OPTIMALISASI FIREWALL PADA JARINGAN KOMPUTER BERSKALA LUAS

Nanan Abidin

ABSTRAK

Suatu konfigurasi firewall yang baik dan optimal dapat mengurangi ancaman-ancaman tersebut. Konfigurasi firewall terdapat 3 jenis diantaranya adalah screened host firewall system (single-homed bastion), screened host firewall system (Dual-homed bastion), dan screened subnet firewall. Dan juga mengkonfigurasikan firewall dengan membuka port-port yang tepat untuk melakukan hubungan koneksi ke internet, karena dengan mengkonfigurasi port-port tersebut suatu firewall dapat menyaring paket-paket data yang masuk yang sesuai dengan policy atau kebijakannya. Arsitektur firewall ini yang akan digunakan untuk mengoptimalkan suatu firewall pada jaringan.

Jaringan komputer bukanlah sesuatu yang baru saat ini. Hampir di setiap perusahaan terdapat jaringan komputer untuk memperlancar arus informasi di dalam perusahaan tersebut. Internet yang mulai populer saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan komputer yang terhubung dan dapat saling berinteraksi. Hal ini dapat terjadi karena adanya perkembangan teknologi jaringan yang sangat pesat. Tetapi dalam beberapa hal terhubung dengan internet bisa menjadi suatu ancaman yang berbahaya, banyak serangan yang dapat terjadi baik dari dalam maupun luar seperti virus, trojan, maupun hacker. Pada akhirnya security komputer dan jaringan komputer akan memegang peranan yang penting dalam kasus ini.

Pendahuluan

Internet seringkali disebut sebagai dunia tanpa batas. Beragam informasi bisa didapat di internet dan siapapun bisa mengakses informasi tersebut. Seiring perkembangan teknologi informasi, internet tak hanya memberikan kontribusi positif bagi kehidupan tetapi juga ancaman. Ancaman lebih menakutkan justru datang dari dunia maya, mulai dari serangan virus, trojan, phishing hingga cracker yang bias mengobok-obok keamanan sistem komputer.

Terhubung ke internet ibaratnya membuka pintu komputer untuk bisa diakses oleh siapapun. Melalui pintu tersebutlah, anda dengan sangat mudah bisa menjelajahi belantara dunia maya entah itu untuk berbelanja online, membaca berita terkini, mengirim e-mail dan lain sebagainya. Namun melalui pintu itu pulalah, hacker bisa masuk dan dengan mudah mengobok-obok bahkan mengambil alih kendali system komputer. Pada banyak kesempatan, kita perlu menentukan pilihan mana yang harus dipercaya dan mana yang tidak.

Sekalipun sesuatu itu berasal dari sumber yang terpercaya dan aman untuk dijalankan. Bisa saja Anda menerima e-mail dari sumber terpercaya yang di dalamnya disertakan sebuah link dan mengkliknya. Namun siapa sangka jika ternyata melalui link tersebut, hacker menyelipkan program jahat untuk memata-matai komputer tanpa sepengetahuan Anda. Untuk itulah, komputer membutuhkan suatu benteng yang mampu melindungi komputer dari ancaman berbahaya di internet. Di dunia maya, benteng ini disebut dengan **firewall**.

Keamanan komputer maupun jaringan komputer, terutama yang terhubung ke internet harus direncanakan dan dikoordinasikan dengan baik agar dapat melindungi sumber daya (resource) dan investasi di dalamnya. Informasi (data) dan service (pelayanan) sudah menjadi sebuah komoditi yang sangat penting. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi suatu

organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi).

Jaringan Komputer

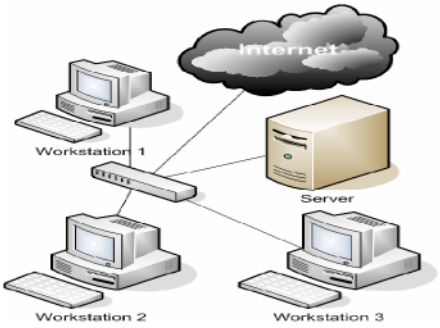
Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung. Informasi dan data bergerak melalui kabel-kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama sama menggunakan hardware/software yang terhubung dengan jaringan. Tiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node.

Sebuah jaringan biasanya terdiri dari 2 atau lebih komputer yang saling berhubungan diantara satu dengan yang lain, dan saling berbagi sumber daya misalnya CDROM, Printer, pertukaran file, atau memungkinkan untuk saling berkomunikasi secara elektronik.

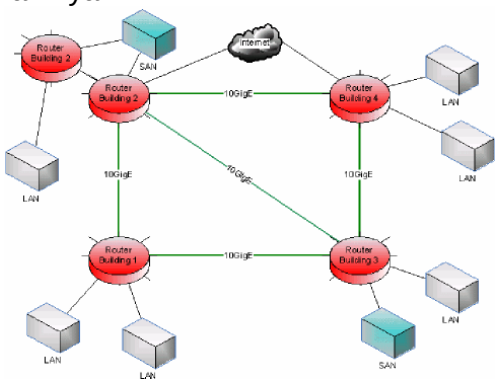
Jenis- Jenis Jaringan

Ada 3 macam jenis jaringan, yaitu :

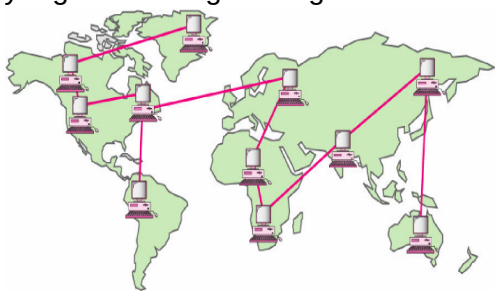
1. Local Area Network (LAN)
   LAN adalah jaringan yang dibatasi oleh area yang relative kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya tidak jauh dari sekitar 1 km persegi.



2. Metropolitan Area Network (MAN)
   MAN biasanya meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu propinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu jaringan Bank dimana beberapa kantor cabang sebuah Bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya.



3. Wide Area Network (WAN)
   Wide Area Networks (WAN) adalah jaringan yang lingkupnya biasanya sudah menggunakan sarana Satelit ataupun kabel bawah laut sebagai contoh keseluruhan jaringan BANK BNI yang ada di Indonesia ataupun yang ada di Negara-negara lain.



Firewall

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).

Dalam dunia nyata, firewall adalah dinding yang bisa memisahkan ruangan, sehingga kebakaran pada suatu ruangan tidak menjalar ke ruangan lainnya. Tapi sebenarnya firewall di Internet lebih seperti pertahanan disekeliling benteng, yakni mempertahankan terhadap serangan dari luar. Gunanya:

- membatasi gerak orang yang masuk ke dalam jaringan internal
- membatasi gerak orang yang keluar dari jaringan internal
- mencegah penyerang mendekati pertahanan yang berlapis

Jadi yang keluar masuk firewall harus *acceptable*. Firewall merupakan kombinasi dari router, server, dan software pelengkap yang tepat.

Firewall merupakan suatu cara/ sistem/mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN) anda.

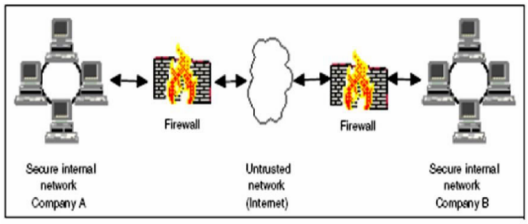


Figure 266. A firewall illustration

Firewall didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dan internet, atau antara kumpulan-kumpulan jaringan lainnya (*Building Internet Firewalls*, oleh Chapman dan Zwicky). *A firewall is a system or group of systems that enforces an access control policy between two networks* (http://www.clark.net/pub/mjr/pubs/fwfaq). *The main purpose of a firewall system is to control access to or from a protected network. It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.* (http://csrc.ncsl.nist.gov/nistpubs/800-10/node3 1 .html).

Tugas – Tugas Firewall

Firewall secara umum di peruntukkan untuk melayani :

- Mesin/Komputer
  Setiap mesin komputer yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.

- Jaringan
  Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang di miliki oleh perusahaan, organisasi dsb.

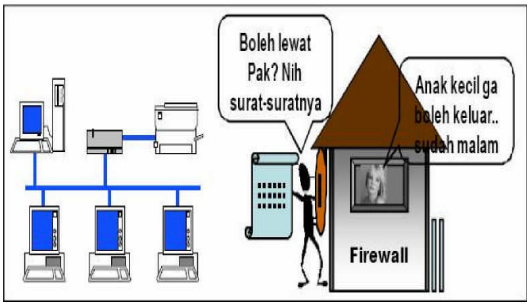
- Firewall mempunyai beberapa tugas: Pertama dan yang terpenting adalah: harus dapat mengimplementasikan kebijakan security di jaringan (*site*

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 trafik 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.

- Ada beberapa hal yang tidak dapat dilakukan oleh firewall :
  - Firewall tidak bisa melindungi dari serangan orang dalam
  - Firewall tidak bisa melindungi serangan yang tidak melalui firewall tersebut (tidak melalui chocke point). Misalnya ada yang memasang dial-up service, sehingga jaringan bisa diakses lewat modem.
  - Firewall tidak bisa melindungi jaringan internal terhadap serangan-serangan model baru.
  - Firewall tidak bisa melindungi jaringan terhadap virus.



Karakteristik Firewall

1. Seluruh hubungan/kegiatan dari dalam ke luar, harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan.

2. Hanya Kegiatan yang terdaftar/ dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur policy pada konfigurasi keamanan lokal. Banyak sekali jenis firewall yang dapat dipilih sekaligus berbagai jenis policy yang ditawarkan.

3. Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. Hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan operating system yang relatif aman.

Teknik Yang Digunakan Firewall

1. Service Control (kendali terhadap layanan). Berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk kedalam ataupun keluar firewall. Biasanya firewall akan mencek no IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxy yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya. Bahkan bisa jadi software pada server itu sendiri, seperti layanan untuk web maupun untuk mail.

2. Direction Conrol (kendali terhadap arah). Berdasarkan arah dari berbagai permintaan (*request*) terhadap layanan yang akan dikenali dan diijinkan lewat firewall.

3. User control (kendali terhadap pengguna). Berdasarkan pengguna/ user untuk dapat menjalankan suatu

layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis,hal ini di karenakan user tersebut tidak di ijinkan untuk melewati firewall. Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

4. Behavior Control (kendali terhadap perlakuan). Berdasarkan seberapa banyak layanan itu telah digunakan. Misal, firewall dapat memfilter email untuk menanggulangi/mencegah spam.

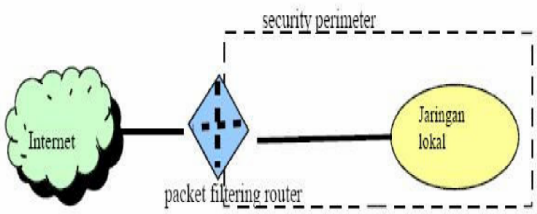
Tipe – Tipe Firewall

1. Packet Filtering Router

Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut. Pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan atau di tolak. Penyaringan packet ini di konfigurasikan untuk menyaring paket yang akan di transfer secara dua arah (baik dari dan ke jaringan lokal). Aturan penyaringan didasarkan pada header IP dan transport header, termasuk juga alamat awal (IP) dan alamat tujuan (IP), protocol transport yang di gunakan (UDP, TCP), serta nomor port yang digunakan. Kelebihan dari tipe ini adalah mudah untuk di implementasikan, transparan untuk pemakai, relatif lebih cepat.

Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal authentikasi. Adapun serangan yang dapat terjadi pada firewall dengan tipe ini adalah:

- IP address spoofing : *Intruder* (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan ip address jaringan lokal yang telah diijinkan untuk melalui firewall.
- Source routing attacks : Tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk membypass firewall.
- Tiny Fragment attacks : *Intruder* membagi IP kedalam bagian-bagian (*fragment*) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header. Penyerang berharap hanya bagian (*fragment*) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua packet dengan protocol TCP dan memiliki offset = 1 pada IP fragment (bagian IP)



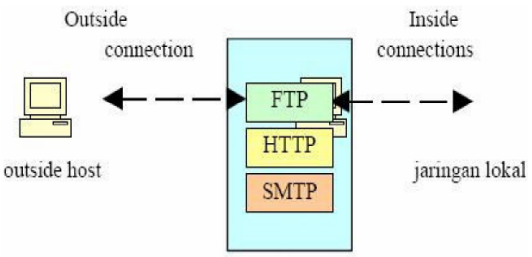
2. Application-Level Gateway

Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu FTP, HTTP, GOPHER dll.

Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal FTP untuk mengakses secara remote, maka gateway akan meminta user memasukkan alamat remote host yang akan di akses.Saat pengguna mengirimkan user ID serta informasi lainnya yang sesuai maka gateway akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada remote host, dan menyalurkan data diantara kedua titik. Apabila data tersebut tidak sesuai maka firewall tidak akan meneruskan

data tersebut atau menolaknya. Lebih jauh lagi, pada tipe ini firewall dapat di konfigurasikan untuk hanya mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati firewall.

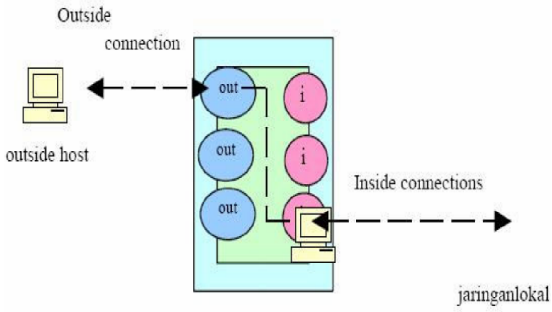
Kelebihannya adalah relatif lebih aman daripada tipe *packet filtering router* lebih mudah untuk memeriksa dan mendata semua aliran data yang masuk pada level aplikasi. Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan. Yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.



3. Circuit-level Gateway

Tipe ketiga ini dapat merupakan sistem yang berdiri sendiri, atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe application-level gateway.tipe ini tidak mengijinkan koneksi TCP end to end (langsung)

Cara kerjanya : Gateway akan mengatur kedua hubungan TCP tersebut, 1 antara dirinya dengan TCP pada pengguna lokal (*inner host*) serta 1 lagi antara dirinya dengan TCP pengguna luar (*outside host*). Saat dua buah hubungan terlaksana, gateway akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang di ijinkan. Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (*internal users*).



Merencanakan Jaringan Dengan Fireawll

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 :

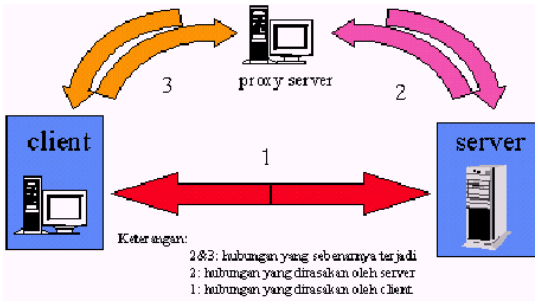
Pertama, bila kita bayangkan jaringan kita berada dalam perlindungan sebuah benteng, komunikasi dapat terjadi melalui pintu-pintu keluar benteng tersebut. Cara ini dikenal sebagai *packet-filtering*, dimana filter hanya digunakan untuk menolak trafik pada kanal yang tidak digunakan atau kanal dengan resiko-security cukup besar, sedangkan trafik pada kanal yang lain masih tetap diperbolehkan. 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 protocol 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	sembarang	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.

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 Transfert 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). 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 merelay 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.

Pembahasan

Untuk melakukan optimalisasi suatu firewall ada beberapa hal yang perlu diperhatikan. Diantaranya :

- Yang pertama kita perlu menentukan *Policy* atau kebijakan firewall tersebut. Kerena penentuan *policy* atau kebijakan merupak hal yang sangat penting, baik atau buruknya sebuah firewall sangat ditentukan oleh *policy* atau kebijakan yang diterapkan. Penentuan kebijakan tersebut meliputi :
  - Menentukan apa saja yang perlu dilayani. Artinya apa saja yang akan dikenai kebijakan yang akan kita buat.
  - Menentukan individu atau kelompok-kelompok yang akan dikenai policy atau kebijakan tersebut.
  - Menentukan layanan-layanan yang dibuthkan oleh tiap-tiap individu atau kelompok yang menggunakan jaringan.
  - Berdasarkan setiap layanan yang digunakan oleh individu atau kelompok tersebut akan ditentukan bagaimanan konfigurasi terbaik yang akan membuatnya semakin nyaman.
  - Menerapkan semua policy atau kebijakan tersebut.

- Berikutnya dapat menganalisis daftar port-port yang digunakan oleh berbagai protocol dan membuka port-port tersebut kedalam firewall dan port-port terebut harus tepat. Server web biasanya diidentifikasikan melalui port 80, FTP (*File Transfer Protocol*) melalui port 21, SSH melaui port 22. Port ini menunjukan port mana yang harus dibuka di sisi server web. Pada PC port-port yang perlu dibuka adalah untuk membuat koneksi keluar, settingan untuk itu biasanya telah dilakukan oleh firewall secara otomatis ketika ketika kita menjalankan sebuah program yang memerlukan koneksi ke internet. Ketika kita telah mengetahui port-port mana saja yang dibutuhkan oleh program buka port-port tersebut kedalam firewall. Sering menemukan dan memanfaatkan titik-titik kelemahan yang ada. Jika kita sedang menggunakan notebook yang terhubung ke hotspot umum tutup port-port yang terbuka. Firewall modern akan secara otomatis mengenali jaringan dan mengkonfigurasi diri sendiri seseuai dengan situasi. Kebanyakan firewall masa kini menawarkan fungsi setting otomatis untuk file dan printer-sharing. Pada firewall lain seperti XP-firewall harus setiap kali dikonfugurasi secara manual. Untuk mengaktifkan file dan printer-sharing, buka port TCP 139 dan 445 serta port UDP 137 dan 138 untuk data masuk. Selain itu kita perlu mengijinkan permintaan echo ICMP. Apabila kita terkoneksi ke internet melalui sebuah router ada baiknya jika mengkonfigurasi router tersebut. Settingan router yang perlu dirubah adalah fungsi *Port Forwarding* yang harus diaktifkan, karena

pada kebanyakan router suatu fungsi *Port Forwarding* biasanya telah dimatikan secara default. Dengan konfigurasi yang tepat, router akan menolak paket IP dengan pengirim palsu.

- Pengoptimalisasian firewall yang berikutnya adalah menentukan konfigurasi suatu firewall dengan tepat. Ada beberapa konfigurasi firewall :

Dual-homed host

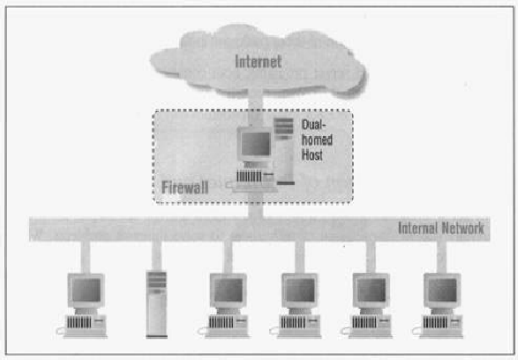


Figure 4–3: Dual-homed host architecture

Dual homed host bisa menjadi router, namun untuk menjadi firewall lalu lalu-lintas IP dalam arsitektur ini benar-benar di-blok. Jadi kalau ada paket yang mau keluar masuk, harus lewat proxy.

•Screened Host

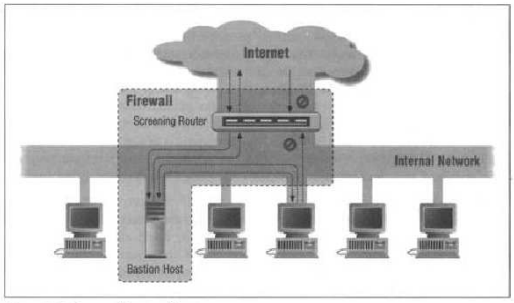


Figure 4–4: Screened host architecture

Menggunakan bastion host yang diletakkan dalam intranet, dan seluruh komunikasi keluar masuk harus melalui proxy pada bastion dan kemudian melalui screening router. Bastion host merupakan sistem/ bagian yang dianggap tempat terkuat dalam sistem keamanan jaringan oleh administrator.atau dapat di sebut bagian terdepan yang dianggap paling kuat dalam menahan serangan, sehingga menjadi bagian terpenting dalam pengamanan jaringan, biasanya merupakan komponen firewall atau bagian terluar sistem publik. Sekilas terlihat bahwa dual-homed architecture lebih aman, tetapi dalam prakteknya banyak kegagalan sistem yang memungkinkan paket lewat dari satu sisi ke sisi lainnya dalam dual homed architecture. Jadi alasan utama menggunakan screened host architecture adalah karena router lebih mudah diamankan ketimbang sebuah komputer/host. Kejelekan utama kedua-duanya adalah mereka memiliki '*single point of failure*'.

Screened Subnet

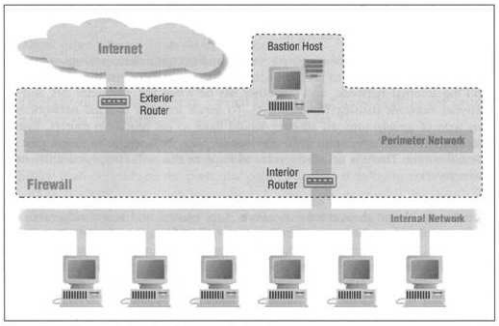


Figure 4–5: Screened subnet architecture (using two routers)

Alasan mengapa Bastion host sering menjadi target serangan. Karena idenya adalah kalau bastion host berhasil dibobol, jangan sampai penyerang masuk ke dalam jaringan internal. Oleh karena itu bastion host diletakkan di perimeter network. Untuk membobol jaringan, hacker harus menyerang exterior router dan interior router. Ada juga yang memiliki perimeter berlapis, dimana syaratnya agar efektif adalah sistem pertahan tiap lapis harus berbeda-beda.

Perimeter network yaitu kalau ada orang yang berhasil menembus ke exterior router dan bastion, maka sang penyerang hanya bisa melihat paket yang berkeliaran di perimeter network saja. Jadi lalu-lintas komunikasi pada jaringan internal (yang relatif sensitif) tidak dapat dilihat oleh penyerang dari

perimeter network.

Bastion host Bertindak sebagai titik masuk koneksi dari luar, termasuk SMTP, FTP dan DNS. Sedangkan untuk melakukan koneksi dari client ke server di Internet dapat dilakukan dengan 2 cara:

- Mengizinkan router-router agar klien bisa berhubungan dengan server Internet secara langsung.
- Menggunakan proxy server pada bastion penting-penting saja. Misalnya hubungan SMTP antara bastion dengan mail server internal. Perhatikan komputer server internal apa saja yang terhubung dengan bastion, karena itulah yang akan menjadi target serangan jika bastion berhasil dihancurkan oleh hacker.

Exterior router pada prakteknya mengizinkan banyak paket keluar, dan hanya sedikit memfilter paket masuk. Namun, biasanya untuk screening network internal, settingnya sama antara internal dan external router. Tugas utama external router adalah untuk memblok paket yang memiliki alamat yang palsu dari luar (karena berusaha menyamar dengan alamat IP salah satu host dalam internal network). Karena pasti dari Internet. Kenapa tidak di internal router? Karena masih bisa dari perimeter net yang sedikit lebih trusted.

Kesimpulan

Suatu keamanan merupakan suatu hal yang sangat penting dalam dunia internet baik keamanan komputer maupun keamanan jaringan yang banyak dipenuhi dengan berbagai ancaman baik dari dalam maupun dari luar, dan firewall merupakan solusi untuk dapat mengatasi keamanan tersebut. Dengan suatu konfigurasi yang tepat pada firewall maka kemungkinan untuk mengamankan suatu data atau komputer pada jaringan menjadi jauh lebih aman.

Konfigrasi suatu firewall yang pertama adalah penentuan *policy* atau kebijakan firewall tersebut tentang apa saja yang akan dikenai kebijakan tersebut, siapa saja yang akan dikenai kebijakan tersebut dan layanan-layanan yang dibutuhkan tiap individu tersebut. Kemudian menentukan port-port yang digunakan oleh berbagai protokol dan membuka port-port tersebut kedalam firewall, dan juga membuka port yang digunakan untuk file sharing dan request ping. Selanjutnya adalah menentukan suatu konfigurasi yang tepat dan sesuai dengan keadaan jaringannya. Screened subnet merupakan konfigurasi yang paling tinggi tingkat keamanannya, karena pada konfigurasi ini digunakan 2 buah paket filtering router, sehingga jaringan local menjadi tidak terlihat (*invisible*) dan tidak dapat mengkonstruksi routing langsung ke internet atau dengan kata lain internet menjadi *invisible* karena router luar yang akan melayani hubungan antara internet dan bastion host, namum bukan berarti jaringan local tidak dapat melakukan koneksi ke internet.

Dengan konfigurasi tersebut memungkinkan firewall kita dapat meningkatkan keamanan yang jauh lebih baik dari ancaman-ancaman internet. Namun tidak menutup kemungkinan bahwa jaringan kita tetap dapat diserang oleh hacker yang serangannya sangat terarah. Namun lebih baik sedikit terlindungi daripada tidak sama sekali.

Referensi

1. Tanembaum, Andrew S. 1996. *Jaringan Komputer Edisi Bahasa Indonesia Jilid 1.* Prenhallindo : Jakarta.
2. Majalah CHIP edisi Mei 2007. *Firewall Yang Sempurna.*
3. http://www.erlangga.co.id/blog/viewtopic.php?t=188&sid=f9320f1898d08eba99484 54883 072f 1b
4. http://students.ukdw.ac.id/~22022807/kommasd.html
5. http://library.adisanggoro.or.id/Security/TransparanDigisec-5firewall.htm
6. http://www.klik-kanan.com/fokus/firewall.shtml
7. http://www.ictwatch.com/internetsehat/download/internetsehat-

modulemanual/modul personalfirewall.pdf
8. http://www.ictwatch.com/internetsehat/download/internetsehat-modulemanual/modul personalfirewall.pdf
9. http://ilmukomputer.com