
FIREWALL SEBAGAI PENGAMAN INTRANET

JUFRIADIF NA`AM

Dosen Tetap Fakultas Ilmu Komputer (FILKOM)

Universitas Putra Indonesia "YPTK" Padang

2003

Abstract

Intranet is an adoption of internet technology connecting local computer network to all computer networks in the world. Intranet is object to the attacks of computer system security. A technique that can solve the problem is by using Firewall technology consisting of three basic architectures i.e dual ported host, screened host, and screened subnet. By using one of the firewall architectures, each computer system in the intranet computer network is secure from the attack.

Keyword:

Intranet, internet, internetworking, LAN, network security, TCP/IP, vulnerability, read access, write access, denial of service, dual ported host, screened host, screened subnet

I. Pendahuluan

Intranet adalah konsep Local Area Network (LAN) yang mengadopsi teknologi Internet, diperkenalkan pada akhir tahun 1995. Kuo Yao Tung (1997) mengatakan : Intranet adalah LAN yang menggunakan standar komunikasi dan segala fasilitas Internet, diibaratkan berInternet dalam lingkungan lokal. Intranet umumnya juga terkoneksi ke Internet sehingga memungkinkan pertukaran informasi dan data dengan jaringan Intranet lainnya (Internetworking) melalui backbone Internet. Kompatibilitas Intranet (sebagaimana Internet) sangat tinggi terhadap sistem lainnya sehingga mudah diterapkan, dipelajari, dikembangkan dan dikonfigurasi ulang. Dukungan aplikasi, program dan sistem operasi yang luas akibat dari popularitas Internet menjadikan Intranet sebagai masa depan LAN.

Salah satu hal terpenting dalam Intranet adalah keamanan jaringan (network security). Isu ini sensitif mengingat jaringan telekomunikasi komersial yang dipakai bersifat umum (public service communication network) sehingga rentan penyusupan dan penyadapan jaringan serta pembajakan data. Sejumlah teknologi keamanan canggih terus dikembangkan seperti firewall, enkripsi, encapsulated data packet, id recognition dan sebagainya, sehingga menjadi kelebihan tersendiri ketika diterapkan dalam Intranet. Berbeda dengan LAN yang menggunakan jaringan komunikasi terproteksi (VPN - Virtual Private Network) sehingga keamanannya relatif lebih terjaga sehingga cukup memakai teknologi enkripsi saja. Terminologi yang lebih berkembang dari Intranet adalah teknologi Extranet yang memiliki pengertian suatu jaringan Intranet yang dapat diakses dari luar baik melalui VPN maupun media komunikasi umum.

Internet merupakan sebuah network of network yang terhubung ke seluruh dunia dengan menggunakan protokol TCP/IP (Transmission Control Protokol/Internet Protokol) untuk berkomunikasi. Internet awalnya digunakan untuk penelitian yang di biayai oleh pemerintahan Amerika Serikat sepanjang dekade 1980, kemudian berkembang secara merata dengan pesatnya keseluruh dunia. Internet tumbuh menjadi fenomenal dengan penambahan jumlah koneksi lebih cepat dari jaringan yang pernah diciptakan seperti jaringan telepon. Jutaan user yang terhubung ke dunia internet, secara kasar separuhnya telah menjadikan bisnis yang baru.(Vinton Cerf,1993)

Dalam beberapa tahun terakhir ini Internet tidak saja berkembang sebagai salah satu media untuk memperoleh dan menyebarkan informasi, tetapi juga berkembang

sebagai suatu landasan teknologi baru yang diterapkan pada lingkungan perusahaan atau organisasi. Perkembangan Internet dan jaringan internal yang semakin pesat menuntut adanya pengamanan terhadap jaringan internal dari kemungkinan adanya serangan dari jaringan eksternal. Untuk perusahaan-perusahaan besar tidak akan mungkin mengambil resiko kehancuran sistem komputerisasi yang telah ada. Untuk menghindari hal itu, maka diperlukan suatu sistem keamanan yang kuat.

Konsep dasar keamanan jaringan menjelaskan lebih banyak mengenai keterjaminan (security) dari sebuah sistem jaringan komputer yang terhubung ke Internet terhadap ancaman dan gangguan yang ditujukan kepada sistem tersebut. Sebenarnya, masalah Network Security ini timbul dari konektivitas jaringan komputer lokal yang kita miliki dengan wide-area network (seperti Internet). Jadi, selama jaringan lokal komputer kita tidak terhubung kepada wide-area network, masalah Network Security tidak begitu penting. Tetapi hal ini bukan berarti memberikan arti bahwa bergabung dengan wide-area network adalah suatu hal yang ‘menakutkan’ dan penuh bahaya. Network Security hanyalah menjelaskan kemungkinan-kemungkinan yang akan timbul dari konektivitas jaringan komputer lokal kita dengan wide-area network.

Secara umum, terdapat 3 (tiga) kata kunci dalam konsep Network Security ini, yaitu:

1. Resiko dan tingkat bahaya
2. Ancaman
3. Kerapuhan sistem (vulnerability)

Resiko Dan Tingkat Bahaya

Dalam hal ini, resiko berarti berapa besar kemungkinan keberhasilan para penyusup dalam rangka memperoleh akses ke dalam jaringan komputer lokal yang dimiliki melalui konektivitas jaringan lokal ke wide-area network. Secara umum, akses-akses yang diinginkan adalah :

- a) *Read Access* : Mampu mengetahui keseluruhan sistem jaringan informasi.
- b) *Write Access* : Mampu melakukan proses menulis ataupun menghancurkan data yang terdapat di sistem tersebut.
- c) *Denial of Service* : Menutup penggunaan utilitas-utilitas jaringan normal dengan cara menghabiskan jatah CPU, bandwidth maupun memory.

Ancaman

Dalam hal ini, ancaman berarti orang yang berusaha memperoleh akses-akses ilegal terhadap jaringan komputer yang dimiliki seolah-olah ia memiliki otoritas terhadap akses ke jaringan komputer.

Kerapuhan Sistem

Kerapuhan sistem lebih memiliki arti seberapa jauh proteksi yang bisa diterapkan kepada network yang dimiliki dari seseorang dari luar sistem yang berusaha memperoleh akses ilegal terhadap jaringan komputer tersebut dan kemungkinan orang-orang dari dalam sistem memberikan akses kepada dunia luar yang bersifat merusak sistem jaringan.

II. Teknologi Firewall

Firewall merupakan sebuah teknologi yang dapat mencegah penyusup masuk kedalam sistem jaringan, dengan menggunakan Internet atau sistem jaringan lainnya, mengakses data atau aplikasi pada komputer anda yaitu dengan cara menolak data atau transmisi yang tidak diotorisasi masuk ke dalam sistem jaringan internal. Sebuah firewall

mempelajari setiap paket data yang dikirim dari atau ke komputer kita dan melihatnya apakah sesuai dengan kriteria yang diberikan. Firewall kemudian akan menyeleksi paket mana yang bisa lewat atau yang harus diblok.

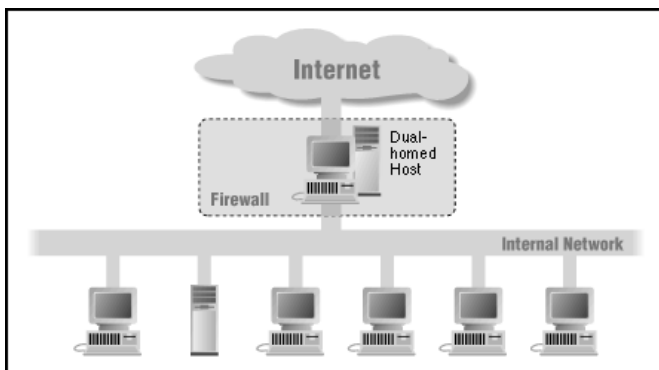
Firewall (dari buku *Building Internet Firewalls*, oleh Chapman dan Zwicky) didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dari internet, atau antara kumpulan-kumpulan jaringan lainnya. Firewall dapat berupa hardware dalam bentuk Router atau PC Router, atau software yang menjalankan sistem gateway, atau kombinasi keduanya. Dengan menggunakan firewall maka kita dapat memproteksi paket-paket data yang dikirim ke jaringan internal.

Tujuan utama *Firewall* digunakan adalah untuk memastikan sumber-sumber yang tidak dipercayai yang berada di jaringan external memasuki dan menyusup kedalam jaringan internal. Secara umumnya boleh dikatakan bahwa *Firewall* mengimplementasikan keamanan sistem jaringan sehingga membatasi hak-hak akses bagi dunia jaringan internal maupun external. Maka, implementasi *Firewall* perlulah memilih sifat komuniti *Firewall* yang sesuai yang dapat mencapai tujuan kita terhindar dari gangguan pihak-pihak yang tidak diizinkan untuk masuk kedalam lingkungan internal kita.

Ada beberapa arsitektur firewall. diantaranya, yaitu: Dual Ported Host, Screened Host dan Screened Subnet.

A. *Dual Ported Host*

Arsitektur Dual Ported host dibuat disekitar komputer dual-homed host, yaitu komputer yang memiliki paling sedikit dua interface jaringan. Untuk mengimplementasikan tipe arsitektur dual Ported host, fungsi routing pada host ini di non-aktifkan. Sistem di dalam dan di luar firewall dapat berkomunikasi dengan dual ported host, tetapi kedua sistem ini tidak dapat berkomunikasi secara langsung.

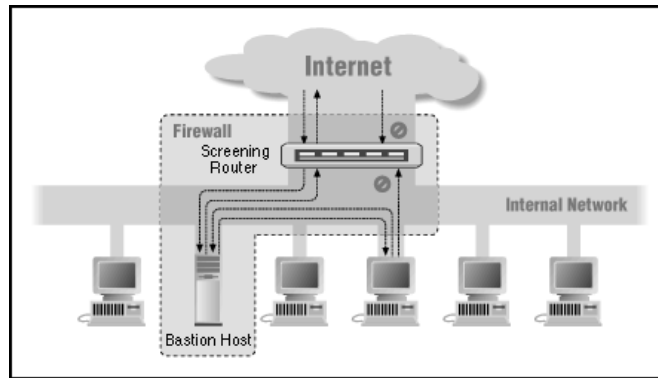


Gambar 1. Arsitektur dual-Ported host

Dual Ported host dapat menyediakan service hanya dengan menyediakan Proxy pada Host tersebut, atau dengan membiarkan user melakukan logging secara langsung pada Dual Ported Host.

B. *Screened Host*

Arsitektur Screened Host menyediakan service dari sebuah Host pada jaringan internal dengan menggunakan Router yang terpisah. Pada arsitektur ini, pengamanan utama dilakukan dengan package filtering.

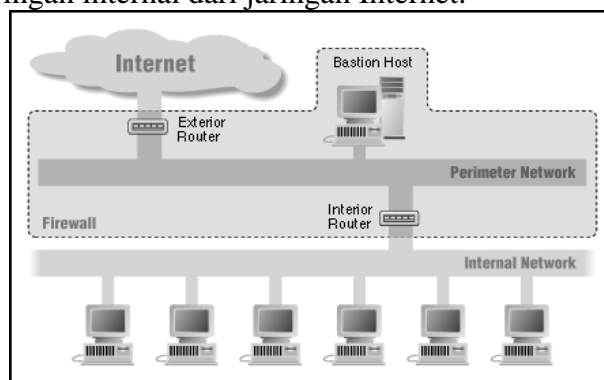


Gambar 3.2 . Arsitektur screened host

Bastion host berada dalam jaringan internal. Packet filtering pada screening router dikonfigurasi sehingga hanya bastion host yang dapat melakukan koneksi ke Internet (misalnya mengantarkan mail yang datang) dan hanya tipe-tipe koneksi tertentu yang diperbolehkan. Tiap sistem eksternal yang mencoba untuk mengakses sistem internal harus berhubungan dengan host ini terlebih dulu. Bastion host diperlukan untuk tingkat keamanan yang tinggi.

C. Arsitektur Screened Subnet

Arsitektur screened subnet menambahkan sebuah layer pengaman tambahan pada arsitektur screened host, yaitu dengan menambahkan sebuah jaringan perimeter yang lebih mengisolasi jaringan internal dari jaringan Internet.



Gambar 3.3. Arsitektur screened subnet

Jaringan perimeter mengisolasi bastion host sehingga tidak langsung terhubung ke jaringan internal. Arsitektur screened subnet yang paling sederhana memiliki dua buah screening router, yang masing-masing terhubung ke jaringan perimeter. Router pertama terletak di antara jaringan perimeter dan jaringan internal, dan router kedua terletak di antara jaringan perimeter dan jaringan eksternal (biasanya Internet). Untuk menembus jaringan internal dengan tipe arsitektur screened subnet, seorang intruder harus melewati dua buah router tersebut sehingga jaringan internal akan relatif lebih aman.

III. Kesimpulan

Dalam beberapa tahun terakhir ini Internet tidak saja berkembang sebagai salah satu media untuk memperoleh dan menyebarkan informasi, tetapi juga berkembang sebagai suatu landasan teknologi baru yang diterapkan pada lingkungan perusahaan atau organisasi. Perkembangan Internet dan jaringan internal yang semakin pesat menuntut adanya pengamanan terhadap jaringan internal dari kemungkinan adanya serangan dari jaringan eksternal. Untuk perusahaan-perusahaan besar tidak akan mungkin mengambil resiko kehancuran sistem komputerisasi yang telah ada. Untuk menghindari hal itu, maka diperlukan suatu sistem keamanan yang kuat.

Dengan menggunakan Firewall maka berapa komputer yang terhubung ke internet akan dapat memproteksi jaringan internal terhadap serangan dari jaringan eksternal yang akan merusak sistem jaringan kita yang terhubung ke Internet. Diharapkan nantinya sistem keamanan jaringan yang menghindari kehilangan data dari ancaman Hacker (Unauthentication).

Daftar Pustaka

1. Lawrie Brown, *Lecture Notes for Use with Network and Internetwork Security by William Stallings*, on-line document. <http://www1.shore.net/~ws/Security-Notes/index.html>
2. Onno W. Purbo, *Keamanan Jaringan Internet*, Elex Media Komputindo, Jakarta, 2000
3. Computer Security Institute, *1999 CSI/FBI Computer Crime and Security Survey*, CSI, Winter 1999. <http://www.gocsi.com>
4. John D. Howard, *An Analysis of Security Incidents on the Internet 1989-1995*, PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 1997
5. G.J Simson, dan Gene Spafford, *Practical UNIX & Internet Security*, O'Reilly & Associates, Inc., 2nd edition, 1996
6. Budi Rahardjo, *Keamanan Sistem Informasi: Beberapa Topik Keamanan di Internet*, Seminar Informasi Infrastruktur Nasional, ITB, 1997
7. William Stallings, *Network and Internetwork Security*, Prentice Hall, 1995
8. Simson Garfinkel, *PGP: Pretty Good Privacy*, O'Reilly & Associates, Inc., 1995
9. <http://www.2600.com>
10. <http://www.cert.org>
11. <http://www.bogor.net/idkf>