Firewall, dari Masa ke Masa

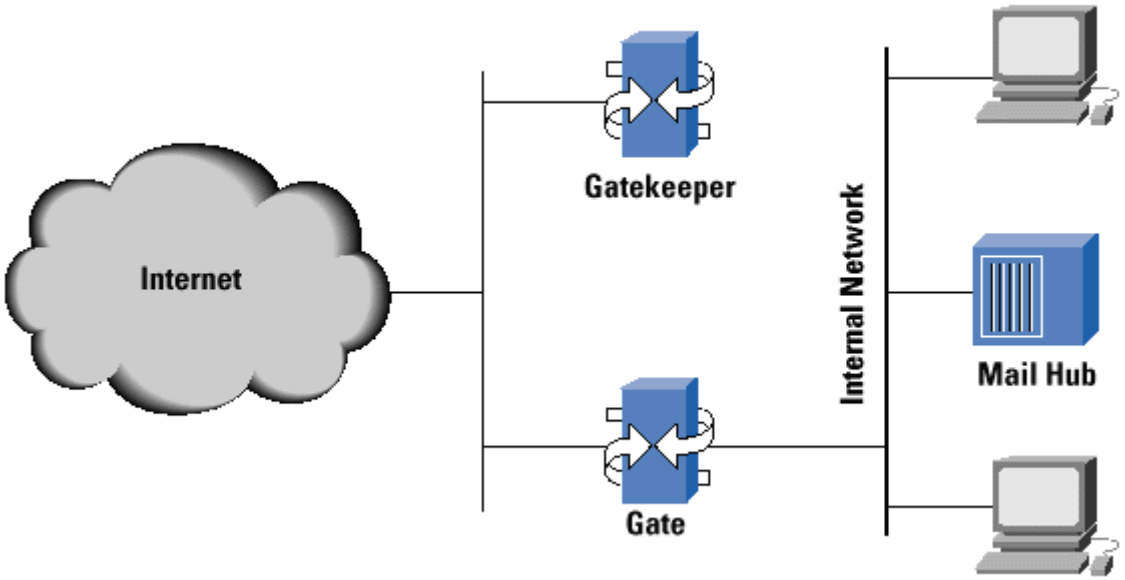
Dewasa ini, minat dan pemahaman terhadap sistem keamanan jaringan (*network security*) semakin meningkat seiring dengan tingginya kebutuhan untuk itu. Hal ini, tidak diragukan lagi, terjadi akibat meluasnya penggunaan internet dan banyaknya perusahaan yang telah mengimplementasikan teknologi informasi berbasis jaringan pada bisnis mereka. Internet firewall, dengan segala kelebihan maupun kekurangannya, adalah salah satu mekanisme pengamanan yang paling banyak dipakai saat ini. Dalam artikel ini, kita akan mempelajari secara sepintas tentang apa itu internet firewall, sejarahnya, serta melihat bagaimana ia digunakan pada saat ini maupun di masa mendatang.

Istilah "firewall" sendiri sebenarnya juga dikenal dalam disiplin lain, dan dalam kenyataannya, istilah ini tidak hanya bersangkutan dengan terminologi jaringan. Kita juga menggunakan firewall, misalnya untuk memisahkan garasi dari rumah, atau memisahkan satu apartemen dengan apartemen lainnya. Dalam hal ini, firewall adalah penahan (*barrier*) terhadap api yang dimaksudkan untuk memperlambat penyebaran api seandainya terjadi kebakaran sebelum petugas pemadam kebakaran datang untuk memadamkan api. Contoh lain dari firewall juga bisa ditemui pada kendaran bermotor, dimana firewall memisahkan antara ruang penumpang dan kompartemen mesin.

Dalam terminologi internet, istilah "firewall" didefinisikan sebagai sebuah titik diantara dua/lebih jaringan dimana semua lalu lintas (trafik) harus melaluinya (*chooke point*); trafik dapat dikendalikan oleh dan diautentifikasi melalui sautu perangkat, dan seluruh trafik selalu dalam kondisi tercatat (*logged*). Dengan kata lain, "firewall adalah penghalang (*barrier*) antara 'kita' dan 'mereka' dengan nilai yang diatur (*arbitrary*) pada 'mereka'" (Chesswick, W & Bellovin, S., 1994).

Network firewall yang pertama muncul pada akhir era 1980-an, berupa perangkat router yang dipakai untuk memisahkan suatu network menjadi jaringan lokal (LAN) yang lebih kecil. Dalam kondisi ini, penggunaan firewall hanya dimaksudkan untuk mengurangi masalah peluberan (*spill over*) data dari LAN ke seluruh jaringan. Hal ini mencegah masalah-masalah semacam error pada manajemen jaringan, atau aplikasi yang terlalu banyak menggunakan sumber daya meluber ke seluruh jaringan. Firewall untuk keperluan sekuriti (*security firewall*) pertama kali digunakan pada awal dekade 1990-an, berupa router IP dengan aturan filter tertentu. Aturan sekuriti saat itu berupa sesuatu seperti: ijinkan setiap orang "di sini" untuk mengakses "ke luar sana", juga cegahlah setiap orang (atau apa saja yang tidak disukai) "di luar sana" untuk masuk "ke sini". Firewall semacam ini cukup efektif, tetapi memiliki kemampuan yang terbatas. Seringkali sangat sulit untuk menggunakan aturan filter secara benar. Sebagai contoh, dalam beberapa kasus terjadi kesulitan dalam mengenali seluruh bagian dari suatu aplikasi yang dikenakan restriksi. Dalam kasus lainnya, aturan filter harus dirubah apabila ada perubahan "di luar sana".

Firewall generasi selanjutnya lebih fleksibel, yaitu berupa sebuah firewall yang dibangun pada apa yang disebut "bastion hosts". Firewall komersial yang pertama dari tipe ini, yang menggunakan filter dan gateway aplikasi (*proxies*), kemungkinan adalah produk dari Digital Equipment Corp. (DEC) yang dibangun berdasarkan firewall korporat DEC. Brian Reid dan tim engineering di laboratorium sistem jaringan DEC di Pallo Alto adalah pencipta firewall DEC. Firewall komersial pertama dikonfigurasi untuk, dan dikirimkan kepada pelanggan pertamanya, sebuah perusahaan kimia besar yang berbasis di pantai timur AS pada 13 Juni 1991. Dalam beberapa bulan kemudian, Marcus Ranum dari Digital Corp. menciptakan security proxies dan menulis ulang sebagian besar kode program firewall. Produk firewall tersebut kemudian diproduksi massal dengan nama dagang DEC SEAL (singkatan dari *Security External Access Link*). DEC SEAL tersusun atas sebuah sistem eksternal yang disebut *gatekeeper* sebagai satu-satunya sistem yang dapat berhubungan dengan internet, sebuah *filtering gateway* yang disebut *gate*, dan sebuah mailhub internal (lihat gambar 1).



Gambar 1: DEC SEAL, Firewall komersial yang pertama.

Dalam rentang waktu yang sama, Chesswick dan Bellovin di Bell labs bereksperimen dengan firewall yang berbasis sirkuit relay. Sebagai hasilnya, *Raptor Eagle* muncul sekitar 6 bulan setelah DEC SEAL diluncurkan, diikuti kemudian oleh produk *ANS InterLock*.

Pada 1 Oktober 1993, *Trusted Information System* (TIS) *Firewall Toolkit* (FWTK) diluncurkan dalam bentuk kode sumber (*source code*) ke komunitas internet. Ini menyediakan basis dari produk firewall komersial dari TIS yang kemudian dinamai *Gauntlet*. Dalam fase ini, FWTK masih digunakan untuk keperluan eksperimen, dan untuk kalangan industri dan pemerintahan sebagai basis dari sekuriti jaringan internet mereka. Pada 1994, *Check Point* menyusul dengan produknya, *Firewall-1* yang memperkenalkan kemudahan penggunaan (*user friendliness*) di dunia sekuriti internet. Generasi firewall sebelum Firewall-1 memerlukan editing file berformat ASCII dengan ASCII editor. Check Point memperkenalkan ikon, warna, kendali mouse, konfigurasi berbasis X-11, dan antarmuka manajemen (management interface) sehingga sangat memudahkan proses instalasi dan administrasi firewall.

Kebutuhan firewall generasi awal lebih mudah untuk didukung karena dibatasi oleh layanan internet yang tersedia pada masa itu. Tipikal organisasi atau bisnis yang terkoneksi ke internet saat itu hanya memerlukan akses yang secure ke remote terminal access (Telnet), file transfer (FTP), electronic mail (SMTP), dan Usenet (Network News Transfer Protocol, NNTP). Dewasa ini kita menambahkan daftar ini dengan akses ke web, live news broadcasts, informasi cuaca, perkembangan bursa saham, music on demand, audio dan videoconferencing, telephony, akses database, filer sharing, dan segudang layanan lainnya.

Apa saja kerapuhan (*vulnerability*) dari layanan-layanan baru ini? Apa resikonya? Seringkali jawabannya adalah “kita belum tahu”.

Jenis-Jenis Firewall

Ada empat jenis firewall, atau lebih tepatnya tiga jenis ditambah dengan satu tipe hybrid (campuran). Disini kita tidak akan membahas setiap jenis secara rinci karena itu membutuhkan pembahasan tersendiri yang lebih teknis dan umumnya sudah tersedia dalam dokumentasi-dokumentasi tentang firewall. Keempat jenis tersebut masing-masing adalah:

1. **Packet Filtering:** Firewall jenis ini memfilter paket data berdasarkan alamat dan opsi-opsi yang sudah ditentukan terhadap paket tersebut. Ia bekerja dalam level IP paket data dan membuat keputusan mengenai tindakan selanjutnya (diteruskan atau tidak diteruskan) berdasarkan kondisi dari paket tersebut. Firewall jenis ini terbagi lagi menjadi tiga subtipe:
    - *Static Filtering*: Jenis filter yang diiplementasikan pada kebanyakan router, dimana modifikasi terhadap aturan-aturan filter harus dilakukan secara manual.
    - *Dynamic Filtering*: Apabila proses-proses tertentu di sisi luar jaringan dapat merubah aturan filer secara dinamis berdasarkan even-even tertentu yang diobservasi oleh router (sebagai contoh, paket FTP dari sisi luar dapat diijinkan apabila seseorang dari sisi dalam me-request sesi FTP).
    - *Stateful Inspection*: Dikembangkan berdasarkan teknologi yang sama dengan dynamic filtering dengan tambahan fungsi eksaminasi secara bertingkat berdasarkan muatan data yang terkandung dalam paket IP.

    Baik dynamic maupun stateful filtering menggunakan tabel status (*state table*) dinamis yang akan membuat aturan-aturan filter sesuai dengan even yang tengah berlangsung.

2. **Circuit Gateways:** Firewall jenis ini beroperasi pada layer (lapisan) transpor pada network, dimana koneksi juga diautorisasi berdasarkan alamat. Sebagaimana halnya Packet Filtering, Circuit Gateway (biasanya) tidak dapat memonitor trafik data yang mengalir antara satu network dengan network lainnya, tetapi ia mencegah koneksi langsung antar network.
3. **Application Gateways:** Firewall tipe ini juga disebut sebagai firewall berbasis proxy. Ia beroperasi di level aplikasi dan dapat mempelajari informasi pada level data aplikasi (yang dimaksudkan disini adalah isi [*content*] dari paket data karena proxy pada dasarnya tidak beroperasi pada paket data). Filterisasi dilakukan berdasarkan data aplikasi, seperti perintah-perintah FTP atau URL yang diakses lewat HTTP. Dapat dikatakan bahwa firewall jenis ini "memecah model client-server".
4. **Hybrid Firewalls:** Firewall jenis ini menggunakan elemen-elemen dari satu atau lebih tipe firewall. Hybrid firewall sebenarnya bukan sesuatu yang baru. Firewall komersial yang pertama, DEC SEAL, adalah firewall berjenis hybrid, dengan menggunakan proxy pada sebuah bastion hosts (mesin yang dilabeli sebagai "gatekeeper" pada gambar 1) dan packet filtering pada gateway ("gate"). Sistem hybrid seringkali digunakan untuk menambahkan layanan baru secara cepat pada sistem firewall yang sudah tersedia. Kita bisa saja menambahkan sebuah *circuit gateway* atau *packet filtering* pada firewall berjenis *application gateway*, karena untuk itu hanya diperlukan kode proxy yang baru yang ditulis untuk setiap service baru yang akan disediakan. Kita juga dapat memberikan autentifikasi pengguna yang lebih ketat pada *Stateful Packet Filer* dengan menambahkan proxy untuk tiap service.

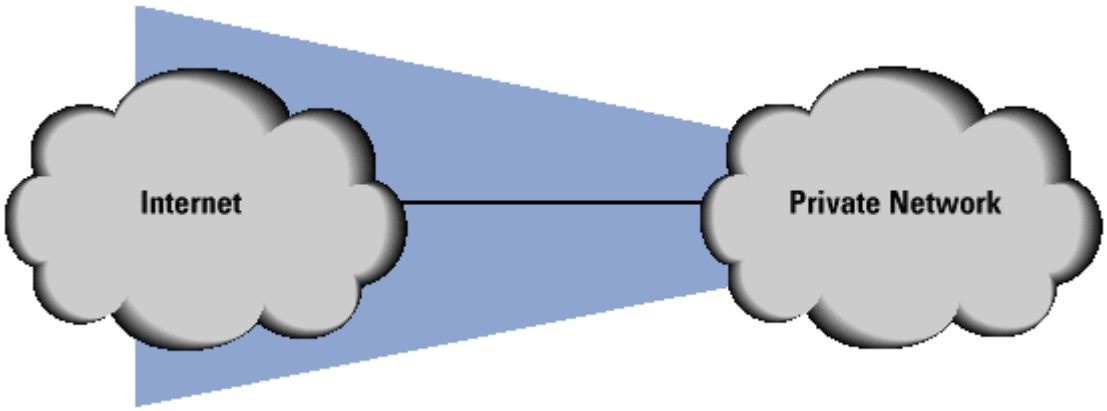
Apapun basis teknologi yang digunakan, sebuah firewall pada dasarnya berlaku sebagai sebuah *gateway* yang terkontrol di antara dua atau lebih *network* dimana setiap trafik harus melewatinya. Sebuah firewall menjalankan aturan sekuriti dan meninggalkan jejak yang dapat ditelusuri.

Pemanfaatan Firewall

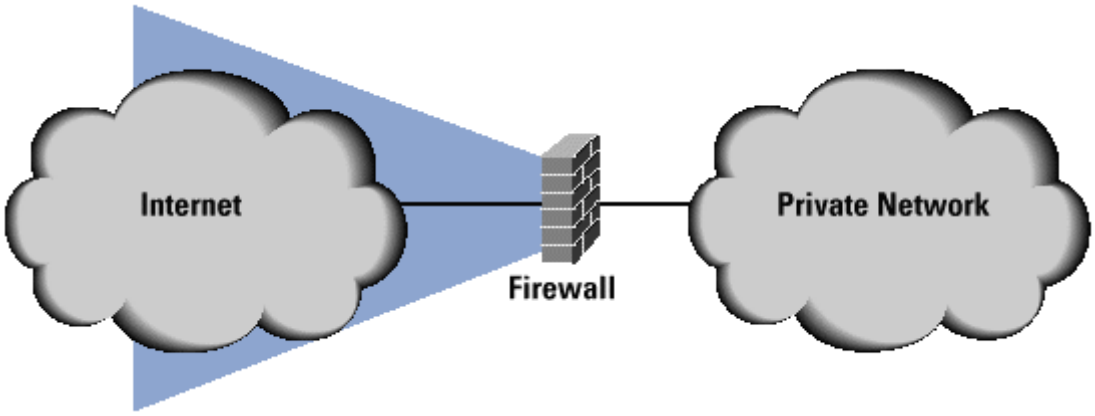
Sebuah firewall mencegat dan mengontrol trafik antar network dengan tingkat kepercayaan (*level of trust*) yang berbeda-beda. Ia adalah bagian dari pertahanan garis depan dari suatu organisasi dan harus menjalankan aturan sekuriti pada network bersangkutan. Dalam definisi Chesswick dan Bellovin, ia menyediakan sebuah jejak (*trail*) yang dapat ditelusuri. Firewall merupakan tempat yang cocok untuk mendukung autentifikasi pengguna yang kuat sebaik komunikasi privat antara dua firewall. Firewall juga merupakan tempat yang tepat untuk memfokuskan keputusan tentang

sekuriti dan untuk menjalankan aturan sekuriti. Ia dapat mencatat aktifitas internetwork dan membatasi wilayah cakupan (*exposure*) dari sebuah organisasi (Chapman & Zuichi, 1995).

Wilayah cakupan yang rentan serangan disebut sebagai "zona resiko". Apabila sebuah organisasi terkoneksi ke internet tanpa menggunakan firewall (gambar 2), maka setiap host dalam network privat dapat mengakses secara langsung setiap resource dalam internet. Dalam hal ini, setiap host di internet dapat menyerang setiap host di network privat. Mengurangi zona resiko adalah tindakan terbaik, dan sebuah firewall internetwork memungkinkan kita untuk membatasi zona resiko. Seperti yang kita lihat di gambar 3, zona resiko termasuk firewall itu sendiri, sehingga setiap host di internet dapat menyerang firewall. Dalam keadaan ini, setiap upaya serangan akan terpusat di satu titik, dan karenanya lebih mudah untuk dikontrol.



Gambar 2: Zona resiko dari network privat yang tidak terproteksi



Gambar 3: Zona resiko dengan firewall

Namun demikian, bukan berarti firewall bisa sepenuhnya diandalkan dalam urusan sekuriti. Firewall tidak dapat membaca pikiran manusia atau mendeteksi paket data dengan muatan yang tidak semestinya. Firewall juga tidak dapat melindungi network dari serangan yang berasal dari dalam (*insider attack*), walaupun ia masih bisa mencatat aktifitas network apabila si penyerang menggunakan gateway untuk melaksanakan aksinya. Firewall juga tidak bisa melindungi koneksi yang tidak melaluinya. Dengan kata lain, apabila seseorang terkoneksi ke internet melalui modem dan saluran telepon, maka tidak ada yang bisa dilakukan oleh firewall. Firewall juga hanya menyediakan sedikit proteksi untuk jenis serangan yang sebelumnya belum dikenal, dan bahkan proteksi yang sangat buruk terhadap serangan virus komputer.

Firewall di Masa Kini

Firewall pertama yang diaplikasikan di internet berupa autetifikasi pengguna yang kuat. Apabila aturan sekuriti mengijinkan akses ke network privat dari jaringan luar, seperti internet, maka dibutuhkan satu jenis mekanisme autentifikasi pengguna. Secara sederhana, autentifikasi dapat diartikan sebagai usaha "untuk meyakinkan keabsahan sebuah identitas". Username dan password merupakan salah satu jenis autentifikasi, tapi bukan autentifikasi yang kuat. Dalam koneksi non-privat, seperti halnya koneksi non-enkripsi yang melintasi jaringan internet, username dan password dapat dicegat untuk dibaca. Autentifikasi yang kuat menggunakan teknik kriptografi, misalnya dengan memanfaatkan sertifikasi maupun dengan menggunakan sebuah peralatan khusus semacam kalkulator (seperti KeyBCA). Mekanisme ini mencegah apa yang disebut sebagai "replay attack" - dimana, sebagai contoh, sebuah username dengan passwordnya dicegat untuk kemudian digunakan oleh yang pihak lain tidak berhak. Karena kedudukannya itu - berada di antara sisi "trust" dan "untrust" dari network - dan karena fungsinya sebagai gateway terkontrol, firewall menjadi tempat yang logis untuk menempatkan layanan semacam ini.

Firewall jenis lain yang bekerja di internet adalah enkripsi *firewall-to-firewall*. Sistem ini pertama kali diaplikasikan pada firewall ANS InterLock. Saat ini, koneksi semacam ini disebut sebagai *Virtual Private Network* (VPN). Ia adalah "privat" karena menggunakan kriptografi. Ia menjadi privat secara "virtual" karena komunikasi privat tersebut mengalir melalui jaringan publik seperti internet. Walaupun VPN telah ada pada masa dimana firewall belum dikenal, namun ia kini mulai sering dijalankan pada firewall. Dewasa ini, kebanyakan pengguna mengharapkan vendor firewall agar juga menyediakan opsi untuk VPN. Disini, firewall bertindak sebagai titik akhir (*end point*) untuk VPN diantara pengguna enterprise dan mobile (telekomuter) sehingga komunikasi yang konfidensial antara perangkat yang terhubung dapat terus terjaga.

Dalam beberapa tahun terakhir, firewall juga populer untuk digunakan sebagai perangkat *content screening*. Beberapa aplikasi firewall di lapangan ini mencakup *virus scanner*, URL *screening*, dan *scanner keyword* (juga dikenal di kalangan pemerintah AS sebagai "guards"). Apabila aturan sekuriti di sebuah organisasi mewajibkan screening terhadap virus komputer, adalah tindakan yang logis untuk melakukan screening terhadap lalu lintas file pada entry point yang terkontrol seperti halnya pada firewall. Faktanya, tersedia standar untuk memasang software antivirus pada aliran data (*data flow*) di firewall untuk mencegat dan menganalisis file data. Demikian pula halnya dengan URL screening – akses ke www yang terkontrol melalui firewall – dan content screening juga merupakan "bagian" yang cocok untuk dilimpahkan pada firewall.

Terlepas dari segala manfaatnya, masih ada juga keraguan di kalangan administrator jaringan untuk memanfaatkan firewall, khususnya menyangkut performa sistem jaringan. Ada anggapan bahwa penggunaan firewall berpotensi untuk menurunkan performa sistem secara signifikan. Sebagai solusinya, belakangan beberapa vendor router dan firewall telah mengembangkan suatu add-on firewall yang relatif baru yang disebut "flow control" untuk menghantarkan Quality of Service (QoS). QoS, sebagai contoh kasus, dapat membatasi besarnya bandwidth network yang dapat dipakai oleh seorang pengguna jaringan, atau membatasi besarnya kapasitas network yang dapat dipakai untuk layanan yang spesifik (seperti FTP atau web). Sekali lagi, karena firewall berfungsi sebagai gateway, maka ia menjadi tempat yang logis untuk menempatkan mekanisme pengaturan QoS.

Masa Depan Firewall

Di masa mendatang, firewall diprediksi akan menjadi pusat pengaturan pada network maupun internetwork. Selama ini, firewall dipandang sebagai komponen sekuriti berskala besar pertama yang pernah dikenal, produk keamanan internet pertama yang sukses secara komersial, dan piranti sekuriti yang paling banyak digunakan. Namun firewall sendiri masih belum sepenuhnya memadai untuk mengamankan sebuah jaringan. Firewall hanyalah salah satu mekanisme yang digunakan

untuk itu. Firewall dituntut untuk mampu berkomunikasi dan berinteraksi dengan piranti (*device*) lainnya. Firewall harus dapat berhubungan dengan sistem kontrol sekuriti jaringan, melaporkan kondisi-kondisi serta even yang sedang berlangsung, dan memungkinkan sistem kontrol merekonfigurasi sensor dan respon sistem secara keseluruhan. Sebuah firewall dapat berhubungan dengan piranti deteksi penyusupan (*intrusion*) pada jaringan untuk mengatur tingkat sensitifitasnya, misalnya dengan mengijinkan koneksi yang ber-autentifikasi dari luar jaringan dalam kondisi tertentu. Sebuah stasiun monitoring yang terpusat dapat memantau semua proses ini, membuat beberapa perubahan, bereaksi terhadap alarm dan peringatan-peringatan lainnya, serta meyakinkan bahwa seluruh software antivirus dan piranti content-screening berfungsi secara normal.

Dewasa ini, beberapa produk telah dibuat berdasarkan teknologi tersebut. Sistem deteksi penyusupan (*Intrusion Detection System*, IDS) dan sistem rekonfigurasi firewall secara otomatis berdasarkan kondisi tertentu kini telah tersedia. Namun teknologi firewall sendiri terus berevolusi ke bentuk yang lebih maju. Firewall kini memainkan peranan penting dalam strategi pengamanan yang bersifat multilayer dan multilevel.

Dengan maraknya penggunaan internet dan intranet, maka penggunaan firewall pada layanan tersebut juga makin berkembang. Ia bukan lagi menjadi satu-satunya mekanisme sekuriti, melainkan akan bekerjasama dengan sistem pengamanan lainnya. Ke depan, firewall kemungkinan akan berkembang dengan memanfaatkan teknologi yang lebih maju, namun ia akan tetap menjadi bagian tak terpisahkan dalam metode dan mekanisme pengamanan jaringan.