FIREWALL DAN IPTABLES PADA JARINGAN KOMPUTER

Peniarsih[1], Iswandir[2]
[1]peniarsih18@gmail.com, [2]iswandir11@gmail.com
[1,2]Universitas Dirgantara Marsekal Suryadarma

Abstrak

Perkembangan teknologi informasi, komputerisasi dan jaringan komputer tentu sangat bermanfaat, diantaranya membuat seseorang dapat berkomunikasi dan berhubungan dengan orang lain tanpa mengenal lagi yang namanya jarak. Telekomputer dapat memiliki lebih dari satu perkerjaaan yang berbeda letak geografisnya dan dapat dilakukannya dengan baik. Begitu juga dengan kebutuhan perusahaan. Perusahaan yang besar dan memiliki banyak cabang di lokasi yang berbeda tentu harus dapat memonitor cabang perusahaanya. Seiring jalannya waktu perkembangan teknologi dan jaringan komputer saat ini , perusahaan tersebut tidak harus langsung datang ke lokasi perusahaan cabang untuk mengecek keadaan perusahaan cabangnya, namun dengan manfaat jaringan komputer perusahaan dapat langsung memeriksa keadaan perusahaan cabangnya tanpa datang langsung ke lokasinya. Perusahaan cabang dapat melakukan *sharing* ke perusahaan. Namun, dampak dari perkembangan itu adalah semakin banyaknya permasalahan yang muncul dalam melindungi jaringan komputer dari gangguan luar seperti virus, spam, DOS, dan sebagainya. Jaringan komputer pun perlu memiliki ’pagar’ layaknya sebuah rumah. ’Pagar’ yang dapat melindungi tempat vital dalam komunikasi data dan menyimpan komponen penting dalam jaringan komputer.

Kata kunci : Firewall, Internet, Jaringan , Iptable

PENDAHULUAN

Latar Belakang

Perkembangan teknologi informasi, komputerisasi dan jaringan komputer tentu sangat bermanfaat, diantaranya membuat seseorang dapat berkomunikasi dan berhubungan dengan orang lain tanpa mengenal lagi yang namanya jarak. Telekomputer dapat memiliki lebih dari satu perkerjaaan yang berbeda letak geografisnya dan dapat dilakukannya dengan baik. Begitu juga dengan kebutuhan perusahaan. Perusahaan yang besar dan memiliki banyak cabang di lokasi yang berbeda tentu harus dapat memonitor cabang perusahaanya. Seiring jalannya waktu perkembangan teknologi dan jaringan komputer saat ini, perusahaan tersebut tidak harus langsung datang ke lokasi perusahaan cabang untuk mengecek keadaan perusahaan cabangnya, namun dengan manfaat jaringan komputer perusahaan dapat langsung memeriksa keadaan perusahaan cabangnya tanpa datang langsung ke lokasinya. Perusahaan cabang dapat melakukan *sharing* ke perusahaan.

Namun, dampak dari perkembangan itu adalah semakin banyaknya permasalahan yang muncul dalam melindungi jaringan komputer dari gangguan luar seperti virus, spam, DOS, dan sebagainya. Maka dari itu, sebuah jaringan komputer pun perlu memiliki ’pagar’ layaknya sebuah rumah. ’Pagar’ yang dapat melindungi tempat vital dalam komunikasi data dan menyimpan komponen penting dalam jaringan komputer.

Dalam istilah komputer, ’pagar’ tersebut sering disebut dengan istilah *firewall.* Sebuah sistem yang mengizinkan paket data lewat untuk paket yang

dianggapnya aman dan menolaknya jika paket data tersebut dianggap tidak aman.

Penulis membahas tentang firewall berserta jenisnya dan manfaat *firewall* pada umumnya. Tentunya penulis bukan ahli jaringan komputer ataupun terlalu paham mengenai *firewall.* Di dalam firewall semua komunikasi yang keluar dan masuk dikontrol. Port yang tidak penting dapat diblokir (ditutup) dan port yang penting dan berbahaya juga dapat diblokir, sehingga hanya pihak yang diijinkan saja yang boleh masuk melalui port tersebut. Cara ini merupakan sistem pengamanan jaringan komputer yang paling efektif dan banyak diguna-kan. Akan tetapi terkadang pemblokiran yang dilakukan sering menjadi tidak fleksibel, ketika dibutuhkan untuk menjalin komu-nikasi dengan apa yang ada di dalam jaringan, firewall tidak mengijinkannya karena mungkin memang berada pada area yang tidak diijinkan. Padahal komu-nikasi yang ingin dilakukan sangatlah penting untuk kelancaran kerja. Misalnya melakukan koneksi dengan internet dan butuh mengakses web server melalui SSH untuk memperbaiki konfigurasinya, sementara port SSH pada server tersebut dilarang untuk diakses dari internet oleh firewall, tentu hal ini akan sangat merepotkan. Untuk menghindari hal-hal semacam ini, ada suatu metode yang sangat efektif yaitu dengan menggunakan metode port knocking. Port knocking adalah suatu metode untuk membangun komunikasi antar komputer dari mana pun selama masing-masing komputer tersebut terhubung dalam suatu jaringan komputer, dengan perangkat komputer yang tidak membuka port komunikasi apapun secara bebas, tetapi perangkat tersebut masih tetap dapat diakses dari luar, dengan menggunakan suatu format konfigurasi port ketukan yang berupa percobaan untuk mengirimkan koneksi pada port ketukan

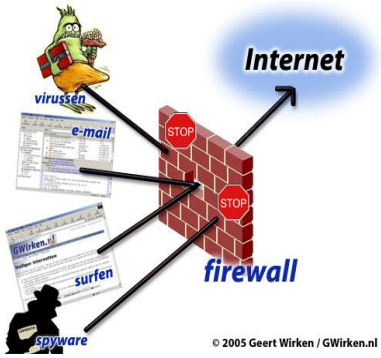
LANDASAN TEORI

Pengertian Firewall

"*Firewall* adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya. Firewall umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah firewall menjadi istilah generik yang merujuk pada sistem yang mengatur komunikasi antar dua jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke Inter-net dan juga tentu saja jaringan korporat di dalamnya, maka perlindungan terhadap aset digital perusahaan tersebut dari serangan para hacker, pelaku spionase, ataupun pencuri data lainnya, menjadi esensial."
Sumber:http://id.wikipedia.org/wiki/Fire wall

Jadi *firewall* adalah suatu mekani-sme untuk melindungi keamanan jaringan komputer dengan menyaring paket data yang keluar dan masuk di jaringan. Paket data yang *'baik'* diperbolehkan untuk melewati jaringan dan paket dapa yang dianggap *'jahat'* tidak diperbolehkan melewati jaringan. Firewall dapat berupa perangkat lunak atau perangkat keras yang ditanam perangkat lunak yang dapat menfilter paket data. Firewall dapat juga berupa suatu sikap yang ditanam dan diajarkan kepada staf IT suatu perusaha-an untuk tidak membocorkan data perusahaan kepada perusahaan. Ini untuk mencegah salah satu jenis hacking yaitu *social enggeneering.* Ataupun memberi kunci pengaman pada alat-alat komputer dan jaringan, contohnya memasukan

server ke dalam ruangan khusus dan dikunci. Kunci ruangan tersebut hanya dipegang oleh staf IT dan diperbolehkan menggunakan ruang tersebut atas seizin staf IT. Ini berfungsi selain menjaga kehilangan alat komputer dan jaringan secara fisik oleh pencuri atau perampokan, namun juga berfungsi menjaga kehilangan data yang tersimpan pada alat komputer tersebut. Bisa saja seseorang mencuri dan menghapus data penting perusahaan. Tentunya ini sangat merugikan perusahaan tersebut.



Gambar ilustrasi firewall

Fungsi Firewall

Fungsi firewall, antara lain:

1. Mengontrol dan mengawasi paket data yang mengalir di jaringan
   Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi firewall. Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan privat. Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain:
   a. Alamat IP dari komputer sumber
   b. Port TCP/UDP sumber dari sumber
   c. Alamat IP dari komputer tujuan
   d. Port TCP/UDP tujuan data pada komputer tujuan
   e. Informasi dari header yang disimpan dalam paket data
2. Melakukan autentifikasi terhadap akses. Applikasi proxy
   Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi
3. Mencatat semua kejadian di jaringan
   Mencatat setiap transaksi kejadian yang terjadi di firewall. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

Cara Kerja Firewall

Cara-cara firewall dalam melindungi jaringan komputer internal, antara lain:

1. Menolak dan memblokir paket data yang datang berdasarkan sumber dan tujaun yang tidak diinginkan.
2. Menolak dan menyaring paket data yang berasal dari jaringan intenal ke internet. Contoh nya ketika ada pengguna jaringan internel akan mengakses situs-situs porno.
3. Menolak dan menyaring paket data berdasakan konten yang tidak diinginkan. Misalnya firewall yang terintegrasi pada suatu antivirus akan menyaring dan mencegah file yang sudah terjangkit virus yang mencoba memasuki jaringan internal.
4. Melaporkan semua aktivitas jaringan dan kegiatan firewall.

Tipe-tipe Firewall

Tipe-tipe Firewall, antara lain:

1. Packet-Filtering Firewall
   Packet-Filtering Firewall adalah tipe firewall yang memeriksa dan membandingkan alamat sumber dari paket lewat dengan aturan atau kebijakan yang telah terdaftar pada filtering firewall. Pada firewall tipe ini akan diatur apakah paket data tersebut akan diperbolehkan lewat atau menolaknya. Aturan atau kebijakan peme-

riksaan didasarkan informasi yang dapat ditangkap dari packet header, yaitu antara lain:

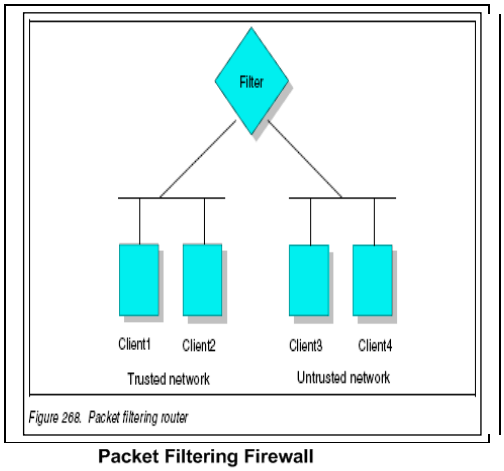
a. IP address sumber dan tujuan
b. Nomor port TCP/UDP sumber dan tujuan
c. Tipe ICMP message

Contoh aturan atau kebijakan packet filtering firewall :

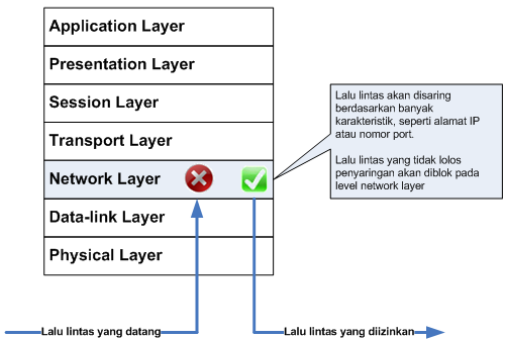
from	to	src port	dst port	proto	rule
*	www	*	80	tcp	allow
*	mail-gw	*	25	tcp	allow
squids	proxy	*	8080, 3128	*	allow
mynet	*	*	*	*	allow
*	*	*	*	*	deny

Gambar contoh rule packet filtering firewall

Ilustrasi cara kerja packet filtering firewall



Packet Filtering Firewall



Gambar ilustrasi packet filtering firewall

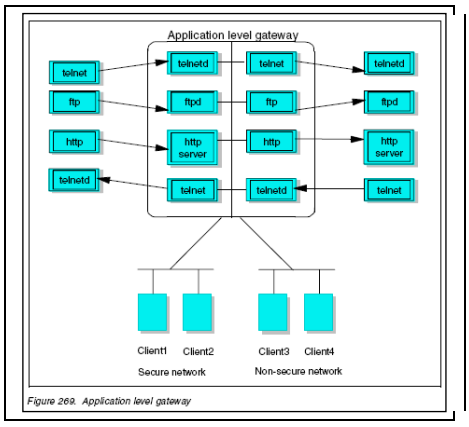
Satu aturan pada firewall jenis adalah melakukan penonaktifan port 23 yaitu protokol yang digunakan untuk telnet. Ini bertujuan untuk mencegah pengguna internet untuk mengakses layanan yang terdapat pada jaringan yang di firewallkan. Firewall ini juga dapat melakukan pengecualian terhadap aplikasi-aplikasi yang dapat berdapat berjalan di jaringan. Inilah salah satu kerumitan pada packet filtering tipe firewall, dikarena sulitnya menbuat aturan atau kebijakan yang akan diberlakuan untuk firewall. Kelebihan packet filtering firewall antara lain relatif mudah dalam pengimplementasikannya, transparan untuk pengguna, dan relatif lebih cepat.

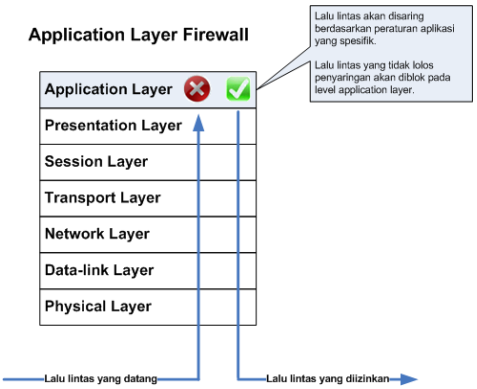
Adapun kekurangan tipe firewall ini antara lain sulit dalam membuat aturan dan kebijakan pada packet filtering firewall ini secara tepat guna dan aturan tersebut akan semakin banyak seiiring dengan banyak alamat IP sumber dan tujuan, port sumber dan tujuan yang dimasukan dalam kebijakan packet filtering firewall ini.

2. Application-Level Gateway (Proxy)
Application-levet gateway sering juga disebut application level firewall atau proxy firewall. Firewall ini tidak memperbolehkan paket data yang datang untuk melewati firewall sacara langsung. Applicatin level gateway menyediakan kontrol tingkat tinggi pada traffic antara dua jaringan yang isi layanan tertentu didalamnya dapat dimonitor dan difilter sesuai dengan kebijakan keamanan jaringan. Firewall tipe ini akan mengatur semua yang berkaitan dengan layer aplikasi, seperti ftp, telner, dll.

Kebanyakan, proxy firewall ini akan melakukan autentifikasi terhadap pengguna sebelum pengguna dapat melewati jaringan. firewall ini juga melakukan mekanisme pencatatan (logging) sebagai bagian dari aturan dan kebijakan keamanan yang diterapkannya. Contohnya apabila ada pengguna salah satu aplikasi seperti telnet untuk mengakses secara remote, maka gateway akan meminta pengguna untuk memasukan alamat remote host. Ketika pengguna mengirimkan username dan password serta informasi lain maka gateway akan melakukan pemeriksaan dan melakukan hubungan terhadap aplikasi tersebut yang sesuai dengan remote host. Apabila tidak sesuai, firewall tidak akan meneruskan dan menolak data tersebut.

Ilustrasi cara kerja application layer firewall





Gambar ilustrasi application layer firewall

Kelebihan application layer firewall antara lain: relatif lebih aman dibandingkan dengan packet filtering firewall, adanya pencatatan log setiap transaksi yang terjadi pada level aplikasi.

Kekurangan application layer firewall antara lain: pemrosesan tambahan yang berlebih pada setiap hubungan yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pengguna dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.

IPTABLE

Iptables adalah salah satu tools firewall pada sistem operasi Linux. Fungsi iptables adalah mengamankan jaringan dengan melakukan penyaringan trafik pada server VPS tanpa panel. DengaMengguakan iptables, dapat mengatur lalu lintas jaringan, termasuk mengizinkan atau memblokir koneksi yang masuk, keluar, atau sekedar melewati server. Iptables, membuat aturan pada server untuk mengelola jenis paket yang dapat diterima, mengatur trafik berdasarkan asal dan tujuan data, mengelola port, dan lainnya. iptables bekerja dengan membandingkan lalu lintas jaringan dengan serangkaian aturan yang telah dibuat. Jadi, semua paket dalam lalu lintas jaringan akan dicek.Pengaturan paket, iptables memiliki beberapa tabel yang berfungsi untuk menentukan arah putaran data. Setiap tabel tersebut memiliki rules atau kumpulan aturan yang disebut **chain**.

Jenis IPTABLE

1. **FILTER**. Tabel ini digunakan untuk menyaring paket yang masuk, keluar, ataupun yang hanya lewat. Caranya. dengan menggunakan beberapa aturan, yaitu:

- **ACCEPT**: Menerima paket yang masuk
- **REJECT**: Menolak/Memblokir paket yang masuk
- **DROP**: Memutuskan koneksi paket
- **LOG**: Mencatat paket

Tabel FILTER memiliki tiga chain, yaitu:

- **INPUT**: Chain ini menangani semua paket yang masuk ke server.
- **OUTPUT**: Chain ini menangani semua paket yang keluar dari server.
- **FORWARD**: Chain ini menangani paket yang diteruskan melalui server.

2. **NAT (Network Address Translation)**. Tabel ini digunakan untuk mengubah alamat asal tujuan dari sebuah paket. Ada dua chain pada tabel NAT:
   - **PRE-ROUTING (dstnat)**: Mengubah destination address pada sebuah paket data.
   - **POST-ROUTING (srcnat)**: Mengubah source address dari sebuah paket data.
3. **MANGLE**. Tabel ini digunakan untuk melakukan penghalusan pada proses pengaturan paket, dan memiliki kemampuan untuk menggunakan semua chain yang ada pada IPTABLES di atas.

PEMBAHASAN

Penggunakan iptables

Penggunakan iptables memiliki akses root ke server dapat langsung mengikuti langkah berikut ini, yaitu:

1. **Instalasi iptables**

   Untuk mengecek versi iptables yang terinstall pada Linux, Anda perlu melakukan koneksi ke server dengan cara menggunakan SSH. Caranya, login dengan username dan password yang dapat ditemukan pada detail SSH di panel VPS. jalankan perintah berikut: sudo iptables –V. Jika perintah tersebut menampilkan output versi iptables seperti gambar di bawah ini, maka iptables memang sudah terinstall pada Linux. root@webtestwriter #sudo iptable-v, iptable vl.6.0. Maka dapat langsung melanjutkan ke langkah outputnya berupa **command not found**, artinya iptables belum terinstall. Jadi, jalankan perintah berikut ini untuk menginstal iptables:

   sudo apt-get update
   sudo apt-get install iptables

   Saat proses instalasi iptables selesai dilaku an. Jika sudah berhasil, cek status konfigurasi dengan menjalankan perintah:

   sudo iptables -L –v

   Command **-L** pada perintah diatas digunakan untuk melihat list semua aturan yang ada.

   Sedangkan command **-v** digunakan untuk menunjukkan informasi list aturan tersebut secara detail. Contoh outputnya seperti ini:

   Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
   pkts bytes target prot opt in out source destination

   Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
   pkts bytes target prot opt in out source destination

   Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
   pkts bytes target prot opt in out source destination

   Iptables yang baru saja diinstall belum memiliki aturan apapun. Se-

hingga semua **paket yang masuk akan diterima tanpa filter**.

2. **Membuat Rules iptables**

   Rules iptables merupakan aturan untuk mengelola lalu lintas jaringan pada server. Rules ini akan ditambahkan pada suatu chain tertentu. Iptables menggunakan perintah -A (**Append**) sebagai tanda bahwa ada rules yang ditambahkan:

   ```
   sudo iptables -A
   ```

   Perintah di atas belum bisa dijalankan karena perintah **Append** tidak bisa berdiri sendiri. Perintah -A membutuhkan argumen pendukung untuk membuat suatu rules. Berikut ini merupakan argumen yang bisa Anda gunakan untuk membuat rules:

   - **-i : Interface** merupakan antarmuka jaringan yang akan Anda filter, seperti **eth0**, **lo**, dll.
   - **-p : Protocol** adalah protokol jaringan yang akan di cek dalam suatu rule. Misalnya **tcp**, **udp**, **icmp**, dll.
   - **-s : Source** adalah alamat trafik berasal (IP address atau hostname)
   - **-dport : Destination Port** merupakan nomor port suatu protokol, seperti **22** untuk SSH dan **80** untuk HTTP.
   - **-j : Jump** merupakan nama target (**ACCEPT, DROP, RETURN**) yang dituju ketika membuat rule yang baru.

   Argumen di atas tidak harus digunakan satu persatu. Sesuaikan saja dengan kebutuhan Anda. Namun, kalau perlu digunakan semua, urutannya harus seperti ini:

   ```
   sudo iptables -A <chain> -i <interface> -p <protocol (tcp/udp) > -s <source> --dport <port no.> -j <target>
   ```

   Menambahkan rules pada chain **INPUT** untuk memfilter koneksi yang masuk dan mencegah koneksi yang dapat membahayakan server. Rules iptables yang akan kami gunakan sebagai contoh adalah:

   1. Mengaktifkan Trafik pada Localhost
   2. Mengaktifkan Koneksi pada Port HTTP, HTTPS dan SSH
   3. Memfilter Koneksi Berdasarkan Sumber Paket
   4. Memutus Koneksi Trafik Lainnya
   5. Menghapus Rules

3. **Mengaktifkan Trafik pada Localhost**

   Untuk mengizinkan trafik pada localhost, jalankan perintah berikut ini:

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

   Perintah di atas memastikan koneksi antara database dan aplikasi web pada localhost bisa berjalan dengan baik.

4. **Mengaktifkan Koneksi pada Port HTTP, HTTPS dan SSH**

   Untuk memberikan izin akses ke port HTTP (**80**), HTTPS (**443**) dan SSH (**22**), jalankan perintah di bawah ini:

   ```
   sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
   sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
   sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
   ```

   Jika sudah, Anda dapat mengecek rules yang baru saja Anda buat dengan perintah:

   ```
   sudo iptables -L –v
   ```

5. **Memfilter Koneksi berdasarkan Sumber Paket**

   Untuk menyaring koneksi yang masuk berdasarkan IP address atau range IP address tertentu, tambahkan IP sumber paket berasal setelah perintah -s seperti ini:

   ```
   sudo iptables -A INPUT -s 192.168.1.2 -j ACCEPT
   ```

   Sebaliknya, untuk memutus koneksi IP tertentu, Anda bisa menjalankan perintah **DROP** berikut ini:

   ```
   sudo iptables -A INPUT -s 192.168.1.2 -j DROP
   ```

   Bisa memutus koneksi dari suatu range IP address dengan menambahkan perintah -m dan modul iprange. Kemudian, masukkan range IP address setelah perintah --src-range. Gunakan tanda pisah tanpa spasi (-) untuk memisahkan range IP Address. Untuk lebih lengkapnya:

   ```
   sudo iptables -A INPUT -m iprange --src-range 192.168.1.130-192.168.1.180 -j DROP
   ```

   Perintah di atas akan memutus koneksi dari range IP address **192.168.130** hingga **192.168.1.180**.

6. **Memutus Koneksi Trafik Lainnya**

   Setelah mengizinkan koneksi masuk dari port tertentu, bagaimana cara memutus semua paket dari trafik diluar rules yang telah Anda buat? Sebab, penting untuk mencegah koneksi asing mengakses server Anda melalui port yang terbuka, kan? Caranya, jalankan perintah berikut ini:

   ```
   sudo iptables -A INPUT -j DROP
   ```

   Nah, sekarang semua trafik dari luar port yang ditentukan pada rules telah terputus.

7. **Menghapus Rules**

   Ada kalanya Anda ingin menghapus semua rules untuk kembali membuat rules dari awal lagi. Untuk melakukannya, jalankan perintah **Flush** berikut ini:

   ```
   sudo iptables -F
   ```

   Anda juga bisa menghapus suatu rule secara spesifik dengan menggunakan perintah **Delete** atau -D. Namun, Anda perlu tahu dulu nomor line dari rule yang akan Anda hapus. Jadi, jalankan perintah di bawah ini:

   ```
   sudo iptables -L --line-numbers
   ```

   Pilih rule yang akan dihapus, kemudian ingatlah **chain** serta **nomornya**. Masukkan chain beserta nomor rule pada perintah delete sebagai berikut:

   ```
   sudo iptables -D [chain] [nomor rule]
   ```

   Sebagai contoh, Anda ingin menghapus rule nomor 2 pada chain INPUT. Maka, perintahnya adalah:

   ```
   sudo iptables -D INPUT 2
   ```

8. **Menyimpan Konfigurasi iptables secara Permanen**

   Rules iptables yang telah dibuat di atas akan hilang ketika server direstart. Jadi, pastikan Anda menyimpan konfigurasi iptables secara permanen dengan perintah di bawah ini:

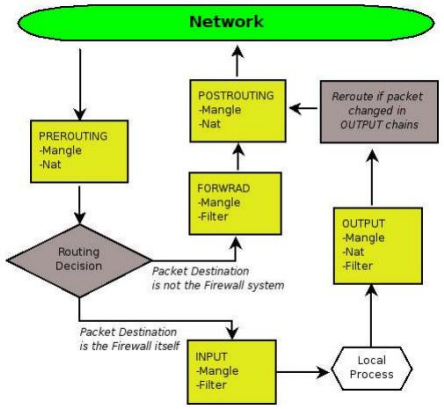
   ```
   sudo /sbin/iptables-save
   ```

   Jalankan perintah tersebut ketika ada perubahan pada rules iptables. Misalnya, ketika Anda ingin menghapus semua rules iptables, maka perlu menjalankan dua perintah berikut ini:

   ```
   sudo iptables -F
   sudo /sbin/iptables-save
   ```

Pengenalan Iptables

Iptables adalah salah satu tools firewall default pada system operasi linux. Iptables ini bekerja baik di kernel 2.4.x-2.6.x sedangkan untuk kernel 2.2.x masih menggunakan ipchains. Perintah 'iptables' digunakan untuk mengelola, memaintain, menginspeksi rule-rule IP packet filter dalam kernel linux.



Gambar Diagram Iptables

Penulis mencoba berbagi sedikit cara mengkonfigurasi firewall pada iptables di sistem operasi linux, khususnya distribusi ubuntu. Penulis menggunakan Ubuntu 8.04 kernel 2.6.24-16-generic dalam mencoba iptables.

Pada ubuntu, biasa telah terinstall iptables secara default. Konsep chain:

1. INPUT
   => semua paket yang masuk ke komputer melalui chain/rantai ini.
2. OUTPUT
   => semua paket yang kelua ke komputer melalui chain/rantai ini.
3. FORWARD
   =>paket data yang diterima dari satu jaringan dan diteruskan ke jaringan lainya.

Perintah umum iptables:

$iptables [-t table] command [match] [target/jump]

Berikut beberapa option dasar yang cukup sering dalam mengkonfigurasi iptables:

- -A
  Tambahan aturan ini ke rantai aturan yang ada. Rantai atau chain yang valid adalah INPUT, FORWARD, dan OUTPUT. Biasanya lebih banyak menggunakan rantai INPUT yang berdampak pada paket data yang masuk
- -L
  Memperlihatkan daftar aturan yang telah dipasang di iptables.
- -m state
  Menjelaskan daftar dari kondisi / state bagi aturan untuk di bandingkan. Beberapa state yang valid, adalah:
  NEW => sambungan baru dan belum pernah terlihat sebelumnya
  RELATED => sambungan baru, tapi berhubungan dengan sambungan lain telah diizinkan.
  ESTABLISHED => sambungan yang telah terjadi.
  INVALID => lalu lintas paket data yang karena berbagai alasan tidak bisa di identifikasi
- -m limit
  Dibutuhkan oleh aturan jika ingin melakukan pembandingan dan pencocokan dalam waktu / jumlah tertentu. Mengizinkan penggunaan option –limit. Berguna untuk membatasi aturan logging.
- --limit
  Kecepatan maksimum pencocokan, diberikan dalam bentuk angka yang diikuti oleh ”/seconf”, ”/minute”, ”/hour”, atau ”/day” tergantung seberapa sering kita ingin melakukan pencocokan aturan. Jika option ini tidak digunakan maka secara defaultnya adalah ”3/hour”
- -p
  Protokol yang digunakan untuk sambungan.

- --dport
  Port tujuan yang digunakan oleh aturan iptables. Bisa berupa satu port, bisa juga satu batasan jangkauan ditulis sebagai start:end, yang akan mencocokan semua port start sampai end
- -j
  Jump ke target yang spesifik. Iptables mempunyai empat target default, yaitu:
  ACCEPT
  ⇨ Accept / menerima paket dan berhenti memproses aturan dalam rantai aturan ini.
  REJECT
  ⇨ Reject /tolak paket data dan beritahu ke pengirim bahwa aturan firewall menolak paket data tersebut, stop pemrosesan aturan dalam rantai aturan ini
  DROP
  ⇨ Diam-diam mengacuhkan paket ini, dan stop pemrosesan aturan di rantai aturan ini.
  LOG
  ⇨ Log/catat paket, dan teruskan pemrosesan aturan di rantai aturan ini.
  ⇨ Mengijinkan penggunaan option --log –prefix dan --log -level
- --log –prefix
  Jika pencatatan dilakukan, letakan text atau tulisan sebelum catatan.
- --log –level
  Pencatatan menggunakan syslog level.
- -i
  Melakukan pencocokan jika paket yang masuk dari interface tertentu.
- -I
  Memasukan aturan ke iptables.
- -v
  Menampilkan lebih banyak informasi di layar

Untuk dapat melihat *manual* iptables, silakan ketik perintah ini pada terminal:

$man iptables

Manualnya terlihat seperti ini:

```
IPTABLES(8)                                                    IPTABLES(8)

NAME
       iptables - administration tool for IPv4 packet filtering and NAT

SYNOPSIS
       iptables [-t table] -[AD] chain rule-specification [options]
       iptables [-t table] -I chain [rulenum] rule-specification [options]
       iptables [-t table] -R chain rulenum rule-specification [options]
       iptables [-t table] -D chain rulenum [options]
       iptables [-t table] -[LFZ] [chain] [options]
       iptables [-t table] -N chain
       iptables [-t table] -X [chain]
       iptables [-t table] -P chain target [options]
       iptables [-t table] -E old-chain-name new-chain-name

DESCRIPTION
       Iptables  is  used  to  set  up, maintain, and inspect the tables of IP
       packet filter rules in the Linux kernel.  Several different tables  may
       be  defined.   Each  table contains a number of built-in chains and may
       also contain user-defined chains.

       Each chain is a list of rules which can match a set of  packets.   Each
Manual page iptables(8) line 1
```

Perintah dasar Iptables:

1. Untuk melihat aturan yang sudah ada di iptables:
   $iptables -L

   Jika komputer baru diinstall, aturan yang terpasang akan terlihat seperti ini:

```
root@ladast-laptop:~# 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
```

2. Untuk mengijinkan sesi sambungan yang terbentuk untuk menerima lalu lintas paket data
   $iptables -A INPUT -m state –state ESTABLISHED, RELATED -j accept

   Contohnya kita akan mengijinkan semua lalu lintas paket data di jaringan untuk masuk adalah sebagai berikut:
   $iptables -A INPUT -p tcp –dport 80 -j ACCEPT

```
root@ladast-laptop:~# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@ladast-laptop:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:www

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ladast-laptop:~# iptables -f
```

Mengijinkan lalu lintas paket data masuk ke defaut port SSH nomor 22, maka harus mengizinkan semua TCP paket data masuk ke port 22, perintahnya:

$iptables -A INPUT -p tcp --dport ssh -j ACCEPT

```
root@ladast-laptop:~# iptables -A INPUT -p tcp --dport ssh -j ACCEPT
root@ladast-laptop:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:www

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

Dari perintah diatas dapat mengetahui bahwa aturan iptables tersebut mangatur agar masukan aturan ini ke rantai input (-A INPUT) artinya kita melihat lalu lintas paket data yang masuk cek protokol yang digunakan adalah TCP (-p tcp). Jika TCP, apakah paket data menuju port SSH (--dport ssh). Jika ya, maka paket diterima,

3. Untuk melakukan pemblokiran paket data.
   Apabila aturan telah memutuskan untuk menerima paket data (ACCEPT), maka aturan selanjutnya tidak akan berefek pada paket data tersebut. Karena aturan yang kita buat mengijinkan SSH dan Web traffic, selama aturan untuk memblok semua traffic kita letakan terakhir sesudah aturan mengijinkan SSH dan Web, maka kita akan tetap dapat menerima traffic SSH dan Web yang kita inginkan. Jadi kita harus menambahkan (-A) aturan untuk mem-block traffic di akhir. Perintahnya:

$iptables -A INPUT -j DROP

```
root@ladast-laptop:~# iptables -A INPUT -j DROP
root@ladast-laptop:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:www
DROP       all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

4. Untuk melakukan pencatatan paket yang di log , perintah yang paling cepat adalah:
   $iptables -I INPUT 5 -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7

5. Untuk menyimpan konfigurasi iptables
   Jika kita *booting* komputer yang kita gunakan, maka apa yang kita lakukan ini akan hilang. Kita pun harun mengetikkan ulang semua perintah yang kita masukan satu per satu ketika komputer hidup. Agar lebih effesien, kita dapat menggunakan iptables-save dan iptables-restore untuk menyimpan dan me*restore* iptables

   Kita dapat menyimpan konfigurasi iptables agar di start setiap kali booting menggunakan perintah:

   $sh -c "iptables-save > /etc/iptables.rules"

   Setelah itu memodifikasi /etc/network/interfaces agar aturan iptables yang kita gunakan dapat berjalan secara automatis. Kita perlu mengetahui ke interface mana aturan yang akan digunakan. Biasanya menggunakan eth0. Untuk interface wireless, kita dapat mencek penggunaaannya mengunakan perintah:
   $ iwconfig

Kita perlu mengedit file /etc/network/interfaces misalnya menggunakan perintah

$ sudo nano /etc/network/interfaces

Apabila telah menemukan nama interface yang digunakan, maka di akhir interface kita dapat menambahkan perintah:

pre-up iptables-restore < /etc/iptables.rules

Selanjutnya di bawahnya kita tambahkan perintah sesudah interface down, menggunakan perintah:

post-down iptables-restore < /etc/iptables.rules

Hasil gambarnya:

6. Untuk menonaktifkan atau mematikan fiewall, maka perintahnya:

   $iptables –F

Adapun jika kesulitan dalam menkonfigurasi iptables secara *command line*, pada ubuntu telah tersedia perangkat lunak yang dapat mengkonfigurasi firewall secara menggunakan GUI yaitu firestater.

- cara menginstall firestarter di ubuntu 8.04
  - ketik perintah ini di terminal
  - sudo apt-get install firestater
- Tampilan dari firestarter pada saat memulai:

PENUTUP

Kesimpulan

Tidak ada satupun sistem buatan manusia yang dikatakan aman. Namun firewall adalah salah satu cara untuk melindungi jaringan dari pihak luar yang akan berbuat jahat ataupun iseng. Membuat aturan dan kebijakan pada firewall secara tepat setidaknya dapat melindungi jaringan dari ganggaun pihak luar. Firewall juga mencatat semua kejadian di jaringan sehingga dapat melakukan pendeteksian dini terhadap segala serangan yang mengancam di jaringan.

Iptables merupakan salah satu perangkat lunak firewall yang bekerja pada sistem operasi linux. Walaupan bersifat *free*,namun iptables cukup *powerfull* asalkan aturan dan kebijakan yang diterapkan di firewall tersebut sangat tepat dalam melindungi jaringan.

Di dalam penulisan jurnal ini, penulis hanya sedikit memberikan penjelasan mengenai iptables. Penulis menyerahkan kepada pembaca untuk dapat berkreasi dan mengembangkan lagi mengenai firewall dan pada iptables ini. Iptables bisa membantu Anda mengamankan server VPS. Cara menggunakan iptables juga cukup mudah. Asalkan Anda paham dengan basic syntaxnya, Anda sudah bisa membuat aturan atau rules iptables untuk keamanan server.Peningkatan keamanan mengguna-

kan iptables saja tentu tidak cukup. Anda perlu menggunakan server VPS yang mumpuni dan memberikan perlindungan keamanan yang baik.

Layanan **Cloud VPS Niagahoster** dapat menjadi salah satu pilihannya. Dengan tambahan fitur keamanan seperti DDoS Detection, Mod Security dan konfigurasi Firewall di VPS, Anda tidak perlu khawatir lagi dengan ancaman dari luar sistem.

Cloud VPS Niagahoster juga memungkinkan Anda untuk memilih **beragam sistem operasi** Linux untuk menginstall iptables di server Anda. Selain itu, dengan **Full Root Access** yang diberikan, Anda mempunyai kontrol penuh terhadap server dan konfigurasinya.

Saran

Sebelum menggunakan Jaringan baiknya cek dulu firewall akan tidak masuk hacker yang akan membahayakan kondisi jaringan. Dimana setiap jaringan harus dibuat firewll untuk keamanan data dan File yang ada didalam jaringan tersebut.

Melindungi jaringan komputer dari gangguan luar seperti virus, spam, DOS, dan sebagainya. Jaringan komputer pun perlu memiliki 'pagar' layaknya sebuah rumah. 'Pagar' yang dapat melindungi tempat vital dalam komunikasi data dan menyimpan komponen penting dalam jaringan komputer.

Daftar Pustaka

Buku:

Pribadi, Harijanto.2008.*Firewall melindungi jaringan dari DdoS menggunakan LINUX+MIKROTIK*. Penerbit Andi : Yogyakarta.

E-Book Online:

Ahmad Muammar. W. K.2004. *FireWall.* Ilmukomputer.com

JiroKul. Bermain dengan Firewall Default.Terbitan Online Kecoak Elektronik http://k-elektronik.org

http://ezine.echo.or.id

Sriwijaya, Riki.2003.Firewall. ilmukomputer.com

FIREWALL.IDS.INDOCISC/BIN

Internet:

http://id.wikipedia.org/wiki/Firewall

http://linux.or.id/node/2929

http://students.ukdw.ac.id/%7E22022807/kommasd.html

http://dwiyatmoko.multiply.com/journal

http://sdn.vlsm.org/share/ServerLinux/node161.html

http://opensource.telkomspeedy.com/wiki/index.php/Mini_Howto_iptables_untuk_Firewal