FIREWALL

1. IPTABLES adalah paket aplikasi (program berbasis Linux) yang saat ini sudah menjadi platform untuk membuat (mensetup) firewall hampir di kebanyakan distro Linux. Dengan menggunakan IPtables seorang pengguna / admin jaringan bisa mengatur lalu lintas paket data yang keluar masuk pada router atau server yang menjadi gateway (pintu gerbang) antara jaringan perusahaan/lokal (LAN) dengan jaringan publik (WAN/internet).

2. Penulisan IPTABLES

   iptables [–t table] command [match][target/jump]

   Contohnya :

   iptables –P FORWARD ACCEPT

   Keterangan :

   - *Table :* IPTables memiliki 3 buah tabel, yaitu NAT, MANGLE dan FILTER. Penggunannya disesuaikan dengan sifat dan karakteristik masing-masing.
   - *Command :* Command pada baris perintah IPTables akan memberitahu apa yang harus dilakukan terhadap lanjutan sintaks perintah. Umumnya dilakukan penambahan atau penghapusan sesuatu dari tabel atau yang lain.

Command	Keterangan
-A **--append**	Perintah ini menambahkan aturan pada akhir chain. Aturan akan ditambahkan di akhir baris pada chain yang bersangkutan, sehingga akan dieksekusi terakhir
-D **--delete**	Perintah ini menghapus suatu aturan pada chain. Dilakukan dengan cara menyebutkan secara lengkap perintah yang ingin dihapus atau dengan menyebutkan nomor baris dimana perintah akan dihapus.
-R **--replace**	Penggunaannya sama seperti --d**elete**, tetapi *command* ini menggantinya dengan entry yang baru.
-I **--insert**	Memasukkan aturan pada suatu baris di chain. Aturan akan dimasukkan pada baris yang disebutkan, dan aturan awal yang menempati baris tersebut akan digeser ke bawah. Demikian pula baris-baris selanjutnya.
-L **--list**	Perintah ini menampilkan semua aturan pada sebuah tabel. Apabila tabel tidak disebutkan, maka seluruh aturan pada semua tabel akan ditampilkan, walaupun tidak ada aturan sama sekali pada sebuah tabel. *Command* ini bisa

	dikombinasikan dengan option –v (verbose), -n (numeric) dan –x (exact).
-F **--flush**	Perintah ini mengosongkan aturan pada sebuah chain. Apabila chain tidak disebutkan, maka semua chain akan di-*flush*.
-N **--new-chain**	Perintah tersebut akan membuat chain baru.
-X **--delete-chain**	Perintah ini akan menghapus chain yang disebutkan. Agar perintah di atas berhasil, tidak boleh ada aturan lain yang mengacu kepada chain tersebut.
-P **--policy**	Perintah ini membuat kebijakan default pada sebuah chain. Sehingga jika ada sebuah paket yang tidak memenuhi aturan pada baris-baris yang telah didefinisikan, maka paket akan diperlakukan sesuai dengan kebijakan default ini.
-E **--rename-chain**	Perintah ini akan merubah nama suatu chain.

- *3. Option :* Option digunakan dikombinasikan dengan command tertentu yang akan menghasilkan suatu variasi perintah.

Option	Command	Keterangan
-v **--verbose**	**--list** **--append** **--insert** **--delete** **--replace**	Memberikan output yang lebih detail, utamanya digunakan dengan --list. Jika digunakan dengan --list, akan menampilkam K (x1.000), M (1.000.000) dan G (1.000.000.000).
-x **--exact**	**--list**	Memberikan output yang lebih tepat.
-n **--numeric**	**--list**	Memberikan output yang berbentuk angka. Alamat IP dan nomor port akan ditampilkan dalam bentuk angka dan bukan hostname ataupun nama aplikasi/servis.
--line-number	**--list**	Akan menampilkan nomor dari daftar aturan. Hal ni akan mempermudah bagi kita untuk melakukan modifikasi aturan, jika kita mau meyisipkan atau menghapus aturan dengan nomor tertentu.
--modprobe	**All**	Memerintahkan IPTables untuk memanggil modul tertentu. Bisa digunakan bersamaan dengan semua *command*.

- *Generic Matches :* Generic Matches artinya pendefinisian kriteria yang berlaku secara umum. Dengan kata lain, sintaks generic matches akan sama untuk semua protokol. Setelah protokol didefinisikan, maka baru didefinisikan aturan yang

lebih spesifik yang dimiliki oleh protokoltersebut. Hal ini dilakukan karena tiap-tiap protokol memiliki karakteristik yang berbeda, sehingga memerlukan perlakuan khusus.

Match	Keterangan
-p **--protocol**	Digunakan untuk mengecek tipe protokol tertentu. Contoh: TCP, UDP, ICMP dan ALL. Daftar protokol bisa dilihat pada **/etc/protocols**. Tanda inversi juga bisa diberlakukan di sini, misal kita menghendaki semua protokol kecuali icmp, maka kita bisa menuliskan **--protokol ! icmp** yang berarti semua kecuali icmp.
-s **--src** **--source**	Kriteria ini digunakan untuk mencocokkan paket berdasarkan alamat IP asal. Alamat di sini bisa berberntuk alamat tunggal seperti 192.168.1.1, atau suatu alamat network menggunakan netmask misal 192.168.1.0/255.255.255.0, atau bisa juga ditulis 192.168.1.0/24 yang artinya semua alamat 192.168.1.x. Kita juga bisa menggunakan inversi.
-d **--dst** **--destination**	Digunakan untuk mecocokkan paket berdasarkan alamat tujuan. Penggunaannya sama dengan *match* **–src**
-i **--in-interface**	*Match* ini berguna untuk mencocokkan paket berdasarkan interface di mana paket datang. *Match* ini hanya berlaku pada chain INPUT, FORWARD dan PREROUTING
-o **--out-interface**	Berfungsi untuk mencocokkan paket berdasarkan interface di mana paket keluar. Penggunannya sama dengan **--in-interface**. Berlaku untuk chain OUTPUT, FORWARD dan POSTROUTING

- *Implicit Matches:* adalah match yang spesifik untuk tipe protokol tertentu. Implicit Match merupakan sekumpulan rule yang akan diload setelah tipe protokol disebutkan. Ada 3 Implicit Match berlaku untuk tiga jenis protokol, yaitu TCP matches, UDP matches dan ICMP matches.

- *Target/Jump: T*arget atau jump adalah perlakuan yang diberikan terhadap paket-paket yang memenuhi kriteria atau match. Jump memerlukan sebuah chain yang lain dalam tabel yang sama. Chain tersebut nantinya akan dimasuki oleh paket yang memenuhi kriteria. Analoginya ialah chain baru nanti berlaku sebagai prosedur/fungsi dari program utama. Sebagai contoh dibuat sebuah chain yang bernama tcp_packets. Setelah ditambahkan aturan-aturan ke dalam chain tersebut, kemudian chain tersebut akan direferensi dari chain input.

  iptables –A INPUT –p tcp –j tcp_packets

Target	Keterangan
-j ACCEPT --jump	Ketika paket cocok dengan daftar *match* dan target ini diberlakukan, maka paket tidak akan melalui baris-baris

ACCEPT	aturan yang lain dalam chain tersebut atau chain yang lain yang mereferensi chain tersebut. Akan tetapi paket masih akan memasuki chain-chain pada tabel yang lain seperti biasa.
-j DROP --jump DROP	Target ini men-*drop* paket dan menolak untuk memproses lebih jauh. Dalam beberapa kasus mungkin hal ini kurang baik, karena akan meninggalkan *dead socket* antara *client* dan *server*. Paket yang menerima target DROP benar-benar mati dan target tidak akan mengirim informasi tambahan dalam bentuk apapun kepada client atau server.
-j RETURN --jump RETURN	Target ini akan membuat paket berhenti melintasi aturan-aturan pada chain dimana paket tersebut menemui target RETURN. Jika chain merupakan *subchain* dari chain yang lain, maka paket akan kembali ke *superset chain* di atasnya dan masuk ke baris aturan berikutnya. Apabila *chain* adalah chain utama misalnya INPUT, maka paket akan dikembalikan kepada kebijakan default dari *chain* tersebut.
-j MIRROR	Apabila kompuuter A menjalankan target seperti contoh di atas, kemudian komputer B melakukan koneksi http ke komputer A, maka yang akan muncul pada browser adalah website komputer B itu sendiri. Karena fungsi utama target ini adalah membalik *source address* dan *destination address.* Target ini bekerja pada chain INPUT, FORWARD dan PREROUTING atau chain buatan yang dipanggil melalui chain tersebut.

3. IPTables memiliki beberapa buah tabel yaitu NAT, MANGLE, dan FILTER. Penjelasannya adalah:

   a. **Table Mangle**: tabel yang bertanggung jawab untuk melakukan penghalusan (mangle) paket seperti merubah quality of service (QOS), TTL, dan MARK di header TCP. Biasanya tabel ini jarang digunakan di lingkungan SOHO.
   b. **Table Filter**: yaitu tabel yang bertanggung jawab untuk pemfilteran paket. Tabel ini mempunyai 3 rantai (chain) yaitu:
      1. **Rantai Forward** yaitu rantai yang memfilter paket-paket yang akan ke server yang dilindungi oleh firewall. Rantai ini digunakan ketika paket-paket datang dari IP Publik dan bukan dari IP lokal.
      2. **Rantai Input:** yaitu rantai yang memfilter paket-paket yang ditujukan ke firewall.
      3. **Rantai Output**: yaitu rantai yang memfilter paket-paket yang berasal dari firewall.
   c. **Tabel NAT**: yaitu rantai yang bertanggung jawab untuk melakukan *Network Address Translation* (NAT). NAT yaitu mengganti field asal atau alamat tujuan dari sebuah paket. Pada tabel ini terdapat 2 rantai, yaitu:

1. **Rantai Pre-Routing:** Merubah paket-paket NAT dimana alamat tujuan dari paket-paket tersebut terjadi perubahan. Biasanya dikenal dengan destination NAT atau DNAT.
2. **Rantai Post-Routing**: Merubah paket-paket NAT dimana alamat sumber dari paket-paket tersebut terjadi perubahan. Biasanya dikenal dengan source NAT atau SNAT.

4. **Forward chain** **:** meneruskan paket dari atau ke luar interface mikrotik. Misal : *virus*
   Input chain **:** paket yang masuk ke dalam interface mikrotik. Misal : *ssh*
   Output chain **:** paket yang keluar dari interface mikrotik. Misal : *Icmp*

5. Jenis NAT:
   1. *Full-cone: adalah bentuk yang paling membatasi perilaku NAT, dimana binding dari local address dan port ke public-side dan port, ketika didirikan, dapat digunakan oleh semua remote host pada setiap remote port address.*
   2. *Restricted-cone: adalah salah satu dimana NAT hanya dapat diakses oleh host tujuan, meskipun dalam kasus ini host tujuan dapat mengirim paket dari port address setelah binding dibuat.*
   3. *Port-restricted-cone: adalah salah satu di mana NAT dapat diakses oleh remote host, meskipun dalam kasus ini remote host harus menggunakan source port address yang sama sebagai original port address yang memicu NAT.*
   4. *Symmetric: adalah NAT di mana pemetaan NAT mengacu khusus untuk koneksi antara local host address dan port number dan destination address dan port number dan local address dan port ke publicside address dan port.*

Latihan (topologi soal shift sebelumnya)

1. Komputer di subnet ANUBIS tidak diizinkan mengakses server OSIRIS
2. Komputer di subnet SETH tidak dapat mengakses komputer di subnet HATHOR pada pukul 10.00 - 19.00
3. Komputer dari jaringan luar dapat mengakses web server di OSIRIS dengan membuat port forwarding ke server
4. Web server di OSIRIS hanya bisa diakses maksimal 5 client
5. Buatlah agar tiap subnet dapat mengakses internet menggunakan SNAT

MAIL SERVER

Mail Server atau *E-Mail Server* adalah perangkat lunak program yang mendistribusikan file atau informasi sebagai respons atas permintaan yang dikirim via email, mail server juga digunakan pada bitnet untuk menyediakan layanan serupa ftp. Selain itu mail server juga dapat dikatakan sebagaiaplikasi yang digunakan untuk penginstalan email.

Protokol Pada Mail Server

- **SMTP** *(Simple Mail Transfer Protocol)* digunakan sebagai standar untuk menampung dan mendistribusikan email.
- **POP3** *(Post Office Protocol v3)* dan **IMAP** *(Internet Mail Application Protocol)* digunakan agar user dapat mengambil dan membaca email secara remote yaitu tidak perlu login ke dalam sistem shelll mesin mail server tetapi cukup menguhubungi port tertentu dengan mail client yang mengimplementasikan protocol POP3 dan IMAP.

Server Pada Mail Server dan Penjelasannya

Pada mail server terdapat 2 server yang berbeda yaitu :

- **Outgoing Server (Sending email) :** Protocol server yang menangani adalah SMTP*(Simple Mail Transfer Protocol)* pada port 25.
- **Incoming Server (Receiving email) :** Protocol server yang menangani adalah POP3 *(Post Office Protocol)* pada port 110 atau IMAP *(Internet Message Access Protocol)* pada port 143.

Penjelasan dari Server yang menangani outgoing email dan incoming email sebagai berikut :

SMTP Server : Saat anda mengirimkan email maka email anda akan ditangani SMTP Server dan akan dikirim ke SMTP Server tujuan, baik secara langsung maupun melalui beberapa SMTP Server dijalurnya. Apabila server tujuan terkoneksi maka email akan dikirim, namun apabila tidak terjadi koneksi maka akan dimasukan ke dalam queue dan di resend setiap 15 menit, apabila dalam 5 hari tidak ada perubahan maka akan diberikan undeliver notice ke inbox pengirim.

POP3 Server : Jika menggunakan POP3 Server, apabila kita akan membaca email maka email pada server di download sehingga email hanya akan ada pada mesin yang mendownload email tersebut (kita hanya bisa membaca email tersebut pada device yang mendownload email tersebut).

IMAP Server : Jika menggunakan IMAP Server, email dapat dibuka kembali lewat device yang berbeda.

Tutorial Installasi

Ke Asisten Masing - Masing.