Pengamanan Sistem Jaringan Komputer dengan Teknologi *Firewall*

Karpen
Teknik Informatika STMIK-AMIK Riau
karpen@stmik-amik-riau.ac.id

Abstrak

Informasi merupakan suatu hal yang sangat penting dalam sebuah sistem komputer, untuk itu harus dijaga dan lindungi dari segala ancaman yang dapat menyebabkan informasi (data) tersebut hilang. Salah satu cara yang dapat digunakan sebagai keamanan data, khususnya dalam sebuah sistem jaringan komputer, baik dari luar (terkoneksi dengan jaringan internet) maupun dari dalam (terkoneksi dengan sistem jaringan intranet) adalah dengan menggunakan teknologi firewall. Konfigurasi dan security policy dari suatu teknologi firewall merupakan kunci utama untuk mendapatkan keamanan data (informasi) yang maksimum.

Kata kunci : Firewall, Packet filter, Internet, Jaringan komputer

1. Pendahuluan

Saat ini era komputeriasi sudah menyebar dengan luas, yang meliputi hampir semua layanan komunikasi yang ada seperti media *internet*, yang menyebabkan semua orang menggunakan media ini sebagai bahan untuk mencari informasi, dan ada pula yang menggunakannya sebagai bahan untuk mencari inforamsi dengan tujuan-tujuan tertentu. Perkembangan dan kemajuan teknologi, khususnya teknologi komputer yang ada memang banyak keuntungan dalam membantu kehidupan manusia. Tetapi dengan kemajuan teknologi juga akan membawa dampak negative yang banyak terjadi, seperti adanya kejahatan komputer, baik yang berasal dari dalam maupun yang berasal dari luar sistem jaringan komputer. Kejahatan komputer akan menyebabkan kerugian dari para pengelola sistem jaringan komputer, yang khususnya berhubungan dengan sejumlah data-data yang merupakan informasi yang sangat penting, yang hanya diperbolehkan untuk diketahui oleh orang-orang tertentu di dalam perusahaan tersebut. Untuk itu keamanan data yang merupakan informasi berharga menjadi prioritas utama untuk diperhatikan dan harus terjamin dari segala kemungkinan kerusakan ataupun penyelahgunaan dari pihak-pihak yang tidak bertanggung jawab, sehingga menyebabkan sistem informasi menjadi rusak dan tidak bisa digunakan lagi sebagaimana yang diinginkan.

Keamanan sistem komputer sangat penting untuk diperhatikan sehubungan dengan sejumlah informasi yang ada, salah satu yang dapat digunakan sebagai pengamanan sistem informasi untuk sejumlah data-data penting adalah dengan menggunakan teknologi *firewall*. Sebagian orang mungkin sudah akrab dengan istilah *firewall* dan mungkin sebagain masih menggap sesuatu hal yang baru dalam sistem jaringan komputer. Kemanan komputer tidak hanya mengandalkan *firewall* yang paling canggih, karena untukitu harus memiliki pengetahuan yanglebih luas tentang teknologi firewall itu sendiri. *Firewall* pada dasarnya merupakan suatu alat yang bersifat melindungi, jika seseorang berhubungan dengan sistem jaringan komputer dan ingin akses yang dilakukannya berjalan dengan aman, *firewall* merupakan salah satu pelindung yang tepat. Pada dasarnya untuk melakukan akses dengan sistem jaringan ada tiga hal yang dilindungi diantaranya yang pertama adalah data, sumber daya dan reputasi.

2. Studi Pustaka

Lukas Tanutama [1] mengatakan bahwa data merupakan hal yang sangat perlu untuk dilindungi, meskipun pada dasarnya sebuah data pada level aplikasi bisa dilakukan pengamanan dengan menggunakan *algoritms kriptografi*, tapi akan lebih baik jika menggunakan *firewall* untuk sistem komputer yang terkoneksi dengan jaringan komputer yang akan befungsi sebagai *Packet filter* pada lalu lintas jaringan. Kejahatan komputer berbeda yang diraskan oleh setiap individu maupun

organisasi, hal disebabkan pendeteksian yang sulit dilakukan dan diketahui yang menyebabkan data dalam harddisk sudah hilang atau bahkan dikirim ketempat lain. Tetapi bisa jadi suatu organisasi yang terkoneksi dengan sistem jaringan komputer, tidak mengetahui bahwa sistem jaringannya sudah dibobol atau disusupi oleh orang lain walaupun mungkin hanya sekedar iseng , tetapi suatu saat bisa saja data-data yang sangat penting akan dikopy ke harddisk lain tanpa disadari.

Penganggu atau penyusup sering memanfaatkan sumber daya komputer yang diberikan secara umum dan dalam melakukan kegiatannya tidak memandang sistem yang dimiliki oleh siapa saja. Kejahatan sistem komputer sering dilandasi dengan adanya ruang kosong pada media storage seperti *harddisk,memory* dan sumber daya lainnya. Tipe dan jenis serangan pada jaringan komputer beragam, seperti *intrusion, denial of servive* dan *informasi theft*. Para *Hacker* akan menggunakan identitas orang lain untuk melakukan kejahatan pada jaringan komputer, hal ini dilatarbelakangi oleh reputasi seseorang yang mengakibatkan rusak. Kejadian seperti ini bisa disebabkan seorang *hacker* tidak menyukai orang tersebut dan menggunakan identitasnya untuk melakukan kejahatan komputer seperti penggunaan *credit card*, pembelian *e-commerce* dan lain sebagainya. Adanya beberapa model kejahatan komputer yang ditimbulkan oleh orang-orang yang tidak memiliki tanggung jawab yang khusus ditujukan pada sistem jaringan komputer yang sering terhubung dengan media *internet* serta banyaknya jenis gangguan atau kejahatan yang terjadi, maka dengan teknologi *firewall* diharapkan dapat mengatasinya, lalu bagaimana teknologi *firewall* dapat melindungi sejumlah informasi dari kejahan jaringan komputer?

Menurut Dony Ariyus [2] *technology firewall* adalah alat yang digunakan untuk mencegah orang luar untuk memperoleh akses ke suatu jaringan internet. *Firewall* pada umumnya merupakan kombinasi dari perangkat lunak (*software*) dan perangkat keras (*hardware*), dan biasanya *firewall* menerapkan pengeluaran rencana atau perintah untuk melakukan sortir address yang tidak dikehendai dan diinginkan. Konfigurasi dari *firewall* akan bergantung kepada kebijakan dariorganisasi atau perusahaan yang akan menerapkan sistem jaringan komputernya. Pada dasarnya kebijakan ini dapat dibagi ke dalam dua bagian yaitu :

1) Apa saja yang tidak diperbolehkan secara eksplisit dianggap tidak diperbolehkan (*prohibited*).
2) Apa saja yang tidak dilarang secara eksplisit dianggap diperbolehkan (*permitted*).

Dede Sopandi [3] mengatakan jaringan komputer adalah gabungan antara teknologi komputer dengan teknologi komunikasi. Gabungan dari kedua teknologi ini akan menghasilkan pengolahan data yang dapat didistribusikan, mencakup pemakaian *database, software aplikasi* dan peralatan *hardware*, otomatisasi perkantoran serta peningkatan efisiensi kerja. Dilihat dari luar area jaringan maka jaringan komputer secara geografis dapat dibedakan menjadi dua yaitu :

1) Jaringan komputer WAN (*Wide Area Network*).
2) LAN (*Lokal Area Network*). Melalui jaringan komputer inilah kantor, gedung, kota bahkan suatu negara dapat disatukan. Sebuah jaringan komputer terbentuk atas *software network* dan *hardware network*. *Software* jaringan yang mendukung untuk sebuah jaringan komputer melliputi :
   1) *PC Operting System*.
   2) *Network Operating System.*
   3) *Protokol*.
   4) Program aplikasi.
   5) *Internet Sharing*.

Sedangkan *hardware* jaringan yang dibutuhkan untuk membentuk sebuah jaringan komputer, meliputi :

1). *Server*.
2). *Workstation*.
3). *Network Interface Card-NIC.*
4). Kabel dan Konektor.
5). Peralatan pendukung, seperti *Hub, Repeater, Bridge dan Router*.

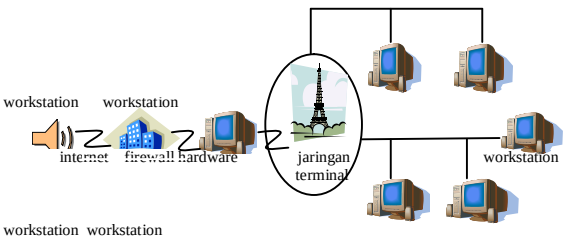
3. Pembahasan Teknologi *Firewall*

Teknologi *firewall* bekerja dengan melakukan pengamatan packet IP (*internet protocol*) yang akan melaluinya. Berdasarkan konfigurasi yang sudah dibentuk dari *firewall* maka semua akses dapat diatur berdasarkan *IP address, port* dan arah informasi. Selanjutnya untuk mengamati teknologi firewall bisa bekerja, dilakukan pemeriksaan prosedur penggunaan IP address, baik itu address statis maupun address dinamis. IP address statis dan dinamis digunakan pada sistem yang terhubung dengan jaringan. Suatu web server akan menyimpan IP address ketika diminta sesuatu pada web page. Hal ini yang sebenarnya akan berfungsi sebagai alamat dimana web server akan mengatahui dimana dan dikirim sesuatu yang diminta oleh user. Semua jaringan komputer akan melakukan penyimpanan IP address (baik itu untuk sementara maupun selamanya) supaya bisa mengirim data ke alamat IP yang sudag terdaftar. Setiap komputer dalam sautu

jaringan mempunyai identifikasi yang unik, yaitu pengalamatan dalam sebuah protocol TCP/IP. IP Address merupakan bilangan biner 32 bit yang dipisahkan oleh tanda pemisah berupa tanda titik pada setiap 8 bitnya. Setiap 8 bit disebut *octet*. Pengalamatan IP berupa nomor 32 bit yangterdiri dari alamat subnet dan host, inilah yang disebut dengan *IP Address*.

Suatu teknologi *firewall* mempunyai karakteristik tertentu dengan tujuan antara lain :

1). Segala lalu lintas jaringan baik dari dalam maupun dari luar harus melewati *firewall*. Hal akan menghalangi semua akses dalam bentuk apapun kecuali melewati *firewall*.
2). Kebijakan keamanan, hanya akan memberikan izin untuk masuk ke server jaringan komputer yang memenuhi syarat tertentu.
3). *Firewall* sendiri bebas terhadap penetrasi, ini menandakan bahwa suatu sistem yang dapat dipercayai dan menjamin keamanan data. Ketiga kriteria *firewall* tersebut dapat mengendalikan akses dan mendukung suatu kebijakan keamanan informasi, yang lebih difokuskan pada *Service Control*, seperti 1).*Service control*, untuk menentukan type layanan internet yang bisa diakses.
2). *Direction control*, yang menentukan arah layanan mana yang harus lebih dulu dan mana yang diizinkan untuk melewati *firewall*.
3). *User control*, control terhadap akses terhadap user yang bisa mengakses *firewall* untuk masuk ke dalam sistem jaringan, khususnya user yang ada dalam *firewall* atau *local user*.
4). *Behavior control*, service khusus yang akan digunakan seperti *E-mail* yang dilakukan filter oleh *firewall* yang tidak diizinkan untuk ke *server* komputer. Teknologi *firewall* untuk kemanan jaringan komputer atau internet dapat digambarkan sebagai berikut :



Gambar.1. Penggunaan firewall pada pengamanan jaringan komputer

Penggunaan teknologi *firewall* diharapkan akan membantu di dalam melakukan pengamanan terhadap data pada jaringan komputer. *Firewall* mempunyai beberapa fungsi dasar, antara lain : 1). Sebagai dinding pengahambat yang tidak mengizinkan user yang tidak punya hak terhadap jaringan komputer untuk melakukan akses, guna melindungi dari hal-hal yang tidak diinginkan. 2). Untuk melakukan monitor kejadian-kejadian yang berhubungan dengan keamanan sistem, yang akan memberikan keterangan kepada sistem seperti : *file log*, alarm yang semua dapat diimplementasikan oleh *system firewall*. 3). Sebagai *platform* dari fungsi internet yang tidak aman, meliputi menterjemahkan alamat jaringan dari local ke alamat internet. 4). Melayanai *platform* untuk *Ipsec* dengan menggunakan *tunnel mode* dan *firewall* yang juga bisa digunakan untuk *vitual private network* (VPN).

Terdapat beberapa macam *type firewall*, dimana masing-masing *type firewall* mempunyai keunggulan dan kelemahan. Secara umum type firewall dapat dibagi tiga yaitu : 1). *Packet Filter Router*. 2). *Application Level Gateway*. 3). *Circuit Level Gatway*.

Firewall dengan *type Packet Follter Router*, menggunakan beberapa ketentuan untuk packet IP, yang mana boleh masuk dan yang mana harus ditolak. *Router* hanya mengatur packet yang telah difilter dengan baik dari jaringan internal maupun ekternal. Beberapa informasi yang disaring melalui suatu packet jaringan diantaranya yaitu : 1). Sumber IP address. 2). Tujuan IP address. 3). IP Protokol dan 4). *Interface*

Packet filter dapat diimplementasikan tanpa instruksi yang lengkap dari *firewall* dan ini banyak tersedia secara gratis diinternet *tool packet filter* seperti 1.) *TCP_Wrappers*,tool ini dapat di pada ftp://ftp.win.tue.n1/pub/security/tcp_wrappers_7.4.tar.gz. 2).*NetGate*, yang dapat didownload pada tool http://hosaka.smallworks.com/netgate/packetfilterin g.html 3). *Internet Packet Filter* yang dapat dilakukan download dengan menggunakan bantuan peralatan tool ftp://coombs.anu.edu.au:/pub/net/kernel/ip_fil3.0.4.tar.gz , 4). *Netlog* , dapat di download pada tool ftp://coast.cs.purdue.edu/pub/tools/unix/tamu/ dan yang lainnya.

Application level gateway juga bisa dikenal dengan *aplikasi proxy firewall*. Pada type ini user harus melakukan kontak dengan getway yang menggunakan aplikasi TCP/IP seperti *TelNet* atau FTP dan gateway yang akan meminta user memasukkan nama dari *remote host* untuk melakukan akses. Jika user memberiakan ID yang falid dan informasi tentang hak akses (*authentication*), gateway yang akan melakukan kontak ke *remote host* dan akan membalas pesan

segment yang dapat digunakan untuk menghubungkan satu host dengan yang lainnya. *Application level gateway* pada dasarnya hanya menggunakan satu *geteway* yang saling berhubungan, hal ini memungkinkan secure dari suatu sistem dapat terjaga dengan baik.Tetapi pengiriman data dari satu host ke host lainnya lebih lambat dibandingkan dengan *packet level router*.

IP antara internet dan internal sistem. Keuntungan dari *proxy server* kemampuan untuk menterjemahkan alamat jaringan (*Network Address Translation* –NAT) yang selalu menyembunyikan alamat IP internal dari jarinan internet, keuntungan utama lainnya adalah adanya layanan keamanan administrator dengan kemampuan yang fleksibel ketika dikembangkan dari sebuah schema alamat jaringan internal jaringan. *Circuit level gateway* pada dasarnya hampir mirip dengan *packet filter firewall*.

4. Penutup

Ketika jaringan internal mengirim packet ke jaringan internet melewati *circuit level gateway* dan dilakukan pengecekan terhadap aturan yang diabaikan oleh administrator, jika packet tidak memenuhi aturan yang diberikan maka packet akan dikirim kembali ke jaringan internal. Proses ini melindungi informasi yang tidak diproteksi dari jaringan internet, dan jika aturan tidak dibuat maka informasi yang tidak diinginkan dikeluarkan dari jaringan *internal* akan bisa tersebar di *internet*.

Circuit level gateway merupakan sistem *proxy server* secara statis menggambarkan lalu lintas jaringan apa yang akan disampaikan. *Circuit proxy* selalu mengizinkan packet yang berisi port number yang dizinkan oleh aturan *policy* (kebijakan), *circuit level gateway* berjalan pada level jaringan model OSI, yang mempunyai tugas untuk menterjemahkan alamat

Pada konteks sistem jaringan komputer atau internet, setiap user tidak mungkin bisa mengakses semua service yang tersedia di internet, hal ini disebabkan user mempunyai tingkat hak akses yang diberikan, jika semua pemakai mempuyai hak akses terhadap semua service yang ada, maka keamanan dari jaringan komputer tersebut tidak berfungsi. Untuk itu harus ada perlakuan khusus yang diberikan khusus kepada para administrator jaringan terhadap user dengan tujuan untuk menjaga agar keamanan jaringan tersebut bisa terjaga, walaupun ini bukan merupakan satu-satunya cara yang bisa mengamankan informasi. Dengan adanya perlakuan khusus pada segi keamanan jaringan komputer ataupun internet akan meminimalkan resiko terhadap serangan, baik dari dalam maupun dari luar jaringan tersebut.

[1] Tanutama, Lukas, 1995. Pengantar Komunikasi Data, Edisi kelima; PT. Elexmedia Komputindo; Gramedia Jakarta.

[2] Ariyus, Doni, 2006. Technology Internet Firewall, Graha Ilmu; Edisi Pertama;Yokyakarta

[3] Sopandi, Dede, 2004. Instalasi dan Konfigurasi Jaringan Komputer; Edisi pertama; Informatika; Bandung.