TUGAS JURNAL WAN

TUGAS JURNAL

JARINGAN KOMPUTER

OPTIMALISASI FIREWALL PADA JARINGAN SKALA LUAS

ABSTRAK

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.

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 portport 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.

BAB I

Pendahuluan

1.1. Latar Belakang

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).

1.2. Tujuan

Berdasarkan dari latar belakang diatas tujuan dari penelitian ini adalah agar dapat mengoptimalisasikan firewall pada jaringan sehingga dapat mengurangi ancamanancaman yang terdapat di dalam dunia internet dan kita menjadi merasa lebih nyaman menjelajahi dunia internet.

1.3. Metode Penelitian

Metode penelitian yang digunakan dalam pembuatan tulisan jurnal ini adalah dengan menggunakan Literatur. Dengan metode tersebut penulis mengumpulkan berbagai informasi yang berhubungan dengan pokok pembahasan pada tulisan jurnal ini.

BAB II

Landasan Teori

2.1. 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.

2.1.1. 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.

Sumber : http://www.itgeorgia.com/images/WebNetwork4.gif

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.

Sumber : http://ops.fhwa.dot.gov/publications/telecomm_handbook/images/

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.

Sumber : Materi Kuliah Bina Nusantara

2.2. 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.

Sumber : Artikel Internet (Firewall)

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/node31.html).

2.2.1 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.

Sumber : Artikel Internet (Modul Personal Firewall)

2.2.2. 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.

2.2.3. 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.

2.2.4. 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)

Sumber : Artikel Internet (Ammar-Firewall)

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.

Sumber : Artikel Internet (Ammar-Firewall)

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 saatu 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).

Sumber : Artikel Internet (Ammar-Firewall)