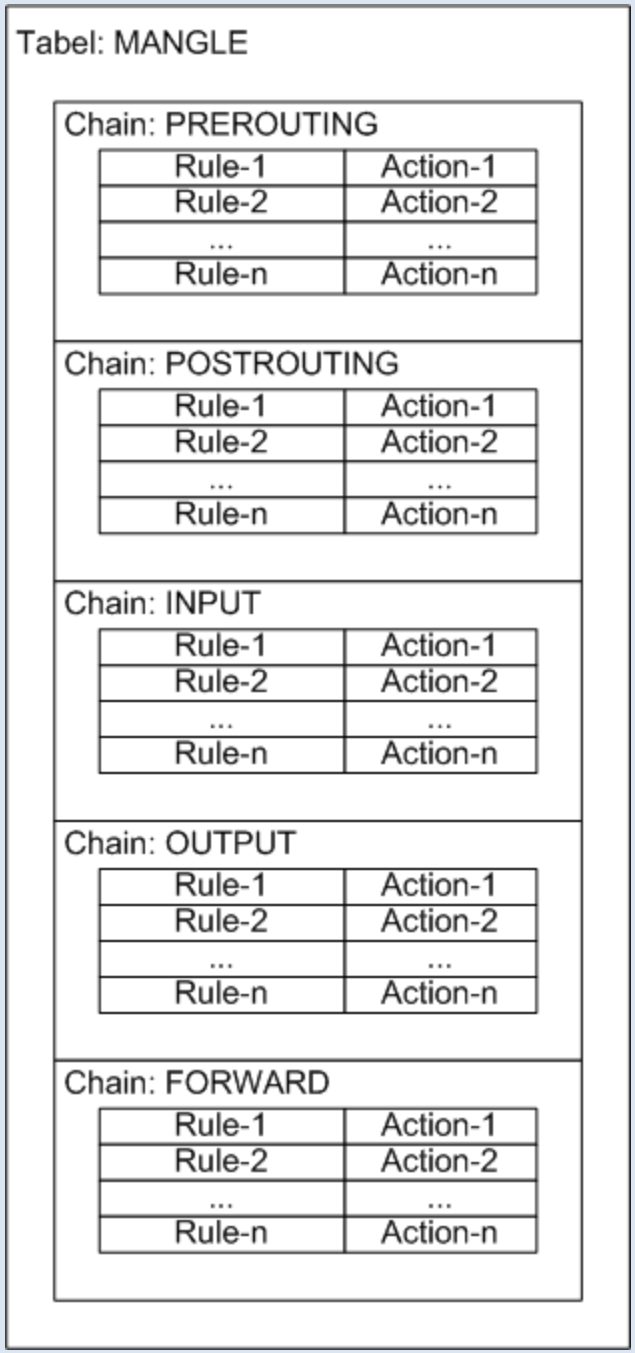
- PREROUTING
- POSTROUTING
- OUTPUT



Tabel Mangle

Terdiri dari 5 built-in chains:

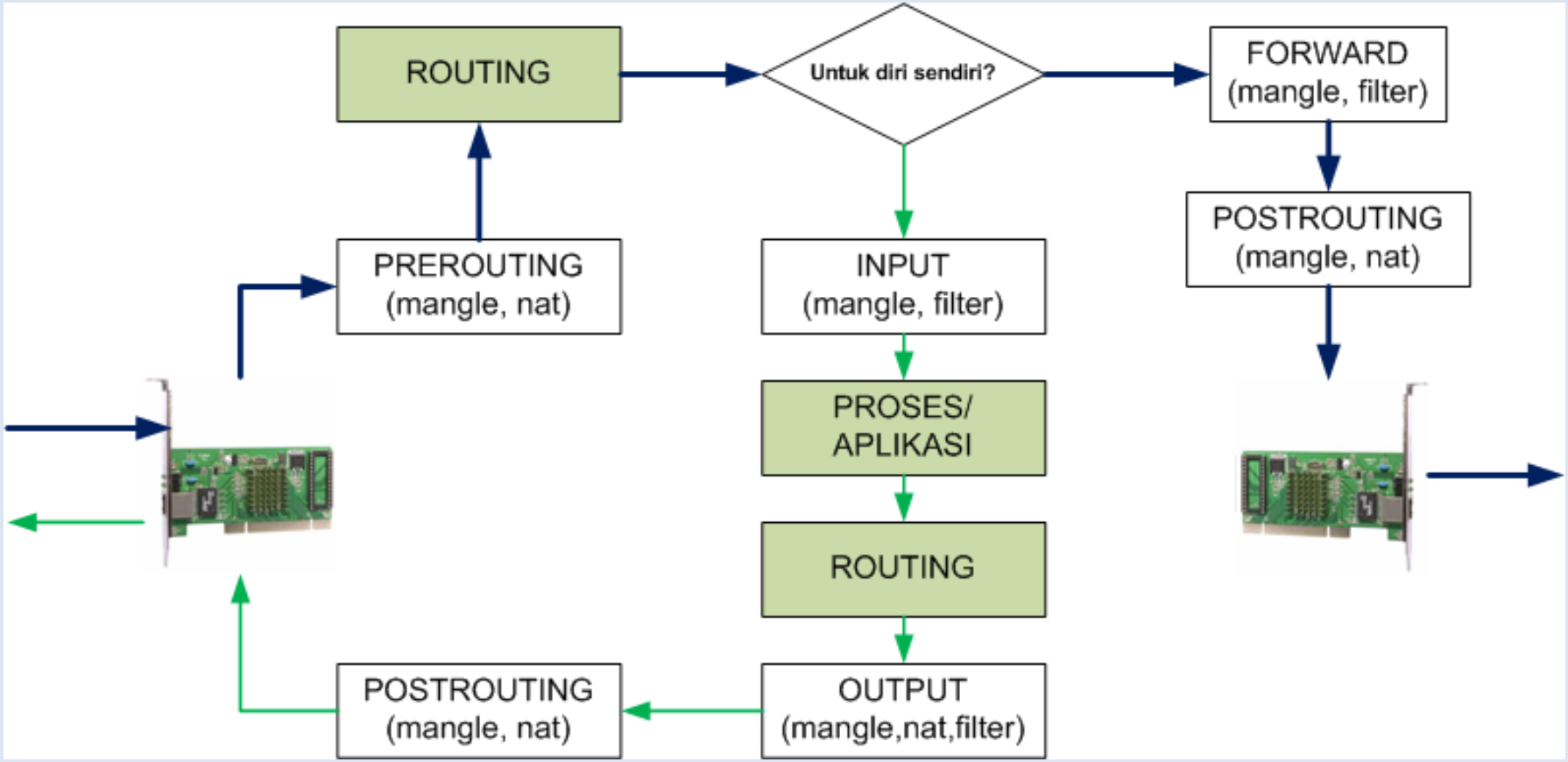
- PREROUTING
- POSTROUTING
- OUTPUT
- INPUT
- FORWARD



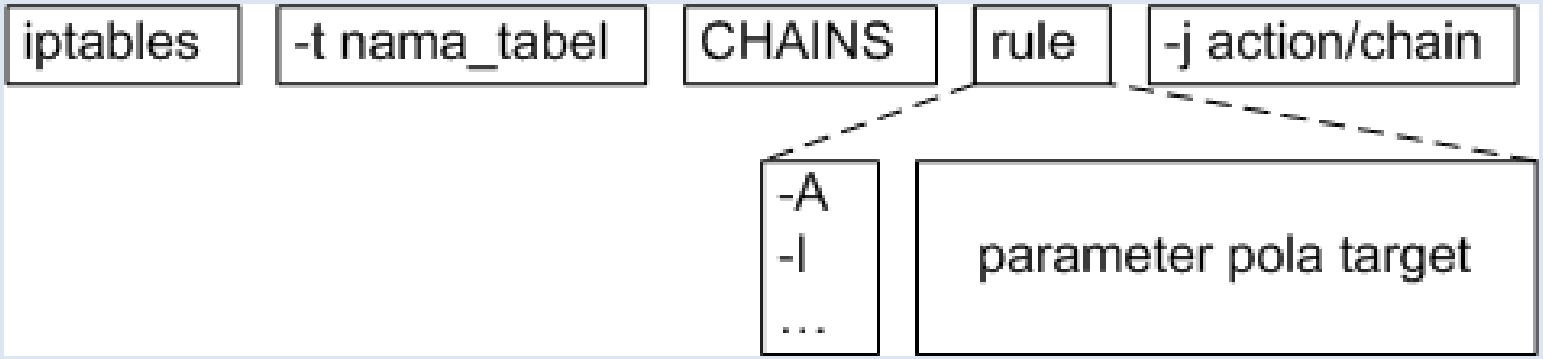
Rules Actions

- **ACCEPT** : proses iptables selesai, diserahkan ke aplikasi
- **REJECT** : proses iptables selesai, packet ditolak (dapat disertai pesan)
- **DROP** : proses iptables selesai,packet ditolak (tanpa pesan)
- **LOG** : informasi packet dikirim ke pengelola log(syslog) dan dilanjutkan ke rule selanjutnya
- **DNAT** : memodifikasi alamat ip tujuan (destination ip address)
- **SNAT** : memodifikasi alamat ip sumber(source ip address)
- **MASQUERADE** : mirip SNAT dengan default source ip address = ip interface firewall (ke luar)
- Nama *chain yang didefinisikan sendiri*

Packet Flow Diagram



Format Perintah iptables



- **A** = **Append**, menambahkan rules diakhir sebuah chain
- **I** = **Insert**, menambahkan rule diawal sebuah chain
- **P** = **Policy**, setting policy sebuah chain built-in
- Parameter pola target bervariasi,

Detil dapat dibaca pada manual iptables

Contoh Parameter Pola Target (1)

-p <protokol>: membandingkan jenis protokol(icmp,tcp,udp,all).

--sport <port> : port sumber (misal: tcp atau udp)

--dport <port>: port tujuan (misal tcp atau udp)

<port> dapat dituliskan sebuah angka atau **awal:akhir** untuk menyatakan rentang port.

--icmp-type <jenis> : jenis datagram icmp, misal: ***echo-reply*** atau ***echo-request***

-s <pola_ip> : membandingkan pola alamat ip sumber

-d <pola_ip : membandingkan pola alamat ip tujuan

-i <interface> : membandingkan nama interface input

-o <interface>: membandingkan nama interface output

Contoh Parameter Pola Target (2)

-m --state <state> : membandingkan dengan parameter kondisi/status header packet. Untuk TCP/UDP dapat berupa:

ESTABLISHED: packet sudah dikenali kedua sisi host.

NEW: packet merupakan packet awal/inisialisasi.

RELATED: packet merupakan lanjutan dari packet yang sudah dikenali. Misal: pembukaan koneksi baru (sekunder) untuk transfer data pada protokol ftp.

INVALID: packet yang tidak dikenali, dapat berupa kesalahan proses pada sistem karena timeout, atau lainnya.

-m multiport [--sports|--dports |ports <port1, port2,…>:

menyatakan beberapa port TCP/UDP yang tidak berurutan.

Jenis Rules

- **Rule administratif** dapat tidak disertai dengan action. Misal: menghapus/melihat rules yang sedang ada di sistem.
- **Rule packet processing** disertai dengan action.

iptables – lihat rules

iptables [-t nama_tabel] [-L] [-n|v]

t = nama tabel, nilai default "filter"

L = list/ menampilkan semua rule yang ada saat ini

n = jangan lakukan konversi ip ke host (no dns lookup)

v = verbose/tampilan informasi lebih rinci

Misal:

 # iptables –L –v

 # iptables –t nat –L -v

iptables – hapus rules pada tabel

iptables [-t nama_tabel] [-F]

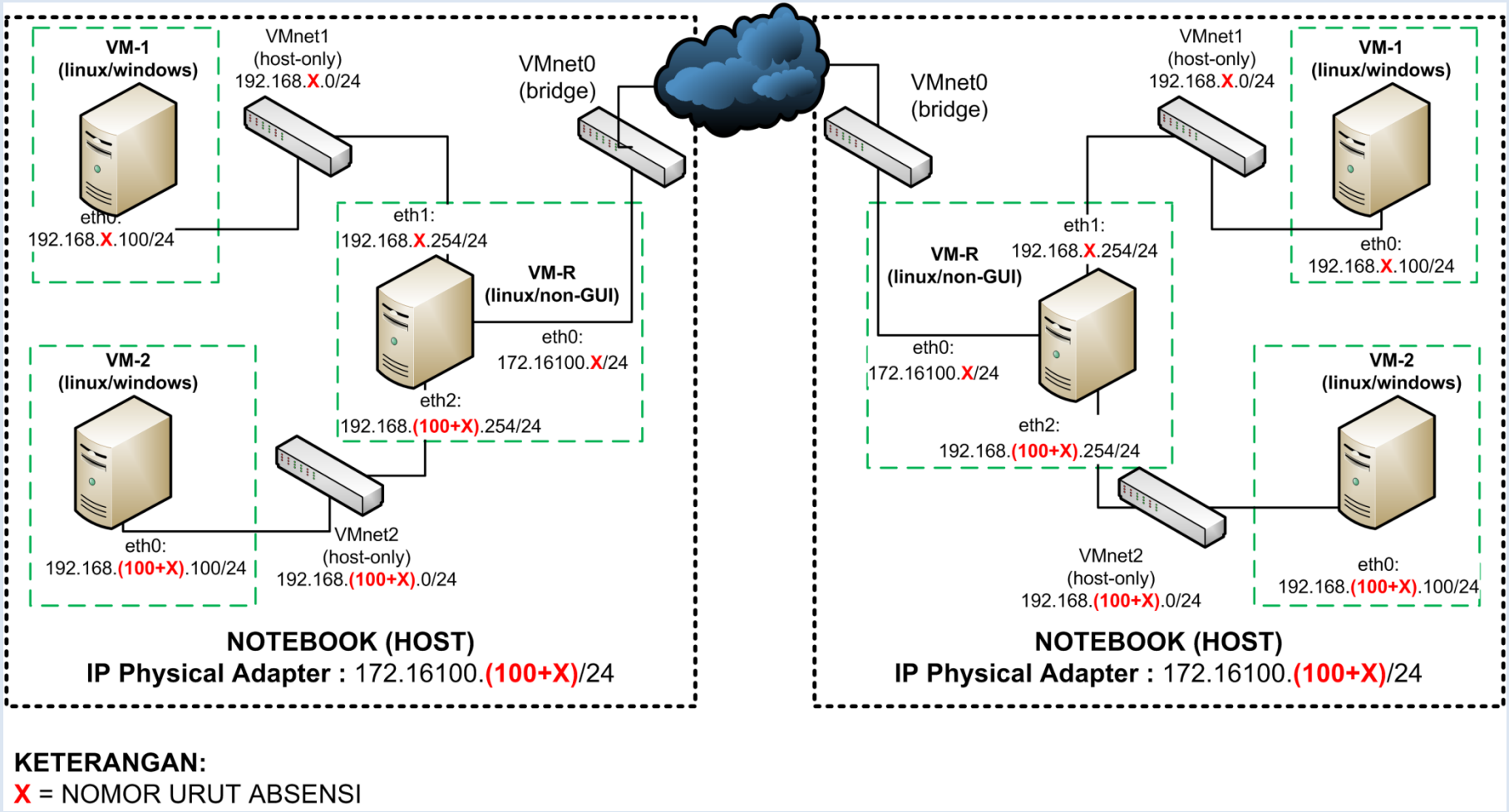
F = Flush/hapus rules

Misal:

 # iptables –F

 # iptables –t nat -F

Topologi Jaringan dan VM



KETERANGAN:
X = NOMOR URUT ABSENSI

Instruksi

- Pastikan hubungan antar notebook atau VM berjalan dengan baik
- Pastikan routing berjalan dengan baik
- Perintah iptables dijalankan pada VM-R

iptables
hapus rules pada semua tabel default

 # iptables -L -v

 # iptables -F
 # iptables -t nat -F
 # iptables -t mangle -F

 # iptables -L -v

Iptables
set default policy (1)

Hapus semua tabel dan rules

iptables -L -v

iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

iptables -L -v

Iptables
set default policy (1)

Hapus semua tabel dan rules

iptables -L -v

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

iptables -L -v

Block semua paket dari VM1

- Hapus semua rules
- Set default policy permisive

iptables –A INPUT –i eth1 –s 192.168.**X**.100 –j DROP

Test ping dan traceroute dari VM1 ke host lain