FIREWALL: SEKURITI INTERNET

Eueung Mulyana & Onno W. Purbo
Computer Network Research Group ITB

Internet merupakan sebuah jaringan komputer yang sangat terbuka di dunia, konsekuensi yang harus di tanggung adalah tidak ada jaminan keamanan bagi jaringan yang terkait ke Internet. Artinya jika operator jaringan tidak hati-hati dalam menset-up sistemnya, maka kemungkinan besar jaringan yang terkait ke Internet akan dengan mudah dimasuki orang yang tidak di undang dari luar. Adalah tugas dari operator jaringan yang bersangkutan, untuk menekan resiko tersebut seminimal mungkin. Pemilihan strategi dan kecakapan administrator jaringan ini, akan sangat membedakan apakah suatu jaringan mudah ditembus atau tidak.

Firewall merupakan alat untuk mengimplementasikan kebijakan security (*security policy*). Sedangkan kebijakan security, dibuat berdasarkan perimbangan antara fasilitas yang disediakan dengan implikasi security-nya. Semakin ketat kebijakan security, semakin kompleks konfigurasi layanan informasi atau semakin sedikit fasilitas yang tersedia di jaringan. Sebaliknya, dengan semakin banyak fasilitas yang tersedia atau sedemikian sederhananya konfigurasi yang diterapkan, maka semakin mudah orang orang '*usil*' dari luar masuk kedalam sistem (akibat langsung dari lemahnya kebijakan security).

Tulisan ini akan mencoba melihat beberapa kebijakan sekuriti yang lazim digunakan pada saat mengkaitkan sebuah jaringan ke Internet.

FIREWALL

Firewall adalah istilah yang biasa digunakan untuk menunjuk pada suatu komponen atau sekumpulan komponen jaringan, yang berfungsi membatasi akses antara dua jaringan, lebih khusus lagi, antara jaringan internal dengan jaringan global Internet. Firewall mempunyai beberapa tugas:

- Pertama dan yang terpenting adalah: harus dapat mengimplementasikan kebijakan security di jaringan (*site security policy*). Jika aksi tertentu tidak diperbolehkan oleh kebijakan ini, maka firewall harus meyakinkan bahwa semua usaha yang mewakili operasi tersebut harus gagal atau digagalkan. Dengan demikian, semua akses ilegal antar jaringan (tidak diotorisasikan) akan ditolak.
- Melakukan filtering: mewajibkan semua traffik yang ada untuk dilewatkan melalui firewall bagi semua proses pemberian dan pemanfaatan layanan informasi. Dalam konteks ini, aliran paket data dari/menuju firewall, diseleksi berdasarkan IP-address, nomor port, atau arahnya, dan disesuaikan dengan kebijakan security.
- Firewall juga harus dapat merekam/mencatat even-even mencurigakan serta memberitahu administrator terhadap segala usaha-usaha menembus kebijakan security.

MERENCANAKAN JARINGAN DENGAN FIREWALL

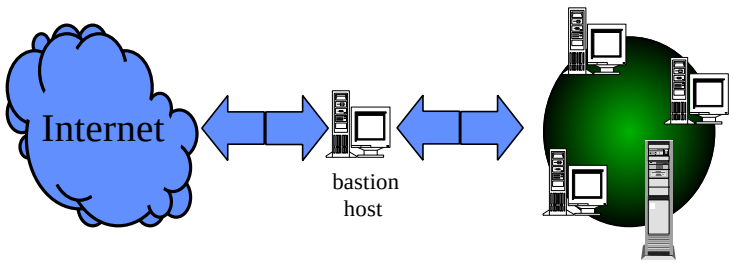
Merencanakan sistem firewall pada jaringan, berkaitan erat dengan jenis fasilitas apa yang akan disediakan bagi para pemakai, sejauh mana level resiko-security yang bisa diterima, serta berapa banyak waktu, biaya dan keahlian yang tersedia (faktor teknis dan ekonomis). Firewall umumnya terdiri dari bagian filter (disebut juga *screen* atau *choke*) dan bagian gateway (*gate*). Filter berfungsi untuk membatasi akses, mempersempit kanal, atau untuk memblok kelas trafik tertentu. Terjadinya pembatasan akses, berarti akan mengurangi fungsi jaringan. Untuk tetap menjaga fungsi komunikasi jaringan dalam lingkungan yang ber-firewall, umumnya ditempuh dua cara:

- Pertama, bila kita bayangkan jaringan kita berada dalam perlindungan sebuah benteng, komunikasi dapat terjadi melalui pintu-pintu keluar benteng tersebut. Cara ini dikenal sebagai *packet-filtering*, dimana filter hanya digunakan untuk menolak trafik pada kanal yang tidak digunakan atau kanal dengan resiko-security cukup besar, sedangkan trafik pada kanal yang lain masih tetap diperbolehkan.
- Cara kedua, menggunakan sistem *proxy*, dimana setiap komunikasi yang terjadi antar kedua jaringan harus dilakukan melalui suatu operator, dalam hal ini *proxy server*. Beberapa protokol, seperti telnet dan SMTP(*Simple Mail Transport Protocol*), akan lebih efektif ditangani dengan evaluasi paket (*packet filtering*), sedangkan yang lain seperti FTP (*File Transport Protocol*), Archie, Gopher dan HTTP (*Hyper-Text Transport Protocol*) akan lebih efektif ditangani dengan sistem proxy. Kebanyakan firewall menggunakan kombinasi kedua teknik ini (*packet filtering* dan *proxy*).

Ada banyak literatur yang membahas masalah security & membagi arsitektur dasar firewall menjadi tiga jenis. Masing masing adalah:

- arsitektur dengan dual-homed host (kadang kadang dikenal juga sebagai *dual homed gateway*/ DHG)
- screened-host (*screened host gateway*/ SHG)
- screened subnet (*screened subnet gateway*/ SSG).

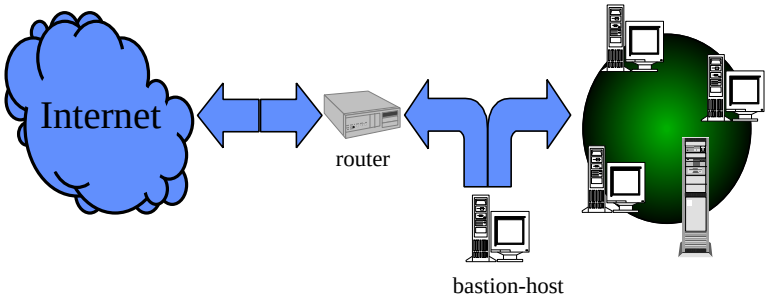
Sistem DHG menggunakan sebuah komputer dengan (paling sedikit) dua network-interface. Interface pertama dihubungkan dengan jaringan internal dan yang lainnya dengan Internet. Dual-homed host nya sendiri berfungsi sebagai bastion host (front terdepan, bagian terpenting dalam firewall).



Arsitektur dengan dual-homed host

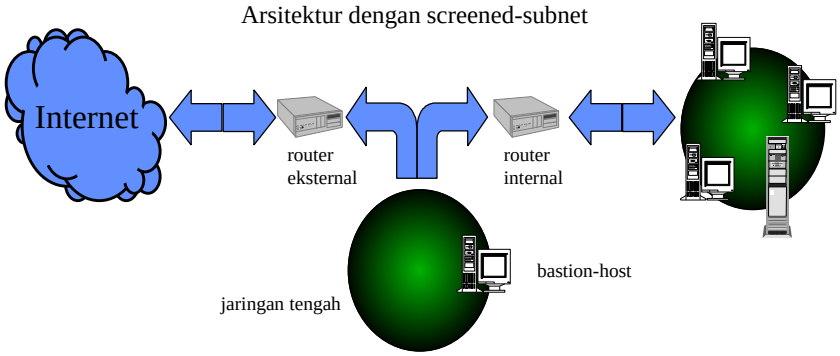
Pada topologi SHG, fungsi firewall dilakukan oleh sebuah screening-router dan bastion host. Router ini dikonfigurasi sedemikian sehingga akan menolak semua trafik kecuali

yang ditujukan ke bastion host, sedangkan pada trafik internal tidak dilakukan pembatasan. Dengan cara ini setiap client servis pada jaringan internal dapat menggunakan fasilitas komunikasi standard dengan Internet tanpa harus melalui proxy.



Arsitektur dengan screened-host

Firewall dengan arsitektur screened-subnet menggunakan dua screening-router dan jaringan tengah (*perimeter network*) antara kedua router tersebut, dimana ditempatkan bastion host. Kelebihan susunan ini akan terlihat pada waktu optimasi penempatan server.



Selanjutnya, bagaimana relevansi arsitektur firewall tersebut terhadap level security? Suatu jaringan harus dapat menangani interaksi client-server, tidak terkecuali dengan kehadiran firewall. Sejauh ini, untuk operasi client internal - server internal, atau client internal - server eksternal, tidak terlalu menimbulkan masalah. Jika kita akan membuat sistem firewall untuk jaringan demikian, hanya dengan memasang proxy server pada bastion host dalam arsitektur yang dipilih, kualitas proteksi firewall yang bersangkutan akan maksimal. Artinya ‘keselamatan’ seluruh jaringan, sekarang hanya tergantung pada baik-tidaknya atau seberapa ‘bagus’ firewall tersebut dan tidak tergantung pada program-program yang lain. Beda halnya bila jaringan kita akan mendukung operasi client eksternal - server internal, atau dengan kata lain: jaringan internal kita menyediakan layanan informasi yang dapat diakses dari luar. Dalam konteks ini, harus diperhitungkan metoda penempatan mesin yang menjalankan program server, supaya mesin tersebut dapat dikenali dari internet dan sedemikian, komunikasi dengan client-nya dapat berlangsung dengan baik tanpa mengorbankan kepentingan security.

Arsitektur dual-homed menawarkan solusi sederhana dan murah. Satu-satunya mesin yang dikenal dari internet dalam sistem ini adalah dual-homed host-nya sendiri, dan dengan demikian ia menjadi satu-satunya mesin alternatif untuk menjalankan

program server. Tetapi akan bermanfaat untuk mengingat, bahwa semakin banyak layanan yang disediakan atau semakin banyak program yang berjalan pada bastion-host, maka peluang penyusupan ke komputer tersebut semakin besar. Karena, seperti diyakini banyak orang, hampir dipastikan tidak ada program apapun yang bebas sama sekali dari bugs, apalagi untuk program-program berukuran besar. Dan sekali bugs ini dapat dieksploitasi oleh seseorang yang kemudian masuk ke dalam bastion-host, maka seluruh komputer di jaringan kita akan menjadi terbuka! Jika faktor ekonomis memaksa kita untuk tetap mengimplementasikan arsitektur DHG, maka ada beberapa nasihat yang patut diperhatikan, diantaranya: menggunakan perangkat lunak server yang telah teruji relatif 'aman' serta berukuran kecil, mereduksi dan mengoptimasi jumlah program yang berjalan, kemudian tidak memberikan *account* reguler pada bastion-host.

Dua arsitektur lainnya, screened-host dan screened-subnet, menyediakan pilihan lebih banyak. Screening-router dapat diatur untuk melakukan operasi packet filtering yang memungkinkan mesin-mesin tertentu dapat dikenali dari luar. Mesin mesin ini, kemudian menjalankan program-program server yang dapat diakses dari internet. Resiko dengan metoda seperti ini adalah penambahan jumlah komputer yang mungkin untuk diserang, sehingga akan lebih baik jika sebelumnya kita menyiapkan mesin-mesin tersebut dengan level security paling tidak sama dengan bastion-host atau kalau bisa, lebih.

PACKET FILTERING

Berbagai kebijakan dapat diterapkan dalam melakukan operasi packet filtering. Pada intinya, berupa mekanisme pengontrollan data yang diperbolehkan mengalir dari dan/atau ke jaringan internal, dengan menggunakan beberapa parameter yang tercantum dalam header paket data: arah (*inbound* atau *outbound*), address asal dan tujuan, port asal dan tujuan, serta jenis protokol transport. Router akan mengevaluasi informasi ini dalam setiap paket data yang mengalir melaluinya, kemudian menetapkan aksi yang harus dilakukan terhadap paket tersebut, berdasarkan set aturan/program dalam packet-filtering. Sehingga keputusan routing dasar router tersebut, kemudian dilengkapi dengan bagian dari kebijakan security jaringan.

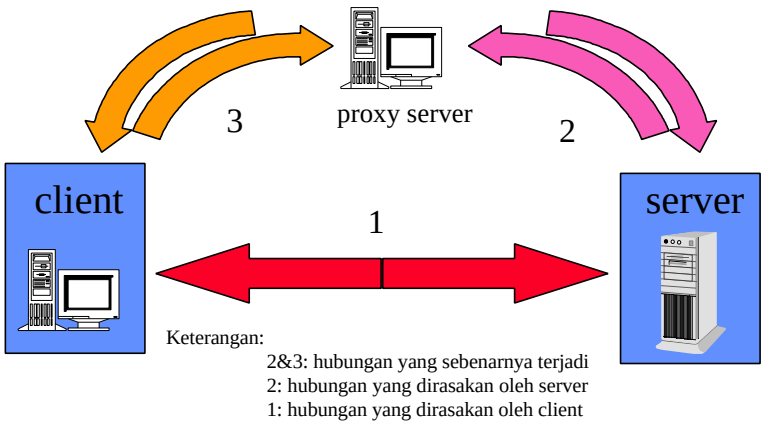
Tabel berikut akan menunjukan contoh konfigurasi operasi packet-filtering, untuk menyediakan **hanya** fasilitas SMTP inbound dan outbound pada jaringan.

Aturan	arah	address asal	address tujuan	protokol	port tujuan	aksi
A	masuk	eksternal	internal	TCP	25	ok
B	keluar	internal	eksternal	TCP	>1023	ok
C	keluar	internal	eksternal	TCP	25	ok
D	masuk	eksternal	internal	TCP	>1023	ok
E	sembaran g	sembarang	sembarang	sembarang	sembarang	deny

Aturan A dan B melayani hubungan SMTP inbound (email datang), aturan C dan D melayani hubungan SMTP outbound (email keluar) serta aturan E merupakan aturan default yang dilakukan bila aturan aturan sebelumnya gagal. Kalau diamati lebih dekat, selain trafik SMTP konfigurasi tersebut juga masih membolehkan hubungan masuk dan keluar pada port >1023 (aturan B dan D), sehingga terdapat kemungkinan bagi program-program server seperti X11 (port 6000), OpenWindows (port 2000), atau kebanyakan program basis-data (Sybase, Oracle, Informix, dll), untuk dihubungi dari luar. Untuk menutup kemungkinan ini, diperlukan evaluasi parameter lain, seperti evaluasi port asal. Dengan cara ini, satu-satunya celah menembus firewall adalah dengan menggunakan port SMTP. Bila kita masih juga kurang yakin dengan kejujuran para pengguna port ini, dapat dilakukan evaluasi lebih lanjut dari informasi ACK.

PROXY

Dalam jaringan yang menerapkan sistem proxy, hubungan komunikasi ke internet dilakukan melalui sistem pendelegasian. Komputer-komputer yang dapat dikenali oleh internet bertindak sebagai ‘wakil’ bagi mesin lain yang ingin berhubungan ke luar. Proxy server untuk (kumpulan) protokol tertentu dijalankan pada dual-homed host atau bastion-host, dimana seluruh pemakai jaringan dapat berkomunikasi dengannya, kemudian proxy server ini bertindak sebagai delegasi. Dengan kata lain setiap program client akan berhubungan dengan proxy server dan proxy server ini lah yang akan berhubungan dengan server sebenarnya di internet. Proxy server akan mengevaluasi setiap permintaan hubungan dari client dan memutuskan mana yang diperbolehkan dan mana yang tidak. Bila permintaan hubungan ini disetujui, maka proxy server me-relay permintaan tersebut pada server sebenarnya.



Ada beberapa istilah menunjuk pada tipe proxy server, diantaranya proxy level aplikasi, proxy level *circuit*, proxy generik atau khusus, proxy cerdas dll. Apapun jenis proxy yang digunakan, ada beberapa konsekuensi implementasi sistem ini:

- pada umumnya memerlukan modifikasi client dan/atau prosedur akses serta menuntut penyediaan program server berbeda untuk setiap aplikasi.
- Penggunaan sistem proxy memungkinkan penggunaan *private IP Address* bagi jaringan internal. Konsekuensinya kita bisa memilih untuk menggunakan IP Address kelas A (10.x.x.x) untuk private IP address yang digunakan dalam jaringan internet;

sehingga komputer yang dapat tersambung dalam jaringan internal dapat mencapai jumlah jutaan komputer.

- Paket SOCKS atau TIS FWTK merupakan contoh paket perangkat lunak proxy yang sering digunakan dan tersedia bebas di internet.

Penutup

Masalah keamanan jaringan merupakan masalah yang sering di menjadi momok bagi rekan-rekan yang ingin mengkaitkan sebuah institusi ke Internet. Tulisan ini berharap untuk memberikan sedikit masukan awal yang menjelaskan bahwa ada beberapa teknik keamanan yang dapat menjamin sekuriti jaringan yang terkait ke Internet.