Bagaimana memilih Firewall yang Tepat

Jim Geovedi
negative@toxic.magnesium.net

Ada banyak sekali tulisan mengenai Firewall, baik berupa artikel, whitepaper, hasil riset, terlebih jika Anda mengetikkan keyword "Firewall" pada mesin pencari pilihan Anda.

Anda dapat mengatakan bahwa saya tidak sepenuhnya menulis artikel ini, karena apa yang saya tulis hanya rangkuman dari banyak konsep, teknologi, ide, yang secara beruntung dapat saya pelajari dari orang lain.

Apakah sudah perlu?

Mungkin Anda pernah membaca berita di portal berita detikinet.com pada bulan November tahun 2002, atau mungkin tahun sebelumnya di detik.com. Terdapat beberapa topik berita yang berkaitan dengan isu keamanan jaringan seperti "Mass Hacking", "Perang Cyber". Ada banyak pihak yang melihat bahwa terhubung dengan Internet adalah sangat tidak aman, rawan dari penyusupan crackers, pengintai. Cukup sulit untuk mendeskripsikan berapa besar risiko yang akan ditanggung, baik secara organisasi maupun individu, dengan terhubung ke jaringan Internet. Bagaimanapun juga, dengan tidak terhubung ke jaringan Internet akan menutup kesempatan-kesempatan untuk mengembangkan usaha, memperluas pasar, atau menanggapi persepsi dari pelanggan. Jika Anda saat ini tidak merasa menghadapi masalah-masalah tersebut, mungkin dalam kurun waktu tiga atau lima tahun kedepan, Anda akan mengalaminya, dapat diumpamakan ketika Internet sudah menjadi keharusan dalam sebuah usaha seperti penggunaan telepon, Fax, papan nama, periklanan dan lain sebagainya.

Hal penting yang harus diingat ketika berurusan dengan keamanan di Internet adalah adanya persamaan antar isu keamanan di Internet dengan

isu keamanan lainnya di dunia nyata. Memang benar, keamanan di Internet adalah hal baru, namun sangat perlu mendapat perhatian khusus demi berlangsungnya kegiatan ber-Internet sebagaimana yang diharapkan. Ingat, jika Anda terhubung dengan jaringan Internet, maka Anda adalah obyek yang sangat rentan untuk mendapatkan serangan, penyusupan, korban dari social-engineering, fraud, dan semua hal-hal buruk yang mungkin terjadi. Saya sangat menyayangkan ketika sebuah perusahaan yang telah menginvestasikan dana sedemikian besar untuk penyediaan infrastruktur, namun tidak dilindungi jaringannya dengan firewall.

Sebagai konsistensi dalam keamanan jaringan, Anda harus mempunyai pengetahuan dalam bidang manajemen dan pandangan arsitektural terhadap kegiatan bisnis yang Anda jalani, tanpanya, Anda mungkin hanya mempunyai sebuah sistem pengaman yang statis.

Mungkin hal yang paling merugikan pada sebuah bisnis yang tengah berlangsung adalah penghentian kegiatan untuk sementara waktu (downtime). Untuk beberapa kasus, downtime dapat berakibat fatal pada bisnis terutama pada bisnis yang memiliki aktifitas non-stop - rumah sakit, bank, bursa saham.

Sebelum melangkah lebih jauh, saya mengajak Anda untuk berpikir kembali mengenai:

1. Apa saja yang harus dilindungi?
2. Seberapa mungkin orang lain akan merusak/mencuri/memanipulasinya?
3. Apa efek yang ditimbulkan jika mereka berhasil?

Untuk menjadi catatan, kerusakan potensial yang sangat tinggi dapat saja terjadi jika tidak terhubung dengan jaringan Internet. Beberapa perusahaan yang merasa tidak nyaman jika terhubung dengan jaringan Internet, menempuh cara dengan mengijinkan karyawan, mitra kerja, atau pihak lain untuk melakukan akses "dial-in".

Seringkali, perusahaan-perusahaan yang sangat ketat melindungi dirinya dengan firewall atau "tanpa terhubung ke Internet sama sekali" mempun-

yai modem yang dapat dipergunakan untuk dial-out ketempat lain atau ke provider. Hal ini juga berpotensi untuk mengundang attack.

Menganalisa kebutuhan

Salah satu metode efektif untuk menentukan jenis Firewall yang dibutuhkan adalah dengan menganalisa kebutuhan-kebutuhan berorientasi pada services yang diberikan atau digunakan. Services yang umum digunakan adalah:

- World Wide Web (WWW) - termasuk diantaranya adalah File Transfer Protocol (FTP), Web-Proxy.
- Electronic Mail (e-mail)
- Remote Connection - Secure Shell (SSH), Telnet.

Berdasarkan services yang digunakan, sebaiknya Anda menentukan apakah Anda membutuhkan perlakuan khusus terutama dikaitkan dengan isu keamanan. Tentukan pula jika Anda membutuhkan jenis audit dan pencatatan terhadap segala aktifitas berdasarkan services tersebut. Sebagai contoh, jika Anda mempunyai sebuah kebijakan keamanan (security policy) yang tidak mengijinkan karyawan melakukan FTP keluar, maka Anda seharusnya juga mempunyai policy yang sama dengan melarang karyawan mengirimkan attachment keluar, atau mengirimkan surat berisi floppy disk menggunakan pos. Konsistensi terhadap keamanan adalah kuncinya.

Selain itu, perlu dipertimbangkan juga kelangsungan dari penggunaan Firewall ini dikemudian hari. Jika Anda menginstall Firewall saat ini, apakah masih dapat terus digunakan selama 4 atau 5 tahun kedepan? Artinya, Anda tentu tidak akan menggunakan hardware yang sama dalam jangka waktu tersebut - lifecycle dari peralatan jaringan umumnya sangat pendek - namun pastikan bahwa arsitektur dasar yang Anda tempatkan akan bisa bertahan dalam jangka yang panjang.

Mengenal jenis Firewall

Sebuah Firewall seharusnya menjadi sebuah pagar antara dua jaringan, diisi oleh suatu sistem yang hanyak mengijinkan beberapa dari sejumlah jenis koneksi untuk lewat. Aspek penting dari sebuah Firewall adalah bagaimana ia melindungi dirinya sendiri dari serangan: sebuah Firewall tidak boleh dengan mudah ditembus, karena jika mudah ditembus maka penyusup akan sangat mudah menguasai jaringan yang ada dibelakangnya.

Bentuk sederhana dan paling populer dari metode firewall adalah "router screening". Kebanyakan dari router komersial telah memiliki kemampuan untuk memilah traffic - mengijinkan hanya traffic yang perlu dan melakukan pemblokiran terhadap traffic yang dianggap tidak perlu. Screering router beroperasi hanya pada level jaringan, dan digunakan untuk menentukan boleh atau tidaknya content lewat berdasarkan header paket TCP/IP. Cukup cepat, fleksibel, dan cenderung murah, namun mereka mempunyai kekurangan untuk menyediakan informasi audit secara detail tentang traffic yang lewat.

Bentuk kedua dari Firewall adalah "dual-homed gateway" dimana sebuah sistem dengan dua Network Interfaces (NIC) yang diletakkan pada jaringan yang dilindungi dan jaringan yang di luar. Firewall akan berfungsi sebagai "proxy" yang mengatur request kepada jaringan yang ada diluar untuk diteruskan kepada pengguna. Proxy firewalls - juga disebut sebagai "application firewalls" - sangat atraktif karena proxy mampu memberikan informasi audit dari data yang diteruskan. Juga dirasakan oleh para ahli keamanan jaringan sebagai metode yang lebih aman karena proxy dapat dikustomisasi menjadi lebih spesifik untuk mengenali attack yang umum dari host yang ada dibelakangnya.

Beberapa waktu terakhir, sejumlah firewall yang menggunakan metode "dynamic packet filtering" muncul dipasaran. Sebuah dynamic packet filter firewall sama seperti sebuah penggabungan proxy firewall dan screening router. Bagi end-user, firewall jenis ini hanya beroperasi pada level jaringan, namun pada faktanya firewall ini mampu menjumlahkan traffic

yang lewat, seperti yang dimiliki oleh proxy firewall. Ketika seorang pengguna terhubung keluar, firewall jenis ini akan mencatat waktu dan mengijinkan data yang diminta untuk masuk kedalam, juga menjumlahkan durasi berapa lama koneksi berlangsung. Dynamic packet filtering adalah teknologi dinamis yang sangat menjanjikan diwaktu mendatang.packet filtering adalah teknologi dinamis yang sangat menjanjikan diwaktu mendatang.

Bikin atau Beli?

Secara tipikal Firewall membutuhkan waktu sekurang-kurangnya satu jam setiap minggunya untuk maintenance. Jika Firewall terhubung dengan jaringan Internet, maka dibutuhkan seseorang yang bertindak sebagai maintainer - sama halnya seperti postmaster, webmaster, dan FTP maintainer, dengan waktu kerja penuh.

Untuk berhemat, Anda dapat membangun Firewall sendiri dengan menggunakan aplikasi opensource yang tersedia banyak di Internet. Tersedia banyak panduan membangun Firewall sendiri di Internet ataupun toko buku. Sebagai contoh, penggunaan Operating System dan aplikasi Firewall yang umum digunakan: Linux dengan IPTables, FreeBSD dengan IPF atau IPFW, dan OpenBSD dengan PF.

Penting untuk menentukan apakah Anda akan membeli Firewall komersil atau membangun sendiri. Faktor penentunya adalah waktu dan uang. Jika Anda mempunyai waktu yang cukup serta karyawan yang mampu, membangun sendiri Firewall mungkin akan menghemat banyak pengeluaran. Namun jika Anda mempunyai budget cukup untuk pembelian dan pemeliharaan maka ada banyak pilihan produk Firewall komersial yang beredar dipasaran.

Sebelum membeli maka sebaiknya...

Memilih Firewall dapat diibaratkan memilih mobil. Diasumsikan sebagai mobil karena sebagian besar dari kita pernah melakukannya, sebelum membeli biasanya kita akan mengumpulkan informasi sebanyak mungkin dan mem-

inta pendapat beberapa orang terhadap suatu jenis mobil yang hendak kita pilih. Cara terbaik untuk memilih Firewall yang tepat untuk keperluan Anda adalah dengan mencari sebanyak mungkin informasi mengenai Firewall dan mengedukasikan diri Anda pada topik seputar Firewall.

Berikut adalah point yang sebaiknya Anda pertimbangkan sebelum Anda membeli.

- Keamanan
  Pikirkan kembali apa keinginan Anda, dan perkirakan bagaimana Firewall akan membantu kelangsungan bisnis Anda. Cobalah cari masukan dari orang lain yang lebih mengerti mengenai Firewall, dan tanyakan pendapat mereka. Cari referensi sebanyak mungkin.

- Vendor
  Cari tahu berapa lama mereka menjual produk Firewall yang mereka tawarkan, tanyakan referensi yang bisa Anda dapatkan. Mintalah selalu detail produk yang ditawarkan.

- Dukungan teknis
  Perkirakan berapa banyak karyawan yang akan ditugaskan untuk mengurus Firewall, juga hitung berapa operational-cost yang diperlukan. Bagaimana kebijakan diperusahaan Anda mengenai upgrade dan downtime pada services. Juga pertimbangkan berapa lama perusahaan akan mengupgradenya dengan yang baru.

- Dokumentasi
  Mintalah salinan dokumentasi sebagai pegangan. Hal yang sama berlaku pada laporan audit dari firewall.

- Operasional
  Periksa apakah Firewall tersebut berikut hardware atau hanya sebuah software yang siap install. Juga periksa kebutuhan-kebutuhan Firewall tersebut, seperti network interface cards, cabling, dan lain-lain. Cari

tahu apakah Firewall tersebut manageable, dan seberapa amankah jika Anda melakukan remote management.

Kebanyakan Firewall dijual sebagai bagian dari paket jasa konsultasi. Ketika sebuah Firewall dijual, biasanya installasi dan dukungan teknis diberikan – tergantung bagaimana negosiasi dan harga yang disetujui.

Sepintas Anda mungkin tidak merasakan perbedaan antara menggunakan Firewall atau tidak. Benar, karena Firewall seharusnya berada pada stealth-mode, Anda seharusnya tidak merasakan adanya perubahan signifikan dari Firewall. Firewall bekerja dengan menghalau paket yang tidak diinginkan dan mem-bypass paket yang diijinkan. Alangkah baiknya jika secara berkala Anda melakukan pemeriksaan rutin terhadap log yang dihasilkan oleh Firewall. Percaya atau tidak, Anda akan dikejutkan dengan berapa banyak percobaan intrusion atau worms yang melindungi jaringan Anda.